

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**

**Canva (for
documentation and
presentation)**

**Splunk Cloud (Free
Trial)**

**Windows Command
Prompt (Admin)**

**Splunk Universal
Forwarder**

Step-by-Step Setup

The screenshot shows the Splunk website's course catalog section. At the top, there's a banner for new training courses. Below it, the navigation bar includes links for Products, Solutions, Why Splunk?, Resources, Company, Support, Trials & Downloads, and a search bar. The main content area features a large graphic with overlapping triangles in red, orange, and grey. A heading "Course Catalog" is prominently displayed. Below it, a text block says: "See all of the courses available to help you turn data into doing, shown in recommended order. Expand your knowledge and understanding of Splunk." A pink button labeled "Start Your Journey" is visible.

The screenshot shows the Splunk Cloud Platform trial sign-up process. It starts with a "FREE TRIAL" banner and the heading "Splunk Cloud Platform Trial". Below that, a sub-headline says "Try Splunk Cloud free for 14 days. No credit card required." To the left is a dashboard preview showing various metrics like device compliance, security incidents, and remote workers. On the right is a form titled "Start Your Cloud Platform Trial" with fields for Business Email, Password, First Name, Last Name, and Job Title. A "Log In" link is also present. At the bottom of the form, there's a question "Would you like me to connect you?" with a small checkbox and an "X" button.

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

The screenshot shows a web browser displaying the Splunk download page at https://www.splunk.com/en_us/download.html. The page features a large, colorful graphic of a triangle composed of orange, red, and yellow segments. On the left, there's a section titled "Universal Forwarder" with a brief description and two buttons: "Get My Free Trial" and "View Product". Below this is another section titled "Additional products" with a "Get My Free Download" button. At the bottom, there are two small pop-up boxes: one about cookie usage and another asking if they can answer product questions.

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

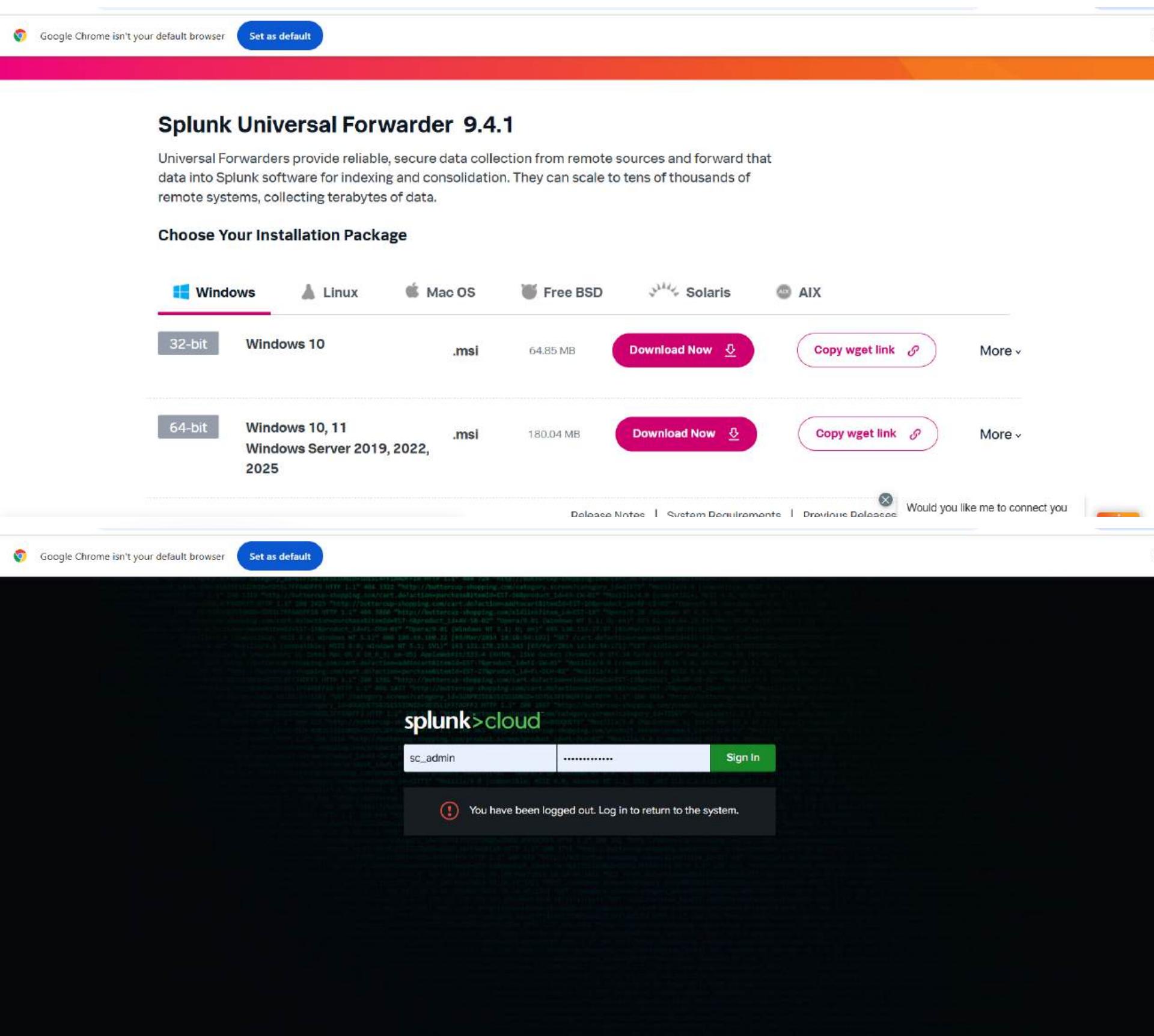
Additional products

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

Hey there! 🌟 Can I answer any product questions for you?

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:

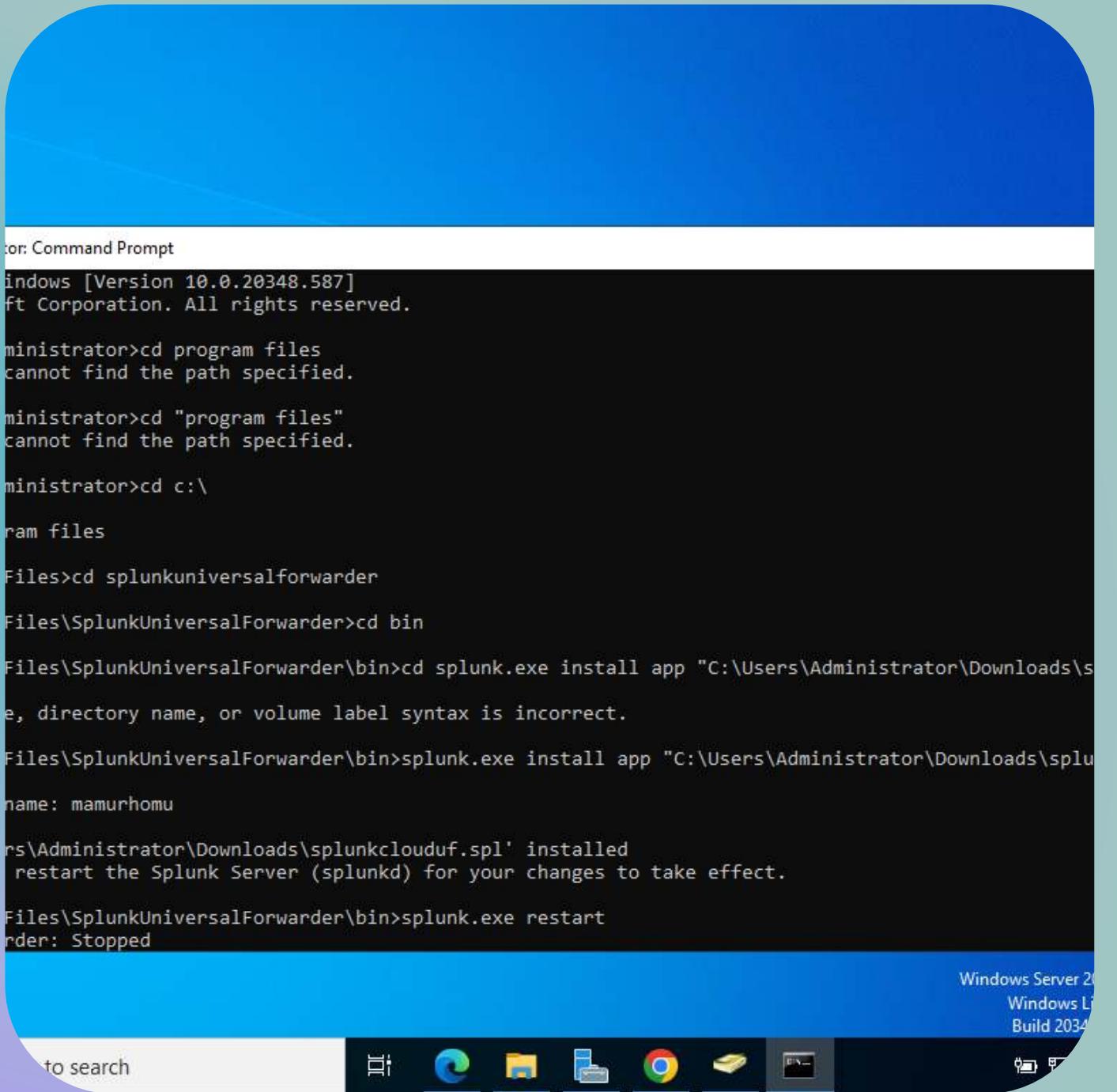
- Accept the license

- Select "Splunk Cloud Instance"

- Customize: run as Local System Account

- Manually enter your admin username & password

- Skip Deployment Server screen → Click Install



```
Administrator: Command Prompt
Windows [Version 10.0.20348.587]
Copyright © 2022 Microsoft Corporation. All rights reserved.

Administrator>cd program files
cannot find the path specified.

Administrator>cd "program files"
cannot find the path specified.

Administrator>cd c:\

ram files

Files>cd splunkuniversalforwarder

Files\SplunkUniversalForwarder>cd bin

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

Files\SplunkUniversalForwarder\bin>splunk.exe install app "C:\Users\Administrator\Downloads\splunkclouduf.spl"
name: mamurhomu

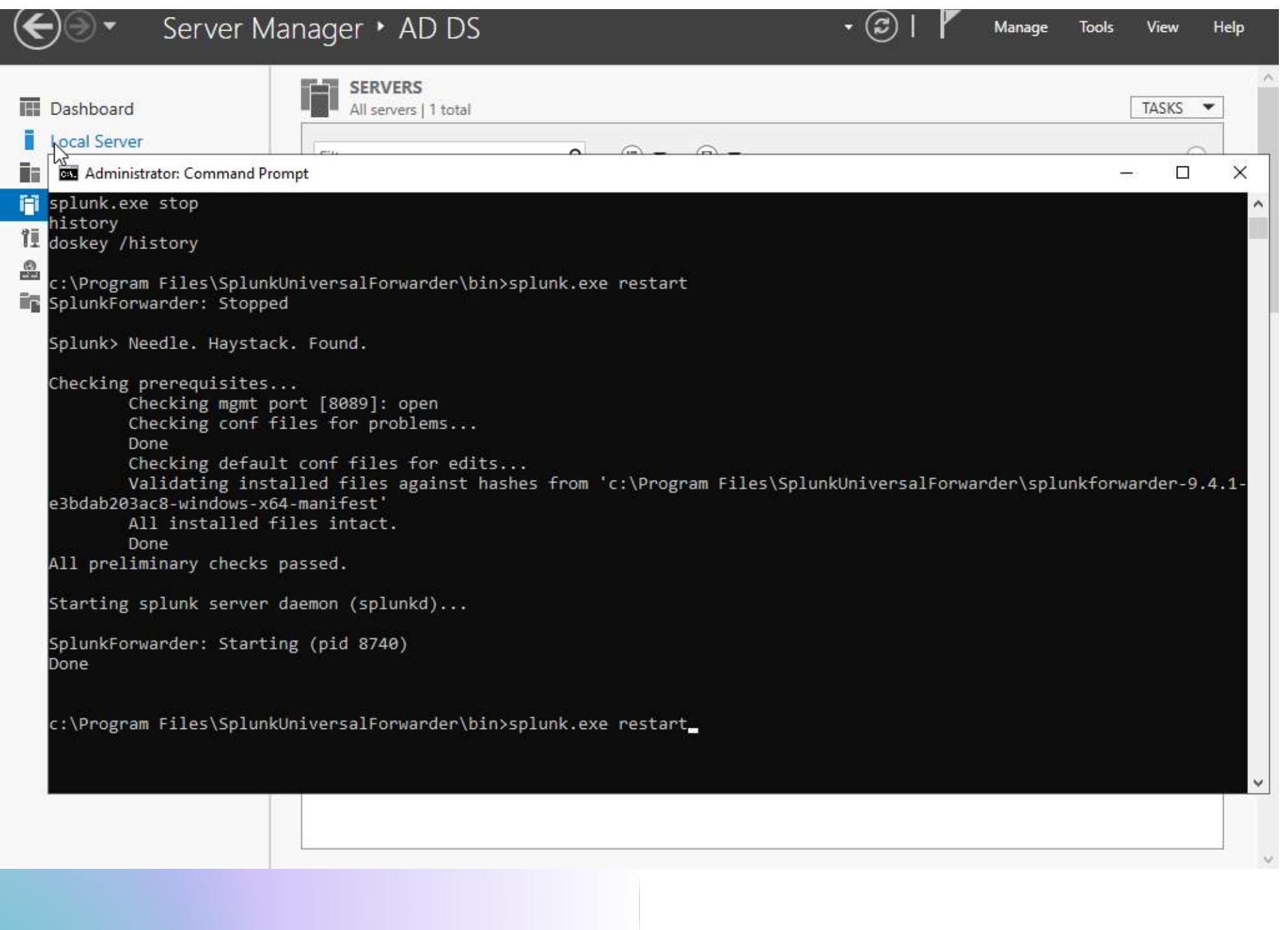
rs\Administrator\Downloads\splunkclouduf.spl' installed
restart the Splunk Server (splunkd) for your changes to take effect.

Files\SplunkUniversalForwarder\bin>splunk.exe restart
order: Stopped

Windows Server 2022
Windows Lineage
Build 20348
```

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"



The screenshot shows the Windows Server Manager interface with the title bar "Server Manager ▸ AD DS". In the center, there's a "COMMAND PROMPT" window titled "Administrator: Command Prompt". The command history and output are as follows:

```
splunk.exe stop
history
doskey /history
c:\Program Files\SplunkUniversalForwarder\bin>splunk.exe restart
SplunkForwarder: Stopped

Splunk> Needle. Haystack. Found.

Checking prerequisites...
  Checking mgmt port [8089]: open
  Checking conf files for problems...
    Done
  Checking default conf files for edits...
  Validating installed files against hashes from 'c:\Program Files\SplunkUniversalForwarder\splunkforwarder-9.4.1-e3bdab203ac8-windows-x64-manifest'
    All installed files intact.
    Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...

SplunkForwarder: Starting (pid 8740)
Done

c:\Program Files\SplunkUniversalForwarder\bin>splunk.exe restart
```

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

The screenshot shows the Splunk Cloud Admin interface. At the top, there's a navigation bar with links for 'Settings', 'Activity', 'Find', and a search bar. Below the navigation is a section titled 'My Bookmarks' with three categories: 'Bookmarks (0)', 'Shared with my organization (0)', and 'Splunk recommended (14)'. Further down are sections for 'Common tasks' and 'Add data' (with a sub-section for 'Process incoming data'). On the right side, there's a sidebar with a 'Table Views' section containing text about preparing data without SPL and links to learn more or view datasets.

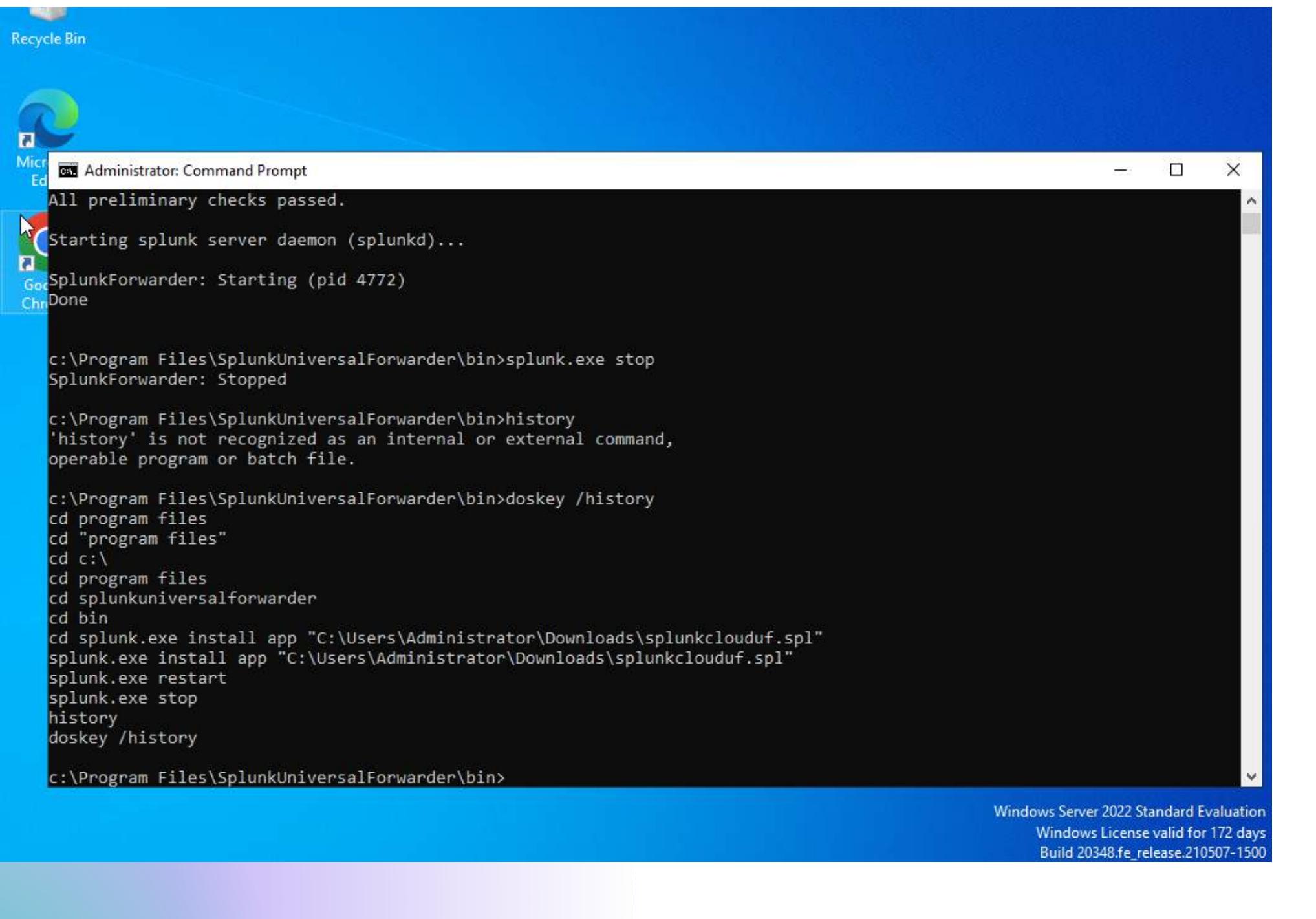
The screenshot shows the Splunk search results page. The URL in the address bar is 'https://en-US/app/search/search?q=search%20index%3D*&sid=1742927141.6520&display.page=search.mode=smart&dispatch.sa'. The interface includes a search bar at the top, followed by a 'Jobs' section with a histogram and a 'Selection' dropdown. Below this is a table of search results. The table has columns for 'Time', 'Event', and 'Details'. The first few rows show log entries from 'DONCARLOS' host, including security events and network interface statistics. The table also includes pagination controls like 'Show: 20 Per Page' and 'View: List'.

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



A screenshot of a Windows Server 2022 Standard Evaluation desktop. A Command Prompt window titled "Administrator: Command Prompt" is open, showing the following command history:

```
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>
```

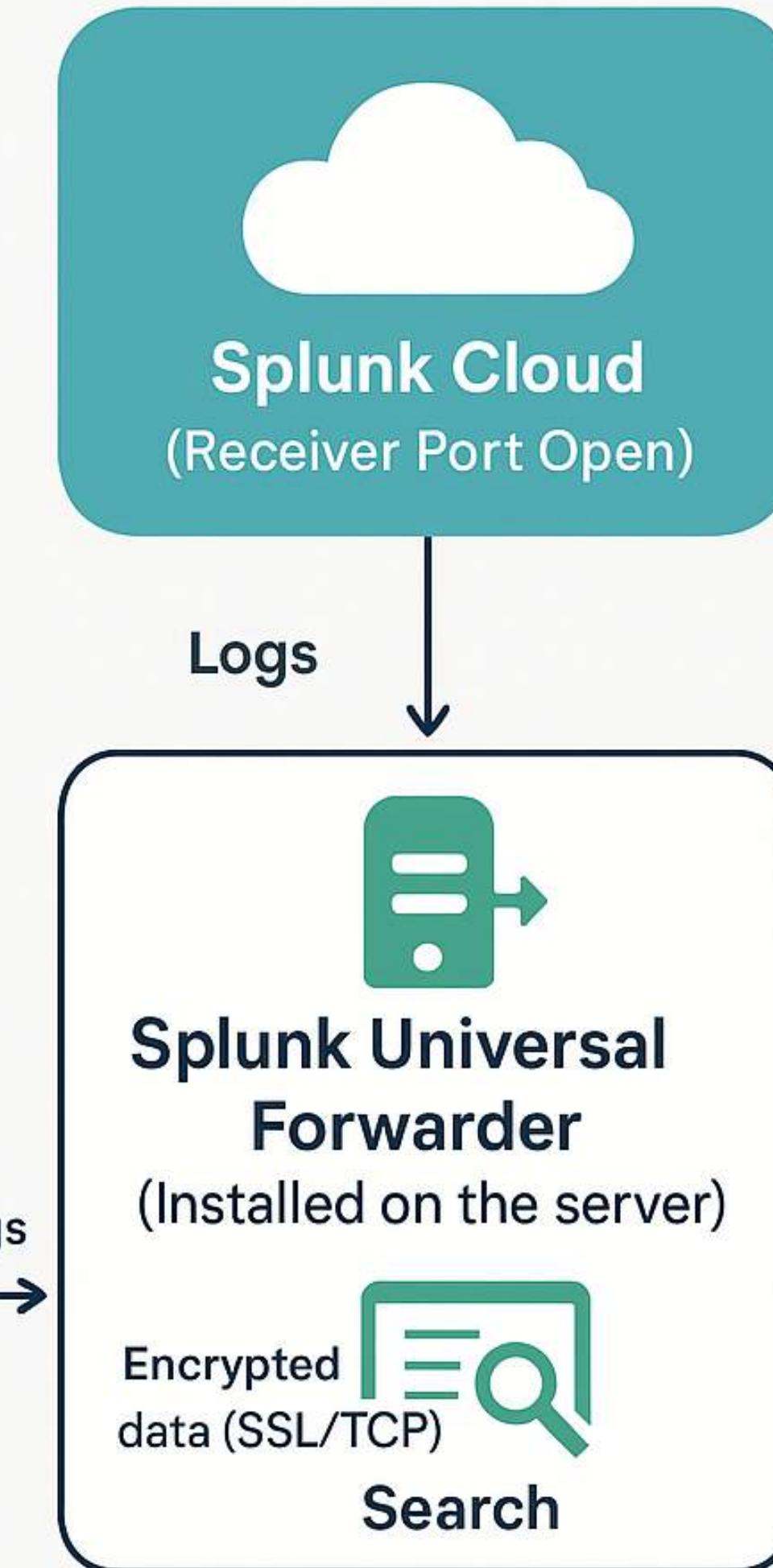
The taskbar at the bottom shows icons for File Explorer, Task View, Start, and a search bar. The status bar at the bottom right indicates "Windows Server 2022 Standard Evaluation", "Windows License valid for 172 days", and "Build 20348.fe_release.210507-1500".

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



Windows Server 2022
(Oracle VirtualBox)



Author

Mamurhomu Adugbo

London, ON

© 2025 Mamurhomu Adugbo. All rights reserved.