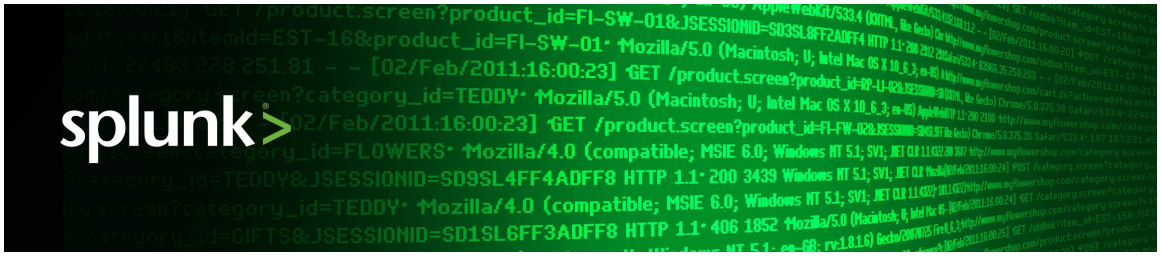

Splunk® Enterprise Installation Manual 7.1.0

System requirements for use of Splunk Enterprise on-premises

Generated: 5/18/2018 8:14 am

System requirements for use of Splunk Enterprise on-premises

Splunk supports using Splunk Enterprise on several computing environments. Learn about the supported environments before you download the software.

The universal forwarder has its own set of hardware requirements. See Universal forwarder system requirements in the *Universal Forwarder* manual.

If you have ideas or requests for new features and you have a current Splunk contract, open a request with Splunk Support.

Supported Operating Systems

The following tables list the available computing platforms for Splunk Enterprise. The first table lists availability for *nix operating systems and the second lists availability for Windows operating systems.

Each table shows available computing platforms (operating system and architecture) and types of Splunk software. A bold **X** in a box that intersects the computing platform and Splunk software type you want means that Splunk software is available for that platform and type.

An empty box means that Splunk software is not available for that platform and type.

If you do not see the operating system or architecture that you are looking for in the list, the software is not available for that platform or architecture. This might mean that Splunk has ended support for that platform. See the list of deprecated and removed computing platforms in Deprecated Features in the *Release Notes*.

Some boxes contain characters other than a check mark. See the bottom of each table to learn what the characters mean and how it could impact your installation.

Confirm support for your computing platform

1. Find the operating system on which you want to install Splunk Enterprise in the **Operating system** column.
2. Find the computing architecture in the **Architecture** column that matches your environment.
3. Find the type of Splunk software that you want to use: Splunk Enterprise, Splunk Free, Splunk Trial, or Splunk Universal Forwarder.

4. If Splunk software is available for the computing platform and software type that you want, proceed to the download page to get it.

Unix operating systems

Operating system	Architecture	Enterprise	Free	Trial	Universal Forwarder
Solaris 10 and 11	x86 (64-bit)				**X**
	SPARC				**X**
Linux, all 2.6 kernel versions	x86 (64-bit)	D	D	D	D
Linux, all 3.x and 4.x kernel versions	x86 (64-bit)	**X**	**X**	**X**	**X**
PowerLinux, Little Endian kernel version 2.6 and later (E)	PowerPC				**X**
zLinux, kernel version 2.6 and later	s390x				**X**
FreeBSD 10 and 11	x86 (64-bit)				**X**
Mac OS X 10.11	Intel		D	D	D
macOS 10.12 and 10.13	Intel		**X**	**X**	**X**
AIX 7.1 and 7.2	PowerPC				**X**
ARM Linux	ARM				**X**

D: Splunk supports this platform and architecture but might remove support in a future release. See Deprecated Features in the *Release Notes* for information on deprecation.
E: Support for PowerLinux on Big Endian kernels was removed.

Windows operating systems

The table lists the Windows computing platforms that Splunk Enterprise supports.

Operating system	Architecture	Enterprise	Free	Trial	

					Universal Forwarder
Windows Server 2008 R2 SP1	x86 (64-bit)				D
Windows Server 2012, Server 2012 R2, and Server 2016	x86 (64-bit)	**X**	**X**	**X**	**X**
Windows 8.1	x86 (64-bit)		D	D	**X**
	x86 (32-bit)		D	D	**X**
Windows 10	x86 (64-bit)		**X**	**X**	**X**
	x86 (32-bit)		***	***	**X**

D: Splunk supports this platform and architecture but might remove support in a future release. See Deprecated Features in the *Release Notes* for information on deprecation.
*** Splunk supports but does not recommend using Splunk Enterprise on this platform and architecture.

Operating system notes

Windows

Some parts of Splunk Enterprise on Windows require elevated user permissions to function properly. See the following topics for information on the components that require elevated permissions and how to configure Splunk Enterprise on Windows:

- Splunk Enterprise architecture and processes
- Choose the Windows user Splunk Enterprise should run as
- Considerations for deciding how to monitor remote Windows data in *Getting Data In*

Operating systems that support the Monitoring Console

The Splunk Enterprise Monitoring Console works only on some versions of Linux and Windows. For information on supported platform architectures for the Monitoring Console, see Supported platforms in the *Troubleshooting Manual*. To learn about the other prerequisites for the Monitoring Console, see Monitoring Console setup prerequisites in *Monitoring Splunk Enterprise*.

Deprecated operating systems and features

As we update Splunk software, we sometimes deprecate and remove support of older operating systems. See Deprecated features in the Release Notes for information on which platforms and features have been deprecated or removed entirely.

Support for some *nix operating systems has ended

Splunk has ended support for Splunk Enterprise on Solaris, FreeBSD, AIX, HP-UX, and 32-bit versions of the Linux kernel. Additionally, all support for HP/UX has been removed. If you need to install Splunk Enterprise on these platforms, you must download an older version of the software.

There are universal forwarder packages available for all platforms except HP/UX, and the *Universal Forwarder* manual provides installation instructions at the following links:

- Install the universal forwarder on Solaris
- Install the universal forwarder on FreeBSD
- Install the universal forwarder on AIX

Creating and editing configuration files on OSes that do not use UTF-8 character set encoding

Splunk software expects configuration files to be in ASCII or Universal Character Set Transformation Format-8-bit (UTF-8) format. If you edit or create a configuration file on an OS that does not use UTF-8 character set encoding, then ensure that the editor you use can save in ASCII or UTF-8.

IPv6 platform support

All Splunk-supported OS platforms can use IPv6 network configurations.

See Configure Splunk for IPv6 in the *Admin Manual* for details on IPv6 support in Splunk Enterprise.

Supported browsers

Splunk Enterprise supports the following browsers:

- Firefox (latest)

- Internet Explorer 11 (Splunk Enterprise does not support this browser in Compatibility Mode.)
- Safari (latest)
- Chrome (latest)

Recommended hardware

To evaluate Splunk Enterprise for a production deployment, use hardware that is typical of your production environment. This hardware should meet or exceed the recommended hardware capacity specifications.

For a discussion of hardware planning for production deployment, see Introduction to capacity planning for Splunk Enterprise in the *Capacity Planning* Manual.

Splunk Enterprise and virtual machines

If you run Splunk Enterprise in a virtual machine (VM) on any platform, performance decreases. This is because virtualization works by providing hardware abstraction on a machine into pools of resources. VMs that you define on the system draw from these resource pools. Splunk Enterprise needs sustained access to a number of resources, particularly disk I/O, for indexing operations. If you run Splunk Enterprise in a VM or alongside other VMs, indexing and search performance can degrade.

Splunk Enterprise and containerized infrastructures

Containerized deployment of Splunk Enterprise is not officially supported. However, Docker images of Splunk Enterprise are available at Docker Hub for developers to evaluate the deployment of Splunk on containerized infrastructures. These Docker images are supported by the community. See https://hub.docker.com/r/splunk/splunk/.

For additional information related to Splunk Enterprise on containerized infrastructures, see Is Splunk supported on Kubernetes on the Splunk Answers site. Please post your questions and feedback for the Splunk product management team in the comments section of that post.

Recommended hardware capacity

The following requirements are accurate for a single instance installation with light to moderate use. For significant enterprise and distributed deployments, see the *Capacity Planning* Manual.

Platform	Recommended hardware capacity/configuration
Non-Windows platforms	2x six-core, 2+ GHz CPU, 12GB RAM, Redundant Array of Independent Disks (RAID) 0 or 1+0, with a 64 bit OS installed.
Windows platforms	2x six-core, 2+ GHz CPU, 12GB RAM, RAID 0 or 1+0, with a 64-bit OS installed.

RAID 0 disk configurations do not provide fault-tolerance. Confirm that a RAID 0 configuration meets your data reliability needs before deploying a Splunk Enterprise indexer on a system configured with RAID 0.

Maintain a minimum of 5GB of free hard disk space on any Splunk Enterprise instance, including forwarders, in addition to the space required for any indexes. See Estimate your storage requirements in *Capacity Planning* for a procedure on how to estimate the space you need. Failure to maintain this level of free space can degrade performance and cause operating system failure and data loss.

Hardware requirements for universal and light forwarders

The universal forwarder has its own set of hardware requirements. See Universal forwarder system requirements in the *Universal Forwarder* manual.

Supported file systems

If you run Splunk Enterprise on a file system that does not appear in this table, the software might run a startup utility named `locktest` to test the viability of the file system. If `locktest` fails, then the file system is not suitable for using with Splunk Enterprise.

Platform	File systems
Linux	ext2, ext3, ext4, btrfs, XFS, NFS 3/4
Solaris (universal forwarder only)	UFS, ZFS, VXFS, NFS 3/4
FreeBSD (universal forwarder only)	FFS, UFS, NFS 3/4, ZFS
Mac OS X	HFS, APFS, NFS 3/4
AIX	JFS, JFS2, NFS 3/4
Windows	NTFS, FAT32

Considerations regarding Network File System (NFS)

When you use Network File System (NFS) as a storage medium for Splunk indexing, consider all of the ramifications of file level storage.

Use block level storage rather than file level storage for indexing your data.

In environments with reliable, high-bandwidth, low-latency links, or with vendors that provide high-availability, clustered network storage, NFS can be an appropriate choice. However, customers who choose this strategy should work with their hardware vendor to confirm that their storage platform operates to the vendor specification in terms of both performance and data integrity.

If you use NFS, note the following:

- Do not use NFS to host hot or warm index **buckets**, because a failure in NFS can cause data loss. NFS works best with cold or frozen buckets.
- Do not use NFS to share cold or frozen index buckets amongst an indexer cluster, as this potentially creates a single point of failure.
- Splunk Enterprise does not support "soft" NFS mounts. These are mounts that cause a program attempting a file operation on the mount to report an error and continue in case of a failure.
- Only "hard" NFS mounts (mounts where the client continues to attempt to contact the server in case of a failure) are reliable with Splunk Enterprise.
- Do not disable attribute caching. If you have other applications that require disabling or reducing attribute caching, then you must provide Splunk Enterprise with a separate mount with attribute caching enabled.
- Do not use NFS mounts over a wide area network (WAN). Doing so causes performance issues and can lead to data loss.

*Considerations regarding system-wide resource limits on *nix systems*

Splunk Enterprise allocates system-wide resources like file descriptors and user processes on *nix systems for monitoring, forwarding, deploying, searching, and other things. The `ulimit` command controls access to these resources which must be set to acceptable levels for Splunk Enterprise to function properly on *nix systems.

The more tasks your Splunk Enterprise instance performs, the more resources it needs. You should increase the `ulimit` values if you start to see your instance run into problems with low resource limits. See I get errors about ulimit in splunkd.log in the *Troubleshooting Manual.*

The following table shows the system-wide resources that the software uses. It provides the minimum recommended settings for these resources for instances that are not forwarders, such as indexers, search heads, cluster masters, license masters, deployment servers, and Monitoring Consoles (MC).

System-wide Resource	ulimit invocation	Recommended min. value
Open files	`ulimit -n`	64000
User processes	`ulimit -u`	16000
Data segment size	`ulimit -d`	1073741824

On machines that run FreeBSD, you might need to increase the kernel parameters for default and maximum process stack size. The following table shows the parameters that must be present in `/boot/loader.conf` on the host.

System-wide Resource	Kernel parameter	Recommended value
Default process data size (soft limit)	`dfldsiz`	2147483648
Maximum process data size (hard limit)	`maxdsiz`	2147483648

On machines that run AIX, you might need to increase the systemwide resource limits for maximum file size (fsize) and resident memory size (rss). The following table shows the parameters that must be present in `/etc/security/limits` for the user that runs Splunk software.

System-wide Resource	ulimit invocation	Recommended value
Data segment size	`ulimit -d`	1073741824
Resident memory size	`ulimit -m`	536870912
Number of open files	`ulimit -n`	8192
File size limit	`ulimit -f`	`-1` (unlimited)

This consideration is not applicable to Windows-based systems.

Considerations regarding solid state disk drives

Solid state drives (SSDs) deliver significant performance gains over conventional hard drives for Splunk in "rare" searches - searches that request small sets of results over large swaths of data - when used in combination with bloom filters. They also deliver performance gains with concurrent searches overall.

Considerations regarding Common Internet File System (CIFS)/Server Message Block (SMB)

Splunk Enterprise supports the use of the CIFS/SMB protocol for the following purposes, on shares hosted by Windows hosts only:

- **Search head pooling** (Search head pooling is a deprecated feature.)
- Storage of cold or frozen **Index buckets**.

When you use a CIFS resource for storage, confirm that the resource has write permissions for the user that connects to the resource at both the file and share levels. If you use a third-party storage device, confirm that its implementation of CIFS is compatible with the implementation that your Splunk Enterprise instance runs as a client.

Do not index data to a mapped network drive on Windows (for example "`Y:\`" mapped to an external share.) Splunk Enterprise disables any index it encounters with a non-physical drive letter.

Considerations regarding environments that use the transparent huge pages memory management scheme

If you run Splunk Enterprise on a Unix machine that makes use of transparent huge memory pages, see Transparent huge memory pages and Splunk performance in the *Release Notes* before you attempt to install Splunk Enterprise.

This consideration is not applicable to Windows operating systems.

Further reading

See the Download Splunk Enterprise page to get the latest available version.

See the release notes for details on known and resolved issues in this release.

See Introduction to Capacity Planning for Splunk Enterprise in the *Capacity Planning* Manual for information on estimating capacity .