# Splunk Enterprise System Administration

# Document Usage Guidelines

- Should be used only for enrolled students
- Not meant to be a self-paced document, an instructor is needed
- Do not distribute


Copyright © 2023 Splunk, Inc. All rights reserved

# Course Prerequisites

- **Either** the following courses:
  - What is Splunk?
  - Intro to Splunk
  - Using Fields
  - Introduction to Knowledge Objects
- **Or** the following courses:
  - Splunk Fundamentals 1 & 2


Copyright © 2023 Splunk, Inc. All rights reserved

# Course Goals

- Identify Splunk components and understand the basics of a Splunk deployment
- Monitor Splunk operations and licensing
- Explore Splunk configuration files
- Install a Splunk app
- Create and manage Splunk indexes
- Create users and roles in Splunk
- Configure distributed search


Copyright © 2023 Splunk, Inc. All rights reserved

# Course Outline

Module 1: Deploying Splunk

Module 2: Monitoring Splunk

Module 3: Licensing Splunk

Module 4: Using Configuration Files

Module 5: Using Apps

Module 6: Creating Indexes

Module 7: Managing Indexes

Module 8: Managing Users

Module 9: Configuring Basic Forwarding

Module 10: Configuring Distributed Search


Copyright © 2023 Splunk, Inc. All rights reserved

# System Administrator versus Data Administrator

## Splunk System Administrator

*System Management*

- Install, configure, and manage Splunk components
- Monitor Splunk operations using the health report and Monitoring Console
- Manage Splunk licensing
- Manage Splunk configuration files
- Install and manage Splunk apps
- Create and manage Splunk indexes
- Manage Splunk user authentication
- Configure Distributed Search

## Splunk Data Administrator

*Data Onboarding and Management*

- Work with users requesting new data sources
- Document existing and newly ingested data sources
- Design and manage inputs from forwarders to capture data
- Manage parsing, event line breaking, timestamp extraction
- Manage Splunk configuration files
- Move configuration through non-production testing as required
- Deploy changes to production


Copyright © 2023 Splunk, Inc. All rights reserved

# Module 1:
# Deploying Splunk


Copyright © 2023 Splunk, Inc. All rights reserved

# Module Objectives

- Provide an overview of Splunk
- Identify Splunk Enterprise components and deployment types
- List Splunk installation prerequisites
- List the steps to install Splunk
- Use Splunk CLI commands
- Explore security best practices


Copyright © 2023 Splunk, Inc. All rights reserved

# Splunk Overview

- Splunk can be deployed in a variety of configurations
- Scales from a single server to a distributed infrastructure
- Four stages of Splunk include:
  - **Input** any text data
  - **Parse** the data into events
  - **Index** and store events
  - **Search** and report

Copyright © 2023 Splunk, Inc. All rights reserved

# Simple Test Server

- Deploying a single, standalone server
  - All functions in a single Splunk instance
  - The result when you download and install Splunk with default settings
- Recommended use:
  - For testing, proof of concept, personal use, and learning
  - Consider having at least one test / development setup at your site

**Note**

This is the initial configuration in class.


Copyright © 2023 Splunk, Inc. All rights reserved | 9 May 2023

# Single Server with Inputs

- Deploying a basic Splunk server
  - Similar to standalone configuration
  - Manage deployment of forwarder configurations
- Deploying Forwarders
  - Install Splunk forwarder at data source (usually production servers)
  - Collect data and send it to Splunk servers

**Note**

Your lab environment evolves to include a separate forwarder.


Copyright © 2023 Splunk, Inc. All rights reserved | 9 May 2023

# Distributed Non-Cluster Environment

- Scale Splunk in various ways
  - Add indexers to handle more inputs
  - Add indexers and search heads to handle more searching

**Note**

You will add a single indexer (search peer) to your environment in a later lab exercise.


Copyright © 2023 Splunk, Inc. All rights reserved

# Distributed Non-Cluster Environment (2)

- Centralize management using dedicated servers for various functions including:
  - Deployment server for forwarder management
  - License Manager
  - Monitoring Console

**Note**

Deployment server management is covered in the *Splunk Enterprise Data Administration* course.


Copyright © 2023 Splunk, Inc. All rights reserved

# Splunk Clustered Environment

- Search head clustering
  - Replicates knowledge objects
- Indexer clustering
  - Replicates data across indexers
  - Single-site or multi-site
  - Allows balance of growth, speed of recovery, and overall disk usage
- Does not require additional licenses
- Discussed in the *Splunk Cluster Administration* class

Copyright © 2023 Splunk, Inc. All rights reserved

# Splunk Core Components and Processes

- Allow users to submit search requests using SPL
- Distribute search requests to the indexers
- Consolidate results and render visualizations of results
- Store search-time knowledge objects (such as field extractions, alerts, and dashboards)

- Receive incoming data from forwarders
- Index and store data in Splunk indexes
- Search data in response to requests from search heads

- Monitor configured inputs and forward the data to the indexers (best practice data collection method)
- Requires minimal resources and typically installed on the machines that produce the data

- Centralizes configuration management for various functions including clustering, licensing, and clients
- Requires systems running Splunk Enterprise

Copyright © 2023 Splunk, Inc. All rights reserved

# Splunk Installation Overview

## Deployment planning

- Splunk Enterprise
- Universal Forwarder

## Pre-installation

- Recommended hardware
- Network ports
- Linux settings
- Time sync
- Startup account

## Installation

- Download
- Installation methods
- Directory structure

## Post-installation

- Run Splunk at boot
- Configure Splunk settings
- Enable Monitoring Console (optional)


Copyright © 2023 Splunk, Inc. All rights reserved

# Software in Splunk Enterprise packages

**Splunk Enterprise** package

**Universal Forwarder** package

Note

The System Administrator is responsible for installing and configuring Splunk components.



Copyright © 2023 Splunk, Inc. All rights reserved

# Server Hardware Recommendations

| Component | Indexer | Search Head |
|---|---|---|
| OS | Linux or Windows 64-bit distribution | |
| Network | 1Gb Ethernet NIC (optional 2nd NIC for a management network) | |
| Memory | 12-128 GB RAM | 12 GB RAM |
| CPU | x86 64-bit chip architecture<br>**12-48 CPU cores** or **24-96 vCPU** (2+ GHz) | x86 64-bit chip architecture<br>**16 CPU cores** or **32 vCPU** (2+ GHz) |
| Disk | Disk subsystem capable of **800+ IOPS**<br>SSD subsystem for hot/warm buckets | 2 x 10K RPM 300GB SAS drives, or better |

- For more detailed information:
  - Attend the *Architecting and Deploying Splunk* class
  - docs.splunk.com/Documentation/Splunk/latest/Capacity/Referencehardware
  - docs.splunk.com/Documentation/Splunk/latest/Installation/Systemrequirements


Copyright © 2023 Splunk, Inc. All rights reserved

# Splunk Default Network Ports

| Usage | Splunk Enterprise | Universal Forwarder |
|---|---|---|
| **splunkd** | **8089** | **8089** |
| Splunk Web | **8000** | - |
| Web app-server proxy | **8065** | - |
| KV Store | **8191** | - |
| S2S receiving port(s) | No default | No default |
| Any network/http input(s) | No default | No default |
| Index replication port(s) | No default | - |
| Search replication port(s) | No default | - |


Copyright © 2023 Splunk, Inc. All rights reserved

# Linux Setting Recommendations

- Setting system resource limits
  - Use **`ulimit -a`** to view settings
  - Increase parameters on indexers and search heads, for example:
    - File descriptors (**`ulimit -n`**) >= 64k, based on buckets and searches
    - Max user processes (**`ulimit -u`**) >= 16k, based on forwarders / concurrent searches
    - Set in configuration files, according to whether Linux is **`initd`** or **`systemd`** -based
  - docs.splunk.com/Documentation/Splunk/latest/Troubleshooting/ulimitErrors
  - docs.splunk.com/Documentation/Splunk/latest/Installation/Systemrequirements
- Turn Transparent Huge Pages (THP) off on Splunk Enterprise servers
  - docs.splunk.com/Documentation/Splunk/latest/ReleaseNotes/SplunkandTHP

```
# ulimit -a
core file size          (blocks, -c) 0
data seg size           (kbytes, -d) unlimited
scheduling priority             (-e) 0
file size               (blocks, -f) unlimited
pending signals                 (-i) 30646
max locked memory       (kbytes, -l) 64
max memory size         (kbytes, -m) unlimited
open files                      (-n) 8192
...
cpu time               (seconds, -t) unlimited
max user processes              (-u) 30646
```


Copyright © 2023 Splunk, Inc. All rights reserved

# Time Synchronization

- Ensure a standardized time configuration on Splunk servers
  - Splunk searches depend on accurate timestamps on events
  - Clock skew between hosts can affect search results
  - Popular protocol is NTP (Network Time Protocol)

splunk> Best Practice


Copyright © 2023 Splunk, Inc. All rights reserved

# Startup Account

- Do not run Splunk as ***super-user***

| | |
|---|---|
| ***NIX** | • Avoid the **root** account |
| **Windows** | • Avoid the **administrator** account<br>• Use a domain account if Splunk must connect to other servers<br>• Alternatively, use a local machine account that can run services |

- Splunk user account must:
  - Read files and directories configured for monitoring by Splunk
    - *NIX: **`/var/log`** is not typically open to non-root accounts
  - Write to the Splunk Enterprise directory (**`SPLUNK_HOME`**)
  - Execute any scripts required (alerts or scripted input)
  - Bind to the network ports Splunk is listening on
    - *NIX: non-root accounts cannot access reserved ports (< 1024)

splunk> Best Practice


Copyright © 2023 Splunk, Inc. All rights reserved

# Installing Splunk Enterprise Server

| | *NIX | Windows |
|---|---|---|
| *Download* | https://www.splunk.com/download | |
| *Install* | • Un-compress **`.tar.gz`** file in the path you want Splunk to run from<br>• Also available as rpm, deb<br>• Default **`SPLUNK_HOME`**: **`/opt/splunk`** | • Execute the **`.msi`** installer and follow the wizard steps<br>• Default **`SPLUNK_HOME`**: **`C:\Program Files\Splunk`** |
| *Post-Install* | • Splunk starts manually<br>• Enable **`boot-start`** to have Splunk start automatically | Splunk starts automatically |

Installation instructions at:
docs.splunk.com/Documentation/Splunk/latest/Installation/Chooseyourplatform


Copyright © 2023 Splunk, Inc. All rights reserved

# Installing Splunk Enterprise on *nix

```
# tar -zxvf ~/splunk-9.0.0-6818ac46f2ec-Linux-x86_64.tgz -C /opt
# /opt/splunk/bin/splunk start --accept-license --answer-yes
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: admin
Password must contain at least:
   * 8 total printable ASCII character(s).
Please enter a new password: xxxxxxxx
Please confirm new password: xxxxxxxx
...
Waiting for web server at http://127.0.0.1:8000 to be available..... Done
...
The Splunk web interface is at http://hostname:8000

#
```


Copyright © 2023 Splunk, Inc. All rights reserved

# Installing Splunk Enterprise on Windows

1

splunk-9.0.0-6818ac46f2ec-x64-release.msi

2

3

4

5

Copyright © 2023 Splunk, Inc. All rights reserved

# Splunk Directory Structure

**Note**

**$SPLUNK_HOME** is used in Splunk documentation as a placeholder for "*the top directory where Splunk is installed*", **not** as an exported environment variable. In this training **SPLUNK_HOME** is used.

**Note**

**SPLUNK_DB** by default refers to **SPLUNK_HOME/var/lib/splunk**



Copyright © 2023 Splunk, Inc. All rights reserved

# Running Splunk at Boot

## Splunk on *NIX

- Does not auto-start at boot time, by default
- Enable auto-start on **`init.d`** -based distributions:

```
# splunk enable boot-start -user username
```

- Enable auto-start on **`systemd`** -based distributions:

```
# splunk enable boot-start -user username -systemd-managed 1
```

**Note**

Splunk best practice is to run Splunk Enterprise as a non-root user.

## Splunk on Windows

- Configured to auto-start at boot time by the installer
- Runs as **`splunkd`** services, and starts child processes
- Managed as any Windows service (can be set to Manual or Disabled)

docs.splunk.com/Documentation/Splunk/latest/admin/ConfigureSplunkToStartAtBootTime


Copyright © 2023 Splunk, Inc. All rights reserved

# The **splunkd** Process

- Runs on port 8089 (default) using SSL
- Spawns and controls Splunk child processes (helpers)
  - Splunk Web proxy, KV store, and Introspection services
  - Each search, scripted input, or scripted alert
- Accesses, processes, and indexes incoming data
- Handles all search requests and returns results
- Viewed using the **splunk status** command:

```
# splunk status
splunkd is running (PID: 2128).
splunk helpers are running (PIDs: 2135 2148 2205 2266).
```


Copyright © 2023 Splunk, Inc. All rights reserved

# Splunk Web

- Browser-based user interface
- Provides a search and management front end for **`splunkd`** process
- Found at **`http://<server_name>:<port>`** (default port 8000)

Copyright © 2023 Splunk, Inc. All rights reserved

# Splunk Web – Server Settings

Select **Settings** > **Server settings** > **General settings**

Used to set server configuration and server options



Copyright © 2023 Splunk, Inc. All rights reserved

# Describing General Settings

Copyright © 2023 Splunk, Inc. All rights reserved

# Describing General Settings – Splunk Web

**Splunk Web**

| | |
|---|---|
| Run Splunk Web | (●) Yes ( ) No |
| Enable SSL (HTTPS) in Splunk Web? | (●) Yes ( ) No |
| Web port * | 8000 |
| App server ports | 8065 |
| | Port number(s) for the python-based application server to listen on. Use comma-separated list to specify more than one port number. |
| Session timeout * | 1h |
| | Set the Splunk Web session timeout. Use the same notation as relative time modifiers, for example 3h, 100s, 6d. |


Copyright © 2023 Splunk, Inc. All rights reserved

# Describing General Settings – Index/KV Store

**Index settings**

Default host name: splunk01

Sets the host field value for all events coming from this serve

Path to indexes: /opt/splunk/var/lib/splunk

Pause indexing if free disk space (in MB) falls below *: 5000

**KV Store**

Port *: 8191

Port that splunkd uses to connect to the KV Store server.

Cancel | Save

Default **host** field for inputs forwarded from this server

Path to the existing indexes: **SPLUNK_DB** (read-only in UI)

Minimum free disk space required or Splunk pauses indexing



Copyright © 2023 Splunk, Inc. All rights reserved

# Restarting the Server from Splunk Web

**Note**

Any changes to **General** settings generate a message. Clicking the indicator opens a message, prompting you to restart.

You can also restart by:

- Selecting **Settings** > **Server controls**
- Using CLI: **`splunk restart`**



Copyright © 2023 Splunk, Inc. All rights reserved

# Splunk Command Line Interface (CLI)

- Executable command (**splunk**) in the **SPLUNK_HOME/bin** directory
- Uses the same syntax on all supported platforms:

| Command | Operation |
|---|---|
| **splunk help** | Display a usage summary |
| **splunk help <object>** | Display the details of a specific object |
| **splunk [start \| stop \| restart]** | Starts and stops the Splunk processes |
| **splunk start --accept-license** | Automatically accept the license without prompt |
| **splunk status** | Display the Splunk process status |
| **splunk show splunkd-port** | Show the port that the **splunkd** listens on |
| **splunk show web-port** | Show the port that Splunk Web listens on |
| **splunk show servername** | Show the server name of this instance |
| **splunk show default-hostname** | Show the default host name used for all data inputs |


Copyright © 2023 Splunk, Inc. All rights reserved

# Basic Security for Splunk Admins

- Change administrator passwords routinely
- Run Splunk with the appropriate user account and roles
- Exercise caution when setting permissions for Splunk users
- Disable **`splunkd`** port **`8089`** on Splunk 8.x Universal Forwarders
- Use a host firewall
- Secure Splunk to Splunk communication
- Replace the default certificates


Copyright © 2023 Splunk, Inc. All rights reserved

# Splunk Security 9.0 Improvements

**New Security Features**

3

Splunk Assist
Upgrade Readiness App
Native Smart Card Auth

**No-action Needed Fixes**

65

Secure by default.
Automatically implemented:
**enforcement mode**

**Action-required Advisories***

8

Require proactive steps to work. Mostly in **warning mode**

** For June 2022*


Copyright © 2023 Splunk, Inc. All rights reserved

# Splunk 9.0 Updates – No Action Needed

- Improved dashboard security with sanitization on input fields
- Increased admin control with greater Splunk roles and capabilities with restriction options
- Updates to third party packages
  - Node.js
  - OpenSSL
- Easier risk management with user-friendly SPL safeguards
- Role-based filtering

Copyright © 2023 Splunk, Inc. All rights reserved

# Splunk 9.0 Updates – Action Required

- Configure any action-required procedures:
  docs.splunk.com/Documentation/Splunk/latest/Security/Updates

## Summary of changes

The following table lists a summary of the changes, the Splunk platforms on which the changes ship, the enforcement mode in which they currently operate, and links to procedures on how to configure Splunk software to enforce the changes.

| Change | Description | Introduced in | Addresses | Current mode | Learn more |
|---|---|---|---|---|---|
| TLS certificate host name validation | Splunk platform instances verify the hostname in the TLS certificate they receive when they connect to other Splunk platform instances. | Splunk Cloud Platform (SCP) 8.2.2202, Splunk Enterprise (SE) 9.0 | SVD-2022-0602, SVD-2022-0603 | Warning | Learn more |
| Python module TLS connection hardening | Python modules on Splunk platform instances always validate TLS connections. | SCP 8.2.2202, SE 9.0 | SVD-2022-0601 | Warning | Learn more |
| TLS certificate host name validation using Splunk CLI | The Splunk Command Line Interface (CLI) validates TLS certificates for any connections it makes to other Splunk platform instances. | SCP 8.2.2203, SE 9.0 | SVD-2022-0606 | Warning | Learn more |
| Universal forwarder security | Universal forwarders always validate connections from | SE 9.0 | SVD-2022-0605 | Enforcement | Learn more |


Copyright © 2023 Splunk, Inc. All rights reserved

# Splunk Security Resources

- Splunk Docs: Product Security page
  www.splunk.com/en_us/product-security.html

Subscribe to receive information on security announcements

- Splunk Docs: Security Update Documentation
  docs.splunk.com/Documentation/Splunk/latest/Security/Updates
- Splunk Lantern: Upgrading Splunk Enterprise
  lantern.splunk.com/Splunk_Platform/Product_Tips/Enterprise/Upgrading_Splunk_Enterprise
- Appendix A: Security Fundamentals


Copyright © 2023 Splunk, Inc. All rights reserved

# More Resources

| | |
|---|---|
| Splunk Documentation | http://docs.splunk.com/Documentation |
| Splunk App Repository | http://splunkbase.splunk.com/ |
| Splunk Community | http://community.splunk.com/ |
| Splunk Blogs | http://www.splunk.com/blog/ |
| Splunk Lantern | http://lantern.splunk.com/ |
| Splunk User Groups | http://usergroups.splunk.com/ |


Copyright © 2023 Splunk, Inc. All rights reserved

# Question: Installing a Search Head

Which Splunk installation package is used to install the Search Head?

A. Splunk Search Head installation package

B. Splunk Enterprise installation package

C. Splunk Heavy Forwarder installation package

D. Splunk Universal Forwarder installation package


Copyright © 2023 Splunk, Inc. All rights reserved

# Answer: Installing a Search Head

Which Splunk installation package is used to install the Search Head?

A. Splunk Search Head installation package

**B. Splunk Enterprise installation package**

C. Splunk Heavy Forwarder installation package

D. Splunk Universal Forwarder installation package

The Splunk Enterprise installation package can be used to install most Splunk server components. The Universal Forwarder (UF) installation package is a lighter version of Splunk that is simply used to forward data to indexers. The other options are not existing packages.


Copyright © 2023 Splunk, Inc. All rights reserved

# Question: Automatic boot start

Which of the following operating systems configures Splunk to boot-start automatically by default?

A. Windows only

B. Linux only

C. Both Windows and Linux

D. Neither Windows and Linux


Copyright © 2023 Splunk, Inc. All rights reserved

# Answer: Automatic boot start

Which of the following operating systems configures Splunk to boot-start automatically by default?

**A. Windows only**

B. Linux only

C. Both Windows and Linux

D. Neither Windows and Linux

On Windows, Splunk is set to start automatically on boot. On Linux, you must manually run a version of the **`splunk enable boot-start`** command.


Copyright © 2023 Splunk, Inc. All rights reserved

# Question: Default install path

What is the default installation path for Splunk (also known as **`SPLUNK_HOME`**) on Linux?

A. `/opt/splunk`
B. `/var/splunk`
C. `/opt/splunk/etc/var/lib`
D. `/opt/splunk_home`


Copyright © 2023 Splunk, Inc. All rights reserved

# Answer: Default install path

What is the default installation path for Splunk (also known as **`SPLUNK_HOME`**) on Linux?

A. **`/opt/splunk`**

B. `/var/splunk`

C. `/opt/splunk/etc/var/lib`

D. `/opt/splunk_home`

On Linux, the default Splunk installation path (**`SPLUNK_HOME`**) is **`/opt/splunk`**. The default Splunk database path (**`SPLUNK_DB`**) where indexes are stored is **`/opt/splunk/etc/var/lib`**.


Copyright © 2023 Splunk, Inc. All rights reserved

# Question: **`splunkd`** port number

Which of the following port numbers is associated with the **`splunkd`** process by default?

A. `8000`

B. `8088`

C. `8089`

D. `9997`



Copyright © 2023 Splunk, Inc. All rights reserved

# Answer: **`splunkd`** port number

Which of the following port numbers is associated with the **`splunkd`** process by default?

A. `8000`

B. `8088`

C. **`8089`**

D. `9997`

Port **`8089`** is used by **`splunkd`** by default.

Port **`8000`** is the default for Splunk Web, and port **`9997`** is often used as a Splunk listening port.


Copyright © 2023 Splunk, Inc. All rights reserved

# Module 1 Lab

**Time:** 15 minutes

**Description:** Configure a Splunk Server

**Tasks:**

- Log into Splunk Web
- Change Splunk server name
- Restart Splunk
- Use command line (CLI) to confirm the status and changes


Copyright © 2023 Splunk, Inc. All rights reserved

# Module 2: Monitoring Splunk


Copyright © 2023 Splunk, Inc. All rights reserved

# Module Objectives

- Use Splunk Health Report
- Enable and use the Monitoring Console (MC)
- Use Splunk Assist
- Use Splunk Diag and Rapid Diag


Copyright © 2023 Splunk, Inc. All rights reserved

# Options for Monitoring Splunk

## Third Party Monitoring

- Not Splunk supported
- Requires integration

## Splunk Alerts & Health Report

- Splunk supported
- Used for monitoring
- Create alerts for each use case

## Splunk Observability

- Splunk supported
- Used for observability
- Create alerts for each use case

## Monitoring Console (MC)

- Splunk supported
- Default dashboards, health checks, and alerts
- Available for Splunk Enterprise and Splunk Cloud


Copyright © 2023 Splunk, Inc. All rights reserved

# Viewing Splunk Health Report

Copyright © 2023 Splunk, Inc. All rights reserved

# Interpreting Health Reports

## Health of Splunk Deployment

- splunkd
  - File Monitor Input
    - BatchReader-0
    - Ingestion Latency
    - TailReader-0
  - Index Processor
    - Buckets
    - Disk Space
    - Index Optimization
  - Indexer Clustering
    - Cluster Bundles
    - Data Durability
    - Data Searchable
    - **Indexers**
    - Indexing Ready

### Indexers

- **Root Cause(s):**
  - The following peers are in ManualDetention status: fool15.sv.splunk.com. This will cause those peers to not accept any data.
- **Unhealthy Instances**
  - fool20.sv.splunk.com

  Generate Diag
- **Last 50 related messages:**
  - 05-06-2021 09:44:13.460 -0700 INFO CMMaster [13103 CMMasterServiceThread] - Sending queued frozen notifications to guid=CD6C111F-1468-4DF2-97C5-545882D94FA2 numIds=1
  - 05-06-2021 09:44:13.460 -0700 INFO CMMaster [13103 CMMasterServiceThread] - Sending queued frozen notifications to guid=25A63B8E-2BFF-4C4F-B986-E04D5B0926D6 numIds=1
  - 05-06-2021 09:44:13.460 -0700 INFO CMMaster [13103 CMMasterServiceThread] - Sending queued frozen notifications to guid=E2F42B5C-D4DE-4465-A296-483311FA4A39 numIds=1


Copyright © 2023 Splunk, Inc. All rights reserved

# Customizing with Health Report Manager

splunk>enterprise Apps Admini... Messages Settings Activity Help Find

Settings > Health Report Manager

## Features

Manage Alerts

Set feature thresholds to determine how Splunk Health Report monitors Splunk components. Threshold values are local to the node. For features related to Search Head Clusters, values are replicated across peers. For more information, refer to our Documentation.

34 Features filter Legend 20 per page < Prev 1 2 Next >

| Name | Actions | Alert Status |
|---|---|---|
| feature:batchreader | Edit Snooze | Enabled |
| feature:buckets | Edit Snooze | Enabled |
| feature:cluster_bundles | Edit Snooze | Enabled |
| feature:data_durability | Edit Snooze | Enabled |
| feature:data_searchable | Edit Snooze | Enabled |
| feature:ddaa_archived_buckets | Edit Snooze | Enabled |
| feature:disk_space | Edit Snooze | Enabled |

**Edit** thresholds and **Snooze** alerts



Copyright © 2023 Splunk, Inc. All rights reserved | 9 May 2023

# Monitoring Console (MC)

A Splunk admin-only app used to monitor and investigate data Splunk collects about itself, such as performance and resource usage

**Note**

You will use MC to monitor your activities as you learn more about Splunk components.


Copyright © 2023 Splunk, Inc. All rights reserved

# Content to Monitor in the MC

**Search**

- Scheduler
- Search activity
- Replication
- KV Store

**Indexing**

- License usage
- Inputs
- SmartStore
- Volumes

**Resources**

- Memory
- Disk
- CPU

**Forwarders**

- Status
- Event counts

**Instances**

- Status
- Health Check


Copyright © 2023 Splunk, Inc. All rights reserved

# Planning for MC in Standalone Mode

- Used on an all-in-one server
  - Runs in **standalone** mode
- Not recommended to run in **standalone** mode for distributed production environments

Copyright © 2023 Splunk, Inc. All rights reserved

# Configuring MC in Standalone Mode

- Runs un-configured in standalone mode by default
- To enable:
  1. Choose **Settings > General Setup**
  2. Select **Mode: Standalone**
  3. **Apply Changes**

Copyright © 2023 Splunk, Inc. All rights reserved

# Planning for MC In Distributed Mode

- Used in a distributed environment
  - Runs in **distributed** mode
- Recommended on its own system
- Same requirements as a Search Head
- Can run on a shared instance only:
  - With a License Manager
  - With a Deployment Server (< 50 clients)
  - With an indexer Cluster Manager node (depending on load)

Copyright © 2023 Splunk, Inc. All rights reserved

# Configuring MC in Distributed Mode

- To enable: 1. **Settings > General Setup**, select 2. **Mode: Distributed**, 3. **Continue**, then 4. **Apply Changes**
- Requires other Splunk Enterprise instances to be configured as distributed search peers to the MC

Copyright © 2023 Splunk, Inc. All rights reserved

# Adding Splunk Instances to the MC

- Repeat for each Search Head, Deployment Server, License Manager, and non-clustered Indexer:
  1. Splunk Web on MC: **Settings > Distributed search > Search peers**
  2. Click **New Search Peer**
  3. Fill in fields and **Save**
- Do not add clustered indexers
  - Discussed in the *Splunk Cluster Administration* course

Copyright © 2023 Splunk, Inc. All rights reserved

# Configuring Monitored Server Roles

Overview | Summary | Health Check | Instances | Indexing ▾ | Search ▾ | Resource Usage ▾ | Forwarders ▾ | Settings ▾ | Run a Search | Monitoring Console

1

- ✓ General Setup
- Forwarder Monitoring Setup
- Alerts Setup
- Overview Preferences
- Health Check Items

## Setup

Current topology of Splunk Enterprise deployment. Learn more

Mode: Standalone | Distributed

### This instance

| Instance (host) | Instance (serverName) | Machine | Server roles | Custom groups | Indexer Cluster(s) | Search Head Cluster(s) | Monitoring | Sta |
|---|---|---|---|---|---|---|---|---|
| MC1.example.com | MC1.example.com | ip-10-0-0-205 | Deployment Server<br>KV Store<br>License Master | | | | ✓ Enabled | |

### Remote instances

3 Instances | filter

Edit Selected Instances ▾ | 25 Per Page ▾

| Instance (host) | Instance (serverName) | Machine | Server roles | Custom groups | Indexer Cluster(s) | Search Head Cluster(s) | Monitoring | State | Problems | Actions |
|---|---|---|---|---|---|---|---|---|---|---|
| IDX1.example.com | IDX1.example.com | ip-10-0-0-202 | Indexer<br>KV Store | | | | ✓ Enabled | Configured | | Edit ▾ |
| IDX2.example.com | IDX2.example.com | ip-10-0-0-203 | Indexer<br>KV Store | | | | ✓ Enabled | Configured | | Edit ▾ |
| SH1.example.com | SH1.example.com | ip-10-0-0-201 | KV Store<br>Search Head | | | | ✓ Enabled | Configured | | Edit ▾ |

2

### Edit Server Roles

SH1.example.com

- Search Head ☑
- Cluster Master ☐
- License Master ☐
- Indexer ☐
- Deployment Server ☐
- KV Store ☑
- SHC Deployer ☐

Cancel | Save



Copyright © 2023 Splunk, Inc. All rights reserved 

# Enabling MC Platform Alerts

- Timely notification of critical conditions helps effectively operate the Splunk environment
- MC **Alerts Setup** provides preconfigured platform alerts
  - Disabled by default
  - Customizable alert schedule, suppression time, and alert actions

Disabled by default


Copyright © 2023 Splunk, Inc. All rights reserved

# MC Health Check

- Series of ad hoc searches that run sequentially:
  - **Monitoring Console > Health Check**
- Comes preconfigured but can be disabled, modified, created, and exported using:
  - **Settings > Health Check Items**

| Check | Category | Tags | Results |
|---|---|---|---|
| System hardware provisioning assessment | System and Environment | best_practices, capacity, scalability | One or more hosts has returned CPU or |
| Assessment of server ulimits | System and Environment | best_practices, operating_system | One or more Splunk instances are runni |
| Event-processing issues | Data Collection | event_breaking, indexing, timestamp_extraction | This health check item was successful. |
| Expiring or expired licenses | Data Indexing | licensing | This health check item was successful. |
| Indexing status | Data Indexing | buckets, indexing | This health check item was successful. |
| License warnings and violations | Data Indexing | indexing, licensing | This health check item was successful. |
| Saturation of event-processing queues | Data Indexing | indexing, queues | This health check item was successful. |
| Search scheduler skip ratio | Data Search | scheduler, searches_skipped | This health check item was successful. |
| Excessive physical memory usage | Splunk Miscellaneous | resource_usage | This health check item was successful. |
| Integrity check of installed files | Splunk Miscellaneous | configuration, installation | This health check item was successful. |
| KV Store status | Splunk Miscellaneous | kv_store | This health check item was successful. |
| Orphaned scheduled searches | Splunk Miscellaneous | configuration, search, searches_skipped | This health check item was successful. |
| Near-critical disk usage | System and Environment | capacity, disk_space, searches_skipped, storage | This health check item was successful. |
| Linux kernel transparent huge pages | System and Environment | best_practices, operating_system | This health check item was successful. |
| Missing forwarders | Data Indexing | batchreader, forwarding, tailreader | This health check item is not applicable |


Copyright © 2023 Splunk, Inc. All rights reserved

# Splunk Assist

- Cloud-connected service for Splunk Enterprise and Cloud
- Generates insights in real time
- Uses helper packages:
  - AppAssist
  - CertAssist
  - ConfigAssist
- Leverages telemetry data
- Operates as part of the MC (starting in Splunk 9.0)

Copyright © 2023 Splunk, Inc. All rights reserved

# What is a Splunk Diag?

- Gathers data and provides insight to your instance

| | |
|---|---|
| **Server specs** | Configuration, OS version, file system, and current open connections |
| **Splunk platform** | Contents of **`SPLUNK_HOME/etc`** such as app configurations, Splunk log files, and index metadata |

- Produces a **`tar.gz`** file and **`diag.log`**
- Does not retrieve customer or index data
  - Examine the file to ensure no proprietary data is included
- Can be Splunked!
  - Ingest the compressed file to view the information in Splunk


Copyright © 2023 Splunk, Inc. All rights reserved

# Diag Example

```
$ ./splunk diag
Collecting components: conf_replication_summary, consensus, dispatch, etc, file_validate, index_files,
index_listing, kvstore, log, profiler, searchpeers, suppression_listing
Skipping components: rest
Selected diag name of: diag-ip-10-0-0-202-2021-04-23_00-38-43
Starting splunk diag...
Logged search filtering is enabled.
Skipping REST endpoint gathering...
Determining diag-launching user...
Getting version info...
Getting system version info...
```

Reports the components it collect and skips

```
The following certificates were excluded from the diag output automatically.
      /opt/splunk/etc/apps/splunk_secure_gateway/lib/certifi/cacert.pem
      /opt/splunk/etc/apps/splunk_secure_gateway/lib/future/backports/test/https_sv
      /opt/splunk/etc/apps/splunk_secure_gateway/lib/future/backports/test/ssl_key.pem
      /opt/splunk/etc/apps/splunk_secure_gateway/lib/future/backports/test/badkey.pem
      /opt/splunk/etc/apps/splunk_secure_gateway/lib/future/backports/test/dh512.pem
```

Reports certificates that were not auto-detected or skipped

```
Copying Splunk profiler files...
Copying Splunk dispatch files...
Copying Splunk consensus files...
Adding manifest files...
Adding cachemanager_upload.json...
Cleaning up...
Splunk diagnosis file created: /opt/splunk/diag-ip-10-0-0-202-2021-04-23_00-38-43.tar.gz
```

When complete, output is saved and file location is displayed


Copyright © 2023 Splunk, Inc. All rights reserved

# Splunk Diagnostics in Splunk Web

- **Instrumentation**
  - Runs diag in Splunk Web
- **RapidDiag**
  - Uses distributed search to run collections from instances
  - Leverages OS and Splunk tools
  - Directly uploads to Splunk Support using command line
  - Available under Health Report in some cases
  - Currently Linux only

Copyright © 2023 Splunk, Inc. All rights reserved

# Question: Installing Monitoring Console

If the Monitoring Console must be installed on a system with another Splunk component, which of the following would be the most recommended location?

A. On any Search Head

B. On a License Manager

C. On any Deployment Server

D. On any Indexer


Copyright © 2023 Splunk, Inc. All rights reserved

# Answer: Installing Monitoring Console

If the Monitoring Console must be installed on a system with another Splunk component, which of the following would be the most recommended location?

A. On any Search Head

**B. On a License Manager**

C. On any Deployment Server

D. On any Indexer

It is recommended to install the MC on it's own system. If collocated with another Splunk component, a License Manager or a *smaller* Deployment Servers (environments with < 50 clients) is most recommended. Avoid Search Heads and Indexers.


Copyright © 2023 Splunk, Inc. All rights reserved

# Question: Cloud Connected Service Insights

Which of the following is a cloud-connected service that leverages telemetry data to provide Splunk environment insights in real-time?

A. Splunk Diag

B. Rapid Diag

C. Splunk Instrumentation

D. Splunk Assist


Copyright © 2023 Splunk, Inc. All rights reserved

# Answer: Cloud Connected Service Insights

Which of the following is a cloud-connected service that leverages telemetry data to provide Splunk environment insights in real-time?

A. Splunk Diag

B. Rapid Diag

C. Splunk Instrumentation

**D. Splunk Assist**

Starting with Splunk 9.0, the MC provides Splunk Assist, a cloud-connected service for Splunk Enterprise and Splunk Cloud that leverages telemetry data to generate insights in real time. Splunk Assist uses helper packages such as AppAssist, CertAssist and ConfigAssist.


Copyright © 2023 Splunk, Inc. All rights reserved

# Question: Splunk Diag Tools

Which of the following is not true about Splunk Diag tools?

A. Splunk Diag must be run from a Search Head

B. Splunk Diag is available on the command line

C. Splunk Diag does not retrieve index data

D. Rapid Diag can collect data from distributed Splunk instances


Copyright © 2023 Splunk, Inc. All rights reserved

# Answer: Splunk Diag Tools

Which of the following is not true about Splunk Diag tools?

**A. Splunk Diag must be run from a Search Head**

B. Splunk Diag is available on the command line

C. Splunk Diag does not retrieve index data

D. Rapid Diag can collect data from distributed Splunk instances

Splunk Diag is available from any Splunk instance.


Copyright © 2023 Splunk, Inc. All rights reserved

# Module 2 Lab

**Time:** 20 minutes

**Description:** Monitoring Splunk

**Tasks:**

- Use the Health Report and Health Report Manager
- Enable Monitoring Console (MC)
- Run a health check and Splunk diag in the MC
- Create a diag using the command line


Copyright © 2023 Splunk, Inc. All rights reserved

# Module 3: Licensing Splunk


Copyright © 2023 Splunk, Inc. All rights reserved

# Module Objectives

- Identify the different Splunk license types
- Describe license violations
- Configure a Splunk License Manager
- Configure Splunk instances as License Peers


Copyright © 2023 Splunk, Inc. All rights reserved

# Splunk License Types

## Enterprise trial license

- Comes with product; Valid for 60 days, after which another license type must be activated
- Same as **Enterprise license**, except for 500 MB/day limit
- A **Sales trial license** is a trial Enterprise license of varying size and duration

## Enterprise license

- Purchased from Splunk; Sets the daily indexing volume amount or compute capacity
- Full functionality for indexing, search head, deployment server, and so on
- No-enforcement license: Allows searching even if you are in a license violation period *

## Free license

- Disables alerts, scheduled searches, authentication, clustering, distributed search, summarization, and forwarding to non-Splunk servers
- Allows 500 MB/day of indexing and forwarding to other Splunk instances

## Forwarder license

- Sets the server up as a heavy forwarder
- Applies to non-indexing forwarders
- Allows authentication, but no indexing

* Except for licenses < 100 GB/day starting in Splunk 8.1


Copyright © 2023 Splunk, Inc. All rights reserved

# Ingest versus Workload Pricing

## Ingest Pricing

- Based on data volume
- Traditional licensing method
- Monitored using MC and Settings > Licensing in Splunk Web

Focus of this topic

## Workload Pricing

- Based on compute capacity
- Provides more control over product expansion (search versus indexing)
- Monitored using MC (for vCPUs) or Cloud Monitoring Console (for SVCs)

www.splunk.com/en_us/products/pricing/faqs.html


Copyright © 2023 Splunk, Inc. All rights reserved

# Measuring Daily License Quota

## Counts for daily license quota

- All data from all sources that is indexed
- **For events:** Measured as the data (full size) that flows through the parsing pipeline per day
- **For metrics:** Measurement capped at 150 bytes per metric event

## Does not count for daily license quota

- Replicated data (Index Clusters)
- Summary indexes
- Splunk internal logs (_internal, _audit, etc. indexes)
- Structural components of an index (metadata, tsidx, etc.)


Copyright © 2023 Splunk, Inc. All rights reserved

# License Requirements With Server Roles and Data

## Server Roles

**Search Heads, Deployment Server** and other Splunk Enterprise instances require the license even if they are not ingesting data

## Data

**Indexers (Search Peers)** also need the license to determine the amount of ingested data allowed


Copyright © 2023 Splunk, Inc. All rights reserved

# Adding a License

- Use Splunk Web or CLI:

```
splunk add licenses <keyfile>
```

- Multiple licenses of the same type are "stacked" (added together)
- Restart Splunk if license group changes are made
- Find licenses under **`SPLUNK_HOME/etc/licenses`**

Copyright © 2023 Splunk, Inc. All rights reserved

# Using a License Manager

All instances collectively share the stack entitlement


Copyright © 2023 Splunk, Inc. All rights reserved

# License Pooling

- Allows licenses to be subdivided and assigned to indexer groups
- Can be created for a given stack
- Provides warnings and violations per pool
- Examples of License Managers with total stack of 500GB

Copyright © 2023 Splunk, Inc. All rights reserved

# Managing Licenses

Select **Settings** > **Licensing**

1. Designate the license server type: Manager or Peer
2. Change license group
3. Add a license
4. Check license alerts and violations
5. View stacks
6. Edit and add pools

Copyright © 2023 Splunk, Inc. All rights reserved

# Viewing License Alerts

From Splunk Web, select
**Licensing > License Alerts**

## All licensing alerts (2)

License alerts notify you of excessive indexing warnings and licensing misconfigurations. If you receive too many warnings, your indexer will be in violation of the license and you will not be able to search. Learn more

**Current:**

| Severity | Time | Message | Indexer | Pool | Stack | Category |
|---|---|---|---|---|---|---|
| | Correct by midnight to avoid violation Learn more | This pool contains slave(s) with 0 warning(s) | splunk02 | auto_generated_pool_enterprise | enterprise | pool_warning_count |
| | Correct by midnight to avoid violation Learn more | This pool is over poolsz=157286400 bytes, please correct before midnight | | auto_generated_pool_enterprise | enterprise | cle_pool_over_quota |

**Permanent:**


Copyright © 2023 Splunk, Inc. All rights reserved | 9 May 2023

# License Alerts

**Alert**

- Occurs when indexing exceeds the allocated daily quota in a pool
- Viewed in Splunk Web > **Messages** (as a “pool warning”)
- Cleared at midnight when daily allocation is reset; may result in a Warning


Copyright © 2023 Splunk, Inc. All rights reserved

# License Alerts, Warnings

**Alert**

- Occurs when indexing exceeds the allocated daily quota in a pool
- Viewed in Splunk Web > **Messages** (as a “pool warning”)
- Cleared at midnight when daily allocation is reset; may result in a Warning

**Warning**

- Occurs if an alert is triggered and license capacity is not increased by midnight (by adding new license or moving capacity from another pool)
- Only occurs once per day


Copyright © 2023 Splunk, Inc. All rights reserved

# License Alerts, Warnings and Violations

**Alert**

- Occurs when indexing exceeds the allocated daily quota in a pool
- Viewed in Splunk Web > **Messages** (as a "pool warning")
- Cleared at midnight when daily allocation is reset; may result in a Warning

**Warning**

- Occurs if an alert is triggered and license capacity is not increased by midnight (by adding new license or moving capacity from another pool)
- Only occurs once per day

**Violation**

- Occurs after 5 warnings on an Enterprise license* in a rolling 30-day period
- Informational only, and does not affect indexing or searches**
- Requires a reset key from Splunk Support or Sales team

* 3 Warnings on a Free license

** Searches are disabled for licenses < 100 GB/day with 45 warnings in a rolling 60-day period



Copyright © 2023 Splunk, Inc. All rights reserved

# Managing License Warnings

- DO NOT ignore license warnings
- Proactively monitor the consumption of your Splunk license
  - MC provides a couple of alerts
  - If possible, give yourself latitude by rearranging license pools

Copyright © 2023 Splunk, Inc. All rights reserved

# Reporting on Workload Licensing

## Monitoring Console

- Available on premises and in cloud (CMC)
- Provides vCPU / SVC usage across workloads
  - By search type, indexes, and source types, and so on

## Splunk App for Chargeback

- Available on premises and in cloud
- Provides Search Resource Usage (SRU) across business units
  - 1 SRU ~= 1 SVC
- Provides forecasts using Splunk Machine Learning


Copyright © 2023 Splunk, Inc. All rights reserved

# Viewing Workload (Monitoring Console)

Cloud Monitoring Console:
**License Usage > Workload**

Usage is contained within provisioned license limits

Copyright © 2023 Splunk, Inc. All rights reserved

# Using the Chargeback App

- Configure customized chargeback/showback models
- Refer to:

  docs.splunk.com/Documentation/ChargebackApp/latest/Use/Overview

SHOWBACK HOME

1. SRU Showback

1. SRU Showback Input Filters

2.1 Search Resource Usage (SRU) by B-Unit | Earliest Time: -1d@d | Latest Time: -0d@d

**Utilization is the Daily Stack Utilization**

| | B-Unit | Users | Departments | Usage | Start Period | End Period | Search Head(s) | # Searches |
|---|---|---|---|---|---|---|---|---|
| 1 | The Analysis Paralysis Team | 62 | 5 | 22.99 SRU | Mon Feb 07 2022 00:00 | Tue Feb 08 2022 00:00 | cb_test,chargeback,cm,es,federated,gmc,itew,shc | 53,318 |
| 2 | The Easily Distracted | 63 | 5 | 21.30 SRU | Mon Feb 07 2022 00:00 | Tue Feb 08 2022 00:00 | cb_test,chargeback,cm,es,gmc,itew,shc | 16,828 |
| 3 | The Splunk T-Shirt Company | 60 | 5 | 12.09 SRU | Mon Feb 07 2022 00:00 | Tue Feb 08 2022 00:00 | chargeback,cm,es,gmc,itew,shc | 28,220 |
| 4 | The Party Planners Group | 49 | 5 | 11.07 SRU | Mon Feb 07 2022 00:00 | Tue Feb 08 2022 00:00 | cb_test,chargeback,cm,es,gmc,itew,shc | 13,399 |
| 5 | Special Projects | 66 | 5 | 7.16 SRU | Mon Feb 07 2022 00:00 | Tue Feb 08 2022 00:00 | cb_test,cm,es,gmc,itew,shc | 11,646 |

**Number of B-Units** **5 B-Units**

**Number of Departments** **25 Departments**

**Number of Users** **290 Users**



Copyright © 2023 Splunk, Inc. All rights reserved

# Question: Event and Metric Licensing

Which of the following is true about Metrics licensing?

A. Events and metrics licensing is measured the same

B. Events licensing is capped at 150 bytes per event

C. Metrics licensing is 150 bytes per metric event

D. Metrics data draws from the same license quota as event data


Copyright © 2023 Splunk, Inc. All rights reserved

# Answer: Event and Metric Licensing

Which of the following is true about Metrics licensing?

A. Events and metrics licensing is measured the same

B. Events licensing is capped at 150 bytes per event

C. Metrics licensing is 150 bytes per metric event

**D. Metrics data draws from the same license quota as event data**

Events are measured as the data (full size) that flows through the parsing pipeline per day. Metrics measurement is *capped* at 150 bytes per metric event. Both types of data input draw from the same license quota.


Copyright © 2023 Splunk, Inc. All rights reserved | 9 May 2023

# Question : Enterprise License

Which of the following Splunk components *do not* require an Enterprise license installed?

A. Search Heads

B. Indexers

C. Heavy Forwarders

D. Universal Forwarders


Copyright © 2023 Splunk, Inc. All rights reserved

# Answer: Enterprise License

Which of the following Splunk components *do not* require an Enterprise license installed?

A. Search Heads

B. Indexers

C. Heavy Forwarders

**D. Universal Forwarders**

Search Heads, Indexers, Heavy Forwarders, Deployment Server and other Splunk Enterprise instances require the Enterprise license even if they are not ingesting data. Universal Forwarders do not require an Enterprise license to be installed.


Copyright © 2023 Splunk, Inc. All rights reserved

# Question : Alerts, Warnings, Violations

Which of the following statements about license alerts, warnings, and violations is true?

A. Alerts not fixed in 24 hours turn into a Violation

B. 30 Warnings turns into a Violation

C. Alerts not fixed by midnight turn into a Warning

D. Free licenses are immune to Warnings


Copyright © 2023 Splunk, Inc. All rights reserved

# Answer: Alerts, Warnings, Violations

Which of the following statements about license alerts, warnings, and violations is true?

A. Alerts not fixed in 24 hours turn into a Violation

B. 30 Warnings turns into a Violation

**C. Alerts not fixed by midnight turn into a Warning**

D. Free licenses are immune to Warnings

Indexing that exceeds the allocated daily quota in a pool is an alert. An alert not fixed by midnight turns into a warning. 5 or more warnings on an enforced Enterprise license (or 3 warnings on a Free license) in a rolling 30-day period is a violation.


Copyright © 2023 Splunk, Inc. All rights reserved

# Module 3 Lab

**Time:** 15 minutes

**Description:** Licensing Splunk

**Tasks:**

- Add licenses
- Modify the license pool
- Enable and modify an MC Alert for licensing


Copyright © 2023 Splunk, Inc. All rights reserved

# Module 4:
# Using Configuration Files


Copyright © 2023 Splunk, Inc. All rights reserved

# Module Objectives

- Describe Splunk configuration directory structure
- Understand configuration layering process
  - Index time process
  - Search time process
- Use Splunk tools to examine configuration settings such as **`btool`**


Copyright © 2023 Splunk, Inc. All rights reserved

# Configuration Files

## Configuration Files (`.conf`)

- Govern aspects of Splunk functionality
- Text files that are generally case sensitive with **`[stanza]`** and **`attribute = value`** format
- Modified using Splunk Web, CLI, REST API, app install, or directly editing
- Saved under **`SPLUNK_HOME/etc`**

```
[default]
host=www

[monitor:///var/log/httpd]
sourcetype = access_common
ignoreOlderThan = 7d
index = web
```

**Note**

For **`.conf`** file documentation and examples view **`SPLUNK_HOME/etc/system/README/`**:
- **`*.conf.spec`**
- **`*.conf.example`**


Copyright © 2023 Splunk, Inc. All rights reserved

# Methods for Modifying Splunk Configurations

- Splunk Web
- Splunk CLI

```
./splunk add monitor /opt/log/www1/access.log -index itops
   -sourcetype access_combined_wcookie -host splunk01
```

- Editing **.conf** files

```
[monitor:///opt/log/www1/access.log]
disabled = false
host = splunk01
index = itops
sourcetype = access_combined_wcookie
```

Copyright © 2023 Splunk, Inc. All rights reserved

# Commonly Used Splunk Configuration Files

| | | |
|---|---|---|
| **Search Head** | `props.conf` | Search-time Field Extractions, lookups, and so on |
| **Indexer** | `props.conf` | Parsing |
| | `inputs.conf` | What data is collected; Which ports to listen to |
| **Forwarder** | `outputs.conf` | Where to forward data |
| | `props.conf` | Limited parsing |
| | `inputs.conf` | What data is collected (*production data*) |


Copyright © 2023 Splunk, Inc. All rights reserved

# Configuration Files Used During Data Input

Search-time Field Extractions, lookups, and so on

Parsing

What data is collected; Which ports to listen to

Where to forward data

Limited parsing

What data is collected (*production data*)



Copyright © 2023 Splunk, Inc. All rights reserved | 9 May 2023

# Configuration Directories

**Warning**

The files in the **default** directories must never be modified.

docs.splunk.com/Documentation/Splunk/latest/Admin/Listofconfigurationfiles



Copyright © 2023 Splunk, Inc. All rights reserved | 9 May 2023

# Default versus Local Configuration

**`default`**

- Shipped with Splunk or app
- Overwritten on update
- Do not modify

**`local`**

- Keeps your changes
- Preserved on update
- Only modify these versions
- Overrides **`default`** settings


Copyright © 2023 Splunk, Inc. All rights reserved

# Merging of Configuration Files

- Splunk merges configuration files
  - Generally when Splunk starts, or when searches are run
  - Into a single run-time model for each file type
  - As a union of all files if no duplicates/conflicts exist
- In case of conflicts, priority is based on the context:
  - **Global context** (index-time)
  - **App/User context** (search-time)

Copyright © 2023 Splunk, Inc. All rights reserved

# File Context and Index-time versus Search-time

| | Global Context | App/User Context |
|---|---|---|
| *Used during:* | **Index-time** | **Search-time** |
| *Used by:* | • User-independent tasks<br>• Background tasks<br>• Input, parsing, indexing | • User-related activity<br>• Searching<br>• Search-time processing |
| *Example use-case:* | A network input to collect syslog data | Mary's private report in the Search app |
| *Example files:* | `inputs.conf`<br>`outputs.conf`<br>`props.conf` | `macros.conf`<br>`savedsearches.conf`<br>`props.conf` |

docs.splunk.com/Documentation/Splunk/latest/Admin/Wheretofindtheconfigurationfiles


Copyright © 2023 Splunk, Inc. All rights reserved

# Index-Time Precedence (Global Context)

## Precedence order

1. System local directory
   `etc/system/local`
2. App local directories*
   `etc/apps/appname/local`
3. App default directories*
   `etc/apps/appname/default`
4. System default directory
   `etc/system/default`

**Note**

* When determining priority of app directories in **global** context (for steps 2 and 3), Splunk uses *lexicographical* order. (Files in apps directory "A" have higher priority than files in apps directory "B".)


Copyright © 2023 Splunk, Inc. All rights reserved

# Example of Index-Time Precedence: No Conflict

**inputs.conf**

```
[a]
ax = 1
ay = 2

[b]
bx = 3
by = 4
bz = 5

[c]
cx = 6
```


Copyright © 2023 Splunk, Inc. All rights reserved

# Example of Index-Time Precedence: Conflict

Copyright © 2023 Splunk, Inc. All rights reserved

# Realistic Example of Index-Time Precedence (1)

Copyright © 2023 Splunk, Inc. All rights reserved 

# Realistic Example of Index-Time Precedence (2)

```
[monitor:///var/log/secure.log]
sourcetype = access_combined
index=security
```

```
[default]
host = server1

[monitor:///opt/log/www1/access.log]
host = websvr1
```

```
[monitor:///var/log/secure.log]
sourcetype = linux_secure

[monitor:///opt/log/www1/access.log]
host = www1
sourcetype = access_combined_wcookie
```

2a 1

**inputs.conf**

```
[default]
host = server1

[monitor:///var/log/secure.log]
sourcetype = linux_secure


[monitor:///opt/log/www1/access.log]
host = websvr1
sourcetype = access_combined_wcookie
```


Copyright © 2023 Splunk, Inc. All rights reserved

# Realistic Example of Index-Time Precedence (3)

```
[monitor:///var/log/secure.log]
sourcetype = access_combined
index=security
```

```
[default]
host = server1

[monitor:///opt/log/www1/access.log]
host = websvr1
```

```
[monitor:///var/log/secure.log]
sourcetype = linux_secure

[monitor:///opt/log/www1/access.log]
host = www1
sourcetype = access_combined_wcookie
```

2b 2a 1

**inputs.conf**

```
[default]
host = server1

[monitor:///var/log/secure.log]
sourcetype = linux_secure
index=security

[monitor:///opt/log/www1/access.log]
host = websvr1
sourcetype = access_combined_wcookie
```


Copyright © 2023 Splunk, Inc. All rights reserved

# Search-Time Precedence (App/User Context)

## Precedence order

1. Current user directory for app
   `etc/users/user/appname/local`
2. App directory - running app
   `etc/apps/appname/local`
   `etc/apps/appname/default`
3. App directories - all other apps*
   `etc/apps/appname/local`
   `etc/apps/appname/default`
4. System directories
   `etc/system/local`
   `etc/system/default`

**Note**

* If objects from the app are exported globally with **`.meta`** file setting, evaluate all other app directories using *reverse lexicographical* order. (Files in apps directory "B" have higher priority than directory "A".)


Copyright © 2023 Splunk, Inc. All rights reserved

# Conf File Example: Server Name

- Using Splunk Web:
  Settings > Server settings > General settings
  - Splunk server name
  - Default host name
- Using the CLI:

```
./splunk set servername uf01

./splunk set default-hostname uf01
```

SPLUNK_HOME/etc/system/local/server.conf

```
[general]
serverName = uf01
```

SPLUNK_HOME/etc/system/local/inputs.conf

```
[default]
host = uf01
```


Copyright © 2023 Splunk, Inc. All rights reserved

# Conf File Example: Index Creation

- Using Splunk Web: **Settings > Indexes > New Index**
  - Index Name: test
  - App: *app_name*
- Using the CLI:

```
./splunk add index test [-app app_name]
```

**SPLUNK_HOME/etc/apps/*app_name*/local/indexes.conf**

```
[test]
coldPath = $SPLUNK_DB/test/colddb
enableDataIntegrityControl = 0
enableTsidxReduction = 0
homePath = $SPLUNK_DB/test/db
maxTotalDataSizeMB = 512000
thawedPath = $SPLUNK_DB/test/thaweddb
```

Note

Not setting the app context with **-app *app_name*** on the CLI results in entries being added to the Search & Reporting (**search**) app.


Copyright © 2023 Splunk, Inc. All rights reserved

# Conf File Example: Receiving Port

- Using Splunk Web:
  Settings > Forwarding and Receiving > Receive Data > New receiving port
  - Listen on this port: 9997
- Using the CLI:

```
./splunk enable listen 9997 [-app app_name]
```

**SPLUNK_HOME/etc/apps/*app_name*/local/inputs.conf**

```
[splunktcp://9997]
connection_host = ip
```

Note

Not setting the app context with **-app *app_name*** on the CLI results in entries being added to the Search & Reporting (**search**) app.


Copyright © 2023 Splunk, Inc. All rights reserved

# Configuration Best Practices

- Avoid storing configurations in **`SPLUNK_HOME/etc/system/local`**
  - Local context settings will *always* take precedence
  - Attempting to override index-time settings in an app will fail
  - Managing these settings with a deployment server is impossible
- Create an app to manage system settings
  - Allows you to manage settings with a deployment server
  - Manage system configurations in an app (e.g. **`DC_app`**) under **`SPLUNK_HOME/etc/apps/<appname>/local`**
  - Refer to the *Splunk Enterprise Data Administration* course

splunk>
Best Practice


Copyright © 2023 Splunk, Inc. All rights reserved

# Validating the Splunk Configuration

## Validating the on-disk configuration

- Performed with **`splunk btool`** CLI
- Syntax: **`splunk btool <conf_file> list`**
- Example: **`splunk btool inputs list`**

## Validating the in-memory configuration

- Performed with **`splunk show config`** CLI or REST API
- Syntax: **`splunk show config <conf_file>`**
- Example: **`splunk show config inputs`**


Copyright © 2023 Splunk, Inc. All rights reserved

# Configuration Validation with **btool**

- **splunk btool <*conf-name*> list [*options*]**
  - Shows on-disk configuration for requested file
  - Useful for checking the configuration scope and permission rules
  - Run **splunk btool check** each time Splunk starts
    - Use **--debug** to display the exact **.conf** file location
    - Add **--user= <*user*> --app=<*app*>** to see the user/app context layering
- Examples:

```
splunk help btool
splunk btool check
splunk btool inputs list
splunk btool inputs list monitor:///var/log
splunk btool inputs list monitor:///var/log --debug
```

docs.splunk.com/Documentation/Splunk/latest/Troubleshooting/Usebtooltotroubleshootconfigurations


Copyright © 2023 Splunk, Inc. All rights reserved

# Example using **btool**

Scenario: What are the **/var/log/secure.log** input configurations and where are they specified?

```
> splunk btool inputs list monitor:///var/log/secure.log --debug

  etc/apps/search/local/inputs.conf    [monitor:///var/log/secure.log]
  system/local/inputs.conf             host = server1
  etc/apps/unix/local/inputs.conf      index = security
  etc/apps/search/local/inputs.conf    sourcetype = linux_secure
...
```

**etc/apps/unix/local/inputs.conf**

```
[monitor:///var/log/secure.log]
sourcetype = access_combined
index = security
```

**etc/apps/search/local/inputs.conf**

```
[monitor:///var/log/secure.log]
sourcetype = linux_secure
```


Copyright © 2023 Splunk, Inc. All rights reserved

# Overriding Defaults

- Override settings in the **`local`** directory at the same scope
  - Do not modify the **`default`** directory version of the **`.conf`** file
  - Do not make a copy of the entire configuration file
  - Only include stanzas and settings you are overriding:
    - **Addition**: Add the new setting with its value
    - **Modification**: Place the existing setting with its new value
    - **Deletion**: Place the existing setting with a non-value
- Example: To disable the attribute **`TRANSFORMS`** for stanza **`[syslog]`**:

```
# etc/system/default/props.conf
[syslog]
TRANSFORMS = syslog-host
REPORT-syslog = syslog-extractions
...
```

```
# etc/system/local/props.conf
[syslog]
TRANSFORMS =
```


Copyright © 2023 Splunk, Inc. All rights reserved

# Reloading Configuration Files After Edit

- Changes made using Splunk Web or the CLI may not require restart
  - A message appears if restart is required (changing some server settings)
- Changes made by editing **`.conf`** files are not automatically detected
- To force reload, go to **`https://servername:webport/debug/refresh`**
  - Reloads many of the configurations, including **`inputs.conf`**, but not all
- To reload all configurations, restart Splunk
  - Splunk Web: **Settings** > **Server controls** > **Restart Splunk**
  - CLI: **`splunk restart`**

Note

A Splunk refresh is only valid for standalone configuration or a search head.


Copyright © 2023 Splunk, Inc. All rights reserved

# Tracking Configuration Changes

- Performed by default by the Configuration Change Tracker
  - Uses active *monitoring* if the Linux **`inotify`** API is available
  - Otherwise uses *polling* which checks **`.conf`** files every 30 seconds
  - Stores changes in the **`_configtracker`** index
- Monitors valid **`.conf`** files in **`default`** and **`local`** folders for:
  - **`SPLUNK_HOME/etc/system`**
  - **`SPLUNK_HOME/etc/apps`**
  - **`SPLUNK_HOME/etc/users`**
  - **`SPLUNK_HOME/etc/slave-apps`**
  - **`SPLUNK_HOME/etc/instance.cfg`**
- Ignores *values* for fields with sensitive data (such as hashed passwords)


Copyright © 2023 Splunk, Inc. All rights reserved

# Question: Configuration Files

Which configuration file tells a Splunk instance which data to ingest?

A. `inputs.conf`
B. `outputs.conf`
C. `server.conf`
D. `props.conf`


Copyright © 2023 Splunk, Inc. All rights reserved

# Answer: Configuration Files

Which configuration file tells a Splunk instance which data to ingest?

A. **`inputs.conf`**

B. `outputs.conf`

C. `server.conf`

D. `props.conf`

**`inputs.conf`** lists data inputs, or in some cases which network ports to listen on for data inputs.
**`outputs.conf`** lists where input data should be sent (for example from forwarders to indexers).
**`server.conf`** lists server settings, and **`props.conf`** lists processing properties for data input.


Copyright © 2023 Splunk, Inc. All rights reserved

# Question: The **`btool`** Utility

Which of the following about btool is true?

A. **`btool`** is used to verify Splunk configuration in memory
B. **`btool`** is used to verify Splunk configuration on disk
C. **`btool`** is a Splunk Support utility you must download
D. **`btool`** is unavailable on a Free license


Copyright © 2023 Splunk, Inc. All rights reserved

# Answer: The **btool** Utility

Which of the following about btool is true?

A. **btool** is used to verify Splunk configuration in memory

B. **btool** is used to verify Splunk configuration on disk

C. **btool** is a Splunk Support utility you must download

D. **btool** is unavailable on a Free license

The **btool** command is used to verify Splunk configuration on disk. To verify Splunk configuration in memory, use the **splunk show config** command or REST API. It is available by default for all Splunk Enterprise installation.


Copyright © 2023 Splunk, Inc. All rights reserved

# Question: Disabling an Attribute

How should an administrator disable the **`[syslog]`** stanza attribute **`TRANSFORMS=syslog-host`** found in **`SPLUNK_HOME/etc/system/default/props.conf`**?

A. In `…/default/props.conf` remove the attribute

B. In `…/default/props.conf` set `TRANSFORMS=`

C. In `…/local/props.conf` set `TRANSFORMS=`

D. In `…/local/props.conf` set `TRANSFORMS=disable`


Copyright © 2023 Splunk, Inc. All rights reserved

# Answer: Disabling an Attribute

How should an administrator disable the **`[syslog]`** stanza attribute **`TRANSFORMS=syslog-host`** found in **`SPLUNK_HOME/etc/system/default/props.conf`**?

A. In `…/default/props.conf` remove the attribute

B. In `…/default/props.conf` set `TRANSFORMS=`

**C. In `…/local/props.conf` set `TRANSFORMS=`**

D. In `…/local/props.conf` set `TRANSFORMS=disable`

The file **`SPLUNK_HOME/etc/system/default/props.conf`** should now be modified by an administrator. In **`SPLUNK_HOME/etc/system/local/props.conf`** you should set **`TRANSFORMS=`** (to a blank value) to disable it.


Copyright © 2023 Splunk, Inc. All rights reserved

# Module 4 Lab

**Time:** 20 minutes

**Description:** Using Configuration files

**Tasks:**

- Make various configuration changes in Splunk
- Observe corresponding configuration file changes
- Use the **`btool`** and the **`splunk show config`** commands to investigate configuration changes
- Use the configuration change tracker


Copyright © 2023 Splunk, Inc. All rights reserved

# Module 5: Using Apps


Copyright © 2023 Splunk, Inc. All rights reserved

# Module Objectives

- Describe Splunk apps and add-ons
- Install an app on a Splunk instance
- Manage app accessibility and permissions


Copyright © 2023 Splunk, Inc. All rights reserved

# Splunk Apps

## Splunk Apps

- Collection of configuration files, scripts, web assets, and so on
- May be focused on specific type of data, vendor, OS, industry, or business need
- May be installed on any Splunk instance
- May be included with Splunk (as a default app)

| App A | App B |
|---|---|
| app.conf | app.conf |
| props.conf | |
| indexes.conf | |
| inputs.conf | inputs.conf |
| tags.conf | |
| transforms.conf | |
| ... | |
| default.meta | default.meta |
| mylookup.csv | |
| myviews.xml | |


Copyright © 2023 Splunk, Inc. All rights reserved

# Viewing Installed Apps

- Apps are installed under **`SPLUNK_HOME/etc/apps`**
- Apps can be visible or hidden in Splunk Web
  - Several apps are installed by default
  - Internal apps used by Splunk should not be modified
- To manage apps in Splunk Web:

On the **Home** view

Within an app

Copyright © 2023 Splunk, Inc. All rights reserved

# Examples of Default Apps

1. Home (**`launcher`**)
   - Access to other apps, help, tutorials
2. Search and Reporting (**`search`**)
   - Full-featured search environment
   - Access to dashboards, reports, and so on
3. Upgrade Readiness App
   - Checks for Python and app compatibility
4. Sample data (**`sample_app`**)
   - Provides baseline structure to create an app
   - Hidden by default

Copyright © 2023 Splunk, Inc. All rights reserved

# Using the Upgrade Readiness App

- Scans Splunk 7.1 and later for app compatibility issues
  - Python 3 runtimes are default in Splunk 8.1+
- Installed by default starting in Splunk 8.2

• • •

Copyright © 2023 Splunk, Inc. All rights reserved

# Discovering Apps On Splunkbase

- Provides Splunk and community-supplied apps and add-ons
  - For Splunk Enterprise, Splunk Cloud, and Splunk SOAR
- Includes Splunk and developer-supported apps

Copyright © 2023 Splunk, Inc. All rights reserved

# Splunk Add-ons

## Splunk Add-ons

- Reusable component supporting other apps
- Often used for data collection
- Any combination of configurations, scripts, data inputs, and so on
- Does **not** contain Splunk Web UI components (reports or dashboards)
- **Technology add-ons (TAs)**: specialized add-ons that help collect, transform, and normalize data feeds from specific sources

| Description | Apps | Add-ons |
|---|---|---|
| Provides Splunk Web UI components (navigable interface, dedicated URL, visualize data) | ✓ | |
| Occupies a unique namespace within Splunk | ✓ | ✓ |
| Can be redistributed and shared using Splunkbase | ✓ | ✓ |
| Contains components intended for reuse by other apps | | ✓ |
| Can depend on add-ons for correct operation | ✓ | ✓ |


Copyright © 2023 Splunk, Inc. All rights reserved

# Installing an App Using Splunk Web

splunk>enterprise | Apps | Administrator | Messages | Settings | Activity | Help | Find

## Apps

Browse more apps | Install app from file | Create app

Showing 1-25 of 25 items

filter

25 per page

| Name | Folder name | Version | Update checking | Visible | Sharing | Status |
|---|---|---|---|---|---|---|
| SplunkForwarder | SplunkForwarder | | Yes | No | App \| Permissions | Disabled \| Enable |

### IT Essentials Work

Install

IT Essentials Work helps you correlate logs and metrics for each entity, and then use that information to observe and understand the performance of your infrastructure. The app helps you get started monitoring and analyzing IT infrastructures such as *nix, Windows, virtualization with out-of-the-box dashboards, and pre-configured performance metric... More

Category: IT Operations | Author: Splunk Inc. | Downloads: 14891 | Released: 2 months ago | Last Updated: a month ago |

View on Splunkbase

### Splunk App for SOAR

Install

The Splunk App for SOAR gets data from your Splunk SOAR instance for manipulation and display in Splunk. This app provides pre-built dashboards and enables you to use Splunk to power SOAR's search engine.

### Install App From File

If you have a .spl or .tar.gz app file to install, you can upload it using this form.

You can replace an existing app via the Splunk CLI. Learn more.

File

Choose File | No file chosen

☐ Upgrade app. Checking this will overwrite the app if it already exists.

Cancel | Upload



Copyright © 2023 Splunk, Inc. All rights reserved

# Installing an App from Splunkbase

1. From Splunk Web **Apps** page, click **Browse more apps**, or click **Apps > Find More Apps**
   - Splunk Web will access http://splunkbase.splunk.com
2. Search for the app you want to install
3. Select **Install**
   - Most apps are free
   - Requires a splunk.com user ID and password
   - App is installed into **`SPLUNK_HOME/etc/apps`**
4. Restart Splunk, if required
5. Configure the app according to its documentation

Note

Anyone can sign up for a user account in splunk.com. A support contract is not required.


Copyright © 2023 Splunk, Inc. All rights reserved

# Installing an App From a File

1. Download the app directly from http://splunkbase.splunk.com
   - File format may be: **`.tar.gz`**, **`.tgz`**, **`.spl`**
2. Install the app using one of these methods:
   - **Splunk Web**: Click **Install app** from file
   - **Command line**:

```
# splunk install app <path-to-appfile>
```

   - **Extract app** in proper location:

```
# cd SPLUNK_HOME/etc/apps
# tar -xf <path-to-appfile>
```

3. Restart Splunk, if required
4. Configure the app according to its documentation


Copyright © 2023 Splunk, Inc. All rights reserved

# Apps on Forwarders

- Universal forwarders don't have a web interface, but may still benefit from an app
- Install the app on a forwarder using one of these methods:
  - **Command line** on the forwarder (**`splunk install app`**)
  - **Extract app** in proper location on the forwarder
  - **Use a deployment server** to deploy the app


Copyright © 2023 Splunk, Inc. All rights reserved

# Creating Apps With Splunk Templates

Splunk Web's built-in app builder provides two templates: **barebones** and **sample_app**.

**Note**

Splunk's sample data (**`sample_app`**) builds a more robust basic application. More information on creating apps is provided in the *Building Splunk Apps* course.



Copyright © 2023 Splunk, Inc. All rights reserved | 9 May 2023

# Deploying Apps In Distributed Environments

- Without clustering, Deployment Server can deploy apps to all tiers
- Alternatively, deploy apps manually or using 3rd party software solutions

**Note**

Work with your Splunk administrator to properly deploy your app in a production environment. More information is provided in the *Forwarder Configuration and Management* course.


Copyright © 2023 Splunk, Inc. All rights reserved | 9 May 2023

# Deploying Apps In Clustered Environments

- With clustering use the deployment methods for the appropriate tier:
  - Deployer to search heads
  - Cluster Manager node to indexers
  - Deployment Server to forwarders
  - Deployment Server to Cluster Manager / Deployer (optional)

**Note**

More information is provided in the *Splunk Enterprise Cluster Administration* course.


Copyright © 2023 Splunk, Inc. All rights reserved | 9 May 2023

# Managing Apps

## Apps

Showing 1-23 of 23 items

filter

25 per page

Add apps

Browse more apps | Install app from file | Create app

| Name | Folder name | Version | Update checking | Visible | Sharing | Status | Actions |
|---|---|---|---|---|---|---|---|
| SplunkForwarder | SplunkForwarder | | Yes | No | App \| Permissions | Disabled \| E | |
| SplunkLightForwarder | SplunkLightForwarder | | Yes | No | App \| Permissions | Disabled \| Enable | |
| Log Event Alert Action | alert_logevent | 8.2.0 | Yes | No | App \| Permissions | Enabled \| Disable | Edit properties \| View objects |
| Webhook Alert Action | alert_webhook | 8.2.0 | Yes | No | App \| Permissions | Enabled \| Disable | Edit properties \| View objects |
| Apps Browser | appsbrowser | 8.2.0 | Yes | No | App \| Permissions | Enabled | Edit properties \| View objects |
| introspection_generator_addon | introspection_generator_addon | 8.2.0 | Yes | No | App \| Permissions | Enabled \| Disable | Edit properties \| View objects |
| journald_input | journald_input | | Yes | No | App \| Permissions | Enabled \| Disable | Edit properties \| View objects |
| Home | launcher | | | | App \| Permissions | Enabled | Launch app \| Edit properties \| |
| learned | learned | | Yes | No | App \| Permissions | Enabled \| Disable | Edit properties \| View objects |
| legacy | legacy | | Yes | No | App \| Permissions | Disabled \| Enable | |
| Python Upgrade Readiness App | python_upgrade_readiness_app | 1.0.0 | Yes | Yes | App \| Permissions | Enabled \| Disable | Launch app \| Edit properties \| |
| sample data | sample_app | | Yes | No | App \| Permissions | Disabled \| Enable | |

Enable or disable app (restart may be required)

Controls access



Copyright © 2023 Splunk, Inc. All rights reserved | 9 May 2023

# App Permissions

- User roles with **read** permission:
  - Can see the app and use it
  - Can add knowledge objects (KOs)
  - Can modify KOs they own
- User roles with **write** permission:
  - Can share KOs they own
  - Can delete KOs used in the app

**Note**

By default, the role "user" does not have write permissions within the search app.

Permissions on a KO generally take precedence over App permissions.

Copyright © 2023 Splunk, Inc. All rights reserved

# Deleting an App

- Consider disabling or moving the app's files to another location
- When an app is deleted:
  - Configuration files and scripts are deleted from the Splunk server
  - User's private app artifacts remain untouched
  - The app can be reinstalled later
- To delete an app:
  1. Select one of these methods:
     - Run: **`splunk remove app <app_folder>`**
     - Navigate to **`SPLUNK_HOME/etc/apps`** and delete the app's folder and all its contents
  2. Restart the Splunk server

**Warning**

Deleting an app folder directly does not check for dependencies. Using the **`splunk remove app`** command is the preferred method.


Copyright © 2023 Splunk, Inc. All rights reserved

# Useful References

- Develop Splunk Apps
  dev.splunk.com/enterprise/docs/developapps
- Splunk Web Framework
  dev.splunk.com/enterprise/docs/developapps/visualizedata/usewebframework/
- Create a Splunk app and set properties
  dev.splunk.com/enterprise/docs/developapps/createapps/
- Install Apps in Splunk Cloud
  docs.splunk.com/Documentation/SplunkCloud/latest/User/SelfServiceAppInstall
- Documentation in **`app.conf.spec`**
  docs.splunk.com/Documentation/Splunk/latest/admin/AppConf


Copyright © 2023 Splunk, Inc. All rights reserved

# Question: Apps and Add-ons

Although Apps and Add-ons can be very similar, which of the following applies to Add-ons only?

A. Occupies a unique namespace within Splunk

B. Can be redistributed and shared using Splunkbase

C. Contains components intended for reuse by other apps

D. Can depend on add-ons for correct operation


Copyright © 2023 Splunk, Inc. All rights reserved

# Answer: Apps and Add-ons

Although Apps and Add-ons can be very similar, which of the following applies to Add-ons only?

A. Occupies a unique namespace within Splunk

B. Can be redistributed and shared using Splunkbase

**C. Contains components intended for reuse by other apps**

D. Can depend on add-ons for correct operation

Add-ons contain components specifically with the intent for reuse by other apps and add-ons.

Both apps and add-ons must be uniquely named, can be redistributed on Splunkbase, and can depend on other add-ons.


Copyright © 2023 Splunk, Inc. All rights reserved

# Question: UFs and Apps

Which of the following is true about Universal Forwarders (UFs) and apps?

A. UFs cannot use an add-ons/apps due to lack of a web interface

B. UFs require a Deployment Server to use add-ons and apps

C. UFs can only use add-ons, not apps

D. UFs can take advantage of add-ons and app


Copyright © 2023 Splunk, Inc. All rights reserved

# Answer: UFs and Apps

Which of the following is true about Universal Forwarders (UFs) and apps?

A. UFs cannot use an add-ons/apps due to lack of a web interface

B. UFs require a Deployment Server to use add-ons and apps

C. UFs can only use add-ons, not apps

**D. UFs can take advantage of add-ons and app**

Universal Forwarders can take advantage of add-ons and apps. Although a UF doesn't have a web interface for Splunk Web, apps can still be installed manually, or pushed to these systems using a Splunk Deployment Server or other distribution method.


Copyright © 2023 Splunk, Inc. All rights reserved

# Question: User Role App Permissions

A user's role has write permissions to an app. What functionality does that provide the user in regards to the app and any contained knowledge objects (KOs)?

A. Ability to modify user role permissions for the app

B. Ability to add/delete/modify the app

C. Ability to add/delete/modify KOs used in the app

D. Ability to modify (not add or delete) KOs used in the app


Copyright © 2023 Splunk, Inc. All rights reserved

# Answer: User Role App Permissions

A user's role has write permissions to an app. What functionality does that provide the user in regards to the app and any contained knowledge objects (KOs)?

A. Ability to modify user role permissions for the app

B. Ability to add/delete/modify the app

**C. Ability to add/delete/modify KOs used in the app**

D. Ability to modify (not add or delete) KOs used in the app


Copyright © 2023 Splunk, Inc. All rights reserved

# Module 5 Lab

**Time:** 20 minutes

**Description:** Using Apps

**Tasks:**

- Explore Splunk apps on Splunkbase
- Install the class app
- Change the app permissions
- Verify if the app dashboard displays reports
- Run the Upgrade Readiness App


Copyright © 2023 Splunk, Inc. All rights reserved

# Module 6: Creating Indexes


Copyright © 2023 Splunk, Inc. All rights reserved

# Module Objectives

- Describe how Splunk indexes function
- Identify the types of index buckets
- Add and work with indexes
- Describe metrics indexes


Copyright © 2023 Splunk, Inc. All rights reserved

# Splunk Indexes

## Splunk Indexes

- Store input data as events
- Includes some pre-configured indexes
- Can be created by a Splunk administrator
- Can be used to limit scope of a search
- Allow the ability to limit access by role
- Found by default under **`SPLUNK_DB`** (**`SPLUNK_HOME/var/lib/splunk`**)

Copyright © 2023 Splunk, Inc. All rights reserved

# Indexes and Access Control

- Access control is set per index
- Segregate events into indexes to limit access by Splunk role

Copyright © 2023 Splunk, Inc. All rights reserved

# Indexes and Retention

- Retention policy is set per index
  - Only one retention policy can be set per index
- Separate events into different indexes based on desired retention

| Events | Index | Retention policy |
|---|---|---|
| Web events | **web** | Keep for 6 months → Delete |
| Security events | **security** | Keep for 12 months → Archive |
| Proxy events | **proxy** | Keep for 8 weeks → Delete |


Copyright © 2023 Splunk, Inc. All rights reserved

# Events and Metrics Indexes

## Events Indexes

- Stores unstructured data such as log data
- Stored as separate events
- Default index type

## Metrics Indexes

- Optimized to ingest, store, and analyze metrics
- Generally measures system health or performance


Copyright © 2023 Splunk, Inc. All rights reserved

# Preconfigured Indexes (Partial List)

| Index name | Purpose |
|---|---|
| **`_internal`** | To index Splunk's own logs and metrics |
| **`_audit`** | To store Splunk audit trails and other optional auditing information |
| **`_introspection`** | To track system performance, Splunk resource usage data, and provide Monitoring Console (MC) with performance data |
| **`_thefishbucket`** | To contain checkpoint information for file monitoring inputs |
| **`summary`** | Default index for summary indexing system |
| **`main`** | Default index for inputs; located in the **`defaultdb`** directory |


Copyright © 2023 Splunk, Inc. All rights reserved

# Buckets

## Buckets

- Part of an index that stores events
- A directory containing a set of raw data and associated index files
- Have a maximum data size and a time span, that can both be configured

Copyright © 2023 Splunk, Inc. All rights reserved

# Data Flow Through an Index

Copyright © 2023 Splunk, Inc. All rights reserved

# Hot and Warm Buckets

- Splunk input data is ingested: read, parsed, goes through the license meter, and is written to a hot bucket
- Hot and warm buckets are stored in the **Home Path**
- Hot buckets roll over to a warm bucket:
  - When they reach max size or time span, or when the indexer is restarted
  - By being renamed to identify the time range of the contained events

```
hot_v1_0
hot_v1_1
```

Hot bucket names

**Home Path**

Youngest event in bucket
Oldest event in bucket
Unique ID

```
db_1389230491_1389230488_5
db_1390579247_1390579086_18
```

Warm bucket names


Copyright © 2023 Splunk, Inc. All rights reserved

# Warm and Cold Buckets

- Warm buckets roll over to a cold bucket:
  - When the **Home Path** maximum size (default: 0 / unconstrained) or the maximum warm bucket count (default: 300 buckets) is reached
  - By moving the oldest Warm bucket to the **Cold Path**
  - Preserving the bucket name
- At search time, Splunk scans the time range on a bucket name to determine whether to open the bucket and search its events

```
db_1389230491_1389230488_5
db_1390579247_1390579086_18
```

Cold bucket names


Copyright © 2023 Splunk, Inc. All rights reserved | 9 May 2023

# Retention, Deletion, and Frozen Buckets

- Oldest bucket is deleted when:
  - All events in the bucket exceed the time retention limit (default: 6 years)
  - Index's "**Max Size of Entire Index**" value is reached (default: ~500 GB)
    - Splunk never exceeds this size, and will delete buckets prior to the retention limit
- Optionally configure the **Frozen Path**
  - Splunk copies bucket's raw data here before deletion
  - Frozen buckets are not searchable
- Frozen data can be brought back (thawed) into Splunk if needed

Copyright © 2023 Splunk, Inc. All rights reserved

# Estimating Index Growth Rate

- Splunk compresses the event's raw data as it is indexed
  - Indexing components are added to each bucket
  - Events with many searchable terms → **Larger index**
  - Events with fewer searchable terms and less variety → **Smaller index**
- **Best practice**:
  - Get a good growth estimate
  - Input your data in a test/dev environment over a sample period
    - If possible, index more than one bucket of events
  - Examine the size of the index's **db** directory compared to the input
    - MC: **Indexing > Indexes and Volumes > Index Detail: Instance**

docs.splunk.com/Documentation/Splunk/latest/Capacity/Estimateyourstoragerequirements


Copyright © 2023 Splunk, Inc. All rights reserved

# Calculating Index Storage

- Limiting size on disk is the most common method of controlling index growth
- Allocate disk space to meet data retention needs, using:
  - **Daily rate** of input
  - **Retention period** (in days)
  - **Compression factor** (~50% = %15 raw data + 35% for Splunk indexing)
  - **Padding** (50 GB recommended)

| Daily rate | x | Retention Period | x | Compress Factor | + | Padding | = | Total |
|---|---|---|---|---|---|---|---|---|
| **5 GB/day** | ***** | **180 days** | ***** | **0.5** | **+** | **50 GB** | **=** | **500 GB** |

- Configure index:

- On average, data for this index is deleted or frozen after ~6 months


Copyright © 2023 Splunk, Inc. All rights reserved

# Adding an Index

- Requires administration rights
- Using Splunk Web:
  - **Settings > Indexes > New Index**

- Using command line:

```
splunk add index <index_name> [-app <app_context>]
```

- Refer to:
  docs.splunk.com/Documentation/Splunk/latest/Indexer/SetupMultipleIndexes


Copyright © 2023 Splunk, Inc. All rights reserved

# Adding an Index With Splunk Web

Accepts alphanumeric, hyphens, and underscores (except at the beginning)

**Events** is the default index data type

Locations of buckets:
- Hot + Warm
- Cold
- Thawed

Optional data integrity check


Copyright © 2023 Splunk, Inc. All rights reserved | 9 May 2023

# Adding an Index With Splunk Web (cont.)

Overall index size (default = 500 GB)

Maximum bucket size:
- **`auto`** = 750 MB
- **`auto_high_volume`** = 10 GB

- Default (blank) is to delete
- Optionally set path

Sets where the **`indexes.conf`** file is saved:
**`SPLUNK_HOME/etc/apps/`*`appname`*`/local/`**

TSIDX Retention Policy (optional):
- Disabled by default; TSIDX files are not compressed
- When enabled, TSIDX files are compressed after this time



Copyright © 2023 Splunk, Inc. All rights reserved

# Initial Data Input Testing

- Use a Splunk test server
  - Should be running same version as production
- Use test indexes
- Procedure:
  1. Obtain sample of production data
  2. In Splunk Web: **Add Data** > **Upload**
  3. Check to see if **sourcetype** and other settings are applied correctly
  4. Delete the test data, change your test configuration, and repeat as necessary

Copyright © 2023 Splunk, Inc. All rights reserved

# Metrics

## Metrics

- Set of structured and numeric measurements containing **timestamp**, **metric name**, **value**, and a **dimension**
- Uses a custom index type ("Metrics"), optimized for metric storage + retrieval
- Discussed in detail in the Working with Metrics in Splunk course

Copyright © 2023 Splunk, Inc. All rights reserved

# Question: Preconfigured Indexes

Which of the following indexes are *not* preconfigured in Splunk?

A. `_audit`

B. `summary`

C. `itops`

D. `main`



Copyright © 2023 Splunk, Inc. All rights reserved

# Answer: Preconfigured Indexes

Which of the following indexes are *not* preconfigured in Splunk?

A. `_audit`

B. `summary`

C. **`itops`**

D. `main`

Splunk comes with these preconfigured indexes: **`_audit`** which stores audit trails, **`summary`** which stores summary indexing for reports, and **`main`** as a default index for inputs.

Indexes for additional input data, such as **`itops`**, must be created manually.


Copyright © 2023 Splunk, Inc. All rights reserved

# Question: Hot Bucket Rollover

What happens when hot buckets roll to warm buckets?

A. Bucket is renamed based on timestamps of the events

B. Bucket is moved to another folder

C. Bucket permissions change so it can no longer be searched

D. Bucket is archived if a Frozen Path is set


Copyright © 2023 Splunk, Inc. All rights reserved

# Answer: Hot Bucket Rollover

What happens when hot buckets roll to warm buckets?

**A. Bucket is renamed based on timestamps of the events**

B. Bucket is moved to another folder

C. Bucket permissions change so it can no longer be searched

D. Bucket is archived if a Frozen Path is set

When a hot bucket rolls over, the bucket is stays in the index's Home Path, and renamed from a hot bucket name format such as **`hot_v1_0`**, to a warm bucket name format based on event timestamps such as **`db_1389230491_1389230488_5`**.


Copyright © 2023 Splunk, Inc. All rights reserved

# Question: Default Frozen Path

What is the default Frozen Path for an index?

A. `SPLUNK_HOME/var/lib/splunk/<index>/colddb`
B. `SPLUNK_HOME/var/lib/splunk/<index>/frozendb`
C. `SPLUNK_HOME/var/lib/splunk/<index>/thaweddb`
D. No default; a Frozen Path must be set manually


Copyright © 2023 Splunk, Inc. All rights reserved

# Answer: Default Frozen Path

What is the default Frozen Path for an index?

A. `SPLUNK_HOME/var/lib/splunk/<index>/colddb`

B. `SPLUNK_HOME/var/lib/splunk/<index>/frozendb`

C. `SPLUNK_HOME/var/lib/splunk/<index>/thaweddb`

D. No default; a Frozen Path must be set manually

A Frozen Path is not set by default and must be entered manually.


Copyright © 2023 Splunk, Inc. All rights reserved

# Module 6 Lab

**Time:** 20 minutes

**Description:** Creating indexes

**Tasks:**

- Create a new index: **`securityops`**
- Add a file monitor input to send events to the **`securityops`** index


Copyright © 2023 Splunk, Inc. All rights reserved

# Module 7: Managing Indexes


Copyright © 2023 Splunk, Inc. All rights reserved

# Module Objectives

- Review Splunk Index Management basics
- Identify data retention recommendations
- Identify backup recommendations
- Move and delete index data
- Describe the use of the Fishbucket
- Restore a frozen bucket


Copyright © 2023 Splunk, Inc. All rights reserved

# Managing Indexes with Splunk Web

From Splunk Web: **Settings** > **Indexes**

## Indexes

A repository for data in Splunk Enterprise. Indexes reside in flat files on the Splunk Enterprise instance known as the indexer. Learn more

New Index

13 Indexes

filter

20 per page

| Name | Actions | Type | App | Current Size | Max Size | Event Count | Earliest Event | Latest Event | Home Path | Frozen Path | Status |
|---|---|---|---|---|---|---|---|---|---|---|---|
| _audit | Edit Delete Disable | Events | system | 4 MB | 488.28 GB | 39.5K | a day ago | a few seconds ago | $SPLUNK_DB/audit/db | N/A | Enabled |
| _internal | Edit Delete Disable | Events | system | 46 MB | 488.28 GB | 675K | a day ago | a few seconds ago | $SPLUNK_DB/_internaldb/db | N/A | Enabled |
| _introspection | Edit Delete Disable | Events | system | 84 MB | 488.28 GB | 107K | a day ago | a few seconds ago | $SPLUNK_DB/_introspection/db | N/A | Enabled |
| _metrics | Edit Delete Disable | Metrics | system | 42 MB | 488.28 GB | 638K | a day ago | a few seconds ago | $SPLUNK_DB/_metrics/db | N/A | Enabled |
| _metrics_rollup | Edit Delete Disable | Metrics | system | 1 MB | 488.28 GB | 0 | | | $SPLUNK_DB/_metrics_rollup/db | N/A | Enabled |
| _telemetr | | | | | 488.28 GB | 11 | a day ago | 18 minutes ago | $SPLUNK_DB/_telemetry/db | N/A | Enabled |
| _thefishb | | | | | 488.28 GB | 0 | | | $SPLUNK_DB/fishbucket/db | N/A | Enabled |
| history | | | | | 488.28 GB | 0 | | | $SPLUNK_DB/historydb/db | N/A | Enabled |
| main | Ed Delete Disable | | | | | | 5 years ago | 2 minutes ago | $SPLUNK_DB/defaultdb/db | N/A | Enabled |
| securityops | Edit Delete Disable | | | | | | 3 months ago | 11 minutes ago | $SPLUNK_DB/securityops/db | N/A | Enabled |
| splunklogger | Edit Delete Enable | | | | | | | | $SPLUNK_DB/splunklogger/db | N/A | Disabled |
| summary | Edit Delete Disable | | | | | | | | $SPLUNK_DB/summarydb/db | N/A | Enabled |

Click index name or **Edit** to launch the **Edit Index** dialog box

Custom indexes can be enabled/disabled or deleted



Copyright © 2023 Splunk, Inc. All rights reserved

# Index Definitions and Data

| | |
|---|---|
| **Index Definition**<br>(`indexes.conf`) | `SPLUNK_HOME/etc/system/default`<br>`SPLUNK_HOME/etc/system/local`<br>`SPLUNK_HOME/etc/apps/<app_name1>/local`<br>`SPLUNK_HOME/etc/apps/<app_name2>/local`<br>`SPLUNK_HOME/etc/apps/...` |
| **Indexed Data**<br>(Buckets) | `SPLUNK_HOME/var/lib/splunk/<index_name>/db`<br>`SPLUNK_HOME/var/lib/splunk/<index_name>/colddb`<br>`SPLUNK_HOME/var/lib/splunk/<index_name>/thaweddb` |


Copyright © 2023 Splunk, Inc. All rights reserved

# The **indexes.conf** File

The index stanza is created in **indexes.conf** of the selected app (in **SPLUNK_HOME/etc/apps/<*appname*>/local/**)

```
[itops]
homePath = /mnt/ssd/splunk/itops/db
coldPath = /mnt/san/splunk/itops/colddb
thawedPath = $SPLUNK_DB/itops/thaweddb
maxDataSize = auto_high_volume
maxTotalDataSizeMB = 307200
enableDataIntegrityControl = 0
```

Index name

Paths must be specified, even when using the defaults

Maximum bucket size:
- **auto** = 750 MB
- **auto_high_volume** = 10 GB

Maximum total size of index = 300 GB


Copyright © 2023 Splunk, Inc. All rights reserved

# Additional **`indexes.conf`** Options

```
[itops]
frozenTimePeriodInSecs = 31536000
maxHotSpanSecs = 86400
homePath.maxDataSizeMB = 100000
coldPath.maxDataSizeMB = 400000
...
```

**Note**

Values shown are the defaults.



Copyright © 2023 Splunk, Inc. All rights reserved

# Viewing Indexing Activity and Health in the MC

- Provides comprehensive indexing activity details
- **Snapshot** shows averages over the previous 15 minutes
- **Historical** exposes trending and possible decaying health

Monitoring Console (MC)

- Volume usage per index
- Index size over time

- Detailed indexing status
- Retention policies
- Bucket configuration details

- Queue fill-ratio
- Indexing rate
- CPU activity

Displays the usage versus capacity, if the volume-based retention is used (**`maxVolumeDataSizeMB`**)


Copyright © 2023 Splunk, Inc. All rights reserved

# Monitoring Indexes with MC

MC: Indexing > Indexes and Volumes > Indexes and Volumes: Instance Index

## Indexes and Volumes: Instance

Index Type
- Event Indexes Only
- All Index Types *

Group: All Indexers

Search produced no results.

Instance: splunk02

Hide Filters

The "All Index Types" option is not compatible with indexers running Splunk Enterprise 6.6 or earlier, whe

Allows you to select index type, indexer group, or instance

Select views: All | Snapshot | Historical

### Snapshots

0.22 GB

Total Index Size

1,

Select an index to see more details

Indexes (9)

| Index | Data Type | Data Age vs Frozen Age (days) | Index Usage (GB) |
|---|---|---|---|
| _audit | event | 1 / 2184 | 0.00 / 488.28 |
| _internal | event | 1 / 30 | 0.04 / 488.28 |
| _introspection | event | 1 / 14 | 0.08 / 488.28 |
| _telemetry | event | 1 / 730 | 0.00 / 488.28 |
| main | event | 1806 / 2184 | 0.08 / 488.28 |
| securityops | event | 91 / 2184 | 0.01 / 500.00 |

Volumes

| Index Directory | Volume Name | Volume Freezing Due to Size | Volume Usage / Ca |
|---|---|---|---|
| home | one | No | 0.00 / 39.06 |
| cold | two | No | 0.00 / 78.13 |

A volume is considered to be freezing or about to freeze data at 95% or more of configured disk usage capacity.

Bucket Size (GB)

Bucket Event Count

Bucket Count

Event Count by Hosts (1)

| Host | Event Count |
|---|---|
| mailsv1 | 4084 |

Event Count by Sources (1)

| Source | Event Count |
|---|---|
| /opt/log/mailsv1/maillog | 4084 |

Event Count by Sour

| Sourcetype |
|---|
| sendmail_syslog |

Settings

Paths

| Setting | Value |
|---|---|
| homePath | volume:one/itops/db |
| homePath_expanded | /opt/home/cb_07/one/itops/db |

Retention policies

| Setting | Value |
|---|---|
| maxTotalDataSizeMB | 102400 |
| frozenTimePeriodInSecs | 188697600 |

Index Structure & Bu

| Setting |
|---|
| maxDataSize |
| maxHotBuckets |



Copyright © 2023 Splunk, Inc. All rights reserved | 9 May 2023

# Index Data Integrity Check

- Validates integrity of indexed data with SHA256-based hashes
- When enabled:
  - Produces hash files for auditing and legal purposes
  - Works on index level, including clustering
  - Does not protect in-flight data from forwarders (use SSL)
- Use the indexer acknowledgment capability (**`useACK`**) to prevent data loss
- Verify integrity of an index/bucket: **`splunk check-integrity …`**

docs.splunk.com/Documentation/Splunk/latest/Security/Dataintegritycontrol


Copyright © 2023 Splunk, Inc. All rights reserved

# Configuring High-volume Indexes

- Set specific options by editing the stanza in **`indexes.conf`**
- **Best practice** for high-volume indexes:
  - Change index default of 3 hot buckets to 10 hot buckets using the **`maxHotBuckets`** key
  - Examine and copy settings of **`main`** index stanza and adjust for use case

**Warning**

Incorrect retention settings can cause premature bucket rotation and even stop Splunk. It is advised to contact Splunk Professional Services before editing retention policies.


Copyright © 2023 Splunk, Inc. All rights reserved

# Strict Time-based Retention Policies

- Scenario: Purge HR data when it is more than 90 days old
- Issues to consider:
  - Splunk freezes entire buckets, not individual events
  - If a bucket spans more than one day, you can't strictly meet the 90 day requirement
- Configuration option:

  **`frozenTimePeriodInSecs = 7776000`** (~90 days)

  **`maxHotSpanSecs = 86400`** (~24 hours)

**Warning**

These options satisfy the strict data retention policy but may negatively impact performance.

Using small **`maxHotSpanSecs`** under indexer clustering is not recommended because it can produce many small buckets.

Monitor bucket size and the rate of accumulation (in terms of bucket count) closely after changes.


Copyright © 2023 Splunk, Inc. All rights reserved

# Buckets on Different Storage Systems

splunk> Best Practice

- Use a high-performance file system to store indexes
  - Bucket time span and storage type affects search performance
- Use multiple storage systems for buckets
  - Specify fastest storage for **Home path** (Hot/Warm buckets)
  - Specify slower, less expensive storage for **Cold path** (Cold buckets)
- Refer to: docs.splunk.com/Documentation/Splunk/latest/Indexer/HowSplunkstoresindexes

Copyright © 2023 Splunk, Inc. All rights reserved

# Volume Stanzas in **indexes.conf**

- Example: Prevent data bursts in one index from triggering indexing issues elsewhere in the same volume
- Issues to consider:
  - Splunk cannot determine the maximum size for non-local volumes
  - Hot/warm and cold buckets can be in different volumes
  - If the volume runs out of space, buckets roll to frozen before **frozenTimePeriodInSecs**
- Configuration Options: Use volume reference for a retention based on size

```
[volume:fast]
path = /mnt/ssd/
maxVolumeDataSizeMB = 800000

[volume:slow]
path = /mnt/raid/
maxVolumeDataSizeMB = 4000000
```

```
[soc]
homePath = volume:fast/soc/db
homePath.maxDataSizeMB = 50000
coldPath = volume:slow/soc/colddb
coldPath.maxDataSizeMB = 200000
```


Copyright © 2023 Splunk, Inc. All rights reserved

# Setting the Last Chance Index

- Provides ability to define a last chance index for events destined for non-existent indexes
  - If **`lastChanceIndex`** setting is not defined, Splunk drops these events
  - Defaults to empty

**indexes.conf**

```
[default]
lastChanceIndex =
```

```
[Input Y]
index = $%^&*
```

**indexes.conf**

```
[default]
lastChanceIndex = lastchance
```

```
[Input Y]
index = $%^&*
```

**lastchance**


Copyright © 2023 Splunk, Inc. All rights reserved

# What to Back Up

- Splunk indexes
  - By default, stored in: **`SPLUNK_HOME/var/lib/splunk/`**
  - See **`indexes.conf`** if custom locations are used
- Monitored source data files (optional)
- Splunk configuration and important files in: **`SPLUNK_HOME/etc`**

  **`apps`**

  **`users`**

  **`system/local`**

  **`licenses`**

  **`init.d`**

  **`passwd`**

  and more


Copyright © 2023 Splunk, Inc. All rights reserved

# Backup Recommendation

- Use the incremental backup of your choice
  - Warm and cold buckets of your indexes
  - Configuration files
  - User files
- Hot buckets cannot be backed up without stopping Splunk
  - Use the snapshot capability of underlying file system to take a snapshot of hot, then back up the snapshot
  - Schedule multiple daily incremental backups of warm buckets for high data volumes


Copyright © 2023 Splunk, Inc. All rights reserved

# Moving an Index

1. Stop Splunk
2. Copy the entire index directory to new location while preserving permissions and all subdirectories

| | |
|---|---|
| Linux | **`cp -rp <source> <target>`** |
| Windows | **`xcopy <source> <target> /s /e /v /o /k`**<br>(or use **Robocopy**) |

3. Edit **`indexes.conf`** to indicate the new location
4. Start Splunk
5. After testing and verifying new index, the old one can be deleted


Copyright © 2023 Splunk, Inc. All rights reserved

# Removing Indexed Events

- Splunk does not provide the ability to modify the contents of an index
- Modify your data input (and any parsing settings) so future events are correct
- For undesired events already in the index, options are:
  - Let the events age out normally (whole bucket ages out)
  - Use the **`delete`** command to hide unwanted events from searches
  - Run **`splunk clean`** command to delete ALL events from the index
  - Delete and re-create the index

**Warning**

These options should be used with extreme caution!


Copyright © 2023 Splunk, Inc. All rights reserved

# Hiding Events Using the **`delete`** Command

- Virtually deletes events by marking them as “deleted”
  - Prevents “deleted” events from appearing in future searches
  - Does not reclaim disk space
  - Cannot be undone
- Only available to users who are members of the **`can_delete`** role
  - By default, no user is a member of this role
- Ensure your search results are limited to the desired events, then pipe to the **`delete`** command:

```
index=soc host=www1 source=access.log | delete
```

Last 4 hours


Copyright © 2023 Splunk, Inc. All rights reserved

# Cleaning Out an Index

- To flush indexed events and reset an index, use the **`clean`** command
  - DATA WILL BE PERMANENTLY DESTROYED
  - Typically used on test/dev systems, not production systems
- Command syntax:

  **`splunk clean [eventdata|userdata|all] [-index index_name]`**
  - **`eventdata`**: Delete indexed events and metadata on each event
  - **`userdata`**: Delete user accounts
  - **`all`**: Everything, including users, saved searches, and alerts

**Warning**

If no index is specified for the **`splunk clean`** command, the default is to clean (destroy) all indexed events from *all* indexes. Always specify an index!


Copyright © 2023 Splunk, Inc. All rights reserved

# Fishbucket

## Fishbucket

- Allows Splunk to track monitored input files
- Contains file metadata which identifies a pointer to the file, and a pointer to where Splunk last read the file
- Exists on all Splunk instances
- Stored in a special subdirectory found at **`SPLUNK_DB/fishbucket`**

Includes:

- **Head**: Pointer to the file
- **Tail**: Pointer showing where Splunk last left off indexing in the file


Copyright © 2023 Splunk, Inc. All rights reserved

# Resetting Input File Monitors

1. Stop Splunk
2. Reset applicable file monitors
   - Individually for each source:

```
splunk cmd btprobe -d SPLUNK_DB/fishbucket/splunk_private_db
  --file <source> --reset
```

   - All sources (use only on test systems / with extreme caution):

```
splunk clean eventdata -index _thefishbucket
```

*or*

```
rm -r SPLUNK_DB/fishbucket
```

3. Start Splunk

**Warning**

Resetting the fishbucket forces re-indexing of all file monitors affected. This results in more license usage.


Copyright © 2023 Splunk, Inc. All rights reserved

# Restoring a Frozen Bucket

- To thaw a frozen bucket:
  1. Copy the bucket directory from the Frozen Path to the index's Thawed Path (**`thaweddb`**) directory
  2. Run **`splunk rebuild <Thawed_Path>`**
     - Does not count against Splunk license
     - Does recreate Splunk indexing files (takes additional storage)
  3. Restart Splunk
- Events in **`thaweddb`** are searchable along with other events
  - Will not be frozen again
  - Do not count against the index max size
- Delete the thawed bucket directory when no longer needed and restart Splunk

Copyright © 2023 Splunk, Inc. All rights reserved

# Further Reading

- docs.splunk.com/Documentation/Splunk/latest/Indexer/HowSplunkstoresindexes
- docs.splunk.com/Documentation/Splunk/latest/Indexer/Setlimitsondiskusage
- docs.splunk.com/Documentation/Splunk/latest/Indexer/Automatearchiving


Copyright © 2023 Splunk, Inc. All rights reserved

# Question: Valid **`indexes.conf`** Entries

Which of the following is an invalid **`indexes.conf`** entry for a newly created **`itops`** index?

A. `homePath = $SPLUNK_DB/itops/db`

B. `coldPath = /mnt/san/splunk/itops/colddb`

C. `maxDataSize = auto_high_volume`

D. `maxTotalDataSizeMB = -1`


Copyright © 2023 Splunk, Inc. All rights reserved

# Answer: Valid **`indexes.conf`** Entries

Which of the following is an invalid **`indexes.conf`** entry for a newly created **`itops`** index?

A. `homePath = $SPLUNK_DB/itops/db`

B. `coldPath = /mnt/san/splunk/itops/colddb`

C. `maxDataSize = auto_high_volume`

D. **`maxTotalDataSizeMB = -1`**

**`maxTotalDataSizeMB`** sets the maximum size of an index, in megabytes, and must be a non-negative integer. The default value is 500 GB. When this value is reached, index buckets are either rolled to frozen (if a Frozen Path is set) or deleted.


Copyright © 2023 Splunk, Inc. All rights reserved

# Question: The Fishbucket

Which of the following is true about the Splunk Fishbucket?

A. Contains no file metadata
B. Allows Splunk to track monitored files
C. Exists only on Splunk Enterprise instances
D. Stored in a special subdirectory found at `SPLUNK_HOME/fishbucket`


Copyright © 2023 Splunk, Inc. All rights reserved

# Answer: The Fishbucket

Which of the following is true about the Splunk Fishbucket?

A. Contains no file metadata

**B. Allows Splunk to track monitored files**

C. Exists only on Splunk Enterprise instances

D. Stored in a special subdirectory found at `SPLUNK_HOME/fishbucket`

The Fishbucket tracks monitored input files, contains file metadata including pointers to where Splunk last read the file, exists on all Splunk instances including Universal Forwarders, and is found under **`SPLUNK_DB/fishbucket`** (which is **`SPLUNK_HOME/var/lib/splunk/fishbucket`**).


Copyright © 2023 Splunk, Inc. All rights reserved

# Question: Restoring a Frozen Bucket

What step is *NOT* used to restore a frozen bucket?

A. Copy the frozen bucket directory to index's Thawed Path

B. Run `splunk thaw <bucket_id>` command

C. Run `splunk rebuild <Thawed_Path>` command

D. Restart Splunk



Copyright © 2023 Splunk, Inc. All rights reserved 

# Answer: Restoring a Frozen Bucket

What step is *NOT* used to restore a frozen bucket?

A. Copy the frozen bucket directory to index's Thawed Path

B. Run **`splunk thaw <bucket_id>`** command

C. Run `splunk rebuild <Thawed_Path>` command

D. Restart Splunk

Restoring (thawing) a frozen bucket requires that: 1. the bucket be copied to the Thawed Path, 2. running a **`splunk rebuild`** command which ingests the data, but does not count against license use, and 3. restarting Splunk.


Copyright © 2023 Splunk, Inc. All rights reserved

# Module 7 Lab

**Time:** 25 minutes

**Description:** Managing Indexes

**Tasks:**

- Use the MC to view **`securityops`** index information
- Configure a time-based retention policy
- Create the **`itops`** index
- Configure a volume-based retention policy for **`itops`**


Copyright © 2023 Splunk, Inc. All rights reserved

# Module 8: Managing Users


Copyright © 2023 Splunk, Inc. All rights reserved

# Module Objectives

- Describe user roles in Splunk
- Add Splunk users using native authentication
- Create a custom role
- Manage users in Splunk


Copyright © 2023 Splunk, Inc. All rights reserved

# Users and Roles

## Users

- Provide access to a Splunk instance
- Supported natively in Splunk, or with external identity providers (such as LDAP and SAML)

## Roles

- Define a Splunk user's capabilities and access to data sources
- Assigned to users

**Web users** → **Web role**

- Search the Web index

**Security users** → **Security role**

- Search the Web, Proxy and Security indexes

**Splunk admins** → **Admin role**

- Splunk administration
- Search all indexes


Copyright © 2023 Splunk, Inc. All rights reserved

# Managing Users and Roles

Copyright © 2023 Splunk, Inc. All rights reserved

# User Authentication in Splunk

## Native authentication

- Creates accounts directly in Splunk (example: **`admin`** user)
- Stores passwords in **`SPLUNK_HOME/etc/passwd`**
- Can be disabled with a blank Splunk **`passwd`** file
- Best Practice: Keep a failsafe account in the **`passwd`** file with a very strong password

## Other supported authentication

- Splunk integration with LDAP
- Scripted authentication API
- Splunk enforces precedence of native authentication over other models


Copyright © 2023 Splunk, Inc. All rights reserved

# Viewing and Managing Users

- Splunk native users can be edited or deleted
- Only time zone and default app can be changed on LDAP and other non-Splunk native users

Copyright © 2023 Splunk, Inc. All rights reserved | 9 May 2023

# Native Authentication: Adding Users

Defaults to search head time zone

Defaults to role's default app (or **Home** if not set in the role)

Defaults to **user** role only



Copyright © 2023 Splunk, Inc. All rights reserved | 9 May 2023

# Identifying Roles

| Built-in role | Overview of capabilities |
|---|---|
| **`admin`** | Has most capabilities; can create custom roles |
| **`power`** | Edit shared objects, saved searches, and alerts, tag events, and so on |
| **`user`** | Create, edit, and run own saved searches, edit own preferences, create and edit event types, and similar tasks |
| **`can_delete`** | Delete by keyword (necessary when using the **`delete`** search operator) |
| **`splunk-system-role`** | Allows Splunk system services to run without a defined user context |
| **`securegateway`** | Register devices or use features of Splunk Secure Gateway |


Copyright © 2023 Splunk, Inc. All rights reserved

# Creating User Roles: Inheritance

Create a name for the role

Inheritance:

- Can be based on one or more existing roles
- Provides inherited capabilities *and* index access


Copyright © 2023 Splunk, Inc. All rights reserved

# Creating User Roles: Capabilities

**Source** drop-down menu filters the displayed role capabilities

Capabilities **inherited** from other roles are pre-checked and cannot be removed


Copyright © 2023 Splunk, Inc. All rights reserved

# Creating User Roles: Indexes

Defines indexes used when user does not specify "**index=<*index_name*>**" in search

Controls which indexes user has access to

Drop-down menu filters the index list

**Note**

Indexes inherited from a parent role are searchable and cannot be disabled. These appear as greyed out check boxes.



Copyright © 2023 Splunk, Inc. All rights reserved | 9 May 2023

# Index Search Restrictions

- Index access is permissive
  - New non-internal indexes are searchable (by default)
- Implement index restriction to meet data access policies
- For test and staging indexes
  - Restrict access to Splunk admins
  - Consider the amount and value of sample ingest data
  - Use **Wildcard** index grouping to restrict access (such as **`*test*`**)

Copyright © 2023 Splunk, Inc. All rights reserved | 9 May 2023

# Creating User Roles: Restrictions

- Use combination of **Indexed fields**, **Values**, **Concatenation option** and click **Add to search filter**
- Also manually type in content


Copyright © 2023 Splunk, Inc. All rights reserved

# Creating User Roles: Resources

- **Infinite** (0): No restrictions
- **Unset** (-1): Allows window limit to be overridden by inherited roles
- **Custom time**: Limit, in seconds

Copyright © 2023 Splunk, Inc. All rights reserved

# The **authorize.conf** File

- Contains the Splunk role configuration
- Should not be modified from the **default** directory:

  **SPLUNK_HOME/etc/system/default/authorize.conf**

- Should only be modified from the **local** directories:

  **SPLUNK_HOME/etc/system/local** or
  **SPLUNK_HOME/etc/apps/<*appname*>/local**

**authorize.conf**
(example entries)

*Role name*

```
[role_webusers]
srchIndexesAllowed = main;websales
srchIndexesDefault = websales
srchMaxTime = 8640000
```


Copyright © 2023 Splunk, Inc. All rights reserved | 9 May 2023

# Creating a Copy of an Existing Role

- Using inheritance:
  - Create a new role and configure the **1. Inheritance** tab
  - Provides all the capabilities and index settings of the inherited role
  - Prevents disabling inherited capabilities or index access
- Without inheritance:
  1. Use **Edit > Clone** in Splunk Web
  2. Modify the new role as needed

Copyright © 2023 Splunk, Inc. All rights reserved

# Example Scenario With **edit_roles_grantable**

## Example scenario:

Separate and delegate user administration tasks

1. Create a new role of **user_admin**
   - New role can assign roles to other users
   - New role cannot grant the **admin** role to self or others
2. Assign **user_admin** role to Amanda Curry (user: **acurry**)

## Issues to consider:

- Capabilities **edit_user** + **edit_roles** allows user to promote themselves to full admin
- Capabilities **edit_user** + **edit_roles_grantable** only allows user to assign a subset of roles they currently have


Copyright © 2023 Splunk, Inc. All rights reserved | 9 May 2023

# Assigning **edit_roles_grantable** Capability

Create new role: **user_admin**

Inheritance: **power**, **user**

Capabilities: **edit_user**, **edit_roles_grantable**



Copyright © 2023 Splunk, Inc. All rights reserved

# Password Policy Management

- Provides options for password rules, expiration, lockout, and history
- Only applies to native Splunk users (not SAML or LDAP passwords)

docs.splunk.com/Documentation/Splunk/latest/Security/Passwordbestpracticesforadministrators


Copyright © 2023 Splunk, Inc. All rights reserved

# Unlocking Users

- For users who have exceeded failed login attempts threshold
  - Configured in **Password Management**

- Using Splunk Web:
  - **Settings** > **Users,** then **Edit** > **Unlock**:

- Using CLI:

```
splunk edit user <locked_user> -locked-out false –auth <admin_user:password>
```


Copyright © 2023 Splunk, Inc. All rights reserved | 9 May 2023

# Admin Passwords

- An Admin password is **required** during installation and to start Splunk for the first time
- To create a password during startup:

```
splunk start --accept-license --answer-yes --no-prompt --seed-passwd <password>
```

- To generate a random password during startup:

```
splunk start --accept-license --answer-yes --no-prompt --gen-and-print-passwd
```

docs.splunk.com/Documentation/Splunk/latest/Security/Secureyouradminaccount


Copyright © 2023 Splunk, Inc. All rights reserved

# Splunk Authentication Options

## Authentication Methods

Select an authentication method. Splunk supports native authentication as well as the following external methods:

Internal ☑ Splunk Authentication (always on)

External
- ◉ None
- ○ LDAP
- ○ SAML

### Multifactor Authentication

Not available with external authentication such as SAML.

- ◉ None
- ○ Duo Security
- ○ RSA Security

Reload authentication configuration

USERS AND AUTHENTICATION

- Roles
- Users
- Tokens
- Password Management
- Authentication Methods

**Note**

More details on using alternate authentication methods is provided in Appendix B.

Scripted access to PAM, RADIUS, or other user account systems are also supported.


Copyright © 2023 Splunk, Inc. All rights reserved

# Configuring LDAP Strategies

## Authentication Methods

Select an authentication method. Splunk supports native authentication as well as the following external me

Internal — Splunk Authentication (always on)

External
- None
- LDAP
- SAML

Configure Splunk to use LDAP

## LDAP strategies

Authentication Methods » LDAP strategies

filter

There are no configurations of this type. Click the "New LDAP" button to create a new configuration.

New LDAP

## Add new

Authentication Methods » LDAP strategies » Add new

LDAP strategy name * AD_splunkers

Enter a unique name for this strategy.

**LDAP connection settings**

Host * 10.0.0.150

Your Splunk server must be able to resolve thi

Port 389

The LDAP server port defaults to 389 if you ar

SSL enabled

You must also have SSL enabled on your LDAI

Bind DN adsuser@buttercupgames.local

This is the distinguished name used to bind to with access to all LDAP users you wish to add bind is sufficient.

Bind DN Password ••••••••••

Enter the password for your Bind DN user.



Copyright © 2023 Splunk, Inc. All rights reserved | 9 May 2023

# Configuring SAML

## Authentication method

Access controls » Authentication method

Select an authentication method. Splunk supports native authentication as well as the following external

Internal — Splunk Authentication (always on)

External — None / LDAP / SAML

Configure Splunk to use SAML

## SAML Groups

Map the groups from your SAML server to roles in Splunk Enterprise.
Once mapped, SAML groups possess the abilities and permissions of the assigned Splunk roles.
Click SAML Configuration to modify your existing SAML setup. Click New Group to add a new SAML group. Learn more

SAML Configuration

0 SAML Groups — filter — 20 pe

| Name | Actions | Roles | Status |
|---|---|---|---|

No SAML Groups are defined.

## SAML Configuration

WARNING: An error in configuring SAML could result in users and admins being locked out of access the local login and revert back to None for authentication if you are locked out:

https://{name}.splunkcloud.com/en-US/account/login?loginType=splunk [replace {name} with y

Be sure to copy this information to a safe place before closing this window.

Configure SAML for Splunk. Learn More

Download the SPMetadata from Sp and add it to

SP Metadata File — Download File

Import Identity Provider (IdP) metadata by browsing Contents text box.

Metadata XML File — Select File

Metadata Contents

**General Settings**

Single Sign On (SSO) URL ?

1. Export Splunk SP Metadata XML
2. **On IdP Server**: Upload Splunk file, configure relationship, export IdP metadata
3. Import IdP metadata
4. Configure settings



Copyright © 2023 Splunk, Inc. All rights reserved | 9 May 2023

# Mapping LDAP / SAML Groups to Roles

- User cannot log in unless they have a Splunk role
- Not all groups must be mapped
- Mappings can be changed at any time

| LDAP strategy name | Host | Port | Connection order | Status | Actions |
|---|---|---|---|---|---|
| AD_splunkers | 10.0.0.150 | 389 | 1 | Enabled \| Disable | Map groups \| Clone \| Delete |

| LDAP Group Name | LDAP Strategy | Group type | Roles |
|---|---|---|---|
| splunkAdmins | AD_splunkers | static | admin |
| splunkBizDev | AD_splunkers | static | user |
| splunkITOps | AD_splunkers | static | power |
| splunkSOC | AD_splunkers | static | soc_analyst |


Copyright © 2023 Splunk, Inc. All rights reserved

# Question: Admin Accounts

Which Splunk instances *require* an admin account?

A. Indexers

B. Search Heads

C. Universal Forwarders

D. All of the above


Copyright © 2023 Splunk, Inc. All rights reserved

# Answer: Admin Accounts

Which Splunk instances *require* an admin account?

A. Indexers

B. Search Heads

C. Universal Forwarders

**D. All of the above**

Splunk requires an admin account on each Splunk instance.


Copyright © 2023 Splunk, Inc. All rights reserved

# Question: Creating Similar Roles

If you want a role that is similar to the **`user`** role but with some capabilities turned off?

A. Create a new role that inherits from **`user`** and remove capabilities
B. Clone the **`user`** role and modify it as needed
C. Give the **`user`** role the **`edit_roles_grantable`** capability
D. Use a supported authentication method such as LDAP or SAML


Copyright © 2023 Splunk, Inc. All rights reserved

# Answer: Creating Similar Roles

If you want a role that is similar to the **`user`** role but with some capabilities turned off?

A. Create a new role that inherits from `user` and remove capabilities

**B. Clone the `user` role and modify it as needed**

C. Give the `user` role the `edit_roles_grantable` capability

D. Use a supported authentication method such as LDAP or SAML

A new role that inherits from `user` role will not allow inherited capabilities to be removed. Instead close the `user` role to make a new copy of that role, and modify as needed.


Copyright © 2023 Splunk, Inc. All rights reserved

# Question: Unlocking a User Account

How can you unlock a Splunk user account?

A. Use Multifactor Authentication

B. Set a value for **Policy Management > Failed Login Attempts**

C. Run `splunk start --seed-passwd <password>`

D. Run `splunk edit user <locked_user> -locked-out false`


Copyright © 2023 Splunk, Inc. All rights reserved

# Answer: Unlocking a User Account

How can you unlock a Splunk user account?

A. Use Multifactor Authentication

B. Set a value for **Failed Login Attempts** under **Policy Management**

C. Run `splunk start --seed-passwd <password>`

D. Run **`splunk edit user <locked_user> -locked-out false`**

Unlocking a user is performed in Splunk Web under **Settings** > **Users** with **Edit** > **Unlock**, or command line with **`splunk edit user <locked_user> -locked-out false`**.


Copyright © 2023 Splunk, Inc. All rights reserved

# Module 8 Lab 8a (1/3)

**Time:** 15 minutes

**Description:** Managing Users and Roles

**Tasks:**

- Edit existing roles
- Create a new role and assign it to a user
- Verify the configurations


Copyright © 2023 Splunk, Inc. All rights reserved

# Module 8 Lab 8b (2/3)

**Time:** 20 minutes

**Description:** Examine User Configuration files

**Tasks:**

- Run the same search as different users
- Check the search results and compare
- Use the **`btool`** command to investigate configurations


Copyright © 2023 Splunk, Inc. All rights reserved

# Module 8 Lab 8c (3/3)

**Time:** 15 minutes

**Description:** Managing Active Directory Users

**Tasks:**

- Configure Splunk to use LDAP
- Map LDAP groups to Splunk roles
- Verify the LDAP configuration

Host: **`10.0.0.150`**
Port: **`389`**
Username: **`aduser@buttercupgames.local`**
Password: **`open.sesam3`**


Copyright © 2023 Splunk, Inc. All rights reserved

# Module 9:
# Configuring Basic Forwarding


Copyright © 2023 Splunk, Inc. All rights reserved

# Module Objectives

- Identify forwarder configuration steps
- Configure a Universal Forwarder
- Understand the Deployment Server


Copyright © 2023 Splunk, Inc. All rights reserved

# Forwarders and Indexers

## Indexer

- Runs on dedicated servers
- Listens on receiving ports
- Stores and indexes the data

## Forwarder

- Gathers the data
- Sends to indexers over network
  - Most production data is on remote servers

Copyright © 2023 Splunk, Inc. All rights reserved

# Universal Forwarders (UF)

## Universal Forwarders (UF)

- Gathers data from a host
- Sends data over the network to receiving ports on receivers (usually an indexer)
- Provided as separate installation binary with a built-in license (no limits)
- Designed to run on production servers

  (minimal CPU / memory use, bandwidth constrained to 256 KBps by default, no web interface, cannot search or index)

Copyright © 2023 Splunk, Inc. All rights reserved

# Universal Forwarder Configuration Steps

1. Configure a receiving port on each indexer (one-time task)
2. Download and install Universal Forwarder
3. Configure forwarding on forwarders
4. Add inputs on forwarders

Copyright © 2023 Splunk, Inc. All rights reserved

# 1. Configure Receiving Port on Each Indexer

- Using Splunk Web:
  1. Select **Settings** > **Forwarding and receiving**
  2. Next to **Configure receiving**, select **Add new**
  3. Enter a port number and click **Save**
  - Stored in most recently visited app: **`SPLUNK_HOME/etc/apps/<app>/local`**
- Using CLI:
  - Run **`splunk enable listen <port>`**
  - Stored in **`SPLUNK_HOME/etc/apps/search/local`**
- Manually in **`inputs.conf`** as:

  **`[splunktcp://port]`**

Copyright © 2023 Splunk, Inc. All rights reserved | 9 May 2023

# 2. Installing a Universal Forwarder

| | *NIX | Windows |
|---|---|---|
| *Download* | www.splunk.com/en_us/download/universal-forwarder.html | |
| *Install* | • Un-compress **.tgz**, **.rpm**, or **.deb** file in the path Splunk will run from<br>• Default **SPLUNK_HOME** is: **/opt/splunkforwarder** | • Execute **.msi** installer (or use the CLI)<br>• Default **SPLUNK_HOME** is: **C:\Program Files\SplunkUniversalForwarder** |

- Silent installation methods exist on all platforms
- Same **splunk** command-line interface in **SPLUNK_HOME/bin**
  - Same commands for start/stop, restart, etc.
  - An admin account and password are required


Copyright © 2023 Splunk, Inc. All rights reserved

# Using the Interactive Windows Installer

- Most forwarder settings can be configured using the installer wizard
  - Can run as a local or domain user without local administrator privileges
- CLI installation is available for scripted installations:

  docs.splunk.com/Documentation/Forwarder/latest/Forwarder/InstallaWindowsuniversalforwarderfromthecommandline

Copyright © 2023 Splunk, Inc. All rights reserved

# 3. Configure Forwarding on Forwarders

- To configure target indexers on forwarders, either:
  - Run **`splunk add forward-server <indexer:receiving_port>`**
  - Modify **`outputs.conf`**
- Splunk logs are automatically sent to indexer's **`_internal`** index
- Example: **`splunk add forward-server 10.1.2.3:9997`** configures **`outputs.conf`** as:

```
[tcpout]
defaultGroup = default-autolb-group

[tcpout-server://10.1.2.3:9997]

[tcpout:default-autolb-group]
disabled = false
server = 10.1.2.3:9997
```

docs.splunk.com/Documentation/Forwarder/latest/Forwarder/Configureforwardingwithoutputs.conf


Copyright © 2023 Splunk, Inc. All rights reserved

# 4. Add Inputs On Forwarders

- Use Splunk CLI

```
./splunk add monitor /opt/log/www2/access.log -sourcetype access_combined_wcookie -index test
```

- Create  Splunk config file (**`inputs.conf`**)

```
[monitor:///opt/log/www2/access.log]
disabled = false
index = test
sourcetype = access_combined_wcookie
```

- Use Spunk Web to **Add Data > Forward**
  - Performed on a Deployment Server
  - Requires deployment clients
  - Requires DS configurations such as server class
  - Discussed in *Splunk Enterprise Data Administration* course

Copyright © 2023 Splunk, Inc. All rights reserved | 9 May 2023

# Forwarder **`outputs.conf`** File

- Points the forwarder to the receivers
  - **`splunktcp`** stanza sets the indexer to listen on a port for feeds from Splunk forwarders
  - **`server`** sets a forwarder's destination to one or more receivers (IP or DNS name + receiver port), separated by commas
- Can specify additional options:
  - Load balancing
  - SSL
  - Compression
  - Alternate indexers
  - Indexer acknowledgement

Copyright © 2023 Splunk, Inc. All rights reserved

# Configuration Validation and Troubleshooting

- To verify the configuration:
  - On forwarder, run: **`splunk list forward-server`**
  - On indexer, run: **`splunk display listen`**
- To verify successful connection:
  - On search head, search: `index=_internal host=<forwarder_hostname>`
- Troubleshooting forwarder connection
  - Check **`SPLUNK_HOME/var/log/splunk/splunkd.log`** on forwarder:
    **`tail -f splunkd.log | egrep 'TcpOutputProc|TcpOutputFd'`**


Copyright © 2023 Splunk, Inc. All rights reserved

# Deployment Server (DS)

## Deployment Server (DS)

- Built-in tool for centrally managing configuration packages as apps for clients
- Includes **Forwarder Management** as the graphical user interface
- Can restart remote Splunk instances
- Requires an Enterprise license and should be on a dedicated server

Note

This topic is covered in the *Splunk Enterprise Data Administration* course.


Copyright © 2023 Splunk, Inc. All rights reserved

# Question: Receiving Ports

What is the minimum number of receiving ports on an indexer so that it can ingest data from 3 Universal Forwarders that each have 2 data inputs?

A. 0 ports

B. 1 port

C. 3 ports

D. 6 ports


Copyright © 2023 Splunk, Inc. All rights reserved

# Answer: Receiving Ports

What is the minimum number of receiving ports on an indexer so that it can ingest data from 3 Universal Forwarders that each have 2 data inputs?

A. 0 ports

**B. 1 port**

C. 3 ports

D. 6 ports

An indexer needs one receiving port to be able to get data from universal forwarders. Many forwarders can forward data to the same port. You can optionally configure more receiving ports.


Copyright © 2023 Splunk, Inc. All rights reserved

# Question: Splunk Web and Forwarders

Which type of forwarders come with Splunk Web?

A. None

B. Linux Universal Forwarders

C. Windows Universal Forwarders

D. Heavy Forwarders


Copyright © 2023 Splunk, Inc. All rights reserved

# Answer: Splunk Web and Forwarders

Which type of forwarders come with Splunk Web?

A. None

B. Linux Universal Forwarders

C. Windows Universal Forwarders

**D. Heavy Forwarders**

A Heavy Forwarder is an instance of Splunk Enterprise, which by default has Splunk Web running. Universal Forwarders do not come with Splunk Web.


Copyright © 2023 Splunk, Inc. All rights reserved

# Question: Forward Server

Running **`splunk add forward-server <indexer:port>`** creates stanzas in which **`.conf`** file?

A. `inputs.conf`

B. `outputs.conf`

C. `indexes.conf`

D. `server.conf`


Copyright © 2023 Splunk, Inc. All rights reserved

# Answer: Forward Server

Running **`splunk add forward-server <indexer:port>`** creates stanzas in which **`.conf`** file?

A. `inputs.conf`

B. **`outputs.conf`**

C. `indexes.conf`

D. `server.conf`

This command creates the stanza **`[tcpout-server://<indexer>:<port>]`** in **`outputs.conf`**. This command is generally run on forwarders to determine where they should send data (normally to indexers or other intermediate forwarders).


Copyright © 2023 Splunk, Inc. All rights reserved

# Module 9 Lab Exercise

**Time:** 20 minutes

**Description:** Configuring Basic Forwarder

**Tasks:**

- Set up your Splunk indexer as the receiver
- Use CLI to configure and prepare your forwarder to send event data to the receiver
- Confirm the forwarder connection with the MC
- View the contents of the **`outputs.conf`** file on the forwarder


Copyright © 2023 Splunk, Inc. All rights reserved

# Module 10:
# Configuring Distributed Search


Copyright © 2023 Splunk, Inc. All rights reserved

# Module Objectives

- Configure distributed search
- Define the roles of the search head and search peers
- Configure Federated Search


Copyright © 2023 Splunk, Inc. All rights reserved

# Distributed Search

## Distributed Search

- Deployment topology that distributes search management and fulfillment activities across multiple Splunk instances
- Provides horizontal scaling
- Managed by search heads:
  - Distributes search requests to “search peers” (indexers)
  - Merges returned results back to the user

Copyright © 2023 Splunk, Inc. All rights reserved

# How Distributed Search Works

1. Universal forwarders (production servers) send data to indexers
2. Indexers (search peers) store their portion of the data
3. Users log on to the search head and run reports
4. The search head dispatches searches to the indexers
5. Indexers run searches in parallel and return their portion of results
6. The search head consolidates the individual results and prepares reports

Copyright © 2023 Splunk, Inc. All rights reserved

# Setting Up Distributed Search

1. Install Splunk on each search head and indexer (search peer)
2. Set up the same indexes on all indexers
3. All search heads and indexers should use a License Manager
4. Add a user to each indexer with a role with **`edit_user`** capability
   - Used only for authenticating a search head to the indexer
5. On the search head, configure indexers by selecting: **Settings > Distributed search**
   - Distributed search is turned on by default, so just add search peers

Copyright © 2023 Splunk, Inc. All rights reserved

# Adding Indexers (Search Peers)

Enter the ***servername:port*** for the indexer

User account with **edit_user** capability


Copyright © 2023 Splunk, Inc. All rights reserved

# Knowledge Bundles and Replication

- Knowledge bundles
  - Distributed to indexers (search peers) by the search head when a distributed search is initiated
  - Contain the knowledge objects required by indexers for searching
  - Found in:

    **`SPLUNK_HOME/var/run`** on the search head

    **`SPLUNK_HOME/var/run/searchpeers`** on the indexer (search peer)
- Replication status of knowledge bundles
  - Splunk Web: **Settings** > **Distributed search** > **Search peers** under the **Replication Status** column


Copyright © 2023 Splunk, Inc. All rights reserved

# Indexer (Search Peer) Failure

- When an indexer goes down:
  1. Forwarders automatically use only available indexers
  2. Offline indexer does not participate in searches
  3. Remaining indexers handle all indexing and searches
  4. Notification is provided
- Notification message sent to user when an indexer goes down during a job:

  **`Search results may be incomplete: the search process on peer indexer_name ended prematurely.`**

- Message shown when an indexer is already down:

Copyright © 2023 Splunk, Inc. All rights reserved

# Viewing Search Peer Status with MC

- Provides a graphical view of the status of indexers (search peers):
  - Median resource usage (Memory, CPU)
  - Top 10 memory-consuming searches
  - Aggregate search runtime

Copyright © 2023 Splunk, Inc. All rights reserved

# Search Peer Quarantine

- Quarantine of an indexer (search peer)
  - Used when an indexer is experiencing performance issues
  - Prevents indexer from participating in future searches
    - Attempts to complete any currently running searches
  - Allows live troubleshooting by not stopping the indexer
  - Only affects the relationship between indexer and search head
- Performed in Splunk Web: **Settings** > **Distributed search** > **Search peers**
- Performed from search head using CLI:

```
splunk edit search-server –auth <user:password> <host:port>
 -action quarantine
```


Copyright © 2023 Splunk, Inc. All rights reserved

# Use Cases for Multiple Search Heads

## Access control

- Control who can access which indexes using what apps
- Dedicate search heads for functional areas: IT Ops, Security, or Business Intelligence (BI)

## Manage geo-dispersed data

- Allow local offices to access their own data while maintaining centralized indexers

## Performance enhancement

- Distribute search loads across multiple servers
- Facilitates horizontal scaling


Copyright © 2023 Splunk, Inc. All rights reserved

# Determining the Number of Search Heads

- Each search head handles ~8 - 12 simultaneous searches
  - Total includes both ad hoc and scheduled searches
  - Exact number depends on types of searches and search head hardware (especially CPU cores)
- Search heads can be added to the distributed group at any time
- Search heads can be:
  - **Dedicated**: Search heads don't share knowledge objects
  - **Clustered**: Share a common set of knowledge objects


Copyright © 2023 Splunk, Inc. All rights reserved

# Dedicated Search Heads

- Each search head
  - Contains its own unique set of reports, dashboards, and so on
  - Dedicated to a team of users with unique knowledge objects
- More than one search head can be configured for the same set of indexers (search peers)

Copyright © 2023 Splunk, Inc. All rights reserved

# Distributed Search Best Practices

Best Practice

- Dedicate a host for each role
  - Combine server roles with caveats
  - Discussed in the *Architecting Splunk Deployments* course
- Disable Splunk Web on instances that don't require it

```
splunk disable webserver
```

- Use Deployment Server
  - Discussed in the *Splunk Enterprise Data Administration* course

Copyright © 2023 Splunk, Inc. All rights reserved

# Distributed Search Best Practices (cont.)

- Forward any data being indexed by the search heads to indexers
  - Centralizes data on indexers, which simplifies management
  - Allows diagnosis from other search heads if one goes down
  - Allows other search heads to access all summary indexes

**outputs.conf**

2

```
[indexAndForward]
index = false

[tcpout]
defaultGroup = default-autolb-group
forwardedindex.filter.disable = true
indexAndForward = false

[tcpout:default-autolb-group]
server=idx1:9997,idx2:9997
```


Copyright © 2023 Splunk, Inc. All rights reserved | 9 May 2023

# Federated Search

## Federated Search

- Conducts searches and joins data from:
  - A local Splunk platform deployment
  - One or more remote “federated providers” (Splunk Enterprise or Cloud environments)
- Supports ad hoc and scheduled searches
- Requires Splunk 8.2 and later
- Replaces Splunk *hybrid search* (an earlier, more limited feature)

Copyright © 2023 Splunk, Inc. All rights reserved

# Configuring Federated Search

On remote search head (RSH) / Federated Provider:

1. Create a service account (Splunk user)
   - Standard mode: User role has read permission for the datasets
   - Transparent mode: User role has **`fsh_manage`** capability

On federated search head (FSH):

2. Configure connection to RSH using hostname and service account
3. Create federated index that maps to index/saved search on the RSH
4. Run search SPL using:

   **`index=federated:<indexname>`**

Copyright © 2023 Splunk, Inc. All rights reserved

# Question: Multiple Search Heads

Which of the following is not a benefit to using multiple search heads?

A. Control who can access search data
B. Allow sites access to their data while maintaining central indexers
C. Improve search performance
D. Improve data ingest performance


Copyright © 2023 Splunk, Inc. All rights reserved

# Answer: Multiple Search Heads

Which of the following is not a benefit to using multiple search heads?

A. Control who can access search data

B. Allow sites access to their data while maintaining central indexers

C. Improve search performance

**D. Improve data ingest performance**

Multiple search heads can provide access control, management of geo-dispersed data, and performance enhancement for search with horizontal scaling. Improve ingest performance by adding additional indexers / search peers and other indexer and forwarder tuning.


Copyright © 2023 Splunk, Inc. All rights reserved

# Question: Setting Up Distributed Search

When setting up distributed search, which of the following steps is incorrect regarding configuring the search heads (SHs) and indexers / search peers?

A. Set up the same indexes on all indexers

B. Configure SHs and indexers to use a License Manager

C. Add a user to indexers with the `edit_user` capability

D. On the indexers configure SHs in **Settings** > **Distributed search**


Copyright © 2023 Splunk, Inc. All rights reserved

# Answer: Setting Up Distributed Search

When setting up distributed search, which of the following steps is incorrect regarding configuring the search heads (SHs) and indexers / search peers?

A. Set up the same indexes on all indexers

B. Configure SHs and indexers to use a License Manager

C. Add a user to indexers with the `edit_user` capability

**D. On the indexers configure SHs in Settings > Distributed search**

On search heads you configured the indexers in Splunk Web under **Settings** > **Distributed search**.


Copyright © 2023 Splunk, Inc. All rights reserved

# Question: Preventing New Searches

How would a Splunk administrator prevent an indexer from participating in new searches while allowing it to service currently running searches?

A. Remove the indexer from the distributed group

B. Quarantine the indexer

C. Stop Splunk on the indexer

D. Stop Splunk on the search head


Copyright © 2023 Splunk, Inc. All rights reserved

# Answer: Preventing New Searches

How would a Splunk administrator prevent an indexer from participating in new searches while allowing it to service currently running searches?

A. Remove the indexer from the distributed group

**B. Quarantine the indexer**

C. Stop Splunk on the indexer

D. Stop Splunk on the search head

Quarantine an indexer in Splunk Web under **Settings** > **Distributed search** > **Search peers** or using **`splunk edit search-server <host:port> -action quarantine`**.


Copyright © 2023 Splunk, Inc. All rights reserved

# Module 10 Lab Exercise

**Time:** 10 minutes

**Description:** Distributed Search

**Tasks:**

- Add a search peer to your search head
- Search for indexes and source types on the search peer


Copyright © 2023 Splunk, Inc. All rights reserved

# Wrap-up Slides


Copyright © 2023 Splunk, Inc. All rights reserved

# Community

- Splunk Community Portal community.splunk.com
  - Answers
  - Discussions
  - Splunk Trust
  - User Groups
  - Ideas
- Splunk Blogs – splunk.com/blog/
- Splunk Apps –splunkbase.com
- Splunk Dev Google Group groups.google.com/forum/#!forum/splunkdev
- Splunk Docs on Twitter – twitter.com/splunkdocs
- Splunk Dev on Twitter – twitter.com/splunkdev
- Splunk Live! – splunklive.splunk.com
- .conf – conf.splunk.com


Copyright © 2023 Splunk, Inc. All rights reserved

# Splunk How-To Channel

- Check out the Splunk Education How-To channel on YouTube:

  splk.it/How-To

- Free, short videos on a variety of Splunk topics

Copyright © 2023 Splunk, Inc. All rights reserved

# Support Programs

- Web
  - Documentation: dev.splunk.com and docs.splunk.com
- Splunk Lantern
  - Guidance from Splunk experts: lantern.splunk.com
- Global Support
  - Support for critical issues, a dedicated resource to manage your account – 24 x 7 x 365
  - Web: splunk.com/index.php/submit_issue
- Enterprise, Cloud, ITSI, Security Support
  - Web: splunk.com/en_us/about-splunk/contact-us.html#tabs/customersupport
  - Phone: (855) SPLUNK-S or (855) 775-8657

Copyright © 2023 Splunk, Inc. All rights reserved

# Splunk Mobile

- Free app available to all Splunk Cloud and Splunk Enterprise customers
- Analyze data and receive actionable alerts on-the-go with mobile-friendly dashboards
- iOS and Android
- See the Product Brief
- Download for iOS splk.it/ios and Android splk.it/android

Copyright © 2023 Splunk, Inc. All rights reserved

# Thank You

splunk>



Copyright © 2023 Splunk, Inc. All rights reserved 

# Appendix A: Security Fundamentals


Copyright © 2023 Splunk, Inc. All rights reserved

# Principles to Minimize Risk – “CIA” Triad

| | |
|---|---|
| **Confidentiality** | Only authorized users can access data |
| **Integrity** | Data is correct, authenticated and reliable / not tampered with |
| **Availability** | Authorized users can access data whenever needed |


Copyright © 2023 Splunk, Inc. All rights reserved

# Layered Security – Defense in Depth

- Firewall Access Controls with dedicated security zones
- Secure pathways for Splunk data transmission
- Security groups locally and in Cloud

- Host-based firewall rules
- Manage host user / system permissions
- Implement other controls in CIS benchmarks

- Splunk-based application controls
- User roles, Splunk certificates, data encryption

- Data ingested into Splunk
- Splunk internal data


Copyright © 2023 Splunk, Inc. All rights reserved

# Security Awareness – Cyber Kill Chain

- Defines steps an enemy uses to attack a target

  www.sans.org/security-awareness-training/blog/applying-security-awareness-cyber-kill-chain

- Should be defended against and intercepted
  - Identify and proactively defend against possible areas of attack or exploits
  - Monitor, identify and respond to attacks quickly at each stage
  - Educate and enforce policies to eliminate human error


Copyright © 2023 Splunk, Inc. All rights reserved

# Basic Security for Splunk Admins

- Change Splunk administrator users passwords routinely
- Run Splunk with the appropriate user account and roles
- Exercise caution when setting permissions for Splunk users
- Bind Splunk 8.x UF management port to localhost only
- Use a host firewall
- Secure Splunk to Splunk communication
- Replace the default certificates


Copyright © 2023 Splunk, Inc. All rights reserved

# Splunk Security 9.0 Improvements

**New Security Features**

3

Splunk Assist
Upgrade Readiness App
Native Smart Card Auth

**No-action Needed Fixes**

65

Secure by default.
Automatically implemented:
**enforcement mode**

**Action-required Advisories***

8

Require proactive steps to work. Mostly in **warning mode**

** For June 2022*


Copyright © 2023 Splunk, Inc. All rights reserved

# Splunk 9.0 Updates – No Action Needed

- Improved dashboard security with sanitization on input fields
- Increased admin control with greater Splunk roles and capabilities with restriction options
- Updates to third party packages
  - Node.js
  - OpenSSL
- Easier risk management with user-friendly SPL safeguards
- Role-based filtering

Copyright © 2023 Splunk, Inc. All rights reserved

# Splunk 9.0 Updates – Action Required

- Configure any action-required procedures:
  docs.splunk.com/Documentation/Splunk/latest/Security/Updates

## Summary of changes

The following table lists a summary of the changes, the Splunk platforms on which the changes ship, the enforcement mode in which they currently operate, and links to procedures on how to configure Splunk software to enforce the changes.

| Change | Description | Introduced in | Addresses | Current mode | Learn more |
|---|---|---|---|---|---|
| TLS certificate host name validation | Splunk platform instances verify the hostname in the TLS certificate they receive when they connect to other Splunk platform instances. | Splunk Cloud Platform (SCP) 8.2.2202, Splunk Enterprise (SE) 9.0 | SVD-2022-0602, SVD-2022-0603 | Warning | Learn more |
| Python module TLS connection hardening | Python modules on Splunk platform instances always validate TLS connections. | SCP 8.2.2202, SE 9.0 | SVD-2022-0601 | Warning | Learn more |
| TLS certificate host name validation using Splunk CLI | The Splunk Command Line Interface (CLI) validates TLS certificates for any connections it makes to other Splunk platform instances. | SCP 8.2.2203, SE 9.0 | SVD-2022-0606 | Warning | Learn more |
| Universal forwarder security | Universal forwarders always validate connections from | SE 9.0 | SVD-2022-0605 | Enforcement | Learn more |


Copyright © 2023 Splunk, Inc. All rights reserved

# Deciding When to Upgrade to Splunk 9.0

**UPGRADE NOW**

- Address time-sensitive security advisories
- Add protection with other embedded security fixes
- Use new security features
- Take advantage of other, non-security related functionality

**WAIT FOR A LATER RELEASE**

- In cases of operational and upgrade planning challenges
- Identify vulnerabilities that impact the environment
- Perform officially documented mitigation steps in the meantime


Copyright © 2023 Splunk, Inc. All rights reserved

# Mitigation When Unable to Upgrade

- Refer to mitigation steps documented on:

  lantern.splunk.com/Splunk_Platform/Product_Tips/Enterprise/Upgrading_Splunk_Enterprise

| Advisory | Info | Partial Mitigation |
|---|---|---|
| SVD-2022-0601 | Splunk Enterprise disabled TLS validation in Python 3 libraries by default | ◦ Review your apps for outbound calls that do not use TLS.<br>◦ Setup infra/reverse-proxy to monitor for outbound service calls.<br>◦ Review network layer controls.<br>◦ Splunk will provide a detection search that lets customers look for TLS clients that do not pass hostname or proper certificate base validation. |
| SVD-2022-0602 | Splunk Enterprise lacked TLS cert validation for Splunk-to-Splunk communication by default | ◦ Ensure Splunk peer communications are configured to use valid certificates. |
| SVD-2022-0603 | Splunk Enterprise lacked TLS hostname validation | ◦ Set infra/reverse proxy to monitor for outbound service calls.<br>◦ Actively review network layer controls (for example, firewall logs) to ensure hosts used in TLS connections are trusted. |
| SVD-2022- | Risky commands warnings in Splunk Enterprise | ◦ Disable unnecessary Splunk Enterprise components and the web.conf |


Copyright © 2023 Splunk, Inc. All rights reserved

# Splunk Security Resources

- Splunk Docs: Product Security page
  www.splunk.com/en_us/product-security.html

Subscribe to receive information on security announcements

- Splunk Docs: Security Update Documentation
  docs.splunk.com/Documentation/Splunk/latest/Security/Updates
- Splunk Lantern: Upgrading Splunk Enterprise
  lantern.splunk.com/Splunk_Platform/Product_Tips/Enterprise/Upgrading_Splunk_Enterprise
- Appendix A: Security Fundamentals


Copyright © 2023 Splunk, Inc. All rights reserved

# Appendix B:
# Splunk Authentication Management


Copyright © 2023 Splunk, Inc. All rights reserved

# Module Objectives

- Overview of integrating Splunk with LDAP
- Overview of integrating Splunk with SAML
- Overview of integrating Splunk with Multifactor Authentication


Copyright © 2023 Splunk, Inc. All rights reserved

# Splunk Authentication Options

- Supported user accounts:
  - Native Splunk accounts
  - LDAP or Active Directory
  - SAML
  - Scripted access to PAM, RADIUS, or other user account systems
- Settings are saved in **`authentication.conf`**

Copyright © 2023 Splunk, Inc. All rights reserved

# Directory Server Integration

- **Best practice:** Integrate Splunk with a directory server
  - Works with multiple LDAP servers, including OpenLDAP and Active Directory
  - Can be configured from Splunk Web or CLI
- User accounts stored in directory server
  - Enforces LDAP user account and password policies
  - Allows users to use same credentials in Splunk as used elsewhere
  - Allows mapping of LDAP groups to Splunk roles

Best Practice


Copyright © 2023 Splunk, Inc. All rights reserved

# LDAP Authentication

LDAP maintains the user credentials - user ID and password, plus other information - centrally and handles all authentication

Copyright © 2023 Splunk, Inc. All rights reserved

# Creating an LDAP Strategy

1. Select **External** authentication method: **LDAP**
2. Click **Configure Splunk to use LDAP**
   - View the list of current LDAP strategies (connections to one or more LDAP nodes on an LDAP server)
   - Multiple LDAP servers can be defined
3. Click **New LDAP** to add a new LDAP strategy
   - Name the strategy and fill out the form

Copyright © 2023 Splunk, Inc. All rights reserved | 9 May 2023

# LDAP Strategy Settings

- Configuration is based on information from LDAP
  - LDAP connection settings
  - User settings
  - Group settings
  - Dynamic group settings
  - Advanced settings

```
host = 10.0.0.150
port = 389
SSLEnabled = 0
bindDN = adsuser@buttercupgames.local
bindDNpassword = <some_hashed_pw>

userBaseDN = OU=splunk,DC=buttercupgames,DC=local
userNameAttribute = samaccountname
realNameAttribute = displayname

groupBaseDN =
  OU=splunk,DC=buttercupgames,DC=local
groupNameAttribute = cn
groupMemberAttribute = member
nestedGroups = 0
groupMappingAttribute = dn

network_timeout = 20
sizelimit = 1000
timelimit = 15
```


Copyright © 2023 Splunk, Inc. All rights reserved

# Mapping LDAP Groups to Roles

## LDAP strategies

New LDAP

Authentication Methods » LDAP strategies

**Successfully saved "AD_splunkers". Successfully performed a bind to the LDAP server.**

Showing 1-1 of 1 item

filter

25 per page

| LDAP strategy name | Host | Port | Connection order | Status | Actions |
|---|---|---|---|---|---|
| AD_splunkers | 10.0.0.150 | 389 | 1 | Enabled \| Disable | Map groups \| Clone \| Delete |

Select to define relationships between LDAP groups and Splunk roles

« Back to strategies

| LDAP Group Name | LDAP Strategy | Group type | Roles |
|---|---|---|---|
| splunkAdmins | AD_splunkers | static | |
| splunkBizDev | AD_splunkers | static | |
| splunkITOps | AD_splunkers | static | |
| splunkSOC | AD_splunkers | static | |

Click an LDAP group name to map it to one or more Splunk roles



Copyright © 2023 Splunk, Inc. All rights reserved | 9 May 2023

# Mapping LDAP Groups to Roles (cont.)

Click one or more role names to map them to to this group

After completing the mapping for all LDAP groups, the mapped roles are shown here

- Not all groups must be mapped
- Mappings can be changed at any time
  - The LDAP server is rechecked each time a user logs into Splunk
  - A user cannot log in unless they have a Splunk role


Copyright © 2023 Splunk, Inc. All rights reserved

# Managing Users in Splunk

- Splunk native users can be edited or deleted
- Only time zone and default app can be changed on LDAP or other users

| Name | Actions | Authentication system | Full name | Email address | Time zone | Default app | Default app inherited from | Roles | Last Login | Status |
|---|---|---|---|---|---|---|---|---|---|---|
| acurry | | LDAP | Amanda | | | search | soc_analyst | soc_analyst | | Active |
| admin | Edit | Splunk | Administrator | 02 | | launcher | system | admin | 9/22/2020, 4:40:45 PM | Active |
| blu | | | | | | launcher | system | user | | Active |
| coryf | | LDAP | Cory Flintoff | | | launcher | system | admin | | Active |
| dhale | | LDAP | Dwight Hale | | | launcher | system | user | | Active |
| emaxwell | Edit | Splunk | | | | search | soc_analyst | soc_analyst | 9/22/2020, 12:16:52 PM | Active |
| gvoronoff | | LDAP | Gabriel Voronoff | | | launcher | system | admin | | Active |


Copyright © 2023 Splunk, Inc. All rights reserved

# SAML 2.0 Single Sign On

Identity provider (IDP) maintains the user credentials and handles authentication

Copyright © 2023 Splunk, Inc. All rights reserved

# Configuring SAML

1 Click **SAML**

2

3 Click **SAML Configuration** to configure the trusted binding and other connection details

4 Click **New Group** to map the new roles

Copyright © 2023 Splunk, Inc. All rights reserved | 9 May 2023

# Configuring SAML – Splunk Settings

- Download the Splunk Service Provider Metadata file
- Import the IdP metadata into Splunk

Copyright © 2023 Splunk, Inc. All rights reserved

# Configuring SAML – General Settings

## Gather SAML configuration information

Protected endpoints on the IdP which Splunk sends authentication requests to

**General Settings**

Single Sign On (SSO) URL ?

Single Log Out (SLO) URL ?

IdP certificate path ?

optional

Leave blank if you store IdP certificates under $SPLUNK_HOME/etc/auth/idpCerts

IdP certificate chains ?

Replicate Certificates ?

Issuer Id ?

Entity ID ?

Sign AuthnRequest



Copyright © 2023 Splunk, Inc. All rights reserved | 9 May 2023

# Configuring SAML – Query and Alias Settings

Endpoint on the IdP to which queries over SOAP are sent

**▼ Attribute Query Requests**

Optional. Used only for vendors that support AQRs, such as IBM, CA, Ping Identity. Confirm with your provider. You must enable either AQRs or authentication extensions for SAML user tokens.

Attribute query URL ?

Sign attribute query request ☑

Sign attribute query response ☑

Username

Password ••••••

**▼ Alias**

Role alias

RealName alias

Mail alias



Copyright © 2023 Splunk, Inc. All rights reserved

# Configuring SAML – Advanced Settings

Leave this empty or pick the correct format configured on the IdP from the drop-down list

Protocol binding used for the SAML sign on/log off requests sent to the IdP

Copyright © 2023 Splunk, Inc. All rights reserved | 9 May 2023

# Creating SAML Groups

- Authorize groups on your SAML server to log into Splunk by mapping them to user roles
- Multiple groups can be mapped to a single user role
- A user must have a Splunk role in order to log in

Copyright © 2023 Splunk, Inc. All rights reserved

# Single Sign On with Reverse Proxy

- Splunk SSO allows you to use a web proxy to handle Splunk authentication
  - Authentication is moved to a web proxy, which passes along authentication to Splunk Web
  - Web proxy can use any method to authenticate (IDP in example)
- docs.splunk.com/Documentation/Splunk/latest/Security/HowSplunkSSOworks

Copyright © 2023 Splunk, Inc. All rights reserved

# Scripted Authentication

- Splunk supports other authentication systems that can be integrated with scripts
- For up-to-date information on scripted authentication
  1. Navigate to **`SPLUNK_HOME/share/splunk/authScriptSamples/`**
  2. Read the **`README`** file
  3. View included sample authentication scripts


Copyright © 2023 Splunk, Inc. All rights reserved

# Duo Multi Factor Authentication

- Splunk supports Duo Security two-factor authentication logins
- LDAP maintains the user credentials including user ID and password, plus other information centrally and handles all authentication

Copyright © 2023 Splunk, Inc. All rights reserved

# Configuring Duo MFA

- Create an account for your Splunk configuration on the Duo website
  - Refer to https://duo.com
- From your search head:
  1. Select Duo Security
  2. Click Configure Duo Security

Copyright © 2023 Splunk, Inc. All rights reserved

# Configuring Duo MFA (cont.)

3. Enter the following info (provided by Duo administrator)
   - Application Secret Key
   - Integration Key
   - Secret Key
   - API Hostname
4. Authentication behavior if Duo is unavailable
5. Connection Timeout (in seconds)
6. Save

Copyright © 2023 Splunk, Inc. All rights reserved | 9 May 2023

# Appendix C:
# Introduction to Splunk Clustering


Copyright © 2023 Splunk, Inc. All rights reserved

# Splunk Clustering

- Requires only Splunk enterprise license
- Discussed in detail in *Splunk Cluster Administration* class
- Supports two types of clusters:

**Search head clustering**

- Replicates knowledge objects across search heads

**Indexer clustering**

- Replicates buckets (data) across indexers
- Can be configured as single-site or multi-site
- Allows balance of growth, speed of recovery, and overall disk usage


Copyright © 2023 Splunk, Inc. All rights reserved

# Splunk Cluster Overview

Additional Components:

- Cluster Manager
- Monitoring Console
- Deployment Server
- Deployer
- License Manager


Copyright © 2023 Splunk, Inc. All rights reserved

# Search Head Cluster

- Accommodates large enterprise use cases
  - Search head high-availability
  - Unified user experience across SHs
  - Search scaling foundation
    - Configuration sharing
    - Artifact replication
    - Job distribution
    - Alert management
    - Load balancing
- Supports external (non-Splunk) load balancers to provide transparent access to the cluster

Copyright © 2023 Splunk, Inc. All rights reserved

# Indexer Clustering and Replication

- Allows for rapid failure recovery
- Replicates buckets amongst the indexers
- Fully configurable, allowing a balance between speed of recovery and overall disk usage
- Requires additional disk space
- Does not require additional license quota
- Allows for Auto Indexer Discovery
  - Forwarders "discover" the available indexers instead of hard-coding **`outputs.conf`**

Copyright © 2023 Splunk, Inc. All rights reserved

# Further Reading: Clustering

- Basic clustering concepts for advanced users

  docs.splunk.com/Documentation/Splunk/latest/Indexer/Basicconcepts

- Configure the search head

  docs.splunk.com/Documentation/Splunk/latest/DistSearch/SHCconfigurationoverview

- Indexer discovery

  docs.splunk.com/Documentation/Splunk/latest/Indexer/indexerdiscovery


Copyright © 2023 Splunk, Inc. All rights reserved

# Appendix D: Adding Data


Copyright © 2023 Splunk, Inc. All rights reserved

# Adding an Input with Splunk Web

- Click the **Add Data** icon
  - On admin's **Home** page
  - On the **Settings** panel
- Or select:
  1. Settings
  2. Data inputs
  3. Add new

Copyright © 2023 Splunk, Inc. All rights reserved

# Select Source

Copyright © 2023 Splunk, Inc. All rights reserved

# Set Source Type: Data Preview

## Set Source Type

data before indexing. If the events look correct and have the right timestamps, click
proper event breaks and timestamps. If you cannot find an appropriate source type for

1 Automatically determined for major data types

View Event Summary

Source type: access_combined_wcookie ▾ | Save As

> Event Breaks
> Timestamp
> Advanced

List ▾ | Format | 20 Per Page ▾ | < Prev | 1 2 3 4 5 6 7 8 ... | Next >

| | Time | Event |
|---|---|---|
| 1 | 7/14/20 5:19:23.000 AM | 211.191.168.25 - - [14/Jul/2020:05:19:23] "POST /oldlink?itemId=EST-27&JSESSIONID=SD3SL3FF2ADFF4954 HTTP 1.1" 200 1391 "http://www.google.com" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 ( .NET CLR 3.5.30729; .NET4.0C)" 677 |
| 2 | 7/14/20 5:19:29.000 AM | 211.191.168.25 - - [14/Jul/2020:05:19:29] "GET /product.screen?productId=WC-SH-A01&JSESSIONID =SD3SL3FF2ADFF4954 HTTP 1.1" 200 1033 "http://www.buttercupgames.com/oldlink?itemId=EST-6" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 ( .NET CLR 3 |
| 3 | 7/14/20 5:19:30.000 AM | 211.191.168.25 - &JSESSIONID =SD3SL3FF2ADFF49 id=EST-16" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 ( .NET CLR 3.5.30729; .NET4.0C)" 862 |
| 4 | 7/14/20 5:19:34.000 AM | 211.191.168.25 - - [14/Jul/2020:05:19:34] "POST /cart.do?action=changequantity&itemId=EST-15&productId=FI-AG-G08&JSESSIONID=SD3SL3FF2ADFF4954 HTTP 1.1" 200 3279 "http://www.buttercupgames.com/category.screen?categoryId=ARCADE" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 ( .NET CLR 3.5.30729; .NET4.0C)" 655 |
| 5 | 7/14/20 5:19:38.000 AM | 211.191.168.25 - - [14/Jul/2020:05:19:38] "GET /product.screen?productId=MB-AG-T01&JSESSIONID =SD3SL3FF2ADFF4954 HTTP 1.1" 200 2316 "http://www.buttercupgames.com/oldlink?itemId=EST-26" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 ( .NET CLR 3.5.30729; .NET4.0C)" 672 |

2 **Data Preview** displays how processed events will be indexed


Copyright © 2023 Splunk, Inc. All rights reserved

# Set Source Type: Data Preview (cont.)

## Set Source Type

This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".

Source: **/opt/log/www1/access.log**

View Event Summary

Source type: access_combined_wcookie ▾ | Save As

List ▾ | Format | 20 Per Page ▾ | < Prev | 1 2 3 4 5 6 7 8 ... | Next >

filter

- Default Settings
  Splunk's default source type settings
- Application
- Database
- Email
- Log to Metrics
- Metrics
- Miscellaneous
- Network & Security
- Operating System
- Structured
- Uncategorized
- Web

- access_combined
  National Center for Supercomputing Applications (NCSA) combined format HTTP web server logs (can be generated by apache or other web servers)
- apache_error
  Error log format produc
  server (typically error_log
- iis
  W3C Extended log format p
  Microsoft Internet Information Services (IIS) web server

3 Optionally choose a different source type

| | Time | Event |
|---|---|---|
| 1 | 7/14/20 5:19:23.000 AM | 211.191.168.25 - - [14/Jul/2020:05:19:23] "POST /oldlink?itemId=EST-27&JSESSIONID=SD3SL3FF2ADFF4954 HTTP 1.1" 200 1391 "http://www.google.com" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 ( .NET CLR 3.5.30729; .NET4.0C)" 677 |
| 2 | 7/14/20 5:19:29.000 AM | 211.191.168.25 - - [14/Jul/2020:05:19:29] "GET /product.screen?productId=WC-SH-A01&JSESSIONID=SD3SL3FF2ADFF4954 HTTP 1.1" 200 1053 "http://www.buttercupgames.com/oldlink?itemId=EST-6" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 ( .NET CLR 3.5.30729; .NET4.0C)" 531 |
| | 0 AM | 211.191.168.25 - - [14/Jul/2020:05:19:30] "GET /product.screen?productId=MB-AG-T01&JSESSIONID=SD3SL3FF2ADFF4954 HTTP 1.1" 200 1434 "http://www.buttercupgames.com/oldlink?itemId=EST-16" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 ( .NET CLR 3.5.30729; .NET4.0C)" 862 |
| | | - [14/Jul/2020:05:19:34] "POST /cart.do?action=changequantity&itemId=EST-15&G08&JSESSIONID=SD3SL3FF2ADFF4954 HTTP 1.1" 200 3279 "http://www.buttercupgamecreen?categoryId=ARCADE" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:20120306 YFF3 Firefox/3.6.28 ( .NET CLR 3.5.30729; .NET4.0C)" 655 |
| | 0 AM | 211.191.168.25 - - [14/Jul/2020:05:19:38] "GET /product.screen?productId=MB-AG-T01&JSESSIONID=SD3SL3FF2ADFF4954 HTTP 1.1" 200 2316 "http://www.buttercupgames.com/oldlink?itemId=EST-26" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 ( .NET CLR 3.5.30729; .NET4.0C)" 672 |


Copyright © 2023 Splunk, Inc. All rights reserved

# Set Source Type (Data Preview - Warning)

## Set Source Type

This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks your data, create a new one by clicking "Save As".

Source: **/opt/log/www1/access.log**

Allows creation of a new source type for a specific source data

View Event Summary

Source type: apache_error

Save As

- Event Breaks
- Timestamp
- Advanced

List | Format | 20 Per Page | < Prev | 1 | 2 | Next >

| | Time | Event |
|---|---|---|
| 1 | 7/14/20 5:57:03.000 AM | 188.173.152.100 - - [14/Jul/2020:05:57:03] "GET /category.screen?categoryId=ACCESSORIES&JSESSIONID=SD2SL6FF10ADFF4967 HTTP 1.1" 200 3994 "http://www.buttercupgames.com" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.52 Safari/536.5" 106<br>188.173.152.100 - - [14/Jul/2020:05:57:10] "GET /oldlink?itemId=EST-15&JSESSIONID=SD2SL6FF10ADFF4967 HTTP 1.1" 200 2992 "http://www.buttercupgames.com/product.screen?productId=DC-SG-G02" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.52 Safari/536.5" 359<br>188.173.152.100 - - [14/Jul/2020:05:57:16] "GET /oldlink?itemId=EST-7&JSESSIONID=SD2SL6FF10ADFF4967 HTTP 1.1" 400 3314 "http://www.buttercupgames.com/oldlink?itemId=EST-7" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.52 Safari/536.5" 316<br>188.173.152.100 - - [14/Jul/2020:05:57:19] "GET /category.screen?categoryId=TEE&JSESSIONID=SD2SL6FF10ADFF4967 HTTP 1.1" 200 2715 "http://www tegoryId=TEE" "Mozilla/5.0 (Windows NT 6.1; WOW64) Chrome/19.0.1084.52 Safari/536.5" 879<br>188.173.152.100 - - [14/Jul/2020:05:57:23] "GET /pr SIONID=SD2SL6FF10ADFF4967 HTTP 1.1" 500 750 "http:/ n?categoryId=NULL" "Mozilla/5.0 (Windows NT 6.1; WO cko) Chrome/19.0.1084.52 Safari/536.5" 157<br>Show all 257 lines |

**Warning**

If events are not separated correctly or have incorrect timestamps, select a different source type from the list or customize the source type settings.



Copyright © 2023 Splunk, Inc. All rights reserved | 9 May 2023

# Input Settings

- Where input configuration is saved
- For **Search & Reporting (search)**: **`SPLUNK_HOME/etc/apps/search/local`**

By default the **default host name** in **General settings** is used

Select index where input will be stored


Copyright © 2023 Splunk, Inc. All rights reserved

# Review

Review the input configuration summary and click **Submit** to finalize

**Note**

Confirm settings before proceeding.

It is easier to use < **Back** and make changes than to rectify later.


Copyright © 2023 Splunk, Inc. All rights reserved

# What Happens Next?

- Indexed events are available for immediate search
  - Splunk may take a minute to start indexing the data
- You are given other options to do more with your data
- Input configuration is saved in:

**SPLUNK_HOME/etc/apps/<*app*>/local/inputs.conf**

```
[monitor:///opt/log/www1/access.log]
index = test
sourcetype = access_combined_wcookie
```

**Note**

Entries in the **`inputs.conf`** file are not created when **Upload** or **Index Once** is selected.


Copyright © 2023 Splunk, Inc. All rights reserved

# Verify your Input

1. Click **Start Searching** or search for **`index=<indexname>`**
2. Verify events and timestamps
3. Confirm the **host**, **source**, and **sourcetype** field values
4. Check the auto-extracted field names

Copyright © 2023 Splunk, Inc. All rights reserved