NFSでKerberosを使用してセキュリティを強化

ONTAP 9

NetApp
December 20, 2024

目次

NFSでKerberosを使用してセキュリティを強化

NFSでのKerberos使用によるセキュリティ強化の概要

ご使用の環境でKerberosが強力な認証に使用されている場合は、Kerberos管理者と協力して要件および適切なストレージシステム構成を決定し、SVMをKerberosクライアントとして有効にする必要があります。

環境が次のガイドラインを満たしている必要があります。

- ONTAP で Kerberos を設定するには、 Kerberos のサーバとクライアントの設定に適したベストプラクティスに従ってサイトが導入されている必要があります。
- Kerberos 認証を必須とする場合は、可能であれば NFSv4 以降を使用します。

  NFSv3 でも Kerberos を使用できますが、Kerberos の高度なセキュリティ機能をフルに活用するには、ONTAP を NFSv4 以降に導入する必要があります。

- サーバアクセスの冗長化を促すため、同じ SPN を使ってクラスタ内の複数のノードのデータ LIF で Kerberos を有効にする必要があります。
- Kerberos を SVM で有効にする場合は、 NFS クライアントの設定に応じて、次のいずれかのセキュリティ方式をボリュームまたは qtree のエクスポートルールに指定する必要があります。
  - `krb5`（Kerberos v5プロトコル）
  - `krb5i`（Kerberos v5プロトコルとチェックサムによる整合性チェック）
  - `krb5p`（Kerberos v5プロトコルとプライバシーサービス）

Kerberos のサーバとクライアントのほかに、次の外部サービスを Kerberos を使用する ONTAP 用に設定する必要があります。

- ディレクトリサービス

  Active Directory や OpenLDAP などのセキュアなディレクトリサービスを環境に導入し、 SSL / TLS 経由の LDAP を使用するように設定してください。NIS を使用すると、要求がクリアテキストで送信されセキュアではないため、 NIS は使用しないでください。

- NTP

  NTPを実行している稼働中のタイムサーバが必要です。これは、時間のずれによるKerberos認証の失敗を防ぐために必要です。

- ドメイン名解決（DNS）

  各UNIXクライアントおよび各SVM LIFについて、KDCのフォワードルックアップゾーンとリバースルックアップゾーンに適切なサービスレコード（SRV）が登録されている必要があります。すべての参加者は、DNSを介して適切に解決できる必要があります。

Kerberos設定の権限の確認

Kerberos では、特定の UNIX 権限が SVM ルートボリューム用およびローカルのユーザおよびグループ用に設定されている必要があります。

手順

1. SVM ルートボリュームについて、関連する権限を表示します。

   `volume show -volume root_vol_name-fields user,group,unix-permissions`

   SVMのルートボリュームを次のように設定しておく必要があります。

名前	設定
UID	ルートまたはID 0
GID	ルートまたはID 0
UNIX権限	755

   これらの値が表示されない場合は、コマンドを使用し `volume modify`て更新します。

2. ローカル UNIX ユーザを表示します。

   `vserver services name-service unix-user show -vserver vserver_name`

   SVMで次のUNIXユーザを設定しておく必要があります。

ユーザ名	ユーザ**ID**	プライマリグループ**ID**	コメント
NFS	500	0	GSS INIT フェーズで必要。 NFSクライアントユーザSPNの最初のコンポーネントがユーザとして使用されます。 NFSクライアントユーザのSPNに対するKerberos-UNIXネームマッピングがある場合は、nfsユーザは必要ありません。
root	0	0	マウントに必要。

   これらの値が表示されていない場合は、コマンドを使用して更新できます `vserver services name-service unix-user modify`。

3. ローカル UNIX グループを表示します。

   ```
   vserver services name-service unix-group show -vserver vserver _name
   ```

   SVMで次のUNIXグループを設定しておく必要があります。

グループ名	グループ**ID**
デーモン	1
root	0

   これらの値が表示されていない場合は、コマンドを使用して更新できます `vserver services name-service unix-group modify`。

NFS Kerberos Realmの設定を作成します。

環境で ONTAP から外部 Kerberos サーバにアクセスする場合は、まず既存の Kerberos Realm を使用するように SVM を設定する必要があります。そのためには、Kerberos KDCサーバの設定値を収集し、コマンドを使用してSVMにKerberos Realm設定を作成する必要があり `vserver nfs kerberos realm create`ます。

必要なもの

認証の問題を回避するために、クラスタ管理者はストレージシステム、クライアント、および KDC サーバ上で NTP を設定しておく必要があります。クライアントとサーバの時間差（クロックスキュー）は、認証エラーの一般的な原因です。

手順

1. Kerberos管理者に問い合わせて、コマンドで指定する適切な設定値を決定し `vserver nfs kerberos realm create`ます。
2. SVM で Kerberos Realm の設定を作成します。

   ```
   vserver nfs kerberos realm create -vserver vserver_name -realm realm_name
   {AD_KDC_server_values |AD_KDC_server_values} -comment "text"
   ```

3. Kerberos Realmの設定が正常に作成されたことを確認します。

   ```
   vserver nfs kerberos realm show
   ```

例

次のコマンドは、 Microsoft Active Directory サーバを KDC サーバとして使用する NFS Kerberos Realm 設定を SVM vs1 で作成します。Kerberos Realm は AUTH.EXAMPLE.COM です。Active Directory サーバの名前は ad-1 で、 IP アドレスは 10.10.8.14 です。許容されるクロックスキューは 300 秒（デフォルト）です。KDC サーバの IP アドレスは 10.10.8.14 で、ポート番号は 88 （デフォルト）です。「Microsoft Kerberos config」はコメントです。

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
AUTH.EXAMPLE.COM -adserver-name ad-1
-adserver-ip 10.10.8.14 -clock-skew 300 -kdc-ip 10.10.8.14 -kdc-port 88
-kdc-vendor Microsoft
-comment "Microsoft Kerberos config"
```

次のコマンドは、 MIT KDC を使用する NFS Kerberos Realm 設定を SVM vs1 で作成します。Kerberos Realm は SECURITY.EXAMPLE.COM です。許容されるクロックスキューは300秒です。KDC サーバの IP アドレスは 10.10.9.1 で、ポート番号は 88 です。KDC ベンダーは UNIX ベンダーを示す Other です。管理サーバの IP アドレスは 10.10.9.1 で、ポート番号は 749 （デフォルト）です。パスワードサーバの IP アドレスは 10.10.9.1 で、ポート番号は 464 （デフォルト）です。「UNIX Kerberos config」はコメントです。

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
SECURITY.EXAMPLE.COM. -clock-skew 300
-kdc-ip 10.10.9.1 -kdc-port 88 -kdc-vendor Other -adminserver-ip 10.10.9.1
-adminserver-port 749
-passwordserver-ip 10.10.9.1 -passwordserver-port 464 -comment "UNIX
Kerberos config"
```

NFS Kerberosで許可される暗号化タイプの設定

デフォルトでは、 ONTAP は、 DES 、 3DES 、 AES-128 、および AES-256 の暗号化タイプをサポートします。コマンドでパラメータを指定する `-permitted-enc -types`と、SVMごとに許可される暗号化タイプを、特定の環境のセキュリティ要件に合わせて設定できます `vserver nfs modify`。

タスクの内容

クライアントの互換性を最大限に高めるために、ONTAPはデフォルトで弱いDES暗号化と強いAES暗号化の両方をサポートしています。つまり、たとえば、セキュリティを強化する必要があり、環境でサポートされている場合は、この手順を使用してDESと3DESを無効にし、クライアントにAES暗号化のみの使用を要求できます。

使用可能な最も強力な暗号化を使用する必要があります。ONTAP の場合は AES-256 です。この暗号化レベルが環境でサポートされていることを、 KDC 管理者に確認する必要があります。

- SVMでAES全体（AES-128とAES-256の両方）を有効または無効にすると、システムが停止します。元のDESプリンシパル/ keytabファイルが削除され、SVMのすべてのLIFでKerberos設定を無効にする必要があるためです。

  この変更を行う前に、SVMでNFSクライアントがAES暗号化を使用していないことを確認する必要があります。

- DES や 3DES の有効化または無効化は、 LIF での Kerberos 設定の変更を一切必要としません。

ステップ

1. 許可されている暗号化タイプを有効または無効にします。

有効または無効にする対象	実行する手順
DES または 3DES	a. SVMのNFS Kerberosで許可されている暗号化タイプを設定します。+ `vserver nfs modify -vserver vserver_name -permitted-enc-types encryption_types` 暗号化タイプが複数ある場合はカンマで区切ります。 b. 変更が成功したことを確認します。+ `vserver nfs show -vserver vserver_name -fields permitted-enc-types`
AES-128またはAES-256	a. Kerberosが有効になっているSVMとLIFを特定します。+ `vserver nfs kerberos interface show` b. 変更対象のNFS Kerberosで許可されている暗号化タイプが設定されているSVM上のすべてのLIFでKerberosを無効にします。+ `vserver nfs kerberos interface disable -lif lif_name` c. SVMのNFS Kerberosで許可されている暗号化タイプを設定します。+ `vserver nfs modify -vserver vserver_name -permitted-enc-types encryption_types` 暗号化タイプが複数ある場合はカンマで区切ります。 d. 変更が成功したことを確認します。+ `vserver nfs show -vserver vserver_name -fields permitted-enc-types` e. SVM上のすべてのLIFでKerberosを再度有効にします。+ `vserver nfs kerberos interface enable -lif lif_name -spn service_principal_name` f. すべてのLIFでKerberosが有効になっていることを確認します。+ `vserver nfs kerberos interface show`

データLIFでKerberosを有効にする

コマンドを使用すると、データLIFでKerberosを有効にできます `vserver nfs kerberos interface enable`。これにより、SVMでNFSのKerberosセキュリティサ

ービスを使用できます。

タスクの内容

Active Directory KDC を使用する場合、使用される SPN の最初の 15 文字は Realm またはドメイン内の SVM 間で一意である必要があります。

手順

1. NFS Kerberos 設定を作成します。

   ```
   vserver nfs kerberos interface enable -vserver vserver_name -lif
   logical_interface -spn service_principal_name
   ```

   ONTAP で Kerberos インターフェイスを有効にするには、 KDC の SPN 用のシークレットキーが必要です。

   Microsoft KDC の場合、 KDC に接続があると、シークレットキーを取得するためのユーザ名とパスワードのプロンプトが CLI で発行されます。Kerberos Realmの別のOUでSPNを作成する必要がある場合は、オプションのパラメータを指定できます `-ou`。

   Microsoft 以外の KDC の場合は、次の 2 つのうちいずれかの方法を使用してシークレットキーを取得できます。

状況	コマンドとともに含める必要のあるパラメータ
KDC からキーを直接取得するための KDC 管理者のクレデンシャルが必要です	`-admin-username` *kdc_admin_username*
KDC 管理者のクレデンシャルはないが、キーが含まれている、 KDC の keytab ファイルはある	`-keytab-uri` {ftp

2. LIFでKerberosが有効になったことを確認します。

   ```
   vserver nfs kerberos-config show
   ```

3. 複数の LIF で Kerberos を有効にするには、手順 1 と 2 を繰り返します。

例

次のコマンドは、 vs1 という SVM の NFS Kerberos 設定を、 OU lab2ou 内の SPN nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM を使用して、 ves03-d1 という論理インターフェイス ves03-d1 に対して作成して検証します。

```
vs1::> vserver nfs kerberos interface enable -lif ves03-d1 -vserver vs2
-spn nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM -ou "ou=lab2ou"

vs1::>vserver nfs kerberos-config show
        Logical
Vserver Interface Address       Kerberos  SPN
------- --------- -------       --------- --------------------------------
vs0     ves01-a1
                  10.10.10.30   disabled  -
vs2     ves01-d1
                  10.10.10.40   enabled   nfs/ves03-
d1.lab.example.com@TEST.LAB.EXAMPLE.COM
2 entries were displayed.
```

著作権に関する情報

商標に関する情報