



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 Tullegee
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 Tulleedge : 初版。 |

目次

| | |
|-----------------------------|--------------------|
| バージョン履歴 | 2 |
| 1 概要 | 3 |
| 2 構成 | 4 |
| 2.1 アクティブクライアント | 4 |
| 2.2 PuTTY-CAC | 4 |
| SecureCRT | 8 |
| 3 免責事項 | 12 |
| 4 詳細情報の入手方法 | 12 |
| 5 お問い合わせ | 12 |

1 概要

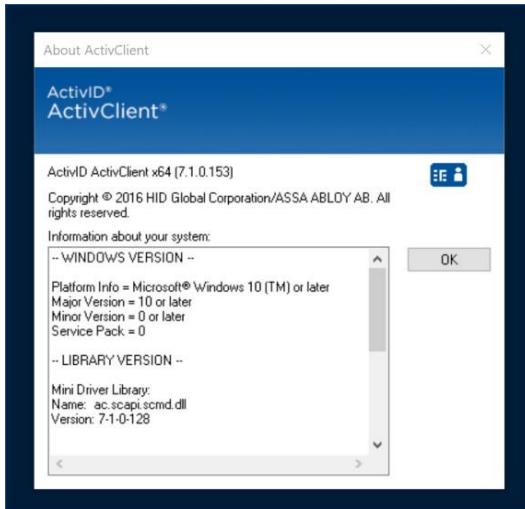
Common Access Card (CAC ; 共通アクセスカード) は、現役軍人、予備役兵、国防総省の民間人、および資格のある請負業者の従業員を対象とした「スマート」なIDカードです。CACには、スマート・カード・リーダーで読み取ることができるX.509証明書が保存されます。サードパーティ製セキュアシェル (SSH) クライアントPuTTY-CACおよびSecureCRTをActivClientソフトウェアと組み合わせて使用し、リーダーおよびCACにアクセスすることで、ONTAPストレージ管理者は、ONTAPで設定されている場合にCACに保存されている公開鍵を使用して認証できます。

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



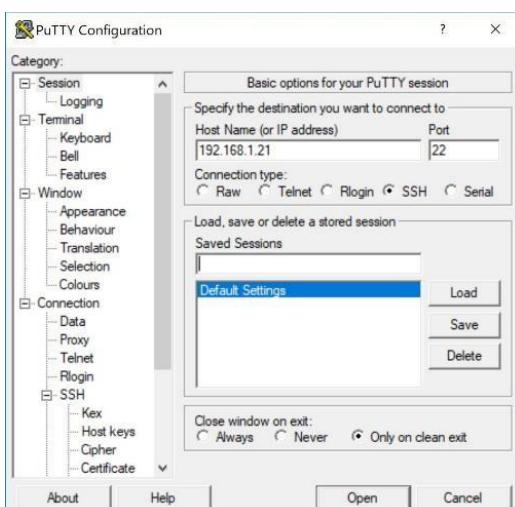
2.2 PuTTY-CAC

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。

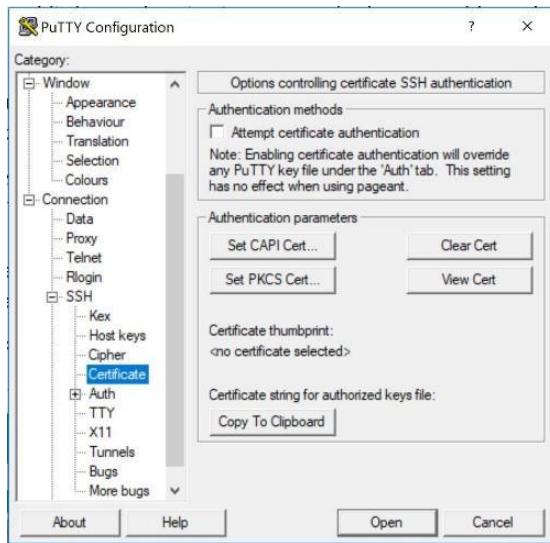
<https://github.com/NoMoreFood/putty-cac/releases>で入手できます。このレポートを検証するためには実行されたテストでは、セクション2.1で説明するActivClientとともにputtcac-64bit-0.70u4-installer.msiを使用しました。

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。



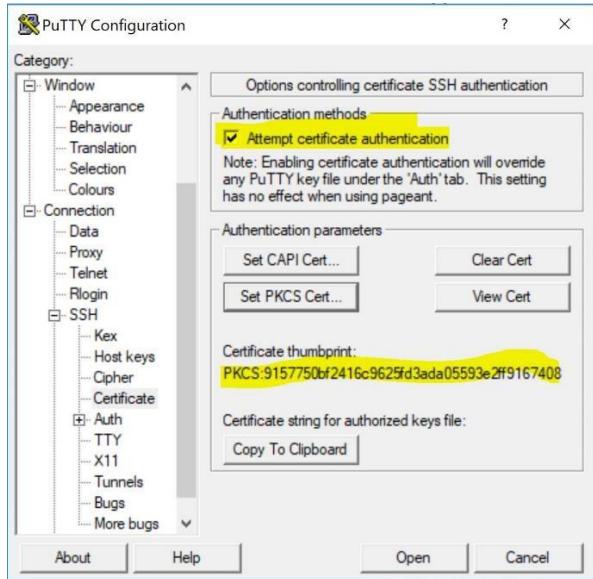
2. SSHを展開し、[Certificates]を選択します。次に、[PKCS証明書の設定]ボタンをクリックします。



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 でクリップボードにコピーします。

```
ssh-rsa
AAAAB3NzaC1yc2EAAAQABAAQDPt/BQFIVHT92M9aySw8TDIpeV9jeHIU8c4QeR+KikwxoQhhlyERqFFchA/J0wZOSXNC+mTsqKFxF zu9ho13Zy/m1fv0BEFZUhpbGsyNvy9aMdTTa/J+zmoEZ3DNAoL5Aew6vf:EgWPa
ektxS9MLJzJzobQo68NchjM9ZFPNsior4cuQlbZyaxT8Sc5b7tGzrcpdYr8C0rbuIVz1e87KaY4ivc1p11inyrwSPf64uvvW1khp0lW9s99K1Cm2xPQ2iso1hg1fbmCVXfV1V1Q16HnkqRuhkLhmbetvHrruD13nn/I2rl.R
qa9Ft/qxvyQwnf0y1Vktuwy+6V PKCS:9:157750bf2416c9625fd3ada05593e2ff9167408=C:\Program Files\HID Global\ActivClient\acpkcs211.d119157750bf2416c9625fd3ada05593e2ff9167408
CN=, OU=CONTRACTOR, OU=PKI, OU=DoD, O=U.S. Government, C=US
```

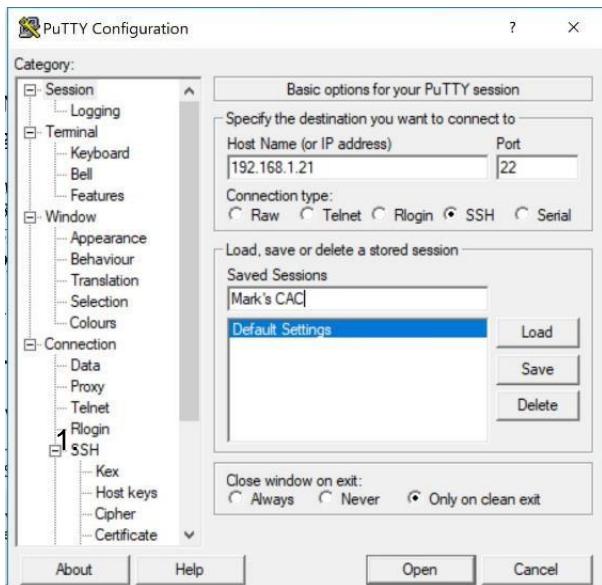
6. ONTAPで公開鍵認証方式を使用して管理者ユーザを作成します。

```
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
AAAAB3NzaC1yc2EAAAQABAAQDPt/BQFIVHT92M9aySw8TDIpeV9jeHIU8c4QeR+KikwxoQhhlyERqFFchA/J0wZOSXNC+mTsqKFxF zu9ho13Zy/m1fv0BEFZUhpbGsyNvy9aMdTTa/J+zmoEZ3DNAoL5Aew6vf:EgWPa
ektxS9MLJzJzobQo68NchjM9ZFPNsior4cuQlbZyaxT8Sc5b7tGzrcpdYr8C0rbuIVz1e87KaY4ivc1p11inyrwSPf64uvvW1khp0lW9s99K1Cm2xPQ2iso1hg1fbmCVXfV1V1Q16HnkqRuhkLhmbetvHrruD13nn/I2rl.R
qa9Ft/qxvyQwnf0y1Vktuwy+6V PKCS:9:157750bf2416c9625fd3ada05593e2ff9167408=C:\Program Files\HID Global\ActivClient\acpkcs211.d119157750bf2416c9625fd3ada05593e2ff9167408
<admin vserver name>" -vserver
```

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。

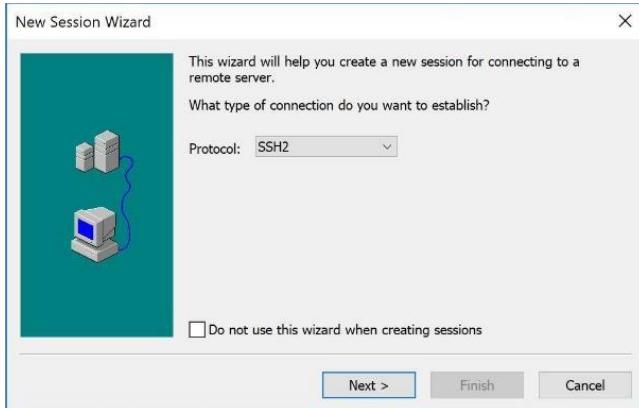


SecureCRT

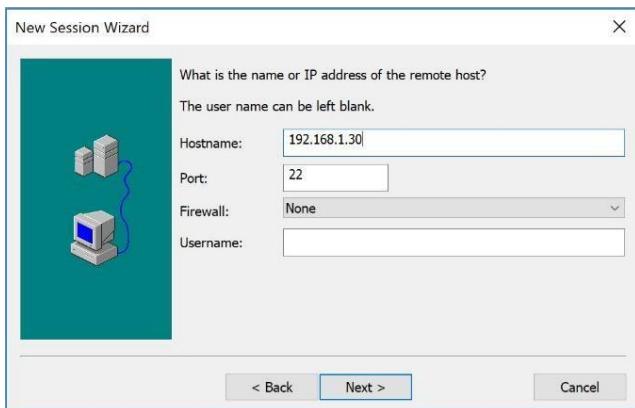
SecureCRTは、[VanDyke Software](#)から市販されているSSHクライアントです。このレポートを検証するために実行されたテストでは、セクション2.1で説明したActivClientとともにSecureCRT scrt833-x64.exeを使用しました。

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

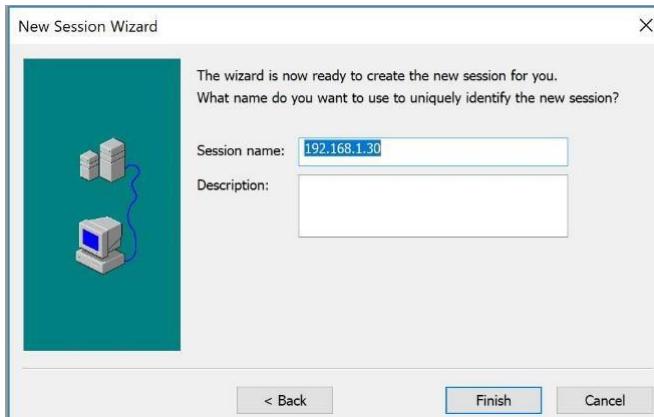
1. SecureCRTでNew Session Wizardを起動し、Nextをクリックします。



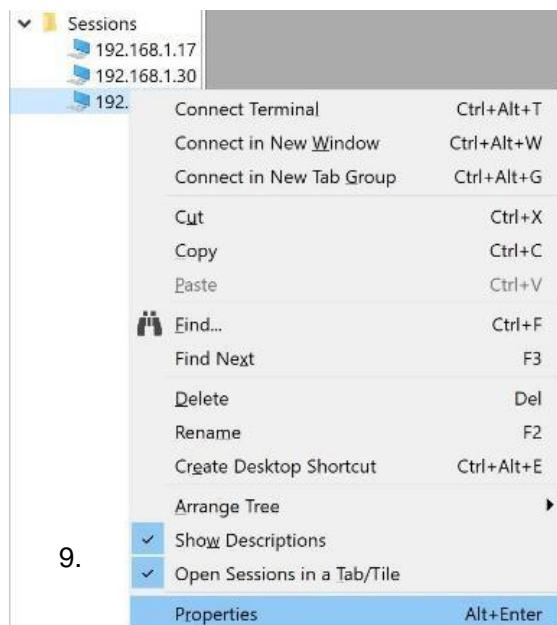
2. [Host Name]フィールドに、ONTAPのクラスタ管理IPアドレスまたはホスト名を入力します。



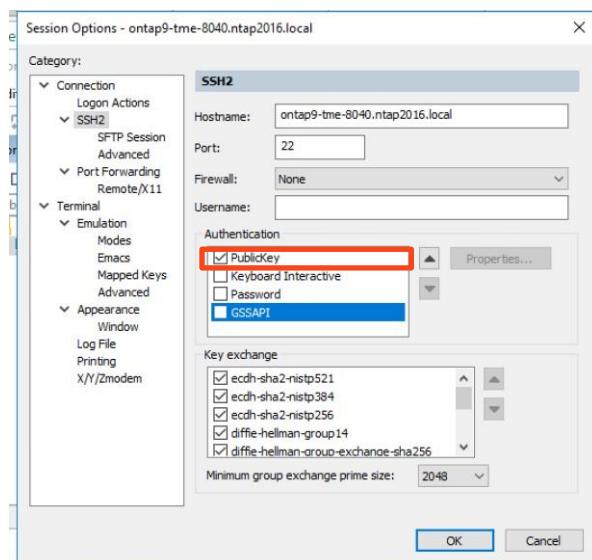
3. 一意のセッション名を入力し、[Finish]をクリックします。



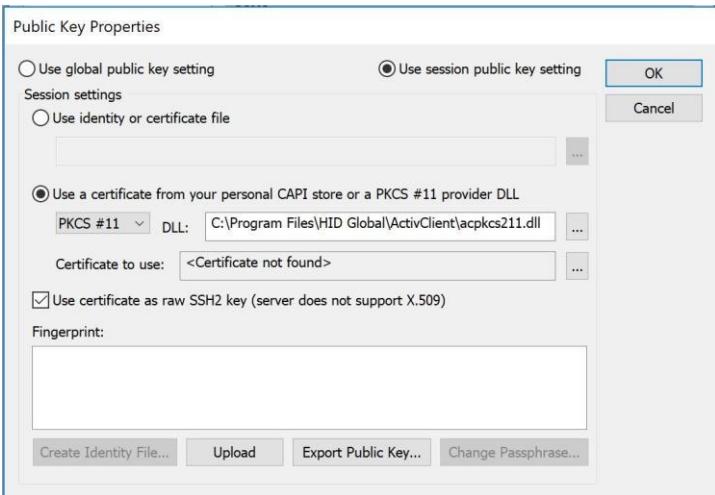
4. [Sessions]ペインで、作成したセッションを右クリックし、[Properties]を選択します。



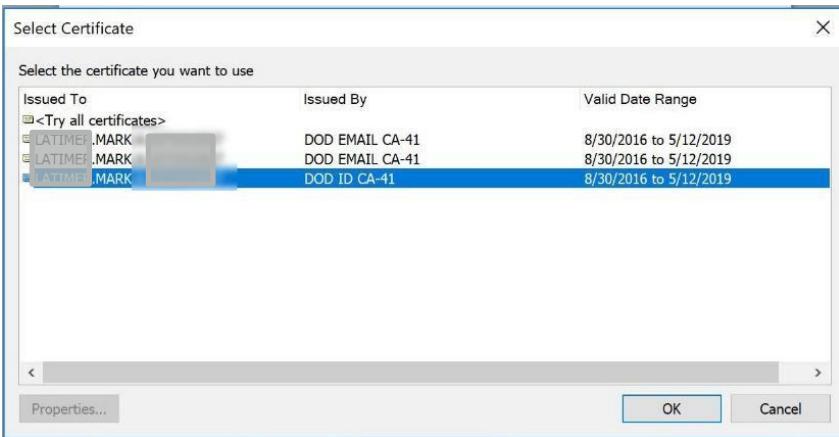
5. [Connection]ペインで、[SSH2]を選択します。右側のペインの[Authentication]セクションで、[PublicKey]以外のすべての項目をオフにします。[PublicKey]をハイライトし、[プロパティ]をクリックします。



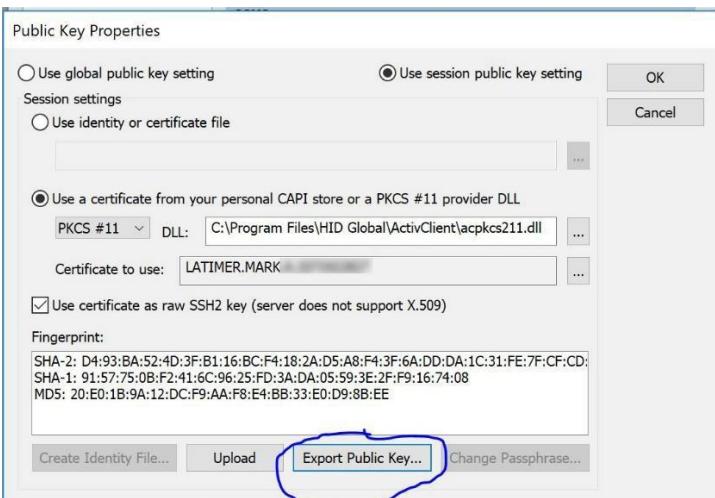
6. Use Session Public Key Setting and PKCS #11を選択します。acpkcs211.dll ActivClient のインストールディレクトリでファイルを参照します。（バージョンによっては、c:\windows\system32 ディレクトリに配置されている場合があります）。



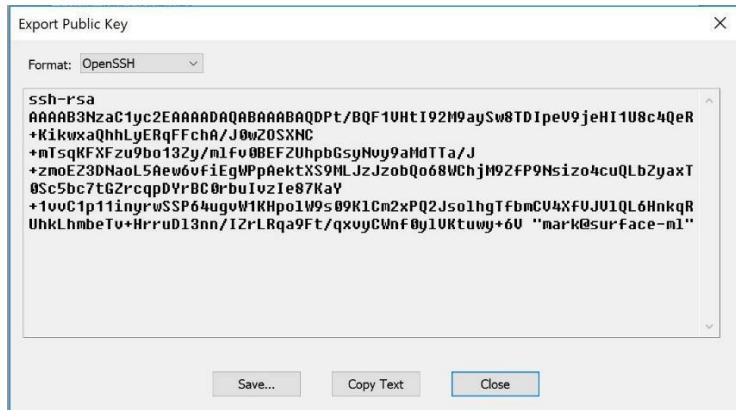
7. [使用する証明書の選択]で、DoD ID証明書を選択し、[OK]をクリックします。



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。

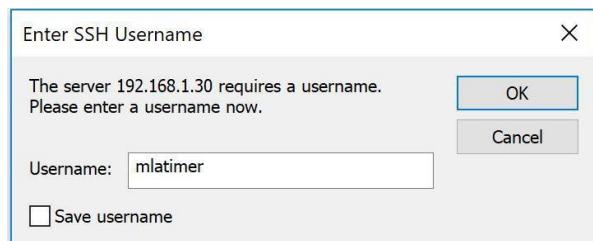
12. ONTAPで公開鍵認証方式を使用して管理者ユーザを作成します。

```
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.
```

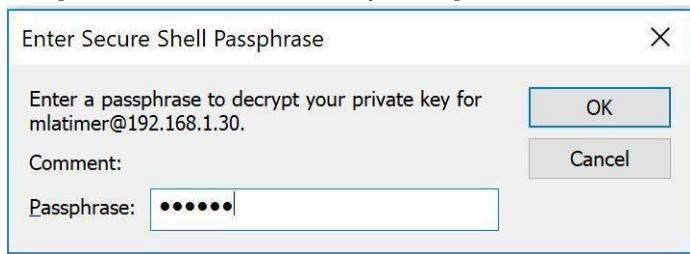
13. 手順10でコピーした公開鍵を、引用符で囲んだ公開鍵を -publickey フィールドに貼り付けて、作成したadminユーザに関連付けます。

```
security login publickey create -username <username> -index 0 -publickey "ssh-rsa
AAAAAB3NzaC1yc2EAAAQABAAQDBh8mgwjshX4P3oXw8Qd+s1p2jW8K73mw8ubYhvb+Alx4ZM9T0QmsmYTtFjQQ+bDbp6
ruqjjoO8hjl+WSVuxUwW5xWRUwYS/rQmhP/2fudSncwd2cuRxMvMHKSruF8ee2WRTj07vu7f4akrCfQL9cOhzh3dEHuFR5qo
OgCgr5nq8v3mZpAyok/C4/uC9Lr8U03mBtz6pBfHlnQRCWgxc20FDFI4pM9Lz93fsIQXCL8xrpCzi0bzH+4DwuglgPJsrfS
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す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

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

NetApp の著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、NetApp によって「現状のまま」提供されています。NetApp は明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。NetApp は、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

NetApp は、ここに記載されているすべての製品に対する変更を隨時、予告なく行う権利を保有します。NetApp による明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、NetApp は責任を負いません。この製品の使用または購入は、NetApp の特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許により保護されている場合があります。

本書に含まれるデータは市販の製品および / またはサービス (FAR 2.101 の定義に基づく) に関係し、データの所有権は NetApp, Inc. にあります。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc. の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b) 項で定められた権利のみが認められます。

商標に関する情報

NetApp、NetApp のロゴ、<https://www.netapp.com/company/legal/trademarks/> に記載されているマークは、NetApp, Inc. の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。