

ISE جي حصت ىل SSH ري فشت تاي مزراوخ مهف 3.3 4

تايوت حمل

[قم دقمل](#)

[قيساس الابل طتمل](#)

[قبول طمل تانوكمل](#)

[فاده ال](#)

[قي في طول دي اوفل](#)

[اهذيفنت ميتل قيسي ئرل تازيمل](#)

[CLI رمل](#)

[نيوكتلر قلاب ال SSH HostKey قيمي مزراوخ](#)

[نيوكتلر قلاب ال SSHD HostKey قيمي مزراوخ](#)

[اهج الصاوع اطل ال افاشكتسا](#)

[قحصلا تم ققحتل](#)

[لجسلا عصا صق](#)

[قعي اشل اقلي س ال](#)

قم دقمل

3.3 4 رادصل ال ISE جي حصت ىل SSH ري فشت تاي مزراوخ لوح دنتسمل اذه فصي

قيساس الابل طتمل

(ISE) كرحم قيوه قم دخ cisco ال نم قيساس ال افرعمل ىقلى تي يغبني تنأ

SSH لوكوتورب لوح افرعمل

فيضم ال حاتم تاي مزراوخ افرعم

قبول طمل تانوكمل

قيلاتل قيدامل تانوكمل او جمارب ال تارادصل ال دنتسمل اذه في دراوال تامولعمل دنتست

- Cisco Identity Services Engine 3.3 Patch 4 جم انرب ال

عصاخ قيلمعم قئي ب في دوجومل ازه ال نم دنتسمل اذه في دراوال تامولعمل عاشنإ مت تناك اذإ. (يضا رتفا) حوسمم نيوكتب دنتسمل اذه في قم دخ تسمل ازه ال عيمج تأدب رمل آل لم تحمل ري ثاتلر كمهف نم دكاتف، لي غشتل دي قكتكبش

فاده ال

نام أال ةقبط لوكوتورب تاي مزرراوخ معدل اهذي فننتو (CLI) رماوأل رطس ةهجاو رماوأل ريوطت ب مق كئابلطتمل اق فو ةي نم أال فعضل طاقن ةجل اعمو، نيوكتلل ةلباقل (SSH).

ةيفيظولأ دئاول

1. NIST تاداشرا عم نسحمل SSH نامأ قفاوت.
2. ةني عم نامأ تاسايسب ءافولل SSH تاي مزرراوخل ةنرم نيوكت تاراخ.

اهذي فننت متي تلأ ةيسئي رلأ تازي ملأ

1. CLI نم نيوكتلل ةلباقل Hostkey و HostKey ةي مزرراوخ.
2. ED فيضم لأ حات فم و ECDSA-SHA2-NISTP256 معد.
3. SSH ل ةنم أال HMAC-SHA2-512 و HMAC-SHA2-256 تالاصتإ معد.

رماوأل CLI

- ةمدخلل SSH فيضم حات فم ةي مزرراوخ
- ةمدخلل SSHd فيضم حات فم
- Service SSHd Host-key ةي مزرراوخ
- ةمدخلل SSHd ةي مزرراوخ

نيوكتلل ةلباقل SSH HostKey ةي مزرراوخ

ةيجراخلأ مداخلأ تالاصتال SSH HostKey ةي مزرراوخ نيوكتلل

؟ service ssh host-key # admin(config) ASC-ise33p4 ةي مزرراوخ :رملأ

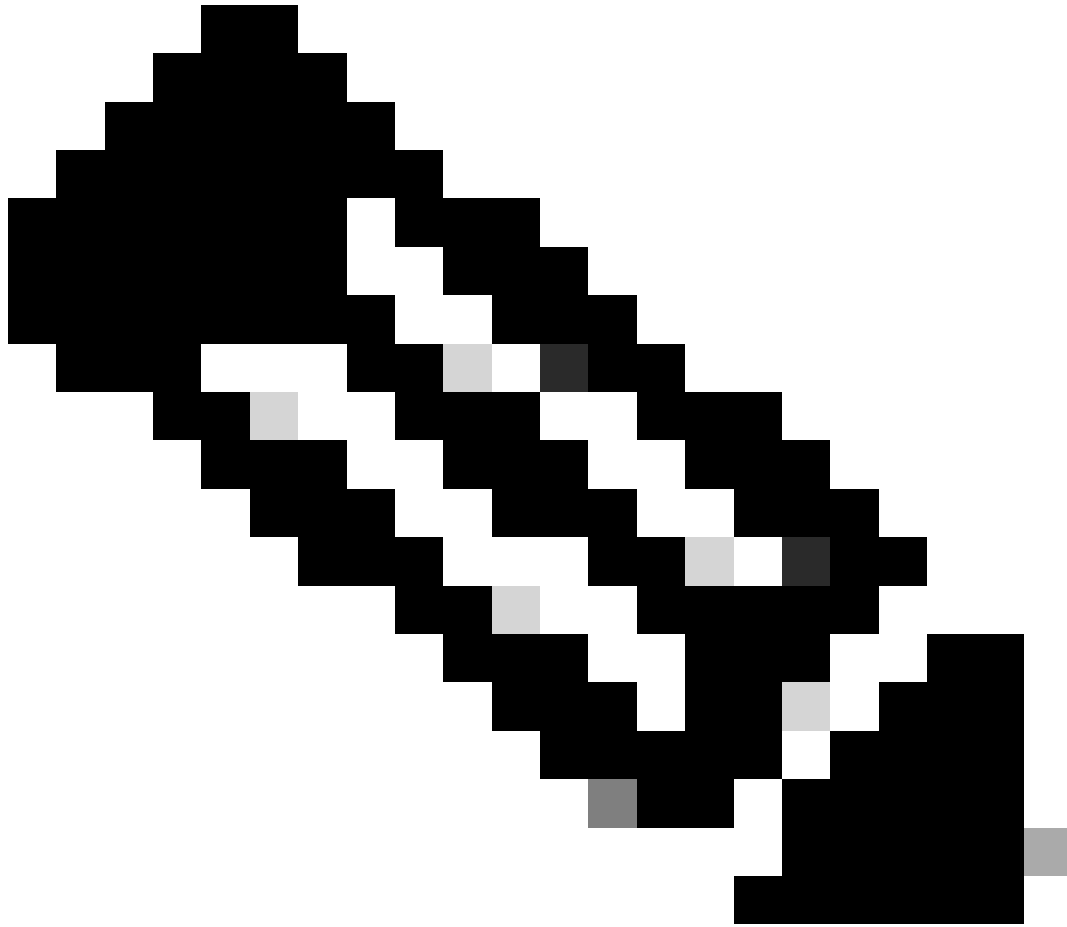
ل:محملأ لامكإلأ

ecdsa-sha2-nistp256 نيوكت ecdsa-sha2-nistp256 algo

rsa-sha2-256 ل rsa-sha2-256 نيوكت

rsa-sha2-512 algo rsa-sha2-512 نيوكت

SSH-rsa algo نيوكت



SSH لةبسنلاب اذه :ةظحالم

نيوكتلل ةلباقلا SSHD HostKey ةيمزراوخ

SSH. مداخة قداصل SSHd فيضم حاتفم نيوكتل

رمألا : ASC-ise33p4/admin(config)# service sshd host-key ؟

لمتحملا لامكإلا :

حاتفم SSH ecdsa 256 فيضم نيوكت host-ecdsa-256

حاتفم SSH ed25519 فيضم نيوكت host-ed25519

SSH فيضم rsa حاتفم نيوكت host-rsa

SSH. مداخة قداصل SSH فيضم حاتفم ةيمزراوخ نيوكتل

رمال: ASC-ise33p4/admin(config)#service sshd host-key-algorithm ؟

لحتحمل الامكال:

ecdsa-sha2-nistp256 نيوكت ecdsa-sha2-nistp256 algo

rsa-sha2-256 ل rsa-sha2-256 algo نيوكت

rsa-sha2-512 algo rsa-sha2-512 نيوكت

SSH-ed25519 تلكش ssh-ed25519 algo

SSH. مداخل قداصل SSHd MAC ةمزرارخ نيوكتل

رمال: ASC-ise33p4/admin(config)#service SSHD mac-algorithm ؟

لحتحمل الامكال:

hmac-sha1 تلكش hmac-sha1 algo

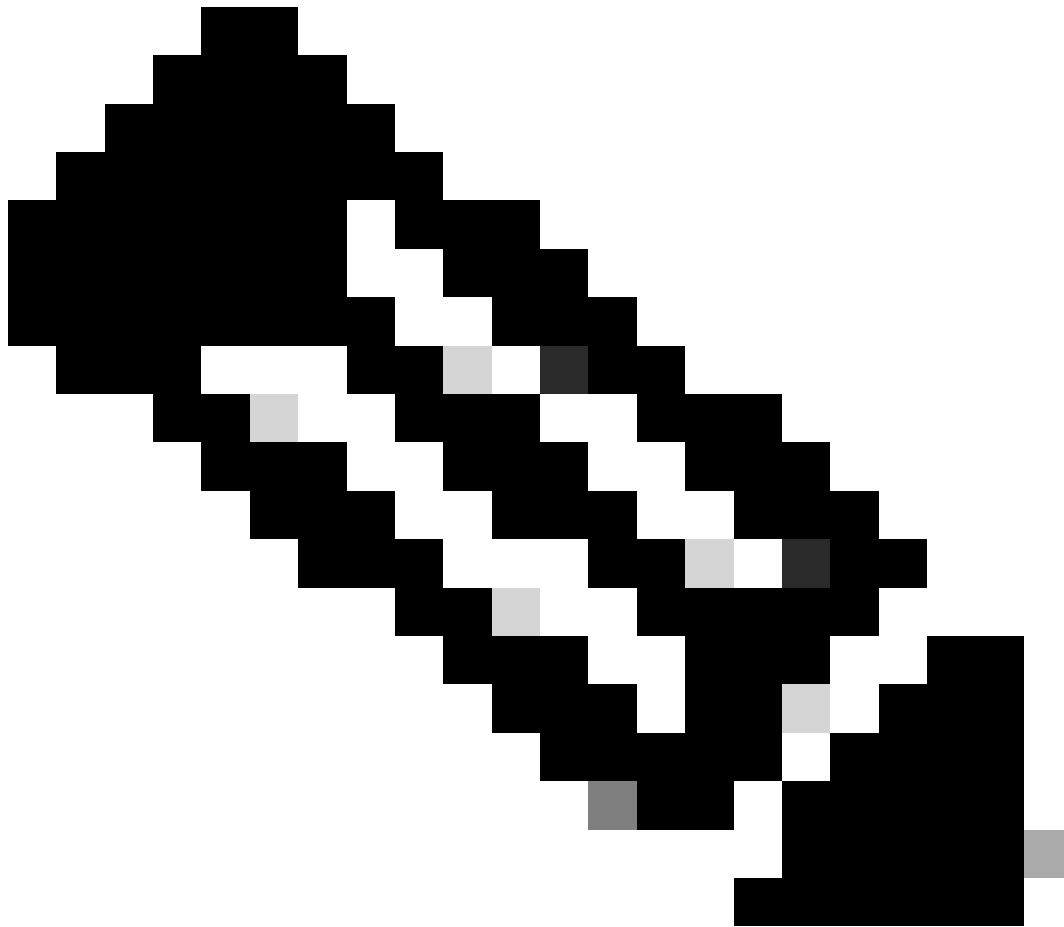
hmac-sha1-etm-openssh.com تلكش hmac-sha1-etm-openssh.com algo

hmac-sha2-256 نيوكت hmac-sha2-256 algo

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

hmac-sha2-512 تلكش hmac-sha2-512 algo

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



SSHd لجأ نم اذه :ةظحالم

اهحالصإو عاطخأل فاشكُتسا

ةحصلال نم ققحتلا

(SSH): نمآال لقنلا لوكوتورب

```
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
```

د.ش.س:

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

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

ةمدخل لا مديكمت

```
service sshd encryption-algorithm128-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
```

لجسلا ةصا صق:

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

```
2025-03-18 08:35:25.241 [تامولعم] service_conf.py update_host_key_algorithms line:575
```

حاجنب ةثدحملا SSH فيضم حيتافم تايمزراوخ

```
2025-03-18 08:35:39.056 [تامولعم] service_conf.py update_host_key_algorithms line:567
```

ةثدحملا SSH فيضم: ecdsa-sha2-nistp256

```
2025-03-18 08:35:39.260 [INFO] service_conf.py restart_sshd line:259 SSHd ليغشت ةداعإ تمت
```

```
2025-03-18 08:48:20.194 [تامولعم] service_conf.py update_host_key_algorithms line:567
```

ةثدحملا SSH فيضم: ecdsa-sha2-nistp256

```
2025-03-18 08:48:20.396 [INFO] service_conf.py restart_sshd line:259 SSHd ليغشت ةداعإ تمت
```

```
2025-03-18 08:48:20.400 [تامولعم] service_conf.py update_host_key_algorithms line:575
```

حاجنب ةثدحملا SSH فيضم حيتافم تايمزراوخ

```
2025-03-18 08:49:00.442 [تامولعم] service_conf.py update_host_key_algorithms line:567
```

ةثدحملا SSH فيضم: ecdsa-sha2-nistp256

```
2025-03-18 08:49:00.672 [INFO] service_conf.py restart_sshd line:259 SSHd ليغشت ةداعإ تمت
```

```
2025-03-18 08:49:00.674 [تامولعم] service_conf.py update_host_key_algorithms line:575
```

حاجنب ةثدحملا SSH فيضم حيتافم تايمزراوخ

ةعئاشلا ةلئسالا

ISE؟ لىل ةنكمملا ةيضارتفالا SSH فيضم حيتافم ةيمزراوخ يه ام :لاؤس

ي:لي امك يهو :ةباجالا

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

ةيضارتفالا SSHd MAC حيتافم ةيمزراوخ يه ام :لاؤس

ي:لي امك يهو :ةباجالا

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

فيضارت فالال SSH فيضم محتات فم وه ام :لاؤس

host-rsa :ةباجإلا

فيضارت فالال SSH فيضم محتات فم وه ام :لاؤس

يولي امك يهو :ةباجإلا

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

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م چ ر ت م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل ا و ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م چ ر ت ل ض ف ا ن ا ة ط ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب Cisco ي ل خ ت . ف ر ت ح م م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا ع م ل ا ح ل ا و ه ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا