

Configuraciones

Parte 1: Local AAA en R1

Objetivo: Proteger acceso por consola y VTY usando base de datos local.

1. Crear usuario local:


```
username Admin1 secret admin1pa55
```

2. Habilitar AAA y asociar autenticación en consola:

```
aaa new-model  
aaa authentication login default local  
line console 0  
login authentication default
```

3. Configurar SSH para acceso remoto:

```
ip domain-name ccnasecurity.com  
crypto key generate rsa modulus 1024  
aaa authentication login SSH-LOGIN local  
line vty 0 4  
transport input ssh  
login authentication SSH-LOGIN
```

 **Verificación:** Login exitoso desde consola y desde PC-A vía SSH.

Parte 2: AAA con TACACS+ en R2

Objetivo: Integrar R2 con servidor TACACS+ y definir autenticación con fallback local.

1. Usuario local de respaldo:

```
username Admin2 secret admin2pa55
```

2. Configuración TACACS+:

```
tacacs-server host 192.168.2.2  
tacacs-server key tacacspa55  
aaa new-model  
aaa authentication login default group tacacs+ local  
line console 0  
login authentication default
```

 **Verificación:** Acceso de PC-B autenticado por TACACS+.

Parte 3: AAA con RADIUS en R3

Objetivo: Integrar R3 con servidor RADIUS y definir autenticación con fallback local.

1. Usuario local de respaldo:

```
username Admin3 secret admin3pa55
```

2. Configuración RADIUS:

```
radius-server host 192.168.3.2
radius-server key radiuspa55
aaa new-model
aaa authentication login default group radius local
line console 0
login authentication default
```

✅ **Verificación:** Acceso de PC-C autenticado por RADIUS.

4. Resultados

- Autenticación local implementada correctamente en R1.
- Integración exitosa con **TACACS+** en R2.
- Integración exitosa con **RADIUS** en R3.
- Todos los logins validados correctamente.
- **Resultado final: 100% completado.**