MODELO DE INFRAESTRUCTURA Y DISEÑO

PROYECTO DE ADMINISTRACION DE SISTEMAS INFORMATICOS EN RED

21 DE ABRIL DE 2025

IVAN HUMARA MIRANDA

Tabla de contenido

Resumen

Mi proyecto presenta un sistema de escritorio remoto en entornos de Linux llamado ThinLinc, que permite a los usuarios acceder a entornos de trabajo de manera segura y eficiente. La solución se implementa con la gestión centralizada de usuarios a través de LDAP, facilitando el control y la administración de permisos, y garantizando que solo los usuarios autorizados puedan utilizar el servicio.

Además, el acceso al servicio se restringe usando una VPN, lo que agrega una capa adicional de seguridad para proteger la transmisión de datos en entornos de red no controlados. Este proyecto resuelve el problema de la seguridad en el acceso remoto, al ofrecer una solución unificada y simplificada.

La implementación de ThinLinc permite la conexión remota con un rendimiento óptimo, mientras que LDAP centraliza la administración de usuarios y políticas de acceso. La restricción a través de VPN asegura que la comunicación se realice en un entorno seguro, reduciendo significativamente el riesgo de intrusiones y de ataques informáticos hacia el servicio. En conjunto, esta arquitectura favorece la continuidad operativa, optimiza la gestión de recursos y se adapta a las exigencias de las organizaciones en términos de seguridad, eficiencia y flexibilidad.

Todo esto montado en los servidores de AWS

Palabras clave

Estos son las palabras clave de mi proyecto

- Ubuntu
- Cendio
- ThinLinc
- ThinLinc Maestro
- ThinLinc Agente
- LDAP
- VPN
- WireGuard
- Alta Disponibilidad
- Balanceo de Carga
- AWS
- Máquina Virtual

Introducción

Durante mi experiencia diaria en entornos académicos y laborales donde se utilizan sistemas Linux, observé una necesidad, la posibilidad de acceder de forma remota y segura a entornos de trabajo, sin comprometer la integridad de los datos ni la disponibilidad de los servicios. En muchos casos, los usuarios necesitaban acceder a sus escritorios desde distintos sitios, ya fuera desde casa, otras oficinas o incluso durante viajes, y las soluciones disponibles eran poco seguras, difíciles de gestionar o simplemente ineficientes en términos de rendimiento.

A raíz de este problema, me surgió la idea de utilizar un sistema de escritorio remoto basado en entornos de Linux llamado ThinLinc, un servicio desarrollado por Cendio, que permite conexiones rápidas, seguras y estables. La elección de ThinLinc se justifica por su enfoque en el rendimiento, la seguridad y su facilidad de integración con herramientas como LDAP y VPN, elementos clave para la centralización de usuarios y la protección de la red.

El proyecto no está planteado como una empresa comercial, sino como una solución técnica que puede ser implementada en organizaciones que requieran acceso remoto seguro, como instituciones educativas, empresas tecnológicas o departamentos de TI. La inclusión de herramientas como WireGuard para la VPN, scripts automatizados para facilitar la gestión, y la posibilidad de desplegar el sistema en la nube con AWS utilizando máquinas virtuales, responde a la necesidad de una solución escalable, segura y fácil de administrar.

En resumen, este proyecto nace como respuesta a un problema real de acceso remoto poco seguros en entornos Linux, y propone una arquitectura unificada que garantiza alta disponibilidad, balanceo de carga y una administración eficiente, todo ello orientado a mejorar la continuidad operativa de cualquier organización.

Objetivos

Objetivo General:

Desarrollar e implementar un sistema de acceso remoto seguro y eficiente para entornos de trabajo Linux, utilizando ThinLinc para la conexión remota, LDAP para la gestión centralizada de usuarios y VPN para asegurar la transmisión de datos, garantizando la integridad, disponibilidad y confidencialidad de la información.

Objetivos Específicos:

1. Implementar ThinLinc para ofrecer una solución de escritorio remoto que permita el acceso a entornos de Linux, con alta disponibilidad y balanceo de carga.
2. Integrar LDAP para gestionar de forma centralizada los usuarios y las políticas de acceso del servidor ThinLinc, asegurando un control adecuado sobre los permisos y accesos a los recursos de la red.
3. Configurar una VPN para restringir el acceso al servicio de escritorio remoto, agregando una capa adicional de seguridad y protegiendo la transmisión de datos en redes no controladas.
4. Optimizar la seguridad del sistema mediante la implementación de prácticas recomendadas para la protección contra intrusiones y ataques informáticos, garantizando la confidencialidad e integridad de los datos transmitidos.
5. Facilitar la administración de usuarios e instalación de los servicios, permitiendo a los administradores gestionar la creación de usuarios e instalación de los servicios de manera automatizada con la utilización de scripts, minimizando el riesgo de errores humanos.

Análisis del contexto

Análisis del contexto

Después de hacer una larga búsqueda sobre servicios similares he llegado a la conclusión que la principal competencia es:

- **NoMachine:** Ofrece acceso remoto para diversos contenidos, incluyendo audio y video. La empresa que provee el servicio es NoMachine S. El coste es de 40€ por dispositivo.
- **VNC Connect:** Ofrece acceso remoto desde computadoras de escritorio o dispositivos móviles. La empresa que provee el servicio es RealVNC.
- **X2Go:** Proporciona un servicio de acceso remoto de código abierto para Linux que utiliza el protocolo NX. Este servicio no es provisto por ninguna empresa en particular. Es gratuito.
- **mRemoteNG:** Ofrece acceso remoto multiprotocolo con pestañas. Este servicio no es provisto por ninguna empresa en particular. Es Gratuito.
- **Chrome Remote Desktop:** Permite a los usuarios acceder de formar remota a través del navegador Chrome. Es gratuito.

Análisis DAFO

Fortalezas

1. Especialización en Linux: Mejor experiencia de usuario para escritorios Linux que muchas soluciones genéricas (Citrix, VMware, etc).
2. Versión gratuita hasta 10 usuarios: Ideal para pequeñas organizaciones, pruebas y entornos educativos.
3. Compatibilidad multiplataforma: Funciona en Windows, macOS, Linux y navegadores web.
4. Seguridad sólida: Basado en SSH, cifrado de extremo a extremo, autenticación fuerte.
5. Bajo consumo de recursos: Funciona bien en conexiones lentas y hardware modesto.
6. Empresa europea: Cumple con estándares de privacidad como GDPR.

Debilidades

1. Menor reconocimiento de marca frente a gigantes como Citrix, Microsoft o VMware.
2. Interfaz técnica: No es la más amigable para usuarios no técnicos o sin experiencia en Linux.
3. Falta de soporte directo a Windows como host: Solo clientes Windows, no servidores.
4. Menos funcionalidades empresariales integradas (auditoría avanzada, balanceo de carga automático, etc.).
5. Dependencia de entornos Linux: Lo que puede limitar su adopción en entornos mixtos.

Oportunidades

Creciente adopción de Linux en entornos de desarrollo y educación.

1. Demanda por soluciones seguras de trabajo remoto sigue en aumento.
2. Auge del software open source y ético: muchas empresas buscan alternativas a grandes corporaciones.
3. Espacio para integrarse con entornos cloud (AWS, Azure, etc.) para mayor escalabilidad.

4. Mercado educativo y de investigación poco atendido por soluciones comerciales grandes.

Amenazas

1. Competencia de soluciones gratuitas o más conocidas como X2Go, Guacamole o VNC.
2. Empresas muy reconocidas como Microsoft, Citrix y VMware ofrecen soluciones con muchos recursos e integraciones.
3. Cambio de tendencias tecnológicas hacia escritorios totalmente web o aplicaciones SaaS.
4. Riesgo de estancamiento si no se expande a más plataformas o añade funcionalidades colaborativas.
5. Proyectos open source similares y gratuitos que pueden cubrir necesidades básicas.

Estado del arte

Estudio de dominio de aplicación del proyecto

En los últimos años, los servicios de acceso remoto han adquirido una gran relevancia debido al crecimiento del teletrabajo, la virtualización de escritorios y la necesidad de acceder a sistemas desde múltiples ubicaciones y dispositivos. Esta forma de trabajar se ha visto reforzada tras la pandemia, impulsando a muchas instituciones y empresas a implementar soluciones seguras y eficientes para trabajar de forma remota.

Para lograr esta forma de trabajar se utilizan las siguientes tecnologías y dispositivos:

- Protocolos de acceso como RDP, VNC y SSH
- Seguridad utilizando cifrado de extremo a extremo, autentificación por claves, integración de servidores LDAP y Kerberos
- Sesiones persistentes
- Clientes multiplataforma ya puede ser desde Windows, Linux a Android, iOS hasta incluso vía navegadores web

Problemas identificados

Desde que se utiliza esta tecnología del acceso remoto ha habido una serie de problemas recurrentes que afectan a los usuarios como a los propios administradores de sistemas.

- **Latencia y rendimiento**, a veces en las sesiones de acceso remoto se vuelven lentas pudiendo dar tirones o respuestas lentas del teclado y ratón.
- **Problemas de compatibilidad** con ciertos dispositivos como los USB o los escáneres e impresoras y también problemas con los sistemas ya que no todos soportan el escritorio remoto.
- **Dificultad en las configuraciones y el mantenimiento**, esto pasa cuando el usuario no tiene experiencia con estos servicios.
- **Experiencias de usuarios deficientes** ya que no todos los servicios proporcionan una buena calidad grafica.
- **Ausencia de sesiones persistentes** no todos los servicios ofrecen las sesiones persistentes es decir si te desconectas pierdes la sesión.
- **Problemas de seguridad** hay algunas tecnologías que no cifran correctamente la conexión.

Todos estos problemas en mayor o menor medida me afectaran en la realización del proyecto, aunque hay algunos que los puedo mitigar como los problemas de seguridad, ya que al usar una VPN es una barrera de seguridad adicional para poder utilizar el servicio, o la ausencia de sesiones la puedo eliminar ya que uso un servicio que si dispone de ello (ThinLinc), por el otro lado hay algunos problemas que no podre evitar, como la latencia y el rendimiento ya que al no estar directamente en la maquina real del usuario siempre tendrá esa ralentización por culpa de la conexión .

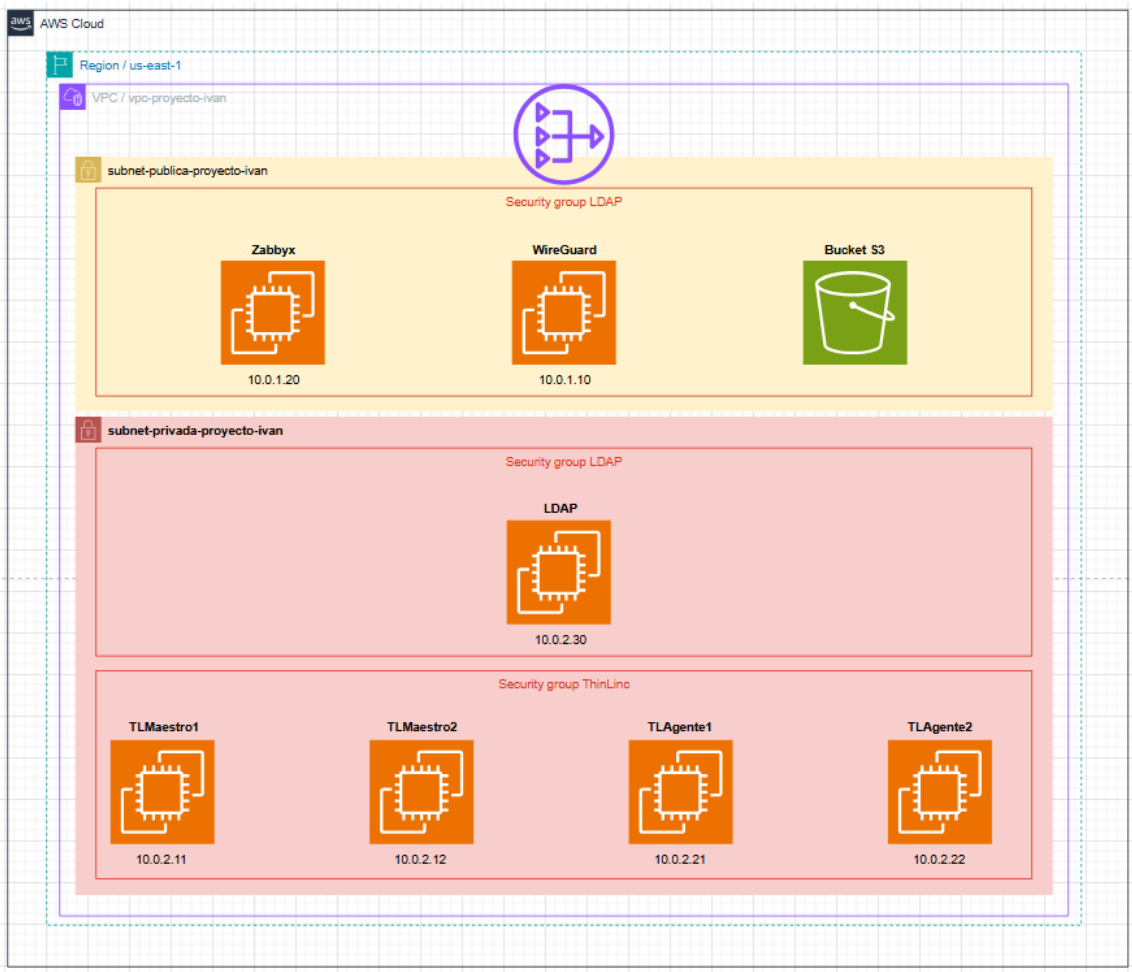
Innovación

El uso de ThinLinc como solución principal en mi proyecto es para mejorar y optimizar lo que ya existe, debido a que ThinLinc se centra en un mayor nivel de seguridad con el uso de SSH, y no crear túneles manuales con VNC, también permitir sesiones persistentes, esta optimizado específicamente para entornos Linux pero a la vez es multiplataforma ya que se puede utilizar en una variedad de SO, incluso en navegadores web, y por ultimo por que es un modelo accesible ya que hasta no llegar a mas de 10 usuarios es gratuito.

Todo esto lo hace ideal para ser usados en entornos laborales o educativos que requieran seguridad y fiabilidad sin gastar una gran cantidad de dinero.

Diseño

Diagrama de arquitectura en AWS



Listado de tecnologías

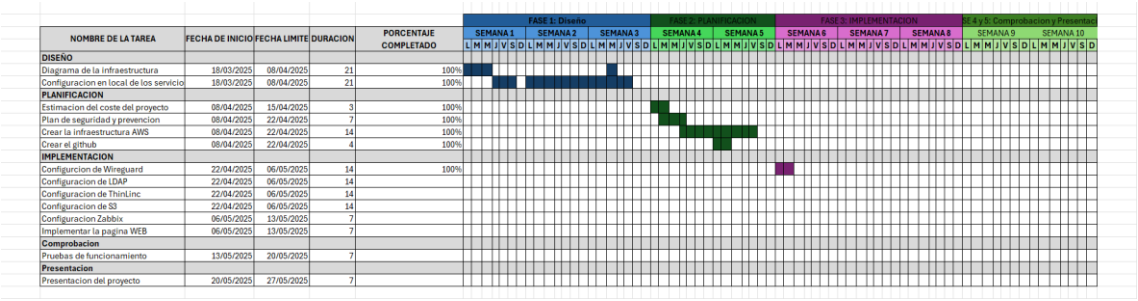
ThinLinc, LDAP, Wireguard, Zabbix, Keepalived

Infraestructura

AWS EC2, S3, Network Load Balancer, Gateway NAT

Planificación

Diagrama de GANT hasta día 21/04/2025



NOMBRE DE LA TAREA	FECHA DE INICIO	FECHA LIMITE	DURACION	PORCENTAJE COMPLETADO
DISEÑO				
Diagrama de la infraestructura	18/03/2025	08/04/2025	21	100%
Configuracion en local de los servicio	18/03/2025	08/04/2025	21	100%
PLANIFICACION				
Estimacion del coste del proyecto	08/04/2025	15/04/2025	3	100%
Plan de seguridad y prevencion	08/04/2025	22/04/2025	7	100%
Crear la infraestructura AWS	08/04/2025	22/04/2025	14	100%
Crear el github	08/04/2025	22/04/2025	4	100%
IMPLEMENTACION				
Configurcion de Wireguard	22/04/2025	06/05/2025	14	100%
Configuracion de LDAP	22/04/2025	06/05/2025	14	
Configuracion de ThinLinc	22/04/2025	06/05/2025	14	
Configuracion de S3	22/04/2025	06/05/2025	14	
Configuracion Zabbix	06/05/2025	13/05/2025	7	
Implementar la pagina WEB	06/05/2025	13/05/2025	7	
Comprobacion				
Pruebas de funcionamiento	13/05/2025	20/05/2025	7	
Presentacion				
Presentacion del proyecto	20/05/2025	27/05/2025	7	

DEFINICION DE ACTIVIDADES Y TAREAS

1. Diseño
    a. Diagrama de la infraestructura
        i. Definir la VPC, las zonas de disponibilidad, las subredes y los grupos de seguridad
    b. Configuración en local de los servicios
        i. Realizar las instalaciones y configuraciones de los servicios en proxmox
2. Planificación
    a. Estimación del coste del proyecto
        i. Hacer una estimación del coste del laboratorio de AWS
    b. Plan de seguridad y prevención
        i. Configurar los grupos de seguridad
        ii. Visualiza los riesgos y prevenirlos
3. Implementación
    a. Creación de la Infraestructura
    b. Configuración de VPN
    c. Configuración de LDAP
    d. Configuración de ThinLinc
        i. Creación de usuarios
    e. Configuración de S3
        i. Implementar la página WEB
    f. Configuración de Zabbix
4. Comprobación
    a. Pruebas de funcionamiento
5. Presentación
    a. Realizar la presentación del proyecto

IDENTIFICACION DE RIESGOS Y PREVENCION

RIESGO	Prevención
Fallos en los scripts	Probar los scripts de forma local antes de meterlos al laboratorio
Gasto total de saldo en AWS	No apurar el saldo de los laboratorios de AWS y cambiar con tiempo
Falta de tiempo	Priorizar las tareas importantes como la VPN y la infraestructura ya que sin ellas no funcionaría nada

CALCULO DE COSTE DEL PROYECTO

Este es el coste promedio que cuesta mantener el servicio en AWS

Servicio	Coste mensual estimado cada mes
EC2 – 7 instancias	53.14$
S3	1.20$
IP elásticas	3.60$
Gateway NAT	32.40$
TOTAL	**90.34$**

ORGANIGRAMA JERARQUICO

Fase 1: Diseño	Diagrama de la infraestructura
	Configuración en local de los servicios
Fase 2: Planificación	Estimación de coste del proyecto
	Plan de seguridad y prevención
Fase 3: Implementación	Creación de la infraestructura
	Configuración de Wireguard
	Configuración de LDAP
	Configuración de ThinLinc
	Creación de S3
Fase 4: Comprobación	Pruebas de funcionamiento
Fase 5: Presentación	Presentar el proyecto

Definición de recursos y logística necesaria para el proyecto

Orden lógico

Es muy importante seguir el orden ya que si se hace desordenado el servicio no funcionaría hasta tenerlo todo montado

1- Diseño: Diagrama de la infraestructura > Configuración en local de los servicios

2- Planificación: Estimación del coste del proyecto > Plan de seguridad y prevención

3- Implementación: Creación de la Infraestructura > Configuración de VPN > Configuración de LDAP > Configuración de ThinLinc > Creación de S3

4- Comprobación: Pruebas de funcionamiento

5- Presentación: Presentación

ASIGNACION DE TIEMPOS Y RECURSOS

SEMANA	ACTIVIDADES	RECURSOS UTILIZADOS
18/03/2025 8/04/2025	Fase 1 diseño	Proxmox, ThinLinc, LDAP
08/04/2025 22/04/2025	Fase 2 planificación	AWS CLI, GitHub, ThinLinc y LDAP en bash
22/04/2025 13/05/2025	Fase 3 implementación	ThinLinc, LDAP, Wireguard, Zabbix, S3
13/05/2025 1/06/2025	Fase 4 – 5 Comprobación y presentación	Wireguard cliente, ThinLinc cliente, Word