

Splunk Cloud Setup with Universal Forwarder

This documentation outlines how to install and configure Splunk Cloud using the Universal Forwarder on Windows Server 2022 within Oracle VirtualBox.

Tools & Technologies Used

Oracle VirtualBox- Windows Server 2022

Splunk Cloud (Free Trial)

Splunk Universal Forwarder

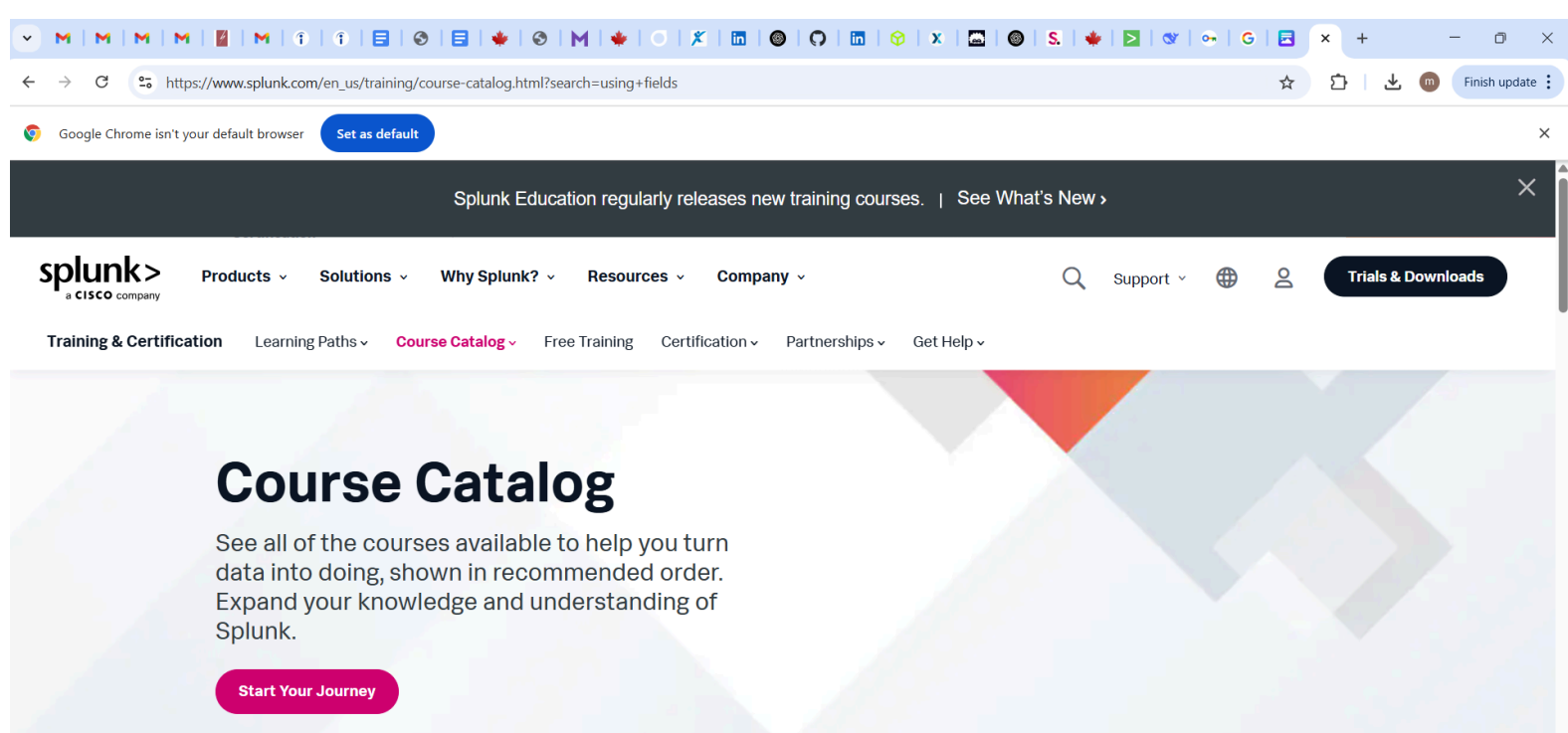
Canva (for documentation and presentation)

Windows Command Prompt (Admin)

Step-by-Step Setup

Step 1: Get a Splunk Cloud Instance

1. Go to: https://www.splunk.com/en_us/cloud.html
2. Click “Start Free Trial” and fill in the form
3. Check your email for login credentials and Splunk Cloud URL
4. Accept the terms and set a new password
5. Navigate to the “Search & Reporting” app once logged in



← → ↻ 📄 https://www.splunk.com/en_us/download/splunk-cloud.html 📄 ☆ 📄 | 📄 📄 Finish update ⋮

Google Chrome isn't your default browser [Set as default](#) ✕

splunk> a CISCO company

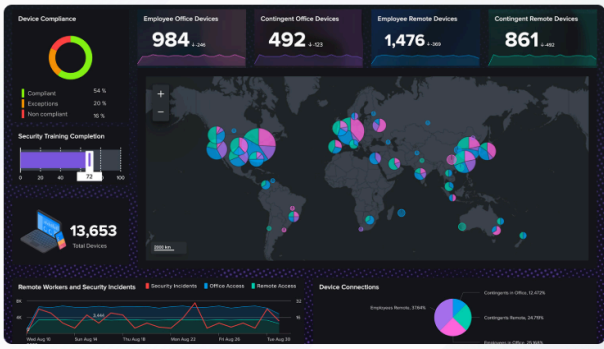
Products ▾ Solutions ▾ Why Splunk? ▾ Resources ▾ Company ▾

🔍 Support ▾ 🌐 👤

FREE TRIAL

Splunk Cloud Platform Trial

Try Splunk Cloud free for 14 days. No credit card required.



Start Your Cloud Platform Trial

Already have a Splunk account? [Log In](#)

Would you like me to connect you directly to someone who can answer your questions?

✕

Step 2: Download Universal Forwarder Credential Package

1. From your Splunk Cloud dashboard, click the gear icon
2. Select Universal Forwarder
3. Click Download Universal Forwarder Credentials (.spl file)

← → ↻ 📄 https://www.splunk.com/en_us/download.html 📄 ☆ 📄 | 📄 📄 Finish update ⋮


Google Chrome isn't your default browser [Set as default](#) ✕

[Get My Free Trial](#) [View Product](#)

Universal Forwarder

The universal forwarder (UF) collects data securely from remote sources, including other forwarders, and sends it into Splunk software for indexing and consolidation. It's the primary way to send data into your Splunk Cloud Platform or Splunk Enterprise instance.

[Get My Free Download](#)



Additional products

Explore more trials and downloads to see which Splunk products are the right fit for you.

Step 3: Install the Splunk Universal Forwarder

1. Visit: https://www.splunk.com/en_us/download/universal-forwarder.html
2. Download the Windows 64-bit .msi installer
3. Run the installer:
 - Accept the license
 - Select "Splunk Cloud Instance"
 - Customize: run as Local System Account
 - Manually enter your admin username & password
 - Skip Deployment Server screen → Click Install

The screenshot shows a web browser window with the URL https://www.splunk.com/en_us/download/universal-forwarder.html. The page title is "Splunk Universal Forwarder 9.4.1". Below the title, a description states: "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." A section titled "Choose Your Installation Package" features tabs for different operating systems: Windows, Linux, Mac OS, Free BSD, Solaris, and AIX. The "Windows" tab is selected, showing two options: "32-bit Windows 10" and "64-bit Windows 10, 11 Windows Server 2019, 2022, 2025". Each option includes a ".msi" file format, a size (64.85 MB and 180.04 MB respectively), a "Download Now" button, a "Copy wget link" button, and a "More" dropdown menu. At the bottom, there are links for "Release Notes", "System Requirements", and "Previous Releases". A small notification at the bottom right asks, "Would you like me to connect you".

Splunk Universal Forwarder 9.4.1

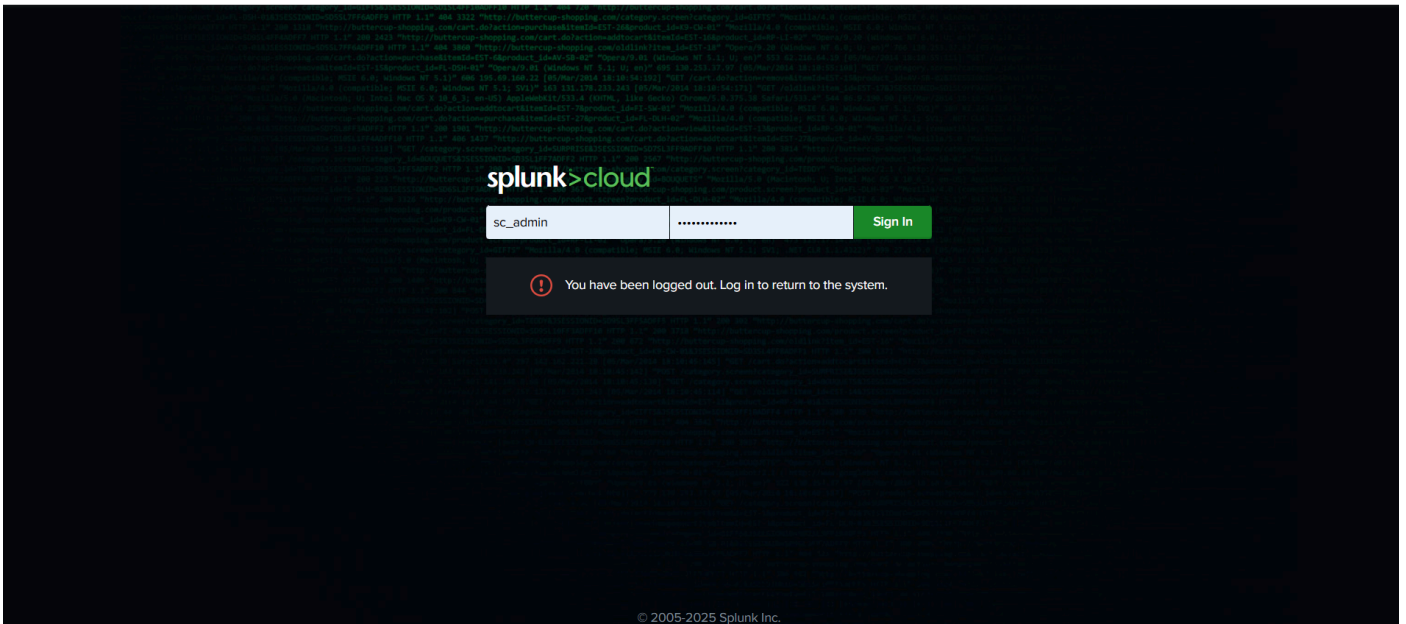
Universal Forwarders provide reliable, secure data collection from remote sources and forward that data into Splunk software for indexing and consolidation. They can scale to tens of thousands of remote systems, collecting terabytes of data.

Choose Your Installation Package

Architecture	Operating System	File Format	Size	Download Now	Copy wget link	More
32-bit	Windows 10	.msi	64.85 MB	Download Now	Copy wget link	More ▾
64-bit	Windows 10, 11 Windows Server 2019, 2022, 2025	.msi	180.04 MB	Download Now	Copy wget link	More ▾

[Release Notes](#) | [System Requirements](#) | [Previous Releases](#)

Would you like me to connect you



© 2005-2025 Splunk Inc.

Step 4: Install the UF Credential Package in CMD

1. Open Command Prompt as Administrator
2. Navigate to Splunk Universal Forwarder bin directory: `cd "C:\Program Files\SplunkUniversalForwarder\bin"`
3. Run the install command: `splunk.exe install app "C:\Users\Administrator\Downloads\splunkclouduf.spl"`

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.20348.587]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd program files
The system cannot find the path specified.

C:\Users\Administrator>cd "program files"
The system cannot find the path specified.

C:\Users\Administrator>cd c:\

c:\>cd program files

c:\Program Files>cd splunkuniversalforwarder

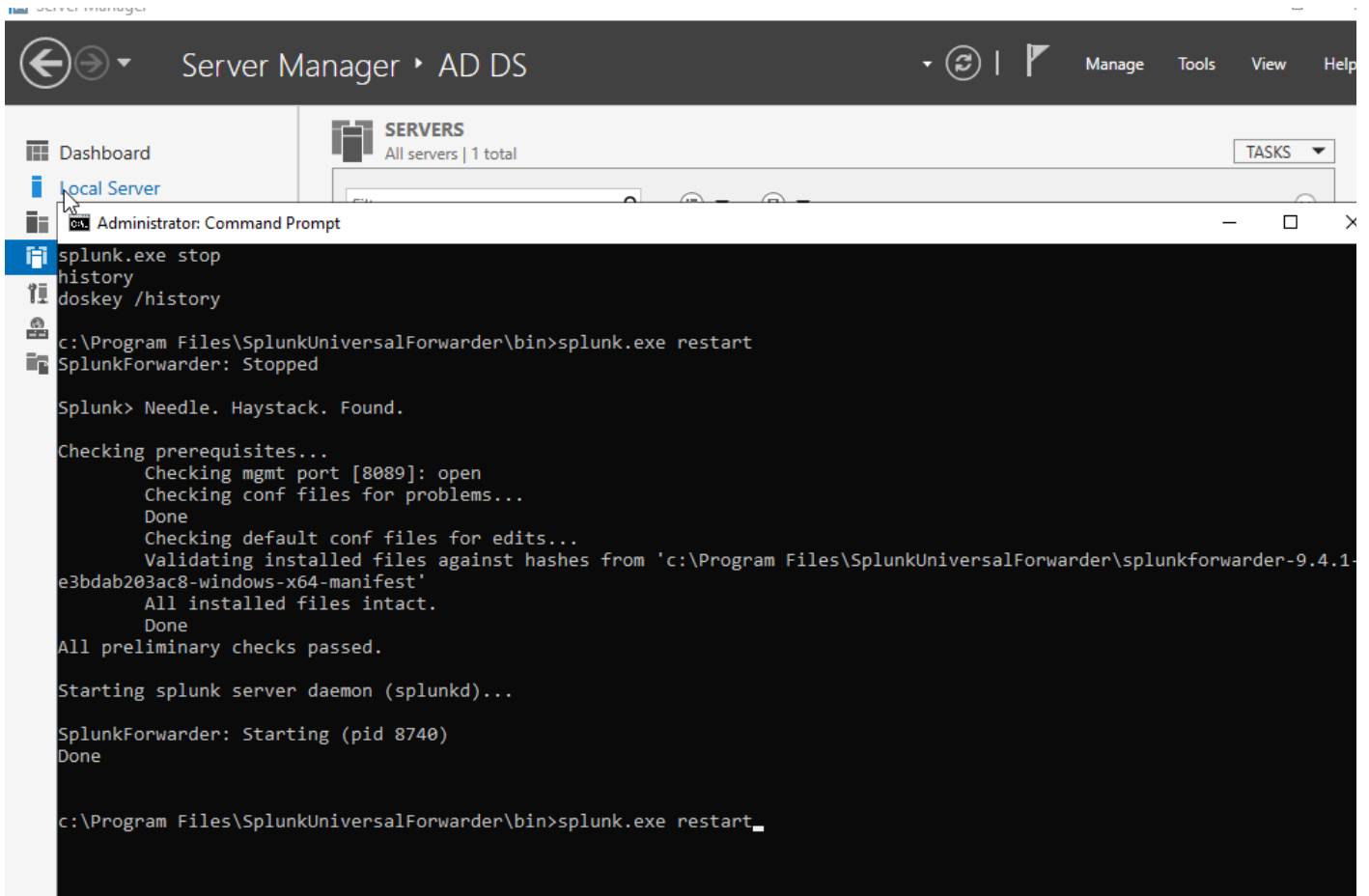
c:\Program Files\SplunkUniversalForwarder>cd bin

c:\Program Files\SplunkUniversalForwarder\bin>cd splunk.exe install app "C:\Users\Administrator\Downloads\splunkclouduf.spl"
The filename, directory name, or volume label syntax is incorrect.

c:\Program Files\SplunkUniversalForwarder\bin>splunk.exe install app "C:\Users\Administrator\Downloads\splunkclouduf.spl"
Splunk username: mamurhomu
Password:
App 'C:\Users\Administrator\Downloads\splunkclouduf.spl' installed
You need to restart the Splunk Server (splunkd) for your changes to take effect.
```

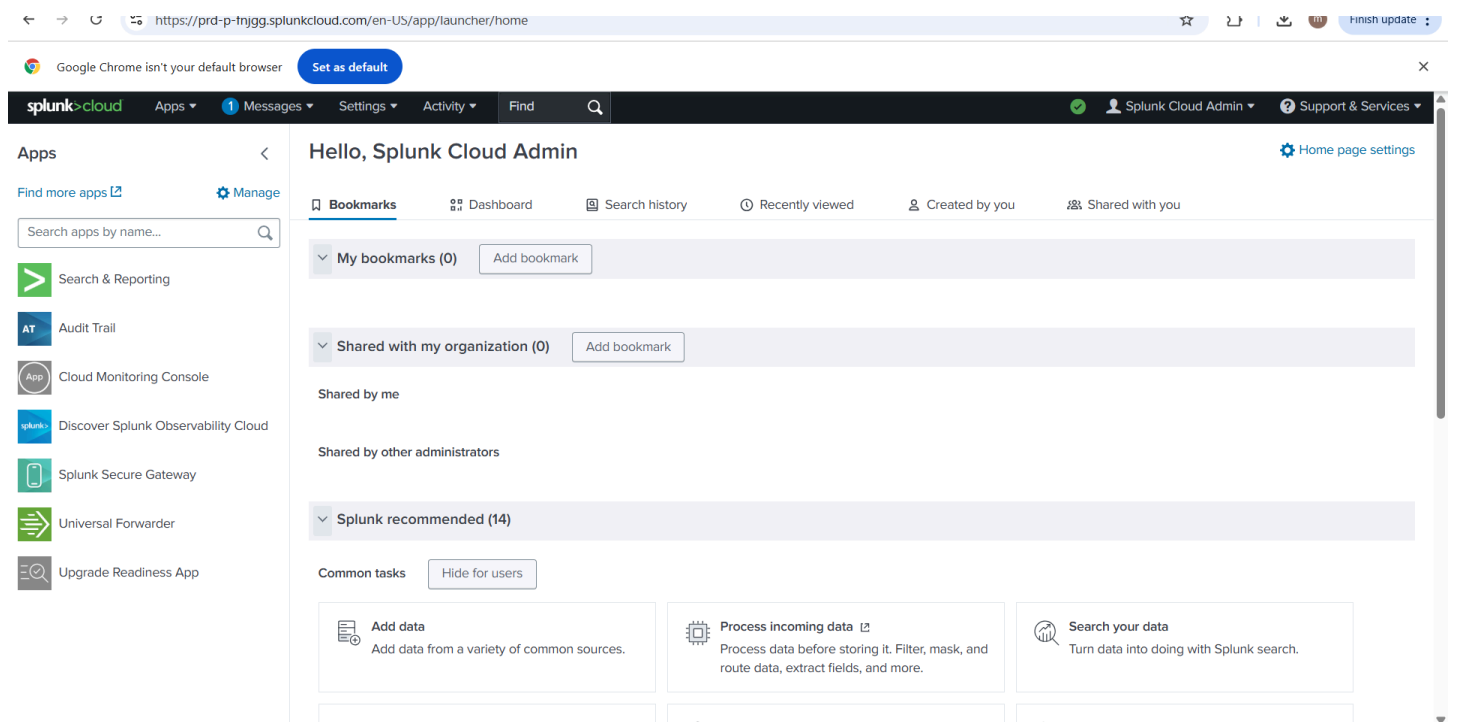
Step 5: Restart the Splunk Forwarder

Run this in Command Prompt: `splunk.exe restart`

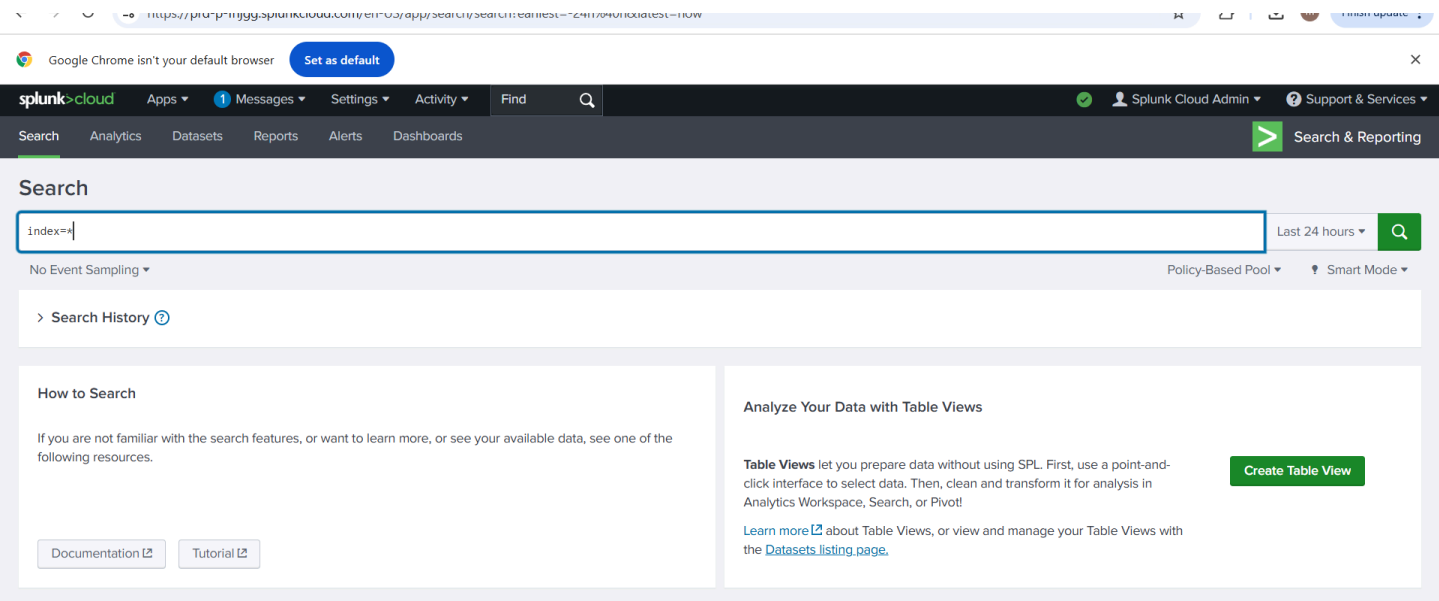


Step 6: Verify Connection

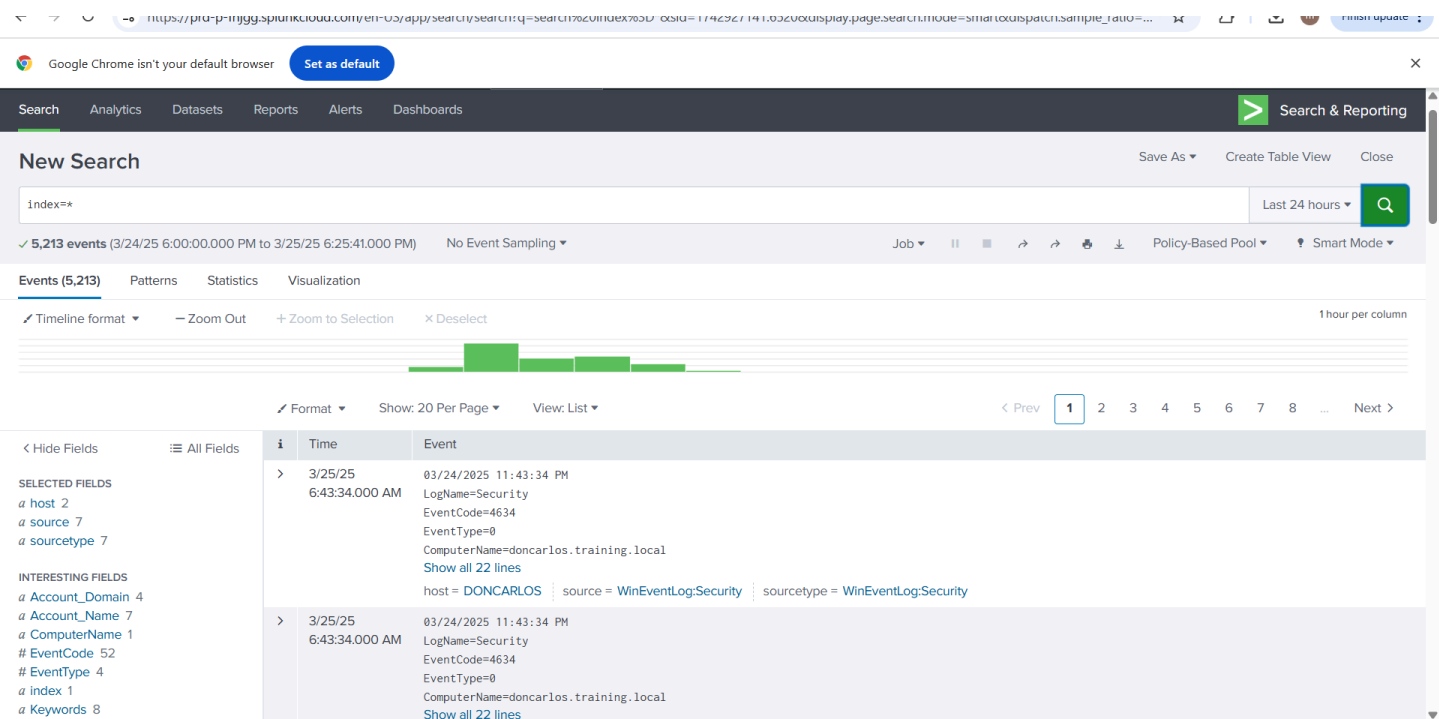
1. Return to Splunk Cloud
2. Click Search & Reporting



3. Search for: index=*4.



Confirm log data is being received



Google Chrome isn't your default browser

Set as default

< Hide Fields

All Fields

Format

Show: 20 Per Page

View: List

< Prev

1

2

3

4

5

6

7

8

...

Next >

a host 2

a source 7

a sourcetype 7

INTERESTING FIELDS

a Account_Domain 4

a Account_Name 7

a ComputerName 1

EventCode 52

EventType 4

a index 1

a Keywords 8

linecount 64

a LogName 3

a Logon_ID 100+

Logon_Type 3

a Message 100+

a OpCode 5

a punct 100+

RecordNumber 100+

a Security_ID 8

a SourceName 18

a splunk_server 1

a TaskCategory 19

a Type 3

499 more fields

+ Extract New Fields

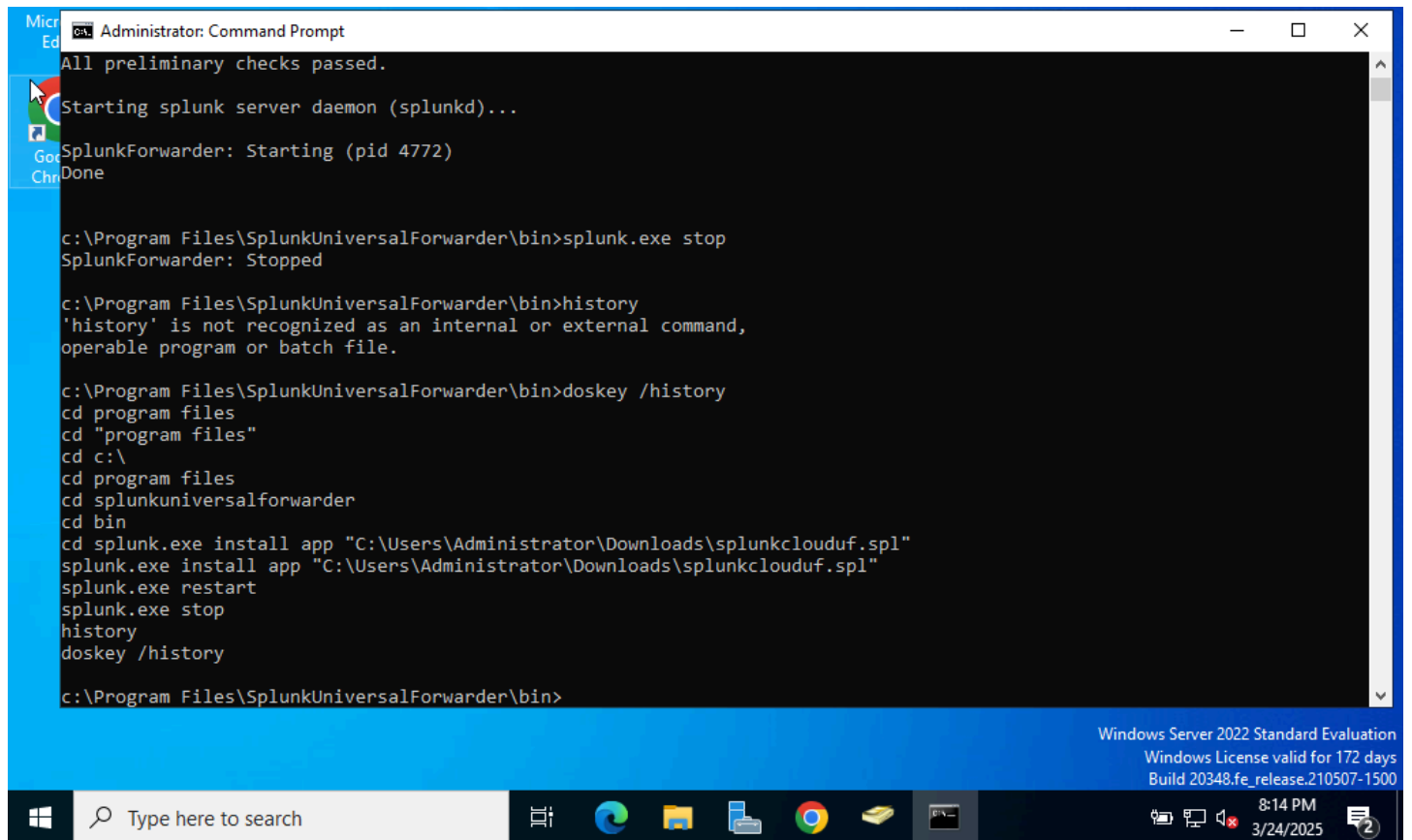
i	Time	Event
		EventType=0 ComputerName=doncarlos.training.local Show all 22 lines host = DONCARLOS source = WinEventLog:Security sourcetype = WinEventLog:Security
>	3/25/25 6:43:34.000 AM	03/24/2025 11:43:34 PM LogName=Security EventCode=4634 EventType=0 ComputerName=doncarlos.training.local Show all 22 lines host = DONCARLOS source = WinEventLog:Security sourcetype = WinEventLog:Security
>	3/25/25 5:11:02.000 AM	03/24/2025 22:11:02.215 -0700 collection="Network Interface" object="Network Interface" counter="Bytes Sent/sec" instance="Intel[R] PRO_1000 MT Desktop Adapter" Show all 6 lines host = DONCARLOS source = Perfmon:Network Interface sourcetype = Perfmon:Network Interface
>	3/25/25 5:11:02.000 AM	03/24/2025 22:11:02.215 -0700 collection="Network Interface" object="Network Interface" counter="Bytes Received/sec" instance="Intel[R] PRO_1000 MT Desktop Adapter" Show all 6 lines host = DONCARLOS source = Perfmon:Network Interface sourcetype = Perfmon:Network Interface
>	3/25/25 5:11:02.000 AM	03/24/2025 22:11:02.205 -0700 collection="CPU Load"

Skills Demonstrated

- Windows Server Command Line- Splunk Cloud and Forwarder Configuration- Real-time Troubleshooting- Credential Handling and Verification- Documentation for Deployment and Training

Screenshots

Screenshots of each step can be added here or uploaded in GitHub repo.



The screenshot shows a Windows Server 2022 Standard Evaluation desktop. An Administrator Command Prompt window is open, displaying the following text:

```
Administrator: Command Prompt
All preliminary checks passed.
Starting splunk server daemon (splunkd)...
SplunkForwarder: Starting (pid 4772)
Done

c:\Program Files\SplunkUniversalForwarder\bin>splunk.exe stop
SplunkForwarder: Stopped

c:\Program Files\SplunkUniversalForwarder\bin>history
'history' is not recognized as an internal or external command,
operable program or batch file.

c:\Program Files\SplunkUniversalForwarder\bin>doskey /history
cd program files
cd "program files"
cd c:\
cd program files
cd splunkuniversalforwarder
cd bin
cd splunk.exe install app "C:\Users\Administrator\Downloads\splunkclouduf.spl"
splunk.exe install app "C:\Users\Administrator\Downloads\splunkclouduf.spl"
splunk.exe restart
splunk.exe stop
history
doskey /history

c:\Program Files\SplunkUniversalForwarder\bin>
```

The Windows taskbar at the bottom shows the Start button, a search bar with the text "Type here to search", and several application icons including File Explorer, Microsoft Edge, and Google Chrome. The system tray on the right indicates the time is 8:14 PM on 3/24/2025, with a notification icon showing 2 alerts.

Author

Mamurhomu Adugbo

London, ON

© 2025 Mamurhomu Adugbo. All rights reserved.