



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	1
タイムサービスを設定	1
NTP サーバの対称認証を管理するコマンドです	1
Active Directory ドメイン内に SMB サーバを作成します	2
SMB 認証用の keytab ファイルを作成します	5

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	<code>cluster time-service ntp server create -server server_name</code>
対称認証を使用して NTP サーバを設定する	<code>cluster time-service ntp server create -server server_ip_address -key-id key_id</code>
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	<code>cluster time-service ntp server modify -server server_name -key-id key_id</code>
共有 NTP キーを設定する	<code>cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value</code> <div>  <p>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</p> </div>
不明なキー ID で NTP サーバを設定する	<code>cluster time-service ntp server create -server server_name -key-id key_id</code>
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。	<code>cluster time-service ntp server create -server server_name -key-id key_id</code> <div>  <p>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。</p> </div>
対称認証を無効にします	<code>cluster time-service ntp server modify -server server_name -authentication disabled</code>

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

次のコマンドは、ドメイン「mydomain.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::> vservers cifs create -vservers 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 vservers cifs show コマンドを実行します

この例では、「SMB_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::> vservers cifs show -vservers 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）。 vservers cifs security modify -vservers 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::> vsserver cifs create -vsserver vs2.example.com -cifs-server  
smb_server02 -domain example.com -ou OU=eng,OU=corp -netbios-aliases  
old_cifs_server01
```

```
cluster1::> vsserver cifs show -vsserver 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::> vsserver cifs create -vsserver 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 vsserver 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。

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。