Habilitación de Secure Shell (SSH) en un punto de acceso (AP)

Contenido

Introducción

Prerequisites

- Requirements
- Componentes Utilizados
- Convenciones

Acceda a la interfaz de línea de comandos (CLI) en el AP Aironet

Configurar

- Configuración de CLI
  - Step-by-Step Instructions
- Configuración de la interfaz gráfica para el usuario
  - Step-by-Step Instructions

Verificación

Troubleshoot

- Desactivar SSH

Información Relacionada

Introducción

Este documento describe cómo configurar un punto de acceso (AP) para habilitar el acceso basado en Secure Shell (SSH).

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

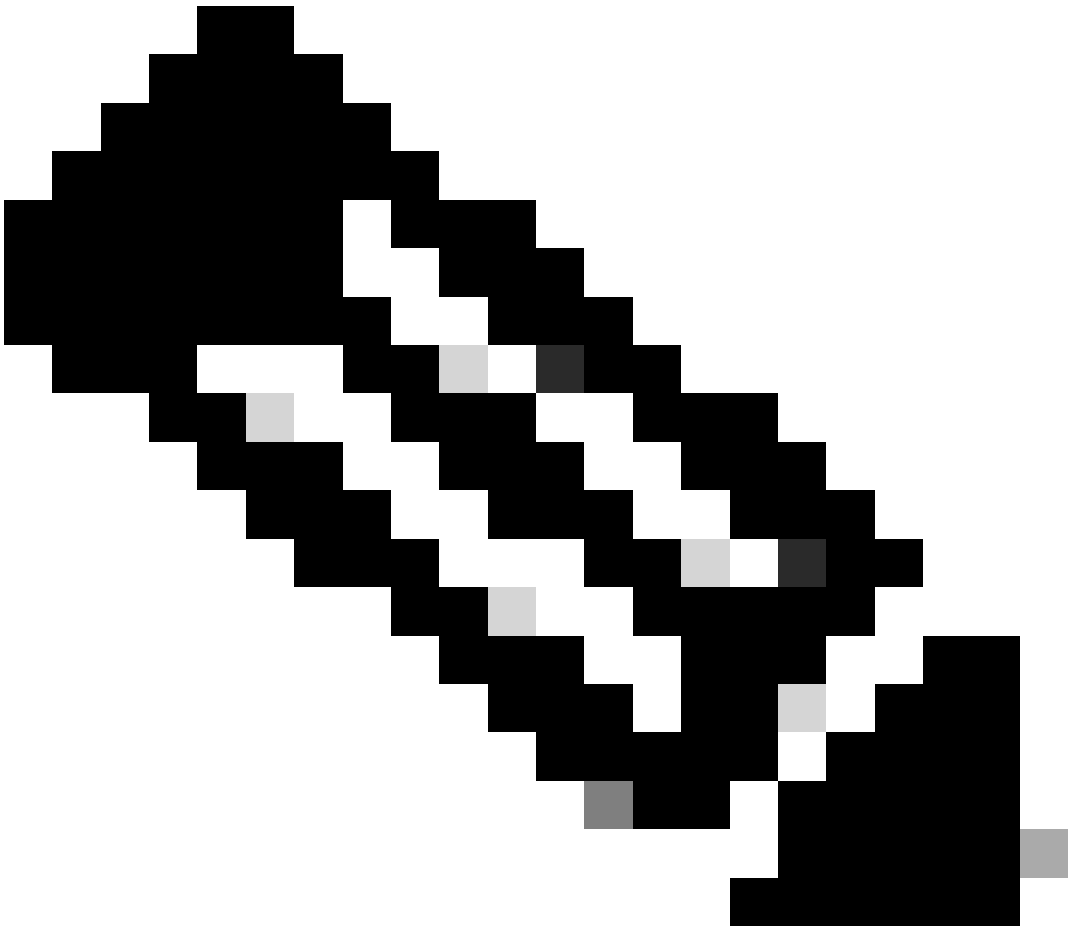
- Conocimiento de cómo configurar los AP de Cisco Aironet
- Conocimientos básicos de SSH y conceptos de seguridad relacionados

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- AP Aironet serie 1200 que ejecuta la versión 12.3(8)JEB del software Cisco IOS®

- PC o computadora portátil con utilidad de cliente SSH



Nota: Este documento utiliza la utilidad de cliente SSH para verificar la configuración. Puede utilizar cualquier utilidad de cliente de terceros para iniciar sesión en el AP con SSH.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Acceda a la interfaz de línea de comandos (CLI) en el AP Aironet

Puede utilizar cualquiera de estos métodos para acceder a la interfaz de línea de comandos (CLI) en el AP de Aironet:

- El puerto de la consola
- TELNET
- SSH

Si el AP tiene un puerto de consola y usted tiene acceso físico al AP, puede utilizar el puerto de consola para iniciar sesión en el AP y cambiar la configuración si es necesario. Para obtener información sobre cómo utilizar el puerto de la consola para iniciar sesión en el AP, refiérase a la sección Conexión a los Puntos de Acceso de la Serie 1200 Localmente del documento Configuración del Punto de Acceso por Primera Vez.

Si solo puede acceder al AP a través de Ethernet, utilice el protocolo Telnet o el protocolo SSH para iniciar sesión en el AP.

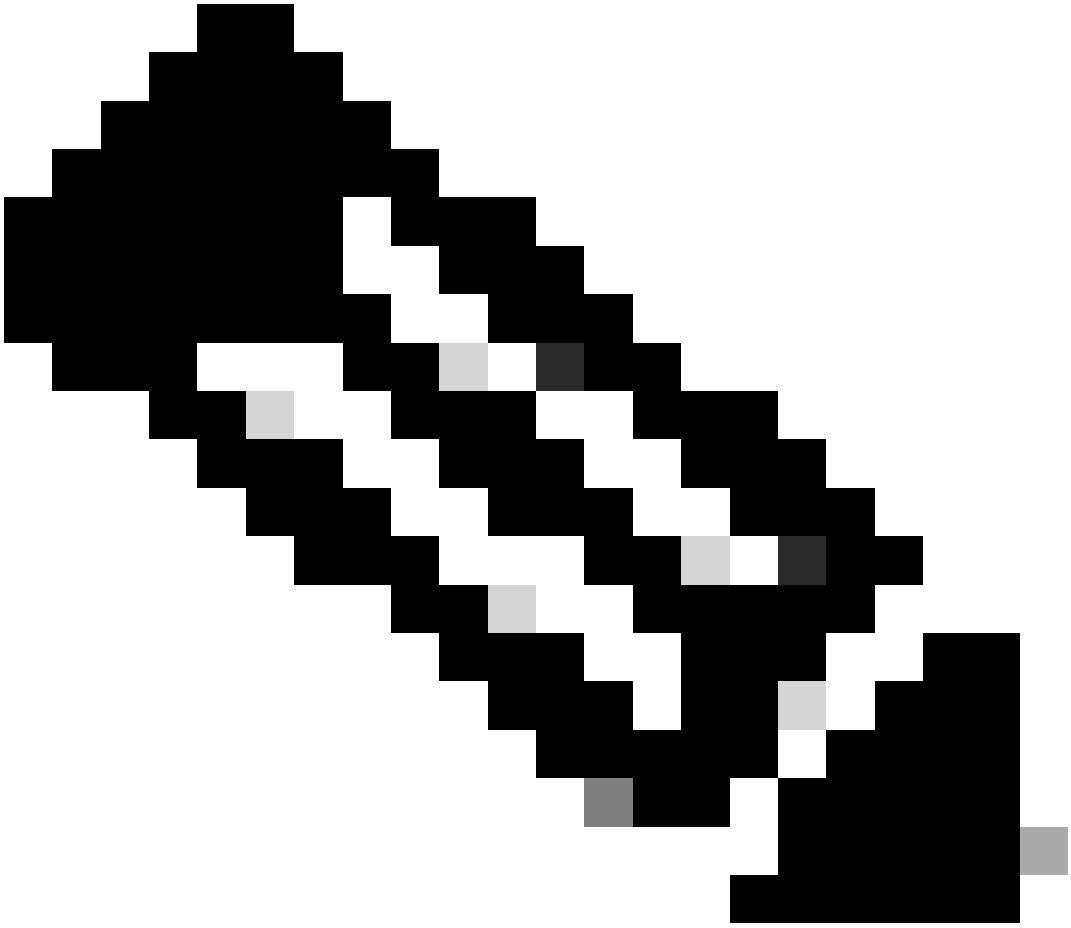
El protocolo Telnet utiliza el puerto 23 para la comunicación. Telnet transmite y recibe datos en texto no cifrado. Debido a que la comunicación de datos ocurre en texto claro, un hacker puede fácilmente poner en riesgo las contraseñas y acceder al AP. RFC 854 define Telnet y extiende Telnet con opciones de muchos otros RFC.

SSH es una aplicación y un protocolo que proporciona un reemplazo seguro de las herramientas R de Berkley. SSH es un protocolo que proporciona una conexión remota segura a un dispositivo de capa 2 o capa 3. Hay dos versiones de SSH: SSH versión 1 y SSH versión 2. Esta versión de software admite ambas versiones de SSH. Si no especifica el número de versión, el AP toma de manera predeterminada la versión 2.

SSH proporciona más seguridad para las conexiones remotas que Telnet porque proporciona un cifrado fuerte cuando se autentica un dispositivo. Este cifrado es una ventaja sobre una sesión de Telnet, en la que la comunicación se realiza en texto no cifrado. Para obtener más información sobre SSH, consulte las Preguntas frecuentes sobre Secure Shell (SSH). La función SSH tiene un servidor SSH y un cliente SSH integrado.

El cliente admite estos métodos de autenticación de usuario:

- RADIUS
- Autenticación y autorización locales.



Nota: La función SSH en esta versión de software no admite la seguridad IP (IPSec).

Puede configurar los AP para SSH con la CLI o la GUI. Este documento explica ambos métodos de configuración.

Configurar

Configuración de CLI

Esta sección proporciona información sobre cómo configurar las funciones con el uso de CLI.

Step-by-Step Instructions

Para activar el acceso basado en SSH en el AP, primero debe configurar el AP como servidor SSH. Siga estos pasos para configurar un servidor SSH en el AP desde CLI:

1. Configure un nombre de host y un nombre de dominio para el AP.

<#root>

AP#

configure terminal

!--- Enter global configuration mode on the AP.

AP<config>#

hostname Test

!--- This example uses "Test" as the AP host name.

Test<config>#

ip domain name domain

!--- This command configures the AP with the domain name "domain name".

2. Genere una clave Rivest, Shamir y Adelman (RSA) para su AP.

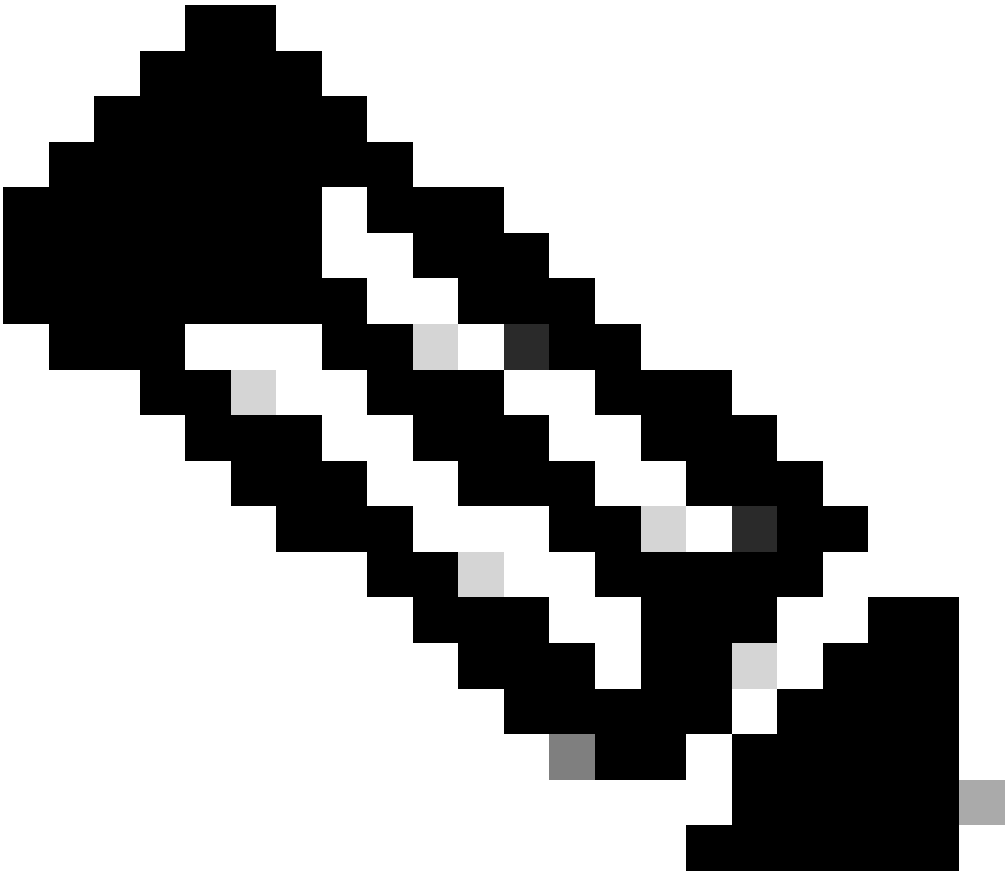
   La generación de una clave RSA activa SSH en el AP. Emita este comando en el modo de configuración global:

<#root>

Test<config>#

crypto key generate rsa rsa_key_size

!--- This generates an RSA key and enables the SSH server.



Nota: El tamaño mínimo recomendado de la clave RSA para el par de llaves es 1024.

3. Configurar la autenticación de usuario en el AP.

   En el AP, puede configurar la autenticación de usuario para utilizar la lista local o un servidor externo de autenticación, autorización y auditoría (AAA). Este ejemplo utiliza una lista generada localmente para autenticar a los usuarios:

   <#root>

   ```
   Test<config>#

   aaa new-model

   !--- Enable AAA authentication.

   Test<config>#

   aaa authentication login default local none
   ```

```
!--- Use the local database in order to authenticate users.

Test<config>#

username Test password Test123

!--- Configure a user with the name "Test".

Test<config>#

username ABC password xyz123

!--- Configure a second user with the name "Domain".
```

Esta configuración configura el AP para realizar la autenticación basada en el usuario con el uso de una base de datos local configurada en el AP. El ejemplo configura dos usuarios en la base de datos local, "Test" y "ABC".

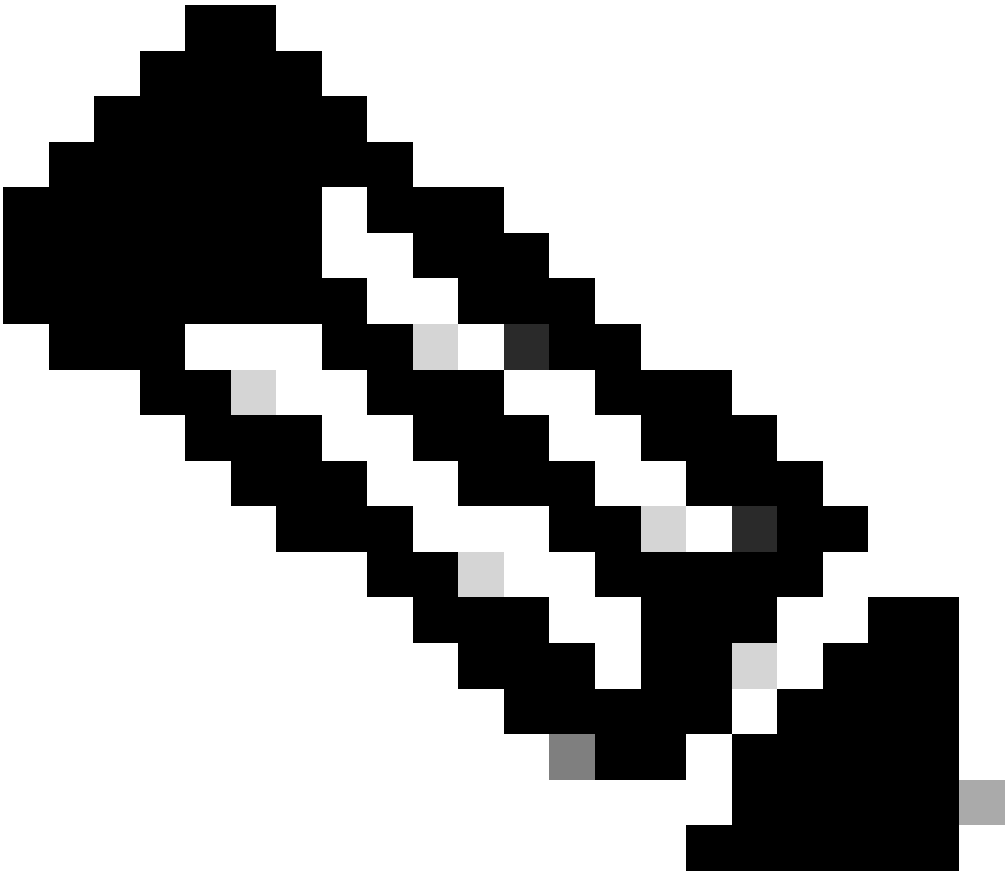
4. Configure los parámetros SSH.

<#root>

```
Test<config>#

ip ssh {[timeout seconds] | [authentication-retries integer]}

!--- Configure the SSH control variables on the AP.
```



Nota: Puede especificar el tiempo de espera en segundos, pero no superar los 120 segundos. El valor predeterminado es 120. Ésta es la especificación que se aplica a la fase de negociación SSH. También puede especificar la cantidad de reintentos de autenticación, pero no superar los cinco reintentos de autenticación. El valor predeterminado es tres.

Configuración de la interfaz gráfica para el usuario

También puede utilizar la GUI para activar el acceso basado en SSH en el AP.

Step-by-Step Instructions

Complete estos pasos:

1. Inicie sesión en el AP a través del navegador.

   Aparece una ventana de estado de resumen.

2. Haga clic en Servicesen el menú de la izquierda.

Aparece la ventana de resumen de servicios.

3. Haga clic en Telnet/SSH para activar y configurar los parámetros de Telnet/SSH.

   Se muestra la ventana Services: Telnet/SSH. Desplácese hacia abajo hasta el área Configuración de shell seguro. Haga clic en Enable junto a Secure Shell e ingrese los parámetros de SSH como se muestra en este ejemplo:

   Este ejemplo utiliza estos parámetros:

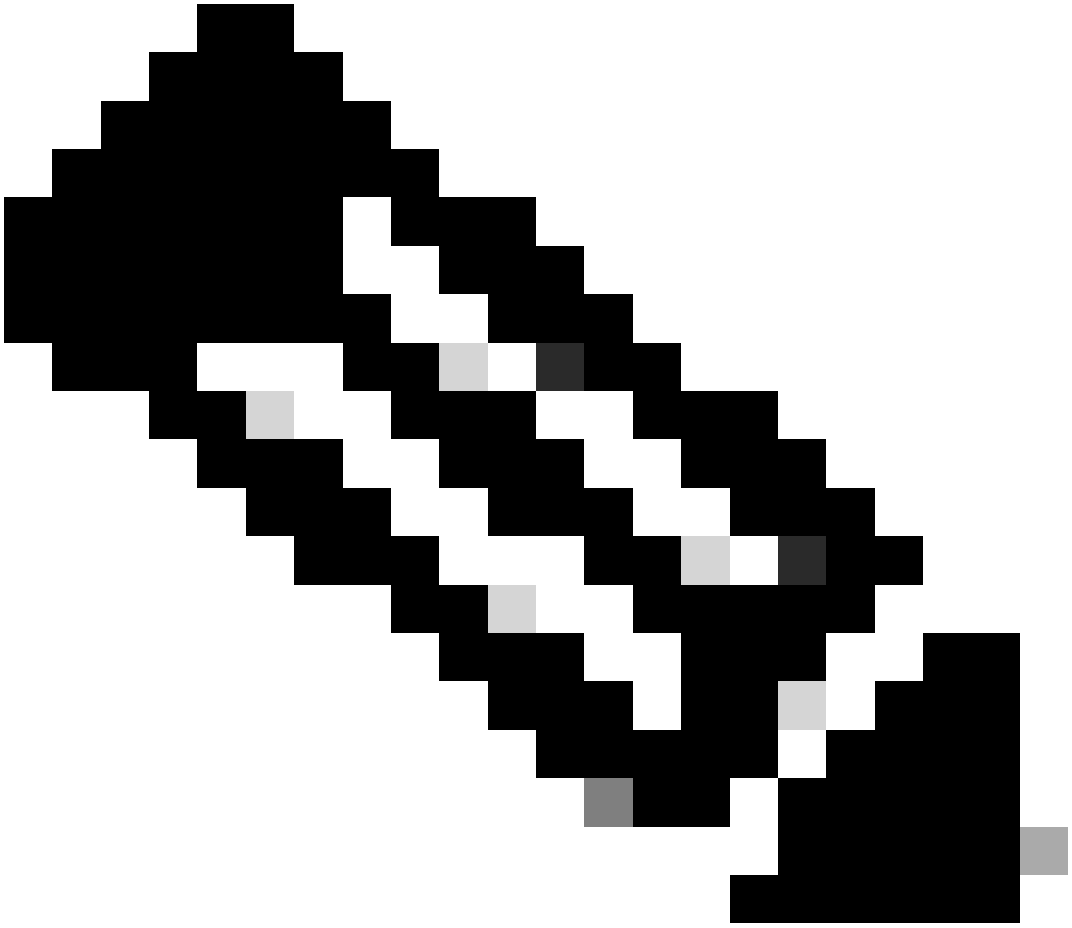
   - Nombre del sistema: Prueba
   - Nombre de dominio: DOMAIN
   - Tamaño de clave RSA: 1024
   - Límite de tiempo de autenticación: 120
   - Reintentos de autenticación: 3

4. Haga clic en Aply para guardar los cambios.

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta Output Interpreter (OIT) es compatible con algunos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.



Nota: solo los usuarios registrados de Cisco pueden acceder a la información y las herramientas internas de Cisco.

- show ip ssh: verifica si SSH está activado en el y le permite verificar la versión de SSH que se ejecuta en el AP. Este resultado incluye un ejemplo:
- show ssh: le permite ver el estado de las conexiones del servidor SSH. Este resultado incluye un ejemplo:

Ahora, inicie una conexión a través de una PC que ejecute software SSH de terceros y luego intente iniciar sesión en el AP. Esta verificación utiliza la dirección IP del AP, 10.0.0.2. Debido a que configuró el nombre de usuario Test, utilice este nombre para acceder al AP a través de SSH:

Troubleshoot

Use esta sección para resolver problemas de configuración.

Si sus comandos de configuración de SSH se rechazan por ilegales, significa que no se ha generado correctamente un par de claves RSA para su AP.

Desactivar SSH

Para desactivar SSH en un AP, debe eliminar el par RSA que se genera en el AP. Para eliminar el par de claves RSA, emita el comando crypto key zeroize rsa en el modo de configuración global. Al eliminar el par de claves RSA, se desactiva automáticamente el servidor SSH. Este resultado incluye un ejemplo:

Información Relacionada

- Página de soporte de Secure Shell (SSH)
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).