Active Directoryドメインでの SMBサーバのセットアップ

ONTAP 9

NetApp
December 20, 2024

目次

Active DirectoryドメインでのSMBサーバのセットアップ

タイムサービスの設定

アクティブ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。

タスクの内容

Active Directoryドメインと同じNTPサーバを時刻の同期に使用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。

手順

1. コマンドを使用してタイムサービスを設定します `cluster time-service ntp server create`。
   - 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. コマンドを使用して、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`。

   ```
   cluster time-service ntp server show
   ```

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

NTPサーバの対称認証の管理用コマンド

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キーを使用した対称認証が含まれているため、ネットワークセキュリティが向上します。

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`

作業	使用するコマンド
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サーバの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サーバの両方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でサーバを設定します。	`cluster time-service ntp server create -server server_name -key-id key_id` キーID、タイプ、および値は、NTPサーバに設定されているキーID、タイプ、および値と同じである必要があります。
対称認証を無効にする	`cluster time-service ntp server modify -server server_name -authentication disabled`

Active DirectoryドメインにSMBサーバを作成する

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

開始する前に

データ処理に使用する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サーバの追加先の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すべてのユーザが、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、権限のあるWindowsアカウントの名前とパスワードを指定する代わりに、keytabファ

イルのURIをAD管理者から提供することができます。URIを受け取ったら、コマンドのパラメータ `vserver cifs`にそのURIを含め `-keytab-uri`ます。

タスクの内容

Activity DirectoryドメインにSMBサーバを作成する場合は、次の点に注意してください。

- 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。
- オプションを使用すると、SMBサーバを別の組織単位（OU）に追加できます `-ou`。
- 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）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、SMBサーバが元のサーバの名前に応答するようにする場合に役立ちます。

その他のオプションのパラメータと命名要件については、のマニュアルページを参照して `vserver cifs`ください。

SMB.1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（DC）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。SMB.2以降では、ONTAP 9 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オプションがに設定され `true`ている場合、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`。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接続に使用されます。です。

"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"ONTAP One"ます。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. コマンドを使用して、SMBサーバの設定を確認します `vserver cifs show`。

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（ONTAP 9 .8以降）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`

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。オプションは `-domain`、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。オプションは `username`、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ファイルの作成

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）としてONTAP管理者が使用できるようにします。このURIは、コマンドでADドメインとのKerberos認証が必要な場合に指定します `vserver cifs`。

AD管理者は、Windows Serverの標準コマンドを使用してkeytabファイルを作成できます `ktpass`。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。そのため、管理者ユーザのパスワードを変更するたびに、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。

著作権に関する情報

商標に関する情報