了解ISE 3.3补丁4上的SSH加密算法

目录

简介

本文档介绍ISE版本3.3补丁4上的SSH加密算法

前提条件

您必须具备思科身份服务引擎(ISE)的基本知识

SSH协议知识

主机密钥算法知识

所需组件

本文档中的信息基于以下软件和硬件版本

- 思科身份服务引擎3.3补丁4

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

目标

开发并实施CLI命令以支持可配置的SSH算法，并根据您的要求解决安全漏洞。

功能优势

1. 根据NIST准则增强SSH安全合规性。
2. 灵活的SSH算法配置选项，以满足特定的安全策略。

实施的主要功能

1. CLI中的可配置主机密钥和主机密钥算法
2. 支持ecdsa-sha2-nistp256和ed主机密钥。
3. 支持用于安全SSH连接的hmac-sha2-256和hmac-sha2-512

CLI命令

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

可配置的SSH HostKey算法

配置用于外部服务器通信的SSH主机密钥算法

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

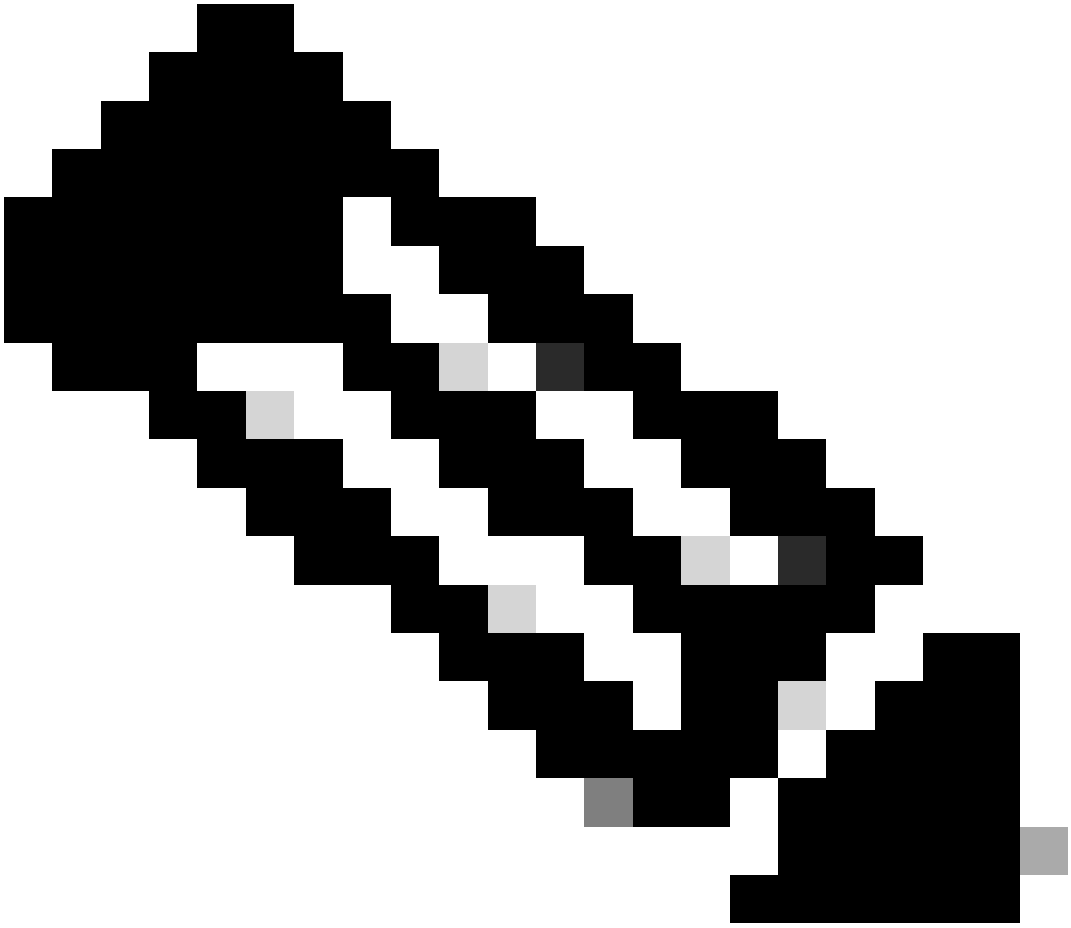
可能完成的任务：

ecdsa-sha2-nistp256配置ecdsa-sha2-nistp256 algo

rsa-sha2-256配置rsa-sha2-256 algo

rsa-sha2-512配置rsa-sha2-512 algo

ssh-rsa配置ssh-rsa algo



注意：这是用于SSH

可配置的SSHD主机密钥算法

配置用于SSH服务器身份验证的SSHD主机密钥。

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

可能完成的任务：

host-ecdsa-256配置ssh host ecdsa 256密钥

host-ed25519配置ssh host ed25519 key

host-rsa配置ssh host rsa密钥

配置用于SSH服务器身份验证的SSHD主机密钥算法。

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

可能完成的任务：

ecdsa-sha2-nistp256配置ecdsa-sha2-nistp256 algo

rsa-sha2-256配置rsa-sha2-256 algo

rsa-sha2-512配置rsa-sha2-512 algo

ssh-ed25519配置ssh-ed25519 algo

配置用于SSH服务器身份验证的SSHD MAC算法。

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

可能完成的任务：

hmac-sha1配置hmac-sha1 algo

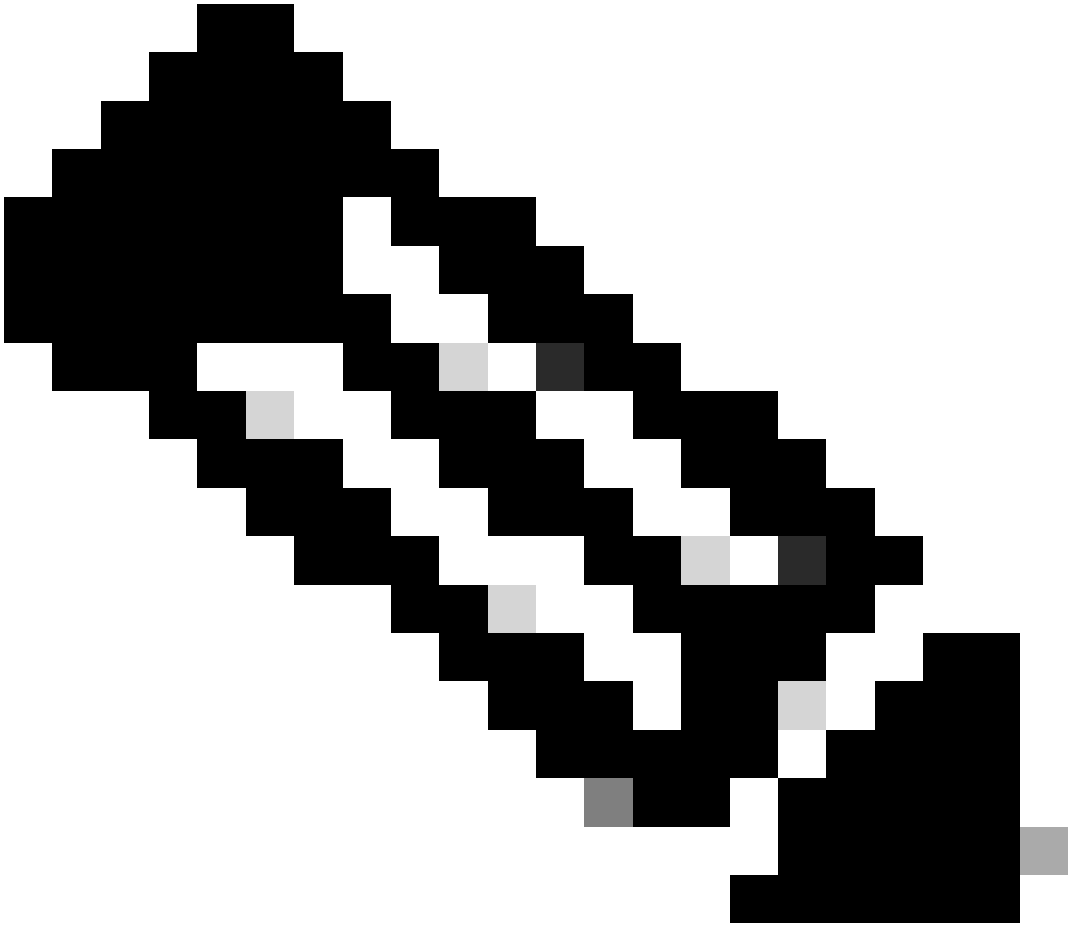
hmac-sha1-etm-openssh.com配置hmac-sha1-etm-openssh.com algo

hmac-sha2-256配置hmac-sha2-256 algo

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

hmac-sha2-512配置hmac-sha2-512 algo

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



注意：这是针对SSHD的

故障排除

验证

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
```

日志片段：

```
isepri33/admin#show logging system confd/confd.log
2025-03-18 08:35:25,241 [INFO] service_conf.py update_host_key_algorithms line:575已成功更新SSH主机密钥算法
2025-03-18 08:35:39,056 [INFO] service_conf.py update_host_key_algorithms行：567主机密钥算法：ecdsa-sha2-nistp256
2025-03-18 08:35:39,260 [INFO] service_conf.py restart_sshd line:259成功重新启动sshd

2025-03-18 08:48:20,194 [INFO] service_conf.py update_host_key_algorithms行：567主机密钥算法：ecdsa-sha2-nistp256
2025-03-18 08:48:20,396 [INFO] service_conf.py restart_sshd line:259成功重新启动sshd
2025-03-18 08:48:20,400 [INFO] service_conf.py update_host_key_algorithms line:575已成功更新SSH主机密钥算法
2025-03-18 08:49:00,442 [INFO] service_conf.py update_host_key_algorithms行：567主机密钥算法：ecdsa-sha2-nistp256
2025-03-18 08:49:00,672 [INFO] service_conf.py restart_sshd line:259成功重新启动sshd
2025-03-18 08:49:00,674 [INFO] service_conf.py update_host_key_algorithms line:575已成功更新SSH主机密钥算法
```

常见问题

问题：ISE上启用的默认SSH主机密钥算法是什么？

回答：它们是：

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

问题：什么是默认SSHD MAC密钥算法？

回答：它们是：

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

问题：默认SSHD主机密钥是什么？

回答：host-rsa

问题：默认SSH主机密钥是什么？

回答：它们是：

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

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。