



NetApp April 24, 2024

This PDF was generated from https://docs.netapp.com/ja-jp/ontap/system-admin/access-serial-port-task.html on April 24, 2024. Always check docs.netapp.com for the latest.

目次

CLI を使用してクラスタにアクセスする(クラスタ管理者のみ) · · · · · · · · · · · · · · · · · · ·	1
シリアルポートを使用してクラスタにアクセスする	1
SSHを使用したクラスタへのアクセス	1
SSH ログインのセキュリティ	4
クラスタへの Telnet アクセスまたは RSH アクセスを有効にします · · · · · · · · · · · · · · · · · · ·	6
Telnet を使用してクラスタにアクセスします	6
RSH を使用してクラスタにアクセスします............................	8

CLI を使用してクラスタにアクセスする(クラスタ 管理者のみ)

シリアルポートを使用してクラスタにアクセスする

クラスタには、ノードのシリアルポートに接続されているコンソールから直接アクセス できます。

手順

1. コンソールで Enter キーを押します。

ログインプロンプトが表示されます。

2. ログインプロンプトで、次のいずれかを実行します。

クラスタにアクセスするアカウント	入力するアカウント名
デフォルトのクラスタアカウント	admin
別の管理ユーザアカウント	username

パスワードプロンプトが表示されます。

3. admin または管理ユーザアカウントのパスワードを入力し、 Enter キーを押します。

SSHを使用したクラスタへのアクセス

管理タスクを実行するために、クラスタへの問題 SSH 要求を行うことができます。SSHはデフォルトで有効になっています。

必要なもの

・を使用するように設定されたユーザアカウントが必要です ssh アクセス方法として。

。 -application のパラメータ security login コマンドは、ユーザアカウントのアクセス方法を指定します。。 security login "マニュアルページ" 追加情報 を含む。

- Active Directory(AD)のドメインユーザアカウントを使用してクラスタにアクセスする場合は、CIFS対応のStorage VMでクラスタの認証トンネルが設定されている必要があり、さらにADのドメインユーザアカウントが ssh アクセス方法としておよび domain を認証方法として指定します。
- IPv6 接続を使用する場合は、クラスタで IPv6 が設定されて有効になっている必要があります。また、フ ァイアウォールポリシーに IPv6 アドレスが設定されている必要があります。

。 network options ipv6 show IPv6が有効になっているかどうかを表示します。。 system services firewall policy show コマンドは、ファイアウォールポリシーを表示します。

このタスクについて

- OpenSSH 5.7 以降のクライアントを使用する必要があります。
- ・サポートされているプロトコルは SSH v2 だけです。 SSH v1 はサポートされていません。
- ONTAPでは、1つのノードで同時に最大64のSSHセッションがサポートされています。

クラスタ管理 LIF がノード上に存在する場合、クラスタ管理 LIF はこの制限をノード管理 LIF と共有します。

着信接続の速度が 1 秒あたり 10 を超えると、サービスは一時的に 60 秒間無効になります。

ONTAP は、 SSH に対して AES および 3DES 暗号化アルゴリズム(cipher とも呼ばれる)のみをサポートしています。

AES では、 128 ビット、 192 ビット、 256 ビットのキー長がサポートされます。3DES のキーの長さは DES 同様に 56 ビットですが、 3 回繰り返されます。

- FIPS モードが有効な場合、SSH クライアントを接続するには、 Elliptic Curve Digital Signature Algorithm (ECDSA)公開鍵アルゴリズムとネゴシエートする必要があります。
- ONTAP CLI に Windows ホストからアクセスする場合は、 PuTTY などのサードパーティのユーティリティを使用できます。
- Windows AD ユーザ名を使用して ONTAP にログインする場合、 ONTAP で AD ユーザ名とドメイン名が 作成されたときと同じように大文字と小文字を区別する必要があります。

AD のユーザ名とドメイン名では、大文字と小文字は区別されませんが、ただし、 ONTAP のユーザ名で は大文字と小文字が区別されます。ONTAP で作成されたユーザ名と、 AD で作成されたユーザ名の大文 字小文字表記が違うと、ログインに失敗します。

SSH認証オプション

• ONTAP 9.3以降では、を実行できます "SSH多要素認証を有効にします" ローカル管理者アカウントの場合。

SSH 多要素認証が有効な場合は、公開鍵とパスワードを使用してユーザが認証されます。

- ONTAP 9.4以降では、次のことが可能です "SSH多要素認証を有効にします" LDAPおよびNISのリモート ユーザ。
- ONTAP 9.13.1以降では、必要に応じてSSH認証プロセスに証明書の検証を追加して、ログインのセキュ リティを強化できます。これを行うには、"X.509証明書を公開鍵に関連付けます"アカウントが使用しま す。SSH公開鍵とX.509証明書の両方を使用してSSHを使用してログインすると、ONTAPは、SSH公開鍵 で認証する前にX.509証明書の有効性をチェックします。証明書の有効期限が切れているか失効している 場合、SSHログインは拒否され、SSH公開鍵は自動的に無効になります。
- ONTAP 9.14.1以降では、オプションでCisco Duo 2要素認証をSSH認証プロセスに追加して、ログインセキュリティを強化できます。Cisco Duo認証を有効にした後の最初のログイン時に、ユーザはSSHセッションのオーセンティケータとして機能するデバイスを登録する必要があります。を参照してください "SSHログイン用のCisco Duo 2FAの設定" ONTAPのCisco Duo SSH認証の設定の詳細については、を参照してください。

手順

1. 管理ホストで、を入力します ssh 次のいずれかの形式でコマンドを実行します。

° ssh username@hostname or IP [command]

° ssh -1 username hostname_or_IP [command]

ADドメインユーザアカウントを使用している場合は、を指定する必要があります username 形式はです domainname\\AD_accountname (ドメイン名のあとにバックスラッシュが2つ付いている場合)または "domainname\AD_accountname" (二重引用符で囲み、ドメイン名のあとにバックスラッシュ1つで囲みま す)。

*hostname_or_IP*は、クラスタ管理LIFまたはノード管理LIFのホスト名またはIPアドレスです。クラスタ管理LIFを使用することを推奨します。IPv4 または IPv6 アドレスを使用できます。

command SSHインタラクティブセッションでは必要ありません。

SSH要求の例

次の例は、「 joe 」という名前のユーザアカウントで、クラスタ管理 LIF が 10.72.137.28 のクラスタにアク セスする SSH 要求を問題で実行する方法を示しています。

\$ ssh joe@10.72.137.28
Password:
cluster1::> cluster show
Node Health Eligibility
----node1 true true
node2 true true
2 entries were displayed.

\$ ssh -l joe 10.72.137.28 cluster show
Password:
Node Health Eligibility
----node1 true true
node2 true true
2 entries were displayed.

次の例は、「 `DOMAIN1' 」という名前のドメインの「 John 」という名前のユーザアカウントが、クラスタ 管理 LIF が 10.72.137.28 であるクラスタにアクセスするための SSH 要求を問題で できることを示していま す。

```
$ ssh DOMAIN1\\john@10.72.137.28
Password:
cluster1::> cluster show
Node Health Eligibility
------
node1 true true
node2 true true
2 entries were displayed.
```

```
$ ssh -1 "DOMAIN1\john" 10.72.137.28 cluster show
Password:
Node Health Eligibility
------
node1 true true
node2 true true
2 entries were displayed.
```

次の例は、「 joe 」という名前のユーザアカウントで SSH MFA 要求を問題で実行し、クラスタ管理 LIF が 10.72.137.32 のクラスタにアクセスする方法を示しています。

```
$ ssh joe@10.72.137.32
Authenticated with partial success.
Password:
cluster1::> cluster show
Node Health Eligibility
-----
node1 true true
node2 true true
2 entries were displayed.
```

関連情報

"管理者認証と RBAC"

SSH ログインのセキュリティ

ONTAP 9.5 以降では、過去のログイン、失敗したログイン、および前回のログイン後に 適用された権限の変更内容に関する情報を表示できます。

セキュリティ関連の情報は、 SSH admin ユーザとしてログインしたときに表示されます。次の条件に関する アラートが表示されます。

• 最後にアカウント名がログインされた時刻。

- ・前回のログイン成功後にログインに失敗した回数。
- 前回のログイン後にロールに変更があったかどうか(管理者アカウントのロールが「admin」から「 backup」に変更された場合など)。
- 前回のログイン後にロールの追加、変更、または削除機能を変更したかどうか。

(i) 疑わしい情報が表示された場合は、ただちにセキュリティ部門に連絡してください。

ログイン時にこの情報を取得するには、次の前提条件を満たしている必要があります。

- SSH ユーザアカウントが ONTAP でプロビジョニングされている必要があります。
- SSH セキュリティログインが作成されている必要があります。
- ・ログインに成功する必要があります。

SSH ログインのセキュリティに関する制限事項とその他の考慮事項

SSH ログインのセキュリティ情報には、次の制限事項および考慮事項が適用されます。

- この情報は、 SSH ベースのログインについてのみ表示されます。
- LDAP / NIS や AD アカウントなどのグループベースの管理者アカウントの場合、ユーザは、メンバーであ るグループが ONTAP で管理者アカウントとしてプロビジョニングされている場合、 SSH ログイン情報 を表示できます。

ただし、これらのユーザについては、ユーザアカウントのロールへの変更に関するアラートを表示することはできません。また、 ONTAP で管理者アカウントとしてプロビジョニングされた AD グループに属するユーザは、前回のログイン後にログインに失敗した回数は表示できません。

- ・ユーザについての情報は、 ONTAP からユーザアカウントが削除されると削除されます。
- ・SSH 以外のアプリケーションへの接続に関する情報は表示されません。

SSH ログインのセキュリティ情報の例

次の例は、ログイン後に表示される情報の種類を示しています。

このメッセージは、ログインに成功するたびに表示されます。

Last Login : 7/19/2018 06:11:32

・前回のログインに失敗したログインがあった場合、次のメッセージが表示されます。

```
Last Login : 4/12/2018 08:21:26
Unsuccessful login attempts since last login - 5
```

前回のログイン後に失敗したログインがあり、権限が変更されている場合、次のメッセージが表示されます。

Last Login : 8/22/2018 20:08:21 Unsuccessful login attempts since last login - 3 Your privileges have changed since last login

クラスタへの Telnet アクセスまたは RSH アクセスを有効にし ます

セキュリティのベストプラクティスとして、事前定義された管理ファイアウォールポリ シーではTelnetとRSHは無効にしています (mgmt)。クラスタが Telnet 要求または RSH 要求を受け入れることができるようにするには、 Telnet または RSH を有効にした新し い管理ファイアウォールポリシーを作成し、その新しいポリシーをクラスタ管理 LIF に 関連付ける必要があります。

このタスクについて

ONTAP では、事前定義されているファイアウォールポリシーは変更できませんが、事前定義されているファ イアウォールポリシーをクローニングして新しいポリシーを作成することもできます mgmt ファイアウォール ポリシーを管理し、新しいポリシーでTelnetまたはRSHを有効にします。ただし、 Telnet および RSH はセキ ュアなプロトコルではないため、 SSH を使用してクラスタにアクセスすることを検討してください。SSH は、セキュアなリモートシェルと対話型のネットワークセッションを提供します。

クラスタへの Telnet アクセスまたは RSH アクセスを有効にするには、次の手順を実行します。

手順

1. advanced 権限モードに切り替えます。

set advanced

- セキュリティプロトコル(RSH または Telnet)を有効にします。
 security protocol modify -application security_protocol -enabled true
- に基づいて新しい管理ファイアウォールポリシーを作成します mgmt 管理ファイアウォールポリシー: system services firewall policy clone -policy mgmt -destination-policy policyname
- 新しい管理ファイアウォールポリシーで Telnet または RSH を有効にします。
 system services firewall policy create -policy policy-name -service security_protocol -action allow -ip-list ip_address/netmask
 すべてのIPアドレスを許可するには、と指定する必要があります -ip-list 0.0.0.0/0
- 新しいポリシーをクラスタ管理 LIF に関連付けます。
 network interface modify -vserver cluster_management_LIF -lif cluster_mgmt
 -firewall-policy policy-name

Telnet を使用してクラスタにアクセスします

管理タスクを実行するために、クラスタへの問題 Telnet 要求を行うことができま す。Telnet はデフォルトでは無効になっています。 必要なもの

Telnet を使用してクラスタにアクセスするには、次の条件を満たしている必要があります。

 アクセス方法として Telnet を使用するように設定されたクラスタローカルユーザアカウントを持っている 必要があります。

。 -application のパラメータ security login コマンドは、ユーザアカウントのアクセス方法を指定します。詳細については、を参照してください security login マニュアルページ

Telnet 要求がファイアウォールを通過できるように、クラスタ管理 LIF またはノード管理 LIF によって使用される管理ファイアウォールポリシーで Telnet が有効になっている必要があります。

デフォルトでは、Telnet は無効になっています。。 system services firewall policy show コマ ンドにを指定します -service telnet パラメータは、ファイアウォールポリシーでTelnetが有効になっ ているかどうかを表示します。詳細については、を参照してください system services firewall policy マニュアルページ

IPv6 接続を使用する場合は、クラスタで IPv6 が設定されて有効になっている必要があります。また、ファイアウォールポリシーに IPv6 アドレスが設定されている必要があります。

。 network options ipv6 show IPv6が有効になっているかどうかを表示します。。 system services firewall policy show コマンドは、ファイアウォールポリシーを表示します。

このタスクについて

• Telnet はセキュアなプロトコルではありません。

クラスタにアクセスするときは、 SSH を使用することを検討してください。SSH は、セキュアなリモー トシェルと対話型のネットワークセッションを提供します。

・ONTAP では、1つのノードについて同時に最大 50 の Telnet セッションがサポートされています。

クラスタ管理 LIF がノード上に存在する場合、クラスタ管理 LIF はこの制限をノード管理 LIF と共有しま す。

着信接続数が1秒あたり10を超えると、サービスは一時的に60秒間無効になります。

ONTAP CLI に Windows ホストからアクセスする場合は、 PuTTY などのサードパーティのユーティリティを使用できます。

手順

1. 管理ホストで次のコマンドを入力します。

telnet hostname_or_IP

*hostname_or_IP*は、クラスタ管理LIFまたはノード管理LIFのホスト名またはIPアドレスです。クラス タ管理 LIF を使用することを推奨します。IPv4 または IPv6 アドレスを使用できます。

Telnet要求の例

次の例は、 Telnet アクセスを使用するように設定された「 joe 」というユーザが、クラスタ管理 LIF が 10.72.137.28 であるクラスタにアクセスする Telnet 要求を問題に送信する方法を示しています。

admin_host\$ telnet 10.72.137.28
Data ONTAP
login: joe
Password:
cluster1::>

RSH を使用してクラスタにアクセスします

クラスタへの問題 RSH 要求を使用して、管理タスクを実行できます。RSH はセキュア なプロトコルではなく、デフォルトでは無効になっています。

必要なもの

RSH を使用してクラスタにアクセスするには、次の条件を満たしている必要があります。

アクセス方法として RSH を使用するように設定された、クラスタのローカルユーザアカウントを持っている必要があります。

。 -application のパラメータ security login コマンドは、ユーザアカウントのアクセス方法を指定します。詳細については、を参照してください security login マニュアルページ

 RSH 要求がファイアウォールを通過できるように、クラスタ管理 LIF またはノード管理 LIF によって使用 される管理ファイアウォールポリシーで RSH がすでに有効になっている必要があります。

デフォルトでは、RSHは無効になっています。。 system services firewall policy show コマン ドにを指定します -service rsh パラメータは、ファイアウォールポリシーでRSHが有効になっている かどうかを表示します。詳細については、を参照してください system services firewall policy マニュアルページ

IPv6 接続を使用する場合は、クラスタで IPv6 が設定されて有効になっている必要があります。また、ファイアウォールポリシーに IPv6 アドレスが設定されている必要があります。

。 network options ipv6 show IPv6が有効になっているかどうかを表示します。。 system services firewall policy show コマンドは、ファイアウォールポリシーを表示します。

このタスクについて

• RSH はセキュアなプロトコルではありません。

クラスタにアクセスするときは、 SSH を使用することを検討してください。SSH は、セキュアなリモートシェルと対話型のネットワークセッションを提供します。

・ONTAP では、1つのノードについて同時に最大 50 の RSH セッションがサポートされています。

クラスタ管理 LIF がノード上に存在する場合、クラスタ管理 LIF はこの制限をノード管理 LIF と共有しま す。

着信接続数が 1 秒あたり 10 を超えると、サービスは一時的に 60 秒間無効になります。

手順

1. 管理ホストで次のコマンドを入力します。

rsh hostname_or_IP -1 username:passwordcommand

*hostname_or_IP*は、クラスタ管理LIFまたはノード管理LIFのホスト名またはIPアドレスです。クラス タ管理 LIF を使用することを推奨します。IPv4 または IPv6 アドレスを使用できます。

commandは、RSH経由で実行するコマンドです。

RSH要求の例

次の例は、RSHアクセスを使用するように設定された「joe」というユーザが、を実行するRSH要求を問題 で 処理する方法を示しています cluster show コマンドを実行します

admin_host\$ rsh 10.72.137.28 -1 joe:password cluster show Node Health Eligibility -----node1 true true node2 true true 2 entries were displayed. admin_host\$ 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。

ネットアップ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、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保 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。ネットアップは、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 れていたとしても、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。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。 ネットアップ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、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップ 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って保護されている場合があります。

権利の制限について:政府による使用、複製、開示は、DFARS 252.227-7013(2014年2月)およびFAR 5252.227-19(2007年12月)のRights in Technical Data -Noncommercial Items(技術データ - 非商用品目に関 する諸権利)条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス(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。本契約に基づき提供されるすべてのネットアップの技術データおよび コンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。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(2014年2月)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、http://www.netapp.com/TM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。