Habilitar Secure Shell (SSH) em um Ponto de Acesso (AP)

Contents

Introdução

Este documento descreve como configurar um ponto de acesso (AP) para habilitar o acesso baseado em Secure Shell (SSH).

Pré-requisitos

Requisitos

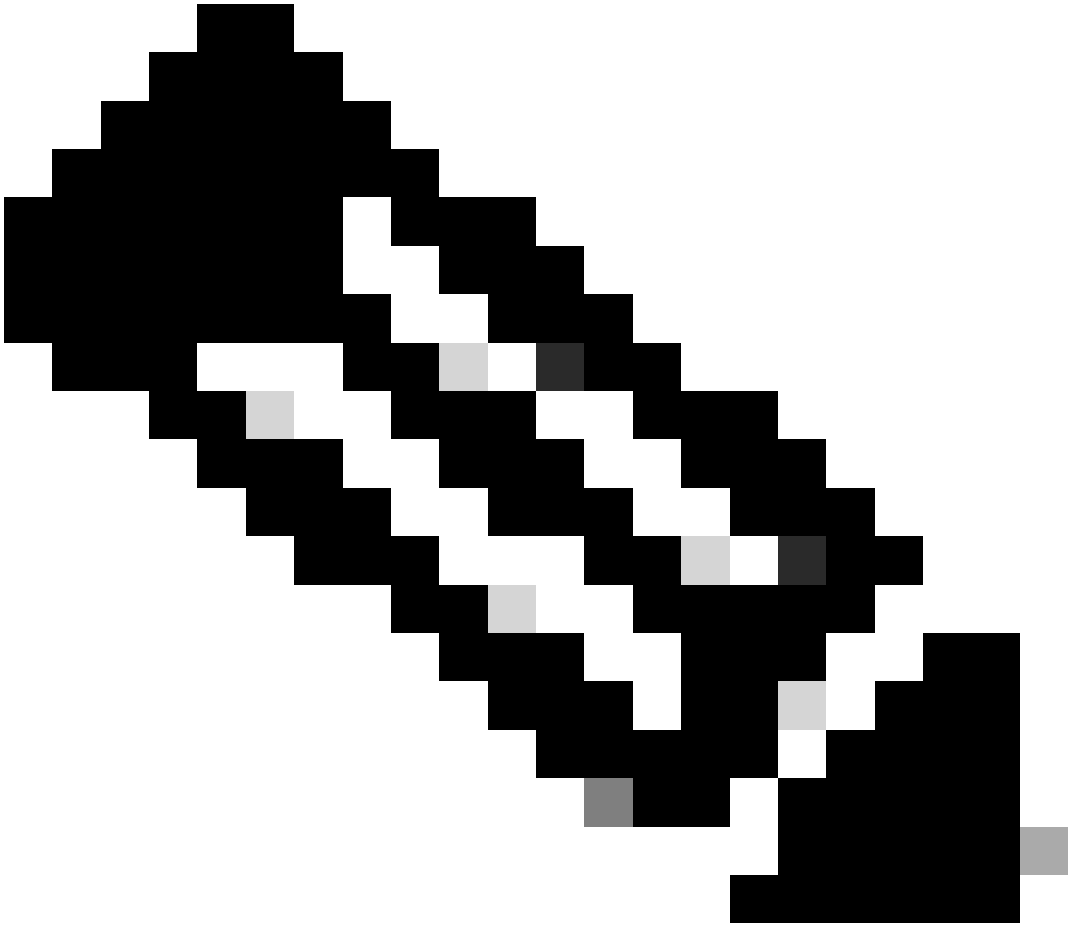
Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Conhecimento de como configurar APs Cisco Aironet
- Conhecimento básico de SSH e conceitos de segurança relacionados

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- AP Aironet 1200 Series que executa o Cisco IOS® Software Release 12.3(8)JEB
- PC ou laptop com utilitário cliente SSH



Observação: este documento usa o utilitário cliente SSH para verificar a configuração. Você pode usar qualquer utilitário cliente de terceiros para fazer login no AP com o uso do SSH.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Acesse a interface de linha de comando (CLI) no AP Aironet

Você pode usar qualquer um destes métodos para acessar a interface de linha de comando (CLI) no AP Aironet:

- Porta do console
- Telnet
- SSH

Se o AP tiver uma porta de console e você tiver acesso físico ao AP, você poderá usar a porta de console para fazer login no AP e alterar a configuração, se necessário. Para obter informações sobre como usar a porta de console para fazer login no AP, consulte a seção Conexão aos Pontos de Acesso 1200 Series Localmente do documentoConfigurar o Ponto de Acesso pela Primeira Vez.

Se você só puder acessar o AP através da Ethernet, use o protocolo Telnet ou o protocolo SSH para fazer login no AP.

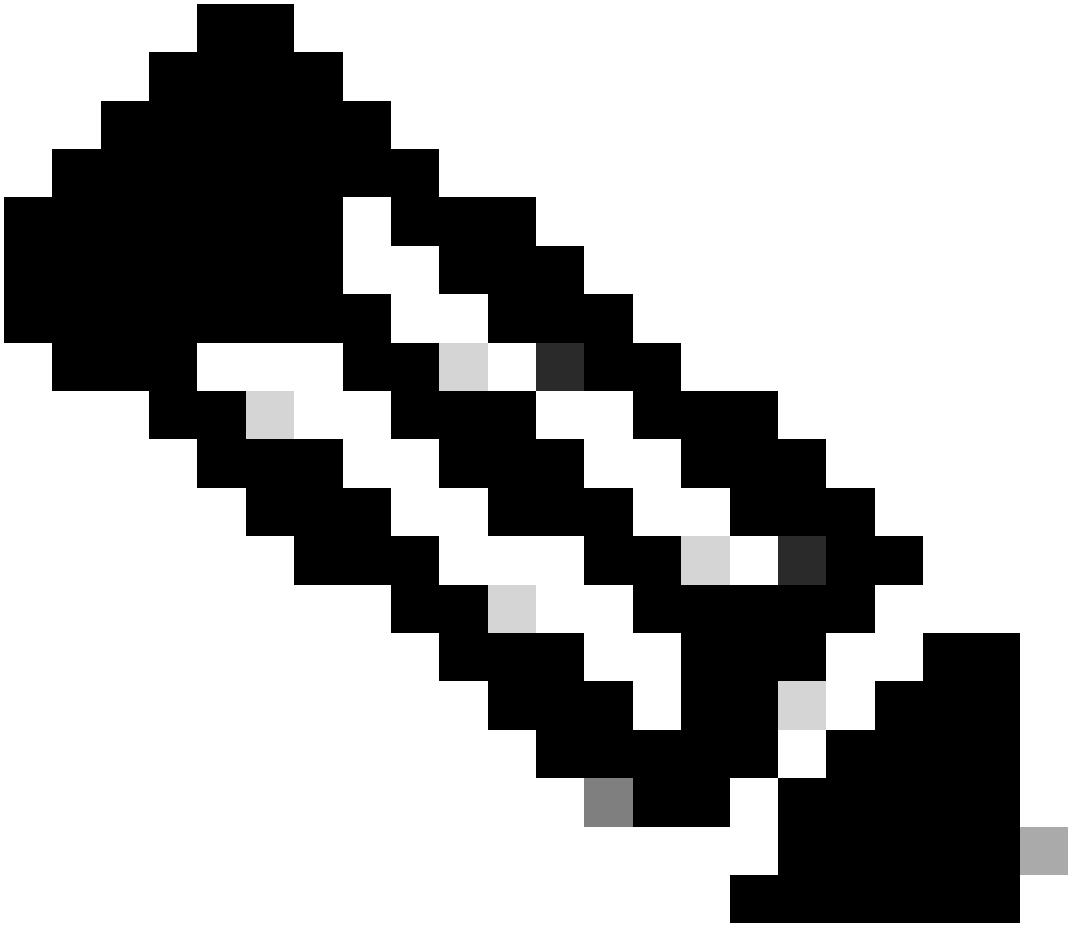
O protocolo Telnet usa a porta 23 para comunicação. O Telnet transmite e recebe dados em texto claro. Como a comunicação de dados acontece em texto claro, um hacker pode facilmente comprometer as senhas e acessar o AP. O RFC 854 define o Telnet e estende o Telnet com opções de muitos outros RFCs.

O SSH é um aplicativo e protocolo que oferece uma substituição segura para as ferramentas Berkley r. O SSH é um protocolo que fornece uma conexão segura e remota a um dispositivo de Camada 2 ou Camada 3. Existem duas versões do SSH: SSH versão 1 e SSH versão 2. Esta versão de software suporta ambas as versões de SSH. Se você não especificar o número da versão, o AP assumirá como padrão a versão 2.

O SSH fornece mais segurança para conexões remotas do que o Telnet, pois fornece criptografia forte quando um dispositivo é autenticado. Essa criptografia é uma vantagem sobre uma sessão Telnet, na qual a comunicação ocorre em texto claro. Para obter mais informações sobre SSH, consulte Perguntas Frequentes sobre Shell Seguro (SSH). O recurso SSH tem um servidor SSH e um cliente integrado SSH.

O cliente oferece suporte aos seguintes métodos de autenticação de usuário:

- RADIUS
- Autenticação e autorização locais.



Observação: o recurso SSH nesta versão de software não suporta IP Security (IPSec).

Você pode configurar APs para SSH com o uso da CLI ou da GUI. Este documento explica os dois métodos de configuração.

Configurar

Configuração de CLI

Esta seção fornece as informações sobre como configurar os recursos com o uso da CLI.

Step-by-Step Instructions

Para habilitar o acesso baseado em SSH no AP, você primeiro deve configurar o AP como um servidor SSH. Siga estas etapas para configurar um servidor SSH no AP a partir da CLI:

1. Configure um nome de host e um nome de domínio para o 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. Gere uma chave Rivest, Shamir e Adelman (RSA) para seu AP.

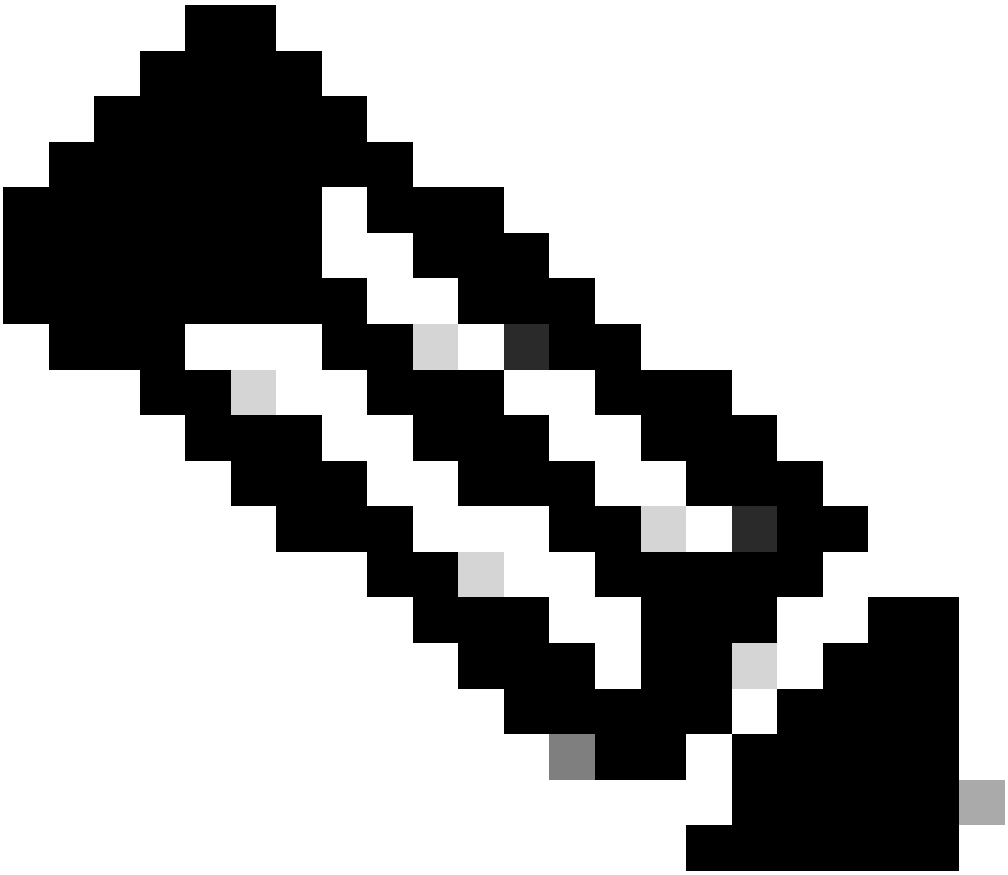
   A geração de uma chave RSA habilita o SSH no AP. Emita este comando no modo de configuração global:

<#root>

Test<config>#

crypto key generate rsa rsa_key_size

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



Observação: o tamanho mínimo recomendado da chave RSA é 1024.

3. Configure a autenticação de usuário no AP.

   No AP, você pode configurar a autenticação de usuário para usar a lista local ou um servidor de autenticação, autorização e contabilização (AAA) externo. Este exemplo usa uma lista gerada localmente para autenticar os usuários:

```
<#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".
```

Essa configuração configura o AP para executar a autenticação baseada no usuário com o uso de um banco de dados local que é configurado no AP. O exemplo configura dois usuários no banco de dados local, "Teste" e "ABC".

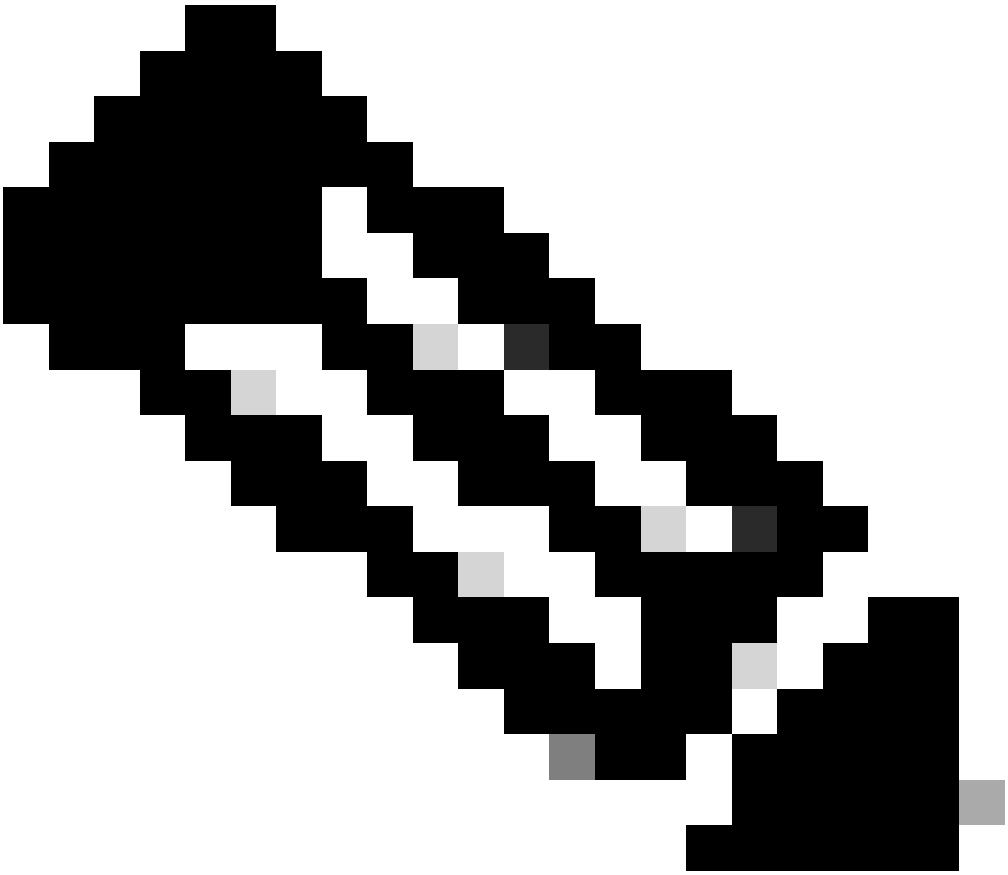
4. Configure os parâmetros SSH.

<#root>

```
Test<config>#

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

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



Observação: você pode especificar o tempo limite em segundos, mas não pode exceder 120 segundos. O padrão é 120. Esta é a especificação que se aplica à fase de negociação SSH. Você também pode especificar o número de tentativas de autenticação, mas não pode exceder cinco. O padrão é três.

Configuração de GUI

Você também pode usar a GUI para ativar o acesso baseado em SSH no AP.

Step-by-Step Instructions

Conclua estes passos:

1. Faça login no AP através do navegador.

   A janela Status do resumo é exibida.

2. Clique em Services no menu à esquerda.

A janela Resumo dos serviços é exibida.

3. Clique em Telnet/SSH para habilitar e configurar os parâmetros Telnet/SSH.

   A janela Serviços: Telnet/SSH é exibida. Role para baixo até a área Secure Shell Configuration. Clique em Enable ao lado de Secure Shell e insira os parâmetros SSH como mostra este exemplo:

   Este exemplo usa estes parâmetros:

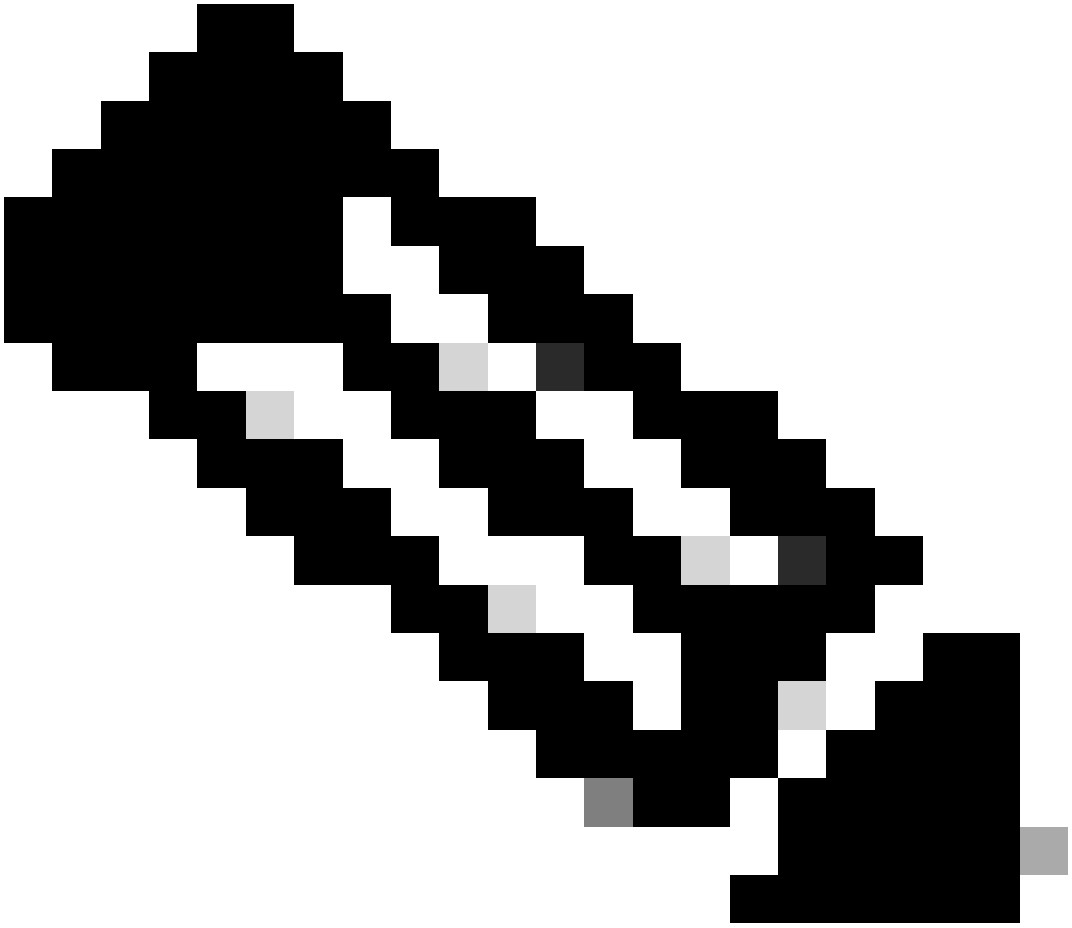
   - Nome do sistema: Teste
   - Nome do domínio: DOMAIN
   - Tamanho da chave RSA: 1024
   - Tempo limite de autenticação: 120
   - Tentativas de Autenticação: 3

4. Clique em Apply para salvar as alterações.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A Output Interpreter Tool (OIT) oferece suporte a determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.



Observação: somente usuários registrados da Cisco podem acessar ferramentas e informações internas da Cisco.

- show ip ssh — Verifica se o SSH está habilitado no AP e permite que você verifique a versão do SSH que é executado no AP. Esta saída fornece um exemplo:
- show ssh — Permite que você exiba o status das conexões do servidor SSH. Esta saída fornece um exemplo:

Agora, inicie uma conexão através de um PC que executa o software SSH de terceiros e, em seguida, faça uma tentativa de fazer login no AP. Essa verificação usa o endereço IP do AP, 10.0.0.2. Como você configurou o nome de usuário Test, use este nome para acessar o AP através de SSH:

Troubleshooting

Use esta seção para resolver problemas de configuração.

Se seus comandos de configuração SSH forem rejeitados como comandos ilegais, você não gerou com êxito um par de chaves RSA para seu AP.

Desabilitar SSH

Para desabilitar o SSH em um AP, você deve excluir o par RSA que é gerado no AP. Para excluir o par RSA, execute o comando crypto key zeroize rsa no modo de configuração global. Ao excluir o par de chaves RSA, você desabilita automaticamente o servidor SSH. Esta saída fornece um exemplo:

Informações Relacionadas

- Página de suporte do Secure Shell (SSH)
- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.