Guía de estudio - Gestión de certificados y cifrado en Windows Server

¡Hola! Te damos la bienvenida a esta nueva guía de estudio.

¿En qué consiste esta guía?

La seguridad en la comunicación de servidores y clientes es fundamental en cualquier infraestructura de TI. La implementación de certificados SSL/TLS y la configuración de cifrado para la protección de datos en tránsito son medidas esenciales para garantizar la integridad y confidencialidad de la información.

En esta guía, exploraremos:

- Automatización de la implementación de certificados SSL/TLS.
- Configuración de cifrado para proteger datos en tránsito mediante HTTPS e IPsec.
- Mejores prácticas y configuraciones avanzadas.

¡Vamos con todo!

Tabla de contenidos

¡Comencemos!

Implementación automatizada de certificados SSL/TLS

Los certificados SSL/TLS permiten cifrar las comunicaciones entre servidores y clientes, protegiéndolas contra ataques de intermediarios y espionaje de datos.

Instalación y configuración de un certificado SSL

Para implementar un certificado SSL en Windows Server, primero se debe obtener un certificado de una autoridad certificadora (CA) o generar un certificado autofirmado.

- **Generar un certificado autofirmado:**

```
New-SelfSignedCertificate -DnsName "servidor.ejemplo.com"
-CertStoreLocation "Cert:\LocalMachine\My"
```

Este comando genera un certificado autofirmado para el dominio `servidor.ejemplo.com`.

- **Exportar el certificado para distribuirlo a otros equipos:**

```
Export-PfxCertificate -Cert "Cert:\LocalMachine\My\<Thumbprint>"
-FilePath "C:\certificado.pfx" -Password (ConvertTo-SecureString -String
"ContraseñaSegura123" -Force -AsPlainText)
```

- **Importar el certificado en otro servidor:**

```
Import-PfxCertificate -FilePath "C:\certificado.pfx" -CertStoreLocation
"Cert:\LocalMachine\My" -Password (ConvertTo-SecureString -String
"ContraseñaSegura123" -Force -AsPlainText)
```

Asignación del certificado a un sitio web en IIS

Una vez instalado el certificado, se debe asignar al sitio web correspondiente:

```
New-WebBinding -Name "SitioWeb" -IPAddress * -Port 443 -Protocol https
Set-ItemProperty "IIS:\Sites\SitioWeb" -Name sslFlags -Value 1
```

Para verificar que el certificado está correctamente asignado:

```
Get-Item "IIS:\SslBindings"
```

Actividad guiada: Implementación de certificados SSL/TLS

1. Iniciar la máquina virtual con Windows Server.
2. Generar un certificado autofirmado.
3. Exportar el certificado y transferirlo a otro servidor.
4. Configurar un sitio en IIS con HTTPS utilizando el certificado.
5. Comprobar su funcionamiento desde un cliente

Configuración de cifrado para proteger datos en tránsito

El cifrado de datos en tránsito protege la información transmitida entre dispositivos, evitando la intercepción de datos confidenciales.

Configuración de HTTPS con TLS seguro

- **Verificar las versiones de TLS habilitadas:**

```
Get-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Proto
cols\TLS 1.2\Client" -Name Enabled
```

- **Habilitar TLS 1.2 si está deshabilitado:**

```
New-Item
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Proto
cols\TLS 1.2\Server" -Force
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Proto
cols\TLS 1.2\Server" -Name Enabled -Value 1
```

Implementación de IPsec para cifrado de comunicaciones internas

IPsec permite cifrar el tráfico de red dentro de una organización para garantizar la seguridad en la comunicación entre servidores.

- **Crear una regla de IPsec para cifrar el tráfico entre dos servidores:**

```
New-NetIPsecRule -DisplayName "Regla IPsec" -InboundSecurity Require
-OutboundSecurity Require -LocalPort Any -RemotePort Any -LocalAddress
192.168.1.100 -RemoteAddress 192.168.1.200
```

- **Verificar las reglas de IPsec activas:**

```
Get-NetIPsecRule
```

- **Eliminar una regla de IPsec si ya no es necesaria:**

```
Remove-NetIPsecRule -DisplayName "Regla IPsec"
```

Actividad guiada: Configuración segura de TLS e IPsec

1. Verificar la versión de TLS habilitada en el servidor.
2. Habilitar y aplicar TLS 1.2 si no está activo.
3. Crear una regla de IPsec para cifrar la comunicación entre dos servidores.

Mejores prácticas para la seguridad con certificados y cifrado

Medida de seguridad	Descripción
Uso de certificados de una CA confiable	Evita el uso de certificados autofirmados en entornos de producción.
Implementación de TLS 1.2 y 1.3	Deshabilitar versiones obsoletas como SSL 3.0 y TLS 1.0.
Cifrado obligatorio en IPsec	Aplicar reglas de IPsec para cifrar la comunicación interna de la red.
Monitorización de eventos de seguridad	Registrar intentos de acceso no autorizado y eventos de certificado.
Automatización de renovaciones de certificados	Evitar fallos de seguridad por vencimiento de certificados.

Tabla 01. Mejores prácticas.
Fuente: ADL.

¡Manos a la obra! - Auditoría y monitoreo de seguridad

1. Verificar los certificados instalados en el sistema.
2. Revisar eventos de seguridad relacionados con certificados en el visor de eventos.
3. Configurar notificaciones para la expiración de certificados.

Reflexiona:

- ¿Por qué es importante usar certificados de una CA confiable en entornos de producción?
- ¿Qué riesgos existen al permitir versiones obsoletas de TLS en un servidor?
- ¿Cómo mejora IPsec la seguridad en la comunicación entre servidores?
- ¿Qué ventajas ofrece la automatización de la gestión de certificados?
- ¿Cómo se pueden monitorear los eventos de seguridad relacionados con certificados en Windows Server?

La correcta gestión de certificados SSL/TLS y la implementación de cifrado son esenciales para proteger la información transmitida en la red. La configuración adecuada de TLS e IPsec mejora la seguridad y evita vulnerabilidades.