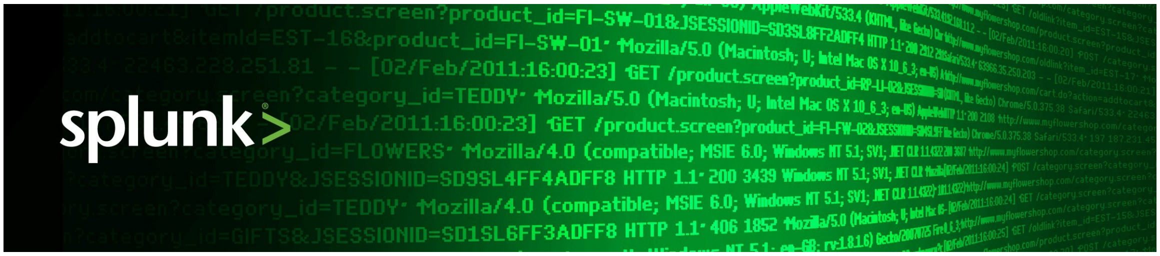

Splunk® Supported Add-ons Splunk Add-on for Unix and Linux released

Generated: 10/29/2018 10:56 am

Table of Contents

Overview

Splunk Add-on for Unix and Linux

Version	6.0.1
Vendor products	All supported Unix operating systems. See Unix operating systems.
Add-on has web UI	Yes. This add-on contains views for configuration.

The Splunk Add-on for Unix and Linux allows a Splunk software administrator to collect *nix data from *nix hosts. You can install the Splunk Add-on for Unix and Linux on a **forwarder** to send data from any number of *nix hosts to a Splunk Enterprise indexer or group of indexers. You can also use the add-on to provide data for other apps, such as Splunk IT Service Intelligence (ITSI) or Splunk Enterprise Security.

The Splunk Add-on for Unix and Linux collects the following data using file inputs:

- Changes to files in the `/etc` directory and subdirectories.
- Changes to files in the `/var/log` directory and subdirectories.

The add-on collects data with the following scripted inputs:

input	description
`bandwidth.sh`	Network statistics via the shell commands `dlstat`, `netstat`, and `sar`
`cpu.sh`	CPU statistics via the shell commands `sar`, `mpstat`, and `iostat`
`df.sh`	Free disk space for each mount point via the shell commands `df`, `mount`, and `fstyp`
`hardware.sh`	Hardware information via the shell commands `cpuinfo`, `df`, `dmesg`, `ifconfig`, `ioscan`, `iostat`, `ip`, `lanscan`, `lsattr`, `lscfg`, `lsdev`, `lsps`, `lspv`, `meminfo`, `mpstat`, `prtconf`, `prtdiag`, `sysctl`, `system_profiler`, `swap`, `swapinfo`, and `top`
`interfaces.sh`	

	Configured network interfaces via the shell commands dmesg, ethtool, ifconfig, kstat, lanscan, lanadmin, and netstat
iostat.sh	Input/output statistics for block devices and partitions via the shell commands darwin_disk_stats, iostat, and sar
lastlog.sh	Last login times for system accounts via the shell commands last, lastb, and lastlogin
lsof.sh	Process information via the shell command lsof
netstat.sh	Network connections, routing tables, and network interface information via the shell command netstat
openPorts.sh	Available network ports via the shell command netstat
openPortsEnhanced.sh	TCP/UDP ports in a listening state, and information on process, process ID, IP version, and so on. via the shell commands lsof, and netstat
package.sh	Lists installed software packages via the shell commands dpkg-query, pkginfo, pkg_info, system_profiler, and swlist
passwd.sh	Shows username and associated user ID, user group ID, and shell
protocol.sh	TCP/UDP transfer statistics via the shell command netstat
ps.sh	Status of current running processes via the shell command ps
rlog.sh	Audit information recorded in /var/log/audit/audit.log by auditd
selinuxChecker.sh	Parses /etc/sysconfig/selinux to check if SELinux is configured
service.sh	Running services and associated details via the shell commands chkconfig, dscl, svcs, and systemctl
sshdChecker.sh	Parses sshd_config for information local sshd configurations
time.sh	System date and time, and NTP server time via the shell commands date and ntpdate
top.sh	

	List of running system processes via the shell commands `ps` and `top`
`update.sh`	Available software updates for installed packages via the shell commands `softwareupdate` and `yum`
`uptime.sh`	System date and uptime information via the shell command `date`
`usersWithLoginPrivs.sh`	Shows system username information
`version.sh`	OS version details via the shell command `uname`
`vmstat.sh`	Process-related memory usage information via the shell commands `prstat`, `prtconf`, `ps`, `sar`, `svmon`, `swap`, `swapinfo`, `sysctl`, `top`, `uptime`, and `vmstat`
`vsftpdChecker.sh`	Parses `vsftpd.conf` for information about local VSFTP server configurations in `/etc`, `/etc/vsftpd`, or `/private/etc`
`who.sh`	Information about all users currently logged in via the shell command `who`

The add-on displays question marks ("?") for blank fields that the scripted inputs return within individual events. This is expected behavior to preserve field spacing.

Download the Splunk Add-on for Unix and Linux from Splunkbase.

For a summary of new features, fixed issues, and known issues, see Release notes for the Splunk Add-on for Unix and Linux.

For information about installing and configuring the Splunk Add-on for Unix and Linux, see Installation and configuration overview for the Splunk Add-on for Unix and Linux.

See Questions related to Splunk Add-on for Unix and Linux on Splunk Answers.

Source types for the Splunk Add-on for Unix and Linux

The Splunk Add-on for Unix and Linux provides the index-time and search-time knowledge for *nix events, metadata, user and group information, collaboration data, and tasks in the following formats:

Source type	Description	CIM data models
`aix_secure`	The AIX security log file	Performance
`bandwidth`	Network statistics	Performance
`bash_history`	A list of commands previously used in a bash shell	n/a
`config_file`	Configuration file information	n/a
`cpu`	CPU state information	Performance
`df`	Available disk space on mounted volumes	Performance
`dhcpd`	Dynamic Host Control Protocol (DHCP) daemon information	Network Sessions
`fs_notification`	File system notification changes	Change Analysis
`hardware`	Hardware specifications	Inventory
`interfaces`	Network interface information	n/a
`iostat`	Input/Output operation information	Performance
`lastlog`	Last login times for system accounts	n/a
`Linux:SELinuxConfig`	SELinux host configuration information	n/a
`linux_secure`	The Linux security log file	Change Analysis, Performance
`lsof`	A list of the open files on a host	n/a
`netstat`	The state of the network (open/listening ports, connections, and so on) on a host	n/a
`openPorts`	A list of the open ports on a host	Application State
`osx_secure`	The security log file for Mac OS X	Change Analysis, Performance
`package`	A list of installed packages	n/a
`protocol`	Network protocol stack information	n/a

ps	Process information	Application State
time	Time service information	n/a
top	Process and system resource information	Application State
Unix:CPUTime	Statistics about the amount of time the CPU dedicated to specific processes	Performance
Unix:ListeningPorts	Network ports that the OS is listening on	Application State
Unix:Service	Unix service information	Application State
Unix:SSHDConfig	Local sshd configuration information	n/a
Unix:Update	A list of software updates for installed packages	n/a
Unix:Uptime	System date and uptime information	Performance
Unix:UserAccounts	User account information	Inventory
Unix:Version	OS version information	Inventory
Unix:VSFTPDConfig	Local VSFTP server configuration information	n/a
usersWithLoginPrivs	Users with elevated login privileges	n/a
vmstat	Virtual memory information	Performance
who	All users currently logged in	n/a

Release notes for the Splunk Add-on for Unix and Linux

Version 6.0.1 of the Splunk Add-on for Unix and Linux was released on September 20, 2018.

The Splunk Add-on for Unix and Linux 6.0.0 introduced breaking changes. If you are upgrading from an earlier version of the Splunk Add-on for Unix and Linux, you must follow the steps outlined in Upgrade the Splunk Add-on for Unix and Linux. Failure to do so can result in data loss.

Compatibility

Version 6.0.1 of the Splunk Add-on for Unix and Linux is compatible with the following software, CIM versions, and platforms:

Splunk platform versions	6.6.x, 7.0.x, 7.1.x, 7.2.x
CIM	4.11
Supported OS for data collection	All supported Unix operating systems. See Unix operating systems.
Vendor products	All supported Unix operating systems. See Unix operating systems.

Script compatibility

Script	CentOS		RHEL		Ubuntu		Solaris			AIX		FreeBS	
	6	7	7.4	6.9	14.04	16.04	10	11.3	11.0	7.1	7.2	9	10
`bandwidth.sh`	Y	Y	Y	Y	Y	Y	Y[1]	Y[2]	Y	Y	Y	N[3]	N[3]
`common.sh`	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
`cpu.sh`	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
`df.sh`	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
`hardware.sh`	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
`interfaces.sh`	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
`iostat.sh`	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
`lastlog.sh`	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	Y	Y
`lsof.sh`	Y	Y	Y	Y	Y	Y	N	N	N	N	N	N	N
`netstat.sh`	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
`openPorts.sh`	Y[5]	Y[5]	Y[5]	Y[5]	Y	Y	Y[5]	Y[5]	Y[5]	Y	Y	Y	Y
`openPortsEnhanced.sh`	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N
`package.sh`	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N[6]
`passwd.sh`	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
`protocol.sh`	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
`ps.sh`	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y[7]	Y[7]
`rlog.sh`	Y	Y[8]	Y[8]	Y	Y[9]	Y	N	N	N	N	N	N	N
`selinuxChecker.sh`	Y	Y	Y	Y	Y	N	N	N	N	N	N	N	N

`service.sh`	Y	Y	Y	Y	N[10]	Y	Y	Y	Y	N	N	N	N
`sshdChecker.sh`	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N
`time.sh`	Y[11]	Y[11]	Y	Y	Y	Y	Y	Y	Y	Y	Y[11]	Y	Y
`top.sh`	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
`update.sh`	Y	Y	Y	Y	N	N	N	N	N	N	N	N	N
`uptime.sh`	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
`usersWithoginPrivs.sh`	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
`version.sh`	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
`vmstat.sh`	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
`vsfptdChecker.sh`	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
`who.sh`	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Notes

1. Supported, requires `netstat -i`. The fields `rxKB_PS` and `txKB_PS` are set to <n/a> because netstat on Solaris 10 and 11 does not provide this information.
2. Supported, requires `dlstat`.
3. Not supported, `sar` is not available.
4. Not supported, `/bin/darwin_disk_stats` is not available.
5. Supported, script indexes `Header` information as an extra event.
6. Not supported, `pkg_info` is deprecated.
7. Supported, `COMMAND` field value is truncated.
8. Supported, error log messages are included.
9. Supported, requires `ausearch`.
10. Not supported, `chkconfig` is not available.
11. Supported, requires `ntpdate`.

Upgrade

Users upgrading to the Splunk Add-on for Unix and Linux version 6.0.1 from version 5.2.4 or earlier must follow prerequisite upgrade steps before performing the installation. See Upgrade the Splunk Add-on for Unix and Linux.

New features

The Splunk Add-on for Unix and Linux version 6.0.1 has the following new features:

- Supported extraction for the `cpu_instance` field. Earlier versions extracted only `cpu=all`. Version 6.0.1 can extract field values for individual core numbers in addition to `cpu=all`.
- Supported extraction for the `mem_page_in` and `mem_page_out` field
- Supported extraction for the `swap_percent` field
- Supported extraction for the `cpu_architecture` field

Fixed issues

Version 6.0.1 of the Splunk Add-on for Unix and Linux has the following fixed issues:

Date resolved	Issue number	Description
2018-09-05	ADDON-19194	Incorrect value in swapUsedPct field in FreeBSD os
2018-09-04	ADDON-18051	Extract cpu_instance field (ITSI OS Module requirement)
2018-09-02	ADDON-18093	Extract field swap_percent (ITSI OS Module requirement)
2018-08-30	ADDON-18095	Extract fields mem_page_in and mem_page_out (ITSI OS Module requirement)
2018-08-27	ADDON-18042	Extract cpu_architecture field (ITSI OS Module requirement)

Known issues

Version 6.0.1 of the Splunk Add-on for Unix and Linux has the following known issues. If no issues appear here, no issues have yet been reported:

Date filed	Issue number	Description
2017-08-29	ADDON-19367	Add-on for Unix and Linux 5.2.3 sometimes not getting data for CPU VMSTAT IOSTAT metrics

Third-party software attributions

The Splunk Add-on for Unix and Linux does not use third-party software or libraries.

Release history for the Splunk Add-on for Unix and Linux

Latest release

The latest version of the Splunk Add-on for Unix and Linux is version 6.0.1. See Release notes for the Splunk Add-on for Unix and Linux for release notes of this latest version.

Version 6.0.0

Version 6.0.0 of the Splunk Add-on for Unix and Linux was released on June 21, 2018.

The Splunk Add-on for Unix and Linux 6.0.0 introduces breaking changes. If you are upgrading from a previous version of the Splunk Add-on for Unix and Linux, you must follow the steps outlined in Upgrade the Splunk Add-on for Unix and Linux. Failure to do so can result in data loss.

Compatibility

Version 6.0.0 of the Splunk Add-on for Unix and Linux is compatible with the following software, CIM versions, and platforms.

Splunk platform versions	6.5.x, 6.6.x, 7.0.x, 7.1.x, 7.2.x
CIM	4.11
Supported OS for data collection	All supported Unix operating systems. See Unix operating systems.
Vendor products	All supported Unix operating systems. See Unix operating systems.

Script compatibility

Script	CentOS		RHEL		Ubuntu		Solaris			AIX		FreeBS	
	6	7	7.4	6.9	14.04	16.04	10	11.3	11.0	7.1	7.2	9	10
`bandwidth.sh`	Y	Y	Y	Y	Y	Y	Y[1]	Y[2]	Y	Y	Y	N[3]	N[3]
`common.sh`	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
`cpu.sh`	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
`df.sh`	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

hardware.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
interfaces.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
iostat.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
lastlog.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	Y	Y
lsof.sh	Y	Y	Y	Y	Y	Y	N	N	N	N	N	N	N
netstat.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
openPorts.sh	Y[5]	Y[5]	Y[5]	Y[5]	Y	Y	Y[5]	Y[5]	Y[5]	Y	Y	Y	Y
openPortsEnhanced.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N
package.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N[6]
passwd.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
protocol.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
ps.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y[7]	Y[7]
rlog.sh	Y	Y[8]	Y[8]	Y	Y[9]	Y	N	N	N	N	N	N	N
selinuxChecker.sh	Y	Y	Y	Y	Y	N	N	N	N	N	N	N	N
service.sh	Y	Y	Y	Y	N[10]	Y	Y	Y	Y	N	N	N	N
sshdChecker.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N
time.sh	Y[11]	Y[11]	Y	Y	Y	Y	Y	Y	Y	Y	Y[11]	Y	Y
top.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
update.sh	Y	Y	Y	Y	N	N	N	N	N	N	N	N	N
uptime.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
usersWithoginPrivs.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
version.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
vmstat.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
vsfptdChecker.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
who.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Notes

1. Supported, requires `netstat -i`. The fields `rxKB_PS` and `txKB_PS` are set to <n/a> because netstat on Solaris 10 and 11 does not provide this information.
2. Supported, requires `dlstat`.
3. Not supported, `sar` is not available.
4. Not supported, `/bin/darwin_disk_stats` is not available.

5. Supported, script indexes `Header` information as an extra event.
6. Not supported, `pkg_info` is deprecated.
7. Supported, `COMMAND` field value is truncated.
8. Supported, error log messages are included.
9. Supported, requires `ausearch`.
10. Not supported, `chkconfig` is not available.
11. Supported, requires `ntpdate`.

Upgrade

All users upgrading to the Splunk Add-on for Unix and Linux version 6.0.0 must follow the prerequisite upgrade steps before performing the installation. See Upgrade the Splunk Add-on for Unix and Linux.

New features

Version 6.0.0 of the Splunk Add-on for Unix and Linux contains the following new and changed features:

- Added support for RedHat Enterprise Linux 7
- Added support for Solaris 10 and Solaris 11
- Linux scripts migrated from net-tools to iproute2 to support current Linux releases

Script updates

- `netstat.sh` (sourcetype=netstat) is updated. The `Proto` field no longer contains the IP address type and the `State` field value is truncated.

```
Proto  Recv-Q  Send-Q  LocalAddress          ForeignAddress
       State
tcp         0       0  127.0.0.1:53350       127.0.0.1:8191
       ESTAB
tcp         0       0  127.0.0.1:8191        127.0.0.1:53324
      ESTAB
tcp         0     128  :::22                 :::*
                 LISTEN
tcp         0     100  ::1:25                :::*
                 LISTEN
```

- `openPorts.sh` (sourcetype=openPorts) is updated. The `protocol` field no longer contains the IP address type.

```
tcp 22
tcp 8089
tcp 25
tcp 8191
tcp 8000
tcp 8065
tcp 22
tcp 25
```

- `interfaces.sh` (sourcetype=interfaces) is updated. The `inetAddr` field now contains the netmask.

```
Name  MAC                inetAddr       inet6Addr
                   Collisions  RXbytes    RXerrors  TXbytes
 TXerrors  Speed      Duplex
eth0  00:50:56:95:a4:f7  10.0.3.235/20
 fe80::250:56ff:fe95:a4f7/64  0           620790375  0
        2982390  0         10000Mb/s  Full
```

- `lastlog.sh` (sourcetype=lastlog) is updated. The `LATEST` field no longer contains the seconds and year in the timestamp, and the `FROM` field only contains an IP address.

```
USERNAME                        FROM
                           LATEST
user1                           10.0.1.1
                       Thu Mar 29 13:04
user2                           10.0.1.1
                       Mon Apr 9 14:34
```

Fixed issues

Version 6.0.0 of the Splunk Add-on for Unix and Linux fixed the following issues:

Date resolved	Issue number	Description
2018-04-12	ADDON-14093	vmstat script error on AIX
2018-03-30	ADDON-12085	recursive search for bash_histories is expensive
2018-03-27	ADDON-14719	Add-on not Supporting current OS Releases
2018-03-27	ADDON-12862, ADDON-12805	vmstat.sh thows ExecProcessor errors on machines with Infiband interfaces
2018-03-23	ADDON-13986	cpu.sh indexed output is missing core number.

Known issues

If no issues appear here, no issues have yet been reported.

Version 6.0.0 of the Splunk Add-on for Unix and Linux has the following known issues:

Date filed	Issue number	Description
2018-05-11	ADDON-18051	Extract cpu_instance field (ITSI OS Module requirement)
2018-05-09	ADDON-18042	Extract cpu_architecture field (ITSI OS Module requirement)

2018-04-19	ADDON-17763	Getting error log message into SplunkD for rlog.sh script execution for CentOS 7 and RHEL 7.4
		Workaround:
		Replace
		`` if [ -n "`service auditd status`" -a "$?" -eq 0 ] ; then{code} ``
		in rlog.sh script with
		`` if [ -n "`service auditd status 2>/dev/null`" -a "$?" -eq 0 ] ; then{code} ``

2018-03-27	ADDON-17560	Data is not getting indexed for service.sh in Ubuntu 14.04
2017-08-29	ADDON-19367	Add-on for Unix and Linux 5.2.3 sometimes not getting data for CPU VMSTAT IOSTAT metrics

Third-party software attributions

The Splunk Add-on for Unix and Linux does not use third-party software or libraries.

Version 5.2.4

The Splunk Add-on for Unix and Linux was last updated in December 2017.

What's new

See the known issues and fixed issues of these release notes for product updates.

Fixed issues

Version 5.2.4 of the Splunk Add-on for Unix and Linux fixed the following issues:

Date resolved	Issue number	Description
2017-04-17	ADDON-8472	Logic failure in rlog.sh creates duplicates when the seekpointer file cannot be updated and silently fails
2017-03-28	ADDON-13680	The dest field is not extracted for some events

Known Issues

Version 5.2.4 of the Splunk Add-on for Unix and Linux has the following known issues:

Date filed	Issue number	Description
2018-08-27	ADDON-19194	Incorrect value in swapUsedPct field in FreeBSD os
2018-05-18	ADDON-18093	Extract field swap_percent (ITSI OS Module requirement)
2018-05-18	ADDON-18095	Extract fields mem_page_in and mem_page_out (ITSI OS Module requirement)
2018-05-11	ADDON-18051	Extract cpu_instance field (ITSI OS Module requirement)
2018-05-09	ADDON-18042	Extract cpu_architecture field (ITSI OS Module requirement)
2018-04-18	ADDON-17747	package.sh not working in FreeBSD 10 and FreeBSD 11
2018-03-28	ADDON-17571	AWS TA and *nix TA lack spec files for eventgen.conf, which causes cluster bundle validation errors, and breaks Manage Indexes page in clustered Splunk Cloud Workaround: Splunk Cloud customers who cannot create indexes on their own due to this bug should file a support case when they need new indexes created.

2017-08-29	ADDON-19367	Add-on for Unix and Linux 5.2.3 sometimes not getting data for CPU VMSTAT IOSTAT metrics
2017-05-09	ADDON-14719	Add-on not Supporting current OS Releases
2017-05-05	ADDON-14708	Upgrade Splunk Add-on for Unix to support RHEL 7.3
2017-03-13	ADDON-14093	vmstat script error on AIX
2017-03-06	ADDON-13986	cpu.sh indexed output is missing core number. Workaround: Edit contents of cpu.sh script as follows: #Need to change to always be 24Hour time with export LC_TIME=POSIX export LC_TIME='POSIX' FORMAT='{cpu=$2; pctUser=$3; pctNice=$4; pctSystem=$5; pctIowait=$6; pctSteal=$7; pctIdle=$NF}'
2016-11-10	ADDON-12085	recursive search for bash_histories is expensive

Version 5.2.3

The Splunk Add-on for Unix and Linux was last updated on April 5, 2016.

What's new

Here's what's new in the latest version of the Splunk App for Unix and Linux:

Publication date	Defect number	Description
2016-4-5	TAG-11060	The add-on has been updated to provide better support for Key Performance Indicators (KPIs) for the Splunk IT Service Intelligence OS Module.

Current known issues

The Splunk App for Unix and Linux has the following known issues:

Publication date	Defect number	Description
2016-2-29	TAG-10164	On some versions of Linux (for example, RedHat), the `rlog.sh` scripted input improperly calls for the status of the `auditd` service, which forces the OS to

		redirect the call to the right service and generates an error in `splunkd.log`.
2015-12-15	TAG-4275	The scripts that come with the add-on rely on system utilities to run properly. If those utilities are not present, the scripts exit silently.

Change Log (what's been fixed)

Publication date	**Defect number**	**Description**
2016-4-5	TAG-11059	The add-on has been updated to provide better support for Key Performance Indicators (KPIs) for the Splunk IT Service Intelligence OS Module.

Version 5.2.2

The Splunk Add-on for Unix and Linux was last updated on February 29, 2016.

What's new

Here's what's new in the latest version of the Splunk App for Unix and Linux:

Publication date	**Defect number**	**Description**
2016-2-29	N/A	Bug fixes.
2016-2-29	TAG-10606	Event type definitions in the add-on have been updated to improve performance.

Current known issues

The Splunk App for Unix and Linux has the following known issues:

Publication date	**Defect number**	**Description**
2016-2-29	TAG-10164	On some versions of Linux (for example, RedHat), the `rlog.sh` scripted input improperly calls for the status of the `auditd` service, which forces the OS to redirect the call to the right service and generates an error in `splunkd.log`.
2015-12-15	TAG-4275	The scripts that come with the add-on rely on system utilities to run properly. If those utilities are not present, the scripts exit silently.

Change Log (what's been fixed)

Publication date	Defect number	Description
2016-2-29	TAG-10606	Event type definitions in the add-on have been updated to improve performance.
2016-2-29	TAG-10537	The add-on now determines the correct operating system version numbers on hosts that run AIX and Solaris.
2016-2-29	TAG-10474	A typo in a field transformation that referenced an invalid `FORMAT` argument has been fixed.
2016-2-29	TAG-9922	The add-on has been updated to not expose file and scripted input configuration controls on Splunk Cloud installations.

Version 5.2.1

The Splunk Add-on for Unix and Linux was last updated on December 15, 2015.

What's new

Here's what's new in the latest version of the Splunk App for Unix and Linux:

Publication date	Defect number	Description
2015-12-15	N/A	Bug fixes.

Current known issues

The Splunk App for Unix and Linux has the following known issues:

Publication date	Defect number	Description
2015-12-15	TAG-4275	On hosts that run AIX, the `vmstat.sh` script does not produce output.

Change Log (what's been fixed)

Publication date	Defect number	Description

2015-12-15	TAG-10147	A problem with `vmstat.sh` where space-delimited and tab-delimited entries were intermingled was fixed.
2015-12-15	TAG-10213	The add-on has been updated to move some of the data it collects into a data model. This is for use with the OS Module for Splunk IT Service Intelligence.
2015-12-15	TAG-4211	A problem where the `rlog.sh` and `[monitor://var/log]` stanzas within the add-on collected `audit.log` twice (in different ways) was fixed.

Version 5.2.0

The Splunk Add-on for Unix and Linux was last updated on September 18, 2015.

What's new

Here's what's new in the latest version of the Splunk App for Unix and Linux:

Publication date	Defect number	Description
2015-9-18	N/A	Bug fixes.
2015-9-18	N/A	The app has been updated to be compatible with Splunk Enterprise version 6.3.

Current known issues

The Splunk App for Unix and Linux has the following known issues:

<table>
<tr><th>Publication date</th><th>Defect number</th><th>Description</th></tr>
<tr><td>2015-10-13</td><td>TAG-4211</td><td>The rlog.sh scripted input and [monitor:///var/log] input stanza both collect audit.log, although in slightly different formats. This might result duplicate data collection. To work around this problem, add a blacklist to [monitor:///var/log] stanza:
[monitor:///var/log]
whitelist=(\.log|log$|messages|secure|auth|mesg$|cron$|acpid$|\.</td></tr>
</table>

```
blacklist=(audit.log|lastlog|anaconda\.syslog)
index=os
disabled = 1
```

Change Log (what's been fixed)

Publication date	**Defect number**	**Description**
2015-9-18	TAG-9589	The add-on no longer breaks search-time extractions for `syslog` on upgrade.
2015-9-18	TAG-9482	The add-on no longer reports incorrect CPU usage when installed on a Solaris 10 host.
2015-9-18	TAG-9353	The `storage`, `storage_used`, and `storage_free` fields now display data in megabytes instead of bytes.
2015-9-18	TAG-9312	The `rlog.sh` scripted input now reads the first line of the `audit.log` file. This fixes a problem where events in Splunk Enterprise did not reflect all contents of the file.
2015-9-18	TAG-9220	The `package.sh` scripted input now populates the `RELEASE` field on Debian Linux systems.
2015-9-18	TAG-3913	The regular expression that defines line breaking patterns for the add-on no longer generates spurious errors in the line-breaking processor.

Version 5.1.2

The Splunk Add-on for Unix and Linux was last updated on April 1, 2015.

What's new

Here's what's new in the latest version of the Splunk App for Unix and Linux:

- Bug fixes.

Current known issues

The Splunk App for Unix and Linux has the following known issues:

- The values for total, used, and free memory that the `vmstat.sh` script displays differ from the values that the native `vmstat` command displays. This is because `vmstat.sh` counts swap cache memory and buffer memory as part of the total free memory available, and subtracts this from total memory to get used memory. This is by design. (TAG-4014, TAG-9010)
- The vmstat scripted input does not work on AIX. (TAG-4518)
- On Linux systems, the `cpu.sh` script does not display the `%steal` CPU counter. (TAG-4114)
- Due to how Mac OS X configures OpenSSL, any Splunk Add-on for Unix and Linux scripts that use a hash (such as `openPortsEnhanced.sh`, `passwd.sh`, and `sshdChecker.sh`) do not work by default. To work around the problem, set the `DYLD_LIBRARY_PATH` variable as follows:

```
export SPLUNK_HOME=<location of Splunk installation>
export DYLD_LIBRARY_PATH=$SPLUNK_HOME/lib
```

(NIX-649, SPL-78856)

- Using the latest version of Sideview Utils with the add-on causes a problem where dashboards do not populate despite the availability of data. To work around the problem, use version 1.3.5 or earlier of Sideview Utils. (NIX-646)
- When you install the app and point it at the indexes which contain your *nix data, it might take up to 15 seconds for that data to begin showing up in the app. This is due to lookup generation. (NIX-467)
- The colors in the Metrics Viewer graphs do not update correctly if you transpose sliders in the Metrics Viewer's threshold bar. (NIX-428)
- When in node view, the Hosts dashboard sometimes shows inconsistent colors with respect to the detailed view colors. (NIX-353, NIX-409)
- When you use Firefox to access the Splunk App for Unix and Linux, the radial graphs in the Home dashboard sometimes do not display correctly. The slices within the graphs sometimes spill out of their containers. To work around the problem, refresh the page. (NIX-370, NIX-413)
- On HP/UX systems, there is no way to obtain the number of threads on a system. This means that the `vmstat` scripted inputs will always return "?" for threads columns on HP/UX.
- On Solaris systems, the `hardware.sh` scripted input sometimes returns empty values for some entries. (NIX-42)
- If you clone an existing alert saved search, you cannot edit the search using the "Settings: Alerts" configuration page. (NIX-537)
- You cannot create custom alerts using Splunk Web; you must do so with configuration files. (NIX-536)

- If you remove the default group, you sometimes receive an error "`Unknown search command: 'all'`" when you load the Home page. (NIX-560)
- In the Hosts page, if you do not wait for all data on a host information card to load before pinning that card, when you select another host, the original host information card does not remain pinned. (NIX-320)
- The app's scripted inputs do not work when the directory that they are hosted in contains spaces. This is particularly an issue with Mac OS X. (NIX-570)
- The full-screen NOC screen legends do not display correctly in Chrome. (NIX-584)
- You are not able to drill down into a specific host on the Hosts dashboard. (NIX-587)

Change Log (what's been fixed)

- Copyright information for the add-on has been updated and corrected. (TAG-9244)
- The add-on no longer incorrectly displays in the Splunk Light Dashboards page. (TAG-9182)
- The `su_authentication` event type within the add-on now has better `su` command event-matching logic. (TAG-8938)
- The `uptime.sh` script in the add-on now handles `ps` output properly on HP-UX machines. (TAG-4204)
- An unnecessary transform for WMI installed apps has been removed. (TAG-4191)
- The `top.sh` script now accounts for the fact that, starting with Mac OS X version 10.9 Mavericks and later, there is no `rshrd` (resident shared address space size) statistic for the `top` command. On Mac OSX 10.9 Mavericks and later, the script now outputs "?" for that statistic, instead of generating an error. (TAG-4077)
- The add-on no longer attempts to automatically learn new source types when you tell it to monitor large directories. (TAG-3986)

Version 5.1.1

The Splunk Add-on for Unix and Linux was last updated on February 13, 2015.

What's new

Here's what's new in the latest version of the Splunk App for Unix and Linux:

- Bug fixes.
- Feature additions to better work with Splunk Light (TAG-3983, TAG-8913).

Current known issues

The Splunk App for Unix and Linux has the following known issues:

- The values for total, used, and free memory that the `vmstat.sh` script displays differ from the values displayed by the native `vmstat` command. This is because `vmstat.sh` counts swap cache memory and buffer memory as part of the total free memory available, and subtracts this from total memory to get used memory. This is by design. (TAG-4014, TAG-9010)
- On Linux systems, the `cpu.sh` script does not display the `%steal` CPU counter. (TAG-4114)
- Due to how Mac OS X configures OpenSSL, any Splunk Add-on for Unix and Linux scripts that use a hash (such as `openPortsEnhanced.sh`, `passwd.sh`, and `sshdChecker.sh`) do not work by default. To work around the problem, set the `DYLD_LIBRARY_PATH` variable as follows:

```
export SPLUNK_HOME=<location of Splunk installation>
export DYLD_LIBRARY_PATH=$SPLUNK_HOME/lib
```

(NIX-649, SPL-78856)

- Using the latest version of Sideview Utils with the add-on causes a problem where dashboards do not populate despite the availability of data. To work around the problem, use version 1.3.5 or earlier of Sideview Utils. (NIX-646)
- When you install the app and point it at the indexes which contain your *nix data, it might take up to 15 seconds for that data to begin showing up in the app. This is due to lookup generation. (NIX-467)
- The colors in the Metrics Viewer graphs do not update correctly if you transpose sliders in the Metrics Viewer's threshold bar. (NIX-428)
- When in node view, the Hosts dashboard sometimes shows inconsistent colors with respect to the detailed view colors. (NIX-353, NIX-409)
- When you use Firefox to access the Splunk App for Unix and Linux, the radial graphs in the Home dashboard sometimes do not display correctly. The slices within the graphs sometimes spill out of their containers. To work around the problem, refresh the page. (NIX-370, NIX-413)
- On HP/UX systems, there is no way to obtain the number of threads on a system. This means that the `vmstat` scripted inputs will always return "?" for threads columns on HP/UX.
- On Solaris systems, the `hardware.sh` scripted input sometimes returns empty values for some entries. (NIX-42)
- If you clone an existing alert saved search, you cannot edit the search

using the "Settings: Alerts" configuration page. (NIX-537)
- You cannot create custom alerts using Splunk Web; you must do so with configuration files. (NIX-536)
- If you remove the default group, you sometimes receive an error "`Unknown search command: 'all'`" when you load the Home page. (NIX-560)
- In the Hosts page, if you do not wait for all data on a host information card to load before pinning that card, when you select another host, the original host information card does not remain pinned. (NIX-320)
- The app's scripted inputs do not work when the directory that they are hosted in contains spaces. This is particularly an issue with Mac OS X. (NIX-570)
- The full-screen NOC screen legends do not display correctly in Chrome. (NIX-584)
- You are not able to drill down into a specific host on the Hosts dashboard. (NIX-587)

Change Log (what's been fixed)

- A cosmetic issue with the "Reset" button on the add-on configuration page has been fixed. (TAG-3976)
- The documentation links in the add-on now go to valid places. (TAG-4421)

Version 5.1.0

The Splunk Add-on for Unix and Linux was last updated on October 6, 2014.

What's new

Here's what's new in the latest version of the Splunk App for Unix and Linux:

- Bug fixes.
- Feature additions to better work with the Splunk App for Enterprise Security.
- The add-on now contains some knowledge layer improvements. (NIX-638)
- The add-on now normalizes timestamps to work with the Change_Analysis data model. (NIX-668)
- The add-on now has higher-resolution icons. (NIX-660)

Current known issues

The Splunk App for Unix and Linux has the following known issues:

- The values for total, used, and free memory that the vmstat.sh script displays differ from the values displayed by the native vmstat command. This is because vmstat.sh counts swap cache memory and buffer memory as part of the total free memory available, and subtracts this from total memory to get used memory. This is by design. (TAG-4014, TAG-9010)
- Due to how Mac OS X configures OpenSSL, any Splunk Add-on for Unix and Linux scripts that use a hash (such as openPortsEnhanced.sh, passwd.sh, and sshdChecker.sh) do not work by default. To work around the problem, set the DYLD_LIBRARY_PATH variable as follows:

```
export SPLUNK_HOME=<location of Splunk installation>
export DYLD_LIBRARY_PATH=$SPLUNK_HOME/lib
```

(NIX-649, SPL-78856)

- Using the latest version of Sideview Utils with the add-on causes a problem where dashboards do not populate despite the availability of data. To work around the problem, use version 1.3.5 or earlier of Sideview Utils. (NIX-646)
- When you install the app and point it at the indexes which contain your *nix data, it might take up to 15 seconds for that data to begin showing up in the app. This is due to lookup generation. (NIX-467)
- The colors in the Metrics Viewer graphs do not update correctly if you transpose sliders in the Metrics Viewer's threshold bar. (NIX-428)
- When in node view, the Hosts dashboard sometimes shows inconsistent colors with respect to the detailed view colors. (NIX-353, NIX-409)
- When you use Firefox to access the Splunk App for Unix and Linux, the radial graphs in the Home dashboard sometimes do not display correctly. The slices within the graphs sometimes spill out of their containers. To work around the problem, refresh the page. (NIX-370, NIX-413)
- On HP/UX systems, there is no way to obtain the number of threads on a system. This means that the vmstat scripted inputs will always return "?" for threads columns on HP/UX.
- On Solaris systems, the hardware.sh scripted input sometimes returns empty values for some entries. (NIX-42)
- If you clone an existing alert saved search, you cannot edit the search using the "Settings: Alerts" configuration page. (NIX-537)
- You cannot create custom alerts using Splunk Web; you must do so with configuration files. (NIX-536)
- If you remove the default group, you sometimes receive an error "Unknown search command: 'all'" when you load the Home page. (NIX-560)
- In the Hosts page, if you do not wait for all data on a host information card

to load before pinning that card, when you select another host, the original host information card does not remain pinned. (NIX-320)
- The app's scripted inputs do not work when the directory that they are hosted in contains spaces. This is particularly an issue with Mac OS X. (NIX-570)
- The full-screen NOC screen legends do not display correctly in Chrome. (NIX-584)
- You are not able to drill down into a specific host on the Hosts dashboard. (NIX-587)

Change Log (what's been fixed)

- A problem with the first-time run experience where a file rename would cause the experience to repeat continuously was fixed. (NIX-664)
- A search macro definition for network monitoring that conflicted with a similar definition in the Splunk Add-on for Windows was corrected. (NIX-663)
- Values defined within stanzas in some configuration files now have proper URI encodings. (NIX-656)
- The `vmstat.sh` script now properly returns results on systems with more than one mass storage device. (NIX-648)
- A problem where event type searches generated false positives because they include the summary index has been fixed. (NIX-644)
- The Splunk Supporting App for Unix and Linux (SA-Nix) no longer overwrites the `action` field. (NIX-641)
- A search-time field extraction that referenced the `syslog` source type has been removed. (NIX-634)
- A typo in the `version.sh` script has been corrected. (NIX-630)
- The `setup.sh` script now properly accepts the `--auth` argument. This enables users to use the script to log into their Splunk Enterprise instance while setting up the Splunk App for Unix and Linux from the command line. (NIX-624)
- A customer-submitted patch to `interfaces.sh` improves how that script gathers network interface error statistics. (NIX-623)

Hardware and software requirements for the Splunk Add-on for Unix and Linux

The Splunk Add-on for Unix and Linux installs on Splunk instances that run on many versions of Unix, including Linux, Solaris, AIX, and HP/UX.

Dependencies

The Splunk Add-on for Unix and Linux requires these software packages to be installed on all supported Unix and Linux operating systems:

- `sysstat`
- `ntpdate`
- `lsof`

Use your OS-specific package manager to install these packages if they are not already installed.

The Splunk Add-on for Unix and Linux requires `net-tools` to be installed on RHEL 7 and CentOS 7. Use your OS-specific package manager to install this package if it is not already installed.

Splunk admin requirements

To install and configure the Splunk Add-on for Unix and Linux, you must be member of the `admin` or `sc_admin` role.

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.

For information about installation locations and environments, see Install the Splunk Add-on for Unix and Linux.

Installation and configuration overview for the Splunk Add-on for Unix and Linux

Complete the following steps to install and configure this add-on:

1. If you are upgrading from a previous version, perform the prerequisite Upgrade the Splunk Add-on for Unix and Linux steps.
2. Install the Splunk Add-on for Unix and Linux.
3. Enable data and scripted inputs for the Splunk Add-on for Unix and Linux.

Installation

Install the Splunk Add-on for Unix and Linux

You can install the Splunk Add-on for Unix and Linux with Splunk Web or from the command line. You can install the add-on onto any type of Splunk Enterprise or Splunk Cloud instance.

1. Get the Splunk Add-on for Unix and Linux by downloading it from http://splunkbase.splunk.com/app/833 or browsing to it using the app browser within Splunk Web.
2. Determine where and how to install this add-on in your deployment, using the tables on this page.
3. Perform any prerequisite steps before installing, if required and specified in the tables on this page.
4. Complete your installation.

If you need step-by-step instructions on how to install an add-on in your specific deployment environment, see the Installation walkthroughs section at the bottom of this page for links to installation instructions specific to a single-instance deployment, distributed deployment, Splunk Cloud, or Splunk Light.

Distributed deployment

Use the tables on this page to determine where and how to install this add-on in a distributed deployment of Splunk Enterprise or any deployment for which you are using forwarders to get your data in. Depending on your environment, your preferences, and the requirements of the add-on, you may need to install the add-on in multiple places.

Where to install this add-on

All supported add-ons can be safely installed to all tiers of a distributed Splunk platform deployment. See Where to install Splunk add-ons in *Splunk Add-ons* for more information.

This table provides a reference for installing this specific add-on to a distributed deployment of the Splunk platform:

	Supported	Required	Comments

Splunk platform instance type			
Search heads	Yes	Yes	Install this add-on to all search heads where Unix or Linux knowledge management is required. As a best practice, turn add-on visibility off on your search heads to prevent data duplication errors that can result from running inputs on your search heads instead of or in addition to your data collection node.
Indexers	Yes	Conditional	Not required if you use heavy forwarders to collect data. Required if you use universal or light forwarders to collect data.
Heavy forwarders	Yes	See comments	This add-on supports forwarders of any type for data collection. The host must run a supported version of *nix.
Universal forwarders	Yes	See comments	
Light forwarders	Yes	See comments	

Distributed deployment feature compatibility

This table describes the compatibility of this add-on with Splunk distributed deployment features:

Distributed deployment feature	Supported	Comments
Search head clusters	Yes	Disable add-on visibility on search heads.
Indexer clusters	Yes	To get data from an indexer cluster member, install the add-on into that member.
Deployment server	Yes	Supported for deploying the configured add-on to multiple nodes.

Installation walkthroughs

The *Splunk Add-Ons* manual includes an Installing add-ons guide that helps you successfully install any Splunk-supported add-on to your Splunk platform.

For a walkthrough of the installation procedure, follow the link that matches your deployment scenario:

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

Upgrade the Splunk Add-on for Unix and Linux

If you are upgrading from version 6.0.0 to 6.0.1, you do not need to take additional action.

To upgrade from version 5.2.4 or earlier, use the following instructions.

Upgrade from 5.2.4 or earlier to 6.0.1

To upgrade from version 5.2.4 or earlier to 6.0.1, begin by making the following changes to your `indexes.conf` file:

Configure indexes.conf

The Splunk Add-on for Unix and Linux versions 6.0.0 and later do not have predefined `os` and `firedalerts` indexes. You must make a local copy of the `indexes.conf` file before performing the upgrade.

If you upgrade the Splunk Add-on for Unix and Linux from version 5.2.4 to version 6.0.1 before making a local copy of `indexes.conf`, the existing index configurations will not be available after the upgrade and the previously indexed data may be lost. If indexes are defined and not copied over, newly ingested data may be lost. If you send data to an undefined index, data will be lost.

1. Copy `$SPLUNK_HOME/etc/apps/Splunk_TA_nix/default/indexes.conf` to `$SPLUNK_HOME/etc/apps/Splunk_TA_nix/local/indexes.conf`.
2. If necessary, create the event indexes. See Create and edit event indexes.

3. To index data in a specific index, edit `inputs.conf` and add `index = indexname` in the `input` stanza.

Configure inputs.conf

You must edit the `inputs.conf` file to set the default indexing location and update the stanza name for bash history.

Default indexing location

The Splunk Add-on for Unix and Linux version 5.2.4 indexes data by default into an `os` index. Versions 6.0.0 and later index data into the default index, typically `main`. If you want to index data with version 6.0.1 into the same index used by version 5.2.4, add `index = <os>` or `<index = firedalerts>` to each `input` stanza in the `inputs.conf` file.

1. Edit `$SPLUNK_HOME/etc/apps/Splunk_TA_nix/local/inputs.conf`.
2. Locate each `input` stanza and add `index = <os>` or `<index = firedalerts>`.

If you do not do these steps, the Splunk Add-on for Unix and Linux 6.0.1 will index data into the default index, typically `main`.

Monitoring bash history

To improve performance, the stanza name for monitoring bash histories was renamed in the Splunk Add-on for Unix and Linux version 6.0.0. You must update the version 5.2.4 `bash_history` stanza name used in the `inputs.conf` file to match the new stanza name used in versions 6.0.0 and later:

1. Edit `$SPLUNK_HOME/etc/apps/Splunk_TA_nix/local/inputs.conf`.
2. Locate the stanza `[monitor:///home/.../.bash_history]`.
3. Rename the stanza name to `[monitor:///home/*/.bash_history]`.

If you do not do these steps, you will see both `[monitor:///home/.../.bash_history]` and `[monitor:///home/*/.bash_history]` in the add-on setup page.

Configure app.conf

The Splunk Add-on for Unix and Linux versions 6.0.0 and later set configuration status to `false` by default. The Splunk Add-on for Unix and Linux will prompt you to perform a full setup the first time that Splunk Web launches it.

If you do not want to reconfigure the add-on after the upgrade is completed, add `is_configured=true` to the `app.conf` file.

1. Edit `$SPLUNK_HOME/etc/apps/Splunk_TA_nix/local/app.conf`.
2. Locate the `install` stanza and add `is_configured=true`.

Configuration

Enable data and scripted inputs for the Splunk Add-on for Unix and Linux

After you have installed the Splunk Add-on for Unix and Linux, you must enable the data and scripted inputs within the add-on so that it collects data from your data collection nodes.

The Splunk Add-on for Unix and Linux has a configuration page which lets you enable the inputs from within Splunk Web. This page is only available on Heavy Forwarders and full instances of Splunk Enterprise. Use this option when you are collecting data from a server with a full instance of Splunk Enterprise installed.

On a Universal Forwarder, you must enable the inputs using the configuration files.

Enable the data and scripted inputs from within Splunk Web

When you configure the add-on from within Splunk Web, the configuration page has into two sections: The **File and Directory Inputs** section and the **Scripted Inputs** section.

1. Log into the Splunk Enterprise instance installed on the server from which you want to collect data.
2. Activate the Splunk Add-on for Unix and Linux. Locate the Splunk Add-on for Unix and Linux on the Apps page, and click the **Set up** link in the row for the Splunk Add-on for Unix and Linux.
3. In the **File and Directory Inputs** section of the configuration page, click the radio buttons below **Enable** or **Disable** to enable or disable the input for the specified file or directory. You can also click the **(All)** link next to either **Enable** or **Disable** to enable all of the displayed inputs.
4. In the **Scripted Inputs** section, click the radio buttons below **Enable** or **Disable** to enable or disable the input for the specified script (as shown under **Name**.) You can also click the **(All)** link next to **Enable** or **Disable** to enable or disable all of the displayed scripted inputs.
5. (Optional) Set the interval for a script by entering a positive number in the **Interval** text box for each script. For example, if you want the `cpu.sh` script to run once an hour, type in `3600` in the "Interval" text box for `cpu.sh`.
6. Click **Save**.

Enable the data and scripted inputs with configuration files

When you configure data and scripted inputs using configuration files, copy only the input stanzas whose configurations you want to change. Do not copy the entire file, as those changes persist even after an upgrade.

1. Create `inputs.conf` in the `$SPLUNK_HOME/etc/apps/Splunk_TA_nix/local` directory.
2. Open `$SPLUNK_HOME/etc/apps/Splunk_TA_nix/local/inputs.conf` for editing.
3. Open `$SPLUNK_HOME/etc/apps/Splunk_TA_nix/default/inputs.conf` for editing.
4. Copy the input stanza text that you want to enable from the `$SPLUNK_HOME/etc/apps/Splunk_TA_nix/default/inputs.conf` file and paste them into the `$SPLUNK_HOME/etc/apps/Splunk_TA_nix/local/inputs.conf` file.
5. In the `$SPLUNK_HOME/etc/apps/Splunk_TA_nix/local/inputs.conf` file, enable the inputs that you want the add-on to monitor by setting the `disabled` attribute for each input stanza to 0.
6. Save the `$SPLUNK_HOME/etc/apps/Splunk_TA_nix/local/inputs.conf` file.
7. Restart the Splunk platform.

Troubleshooting

Troubleshoot the Splunk Add-on for Unix and Linux

General troubleshooting

For 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*.

Missing data from scripts

If data is missing from the script output, you can run the scripts in debug mode and use the additional information to look for the cause of the missing data.

1. Navigate to `$SPLUNK_HOME/etc/apps/Splunk_TA_nix/bin`.
2. Run `sh <script_name> --debug` to run the script in debug mode.
3. The debug output is saved in `debug--<script_name>--<date_and_time_of_execution>`. This file contains the command that was executed, and its output or the failure reason. Use this information to resolve the missing data issue.

Unexpected values for `cpu_load_percent` and `cpu_user_percent` fields

The Splunk Add-on for Unix and Linux version 6.0.1 enhances field extraction for the sourcetype `cpu` by extracting `cpu_user_percent` and `cpu_load_percent` fields for specific core numbers as well as for all instances. To query across all, which is what previous versions of the add-on do, use `cpu=all`. To query for a specific core number, include the number in your query, such as `cpu=1`.