SVM への NFS アクセスを設定

ONTAP 9

NetApp
April 24, 2024

目次

SVM への NFS アクセスを設定

SVM を作成します。

NFS クライアントへのデータアクセスを提供するための SVM がクラスタ内に 1 つもない場合は、作成する必要があります。

作業を開始する前に

- ONTAP 9.13.1以降では、Storage VMに最大容量を設定できます。また、SVMの容量レベルがしきい値に近づいたときにアラートを設定することもできます。詳細については、を参照してください SVM容量の管理。

手順

1. SVM を作成します。

   `vserver create -vserver` *`vserver_name`* `-rootvolume` *`root_volume_name`* `-aggregate` *`aggregate_name`* `-rootvolume-security-style unix -language C.UTF-8 -ipspace` *`ipspace_name`*

   - にUNIX設定を使用します `-rootvolume-security-style` オプション
   - デフォルトのC.UTF-8を使用します `-language` オプション
   - 。 `ipspace` 設定はオプションです。

2. 新しく作成した SVM の設定とステータスを確認します。

   `vserver show -vserver` *`vserver_name`*

   。 `Allowed Protocols` フィールドにはNFSを含める必要があります。このリストはあとで編集できます。

   。 `Vserver Operational State` フィールドにはを表示する必要があります `running` 状態。が表示された場合 `initializing` 状態にすると、ルートボリュームの作成などの中間処理が失敗したため、SVM を削除して再作成する必要があります。

例

次のコマンドは、データアクセス用の SVM を IPspace ipspaceA 内に作成します。

```
cluster1::> vserver create -vserver vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style unix -language C.UTF-8 -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

次のコマンドは、1GBのルートボリュームでSVMが作成され、自動的に起動されてに追加されたことを示しています `running` 状態。ルートボリュームには、ルールを含まないデフォルトのエクスポートポリシーがあ

るため、ルートボリュームは作成時にエクスポートされません。

```
cluster1::> vserver show -vserver vs1.example.com
                                    Vserver: vs1.example.com
                               Vserver Type: data
                            Vserver Subtype: default
                               Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                Root Volume: root_vs1
                                  Aggregate: aggr1
                                 NIS Domain: -
                  Root Volume Security Style: unix
                                 LDAP Client: -
               Default Volume Language Code: C.UTF-8
                             Snapshot Policy: default
                                     Comment:
                               Quota Policy: default
                List of Aggregates Assigned: -
 Limit on Maximum Number of Volumes allowed: unlimited
                         Vserver Admin State: running
                   Vserver Operational State: running
   Vserver Operational State Stopped Reason: -
                           Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
                        Disallowed Protocols: -
                            QoS Policy Group: -
                                 Config Lock: false
                               IPspace Name: ipspaceA
```

ONTAP 9.13.1以降では、アダプティブQoSポリシーグループテンプレートを設定して、SVM内のボリュームにスループットの下限と上限の制限を適用できます。このポリシーはSVMの作成後にのみ適用できます。このプロセスの詳細については、を参照してください アダプティブポリシーグループテンプレートを設定します。

SVM で NFS プロトコルが有効になっていることを確認します

SVM で NFS を設定して使用する前に、プロトコルが有効になっていることを確認する必要があります。

このタスクについて

この作業は通常、SVMのセットアップ時に実行します。ただし、セットアップ時にプロトコルを有効にしなかった場合でも、を使用してあとから有効にすることができます `vserver add-protocols` コマンドを実行します

作成したプロトコルは、 LIF から追加または削除することはできません。

を使用して、SVMのプロトコルを無効にすることもできます `vserver remove-protocols` コマンドを実行します

手順

1. 現在 SVM で有効になっているプロトコルと無効になっているプロトコルを確認します。

   `vserver show -vserver vserver_name -protocols`

   を使用することもできます `vserver show-protocols` コマンドを使用して、クラスタ内のすべてのSVMで現在有効になっているプロトコルを表示します。

2. 必要に応じて、プロトコルを有効または無効にします。
   - NFSプロトコルを有効にする手順は次のとおりです。 [+] `vserver add-protocols -vserver vserver_name -protocols nfs`
   - プロトコルを無効にするには： [+] `vserver remove-protocols -vserver vserver_name -protocols protocol_name[,protocol_name,…]`
3. 有効 / 無効なプロトコルが正しく更新されたことを確認します。

   `vserver show -vserver vserver_name -protocols`

例

次のコマンドは、 vs1 という SVM で現在有効 / 無効（許可 / 不許可）になっているプロトコルを表示します。

```
vs1::> vserver show -vserver vs1.example.com -protocols
Vserver           Allowed Protocols         Disallowed Protocols
-----------       ----------------------    ------------------------
vs1.example.com   nfs                       cifs, fcp, iscsi, ndmp
```

次のコマンドは、を追加することでNFS経由のアクセスを許可します `nfs` vs1というSVMで有効になっているプロトコルのリストに移動します。

```
vs1::> vserver add-protocols -vserver vs1.example.com -protocols nfs
```

SVM ルートボリュームのエクスポートポリシーを開きます

SVM ルートボリュームのデフォルトのエクスポートポリシーには、すべてのクライアントに NFS 経由のアクセスを許可するルールが含まれている必要があります。このようなルールを追加しないと、 SVM とそのボリュームに対する NFS クライアントのアクセスがすべて拒否されます。

このタスクについて

新しい SVM が作成されると、デフォルトのエクスポートポリシー（ default ）が、 SVM のルートボリュームに対して自動的に作成されます。SVM 上のデータにクライアントからアクセスできるようにするには、デフ

ォルトのエクスポートポリシーのルールを 1 つ以上作成する必要があります。

デフォルトのエクスポートポリシーを使用するすべての NFS クライアントに対してアクセスが許可されていることを確認してから、ボリュームまたは qtree ごとにカスタムのエクスポートポリシーを作成して各ボリュームへのアクセスを制限します。

手順

1. 既存の SVM を使用している場合は、デフォルトのルートボリュームエクスポートポリシーを確認します。

   `vserver export-policy rule show`

   次のようなコマンド出力が表示されます。

   ```
   cluster::> vserver export-policy rule show -vserver vs1.example.com
   -policyname default -instance

                                       Vserver: vs1.example.com
                                   Policy Name: default
                                    Rule Index: 1
                               Access Protocol:  nfs
   Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
                                RO Access Rule: any
                                RW Access Rule: any
   User ID To Which Anonymous Users Are Mapped: 65534
                      Superuser Security Types: any
                  Honor SetUID Bits in SETATTR: true
                     Allow Creation of Devices: true
   ```

   オープンアクセスを許可するこのようなルールが存在する場合、このタスクは完了です。表示されない場合は、次の手順に進みます。

2. SVM ルートボリュームのエクスポートルールを作成します。

   `vserver export-policy rule create -vserver vserver_name -policyname default -ruleindex 1 -protocol nfs -clientmatch 0.0.0.0/0 -rorule any -rwrule any -superuser any`

   Kerberosで保護されたボリュームのみをSVMに含める場合は、エクスポートルールオプションを設定できます `-rorule`、 `-rwrule`および `-superuser` ルートボリュームのをに設定します `krb5` または `krb5i`。例：

   `-rorule krb5i -rwrule krb5i -superuser krb5i`

3. を使用してルールの作成を確認します `vserver export-policy rule show` コマンドを実行します

結果

これで、 SVM で作成されたすべてのボリュームまたは qtree に、すべての NFS クライアントからアクセスできるようになります。

NFS サーバを作成します

クラスタでNFSのライセンスが有効であることを確認したら、を使用できます `vserver nfs create` コマンドを使用してSVMにNFSサーバを作成し、SVMがサポートするNFSのバージョンを指定します。

このタスクについて

SVM は、 NFS の 1 つ以上のバージョンをサポートするように設定できます。NFSv4 以降をサポートする場合は、次の点に注意してください。

- NFSv4 ユーザ ID マッピングドメイン名が、 NFSv4 サーバとターゲットクライアントで同じである必要があります。

  NFSv4 サーバとクライアントで同じ名前が使用されていれば、 LDAP または NIS のドメイン名と同じにする必要はありません。

- ターゲットクライアントで NFSv4 数値 ID 設定がサポートされている必要があります。
- セキュリティ上の理由から、 NFSv4 環境では、 LDAP をネームサービスに使用する必要があります。

作業を開始する前に

SVM を、 NFS プロトコルを許可するように設定しておく必要があります。

手順

1. クラスタ上で NFS のライセンスが有効であることを確認します。

   ```
   system license show -package nfs
   ```

   表示されない場合は、営業担当者にお問い合わせください。

2. NFS サーバを作成します。

   ```
   vserver nfs create -vserver vserver_name -v3 {enabled|disabled} -v4.0
   {enabled|disabled} -v4-id-domain nfsv4_id_domain -v4-numeric-ids
   {enabled|disabled} -v4.1 {enabled|disabled} -v4.1-pnfs {enabled|disabled}
   ```

   NFS バージョンは任意の組み合わせで有効にすることができます。pNFSをサポートする場合は、両方を有効にする必要があります `-v4.1` および `-v4.1-pnfs` オプション（ Options ）

   v4 以降を有効にする場合は、次のオプションが正しく設定されていることも確認する必要があります。

   - `-v4-id-domain`

     （オプション）このパラメータは、 NFSv4 プロトコルの定義に応じて、ユーザ名およびグループ名の文字列形式のドメイン部分を指定します。デフォルト ONTAP では、 NIS ドメインが設定されている場合は NIS ドメインを、設定されていない場合は DNS ドメインが使用されます。ターゲットクライアントで使用されているドメイン名に一致する値を指定する必要があります。

   - `-v4-numeric-ids`

     （オプション）このパラメータは、 NFSv4 所有者属性で数値文字列識別子のサポートを有効にするか

どうかを指定します。デフォルト設定は enabled ですが、ターゲットクライアントがこの設定をサポートすることを確認する必要があります。

NFSのその他の機能は、を使用してあとから有効にすることができます `vserver nfs modify` コマンドを実行します

3. NFS が実行されていることを確認します。

   `vserver nfs status -vserver` *`vserver_name`*

4. NFS が必要に応じて設定されていることを確認します。

   `vserver nfs show -vserver` *`vserver_name`*

例

次のコマンドは、 NFSv3 と NFSv4.0 が有効な vs1 という名前の SVM 上に NFS サーバを作成します。

```
vs1::> vserver nfs create -vserver vs1 -v3 enabled -v4.0 enabled -v4-id
-domain my_domain.com
```

次のコマンドは、 vs1 という名前の新しい NFS サーバのステータスと設定値を確認します。

```
vs1::> vserver nfs status -vserver vs1
The NFS server is running on Vserver "vs1".

vs1::> vserver nfs show -vserver vs1

                            Vserver: vs1
                  General NFS Access: true
                              NFS v3: enabled
                            NFS v4.0: enabled
                        UDP Protocol: enabled
                        TCP Protocol: enabled
                 Default Windows User: -
                  NFSv4.0 ACL Support: disabled
    NFSv4.0 Read Delegation Support: disabled
   NFSv4.0 Write Delegation Support: disabled
             NFSv4 ID Mapping Domain: my_domain.com
...
```

LIF を作成

LIF は、物理ポートまたは論理ポートに関連付けられた IP アドレスです。コンポーネントに障害が発生しても、 LIF は別の物理ポートにフェイルオーバーまたは移行できるため、引き続きネットワークと通信できます。

必要なもの

- 基盤となる物理または論理ネットワークポートが管理用に設定されている必要があります `up` ステータス。
- サブネット名を使用して LIF の IP アドレスとネットワークマスク値を割り当てる場合は、そのサブネットがすでに存在している必要があります。

  サブネットには、同じレイヤ 3 サブネットに属する IP アドレスのプールが含まれています。これらはを使用して作成されます `network subnet create` コマンドを実行します

- LIF で処理するトラフィックのタイプを指定するメカニズムが変更されました。ONTAP 9.5 以前では、LIF はロールを使用して処理するトラフィックのタイプを指定していました。ONTAP 9.6 以降では、サービスポリシーを使用して、処理するトラフィックのタイプを指定します。

このタスクについて

- 同じネットワークポート上に IPv4 と IPv6 の両方の LIF を作成できます。
- Kerberos 認証を使用する場合は、複数の LIF で Kerberos を有効にします。
- クラスタ内のLIFの数が多い場合は、を使用して、クラスタでサポートされるLIFの容量を確認できます `network interface capacity show` コマンドとを使用して、各ノードでサポートされるLIFの容量を確認します `network interface capacity details show` コマンド（advanced権限レベル）。
- ONTAP 9.7 以降では、同じサブネット内に SVM 用の他の LIF がすでに存在する場合、 LIF のホームポートを指定する必要はありません。ONTAP は、同じサブネットにすでに設定されている他の LIF と同じブロードキャストドメインにある指定したホームノード上のランダムなポートを自動的に選択します。

ONTAP 9.4 以降では、 FC-NVMe がサポートされます。FC-NVMe LIF を作成する場合は、次の点に注意してください。

- LIF を作成する FC アダプタで NVMe プロトコルがサポートされている必要があります。
- データ LIF で使用できるデータプロトコルは FC-NVMe のみです。
- SAN をサポートする Storage Virtual Machine （ SVM ）ごとに、管理トラフィックを処理する LIF を 1 つ設定する必要があります。
- NVMe の LIF とネームスペースは、同じノードでホストする必要があります。
- データトラフィックを処理する NVMe LIF は SVM ごとに 1 つだけ設定できます。

手順

1. LIF を作成します。

   ```
   network interface create -vserver vserver_name -lif lif_name -role data -data
   -protocol nfs -home-node node_name -home-port port_name {-address IP_address
   -netmask IP_address | -subnet-name subnet_name} -firewall-policy data -auto
   -revert {true|false}
   ```

オプション	説明
• ONTAP 9.5 以前 *	`network interface create -vserver *vserver_name* -lif *lif_name* -role data -data-protocol nfs -home-node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*

-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true	false}`
• ONTAP 9.6 以降 *	`network interface create -vserver *vserver_name* -lif *lif_name* -role data -data-protocol nfs -home-node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*
-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true	false}`

- 。 `-role` サービスポリシーを使用してLIFを作成する場合はパラメータは必要ありません（ONTAP 9.6以降）。
- 。 `-data-protocol` パラメータはLIFの作成時に指定する必要があります。あとで変更するには、データLIFを削除して再作成する必要があります。

  。 `-data-protocol` サービスポリシーを使用してLIFを作成する場合はパラメータは必要ありません（ONTAP 9.6以降）。

- `-home-node` は、の実行時にLIFが戻るノードです `network interface revert` LIFに対してコマンドを実行します。

  を使用して、LIFをホームノードおよびホームポートに自動的にリバートするかどうかを指定することもできます `-auto-revert` オプション

- `-home-port` は、の実行時にLIFが戻る物理ポートまたは論理ポートです `network interface revert` LIFに対してコマンドを実行します。
- でIPアドレスを指定できます `-address` および `-netmask` オプションを選択するか、を使用してサブネットからの割り当てを有効にします `-subnet_name` オプション
- サブネットを使用して IP アドレスとネットワークマスクを指定した場合、サブネットにゲートウェイが定義されていると、そのサブネットを使用して LIF を作成するときにゲートウェイへのデフォルトルートが SVM に自動的に追加されます。
- サブネットを使用せずに手動で IP アドレスを割り当てると、クライアントまたはドメインコントローラが別の IP サブネットにある場合にゲートウェイへのデフォルトルートの設定が必要になることがあります。。 `network route create` のマニュアルページには、SVM内での静的ルートの作成に関する情報が記載されています。
- をクリックします `-firewall-policy` オプションで、同じデフォルトを使用します `data` をLIFのロールとして使用します。

  必要に応じて、カスタムファイアウォールポリシーをあとから作成して追加できます。

  > ONTAP 9.10.1以降では、ファイアウォールポリシーは廃止され、完全にLIFのサービスポリシーに置き換えられました。詳細については、を参照してください "LIF のファイアウォールポリシーを設定します"。

- `-auto-revert` 起動時、管理データベースのステータスが変わったとき、ネットワーク接続が確立されたときなどの状況で、データLIFがホームノードに自動的にリバートされるかどうかを指定できます。デフォルト設定はです `false`に設定することもできます `false` 環境内のネットワーク管理ポリシーによって異なります。

2. を使用して、LIFが正常に作成されたことを確認します `network interface show` コマンドを実行します
3. 設定した IP アドレスに到達できることを確認します。

対象	使用
IPv4 アドレス	`network ping`
IPv6アドレス	`network ping6`

4. Kerberos を使用する場合は、手順 1~3 を繰り返して追加の LIF を作成します。

   これらの各 LIF で Kerberos を個別に有効にする必要があります。

例

次のコマンドでは、を使用してLIFを作成し、IPアドレスとネットワークマスク値を指定します `-address` および `-netmask` パラメータ：

```
network interface create -vserver vs1.example.com -lif datalif1 -role data
-data-protocol nfs -home-node node-4 -home-port e1c -address 192.0.2.145
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

次のコマンドは、 LIF を作成し、 IP アドレスとネットワークマスク値を指定したサブネット（ client1_sub ）から割り当てています。

```
network interface create -vserver vs3.example.com -lif datalif3 -role data
-data-protocol nfs -home-node node-3 -home-port e1c -subnet-name
client1_sub -firewall-policy data -auto-revert true
```

次のコマンドは、 cluster-1 内のすべての LIF を表示します。datalif1 および datalif3 というデータ LIF には IPv4 アドレスを設定しています。一方、 datalif4 には IPv6 アドレスを設定しています。

```
network interface show

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
cluster-1
            cluster_mgmt up/up    192.0.2.3/24     node-1       e1a
true
node-1
            clus1        up/up    192.0.2.12/24    node-1       e0a
true
            clus2        up/up    192.0.2.13/24    node-1       e0b
true
            mgmt1        up/up    192.0.2.68/24    node-1       e1a
true
node-2
            clus1        up/up    192.0.2.14/24    node-2       e0a
true
            clus2        up/up    192.0.2.15/24    node-2       e0b
true
            mgmt1        up/up    192.0.2.69/24    node-2       e1a
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
5 entries were displayed.
```

次のコマンドは、に割り当てられたNASデータLIFを作成する方法を示しています `default-data-files` サービスポリシー：

```
network interface create -vserver vs1 -lif lif2 -home-node node2 -homeport
e0d -service-policy default-data-files -subnet-name ipspace1
```

ホスト名解決に使用する **DNS** を有効にします

を使用できます `vserver services name-service dns` コマンドを使用してSVM

でDNSを有効にし、ホスト名解決にDNSを使用するように設定します。ホスト名は外部DNS サーバを使用して解決されます。

必要なもの

ホスト名を検索するために、サイト規模の DNS サーバが使用可能である必要があります。

単一点障害を回避するには、複数の DNS サーバを設定する必要があります。。 `vserver services name-service dns create` 入力したDNSサーバ名が1つだけの場合は警告が表示されます。

このタスクについて

SVM での動的 DNS の設定については、『ネットワーク管理ガイド』を参照してください。

手順

1. SVM で DNS を有効にします。

   `vserver services name-service dns create -vserver` *`vserver_name`* `-domains` *`domain_name`* `-name-servers` *`ip_addresses`* `-state enabled`

   次のコマンドは、 SVM vs1 で外部 DNS サーバを有効にします。

   ```
   vserver services name-service dns create -vserver vs1.example.com
   -domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
   enabled
   ```

   ONTAP 9.2以降では、 `vserver services name-service dns create` コマンドは設定の自動検証を実行し、ONTAP がネームサーバに接続できない場合はエラーメッセージを報告します。

2. を使用して、DNSドメイン設定を表示します `vserver services name-service dns show` コマンドを実行します

   次のコマンドは、クラスタ内のすべての SVM の DNS 設定を表示します。

   ```
   vserver services name-service dns show
                                                Name
   Vserver           State     Domains             Servers
   ----------------- --------- ------------------- -------------
   cluster1          enabled   example.com         192.0.2.201,
                                                   192.0.2.202
   vs1.example.com   enabled   example.com         192.0.2.201,
                                                   192.0.2.202
   ```

   次のコマンドは、 SVM vs1 の DNS 設定の詳細を表示します。

```
vserver services name-service dns show -vserver vs1.example.com
               Vserver: vs1.example.com
               Domains: example.com
          Name Servers: 192.0.2.201, 192.0.2.202
    Enable/Disable DNS: enabled
        Timeout (secs): 2
      Maximum Attempts: 1
```

3. を使用してネームサーバのステータスを検証します `vserver services name-service dns check` コマンドを実行します

   。 `vserver services name-service dns check` コマンドはONTAP 9.2以降で使用できます。

```
vserver services name-service dns check -vserver vs1.example.com

Vserver           Name Server     Status       Status Details
----------------  -------------   ----------
--------------------------
vs1.example.com   10.0.0.50         up         Response time (msec): 2
vs1.example.com   10.0.0.51         up         Response time (msec): 2
```

ネームサービスを設定

ネームサービスの概要を設定

ストレージシステムの構成によっては、クライアントに適切なアクセス権を提供するために ONTAP でホスト、ユーザ、グループ、またはネットグループ情報を検索できるようにする必要があります。この情報を取得するためには、 ONTAP がローカルまたは外部のネームサービスにアクセスできるようにネームサービスを設定する必要があります。

NIS や LDAP などのネームサービスは、クライアント認証時の名前検索を容易にするために使用する必要があります。特に NFSv4 以降を導入する際は、セキュリティ強化のために、可能なかぎり LDAP を使用することを推奨します。外部ネームサーバが使用できない場合に備えて、ローカルのユーザとグループも設定する必要があります。

ネームサービス情報は、すべてのソースで同期を維持する必要があります。

ネームサービススイッチテーブルを設定します

ONTAP がローカルまたは外部のネームサービスに問い合わせてホスト、ユーザ、グループ、ネットグループ、またはネームマッピングの情報を取得できるようにするには、ネームサービススイッチテーブルを正しく設定する必要があります。

必要なもの

ホスト、ユーザ、グループ、ネットグループ、またはネームマッピングで現在の環境に該当するように使用するネームサービスを決定しておく必要があります。

ネットグループの使用を計画する場合、ネットグループ内に指定されているすべての IPv6 アドレスは、 RFC 5952 での指定どおりに短縮および圧縮されている必要があります。

このタスクについて

使用されていない情報ソースは含めないでください。たとえば、環境でNISが使用されていない場合は、を指定しないでください `-sources nis` オプション

手順

1. ネームサービススイッチテーブルに必要なエントリを追加します。

   `vserver services name-service ns-switch create -vserver` *`vserver_name`* `-database` *`database_name`* `-sources` *`source_names`*

2. ネームサービススイッチテーブルに想定されるエントリが適切な順序で格納されていることを確認します。

   `vserver services name-service ns-switch show -vserver` *`vserver_name`*

   修正する場合は、を使用する必要があります `vserver services name-service ns-switch modify` または `vserver services name-service ns-switch delete` コマンド

例

次の例は、 SVM vs1 がローカルネットグループファイルを使用し、外部 NIS サーバがネットグループ情報をこの順序で検索するように、ネームサービススイッチテーブルに新しいエントリを作成します。

```
cluster::> vserver services name-service ns-switch create -vserver vs1
-database netgroup -sources files,nis
```

完了後

- データアクセスを提供するには、 SVM 用に指定したネームサービスを設定する必要があります。
- SVM 用のネームサービスを削除する場合は、ネームサービススイッチテーブルからも削除する必要があります。

  ネームサービススイッチテーブルからネームサービスを削除しないと、ストレージシステムへのクライアントアクセスが想定どおりに機能しない場合があります。

ローカル **UNIX** ユーザおよびグループを設定する

ローカル **UNIX** ユーザおよびグループの概要を設定する

SVM 上で、認証およびネームマッピングにローカル UNIX ユーザおよびグループを使用できます。UNIX ユーザおよびグループは、手動で作成することも、 Uniform Resource Identifier （ URI ）から UNIX ユーザまたはグループを含むファイルをロードすることも

できます。

クラスタ内のローカル UNIX ユーザグループおよびグループメンバーの合計数に対するデフォルトの上限値は 32 、 768 です。クラスタ管理者はこの制限を変更できます。

ローカル **UNIX** ユーザを作成します

を使用できます `vserver services name-service unix-user create` コマンドを使用してローカルUNIXユーザを作成します。ローカル UNIX ユーザは、 SVM 上に UNIX ネームサービスオプションとして作成し、ネームマッピングの処理で使用する UNIX ユーザです。

ステップ

1. ローカル UNIX ユーザを作成します。

   `vserver services name-service unix-user create -vserver` *`vserver_name`* `-user` *`user_name`* `-id` *`integer`* `-primary-gid` *`integer`* `-full-name` *`full_name`*

   `-user` *`user_name`* ユーザ名を指定します。ユーザ名は 64 文字以内にする必要があります。

   `-id` *`integer`* 割り当てるユーザIDを指定します。

   `-primary-gid` *`integer`* プライマリグループIDを指定します。これにより、ユーザがプライマリグループに追加されます。ユーザを作成したあと、手動でユーザを目的の追加グループに追加できます。

例

次のコマンドは、 johnm というローカル UNIX ユーザ（フルネームは「 John Miller 」）を vs1 という SVM 上に作成します。ユーザ ID は 123 で、プライマリグループ ID は 100 です。

```
node::> vserver services name-service unix-user create -vserver vs1 -user
johnm -id 123
-primary-gid 100 -full-name "John Miller"
```

URI からローカル **UNIX** ユーザをロードします

SVMで個 々 のローカルUNIXユーザを手動で作成する別の方法として、ローカルUNIXユーザのリストをUniform Resource Identifier（URI）からSVMにロードすることで、タスクを簡易化できます。 (`vserver services name-service unix-user load-from-uri`）。

手順

1. ロードするローカル UNIX ユーザのリストが含まれているファイルを作成します。

   ファイルには、UNIX内のユーザ情報が含まれている必要があります `/etc/passwd` 形式：

   `user_name: password: user_ID: group_ID: full_name`

このコマンドにより、の値が破棄されます *password* フィールドと、の後のフィールドの値 *full_name* フィールド (*home_directory* および *shell*）。

サポートされる最大ファイルサイズは 2.5MB です。

2. リストに重複した情報が含まれていないことを確認します。

   リストに重複したエントリが含まれている場合、リストのロードは失敗し、エラーメッセージが表示されます。

3. ファイルをサーバにコピーします。

   サーバには、 HTTP 、 HTTPS 、 FTP 、または FTPS 経由でストレージシステムから到達できる必要があります。

4. ファイルの URI を確認します。

   この URI は、ファイルの場所を示すためにストレージシステムに指定するアドレスです。

5. ローカル UNIX ユーザのリストが含まれているファイルを、 URI から SVM にロードします。

   `vserver services name-service unix-user load-from-uri -vserver` *vserver_name* `-uri {ftp|http|ftps|https}://`*uri* `-overwrite {true|false}`

   `-overwrite {true false}` は、エントリを上書きするかどうかを指定します。デフォルトはです `false`。

例

次のコマンドは、ローカルUNIXユーザのリストをURIからロードします `ftp://ftp.example.com/passwd` vs1という名前のSVMに追加します。URI を使用してロードした情報によって SVM 内の既存のユーザが上書きされることはありません。

```
node::> vserver services name-service unix-user load-from-uri -vserver vs1
-uri ftp://ftp.example.com/passwd -overwrite false
```

ローカル **UNIX** グループを作成します

を使用できます `vserver services name-service unix-group create` コマンドを使用して、SVMに対してローカルなUNIXグループを作成します。ローカル UNIX グループはローカル UNIX ユーザとともに使用されます。

ステップ

1. ローカル UNIX グループを作成します。

   `vserver services name-service unix-group create -vserver` *vserver_name* `-name` *group_name* `-id` *integer*

   `-name` *group_name* グループ名を指定します。グループ名は 64 文字以内にする必要があります。

`-id integer` 割り当てるグループIDを指定します。

例

次のコマンドは、 vs1 という名前の SVM 上に eng という名前のローカルグループを作成します。グループ ID は 101 です。

```
vs1::> vserver services name-service unix-group create -vserver vs1 -name
eng -id 101
```

ローカル **UNIX** グループにユーザを追加します

を使用できます `vserver services name-service unix-group adduser` コマンドを使用して、SVMに対してローカルなUNIXグループにユーザを追加します。

ステップ

1. ローカル UNIX グループにユーザを追加します。

`vserver services name-service unix-group adduser -vserver vserver_name -name group_name -username user_name`

`-name group_name` ユーザのプライマリグループに加えて、ユーザを追加するUNIXグループの名前を指定します。

例

次のコマンドは、 vs1 という SVM の eng というローカル UNIX グループに、 max という名前のユーザを追加します。

```
vs1::> vserver services name-service unix-group adduser -vserver vs1 -name
eng
-username max
```

URI からローカル **UNIX** グループをロードします

個 々 のローカルUNIXグループを手動で作成する別の方法として、を使用して、ローカルUNIXグループのリストをUniform Resource Identifier（URI）からSVMにロードすることができます `vserver services name-service unix-group load-from-uri` コマンドを実行します

手順

1. ロードするローカル UNIX グループのリストが含まれているファイルを作成します。

   ファイルには、UNIX内のグループ情報が含まれている必要があります `/etc/group` 形式：

   group_name: password: group_ID: comma_separated_list_of_users

このコマンドにより、の値が破棄されます *password* フィールド。

サポートされる最大ファイルサイズは 1MB です。

グループファイルの 1 行の最大長は、 32 、 768 文字です。

2. リストに重複した情報が含まれていないことを確認します。

   重複するエントリがリストに含まれていてはいけません。含まれていると、リストのロードに失敗します。SVMにすでにエントリがある場合は、を設定する必要があります `-overwrite` パラメータの値 `true` 既存のすべてのエントリを新しいファイルで上書きするか、または既存のエントリと重複するエントリが新しいファイルに含まれていないことを確認します。

3. ファイルをサーバにコピーします。

   サーバには、 HTTP 、 HTTPS 、 FTP 、または FTPS 経由でストレージシステムから到達できる必要があります。

4. ファイルの URI を確認します。

   この URI は、ファイルの場所を示すためにストレージシステムに指定するアドレスです。

5. ローカル UNIX グループのリストが含まれているファイルを、 URI から SVM にロードします。

   `vserver services name-service unix-group load-from-uri -vserver` *`vserver_name`* `-uri {ftp|http|ftps|https}://`*`uri`* `-overwrite {true|false}`

   `-overwrite true false}` は、エントリを上書きするかどうかを指定します。デフォルトはです `false`。このパラメータをに指定した場合 `true`と指定ONTAP したSVMの既存のローカルUNIXグループデータベース全体が、ロードするファイルのエントリで置き換えられます。

例

次のコマンドは、ローカルUNIXグループのリストをURIからロードします `ftp://ftp.example.com/group` vs1という名前のSVMに追加します。URI を使用してロードした情報によって SVM 内の既存のグループが上書きされることはありません。

```
vs1::> vserver services name-service unix-group load-from-uri -vserver vs1
-uri ftp://ftp.example.com/group -overwrite false
```

ネットグループの使用

ネットグループの概要の使用

ネットグループは、ユーザ認証に使用でき、また、エクスポートポリシールールでクライアントを照合するためにも使用できます。を使用して、外部ネームサーバ（LDAPまたはNIS）からネットグループへのアクセスを提供したり、Uniform Resource Identifier（URI）からSVMにネットグループをロードしたりできます `vserver services name-service netgroup load` コマンドを実行します

必要なもの

ネットグループを使用する前に、次の条件を満たしていることを確認する必要があります。

- ネットグループ内のすべてのホストは、ソース（ NIS 、 LDAP 、またはローカルファイル）に関係なく、フォワードおよびリバース DNS ルックアップの一貫性を提供するために、フォワード（ A ）およびリバース（ PTR ）の両方の DNS レコードを持つ必要があります。

  また、クライアントの IP アドレスが複数の PTR レコードを持つ場合は、それらすべてのホスト名がネットグループのメンバーであり、対応する A レコードを持っている必要があります。

- ネットグループ内のすべてのホストの名前が、そのソース（ NIS 、 LDAP 、またはローカルファイル）に関係なく、正しいスペルで、かつ大文字 / 小文字を正しく使用している必要があります。ネットグループで使用されているホスト名に不整合があると、エクスポートチェックの失敗など、予期しない動作が発生する可能性があります。
- ネットグループ内に指定されているすべての IPv6 アドレスは、 RFC 5952 での指定どおりに短縮および圧縮されている必要があります。

  たとえば、 2011 ： hu9 ： 0 ： 0 ： 0 ： 0 ： 3 ： 1 は 2011 ： hu9 ： 3 ： 1 に短縮する必要があります。

このタスクについて

ネットグループについては次の処理を実行できます。

- を使用できます `vserver export-policy netgroup check-membership` クライアントIPが特定のネットグループのメンバーであるかどうかを確認するためのコマンド。
- を使用できます `vserver services name-service getxxbyyy netgrp` コマンドを使用して、クライアントがネットグループの一部であるかどうかを確認します。

  検索を実行する基盤となるサービスは、設定済みのネームサービススイッチの順序に基づいて選択されます。

ネットグループを **SVM** にロードする

エクスポートポリシールールでクライアントの照合に使用できる方法の 1 つは、ネットグループにリストされているホストを使用することです。ネットグループは、外部ネームサーバに格納されているネットグループを使用する代わりに、Uniform Resource Identifier（URI）を使用してSVMにロードすることもできます (`vserver services name-service netgroup load`）。

必要なもの

ネットグループファイルは、 SVM にロードする前に、次の要件を満たしている必要があります。

- ファイルは、 NIS の設定に使用されるのと同じ適切なネットグループテキストファイル形式を使用する必要があります。

  ONTAP は、ロードを行う前にネットグループテキストファイル形式をチェックします。ファイルにエラーが含まれている場合、ファイルはロードされず、ファイルで実行する必要のある修正を示すメッセージが表示されます。エラーを修正後に、ネットグループファイルを指定した SVM に再ロードできます。

- ネットグループファイル内のホスト名に含まれる英文字は、すべて小文字にする必要があります。
- サポートされる最大ファイルサイズは 5MB です。
- ネットグループでサポートされる最大ネストレベルは 1000 です。
- ネットグループファイルでホスト名を定義する際に使用できるのは、プライマリ DNS ホスト名のみです。

  エクスポートへのアクセスに関する問題を回避するために、ホスト名の定義には DNS CNAME やラウンドロビンレコードを使用しないでください。

- ネットグループファイル内の 3 つの値のうちユーザおよびドメインの部分は、 ONTAP でサポートされていないので空にしておく必要があります。

  ホスト / IP の部分のみがサポートされます。

このタスクについて

ONTAP は、ローカルネットグループファイルを対象としたホスト単位のネットグループ検索をサポートしています。ネットグループファイルをロードしたあと、ホスト単位のネットグループ検索を有効にするために netgroup.byhost マップが ONTAP によって自動的に作成されます。これにより、エクスポートポリシールールを処理してクライアントアクセスを評価する際のローカルネットグループ検索にかかる時間が大幅に短縮されます。

ステップ

1. URI から SVM にネットグループをロードします。

   `vserver services name-service netgroup load -vserver` *`vserver_name`* `-source {ftp|http|ftps|https}://`*`uri`*

   ネットグループファイルのロードと netgroup.byhost マップの構築には、数分かかる場合があります。

   ネットグループの更新が必要な場合は、ネットグループファイルを編集し、更新されたファイルを SVM にロードすることができます。

例

次のコマンドは、HTTPのURLを使用して、ネットグループ定義をvs1というSVMにロードします `http://intranet/downloads/corp-netgroup`：

```
vs1::> vserver services name-service netgroup load -vserver vs1
-source http://intranet/downloads/corp-netgroup
```

ネットグループの定義の状態を確認します

ネットグループをSVMにロードしたら、を使用できます `vserver services name-service netgroup status` ネットグループの定義のステータスを確認するコマンド。これにより、ネットグループの定義が SVM の基盤となるすべてのノードで一貫した状態になっているかどうかを確認することができます。

手順

1. 権限レベルを advanced に設定します。

   ```
   set -privilege advanced
   ```

2. ネットグループの定義のステータスを確認します。

   ```
   vserver services name-service netgroup status
   ```

   追加情報をより詳細なビューで表示できます。

3. admin 権限レベルに戻ります。

   ```
   set -privilege admin
   ```

例

権限レベルを設定したあと、次のコマンドを実行すると、すべての SVM のネットグループのステータスが表示されます。

```
vs1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when
         directed to do so by technical support.
Do you wish to continue? (y or n): y

vs1::*> vserver services name-service netgroup status
Virtual
Server    Node            Load Time           Hash Value
--------- --------------- -------------------
--------------------------------
vs1
          node1           9/20/2006 16:04:53
e6cb38ec1396a280c0d2b77e3a84eda2
          node2           9/20/2006 16:06:26
e6cb38ec1396a280c0d2b77e3a84eda2
          node3           9/20/2006 16:08:08
e6cb38ec1396a280c0d2b77e3a84eda2
          node4           9/20/2006 16:11:33
e6cb38ec1396a280c0d2b77e3a84eda2
```

NIS ドメイン設定を作成します

現在の環境でネームサービスにNetwork Information Service（NIS；ネットワーク情報サービス）が使用されている場合は、を使用してSVMのNISドメイン設定を作成する必要があります `vserver services name-service nis-domain create` コマンドを実行します

必要なもの

SVM に NIS ドメインを設定するためには、設定済みのすべての NIS サーバが使用可能でアクセスできる状態になっている必要があります。

ディレクトリ検索での NIS の使用を予定している場合、 NIS サーバ内のマップに 1 、 024 文字を超えるエントリを持たせることはできません。この制限に従っていない NIS サーバを指定しないでください。そうしないと、 NIS エントリに依存したクライアントアクセスに失敗する可能性があります。

このタスクについて

複数の NIS ドメインを作成できます。ただし、に設定されているものだけを使用できます `active`。

NISデータベースにが含まれている場合 `netgroup.byhost` マップ、ONTAP は、検索を高速化するために使用できます。。 `netgroup.byhost` および `netgroup` クライアントアクセスの問題を回避するために、ディレクトリ内のマップは常に同期されている必要があります。ONTAP 9.7以降ではNISが使用されます `netgroup.byhost` エントリはを使用してキャッシュできます `vserver services name-service nis-domain netgroup-database` コマンド

ホスト名解決にNISを使用することはサポートされていません。

手順

1. NIS ドメイン設定を作成します。

   ```
   vserver services name-service nis-domain create -vserver vs1 -domain
   domain_name -active true -servers IP_addresses
   ```

   最大 10 台の NIS サーバを指定できます。

   > ONTAP 9.2以降では、フィールドが表示されます `-nis-servers` フィールドを置き換えます `-servers`。この新しいフィールドには、NISサーバのホスト名またはIPアドレスを指定できます。

2. ドメインが作成されたことを確認します。

   ```
   vserver services name-service nis-domain show
   ```

例

次のコマンドは、 IP アドレス 192.0.2.180 の NIS サーバを使用して、 vs1 という名前の SVM に、 nisdomain という NIS ドメインのアクティブな NIS ドメイン設定を作成します。

```
vs1::> vserver services name-service nis-domain create -vserver vs1
-domain nisdomain -active true -nis-servers 192.0.2.180
```

LDAP を使用する

LDAP の使用方法の概要

現在の環境で LDAP がネームサービス用に使用されている場合は、 LDAP 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 LDAP クライアントとして有効にする必要があります。

ONTAP 9.10.1 以降では、 LDAP チャネルバインドがデフォルトで Active Directory とネームサービスの両方の LDAP 接続でサポートされます。ONTAP は、 Start-TLS または LDAPS が有効で、セッションセキュリティが署名または封印に設定されている場合にのみ、 LDAP 接続でチャネルバインドを試行します。ネームサーバとのLDAPチャネルバインディングを無効または再度有効にするには、を使用します `-try-channel-binding` パラメータと `ldap client modify` コマンドを実行します

詳細については、を参照してください "2020 年の Windows 向け LDAP チャネルバインドおよび LDAP 署名の要件"。

- LDAP for ONTAP を設定する前に、サイト環境が LDAP サーバおよびクライアント設定のベストプラクティスを満たしていることを確認する必要があります。具体的には、次の条件を満たす必要があります。
  - LDAP サーバのドメイン名が LDAP クライアント上のエントリと一致している必要があります。
  - LDAP サーバでサポートされている LDAP ユーザパスワードハッシュタイプには、 ONTAP でサポートされているハッシュタイプが含まれている必要があります。
    - crypt （すべてのタイプ）および SHA-1 （ SHA 、 SSHA ）
    - ONTAP 9.8 以降では、 SHA-2 ハッシュ（ SHA-256 、 SSH-384 、 SHA-512 、 SSHA-256 、 SSHA-384 および SSHA-512 ）もサポートされます。
  - LDAP サーバにセッションセキュリティ対策が必要な場合は、 LDAP クライアントで設定する必要があります。

    次のセッションセキュリティオプションを使用できます。

    - LDAP 署名（データの整合性チェックを提供）および LDAP の署名と封印（データの整合性チェックと暗号化を提供）
    - START TLS
    - LDAPS （ LDAP over TLS または SSL ）
  - 署名および封印された LDAP クエリを有効にするには、次のサービスが設定されている必要があります。
    - LDAP サーバで GSSAPI （ Kerberos ） SASL がサポートされている必要があります。
    - LDAP サーバに、 DNS A/AAAA レコード、および DNS サーバで設定された PTR レコードが必要です。
    - Kerberos サーバに、 DNS サーバ上に存在する SRV レコードが必要です。
  - TLS または LDAPS を開始できるようにするには、次の点を考慮する必要があります。
    - ネットアップでは、 LDAPS ではなく Start TLS を使用することを推奨します。
    - LDAPS を使用している場合は、 ONTAP 9.5 以降で LDAP サーバの TLS または SSL が有効になっている必要があります。ONTAP 9.0~9.4 では SSL はサポートされません。
    - 証明書サーバがドメインで設定済みである必要があります。
  - LDAP リファーラル追跡を有効にするには（ ONTAP 9.5 以降）、次の条件を満たしている必要があります。
    - 両方のドメインで、次のいずれかの信頼関係を設定する必要があります。

    - 双方向
    - 一方向。一次は紹介ドメインを信頼します
    - 親子
  - 参照されているすべてのサーバ名を解決するように DNS が設定されていること。
  - bind-as-cifs-server が true に設定されている場合、認証には両ドメインのパスワードが同じであることが必要です。

> 次の設定は LDAP リファーラル追跡でサポートされません。
>
> - すべての ONTAP バージョン：
> - 管理 SVM 上の LDAP クライアント
> - ONTAP 9.8 以前では（ 9.9.1 以降でサポートされています）：
> - LDAPの署名と封印（ `-session-security` オプション）
> - 暗号化されたTLS接続（ `-use-start-tls` オプション）
> - LDAPSポート636（ `-use-ldaps-for-ad-ldap` オプション）

- SVM で LDAP クライアントを設定するときは、 LDAP スキーマを入力する必要があります。

  ほとんどの場合、デフォルトの ONTAP スキーマのいずれかが適しています。ただし、環境で使用する LDAP スキーマがこれらと異なる場合は、 LDAP クライアントを作成する前に、 ONTAP 用の新しい LDAP クライアントスキーマを作成する必要があります。環境の要件については、 LDAP 管理者にお問い合わせください。

- LDAP をホスト名解決に使用することはサポートされていません。

を参照してください。

- "ネットアップテクニカルレポート 4835 ：『 How to Configure LDAP in ONTAP 』"
- "自己署名ルート CA 証明書を SVM にインストールします"

新しい **LDAP** クライアントスキーマを作成します

環境で使用する LDAP スキーマが ONTAP のデフォルトと異なる場合は、 LDAP クライアント設定を作成する前に、 ONTAP 用の新しい LDAP クライアントスキーマを作成する必要があります。

このタスクについて

ほとんどの LDAP サーバでは、 ONTAP が提供する次のデフォルトスキーマを使用できます。

- MS-AD-BIS （ほとんどの Windows Server 2012 以降の AD サーバで推奨されるスキーマ）
- AD-IDMU （ Windows Server 2008 、 Windows Server 2012 、およびそれ以降の AD サーバ）
- AD-SFU （ Windows Server 2003 以前の AD サーバ）
- RFC-2307 （ UNIX LDAP サーバ）

デフォルト以外の LDAP スキーマを使用する必要がある場合は、 LDAP クライアント設定を作成する前にスキーマを作成する必要があります。新しいスキーマを作成する前に、 LDAP 管理者に問い合わせてください。

ONTAP に用意されているデフォルトの LDAP スキーマは変更できません。新しいスキーマを作成するには、コピーを作成し、それに応じてコピーを変更します。

手順

1. 既存の LDAP クライアントスキーマテンプレートを表示して、コピーするスキーマを特定します。

   ```
   vserver services name-service ldap client schema show
   ```

2. 権限レベルを advanced に設定します。

   ```
   set -privilege advanced
   ```

3. 既存の LDAP クライアントスキーマのコピーを作成します。

   ```
   vserver services name-service ldap client schema copy -vserver vserver_name
   -schema existing_schema_name -new-schema-name new_schema_name
   ```

4. 新しいスキーマを変更し、環境に合わせてカスタマイズします。

   ```
   vserver services name-service ldap client schema modify
   ```

5. admin 権限レベルに戻ります。

   ```
   set -privilege admin
   ```

LDAP クライアント設定を作成します

環境内の外部LDAPサービスまたはActive DirectoryサービスにONTAPからアクセスする場合は、まずストレージシステム上にLDAPクライアントを設定する必要があります。

必要なもの

Active Directoryドメイン解決リストの最初の3つのサーバのいずれかが稼働し、データを提供している必要があります。そうしないと、このタスクは失敗します。

> ⓘ 複数のサーバがあり、そのうちどの時点でも3台以上のサーバがダウンしています。

手順

1. LDAP管理者に問い合わせて、の適切な設定値を確認してください `vserver services name-service ldap client create` コマンドを実行します

   a. LDAP サーバへのドメインベースまたはアドレスベースの接続を指定します。

      - `-ad-domain` および `-servers` オプションを同時に指定することはできません。

        - を使用します `-ad-domain` Active DirectoryドメインでLDAPサーバ検出を有効にするオプション。

- を使用できます `-restrict-discovery-to-site` LDAPサーバ検出を、指定したドメインのCIFSデフォルトサイトに制限するオプション。このオプションを使用する場合は、CIFSのデフォルトサイトも指定する必要があります。 `-default-site`。

- を使用できます `-preferred-ad-servers` カンマで区切ってIPアドレスで1つ以上の優先Active Directoryサーバを指定するオプション。クライアントが作成されたら、を使用してこのリストを変更できます `vserver services name-service ldap client modify` コマンドを実行します

- を使用します `-servers` カンマで区切ってIPアドレスで1つ以上のLDAPサーバ（Active DirectoryまたはUNIX）を指定するオプション。

> 。 `-servers` オプションはONTAP 9.2で廃止されました。ONTAP 9.2以降では、`-ldap-servers` フィールドがに置き換わります `-servers` フィールド。このフィールドには、LDAPサーバのホスト名またはIPアドレスを指定できます。

b. デフォルトまたはカスタムの LDAP スキーマを指定します。

ほとんどの LDAP サーバでは、 ONTAP が提供するデフォルトの読み取り専用スキーマを使用できます。他のスキーマを使用する必要がある場合を除き、デフォルトのスキーマを使用することを推奨します。その場合は、デフォルトスキーマ（読み取り専用）をコピーし、コピーを変更することによって、独自のスキーマを作成できます。

デフォルトのスキーマ：

- MS-AD-BIS を参照してください

  RFC 2307bis に基づいて、ほとんどの標準的な Windows 2012 以降の LDAP 環境で優先される LDAP スキーマです。

- `AD-IDMU`

  Active Directory Identity Management for UNIX に基づいて、このスキーマは Windows Server 2008 、 Windows Server 2012 、およびそれ以降のほとんどの AD サーバに適しています。

- `AD-SFU`

  Active Directory Services for UNIX に基づいて、このスキーマは Windows 2003 以前のほとんどの AD サーバに適しています。

- `RFC-2307`

  RFC-2307 （ネットワーク情報サービスとして LDAP を使用するためのアプローチ）に基づいて、このスキーマはほとんどの UNIX AD サーバに適しています。

c. バインド値を選択します。

- `-min-bind-level {anonymous|simple|sasl}` 最小バインド認証レベルを指定します。

  デフォルト値はです **`anonymous`**。

- `-bind-dn` *`LDAP_DN`* バインドユーザを指定します。

  Active Directory サーバの場合は、アカウント（ DOMAIN\user ）またはプリンシパル（

user@domain.com ）の形式でユーザを指定する必要があります。それ以外の場合は、識別名（ CN=user 、 DC=domain 、 DC=com ）の形式でユーザを指定する必要があります。

- `-bind-password` *`password`* バインドパスワードを指定します。

d. 必要に応じて、セッションセキュリティオプションを選択します。

LDAP サーバで必要な場合は、 LDAP の署名と封印または LDAP over TLS を有効にすることができます。

- `--session-security {none|sign|seal}`

  署名を有効にできます (`sign`、データ整合性）、署名と封印 (`seal`、データ整合性と暗号化）、またはどちらでもない `none`、署名または封印なし）。デフォルト値はです `none`。

  また、を設定する必要があります `-min-bind-level {sasl}` バインド認証をにフォールバックする場合を除きます **`anonymous`** または **`simple`** 署名と封印のバインドが失敗した場合。

- `-use-start-tls {true|false}`

  に設定すると **`true`** LDAPサーバがサポートしており、LDAPクライアントはサーバへの暗号化されたTLS接続を使用します。デフォルト値はです **`false`**。このオプションを使用するには、LDAP サーバの自己署名ルート CA 証明書をインストールする必要があります。

> Storage VMでSMBサーバがドメインに追加されており、LDAPサーバがSMBサーバのホームドメインのドメインコントローラの1つである場合は、 `-session-security -for-ad-ldap` オプションを使用します `vserver cifs security modify` コマンドを実行します

e. ポート、クエリ、およびベースの値を選択します。

デフォルト値を推奨しますが、実際の環境に適しているかどうかを LDAP 管理者に確認する必要があります。

- `-port` *`port`* LDAPサーバポートを指定します。

  デフォルト値はです `389`。

Start TLS を使用した LDAP 接続の保護を予定している場合は、デフォルトのポート 389 を使用する必要があります。Start TLS は LDAP のデフォルトポート 389 経由でプレーンテキスト接続として開始され、その後 TLS 接続にアップグレードされます。ポートを変更すると、 Start TLS は失敗します。

- `-query-timeout` *`integer`* クエリータイムアウトを秒単位で指定します。

  指定できる範囲は 1~10 秒です。デフォルト値はです `3` 秒。

- `-base-dn` *`LDAP_DN`* ベースDNを指定します。

  必要に応じて複数の値を入力できます（ LDAP リファーラル追跡を有効にした場合など）。デフォルト値はです `""` （ルート）。

- `-base-scope {base|onelevel|subtree}` は、ベース検索範囲を指定します。

  デフォルト値はです `subtree`。

- `-referral-enabled {true|false}` LDAPリファーラル追跡を有効にするかどうかを指定します。

  ONTAP 9.5 以降では、 LDAP リファーラル追跡を有効にすると、必要なレコードが他の LDAP サーバにあることを示す LDAP リファーラル応答がプライマリ LDAP サーバから返された場合に、ONTAP LDAP クライアントがそれらの LDAP サーバに対してルックアップ要求を実行することができます。デフォルト値はです **`false`**。

参照された LDAP サーバにあるレコードを検索するには、参照されたレコードのベース DN を LDAP クライアント設定の一部としてベース DN に追加する必要があります。

2. Storage VMにLDAPクライアント設定を作成します。

```
vserver services name-service ldap client create -vserver vserver_name -client
-config client_config_name {-servers LDAP_server_list | -ad-domain ad_domain}
-preferred-ad-servers preferred_ad_server_list -restrict-discovery-to-site
{true|false} -default-site CIFS_default_site -schema schema -port 389 -query
-timeout 3 -min-bind-level {anonymous|simple|sasl} -bind-dn LDAP_DN -bind
-password password -base-dn LDAP_DN -base-scope subtree -session-security
{none|sign|seal} [-referral-enabled {true|false}]
```

> LDAPクライアント設定を作成するときは、Storage VM名を指定する必要があります。

3. LDAP クライアント設定が正常に作成されたことを確認します。

```
vserver services name-service ldap client show -client-config
client_config_name
```

例

次のコマンドでは、LDAPのActive Directoryサーバと連携するために、Storage VM vs1でldap1という名前の新しいLDAPクライアント設定を作成します。

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level simple -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100
```

次のコマンドでは、署名と封印が必要なLDAPのActive Directoryサーバと連携するために、Storage VM vs1でldap1という名前の新しいLDAPクライアント設定を作成します。LDAPサーバの検出は指定したドメインの特定のサイトに制限されます。

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -restrict
-discovery-to-site true -default-site cifsdefaultsite.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100 -session-security seal
```

次のコマンドでは、LDAPリファーラル追跡が必要なLDAPのActive Directoryサーバと連携するために、Storage VM vs1でldap1という名前の新しいLDAPクライアント設定を作成します。

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
"DC=adbasedomain,DC=example1,DC=com; DC=adrefdomain,DC=example2,DC=com"
-base-scope subtree -preferred-ad-servers 172.17.32.100 -referral-enabled
true
```

次のコマンドでは、ベースDNを指定することで、Storage VM vs1のldap1という名前のLDAPクライアント設定を変更します。

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn CN=Users,DC=addomain,DC=example,DC=com
```

次のコマンドは、リファーラル追跡を有効にすることで、Storage VM vs1のldap1という名前のLDAPクライアント設定を変更します。

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn "DC=adbasedomain,DC=example1,DC=com;
DC=adrefdomain,DC=example2,DC=com"  -referral-enabled true
```

LDAP クライアント設定を **SVM** に関連付けます

SVMでLDAPを有効にするには、を使用する必要があります `vserver services name-service ldap create` LDAPクライアント設定をSVMに関連付けるコマンド。

必要なもの

- LDAP ドメインがネットワーク内にすでに存在しており、 SVM が配置されているクラスタからアクセスできる必要があります。
- LDAP クライアント設定が SVM に存在している必要があります。

手順

1. SVMでLDAPを有効にします。

`vserver services name-service ldap create -vserver vserver_name -client-config client_config_name`

> ONTAP 9.2以降では、 `vserver services name-service ldap create` コマンドは設定の自動検証を実行し、ONTAP がネームサーバに接続できない場合はエラーメッセージを報告します。

次のコマンドは、「 vs1 」という SVM で LDAP を有効にし、「 ldap1 」という LDAP クライアント設定を使用するように設定します。

```
cluster1::> vserver services name-service ldap create -vserver vs1
-client-config ldap1 -client-enabled true
```

2. vserver services name-service ldap check コマンドを使用して、ネームサーバのステータスを検証します。

   次のコマンドは、 SVM vs1. 上の LDAP サーバを検証します。

```
cluster1::> vserver services name-service ldap check -vserver vs1

| Vserver: vs1                                                |
| Client Configuration Name: c1                               |
| LDAP Status: up                                             |
| LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13".                                              |
```

   ネームサービスのチェックコマンドは ONTAP 9.2 以降で使用できます。

ネームサービススイッチテーブルで **LDAP** ソースを確認します

ネームサービスの LDAP ソースが SVM のネームサービススイッチテーブルに正しく表示されていることを確認する必要があります。

手順

1. 現在のネームサービススイッチテーブルの内容を表示します。

   `vserver services name-service ns-switch show -vserver svm_name`

   次のコマンドは、 SVM My_SVM の結果を表示します。

```
ie3220-a::> vserver services name-service ns-switch show -vserver My_SVM
                                Source
Vserver         Database        Order
--------------- ------------    ---------
My_SVM          hosts           files,
                                dns
My_SVM          group           files,ldap
My_SVM          passwd          files,ldap
My_SVM          netgroup        files
My_SVM          namemap         files
5 entries were displayed.
```

`namemap` ネームマッピング情報を検索するソースとその検索順序を指定します。UNIX のみの環境では、このエントリは必要ありません。ネームマッピングは、 UNIX と Windows の両方を使用する混在環境でのみ必要になります。

2. を更新します `ns-switch` 必要に応じて入力：

ns-switch エントリの更新対象	入力するコマンド
ユーザ情報	`vserver services name-service ns-switch modify -vserver` *`vserver_name`* `-database passwd -sources ldap,files`
グループ情報	`vserver services name-service ns-switch modify -vserver` *`vserver_name`* `-database group -sources ldap,files`
ネットグループ情報	`vserver services name-service ns-switch modify -vserver` *`vserver_name`* `-database netgroup -sources ldap,files`

NFS で Kerberos を使用してセキュリティを強化します

NFS での Kerberos 使用によるセキュリティ強化の概要

Kerberos を強力な認証に使用している環境では、 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設定を決定し、 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に従う必要があります。

- 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

  タイムサーバで NTP を実行している必要があります。これは、時刻のずれによる Kerberos 認証の失敗を回避するために必要です。

- ドメイン名解決（ DNS ）

  それぞれの UNIX クライアントおよび SVM LIF について、 KDC の前方参照ゾーンと逆引き参照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。すべてのコンポーネントを DNS で正しく解決できる必要があります。

Kerberos 設定の権限を確認します

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	root または ID 0
GID	root または ID 0

名前	設定
UNIX 権限	755

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

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（ **Comment** ）
NFS	500ドル	0	GSS INIT フェーズで必要。 NFS クライアントユーザの 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。
ルート	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、を使用できます `vserver services name-service unix-user modify` コマンドを使用して更新します。

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.
ルート	0

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

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、を使用する必要があります `vserver nfs kerberos realm create` SVMにKerberos Realm設定を作成するコマンド。

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. で指定する適切な設定値を決定するには、Kerberos管理者に問い合わせてください `vserver nfs kerberos realm create` コマンドを実行します
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 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 で許可されている暗号化タイプを設定する

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。を使用して、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` コマンドにを指定します `-permitted-enc-types` パラメータ

このタスクについて

クライアントの互換性を最大にするために、 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、セキュリティの向上を必要としていて環境でこの機能がサポートされている場合は、この手順を使用して、 DES と 3DES を無効にしてクライアントに 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 上で 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 上で Kerberos 構成を無効にすることが必要になるからです。

  この変更を行う前に、 SVM 上で NFS クライアントが AES 暗号化に依存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. 許可されている必要な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** を有効にします

を使用できます `vserver nfs kerberos interface enable` コマンドを使用してデータLIFでKerberosを有効にします。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。

このタスクについて

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、オプションのを指定できます `-ou` パラメータ

   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 が有効になっていることを確認します。

   `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.
```