テクニカル レポート

共通アクセスカードを使用したONTAP SSH認証

NetApp
Dan Tulledge
2018年9月| TR-4717

概要

このテクニカルレポートでは、サードパーティのSSHクライアントとActivClientソフトウェアを組み合わせて、Common Access Card（CAC；共通アクセスカード）に保存されている公開鍵を使用してONTAPストレージ管理者を認証するための設定およびテストについて説明します（ONTAPで設定されている場合）。

<<本レポートは機械翻訳による参考訳です。公式な内容はオリジナルである英語版をご確認ください。>>

バージョン履歴

バージョン	日付	ドキュメント バージョン履歴
バージョン1.0	2018年9月	Dan Tulledge：初版。

目次

1 概要

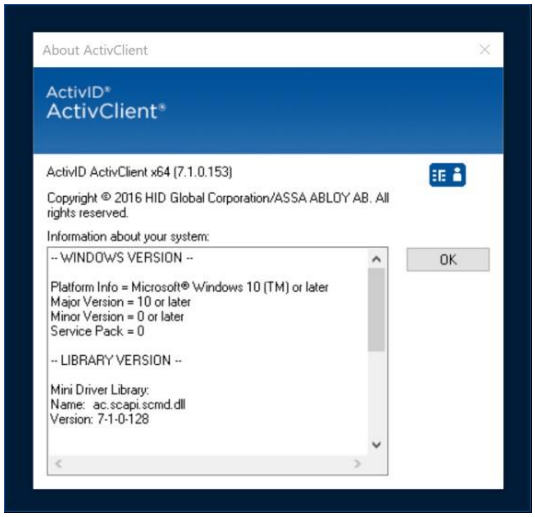
Common Access Card（CAC；共通アクセスカード）は、現役軍人、予備役兵、国防総省の民間人、および資格のある請負業者の従業員を対象とした「スマート」なIDカードです。CACには、スマート・カード・リーダーで読み取ることができるX.509証明書が保存されます。サードパーティ製セキュアシェル（SSH）クライアントPuTTY-CACおよびSecureCRTをActivClientソフトウェアと組み合わせて使用し、リーダーおよびCACにアクセスすることで、ONTAPストレージ管理者は、ONTAPで設定されている場合にCACに保存されている公開鍵を使用して認証できます。

2 構成

2.1 アクティブクライアント

HID GlobalのActivClientソフトウェアは、スマート・カード・リーダーに挿入されたCACに格納されているX.509証明書にアクセスするために、PuTTY-CACおよびSecureCRT SSHクライアント・ソフトウェアによって使用されます。このレポートを検証するために実行されたテストでは、Windows 10 Enterprise OSバージョン1709、OSビルド16299.611で実行されているActivID ActivClient x64（7.1.0.153）を使用しました。

図1）ActivID ActivClientについて

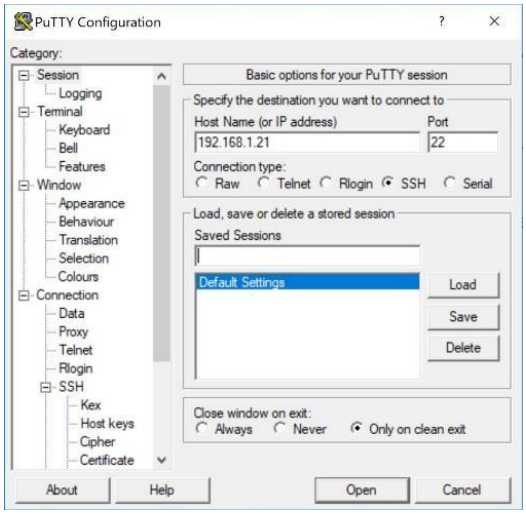


2.2 PuTTY-CAC

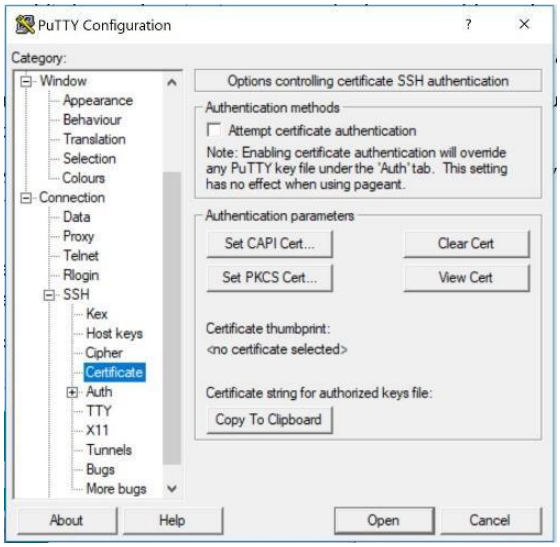
PuTTY-CACはパブリックドメインのSSHクライアントソフトウェアです。https://github.com/NoMoreFood/putty-cac/releasesで入手できます。このレポートを検証するために実行されたテストでは、セクション2.1で説明するActivClientとともにputtycac-64bit-0.70u4-installer.msiを使用しました。

authentication-method publickeyを使用してONTAPアプリケーションsshにアクセスする設定手順

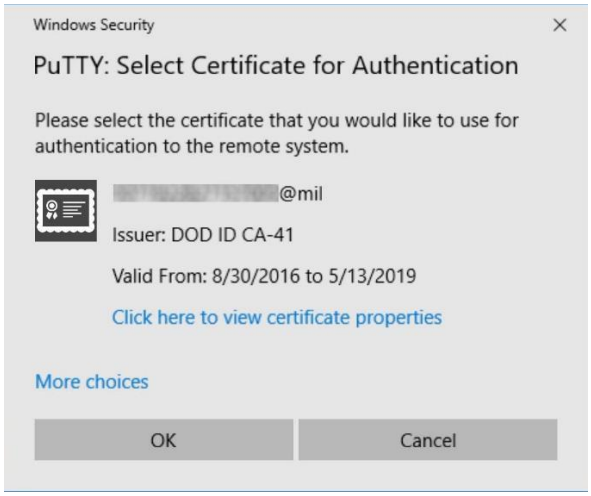
1. Putty-CACを開きます。[Host Name]フィールドに、ONTAPのクラスタ管理IPアドレスまたはホスト名を入力します。



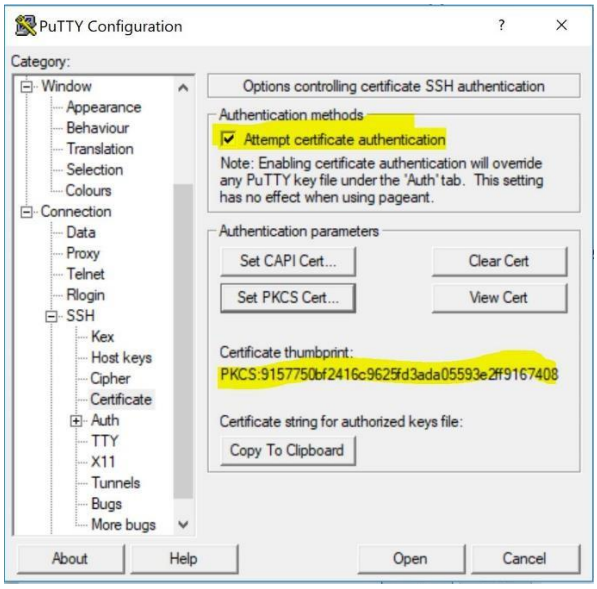
2. SSHを展開し、[Certificates]を選択します。次に、[PKCS証明書の設定]ボタンをクリックします。



3. `acpkcs211.dll` ActivClientのインストールディレクトリにあるファイルを参照します `C:\Program Files\HID Global\ActivClient`。（バージョンによっては、`c:\windows\system32` ディレクトリに配置されている場合があります）。 次に、証明書を選択します。



4. [Attempt Certificate Authentication]チェックボックスがオンになっており、証明書のサムプリントが表示されていることを確認します。[クリップボードにコピー]をクリックします。



5. テキストエディタを開き、クリップボードの内容を貼り付け、[最大]を選択し `=C:\ Program Files\HID Global\ActivClient\acpkcs211` てクリップボードにコピーします。

6. ONTAPで公開鍵認証方式を使用して管理者ユーザを作成します。

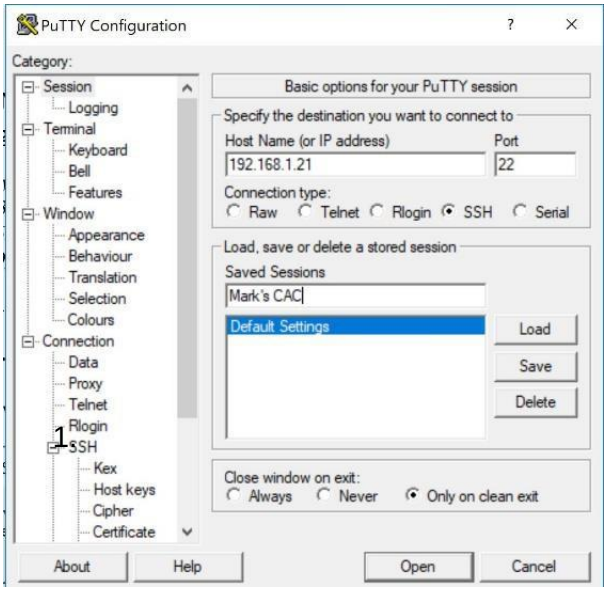
```
security login create -user-or-group-name <username> -application ssh -authentication-method
publickey

Warning: For successful authentication, ensure you create a public key for user "<username>"
using
"security login publickey create" interface.
```

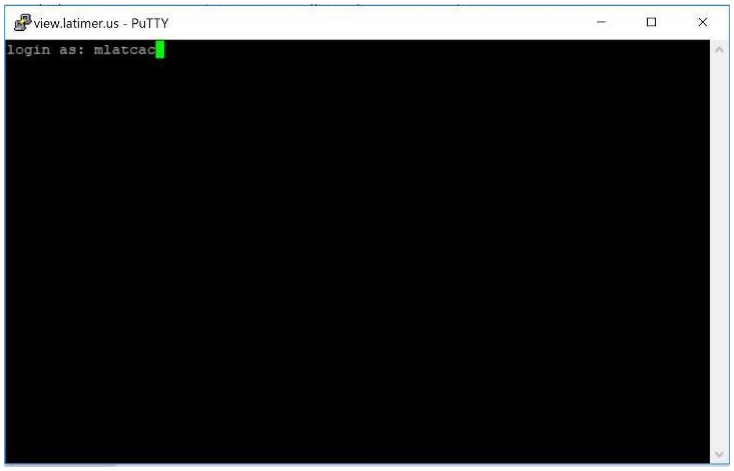
7. 手順5でコピーした公開鍵を、引用符で囲んだ公開鍵を `-publickey` フィールドに貼り付けて、作成したadminユーザに関連付けます。

```
security login publickey create -username <username> -index 0 -publickey "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDBh8mgwjshX4P3oXw8Qd+s1p2jW8K73mw8ubYhvb+Alx4ZM9T0QmsmYTtFjQQ+bDbp6
ruqjjoO8hjl+WSVuxUwW5xWRUwYS/rtQmhP/2fudSncwd2cuRxMvMHKSruF8ee2WRTjO7vu7f4akrCfQL9cOhzh3dEHuFR5qo
OgCgr5nq8v3mZpAyoK7C4/uC9Lr8UO3mBctZ6pBfHLnQRCWgxc20FDFI4pM9Lz93fSIQXCCL8xrpCzi0bzH+4Dwug1gPJsrfS
a7Ki3s1SfNtiAWVqSh78D4iHYT8XjJr1TGVjsvZLg0/UUpwx5nvcRBWME9EczWi623tPO5fsUSGhQtCPn" -vserver
<admin vserver name>
```

8. Putty-CACで[Session]をクリックし、セッションに一意の名前を付けて保存します。



9. [開く]をクリックし、ONTAPで作成したアカウントのユーザー名とCACトークンPINを使用してログインします。

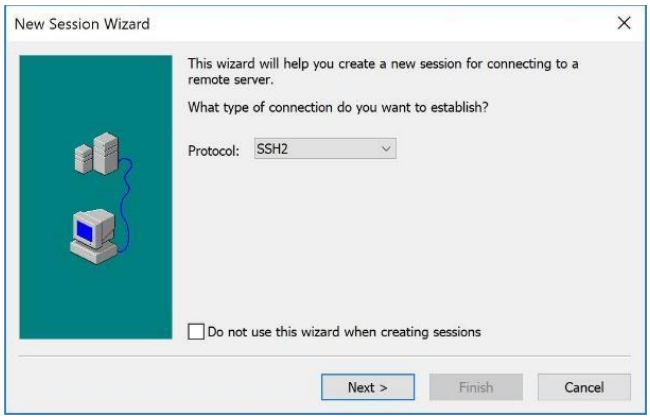


SecureCRT

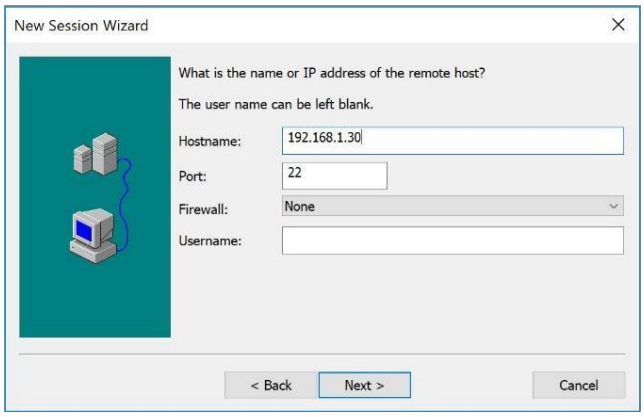
SecureCRTは、VanDyke Softwareから市販されているSSHクライアントです。このレポートを検証するために実行されたテストでは、セクション2.1で説明したActivClientとともにSecureCRT scrt833-x64.exeを使用しました。

authentication-method publickeyを使用してONTAPアプリケーションsshにアクセスする設定手順

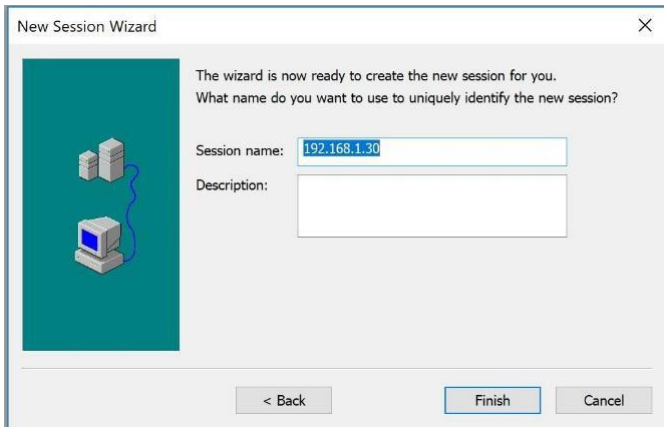
1. SecureCRTでNew Session Wizardを起動し、Nextをクリックします。



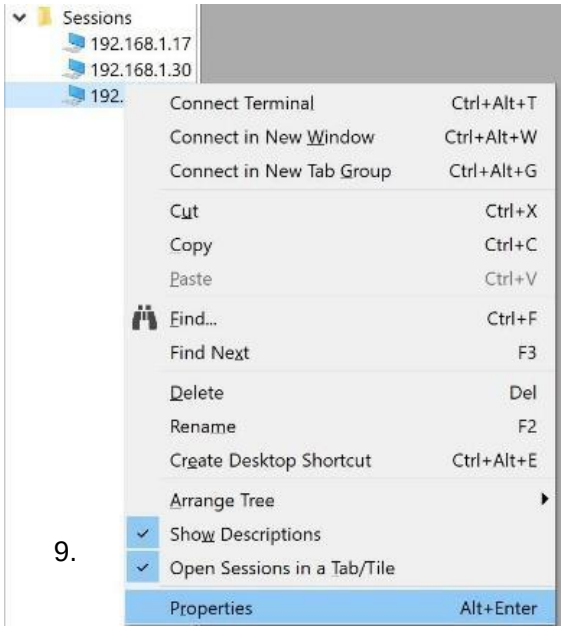
2. [Host Name]フィールドに、ONTAPのクラスタ管理IPアドレスまたはホスト名を入力します。



3. 一意のセッション名を入力し、[Finish]をクリックします。

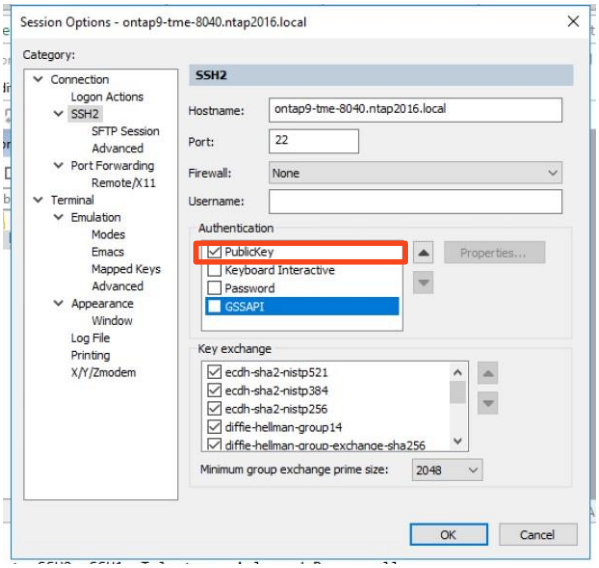


4. [Sessions]ペインで、作成したセッションを右クリックし、[Properties]を選択します。

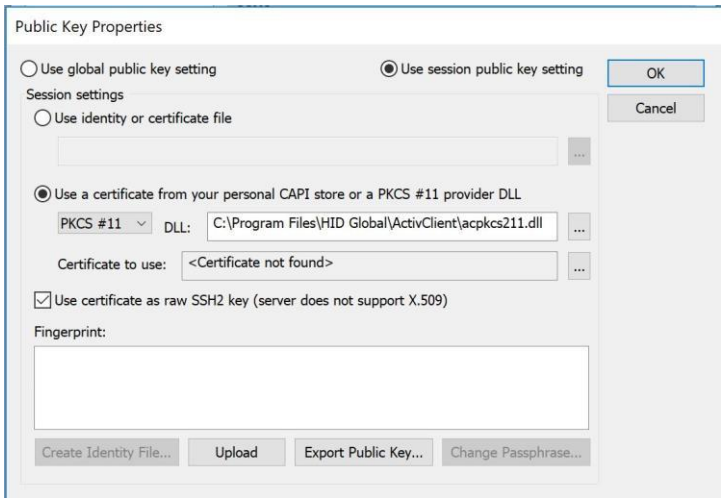


9.

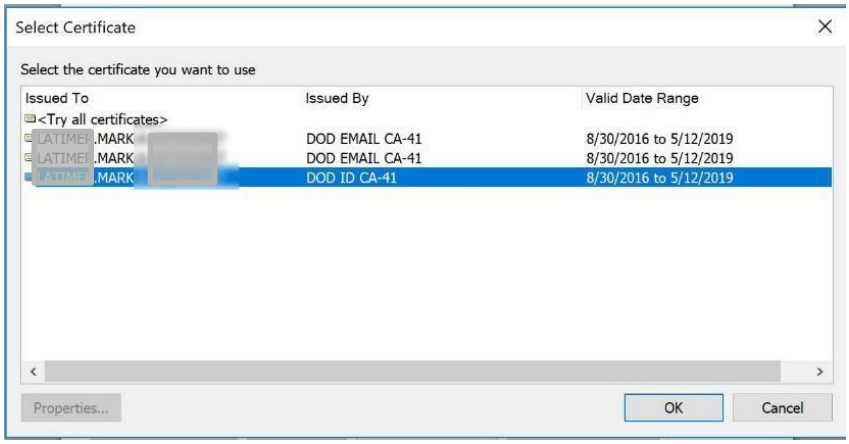
5. [Connection]ペインで、[SSH2]を選択します。右側のペインの[Authentication]セクションで、[PublicKey]以外のすべての項目をオフにします。[PublicKey]をハイライトし、[プロパティ]をクリックします。



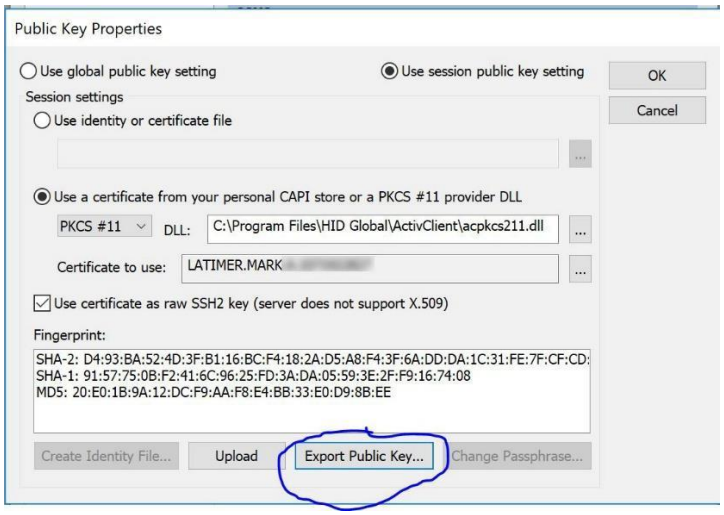
6. Use Session Public Key Setting and PKCS #11を選択します。`acpkcs211.dll` ActivClient のインストールディレクトリでファイルを参照します。（バージョンによっては、`c:\windows\system32` ディレクトリに配置されている場合があります）。



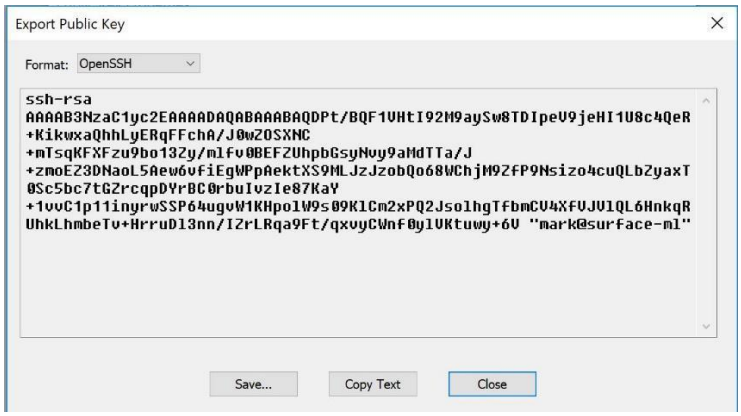
7. [使用する証明書の選択]で、DoD ID証明書を選択し、[OK]をクリックします。



8. [Use Certificate as Raw SSH2 Key]チェックボックスをオンにして、[Export Public Key]をクリックします。



9. [テキストのコピー]ボタンをクリックし、[閉じる]をクリックします。



10. 手順9のクリップボードの内容をテキストエディタに貼り付け、引用符で囲んだ最後のビット（名前、コンピュータ名）を削除して、公開鍵をコピーします。
11. [閉じる]をクリックし、[OK]をクリックしてから、もう一度[OK]をクリックします。
12. ONTAPで公開鍵認証方式を使用して管理者ユーザを作成します。

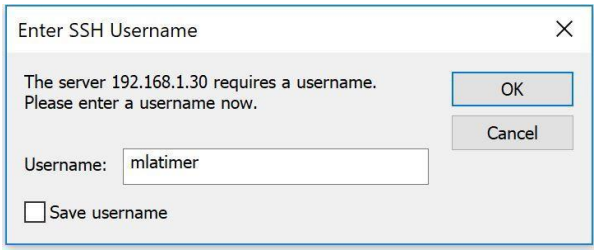
```
security login create -user-or-group-name <username> -application ssh -authentication-method
publickey

Warning: For successful authentication, ensure you create a public key for user "<username>"
using
"security login publickey create" interface.
```

13. 手順10でコピーした公開鍵を、引用符で囲んだ公開鍵を `-publickey` フィールドに貼り付けて、作成したadminユーザに関連付けます。

```
security login publickey create -username <username> -index 0 -publickey "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDBh8mgwjshX4P3oXw8Qd+s1p2jW8K73mw8ubYhvb+Alx4ZM9T0QmsmYTtFjQQ+bDbp6
ruqjjoO8hjl+WSVuxUwW5xWRUwYS/rtQmhP/2fudSncwd2cuRxMvMHKSruF8ee2WRTjO7vu7f4akrCfQL9cOhzh3dEHuFR5qo
OgCgr5nq8v3mZpAyoK7C4/uC9Lr8UO3mBctZ6pBfHLnQRCWgxc20FDFI4pM9Lz93fSIQXCCL8xrpCzi0bzH+4Dwug1gPJsrfS
a7Ki3s1SfNtiAWVqSh78D4iHYT8XjJr1TGVjsvZLg0/UUpwx5nvcRBWME9EczWi623tPO5fsUSGhQtCPn" -vserver
<admin vserver name>
```

14. SecureCRTで、作成したセッションを開きます。[SSHユーザ名の入力]ボックスに、ONTAPで作成したアカウントのユーザ名を入力します。



15. [Enter Secure Shell Passphrase]ボックスに、トークンPIN番号を入力します。

3 免責事項

NetAppは、本ドキュメントで提供されるいかなる情報または推奨事項の正確性、信頼性、有用性についても、または本ドキュメントで提供されるいかなる情報の使用または推奨事項の順守による結果についても、表明または保証は一切行いません。本ドキュメントに記載された情報は現状のまま提供され、本ドキュメントに記載された情報の使用、または推奨事項や手法の実装は、お客様が評価してお客様の運用環境に統合できるかどうかに応じて、お客様の責任となります。本ドキュメントおよびここに記載の情報は、本ドキュメントに記載のNetApp製品のみに関連して使用できるものとします。

4 詳細情報の入手方法

- HID ActivID ActivClient
- GithubのPuTTY-CAC
- VandykeソフトウェアSecureCRT
- ONTAP 9管理者認証とRBACパワーガイド

5 お問い合わせ

本テクニカル レポートの品質向上について、ご意見をお寄せください。

連絡先は、docfeedback@netapp.com（英語）です。

ご連絡の際は、件名に「TECHNICAL REPORT xxxx

確認応答

この文書の発行に貢献したMark Latimerに感謝します。

本ドキュメントに記載されている製品や機能のバージョンがお客様の環境でサポートされるかどうかについては、NetApp サポート サイトで Interoperability Matrix Tool (IMT)を参照してください。NetApp IMT には、NetApp がサポートする構成を構築するために使用できる製品コンポーネントやバージョンが定義されています。サポートの可否は、お客様の実際のインストール環境が公表されている仕様に従っているかどうかによって異なります。

機械翻訳に関する免責事項

原文は英語で作成されました。英語と日本語訳の間に不一致がある場合には、英語の内容が優先されます。公式な情報については、本資料の英語版を参照してください。翻訳によって生じた矛盾や不一致は、法令の順守や施行に対していかなる拘束力も法的な効力も持ちません。

著作権に関する情報

商標に関する情報