NFSを使用したファイルアクセスの管理

ONTAP 9

NetApp
April 24, 2024

目次

NFSを使用したファイルアクセスの管理

NFSv3 を有効または無効にします

NFSv3を有効または無効にするには、を変更します `-v3` オプションこれにより、NFSv3プロトコルを使用してクライアントがファイルにアクセスできるようになります。デフォルトでは、 NFSv3 が有効になっています。

ステップ

1. 次のいずれかを実行します。

状況	入力するコマンド
NFSv3 を有効にします	`vserver nfs modify -vserver vserver_name -v3 enabled`
NFSv3を無効にする	`vserver nfs modify -vserver vserver_name -v3 disabled`

NFSv4.0 を有効または無効にする

NFSv4.0を有効または無効にするには、 `-v4.0` オプションこれにより、 NFSv4.0 プロトコルを使用してクライアントがファイルにアクセスできるかどうかを指定できます。ONTAP 9.9.1では、NFSv4.0がデフォルトで有効になります。それより前のリリースでは、デフォルトで無効になっていました。

ステップ

1. 次のいずれかを実行します。

状況	入力するコマンド
NFSv4.0 を有効にする	`vserver nfs modify -vserver vserver_name -v4.0 enabled`
NFSv4.0 を無効にする	`vserver nfs modify -vserver vserver_name -v4.0 disabled`

NFSv4.1を有効または無効にする

NFSv4.1を有効または無効にするには、 `-v4.1` オプションこれにより、NFSv4.1プロトコルを使用してクライアントがファイルにアクセスできるようになります。ONTAP 9.9.1では、NFSv4.1がデフォルトで有効になります。以前のリリースでは、デフォルトで無効になっていました。

ステップ

1. 次のいずれかを実行します。

状況	入力するコマンド
NFSv4.1を有効にする	`vserver nfs modify -vserver vserver_name -v4.1 enabled`
NFSv4.1を無効にする	`vserver nfs modify -vserver vserver_name -v4.1 disabled`

NFSv4ストレージプールの制限を管理します

ONTAP 9.13以降では、クライアントあたりのストレージプールのリソース制限に達したときに、NFSv4サーバがNFSv4クライアントに対するリソースを拒否するように設定できます。クライアントがNFSv4ストレージプールリソースを大量に消費すると、NFSv4ストレージプールリソースが使用できないために他のNFSv4クライアントがブロックされる可能性があります。

この機能を有効にすると、各クライアントによるアクティブなストレージプールリソース消費量を表示することもできます。これにより、システムリソースを使い果たしているクライアントを識別しやすくなり、クライアントごとのリソース制限を課すことができます。

消費されたストレージプールリソースを表示します

。 `vserver nfs storepool show` コマンドは、消費されたストレージプールリソースの数を表示します。ストレージプールは、NFSv4クライアントが使用するリソースのプールです。

ステップ

1. 管理者としてを実行します `vserver nfs storepool show` コマンドを使用してNFSv4クライアントのstorepool情報を表示します。

例

次の例は、NFSv4クライアントのストレージプール情報を表示します。

```
cluster1::*> vserver nfs storepool show

Node: node1

Vserver: vs1

Data-Ip: 10.0.1.1

Client-Ip Protocol IsTrunked OwnerCount OpenCount DelegCount LockCount

-------------- --------- --------- ---------- ---------- ----------
---------

10.0.2.1          nfs4.1     true    2 1 0 4

10.0.2.2          nfs4.2     true    2 1 0 4

2 entries were displayed.
```

ストレージプール制限の制御を有効または無効にします

管理者は、次のコマンドを使用して、ストレージプールの制限制御を有効または無効にできます。

ステップ

1. 管理者は、次のいずれかの操作を実行します。

状況	入力するコマンド
ストレージプール制限の制御を有効にします	`vserver nfs storepool config modify -limit-enforce enabled`
ストレージプール制限の制御を無効にします	`vserver nfs storepool config modify -limit-enforce disabled`

ブロックされたクライアントのリストを表示します

ストレージプール制限が有効になっている場合、管理者は、クライアントごとのリソースしきい値に達したときにブロックされたクライアントを確認できます。管理者は次のコマンドを使用して、ブロックされたクライアントとしてマークされているクライアントを確認できます。

手順

1. を使用します `vserver nfs storepool blocked-client show` コマンドを使用してNFSv4ブロッククライアントリストを表示します。

ブロックされたクライアントリストからクライアントを削除します

クライアントあたりのしきい値に達したクライアントは切断され、ブロッククライアントキャッシュに追加されます。管理者は次のコマンドを使用して、ブロッククライアントキャッシュからクライアントを削除できます。これにより、クライアントはONTAP NFSv4サーバに接続できるようになります。

手順

1. を使用します `vserver nfs storepool blocked-client flush -client-ip <ip address>` コマンドを実行して、storepoolブロックされたクライアントキャッシュをフラッシュします。
2. を使用します `vserver nfs storepool blocked-client show` コマンドを使用して、クライアントがブロッククライアントキャッシュから削除されたことを確認します。

例

この例では、IPアドレスが「10.2.1.1」のブロックされたクライアントがすべてのノードからフラッシュされています。

```
cluster1::*>vserver nfs storepool blocked-client flush -client-ip 10.2.1.1

cluster1::*>vserver nfs storepool blocked-client show

Node: node1

Client IP
----------
10.1.1.1

1 entries were displayed.
```

pNFS を有効または無効にします

pNFS は、 NFS クライアントがストレージデバイスに対する読み取り / 書き込み処理を直接かつ並行して実行し、ボトルネックとなる可能性がある NFS サーバをバイパスできるようにすることで、パフォーマンスを向上します。pNFS（Parallel NFS）を有効または無効にするには、を変更します `-v4.1-pnfs` オプション

ONTAP リリースの種類	**pNFS** のデフォルト値
9.8以降	無効
9.7以前	有効

必要なもの

pNFS を使用するには、 NFSv4.1 のサポートが必要です。

pNFS を有効にする場合は、まず NFS リファーラルを無効にする必要があります。両方を同時に有効にすることはできません。

SVM で pNFS と Kerberos を併用する場合は、 SVM 上のすべての LIF で Kerberos を有効にする必要があります。

ステップ

1. 次のいずれかを実行します。

状況	入力するコマンド
pNFS を有効にします	`vserver nfs modify -vserver vserver_name -v4.1-pnfs enabled`
pNFS を無効にします	`vserver nfs modify -vserver vserver_name -v4.1-pnfs disabled`

関連情報

- NFSトランキングの概要

TCP および UDP 経由の NFS アクセスを制御します

TCPおよびUDP経由のStorage Virtual Machine（SVM）へのNFSアクセスを有効または無効にするには、を変更します `-tcp` および `-udp` パラメータを指定します。これにより、環境で NFS クライアントが TCP または UDP 経由でデータにアクセスできるかどうかを制御できます。

このタスクについて

これらのパラメータは NFS のみに適用されます。補助プロトコルには影響しません。たとえば、 TCP 経由の NFS が無効になっていても、 TCP 経由でのマウント処理は成功します。TCP または UDP トラフィックを完全にブロックするには、エクスポートポリシールールを使用します。

> コマンドの失敗を防ぐために、 NFS に対して TCP を無効にする前に SnapDiff RPC サーバをオフにする必要があります。TCPを無効にするには、コマンドを使用します `vserver snapdiff-rpc-server off -vserver vserver name`。

ステップ

1. 次のいずれかを実行します。

設定する NFS アクセスの状態	入力するコマンド
TCP 経由で有効化	`vserver nfs modify -vserver vserver_name -tcp enabled`
TCP 経由で無効化	`vserver nfs modify -vserver vserver_name -tcp disabled`
UDP経由で有効化	`vserver nfs modify -vserver vserver_name -udp enabled`
UDP 経由で無効にしました	`vserver nfs modify -vserver vserver_name -udp disabled`

非予約ポートからの NFS 要求を制御します

非予約ポートからのNFSマウント要求を拒否するには、を有効にします `-mount -rootonly` オプション非予約ポートからのすべてのNFS要求を拒否するには、を有効にします `-nfs-rootonly` オプション

このタスクについて

デフォルトでは、オプションです `-mount-rootonly` はです `enabled`。

デフォルトでは、オプションです `-nfs-rootonly` はです `disabled`。

これらのオプションは、 NULL 手順には適用されません。

ステップ

1. 次のいずれかを実行します。

状況	入力するコマンド
非予約ポートからの NFS マウント要求を許可します	`vserver nfs modify -vserver vserver_name -mount -rootonly disabled`
非予約ポートからの NFS マウント要求を拒否します	`vserver nfs modify -vserver vserver_name -mount -rootonly enabled`
非予約ポートからのすべての NFS 要求を許可します	`vserver nfs modify -vserver vserver_name -nfs -rootonly disabled`
非予約ポートからのすべての NFS 要求を拒否します	`vserver nfs modify -vserver vserver_name -nfs -rootonly enabled`

不明な UNIX ユーザ向けに、 NTFS ボリュームまたは qtree への NFS アクセスを処理する

ONTAP は、 NTFS セキュリティ形式のボリュームまたは qtree への接続を試みる UNIX ユーザを識別できない場合、そのユーザを Windows ユーザに明示的にマッピングできません。ONTAP は、セキュリティを厳しくするためにそのようなユーザに対してアクセスを拒否するように設定することも、そうしたユーザをデフォルトの Windows ユーザにマッピングしてすべてのユーザに最小限のレベルのアクセスを保証するように設定することもできます。

必要なもの

このオプションを有効にする場合は、デフォルトの Windows ユーザを設定する必要があります。

このタスクについて

UNIX ユーザが NTFS セキュリティ形式のボリュームまたは qtree へのアクセスを試みる場合、その UNIX ユーザは、 ONTAP が NTFS アクセス権を適切に評価できるように、まず Windows ユーザにマッピングされている必要があります。ただし、 ONTAP は、設定されているユーザ情報ネームサービスソースでその UNIX ユーザの名前を検索できなかった場合、特定の Windows ユーザにその UNIX ユーザを明示的にマッピングすることができません。このような不明な UNIX ユーザの処理方法は、次の方法で決定できます。

- 不明な UNIX ユーザに対してアクセスを拒否する。

  この場合、 NTFS ボリュームまたは qtree へのアクセス権を取得するためにすべての UNIX ユーザに明示的なマッピングを要求することで、より厳しいセキュリティが適用されます。

- 不明な UNIX ユーザをデフォルトの Windows ユーザにマッピングする。

  これにより、セキュリティは低下しますが、すべてのユーザがデフォルトの Windows ユーザを介して NTFS ボリュームまたは qtree への最小限のレベルのアクセス権を取得できるようになるため、利便性が向上します。

手順

1. 権限レベルを advanced に設定します。

   ```
   set -privilege advanced
   ```

2. 次のいずれかを実行します。

不明な UNIX ユーザへのデフォルトの Windows ユーザのマッピング	入力するコマンド
有効	`vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user enabled`
無効	`vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user disabled`

3. admin 権限レベルに戻ります。

   ```
   set -privilege admin
   ```

非予約ポートを使用して **NFS** エクスポートをマウントするクライアントに関する注意事項

。 `-mount-rootonly` 非予約ポートを使用してNFSエクスポートをマウントするクライアントをサポートする必要があるストレージシステムでは、ユーザがrootとしてログインしている場合でも、オプションを無効にする必要があります。Hummingbird クライアントや Solaris NFS / IPv6 クライアントがこれに該当します。

状況に応じて `-mount-rootonly` オプションが有効になっている場合、ONTAP では、非予約ポート（1、023より大きいポート）を使用するNFSクライアントでNFSエクスポートをマウントすることはできません。

ドメインを検証してネットグループのより厳密なアクセスチェックを実行します

デフォルトでは、 ONTAP はネットグループに対するクライアントアクセスを評価する際に追加の検証を実行します。この追加チェックにより、クライアントのドメインが Storage Virtual Machine （ SVM ）のドメイン設定に一致していることが確認されます。一致しない場合、 ONTAP はクライアントアクセスを拒否します。

このタスクについて

ONTAP は、クライアントアクセス用のエクスポートポリシールールおよびネットグループが含まれているエクスポートポリシールールを評価する際に、クライアントの IP アドレスがそのネットグループに属しているかどうかを ONTAP が確認する必要があります。そのために、 ONTAP は、 DNS を使用してクライアントの IP アドレスをホスト名に変換し、 Fully Qualified Domain Name （ FQDN ；完全修飾ドメイン名）を取得します。

ネットグループファイルにホストの短い名前のみがリストされていて、そのホストの短い名前が複数のドメインに存在している場合は、異なるドメインのクライアントがこのチェックなしでアクセス権を取得することが可能です。

この問題を回避するために、 ONTAP は、ホストについて DNS から返されたドメインを SVM 用に設定されている DNS ドメイン名のリストと比較します。一致した場合は、アクセスが許可されます。一致しない場合、アクセスは拒否されます。

この検証はデフォルトで有効になっています。これを管理するには、を変更します `-netgroup-dns-domain-search` パラメータ。advanced権限レベルで使用できます。

手順

1. 権限レベルを advanced に設定します。

   ```
   set -privilege advanced
   ```

2. 必要な操作を実行します。

ネットグループのドメイン検証の設定	入力するコマンド
有効	`vserver nfs modify -vserver vserver_name -netgroup-dns-domain-search enabled`
無効	`vserver nfs modify -vserver vserver_name -netgroup-dns-domain-search disabled`

3. 権限レベルを admin に設定します。

   ```
   set -privilege admin
   ```

NFSv3 サービスで使用されるポートを変更します

ストレージシステム上の NFS サーバは、マウントデーモンや Network Lock Manager などのサービスを使用して、特定のデフォルトネットワークポート経由で NFS クライアントと通信します。デフォルトポートは、ほとんどの NFS 環境で正しく機能するので変更する必要はありませんが、別の NFS ネットワークポートを NFSv3 環境で使用する場合はそうすることができます。

必要なもの

ストレージシステムで NFS ポートを変更するには、すべての NFS クライアントがシステムに再接続する必要があるため、変更に先立ってこの情報をユーザに伝えておく必要があります。

このタスクについて

NFS マウントデーモン、 Network Lock Manager （ NLM ；ネットワークロックマネージャ）、 Network Status Monitor （ NSM ；ネットワークステータスモニタ）、および NFS クォータデーモンの各サービスで使用されるポートを Storage Virtual Machine （ SVM ）ごとに設定できます。ポート番号の変更は、 TCP と UDP の両方でデータにアクセスする NFS クライアントに影響します。

NFSv4 および NFSv4.1 のポートは変更できません。

手順

1. 権限レベルを advanced に設定します。

   ```
   set -privilege advanced
   ```

2. NFS へのアクセスを無効にします。

   ```
   vserver nfs modify -vserver vserver_name -access false
   ```

3. 特定の NFS サービスの NFS ポートを設定します。

   ```
   vserver nfs modify -vserver vserver_namenfs_port_parameterport_number
   ```

NFS ポートのパラメータ	説明	デフォルトのポート
`-mountd-port`	NFS マウントデーモン	635
`-nlm-port`	Network Lock Manager の略	4045
`-nsm-port`	Network Status Monitor サービスの略	4046
`-rquotad-port`	NFS クォータデーモン	4049

   デフォルトポートに加えて、 1 、 024~65 、 535 の範囲のポート番号を使用できます。各 NFS サービスは一意のポートを使用する必要があります。

4. NFS へのアクセスを有効にします。

```
vserver nfs modify -vserver vserver_name -access true
```

5. を使用します `network connections listening show` ポート番号の変更を確認するコマンド。
6. admin 権限レベルに戻ります。

```
set -privilege admin
```

例

次のコマンドは、 vs1 という SVM で NFS マウントデーモンのポートを 1113 に設定します。

```
vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
         them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -access false

vs1::*> vserver nfs modify -vserver vs1 -mountd-port 1113

vs1::*> vserver nfs modify -vserver vs1 -access true

vs1::*> network connections listening show
Vserver Name     Interface Name:Local Port        Protocol/Service
---------------- -------------------------------  ----------------
Node: cluster1-01
Cluster          cluster1-01_clus_1:7700          TCP/ctlopcp
vs1              data1:4046                       TCP/sm
vs1              data1:4046                       UDP/sm
vs1              data1:4045                       TCP/nlm-v4
vs1              data1:4045                       UDP/nlm-v4
vs1              data1:1113                       TCP/mount
vs1              data1:1113                       UDP/mount
...
vs1::*> set -privilege admin
```

NFS サーバを管理するためのコマンドです

ONTAP には、 NFS サーバを管理するためのコマンドが用意されています。

状況	使用するコマンド
NFS サーバを作成します	`vserver nfs create`
NFS サーバを表示する	`vserver nfs show`

NFS サーバを変更する	`vserver nfs modify`
NFS サーバを削除する	`vserver nfs delete`
を非表示にします `.snapshot` NFSv3マウントポイント下のディレクトリリスト への明示的なアクセス `.snapshot` このオプションが有効になっていても、ディレクトリは許可されます。	`vserver nfs` を使用したコマンド `-v3-hide-snapshot` オプションを有効にします

詳細については、各コマンドのマニュアルページを参照してください。

ネームサービスの問題をトラブルシューティングする

ネームサービスの問題でクライアントでアクセスエラーが発生した場合は、を使用できます `vserver services name-service getxxbyyy` さまざまなネームサービス検索を手動で実行し、検索の詳細と結果を調べてトラブルシューティングに役立てるためのコマンドファミリー。

このタスクについて

- 各コマンドでは、次の情報を指定できます。
  - 検索を実行するノードまたは Storage Virtual Machine （ SVM ）の名前。

    これにより、特定のノードまたは SVM でネームサービス検索をテストして、想定されるネームサービス設定問題の検索を絞り込むことができます。

  - 検索に使用されるソースを表示するかどうか。

    これにより、正しいソースが使用されているかどうかを確認できます。

- ONTAP は、設定されているネームサービススイッチの順序に基づいて、検索を実行するためのサービスを選択します。
- これらのコマンドは advanced 権限レベルで使用できます。

手順

1. 次のいずれかを実行します。

取得する情報	使用するコマンド

ホスト名のIPアドレス	`vserver services name-service getxxbyyy getaddrinfo` `vserver services name-service getxxbyyy gethostbyname` （IPv4アドレスのみ）
グループIDごとのグループのメンバー	`vserver services name-service getxxbyyy getgrbygid`
グループ名ごとのグループのメンバー	`vserver services name-service getxxbyyy getgrbyname`
ユーザが属しているグループのリスト	`vserver services name-service getxxbyyy getgrlist`
IPアドレスのホスト名	`vserver services name-service getxxbyyy getnameinfo` `vserver services name-service getxxbyyy gethostbyaddr` （IPv4アドレスのみ）
ユーザ名別のユーザ情報	`vserver services name-service getxxbyyy getpwbyname` RBACユーザの名前解決をテストするには、を指定します `-use-rbac` パラメータの形式 `true`。
ユーザIDごとのユーザ情報	`vserver services name-service getxxbyyy getpwbyuid` RBACユーザの名前解決をテストするには、を指定します `-use-rbac` パラメータの形式 `true`。
クライアントのネットグループメンバーシップ	`vserver services name-service getxxbyyy netgrp`
ホスト単位のネットグループ検索を使用したクライアントのネットグループメンバーシップ	`vserver services name-service getxxbyyy netgrpbyhost`

次の例は、ホストacast1.eng.example.comのIPアドレスの取得を試みることでSVM vs1のDNSルックアップをテストします。

```
cluster1::*> vserver services name-service getxxbyyy getaddrinfo -vserver
vs1 -hostname acast1.eng.example.com -address-family all -show-source true
Source used for lookup: DNS
Host name: acast1.eng.example.com
Canonical Name: acast1.eng.example.com
IPv4: 10.72.8.29
```

次の例は、501768というUIDを持つユーザのユーザ情報の取得を試みることでSVM vs1のNIS検索をテストします。

```
cluster1::*> vserver services name-service getxxbyyy getpwbyuid -vserver
vs1 -userID 501768 -show-source true
Source used for lookup: NIS
pw_name: jsmith
pw_passwd: $1$y8rA4XX7$/DDOXAvc2PC/IsNFozfIN0
pw_uid: 501768
pw_gid: 501768
pw_gecos:
pw_dir: /home/jsmith
pw_shell: /bin/bash
```

次の例は、ldap1というユーザのユーザ情報の取得を試みることでSVM vs1のLDAP検索をテストします。

```
cluster1::*> vserver services name-service getxxbyyy getpwbyname -vserver
vs1 -username ldap1 -use-rbac false -show-source true
Source used for lookup: LDAP
pw_name: ldap1
pw_passwd: {crypt}JSPM6yc/ilIX6
pw_uid: 10001
pw_gid: 3333
pw_gecos: ldap1 user
pw_dir: /u/ldap1
pw_shell: /bin/csh
```

次の例は、クライアントdnshost0がネットグループlnetgroup136のメンバーであるかどうかを調べることでSVM vs1のネットグループ検索をテストします。

```
cluster1::*> vserver services name-service getxxbyyy netgrp -vserver vs1
-netgroup lnetgroup136 -client dnshost0 -show-source true
Source used for lookup: LDAP
dnshost0 is a member of lnetgroup136
```

1. 実行したテストの結果を分析し、必要な措置を取ります。

状況	を確認します
ホスト名または IP アドレスの検索に失敗したか、正しくない結果が得られました	DNS設定
検索で間違ったソースが照会されました	ネームサービススイッチの設定

状況	を確認します
ユーザまたはグループの検索に失敗したか、正しくない結果が得られた	• ネームサービススイッチの設定 • ソースの設定（ローカルファイル、NISドメイン、LDAPクライアント） • ネットワーク設定（ LIF 、ルートなど）
ホスト名の検索に失敗したかタイムアウトになり、DNS の短縮名（例： host1 ）が DNS サーバで解決されない	Top-Level Domain（TLD；最上位レベルのドメイン）クエリのDNS設定。を使用して、TLDクエリを無効にできます `-is-tld-query-enabled false` オプションをに設定します `vserver services name-service dns modify` コマンドを実行します

関連情報

"ネットアップテクニカルレポート 4668 ：『 Name Services Best Practices Guide 』"

ネームサービスの接続を確認

ONTAP 9.2 以降では、 DNS ネームサーバと LDAP ネームサーバが ONTAP に接続されているかどうかを確認できます。これらのコマンドは admin 権限レベルで使用できます。

このタスクについて

DNS または LDAP ネームサービスの設定が有効かどうかは、必要に応じてネームサービス設定チェックを使用して確認できます。この検証チェックは、コマンドラインまたは System Manager で実行できます。

DNS 設定の場合、すべてのサーバがテストされ、設定が有効とみなされるためにはすべてのサーバが動作している必要があります。LDAP 設定の場合は、いずれかのサーバが稼働していれば設定は有効です。ネームサービスコマンドでは、以外の設定チェックが適用されます `skip-config-validation` フィールドはtrue（デフォルトはfalse）です。

ステップ

1. 適切なコマンドを使用して、ネームサービスの設定を確認します。設定されているサーバのステータスが UI に表示されます。

確認する項目	使用するコマンド
DNS の設定ステータス	`vserver services name-service dns check`
LDAPの設定ステータス	`vserver services name-service ldap check`

```
cluster1::> vserver services name-service dns check -vserver vs0

Vserver         Name Server     Status  Status Details
--------------  --------------- ------- -------------------------
 vs0            10.11.12.13     up      Response time (msec): 55
 vs0            10.11.12.14     up      Response time (msec): 70
 vs0            10.11.12.15     down    Connection refused.
+-------------------------------------------------------------+
```

```
cluster1::> vserver services name-service ldap check -vserver vs0

| Vserver: vs0                                                |
| Client Configuration Name: c1                               |
| LDAP Status: up                                             |
| LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13".                                              |
```

設定されているサーバ（ name-servers/ldap-servers ）の少なくとも 1 つが到達可能でサービスを提供していれば、設定の検証は成功です。到達不能なサーバがある場合は、警告が表示されます。

ネームサービススイッチエントリを管理するコマンド

ネームサービススイッチエントリは、作成、表示、変更、および削除することで管理できます。

状況	使用するコマンド
ネームサービススイッチエントリを作成します	`vserver services name-service ns-switch create`
ネームサービススイッチエントリを表示します	`vserver services name-service ns-switch show`
ネームサービススイッチエントリを変更する	`vserver services name-service ns-switch modify`
ネームサービススイッチエントリを削除する	`vserver services name-service ns-switch delete`

詳細については、各コマンドのマニュアルページを参照してください。

関連情報

"ネットアップテクニカルレポート 4668 ：『 Name Services Best Practices Guide 』"

ネームサービスキャッシュを管理するコマンド

ネームサービスキャッシュは、 Time-To-Live （ TTL ）値を変更することで管理できます。TTL 値は、ネームサービス情報がキャッシュに保持される期間です。

TTL 値を変更する対象	使用するコマンド
UNIX ユーザ	`vserver services name-service cache unix-user settings`
UNIX グループ	`vserver services name-service cache unix-group settings`
UNIX ネットグループ	`vserver services name-service cache netgroups settings`
ホスト	`vserver services name-service cache hosts settings`
グループメンバーシップ	`vserver services name-service cache group-membership settings`

関連情報

"ONTAP 9コマンド"

ネームマッピングの管理用コマンド

ONTAP には、ネームマッピングを管理するためのコマンドが用意されています。

状況	使用するコマンド
ネームマッピングを作成します	`vserver name-mapping create`
特定の位置にネームマッピングを挿入します	`vserver name-mapping insert`
ネームマッピングを表示します	`vserver name-mapping show`
2 つのネームマッピングの位置を入れ替えます 注：ネームマッピングにIP修飾子エントリが設定されている場合、スワップは許可されません。	`vserver name-mapping swap`
ネームマッピングを変更する	`vserver name-mapping modify`

ネームマッピングを削除する	`vserver name-mapping delete`
ネームマッピングが正しいことを確認します	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

詳細については、各コマンドのマニュアルページを参照してください。

ローカル UNIX ユーザを管理するためのコマンド

ONTAP には、ローカル UNIX ユーザを管理するための固有のコマンドが用意されています。

状況	使用するコマンド
ローカル UNIX ユーザを作成します	`vserver services name-service unix-user create`
URI からローカル UNIX ユーザをロードします	`vserver services name-service unix-user load-from-uri`
ローカル UNIX ユーザを表示します	`vserver services name-service unix-user show`
ローカル UNIX ユーザを変更する	`vserver services name-service unix-user modify`
ローカル UNIX ユーザを削除する	`vserver services name-service unix-user delete`

詳細については、各コマンドのマニュアルページを参照してください。

ローカル UNIX グループを管理するためのコマンド

ONTAP には、ローカル UNIX グループを管理するための固有のコマンドが用意されています。

状況	使用するコマンド
ローカル UNIX グループを作成します	`vserver services name-service unix-group create`
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`
URI からローカル UNIX グループをロードします	`vserver services name-service unix-group load-from-uri`

ローカル UNIX グループを表示します	`vserver services name-service unix-group show`
ローカル UNIX グループを変更する	`vserver services name-service unix-group modify`
ローカル UNIX グループからユーザを削除します	`vserver services name-service unix-group deluser`
ローカル UNIX グループを削除する	`vserver services name-service unix-group delete`

詳細については、各コマンドのマニュアルページを参照してください。

ローカル UNIX ユーザ、グループ、およびグループメンバーに対する制限

ONTAP では、クラスタ内の UNIX ユーザおよびグループの最大数の制限と、この制限を管理するためのコマンドが導入されました。これらの制限は、管理者がクラスタ内にローカル UNIX ユーザおよびグループを過剰に作成できないようにすることで、パフォーマンスの問題を回避するのに役立ちます。

ローカル UNIX ユーザグループとグループメンバーの合計数には制限があります。ローカル UNIX ユーザについては別途制限があります。これらの制限はクラスタ全体に適用されます。これらの新しい制限はそれぞれデフォルト値に設定されており、あらかじめ割り当てられたハードリミットまで引き上げることができます。

データベース	デフォルトの制限です	ハードリミット
ローカル UNIX ユーザ	３２、７６８	六五、五三六
ローカル UNIX グループおよびグループメンバー	３２、７６８	六五、五三六

ローカル UNIX ユーザおよびグループの制限を管理します

ONTAP には、ローカル UNIX ユーザおよびグループに対する制限を管理するための固有のコマンドが用意されています。クラスタ管理者は、これらのコマンドを使用して、過剰な数のローカル UNIX ユーザおよびグループに関連していると考えられる、クラスタ内のパフォーマンスの問題のトラブルシューティングを行うことができます。

このタスクについて

これらのコマンドは、 advanced 権限レベルのクラスタ管理者が使用できます。

ステップ

1. 次のいずれかを実行します。

状況	使用するコマンド
ローカル UNIX ユーザの制限に関する情報を表示する	`vserver services unix-user max-limit show`
ローカル UNIX グループの制限に関する情報を表示します	`vserver services unix-group max-limit show`
ローカル UNIX ユーザの制限を変更する	`vserver services unix-user max-limit modify`
ローカル UNIX グループの制限を変更する	`vserver services unix-group max-limit modify`

詳細については、各コマンドのマニュアルページを参照してください。

ローカルネットグループの管理用コマンド

URI からのロード、ノード間でのステータスの確認、表示、削除を行うことで、ローカルネットグループを管理できます。

状況	使用するコマンド
URI からネットグループをロードします	`vserver services name-service netgroup load`
ノード間でのネットグループのステータスを確認します	`vserver services name-service netgroup status` advanced 権限レベル以上で使用できます。
ローカルネットグループを表示します	`vserver services name-service netgroup file show`
ローカルネットグループを削除する	`vserver services name-service netgroup file delete`

詳細については、各コマンドのマニュアルページを参照してください。

NIS ドメイン設定を管理するコマンドです

ONTAP には、 NIS ドメイン設定を管理するためのコマンドが用意されています。

状況	使用するコマンド
NIS ドメイン設定を作成します	`vserver services name-service nis-domain create`

NISドメイン設定を表示する	`vserver services name-service nis-domain show`
NIS ドメイン設定のバインドステータスを表示します	`vserver services name-service nis-domain show-bound`
NIS統計を表示する	`vserver services name-service nis-domain show-statistics` advanced 権限レベル以上で使用できます。
NIS の統計を消去します	`vserver services name-service nis-domain clear-statistics` advanced 権限レベル以上で使用できます。
NIS ドメイン設定を変更する	`vserver services name-service nis-domain modify`
NIS ドメイン設定を削除する	`vserver services name-service nis-domain delete`
ホスト単位のネットグループ検索でのキャッシュを有効にします	`vserver services name-service nis-domain netgroup-database config modify` advanced 権限レベル以上で使用できます。

詳細については、各コマンドのマニュアルページを参照してください。

LDAP クライアント設定の管理用コマンド

ONTAP には、 LDAP クライアント設定を管理するためのコマンドが用意されています。

> SVM 管理者は、クラスタ管理者が作成した LDAP クライアント設定を変更したり削除したりできません。

状況	使用するコマンド
LDAP クライアント設定を作成します	`vserver services name-service ldap client create`
LDAP クライアント設定を表示します	`vserver services name-service ldap client show`
LDAP クライアント設定を変更します	`vserver services name-service ldap client modify`
LDAP クライアントのバインドパスワードを変更します	`vserver services name-service ldap client modify-bind-password`
LDAP クライアント設定を削除します	`vserver services name-service ldap client delete`

詳細については、各コマンドのマニュアルページを参照してください。

LDAP 設定を管理するためのコマンド

ONTAP には、 LDAP 設定を管理するためのコマンドが用意されています。

状況	使用するコマンド
LDAP 設定を作成します	`vserver services name-service ldap create`
LDAP 設定を表示します	`vserver services name-service ldap show`
LDAP 設定を変更します	`vserver services name-service ldap modify`
LDAP 設定を削除します	`vserver services name-service ldap delete`

詳細については、各コマンドのマニュアルページを参照してください。

LDAP クライアントスキーマテンプレートを管理するためのコマンド

ONTAP には、 LDAP クライアントスキーマテンプレートを管理するための固有のコマンドが用意されています。

> SVM 管理者は、クラスタ管理者が作成した LDAP クライアントスキーマを変更したり削除したりできません。

状況	使用するコマンド
既存の LDAP スキーマテンプレートをコピーします	`vserver services name-service ldap client schema copy` advanced 権限レベル以上で使用できます。
LDAP スキーマテンプレートを表示します	`vserver services name-service ldap client schema show`
LDAP スキーマテンプレートを変更します	`vserver services name-service ldap client schema modify` advanced 権限レベル以上で使用できます。
LDAP スキーマテンプレートを削除します	`vserver services name-service ldap client schema delete` advanced 権限レベル以上で使用できます。

詳細については、各コマンドのマニュアルページを参照してください。

NFS Kerberos インターフェイス設定を管理するコマンドです

ONTAP には、 NFS Kerberos インターフェイスの設定を管理するためのコマンドが用意されています。

状況	使用するコマンド
LIF で NFS Kerberos を有効にします	`vserver nfs kerberos interface enable`
NFS Kerberos インターフェイスの設定を表示します	`vserver nfs kerberos interface show`
NFS Kerberos インターフェイスの設定を変更します	`vserver nfs kerberos interface modify`
LIF で NFS Kerberos を無効にします	`vserver nfs kerberos interface disable`

詳細については、各コマンドのマニュアルページを参照してください。

NFS Kerberos Realm 設定を管理するコマンド

ONTAP には、 NFS Kerberos Realm の設定を管理するための固有のコマンドが用意されています。

状況	使用するコマンド
NFS Kerberos Realm の設定を作成します	`vserver nfs kerberos realm create`
NFS Kerberos Realm の設定を表示します	`vserver nfs kerberos realm show`
NFS Kerberos Realm の設定を変更します	`vserver nfs kerberos realm modify`
NFS Kerberos Realm の設定を削除します	`vserver nfs kerberos realm delete`

詳細については、各コマンドのマニュアルページを参照してください。

エクスポートポリシーを管理するためのコマンド

ONTAP には、エクスポートポリシーを管理するためのコマンドが用意されています。

状況	使用するコマンド

エクスポートポリシーに関する情報を表示します	`vserver export-policy show`
エクスポートポリシーの名前を変更します	`vserver export-policy rename`
エクスポートポリシーをコピーする	`vserver export-policy copy`
エクスポートポリシーを削除する	`vserver export-policy delete`

詳細については、各コマンドのマニュアルページを参照してください。

エクスポートルールを管理するためのコマンド

ONTAP には、エクスポートルールを管理するためのコマンドが用意されています。

状況	使用するコマンド
エクスポートルールを作成します	`vserver export-policy rule create`
エクスポートルールに関する情報を表示する	`vserver export-policy rule show`
エクスポートルールを変更する	`vserver export-policy rule modify`
エクスポートルールを削除する	`vserver export-policy rule delete`

異なるクライアントを照合する同一のエクスポートルールが複数設定されている場合は、エクスポートルールの管理時にそれらのルールの同期を必ず維持するようにしてください。

詳細については、各コマンドのマニュアルページを参照してください。

NFS クレデンシャルキャッシュを設定する

NFS クレデンシャルキャッシュの Time-To-Live を変更する理由

ONTAP は、アクセス高速化とパフォーマンス向上のために、クレデンシャルキャッシュを使用して、 NFS エクスポートアクセスでのユーザ認証に必要な情報を格納します。情報がクレデンシャルキャッシュに格納される期間を設定して、環境に合わせてカスタマイズできます。

NFS クレデンシャルキャッシュの Time-To-Live （ TTL ）の変更が問題の解決に役立つ場合があります。どのような状況がこれに該当するか、またそうした変更がどのような影響を及ぼすかを理解しておく必要があります。

理由

次の状況では、デフォルト TTL の変更を検討してください。

問題	修正アクション
環境内のネームサーバで ONTAP からの要求の負荷が高いためにパフォーマンスが低下している。	キャッシュされている受理および拒否のクレデンシャルに対する TTL を長くして、 ONTAP からネームサーバへの要求数を減らします。
ネームサーバ管理者がこれまで拒否されていた NFS ユーザに対してアクセスを許可する変更を行った。	キャッシュされている拒否されたクレデンシャルに対する TTL を短くして、 ONTAP ユーザが新しいクレデンシャルを外部ネームサーバに要求して NFS ユーザがアクセスできるようになるまでの待機時間を短縮します。
ネームサーバ管理者がこれまで許可されていた NFS ユーザに対してアクセスを拒否する変更を行った。	キャッシュされている受理されたクレデンシャルに対する TTL を短くして、 ONTAP が新しいクレデンシャルを外部ネームサーバに要求して NFS ユーザがアクセスを拒否されるようになるまでの時間を短縮します。

結果

受理および拒否のクレデンシャルをキャッシュしておく期間を個別に変更することができます。ただし、こうした変更の長所と短所の両方に注意する必要があります。

状況	利点は ...	欠点は ...
クレデンシャルのキャッシュ時間を長くしてください	ONTAP がクレデンシャルの要求をネームサーバに送信する頻度が低下し、ネームサーバの負荷が軽減されます。	それまではアクセスが許可されていたが今後は許可されなくなる NFS ユーザに対し、アクセスを拒否するのにかかる時間が長くなります。
受理されたクレデンシャルのキャッシュ時間を短くします	それまではアクセスが許可されていたが今後は許可されなくなる NFS ユーザに対し、アクセスを拒否するのにかかる時間が短くなります。	ONTAP がクレデンシャルの要求をネームサーバに送信する頻度が高くなり、ネームサーバの負荷が増大します。
拒否されたクレデンシャルのキャッシュ時間を長くします	ONTAP がクレデンシャルの要求をネームサーバに送信する頻度が低下し、ネームサーバの負荷が軽減されます。	それまではアクセスが許可されていなかったが今後は許可されるようになる NFS ユーザに対し、アクセスを許可するのにかかる時間が長くなります。

状況	利点は ...	欠点は ...
拒否されたクレデンシャルのキャッシュ時間を短くします	それまではアクセスが許可されていなかったが今後は許可されるようになる NFS ユーザに対し、アクセスを許可するのにかかる時間が短くなります。	ONTAP がクレデンシャルの要求をネームサーバに送信する頻度が高くなり、ネームサーバの負荷が増大します。

キャッシュされた **NFS** ユーザクレデンシャルの **Time-To-Live** を設定してください

Storage Virtual Machine （ SVM ）の NFS サーバを変更することで、 ONTAP が NFS ユーザのクレデンシャルを内部キャッシュに格納する期間である Time-To-Live （ TTL ）を設定できます。これにより、ネームサーバの高負荷に関する問題や、 NFS ユーザアクセスに影響を及ぼすクレデンシャルの変更に関する問題を軽減できます。

このタスクについて

これらのパラメータは advanced 権限レベルで使用できます。

手順

1. 権限レベルを advanced に設定します。

   ```
   set -privilege advanced
   ```

2. 必要な操作を実行します。

TTL を変更するキャッシュ対象	使用するコマンド
受理のクレデンシャル	`vserver nfs modify -vserver vserver_name -cached -cred-positive-ttl time_to_live` TTL の測定単位はミリ秒です。ONTAP 9.10.1以降では、デフォルトは1時間（3,600,000ミリ秒）です。 ONTAP 9.9.1以前では、デフォルトは24時間（86、400,000ミリ秒）です。 この値の許容範囲は 1 分（ 60 、 000 ミリ秒） ~7 日間（ 604 、 800 、 000 ミリ秒）です。
拒否のクレデンシャルです	`vserver nfs modify -vserver vserver_name -cached -cred-negative-ttl time_to_live` TTL の測定単位はミリ秒です。デフォルトは 2 時間（ 7,200,000 ミリ秒）です。この値の許容範囲は 1 分（ 60 、 000 ミリ秒） ~7 日間（ 604 、 800 、 000 ミリ秒）です。

3. admin 権限レベルに戻ります。

   ```
   set -privilege admin
   ```

エクスポートポリシーキャッシュを管理します

エクスポートポリシーキャッシュをフラッシュします

ONTAP は、アクセスを高速化するために、エクスポートポリシーに関連する情報の格納に複数のエクスポートポリシーキャッシュを使用します。エクスポートポリシーキャッシュを手動でフラッシュします (`vserver export-policy cache flush`)古い可能性がある情報を削除し、ONTAP が適切な外部リソースから最新情報を取得するように強制します。これは、 NFS エクスポートへのクライアントアクセスに関するさまざまな問題の解決に役立ちます。

このタスクについて

エクスポートポリシーキャッシュの情報は、次の理由で古くなる可能性があります。

- エクスポートポリシールールが最近変更された
- ネームサーバでホスト名レコードが最近変更された
- ネームサーバでネットグループエントリが最近変更された
- ネットグループの完全なロードを妨げていたネットワーク停止からのリカバリが発生しました

手順

1. ネームサービスキャッシュを有効にしていない場合は、 advanced 権限モードで次のいずれかを実行します。

フラッシュ対象	入力するコマンド
すべてのエクスポートポリシーキャッシュ（showmount を除く）	`vserver export-policy cache flush -vserver vserver_name`
エクスポートポリシールールアクセスキャッシュ	`vserver export-policy cache flush -vserver vserver_name -cache access` オプションのを指定できます `-node` アクセスキャッシュをフラッシュするノードを指定するパラメータ。
ホスト名キャッシュ	`vserver export-policy cache flush -vserver vserver_name -cache host`
ネットグループキャッシュ	`vserver export-policy cache flush -vserver vserver_name -cache netgroup` ネットグループの処理は大量のリソースを消費します。ネットグループキャッシュのフラッシュは、古いネットグループが原因で発生したクライアントアクセス問題の解決を試みる場合にのみ行ってください。

フラッシュ対象	入力するコマンド
showmount キャッシュ	`vserver export-policy cache flush -vserver vserver_name -cache showmount`

2. ネームサービスキャッシュが有効になっている場合は、次のいずれかを実行します。

フラッシュ対象	入力するコマンド
エクスポートポリシールールアクセスキャッシュ	`vserver export-policy cache flush -vserver vserver_name -cache access` オプションのを指定できます `-node` アクセスキャッシュをフラッシュするノードを指定するパラメータ。
ホスト名キャッシュ	`vserver services name-service cache hosts forward-lookup delete-all`
ネットグループキャッシュ	`vserver services name-service cache netgroups ip-to-netgroup delete-all` `vserver services name-service cache netgroups members delete-all` ネットグループの処理は大量のリソースを消費します。ネットグループキャッシュのフラッシュは、古いネットグループが原因で発生したクライアントアクセス問題の解決を試みる場合にのみ行ってください。
showmount キャッシュ	`vserver export-policy cache flush -vserver vserver_name -cache showmount`

エクスポートポリシーネットグループのキューとキャッシュを表示します

ONTAP では、ネットグループのインポート時および解決時にネットグループキューを使用し、結果として得られる情報を格納するためにネットグループキャッシュを使用します。エクスポートポリシーのネットグループ関連の問題をトラブルシューティングする場合は、を使用できます `vserver export-policy netgroup queue show` および `vserver export-policy netgroup cache show` ネットグループキューのステータスおよびネットグループキャッシュの内容を表示するコマンド。

ステップ

1. 次のいずれかを実行します。

エクスポートポリシーネットグループに関する表示対象	入力するコマンド
キュー	`vserver export-policy netgroup queue show`

キャッシュ	`vserver export-policy netgroup cache show -vserver vserver_name`

詳細については、各コマンドのマニュアルページを参照してください。

クライアント IP アドレスがネットグループのメンバーであるかどうかを確認します

ネットグループに関連するNFSクライアントアクセスの問題をトラブルシューティングする場合は、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。

このタスクについて

ネットグループメンバーシップのチェックにより、クライアントがネットグループのメンバーであることまたはメンバーでないことを ONTAP が認識しているかどうかを確認できます。また、ネットグループ情報の更新中に ONTAP ネットグループキャッシュが一時的な状態にあるかどうかもわかります。この情報は、クライアントに対して予期せずアクセスが許可または拒否される理由を理解するのに役立ちます。

ステップ

1. クライアントIPアドレスのネットグループメンバーシップを確認します。 `vserver export-policy netgroup check-membership -vserver vserver_name -netgroup netgroup_name -client-ip client_ip`

   このコマンドによって次のような結果が返されることがあります。

   - クライアントはネットグループのメンバーです。

     これは、リバースルックアップスキャンまたはホスト単位のネットグループ検索によって確認されました。

   - クライアントはネットグループのメンバーです。

     クライアントが ONTAP のネットグループキャッシュに見つかりました。

   - クライアントはネットグループのメンバーではありません。
   - ONTAP が現在ネットグループキャッシュを更新中なので、まだクライアントのメンバーシップを決定できません。

     これが完了するまで、メンバーシップの判断を明示的に下すことはできません。を使用します `vserver export-policy netgroup queue show` ネットグループのロードを監視し、完了後にチェックを再試行するコマンド。

例

次の例は、 IP アドレスが 172.17.16.72 のクライアントが SVM vs1 上のネットグループ mercury のメンバーであるかどうかをチェックします。

```
 cluster1::> vserver export-policy netgroup check-membership -vserver vs1
-netgroup  mercury -client-ip 172.17.16.72
```

アクセスキャッシュのパフォーマンスを最適化

複数のパラメータを設定して、アクセスキャッシュを最適化したり、パフォーマンスとアクセスキャッシュに格納される情報の鮮度とのバランスをとったりすることができます。

このタスクについて

アクセスキャッシュの更新期間を設定するときは、次の点に注意してください。

- 値を大きくすると、アクセスキャッシュ内のエントリの保持期間が長くなります。

  長所としては、 ONTAP がアクセスキャッシュエントリの更新時に消費するリソースの減少によるパフォーマンスの向上が挙げられます。短所は、エクスポートポリシールールが変更されてアクセスキャッシュエントリが古くなった場合、エントリの更新にかかる時間が長くなることです。その結果、アクセスできるはずのクライアントが拒否され、拒否されるはずのクライアントがアクセス権を取得する可能性があります。

- 値を小さくすると、 ONTAP によるアクセスキャッシュエントリの更新頻度が高くなります。

  長所は、エントリの鮮度が向上し、クライアントに対するアクセスの許可または拒否が正しく行われる可能性が高くなることです。短所としては、 ONTAP がアクセスキャッシュエントリの更新時に消費するリソースの増加によるパフォーマンスの低下が挙げられます。

手順

1. 権限レベルを advanced に設定します。

   ```
   set -privilege advanced
   ```

2. 必要な操作を実行します。

変更の対象	入力するコマンド
正のエントリの更新期間	`vserver export-policy access-cache config modify-all-vservers -refresh -period-positive timeout_value`
負のエントリの更新期間	`vserver export-policy access-cache config modify-all-vservers -refresh -period-negative timeout_value`
古いエントリのタイムアウト時間	`vserver export-policy access-cache config modify-all-vservers -harvest -timeout timeout_value`

3. 新しいパラメータ設定を確認します。

```
vserver export-policy access-cache config show-all-vservers
```

4. admin 権限レベルに戻ります。

```
set -privilege admin
```

ファイルロックを管理します

プロトコル間のファイルロックについて

ファイルロックは、あるユーザが以前に開いていたファイルに別のユーザがアクセスするのを防ぐために、クライアントアプリケーションで使用される方法です。ONTAP でファイルをロックする方法は、クライアントのプロトコルによって異なります。

クライアントが NFS クライアントである場合、ロックは任意に設定します。クライアントが SMB クライアントである場合、ロックは必須となります。

NFS ファイルと SMB ファイルのロックの違いのため、 SMB アプリケーションですでに開いているファイルに NFS クライアントからアクセスすると、エラーになる場合があります。

NFS クライアントが SMB アプリケーションによってロックされたファイルにアクセスすると、次のいずれかの状態になります。

- mixed形式またはNTFS形式のボリュームでは、などのファイル操作が行われます `rm`、 `rmdir`および `mv` NFSアプリケーションが失敗するように原因 できますか。
- NFS の読み取りと書き込みの処理は、 SMB の読み取り拒否および書き込み拒否のオープンモードによってそれぞれ拒否されます。
- また、ファイルの書き込み対象となる範囲が、排他的な SMB バイトロックでロックされている場合も、NFS の書き込みの処理はエラーになります。

UNIX セキュリティ形式のボリュームでは、 NFS のリンク解除および名前変更の処理で SMB のロック状態が無視され、ファイルへのアクセスが許可されます。UNIX セキュリティ形式のボリュームでのその他すべての NFS 処理では、 SMB のロック状態が考慮されます。

ONTAP による読み取り専用ビットの処理方法

読み取り専用ビットは、ファイルが書き込み可能（無効）なのか読み取り専用（有効）なのかを示すために、ファイルごとに設定されます。

Windows を使用する SMB クライアントは、ファイルごとの読み取り専用ビットを設定できます。NFS クライアントは、ファイルごとの読み取り専用ビットを設定しません。 NFS クライアントは、ファイルごとの読み取り専用ビットを使用するプロトコル操作を行わないためです。

ONTAP は、 Windows を使用する SMB クライアントによってファイルが作成される際に、そのファイルに読み取り専用ビットを設定できます。ファイルが NFS クライアントと SMB クライアント間で共有されている場合も、 ONTAP は読み取り専用ビットを設定できます。一部のソフトウェアは、 NFS クライアントおよび SMB クライアントで使用される場合、読み取り専用ビットが有効になっている必要があります。

NFS クライアントと SMB クライアント間で共有されるファイルに対して、適切な読み取りおよび書き込み権限を保持するために、読み取り専用ビットが次の規則に従って処理されます。 ONTAP

- NFS は、読み取り専用ビットが有効になっているファイルを書き込み権限ビットが無効になっているファイルとして扱います。
- NFS クライアントがすべての書き込み権限ビットを無効にしたときに、これらのうち少なくとも 1 つが以前有効であったら、 ONTAP はそのファイルの読み取り専用ビットを有効にします。
- NFS クライアントがすべての書き込み権限ビットを有効にすると、 ONTAP はそのファイルの読み取り専用ビットを無効にします。
- あるファイルの読み取り専用ビットが有効になっているときに、 NFS クライアントがそのファイルの権限を調べようとすると、そのファイルの権限ビットは NFS クライアントには送信されず、代わりに書き込み権限ビットがマスクされた権限ビットが ONTAP クライアントに送信されます。
- ファイルの読み取り専用ビットが有効になっているときに、 SMB クライアントがこの読み取り専用ビットを無効にすると、 ONTAP はそのファイルに対する所有者の書き込み権限ビットを有効にします。
- 読み取り専用ビットが有効になっているファイルに書き込めるのは、 root のみです。

> ファイル権限の変更は、 SMB クライアントではすぐに反映されますが、 NFS クライアントが属性のキャッシュを有効にしている場合は NFS クライアントではすぐに反映されないことがあります。

共有パスコンポーネントのロックの処理に関する **ONTAP** と **Windows** の違い

Windows とは異なり、 ONTAP では、ファイルが開いているときにそのファイルのパスの各コンポーネントがロックされません。この動作は SMB 共有パスにも影響します。

ONTAP 原因ではパスの各コンポーネントがロックされないため、開いているファイルまたは共有より上のパスコンポーネントの名前を変更できます。このため、特定のアプリケーションで原因の問題が発生したり、SMB 構成の共有パスを無効な名前に変更したりすることができます。原因によって共有にアクセスできなくなる可能性があります。

パスコンポーネントの名前変更による問題を回避するには、Windows Access Control List（ACL；アクセス制御リスト）のセキュリティ設定を適用して、ユーザやアプリケーションが重要なディレクトリの名前を変更できないようにします。

の詳細を確認してください "クライアントがアクセスしている間にディレクトリの名前を変更しないようにする方法"。

ロックに関する情報を表示します

有効になっているロックの種類とロックの状態、バイト範囲ロック、共有ロックモード、委譲ロック、および便宜的ロックの詳細、永続性ハンドルを使用してロックが開かれているかどうかなど、現在のファイルロックに関する情報を表示できます。

このタスクについて

NFSv4 または NFSv4.1 を使用して確立されたロックについては、クライアント IP アドレスを表示できません。

デフォルトでは、すべてのロックに関する情報が表示されます。コマンドパラメータを使用すると、特定の

Storage Virtual Machine （ SVM ）のロックに関する情報を表示したり、他の条件によってコマンドの出力をフィルタリングしたりできます。

。 `vserver locks show` コマンドは、次の4種類のロックに関する情報を表示します。

- バイト範囲ロック。ファイルの一部のみをロックします。
- 共有ロック。開いているファイルをロックします。
- 便宜的ロック。 SMB を使用してクライアント側キャッシュを制御します。
- 委譲。 NFSv4.x を使用してクライアント側キャッシュを制御します

オプションのパラメータを指定すると、各ロックタイプに関する重要な情報を確認できます。詳細については、コマンドのマニュアルページを参照してください。

ステップ

1. を使用して、ロックに関する情報を表示します `vserver locks show` コマンドを実行します

例

次の例は、パスのファイルに対するNFSv4ロックに関する概要情報を表示します `/vol1/file1`。共有ロックのアクセスモードは write-deny_none であり、書き込み委譲でロックが許可されています。

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path                LIF         Protocol  Lock Type   Client
------- ------------------------- ----------- --------- -----------
-------
vol1    /vol1/file1                lif1        nfsv4     share-level -
               Sharelock Mode: write-deny_none
                                                          delegation  -
               Delegation Type: write
```

次の例は、パスのファイルに対するSMBロックに関するoplockおよび共有ロックの詳細情報を表示します `/data2/data2_2/intro.pptx`。IP アドレスが 10.3.1.3 のクライアントに対して、共有ロックのアクセスモードを write-deny_none として、永続性ハンドルが許可されています。バッチの oplock レベルで oplock リースが許可されています。

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx

                    Vserver: vs1
                     Volume: data2_2
         Logical Interface: lif2
               Object Path: /data2/data2_2/intro.pptx
                 Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
             Lock Protocol: cifs
                 Lock Type: share-level
   Node Holding Lock State: node3
```

```
                Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: -
   Shared Lock Access Mode: write-deny_none
       Shared Lock is Soft: false
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: durable
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

                   Vserver: vs1
                    Volume: data2_2
         Logical Interface: lif2
               Object Path: /data2/data2_2/test.pptx
                 Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
             Lock Protocol: cifs
                 Lock Type: op-lock
   Node Holding Lock State: node3
                Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: -
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

ロックを解除します

ファイルロックが原因でクライアントがファイルにアクセスできなくなっている場合は、現在有効なロックの情報を表示して、特定のロックを解除することができます。ロックの解除が必要になるケースとしては、アプリケーションのデバッグなどが挙げられます。

このタスクについて

。 `vserver locks break` コマンドは、advanced権限レベル以上でのみ使用できます。詳細については、コマンドのマニュアルページを参照してください。

手順

1. ロックを解除するために必要な情報を確認するには、を使用します `vserver locks show` コマンドを実行します

   詳細については、コマンドのマニュアルページを参照してください。

2. 権限レベルを advanced に設定します。

   ```
   set -privilege advanced
   ```

3. 次のいずれかを実行します。

ロックを解除するための指定項目	入力するコマンド
SVM 名、ボリューム名、 LIF 名、およびファイルパス	`vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif`
ロック ID	`vserver locks break -lockid UUID`

4. admin 権限レベルに戻ります。

   ```
   set -privilege admin
   ```

NFS での FPolicy の first-read および first-write フィルタの動作

外部 FPolicy サーバを使用して FPolicy が有効になっていて、読み取り / 書き込み処理が監視対象イベントの場合、読み取り / 書き込み要求のトラフィックが多いと NFS クライアントで応答時間が長くなります。NFS クライアントの場合、 FPolicy で first-read フィルタと first-write フィルタを使用すると、 FPolicy 通知の数が減り、パフォーマンスが向上します。

NFS では、クライアントはファイルに対して I/O を実行する際に、ファイルのハンドルを取得します。このハンドルは、サーバとクライアントのリブート後も有効なままになる場合があります。このため、クライアントはハンドルを自由にキャッシュし、ハンドルを再取得しなくてもハンドルに対する要求を送信できます。通常のセッションでは、大量の読み取り / 書き込み要求がファイルサーバに送信されます。これらのすべての要

求について通知が生成されると、次の問題が発生する可能性があります。

- 追加の通知処理により負荷が増大し、応答時間が長くなります。
- サーバに影響のない通知も含め、多数の通知が FPolicy サーバに送信される。

クライアントから特定のファイルに対する最初の読み取り / 書き込み要求を受信すると、キャッシュエントリが作成され、読み取り / 書き込みの数が増分されます。この要求は初回読み取り / 書き込み処理とマークされ、 FPolicy イベントが生成されます。NFS クライアント用の FPolicy フィルタを計画して作成する前に、FPolicy フィルタの基本的な仕組みを理解しておく必要があります。

- first-read ：初回読み取りのクライアント要求をフィルタリングします。

  このフィルタはNFSイベントに使用されます `-file-session-io-grouping-count` および `-file-session-io-grouping-duration` FPolicyが処理される初回読み取り要求は、設定によって決まります。

- first-write ：初回書き込みのクライアント要求をフィルタリングします。

  このフィルタはNFSイベントに使用されます `-file-session-io-grouping-count` および `-file-session-io-grouping-duration` 設定により、FPolicyが処理された初回書き込み要求が決まります。

NFS サーバのデータベースには、次のオプションが追加されます。

```
file-session-io-grouping-count: Number of I/O Ops on a File to Be Clubbed
and Considered as One Session
for Event Generation
file-session-io-grouping-duration: Duration for Which I/O Ops on a File to
Be Clubbed and Considered as
One Session for Event Generation
```

NFSv4.1 サーバ実装 ID を変更する

NFSv4.1 プロトコルには、サーバのドメイン、名前、および日付を記録したサーバ実装 ID が含まれています。サーバ実装 ID のデフォルト値は変更できます。デフォルト値を変更すると、たとえば、使用率の統計を収集したり、相互運用性の問題をトラブルシューティングしたりするときに役立ちます。詳細については、 RFC 5661 を参照してください。

このタスクについて

3 つのオプションのデフォルト値は次のとおりです。

オプション	オプション名	デフォルト値
NFSv4.1 実装 ID - ドメイン	`-v4.1-implementation-domain`	NetApp.com にアクセスします

オプション	オプション名	デフォルト値
NFSv4.1 実装 ID の名前	`-v4.1-implementation-name`	クラスタバージョンの名前
NFSv4.1 実装 ID - 日付	`-v4.1-implementation-date`	クラスタバージョンの日付

手順

1. 権限レベルを advanced に設定します。

   ```
   set -privilege advanced
   ```

2. 次のいずれかを実行します。

変更する **NFSv4.1** 実装 **ID** のオプション	入力するコマンド
ドメイン	`vserver nfs modify -v4.1 -implementation-domain domain`
名前	`vserver nfs modify -v4.1 -implementation-name name`
日付	`vserver nfs modify -v4.1 -implementation-date date`

3. admin 権限レベルに戻ります。

   ```
   set -privilege admin
   ```

NFSv4 ACLs を管理します

NFSv4 ACL を有効化する利点

NFSv4 ACL を有効化すると多くの利点を得られます。

NFSv4 ACL を有効にする利点は次のとおりです。

- ファイルやディレクトリへのユーザアクセスのより詳細な制御
- NFS セキュリティが向上します
- CIFS との相互運用性の向上
- NFS のユーザあたりの最大グループ数は 16 ではなくなりました

NFSv4 ACL の仕組み

NFSv4 ACL を使用しているクライアントは、システム上のファイルとディレクトリに ACL を設定し、その ACL を表示することができます。ACL が設定されているディレク

トリ内にファイルやサブディレクトリを新しく作成すると、新しいファイルやサブディレクトリには、その ACL 内の ACE のうち、該当する継承フラグが指定された ACL エントリ（ACE ）がすべて継承されます。

ファイルやディレクトリが NFSv4 要求によって作成される場合、作成されるファイルやディレクトリの ACL は、ファイル作成要求に ACL が含まれているか、または標準の UNIX ファイルアクセス権限のみが含まれているか、および親ディレクトリに ACL が設定されているかどうかによって異なります。

- 要求に ACL が含まれる場合は、その ACL が使用されます。
- 要求に標準 UNIX ファイルアクセス権限のみが含まれ、親ディレクトリに ACL がある場合、親ディレクトリの ACL の ACE に適切な継承フラグのタグが付けられていれば、それらの ACE が新しいファイルやディレクトリに継承されます。

親ACLは、の場合でも継承されます `-v4.0-acl` がに設定されます `off`。

- 要求に標準の UNIX ファイルアクセス権限のみが含まれ、親ディレクトリに ACL がない場合は、クライアントのファイルモードを使用して標準の UNIX ファイルアクセス権限が設定されます。
- 要求に標準 UNIX ファイルアクセス権限のみが含まれ、親ディレクトリに継承できない ACL がある場合は、モードビットのみを使用して新しいオブジェクトが作成されます。

状況に応じて `-chown-mode` パラメータがに設定されました `restricted` でコマンドを使用します `vserver nfs` または `vserver export-policy rule` ファミリーの場合、NFSv4 ACLで設定されたディスク上の権限でroot以外のユーザがファイル所有権を変更できる場合でも、スーパーユーザのみがファイル所有権を変更できます。詳細については、関連するマニュアルページを参照してください。

NFSv4 ACL の変更を有効または無効にします

ONTAP がを受信したとき `chmod` ACLが設定されたファイルまたはディレクトリに対するコマンド。デフォルトでは、ACLは保持され、モードビットの変更を反映するように変更されます。を無効にすることができます `-v4-acl-preserve` 代わりにACLをドロップする場合に動作を変更するパラメータ。

このタスクについて

unified セキュリティ形式を使用している場合、このパラメータは、クライアントがファイルまたはディレクトリに対する chmod 、 chgroup 、または chown コマンドを送信したときに NTFS ファイルアクセス権が保持されるか破棄されるかの指定も行います。

このパラメータのデフォルトは enabled です。

手順

1. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

2. 次のいずれかを実行します。

状況	入力するコマンド

既存の NFSv4 ACL の保持と変更を有効にする（デフォルト）	`vserver nfs modify -vserver vserver_name -v4-acl -preserve enabled`
保持を無効にして、モードビットを変更するときに NFSv4 ACL を破棄します	`vserver nfs modify -vserver vserver_name -v4-acl -preserve disabled`

3. admin 権限レベルに戻ります。

   ```
   set -privilege admin
   ```

ONTAP での NFSv4 ACL を使用したファイル削除の可否の判別方法

ファイルを削除できるかどうかを判別するために、 ONTAP は、そのファイルの DELETE ビットと、ファイルが含まれるディレクトリの DELETE_CHILD ビットの組み合わせを使用します。詳細については、 NFS 4.1 RFC 5661 を参照してください。

NFSv4 ACL を有効または無効にします

NFSv4 ACLを有効または無効にするには、を変更します `-v4.0-acl` および `-v4.1-acl` オプション（ Options ）これらのオプションは、デフォルトでは無効になっています。

このタスクについて

。 `-v4.0-acl` または `-v4.1-acl` オプションは、NFSv4 ACLの設定と表示を制御します。アクセスチェックでのNFSv4 ACLの適用は制御しません。

ステップ

1. 次のいずれかを実行します。

状況	作業
NFSv4.0 ACL を有効にする	次のコマンドを入力します。 `vserver nfs modify -vserver vserver_name -v4.0-acl enabled`
NFSv4.0 ACL を無効にする	次のコマンドを入力します。 `vserver nfs modify -vserver vserver_name -v4.0-acl disabled`
NFSv4.1 ACLを有効にする	次のコマンドを入力します。 `vserver nfs modify -vserver vserver_name -v4.1-acl enabled`

NFSv4.1 ACLを無効にする	次のコマンドを入力します。 `vserver nfs modify -vserver vserver_name -v4.1-acl disabled`

NFSv4 ACL の ACE の最大数を変更する

パラメータを変更すると、各NFSv4 ACLに許可されるACEの最大数を変更できます `-v4-acl-max-aces`。デフォルトでは、 ACL あたりの ACE の数は 400 個に制限されています。この制限を引き上げることで、 400 個を超える ACE を含む ACL のデータを、ONTAP を実行するストレージシステムに移行できるようになります。

このタスクについて

この制限値を増やすと、 NFSv4 ACL を含むファイルにアクセスするクライアントのパフォーマンスが低下することがあります。

手順

1. 権限レベルを advanced に設定します。

   ```
   set -privilege advanced
   ```

2. NFSv4 ACL の ACE の最大数を変更します。

   ```
   vserver nfs modify -v4-acl-max-aces max_ace_limit
   ```

   の有効な範囲

   `max_ace_limit` はです `192` 終了： `1024`.

3. admin 権限レベルに戻ります。

   ```
   set -privilege admin
   ```

NFSv4 ファイル委譲を管理します

NFSv4 読み取りファイル委譲を有効または無効にします

NFSv4読み取りファイル委譲を有効または無効にするには、を変更します `-v4.0-read-delegation`または オプション読み取りファイル委譲を有効にすると、ファイルのオープンとクローズに伴うメッセージのオーバーヘッドを大幅に軽減できます。

このタスクについて

デフォルトでは、読み取りファイル委譲は無効です。

読み取りファイル委譲を有効にした場合の欠点は、サーバのリブートまたはリスタート後、クライアントのリブートまたはリスタート後、あるいはネットワークを分割したあとに、サーバおよびそのクライアントが委譲

をリカバリする必要があることです。

ステップ

1. 次のいずれかを実行します。

状況	作業
NFSv4 読み取りファイル委譲を有効にする	次のコマンドを入力します。 `vserver nfs modify -vserver vserver_name -v4.0 -read-delegation enabled`
NFSv4.1 読み取りファイル委譲を有効にします	次のコマンドを入力します。 [+] `vserver nfs modify -vserver vserver_name -v4.1 -read-delegation enabled`
NFSv4 読み取りファイル委譲を無効にする	次のコマンドを入力します。 `vserver nfs modify -vserver vserver_name -v4.0 -read-delegation disabled`
NFSv4.1読み取りファイル委譲を無効にする	次のコマンドを入力します。 `vserver nfs modify -vserver vserver_name -v4.1 -read-delegation disabled`

結果

ファイル委譲オプションの変更はすぐに反映されます。NFS のリブートやリスタートは必要ありません。

NFSv4 書き込みファイル委譲を有効または無効にします

書き込みファイル委譲を有効または無効にするには、を変更します `-v4.0-write-delegation`または オプション書き込みファイル委譲を有効にすると、ファイルのオープンとクローズだけでなく、ファイルおよびレコードのロックに関連するメッセージのオーバーヘッドを大幅に軽減できます。

このタスクについて

デフォルトでは、書き込みファイル委譲は無効です。

書き込みファイル委譲を有効にした場合の欠点は、サーバのリブートまたはリスタート後、クライアントのリブートまたはリスタート後、あるいはネットワークを分割したあとに、サーバおよびそのクライアントが委譲をリカバリするための追加タスクを実行する必要があることです。

ステップ

1. 次のいずれかを実行します。

状況	作業
NFSv4 書き込みファイル委譲を有効にします	次のコマンドを入力します。 `vserver nfs modify -vserver vserver_name -v4.0 -write-delegation enabled`
NFSv4.1書き込みファイル委譲を有効にする	次のコマンドを入力します。 `vserver nfs modify -vserver vserver_name -v4.1 -write-delegation enabled`
NFSv4 書き込みファイル委譲を無効にする	次のコマンドを入力します。 `vserver nfs modify -vserver vserver_name -v4.0 -write-delegation disabled`
NFSv4.1 書き込みファイル委譲を無効にします	次のコマンドを入力します。 `vserver nfs modify -vserver vserver_name -v4.1 -write-delegation disabled`

結果

ファイル委譲オプションの変更はすぐに反映されます。NFS のリブートやリスタートは必要ありません。

NFSv4 ファイルおよびレコードロックを設定する

NFSv4 ファイルおよびレコードロックについて

NFSv4 クライアントの場合、 ONTAP は NFSv4 のファイルロックメカニズムをサポートしているため、すべてのファイルのロック状態がリースベースモデルで保持されます。

"ネットアップテクニカルレポート 3580 ：『 NFSv4 の拡張内容とベスト・プラクティス・ガイド - Data ONTAP での実装』"

NFSv4 ロックリース期間を指定します

NFSv4ロックリース期間（ONTAP がクライアントに解除不能なロックを付与する期間）を指定するには、を変更します `-v4-lease-seconds` オプションリース期間を短くするとサーバのリカバリにかかる時間が短縮され、リース期間を長くすると、大量のクライアントを処理するサーバに効果的です。

このタスクについて

デフォルトでは、このオプションはに設定されています `30`。このオプションの最小値はです `10`。このオプションの最大値はロック猶予期間です。この期間は、で設定できます `locking.lease_seconds` オプション

手順

1. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

2. 次のコマンドを入力します。

```
vserver nfs modify -vserver vserver_name -v4-lease-seconds number_of_seconds
```

3. admin 権限レベルに戻ります。

```
set -privilege admin
```

NFSv4 ロック猶予期間を指定します

NFSv4ロック猶予期間（サーバリカバリ中にクライアントがロック状態をONTAP に再要求する期間）を指定するには、を変更します `-v4-grace-seconds` オプション

このタスクについて

デフォルトでは、このオプションはに設定されています `45`。

手順

1. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

2. 次のコマンドを入力します。

```
vserver nfs modify -vserver vserver_name -v4-grace-seconds number_of_seconds
```

3. admin 権限レベルに戻ります。

```
set -privilege admin
```

NFSv4 リファーラルの仕組み

NFSv4 リファーラルを有効にすると、 ONTAP は NFSv4 クライアントに対して「 SVM 内」のリファーラルを提供します。SVM 内リファーラルでは、 NFSv4 要求を受け取ったクラスタノードが、 NFSv4 クライアントに Storage Virtual Machine （ SVM ）の別の論理インターフェイス（ LIF ）を紹介します。

NFSv4 クライアントは、それ以降、ターゲット LIF でリファーラルを受け取ったパスにアクセスする必要があります。元のクラスタノードがこのようなリファーラルを返すのは、データボリュームが存在するクラスタノード上の SVM に LIF があるため、クライアントがデータにより高速にアクセスでき、余分なクラスタ通信が回避されると判断された場合です。

NFSv4 リファーラルを有効または無効にします

Storage Virtual Machine（SVM）でNFSv4リファーラルを有効にするには、オプションを有効にします `-v4-fsid-change` および `-v4.0-referrals`または。NFSv4 リファ

ーラルを有効にすると、この機能をサポートする NFSv4 クライアントのデータへのアクセス速度を向上させることができます。

必要なもの

NFS リファーラルを有効にする場合は、まず Parallel NFS を無効にする必要があります。両方を同時に有効にすることはできません。

手順

1. 権限レベルを advanced に設定します。

   ```
   set -privilege advanced
   ```

2. 次のいずれかを実行します。

状況	入力するコマンド
NFSv4 リファーラルを有効にする	`vserver nfs modify -vserver vserver_name -v4-fsid -change enabled` `vserver nfs modify -vserver vserver_name -v4.0-referrals enabled`
NFSv4 リファーラルを無効にする	`vserver nfs modify -vserver vserver_name -v4.0 -referrals disabled`
NFSv4.1リファーラルを有効にする	`vserver nfs modify -vserver vserver_name -v4-fsid -change enabled` `vserver nfs modify -vserver vserver_name -v4.1-referrals enabled`
NFSv4.1リファーラルを無効にする	`vserver nfs modify -vserver vserver_name -v4.1 -referrals disabled`

3. admin 権限レベルに戻ります。

   ```
   set -privilege admin
   ```

NFS統計の表示

パフォーマンスを監視して問題を診断するために、ストレージシステム上の Storage Virtual Machine （ SVM ）の NFS 統計を表示することができます。

手順

1. を使用します `statistics catalog object show` コマンドを使用して、データを表示できるNFSオブジェクトを特定します。

   ```
   statistics catalog object show -object nfs*
   ```

2. を使用します `statistics start` およびオプションです `statistics stop` 1つ以上のオブジェクトからデータサンプルを収集するコマンド。

3. を使用します `statistics show` コマンドを使用してサンプルデータを表示します。

例：**NFSv3**のパフォーマンスの監視

次の例は、 NFSv3 プロトコルのパフォーマンスデータを表示します。

次のコマンドは、新しいサンプルのデータ収集を開始します。

```
vs1::> statistics start -object nfsv3 -sample-id nfs_sample
```

次のコマンドは、正常に行われた読み取り要求および書き込み要求の数と読み取り要求と書き込み要求の総数を比較するカウンタを指定して、サンプルからデータを表示します。

```
vs1::> statistics show -sample-id nfs_sample -counter
read_total|write_total|read_success|write_success

Object: nfsv3
Instance: vs1
Start-time: 2/11/2013 15:38:29
End-time: 2/11/2013 15:38:41
Cluster: cluster1

    Counter                                                     Value
    -------------------------- ---------------------------
    read_success                                                40042
    read_total                                                  40042
    write_success                                             1492052
    write_total                                               1492052
```

関連情報

"パフォーマンス監視のセットアップ"

DNS統計を表示します。

パフォーマンスを監視して問題を診断するために、ストレージシステム上のStorage Virtual Machine（SVM）のDNS統計を表示することができます。

手順

1. を使用します `statistics catalog object show` コマンドを使用して、データを表示できるDNSオブジェクトを特定します。

   ```
   statistics catalog object show -object external_service_op*
   ```

2. を使用します `statistics start` および `statistics stop` 1つ以上のオブジェクトからデータサンプルを収集するコマンド。

3. を使用します `statistics show` コマンドを使用してサンプルデータを表示します。

DNS 統計を監視しています

次の例は、 DNS クエリのパフォーマンスデータを表示します。次のコマンドは、新しいサンプルのデータ収集を開始します。

```
vs1::*> statistics start -object external_service_op -sample-id
dns_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
dns_sample2
```

次のコマンドは、送信した DNS クエリの数と、受信した / 失敗した / タイムアウトになった DNS クエリの数を比較するカウンタを指定して、サンプルからデータを表示します。

```
vs1::*> statistics show -sample-id dns_sample1 -counter
num_requests_sent|num_responses_received|num_successful_responses|num_time
outs|num_request_failures|num_not_found_responses

Object: external_service_op
Instance: vs1:DNS:Query:10.72.219.109
Start-time: 3/8/2016 11:15:21
End-time: 3/8/2016 11:16:52
Elapsed-time: 91s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    num_not_found_responses                                        0
    num_request_failures                                           0
    num_requests_sent                                              1
    num_responses_received                                         1
    num_successful_responses                                       1
    num_timeouts                                                   0
6 entries were displayed.
```

次のコマンドは、特定のサーバの DNS クエリに対して特定のエラーを受信した回数を示すカウンタを指定して、サンプルからデータを表示します。

```
vs1::*> statistics show -sample-id dns_sample2 -counter
server_ip_address|error_string|count

Object: external_service_op_error
Instance: vs1:DNS:Query:NXDOMAIN:10.72.219.109
Start-time: 3/8/2016 11:23:21
End-time: 3/8/2016 11:24:25
Elapsed-time: 64s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    count                                                           1
    error_string                                             NXDOMAIN
    server_ip_address                                   10.72.219.109
3 entries were displayed.
```

関連情報

"パフォーマンス監視のセットアップ"

NIS統計を表示する

パフォーマンスを監視して問題を診断するために、ストレージシステム上のStorage Virtual Machine（SVM）のNIS統計を表示することができます。

手順

1. を使用します `statistics catalog object show` コマンドを使用して、データを表示できるNISオブジェクトを特定します。

   ```
   statistics catalog object show -object external_service_op*
   ```

2. を使用します `statistics start` および `statistics stop` 1つ以上のオブジェクトからデータサンプルを収集するコマンド。
3. を使用します `statistics show` コマンドを使用してサンプルデータを表示します。

NIS 統計を監視する

次の例は、 NIS クエリのパフォーマンスデータを表示します。次のコマンドは、新しいサンプルのデータ収集を開始します。

```
vs1::*> statistics start -object external_service_op -sample-id
nis_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
nis_sample2
```

次のコマンドは、送信した NIS クエリの数と、受信した / 失敗した / タイムアウトになった NIS クエリの数を比較するカウンタを指定して、サンプルからデータを表示します。

```
vs1::*> statistics show -sample-id nis_sample1 -counter
instance|num_requests_sent|num_responses_received|num_successful_responses
|num_timeouts|num_request_failures|num_not_found_responses

Object: external_service_op
Instance: vs1:NIS:Query:10.227.13.221
Start-time: 3/8/2016 11:27:39
End-time: 3/8/2016 11:27:56
Elapsed-time: 17s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    num_not_found_responses                                         0
    num_request_failures                                            1
    num_requests_sent                                               2
    num_responses_received                                          1
    num_successful_responses                                        1
    num_timeouts                                                    0
6 entries were displayed.
```

次のコマンドは、特定のサーバの NIS クエリに対して特定のエラーを受信した回数を示すカウンタを指定して、サンプルからデータを表示します。

```
vs1::*> statistics show -sample-id nis_sample2 -counter
server_ip_address|error_string|count

Object: external_service_op_error
Instance: vs1:NIS:Query:YP_NOTFOUND:10.227.13.221
Start-time: 3/8/2016 11:33:05
End-time: 3/8/2016 11:33:10
Elapsed-time: 5s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    count                                                           1
    error_string                                           YP_NOTFOUND
    server_ip_address                                    10.227.13.221
3 entries were displayed.
```

関連情報

"パフォーマンス監視のセットアップ"

VMware vStorage over NFS がサポートされるようになりました

ONTAP は、 NFS 環境で特定の VMware vStorage API for Array Integration （ VAAI ）機能をサポートしています。

サポートされている機能

次の機能がサポートされます。

- コピーオフロード

  ESXi ホストで、仮想マシンや仮想マシンディスク（ VMDK ）のコピーを、ホストを介さずにソースとデスティネーションのデータストア間で直接実行できます。これにより、 ESXi ホストの CPU サイクルやネットワーク帯域幅を節約できます。ソースボリュームがスパースボリュームの場合、コピーオフロードでスペース効率が保持されます。

- スペースリザベーション

  スペースをリザーブして VMDK ファイル用のストレージスペースを確保します。

制限

NFS で VMware vStorage を使用する際には、次の制限事項があります。

- 次の場合にコピーオフロード処理が失敗することがあります。
  - ソースボリュームまたはデスティネーションボリュームで wafliron を実行中に、ボリュームが一時的にオフラインになっている
  - ソースボリュームまたはデスティネーションボリュームを移動しているとき
  - ソースまたはデスティネーションの LIF を移動しているとき
  - テイクオーバーまたはギブバック処理を実行しているとき
  - スイッチオーバーまたはスイッチバック処理を実行しているとき
- 次のシナリオでは、ファイルハンドル形式の違いが原因でサーバ側のコピーが失敗する可能性があります。

  qtree のエクスポートを現在行っているか、以前行っていた SVM から、これまでに qtree をエクスポートしたことがない SVM へのデータのコピーを試みます。上記の制限を回避するために、デスティネーション SVM で少なくとも 1 つの qtree をエクスポートすることができます。

関連情報

"Data ONTAP では、 VAAI オフロード処理はどのようにサポートされていますか。"

VMware vStorage over NFS を有効または無効にします

を使用して、Storage Virtual Machine（SVM）でVMware vStorage over NFSのサポートを有効または無効にできます `vserver nfs modify` コマンドを実行します

このタスクについて

デフォルトでは、 VMware vStorage over NFS のサポートは無効になっています。

手順

1. SVM での現在の vStorage のサポートステータスを表示します。

   ```
   vserver nfs show -vserver vserver_name -instance
   ```

2. 次のいずれかを実行します。

状況	入力するコマンド
VMware vStorage のサポートを有効にします	`vserver nfs modify -vserver vserver_name -vstorage enabled`
VMware vStorage のサポートを無効にします	`vserver nfs modify -vserver vserver_name -vstorage disabled`

完了後

この機能を使用する前に、 NFS Plug-in for VMware VAAI をインストールしておく必要があります。詳細については、「 NetApp NFS Plug-in for VMware VAAI のインストール」を参照してください。

関連情報

"ネットアップのマニュアル： NetApp NFS Plug-in for VMware VAAI"

rquota のサポートを有効または無効にします

ONTAP は、 remote quota protocol バージョン 1 （ rquota v1 ）をサポートしています。rquota プロトコルを使用すると、 NFS クライアントは、リモートマシンからユーザのクォータ情報を取得できます。Storage Virtual Machine（SVM）でrquotaを有効にするには、を使用します `vserver nfs modify` コマンドを実行します

このタスクについて

デフォルトでは、 rquota は無効です。

ステップ

1. 次のいずれかを実行します。

状況	入力するコマンド
SVM で rquota のサポートを有効にします	`vserver nfs modify -vserver vserver_name -rquota enable`
SVM で rquota のサポートを無効にします	`vserver nfs modify -vserver vserver_name -rquota disable`

クォータの詳細については、を参照してください "論理ストレージ管理"。

TCP 転送サイズを変更することで NFSv3 / NFSv4 のパフォーマンスが向上します

TCP 最大転送サイズを変更することで、高レイテンシのネットワーク経由でストレージシステムに接続する NFSv3 / NFSv4 クライアントのパフォーマンスを向上させることができます。

レイテンシが 10 ミリ秒を超えるワイドエリアネットワーク（ WAN ）またはメトロエリアネットワーク（ MAN ）などの高レイテンシネットワークを介してクライアントがストレージシステムにアクセスしている場合は、 TCP 最大転送サイズを変更することで、ネットワーク接続のパフォーマンスを向上させることができます。ローカルエリアネットワーク（ LAN ）などの低レイテンシネットワークでストレージシステムにアクセスするクライアントは、これらのパラメータを変更してもパフォーマンスの向上はあまり期待できません。スループットの向上がレイテンシの影響を上回らない場合は、これらのパラメータを使用しないでください。

ストレージ環境がこれらのパラメータの変更の恩恵を受けるかどうかを判断するには、まずパフォーマンスの低い NFS クライアントで総合的なパフォーマンス評価を行ってください。パフォーマンスの低さが、クライアント上の過剰なラウンドトリップによるレイテンシとデータ量の少ない要求によるものかどうかを確認します。このような状況では、クライアントとサーバは、接続を介して送信される小さな要求と応答を待機するデューティサイクルの大部分を消費するため、使用可能な帯域幅を完全に使用することはできません。

NFSv3 と NFSv4 の要求サイズを大きくすることで、クライアントとサーバは使用可能な帯域幅をより効果的に使用できるようになり、単位時間あたりの移動データ量が多くなります。そのため、接続の全体的な効率が向上します。

ストレージシステムとクライアントの間で設定が異なる場合があることに注意してください。ストレージシステムとクライアントでサポートされる転送処理の最大サイズは 1MB です。ただし、ストレージシステムで最大転送サイズを 1MB に設定しても、クライアントがサポートするサイズが 64KB であると、マウントの転送サイズは 64KB 以下に制限されます。

これらのパラメータを変更する前に注意しなければならないのは、変更すると、大量の応答をアセンブルして送信するのに時間がかかり、ストレージシステムでメモリ消費が増えるということです。ストレージシステムへの高レイテンシ接続が増えるほど、メモリ消費量も増加します。メモリ容量が多いストレージシステムでは、この変更による影響はほとんどありません。メモリ容量が少ないストレージシステムでは、パフォーマンスが著しく低下する可能性があります。

これらのパラメータを効果的に使用するには、クラスタの複数のノードからデータを取得する必要があります。クラスタネットワーク固有のレイテンシによって、応答の全体的なレイテンシが増加する可能性があります。これらのパラメータを使用するときに、全体的なレイテンシが増大する傾向があります。そのため、レイテンシの影響を受けやすいワークロードは悪影響を受ける可能性があります。

NFSv3 と NFSv4 の TCP 最大転送サイズを変更する

を変更できます `-tcp-max-xfer-size` NFSv3およびNFSv4.xプロトコルを使用するすべてのTCP接続の最大転送サイズを設定するオプション。

このタスクについて

これらのオプションは Storage Virtual Machine （ SVM ）ごとに変更できます。

ONTAP 9以降では、を参照してください `v3-tcp-max-read-size` および `v3-tcp-max-write-size` オプションは廃止されました。を使用する必要があります `-tcp-max-xfer-size` 代わりにオプション。

手順

1. 権限レベルを advanced に設定します。

   ```
   set -privilege advanced
   ```

2. 次のいずれかを実行します。

状況	入力するコマンド
NFSv3 または NFSv4 の TCP 最大転送サイズを変更する	`vserver nfs modify -vserver vserver_name -tcp-max-xfer-size integer_max_xfer_size`

オプション	範囲	デフォルト
`-tcp-max-xfer-size`	8192~1048576 バイト	65536バイト

> 最大転送サイズには、 4KB （ 4096 バイト）の倍数を入力する必要があります。要求が要件を満たしていない場合は、パフォーマンスが低下します。

3. を使用します `vserver nfs show -fields tcp-max-xfer-size` コマンドを使用して変更を確認します。
4. 静的マウントを使用しているクライアントがある場合、新しいパラメータサイズを有効にするには、いったんアンマウントしてから再度マウントします。

例

次のコマンドは、 vs1 という SVM で NFSv3 と NFSv4.x の TCP 最大転送サイズを 1 、 048 、 576 バイトに設定します。

```
vs1::> vserver nfs modify -vserver vs1 -tcp-max-xfer-size 1048576
```

NFS ユーザに許可するグループ ID の数を設定します

ONTAP は、 Kerberos （ RPCSEC_GSS ）認証を使用して NFS ユーザクレデンシャル

を処理する場合、デフォルトで最大 32 個のグループ ID をサポートしています。AUTH_SYS 認証を使用する場合は、 RFC 5331 で定義されているとおり、グループ ID のデフォルトの最大数は 16 個です。デフォルト数を超えるグループに属しているユーザがいる場合は、この最大数を 1 、 024 まで増やすことができます。

このタスクについて

デフォルト数を超えるグループ ID がクレデンシャルに設定されている場合、残りのグループ ID は切り捨てられ、そのユーザがストレージシステムのファイルにアクセスしようとするとエラーが発生する可能性があります。SVM あたりの最大グループ数は、環境内の最大グループ数と同じ数に設定する必要があります。

次の表に、の2つのパラメータを示します `vserver nfs modify` 3つの設定例でグループIDの最大数を決定するコマンド。

パラメータ	設定	結果として得られるグループ ID の上限数

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`32`
	
	`disabled`
	
	これらはデフォルト設定です。
		RPCSEC_GSS ： 32
		
		AUTH_SYS ： 16

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`256`
	
	`disabled`
		RPCSEC_GSS：256
		
		AUTH_SYS ： 16

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`512`
	
	`enabled`
		RPCSEC_GSS：512
		
		AUTH_SYS：512

手順

1. 権限レベルを advanced に設定します。

   ```
   set -privilege advanced
   ```

2. 必要な操作を実行します。

許可される補助グループの最大数の設定対象	入力するコマンド
RPCSEC_GSS の場合のみ、 AUTH_SYS はデフォルト値の 16 に設定されます	`vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups disabled`
RPCSEC_GSS と AUTH_SYS の両方	`vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups enabled`

3. を確認します `-extended-groups-limit` AUTH_SYSが拡張グループを使用しているかどうかを確認します。 `vserver nfs show -vserver vserver_name -fields auth-sys-extended-groups,extended-groups-limit`
4. admin 権限レベルに戻ります。

   ```
   set -privilege admin
   ```

例

次の例は、拡張されたグループを AUTH_SYS 認証で有効にし、 AUTH_SYS 認証と RPCSEC_GSS 認証の両方で拡張グループの最大数を 512 に設定します。これらの変更は、 vs1 という SVM にアクセスするクライアントに対してのみ行われます。

```
vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
         them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -auth-sys-extended-groups enabled
-extended-groups-limit 512

vs1::*> vserver nfs show -vserver vs1 -fields auth-sys-extended-
groups,extended-groups-limit
vserver auth-sys-extended-groups extended-groups-limit
------- ------------------------ ---------------------
vs1     enabled                  512

vs1::*> set -privilege admin
```

NTFS セキュリティ形式のデータへの root ユーザアクセスを制御する

NTFS セキュリティ形式のデータへの NFS クライアントアクセスを許可したり、 NTFS クライアントによる NFS セキュリティ形式データへのアクセスを許可したりするように ONTAP を設定することができます。NFS データストアで NTFS セキュリティ形式を使用する際には、 root ユーザによるアクセスの処理方法を決定し、それに応じて Storage Virtual Machine （ SVM ）を設定する必要があります。

このタスクについて

root ユーザが NTFS セキュリティ形式のデータにアクセスする際には、次の 2 つのオプションがあります。

- 他の NFS ユーザと同様に root ユーザを Windows ユーザにマッピングし、 NTFS ACL に従ってアクセスを管理する。
- NTFS ACL を無視してフルアクセスを root に対して提供する。

手順

1. 権限レベルを advanced に設定します。

   ```
   set -privilege advanced
   ```

2. 必要な操作を実行します。

root ユーザへの対処方法	入力するコマンド
Windows ユーザにマッピングする	`vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root disabled`
NT ACL チェックをバイパスします	`vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root enabled`

   デフォルトでは、このパラメータは無効になっています。

   このパラメータが有効になっていても root ユーザに対するネームマッピングが存在しない場合、 ONTAP はデフォルトの SMB 管理者のクレデンシャルを監査に使用します。

3. admin 権限レベルに戻ります。

   ```
   set -privilege admin
   ```