SSH-Verschlüsselungsalgorithmen auf ISE 3.3 Patch 4 verstehen

Inhalt

Einleitung

Dieses Dokument beschreibt SSH-Verschlüsselungsalgorithmen auf der ISE Version 3.3 Patch 4.

Voraussetzungen

Sie müssen über die Grundkenntnisse der Cisco Identity Service Engine (ISE) verfügen.

Kenntnisse über das SSH-Protokoll

Kenntnisse zu Host-Key-Algorithmen

Erforderliche Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen

- Patch 4 der Cisco Identity Services Engine 3.3

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Ziele

Entwicklung und Implementierung von CLI-Befehlen zur Unterstützung konfigurierbarer SSH-Algorithmen, um Sicherheitslücken entsprechend Ihrer Anforderungen zu schließen

Funktionsvorteile

1. Verbesserte SSH-Sicherheit und Konformität mit NIST-Richtlinien
2. Flexible Konfigurationsoptionen für SSH-Algorithmen zur Erfüllung bestimmter Sicherheitsrichtlinien.

Wichtigste implementierte Funktionen

1. Konfigurierbarer HostKey und Hostkey-Algorithmus über CLI.
2. Unterstützung für ecdsa-sha2-nistp256 und ed host key.
3. Unterstützung für hmac-sha2-256 und hmac-sha2-512 für sichere SSH-Verbindungen

CLI-Befehle

- Service-SSH-Host-Schlüssel-Algorithmus
- Service-sshd-Hostschlüssel
- Service-sshd Host-Schlüssel-Algorithmus
- Service-Sshd-MAC-Algorithmus

Konfigurierbarer SSH HostKey-Algorithmus

So konfigurieren Sie den SSH HostKey-Algorithmus für die Kommunikation mit externen Servern

Befehl: asc-ise33p4/admin(config)# service ssh host-key-algorithmus ?

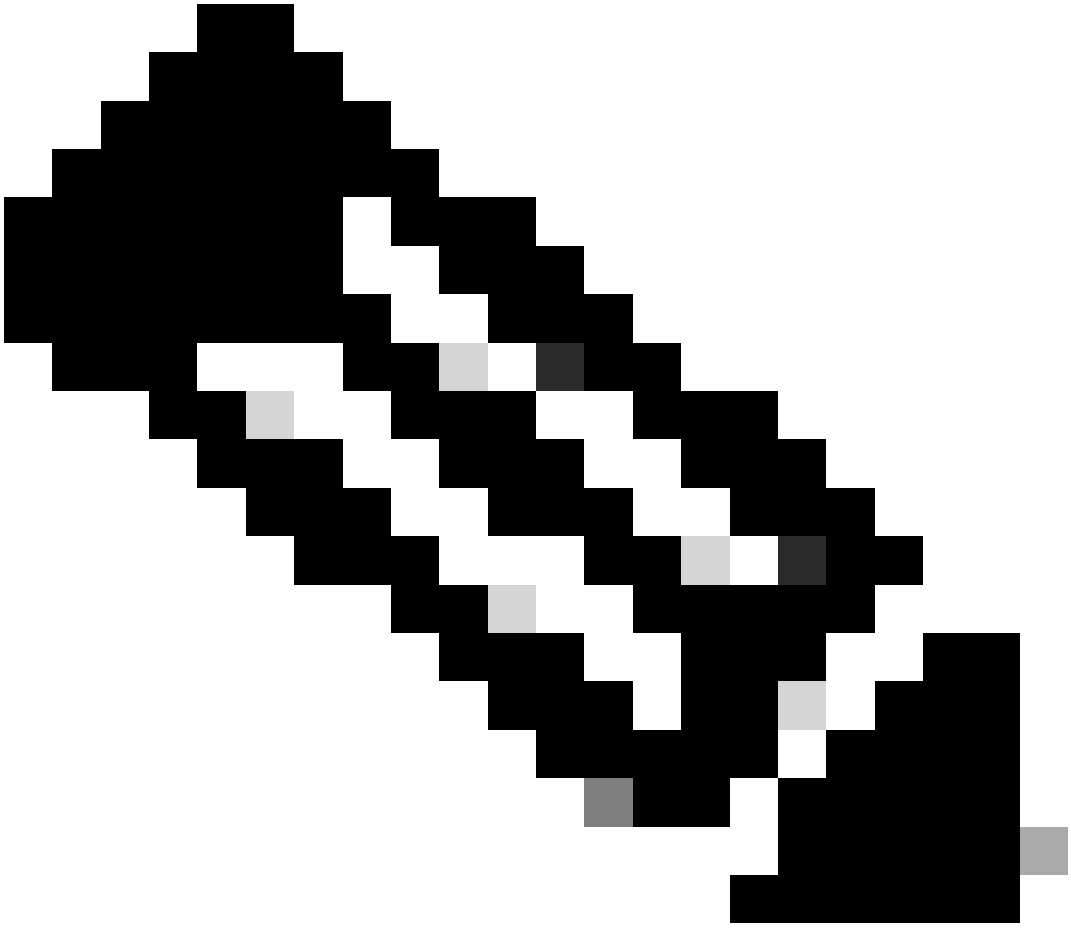
Mögliche Ergänzungen:

ecdsa-sha2-nistp256 Konfigurieren von ecdsa-sha2-nistp256 Algo

rsa-sha2-256 Konfigurieren rsa-sha2-256 algo

rsa-sha2-512 Konfigurieren rsa-sha2-512 algo

ssh-rsa Konfigurieren von ssh-rsa algo



Anmerkung: Dies gilt für SSH

Konfigurierbarer SSHD HostKey-Algorithmus

So konfigurieren Sie den SSHD-Hostschlüssel für die SSH-Serverauthentifizierung.

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

Mögliche Ergänzungen:

host-ecdsa-256 Konfigurieren des Schlüssels ssh host ecdsa 256

host-ed25519 Konfigurieren Sie den Schlüssel ssh host-ed25519

host-rsa Konfigurieren des RSA-Schlüssels für den Host

So konfigurieren Sie den SSHD-Hostschlüsselalgorithmus für die SSH-Serverauthentifizierung.

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

Mögliche Ergänzungen:

ecdsa-sha2-nistp256 Konfigurieren von ecdsa-sha2-nistp256 Algo

rsa-sha2-256 Konfigurieren rsa-sha2-256 algo

rsa-sha2-512 Konfigurieren rsa-sha2-512 algo

ssh-ed25519 ssh-ed25519 konfigurieren algo

So konfigurieren Sie den SSHD-MAC-Algorithmus für die SSH-Serverauthentifizierung:

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

Mögliche Ergänzungen:

hmac-sha1 Konfigurieren hmac-sha1 algo

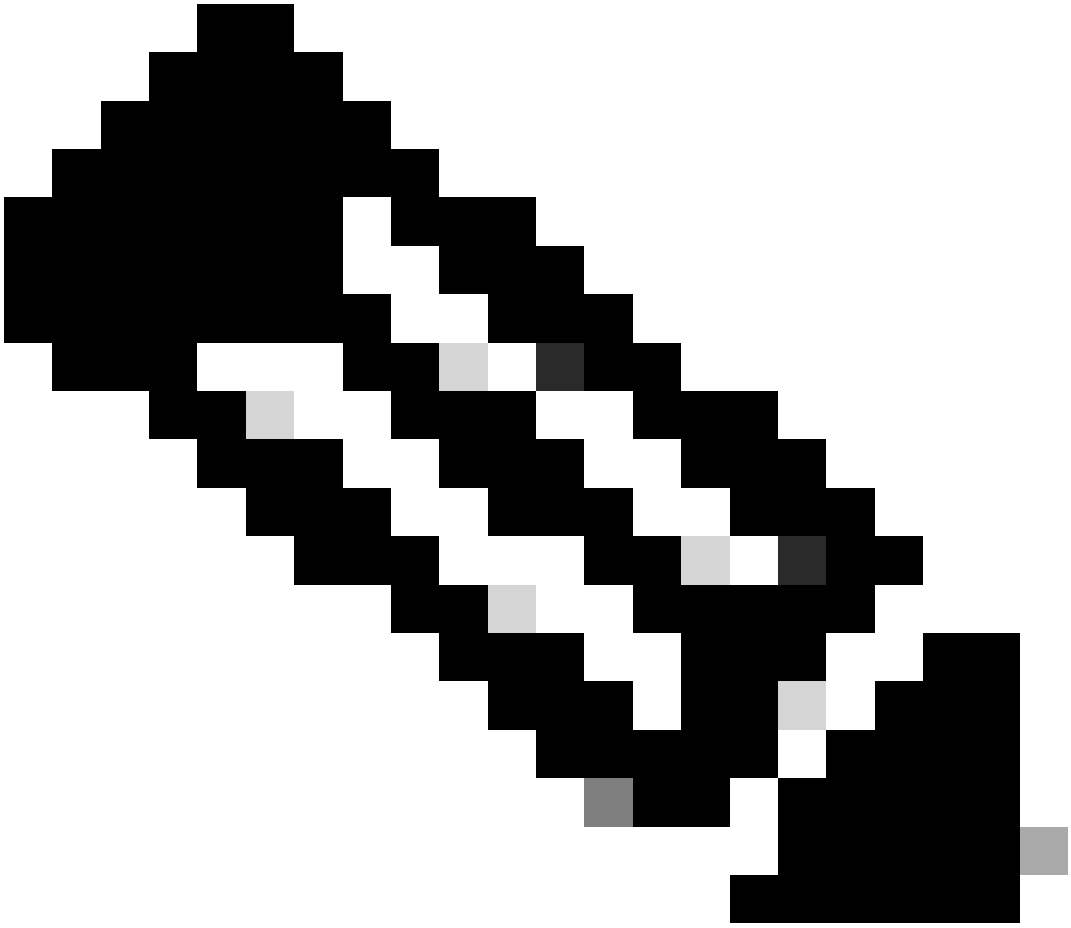
hmac-sha1-etm-openssh.com Konfigurieren hmac-sha1-etm-openssh.com algo

hmac-sha2-256 Konfigurieren Sie hmac-sha2-256 Algo

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

hmac-sha2-512 Konfigurieren Sie hmac-sha2-512 algo

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



Anmerkung: Dies gilt für SSHD

Fehlerbehebung

Überprüfung

SSH:
isepri33/admin(config)#service ssh host-key-algorithmus ecdsa-sha2-nistp256

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

SSHD:

isepri33/admin(config)#service sshd host-key-algorithmus 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-algorithmus ecdsa-sha2-nistp256
service sshd mac-algorithmus hmac-sha1 hmac-sha2-256 hmac-sha2-512
service sshd host-key host-rsa
```

Protokollausschnitt:

```
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 SSH Host Keys Algorithms erfolgreich aktualisiert
2025-03-18 08:35:39,056 [INFO] service_conf.py update_host_key_algorithms line:567 Host key Algorithmen: ecdsa-sha2-nistp256
2025-03-18 08:35:39,260 [INFO] service_conf.py restart_sshd line:259 sshd erfolgreich neu gestartet

2025-03-18 08:48:20,194 [INFO] service_conf.py update_host_key_algorithms line:567 Host key Algorithmen: ecdsa-sha2-nistp256
2025-03-18 08:48:20,396 [INFO] service_conf.py restart_sshd line:259 sshd erfolgreich neu gestartet
2025-03-18 08:48:20,400 [INFO] service_conf.py update_host_key_algorithms line:575 SSH Host Keys Algorithms erfolgreich aktualisiert
2025-03-18 08:49:00,442 [INFO] service_conf.py update_host_key_algorithms line:567 Host key Algorithmen: ecdsa-sha2-nistp256
2025-03-18 08:49:00,672 [INFO] service_conf.py restart_sshd line:259 sshd erfolgreich neu gestartet
2025-03-18 08:49:00,674 [INFO] service_conf.py update_host_key_algorithms line:575 SSH Host Keys Algorithms erfolgreich aktualisiert
```

Häufig gestellte Fragen

Frage: Welcher SSH-Hostschlüsselalgorithmus ist auf der ISE standardmäßig aktiviert?

Antwort: Dazu gehören:

- RSA-SHA2-256
- RSA-SHA2-512

Frage: Welcher SSHD-MAC-Schlüsselalgorithmus wird standardmäßig verwendet?

Antwort: Dazu gehören:

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

Frage: Was ist der Standard-SSHD-Hostschlüssel?

Antwort: Host-RSA

Frage: Wie lautet der Standard-SSH-Hostschlüssel?

Antwort: Dazu gehören:

- RSA-SHA2-256
- RSA-SHA2-512
- SSH-RSA

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.