CLIを使用したクラスタへのアクセス（クラスタ管理者のみ）

ONTAP 9

NetApp
December 20, 2024

目次

CLIを使用したクラスタへのアクセス（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た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
テフオルトノ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

ONTAPクラスタにSSH要求を発行して管理タスクを実行できます。SSHはデフォルトで有効になっています。

開始する前に

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

  コマンドのパラメータ[`security login`は、 `-application`ユーザアカウントのアクセス方法を指定します。リンクの詳細については、ONTAPコマンドリファレンスを参照してください。https://docs NetApp .com /us-en/ ONTAP -cli/security-login-create.html#description^][`security login`コマンドを参照してください。

- 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アクセス方式および `domain`認証方式としてを使用してクラスタに追加されている必要があり`ssh`ます。

タスクの内容

- 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がノード上にある場合、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。

  着信接続のレートが1秒あたり10を超える場合、サービスは60秒間一時的に無効になります。

- 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は、128ビット、192ビット、および256ビットのキー長でサポートされます。3DESのキー長は元のDESと同様に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。
- WindowsホストからONTAP CLIに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は、ONTAPでADユーザ名とドメイン名が作成されたときと同じ大文字または小文字を使用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。ただし、ONTAP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一致しないと、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、ローカル管理者アカウントを使用できます"SSH多要素認証を有効にします"。

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

- ONTAP 9 .4以降では、LDAPおよびNISのリモートユーザに対応できます"SSH多要素認証を有効にします"。
- 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、ONTAP管理者はログインセキュリティを強化できます"SSH認証プロセスへのCisco Duo 2要素認証の追加"。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。
- ONTAP 9 .15.1以降では、管理者は、ユーザの信頼スコアに基づいて、SSHユーザに追加の適応認証を提供でき"動的許可の設定"ます。

手順

1. ONTAPクラスタのネットワークにアクセスできるホストから、次のいずれかの形式でコマンドを入力し`ssh`ます。

   - **ssh *username@hostname_or_IP* [*command*]**
   - **ssh -l *username hostname_or_IP* [*command*]**

ADのドメインユーザアカウントを使用している場合は、（ドメイン名のあとにバックスラッシュ2つ）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）の形式で *domainname\\AD_accountname*`指定する必要があります `*username*。

`*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 -l "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

"カンリシヤニンシヨウト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のPrivilegesに対する変更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場合に表示されます。次の状態に関するアラートが表示されます。

- アカウント名が最後に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が変更されたかどうか（admin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、または削除機能が変更されたかどうか。

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およびその他の考慮事項

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

- この情報は、SSHベースのログインの場合にのみ表示されます。
- グループベースの管理者アカウント（LDAP / NISおよびADアカウントなど）の場合、自分が属しているグループが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れば、ユーザは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の変更に関するアラートを表示できません。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、前回のログイン以降にログインに失敗した回数を表示できません。
- ユーザについて保持されている情報は、ユーザアカウントがONTAPから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。

- 次のメッセージは、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
```

- 前回のログインに成功してからログインに失敗した場合は、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アクセスを有効にする

セキュリティのベストプラクティスとして、TelnetとRSHはデフォルトで無効になっています。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、デフォルトの管理サービスポリシーでサービスを有効にする必要があります。

TelnetとRSHはセキュアなプロトコルではありません。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および対話型ネットワークセッションを提供します。詳細については、を参照してください "SSHを使用したクラスタへのアクセス"。

タスクの内容

- ONTAPでは、1つのノードで同時に最大50のTelnetセッションまたはRSHセッションがサポートされます。

  クラスタ管理LIFがノード上にある場合、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。

  着信接続のレートが1秒あたり10を超える場合、サービスは60秒間一時的に無効になります。

- rshコマンドにはadvanced権限が必要です。

ONTAP 9 .10.1以降

手順

1. RSHまたはTelnetセキュリティプロトコルが有効になっていることを確認します。

   ```
   security protocol show
   ```

   a. RSHまたはTelnetセキュリティプロトコルが有効になっている場合は、次の手順に進みます。

   b. RSHまたはTelnetセキュリティプロトコルが有効になっていない場合は、次のコマンドを使用して有効にします。

      ```
      security protocol modify -application <rsh/telnet> -enabled true
      ```

2. またはサービスが管理LIFに存在することを確認し `management-rsh-server` `management-telnet-server` ます。

   ```
   network interface show -services management-rsh-server
   ```

   または

   ```
   network interface show -services management-telnet-server
   ```

   a. またはサービスが存在する場合は `management-rsh-server` `management-telnet-server` 、次の手順に進みます。

   b. またはサービスが存在しない場合は `management-rsh-server` `management-telnet-server` 、次のコマンドを使用して追加します。

      ```
      network interface service-policy add-service -vserver cluster1 -policy
      default-management -service management-rsh-server
      ```

   ```
   network interface service-policy add-service -vserver cluster1 -policy
   default-management -service management-telnet-server
   ```

ONTAP 9 .9以前

タスクの内容

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`mgmt`管理ファイアウォールポリシーをクローニングし、そのポリシーでTelnetまたはRSHを有効にすることで、新しいポリシーを作成できます。

手順

1. advanced権限モードに切り替えます。

   ```
   set advanced
   ```

2. 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
   ```

3. `mgmt`管理ファイアウォールポリシー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。

```
system services firewall policy clone -policy mgmt -destination-policy
policy-name
```

4. 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、次のように指定します。 `-ip-list 0.0.0.0/0`

5. 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 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。

TelnetとRSHはセキュアなプロトコルではありません。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および対話型ネットワークセッションを提供します。詳細については、を参照してください "SSHを使用したクラスタへのアクセス"。

開始する前に

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。

  コマンドのパラメータ `security login`は、 `-application`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、 `security login`のマニュアルページを参照してください。

タスクの内容

- 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がノード上にある場合、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。

- WindowsホストからONTAP CLIに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。
- rshコマンドにはadvanced権限が必要です。

ONTAP 9 .10.1以降

手順

1. Telnetセキュリティプロトコルが有効になっていることを確認します。

   ```
   security protocol show
   ```

   a. Telnetセキュリティプロトコルが有効になっている場合は、次の手順に進みます。

   b. Telnetセキュリティプロトコルが有効になっていない場合は、次のコマンドを使用して有効にします。

      ```
      security protocol modify -application telnet -enabled true
      ```

2. 管理LIFにサービスが存在することを確認し `management-telnet-server` ます。

   ```
   network interface show -services management-telnet-server
   ```

   a. サービスが存在する場合は `management-telnet-server` 、次の手順に進みます。

   b. サービスが存在しない場合は `management-telnet-server` 、次のコマンドを使用して追加します。

      ```
      network interface service-policy add-service -vserver cluster1 -policy
      default-management -service management-telnet-server
      ```

ONTAP 9 .9以前

開始する前に

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。

- 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`コマンドで `-service telnet`パラメータを指定すると、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が表示されます。詳細については、 `system services firewall policy`のマニュアルページを参照してください。

- 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、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`コマンドは、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。

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のクラスタにアクセスするためのTelnet要求を発行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を使用したクラスタへのアクセス

クラスタに対してRSH要求を発行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。

TelnetとRSHはセキュアなプロトコルではありません。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および対話型ネットワークセッションを提供します。詳細については、を参照してください "SSHを使用したクラスタへのアクセス"。

開始する前に

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。

  コマンドのパラメータ `security login`は、 `-application`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、 `security login`のマニュアルページを参照してください。

タスクの内容

- ONTAPでは、1つのノードで同時に最大50のRSHセッションがサポートされます。

  クラスタ管理LIFがノード上にある場合、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。

  着信接続のレートが1秒あたり10を超える場合、サービスは60秒間一時的に無効になります。

- rshコマンドにはadvanced権限が必要です。

ONTAP 9 .10.1以降

手順

1. RSHセキュリティプロトコルが有効になっていることを確認します。

   ```
   security protocol show
   ```

   a. RSHセキュリティプロトコルが有効になっている場合は、次の手順に進みます。

   b. RSHセキュリティプロトコルが有効になっていない場合は、次のコマンドを使用して有効にします。

      ```
      security protocol modify -application rsh -enabled true
      ```

2. 管理LIFにサービスが存在することを確認し `management-rsh-server` ます。

   ```
   network interface show -services management-rsh-server
   ```

   a. サービスが存在する場合は `management-rsh-server` 、次の手順に進みます。

   b. サービスが存在しない場合は `management-rsh-server` 、次のコマンドを使用して追加します。

      ```
      network interface service-policy add-service -vserver cluster1 -policy
      default-management -service management-rsh-server
      ```

ONTAP 9 .9以前

開始する前に

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。

- 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。 `-service rsh`パラメータを指定してsystem services firewall policy showコマンドを実行すると、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が表示されます。詳細については、 `system services firewall policy`のマニュアルページを参照してください。

- 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、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`コマンドは、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。

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 -l 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、コマンドを実行するRSH要求を発行する方法を示してい `cluster show`ます。

```
admin_host$ rsh 10.72.137.28 -l joe:password cluster show

Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.

admin_host$
```

著作権に関する情報

商標に関する情報