

IMPLANTACIÓN DE GRANJA RDS CON ALTA DISPONIBILIDAD

ADRIÁN CABELLO RIVERA

2º ASIR

IES MEDINA AZAHARA

Este trabajo tiene licencia [CC BY-NC 4.0](https://creativecommons.org/licenses/by-nc/4.0/).©



CC POR 4.0



ÍNDICE

1. INTRODUCCIÓN	2
1.2 Objetivos del Proyecto.....	3
Alternativas y propuesta de solución	3
Requisitos	4
Requisitos funcionales	4
Requisitos no funcionales	5
Requisitos de Hardware y Software.....	6
1.3 Enfoque y método seguido.....	7
1.4 Planificación del Proyecto	7
1.5 Costos del Proyecto	9
Hardware:.....	9
Software:	9
2. Documentación técnica.....	10
2.1 VMWare.....	10
2.2 ESXi.....	11
2.2.1 Requisitos para la instalación	11
2.3 Conceptos Básicos	12
2.4 Granja RDS	12
Diagrama de funcionamiento.....	13
Diagrama de la arquitectura de la granja RDS HA.....	16
RECURSOS NECESARIOS.....	18
2.6 Instalación de ESXi	22
2.7 Instalación de vCenter.....	26
2.8 Configuraciones de sistemas	33
2.9 Configuración de Sophos	39
2.11 Configuración de la Alta Disponibilidad	39
Seguimiento y control.....	40
Prueba de conectividad entre RDS1 y BROKER1 "VLAN SERVIDORES".	41
3. CONCLUSIONES	48
Conclusiones y logros alcanzados	48
Desafíos Enfrentados	49
4. BIBLIOGRAFÍA	49

Granja RDS en HA

1. INTRODUCCIÓN

1.1 Contexto y justificación del Proyecto

En el entorno actual de TI, la alta disponibilidad (HA) y la continuidad del negocio son fundamentales para garantizar que los servicios críticos estén siempre operativos. Las granjas de servicios de escritorio remoto (RDS) son esenciales para proporcionar acceso remoto a aplicaciones y escritorios a usuarios finales. Implementar una granja RDS en un entorno de alta disponibilidad asegura que estos servicios sean robustos y puedan resistir fallos de hardware o software.

Este proyecto se justifica por la necesidad de mejorar la resiliencia y disponibilidad de los servicios de TI en una organización mediante la implementación de una infraestructura RDS en HA. La infraestructura de alta disponibilidad es especialmente relevante en entornos de medianas a grandes empresas, tanto en sectores privados como públicos, donde la interrupción del acceso a aplicaciones críticas puede tener un impacto significativo en la productividad y las operaciones diarias.

Ejemplos de organizaciones donde la implementación de una granja RDS en alta disponibilidad ya está en uso:

- Sector financiero: Bancos y empresas de servicios financieros que requieren acceso constante a aplicaciones de trading y gestión de cuentas.
- Salud: Hospitales y clínicas que necesitan acceso permanente a sistemas de gestión de pacientes y aplicaciones de registros médicos electrónicos.
- Educación: Universidades y centros educativos que proporcionan acceso remoto a aplicaciones de aprendizaje y recursos académicos.
- Gobierno: Instituciones gubernamentales que necesitan mantener la continuidad de servicios públicos críticos.

Las ventajas de implementar una infraestructura RDS en alta disponibilidad incluyen:

- Reducción de tiempos de inactividad: Al distribuir la carga entre varios servidores y disponer de redundancia, se minimizan las interrupciones del servicio.

- Mejora de la experiencia del usuario: Los usuarios experimentan menos caídas de servicio y tiempos de respuesta más rápidos.
- Escalabilidad: La infraestructura puede adaptarse fácilmente a un aumento en el número de usuarios o en la demanda de recursos.
- Recuperación ante desastres: La capacidad de recuperación rápida en caso de fallos de hardware o software garantiza la continuidad del negocio.

1.2 Objetivos del Proyecto

1. Implementar una granja de servidores RDS con alta disponibilidad.
2. Configurar y optimizar la infraestructura.
3. Asegurar que los servicios RDS sean redundantes y puedan soportar fallos.
4. Realizar pruebas de alta disponibilidad para garantizar la continuidad del servicio.
5. Monitorizar los recursos para mantener un rendimiento óptimo.

Alternativas y propuesta de solución

Alternativa	Ventajas	Desventajas
Citrix Virtual Apps and Desktops	<ul style="list-style-type: none"> - Altamente escalable - Robustas capacidades de gestión de usuarios y aplicaciones - Excelente rendimiento en redes de alta latencia 	<ul style="list-style-type: none"> - Costo elevado de licencias y mantenimiento - Curva de aprendizaje para el personal técnico si no están familiarizados con Citrix
Microsoft Azure Virtual Desktop (AVD)	<ul style="list-style-type: none"> - Integración nativa con servicios de Microsoft - Pago por uso que puede reducir costes iniciales - Escalabilidad flexible basada en la nube 	<ul style="list-style-type: none"> - Dependencia de la conectividad a Internet - Posibles costes adicionales asociados a la infraestructura de la nube
Implementación con Proxmox	<ul style="list-style-type: none"> - Plataforma de virtualización de código abierto con soporte para alta disponibilidad - Menor costo en comparación con soluciones comerciales - Comunidad activa y soporte 	<ul style="list-style-type: none"> - Puede requerir capacitación adicional del personal si no están familiarizados con Proxmox - Menor integración con algunas herramientas empresariales en comparación con soluciones comerciales

	empresarial disponible	
--	------------------------	--

Propuesta de Solución:

Implementar una granja de servidores RDS con alta disponibilidad utilizando VMware.

Justificación:

- **Familiaridad del Personal:** El personal de TI ya está familiarizado con VMware y ESXi, lo que reduce el tiempo de capacitación y facilita la implementación.
- **Costo y Recursos Existentes:** La organización ya posee licencias de VMware y hardware compatible, lo que minimiza los costos adicionales.
- **Flexibilidad y Escalabilidad:** VMware y ESXi proporcionan una plataforma virtualizada flexible que puede adaptarse fácilmente a cambios en la demanda.
- **Redundancia y Resiliencia:** La capacidad de configurar alta disponibilidad y recuperación ante desastres garantiza que los servicios RDS sean robustos y puedan soportar fallos.
- **Rendimiento y Monitoreo:** Las herramientas de VMware permiten un monitoreo detallado del rendimiento, asegurando que los recursos sean utilizados de manera óptima.

Requisitos

Requisitos funcionales

Usuario centralizado y gestión de sesiones:

Esta infraestructura permitirá la gestión centralizada de usuarios y sesiones, incluida la capacidad de asignar permisos, acceso de usuarios, controlar el uso de recursos y monitorear la actividad de los usuarios.

Alta disponibilidad y recuperación ante desastres:

La infraestructura RDS tiene como objetivo garantizar una alta disponibilidad y recuperación ante desastres, después de un desastre, minimizar el tiempo de inactividad y garantizar la continuidad del servicio en caso de una interrupción.

Escalabilidad y flexibilidad:

Ofrece ser escalable y flexible para adaptarse de acuerdo con las necesidades cambiantes de la organización, lo que permite agregar o eliminar recursos fácilmente según sea necesario.

Integración con Active Directory:

Integración con Active Directory para centralizar el acceso y las políticas.

Requisitos no funcionales**Rendimiento:**

La solución proporcionará un rendimiento óptimo incluso en condiciones de alta carga de usuarios y recursos.

Seguridad:

Se integran medidas para proteger los datos corporativos y evitar el acceso no autorizado.

Facilidad de uso:

La interfaz de usuario debe ser intuitiva y fácil de usar para administradores y usuarios finales.

Mantenimiento y soporte:

Se intenta proporcionar un plan integral de mantenimiento y soporte para poder garantizar que el servicio RDS funcione continuamente en la infraestructura y resolver problemas rápidamente.

Requisitos de Hardware y Software**Hardware:**

Requisitos de Hardware y Software

Hardware:

- Servidores:
 - Procesador: Mínimo 8 núcleos (16 hilos), recomendados procesadores Intel Xeon o AMD EPYC.
 - Memoria RAM: Mínimo 64 GB, recomendados 128 GB o más dependiendo de la cantidad de usuarios.
 - Almacenamiento: Unidades SSD o NVMe con capacidad mínima de 1 TB para almacenamiento rápido y confiable.
 - Red: Tarjetas de red de 10 Gbps para asegurar alta velocidad de conexión y reducir la latencia.
- Almacenamiento:
 - Capacidad: Al menos 2 TB de almacenamiento, escalable según el número de usuarios y el tamaño de sus perfiles.
 - Velocidad: Almacenamiento basado en SSD o NVMe para asegurar tiempos de respuesta rápidos.
- Dispositivos de red:
 - Switches y routers que soporten conexiones de 10 Gbps.
 - Redundancia en los dispositivos de red para asegurar alta disponibilidad.

Software:

Sistemas operativos Windows Server con la correspondiente licencia para cada servidor de la granja.

Software de copia de seguridad Veeam Backup y Replication para realizar las copias de seguridad.

- Sistema operativo TrueNAS para instalar en el servidor de almacenamiento donde se guardarán las copias de seguridad.

*La combinación de Veeam Backup & Replication con TrueNAS proporciona una solución robusta, confiable y rentable para la protección y gestión de datos. Veeam asegura que las copias de seguridad se realicen y se recuperen de manera eficiente, mientras que TrueNAS proporciona un almacenamiento escalable y seguro para estas copias, maximizando la integridad y disponibilidad de los datos.

Otras opciones posibles podrían ser:

Software de copia de seguridad:

- Acronis Cyber Backup

- Commvault
- Veritas Backup Exec

Sistemas operativos para almacenamiento:

- OpenMediaVault
- XigmaNAS
- Unraid

1.3 Enfoque y método seguido

El proyecto se desarrollará siguiendo un enfoque basado en etapas, comenzando con la planificación y definición de requisitos, pasando por la implementación y configuración de la infraestructura, y culminando con pruebas y monitorización. Se utilizarán tecnologías de virtualización de VMWare y configuraciones específicas para asegurar la alta disponibilidad de los servicios RDS.

1.4 Planificación del Proyecto

Fase del Proyecto	Actividad	Descripción	Duración
Preparación del entorno	Configuración del entorno de los servidores	Instalación y configuración inicial de los sistemas operativos en los servidores y configuración básica de red.	3 semanas
Preparación del entorno	Configuración de Active Directory y VLANs en Sophos Firewall	Instalación y configuración de un entorno de Active Directory para autenticación de usuarios y configuración de VLANs en el Sophos Firewall para segmentar la red y mejorar la seguridad.	3 semanas
Preparación del entorno	Instalación de roles y características necesarias	Instalación de los roles de Servicios de Escritorio Remoto (RDS), incluyendo Servidor de Sesión de Escritorio Remoto, Broker de Conexiones, etc. Configuración de características necesarias como el servicio de almacenamiento de archivos para el NAS.	3 semanas
Configuración de la granja RDS	Configuración del rol de Servicios de Escritorio Remoto (RDS)	Configuración de los servidores host de sesión de escritorio remoto y creación de una colección de servidores para alojar	4 semanas

		aplicaciones y escritorios de usuarios. Configuración de políticas de grupo para la administración centralizada.	
Configuración de la granja RDS	Configuración del Sophos Firewall y del almacenamiento NAS	Configuración de reglas de firewall en el Sophos para permitir el tráfico necesario para la granja RDS y asegurar la comunicación segura. Configuración del almacenamiento NAS para el almacenamiento de copias de seguridad.	4 semanas
Pruebas y validación	Pruebas de funcionalidad	Pruebas exhaustivas para verificar el funcionamiento de la granja RDS, incluyendo acceso remoto, autenticación de usuarios y rendimiento del sistema. Pruebas de acceso desde diferentes VLANs y ubicaciones remotas.	2 semanas
Pruebas y validación	Pruebas de resiliencia	Pruebas de tolerancia a fallos y procedimientos de recuperación para evaluar la capacidad de la infraestructura RDS para mantener la disponibilidad del servicio en caso de fallos de hardware o software.	2 semanas
Implementación y puesta en marcha	Implementación de la granja RDS	Una vez completadas las pruebas y validación, implementación en producción para proporcionar una transición fluida desde el entorno de prueba.	1 semana

Calendario 2024

- Preparación del entorno
- Configuración de la granja RDS
- Pruebas y validación
- Implementación y puesta en marcha

Marzo

Lu	Ma	Mi	Ju	Vi	Sa	Do
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Abril

Lu	Ma	Mi	Ju	Vi	Sa	Do
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

Mayo

Lu	Ma	Mi	Ju	Vi	Sa	Do
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

Junio

Lu	Ma	Mi	Ju	Vi	Sa	Do
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

1.5 Costos del Proyecto

Hardware:

Servidores físicos: Un coste aproximado de unos 3.000€, que puede variar según las especificaciones técnicas que se deseen para cada servidor y la marca.

Almacenamiento: Dependiendo de la capacidad y velocidad de los discos duros, puede variar el precio de 100€ a 500€ aproximadamente.

NAS: Un servidor de almacenamiento con un coste aproximado de 1500 euros aunque puede variar según la marca y características.

Sophos Firewall: Aproximadamente unos 2000 euros aunque puede variar.

Software:

Licencias de Windows: El coste de las licencias depende según la edición elegida, según la web de Microsoft pongamos unos 1000€ por servidor.

Licencias de Acceso de cliente (CALs): Varía según el número de usuarios que acceden a los servidores RDS. En Microsoft, 5 CAL de usuario o dispositivo asciende a 1.172€.

Herramientas de respaldo: Se contará con el uso de la herramienta Veeam Data Platform Essentials cuyo coste anual de licencia es de 74,47€ para pequeñas empresas con hasta 50 cargas de trabajo.

TrueNAS Core: Sistema operativo para servidor de almacenamiento NAS (gratuito).

Componente	Cantidad	Precio Unitario (€)	Precio Total (€)
Hardware			
Servidores físicos	1	3000	3000
Almacenamiento	1	300	300
NAS	1	1500	1500
Sophos Firewall	1	2000	2000
Software			
Licencias de Windows	10	1000	10000
Licencias de Acceso de cliente (CALs)	5	234.40	1172
Herramientas de respaldo (Veeam)	1	74.47	74.47
TrueNAS Core (gratuito)	1	0	0
Totales			18046.47

2. Documentación técnica

2.1 VMWare

VMWare es una de las plataformas de virtualización más utilizadas en la industria, proporcionando una solución robusta y escalable para la gestión de máquinas virtuales. Con VMWare, es posible crear y gestionar entornos virtuales que optimizan el uso de recursos y mejoran la eficiencia operativa.

2.2 ESXi

ESXi es un hipervisor de tipo 1 desarrollado por VMWare, que permite ejecutar múltiples sistemas operativos en un solo hardware físico. Es conocido por su eficiencia y fiabilidad, y es una pieza clave en la creación de entornos virtualizados de alta disponibilidad.

2.2.1 Requisitos para la instalación

Para la instalación de ESXi, se requieren los siguientes componentes:

- Hardware compatible con VMWare ESXi.
 - ◆ ESXi 6.5 requiere un equipo host con al menos dos núcleos de CPU.
 - ◆ ESXi 6.5 admite procesadores x86 de 64 bits desde septiembre de 2006. Esto incluye una amplia gama de procesadores de varios núcleos. Para obtener una lista completa de procesadores compatibles, consulte la guía de compatibilidad de VMware en <http://www.vmware.com/resources/compatibility>.
 - ◆ ESXi 6.5 requiere que el bit NX/XD esté habilitado para la CPU en el BIOS.
 - ◆ ESXi 6.5 requiere un mínimo de 4 GB de RAM física. Se recomienda proporcionar al menos 8 GB de RAM para ejecutar máquinas virtuales en entornos de producción típicos.
 - ◆ Para admitir máquinas virtuales de 64 bits, se debe habilitar la compatibilidad para virtualización de (Intel VT-x o RVI AMD) en CPU x64.
 - ◆ Una o más controladoras Gigabit o Ethernet más rápidas. Para obtener una lista de modelos de adaptadores de red compatibles, consulte la Guía de compatibilidad de VMware en <http://www.vmware.com/resources/compatibility>.
 - ◆ Disco SCSI o un LUN RAID local que no sea de red con espacio sin particionar para las máquinas virtuales.
- Acceso a una red estable.
 - ◆ Una red estable es una red informática que mantiene un funcionamiento continuo y confiable, con alta disponibilidad, baja latencia, redundancia para evitar caídas, seguridad contra amenazas, gestión eficiente del tráfico y buen mantenimiento.
- Licencias adecuadas de VMWare.
 - ◆ <https://docs.vmware.com/es/VMware-vSphere/6.5/com.vmware.vsphere.vcenterhost.doc/GUID-7AFCC64B-7D94-48A0-86CF-8E7EF55DF68F.html>
- Un dispositivo de almacenamiento para hospedar las máquinas virtuales.

2.3 Conceptos Básicos

- Virtualización: La creación de una versión virtual de algo, como hardware de computadora, sistemas operativos, dispositivos de almacenamiento, etc.
- Hipervisor: Software que crea y ejecuta máquinas virtuales.
- Alta Disponibilidad (HA): Característica que asegura que los sistemas continúen operativos a pesar de fallos en el hardware o el software.
- RDS (Remote Desktop Services): Tecnología de Microsoft que permite a los usuarios acceder a escritorios y aplicaciones de manera remota.

2.4 Granja RDS

Una granja RDS (Remote Desktop Services Farm) es una infraestructura de tecnología de la información compuesta por un grupo de servidores que trabajan en conjunto para proporcionar servicios de escritorio remoto a los usuarios. Estos servidores están configurados para compartir la carga de trabajo y proporcionar redundancia, lo que significa que si uno de los servidores falla, los otros pueden continuar proporcionando servicios sin interrupciones significativas.

Características principales de una granja RDS:

Distribución de la carga: Los servidores en una granja RDS distribuyen equitativamente las solicitudes de los usuarios, lo que permite un uso eficiente de los recursos y una mejor experiencia del usuario al evitar sobrecargas en un solo servidor.

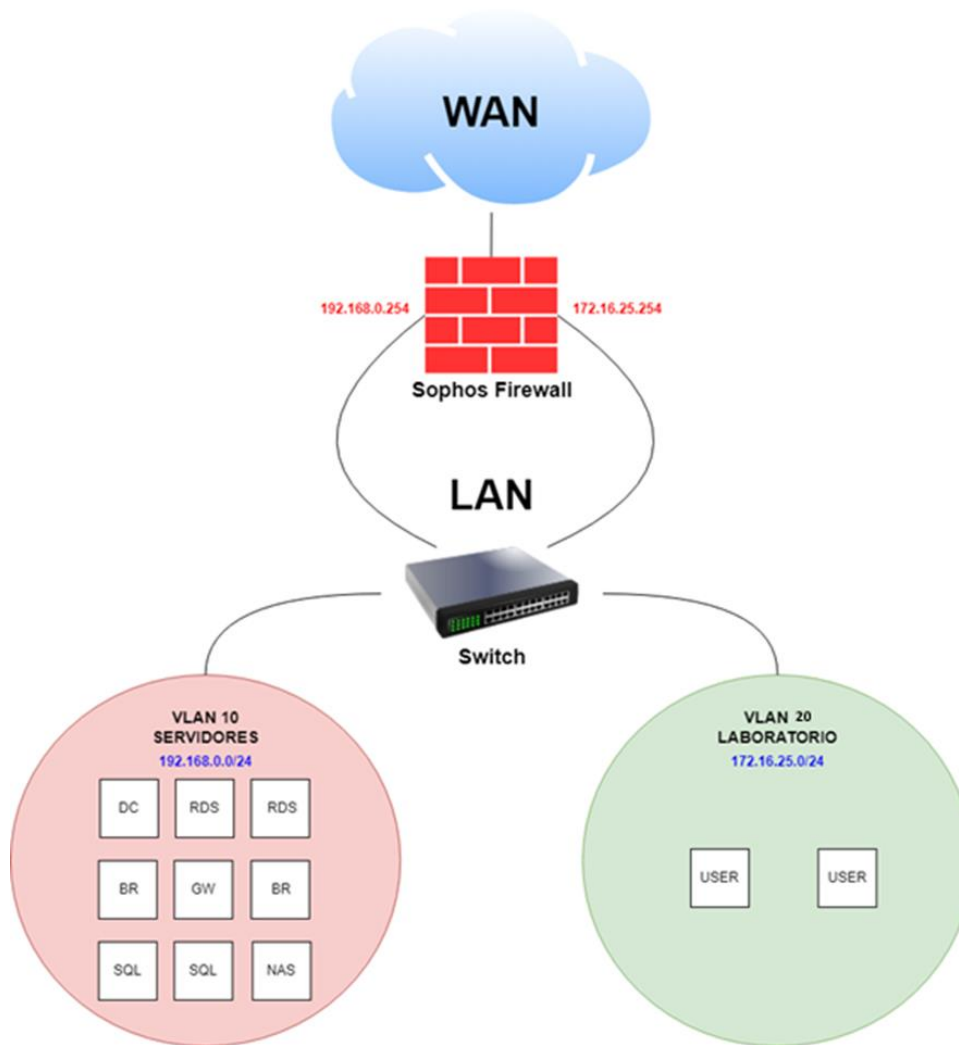
Alta disponibilidad: Gracias a la redundancia, la granja RDS puede seguir operando incluso si uno o varios servidores fallan. Esto garantiza que los usuarios tengan acceso continuo a sus aplicaciones y escritorios remotos.

Escalabilidad: Las granjas RDS pueden escalarse fácilmente añadiendo más servidores según sea necesario, lo que permite adaptarse a un número creciente de usuarios sin sacrificar el rendimiento.

Gestión centralizada: Una granja RDS permite una gestión centralizada de los servidores, facilitando tareas de administración como actualizaciones de software, configuraciones de seguridad y monitoreo del rendimiento.

Diagrama de funcionamiento

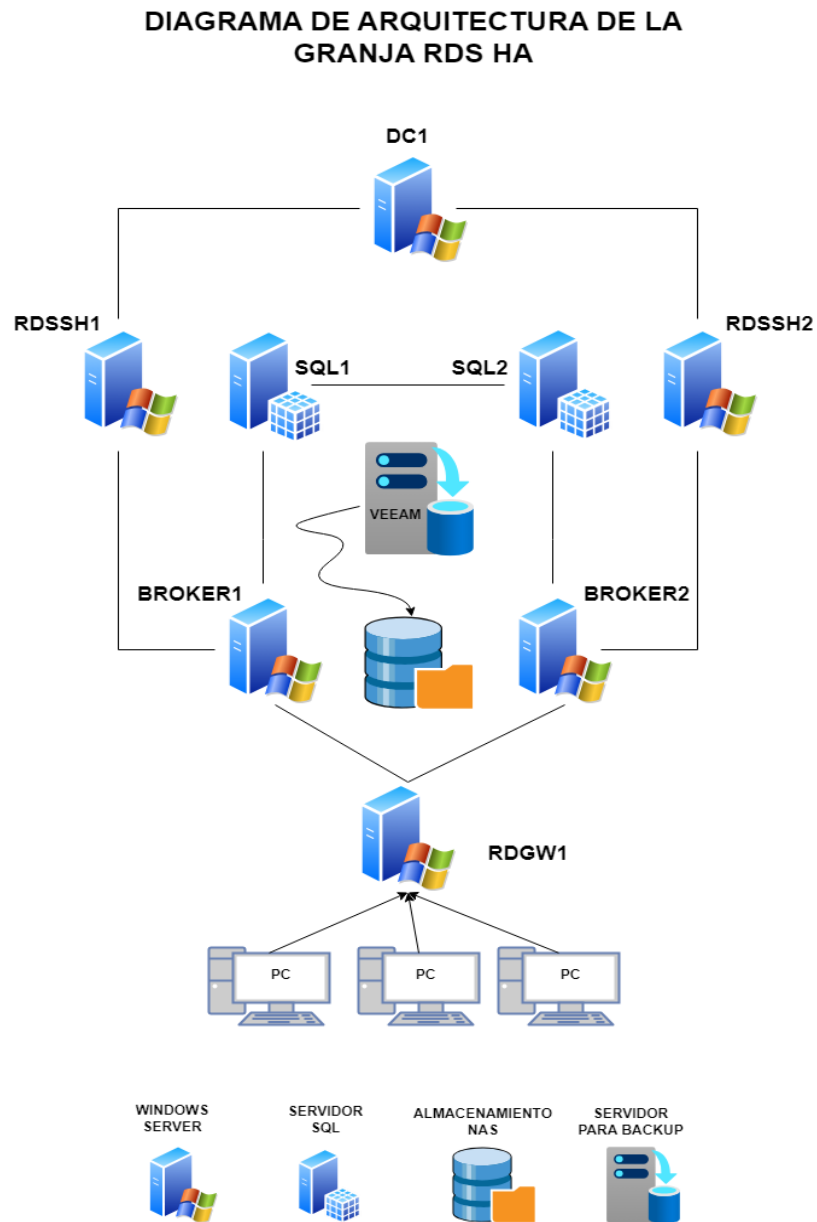
DIAGRAMA DE FUNCIONAMIENTO DE LA ESTRUCTURA DE RED EN LA GRANJA RDS



*SERVIDORES: VLAN creada para la infraestructura RDS.

*LABORATORIO: VLAN creada para los clientes y pruebas, estando separada de la red de servidores pero accesible mediante creación de reglas de firewall.

Diagrama de la arquitectura de la granja RDS HA



DC: Controlador de dominio.

BROKER: Balanceador.

RDGW: Puerta de enlace.

RDSSH: Host de sesión de escritorio remoto.

RECURSOS NECESARIOS

Para la realización de la infraestructura RDS propuesta en el proyecto, debido a la escasez de recursos, se han utilizado diferentes máquinas virtuales ubicadas en un entorno de laboratorio con un hipervisor instalado en un servidor físico, aunque también con varias limitaciones de recursos. El hipervisor utilizado es VMware ESXI, y todo el entorno está instalado en máquinas virtuales con un sistema operativo Windows Server.

En total contamos con 9 máquinas del lado servidor, contando el controlador de dominio DC01, dos agentes de conexión y web access, ambos roles instalados en el mismo servidor, BROKER01 y BROKER02, y por último dos servidores RDS Session Host, RDS01 y RDS02, además de un servidor de ficheros llamado FS02 para unidades de red compartidas, otro llamado TRUENAS para el almacenamiento de copias de seguridad, un servidor SQL para la alta disponibilidad del broker y por último otra llamada Veeam para realizar dichas copias.

Además, también se ha creado una máquina virtual con Sophos Firewall.

Del lado cliente se han configurado dos máquinas virtuales, y varios usuarios de dominio.

Para un funcionamiento ideal y que soporte gran cantidad de usuarios y carga los servidores implementados serían:

1. Controlador de Dominio (DC01)

Nombre: DC01

Sistema Operativo: Windows Server 2022

Función: Controlador de Dominio y Servidor de Certificación de Autoridad (CA)

Hardware:

Procesador: Intel Xeon E-2236, 6 núcleos

RAM: 32 GB

Almacenamiento: SSD de 1 TB

Interfaces de Red: 2 interfaces Gigabit Ethernet, configuradas en modo redundante

2. Agente de Conexión y Web Access (BROKER01 y BROKER02)

Nombre: BROKER01, BROKER02

Sistema Operativo: Windows Server 2022

Función: Agente de Conexión y Web Access

Hardware:

Procesador: Intel Xeon Silver 4214, 12 núcleos

RAM: 64 GB

Almacenamiento: SSD de 512 GB para el sistema operativo y HDD de 2 TB para datos

Interfaces de Red: 2 interfaces Gigabit Ethernet, configuradas en modo redundante

3. Servidor RDS Session Host (RDS01 Y RD02)

Nombre: RDS01, RDS02

Sistema Operativo: Windows Server 2022

Función: Servidor de Host de Sesión de Escritorio Remoto

Hardware:

Procesador: Intel Xeon Gold 5218, 16 núcleos

RAM: 128 GB

Almacenamiento: SSD de 1 TB para el sistema operativo y HDD de 4 TB para perfiles de usuario y datos

Interfaces de Red: 2 interfaces Gigabit Ethernet, configuradas en modo redundante

4. Servidor de Archivos (FS01)

Nombre: FS01

Sistema Operativo: Windows Server 2022

Función: Servidor de Archivos para Unidades Compartidas

Hardware:

Procesador: Intel Xeon E-2278G, 8 núcleos

RAM: 64 GB

Almacenamiento: RAID 10 con 4 SSD de 1 TB cada uno para alta disponibilidad y rendimiento

Interfaces de Red: 2 interfaces Gigabit Ethernet, configuradas en modo redundante

5. NAS para Copias de Seguridad (TrueNAS)

Nombre: TrueNAS01

Sistema Operativo: TrueNAS

Función: Almacenamiento de Copias de Seguridad

Hardware:

Procesador: Intel Xeon Silver 4210, 10 núcleos

RAM: 64 GB

Almacenamiento: RAID 6 con 6 HDD de 4 TB cada uno, proporcionando alta capacidad y redundancia

Interfaces de Red: 2 interfaces Gigabit Ethernet, configuradas en modo redundante

6. Servidor de Copias de Seguridad (Veeam)

Nombre: Veeam

Sistema Operativo: Windows Server 2022

Función: Servidor de Copias de Seguridad con Veeam Backup & Replication

Hardware:

Procesador: Intel Xeon E-2236, 6 núcleos

RAM: 32 GB

Almacenamiento: SSD de 512 GB para el sistema operativo y HDD de 2 TB para almacenamiento temporal de copias de seguridad

Interfaces de Red: 2 interfaces Gigabit Ethernet, configuradas en modo redundante

7.Firewall (Sophos UTM)

Nombre: Sophos

Sistema Operativo: Sophos UTM

Función: Firewall de Red y Gestión de Seguridad

Hardware:

Procesador: Intel Xeon E-2234, 4 núcleos

RAM: 16 GB

Almacenamiento: SSD de 256 GB

Interfaces de Red: 4 interfaces Gigabit Ethernet, configuradas para la segmentación de la red y la redundancia

8. Servidor SQL (SQL01)

Nombre: SQL01

Sistema Operativo: Windows Server 2022 con SQL Server 2019

Función: Servidor de Base de Datos para Alta Disponibilidad del Connection Broker

Hardware:

Procesador: Intel Xeon Gold 6230, 20 núcleos

RAM: 128 GB

Almacenamiento: RAID 10 con 4 SSD de 2 TB cada uno para alta disponibilidad y rendimiento

Interfaces de Red: 2 interfaces Gigabit Ethernet, configuradas en modo redundante

Sin embargo, como ya se ha comentado anteriormente, debido a la escasez de los recursos, toda la infraestructura se ha configurado en máquinas virtuales, todas con un procesador de 2 núcleos, una memoria ram de 2GB y un almacenamiento de 40GB.

2.6 Instalación de ESXi

Estos son los pasos a seguir para la instalación del Hipervisor ESXi de VMWare:

Descarga la ISO de ESXi:

Ve al sitio web de VMware y descarga la imagen ISO de ESXi 6.5.0 U1.

Crea un medio de instalación:



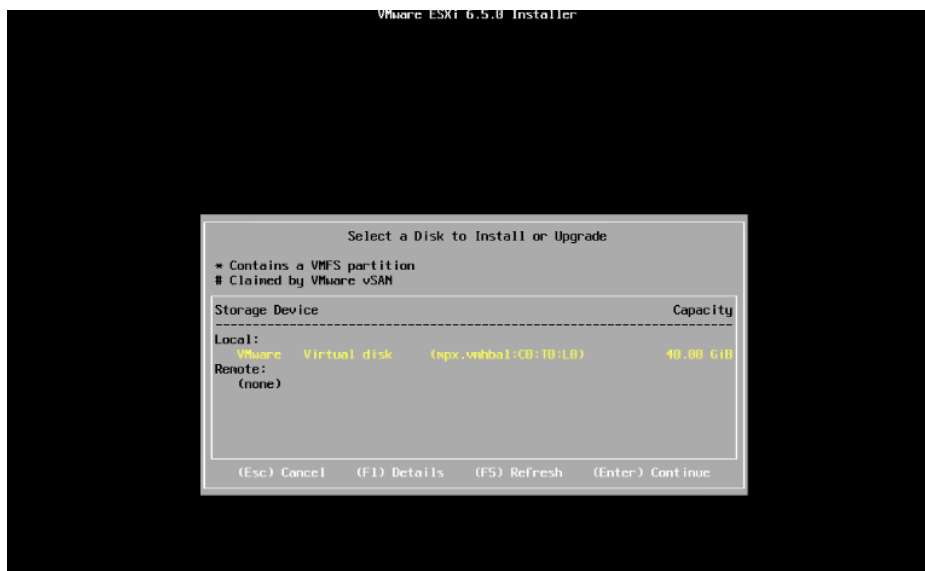
Inicia el instalador de ESXi:

```

Loading ESXi installer
Loading /ueaseln.t00
Loading /esx_dvfi.v00
Loading /esxapi.v00
Loading /lsu_hp_h.v00
Loading /lsu_lsi.v00
Loading /lsu_lsi_.v01
Loading /lsu_lsi_.v02
Loading /lsu_lsi_.v03
Loading /native_n.v00
Loading /rste.v00
Loading /vmware_c.v00
Loading /vsan.v00
Loading /vsanheal.v00
Loading /vsanmgmt.v00
Loading /tools.t00
Loading /Fujitsu_.v00
Loading /xorg.v00
Loading /imgdb.tgz
Loading /imgpayld.tgz
UEFI Secure Boot is not enabled
Shutting down firmware services...
Relocating modules and starting up the kernel...

```

Selecciona el disco de instalación:



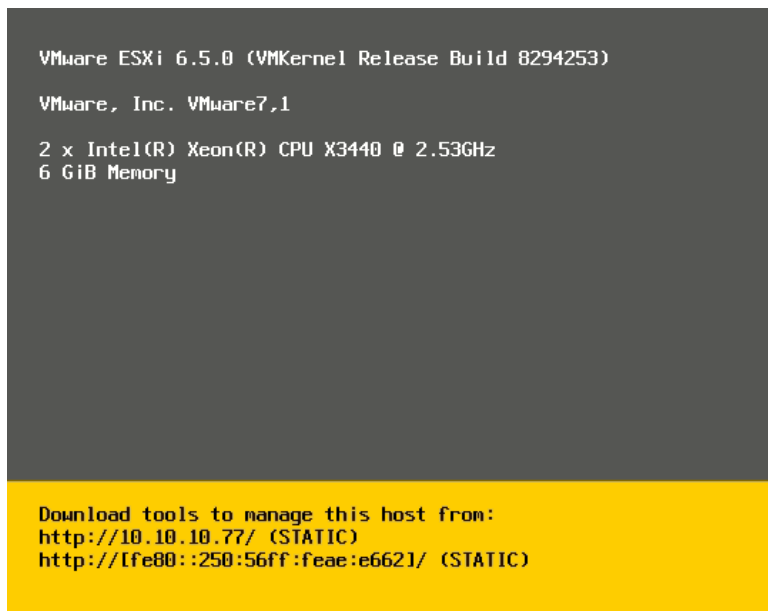
Establece la contraseña de root:



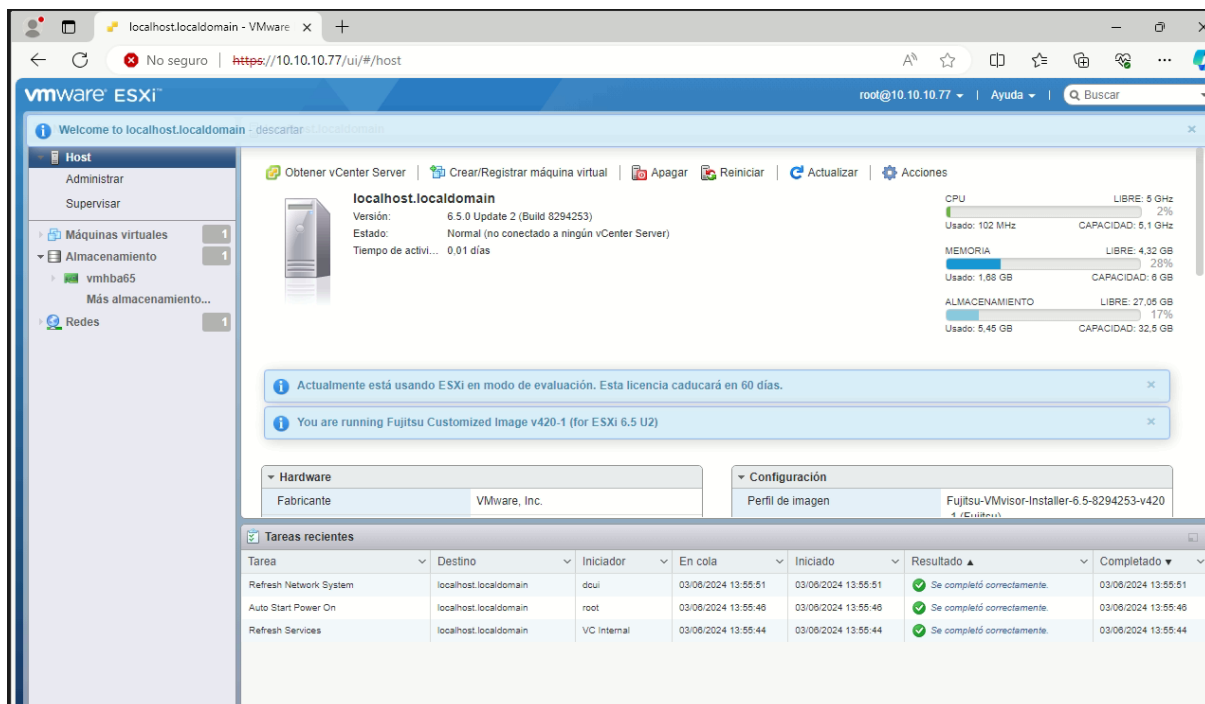
Confirma y comienza la instalación de ESXi.

Una vez completada la instalación, reinicia el servidor.

Conéctate a la dirección IP asignada al servidor ESXi.



Configura el servidor:



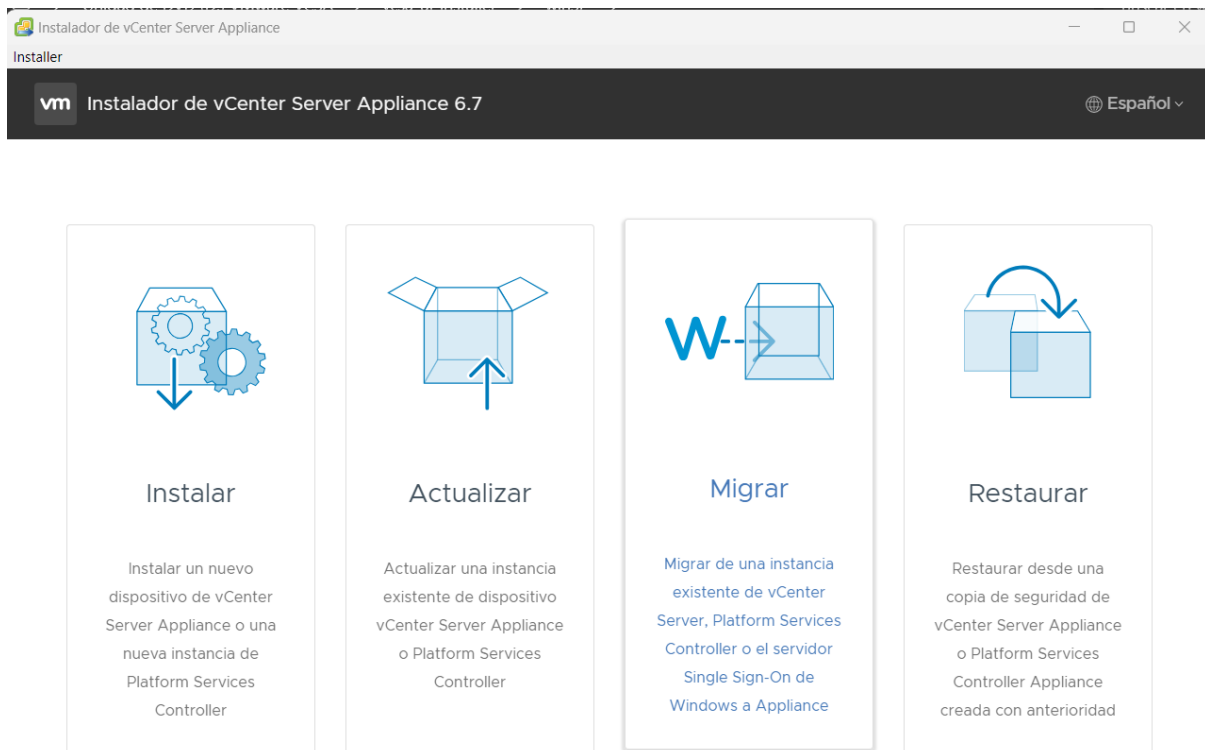
2.7 Instalación de vCenter

¿Qué es vCenter?

vCenter es una plataforma de gestión centralizada para entornos virtualizados, desarrollada por VMware. Permite administrar múltiples hosts de VMware ESXi y sus máquinas virtuales desde una única interfaz. Con vCenter, se pueden realizar tareas como la automatización de operaciones, la implementación y monitoreo de máquinas virtuales, y la gestión de recursos y rendimiento. Es esencial para optimizar y escalar infraestructuras de virtualización en entornos empresariales.

Instalación de vCenter Server Appliance (vCSA)

Selecciona la Opción de Despliegue:



Configura la Información del Servidor:

Instalador de vCenter Server Appliance

Installer

vm

Instalar - Etapa 1: Implementar vCenter Server Appliance con una instancia de Platform Services Controller integrada

1 Introducción

2 Contrato de licencia de usuario final

3 Seleccionar tipo de implementación

4 Destino de implementación del dispositivo

5 Configurar máquina virtual de disp...

6 Seleccionar tamaño de implement...

7 Seleccionar almacén de datos

8 Ajustar la configuración de red

9 Listo para finalizar la etapa 1

Destino de implementación del dispositivo

Especifique la configuración de destino de la implementación del dispositivo. El destino es el host ESXi o la instancia de vCenter Server en los que se implementará el dispositivo.

Nombre de host ESXi o de vCenter Server

10.10.10.77

Puerto HTTPS

443

Nombre de usuario

root

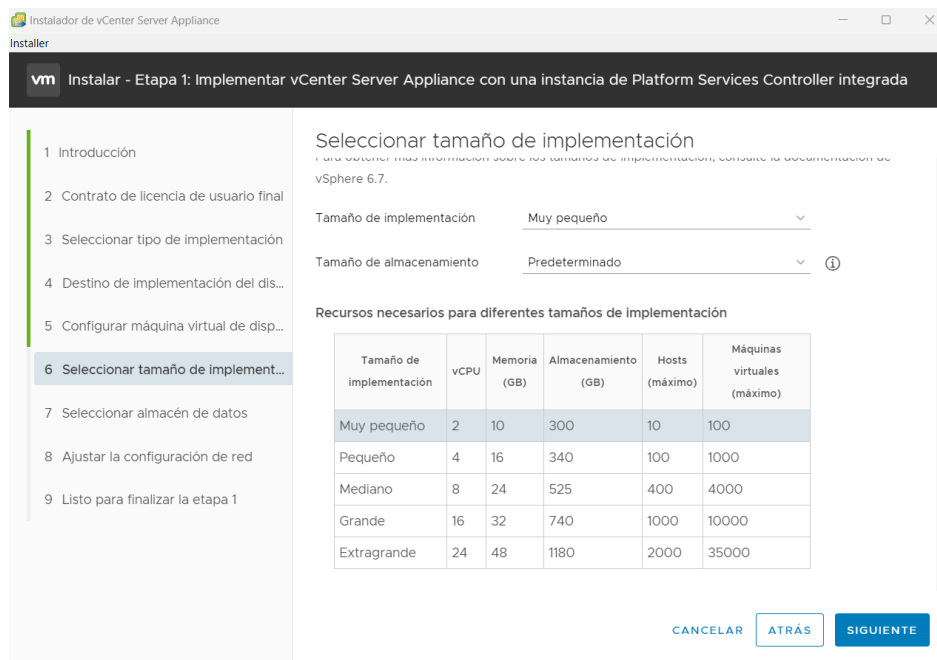
Contraseña

CANCELAR

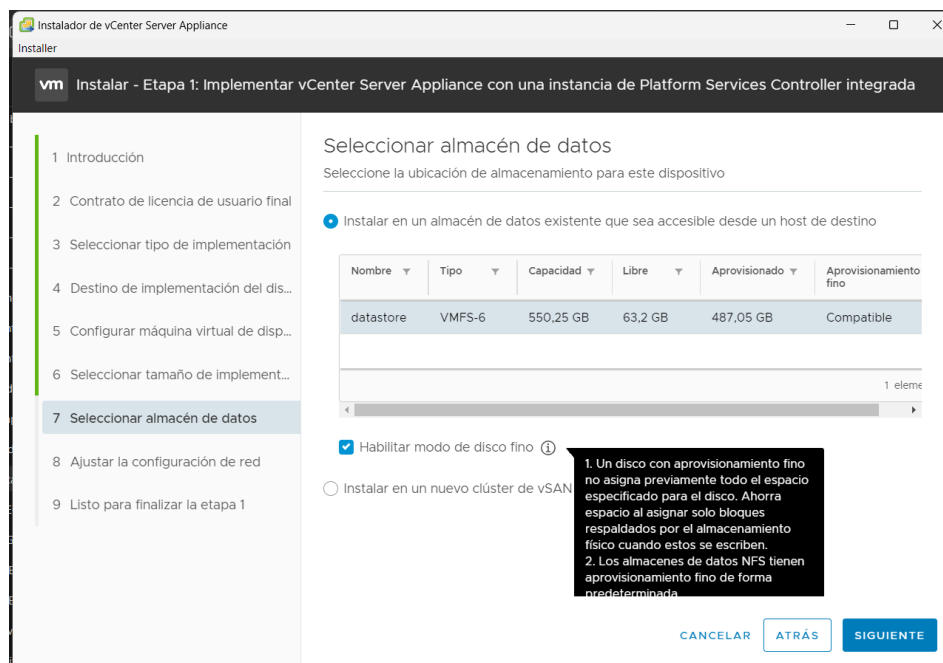
ATRÁS

SIGUIENTE

Especifica el Tamaño del Appliance:



Selecciona el Almacenamiento:



Configura la Red:

Instalador de vCenter Server Appliance
Installer

vm Instalar - Etapa 1: Implementar vCenter Server Appliance con una instancia de Platform Services Controller integrada

1 Introducción
2 Contrato de licencia de usuario final
3 Seleccionar tipo de implementación
4 Destino de implementación del dis...
5 Configurar máquina virtual de disp...
6 Seleccionar tamaño de implement...
7 Seleccionar almacén de datos
8 **Ajustar la configuración de red**
9 Listo para finalizar la etapa 1

Ajustar la configuración de red

Ajustar la configuración de red de este dispositivo

Red	VM Network	①
Versión de IP	IPv4	
Asignación de IP	estática	
FQDN	FQDN (opcional)	①
Dirección IP	10.10.10.78	
Longitud de prefijo o máscara de subred	255.255.255.0	①
Puerta de enlace predeterminada	10.10.10.254	

CANCELAR ATRÁS SIGUIENTE

Completa la Etapa 1:

Instalador de vCenter Server Appliance
Installer

vm Instalar - Etapa 1: Implementar vCenter Server Appliance con una instancia de Platform Services Controller integrada

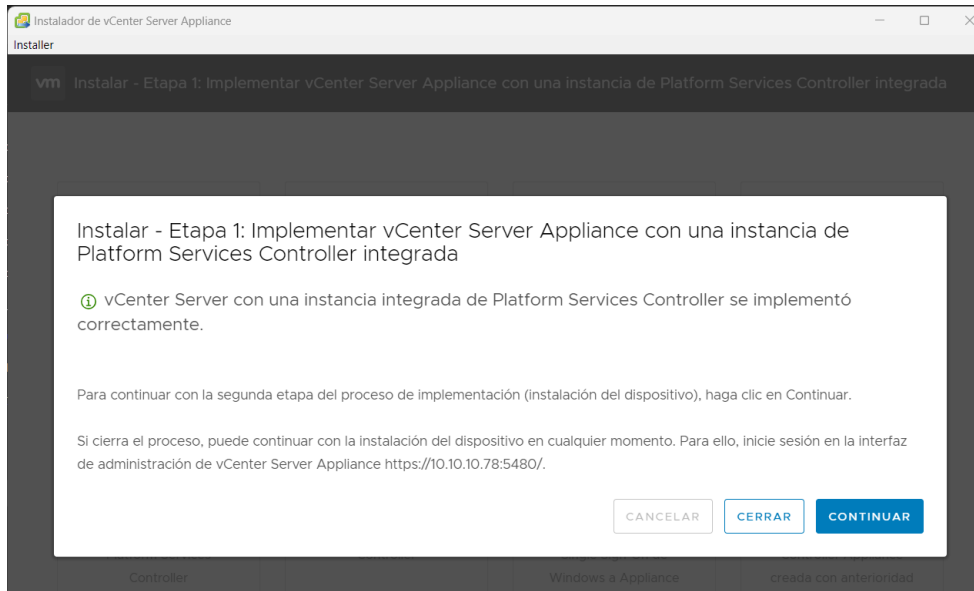
Instalar - Etapa 1: Implementar vCenter Server Appliance con una instancia de Platform Services Controller integrada

6%

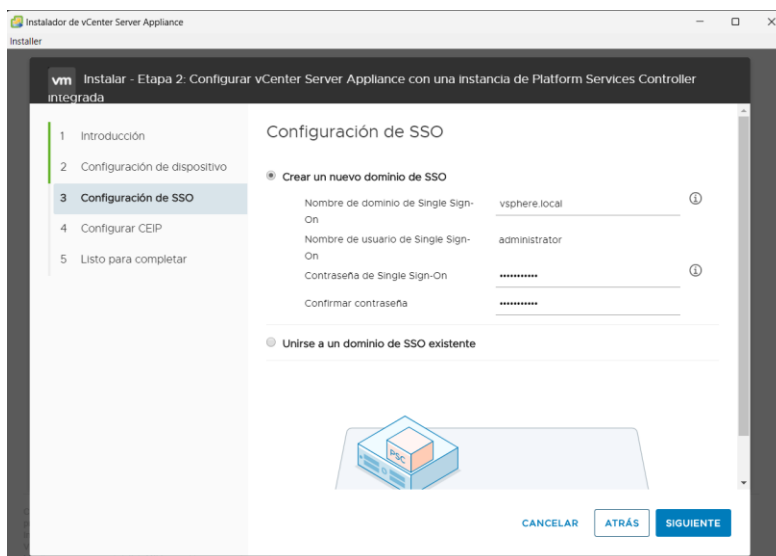
Implementando el dispositivo

CANCELAR

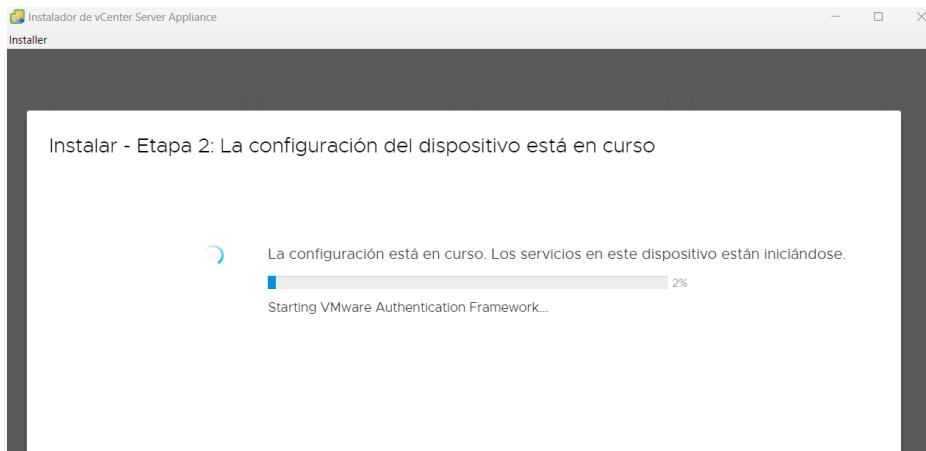
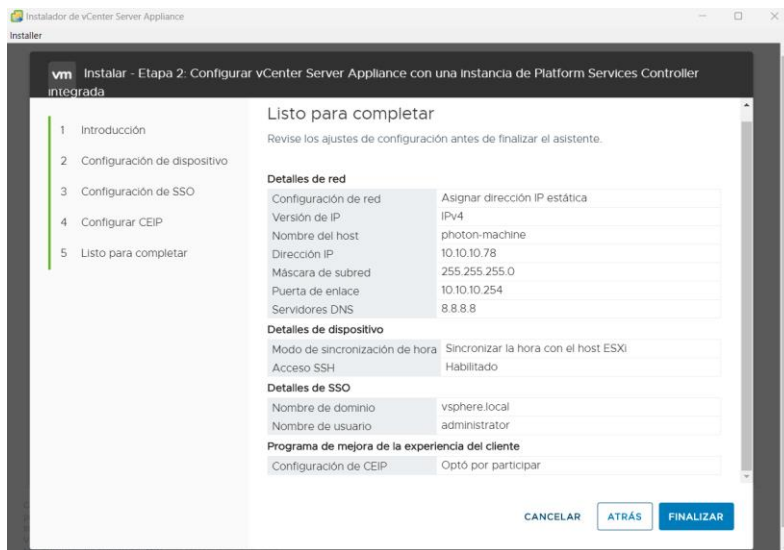
Server Appliance o una nueva instancia de Platform Services Controller
vCenter Server Appliance o Platform Services Controller
Server, Platform Services Controller o el servidor Single Sign-On de Windows a Appliance
vCenter Server Appliance o Platform Services Controller Appliance creada con anterioridad



Configurar vCenter Server:



Finaliza la Instalación:



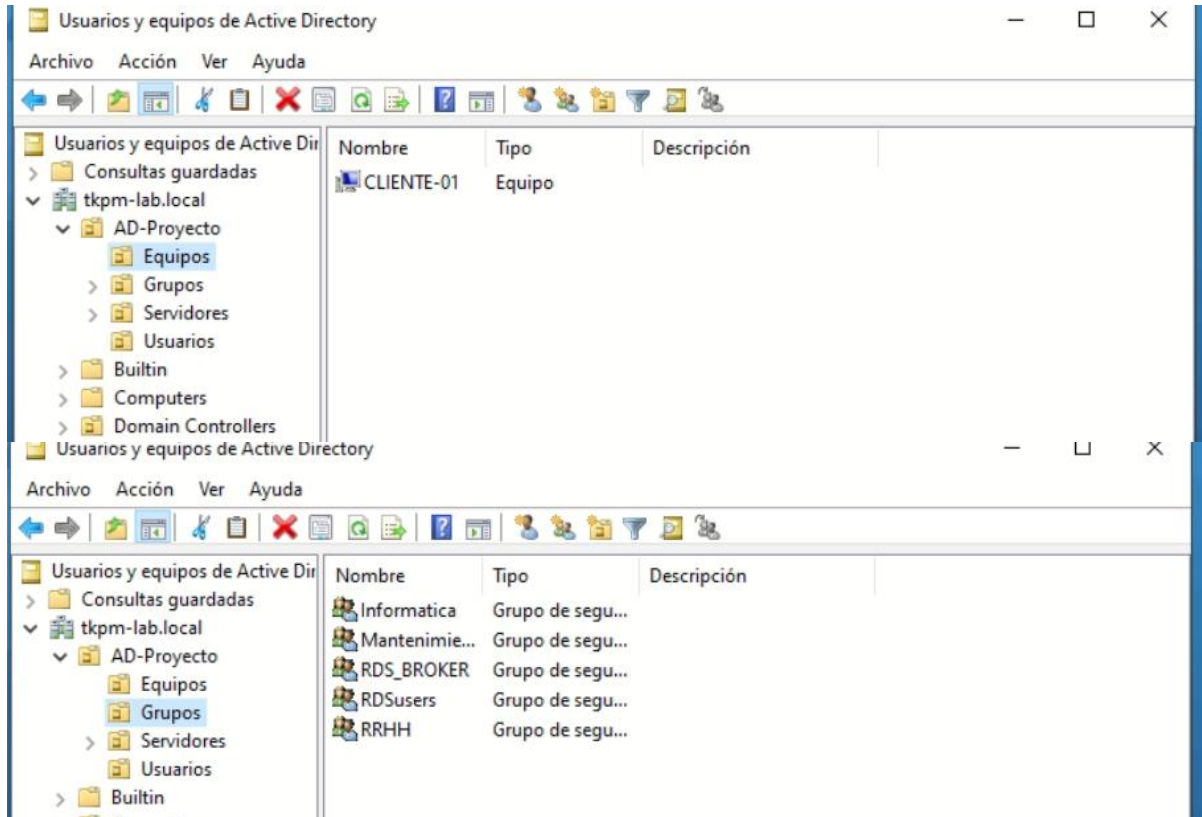
2.8 Configuraciones de sistemas

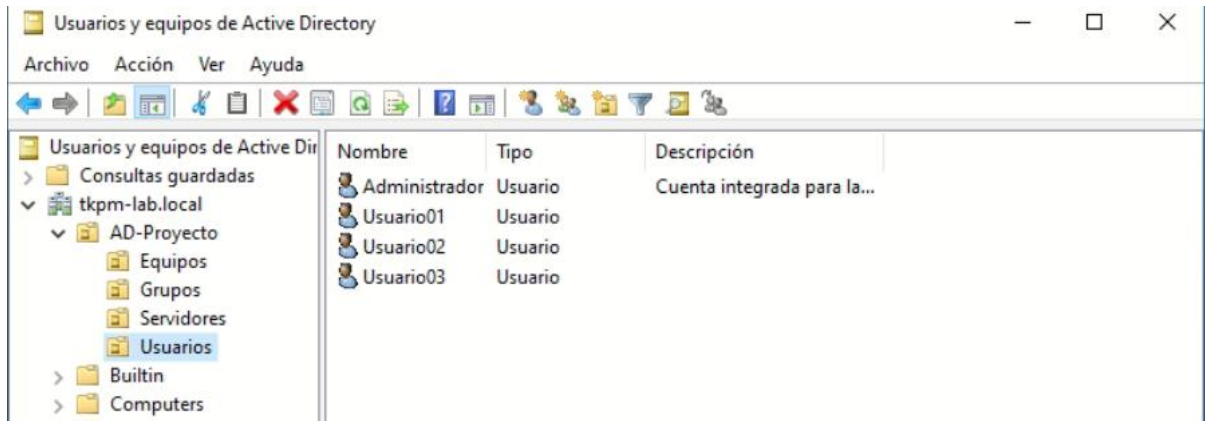
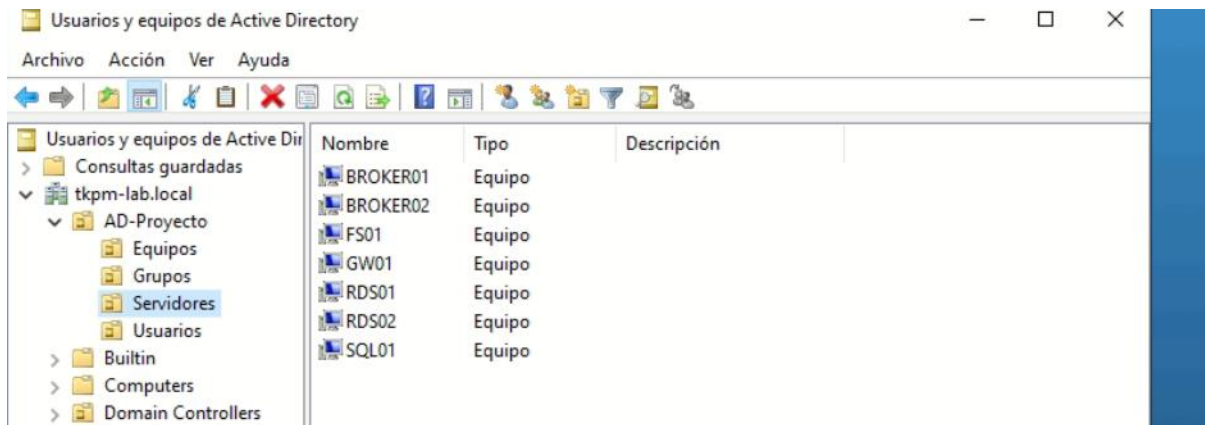
Las configuraciones de los sistemas se han realizado de la siguiente manera:

Para los BROKER y el otro RDS los roles se instalan todos juntos al realizar la instalación de estos en uno de los servidores de la granja (en este caso se ha usado RDS01).

DC01:

- Active Directory:





- DNS:

Administrador de DNS

Archivo Acción Ver Ayuda

DNS

- SERVER-TKPM
 - Zonas de búsqueda directa
 - _msdcs.tkpm-lab.local
 - tkpm-lab.local
 - Zonas de búsqueda inversa
 - 0.168.192.in-addr.arpa
 - Puntos de confianza
 - Reenviadores condicionales

Nombre	Tipo	Datos	Marca
(igual que la carpeta principal)	Inicio de autoridad (SOA)	[539], server-tkpm.tkpm-lab.local.	static
(igual que la carpeta principal)	Servidor de nombres (NS)	server-tkpm.tkpm-lab.local.	static
(igual que la carpeta principal)	Host (A)	192.168.0.90	22/05/2022
BROKER01	Host (A)	192.168.0.91	static
BROKER02	Host (A)	192.168.0.92	static
CLIENTE-01	Host (A)	172.16.25.108	16/05/2022
FS01	Host (A)	192.168.0.101	16/05/2022
GW01	Host (A)	192.168.10.97	20/05/2022
rds	Host (A)	192.168.0.92	static
rds	Host (A)	192.168.0.91	static
RDS01	Host (A)	192.168.0.93	23/05/2022
RDS02	Host (A)	192.168.0.94	22/04/2022
server-tkpm	Host (A)	192.168.0.90	static
SQL01	Host (A)	192.168.0.95	22/05/2022
truenas	Host (A)	192.168.0.100	static

Administrador de DNS

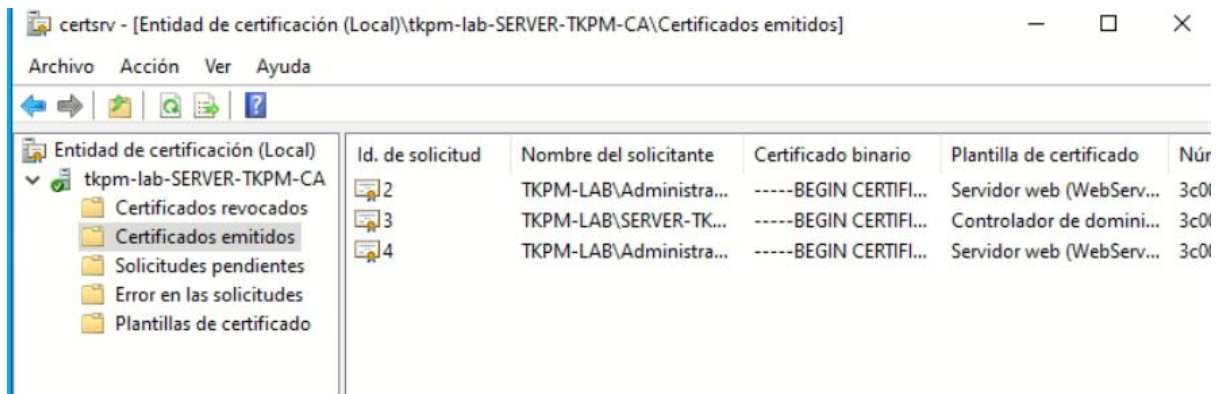
Archivo Acción Ver Ayuda

DNS

- SERVER-TKPM
 - Zonas de búsqueda directa
 - _msdcs.tkpm-lab.local
 - tkpm-lab.local
 - Zonas de búsqueda inversa
 - 0.168.192.in-addr.arpa
 - Puntos de confianza
 - Reenviadores condicionales

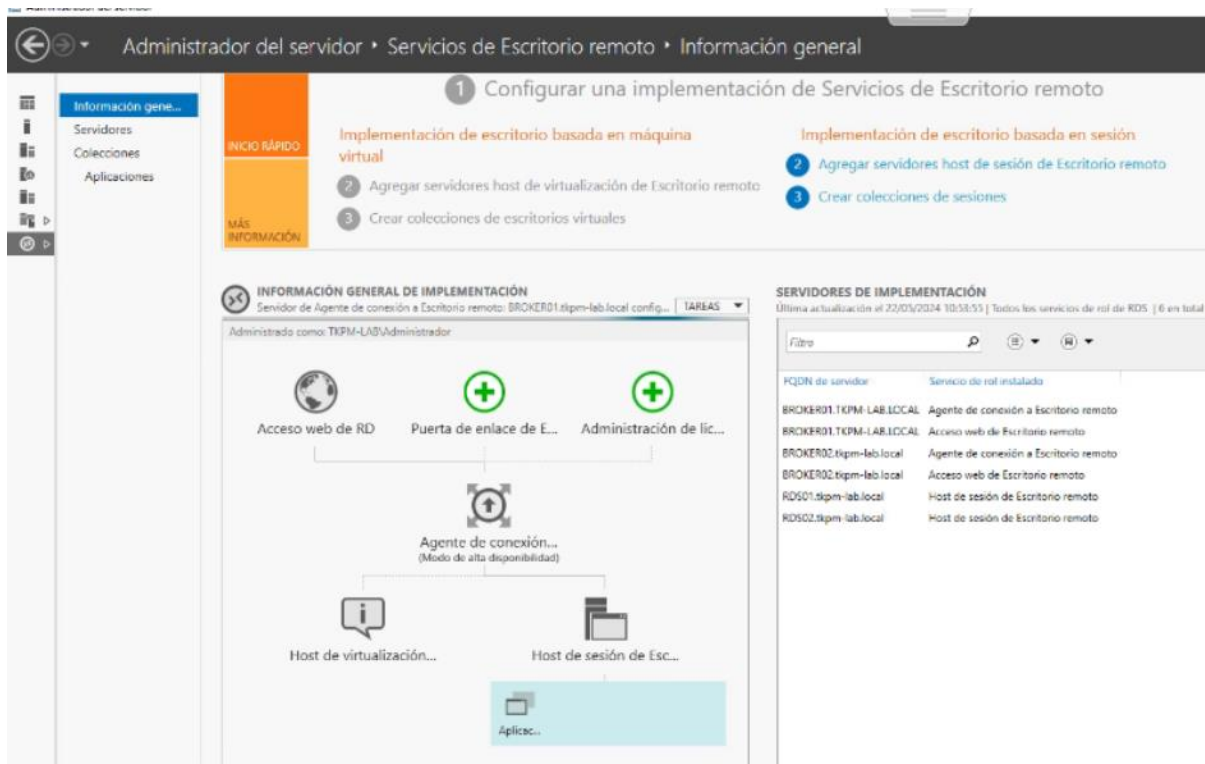
Nombre	Tipo	Datos	Marca de
(igual que la carpeta principal)	Inicio de autoridad (SOA)	[37], server-tkpm.tkpm-lab.local.	static
(igual que la carpeta principal)	Servidor de nombres (NS)	server-tkpm.tkpm-lab.local.	static
192.168.0.100	Puntero (PTR)	truenas.tkpm-lab.local.	static
192.168.0.101	Puntero (PTR)	FS01.tkpm-lab.local.	16/05/2022
192.168.0.90	Puntero (PTR)	SERVER-TKPM.tkpm-lab.local.	22/05/2022
192.168.0.91	Puntero (PTR)	rds.tkpm-lab.local.	static
192.168.0.92	Puntero (PTR)	rds.tkpm-lab.local.	static
192.168.0.93	Puntero (PTR)	RDS01.tkpm-lab.local.	23/05/2022
192.168.0.94	Puntero (PTR)	RDS02.tkpm-lab.local.	23/04/2022
192.168.0.95	Puntero (PTR)	SQL01.tkpm-lab.local.	25/05/2022
192.168.0.97	Puntero (PTR)	GW01.tkpm-lab.local.	23/04/2022

- CA:

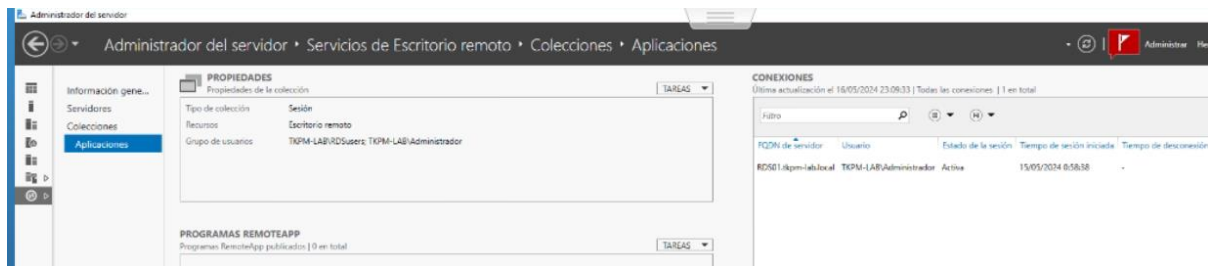


RDS:

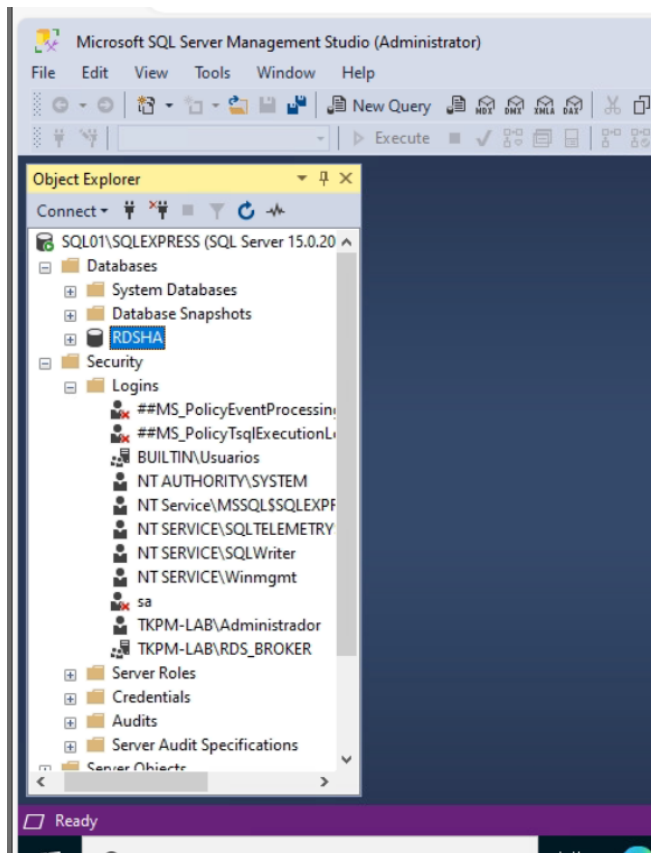
- Roles



- Colecciones



SQL:



2.9 Configuración de Sophos

SOPHOS

Sophos Firewall

- MONITORIZAR Y ANALIZAR**
- Control Center
- Actividades actuales
- Informes
- Protección de día cero
- Diagnósticos
- PROTEGER**
- Reglas y políticas
- Prevención de intrusiones
- Web
- Aplicaciones
- Inalámbrico
- Correo electrónico
- Servidor web
- Protección avanzada
- CONFIGURAR**
- VPN de acceso remoto
- VPN de sitio a sitio
- RED**
- Enrutamiento
- Autenticación
- Servicios de sistema
- SISTEMA**
- Sophos Central
- Perfiles
- Hosts y servicios
- Administración
- Copia de seguridad y firmware
- Correo electrónico
- Servidor web
- Protección avanzada
- CONSEJOS**
- Guías explicativas
- Visor de registros
- Ayuda
- admin@FW_1

RED

Interfaces	Zonas	Administrador de vínculo WAN	DNS	DHCP	Anuncio de enrutador IPv6	WAN móvil
GuestAP WiFi Protección de redes inalámbricas	Desconectado	Autonegociado	10.255.0.1/255.255.255.0 Estática			Hardware: GuestAP
Port1 LAN Físico	Conectados	1000 Mbps - Full Duplex Autonegociado	172.16.16.16/255.255.255.0 Estática			Hardware: Port1
Port2 WAN Físico	Conectados	1000 Mbps - Full Duplex Autonegociado	10.10.10.253/255.255.255.0 Estática			Hardware: Port2
Port3 LAB Físico	Conectados	1000 Mbps - Full Duplex Autonegociado	172.16.25.254/255.255.255.0 Estática			Hardware: Port3
Port4 DMZ Físico	Conectados	1000 Mbps - Full Duplex Autonegociado	192.168.10.254/255.255.255.0 Estática			Hardware: Port4
Port5 SRV Físico	Conectados	1000 Mbps - Full Duplex Autonegociado	192.168.0.254/255.255.255.0 Estática			Hardware: Port5

Traffic to Internet...

entrada 8.16 GB, salida 314.84 MB

This group on the first match basis if user selects automatic grouping option. This is the d...

Traffic to Interna...

entrada 5.72 MB, salida 3.20 MB

To LAN, WiFi, VPN, DMZ, Firewall rules with the destination zone as LAN, WiFi, VPN, DMZ wo...

ld be added to this group on the first match basis if user selects automatic grouping option...

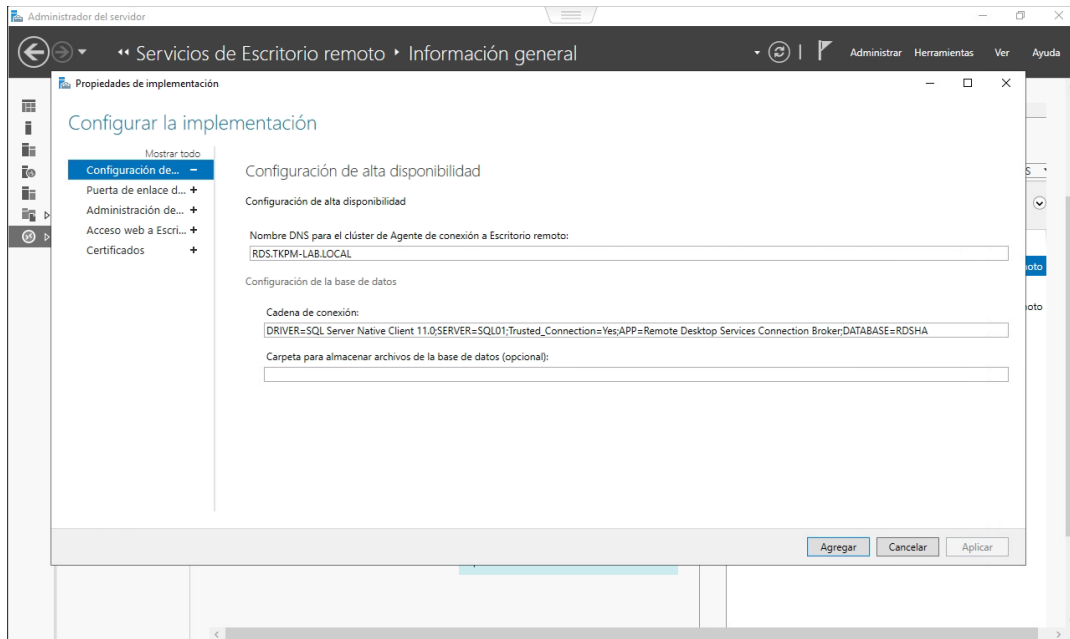
LAB TO SRV

entrada 5.72 MB, salida 3.20 MB

LAB, Cualquier host SRV, Cualquier host Cualquier servicio #14 Aceptar

2.11 Configuración de la Alta Disponibilidad

Configurar la alta disponibilidad implica asegurarse de que todos los componentes críticos del sistema RDS están redundados y que el sistema pueda manejar fallos sin interrumpir el servicio. Esto incluye la configuración de múltiples servidores RDS, balanceadores de carga y almacenamiento redundante.



Seguimiento y control

Para comprobar el correcto funcionamiento de toda la infraestructura de la granja RDS se han realizado diferentes pruebas entre los distintos equipos de los que se dispone, para garantizar la continua conectividad y permanencia en funcionamiento de la infraestructura en caso de fallos. Entre ellas se encuentran:

Conectividad entre las Vlan de la infraestructura y entre los mismos equipos de cada Vlan (Ping, tracert...)

Prueba de conectividad entre RDS1 y BROKER1 "VLAN SERVIDORES".

```
Administrador: Símbolo del sistema
Microsoft Windows [Versión 10.0.20348.587]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\Administrador.TKPM-LAB>ping 192.168.0.91 -t

Haciendo ping a 192.168.0.91 con 32 bytes de datos:
Respuesta desde 192.168.0.91: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.91: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.91: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.91: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.0.91:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
        (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms
Control-C
^C
C:\Users\Administrador.TKPM-LAB>tracert 192.168.0.91

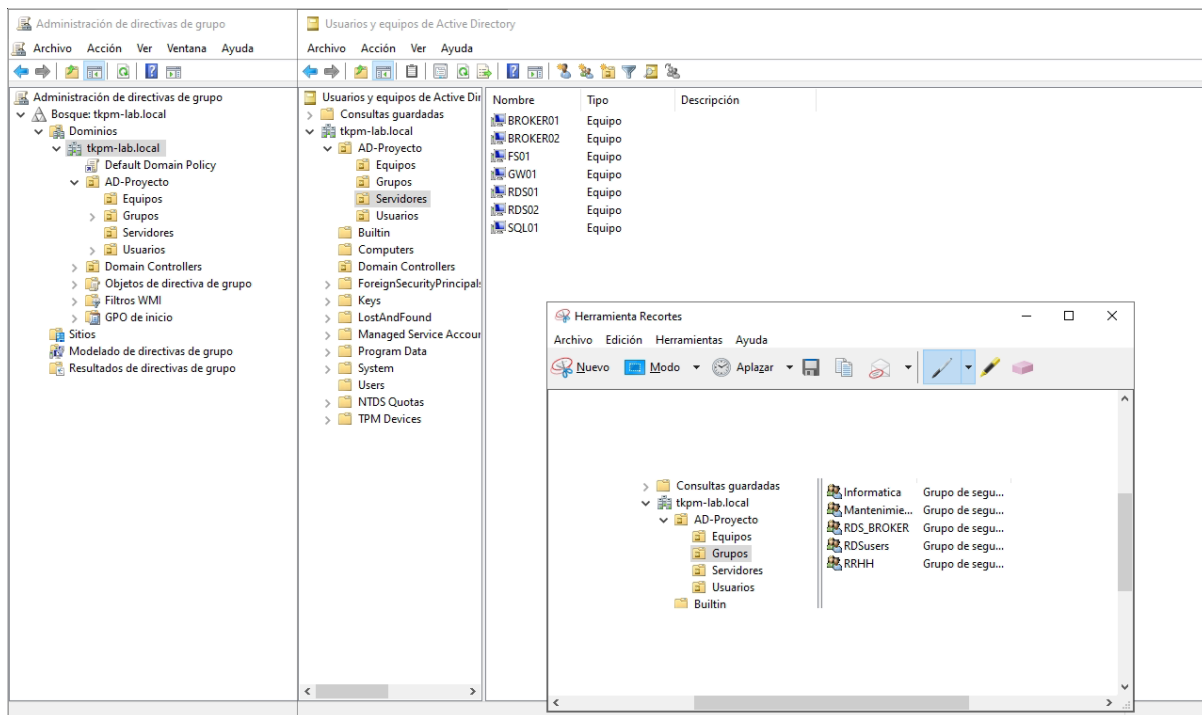
Traza a la dirección BROKER01.tkpm-lab.local [192.168.0.91]
sobre un máximo de 30 saltos:

    1    <1 ms    <1 ms    <1 ms  BROKER01.tkpm-lab.local [192.168.0.91]

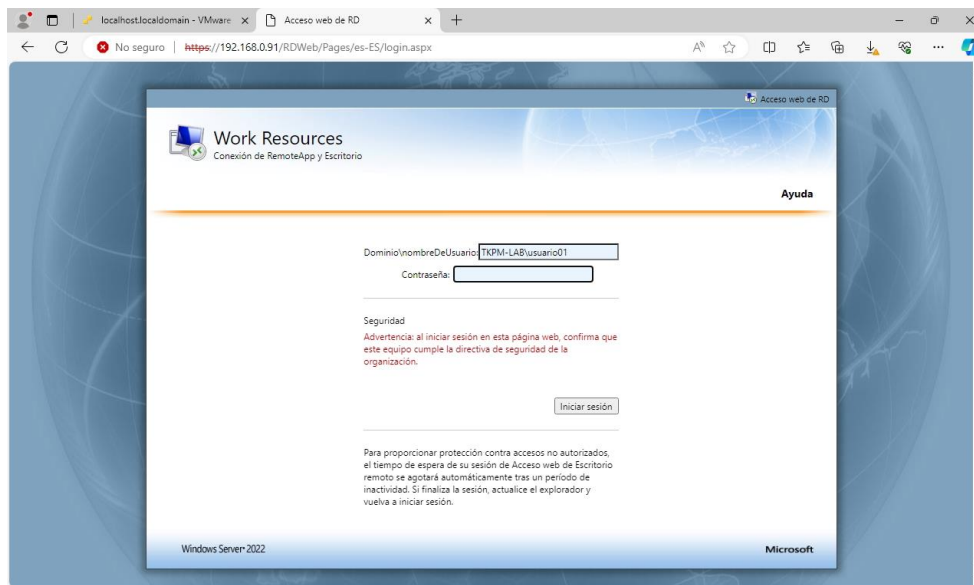
Traza completa.

C:\Users\Administrador.TKPM-LAB>
```

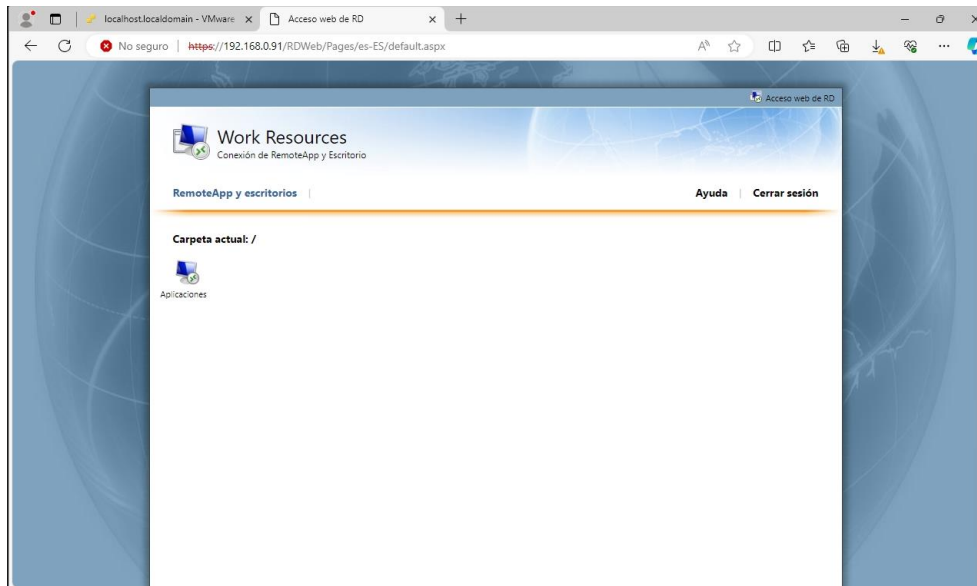
Organización de Active Directory



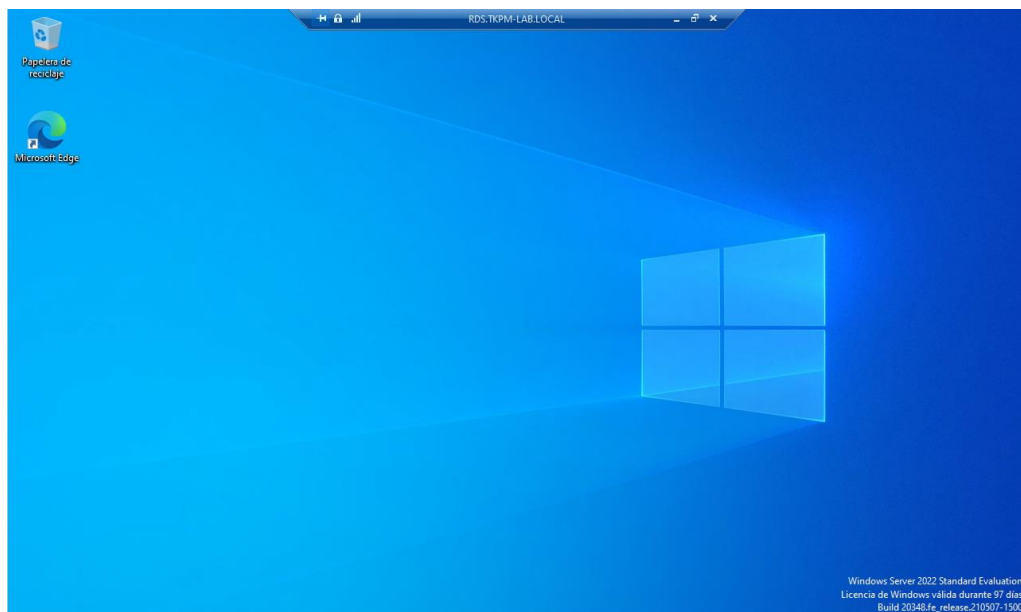
Funcionamiento del acceso web:



Cuando logueamos aparecen las aplicaciones que tenemos compartidas en nuestra colección.



Conexión establecida.



Está respondiendo el BROKER02, porque la última vez que se probó el HA, quedo como maestro, ahora apagaremos la máquina BROKER02.

Y ahora relanzamos el ping.

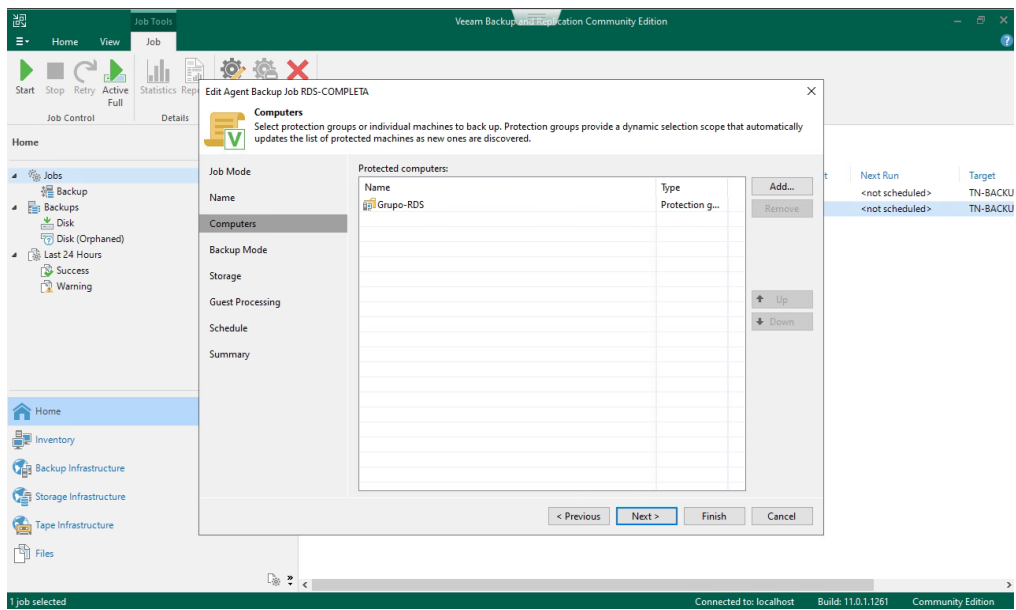
```
Estadísticas de ping para 192.168.0.92:
  Paquetes: enviados = 47, recibidos = 42, perdidos = 5
    (10% perdidos),
  Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
Control-C
^C
C:\Users\Administrador>ping RDS.TKPM-LAB.LOCAL -t

Haciendo ping a RDS.TKPM-LAB.LOCAL [192.168.0.91] con 32 bytes de datos:
Respuesta desde 192.168.0.91: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.91: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.91: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.91: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.91: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.91: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.91: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.91: bytes=32 tiempo<1m TTL=128
```

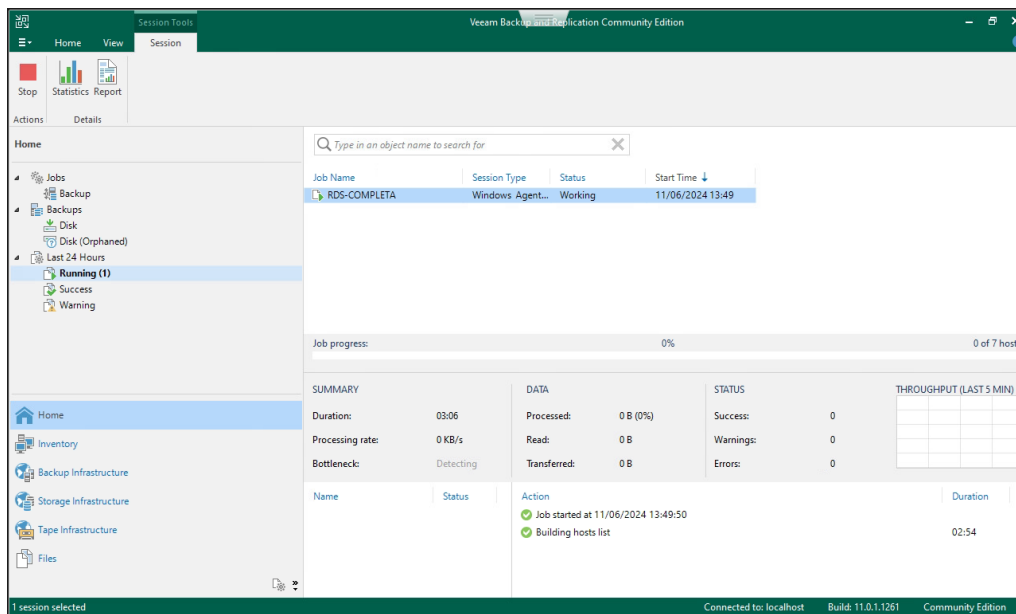
Comienza a contestar el BROKER01.

Copias de seguridad y recuperación ante desastres.

Configuración de Job de copias del grupo de servidores de la granja.



Job lanzado desde el veeam.



3. CONCLUSIONES

Conclusiones y logros alcanzados

La configuración con dos brokers ha garantizado la alta disponibilidad del servicio RDS, mejorando significativamente su fiabilidad y continuidad. Además, la integración de un servidor de copias de seguridad en TrueNAS ha proporcionado una solución robusta para la protección de datos, permitiendo una recuperación rápida en caso de desastre.

La distribución de la carga de trabajo entre los brokers ha optimizado el rendimiento del sistema y ha reducido el tiempo de inactividad, ofreciendo una experiencia de usuario más eficiente. Esta configuración equilibrada también ha permitido una gestión más eficiente de los recursos, evitando la sobrecarga de un único broker y asegurando un rendimiento constante en toda la granja RDS.

Desafíos Enfrentados

Entre los desafíos más significativos se encuentran la configuración inicial compleja de los brokers y la integración con el servidor de copias de seguridad. La implementación de un sistema de failover automático y sin interrupciones también presentó dificultades técnicas. Por último, asegurar la compatibilidad y la configuración correcta de TrueNAS requirió ajustes específicos y pruebas.

Personalmente en la idea principal de la infraestructura no encontraba demasiada dificultad, pero sin embargo durante todo el proceso de despliegue se han ido encontrando fallos que cada vez lo complican un poco más. Se han utilizado conocimientos y herramientas adquiridos durante el curso pero a su vez se han adquirido y añadido nuevos conocimientos necesarios para poder desplegar toda la infraestructura, como por ejemplo la instalación y puesta a punto de un servidor NAS o un SQL Server en windows.

4. BIBLIOGRAFÍA

- RDR-IT.(2024). Web dedicada al desarrollo de guías sobre Windows y Linux.
<https://rdr-it.io/es/implementar-una-granja-de-servidores-rds-windows-2012r2-2016-2019/prepare-el-entorno-para-la-granja-de-rds/>
- Microsoft Learn.(2024). Introducción a Servicios de Escritorio Remoto.
<https://learn.microsoft.com/es-es/windows-server/remote/remote-desktop-services/welcome-to-rds>
- Del Incl.(2024). Servidores Dell.
<https://www.dell.com/es-es/shop/servidores-dell-poweredge/sr/servers/2501-3500?appliedRefinements=37445>
- Microsoft.(2024). Precios y licencias de Windows Server.
<https://www.microsoft.com/es-es/windows-server/pricing>
- Microsoft.(2024). CAL de Escritorio remoto de Windows Server
<https://www.microsoft.com/es-es/d/cal-de-escritorio-remoto-de-windows-server-2022/dg7gmgf0d7hx/0003>
- Veeam Software.(2024). Software de Backup y Replicación.
<https://www.veeam.com/es/smb-vmware-hyper-v-essentials.html#:~:text=Veeam%20Data%20Platform%20Essentials%20.>
- Leonardo Ojeda.(2024). Blog dedicado a IT.
<https://ojedaleonardo.com/windows-server/servicios-de-escritorio-remoto-en-alta-disponibilidad/>
- Servermall.(2024). Web de venta de servidores.
<https://servermall.com>
- Sophos Limited(2024). Página oficial de Sophos Firewall.
<https://docs.sophos.com/nsg/sophos-firewall/18.5/Help/en-us/webhelp/onlinehelp/index.html>
- iXsystems, Inc. (2024). Página de TrueNAS.
<https://www.truenas.com/>
- Amazon(2024). Servidores NAS.
<https://www.amazon.es/Servidor-NAS/s?k=Servidor+NAS>
- Microsoft Learn.(2024). Servicios de Escritorio remoto: Alta disponibilidad
<https://learn.microsoft.com/es-es/windows-server/remote/remote-desktop-services/rds-plan-high-availability>
- Youtube(2024). Videos sobre VLANS.
<https://www.youtube.com/watch?v=uhlBapBzB38>