About the universal forwarder

About the universal forwarder

Universal forwarders stream data from your machine to a data receiver. Your receiver is usually a Splunk platform index where you store your data. You can use the universal forwarder to monitor your data in real time.

Use the universal forwarder to ensure that your data is correctly formatted before sending it to Splunk. You can also manipulate your data before it reaches the indexes or manually add the data.

Benefits of the universal forwarder

Universal forwarders provide the following benefits:

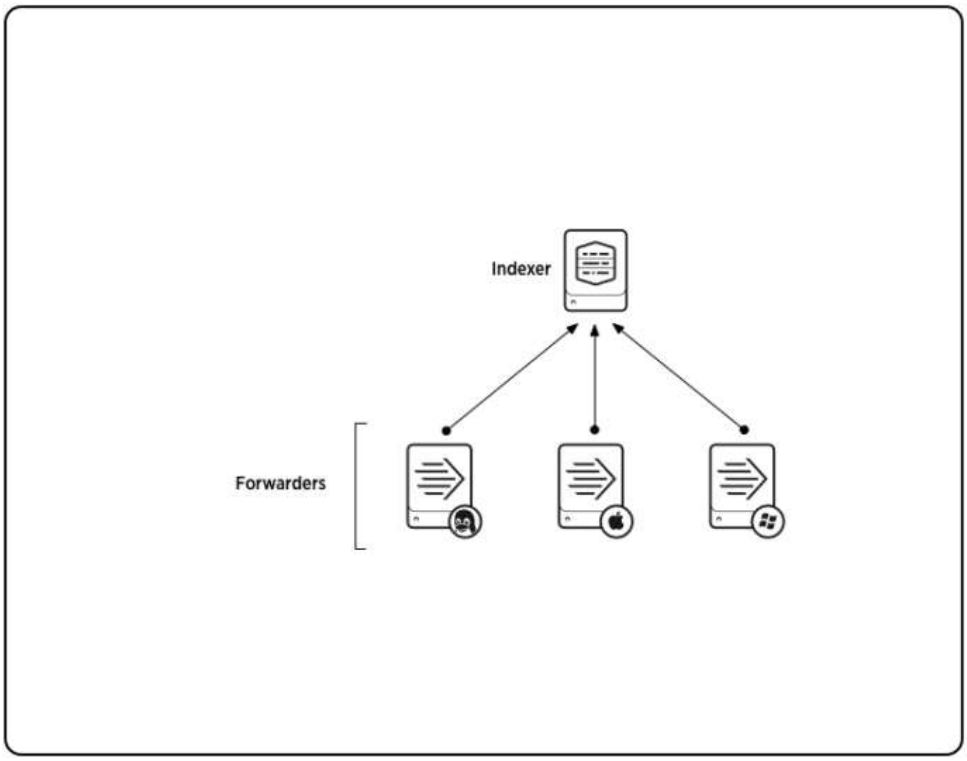
- They are highly scalable
- They use significantly less hardware resources than other Splunk products
- You can install thousands of them without impacting network performance and cost
- The universal forwarder does not have a user interface, which helps minimize resource use

In general, forwarders provide the following capabilities:

- Metadata tagging, including source, source type, and host
- Configurable buffering
- Data compression
- SSL security
- Use of any available network ports

Configuring the universal forwarder

The following diagram shows the most common configuration for the universal forwarder.



- To download the universal forwarder, visit the Splunk universal forwarder download page.
- See Deploy the universal forwarder to create your configuration.
- See Advanced configurations for the universal forwarder for examples of more advanced forwarder configurations.

Deploy the universal forwarder

Universal forwarder deployment prerequisites

Before you can deploy the universal forwarder, see the following universal forwarder prerequisites sections:

- Decide if you want to use the Splunk deployment server
- Computer hardware requirements
- Compatible operating systems

Decide if you want to use the Splunk deployment server

To personalize how data is sent to the indexer, you edit the universal forwarder's configuration files. Through the deployment server, you can edit multiple universal forwarders at once by manually editing a single file. See About deployment server and forwarder management in the *Updating Splunk Enterprise Instances* manual.

Computer hardware requirements

The universal forwarder has the following minimum processing, RAM, and disk space requirements:

Component	Required space
Processing	1.5Ghz
RAM	512MB
Free Disk Space	5GB

Compatible operating systems

For compatible operating systems, see Supported operating systems in the Splunk Enterprise *Installation manual.*

Deploy the universal forwarder

To deploy the universal forwarder:

1. Make sure you fulfill the necessary prerequisites. See Universal forwarder prerequisites.
2. Install the universal forwarder:
    - For Windows, see Install a Windows universal forwarder.
    - For *nix, see Install a *nix universal forwarder.
3. To send data to Splunk Enterprise, enable a Splunk Enterprise indexer receiver. See Enable a receiver for Splunk Enterprise.
4. To send data to Splunk Cloud Platform, you must obtain permissions to use the Splunk Cloud indexer. See Install and configure the Splunk Cloud Platform universal forwarder credentials package.
5. (Optional) To further modify how data is sent to the indexer, configure the universal forwarder. See Configure the universal forwarder using configuration files.
6. Start or restart the universal forwarder. See Start or stop the universal forwarder.

Install the universal forwarder

Install a Windows universal forwarder

Install a Windows universal forwarder using an installer or the command line. Use the installer for larger deployments and the command line for smaller deployments. Before you begin, see the universal forwarder deployment prerequisites. See Deploy the universal forwarder for a list of high-level steps to take before and after installing the universal forwarder.

You can choose from the following installation methods:

- Install from an installer
- Install from the command line

Version 9.1.0 and higher does not work with version 3 of the Splunk-to-Splunk protocol. Upgrade all of your instances if possible, but if you must use the old version of the Splunk-to-Splunk protocol, see the Troubleshooting guide. The latest forwarders will not communicate with the indexers running Splunk Enterprise 7.0 or lower.

About the least-privileged user

Do not run the universal forwarder as a local system account or domain user, as doing this would provide the user with high-risk permissions that aren't necessarily needed. When you install version 9.1 or higher of the universal forwarder, the installer creates a virtual account as a "least- privileged" user called splunkforwarder, which provides only the capabilities necessary to run the universal forwarder.

Since local user groups are not available on the domain controller, the GROUPPERFORMANCEMONITORUSERS flag is unavailable, which might affect Windows Management Instrumentation and performance monitor inputs. To mitigate input issues, when you're installing with the installer make the default account the local system on the domain controller.

If you choose a different account to run the universal forwarder during installation, the universal forwarder service varies based on your choice:

- If you choose Local System, the universal forwarder runs as the administrator of the local machine with full privileges.
- If you choose a domain account with Windows administrator privileges, the universal forwarder runs as a Windows administrator with full privileges.
- If you choose a domain account without Windows administrator privileges, you select the privileges, see https://www.microsoft.com/en-us/security/business/security-101/what-is-privileged-access-management-pam for more information.

Once you choose a non-administrator user to run the universal forwarder, this user becomes a "least privileged user" with limited permissions on Windows.

Security and performance implications for least privileged user

Least privilege mode is enabled to read any file on Windows version 9.1.0 and later. A non-admin user that cannot access some files before turning on least privilege mode might be able to access those files after enablement in the following situations:

- You upgrade the universal forwarder from an older version to a version that supports least privilege mode.
- Before upgrade, your universal forwarder runs as a non-local administrator.
- Prior to upgrade, you have inputs to monitor a directory with many files, or inputs with scripts to read many files, where users have no permission to access those files.

Since the universal forwarder is able to read far more files than before, the forwarder consumes more resources such as CPU, memory, and disk input/output. You can resolve this on Windows in one of two ways:

- During installation, you can use the PRIVILEGEBACKUP=0 installation configuration flag.
- After installation, you can remove the SeBackupPrivilege capability from the Windows local security policy. See the Microsoft documentation for more information.

Manage SePrivilegeUser permissions

On Windows, the SeSecurityPrivilege privilege is READ/WRITE by design, This means that the user with this privilege can modify and delete Security Event Logs.

If you do not want your least-privileged user to be able to modify Security Event Logs, do not grant the SeSecurityPrivilege privilege. Instead, update the EventlogReaders group with a user that has permissions to run the universal forwarder. Add the least privileged user to the Windows "EventLogReaders" group manually so that it has read only permission to collect security event logs.

If a universal forwarder is running on Domain Controllers, the "EventLogReaders" group is not available by Windows design because there is no local user or group on the domain controller. In this case, the SeSecurityPrivilege is your best option.

Install a Windows universal forwarder from an installer

To install a Windows universal forwarder from an installer:

1. Download the Splunk universal forwarder from splunk.com. Select the MSI file to start the installation.
2. On the first screen of the installer, select **Check this box to accept the License Agreement** and select whether you are installing on Splunk Enterprise or Splunk Cloud Platform.
3. Select **Next** to create an administrator account.

1. Select "Customize options" to optionally change the following:
2. In the **Destination Folder** dialog box, select **Change** and specify a different installation directory.
3. On the **Certificate Information** page, select **Next** as a best practice. Do not specify any parameters.
4. By default the universal forwarder is installed with a least-privileged user. You can use the radio buttons to change the account on which the universal forwarder runs.
5. To allow the least privileged user to enable universal forwarder features, grant all or some of the following permissions in the dialog box: Grant Windows privileges to enable universal forwarder features:

Permission	Function
SeBackupPrivilege	Select to grant the least privileged user READ ONLY permissions for files.
SeSecurityPrivilege	Select to allow the user to collect Windows security event logs. NOTE: The SeSecurityPrivilege permissions are READ/WRITE by design on Windows. This means that the user can also modify and delete Security Event Logs. To mitigate this issue, see "Manage SePrivilegeUser permissions" in this topic.
SeImpersonatePrivilege	Select to enable the capability to add the least privilege user to new Windows users/groups after the universal forwarder installation. This grants more permissions to the universal forwarder to collect data from secure sources.

Permission	Function

Grant Windows groups privileges to enable universal forwarder features:

Permission	Function
Performance Monitor Users	Select for WMI/perfmon inputs to collect performance data.

6. Create credentials for your administrator account. The default username is "Admin" and you can check **Generate a password** to automatically create a password. You can also manually create your own username and password.
7. Perform one of the following steps depending upon your requirements:
    - In the **Deployment Server** pane, enter a host name or IP address and management port for the deployment server that you want the universal forwarder to connect to and select **Next**.
    - In the **Receiving Indexer** pane, enter a host name or IP address and the receiving port for the receiving indexer that you want the universal forwarder to send data to and select **Next**.
8. Select **Install**. The installer runs and displays the **Installation Completed** dialog box. The universal forwarder automatically starts.
9. From the Windows Control Panel, confirm that the `SplunkForwarder` service is running.

Install a Windows universal forwarder from the command line

You can install the universal forwarder on a Windows machine from a command prompt or a PowerShell window.

Note the following when installing from the command line:

- When installing version 9.1.0 and higher of the universal forwarder with the command line, the default account on the domain controllers is the local system. If the USE_VIRTUAL_ACCOUNT or LOGON_USERNAME flags is enabled, then the GROUPPERFORMANCEMONITORUSERS flag must be 0, otherwise the installation fails. If you have problems on WMI/perfmon inputs, see the Troubleshooting topic.
- If you have enabled Windows to automatically run scripts, Splunk installation might fail if the autorun script fails. As a workaround, you can install the forwarder with the following command: cmd /D msiexec.exe /i.
- You can install the universal forwarder on a Windows machine from a command prompt or a PowerShell window.
- In some circumstances, the Microsoft installer might present a reboot prompt during the uninstall process. You can safely ignore the reboot request without rebooting.

Install the universal forwarder with installation flags

Review the supported command line flags table to determine the flags you need to accomplish your command line installation task.

From a command prompt or PowerShell window, run the `msiexec.exe` installer program with the appropriate flags, using the following syntax:

```
msiexec.exe /i splunkuniversalforwarder.msi [<flag>=<value>]...[<flagN>=<value>]
```

Follow the prompts on screen to complete the installation. Panes for flags that you have specified in the command line do not appear.

Install the universal forwarder silently

If your Windows machine has User Account Control (UAC) enabled, you must run a silent installation as a Windows administrator user.

Review the supported command line flags table to determine the flags you need to accomplish the command-line installation task.

From a command prompt or PowerShell window, run `msiexec.exe` with the appropriate flags and add `AGREETOLICENSE=yes /quiet` to the end of the command string, as follows:

```
msiexec.exe /i splunkuniversalforwarder.msi [<flag>=<value>]...[<flagN>=<value>] AGREETOLICENSE=yes /quiet
```

The installation completes silently and the universal forwarder starts if there is no error during installation.

Install the universal forwarder and enable verbose logging during installation

For more information on the `msiexec` logging command, see To set logging level on MS TechNet.

1. Review the supported command line flags table to determine the flags you need to accomplish your command-line installation task.
2. From a command prompt or PowerShell window, run the `msiexec.exe` installer program with the appropriate flags, using the following syntax:

   ```
   msiexec.exe /i splunkuniversalforwarder.msi [<flag>=<value>]...[<flagN>=<value>] /L*v logfile.txt
   ```
3. Follow the prompts on screen to complete the installation. Installer configuration panes for flags that you have specified in the command line do not appear.

Examples

Install the universal forwarder silently, agree to the license, and set the forwarder admin credentials to "SplunkAdmin/Ch@ng3d!"

Always create a password for the Splunk `admin` user. If you do not, then the universal forwarder can start with no defined users, which means that you cannot log in or make changes to the initial forwarder configuration.

```
msiexec.exe /i splunkforwarder_x64.msi AGREETOLICENSE=yes SPLUNKUSERNAME=SplunkAdmin
SPLUNKPASSWORD=Ch@ng3d! /quiet
```

Install the universal forwarder to run as the Local System user and request configuration from deployment server deploymentserver1

You might do this for new deployments of the forwarder.

```
msiexec.exe /i splunkuniversalforwarder_x86.msi DEPLOYMENT_SERVER="deploymentserver1:8089"
AGREETOLICENSE=Yes /quiet
```

Install the universal forwarder to run as a domain user, but do not launch it immediately

You might do this when you are preparing a machine to clone the forwarder software.

```
msiexec.exe /i splunkuniversalforwarder_x86.msi LOGON_USERNAME="AD\splunk" LOGON_PASSWORD="splunk123"
DEPLOYMENT_SERVER="deploymentserver1:8089" LAUNCHSPLUNK=0 AGREETOLICENSE=Yes /quiet
```

Install the universal forwarder, enable indexing of the Windows security and system event logs, and run the installer in silent mode

You might run this command to collect the Security and System event logs without any prompts during the installation..

```
msiexec.exe /i splunkuniversalforwarder_x86.msi RECEIVING_INDEXER="indexer1:9997" WINEVENTLOG_SEC_ENABLE=1
WINEVENTLOG_SYS_ENABLE=1 AGREETOLICENSE=Yes /quiet
```

Supported command line flags

Use command-line flags to configure your forwarder at installation time. The flags specify settings that include:

- The user the universal forwarder runs as. (When you specify a flag, confirm the user you specify has the appropriate permissions to access the content you want to forward.)
- The receiving Splunk instance to which the universal forwarder will send data.
- A deployment server for updating the forwarder configuration.
- The Windows event logs that the forwarder will index.
- Whether the universal forwarder will start automatically when the installation is completed.

The installer for the full version of Splunk Enterprise has its own set of installation flags. For information on the full Splunk Enterprise installer, see Install on Windows in the Splunk Enterprise *Installation Manual*.

The following list shows the flags available and provides a few examples of various configurations.

Flag	Purpose	Default
`AGREETOLICENSE`	Agrees to the license. You must set `AGREETOLICENSE` to `Yes` to perform a silent installation. The flag does not work when you click the MSI to start installation.	`No`
`INSTALLDIR="<directory_path>"`	Specifies the installation directory. Do not install the universal forwarder over an existing installation of full Splunk Enterprise.	`C:\Program Files\Splunk UniversalForwarder`

`LOGON_USERNAME="<domain\username>"`
 	
`LOGON_PASSWORD="<pass>"`
	Provide domain\username and password information for the user to run the `SplunkForwarder` service. Specify the domain with the username in the format: `domain\username`. If you don't include these flags, the universal forwarder installs to run as the Local System user.	n/a

`RECEIVING_INDEXER="<host:port>"`	(Optional) Specify the receiving indexer to which the universal forwarder will forward data. Enter the name (hostname or IP address) and **receiving port** of the receiver. `RECEIVING_INDEXER="<host:port>"` accepts only a single receiver. To specify multiple receivers (to implement load balancing), configure your setting through the CLI or `outputs.conf`. **Note:** If you do not specifyRECEIVING_INDEXER="" and also do not specify DEPLOYMENT_SERVER, the universal forwarder cannot determine which indexer to forward to.	n/a
`DEPLOYMENT_SERVER="<host:port>"`	Specify a **deployment server** for pushing configuration updates to the universal forwarder. Enter the deployment server name (hostname or IP address) and port. **Note:** If you do not specify `DEPLOYMENT_SERVER="<host:port>"` and also do not specify `RECEIVING_INDEXER`, the universal forwarder cannot determine the receiving indexer.	n/a

Flag	Purpose	Default
LAUNCHSPLUNK	Specify whether the universal forwarder starts when the installation finishes.	1 (yes)
SERVICESTARTTYPE	Specify whether the universal forwarder starts when the system reboots. **Note:** By setting LAUNCHSPLUNK to 0 and SERVICESTARTTYPE to auto, the universal forwarder does not start forwarding until the next system boot. This is useful when you want to clone a system image.	auto
MONITOR_PATH="<directory_path>"	Specify a file or directory to monitor.	n/a
WINEVENTLOG_APP_ENABLE= WINEVENTLOG_SEC_ENABLE WINEVENTLOG_SYS_ENABLE WINEVENTLOG_FWD_ENABLE WINEVENTLOG_SET_ENABLE	Enable these Windows event logs. • application • security • system • forwarders • setup You can specify more than one of these flags in a command.	0 (no)
PERFMON=<input_type>,<input_type>,...	Enable Performance Monitor inputs. <input_type> can be any of these: cpu memory network diskspace	n/a
ENABLEADMON	Enable Active Directory monitoring for a remote deployment.	0 (not enabled)
* CERTFILE=<c:\path\to\certfile.pem> • ROOTCACERTFILE=<c:\path\to\rootcacertfile.pem> • CERTPASSWORD=<password>	Supply SSL certificates: • Path to the cert file that contains the public/private key pair. • (Optional) Path to the file that contains the Root CA certificate for verifying CERTFILE is legitimate. • Password for private key of CERTFILE (optional). **Note:** You must set RECEIVING_INDEXER for these flags to have any effect.	n/a
CLONEPREP	Delete any instance-specific data in preparation for creating a clone of a machine. This runs the splunk clone-prep-clear-config CLI command, which removes machine-specific information from configuration files after the instance runs for the first time.	0 (do not prepare the instance for cloning.)
SET_ADMIN_USER	Specify if the user you specify is an administrator. You must set both the LOGON_USERNAME and LOGON_PASSWORD flags when you set SET_ADMIN_USER.	0
SPLUNKUSERNAME	Create a username for the Splunk administrator user. If you use the /quiet flag to specify a quiet	N/A

Flag	Purpose	Default
	installation and do not specify SPLUNKUSERNAME, then the software uses the default value of admin. You must still specify a password with the SPLUNKPASSWORD or GENRANDOMPASSWORD flags for the installation to add the credentials successfully.	
SPLUNKPASSWORD	Create a password for the Splunk administrator user. The password must meet eligibility requirements and be in plain text. If you specify a quiet installation with the /quiet flag and do not specify SPLUNKPASSWORD or the SPLUNKUSERNAME flag, and GENRANDOMPASSWORD is 0, then the universal forwarder installs without a user and you must create one by editing the user-seed.conf configuration file.	N/A
SPLUNKPASSWORD	When you set a password using the SPLUNKPASSWORD flag, you can also set password eligibility requirements for password creation and modification. The MINPASSWORDLEN flag specifies the minimum length that a password must be to meet these eligibility requirements. You cannot set SPLUNKPASSWORD to 0 or a negative integer. Any new password you create and any existing password you change must meet the new requirements after you set SPLUNKPASSWORD.	> 1
MINPASSWORDDIGITLEN	When you set a password using the SPLUNKPASSWORD flag, you can also set password eligibility requirements for password creation and modification. The MINPASSWORDDIGITLEN flag specifies the minimum number of numeral (0 through 9) characters that a password must contain to meet these eligibility requirements. It cannot be set to a negative integer. Any new password you create and any existing password you change must meet the new requirements after you set this flag.	0
MINPASSWORDLOWERCASELEN	When you set a password using the SPLUNKPASSWORD flag, you can also set password eligibility requirements for password creation and modification. The MINPASSWORDLOWERCASELEN flag specifies the minimum number of lowercase ('a' through 'z') characters that a password must contain to meet these eligibility requirements going forward. It cannot be set to a negative integer. Any new password you create and any existing password you change must meet the new requirements after you set this flag.	0
MINPASSWORDUPPERCASELEN	When you set a password using the SPLUNKPASSWORD flag, you can also set password eligibility requirements for password creation and modification. The MINPASSWORDUPPERCASELEN flag specifies the minimum number of uppercase ('A' through 'Z') characters that a password must contain to meet these eligibility requirements going forward. It cannot be set to a negative integer. Any new password you create and any existing	0

Flag	Purpose	Default
	password you change must meet the new requirements after you set this flag.	
MINPASSWORDSPECIALCHARLEN=<integer>	When you set a password using the SPLUNKPASSWORD flag, you can also set password eligibility requirements for password creation and modification. The MINPASSWORDSPECIALCHARLEN flag specifies the minimum number of special characters that a password must contain to meet these eligibility requirements going forward. It cannot be set to a negative integer. The ':' (colon) character cannot be used as a special character. Any new password you create and any existing password you change must meet the new requirements after you set this flag.	0
GENRANDOMPASSWORD	Generate a random password for the admin user and write the password to the installation log file. The installer writes the credentials to %TEMP%\splunk.log. After the installation completes, you can use the findstr utility to search that file for the word "PASSWORD". After you get the credentials, delete the installation log file, as retaining the file represents a significant security risk.	1
USE_LOCAL_SYSTEM	Install the universal forwarder as a local system	0
PRIVILEGEBACKUP	Grant the Windows privilege SeBackupPrivilege to allow file monitor inputs to read(not write) any files.	1
PRIVILEGESECURITY	Grant the Windows privilege SeSecurityPrivilege to allow WinEventLog inputs to collect security event logs.	1
PRIVILEGEIMPERSONATE	Grant the Windows privilege SeImpersonatePrivilege to allow customers grant more permissions for UF by manually adding UF user to other local user/security groups. Without this SeImpersonatePrivilege privilege, you might not be able to grant more permissions by adding the Splunk forwarder user to any Windows group. This includes the Windows builtin group Performance Monitor Users (as mentioned in the next row) to enable WMI & perfmon inputs.	1
GROUPPERFORMANCEMONITORUSERS	Add universal forwarder user to Windows Performance Monitor Users to allow WMI and perfmon inputs to collect data.	1

Troubleshooting

By default, the universal forwarder uses a local system account on the domain controller and as of 9.1, the default user is the least privileged user. Since the universal forwarder user is not added to the local admin group by default, you might experience permission issues, particularly if you have installed any custom add-ons that require additional permissions. You can manually grant the additional permissions by adding the universal forwarder user to user groups:

- Add to specific groups based on the required permission. Refer to your Microsoft Active Directory security group documentation.
- Add the user to some local or global user groups. To learn more about groups and group policies, see Prepare your Windows network to run Splunk Enterprise as a network or domain user.

Install a *nix universal forwarder

The following tasks describe how to install the universal forwarder software on a *nix host, such as Linux, Solaris, or Mac OS X. These tasks describe how to install directly onto the host, rather than use a deployment tool. This type of deployment best suits these needs:

- Small deployments.
- Proof-of-concept test deployments.
- System image or virtual machine for eventual cloning.

The universal forwarder installation packages are available for download from splunk.com.

On *nix operating systems, the installation comes as a tar file or an installation package (.rpm, .deb, .pkg, etc.)

A tar file contains only the files needed to install and run the universal forwarder and can be installed wherever you have permissions. Installation packages contain logic that checks for software dependencies and install in a predetermined place, depending on your operating system.

To install the universal forwarder on a *nix host, follow the directions later in this topic for your specific OS.

- Install on Linux
- Install on Solaris
- Install on Mac OS X
- Install on FreeBSD
- Install on AIX

Version 9.1.0 deprecates version 3 of the Splunk-to-Splunk protocol. You should upgrade all of your instances if possible, but if you do want to use the old version of the Splunk-to-Splunk protocol, see [https://docs.splunk.com/Documentation/Forwarder/9.4.0/Forwarder/Troubleshoottheuniversalforwarder Troubleshoot the universal forwarder] to learn how to enable that behaviour. With this deprecation introduced in 9.1.0, the latest forwarders will not be able to talk to the indexers running Splunk 7.0 or earlier.

Default installation location

The universal forwarder installs by default in the `/opt/splunkforwarder` directory. The default installation directory for Splunk Enterprise is `/opt/splunk`.

About installing with tar files

When you install the universal forwarder using a tar file:

- Some non-GNU versions of `tar` might not have the `-C` argument available. In this case, to install in a specific directory, you can either `cd` to the directory where you want to install the forwarder or place the tar file in that directory before you run the `tar` command.
- The universal forwarder does not create the `splunk` user on the machine. If you want the forwarder to run as a specific user, you must create the user manually before you install.
- Confirm that the disk partition has enough space to hold the uncompressed volume of the data you plan to index.

Do not install the universal forwarder over an existing installation of Splunk Enterprise.

Install the universal forwarder on Linux

About the splunkfwd user

Running the universal forwarder as ROOT or SUDO is not a security best practice, as it provides a lot of high-risk permissions that are not necessary to run the universal forwarder. To better secure your configuration, when you install the forwarder on Linux, the universal forwarder installer creates a non-root user called splunkfwd. splunkfwd is a new "least privileged" user that provides only the capabilities necessary to run the universal forwarder.

To learn more about how to add, enable, disable, and troubleshoot splunkfwd users, see Manage a Linux least privileged user.

For the universal forwarder to create a splunkfwd user at installation, your system must meet the following criteria:

- One or more universal forwarders; least privileged mode does not run on other systems or applications.
- `systemd` version 219 or greater.
- Linux x86_64, ARM, ARM64

Least privileged (splunkfwd) user security and performance implications

Least privilege mode is enabled to read any file permission on Linux version 9.0.0 and later.

A non-root or non-admin user that could not access some files before upgrade to least privilege user, may be able to access those files after upgrade in the following situations:

- You upgrade the universal forwarder from old versions to a least privilege version.
- Before upgrade, your universal forwarder is running as non-root or non-local admin.
- Prior to upgrade, you have inputs to monitor a directory with many files, or inputs with scripts to read many files, where users have no permission to access those files

In addition to security issues, this can lead to potential performance issues. Since the universal forwarder is able to read far more files than before, more resources such as CPU, memory, and disk input/output are consumed.

To avoid this, you can disable the "read any file" capability manually. To do this, edit the unit file to remove the CAP_DAC_READ_SEARCH capability.

Install on Linux

As of Splunk 9.1, the universal forwarder installs a new least privileged user called splunkfwd. This means that the user name for Splunk Enterprise, "Splunk", and your universal forwarder user name, "splunkfwd", will be different. We recommend that you implement the splunkfwd user, however, if your system requires that your Splunk Enterprise and universal forwarder names be identical, see Manage a Linux least-privileged user in this manual.

1. Login as ROOT to the machine on which you want to install the universal forwarder.
2. Create the Splunk user and group.
   ```
   useradd -m splunkfwd
   groupadd splunkfwd
   ```
3. Install the Splunk software, as described in the installation instructions for your platform in Installation instructions. Create the `$SPLUNK_HOME` directory wherever desired.
   ```
   export SPLUNK_HOME="/opt/splunkforwarder"
   mkdir $SPLUNK_HOME
   ```
4. Make sure the `splunkforwarder` package is present in `$SPLUNK_HOME`:

For a tar package:	`tar xvzf splunkforwarder_package_name.tgz`
For an rpm package:	♦ If necessary, change permissions on the file: `chmod 644 splunkforwarder_package_name.rpm` ♦ Install in the default directory `opt/splunkforwarder`: `rpm -i splunkforwarder_package_name.rpm`
For a .deb package:	`dpkg -i splunkforwarder_package_name.deb`

5. Run the `chown` command to change the ownership of the splunk directory and everything under it to the user that will run the software.
   ```
   chown -R splunkfwd:splunkfwd $SPLUNK_HOME
   ```
   If you change users, you must run this command again

   .

   If the `chown` binary on your system does not support changing group ownership for files, you can use the `chgrp` command instead. See the Man pages on your system for additional information on changing group ownership.
6. Switch to ROOT or SUDO and run
   ```
   sudo $SPLUNK_HOME/bin/splunk start
   ```
   Or

   ```
   sudo $SPLUNK_HOME/bin/splunk start --accept-license
   ```

For post-installation configuration and credential creation, see the Configure the universal forwarder chapter in this manual.

Install the universal forwarder on Solaris

The universal forwarder is available for Solaris as a tar file or a PKG file.

To install a universal forwarder on a Sun SPARC system that runs Solaris, confirm that you have patch level SUNW_1.22.7 or later of the C library (libc.so.1). If you do not have this library, the universal forwarder cannot run.

Once you have installed the forwarder, see Configure the universal forwarder chapter in this manual to configure your forwarder and create credentials.

Install from a tar file

Use the `tar` command to install the forwarder.

- To install into the folder `/opt/splunkforwarder`:

1. Uncompress the tar file. `uncompress splunkforwarder-<version-os-arch>.tar.Z`
2. Extract the tar file. `tar xvf splunkforwarder-<version-os-arch>.tar -C /opt`

- To install into the current working directory under the `splunkforwarder` folder:

1. Uncompress the tar file. `uncompress splunkforwarder-<version-os-arch>.tar.Z`
2. Extract the tar file. `tar xvf splunkforwarder-<version-os-arch>.tar`

Once you have installed the forwarder, see Configure the universal forwarder chapter in this manual to configure your forwarder and create credentials.

Install the universal forwarder on Mac OS X

The universal forwarder is available for Mac OS X as a tar file or a DMG package.

Install the universal forwarder from the Finder

1. Navigate to the folder or directory where the installer is located.
2. Double-click the DMG file.
   A Finder window that contains the `splunkforwarder.pkg` opens.
3. Double-click the `Install Splunk Universal Forwarder` icon to start the installer.
4. The **Introduction** panel lists version and copyright information. Click **Continue**.
5. The **License** panel lists shows the software license agreement. Click **Continue**.
6. You are asked to agree to the terms of the software license agreement. Click **Agree**.
7. In the **Installation Type** panel, click **Install**. This installs the universal forwarder in the default directory `/Applications/SplunkForwarder`.
8. You are prompted to type the password that you use to login to your computer.
9. When the installation completes, a popup informs you that an initialization must be performed. Click **OK**.
10. A terminal window appears and you are prompted to specify a username and password to use with the universal forwarder.

    The password must be at least eight characters in length. The cursor will not advance as you type. Make note of your username and password. You will use these credentials to authenticate when using CLI commands on the forwarder.
11. A popup appears asking what you would like to do. Click **Start Splunk**.
12. Close the **Install Splunk Forwarder** window.

    The installer places a shortcut on the desktop so that you can start or stop the universal forwarder from your desktop at any time.

Once you have installed the forwarder, see Configure the universal forwarder chapter in this manual to configure your forwarder and create credentials.

Install from a tar file

Use the `tar` command to install the forwarder.

- To install the forwarder into the folder `/Applications/splunkforwarder`, run:

```
tar xvzf splunkforwarder.tgz -C /Applications
```

- To install the forwarder into the current working directory under the `splunkforwarder` folder, run:

```
tar xvzf splunkforwarder.tgz
```

Once you have installed the forwarder, see Configure the universal forwarder chapter in this manual to configure your forwarder and create credentials.

Install the universal forwarder on FreeBSD

The universal forwarder is available for FreeBSD as a .txz file package.

Prerequisites

FreeBSD best practices maintain a small root filesystem. Verify that the root filesystem has sufficient free space for the universal forwarder installation.

The package installs the forwarder in the default directory, `/opt/splunkforwarder`. If `/opt` does not exist, you might receive an error message.

Once you have installed the forwarder, see Configure the universal forwarder chapter in this manual to configure your forwarder and create credentials.

Basic FreeBSD installation

1. Download the FreeBSD package file from splunk.com (login required.)
2. Install the universal forwarder on FreeBSD using the `pkg` command:
   `pkg install splunkforwarder-<version>-freebsd-<version>-amd64.txz`
3. Start the universal forwarder service and create a local user and password. See Configure the universal forwarder chapter in this manual to configure your forwarder and create credentials.

After installing the forwarder on FreeBSD

These instructions ensure that the forwarder functions properly on FreeBSD. If your host has less than 2 GB of memory, reduce the `kern.maxdsiz` and `kern.dfldsiz` values accordingly.

1. Add the following to `/boot/loader.conf`
   ```
   kern.maxdsiz="2147483648" # 2GB
   kern.dfldsiz="2147483648" # 2GB
   machdep.hlt_cpus=0
   ```
2. Add the following to `/etc/sysctl.conf`:
   ```
   vm.max_proc_mmap=2147483647
   ```
3. Restart the FreeBSD host for the changes to effect.

Once you have installed the forwarder, see Configure the universal forwarder chapter in this manual to configure your forwarder and create credentials.

Install the universal forwarder on AIX

The universal forwarder is available for AIX as a tar file. The default installation directory is `/opt/splunkforwarder`.

Do not use the AIX version of `tar` to unarchive the file. Use the GNU version instead. The GNU version comes with the AIX Toolbox for Linux Applications package that comes with a base AIX installation. If your AIX does not come with this package installed, you can download it from IBM. See IBM AIX Toolbox download information.

1. Confirm that the user that the universal forwarder runs as has permission to read the `/dev/random` and `/dev/urandom` devices.
2. Expand the tar file into an appropriate directory:
   `tar xvzf splunkforwarder-<...>.tgz`

Once you have installed the forwarder, see Configure the universal forwarder chapter in this manual to configure your forwarder and create credentials.

Enable the universal forwarder to automatically start at boot time

The AIX version of the universal forwarder does not register itself to auto-start on reboot. You can register it by running the following command from the `$SPLUNK_HOME/bin` directory at a prompt:

```
./splunk enable boot-start
```

This command invokes the following system commands to register the forwarder in the System Resource Controller (SRC):

```
mkssys -G splunk -s splunkd -p <path to splunkd> -u <splunk user> -a _internal_exec_splunkd -S -n 2 -f 9
```

When you enable automatic boot start, the SRC handles the run state of the forwarder. This means that you must use a different command to start and stop the forwarder manually:

- `/usr/bin/startsrc -s splunkd` to start the forwarder.
- `/usr/bin/stopsrc -s splunkd` to stop the forwarder.

If you attempt to start and stop the forwarder using the `./splunk [start|stop]` method from the `$SPLUNK_HOME` directory, the SRC catches the attempt and the forwarder displays the following message:

```
Splunk boot-start is enabled. Please use /usr/bin/[startsrc|stopsrc] -s splunkd to [start|stop] Splunk.
```

To prevent this message from occurring and restore the ability to start and stop the forwarder from the `$SPLUNK_HOME` directory, disable boot start:

```
./splunk disable boot-start
```

- For more information on the `mkssys` command line arguments, see Mkssys command on the IBM pSeries and AIX Information Center website.
- For more information on the SRC, see System resource controller on the IBM Knowledge Center website.

Next steps

Once you have installed the forwarder, see Configure the universal forwarder chapter in this manual to configure your forwarder and create credentials.

Upgrade or uninstall the universal forwarder

Upgrade the universal forwarder

Before upgrading, see About upgrading READ THIS FIRST in the Splunk Enterprise *Installation Manual* for information about any changes that affect the universal forwarder.

See the following instructions to upgrade the Windows universal forwarder or the *nix universal forwarder:

- Upgrade the Windows universal forwarder
- Upgrade the *nix universal forwarder

As of version 9.0, the configuration change tracker is enabled by default. To track your indexer configuration logs using this functionality, either upgrade your indexers to 9.0 or enable index(_configtracker) for your indexers.

Upgrade the Windows universal forwarder

When you upgrade a universal forwarder, the installer updates the software without changing its configuration. You must make any necessary configuration changes after you complete the upgrade. A deployment server can assist in the configuration update process.

There are several forwarder upgrade scenarios:

- You can upgrade a single forwarder with the GUI installer
- You can upgrade a single forwarder with the command line installer
- You can perform a remote upgrade of a group of forwarders (good for deployments of any size)

As best practice when upgrading a Windows universal forwarder on Splunk Cloud Platform, run the most recent forwarder version, even if the forwarder is a higher version number than your Splunk Cloud Platform environment.

When you upgrade on Windows, make sure to stop Splunk. If Splunk is running during upgrade, the upgrade fails with error "ERROR: In order to migrate, Splunkd must not be running." "

Confirm that an upgrade is necessary

Begin by checking the forwarder compatibility. To determine if you need to upgrade your forwarder version to remain in support or use specific features, see the appropriate topic for your deployment:

- Splunk Cloud Platform: Supported forwarder versions in the *Splunk Cloud Platform Service Description*.
- Splunk Enterprise: Compatibility between forwarders and Splunk Enterprise indexers in the *Splunk Products Version Compatibility Matrix*.

If your forwarders are on the same major release of Splunk software as the indexers, they are compatible. However, you might need an upgrade to a different minor release due to a technical issue in a specific feature. Before upgrading forwarders, review the Known Issues and Fixed Issues.

You must perform any platform architecture changes manually

Use the following task to upgrade in the following scenarios:

- To upgrade a 32-bit version of the universal forwarder with a 64-bit universal forwarder installer.
- To upgrade to 9.1 or later so that you can use a least-privileged user on your forwarder.

1. Stop splunkd if it is running.
2. Back up your configurations, including any apps or add-ons (in `%SPLUNK_HOME%\etc\apps`). Also back up the checkpoint files located in `%SPLUNK_HOME%\var\lib\splunk\modinputs`.
3. Uninstall the existing 32-bit forwarder, as described in Uninstall the universal forwarder.
4. Install the 64-bit or 9.1 forwarder, as described in Install the universal forwarder from an installer.
5. Restore apps, configurations and checkpoints by copying them to the appropriate directories:
   `%SPLUNK_HOME%\etc\system\local` for configuration files.
   `%SPLUNK_HOME%\etc\apps` for apps and add-ons.
   `%SPLUNK_HOME%\var\lib\splunk\modinputs` for checkpoint files.

Back your files up

Before you perform an upgrade, back up configuration files. See Back up configuration information in the Splunk Enterprise *Admin* manual.

There is no means of downgrading to a previous version. If you need to revert to an older forwarder release, uninstall the current version and reinstall the older release.

Upgrade a single forwarder using the GUI installer

You can upgrade a single forwarder with the GUI installer. The installer stops the forwarder as part of the upgrade process.

1. Stop splunkd if it is running.
2. Download the new MSI file from the universal forwarder download page.
3. Double-click the MSI file. The installer displays the "Accept license agreement" panel.
4. Accept the license agreement and click "Install." The installer upgrades the forwarder, retains the existing configuration, and starts automatically when you complete the installation.

The installer puts a log of upgrade changes in the `%TEMP%` directory (This is usually the `C:\TEMP` directory but can be different based on your Windows machine configuration.) It also reports any errors in the Application Event Log.

Upgrade a single forwarder using the command line

You can upgrade a single forwarder by running the command line installer.

You cannot make configuration changes during an upgrade. The installer ignores any command line flags that you specify except for the `AGREETOLICENSE` flag.

1. Stop splunkd if it is running.
2. Download the new MSI file from the Splunk universal forwarder download page.
3. Run `msiexec.exe` to Install the universal forwarder from the command line.
   - For 32-bit platforms, use `splunkuniversalforwarder-<...>-x86-release.msi`.

```
msiexec.exe /i splunkuniversalforwarder-<...>-x86-release.msi [AGREETOLICENSE=Yes /quiet]
```

- For 64-bit platforms, use `splunkuniversalforwarder-<...>-x64-release.msi`.

```
msiexec.exe /i splunkuniversalforwarder-<...>-x64-release.msi [AGREETOLICENSE=Yes /quiet]
```

The value of `<...>` varies according to the particular release, for example, `splunkuniversalforwarder-6.3.0-aa7d4b1ccb80-x64-release.msi`.

4. Wait for the upgrade to complete. The forwarder starts automatically when you complete the installation.

The installer puts a log of upgrade changes in the `%TEMP%` directory. It also reports any errors in the Application Event Log.

Perform a remote upgrade of one or more forwarders

You can use a deployment tool such as Group Policy or System Center Configuration Manager to distribute the forwarder software among a group of forwarders in your environment. You might want to test the upgrade locally on one machine before performing a remote upgrade across all your forwarders.

The Splunk Enterprise deployment server cannot distribute the universal forwarder, only its apps and configurations. Do not attempt to use deployment server to distribute universal forwarders.

1. Download the new MSI file from the Splunk universal forwarder download page.
2. Load the MSI into your deployment tool. In the tool, specify the command line as follows.

```
msiexec.exe /i splunkuniversalforwarder-<...>.msi AGREETOLICENSE=Yes /quiet
```

3. Start the deployment with your deployment tool.
4. Use the deployment monitor to verify that the universal forwarders function properly.

Upgrade the nix universal forwarder

You have several scenarios for upgrading a *nix universal forwarder:

- Upgrade a single forwarder manually.
- Perform a remote upgrade of a group of forwarders. (Use this option for deployments of any size)

When you upgrade, the RPM/DEB package installer retrieves the file owner of SPLUNK_HOME/etc/myinstall/splunkd.xml. If a previous user exists, the RPM/DEB package installer will not create a splunkfwd user and instead will reuse the existing user. If you wish to create a least privileged user, that is, the splunkfwd user, you must remove the existing user first.

As best practice when upgrading a *nix universal forwarder on Splunk Cloud Platform, run the most recent forwarder version, even if the forwarder is a higher version number than your Splunk Cloud Platform environment.

Confirm that an upgrade is necessary

Begin by checking the forwarder compatibility. To determine if you need to upgrade your forwarder version to remain in support or use specific features, see the appropriate topic for your deployment:

- Splunk Cloud Platform: Supported forwarder versions in the *Splunk Cloud Platform Service Description*
- Splunk Enterprise: Compatibility between forwarders and Splunk Enterprise indexers in the *Splunk Products Version Compatibility Matrix*.

If your forwarders are on the same major release of Splunk software as the indexers, they are compatible. However, you might need an upgrade to a different minor release due to a technical issue in a specific feature. Before upgrading

forwarders, review the Known Issues and Fixed Issues.

Back your files up

Before you perform the upgrade, back up your configuration files. See Back up configuration information in the Splunk Enterprise *Admin Manual*.

If you need to revert to an older forwarder release, uninstall the upgrade and reinstall the older release.

Confirm that you do not have scripts in place to auto-start forwarders. If you do, disable such scripts for now. You can re-enable them later, after the upgrade.

How upgrading works

After you perform the installation of the new forwarder, you must restart it for any changes to take effect. You can run the migration preview utility at that time to see what will change before the files are updated. If you choose to view the changes before proceeding, the forwarder writes the proposed changes to `$SPLUNK_HOME/var/log/splunk/migration.log.<timestamp>`

Upgrade a single forwarder

There are several packages that you can use to upgrade a universal forwarder. Tar files and pre-built package such as an .rpm, .deb, or .dmg file are available depending on the operating system.

If you use a .tar file to upgrade a forwarder, expand it into the same directory with the same ownership as the existing universal forwarder instance. This overwrites and replaces matching files but does not remove unique files.

If you use an RPM file, use the RPM package manager (`rpm -U <splunk_package_name>.rpm`) from a shell prompt to perform the upgrade.

If you use a .dmg file (on MacOS), double-click it and follow the instructions. After the installation starts, specify the same installation directory as your existing installation.

On hosts that run AIX, do not use the AIX version of `tar` to unarchive a tar file during an upgrade. Use the GNU version of `tar` instead. This version comes with the AIX Toolbox for Linux Applications package that comes with a base AIX installation. If your AIX does not come with this package installed, you can download it from IBM. See IBM AIX Toolbox download information.

1. Stop the forwarder.

```
$SPLUNK_HOME/bin/splunk stop
```

2. Install the universal forwarder package directly over the existing deployment.

As best practice when upgrading a *nix universal forwarder on Splunk Cloud Platform, run the most recent forwarder version, even if the forwarder is a higher version number than your Splunk Cloud Platform environment.

3. Start the forwarder again.

```
$SPLUNK_HOME/bin/splunk start
```

The forwarder displays the following:

```
This appears to be an upgrade of Splunk.
--------------------------------------------------------------------------------
Splunk has detected an older version of Splunk installed on this machine. To
finish upgrading to the new version, Splunk's installer will automatically
update and alter your current configuration files. Deprecated configuration
files will be renamed with a .deprecated extension.
You can choose to preview the changes that will be made to your configuration
files before proceeding with the migration and upgrade:
If you want to migrate and upgrade without previewing the changes that will be
made to your existing configuration files, choose 'y'.
If you want to see what changes will be made before you proceed with the
upgrade, choose 'n'.
Perform migration and upgrade without previewing configuration changes? [y/n]
```

4. Choose whether you want to run the migration preview script to see what changes will be made to your existing configuration files, or proceed with the migration and upgrade right away. If you choose to view the expected changes, the script provides a list of those changes.

5. Once you have reviewed these changes and are ready to proceed with migration and upgrade, run `$SPLUNK_HOME/bin/splunk start` again.

You can complete the last three steps in one line.

- To accept the license and view the expected changes (answer 'n') before continuing the upgrade:

```
$SPLUNK_HOME/bin/splunk start --accept-license --answer-no
```

- For Linux upgrade you must use sudo to upgrade as the root user.

```
sudo $SPLUNK_HOME/bin/splunk start --accept-license --answer-no
```

- To accept the license and begin the upgrade without viewing the changes (answer 'y'):

```
$SPLUNK_HOME/bin/splunk start --accept-license --answer-yes
```

Perform a remote upgrade

To perform a remote upgrade, first perform an upgrade on a test machine. Then, create a script to automate the upgrade on remote machines. You can use the following script, but you might need to modify the script to meet the needs of an upgrade.

1. Upgrade the universal forwarder on a test machine, as described in Install a nix universal forwarder.

2. Create a script wrapper for the upgrade commands.

3. Run the script on representative target machines to verify that it works with all required shells.

4. Execute the script against the desired set of hosts.

```
#!/bin/sh

# This script provides an example of how to deploy the universal forwarder
# to many remote hosts via ssh and common Unix commands.
#
# Note that this script will only work unattended if you have SSH host keys
# setup & unlocked.
# To learn more about this subject, do a web search for "openssh key management".


# ----------- Adjust the variables below -----------

# Populate this file with a list of hosts that this script should install to,
# with one host per line.  You may use hostnames or IP addresses, as
# applicable.  You can also specify a user to login as, for example, "foo@host".
#
# Example file contents:
# server1
# server2.foo.lan
# you@server3
# 10.2.3.4

HOSTS_FILE="/path/to/splunk.install.list"

# This is the path to the tar file that you wish to push out.  You may
# wish to make this a symlink to a versioned tar file, so as to minimize
# updates to this script in the future.

SPLUNK_FILE="/path/to/splunk-latest.tar.gz"

# This is where the tar file will be stored on the remote host during
# installation.  The file will be removed after installation.  You normally will
# not need to set this variable, as $NEW_PARENT will be used by default.
#
# SCRATCH_DIR="/home/your_dir/temp"

# The location in which to unpack the new tar file on the destination
# host.  This can be the same parent dir as for your existing
# installation (if any).  This directory will be created at runtime, if it does
# not exist.

NEW_PARENT="/opt"

# After installation, the forwarder will become a deployment client of this
# host.  Specify the host and management (not web) port of the deployment server
# that will be managing these forwarder instances.  If you do not wish to use
# a deployment server, you may leave this unset.
#
# DEPLOY_SERV="splunkDeployMaster:8089"

# A directory on the current host in which the output of each installation
# attempt will be logged.  This directory need not exist, but the user running
# the script must be able to create it.  The output will be stored as
# $LOG_DIR/<[user@]destination host>.  If installation on a host fails, a
# corresponding file will also be created, as
# $LOG_DIR/<[user@]destination host>.failed.

LOG_DIR="/tmp/splunkua.install"

# For conversion from normal Splunk Enterprise installs to the universal forwarder:
# After installation, records of progress in indexing files (monitor)
```

```
# and filesystem change events (fschange) can be imported from an existing
# Splunk Enterprise (non-forwarder) installation.  Specify the path to that installation here.
# If there is no prior Splunk Enterprise instance, you may leave this variable empty ("").
#
# NOTE: THIS SCRIPT WILL STOP THE SPLUNK ENTERPRISE INSTANCE SPECIFIED HERE.
#
# OLD_SPLUNK="/opt/splunk"

# If you use a non-standard SSH port on the remote hosts, you must set this.
# SSH_PORT=1234

# You must remove this line, or the script will refuse to run.  This is to
# ensure that all of the above has been read and set. :)

UNCONFIGURED=1

# ----------- End of user adjustable settings -----------


# helpers.

faillog() {
  echo "$1" >&2
}

fail() {
  faillog "ERROR: $@"
  exit 1
}

# error checks.

test "$UNCONFIGURED" -eq 1 && \
  fail "This script has not been configured.  Please see the notes in the script."
test -z "$HOSTS_FILE" && \
  fail "No hosts configured!  Please populate HOSTS_FILE."
test -z "$NEW_PARENT" && \
  fail "No installation destination provided!  Please set NEW_PARENT."
test -z "$SPLUNK_FILE" && \
  fail "No splunk package path provided!  Please populate SPLUNK_FILE."
if [ ! -d "$LOG_DIR" ]; then
  mkdir -p "$LOG_DIR" || fail "Cannot create log dir at \"$LOG_DIR\"!"
fi

# some setup.

if [ -z "$SCRATCH_DIR" ]; then
  SCRATCH_DIR="$NEW_PARENT"
fi
if [ -n "$SSH_PORT" ]; then
  SSH_PORT_ARG="-p${SSH_PORT}"
  SCP_PORT_ARG="-P${SSH_PORT}"
fi

NEW_INSTANCE="$NEW_PARENT/splunkforwarder" # this would need to be edited for non-UA...
DEST_FILE="${SCRATCH_DIR}/splunk.tar.gz"

#
#
# create script to run remotely.
#
#
```

```
REMOTE_SCRIPT="
  fail() {
    echo ERROR: \"\$@\" >&2
    test -f \"$DEST_FILE\" && rm -f \"$DEST_FILE\"
    exit 1
  }
"

###   try untarring tar file.
REMOTE_SCRIPT="$REMOTE_SCRIPT
  (cd \"$NEW_PARENT\" && tar -zxf \"$DEST_FILE\") || fail \"could not untar /$DEST_FILE to $NEW_PARENT.\"
"

###   setup seed file to migrate input records from old instance, and stop old instance.
if [ -n "$OLD_SPLUNK" ]; then
  REMOTE_SCRIPT="$REMOTE_SCRIPT
    echo \"$OLD_SPLUNK\" > \"$NEW_INSTANCE/old_splunk.seed\" || fail \"could not create seed file.\"
    \"$OLD_SPLUNK/bin/splunk\" stop || fail \"could not stop existing splunk.\"
  "
fi

###   setup deployment client if requested.
if [ -n "$DEPLOY_SERV" ]; then
  REMOTE_SCRIPT="$REMOTE_SCRIPT
    \"$NEW_INSTANCE/bin/splunk\" set deploy-poll \"$DEPLOY_SERV\" --accept-license --answer-yes \
      --auto-ports --no-prompt || fail \"could not setup deployment client\"
  "
fi

###   start new instance.
REMOTE_SCRIPT="$REMOTE_SCRIPT
  \"$NEW_INSTANCE/bin/splunk\" start --accept-license --answer-yes --auto-ports --no-prompt || \
    fail \"could not start new splunk instance!\"
"

###   remove downloaded file.
REMOTE_SCRIPT="$REMOTE_SCRIPT
  rm -f "$DEST_FILE" || fail \"could not delete downloaded file $DEST_FILE!\"
"

#
#
# end of remote script.
#
#

exec 5>&1 # save stdout.
exec 6>&2 # save stderr.

echo "In 5 seconds, will copy install file and run the following script on each"
echo "remote host:"
echo
echo "====================="
echo "$REMOTE_SCRIPT"
echo "====================="
echo
echo "Press Ctrl-C to cancel..."
test -z "$MORE_FASTER" && sleep 5
echo "Starting."

# main loop.  install on each host.
```

```
for DST in `cat "$HOSTS_FILE"`; do
  if [ -z "$DST" ]; then
    continue;
  fi

  LOG="$LOG_DIR/$DST"
  FAILLOG="${LOG}.failed"
  echo "Installing on host $DST, logging to $LOG."

  # redirect stdout/stderr to logfile.
  exec 1> "$LOG"
  exec 2> "$LOG"

  if ! ssh $SSH_PORT_ARG "$DST" \
      "if [ ! -d \"$NEW_PARENT\" ]; then mkdir -p \"$NEW_PARENT\"; fi"; then
    touch "$FAILLOG"
    # restore stdout/stderr.
    exec 1>&5
    exec 2>&6
    continue
  fi

  # copy tar file to remote host.
  if ! scp $SCP_PORT_ARG "$SPLUNK_FILE" "${DST}:${DEST_FILE}"; then
    touch "$FAILLOG"
    # restore stdout/stderr.
    exec 1>&5
    exec 2>&6
    continue
  fi

  # run script on remote host and log appropriately.
  if ! ssh $SSH_PORT_ARG "$DST" "$REMOTE_SCRIPT"; then
    touch "$FAILLOG" # remote script failed.
  else
    test -e "$FAILLOG" && rm -f "$FAILLOG" # cleanup any past attempt log.
  fi

  # restore stdout/stderr.
  exec 1>&5
  exec 2>&6

  if [ -e "$FAILLOG" ]; then
    echo "    FAILED  "
  else
    echo "      SUCCEEDED"
  fi
done

FAIL_COUNT=`ls "${LOG_DIR}" | grep -c '\.failed$'`
if [ "$FAIL_COUNT" -gt 0 ]; then
  echo "There were $FAIL_COUNT remote installation failures."
  echo "  ( see ${LOG_DIR}/*.failed )"
else
  echo
  echo "Done."
fi

# Voila.
```

Uninstall the universal forwarder

Before you uninstall the forwarder, stop it and remove it from any system start-up scripts first. Run these commands from a shell or command prompt or Terminal or PowerShell window.

1. If you configured the universal forwarder to start on boot, remove it from your boot scripts before you uninstall.

Unix	Windows
`cd $SPLUNK_HOME` `./splunk disable boot-start`	`cd %SPLUNK_HOME%` `.\splunk disable boot-start`

2. Stop the forwarder.

Unix	Windows
`./splunk stop`	`.\splunk stop`

Uninstall the universal forwarder with your package management utilities

Use your local package management commands to uninstall the universal forwarder. Files that were not originally installed by the package will be retained. These include configuration and index files within the installation directory.

In these instructions, `$SPLUNK_HOME` refers to the universal forwarder installation directory. On Windows, this is `C:\Program Files\SplunkUniversalForwarder` by default. For most Unix platforms, the default installation directory is `/opt/splunkforwarder`. On Mac OS X, it is `/Applications/splunkforwarder`.

RedHat Linux

- Run the following command to uninstall the forwarder.

```
rpm -e splunk_product_name
```

Debian Linux

1. Run the following command to uninstall the forwarder.

```
dpkg -r splunkforwarder
```

2. (Optional) Run the following command to purge all universal forwarder files, including configuration files.

```
dpkg -P splunkforwarder
```

FreeBSD

1. Run the following command to uninstall the forwarder.

```
pkg_delete splunkforwarder
```

2. (Optional) Run the following command to uninstall the forwarder from a different location.

```
pkg_delete -p <location> splunkforwarder
```

Solaris

- Run the following command to uninstall the forwarder.

```
pkgrm splunkforwarder
```

Uninstall the universal forwarder on *nix systems manually

If you are not able to use package management commands, or you run HP-UX, use these instructions to uninstall the software manually.

1. Stop the forwarder.

   ```
   $SPLUNK_HOME/bin/splunk stop
   ```
2. Find any lingering processes that contain "splunk" in their name and use the `kill` to end them.

Linux and Solaris	FreeBSD and Mac OS X
`kill -9 `ps -ef | grep splunk | grep -v grep | awk '{print $2;}'``	`kill -9 `ps ax | grep splunk | grep -v grep | awk '{print $1;}'``

3. Remove the universal forwarder installation directory, `$SPLUNK_HOME`.

   ```
   rm -rf /opt/splunkforwarder
   ```
4. (Optional) On Mac OS X, use the Finder to remove the installation directory by dragging the folder into the Trash.
5. (Optional) Delete any `splunk` users and groups that you created, if they exist.

Linux, Solaris, and FreeBSD	Mac OS X
`userdel splunk` `groupdel splunk`	Use the **System Preferences > Accounts** control panel to manage users and groups.

Note: Where the service is configured to run on *nix under systemd, use the following commands:

```
systemctl stop splunkforwarder

systemctl disable splunkforwarder
```

Uninstall the Windows universal forwarder

Under some circumstances, the Microsoft installer might present a reboot prompt during the uninstall process. You can safely ignore this request without rebooting.

1. Stop the `SplunkForwarder` service. You have several options:
   Use a PowerShell or command prompt to stop the forwarder.
   ```
   cd  %SPLUNK_HOME%\bin
   .\splunk stop
   ```

   Use a PowerShell or command prompt to stop the `SplunkForwarder` service.

   `NET STOP SplunkForwarder` Use the Services MMC snap-in (**Start > Administrative Tools > Services**) to stop the `SplunkForwarder` service.
2. Open the Control Panel and use the **Add or Remove Programs** application to start the uninstallation process. On Windows 7, 8, 10, Server 2008, and Server 2012, that option is available under **Programs and Features.**
3. Follow the installer prompts to remove the forwarder from the Windows host.

Uninstall the Windows universal forwarder from the command line

You can also use the Services MMC snap-in (**Start > Administrative Tools > Services**) to stop the `SplunkForwarder`

service.

1. Use a PowerShell window or command prompt to stop the `SplunkForwarder` service.

```
cd  %SPLUNK_HOME%\bin
.\splunk stop
```

2. Run the Microsoft Installer to perform the uninstallation.

```
msiexec /x splunkuniversalforwarder-<...>-x86-release.msi
```

The installer has one supported flag that you can use during uninstallation.

Flag	Description	Default
`REMOVE_FROM_GROUPS=1|0`	Specifies whether or not to take away rights and administrative group membership from the user you installed the forwarder as. This flag is available only when you uninstall the universal forwarder. If you set this flag to 1, the installer takes away group membership and elevated rights from the user you installed the forwarder as. If you set this flag to 0, the installer does not take away group membership and elevated rights from the user	1 (Take away elevated rights and group membership on uninstall.)

Configure the universal forwarder

Enable a receiver for Splunk Enterprise

A receiver is a Splunk component that you configure to listen on a specific network port for incoming data from a forwarder. For Splunk Enterprise, the receiver is usually an indexer or a cluster of indexers.

For Splunk Enterprise forwarder and indexer compatibility see Compatibility between forwarders and Splunk Enterprise indexers in the *Splunk Products Version Compatibility Matrix* manual.

Sometimes the receiver is another forwarder, which is called an intermediate forwarder. To learn more about how intermediate forwarders work, see Configure an intermediate forwarder.

To enable to a receiver for the Splunk Cloud Platform, see Enable a receiver for the Splunk Cloud Platform.

Configure a receiver using Splunk Web

Use Splunk Web to configure a receiver:

1. Log into Splunk Web as a user with the admin role.
2. In Splunk Web, go to **Settings > Forwarding and receiving**.
3. Select "Configure receiving."
4. Verify if there are existing receiver ports open. You cannot create a duplicate receiver port. The conventional receiver port configured on indexers is port `9997`.
5. Optionally select "New Receiving Port."
6. Add a port number and save.

Splunk Web is only available with Splunk Enterprise, not the universal forwarder.

Configure a receiver using the command line

Use the command line interface (CLI) to configure a receiver:

1. Open a shell prompt
2. Change the path to $SPLUNK_HOME/bin
3. Type: `splunk enable listen <port> -auth <username>:<password>`.
4. Restart Splunk software for the changes to take effect.

*nix example	Windows example
`./splunk enable listen 9997 -auth admin:password`	`splunk enable listen 9997 -auth admin:password`

Configure a receiver using a configuration file

Configure a receiver using the `inputs.conf` file:

1. Open a shell prompt
2. Change the path to `$SPLUNK_HOME/etc/system/local`.
3. Edit the `inputs.conf` file.

4. Create a `[splunktcp]` stanza and define the receiving port. Example:

   ```
   [splunktcp://9997]
   disabled = 0
   ```
5. Save the file.
6. Restart Splunk software for the changes to take effect.

Enable a receiver for the Splunk Cloud Platform

A receiver is a Splunk component that you configure to listen on a specific network port for incoming data from a forwarder. This can include indexers, another forwarder, or Edge Processors.

A Splunk Cloud Platform receiving port is configured and enabled by default. You need to install and configure the Splunk Cloud Platform universal forwarder credentials package on your forwarders to access it. You can install the forwarder credentials on individual forwarders, or install the forwarder credentials on many forwarders using a deployment server. See the following options:

- Install the forwarder credentials on individual forwarders in *nix.
- Install the forwarder credentials on many forwarders using a deployment server in *nix.
- Install the forwarder credentials on individual forwarders in Windows.
- Install the forwarder credentials on many forwarders using a deployment server in Windows.
- Renew certificates in the Splunk Cloud Universal Forwarder credentials package.

Alternatively, for enhanced data processing before routing the data to Splunk Cloud indexers, you can use the Edge Processor as a receiver for Splunk Cloud Platform. See About the Edge Processor Solution for more information.

Install the forwarder credentials on individual forwarders in *nix

1. From your Splunk Cloud Platform instance, go to **Apps > Universal Forwarder**.
2. Click **Download Universal Forwarder Credentials**.
3. Note the location where the credentials package `splunkclouduf.spl` has been downloaded.
4. Copy the file to a temporary directory, this is usually your "/tmp" folder.
5. Install the `splunkclouduf.spl` app by entering the following in command line: `$SPLUNK_HOME/bin/splunk install app /tmp/splunkclouduf.spl`.
6. When you are prompted for a user name and password, enter the user name and password for the Universal Forwarder. The following message displays if the installation is successful: `App '/tmp/splunkclouduf.spl' installed`.
7. Restart the forwarder to enable the changes by entering the following command: `./splunk restart`.

Install the forwarder credentials on many forwarders using a deployment server in *nix

1. From your Splunk Cloud Platform instance, go to **Apps > Universal Forwarder**.
2. Click **Download Universal Forwarder Credentials**.
3. Note the location where the credentials file was downloaded. The credentials file is named `splunkclouduf.spl`.
4. Copy the file to your system's temporary (/tmp) folder.
5. (optional) Use file management tools to move the `splunkclouduf.spl` file to the `$SPLUNK_HOME/etc/deployment-apps/` directory on the deployment server.
6. In a shell or command prompt, unpack the credentials package by running the following command: `tar xvf splunkclouduf.spl`
   .

7. Navigate to the `/bin` subdirectory of the deployment server.
8. Install the credentials package by running the following command:
   `splunk install app <'full path to splunkclouduf.spl'> -auth <username>:<password>`
   where `<"full path to splunkclouduf.spl">` is the path to the directory where the `splunkclouduf.spl` file is located and `<username>:<password>` are the username and password of an existing admin account on the deployment server.
9. Restart the deployment server by running the following command:
   `/splunk restart`
   .

Install the forwarder credentials on individual forwarders in Windows

1. From your Splunk Cloud Platform instance, go to **Apps > Universal Forwarder**.
2. Click **Download Universal Forwarder Credentials**.
3. Note the location where the credentials file was downloaded. The credentials file is named `%HOMEPATH%\Downloads`.
4. Copy the file to your system's temporary (\tmp) folder.
5. Install the `splunkclouduf.spl` app by entering the following command: `%SPLUNK_HOME%\bin\splunk.exe install app %HOMEPATH%\Downloads\splunkclouduf.spl`.
6. When you are prompted for a username and password, enter the username and password for the Universal Forwarder. The following message displays if the installation is successful:
   `App %HOMEPATH%\Downloads\splunkclouduf.spl installed`.
7. Restart the forwarder to enable the changes by entering the following command. `.\splunk.exe restart`.

Install the forwarder credentials on many forwarders using a deployment server in Windows

1. From your Splunk Cloud Platform instance, go to **Apps > Universal Forwarder**.
2. Click **Download Universal Forwarder Credentials**.
3. Note the location where the credentials file `splunkclouduf.spl` was downloaded.
4. Copy the file to your system's temporary (\tmp) folder.
5. (optional) Use file management tools to move the `splunkclouduf.spl` file to the `$SPLUNK_HOME\etc\deployment-apps\` directory on the deployment server.
6. In a shell or command prompt, unpack the credentials package by running the following command:
   `tar xvf splunkclouduf.spl`
   .
7. Navigate to the `\bin` subdirectory of the deployment server.
8. Install the credentials package by running the following command:
   `splunk install app <"full path to splunkclouduf.spl"> -auth <username>:<password>`
   where `<"full path to splunkclouduf.spl">` is the path to the directory where the `splunkclouduf.spl` file is located and `<username>:<password>` are the username and password of an existing admin account on the deployment server.
9. Restart the deployment server by running the following command:
   `\splunk restart`

.

Renew certificates in the Splunk Cloud Universal Forwarder credentials package

In versions 9.3.0 and higher of universal and heavy forwarders that connect to Splunk Cloud Platform versions 9.2.2406 and higher, the TLS certificates that come with the Splunk Cloud Universal Forwarder credentials package can be renewed automatically after a certain period of time. You can also renew the certificates manually at your leisure.

Prerequisites for using automatic TLS certificate renewal on forwarders to Splunk Cloud Platform

To use automatic renewal of TLS certificates on forwarders that send data to Splunk Cloud Platform, you must have all of the following. Forwarder certificate rotation does not work in configurations other than the ones that appear here:

- Your Splunk Cloud Platform environment must be hosted in a commercial Amazon Web Services (AWS) environment.
- Currently, the environment can be hosted in any AWS region except for the following: ap-northeast-2, ap-south-1, eu-north-1, eu-south-1, me-central-1, or sa-east-1
- The environment must run Splunk Cloud Platform version 9.2.2406 or higher.
- Forwarders that you connect to the environment must run version 9.3.0 or higher.
- You must configure at least one forwarding output group or channel on the forwarder to send data to Splunk Cloud Platform. There is no support for using automatic certificate rotation on forwarders that only send data to Splunk Enterprise.
- You can use automatic certificate rotation with universal or heavy forwarders, but you must connect the forwarders directly to your Splunk Cloud Platform instance. There is no support for using automatic certificate rotation when you connect forwarding output channels to either intermediate forwarders or Edge Processor.

How automatic TLS certificate renewal on forwarders to Splunk Cloud Platform works

The autoCertRotation setting in the outputs.conf configuration file controls whether or not a universal or heavy forwarder automatically renews TLS certificates that have been installed through the Splunk Cloud Platform Universal Forwarder Credentials package.

A value of "true" for the setting means that the forwarder attempts to renew the certificates inside the credentials package, up to and including their expiration time. A value of "false" means that the forwarder does not attempt to renew certificates in the credentials package. By default, automatic certificate rotation does not occur.

A forwarder certificate becomes eligible for renewal when:

- It has been configured for the forwarder to use it, and
- It is within its validity window, which means the current date must be between its 'Not Before' and 'Not After' dates, inclusive, and
- Less than or equal to 50% of its validity period remains. For example, a certificate with a validity period of 52 weeks is eligible for renewal after 26 weeks from its start of validity.

When a certificate on a forwarder enters its renewal eligibility period, the forwarder contacts the Splunk Cloud Platform instance to retrieve an updated certificate. If it is successful, it downloads the certificate and installs it immediately. There is no need to restart or reload the forwarder configuration.

Configure automatic TLS certificate renewal on forwarders to Splunk Cloud Platform

To configure automatic TLS certificate rotation on the forwarder, follow this procedure:

1. On the forwarder, open the $SPLUNK_HOME/etc/system/local/outputs.conf file for editing.
2. In the tcpout stanza(s) which represent the forwarding output group(s) that forward data to Splunk Cloud Platform, add the following line to the configuration file:

```
[tcpout:<splunkcloud>]
autoCertRotation = true
```

3. Save the file and close it.
4. Restart the forwarder or reload its configuration. The change takes effect immediately.

While it is possible to define automatic certificate rotation at any tcpout stanza level, there is no support for doing so at the global [tcpout] level when the forwarder sends data to multiple receivers. Additionally, there is no support for doing so for multiple [tcpout] output groups.If the forwarder sends data to both a Splunk Enterprise and a Splunk Cloud Platform instance, add the configuration to the tcpout stanza that represents the connection to your Splunk Cloud Platform instance only.If the forwarder connects to multiple Splunk Cloud Platform instances, add the setting to only one of the tcpout stanzas that forwards data to Splunk Cloud Platform.There is no support for configuring automatic certificate rotation for multiple Splunk Cloud Platform environments from a single forwarder.

Manually renew TLS certificates on forwarders to Splunk Cloud Platform

You can always manually renew TLS certificates on a universal or heavy forwarder that sends data to Splunk Cloud Platform. To do this, follow this procedure:

1. Download the latest version fo the unviersal forwarder credentials package from the Splunk website.
2. Install the updated universal forwarder credentials package using the instructions that appear earlier in this topic.
3. As the last step, rather than restarting the instance, reload the configuration by running the following command:

```
curl -i -u <username>:<password> https://<url of forwarder>:8089/services/data/outputs/tcp/default/_reload
```

If you want to reload the configuration without restarting on Windows machines, you must download and install the Windows version of the curl web transfer tool from the curl website. You can then follow the steps in this procedure.

Configure the universal forwarder using configuration files

Optionally edit the Universal forwarder configuration files to further modify how your machine data is streamed to your indexers. See the following steps:

1. Find the configuration files.
2. Edit the configuration files.
3. Restart the universal forwarder.

Find the configuration files

Navigate to `outputs.conf` in `$SPLUNK_HOME/etc/system/local/` to locate your Universal Forwarder configuration files.

Key configuration files:

- inputs.conf controls how the forwarder collects data.
- outputs.conf controls how the forwarder sends data to an indexer or other forwarder.
- server.conf for connection and performance tuning.
- deploymentclient.conf for connecting to a deployment server.

Edit the configuration files

You can edit them however you normally edit files, such as through a text editor or the command line, or you can use the Splunk Deployment Server.

When you make configuration changes with the CLI, the universal forwarder writes the configuration files. This prevents typos and other mistakes that can occur when you edit configuration files directly.

The forwarder writes configurations for forwarding data to `outputs.conf` in `$SPLUNK_HOME/etc/system/local/`).

Edit the configuration files through the command line

You can choose to edit the configuration files through the command line. For more details on using the CLI in general, see Administer Splunk Enterprise with the CLI in the Splunk Enterprise *Admin Manual*.

The general syntax for a CLI command is:

```
./splunk <command> [<object>] [[-<parameter>] <value>]...
```

See the following examples of using the command line to edit configuration files:

Configure the universal forwarder to connect to a receiving indexer

From a shell or command prompt on the forwarder, run the command:

```
./splunk add forward-server <host name or ip address>:<listening port>
```

For example, to connect to the receiving indexer with the hostname `idx.mycompany.com` and that host listens on port 9997 for forwarders, type in:

```
./splunk add forward-server idx1.mycompany.com:9997
```

Configure the universal forwarder to connect to a deployment server

From a shell or command prompt on the forwarder, run the command:

```
./splunk set deploy-poll <host name or ip address>:<management port>
```

For example, if you want to connect to the deployment server with the hostname `ds1.mycompany.com` on the default management port of 8089, type in:

```
./splunk set deploy-poll ds1.mycompany.com:8089
```

Configure a data input on the forwarder

The Splunk Enterprise *Getting Data In* manual has information on what data a universal forwarder can collect.

1. Determine what data you want to collect.

2. From a shell or command prompt on the forwarder, run the command that enables that data input. For example, to monitor the `/var/log` directory on the host with the universal forwarder installed, type in:

```
./splunk add monitor /var/log
```

The forwarder asks you to authenticate and begins monitoring the specified directory immediately after you log in.

Start or stop the universal forwarder

After you install the universal forwarder, you must start it. Also, if you make changes to the universal forwarder, you must start or restart it:

- Restart the universal forwarder
- Start the universal forwarder
- Stop the universal forwarder

Restart the universal forwarder

Some configuration changes might require that you restart the forwarder.

To restart the universal forwarder, use the same CLI `restart` command that you use to restart a full Splunk Enterprise instance:

- **On Windows:** Go to `%SPLUNK_HOME%\bin` and run this command:

```
splunk restart
```

- **On *nix systems:** From a shell prompt on the host, go to `$SPLUNK_HOME/bin`, and run this command:

```
./splunk restart
```

Start the universal forwarder

See the following steps to start the universal forwarder:

1. Set up environment variables on your machine, which are necessary to run these commands. It is possible these variables have automatically been set up. See Change default values in the *Admin Manual*.
2. Run the following commands to start the universal forwarder at any time. If this is your first time starting the forwarder, you may be asked to review and accept a license agreement and create a username and password,

- To start the universal forwarder, run this command.

Unix	Windows
`cd $SPLUNK_HOME/bin` `./splunk start`	`cd %SPLUNK_HOME%\bin` `.\splunk start`

- If you want to accept the license agreement without reviewing it when you start the forwarder for the first time, run this command.

Unix	Windows
`cd $SPLUNK_HOME/bin` `./splunk start --accept-license`	`cd %SPLUNK_HOME%\bin` `.\splunk start --accept-license`

- If you want to restart the forwarder after you make a configuration change, run this command. When you do, the forwarder first stops itself, then starts itself again.

Unix	Windows
`cd $SPLUNK_HOME/bin` `./splunk restart`	`cd %SPLUNK_HOME%\bin` `.\splunk restart`

- Additionally, you can configure the universal forwarder to start at boot time. See Configure Splunk Enterprise to start at boot time for the procedure.

The universal forwarder prompts for administrator credentials the first time you start it

When you start the forwarder for the first time under most conditions, it prompts you to create credentials for the Splunk administrator user. The following text appears:

```
This appears to be your first time running this version of Splunk.

Splunk software must create an administrator account during startup. Otherwise, you cannot log in.
Create credentials for the administrator account.
Characters do not appear on the screen when you type in credentials.

Please enter an administrator username:
```

1. Type in the name you want to use for the administrator user. This is the user that you log into the universal forwarder with, not the user that you use to log into your machine or onto splunk.com. You can press Enter to use the default username of `admin`.
   The following text appears:
   ```
   Password must contain at least:
   * 8 total printable ASCII character(s).
   Please enter a new password:
   ```
2. Type in the password that you want to assign to the user. The password must meet the requirements that the prompt displays.

See Create a secure administrator password in *Securing Splunk* for additional information about creating a secure password.

Start Splunk Enterprise without prompting, or by answering "yes" to any prompts

There are two other `start` options: `no-prompt` and `answer-yes`.

- If you run `$SPLUNK_HOME/bin/splunk start --no-prompt`, Splunk Enterprise proceeds with startup until it has to ask a question. Then, it displays the question and why it has to quit, and quits. In this scenario, it does not prompt for administrator credentials. You must manually create the credentials and restart before you can log in. See "Create administrator credentials manually" later in this topic for the procedure.
- If you run `SPLUNK_HOME/bin/splunk start --answer-yes`, Splunk Enterprise proceeds with startup and automatically answers "yes" to all yes/no questions that it encounters during startup. It displays each question and answer as it continues.

If you run start Splunk Enterprise with all three options in one line, the following happens:

- The software accepts the license automatically and does not ask you to accept it.
- The software answers "yes" to any "yes/no" question.
- The software quits if it encounters a question that cannot be answered "yes" or "no".

Stop the universal forwarder

You must stop the universal forwarder if you do not want it to forward data any more, or as part of a restart sequence when you make a configuration change that requires a restart.

The following commands use environment variables that might not be automatically set on your host. The environment variables represent where the universal forwarder has been installed on the host. To learn how to set these environment variables, see Change default values in the *Admin Manual*.

- Run the following commands to stop the universal forwarder.

Unix	Windows
`cd $SPLUNK_HOME/bin` `./splunk stop`	`cd %SPLUNK_HOME%\bin` `.\splunk stop`

Forward data

Configure an intermediate forwarder

Intermediate forwarding is where a forwarder receives data from one or more forwarders and then sends that data on to another indexer. This kind of setup is useful when, for example, you have many hosts in different geographical regions and you want to send data from those forwarders to a central host in that region before forwarding the data to an indexer. All forwarder types can act as an intermediate forwarder.

Configure intermediate forwarding

Set up the intermediate forwarding tier

1. Install the forwarder on your intermediate host.
2. See Configure the forwarder to configure the intermediate forwarder to send data to a receiving indexer if you are using Splunk Enterprise. For Splunk Cloud, see Install and configure the Splunk Cloud Platform universal forwarder credentials package to set up credentials.
    1. If you install the forwarder on Windows, you can specify the receiving indexer during the installation process.
3. Configure the intermediate forwarder to receive data. See Configure a receiver using a configuration file.
4. (Optional) Configure any local data inputs on the intermediate forwarder. See Configure local data inputs.
5. Restart the forwarder services.

You can repeat these steps to add more forwarders to the intermediate tier.

Configure forwarders to use the intermediate forwarding tier

1. Install the universal forwarder.
2. Configure the forwarder to send data to the intermediate forwarder. In this scenario, the intermediate forwarder acts as the receiver.
3. Configure local data inputs on the forwarder.
4. Restart the forwarder services.

Test the configuration

1. In Splunk Web, log into your Splunk deployment.
2. Open the Search and Reporting app.
3. Run a search that contains a reference to one of the hosts that you configured to send data to the intermediate forwarder

    ```
    host=<name or ip address of forwarder> index=_internal
    ```

    If you do not see events, then the host has not been configured properly. See Troubleshoot the universal forwarder for possible fixes.

See also

If you have access to the Edge Processor solution, you can use Edge Processors to fulfill many of the same requirements as an intermediate forwarder tier. For example, you can send data from multiple forwarders in different geographical regions to an Edge Processor that serves as a central host in a specific region, and then send data from that Edge Processor to an indexer. You can also use the Edge Processor to transform the data before routing it to an indexer. For more information, see About the Edge Processor solution in the *Use Edge Processors* manual.

Configure forwarding with outputs.conf

The outputs.conf file defines how forwarders send data to receivers. You can specify some output configurations at installation time (Windows universal forwarders only) or the CLI, but most advanced configuration settings require that you edit `outputs.conf`.

The topics that describe various forwarding topologies, such as load balancing and intermediate forwarding, provide detailed examples on configuring `outputs.conf` to support those topologies.

Although `outputs.conf` is a required file for configuring forwarders, it addresses only the outputs from the forwarder, where you want the forwarder to send the data it collects. To specify the data that you want to collect from the forwarder, you must separately configure the inputs, as you would for any Splunk instance. See Add data and configure inputs in *Getting Data In*.

Edit outputs.conf to configure forwarding

This procedure details the steps you must take to edit the default `outputs.conf` which is in `$SPLUNK_HOME/etc/system/local`. You might have to edit the file in other places, as sections in this topic explain. For an example of what an `outputs.conf` file looks like, see "Examples of outputs.conf" later in this topic.

1. On the host that forwards that data that you want to collect, open a shell or command prompt or PowerShell window.
2. Go to the configuration directory for the forwarder.

Unix	Windows
`cd $SPLUNK_HOME/etc/system/local`	`cd %SPLUNK_HOME%\etc\system\local`

3. Open `outputs.conf` for editing with a text editor.

Unix	Windows
`vi outputs.conf`	`notepad outputs.conf`

4. Edit outputs.conf. Add a minimum of at least one forwarding target group or a single receiving host.
5. Save the `outputs.conf` file and close it.
6. Restart the universal forwarder to complete your changes.

Unix	Windows
`cd $SPLUNK_HOME/bin` `./splunk restart`	`cd %SPLUNK_HOME%\bin` `.\splunk restart`

Types of outputs.conf files

A single forwarder can have multiple `outputs.conf` files. For example, one can be located in an apps directory and another in `$SPLUNK_HOME/etc/system/local`. No matter how many `outputs.conf` files the forwarder has and where they

reside, the forwarder combines all their settings, using the rules of configuration file precedence. The forwarder contains both default and custom `outputs.conf` files.

Default versions of outputs.conf

The universal forwarder ships with these default versions of `outputs.conf`:

- One in `$SPLUNK_HOME/etc/system/default`.
- Another in `$SPLUNK_HOME/etc/apps/SplunkUniversalForwarder/default`.

The default version in the `SplunkUniversalForwarder` app has precedence over the version under `/etc/system/default`.

Do not edit default versions of any configuration files. See About configuration files.

Custom versions of outputs.conf

When you configure forwarding behavior, those changes get saved in custom versions of `outputs.conf`. There are several ways you can specify forwarding behavior:

- While installing the forwarder (on the Windows universal forwarder only.)
- By running CLI commands.
- By directly editing an `outputs.conf` file.

The forwarder automatically creates or edits custom versions of `outputs.conf` in response to the first three methods. The locations of those versions vary, depending on the type of forwarder and other factors.

- If you use the CLI to make changes to universal forwarder output behavior, the CLI creates or edits a copy of `outputs.conf` in `$SPLUNK_HOME/etc/system/local`.
- The Windows installation process writes configuration changes to an `outputs.conf` file located in the `MSICreated` app.

In addition to any `outputs.conf` files that you create and edit indirectly (for example, through the CLI), you can also create or edit an `outputs.conf` file directly with a text editor. You should work with a single copy of the file, which you place in `$SPLUNK_HOME/etc/system/local/`. If a copy of the file already exists in that directory, because of configuration changes made through the CLI, edit that copy. For purposes of distribution and management simplicity, you can combine settings from all non-default versions into a single custom `outputs.conf` file.

The universal forwarder must be restarted after you make changes to `outputs.conf`.

For information on `outputs.conf`, see the outputs.conf spec file.

Configuration levels for outputs.conf

There are two types of output processors for forwarding data: `tcpout` and `syslog`. The universal forwarder only has the `tcpout` processor, which uses the `[tcpout]` header in `outputs.conf`.

You can configure the `tcpout` processor at three levels of stanzas:

- **Global.** (Optional) At the global level, you specify any attributes that you want to apply globally, as well as certain attributes only configurable at the system-wide level for the output processor.
- **Target group.** A target group defines settings for one or more receiving indexers. There can be multiple target

groups per output processor. Most configuration settings can be specified at the target group level.
- **Single server.** (Optional) You can specify configuration values for single servers (receivers) within a target group.

Configurations at the more specific levels take precedence over the global level. For example, if you specify `compressed=true` for a target group, the forwarder sends the hosts in that target group compressed data, even if you set the `compressed` attribute to "false" for the global level.

Outputs.conf global stanza

The global stanza in `outputs.conf` lets you set any attributes that you want to apply globally. While this stanza is optional, there are several attributes that you can set only at the global level, including `defaultGroup`.

The `[tcpout]` header specifies the global stanza for the `tcpout` processor. Following is an example of a global tcpout stanza.

```
[tcpout]
defaultGroup=indexer1
compressed=true
```

This global stanza includes two attribute/value pairs:

- **defaultGroup=indexer1** This tells the forwarder to send all data to the "indexer1" target group. See "Default target groups".
- **compressed=true** This tells the forwarder to compress the data before it forwards the data to receiving indexers in the target groups. If you set `compressed` to "false", the forwarder sends raw data.

Set default target groups in outputs.conf

The `defaultGroup` attribute lets you set default groups for automatic forwarding at the global level, in your `[tcpout]` stanza.

The defaultGroup specifies one or more target groups that you define later in `tcpout:<target_group>` stanzas. The forwarder sends all events to the specified groups.

```
[tcpout]
defaultGroup= <target_group1>, <target_group2>, ...
```

If you do not want to forward data automatically, do not set the `defaultGroup` attribute.

Outputs.conf target group stanza

The target group identifies a set of receivers. It also specifies how the forwarder sends data to those receivers. You can define multiple target groups.

Here is the basic pattern for the target group stanza.

```
[tcpout:<target_group>]
server=<receiving_server1>, <receiving_server2>, ...
<attribute1> = <val1>
<attribute2> = <val2>
...
```

You can specify a receiving server in a target group by using the format `<ipaddress_or_hostname>:<port>`, where `<port>` is the receiving host **receiving port**. For example, `myhost.splunk.com:9997`. When you specify multiple receivers, the forwarder load balances among them.

A target group stanza name cannot have spaces or colons in it. Splunk software ignores target groups whose stanza names contain spaces or colons in them.

See Define typical deployment topologies later in this topic for information on how to use the target group stanza to define several deployment topologies.

Outputs.conf single-host stanza

You can define a specific configuration for an individual receiving indexer. However, the receiver must also be a member of a target group.

When you define an attribute at the single-host level, it takes precedence over any definition at the target group or global level.

Here is the syntax for defining a single-host stanza:

```
[tcpout-server://<ipaddress_or_hostname>:<port>]
<attribute1> = <val1>
<attribute2> = <val2>
...
```

Examples of outputs.conf

The following `outputs.conf` example contains three stanzas for sending data to Splunk receivers.

- Global settings. In this example, there is one setting, to specify a `defaultGroup`.
- Settings for a single target group consisting of two receivers. Here, we specify a load-balanced target group consisting of two receivers.
- Settings for one receiver within the target group. In this stanza, you can specify any settings specific to the `mysplunk_indexer1` receiver.

```
[tcpout]
defaultGroup=my_indexers

[tcpout:my_indexers]
server=mysplunk_indexer1:9997, mysplunk_indexer2:9996

[tcpout-server://mysplunk_indexer1:9997]
```

Define typical forwarder deployment topologies

You can configure a forwarder to support several typical deployment topologies. See the other topics in the "Forward data" chapter for information on how to configure forwarders for other topologies.

Configure load balancing on a universal forwarder with outputs.conf

When you specify a target group with multiple receivers in `outputs.conf` on a forwarder, the forwarder performs **load balancing** between the receivers.

In the example that follows, the target group consists of three receivers. The forwarder balances load between the three receivers you specify. If one receiver goes down, the forwarder automatically switches to the next available receiver.

```
[tcpout:my_LB_indexers]
server=10.10.10.1:9997,10.10.10.2:9997,10.10.10.3:9997
```

Note: While 9997 is the standard network port for receiving data from forwarders, you can specify any network port above 1024 to receive data.

Configure data cloning on a universal forwarder with outputs.conf

When you specify multiple target groups with a separate stanza for each group in `outputs.conf`, the forwarder performs **data cloning** between the groups. In data cloning, the forwarder sends copies of all its events to the receivers in two or more target groups. Data cloning usually results in similar, but not necessarily exact, copies of data on the receiving indexers. An example of how to configure data cloning follows.

```
[tcpout]
defaultGroup=indexer1,indexer2

[tcpout:indexer1]
server=10.1.1.197:9997

[tcpout:indexer2]
server=10.1.1.200:9997
```

The forwarder sends duplicate data streams to the servers specified in both the `indexer1` and `indexer2` target groups.

Configure data cloning with load balancing on a universal forwarder

You can combine load balancing with data cloning. For example:

```
[tcpout]
defaultGroup=cloned_group1,cloned_group2

[tcpout:cloned_group1]
server=10.10.10.1:9997, 10.10.10.2:9997, 10.10.10.3:9997

[tcpout:cloned_group2]
server=10.1.1.197:9997, 10.1.1.198:9997, 10.1.1.199:9997, 10.1.1.200:9997
```

The forwarder sends full data streams to both the `cloned_group1` and `cloned_group2` groups. The forwarders load-balance the data within each group, rotating among receivers every 30 seconds (the default frequency).

Common attributes for outputs.conf

The `outputs.conf` file provides a large number of configuration options that offer considerable control and flexibility in forwarding. Of the attributes available, several are of particular interest:

Attribute	Default	Where configured	Value
`defaultGroup`	n/a	global stanza	A comma-separated list of one or more target groups. Forwarder sends all events to all specified target groups.
`server`	n/a	target group stanza	Required. Specifies the hosts that function as receivers for the forwarder. This must be set to a value using the format `<ipaddress_or_servername>:<port>`, where `<port>` is the receiving server's receiving port.
`disabled`	false	any stanza level	Specifies whether the stanza is disabled. If set to "true", it is equivalent to the stanza not being there.
`sendCookedData`	true	global or target group stanza	Specifies whether data is cooked before forwarding.
`compressed`	false	global or target group stanza	Specifies whether the forwarder sends compressed data.
`ssl....`	n/a	any stanza level	Set of attributes for configuring SSL. See "Configure Splunk indexing and forwarding to use TLS certificates" in the *Securing Splunk Enterprise* manual for information on how to use these attributes.
`useACK`	false	global or target group stanza	Specifies whether the forwarder waits for indexer acknowledgment confirming that the data has been written to the file system.
`dnsResolutionInterval`	300	global or target group stanza	Specifies base time interval in seconds at which indexer DNS names will be resolved to IP address.
`autoLBVolume`	0	global or target group stanza	Specifies, in bytes, how much data a forwarder that has been configured for load balancing sends to an indexer before it selects another indexer.

The `outputs.conf.spec` file, which you can find here, along with several examples, provides details for these and all other configuration options. In addition, most of these settings are discussed in topics that deal with specific forwarding scenarios.

DNS resolution interval

The `dnsResolutionInterval` attribute specifies the base time interval (in seconds) at which receiver DNS names will be resolved to IP addresses. The forwarder uses this value to compute the run-time interval as follows:

```
run-time interval = dnsResolutionInterval + (number of receivers in server attribute - 1) * 30
```

The run-time interval increases by 30 seconds for each additional receiver that you specify in the `server` attribute (each additional receiver across which the forwarder load-balances.) The `dnsResolutionInterval` attribute defaults to 300 seconds.

For example, if you leave the attribute at the default setting of 300 seconds and the forwarder is load-balancing across 20 indexers, DNS resolution will occur every 14 1/2 minutes:

```
(300 + ((20 - 1) * 30)) = 870 seconds = 14.5 minutes
```

If you change `dnsResolutionInterval` to 600 seconds, and keep the number of load-balanced indexers at 20, DNS resolution will occur every 19 1/2 minutes:

```
(600 + ((20 - 1) * 30)) = 1170 seconds = 19.5 minutes
```

Configure the universal forwarder to send data over HTTP

Configure the universal forwarder to send data over hyper text transfer protocol (HTTP) between Splunk platform instances when you are unable to open network traffic to use the Splunk to Splunk (S2S) service.

Note the following limitations:

- A Splunk universal forwarder instance can perform either httpout or tcpout, but not both at the same time. There is currently no support to send ACKs to the client transaction.
- HTTPOUT cannot be used to send data among universal forwarders. It is used for the communication between the universal forwarder and an indexer or the universal forwarder and a heavy forwarder.
- EVENT_BREAKER and EVENT_BREAKER_ENABLE in props.conf can be used to help find event breaking boundaries for unparsed data indexing.

To configure a universal forwarder to send data over HTTP, add an `httpout` stanza to the outputs.conf file on your universal forwarder.

If httpout is configured, chunkedlinebreaker will be disabled.

Example httpout stanza

```
[httpout]
httpEventCollectorToken = eb514d08-d2bd-4e50-a10b-f71ed9922ea0
uri = https://10.222.22.122:8088
```

Example httpout stanza, with batch control

```
[httpout]
httpEventCollectorToken = eb514d08-d2bd-4e50-a10b-f71ed9922ea0
uri = https://10.222.22.122:8088
batchSize = 32768 #32kb batch size instead of 64kb default
batchTimeout = 10 #10 second timeout instead of 30s default
```

Available parameters for the httpout stanza

Parameter name	Description
`httpEventCollectorToken= <authToken>`	Authentication Token is used by the HEC endpoint to configure and validate against the HTTP transaction.
`uri = <uri>`	A Uniform Resource Identifier (URI) is the `IP:Port` combination of the indexer or load balancer. An empty URI disables the processor.
`batchSize = <size in Bytes>`	(Optional) Indicates how much data can be batched in one HTTP request. Default batch size is 64KB.
`batchTimeout = <time in secs>`	(Optional) Indicates if the above batch size does not fill, then instead of waiting, sends a timeout. Default is 30 seconds.

If batchTimeout becomes true, the accumulated pipeline data is sent over the HTTP connection.

Send data over HTTP using a load balancer

Use this example to configure a load balancer configuration using NGINX.

> Note: The Splunk Universal Forwarder supports Network Load Balancers (NLB) and Application Load Balancers (ALB) only when you use HTTP out.

```
events {
        worker_connections 768;
         multi_accept on;
}
http {
        upstream hec {
                keepalive 32
                server <HEC Server 1 IP>:8088;
                server <HEC Server 2 IP>:8088;
                server <HEC Server 3 IP>:8088;
        }
        server {
                listen 80;
                location / {
                        proxy_pass http://hec;
                        proxy_http_version 1.1;
                        proxy_set_header Connection "";
                }
        }
        server {
                listen 443 ssl;
                ssl_certificate server.pem;
                ssl_certificate_key server.pem;
                location / {
                        proxy_pass https://hec;
                        proxy_http_version 1.1;
                        proxy_set_header Connection "";
                }
        }
        access_log /var/log/nginx/access.log;
        error_log /var/log/nginx/error.log;
}
```

For more information on load balancer configuration, see the Configure load balancing for Splunk Enterprise topic in the *Forwarding manual*

LB_CHUNK_BREAKER configurations

> Starting in version 8.1.1 of the Splunk software, LB_CHUNK_BREAKER has been deprecated in favor of EVENT BREAKER.

`LB_CHUNK_BREAKER` is a configuration option for breaking events on your Splunk universal forwarder for sending over HTTP.

Since HTTP is a synchronous protocol, it is possible that a chunk of events read by the universal forwarder can be sent with one or more events breaking before sending. The `LB_CHUNK_BREAKER` configuration aids the universal forwarder in properly defining event boundaries to avoid any events being improperly broken before sending.

If `LB_CHUNK_BREAKER` is not defined then the universal forwarder will use your deployment's `EVENT BREAKER` settings. if `EVENT BREAKER` and `LB_CHUNK_BREAKER` are not defined, then the default pattern (`[\r\n]+`) will be used.

Splunk TCP leverages an asynchronous protocol that prevents this type of event breaking from occurring. If you are able to use Splunk TCP settings it is the preferred method for sending and receiving data in Splunk Enterprise and Splunk Cloud Platform from Splunk forwarders.

Example props.conf files on universal forwarder

```
#The capture group of (.) is the new event, it must be preceded by the string "xyz".
[customersource1]
LB_CHUNK_BREAKER = xyz(.)

#The capture group of (\n) defines new events and must be preceded by the string "xyz"
[customersource2]
LB_CHUNK_BREAKER = xyz(\n)

# The following regex pattern establishes event boundaries for Java traces.
[log4j]
LB_CHUNK_BREAKER = ([\r\n]+)\d{4}-\d\d-\d\d

#Carriage return and a new line feed is the default pattern for LB_CHUNK_BREAKER. It will be used if no
stanza is added by the user. This pattern also matched most access logs.
[access_combined]
LB_CHUNK_BREAKER = ([\r\n]+)
```

Splunk TCP and HTTP output stanza precedence

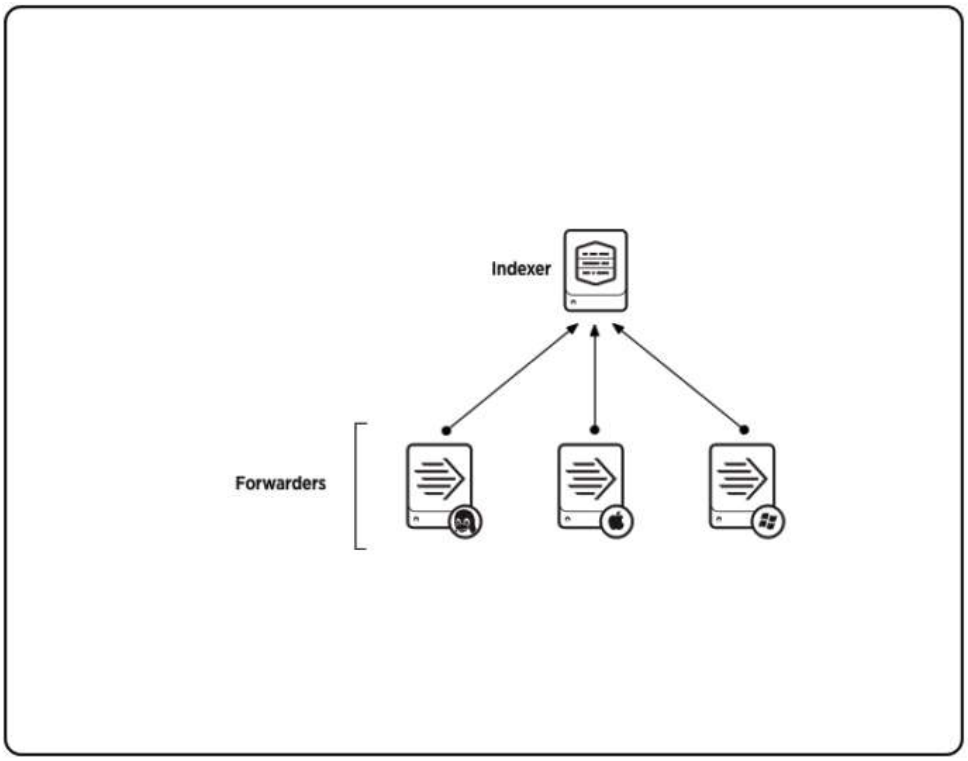
When a single Splunk Universal Forwarder has both tcp output settings and http output settings, http output will take precedence. The tcp output settings will be ignored in favor of http output configurations.

Troubleshoot HTTP Out

- In case of partial insertion of data, the client will resend all the data in the HTTP transaction, potentially resulting in duplicate events appearing on your receiver or indexer. Currently, the server sends how many segments it inserts successfully. The client has to implement to keep track of those segment counts and replay only the errored segments.
- There can be multiple chunks/segments of data in the same HTTP transaction
- If some segments inserted without an error but later receive an error (for example, "queue full", or "server busy"), then the server replies with an HTTP error.

Consolidate data from multiple hosts

One of the most common forwarding use cases is to consolidate data that originates across numerous machines. Forwarders located on the machines send the data to a central Splunk deployment. This diagram illustrates a common scenario, where universal forwarders residing on machines running diverse operating systems send data to a single Splunk instance, which indexes and provides search capabilities across all the data.



The diagram illustrates a small deployment. In practice, the number of universal forwarders in a data consolidation use case could number into the thousands.

1. Determine the data and machines you need to access.

2. Install a Splunk instance on a host.

This instance functions as the **receiver**. Data goes there to be indexed and searched.

3. Using the CLI, enter this command from `$SPLUNK_HOME/bin/`:

```
./splunk enable listen <port> -auth <username>:<password>
```

- `<port>` is the network port you want the receiver to listen on.

4. Install universal forwarders on each machine that will generate data.

5. Configure inputs for each forwarder.

To learn what Splunk software can index and how to configure inputs, see What data can I index? in *Getting Data In*.

6. Configure each universal forwarder to send data to the receiver. For Windows forwarders, you can do this at installation time or through the CLI after installation. For *nix forwarders, you must do this through the CLI.

```
./splunk add forward-server <host>:<port> -auth <username>:<password>
```

- `<host>:<port>` are the host and receiver port number of the receiver. For example, `splunk_indexer.acme.com:9997`.

Alternatively, if you have many forwarders, you can use an `outputs.conf` file to specify the receiver. For example:

```
[tcpout:my_indexers]
server= splunk_indexer.acme.com:9997
```

You can create this file once and distribute copies of it to each forwarder.

How to forward data to Splunk Cloud Platform

To forward data to your Splunk Cloud Platform instance, you perform the following procedures:

1. Download and install the universal forwarder software.
2. Download the Splunk universal forwarder credentials package.
3. Install the Splunk universal forwarder credentials package on the universal forwarder machine. See Install and configure the Splunk Cloud Platform universal forwarder credentials package.
4. To manage forwarders using Splunk Web, configure the universal forwarder to act as a deployment client.
5. Configure inputs to collect data from the host that the universal forwarder is on. For an overview, see Configure the universal forwarder. For detailed examples of using the CLI to add inputs, see the individual data topics in *Getting Data In*.

For details on installing Splunk Cloud Platform, see the platform-specific installation instructions in the Splunk Cloud Platform *Admin Manual* for the type of data you want to forward.

- Get Windows Data into Splunk Cloud Platform
- Get *nix data into Splunk Cloud Platform
- Forward data from files and directories to Splunk Cloud Platform

Working with the universal forwarder

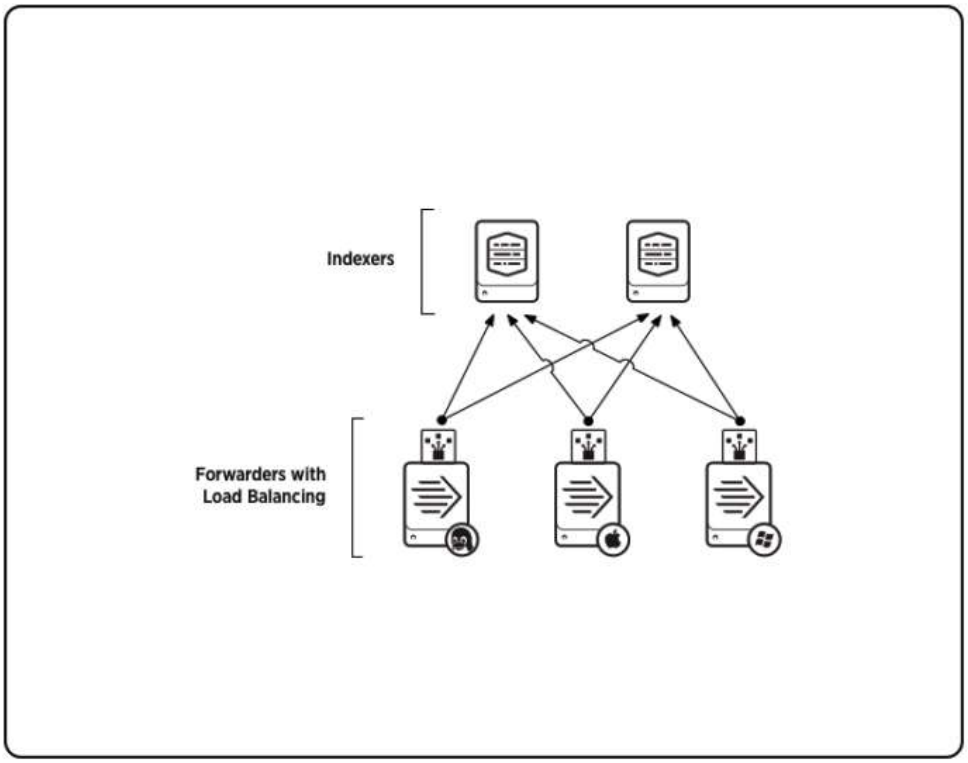
Advanced configurations for the universal forwarder

See the following Universal Forwarder advanced setup examples:

Load balancing

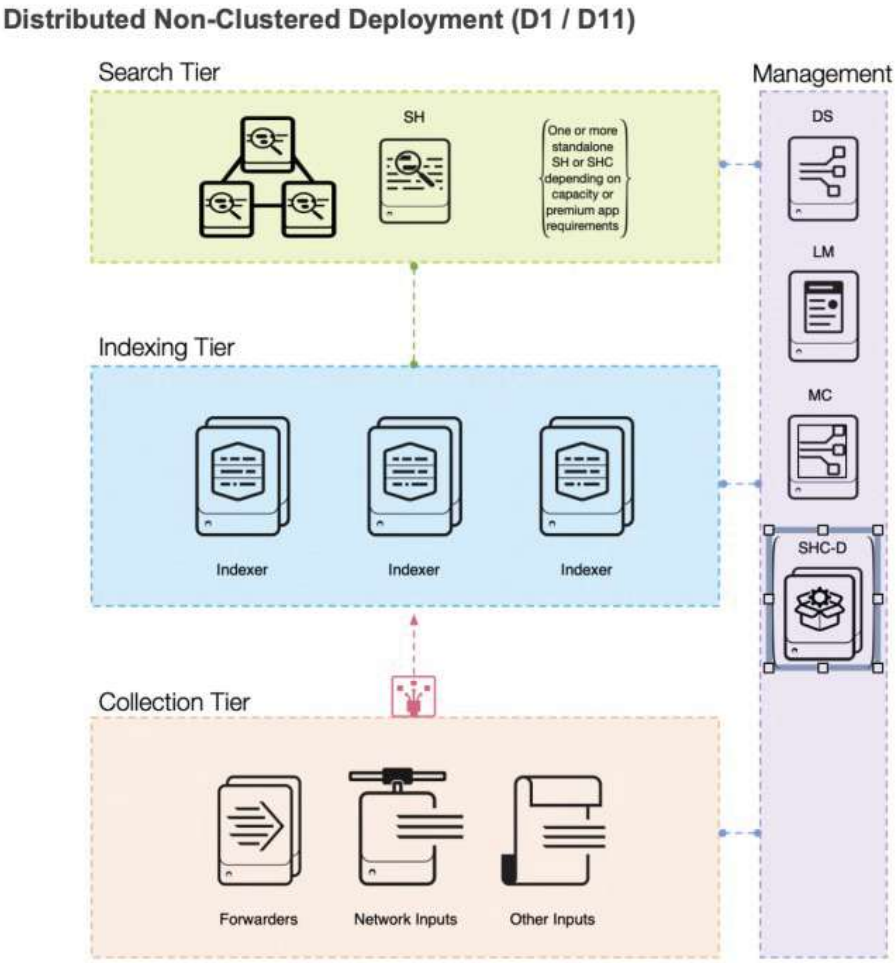
During **load balancing**, a forwarder distributes data across several receiving instances. Each receiver gets a portion of the total data, and together the receivers hold all the data. If a host goes down, the forwarder sends data to the next available receiver. Forwarders perform load balancing automatically. See Set up load balancing in the *Forwarding Data* manual.

The forwarder routes data to different indexers on a specified time or volume interval that you can specify. For example, if you have a load-balanced group that consists of indexer A, B, and C, at a specified interval, the forwarder switches the data stream to another indexer in the group at random. The forwarder might switch from indexer B to indexer A to indexer C, and so on. If one indexer is down, the forwarder immediately switches to another.



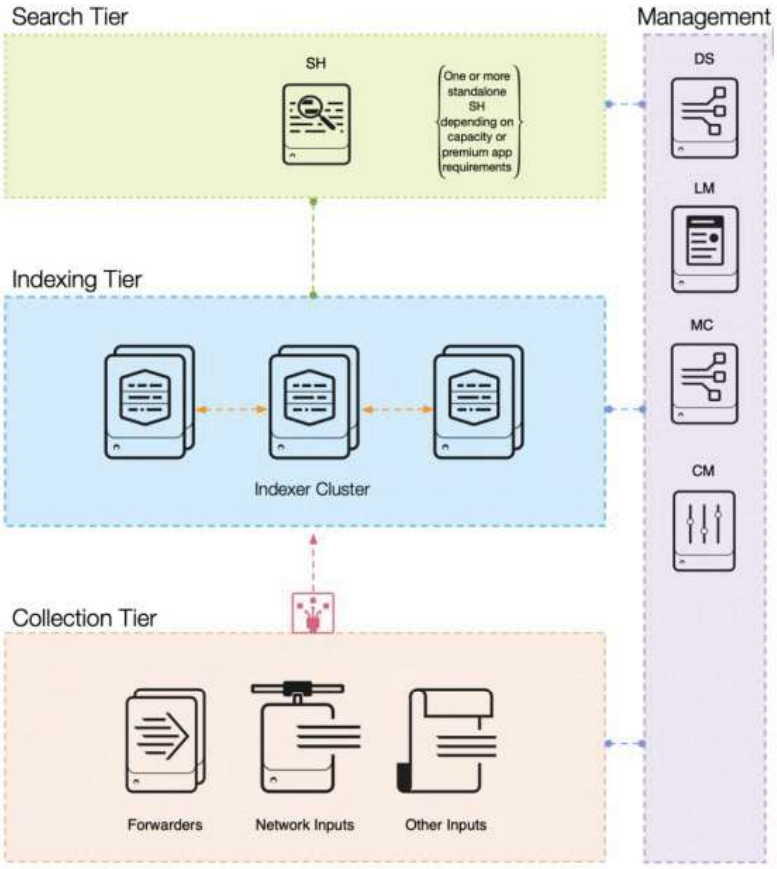
Distributed deployment

In a distributed deployment, the indexing logic and the data search logic are separated. It has both an indexer getting data from several inputs, and a search head, which searches across all the data found in this indexer. This is a great option if your daily data volume exceeds the capacity of a single-server deployment, or you want highly available data ingest. See Scale your deployment with Splunk Enterprise components in the *Distributed Deployment Manual*.



Distributed clustered deployment

This setup includes **Indexer clustering** with an appropriately configured data replication policy. In addition to being distributed, you combine multiple indexers to form an indexer cluster. This configuration keeps multiple copies of your data, increasing protection from data loss and availability of data. See Scale your deployment with Splunk Enterprise components in the *Distributed Deployment Manual*.



For more examples of advanced configurations, see https://www.splunk.com/pdfs/technical-briefs/splunk-validated-architectures.pdf for detailed information on advanced Universal Forwarder setups.

About management mode for the universal forwarder

The management mode feature for the universal forwarder is available for versions 9.1.0 and higher to improve security. You can control how CLI commands and local REST API calls communicate with the `splunkd` process through the management mode feature. You can configure how the universal forwarder communicates, either through Transmission Control Protocol (TCP) or Unix Domain Sockets (UDS). The default management mode is auto, which uses UDS if it is available on your operating system.

UDS-supported operating systems

UDS is available on the following operating systems:

- Linux
- macOS
- Windows Server 2019 and higher
- Windows 10 build 17063 and higher

For operating systems that don't support UDS, TCP is used instead.

Types of management modes

The following table lists the types of management modes:

Mode	Function
auto	CLI commands and local REST API calls communicate with the `splunkd` process through UDS if UDS is supported. If UDS is not supported, TCP is used instead.
tcp	CLI commands and local REST API calls communicate with the `splunkd` process through the management port bound to localhost.
none	CLI commands and local REST API calls are restricted from communicating through the management port.

Check and change your management mode

Upgrading the universal forwarder from version 9.0.0 and lower to the latest version does not change your existing settings. If this is the case, you must change your management mode to UDS when upgrading to 9.1.0 and higher if it's available on your operating system.

To check all applicable configurations in your management mode, run the following command:

```
./splunk btool server list --debug | egrep "disableDefaultPort|mgmtMode"
```

To change your management mode, follow these steps:

1. Navigate to the server.conf file in the $SPLUNK_HOME/etc/system/local/ folder.
2. Set the `mgmtMode` parameter to your desired mode.
3. Restart the Splunk platform by running the `./splunk restart` command.

Manage a Linux least-privileged user

Installing a Splunk universal forwarder automatically creates a least-privileged user. This is a non-root user with permissions specific to the successful operation of the universal forwarder features and add-ons.

To install the universal forwarder with a least-privileged user, see Install a Linux universal forwarder.

Least-privileged users are created when you install or update any Linux installation packaging format, including, .deb, .rpm, and .tgz. formats.

The least-privileged user possesses `AmbientCapabilities` that lets the user operate universal forwarder features and common add-ons without permission issues. These capabilities are:

Capability	Desc	Use
`CAP_DAC_READ_SEARCH`	Bypass file read permission checks and directory read and execute permission checks;	Collects data from files outside of `$SPLUNK_HOME`

Least privileged user security and performance implications

Least privilege mode is enabled to read any file permission on Linux version 9.0.0 and later.

A non-root or non-admin user that could not access some files before upgrade to least privilege user, may be able to access those files after upgrade in the following situations:

- You upgrade the universal forwarder from old versions to a least privilege version.
- Before upgrade, your universal forwarder is running as non-root or non-local admin.
- Prior to upgrade, you have inputs to monitor a directory with many files, or inputs with scripts to read many files, where users have no permission to access those files

In addition to security issues, this can lead to potential performance issues. Since the universal forwarder is able to read far more files than before, more resources such as CPU, memory, and disk input/output are consumed.

To avoid this, you can disable the "read any file" capability manually. To do this, edit the unit file to remove the CAP_DAC_READ_SEARCH capability.

Disable, enable, or change least-privileged user

The least-privileged user is enabled automatically during installation or upgrade. You can manually enable or disable it. To disable it, stop Splunk and run:

```
[sudo] $SPLUNK_HOME/bin/splunk disable boot-start
```

This command removed the unit file as well as the startup file. This will remove unit files from both locations:

```
/usr/lib/systemd/system
/etc/systemd/system
```

To enable or overwrite an existing least-privileged user configuration, run:

```
[sudo] $SPLUNK_HOME/bin/splunk enable boot-start
```

This command will grant least-privilege capabilities by default, and the unit file is created in the user level directory.

To change users, you must run this command again.

```
chown -R splunkfwd:splunkfwd $SPLUNK_HOME
```

Troubleshooting

JournalD input does not show results

If you are using a dedicated user ID, make sure the splunkfwd user ID is in the correct group when starting Splunk using systemd.

Manually enable a least privilege user

If you encounter an error during installation that prevents the creation of a least-privileged user, you can use the following command to manually create or recreate the default least privileged user:

```
[sudo] $SPLUNK_HOME/bin/splunk enable boot-start -systemd-managed 1 -user <username> -group <groupname>
```

This creates a unit file with the following permissions:

```
######## Added for least privilege mode #########
NoNewPrivileges=yes
AmbientCapabilities=CAP_DAC_READ_SEARCH
################################################
```

Editing unit files

Splunk software potentially creates two unit files in two locations when you Install the least privileged user on a Linux machine. If you have error messages, you may have to check and edit both files. To locate both files run the following command:

```
./splunk display boot-start
```

Error messages

Error message	Description
Cannot create file /etc/systemd/system/SplunkForwarder.service: permission denied.	You must create the unit file manually or the current user does not have permission to create the unit file.
Failed to auto-set default user. Please create the unit file manually.	The system cannot find a valid Linux user.
Failed to create splunk unit file. Please create the unit file manually	Usually a system error, for example, the system cannot create the folder, create the startup file, or reload systemd.

Reference

About the unit files created for the least privileged user

Splunk software potentially creates two unit files in different locations when you Install the least-privileged user on a Linux machine.

- If the first unit file is created successfully at installation, no further unit files are created.
- If the first file fails during installation, another file is created on the user level in the local folder.
- If you use the `[sudo] $SPLUNK_HOME/bin/splunk enable boot-start` command after a least privileged user is created, a new file is created locally. This either creates a new file in the local directory or overwrites any local file that exists.
- The local file takes precedence over the system file.

To see your unit files and their location in your environment, you can run `Splunk display boot-start`.

/usr/lib/systemd/system	where services are provided by installed packages	This is automatically created during installation, and can be overwritten during upgrade or by running `[sudo] $SPLUNK_HOME/bin/splunk enable boot-start`
/etc/systemd/system	where system-wide user services are placed by the system administrator	Created when running `splunk enable boot-start -systemd-managed 1`

Reference unit file template

This is an example of a unit file template. You can use it to manually create a unit file.

```
#This unit file replaces the traditional start-up script for systemd
#configurations, and is used when enabling boot-start for Splunk on
#systemd-based Linux distributions.

[Unit]
Description=Systemd service file for Splunk, generated by 'splunk enable boot-start'
After=network.target

[Service]

######## Added for least privilege mode #########
NoNewPrivileges=yes
AmbientCapabilities=CAP_DAC_READ_SEARCH
################################################

Type=simple
Restart=always
ExecStartPre=-/bin/bash -c "chown -R splunkfwd:splunkfwd /opt/splunkforwarder
ExecStart=/opt/splunkfwd/bin/splunkfwd_internal_launch_under_systemd
KillMode=mixed
KillSignal=SIGINT
TimeoutStopSec=360
LimitNOFILE=65536
SuccessExitStatus=51 52
RestartPreventExitStatus=51
RestartForceExitStatus=52
User=splunkfwd
Group=splunkfwd
Delegate=true
CPUShares=1024
MemoryLimit=<value>
PermissionsStartOnly=true
ExecStartPost=/bin/bash -c "chown -R splunkfwd:splunkfwd /sys/fs/cgroup/cpu/system.slice/%n"
ExecStartPost=/bin/bash -c "chown -R splunkfwd:splunkfwd /sys/fs/cgroup/memory/system.slice/%n"

[Install]
WantedBy=multi-user.target
```

Control forwarder access

You can configure Splunk Enterprise to allow communication from authorized forwarders through the use of tokens. A token is a unique key that is generated and enabled on the indexer, and configured on the forwarder. A forwarder attempting to send data to an indexer without the correct token value will be rejected. Forwarder access control is independent of Secure Sockets Layer (SSL,) and can be used in environments that do not have SSL enabled between Splunk platform instances.

Prerequisites to configuring forwarder access control

The token creation process requires command line access to the management port of the Splunk platform indexers and an administrative level Splunk Enterprise account to create and enable tokens. To access the REST API, use the `curl` command. There's no integrated support for `curl` on the Windows Operating System (OS.) You can use a Linux system to configure and manage tokens, or find a supported Windows OS tool.

Forwarder access controls are not available for Splunk Cloud.

Once a token is generated, it must be enabled on the Splunk platform indexers and configured in the outputs.conf on the forwarders that connect to the indexer. For forwarder configuration management options, see Best practices for deploying configuration updates across universal forwarders in the *Updating Splunk Enterprise Instances* manual.

Token management

The token is created on the receiver. The receiver can be a heavy forwarder, or an indexer.

Generate a token

Before you can configure token-based authentication, you must generate a token to use:

1. From a command or shell prompt, use the REST API to connect to a Splunk Enterprise indexer to create the token:

   ```
   curl -v -k -u <user>:<password>
   https://<host>:<management_port>/services/data/inputs/tcp/splunktcptoken -d "name=<token_name>"
   ```

   In this command:

- `user` and `password` are the administrative credentials you'll use to log into the Splunk platform indexer.
- `host` is the host name or IP address of the indexer.
- `management_port` is the TCP management port on the indexer (default: 8089.)
- `token_name` is the friendly name that you want to assign the token.

- The REST command response is returned to the command line and includes the token value. Copy the token value into a password management vault or other repository for later use in configuring the forwarders.
- The token must be enabled on the indexer before it can be used for forwarder authentication.

For example, to create a token named "my_token" on the host `idx1.mycompany.com` using the Splunk admin user and password:

```
curl -v -k -u admin:changeme https://idx1.mycompany.com:8089/services/data/inputs/tcp/splunktcptoken -d
"name=my_token"
```

The REST response includes the token value:

```
<s:key name = "token">808F7BD7-1444-4910-B8F5-87B83D694E18</s:key>
```

Enable a token

A token can be enabled using the REST API, or by modifying the inputs.conf of the receiving indexer.

To use the REST API to enable a token, from a command or shell prompt, run:

```
curl -v -k  -X "POST" -u <user>:<password>
https://<host>:<management_port>/services/data/inputs/tcp/splunktcptoken/<token_name>/enable
```

Optionally, use the inputs.conf to enable a token:

1. Edit `inputs.conf` on the indexer and add the stanza:

   ```
   [splunktcptoken://<token_name>]
   disabled = 0
   token = <token_value>
   ```
2. Restart Splunk Enterprise services.

Disable a token

To disable a token using the REST API, use the following command:

```
curl -v -k  -X "POST" -u <username>:<password>
https://<host>:<management_port>/services/data/inputs/tcp/splunktcptoken/<token_name>/disable
```

Delete a token

To remove a token using the REST API, use the following command:

```
curl -v -k -X "DELETE" -u <username>:<password>
https://<host>:<management_port>/services/data/inputs/tcp/splunktcptoken/<token_name>
```

List tokens

To receive a list of configured tokens using the REST API, use the following command:

```
curl -v -k -u <user>:<password> https://<host>:<management_port>/services/data/inputs/tcp/splunktcptoken
```

Configure the forwarder with a token

Add the token value to the forwarder's outputs.conf under the `[tcpout]` stanza to configure authentication with an indexer.

1. Edit the outputs.conf for the forwarder and add the `token` value under the `[tcpout]` stanza:

   ```
   [tcpout]
   server=idx1.mycompany.com:9997
   token = <token_value>
   ...
   ```
2. Restart the forwarder services.

Confirm that the forwarder and indexer can communicate using the tokens

When you configure a forwarder with a token, the communication process with the indexer becomes:

- The forwarder connects to the indexer.
- The indexer requests authentication.
- The forwarder provides the token to the indexer.
- The indexer compares the token it received with the token it has.
- If the tokens match, the indexer accepts the TCP connection and sets up the data stream. If the tokens do not match, the indexer rejects the connection and logs an entry in the `splunkd.log`.

A forwarder without the correct token value for an indexer cannot forward data to that indexer.

Common error messages

A forwarder that does not have the correct token generates this event in `splunkd.log`:

```
ERROR TcpInputProc - Exception: Token sent by forwarder does not match configured tokens
src=127.0.0.1:58798! for data received from src=127.0.0.1:58798
```

A forwarder that does not submit a token to an indexer with a token enabled generates this event in `splunkd.log`:

```
ERROR TcpInputProc - Invalid S2S token=Token not sent by forwarder for data received from
src=127.0.0.1:58796
```

Troubleshoot the universal forwarder

Troubleshoot the universal forwarder

See common Splunk Universal Forwarder errors and how to fix them. For more troubleshooting information, check out the Splunk Community.

Warning appears in the universal forwarder when you run an SPL command

When you run an SPL command in the universal forwarder, the following messages may appear:

- Warning: Attempting to revert the SPLUNK_HOME ownership
- Warning: Executing "chown -R splunk /opt/splunkforwarder".

These warning do not affect functionality and can be ignored.

Splunk isn't receiving data from the universal forwarder

1. In the indexer user interface, go to **forwarding and receiving**, or go to inputs.conf.
2. Identify or select a port in **Received Data** to listen to. Make sure it is the same port set in outputs.conf for the forwarder to send data to. See Configure the universal forwarder using configuration files. Usually, the port 9997 splunktcp is preferred.
3. Check that the destination host for your indexers, including the IP address and hostname, is correct in outputs.conf.
4. After configuring your change, restart your Universal Forwarder. See Start or stop the Universal Forwarder.

Splunk is only receiving "\x00\" data

1. Go to your indexer user interface.
2. Ensure you are receiving data from **Forwarding and receiving** in indexer settings, and not **Data inputs -> TCP/UDP**.

Ingestion lagging

The most common cause of ingestion lagging is that you are taking in too much data from one sourcetype, which is blocking data from other sourcetypes. You can solve this by shortening your data ingestion intervals using the universal forwarder user interface, or inputs.conf.

Problems running 9.1 with older versions of indexers

Version 3 of the Splunk-to-Splunk protocol is deprecated as of version 9.0.0. If you use version 3 of the Splunk-to-Splunk protocol by setting negotiateProtocolLevel=0, then by default the forwarder switches to the latest Splunk-to-Splunk protocol in order to connect with other Splunk platform instances. The forwarder will also then generate warning logs.

Here are some example warning logs:

```
10-05-2022 21:14:48.078 +0000 WARN AutoLoadBalancedConnectionStrategy
[10422 TcpOutEloop] - Forwarder configured to use protocol level=0,
which is no longer supported, will use the lowest supported protocol level=1
```

```
10-05-2022 21:14:48.078 +0000 WARN AutoLoadBalancedConnectionStrategy
[10422 TcpOutEloop] - Indexer configured to use protocol level=0,
which is no longer supported, will use the lowest supported protocol level=1
```

To enable version 3 of Splunk-to-Splunk protocol, add `enableOldS2SProtocol = true` into the outputs.conf in the top [tcpout] stanza:

```
[tcpout]
enableOldS2SProtocol = true
```

Release Notes

Known issues

This topic lists known issues that are specific to the universal forwarder. For information on fixed issues, see Fixed issues.

Universal forwarder issues

Date filed	Issue number	Description
2024-10-24	SPL-265068, SPL-266372, SPL-266374, SPL-266375, SPL-266377	UF Windows installer re-grant user privileges during upgrade

2024-09-27	SPL-263518	Upgrade removes group=per_(source|sourcetype|index|host)_thruput in metrics.log for universalforwarders.
		
		Workaround:
		------ON UF ONLY-------
		
		in default-mode.conf add following line
		
		`#Turn off a processor`
		`[pipeline:indexerPipe]`
		`disabled_processors= index_thruput, indexer, indexandforward, latencytracker, diskusage, signing,tcp-output-generic-processor, syslog-output-generic-processor, http-output-generic-processor, stream-output-processor, s2soverhttpoutput, destination-key-processor`

2024-04-19	SPL-254532, SPL-265719, SPL-265720, SPL-265721, SPL-265722, SPL-265723, SPL-265724, SPL-265725, SPL-265726, SPL-265892, SPL-265908	UF 9.1.2 Windows Security events stop forwarding when Windows event log service is restarted Workaround: Restart the UF
2022-08-17	SPL-228646, SPL-228645	Restart is needed when AWS access key pairs rotate (w/o grace period) or other S3 config settings for Ingest Actions become invalid
2022-06-23	SPL-226019	Warning appears in the universal forwarder whenever any spl command is run: Warning: Attempting to revert the SPLUNK_HOME ownership Warning: Executing "chown -R splunk /opt/splunkforwarder". This warning is expected and will not affect functionality.
2022-03-23	SPL-221239	System Introspect App fails when universal forwarder is installed at non-admin user

Fixed issues

The following issues were fixed in releases of the universal forwarder.

9.4.0

Version 9.4.0 was released on December 16, 2024. This release fixes the following universal forwarder issues:

Universal forwarder issues

Date resolved	Issue number	Description
2025-03-12	SPL-248479, SPL-253092	Forwarders enter a state of constant blocking, and Splunk Cloud indexers might fail to process events. This can result in the events being sent to a non-searchable queue, the Dead Letter Queue (DLQ), due to a Persistent Queue issue with the S2S protocol

If no issues are shown, there are no new Universal Forwarder specific fixes to highlight in this version.

Third-party software

Some of the components included in the universal forwarder are licensed under free or open source licenses. We wish to thank the contributors to those projects. See the Splunk Enterprise third-party software notices.