



ドメインコントローラ接続の管理

ONTAP 9

NetApp
December 20, 2024

目次

ドメインコントローラ接続の管理	1
検出されたサーバに関する情報を表示する	1
サーバのリセットと再検出	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の追加	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接続を有効にする	4
ドメインコントローラへの暗号化接続を有効にする	5

ドメインコントローラ接続の管理

検出されたサーバに関する情報を表示する

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サーバの停止と起動](#)

サーバのリセットと再検出

CIFSサーバでサーバをリセットおよび再検出すると、LDAPサーバおよびドメインコントローラに関するCIFSサーバに格納されている情報が破棄されます。サーバ情報を破棄したあと、CIFSサーバはこれらの外部サーバに関する最新の情報を再取得します。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

次の例では、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の表示](#)

[CIFSサーバの停止と起動](#)

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。これにより、検出対象をサイトまたは優先DCのプールに限定できます。これにより、環境によってはパフォーマンスが向上する可能性があります。

タスクの内容

デフォルトでは、動的検出プロセスによって、使用可能なすべてのDC (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を含む) 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、検出方法を変更することができます。

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

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

SMBサーバのパラメータは、``default-site` 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。

- サーバ検出は実行されず、優先DCのみを使用してSMBサーバを設定します。

このモードを使用するには、まずSMBサーバの優先DCを定義する必要があります。

開始する前に

advanced権限レベルが必要です。

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}`

パラメータのオプション mode :

- all
使用可能なすべてのDCを検出します（デフォルト）。
- site
DC検出をサイトに限定します。
- 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の追加

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1つ以上のドメインコントローラを追加できます。

タスクの内容

指定したドメインの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は、新しいリストが既存のリストにマージされます。

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, ...`には、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::> vservers cifs domain preferred-dc add -vservers 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を追加、表示、削除する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>vservers cifs domain preferred-dc add</code>
優先ドメインコントローラを表示する	<code>vservers cifs domain preferred-dc show</code>
優先ドメインコントローラを削除する	<code>vservers 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接続を有効にする

SMB 1.0以降では、ONTAP 9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。この処理は、ドメインコントローラでSMB 1.0を無効にしている場合に必要です。ONTAP 9 .2以降では、SMB2がデフォルトで有効になっています。

タスクの内容

コマンドオプションを使用すると、`smb2-enabled-for-dc-connections`を使用している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では有効になり、SMB 2.0では無効になります。ONTAP 9 .2のシステムデフォルトは、SMB 1.0では有効、SMB 2.0では有効です。ドメインコントローラが最初にSMB 2.0をネゴシエートできない場合は、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SMB 1.0が無効になっている場合は、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。

詳細については以下を参照してください。

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



がwhileに `-smb1-enabled` 設定されて `false` いる場合 `-smb1-enabled-for-dc-connections true`、ONTAPはクライアントとしてのSMB 1.0の接続を拒否しますが、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. オプションを使用して、該当するコマンドを実行し `-smb2-enabled-for-dc-connections` ます。

SMB2 の設定	入力するコマンド
有効	<code>vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc-connections true</code>
無効にする	<code>vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc-connections false</code>

ドメインコントローラへの暗号化接続を有効にする

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。

タスクの内容

このオプションをに設定 `true` すると、ONTAPでドメインコントローラ (DC) 通信の暗号化が必要になります `-encryption-required-for-dc-connection`。デフォルトはです。 `false` 暗号化はONTAP 3でしかサポートされないため、このオプションを設定するとSMB3プロトコルのみがSMB-DC接続に使用されません。

暗号化されたDC通信が必要な場合、ONTAPはSMB3接続のみをネゴシエートするため、この `-smb2-enabled-for-dc-connections` 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。