Hyper-V over SMBおよびSQL Server over SMBでノンストップオペレーションを実現するためのONTAP設定

ONTAP 9

NetApp
February 12, 2026

目次

Hyper-V over SMBおよびSQL Server over SMBでノンストップ オペレーションを実現するためのONTAP設定

Hyper-V over SMBおよびSQL Server over SMBでノンストップ オペレーションを実現するためのONTAP設定 - 概要

SMBを介したノンストップ オペレーションを実現するHyper-VおよびSQL Server環境を使用するためには、ONTAPのさまざまな設定手順を実行する必要があります。

Hyper-V over SMBおよびSQL Server over SMBでノンストップ オペレーションを実現するようONTAPを設定する前に、次の作業を完了する必要があります。

- クラスタでタイム サービスをセットアップします。
- SVM用のネットワークをセットアップします。
- SVMを作成します。
- SVMでデータLIFインターフェイスを設定します。
- SVMでDNSを設定します。
- SVMに必要なネーム サービスをセットアップします。
- SMBサーバを作成します。

関連情報

Hyper-VまたはSQL Server over SMB構成の計画

設定要件と考慮事項

Kerberos認証およびNTLMv2認証の許可の確認（Hyper-V over SMB共有）

Hyper-V over SMBのノンストップオペレーションでは、データSVM上のCIFSサーバとHyper-VサーバでKerberos認証とNTLMv2認証の両方が許可されている必要があります。CIFSサーバとHyper-Vサーバの両方で、許可される認証方法を制御する設定を確認する必要があります。

タスク概要

継続的な可用性を実現する共有接続を確立するには、Kerberos認証が必要です。リモートVSSプロセスの一部ではNTLMv2認証が使用されます。そのため、Hyper-V over SMB構成では、両方の認証方法を使用した接続をサポートする必要があります。

Kerberos 認証と NTLMv2 認証の両方を許可するには、次の設定を構成する必要があります：

- ストレージ仮想マシン（SVM）で SMB のエクスポート ポリシーを無効にする必要があります。

SVM では Kerberos 認証と NTLMv2 認証の両方が常に有効になっていますが、エクスポート ポリシーを使用して認証方法に基づいてアクセスを制限できます。

SMBのエクスポート ポリシーはオプションであり、デフォルトでは無効になっています。エクスポート ポリシーが無効になっている場合、CIFSサーバではKerberos認証とNTLMv2認証の両方がデフォルトで許可されます。

- CIFS サーバーと Hyper-V サーバーが属するドメインは、Kerberos 認証と NTLMv2 認証の両方を許可する必要があります。

Active Directoryドメインでは、Kerberos認証がデフォルトで有効になっています。ただし、Security Policy設定またはGroup Policiesを使用して、NTLMv2認証を無効にできます。

手順

1. SVM でエクスポート ポリシーが無効になっていることを確認するには、次の手順を実行します：
   a. 権限レベルをadvancedに設定します。

      set -privilege advanced

   b. `-is-exportpolicy-enabled` CIFS サーバー オプションが `false`に設定されていることを確認します：

      vserver cifs options show -vserver *vserver_name* -fields vserver,is-exportpolicy-enabled

   c. admin権限レベルに戻ります。

      set -privilege admin

2. SMB のエクスポート ポリシーが無効になっていない場合は、無効にします：

   vserver cifs options modify -vserver *vserver_name* -is-exportpolicy-enabled false

3. ドメインで NTLMv2 認証と Kerberos 認証の両方が許可されていることを確認します。

   ドメインで許可されている認証方法を確認する方法については、Microsoft TechNetライブラリを参照してください。

4. ドメインが NTLMv2 認証を許可していない場合は、Microsoft のドキュメントに記載されているいずれかの方法を使用して NTLMv2 認証を有効にします。

例

次のコマンドは、SVM vs1でSMBのエクスポート ポリシーが無効になっていることを確認します。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields vserver,is-
exportpolicy-enabled

vserver  is-exportpolicy-enabled
-------- ------------------------
vs1      false

cluster1::*> set -privilege admin
```

ドメイン アカウントがONTAPのデフォルトUNIXユーザにマッピングされていることを確認します

Hyper-V と SQL Server は、継続的に利用可能な共有への SMB 接続を確立するためにドメインアカウントを使用します。接続を正常に確立するには、コンピューターアカウントを UNIX ユーザーに正しくマッピングする必要があります。これを実現する最も簡単な方法は、コンピューターアカウントをデフォルトの UNIX ユーザーにマッピングすることです。

タスク概要

Hyper-V と SQL Server は、SMB 接続を作成するためにドメイン コンピュータ アカウントを使用します。さらに、SQL Server は、SMB 接続を作成するサービス アカウントとしてドメイン ユーザー アカウントも使用します。

ストレージ仮想マシン（SVM）を作成すると、ONTAPは自動的に `pcuser`という名前のデフォルトユーザ（`UID`は `65534`）と `pcuser`という名前のグループ（`GID`は `65534`）を作成し、そのデフォルトユーザを `pcuser`グループに追加します。クラスタをData ONTAP 8.2にアップグレードする前から存在していたSVM上でHyper-V over SMBソリューションを設定する場合、デフォルトユーザとデフォルトグループが存在しない可能性があります。存在しない場合は、CIFSサーバのデフォルトUNIXユーザを設定する前に、これらを作成する必要があります。

手順

1. デフォルトの UNIX ユーザーが存在するかどうかを確認します：

   ```
   vserver cifs options show -vserver <vserver_name>
   ```

2. デフォルト ユーザー オプションが設定されていない場合は、デフォルト UNIX ユーザーとして指定できる UNIX ユーザーが存在するかどうかを確認します：

```
vserver services unix-user show -vserver <vserver_name>
```

3. デフォルト ユーザー オプションが設定されておらず、デフォルト UNIX ユーザーとして指定できる UNIX ユーザーがいない場合は、デフォルト グループとデフォルト UNIX ユーザーを作成し、デフォルト ユーザーをグループに追加します。

   通常、デフォルトユーザーにはユーザー名「pcuser」が与えられ、UIDは `65534`に割り当てられます。通常、デフォルトグループにはグループ名「pcuser」が与えられます。グループに割り当てられるGIDは `65534`である必要があります。

   a. デフォルト グループを作成します：

   ```
   vserver services unix-group create -vserver <vserver_name> -name
   pcuser -id 65534
   ```

   b. デフォルト ユーザーを作成し、デフォルト ユーザーをデフォルト グループに追加します：

   ```
   vserver services unix-user create -vserver <vserver_name> -user
   pcuser -id 65534 -primary-gid 65534
   ```

   c. デフォルトのユーザーとデフォルトのグループが正しく構成されていることを確認します：

   ```
   vserver services unix-user show -vserver <vserver_name>
   ```

   ```
   vserver services unix-group show -vserver <vserver_name> -members
   ```

4. CIFS サーバーのデフォルト ユーザーが設定されていない場合は、次の手順を実行します：

   a. デフォルトのユーザを設定します。

   ```
   vserver cifs options modify -vserver <vserver_name> -default-unix
   -user pcuser
   ```

   b. デフォルトの UNIX ユーザーが正しく設定されていることを確認します：

   ```
   vserver cifs options show -vserver <vserver_name>
   ```

5. アプリケーション サーバーのコンピュータ アカウントがデフォルト ユーザーに正しくマッピングされていることを確認するには、SVM 上にある共有にドライブをマッピングし、 `vserver cifs session show`コマンドを使用して Windows ユーザーと UNIX ユーザーのマッピングを確認します。

`vserver cifs options`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+cifs+options["ONTAPコマンドリファレンス"^]をご覧ください。

例

次のコマンドは、CIFSサーバのデフォルト ユーザが設定されていないことを確認し、`pcuser`ユーザと`pcuser`グループが存在することを確認します。`pcuser`ユーザは、SVM vs1上のCIFSサーバのデフォルトユーザとして割り当てられています。

```
cluster1::> vserver cifs options show

Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : -
  Guest Unix User        : -
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -



cluster1::> vserver services unix-user show
          User            User   Group  Full
Vserver   Name            ID     ID     Name
--------- --------------- ------ ------ ----------------
vs1       nobody          65535  65535  -
vs1       pcuser          65534  65534  -
vs1       root            0      1      -

cluster1::> vserver services unix-group show -members
Vserver        Name                ID
vs1            daemon              1
       Users: -
vs1            nobody              65535
       Users: -
vs1            pcuser              65534
       Users: -
vs1            root                0
       Users: -

cluster1::> vserver cifs options modify -vserver vs1 -default-unix-user
pcuser
```

```
cluster1::> vserver cifs options show

Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : pcuser
  Guest Unix User        : -
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -
```

SVMルート ボリュームのセキュリティ形式がNTFSに設定されていることの確認

Hyper-VおよびSQL Server over SMBのノンストップオペレーションを確実に成功させるには、ボリュームをNTFSセキュリティ形式で作成する必要があります。Storage Virtual Machine（SVM）上に作成されたボリュームにはルートボリュームのセキュリティ形式がデフォルトで適用されるため、ルートボリュームのセキュリティ形式はNTFSに設定する必要があります。

タスク概要

- SVM を作成するときに、ルート ボリュームのセキュリティ スタイルを指定できます。
- SVM がルート ボリュームを NTFS セキュリティ スタイルに設定して作成されていない場合は、後で `volume modify`コマンドを使用してセキュリティ スタイルを変更できます。

手順

1. SVM ルート ボリュームの現在のセキュリティ スタイルを確認します：

   volume show -vserver *vserver_name* -fields vserver,volume,security-style

2. ルート ボリュームが NTFS セキュリティ形式のボリュームでない場合は、セキュリティ形式を NTFS に変更します：

   volume modify -vserver *vserver_name* -volume root_volume_name -security-style ntfs

3. SVM ルート ボリュームが NTFS セキュリティ スタイルに設定されていることを確認します：

   volume show -vserver *vserver_name* -fields vserver,volume,security-style

例

次のコマンドは、SVM vs1のルート ボリュームのセキュリティ形式がNTFSになっていることを確認します。

```
cluster1::> volume show -vserver vs1 -fields vserver,volume,security-style
vserver  volume     security-style
-------- ---------- --------------
vs1      vs1_root   unix

cluster1::> volume modify -vserver vs1 -volume vs1_root -security-style
ntfs

cluster1::> volume show -vserver vs1 -fields vserver,volume,security-style
vserver  volume     security-style
-------- ---------- --------------
vs1      vs1_root   ntfs
```

必要なCIFSサーバ オプションの設定の確認

必要な CIFS サーバ オプションが有効になっており、Hyper-V および SQL Server over SMB の無停止操作の要件に従って設定されていることを確認する必要があります。

タスク概要

- SMB 2.x および SMB 3.0 を有効にする必要があります。
- パフォーマンスを強化するコピー オフロードを使用するには、ODX コピー オフロードを有効にする必要があります。
- Hyper-V over SMB ソリューションがリモート VSS 対応バックアップ サービスを使用する場合は、VSS シャドウ コピー サービスを有効にする必要があります（Hyper-V のみ）。

手順

1. Storage Virtual Machine（SVM）で必要なCIFSサーバ オプションが有効になっていることを確認します。
   a. 権限レベルをadvancedに設定します。

      `set -privilege advanced`

   b. 次のコマンドを入力します。

      `vserver cifs options show -vserver *vserver_name*`

      次のオプションを `true`に設定する必要があります：

      - `-smb2-enabled`
      - `-smb3-enabled`
      - `-copy-offload-enabled`
      - `-shadowcopy-enabled`（Hyper-V のみ）
2. いずれかのオプションが `true`に設定されていない場合は、次の操作を実行します：
   a. `vserver cifs options modify`コマンドを使用して `true`に設定します。

b. `vserver cifs options show`コマンドを使用して、オプションが `true`に設定されていることを確認します。

3. admin権限レベルに戻ります。

```
set -privilege admin
```

例

次のコマンドは、SVM vs1 で Hyper-V over SMB 構成に必要なオプションが有効になっていることを確認します。この例では、オプション要件を満たすために ODX コピー オフロードを有効にする必要があります。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled,copy-offload-enabled,shadowcopy-enabled
vserver smb2-enabled smb3-enabled copy-offload-enabled shadowcopy-enabled
------- ------------ ------------ -------------------- ------------------
vs1     true         true         false                true

cluster-1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

cluster-1::*> vserver cifs options show -vserver vs1 -fields copy-offload-
enabled
vserver  copy-offload-enabled
-------- --------------------
vs1      true

cluster1::*> set -privilege admin
```

パフォーマンスと冗長性を高めるための**SMB**マルチチャネルの設定

ONTAP 9.4以降では、SMBマルチチャネルを設定して、1つのSMBセッションでONTAPとクライアントの間に複数の接続を確立することができます。これにより、Hyper-VおよびSQL Server over SMB構成のスループットとフォールト トレランスが向上します。

開始する前に

SMBマルチチャネル機能は、クライアントがSMB 3.0以降のバージョンでネゴシエートする場合にのみ使用できます。ONTAPのSMBサーバでは、SMB 3.0以降がデフォルトで有効になっています。

タスク概要

SMBクライアントは、ONTAPクラスタで適切な設定が見つかると、複数のネットワーク接続を自動的に検出して使用します。

SMBセッションあたりの同時接続数は、導入しているNICによって異なります。

- クライアントと**ONTAP**クラスタ上の**1G NIC**

  クライアントから確立される接続数はNICごとに1つで、すべての接続にセッションがバインドされます。

- クライアントおよび**ONTAP**クラスタ上の**10G**以上の容量の**NIC**

  クライアントから確立される接続数はNICごとに最大4つで、すべての接続にセッションがバインドされます。クライアントは10G以上の複数のNICで接続を確立することができます。

さらに、次のパラメータを変更することができます（advanced権限）。

- `-max-connections-per-session`

  各マルチチャネル セッションに許可される最大接続数。デフォルトの接続数は32です。

  デフォルトよりも多くの接続を許可する場合は、クライアントの設定も調整する必要があります（クライアントもデフォルトの接続数は32です）。

- `-max-lifs-per-session`

  各マルチチャネル セッションで通知されるネットワーク インターフェイスの最大数。デフォルトのネットワーク インターフェイス数は256です。

手順

1. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

2. SMBサーバでSMBマルチチャネルを有効にします。

```
vserver cifs options modify -vserver <vserver_name> -is-multichannel
-enabled true
```

3. SMBマルチチャネル セッションがONTAPのレポート対象になっていることを確認します。

```
vserver cifs session show
```

4. admin権限レベルに戻ります。

```
set -privilege admin
```

例

次の例は、すべてのSMBセッションに関する情報を表示します。1つのセッションに対して複数の接続が表示されています。

```
cluster1::> vserver cifs session show
Node:    node1
Vserver: vs1
Connection Session                                          Open
Idle
IDs        ID      Workstation      Windows User          Files
Time
---------- ------- ---------------- ---------------- ---------
---------------
138683,
138684,
138685     1       10.1.1.1         DOMAIN\                   0
4s
                                    Administrator
```

次の例は、セッションID 1が割り当てられたSMBセッションに関する詳細情報を表示します。

```
cluster1::> vserver cifs session show -session-id 1 -instance

Vserver: vs1
                          Node: node1
                    Session ID: 1
                Connection IDs: 138683,138684,138685
              Connection Count: 3
   Incoming Data LIF IP Address: 192.1.1.1
         Workstation IP Address: 10.1.1.1
       Authentication Mechanism: NTLMv1
          User Authenticated as: domain-user
                  Windows User: DOMAIN\administrator
                     UNIX User: root
                   Open Shares: 2
                    Open Files: 5
                    Open Other: 0
                Connected Time: 5s
                     Idle Time: 5s
              Protocol Version: SMB3
        Continuously Available: No
             Is Session Signed: false
                  NetBIOS Name: -
```

NTFSデータ ボリュームの作成

Hyper-VまたはSQL Server over SMBアプリケーション サーバで使用する、継続的可用性を備えた共有を設定する前に、Storage Virtual Machine（SVM）上にNTFSデータ ボリュームを作成する必要があります。ボリューム設定ワークシートを使用してデータ ボリュームを作成します。

タスク概要

データボリュームをカスタマイズするために使用できるオプションパラメータがあります。ボリュームのカスタマイズの詳細については、"論理ストレージ管理"を参照してください。

データ ボリュームを作成する際には、以下のものが含まれるボリューム内にジャンクション ポイントを作成しないようにしてください。

- ONTAPによってシャドウ コピーが作成されるHyper-Vファイル
- SQL Serverを使用してバックアップされるSQL Serverデータベース ファイル

> mixedセキュリティ形式やUNIXセキュリティ形式を使用するボリュームを誤って作成した場合、そのボリュームをNTFSセキュリティ形式のボリュームに変更して、ノンストップ オペレーション用の継続的可用性を備えた共有の作成に直接使用することはできません。Hyper-V over SMBおよびSQL Server over SMBのノンストップ オペレーションは、この構成で使用されるボリュームがNTFSセキュリティ形式のボリュームとして作成されていない場合は適切に機能しません。ボリュームを削除するか、NTFSセキュリティ形式を使用してボリュームを再作成する必要があります。または、Windowsホストにボリュームをマッピングし、ボリュームにACLを適用して、ボリューム内のすべてのファイルとフォルダにACLを反映させます。

手順

1. 次のコマンドを入力して、データ ボリューム作成します。

ルート ボリュームのセキュリティ スタイルが...である **SVM** にボリュームを作成する場合	コマンドを入力してください...
NTFS	**volume create -vserver *vserver_name* -volume *volume_name* -aggregate *aggregate_name* -size integer[KB|MB|GB|TB|PB] -junction-path *path***
NTFS以外	**volume create -vserver *vserver_name* -volume *volume_name* -aggregate *aggregate_name* -size integer[KB|MB|GB|TB|PB]- security-style ntfs -junction-path path**

2. ボリュームの設定が正しいことを確認します。

   volume show -vserver *vserver_name* -volume *volume_name*

継続的可用性を備えたSMB共有の作成

データ ボリュームを作成したら、アプリケーション サーバが Hyper-V 仮想マシンおよび構成ファイルと Microsoft SQL Server データベース ファイルにアクセスするために使用する、継続的に利用可能な共有を作成できます。SMB 共有を作成する際には、共有構成ワークシートを使用してください。

手順

1. 既存のデータ ボリュームとそのジャンクション パスに関する情報を表示します：

   volume show -vserver *vserver_name* -junction

2. 継続的可用性を備えたSMB共有を作成します。

   vserver cifs share create -vserver *vserver_name* -share-name *share_name* -path *path* -share-properties oplocks,continuously-available -symlink "" [-comment text]

   - 必要に応じて、共有設定にコメントを追加できます。
   - デフォルトでは、オフライン ファイル共有プロパティは共有上に構成され、 `manual`に設定されています。
   - ONTAP は、Windows のデフォルトの共有権限 `Everyone` / `Full Control`を使用して共有を作成します。

3. 共有構成ワークシート内のすべての共有に対して前の手順を繰り返します。
4. `vserver cifs share show`コマンドを使用して、構成が正しいことを確認します。
5. 各共有にドライブをマッピングし、**Windows** プロパティ ウィンドウを使用してファイル権限を設定することで、継続的に利用可能な共有上の NTFS ファイル権限を設定します。

例

次のコマンドは、ストレージ仮想マシン（SVM、旧称Vserver）vs1上に「`data2`」という名前の継続的可用性共有を作成します。 `-symlink`パラメータを `""`に設定することで、シンボリックリンクが無効になります：

```
cluster1::> volume show -vserver vs1 -junction
                      Junction                  Junction
Vserver   Volume      Active   Junction Path    Path Source
--------- ----------- -------- ---------------- ------------
vs1       data        true     /data            RW_volume
vs1       data1       true     /data/data1      RW_volume
vs1       data2       true     /data/data2      RW_volume
vs1       vs1_root    -        /                -

cluster1::> vserver cifs share create -vserver vs1 -share-name data2 -path
/data/data2 -share-properties oplocks,continuously-available -symlink ""

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data/data2
             Share Properties: oplocks
                               continuously-available
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

ユーザ アカウント（SMB共有のSQL Server用）へのSeSecurityPrivilege権限の追加

SQL サーバーのインストールに使用されるドメイン ユーザー アカウントには、ドメイン ユーザーにデフォルトで割り当てられていない権限を必要とする CIFS サーバー上の特定のアクションを実行するための “SeSecurityPrivilege” 権限を割り当てる必要があります。

開始する前に

SQL Server のインストールに使用するドメイン アカウントが既に存在している必要があります。

タスク概要

SQL Serverインストーラのアカウントに権限を追加する際、ONTAPはドメイン コントローラに接続してアカウントを検証することがあります。ONTAPがドメイン コントローラに接続できない場合、コマンドが失敗す

ることがあります。

手順

1. 「SeSecurityPrivilege」権限を追加します：

   vserver cifs users-and-groups privilege add-privilege -vserver *vserver_name* -user-or-group-name *account_name* -privileges SeSecurityPrivilege

   `-user-or-group-name`パラメータの値は、Microsoft SQL Server のインストールに使用されるドメイン ユーザー アカウントの名前です。

2. 権限がアカウントに適用されていることを確認します：

   vserver cifs users-and-groups privilege show -vserver *vserver_name* -user-or-group-name *account_name*

例

次のコマンドは、ストレージ仮想マシン（SVM）vs1のEXAMPLEドメイン内のSQL Serverインストーラーのアカウントに"`SeSecurityPrivilege`"権限を追加します：

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\SQLinstaller -privileges
SeSecurityPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name           Privileges
--------- ---------------------       ---------------
vs1       EXAMPLE\SQLinstaller        SeSecurityPrivilege
```

VSSシャドウ コピーのディレクトリ階層の設定（Hyper-V over SMB共有用）

オプションとして、SMB共有内のシャドウ コピーを作成するディレクトリの最大階層を設定できます。このパラメータは、ONTAPがシャドウ コピーを作成するサブディレクトリの最大階層を手動で制御する場合に便利です。

開始する前に

VSSシャドウ コピー機能を有効にする必要があります。

タスク概要

デフォルトでは、最大5つのサブディレクトリのシャドウ コピーが作成されます。値を `0`に設定すると、ONTAPはすべてのサブディレクトリのシャドウ コピーを作成します。

シャドウ コピー セットのディレクトリ階層に5つ以上のサブディレクトリ、またはすべてのサブディレクトリを含めるように指定できますが、Microsoftの要件では、シャドウ コピー セットの作成は60秒以内に完了する必要があります。この時間内に完了しない場合、シャドウ コピー セットの作成は失敗します。選択するシャドウ コピー ディレクトリの階層によって、作成時間が制限時間を超えないようにする必要があります。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. VSSシャドウ コピー ディレクトリの深さを必要なレベルに設定します：

   ```
   vserver cifs options modify -vserver vserver_name -shadowcopy-dir-depth
   integer
   ```

   ```
   vserver cifs options modify -vserver vs1 -shadowcopy-dir-depth 6
   ```

3. admin権限レベルに戻ります。

   ```
   set -privilege admin
   ```

著作権に関する情報

商標に関する情報