

Especificación y desarrollo de una herramienta gráfica de configuración de escenarios de red virtuales para entornos de ciberdefensa

Trabajo Fin de Máster

Ricardo José Ruiz Fernández

Tutor: Manuel Álvarez-Campana

Índice

- ❑ **Introducción y objetivos**
- ❑ Infraestructura del MCCD
- ❑ Desarrollo de la herramienta
- ❑ Interfaz de usuario
- ❑ Conclusiones

Introducción

- ❑ Convenio entre el MCCD* y la UPM
- ❑ *“Generador de escenarios para el Campo de Maniobras del MCCD”*
- ❑ Enero 2016 – Diciembre 2016
- ❑ Docencia en Ciberdefensa y redes

****MCCD = Mando Conjunto de Ciberdefensa***



Objetivos

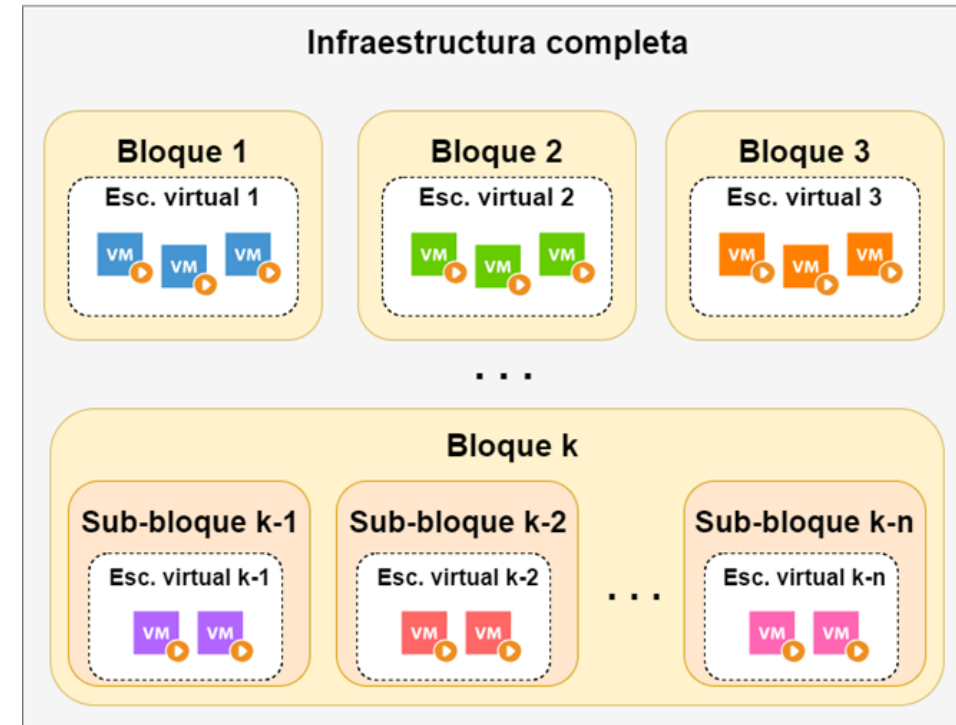
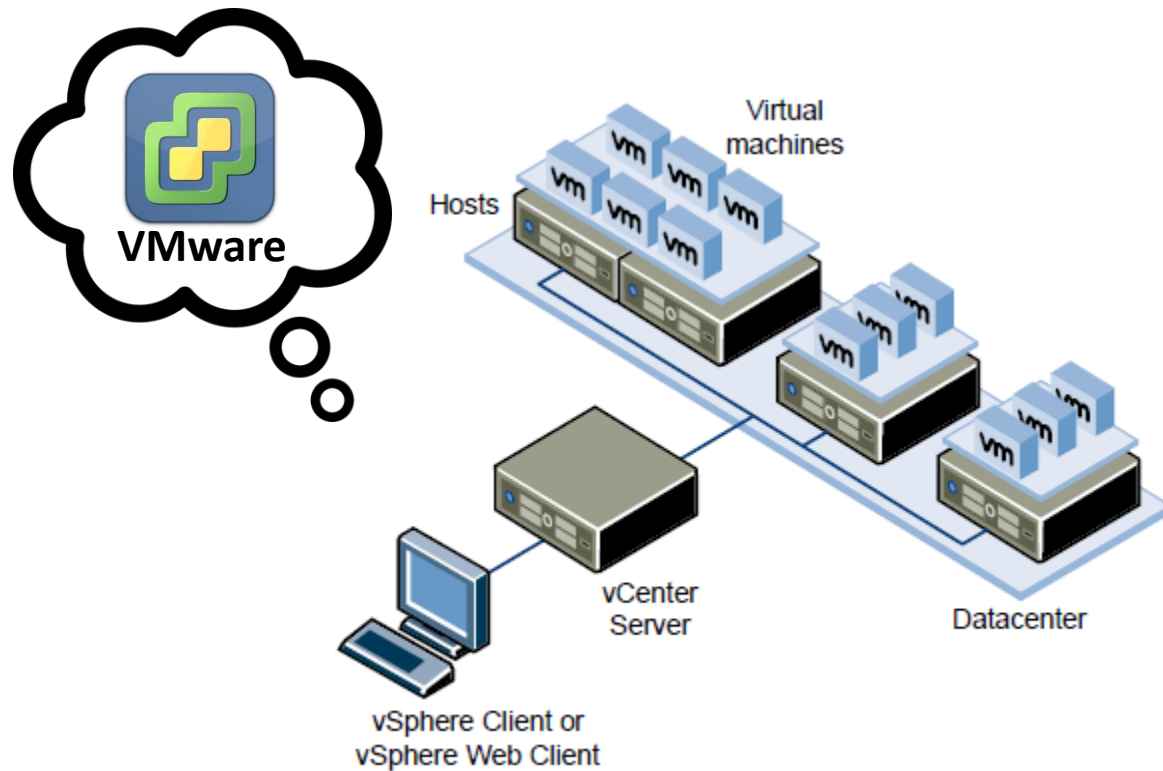
- ❑ Facilitar acceso y configuración de escenarios virtuales en el Campo de Maniobras del MCCD
- ❑ Representación y manipulación de las topologías de red
- ❑ Acceso remoto mediante una aplicación web
- ❑ Sencilla e intuitiva, minimizando intervención del usuario
- ❑ Acceso seguro y controlado



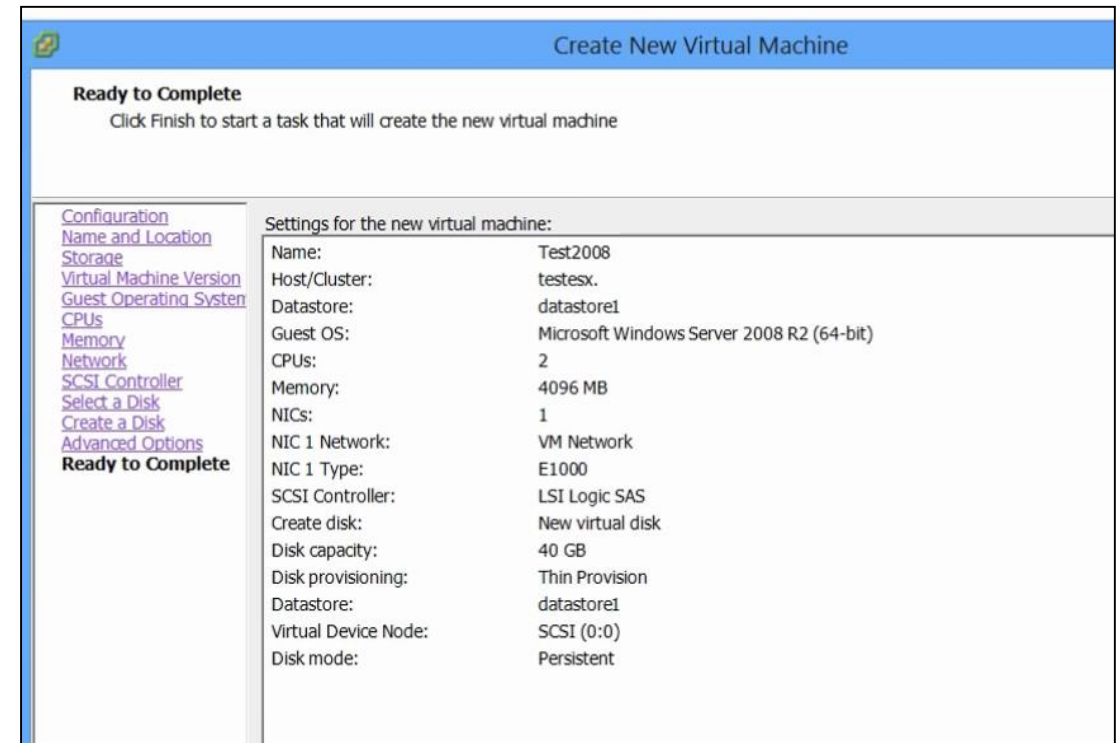
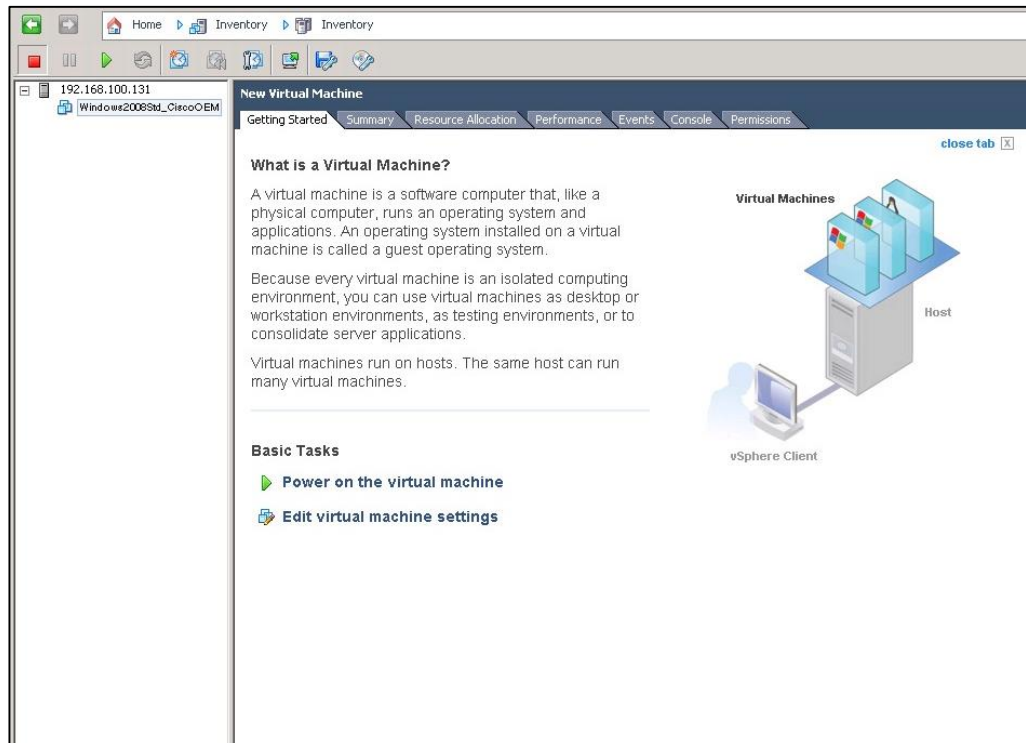
Índice

- ☐ Introducción y objetivos
- ☒ **Infraestructura del MCCD**
- ☐ Desarrollo de la herramienta
- ☐ Interfaz de usuario
- ☐ Conclusiones

El Campo de Maniobras del MCCD



Acceso al Campo de Maniobras (solución previa)

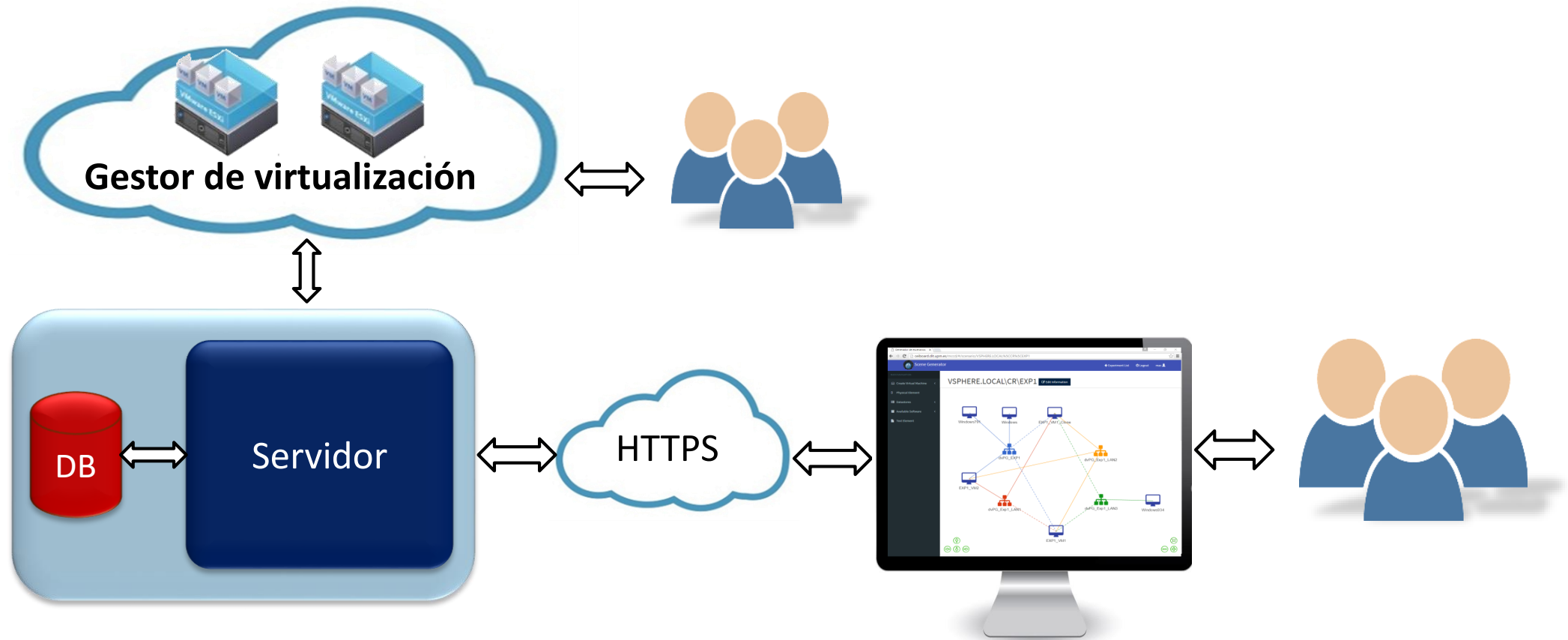


Mediante *vSphere Client*: Proceso lento y complejo

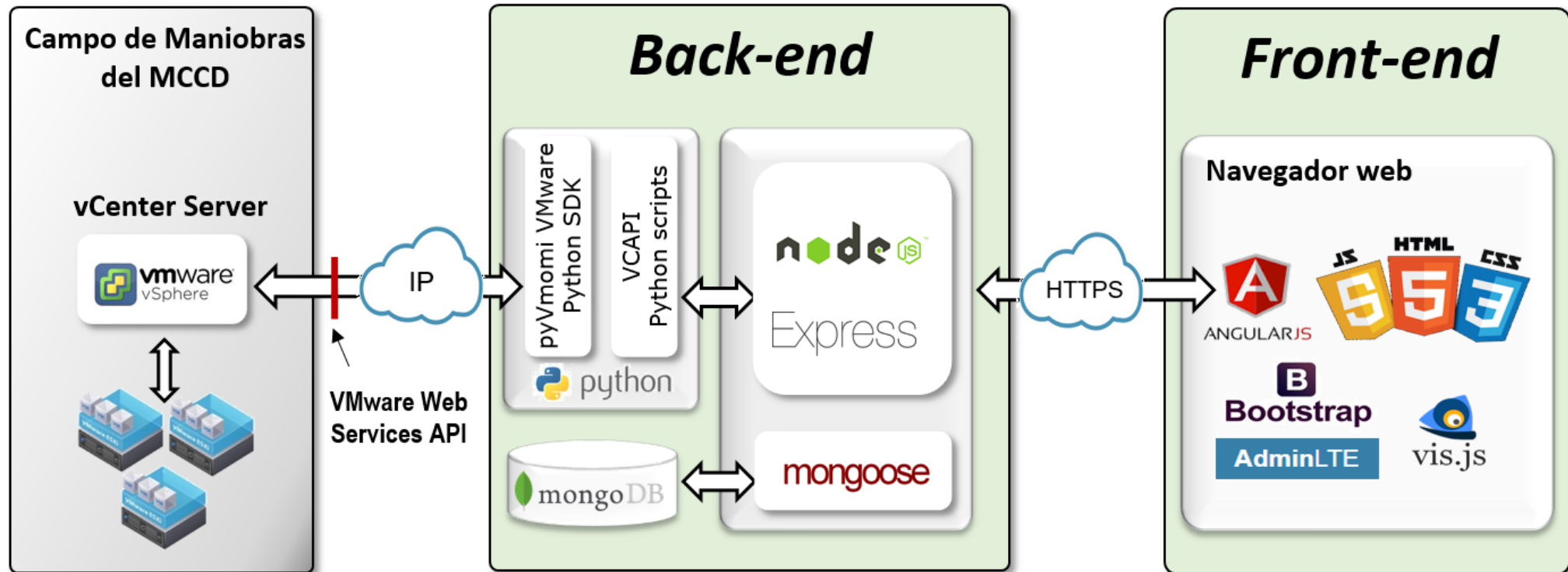
Índice

- ☐ Introducción y objetivos
- ☐ Infraestructura del MCCD
- ☒ **Desarrollo de la herramienta**
- ☐ Interfaz de usuario
- ☐ Conclusiones

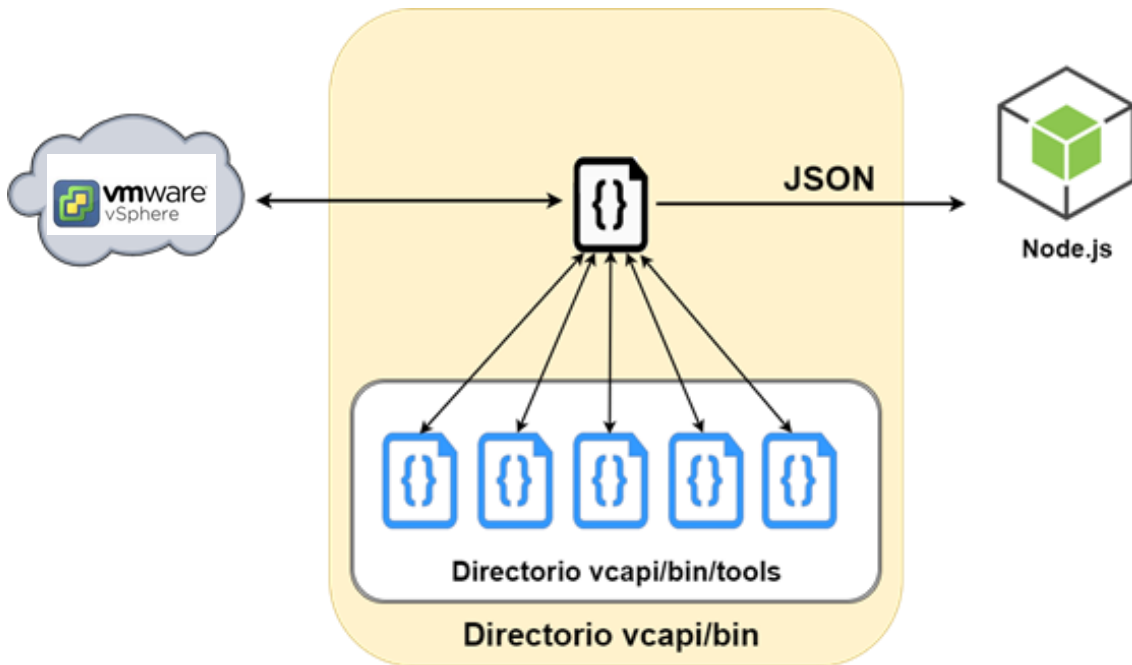
Arquitectura de la solución propuesta



Arquitectura detallada



Interacción con VMware (interfaz VCAPI)



- ☐ Desarrollo de librería VCAPI (Python)
- ☐ Funciones
 - ☐ Control de acceso (**Single Sign-On**)
 - ☐ Listado de escenarios
 - ☐ Máquinas virtuales: crear/clonar/borrar/renombrar
 - ☐ Conexión a redes
 - ☐ Configuración de direcciones IP
 - ☐ Abrir consola de una máquina
 - ☐ Manejo de templates (plantillas)
 - ☐ **Desplegar servidor DHCP**
 - ☐ Montar USB
 - ☐ **Subir/bajar archivo**
 - ☐ ...

Índice

- ☐ Introducción y objetivos
- ☐ Infraestructura del MCCD
- ☐ Desarrollo de la herramienta
- ☒ **Interfaz de usuario**
- ☐ Conclusiones

Pantalla de login

CYDECAN


usuario11@exp.cm

Sign in

Cyber Defence Canvas




Listado de escenarios


 Cyber Defence Canvas


[Download Logs](#) [Logout](#) [EXP\admin](#)


List of experiments of EXP\admin

EXP\EXP1

 **Description:** Descripción del experimento 2 con espacios y todo y le pongo más cosas para completar

 **Number of machines:** 5


 **Resource Pool:**
RP_Experimento_1_UPM


 **Datastores:**


FREENAS-EXP12-VOL3_EXPERIMENTO1:
60.1 GB/89.8 GB


[Open](#) [Deactivate](#)

EXP\EXP2

 **Description:** Descripción del experimento 2

 **Number of machines:** 2

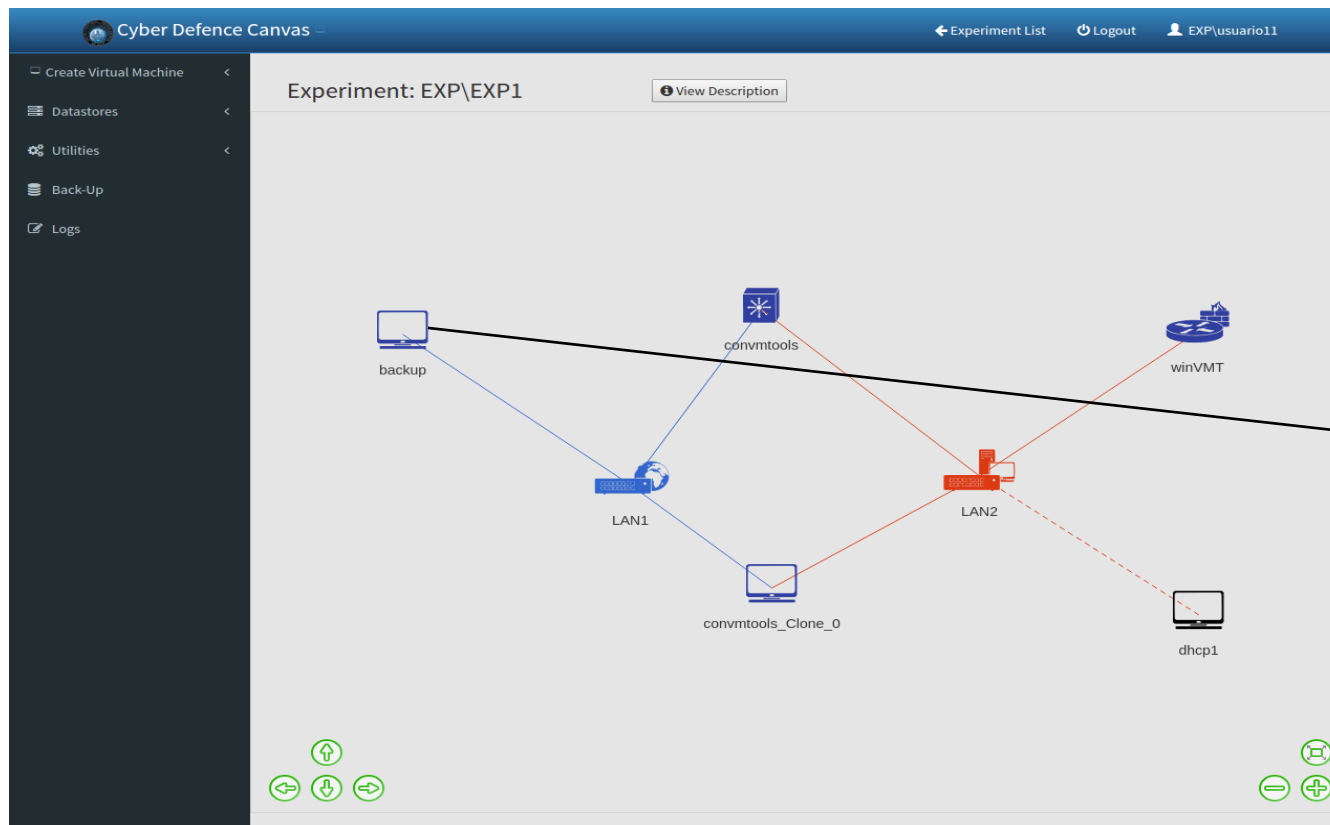
 **Resource Pool:**
RP_Experimento_2_UPM

 **Datastores:**

FREENAS-EXP12-VOL1-EXPERIMENTO2:
1.4 GB/10.8 GB

[Open](#) [Deactivate](#)

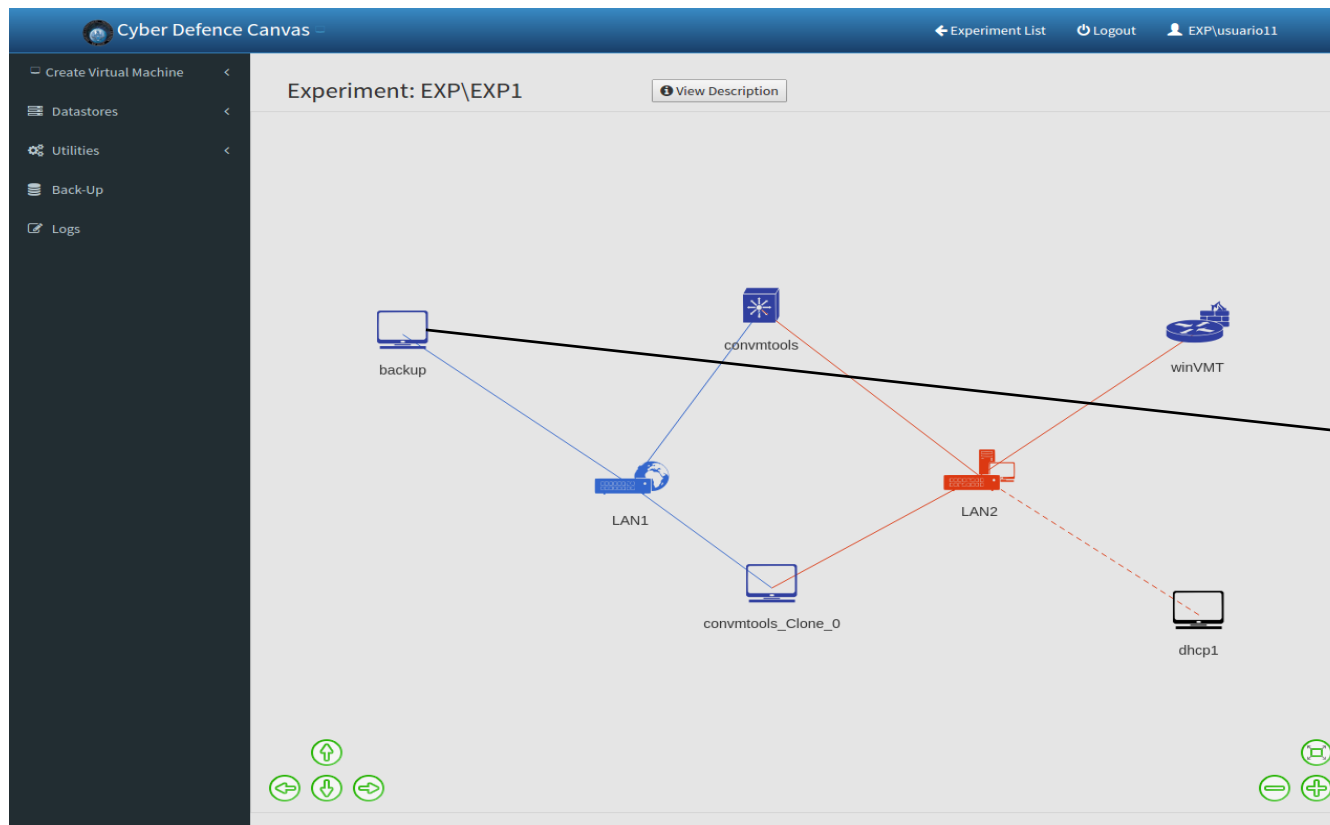
Vista del escenario



Detalles de las máquinas

backup	
VM Details	
VM Actions	
Connections	
Snapshots	
Software	
Name:	backup
Power Status:	poweredOn
Machine OS:	Microsoft Windows Server 2008 R2 (64-bit)
Host Name:	
Guest State:	notRunning
VM Tools:	toolsNotInstalled
Memory:	4.0 GB
Machine Status:	green
Storage:	126.1 MB / 1 GB
Protected with Backup:	true

Vista del escenario



Opciones de las máquinas

backup

VM Details VM Actions Connections Snapshots Software

Power Options: Off Restart

Console: Open Console

VMWare tools: Mount

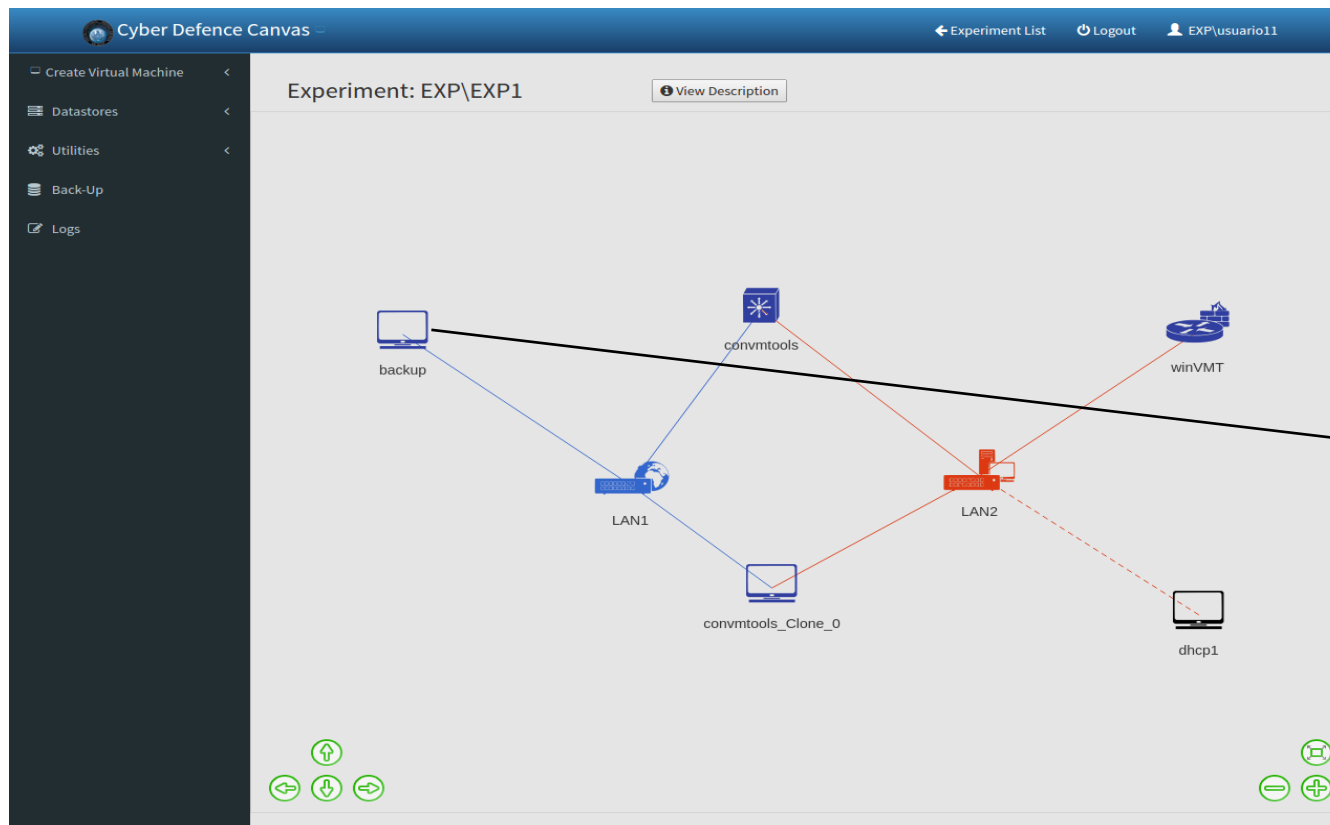
Template: Create Template

Icon: Change

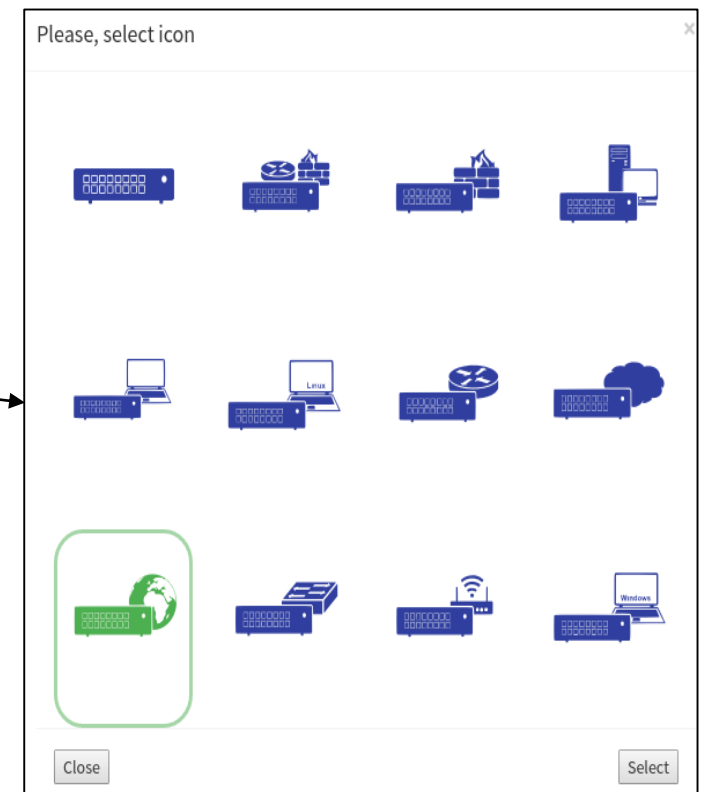
Delete Machine: Delete Machine

Clone Machine: Clone

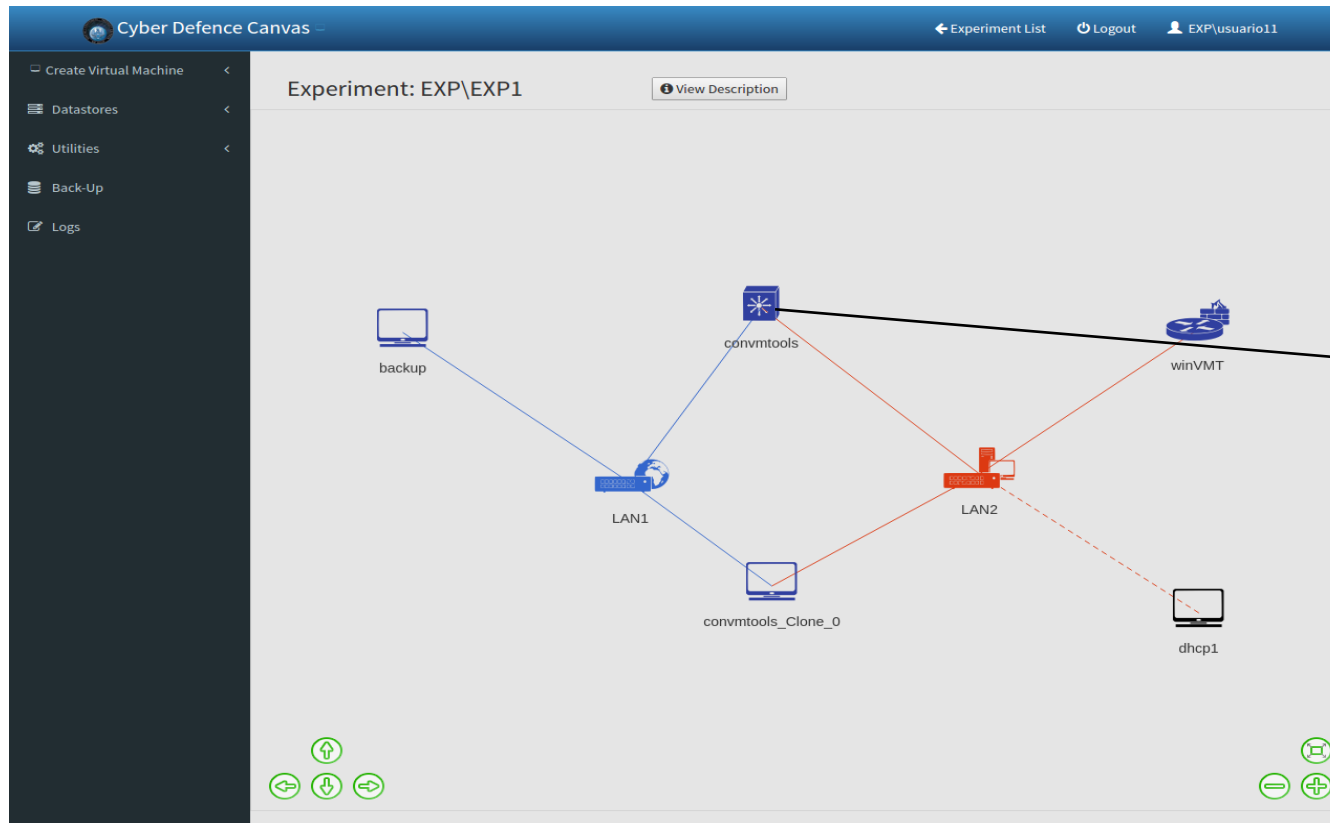
Vista del escenario



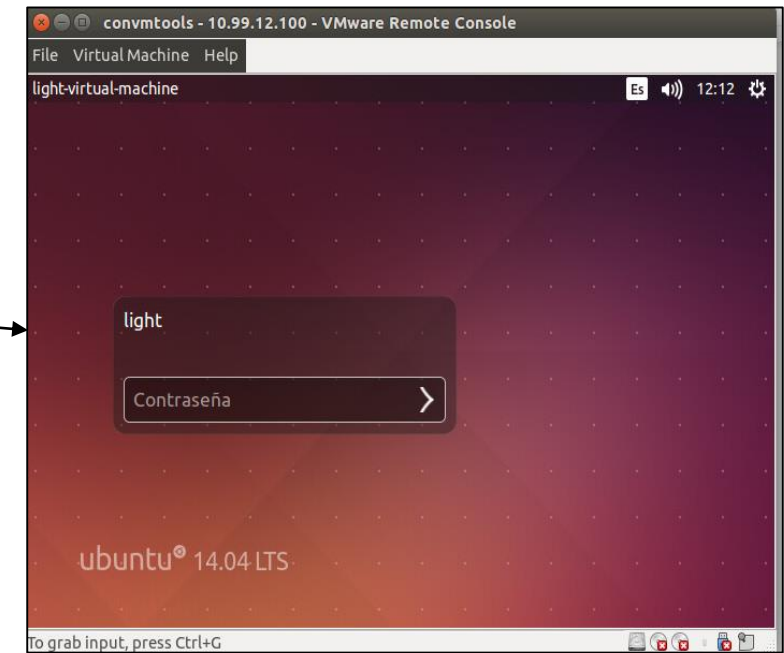
Acción de selección de icono



Vista del escenario



Acción de abrir la consola



Índice

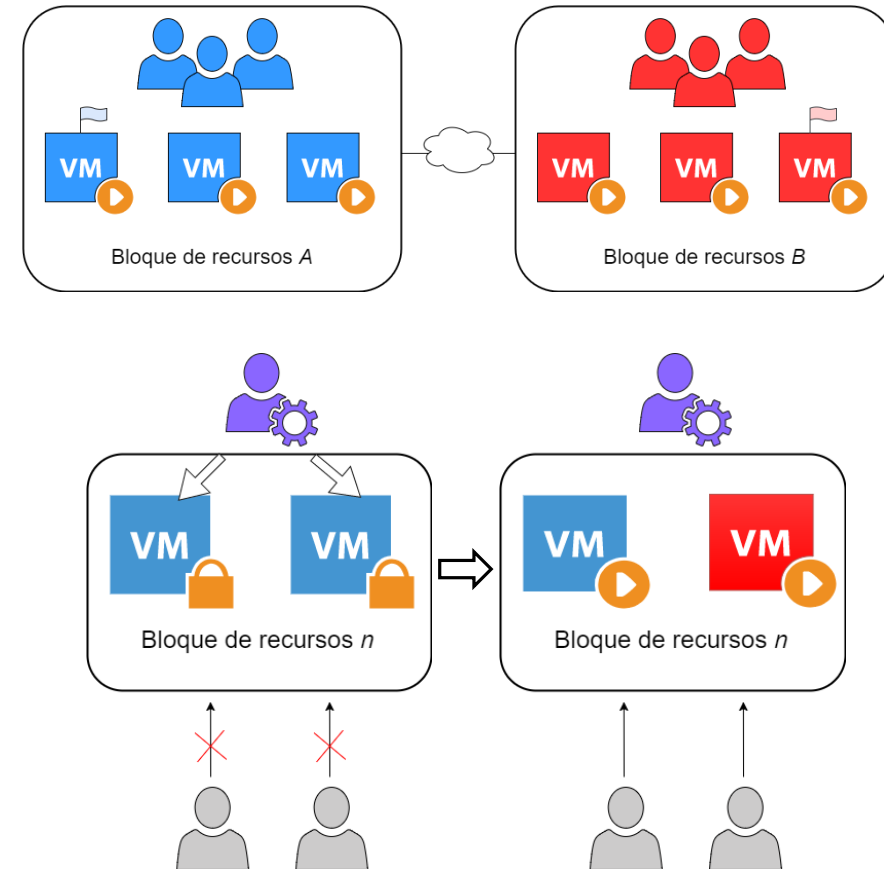
- ☐ Introducción y objetivos
- ☐ Infraestructura del MCCD
- ☐ Desarrollo de la herramienta
- ☐ Interfaz de usuario
- ☒ **Conclusiones**

Conclusiones

- ❑ Herramienta gráfica que facilita el acceso y configuración de escenarios virtuales
 - ❑ Novedosa (no se han encontrado soluciones similares)
 - ❑ Basada en tecnologías WEB más recientes (como AngularJS, MongoDB o Node.js)
 - ❑ Intuitiva y fácil de usar, proporcionando acceso a funciones más frecuentes
- ❑ Utilidad para entrenamiento y formación en ciberdefensa (y otros ámbitos)
- ❑ Permite concentrarse en el curso sin importar la tecnología de virtualización
- ❑ Actualmente en uso por parte del MCCD

Líneas de trabajo

- ❑ Más funcionalidades para los administradores
- ❑ Integración con otras herramientas
- ❑ Adaptación a otras tecnologías de virtualización
- ❑ Aplicación en otros ámbitos



Difusión de resultados

- *I Jornadas de Ciberdefensa 2016* del MCCD (Madrid, mayo 2016)
- *1st Cyber Defence Academy Day* de EDA (Bruselas, septiembre 2016)
- *III Jornadas Nacionales de Investigación en Ciberseguridad* (Madrid, junio 2017)
- *VMWorld Europe* (Barcelona, septiembre 2017)
- Futuras publicaciones



EUROPEAN
DEFENCE
AGENCY



JNIC2017

