✅ STEP-BY-STEP: VALIDATE SPLUNK UNIVERSAL FORWARDER COMPATIBILITY

✅ Step 1: Check Official Compatibility

Start by checking the official Splunk documentation:

- 📘 **Splunk Supported Platforms (Universal Forwarder):**
  https://docs.splunk.com/Documentation/Forwarder/latest/Forwarder/SupportedPlatforms

Make sure:

- OS is **listed** (Windows Server 2019 and RHEL 8 are supported ✅)
- Your system architecture (64-bit) is supported
- You meet system requirements for CPU, RAM, and storage

🖥️ Step 2: Validate Windows Server 2019 Compatibility

2.1 Run System Checks

Open PowerShell as Admin:

powershell
CopyEdit
```
systeminfo
```

Look for:

- OS: Windows Server 2019
- Architecture: 64-bit (x64-based PC)
- Memory: ≥ 1 GB free

2.2 Firewall & Network

- Ensure port **9997 (TCP)** is open (used by Splunk UF to send data)
- Allow outbound access to Splunk Indexer or cloud instance

2.3 Install Dependencies

Usually, no extra dependencies for Windows. But make sure:

- PowerShell is available
- Windows Event Logs are accessible (for log collection)

🐧 Step 3: Validate RHEL 8 Compatibility

3.1 Check OS and Kernel

bash
CopyEdit

```
cat /etc/redhat-release
uname -r
```

Look for:

- RHEL 8.x
- Kernel version supported by Splunk (generally ok unless heavily customized)

3.2 Required Packages

Check for `tar`, `wget`, `systemctl`, and optionally `firewalld`

bash
CopyEdit

```
sudo yum install wget tar
```

3.3 Firewall & SELinux

- Open port 9997 in firewall:

bash
CopyEdit
```
sudo firewall-cmd --permanent --add-port=9997/tcp
sudo firewall-cmd --reload
```

- Set SELinux to permissive (or configure policies):

bash
CopyEdit
```
sudo setenforce 0
```

☁️ Step 4: Hybrid Cloud/On-Prem Environments

This means Splunk UF may run:

- On **cloud servers** (e.g., AWS EC2, Azure VMs)
- On **on-prem physical/virtual machines**

4.1 Cloud VMs (AWS/Azure)

- Ensure outbound connectivity to your Splunk indexer or HEC endpoint
- Check for any network security group/firewall restrictions

4.2 Check for Log Accessibility

- Windows: Event Viewer logs
- Linux: `/var/log/secure`, `/var/log/messages`, custom logs

🧪 Step 5: Test Deployment Compatibility

Now install Splunk UF (test install, no config yet):

🪟 **Windows:**

1. Download the UF installer (.msi) from:
   https://www.splunk.com/en_us/download/universal-forwarder.html

2. Run:

powershell
CopyEdit
```
msiexec /i splunkforwarder-x64.msi LAUNCHSPLUNK=1 AGREETOLICENSE=Yes
/quiet
```

🐧 **RHEL:**
bash
CopyEdit
```
cd /opt
wget -O splunkforwarder.tgz
"https://download.splunk.com/products/universalforwarder/releases/X.X.
X/linux/splunkforwarder-X.X.X-Linux-x86_64.tgz"
tar -xvzf splunkforwarder.tgz
cd splunkforwarder/bin
./splunk start --accept-license
```

Replace `X.X.X` with the correct version number.

✅ Step 6: Confirm Successful Start

Run:

bash
CopyEdit
```
./splunk status
```

or check the Windows Service:

powershell

CopyEdit

```
Get-Service splunkforwarder
```

If it's **running**, your system is compatible!

🧾 Step 7: Document the Compatibility Validation

For each environment:

- OS & version
- UF install status
- Logs path availability
- Port/firewall status
- Network connectivity test (e.g., `telnet your.splunk.server 9997`)