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

Generated: 8/10/2022 11:03 am

Copyright (c) 2022 Splunk Inc. All Rights Reserved

Table of Contents

Overview

About the Splunk Add-on for Unix and Linux

Version	8.7.0
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 data from Unix and Linux hosts. Install the Splunk Add-on for Unix and Linux on a **forwarder** to send data from any number of 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.

File Monitoring Inputs

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

- Monitoring `/etc` directory
- Monitoring `/var/log` directory
- Monitoring `/home/*/.bash_history` directory
- Monitoring `/root/.bash_history` directory
- Monitoring `/var/adm` directory
- Monitoring `/Library/` Logs

Scripted Inputs

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`
`cpu_metric.sh`	CPU statistics and OS info via the shell commands `hostname`, `ifconfig`, `uname`, `sar`, `mpstat`, and `iostat`
`df.sh`	Free disk space for each mount point via the shell commands `df`, `mount`, and `fstyp`
`df_metric.sh`	Statistics of free disk space for each mount point and OS info via the shell commands `hostname`, `ifconfig`, `uname`, `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`
`interfaces_metric.sh`	Statistics of configured network interfaces and OS info via the shell commands `hostname`, `ifconfig`, `uname`, `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`

Input	Description
iostat_metric.sh	Statistics of Input/output statistics for block devices and partitions and OS info via the shell commands hostname, ifconfig, uname, 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
nfsiostat.sh	Collects NFS mounts data via the shell command nfsiostat. Requires the nfs-utils package.
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, 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
ps_metric.sh	Statistics of the status of currently running processes and OS info via the shell command hostname, ifconfig, uname and ps
rlog.sh	Linux Auditing System events 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 and chronyc, date andntpdate
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
vmstat_metric.sh	Statistics of process-related memory usage information and OS info via the shell commands hostname, ifconfig, uname 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 Splunk Community page for 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	Authentication
auditd	Auditd logs translated with ausearch	n/a
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
cpu_metric	Statistical information of CPU	n/a
df	Available disk space on mounted volumes	Performance
df_metric	Statistical information of available disk space on mounted volumes	n/a
dhcpd	Dynamic Host Control Protocol (DHCP) daemon information	Network Sessions
fs_notification	File system notification changes	Endpoint
hardware	Hardware specifications	Inventory
interfaces	Network interface information	Inventory
interfaces_metric	Statistical information of network interface.	n/a
iostat	Input/Output operation information	Performance
iostat_metric	Statistical information of input/output operation.	n/a
lastlog	Last login times for system accounts	n/a
linux_audit	The Linux audit log file.	Authentication, Change
Linux:SELinuxConfig	SELinux host configuration information	n/a
linux_secure	The Linux security log file	Authentication, Change
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	Endpoint
nfsiostat	Collects NFS mounts data	Performance

Source type	Description	CIM data models
openPorts	A list of the open ports on a host	n/a
osx_secure	The security log file for Mac OS X	
package	A list of installed packages	n/a
protocol	Network protocol stack information	n/a
ps	Process information	Performance
ps_metric	Process statistical information	n/a
time	Time service information	n/a
top	Process and system resource information	n/a
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	n/a
Unix:Service	Unix service information	Endpoint
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
vmstat_metric	Virtual memory statistical information	n/a
who	All users currently logged in	n/a

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

Version 8.7.0 of the Splunk Add-on for Unix and Linux was released on July 26, 2022.

Compatibility

Version 8.7.0 of the Splunk Add-on for Unix and Linux is compatible with the following software, CIM versions, and platforms:

Splunk platform versions	8.1.x, 8.2.x, 9.0.0
CIM	4.20.2
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.

See the Scripted input reference for the Splunk Add-on for Unix and Linux page in the *Reference* chapter of this manual to learn more about scripted inputs and their operating system compatibility.

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 8.7.0 of the Splunk Add-on for Unix and Linux has the following new features:

- Enhanced df, interfaces and ps scripts to make the add-on more robust and efficient across various operating systems.
- Support for RHEL v8.6 and RHEL v9.
- Breaking Change: For ps and ps_metric scripts, ELAPSED and PSR were removed from kernel outputs except for AIX and SunOS as part of v8.7.0.

For more information on the enhanced scripts, see the Reference Section.

Bug fixes

- Fixed the issue where events were breaking when forwarded from UF via the httpout method.
- Fixed the issue where package.sh throws awk regular expression syntax error.
- Fixed the issue where df_metric.sh script gave erroneous output when a hyphen character '-' is present in the IUse% field.

Fixed issues

Version 8.7.0 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:

Known issues

Version 8.7.0 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:

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

The latest version of the Splunk Add-on for Unix and Linux is version 8.7.0. See Release notes for the Splunk Add-on for Unix and Linux for release notes of this latest version.

Version 8.6.0

Version 8.6.0 of the Splunk Add-on for Unix and Linux was released on July 1, 2022.

Compatibility

Version 8.6.0 of the Splunk Add-on for Unix and Linux is compatible with the following software, CIM versions, and platforms:

Splunk platform versions	8.1.x, 8.2.x, 9.0.0
CIM	4.20.2
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.

See the Scripted input reference for the Splunk Add-on for Unix and Linux page in the *Reference* chapter of this manual to learn more about scripted inputs and their operating system compatibility.

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 8.6.0 of the Splunk Add-on for Unix and Linux has the following new features:

- Enhanced iostat scripts to make the add-on more robust and efficient across various operating systems.
- Support for cpu.sh and cpu_metric.sh script on macOS > v10.11.
- Support for update.sh script on Ubuntu OS.
- Support for Ubuntu OS v22.04.
- Support for macOS v12.4.

For more information on the enhanced iostat scripts, see the Reference Section.

Bug fixes

- Fixed the issue with df.sh not extracting type field correctly on AIX operating systems when file systems names are long.
- Removed extractions for deprecated fs_notification sourcetype.
- Fixed the issue with df_metric.sh not generating output as expected when the output of command misses certain fields or contains an empty row.
- Renamed setup.env_cloud.xml to ta_nix_configuration.env_cloud.xml to avoid errors on Splunk Cloud while updating permissions.
- Fixed the issue with hardware.sh displaying errors when there are disks with no volume groups attached on AIX operating systems.
- Fixed the issue with the hardware.sh displaying errors when there are disks part of an inactive volume group on AIX operating systems.

Fixed issues

Version 8.6.0 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:

Known issues

Version 8.6.0 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:

Third-party software attributions

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

Version 8.5.0

Version 8.5.0 of the Splunk Add-on for Unix and Linux was released on April 21, 2022.

Compatibility

Version 8.5.0 of the Splunk Add-on for Unix and Linux is compatible with the following software, CIM versions, and platforms:

Splunk platform versions	8.1.x, 8.2.x
CIM	4.20.2
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.

See the Scripted input reference for the Splunk Add-on for Unix and Linux page in the *Reference* chapter of this manual to learn more about scripted inputs and their operating system compatibility.

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 8.5.0 of the Splunk Add-on for Unix and Linux has the following new features:

- Support for Least Privilege Mode functionality of the Splunk Universal Forwarder
- Support for the latest flavors of Unix/Linux (RHEL 8.5 and MacOS 12.2)
- Updated the logic in 'iostat.sh' and 'iostat_metric.sh' scripts to calculate 'avgWaitMillis' when 'await' is missing from the output of the raw command
- Added 6 new fields in 'iostat.sh' and 'iostat_metric.sh' for Linux kernels:
    - rAvgWaitMillis (Read request processing wait time)
    - wAvgWaitMillis (Write request processing completion wait time)

- rrqmPct (The percentage of read requests merged together before being sent to the device)
- wrqmPct (The percentage of write requests merged together before being sent to the device)
- rAvgReqSZkb (Average read request size in KB)
- wAvgReqSZkb (Average write request size in KB)

Bug fixes

- Fixed output of nfsiostat.sh script for Ubuntu 20.04

Fixed issues

Version 8.5.0 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:

Known issues

Version 8.5.0 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:

Third-party software attributions

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

Version 8.4.0

Version 8.4.0 of the Splunk Add-on for Unix and Linux was released on December 07, 2021.

Compatibility

Version 8.4.0 of the Splunk Add-on for Unix and Linux is compatible with the following software, CIM versions, and platforms:

Splunk platform versions	8.1.x, 8.2.x
CIM	4.20.2
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.

See the Scripted input reference for the Splunk Add-on for Unix and Linux page in the *Reference* chapter of this manual to learn more about scripted inputs and their operating system compatibility.

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 8.4.0 of the Splunk Add-on for Unix and Linux has the following new features:

- Support for the latest vendor products of Nix (RHEL 8.4, Ubuntu 21.04, FreeBSD 13, and macOS 11.6)
- Support for INode fields of all the OSs in the 'df' and 'df_metric' scripts' output
- Support for the latest CIM version (4.20.2)
- Added 'user_name' and 'src_user_name' fields to the 'linux_secure' and 'linux_audit' sourcetypes
- Reinstated the 'process' tag for the 'top' and 'ps' eventtypes

Bug fixes

- Fixed the normalisation issue for the 'pctCPU' and 'pctMEM' fields when value is either <0 or >100 in output of 'ps' and 'ps_metric' scripts.
- Fixed the issue in 'iostat' and 'iostat_metric' scripts to support the latest version of the sysstat package.
- Fixed the field extraction where the value of the 'user' was truncated when it contained special characters for the 'aix_secure', 'osx_secure', linux_secure', and 'syslog' sourcetypes.
- Fixed the 'df' and 'df_metric' scripts for the incorrect data when mount point has a space character for Linux kernel OSs.
- Fixed the 'rlog' script to remove the unwanted error in the splunkd logs when no new data is available.
- Fixed the 'interfaces' and 'interfaces_metric' scripts to remove the warning of awk regular expression syntax.

Fixed issues

Version 8.4.0 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:

Known issues

Version 8.4.0 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
2022-03-14	ADDON-49319	seekptr checksum errors seen while trying to monitor /etc folder
2022-03-09	ADDON-49067	Update.sh is throwing a few permission errors before the output in RHEL in LPM
2021-01-20	ADDON-33139	Input netstat.sh and openPorts.sh gives error in splunkd.log when add-on is installed on macOS v10.15.7
2020-06-18	ADDON-27321	nfsiostat.sh fails with ImportError: This package should not be accessible on Python 3
2020-04-24	ADDON-26293	Field values gets broke when values has space for 'lsof' and 'userswithloginprivs' source types
2020-04-24	ADDON-26292	Additional error of broken pipe is getting logged under splunkd.log along with correct data for cpu.sh on Solaris OS
2020-04-20	ADDON-26131, ADDON-33138	Input protocol.sh gives error in splunkd.log when add-on is installed on macOS

Third-party software attributions

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

Version 8.3.1

Version 8.3.1 of the Splunk Add-on for Unix and Linux was released on July 26, 2021.

Compatibility

Version 8.3.1 of the Splunk Add-on for Unix and Linux is compatible with the following software, CIM versions, and platforms:

Splunk platform versions	8.0.x, 8.1.x, 8.2.x
CIM	4.18
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.

See the Scripted input reference for the Splunk Add-on for Unix and Linux page in the *Reference* chapter of this manual to learn more about scripted inputs and their operating system compatibility.

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 8.3.1 of the Splunk Add-on for Unix and Linux has the following new features:

- Updated the setup page of the add-on to make it compatible with jQuery3.

Fixed issues

Version 8.3.1 of the Splunk Add-on for Unix and Linux has the following fixed issues:

Known issues

Version 8.3.1 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
2021-01-20	ADDON-33139	Input netstat.sh and openPorts.sh gives error in splunkd.log when add-on is installed on macOS v10.15.7
2020-06-18	ADDON-27321	nfsiostat.sh fails with ImportError: This package should not be accessible on Python 3
2020-04-24	ADDON-26293	Field values gets broke when values has space for 'lsof' and 'userswithloginprivs' source types
2020-04-24	ADDON-26292	Additional error of broken pipe is getting logged under splunkd.log along with correct data for cpu.sh on Solaris OS
2020-04-20	ADDON-26130	When there is no new data available to be ingested in audit.log, rlog.sh script throws error in splunkd.log
2020-04-20	ADDON-26131, ADDON-33138	Input protocol.sh gives error in splunkd.log when add-on is installed on macOS

Third-party software attributions

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

Version 8.3.0

Version 8.3.0 of the Splunk Add-on for Unix and Linux was released. on February 3, 2021.

Compatibility

Version 8.3.0 of the Splunk Add-on for Unix and Linux is compatible with the following software, CIM versions, and platforms:

Splunk platform versions	7.2.x, 7.3.x, 8.0.x, 8.1.x
CIM	4.18
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.

See the Scripted input reference for the Splunk Add-on for Unix and Linux page in the *Reference* chapter of this manual to learn more about scripted inputs and their operating system compatibility.

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 8.3.0 of the Splunk Add-on for Unix and Linux has the following new features:

- Support of CentOS 8, RHEL 8.3, Solaris 11.4, Ubuntu 20.10, FreeBSD 12.2, macOS 10.15
- Common Information Model (CIM) version 4.18 compatibility
- Enhanced CIM mappings and extractions for 'linux_secure' and 'aix_secure' sourcetypes

- Enhanced CIM mappings and extractions for 'dhcpd' sourcetype
- Mapped Endpoint.FileSystem data model to 'fs_notification' sourcetype
- Mapped Performance.CPU data model to 'ps' sourcetype
- Mapped Perfomance.Storage data model to 'nfsiostat' sourcetype
- Mapped Endpoint.Ports data model to 'netstat' sourcetype
- Removed DM mappings from 'top' and 'Unix:ListeningPorts' sourcetypes
- Added the `reason` CIM field for the 'Authentication.Failed_Authentication' data model

Fixed issues

Version 8.3.0 of the Splunk Add-on for Unix and Linux has the following fixed issues:

Date resolved	Issue number	Description
2021-01-28	ADDON-31685	The 'top.sh' script that Splunk_TA_nix app uses does not correctly extract the fields of the 'top' linux command in FreeBSD

Known issues

Version 8.3.0 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
2021-01-20	ADDON-33139	Input netstat.sh and openPorts.sh gives error in splunkd.log when add-on is installed on macOS v10.15.7
2020-06-18	ADDON-27321	nfsiostat.sh fails with ImportError: This package should not be accessible on Python 3
2020-04-24	ADDON-26293	Field values gets broke when values has space for 'lsof' and 'userswithloginprivs' source types
2020-04-24	ADDON-26292	Additional error of broken pipe is getting logged under splunkd.log along with correct data for cpu.sh on Solaris OS
2020-04-20	ADDON-26130	When there is no new data available to be ingested in audit.log, rlog.sh script throws error in splunkd.log
2020-04-20	ADDON-26131, ADDON-33138	Input protocol.sh gives error in splunkd.log when add-on is installed on macOS

Third-party software attributions

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

Version 8.2.0

Version 8.2.0 of the Splunk Add-on for Unix and Linux was released on September 21, 2020.

Compatibility

Version 8.2.0 of the Splunk Add-on for Unix and Linux is compatible with the following software, CIM versions, and platforms:

Splunk platform versions	7.1.x, 7.2.x, 7.3.x, 8.0.x
CIM	4.16
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.

See the Scripted input reference for the Splunk Add-on for Unix and Linux page in the *Reference* chapter of this manual to learn more about scripted inputs and their operating system compatibility.

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 8.2.0 of the Splunk Add-on for Unix and Linux has the following new features:

- Updated and added new CIM field compatibility for various sourcetypes.
- Removed deprecated CIM models and upgraded to new CIM models.

Fixed issues

Version 8.2.0 of the Splunk Add-on for Unix and Linux has the following fixed issues:

Date resolved	Issue number	Description
2020-08-18	ADDON-27953	Metric scripts produce error if there are spaces in the OSName variable

Known issues

Version 8.2.0 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
2020-12-04	ADDON-31685	The 'top.sh' script that Splunk_TA_nix app uses does not correctly extract the fields of the 'top' linux command in FreeBSD Workaround: Amended script under "elif ["x$KERNEL" = "xFreeBSD"] ; then" from: FORMAT_DOMAIN='{pr=$4; ni=$5; virt=$6; res=$7; stateRaw=$8; cpuTIME=$9; pctCPU=0+$10; command=$11}'

Date filed	Issue number	Description
		to FORMAT_DOMAIN='{pr=$4; ni=$5; virt=$6; res=$7; stateRaw=$8; cpuTIME=$10; pctCPU=$11; command=$12}' This aligns the columns correctly.
2020-06-18	ADDON-27321	nfsiostat.sh fails with ImportError: This package should not be accessible on Python 3
2020-04-24	ADDON-26293	Field values gets broke when values has space for 'lsof' and 'userswithloginprivs' source types
2020-04-24	ADDON-26292	Additional error of broken pipe is getting logged under splunkd.log along with correct data for cpu.sh on Solaris OS
2020-04-20	ADDON-26130	When there is no new data available to be ingested in audit.log, rlog.sh script throws error in splunkd.log
2020-04-20	ADDON-26131, ADDON-33138	Input protocol.sh gives error in splunkd.log when add-on is installed on macOS

Third-party software attributions

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

Version 8.1.0

Version 8.1.0 of the Splunk Add-on for Unix and Linux was released on June 24, 2020.

Compatibility

Version 8.1.0 of the Splunk Add-on for Unix and Linux is compatible with the following software, CIM versions, and platforms:

Splunk platform versions	7.1.x, 7.2.x, 7.3.x, 8.0.x
CIM	4.15
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.

See the Scripted input reference for the Splunk Add-on for Unix and Linux page in the *Reference* chapter of this manual to learn more about scripted inputs and their operating system compatibility.

New features

Version 8.1.0 of the Splunk Add-on for Unix and Linux has the following new features:

- Support for the metrics index for collecting statistical information of `cpu`, `df`, `iostat`, `interfaces`, `vmstat`, and `ps` sources.
- Additional support of the **chrony** command to get time-service information.

Fixed issues

Version 8.1.0 of the Splunk Add-on for Unix and Linux has the following fixed issues:

Date resolved	Issue number	Description
2020-06-16	ADDON-26155	Header data is also getting indexed as an event for "interfaces", "lastlog", "who" and "top" sourcetypes
2020-06-16	ADDON-16732	Script crashing, needs to be updated since ntpdate is deprecated
2020-06-02	ADDON-21184	service.sh outputs time as a service
2020-05-27	ADDON-26291	Fields are not getting extracted for 'auditd', 'lastlog' and 'netstat' Source type

Known issues

Version 8.1.0 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
2020-07-27	ADDON-27953	Metric scripts produce error if there are spaces in the OSName variable
2020-06-18	ADDON-27321	nfsiostat.sh fails with ImportError: This package should not be accessible on Python 3
2020-04-24	ADDON-26292	Additional error of broken pipe is getting logged under splunkd.log along with correct data for cpu.sh on Solaris OS
2020-04-24	ADDON-26293	Field values gets broke when values has space for 'lsof' and 'userswithloginprivs' source types
2020-04-20	ADDON-26130	When there is no new data available to be ingested in audit.log, rlog.sh script throws error in splunkd.log
2020-04-20	ADDON-26131, ADDON-33138	Input protocol.sh gives error in splunkd.log when add-on is installed on macOS

Third-party software attributions

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

Version 8.0.0

Version 8.0.0 of the Splunk Add-on for Unix and Linux was released on April 28, 2020.

Compatibility

Version 8.0.0 of the Splunk Add-on for Unix and Linux is compatible with the following software, CIM versions, and platforms:

Splunk platform versions	7.1.x, 7.2.x, 7.3.x, 8.0.x
CIM	4.15
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		FreeBSD			FreeNAS	Mac OS	
	6	7	6.9	7.4	8.0	14.04	16.04	10	11.3	11.0	7.1	7.2	9	10	11	11.3U1[13]	10.11	1
bandwidth.sh	Y	Y	Y	Y	Y	Y	Y	Y[1]	Y[2]	Y	Y	Y	N[3]	N[3]	N[3]	N[3]	Y	N[3]
common.sh	Y	Y	Y	Y	Y	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	Y	Y	Y	Y	N[3]
df.sh	Y	Y	Y	Y	Y	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	Y	Y	Y	Y	Y
interfaces.sh	Y	Y	Y	Y	Y	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	Y	Y	Y	N[4]	N[4]
lastlog.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	Y	Y	Y	Y	Y	Y
lsof.sh	Y[14]	Y[14]	Y[14]	Y[14]	Y[14]	Y[14]	Y[14]	N	N	N	N	N	N	Y[14]	Y[14]	Y[14]	Y[14]	Y[1]
netstat.sh	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	N	N	N	N	Y	N	N
nfsiostat.sh[12]	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N
openPorts.sh	Y[5]	Y[5]	Y[5]	Y[5]	Y[5]	Y	Y	Y[5]	Y[5]	Y[5]	Y	Y	Y	Y	Y	Y	Y	Y
openPortsEnhanced.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	N	N	Y	Y
package.sh	Y[14]	Y[14]	Y[14]	Y[14]	Y[14]	Y[14]	Y[14]	Y[14]	Y[14]	Y[14]	Y[14]	Y[14]	Y[14]	Y[6, 14, 16]	Y[6, 14, 16]	Y[14, 16]	Y[14]	Y[1]
passwd.sh	Y	Y	Y	Y	Y	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	Y	Y	Y	Y	Y
ps.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y[7]	Y[7]	Y[7]	Y	Y	Y
rlog.sh	Y	Y[8]	Y	Y[8]	Y[8]	Y[9]	Y	N	N	N	N	N	N	N	N	N	N	N
selinuxChecker.sh	Y	Y	Y	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N
service.sh	Y	Y	Y	Y	Y	N[10]	Y	Y	Y	Y	N	N	N	N	N	N	Y	Y
sshdChecker.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	N	N	N	N
time.sh	Y[11]	Y[11]	Y	Y	Y[11]	Y	Y	Y	Y	Y	Y	Y[11]	Y	Y	Y	Y	Y	Y
top.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
update.sh	Y	Y	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N	Y	Y
uptime.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
usersWithLoginPrivs.sh	Y	Y	Y	Y	Y	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	Y	Y	Y	Y	Y
vmstat.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
vsftpdChecker.sh	Y[15]	Y[15]	Y[15]	Y[15]	Y[15]	Y[15]	Y[15]	Y[15]	Y[15]	Y[15]	Y[15]	Y[15]	Y[15]	Y[15]	Y[15]	N	Y[15]	Y[1]
who.sh	Y	Y	Y	Y	Y	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. Supported. `pkg_info` is deprecated, and `pkg info` is being used.
7. Supported, `COMMAND` field value is truncated.
8. Supported, error log messages are included. Not supported for RHEL/CentOS version 7.3.
9. Supported, requires `ausearch`.
10. Not supported, `chkconfig` is not available.
11. Supported, requires `ntpdate` or `chrony` for RHEL version 8.
12. Supported with only Linux OS configurations, requires the `nfs-utils` package.
13. Only FreeNAS 11.3U1 is supported.
14. Bash shell is required to run the script. Install the bash package for the input.
15. Requires `vsftpd` package.
16. Data for **Name**, **Version** and **Architecture** of the package will be ingested by the Splunk software.

New features

Version 8.0.0 of the Splunk Add-on for Unix and Linux has the following new features:

- Common Information Model (CIM) version 4.15 compatibility.
- Support for RHEL version 8.0
- Increased `ps.sh COMMAND` field width to accommodate long values.
- Ability to capture `sshd-authentication` events that do not have `from` in the event
- Support for FreeNAS version 11.3U1.

Fixed issues

Version 8.0.0 of the Splunk Add-on for Unix and Linux has the following fixed issues:

Date resolved	Issue number	Description
2020-04-16	ADDON-17763	Getting error log message into SplunkD for rlog.sh script execution for CentOS 7 and RHEL 7.4
2020-04-16	ADDON-17607	openPorts.sh script indexed "Header" information into Splunk as an extra event.
2020-04-16	ADDON-21209	'Description' field is not properly extracted from events for service.sh script in CentOS 7 configurations
2020-03-31	ADDON-21887	cpu.sh and vmstat.sh return aggregate results for SunOS as opposed to snapshot
2019-12-11	ADDON-23937	interfaces script throwing error when touching disabled and not configured interfaces - familysearch.splunkcloud.com
2019-12-09	ADDON-23292, ADDON-16135	Search Job Alerts for Splunk defined eventtype

Known issues

Version 8.0.0 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
2020-06-18	ADDON-27321	nfsiostat.sh fails with ImportError: This package should not be accessible on Python 3
2020-04-24	ADDON-26293	Field values gets broke when values has space for 'lsof' and 'userswithloginprivs' source types
2020-04-24	ADDON-26292	Additional error of broken pipe is getting logged under splunkd.log along with correct data for cpu.sh on Solaris OS
2020-04-24	ADDON-26291	Fields are not getting extracted for 'auditd', 'lastlog' and 'netstat' Source type
2020-04-21	ADDON-26155	Header data is also getting indexed as an event for "interfaces", "lastlog", "who" and "top" sourcetypes
2020-04-20	ADDON-26130	When there is no new data available to be ingested in audit.log, rlog.sh script throws error in splunkd.log
2020-04-20	ADDON-26131, ADDON-33138	Input protocol.sh gives error in splunkd.log when add-on is installed on macOS
2019-01-31	ADDON-21184	service.sh outputs time as a service
2018-04-18	ADDON-17753	Truncation of COMMAND field value in UI of FreeBSD 9,10 and 11 version
2018-03-27	ADDON-17560	Data is not getting indexed for service.sh in Ubuntu 14.04

Third-party software attributions

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

Version 7.0.1

Version 7.0.1 of the Splunk Add-on for Unix and Linux was released on March 14, 2020.

Compatibility

Version 7.0.1 of the Splunk Add-on for Unix and Linux is compatible with the following software, CIM versions, and platforms:

Splunk platform versions	7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0
CIM	4.12
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		FreeBSD			Mac OS X	
	6	7	7.4	6.9	14.04	16.04	10	11.3	11.0	7.1	7.2	9	10	11	10.11	10.12
`bandwidth.sh`	Y	Y	Y	Y	Y	Y	Y[1]	Y[2]	Y	Y	Y	N[3]	N[3]	N[3]	Y	N[3]
`common.sh`	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Script	CentOS		RHEL		Ubuntu		Solaris			AIX		FreeBSD			Mac OS X	
cpu.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N[3]
df.sh	Y	Y	Y	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	Y	Y	Y
interfaces.sh	Y	Y	Y	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	Y	N[4]	N[4]
lastlog.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	Y	Y	Y	Y	Y
lsof.sh	Y	Y	Y	Y	Y	Y	N	N	N	N	N	N	N	N	Y	Y
netstat.sh	Y	Y	Y	Y	Y	Y	N	N	N	N	N	N	N	N	N	N
nfsiostat.sh[12]	Y	Y	Y	Y	Y	Y	N	N	N	N	N	N	N	N	N	N
openPorts.sh	Y[5]	Y[5]	Y[5]	Y[5]	Y	Y	Y[5]	Y[5]	Y[5]	Y	Y	Y	Y	Y	Y	Y
openPortsEnhanced.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	N	Y	Y
package.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N[6]	N[6]	Y	Y
passwd.sh	Y	Y	Y	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	Y	Y	Y
ps.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y[7]	Y[7]	Y[7]	Y	Y
rlog.sh	Y	Y[8]	Y[8]	Y	Y[9]	Y	N	N	N	N	N	N	N	N	N	N
selinuxChecker.sh	Y	Y	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N
service.sh	Y	Y	Y	Y	N[10]	Y	Y	Y	Y	N	N	N	N	N	Y	Y
sshdChecker.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	N	N	N
time.sh	Y[11]	Y[11]	Y	Y	Y	Y	Y	Y	Y	Y	Y[11]	Y	Y	Y	Y	Y
top.sh	Y	Y	Y	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	N	Y	Y
uptime.sh	Y	Y	Y	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	Y	Y	Y
version.sh	Y	Y	Y	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	Y	Y	N
vsfptdChecker.sh	Y	Y	Y	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	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`.
12. Supported with only Linux OS configurations, requires the `nfs-utils` package.

Upgrade

Users upgrading to the Splunk Add-on for Unix and Linux version 7.0 or later 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

Version 7.0.1 of the Splunk Add-on for Unix and Linux has the following new features:

- Default support for Python3

Fixed issues

Version 7.0.1 of the Splunk Add-on for Unix and Linux has the following fixed issues:

Date resolved	Issue number	Description
2019-09-26	ADDON-21212	interfaces script throwing error when touching disabled and not configured interfaces.

Known issues

Version 7.0.1 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
2020-04-24	ADDON-26293	Field values gets broke when values has space for 'lsof' and 'userswithloginprivs' source types
2020-04-24	ADDON-26292	Additional error of broken pipe is getting logged under splunkd.log along with correct data for cpu.sh on Solaris OS
2020-04-24	ADDON-26291	Fields are not getting extracted for 'auditd', 'lastlog' and 'netstat' Source type
2019-10-23	ADDON-24037	interfaces.sh script doesnot work with "ifconfig" command Workaround: If the system doesn't "ip" command and contains only "ifconfig" command, the interfaces.sh script may return incorrect results. In such cases, change CMD_LIST_INTERFACES to CMD_LIST_UP_INTERFACES in line 28. So the code look like: """ CMD_LIST_UP_INTERFACES ="eval ifconfig | tee $TEE_DEST | grep 'Link encap:|mtu' | grep -Ev lo | tee -a $TEE_DEST | cut -d' ' -f1 | cut -d':' -f1 | tee -a $TEE_DEST | sort -u | tee

Date filed	Issue number	Description
		-a $TEE_DEST" """
2019-02-05	ADDON-21209	'Description' field is not properly extracted from events for service.sh script in CentOS 7 configurations
2019-01-31	ADDON-21184	service.sh outputs time as a service
2018-04-18	ADDON-17753	Truncation of COMMAND field value in UI of FreeBSD 9,10 and 11 version
2018-04-03	ADDON-17607	openPorts.sh script indexed "Header" information into Splunk as an extra event.

Third-party software attributions

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

Version 7.0

Version 7.0 of the Splunk Add-on for Unix and Linux was released on October 21, 2019.

Compatibility

Version 7.0 of the Splunk Add-on for Unix and Linux is compatible with the following software, CIM versions, and platforms:

Splunk platform versions	7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0
CIM	4.12
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		FreeBSD			Mac OS X	
	6	7	7.4	6.9	14.04	16.04	10	11.3	11.0	7.1	7.2	9	10	11	10.11	10.12
bandwidth.sh	Y	Y	Y	Y	Y	Y	Y[1]	Y[2]	Y	Y	Y	N[3]	N[3]	N[3]	Y	N[3]
common.sh	Y	Y	Y	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	Y	Y	N[3]
df.sh	Y	Y	Y	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	Y	Y	Y
interfaces.sh	Y	Y	Y	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	Y	N[4]	N[4]
lastlog.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	Y	Y	Y	Y	Y
lsof.sh	Y	Y	Y	Y	Y	Y	N	N	N	N	N	N	N	N	Y	Y
netstat.sh	Y	Y	Y	Y	Y	Y	N	N	N	N	N	N	N	N	N	N
nfsiostat.sh[12]	Y	Y	Y	Y	Y	Y	N	N	N	N	N	N	N	N	N	N
openPorts.sh	Y[5]	Y[5]	Y[5]	Y[5]	Y	Y	Y[5]	Y[5]	Y[5]	Y	Y	Y	Y	Y	Y	Y

Script	CentOS		RHEL		Ubuntu		Solaris			AIX		FreeBSD			Mac OS X	
openPortsEnhanced.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	N	Y	Y
package.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N[6]	N[6]	Y	Y
passwd.sh	Y	Y	Y	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	Y	Y	Y
ps.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y[7]	Y[7]	Y[7]	Y	Y
rlog.sh	Y	Y[8]	Y[8]	Y	Y[9]	Y	N	N	N	N	N	N	N	N	N	N
selinuxChecker.sh	Y	Y	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N
service.sh	Y	Y	Y	Y	N[10]	Y	Y	Y	Y	N	N	N	N	N	Y	Y
sshdChecker.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	N	N	N
time.sh	Y[11]	Y[11]	Y	Y	Y	Y	Y	Y	Y	Y	Y[11]	Y	Y	Y	Y	Y
top.sh	Y	Y	Y	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	N	Y	Y
uptime.sh	Y	Y	Y	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	Y	Y	Y
version.sh	Y	Y	Y	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	Y	Y	N
vsfptdChecker.sh	Y	Y	Y	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	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`.
12. Supported with only Linux OS configurations, requires the `nfs-utils` package.

Upgrade

Users upgrading to the Splunk Add-on for Unix and Linux version 7.0 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

Version 7.0 of the Splunk Add-on for Unix and Linux has the following new features:

- Support for Python3

Fixed issues

Version 7.0 of the Splunk Add-on for Unix and Linux has the following fixed issues:

Date resolved	Issue number	Description
2019-09-26	ADDON-21212	interfaces script throwing error when touching disabled and not configured interfaces.

Known issues

Version 7.0 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
2020-04-24	ADDON-26293	Field values gets broke when values has space for 'lsof' and 'userswithloginprivs' source types
2020-04-24	ADDON-26292	Additional error of broken pipe is getting logged under splunkd.log along with correct data for cpu.sh on Solaris OS
2020-04-24	ADDON-26291	Fields are not getting extracted for 'auditd', 'lastlog' and 'netstat' Source type
2019-02-05	ADDON-21209	'Description' field is not properly extracted from events for service.sh script in CentOS 7 configurations
2019-01-31	ADDON-21184	service.sh outputs time as a service
2018-04-18	ADDON-17753	Truncation of COMMAND field value in UI of FreeBSD 9,10 and 11 version
2018-04-03	ADDON-17607	openPorts.sh script indexed "Header" information into Splunk as an extra event.

Third-party software attributions

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

Version 6.0.2

Version 6.0.2 of the Splunk Add-on for Unix and Linux was released on February 18, 2019.

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 6.0.2 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	4.12
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		FreeBSD			Mac OS X	
	6	7	7.4	6.9	14.04	16.04	10	11.3	11.0	7.1	7.2	9	10	11	10.11	10.12
bandwidth.sh	Y	Y	Y	Y	Y	Y	Y[1]	Y[2]	Y	Y	Y	N[3]	N[3]	N[3]	Y	N[3]
common.sh	Y	Y	Y	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	Y	Y	N[3]
df.sh	Y	Y	Y	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	Y	Y	Y
interfaces.sh	Y	Y	Y	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	Y	N[4]	N[4]
lastlog.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	Y	Y	Y	Y	Y
lsof.sh	Y	Y	Y	Y	Y	Y	N	N	N	N	N	N	N	N	Y	Y
netstat.sh	Y	Y	Y	Y	Y	Y	N	N	N	N	N	N	N	N	N	N
nfsiostat.sh[12]	Y	Y	Y	Y	Y	Y	N	N	N	N	N	N	N	N	N	N
openPorts.sh	Y[5]	Y[5]	Y[5]	Y[5]	Y	Y	Y[5]	Y[5]	Y[5]	Y	Y	Y	Y	Y	Y	Y
openPortsEnhanced.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	N	Y	Y
package.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N[6]	N[6]	Y	Y
passwd.sh	Y	Y	Y	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	Y	Y	Y
ps.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y[7]	Y[7]	Y[7]	Y	Y
rlog.sh	Y	Y[8]	Y[8]	Y	Y[9]	Y	N	N	N	N	N	N	N	N	N	N
selinuxChecker.sh	Y	Y	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N
service.sh	Y	Y	Y	Y	N[10]	Y	Y	Y	Y	N	N	N	N	N	Y	Y
sshdChecker.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	N	N	N
time.sh	Y[11]	Y[11]	Y	Y	Y	Y	Y	Y	Y	Y	Y[11]	Y	Y	Y	Y	Y
top.sh	Y	Y	Y	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	N	Y	Y
uptime.sh	Y	Y	Y	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	Y	Y	Y
version.sh	Y	Y	Y	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	Y	Y	N

Script	CentOS		RHEL		Ubuntu		Solaris			AIX		FreeBSD			Mac OS X	
vsftpdChecker.sh	Y	Y	Y	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	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`.
12. Supported with only Linux OS configurations, requires the `nfs-utils` package.

Upgrade

Users upgrading to the Splunk Add-on for Unix and Linux version 6.0.2 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

Version 6.0.2 of the Splunk Add-on for Unix and Linux has the following new features:

- Improved load balancing on the universal forwarder.
- Support of iostats for NFS mounts for Linux OS configurations.
- Added `KV_MODE = multi` parameter in `props.conf` under `package` sourcetype stanza for search time extractions.
- See Make CPU core statistics info in FreeBSD similar to other supported OS configurations.

Fixed issues

Version 6.0.2 of the Splunk Add-on for Unix and Linux has the following fixed issues:

Date resolved	Issue number	Description
2019-02-04	ADDON-20084	For CIM All_Application_State model field service is labeled as "Unknown"
2019-01-17	ADDON-17448	CPU core is not properly indexed with Splunk_TA_nix with FreeBSD11 OS
2018-12-19	ADDON-17431	Eventtype unix_runlevel_change name mismatch in eventtypes.conf and tags.conf

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
2019-10-11	ADDON-23937	interfaces script throwing error when touching disabled and not configured interfaces - familysearch.splunkcloud.com
2019-09-12	ADDON-23292, ADDON-16135	Search Job Alerts for Splunk defined eventtype Workaround: None known
2019-02-05	ADDON-21209	'Description' field is not properly extracted from events for service.sh script in CentOS 7 configurations
2019-01-31	ADDON-21184	service.sh outputs time as a service

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}`

2018-04-18	ADDON-17753	Truncation of COMMAND field value in UI of FreeBSD 9,10 and 11 version
2018-04-03	ADDON-17607	openPorts.sh script indexed "Header" information into Splunk as an extra event.
2018-03-27	ADDON-17560	Data is not getting indexed for service.sh in Ubuntu 14.04

Third-party software attributions

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

Version 6.0.1

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		FreeBSD			Mac OS X	
	6	7	7.4	6.9	14.04	16.04	10	11.3	11.0	7.1	7.2	9	10	11	10.11	10.12
bandwidth.sh	Y	Y	Y	Y	Y	Y	Y[1]	Y[2]	Y	Y	Y	N[3]	N[3]	N[3]	Y	N[3]
common.sh	Y	Y	Y	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	Y	Y	N[3]
df.sh	Y	Y	Y	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	Y	Y	Y
interfaces.sh	Y	Y	Y	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	Y	N[4]	N[4]
lastlog.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	Y	Y	Y	Y	Y
lsof.sh	Y	Y	Y	Y	Y	Y	N	N	N	N	N	N	N	N	Y	Y
netstat.sh	Y	Y	Y	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	Y	Y	Y
openPortsEnhanced.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	N	Y	Y
package.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N[6]	N[6]	Y	Y
passwd.sh	Y	Y	Y	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	Y	Y	Y
ps.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y[7]	Y[7]	Y[7]	Y	Y
rlog.sh	Y	Y[8]	Y[8]	Y	Y[9]	Y	N	N	N	N	N	N	N	N	N	N
selinuxChecker.sh	Y	Y	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N
service.sh	Y	Y	Y	Y	N[10]	Y	Y	Y	Y	N	N	N	N	N	Y	Y
sshdChecker.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	N	N	N
time.sh	Y[11]	Y[11]	Y	Y	Y	Y	Y	Y	Y	Y	Y[11]	Y	Y	Y	Y	Y
top.sh	Y	Y	Y	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	N	Y	Y
uptime.sh	Y	Y	Y	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	Y	Y	Y
version.sh	Y	Y	Y	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	Y	Y	N
vsfptdChecker.sh	Y	Y	Y	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	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
2019-02-05	ADDON-21209	'Description' field is not properly extracted from events for service.sh script in CentOS 7 configurations

Date filed	Issue number	Description
2019-01-31	ADDON-21184	service.sh outputs time as a service
2018-10-24	ADDON-20084	For CIM All_Application_State model field service is labeled as "Unknown"

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}`

2018-04-18	ADDON-17753	Truncation of COMMAND field value in UI of FreeBSD 9,10 and 11 version
2018-04-03	ADDON-17607	openPorts.sh script indexed "Header" information into Splunk as an extra event.

Third-party software attributions

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

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		FreeBSD			Mac OS X	
	6	7	7.4	6.9	14.04	16.04	10	11.3	11.0	7.1	7.2	9	10	11	10.11	10.12
`bandwidth.sh`	Y	Y	Y	Y	Y	Y	Y[1]	Y[2]	Y	Y	Y	N[3]	N[3]	N[3]	Y	N[3]
`common.sh`	Y	Y	Y	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	Y	Y	N[3]

Script	CentOS		RHEL		Ubuntu		Solaris			AIX		FreeBSD			Mac OS X	
df.sh	Y	Y	Y	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	Y	Y	Y
interfaces.sh	Y	Y	Y	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	Y	N[4]	N[4]
lastlog.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	Y	Y	Y	Y	Y
lsof.sh	Y	Y	Y	Y	Y	Y	N	N	N	N	N	N	N	N	Y	Y
netstat.sh	Y	Y	Y	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	Y	Y	Y
openPortsEnhanced.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	N	Y	Y
package.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N[6]	N[6]	Y	Y
passwd.sh	Y	Y	Y	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	Y	Y	Y
ps.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y[7]	Y[7]	Y[7]	Y	Y
rlog.sh	Y	Y[8]	Y[8]	Y	Y[9]	Y	N	N	N	N	N	N	N	N	N	N
selinuxChecker.sh	Y	Y	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N
service.sh	Y	Y	Y	Y	N[10]	Y	Y	Y	Y	N	N	N	N	N	Y	Y
sshdChecker.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	N	N	N
time.sh	Y[11]	Y[11]	Y	Y	Y	Y	Y	Y	Y	Y	Y[11]	Y	Y	Y	Y	Y
top.sh	Y	Y	Y	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	N	Y	Y
uptime.sh	Y	Y	Y	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	Y	Y	Y
version.sh	Y	Y	Y	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	Y	Y	N
vsfptdChecker.sh	Y	Y	Y	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	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
2019-02-05	ADDON-21212	interfaces script throwing error when touching disabled and not configured interfaces.
2019-02-05	ADDON-21209	'Description' field is not properly extracted from events for service.sh script in CentOS 7 configurations
2019-01-31	ADDON-21184	service.sh outputs time as a service

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}`

2018-04-18	ADDON-17753	Truncation of COMMAND field value in UI of FreeBSD 9,10 and 11 version
2018-04-03	ADDON-17607	openPorts.sh script indexed "Header" information into Splunk as an extra event.
2018-03-27	ADDON-17560	Data is not getting indexed for service.sh in Ubuntu 14.04

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
2019-04-24	ADDON-21887	cpu.sh and vmstat.sh return aggregate results for SunOS as opposed to snapshot Workaround: Current workaround is to implement (for example): mpstat -p 1 2 as opposed to mpstat -p 1 1 to reflect the most recent non-aggregated result from the script output.
2018-08-27	ADDON-19194	Incorrect value in swapUsedPct field in FreeBSD os
2018-04-18	ADDON-17753	Truncation of COMMAND field value in UI of FreeBSD 9,10 and 11 version
2018-04-18	ADDON-17747	package.sh not working in FreeBSD 10 and FreeBSD 11
2018-04-03	ADDON-17607	openPorts.sh script indexed "Header" information into Splunk as an extra event.
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.
2018-03-20	ADDON-17448	CPU core is not properly indexed with Splunk_TA_nix with FreeBSD11 OS
2018-03-19	ADDON-17431	Eventtype unix_runlevel_change name mismatch in eventtypes.conf and tags.conf
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}'

Date filed	Issue number	Description
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:

Publication date	Defect number	Description

2015-10-13	TAG-4211	The `rlog.sh` scripted input and `[monitor:///var/log]` input stanza both collect `audit.log`, although in slightly different formats. This might result in duplicate data collection. To work around this problem, add a blacklist to the `[monitor:///var/log]` stanza:
		
		`[monitor:///var/log]`
		`whitelist=(\.log|log$\|messages\|secure\|auth\|mesg$|cron$\|acpid$|\.out)`
		`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, and AIX.

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`
- `nfs-utils`
- `bash`
- `chrony`

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 7/8 and CentOS 7/8.

Splunk admin requirements

To install and configure the Splunk Add-on for Unix and Linux, you must be a member of the `admin` role or if you are a member of the `sc_admin` role then you need to provide the capabilities `edit_monitor` and `edit_scripted` to the user/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*.
- 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 Platform 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, or Splunk Cloud Platform.

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:

Splunk platform instance type	Supported	Required	Comments
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 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	This add-on supports forwarders of any type for data collection. The host must run a supported version of *nix.

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 Platform

Upgrade the Splunk Add-on for Unix and Linux

Upgrade from version 8.6.0 to version 8.7.0 of the Splunk Add-on for Unix and Linux is seamless. There are no additional steps required for this version upgrade. See the Install the Splunk Add-on for Unix and Linux topic in this manual.

Use the installation steps in this manual to upgrade from versions 7.0 and above to the latest version of this add-on.

Before upgrading to the Splunk Add-on for Unix and Linux versions 8.1.0 and higher, verify that you have the bash shell installed on your system. If the bash shell is not installed, the lsof and package inputs will not work.

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.

> Verify that you have execute rights for the bin folder. The scripts will display permission denied in the splunkd.log if you don't. Splunk must be installed and executed as root user for this Add-on to work properly.

See the Scripted input reference for the Splunk Add-on for Unix and Linux page in this manual for more information.

Collect statistical data from metrics indexes

> Versions 7.2 and later of the Splunk platform support metric index data collection.

Create a metric index for each supported source type for which you would like to collect data. The Splunk Add-on for Unix and Linux supports metric index data collection for the following source types:

- `cpu_metric`
- `df_metric`
- `interfaces_metric`
- `iostat_metric`
- `ps_metric`
- `vmstat_metric`

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 three sections: The **File and Directory Inputs** section, the **Scripted Metric Input** section and the **Scripted Event 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 Metric 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 metric inputs.
5. Set the index for a metric input by selecting the metric index from the Index selection dropdown. **Metric Index** is mandatory when configuring the metric input.

6. In the **Scripted Event 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 event inputs.
7. (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`.
8. 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. For any metric input, after enabling the metric input in the `$SPLUNK_HOME/etc/apps/Splunk_TA_nix/local/inputs.conf` file, configure an index for the enabled input by setting the `index` attribute for each metric input stanza to any preconfigured metric-index name.
7. Save the `$SPLUNK_HOME/etc/apps/Splunk_TA_nix/local/inputs.conf` file.
8. Restart the Splunk instance.

Enable data and scripted inputs with the command line

To configure inputs using the command line interface (CLI). Use the following steps:

1. Navigate to `$SPLUNK_HOME/bin/`.
2. To enable all inputs, except metric inputs, enter the following command:
   `./splunk cmd sh $SPLUNK_HOME/etc/apps/Splunk_TA_nix/bin/setup.sh --enable-all`
3. To enable all inputs, including metric inputs, enter the following command:
   `./splunk cmd sh /opt/splunk/etc/apps/Splunk_TA_nix/bin/setup.sh --enable-all --metric-index <valid metric index>`
4. To list all inputs, enter the following command:
   `./splunk cmd sh $SPLUNK_HOME/etc/apps/Splunk_TA_nix/bin/setup.sh --list-all`
5. To identify other commands, enter the following command:
   `./splunk cmd sh $SPLUNK_HOME/etc/apps/Splunk_TA_nix/bin/setup.sh --usage` OR `./splunk cmd sh $SPLUNK_HOME/etc/apps/Splunk_TA_nix/bin/setup.sh --help`
6. Restart the Splunk platform.

Configuration of file monitoring input for AIX

You must monitor the following files and directories and assign corresponding sourcetypes in AIX in order to utilize CIM mappings and field extractions.

File Name	sourcetype
`/var/adm/auth.log` or `path to security logs`	aix_secure

File Name	sourcetype
`/var/adm/messages` or `path to system logs`	syslog

Troubleshooting

Troubleshoot the Splunk Add-on for Unix and Linux

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*.

Errors seen in splunkd for rlog.sh script

```
Error parsing start date (MM/DD/YYYY)
```

Locales other than `en_US.UTF-8` are currently not supported by `ausearch` command which is being used in rlog.sh. If you are using locales other than `en_US.UTF-8` you will have to use the locale as `en_US.UTF-8` or its equivalent depending on your country.

Errors seen in output of Update.sh script

```
2021-12-23 06:50:15,873 [ERROR] yum:13717:MainThread @logutil.py:194 - [Errno 13] Permission denied:
'/var/log/rhsm/rhsm.log' - Further logging output will be written to stderr

2021-12-23 06:50:15,875 [ERROR] yum:13717:MainThread @identity.py:156 - Reload of consumer identity cert
/etc/pki/consumer/cert.pem raised an exception with msg: [Errno 13] Permission denied:
'/etc/pki/consumer/key.pem'
```

If you see errors similar or same as above errors, then provide the necessary permissions for the user running splunkd to read those files.

sshdChecker.sh and vsftpdChecker.sh scripted inputs giving some file permission errors

If you see file permission errors for the files 'sshd_config' (for sshdChecker.sh) and 'vsftpd.conf' (for vsftpdChecker.sh), then please provide the necessary permissions for the user running splunkd to read those files.

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 enhanced 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`.

Multiple events in package source type

In the `package`sourcetype of the Splunk Add-on for Unix and Linux version 6.0.1, all installed software packages are listed in one event, and there are no field extractions. In version 6.0.2 of the Splunk Add-on for Unix and Linux, events are divided into separate events per software package, and fields are extracted automatically for each event. This also applies to existing events.

Make CPU core statistics info in FreeBSD OS similar to other supported OS configurations

In version 6.0.1 of the Splunk Add-on for Unix and Linux 6.0.1, the `cpu` sourcetype for FreeBSD OS has CPU statistics for all cores as a single event, whereas for other OS configurations, there are separate events for separate cores as well as single event for all cores. In version 6.0.2 of the Splunk Add-on for Unix and Linux, `cpu.sh` script output data for FreeBSD OS is consistent with other OS configurations.

Not getting data from `nfsiostat` scripts

See Missing data from scripts to check the script behavior in debug mode.

If the output of script file in debug mode is "Not found command `nfsiostat` on this host," then install the `nfsutils` package. If data is not indexed after installing this package, then check the script in debug mode again. If the output is "No NFS mount points were found," then the NFS file system is missing. You need to set up NFS mount to get this data into your Splunk platform deployment.

COMMAND field is truncated in the data collected from ps.sh scripted input

If your environment contains any commands longer than 100 characters, perform the following steps to extend your deployment's maximum command length:

1. Navigate to `$SPLUNK_HOME/etc/apps/Splunk_TA_nix/bin`.
2. Open a CLI and enter `vi ps.sh`
3. Navigate to to line 21, and change `%-100.100s` to a command length that fits your environment. For example, `%-200.200s`.
4. Save your changes.

LC_CTYPE error for rlog.sh input

If you receive the error `"locale: Cannot set LC_ALL to default locale: No such file or directory`, verify the following:

If you are connecting to a Linux or Unix machine using a Mac OS Terminal, verify that the `locale` set is the same for both

operating system (OS) platforms.

- If the `locale` sets do not match, sync them, using the commands specific to your OS platform.
- As a best practice, keep `LANG="en_US.UTF-8"`. Alternate values are supported, as long as the values are the same for your remote machine and the machine from which you are logging in.

Scripted input not working due to insufficient permissions

Verify that you have execute rights for the `bin` folder. The scripts will display **permission denied** in the `splunkd.log` if you don't. Splunk must be installed and executed as root user for this Add-on to work properly.

Reference

Lookups for the Splunk Add-on for Unix and Linux

The Splunk Add-on for Unix and Linux contains the following lookup files:

File Name	Description
nix_da_update_status.csv	Maps sourcetypes to required update status.
nix_da_version_ranges.csv	Maps sourcetypes to OS-provided version information.
nix_endpoint_change_vendor_action.csv	Maps actions for windows registry and file system change notifications.
nix_fs_notification_change_type.csv	Maps sourcetypes and change types for file system change notifications.
nix_linux_audit_action_object_category.csv	Maps operations(op) to category and action for linux audit logs.
nix_object_category.csv	Maps object and object_category for windows registry and file system change notifications.
nix_status.csv	Maps status id and status for windows registry and file system change notifications
nix_user_types.csv	Maps sourcetypes and user types for windows registry and file system change notifications.
nix_vendor_actions.csv	Maps vendor_action and action for security logs..

Scripted input reference for the Splunk Add-on for Unix and Linux

See the following information about scripted inputs for the Splunk Add-on for Unix and Linux.

Script compatibility

Script	CentOS	RHEL								Ubuntu				Solaris			A
	7	7.4	7.8	8.0	8.2/ 8.3	8.4	8.5	8.6	9	14.04	16.04	18.04	22.04	10	11.3/ 11.4	11.0	7.1
bandwidth.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y[1]	Y[2]	Y	Y
common.sh	Y	Y	Y	Y	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	Y	Y	Y	Y
cpu_metric.sh	Y	Y	Y	Y	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	Y	Y	Y	Y
df_metric.sh	Y	Y	Y	Y	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	Y	Y	Y	Y
interfaces.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
interfaces_metric.sh	Y	Y	Y	Y	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	Y	Y	Y	Y
iostat_metric.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Script	CentOS	RHEL								Ubuntu				Solaris			A
lastlog.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N
lsof.sh	Y[14]	Y[14]	Y[14]	Y[14]	Y[14]	Y[14]	Y[14]	Y[14]	Y[14]	Y[14]	Y[14]	Y[14]	Y[14]	N	N	N	N
netstat.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N
nfsiostat.sh[12]	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N
openPorts.sh	Y[5]	Y[5]	Y[5]	Y[5]	Y[5]	Y[5]	Y[5]	Y[5]	Y[5]	Y	Y	Y	Y	Y[5]	Y[5]	Y[5]	Y
openPortsEnhanced.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
package.sh	Y[14]	Y[14]	Y[14]	Y[14]	Y[14]	Y[14]	Y[14]	Y[14]	Y[14]	Y[14]	Y[14]	Y[14]	Y[14]	Y[14]	Y[14]	Y[14]	Y[14]
passwd.sh	Y	Y	Y	Y	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	Y	Y	Y	Y
ps.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
ps_metric.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
rlog.sh	Y[8]	Y[8]	Y[8]	Y[8]	Y[8]	Y[8]	Y[8]	Y[8]	Y[8]	Y[9]	Y	Y	Y	N	N	N	N
selinuxChecker.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	N	N	N	N
service.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	N[10]	Y	Y	Y	Y	Y	Y	N
sshdChecker.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
time.sh	Y[11]	Y	Y[11]	Y[11]	Y[11]	Y[11]	Y[11]	Y[11]	Y[11]	Y	Y	Y	Y	Y	Y	Y	Y
top.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
update.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N
uptime.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
usersWithLoginPrivs.sh	Y	Y	Y	Y	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	Y	Y	Y	Y
vmstat.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
vmstat_metric.sh	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
vsftpdChecker.sh	Y[15]	Y[15]	Y[15]	Y[15]	Y[15]	Y[15]	Y[15]	Y[15]	Y[15]	Y[15]	Y[15]	Y[15]	Y[15]	Y[15]	Y[15]	Y[15]	Y[15]
who.sh	Y	Y	Y	Y	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. Supported. `pkg_info` is deprecated, and `pkg info` is being used.
7. Supported, `COMMAND` field value is truncated.
8. Supported, error log messages are included. Not supported for RHEL/CentOS version 7.3.
9. Supported, requires `ausearch`.
10. Not supported, `chkconfig` is not available.

11. Supported, requires `ntpdate` or `chrony` for RHEL version 8.
12. Supported with only Linux OS configurations, requires the `nfs-utils` package.
13. Only FreeNAS 11.3U1 is supported.
14. Bash shell is required to run the script. Install the bash package for the input.
15. Requires `vsftpd` package.
16. Data for **Name**, **Version** and **Architecture** of the package will be ingested by the Splunk software.

Robust implementation of scripts for Splunk Add-on for Unix and Linux

Version 8.7.0

As part of version 8.7.0 of the Splunk Add-on for Unix and Linux, we updated the implementation of ps, interfaces and df scripts to make them more robust and to work more efficiently across all supported operating systems.

Changes made as part of ps and df scripts

The tables below show field names extracted for ps and df scripts. It lists the normalized field names which the ps and df scripts previously output before version 8.7.0 and also displays the new 'raw' field names output starting with version 8.7.0. We've also maintained a backward compatibility of the older fields along with adding the new fields from the raw output.

Tables for ps scripts

ps.sh				
Fields in old script's output	**Equivalent fields in new script's output for Linux Kernel OSs**	**Equivalent fields in new script's output for (Darwin & FreeBSD) Kernel OSs**	**Equivalent fields in new script's output for Solaris Kernel OSs**	**Equivalent fields in new script's output for AIX Kernel OSs**
CPUTIME	TIME	TIME	TIME	TIME
RSZ_KB	RSS	RSS	RSS	RSS
S	STAT	STAT	S	S
TTY	TTY	TT	TTY	TT
VSZ_KB	VSZ	VSZ	VSZ	VSZ
pctCPU	CPU	CPU	CPU	CPU
pctMEM	MEM	MEM	MEM	MEM

ps_metric.sh	
Fields in Old script's output	**Equivalent fields in new script's output for all supported Kernals**
metric_name:ps_metric.RSZ_KB	metric_name:ps_metric.RSS
metric_name:ps_metric.VSZ_KB	metric_name:ps_metric.VSZ
metric_name:ps_metric.pctCPU	metric_name:ps_metric.CPU
metric_name:ps_metric.pctMEM	metric_name:ps_metric.MEM

: For ps and ps_metric scripts, ELAPSED and PSR were removed from kernel outputs except for AIX and SunOS as part of v8.7.0.

For the USER field in ps scripts, the add-on previously removed the preceding underscore (if any) from the value and then ingested the field. From v8.7.0 onwards, the add-on will be ingesting the value of the field as it is. If this field is used by any of your applications or use cases, Splunk best practice is to update them accordingly.

Tables for df scripts

df.sh				
Fields in old script's output	**Equivalent fields in new script's output for Linux Kernel OSs**	**Equivalent fields in new script's output for (Darwin & FreeBSD) Kernel OSs**	**Equivalent fields in new script's output for Solaris Kernel OSs**	**Equivalent fields in new script's output for AIX Kernel OSs**
Size	Size	Size	Size	1024-blocks
Avail	Avail	Avail	Available	Available
UsePct	Use_	Capacity	Capacity	Capacity
INodes	Inodes	INodes	INodes	INodes
IUsed	IUsed	iused	IUsed	Iused
IFree	IFree	ifree	IFree	Ifree
IUsePct	IUse_	IUsePct	IUsePct	IUsePct

df_metric.sh				
Fields in Old script's output	**Equivalent fields in new script's output for Linux Kernel OSs**	**Equivalent fields in new script's output for (Darwin) Kernel OSs**	**Equivalent fields in new script's output for (FreeBSD) Kernel OSs**	**Equiva scr Sola**
metric_name:df_metric:Size	metric_name:df_metric:1K-blocks	metric_name:df_metric:1024-blocks	metric_name:df_metric:1024-blocks	metric_n
metric_name:df_metric:Avail	metric_name:df_metric:Avail	metric_name:df_metric:Availble	metric_name:df_metric:Avail	metric_n
metric_name:df_metric:UsePct	metric_name:df_metric:Use	metric_name:df_metric:Capacity	metric_name:df_metric:Capacity	metric_n
metric_name:df_metric:INodes	metric_name:df_metric:Inodes	metric_name:df_metric:INodes	metric_name:df_metric:INodes	metric_n
metric_name:df_metric:IUsed	metric_name:df_metric:IUsed	metric_name:df_metric:iused	metric_name:df_metric:iused	metric_n
metric_name:df_metric:IFree	metric_name:df_metric:IFree	metric_name:df_metric:ifree	metric_name:df_metric:ifree	metric_n
metric_name:df_metric:IUsePct	metric_name:df_metric:IUse	metric_name:df_metric:IUsePct	metric_name:df_metric:IUsePct	metric_n
metric_name:df_metric:Used	metric_name:df_metric:Used	metric_name:df_metric:Used	metric_name:df_metric:Used	metric_n
metric_name:df_metric:Size_KB	metric_name:df_metric:1K-blocks	metric_name:df_metric:1024-blocks	metric_name:df_metric:1024-blocks	metric_n
metric_name:df_metric:Avail_KB	metric_name:df_metric:Avail	metric_name:df_metric:Available	metric_name:df_metric:Available	metric_n

Changes made as part of interfaces scripts

We have made the interfaces scripts less error prone in case the output of the raw command changes. No new fields were added for interfaces scripts as part of v8.7.0

Version 8.6.0

As part of version 8.6.0 of the Splunk Add-on for Unix and Linux, we updated the implementation of iostat scripts to make them more robust and to work more efficiently across all supported operating systems.

The most significant change is in regards to field extractions; Splunk best practice is now to extract data into both the raw field names output by the iostat command as well as the normalized field names that the add-on previously used. This enables you to build Splunk content (searches, reports, dashboards, etc) and leverage all the data points produced by the iostat command.

The table below shows an example of field names extracted on Ubuntu OS. It lists the normalized field names which the iostat script previously displayed before version 8.6.0 and also displays the new 'raw' field names output starting with version 8.6.0. Splunk maintains backward compatibility of existing content as older fields are extracted, but Splunk best practice is to update content to use the new field names.

Old field extraction names	New field extraction names
rReq_PS	r_s
rKB_PS	rkB_s
rrqmPct	rrqm
rAvgReqSZkb	rareq_sz
rAvgWaitMillis	r_await
wReq_PS	w/s
wKB_PS	wKB_s
wrqmPct	wrqm
wAvgWaitMilli	w_await
wAvgReqSZkb	wareq_sz
avgQueueSZ	aqu_sz
bandwUtilPct	util
avgSvcMillis	svctm
avgWaitMillis	await