Splunk® IT Service Intelligence
Install and Upgrade Manual 4.16.0 Cloud only

Generated: 5/04/2023 9:04 pm

Table of Contents

Introduction

About Splunk IT Service Intelligence

Splunk IT Service Intelligence (ITSI) uses the Splunk platform's searching and reporting capabilities to provide IT operations analysts with an overall view of their organization's service health. ITSI is built on the Splunk operational intelligence platform and uses the search and correlation capabilities of the platform to enable you to collect, monitor, and report on data from IT devices, systems, and applications. As issues are identified, analysts can quickly investigate and resolve them. ITSI provides visibility into your services, actionable insight into the performance of your IT operations, and features for tracking alerts. You can capture, monitor, and report on data from devices, systems, and applications across your environment. As issues are identified, analysts can quickly investigate and resolve them.

Use IT Service Intelligence to do the following:

- Monitor the health of your services with the Service Analyzer
- Triage and investigate issues using Episode Review
- Troubleshoot issues using deep dives

This manual is written for a user capable of installing, configuring, and administering Splunk software. If you need training on the Splunk platform and IT Service Intelligence, see Splunk Training and Certification.

Other manuals for Splunk IT Service Intelligence include the following:

- *Release Notes*
- *Administration Manual*
- *Entity Integrations Manual*
- *Service Insights Manual*
- *Event Analytics Manual*
- *Modules*
- *REST API Reference*

Share data in Splunk IT Service Intelligence

When Splunk IT Service Intelligence is deployed on Splunk Enterprise, the Splunk platform sends usage data to Splunk Inc. ("Splunk") to help improve Splunk IT Service Intelligence in future releases. For information about how to opt in, and how the data is collected, stored, and governed, see Share data in Splunk Enterprise.

What data is collected

Splunk IT Service Intelligence collects the following basic usage information:

Component	Description	Exampl

`app.ITSI.performanceMetrics`	Reports the time taken for a specific method to finish and non-identifiable supporting	`{`
		`app: itsi`
		`component: app.ITSI.performanceMe`
		`data: {`
		`averageTime: 1.616857230663299`

Component	Description	Exampl
	parameters to clean up the data (measured per 24 hours).	cumulativeTime: 6.467428922653 medianTime: 1.1328552961349487 method: itoa_object.get_bulk numberOfObjects: 1012 numberOfTransactions: 4 p90Time: 2.975279831886292 } deploymentID: 616ee3e9-532b-5b32- eventID: 9157E0BA-1A2A-48CC-A738- executionID: 38A07E6C-2CA7-4B6A-8 optInRequired: 3 timestamp: 1592906482 type: aggregate visibility: [support anonymous] }

app.ITSI.entityTypes	Reports the number of entities for each entity type (custom entity types are hashed).	{
		app: itsi
		component: app.ITSI.entityTypes
		data: {
		countOfAssociatedEntities: 10
		entityTypeIds:
		a0745f7ed88cfac6058d1d4cfb57bc71127a
		}
		deploymentID: 417a2431-e14d-5550-
		eventID: 51F77E4B-D866-49FB-B2F5-
		executionID: 661BB29D-A390-4B40-B
		optInRequired: 3
		timestamp: 1592820124
		type: aggregate
		visibility: [
		anonymous
		support
		]
		}

app.ITSI.entityTypeToEntityRatio	Ratio of in-use entity types to entities.	{
		app: itsi
		component: app.ITSI.entityTypeToE
		data: {
		entityTypeToEntityRatio: 0.0007
		numberOfEntities: 5028
		numberOfEntityTypes: 4
		}
		deploymentID: 616ee3e9-532b-5b32-
		eventID: BAC39F03-20BB-4D88-969F-
		executionID: 38A07E6C-2CA7-4B6A-8
		optInRequired: 3
		timestamp: 1592906593
		type: aggregate
		visibility: [
		support
		anonymous
		]
		}

Component	Description	Exampl
app.ITSI.serviceToEntityRatio	Reports the ratio of in-use services to entities.	{ app: itsi component: app.ITSI.serviceToEnti data: { numberOfEntities: 128 numberOfServices: 8 serviceToEntityRatio: 0.0625 } deploymentID: 639ae7f7-0af0-5a0f- eventID: 6A71F467-B4FE-4D4C-99F4- executionID: EC2EE972-58C2-441F-9 optInRequired: 3 timestamp: 1592820188 type: aggregate visibility: [anonymous support] }
app.ITSI.kpiToEntityRatio	Reports the ratio of in-use KPIs to entities.	{ app: itsi component: app.ITSI.kpiToEntityRa data: { kpiToEntityRatio: 0.206896551724 numberOfEntities: 87 numberOfKpis: 18 } deploymentID: 121370bf-b9ce-54c5- eventID: 3341F59D-8290-4683-B4A9- executionID: CC1CAA21-78DD-46C5-B optInRequired: 3 timestamp: 1592733807 type: aggregate visibility: [anonymous support] }
app.ITSI.sharedBaseSearchToEntityRatio	Reports the ratio of in-use shared base searches to entities.	{ app: itsi component: app.ITSI.sharedBaseSea data: { numberOfEntities: 25080 numberOfSharedBaseSearches: 5 sharedBaseSearchToEntityRatio: } deploymentID: 616ee3e9-532b-5b32- eventID: 8F418716-926D-4D67-B31A- executionID: 38A07E6C-2CA7-4B6A-8 optInRequired: 3 timestamp: 1592906664 type: aggregate visibility: [support

Component	Description	Exampl
		anonymous] }

app.ITSI.serviceAssociatedEntityToServiceUnassociatedEntityRatio	Reports the number of entities by service association.	{
		app: itsi
		component:
		app.ITSI.serviceAssociatedEntityToSe
		data: {
		numberOfServiceAssociatedEntiti
		numberOfServiceUnassociatedEnti
		serviceAssociatedEntityToServic
		}
		deploymentID: 616ee3e9-532b-5b32-
		eventID: 965EC96C-33E4-44E2-B885-
		executionID: 38A07E6C-2CA7-4B6A-8
		optInRequired: 3
		timestamp: 1592906664
		type: aggregate
		visibility: [
		anonymous
		support
		]
		}

app.session.ITSI.pageLoad	Reports the time taken for a React component to load with associated metadata.	{
		component: app.session.ITSI.pageI
		data: {
		app: itsi
		loadTime: 18398.775000008754
		metadata: {
		activeTabId: EVENT_DATA_SEARC
		isInitialAppMount: true
		}
		mode: development
		page: entity_detail
		}
		deploymentID: 2b623070-88c3-51a2-
		eventID: 768b9773-57c9-9549-5527-
		experienceID: 8268d610-95d7-5a6d-
		optInRequired: 3
		timestamp: 1592356630
		userID:
		5f4dba230c6b7e300aec79ea85261914c069
		version: 4
		visibility: anonymous,support
		}

app.session.pageView	Reports the pages a user has visited.	{
		component: app.session.pageview
		data: {
		app: itsi
		page: notable_event_aggregation
		}
		deploymentID: 0e55c2be-a373-5e5f-
		eventID: e4df5657-d13f-8f66-3958-
		experienceID: 6cac0958-68e6-5a3b-

Component	Description	Exampl
		optInRequired: 3 timestamp: 1592850392 userID: 36966f73a802b0f3e37b385983f3d21d556b version: 4 visibility: anonymous,support }
app.session.udf.telemetry	Reports information about visualizations and configurations that users implement in beta glass tables.	component: app.session.udf.telemetry data: { [-] app: itsi definition: { [-] inputs: { [-] input1: { [-] options: { [-] items: 3 } titleLength: 6 type: input.dropdown } } layout: { [-] globalInputs: [[-] input1] options: { [-] height: 750 width: 1300 } structure: [[-] { [-] item: viz_eGQh2uAJ position: { [-] h: 730 w: 1280 x: 10 y: 10 } type: block } { [-] item: viz_2WcVmXz0 position: { [-] h: 450 w: 770 x: 260 y: 20 } type: block] type: absolute } titleLength: 26 visualizations: { [-] viz_2WcVmXz0: { [-] options: { [-] preserveAspectRatio: tr src: true }

Component	Description	Exampl
		type: viz.img } viz_5HKW2R1q: { [-] options: { [-] legend.placement: top } titleLength: 29 type: viz.line } } } definitionInfo: { [-] componentCounts: { [-] dataSourceTypeCounts: { [-] ds.test: 11 } inputTypeCounts: { [-] input.dropdown: 1 } vizTypeCounts: { [-] abslayout.line: 6 viz.img: 1 viz.line: 2 viz.rectangle: 1 viz.singlevalue: 8 viz.table: 1 viz.text: 3 } } numDataSources: 11 numInputs: 1 numViz: 22 } page: boston_marathon__absolute pageAction: dashboard.initializ udfVersion: 5.2.0 } deploymentID: e5fc210a-8e27-54b6- eventID: 40c251b1-09ad-cb2d-cb64- experienceID: 10fa783d-65c5-0ece- timestamp: 1569281682 userID: 0b9a7eef9855fe028ae96a4eeea30356bdd6 version: 3 visibility: anonymous,support

app.ITSI.entityLifecycleManagement	Number of entity lifecycle management policies having auto retire feature enabled on the Splunk system.	{
		"timestamp":1648091047,
		"component":"app.ITSI.entityLifec
		"executionID":"64FB8F4D-5BB9-4D0E
		"data":{
		"countOfRetirableEntities":0,
		"countOfEntityTypesUnderManage
		"countOfDisabledEntityManageme
		"countOfEnabledEntityManagemen
		"countOfEntitiesUnderManagemen
		"countOfRetiredEntities":2,
		"countOfAutoRetireEntityManage
		"avgPolicyRunTime":4.65,

Component	Description	Exampl
		"avgPolicyLookbackPeriod":26 }, "optInRequired":3, "visibility":["anonymous", "support"], "eventID":"0F66ABC6-83C4-4CD2-B76 "type":"aggregate", "deploymentID":"91182b71-8c10-501 "app":"itsi" }

app.ITSI.calculationWindowUsage	Information about the types of calculation windows in ITSI.	{
		app: itsi
		component: app.ITSI.calculationWi
		data: {
		customWindow: {
		calculationWindowValueCount:
		{
		calculationWindowValue: 3
		count: 1
		}
		]
		totalCount: 1
		}
		predefinedWindow: {
		calculationWindowValueCount:
		{
		calculationWindowValue: 5
		count: 8
		}
		]
		totalCount: 8
		}
		}
		deploymentID: a3b9b625-8392-5205-
		eventID: 4ECEA390-74EB-48CF-B387-
		executionID: 110B8DAD-B7F2-4E8B-8
		optInRequired: 3
		timestamp: 1665082511
		type: aggregate
		visibility: [
		anonymous
		support
		]
		}

app.ITSI.knowledgeObjectsCounts	Provides a count of various knowledge objects in ITSI.	{
		"data":{
		"knowledgeObjects":{
		"authoredContentPacks": {
		"totalCount": 1
		},
		"eventManagementStates":{
		"totalCount":6,
		"privateCount":0,
		"publicCount":6

Component	Description	Exampl


```
},
"glassTables":{
   "privateCount":0,
   "publicCount":2,
   "totalCount":2
},
"contentPacks":{
   "totalCount":1,
   "DA-ITSI-CP-CUST-639293
},
"services":{
   "kpis":{
      "adhocCount":2,
      "totalCount":1013,
      "sharedBaseSearchCou
      "dataModelCount":0,
      "metricsCount":0
   },
   "dependServicesCount":8
   "servicesLinkedToATempl
   "totalCount":96,
   "servicesNotInGlobal":2
},
"deepDives":{
   "publicCount":1,
   "privateCount":1,
   "totalCount":2
},
"correlationSearches":{
   "totalCount":7
},
"maintenanceWindows":{
   "totalCount":0
},
"homeViews":{
   "privateCount":0,
   "totalCount":11,
   "publicCount":11
},
"entityManagementRules":{
   "totalCount":1
},
"kpiBaseSearches":{
   "totalCount":99
},
"entityManagementPolicies"
   "totalCount":0
},
"authoredContentPacks":{
   "totalCount":1
},
"entityTypes":{
   "totalCount":10
},
"entities":{
   "totalCount":2216
},
"kpiTemplates":{
   "totalCount":33
```

Component	Description	Exampl

		},
		"notableEventAggregationPol
		"totalCount":6
		},
		"customThresholdWindows":{
		"totalCount":0
		},
		"kpiThresholdTemplates":{
		"totalCount":36
		},
		"teams":{
		"totalCount":5
		},
		"serviceTemplates":{
		"totalCount":10
		}
		}
		}
		}

Planning

Plan your ITSI deployment

Deploy Splunk IT Service Intelligence (ITSI) on a configured Splunk platform installation. Review the system and hardware requirements and the search head and indexer considerations before deploying IT Service Intelligence.

Preparation for deployment

Before you deploy IT Service Intelligence, perform the following steps:

1. Compile a list of services, KPIs, and glass table views that you want to create.
2. Compile a list of your entities. Entities are usually hosts, but can also be users, mobile devices, and so on. Entities for hosts must include, at a minimum, the IP address, host name, and designated role. For example, web, db, or app server.
3. Make sure your Splunk ITSI instance includes the default `admin` user. Deleting or renaming this user breaks ITSI installation and operation.
4. Verify your existing hardware performance using the following search query:

   ```
   index=_introspection sourcetype=splunk_resource_usage component=Hostwide earliest=-5m | timechart avg(data.cpu_user_pct) by host
   ```

   If the query takes more than 2-5 seconds to complete, check performance in the Job Inspector to investigate the issue. This slowness might indicate your current hardware is insufficient or badly configured, or you might have a high latency dispatch that requires architecture changes.
5. Confirm Splunk Enterprise version compatibility. See the Splunk products version compatibility matrix.

Available deployment architectures

You can deploy Splunk IT Service Intelligence in a single instance deployment or a distributed search deployment. Splunk IT Service Intelligence is also available in Splunk Cloud Platform. Before you deploy Splunk IT Service Intelligence on premises, familiarize yourself with the components of a Splunk platform deployment. See Components of a Splunk Enterprise deployment in the *Capacity Planning Manual*.

Single instance deployments

For a simple and small deployment, install ITSI on a single Splunk platform instance. A single instance functions as both a search head and an indexer. Use forwarders to collect your data and send it to the single instance for parsing, storing, and searching.

You can use a single instance deployment for a lab or test environment, or a small system with one or two users running concurrent searches. For instructions on installing ITSI on a single Splunk Enterprise instance, see Install Splunk IT Service Intelligence on a single instance.

Distributed deployments

You can deploy ITSI across any distributed architecture supported by Splunk Enterprise. This includes all types of deployment topologies, from small departmental deployments using a single instance for both indexer and search head, to large enterprise deployments using several search heads, dozens of indexers, and hundreds of forwarders. See Types of

distributed deployments in the Splunk Enterprise *Distributed Deployment Manual*.

- For information about installing ITSI in a distributed environment, see Where to install IT Service Intelligence in a distributed environment.
- Improve search performance by using an index cluster and distributing the workload of searching data across multiple nodes. Using multiple indexers allows both the data collected by the forwarders and the workload of processing the data to be distributed across the indexers.
- Use forwarders to collect your data and send it to the indexers.

In a distributed search deployment, and to implement search head clustering, configure the search head to forward all data to the indexers. See Best practice: Forward search head data to the indexer layer in the Splunk Enterprise *Distributed Search* manual.

To properly scale your distributed search deployment with ITSI, see Introduction to capacity planning for Splunk Enterprise in the *Capacity Planning Manual* and Indexer and search head sizing examples.

Cloud deployments

Splunk IT Service Intelligence is available as a service in Splunk Cloud Platform. The Splunk Cloud Platform deployment architecture varies based on data and search load. Splunk Cloud Platform customers work with Splunk Support to set up, manage, and maintain their cloud infrastructure. For information on Splunk Cloud Platform deployments, see Splunk Cloud Platform deployment types in the *Splunk Cloud Platform Admin Manual*.

Splunk Enterprise system requirements

Splunk IT Service Intelligence requires a 64-bit OS install on all search heads and indexers. For a list of supported operating systems, browsers, and file systems, see System requirements for use of Splunk Enterprise on-premises in the Splunk Enterprise *Installation Manual*.

Use this table to determine the compatibility of the IT Service Intelligence versions and Splunk platform versions. Cloud only versions of ITSI are not listed on this table. To determine compatibility with Splunk Cloud Platform versions, see Splunk Cloud Platform system requirements.

ITSI is incompatible with Splunk Enterprise versions 7.2.0 - 7.2.3.

Splunk IT Service Intelligence version	Splunk platform version
4.15.x **Note:** If you plan to upgrade to Python 3, you must be on Splunk Enterprise version 8.x. For more information, see Python 3 migration with ITSI.	**9.0.x** **8.2.x** **8.1.x**
4.13.x If you plan to upgrade to Python 3, you must be on Splunk Enterprise version 8.x. For more information, see Python 3 migration with ITSI.	**9.0.x** **8.2.x** **8.1.x**
4.11.x **Note:** If you plan to upgrade to Python 3, you must be on Splunk Enterprise version 8.x. For more information, see Python 3 migration with ITSI.	**9.0.x** **8.2.x**

Splunk IT Service Intelligence version	Splunk platform version
	8.1.x
4.9.x If you plan to upgrade to Python 3, you must be on Splunk Enterprise version 8.x. For more information, see Python 3 migration with ITSI.	**8.2.x**
	8.1.x
	8.0.x

Workaround

To prevent ITSI Event Analytics from duplicating events on Splunk Enterprise versions **7.1.x** and **7.2.4** - **7.2.10**, create a `limits.conf` file on all search heads at `$SPLUNK_HOME/etc/apps/SA-ITOA/local/` and add the following stanza:

```
[search]
phased_execution_mode = auto
```

If you don't plan to use Event Analytics, the workaround isn't necessary.

Splunk Cloud Platform system requirements

Use this table to determine the compatibility of the IT Service Intelligence versions and Splunk Cloud Platform versions.

Splunk IT Service Intelligence version	Splunk Cloud platform version
4.16.x (Cloud only) **Note:** If you plan to upgrade to Python 3, you must be on Splunk Enterprise version 8.x. For more information, see Python 3 migration with ITSI.	**9.0.2209, 9.0.2208**
4.15.x If you plan to upgrade to Python 3, you must be on Splunk Enterprise version 8.x. For more information, see Python 3 migration with ITSI.	**9.0.2209, 9.0.2208, 9.0.2205**
	8.2.2203, **8.2.2201**
4.14.x (Cloud only) **Note:** If you plan to upgrade to Python 3, you must be on Splunk Enterprise version 8.x. For more information, see Python 3 migration with ITSI.	**9.0.2209, 9.0.2208, 9.0.2205**
	8.2.2203, 8.2.2202
4.13.x If you plan to upgrade to Python 3, you must be on Splunk Enterprise version 8.x. For more information, see Python 3 migration with ITSI.	**9.0.2209, 9.0.2208, 9.0.2205**
	8.2.2203, 8.2.2202, 8.2.2201
4.12.x (Cloud only) **Note:** If you plan to upgrade to Python 3, you must be on Splunk Enterprise version 8.x. For more information, see Python 3 migration with ITSI.	**9.0.2209, 9.0.2208, 9.0.2205, 9.0.2203**
	8.2.2203, 8.2.2202, 8.2.2201
4.11.x If you plan to upgrade to Python 3, you must be on Splunk Enterprise version 8.x. For more information, see Python 3 migration with ITSI.	**8.2.2202**

Splunk IT Service Intelligence version	Splunk Cloud platform version
4.10.x (Cloud only) **Note:** If you plan to upgrade to Python 3, you must be on Splunk Enterprise version 8.x. For more information, see Python 3 migration with ITSI.	**8.2.2202, 8.2.2201**
4.9.x If you plan to upgrade to Python 3, you must be on Splunk Enterprise version 8.x. For more information, see Python 3 migration with ITSI.	**8.2.2201**
4.8.x (Cloud only) **Note:** If you plan to upgrade to Python 3, you must be on Splunk Enterprise version 8.x. For more information, see Python 3 migration with ITSI.	**7.2.4** - **7.2.10** **8.0.x** **8.1.x**
4.7.x If you plan to upgrade to Python 3, you must be on Splunk Enterprise version 8.x. For more information, see Python 3 migration with ITSI.	**7.2.4** - **7.2.10** **8.0.x** **8.1.x**

Hardware requirements

CPU core count and RAM are critical factors in indexer and search head performance. ITSI requires minimum hardware specifications that you increase according to your needs and usage of ITSI. These specifications also apply for a single instance deployment of ITSI.

Note that a search head in this case refers to a dedicated ITSI search head infrastructure. If ITSI shares a search head with other applications, additional resources are required beyond 16 cores and 12 GB of RAM.

Machine role	Minimum CPU	Minimum RAM	Minimum vCPU
Search head	16 cores required, 24+ recommended, or 32 vCPU at 2Ghz or greater speed per core	12 GB required, 16+ recommended	32 vCPU required, 48+ recommended
Indexer	16 cores	32 GB	32 vCPU required, 48+ recommended

Indexing is an I/O-intensive process. The indexers require sufficient disk I/O to ingest and parse data efficiently while responding to search requests. For the latest IOPS requirements to run Splunk Enterprise, see Reference Hardware: Indexer in the Splunk Enterprise *Capacity Planning Manual*.

You might need to increase the hardware specifications of your own ITSI deployment above the minimum hardware requirements depending on your environment. Depending on your system configuration, refer to the mid-range or high-performance specifications for Splunk platform reference hardware. See Mid-range specification and High-performance specification in the Splunk Enterprise *Capacity Planning Manual*.

If the number of indexer CPU cores in your deployment exceeds the minimum hardware specifications, you can implement one of the parallelization settings to improve the indexer performance for specific use cases. See Parallelization settings in the *Capacity Planning Manual*.

Operating system requirements

For a list of supported operating systems, browsers, and file systems, see System requirements for use of Splunk Enterprise on-premises in the Splunk Enterprise *Installation Manual*.

Ubuntu

When installing IT Service Intelligence on Ubuntu, use Bash shell. Do not use Dash shell as it can result in defunct processes.

ITSI license requirements

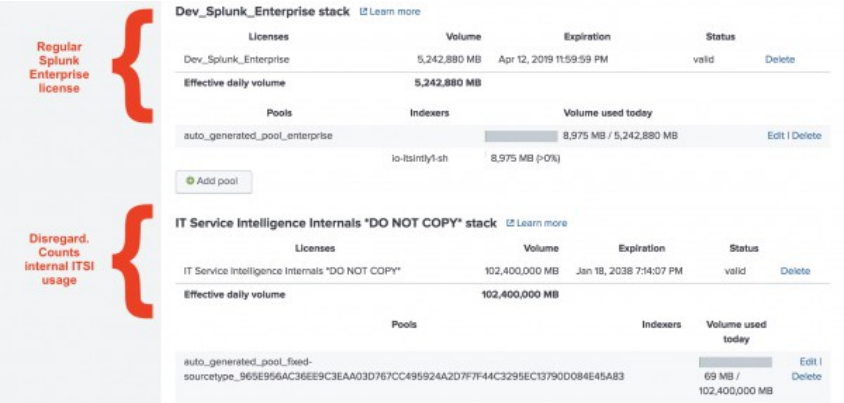
ITSI requires a separate ITSI license in addition to your Splunk Enterprise license. Install both the ITSI license and the Splunk Enterprise license on the license master. Your Splunk representative will provide you with an appropriate ITSI license at the time of purchase. For ITSI license installation instructions, see Install a license in the Splunk Enterprise *Installation and Configuration Manual*.

Splunk ITSI is a right-to-use (RTU) license. Splunk ITSI meters Splunk indexes for ingest-based license usage and capacity consumption calculations. These Splunk indexes are identified based on:

- Direct ingestion of data into Splunk and use of that data for ITSI use cases
- Indexes containing data used to populate ITSI KPIs

Once the indexes are identified, then license usage is measured on ingest calculation for data sources and indexes used by Splunk ITSI.

IT Service Intelligence ships with an internal **license stack** called the IT Service Intelligence Internals *DO NOT COPY* stack. Because ITSI Event Analytics functionality generates a large number of notable events, this internal stack ensures that you don't pay for these generated events. The sourcetypes used to track notable events and episodes are counted on this special stack with no impact on your Splunk Enterprise license. When calculating your daily license usage, disregard this stack, as it only counts internal ITSI usage.



However, if ITSI is installed on multiple environments with multiple license masters, and any indexer interacts with both environments, a duplicate licensing error occurs because both environments have the same auto-generated ITSI license stack. To remedy this issue, delete the internal license, install a secondary internal license, and disable the license_checker modular inputs:

1. Click **Settings** > **Licensing** and delete the **IT Service Intelligence Internals *DO NOT COPY* stack**.
2. Click **Add license** and upload the following license key file:
   Expand to see the license key file


```
<license><signature>UrBfGVqTyzcpKMr7JDHsEFIVO1RLRWn9dZaKBm5BTRzdz6MIhE1XRf4FJ5JVpUxquLwf1LCkJ4QV78uq4kLClh
vWuGPYNaMBmGe9w8MnWQi2TlMeTwwVHNoX6FB3TiNujQj3g+sQsP0IYTdtV98etDRNwOYIkuLFPap6dhvBIulBkFiBhGI+ELmHV7LRGcVgJY
F8zpOjVXSQMh0RL+6MWbrVdkKZU5ducxDJcpUEjp0PR3QePtczXm5ZdETui42mtpyiZsMlcYMGmQWS9erKst5EX8R9BSyudZkbZL4uoSVdVv
91Ml1GLb2pbgQQLm/Qwb2XaCk5QNo4Odv4A==</signature>
<payload>
<type>fixed-sourcetype</type>
<group_id>Enterprise</group_id>
<quota>107374182400000</quota>
<max_violations>5</max_violations>
<window_period>30</window_period>
<creation_time>1594969200</creation_time>
<label>IT Service Intelligence Internals *DO NOT COPY*</label>
<expiration_time>2163221999</expiration_time>
<features>
<feature>Auth</feature>
<feature>FwdData</feature>
<feature>LocalSearch</feature>
<feature>ScheduledSearch</feature>
<feature>Alerting</feature>
<feature>SplunkWeb</feature>
</features>
<add_ons>
<add_on name="itsi" type="app">
<parameter key="size" value="1"/>
</add_on>
</add_ons>
<sourcetypes>
<sourcetype>itsi_*</sourcetype>
</sourcetypes>
<guid>2AEECCCF-EDBC-499E-862C-8C79844114D4</guid>
</payload>
</license>
```


3. Click **Settings** > **Data inputs** > **IT Service Intelligence license checker** and disable both inputs.

Java requirements

IT Service Intelligence requires Java 8.x - 11.x to run anomaly detection and event management features. ITSI supports OpenJDK and Oracle JDK 8-11. Java installation is required on search heads only, not indexers or forwarders.

> Using 32-bit JRE/JDK on ITSI versions 4.3.x and later might cause the Rules Engine to fail with unclear errors in the search.log. If this occurs, perform the workaround described in ITSI-4663.

IT Service Intelligence search head considerations

IT Service Intelligence does not require a dedicated search head. However, ITSI is not supported on the same search head as Splunk Enterprise Security. For scalability beyond about 200 discrete KPIs, a search head cluster is a more

stable option.

You can't disable real-time searches on either the indexer tier or the search head tier where ITSI is running, otherwise ITSI notable event grouping stops working.

Virtual machines

When running a search head on a virtual machine, make sure to allocate all available CPU and RAM to the search head.

Forward search head data to indexers

ITSI runs KPI searches on the search head and by default stores data in the local `itsi_summary` index. It is considered a best practice to forward all internal data from search heads to indexers. There are two basic search head configuration scenarios for forwarding data to indexers:

Search head type	Configuration
Non-clustered search heads	Configure search heads to forward data to indexers.
Clustered search heads	In this scenario, you must configure outputs.conf to forward data from search heads to indexers. Then use the deployer to push the configuration file to cluster members.

For detailed instructions on how to configure search heads to forward data to indexers, see Best practice: Forward search head data to the indexer layer in the Splunk Enterprise *Distributed Search* manual.

IT Service Intelligence and search head clustering

Search head clusters increase the search load on indexers. Add more indexers or allocate additional CPU cores to the indexers when implementing a search head cluster. See System requirements and other deployment considerations for search head clusters and Search head clustering architecture in the *Distributed Search Manual*.

Search head scaling considerations for Splunk IT Service Intelligence

Consider the following guidelines when implementing a search head cluster:

Factor	Increase this specification
A large number of concurrent searches	Increase CPU cores Increase RAM
A high number of real-time searches being run A large number of users logging in at the same time	Increase CPU cores
A large number of enabled correlation searches	Increase RAM

For instructions on deploying ITSI in a search head cluster environment, see Install IT Service Intelligence in a search head cluster environment.

If you plan to use ITSI's Event Analytics solution, including Episode Review, you must have a stable search head cluster environment. The search head cluster must be healthy, which means it is not skipping searches and can handle the current load in your production environment.

Indexer clustering support

IT Service Intelligence supports both single site and multisite indexer cluster architectures. See The basics of indexer cluster architecture and Multisite indexer cluster architecture in the Splunk Enterprise *Managing Indexers and Clusters of Indexers* manual.

By default, ITSI writes to a common set of indexes. See Configure indexes in ITSI in this manual. If you plan to run more than one instance of ITSI that searches and writes to the same indexing tier, follow the instructions at Configure multiple ITSI deployments to use the same indexing layer.

For a multisite indexer cluster architecture, do the following:

- Enable summary replication. See Replicated summaries in the Splunk Enterprise *Managing Indexers and Clusters of Indexers* manual.
- Set the ITSI search head to `site0` to disable search affinity. See Disable search affinity in the Splunk Enterprise *Managing Indexers and Clusters of Indexers* manual.

If you use indexer clustering, the method you use to deploy apps and configuration files to indexer peers is different. See Manage common configurations across all cluster peers and Manage app deployment across all cluster peers in the Splunk Enterprise *Managing Indexers and Clusters of Indexers* manual.

If you use indexer clustering and also leverage ITSI's Event Analytics functionality, you need to configure your cluster masters and search heads so the Rules Engine can be resilient to indexer cluster rolling restarts and upgrades. For instructions to complete this one-time setup, see Configure the Rules Engine to handle indexer cluster rolling restarts and upgrades.

Real-time search requirements

You can't disable real-time searches on either the indexer tier or the search head tier where ITSI is running, otherwise ITSI notable event grouping stops working. Other ITSI features will also break, including Anomaly Detection and KPI alerting.

ITSI uses an *indexed* real-time search in place of the default real-time search. Indexed real-time searches allow your real-time searches to run after the events are indexed, which greatly improves indexing performance. You can change this default setting in indexes.conf with no negative effects. For instructions, see Indexed real-time search in the Splunk Enterprise *Search Manual*.

By default, only users with the admin role can run and save real-time searches. For more information on managing roles and assigning them to users, see Create and manage roles with Splunk Web in the *Securing the Splunk Platform* manual.

SSL requirements

An SSL configuration is required to run ITSI. SSL must be enabled on the splunkd port, port 8089, in order for certain utilities and scripts to function properly, including the following:

- kvstore_to_json.py
- command_check_for_kvstore_size.py
- disable_enable_itsi.py
- itsi_reset_default_team.py
- Migration and upgrade

A non-SSL environment is not supported. To secure your Splunk Enterprise deployment with SSL, see About securing Splunk Enterprise with SSL.

Performance considerations

ITSI works by way of KPI collection through searches against information stored within the Splunk Enterprise environment. ITSI production deployments might require additional hardware, depending on several factors, including the existing unused capacity of the environment, the number of concurrent KPI searches, the version of Splunk Enterprise in production, and other performance considerations specific to each deployment.

For more information, see Determine when to scale your Splunk Enterprise deployment in the Splunk Enterprise *Capacity Planning Manual*.

Planning your hardware requirements

ITSI performance depends on the ability to perform multiple fast, concurrent searches. Performance results depend on both search optimization and the capacity of your deployment to run multiple concurrent searches.

When planning your ITSI hardware requirements, consider these ITSI-specific factors that impact performance:

- Average KPI run time
- Frequency of KPIs (1, 5, or 15 minute)
- Number of entities that are being referenced per KPI

Also consider the following Splunk Enterprise factors that might impact performance:

- Average daily index volume. See How indexed data affects Splunk Enterprise performance in the *Capacity Planning Manual*.
- Number of concurrent users. See How concurrent users affect Splunk Enterprise performance in the *Capacity Planning Manual*.

ITSI capacity planning

ITSI capacity planning is governed by several variables. The three key variables in determining how many indexers and search heads you need are average KPI run time, the frequency of KPIs (1, 5, or 15 minute), and the number of entities being referenced per KPI. These variables can vary significantly in real-world deployments. Contact your Splunk sales representative for specific ITSI capacity planning recommendations based on your environment.

You must consider several other variables that impact the number of indexers and search heads you need, including the number of cores on those machines, the total amount of data being indexed, and total number of concurrent users.

Indexer and search head sizing examples

The following examples show roughly the number of indexers and search heads required to run the specified number of KPIs. These numbers are for example purposes only and vary based on your environment.

The following variables are fixed for each of the following examples:

- 5-minute KPIs
- 12 cores per search head and indexer
- Environment dedicated to ITSI alone

- Splunk Enterprise version 6.6 or later
- Use of "entity" refers to entities stored in the KV store and in the examples is a per-KPI measure, not the total number of entities in the system. If simple entity splits are done for KPIs and are not based on entities in a KV store, but extracted fields in Splunk searches, they need not be considered entities.
- 1 indexer required per 100 GB indexed

Example Set 1: Average run time per KPI = 10 seconds

Example A: 0 Entities per KPI, 100 GB indexed per day

KPIs	Indexers	Search heads
100	1 indexer	1 search head
500	2 indexers	1 search head
1,000	3 indexers	2 search heads

Rough capacity plan:

~ (Per 500 KPIs 1+ search head, 1+ indexer) + 1 Indexer.

Example B: 50 entities per KPI, 500 GB indexed per day

KPIs	Indexers	Search heads
100	5 indexers	1 search head
500	5 indexers	2 search heads
1,000	5 indexers	3 search heads

Rough capacity plan:

~ (Per 333 KPIs 1+ search head)

Example Set 2: Average run time per KPI = 5 seconds

Example A: 0 entities per KPI, 100 GB indexed per day

KPIs	Indexers	Search heads
100	1 indexer	1 search head
500	1 indexer	1 search head
1,000	2 indexers	2 search heads

Rough capacity plan:

~ (Per 950 KPIs 1+ search head), (Per 730 KPIs 1+ indexer)

Example B: 50 entities per KPI, 500 GB indexed per day

KPIs	Indexers	Search heads
100	5 indexer	1 search head
500	5 indexer	1 search head

KPIs	Indexers	Search heads
1,000	5 indexers	3 search heads

Rough capacity plan:

~ (Per 333 KPIs 1+ search head)

> It is important to distinguish between the number of KPIs and the number of KPI searches. When using KPI base searches, these requirements can be dramatically different. It's the number of actual search jobs that matters.

KV store size limits

Splunk IT Service Intelligence requires the **KV store** to store certain information on the search head. Also, in a dedicated search head environment, KPI data is stored locally. You need a minimum of 30 GB of free storage in `$SPLUNK_HOME`.

The limit of a single batch save to a KV store collection is 50 MB. As a result, if one KPI base search is in use by multiple services, and the total size of your services exceeds 50 MB, ITSI generates an error. Additionally, if the number of objects, such as services and KPIs, exceeds the KV store memory limits, services might be lost during a backup or migration. To avoid these issues, check the total amount of data that your services contain, and, if necessary, increase the KV store size limit in `limits.conf`.

1. Use the Backup/Restore UI or the `kvstore_to_json.py` script to create a backup of your system. For more information, see Back up and restore ITSI KV store data.
2. If the size of `itsi_services___service___0.json` exceeds 50 MB, increase the KV store size limit.
3. Add the following stanza to `$SPLUNK_HOME/etc/apps/SA-ITOA/local/limits.conf`:

   ```
   [kvstore]
   max_size_per_batch_save_mb = 50
   ```
4. Increase the value of `max_size_per_batch_save_mb` to a higher value.
5. Additionally, if you have more than 1,000 KPIs and services combined, add the following stanza to `$SPLUNK_HOME/etc/apps/SA-ITOA/local/limits.conf`:

   ```
   [kvstore]
   max_size_per_result_mb = 100
   ```
6. Increase the value of `max_size_per_result_mb` to roughly 50 MB per 1,000 KPIs.

Search macros in ITSI

ITSI uses search macros to simplify and consolidate lengthy KPI searches. You can view a complete list of search macros used in ITSI, including macro definitions and usage details in macros.conf. For more information on search macros, see Use search macros in searches in the Splunk Enterprise *Knowledge Manager* Manual.

HTTP event collector

ITSI uses HTTP Event Collector (HEC) for event management. HEC runs as a separate app called `splunk_httpinput` and stores its input configuration in `$SPLUNK_HOME/etc/apps/splunk_httpinput/local`.

HEC requires that port 8088 be open for local traffic. You do not need any additional HEC configuration.

For more information about HTTP Event Collector, see Set up and use HTTP Event Collector in Splunk Web in the Splunk

Enterprise *Getting Data In* manual.

ITSI compatibility with other apps

Do not install ITSI and Splunk Enterprise Security on the same search head or search head cluster. With the exception of Enterprise Security, you can deploy ITSI on Splunk Enterprise instances with other Splunk apps.

For ITSI compatibility with all related apps and add-ons, see ITSI compatibility with other apps and add-ons.

For a comprehensive evaluation of your environment, consult Splunk Professional Services or your support representative.

ITSI compatibility with related apps and add-ons

This table lists versions of IT Service Intelligence (ITSI) and their compatible versions of the following related products:

- As of version 4.9.0, SAI is no longer packaged with ITSI. For more information, see ITSI entity discovery searches. SAI will reach End of Life on August 2022.
- The **Machine Learning Toolkit** (MLTK) is required if you want to leverage ITSI's Predictive Analytics functionality. For more information, see Set up Predictive Analytics in ITSI. You must also install the Python for Scientific Computing Add-on version 3.0.2 or higher in order to use MLTK.
- The **Common Information Model** (CIM) is required for bidirectional ticketing with ServiceNow. For more information, see Overview of episode actions in ITSI.
- The **Splunk Add-on for ServiceNow** is required for integration with ServiceNow.

For compatibility between ITSI and Splunk Enterprise versions, see the Splunk products version compatibility matrix.

For compatibility between Splunk Enterprise and other Splunk apps and add-ons, see the specific app or add-on page on Splunkbase.

For instructions on upgrading ITSI, see Before you upgrade IT Service Intelligence.

IT Service Intelligence (ITSI)	Splunk App for Infrastructure (SAI)	Machine Learning Toolkit (MLTK)	Common Information Model (CIM)	Splunk Add-on for ServiceNow
4.16.x (Cloud only)	N/A	5.3.3	5.x	7.x
4.15.x	N/A	5.3.3	4.x, 5.x	7.x
4.14.x (Cloud only)	N/A	5.x	4.x, 5.x	7.x
4.13.x	N/A	5.x	4.x, 5.x	7.x
4.12.x (Cloud only)	2.2.5	5.x	4.x, 5.x	7.x
4.11.x	2.2.5	5.x	4.x, 5.x	7.x
4.10.x (Cloud Only)	2.2.4	5.x	4.x	7.x
4.9.x	2.2.4	**Python 3**: 5.x	**Python 3**: 4.x	**Python 3**: 7.x
		Python 2: 3.2.0 - 4.4.2	**Python 2**: 4.13.0 - 4.18.0	**Python 2**: 4.x - 5.x
4.8.x (Cloud only)	2.2.1, 2.2.2, 2.2.3	**Python 3**: 5.x	**Python 3**: 4.14.0 - 4.18.0	**Python 3**: 5.0.x, 6.x

IT Service Intelligence (ITSI)	Splunk App for Infrastructure (SAI)	Machine Learning Toolkit (MLTK)	Common Information Model (CIM)	Splunk Add-on for ServiceNow
		~~**Python 2**: 3.2.0 - 4.4.2~~	~~**Python 2**: 4.13.0 - 4.18.0~~	~~**Python 2**: 4.x - 5.x~~

Python 3 migration with ITSI

On January 1, 2020, Python version 2.x was officially deprecated by the Python Software Foundation. Python packages and tools have ended or are ending support for Python 2, and new Python packages don't support Python 2. To maintain compatibility with the many third party projects that use Python, Splunk has migrated Splunk Cloud Platform and Splunk Enterprise, supported Premium Solutions, and supported Splunkbase apps and add-ons to be compatible with Python 3.7.

Splunk has released Splunk Cloud Platform and Splunk Enterprise versions 8.x to support the migration from Python 2 to Python 3. Splunk has migrated impacted features to Python 3.7, and versions 8.x include both the Python 2.7 and Python 3.7 runtimes, to help customers and developers transition Python in apps from Python 2 to Python 3. Splunk will remove the Python 2.7 runtime altogether in a future release.

This page helps identify prerequisites, required changes, and steps for migrating ITSI to Python 3 alongside your Splunk Enterprise deployment. This topic covers the following upgrade scenarios:

- Migrating ITSI and Splunk Enterprise to Python 3
- Upgrading to Splunk Enterprise version 8.x with Python 2
- Upgrading to ITSI 4.4.x or later without upgrading to Splunk Enterprise version 8.x

Scenario 1: Migrate ITSI and Splunk Enterprise to Python 3

You must upgrade ITSI and all other associated add-ons to the newest versions before upgrading to Splunk Enterprise version 8.x. If you upgrade Splunk Enterprise first, ITSI breaks.

In order to upgrade to Splunk Enterprise 8.x, you must also upgrade to ITSI version 4.4.x or later. All ITSI versions prior to 4.4.x are incompatible with Splunk Enterprise version 8.x, even if you use the Python 2.7 runtime. For more information about ITSI compatibility with Splunk Enterprise, see the Splunk products version compatibility matrix.

The only post-upgrade impact for Python 3 migration relates to ITSI Predictive Analytics customers. If you currently leverage ITSI's Predictive Analytics capabilities, you must retrain all of your predictive models after you migrate ITSI to Python 3. For information about Predictive Analytics, see Overview of Predictive Analytics in ITSI.

Perform the following steps *in this order* to migrate ITSI to Python 3. Some steps are only required if you're using Predictive Analytics.

1. Upgrade to ITSI version 4.4.x or later

For more information, see Upgrade IT Service Intelligence on a single instance or Upgrade IT Service Intelligence in a search head cluster environment depending on your deployment architecture.

2. Upgrade the Machine Learning Toolkit

If you're using Predictive Analytics, upgrade your MLTK to version 5.0.0 or later. For ITSI version compatibility with the MLTK, see ITSI compatibility with other apps and add-ons.

3. Upgrade required add-ons

If you have an integration with ServiceNow and/or leverage ITSI's bidirectional ticketing functionality, you must upgrade the Splunk Add-on for ServiceNow and the Common Information Model (CIM) to the newest releases which are Python 3 compatible.

- Upgrade the Splunk Add-on for ServiceNow to version 5.0.x. For instructions, see Upgrade the Splunk Add-on for ServiceNow.
- Upgrade the Common Information Model to version 4.15.0. For instructions, see Install the Splunk Common Information Model Add-on.

For ITSI version compatibility with these add-ons, see ITSI compatibility with other apps and add-ons.

4. Upgrade Splunk Enterprise using the Python 3 runtime

Upgrade your Splunk Enterprise instance to version 8.x and perform the Python 3 migration. For more information, see Upgrade using the Python 3 runtime and dual-compatible Python syntax in custom scripts in the Splunk Enterprise *Installation Manual*.

In distributed environments, always run the same Python version on both indexers and search heads.

5. Retrain Predictive Analytics models

If you're using Predictive Analytics, confirm that data ingested to train any predictive models is still stored in Splunk software. If data has exceeded retention timeframes, re-ingest the data to feed the models.

Retrain all predictive models saved into each of your services. Retraining a model automatically replaces the existing model. For instructions, see Retrain a predictive model in ITSI.

Scenario 2: Upgrade to Splunk Enterprise 8.x with Python 2

If you upgrade to Splunk Enterprise version 8.x but want to use the Python 2 runtime, you still need to upgrade ITSI to version 4.4.x or later. However, you must use a pre-5.0.0 version of the Machine Learning toolkit.

1. Upgrade Splunk Enterprise using the Python 2 runtime

Upgrade your Splunk Enterprise instance to version 8.x using the Python 2 runtime. For more information, see Upgrade using the Python 2 runtime and make minimal changes to Python code in the Splunk Enterprise *Installation Manual*.

2. Upgrade to ITSI version 4.4.x or later

For more information, see Upgrade IT Service Intelligence on a single instance or Upgrade IT Service Intelligence in a search head cluster environment depending on your deployment architecture.

3. (Optional) Upgrade required add-ons

The Splunk Add-on for ServiceNow and the Common Information Model (CIM) can remain on older versions, or you can upgrade them if needed. For ITSI compatibility with these add-ons, see ITSI compatibility with other apps and add-ons.

Scenario 3: Upgrade to ITSI 4.4.x or later without Splunk Enterprise 8.x

ITSI version 4.4.x and later supports both the Python 2.7 and Python 3.7 runtimes. Therefore, you can upgrade to ITSI 4.4.x or later while still remaining on Splunk Enterprise versions 7.2.x - 7.3.x. For ITSI compatibility with Splunk Enterprise, see Splunk Enterprise system requirements.

The Splunk Add-on for ServiceNow and the Common Information Model (CIM) can remain on older versions, or you can upgrade them if needed. For ITSI compatibility with these add-ons, see ITSI compatibility with other apps and add-ons.

Do not upgrade the Machine Learning Toolkit to version 5.0.0. Version 5.0.0 is only compatible with Python 3.

> Upon startup, you might encounter errors stating you have an invalid Python version. You can ignore these warnings as they have no impact on functionality. Once you upgrade to Splunk Enterprise version 8.0.0 or later the warnings no longer appear.

Installation

Install Splunk IT Service Intelligence on a single instance

Splunk IT Service Intelligence (ITSI) version 4.16.x is a cloud-only release. Splunk Cloud Platform customers have to work with Support to install or uninstall ITSI. To file a ticket on the Splunk Support Portal, see Support and Services.

Install ITSI in a FIPS enabled environment

IT Service Intelligence can be deployed in a Federal Information Processing Standard (FIPS) compliant mode. Splunk Enterprise and the universal forwarder use an embedded cryptographic FIPS module on various operating systems.

Security considerations for turning on FIPS mode

When you turn on FIPS mode, note the following:

- Do not consider turning on FIPS mode on Splunk Enterprise as the only security enhancement. FIPS mode is one of several strategies you can employ to improve security for Splunk software.
- You must turn on FIPS mode before you start Splunk Enterprise the first time. FIPS mode is active only when you activate it on a machine that runs a FIPS-compliant operating system kernel that has FIPS mode turned on. If you run Splunk Enterprise on a Linux machine that that is already in FIPS mode, Splunk Enterprise automatically turns on FIPS mode.
- Turning on FIPS mode can potentially reduce Splunk Enterprise performance.
- The FIPS module turns off the use of some cryptographic algorithms in Python that Splunk uses to run apps (for example, Message Digest 5 and Rivest Cipher 4).
- Any Splunk apps that you want to run on a FIPS environment must be certified to run in FIPS mode and cannot have dependencies on algorithms like MD5 or RC4.

Enable FIPS mode on operating system

In ITSI, the Rules Engine and Metrics Anomaly Detection have an external Java process component. In order to meet security requirements, activate FIPS on both the operating system as well as on your Splunk platform. To activate FIPS for your OS/kernel, please refer to the official documentation provided by your operating system vendor.

Compatibility Matrix

If you need to adhere to the FIPS standard, you must prepare your environment for FIPS compliance before deploying ITSI.

Java Build	CentOS 7	CentOS 8	Windows Server 2019	Windows Server 2022
OracleJDK 8				
OracleJDK 11				
OpenJDK 8				
OpenJKD 11				

OpenJDK builds shipped by default with CentOS 8 don't work in a FIPS environment due to compatibility issues with FIPS. We recommend using OracleJDK for CentOS 8, or use the OpenJDK build available from Eclipse Adoptium platform or the Java JDK Archive. For more information, see Download Oracle JDK.

Download Oracle JDK

OracleJDK builds are available on the official Oracle website. Install the build and set the system variable `JAVA_HOME` to point to the build installation directory.

Download OpenJDK

OpenJDK for CentOS 7

- OpenJDK 8 for CentOS 7 can be installed using the command:

```
sudo yum install java-1.8.0-openjdk
```

- OpenJDK 11 for CentOS 7 can be installed using the command:

```
sudo yum install java-11-openjdk
```

- OpenJDK builds from the Java JDK archive are available at Archived OpenJDK General-Availability Releases
- OpenJDK builds from the Eclipse Adoptium Archive are available at Adoptium Archive.
- The Microsoft build of OpenJDK is available at OpenJDK 11.

OpenJDK for CentOS 8

- OpenJDK builds from the Java JDK archive are available at Archived OpenJDK General-Availability Releases
- OpenJDK builds from the Eclipse Adoptium Archive are available at Adoptium Archive.
- The Microsoft build of OpenJDK is available at OpenJDK 11.

OpenJDK for Windows

- OpenJDK 8 and 11 for Windows are available on the official website of Eclipse Adoptium Adoptium Archive.
- OpenJDK builds from the Java JDK archive are available at Archived OpenJDK General-Availability Releases.
- The Microsoft build of OpenJDK is available at OpenJDK 11.

Turn on FIPS mode in Splunk Enterprise

After FIPS is activated on the operating system level, turn on FIPS mode in Splunk upon initial Splunk software installation. If you install the software without FIPS mode turned on, you cannot turn on FIPS during an upgrade later, and must either reinstall, or install a new version. Follow the steps in Secure Splunk Enterprise with FIPS to turn on FIPS mode in Splunk Enterprise.

Verify that Rules Engine is running

1. Log in to Splunk Enterprise.
2. Install ITSI. For more information, see:

- Install Splunk IT Service Intelligence on a single instance.
- Where to install IT Service Intelligence in a distributed environment.
- Install IT Service Intelligence in a search head cluster environment.

3. Navigate to **ITSI** > **Dashboards** > **Event Analytics Monitoring**.
4. Check that **Number of Rules Engine Processes** value is 1.

Troubleshooting

Rules Engine processes are 0

Check if Java Version is detected in the dashboard Event Analytics Monitoring. If no Java Version is detected then the system variable JAVA_HOME might have been set incorrectly. Set the system variable to the path which points to the desired Java build directory and then restart the realtime search itsi_event_grouping by disabling it and then enabling it again.

Where to install IT Service Intelligence in a distributed environment

Splunk IT Service Intelligence (ITSI) version 4.16.x is a cloud-only release. Splunk Cloud Platform customers have to work with Support to install or uninstall ITSI. To file a ticket on the Splunk Support Portal, see Support and Services.

Install IT Service Intelligence in a search head cluster environment

Splunk IT Service Intelligence (ITSI) version 4.16.x is a cloud-only release. Splunk Cloud Platform customers have to work with Support to install or uninstall ITSI. To file a ticket on the Splunk Support Portal, see Support and Services.

Configure indexes in ITSI

In a Splunk Cloud Platform deployment, customers work with Splunk Support to set up, manage, and maintain their cloud index parameters. See Manage Splunk Cloud indexes in the *Splunk Cloud Admin Manual*. To file a ticket on the Splunk Support Portal, see Support and Services.

Uninstall Splunk IT Service Intelligence

Splunk IT Service Intelligence (ITSI) version 4.16.x is a cloud-only release. Splunk Cloud Platform customers have to work with Support to install or uninstall ITSI. To file a ticket on the Splunk Support Portal, see Support and Services.

Upgrading

Before you upgrade IT Service Intelligence

ITSI version 4.16.x is a Splunk Cloud Platform only release and is not available on-premises. Splunk Cloud Platform customers must work with Support to coordinate upgrades to IT Service Intelligence.

Steps to address the Apache Log4j vulnerabilities in ITSI or IT Essentials Work

On Friday December 10, 2021, a serious remote code execution (RCE) vulnerability, commonly known as Log4Shell, was discovered in the popular open-source Apache Log4j (versions 2.0 to 2.14.1) logging library. Over subsequent days, additional vulnerabilities have been discovered. See Apache Log4j 2 in Apache documentation for more info. The Apache Software Foundation released a series of emergency patches for these vulnerabilities. For more information on addressing the vulnerabilities, see Splunk Security Advisory for Apache Log4j (CVE-2021-44228 and CVE-2021-45046).

Impacted version	Immediate workaround	Intermediate upgrade (Skip unless already in progress)	Final fix
ITSI and ITE Work versions 4.11.0, 4.9.x (on-premises and cloud) ITSI 4.7.x (on-premises and cloud)	See the workaround steps provided on this page after this table. Follow these steps in your existing ITSI installation to reduce your exposure to the CVE-2021-44228 vulnerability. Cloud customers: Splunk Cloud TechOps is upgrading impacted versions.	Upgrade to the maintenance version that includes the fix for CVE-2021-44228: • 4.7.x > 4.7.3 • 4.9.x > 4.9.5 • 4.11.0 > 4.11.1 See Version-specific upgrade notes for ITSI for steps to take after you upgrade.	Upgrade to the maintenance version that includes version 2.16.0 or later of Apache Log4j libraries, which addresses both CVE-2021-44228 and CVE-2021-45046. • 4.7.x > 4.7.4 • 4.9.x > 4.9.6 • 4.11.x > 4.11.3 See Version-specific upgrade notes for ITSI for steps to take after you upgrade.
ITSI and ITE Work 4.10.x - Cloud-only version ITSI 4.5.x, 4.6.x, and 4.8.x - Cloud-only versions	Splunk Cloud TechOps is upgrading impacted versions.	All cloud stacks will be upgraded to the closest latest minor version with the fix for CVE-2021-44228. 4.5.x and 4.8.x will be upgraded to 4.9.5.	All cloud stacks will be updated to the closest latest minor version with the 2.16.0 or later version of Apache Log4j. 4.5.x and 4.8.x will be upgraded to 4.9.6.
ITSI version 4.4.x (No longer supported as of October 22, 2021)	See the workaround steps provided on this page after this table. Follow these steps in your existing ITSI installation to reduce your exposure to the CVE-2021-44228 vulnerability.	Upgrade to the 4.7.3. maintenance version that includes the fix for the RCE vulnerability (CVE-2021-44228). See Version-specific upgrade notes for ITSI for steps to take after you upgrade.	Upgrade to the 4.7.4 maintenance version that includes version 2.16.0 or later of Apache Log4j libraries, which addresses both CVE-2021-44228 and CVE-2021-45046. See Version-specific upgrade notes for ITSI for steps to take after you upgrade.

Impacted version	Immediate workaround	Intermediate upgrade (Skip unless already in progress)	Final fix

Workaround steps for self-managed deployments on standalone search heads on *nix

Follow these steps to implement a workaround for CVE-2021-44228 in self-managed deployments of Splunk IT Service Intelligence or IT Essentials Work on standalone search heads on *nix environments. You can use this fix as a workaround until you have time to upgrade to a maintenance version that addresses the vulnerability. These changes will not disrupt any user functionality. These changes require a maintenance window of about eight to ten minutes.

Prerequisites

- You must have administrative access to the operating system on the machine where ITSI is installed to perform these steps.

For all search heads where ITSI or ITE Work is installed, perform the following procedures.

$SPLUNK_HOME is the directory where you installed Splunk Enterprise.

Steps

1. Open a shell prompt.
2. Go to the folder $SPLUNK_HOME/bin.
3. Stop the Splunk process.

   ```
   cd $SPLUNK_HOME/opt/splunk/bin
   ./splunk stop
   ```
4. Go to the etc/apps/SA-ITOA/lib/java/event_management/libs/ directory:

   ```
   cd $SPLUNK_HOME/etc/apps/SA-ITOA/lib/java/event_management/libs/
   ```
5. Run the command that corresponds to your version of ITSI or IT Essentials Work to delete the JndiLookup classes from the log4j jar file.
   - ITSI or IT Essentials Work version 4.7.x, 4.9.x, or 4.11.x:
     ```
     zip -q -d log4j-core-2.13.2.jar org/apache/logging/log4j/core/lookup/JndiLookup.class
     ```
     Once the above command executes successfully, if there are log4j .jar files with versions lower than 2.13.2 in this directory, you can safely delete these .jar files with lower versions.
   - ITSI version 4.4.x:
     ```
     zip -q -d log4j-core-2.5.jar org/apache/logging/log4j/core/lookup/JndiLookup.class
     ```
     Once the above command executes successfully, if there are log4j .jar files with versions lower than 2.5 in this directory, you can safely delete these .jar files with lower versions.
6. Go to the etc/apps/SA-ITSI-MetricAD/lib/ directory.
   ```
   cd $SPLUNK_HOME/etc/apps/SA-ITSI-MetricAD/lib/
   ```
7. Run the command that corresponds to your version of ITSI or IT Essentials Work to delete JndiLookup classes from the log4j jar file.
   - ITSI version 4.7.x, 4.9.x, 4.11.0:

     ```
     zip -q -d org.apache.logging.log4j.log4j-core-2.13.2.jar
     ```

```
org/apache/logging/log4j/core/lookup/JndiLookup.class
```

Once the above command executes successfully, if there are log4j .jar files with versions lower than 2.13.2 in this directory, you can safely delete these .jar files with lower versions.

- ITSI version 4.4.x:

```
zip -q -d org.apache.logging.log4j.log4j-core-2.3.jar
org/apache/logging/log4j/core/lookup/JndiLookup.class
```

Once the above command executes successfully, if there are log4j .jar files with versions lower than 2.3 in this directory, you can safely delete these .jar files with lower versions.

8. Delete older versions of log4j .jar files from the search head. To view a list of the files and their locations, see Version-specific upgrade notes for ITSI.
9. Restart Splunk Enterprise:

```
cd $SPLUNK_HOME/opt/splunk/bin
./splunk start
```

Workaround steps for self-managed deployments on standalone search heads on Windows

Follow these steps to implement a workaround for CVE-2021-44228 in self-managed deployments of Splunk IT Service Intelligence or IT Essentials Work on standalone search heads on Windows environments. You can use this fix as a workaround until you have time to upgrade to a maintenance version that addresses the vulnerability. These changes will not disrupt any user functionality. These changes require a maintenance window of about eight to ten minutes.

Prerequisites

- You must have administrative access to the operating system on the machine where ITSI is installed to perform these steps.
- You need a zip utility installed on Windows. The instructions below provide the command prompt syntax for 7zip.

For all search heads where ITSI or ITE Work is installed, perform the following procedure.

$SPLUNK_HOME is the directory where you installed Splunk Enterprise.

Steps

1. Use the Services control panel to stop the Splunk process.
2. Go to the etc/apps/SA-ITOA/lib/java/event_management/libs/ directory:

```
cd $SPLUNK_HOME\etc\apps\SA-ITOA\lib\java\event_management\libs
```

3. Run the command that corresponds to your version of ITSI or IT Essentials Work to delete the JndiLookup classes from the log4j jar file.
    - ITSI or IT Essentials Work version 4.7.x, 4.9.x, or 4.11.x:

```
$SPLUNK_HOME\etc\apps\SA-ITOA\lib\java\event_management\libs>"C:\Program Files\7-Zip\7z.exe"
D .\log4j-core-2.13.2.jar org\apache\logging\log4j\core\lookup\JndiLookup.class
```

Once the above command executes successfully, if there are log4j .jar files with versions lower than 2.13.2 in this directory, you can safely delete these .jar files with lower versions.

    - ITSI version 4.4.x:

```
$SPLUNK_HOME\etc\apps\SA-ITOA\lib\java\event_management\libs>"C:\Program Files\7-Zip\7z.exe"
D .\log4j-core-2.5.jar org\apache\logging\log4j\core\lookup\JndiLookup.class
```

Once the above command executes successfully, if there are log4j .jar files with versions lower than 2.5 in this directory, you can safely delete these .jar files with lower versions.

4. Go to the etc/apps/SA-ITSI-MetricAD/lib/ directory.
   ```
   cd $SPLUNK_HOME\etc\apps\SA-ITSI-MetricAD\lib\
   ```
5. Run the command that corresponds to your version of ITSI or IT Essentials Work to delete JndiLookup classes from the log4j jar file.
   - ITSI version 4.7.x, 4.9.x, 4.11.0:

     ```
     $SPLUNK_HOME\etc\apps\SA-ITSI-MetricAD\lib\>"C:\Program Files\7-Zip\7z.exe" D
     .\org.apache.logging.log4j.log4j-core-2.13.2.jar
     org\apache\logging\log4j\core\lookup\JndiLookup.class
     ```

     Once the above command executes successfully, if there are log4j .jar files with versions lower than 2.13.2 in this directory, you can safely delete these .jar files with lower versions.

   - ITSI version 4.4.x:

     ```
     $SPLUNK_HOME\etc\apps\SA-ITSI-MetricAD\lib\>"C:\Program Files\7-Zip\7z.exe" D
     .\org.apache.logging.log4j.log4j-core-2.3.jar
     org\apache\logging\log4j\core\lookup\JndiLookup.class
     ```

     Once the above command executes successfully, if there are log4j .jar files with versions lower than 2.3 in this directory, you can safely delete these .jar files with lower versions.

6. Delete older versions of log4j .jar files from the search head. To view a list of the files and their locations, see Version-specific upgrade notes for ITSI.
7. Use the Services control panel to restart Splunk Enterprise.

Workaround steps for self-managed deployments on a search head cluster on *nix

Follow these steps to implement a workaround for CVE-2021-44228 in self-managed deployments of Splunk IT Service Intelligence or IT Essentials Work on search head clusters on *nix environments. You can use this fix as a workaround until you have time to upgrade to a maintenance version that addresses the vulnerability. These changes require a maintenance window of about eight to ten minutes.

Prerequisite
You must have administrative access to the operating system on the machine where ITSI or IT Essentials Work is installed to perform these steps.

For all search head clusters where ITSI or ITE Work is installed, perform the following procedures.

$SPLUNK_HOME is the directory where you installed Splunk Enterprise.

Steps

1. Log on to the deployer.
2. Go to the etc/shcluster/apps/SA-ITOA/lib/java/event_management/libs/ directory.
   ```
   cd $SPLUNK_HOME/etc/shcluster/apps/SA-ITOA/lib/java/event_management/libs/
   ```
3. Run the command that corresponds to your version of ITSI or IT Essentials Work to delete the JndiLookup classes from the log4j jar file.
   - ITSI or IT Essentials Work version 4.7.x, 4.9.x, or 4.11.x:
     ```
     zip -q -d log4j-core-2.13.2.jar org/apache/logging/log4j/core/lookup/JndiLookup.class
     ```
   - ITSI version 4.4.x:

```
zip -q -d log4j-core-2.5.jar org/apache/logging/log4j/core/lookup/JndiLookup.class
```

4. Make a note of the updated jar's checksum.
   - ITSI or IT Essentials Work version 4.7.x, 4.9.x, or 4.11.x:
     On *nix:
     ```
     sha256sum log4j-core-2.13.2.jar
     ```
   - ITSI version 4.4.x:
     ```
     sha256sum log4j-core-2.5.jar
     ```
5. Go to the etc/shcluster/apps/SA-ITSI-MetricAD/lib/ directory.
   ```
   cd $SPLUNK_HOME/etc/shcluster/apps/SA-ITSI-MetricAD/lib/
   ```
6. Run the command that corresponds to your version of ITSI or IT Essentials Work to delete JndiLookup classes from the log4j jar file.
   - ITSI version 4.7.x, 4.9.x, 4.11.0:

     ```
     zip -q -d org.apache.logging.log4j.log4j-core-2.13.2.jar
     org/apache/logging/log4j/core/lookup/JndiLookup.class
     ```
   - ITSI version 4.4.x:

     ```
     zip -q -d org.apache.logging.log4j.log4j-core-2.3.jar
     org/apache/logging/log4j/core/lookup/JndiLookup.class
     ```
7. Make note of the updated jar's checksum
   - ITSI version 4.7.x, 4.9.x, 4.11.0:

     ```
     sha256sum  org.apache.logging.log4j.log4j-core-2.13.2.jar
     ```
   - ITSI version 4.4.x:

     ```
     sha256sum  org.apache.logging.log4j.log4j-core-2.3.jar
     ```
8. Delete the older versions of log4j .jar files from the deployer before deploying the updated jars. To view a list of the files and their locations, see Version-specific upgrade notes for ITSI.
9. Deploy the updated jars to search heads with the following command. The -target parameter specifies the URI and management port for any member of the cluster. The -auth parameter specifies credentials for the deployer instance.
   ```
   $SPLUNK_HOME/bin/splunk apply shcluster-bundle -target <URI>:<management_port> -auth
   <username>:<password>
   ```
10. Wait for deployment and rolling restart to complete.
11. Log on to the search heads and verify the updated jar's checksums.
    1. Go to the etc/apps/SA-ITOA/lib/java/event_management/libs/ directory.
       ```
       cd $SPLUNK_HOME/etc/apps/SA-ITOA/lib/java/event_management/libs/
       ```
    2. Verify that the checksum of the jar matches the checksum you made note of earlier.
       - ITSI or IT Essentials Work version 4.7.x, 4.9.x, or 4.11.x:
         ```
         sha256sum log4j-core-2.13.2.jar
         ```
       - ITSI version 4.4.x:
         ```
         sha256sum log4j-core-2.5.jar
         ```
    3. Go to the etc/apps/SA-ITSI-MetricAD/lib/ directory.
       ```
       cd $SPLUNK_HOME/etc/apps/SA-ITSI-MetricAD/lib/
       ```
    4. Verify that the checksum of the jar matches the checksum you made note of earlier.
       - ITSI version 4.7.x, 4.9.x, 4.11.0:

         ```
         sha256sum  org.apache.logging.log4j.log4j-core-2.13.2.jar
         ```
       - ITSI version 4.4.x:

         ```
         sha256sum  org.apache.logging.log4j.log4j-core-2.3.jar
         ```

Workaround steps for self-managed deployments on a search head cluster on Windows

Follow these steps to implement a workaround for CVE-2021-44228 in self-managed deployments of Splunk IT Service

Intelligence or IT Essentials Work on search head clusters in a Windows environment. You can use this fix as a workaround until you have time to upgrade to a maintenance version that addresses the vulnerability. These changes require a maintenance window of about eight to ten minutes.

Prerequisite
You must have administrative access to the operating system on the machine where ITSI or IT Essentials Work is installed to perform these steps.

For all search head clusters where ITSI or ITE Work is installed, perform the following procedures.

> $SPLUNK_HOME is the directory where you installed Splunk Enterprise.

Steps

1. Log on to the deployer.
2. Go to the etc/shcluster/apps/SA-ITOA/lib/java/event_management/libs/ directory.
   ```
   cd $SPLUNK_HOME\etc\shcluster\apps\SA-ITOA\lib\java\event_management\libs\
   ```
3. Run the command that corresponds to your version of ITSI or IT Essentials Work to delete the JndiLookup classes from the log4j jar file.
   - ITSI or IT Essentials Work version 4.7.x, 4.9.x, or 4.11.x:
     ```
     $SPLUNK_HOME\etc\shcluster\apps\SA-ITOA\lib\java\event_management\libs>"C:\Program Files\7-Zip\7z.exe" D .\log4j-core-2.13.2.jar org\apache\logging\log4j\core\lookup\JndiLookup.class
     ```
     > Once the above command executes successfully, if there are log4j .jar files with versions lower than 2.13.2 in this directory, you can safely delete these .jar files with lower versions.
   - ITSI version 4.4.x:
     ```
     $SPLUNK_HOME\etc\shcluster\apps\SA-ITOA\lib\java\event_management\libs>"C:\Program Files\7-Zip\7z.exe" D .\log4j-core-2.5.jar org\apache\logging\log4j\core\lookup\JndiLookup.class
     ```
     > Once the above command executes successfully, if there are log4j .jar files with versions lower than 2.5 in this directory, you can safely delete these .jar files with lower versions.
4. Make a note of the updated jar's checksum.
   - ITSI or IT Essentials Work version 4.7.x, 4.9.x, or 4.11.x:
     ```
     $SPLUNK_HOME\etc\shcluster\apps\SA-ITOA\lib\java\event_management\libs>"C:\Program Files\7-Zip\7z.exe" h .\log4j-core-2.13.2.jar
     ```
   - ITSI version 4.4.x:
     ```
     $SPLUNK_HOME\etc\shcluster\apps\SA-ITOA\lib\java\event_management\libs>"C:\Program Files\7-Zip\7z.exe" h .\log4j-core-2.5.jar
     ```
5. Go to the etc/shcluster/apps/SA-ITSI-MetricAD/lib/ directory.
   ```
   cd $SPLUNK_HOME\etc\shcluster\apps\SA-ITSI-MetricAD\lib\
   ```
6. Run the command that corresponds to your version of ITSI or IT Essentials Work to delete JndiLookup classes from the log4j jar file.
   - ITSI version 4.7.x, 4.9.x, 4.11.0:
     ```
     $SPLUNK_HOME\etc\shcluster\apps\SA-ITSI-MetricAD\lib>"C:\Program Files\7-Zip\7z.exe" D .\org.apache.logging.log4j.log4j-core-2.13.2.jar org\apache\logging\log4j\core\lookup\JndiLookup.class
     ```
     > Once the above command executes successfully, if there are log4j .jar files with versions lower than 2.13.2 in this directory, you can safely delete these .jar files with lower versions.
   - ITSI version 4.4.x:

```
$SPLUNK_HOME\etc\shcluster\apps\SA-ITSI-MetricAD\lib>"C:\Program Files\7-Zip\7z.exe" D
.\org.apache.logging.log4j.log4j-core-2.3.jar
org\apache\logging\log4j\core\lookup\JndiLookup.class
```

Once the above command executes successfully, if there are log4j .jar files with versions lower than 2.3 in this directory, you can safely delete these .jar files with lower versions.

7. Make note of the updated jar's checksum
   - ITSI version 4.7.x, 4.9.x, 4.11.0:

     ```
     $SPLUNK_HOME\etc\shcluster\apps\SA-ITSI-MetricAD\lib\>"C:\Program Files\7-Zip\7z.exe" h
     .\org.apache.logging.log4j.log4j-core-2.13.2.jar
     ```
   - ITSI version 4.4.x:

     ```
     $SPLUNK_HOME\etc\shcluster\apps\SA-ITSI-MetricAD\lib\>"C:\Program Files\7-Zip\7z.exe" h
     .\org.apache.logging.log4j.log4j-core-2.3.jar
     ```
8. Delete the older versions of log4j .jar files from the deployer before deploying the updated jars. To view a list of the files and their locations, see Version-specific upgrade notes for ITSI.
9. Deploy updated jars to search heads with the following command. The -target parameter specifies the URI and management port for any member of the cluster. The -auth parameter specifies credentials for the deployer instance.

   ```
   $SPLUNK_HOME\bin\splunk apply shcluster-bundle -target <URI>:<management_port> -auth
   <username>:<password>
   ```
10. Wait for deployment and rolling restart to complete.
11. Log on to the search heads and verify the updated jar's checksums.
    1. Go to the etc/apps/SA-ITOA/lib/java/event_management/libs/ directory.

       ```
       cd $SPLUNK_HOME\etc\apps\SA-ITOA\lib\java\event_management\libs\
       ```
    2. Verify that the checksum of the jar matches the checksum you made note of earlier.
       - ITSI or IT Essentials Work version 4.7.x, 4.9.x, or 4.11.x:

         ```
         $SPLUNK_HOME\etc\apps\SA-ITOA\lib\java\event_management\libs>"C:\Program
         Files\7-Zip\7z.exe" h .\log4j-core-2.13.2.jar
         ```
       - ITSI version 4.4.x:

         ```
         $SPLUNK_HOME\etc\apps\SA-ITOA\lib\java\event_management\libs>"C:\Program
         Files\7-Zip\7z.exe" h .\log4j-core-2.5.jar
         ```
    3. Go to the etc/apps/SA-ITSI-MetricAD/lib/ directory.

       ```
       cd $SPLUNK_HOME\etc\apps\SA-ITSI-MetricAD\lib\
       ```
    4. Verify that the checksum of the jar matches the checksum you made note of earlier.
       - ITSI version 4.7.x, 4.9.x, 4.11.0:

         ```
         $SPLUNK_HOME\etc\apps\SA-ITSI-MetricAD\lib\>"C:\Program Files\7-Zip\7z.exe" h
         .\org.apache.logging.log4j.log4j-core-2.13.2.jar
         ```
       - ITSI version 4.4.x:

         ```
         $SPLUNK_HOME\etc\apps\SA-ITSI-MetricAD\lib\>"C:\Program Files\7-Zip\7z.exe" h
         .\org.apache.logging.log4j.log4j-core-2.3.jar
         ```

Upgrade IT Service Intelligence on a single instance

ITSI version 4.16.x is a Splunk Cloud Platform only release and is not available on-premises. Splunk Cloud Platform customers must work with Support to coordinate upgrades to IT Service Intelligence.

Upgrade IT Service Intelligence in a search head cluster environment

ITSI version 4.16.x is a Splunk Cloud Platform only release and is not available on-premises. Splunk Cloud Platform customers must work with Support to coordinate upgrades to IT Service Intelligence.

Roll back an upgrade of ITSI

ITSI version 4.16.x is a Splunk Cloud Platform only release and is not available on-premises. Splunk Cloud Platform customers must work with Support to coordinate upgrades to IT Service Intelligence.

Version-specific upgrade notes for ITSI

Consider the following guidelines when upgrading to specific versions of IT Service Intelligence.

After upgrading to version 4.11.4

After you upgrade to 4.11.4, the log4j 2.17.1 libraries are deployed and linked. Because the 4.11.4 version of Splunk IT Service Intelligence fix a product security issue, you might want to manually remove lower versions of log4j. In a typical deployment, lower versions of the log4j files are found in these locations:

- $SPLUNK_HOME/etc/apps/SA-ITOA/lib/java/event_management/libs/.bkup/log4j-api-2.17.0.jar
- $SPLUNK_HOME/etc/apps/SA-ITOA/lib/java/event_management/libs/.bkup/log4j-slf4j-impl-2.17.0.jar
- $SPLUNK_HOME/etc/apps/SA-ITOA/lib/java/event_management/libs/.bkup/log4j-core-2.17.0.jar
- $SPLUNK_HOME/etc/apps/SA-ITSI-MetricAD/lib/org.apache.logging.log4j.log4j-slf4j-impl-2.17.0.jar
- $SPLUNK_HOME/etc/apps/SA-ITSI-MetricAD/lib/org.apache.logging.log4j.log4j-api-2.17.0.jar
- $SPLUNK_HOME/etc/apps/SA-ITSI-MetricAD/lib/org.apache.logging.log4j.log4j-core-2.17.0.jar

In a search head cluster deployment, lower versions of the log4j files are found in these locations:

- $SPLUNK_HOME/etc/shcluster/apps/SA-ITOA/lib/java/event_management/libs/.bkup/log4j-api-2.17.0.jar
- $SPLUNK_HOME/etc/shcluster/apps/SA-ITOA/lib/java/event_management/libs/.bkup/log4j-slf4j-impl-2.17.0.jar
- $SPLUNK_HOME/etc/shcluster/apps/SA-ITOA/lib/java/event_management/libs/.bkup/log4j-core-2.17.0.jar
- $SPLUNK_HOME/etc/shcluster/apps/SA-ITSI-MetricAD/lib/org.apache.logging.log4j.log4j-slf4j-impl-2.17.0.jar
- $SPLUNK_HOME/etc/shcluster/apps/SA-ITSI-MetricAD/lib/org.apache.logging.log4j.log4j-api-2.17.0.jar
- $SPLUNK_HOME/etc/shcluster/apps/SA-ITSI-MetricAD/lib/org.apache.logging.log4j.log4j-core-2.17.0.jar

If there are log4j .jar files with versions lower than 2.17.1 in these directories, you can safely remove these as well.

After upgrading to version 4.11.3

After you upgrade to 4.11.3, the log4j 2.17.0 libraries are deployed and linked. Because the 4.11.3 version of Splunk IT Service Intelligence fix a product security issue, you might want to manually remove lower versions of log4j. In a typical deployment, lower versions of the log4j files are found in these locations:

- $SPLUNK_HOME/etc/apps/SA-ITOA/lib/java/event_management/libs/.bkup/log4j-api-2.16.0.jar
- $SPLUNK_HOME/etc/apps/SA-ITOA/lib/java/event_management/libs/.bkup/log4j-slf4j-impl-2.16.0.jar
- $SPLUNK_HOME/etc/apps/SA-ITOA/lib/java/event_management/libs/.bkup/log4j-core-2.16.0.jar

- $SPLUNK_HOME/etc/apps/SA-ITSI-MetricAD/lib/org.apache.logging.log4j.log4j-slf4j-impl-2.16.0.jar
- $SPLUNK_HOME/etc/apps/SA-ITSI-MetricAD/lib/org.apache.logging.log4j.log4j-api-2.16.0.jar
- $SPLUNK_HOME/etc/apps/SA-ITSI-MetricAD/lib/org.apache.logging.log4j.log4j-core-2.16.0.jar

In a search head cluster deployment, lower versions of the log4j files are found in these locations:

- $SPLUNK_HOME/etc/shcluster/apps/SA-ITOA/lib/java/event_management/libs/.bkup/log4j-api-2.16.0.jar
- $SPLUNK_HOME/etc/shcluster/apps/SA-ITOA/lib/java/event_management/libs/.bkup/log4j-slf4j-impl-2.16.0.jar
- $SPLUNK_HOME/etc/shcluster/apps/SA-ITOA/lib/java/event_management/libs/.bkup/log4j-core-2.16.0.jar
- $SPLUNK_HOME/etc/shcluster/apps/SA-ITSI-MetricAD/lib/org.apache.logging.log4j.log4j-slf4j-impl-2.16.0.jar
- $SPLUNK_HOME/etc/shcluster/apps/SA-ITSI-MetricAD/lib/org.apache.logging.log4j.log4j-api-2.16.0.jar
- $SPLUNK_HOME/etc/shcluster/apps/SA-ITSI-MetricAD/lib/org.apache.logging.log4j.log4j-core-2.16.0.jar

If there are log4j .jar files with versions lower than 2.17.0 in these directories, you can safely remove these as well.

After upgrading to version 4.11.2

After you upgrade to 4.11.2, the log4j 2.16.0 libraries are deployed and linked. Because the 4.11.2 version of Splunk IT Service Intelligence fix a product security issue, you might want to manually remove lower versions of log4j. In a typical deployment, lower versions of the log4j files are found in these locations:

- $SPLUNK_HOME/etc/apps/SA-ITOA/lib/java/event_management/libs/.bkup/log4j-api-2.15.0.jar
- $SPLUNK_HOME/etc/apps/SA-ITOA/lib/java/event_management/libs/.bkup/log4j-slf4j-impl-2.15.0.jar
- $SPLUNK_HOME/etc/apps/SA-ITOA/lib/java/event_management/libs/.bkup/log4j-core-2.15.0.jar
- $SPLUNK_HOME/etc/apps/SA-ITSI-MetricAD/lib/org.apache.logging.log4j.log4j-slf4j-impl-2.15.0.jar
- $SPLUNK_HOME/etc/apps/SA-ITSI-MetricAD/lib/org.apache.logging.log4j.log4j-api-2.15.0.jar
- $SPLUNK_HOME/etc/apps/SA-ITSI-MetricAD/lib/org.apache.logging.log4j.log4j-core-2.15.0.jar

In a search head cluster deployment, lower versions of the log4j files are found in these locations:

- $SPLUNK_HOME/etc/shcluster/apps/SA-ITOA/lib/java/event_management/libs/.bkup/log4j-api-2.15.0.jar
- $SPLUNK_HOME/etc/shclusters/apps/SA-ITOA/lib/java/event_management/libs/.bkup/log4j-slf4j-impl-2.15.0.jar
- $SPLUNK_HOME/etc/shcluster/apps/SA-ITOA/lib/java/event_management/libs/.bkup/log4j-core-2.15.0.jar
- $SPLUNK_HOME/etc/shcluster/apps/SA-ITSI-MetricAD/lib/org.apache.logging.log4j.log4j-slf4j-impl-2.15.0.jar
- $SPLUNK_HOME/etc/shcluster/apps/SA-ITSI-MetricAD/lib/org.apache.logging.log4j.log4j-api-2.15.0.jar
- $SPLUNK_HOME/etc/shcluster/apps/SA-ITSI-MetricAD/lib/org.apache.logging.log4j.log4j-core-2.15.0.jar

If there are log4j .jar files with versions lower than 2.16.0 in these directories, you can safely remove these as well.

After upgrading to version 4.11.1

After you upgrade to 4.11.1, the log4j 2.15.0 libraries are deployed and linked. Because the 4.11.1 version of Splunk IT Service Intelligence fix a product security issue, you might want to manually remove lower versions of log4j. In a typical deployment, lower versions of the log4j files are found in these locations:

- $SPLUNK_HOME/etc/apps/SA-ITOA/lib/java/event_management/libs/.bkup/log4j-api-2.13.2.jar
- $SPLUNK_HOME/etc/apps/SA-ITOA/lib/java/event_management/libs/.bkup/log4j-slf4j-impl-2.13.2.jar
- $SPLUNK_HOME/etc/apps/SA-ITOA/lib/java/event_management/libs/.bkup/log4j-core-2.13.2.jar
- $SPLUNK_HOME/etc/apps/SA-ITSI-MetricAD/lib/org.apache.logging.log4j.log4j-slf4j-impl-2.13.2.jar

- $SPLUNK_HOME/etc/apps/SA-ITSI-MetricAD/lib/org.apache.logging.log4j.log4j-api-2.13.2.jar
- $SPLUNK_HOME/etc/apps/SA-ITSI-MetricAD/lib/org.apache.logging.log4j.log4j-core-2.13.2.jar

In a search head cluster deployment, lower versions of the log4j files are found in these locations:

- $SPLUNK_HOME/etc/shcluster/apps/SA-ITOA/lib/java/event_management/libs/.bkup/log4j-api-2.13.2.jar
- $SPLUNK_HOME/etc/shcluster/apps/SA-ITOA/lib/java/event_management/libs/.bkup/log4j-slf4j-impl-2.13.2.jar
- $SPLUNK_HOME/etc/shcluster/apps/SA-ITOA/lib/java/event_management/libs/.bkup/log4j-core-2.13.2.jar
- $SPLUNK_HOME/etc/shcluster/apps/SA-ITSI-MetricAD/lib/org.apache.logging.log4j.log4j-slf4j-impl-2.13.2.jar
- $SPLUNK_HOME/etc/shcluster/apps/SA-ITSI-MetricAD/lib/org.apache.logging.log4j.log4j-api-2.13.2.jar
- $SPLUNK_HOME/etc/shcluster/apps/SA-ITSI-MetricAD/lib/org.apache.logging.log4j.log4j-core-2.13.2.jar

If there are log4j .jar files with versions lower than 2.15.0 in these directories, you can safely remove these as well.

After upgrading to version 4.9.6

After you upgrade to 4.9.6, the log4j 2.16.0 libraries are deployed and linked. Because the 4.9.6 version of Splunk IT Service Intelligence fix a product security issue, you might want to manually remove lower versions of log4J. In a typical deployment, lower versions of the log4J files are found in these locations:

- $SPLUNK_HOME/etc/apps/SA-ITOA/lib/java/event_management/libs/.bkup/log4j-api-2.15.0.jar
- $SPLUNK_HOME/etc/apps/SA-ITOA/lib/java/event_management/libs/.bkup/log4j-slf4j-impl-2.15.9.jar
- $SPLUNK_HOME/etc/apps/SA-ITOA/lib/java/event_management/libs/.bkup/log4j-core-2.15.0.jar
- $SPLUNK_HOME/etc/apps/SA-ITSI-MetricAD/lib/org.apache.logging.log4j.log4j-slf4j-impl-2.15.0.jar
- $SPLUNK_HOME/etc/apps/SA-ITSI-MetricAD/lib/org.apache.logging.log4j.log4j-api-2.15.0.jar
- $SPLUNK_HOME/etc/apps/SA-ITSI-MetricAD/lib/org.apache.logging.log4j.log4j-core-2.13.2.jar

In a search head cluster deployment, lower versions of the log4j files are found in these locations:

- $SPLUNK_HOME/etc/shcluster/apps/SA-ITOA/lib/java/event_management/libs/.bkup/log4j-api-2.15.0.jar
- $SPLUNK_HOME/etc/shcluster/apps/SA-ITOA/lib/java/event_management/libs/.bkup/log4j-slf4j-impl-2.15.9.jar
- $SPLUNK_HOME/etc/shcluster/apps/SA-ITOA/lib/java/event_management/libs/.bkup/log4j-core-2.15.0.jar
- $SPLUNK_HOME/etc/shcluster/apps/SA-ITSI-MetricAD/lib/org.apache.logging.log4j.log4j-slf4j-impl-2.15.0.jar
- $SPLUNK_HOME/etc/shcluster/apps/SA-ITSI-MetricAD/lib/org.apache.logging.log4j.log4j-api-2.15.0.jar
- $SPLUNK_HOME/etc/shcluster/apps/SA-ITSI-MetricAD/lib/org.apache.logging.log4j.log4j-core-2.13.2.jar

If there are log4j .jar files with versions lower than 2.16.0 in these directories, you can safely remove these as well.

After upgrading to version 4.9.5

After you upgrade to 4.9.5, the log4j 2.15.0 libraries are deployed and linked. Because the 4.9.5 version of Splunk IT Service Intelligence fix a product security issue, you might want to manually remove lower versions of log4J. In a typical deployment, lower versions of the log4J files are found in these locations:

- $SPLUNK_HOME/etc/apps/SA-ITOA/lib/java/event_management/libs/.bkup/log4j-api-2.13.2jar
- $SPLUNK_HOME/etc/apps/SA-ITOA/lib/java/event_management/libs/.bkup/log4j-slf4j-impl-2.13.2.jar
- $SPLUNK_HOME/etc/apps/SA-ITOA/lib/java/event_management/libs/.bkup/log4j-core-2.13.2.jar
- $SPLUNK_HOME/etc/apps/SA-ITSI-MetricAD/lib/org.apache.logging.log4j.log4j-slf4j-impl-2.13.2.jar
- $SPLUNK_HOME/etc/apps/SA-ITSI-MetricAD/lib/org.apache.logging.log4j.log4j-api-2.13.2.jar

- $SPLUNK_HOME/etc/apps/SA-ITSI-MetricAD/lib/org.apache.logging.log4j.log4j-core-2.13.2.jar

In a search head cluster deployment, lower versions of the log4j files are found in these locations:

- $SPLUNK_HOME/etc/shcluster/apps/SA-ITOA/lib/java/event_management/libs/.bkup/log4j-api-2.13.2jar
- $SPLUNK_HOME/etc/shcluster/apps/SA-ITOA/lib/java/event_management/libs/.bkup/log4j-slf4j-impl-2.13.2.jar
- $SPLUNK_HOME/etc/shclusters/apps/SA-ITOA/lib/java/event_management/libs/.bkup/log4j-core-2.13.2.jar
- $SPLUNK_HOME/etc/shcluster/apps/SA-ITSI-MetricAD/lib/org.apache.logging.log4j.log4j-slf4j-impl-2.13.2.jar
- $SPLUNK_HOME/etc/shcluster/apps/SA-ITSI-MetricAD/lib/org.apache.logging.log4j.log4j-api-2.13.2.jar
- $SPLUNK_HOME/etc/shcluster/apps/SA-ITSI-MetricAD/lib/org.apache.logging.log4j.log4j-core-2.13.2.jar

If there are log4j .jar files with versions lower than 2.15.0 in these directories, you can safely remove these as well.

After upgrading to version 4.9.0

As of version 4.9.0, the Splunk App for Infrastructure will no longer be packaged with ITSI. You will no longer be able to integrate or import entities from SAI to ITSI. Additionally, all `servicesNS/nobody/SA-ITOA/itoa_entity_exchange/` REST endpoints will be disabled and return error codes. Additionally, the `itsi_im_metrics` index has replaced the `em_metrics` index.

Instead, you will be able to run discovery entity saved searches directly from ITSI. Your existing SAI entities will still be discovered as native entities in ITSI.

To enable entity discovery for these existing SAI entities, you must update your data sources and enable saved searches. For more information, see Use the ITSI entity discovery search.

After upgrading to version 4.7.4

After you upgrade to 4.7.4, the log4j 2.16.0 libraries are deployed and linked. Because the 4.7.4 versions of Splunk IT Service Intelligence fix a product security issue, you might want to manually remove lower versions of log4J. In a typical deployment, lower versions of the log4J files are found in these locations:

- $SPLUNK_HOME/etc/apps/SA-ITOA/lib/java/event_management/libs/.bkup/log4j-api-2.15.0.jar
- $SPLUNK_HOME/etc/apps/SA-ITOA/lib/java/event_management/libs/.bkup/log4j-slf4j-impl-2.15.0.jar
- $SPLUNK_HOME/etc/apps/SA-ITOA/lib/java/event_management/libs/.bkup/log4j-core-2.15.0.jar
- $SPLUNK_HOME/etc/apps/SA-ITSI-MetricAD/lib/org.apache.logging.log4j.log4j-slf4j-impl-2.15.0.jar
- $SPLUNK_HOME/etc/apps/SA-ITSI-MetricAD/lib/org.apache.logging.log4j.log4j-api-2.15.0.jar
- $SPLUNK_HOME/etc/apps/SA-ITSI-MetricAD/lib/org.apache.logging.log4j.log4j-core-2.15.0.jar

In a search head cluster deployment, lower versions of the log4j files are found in these locations:

- $SPLUNK_HOME/etc/shcluster/apps/SA-ITOA/lib/java/event_management/libs/.bkup/log4j-api-2.15.0.jar
- $SPLUNK_HOME/etc/shcluster/apps/SA-ITOA/lib/java/event_management/libs/.bkup/log4j-slf4j-impl-2.15.0.jar
- $SPLUNK_HOME/etc/shcluster/apps/SA-ITOA/lib/java/event_management/libs/.bkup/log4j-core-2.15.0.jar
- $SPLUNK_HOME/etc/shcluster/apps/SA-ITSI-MetricAD/lib/org.apache.logging.log4j.log4j-slf4j-impl-2.15.0.jar
- $SPLUNK_HOME/etc/shcluster/apps/SA-ITSI-MetricAD/lib/org.apache.logging.log4j.log4j-api-2.15.0.jar
- $SPLUNK_HOME/etc/shcluster/apps/SA-ITSI-MetricAD/lib/org.apache.logging.log4j.log4j-core-2.15.0.jar

If there are log4j .jar files with versions lower than 2.16.0 in these directories, you can safely remove these as well.

After upgrading to version 4.7.3

After you upgrade to 4.7.3, the log4j 2.15.0 libraries are deployed and linked. Because the 4.7.3 version of Splunk IT Service Intelligence fix a product security issue, you might want to manually remove lower versions of log4J. In a typical deployment, lower versions of the log4J files are found in these locations:

- $SPLUNK_HOME/etc/apps/SA-ITOA/lib/java/event_management/libs/.bkup/log4j-api-2.13.2.jar
- $SPLUNK_HOME/etc/apps/SA-ITOA/lib/java/event_management/libs/.bkup/log4j-slf4j-impl-2.13.2.jar
- $SPLUNK_HOME/etc/apps/SA-ITOA/lib/java/event_management/libs/.bkup/log4j-core-2.13.2.jar
- $SPLUNK_HOME/etc/apps/SA-ITSI-MetricAD/lib/org.apache.logging.log4j.log4j-slf4j-impl-2.13.2.jar
- $SPLUNK_HOME/etc/apps/SA-ITSI-MetricAD/lib/org.apache.logging.log4j.log4j-api-2.13.2.jar
- $SPLUNK_HOME/etc/apps/SA-ITSI-MetricAD/lib/org.apache.logging.log4j.log4j-core-2.13.2.jar

In a search head cluster deployment, lower versions of the log4j files are found in these locations:

- $SPLUNK_HOME/etc/shcluster/apps/SA-ITOA/lib/java/event_management/libs/.bkup/log4j-api-2.13.2.jar
- $SPLUNK_HOME/etc/shcluster/apps/SA-ITOA/lib/java/event_management/libs/.bkup/log4j-slf4j-impl-2.13.2.jar
- $SPLUNK_HOME/etc/shcluster/apps/SA-ITOA/lib/java/event_management/libs/.bkup/log4j-core-2.13.2.jar
- $SPLUNK_HOME/etc/shcluster/apps/SA-ITSI-MetricAD/lib/org.apache.logging.log4j.log4j-slf4j-impl-2.13.2.jar
- $SPLUNK_HOME/etc/shcluster/apps/SA-ITSI-MetricAD/lib/org.apache.logging.log4j.log4j-api-2.13.2.jar
- $SPLUNK_HOME/etc/shcluster/apps/SA-ITSI-MetricAD/lib/org.apache.logging.log4j.log4j-core-2.13.2.jar

If there are log4j .jar files with versions lower than 2.15.0 in these directories, you can safely remove these as well.

After upgrading to version 4.6.1

A new metrics-based summary index was introduced in ITSI version 4.6.0. To provide a more continuous experience, a backfill process queue modular input was added to migrate data from the itsi_summary index to the new metrics-based index.

In version 4.6.1, the modular input for backfill functionality is disabled by default as opposed to running automatically. If you upgraded to version 4.6.1 or higher and you need to use the Service Analyzer to inspect service or KPI data from before the upgrade, enable the backfill modular input. If you choose not to enable it, note that sparklines on the Service Analyzer might appear flat for about 1-15 minutes after upgrade due to lack of data.

To enable the modular input, perform the following steps:

1. Within ITSI, go to **Settings** > **Data Inputs**.
2. Open the modular input called **IT Service Intelligence Metrics Backfill Process Queue**.
3. Click **Enable**.

Optionally, you can modify the default configurations to backfill more or less data. If you do modify the defaults, first determine if your environment can backfill data at a higher rate than set by the default throttle and concurrent search settings.

For more information about the metrics index, see ITSI metrics summary index reference in the *Administration Manual*.

After upgrading to version 4.4.x

Consider the following when upgrading to version 4.4.x:

Copy SA-ITOA to the license master

Version 4.4.x has an additional requirement of copying `SA-ITOA` to the license master and manually disabling all inputs in `inputs.conf`. For instructions, see ITSI-4813 in the IT Service Intelligence *Release Notes*.

itsi_rules_engine.properties

As of version 4.4.x, you can make changes to a local copy of the `itsi_rules_engine.properties` file at `$SPLUNK_HOME/etc/apps/SA-ITOA/local/` and these changes will take precedence over the default file. Previously, this file was not treated like a regular Splunk .conf file, so changes to a local copy of the file had no impact. For more information, see Configuration file precedence in the Splunk Enterprise *Admin Manual*.

If you've made changes to the default file in the past, make a copy of these changes before upgrading to 4.4.x. After you upgrade, create a blank `itsi_rules_engine.properties` file at `$SPLUNK_HOME/etc/apps/SA-ITOA/local/` and add these changed settings to the local file. This step ensures that your changes to the file will persist through future upgrades.

Make all future changes to `itsi_rules_engine.properties` in the local file rather than the default file. For the contents of the file, see Rules Engine properties reference in ITSI in the *Event Analytics Manual*.

After upgrading to version 4.2.x

The `Entity Alias Filtering` field used in KPI searches was removed in version 4.2.0. With the removal of entity alias filtering, ITSI now strictly matches entities against KPI search results using both the alias key and value, whereas before it only used the alias value.

This strict association change can cause some entities to not be included in KPI results. If this is the case, a message appears in Splunk Web with a link to documentation on how to fix potentially broken entities. For information, see Removed features in Splunk IT Service Intelligence.

After upgrading to version 4.0.4

To initiate the fix for ITSI-1868 concerning entity rules, you need to trigger the service-entity rule change handler. To trigger the handler, run the kvstore_to_json mode 4 option, which will regenerate your KPI search schedules.

After upgrading to version 4.0.x

1. Remove unnecessary XML files from the ITSI OS Module that were removed or renamed as of ITSI 4.0.0. Remove the following files from `$SPLUNK_HOME/etc/apps/DA-ITSI-OS/default/data/ui/panels`:

    - cpu_memory_usage.xml
    - memory_free_percent.xml
    - memory_disk_ops.xml
    - forecast_network.xml
    - storage_volumes_most_used.xml
    - storage_devices_iostats_chart.xml

- Version 4.0.x ships with an internal **license stack** called `IT Service Intelligence Internals *DO NOT COPY* stack` to ensure that you don't pay for notable events generated by ITSI. The sourcetypes used to track notable events and episodes are counted on this special stack with no impact on your Splunk Enterprise license. When calculating your daily license usage, disregard this stack.

After upgrading to version 3.1.x

1. If you have a dedicated license master, remove `SA-ITOA` from the license master since ITSI no longer requires the add-on as of version 3.1.x.
2. When the objects in ITSI are exported during a backup or migration, if the number of KPIs linked to a service is high, the instance can hit a KV store memory size limit causing some objects to be dropped from the backup and lost after the upgrade.

   Workaround: Increase the KV store bulk get limit in `$SPLUNK_HOME/etc/apps/SA-ITOA/local/limits.conf` and retry the backup or upgrade. Increase the `max_size_per_result_mb` value as necessary.

   ```
   [kvstore]
   # The maximum size, in megabytes (MB), of the result that will be returned for a single query to a
   collection.
   # ITSI requires approximately 50MB per 1,000 KPIs. Override this value if necessary.
   # Default: 500 MB
   max_size_per_result_mb = 500
   ```

This action increases the memory used by the KV store during operations.

Troubleshoot an upgrade of IT Service Intelligence

Use this information to troubleshoot post-upgrade issues.

The ITSI upgrade page is stuck

The migration process is interrupted and ITSI upgrade page is stuck even after a restart.

Cause

Interruptions to the migration process, such as a Splunk restart, might cause the migration page to become stuck.

Resolution

First, check the upgrade status by running the following command:

```
curl -k -u admin:changeme -X GET https://localhost:8089/servicesNS/nobody/SA-ITOA/migration/info
```

Sample response:

```
{
    "is_running": true,
    "start_time": {
        "since_unix_epoch": 1593203210.6703181,
        "utc": "2020-06-26T20:26:50Z"
    },
```

```
    "skip_local_failure": true
}
```

If `is_running` is `true` and the migration has been stuck for a long time, you can clear the itsi_migration_status KV store collection and then go to the ITSI app upgrade page to trigger another migration. The following command clears the upgrade KV store collection:

```
curl -k -u admin:changeme -X DELETE
https://localhost:8089/servicesNS/nobody/SA-ITOA/storage/collections/data/itsi_migration_status
```

Teams validation checks, UI loading, and team creation script fail

The ITSI teams validation checks, UI loading, and the team creation script fail when your Splunk Enterprise instance has a role issue. Roles issues often happen on deployments where a role is missing. For example `role_A` inherits from `role_B`, but at some point the app where `role_B` is defined was removed.

First, run the following search to determine whether you're experience this issue:

```
index=_internal source=*splunkd.log* ( ERROR "Error retrieving info for role" ) OR ( WARN "Unknown role" )
```

If there's a role issue, the following errors appear every minute for each broken role:

```
11-22-2019 09:22:13.260 -0800 ERROR AdminHandler:AuthenticationHandler - Error retrieving info for role:
role_B
```

If this is the case, identify all the roles that are trying to link to the missing roles with the following btool command:

```
./splunk btool authorize list | grep role_B
```

For more information, see Use btool to troubleshoot configurations in the Splunk Enterprise *Troubleshooting Manual*.

To fix the issue, perform one of the following steps:

- Create a local version of authorize.conf at `$SPLUNK_HOME/etc/apps/SA-ITOA/local/` and modify the import list.
- Use the UI to edit the role.
- Recreate the missing role.

Knowledge objects are missing after upgrade

If some objects, such as service analyzers, glass tables, or deep dives, are missing from the UI or unaccessible after you upgrade, the ACL objects corresponding to the objects might be missing or corrupted.

1. See if the object exists in the KV store. Even if it does exist, there could be duplicates, which you'll address in the next step. Check the list of knowledge objects by name at the following endpoints:
    - ◊ curl -k -u admin:password https://<host>:<admin_port>/servicesNS/nobody/SA-ITOA/itoa_interface/deep_dive
        - · curl -k -u admin:password https://<host>:<admin_port>/servicesNS/nobody/SA-ITOA/itoa_interface/glass_table
            - curl -k -u admin:password https://<host>:<admin_port>/servicesNS/nobody/SA-ITOA/itoa_interface/home_view
                - ♦ curl -k -u admin:password https://<host>:<admin_port>/servicesNS/nobody/SA-ITOA/itoa_interface/event_m
                    - ◊ curl -k -u admin:password https://<host>:<admin_port>/servicesNS/nobody/SA-ITOA/event_manage

- curl -k -u admin:password https://<host>:<admin_port>/servicesNS/nobody/SA-ITOA/event_

The value of the _key attribute is called obj_id or object ID in the next steps.

◊ Check if a corresponding ACL object exists with the ID of the object you're looking for at the following endpoint:
curl -k -u admin:password https://<host>:<admin_port>/servicesNS/nobody/SA-UserAccess/storage/

1. If one ACL object exists with the corresponding object ID, and the object is still missing from the UI, contact Splunk Support.
2. If two ACL objects exists with the corresponding object ID, delete one of them by running the following command:
   curl -k -u admin:password -X DELETE https://<host>:<admin_port>/servicesNS/nobody/SA-UserAccess/
3. If no ACL object exists with the corresponding object ID, manually create an ACL object with the following command:
   curl -k -u admin:password https://<host>:<admin_port>/servicesNS/nobody/SA-UserAccess/
   -H "Content-Type: application/json" -X POST -d '{"obj_type":"<OBJ_TYPE>","acl_owner":"nobody","acl_id":"<ACL
   Replace the tokens with the following values:

Object name	OBJ_TYPE	OBJ_STORENAME
Service analyzer	home_view	itsi_service_analyzer
Deep dive	deep_dive	itsi_pages
Glass table	glass_table	itsi_pages
Episode review	event_management_state	itsi_event_management
Notable event aggregation policy	notable_aggregation_policy	itsi_notable_event_aggregation_
Correlation search	correlation_search	itsi_correlation_search

ACL_ID must be a unique value.

The Global team is missing after upgrade

All services in ITSI must be assigned to a team. If migration fails with the error `Failed to import Team settings`, you can manually run the Python script called `itsi_reset_default_team.py`. The script manually creates the Global team in the KV store which completes the migration.

To run the script, perform the following steps:

1. Run the following commands on any search head in your ITSI deployment:

   ```
   cd $SPLUNK_HOME/etc/apps/SA-ITOA/bin
   $SPLUNK_HOME/bin/splunk cmd python itsi_reset_default_team.py
   ```
2. Provide the splunkd port number and your Splunk username and password when prompted.
   After the script finishes successfully, the Global team is created in the KV store.
3. Restart your Splunk software.

Duplicate Windows or VMware entities after entity import

Cause

The ITSI Import Objects - VMware VM saved searches fails to merge entities with the `host` field and may create duplicate entities.

Resolution

Update the saved search.

1. Disable the ITSI Import Objects - VMware VM saved search.
2. Copy the ITSI Import Objects - VMware VM saved search and change the `entity_merge_field` attribute to `host`.
3. Enable the updated ITSI Import Objects - VMware VM search.

Duplicate ITSI license error

Cause

Two ITSI licenses are being flagged as duplicates on the system.

Resolution

Enable `AllowDuplicateKeys` in the license XML.

1. Go to the node where search peers are configured.
2. Identify the Splunk licenses (Enterprise, ITSI, non ITSI) currently installed. Ignore licenses under **IT Service Intelligence Internals DO NOT COPY**.
3. Navigate to http://LM_IP/en-US/manager/system/licensing/licenses and check if the `AllowDuplicateKeys` capability is enabled for each of the license identified in step 1.
4. If not enabled, procure a new license from Splunk support and replace it.
5. Make sure all licenses in the stack have the capability enabled.
6. Restart Splunk.

Here is a sample license with `AllowDuplicateKeys` enabled:

```
<?xml version="1.0" encoding="UTF-8"?>
<license>
  <signature>UktliszY9Qpn3FiNwRqNHpTyYLfPW4ehn0LZOyamhD8Iuj6jhULWKRkuRq5dSE9Q67pc8NoLpyHRTU5s1cDXL+1vSWzfw
ooWszTvnh3pFxxQExnniRveifUqq7Xc15lVoab6WMxq4DmggAoco39e6UeNPGS2l+b6ASZ8jVm8xj7kzsmBTPQF0+nH1eAX0EE6Y9rC8
/B4k9cTzZKeWPlfDU7OvoZT2rmirLdURUXaaRE9khwH68iMsID8ODqSzH2+bboAaaFXAbh
/PU2HqYUzumzxzqf4s7fTlGmwCY+lMAUQHXaZV7eaCY35A762XWbYZ90k9BS+lboiI2MLOYVPOQ==</signature>
  <payload>
    <type>enterprise</type>
    <group_id>Enterprise</group_id>
    <quota>1</quota>
    <max_violations>5</max_violations>
    <window_period>30</window_period>
    <creation_time>1618383600</creation_time>
    <label>Splunk IT Service Intelligence Internal License DO NOT DISTRIBUTE</label>
    <expiration_time>1659205961</expiration_time>
    <features>
      <feature>Auth</feature>
      <feature>FwdData</feature>
      <feature>LocalSearch</feature>
      <feature>ScheduledSearch</feature>
      <feature>AllowDuplicateKeys</feature>
      <feature>Alerting</feature>
      <feature>SplunkWeb</feature>
    </features>
    <add_ons>
      <add_on name="itsi" type="app">
        <parameter key="size" value="1000000"/>
      </add_on>
    </add_ons>
    <sourcetypes/>
  <guid>F4C8DBB2-84F2-4A82-AA43-CA7CA786B360</guid></payload>
</license>
```

Prechecks fail during the upgrade

One of the migration jobs that run during the ITSI upgrade process displays a **Failed** status.

Cause

Errors with specific ITSI objects, such as as services or KPIs, are causing issues with the upgrade and need to be addressed.

Resolution

When one of the checks fail, you can either select **Proceed anyway** or **Restart upgrade**:

- When you select **Proceed anyway**, the precheck job runs again but ignores any failed prechecks and continues with the upgrade. You can choose to fix the errors identified by the prechecks at a later time.
- When you select **Restart upgrade**, the prechecks run again. If there are still failed prechecks, contact Splunk Support.

ITSI upgrade paths

Use the following table to determine the upgrade path for your version of IT Service Intelligence. ITSI supports direct upgrades from up to three versions prior to the one you're upgrading to. To upgrade from earlier versions, perform step upgrades, and follow the on-prem upgrade path if you are performing step upgrades from an on-prem version. When

upgrading ITSI, Splunk Cloud Platform customers work with Splunk Support to coordinate upgrades to IT Service Intelligence.

ITSI Version	Cloud upgrade path	On-premises upgrade path
4.17.x	Direct upgrade for the following: • 4.14.x 4.17.x • 4.15.x 4.17.x • 4.16.x 4.17.x Step upgrade for the following: • 4.9.x 4.12.x 4.15.x 4.17.x • 4.10.x 4.11.x 4.14.x 4.17.x	
4.16.x (Cloud only)	Direct upgrade for the following: • 4.13.x 4.16.x • 4.14.x 4.16.x • 4.15.x 4.16.x Step upgrade for the following: • 4.9.x 4.11.x 4.14.x 4.16.x • 4.10.x 4.12.x 4.13.x 4.16.x **Note:** Note: Splunk Cloud Platform customers work with Splunk Support to coordinate upgrades to IT Service Intelligence.	N/A
4.15.x	Direct upgrade for the following: • 4.12.x 4.15.x • 4.14.x 4.15.x	• 4.9.x 4.11.x 4.13.x 4.15.x • 4.13.x 4.15.x
4.14.x (Cloud only)	Direct upgrade for the following: • 4.11.x 4.14.x • 4.12.x 4.14.x • 4.13.x 4.14.x Step upgrade for the following: • 4.9.x 4.12.x 4.14.x • 4.10.x 4.13.x 4.14.x **Note:** Note: Splunk Cloud Platform customers work with Splunk Support to coordinate upgrades to IT Service Intelligence.	N/A
4.13.x	Direct upgrade for the following: • 4.9.x 4.10.x, 4.11.x, or 4.12.x • 4.10.x 4.13.x	• 4.9.x 4.11.x 4.13.x • 4.11.x 4.13.x
4.12.x (Cloud Only)	Direct upgrade for the following: • 4.9.x 4.12.x • 4.10.x 4.12.x • 4.11.x 4.12.x	N/A

ITSI Version	Cloud upgrade path	On-premises upgrade path
	Note: Splunk Cloud Platform customers work with Splunk Support to coordinate upgrades to IT Service Intelligence.	
4.11.x	Direct upgrade for the following: • 4.8.x 4.11.x • 4.9.x 4.11.x • 4.10.x 4.11.x	Direct upgrade path for: • 4.9.x 4.11.x
4.10.x (Cloud Only)	Direct upgrade for the following: • 4.7.x 4.10.x • 4.8.x 4.10.x • 4.9.x 4.10.x Step upgrade for versions older than 4.7.x **Note:** Note: Splunk Cloud Platform customers work with Splunk Support to coordinate upgrades to IT Service Intelligence.	N/A
4.9.x	Direct upgrade for the following: • 4.6.x 4.9.x • 4.7.x 4.9.x • 4.8.x 4.9.x Step upgrade for versions older than 4.6.x	4.7.x 4.9.x
4.8.x (Cloud Only)	Direct upgrade for the following: • 4.5.x 4.8.x • 4.6.x 4.8.x • 4.7.x 4.8.x Step upgrade for versions older than 4.5.x **Note:** Note: Splunk Cloud Platform customers work with Splunk Support to coordinate upgrades to IT Service Intelligence.	N/A
4.7.x	Direct upgrade for the following: • 4.4.x 4.7.x • 4.5.x 4.7.x • 4.6.x 4.7.x Step upgrade for versions older than 4.4.x	4.5.x 4.7.x