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

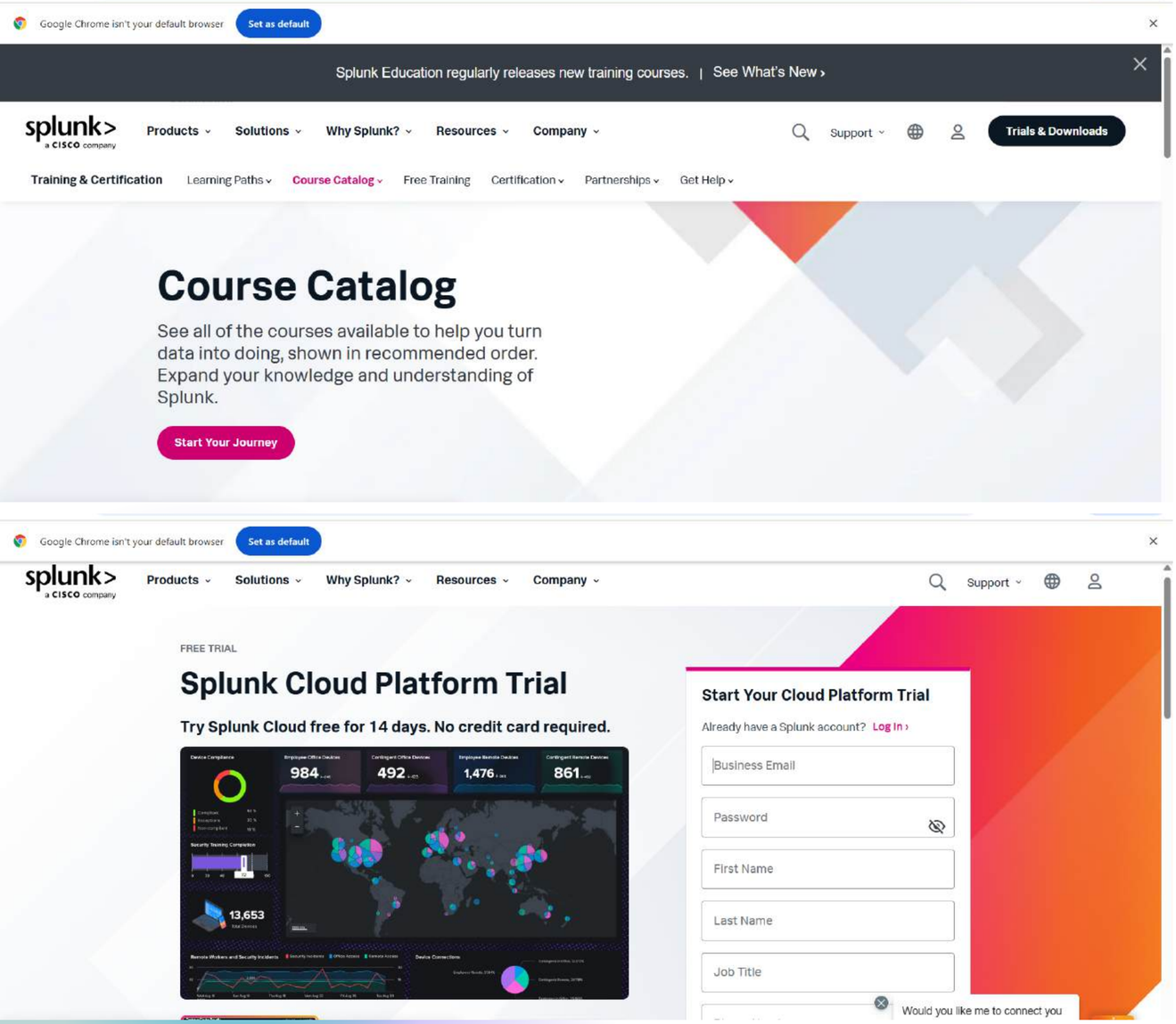
Splunk Cloud (Free Trial)

Splunk Universal Forwarder

Canva (for documentation and presentation)

Windows Command Prompt (Admin)

Step-by-Step Setup



Step 1: Get a Splunk Cloud Instance

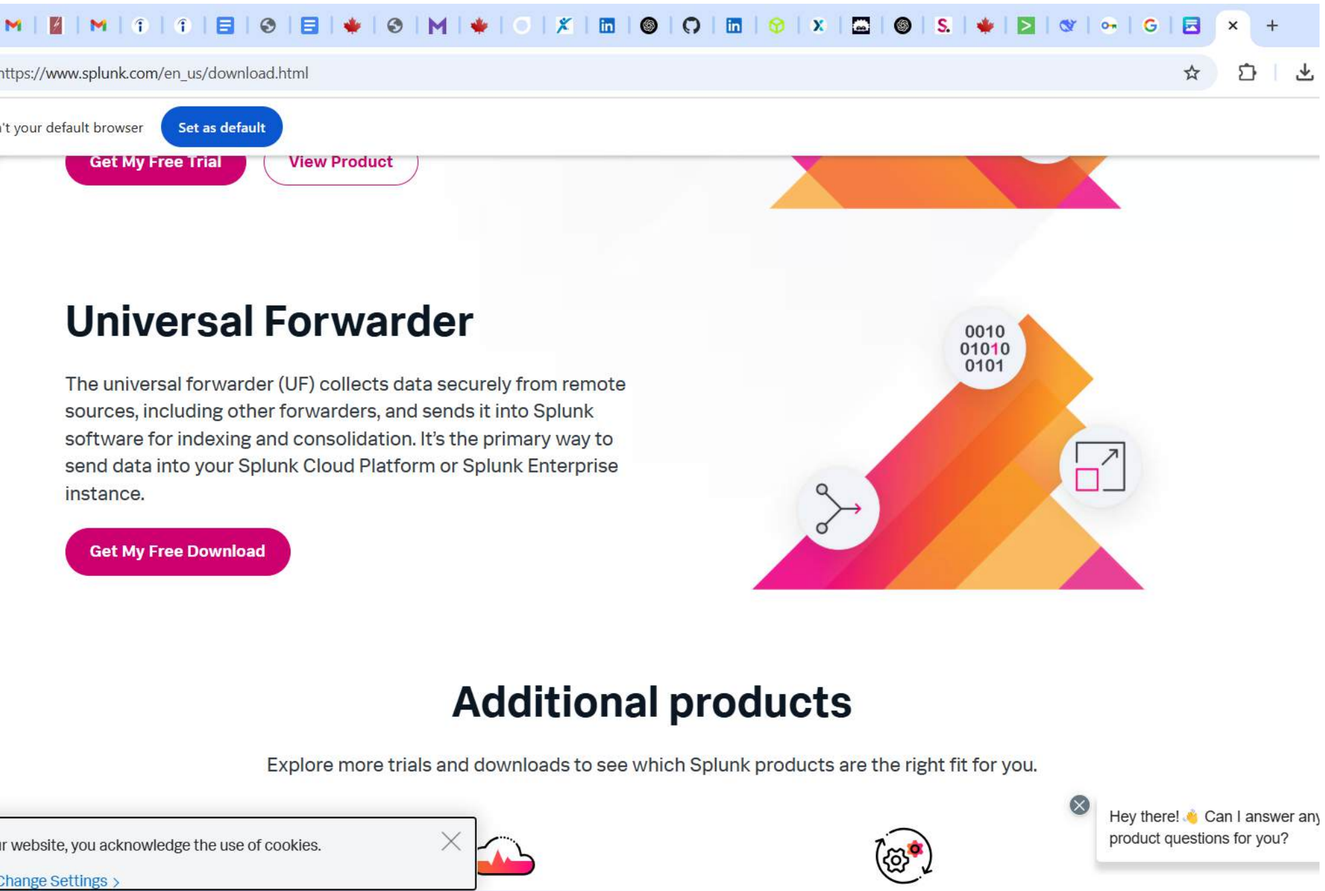
1. Go to: https://www.splunk.com/en_us/cloud.html

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

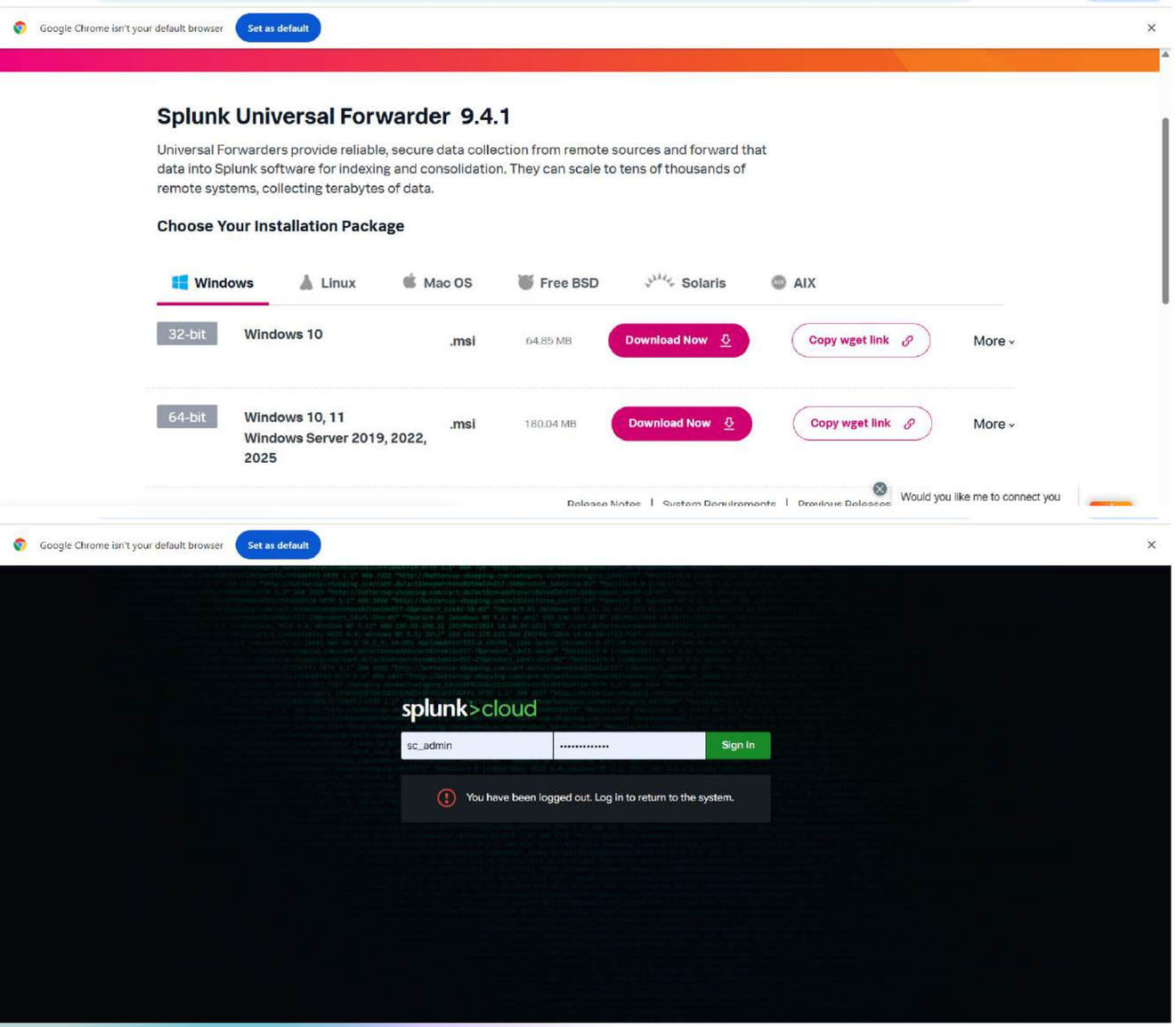


Step 2: Download Universal Forwarder Credential Package

1. From your Splunk Cloud dashboard, click the gear icon

2. Select Universal Forwarder

3. Click Download Universal Forwarder Credentials (.spl file)



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:

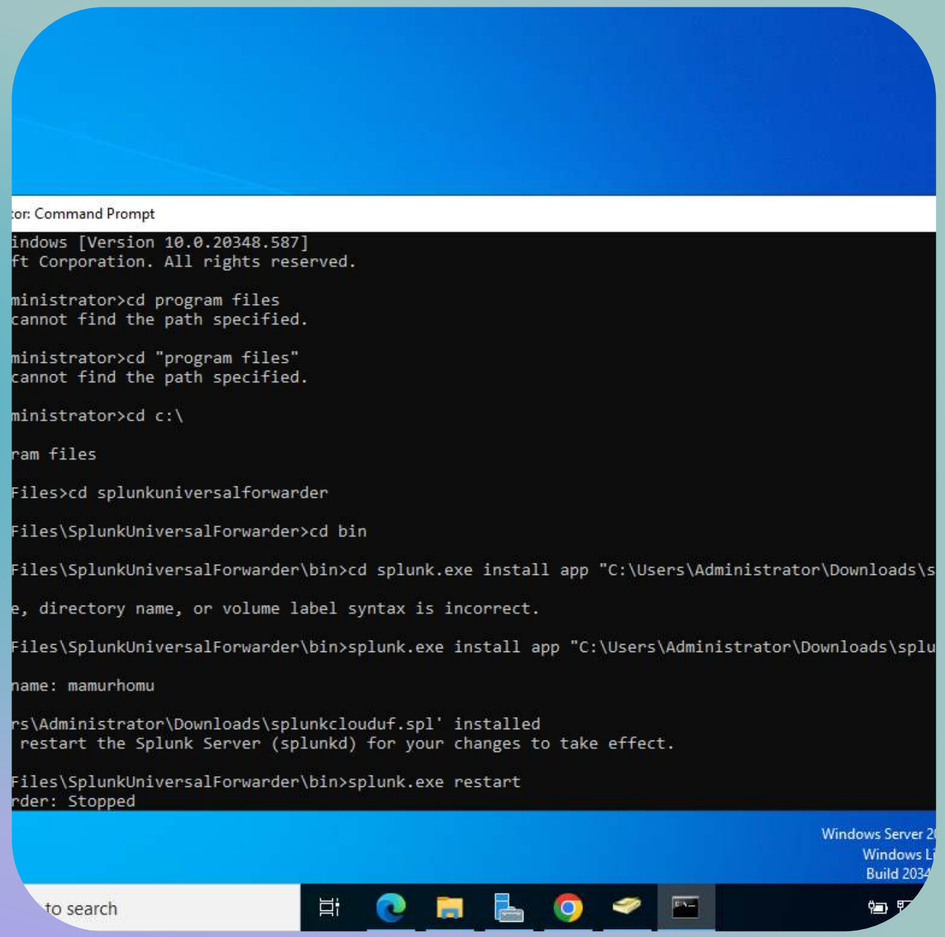
- Accept the license

- Select "Splunk Cloud Instance"

- Customize: run as Local System Account

- Manually enter your admin username & password

- Skip Deployment Server screen → Click Install

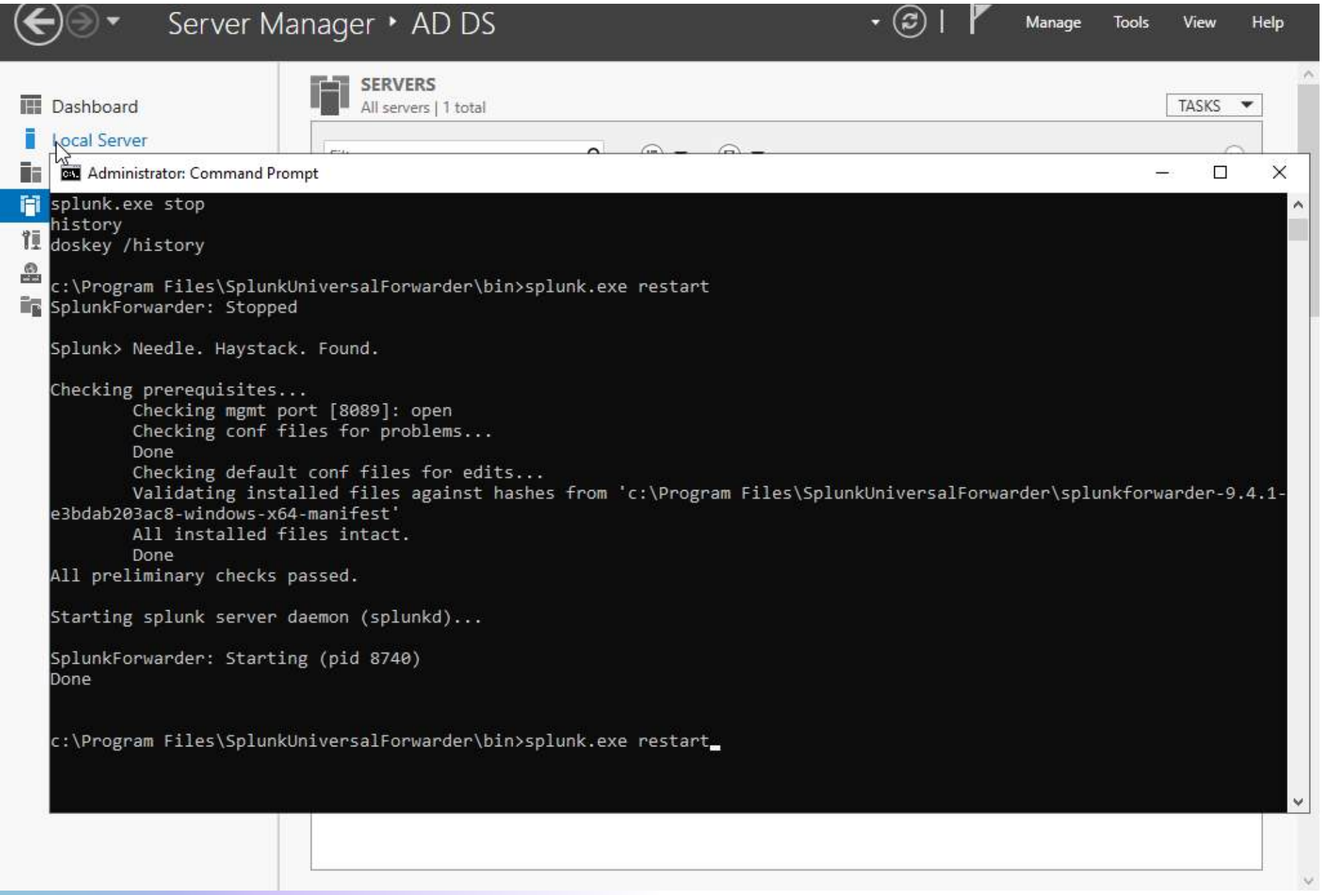


Step 4: Install the UF Credential Package in CMD

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"



Step 5: Restart the Splunk Forwarder

Run this in Command Prompt: splunk.exe restart

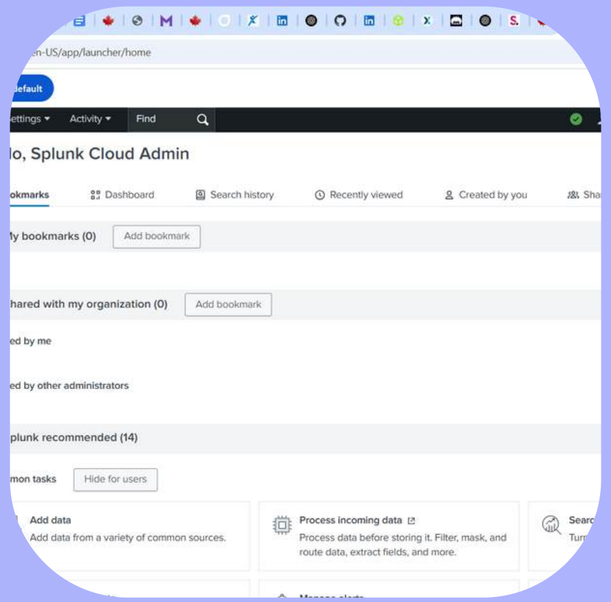
Step 6: Verify Connection

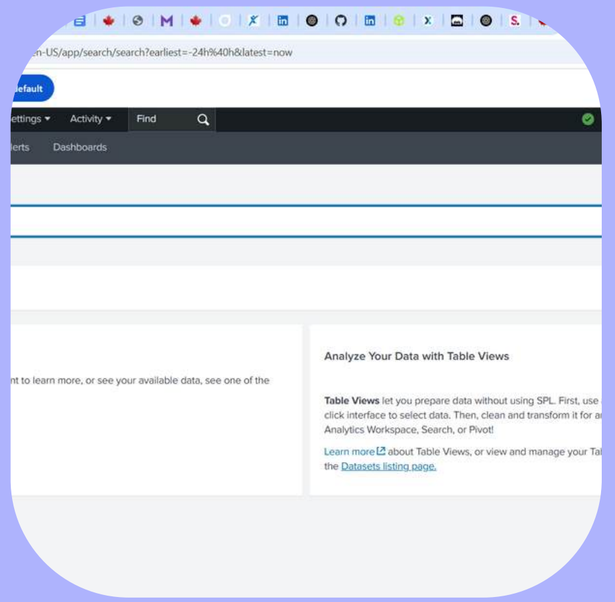
1. Return to Splunk Cloud

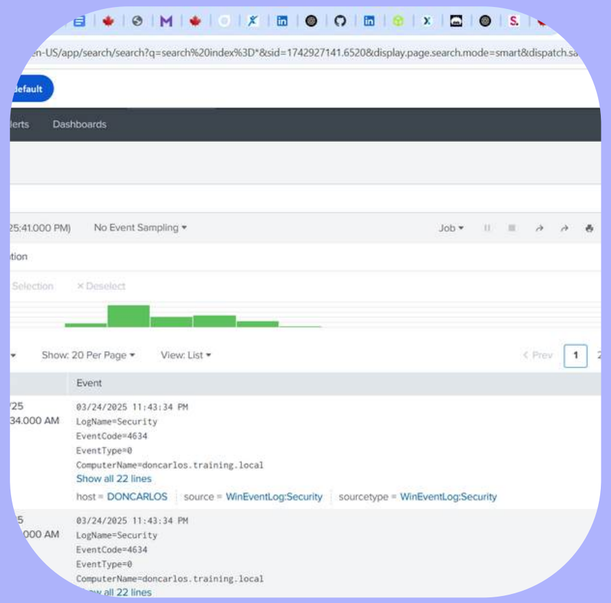
2. Click Search & Reporting

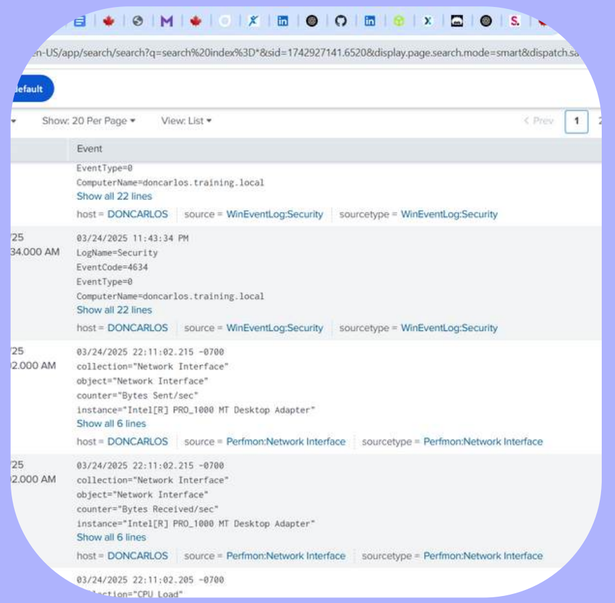
3. Search for: index=*4.

Confirm log data is being received



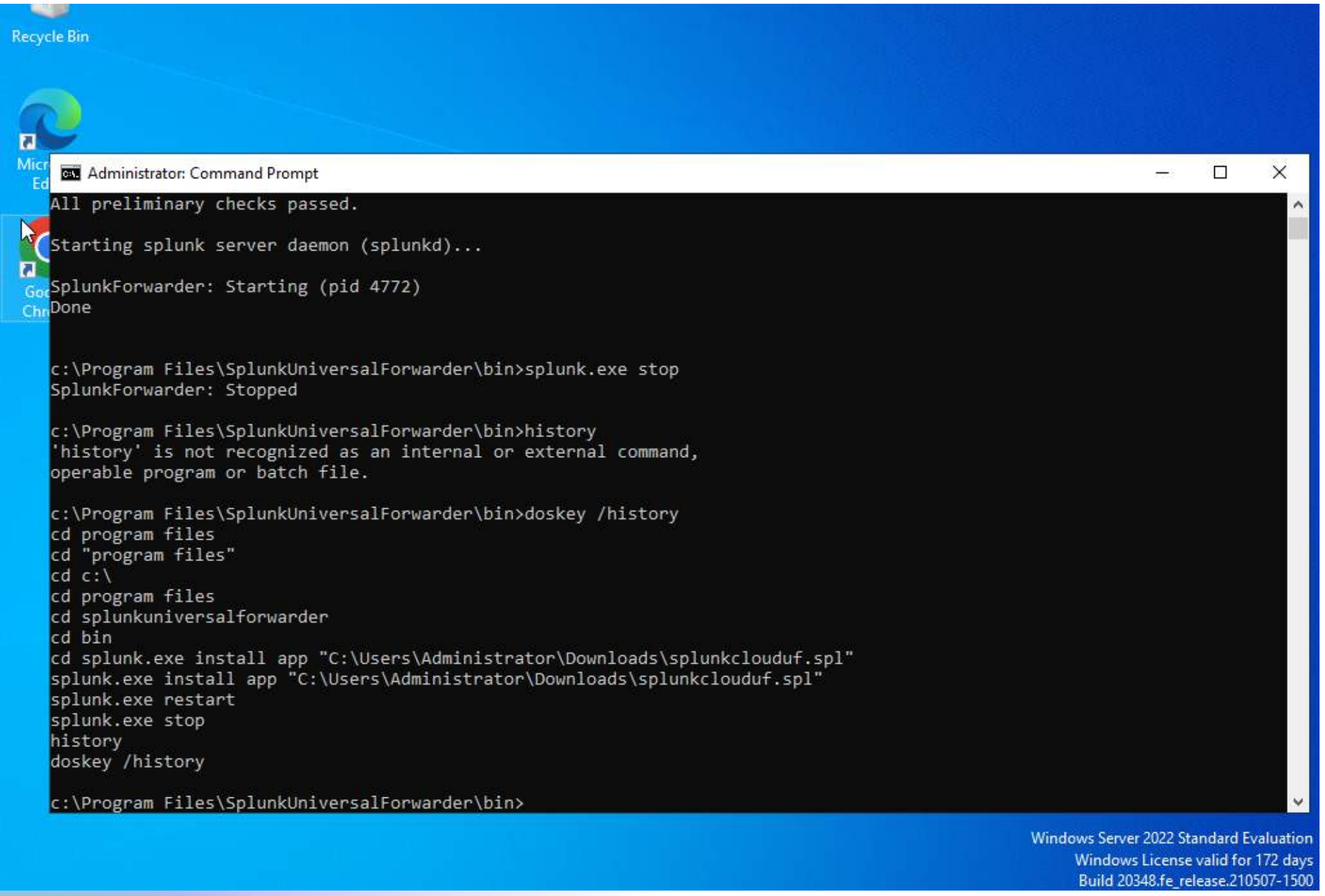






Skills Demonstrated

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

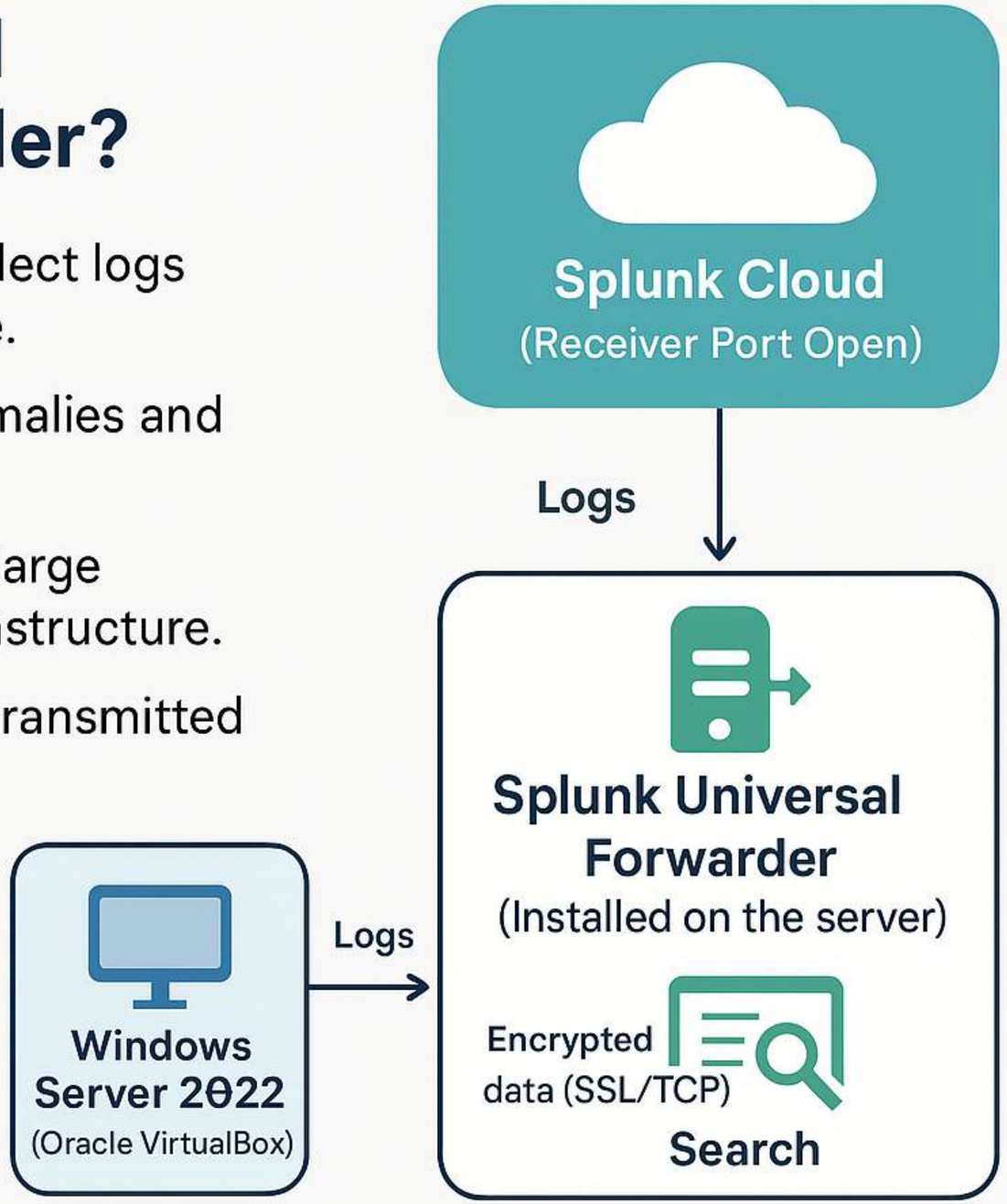


Screenshots

Screenshots

Why Use Splunk Cloud with Universal Forwarder?

- Centralized Log Management: Collect logs from multiple sources in one place.
- Real-Time Monitoring: Detect anomalies and threats instantly.
- Scalability: Splunk Cloud handles large volumes of data without local infrastructure.
- Security: Logs are encrypted and transmitted securely.
- Search & Correlation: Powerful query language (SPL) to analyze events.
- Dashboards & Alerts: Create visualizations and set real-time alerts for incidents



Author

Mamurhomu Adugbo

London, ON