Command Line Interface （ CLI ）にログイン するときこの資料に私用 セキュア シェル（ SSH ）キーを生成し Cisco E メール セキュリティ アプライアンス（ ESA ）でユーザ名および認証のためにそれを記述されています使用する方法を。

パスワードなしで ESA にログオンのための SSH 公開キー 認証の設定方法

公開鍵 認証（ PKI ）は生成された公共/私用 keypair に頼る認証方式です。 非常に有用なプロパティがある PKI を使うと、特別な「キー」は生成されます: キーの公共半分を読むことができるだれでもキーの私用半分にアクセスできる人によってしか読むことができない有能な暗号化 データです。 このように、キーの公共半分にアクセスできることはまた私用半分の機密情報をだれでもに送信 し、人は私用半分に実際アクセスできることを確認することを可能にします。 この手法がどのように認証するのに使用できるか見ることは容易です。

ユーザとして、keypair を生成し、次に ESA のようなリモート システムにキーの公共半分を、置くことができます。 そのリモート システムは keypair の私用半分にアクセスできることをユーザ ID を認証それからでき示します持っていることによってちょうど口グインすることを可能にします。 これは SSH の中のプロトコル レベルでされ、自動的に起こります。

それはが、プライベートキーのプライバシーを保護する必要があることを、意味して下さい。 ルートを持っていない共用システムでこれはパスワードに同様に機能するパスフレーズのプライベートキーの暗号化によって達成することができます。 公開キー 認証を行うために SSH がプライベートキーを読むことができる前にプライベートキーが復号化することができるようにパスフレーズを供給するように頼まれます。 より多くのセキュアなシステムで（唯一のユーザであるマシン、または他人は物理アクセスをアクセスできないホームのマシンのように）コンピュータで非暗号化プライベートキーを作成することによって（パスフレーズ無しで）またはパスフレーズを一度入力し、時間の間にメモリでキーをキャッシュすることによってこのプロセスを簡素化できます。 OpenSSH はこのプロセスを簡素化する ssh エージェントと呼ばれるツールが含まれています。

Linux/Unix 用の ssh-keygen 例

パスワードなしで ESA に接続するべき Linux/UNIXワークステーション（またはサーバを）設定するために次のステップを完了して下さい。 この例では、パスフレーズとして規定 しません。

1) ワークステーション（かサーバで）、Unix コマンド **ssh-keygen** を使用してプライベートキーを生成して下さい:

```
$ ssh-keygen -b 2048 -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/[USERID]/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/[USERID]/.ssh/id_rsa.
Your public key has been saved in /home/[USERID]/.ssh/id_rsa.pub.
The key fingerprint is:
00:11:22:77:f6:a9:1e:19:f0:ca:28:9c:ff:00:11:22 [USERID]@hostname.com
```

```
The key's randomart image is:
+--[ RSA 2048]----+
| +... +|
| o= o+|
| o o ..|
| . ..o . + |
| . ES. o + |
| o + . . |
| o . . |
| o o |
| . . |
+-----------------+
```

（上記の *the は Ubuntu から 14.04.1）生成されました

2）公開キー ファイル（id_rsa.pub）を作成し、#1 でコピーします出力を開いて下さい:

```
$ cat .ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDJg9W3DeGf83m+E/PLGzUFPalSoJz5F
t54Wl2wUS36NLxm4IO4Xfrrb5bA97I+ZA4YcB1l/HsFLZcoljAK4uBbmpY5kXg96A6Wf
mIYMnl+nV2vrhrODgbcicEAdMcQN3wWHXiEWacV+6u+FlHlonkSAIDEug6vfnd+bsbcP
Zz2uYnx1llxbVtGftbWVssBK3LkFp9f0GwDiYs7LsXvQbTkixrECXqeSrr+NLzhU5hf6
eb9Kn8xjytf+eFbYAslam/NEfl9i4rjide1ebWN+LnkdcE5eQ0ZsecBidXv0KNf45RJa
KgzF7joke9niLfpf2sgCTiFxg+qZ0rQludntknw [USERID]@hostname.com
```

3) アプライアンスにログインし、#1 で作成した設定し、変更を**保存して下さい**パブリック SSH キーを使用してワークステーション（かサーバを）認識するために ESA を。 ログオンの間にパスワードプロンプトに注意して下さい:

```
$ ssh admin@192.168.0.199
******************************
CONNECTING to myesa.local
Please stand by...
******************************

Password:[PASSWORD]
Last login: Mon Aug 18 14:11:40 2014 from 192.168.0.200
Copyright (c) 2001-2013, Cisco Systems, Inc.


AsyncOS 8.5.6 for Cisco C100V build 074

Welcome to the Cisco C100V Email Security Virtual Appliance

myesa.local> sshconfig

Currently installed keys for admin:

Choose the operation you want to perform:
- NEW - Add a new key.
- USER - Switch to a different user to edit.
[]> new

Please enter the public SSH key for authorization.
```

```
Press enter on a blank line to finish.
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDJg9W3DeGf83m+E/PLGzUFPalSoJz5F
t54Wl2wUS36NLxm4IO4Xfrrb5bA97I+ZA4YcB1l/HsFLZcoljAK4uBbmpY5kXg96A6Wf
mIYMnl+nV2vrhrODgbcicEAdMcQN3wWHXiEWacV+6u+FlHlonkSAIDEug6vfnd+bsbcP
Zz2uYnx1llxbVtGftbWVssBK3LkFp9f0GwDiYs7LsXvQbTkixrECXqeSrr+NLzhU5hf6
eb9Kn8xjytf+eFbYAslam/NEfl9i4rjide1ebWN+LnkdcE5eQ0ZsecBidXv0KNf45RJa
KgzF7joke9niLfpf2sgCTiFxg+qZ0rQludntknw [USERID]@hostname.com

Currently installed keys for admin:
1. ssh-rsa AAAAB3NzaC1yc2EAA...rQludntknw ([USERID]@hostname.com)

Choose the operation you want to perform:
- NEW - Add a new key.
- DELETE - Remove a key.
- PRINT - Display a key.
- USER - Switch to a different user to edit.
[]>

myesa.local> commit
```

4) アプライアンスおよび再ログインから終了して下さい。 パスワードプロンプトが取除かれ、アクセスが直接認められることを注意して下さい:

```
myesa.local> exit

Connection to 192.168.0.199 closed.
robert@ubuntu:~$ ssh admin@192.168.0.199
******************************
CONNECTING to myesa.local
Please stand by...
******************************

Last login: Mon Aug 18 14:14:50 2014 from 192.168.0.200
Copyright (c) 2001-2013, Cisco Systems, Inc.


AsyncOS 8.5.6 for Cisco C100V build 074

Welcome to the Cisco C100V Email Security Virtual Appliance
myesa.local>
```

Windows のための ssh-keygen 例

パスワードなしで ESA に接続するべき Windows ワークステーション (かサーバを) 設定するために次のステップを完了して下さい。 この例では、パスフレーズとして規定 しません。

> **注**Windows から使用されるコンソール アプリケーションに変化があります。 コンソール アプリケーションのための推奨をはたらかせるソリューションを研究し、見つける必要があります。 この例は PuTTy および PuTTyGen を使用します。

1) PuttyGen を開いて下さい。

2) 生成するべきキーの型に関しては SSH-2 RSA を選択して下さい。

3) **Generate ボタンを**クリックして下さい。

4) 経過表示バーの下でエリアのマウスを移動して下さい。 経過表示バーが完全なとき、PuTTYgen はキーペアを作成します。

5) キー パスフレーズ フィールドのパスフレーズを入力して下さい。 確認パスフレーズ フィールドの同じパスフレーズを入力して下さい。 パスフレーズなしでキーを

6) プライベートキーを保存するために **Save private key ボタンを**クリックして下さい。

注プライベートキーを保存して下さい。 それがマシンに接続することを必要とします。

7) OpenSSH authorized_keys に分類されるテキスト フィールドでファイルを貼り付けるための公開キーと右クリックし、『Select All』 を選択 して下さい。

8) 同じテキスト フィールドで再度右クリックし、『Copy』 を選択 して下さい。

9) PuTTy を使用する、

```
login as: admin
Using keyboard-interactive authentication.
Password: [PASSWORD]
Last login: Mon Aug 18 11:46:17 2014 from 192.168.0.201
Copyright (c) 2001-2013, Cisco Systems, Inc.


AsyncOS 8.5.6 for Cisco C100V build 074

Welcome to the Cisco C100V Email Security Virtual Appliance
myesa.local> sshconfig

Currently installed keys for admin:

Choose the operation you want to perform:
- NEW - Add a new key.
- USER - Switch to a different user to edit.
[]> new

Please enter the public SSH key for authorization.
Press enter on a blank line to finish.
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEAj6ReI+gqLU3W1uQAMUG0620B+tpdkjkgBn
5NfYc+qrtyB93stG38O1T4s0zHnhuKJLTdwBg/JHdFuNO77BY+21GYGS27dMp3UT9/VuQ
TjP8DmWKOa+8Mpc9ePdCBZp1C4ct9oroidUT3V3Fbl5M9rL8q4/gonSi+7iFc9uOaqgDM
/h+RxhYeFdJLechMY5nN0adViFloKGmV1tz3K9t0p+jEW5l9TJf+fl5X6yxpBBDoNcaB9
jNwQ5v7vcIZBv+fl98OcXD9SNt08G0XaefyD2VuphtNA5EHwx+f6eeA8ftlmO+PgtqnAs
c2T+i3BAdC73xwML+1IG82zY51pudntknw rsa-key-20140818

Currently installed keys for admin:
1. ssh-rsa AAAAB3NzaC1yc2EAA...51pudntknw (rsa-key-20140818)

Choose the operation you want to perform:
- NEW - Add a new key.
```

```
- DELETE - Remove a key.
- PRINT - Display a key.
- USER - Switch to a different user to edit.
[]>

myesa.local> commit
```

10) ESA のための PuTTy コンフィギュレーションウィンドウおよび既存保存されたセッションから、**> SSH >** *認証* フィールドのための*プライベートキーファイル*の **Auth** および、『Browse』 をクリック し、見つけますステップ #6 からの保存されたプライベートキーを『Connection』 を選択 して下さい。

11) PuTTy のセッション (プロファイル) を保存し、『Open』 をクリック して下さい。 前もって構成されたセッションから既に保存されないか、または規定 されて ユーザ名と口グインして下さい。 口グオンした場合「公開キー「との認証の包含に[保存されたプライベートキーのファイル名]」注意して下さい:

```
login as: admin
Using keyboard-interactive authentication.
Password: [PASSWORD]
Last login: Mon Aug 18 11:46:17 2014 from 192.168.0.201
Copyright (c) 2001-2013, Cisco Systems, Inc.


AsyncOS 8.5.6 for Cisco C100V build 074

Welcome to the Cisco C100V Email Security Virtual Appliance
myesa.local> sshconfig

Currently installed keys for admin:

Choose the operation you want to perform:
- NEW - Add a new key.
- USER - Switch to a different user to edit.
[]> new

Please enter the public SSH key for authorization.
Press enter on a blank line to finish.
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEAj6ReI+gqLU3W1uQAMUG0620B+tpdkjkgBn
5NfYc+qrtyB93stG38O1T4s0zHnhuKJLTdwBg/JHdFuNO77BY+21GYGS27dMp3UT9/VuQ
TjP8DmWKOa+8Mpc9ePdCBZp1C4ct9oroidUT3V3Fbl5M9rL8q4/gonSi+7iFc9uOaqgDM
/h+RxhYeFdJLechMY5nN0adViFloKGmV1tz3K9t0p+jEW5l9TJf+fl5X6yxpBBDoNcaB9
jNwQ5v7vcIZBv+fl98OcXD9SNt08G0XaefyD2VuphtNA5EHwx+f6eeA8ftlmO+PgtqnAs
c2T+i3BAdC73xwML+1IG82zY51pudntknw rsa-key-20140818

Currently installed keys for admin:
1. ssh-rsa AAAAB3NzaC1yc2EAA...51pudntknw (rsa-key-20140818)

Choose the operation you want to perform:
- NEW - Add a new key.
- DELETE - Remove a key.
- PRINT - Display a key.
- USER - Switch to a different user to edit.
```

```
[]>

myesa.local> commit
```

関連情報

- Cisco 電子メール セキュリティ アプライアンス - エンド ユーザ ガイド
- テクニカルサポートとドキュメント - Cisco Systems