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 \sim 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。



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。

		Cluster Lockdown
		Cluster is not locked down.
Cluster Lockdown	?	Cluster lockdown makes your connection to the cluster more secure. To lock down the cluster, delete all keys in the cluster and disable remote login with password.
Cluster is not locked down.		Name
Cluster lockdown makes your connection to the cluster more secure. To lock down the cluster, delete all keys in the cluster and disable		Key
Enable Remote Login with Password New Public Key		ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC+Tu6tcznsoZ/cynKOxB 3kyaMvg0HrjmlISCMKf6f9yD5M6mcHgUScf387xt8wW80wp8qXjA 4J61p8AtbnZCunp0LU2WtVLNCuLhAs2197cSDj1RtBSNxygSkPyRwj G6Dc3AoCFwpZCa5yGNne4dtatZY7mAO8DdUuXXURcZCJX36bal
	/	M1rKQZ+zWCEUFcIWOvHd15EEc5t1unzGRJ6ZOhXbeFbz4xqHzvGfl
		< Back Save

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。

xception while verifying public key.	×
Cluster is not locked down.	
Cluster lockdown makes your connection to the cluster more se	cure.
o lock down the cluster, delete all keys in the cluster and disabl	e
emote login with password.	
emote login with password. Jame	
emote login with password. Jame windowsuser2	
emote login with password. Name windowsuser2 Key ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC+Tu6tcznsoZ/cynH	(OxB
emote login with password. Name windowsuser2 (ey ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC+Tu6tcznsoZ/cynł 3kyaMvg0HrjmIISCMKf6f9yD5M6mcHgUScf387xt8wW80wp8	(OxB iqXjA
emote login with password. Name windowsuser2 (ey ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC+Tu6tcznsoZ/cynk 3kyaMvg0HrjmlISCMKf6f9yD5M6mcHgUScf387xt8wW80wp8 4J61p8AtbnZCunp0LU2WtVLNCuLhAs2197cSDj1RtBSNxygSkf	(OxB qXjA PyRwj

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< th=""><th>IP></th><th></th></cvm<>	IP>	
	Windows PowerShell S C:¥Users¥tak> ssh nutanix@ The authenticity of host 'I COSA key fingerprint is SHA256:AHY2v2idr8VizWPrgoVs4GDQAbsz8vgViswLDA7CMxs. Are you sure you want to continue connecting (yes/no)? yes Yarning: Permanently added '10.148.106.51' (ECDSA) to the list of known hosts. Uutanix Controller VM Enter passphrase for key 'C:¥Users¥tak/.ssh/id_rsa': _	-

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。

☑ 管理者: Windows F	PowerShell
PS C:\Window	ws\system32> get-service ssh-agent set-service -StartupType Manual
PS C:\Window	ws\system32> start-service ssh-agent
PS C:\Window	ws\system32> get-service ssh-agent select-object DisplayName,Name,Status,StartType fl
DisplayName	: OpenSSH Authentication Agent
Name	: ssh-agent
Status	: Running
StartType	: Manual

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。

Windows PowerShell	
PS C:¥Users¥tak> s <mark>sh-add</mark> Enter passphrase for C:¥Users¥tak/.ssh/id_rsa: Identity added: C:¥Users¥tak/.ssh/id_rsa (C:¥Users¥tak/.s PS C:¥Users¥tak> _	ssh/id_rsa)

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。



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。

Tera Term - [未接続] VT - □ × T75/ル(F) 編集(E) 設定(S) コントロール(O) ウィンドウ(W) ヘルプ(H) TTSSH: 鍵生成 					
ファイル(F) 編集(E) 設定(S) コントロール(O) ウィンドウ(W) ヘルプ(H) TTSSH: 鍵生成 鍵の種類 ○ RSA1 ⓒ RSA ○ ECDSA-256 ⓒ ECDSA-384 ○ ECDSA-521 ⓒ ED25519 縦砲のパスフレーズ: パスフレーズの確認: コメント(O): ラウンド数(N): 16 公開鍵の保存(I)	📶 Tera Term - [未接続]	VT		_	\times
TTSSH: 鍵生成 縦の種類 ○ RSA1 ③ RSA ○ DSA ○ ECDSA-256 ○ ECDSA-384 ○ ECDSA-521 ○ ED25519 縦砲のパスフレーズ: パスフレーズの確認: コメント(O): ○ bcrypt KDF形式(K) 方ウンド数(N): 16 公開鍵の保存(I) 秘密鍵の保存(P)	ァイル(F) 編集(E) 設)	定(S) コントロール(O) ウィンド	(W) ヘルプ(H)		
健の種類 ○ RSA1 ● RSA ○ DSA ○ ECDSA-256 ○ ECDSA-384 ○ ECDSA-521 ○ ED25519 送のパスフレーズ: パスフレーズの確認: コメント(O): ジント(O): ジント(O): シント(O): シーンド数(N): 16	TTS	SH: 鏈生成		×	^
 ○ ECDSA-521 ○ ED25519 ペルプ(H) 鍵のパスフレーズ: パスフレーズの確認: コメント(O): 」 bcrypt KDF形式(K) ラウンド数(N): 16 公開鍵の保存(I) 秘密鍵の保存(P) 		鍵の種類 〇 RSA1	SA ビット数(B): A-384 3072	生成(G) 閉じる(C)	
鍵のパスフレーズ: パスフレーズの確認: コメント(O): ✓ bcrypt KDF形式(K) ラウンド数(N): 16 公開鍵の保存(I) 秘密鍵の保存(P)		O ECDSA-521 O ED255	19	ヘルプ(H)	
コメント(O): ラウンド数(N): 16 △ bcrypt KDF形式(K) ふ閉鍵の保存(I)		鍵のパスフレーズ: パスフレーズの確認:			
✓ bcrypt KDF形式(K) ラウンド数(N): 16 公開鍵の保存(I) 秘密鍵の保存(P)		コメント(O):			
公開鏈の保存(I) 秘密鏈の保存(P)	E	☐ bcrypt KDF形式(K)	ラウンド数(N): 16	; ;	
		公開鍵の保存(I)	秘密鍵の保存(P)		

「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。

<u>∭</u> Tera Term - [未接続] VT ファイル(F) 編集(F) 設定(S) コントロール(O) ウィンドウ(W) ヘルブ(H)	_	\times
■ TTSSH: 鍵生成	×	^
鍵の種類 ○ RSA1 ● RSA ○ DSA ビット数(B):	生成(G) 閉じる(C)	
O ECDSA-256 O ECDSA-384 3072 O ECDSA-521 O ED25519	ヘルプ(H)	
????????? 縺のパスフレーズ: ●●●●●●●●●● パスフレーズの確認: ●●●●●●●●●●		
□ bcrypt KDF形式(K) ラウンド数(N): 16 公開鍵の保存(I) 秘密鍵の保存(P)		
		~

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。

	Cluster Lockdo	wn	
	다. Cluster	is not locked down.	
luster Lockdown	Cluster lock To lock dow remote login	down makes your connection to the cluster more sec n the cluster, delete all keys in the cluster and disable n with password.	ure.
Cluster is not locked down.	Name windows	iser	
Cluster lockdown makes your connection to the cluster more secure. To lock down the cluster, delete all keys in the cluster and disable remote login with password	Key ssh-rsa		
Enable Remote Login with Password How Public Key	AAAAB3N 3kyaMvg(4J61p8Ati G6Dc3Ao	IzaC1yc2EAAAADAQABAAABAQC+Tu6tcznsoZ/cynKi)HrjmlISCMKf6f9yD5M6mcHgUScf387xt8wW80wp8c onZCunp0LU2WtVLNCuLhAs2197cSDj1RtBSNxygSkP CFwpZCa5yGNne4dtatZY7mAO8DdUuXXURcZCJX3	DxB XjA /Rwj 6bal
	M1rKQZ+z	WCEUFclWOvHd15EEc5t1unzGRJ6ZOhXbeFbz4xqHz	vGf

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。

SSH認証	- 🗆 X	< SSH認言	Œ				3
ログイン中: 10.148.106.51		ログイン	中: 10.148.10	5.51			
認証が必要です。		認証が	必要です。				
ユーザ名(N):	-	-د	ザ名(N):	nutanix		-	
パスフレーズ(P):	-	10	スフレーズ(P):			•	
✓ パスワードをメモリ上に記憶する(M)			バスワードをメモ	リ上に記憶する(M	(N		
□ エージェント転送する(O)			エージェント転送	苦する(O)			
認証方式		122 8正	方式				
 ブレインパスワードを使う(L) 		0	プレインバスワー	ドを使う(L)			
○ RSA/DSA/ECDSA/ED25519鍵を使う			RSA/DSA/ECO	DSA/ED25519键	E使う		
秘密鍵(K):			秘密鏈(K):		C:¥Users¥tak¥Docu	ments¥id_rsa	
○ rhosts(SSH1)を使う		0	rhosts(SSH1)	を使う			
ローカルのユーザ名 (U):			ローカルのユー	ザ名(U):			
ホスト鍵(F):			ホスト鍵(F):				
O 333333333333333333333333333333333333		0	******	?????(I)			
○ Pageantを使う		0	Pageantを使う	5			

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。

e Key Conversions Help			
Key No key.			
Actions			
Actions Generate a public/private key pair Load an existing private key file		(Generate
Actions Senerate a public/private key pair Load an existing private key file Save the generated key		Save public key	Generate I Save p
Actions Generate a public/private key pair Load an existing private key file Save the generated key Parameters	0.000	Save public key	Generate Save pro-r key

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。

PuTTY Key Genera	ator	>
e Key Convers	ions Help	
Kev		
Please generate son	me randomness by moving the mouse over the blank area.	

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。

	😴 PuTTY Key Generator	\times
键の生成が終わると右の図のとうに生成され	File Key Conversions Help	
疑の上成り 利力 ると石の因のように上成され	Key Duble law for earlier into One SSU at the inert law flat	
た鍵の情報が表示されます。	Public Key for pasting into OpenSSH authonzed_keys file: ssh-fsa haAAAB3NzaC1vc2EAAAADAQABAAABAQCsQEQvMixBYdK4wEPv1IYItWYHoCida36m8PCvfieBoetE0EY	6880
上は公開鍵のテキストのため、これをコピー	Tdl64d3fQ640241EqmjQYr4TRAe0W0w640heNPx7w8RCzyMb/vWC5qzwauyw/Purjw77ZnPpg1tUho0bN Ok3rCdCn4+7mBXklCwHBoAPDohU7chQ4FqH2vMmJNGLPqt868ojCqqCHMfpJtgf9/1wpzBPm8345LNsMo vmfY8nGYfkI/YNLLwKWaps02dFlZyepGndWTnKE5wGHbe	ILW ixqua
してテキストファイルに保存します ¹³ 。	Rey tingerprint. ssntsa zuto SHA200.b turzuunisma vigActirv+uAkAulikin trygk/00mvijg	
この公開鍵のテキストは次の手順で利用しま	Key comment: rsa-key-20240403	
	Key passphrase:	
す。	Confirm passphrase:	
	Actions	
	Generate a public/private key pair Generate	
	Load an existing private key file Load	
	Save the generated key Save public key Save private	key
下の Save private key のボタンを押すこと	Parameters	
で、公開鍵および秘密鍵がファイルに保存さ	Type of key to generate:	SA)
れます。	Number of bits in a generated key: 2048	

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 ヘ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。

		Cluster Lockdown	p.,
Cluster Lockdown	2	Cluster is not locked down. Cluster lockdown makes your connection to the cluster more secure. To lock down the cluster, delete all keys in the cluster and disable	
Cluster is not locked down. Cluster lockdown makes your connection to the cluster more secure. To lock down the cluster, delete all keys in the cluster and disable remote login with password. Enable Remote Login with Password + New Public Key		Name windowsluser Key ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC+Tu6tcznsoZ/cynKOxB 3kyaMvg0HrjmIISCMKf6f9yD5M6mcHgUScf387xt8wW80wp8qXjA 4J61p8AtbnZCunp0LU2WtVLNCuLhAs2197cSDj1RtBSNxygSkPyRwj G6Dc3AoCFwpZCa5yGNne4dtatZY7mAO8DdUuXXURcZCJX36bal M1rKQZ+zWCEUFcIWOvHd15EEc5t1unzGRJ6ZOhXbeFbz4xqHzvGfl 4 Back	

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。

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 AAAAB3NzaClyc2EAAAADAQABxxABAQCsQEOvMixFtYdK4wE lPyllYltWYHnCjda3i6ro8PCvfjeBcetF0FY6B8QTdI64d3 fQ640241EqrmjQYr4TRAe0W0w640heNPx7w8RCzyMb/vWC5 qzwauyw/Purjw77ZnPpgltUho0bNLW0k3rCdCn4+7mBXklC wHBoAPDohU7chQ4FqH2vMmJNGLPqt868ojCqqCHsspJfgf9 /1wpzBPm8345LNsMoxquavmfY8nGYfkI/YNLLwKWapsO2dF lZyepGndWTnKE5wGHbe+18Z8JC4MInNC8WS43nfHCd8HLta 6X6nzfsz2PNIJJMrIGOGlfP360DqA0XCGW5ErbackDh

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。

😴 PuTTY K	ey Generator
File Key	Conversions Help
Key	Import key
No key.	Export OpenSSH key
	Export OpenSSH key (force new file format)
	Export ssh.com key

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)

PuTTYgen: Enter Passphrase	×
Enter passphrase for key C:\Users\tak\Documents\id_rsa	,
OK Cancel	

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。

le Key Conversi	ons Help			
Public key for pasting	into OpenSSH autho	rized keys file:		
ssh-rsa AAAAB3NzaC1yc2E 4L9QALUpqLZu0T +zvoKPpx4EH098m +qfdGhRsvjytTH3O	AAAABIwAAAYEAzg xq3tme65Eu+IFWKiyy ryVf0/GVIvXaYdKkW 6ddSMj03f5H96sfpE9	cWAvVjf/DDphTdf(d8/hvzNFPvQsnw1 GM0ghc Ezz6sE1UDhwlnLx1	SEYnpQ/KYoN6PO0XFRU XcUFwNDr ILyUt	18NzseZBwnhqlh8OcHeY
Key fingerprint:	ssh-rsa 3072 SHA25	6:T08VzEFAQayPL	fJQO+iBiiQs5gDKaCps11Q	aLgv3lKg
Key comment:	imported-openssh-ke	y		
Key passphrase:	•••••			
Confirm passphrase:	•••••			
Actions				
Generate a public/pr	ivate key pair			Generate
Load an existing priv	ate key file			Load
Save the generated	key		Save public key	Save private key
Parameters				
Type of key to gener RSA	ate: ODSA	OECDSA	OEdDSA	O SSH-1 (RSA)
Number of hits in a g	enerated key:			2048

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。

🗟 ログイン		-	-		×
💽 新しいサイト	セッション 転送プロトコル(F) SFTP ~ ホスト名(H) ユーザ名(U) nutanix((保存(S) ▼	パスワード(P)	ポー] [] 設定	卜番号(R 22 〔(D)	

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。

環境 □ 常に SSH2 の認証をバイパスする(B):ディレクトリ 認証オプション		
□ 日本日本 □ Pagent での認証を試みる(P) ○ SFTP ○ SSH2 でキーボードによる認証を許可する(I) ○ JIL □ パスワードを自動送信する(P) □ ボージェントの転送を許可する(F) 認証条件 □ I - ジェントの転送を許可する(F) 秘密鍵(K) □ SSH □ I - ジェントの転送を許可する(F) ● 認証 ○ CSSAPI ○ GSSAPI ○ GSSAPI ○ GSSAPI/SSPI 認証を許可する (SSH-2)(G) □ GSSAPI/SSPI 証明書の権利季課を許可する(C)		
 	ヘルプ(H)

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。

	□ ログイン - ▼	閉じる	ヘルプ(H)
T (5		14100	46764

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。

警告	? ×
	不明なサーバーへの接続を続行し、ホスト鍵をキャッシュに追加しま すがよろしいですか?
	このホスト鏈はこのサーバーのキャッシュにありません: 1 (パート 22)
	サーバーがユーザーが考えているコンピューターである保証はありません。
	ecdsa-sha2-nistp521 の鏈指紋: ecdsa-sha2-nistp521 521 ObkaLUPaTyVII5Eom8Gs5nGnx8INA8ujDCEPcvxul8U
	このホストを信頼する場合、承認を選択すると WinSCP のキャッシュに追加され、接続を続行 します。 今回のみ接続を続行し、鍵をキャッシュしない場合は一度だけ接続を選択してください。 このホストを信頼しない場合、キャンセルを選択して接続を破棄します。
	鍵指紋をクリップボードにコピー(C)
	承認(A) ▼ キャンセル ヘルプ(H)

認証バナー – nutanix@'

□このバナーを二度と表示しない(N)

続ける

н

ヘルプ(H)

 \times

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。

🔁 Documents – nutanix@	2	- WinSCP						1
ローカル(L) マーク(M) ファイ)	ル(F) コマンド(C) タブ(T) オブション(O) リモート(R) ヘルプ(H)					
		10	「転送設定 デフォルト		a .			
			- +0.238/AC 7 74/01					
nutanix@10.148.106.52	× 🚽 新し	1197 -					1.	
📲 マイドキュメント 🔹 🎽	• 🛛 • 🗌	+ t_ X	G 🔓	📕 nute 🔹 🎽 👻 💌			ファイルの検索	
「風 アップロード・ 2] 編集	·× A	🕞 プロパティ 🖌 🎦 🕯	新規 🗸 📑 📃 💟	ダウンロード ・ 日 日	* × × 4	🕞 ブロバティ 🖌 🎦 新き	現 - 🛨 📃 🖸	4
C:¥Users¥tak¥Documents¥				/home/nutanix/				
名前	サイズ	種類	更新日時	名前 ^	サイズ	更新日時	パーミッション	^
t.		ひとつ上のディレクトリ	2024/04/03 13:21:30	t		2021/10/11 10:58:58	rwxr-xr-x	
id_rsa.pub	1 KB	PUB ファイル	2024/04/02 15:40:41	adonis-pe		2024/02/12 16:44:28	rwxr-x	
imported.ppk	3 KB	PPK Jr11	2024/04/03 13:21:24	api_artifacts_pe		2024/02/12 16:44:28	rwxr-x	
imported.txt	1 KB	テキストドキュメント	2024/04/03 13:21:30	aplos		2024/02/12 16:44:36	rwxrwxrwx	
winscp.ppk	2 KB	PPK ファイル	2024/04/03 12:11:46	athena		2021/07/05 17:42:59	rwxrwxrwx	
winscp_pukey.txt	1 KB	テキストドキュメント	2024/04/03 12:11:58	bin		2024/02/12 16:44:23	rwxrwxrwx	
				certs		2024/04/02 18:46:04	rwxr-x	
				cluster		2024/02/12 16:44:23	rwxrwxrwx	
				config		2024/04/05 14:42:00	rwxr-x	
				data		2024/04/04 21:27:49	rwxr-x	
				diagnostics		2024/02/12 16:44:23	rwxrwxrwx	
				etc		2024/02/12 16:44:23	rwxrwxrwx	
				flow		2024/02/12 16:44:23	rwxrwxrwx	
				foundation		2023/11/25 2:49:16	rwxr-x	
				ikat_control_plane		2024/02/12 16:44:43	rwxrwxrwx	
				ikat_proxy		2024/02/12 16:44:40	rwxrwxrwx	
				jaeger-agent		2024/02/12 16:44:28	rwxr-x	
			>	lib ≰		2024/02/12 16:44:23	rwxrwxrwx	~
0.P. (A 5 30 KP th) / 0.FT	B (A = 7-4	(1	, ±b ≠ =	0.P. (A 13.3 MP #) /0				
0 15 (主 5.39 KB 中) / 0 個	日 (王5)71	JV+7	4 非表示	0 B (王12,2 MB 中) / 0	1回日 (王45)7	(1)//+)	26 非表	275
						SCP	0:00:01	

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。

ファイル(F)	編集(E)	設定(S)	コントロール	(O)
新し	い接続(N)		Alt+N	Ð
セッシ	リョンの複製	(U)	Alt+D	f f
Cygv	vin接続(G)		Alt+G	
ログ(L)			-
ログを	e中断(I)			1
ログは	コメントを付	加(O)		
ログを	表示(V)			
ログダ	イアログを表	ŧ示(W)		
ログを	ē終了(Q)			Ľ,
ファイ	ル送信(S)			Ď
転送	(T)			> 5
SSH	SCR			в
ディレ	クトリを変更	Ī(C)		a

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

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。

Pageant Key List				×
Fingerprint type:	SHA256 V		Re-encrypt	Remove
, au ney	ride ney (circlypted)		no onoypt	Close

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。

ISA 2048	SHA256:B10FzU0	0nfsm3lVfJXcfIPv+UX	«kAQMMYPygk700mWjg	g rsa-key-20240403	
gerprint type	SHA256	~			

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。

高度なサイトの設定		?	\times					
環境 - ディレクトリ - ごみ箱 - 暗号化 - SFTP - シェル 接続 - プロキシ - アロキシ - ドンネル SSH - 認証 - パグ対策 メモ	 □ 常に SSH2 の認証をバイパスする(B): 認証オブション ☑ Pagent での認証を試みる(P) ☑ SSH2 でキーボードによる認証を許可する(I) ☑ パスワードを自動送信する(P) 							
	認証条件 □エージェントの転送を許可する(F) 秘密鍵(K) 	[

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。

SSH認証					-		×
ログイン中: 10.148.106.52							
認証が必要です.							
ユーザ名(N):	nutanix				·		
パスフレーズ(P):				-			
☑ パスワードをメモ	リ上に記憶する(N	(N					
□エージェント転送	送する(O)						
認証方式							
○ プレインパスワー	-ドを使う(L)						
O RSA/DSA/EC	DSA/ED25519鍵を	を使う					
秘密鍵(K);							
O rhosts(SSH1)	を使う						
ローカルのユー	ザ名(U):						
ホスト鍵(F);							
O 1111111111	?????(I)						
● Pageantを使う	ð						
				OK		接続断	(D)

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

<u>https://learn.microsoft.com/ja-jp/windows-server/administration/openssh/openssh_overview</u> 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。