Active Directory ドメイン内に SMB サーバをセットアップする

ONTAP 9

NetApp
April 24, 2024

目次

Active Directory ドメイン内に SMB サーバをセットアップする

タイムサービスを設定

Active Directory ドメインコントローラで SMB サーバを作成する前に、クラスタ時間と SMB サーバが所属するドメインのドメインコントローラの時間のずれが 5 分以内であることを確認する必要があります。

このタスクについて

Active Directory ドメインと同じ NTP サーバを使用して時刻を同期するようにクラスタ NTP サービスを設定する必要があります。

ONTAP 9.5 以降では、対称認証を使用するように NTP サーバをセットアップできます。

手順

1. を使用してタイムサービスを設定します `cluster time-service ntp server create` コマンドを実行します
   - 対称認証を使用せずにタイムサービスを設定するには、次のコマンドを入力します。 `cluster time-service ntp server create -server server_ip_address`
   - 対称認証を使用してタイムサービスを設定するには、次のコマンドを入力します。 `cluster time-service ntp server create -server server_ip_address -key-id key_id` `cluster time-service ntp server create -server 10.10.10.1` `cluster time-service ntp server create -server 10.10.10.2`
2. を使用して、タイムサービスが正しく設定されていることを確認します `cluster time-service ntp server show` コマンドを実行します

   `cluster time-service ntp server show`

   ```
   Server                          Version
   ------------------------------- -------
   10.10.10.1                      auto
   10.10.10.2                      auto
   ```

NTP サーバの対称認証を管理するコマンドです

ONTAP 9.5 以降では、ネットワークタイムプロトコル（ NTP ）バージョン 3 がサポートされます。NTPv3 には SHA-1 鍵を使用した対称認証機能が含まれ、ネットワークセキュリティが強化されます。

作業	使用するコマンド
対称認証を使用せずに NTP サーバを設定する	`cluster time-service ntp server create -server server_name`
対称認証を使用して NTP サーバを設定する	`cluster time-service ntp server create -server server_ip_address -key-id key_id`
既存の NTP サーバに対して対称認証を有効にする必要なキー ID を追加することで、既存の NTP サーバを変更して認証を有効にすることができます	`cluster time-service ntp server modify -server server_name -key-id key_id`
共有 NTP キーを設定する	`cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value` 共有キーは ID で参照されます。ID 、そのタイプ、および値が、ノードと NTP サーバで同じである必要があります
不明なキー ID で NTP サーバを設定する	`cluster time-service ntp server create -server server_name -key-id key_id`
NTP サーバで設定されていないキー ID でサーバを設定する。	`cluster time-service ntp server create -server server_name -key-id key_id` キー ID 、タイプ、および値が、 NTP サーバで設定されたキー ID 、タイプ、および値と同じである必要があります。
対称認証を無効にします	`cluster time-service ntp server modify -server server_name -authentication disabled`

Active Directory ドメイン内に SMB サーバを作成します

を使用できます `vserver cifs create` コマンドを使用してSVM上にSMBサーバを作成し、所属先のActive Directory（AD）ドメインを指定します。

作業を開始する前に

データ処理に使用している SVM および LIF が、 SMB プロトコルを許可するように設定されている必要があります。LIF は、 SVM 上で設定されている DNS サーバ、および SMB サーバの追加先ドメインの AD ドメインコントローラに接続できる必要があります。

SMB サーバの追加先となる AD ドメイン内のマシンアカウントの作成を許可されているユーザなら誰でも、

SVM 上に SMB サーバを作成できます。これには、他のドメインのユーザを含めることができます。

ONTAP 9.7 以降では、権限がある Windows アカウントの名前とパスワードの代わりに、 keytab ファイルの URI を AD 管理者から提供される場合があります。URIを受け取ったら、に含めます `-keytab-uri` パラメータと `vserver cifs` コマンド

このタスクについて

Activity Directory ドメインで SMB サーバを作成する場合の条件は次のとおりです。

- ドメインを指定するときは Fully Qualified Domain Name （ FQDN ；完全修飾ドメイン名）を使用する必要があります。
- デフォルト設定では、 SMB サーバマシンアカウントは Active Directory CN=Computer オブジェクトに追加されます。
- を使用して、SMBサーバを別の組織単位（OU）に追加することもできます `-ou` オプション
- 必要に応じて、 SMB サーバの 1 つ以上の NetBIOS エイリアス（最大 200 個）をカンマで区切って追加できます。

  SMB サーバの NetBIOS エイリアスを設定すると、他のファイルサーバのデータを SMB サーバに統合して、 SMB サーバが元のファイルサーバの名前に応答するようにする場合に役立ちます。

。 `vserver cifs` マニュアルページには、追加のオプションパラメータと命名要件が記載されています。

> 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（ DC ）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、 SMB 2.0 がデフォルトで有効になります。

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。ONTAP では、ドメインコントローラの通信に暗号化が必要です `-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。。

"SMBの管理" SMB サーバ設定オプションの詳細については、を参照してください。

手順

1. クラスタでSMBのライセンスが有効になっていることを確認します。 `system license show -package cifs`

   SMBライセンスはに含まれています。 "ONTAP One"。ONTAP Oneをお持ちでなく、ライセンスがインストールされていない場合は、営業担当者にお問い合わせください。

   SMB サーバを認証のみに使用する場合は、 CIFS ライセンスは必要ありません。

2. ADドメインにSMBサーバを作成します。 `vserver cifs create -vserver vserver_name -cifs-server smb_server_name -domain FQDN [-ou organizational_unit][-netbios-aliases NetBIOS_name, ...][-keytab-uri {(ftp|http)://hostname|IP_address}][-comment text]`

   ドメインに参加する場合、このコマンドの実行には数分かかることがあります。

次のコマンドは、ドメイン「 example.com`": 」に SMB サーバ「 'smb_server01' 」を作成します

```
cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
smb_server01 -domain example.com
```

次のコマンドは、ドメイン「 m ydomain.com`" 」に SMB サーバ「 'smb_server02' 」を作成し、 keytab ファイルを使用して ONTAP 管理者を認証します。

```
cluster1::> vserver cifs create -vserver vs1.mydomain.com -cifs-server
smb_server02 -domain mydomain.com -keytab-uri
http://admin.mydomain.com/ontap1.keytab
```

3. を使用してSMBサーバの設定を確認します `vserver cifs show` コマンドを実行します

   この例では、「 `s MB_SERVER01' 」という名前の SMB サーバが SVM vs1.example.com 上に作成され、「 example.com`" ドメイン」に追加されたことがコマンド出力に示されています。

```
cluster1::> vserver cifs show -vserver vs1

                                          Vserver: vs1.example.com
                        CIFS Server NetBIOS Name: SMB_SERVER01
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description: -
                          List of NetBIOS Aliases: -
```

4. 必要に応じて、ドメインコントローラとの暗号化通信を有効にします（ONTAP 9.8以降）。 `vserver cifs security modify -vserver svm_name -encryption-required-for-dc-connection true`

例

次のコマンドは、 SVM vs2.example.com の「 example.com`" 」ドメインに「 'MB_Server02' 」という名前の SMB サーバを作成します。マシン・アカウントは '`OU=eng 、 OU=corp 、 DC=example 、 DC=com コンテナに作成されますSMB サーバには NetBIOS エイリアスが割り当てられます。

```
cluster1::> vserver cifs create -vserver vs2.example.com –cifs-server
smb_server02 -domain example.com –ou OU=eng,OU=corp -netbios-aliases
old_cifs_server01

cluster1::> vserver cifs show -vserver vs1
                                          Vserver: vs2.example.com
                        CIFS Server NetBIOS Name: SMB_SERVER02
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description: -
                          List of NetBIOS Aliases: OLD_CIFS_SERVER01
```

次のコマンドは、別のドメインのユーザ（ここでは信頼できるドメインの管理者）が、 SVM vs3.example.com 上に「 smb_server03 」という名前の SMB サーバを作成できるようにします。。 `-domain` optionは、SMBサーバを作成するホームドメイン（DNSの設定で指定）の名前を指定します。。 `username` オプションは、信頼できるドメインの管理者を指定します。

- ホームドメイン： example.com
- 信頼できるドメイン： trust.lab.com
- 信頼できるドメインのユーザ名： Administrator1

```
cluster1::> vserver cifs create -vserver vs3.example.com -cifs-server
smb_server03 -domain example.com

Username: Administrator1@trust.lab.com
Password: . . .
```

SMB 認証用の keytab ファイルを作成します

ONTAP 9.7 以降 ONTAP では、 keytab ファイルを使用した Active Directory （ AD ）サーバとの SVM 認証がサポートされます。AD管理者はkeytabファイルを生成し、Uniform Resource Identifier（URI;ユニフォームリソース識別子）としてONTAP 管理者が使用できるようにします。このファイルは、に指定します `vserver cifs` コマンドを実行するには、ADドメインとのKerberos認証が必要です。

AD管理者は、標準のWindows Serverを使用してkeytabファイルを作成できます `ktpass` コマンドを実行しますこのコマンドは、認証が必要なプライマリドメインで実行する必要があります。。 `ktpass` コマンドを使用してkeytabファイルを生成できるのはプライマリドメインユーザのみです。信頼できるドメインユーザを使用して生成されたキーはサポートされていません。

keytab ファイルは、特定の ONTAP 管理者ユーザ用に生成されます。管理者ユーザのパスワードが変更され

ないかぎり、特定の暗号化タイプとドメインに対して生成されたキーは変更されません。したがって、管理者ユーザのパスワードを変更した場合は、そのたびに新しい keytab ファイルが必要になります。

次の暗号化タイプがサポートされています。

- AES256-SHA1
- des-cbc-md5

> ONTAP では、 DES-CBC-CRC 暗号化タイプはサポートされていません。

- RC4-HMAC

最も高度な暗号化タイプは AES256 です。 ONTAP システムで有効な場合は AES256 を使用してください。

keytab ファイルは、管理パスワードを指定して生成するか、ランダムに生成されたパスワードを使用して生成できます。ただし、 keytab ファイル内のキーを復号化するために AD サーバ側で管理者ユーザに固有な秘密鍵が必要になるため、ある時点で使用できるパスワードオプションはどちらか 1 つだけです。特定の管理者の秘密鍵を変更すると、 keytab ファイルは無効になります。