Splunk SIEM & Active Directory Lab

---

1. Overview

Objective: This is a virtualized Home Lab environment consisting of an Active Directory Domain Controller, a Windows Client machine, and a Splunk Enterprise Server. The goal is to simulate an attack scenario where successful authentication triggers telemetry sent to Splunk, which subsequently triggers a Shuffle playbook and Slack notification.

Architecture:

- **Cloud Provider:** Vultr Cloud Service.
- **Network:** Virtual Private Cloud (VPC) for internal communication3.
- **Components:**

  Domain Controller: Windows Server 2022 (Heeruzen-ADDC01)

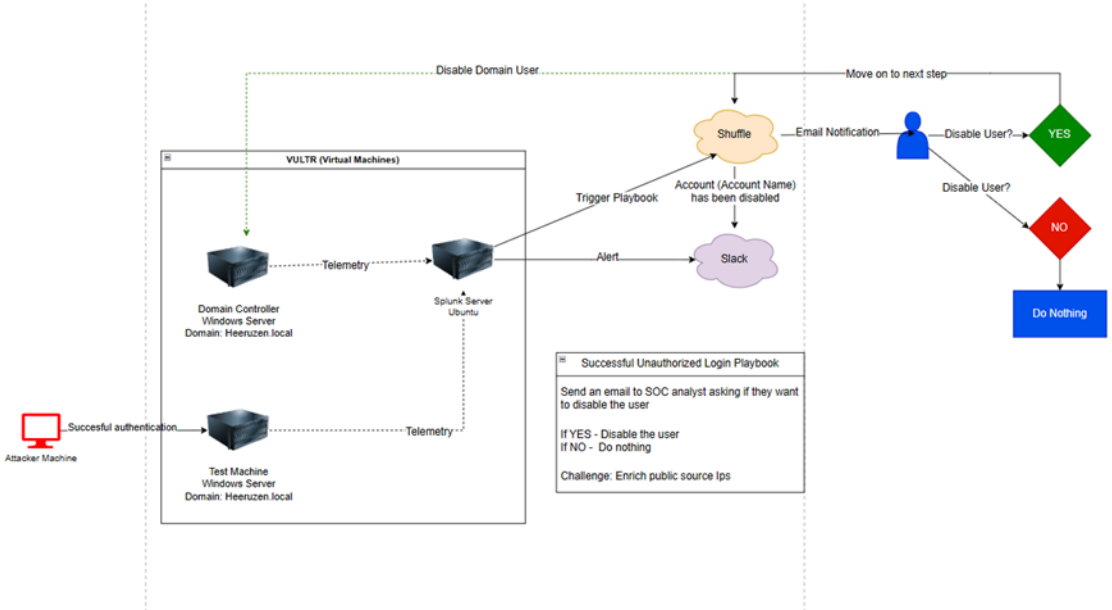
  Splunk Server: Ubuntu Server (Heeruzen-Splunk)

  Test Machine: Windows Server 2022 (Heeruzen.local).

  Attacker Machine: Host Machine.

Workflow:

1. Attacker scans and authenticates to the Test Machine.
2. Telemetry is forwarded to the Splunk Server.
3. Splunk alerts trigger a Shuffle playbook.
4. Shuffle prompts a SOC analyst (via email) to disable the user.
5. If approved, Shuffle relays the command to the Domain Controller to disable the user and notifies Slack.



---

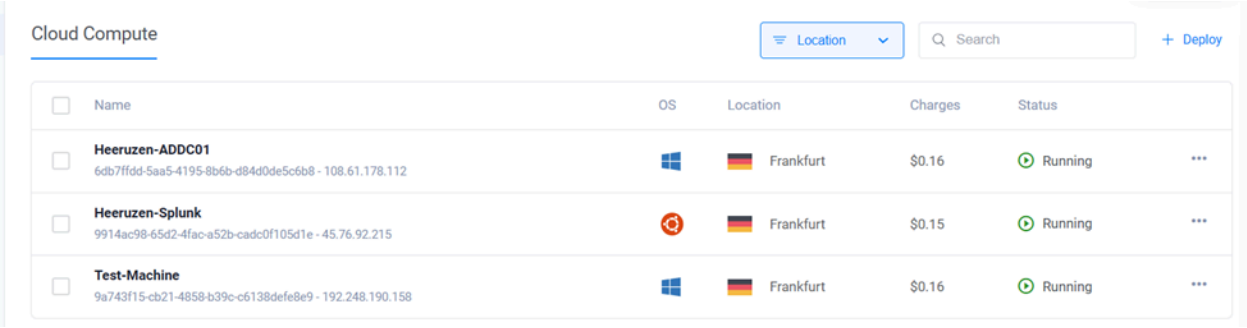
2. Infrastructure Setup (Vultr)

2.1 Virtual Machine Deployment

Three virtual machines were deployed in the Frankfurt location:

1. **Heeruzen-ADDC01** (Windows Server) - IP: 45.77.67.220.
2. **Heeruzen-Splunk** (Ubuntu) - IP: 45.76.92.215.

3. **Test-Machine** (Windows Server) - IP: 95.179.240.136.



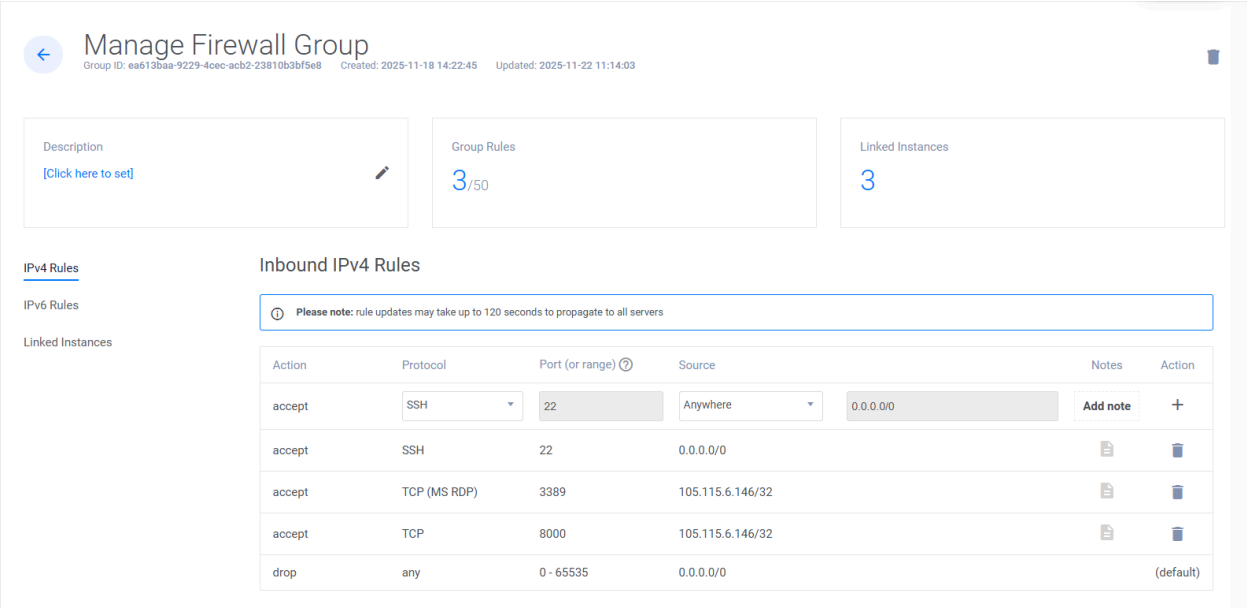
2.2 Network Configuration (VPC)

A VPC network (Heeruzen-local2) was created with the subnet `10.10.0.0/24` to allow private communication between the servers.

2.3 Firewall Configuration

Firewall rules were established to allow SSH (Port 22) and RDP (Port 3389) traffic.

Note: Public IPs are dynamic; firewall rules required updates whenever the administration IP changed.



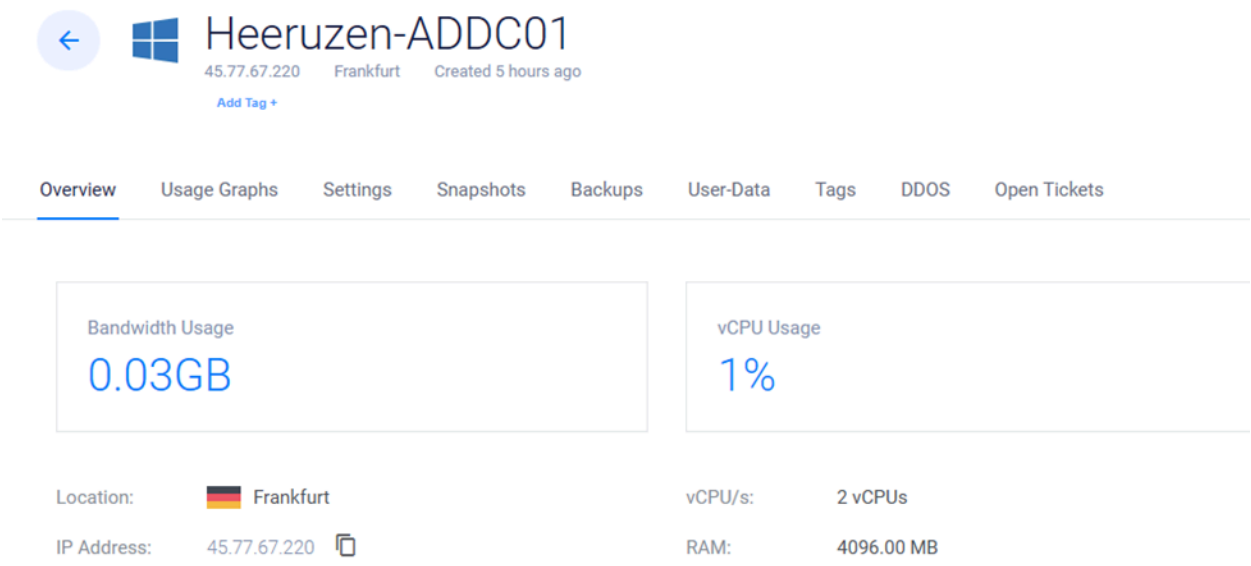
2.4 Interface Configuration & Connectivity Testing

Private IP addresses were assigned to the VPC interfaces:

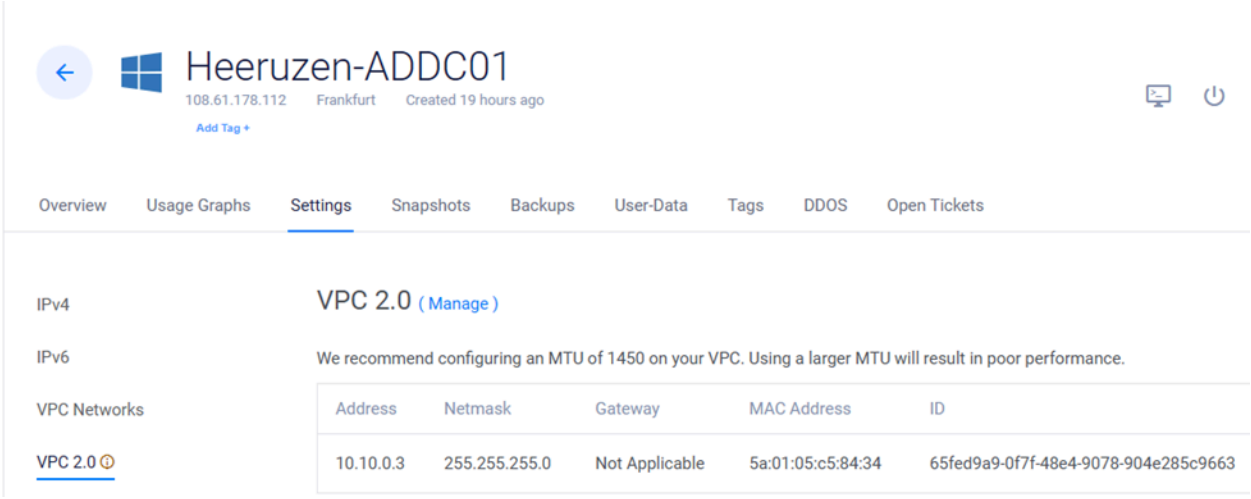
- **ADDC01:** 10.10.0.319.
- **Splunk Server:** 10.10.0.420.
- **Test Machine:** 10.10.0.521.

Connectivity was verified via ping tests between the machines.

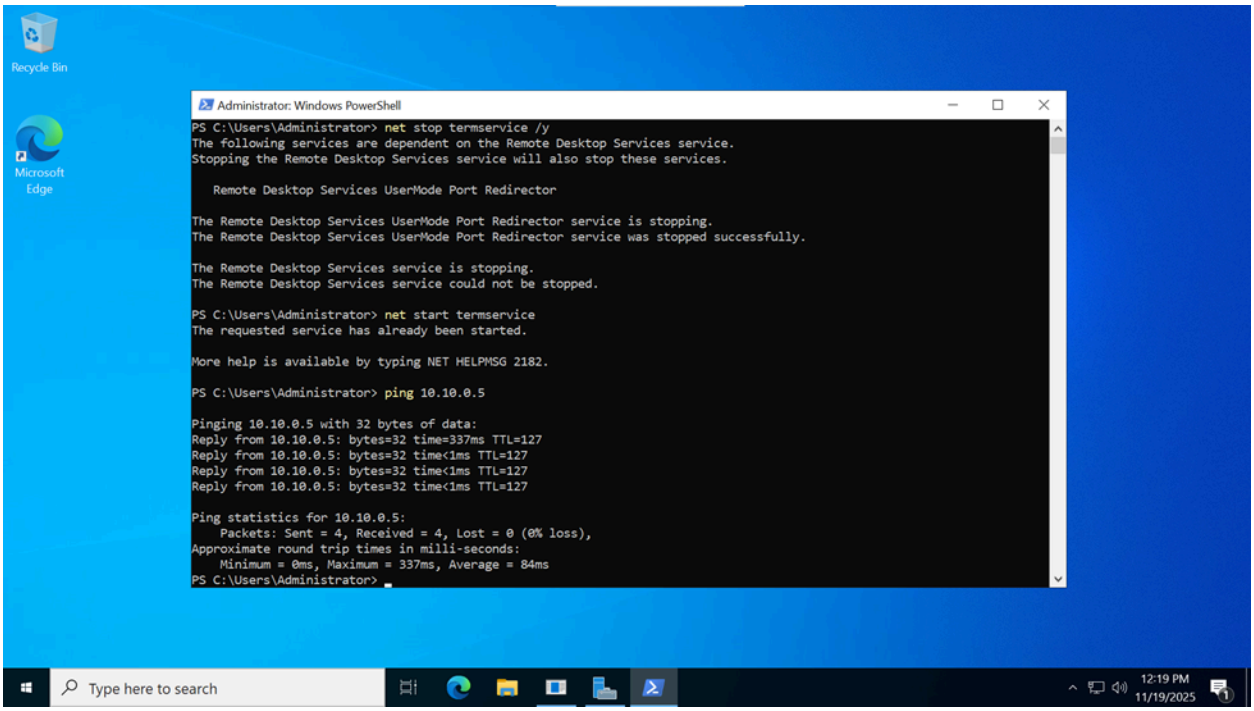
ADDC01 Overview/IP Settings



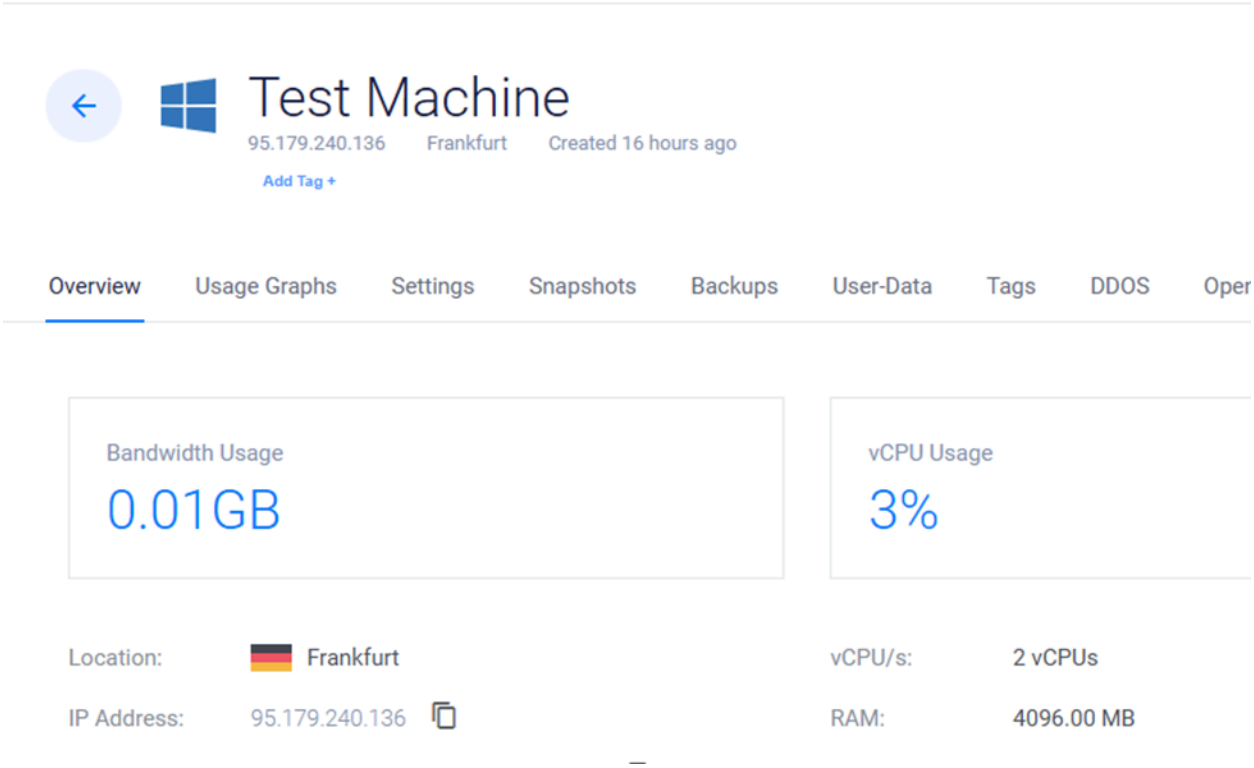
ADDC01 VPC Settings



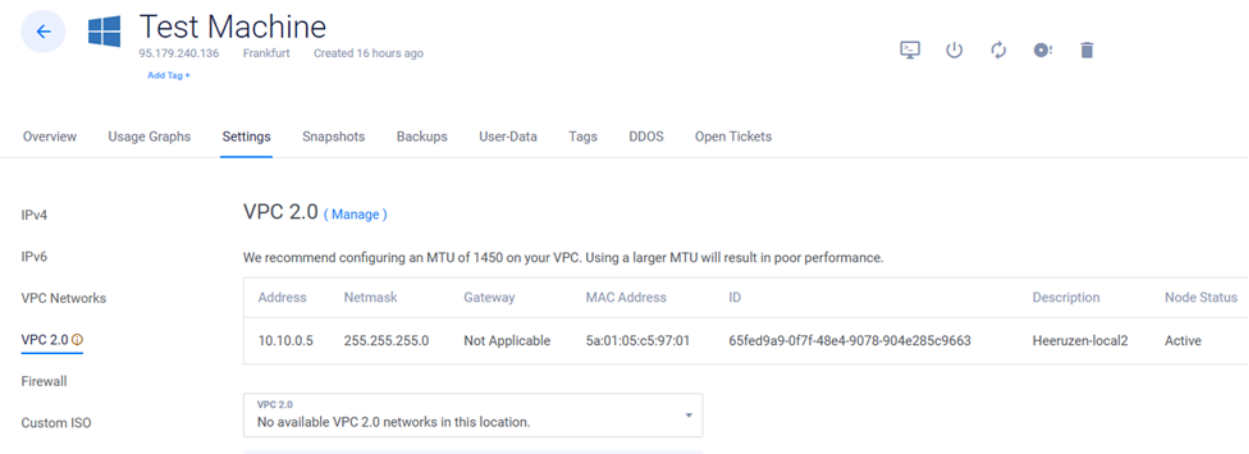
PowerShell Ping Test from ADDC01 to 10.10.0.5



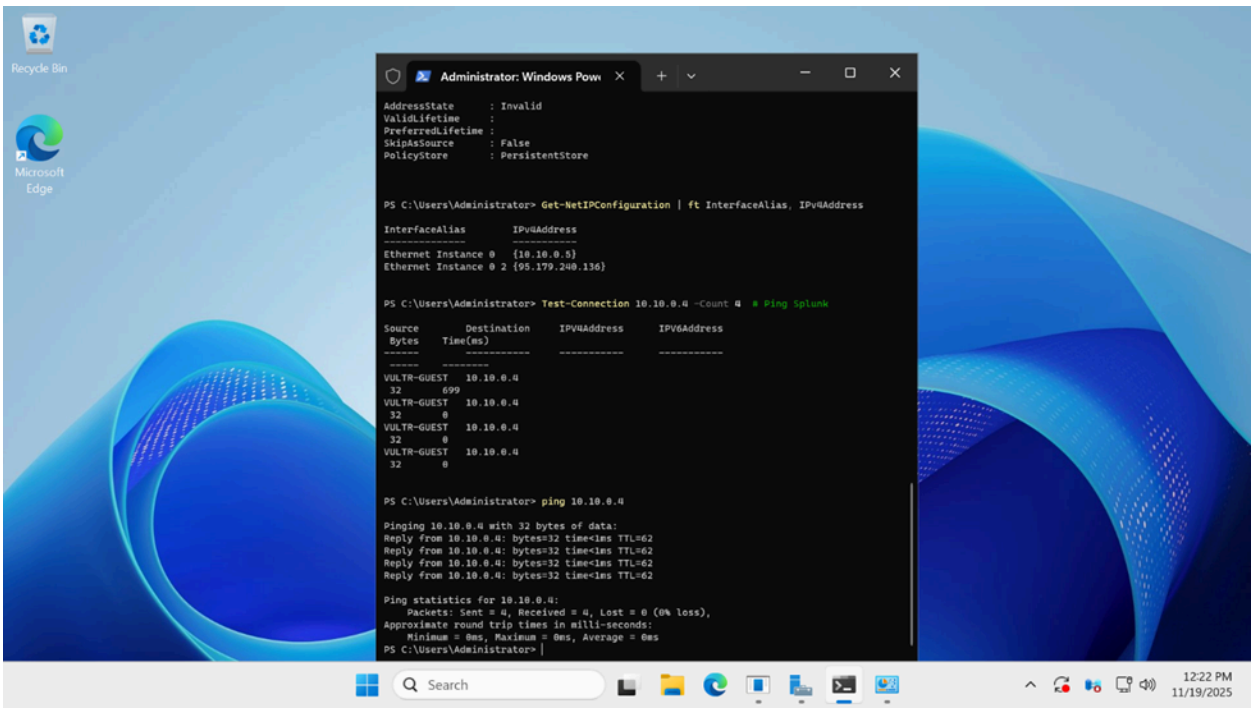
Test Machine Overview/IP Settings



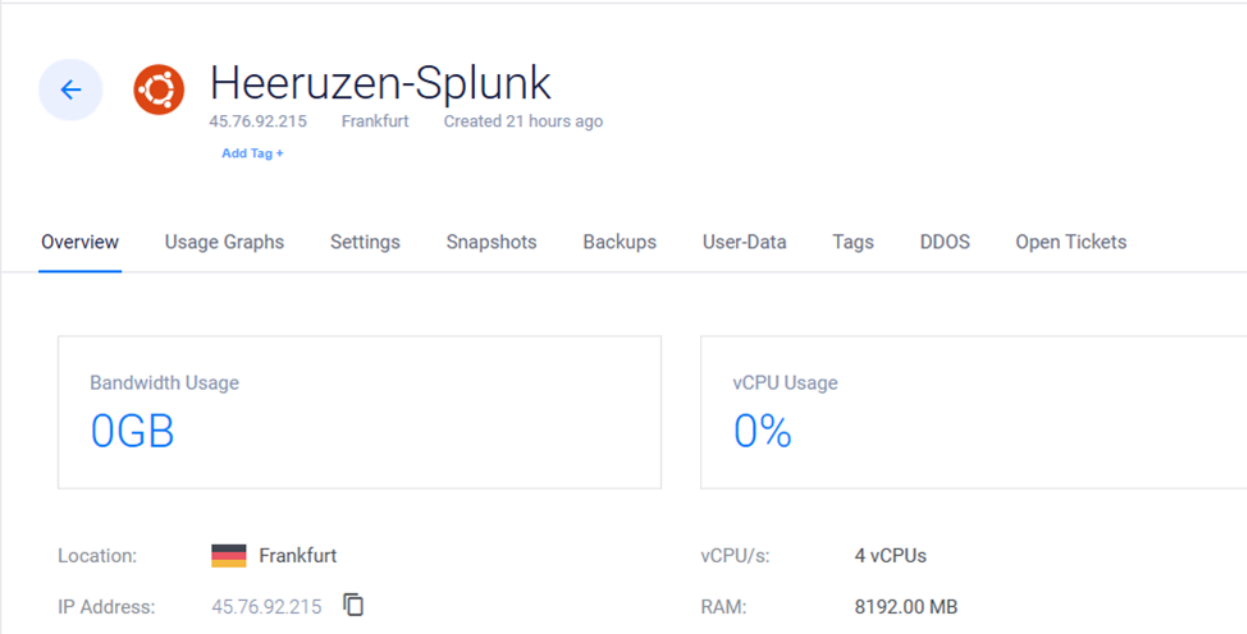
Test Machine VPC Settings



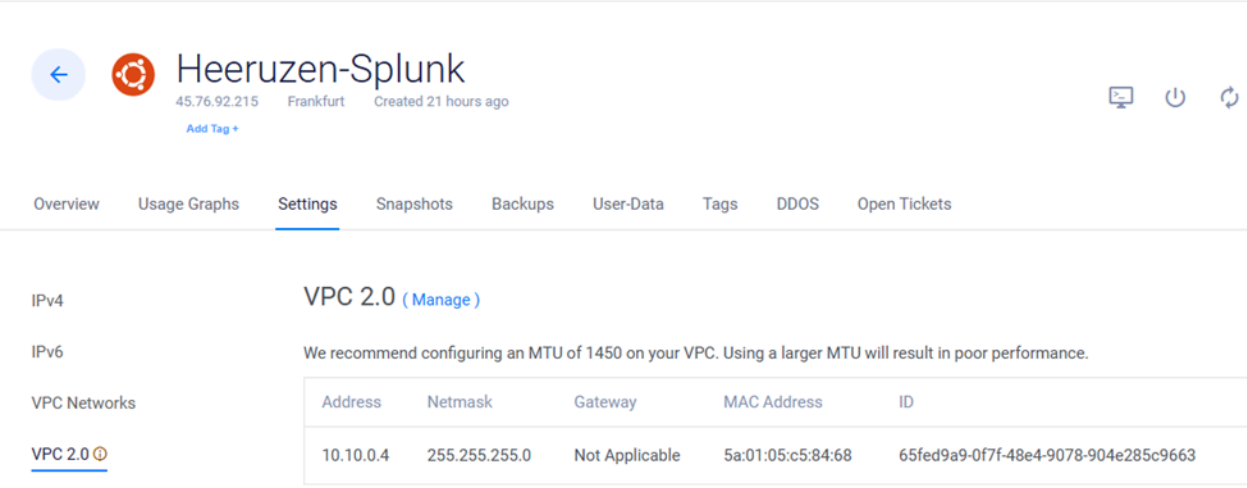
PowerShell Ping Test from Test Machine to Splunk



Splunk Server Overview/IP Settings



Splunk Server VPC Settings



Linux Ping Test from Splunk Server to 10.10.0.5

```
root@Heeruzen-Splunk:~# ping 10.10.0.5
PING 10.10.0.5 (10.10.0.5) 56(84) bytes of data.
64 bytes from 10.10.0.5: icmp_seq=1 ttl=126 time=0.643 ms
64 bytes from 10.10.0.5: icmp_seq=2 ttl=126 time=0.587 ms
64 bytes from 10.10.0.5: icmp_seq=3 ttl=126 time=0.572 ms
64 bytes from 10.10.0.5: icmp_seq=4 ttl=126 time=0.653 ms
64 bytes from 10.10.0.5: icmp_seq=5 ttl=126 time=0.674 ms
64 bytes from 10.10.0.5: icmp_seq=6 ttl=126 time=0.713 ms
^C
--- 10.10.0.5 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5152ms
rtt min/avg/max/mdev = 0.572/0.640/0.713/0.048 ms
```

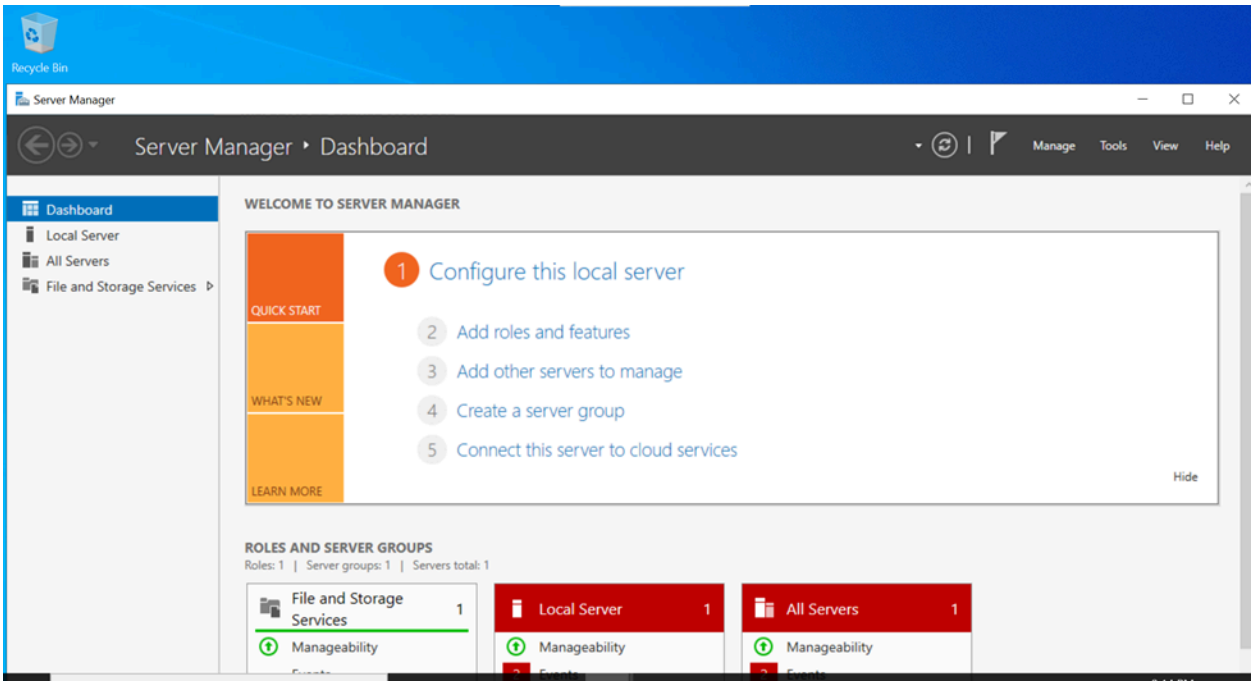
---

3. Active Directory Configuration

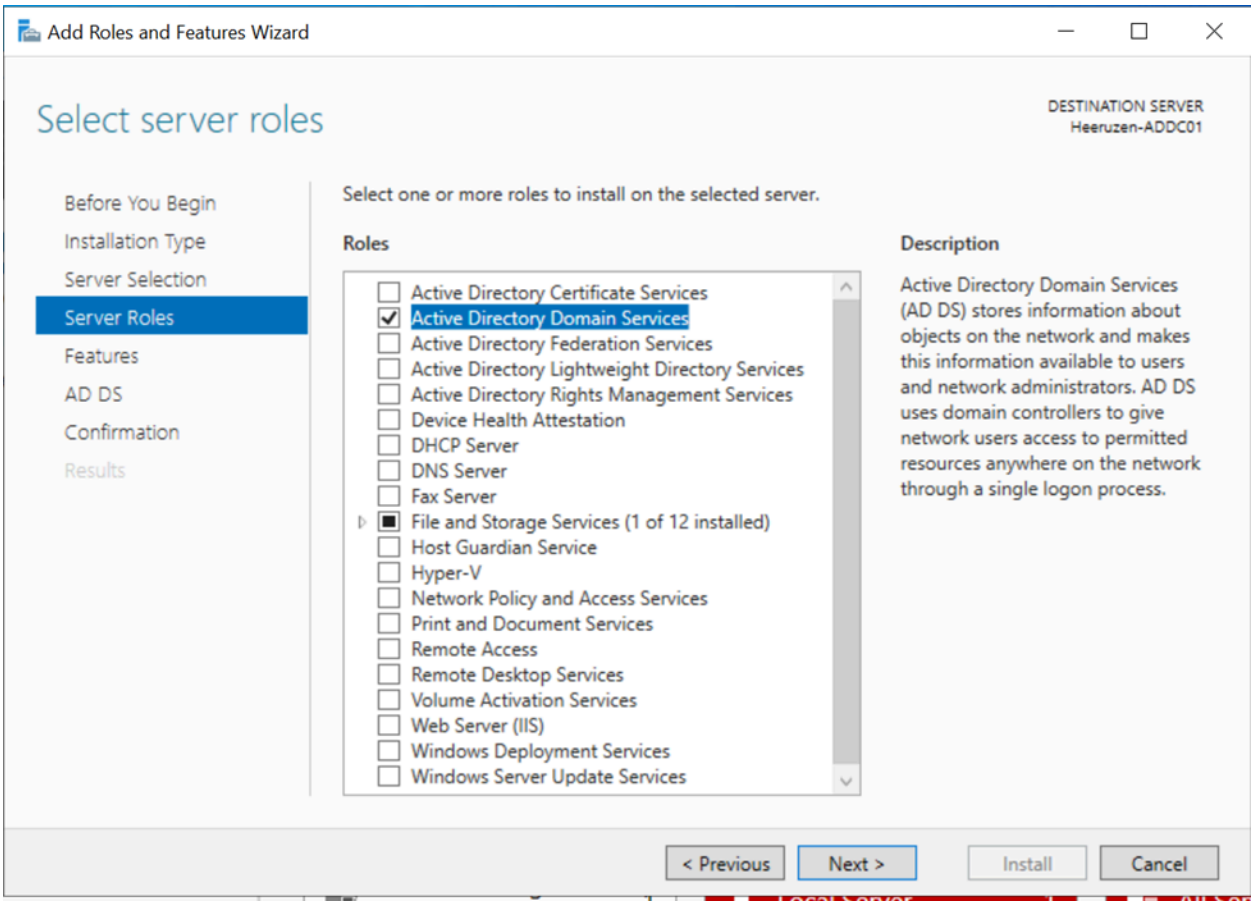
3.1 Domain Controller Promotion

On the `Heeruzen-ADDC01` server, the "Active Directory Domain Services" role was installed via Server Manager.

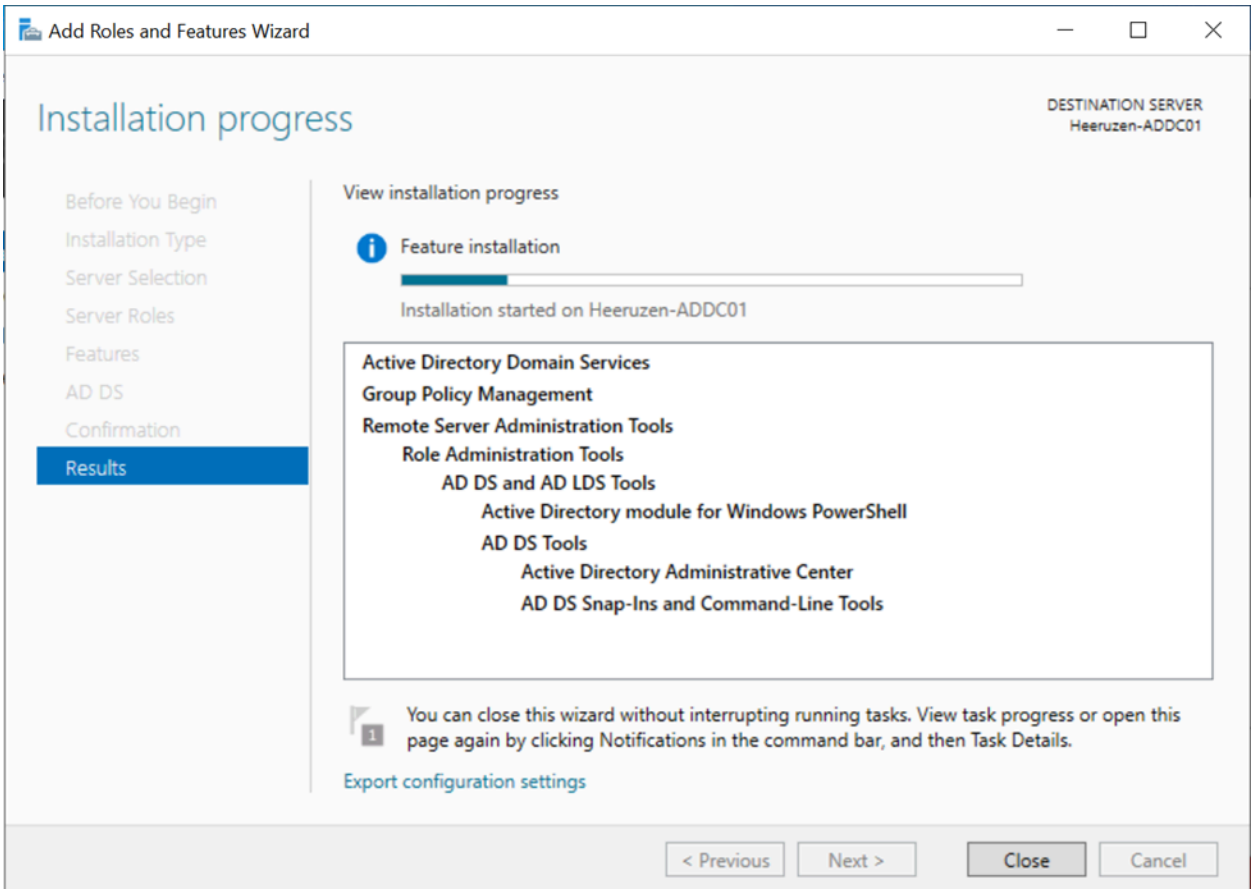
Server Manager Dashboard



Select Server Roles - AD DS Checked

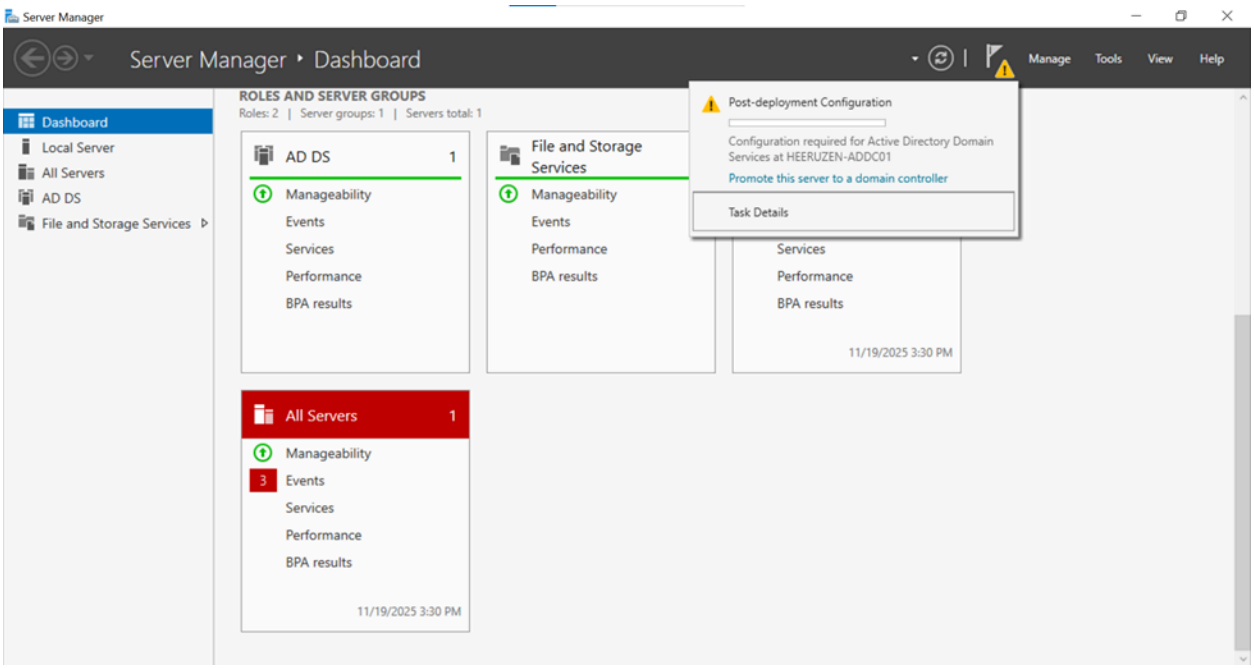


Installation Progress

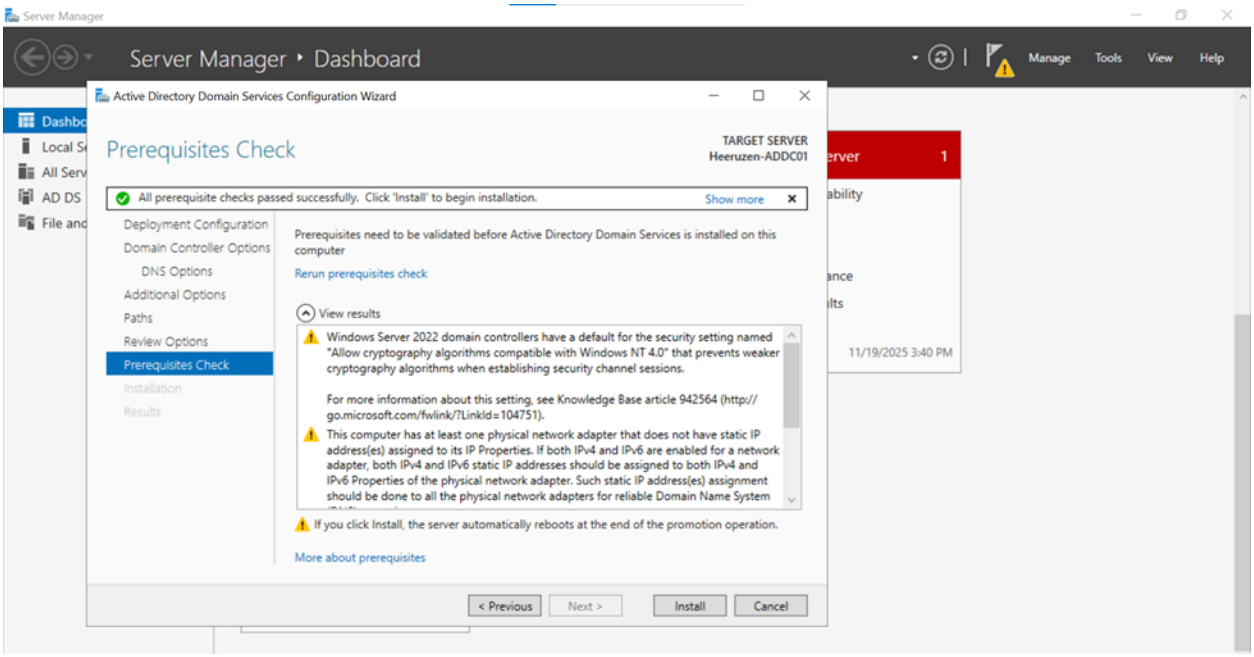


Following installation, the server was promoted to a Domain Controller, establishing the new forest `Heeruzen.local`

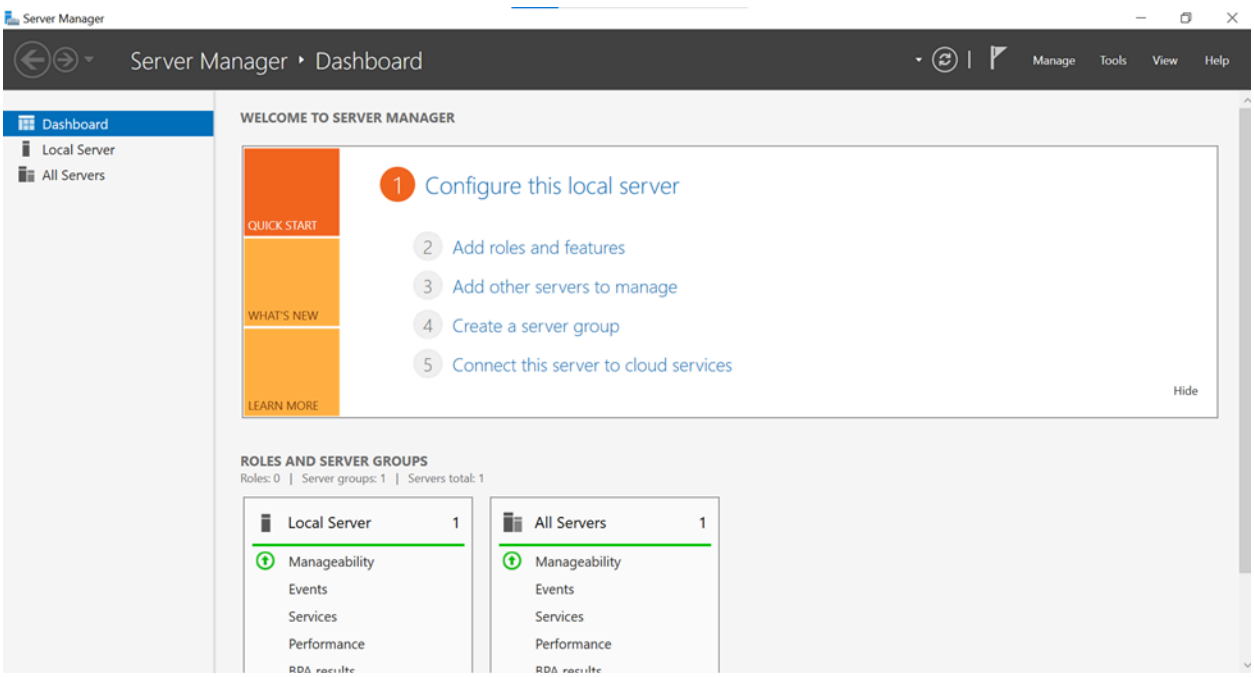
Post-deployment Configuration Notification



Prerequisites Check before Installation



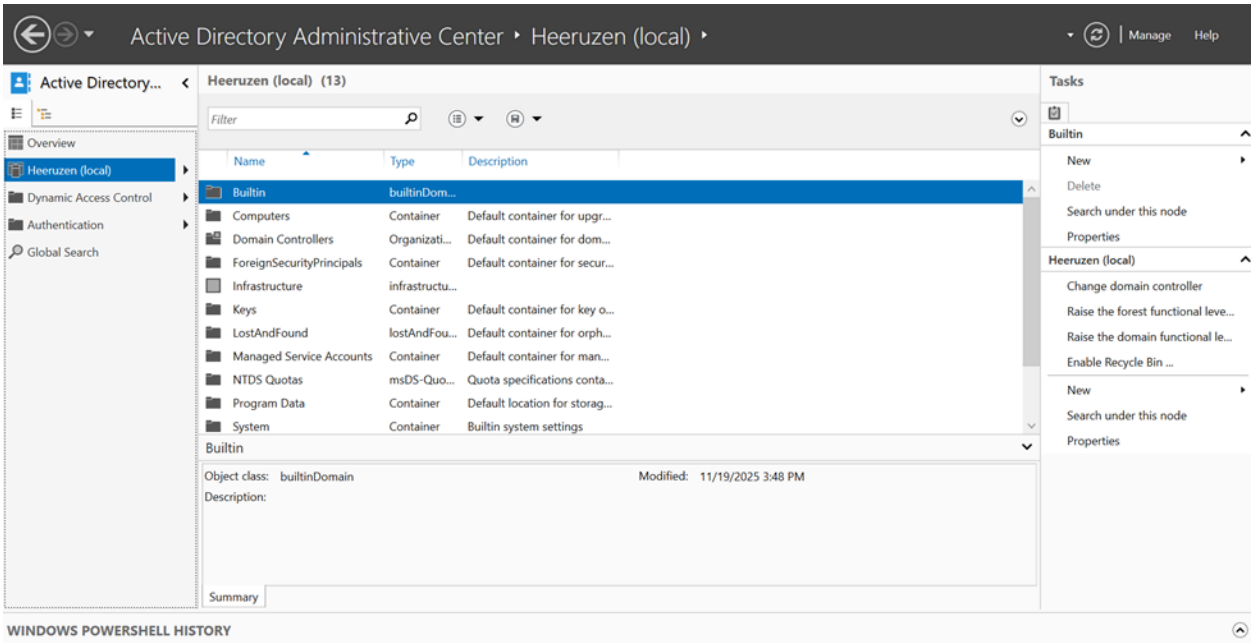
Server Manager showing AD DS Installed



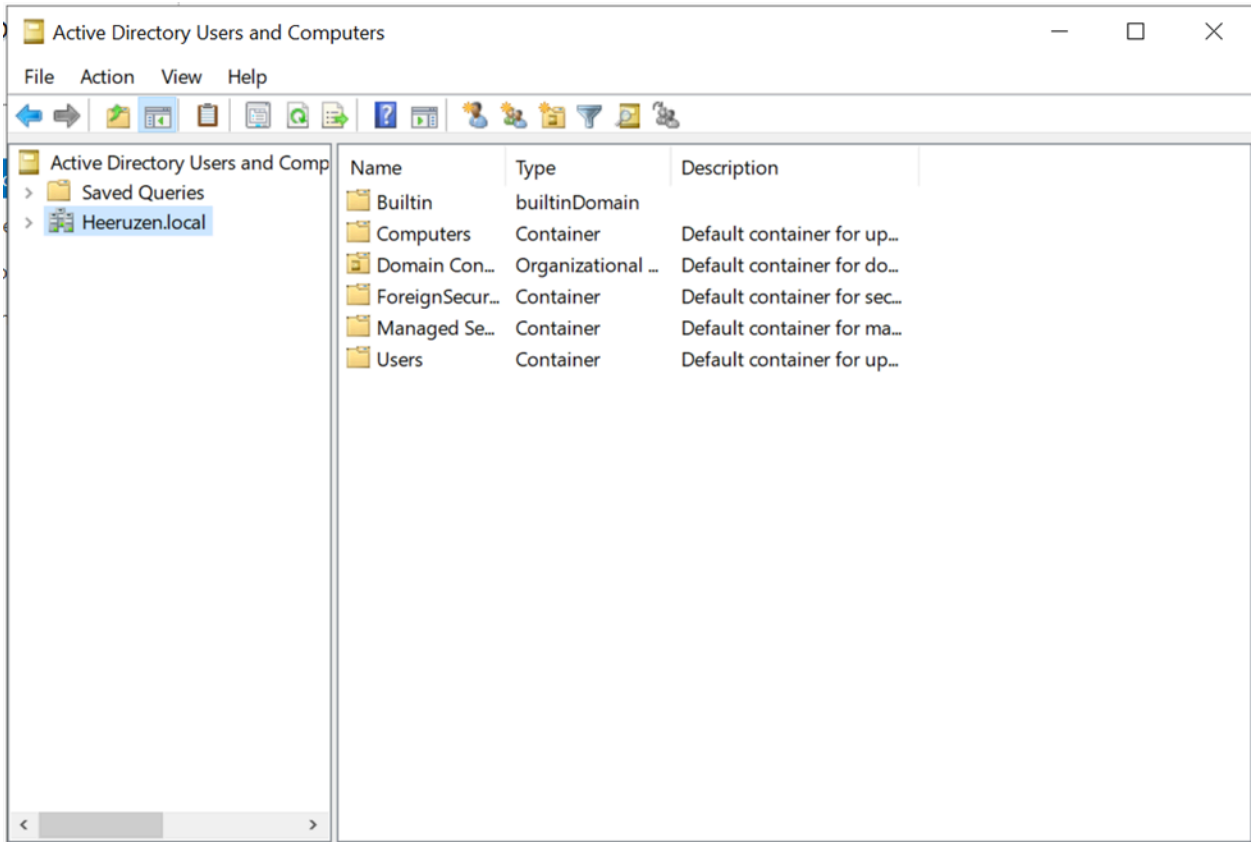
3.2 User Configuration

Using the Active Directory Administrative Center and Users and Computers tool, a new user named **Clark Israel** was created24.

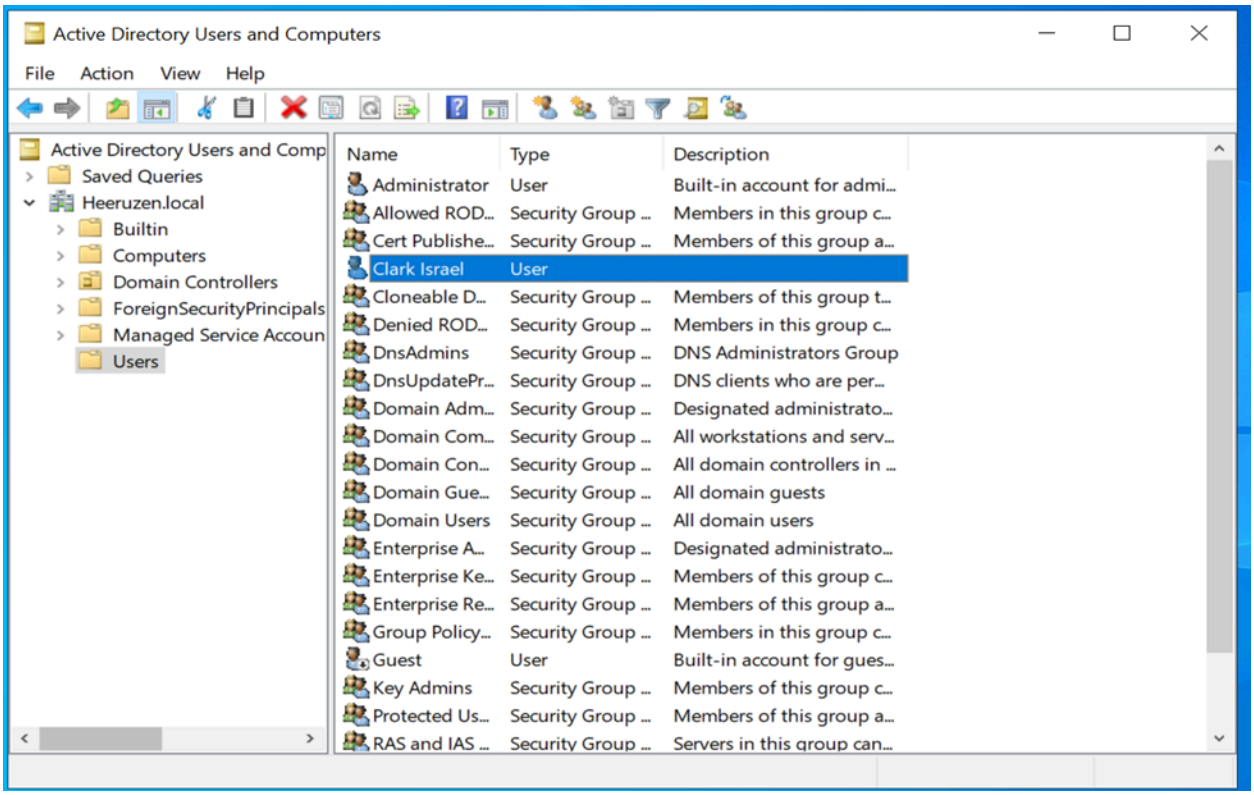
Active Directory Administrative Center



Active Directory Users and Computers



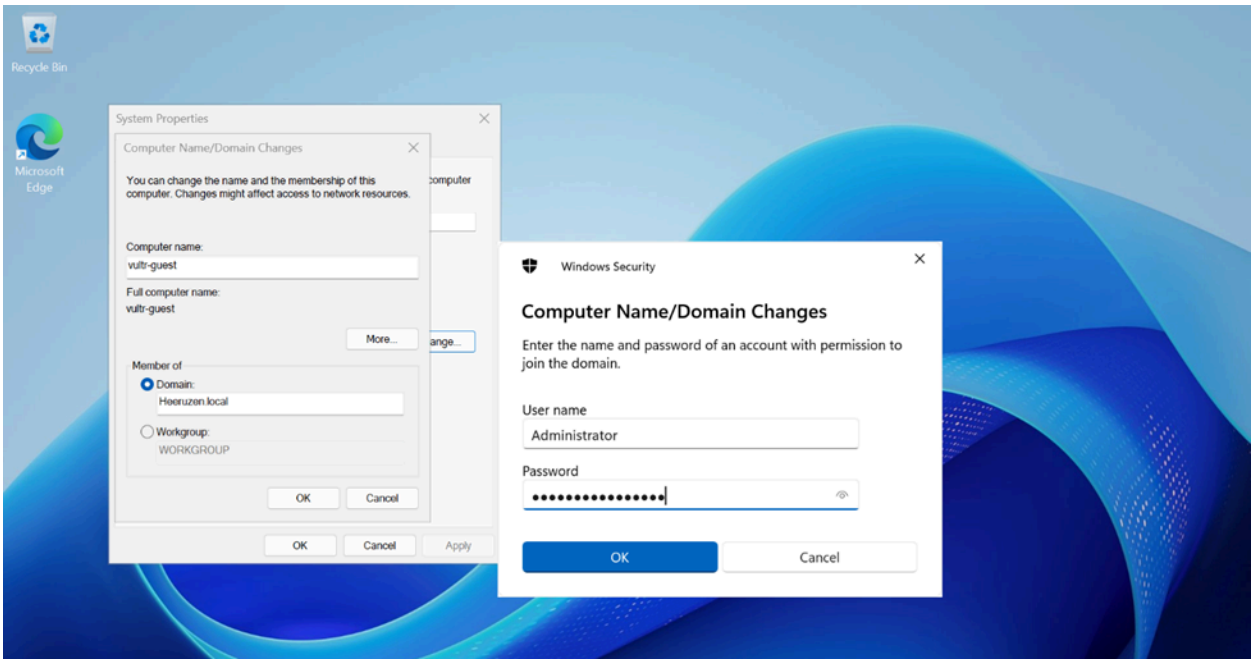
List of Users showing Clark Israel



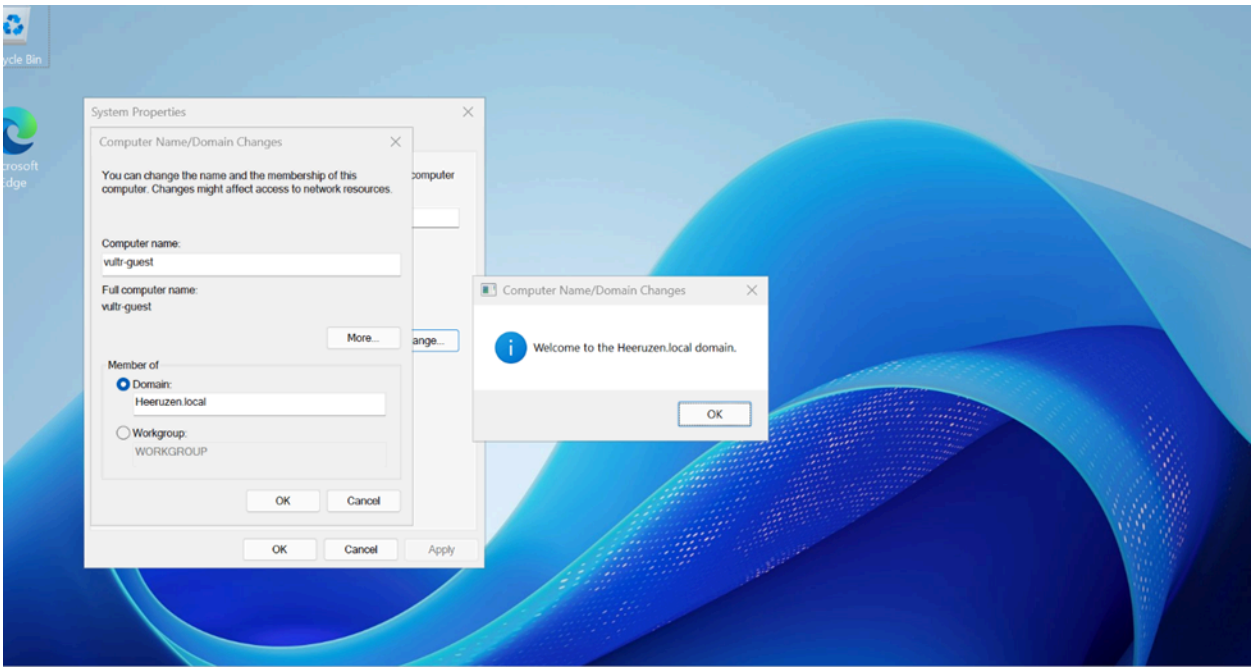
3.3 Joining the Test Machine to the Domain

The `Test-Machine` was configured to join the `Heeruzen.local` domain using Administrator credentials.

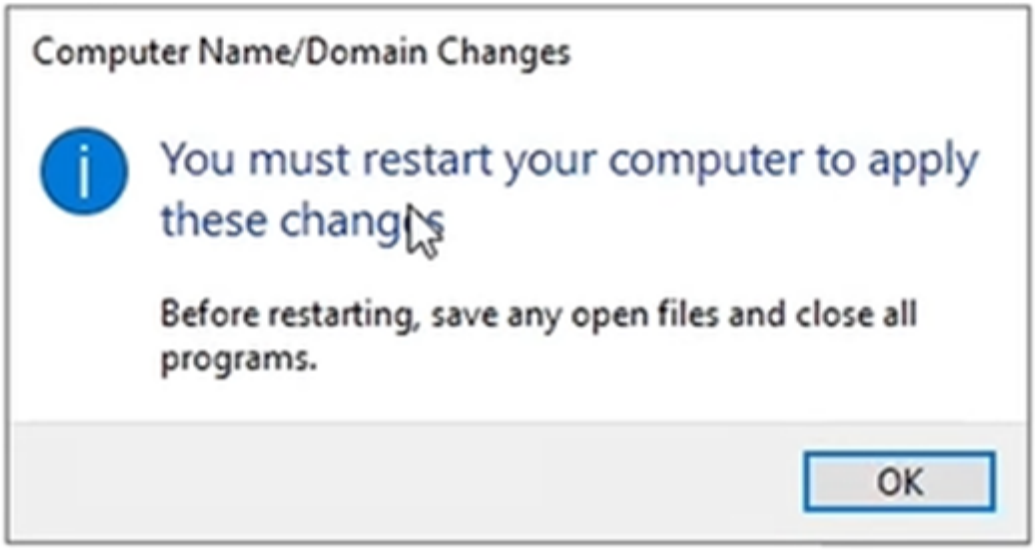
Computer Name/Domain Changes Dialog



Welcome to the Heeruzen.local domain Message



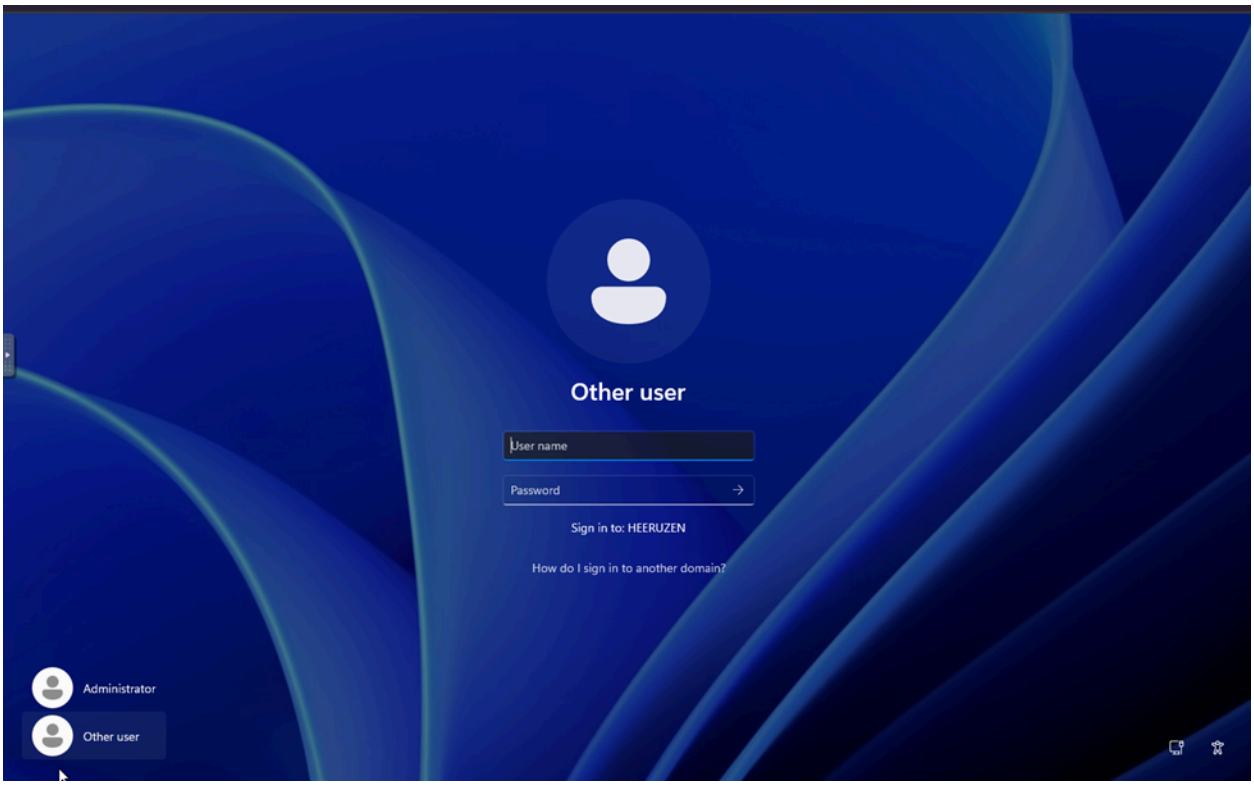
Restart Prompt



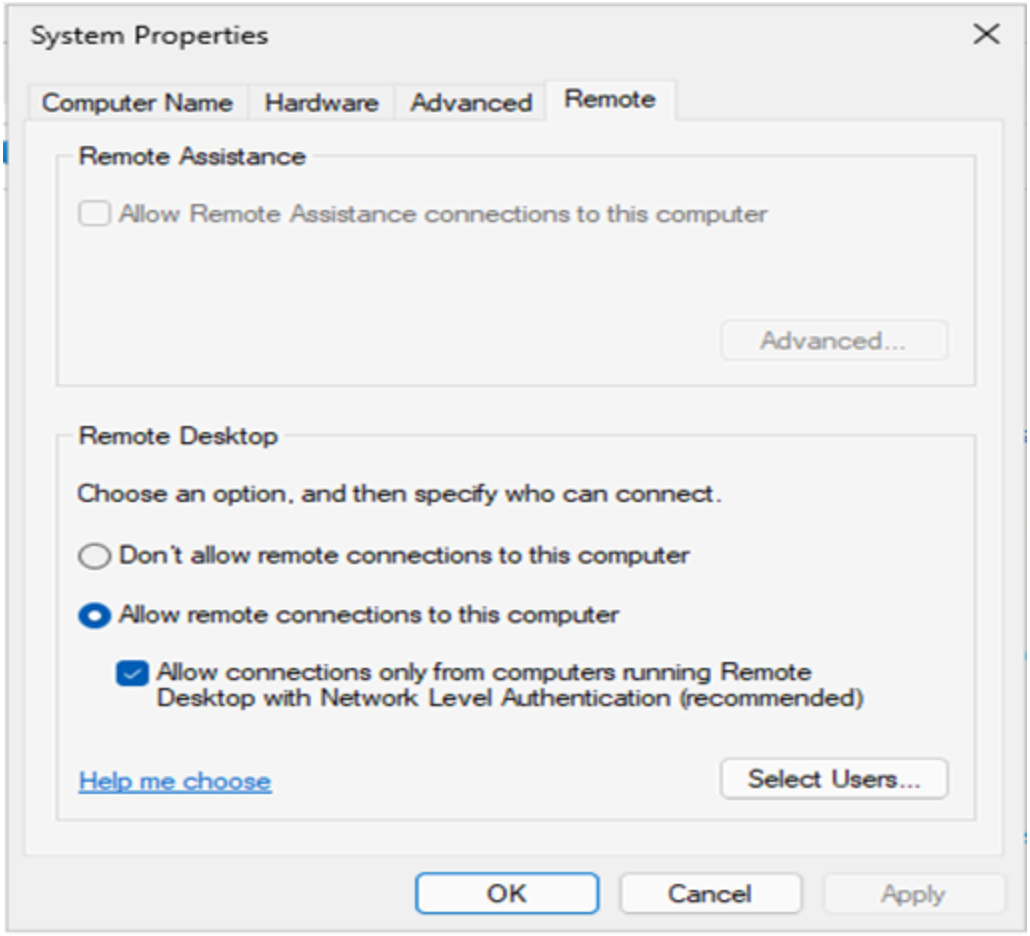
3.4 Client Login & RDP Configuration

After restarting, login was performed using the new domain user credentials26. To facilitate remote management, RDP access was explicitly enabled for the user `heeruzen.local\clrkisreal` in System Properties.

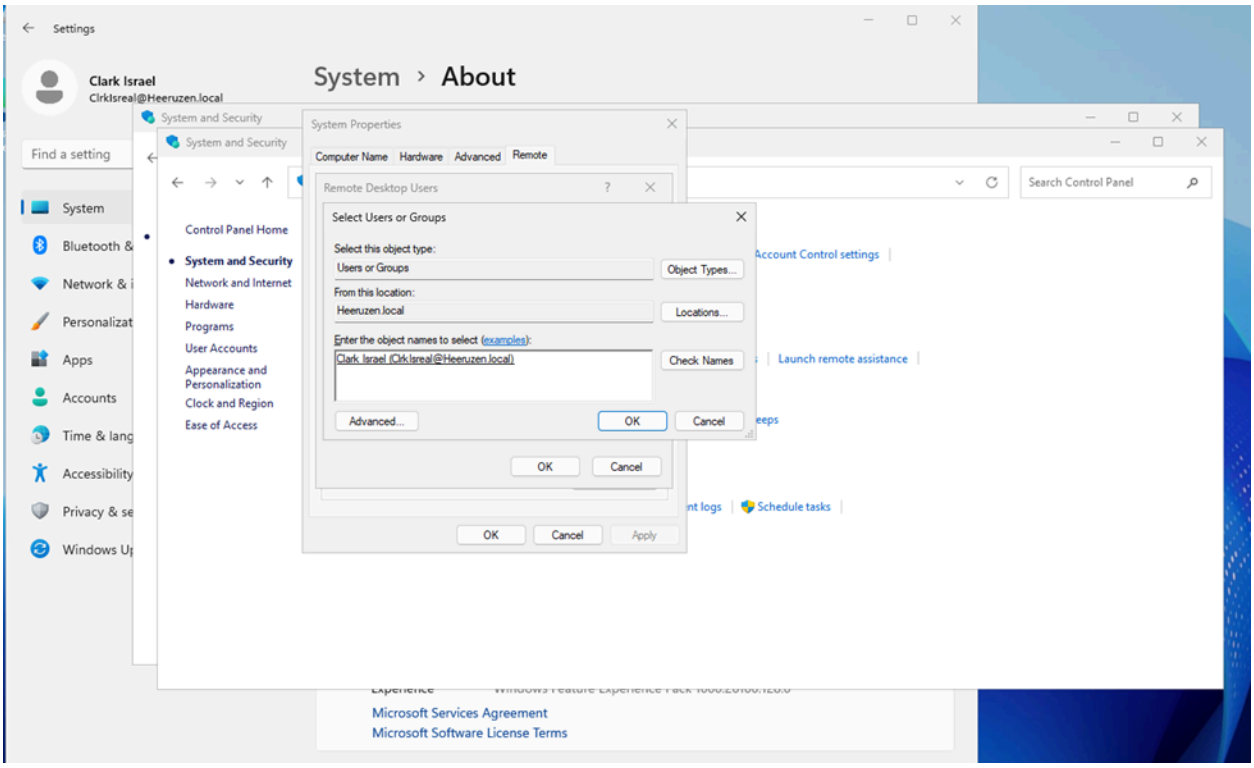
Windows 11 Login Screen for Other User



System Properties - Remote Desktop Settings

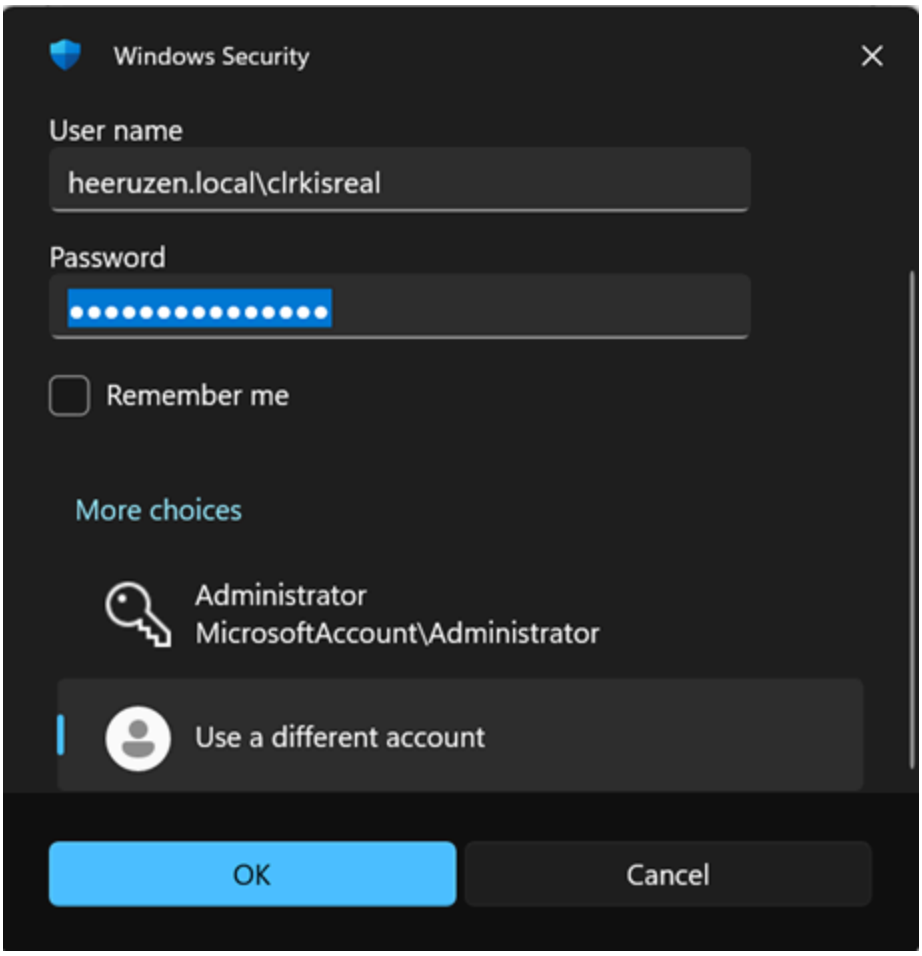


Selecting Users for Remote Desktop

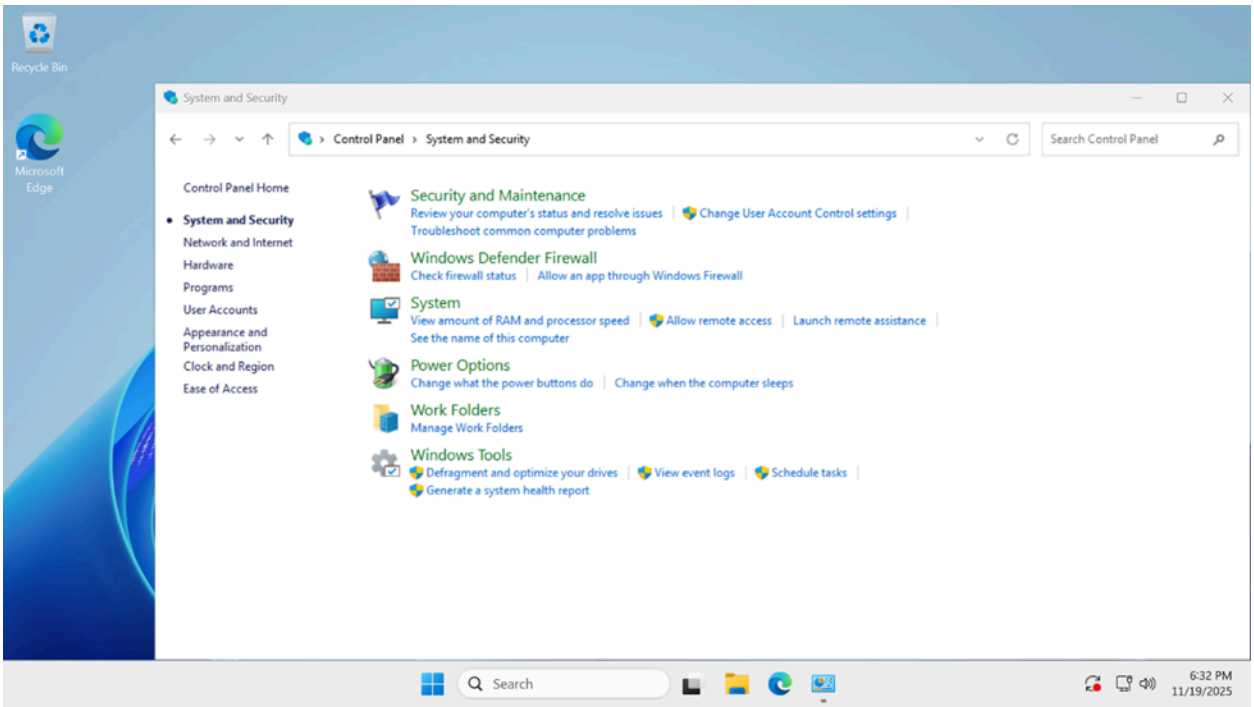


RDP connection was successfully tested with the new user credentials

Windows Security Credential Prompt



Successful RDP Desktop Session



4. Splunk Enterprise Server Setup

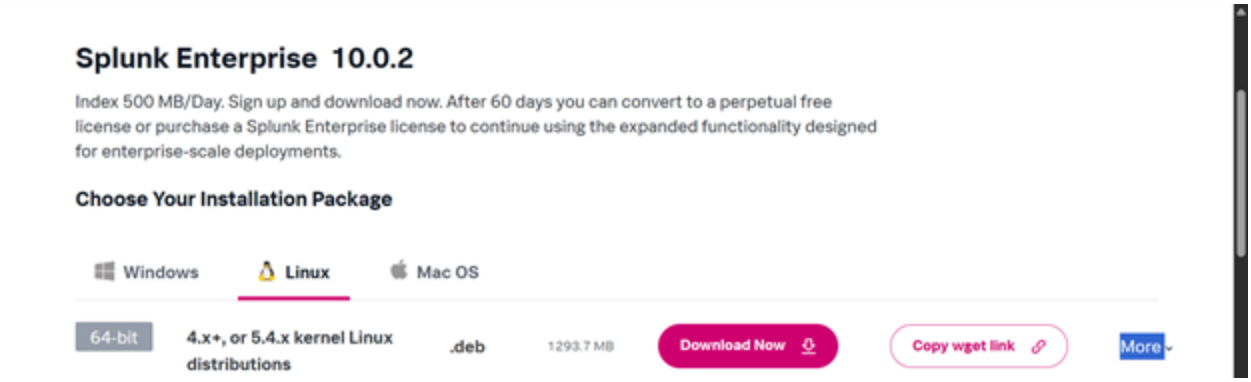
4.1 Installation on Ubuntu

A connection was established to the Ubuntu server via SSH29. Splunk Enterprise 10.0.2 was downloaded using `wget` and installed using `dpkg`.

SSH Terminal Login

```
PS C:\Users\davix> ssh root@45.76.92.215
root@45.76.92.215's password:
Welcome to Ubuntu 25.10 (GNU/Linux 6.17.0-6-generic x86_64)

 * Documentation:  https://docs.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Thu Nov 20 20:20:08 UTC 2025

  System load:  0.0                Processes:               171
  Usage of /:   8.2% of 149.47GB   Users logged in:         0
  Memory usage: 5%                 IPv4 address for enp1s0: 45.76.92.215
  Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

0 updates can be applied immediately.


Last login: Thu Nov 20 08:09:50 2025 from 102.91.92.103
```

Splunk Download Page



Wget Download Command in Terminal

```
wget -O splunk-10.0.2-e2d18b4767e9-linux-amd64.deb
```

```
root@Heeruzen-Splunk:~# wget -O splunk-10.0.2-e2d18b4767e9-linux-amd64.deb "https://download.splunk.com/products/splunk/
releases/10.0.2/linux/splunk-10.0.2-e2d18b4767e9-linux-amd64.deb"
--2025-11-20 20:32:18--  https://download.splunk.com/products/splunk/releases/10.0.2/linux/splunk-10.0.2-e2d18b4767e9-li
nux-amd64.deb
Resolving download.splunk.com (download.splunk.com)... 3.167.227.17, 3.167.227.30, 3.167.227.98, ...
Connecting to download.splunk.com (download.splunk.com)|3.167.227.17|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1356540912 (1.3G) [binary/octet-stream]
Saving to: ‘splunk-10.0.2-e2d18b4767e9-linux-amd64.deb’

splunk-10.0.2-e2d18b4767e9-li 100%[===================================================>]   1.26G   237MB/s    in 5.1s

2025-11-20 20:32:24 (252 MB/s) - ‘splunk-10.0.2-e2d18b4767e9-linux-amd64.deb’ saved [1356540912/1356540912]

root@Heeruzen-Splunk:~#
```

DPKG Installation Process

```
dpkg -i  splunk-10.0.2-e2d18b4767e9-linux-amd64.deb
```

```
root@Heeruzen-Splunk:~# dpkg -i  splunk-10.0.2-e2d18b4767e9-linux-amd64.deb
Selecting previously unselected package splunk.
(Reading database ... 100980 files and directories currently installed.)
Preparing to unpack splunk-10.0.2-e2d18b4767e9-linux-amd64.deb ...
verify that this sytem has all the commands we will require to perform the preflight step
no need to run the splunk-preinstall upgrade check
Unpacking splunk (10.0.2) ...
Setting up splunk (10.0.2) ...
find: ‘/opt/splunk/lib/python3.7/site-packages’: No such file or directory
complete
```

4.2 Initializing Splunk

The Splunk binary was started from `/opt/splunk/bin`, and the administrator credentials (`heeruzen.local`) were configured31.

Navigating directories and starting Splunk

```
cd /opt/splunk
cd bin>
./splunk start
```

```
root@Heeruzen-Splunk:~# cd /opt/splunk
root@Heeruzen-Splunk:/opt/splunk# ls
LICENSE.txt        copyright.txt  include           openssl            share
README-splunk.txt  etc            lib               opt                splunk-10.0.2-e2d18b4767e9-linux-amd64-manifest
bin                ftr            license-eula.txt  quarantined_files  swidtag
root@Heeruzen-Splunk:/opt/splunk# cd bin
root@Heeruzen-Splunk:/opt/splunk/bin# ./splunk start
```

Setting Administrator Credentials

```
Please enter an administrator username: heeruzen.local
Password must contain at least:
   * 8 total printable ASCII character(s).
Please enter a new password:
```

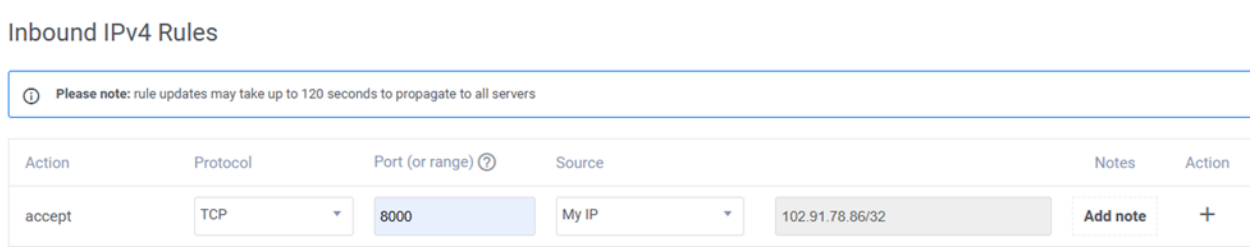
Splunk Start Complete Message

```
Starting splunk server daemon (splunkd)...
Using configuration from /opt/splunk/share/openssl3/openssl.cnf
........+.......++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*........+...........+.+++++++++++++++++
++++++++++++++++++++++++++++++++++++++++++++++++++*...+......+.......................+....+...+.........+......+...+.....
.........+..........+..+.........+.+...+........+.........+.+...+......++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++
....+..........++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.......+.....+.+.....+...+....+........
...+......+...+.+...........+..........++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*...+..+......+.
.........+...+...........+...+...............+.......+...............+........+.+......+.....+.+..+...+....+.........+..
+.........+...+..........+...........+..........+......+...............+......+...+.....+....+..+.+.....+...++++++++++++
++++++++++++++++++++++++++++++++++++++++++++++++++++++
Warning: ignoring -extensions option without -extfile
Certificate request self-signature ok
subject=CN = Heeruzen-Splunk, O = SplunkUser
Done


Waiting for web server at http://127.0.0.1:8000 to be available...........
```

4.3 Web Interface Access

Firewall rules (both on Vultr and the local Ubuntu UFW) were updated to allow traffic on Port 8000. The web interface was accessed at `45.76.92.215:8000`.

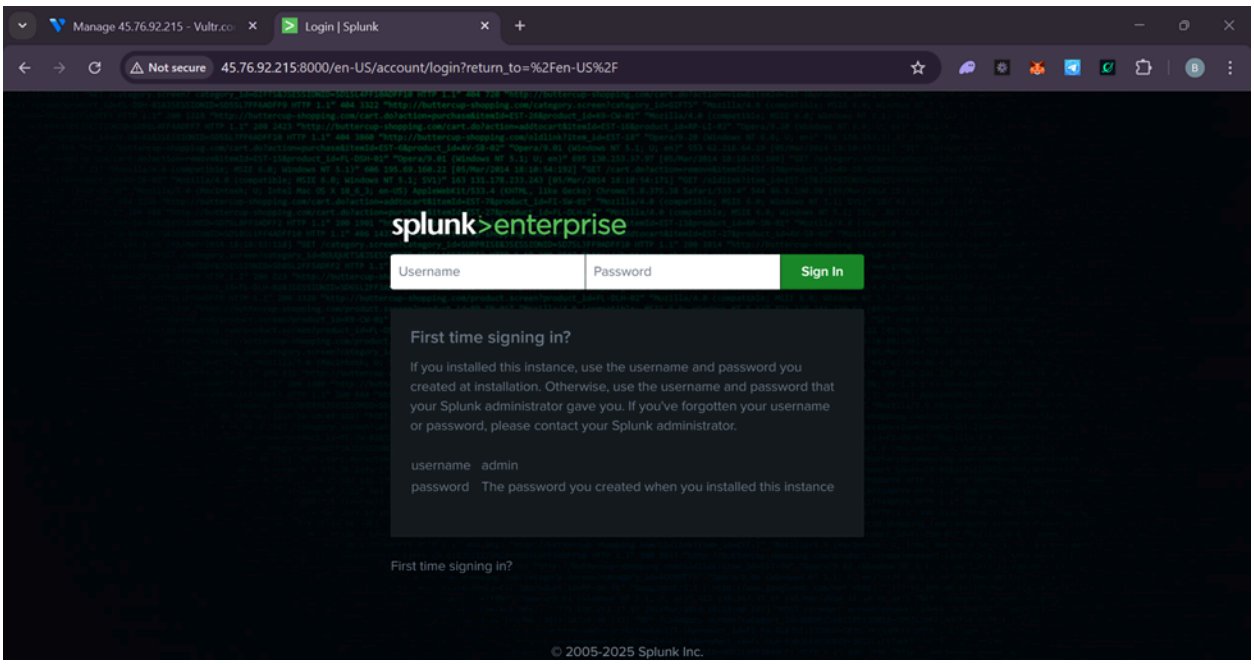
Vultr Firewall Rules allowing Port 8000



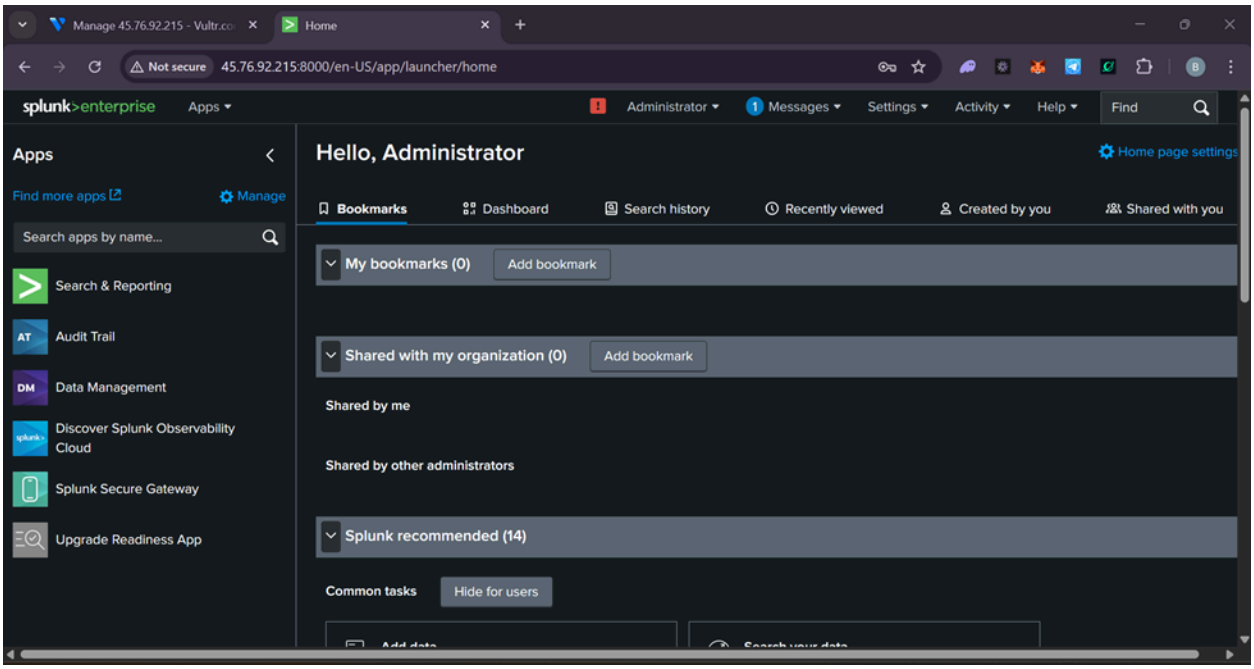
Terminal Command `ufw allow 8000`

```
root@Heeruzen-Splunk:~# ufw allow 8000
Rule added
Rule added (v6)
root@Heeruzen-Splunk:~#
```

Splunk Enterprise Web Login Screen



Splunk Administrator Dashboard

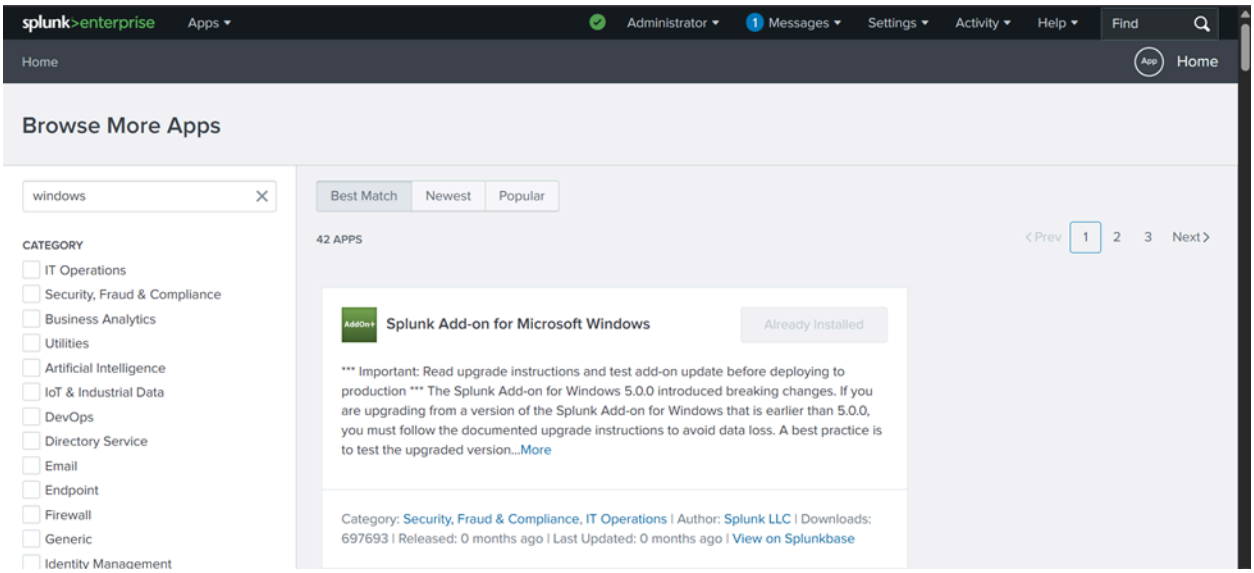


5. Splunk Configuration (Ingestion)

5.1 App Installation

The "Splunk Add-on for Microsoft Windows" was installed to parse Windows data correctly.

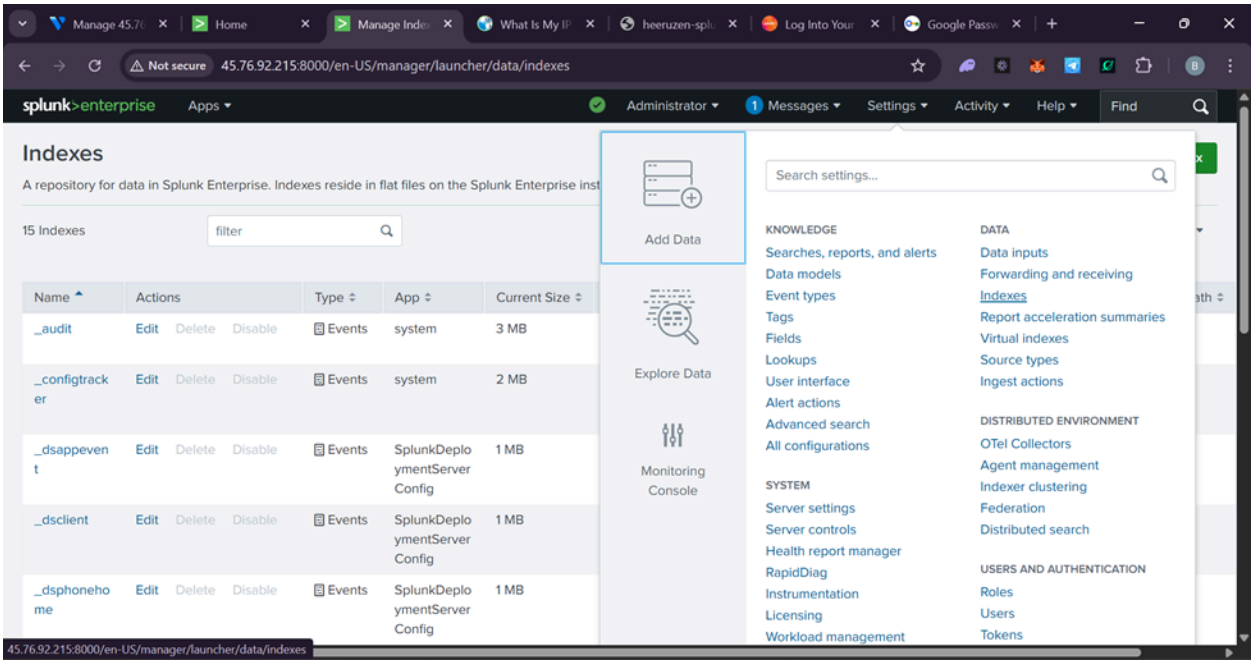
Browse More Apps - Windows Add-on



5.2 Index and Receiver Configuration

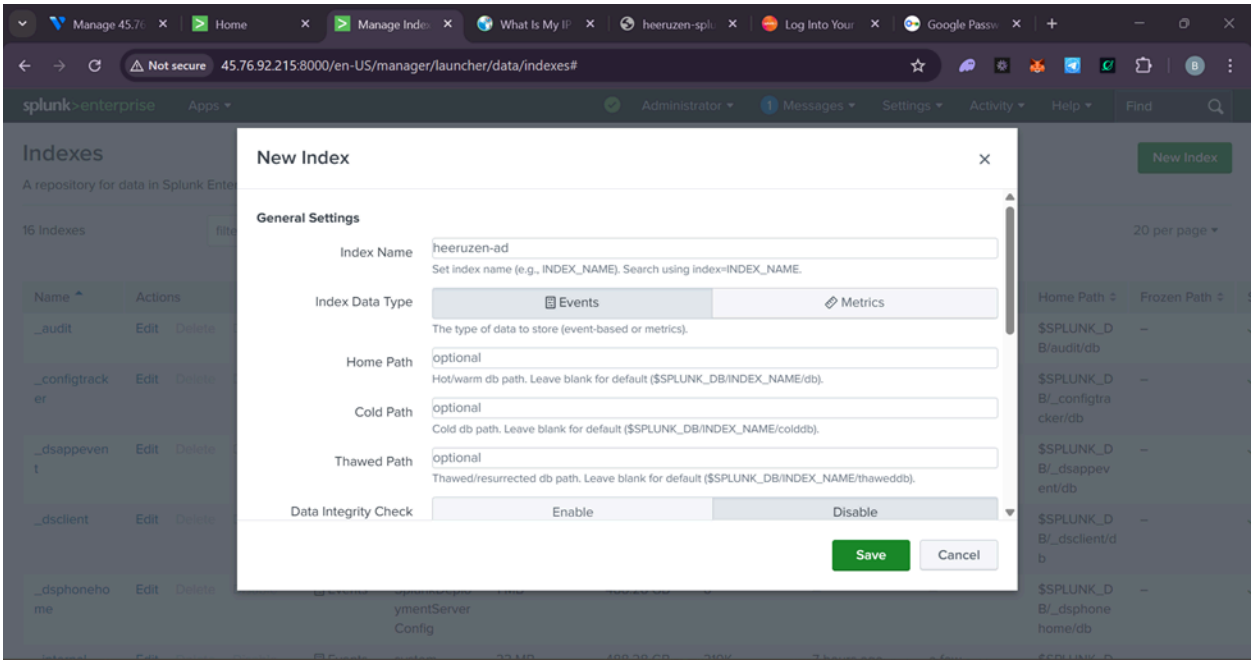
A new index named `heeruzen-ad` was created to store the incoming data.

Splunk Indexes List

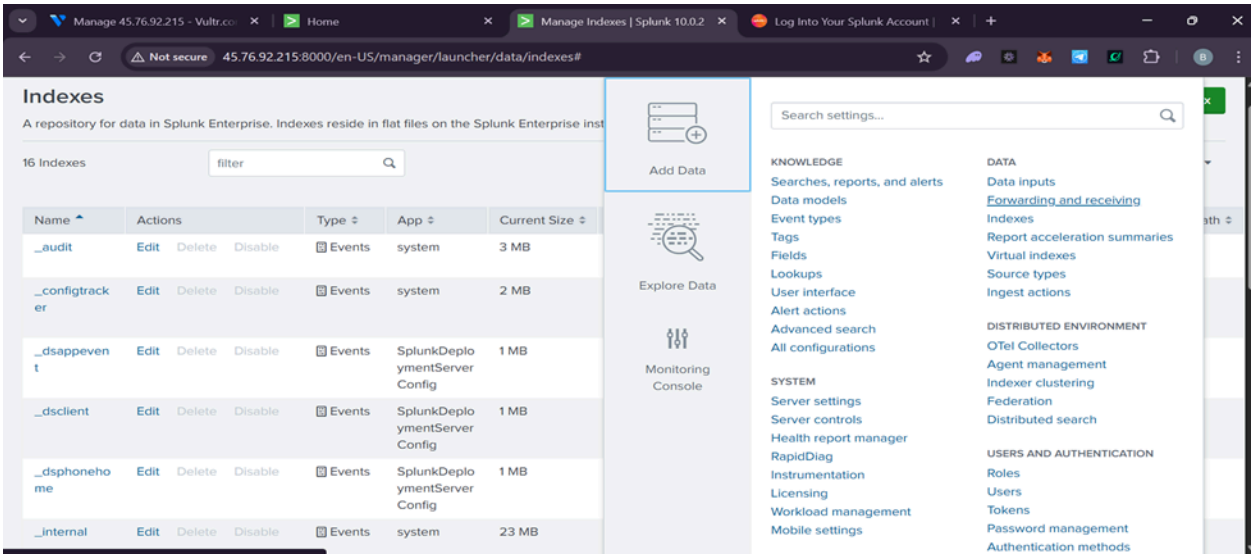


New Index Creation Dialog

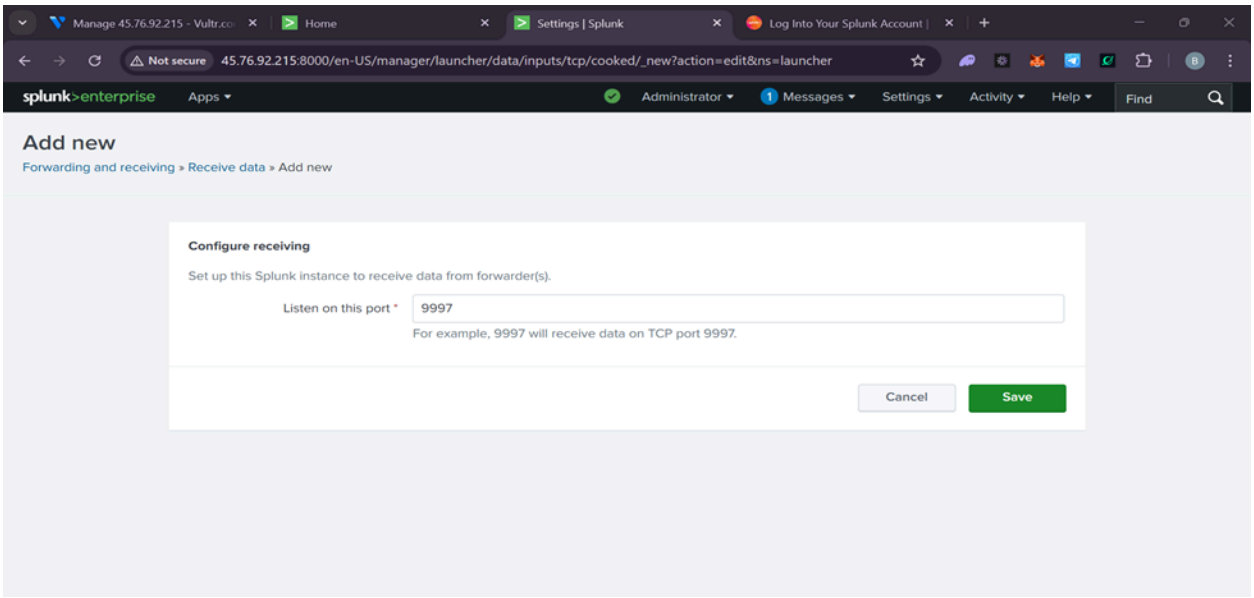
New Index: heeruzen-ad



Settings > Indexes Menu

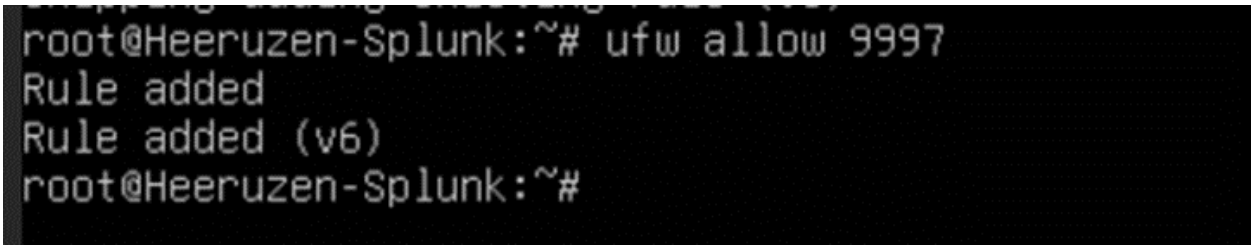


Configure Receiving Port 9997



Terminal Command

Configure Splunk SSH to listen for incoming data on the default forwarding port **9997**. The firewall was updated to allow this traffic. `ufw allow 9997`



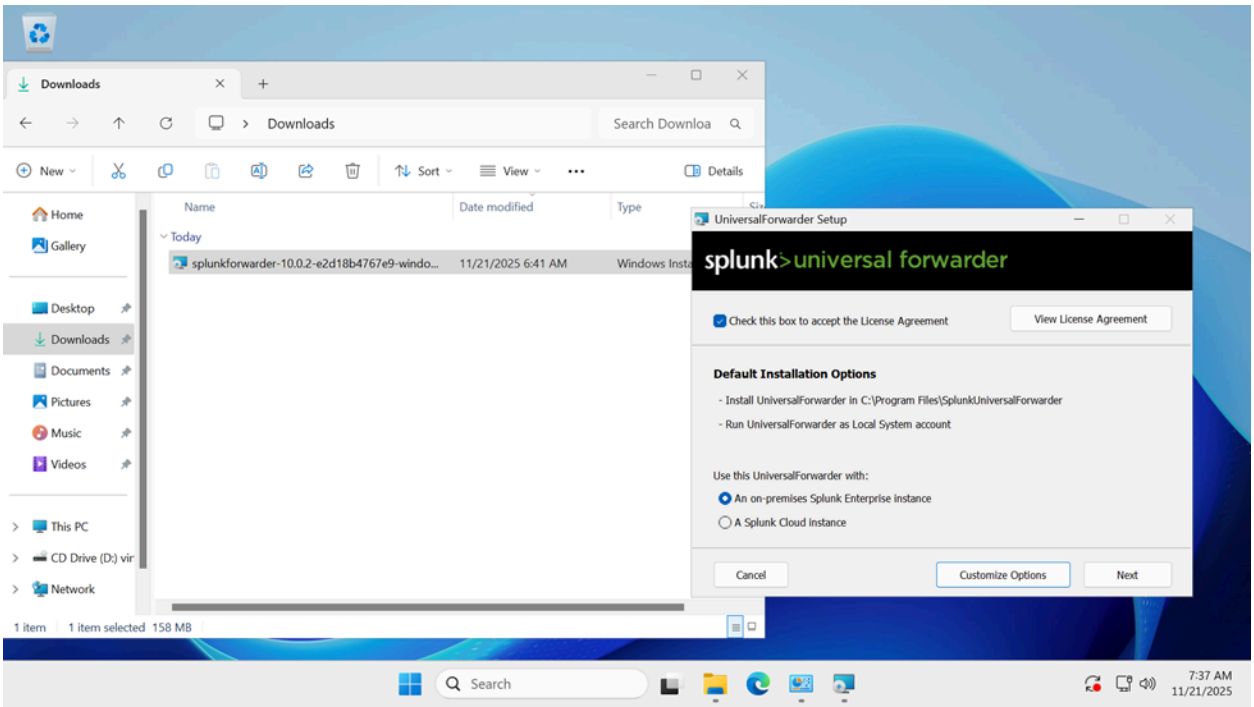
---

6. Universal Forwarder Deployment

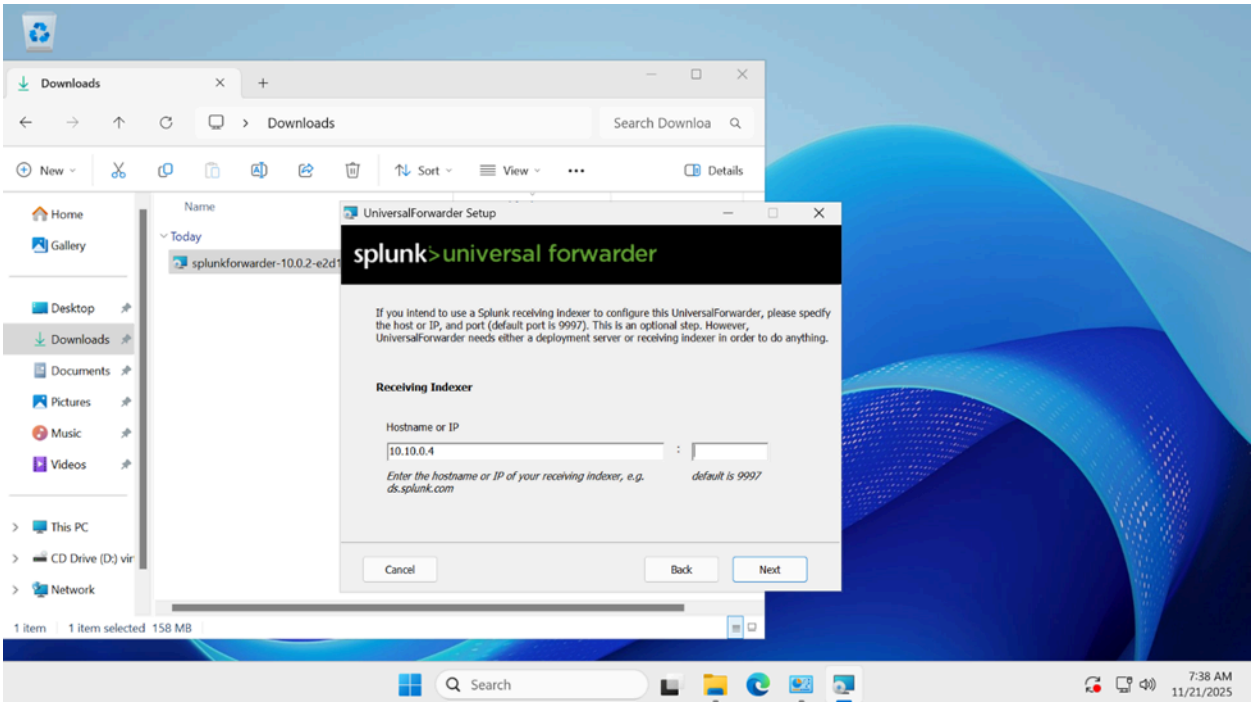
6.1 Installation on Windows

The Splunk Universal Forwarder was installed on the Test Machine (`95.179.240.136`). During installation, the Receiving Indexer was set to the Splunk Private IP `10.10.0.4` .

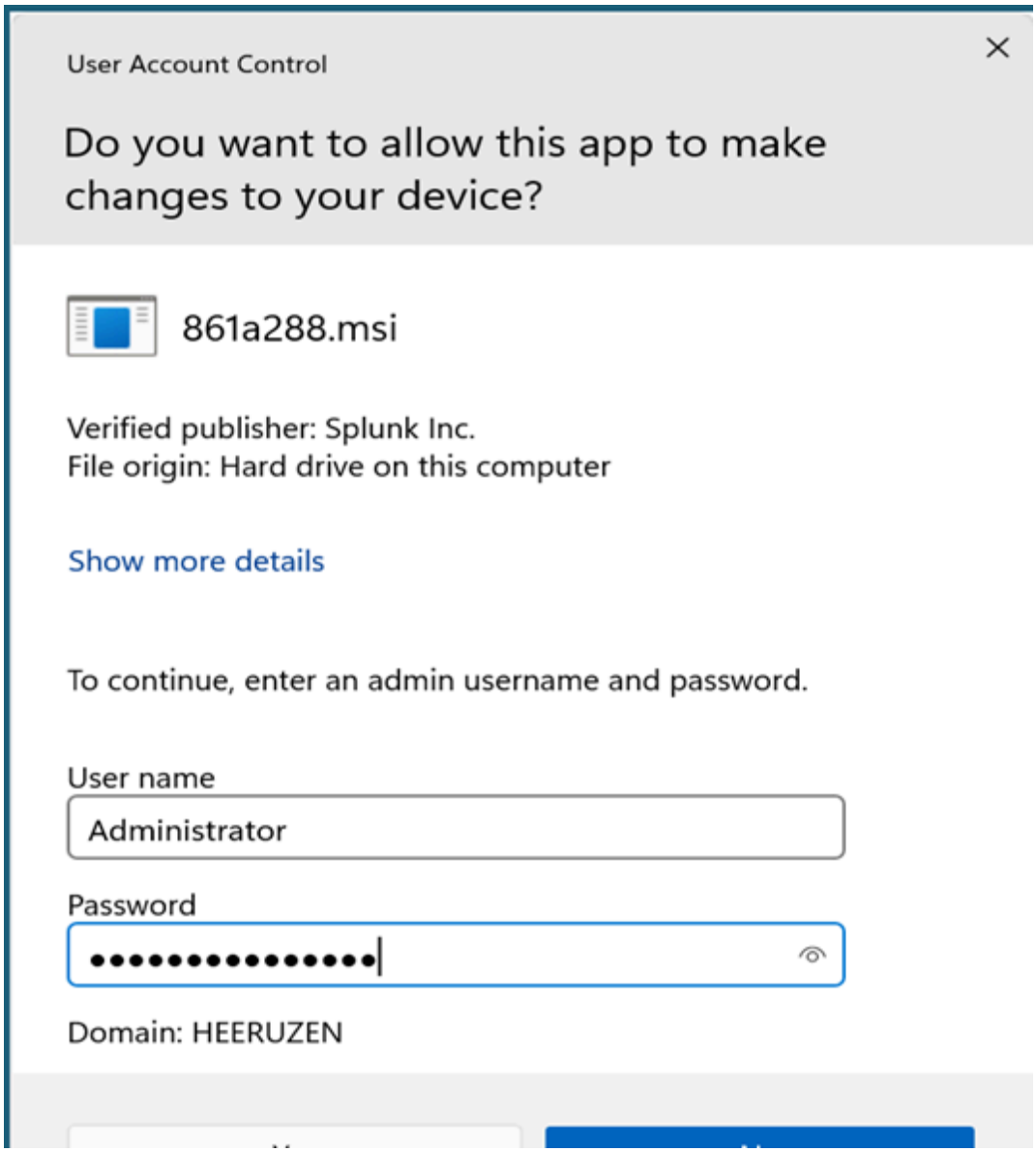
Universal Forwarder Setup Wizard



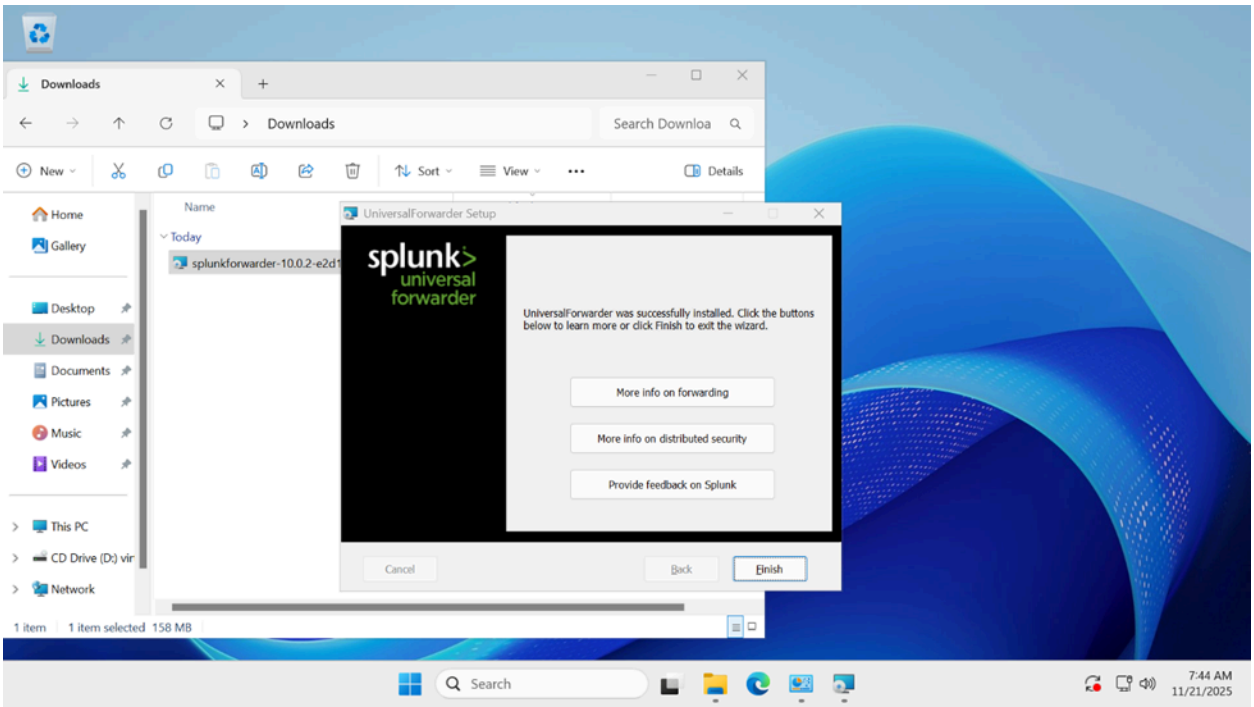
Configuring Receiving Indexer IP



Installation User Account Control Prompt



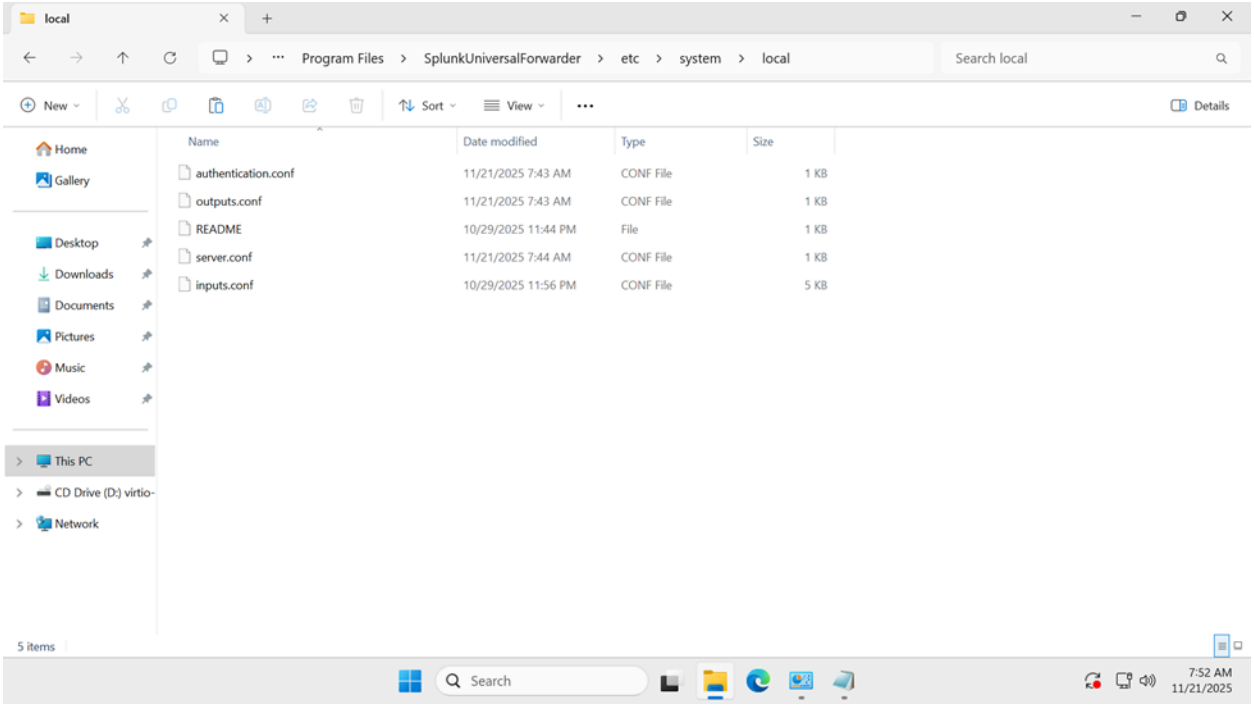
Installation Finished Dialog



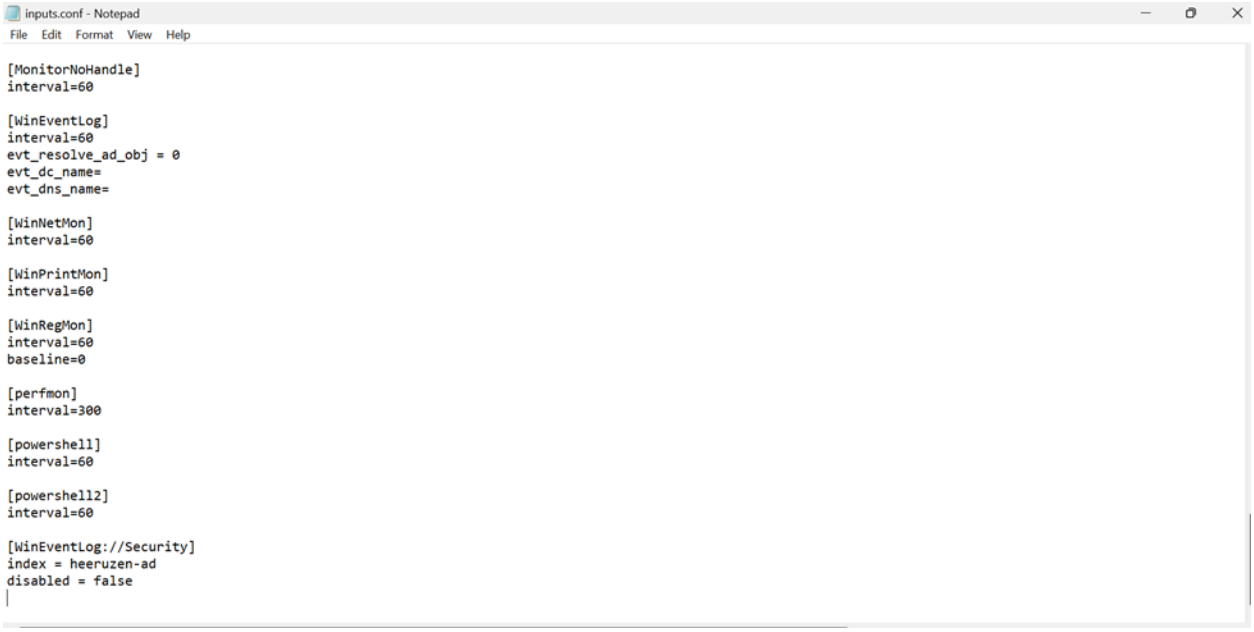
6.2 Configuration (inputs.conf)

The `inputs.conf` file was copied from the default folder to `/etc/system/local` and edited to define the input parameters. The configuration was set to monitor Security logs and send them to the `heeruzen-ad` index.

File Explorer showing inputs.conf location



Notepad edit of inputs.conf



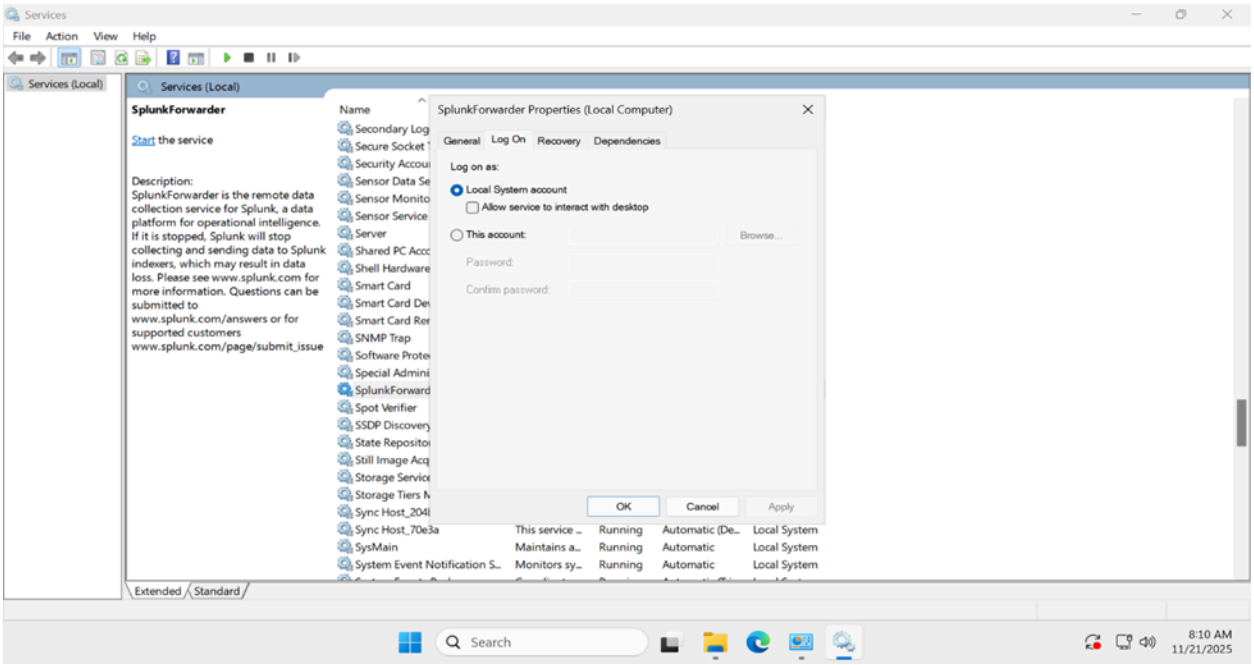

```
[WinEventLog://Security]
index = heeruzen-ad
```

```
disabled = false
```

6.3 Service Configuration

The "SplunkForwarder" service logon account was changed to "Local System account" to ensure proper permissions, and the service was restarted.

Services.msc Properties for SplunkForwarder

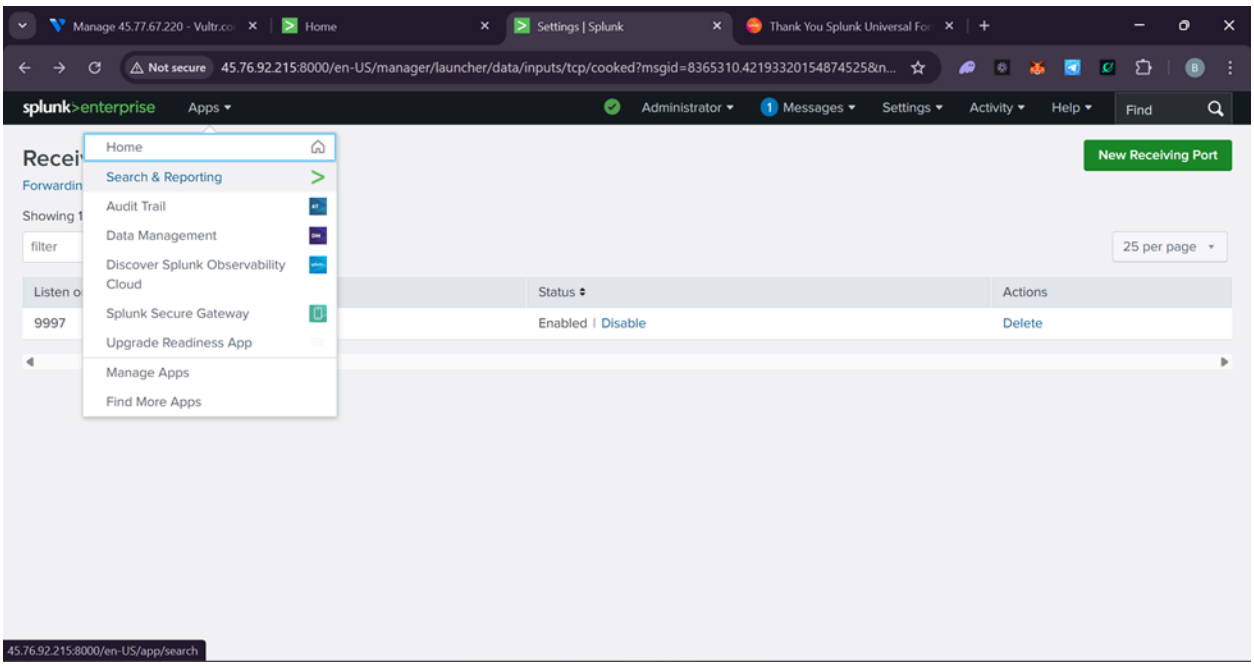


7. Verification and Telemetry

7.1 Verifying Data Reception

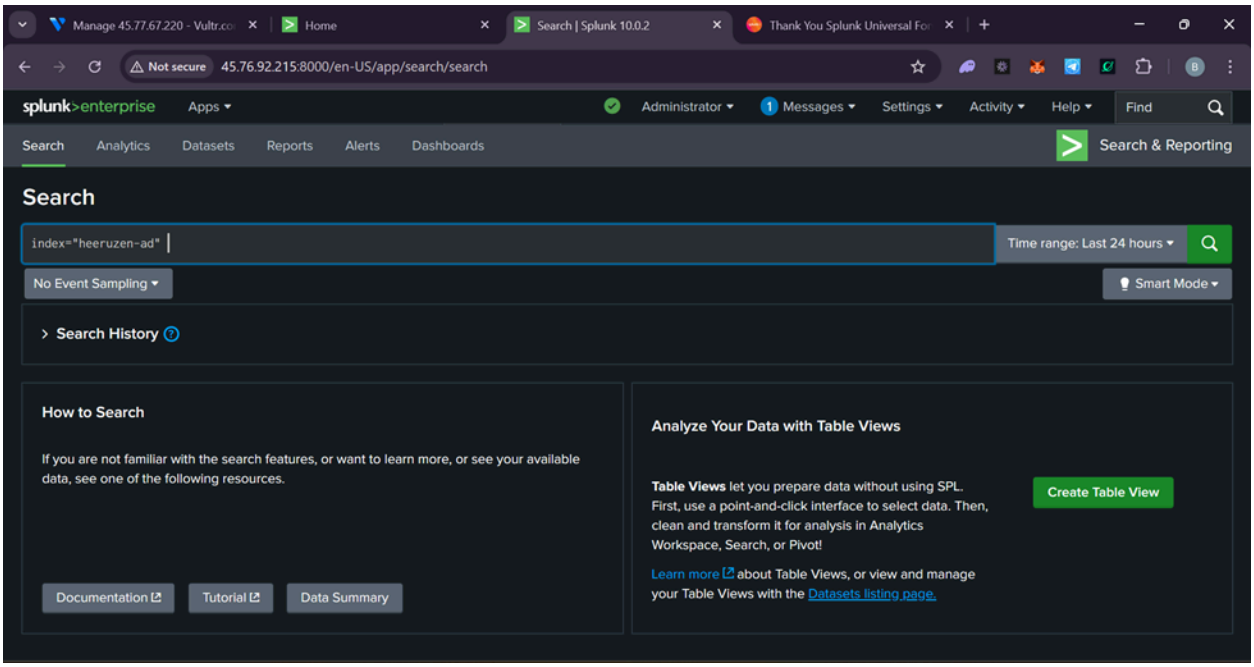
On the Splunk Web Interface, I checked "Forwarding and receiving" to confirm port 9997 was enabled.

Splunk Menu - Search & Reporting



7.2 Search Query

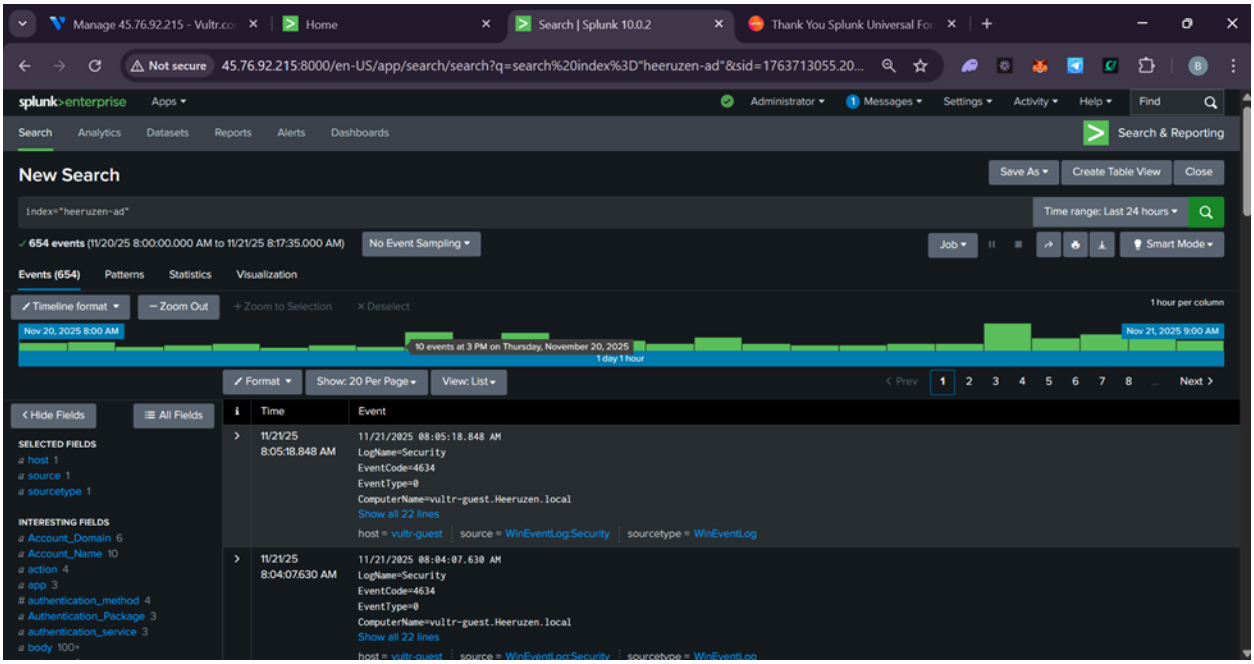
A search query `index="heeruzen-ad"` was executed over the last 24 hours.



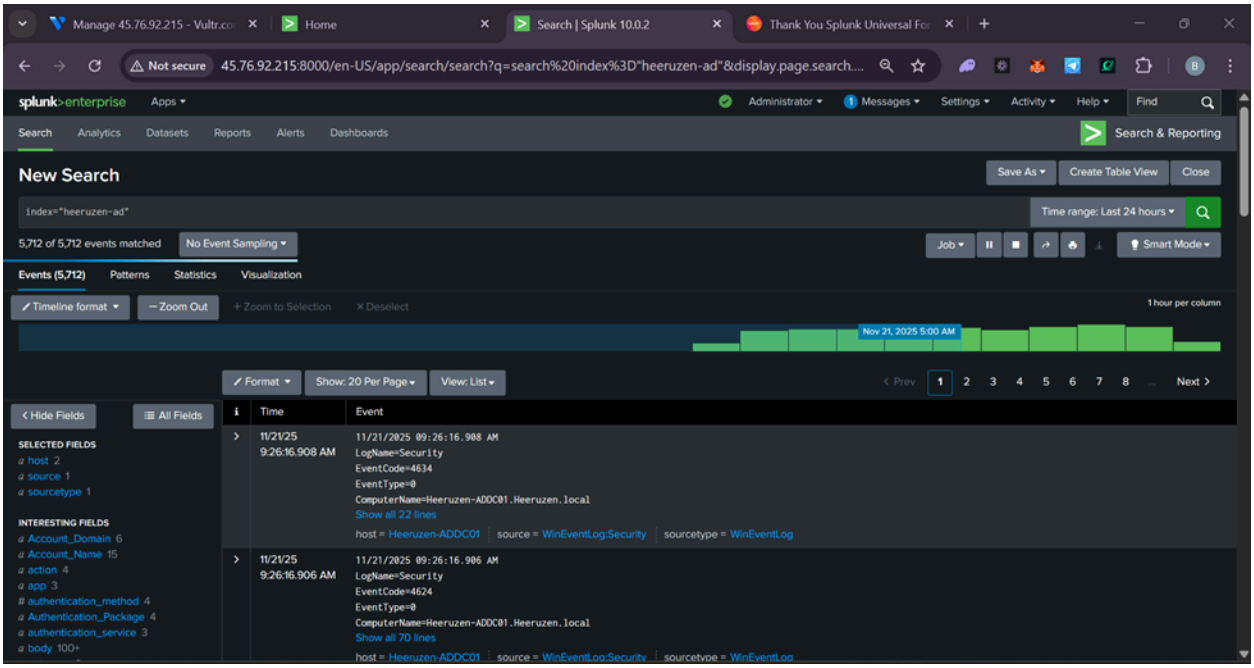
7.3 Results

Telemetry was successfully received from the `vultr-guest` (Test Machine). The Universal Forwarder was subsequently installed on the Domain Controller, and telemetry was verified for both hosts (`Heeruzen-ADDC01` and `vultr-guest`).

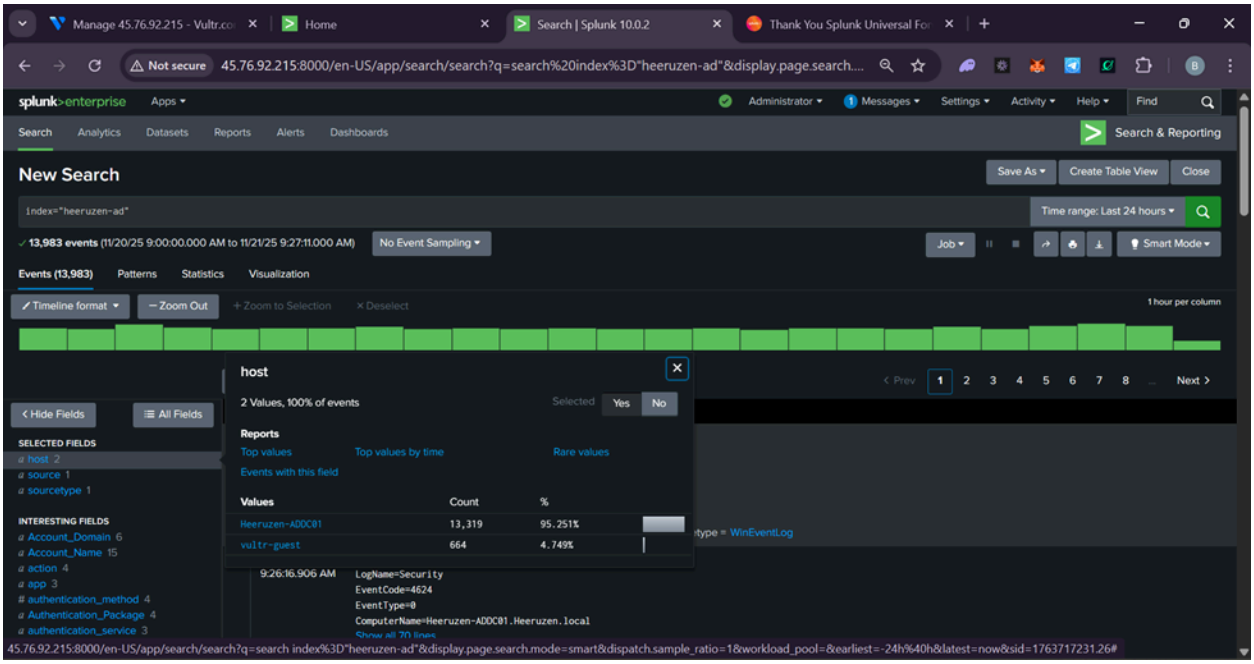
Events from vultr-guest - Test Machine



Events result from Heeruzen-ADDC01



Host Visualization showing traffic from both sources



Conclusion

Building this Splunk monitoring lab was a major step forward in strengthening my hands-on cybersecurity foundation. Starting from a clean Vultr setup, I deployed a Domain Controller, a Windows Test Machine, and an Ubuntu-based Splunk Enterprise server—each configured to communicate within a controlled cloud environment.

By joining machines to the domain, enabling RDP access through domain credentials, configuring firewall rules, and installing the Splunk Universal Forwarder, I created a reliable end-to-end pipeline for real Windows event telemetry. This means authentication logs, security events, and host activity are now continuously forwarded to Splunk for centralized monitoring.

Throughout this process, I gained practical experience with:

- Cloud networking and firewall rule management
- Active Directory setup and domain/user administration
- Splunk Enterprise configuration and index management
- Forwarder deployment and Windows Security log ingestion

This environment now closely mirrors what real organizations use for blue-team monitoring and security operations. It's a strong addition to my cybersecurity portfolio and a foundation I can keep expanding as I progress in detection engineering, SIEM operations, and defensive security.

Future Improvements

While the core logging pipeline is complete, there are several realistic improvements I plan to add to strengthen the environment:

1. Add More Data Sources

- Deploy Linux servers and forward syslog data
- Ingest firewall or IDS logs (e.g., Suricata)

- Add PowerShell logging, Sysmon, and Command Line Auditing for deeper visibility

2. Strengthen Detection Engineering

- Create correlation rules for brute force, privilege escalation, and suspicious process activity
- Build dashboards for user behavior, authentication trends, and host activity

3. Expand Active Directory Use Cases

- Add more users, groups, and policies
- Create fake departments and permission structures
- Simulate real-world authentication patterns

4. Implement Endpoint Hardening

- Configure AppLocker, ASR rules, or LAPS
- Deploy Sysmon with a custom configuration

Errors Encountered and Fixed.

VPC Error Fix
FIX RDP ERROR