

ISE 3.3 패치 4의 SSH 암호화 알고리즘 이해

목차

[소개](#)

[전제 조건](#)

[필수 구성 요소](#)

[목표](#)

[기능적 이점](#)

[주요 기능 구현](#)

[CLI 명령](#)

[구성 가능한 SSH HostKey 알고리즘](#)

[구성 가능한 SSHD HostKey 알고리즘](#)

[문제 해결](#)

[다음을 확인합니다.](#)

[로그 조각:](#)

[FAQ](#)

소개

이 문서에서는 ISE 버전 3.3 패치 4의 SSH 암호화 알고리즘에 대해 설명합니다

전제 조건

Cisco ISE(Identity Service Engine)에 대한 기본 지식이 있어야 합니다

SSH 프로토콜에 대한 지식

호스트 키 알고리즘에 대한 지식

필수 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Identity Services Engine 3.3 패치 4

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

목표

구성 가능한 SSH 알고리즘을 지원하는 CLI 명령을 개발 및 구현하여 요구 사항에 따라 보안 취약성

을 해결합니다.

기능적 이점

1. NIST 지침에 따라 향상된 SSH 보안 규정 준수.
2. SSH 알고리즘의 유연한 구성 옵션을 통해 특정 보안 정책을 충족합니다.

주요 기능 구현

1. CLI에서 구성 가능한 HostKey 및 Hostkey 알고리즘
2. ecdsa-sha2-nistp256 및 ed 호스트 키 지원
3. 보안 SSH 연결을 위한 hmac-sha2-256 및 hmac-sha2-512 지원

CLI 명령

- 서비스 ssh 호스트 키 알고리즘
- 서비스 sshd 호스트 키
- 서비스 sshd 호스트 키 알고리즘
- 서비스 sshd mac 알고리즘

구성 가능한 SSH HostKey 알고리즘

외부 서버 통신을 위한 SSH HostKey 알고리즘 구성

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

가능한 완료:

ecdsa-sha2-nistp256 ecdsa-sha2-nistp256 algo 구성

rsa-sha2-256 rsa-sha2-256 algo 구성

rsa-sha2-512 rsa-sha2-512 algo 구성

ssh-rsa ssh-rsa algo 구성



참고: SSH용입니다.

구성 가능한 SSHD HostKey 알고리즘

SSH 서버 인증을 위해 SSHD 호스트 키를 구성합니다.

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

가능한 완료:

`host-ecdsa-256 ssh host ecdsa 256 키 구성`

`host-ed25519 ssh host ed25519 키 구성`

`host-rsa ssh 호스트 rsa 키 구성`

SSH 서버 인증을 위한 SSHD 호스트 키 알고리즘을 구성합니다.

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

가능한 완료:

ecdsa-sha2-nistp256 ecdsa-sha2-nistp256 algo 구성

rsa-sha2-256 rsa-sha2-256 algo 구성

rsa-sha2-512 rsa-sha2-512 algo 구성

ssh-ed25519 ssh-ed25519 algo 구성

SSH 서버 인증을 위해 SSHD MAC 알고리즘을 구성합니다.

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

가능한 완료:

hmac-sha1 hmac-sha1 algo 구성

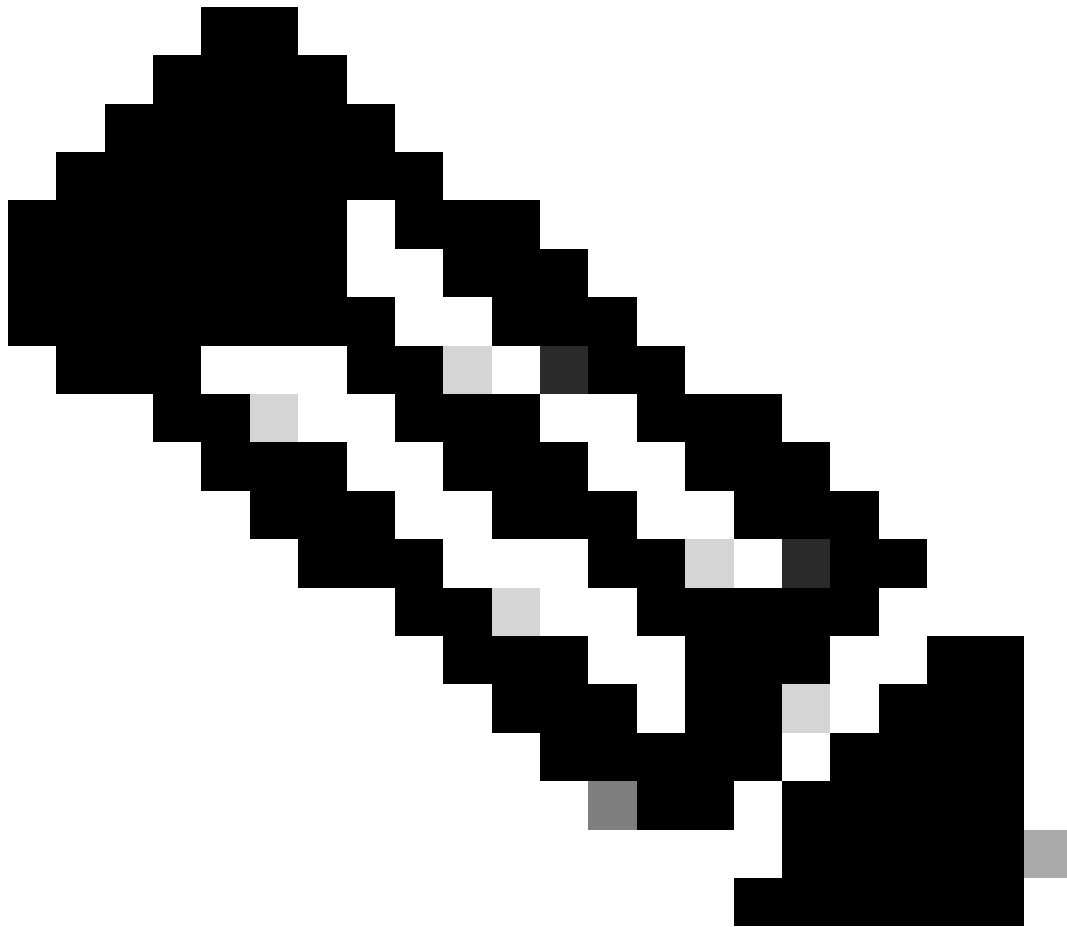
hmac-sha1-etm-openssh.com hmac-sha1-etm-openssh.com algo 구성

hmac-sha2-256 hmac-sha2-256 algo 구성

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

hmac-sha2-512 hmac-sha2-512 algo 구성

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



참고: SSHD용입니다.

문제 해결

다음을 확인합니다.

SSH:

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

```
isepri33/admin#show running-config service ssh
```

```
서비스 ssh host-key-algorithm ecdsa-sha2-nistp256
```

SSHD:

```
isepri33/admin(config)#service sshd 호스트 키 알고리즘 ecdsa-sha2-nistp256
```

```
isepri33/admin#show running-config service sshd
```

서비스 sshd 활성화

서비스 sshd 암호화 알고리즘 aes128-ctr aes128-gcm-openssh.com aes256-ctr aes256-gcm-openssh.com chacha20-poly1305-openssh.com

서비스 sshd 호스트 키 알고리즘 ecdsa-sha2-nistp256

서비스 sshd mac-algorithm hmac-sha1 hmac-sha2-256 hmac-sha2-512

service sshd host-key host-rsa

로그 조각:

```
isepri33/admin#show logging system confd/confd.log
```

2025-03-18 08:35:25,241 [정보] service_conf.py update_host_key_algorithms 라인:575 업데이트된 SSH 호스트 키 알고리즘 성공

2025-03-18 08:35:39,056 [정보] service_conf.py update_host_key_algorithms 라인:567 호스트 키 알고리즘: ecdsa-sha2-nistp256

2025-03-18 08:35:39,260 [정보] service_conf.py restart_sshd line:259 sshd를 성공적으로 다시 시작했습니다.

2025-03-18 08:48:20,194 [정보] service_conf.py update_host_key_algorithms 라인:567 호스트 키 알고리즘: ecdsa-sha2-nistp256

2025-03-18 08:48:20,396 [정보] service_conf.py restart_sshd line:259 sshd를 성공적으로 다시 시작했습니다.

2025-03-18 08:48:20,400 [정보] service_conf.py update_host_key_algorithms 라인:575 SSH 호스트 키 알고리즘 성공적으로 업데이트

2025-03-18 08:49:00,442 [정보] service_conf.py update_host_key_algorithms 라인:567 호스트 키 알고리즘: ecdsa-sha2-nistp256

2025-03-18 08:49:00,672 [정보] service_conf.py restart_sshd line:259 sshd를 성공적으로 다시 시작했습니다.

2025-03-18 08:49:00,674 [정보] service_conf.py update_host_key_algorithms 라인:575 SSH 호스트 키 알고리즘 성공적으로 업데이트

FAQ

질문: ISE에서 활성화되는 기본 SSH 호스트 키 알고리즘은 무엇입니까?

답변: 제품:

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

질문: 기본 SSHD MAC 키 알고리즘은 무엇입니까?

답변: 제품:

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

질문: 기본 SSHD 호스트 키는 무엇입니까?

답변: 호스트 rsa

질문: 기본 SSH 호스트 키는 무엇입니까?

답변: 제품:

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

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.