ドメインコントローラ接続を管理します

ONTAP 9

NetApp
April 24, 2024

目次

ドメインコントローラ接続を管理します

検出されたサーバに関する情報を表示します

CIFS サーバで検出された LDAP サーバおよびドメインコントローラに関する情報を表示できます。

ステップ

1. 検出されたサーバに関する情報を表示するには、次のコマンドを入力します。 `vserver cifs domain discovered-servers show`

例

次の例は、 SVM vs1 で検出されたサーバを表示します。

```
cluster1::> vserver cifs domain discovered-servers show

Node: node1
Vserver: vs1

Domain Name     Type     Preference DC-Name     DC-Address    Status
--------------- -------- ---------- ----------- ------------- -------
example.com     MS-LDAP  adequate   DC-1        1.1.3.4       OK
example.com     MS-LDAP  adequate   DC-2        1.1.3.5       OK
example.com     MS-DC    adequate   DC-1        1.1.3.4       OK
example.com     MS-DC    adequate   DC-2        1.1.3.5       OK
```

関連情報

サーバのリセットおよび再検出

CIFS サーバを停止または起動しています

サーバをリセットおよび再検出します

CIFS サーバでサーバのリセットと再検出を行うと、 LDAP サーバおよびドメインコントローラに格納されている情報が CIFS サーバに破棄されます。サーバの情報が破棄されたあと、それらの外部サーバに関する最新の情報が再取得されます。これは、接続されているサーバが適切に応答しない場合に役立ちます。

手順

1. 次のコマンドを入力します。 `vserver cifs domain discovered-servers reset-servers -vserver` *`vserver_name`*
2. 再検出されたサーバに関する情報を表示します。 `vserver cifs domain discovered-servers show -vserver` *`vserver_name`*

例

次の例は、 Storage Virtual Machine （ SVM 、旧 Vserver ） vs1 のサーバをリセットして再検出します。

```
cluster1::> vserver cifs domain discovered-servers reset-servers -vserver
vs1

cluster1::> vserver cifs domain discovered-servers show

Node: node1
Vserver: vs1

Domain Name     Type     Preference DC-Name     DC-Address    Status
--------------- -------- ---------- ----------- ------------- -------
example.com     MS-LDAP  adequate   DC-1        1.1.3.4       OK
example.com     MS-LDAP  adequate   DC-2        1.1.3.5       OK
example.com     MS-DC    adequate   DC-1        1.1.3.4       OK
example.com     MS-DC    adequate   DC-2        1.1.3.5       OK
```

関連情報

検出されたサーバに関する情報を表示する

CIFS サーバを停止または起動しています

ドメインコントローラの検出を管理します

ONTAP 9.3 以降では、ドメインコントローラ（ DC ）の検出に使用するデフォルトプロセスを変更できます。サイトまたは優先 DC のプールに検出を制限できるため、環境によってはパフォーマンスの向上につながります。

このタスクについて

デフォルトでは、任意の優先 DC 、ローカルサイト内のすべての DC 、およびすべてのリモート DC を含めて、使用可能なすべての DC が検出されます。そのため、一部の環境では、認証時および共有へのアクセス時にレイテンシが発生する可能性があります。使用する DC のプールが決まっている場合、またはリモート DC が不適切またはアクセスできない場合は、検出方法を変更できます。

ONTAP 9.3以降のリリースでは、 `discovery-mode` のパラメータ `cifs domain discovered-servers` コマンドでは、次のいずれかの検出オプションを選択できます。

- ドメイン内のすべての DC が検出されます。
- ローカルサイト内の DC だけが検出されます。

  。 `default-site` SMBサーバのパラメータは、sites-and-servicesでサイトに割り当てられていないLIFでこのモードを使用するように定義できます。

- サーバの検出は実行せず、優先 DC のみを使用するように SMB サーバを設定します。

  このモードを使用するには、最初に SMB サーバに対して優先 DC を定義する必要があります。

ステップ

1. 目的の検出オプションを指定します。 `vserver cifs domain discovered-servers discovery-mode modify -vserver *vserver_name* -mode {all|site|none}`

   のオプション `mode` パラメータ：

   - `all`

     使用可能なすべての DC を検出します（デフォルト）。

   - `site`

     DC の検出対象をサイトに制限します。

   - `none`

     優先 DC のみを使用し、検出は実行しません。

優先ドメインコントローラを追加する

ONTAP は DNS を介してドメインコントローラを自動的に検出します。必要に応じて、特定のドメインに対する優先ドメインコントローラのリストにドメインコントローラを追加することができます。

このタスクについて

指定したドメインに優先ドメインコントローラリストがすでに存在する場合、新しいリストが既存のリストに統合されます。

ステップ

1. 優先ドメインコントローラのリストに追加するには、次のコマンドを入力します。+ `vserver cifs domain preferred-dc add -vserver *vserver_name* -domain *domain_name* -preferred -dc IP_address, …+`

   `-vserver *vserver_name*` Storage Virtual Machine（SVM）名を示します。

   `-domain *domain_name*` 指定したドメインコントローラが属するドメインの完全修飾Active Directory名を指定します。

   `-preferred-dc *IP_address*`はい。 優先ドメインコントローラの1つ以上のIPアドレスを優先順にカンマで区切って指定します。

例

次のコマンドでは、SVM vs1上のSMBサーバがcifs.lab.example.comドメインへの外部アクセスを管理するために使用する優先ドメインコントローラのリストに、ドメインコントローラ172.17.102.25と172.17.102.24を追加します。

```
cluster1::> vserver cifs domain preferred-dc add -vserver vs1 -domain
cifs.lab.example.com -preferred-dc 172.17.102.25,172.17.102.24
```

関連情報

優先ドメインコントローラの管理用コマンド

優先ドメインコントローラの管理用コマンド

優先ドメインコントローラの追加、表示、削除を行うコマンドについて説明します。

状況	使用するコマンド
優先ドメインコントローラを追加する	`vserver cifs domain preferred-dc add`
優先ドメインコントローラを表示する	`vserver cifs domain preferred-dc show`
優先ドメインコントローラを削除する	`vserver cifs domain preferred-dc remove`

詳細については、各コマンドのマニュアルページを参照してください。

関連情報

優先ドメインコントローラの追加

ドメインコントローラへの **SMB2** 接続を有効にします

ONTAP 9.1 以降では、 SMB バージョン 2.0 からドメインコントローラへの接続を有効にすることができます。これは、ドメインコントローラで SMB 1.0 を無効にしている場合は必須です。ONTAP 9.2 以降では、 SMB2 がデフォルトで有効になります。

このタスクについて

。 `smb2-enabled-for-dc-connections` コマンドオプションを使用すると、使用しているONTAP のリリースに応じたシステムデフォルトが有効になります。ONTAP 9.1 のシステムデフォルトでは、 SMB 1.0 が有効、 SMB 2.0 が無効になります。ONTAP 9.2 のシステムデフォルトでは、 SMB 1.0 が有効になり、 SMB 2.0 が有効になります。ドメインコントローラは、最初に SMB 2.0 をネゴシエートし、失敗した場合は SMB 1.0 を使用します。

SMB 1.0 は、 ONTAP からドメインコントローラに対して無効にすることができます。ONTAP 9.1 では、SMB 1.0 を無効にした場合、ドメインコントローラと通信するために SMB 2.0 を有効にする必要があります。

詳細情報：

- "有効なSMBのバージョンの確認"。
- "サポートされる SMB のバージョンと機能"。

> 状況 `-smb1-enabled-for-dc-connections` がに設定されます `false` 間 `-smb1-enabled` がに設定されます `true`ONTAP では、クライアントとしてのSMB 1.0の接続は拒否されますが、サーバとしてのSMB 1.0のインバウンド接続は引き続き受け入れます。

手順

1. SMBセキュリティ設定を変更する前に、有効になっているSMBのバージョンを確認します。 `vserver cifs security show`
2. リストを下にスクロールして SMB のバージョンを確認します。
3. を使用して、該当するコマンドを実行します `smb2-enabled-for-dc-connections` オプション

SMB2 の設定	入力するコマンド
有効	`vserver cifs security modify -vserver` *`vserver_name`* `-smb2-enabled-for-dc -connections true`
無効	`vserver cifs security modify -vserver` *`vserver_name`* `-smb2-enabled-for-dc -connections false`

ドメインコントローラへの暗号化接続を有効にします

ONTAP 9.8 以降では、ドメインコントローラへの接続を暗号化するように指定できます。

このタスクについて

ONTAP では、ドメインコントローラ（DC）通信の暗号化が必要です `-encryption-required-for-dc -connection` オプションはに設定されています `true`;デフォルトはです `false`。このオプションを設定すると、 SMB3 でのみ暗号化がサポートされるため、 SMB3 プロトコルのみが使用されます。

暗号化されたDC通信が必要な場合は、を参照してください `-smb2-enabled-for-dc-connections` ONTAP はSMB3接続のみをネゴシエートするため、このオプションは無視されます。DC が SMB3 と暗号化をサポートしていない場合、 ONTAP は接続しません。

ステップ

1. DCとの暗号化通信を有効にします。 `vserver cifs security modify -vserver` *`svm_name`* `-encryption-required-for-dc-connection true`