Guía de estudio - Políticas de autenticación y acceso, parte II

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

¿En qué consiste esta guía?

El fortalecimiento de la seguridad en sistemas Unix/Linux requiere no solo la autenticación mediante claves, sino también una gestión fina de quién puede acceder al sistema. En esta segunda parte, profundizaremos en el uso avanzado de las directivas AllowUsers, AllowGroups, DenyUsers y DenyGroups en el archivo de configuración de OpenSSH (sshd_config).

Estas directivas permiten definir políticas de acceso granulares basadas en usuarios y grupos, facilitando la administración en entornos con múltiples usuarios y minimizando riesgos de acceso no autorizado.

¡Vamos con todo!

Tabla de contenidos

¡Comencemos!

Descripción detallada de las directivas

AllowUsers

- **Función:**
  Permite especificar explícitamente qué usuarios pueden conectarse mediante SSH.
- **Sintaxis y características:**
  - Se pueden incluir nombres de usuario individuales.
  - Es posible usar patrones para limitar accesos basados en la dirección IP o el nombre de host.

Ejemplo

```
AllowUsers juan maria admin@192.168.1.*
```

- En este ejemplo:
  - Los usuarios *juan* y *maria* pueden conectarse desde cualquier dirección.
  - El usuario *admin* solo podrá conectarse desde IPs que empiecen por 192.168.1.

DenyUsers

- **Función:**
  Especifica usuarios que no podrán acceder, incluso si están incluidos en AllowUsers o en la lista de usuarios existentes en el sistema.

Ejemplo de uso:

```
DenyUsers pepe temporario
```

- Aquí se deniega el acceso a los usuarios *pepe* y *temporario*.

AllowGroups

- **Función:**
  Permite que solo los usuarios pertenecientes a uno o varios grupos autorizados puedan autenticarse vía SSH.

Sintaxis y ejemplo:

```
AllowGroups sshusers admins
```

- En este caso, únicamente los usuarios que formen parte de los grupos *sshusers* o *admins* podrán iniciar sesión.

DenyGroups

- **Función:**
  Bloquea el acceso a todos los usuarios que pertenezcan a determinados grupos, sin importar si individualmente están permitidos en AllowUsers.

Ejemplo de uso:

```
DenyGroups invitados temporales
```

- Aquí, cualquier usuario que pertenezca a los grupos *invitados* o *temporales* se verá impedido de conectarse.

Orden de evaluación y recomendaciones

Orden de procesamiento

1. DenyUsers y DenyGroups:
   Se evalúan primero, lo que significa que si un usuario está listado en alguna de estas directivas, se bloqueará el acceso, sin importar si está incluido en AllowUsers o AllowGroups.

2. AllowUsers y AllowGroups:
   Se evalúan después; por ello, es recomendable definir primero las restricciones generales (deny) y luego especificar los accesos permitidos (allow).

Recomendaciones prácticas

- **Combinación cautelosa:**
  Utiliza las directivas de Deny para excluir accesos conocidos como riesgosos, y Allow para autorizar a usuarios o grupos específicos.

- **Evitar conflictos:**
  Asegúrate de que las directivas no se contradigan. Por ejemplo, no incluyas a un usuario en AllowUsers si luego lo excluyes con DenyUsers.

- **Pruebas en entorno controlado:**
  Antes de implementar cambios en producción, prueba la configuración en un entorno controlado para evitar bloqueos accidentales.

Tabla resumen de directivas

Directiva	Propósito	Ejemplo
AllowUsers	Permite el acceso únicamente a usuarios especificados.	`AllowUsers juan maria admin@192.168.1.*`
DenyUsers	Niega el acceso a usuarios específicos.	`DenyUsers pepe temporario`
AllowGroups	Permite el acceso solo a usuarios pertenecientes a ciertos grupos.	`AllowGroups sshusers admins`
DenyGroups	Niega el acceso a todos los usuarios de ciertos grupos.	`DenyGroups invitados temporales`

Actividad guiada: Configuración básica con AllowUsers y DenyUsers

1. **Iniciar la máquina virtual con Rocky Linux.**
2. **Abrir el archivo de configuración:**

```
sudo nano /etc/ssh/sshd_config
```

3. **Agregar las siguientes líneas (o modificarlas si ya existen):**

```
AllowUsers juan maria admin@192.168.1.*
DenyUsers temporario
```

4. **Guardar los cambios y reiniciar SSH:**

```
sudo systemctl restart ssh
```

¡Manos a la obra! - Configuración avanzada con AllowGroups y DenyGroups

Asegúrate de que los grupos existen y que los usuarios pertenecen al grupo correcto:

```
groups juan
```

```
sudo usermod -aG sshusers juan  # Agrega a juan al grupo sshusers si no está
```

Editar el archivo `sshd_config`:

```
sudo nano /etc/ssh/sshd_config
```

Incluir las directivas:

```
AllowGroups sshusers admins
DenyGroups invitados
```

Guardar y reiniciar el servicio:

```
sudo systemctl restart ssh
```

Reflexiona:

- ¿Qué sucedería si un usuario se encuentra listado tanto en AllowUsers como en DenyUsers? ¿Cómo se resuelve este conflicto?
- ¿Cuáles son las ventajas de administrar el acceso a través de grupos en lugar de usuarios individuales en entornos con muchos usuarios?
- ¿De qué manera puede mejorar la seguridad del sistema la implementación conjunta de Allow y Deny en la configuración de SSH?
- ¿Qué procedimientos recomendarías para validar que la política de acceso implementada no bloquee inadvertidamente a usuarios autorizados?

El uso de las directivas AllowUsers, AllowGroups, DenyUsers y DenyGroups en el archivo sshd_config permite implementar políticas de acceso sofisticadas y adaptadas a las necesidades de seguridad de cada entorno. Al comprender la forma en que se evalúan y se combinan estas directivas, los administradores pueden limitar el acceso a usuarios y grupos específicos, reduciendo la exposición a intentos de acceso no autorizados. Se recomienda realizar pruebas exhaustivas tras cualquier cambio para asegurar la correcta aplicación de las políticas.