Veeam Decoys

Contents

Introduction

Today, the number of existing attacks on organizations is exponential. Therefore, companies need to implement best practices for IT risk management, as well as implement the best solutions for data protection, incident detection, and incident management.

In the world of security, there are many frameworks that allow organizations to improve their IT security level. For this, it is always necessary to maintain early detection of lateral movements, connection attempts from unauthorized sources, scans occurring on the internal network, or simply an inventory of ports used on servers in a VLAN or multiple VLANs / Networks.

Therefore, there exists a concept and technology that allows us to create services to detect these types of lateral movements or connection attempts to anticipate a security incident. As is publicly known, many Ransomware groups also focus on destroying data backups.

For this reason, this project was developed to create services that simulate being productive so that, in case of any attempt at attack, connection, or authentication, it is detected, and the organization's IT security area can apply the necessary measures or its incident response plan.

Statistics

These types of services were tested on the internet, obtaining a behavioral pattern of what attackers or Bots look for on the internet. It should be noted that this solution is to be implemented in the organization's internal networks, but the objective was to have scans or attacks that exist on the internet to know the quantity and resource consumption. In fact, it is the best place to receive connection attempts or sequential and random scans. Some of the statistical data obtained were as follows:

Number of days with exposed services: **15**

Number of exposed services: **7**

CPU: **1 vCPU**

RAM: **2 GB**

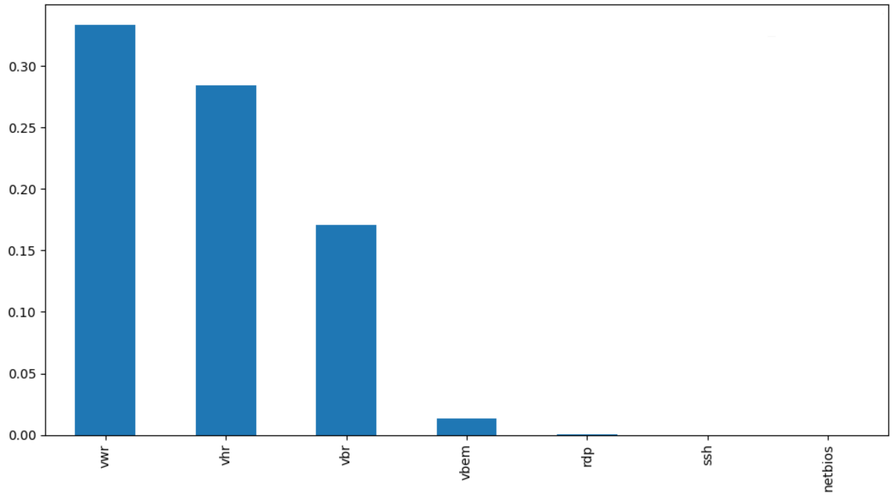
Storage: **50 GB**

Computing resource consumption only had a maximum usage of **28%** CPU on one day out of the 15 days; the other days always had a maximum of **5%** per day. RAM consumption always remained at **40%** during the 15 days of the test. Regarding disk usage, the total growth in use was 8%, and specifically in the log files of the Appliance related to the services, it was **120 MB**. In resource utilization, we can observe low usage, as the Appliance was scanned 24 hours a day from different IP addresses. Since the objective of the Appliance is to be implemented in the **organization's internal networks**, 24-hour scanning every day will not be executed. Therefore, it will not be necessary to add more computing resources.

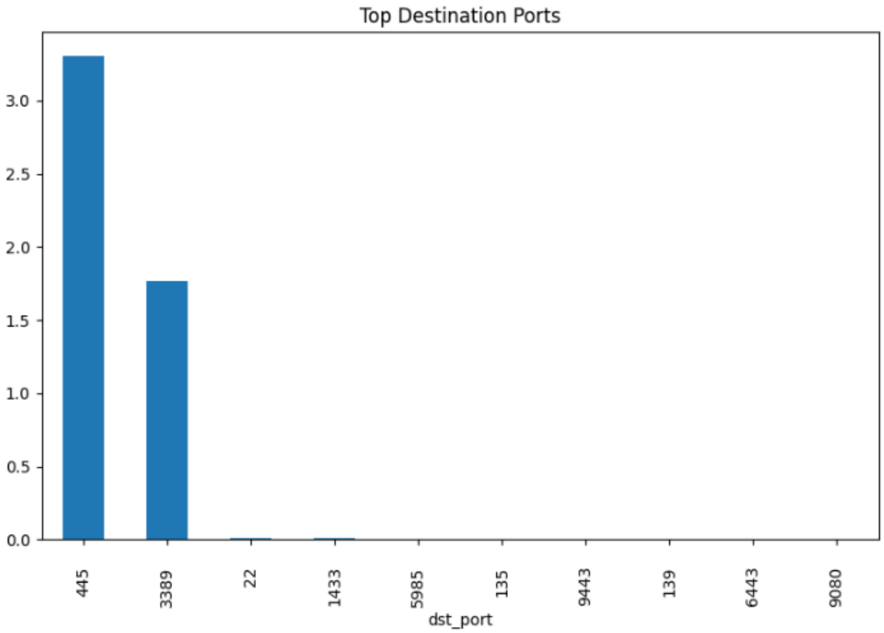
Regarding the statistics of scans or attacks received by the Appliance during the 15 days exposed on the internet, it is possible to say:

A total of Events analyzed: **5.116.389**

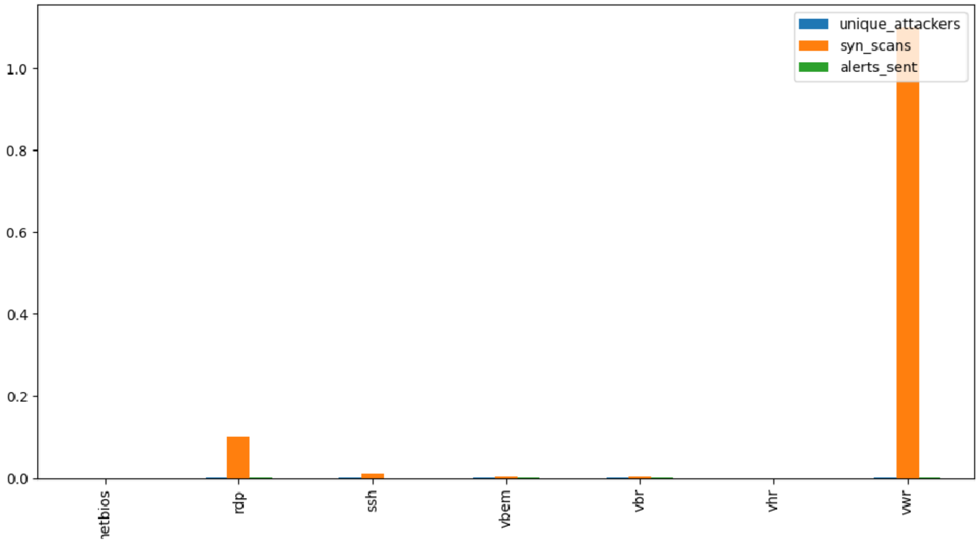
The effectiveness of the services was:



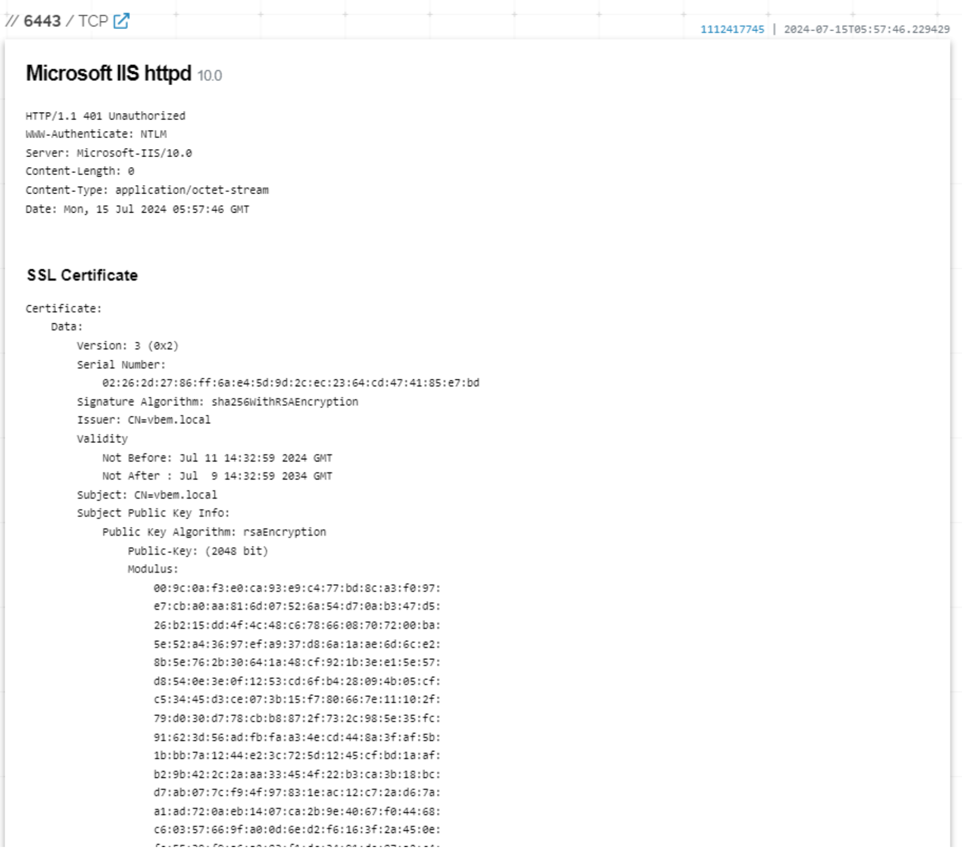
As can be observed in the previous graph, the most scanned service was "Veeam Windows Repository," since traditionally, bots or threat actors look for Microsoft Windows servers without updates to exploit vulnerabilities, which correlates with the most scanned ports, as shown in the following graph.



Then, when analyzing the different types of scans, we observe the majority associated with the TCP "SYN" flag, scanning the "Veeam Windows Repository" and the "Remote Desktop Protocol" service:



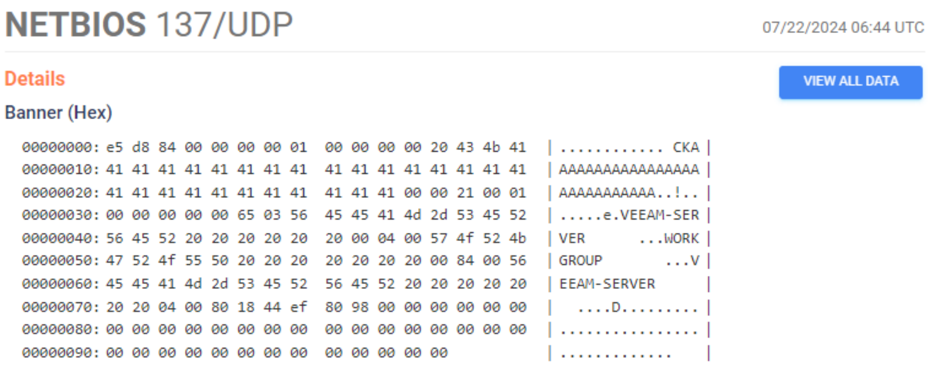
And finally, the public systems that perform monitoring and scanning of widely known ports such as shodan.io and censys.io. Example of Shodan:



```
HTTP/1.1 401 Unauthorized
WWW-Authenticate: NTLM
Server: Microsoft-IIS/10.0
Content-Length: 0
Content-Type: application/octet-stream
Date: Mon, 15 Jul 2024 05:57:46 GMT
```

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            02:26:2d:27:86:ff:6a:e4:5d:9d:2c:ec:23:64:cd:47:41:85:e7:bd
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN=vbem.local
        Validity
            Not Before: Jul 11 14:32:59 2024 GMT
            Not After : Jul  9 14:32:59 2034 GMT
        Subject: CN=vbem.local
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:9c:0a:f3:e0:ca:93:e9:c4:77:bd:8c:a3:f0:97:
                    e7:cb:a0:aa:81:6d:07:52:6a:54:d7:0a:b3:47:d5:
                    26:b2:15:dd:4f:4c:48:c6:78:66:08:70:72:00:ba:
                    5e:52:a4:36:97:ef:a9:37:d8:6a:1a:ae:6d:6c:e2:
                    8b:5e:76:2b:30:64:1a:48:cf:92:1b:3e:e1:5e:57:
                    d8:54:0e:3e:0f:12:53:cd:6f:b4:28:09:4b:05:cf:
                    c5:34:45:d3:ce:07:3b:15:f7:80:66:7e:11:10:2f:
                    79:d0:30:d7:78:cb:b8:87:2f:73:2c:98:5e:35:fc:
                    91:62:3d:56:ad:fb:fa:a3:4e:cd:44:8a:3f:af:5b:
                    1b:bb:7a:12:44:e2:3c:72:5d:12:45:cf:bd:1a:af:
                    b2:9b:42:2c:2a:aa:33:45:4f:22:b3:ca:3b:18:bc:
                    d7:ab:07:7c:f9:4f:97:83:1e:ac:12:c7:2a:d6:7a:
                    a1:ad:72:0a:eb:14:07:ca:2b:9e:40:67:f0:44:68:
                    c6:03:57:66:9f:a0:0d:6e:d2:f6:16:3f:2a:45:0e:
```

Censys:



NETBIOS 137/UDP

07/22/2024 06:44 UTC

Details

Banner (Hex)

```
00000000: e5 d8 84 00 00 00 00 01  00 00 00 00 20 43 4b 41  |............ CKA|
00000010: 41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41  |AAAAAAAAAAAAAAAA|
00000020: 41 41 41 41 41 41 41 41  41 41 41 00 00 21 00 01  |AAAAAAAAAAA..!..|
00000030: 00 00 00 00 00 65 03 56  45 45 41 4d 2d 53 45 52  |.....e.VEEAM-SER|
00000040: 56 45 52 20 20 20 20 20  20 00 04 00 57 4f 52 4b  |VER      ...WORK|
00000050: 47 52 4f 55 50 20 20 20  20 20 20 20 00 84 00 56  |GROUP       ...V|
00000060: 45 45 41 4d 2d 53 45 52  56 45 52 20 20 20 20 20  |EEAM-SERVER     |
00000070: 20 20 04 00 80 18 44 ef  80 98 00 00 00 00 00 00  |  ....D.........|
00000080: 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000090: 00 00 00 00 00 00 00 00  00 00 00 00 00           |.............   |
```

Characteristics

This system has the following services:

Veeam Backup Server
Veeam Hardened Repository
Veeam Windows Repository
Veeam Backup Enterprise Manager
SSH
Remote Desktop (RDP)
Netbios

And the following characteristics:

Terminal User Interface
Logs
Log Forwarding
Email Notifications
Multiple Network Interface Configuration
List of Used Ports
Service Management
Configuration File Editing
Remote Management

Each of the services allows for the detection of connection attempts and scans to the different ports used by each service, capturing credentials, IP addresses, source ports, source IP addresses, and specific queries to certain services. All captures are generated in Syslog format to be forwarded to a centralized SysLog server or to send notifications by email.

Additionally, the Appliance supports the use of multiple network interfaces, so that with just one Appliance, it's possible to implement the services across multiple networks, thus allowing for a distributed deployment of the services.

Software and Hardware Requirements

Virtual Hardware Requirements | OVA

The minimum requirements needed to use the Appliance are as follows:

Processor: 1 vCPU
RAM: 2 GB
Storage: 50 GB
Network: 1 GB / 10GB / VMXNET 3
Hypervisor: vSphere 8.0 or higher.

Rocky Linux Requirements | Manual Installation

Operating System: Minimal installation of Rocky Linux 9.4 (Tested only on this distro, may support other Red Hat-based distributions)
Processor: 1 CPU
RAM Memory: 2 GB
Storage: 50 GB
Network: 1 GB / 10 GB
Firewall: Disabled
SELinux: Disabled

With the above requirements, it will be possible to use all services on multiple network interfaces.

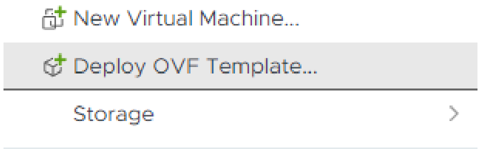
Deployment

Virtual Appliance Deployment

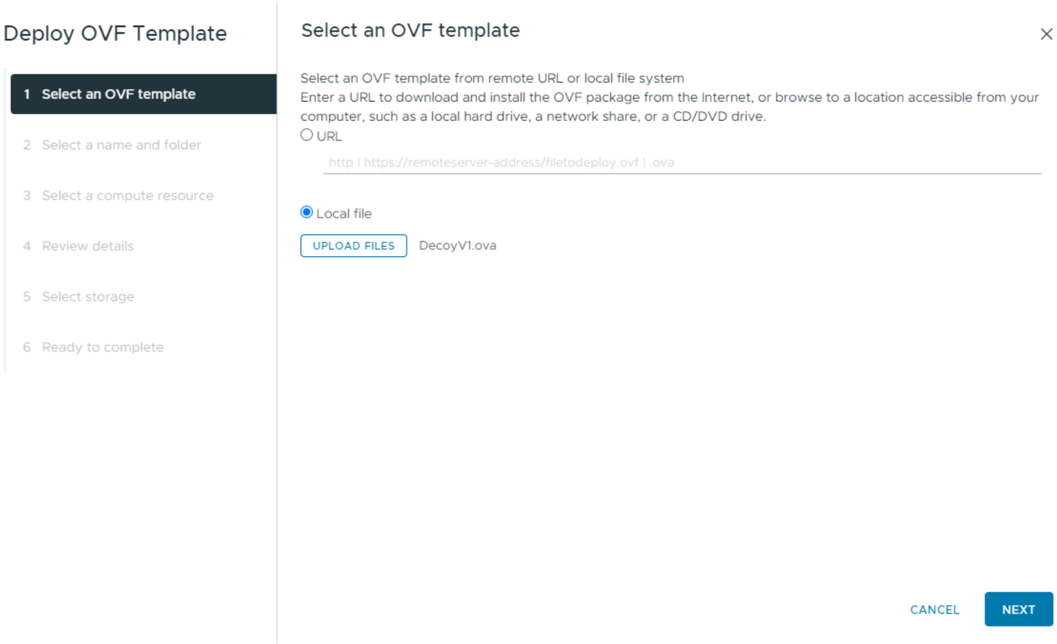
Download the OVA image from:

https://dl.24xsiempre.com/DecoyV1.ova

Then import the Appliance directly from vCenter by selecting "Deploy OVF Template":



And then enter the path where the OVA was downloaded, to select it, then click on "Next":



Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

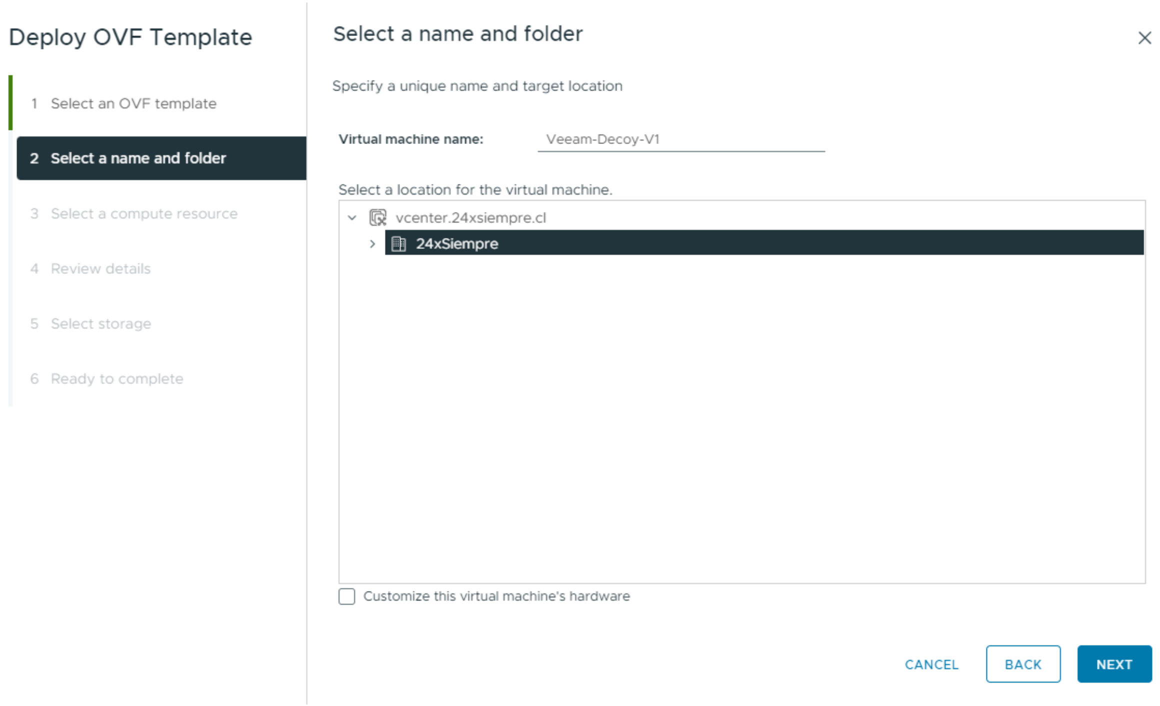
○ URL

http | https://remoteserver-address/filetodeploy.ovf | .ova

● Local file

UPLOAD FILES DecoyV1.ova

Enter the VM name, select the vCenter, Datacenter, and VM Folder where the VM will be hosted, then click on "Next":



Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 Select storage
6 Ready to complete

Select a name and folder

Specify a unique name and target location

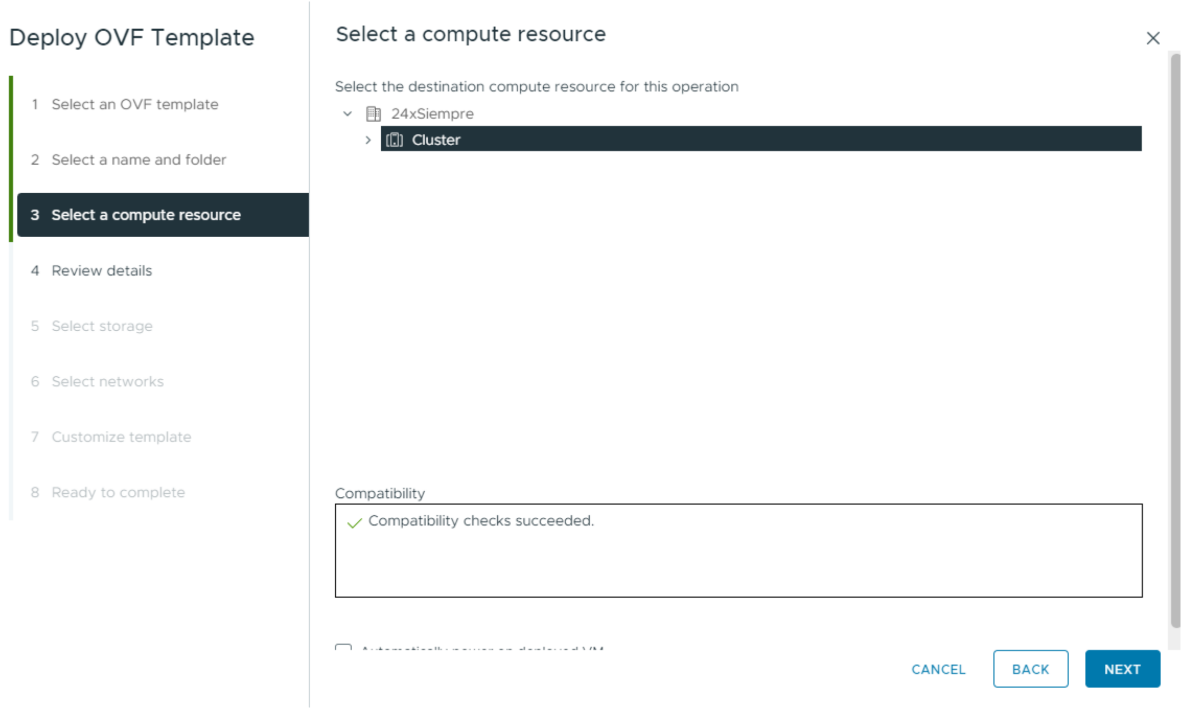
Virtual machine name: Veeam-Decoy-V1

Select a location for the virtual machine.

- vcenter.24xsiempre.cl
  - 24xSiempre

□ Customize this virtual machine's hardware

Then select the compute resources and click on "Next":



Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 Select storage
6 Select networks
7 Customize template
8 Ready to complete

Select a compute resource

Select the destination compute resource for this operation

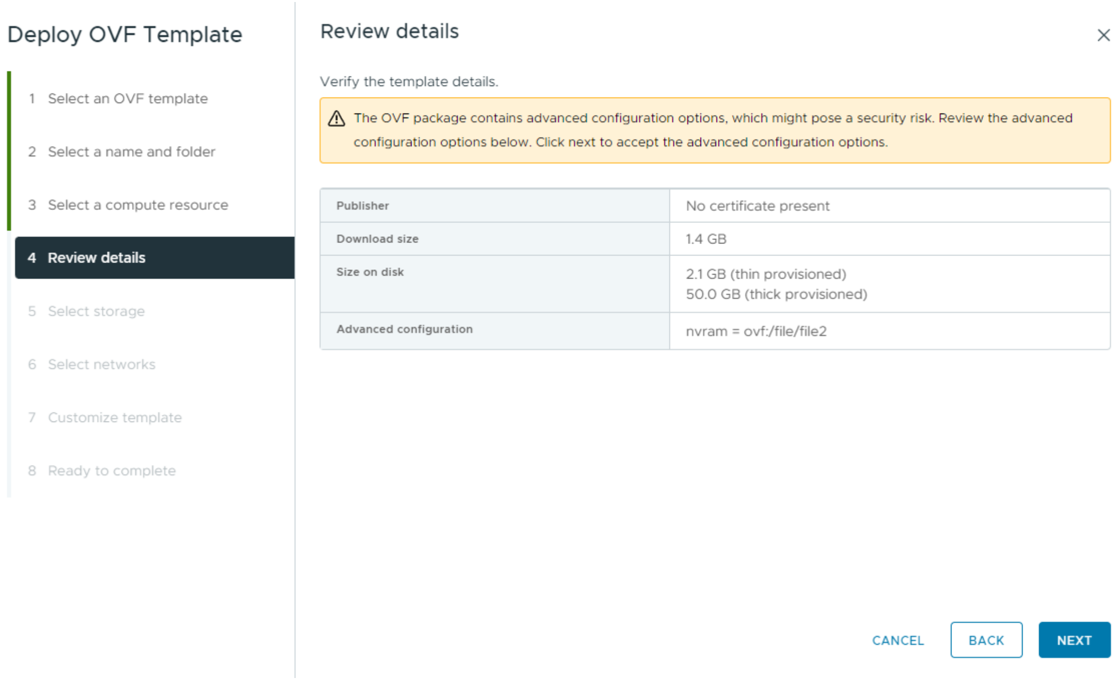
- 24xSiempre
  - Cluster

Compatibility

✓ Compatibility checks succeeded.

□ Automatically power on deployed VM

Now the wizard will display a message that the OVA has advanced configurations, click "Next":



Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Select networks

7 Customize template

8 Ready to complete

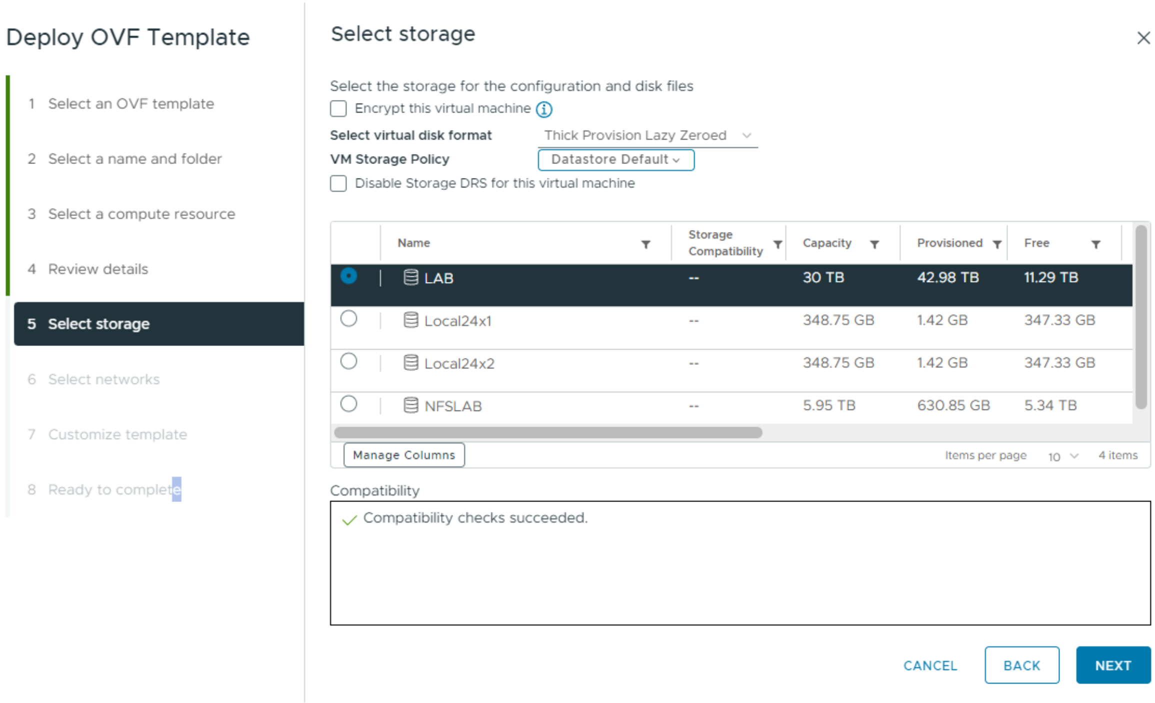
Review details

Verify the template details.

⚠ The OVF package contains advanced configuration options, which might pose a security risk. Review the advanced configuration options below. Click next to accept the advanced configuration options.

Publisher	No certificate present
Download size	1.4 GB
Size on disk	2.1 GB (thin provisioned) 50.0 GB (thick provisioned)
Advanced configuration	nvram = ovf:/file/file2

Now it's necessary to select the Storage where the Appliance will be hosted, and then click on "Next":



Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Select networks

7 Customize template

8 Ready to complete

Select storage

Select the storage for the configuration and disk files

□ Encrypt this virtual machine ⓘ

Select virtual disk format Thick Provision Lazy Zeroed

VM Storage Policy Datastore Default

□ Disable Storage DRS for this virtual machine

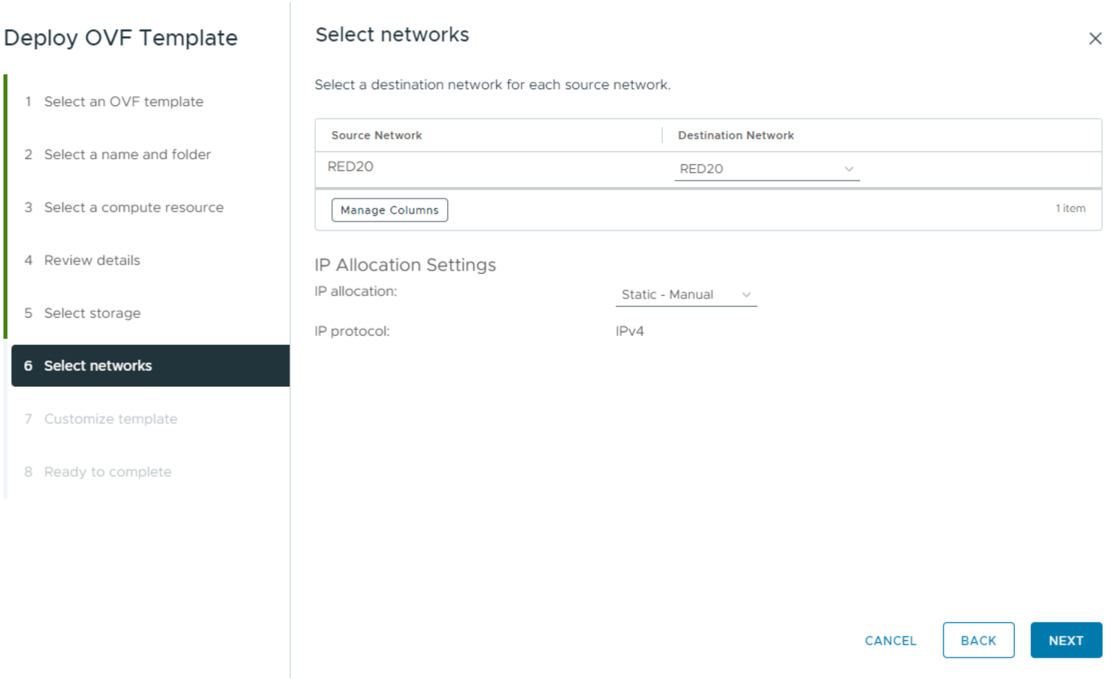
	Name	Storage Compatibility	Capacity	Provisioned	Free
●	LAB	--	30 TB	42.98 TB	11.29 TB
○	Local24x1	--	348.75 GB	1.42 GB	347.33 GB
○	Local24x2	--	348.75 GB	1.42 GB	347.33 GB
○	NFSLAB	--	5.95 TB	630.85 GB	5.34 TB

Manage Columns Items per page 10 4 items

Compatibility

✓ Compatibility checks succeeded.

In this step, configure and select which Network / VLAN will be used for the first network interface of the Appliance, configure the "Destination Network" and click on "Next":



Select networks

Select a destination network for each source network.

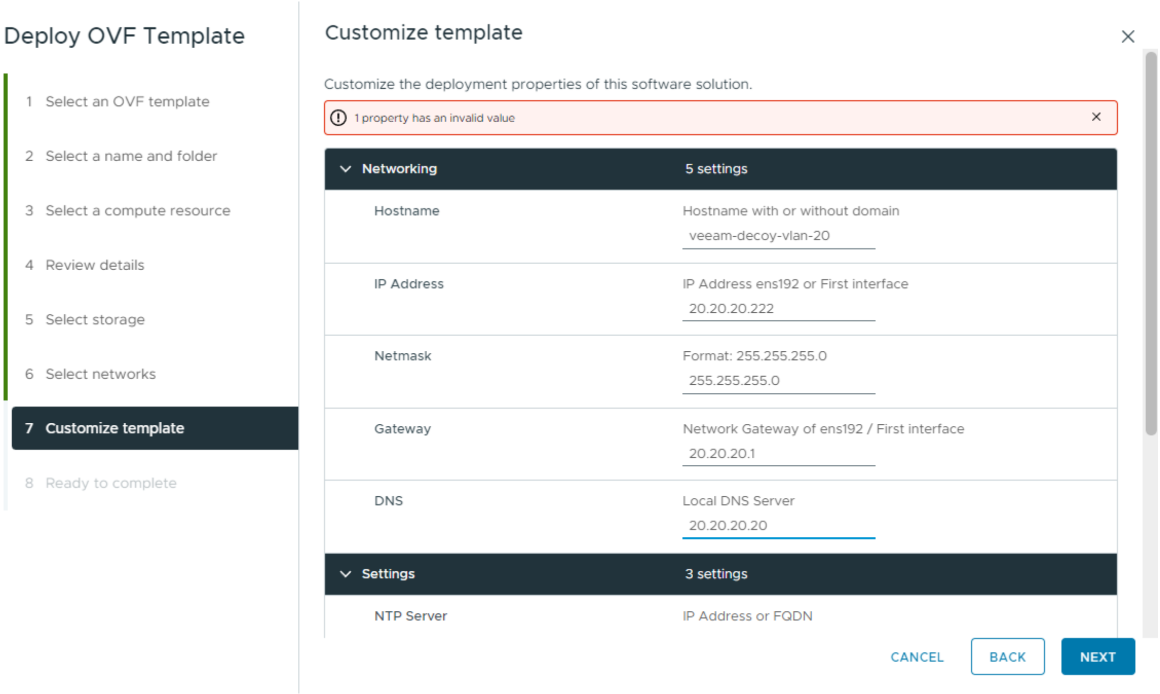
Source Network	Destination Network
RED20	RED20

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

Now we will configure the Appliance to add the necessary network data in the first part of "Networking":



Customize template

Customize the deployment properties of this software solution.

1 property has an invalid value

Networking 5 settings

Hostname: Hostname with or without domain — veeam-decoy-vlan-20

IP Address: IP Address ens192 or First interface — 20.20.20.222

Netmask: Format: 255.255.255.0 — 255.255.255.0

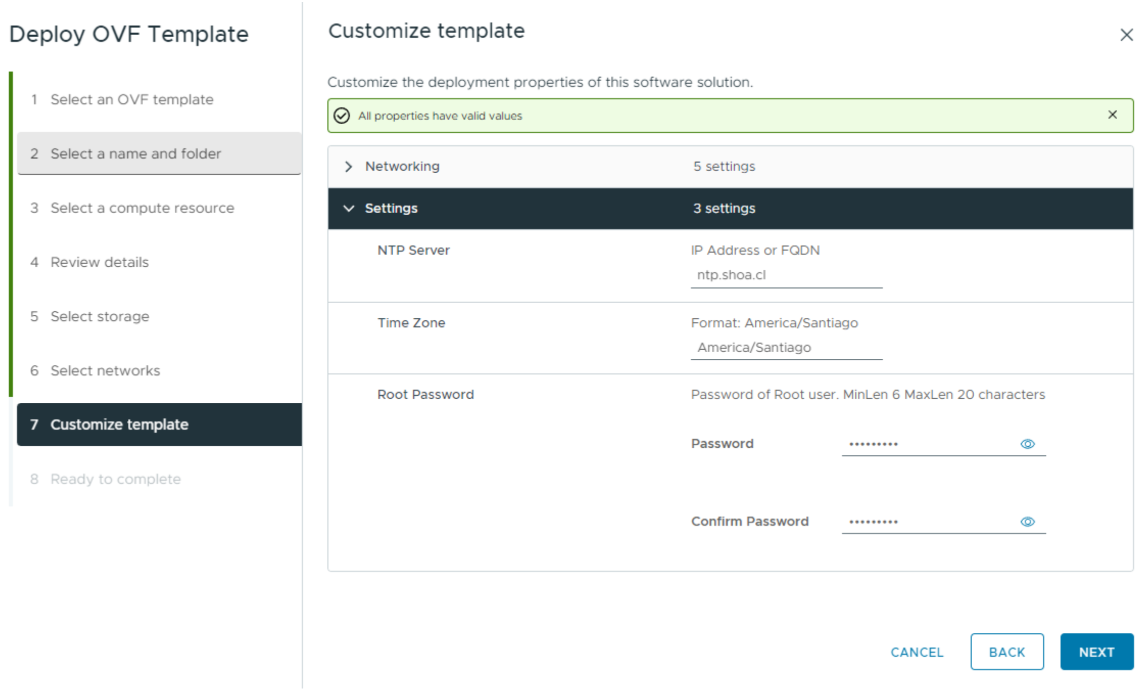
Gateway: Network Gateway of ens192 / First interface — 20.20.20.1

DNS: Local DNS Server — 20.20.20.20

Settings 3 settings

NTP Server: IP Address or FQDN

Then in "Settings" enter the requested data and click on "Next":



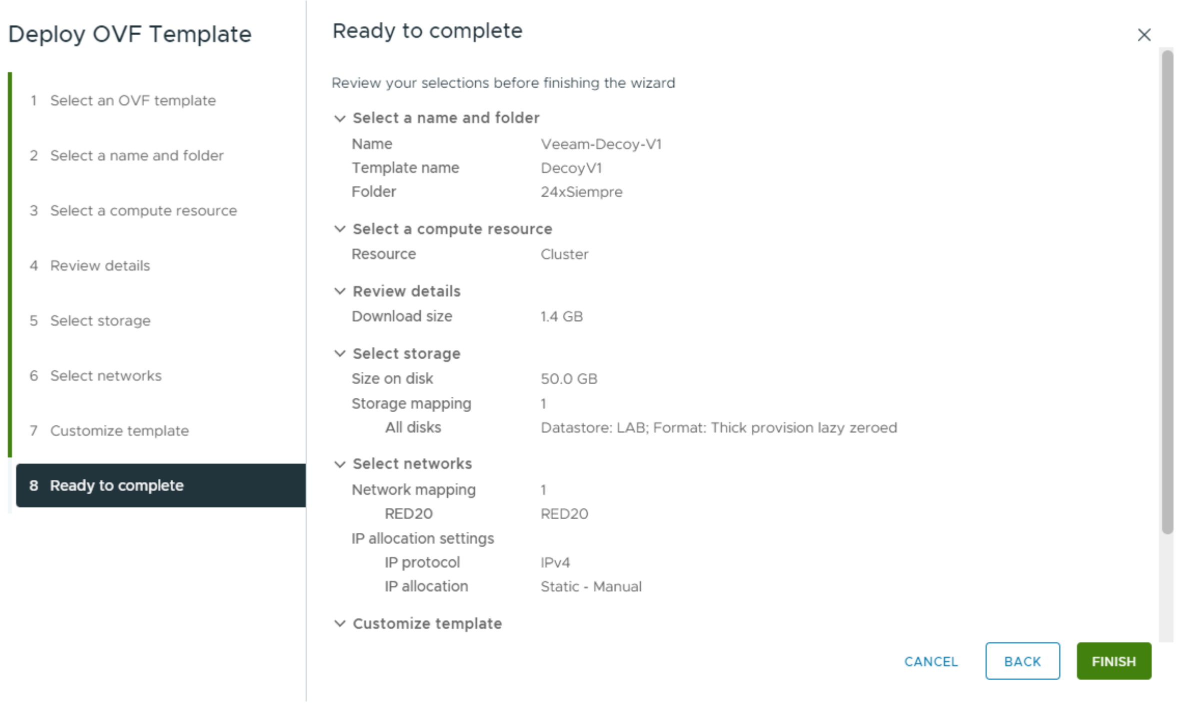
Customize template

Customize the deployment properties of this software solution.

All properties have valid values

Networking	5 settings
Settings	3 settings
NTP Server	IP Address or FQDN ntp.shoa.cl
Time Zone	Format: America/Santiago America/Santiago
Root Password	Password of Root user. MinLen 6 MaxLen 20 characters Password ••••••••• Confirm Password •••••••••

And in the last option, review the applied configurations and then click on "Finish" and wait for the Appliance deployment:



Ready to complete

Review your selections before finishing the wizard

Select a name and folder

Name	Veeam-Decoy-V1
Template name	DecoyV1
Folder	24xSiempre

Select a compute resource

Resource	Cluster

Review details

Download size	1.4 GB

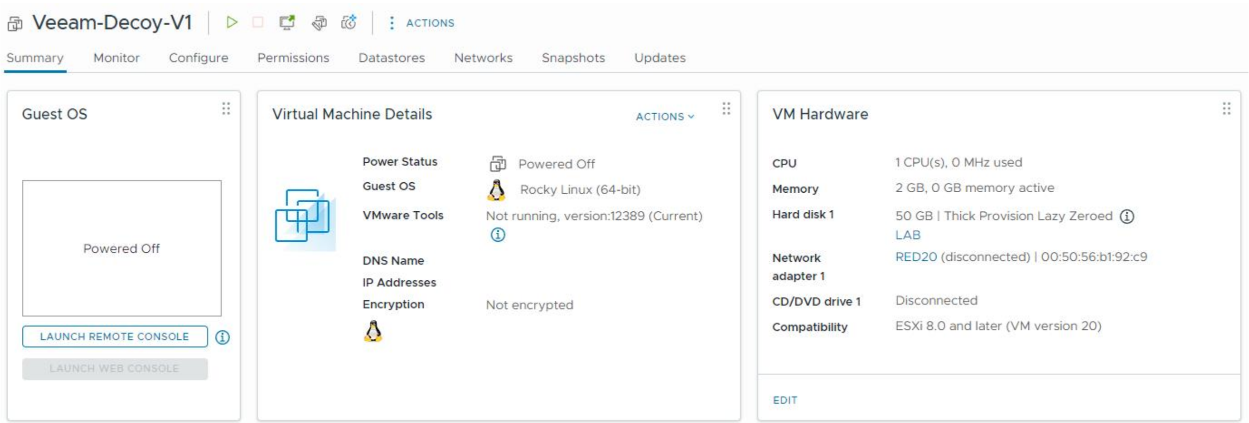
Select storage

Size on disk	50.0 GB
Storage mapping	1
All disks	Datastore: LAB; Format: Thick provision lazy zeroed

Select networks

Network mapping	1
RED20	RED20
IP allocation settings	
IP protocol	IPv4
IP allocation	Static - Manual

Customize template



Guest OS

Powered Off

Virtual Machine Details

Power Status: Powered Off
Guest OS: Rocky Linux (64-bit)
VMware Tools: Not running, version:12389 (Current)
DNS Name:
IP Addresses:
Encryption: Not encrypted

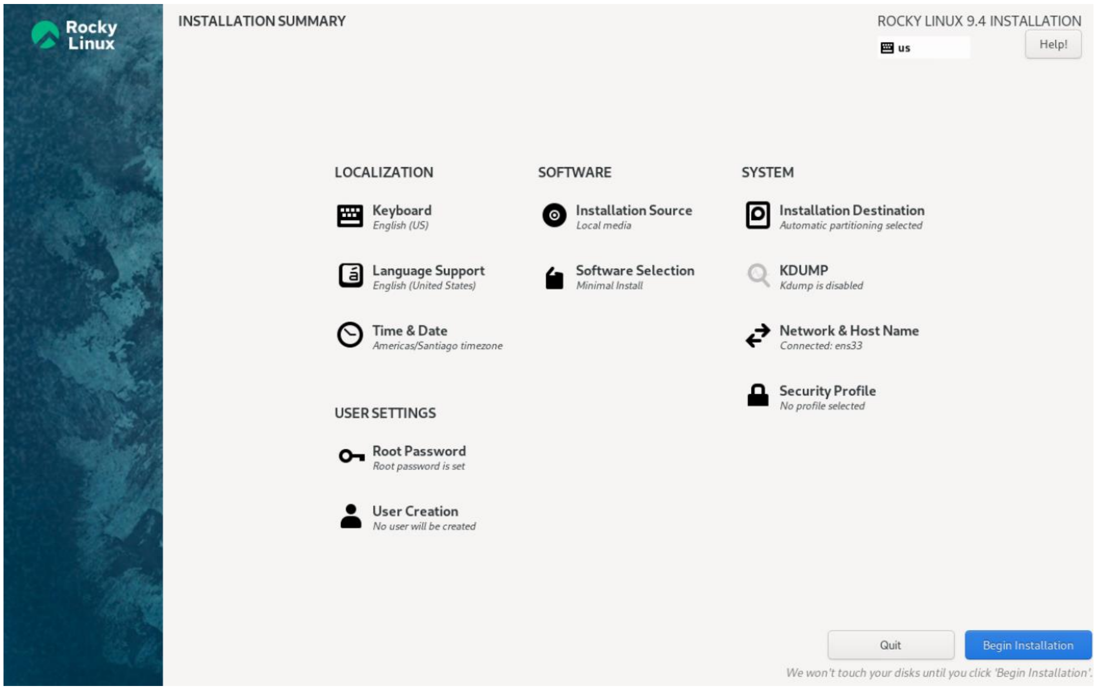
VM Hardware

CPU: 1 CPU(s), 0 MHz used
Memory: 2 GB, 0 GB memory active
Hard disk 1: 50 GB | Thick Provision Lazy Zeroed
LAB
Network adapter 1: RED20 (disconnected) | 00:50:56:b1:92:c9
CD/DVD drive 1: Disconnected
Compatibility: ESXi 8.0 and later (VM version 20)

Power on the Appliance.

Manual Installation on Rocky Linux 9.4

To install the system directly on a Linux server with Rocky Linux 9.4, it is necessary to verify that the Rocky Linux installation type is set to the "Minimal" option:



LOCALIZATION

Keyboard: English (US)

Language Support: English (United States)

Time & Date: Americas/Santiago timezone

SOFTWARE

Installation Source: Local media

Software Selection: Minimal Install

SYSTEM

Installation Destination: Automatic partitioning selected

KDUMP: Kdump is disabled

Network & Host Name: Connected: ens33

Security Profile: No profile selected

USER SETTINGS

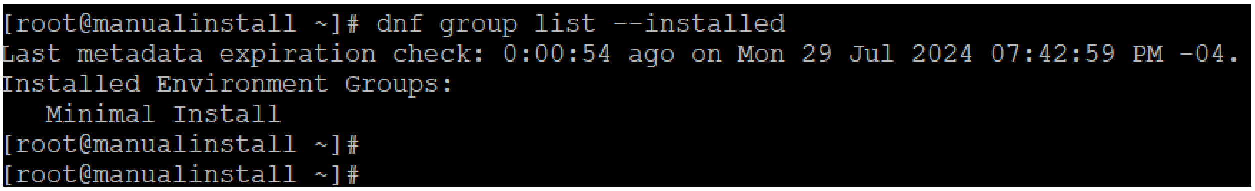
Root Password: Root password is set

User Creation: No user will be created

We won't touch your disks until you click 'Begin Installation'.

From the Linux command line, it is also possible to verify the installation type using the following command:

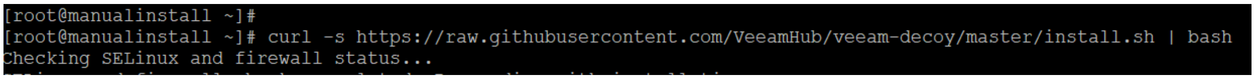
```
dnf group list --installed
```



```
[root@manualinstall ~]# dnf group list --installed
Last metadata expiration check: 0:00:54 ago on Mon 29 Jul 2024 07:42:59 PM -04.
Installed Environment Groups:
   Minimal Install
[root@manualinstall ~]#
[root@manualinstall ~]#
```

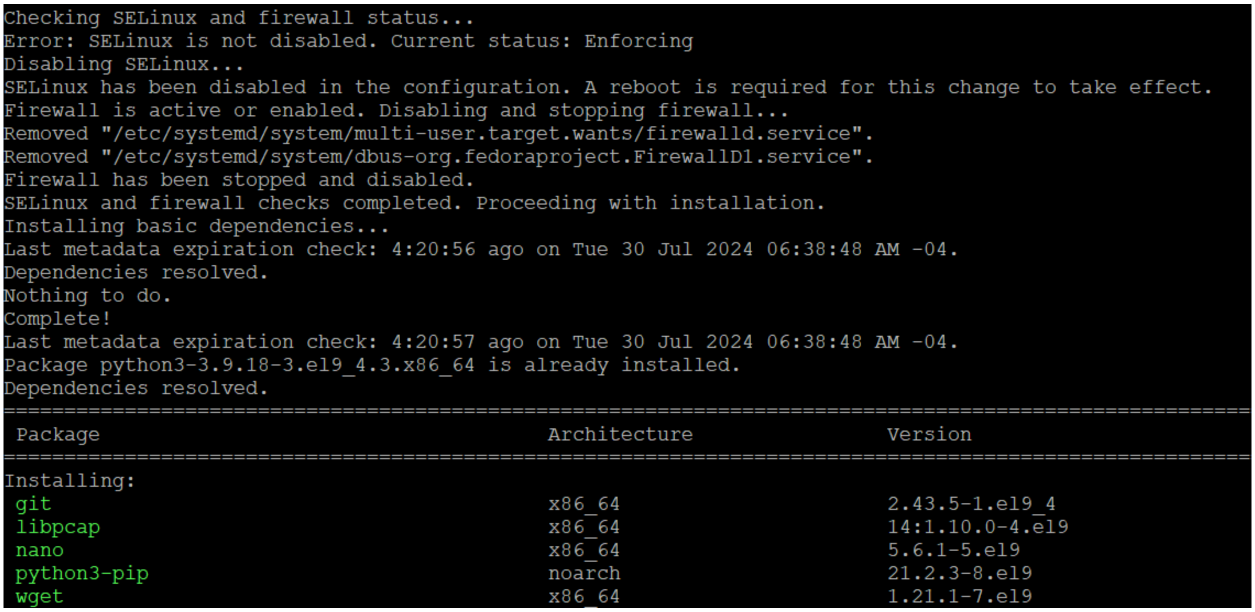
And perform the installation with the following command:

```
curl -s https://raw.githubusercontent.com/VeeamHub/veeam-decoy/master/install.sh| bash
```



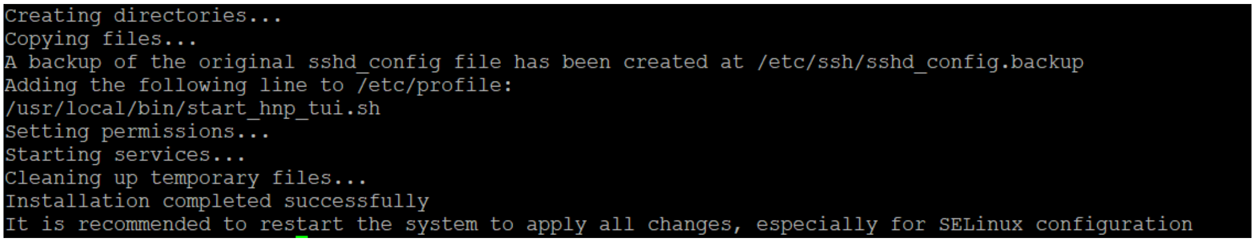
```
[root@manualinstall ~]#
[root@manualinstall ~]# curl -s https://raw.githubusercontent.com/VeeamHub/veeam-decoy/master/install.sh | bash
Checking SELinux and firewall status...
```

It will begin with the installation and configuration of the services:



```
Checking SELinux and firewall status...
Error: SELinux is not disabled. Current status: Enforcing
Disabling SELinux...
SELinux has been disabled in the configuration. A reboot is required for this change to take effect.
Firewall is active or enabled. Disabling and stopping firewall...
Removed "/etc/systemd/system/multi-user.target.wants/firewalld.service".
Removed "/etc/systemd/system/dbus-org.fedoraproject.FirewallD1.service".
Firewall has been stopped and disabled.
SELinux and firewall checks completed. Proceeding with installation.
Installing basic dependencies...
Last metadata expiration check: 4:20:56 ago on Tue 30 Jul 2024 06:38:48 AM -04.
Dependencies resolved.
Nothing to do.
Complete!
Last metadata expiration check: 4:20:57 ago on Tue 30 Jul 2024 06:38:48 AM -04.
Package python3-3.9.18-3.el9_4.3.x86_64 is already installed.
Dependencies resolved.
=======================================================================================================
 Package                                     Architecture                Version
=======================================================================================================
Installing:
 git                                         x86_64                      2.43.5-1.el9_4
 libpcap                                     x86_64                      14:1.10.0-4.el9
 nano                                        x86_64                      5.6.1-5.el9
 python3-pip                                 noarch                      21.2.3-8.el9
 wget                                        x86_64                      1.21.1-7.el9
```

Upon successful completion, it will display:



```
Creating directories...
Copying files...
A backup of the original sshd_config file has been created at /etc/ssh/sshd_config.backup
Adding the following line to /etc/profile:
/usr/local/bin/start_hnp_tui.sh
Setting permissions...
Starting services...
Cleaning up temporary files...
Installation completed successfully
It is recommended to restart the system to apply all changes, especially for SELinux configuration
```

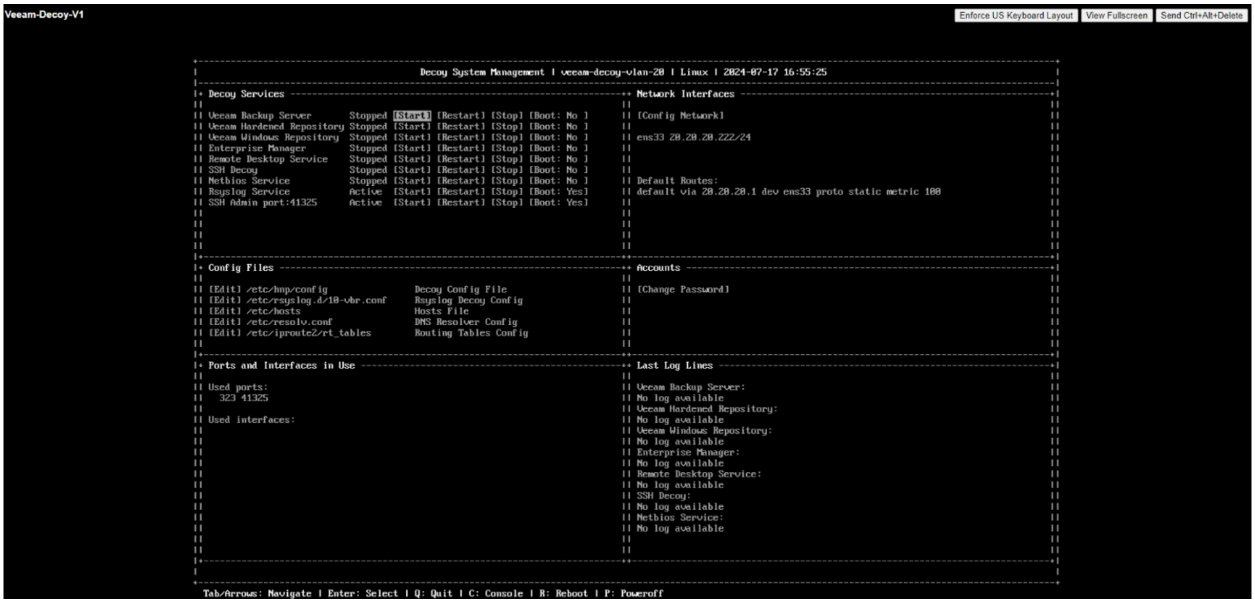
And finally, restart the server with the command:

```
reboot
```

After restarting the server, connect via SSH on port **41325**. If it's a virtual machine, it will also be possible to access it through the Console. Finally, if it's a physical machine, access it through IPMI.

Configuration

With the Appliance deployed and powered on in the virtual environment, there are two options to access and apply the necessary configurations: through the vCenter "Web Console" or via SSH with a specific port. For the correct functioning of the services, the user to be used is "**root**". In case of manual installation, if it's not possible to use "**root**", it must be a user with "**sudo**" permissions.



```
+------------------------------------------------------------------------------------------------------------------+
|                      Decoy System Management | veeam-decoy-vlan-20 | Linux | 2024-07-17 16:55:25                  |
|------------------------------------------------------------------------------------------------------------------|
|+ Decoy Services ------------------------------------------------++ Network Interfaces -------------------------+|
||                                                                ||                                             ||
|| Veeam Backup Server       Stopped [Start] [Restart] [Stop] [Boot: No ]  || [Config Network]                   ||
|| Veeam Hardened Repository Stopped [Start] [Restart] [Stop] [Boot: No ]  ||                                    ||
|| Veeam Windows Repository  Stopped [Start] [Restart] [Stop] [Boot: No ]  || ens33 20.20.20.222/24              ||
|| Enterprise Manager        Stopped [Start] [Restart] [Stop] [Boot: No ]  ||                                    ||
|| Remote Desktop Service    Stopped [Start] [Restart] [Stop] [Boot: No ]  ||                                    ||
|| SSH Decoy                 Stopped [Start] [Restart] [Stop] [Boot: No ]  ||                                    ||
|| Netbios Service           Stopped [Start] [Restart] [Stop] [Boot: No ]  || Default Routes:                    ||
|| Rsyslog Service           Active  [Start] [Restart] [Stop] [Boot: Yes]  || default via 20.20.20.1 dev ens33 proto static metric 100 ||
|| SSH Admin port:41325      Active  [Start] [Restart] [Stop] [Boot: Yes]  ||                                    ||
||                                                                ||                                             ||
||                                                                ||                                             ||
||                                                                ||                                             ||
||                                                                ||                                             ||
|+----------------------------------------------------------------++---------------------------------------------+|
|+ Config Files --------------------------------------------------++ Accounts -----------------------------------+|
||                                                                ||                                             ||
|| [Edit] /etc/hnp/config            Decoy Config File            || [Change Password]                           ||
|| [Edit] /etc/rsyslog.d/10-vbr.conf Rsyslog Decoy Config         ||                                             ||
|| [Edit] /etc/hosts                 Hosts File                   ||                                             ||
|| [Edit] /etc/resolv.conf           DNS Resolver Config          ||                                             ||
|| [Edit] /etc/iproute2/rt_tables    Routing Tables Config        ||                                             ||
||                                                                ||                                             ||
|+----------------------------------------------------------------++---------------------------------------------+|
|+ Ports and Interfaces in Use -----------------------------------++ Last Log Lines -----------------------------+|
||                                                                ||                                             ||
|| Used ports:                                                    || Veeam Backup Server:                        ||
||   323 41325                                                    || No log available                            ||
||                                                                || Veeam Hardened Repository:                  ||
|| Used interfaces:                                               || No log available                            ||
||                                                                || Veeam Windows Repository:                   ||
||                                                                || No log available                            ||
||                                                                || Enterprise Manager:                         ||
||                                                                || No log available                            ||
||                                                                || Remote Desktop Service:                     ||
||                                                                || No log available                            ||
||                                                                || SSH Decoy:                                  ||
||                                                                || No log available                            ||
||                                                                || Netbios Service:                            ||
||                                                                || No log available                            ||
||                                                                ||                                             ||
||                                                                ||                                             ||
|+----------------------------------------------------------------++---------------------------------------------+|
|                                                                                                                  |
+------------------------------------------------------------------------------------------------------------------+
  Tab/Arrows: Navigate | Enter: Select | Q: Quit | C: Console | R: Reboot | P: Poweroff
```

If it's necessary to access via SSH, the port to use is **41325** with the root user and the password configured previously.

The TUI will be displayed through "Web Console" or "SSH" with the administrative port. This interface consists of the following options:

Decoy Services: Here, all services configured in the Appliance are listed. It has the entire lifecycle of services through systemd and, if necessary, allows configuring the service at system startup.

Network Interfaces: This allows network configuration, including if there are multiple network interfaces, enabling viewing active interfaces and their respective network routes.

Config Files: This is the most important part, as it allows direct editing of configuration files for the proper functioning of the Appliance. The editor is nano.

Accounts: Allows changing the root user's password.

Ports and Interfaces in Use: Shows the status of interfaces, open ports of all running services, updates instantly when a service starts.

Last Log Lines: Shows the last log line of the service, to identify errors or if the service is being accessed.

And finally, in the TUI "Footer", there are 4 options:

Q: Quit, to exit the TUI
C: Console, to enter the Linux CLI (Experimental)
R: Reboot, to restart the Appliance after confirmation
P: Poweroff, to shut down the Appliance after confirmation

Decoy Services

Here, the entire lifecycle of services is managed, therefore, in the menu it will always appear, for example:

Veeam Backup Server   Stopped [Start] [Restart] [Stop] [Boot: No]

“**Stopped**” is the current service state. It can have two additional states: "**Active**," which means it is running, and "Failed," which means the log files or configuration file should be reviewed.

“**Start**” is the button to start the service. When executed, it shows a message indicating whether it was successful.

“**Restart**” is the button to restart the service. When executed, it shows a message indicating whether it was successful or not.

“**Stop**” is the button to stop the service. When executed, it shows a message indicating whether it was successful.

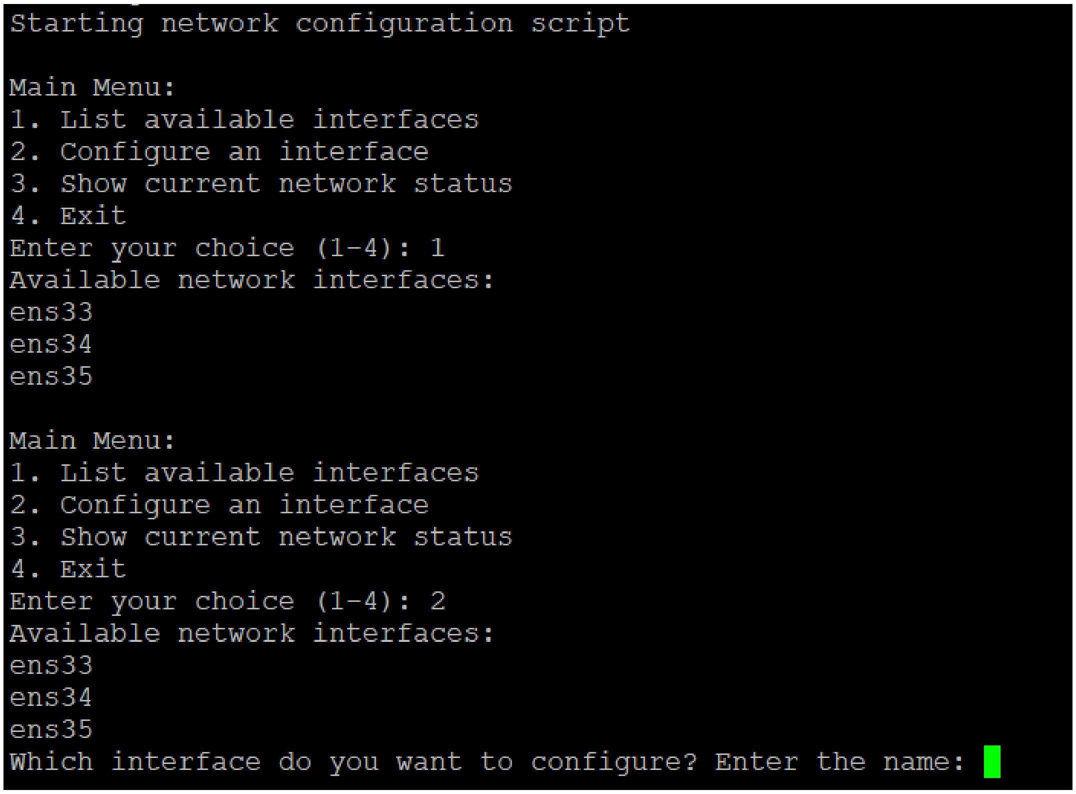
“**Boot: No**” Shows the current state of whether the service starts with the operating system. If the state is "**No**", the service must be started manually. If the state is "**Yes**", the service already runs when the operating system starts.

Network Interfaces

Here, the network configuration is managed for one or multiple interfaces where, upon executing:

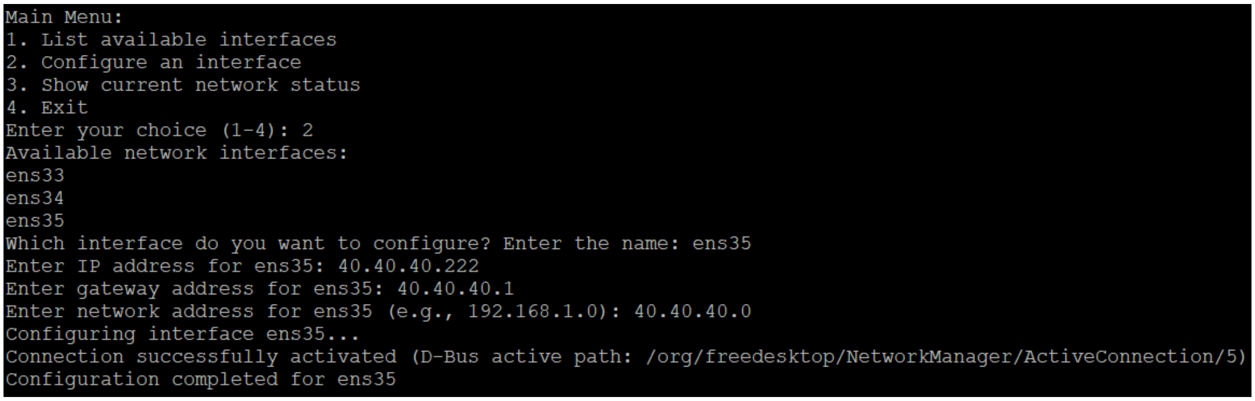
[Config Network]

It will display a configuration wizard; you only need to add the requested information:



```
Starting network configuration script

Main Menu:
1. List available interfaces
2. Configure an interface
3. Show current network status
4. Exit
Enter your choice (1-4): 1
Available network interfaces:
ens33
ens34
ens35

Main Menu:
1. List available interfaces
2. Configure an interface
3. Show current network status
4. Exit
Enter your choice (1-4): 2
Available network interfaces:
ens33
ens34
ens35
Which interface do you want to configure? Enter the name:
```

If you want to configure one or several interfaces, the following data will be requested:



```
Main Menu:
1. List available interfaces
2. Configure an interface
3. Show current network status
4. Exit
Enter your choice (1-4): 2
Available network interfaces:
ens33
ens34
ens35
Which interface do you want to configure? Enter the name: ens35
Enter IP address for ens35: 40.40.40.222
Enter gateway address for ens35: 40.40.40.1
Enter network address for ens35 (e.g., 192.168.1.0): 40.40.40.0
Configuring interface ens35...
Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/5)
Configuration completed for ens35
```

IP address, Gateway, and Network of the selected interface. After configuring the network interfaces, it is recommended to restart the Appliance to ensure the persistence of the configured data. If there is no connection, validate the configuration through the Web Console.

Config Files

This is the most important part of the configuration. After defining the network interfaces, it is necessary to configure which services will function on which interfaces. The services can run on multiple interfaces as long as no other service is using common ports. For example, if you configure "Veeam Windows Repository" and "Veeam Hardened Repository" on the same network interface, one of the services will not work, as both services use ports **6160** and **6162**.

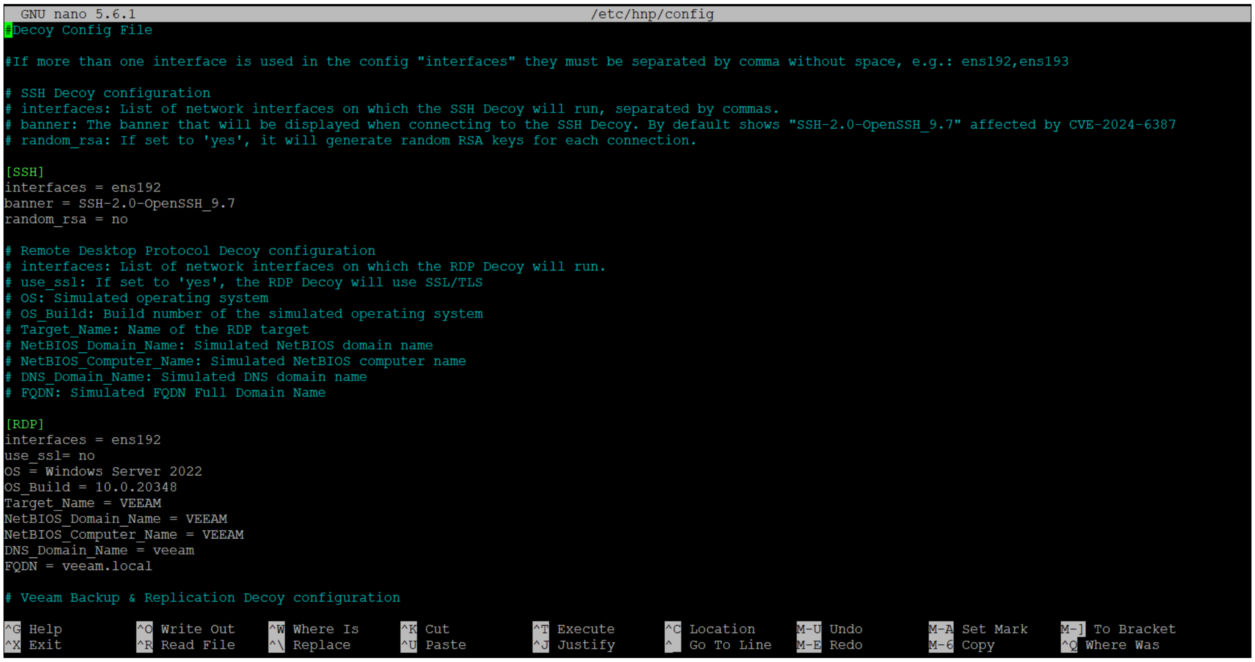
Now, moving on to the service configuration, within the TUI, enter the "Config Files" box, select "Decoy Config File" to edit the main configuration file:

[Edit] /etc/hnp/config Decoy Config File

Upon selection, the "nano" editor will be displayed with the contents of the configuration file. This file contains all the information for each variable to be configured. For the services, it is only necessary to change the variable:

interfaces = en192,ens224

For each of the services, to make them function on one or multiple interfaces. In the case of using multiple interfaces for one or several services, follow the format indicated in the configuration file to enter the interfaces with commas and without spaces.

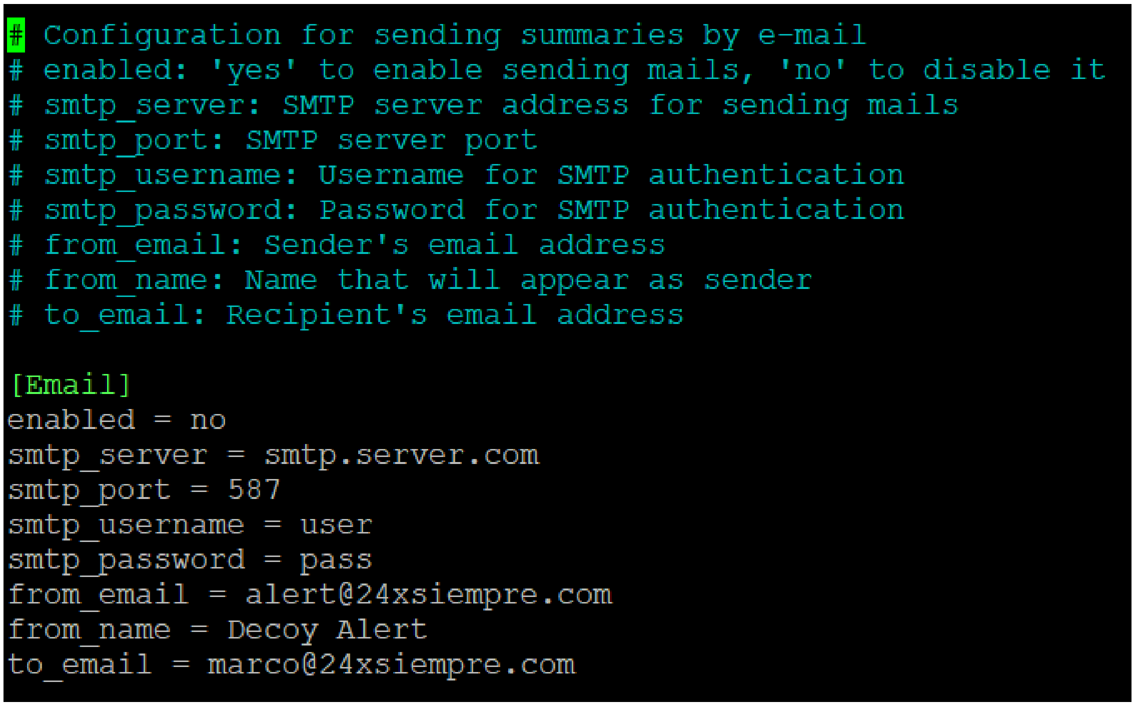


```
  GNU nano 5.6.1                                   /etc/hnp/config
#Decoy Config File

#If more than one interface is used in the config "interfaces" they must be separated by comma without space, e.g.: ens192,ens193

# SSH Decoy configuration
# interfaces: List of network interfaces on which the SSH Decoy will run, separated by commas.
# banner: The banner that will be displayed when connecting to the SSH Decoy. By default shows "SSH-2.0-OpenSSH_9.7" affected by CVE-2024-6387
# random_rsa: If set to 'yes', it will generate random RSA keys for each connection.

[SSH]
interfaces = ens192
banner = SSH-2.0-OpenSSH_9.7
random_rsa = no

# Remote Desktop Protocol Decoy configuration
# interfaces: List of network interfaces on which the RDP Decoy will run.
# use_ssl: If set to 'yes', the RDP Decoy will use SSL/TLS
# OS: Simulated operating system
# OS_Build: Build number of the simulated operating system
# Target_Name: Name of the RDP target
# NetBIOS_Domain_Name: Simulated NetBIOS domain name
# NetBIOS_Computer_Name: Simulated NetBIOS computer name
# DNS_Domain_Name: Simulated DNS domain name
# FQDN: Simulated FQDN Full Domain Name

[RDP]
interfaces = ens192
use_ssl= no
OS = Windows Server 2022
OS_Build = 10.0.20348
Target_Name = VEEAM
NetBIOS_Domain_Name = VEEAM
NetBIOS_Computer_Name = VEEAM
DNS_Domain_Name = veeam
FQDN = veeam.local

# Veeam Backup & Replication Decoy configuration

^G Help         ^O Write Out    ^W Where Is     ^K Cut          ^T Execute      ^C Location     M-U Undo        M-A Set Mark    M-] To Bracket
^X Exit         ^R Read File    ^\ Replace      ^U Paste        ^J Justify      ^  Go To Line   M-E Redo        M-6 Copy        ^Q Where Was
```

All options in the configuration file are configurable, meaning you can change the type of operating system, banners, and domain to simulate.

Alerts

In the same configuration file /etc/hnp/config, it's possible to configure email notifications if necessary. Under "[Email]" there are multiple options including enabling or disabling the service.



```
# Configuration for sending summaries by e-mail
# enabled: 'yes' to enable sending mails, 'no' to disable it
# smtp_server: SMTP server address for sending mails
# smtp_port: SMTP server port
# smtp_username: Username for SMTP authentication
# smtp_password: Password for SMTP authentication
# from_email: Sender's email address
# from_name: Name that will appear as sender
# to_email: Recipient's email address

[Email]
enabled = no
smtp_server = smtp.server.com
smtp_port = 587
smtp_username = user
smtp_password = pass
from_email = alert@24xsiempre.com
from_name = Decoy Alert
to_email = marco@24xsiempre.com
```

Emails will be sent every 5 minutes, only if there are connections to the service. Otherwise, no email will be sent, and it will be reported that there were no connections to report.

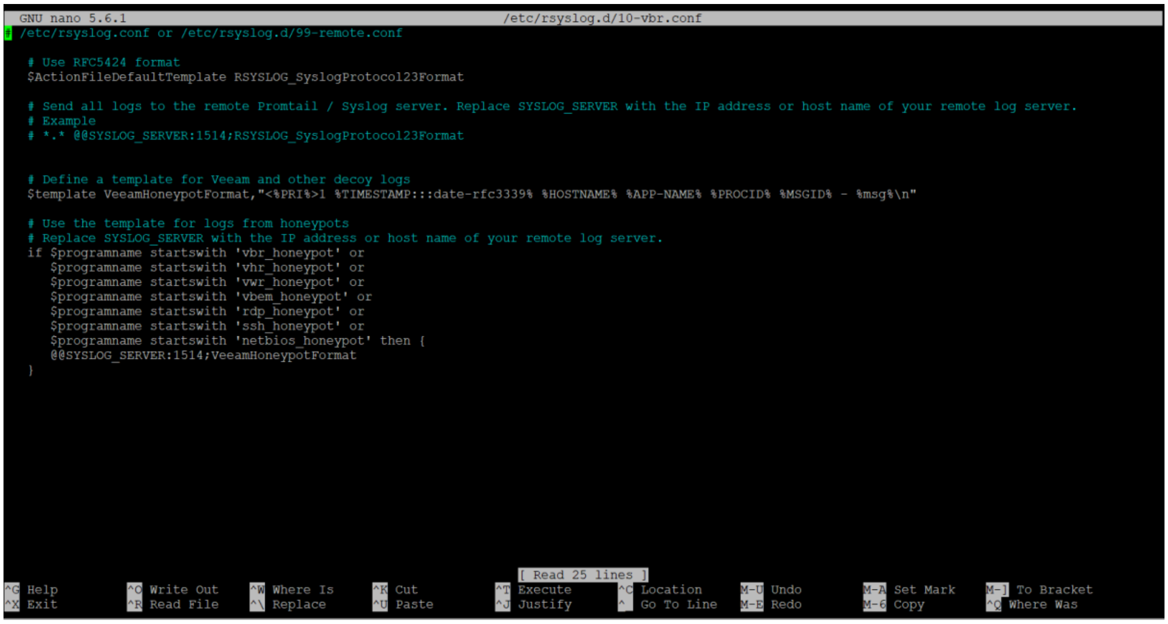
Integration Syslog Server

A key feature of this appliance is the configuration and support for forwarding logs to a centralized SysLog server. All generated records or logs use RFC 5424, which is the same RFC used by Veeam in its logs.

Therefore, to configure log forwarding, you only need to edit the "Rsyslog" configuration, which is present in the TUI, under "Config Files" as:

[Edit] /etc/rsyslog.d/10-vbr.conf   Rsyslog Decoy Config

This configuration is subject to "rsyslog", so when editing the rsyslog file, you only need to change the IP address or name of the Syslog server where the logs should be sent:



```
  GNU nano 5.6.1                                         /etc/rsyslog.d/10-vbr.conf
# /etc/rsyslog.conf or /etc/rsyslog.d/99-remote.conf

   # Use RFC5424 format
   $ActionFileDefaultTemplate RSYSLOG_SyslogProtocol23Format

   # Send all logs to the remote Promtail / Syslog server. Replace SYSLOG_SERVER with the IP address or host name of your remote log server.
   # Example
   # *.* @@SYSLOG_SERVER:1514;RSYSLOG_SyslogProtocol23Format


   # Define a template for Veeam and other decoy logs
   $template VeeamHoneypotFormat,"<%PRI%>1 %TIMESTAMP:::date-rfc3339% %HOSTNAME% %APP-NAME% %PROCID% %MSGID% - %msg%\n"

   # Use the template for logs from honeypots
   # Replace SYSLOG_SERVER with the IP address or host name of your remote log server.
   if $programname startswith 'vbr_honeypot' or
      $programname startswith 'vhr_honeypot' or
      $programname startswith 'vwr_honeypot' or
      $programname startswith 'vbem_honeypot' or
      $programname startswith 'rdp_honeypot' or
      $programname startswith 'ssh_honeypot' or
      $programname startswith 'netbios_honeypot' then {
      @@SYSLOG_SERVER:1514;VeeamHoneypotFormat
   }










                                                                  [ Read 25 lines ]
^G Help          ^O Write Out     ^W Where Is      ^K Cut           ^T Execute       ^C Location      M-U Undo         M-A Set Mark     M-] To Bracket
^X Exit          ^R Read File     ^\ Replace       ^U Paste         ^J Justify       ^/ Go To Line    M-E Redo         M-6 Copy         ^Q Where Was
```

You only need to change the IP address or server name and port of “SYSLOG_SERVER:1514” :

. @@SYSLOG_SERVER:1514;RSYSLOG_SyslogProtocol23Format

And in:

@@SYSLOG_SERVER:1514;VeeamHoneypotFormat

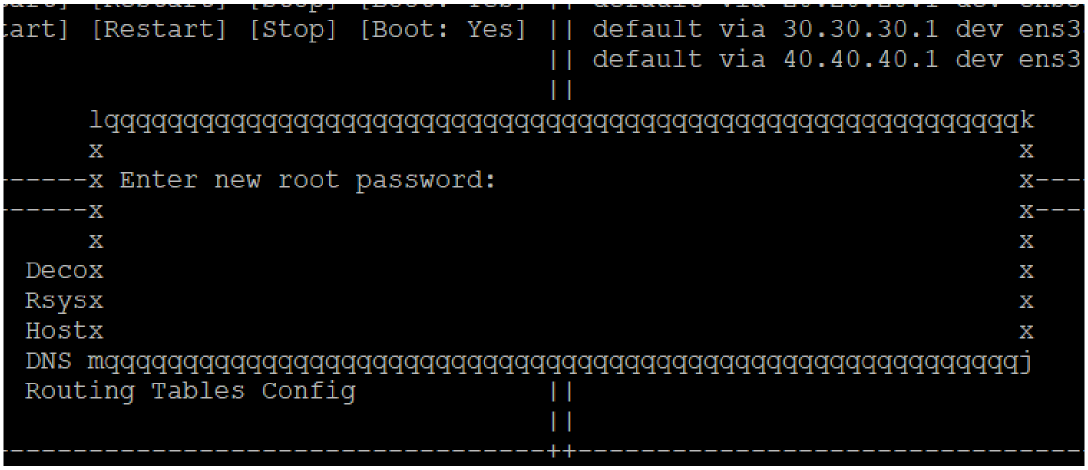
It's important to note that if the Syslog Server only accepts UDP connections, there should be only one @ before the IP address or FQDN. If there are two @@, it's via TCP. By using RFC 5424, it's compatible with any centralized Syslog server.

Accounts

This configuration is only for changing the password of the "Root" user, so when executing the button:

[Change Password]

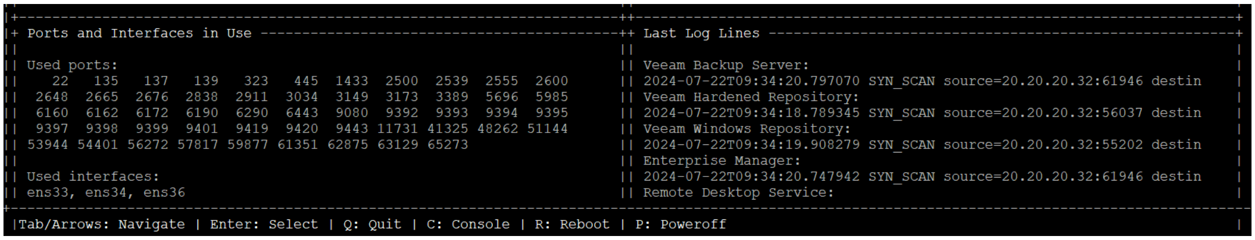
It will request the entry of a new password in the same TUI interface, then this new password will be necessary to log in via console or SSH.



```
art] [Restart] [Stop] [Boot: Yes] || default via 30.30.30.1 dev ens3
                                  || default via 40.40.40.1 dev ens3
                                  ||
    lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk
    x                                                             x
-----x Enter new root password:                                   x---
-----x                                                            x---
    x                                                             x
 Decox                                                            x
 Rsysx                                                            x
 Hostx                                                            x
 DNS mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
 Routing Tables Config            ||
                                  ||
----------------------------------++--------------------------------
```

Port Status and Logs

For this stage, the boxes "Ports and Interfaces in Use" and "Last Log Lines" allow us to identify which ports are being used and the active network interfaces directly in the TUI. If it's necessary to review more detailed information, it's possible to access the Appliance's command line.



```
|+--------------------------------------------------------------------++---------------------------------------------------------------------+
|+ Ports and Interfaces in Use ---------------------------------------++ Last Log Lines ------------------------------------------------------+
||                                                                    ||                                                                     |
|| Used ports:                                                        || Veeam Backup Server:                                                |
||    22   135   137   139   323   445  1433  2500  2539  2555  2600  || 2024-07-22T09:34:20.797070 SYN_SCAN source=20.20.20.32:61946 destin |
||  2648  2665  2676  2838  2911  3034  3149  3173  3389  5696  5985  || Veeam Hardened Repository:                                          |
||  6160  6162  6172  6190  6290  6443  9080  9392  9393  9394  9395  || 2024-07-22T09:34:18.789345 SYN_SCAN source=20.20.20.32:56037 destin |
||  9397  9398  9399  9401  9419  9420  9443 11731 41325 48262 51144  || Veeam Windows Repository:                                           |
|| 53944 54401 56272 57817 59877 61351 62875 63129 65273              || 2024-07-22T09:34:19.908279 SYN_SCAN source=20.20.20.32:55202 destin |
||                                                                    || Enterprise Manager:                                                 |
|| Used interfaces:                                                   || 2024-07-22T09:34:20.747942 SYN_SCAN source=20.20.20.32:61946 destin |
|| ens33, ens34, ens36                                                || Remote Desktop Service:                                             |
+------------------------------------------------------------------------------------------------------------------------------------------+
 |Tab/Arrows: Navigate | Enter: Select | Q: Quit | C: Console | R: Reboot | P: Poweroff                                                   |
```

If it's necessary to review the local log files, they can all be found in the path:

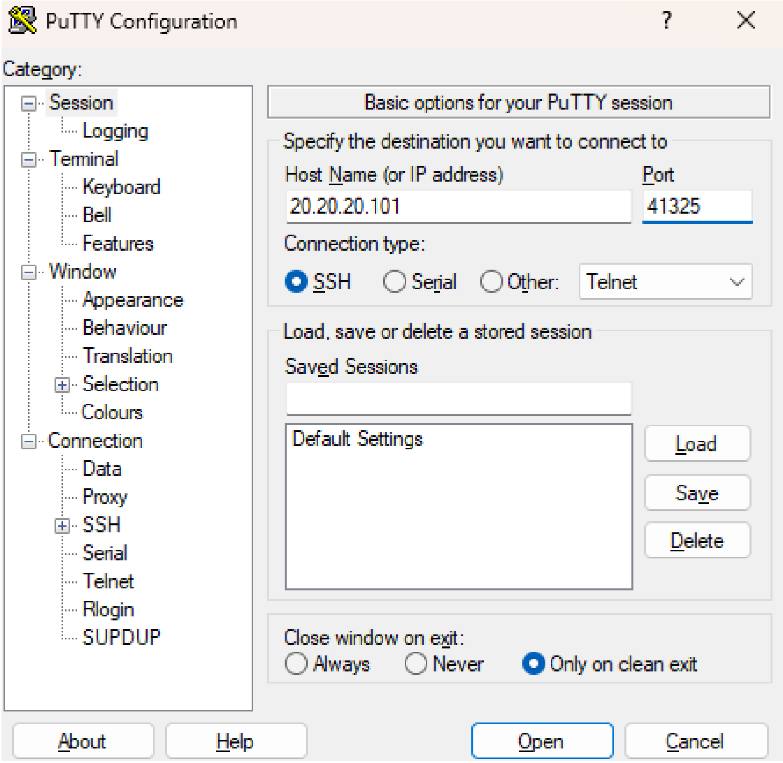
`/var/log/hnp/`

Administrative Access via SSH

Additionally, since in some cases it's not possible to maintain access to the web console of virtual machines or only remote access is needed to manage some Appliance configuration, in the TUI, you can observe the service:

SSH Admin port:41325

Which is the SSH service running on a custom port and within the ranges also used by Veeam. If necessary, it can be started directly from the TUI and configured to run on Appliance restart. Then you only need to connect with your preferred SSH client, for example, Putty:



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 20.20.20.101

Port: 41325

Connection type: ● SSH ○ Serial ○ Other: Telnet

Load, save or delete a stored session

Saved Sessions: Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

Recommendations

The main recommendation for the use of this project is the deployment of multiple Appliances in multiple **internal** VLANs or virtual networks (since it doesn't require many resources) to obtain extensive monitoring of lateral movements in case of any type of incident in the organization. Of course, the Syslog concentrator should always exist, either locally or in the cloud, so that the corresponding analyses are carried out and, in case of an attack, the central Syslog server is not affected.

On the other hand, when implementing the different network interfaces, associate the IP addresses with their respective DNS. For example, if one of the interfaces is providing the "Veeam Backup Server" service, associate it with the FQDN "veeam.yourdomain.local", of course, replacing the domain with that of the organization, likewise with other services.

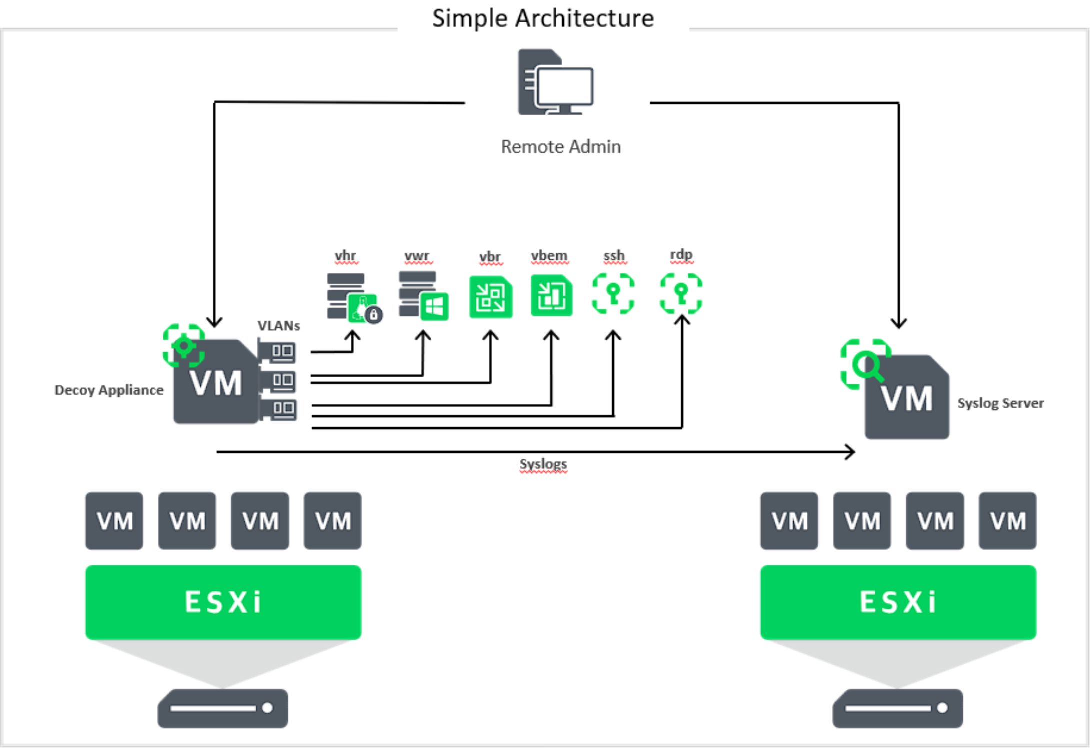
Also, when using multiple services from a single network interface of the Appliance, some ports come into conflict, as they are also used by another service. For example, enabling "Veeam Hardened Repository" and "Veeam Windows Repository" on the same interface will cause an error and the service will not function correctly. Preferably, use the repositories on different interfaces.

This machine does not need to be protected or backed up by Veeam, as it is disposable in case of any problem and should only be redeployed through the OVA or manual installation.

Finally, a very good practice is to **disable** the **SSH ADMIN** management interface that operates on port **41325**, to prevent connection attempts to that port.

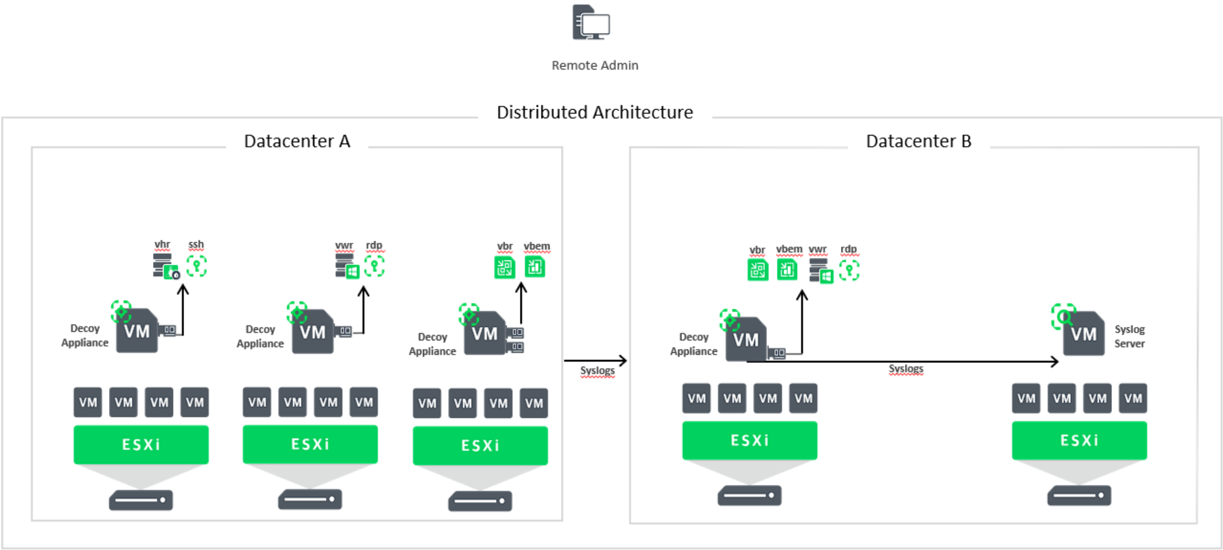
Example Architectures

1. Simple Architecture



In this simple architecture, everything is deployed in a single Appliance with multiple network interfaces, associated with different networks, allowing with very few resources to have the various Veeam services, waiting for any unknown connection attempt, network scanning looking for services, or any lateral movement related to Veeam.

2. Distributed Architecture



In this distributed architecture, multiple Appliances are implemented in different hosts or virtual environments with multiple network interfaces or just one, to provide services. This architecture seeks to further expand the detection surface by distributing the services. It can be in different data centers as well as in different virtualization hosts in a single data center.