テクニカル レポート

Name Services Best Practices Guide

ONTAP 9.3

NetApp
Chris Hurley
2018年3月| TR-4668

概要

このドキュメントでは、NetApp® ONTAP® にCIFS / SMBやNFSなどのネットワーク接続型ストレージ（NAS）ソリューションを実装する際のベストプラクティス、制限事項、推奨事項、考慮事項を包括的に説明します。

情報の分類

パブリック

バージョン履歴

バージョン	日付	ドキュメント バージョン履歴
バージョン1.0	2018年3月	Chris Hurley：初版執筆。 TR-4379への完全な更新古いドキュメントは TR-4379で参照できます。

目次

表一覧

図一覧

ベストプラクティス一覧

1 概要

NetApp ONTAPオペレーティングシステムでは、Storage Virtual Machine（SVM）を使用して単一のネームスペースの下にクライアントを統合できます。これらのSVMは、最大24ノードのクラスタに配置できます。各SVMでは、認証目的でLDAP、NIS、DNS、およびローカルファイル設定を個別に提供できます。これらの機能は「ネームサービス」とも呼ばれます。

外部サーバは、UID、GID、グループメンバーシップ、ホームディレクトリ、およびその他の情報、およびネットグループおよび名前解決機能。これらの外部サーバを使用すると、管理オーバーヘッドを増やすことなく、グローバルな場所にまたがる大規模な環境を管理できます。また、データベースのローカライズされたコピーをクライアントやサーバに提供することで、WANのレイテンシを低減できます。

1.1 スコープ

本ドキュメントでは、次のトピックについて説明します。

- ONTAP NASの概要
- ネームサービスの概要
- サポートされる構成
- NASでネームサービスを使用するメリット
- 構成とベストプラクティス

注：このドキュメントでは、9.3以降のバージョンのONTAPのみを対象としています。ONTAPでは他のバージョンへの参照がいくつかあります。

1.2 対象読者および前提条件

本テクニカル レポートは、ストレージ管理者、システム管理者、およびデータセンター管理者を対象としており、以下の点に精通していることを前提としています。

ONTAPとサポート対象のプラットフォーム（FAS、AFF、Select、クラウド）

ネットワークファイル共有プロトコル

注： このドキュメントでは、advancedレベルとdiagレベルのコマンドについて説明しています。これらのコマンドを使用する際には、細心の注意を払ってください。ご質問やご不明な点がある場合は、NetAppサポートにお問い合わせください。

1.3 ネームサービスとは

ネームサービスは、NetAppストレージシステムからの名前要求を処理するオブジェクトです。名前要求は、ユーザ、グループ、ネットグループ、またはホスト名に対するもので、ローカルリソースまたは外部リソースから取得できます。該当するリソースは、次のとおりです。

ローカルファイル（hosts、passwd、netgroupなど）

- DNS
- NIS
- LDAP
- Active Directory

1.4 Storage Virtual Machine（SVM）のタイプ

ONTAPには複数のタイプのSVMが含まれます。

- **データSVM** はデータアクセスに使用されます。
- **クラスタSVM** はクラスタの管理に使用される

2 ONTAPのNAS

ONTAP 9オペレーティングシステムは、NASの運用を実行するクライアントにワールドクラスのエンタープライズレベルのストレージを提供し、次のようなユースケースに対応します。

- ホーム ディレクトリ
- アプリケーションデータベースのホスティング
- アーカイブとステージング
- ソフトウェアソース管理
- ログファイルノストレージ
- ビデオ ストリーミング
- 非構造化データの共有

ONTAPオペレーティングシステムは、CIFSとNFSの両方で最先端のテクノロジをサポートしているため、世界中のデータセンターで最新かつ優れた機能セットを活用できます。

サポートされるプロトコルバージョンは次のとおりです。

- NFSv3、NFSv4、NFSv4.1
- SMB 1.0、SMB 2.x、およびSMB 3.x

これらのプロトコルでサポートされる機能の詳細については、TR-4067および TR-4191を参照してください。

注： SMB1.0はサポート対象として記載されていますが、セキュリティの問題との脆弱性があるため、ご使用の環境では推奨されず無効にする必要があります。

2.1 ONTAPオペレーティングシステムでのNAS要求の動作

ONTAPでNAS処理を実行する場合、クラスタには最大24ノードを含めることができます。各物理ノードは、ボリュームやデータLIFなどの仮想オブジェクトを所有できます。SVMはクラスタ内のすべてのノードにまたがっており、論理ストレージエンティティを単一のネームスペースでやり取りできます。NASクライアントがCIFSまたはNFSを使用してONTAPシステムに接続しようとすると、DNS、クライアント設定、およびIPアドレスを所有するLIFをホストするノードに基づいて、その要求が24ノードクラスタ内の任意のノードに到達する可能性があります。データLIFをホストしているノードが、アクセスを要求されたデータボリュームを所有していないNAS処理で使用されている場合は、 次に、NAS要求が最適化されたONTAPプロトコルに解析され、トラフィックは専用の高速イーサネット（10GbEまたは40GbE）クラスタバックエンドネットワークを経由します。

NASの基本

次のセクションでは、NAS要求の基本的な相互作用について概要を説明します。

ボリューム

ONTAPシステム内のユーザデータはすべてフレキシブルボリューム（NetApp FlexVol®ボリューム）に格納されます。これらのボリュームは、物理ディスクスペース（アグリゲート）をホストするノードに対してローカルに配置されます。ONTAPでは、データが物理的に配置されているノードに関係なく、クラスタ内のどこからでもデータにアクセスできます。

注： ONTAPには、FlexGroup®と呼ばれるコンテナにデータを格納する機能もあります。この概念については、本テクニカルレポートでは説明していません。FlexGroupボリュームへのデータの格納方法の詳細については、TR-4557を参照してください。

論理インターフェイス

各SVMは、ボリュームや論理インターフェイス（LIF）などのストレージオブジェクトを所有します。LIFは、割り当てられているロールと許可されているデータプロトコルに応じて、管理トラフィック、データトラフィ

ック、またはクラスタトラフィックをホストできます。オプションを使用する `-data-protocol` と、ストレージ管理者は、データLIFで許可するデータプロトコルを指定できます。あるデータLIFでデータプロトコルが許可されると、LIFはそのプロトコルに対して特定のポートのリストをリスンします。NASプロトコル（CIFSおよびNFS）の場合、表1に示すポートは、データLIFでプロトコルが許可されたときに開かれます。

表1）プロトコル対応データLIFのNFS / CISトラフィック用ポート

プロトコル	ポート
NFS	2049：NFS 2049（プログラムバージョン400010）：vStorage 111:ポートマッパー 635：mountd 4045：ネットワークロックマネージャ（NLM） 4046：Network Status Monitor（NSM；ネットワークステータスモニタ） 4049：rquota
CIFS	135：RPC 139：NetBIOS 445：SMB 40001：SMB監視
FlexCache	2050：FlexCache（元のボリュームから7-Mode FlexCacheへ）

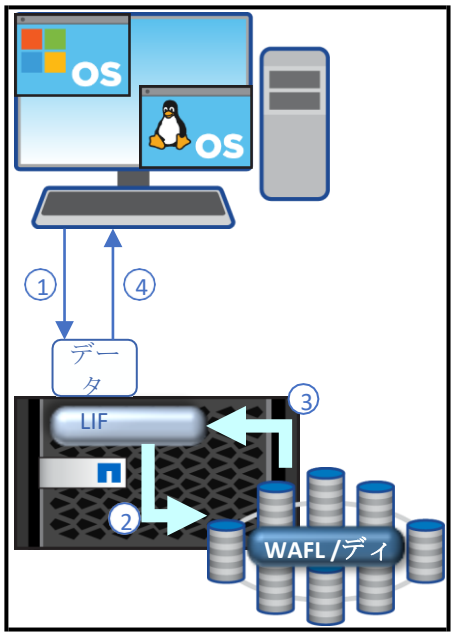
SVMに対してNAS要求が送信されると、要求は常にデータLIFに到達します（などの呼び出しを含む `showmount`）。選択するデータLIFは、クライアントの名前解決設定によって異なります。ONTAPには、LIFアドレスをDNSサーバに自動的に登録できるDDNSクライアントがあります。詳細については、本ドキュメントの「DDNS」セクションを参照してください。ONTAPに搭載されたDNSロードバランサを使用すると、使用頻度の低いLIFとノードの組み合わせにクライアントを転送できます。ONTAPでのDNSロードバランシングの詳細については、TR-4073、TR-4182または TR-4523を参照してください。

NAS要求を受信すると、データLIFはNASレイヤを通過して処理と処理を行います。

NASレイヤ

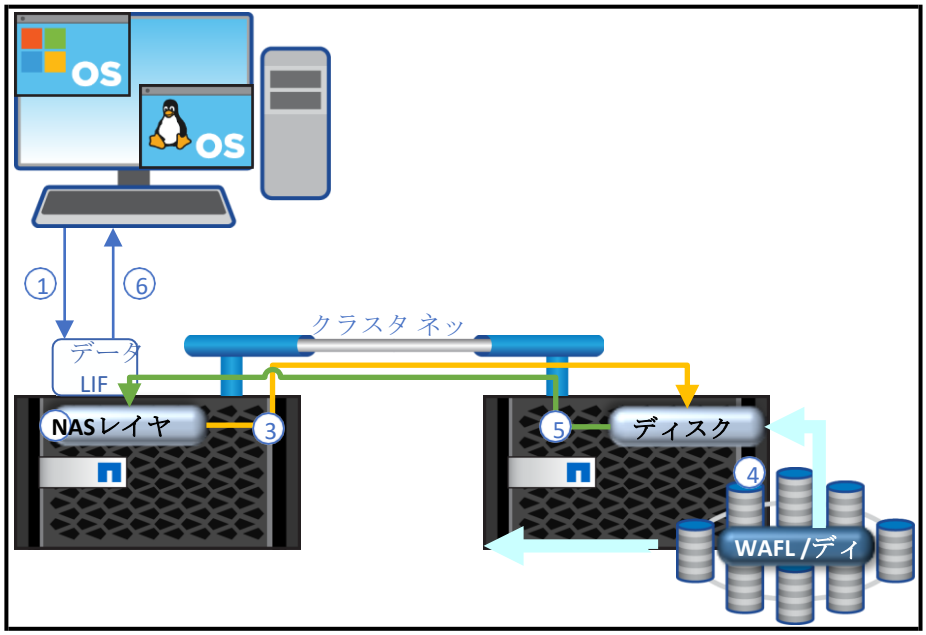
NAS要求が物理インターフェイスに到達すると、その要求はNASレイヤに転送されて処理されます。NASレイヤは、要求がクラスタ内の適切なパスを通過するように、セキュリティデーモン（SecD）やボリュームロケーションデータベース（VLDB）などのクラスタプロセスにRPC呼び出しを送信して、ユーザクレデンシャル、データローカリティ、およびその他のNAS構成要素を決定します。要求されているデータが、クライアントから要求を受信したデータLIFを現在ホストしているノードに対してローカルである場合、要求はONTAPダイレクトI/Oパスメカニズムを使用してディスクに直接送信されます。データがクラスタ内の別のノードにある場合、要求はクラスタネットワークを経由します。

図1）ONTAPのNASプロトコルパス（同じノード上のLIFとボリューム）



1. NAS要求がクライアントからSVMデータLIFに送信されます。
2. NASレイヤは、すべてのNAS要求を受信して処理します。認証が必要な場合は、認証を実行するためにRPC呼び出しがSecDに送信されます。
3. ローカルの場合、ディスク要求はディスクに直接送信されます。
4. 応答はスタックを通過してNASクライアントに返されます。

図2）ONTAPのNASプロトコルパス（LIFとボリュームが異なるノードにある場合）



1. NAS要求がクライアントからSVMデータLIFに送信される
2. NASレイヤは、すべてのNAS要求を受信して処理します。認証が必要な場合は、認証を実行するためにRPC呼び出しがSecDに送信されます。
3. リモートの場合、ディスク要求はクラスタネットワーク経由でデータのローカルノードに送信されます。
4. ディスクレイヤで要求が処理され、ディスクに対する読み取り/書き込みが行われます。
5. ディスクレイヤの応答は、スタックを経由して、NASレイヤ要求を処理したノードに返されます。
6. 応答はスタックを通過してNASクライアントに返されます。

セキュリティデーモン（SecD）

SecDは、ノード単位で実行されるアプリケーションです。SecDアプリケーションは、Active Directory、DNS NIS、LDAPなどのネームサービス検索のほか、クレデンシャルクエリとネームマッピングを処理します。SecDはノード固有です。つまり、クラスタ内の各ノードにSecDプロセスが存在します。NAS要求がデータLIFに到達すると、そのデータLIFをホストしているノードが、ユーザやホストの認証に使用されるSecDアプリケーションもホストします。

SecDは、NAS要求を受信したノード上の外部ネームサービスと通信するため、ネームサービスサーバにルーティング可能なLIFがSVM内に少なくとも1つ必要です。SecDは、NAS要求を処理するノードからネームサービスサーバにアクセスできない場合、必要に応じてネームサービス要求をリモートノードにインテリジェントに転送できます。

管理ゲートウェイデーモン（mgwd）

ONTAPオペレーティングシステムの管理ゲートウェイは、まさにそのようなものです。クラスタを管理するためのゲートウェイです。クラスタの健全性/クォーラムの維持とレポート、管理ソフトウェア（NetApp OnCommand®System Managerなど）からのSSHログイン、SNMP、およびNetApp Manageability SDK呼び出しの受信、エクスポートルールの処理、およびエクスポートキャッシュの保守を担当します。さらに、RPCを介して他のすべてのクラスタアプリケーションと通信し、設定の読み取り/書き込み要求を送受信します。LIF

ベストプラクティス1）SecD LIFとデータLIF

データの局所性を有効にするために、ネームサービスへの適切なルーティングが行われるSVMの各ノードにデータLIFを配置することを推奨します。これが不可能な場合でも、NAS環境のネームサービスにルーティングできるデータLIFがSVMごとに少なくとも1つ必要です。

3 ネーム サービス

ネームサービスは、ユーザ、グループ、ネットグループを含む外部サーバです。エンタープライズ環境でホスト情報を提供します。この定義には、NIS、LDAP、DNSのほか、ローカルファイルとMicrosoft Windows Active Directoryが含まれます。

3.1 ネームサービスを使用するメリット

数千のユーザとホストを持つ大規模な環境では、個々のマシンでユーザ、グループ、ネットグループ、およびホスト解決用の個別のフラットファイルを管理することは事実上不可能です。ネームサービスサーバを使用すると、管理者はビジネスクリティカルなオブジェクトの最新情報のデータベースを保持できます。このデータベースとクライアントマシンとストレージデバイスは、エンタープライズ環境全体でこれらのオブジェクトの整合性を確保するために相互に通信できます。すべてのクライアントとストレージが同じデータベースで同じサーバにアクセスしている場合、クレデンシャルの取得やホスト名解決に間違いはありません。

ネームサービスサーバを使用するその他の利点は次のとおりです。

- ユーザ、グループ、ネットグループ、およびホスト名の統合
- ネームサービスサーバデータベースのサイトレプリケーションによるディザスタリカバリ
- サイトレプリケーションを使用してサーバデータベースのローカライズされたコピーを作成することにより、WANレイテンシを低減
- ロードバランシングとフェイルオーバー機能

3.2 ONTAPオペレーティングシステムのネームサービス

ONTAPバージョン9.3以降では、ネームサービス機能の設定がという独自のコマンドセットに移行されました `vserver services name-service`。これにより、SVMとクラスタに関連付けられているすべてのネームサービスを1つのエントリで設定できます。

```
cluster::> vserver services name-service>
    dns         ldap        netgroup    nis-domain ns-switch unix-group     unix-user
```

その他のネームサービス診断コマンド（など）getXXbyYYは **advanced** 権限レベルで用意されています。これらのコマンドは、設定の整合性の確認や問題のトラブルシューティングに役立ちます。このコマンドセットの詳細については、このドキュメントの該当箇所を参照してください。

```
cluster::> vserver services name-service> set 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

cluster::vserver services name-service*>
    dns         getxxbyyy ldap        netgroup    nis-domain ns-switch
    unix-group unix-user
```

ns-switchとは何ですか。

ns-switchは、ネームサービス スイッチです。これは、SVMがユーザ/グループ、ホスト、ネームマップ、ネットグループの検索に使用するネームサービスソースの順序と、使用するネームサービスソースを制御します。

現在のns-switch設定を表示するには：

```
cluster:> vserver services name-service*> ns-switch show -vserver svm1
                                                 Source
Vserver          Database       Enabled          Order
---------------------------------- ------------ ---------- ------------------------
svm1             hosts          true             files,dns
svm1             group          true             files,ldap
svm1             passwd         true             files,ldap
svm1             netgroup       true             files
svm1             namemap        true             files
```

上記の例では、ONTAPで詳細な制御 `passwd, group, netgroup`などがサポートされているため、ns-switch機能は標準のUNIX `nsswitch.conf` ファイルと同等になります。

nmスイッチとは何ですか。

nm-switchは *ネームマッピング* スイッチです。このパラメータは、SVMがUNIXユーザとWindowsユーザ（およびその逆）のマッピングに使用するネームマッピングソースを制御します。このような唯一の環境マルチプロトコル環境。ネームマッピングルールは、クラスタ内のローカルテーブルまたはLDAPサーバに配置できます。

現在のnmスイッチ設定を変更するには、次の手順を実行します。

```
cluster::> name-service ns-switch modify -vserver svm1 -database namemap -sources
    files ldap
```

ns-switchおよびnm-switchの処理順序

ns-switchおよびnm-switchに複数のソースを指定する場合は、検索が成功または失敗した場合の動作を考慮することが重要です。

ns-switchまたはnm-switchで複数のネームサービスソースを使用している場合は、次のようになります。

- 照会されたオブジェクトが最初のソースに存在し、応答が成功すると、処理は終了します。次のネームサービスソースは、オブジェクトが両方の場所に存在する場合でも試行されません。
- オブジェクトがどのネームサービスソースにも存在しない場合、処理は失敗します。

そのため、ネームサービスソースを優先度順にリストすることが重要です。

ONTAPはどのような場合にネームマップを使用しますか。

ONTAPは必ずしもnamemap（usermap）とは限りません。UNIXセキュリティ形式のボリュームまたはqtreeにアクセスするNFSクライアントがある場合は、使用されるクレデンシャルが渡されます。このシナリオでは、namemapプロセスはトリガーされません。ボリュームまたはqtreeのセキュリティ形式がntfsの場合、ONTAPは常にユーザマップを作成します。これは、そのルーツであるONTAPがUNIXベースのOSであるためです。デフォルトでは、すべてのユーザがローカルのONTAP UNIXユーザpcuserにマッピングされます。SMBのみの環境では、このデフォルトのマップで十分です。また、プロトコルがボリュームまたはqtreeのセキュリティ形式と一致しない場合も、ONTAPは常にユーザマップを作成します。詳細なマトリックスについては、表2を参照してください。

ONTAPでのネームマッピングの処理の順序

ユーザがNASマウントまたは共有に対して認証を試みると、ONTAPは特定の順序でネームマッピングメカニズムを使用して有効なユーザまたはネームマップエントリを検索します。これは、最終的には、のnamemap値に指定されたネームサービスデータベース値に依存し `vserver services name-service ns-switch` ます。次の例では、ONTAPは最初にローカルファイルを試行し、次にLDAPを試行します。ネームマップ値の「ローカルファイル」とは、のSVMのネームマッピングテーブル内のエントリを意味します `vserver name-mapping`。

```
cluster::> vserver services name-service ns-switch show -vserver svm1 -database namemap

                      Vserver: svm1
Name Service Switch Database: namemap
   Name Service Source Order: files, ldap
```

LDAPをネームマッピングに使用する場合、ONTAPはLDAPクライアントスキーマで使用するように設定されているすべての属性を使用します。つまり、NTFSボリュームまたはqtreeにアクセスするNFSクライアントの場合、この `windows- account-attribute` フィールドはNFSユーザを検索し、Windowsクレデンシャルの生成に使用されます。UNIXボリュームまたはqtreeにアクセスするSMBクライアントの場合、`windows-to-unix-attribute` フィールドはActive Directoryで検索されます。

ベストプラクティス2）ネームマップでの外部サービスの指定

ネームマップデータベースに外部サービスが実際に非対称ネームマッピングに使用されている場合にのみ、外部サービスを指定してください。ネームマッピングエントリがないディレクトリサーバを指定すると、要求のレイテンシが増加し、認証に時間がかかり、失敗する場合もあります。

ユーザのネームサービスエントリに明示的なネームマッピングが見つからない場合、ONTAPはユーザ名に基づいて暗黙的にマッピングを試みます。プロトコルのauthenticanプロセスで渡された特定のユーザ名は、他のプロトコルのディレクトリで検索されます。これは、NFS経由で渡されたユーザー名がActive Directoryで検索されることを意味します。同じユーザ名が見つかった場合は、それらのWindowsクレデンシャルがNFSユーザのクレデンシャルに関連付けられます。SMB経由で渡されたユーザ名は、SVMのns-switchソースから検索されます。同じユーザ名が見つかった場合、それらのUNIXクレデンシャルがSMBユーザのクレデンシャルに関連付けられます。ONTAPがユーザ名の暗黙的なマッピングを見つけられない場合は、NFSサーバまたはCIFS / SMBサーバに設定されているデフォルト値がフォールバックされます。この値の使用方法は、アクセスを試みたプロトコル、ボリュームのセキュリティ形式、および要求したネームマッピング方向によって異なります。次の表に相違点を示します。

ベストプラクティス3）ローカルファイルの指定

外部ネームサービスを使用できないときにrootユーザまたはその他のUNIXユーザが解決できない状況を回避するには、最初のネームサービスデータベースオプションとして「files」を指定します。

表2）マルチプロトコルNASアクセスのネームマッピング/デフォルトユーザに関する考慮事項

アクセスプロトコル	ボリューム/ qtreeのセキュリティ形式	ネームマッピングの方向	デフォルトユーザ
NFS	UNIX	該当なし（v3：UID検索のみ）（v4：ユーザ名検索）	N/A
NFS	NTFS	UNIX -> Windows	デフォルトのWindowsユーザ（NFSサーバオプションdefault-win-user）
CIFS / SMB	UNIX	Windows -> UNIX	デフォルトのUNIXユーザ（CIFSサーバオプションdefault-unix-user、デフォルトはpcuser）
CIFS / SMB	NTFS	Windows -> UNIX（初期認証） 最初のエントリ後に使用されるNTFS ACL。	デフォルトのUNIXユーザ（CIFSサーバオプションdefault-unix-user、デフォルトはpcuser）

4 新機能

ONTAPの最近のバージョンでは、ネームサービスに新しい機能が追加されています。以下はその一部です。

- DNSとNISの統計
- `getXXbyYY` サポートする
- NISトラブルシューティング ツール（バインドされたサーバのトレースと表示）の強化
- ネーム サービスのキュー ステータス
- ネーム サービス設定のミラーリングと修復
- ネームサービスのキャッシュと管理（ONTAP 9.3）
  詳細については、本ドキュメントの「ONTAPでのキャッシュ」セクションを参照してください。
- ネームサービスの接続チェック（LDAPおよびDNS）

5 サポートされるNS-スイッチ構成

表3 に、ONTAPオペレーティングシステムでサポートされるネームサービススイッチデータベースのリストを示します。

表3）ONTAPでサポートされるネームサービスソース

NS-スイッチデータベース	サポートされるネームサービスソース
ホスト	DNS、ローカルファイル
passwd（ユーザ）	NIS、LDAP、ローカルファイル
グループ	NIS、LDAP、ローカルファイル
Netgroup	NIS、LDAP、ローカルファイル
Namemap	LDAP、ローカルファイル

5.1 ホスト

ONTAPオペレーティングシステムでは、SVMのDNSファイルとローカルファイルの両方でホスト名検索（エクスポートポリシールールでの使用など）を使用できます。

注： LDAPおよびNISを使用したホスト名解決は現在サポートされていません。

DNSサーバ設定の確認

バージョン9.2以降のONTAPでは、個 々 のSVMのDNS設定をチェックする方法が提供されています。このチェックは、DNS設定の再構成時またはオンデマンドで呼び出されます。DNSサーバの再設定時に、DNSサーバが応答しないことが検出された場合、新しい設定は破棄されます。この動作は、修飾子を使用してスキップでき `-skip-config- validation`ます。DNSチェッカーを呼び出すと、「example」という名前に特定のSVMのドメイン名を加えたDNSクエリが送信されます。SVMのドメイン名が「example.com」の場合はONTAP、SVMに設定されている各DNSサーバで「example.example.com」が照会されます。ONTAPはまた、応答の応答時間を推測し、結果を表示します。

例：

```
cluster::> vserver services name-service dns check -vserver svm1
                                  Name Server
Vserver        Name Server      Status        Status Details
-------------- ---------------- ------------- ----------------------------------------------
svm1           203.0.113.44     down          Operation timed out.
svm1           203.0.113.93     up            Response time (msec): 2
svm1           198.51.100.200   up            Response time (msec): 2
3 entries were displayed.
```

アップグレードに関する考慮事項

クラスタを8.2.x以前からアップグレードする場合、ONTAPはクラスタSVMを使用してDNS検索をフォールバックできなくなります。まず、アップグレードの前に、データSVMのDNSが適切に設定されていることを確認します。ホスト名解決のためにONTAPがクラスタのDNSサーバにフォールバックしなくなります。次に、データSVMでローカルホスト名が使用されている場合は、クラスタ管理SVMとデータSVMの両方にホスト名とIPアドレスが存在することを確認します。これらの手順により、システムが停止する可能性が低くなります。これらのホスト名は、ローカルファイルではなくDNSから取得するのが理想的です。

5.2 ユーザおよびグループ情報

ユーザおよびグループの情報（UID / GIDなど）は、すべてのバージョンのONTAPでファイル、NIS、またはLDAPに格納できます。Data ONTAP 8.3以降では、ユーザとグループが同じSVM内の異なるネームサービスデータベースを利用できます（グループ専用のローカルファイル、LDAP、ユーザ用のファイルなど）。

例：

```
cluster::> name-service ns-switch show -vserver svm1 -database group,passwd
  (vserver services name-service ns-switch show)
                                 Source
Vserver          Database        Order
---------------- --------------- ------------
svm1             group           files
svm1             passwd          ldap,
                                 files
2 entries were displayed.
```

NetAppでは、セキュリティと拡張性を確保するために、ユーザとグループにLDAPを使用することを推奨しています。LDAPでは、暗号化された検索を提供でき、NIS設定よりも多くのサーバでの使用がサポートされるためです。他の多くのアプリケーションがONTAP以外の認証に同じLDAPソースを使用できるため、ローカルファイルを使用するよりも推奨されます。

ローカル ユーザおよびローカル グループの制限

ローカルユーザとローカルグループが作成されると、ONTAPオペレーティングシステムを適切に実行するためのレプリケートされたデータベーステーブルのサイズとメモリ割り当てが大きくなります。テーブルの読み取り/書き込み時にこれらのデータベースがメモリ不足になると、クラスタが停止する可能性があります。そのため、ONTAPにはローカルユーザとローカルグループに対するハードリミットがあります。この最大数はクラスタ全体で、すべてのSVMに影響します。

ベストプラクティス4）ローカルUNIXユーザおよびグループ

Data ONTAP 8.2.3より前のバージョンのオペレーティングシステムでは、ローカルユーザとローカルグループにハードリミットはありませんでした。ただし、実質的な制限がないわけではありません。NetAppでは、**「エラー！参照ソースが見つかりません。**8.2.3より前のバージョンのONTAPオペレーティングシステムを使用している場合。

注： この制限は、ローカルUNIXユーザおよびグループに適用されます。ローカルCIFSユーザおよびグループ（vserver cifs users-and-groups）には個別の制限があります。

表4）ONTAPのローカルユーザとローカルグループの制限

	ローカルUNIXユーザ制限（デフォルトおよび最大）	ローカルUNIXグループの制限（デフォルトおよび最大）
拡張/ファイル専用モードを使用しないローカルファイル	32,768（デフォルト） 65、536（最大）	32,768（デフォルト） 65、536（最大）
スケール/ファイル専用モードのローカルファイル	パスワードファイルのサイズ：10MB*	グループファイルサイズ：25MB
	注： groupファイルとpasswdファイルのサイズは上書きでき `-skip-file-size-check` ますが、ファイルサイズが大きい場合はテストされていません。 ユーザ数：40万人 グループ：15k グループメンバーシップ：3000k SVM：6	

前述したように、ローカルUNIXユーザとローカルグループの最大数はクラスタ全体で、SVMが複数あるクラスタに影響します。したがって、クラスタにSVMが4つある場合は、各SVMの最大ユーザ数の合計が、クラスタの最大数に達している必要があります。追加のローカルエントリが必要で、外部ネームサービスがオプションでない場合は、拡張/ファイル専用モードのセクションを参照してください。

例：

- SVM1のローカルUNIXユーザ数は2,000
- SVM2のローカルUNIXユーザ数は40,000
- SVM3のローカルUNIXユーザ数は20
- これにより、SVM4では23、516人のローカルUNIXユーザを作成できます。

制限を超えてUNIXユーザまたはグループを作成しようとすると、エラーメッセージが表示されます。

例：

```
cluster::> unix-group create -vserver svm1 -name test -id 12345

Error: command failed: Failed to add "test" because the system limit of {limit number}
       "local unix groups and members" has been reached.
```

制限は、advanced権限レベルで次のコマンドで制御します。

```
cluster::*> unix-user max-limit
    modify show
```

UNIXユーザおよびグループの制限に関するアップグレード時の考慮事項

ハードリミットが設定されたONTAPバージョンにアップグレードする場合、既存のユーザとグループはチェックされません。そのため、クラスタですでに上限を超えている場合はアップグレードは成功しますが、新しいユーザやグループを作成することはできません。また、制限を超えている間に問題が発生すると、サポートの問題が発生する可能性があります（たとえば、サポートではお客様の構成が「サポートされていない」とみなされます）。ユーザとグループの数を制限より少なくすることを強く推奨します。この処理は、アップグレードの前後に実行できます。

5.3　ネットグループ

ネットグループは、すべてのバージョンのONTAPシステムで、ファイル、NIS、およびLDAPでの使用がサポートされています。ネットグループでは、セキュリティと拡張性のためにLDAPを使用することを推奨していますNetApp。ネットグループを使用する場合は、NetApp netgroup.byhost機能（Data ONTAP 8.2.3以降で使用可能）を活用して検索を高速化し、パフォーマンスを向上させることを強く推奨します。LDAPでのネットグループおよびnetgroup.byhostマップの設定については、TR-4073：『Secure Unified Authentication』を参照してください。

LDAPネットグループ

NISではなくLDAPでネットグループ機能を活用することも可能です。ネットグループを使用すると、ストレージ管理者はグループを使用して一連のホストへのアクセスを制御できます。ホストごとに多数の異なるルールを作成する必要はありません。LDAPをNISサーバとして使用する方法については、RFC-2307を参照してください。

LDAPのNISオブジェクトとNIS属性について

LDAPのNISオブジェクトタイプは、objectClass属性によって決まります。オブジェクトに設定されたobjectClass属性は、ONTAPおよびその他のLDAPクライアントがネットグループ関連オブジェクトをLDAPに照会する方法を決定します。ネットグループの場合、デフォルトでnisNetgroupオブジェクトクラスが使用されます。

表5）LDAPにおけるNISオブジェクトのオブジェクトクラスと属性

オブジェクトクラス	使用目的	使用されるNIS属性
ニスマップ	NISマップの抽象化	nisMapName
nisObject	ホスト単位のネットグループエントリ	nisMapName
		nisMapEntry
nisNetgroup	ネットグループメンバー ネストされたネットグループメンバー	nisNetgroupTriple
		memberNisNetgroup

NISオブジェクトの用語

次のセクションでは'NISオブジェクトの特定の側面を定義する用語について説明します

期間	定義
NISマップ	NISマップは、LinuxおよびUNIXクライアントの/etcディレクトリにある一般的なファイルを一元管理および置換するように設計されています。 ONTAPで現在サポートされているNISマップタイプは次のとおりです。 passwd.bynameおよびpasswd.byuid group.bynameおよびgroup.bygid netgroup netgroup.byhost（8.2.3以降） NISでのホスト名解決は現在サポートされていません。NISマップの詳細については、http://docs.oracle.com/cd/E19683-01/817-4843/anis1-24268/index.htmlを参照してください。
Netgroup	ネットグループは、権限およびエクスポートアクセスのチェックに使用される（ホスト、ユーザ、ドメイン）トリプル（タプル）のセットです。ONTAPは現在、ネットグループエントリ内のホストのみをサポートしています。 ネットグループの詳細については、『http://linux.die.net/man/5/netgroup and http://www.freebsd.org/cgi/man.cgi?query=netgroup&sektion=5』を参照してください。
三重	ネットグループのトリプル（タプル）は、ネットグループファイル内の一連のエントリを表し、ホスト、ユーザ、ドメインを構成します。ONTAPで使用される有効なトリプルは、（host、、、）で構成されます。ネットグループのトリプルで使用されるホスト名は、ONTAPでのDNS解決が必要です。ネットグループ変換のベストプラクティスについては、TR-4067のネームサービスのベストプラクティスを参照してください。
netgroup.byhost	netgroup.byhostエントリは、ネットグループ全体を照会するのではなく、ホスト単位でネームサービスにグループメンバーシップを照会することで、ネットグループ検索を高速化するために使用されます。エントリが多いネットグループの場合は、検索時間が大幅に短縮され、パフォーマンスが向上します。

ONTAPオペレーティングシステムとActive Directory LDAP for Netgroupsとの相互作用

ONTAPオペレーティングシステムで提供されるLDAPクライアントスキーマ（AD-IDMU、RFC-2307など）では、次の属性によってネットグループとそのメンバーの検索が制御されます。

```
-nis-netgroup-object-class
-nis-netgroup-triple-attribute
-member-nis-netgroup-attribute
-cn-netgroup-attribute
```

ONTAP 8.2.3以降のバージョンでは、netgroup.byhostのサポートに次の属性が追加されています。

```
-nis-object-class
-nis-mapname-attribute
-nis-mapentry-attribute
```

デフォルトスキーマが新しいスキーマにコピーされている場合にのみ、LDAPクライアントスキーマを変更してデフォルト属性を変更できます。ONTAPのデフォルトスキーマは読み取り専用です。デフォルトスキーマの詳細については、このドキュメントのLDAPスキーマに関するセクションを参照してください。

Active DirectoryにWindows Server for NISをインストールすると、コンテナが `DefaultMigrationContainer30` 作成されます。このコンテナは、NISネットグループの移行先となるデフォルトのコンテナです。別のコンテナを使用するには、この情報をホストする新しいOUまたはコンテナを作成し、移行時に指定します。

Active Directoryスキーマには、Windows 2008以降でデフォルトで追加された次のスキーマ属性があります（ONTAPで使用されるデフォルト属性は太字で示されています）。

```
memberNisNetgroup
msSFU-30-Netgroup-Host-At-Domain
msSFU-30-Netgroup-User-At-Domain
msSFU-30-Nis-Domain
msSFU-30-Nis-Map-Config
msSFU-30-Yp-Servers
NisMap
NisMapEntry
NisMapName
NisNetgroup
NisNetgroupTriple
NisObject
```

ADベースLDAPでのネットグループの作成

Active Directoryネットグループは、ユーティリティ nis2adおよび nismapを使用するか、ADSI Editなどのツールを使用して制御できます。

nis2adを使用すると、既存のマップをNISからADに移行したり、ローカルファイルからNISマップを作成したりできます。このユーティリティは、Windows 2008以降のUNIXのID管理機能に含まれています。ただし、IdMUによって作成されたデフォルトの「ネットグループ」NISマップ以外で新しいNISマップを作成する場合を除き、通常は必要ありません。

nismapコマンドを使用すると、nis2adの機能に加えて、NISマップをきめ細かく管理できます。

NIS用のサーバとともにUNIX用のID管理をインストールすると、NIS用のサーバを表示および管理するためのWindows MMCが作成されます。ただし、NIS MMC用のサーバを使用してNISマップを作成または削除することはできません。例については、TR-4073：『Secure Unified Authentication』を参照してください。

注: MicrosoftはIdMUを廃止しましたが、ONTAPでのLDAPクライアントの設定に必要なRFC2307bisスキーマ拡張機能はActive Directoryに残ります。特定のバージョンのWindows ADでRFC2307属性を管理する方法については、Microsoftのドキュメントを参照してください。

サードパーティスキーマ拡張

Active Directoryは、Microsoft Windowsのディレクトリサービスで使用するLDAPバックエンドを提供します。また、Active DirectoryをUNIX ID管理サーバとして機能させるための追加のスキーマ拡張も提供します。UNIX用のサービス（Windows 2003以前）やUNIX用のID管理（Windows 2003R2以降）など、LDAPクライアントがUNIX属性をバインドおよび検索できるようにする無料のスキーマ拡張機能が用意されています。ONTAPでは、設定を簡単にするために、AD-SFU、AD-IDMU、およびRFC-2307スキーマタイプ用のデフォルトの読み取り専用スキーマが提供されています。

Microsoft Active Directoryの統合ツールに加えて、CentrifyのVintelaアプリケーションスイートなどのサードパーティツールがあり、スキーマを拡張し、管理用のGUIを提供します。ONTAPは、RFC-2307標準に準拠したすべてのスキーマ拡張をサポートしています。ONTAPでサードパーティのスキーマ拡張を使用するには、スキーマ属性が利用されているベンダーの製品ドキュメントを参照し、それに応じてONTAPでクライアントスキーマを変更します。TR-4073：『Secure Unified Authentication』では、サードパーティベンダーで使用するカスタムLDAPスキーマの作成方法について説明しています。スキーマを提供するユーザに関係なく、LDAPサーバについても同じ一般的なベストプラクティスが適用されます。

LDAPネットグループの最適化

LDAPサーバを最適化すると、ONTAPオペレーティングシステムを実行しているストレージシステムからの検索を高速化できます。次に、使用可能な一般的なベストプラクティスを示します。これらのベストプラクティスを実装するための具体的なベストプラクティスや手順については、LDAPベンダーにお問い合わせください。

ベストプラクティス5）LDAPの最適化

- 高速WANまたはLAN接続を備えたLDAPサーバを使用します。
- LDAPサーバの負荷を分散して、CPU、メモリ、ネットワーク負荷を軽減します。
- LDAPサーバのDNSにサービスレコード（SRV）があることを確認します。Microsoft Active Directoryは、ドメインコントローラでもあるすべてのLDAPサーバに対して、デフォルトでこれを実行します。
- LDAPサーバデータベースが非常に大きい場合は、ベース、ユーザ、グループ、およびネットグループDN設定でDNフィルタリングを使用します。大規模は主観的な用語であり、ネットワーク、LDAPサーバのサイズ、LDAPサーバの負荷、オブジェクトの数などの要因によって異なることに注意してください。
- フォルダ構造の下位レベルでLDAPを検索すると、クエリが高速化されます。
- 可能であれば、未使用のユーザやグループなどを削除して、オブジェクトの数を減らしてみてください。
- LDAPでUNIXオブジェクトを照会するためにActive Directoryフォレスト内の複数のドメインを使用しようとする場合は、グローバルカタログLDAP検索が必要です。LDAPリファーラルは現在ONTAPでサポートされていません。
- すべてのLDAPサーバに、各オブジェクトのスキーマ属性に正確で完全な情報が含まれていることを確認します。たとえば、すべてのユーザにGID番号を割り当てる必要があります。
- すべてのLDAPサーバに整合性のあるスキーマのコピーがあることを確認します。Active Directoryでは、デフォルトで15分間隔のレプリケーションが実行されます。
- サーバのCPUやメモリ使用量などを監視して、サーバが過剰に動作しないようにします。
- 問題を解決するために、低速なLDAPサーバや動作に問題があるLDAPサーバをできるだけ早くクライアント設定から削除してください。
- メンテナンス中のLDAPサーバは、必ず設定から削除してください。

注： LDAPリファーラル、グローバルカタログ検索、およびその他のLDAP設定の詳細については、TR-4073：『Secure Unified Authentication』を参照してください。

ローカルファイル

このセクションでは、ネームサービスとして使用するローカルファイルについて説明します。ONTAPオペレーティングシステムでは、ローカルファイルはレプリケートされたデータベース（`unix-users``unix-groups`など）内のエントリで、Data ONTAP 7-Modeなどの他のオペレーティングシステムに見られるフラットファイルを置き換えます（など） `/etc/passwd`。`/etc/group`これにより、クラスタはすべてのメンバーノードに関する最新の情報を保持できます。

線の長さの制限

ONTAPオペレーティングシステムのネットグループファイルには、行の長さとネストされたネットグループの数に制限があります。この情報は、ネットグループのベストプラクティスの制限に関するセクションで説明されています。

入力ミスの処理

`-load-from-uri` ONTAPオペレーティングシステムの機能を使用してネットグループをローカルのクラスタにインポートする場合は、ファイルにタイプミスがないように細心の注意を払ってアクセスの問題を回避する必要があります。Data ONTAP 8.2.3以降では、アップロードの前にファイルがチェックされ、誤字脱字の可能性があることを警告します。ネットグループファイルに入力ミスがあると、原因アクセスの問題（アクセスを許可する必要があるクライアントへのアクセスを拒否するなど）が発生する可能性があります。これは、ローカルおよびリモートのネットグループホストの解決に影響する可能性があります。

URIからのネットグループのロード

ネットグループをURIからクラスタ上のローカルファイルにロードする際、ネットグループキャッシュは自

動的にフラッシュされません。そのため、あるホスト名またはIPがキャッシュ内にすでに存在していて（正または負の）ネットグループファイルがその特定のホスト名またはIPを反映するように変更された場合、 キャッシュが手動でフラッシュされるか、エントリのTTLが期限切れになるまで、変更は有効になりません。グローバルキャッシュでは、ノードの起動時やLIFの移行時に外部ネットグループソースを照会する必要性は制限されますが、手動でキャッシュをフラッシュすると再取り込みが必要になるため、しばらく時間がかかるか、大量の要求がリソースを使い果たしてアクセスできなくなる可能性があります。したがって、このような変更はメンテナンス時間内に行うことをお勧めします。ネットグループ情報を格納するキャッシュの詳細については、このドキュメントの「キャッシュ調整可能」のセクションを参照してください。URIからのファイルのロードにはファイルサイズの制限があることに注意してください。

ローカルファイル同期の問題

まれに、ローカルファイルのエントリがクラスタのRDB内のエントリと同期していないことがあります。たとえば、ネットグループファイルが最近ロードされたときにエントリのロード中に何らかの問題が発生した場合、クラスタ内のネットグループがロードされたローカルファイルの内容を正しく表していない可能性があります。

ファイルがロードされるたびに、ファイルバージョンが割り当てられます。RDBが更新されるたびに、ファイルと同じバージョン番号が割り当てられます。バージョンが同期されているかどうかを確認するには、diag権限で次のコマンドを使用します。

```
cluster::*> name-service file-version ?
  (vserver services name-service file-version show)
  show                        *Display the DB and file version
```

ファイルバージョンの不一致を修正するには、diag権限で次のコマンドを使用します。

```
cluster::*> name-service repair-configs ?
  (vserver services name-service repair-configs)
-node <nodename>                                                    *Node
-vserver <vserver name>                                             *Vserver (default: svm1)
-configuration {ns-switch|hosts|unix-user|unix-group|dns|netgroup|nis-domain|all} *Configuration
```

netgroup.byhost

netgroup.byhostエントリを使用すると、ネットグループ全体をダウンロードするのではなく、NISおよびLDAPにホスト別のグループメンバーシップを照会することで、ネットグループエントリ検索を大幅に高速化できます。ネームサービスソース（NISサーバまたはLDAPサーバ）は、特定のホストが属するネットグループのテーブルを作成し、サーバによってメンバーシップが変更されたときに自動的に維持します。これにより、クラスタはネットグループ内のすべてのエントリにアクセスを照会する必要がなくなり、ネームサーバが効率的に単一のホストを検索できるようになります。エントリが多数あるネットグループを含む大規模な環境では、検索にかかる時間が大幅に短縮され、クエリのタイムアウトによるアクセスの問題が回避されます。netgroup.byhostのサポートがONTAP 8.2.3で追加されました。

注： netgroup.byhostは、NISサーバに対してデフォルトで有効になっています。設定の変更は必要ありません。LDAPのnetgroup.byhostでは、既存のスキーマに応じて設定の変更が必要になる場合があります。

ベストプラクティス6）netgroup.byhostに関する考慮事項

netgroup.byhostを使用する場合は、ホストに必要なアクセス結果を得るために、次の条件を満たす必要があります。

- ホスト名のDNSレコードのフォワードおよびリバース
- ネットグループファイル内のホストの三重エントリ（例：host、、、）
- ホストのnetgroup.byhostエントリのネットグループ仕様

注： NetAppでは、大規模なネットグループ（メンバー数が1、000を超える）環境でnetgroup.byhost機能を使用することを強く推奨します。

ONTAPオペレーティングシステムでのLDAPのnetgroup.byhostサポートの有効化

ONTAPオペレーティングシステムでは、netgroup.byhostのサポートはデフォルトでは有効になっていません。LDAPクライアント設定のいくつかのオプションを変更する必要があります。

```
-is-netgroup-byhost-enabled [true]
-netgroup-byhost-dn [DN with netgroup.byhost entries] (optional)
-netgroup-byhost-scope [base|onelevel|subtree]
```

DNとスコープは、netgroup.byhost機能に必要なフィルタを指定するために使用されます。詳細については、使用しているONTAPリリースのアドミニストレーションガイドを参照してください。この例については、TR-4073：『Secure Unified Authentication』を参照してください。

ネットグループの処理の仕組み

次に、ONTAPオペレーティングシステムでのネットグループ処理の概要を示します。

1. まず、マウント要求がIPアドレスから受信されます。
2. 後方検索では、SVMのDNS設定を使用してFQDNを取得します。

   注： NASを使用するすべてのホストでPTRレコードを使用することを強く推奨します。PTRレコードを使用すると、CIFSでKerberosを活用し、エクスポートポリシーとルールを適切かつ効率的に解決できます。

3. FQDN（*hostname.domainname.comなど*）が取得されると、netgroup.byhostキャッシュでエントリが検索されます。キャッシュ内に有効な期限切れでないエントリがある場合は、その結果が使用されます。
4. 次に、netgroup.bynameキャッシュが参照されます。検索対象のネットグループに期限切れでない有効なエントリがある場合は、その結果が使用されます。
5. ONTAPは、ns-switchソースを順番に参照します。ソースでnetgroup.byhostが有効になっている場合は、ソースで手順5aを実行します。有効になっていない場合は、手順5bを実行します。（ファイルではnetgroup.byhostを使用できません）。
   a. データベース（LDAPまたはNIS）は、次の順序で検索されます。結果が見つかった場合は、ネットグループのIP-to-hostnameキャッシュに格納されます。見つからない場合は、手順5bに進みます。
      i. *hostname.domainname.com**
      ii. *hostname.**（NFS設定 `netgroup-dns-domain-search` が有効で、DNSドメイン検索がDNS設定に正しく表示されている場合）
      iii. IP アドレス

      注： リバースルックアップが失敗した場合は、この手順に直接進みます。

      iv. ワイルドカード検索：*。*（最終手段）
   b. データベース（LDAP、NIS、またはファイル）の完全なネットグループメンバーシップが要求され、netgroup.bynameキャッシュに格納されます。その後、クライアントのnetgroup.byhostと同じ方法で結果が検索されます。その結果がnetgroup.byhostキャッシュにキャッシュされ、以降のアクセスが高速化されます。

6 ONTAPでのキャッシュ

6.1 グローバルネームサービスキャッシュ

ONTAP 9.3では、ネームサービスキャッシュをメモリの外に移動して永続的キャッシュに移動し、クラスタ内のすべてのノード間で非同期的にレプリケートする新しいキャッシュメカニズムが提供されています。これにより、フェイルオーバー時の信頼性と耐障害性が向上します。また、ノードメモリではなくディスクにキャッシュされるため、ネームサービスエントリの制限も高くなります。

ネームサービスキャッシュはデフォルトで有効になっています。ネームサービスキャッシュを有効にしてONTAP 9.3で従来のキャッシュコマンドを試行すると、次のようなエラーが発生します。

```
Error: show failed: As name service caching is enabled, "Netgroups" caches no longer exist. Use
the command "vserver services name-service cache netgroups members show" (advanced privilege
level) to view the corresponding name service cache entries.
```

ネームサービスキャッシュは `name-service cache` 、コマンドセットの下の一元的な場所で制御されます。これにより、キャッシュの設定から古いエントリの消去まで、キャッシュ管理が容易になります。

グローバルネームサービスキャッシュは `vserver services name- service cache`、**advanced** 権限のコマンドを使用して個々のキャッシュで無効にできますが、無効にすることは推奨されません。詳細については、このドキュメントの以降のセクションを参照してください。

ONTAPには、外部ネームサービスを使用できないときにキャッシュを使用するという別の利点もあります。キャッシュ内にエントリがある場合は、エントリのTTLが期限切れかどうかに関係なく、外部ネームサービスサーバにアクセスできないときにONTAPがそのキャッシュエントリを使用するため、SVMが提供するデータへの継続的なアクセスが提供されます。

ホストキャッシュ

ホストキャッシュには、前方検索と後方検索の2つの個別のホストキャッシュがありますが、ホストキャッシュ設定は全体として制御されます。レコードがDNSから取得されると、そのレコードのTTLがキャッシュTTLに使用されます。それ以外の場合は、ホストキャッシュ設定のデフォルトのTTL（24時間）が使用されます。負のエントリ（ホストが見つからない）のデフォルトは60秒です。DNS設定を変更しても、キャッシュの内容には影響しません。

注： `network ping` コマンドでホスト名を検索する必要がある場合、このコマンドではネームサービスのホストキャッシュは使用されません。

ユーザーおよびグループキャッシュ

ユーザキャッシュとグループキャッシュは、passwd（ユーザ）、グループメンバーシップ、およびグループメンバーシップの3つのカテゴリで構成されます。

注： クラスタRBACアクセスではキャッシュは使用されません。

パスワード（ユーザー）キャッシュ

ユーザキャッシュは、passwdとpasswd-by-uidの2つのキャッシュで構成されます。キャッシュは、homedirやshellなどの他のデータはNASアクセスとは無関係であるため、スペースを節約するために、ユーザデータの名前、uid、およびgidの側面のみをキャッシュします。エントリがpasswdキャッシュに配置されると、対応するエントリがpasswd-by-uidキャッシュに作成されます。同じように、あるエントリがあるキャッシュから削除されると、対応するエントリはもう一方のキャッシュから削除されます。ユーザ名とuidのマッピングが分離されていない環境では、この動作を無効にするオプションがあります。

グループキャッシュ

passwdキャッシュと同様に、グループキャッシュはgroupおよびgroup-by-gidという2つのキャッシュで構成されます。エントリがグループキャッシュに配置されると、対応するエントリがgroup-by-gidキャッシュに作成されます。同じように、あるエントリがあるキャッシュから削除されると、対応するエントリはもう一方のキ

ャッシュから削除されます。フルグループメンバーシップはスペースを確保するためにキャッシュされず、NASデータアクセスには必要ありません。したがって、グループ名とGIDのみがキャッシュされます。グループ名とGIDのマッピングが分離されていない環境では、この動作を無効にするオプションがあります。

グループメンバーシップキャッシュ

ONTAPには、グループメンバーシップ情報も保存されます。ファイル環境およびNIS環境では、特定のユーザが属しているグループのリストを効率的に収集する方法がありません。 したがって、これらの環境では、ONTAPはグループメンバーシップキャッシュを使用して効率化を実現しますが、LDAPはこのキャッシュを使用してグループメンバーシップの検索結果を格納します。グループメンバーシップキャッシュは単一のキャッシュで構成され、ユーザが属しているグループのリストが格納されます。NISの場合、 `nis-domain group-database` この動作を制御するためのコマンドセットが用意されています。ONTAPはNISからグループ情報を収集し、ユーザとグループのメンバーシップのマップを24時間ごとに作成します。これは、グループメンバーシップの検索時に参照されます。

ネットグループキャッシュ

ONTAP 9.3以降では、さまざまなネットグループキャッシュがnetgroup.byhostとnetgroup.bynameキャッシュの2つのキャッシュに統合されました。netgroup.byhostキャッシュは、ホストが属するネットグループに対して参照される最初のキャッシュです。次に、この情報を使用できない場合、クエリは完全なネットグループメンバーを収集し、ホストと比較することに戻ります。情報がキャッシュにない場合は、ネットグループns-switchソースに対して同じプロセスが実行されます。ネットグループ経由のアクセスを要求しているホストがネットグループメンバーシップ検索プロセスで見つかった場合、以降のアクセスを高速化するために、そのIPとネットグループのマッピングが常にnetgroup.byhostキャッシュに追加されます。また、メンバーキャッシュのTTLを低くして、ネットグループメンバーシップの変更をTTL期間内にONTAPキャッシュに反映できるようにする必要があります。動的な動的ネットグループが存在する環境では、これらの環境の最適な構成方法の詳細について、本ドキュメントのネットグループのベストプラクティスに関するセクションを参照してください。

キャッシュエントリの表示

上記のそれぞれにサービスキャッシュがあり、表示されます。これを使用して、ネームサービスサーバから想定した結果が得られたかどうかを確認できます。各キャッシュには独自のオプションがあり、キャッシュの結果をフィルタリングして探しているものを見つけることができます。キャッシュを表示するには、`name-services cache <cache> <subcache> show` コマンドを使用します。

キャッシュはSVMごとに一意であるため、キャッシュはSVM単位で表示することを推奨します。以下に、キャッシュとオプションの例を示します。

```
cluster::*> name-service cache hosts forward-lookup show ?
  (vserver services name-service cache hosts forward-lookup show)
  [ -instance | -fields <fieldname>, ... ]
  [ -vserver <vserver name> ]                                          *Vserver
  [[-host] <text>]                                                     *Hostname
  [[-protocol] {Any|ICMP|TCP|UDP}]                                     *Protocol
(default: *)
  [[-sock-type] {SOCK_ANY|SOCK_STREAM|SOCK_DGRAM|SOCK_RAW}]            *Sock Type
(default: *)
  [[-flags] {FLAG_NONE|AI_PASSIVE|AI_CANONNAME|AI_NUMERICHOST|AI_NUMERICSERV}]  *Flags (default:
*)
  [[-family] {Any|Ipv4|Ipv6}]                                          *Family (default:
*)
  [ -canonname <text> ]                                                *Canonical Name
  [ -ips <IP Address>, ... ]                                           *IP Addresses
  [ -ip-protocol {Any|ICMP|TCP|UDP}, ... ]                             *Protocol
  [ -ip-sock-type {SOCK_ANY|SOCK_STREAM|SOCK_DGRAM|SOCK_RAW}, ... ]    *Sock Type
  [ -ip-family {Any|Ipv4|Ipv6}, ... ]                                  *Family
  [ -ip-addr-length <integer>, ... ]                                   *Length
  [ -source {none|files|dns|nis|ldap|netgrp_byname} ]                  *Source of the
Entry
  [ -create-time <"MM/DD/YYYY HH:MM:SS"> ]                             *Create Time
  [ -ttl <integer> ]                                                   *DNS TTL
```

```
cluster::*> name-service cache unix-user user-by-id show
  (vserver services name-service cache unix-user user-by-id show)
Vserver    UID          Name          GID            Source Create Time
---------- ------------ ------------- -------------- ------ -------------------
svm1       0            root          1              files  1/25/2018 15:07:13
svm2
           0            root          1              files  1/24/2018 21:59:47
2 entries were displayed.
If there are no entries in a particular cache, the following message will be shown:
cluster::*> name-service cache netgroups members show
  (vserver services name-service cache netgroups members show)
This table is currently empty.
```

キャッシュエントリのクリア

次の手順は、さまざまなネームサービスキャッシュからキャッシュエントリを手動で消去する方法を示しています。この処理は、URIから新しいネットグループファイルをロードする場合やアクセス拒否の問題をトラブルシューティングする場合など、必要な場合にのみ実行してください。

グローバルネームサービスキャッシュの導入に伴い、ネットグループキャッシュのクリアが簡易化され、vserver name-service cacheコマンドセットから一元管理できるようになりました。キャッシュエントリは個別に消去することも、キャッシュ全体を消去することもできます。キャッシュをクリアすると、キャッシュにデータを再格納する必要があるため、キャッシュをクリアした場合、特に大量にクリアした場合に遅延が発生する可能性があることに注意してください。

ホストキャッシュをクリアするには

```
cluster::*> name-service cache hosts reverse-lookup ?
  (vserver services name-service cache hosts reverse-lookup)
  delete                      *Delete an entry
  delete-all                  *Delete all the entries for the vserver
```

```
cluster::*> name-service cache hosts forward-lookup ?
  (vserver services name-service cache hosts forward-lookup)
  delete                      *Delete an entry
  delete-all                  *Delete all the entries for the vserver
```

IP-to-netgroupキャッシュをクリアするには、次の手順を実行します。

```
cluster ::*> name-service cache netgroups ip-to-netgroup ?
  (vserver services name-service cache netgroups ip-to-netgroup)
  delete                      *Delete netgroup.byhost cache entry
  delete-all                  *Delete all the entries for the vserver
```

ネットグループメンバーキャッシュをクリアするには：

```
cluster::*> name-service cache netgroups members ?
  (vserver services name-service cache netgroups members)
  delete                      *Delete netgroup cache entry
  delete-all                  *Delete all the entries for the vserver
```

ユーザーキャッシュをクリアするには：

```
cluster::*> name-service cache unix-user user-by-id ?
  (vserver services name-service cache unix-user user-by-id)
  delete                      *Delete an entry
  delete-all                  *Delete all the entries for the vserver
```

```
cluster::*> name-service cache unix-user user-by-name ?
  (vserver services name-service cache unix-user user-by-name)
  delete                      *Delete an entry
  delete-all                  *Delete all the entries for the vserver
```

グループキャッシュをクリアするには：

```
cluster::*> name-service cache unix-group group-by-gid ?
  (vserver services name-service cache unix-group group-by-gid)
  delete                      *Delete an entry
  delete-all                  *Delete all the entries for the vserver
```

```
cluster::*> name-service cache unix-group group-by-name ?
  (vserver services name-service cache unix-group group-by-name)
  delete                      *Delete an entry
  delete-all                  *Delete all the entries for the vserver
```

グループメンバーシップキャッシュをクリアするには、次の手順を実行します。

```
cluster::*> name-service cache group-membership ?
  (vserver services name-service cache group-membership)
  delete                      *Delete an entry
  delete-all                  *Delete all the entries for the vserver
```

キャッシュチューニング可能

次のセクションでは、ONTAPのネームサービスキャッシュ用のTTLSおよびその他の調整可能な機能について説明します。すべてのネームサービス調整可能ファイルは、コマンドを使用して変更でき `name-service cache <hosts/unix- user/unix-group/group-membership/netgroup> settings modify`ます。ホストキャッシュの例を次に示します。

```
cluster::*> name-service cache hosts settings modify ?
  (vserver services name-service cache hosts settings modify)
    -vserver <vserver name>                                *Vserver
  [[-is-enabled] {true|false}]                             *Is Cache Enabled?
  [ -is-negative-cache-enabled {true|false} ]              *Is Negative Cache Enabled?
  [ -ttl <[<integer>h][<integer>m][<integer>s]> ]          *Time to Live
  [ -negative-ttl <[<integer>h][<integer>m][<integer>s]> ] *Negative Time to Live
```

TTLS

各キャッシュには、TTLS用の独自の調整可能なものがあります。TTLは、エントリがキャッシュに保持されてからネームサービスソースに対して再度検索されるまでの時間です。前述したように、エントリの有効期限が切れていて、ONTAPが特定のエントリについて外部ソースに接続できない場合でも、キャッシュされた値が引き続き使用され、ネットワークエラーやネームサービスサーバに関するその他の予期しない問題が原因でアクセスが突然終了しないようにします。TTLSは、コマンドを使用して個 々 のキャッシュごとに変更できます `name- service cache <hosts/unix-user/unix-group/group-membership/netgroup> settings modify`。ほとんどのキャッシュには、変更可能な同様の設定があります。各キャッシュのデフォルト値の表を次に示します。

表6）グローバルネームサービスキャッシュTTLのデフォルト

キャッシュ	デフォルトTTL	デフォルトの負のTTL
ホスト	24時間	1 カ月
UNIXユーザ	24時間	1 カ月
UNIXグループ	24時間	1 カ月

キャッシュ	デフォルトTTL	デフォルトの負のTTL
グループメンバーシップ	24時間	N/A
netgroup.byhost	24時間	1 カ月
netgroup.byname	24時間	N/A

注： グループメンバーシップキャッシュとnetgroup.bynameキャッシュの場合、負のエントリはありません。グループまたはネットグループが存在しない場合、その障害はキャッシュされません。

セッテイノヘンコウニヨルキャッシュヘノエイキョウ

設定の変更がキャッシュのフラッシュまたはリロードのタイミングに影響する理由はさまざまです。次の表は、さまざまな設定変更と、変更がキャッシュに与える影響を示しています。

構成	アクション	キャッシュへの影響
DNSホスト	DNSホストノサクセイ	作成するホスト、IP、およびエイリアスの前方検索キャッシュおよび後方検索キャッシュからネガティブキャッシュエントリを削除します。
	DNS hosts変更	IPおよび古いホスト/エイリアスの前方検索キャッシュおよび後方検索キャッシュから正のキャッシュエントリを削除します。 新しく設定したホストおよびエイリアスの前方検索キャッシュからネガティブキャッシュエントリを削除する
	DNSホストの削除	ホスト、IP、およびエイリアスの前方検索キャッシュおよび後方検索キャッシュから正のキャッシュエントリを削除します。
UNIXユーザ	unix-user create	作成される新しいユーザ名とuidのby-nameおよびby-idキャッシュからネガティブキャッシュエントリを削除します。
	unix-user modify （変更できるのはuidのみです）	作成される新しいuidのby-idキャッシュから負のキャッシュエントリを削除します。 usernameおよびold uidのby-nameおよびby-idキャッシュから正のキャッシュエントリを削除します。
	UNIXユーザの削除	作成される新しいユーザ名およびuidのby-nameおよびby-idキャッシュから正のキャッシュエントリを削除します。

構成	アクション	キャッシュへの影響
	load-from-uri（通常モード）	新しいユーザが追加されます。「unix-user create」の動作に従います。 既存のユーザに対して変更されたUIDを取得しています。「unix-user modify」の動作に従います。 ユーザ名が変更されている既存のuidに従った「unix-user delete」動作のユーザ名が変更されています。新しいユーザ名の「unix-user create」動作に従います。
	load-from-uri（ファイル専用モード）	既存の見積もりへの影響はありません。この場合、キャッシュは変更されません。
UNIXグループ	unix-group create	作成される新しいgroupnameおよびgidのby-nameおよびby-idキャッシュからネガティブキャッシュエントリを削除します。
	unix-group modify（変更できるのはgidのみ）	新しいgidが作成されるために、by-idキャッシュからネガティブキャッシュエントリを削除します。 groupnameおよび古いgidのby-nameおよびby-idキャッシュから正のキャッシュエントリを削除します。
	UNIXグループの削除	作成する新しいユーザ名およびユーザIDのby-nameおよびby-idキャッシュから正のキャッシュエントリを削除します。
	unix-group adduser	グループメンバーシップキャッシュからユーザのエントリを削除します。
	UNIXグループの追加ユーザ	グループメンバーシップキャッシュからすべてのユーザのエントリを削除します。
	load-from-uri（通常モード）	新しいグループが作成されます。unix-group createの動作に従います。 既存のグループのGIDを変更しています。unix-group modifyの動作に従います。 グループを削除します。unix-group deleteの動作に従います。 新しいグループに追加中のユーザ - 「unix-group adduser」の動作に従います。 グループから削除中のユーザ - 「unix-group deluser」の動作に従います。
	load-from-uri（ファイル専用モード）	既存の見積もりへの影響はありません。この場合、キャッシュは変更されません。

構成	アクション	キャッシュへの影響
ネットグループ	ネットグループの負荷	既存の見積もりへの影響はありません。この場合、キャッシュは変更されません。
NSスイッチ	ns-switch変更	既存の見積もりへの影響はありません。この場合、キャッシュは変更されません。
DNS設定	DNS変更	既存の見積もりへの影響はありません。この場合、キャッシュは変更されません。
LDAP設定	LDAPクライアント変更	既存の見積もりへの影響はありません。この場合、キャッシュは変更されません。

6.2 NASレイヤーキャッシュ

次に、ONTAPオペレーティングシステムのNASレイヤで使用されるレイヤについて説明します。NASレイヤの詳細については、このドキュメントの対応するセクションを参照してください。NASレイヤキャッシュはノードレベルで保持され、グローバルネームサービスキャッシュとは異なり、クラスタ内ではレプリケートされません。キャッシュの変更はdiag権限レベルで行われます。他のdiagコマンドと同様に、注意してください。

エクスポートポリシーキャッシュ

エクスポートキャッシュには、特定のエクスポートへのマウントアクセスを要求したクライアントが、そのボリュームまたはqtreeに適用されているエクスポートポリシーとルールに基づいてアクセスを許可されたかどうかに関する情報が格納されます。このキャッシュは `vserver export-policy access-cache config` コマンドで管理されます。次に、キャッシュの属性について説明します。

- 正のエントリのTTL：アクセスキャッシュ内の正のエントリのTTLです。クライアントアクセス時に、アクセスを許可しているアクセスキャッシュエントリのTTLが期限切れになると、そのアクセスキャッシュエントリが更新されます。更新の実行中は、アクセスキャッシュエントリの既存の情報でクライアントアクセスが評価されます。
- 負のエントリのTTL：アクセスキャッシュ内の負のエントリのTTLです。クライアントアクセス時に、アクセスを拒否しているアクセスキャッシュエントリのTTLが期限切れになると、そのアクセスキャッシュエントリが更新されます。更新の実行中は、アクセスキャッシュエントリの既存の情報でクライアントアクセスが評価されます。
- [TTL for Entries with Failure]：一致ルールの取得中にエラーが発生したアクセスキャッシュエントリのTTLです。
- ハーベストタイムアウト：Data ONTAPがアクセスキャッシュに保存されているエントリをこの期間使用しない場合、そのエントリは削除されます。

エクスポートポリシーキャッシュのフラッシュ

エクスポートポリシーキャッシュは、エクスポートポリシールールを変更することでフラッシュされます。また、ONTAPには、エクスポートポリシーを変更することなくエクスポートキャッシュを手動でフラッシュできる一連のコマンドが用意されています。これは、SVM、ノード、エクスポートポリシーごとに実行します。個々のIPをキャッシュからフラッシュすることもできます。コマンドはdiagレベルのコマンドです。

```
cluster::*> diag exports nblade access-cache flush
    -vserver <vserver name>    *Vserver
   [-node] <nodename>          *Node
   [-policy] <text>            *Export Policy Name
  [ -address <IP Address> ]    *IP Address
```

注： ネームサービスサーバが使用できない場合や通常よりもレイテンシが高い場合は、キャッシュをフラッシュしないでください。キャッシュへのデータの再取り込みが試行されると、原因クライアントが停止する可能性があります。ネームサービスの応答時間を評価する方法については、このドキュメントのネームサービス統計に関するセクションを参照してください。

クレデンシャルキャッシュ

NFSユーザがストレージシステム上のNFSエクスポートへのアクセスを要求すると、ONTAPはユーザを認証するために外部ネームサーバまたはローカルファイルからユーザクレデンシャルを取得する必要があります。次にONTAPは、取得したクレデンシャルを以降の参照用に内部のクレデンシャル キャッシュに格納します。NFSクレデンシャル キャッシュの仕組みを理解しておくと、パフォーマンスおよびアクセスに関する潜在的な問題に対処できます。これらのNASレイヤのクレデンシャルキャッシュは `diag nblade credentials`、コマンド（**diagnostic** 権限レベル）を使用してフラッシュおよび表示できます。

```
cluster::*> diag nblade credentials
    count flush show
```

NFSプロトコルの場合は、キャッシュタイムアウト値を変更できます。NetAppでは、必要な場合を除き、これらの時間を変更することを推奨これらの値の変更の必要性は、サポートケースによって決定されます。これらのキャッシュを変更する必要がある場合は、次の方法で値を調整できます。

```
cluster::*> nfs modify -vserver svm1 -cached-?
  [ -cached-cred-positive-ttl {60000..604800000} ]  *Time To Live Value (in msecs) of a Positive
Cached Credential
  [ -cached-cred-negative-ttl {60000..604800000} ]  *Time To Live Value (in msecs) of a Negative
Cached Credential
  [ -cached-transient-err-ttl {30000..300000} ]     *Time To Live Value (in msecs) of a Cached
Entry for a Transient Error
```

必要に応じて、個 々 のユーザを次のキャッシュで表示できます。

```
cluster::*> diag nblade credentials show -node node-01 -vserver svm1 -unix-user-id 1301

Getting credential handles.
1 handles found....

Getting cred 0 for user.
          Global Virtual Server: 10
          Cred Store Uniquifier: 1
Cifs SuperUser Table Generation: 0
               Locked Ref Count: 0
                     Info Flags: 1
          Alternative Key Count: 0
        Additional Buffer Count: 0
                Creation Time: 4214881195 ms
        Time Since Last Refresh: 20539 ms
Windows Creds:
        Flags: 0
        Primary Group: S-0-0
Unix Creds:
        Flags: 0
        Domain ID: 0
        Uid: 1301
        Gid: 1201
        Additional Gids:
                Gid 0: 1201
                Gid 1: 1203
                Gid 2: 1206
```

また、キャッシュの手動フラッシュは必要な場合にのみ実行する必要があります。これは、アクセス時に原因のレイテンシが発生し、キャッシュへの再格納時にシステムが停止する可能性があるためです。クレデンシャルキャッシュは、`-auth-sys-extended-groups` オプションを使用するときにも有効です。拡張グループを有効にすると、クラスタはグループメンバーシップキャッシュを使用して、ユーザがメンバーであるグループのリストを追跡します。

NFS /ネームサービスデータベース（NSDB）キャッシュ

ONTAPには、NASレイヤキャッシュに加えて、NFSv4 IDとネームマッピングが関係する場合のNFSキャッシュの概念があります。NSDBキャッシュでは、ネームサービスサーバ（NISやLDAPなど）に接続してクレデンシャルを取得する必要が常になくなるのではなく、NFSクレデンシャルが30分間保持されます。ONTAP 8.3.1以降では 、**diagnostic** 権限コマンドを使用してNSDBキャッシュをクリアすることもできます `diag nblade nfs nsdb-cache clear`。ONTAP 9.0以降では、でキャッシュを表示でき `diag nblade nfs nsdb-cache show`ます。

```
cluster::> set diag
cluster::*> diag nsdb-cache show -node node-03 -vserver svm1 -unix-user-name nfs_user
  (diag nblade nfs nsdb-cache show)

           Node: node-03
        Vserver: svm1
  Unix user name: nfs_user
   Creation time: 2146204100
Last Access time: 2146261100
  Number of hits: 19
```

SecDキャッシュ

SecDは、ネームサービスから取得した情報をキャッシュするONTAPオペレーティングシステムのもう1つの領域です。ONTAP 9.3以降では、グローバルネームサービスキャッシュの導入に伴い、これまで使用可能だったSecDキャッシュの多くが廃止されました。残りのSecDキャッシュのほとんどは、CIFS / SMBアクセスに対応します。SecDキャッシュはdiag権限レベルで管理されます。これらのキャッシュのほとんどは24時間後に期限切れになります。

設定とクエリに使用できるキャッシュは次のとおりです。

```
cluster::*> diag secd cache show-config -cache-name ? -node node-02
  ad-to-netbios-domain
  netbios-to-ad-domain
  ems-delivery
  log-duplicate
  name-to-sid
  sid-to-name
  schannel-key
  username-to-creds
  ad-sid-to-local-membership
  nis-group-membership
  groupname-to-info
  groupid-to-name
  userid-to-name
  username-to-info
  ldap-netgroupname-to-members
  ldap-groupname-to-info-batch
  ldap-username-to-info-batch
  name-mapping-windows-to-unix
  user-realmname-to-short-name
```

注：あるノードでキャッシュが変更されるたびに、クラスタ内のすべてのノードでキャッシュを変更する必要があります。

キャッシュを変更すると、NASの動作が変わる可能性があります。キャッシュをアグレッシブにすると、キャッシュ更新のためのシステムの負荷が大きくなる可能性があります。キャッシュのアグレッシブさが低いと、ネームサービス要求の不整合が発生する可能性があります（つまり、ネットグループから削除されたホストはフラッシュされるまでキャッシュに残ります）。

SecDキャッシュを調整するには、次のコマンドを使用します。

```
cluster::> set diag
cluster::*> diag secd cache set-config -node [nodename] -cache-name [cache] -lifetime [in
seconds]
Example of modifying a cache:
cluster::*> diag secd cache set-config -node node-01 -cache-name sid-to-name -life-time 3600
```

キャッシュ設定の表示例：

```
cluster::*> diag secd cache show-config -node node-01 -cache-name sid-to-name
Current Entries: 0
    Max Entries: 2500
 Entry Lifetime: 3600
```

注： SecDキャッシュの変更は、リブート後は維持されません。

SecDキャッシュのクリア

secdキャッシュをクリアするには、diag secd cache clearコマンドを使用します。

```
cluster::*> diag secd cache clear -node node-02 -vserver svm1 -cache-name ?
  ad-to-netbios-domain
  netbios-to-ad-domain
  ems-delivery
  log-duplicate
  name-to-sid
  sid-to-name
  schannel-key
  ad-sid-to-local-membership
  nis-group-membership
  name-mapping-windows-to-unix
  user-realmname-to-short-name
```

SecD Kerberosクレデンシャルのクリア

ONTAPのKerberosクレデンシャルが古くなった場合（CIFS Kerberos認証のドメイン時間のずれが5分以内の範囲にない場合など）、1つ以上のSVMのKerberosクレデンシャルキャッシュをクリアできます。

```
cluster::*> diag secd
      *Vserver cache clear-krb-creds ?
   [-node] <nodename>          *Node
  [ -vserver <vserver> ]
```

表7）SecDキャッシュの経過時間

キャッシュ名	デフォルトの更新時間	推奨される更新時間
AD-to-netbios-domain	0	0
ad-sidからlocal-membershipへad-sidからlocal-membershipへ	86400	86400
EMSハイシン	300	300
lif-bad-route-to-target	14400	14400
ログ-複製	300	300
名前からSID	86400	86400
NetBIOSからADドメインへ	0	0
SChannelキー	0	0
SIDと名前	86400	86400

注： NetAppでは、NetAppサポートの指示がないかぎりSecDキャッシュを変更しないことを推奨しています。

7 ベストプラクティス

7.1 ネームサービス（ns-switch）とネームマッピング（nm-switch）

次のセクションでは、ONTAPオペレーティングシステムでのネームサービス（ns-switch）構成とネームマッピング（nm-switch）構成のベストプラクティスについて説明します。

ベストプラクティス7）Nmスイッチとns-switchの構成
nm-switchまたはns-switchサービスが実際に使用されていない場合は、外部ネームサービスを使用するように設定しないでください。たとえば、NISを使用してユーザ名を指定しない場合は、ns-switch passwdおよびgroupデータベースは使用しないでください。非対称ネームマッピングルールにLDAPを使用していない場合は、nm-switchにLDAPを含めたり、ns-switchにnamemapデータベースを含めたりしないでください。

7.2 ネームサーバ設定のベストプラクティス

次のセクションでは、ONTAPでネームサーバを使用する場合のベストプラクティスについて説明します。

ネームサーバとは

ネームサーバは、ネームサービスのデータベースを提供する外部サーバです。ネームサーバには次のものが含まれますが、これらに限定されません。

- DNS
- LDAP
- NIS

ネームサーバの転送情報

ネームサーバは外部サーバであるため、標準のネットワーク転送プロトコルを利用し、レイテンシや再送信など、イーサネットネットワーク上で実行されているプロトコルと同じ問題の影響を受けます。

UDPかTCPか。

一部のネームサーバでは、DNSなどのネットワーク転送にTCPとUDPの両方を利用できます。DNSはデフォルトでUDPを使用します。ただし、ONTAPオペレーティングシステムでは、DNS応答パケットが512バイトを超える場合、TCPを使用して残りの情報が取得されます。

サービス	トランスポート
NIS	管理ゲートウェイを使用するUDP（mgwd） セキュリティデーモンを使用したTCP（SecD）
LDAP	TCP
DNS	デフォルトはUDP。TCPにフォールバックします。

UDPは User Datagram Protocol（ユーザデータグラムプロトコル）の略であり、信頼性が低く制限されているため、一般的に2つのプロトコルのうちより小さいものと見なされています。TCPは Transmission Control Protocolの略で、ネットワーク接続に2つのネットワークエンティティ間でパケットが到着することを保証する方法が必要な場合に使用されます。ほとんどのネームサーバは転送にTCPを使用します。ただし、DNSサーバは、速度や完全なネットワークカンバセーション（再送信なし）の必要性など、TCPよりもいくつかの利点があるため、ホスト名検索にUDPコールを使用します。NISサーバも、TCPと同じ利点があるため、UDP呼び出しを使用します。

ネームサーバの接続情報

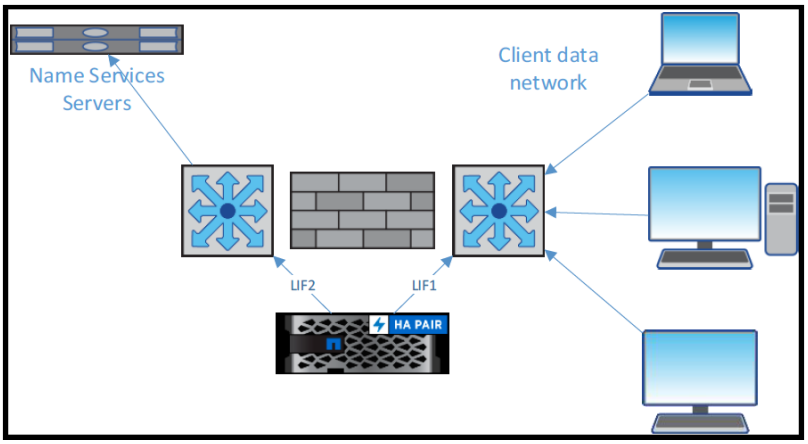
多くの場合、企業は通常のユーザデータネットワークから分離されたネットワークにネームサービスサーバを配置することがあります。この種の構成ではセキュリティが最優先ですが、ネームサービスサーバにアクセスできなくなった場合に提供されるデータの可用性に影響する可能性があります。ONTAPがネームサービス呼び出しを行う必要がある場合、ネームサービス呼び出しは、インバウンドNAS（NFSまたはSMB）パケットを受信したノードから開始されます。LIFがそのノードからネームサービスサーバにアクセスできない場合、NAS接続に失敗する可能性があります。次の例を考えてみましょう。

ネームサービスサーバは192.0.2.0/24ネットワークにあります。

通常のクライアントデータネットワークは203.0.113.0/24ネットワーク経由です。

203.0.113.0/24ネットワークが192.0.2.0/24ネットワークに到達できる内部ルートは存在しません。

ONTAPには、クライアントがアクセスできるように、LIFが203.0.113.0/24ネットワーク上にあるSVMがあります。



ONTAPがネームサービスサーバと適切に通信するためには、192.0.2.0/24ネットワーク内の同じSVM上にLIFを配置する必要があります。

上記のシナリオでは、2つのネットワークがクラスで分離されているため、ネームサービス用の特定のルートを作成する必要はありません。ネームサービスも203.0.113.0/24ネットワークに存在し、かつ特定の範囲内にのみ存在する場合は、ONTAP LIFとネームサービスサーバが別々のレイヤ2ブロードキャストドメインに存在する場合は、SVMにルートを作成する必要があります。これは、ONTAPから発信されるネームサービストラフィックが正しいインターフェイスを出力してネームサービスサーバに到達するようにするためです。

ベストプラクティス8）ネームサービスの接続

ネームサービスサーバと通信できる各ノードにLIFを配置することを推奨します。

LANとWAN

エンタープライズNAS環境では、多くの場合、世界中にサイトがあります。多くの場合、これらのサイトは小規模であり、サイトに対してローカルなネームサービスサーバなどのリソースがありません。このようなシナリオでは、ネームサービスサーバへのWANレイテンシがネームサービスの2秒（2000ミリ秒）を超えないようにすることが重要です。ネームサービスのレイテンシを表示する方法については、このドキュメントのネームサービスの統計に関するセクションを参照してください。

ベストプラクティス9）WAN経由のネームサービス

ネームサービスサーバは、NASアクセスが必要なすべてのサイトに対してローカルであるか、少なくともWAN経由のレイテンシが2秒を超えないように十分に近いサイトに配置することを推奨します。

注: WANを使用する必要がある場合は、最適な結果を得るために遅延監視を有効にしてください。

ネームサーバの一般的なベストプラクティス

次に、ネームサーバの耐障害性とパフォーマンスを最大限に高めるためのネームサーバのベストプラクティスの一般的なリストを示します。

ベストプラクティス10）ネームサービスの一般的なベストプラクティス

- 冗長性とロードバランシングのために、必ず複数のサーバを設定してください。
- すべてのネームサーバが同期されていることを確認します。
- ネームサーバを含むすべてのホストのフォワードルックアップレコードとリバースルックアップレコードが存在することを確認します。
- ネームサーバに過負荷（CPU、RAM、ネットワーク接続など）がなく、ONTAPストレージのニーズによって生成される負荷を処理できることを確認します。
- 本番ネームサーバには、可能なかぎり仮想マシンを使用しないでください。
- ネームサーバに仮想マシンを使用する場合は、それらのネームサーバに依存するNFSデータストアで仮想マシンをホストしないでください。
- 機能するネームサービスサーバおよび構成が設定されていないSVM（ns-switch、nm-switch）上のネームサービスは、絶対に指定しないでください。
- 最良の結果を得るには、ONTAP 9.3でネームサービスキャッシュを使用してください。

注： 特にNFSv4.xでは、SVMがリストに含まれるサービスを使用して存在しないUID / GIDマッピングを解決しようとするため、SVMでネームサービスの設定を誤るとハングする可能性があります。サーバが設定されておらず、外部ネームサービス（LDAPやNISなど）が指定されている場合、名前検索の要求は無期限に実行され、などのコマンド `ls` がハングしたように見えます。

ネームサービスソースとしてのLDAP

LDAPをネームサービスソースとして設定する場合は、複数のLDAP設定を作成して、特定のSVMまたはクラスタに関連付けることができます。次のコマンドで表示される設定が複数のSVMで同じである場合は、クラスタに対してLDAPクライアントを作成し、SVM間で共有する必要があります。これにより、複数のSVMにわたる単一のLDAP構成を簡単に管理できます。

```
cluster::*> ldap client modify ?
  [ -vserver <vserver name> ]                          Vserver (default: cluster)
   [-client-config] <text (size 1..32)>                Client Configuration Name
  { [[-ldap-servers] <text>, ...]                      LDAP Server List
  | [ -ad-domain <TextNoCase> ]                        Active Directory Domain
    [ -preferred-ad-servers <IP Address>, ... ]        Preferred Active Directory Servers
    [ -bind-as-cifs-server {true|false} ] }            Bind Using the Vserver's CIFS Credentials
  [ -schema <text> ]                                   Schema Template
  [ -port {1..65535} ]                                 LDAP Server Port
  [ -query-timeout {0..10} ]                           Query Timeout (sec)
  [ -min-bind-level {anonymous|simple|sasl} ]          Minimum Bind Authentication Level
  [ -bind-dn <LDAP DN> ]                               Bind DN (User)
  [ -base-dn <LDAP DN> ]                               Base DN
  [ -base-scope {base|onelevel|subtree} ]              Base Search Scope
  [ -user-dn <LDAP DN> ]                               *User DN
  [ -user-scope {base|onelevel|subtree} ]              *User Search Scope
  [ -group-dn <LDAP DN> ]                              *Group DN
  [ -group-scope {base|onelevel|subtree} ]             *Group Search Scope
  [ -netgroup-dn <LDAP DN> ]                           *Netgroup DN
  [ -netgroup-scope {base|onelevel|subtree} ]          *Netgroup Search Scope
  [ -use-start-tls {true|false} ]                      Use start-tls Over LDAP Connections
  [ -is-netgroup-byhost-enabled {true|false} ]         *Enable Netgroup-By-Host Lookup
  [ -netgroup-byhost-dn <LDAP DN> ]                    *Netgroup-By-Host DN
  [ -netgroup-byhost-scope {base|onelevel|subtree} ] *Netgroup-By-Host Scope
  [ -session-security {none|sign|seal} ]               Client Session Security
  [ -skip-config-validation [true] ]                   Skip Configuration Validation
```

ベストプラクティス11）LDAPクライアント設定

ベストプラクティスとして、クラスタSVMに対して単一のLDAPクライアント設定を作成し、管理を容易にするために複数のSVMで共有することを推奨します。

仮想マシンでホストされるネームサービスサーバ

ネームサーバ（DNSやLDAPなど）は、ESXiやHyper-Vなどの仮想環境で実行されている仮想マシンでホストされている場合があります。この設定はまったく問題ありませんが、次の点も考慮する必要があります。

- VM上のネームサーバは、ネームサーバが適切に応答できるように、常に専用のリソース（RAM、CPUなど）をオペレーティングシステムに割り当てておく必要があります。
- データストア上のネームサーバは、サービスを提供するデバイスと相互依存関係を持たないようにする必要があります。たとえば、DNSを提供するVMが、エクスポートポリシーによるクライアント解決を適切に行うためにDNSを必要とするNFSデータストアでホストされている場合、そのデータストアをDNSサーバに依存するストレージと同じストレージでホストしないでください。
- ネームサーバなどの重要なサーバを持つVMをホストするNFSデータストアの場合は、ローカルホストエントリまたはIPアドレスを使用して、エクスポートに対するDNSの依存関係を削除する専用のエクスポートポリシールールを使用することを推奨します。

ベストプラクティス12）仮想化ネームサービス

ベストプラクティスとして、ONTAPクラスタ内のSVM用に設定されたネームサービスサーバが、クラスタ内のSVMでホストされるハイパーバイザーデータストアに依存していないことを確認することを推奨します。これらのネームサービスサーバが最適なサーバである場合は、物理マシンであるか、ハイパーバイザーデータストアがこのONTAPクラスタによってホストされていないネームサーバのエントリが少なくとも1つあることを確認してください。

7.3 ホスト名解決のベストプラクティス

次のセクションでは、ONTAPオペレーティングシステムにおけるホスト名解決のベストプラクティスについて説明します。

DNSロードバランサ

環境によっては、DNSロードバランサを使用してDNSサービスの耐障害性を確保する方法が一般的です。特定のロードバランシング構成では、DNSクエリの応答を、ONTAPが照会したIPアドレスとは異なるIPアドレスから原因で応答することができます。このシナリオは、セキュリティ上の理由からONTAPによって拒否されますが、必要に応じて変更できます。この構成がご使用の環境の場合は、次のコマンドを使用して、この動作を許可するようにONTAPを変更します。

```
cluster::*> dns modify -vserver svm1 -require-source-address-match false
```

フォワードルックアップ名とリバースルックアップ名

名前解決を設定する場合は、一致するホスト名ごとに前方検索（Aレコード）と後方検索（PTRレコード）の両方を設定することが常にベストプラクティスです。エクスポートポリシーの処理では、ONTAPは前方検索を使用して、受信クライアントに対してエクスポートルールを評価します。ネットグループ処理では、ネットグループメンバーシップを決定するときにPTRレコードが評価されます。環境ではエイリアス（CNAMEレコード）が便利ですが、NASリソースへのアクセスを許可するために使用できない場合があります。CNAMEを使用する場合は、NASアクセスに使用される認証方式を検討してください。

ベストプラクティス13）ホストのフォワードレコードとリバースレコード

- DNSシステムで、すべてのホストが一致するフォワード（Aレコード）とリバース（PTRレコード）を持っていることを確認します。これを確認する方法については、本ドキュメントの付録を参照してください。
- 可能な場合は、NASリソースへのアクセスを許可するためにCNAMEを使用しないでください。

複数のDNS検索ドメイン

ONTAPオペレーティングシステムでは、ホスト名解決に複数のDNS検索ドメインを使用するようにSVMを設定できます。ただし、リスト内の名前がホストに対して有効でない場合、DNSのホスト名解決にかなりの時間がかかることがあるため、エクスポートポリシールールで原因の問題が発生する可能性があります。ホスト名を解決できない場合、ONTAPは各DNSサフィックスを使用してDNS要求を再試行し、結果がないリストを使い切るか、DNSサーバから実際の結果を取得します。

ベストプラクティス14）複数のDNS検索ドメイン

- 構成内の環境に適用可能な検索ドメインのみを使用してください。可能であれば、検索ドメインを1つだけ使用してください。
- 複数の検索ドメインが必要な場合は、最もよく使用されるDNS検索ドメインがDNS設定の最初に表示されていることを確認します。
- ホスト名解決の失敗を回避するために、すべてのDNSサーバが構成にリストされているDNSゾーンに正しく転送されることを確認します。
- 可能な場合は、ネットグループやエクスポートポリシーなどで完全修飾ドメイン名（FQDN）を使用して、クラスタが検索ドメインリストでホスト名を解決しないようにします。
- PTR /リバースルックアップレコードがDNSに存在することを確認します。これは、エクスポートポリシールールの名前解決が完全に機能するための要件です。この方法の詳細については、本ドキュメントの付録を参照してください。

DNSの既知の問題

以下は、ONTAPの既知のDNSの問題の一覧です。このリストは、原因の問題が発生する可能性があるシナリオを回避するためのものですが、包括的なものではありません。

- ONTAP 9では、新しい「不良」DNSキャッシュメカニズムが導入されています。DNSサーバ要求にタイムアウトが発生すると、DNSサーバは10分間「bad」としてマークされ、この間は使用されません。「dns modify」を使用してDNS設定を変更すると、キャッシュがフラッシュされます。 このタイムアウト値は変更できません。
- 現在のところ、ONTAPでは、ホスト名のマッピングにDNSまたはローカルファイルのみを使用できます。LDAPおよびNISはホスト名ではサポートされていません。
- SVMのローカルファイルホスト名は、Data ONTAP 8.3以降のバージョンでのみサポートされます。
- DNSレコードにフォワードルックアップとリバースルックアップの両方がない場合、エクスポートでのアクセスのルックアップが失敗する可能性があります。
- ホスト名やネットグループなどにFully Qualified Domain Name（FQDN；完全修飾ドメイン名）を使用している場合、RFC-1535ではドット（.）を追加することを推奨しています。 FQDNの末尾に「絶対ルート」FQDNを指定します。たとえば、hostname.example.comと入力します。詳細については、ルート化とルート化されていない FQDN。

ベストプラクティス15）一般的なDNSとホスト名解決

- 高速DNS検索には、DNS設定で関連するDNS検索ドメインのみを使用します。
- 単一点障害を回避するために、データベース（Active Directory DNSなど）をレプリケートするDNSサーバを複数用意します。
- ローカルまたは最速のDNSサーバが最初に表示されていることを確認します。
- NASクライアントの問題を回避するために、メンテナンス中のDNSサーバを削除します。
- すべてのDNSサーバに同じ情報が含まれていることを確認します。
- パブリックDNSサーバには、NASデータを適切に提供するために必要な情報が含まれないため、内部DNSサーバのみを指定してください。

注： IPv6はデフォルトで無効になっています。

7.4 ユーザとグループのベストプラクティス

ネーム マッピング

ネームマッピングは、SMB経由でUNIX形式のボリューム/ qtreeにアクセスする場合や、NFS経由でNTFS形式のボリューム/ qtreeにアクセスする場合に使用されます。ほとんどの環境では、Windows ADとUNIX LDAPの両方でユーザ名を1対1でマッピングできます。そのための最も簡単な方法は、同じActive Directoryドメインを使用して特定のSVMのCIFS認証として機能し、AD DCをSVMのLDAPクライアントサーバとして設定することです。RedHatのIdentity Managerなど、UNIX LDAPの実装を個別に行う必要がある場合があります。このような場合は、LDAPサーバとWindows AD環境で同じユーザに定義されているユーザ名が、ネームマッピングをイーストするために同じユーザ名を使用するようにします。これを達成できない場合は、正規表現準拠ルールをネームマッピングルールに追加できるように、一方をもう一方に変換できるパターンを使用することを推奨します。パターンを持たないカスタムのネームマッピングは、絶対に使用しないでください。 その場合は、LDAPとSVMのLDAPクライアントスキーマ属性を活用して非対称のネームマッピングを使用し、管理性と拡張性を最大限に高めます。

ベストプラクティス16）ユーザとグループのネームマッピング

マルチプロトコルアクセスで最も迅速かつ信頼性の高いネームマッピング結果を得るには、Windows環境とUNIX環境の間でユーザ名を一致させる必要があります。

条件

ONTAPオペレーティングシステムでは、システム上でローカルに許可されるユーザとグループの数に制限があります。表8 にこれらの制限を示します。

表8）ONTAPでのユーザおよびグループの制限（非スケールモード）

最大	Value
ユーザおよびグループあたりの文字数（名前の長さ）	64文字
load-from-uriのファイルサイズ（unix-user、unix-group）	UNIXユーザ：2.5MB UNIXグループ：1MB **注:** 制限を超えると、負荷は失敗します。

最大	Value
クラスタ全体のローカルUNIXユーザおよびグループとメンバー	UNIXユーザ：32、768（デフォルト） 65、536（最大） UNIXグループおよびメンバー：32、768（デフォルト） 65、536（最大）
UNIXグループの単一行（-load-from-uri）	32、768文字
ネームマッピングルール	SVMあたり1、024

スケールモード/ファイル専用モード

スケールモード/ファイル専用モード

ONTAP 9.1以降では、ローカルユーザとローカルグループの拡張モード/ファイル専用モードで **診断**レベルのネームサービスオプションを有効にし、この `load-from-uri` 機能を使用してクラスタにファイルをロードすることで、ローカルユーザとローカルグループの制限を拡張できます。 ユーザとグループの数を増やす。表9 に、これらの新しい制限の概要を示します。拡張モード/ファイル専用モードでは、ネームサービスサーバやネットワークなどに外部の依存関係が不要になるため、ネームサービス検索のパフォーマンスが向上します。ただし、ファイル管理によってストレージ管理のオーバーヘッドが増大し、人為的ミスの可能性が高まるため、このパフォーマンスにはネームサービスの管理が容易になりません。また、ローカルファイル管理はクラスタごとに行う必要があるため、複雑さがさらに増します。

ベストプラクティス17）ローカルUNIXユーザおよびグループでのファイルのみモードの使用

オプションを十分に評価し、環境に適した決定を下してください。また、64kを超えるユーザ/グループを必要とするネームサービス環境が必要な場合にのみ、ファイルのみモードを検討してください。

UNIXユーザおよびグループのファイルのみのモードの詳細については、TR-4067：『NFS Best Practice and Implementation Guide』を参照してください。

表9）ONTAPでのユーザおよびグループの制限（拡張/ファイル専用モード）

最大	Value
load-from-uriのファイルサイズ（unix-user、unix-group）	UNIXユーザ：10MB UNIXグループ： 25MB **注：** このオプションを設定すると制限を超えることができます `-skip-file-size-check`が、ファイルサイズが大きい場合はテストされていません。
クラスタ全体のローカルUNIXユーザおよびグループとメンバー	ユーザ数：40万人 グループ：15k グループメンバーシップ：3000k SVM：6

7.5 ネットグループのベストプラクティス

ルートFQDNとルート以外のFQDN

LDAP、NIS、またはローカルファイルでネットグループを設定する場合は、複数の方法でホスト名をトリプルで定義できます。短縮名、root化されていないFQDN、またはroot化されたFQDNを使用できます。RFC-1535では、名前の指定方法によってFQDNに違いがあると記載されています。RFCから：

現在のDomain Name Serverクライアントは、IPドット付きクワッドアドレスを記憶する負担を軽減するように設計されています。そのため、人間が読める名前をアドレスやその他のリソースレコードに変換します。変換プロセスの一部には、完全修飾ドメイン名（FQDN）ではないホスト名の理解と処理が含まれます。

ルート化された絶対FQDNの形式は〔name〕〔.〕です。ルート化されていないドメイン名の形式は〔name〕です

ドメイン名には多くの部分があり、通常はホスト、ドメイン、およびタイプが含まれます。例：foobar.company.comまたはfooschool.university.edu。

ONTAPでは、DNSサーバにエントリが存在しないシナリオでは、ルート化されたFQDN（末尾にドットが付いたFQDN）が効率的に処理されます。ルート化されたFQDNを使用すると、末尾のドットが削除され（DNSのみ）、クラスタはFQDNを「現状のまま」検索し、検索を1回だけ試行します。FQDNは、ルートFQDN（末尾にドット）として設定されている場合にのみ「そのまま」試行されます。エントリの末尾にドットがなく、FQDNがDNSに見つからない場合、検索ドメインはFQDNに追加され、すべての検索ドメインが試行されるか、一致するものが見つかるまで、この組み合わせ名でDNSが照会されます。

ONTAPでは、ルート化されていないFQDN（ドット付きの任意のホスト名エントリ）が最初に「現状のまま」解決しようとし、次にクラスタが検索ドメインをFQDNの末尾に追加しようとします。たとえば、ルート化されていないFQDNは次のようになります。

```
hostname.example.com
```

DNS設定の検索ドメインに「example.com」などが含まれている場合、再試行検索は次のようになります。

```
hostname.example.com.example.com
```

その後、クラスタはすべての検索ドメインを循環し、失敗したレコードに不要なレイテンシを追加します。ルート化されたFQDNを使用すると、この動作が防止されます。

ドットのないホスト名が検出されると、最初に検索ドメインをホスト名の末尾に追加して「現状のまま」解決しようとします。

SERVFAILエラーまたはDNSサーバタイムアウトが発生した場合は、次のサーバが試行されます。

注: 特定のDNSサーバーでショートネームを「そのまま」検索すると、応答は「NXDOMAIN」ではなく「SERVFAIL」になります。Windows DNSサーバは、このように応答するDNSサーバのタイプの1つです。「NXDOMAIN」は信頼できる「名前が見つかりません」回答であり、「SERVFAIL」は一時的なエラーと見なされます。ONTAPは、SVM用に設定されているすべてのDNSサーバを介してこの短縮名を「as-is」で検索します。これにより、ルックアップに不要なレイテンシが追加される可能性があります。ネットグループから定期的に解決できない短縮名は使用しないか、削除することを推奨します。

ベストプラクティス18）ネットグループホスト

ネットグループトリプルのホスト文字列には、ルート化されたFQDNを使用することを推奨します。

ネットグループとDHCP /動的DNS

一部のシナリオでは、Dynamic Host Configuration Protocol（DHCP）またはDynamic DNS（DDNS）を実行しているサーバからホスト名にIPアドレスリースが付与されます。

DHCPとは何ですか。

DHCPは、リースモデルに基づいてクライアントとサーバにIPアドレスを自動的に提供するプロトコルです。これは、管理を容易にするためと、IP番号の制限を回避するために行われます。

DDNSとは

DDNSは、クライアントがDNSサーバ上の自身の名前レコードを自動的に更新できるようにする方法です。多くの場合、ホスト名解決を自動化して管理と管理のオーバーヘッドを削減するために、DHCPと組み合わせて使用されます。場合によっては、DHCPサーバがクライアントに代わってDNSサーバの更新を実行します。

これがネットグループに影響するのはなぜですか。

ネットグループの作成時には、静的なホスト名またはIPアドレスを追加します。DHCPとDDNSの性質上、ネットグループでのIPアドレスの使用は非始動です。そのため、ホスト名を使用する必要があり、エクスポートポリシールールの検証のためにネットグループメンバーを解決する際にONTAPによってDNSルックアップが利用されます。ONTAPでは、キャッシュを多用してNASの全体的なパフォーマンスを向上させるため、ネットグループメンバーのIPアドレスがDCHP / DDNSによって変更された場合、キャッシュが更新されるまでクラスタはその新しい情報で更新されません。キャッシュTTLSについては、このドキュメントで説明しており、調整することができます。また、キャッシュは手動でフラッシュできます。

注： キャッシュを手動でフラッシュするにはキャッシュが再取り込みされる必要があります。これには時間がかかることがあります。また、大量の要求がリソースを消費してアクセスできなくなる状況が発生する可能性があります。

ONTAP 9.3におけるネットグループとDHCP / DDNSの改善点

ONTAP 9.3ではキャッシュが改善されており、動的な環境でDHCP/DDNSとネットグループを一緒に使用して、必要に応じてクライアントプールを動的にスケールアップ/ダウンできます。改善点の詳細については、このドキュメントの「キャッシュ」セクションを参照してください。このような動的なクライアントプールを考慮して環境を最適化するには、次の点を考慮してください。

- DNSサーバに登録されているホスト名エントリのTTLSが、DDNSホスト名が再利用される前に期限切れになるまで十分に小さくなっていることを確認してください。これはONTAP DNSキャッシュに反映されます。
- ネットグループTTLSが、DDNSホスト名とネットグループポリシーおよび切り替えに従って適切に設定されていることを確認してください。
- netgroup.byhostのキャッシュは、IPアドレス別です。アクセスから24時間以内に特定のIPアドレスを再利用すると、他の変更に関係なく、同じネットグループがそのIPアドレスに適用されます。このTTLは変更できます。
- netgroup.byホストキャッシュにエントリがない場合は、ネットグループメンバーキャッシュが一致するかどうかを調べます。ネットグループメンバーキャッシュのデフォルトのTTLは20分で、ソースでByHostが有効になっていない場合にのみ値が入力されます。
- ソースに対してnetgroup.byhostが有効になっている場合、そのソースに対してネットグループメンバーのクエリは使用されません。
- 各キャッシュのTTLSは、このドキュメントのキャッシュ調整可能セクションに記載されています。

ネットグループの一般的なベストプラクティス

ネットグループのベストプラクティスには2つのカテゴリがあります。1つ目は一般的なネットグループの害虫対策であり、2つ目はネットグループに外部サーバを使用する場合のベストプラクティスです。ベストプラクティスは、次の2つの表に分割されています。

ベストプラクティス19）ネットグループの一般的なベストプラクティス

- ソース間で同じネットグループ構成を使用します。
- LDAPでネットグループを使用する場合は、netgroup.byhostマッピングを活用します。
- ネットグループのトリプルの「domain」と「user」の部分は空白のままにします。NetAppでは、ホストベースのネットグループエントリ（ホスト名など）のみがサポートされます。
- ネットグループ内のホスト名にフォワードDNSエントリとリバースDNSエントリが存在することを確認します。
- ネットグループを定期的にクリーンアップして古いエントリを排除し、アクセスを高速化します。冗長性を確保するには、複数のネームサービスサーバを使用してください。

ベストプラクティス20）外部サーバのネットグループ

- 構成内のすべてのサーバに同じ情報が含まれていることを確認します。
- メンテナンス中にサーバをリストから削除します。
- 可能な場合はLDAPのnetgroup.byhostマッピングを有効にします（8.2.3以降で使用可能）。
- ネットグループ内のすべてのホストについて、フォワードおよびリバース（PTR）DNSレコードが存在することを確認します。これは、ホスト名/エクスポートポリシーの名前解決が完全に機能するために必要な要件です。この方法の詳細については、本ドキュメントの付録を参照してください。
- ファイルからネットグループをロードする場合は、キャッシュが有機的に更新されるのを待つか、キャッシュを手動でフラッシュするように準備してください。
- DHCPやDDNSを使用している場合は、ネットグループキャッシュに正確なホストIP情報を反映するために、ネットグループキャッシュを手動でフラッシュしなければならないことがあります。
- LDAPのバインドと検索を保護するには、ONTAP 9.0以降で使用できるLDAPの署名と封印の使用を検討してください。詳細については、TR-4073：『Secure Unified Authentication』を参照してください。

条件

次の表に、ONTAP 8.3以降のオペレーティングシステムのバージョンにおけるネットグループの制限を示します。

最大	Value
ネツトクルウフノネツトノセイケン	1,000
load-from-uriのファイルサイズの制限	5 MB **注:** 制限を超えると、負荷は失敗します。
単一ネットグループの最大行数（ローカルファイル）	4096
NISサーバ数	10
NISデータベースの回線制限（NISマップ）:外部NISサーバ	1024

7.6 アップグレード前のエクスポートポリシーとルールのベストプラクティスに

関する考慮事項

アップグレード前に、エクスポートポリシールールとクライアント一致を削除することを推奨します。ルールのクライアント一致に解決できないホスト名が含まれている場合、そのエクスポートポリシーを使用するボリュームへのNASアクセスが侵害される可能性が常にあります。

ベストプラクティス21）輸出ポリシーの一般的なベストプラクティス

- エクスポートポリシールールまたはネットグループでホスト名を使用する場合は、すべてのホスト名がDNSで解決されることを確認します（フォワードルックアップとリバースルックアップ）。
- 短縮名は使用しないでください。Fully Qualified Domain Name（FQDN；完全修飾ドメイン名）は解決までの時間が大幅に短縮され、エクスポートポリシールールの評価パフォーマンスが向上します。場合によっては、短縮名が他のエクスポートルールのCAN原因の停止を解決できないことがあります。
- CNAMEは使用しないでください。せいぜい、輸出の評価は遅くなります。最悪の場合、アクセスを許可する必要があるホストへのアクセスは拒否されます。
- エクスポートポリシールールは、可能であれば頻繁に変更しないでください。変更ごとにキャッシュに再度データを取り込む必要があるため、クラスタはその機能に時間とリソースを費やす必要があります。これにより、アクセス要求のレイテンシが増大する可能性があります。
- エクスポートポリシールールで大規模なネットグループまたは多数のホスト名（数千台のホスト）を使用している場合は、すべてのホストがDNSで適切に解決され、FQDNまたはIPアドレスが使用されていることを確認してください。
- ネットグループ/ホスト名で大量のチャーンが発生する（状況が頻繁に変化する）場合は、それを反映するように適切なキャッシュが設定されていることを確認してください。詳細については、このドキュメントのキャッシュ調整可能に関するセクションを参照してください。

導入前

エクスポートポリシーとルールセットをロールアウトする前に、使用されているすべてのホストとネットグループを確認して、DNSでの名前解決とネットグループ検索が適切に機能するようにしてください。

ホストおよびネットグループのエントリの確認

コマンド `vserver services name-service getXXbyYY`（**advanced** 権限）を使用すると、コマンドラインからネームサービス検索を実行して、エクスポートとファイルへの意図した権限を提供するためのクエリに対する外部サーバの想定される応答が得られることを確認できます。デフォルトでは、このコマンドセットはキャッシュを使用またはウォームアップしません。キャッシュを照会してウォームアップする場合は、`-use- cache` オプションをに変更できますが、ネットグループなどの一部のサブクエリではキャッシュのウォームアップがサポートされていません。また、 `-show-source` オプションを使用して、結果を返したソースを指定することもできます。このコマンドの例は次のとおりです。

```
cluster::*> name-service getxxbyyy gethostbyaddr 192.0.2.100 -node node-02 -vserver svm1 -show-
source true -use-cache true
  (vserver services name-service getxxbyyy gethostbyaddr)
Source used for lookup: DNS
IP address: 192.0.2.100
Host name: hostname.ntap.local
```

特定のIPアドレスがネットグループの一部であるかどうかを確認することもできます。以下を使用します。`getXXbyYY` コマンド：

```
cluster::*> name-service getxxbyyy netgrpcheck -node node-01 -vserver svm1 -netgroup netgroup1 -
clientIP 198.51.100.233 -show-source true
  (vserver services name-service getxxbyyy netgrpcheck)
Success. Client 198.51.100.233 is member of netgroup netgroup1
Searched using NETGROUP_BYNAME
Source used for lookup: LDAP
```

このコマンドの使用方法の詳細については、本書の「診断とトラブルシューティング」セクションを参照してください。

導入後

エクスポートポリシーとルールを導入したら、コマンドを使用してクライアントアクセスを確認して `export- policy check-access`ください。

エクスポートポリシールールのアクセス検証

ONTAPでは export-policy check-access、コマンドを使用して、特定のホスト、ボリューム/ qtree、およびエクスポートポリシーのアクセスをチェックできます。この関数はホスト名の解決を考慮しないため、IPアドレスのみをチェックできます。名前解決の場合は、name- services getXXbyYY このコマンドを使用する前に、コマンドセットを使用して解決が正しいことを確認します。次の出力が表示されます。

```
NAME
vserver export-policy check-access -- Given a Volume And/or a Qtree, Check to See If the Client
Is Allowed Access

AVAILABILITY
This command is available to cluster and Vserver administrators at the admin privilege level.

DESCRIPTION
The vserver export-policy check-access command checks whether a specific client is allowed access
to a specific export path. This enables you to test export policies to ensure they work as
intended and to troubleshoot client access issues.

The command takes the volume name (and optionally the qtree name) as input and computes the
export path for the volume/qtree. It evaluates the export policy rules that apply for each path
component and displays the policy name, policy owner, policy rule index and access rights for
that path component. If no export policy rule matches the specified client IP address access is
denied and the policy rule index will be set to 0. The output gives a clear view on how the
export policy rules are evaluated and helps narrow down the policy and (where applicable) the
specific rule in the policy that grants or denies access. This command is not supported on
Infinite Volumes.
```

export-policy check-accessの例：

```
cluster::*> vserver export-policy check-access -vserver svm1 -client-ip 1.2.3.4 -volume flex_vol
-authentication-method sys -protocol nfs3 -access-type read

                                          Policy    Policy       Rule
Path                              Policy  Owner     Owner Type  Index Access
--------------------------------- ------- --------- ----------- ----- ------
/                                 default vs1_root  volume          1 read
/dir1                             default vs1_root  volume          1 read
/dir1/dir2                        default vs1_root  volume          1 read
/dir1/dir2/flex1                  data    flex_vol  volume         10 read
4 entries were displayed.
```

8 ネームサービス統計

8.1 グローバルキャッシュ統計

新しいグローバルネームサービスキャッシュには、キャッシュの速度と、API単位またはDB単位でのオフボックス解決の速度に関する統計が含まれています。カウンタマネージャには次のオブジェクトがあります。

```
nscc_api
nscc_db
nscc_rpc
mcached_mdb
```

上記のオブジェクトは、主にキャッシュパフォーマンスの問題に使用されます。外部ネームサーバの問題の診断には使用しないでください。それを支援する他のカウンターがあります。

8.2 外部サービス統計

ONTAP 9では、外部サービス用のカウンタマネージャの新しい値が追加されました。これにより、外部ネームサービスサーバのパフォーマンスを監視し、ONTAPが応答時間を認識する方法を監視できます。オブジェクトは次のとおりです。

```
external_service_op
external_service_op_error
external_service_server
```

DNS統計

DNSサーバの統計情報は、external_service_opオブジェクトとexternal_service_op_errorオブジェクトにのみ保持されます。統計を利用するには、統計収集ジョブを開始する必要があります。複数のオブジェクトをキャプチャに含めるには、パイプ記号（|）を使用します。

```
cluster::*> statistics start -object external_service_op|external_service_op_error
```

収集間隔が完了したら、統計を停止します。

```
cluster::*> statistics stop
```

sample-id：sample_91613の統計収集を停止しています

統計を表示するには：

```
cluster::*> statistics show -sample-id [sample ID]
```

external_service_op用に収集された統計の出力例：

```
Object: external_service_op
Instance: svm1:DNS:Query:198.51.100.181
Start-time: 7/13/2016 11:48:41
End-time: 7/13/2016 11:49:34
Elapsed-time: 53s
Scope: svm1

    Counter                                                     Value
-------------------------------- --------------------------------------------
    instance_name                   svm1:DNS:Query:198.51.100.181
    last_modified_time                   Wed Jul 13 11:48:48 2016
    node_name                                              node-01
    num_not_found_responses                                      0
    num_request_failures                                         0
    num_requests_sent                                            1
    num_responses_received                                       1
    num_successful_responses                                     1
    num_timeouts                                                 0
    operation                                              DNS Query
    request_latency                                          1892us
    request_latency_hist                                         -
                              <20us                              0
                              <40us                              0
                              <60us                              0
                              <80us                              0
                             <100us                              0
                             <200us                              0
                             <400us                              0
                             <600us                              0
                             <800us                              0
                               <1ms                              0
                               <2ms                              0
                               <4ms                              0
                               <6ms                              0
                               <8ms                              0
                              <10ms                              0
                              <12ms                              0
                              <14ms                              0
                              <16ms                              0
                              <18ms                              0
                              <20ms                              1
                              <40ms                              0
                              <60ms                              0
                              <80ms                              0
                             <100ms                              0
                             <200ms                              0
                             <400ms                              0
                             <600ms                              0
                             <800ms                              0
                                <1s                              0
                                <2s                              0
                                <4s                              0
                                <6s                              0
                                <8s                              0
                               <10s                              0
                               <20s                              0
                               <30s                              0
                               <60s                              0
                               <90s                              0
                              <120s                              0
                              >120s                              0
    server_ip_address                              198.51.100.181
    server_name                                                  -
    service_name                                               DNS
    vserver_name                                              svm1
    vserver_uuid                              05e7ab78-2d84-11e6-a796-
                                                      00a098696ec7
```

EXTERNAL_SERVICE_OP_ERRORについて収集された統計の出力例：

```
Object: external_service_op_error
Instance: svm1:DNS:Query:NXDOMAIN:198.51.100.181
Start-time: 7/13/2016 11:48:41
End-time: 7/13/2016 11:49:34
Elapsed-time: 53s
Scope: svm1

    Counter                                                     Value
    -------------------------------------- ----------------------------------------
    count                                                           0
    error_string                                             NXDOMAIN
    instance_name              svm1:DNS:Query:NXDOMAIN:198.51.100.181
    last_modified_time                       Thu Jun 30 09:46:14 2016
    node_name                                                  node-01
    operation_name                                           DNS Query
    server_ip_address                                  198.51.100.181
    server_name                                                     -
    service_name                                                  DNS
    vserver_name                                                 svm1
    vserver_uuid                             05e7ab78-2d84-11e6-a796-
                                                             00a098696ec7
    count                                                           0
    error_string                                             NXDOMAIN
    instance_name              svm1:DNS:Query:NXDOMAIN:198.51.100.181
    last_modified_time                       Thu Jun 30 10:10:20 2016
    node_name                                                  node-02
    operation_name                                           DNS Query
    server_ip_address                                  198.51.100.181
    server_name                                                     -
    service_name                                                  DNS
    vserver_name                                                 svm1
    vserver_uuid                             05e7ab78-2d84-11e6-a796-
                                                             00a098696ec7
```

LDAP / NIS / Active Directory外部統計

LDAP、NIS、およびActive Directoryサーバの統計は、すべてのexternal_serviceオブジェクトにのみ保持されます。統計を利用するには、統計収集ジョブを開始する必要があります。複数のオブジェクトをキャプチャに含めるには、パイプ記号（|）を使用します。

統計を利用するには、統計収集ジョブを開始する必要があります。複数のオブジェクトをキャプチャに含めるには、パイプ記号（|）を使用します。

```
cluster::*> statistics start -object
external_service_server|external_service_op|external_service_op_error
```

収集間隔が完了したら、統計を停止します。

```
cluster::*> statistics stop
```

sample-id：sample_91613の統計収集を停止しています

統計を表示するには：

```
cluster::*> statistics show -sample-id [sample ID]
```

注：これらの統計の出力は広範囲に及ぶ可能性があるため、ここでは例を示しません。

統計から全体的なサーバ応答を取得するために、external_service_serverオブジェクトには次のカウンタがあります。

```
cluster::*> statistics show -object external_service_server -counter ?
  connect_failures
  connect_latency_hist
  instance_name
  instance_uuid
  last_modified_timestamp
  node_name
  node_uuid
  num_connect_attempts
  process_name
  server_ip_address
  server_name
  service_name
  vserver_name
  vserver_uuid
```

個々の呼び出しの遅延を把握するには、external_service_opオブジェクトを使用します。このオブジェクトには次のカウンタがあります。

```
cluster::*> statistics show -object external_service_op -counter ?
  instance_name
  instance_uuid
  last_modified_timestamp
  node_name
  node_uuid
  num_not_found_responses
  num_request_failures
  num_requests_sent
  num_responses_received
  num_successful_responses
  num_timeouts
  operation
  process_name
  request_latency
  request_latency_hist
  server_ip_address
  server_name
  service_name
  vserver_name
  vserver_uuid
```

エラーを理解するには、external_service_op_errorオブジェクトを使用します。

```
cluster::*> statistics show -object external_service_op_error -counter ?
  count
  error_string
  instance_name
  instance_uuid
  last_modified_timestamp
  node_name
  node_uuid
  operation_name
  process_name
  server_ip_address
  server_name
  service_name
  vserver_name
  vserver_uuid
```

SecD外部サーバの統計

また、ONTAPはdiag権限レベルでsecd統計情報を提供し、secdプロセスに固有の接続に関するサーバ接続や障害などの情報を提供します。これらの統計のほとんどは最近のクエリに対してのみ提供されるため、常に表示されるとは限りません。

SecD接続統計の例：

```
cluster::*> diag secd connections show -node node2 -vserver svm1
[ Cache: LSA/domain.example.com ]
  Queue> Waiting: 0, Max Waiting: 1, Wait Timeouts: 0, Avg Wait: 0.00ms
  Performance> Hits: 4, Misses: 1, Failures: 0, Avg Retrieval: 8.20ms

 + Rank: 01 - Server: 198.51.100.120 (2k8-dc-1.domain.example.com)
              Connected through the 198.51.100.9 interface, 0.0 mins ago
              Used 5 time(s), and has been available for 2 secs
              RTT in ms: mean=1.00, min=1, max=1, med=1, dev=0.00 (0.0 mins of data)

[ Cache: LDAP (Active Directory)/domain.example.com ]
  Queue> Waiting: 0, Max Waiting: 1, Wait Timeouts: 0, Avg Wait: 0.00ms
  Performance> Hits: 1, Misses: 1, Failures: 0, Avg Retrieval: 6.00ms

 + Rank: 01 - Server: 198.51.100.120 (2k8-dc-1.domain.example.com)
              Connected through the 198.51.100.9 interface, 0.0 mins ago
              Used 2 time(s), and has been available for 2 secs
              RTT in ms: mean=4.00, min=1, max=7, med=7, dev=3.00 (0.0 mins of data)

[ Cache: LDAP (NIS & Name Mapping)/<no key> ]
  Queue> Waiting: 0, Max Waiting: 1, Wait Timeouts: 0, Avg Wait: 0.00ms
  Performance> Hits: 4, Misses: 1, Failures: 0, Avg Retrieval: 0.60ms

 + Rank: 01 - Server: 198.51.100.120 (198.51.100.120)
              Connected through the 198.51.100.9 interface, 0.0 mins ago
              Used 5 time(s), and has been available for 2 secs
              RTT in ms: mean=8.60, min=2, max=22, med=4, dev=7.58 (0.0 mins of data)
```

9 ネームサービスの問題の診断とトラブルシューティング

次のセクションでは、ネームサービスの問題を診断するためのヒントをいくつか示します。

ネームサービスの問題の一般的な原因

RTTが高くなったりエラーが増加したりする一般的な原因には、次のようなものがあります。

- 低速のLANまたはWANリンク
- クライアントおよびストレージシステムに長距離を転送する必要があるネームサービスサーバ
- ネットワークの切断/切断/停止
- ネームサービスサーバがビジー状態または過負荷状態（TCP接続が多すぎる、CPUが上限に達している、負荷を分散するためのサーバが不足しているなど）
- ネームサービスへのTCPまたはUDP接続をブロックするファイアウォールルール

ネームサービス停止の一般的な症状

- ユーザとグループの名前解決に時間がかかるか失敗する
- 権限/マウント/ CIFS共有のアクセスに関する問題
- NFSファイルのリスト表示に時間がかかる、またはハングアップする
- DNSプロセスまたはSecDプロセスに関するログのエラー（event log show on the cluster）

ホストでエクスポートポリシーアクセスを確認

次のコマンドを使用します。

```
cluster::*> vserver export-policy check-access -vserver svm1 -client-ip 1.2.3.4 -volume flex_vol
-authentication-method sys -protocol nfs3 -access-type read

                                          Policy    Policy       Rule
Path                            Policy    Owner     Owner Type  Index Access
------------------------------- --------- --------- ----------- ----- ------
/                               default   vs1_root  volume          1 read
/dir1                           default   vs1_root  volume          1 read
/dir1/dir2                      default   vs1_root  volume          1 read
/dir1/dir2/flex1                data      flex_vol  volume         10 read
```

NFSエクスポートポリシーのアクセスキャッシュを変更します。

また、アクセスキャッシュの更新間隔を制御するNASレイヤでNFSエクスポートポリシーのアクセスキャッシュ属性を変更することもできます。デフォルト値を確認するには 、**advanced** 権限に切り替える必要があります。

```
cluster::*> export-policy access-cache config show -vserver svm1

                           Vserver: svm1
    TTL For Positive Entries (Secs): 3600
    TTL For Negative Entries (Secs): 3600
TTL For Entries with Failure (Secs): 5
            Harvest Timeout (Secs): 86400
```

注：値の詳細については、を `man export-policy access-cache config modify`参照してください。

外部ネームサービスの応答を確認

ONTAPでは、バージョン8.3以降のネームサービスに標準のlibc関数を使用します。次のgetXXbyYY標準呼び出しは、ONTAPのクラスタシェルで使用できます。

表10）getXXbyYY関数の説明

機能	機能
getaddrinfo	ホスト名を使用して完全なIPアドレス情報を取得する
Getgrbygid	グループID（GID）を使用して、グループ名、GID、およびメンバーを取得する
Getgrbyname	グループ名を使用してグループ名、GID、メンバーを取得する
Getgrlist	ユーザ名のグループメンバーシップリスト（GID）を取得する
gethostbyaddr	IPアドレスからホスト名情報を取得する
gethostbyname	ホスト名からIPアドレス情報を取得する
getnameinfo	IPアドレスからホスト名情報を取得する
Getpwbyname	ユーザ名を使用してpasswdエントリ情報を取得する
Getpwbyuid	ユーザID（UID）を使用してpasswdエントリ情報を取得する
Netgrp	クライアントがネットグループの一部かどうかの確認

機能	機能
Netgrpbyhost	ホスト単位のネットグループ クエリを使用して、クライアントがネットグループの一部かどうかをチェックします。

getXXbyYY次のコマンドを使用したネットグループ検索の例：

```
cluster::*> getxxbyyy netgrpbyhost -node node-01 -vserver svm1 -netgroup netgroup2 -clientIP
198.51.100.140
  (vserver services name-service getxxbyyy netgrpbyhost)
Netgroup.byhost not enabled in all the configured sources
Hostname resolved to: centos65.domain.example.com
```

を使用したユーザ検索の例 getXXbyYY：

```
cluster::*> getxxbyyy getpwbyuid -node node-01 -vserver svm1 -userID 1107
  (vserver services name-service getxxbyyy getpwbyuid)
pw_name: ldapuser2
pw_passwd:
pw_uid: 1107
pw_gid: 10005
pw_gecos:
pw_dir:
pw_shell: /bin/sh
```

getXXbyYYを使用したトラブルシューティング

この getXXbyYY コマンドには、管理者が要求中に使用されているネームサービスソースを表示するためのフラグもあります。これは問題のトラブルシューティングに役立ちます。

```
     [-show-source {true|false}] - Source used for Lookup
         Use this parameter to specify if source used for lookup needs to be
         displayed
```

また、使用するネームサービスをより詳細に表示する非表示フラグもあり called show-granular-errます。

提供されたトラブルシューティングフラグを使用してgetXXbyYYを使用したユーザ検索の例：

```
cluster::*> getxxbyyy getpwbyname -node node-01 -vserver svm1 -username root -show-source true
-show-granular-err true
  (vserver services name-service getxxbyyy getpwbyname)
Source used for lookup: NIS
pw_name: root
pw_passwd: ABCD!efgh12345$67890
pw_uid: 0
pw_gid: 1
pw_gecos:
pw_dir:
pw_shell: /bin/sh
NIS:
Error code:    NS_ERROR_NONE
Error message: No error
LDAP:
Error code:    NS_ERROR_NONE
Error message: No error
DNS:
Error code:    NS_ERROR_NONE
Error message: No error
FILES:
Error code:    NS_ERROR_NONE
Error message: No error
Deterministic Result: Success
```

次の例では、検索時に失敗したネームサービスソースを簡単に確認できます。提供されたトラブルシューティングフラグを使用してgetXXbyYYを使用したユーザおよびグループの検索に失敗した例：

```
cluster::*> getxxbyyy getgrbyname -node node-01 -vserver svm1 -groupname group1 -show-source true
-show-granular-err true
  (vserver services name-service getxxbyyy getgrbyname)
NIS:
Error code:    NS_ERROR_NONE
Error message: No error
LDAP:
Error code:    NS_ERROR_CONN_ERR
Error message: Connection error
DNS:
Error code:    NS_ERROR_NONE
Error message: No error
FILES:
Error code:    NS_ERROR_NOT_FOUND
Error message: Entry not found
Deterministic Result: Transient Error
```

```
cluster::*> getxxbyyy getpwbyname -node node-01 -vserver svm1 -username ldapuser -show-source
true
-show-granular-err true
  (vserver services name-service getxxbyyy getpwbyname)
NIS:
Error code:    NS_ERROR_CONN_ERR
Error message: Connection error
LDAP:
Error code:    NS_ERROR_NONE
Error message: No  error
DNS:
Error code:    NS_ERROR_NONE
Error message: No error
FILES:
Error code:    NS_ERROR_NOT_FOUND
Error message: Entry not found
Deterministic Result: Transient Error
```

ベストプラクティス22）ネームサービスサーバの数

すべてのネームサービスサーバ（LDAP、DNS、NIS、Active Directoryなど）のファストイーサネット接続に複数のネームサービスサーバを配置することを推奨します。複数のサーバが冗長性とロードバランシングを提供し、NAS環境における単一点障害を排除します。

ネームサーバのタイムアウト値

次の表に、ONTAPオペレーティングシステムでのネームサービスのさまざまなタイムアウトを示します。

表11）ネームサーバのタイムアウト

ネームサービスタイムアウトタイプ	タイムアウトチ
LDAPサーバのバインド	5秒（設定不可）
LDAPクエリ	3秒（デフォルト）、10秒（最大）
SecD RPCコール	23秒（設定不可）
DNSクエリ	2秒（デフォルト）、5秒（最大）
SecDサーバ接続	2秒のping応答（設定不可）
「不正な」DNSサーバキャッシュ	10分（設定不可）

付録

ここでは、このテクニカルレポートの主要なセクションに含まれていないトピックについて説明します。これには、トラブルシューティング、便利なコマンド、およびその他のトピックが含まれます。このセクションは、本ドキュメントの期間中に変更されることがあります。すべてのユースケースをカバーするわけではありません。

DNS用語

次の表は、一般的に使用されるDNS用語の定義を示しています。

A	ホスト名からIPへの解決を実行するIPv4アドレスのリソースレコード
AAAA	ホスト名からIPへの解決を実行するIPv6アドレスのリソースレコード
お父さん	重複アドレス検出
DDNS	動的DNS：DNSレコードの動的更新
DNS	ドメインネームシステム：ホスト名をIPアドレスにマッピングします。その逆も同様です。
FQDN	Fully Qualified Domain Name：DNSサフィックスが付加されたホスト名（例：host.example.comはFQDN）
PTR	IPからホスト名への解決のためのポインタ・レコード
RR	DNSリソースレコード
SOA	Start of authority record：レコードの信頼できるソースとなるDNSサーバを指定します。
TTL	Time-To-Live：DNSレコードが更新されるまでキャッシュに残っている時間

DNSエントリをテストするためのクライアントからのホスト名の照会

ネットグループ内のホスト名のベストプラクティスに従って、すべてのホスト名をフォワードルックアップとリバースルックアップでDNSに解決できる必要があります。クライアントからこの機能をテストするには、dig（ドメイン情報グローパー）とnslookup（ネームサービスルックアップ）の2つの主要ツールを使用できます。

- DIGのマニュアルページ
- nslookupのマニュアルページ
- Windows nslookupリファレンス

DNSエラータイプのリストについては、RFC-2929を参照してください。

掘削の例

DIGの例：ホスト名の前方検索：

```
# dig centos64.example.com -t any

; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.30.rc1.el6_6.1 <<>> centos64.example.com -t any
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15976
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;centos64.example.com. IN ANY

;; ANSWER SECTION:
centos64.example.com. 3600 IN A    198.51.100.140

;; Query time: 0 msec
;; SERVER: 198.51.100.120#53(198.51.100.120)
;; WHEN: Mon Apr 13 16:06:33 2015
;; MSG SIZE rcvd: 67
```

DIGの例：リバースルックアップ：

```
# dig -x 198.51.100.140

; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.30.rc1.el6_6.1 <<>> -x 198.51.100.140
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14692
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;140.100.51.198.in-addr.arpa.   IN      PTR

;; ANSWER SECTION:
140.100.51.198.in-addr.arpa. 3600 IN    PTR     centos64.example.com.

;; Query time: 0 msec
;; SERVER: 198.51.100.120#53(198.51.100.120)
;; WHEN: Mon Apr 13 16:08:19 2015
;; MSG SIZE rcvd: 92
```

掘削例：SRVレコード：

```
# dig _ldap._tcp.example.com -t srv

; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.30.rc1.el6_6.1 <<>> _ldap._tcp.example.com -t srv
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41418
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 2

;; QUESTION SECTION:
;_ldap._tcp.example.com. IN        SRV

;; ANSWER SECTION:
_ldap._tcp.example.com. 600 IN SRV 0 100 389 2k8-dc-1.example.com.

;; ADDITIONAL SECTION:
2k8-dc-1.example.com. 3600 IN A    198.51.100.120
2k8-dc-1.example.com. 3600 IN AAAA fd20:8b1e:b255:8599:5457:61d9:fc87:423f

;; Query time: 1 msec
;; SERVER: 198.51.100.120#53(198.51.100.120)
;; WHEN: Mon Apr 13 16:01:34 2015
;; MSG SIZE rcvd: 150
```

DIGの例：存在しないレコード：

```
# dig fail.example.com

; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.30.rc1.el6_6.1 <<>> fail.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 64486
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;fail.example.com.              IN      A

;; AUTHORITY SECTION:
example.com.            60      IN      SOA     ns1.example.com. ops.support.example.com.
1272525332 14400 20000 3600000 60

;; Query time: 132 msec
;; SERVER: 198.51.100.120#53(198.51.100.120)
;; WHEN: Mon Apr 13 16:02:21 2015
;; MSG SIZE rcvd: 85
```

nslookupの例

nslookupの例：前方検索：

```
# nslookup -type=any centos64.example.com.
Server:         198.51.100.120
Address:        198.51.100.120#53

Name:   centos64.example.com
Address: 198.51.100.140
Nslookup example: reverse lookup:
# nslookup -type=ptr 198.51.100.140
Server:         198.51.100.120
Address:        198.51.100.120#53

140.100.51.198.in-addr.arpa     name = centos64.example.com.
```

nslookupの例：SRVレコード：

```
# nslookup -type=srv _ldap._tcp.example.com
Server:         198.51.100.120
Address:        198.51.100.120#53

_ldap._tcp.example.com     service = 0 100 389 2k8-dc-1.example.com.
```

nslookupの例：存在しないレコード：

```
# nslookup -type=any fail.example.com
Server:         198.51.100.120
Address:        198.51.100.120#53

** server can't find fail.example.com: NXDOMAIN
```

参考資料

TR-4073：『Secure Unified Authentication』

TR-4182：『ONTAP構成でのイーサネットストレージのベストプラクティス』

TR-4191：『Best Practices Guide for ONTAP 8.2.x and 8.3 Windows File Services』

TR-4523：『DNS Load Balancing in ONTAP』

TR-4557：『NetApp FlexGroup Technical Overview』

本ドキュメントに記載されている製品や機能のバージョンがお客様の環境でサポートされるかどうかについては、NetApp サポート サイトで Interoperability Matrix Tool (IMT)を参照してください。NetApp IMT には、NetApp がサポートする構成を構築するために使用できる製品コンポーネントやバージョンが定義されています。サポートの可否は、お客様の実際のインストール環境が公表されている仕様に従っているかどうかによって異なります。

機械翻訳に関する免責事項

原文は英語で作成されました。英語と日本語訳の間に不一致がある場合には、英語の内容が優先されます。公式な情報については、本資料の英語版を参照してください。翻訳によって生じた矛盾や不一致は、法令の順守や施行に対していかなる拘束力も法的な効力も持ちません。

著作権に関する情報

商標に関する情報