SISTEMA INTEGRAL DE SERVICIOS Y ALTA DISPONIBILIDAD

Propuesta de proyecto

VICTOR FERNANDEZ OLVERA
IES CAMP DE MORVEDRE
ASIR 2CFGS

Índice

1. Introducción 2
2. Análisis de la problemática 2
2.1. Riesgo de pérdida de datos y continuidad del negocio 2
2.2. Vulnerabilidad y conectividad 2
2.3. Vulnerabilidad en seguridad física 2
3. Objetivos específicos 3
4. Alcance y límites (Viabilidad) 4
5. Fases o etapas del proyecto 5
6. Herramientas y elementos a utilizar 6
6.1. Infraestructura de Hardware 6
6.2. Herramientas de monitorización y simulación 6
7. Fechas propuestas de inicio, desarrollo y finalización del proyecto 6

1. Introducción

Esta propuesta presenta el proyecto sistema integral de servicios y alta disponibilidad, enfocado en diseñar, implementar y administrar una infraestructura de red y servicios robusta y segura para una pequeña o mediana empresa. El objetivo es centralizar servicios clave como web, correo, base de datos, etc.., para asegurar la continuidad del negocio y garantizar la integridad de la información mediante técnicas de alta disponibilidad, seguridad perimetral y planes de copias de seguridad automatizados.

2. Análisis de la problemática

Las PYMES a menudo carecen de infraestructuras informáticas que garanticen la continuidad operativa ante fallos de hardware, ataques de seguridad o errores humanos, poniendo en riesgo datos críticos y la operación diaria. El proyecto busca abordar estas vulnerabilidades. Vamos a analizar punto por punto cada una de estas vulnerabilidades.

2.1. Riesgo de pérdida de datos y continuidad del negocio

Muchas organizaciones dependen de sistemas sin redundancia ni planes de respaldo automatizados y probados. Un fallo en el servidor principal paraliza las operaciones, resultando en pérdidas económicas.

2.2. Vulnerabilidad y conectividad

La falta de una configuración de red segmentada y servicios de red sin protección (sin firewall, protocolos inseguros) expone la infraestructura a accesos no autorizados y ataques.

2.3. Vulnerabilidad en seguridad física

El hardware crítico puede estar expuesto a fallos ambientales o físicos sin monitorización adecuada, lo que puede afectar directamente al rendimiento y a la disponibilidad de los servicios.

3. Objetivos específicos

Vamos a abordar las medidas para combatir las debilidades de las PYMES.

- Implementar un sistema operativo de servidor y configurar cuentas de usuario y políticas de seguridad.

- Diseñar e implementar una arquitectura de alta disponibilidad para servicios críticos como la web, la base de datos, el correo entre otros, mediante técnicas de virtualización y redundancia, como por ejemplo una RAID o clustering.

- Desplegar servicios de red e Internet como un servidor web y servidor de correo, asegurando su configuración y funcionamiento.

- Diseñar y configurar una base de datos e implementar tareas de administración y automatización en el sistema gestor de bases de datos.

- Establecer un plan de copias de seguridad automatizado y probado, así como un plan de restauración.

- Segmentar la red mediante la configuración de VLANs y el uso de un router para su interconexión.

- Monitorizar el rendimiento del sistema en tiempo real e implementar scrips para automatizar tareas administrativas.

- Crear documentación detallada de la instalación, configuración y recomendaciones de uso de los servicios.

4. Alcance y límites (Viabilidad)

Respecto al alcance del proyecto realizaríamos las siguientes mejoras.

El proyecto se centrará en la implementación de un entorno de red y servidores virtualizado, simulando la infraestructura de una PYME.

Para la infraestructura virtualizada se utilizará un hipervisor como VirtualBox o Hyper-V para desplegar un mínimo de tres máquinas virtuales.

Una máquina virtual como servidor principal alojando el sistema gestor de base de datos, el servidor web y el servidor de correo.

Otra máquina virtual como servidor redundante o secundario, configurado para alta disponibilidad del servicio Web y/o base de datos.

Y una última máquina virtual cliente para pruebas de conectividad, acceso a servicios y simulación de usuarios.

Continuamos con la implementación de un sistema de almacenamiento redundante de forma virtual y el desarrollo e implementación de un plan de copias de seguridad y restauración automatizado.

Diseñaríamos y configuraríamos una base de datos normalizada para alojar el contenido de un gestor de contenidos.

Implementaríamos VLANs y configuraríamos un router virtual para la interconexión de redes segmentadas.

Crearíamos scrips para la automatización de tareas administrativas del sistema operativo y del sistema gestor de base de datos.

Elaboraríamos documentación detallada de la instalación, configuración y recomendaciones de uso de todos los servicios.

Respecto a límites de viabilidad.

Para garantizar la finalización del proyecto en el tiempo asignado se establecen los siguientes límites:

Todo el proyecto se desarrollará en un entorno de virtualización.

La implementación física como el cableado estructurado, rack, dispositivos físicos de interconexión como switches o firewalls dedicados, queda fuera del alcance. Se simulará la topología y la configuración de red únicamente a nivel de software.

Se realizarán pruebas funcionales de los servicios, pero las pruebas de rendimiento y carga intensivas a nivel de producción no se realizarán en profundidad.

Se priorizará el uso de software libre como linux, apache, nginx, MySQL, postgreSQL, etc., para mantener la viabilidad económica.

5. Fases o etapas del proyecto

Fase	Título	Descripción de Tareas Clave	Duración Propuesta
Fase 1	Definición de la arquitectura y criterio preventivo	Diseño del modelo lógico de base de datos, selección del S.O. y tecnologías. Definición de la arquitectura de alta disponibilidad y el esquema de VLANs. Planificación de copias de seguridad.	1 semana
Fase 2	Montaje y despliegue	Instalación del S.O. en las máquinas virtuales. Creación de cuentas de usuario y grupos. Configuración del entorno de virtualización. Implementación de RAID virtual para el almacenamiento.	2 semanas
Fase 3	Configuración avanzada y lógica proactiva	Configuración de VLANs y enrutamiento inter-VLAN. Instalación y configuración de servidores Web y Correo. Diseño físico e implantación del sistema gestor de base de datos y la base de datos. Instalación y personalización de un sistema de gestión de contenidos. Creación de scripts de automatización para las copias de la base de datos.	3.5 semanas
Fase 4	Validación de la fiabilidad y entrega final	Implementación de solución de servidor redundante. Prueba de las copias de seguridad y restauración. Monitorización de rendimiento y documentación final. Presentación del proyecto.	2.5 semanas

6. Herramientas y elementos a utilizar

6.1. Infraestructura de Hardware

- El hardware base para la simulación contaría de un PC o portatil con capacidad de virtualización.
- Como hipervisor utilizaríamos virtualBox o Hyper-V para crear el entorno de máquinas virtuales.
- Como sistemas operativos utilizaríamos distribuciones de linux server como por ejemplo ubuntu server y un sistema operativo cliente como linux desktop.

6.2. Herramientas de monitorización y simulación

- Para los servicios un servidor Web como apache o nginx, para el servidor de correo postfix o dovecot y para el sistema gestor de base de datos MySQL o postgreSQL.
- Como herramientas de simulación de red packettTracer para el diseño inicial y para la configuración de red en el hipervisor (VLANs virtuales).
- Como herramientas de monitorización en tiempo real nagios o zabbix simulado.
- Para lenguajes de scripting usaríamos bash o powershell.

7. Fechas propuestas de inicio, desarrollo y finalización del proyecto

- Fecha de Inicio Propuesta:

  Del 26 de enero al 1 de marzo.

- Fecha de Desarrollo (Inicio Fase 2 a Final Fase 3):

  Del 2 de marzo al 8 de abril.

- Fecha de Finalización (Entrega Final):

  Del 9 al 26 de abril.