Real-Time Analysis of Linux System Logs Using Splunk Enterprise

Report submitted
in fulfillment of the requirement for award of the course of

Certified IT Infrastructure and Cyber SOC Analyst

By

AKSHAYA K V

Under the guidance of
Alex Davy
Junior Cybersecurity Instructor

REDTEAM®
HACKER ACADEMY

September, 2024

ABSTRACT

This project focuses on integrating Linux log data into Splunk Enterprise to enhance real-time monitoring and analysis of system logs. As organizations face growing data volumes, effective log management becomes crucial for identifying issues, ensuring compliance, and optimizing performance. The project outlines methodologies for collecting and forwarding Linux logs, configuring Forwarders, and establishing efficient data pipelines. It also covers the development of dashboards and alerts for proactive incident management. By implementing this integrated logging solution, organizations can improve visibility into IT operations, streamline troubleshooting, and strengthen their security posture. This guide provides clear steps and best practices for leveraging Splunk Enterprise for effective Linux log management.

LIST OF FIGURES

TABLE OF CONTENTS

Chapter 1

INTRODUCTION

1.1 Introduction

In today's data-driven landscape, organizations face challenges in managing vast log data from various systems, particularly Linux servers. Logs are essential for troubleshooting, performance monitoring, security compliance, and user behavior analysis. However, manually reviewing these logs can be inefficient, delaying incident responses. This project focuses on integrating Linux log data into Splunk Enterprise, highlighting the processes for collecting, forwarding, and analyzing log information. By leveraging Splunk's capabilities, organizations can enhance system visibility, improve operational efficiency, and support proactive decision-making.

We will cover the configuration of log collection agents on Linux servers, the establishment of data pipelines to Splunk, and the creation of dashboards and alerts for effective log management. This comprehensive approach aims to empower enterprises to utilize their log data effectively, positioning Splunk Enterprise as a key component of their IT strategy..

1.2 Splunk Overview

Splunk Enterprise is a robust analytics platform for real-time log monitoring and management, comprising three core components:

1. **Forwarder:** Collects log data from various sources, such as system and application logs, and sends it to the Indexer. There are

two types: the Universal Forwarder (lightweight) and the Heavy Forwarder (capable of parsing data).

2. **Indexer:** Processes incoming log data by parsing, extracting key fields, and storing it in a searchable format, optimizing search performance and managing data retention.

3. **Search Head:** Provides a user interface for querying, analyzing, and visualizing indexed data. It supports dashboard creation and alert setup, enhancing data insights.

1.3 Linux Logs

Common Linux log files include:

- **/var/log/syslog:** General system logs useful for troubleshooting.
- **/var/log/auth.log:** Records authentication events, aiding security monitoring.
- **/var/log/secure:** Focuses on security-related events for compliance audits.
- **/var/log/kern.log:** Captures kernel messages for diagnosing system issues.

- **Custom application logs:** Specific logs from applications providing insights into performance and errors.

1.4 Benefits of Centralized Log Management

- **Simplified Troubleshooting:** Aggregates logs for easier issue identification and resolution.
- **Enhanced Security Monitoring:** Improves visibility and enables real-time alerts for suspicious activities.
- **Regulatory Compliance:** Facilitates adherence to data retention and reporting standards.
- **Performance Insights:** Analyzes metrics to optimize system performance and capacity planning.
- **Streamlined Incident Response:** Allows for quicker assessment and action during incidents, minimizing downtime.

Chapter 2
OBJECTIVES

2.1 Log Collection Centralization

Collect and centralize Linux system logs (e.g., /var/log/ files) from multiple Linux servers into Splunk Enterprise.

Tasks :

- Install the Splunk Universal Forwarder on each Linux system to forward logs.
- Define the specific log files to be collected (e.g., syslogs, auth logs, application logs).
- Ensure logs are securely transmitted to the Splunk indexer using encryption (e.g., TLS)

2.2 Data Parsing Normalization

Ensure the logs are parsed, normalized, and structured in a readable format for analysis.

Tasks :

- Set up appropriate inputs.conf and props.conf configurations for proper parsing of log formats.
- Use field extractions and data models to structure the data for easy querying.

2.3 Real-Time Monitoring Alerts

Set up real-time monitoring and alerting based on specific Linux system events.

Tasks :

- Create alerts for critical events such as unauthorized login attempts, system errors, or resource overload.
- Implement dashboards to monitor key metrics in real-time (e.g., CPU usage, memory consumption, failed logins).

2.4 Security Compliance

Use Linux log data to monitor security events and ensure compliance with organizational or regulatory standards.

Tasks :

- Set up specific searches for security events (e.g., SSH brute force attempts, sudo privilege escalations).
- Ensure retention policies are in place to comply with data retention regulations.
- Implement role-based access controls (RBAC) in Splunk to restrict access to sensitive log data.

2.5 Performance Optimization

Optimize data ingestion and storage to handle large volumes of Linux logs without impacting performance.

Tasks :

- Implement indexing and retention strategies to manage the volume of logs effectively.
- Ensure the forwarders are configured to throttle the log data if necessary to prevent overloading the network.

2.6 Troubleshooting Auditing

Enable efficient troubleshooting of Linux systems using collected logs.

Tasks :

- Set up dashboards or queries for quick identification of errors, warnings, and audit trails.
- Provide tools for auditing user activity, system changes, and process execution.

2.7 Scalability Future Growth

Design the solution to scale with the organization’s infrastructure as more Linux systems or services are added.

Tasks :

- Ensure scalability by deploying additional forwarders or increasing indexing capacity.
- Plan for the inclusion of logs from containers, cloud services, or other Linux-based environments in the future.

Chapter 3

SYSTEM ARCHITECTURE

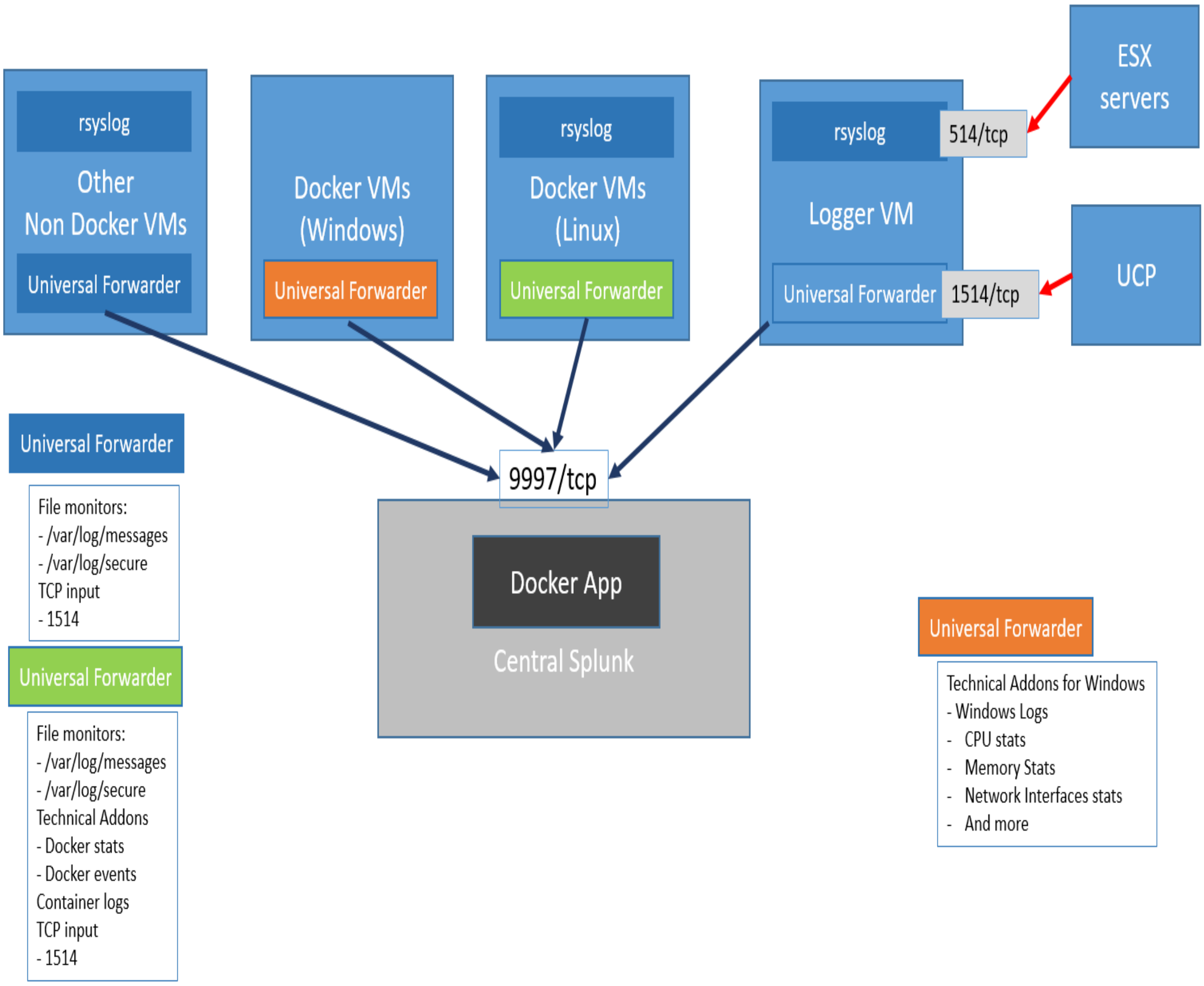


Figure 3.1: Splunk Architecture

Components

- **Central Splunk:** This is the core of the logging infrastructure, responsible for collecting, indexing, and analyzing logs from various sources.
- **Universal Forwarder:** These lightweight agents are deployed on different machines (Docker VMs, other VMs, Logger VM) to collect and forward logs to the Central Splunk instance.
- **Docker App:** Resides within Central Splunk, specifically designed to handle and process logs originating from Docker containers.
- **Other Non-Docker VMs:** Collect system and application logs from these machines.
- **Docker VMs (Windows):** Collect system and application logs, including Docker container logs, from Windows-based Docker hosts.
- **Docker VMs (Linux):** Collect system and application logs, including Docker container logs, from Linux-based Docker hosts.
- **Logger VM:** A dedicated virtual machine likely responsible for collecting logs from network devices or other specialized sources.

- **ESX Servers:** Represent VMware ESXi hypervisors. It's implied they send logs to the Logger VM, likely via syslog (port 514/tcp).
- **UCP:** Likely stands for ”Universal Container Platform,” which could be a container orchestration system like Docker Swarm or Kubernetes. It sends logs to the Logger VM, likely via syslog (port 1514/tcp).

Data Flow

This diagram illustrates a centralized logging architecture using Splunk. Various systems, including Docker VMs (both Windows and Linux), other non-Docker VMs, and ESX servers, send logs to Universal Forwarders. These forwarders collect logs from files (/var/log/messages, /var/log/secure), TCP port 1514, and through specialized Technical Addons for Windows. The Universal Forwarders then transmit these logs to a central Splunk instance (Docker App) via TCP port 9997. Additionally, a Logger VM serves as an intermediary, receiving logs via rsyslog (ports 514 and 1514) and forwarding them to the central Splunk instance, likely after some initial processing or filtering. This setup ensures a centralized point for log aggregation, analysis, and management, simplifying security monitoring and troubleshooting across the infrastructure.

Advantages

- Simplified Log Management
- Single Point of Truth
- Improved Security Monitoring
- Enhanced Troubleshooting
- Scalability
- Real-time Visibility

Disadvantages

- Complexity
- Resource Consumption
- Cost
- Scalability Issues
- Vendor Lock-in

Tools and Technologies

- Splunk Enterprise
- Splunk Universal Forwarder (Linux)
- Linux (Ubuntu, CentOS, or another distribution)
- Linux Log Files (auth.log, syslog, etc.)
- Search Processing Language (SPL)
- Dashboards Alerts
- Reporting Tools in Splunk

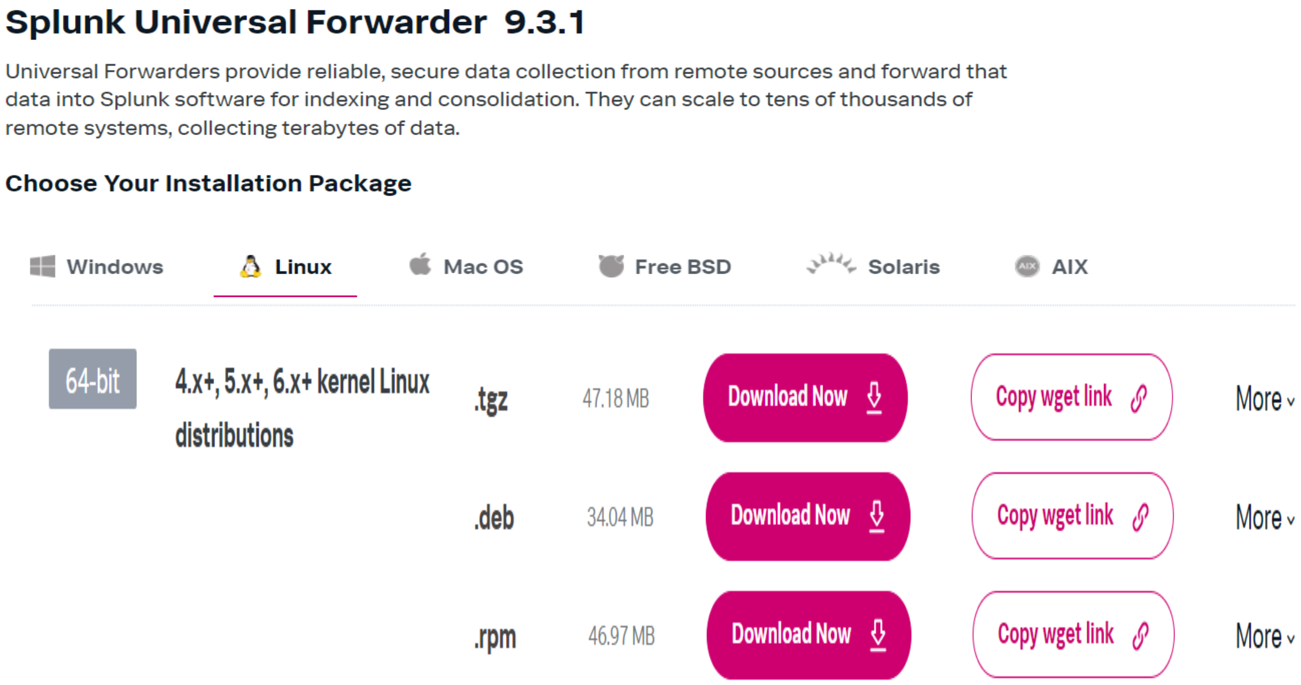
Chapter 4

SETUP AND CONFIGURATION

4.1 Installing Splunk Forwarder on Linux

4.1.1 Download Splunk Universal Forwarder

- Visit the Splunk Download Page.



Splunk Universal Forwarder 9.3.1

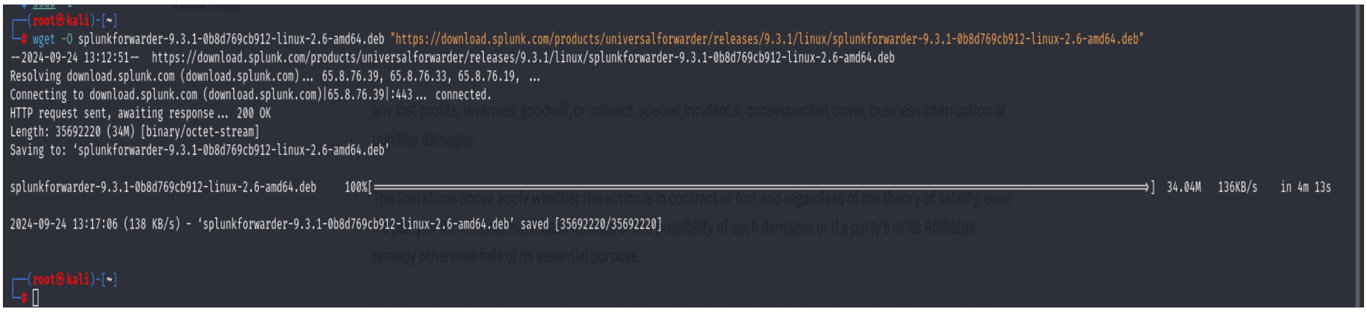
Universal Forwarders provide reliable, secure data collection from remote sources and forward that data into Splunk software for indexing and consolidation. They can scale to tens of thousands of remote systems, collecting terabytes of data.

Choose Your Installation Package

64-bit	4.x+, 5.x+, 6.x+ kernel Linux distributions	.tgz	47.18 MB	Download Now	Copy wget link	More
		.deb	34.04 MB	Download Now	Copy wget link	More
		.rpm	46.97 MB	Download Now	Copy wget link	More

Figure 4.1: Splunkforwarder Installation Package

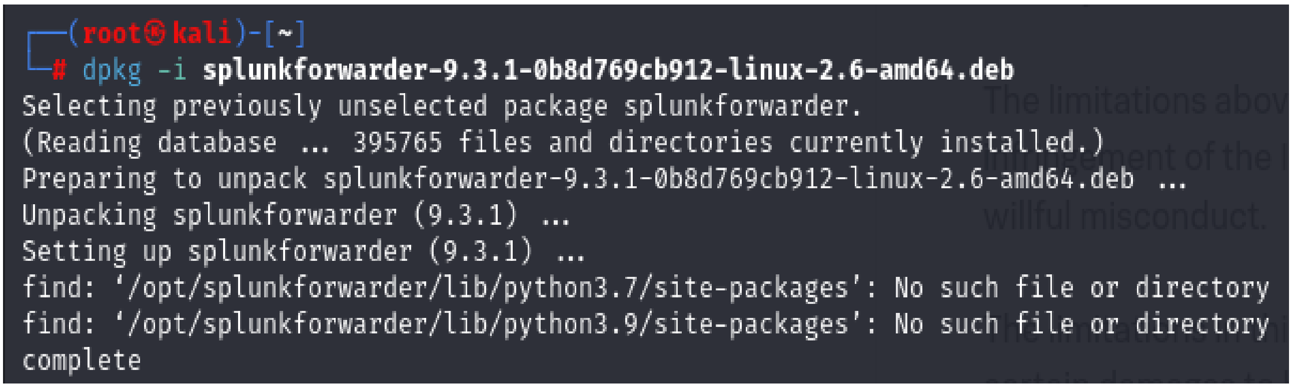
- Choose the package for your Linux distro (.deb).



```
┌──(root㉿kali)-[~]
└─# wget -O splunkforwarder-9.3.1-0b8d769cb912-linux-2.6-amd64.deb "https://download.splunk.com/products/universalforwarder/releases/9.3.1/linux/splunkforwarder-9.3.1-0b8d769cb912-linux-2.6-amd64.deb"
--2024-09-24 13:12:51--  https://download.splunk.com/products/universalforwarder/releases/9.3.1/linux/splunkforwarder-9.3.1-0b8d769cb912-linux-2.6-amd64.deb
Resolving download.splunk.com (download.splunk.com)... 65.8.76.39, 65.8.76.33, 65.8.76.19, ...
Connecting to download.splunk.com (download.splunk.com)|65.8.76.39|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 35692220 (34M) [binary/octet-stream]
Saving to: ‘splunkforwarder-9.3.1-0b8d769cb912-linux-2.6-amd64.deb’

splunkforwarder-9.3.1-0b8d769cb912-linux-2.6-amd64.deb     100%[==============================================>]  34.04M   136KB/s    in 4m 13s

2024-09-24 13:17:06 (138 KB/s) - ‘splunkforwarder-9.3.1-0b8d769cb912-linux-2.6-amd64.deb’ saved [35692220/35692220]


┌──(root㉿kali)-[~]
└─# ▯
```

Figure 4.2: Splunk Forwarder Downloded

- Install for Ubuntu/Debian: **sudo dpkg -i splunkforwarder-¡version¿-Linux-x86**$_6$4.*deb*

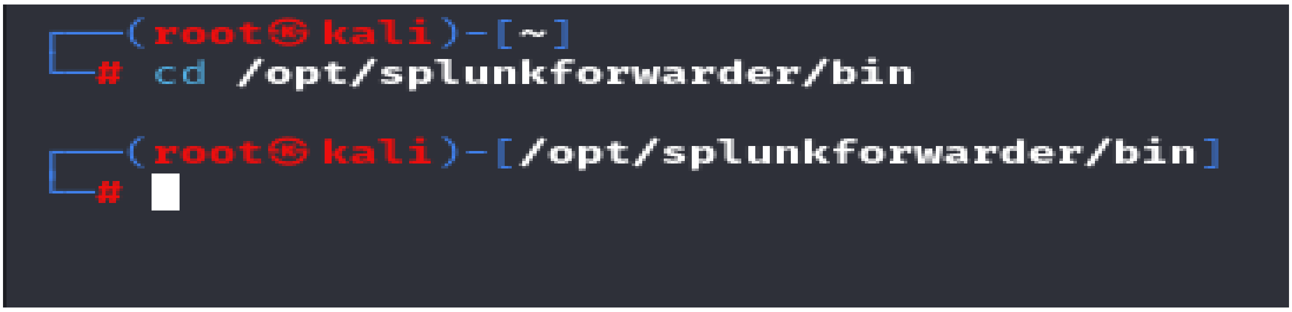


```
┌──(root㉿kali)-[~]
└─# dpkg -i splunkforwarder-9.3.1-0b8d769cb912-linux-2.6-amd64.deb
Selecting previously unselected package splunkforwarder.
(Reading database ... 395765 files and directories currently installed.)
Preparing to unpack splunkforwarder-9.3.1-0b8d769cb912-linux-2.6-amd64.deb ...
Unpacking splunkforwarder (9.3.1) ...
Setting up splunkforwarder (9.3.1) ...
find: ‘/opt/splunkforwarder/lib/python3.7/site-packages’: No such file or directory
find: ‘/opt/splunkforwarder/lib/python3.9/site-packages’: No such file or directory
complete
```

Figure 4.3: Splunk Forwarder Installed

4.1.2 Change Directory

- Change the Directory to : **cd /opt/splunkforwarder/bin**



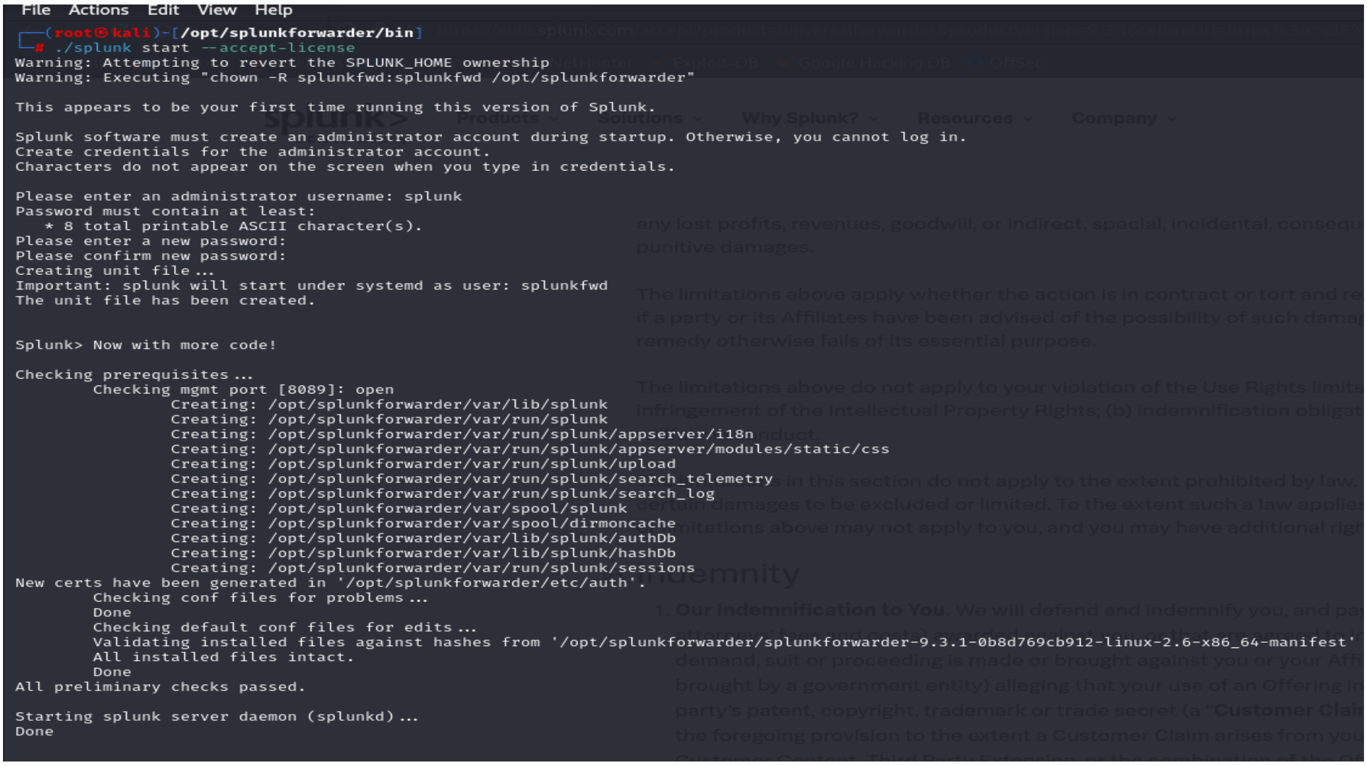
```
┌──(root㉿kali)-[~]
└─# cd /opt/splunkforwarder/bin

┌──(root㉿kali)-[/opt/splunkforwarder/bin]
└─# █
```

Figure 4.4: Directory Changed

4.1.3 Start Splunk Forwarder

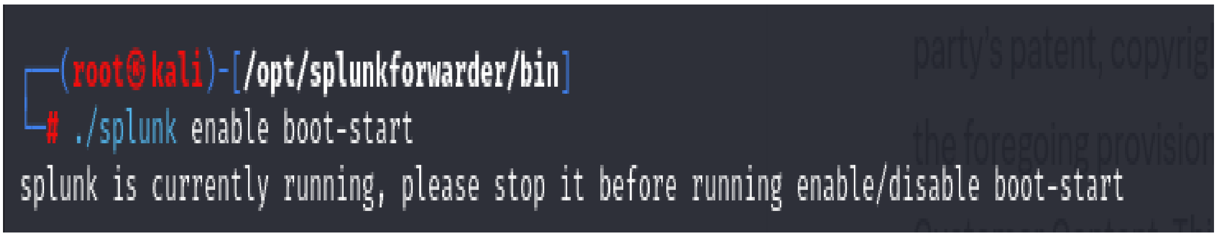
- After installation, start the forwarder : **./splunk start –accept-license**.

- Enable it to start on boot : **./splunk enable boot-start**



```
┌──(root㉿kali)-[/opt/splunkforwarder/bin]
└─# ./splunk start --accept-license
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"

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: splunk
Password must contain at least:
   * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
Creating unit file...
Important: splunk will start under systemd as user: splunkfwd
The unit file has been created.


Splunk> Now with more code!

Checking prerequisites...
        Checking mgmt port [8089]: open
                Creating: /opt/splunkforwarder/var/lib/splunk
                Creating: /opt/splunkforwarder/var/run/splunk
                Creating: /opt/splunkforwarder/var/run/splunk/appserver/i18n
                Creating: /opt/splunkforwarder/var/run/splunk/appserver/modules/static/css
                Creating: /opt/splunkforwarder/var/run/splunk/upload
                Creating: /opt/splunkforwarder/var/run/splunk/search_telemetry
                Creating: /opt/splunkforwarder/var/run/splunk/search_log
                Creating: /opt/splunkforwarder/var/spool/splunk
                Creating: /opt/splunkforwarder/var/spool/dirmoncache
                Creating: /opt/splunkforwarder/var/lib/splunk/authDb
                Creating: /opt/splunkforwarder/var/lib/splunk/hashDb
                Creating: /opt/splunkforwarder/var/run/splunk/sessions
New certs have been generated in '/opt/splunkforwarder/etc/auth'.
        Checking conf files for problems...
        Done
        Checking default conf files for edits...
        Validating installed files against hashes from '/opt/splunkforwarder/splunkforwarder-9.3.1-0b8d769cb912-linux-2.6-x86_64-manifest'
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Done
```

Figure 4.5: Splunk Forwarder starts



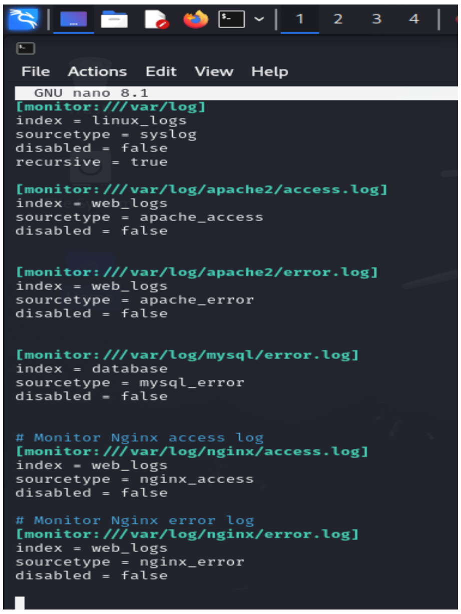
```
┌──(root㉿kali)-[/opt/splunkforwarder/bin]
└─# ./splunk enable boot-start
splunk is currently running, please stop it before running enable/disable boot-start
```

Figure 4.6: Splunk Forwarder boot-start

4.1.4 Configure Inputs

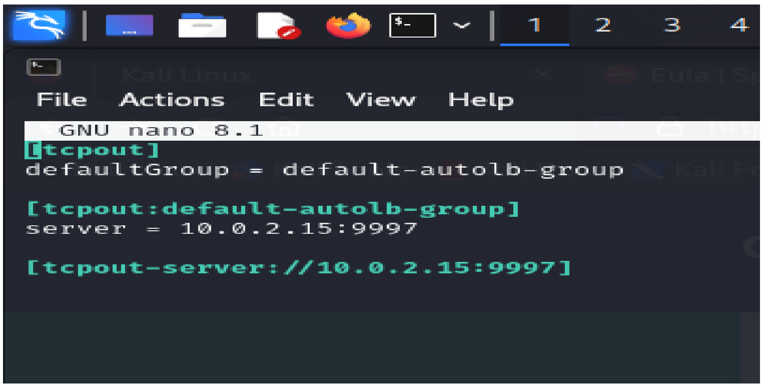
- Navigate to the Splunk Forwarder Directory: The inputs.conf file for the Universal Forwarder is located in the local directory under the system settings.

- Navigate to the appropriate directory
- Create or Edit the inputs.conf File
  - If inputs.conf doesn't exist in the /local/ directory, you can create a new one: **sudo nano inputs.conf**
  - If outputs.conf doesn't exist in the /local/ directory, you can create a new one: **sudo nano outputs.conf**
  - If the file already exists, open it with a text editor like nano or vi to modify it.
- Define Logs to Collect: You can configure Splunk to monitor specific files or directories by adding entries.



```
[monitor:///var/log]
index = linux_logs
sourcetype = syslog
disabled = false
recursive = true

[monitor:///var/log/apache2/access.log]
index = web_logs
sourcetype = apache_access
disabled = false


[monitor:///var/log/apache2/error.log]
index = web_logs
sourcetype = apache_error
disabled = false


[monitor:///var/log/mysql/error.log]
index = database
sourcetype = mysql_error
disabled = false


# Monitor Nginx access log
[monitor:///var/log/nginx/access.log]
index = web_logs
sourcetype = nginx_access
disabled = false

# Monitor Nginx error log
[monitor:///var/log/nginx/error.log]
index = web_logs
sourcetype = nginx_error
disabled = false
```

Figure 4.7: inputs.conf file

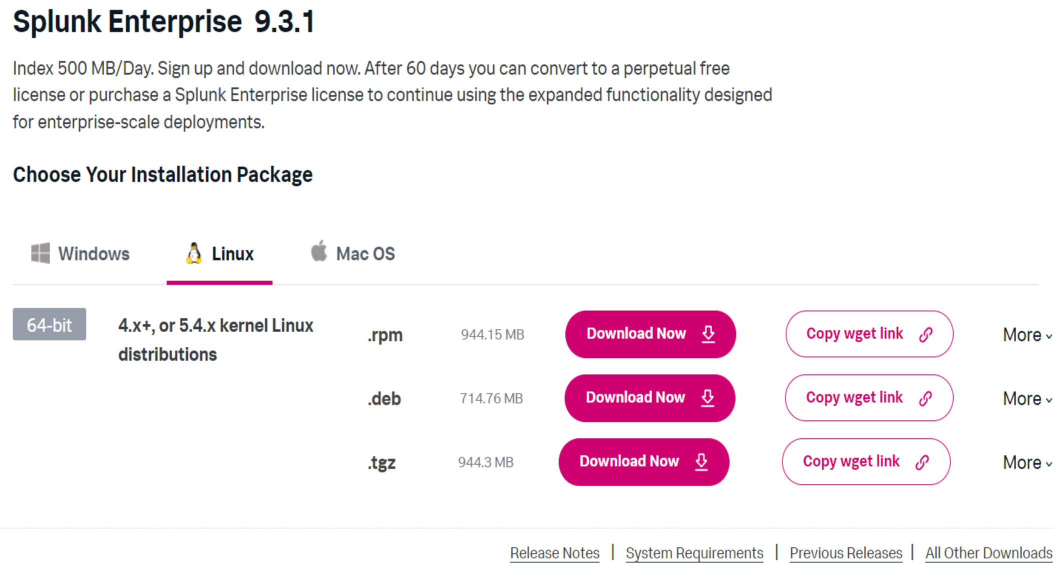


```
  GNU nano 8.1
[tcpout]
defaultGroup = default-autolb-group

[tcpout:default-autolb-group]
server = 10.0.2.15:9997

[tcpout-server://10.0.2.15:9997]
```

Figure 4.8: inputs.conf file

4.1.5 Download Splunk Enterprise On Windows

- Visit the Splunk Download Page.
- Download the Windows installer (.msi).



Splunk Enterprise 9.3.1

Index 500 MB/Day. Sign up and download now. After 60 days you can convert to a perpetual free license or purchase a Splunk Enterprise license to continue using the expanded functionality designed for enterprise-scale deployments.

Choose Your Installation Package

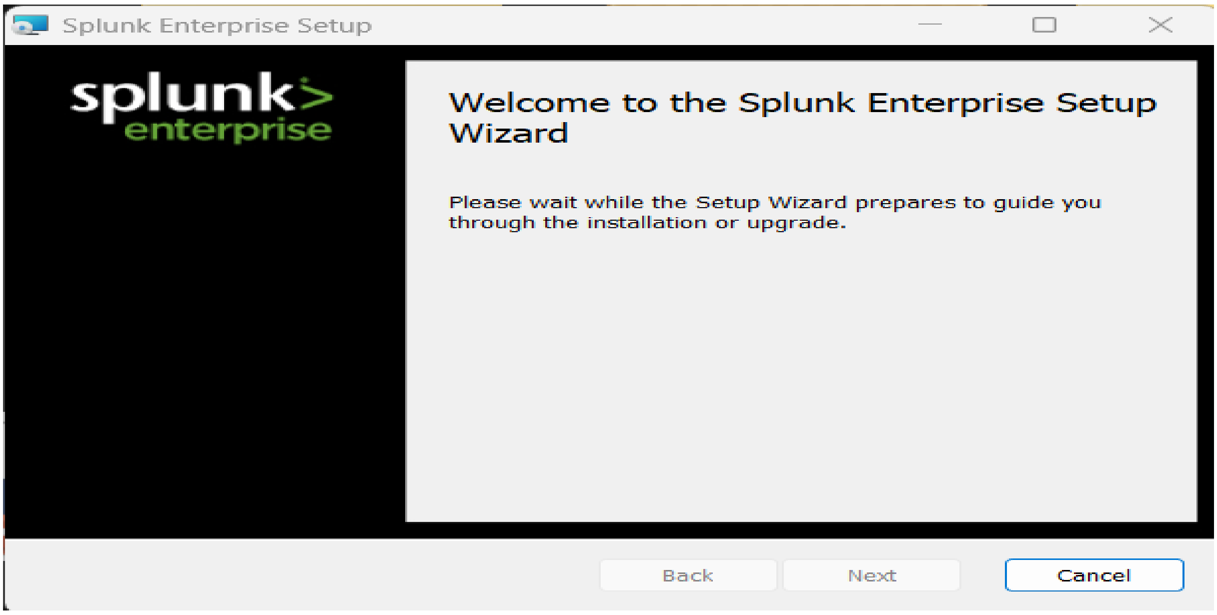
64-bit	4.x+, or 5.4.x kernel Linux distributions	.rpm	944.15 MB	Download Now	Copy wget link	More
		.deb	714.76 MB	Download Now	Copy wget link	More
		.tgz	944.3 MB	Download Now	Copy wget link	More

Release Notes | System Requirements | Previous Releases | All Other Downloads

Figure 4.9: Installation Package

4.2 Install Splunk Enterprise

- Run the installer by double-clicking the .msi file.



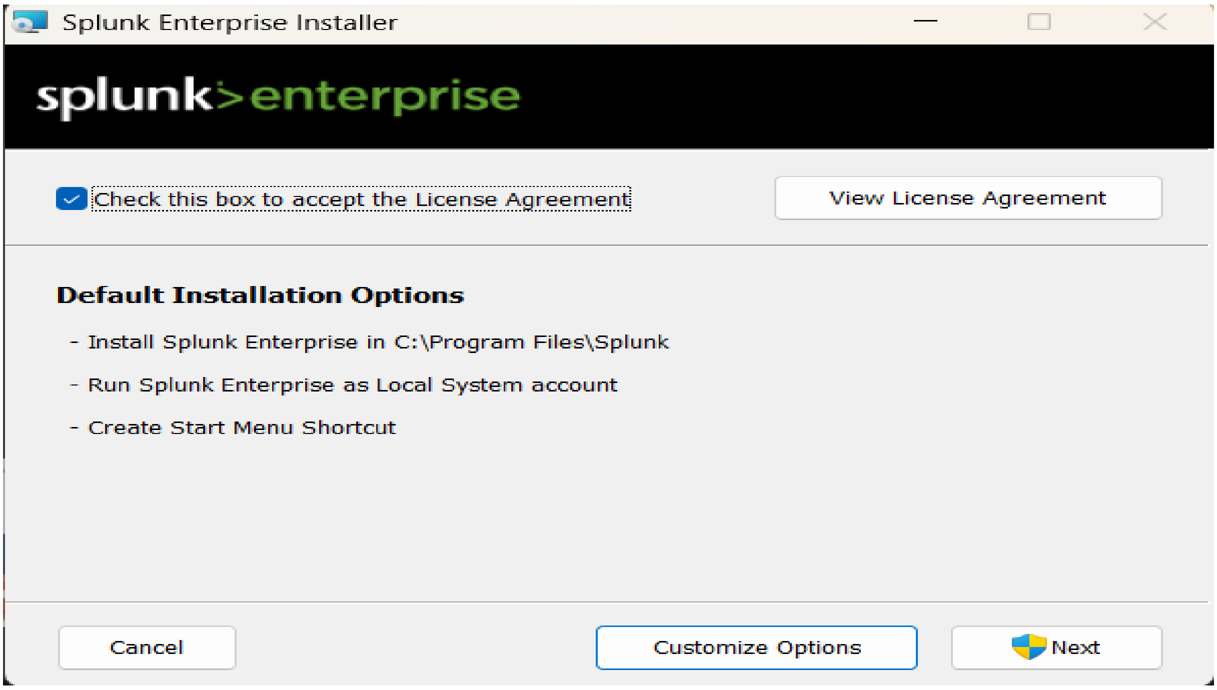
Splunk Enterprise Setup

Welcome to the Splunk Enterprise Setup Wizard

Please wait while the Setup Wizard prepares to guide you through the installation or upgrade.

Figure 4.10: Setup Wizard

- Follow the installation wizard, accept the license agreements and click **Customize Options**



Splunk Enterprise Installer

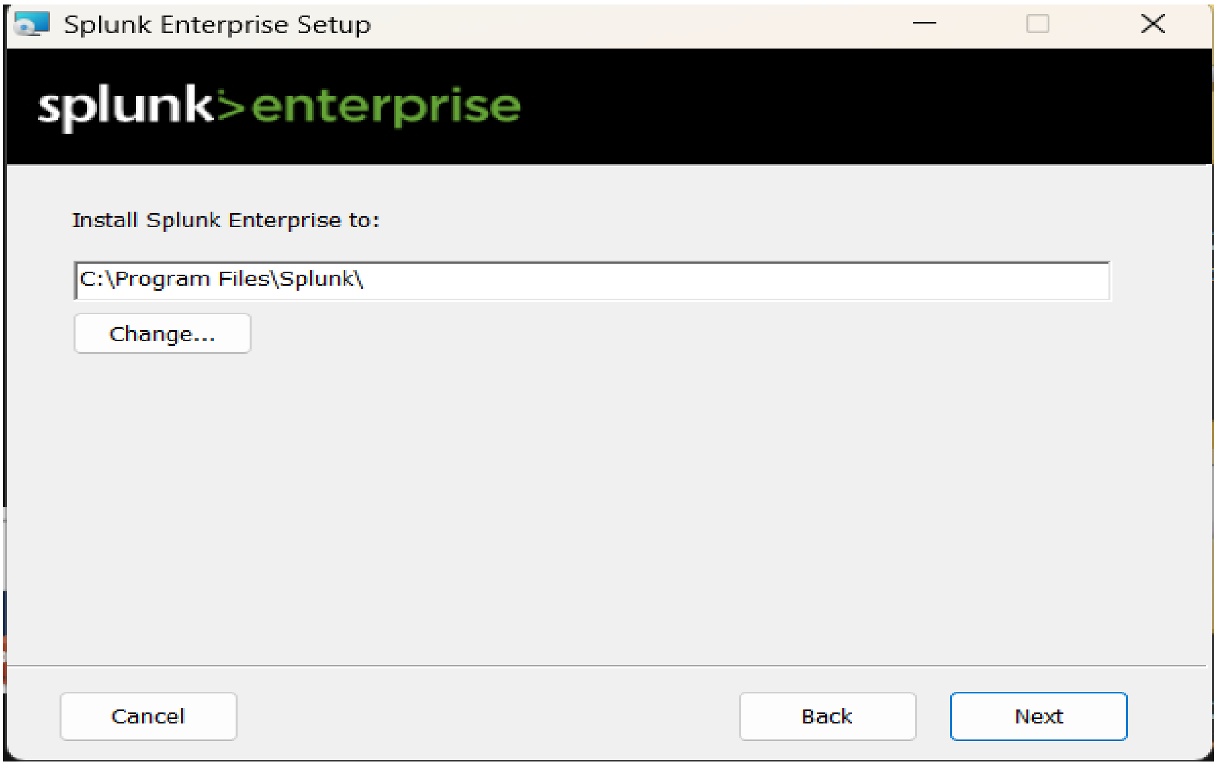
☑ Check this box to accept the License Agreement

Default Installation Options

- Install Splunk Enterprise in C:\Program Files\Splunk
- Run Splunk Enterprise as Local System account
- Create Start Menu Shortcut

Figure 4.11: Splunk Enterprise Installation

- Choose the installation directory (default: C:Files)

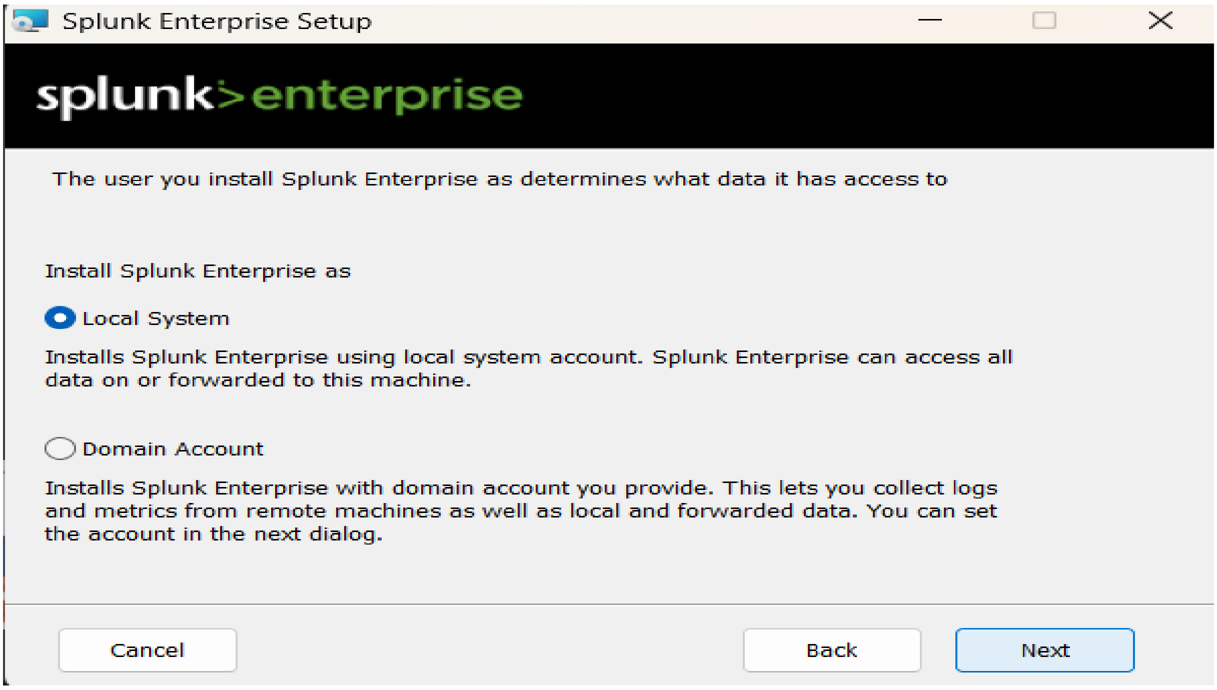

Splunk Enterprise Setup

Install Splunk Enterprise to:

C:\Program Files\Splunk\

Figure 4.12: Install Splunk Enterprise to C Drive

- Install Splunk Enterprise as **Local System**


Splunk Enterprise Setup

The user you install Splunk Enterprise as determines what data it has access to

Install Splunk Enterprise as

● Local System

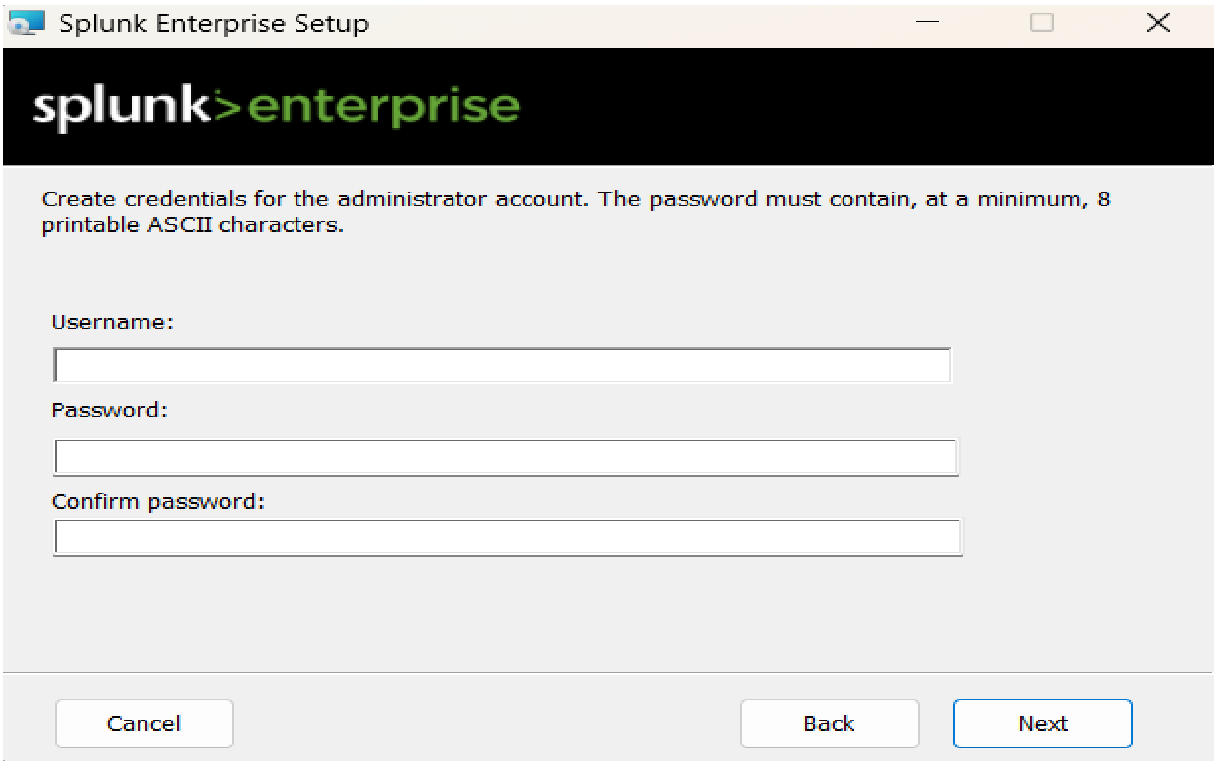
Installs Splunk Enterprise using local system account. Splunk Enterprise can access all data on or forwarded to this machine.

○ Domain Account

Installs Splunk Enterprise with domain account you provide. This lets you collect logs and metrics from remote machines as well as local and forwarded data. You can set the account in the next dialog.

Figure 4.13: Data Access

- Create Credentials for the Administrator Account



Splunk Enterprise Setup

Create credentials for the administrator account. The password must contain, at a minimum, 8 printable ASCII characters.

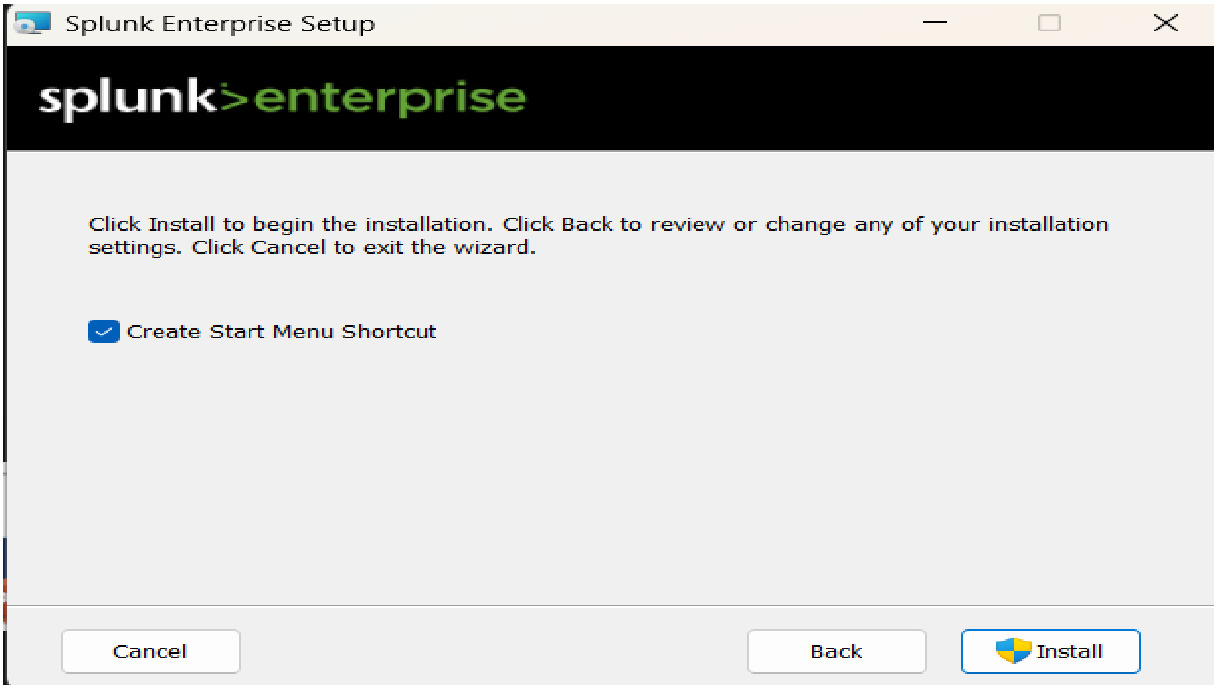
Username:

Password:

Confirm password:

Figure 4.14: Credential Creation

- Click **Install** to begin Installation



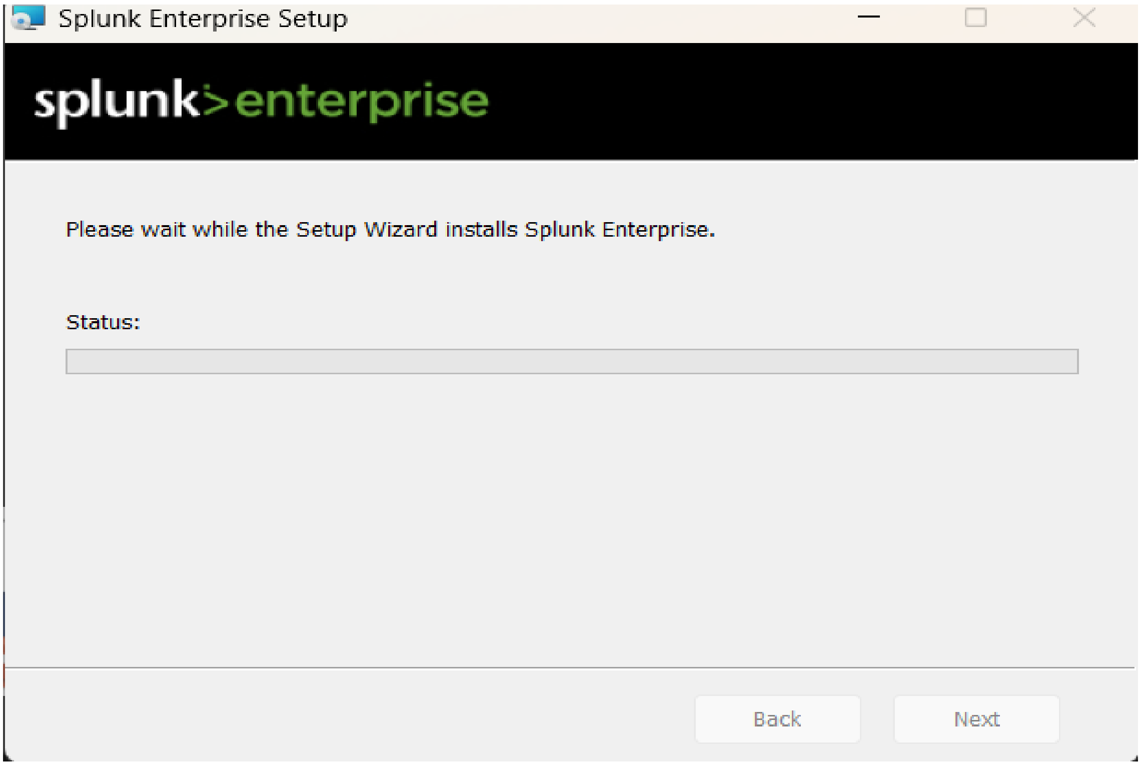
Splunk Enterprise Setup

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

☑ Create Start Menu Shortcut

Figure 4.15: Intallation Begin

- Wait for Setup Wizard Installs Splunk Enterprise

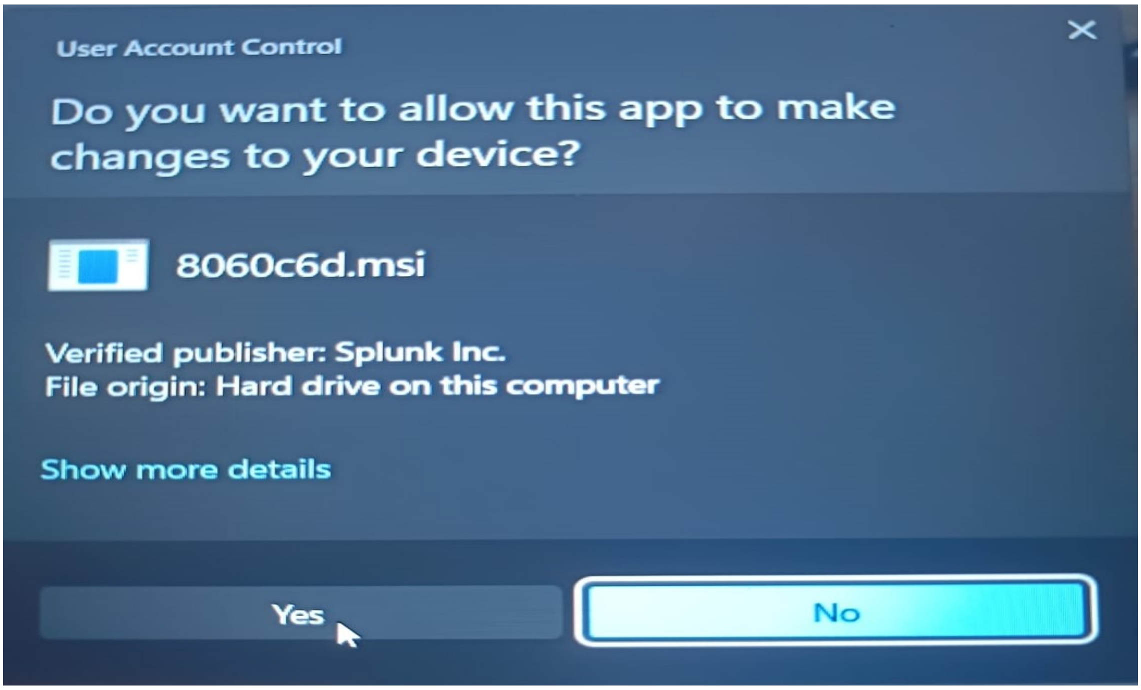


Please wait while the Setup Wizard installs Splunk Enterprise.

Status:

Figure 4.16: Waiting For Installation

- Waiting For Installation a pop up will appear click **Yes** to continue



User Account Control

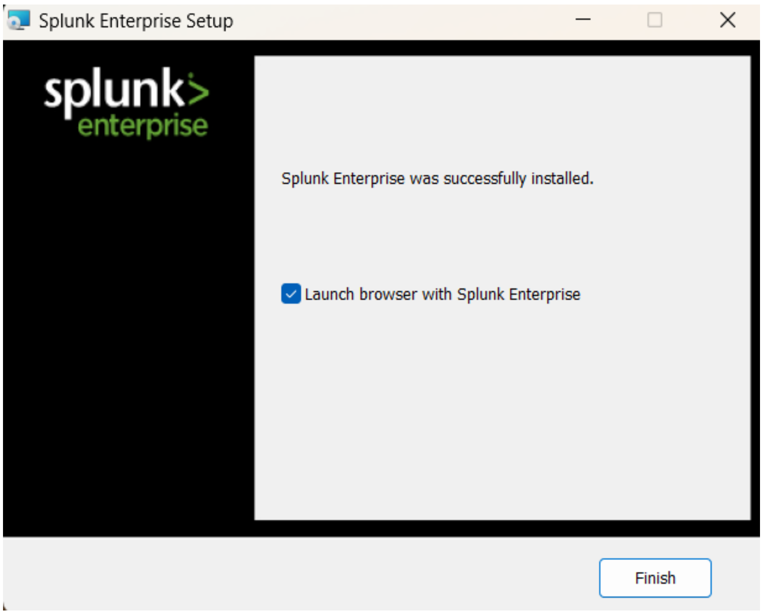
Do you want to allow this app to make changes to your device?

8060c6d.msi

Verified publisher: Splunk Inc.
File origin: Hard drive on this computer

Figure 4.17: Pop up

- Splunk Enterprise Was successfully installed. Click **Finish** to continue



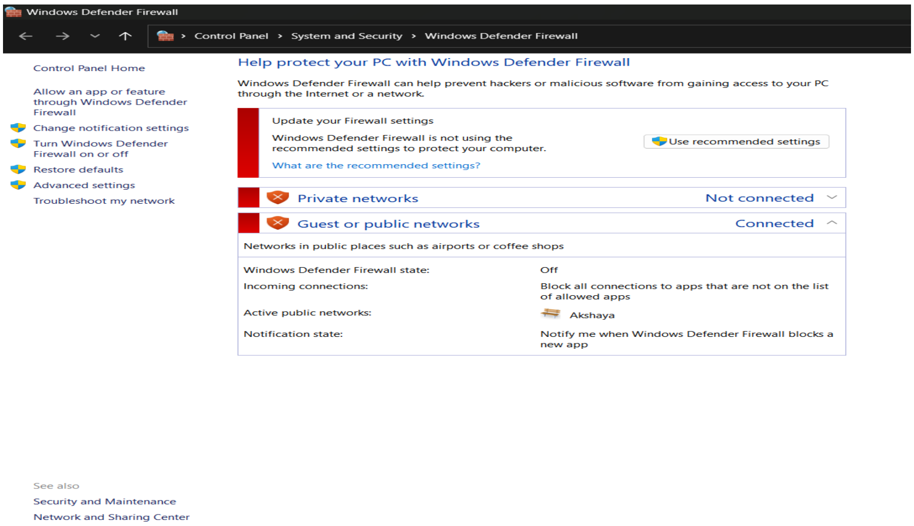
Splunk Enterprise was successfully installed.

☑ Launch browser with Splunk Enterprise

Figure 4.18: Splunk Enterprise Installation Successfully

4.3 Firewall Configuration

- Open Windows Defender Firewall : **Control panel - System and Security -Windows Defender Firewall**


Windows Defender Firewall
Control Panel > System and Security > Windows Defender Firewall
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
Use recommended settings
See also
Security and Maintenance
Network and Sharing Center

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Update your Firewall settings

Windows Defender Firewall is not using the recommended settings to protect your computer.

What are the recommended settings?

Private networks — Not connected

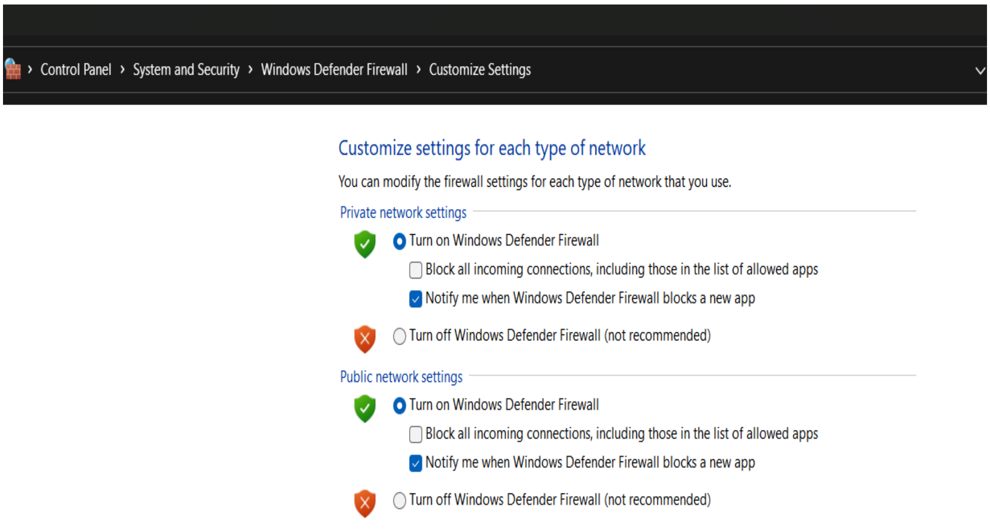
Guest or public networks — Connected

Networks in public places such as airports or coffee shops

Windows Defender Firewall state:	Off
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active public networks:	Akshaya
Notification state:	Notify me when Windows Defender Firewall blocks a new app

Figure 4.19: Windows Defende Firewall With Advanced Security Page

- Turn on Windows Defender Firewall in Private and Public Network **Control Panel - System and Security - Windows Defender Firewall - Customize Setting**


Control Panel › System and Security › Windows Defender Firewall › Customize Settings

Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Private network settings

● Turn on Windows Defender Firewall

□ Block all incoming connections, including those in the list of allowed apps

☑ Notify me when Windows Defender Firewall blocks a new app

○ Turn off Windows Defender Firewall (not recommended)

Public network settings

● Turn on Windows Defender Firewall

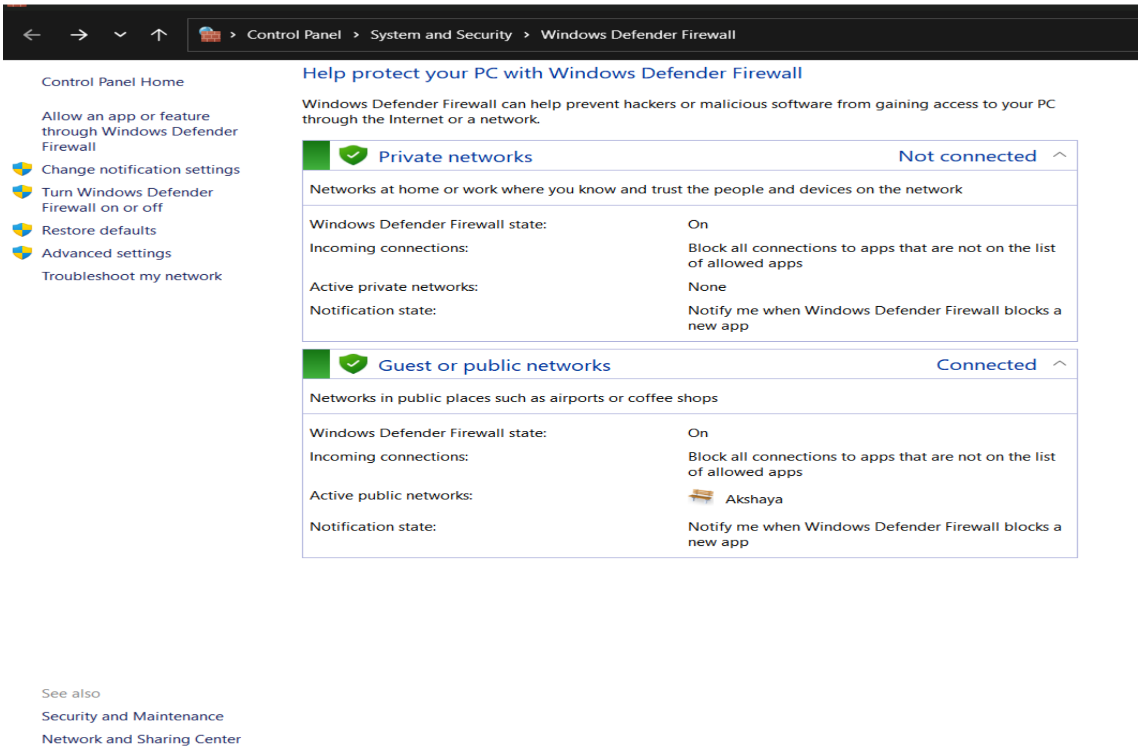
□ Block all incoming connections, including those in the list of allowed apps

☑ Notify me when Windows Defender Firewall blocks a new app

○ Turn off Windows Defender Firewall (not recommended)

Figure 4.20: Customize Setting Page

- Windows Defender Firewall Public and Private Enabled


Control Panel › System and Security › Windows Defender Firewall
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Security and Maintenance
Network and Sharing Center

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Private networks — Not connected

Networks at home or work where you know and trust the people and devices on the network

Windows Defender Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active private networks:	None
Notification state:	Notify me when Windows Defender Firewall blocks a new app

Guest or public networks — Connected

Networks in public places such as airports or coffee shops

Windows Defender Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active public networks:	Akshaya
Notification state:	Notify me when Windows Defender Firewall blocks a new app

Figure 4.21: Windows Defende Firewall With Advanced Security Page

- Click **Inbound Rules** to set rule

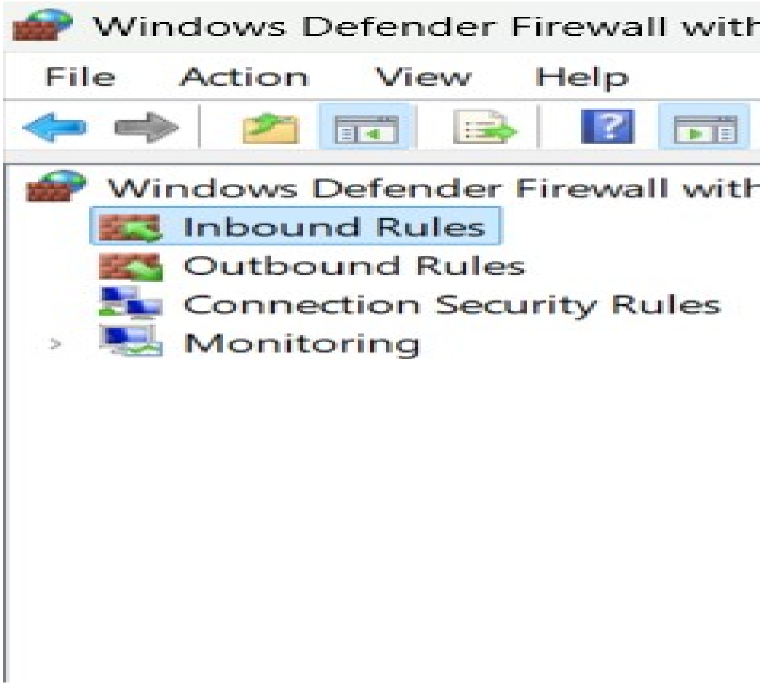

Windows Defender Firewall with
File
Action
View
Help
Windows Defender Firewall with
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring

Figure 4.22: Inbound Rule

- Click **New Rule** to set rule

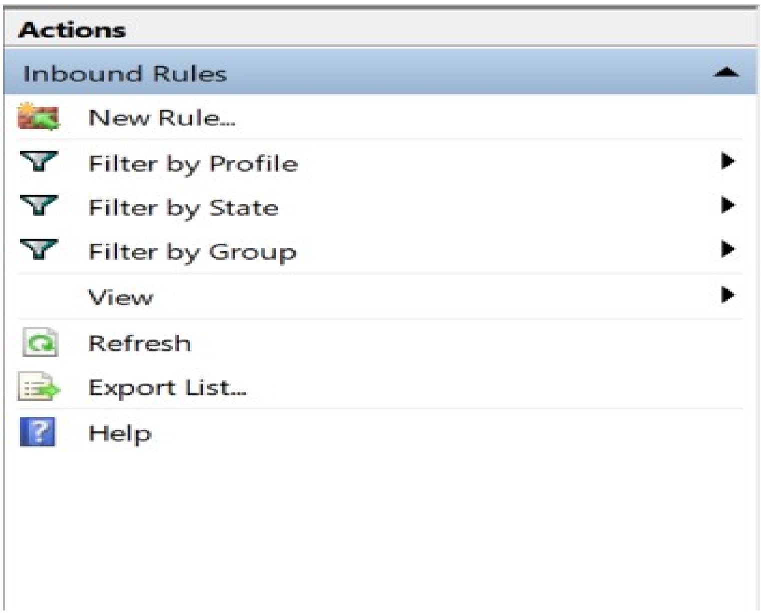
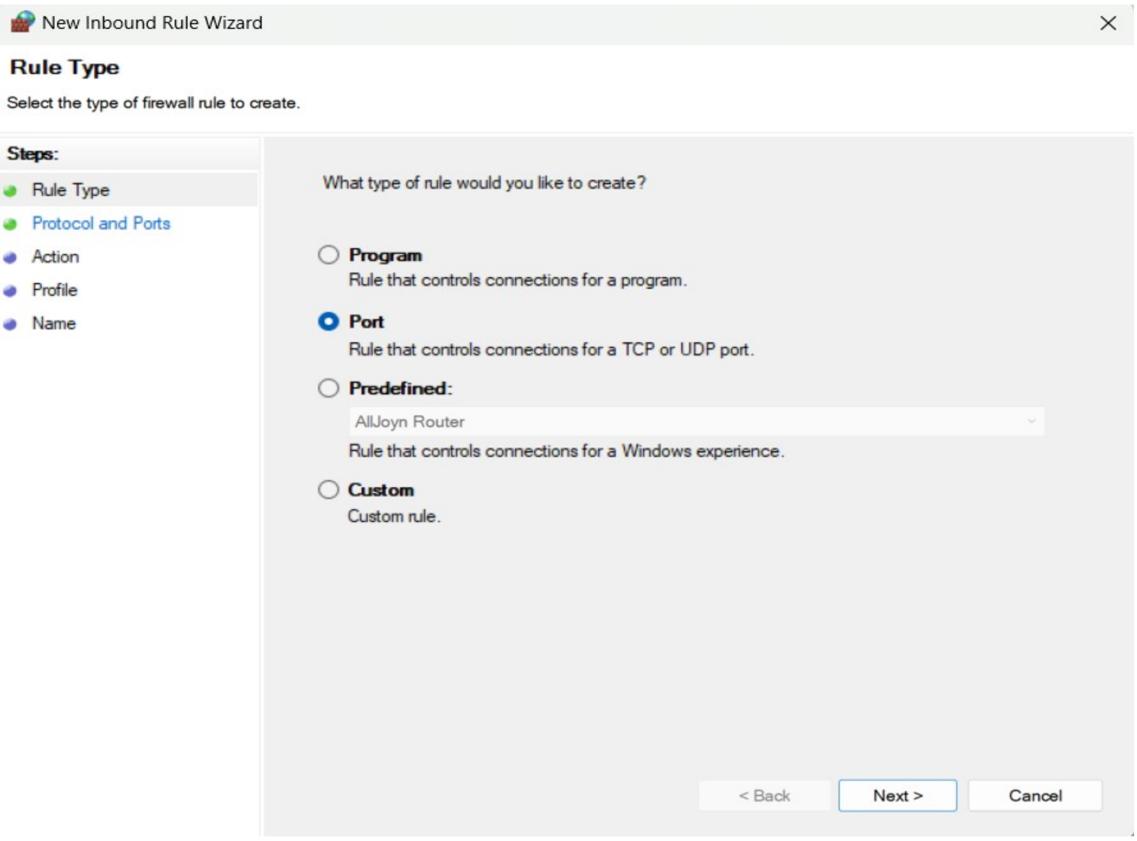


Figure 4.23: New Rule

- Select the type of Firewall Rule to create : **Port**



New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

What type of rule would you like to create?

○ **Program**
Rule that controls connections for a program.

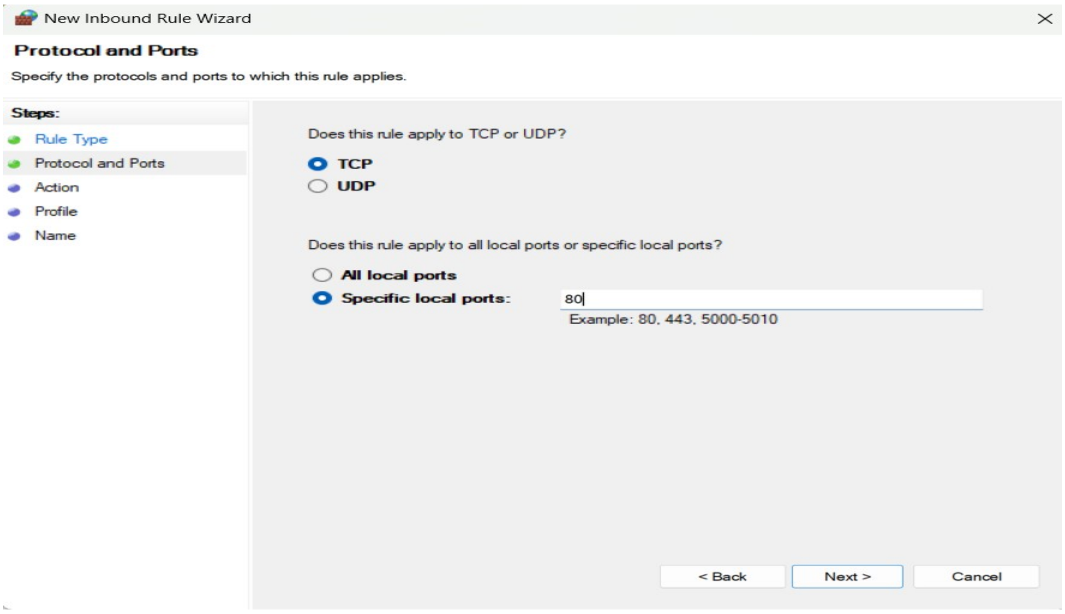
● **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
AllJoyn Router
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

Figure 4.24: Rule Creation

- Specify the protocols and port to rule applies. Select **TCP and Specfic local ports : 80**



New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Does this rule apply to TCP or UDP?

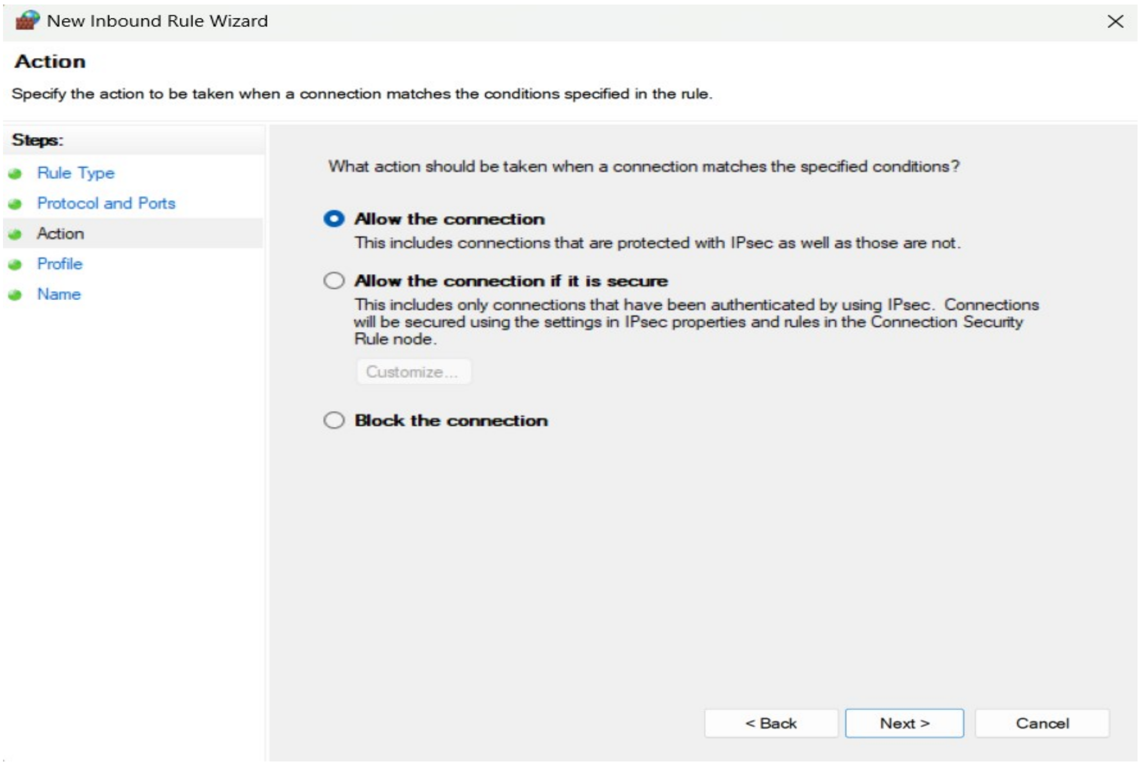
● **TCP**
○ **UDP**

Does this rule apply to all local ports or specific local ports?

○ **All local ports**
● **Specific local ports:** 80
Example: 80, 443, 5000-5010

Figure 4.25: Rule Creation

- Specify the action to be taken when a connection matches the condition specified in the rule : **Allow the connection**



New Inbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What action should be taken when a connection matches the specified conditions?

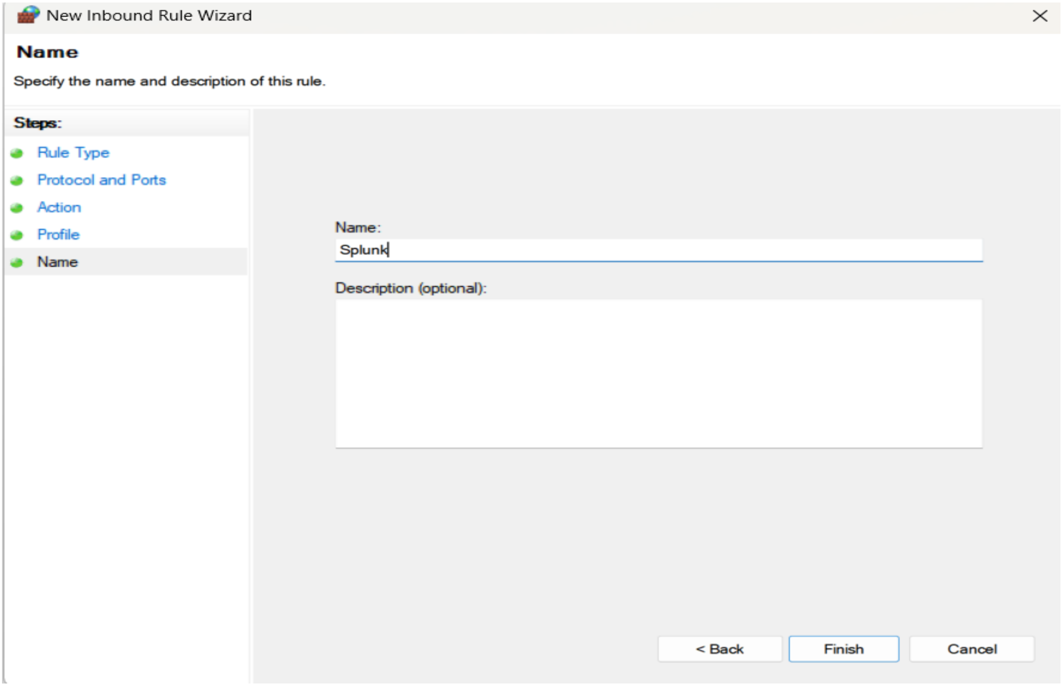
● **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

○ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

○ **Block the connection**

Figure 4.26: Connection

- Specify the Name for the rule.



New Inbound Rule Wizard

Name

Specify the name and description of this rule.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Name:
Splunk

Description (optional):

Figure 4.27: Name the Rule

- Inbound Rule Created Successfully

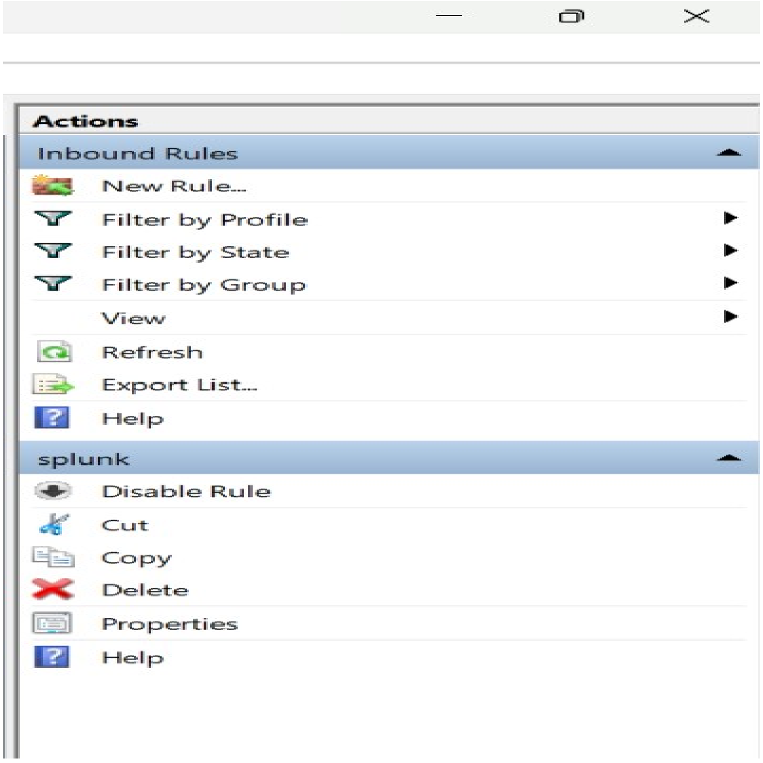


Figure 4.28: Rule Created

- Setup Outbound Rules

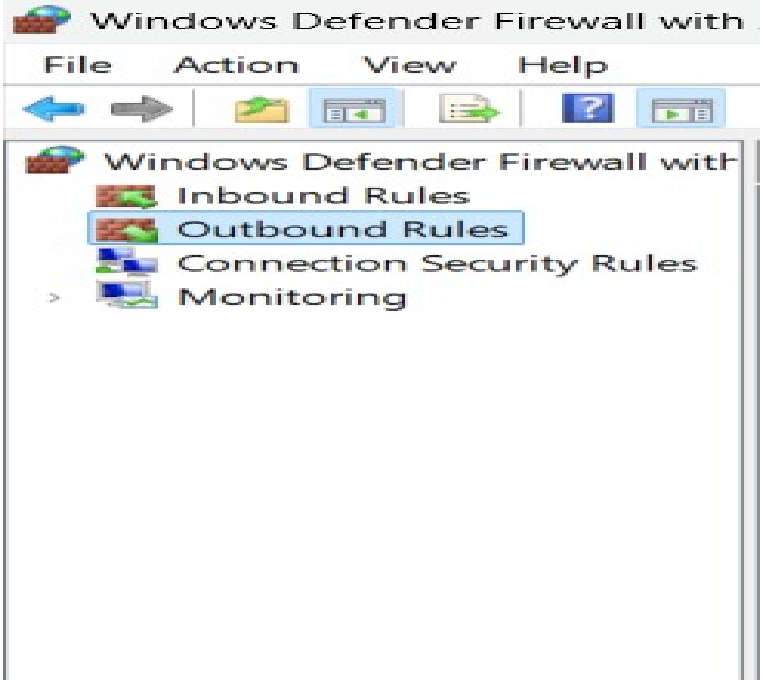
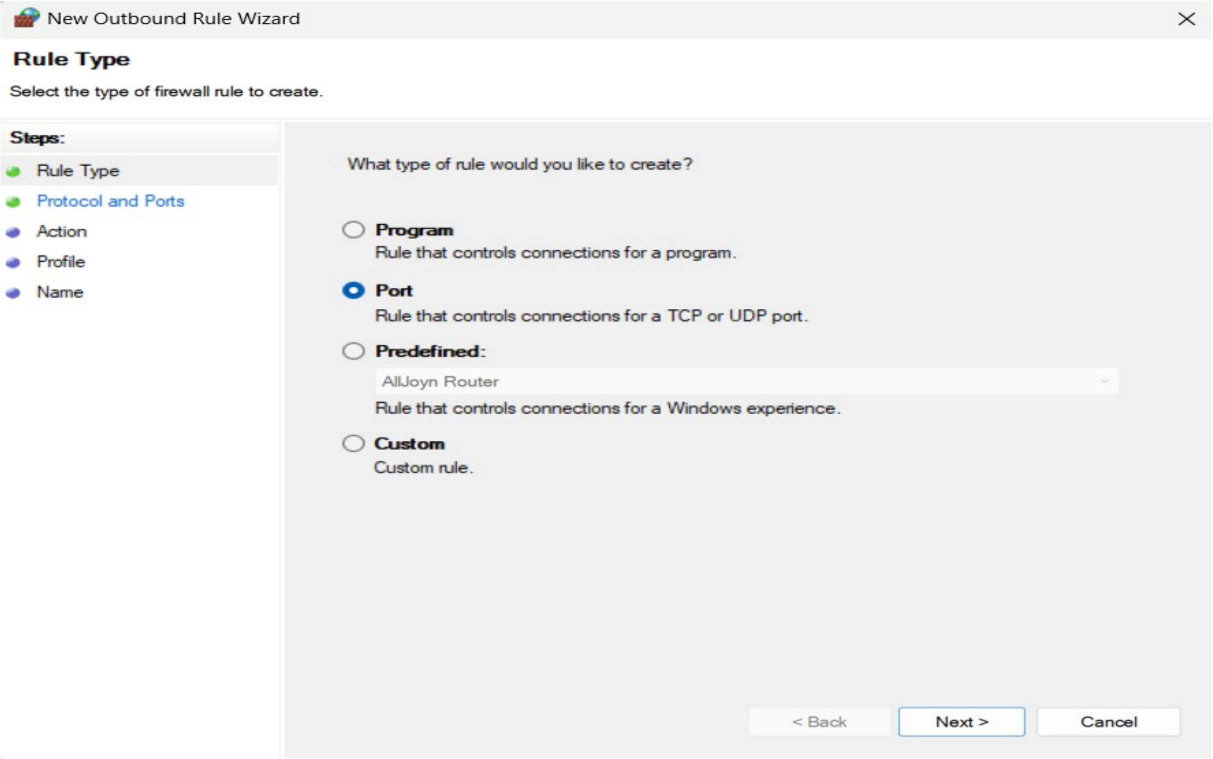

Windows Defender Firewall with
File
Action
View
Help
Windows Defender Firewall with
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring

Figure 4.29: Outbound Rules Window

- Click New Rule to select the type of rule to create : **Port**



New Outbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

What type of rule would you like to create?

○ **Program**
Rule that controls connections for a program.

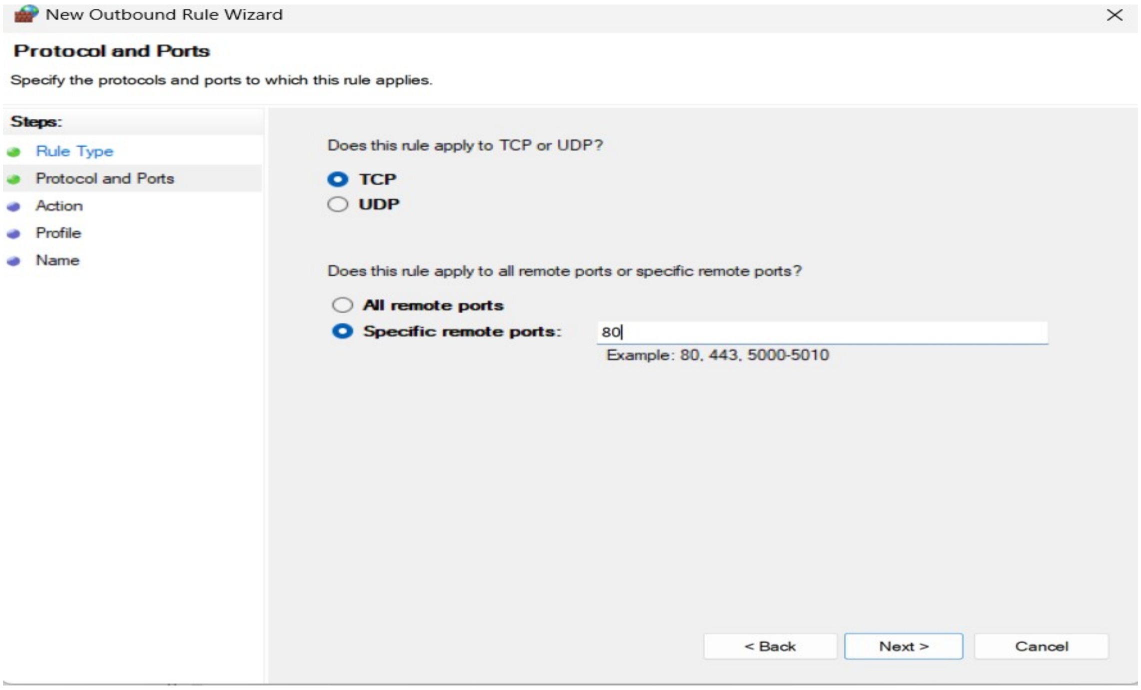
● **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
AllJoyn Router
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

Figure 4.30: Type Selection

- Specify the protocols and port : **TCP and Port:80**



New Outbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Does this rule apply to TCP or UDP?

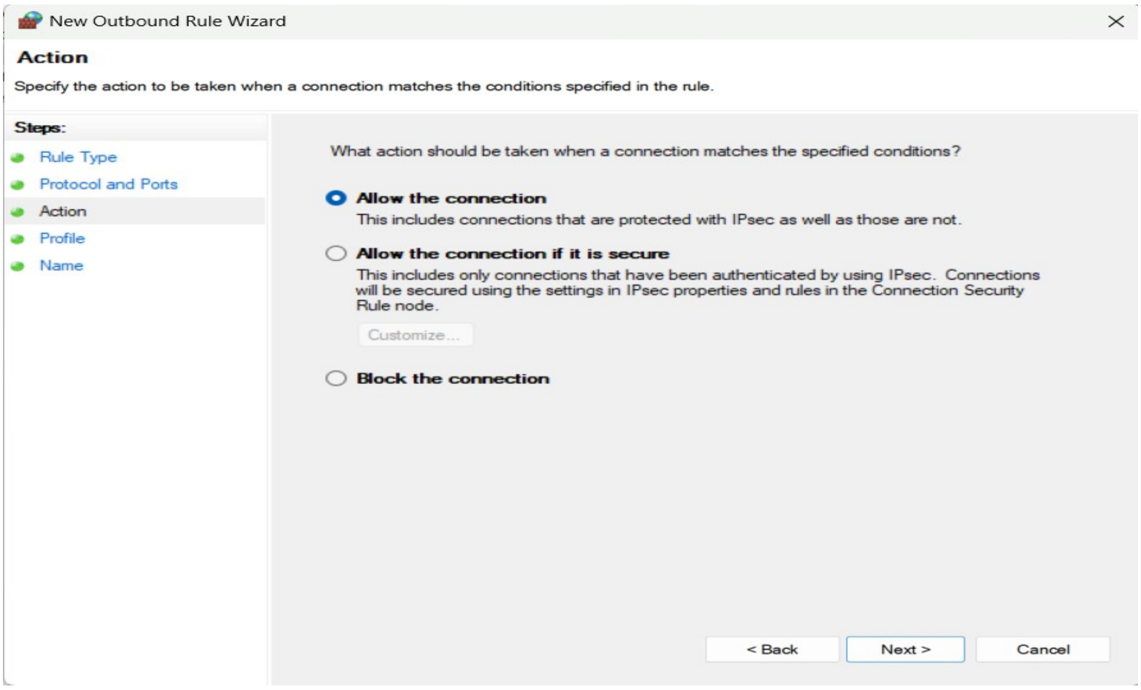
● **TCP**
○ **UDP**

Does this rule apply to all remote ports or specific remote ports?

○ **All remote ports**
● **Specific remote ports:** 80
Example: 80, 443, 5000-5010

Figure 4.31: Protocols and port

- Specify the connection matches specified in the rule : **Allow the Connection**



New Outbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

What action should be taken when a connection matches the specified conditions?

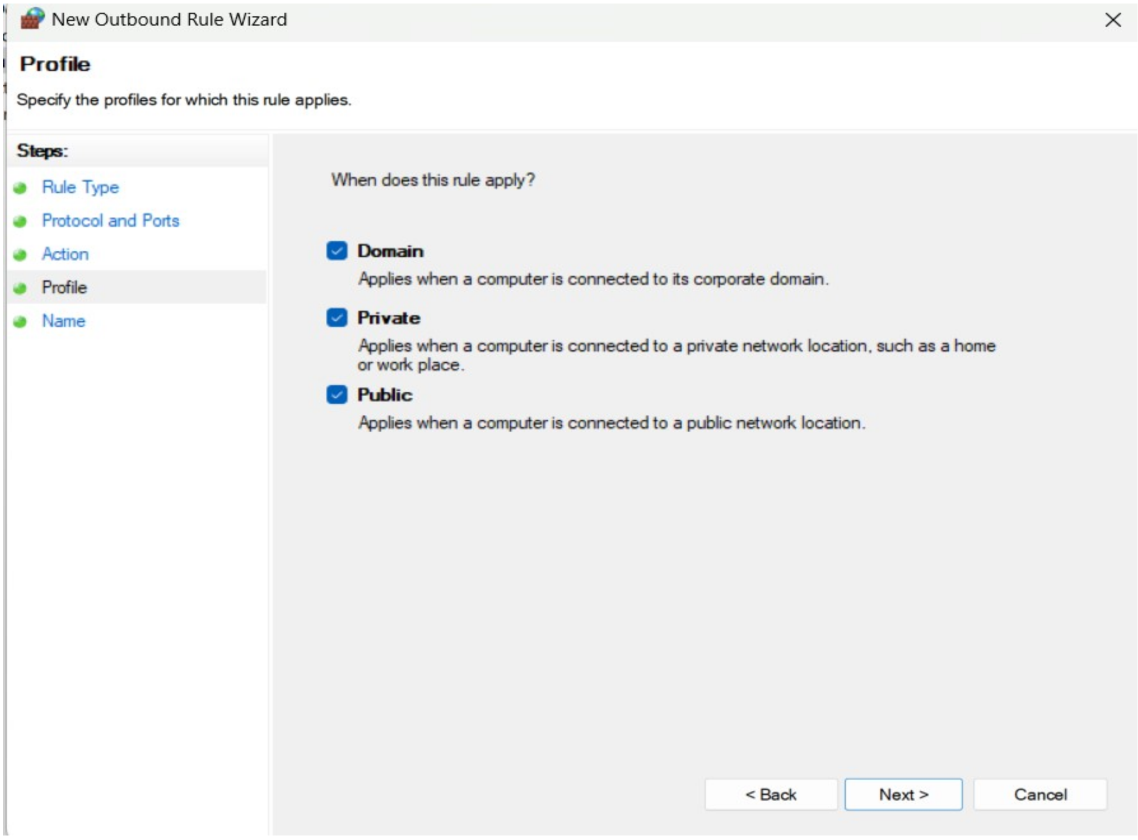
● **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

○ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

○ **Block the connection**

Figure 4.32: Type Selection

- Specify the profiles for rules applies: **Port**


New Outbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

When does this rule apply?

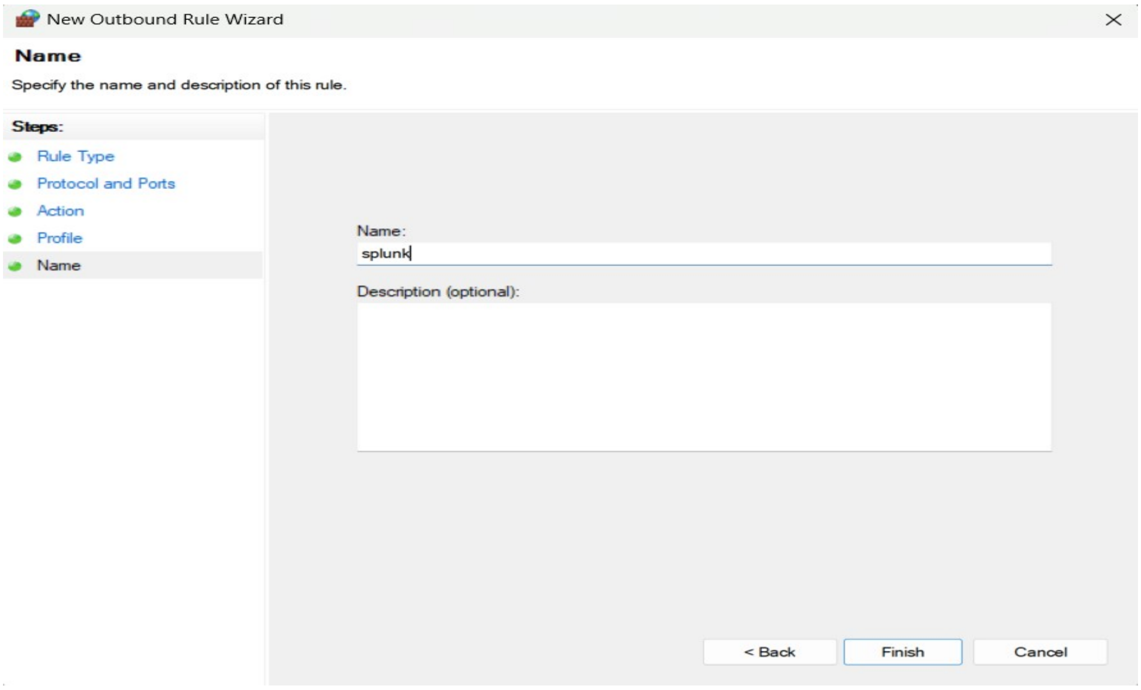
☑ **Domain**
Applies when a computer is connected to its corporate domain.

☑ **Private**
Applies when a computer is connected to a private network location, such as a home or work place.

☑ **Public**
Applies when a computer is connected to a public network location.

Figure 4.33: Profile Applies

- Specify the Name for the rule : **splunk**


New Outbound Rule Wizard

Name

Specify the name and description of this rule.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Name:
splunk

Description (optional):

Figure 4.34: Rule Name

- Outbound Rule created

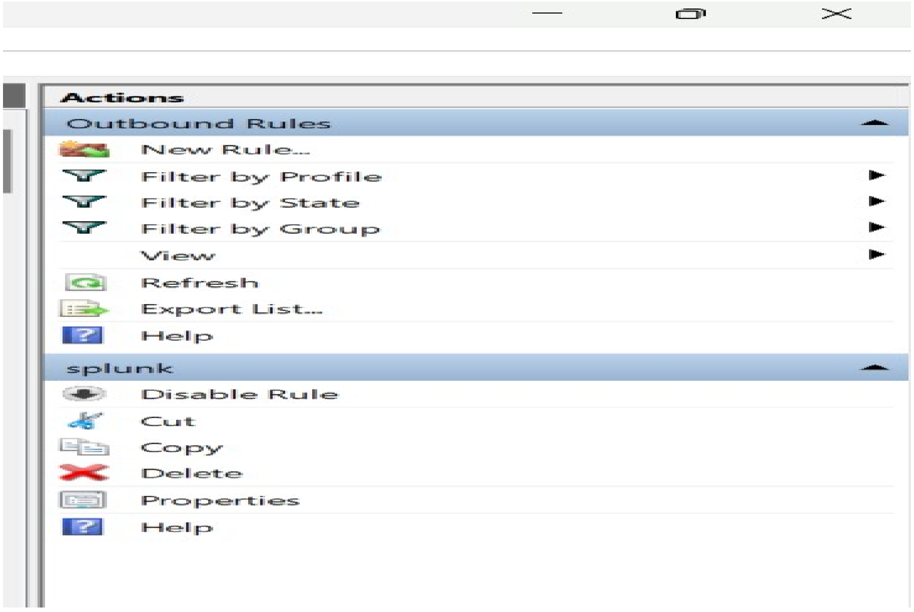
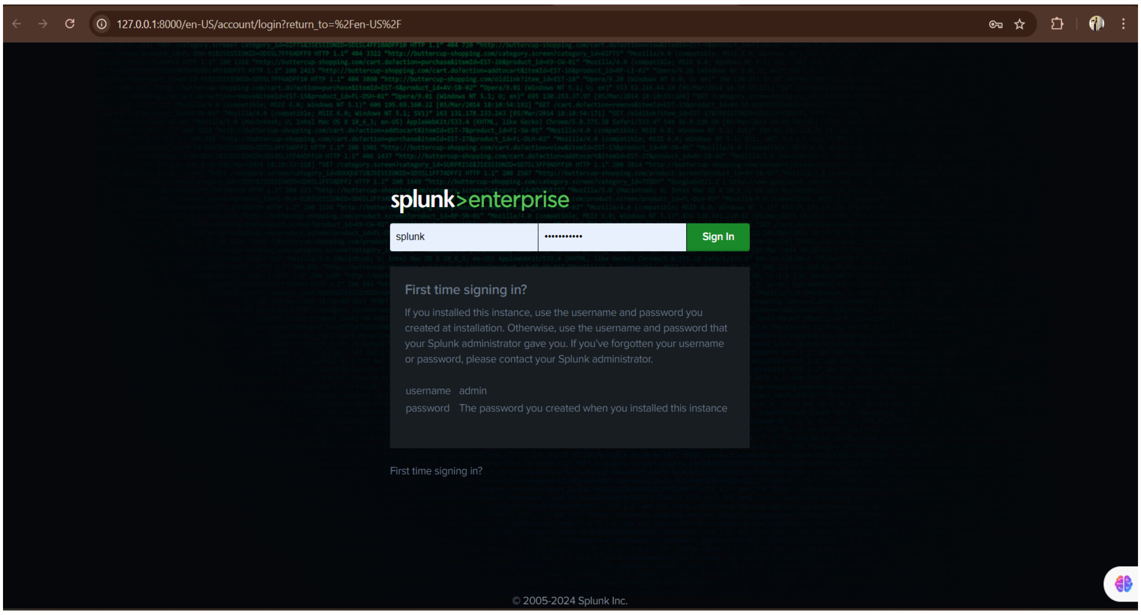


Figure 4.35: Rule created Successfully

4.4 Start Splunk Enterprise

- After installation, Splunk will automatically start as a service.
- Access the web interface at **http://localhost:8000 or http://"Windows-IP":8000 from another machine.**



127.0.0.1:8000/en-US/account/login?return_to=%2Fen-US%2F

splunk>enterprise

splunk ••••••••••• Sign In

First time signing in?

If you installed this instance, use the username and password you created at installation. Otherwise, use the username and password that your Splunk administrator gave you. If you've forgotten your username or password, please contact your Splunk administrator.

username admin
password The password you created when you installed this instance

First time signing in?

© 2005-2024 Splunk Inc.

Figure 4.36: Login Page

4.4.1 Configure Splunk to Receive Data

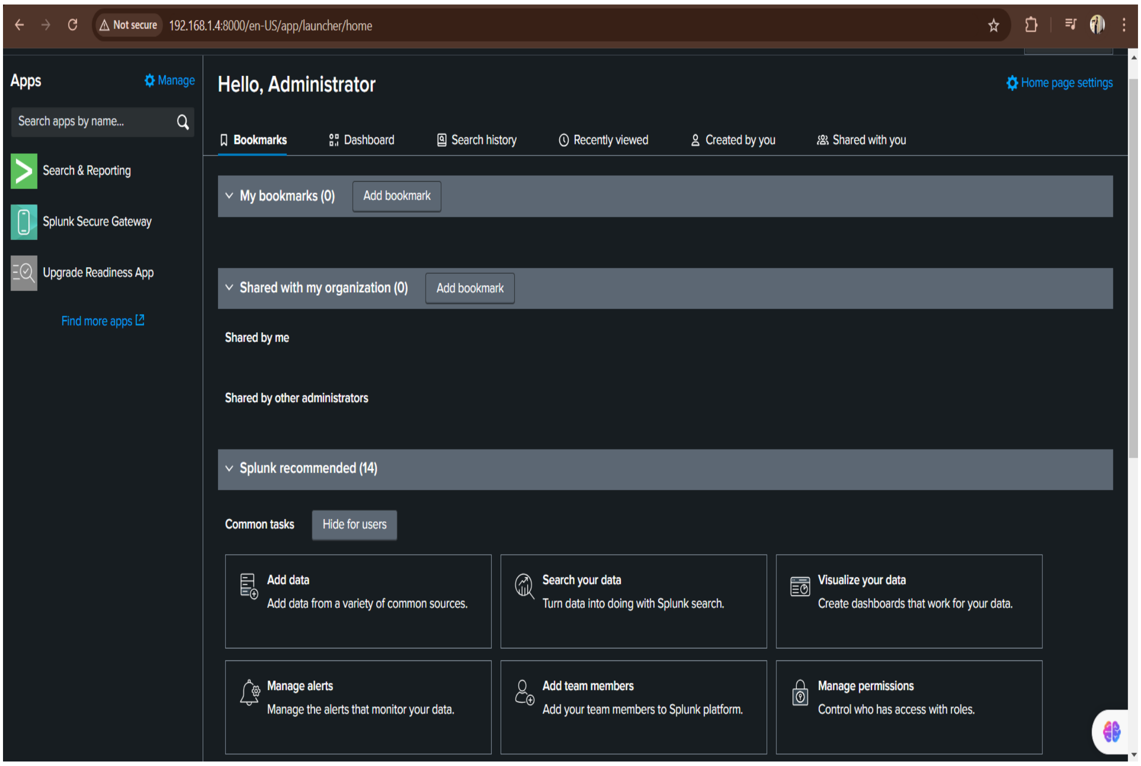
- In the Splunk Web interface, navigate to Settings - Forwarding and Receiving.
- Configure Splunk to listen on port 9997 (or the port defined in the forwarder).

4.5 Enable Receiving Data on Splunk Enterprise

On your Splunk Enterprise (installed on Windows):

4.5.1 Log into Splunk Enterprise:

- Open a web browser.
- Navigate to **http://"your-splunk-ip":8000** "your-splunk-ip" with the actual IP address of your Splunk Enterprise server).
- Log in using your Splunk admin credentials.



Add data
Add data from a variety of common sources.

Search your data
Turn data into doing with Splunk search.

Visualize your data
Create dashboards that work for your data.

Manage alerts
Manage the alerts that monitor your data.

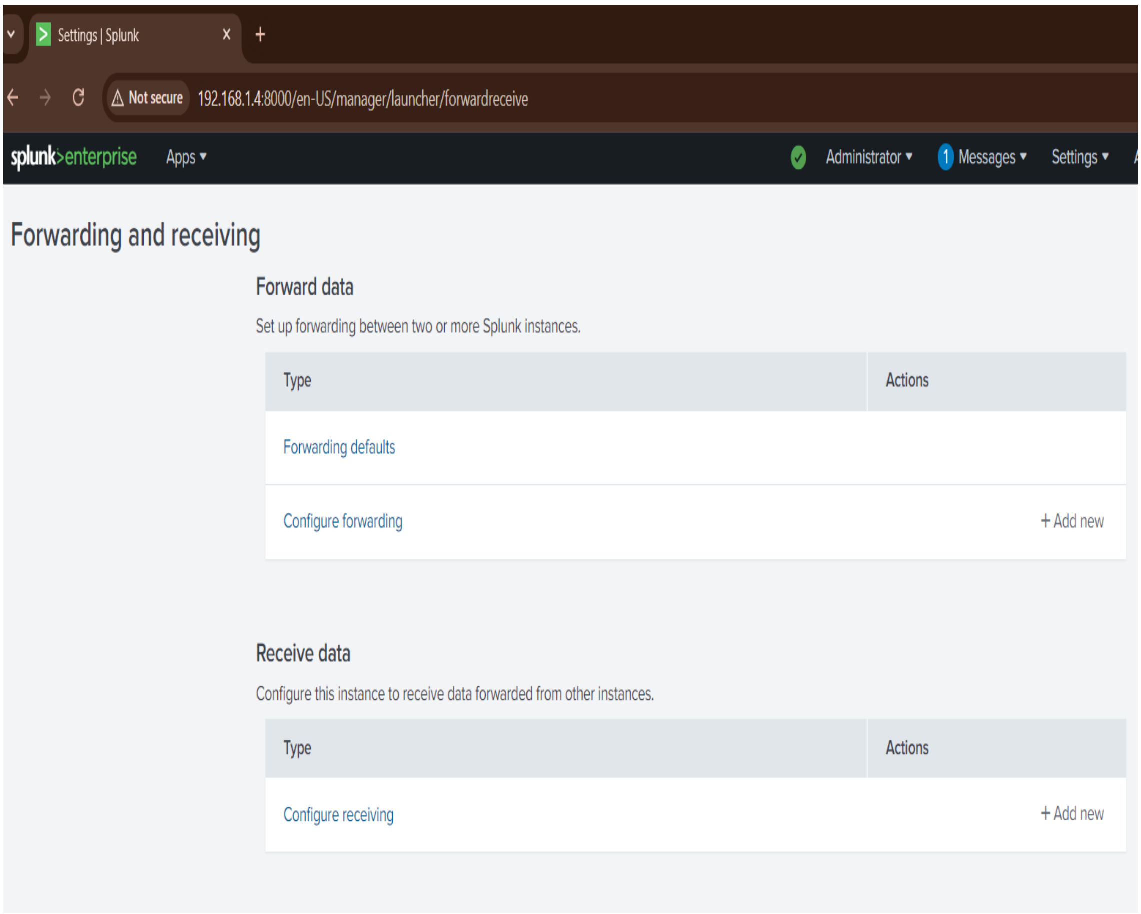
Add team members
Add your team members to Splunk platform.

Manage permissions
Control who has access with roles.

Figure 4.37: Home Page

4.5.2 Go to Settings to Enable Data Input:

- In the top-right corner, click on the **Settings gear icon**
- Under Data in the Settings menu, select Forwarding and receiving. **Settings - Data - Forwarding and receiving**



Forwarding and receiving

Forward data

Set up forwarding between two or more Splunk instances.

Type	Actions
Forwarding defaults	
Configure forwarding	+ Add new

Receive data

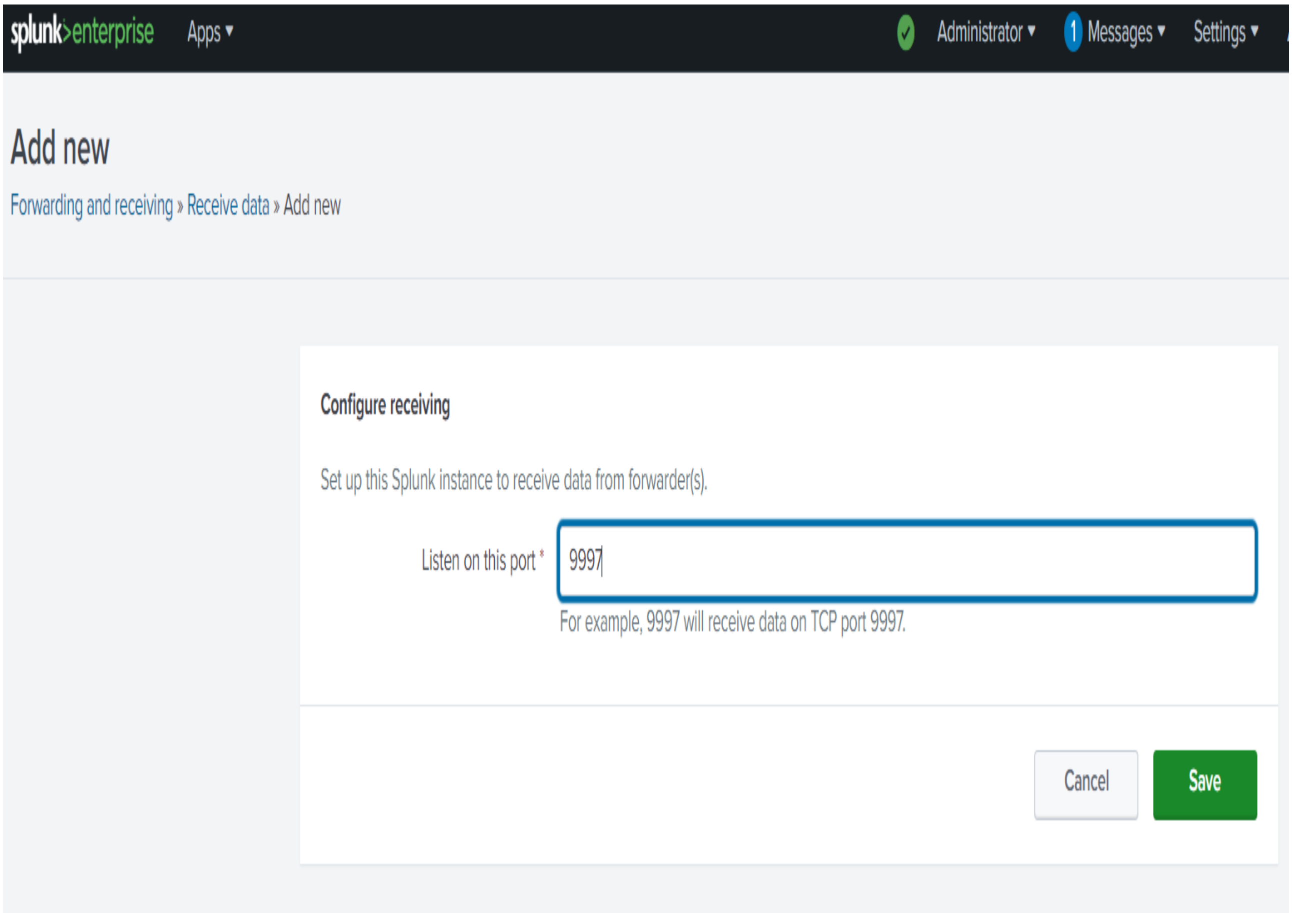
Configure this instance to receive data forwarded from other instances.

Type	Actions
Configure receiving	+ Add new

Figure 4.38: Forwarding and Receiving Page

4.5.3 Configure Receiving Port:

- Under the Receive Data section, click on Add new.
- **Receive Data - Add New**



Add new

Forwarding and receiving » Receive data » Add new

Configure receiving

Set up this Splunk instance to receive data from forwarder(s).

Listen on this port * 9997

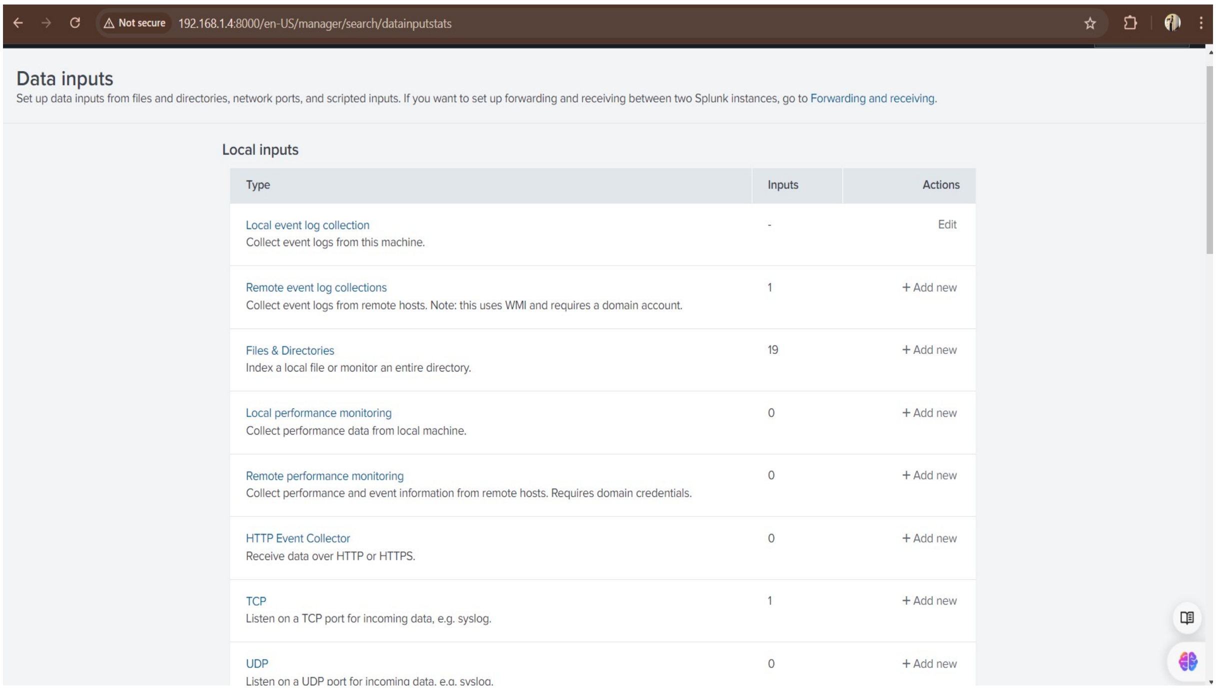
For example, 9997 will receive data on TCP port 9997.

Figure 4.39: Configure Receiving

- In the dialog that appears, specify Port: **9997** (which is the default port used by Splunk Forwarders).
- Click **Save**

4.5.4 Verify Data Inputs:

- Go to **Settings - Data inputs - Forwarded Data**



Data inputs

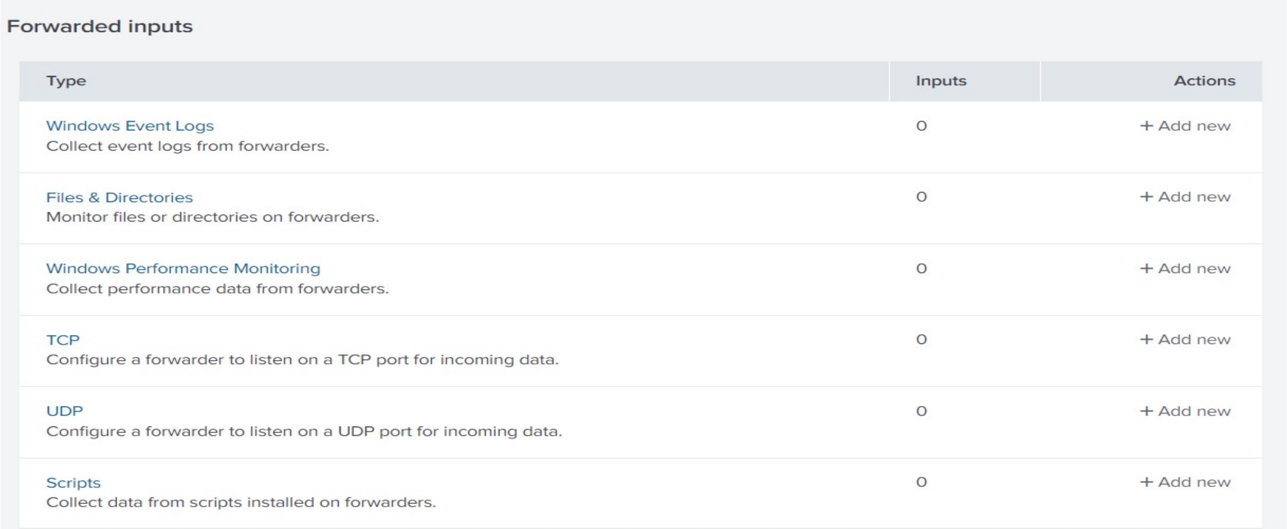
Set up data inputs from files and directories, network ports, and scripted inputs. If you want to set up forwarding and receiving between two Splunk instances, go to Forwarding and receiving.

Local inputs

Type	Inputs	Actions
Local event log collection Collect event logs from this machine.	-	Edit
Remote event log collections Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.	1	+ Add new
Files & Directories Index a local file or monitor an entire directory.	19	+ Add new
Local performance monitoring Collect performance data from local machine.	0	+ Add new
Remote performance monitoring Collect performance and event information from remote hosts. Requires domain credentials.	0	+ Add new
HTTP Event Collector Receive data over HTTP or HTTPS.	0	+ Add new
TCP Listen on a TCP port for incoming data, e.g. syslog.	1	+ Add new
UDP Listen on a UDP port for incoming data, e.g. syslog.	0	+ Add new

Figure 4.40: Data Inputs

- You should see the forwarder listed, indicating it is sending data



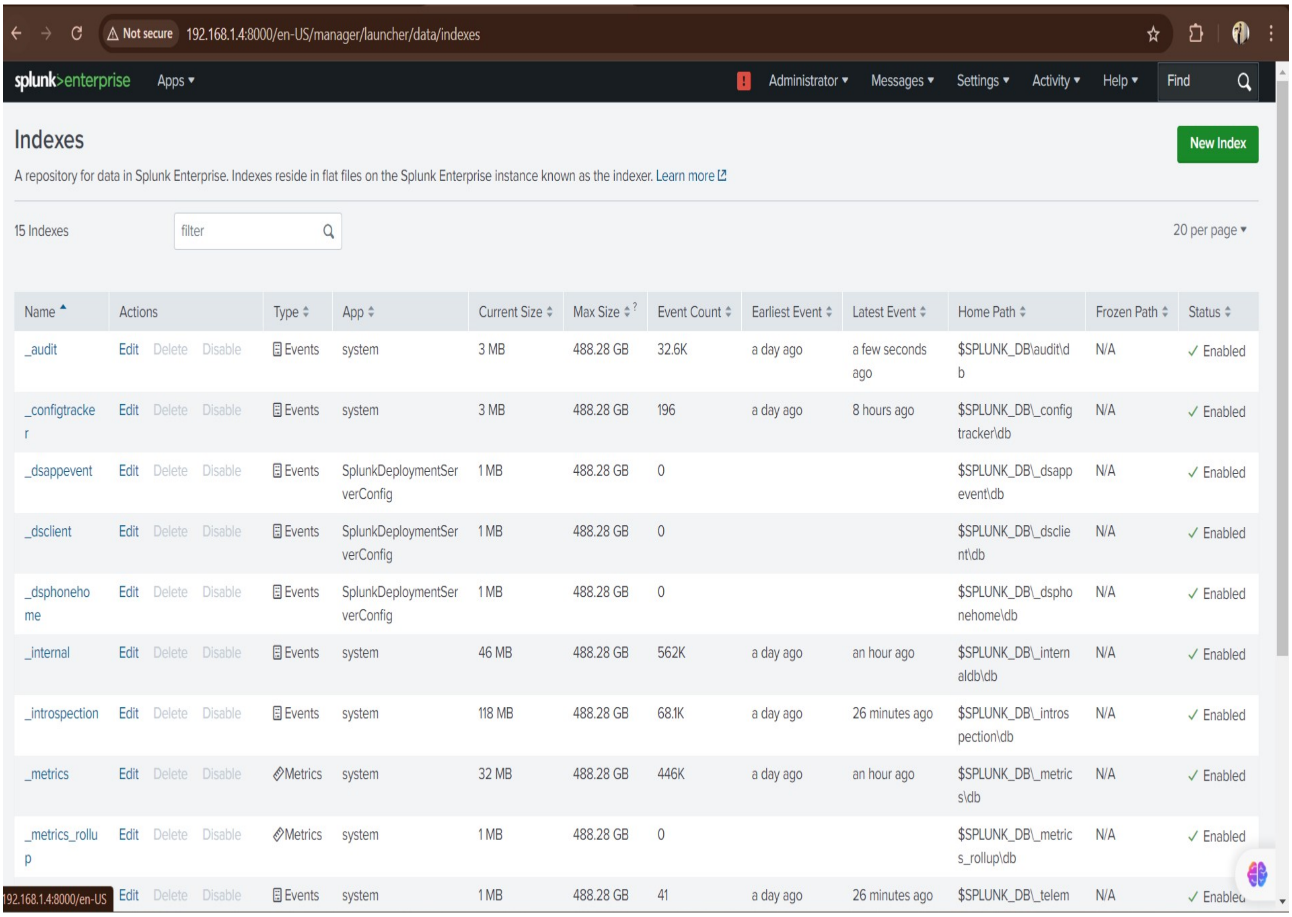
Forwarded inputs

Type	Inputs	Actions
Windows Event Logs Collect event logs from forwarders.	0	+ Add new
Files & Directories Monitor files or directories on forwarders.	0	+ Add new
Windows Performance Monitoring Collect performance data from forwarders.	0	+ Add new
TCP Configure a forwarder to listen on a TCP port for incoming data.	0	+ Add new
UDP Configure a forwarder to listen on a UDP port for incoming data.	0	+ Add new
Scripts Collect data from scripts installed on forwarders.	0	+ Add new

Figure 4.41: Forwarded Inputs

4.5.5 Create or Verify Indexes

- Go to **Settings - Indexes**
- Check if indexes such as linux logs and security exist. If not, you need to create them.



Indexes

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

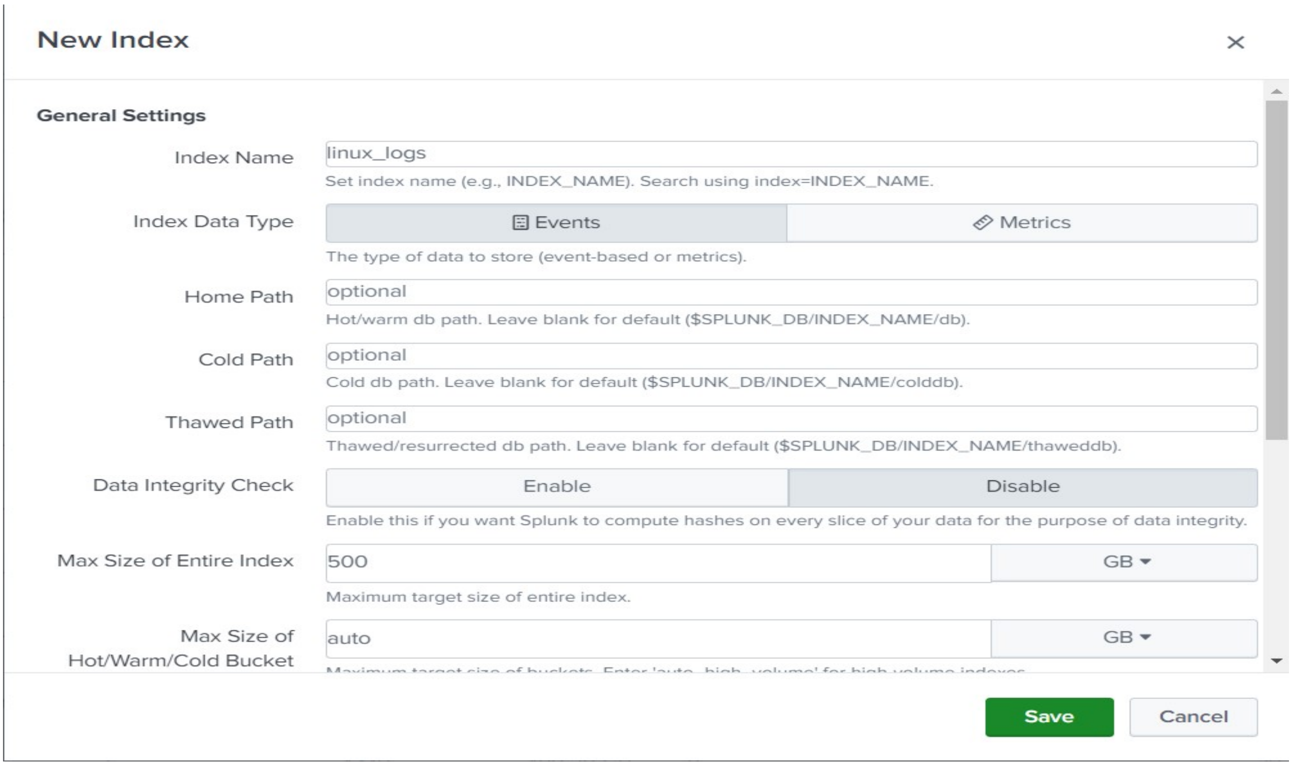
15 Indexes filter 20 per page ▾

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	3 MB	488.28 GB	32.6K	a day ago	a few seconds ago	$SPLUNK_DB\audit\db	N/A	✓ Enabled
_configtracker	Edit Delete Disable	Events	system	3 MB	488.28 GB	196	a day ago	8 hours ago	$SPLUNK_DB_configtracker\db	N/A	✓ Enabled
_dsappevent	Edit Delete Disable	Events	SplunkDeploymentServerConfig	1 MB	488.28 GB	0			$SPLUNK_DB_dsappevent\db	N/A	✓ Enabled
_dsclient	Edit Delete Disable	Events	SplunkDeploymentServerConfig	1 MB	488.28 GB	0			$SPLUNK_DB_dsclient\db	N/A	✓ Enabled
_dsphonehome	Edit Delete Disable	Events	SplunkDeploymentServerConfig	1 MB	488.28 GB	0			$SPLUNK_DB_dsphonehome\db	N/A	✓ Enabled
_internal	Edit Delete Disable	Events	system	46 MB	488.28 GB	562K	a day ago	an hour ago	$SPLUNK_DB_internaldb\db	N/A	✓ Enabled
_introspection	Edit Delete Disable	Events	system	118 MB	488.28 GB	68.1K	a day ago	26 minutes ago	$SPLUNK_DB_introspection\db	N/A	✓ Enabled
_metrics	Edit Delete Disable	Metrics	system	32 MB	488.28 GB	446K	a day ago	an hour 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
	Edit Delete Disable	Events	system	1 MB	488.28 GB	41	a day ago	26 minutes ago	$SPLUNK_DB_telem	N/A	✓ Enabled

Figure 4.42: Indexs

Create New Index (if required):

- Click **New Index**
- Provide a name like **linux logs** or **security** set other options as needed, and click **Save**



New Index

General Settings

Index Name: linux_logs
Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME.

Index Data Type: [✓ Events] Metrics
The type of data to store (event-based or metrics).

Home Path: optional
Hot/warm db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/db).

Cold Path: optional
Cold db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/colddb).

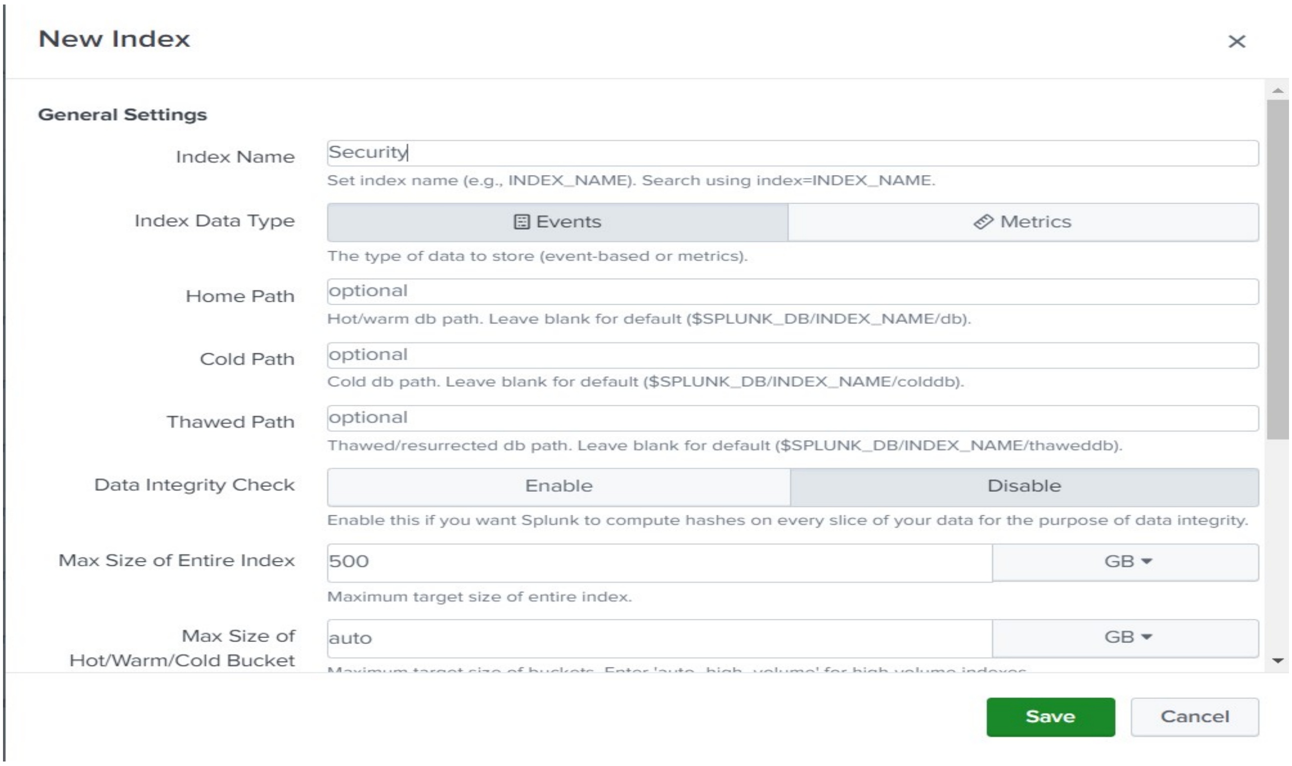
Thawed Path: optional
Thawed/resurrected db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/thaweddb).

Data Integrity Check: Enable [✓ Disable]
Enable this if you want Splunk to compute hashes on every slice of your data for the purpose of data integrity.

Max Size of Entire Index: 500 GB
Maximum target size of entire index.

Max Size of Hot/Warm/Cold Bucket: auto GB
Maximum target size of buckets. Enter 'auto_high_volume' for high-volume indexes.

Figure 4.43: Forwarded Inputs



New Index

General Settings

Index Name: Security
Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME.

Index Data Type: [✓ Events] Metrics
The type of data to store (event-based or metrics).

Home Path: optional
Hot/warm db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/db).

Cold Path: optional
Cold db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/colddb).

Thawed Path: optional
Thawed/resurrected db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/thaweddb).

Data Integrity Check: Enable [✓ Disable]
Enable this if you want Splunk to compute hashes on every slice of your data for the purpose of data integrity.

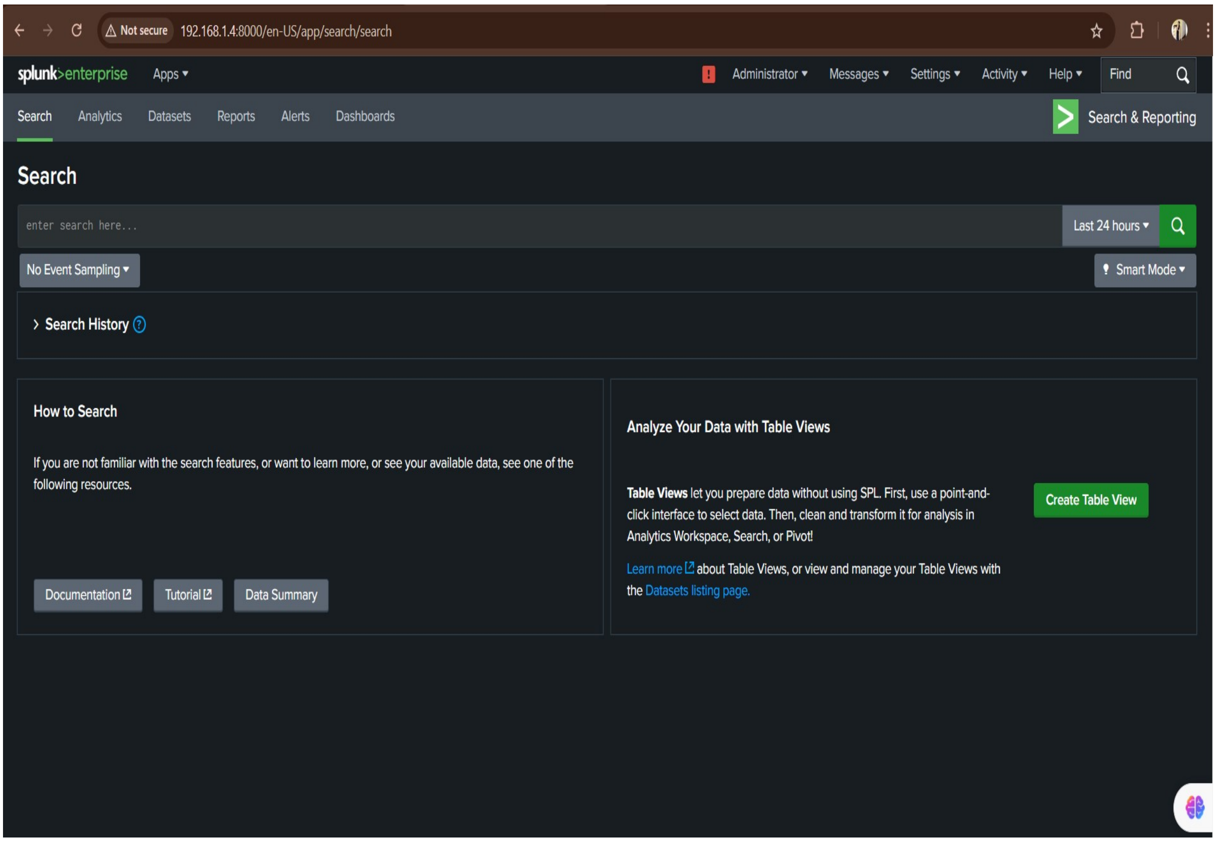
Max Size of Entire Index: 500 GB
Maximum target size of entire index.

Max Size of Hot/Warm/Cold Bucket: auto GB
Maximum target size of buckets. Enter 'auto_high_volume' for high-volume indexes.

Figure 4.44: Forwarded Inputs

4.6 Search for the Linux Logs

- In the Splunk Enterprise web interface, click on **Search and Reporting** from the main menu.
- Use the following search query to view Linux logs: **index=linux logs OR index=security — head 100**



If you are not familiar with the search features, or want to learn more, or see your available data, see one of the following resources.

Table Views let you prepare data without using SPL. First, use a point-and-click interface to select data. Then, clean and transform it for analysis in Analytics Workspace, Search, or Pivot!

Learn more about Table Views, or view and manage your Table Views with the Datasets listing page.

Figure 4.45: Search and Reporting Page

4.7 View Dashboards and Reports

4.8 Create Dashboards

- In the **Search and Reporting app**, after running a search, click on **Save As - Dashboard Panel**
- You can create custom dashboards to visualize specific log data like authentication attempts, system errors, etc.

Chapter 5

RESULTS AND DISCUSSIONS

The integration of Linux logs into Splunk Enterprise yielded significant results that demonstrate the value of centralized log management and analysis. This section discusses the outcomes of the project, the implications of the findings, and insights derived from the implementation process.

5.1 Results

- **Successful Log Data Collection:** The deployment of the Splunk Universal Forwarder on multiple Linux systems facilitated the efficient collection of various log files, including:
- /var/log/syslog
- /var/log/auth.log
- /var/log/secure
- /var/log/kern.log

- Custom application logs

The Forwarder successfully transmitted these logs to the Splunk Indexer, confirming that the data pipeline was functioning correctly.

- **Improved Search and Analysis Capabilities:** Once the log data was ingested into Splunk Enterprise, users were able to utilize the powerful search capabilities of the platform. Searches were executed across all log data, enabling quick identification of issues and trends. The ability to query large datasets in real-time allowed for more effective troubleshooting and performance monitoring.
- **Enhanced Security Monitoring:** The project allowed for continuous monitoring of security-related logs, which enabled the detection of unauthorized access attempts and unusual activity patterns. Alerts were configured to notify IT teams of potential security incidents, thereby improving the organization's overall security posture.
- **Operational Insights and Reporting:** The creation of dashboards and reports provided valuable insights into system performance, user activity, and security events. These visualizations facilitated better decision-making and helped teams focus on critical issues.
- **Compliance Support:** The systematic collection and retention of logs positioned the organization to meet various regulatory com-

pliance standards. The ability to retrieve and analyze logs on demand ensured that the organization was audit-ready.

5.2 Discussion

The results of the project highlight several important considerations:

- **Centralized Log Management:** The shift to a centralized log management solution using Splunk Enterprise has proven beneficial in simplifying the management of log data. By consolidating logs from various Linux systems into a single platform, the organization reduced the complexity and time associated with troubleshooting and incident response.

- **Scalability and Flexibility:** Splunk's architecture allows for easy scalability, making it suitable for organizations of all sizes. As the organization grows, adding new log sources and expanding the Splunk deployment can be done seamlessly, ensuring continued effectiveness in log management.

- **Real-time Insights:** The ability to analyze log data in real-time provides organizations with timely insights into their IT operations. This capability is crucial for proactive incident management and supports the shift towards more data-driven decision-making.

- **Enhanced Security Measures:** With the enhanced visibility provided by centralized log management, organizations can adopt a more proactive security stance. Continuous monitoring of security logs allows for quicker identification and remediation of threats, reducing the risk of data breaches.
- **Challenges and Considerations:** Despite the successes, some challenges were encountered during implementation, including:
- Initial configuration complexity, particularly in setting up Forwarders and ensuring proper data routing.
- The need for training staff to effectively use Splunk and interpret the data being collected.
- Managing the volume of logs generated, which requires careful planning regarding data retention and storage.

In conclusion, the integration of Linux logs into Splunk Enterprise has provided substantial benefits in log management, security monitoring, and compliance. The positive results indicate that with proper implementation and ongoing enhancements, organizations can significantly improve their operational insights and incident response capabilities. Future projects should focus on addressing the challenges encountered and exploring additional integrations and automations to further enhance the logging infrastructure.

Chapter 6

CONCLUSION AND RECOMMENDATIONS

6.1 Conclusion

This project successfully demonstrated the integration of Linux logs into Splunk Enterprise, showcasing the advantages of centralized log management for enhanced monitoring, analysis, and optimization of IT operations. By configuring the Splunk Forwarder on Linux systems, we efficiently collected and forwarded critical logs, such as /var/log/syslog, /var/log/auth.log, and various application-specific logs to Splunk Enterprise. The implementation provided several significant benefits, including:

- **Improved Troubleshooting:** Centralized log data enabled faster identification and resolution of system issues, streamlining the troubleshooting process for IT teams.

- **Enhanced Security Monitoring:** Continuous monitoring of security logs facilitated the detection of unauthorized access attempts and potential security threats, strengthening the overall security posture.
- **Regulatory Compliance:** The logging solution supported compliance with industry standards by ensuring that logs were systematically collected, stored, and available for audits.

Overall, integrating Linux logs into Splunk Enterprise not only enhanced operational efficiency but also improved the organization's ability to respond proactively to incidents.

6.2 Recommendations

To build upon the successes of this project and further enhance the log management capabilities, the following recommendations are made:

- **Broaden Log Source Coverage:** Consider integrating additional log sources, such as cloud environments, network devices, and IoT systems, to gain a more comprehensive view of the entire IT landscape.

- **Utilize Machine Learning Features:** Leverage Splunk's machine learning capabilities to analyze log data for patterns and anomalies. This can help in predicting potential issues before they escalate, allowing for proactive management.

- **Develop Custom Dashboards:** Create specialized dashboards tailored to different user roles within the organization (e.g., IT operations, security, compliance). Custom dashboards can enhance the relevance of data presented and improve decision-making processes.

- **Implement Advanced Alerting:** Establish more granular and context-aware alerting mechanisms to reduce false positives and ensure critical alerts are prioritized, enabling faster incident response.

- **Training and Documentation:** Providing ongoing training for IT staff on using Splunk effectively, along with comprehensive documentation, can enhance the team's capabilities in log management and incident response.

- **Document Procedures:** Maintain thorough documentation of processes, configurations, and best practices for using Splunk. This will facilitate knowledge transfer and help new team members onboard effectively.

- **Integrate with Automation Tools:** Explore the integration of automation tools to streamline incident response workflows, reducing manual intervention and speeding up remediation efforts.

By implementing these recommendations, organizations can further enhance their use of Splunk Enterprise for Linux log management, resulting in improved operational insights, increased security posture, and better compliance management.

Reference

[1] Splunk Enterprise - https://www.splunk.com/en$_{u}s/download/splunk-enterprise.html$

[2] Splunk Documentation - https://docs.splunk.comhttps://docs.splunk.com

[3] Splunk Forwarder - https://www.splunk.com/en$_{u}s/download/universal-forwarder.html$

[4] Linux System Logs - https://www.tecmint.com/manage-log-files-in-linux/https://www.tecmint.com/manage-log-files-in-linux/

[5] Splunk Best Practices for Data Collection - https://www.splunk.com/en$_{u}s/resources.html$