Splunk® Supported Add-ons
Splunk Add-on for Tomcat released

Generated: 11/05/2022 12:00 pm

Table of Contents

Overview

About the Splunk Add-on for Tomcat

Version	3.1.1
Vendor Products	Apache Tomcat 8.0, 8.5.61 and 9.0.41, 10.0.12, 10.0.23

The Splunk Add-on for Tomcat allows a Splunk software administrator to pull Tomcat logs from a local Tomcat server and Tomcat performance data from local and remote Tomcat servers. This add-on provides the inputs and **CIM**-compatible knowledge to use with other Splunk apps, such as Splunk Enterprise Security, the Splunk App for PCI Compliance, and Splunk IT Service Intelligence.

You must also install and configure the Splunk Add-on for Java Management Extensions (JMX) if you want to collect Tomcat performance data provided by MBean attributes.

Download the Splunk Add-on for Tomcat from Splunkbase at http://splunkbase.splunk.com/app/2911.

See the Splunk Community page for questions related to Splunk Add-on for Tomcat.

Hardware and software requirements for the Splunk Add-on for Tomcat

Prerequisites

The Splunk Add-on for Tomcat supports multiple data inputs, each capable of collecting different data from your Tomcat servers. For more information about which kind of data you can collect with which input, refer to the source types page.

Collecting local log files

If you want to collect local Tomcat log files, you must install a Splunk Enterprise forwarder or single instance directly on the machine running your Tomcat server, so it can access the logs locally.

Enable the logs you want to collect on the Tomcat server.

For instructions on enabling catalina, localhost, manager, and host-manager logs, see https://tomcat.apache.org/tomcat-10.0-doc/logging.html.

For instructions on enabling localhost_access_log, see https://tomcat.apache.org/tomcat-10.0-doc/config/valve.html#Access_Logging.

Collecting performance metrics from MBean attributes

The following is required if you would like to collect Tomcat server performance metrics from MBean attributes. You need to collect these metrics if you are planning to use Splunk IT Service Intelligence.

- Install the Splunk Add-on for Java Management Extensions (JMX) to your search heads and to at least one heavy forwarder. See the *Splunk Add-on for Java Management Extensions* documentation for installation and configuration information.

- Enable JMX remote on the Tomcat servers for which you would like to collect performance metrics. This enables the Splunk Add-on for JMX to make the JMX connection to the Tomcat server. See https://tomcat.apache.org/tomcat-10.0-doc/monitoring.html for information.
- Java Runtime 1.7 or later must be installed on the same machine as the Splunk Add-on for Tomcat.

Splunk platform requirements

Because this add-on runs on the Splunk platform, all of the system requirements apply for the Splunk software that you use to run this add-on.

- For Splunk Enterprise system requirements: see System Requirements in the Splunk Enterprise *Installation Manual*.
- For Splunk Light system requirements: see System Requirements in the Splunk Light *Installation Manual*.
- If you are managing on-premises forwarders to get data into Splunk Cloud, see System Requirements in the Splunk Enterprise *Installation Manual*, which includes information about forwarders.

Installation overview for the Splunk Add-on for Tomcat

Install and configure this add-on on your supported platform.

1. Download the add-on from Splunkbase.
2. If you want to collect performance metrics, install the latest version of Splunk Add-on for Java Management Extensions (JMX) on the Splunk Enterprise instance responsible for JMX data collection, usually a heavy forwarder.
3. Install the Splunk Add-On for Tomcat.
4. If collecting performance metrics, configure JMX inputs for the Splunk Add-on for Tomcat.
5. Set up the Splunk Add-on for Tomcat to configure the modular input for thread information and monitor inputs for local logs.
6. Enable and validate inputs for the Splunk Add-on for Tomcat.
7. Enable saved searches for the Splunk Add-on for Tomcat.

Installation and Configuration

Install the Splunk Add-on for Tomcat

Installation instructions

See Installing add-ons in *Splunk Add-Ons* for detailed instructions describing how to install a Splunk add-on in the following deployment scenarios:

- Single-instance Splunk Enterprise
- Distributed Splunk Enterprise
- Splunk Cloud
- Splunk Light

Distributed deployments

Use the tables below to determine where and how to install this add-on in a distributed deployment of Splunk Enterprise.

Where to install this add-on

This table provides a quick reference for installing this add-on to a distributed deployment of Splunk Enterprise.

Splunk instance type	Supported	Required	Comments
Search Heads	Yes	Yes	Install this add-on to all search heads where Tomcat knowledge management is required.
Indexers	Yes	Conditional	Not required if you use heavy forwarders to monitor Tomcat log files directly on Tomcat machines. Required if you use universal forwarders for monitor inputs.
Heavy Forwarders	Yes	Yes	This add-on requires heavy forwarders to perform data collection using JMX and modular inputs. Heavy forwarder needs to be installed directly on the Tomcat server for file monitoring of local logs.
Universal Forwarders	Yes	No	Supported for monitor inputs only. Universal forwarder needs to be installed directly on the Tomcat server for file monitoring of local logs. You must also install this add-on on your indexers if you use a universal forwarder rather than a heavy forwarder to monitor local Tomcat log files.

Distributed deployment feature compatibility

This table provides a quick reference for the compatibility of this add-on with Splunk distributed deployment features.

Distributed deployment feature	Supported	Comments
Search Head Clusters	Yes	You can install this add-on on a search head cluster for all search-time functionality, but configure inputs on forwarders to avoid duplicate data collection. Before installing this add-on to a cluster, make the following changes to the add-on package (if the file is present): 1. Remove the `inputs.conf` file.

Distributed deployment feature	Supported	Comments
Indexer Clusters	Yes	Before installing this add-on to a cluster, make the following changes to the add-on package (if the file is present): 1. Remove the `inputs.conf` file.
Deployment Server	Yes	Note: • Using a deployment server to deploy the configured add-on to multiple forwarders acting as data collectors may cause duplication of data if multiple forwarders are collecting data from the same remote Tomcat server. • The add-on uses the credential vault to secure your credentials, and this credential management solution is incompatible with the deployment server. Make sure that the deployment server and forwarder uses the same credential vault. Alternatively, configure the add-on on the deployment server with Tomcat credentials in plain text and after pushing the configured add-on to the forwarder, the credentials would be encrypted.

Configure JMX inputs for the Splunk Add-on for Tomcat

The Splunk Add-on for Tomcat relies on the Splunk Add-on for JMX to collect performance metrics for local or remote Tomcat servers using MBean attributes. The Splunk Add-on for Tomcat provides a `jmx_templates.conf` file that the Splunk Add-on for JMX can invoke.

If you do not want to collect performance metrics for the Tomcat server and only want to collect local logs or thread information for Tomcat threads, you do not need to perform this configuration. This configuration is necessary if you want to use your Tomcat data with Splunk IT Service Intelligence.

To collect MBean attributes from a Tomcat server, Java Runtime 1.7 or later must be installed on the same machine as the Splunk Add-on for Tomcat. You also need to enable JMX remote on the Tomcat server. See Tomcat documentation.

1. Install the Splunk Add-on for JMX on the Splunk Enterprise instance responsible for JMX data collection, usually a heavy forwarder. This add-on can collect JMX metrics locally or remotely.

2. Go to Splunk Web and access the configuration pages for the Splunk Add-on for JMX, either by clicking **Splunk Add-on for JMX** in the left nav, or going to **Apps > Manage Apps**, then clicking **Launch app** in the row for Splunk Add-on for JMX.

3. Click **Add Server** to add a new JMX server.

4. Enter a **Name** and an optional **JVM Description** for your Tomcat server.

5. For **Connection Type**, select one of the following from the dropdown menu:

Connection type	Local or remote	Special instructions
Use URL directly	The Tomcat server can be local (installed on the same server as the Splunk Add-on for JMX) or remote.	Use the hostname rather than the IP address in the URL. For example: `service:jmx:rmi:///jndi/rmi://tomcat.linux.demo:8888/jmxrmi`
rmi	The Tomcat server can be local (installed on the same	If you select this option, set the **Stub Source** to `jndi`. Use the hostname rather than the IP address. Example Host: `tomcat.linux.demo`; Example Port: `8888`.

Connection type	Local or remote	Special instructions
	server as the Splunk Add-on for JMX) or remote.	
Customized script	The Tomcat server must be installed on the same server as the Splunk Add-on for JMX.	None.
Process id	The Tomcat server must be installed on the same server as the Splunk Add-on for JMX.	None
Process file	The Tomcat server must be installed on the same server as the Splunk Add-on for JMX.	None

6. Click **Create**.

7. Navigate to the task configurations by clicking **Configurations > Tasks**.

8. Click **Add Task** to create a new JMX task.

9. Enter a **Name** and optional **Description** for your task, then select the server that you just configured in the **Servers** tab.

10. On the **Templates** tab, select one or more of the predefined templates for Tomcat to collect the data that you want.

11. On the **Settings** tab, set the Source Type to `tomcat:jmx`.

12. Click **Create** to enable your JMX input.

13. Validate that data is coming in by searching for:

```
sourcetype=tomcat:jmx
```

For more information about configuring JMX inputs, refer to Configure the inputs for the Splunk Add-on for JMX in the Splunk Add-on for Java Management Extensions manual.

Set up the Splunk Add-on for Tomcat

After you have installed the Splunk Add-on for Tomcat, you need to configure the inputs for the add-on. If you want to collect local Tomcat logs only, you can perform this configuration using either the Settings > Data Inputs > Files & directories page or by editing the `inputs.conf` file directly.

If you want to collect thread info for all threads from Tomcat servers, you must complete the Splunk Add-on for Tomcat Input page to configure the dumpAllThreads input.

If you want to collect performance data from Tomcat servers you need to configure a JMX connection to the Tomcat server in the Splunk Add-on for JMX as described in Configure JMX inputs for the Splunk Add-on for Tomcat. You do not need to complete the Splunk Add-on for Tomcat setup page if this is the only data you want to collect.

Set up basic authentication using Splunk Web

Complete these steps to set up the Splunk Add-on for Tomcat using Splunk Web:

1. In Splunk Web, navigate the Splunk Add-on for Tomcat either by clicking the name of this add-on on the left navigation banner on through your Splunk platform Home page or by going to **Manage Apps**, then clicking **Launch App** in the row for the Splunk Add-on for Tomcat.
2. Go to the Tomcat **Account** tab.
3. Click **Add**.
4. In the **Add Account** dialog box, fill in the required fields:

Field	Description
Name	Add a unique name for Account.
Tomcat JMX URL	Enter the URL of your Tomcat instance in **service:jmx:rmi:///jndi/rmi://<ip-address>:<port>/jmxrmi** format.
Tomcat JMX username	Add server username.
Tomcat JMX password	Add server password.

   Note: JMX remote must be enabled on the Tomcat server in order to establish the JMX connection. See https://tomcat.apache.org/tomcat-10-doc/monitoring.html for information.

5. Click **Add**:
   - If the entered information is authenticated successfully, the add-on saves the account information.
   - If you have entered incorrect credentials or an incorrect url, an error message appears on the dialog box. If you see such message, verify the information you have entered and try again.

Configure file monitor inputs in inputs.conf

If you would like to collect only local Tomcat log files, you can edit `inputs.conf` directly to create the file monitor inputs instead of using the Settings > Data Inputs > Files & directories page.

Note: If you would also like to collect thread information, you must use the Configuration/Inputs page for the Splunk Add-on for Tomcat.

1. Create an `inputs.conf` file in `$SPLUNK_HOME/etc/apps/Splunk_TA_tomcat/local`.

2. Add the following stanzas. Modify the directory name as per the actual directory your Tomcat files are stored in.

```
[monitor:///Applications/apache-tomcat-10.0.12/logs/catalina.*.log]
disabled = false
followTail = false
index = main
sourcetype = tomcat:runtime:log

[monitor:///Applications/apache-tomcat-10.0.12/logs/localhost.*.log]
disabled = false
followTail = false
index = main
sourcetype = tomcat:runtime:log

[monitor:///Applications/apache-tomcat-10.0.12/logs/manager.*.log]
disabled = false
followTail = false
```

```
index = main
sourcetype = tomcat:runtime:log

[monitor:///Applications/apache-tomcat-10.0.12/logs/host-manager.*.log]
disabled = false
followTail = false
index = main
sourcetype = tomcat:runtime:log

[monitor:///Applications/apache-tomcat-10.0.12/logs/localhost_access_log.*.txt]
disabled = true
followTail = false
index = main
sourcetype = tomcat:access:log

[monitor:///Applications/apache-tomcat-10.0.12/logs/localhost_access_log_splunk.*.txt]
disabled = false
followTail = false
index = main
sourcetype = tomcat:access:log:splunk
```

To collect CIM-compatible data using the `tomcat:access:log:splunk` sourcetype, you must Configure the Splunk recommended fields in the Splunk add-on for Tomcat.

3. Save the file.

4. Restart the Splunk platform to put these configuration changes into effect.

Optional Splunk Web configurations

Configure logging level using Splunk Web

1. Go to the Splunk Add-on for Tomcat's landing page, either by clicking the name of this add-on on the left navigation banner on your on the Splunk software's home page or by going to **Manage Apps**, then clicking **Launch App** in the row for the Splunk Add-on for Tomcat.
2. Click the **Configuration** tab.
3. Go to the **Logging** tab.
4. (Optional) If you want to change the logging level, select a new level from the drop-down menu.
5. Click **Save** to save your configurations.

â â ==Set up the add-on using configuration files== **Prerequisites**

- Only users with file system access, such as system administrators, can set up the Splunk Add-on for Tomcat using configuration files.
- Review the steps in How to edit a configuration file in the Splunk Enterprise *Admin Manual*.

Never change or copy the configuration files in the default directory. The files in the default directory must remain intact and in their original location. Make changes to the files in the local directory.

Steps

Complete these steps to set up the Splunk Add-on for Tomcat using configuration files:

1. Navigate to `$SPLUNK_HOME/etc/apps/Splunk_TA_tomcat` and create a `/local` directory if it does not already exist.
2. Create a file called `splunk_ta_tomcat_account.conf` in the `$SPLUNK_HOME/etc/apps/Splunk_TA_tomcat/local` directory.
3. For each unique account name you want to keep, create a stanza. Make the stanza name same as the account name:

Stanza	Setting	Description
`[account_name]`	jmx_url	JMX URL to connect to the Tomcat server of the form service:jmx:rmi:///jndi/rmi://<ip-address>:<port>/jmxrmi
	username	Username of the Tomcat server
	password	Password of the Tomcat server

4. Review the values for the settings in the `$SPLUNK_HOME/etc/apps/Splunk_TA_tomcat/default/splunk_ta_tomcat_settings.conf` file. The values for the settings are listed in the following table. To use different values, create a file called `splunk_ta_tomcat_settings.conf` in the `$SPLUNK_HOME/etc/apps/Splunk_TA_tomcat/local` directory. Add only the stanzas and settings that you want to change to the file in the `local` directory.

Stanza	Setting	Description
[logging]	loglevel	Specifies the verbosity of the logs. Default is `INFO`. Log level can be `DEBUG`, `INFO` or `ERROR`.

5. Save your changes.
6. Restart your Splunk instance.

If you have multiple search heads that are not in a search head cluster, perform these preceding steps on each search head to support search-time push integration. Configure data collection only on your data collection nodes, typically one or more heavy forwarders.

Configure dumpAllThreads inputs for the Splunk Add-on for Tomcat

After you have set up the Splunk Add-on for Tomcat, validate that the correct inputs have been created. You need to update and enable the dumpAllThreads input to collect thread information from your Tomcat servers. You can enable the input either through Splunk Web or through the configuration files.

The file monitoring inputs for the local Tomcat logs are enabled by default, but it is a good idea to confirm that they have been created.

Configure Tomcat inputs via Splunk web

1. In the Splunk Add-on for Tomcat, click the **Inputs** tab.
2. Click **Create New Input**.
3. In the **Add Input** box, complete the following fields:

Field	Description
Name	Enter a unique name for the input.
Tomcat Account	Select your Tomcat account name configured under the Configurations page.
Collection Interval	The data collection interval, in seconds.
Index	The index that stores the collected data from this input. The default index is main.

4. Click Save.

Configure Tomcat inputs via inputs.conf

To configure inputs manually in `inputs.conf`, create stanzas using the following parameters and add them to `$SPLUNK_HOME/etc/apps/Splunk_TA_tomcat/local/inputs.conf`. If the file or path does not exist, create it.

```
[tomcat://<name>]
account = <string>
object_name = java.lang:type=Threading
operation_name = dumpAllThreads
signature = boolean, boolean
params = true, true
split_array = true
duration = <integer>
```

If you want to use the default inputs, the default value of the inputs can be found in `$SPLUNK_HOME/etc/apps/Splunk_TA_tomcat/default/inputs.conf`. You can copy the file to the local folder and edit it using the parameters table below.

Input Parameters

Each attribute in the following table corresponds to a field in Splunk Web:

Attribute	Corresponding field in Splunk Web	Description
`account`	Tomcat Account	Account from which data is to be collected.
`object_name`	ObjectName	The object name of the MBean on which the method is to be invoked. Supported is `java.lang:type=Threading`
`operation_name`	OperationName	The name of the operation to be invoked. Supported is `dumpAllThreads`
`signature`	Signature	Enter the java data types separated by comma. Supported is `boolean, boolean`
`params`	Parameters	Enter the values for the data types(entered in Signature) separated by comma. Supported is `true, true`
`split_array`	SplitArray	False] True to split up the whole data chunk into events and false if otherwise. Supported is `true`
`duration`	Collection Interval	Collection interval at which the data should be collected.
`index`	Index	The index in which to store Tomcat input data. The default is *default*.

Validate file monitoring inputs

Validate that file monitoring inputs have been successfully created.

1. Go to **Settings > Data inputs > Files & directories**.

2. Click **App** in the column headings to organize the results by app name, then scroll to **Splunk_TA_tomcat** in that column.

3. Review the list of files being monitored to ensure it is as you expect. They should be enabled by default.

Note: If you subsequently change the directory in which the log files are stored, generate new file monitoring inputs for the new location by using **Settings > Data inputs > Files & directories** page or update the local copy of inputs.conf file

Validate Data Collection

To verify the add-on has been installed successfully and that all expected data is being ingested into the Splunk platform, run the following searches depending on which inputs you have configured.

Performance data and thread information:

```
sourcetype=tomcat:jmx
```

catalina*.log, localhost*.log, manager*.log, and host-manager*.log:

```
sourcetype=tomcat:runtime:log
```

locahost_access_log*.txt:

```
sourcetype=tomcat:access:log
```

locahost_access_log_splunk*.txt:

```
sourcetype=tomcat:access:log:splunk
```

Enable saved searches for the Splunk Add-on for Tomcat

The Splunk Add-on for Tomcat includes two preconfigured lookup generation saved searches that you need to enable if you are using this add-on with Splunk IT Service Intelligence. These saved searches are based on the data collected through JMX and file based logs. You need to configure JMX inputs and set up the Splunk Add-on for Tomcat in order to collect the data. After the data has been indexed by the Splunk platform, you can manually run the saved searches in order to populate the lookup files then set a frequency to run them that matches the frequency of configuration changes in your environment.

Saved search name	Description
Tomcat application server	Saved search which populates the `application_server` and `appserver_port_number` fields using the `tomcat_application_server_lookup` KV store lookup.
Tomcat version number	Saved search which populates the `version_number` field using the `tomcat_version_number_lookup` KV store lookup.

You can review and enable these saved searches either in Splunk Web or in the configuration files.

Access and enable saved searches in Splunk Web

To access and enable the saved searches in Splunk Web:

1. Go to **Settings > Searches, reports, and alerts**.

2. Set the app context to **Splunk Add-on for Tomcat**.

3. Click **Enable** next to the searches you would like to enable.

Access and enable saved searches in `savedsearches.conf`

To access and enable the saved searches in the configuration files:

1. Go to `$SPLUNK_HOME/etc/apps/Splunk_TA_tomcat/default/savedsearches.conf`.

2. Copy the file to `/local`.

3. In the local copy, for each search that you want to enable, change `Disabled = 1` to `Disabled = 0`.

Migrating from CSV lookups to KV store lookups

1. Disable the savedsearch Tomcat version number and Tomcat application server from Splunk Web on the search head.
2. Execute the below two SPL queries to migrate existing CSV lookup data to KVStore from your search heads:
    1. `| inputlookup tomcat_application_server_lookup.csv | outputlookup tomcat_application_server_lookup`
    2. `| inputlookup tomcat_version_number_lookup.csv | outputlookup tomcat_version_number_lookup`
3. Enable the savedsearch Tomcat version number and Tomcat application server from Splunk Web on the search head.

Troubleshoot the Splunk Add-on for Tomcat

General troubleshooting

For helpful troubleshooting tips that you can apply to all add-ons, see Troubleshoot add-ons in *Splunk Add-ons*. For additional resources, see Support and resource links for add-ons in *Splunk Add-ons*.

Splunk Add-on for Tomcat logs

This add-on has 3 logs that are located at `$SPLUNK_HOME/var/log/splunk`:

- `splunk_ta_tomcat_main.log`
- `splunk_ta_tomcat_setup.log`
- `splunk_ta_tomcat_util.log`

To check for errors in the internal logs for this add-on, you can perform this search:

```
index=_internal source=*ta_tomcat*
```

You can configure the logging verbosity on the setup page for the add-on. Supported log levels are INFO, DEBUG, and ERROR.

To check for JMX errors, you can perform this search of the JMX internal logs:

```
index=_internal sourcetype=jmx
```

Getting errors when Splunk add-on for Tomcat is installed on Splunk Universal Forwarder

While installing Splunk add-on for Tomcat on Universal forwarder, if you get the below error:

```
08-15-2021 10:41:53.124 +0900 ERROR ModularInputs - Introspecting scheme=tomcat: Unable to run
"/opt/splunkforwarder/bin/python3.7 /opt/splunkforwarder/etc/apps/Splunk_TA_tomcat/bin/tomcat.py --scheme":
child failed to start: No such file or directory
08-15-2021 10:41:53.124 +0900 ERROR ModularInputs - Unable to initialize modular input "tomcat" defined in
the app "Splunk_TA_tomcat": Introspecting scheme=tomcat: Unable to run "/opt/splunkforwarder/bin/python3.7
/opt/splunkforwarder/etc/apps/Splunk_TA_tomcat/bin/tomcat.py --scheme": child failed to start: No such file
or directory.
```

You can ignore this error as the Splunk add-on for Tomcat's modular input requires a heavy forwarder which ships Python in it. As Python isn't provided with Splunk Universal Forwarder, you would get this error if a Python executable is not found on your Splunk universal forwarder machine.

Upgrade the Splunk Add-on for Tomcat

To upgrade Splunk Add-on for Tomcat from v2.1.0 to v3.0.0:

1. In Splunk Web, navigate to **Settings > Data Inputs** and click on **Splunk Add-on for Tomcat**
2. Disable the inputs configured in your existing version of the Splunk Add-on for Tomcat.
3. Upgrade the add-on to version v3.0.0 either by clicking the **Upgrade** button, or by following the installation steps in the *Install* topic of this manual.
4. In Splunk Web, navigate to the Splunk Add-on for Tomcat.
5. On the Splunk Add-on for Tomcat configuration page, navigate to the **Account** tab, by clicking **Configuration > Account**. Configure your Tomcat account, see the Set up the Splunk Add-on for Tomcat topic in this manual for more information.
6. Navigate to the **Inputs** page, by clicking **Inputs** tab
7. Add the account you have configured by editing the **dumpAllThreads** input
8. Enable the reconfigued **dumpAllThreads** input
9. (Optional) If you are using the savedsearches of Tomcat, refer the *Migrating from CSV lookups to KV store lookups* under Enable saved searches for the Splunk Add-on for Tomcat section for detailed steps.

Before upgrading the Splunk add-on for Tomcat to version 2.1.0 from version 2.0.1 or below, follow these steps: If you want to use the `tomcat:access:log:splunk` sourcetype to collect CIM-compatible data, follow these steps to Configure Splunk recommended fields in Splunk add-on for Tomcat instead.

> Splunk Cloud Platform deployments on Victoria Experience do not require Inputs Data Manager (IDM). If your deployment is on Victoria Experience you can run add-ons that contain scripted and modular inputs directly on the search head. To determine if your deployment has the Classic or Victoria experience, see Determine your Splunk Cloud Platform Experience.

For the Classic Experience:

1. Disable the "dumpAllThreads" input if enabled, on your Heavy Forwarder (HF) or Inputs Data Manager (IDM) from the user interface.
2. Upgrade the Splunk add-on for Tomcat to the version 2.1.0.
3. Restart your Splunk instance.

4. Enable the "dumpAllThreads" input.

Configure Splunk recommended fields in Splunk add-on for Tomcat

Splunk best practice is to utilize the `tomcat:access:splunk:log` source type in order for logs to be CIM-compliant.

In order to utilize this source type, you must follow these steps to disable Tomcat add-on inputs.

- File monitor input for the `tomcat:access:log` sourcetype: Settings > Data Inputs > Files & directories > input for `tomcat:access:log` sourcetype > Disable
- dumpAllThreads: Settings > Data Inputs > Splunk Add-on for Tomcat > dumpAllThreads > Disable

1. Open the back-end access to your tomcat server.
2. Stop the tomcat server.
3. Navigate to $CATALINA_HOME/conf/ and open the `server.xml` in a text editor.
4. Search for the line `org.apache.catalina.valves.AccessLogValve` in the file.
5. Update the `prefix` and `pattern` keys as below:

```
prefix="localhost_access_log_splunk" suffix=".txt"


pattern="%t, x_forwarded_for=&quot;%{X-Forwarded-For}i&quot;, remote_ip=&quot;%a&quot;,
remote_host=&quot;%h&quot;, server=&quot;%v&quot;, server_port=%p, user=&quot;%u&quot;,
http_method=%m, uri_path=&quot;%U&quot;, uri_query=&quot;%q&quot;, status=%s,  bytes_sent=%b,
response_time=%F, http_content_type=&quot;%{Content-Type}o&quot;,
http_user_agent=&quot;%{User-Agent}i&quot;, http_referrer=&quot;%{Referer}i&quot;,
url=&quot;%{Host}i%U%q&quot;"
```

6. Save the `server.xml` file.
7. Start the tomcat server.
8. Reconfigure the add-on and check the checkbox for "Enable data collection from Tomcat log files".
9. Enable the dumpAllThread input.

Optionally, you can configure the Tomcat server to authenticate the User, since the tomcat:access:log:splunk source type supports user field mapping. You can follow the steps mentioned in the documentation for Tomcat.

Reference

Lookups for the Splunk Add-on for Tomcat

The Splunk Add-on for Tomcat has four **lookups**. The lookup files map fields from Tomcat systems to CIM-compliant values in the Splunk platform. The lookup files are located in `$SPLUNK_HOME/etc/apps/Splunk_TA_tomcat/lookups`.

Filename	Description
`tomcat_severity.csv`	Maps the `log_level` field to a CIM-compliant value for the `severity` field.
`tomcat_http_status.csv`	Maps the `status` field to CIM-compliant value for the `action` field.
`tomcat_version_number_lookup`	This KV store lookup is populated with the `version_number` field in all events. Generated from the "Tomcat version number" saved search.
`tomcat_application_server_lookup`	This KV store lookup is populated with the `application_server` and `appserver_port_number` fields in all events. Generated from the "Tomcat application server" saved search.
`tomcat_thread_states.csv`	Maps the `threadState` field to `thread_state` defined by the ITSI AppServer data model.

Source types for the Splunk Add-on for Tomcat

The Splunk Add-on for Tomcat supports the following data sources. All access logs that need to be CIM-Compliant should use the `tomcat:access:log:splunk` sourcetype.

Data source	Collection method	source type	CIM data models	ITSI data models
Thread information from JMX MBean operations	Modular input (dumpAllThreads)	`tomcat:jmx`	JVM, Performance	Application Server data model objects: Inventory, Performance
Performance metrics from JMX MBean attributes	Splunk Add-on for JMX			
Catalina*.log, localhost*.log, manager*.log, host-manager*.log	File monitoring	`tomcat:runtime:log`	N/A	Application Server data model object: Inventory
localhost_access_log_splunk*.txt	File monitoring	`tomcat:access:log:splunk`	Web	localhost_access_log*.t
localhost_access_log*.txt	File monitoring	`tomcat:access:log`	N/A	Application Server data model objects: Inventory, Performance

You can view the recommended fields section to collect data using the `tomcat:access:log:splunk` sourcetype.

Release notes

Release notes for the Splunk Add-on for Tomcat

About this release

Version 3.1.1 of the Splunk Add-on for Tomcat was released on Sept 20, 2022.

Compatibility

Version 3.1.1 of the Splunk Add-on for Tomcat is compatible with the following software, CIM versions, and platforms.

Splunk software versions	8.1.x, 8.2.x, 9.0.x
CIM	5.0.1
Platforms	Windows and Linux
Vendor Products	Apache Tomcat 8.0, 8.5.61, 9.0.41, 10.0.12, and 10.0.23

The field alias functionality is compatible with the current version of this add-on. The current version of this add-on does not support older field alias configurations.

For more information about the field alias configuration change, refer to the Splunk Enterprise Release Notes.

New features

- Support for Tomcat server version 10.0.23
- CIM compatibility with version 5.0.1
- Fixed multiple security vulnerabilities found in the fastjson, commons-configuration2 and log4j libraries:
    - Upgraded the fastjsonlog4j library from version 1.2.78 to 1.2.83
    - Upgraded the log4j library from version 2.16.0 to 2.18.0
    - Upgraded the commons-configuration2 library from version 2.7 to 2.8.0

Fixed issues

Version 3.1.1 of the Splunk Add-on for Tomcat has the following fixed issues.

Known issues

Version 3.1.1 of the Splunk Add-on for Tomcat has the following known issues.

Third-party software attributions

Some of the components included in this add-on are licensed under free or open source licenses. We wish to thank the contributors to those projects.

A complete listing of third-party software information for this add-on is available as a text edit file for download: Splunk Add-on for Tomcat third-party software credits.

Release history for the Splunk Add-on for Tomcat

Latest release

The most recent versions of the Splunk Add-on for Tomcat is version 3.1.1. See Release notes for the Splunk Add-on for Tomcat for the release notes of this latest version.

Version 3.0.2

The log4j library used in the Splunk Add-on for Tomcat was updated to version 2.16 in December 2021. Since then log4j has released version 2.17.1 which addresses additional vulnerabilities. These vulnerabilities are rated as moderate severity and the add-on does not use the affected code path. However, this add-on will be updated to the recommended version of 2.17.1 in an upcoming release.

Version 3.0.2 of the Splunk Add-on for Tomcat was released on Dec 17, 2022.

Compatibility

Version 3.0.2 of the Splunk Add-on for Tomcat is compatible with the following software, CIM versions, and platforms.

Splunk software versions	8/0x, 8.1.x, 8.2.x
CIM	4.20
Platforms	Windows and Linux
Vendor Products	Apache Tomcat 8.0, 8.5.61, 9.0.41, and 10.0.12

The field alias functionality is compatible with the current version of this add-on. The current version of this add-on does not support older field alias configurations.

For more information about the field alias configuration change, refer to the Splunk Enterprise Release Notes.

New features

- Upgraded the fastjson library from version 1.2.78 to 1.2.83.
- Upgraded the log4j library from version 2.16.0 to 2.18.0.
- Fixed a security vulnerability found in the fastjson and log4j library.

Fixed issues

Version 3.0.2 of the Splunk Add-on for Tomcat has the following fixed issues.

Known issues

Version 3.0.2 of the Splunk Add-on for Tomcat has the following known issues.

Third-party software attributions

Some of the components included in this add-on are licensed under free or open source licenses. We wish to thank the contributors to those projects.

A complete listing of third-party software information for this add-on is available as a text edit file for download:
Splunk Add-on for Tomcat third-party software credits.

Version 3.0.2

About this release

The log4j library used in the Splunk Add-on for Tomcat was updated to version 2.16 in December 2021. Since then log4j has released version 2.17.1 which addresses additional vulnerabilities. These vulnerabilities are rated as moderate severity and the add-on does not use the affected code path. However, this add-on will be updated to the recommended version of 2.17.1 in an upcoming release.

Version 3.0.2 of the Splunk Add-on for Tomcat was released on December 17, 2021.

Compatibility

Version 3.0.2 of the Splunk Add-on for Tomcat is compatible with the following software, CIM versions, and platforms.

Splunk software versions	8.0.x, 8.1.x, 8.2.x
CIM	4.20
Platforms	Windows and Linux
Vendor Products	Apache Tomcat 8.0, 8.5.61, 9.0.41, and 10.0.12

The field alias functionality is compatible with the current version of this add-on. The current version of this add-on does not support older field alias configurations.

For more information about the field alias configuration change, refer to the Splunk Enterprise Release Notes.

New features

- Upgraded the log4j library from version 2.15.0 to 2.16.0.
- Fixed a security vulnerability found in the log4j library

Version 3.0.2

Version 3.0.2 fixed a security vulnerability found in the log4j library.

Fixed issues

Version 3.0.2 of the Splunk Add-on for Tomcat has the following fixed issues.

Known issues

Version 3.0.2 of the Splunk Add-on for Tomcat has the following known issues.

Third-party software attributions

Some of the components included in this add-on are licensed under free or open source licenses. We wish to thank the contributors to those projects.

A complete listing of third-party software information for this add-on is available as a PDF file for download:
Splunk Add-on for Tomcat third-party software credits.

Version 3.0.1

About this release

Version 3.0.1 of the Splunk Add-on for Tomcat was released on December 14, 2021.

Compatibility

Version 3.0.1 of the Splunk Add-on for Tomcat is compatible with the following software, CIM versions, and platforms.

Splunk software versions	8.0.x, 8.1.x, 8.2.x
CIM	4.20.0
Platforms	Windows and Linux
Vendor Products	Apache Tomcat 8.0, 8.5.61, 9.0.41, and 10.0.12

The field alias functionality is compatible with the current version of this add-on. The current version of this add-on does not support older field alias configurations.

For more information about the field alias configuration change, refer to the Splunk Enterprise Release Notes.

New features

This release supports versions 3.0.1 of the Splunk Add-on for Tomcat.

Version 3.0.1

Version 3.0.1 fixed a security vulnerability found in the log4j library.

Fixed issues

Version 3.0.1 of the Splunk Add-on for Tomcat has the following fixed issues.

Known issues

Version 3.0.1 of the Splunk Add-on for Tomcat has the following known issues.

Third-party software attributions

Some of the components included in this add-on are licensed under free or open source licenses. We wish to thank the contributors to those projects.

A complete listing of third-party software information for this add-on is available as a PDF file for download:
Splunk Add-on for Tomcat third-party software credits.

Version 3.0.0

About this release

Version 3.0.0 of the Splunk Add-on for Tomcat was released on October 28, 2021.

Compatibility

Version 3.0.0 of the Splunk Add-on for Tomcat is compatible with the following software, CIM versions, and platforms.

Splunk software versions	8.0.x, 8.1.x, 8.2.x
CIM	4.20.0
Platforms	Windows and Linux
Vendor Products	Apache Tomcat 8.0, 8.5.61, 9.0.41, and 10.0.12

The field alias functionality is compatible with the current version of this add-on. The current version of this add-on does not support older field alias configurations.

For more information about the field alias configuration change, refer to the Splunk Enterprise Release Notes.

New features

Version 3.0.0 of the Splunk Add-on for Tomcat has the following new features.

- Migrated the TA from setup page to a fast and intuitive UI with an improved look and feel.
- Support of the Tomcat server version 10.0.12.

- Support of multiple accounts and multiple inputs.
- Removed python2 support. Splunk only supports python3 for future releases.
- Provided server validation while configuring the account on the configuration page.
- Compatibility with CIM version 4.20.

Field changes

The following sections contain information on fields and data models that have been added, modified, or removed in this release.

Fields added and removed

No fields have been added or removed between Tomcat v2.1.0 and Tomcat v3.0.0.

Fields modified

Sourcetype	CIM Field	Operation	Vendor Field Before	Vendor field after	Sample value before	Sample valu
`tomcat:access:log:splunk`	category	<add>	category	category	78	image/gif
`tomcat:access:log:splunk`	url_domain	<add>	url_domain	url_domain	ec2.splunkit.io	i-test-instance.ec2.
`tomcat:access:log:splunk`	http_referrer_domain	<add>	http_referrer_domain	http_referrer_domain	ec2.splunkit.io	i-test-instance.ec2.

CIM changes

There is no CIM addition, modification, or removal between Tomcat v2.1.0 and Tomcat v3.0.0.

Fixed issues

Version 3.0.0 of the Splunk Add-on for Tomcat has the following fixed issues.

Known issues

Version 3.0.0 of the Splunk Add-on for Tomcat has the following known issues.

Date filed	Issue number	Description
2021-10-04	ADDON-42989, ADDON-21304	Getting "Config file: splunk_ta_tomcat_account does not exist." error in splunk_ta_tomcat_main.log on add-on installation Workaround: This error message can be ignored safely and once the account is configured, this error message will no longer be logged.

Third-party software attributions

Some of the components included in this add-on are licensed under free or open source licenses. We wish to thank the contributors to those projects.

A complete listing of third-party software information for this add-on is available as a PDF file for download:
Splunk Add-on for Tomcat third-party software credits.

Version 2.1.0

Version 2.1.0 of the Splunk Add-on for Tomcat was released on February 4, 2021. Version 2.1.0 of the Splunk Add-on for Tomcat is compatible with the following software, CIM versions, and platforms.

Splunk software versions	7.2.x, 7.3.x, 8.0.x, 8.1.x
CIM	4.18
Platforms	Windows and Linux
Vendor Products	Apache Tomcat 8.0, 8.5.61 and 9.0.41

The field alias functionality is compatible with the current version of this add-on. The current version of this add-on does not support older field alias configurations.

For more information about the field alias configuration change, refer to the Splunk Enterprise Release Notes.

New features

Version 2.1.0 of the Splunk Add-on for Tomcat has the following new features.

- Support for Apache Tomcat server latest version 9.0.41.
- Added the new `tomcat:access:log:splunk` sourcetype to fully comply with the Web CIM model. Provided guidance on configuring Tomcat logging for this new sourcetype.
- Compatibility with the OpenJDK 11 and OracleJDK 11.
- Compatibility with the Common Information Model (CIM) version 4.18.
- Enhanced UX through instant validations for the fields that are required on the setup page.

Fixed issues

Version 2.1.0 of the Splunk Add-on for Tomcat has the following fixed issues.

Date resolved	Issue number	Description
2021-01-06	ADDON-23979	Field version_number_tmp is not getting extracted for Tomcat version 9

Known issues

Version 2.1.0 of the Splunk Add-on for Tomcat has the following known issues.

Date filed	Issue number	Description
2019-02-04	ADDON-21204	tomcat_server.conf not correctly updating to reflect changes made on setup page in UI
2019-01-28	ADDON-21046	Setup page UI issue in Tomcat add-on 1.1.0
2016-03-17	ADDON-8342	Consistency required for field host on data from log files and in jmx url.
2015-09-07	ADDON-5383	Fails to generate eventgen data on Windows platform

Date filed	Issue number	Description
2015-09-03	ADDON-5325	Support requireClientCert = true in server.conf.

Third-party software attributions

Version 2.1.0 of the Splunk Add-on for Tomcat incorporates the following third-party software or libraries.

- slf4j
- Apache Commons Logging
- Apache log4j
- fastjson
- Apache Commons Configuration
- Apache Commons Collections
- Apache Commons Pool
- Apache Commons IO
- guava
- Httplib2
- future

Version 2.0.1

Version 2.0.1 of the Splunk Add-on for Tomcat was released on March 1, 2019. Version 2.0.1 of the Splunk Add-on for Tomcat is compatible with the following software, CIM versions, and platforms.

Splunk software versions	7.0.x, 7.1.x, 7.2.x, 8.0.x
CIM	4.13 or later
Platforms	Windows and Linux
Vendor Products	Apache Tomcat 8.x or later

New features

Version 2.0.1 of the Splunk Add-on for Tomcat has the following new features.

- Default support for Python 3

Fixed issues

Version 2.0.1 of the Splunk Add-on for Tomcat has no fixed issues.

Known issues

Version 2.0.1 of the Splunk Add-on for Tomcat has the following known issues.

Date filed	Issue number	Description
2019-10-18	ADDON-23979	Field version_number_tmp is not getting extracted for Tomcat version 9
2019-02-04	ADDON-21204	tomcat_server.conf not correctly updating to reflect changes made on setup page in UI

Date filed	Issue number	Description
2019-01-28	ADDON-21046	Setup page UI issue in Tomcat add-on 1.1.0
2019-01-22	ADDON-21010	Not passing validation checks in Splunk Cloud 7.0.x for GUI install
2016-03-17	ADDON-8342	Consistency required for field host on data from log files and in jmx url.
2015-09-07	ADDON-5383	Fails to generate eventgen data on Windows platform
2015-09-03	ADDON-5325	Support requireClientCert = true in server.conf.

Third-party software attributions

Version 2.0.1 of the Splunk Add-on for Tomcat incorporates the following third-party software or libraries.

Version 2.0.0

Version 2.0.0 of the Splunk Add-on for Tomcat was released on October 21, 2019. Version 2.0.0 of the Splunk Add-on for Tomcat is compatible with the following software, CIM versions, and platforms.

Splunk software versions	7.0.x, 7.1.x, 7.2.x, 8.0.x
CIM	4.13 or later
Platforms	Windows and Linux
Vendor Products	Apache Tomcat 8.x or later

New features

Version 2.0.0 of the Splunk Add-on for Tomcat has the following new features.

- Support for Python 3

Fixed issues

Version 2.0.0 of the Splunk Add-on for Tomcat has no fixed issues.

Known issues

Version 2.0.0 of the Splunk Add-on for Tomcat has the following known issues.

Date filed	Issue number	Description
2019-10-18	ADDON-23979	Field version_number_tmp is not getting extracted for Tomcat version 9
2019-02-04	ADDON-21204	tomcat_server.conf not correctly updating to reflect changes made on setup page in UI
2019-01-28	ADDON-21046	Setup page UI issue in Tomcat add-on 1.1.0

Date filed	Issue number	Description
2019-01-22	ADDON-21010	Not passing validation checks in Splunk Cloud 7.0.x for GUI install
2016-03-17	ADDON-8342	Consistency required for field host on data from log files and in jmx url.
2015-09-07	ADDON-5383	Fails to generate eventgen data on Windows platform
2015-09-03	ADDON-5325	Support requireClientCert = true in server.conf.

Third-party software attributions

Version 2.0.0 of the Splunk Add-on for Tomcat incorporates the following third-party software or libraries.

- slf4j
- Apache Commons Logging
- Apache log4j
- fastjson
- Apache Commons Configuration
- Apache Commons Collections
- Apache Commons Pool
- Apache Commons IO
- guava
- Httplib2
- future

Version 1.1.0

About this release

Version 1.1.0 of the Splunk Add-on for Tomcat was released on April 1, 2016. Version 1.1.0 of the Splunk Add-on for Tomcat is compatible with the following software, CIM versions, and platforms.

Splunk software versions	6.5.x, 6.6.x, 7.0.x, 7.1.x, 7.2.x
CIM	4.2 or later
Platforms	Windows and Linux
Vendor Products	Apache Tomcat 8.x or later

New features

Version 1.1.0 of the Splunk Add-on for Tomcat has the following new features.

Date	Issue number	Description
2015-10-19	ADDON-6103	ITSI AppServer module integration: modify the Splunk Add-on for Tomcat to collect the necessary data for populating the inventory and recommended KPIs for ITSI AppServer module.
2016-03-16	ADDON-8322	Add the following new JMX templates to support mapping to the AppServer ITSI module: tomcat_connector, tomcat_global_request_processor, tomcat_webapp_class_loader, tomcat_manager.

Date	Issue number	Description
2016-03-16	ADDON-8321	Add theTomcat version number and Tomcat application server saved searches.
2016-02-18	ADDON-7832	Add extraction and mapping for two additional fields: `thread_id` and `thread_state`.

Fixed issues

Version 1.1.0 of the Splunk Add-on for Tomcat has no fixed issues.

Known issues

Version 1.1.0 of the Splunk Add-on for Tomcat has the following known issues.

Date filed	Issue number	Description
2016-03-17	ADDON-8342	When configuring a JMX input using the "Use URL directly" method, the admin needs to use a hostname rather than an IP address so that the host field will be consistent.
2016-01-30	ADDON-7646	FIPS mode is not supported by this add-on. For a workaround, see Add-ons and FIPS mode in the *Splunk Add-ons* manual.
2016-01-13	ADDON-5325	`requireClientCert=true` in `server.conf` is not supported by add-ons using modular inputs and REST. If this setting is enabled in `server.conf`, communication is broken between the modular input and splunkd and the add-on stops collecting data. The following error appears in the `splunkd.log`: "SSL3_GET_CLIENT_CERTIFICATE:peer did not return a certificate." The workaround is to set `requireClientCert=false`.
2015-09-09	ADDON-5437	If the Splunk Add-on for ServiceNow or the Splunk Add-on for Box is installed and data inputs have been configured in one of these add-ons, then the inputs are disabled, the Splunk Add-on for JMX is unable to get data from a configured Tomcat server. This affects Splunk Add-on for JMX 3.0.2 or older.
2015-09-07	ADDON-5383 /APPSC-432	Fails to generate eventgen data on Windows platform.

Third-party software attributions

Version 1.1.0 of the Splunk Add-on for Tomcat incorporates the following third-party software or libraries.

- slf4j
- Apache Commons Logging
- Apache log4j
- fastjson
- Apache Commons Configuration
- Apache Commons Collections
- Apache Commons Pool
- Apache Commons IO
- guava

Version 1.0.0

Version 1.0.0 of the Splunk Add-on for Tomcat has the same compatibility specifications as version 1.1.0.

New features

Version 1.0.0 of the Splunk Add-on for Tomcat had the following new feature.

Date	Issue number	Description
2015-09-10	ADDON-4795	Create a new add-on for Apache Tomcat java server.

Known issues

Version 1.0.0 of the Splunk Add-on for Tomcat had the following known issues.

Date filed	Defect number	Description
2016-01-30	ADDON-7646	FIPS mode is not supported by this add-on. For a workaround, see Add-ons and FIPS mode in the *Splunk Add-ons* manual.
2016-01-13	ADDON-5325	`requireClientCert=true` in `server.conf` is not supported by add-ons using modular inputs and REST. If this setting is enabled in `server.conf`, communication is broken between the modular input and splunkd and the add-on stops collecting data. The following error appears in the `splunkd.log`: "SSL3_GET_CLIENT_CERTIFICATE:peer did not return a certificate." The workaround is to set `requireClientCert=false`.
2015-09-09	ADDON-5437	If the Splunk Add-on for ServiceNow or the Splunk Add-on for Box is installed and data inputs have been configured in one of these add-ons, then the inputs are disabled, the Splunk Add-on for JMX is unable to get data from a configured Tomcat server. This affects Splunk Add-on for JMX 3.0.2 or older.

Third-party software attributions

Version 1.0.0 of the Splunk Add-on for Tomcat incorporated the following third-party software or libraries.

- slf4j
- Apache Commons Logging
- Apache log4j
- fastjson
- Apache Commons Configuration
- Apache Commons Collections
- Apache Commons Pool
- Apache Commons IO
- guava