

# Veeam Decoys

# Contenidos

Introducción.....	3
Estadísticas.....	3
Características.....	7
Requerimientos de Hardware y Software.....	8
Requerimientos de Hardware Virtual   OVA.....	8
Requerimientos Rocky Linux   Instalación Manual.....	8
Despliegue.....	9
Despliegue de Appliance Virtual.....	9
Instalación Manual en Rocky Linux 9.x.....	15
Configuración.....	17
Decoy Services.....	18
Network Interfaces.....	19
Config Files.....	20
Alertas.....	21
Integración Syslog Server.....	22
Accounts.....	23
Estado de Puertos y Logs.....	23
Acceso Administración via SSH.....	24
Recomendaciones.....	25
Arquitecturas de Ejemplo.....	26
1. Arquitectura Simple.....	26
2. Arquitectura Distribuida.....	27

# Introducción

Hoy la cantidad de ataques a las organizaciones es exponencial, por lo que las empresas necesitan aplicar buenas prácticas para gestionar riesgo en IT y las mejores soluciones de protección de datos, detección de incidentes y gestión de incidentes.

Dentro del mundo de la seguridad existen muchos framework que permiten a las organizaciones mejorar su nivel de seguridad en IT, para lo cual siempre es necesario mantener una detección temprana de los movimientos laterales, intentos de conexión desde un origen no permitido, escaneos que ocurren en la red interna, o simplemente un levantamiento de los puertos utilizados en los servidores en una VLAN o en múltiples VLANs / Redes.

Por tanto, existe el concepto y la tecnología que nos permite crear servicios para detectar este tipo de movimientos laterales o intentos de conexión para anticiparse a un incidente de seguridad. Como es de público conocimiento, muchos grupos de Ransomware también se enfocan en destruir las copias de respaldo de los datos.

Por lo anterior, este proyecto se desarrolló para crear servicios productivos y detectar, en caso de intento de ataque, conexión, autenticación y el área de seguridad informática de la organización aplique las medidas necesarias o su plan de respuesta ante incidentes.

## Estadísticas

Este tipo de servicios fueron testeados en internet, logrando obtener un patrón de comportamiento de lo que buscan los atacantes o Bots en internet, cabe señalar, **que esta solución es para implementarla en las redes internas de la organización**, pero el objetivo era tener escaneos o ataques que existen en internet para lograr saber la cantidad y el consumo de recursos. De hecho, es el mejor lugar para recibir intentos de conexión o escaneos secuenciales y aleatorios, algunos de los datos estadísticos que se obtuvieron fueron los siguientes:

Cantidad de días con Servicios expuestos: **15**

Cantidad de Servicios expuestos: **7**

CPU: **1 vCPU**

RAM: **2 GB**

Almacenamiento: **50 GB**

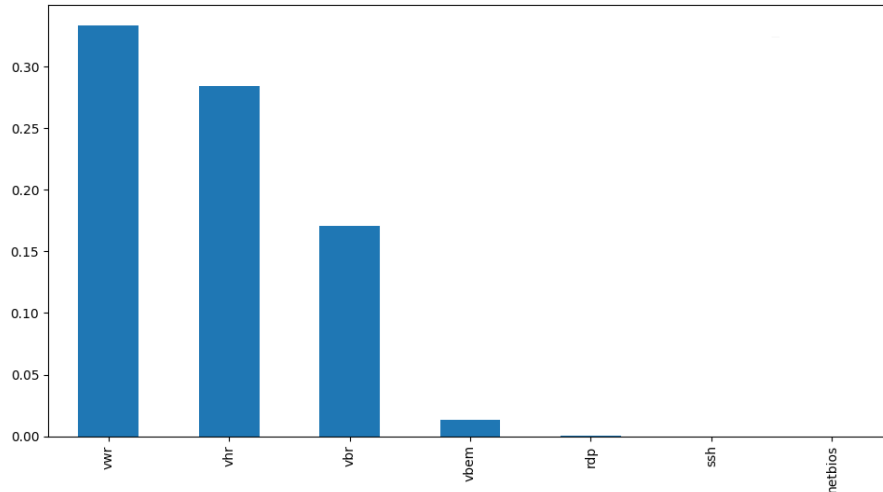
El consumo de recursos de cómputo solo tuvo un máximo de uso al **28%** de CPU un día de los 15 días, los demás días siempre fueron con un máximo de **5%** por día, el consumo de RAM siempre se mantuvo en **40%** durante los 15 días de la prueba y con respecto al uso de disco, el crecimiento el uso en total fue de un **8%** y específicamente en los archivos de log del Appliance relacionado con los servicios fue de **120 MB**. En la utilización de recursos podemos observar un bajo uso, ya que el Appliance era escaneado las 24 horas

del día, por distintas direcciones IP, como el objetivo del Appliance es para implementarlo en las redes internas de las organizaciones, el escaneo de 24 hora todos los días, no será ejecutado, por tanto, no será necesario agregar más recursos de cómputo.

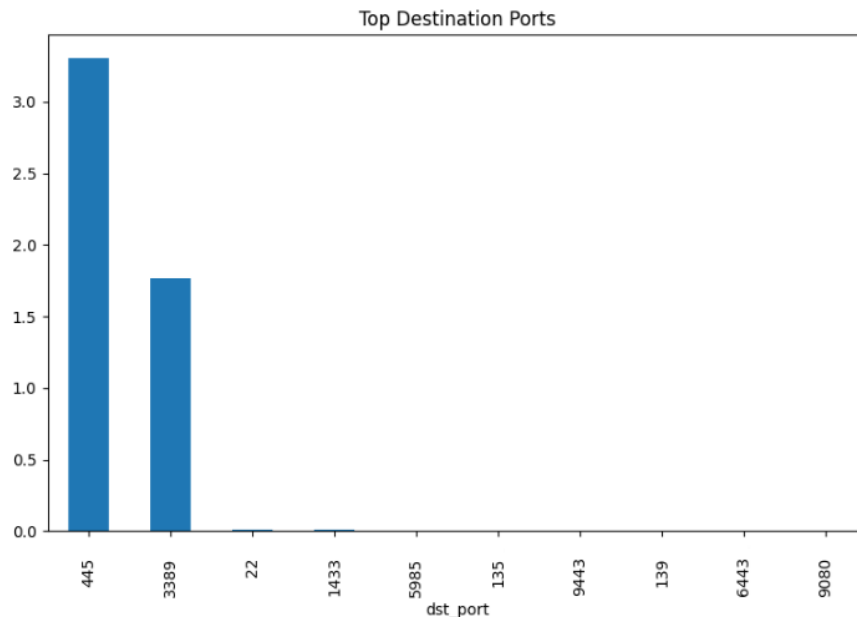
Con respecto a las estadísticas de los escaneos o ataques recibidos por el Appliance durante los 15 días expuesto en internet, es posible decir:

Se analizaron un total de Eventos: **5116389**

La efectividad de los servicios fue:



Como se puede observar en el grafico anterior, el servicio más escaneado fue “Veeam Windows Repository”, ya que tradicionalmente los robots o actores de amenaza buscan servidores Microsoft Windows sin actualizaciones para explotar las vulnerabilidades lo que se correlaciona con los puertos más escaneados, como se visualiza en el siguiente gráfico.





Censys:

## NETBIOS 137/UDP

07/22/2024 06:44 UTC

### Details

[VIEW ALL DATA](#)

#### 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 | AAAAAAAAAAAAAA |
00000020: 41 41 41 41 41 41 41 41 41 41 41 00 00 21 00 01 | AAAAAAAAAA... |
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 00 00 00 | ..... |
```

# Características

Este sistema cuenta con los siguientes servicios:

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

Y las siguientes características:

- Terminal User Interface**
- Logs**
- Reenvío de Logs**
- Notificaciones por Email**
- Configuración Múltiples Interfaces de Red**
- Lista de Puertos usados**
- Gestión de Servicios**
- Edición de Archivos de Configuración**
- Gestión Remota**

Cada uno de los servicios permite detectar intentos de conexión, escaneos, a los diferentes puertos utilizados por cada uno de los servicios, capturando las credenciales, direcciones IP, puertos de origen, dirección ip de origen, consultas específicas a ciertos servicios, todas las capturas son generadas en formato Syslog para reenviar a un servidor SysLog centralizado o enviar las notificaciones por correo.

Además, el Appliance soporta la utilización de múltiples interfaces de red, para que, con solo 1 Appliance se posible implementar los servicios en múltiples redes, permitiendo así, un despliegue de los servicios de forma distribuida.

# Requerimientos de Hardware y Software

## Requerimientos de Hardware Virtual | OVA

Los requerimientos mínimos necesarios para utilizar el Appliance son los siguientes:

**Procesador:** 1 vCPU

**Memoria RAM:** 2 GB

**Almacenamiento:** 50 GB

**Red:** 1 GB / 10GB / VMXNET 3

**Hipervisor:** vSphere 8.0 o superior.

## Requerimientos Rocky Linux | Instalación Manual

Para instalar estos servicios directamente en un servidor Rocky Linux 9.4 ya instalado es necesario contar con:

**Sistema Operativo:** Instalación mínima de Rocky Linux 9.4 (Probado solo en esta distro, puede soportar otras distribuciones basadas en redhat)

**Paquetes Python:**

**Procesador:** 1 CPU

**Memoria RAM:** 2 GB

**Almacenamiento:** 50 GB

**Red:** 1 GB / 10 GB

**Firewall:** Deshabilitado

**SELinux:** Deshabilitado

Con los requerimientos anteriores, será posible utilizar todos los servicios en múltiples interfaces de red.



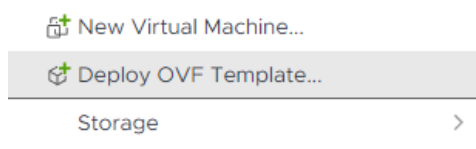
# Despliegue

## Despliegue de Appliance Virtual.

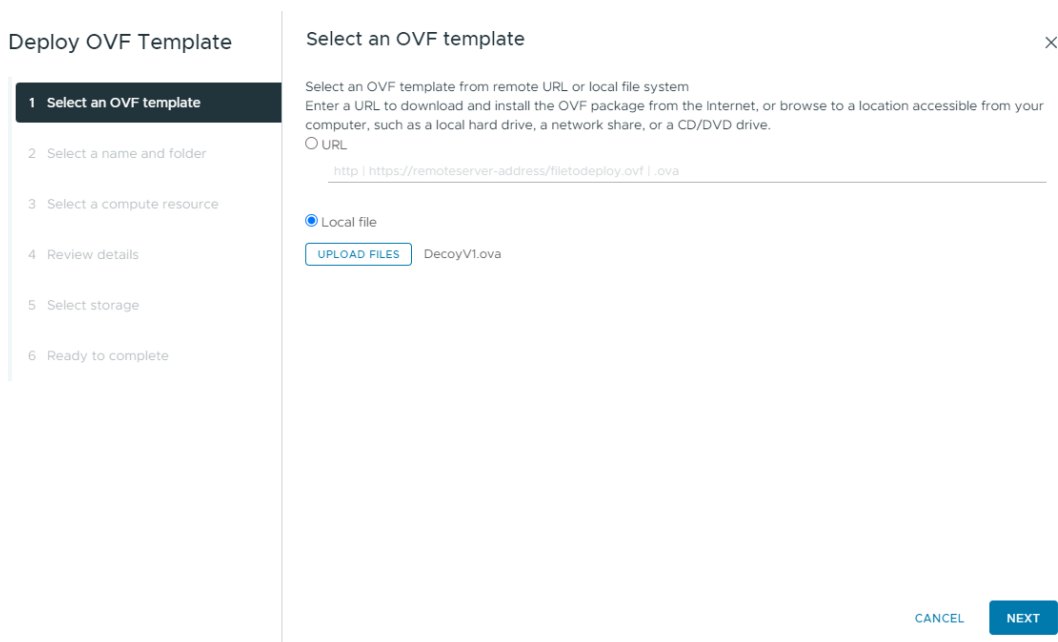
Descarga la imagen OVA desde:

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

Para luego importar el Appliance directamente desde vCenter seleccionando “Deploy OVF Template”:



Y después ingresa a la ruta donde se descargó el OVA, para seleccionarlo, luego clic en “Next”:



Ingresa el nombre de la VM, selecciona el vCenter, Datacenter y Carpera de VM donde se alojará la VM, para luego hacer clic en “Next”:

The screenshot shows the 'Deploy OVF Template' wizard with step 2, 'Select a name and folder', highlighted. The main panel is titled 'Select a name and folder' and includes a close button (X) in the top right. It contains the following elements:

- Instruction: 'Specify a unique name and target location'
- Field: 'Virtual machine name:' with the value 'Veeam-Decoy-V1' entered.
- Section: 'Select a location for the virtual machine.'
- Tree view showing a folder structure: 'vcenter.24xsiempre.cl' expanded to show a sub-folder '24xSiempre', which is selected.
- Checkbox: 'Customize this virtual machine's hardware' (unchecked).
- Buttons: 'CANCEL', 'BACK', and 'NEXT' at the bottom right.

Luego seleccionar cuáles serán los recursos de cómputo y hacer clic en “Next”:

The screenshot shows the 'Deploy OVF Template' wizard with step 3, 'Select a compute resource', highlighted. The main panel is titled 'Select a compute resource' and includes a close button (X) in the top right. It contains the following elements:

- Instruction: 'Select the destination compute resource for this operation'
- Tree view showing a folder structure: '24xSiempre' expanded to show a sub-folder 'Cluster', which is selected.
- Section: 'Compatibility' with a message: '✓ Compatibility checks succeeded.'
- Checkbox: 'Automatically remove the destination VM' (unchecked).
- Buttons: 'CANCEL', 'BACK', and 'NEXT' at the bottom right.

Ahora el asistente mostrará el mensaje que el OVA posee configuraciones avanzada, clic "Next":

### Deploy OVF Template

- Select an OVF template
- Select a name and folder
- Select a compute resource
- Review details**
- Select storage
- Select networks
- Customize template
- 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

CANCEL BACK NEXT

Ahora es necesario seleccionar el Almacenamiento donde se alojará el Appliance y después clic en "Next":

### Deploy OVF Template

- Select an OVF template
- Select a name and folder
- Select a compute resource
- Review details
- Select storage**
- Select networks
- Customize template
- 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
<input checked="" type="radio"/>	LAB	--	30 TB	42.98 TB	11.29 TB
<input type="radio"/>	Local24x1	--	348.75 GB	1.42 GB	347.33 GB
<input type="radio"/>	Local24x2	--	348.75 GB	1.42 GB	347.33 GB
<input type="radio"/>	NFSLAB	--	5.95 TB	630.85 GB	5.34 TB

Manage Columns Items per page 10 ▾ 4 items

Compatibility

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

En este paso se configura y selecciona cual será la Red / Vlan que se usará en la primera interfaz de red del Appliance, configurar el “Destination Network” y hacer clic en “Next”:

### Deploy OVF Template

- Select an OVF template
- Select a name and folder
- Select a compute resource
- Review details
- Select storage
- 6 Select networks**
- Customize template
- Ready to complete

### Select networks

Select a destination network for each source network.

Source Network	Destination Network
RED20	RED20

Manage Columns 1 item

#### IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

CANCEL BACK NEXT

Ahora configuraremos el Appliance para agregar en la primera parte de “Networking”, los datos necesarios de red:

### Deploy OVF Template

- Select an OVF template
- Select a name and folder
- Select a compute resource
- Review details
- Select storage
- Select networks
- 7 Customize template**
- Ready to complete

### 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

CANCEL BACK NEXT

Luego en “Settings” ingresar los datos solicitados y hacer clic en “Next”:

The screenshot shows the 'Customize template' step of a deployment wizard. On the left, a sidebar titled 'Deploy OVF Template' lists eight steps: 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 (highlighted), and 8. Ready to complete. The main panel is titled 'Customize template' and contains a green success message: 'All properties have valid values'. Below this, there are three sections of settings: 'Networking' (5 settings), 'Settings' (3 settings), and 'Root Password'. The 'Settings' section includes: 'NTP Server' with value 'ntp.shoa.cl', 'Time Zone' with value 'America/Santiago', and 'Root Password' with fields for 'Password' and 'Confirm Password'. At the bottom right, there are three buttons: 'CANCEL', 'BACK', and 'NEXT'.

Y en la última opción, revisar las configuraciones aplicadas para luego hacer clic en “Finish” y esperar el despliegue del Appliance:

The screenshot shows the 'Ready to complete' step of a deployment wizard. On the left, the same 'Deploy OVF Template' sidebar is shown, but step 8 'Ready to complete' is highlighted. The main panel is titled 'Ready to complete' and contains a review of selections: '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), and 'Customize template'. At the bottom right, there are three buttons: 'CANCEL', 'BACK', and 'FINISH'.

Veeam-Decoy-V1 | ACTIONS

Summary Monitor Configure Permissions Datastores Networks Snapshots Updates

### Guest OS

Powered Off

LAUNCH REMOTE CONSOLE ⓘ

LAUNCH WEB CONSOLE

### 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

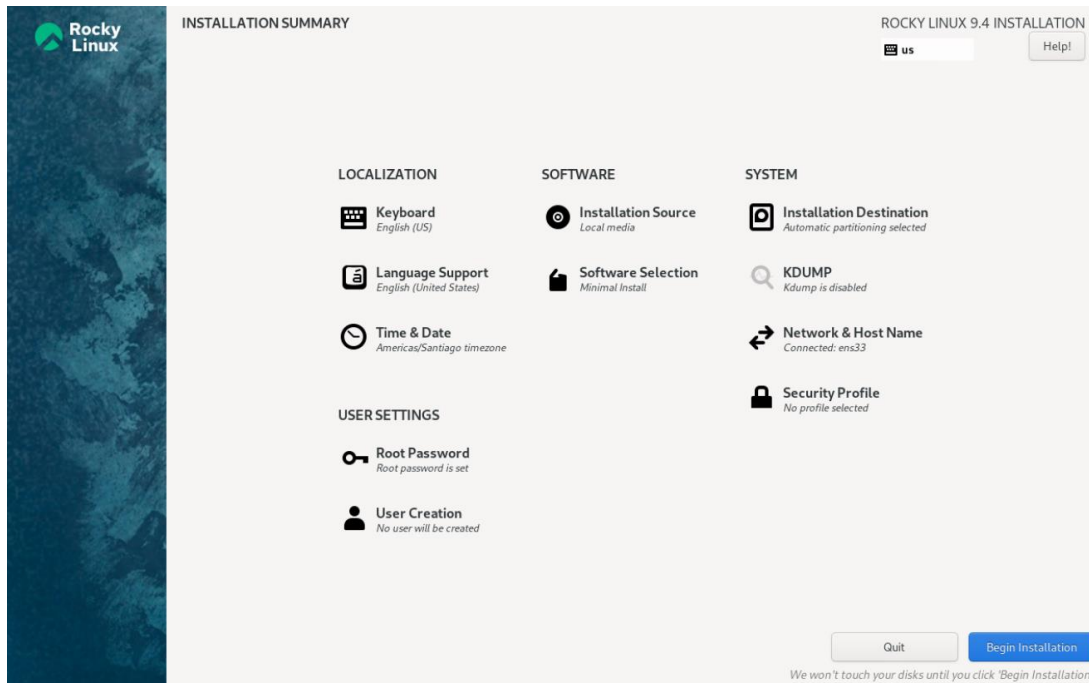
**Compatibility** ESXi 8.0 and later (VM version 20)

EDIT

Encender el Appliance.

# Instalación Manual en Rocky Linux 9.x

Para instalar el sistema directamente en un servidor Linux con Rocky Linux 9.4, es necesario validar el tipo de instalación de Rocky Linux sea la opción “Mínimal”:



Desde la línea de comando de Linux también es posible validar el tipo de instalación con el siguiente comando:

```
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 ~]#
```

Y realizar la instalación con el siguiente comando:

```
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...
```

Comenzará con la instalación y configuración de los servicios:

```
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
=====
```

Y al finalizar exitosamente mostrará:

```
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
```

Y por último reiniciar el servidor con el comando:

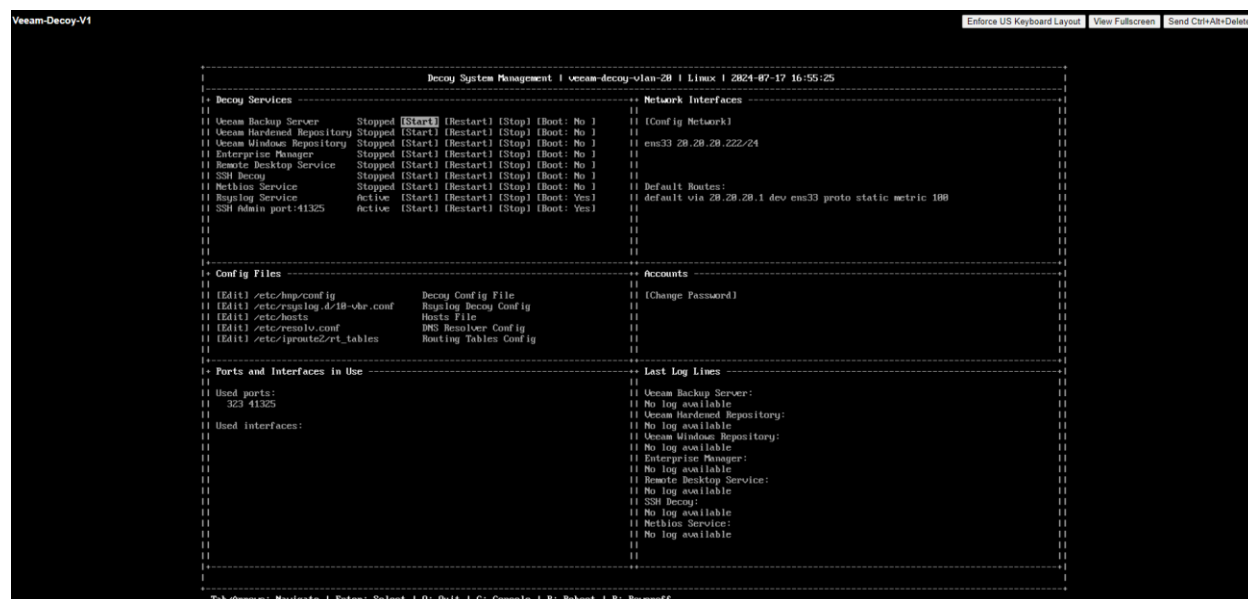
reboot

Después de haber reiniciado el servidor, conectarse via SSH por el puerto **41325**, en caso de que sea una máquina virtual, también será posible ingresar por Consola y por último si la maquina es física, ingresar por IPMI.



# Configuración

Ya con el Appliance desplegado y encendido en el ambiente virtual, existen dos opciones para ingresar y aplicar las configuraciones necesarias a través del “Web Console” de vCenter o a través de SSH con un puerto específico. Para el funcionamiento correcto de los servicios, el usuario a utilizar es “root”, en caso de instalación manual si no es posible usar “root” debe ser un usuario con permisos “sudo”.



```
Decoy System Management | veeam-decoy-vlan-20 | Linux | 2024-07-17 16:55:25
-----
Decoy Services                                     Network Interfaces
-----
|| Ueam Backup Server      Stopped [Start] (Restart) [Stop] (Boot: No) || [Config Network] || | | | |
|| Ueam Hardened Repository Stopped [Start] (Restart) [Stop] (Boot: No) || ||
|| Ueam Windows Repository Stopped [Start] (Restart) [Stop] (Boot: No) || ems33 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) || ||
|| Nmaplog Service         Active [Start] (Restart) [Stop] (Boot: Yes) || default via 20.20.20.1 dev ems33 proto static metric 100 ||
|| SSH Admin port:41325    Active [Start] (Restart) [Stop] (Boot: Yes) || ||
|| || || || ||
|| || || || ||
|| || || || ||
|| || || || ||
-----
Config Files                                       Accounts
-----
|| Edit /etc/ump/config      Decoy Config File || [Change Password] || | | | |
|| Edit /etc/mapping_d/10-ubr.conf Mapping Decoy Config || ||
|| Edit /etc/hosts          Hosts File || ||
|| Edit /etc/resolv.conf    DNS Resolver Config || ||
|| Edit /etc/iproute2/rtnetables Routing Tables Config || ||
|| || || || ||
-----
Ports and Interfaces in Use                       Last Log Lines
-----
|| Used ports: || || Ueam Backup Server: || | |
|| 323 41325 || || No log available ||
|| || || Ueam Hardened Repository: ||
|| Used interfaces: || || No log available ||
|| || || Ueam 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
```

Si es necesario ingresar por SSH, el puerto a utilizar es **41325** con el usuario root y la contraseña configurada anteriormente.

Ya sea por “Web Console” o “SSH” con el puerto administrativo el TUI será visualizado, esta interfaz se compone de las siguientes opciones:

**Decoy Services:** Aquí se listan todos los servicios que están configurados en el Appliance, posee todo el ciclo de vida de los servicios a través de systemd y si es necesario configurar el servicio al inicio del sistema operativo.

**Network Interfaces:** Aquí permite ejecutar la configuración de la red, incluyendo si existen múltiples interfaces de red, permitiendo visualizar las interfaces activas y sus respectivas rutas de red.

**Config Files:** Esta parte es la más importante, ya que permite editar directamente los archivos de configuración para el correcto funcionamiento del Appliance. El editor es nano.

**Accounts:** Permite cambiar la contraseña del usuario root.

**Ports and Interfaces in Use:** Muestra el estado de las interfaces, los puertos abiertos de todos los servicios que se ejecutan, se actualiza al instante cuando se inicie un servicio.

**Last Log Lines:** Muestra la última línea del log del servicio, para identificar errores o si está siendo accedido el servicio.

Y, por último, en el “Footer” del TUI, existen 4 opciones:

**Q:** Quit, para salir del TUI

**C:** Console, para ingresar al CLI de Linux (Experimental)

**R:** Reboot, para reiniciar el Appliance previa confirmación.

**P:** Poweroff, para apagar el Appliance previa confirmación.

## Decoy Services

Aquí se gestiona todo el ciclo de vida de los servicios, por tanto, en el menú siempre aparecerá, por ejemplo:

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

“**Stopped**” es el estado del servicio actual, puede tener dos estados adicionales “**Active**” que se encuentra en ejecución y “**Failed**” se debe revisar los archivos de logs o el archivo de configuración.

“**Start**” es el botón para iniciar el servicio, cuando se ejecuta muestra mensaje, exitoso o no.

“**Restart**” es el botón para reiniciar el servicio, cuando se ejecuta muestra mensaje, exitoso o no.

“**Stop**” es el botón para detener el servicio, cuando se ejecuta muestra mensaje, exitoso o no

“**Boot: No**” Muestra el estado actual si el servicio se inicia con el sistema operativo, si es estado es “**No**”, el servicio debe iniciarse manualmente, si el estado es “**Yes**” el servicio ya se ejecuta al iniciar el sistema operativo.

# Network Interfaces

Aquí se gestiona a la configuración de red, de una o múltiples interfaces donde al ejecutar:

## [Config Network]

Mostrará una asistente de configuración, solo se debe agregar la información solicitada:

```
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: █
```

Si se desea configurar una o varias interfaces, se solicitará los siguientes datos:

```
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
```

Dirección IP, Gateway y Red de la interfaz seleccionada. Después de la configuración de las interfaces de red, es recomendable reiniciar el Appliance para garantizar la persistencia de los datos configurados. En caso de no tener conexión, validar la configuración por Web Console.

## Config Files

Aquí es la parte más importante de configuración, ya después de haber definido las interfaces de red, es necesario configurar los servicios en cuales interfaces van a funcionar, los servicios pueden ejecutarse en múltiples interfaces, siempre y cuando, no exista otro servicio usando puertos en común. Por ejemplo, si se configura “Veeam Windows Repository” y “Veeam Hardened Repository” en la misma interfaz de red, uno de los servicios no funcionara, ya que ambos servicios ocupan los puertos 6160 y 6162.

Ahora entrando en la configuración de los servicios, dentro del TUI, entrar a la caja “Config Files”, seleccionar “Decoy Config File” para editar el archivo de configuración principal:

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

Al seleccionar, se mostrará el editor “nano” con el contenido del archivo de configuración, éste archivo, tiene toda la información de cada variable a configurar, para los servicios, solo es necesario cambiar la variable:

**interfaces = en192,ens224**

En cada uno de los servicios, para que funcionen en una o múltiples interfaces. En el caso de usar múltiples interfaces en uno o varios servicios, seguir el formato que indica el archivo de configuración para ingresar las interfaces con coma y sin espacio.

```
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-G Copy      ^_ Where Was
```

Todas las opciones que se encuentran en el archivo de configuración son configurables, es decir, es posible cambiar el tipo de sistema operativo, banners, dominio a simular.

## Alertas

En el mismo archivo de configuración `/etc/hnp/config` es posible configurar las notificaciones por email, si es necesario, en “[Email]” tiene las múltiples opciones incluyendo habilitar o deshabilitar el servicio.

```
# 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
```

El envío de correos será cada 5 minutos, solo si se encuentran conexiones en el servicio, de lo contrario, no se enviará ningún correo y se informará que no existieron conexiones para reportar.

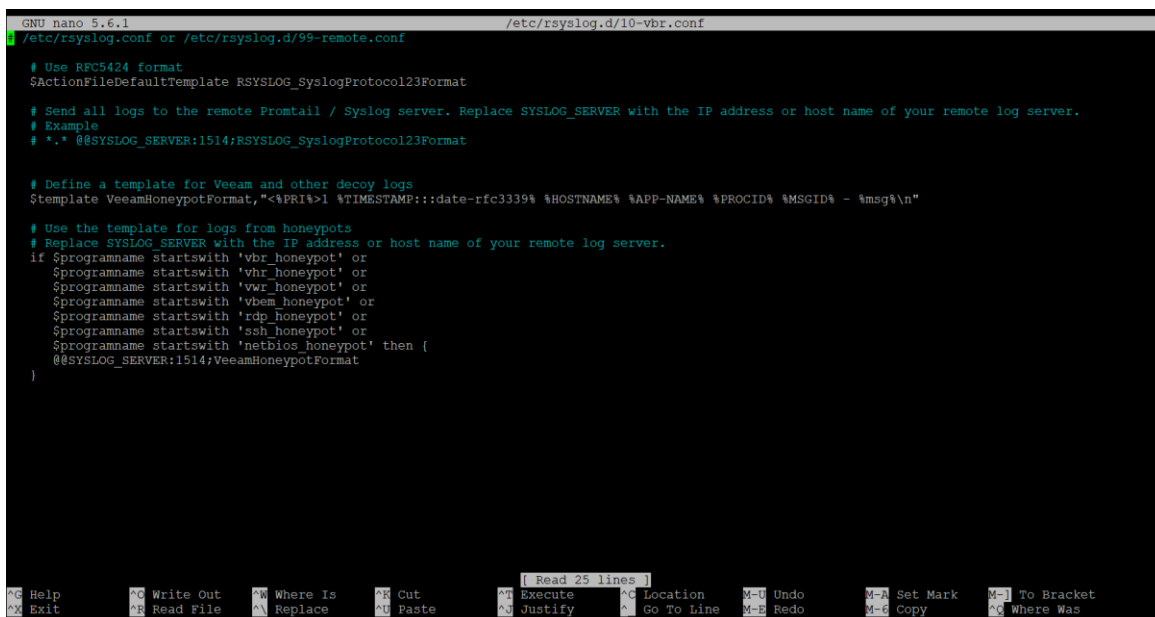
## Integración Syslog Server

Una característica clave en este Appliance, es la configuración y soporte de reenvío de logs a un servidor SysLog centralizado, todos los registros o logs generados están usando el RFC 5424 que es el misma RFC que ocupa Veeam en sus logs.

Por tanto, para configurar el reenvío de logs, solo se debe editar la configuración de “Rsyslog” que se encuentra presente en el TUI, dentro de “Config Files” como:

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

Esta configuración está sujeta a “rsyslog”, por tanto, al editar el archivo de rsyslog, solo se debe cambiar la dirección ip o nombre del servidor Syslog donde se debe enviar los registros:



```
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_honeygot' or
   $programname startswith 'vhr_honeygot' or
   $programname startswith 'vwr_honeygot' or
   $programname startswith 'vbm_honeygot' or
   $programname startswith 'rdp_honeygot' or
   $programname startswith 'ssh_honeygot' or
   $programname startswith 'netbios_honeygot' then {
    @@SYSLOG_SERVER:1514;VeeamHoneyPotFormat
}
```

Solo se debe cambiar la dirección ip o nombre de servidor y puerto de “SYSLOG\_SERVER:1514” :

```
# *.* @@SYSLOG_SERVER:1514:RSYSLOG_SyslogProtocol23Format
```

Y en:

```
@@SYSLOG_SERVER:1514;VeeamHoneyPotFormat
```

Es importante señalar si el Syslog Server solo acepta conexiones UDP, debe ser solo un @ delante de la dirección ip o FQDN, si tiene dos @@ es via TCP. Al utilizar el RFC 5424, es compatible con cualquier servidor centralizado de Syslog.

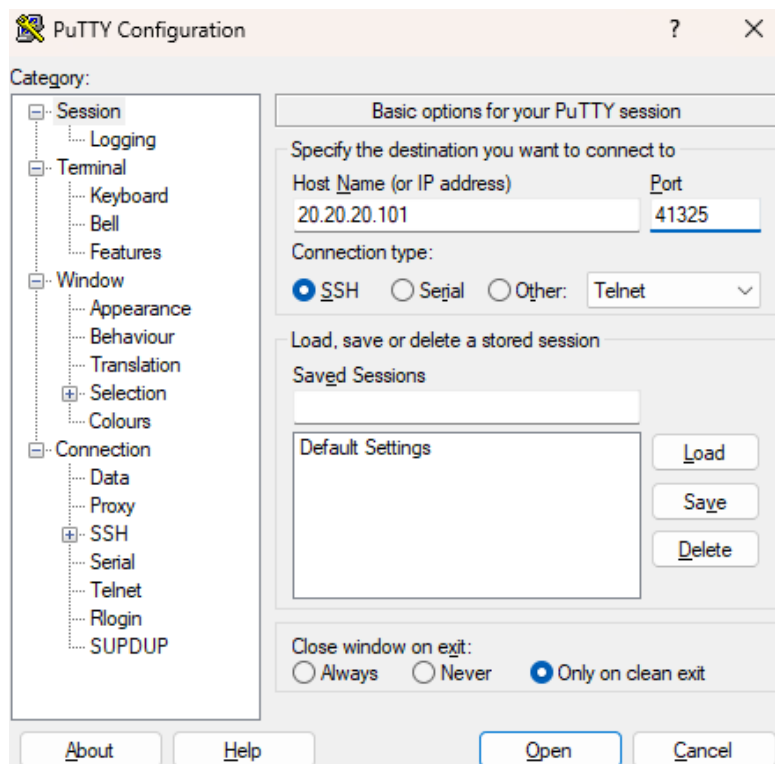


## Acceso Administración via SSH

Además, ya que en algunos casos no es posible mantener acceso a la consola web de las máquinas virtuales o solo es necesario un acceso remoto para gestionar alguna configuración del Appliance, en el TUI se puede observar el servicio:

### SSH Admin port:41325

Es cual es el servicio SSH corriendo en un puerto personalizado y entro de los rangos que también utiliza Veeam, si es necesario, puede ser iniciado directamente desde el TUI y configurado para que se ejecute al reinicio del Appliance. Luego solo es conectarse con el cliente SSH de preferencia, por ejemplo, Putty:





## Recomendaciones.

La principal recomendación para la utilización de este proyecto es el despliegue de múltiples Appliances y en múltiples VLANs o redes virtuales **internas** (ya que no requiere muchos recursos), para obtener un amplio monitoreo de movimientos laterales en caso de algún tipo de incidente en la organización, por supuesto debe siempre existir ya sea localmente o en la nube el concentrador de Syslog, para que se realicen los análisis correspondientes y en caso de ataque no sea afectado el servidor central de Syslog.

Por otra parte, cuando se implemente las distintas interfaces de red, asociar las direcciones IP con su respectivo DNS, es decir, por ejemplo, si una de las interfaces está prestando el servicio de “Veeam Backup Server” asociarlo al FQDN “veeam.tudominio.local”, por supuesto, reemplazando el dominio con el de la organización, así mismo, con otros servicios.

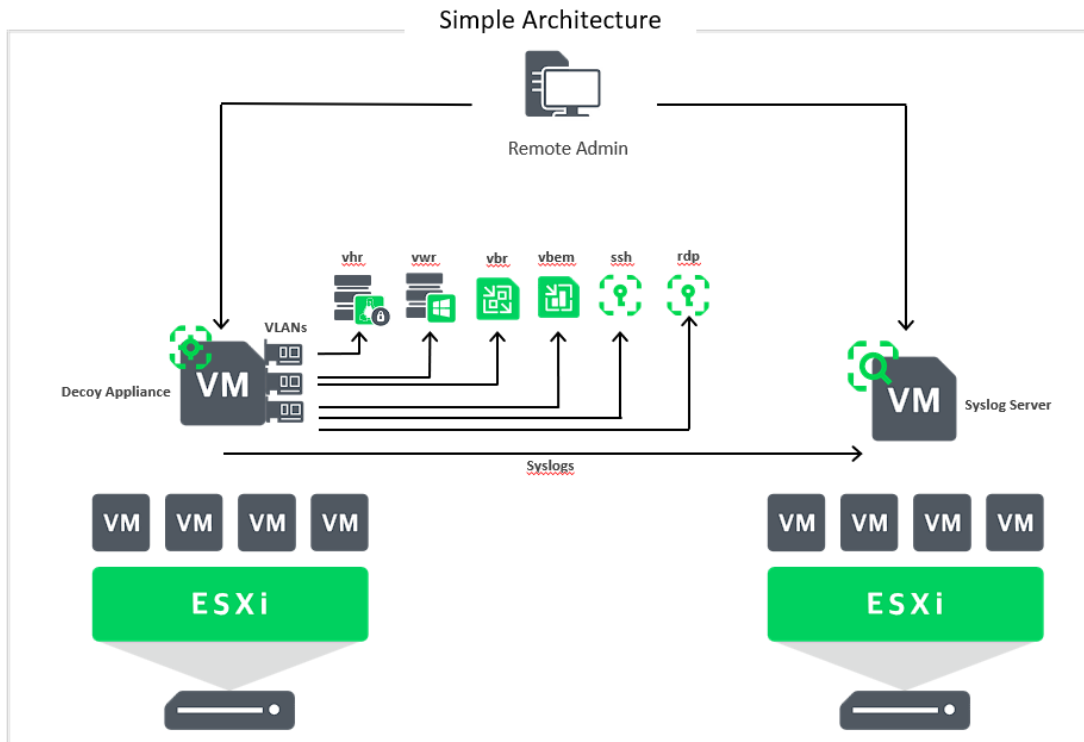
También, cuando se utilizan múltiples servicios desde una sola interfaz de red del Appliance, algunos puertos entran en conflicto, ya que también son usados por otro servicio, por ejemplo, habilitar en la misma interfaz “Veeam Hardened Repository” y “Veeam Windows Repository” ocasionara un error y el servicio no funcionara correctamente, de preferencia, utilizar los repositorios en distintas interfaces.

Esta máquina no necesita ser protegida o respaldada por Veeam, ya que es descartable en caso de cualquier problema y solo se debe desplegar nuevamente a través del OVA o la instalación manual.

Por ultimo y no menos importante, una muy buena práctica es **deshabilitar** la interfaz de administración **SSH ADMIN** que funciona en el puerto **41325**, para evitar intentos de conexión a ese puerto.

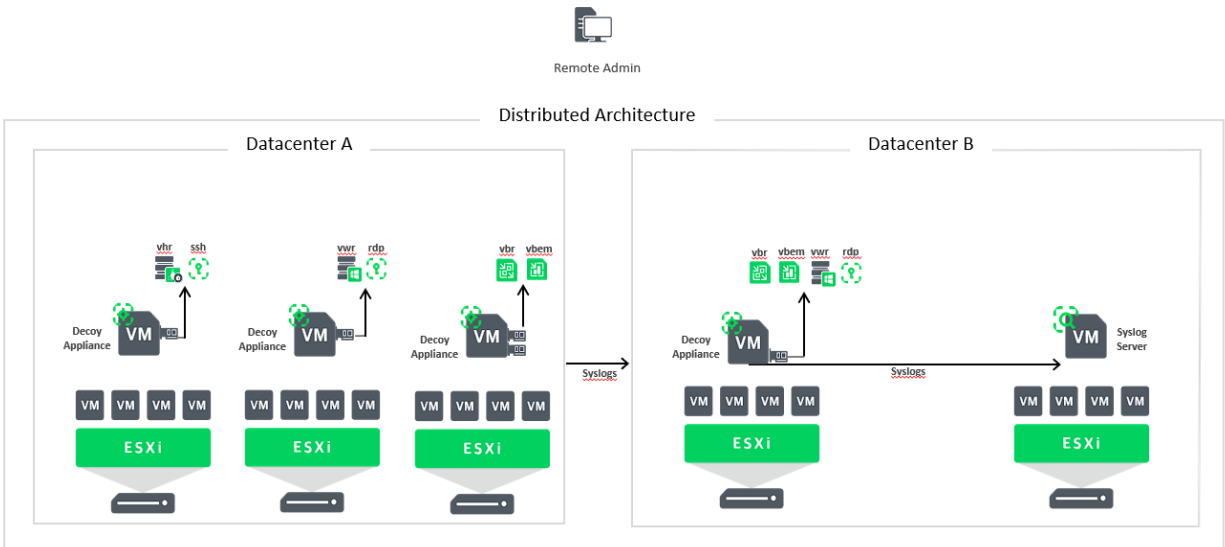
# Arquitecturas de Ejemplo

## 1. Arquitectura Simple



En esta arquitectura simple, todo es desplegado en un solo Appliance con múltiples interfaces de red, asociadas a distintas redes, permitiendo con muy pocos recursos tener los distintos servicios de Veeam, esperando por cualquier intento de conexión que sea desconocido, escaneo de las redes buscando servicios o cualquier movimiento lateral que tenga relación con Veeam.

## 2. Arquitectura Distribuida



En esta arquitectura distribuida, se implementan múltiples Appliances en distintos hosts o ambientes virtuales con múltiples interfaces de red o solo una, para proveer los servicios, esta arquitectura busca expandir aún más la superficie de detección distribuyendo los servicios. Puede ser en distintos centros de datos como también en distintos hosts de virtualización en un solo centro de datos.