公開鍵認証を使用した Nutanix クラスタへの SSH アクセス

2024 年 4 月版

SSH および公開鍵認証について

Nutanix クラスタの CVM や Prism Central の仮想マシン(PCVM)等に対する一部複雑な操作の実施や問題調査、問題対応の際には、SSH (Secure SHell)と呼ばれる、通信を暗号化することで盗聴の危険性をなくした安全なコマンドラインでの遠隔操作が利用されます。この SSH でのアクセスでは nutanix ユーザ(あるいは admin ユーザ)に対するパスワードによる認証が一般的に使用されております。
より安全なシステムの運用のため、パスワードによる認証よりも安全性の高い公開鍵認証による認証が推奨されます。公開鍵認証を有効にした上でパスワードでの認証をオフにすることによりパスワード類推攻撃や総当たり攻撃といったパスワードを標的とした攻撃が無効化され、より安全性が高まります。

この文書では、日本国内での事情を鑑み、Windows にてよく利用されている SSH や SFTP の方法での、公開鍵認証でのアクセス方法、そのために必要な SSH での公開鍵の作成方法についてを説明します。
Windows における SSH の公開鍵の作成方法と、公開鍵を利用したアクセス方法について説明します。

具体的には、**1.Windows 標準の OpenSSH の利用**にて、Windows10(1809 以降)や Windows Server 2019, 2022 に標準で付属している OpenSSH を使用した CVM への SSH のアクセスについて説明します。この方法はあまり使われていないと思いますが、Windows に標準で存在しサードパーティー製のアプリケーションを追加で導入する必要がないという利点があります。

続く **2. Tera Term** では、国内で利用事例が非常に多い Tera Term を使用した公開鍵認証でのアクセス方法を説明します。また、同じく利用事例の多い SFTP ソフトウェアであります WinSCP での公開鍵認証でのアクセスについてを **3. WinSCP** にて説明します。
この 3 つの章については**いずれの章も独立しているため必要な部分だけをご参照**頂いて構いません。

最後に、**4.Pagent** にて Pagent とよばれるエージェントを利用した WinSCP および Tera Term での都度のパスフレーズ入力を省略したアクセスについてを説明します。Pagent の利用はオプションであり、これを実施する必要はありませんが、実施する事でログインの際のつどのパスフレーズの入力を省略、利便性を高めることができます。ご参考になれば幸いです。

なお、Tera Term と並んで利用頻度の高い PuTTY での公開鍵認証については以下弊社 KB-1895 の **How to set up password-less SSH from Windows(using PuTTY)**の項目をご確認ください。
https://portal.nutanix.com/kb/1895

1. Windows 標準の OpenSSH の利用

Windows 10 以降の Windows クライアント、Windows Server 2016 以降の Windows Server では SSH のオープンソースの実装である OpenSSH が標準で用意されており、オプションにてインストールを選択できます。
ご利用の環境に OpenSSH クライアントが導入されているかは、「設定」アプリケーションのアプリと機能のオプション機能の管理にて確認頂けます

もしオプション機能に OpenSSH クライアントの記載がなく、まだインストールがされていない場合は「＋機能の追加」をご選択いただくことで追加でインストールも可能です。

もう一つの OpenSSH ～ Windows Subsystem for Linux での OpenSSH

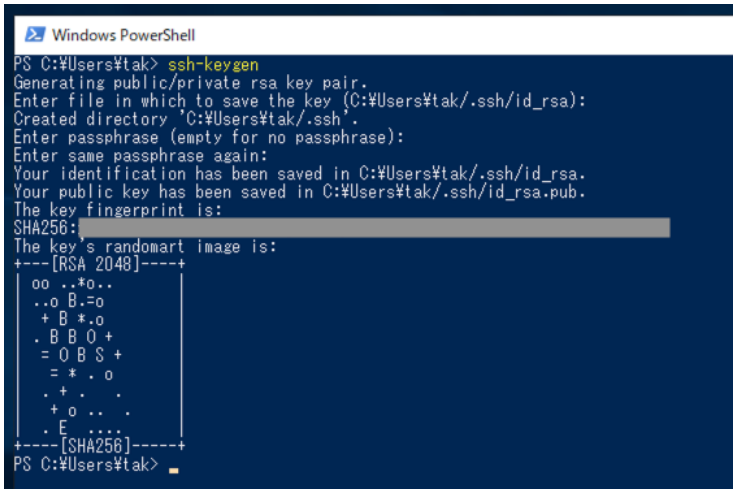
Windows, Windows Server には Windows Subsystem for Linux(WSL)という追加コンポーネントがあり、Windows 上で Linux のソフトウェアを共存してご利用頂けます。なお、WSL には NTKernel 上のサブシステムだった WSL1 と、仮想化を利用し Linux カーネルそのものを動作させる WSL2 があり、現在は WSL2 が一般的に利用されております。

この WSL2 の上の Linux では Linux で利用されている OpenSSH がご利用頂けます。
ただし、本ドキュメントでは WSL2 上での OpenSSH については取り扱いません。

1.1. ssh-keygen による鍵生成

OpenSSH クライアントが導入されている Windows には、ssh-keygen.exe と呼ばれる SSH での公開鍵作成コマンドが用意されております。ssh-keygen による公開鍵の作成は以下になります[1]。

```
ssh-keygen
```

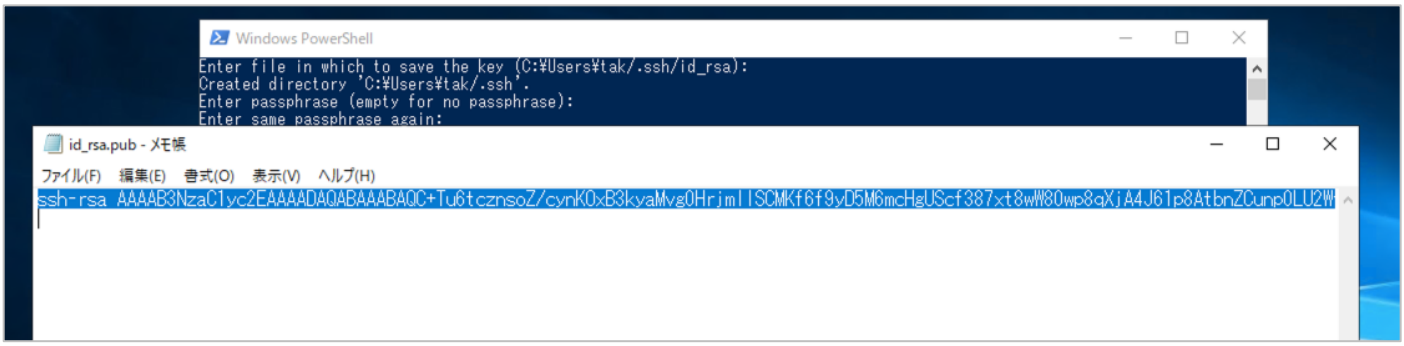


実行すると公開鍵と秘密鍵の保存先を聞かれますので、これは単にリターンを押しデフォルトのパスのファイルに保存します。なお、デフォルトではこの作成された鍵はユーザのホームディレクトリの下の .ssh フォルダの下に、以下のファイル名で作成されます[2]。

秘密鍵: %HOMEPATH%¥id_rsa

公開鍵: %HOMEPATH%¥id_rsa.pub

その後、パスフレーズを入力します。このパスフレーズは秘密鍵にアクセスするときに必要となります。公開鍵認証では秘密鍵と公開鍵の 2 つをセットで扱い、公開鍵はその名の通り人に見られても問題がない情報で、リモートサイトなどに登録される鍵、秘密鍵は他人に見られないように管理するべき鍵となります。このうち公開鍵である id_rsa.pub をテキストエディタで開き、その内容を「**1 行で**」**コピー**します。(余計な改行が入らないよう気をつけてください)

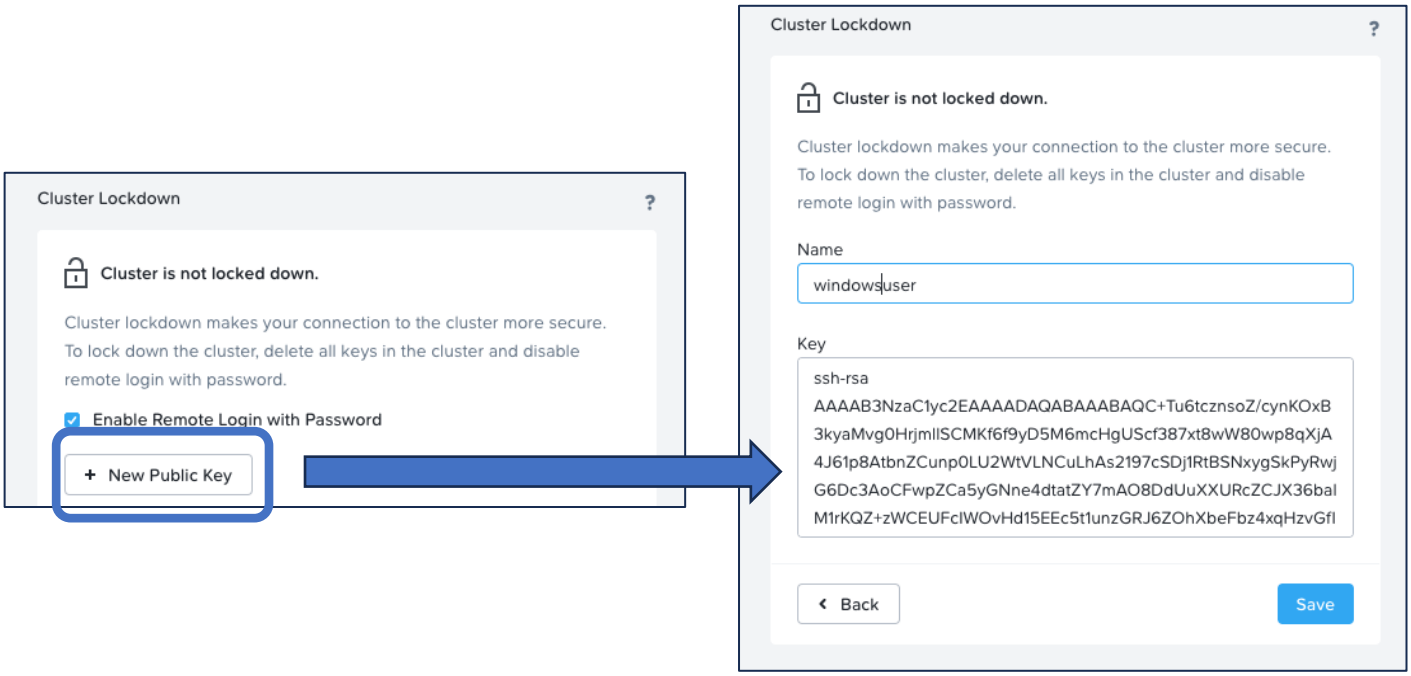


---

[1] CVM の SSH サーバでは ed21159 の暗号形式はサポートされておりません。利用する暗号化形式については rsa 形式が推奨となります。デフォルトでは 2048bit の鍵が生成されますが、より高い暗号化強度を希望される場合は、-b 4096 オプションを指定し 4096bit の鍵を生成してください

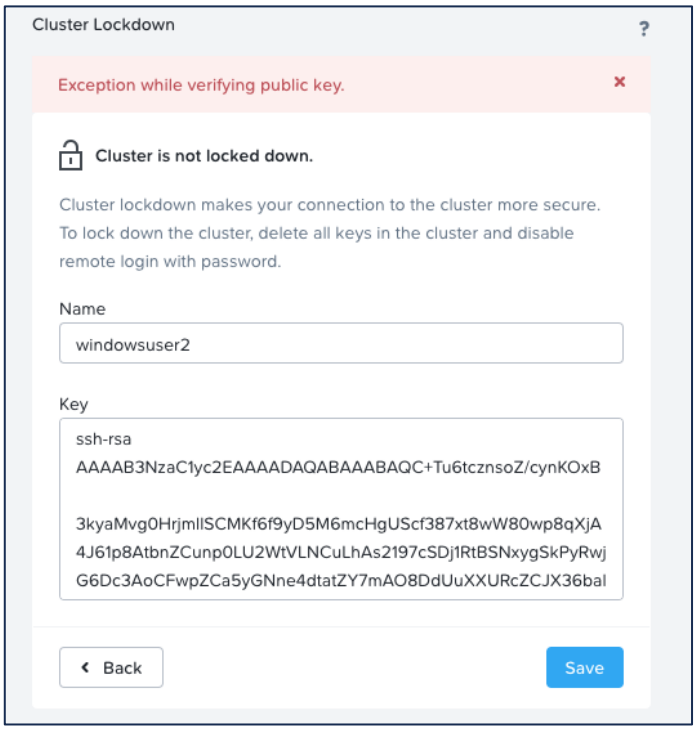
[2] ファイル名は id_<暗号方式>, id_<暗号方式>.pub になり、デフォルトの暗号化形式は rsa のためです。また、ssh-keygen の実行時にファイル名を記入し変更することもできます。

CVM へ公開鍵認証でアクセスする場合は、Prism にログイン、右上の歯車のマークをクリックして表示される Settings (設定)にある Cluster Lockdown のページにて公開鍵を登録します。



Name には任意の名称を、Key に先ほど 1 行でコピーした公開鍵をペーストします。

なお、1 行でペーストしていない、余計な改行が入っている場合は以下の様に **Exception whille verifying public key** のエラーが表示されます。



上記のエラーメッセージが出た場合は、Key に入力したテキストの途中に改行がないかご確認ください。

1.2. ssh コマンドでの接続

公開鍵が登録されたら、CVM への通信を試みます。

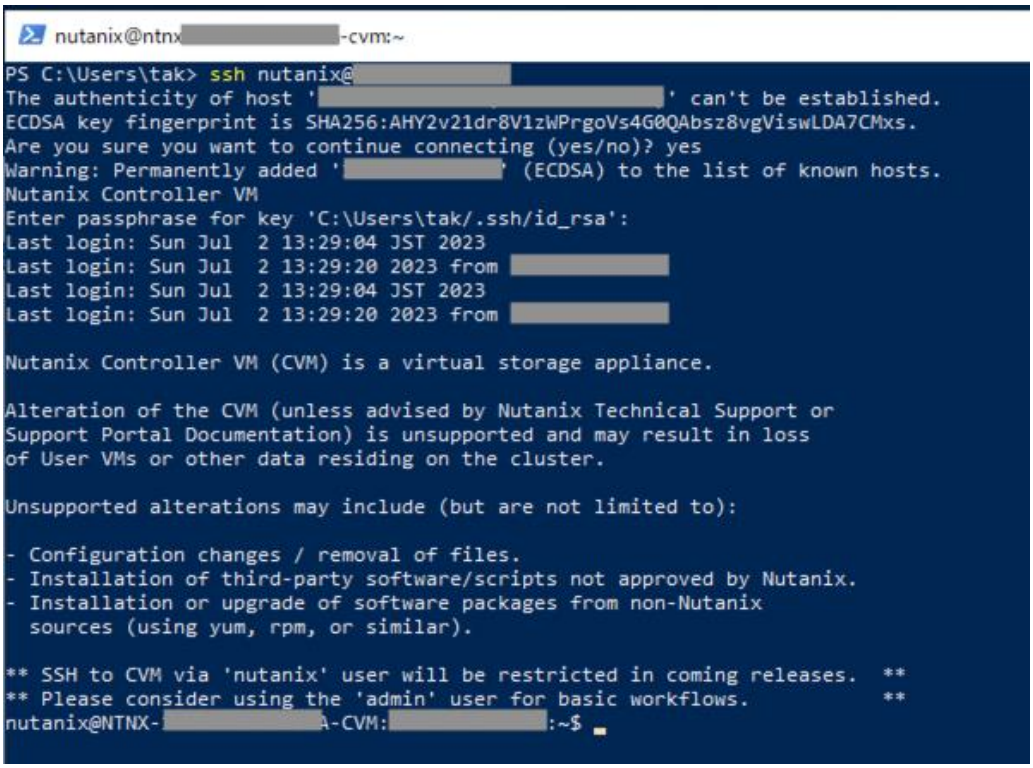
Windows のコマンドプロンプトウィンドウにて ssh コマンドを実行します。これはパスワードによる認証の場合も公開鍵認証の場合も変わりません。

```
ssh nutanix@<CVM IP>
```

その CVM への初回接続の場合、CVM のホスト側の証明書のフィンガープリントが表示され、確認が求められます。Yes を押して続けてください。

Prism にて公開鍵を登録していた場合、ssh コマンドと CVM の ssh サーバとの間でその情報がやりとりされ、公開鍵による認証が行われます。このときに、秘密鍵へのアクセスのため、ssh-keygen で設定したパスフレーズの入力が求めらます。[3]

また、ssh-agent を使用することで ssh コマンドでのパスフレーズの入力を省略できます。



CVM へのログインに成功すると、上図のようにサポートに関する注意書きが表示され、そのごコマンドを受け付けるプロンプトが表示されます。

---

[3] このパスフレーズは手元のマシンにある秘密鍵のアクセスのためだけにローカルで使用され、ネットワークへ流されることはありません

1.3. (オプション) ssh-agent

ssh コマンドでは手元にある秘密鍵へアクセスにするためつどパスフレーズを入力する必要があります。ssh-agent を利用する事でこの都度のパスフレーズの入力を省略できます。

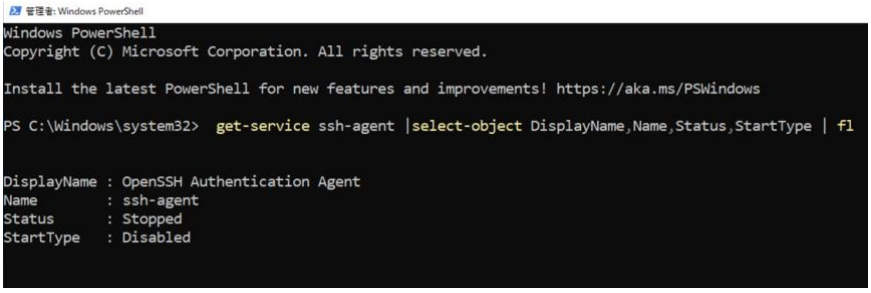
ssh-agent はバックグラウンドで動作するサービスで、ssh-add コマンドで追加された秘密鍵をメモリ上に保持、ssh コマンドと連携しつど秘密鍵のファイルへアクセスするのではなくメモリ上に存在する秘密鍵を利用する事でパスフレーズの入力を省略します。結果、SSH コマンドの利用時につどパスフレーズを入力する必要がなくなり、ローカルのコマンドの実行に近い利便性がえられます。これはパスワードでの認証にない利点になります。

ssh-agent を実行するには管理者権限が必要になります。メニューより Windows Power Shell(管理者)を選択、管理者権限での PowerShell を起動、以下コマンドを実行、現在の ssh-agent の状態を確認します[4]

```
Get-Service ssh-agent |select-object DisplayName,Name,Status,StartType | fl
```

Status が Stopped の場合起動していません。つど手動で起動するには以下のコマンドを使用します。

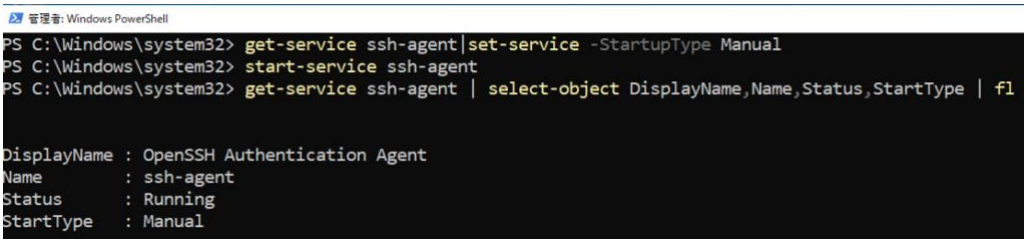
```
Get-Service ssh-agent | Set-Service -StartType Manual

Start-Service ssh-agent
```



また、Windows 起動時に自動起動させるには 1 行目を以下のコマンドにします。

```
Get-Service ssh-agent | Set-Service -StartType Automatic
```

再び Get-Service を使用して起動したかを確認します。



Status が Running になっていれば ssh-agent は起動しています。
ssh-agent が起動していれば管理者権限の PowerShell は閉じて構いません。

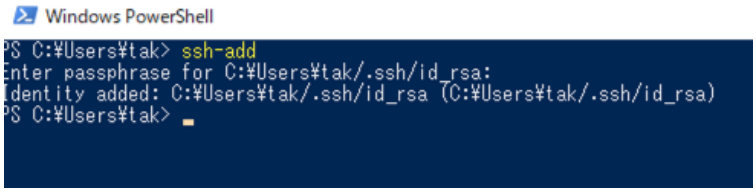
---

[4] コマンドの末尾の | fl は Format-List コマンドレットを通してリスト形式で表示させるためになります

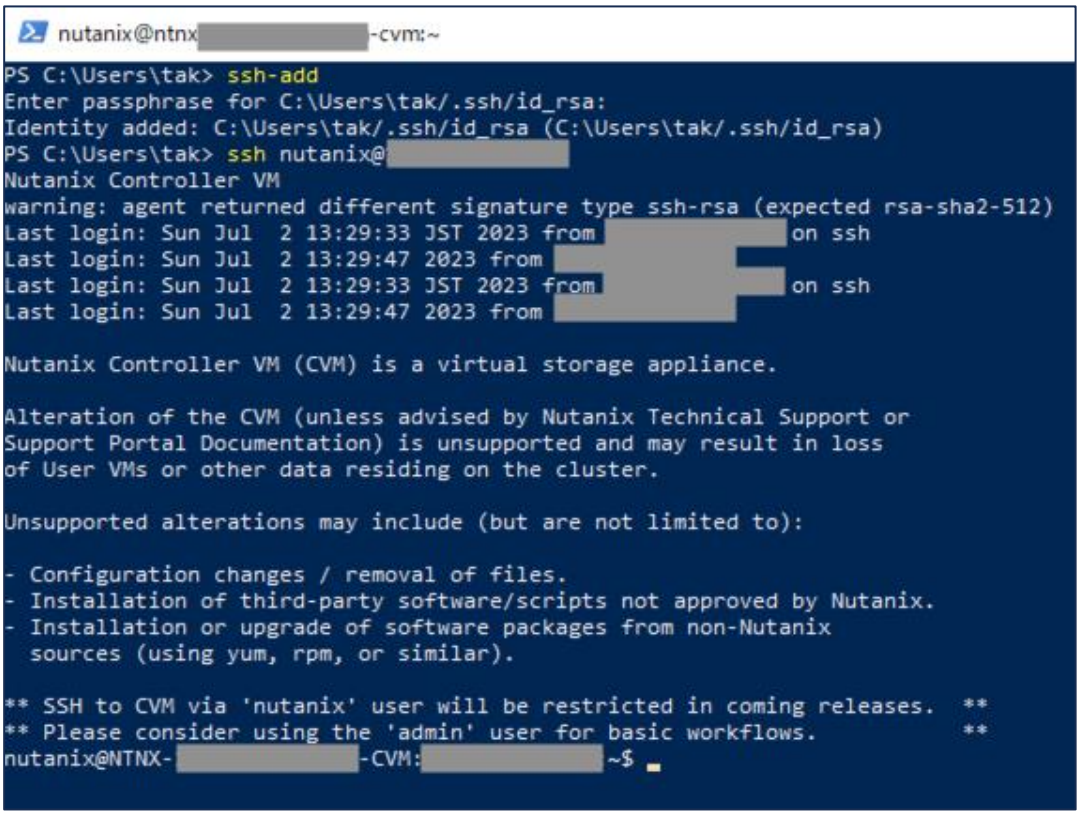
では、ssh-agent を利用した CVM へのログインを試みます。
通常の PowerShell を起動し、ssh-add コマンドで ssh-agent に秘密鍵を登録します。

```
ssh-add
```

ssh-add コマンドは引数に指定されたパスの秘密鍵を登録しますが、引数を指定しない場合はデフォルトの鍵[5]を登録します。



その後、ssh コマンドにて CVM へのログインを試みます。
すると、パスフレーズを聞かれることなくログインができます。

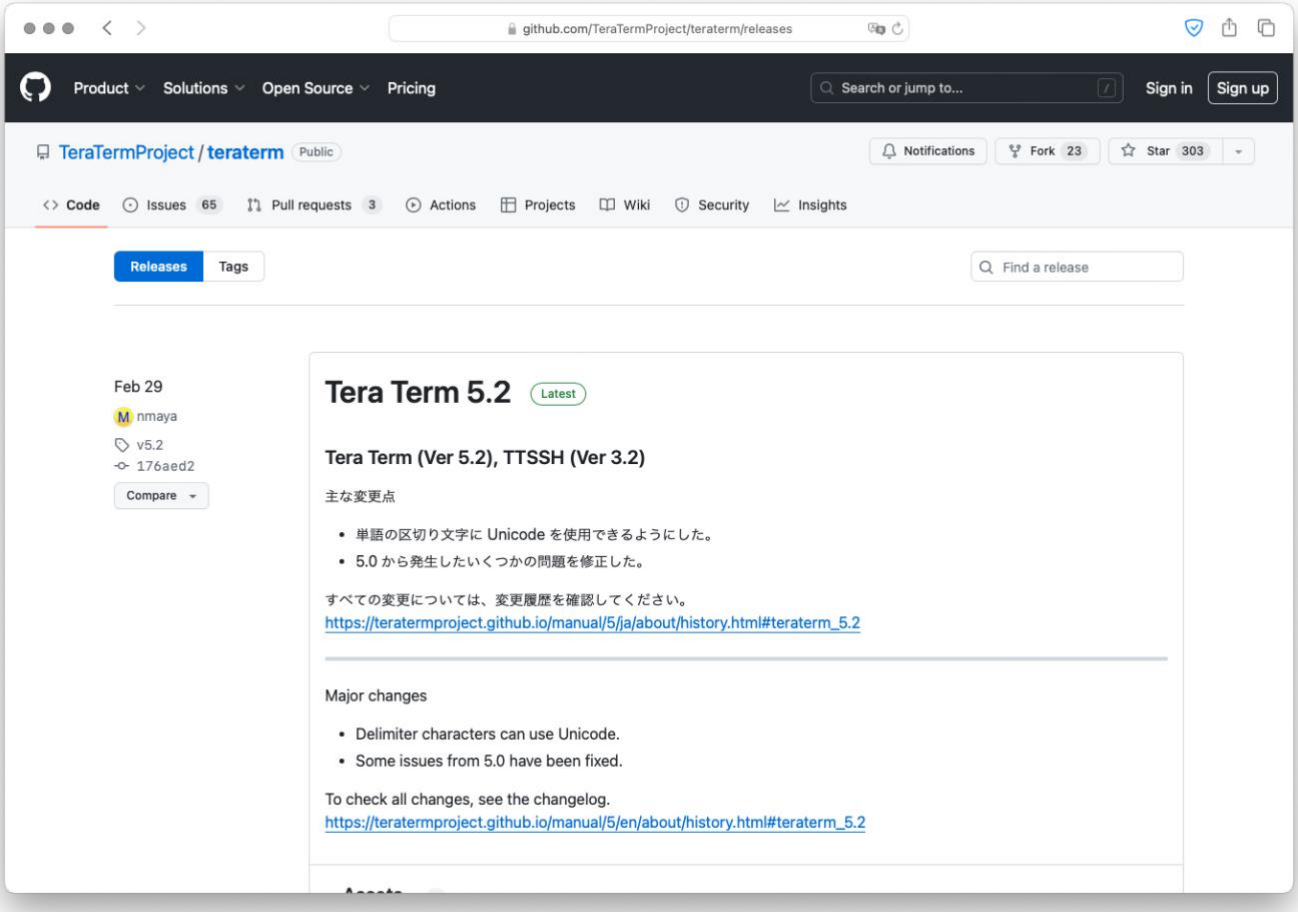


ssh-agent の利用は必須ではありませんが、CVM やその他に SSH でログインする機会が多い場合は繰り返しのパスフレーズの入力が省略でき、作業の効率化が図れます。

[5] ssh-add コマンドの動作としてはホームフォルダにある.ssh フォルダの下にある id_rsa,id_dsa,identity が対象になりますが、ここでは id_rsa しかないためこの鍵だけが登録されます。

2. Tera Term

Tera Term は Windows で動作する端末ソフトウェアで、古くはシリアル経由での接続に利用され、また telnet や SSH などのネットワーク越しでのリモートログインのプロトコルをサポートしており SSH での接続時によく利用されているソフトウェアになります[6]。



https://github.com/TeraTermProject/teraterm/releases

この章では Tera Term での公開鍵認証を用いた CVM への接続について説明します。

なお、Tera Term のダウンロードおよびインストール、基本的な操作についてはこのドキュメントでは取り扱いません。それらについては別途ドキュメントなどをご確認ください。

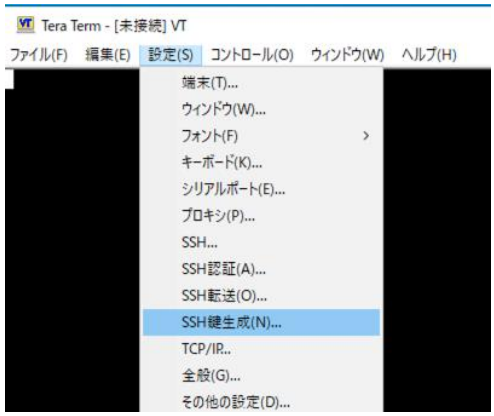
---

[6] 現在、Tera Term については GitHub にてソースコードおよびバイナリが配布されております。

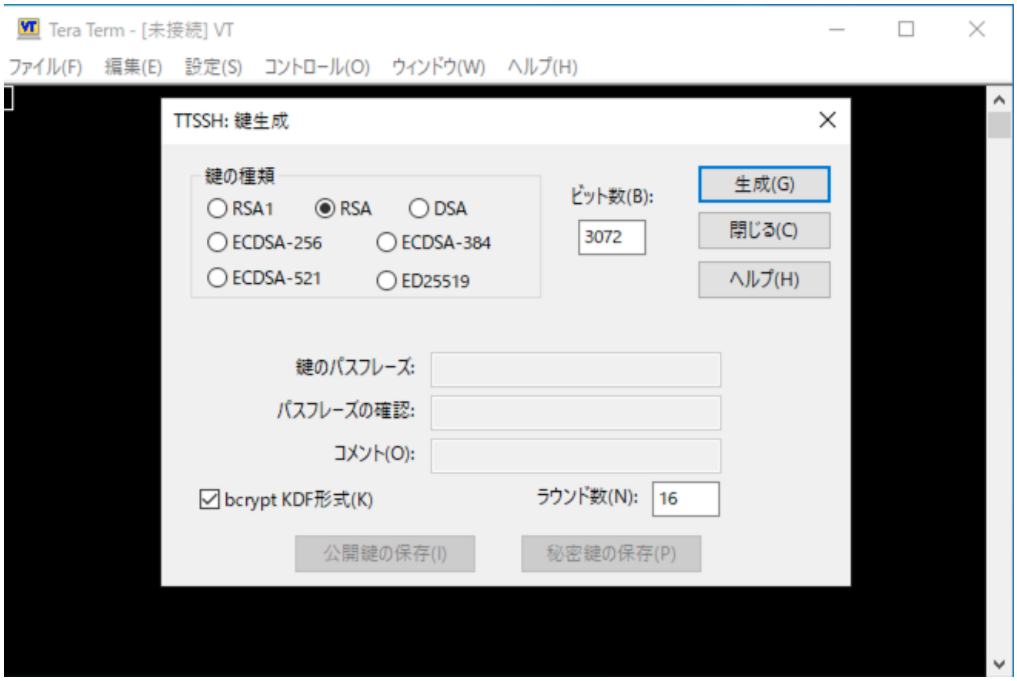
2.1. Tera Term での鍵生成

Tera Term では 1.1.ssh-keygen にて作成した秘密鍵と公開鍵のペアを利用する事ができます。また、Tera Term 自身が鍵生成の機能を有しており、自身で鍵を作成する事もできます[7]。

ここでは、Tera Term 自身での鍵生成を試します。
まず、Tera Term を起動、どこにも接続をしない状態で「設定」の「SSH 鍵生成」を選択します



TTSSH:鍵生成の画面にて、「鍵の種類」を RSA にして[8]「生成」ボタンを押します。



「生成」を押して少し待つと鍵が作成されます。

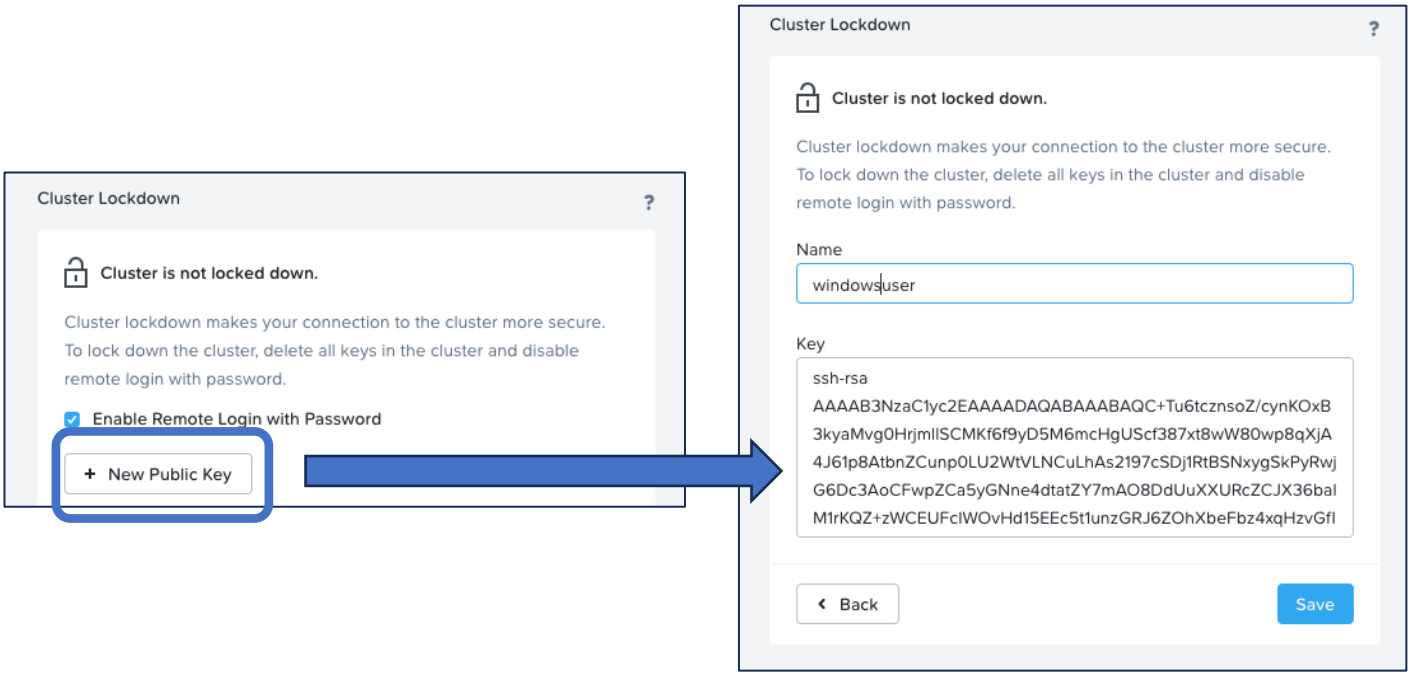
---

[7] なお、3.1.1.で説明します ppk 形式の秘密鍵についても利用が可能です。Tera Term と WinSCP を併用される場合は、WinSCP 側で ppk 形式の鍵を作って、TeraTerm でも読み込む方が楽な場合もあるかと存じます。

[8] RSA を指定すると「ビット数」の入力が可能になります。デフォルトでは 3072 ですが、これを 2048 にする、あるいは 4096 にしていただいても構いません。

鍵の作成が終わるとパスフレーズの入力が可能になるので適宜パスフレーズを入力、下の「公開鍵の保存」「秘密鍵の保存」ぼたんでそれぞれファイルを保存します。なお、デフォルトでは「ドキュメント」フォルダの下に id_rsa.pub (公開鍵), id_rsa(秘密鍵)のファイル[9]を作成します。

CVM へ公開鍵認証でアクセスする場合は、Prism にログイン、右上の歯車のマークをクリックして表示される Settings (設定)にある Cluster Lockdown のページにて公開鍵を登録します。



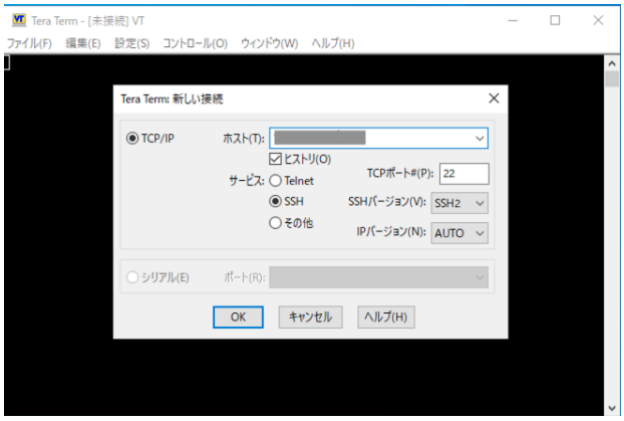
Name には任意の名称を、Key には id_rsa.pub の中のテキストを 1 行でペーストします[10]。

[9] 名前から分かるとおり、このファイルは ssh-keygen で作成したファイルと同じになります。

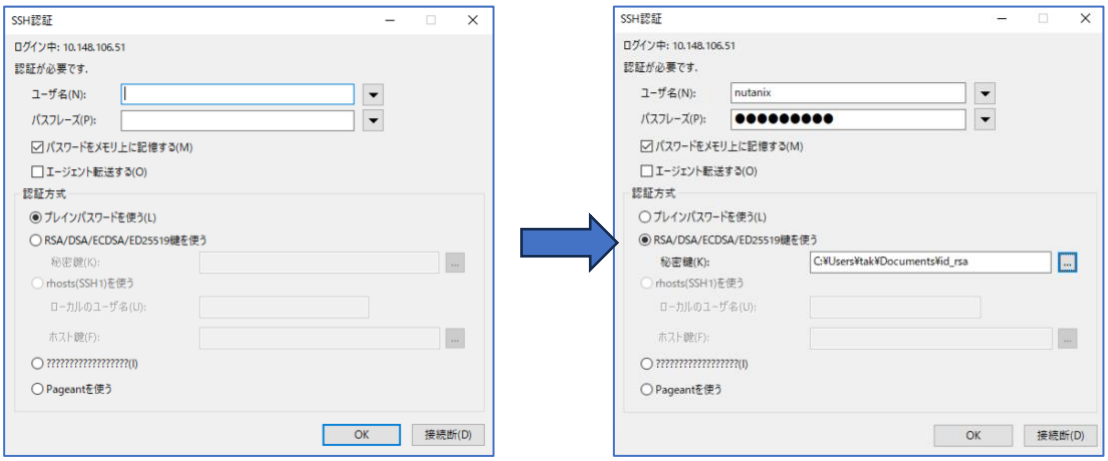
[10] この手順は 1.1. ssh-keygen での鍵生成と同じです。余計な改行を含まないなどの注意も同じになります。

2.2. Tera Term での接続

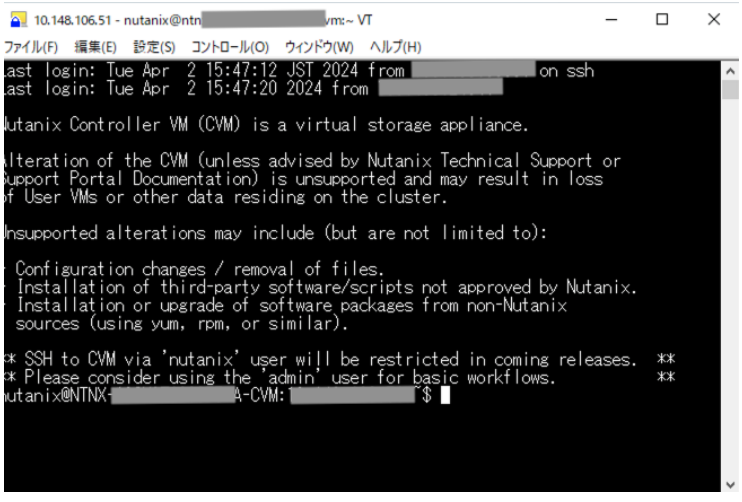
Tera Term を起動、あるいは起動している Tera Term の「ファイル」メニューから「新しい接続...」を選択、表示されたパネルに CVM の IP アドレスを記入、サービスが SSH になっているのを確認の上、OK を押し接続を行います。



SSH 認証というパネルが開きますので、まず「認証方式」にて RSA/DSA/ECDSA/DC25519 鍵を使う」を選択、その右側の「...」のボタンを押して作成した id_rsa ファイルを選択します[11]。その後、上の「パスフレーズ」に秘密鍵に設定したパスフレーズの入力、OK を押して接続を試みます。



接続に成功すると右図のように CVM のログイン時のメッセージがウィンドウに表示されプロンプトから CVM の操作が可能になります。



11 このとき ppk 形式の秘密鍵ファイルを読み込むこともできます。

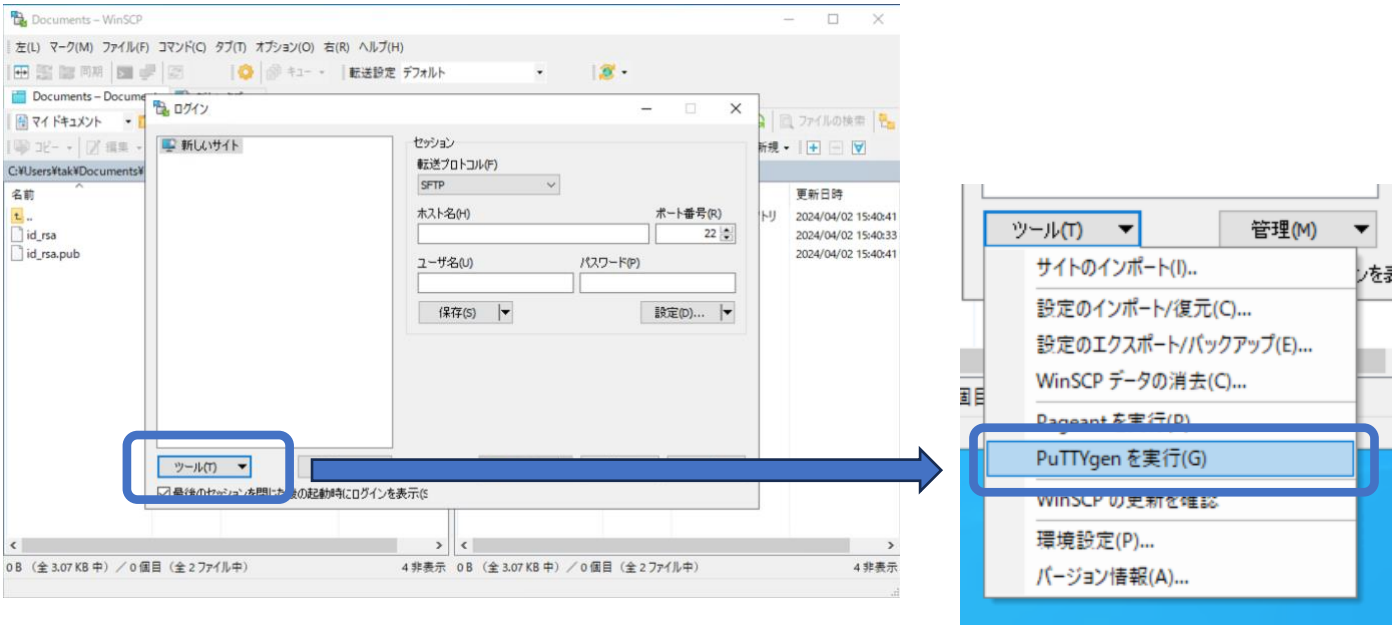
3. WinSCP

WinSCP は Windows で動作する SCP/SFTP のソフトウェアになります。CVM にて作成されたログのアーカイブファイルのダウンロードの際に WinSCP を使用し SFTP にて接続、ダウンロードを行うなどで利用されます。
WinSCP の使用する SCP/SFTP と言うプロトコルは、SSH をベースとし SSH により提供される暗号化された通信路を使用しファイルをコピー(SCP)、あるいはファイルの総受信(SFTP)を行うものになります。

ここでは、WinSCP にて公開鍵認証を用い CVM への接続する方法を説明します。

3.1.1. ppk 形式での鍵生成

Windows 標準の OpenSSH や TeraTerm と異なり、WinSCP では ppk とよばれるファイル形式[12]での公開鍵、秘密鍵を利用します。ここでは WinSCP での ppk 形式の鍵の生成を説明します。
まず WinSCP を起動、「ログイン」のパネルの下側にある「ツール」メニューから PuTTYgen を実行を選択します。



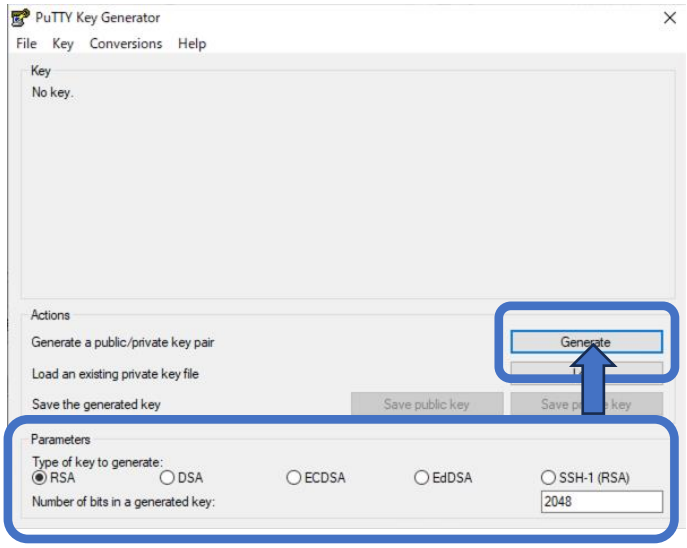
選択すると、PuTTY Key Generator というパネルが開きます(次ページ右上図)

[12] ppk は Putty Private Key の略で、PuTTY とよばれる SSH に対応した端末ソフトウェアで利用される鍵の形式になります。

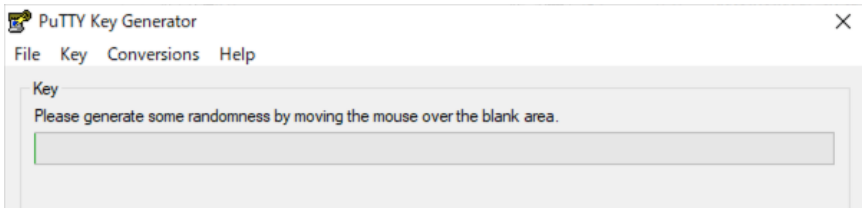
パネルの下の Parameters にて RSA が選択されているのを確認します。

また Number of bits in a generated key:が 2048 になっているを確認します。あるいは 4096 などより大きい数字を設定をおこないます。

その後、Generate のボタンを押します。



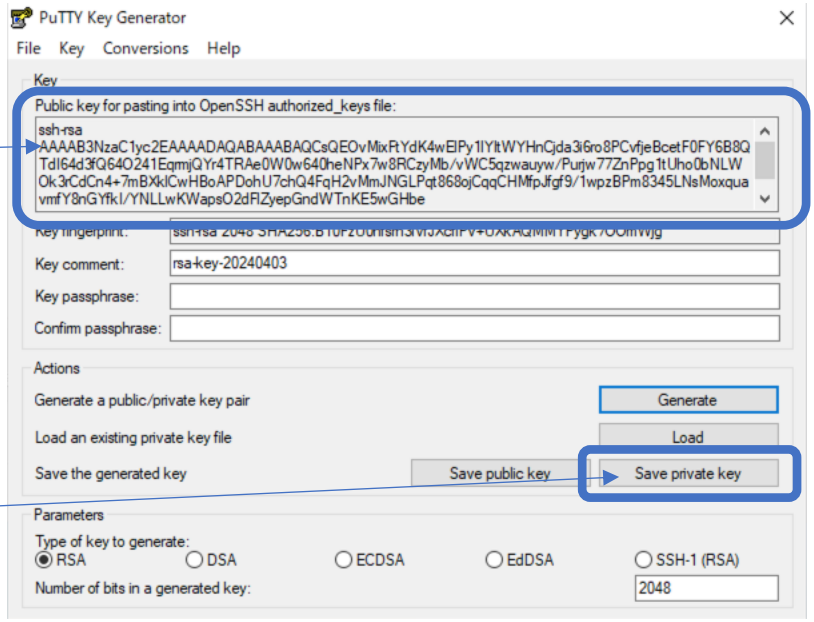
するとパネルの上部にプログレスバー(下図)が表示されますので**ここでマウスを適当に動かし続けます。**



プログレスバーの緑が右端まで到達しますと、鍵の生成が行われます。

鍵の生成が終わると右の図のように生成された鍵の情報が表示されます。
上は公開鍵のテキストのため、これをコピーしてテキストファイルに保存します[13]。
この公開鍵のテキストは次の手順で利用します。

下の Save private key のボタンを押すことで、公開鍵および秘密鍵がファイルに保存されます。



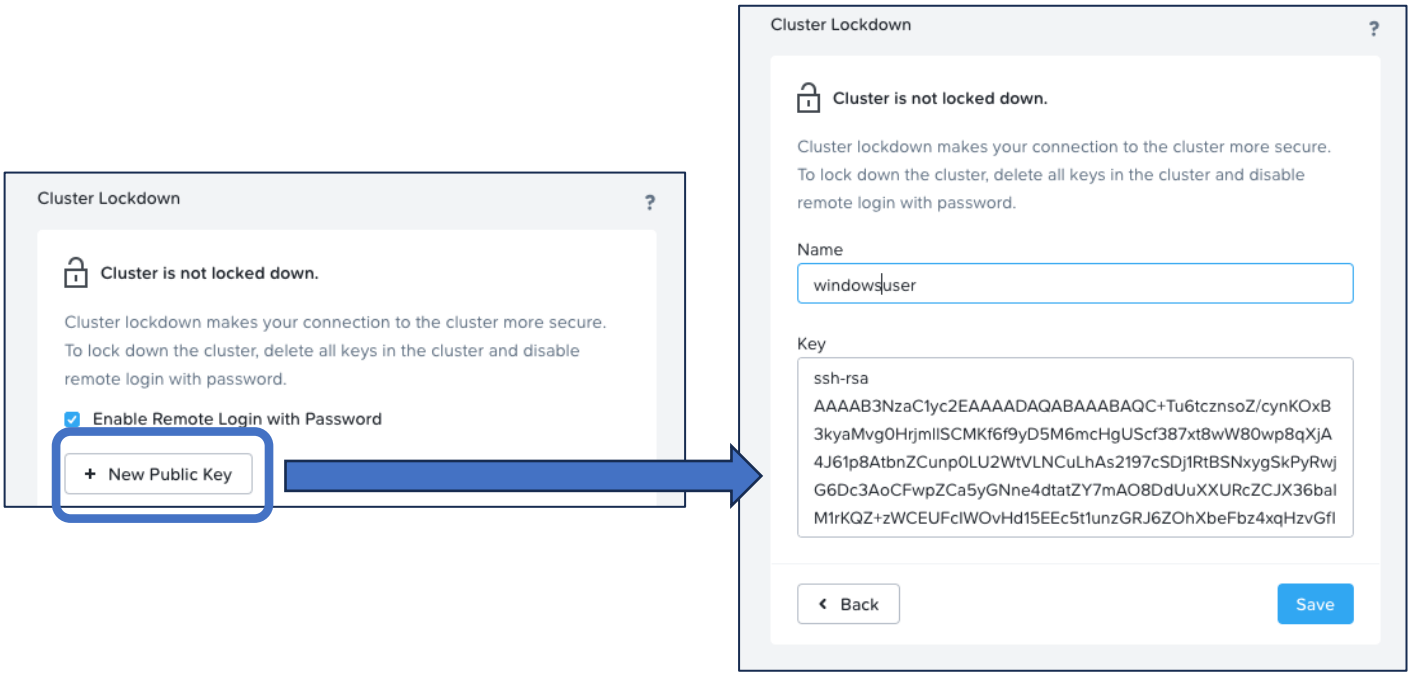
ただし **Save private key を押す前に上の Key passphrase と Comfirm passphrase に先にパスフレーズの入力**してください。入力後 Save private key を押すことで、パスフレーズで保護された秘密鍵が保存されます。

---

[13] Save Public Key のボタンからも公開鍵を保存できますが、保存したテキストの表現が上記のテキストと異なり、そのまま Prism へコピーペーストができないものになります。上のテキストをコピーペーストする方が容易となります。

秘密鍵は ppk 形式で保存されます。なおデフォルトのファイル名はなく空欄のため何かファイル名を指定する必要があります。なお、ここでは winscp を指定、winscp.ppk というファイルで保存しております。ドキュメントフォルダがデフォルトの保存先フォルダになります。

CVM へ公開鍵認証でアクセスする場合は、Prism にログイン、右上の歯車のマークをクリックして表示される Settings (設定)にある Cluster Lockdown のページにて先ほど保存した公開鍵を登録します。



Name には任意の名称を、Key には先ほど保存した公開鍵のテキストを 1 行でペーストします[14]。

Save Public Key で保存したテキストファイルの場合:

PuTTY Key Generator の Save Public Key を使用して保存したテキストは以下になります。

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-20240403"
AAAAB3NzaC1yc2EAAAADAQABxxABAQCsQEOvMixFtYdK4wElPy1lYItWYHnCjda3
i6ro8PCvfjeBcetF0FY6B8QTdI64d3fQ64O241EqrmjQYr4TRAe0W0w640heNPx7
w8RCzyMb/vWC5qzwauyw/Purjw77ZnPpg1tUho0bNLWOk3rCdCn4+7mBXklCwHBo
APDohU7chQ4FqH2vMmJNGLPqt868ojCqqCHsspJfgf9/1wpzBPm8345LNsMoxqua
vmfY8nGYfkI/YNLLwKWapsO2dFlZyepGndWTnKE5wGHbe+18Z8JC4MInNC8WS43n
fHCd8HLta6X6nzfsz2PNIJJMrIGOGlfP360DqAOXCGW5ErbackDh
---- END SSH2 PUBLIC KEY ----
```

これは Prism に登録すべきテキストとは異なるため、そのままでは利用できないものとなります。

これを手作業で変更するには、以下の手順になります

1. ---- から始まる 1 行目と最終行を削除する
2. 2 行目の Comment:の行を削除する
3. 先頭に ssh-rsa と 1 つスペースを入れる
4. 改行を削除、1 行にまとめる

すると右のテキストになります。

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABxxABAQCsQEOvMixFtYdK4wE
lPy1lYItWYHnCjda3i6ro8PCvfjeBcetF0FY6B8QTdI64d3
fQ64O241EqrmjQYr4TRAe0W0w640heNPx7w8RCzyMb/vWC5
qzwauyw/Purjw77ZnPpg1tUho0bNLWOk3rCdCn4+7mBXklC
wHBoAPDohU7chQ4FqH2vMmJNGLPqt868ojCqqCHsspJfgf9
/1wpzBPm8345LNsMoxquavmfY8nGYfkI/YNLLwKWapsO2dF
lZyepGndWTnKE5wGHbe+18Z8JC4MInNC8WS43nfHCd8HLta
6X6nzfsz2PNIJJMrIGOGlfP360DqAOXCGW5ErbackDh
```

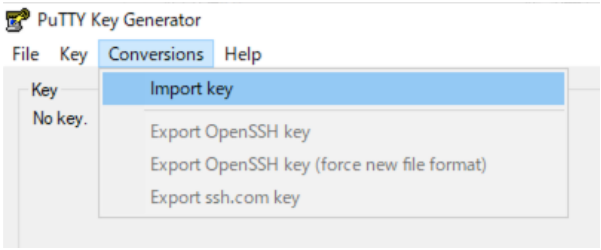
[14] この手順は 1.1. ssh-keygen での鍵生成と同じです。余計な改行を含まないなどの注意も同じになります。

3.1.2. (オプション)OpenSSH 形式の鍵のインポート

既に ssh-keygen で作成した鍵がありこれを利用したいという場合ですが、WinSCP にて鍵をインポートし ppk 形式に変換して利用することが可能です。

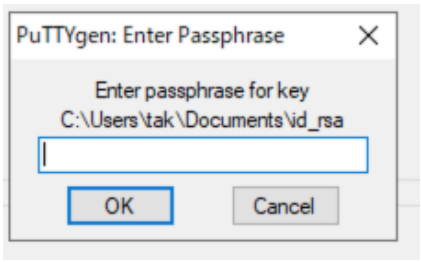
3.1.1 の手順と同じく WinSCP を起動、「ログイン」のパネルの下側にある「ツール」メニューから PuTTYgen を実行を選択します

Putty Key Generator のパネルのメニューから Conversions を選択、Import Key をクリックします。

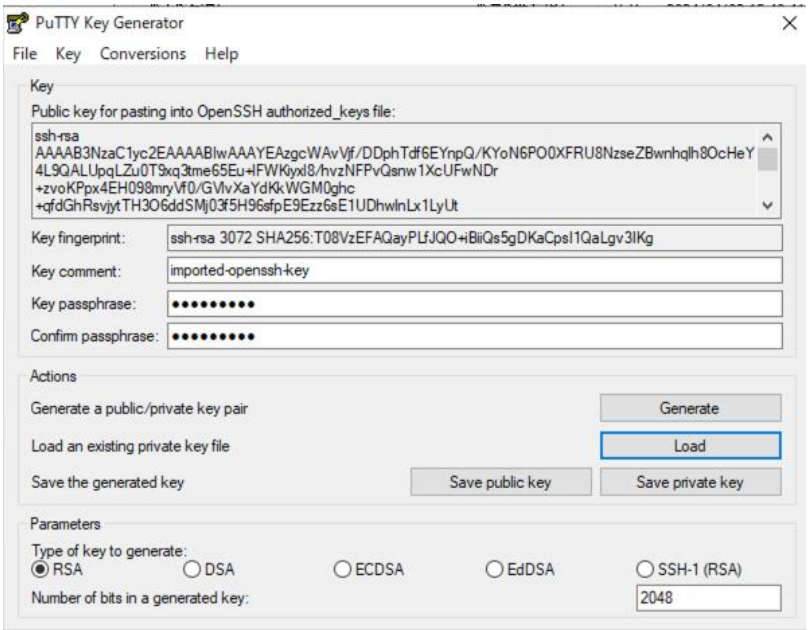


するとファイルを選択する画面が表示されるため、ssh-keygen で作成した OpenSSH 形式の秘密鍵のファイル(id_rsa など.pub のつかない方)を選択します。

秘密鍵にパスフレーズが設定されている場合パスフレーズの入力を求められますのでこちらを入力します(右図)



以下画面が現れますので、こちらで Key passphrase および Comfirm passphrase にパスフレーズを入力後、Save private key にて ppk 形式の秘密鍵を保存してください。なお公開鍵についてはパネルの上側のテキストを利用する、あるいは変換前の OpenSSH 形式の公開鍵ファイルの記載を流用します[15]。



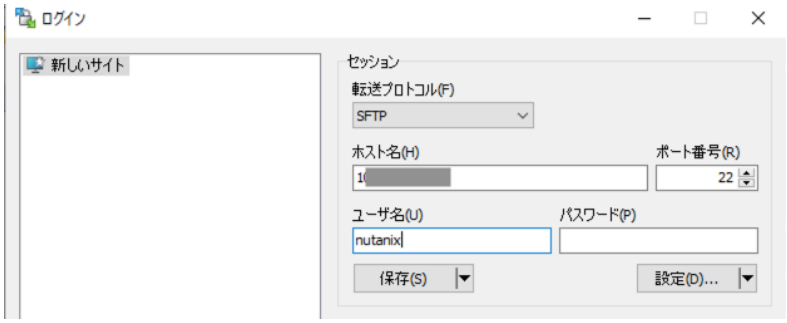
インポートしたキーについても、前ページの Prism への公開鍵の登録方法と同じ手順で公開鍵の登録を行います。公開鍵を登録しないと CVM へはアクセスできないのでご注意ください。

---

[15] OpenSSH 形式でも WinSCP など ppk 形式の秘密鍵を使う場合も、公開鍵についてはただのテキストファイルでその内容をリモートサイトに登録するものとなり、またインポートはあくまで秘密鍵のファイル形式を変換するだけで、秘密鍵/公開鍵そのものの内容は同一のためです。

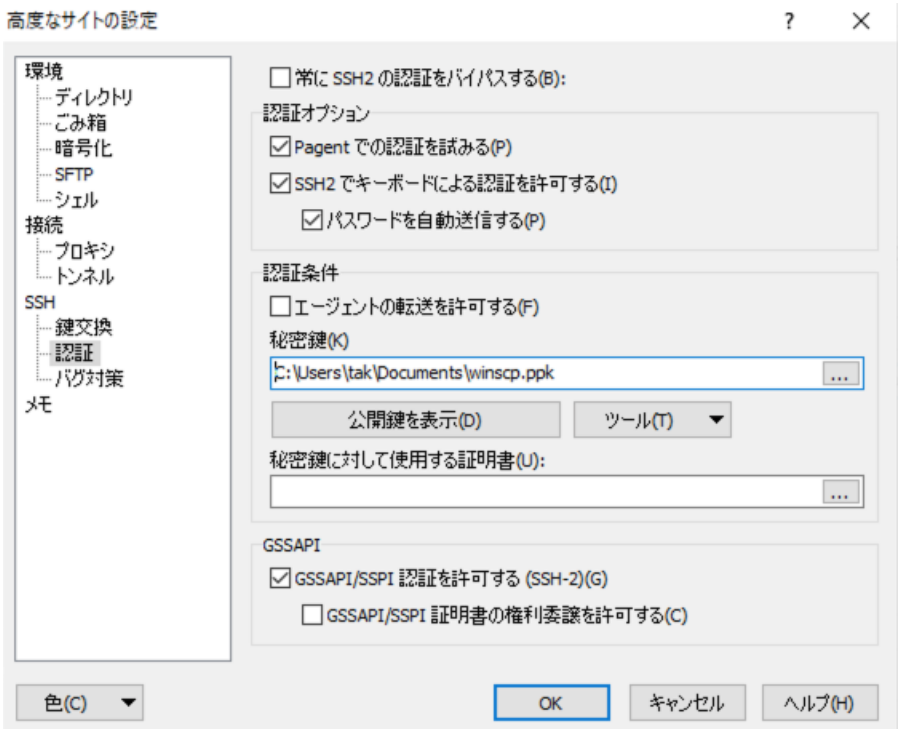
3.2. WinSCP での接続

WinSCP を起動、あるいは起動している WinSCP のログインパネルのホスト名に CVM の IP アドレスを入力、ユーザ名に nutanix と記入します。パスワード[16]は空欄にしておきます。



次に右側にある「設定...」を押して設定パネルを開きます。

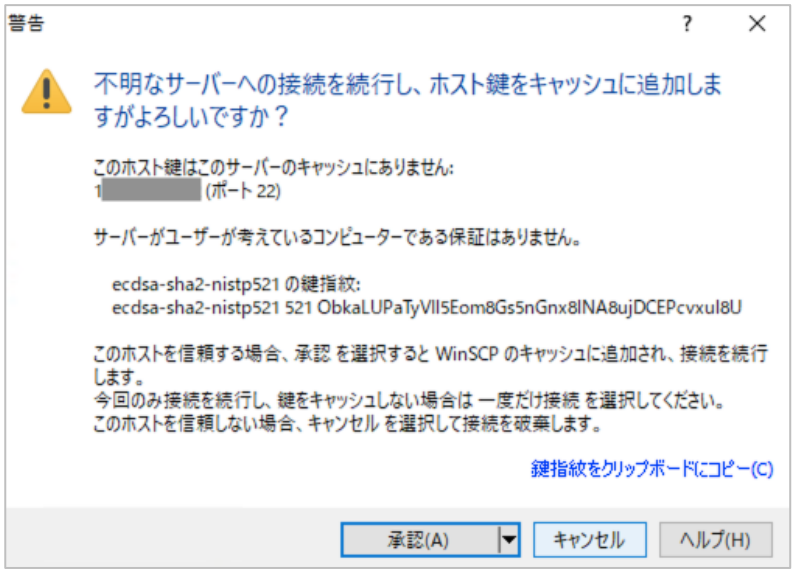
高度なサイトの設定パネルの左側、SSH の下にある認証を選択、右側の認証条件にて秘密鍵の右端の ... をクリック、先ほど作成した(あるいはインポートした)秘密鍵の ppk 形式のファイルを選択します。



OK を押して保存、ログインのパネルの下側、緑のログインを押します。

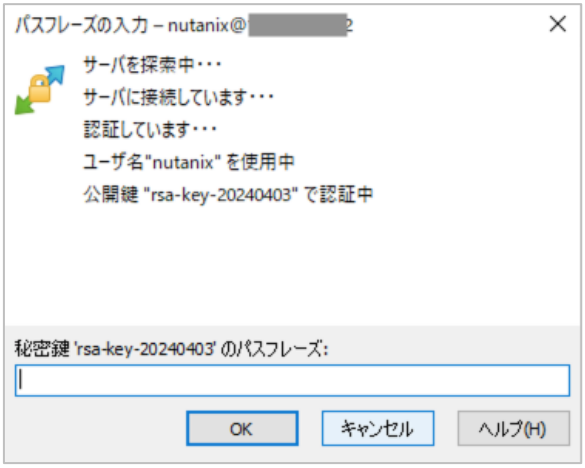
[16] このパスワード欄はパスワードでの認証の際のみ使用され、秘密鍵のパスフレーズとしては利用されません。WinSCP ではデフォルトでパスワードでの認証も試みるため、パスワード欄にパスワードを入れておくと公開鍵認証に失敗した場合にパスワードを送って認証を試みてしまうので、空欄にしておくのが安全になります。

初回の接続時には送付されてくるホストの鍵の確認が入ります。
必要に応じて鍵指紋(フィンガープリント)を確認して承認を押します。

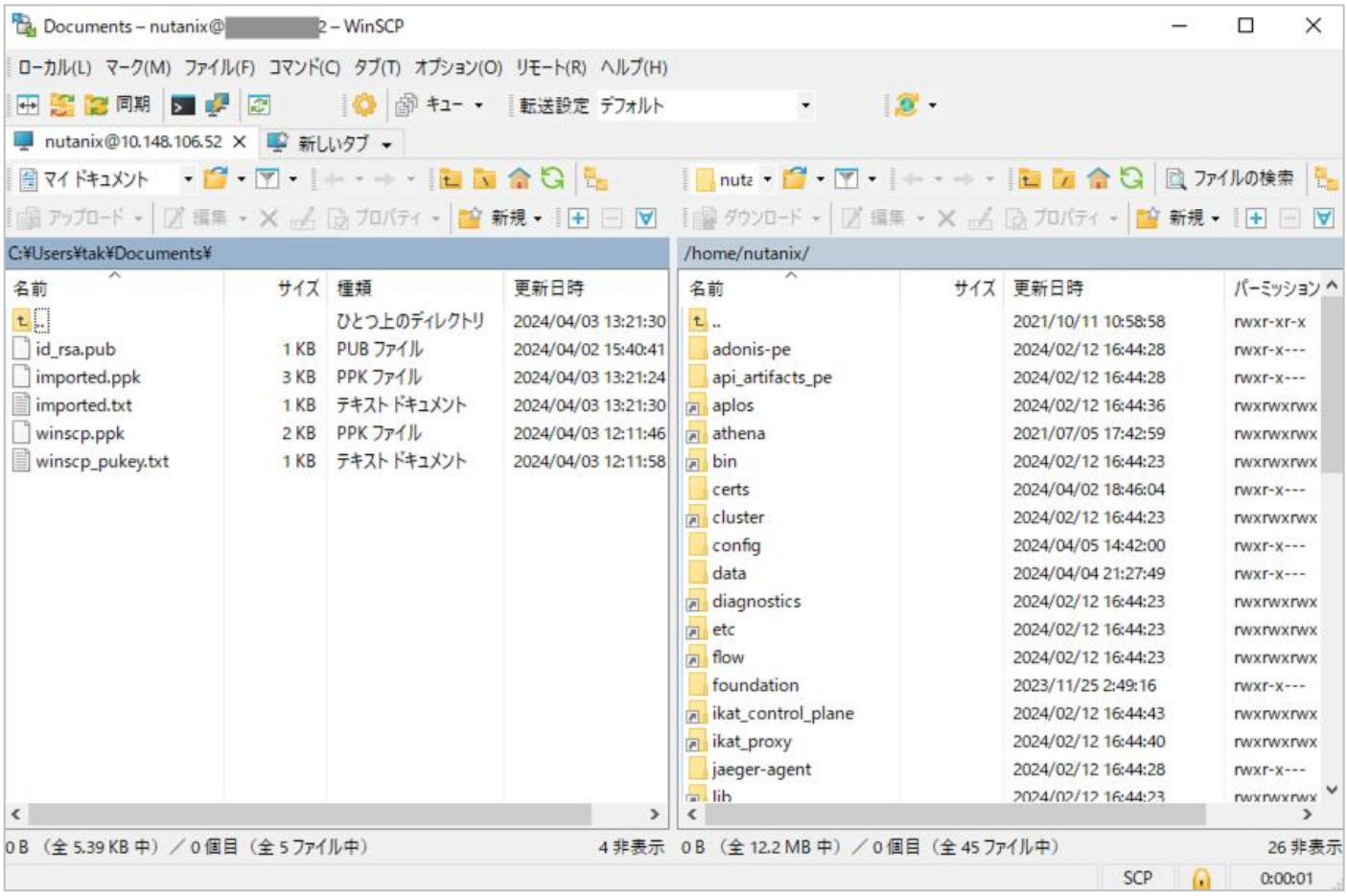


CVM への接続時にはバナーが表示されます。
続けるを押すことで処理を進めます。
また、接続のたびに表示されるのが面倒な場合は、
左下の「このバナーを二度と表示しない」に
チェックを入れてから続けるを押します。

パスフレーズの入力を求められるので、ここで ppk 形式の秘密鍵ファイルに設定したパスフレーズを入力します。



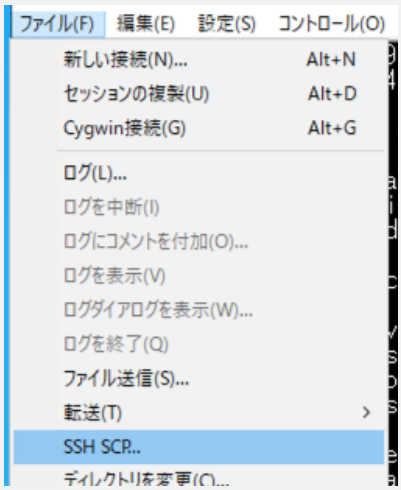
接続に成功するとメインのウィンドウの右側に、CVM の/home/nutanix 以下が表示されます。



Tera Term の SSH SCP 機能は使えないのか?

Tera Term には既に接続している SSH の通信路を利用して SCP を実行する機能があります。これはファイルの SSH SCP というメニューから実施できます。

ただし、CVM ではこうした 1 つの SSH の接続での複数の通信をオフにしているため、Tera Term の SSH SCP はご利用頂けません。
WinSCP など別途ソフトウェアで SFTP をご利用ください。



4. (オプション) Pagent

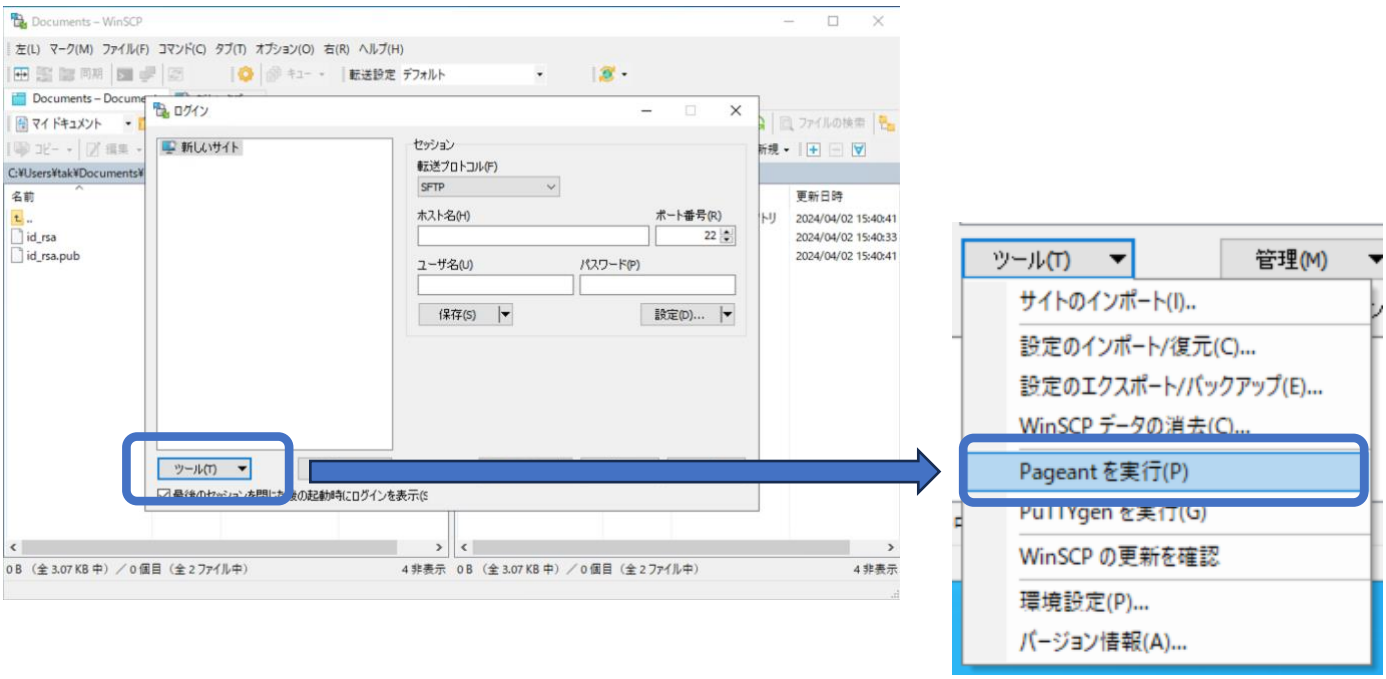
Windows 標準の OpenSSH では ssh-agent というサービスを事前に起動しておくことで、秘密鍵を登録、ssh コマンドで接続の際の秘密鍵のパスフレーズの入力を省略できました。

Tera Term や WinSCP では Windows 標準の OpenSSH の ssh-agent を利用する事はできませんが、その代わりに Pagent という類似のサービスを利用することで同じようにパスフレーズの省略をおこなうことができます。

Pagent は単体でも配布されておりますが、PuTTY や WinSCP に付属もしております。
ここでは、WinSCP に付属の Pagent を使用したパスフレーズの入力の省略を試みます。

4.1. (オプション) Pagent の起動

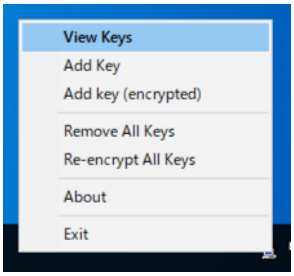
WinSCP を利用する場合は、ログインパネルのツールより Pagent を実行、を選択します。

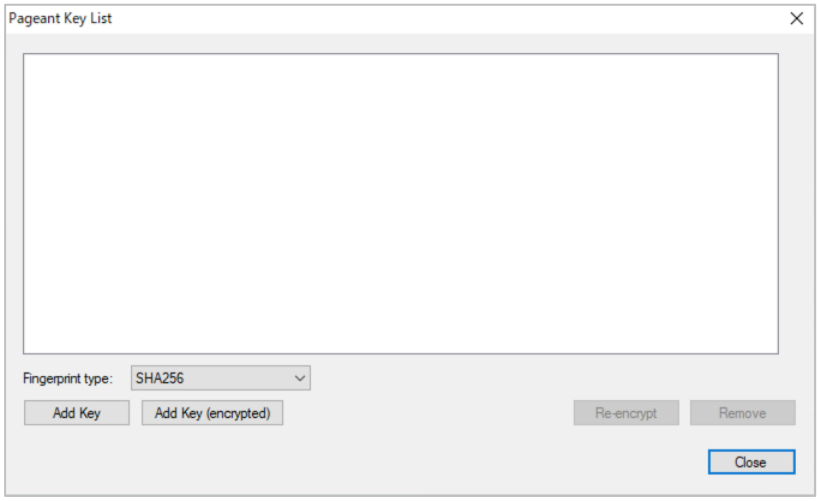


Pagent が起動すると、タスクバーに小さなアイコンが表示されます。

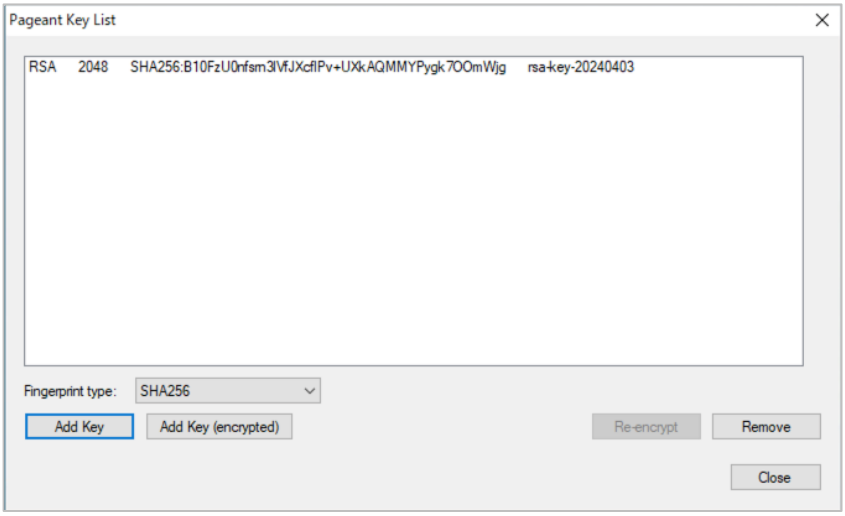
[17] WinSCP での Pagent は C:¥Program Files (x86)¥WinSCP¥PuTTY¥ 以下の pagent.exe が実体です。これを直接起動しても構いません。

Pagent のアイコンを右クリックするとメニューが表示されます。
こちらで View Keys を選択すると、以下の様な鍵の一覧パネルが表示されます。
なお起動直後は何のキーも登録されていないので空になります。





パネルの Add key を押す、あるいはタスクバーのアイコンからのメニューで Add Key を選択すると、ファイルの選択画面が表示されますのでここで ppk 形式の秘密鍵を選択[18]、秘密鍵ファイルのパスフレーズを聞かれますので入力しますと、鍵が登録されます。

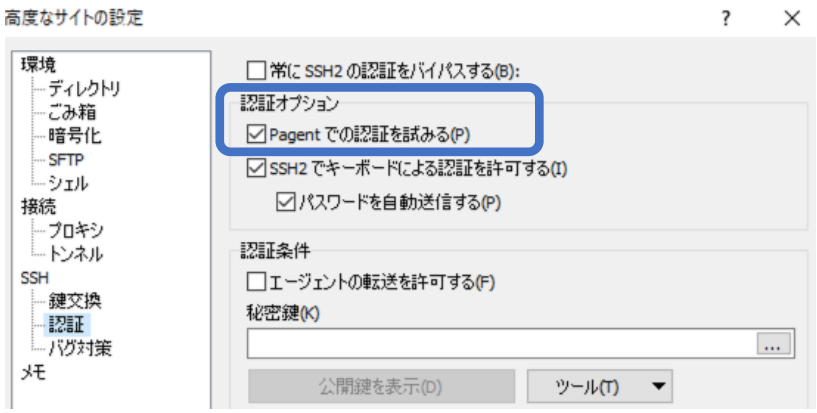


これで Pagent の準備は終了です。

[18] コマンドラインやスタートアップアイテムから pagent.exe を起動する際、引数として ppk 形式の秘密鍵ファイルのパスを指定する事で、起動時に指定の秘密鍵の読み込みを試みます。パスフレーズの入力を促されますので入力すると、秘密鍵が登録されます。

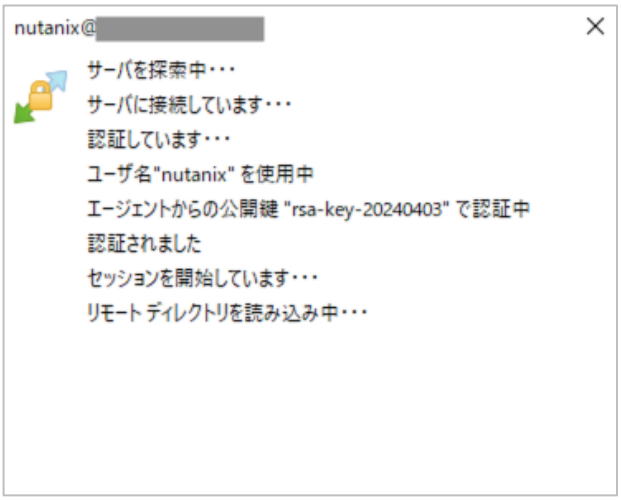
4.2. (オプション) Pagent を使用した WinSCP での接続

先の 3.2.の手順と同じく、WinSCP を起動、あるいは起動している WinSCP のログインパネルのホスト名に CVM の IP アドレスを入力、ユーザ名に nutanix と記入します。パスワード[19]は空欄にしておき、設定から SSH の認証を選択、認証オプションの「Pagent での認証を試みる」を確認します。



これはデフォルトでオンになります。オンである事を確認したら、ログインを実行します。

すると、パスフレーズの入力などが表示されずにメインのウィンドウにて CVM の/home/nutanix 以下が表示されます。



このときのパネルの表示は右図のようになります。「エージェントからの公開鍵　・・・で認証中」とあるように、Pagent により秘密鍵の処理が行われるため、あらためて秘密鍵のファイルのパスフレーズを入力する必要がなくなる次第です。

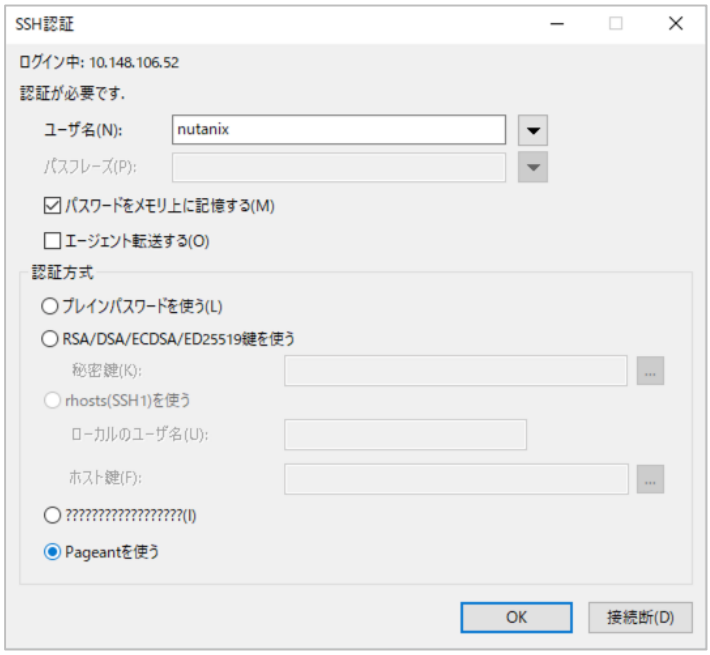
[19] このパスワード欄はパスワードでの認証の際のみ使用され、秘密鍵のパスフレーズとしては利用されません。WinSCP ではデフォルトでパスワードでの認証も試みるため、パスワード欄にパスワードを入れておくと公開鍵認証に失敗した場合にパスワードを送って認証を試みてしまうので、空欄にしておくのが安全になります。

4.3. (オプション) Pagent を使用した TeraTerm での接続

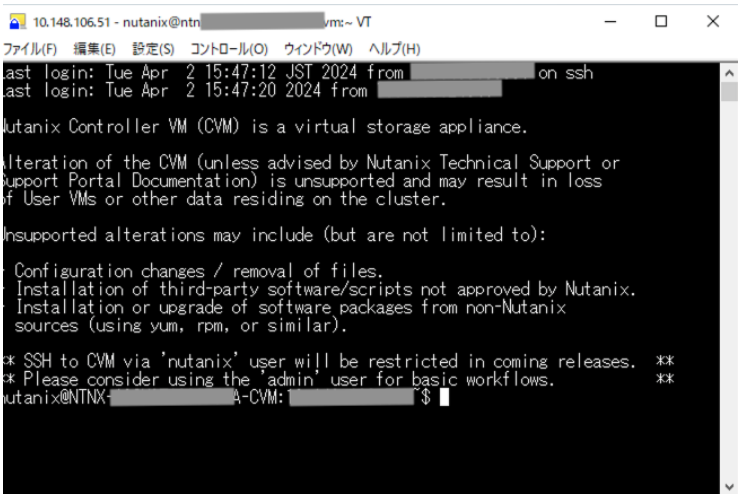
Tera Term でも Pagent はご利用いただけます

。

まず 2.2.と同じように CVM への接続を試みます。以下の SSH 認証のパネルが表示されたところで、一番下の Pagent を使う を選択、OK を押します。



すると、パスフレーズの入力なくしてログインが行われます。



参考情報

・OpenSSH for Windows の概要

https://learn.microsoft.com/ja-jp/windows-server/administration/openssh/openssh_overview

Windows 10 (ビルド 1809 以降)、Windows Sever 2019, 2022 にて利用可能な、Windows 標準での OpenSSH に関するマイクロソフト社のドキュメントになります。

・Tera Term Home Page

https://teratermproject.github.io/

Tera Term は 1994 年に寺西高氏が開発された端末ソフトウェアで、現在は上記ページの Tera Term Project にて開発が進められております。本ドキュメントの作成時点でのバージョンは 5.2 で、このバージョンにて確認を行いました。

・WinSCP

https://winscp.net/eng/docs/lang:jp

WinSCP は Windows 上で動作するオープンソースでグラフィカルな FTP,FTPS,SFTP クライアントプログラムになります。

・Deprecating scp

LWN.net の記事: https://lwn.net/Articles/835962/

Redhat 社のブログ: https://www.redhat.com/ja/blog/openssh-scp-deprecation-rhel-9-what-you-need-know

SSH では長らく、SSH による安全な通信路を用いてリモートとローカルの間でファイルをコピーする方法として SCP が提供されておりました。が、現在 SCP についてはそのプロトコルの脆弱性から利用が非推奨となっております。ファイルのコピーについては、より安全な SFTP の利用が推奨となります。

・How to create a password-less SSH login to your Nutanix cluster

https://portal.nutanix.com/kb/1895

Nutanix KB-1895 では macOS や Linux に搭載の OpenSSH での ssh-keygen での鍵の生成および公開鍵認証でのアクセスについて記載しております。また、Windows 環境での PuTTY での公開鍵認証でのアクセスについてもこちらの KB。

本ドキュメントはこの KB-1895 を補足する、とくに日本での利用の多い Tera Term や WinSCP の利用方法を解説するために作成されました。