



# 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	1
検出されたサーバに関する情報を表示します	1
サーバをリセットおよび再検出します	1
ドメインコントローラの検出を管理します	2
優先ドメインコントローラを追加する	3
優先ドメインコントローラの管理用コマンド	4
ドメインコントローラへの SMB2 接続を有効にします	4
ドメインコントローラへの暗号化接続を有効にします	5

# 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::> vsriver cifs domain discovered-servers reset-servers -vsriver
vs1
```

```
cluster1::> vsriver 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::> vsync cifs domain preferred-dc add -vsync 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	<code>vsync cifs domain preferred-dc add</code>
優先ドメインコントローラを表示する	<code>vsync cifs domain preferred-dc show</code>
優先ドメインコントローラを削除する	<code>vsync cifs domain preferred-dc remove</code>

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	<pre>vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc -connections true</pre>
無効	<pre>vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc -connections false</pre>

## 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`

## 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。

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权を有し、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权については、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。