

Entender os algoritmos de criptografia SSH no ISE 3.3 Patch 4

Contents

[Introdução](#)

[Pré-requisitos](#)

[Componentes necessários](#)

[Objetivos](#)

[Benefícios funcionais](#)

[Principais recursos implementados](#)

[Comandos CLI](#)

[Algoritmo HostKey SSH configurável](#)

[Algoritmo HostKey SSHD configurável](#)

[Troubleshooting](#)

[Verificar](#)

[Trecho de log:](#)

[FAQ](#)

Introdução

Este documento descreve sobre os algoritmos de criptografia SSH no ISE versão 3.3 Patch 4

Pré-requisitos

Você deve ter o conhecimento básico do Cisco Identity Service Engine (ISE)

Conhecimento sobre o protocolo SSH

Conhecimento sobre algoritmos de chave de host

Componentes necessários

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

- Cisco Identity Services Engine 3.3 Patch 4

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.

Objetivos

Desenvolva e implemente comandos CLI para suportar algoritmos SSH configuráveis, abordando vulnerabilidades de segurança de acordo com seus requisitos.

Benefícios funcionais

1. Conformidade aprimorada de segurança SSH com diretrizes NIST.
2. Opções flexíveis de configuração para algoritmos SSH para atender a políticas de segurança específicas.

Principais recursos implementados

1. HostKey e Algoritmo de Chave de Host configuráveis a partir da CLI.
2. Suporte para ecdsa-sha2-nistp256 e chave de host final.
3. Suporte para hmac-sha2-256 e hmac-sha2-512 para conexões SSH seguras

Comandos CLI

- Service ssh host-key-algorithm
- Service sshd host-key
- Service sshd host-key-algorithm
- Service sshd mac-algorithm

Algoritmo HostKey SSH configurável

Para configurar o algoritmo HostKey SSH para comunicação externa do servidor

Comando: asc-ise33p4/admin(config)# service ssh host-key-algorithm ?

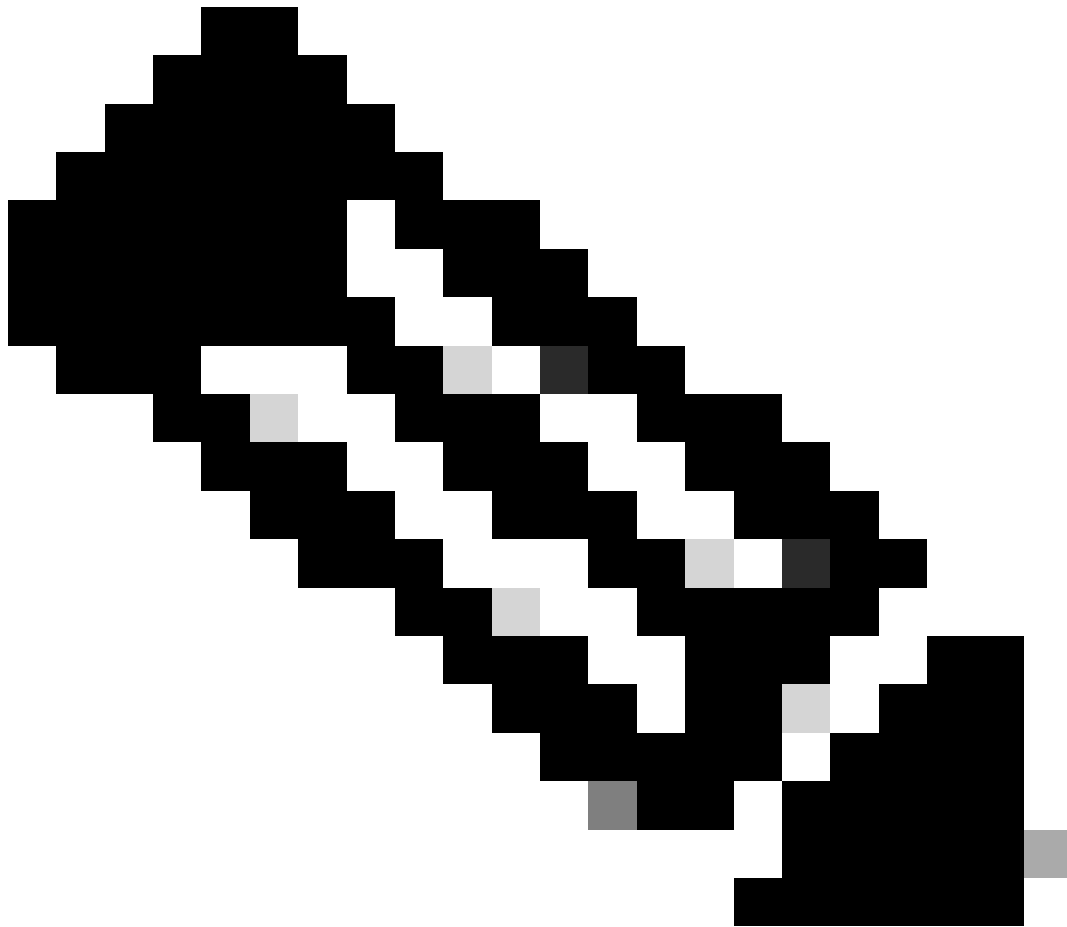
Possíveis conclusões:

ecdsa-sha2-nistp256 Configurar ecdsa-sha2-nistp256 algo

rsa-sha2-256 Configurar rsa-sha2-256 algo

rsa-sha2-512 Configurar rsa-sha2-512 algo

ssh-rsa Configure ssh-rsa algo



Note: Isto é para SSH

Algoritmo HostKey SSHD configurável

Para configurar a HostKey SSHD para a autenticação do servidor SSH.

Comando: `asc-ise33p4/admin(config)# service sshd host-key ?`

Possíveis conclusões:

host-ecdsa-256 Configurar ssh host ecdsa 256 chave

host-ed25519 Configurar chave ssh host ed25519

host-rsa Configurar ssh host rsa key

Para configurar o algoritmo de chave de host SSHD para a autenticação do servidor SSH.

Comando: asc-ise33p4/admin(config)#service sshd host-key-algorithm ?

Possíveis conclusões:

ecdsa-sha2-nistp256 Configurar ecdsa-sha2-nistp256 algo

rsa-sha2-256 Configurar rsa-sha2-256 algo

rsa-sha2-512 Configurar rsa-sha2-512 algo

ssh-ed25519 Configurar ssh-ed25519 algo

Para configurar o algoritmo MAC SSHD para a autenticação do servidor SSH.

Comando: asc-ise33p4/admin(config)#service sshd mac-algorithm ?

Possíveis conclusões:

hmac-sha1 Configurar hmac-sha1 algo

hmac-sha1-etm-openssh.com Configurar hmac-sha1-etm-openssh.com algo

hmac-sha2-256 Configurar hmac-sha2-256 algo

hmac-sha2-256-etm-openssh.com Configurar hmac-sha2-256-etm@openssh.com algo

hmac-sha2-512 Configurar hmac-sha2-512 algo

hmac-sha2-512-etm-openssh.com Configurar hmac-sha2-512-etm@openssh.com algo



Note: Isto é para SSHD

Troubleshooting

Verificar

SSH:

```
isepri33/admin(config)#service ssh host-key-algorithm ecdsa-sha2-nistp256
```

```
isepri33/admin#show running-config service ssh  
service ssh host-key-algorithm ecdsa-sha2-nistp256
```

SSHD:

```
isepri33/admin(config)#service sshd host-key-algorithm ecdsa-sha2-nistp256
```

```
isepri33/admin#show running-config service sshd
service sshd enable
service sshd encryption-algorithm aes128-ctr aes128-gcm-openssh.com aes256-ctr aes256-gcm-openssh.com chacha20-poly1305-openssh.com
service sshd host-key-algorithm ecdsa-sha2-nistp256
service sshd mac-algorithm hmac-sha1 hmac-sha2-256 hmac-sha2-512
service sshd host-key host-rsa
```

Trecho de log:

```
isepri33/admin#show logging system confd/confd.log
2025-03-18 08:35:25,241 [INFO] service_conf.py update_host_key_algorithm line:575 Algoritmos de chaves de host SSH atualizados com êxito
2025-03-18 08:35:39,056 [INFO] service_conf.py update_host_key_algorithm line:567 Algoritmos de chave de host: ecdsa-sha2-nistp256
2025-03-18 08:35:39,260 [INFO] service_conf.py restart_sshd line:259 Sshd reiniciado com êxito

2025-03-18 08:48:20,194 [INFO] service_conf.py update_host_key_algorithm line:567 Algoritmos de chave de host: ecdsa-sha2-nistp256
2025-03-18 08:48:20,396 [INFO] service_conf.py restart_sshd line:259 Sshd reiniciado com êxito
2025-03-18 08:48:20,400 [INFO] service_conf.py update_host_key_algorithm line:575 Algoritmos de chaves de host SSH atualizados com êxito
2025-03-18 08:49:00,442 [INFO] service_conf.py update_host_key_algorithm line:567 Algoritmos de chave de host: ecdsa-sha2-nistp256
2025-03-18 08:49:00,672 [INFO] service_conf.py restart_sshd line:259 Sshd reiniciado com êxito
2025-03-18 08:49:00,674 [INFO] service_conf.py update_host_key_algorithm line:575 Algoritmos de chaves de host SSH atualizados com êxito
```

FAQ

Pergunta: Qual é o algoritmo de chave de host SSH padrão habilitado no ISE?

Resposta: São elas:

- rsa-sha2-256
- rsa-sha2-512

Pergunta: Quais são os algoritmos de chave MAC SSHD padrão?

Resposta: São elas:

- hmac-sha1
- hmac-sha2-256
- hmac-sha2-512

Pergunta: Qual é a chave de host SSHD padrão?

Resposta: host-rsa

Pergunta: Qual é a chave de host SSH padrão?

Resposta: São elas:

- rsa-sha2-256
- rsa-sha2-512
- ssh-rsa

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.