Guía de estudio - Configuración y seguridad de servicios críticos en Server Core

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

¿En qué consiste esta guía?

Windows Server Core es una opción de instalación optimizada para seguridad y rendimiento, especialmente útil para la ejecución de servicios críticos como DNS y DHCP. Su administración sin interfaz gráfica reduce la superficie de ataque y mejora la estabilidad del sistema.

En esta guía, abordaremos:

- Configuración segura de DNS en Server Core.
- Implementación y seguridad del servicio DHCP.
- Buenas prácticas y medidas de protección para servicios críticos.

¡Vamos con todo!

Tabla de contenidos

Guía de estudio - Configuración y seguridad de servicios críticos en Server Core 1
¿En qué consiste esta guía? 1
Tabla de contenidos 2
Configuración segura de DNS en Server Core 3
Instalación del servidor DNS 3
Configuración básica del servidor DNS 3
Seguridad en DNS 3
Actividad guiada: Configuración segura de DNS 4
Configuración segura de DHCP en Server Core 4
Instalación del servidor DHCP 4
Configuración del servidor DHCP 4
Seguridad en DHCP 5
Buenas prácticas de seguridad para servicios críticos 5
¡Manos a la obra! - Configuración segura de DHCP 6

¡Comencemos!

Configuración segura de DNS en Server Core

El servicio DNS (Domain Name System) es fundamental para la resolución de nombres dentro de una red. Una configuración segura es clave para evitar ataques como la suplantación de DNS y las consultas malintencionadas.

Instalación del servidor DNS

Para instalar el rol de DNS en Server Core, usar:

```
Install-WindowsFeature -Name DNS -IncludeManagementTools
```

Verificar la instalación:

```
Get-WindowsFeature -Name DNS
```

Configuración básica del servidor DNS

- **Crear una nueva zona DNS primaria:**

```
Add-DnsServerPrimaryZone -Name "empresa.local" -ZoneFile
"empresa.local.dns"
```

- **Agregar un registro A:**

```
Add-DnsServerResourceRecordA -ZoneName "empresa.local" -Name "www"
-IPv4Address "192.168.1.100"
```

- **Configurar reenviadores para mejorar la resolución de nombres:**

```
Set-DnsServerForwarder -IPAddress "8.8.8.8","8.8.4.4"
```

Seguridad en DNS

- **Habilitar solo consultas de red internas:**

```
Set-DnsServerSetting -DisableRecursion $true
```

- **Restringir transferencia de zona solo a servidores autorizados:**

```
Set-DnsServerZoneTransferPolicy -ZoneName "empresa.local" -AllowTransfer
OnlyToServers -NameServers "192.168.1.2"
```

- **Habilitar el registro de eventos DNS para auditoría:**

```
Set-DnsServerDiagnostics -All $true
```

Actividad guiada: Configuración segura de DNS

1. Iniciar la máquina virtual con Windows Server Core
2. Instalar el rol de servidor DNS en Server Core.
3. Crear una zona primaria y agregar registros de host.
4. Configurar reenviadores DNS y seguridad en transferencia de zona.

Configuración segura de DHCP en Server Core

El servicio DHCP (Dynamic Host Configuration Protocol) es esencial para la asignación automática de direcciones IP en una red. Su configuración adecuada evita la asignación indebida de direcciones y protege la infraestructura de red.

Instalación del servidor DHCP

Para instalar el rol DHCP en Server Core:

```
Install-WindowsFeature -Name DHCP -IncludeManagementTools
```

Verificar la instalación:

```
Get-WindowsFeature -Name DHCP
```

Configuración del servidor DHCP

- **Autorizar el servidor DHCP en Active Directory:**

```
Add-DhcpServerInDC
```

- **Crear un nuevo ámbito DHCP:**

```
Add-DhcpServerV4Scope -Name "Red Empresarial" -StartRange 192.168.1.100
-EndRange 192.168.1.200 -SubnetMask 255.255.255.0 -State Active
```

- **Configurar la puerta de enlace predeterminada:**

```
Set-DhcpServerV4OptionValue -ScopeId 192.168.1.0 -OptionId 3 -Value
"192.168.1.1"
```

- **Asignar servidores DNS a los clientes DHCP:**

```
Set-DhcpServerV4OptionValue -ScopeId 192.168.1.0 -OptionId 6 -Value
"192.168.1.2"
```

Seguridad en DHCP

- **Habilitar registro de auditoría en DHCP:**

```
Set-DhcpServerAuditLog -Enable $true -Path
"C:\Windows\System32\dhcp\audit.log"
```

- **Restringir la concesión de direcciones a clientes autorizados:**

```
Set-DhcpServerSetting -ConflictDetectionAttempts 2
```

- **Configurar el servidor DHCP para evitar ataques Rogue DHCP:**

```
Set-DhcpServerSecurityGroup -Name "DHCP Administrators"
```

Buenas prácticas de seguridad para servicios críticos

Medida de seguridad	Descripción
Uso de cuentas con privilegios mínimos	Asignar permisos solo a los usuarios y grupos necesarios.
Implementación de registros de auditoría	Habilitar el registro de eventos en DNS y DHCP para monitoreo.
Configuración de listas de control de acceso (ACL)	Restringir acceso a configuraciones clave de los servicios.
Respaldo regular de configuraciones	Guardar copias de seguridad de zonas DNS y configuración DHCP.
Actualización de software y parches de seguridad	Mantener el servidor actualizado con los últimos parches de seguridad.

Tabla 01. Buenas prácticas.
Fuente: ADL.

¡Manos a la obra! - Configuración segura de DHCP

1. Iniciar la máquina virtual con Windows Server Core con AD funcionando
2. Instalar el servicio DHCP y autorizar el servidor en Active Directory.
3. Crear un ámbito DHCP y asignar configuraciones de red.
4. Configurar auditoría y restricciones de concesión de direcciones IP.

Reflexiona:

- ¿Cuáles son los principales riesgos de seguridad en servidores DNS y DHCP?
- ¿Por qué es importante restringir la transferencia de zonas en DNS?
- ¿Cómo se puede evitar la asignación de direcciones IP por servidores DHCP no autorizados?
- ¿Qué impacto tiene la auditoría en la detección de problemas en servicios críticos?
- ¿Cuáles son las mejores prácticas para proteger la infraestructura de red en Server Core?

La configuración segura de DNS y DHCP en Server Core es fundamental para garantizar la estabilidad y seguridad de la red empresarial. Mediante la aplicación de buenas prácticas de seguridad, se pueden mitigar riesgos de ataques y mejorar la gestión de estos servicios críticos.