Technical Report

Name Services Best Practices Guide

Justin Parisi, NetApp
October 2016 | TR-4379

Abstract

This document provides a comprehensive list of best practices, limits, recommendations, and considerations when implementing network-attached storage (NAS) solutions such as CIFS/SMB and NFS in NetApp® clustered Data ONTAP®.

Data Classification

Public

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF BEST PRACTICES

Version History

Version	Date	Document Version History
Version 2.4	October 2016	Updated for ONTAP 9.1
Version 2.3	July 2016	Updated for ONTAP 9.0
Version 2.2	May 2016	Updated for ONTAP 8.3.2
Version 2.1	July 2015	Updated for ONTAP 8.3.1
Version 2.0	May 2015	Updated for ONTAP® 8.3
Version 1.0	February 2015	Initial release

1 Introduction

The NetApp ONTAP operating system provides the ability to unify clients under a single namespace by way of storage virtual machines (SVMs). These SVMs can live on clusters that are up to 24 nodes in size. Each SVM provides the ability to offer individualized LDAP, NIS, DNS, and local file configuration for authentication purposes. These features are also known as “name services.”

External servers can provide replicated copies of databases containing user information, such as UID, GID, group membership, home directory, and other information, as well as netgroup and name resolution capabilities. These external servers make it possible to manage large environments that span global locations without extra administrative overhead and with the ability to reduce WAN latency by providing localized copies of databases to clients and servers.

1.1 Scope

This document covers the following topics:

- ONTAP NAS overview
- Name service overview
- Supported configurations
- Benefits of using name services with NAS
- Configurations and best practices

Note: This document covers only versions of clustered Data ONTAP later than 8.2.

1.2 Intended Audience and Assumptions

This technical report is for storage administrators, system administrators, and data center managers. It assumes basic familiarity with the following:

- NetApp FAS systems and the Data ONTAP operating system
- Network file-sharing protocols

Note: This document contains advanced and diag-level commands. Exercise caution when using these commands. If you have questions or concerns, contact NetApp Support for assistance.

1.3 What Is a Name Service?

Name services are objects that process name requests from NetApp storage systems. Name requests can be for users, groups, netgroups, or host names and can be external resources. This includes:

- Local files (hosts, passwd, netgroup, and so on)
- DNS
- NIS
- LDAP

1.4 Storage Virtual Machine (SVM) Types

Clustered Data ONTAP includes multiple types of SVMs:

- **Data SVMs** are used for data access.
- **Cluster SVMs** are used for cluster administration.
- **Node SVMs** (8.2.x and earlier) are used for node administration. These SVMs have been deprecated in clustered Data ONTAP 8.3 and later.

2 NAS in ONTAP

The ONTAP 9 operating system provides world-class enterprise-level storage to clients running NAS operations for use cases including, but not limited to:

- Home directories
- Application database hosting
- Archiving and staging
- Software source control
- Log file storage
- Video streaming

The ONTAP operating system supports cutting-edge technologies in both CIFS and NFS so that the latest and greatest feature sets can be leveraged in data centers across the globe.

Supported protocol versions include:

- NFSv3, NFSv4, and NFSv4.1
- SMB 1.0, SMB 2.0, and SMB 3.0

For more information about supported features for these protocols, see TR-4067 and TR-4191.

2.1 How NAS Requests in the Clustered Data ONTAP Operating System Work

A cluster can contain up to 24 nodes for NAS operations in ONTAP. Each physical node can own virtual objects such as volumes or data LIFs. An SVM spans all nodes in a cluster and allows interaction of logical storage entities under a single namespace. When a NAS client attempts to connect to an ONTAP system by using CIFS or NFS, that request can potentially reach any node in a 24-node cluster based on DNS and client settings. If a node hosting a data LIF is used in a NAS operation that does not own the data volume being requested for access, then traffic passes through a dedicated 10GB Ethernet (10GbE) cluster back-end network.

NAS Basics

The following section covers the basic interaction of NAS requests at a high level.

Volumes

All user data in clustered Data ONTAP systems lives in flexible volumes (NetApp FlexVol® volumes). These volumes are located locally to the node that hosts the physical disk space (aggregate). In ONTAP, data can be accessed anywhere in a cluster, regardless of on which node it physically lives.

Logical Interfaces

Each SVM owns storage objects, such as volumes and logical interfaces (LIFs). LIFs can host management, data, or cluster traffic, depending on the assigned role and data protocols allowed. The option `-data-protocol` allows a storage administrator to specify which data protocols are allowed on the data LIF. When a data protocol is allowed on a data LIF, the LIF then listens on a specific list of ports for the protocol. For NAS protocols (CIFS and NFS), the ports listed in Table 1 are opened when the protocol is allowed on a data LIF.

Table 1) Ports for CIFS and NFS traffic on protocol-enabled data LIFs.

Protocol	Ports
NFS	2049: NFS 2049 (program version 400010): vStorage 111: portmapper 635: mountd 4045: Network Lock Manager (NLM) 4046: Network Status Monitor (NSM) 4049: rquota
CIFS	135: RPC 139: NetBIOS 445: SMB 40001: SMB Witness

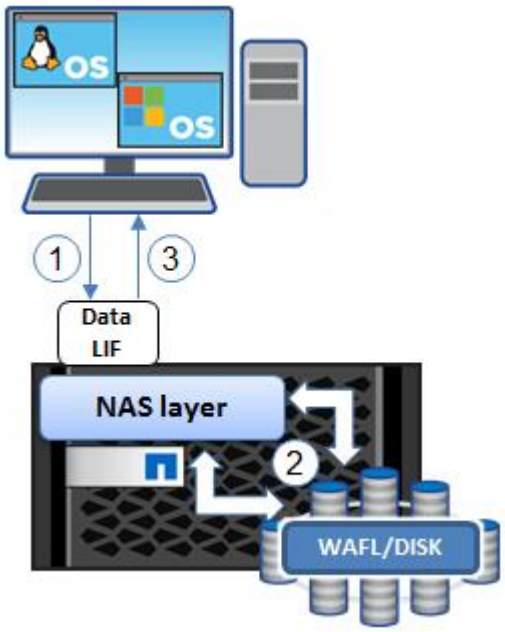
When a NAS request is made to an SVM, the request always arrives on a data LIF (including calls such as `showmount`). The data LIF chosen depends on the client and/or DNS load balancing. For more information about DNS load balancing in clustered Data ONTAP, see TR-4073 or TR-4182.

When a data LIF receives a NAS request, it passes through the NAS layer for processing and handling.

NAS Layer

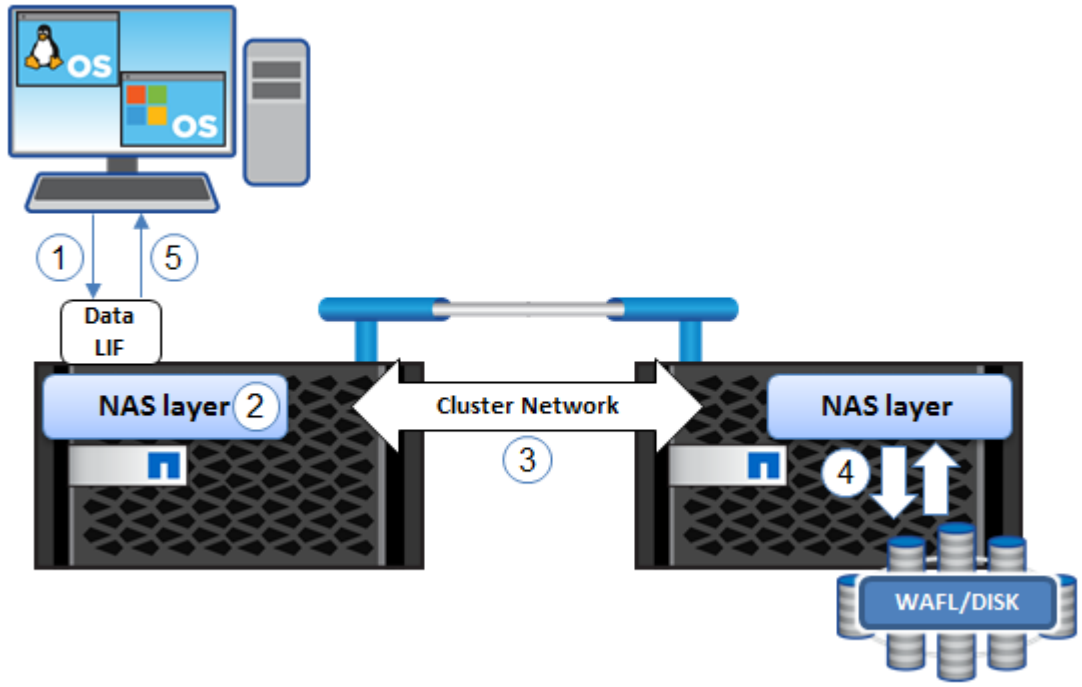
When a NAS request arrives on a physical interface, that request is forwarded to the NAS layer for processing. The NAS layer sends RPC calls to cluster processes, such as security daemon (SecD) and the volume location database (VLDB), to determine data locality, user credentials, and other NAS configuration aspects so that the request passes through the appropriate paths in the cluster. If the data being requested is local to the data LIF that receives the request from the client, then the request goes straight to disk by way of NAS fast path mechanisms. If the data is on another node in the cluster, then the request traverses the cluster interconnect network.

Figure 1) NAS protocol path in ONTAP: local request.



1. NAS request is sent from the client to the SVM data LIF.
2. NAS layer is bypassed because data is local. Request is sent right to disk.
3. Request passes back through the stack and is sent back to the NAS client on the same data LIF on which it arrived.

Figure 2) NAS protocol path in ONTAP: remote request.



1. NAS request is sent from the client to the SVM data LIF.
2. NAS layer receives all NAS requests and processes them.
3. If remote, NAS request is sent over the cluster network to the NAS layer local to the data.
4. NAS layer processes the request and reads from/writes to disk.
5. Request passes back through the stack and is sent back to the NAS client on the same data LIF on which it arrived.

When the request reaches the NAS layer, an RPC call is sent to the SecD so that the user requesting access can authenticate with the SVM.

Security Daemon (SecD)

SecD is an application that runs on a per-node basis. The SecD application handles name service lookups such as Active Directory, DNS NIS, and LDAP, as well as credential queries, caching, and name mapping. SecD is node-specific, which means that a SecD process exists on each node in a cluster. When a NAS request arrives on a data LIF, the node that hosts that data LIF also hosts the SecD application used for authentication and authorization of the user.

SecD communicates with external name services by way of API calls, so there needs to be at least one LIF in the SVM that is routable to the name service servers. In the Data ONTAP 8.3 operating system and later versions, SecD is able to intelligently forward name service requests to remote nodes when necessary, such as during CIFS server creation.

Management Gateway Daemon (mgwd)

The management gateway in the clustered Data ONTAP operating system is exactly what it sounds like: It is the gateway into managing a cluster. It is responsible for maintaining and reporting cluster health/quorum; receiving SSH logins, SNMP, and NetApp Manageability SDK calls from management software (such as NetApp OnCommand® System Manager); processing export rules; and caching results. In addition, it interacts with all of the other cluster applications through RPC to send and receive requests for configuration reads and writes.

Best Practice 1: SecD and Data LIFs

In versions earlier than the Data ONTAP 8.3 operating system, SecD did not have the ability to route to any node in the cluster. As a result, any operation that leveraged SecD (for instance, CIFS server creation) had to be performed on a node that owned a data LIF that was routable to name services. These requests could fall back onto node management LIFs, provided they were routable. In clustered Data ONTAP 8.2.x and earlier, NetApp recommends having a data or node management LIF that is routable to name services (such as LDAP, AD, and so on) on every node in the cluster for SVMs. For more information about DNS host name lookup behavior, see the section in this document about host names. Data ONTAP 8.3 and later versions do not have this limitation, but a best practice is still to have a data LIF on each node that routes properly to name services to enable data locality. However, it is still a requirement to have at least one data LIF per SVM that can route to name services for NAS environments. Data ONTAP 8.3 and later versions do not include fallback to management LIFs for name service requests for SecD, however, so each SVM is required to have at least one data LIF that is routable to name services.

3 Name Services

Name services are external servers that contain user and host information in an enterprise environment. This definition includes NIS, LDAP, and DNS, as well as local files and Microsoft Windows Active Directory.

3.1 Benefits of Using Name Services

In large environments with thousands of users and hosts, managing individual flat files for users, groups, netgroups, and host resolution is virtually impossible. Name service servers allow administrators to keep a database of current information for business-critical objects with which client machines and storage devices can interact for consistency of these objects across an enterprise environment. When all clients and storage access the same servers with the same databases, there can be no mistake in credential retrieval or host name resolution.

Other benefits of using name service servers include:

- Consolidation of users, groups, netgroups, and host names
- Disaster recovery through site replication of name service server databases
- Reduction in WAN latency by way of site replication to produce localized copies of server databases
- Load balancing and failover functionality

3.2 Name Services in Clustered Data ONTAP Operating Systems

In clustered Data ONTAP system versions earlier than 8.2.x, name services (DNS, NIS, LDAP, and so on) were all handled by the authentication process called SecD, which is the security daemon. Configuration for nsswitch.conf functionality was done under SVM options.

In Data ONTAP 8.3 operating systems and later versions, configuration of name services functionality has been moved to its own command set called `vserver services name-service`:

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

Additional diagnostic commands, such as `getXXbyYY`, exist at the advanced privilege level:

```
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
```

To view the current ns-switch configuration:

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

Note that in the preceding, support for granular control over `passwd`, `group`, `netgroup`, and so on has been added, making the ns-switch functionality in Data ONTAP 8.3 and later comparable to standard `nsswitch.conf` files.

In addition to added ns-switch functionality, other new features have been added to name services:

- DNS and NIS statistics
- `getXXbyYY` support
- Improved NIS troubleshooting tools (tracing and showing bound servers)
- Name service queue status
- Name service configuration mirroring and repair

Order of Operations for ns-switch and nm-switch

When specifying multiple sources for ns-switch and nm-switch, it is important to consider what happens in the event of successful or unsuccessful lookups.

If using multiple name service sources in ns-switch and/or nm-switch, the following are true:

- When a successful query is made, the operation is finished. The next name service source is not tried, even if the object exists in both places.
- If the object doesn't exist in any name service source, the operation fails.

Therefore, it's important to list name service sources in order of priority.

4 Supported Configurations

Table 2 shows a list of the supported name service switch databases in the Data ONTAP 8.3 operating system.

Table 2) Supported name service databases in clustered Data ONTAP.

Ns-switch Database	Supported Name Services
Hosts	DNS, local files
Passwd (users)	NIS, LDAP, local files
Group	NIS, LDAP, local files
Netgroup	NIS, LDAP, local files
Namemap	LDAP, local files

4.1 Host Names

In the Data ONTAP 8.3 operating system and later versions, host name lookups (such as for use with export policy rules) are supported for use in both DNS and local files for SVMs. In versions of Data ONTAP earlier than 8.3, host names were supported only for use with DNS in data SVMs. However, host names could be provided at the cluster SVM level.

Note: For more clarification about the differences between data and cluster SVMs, see the section in this document about Storage Virtual Machine (SVM) Types.

Clustered Data ONTAP 8.3 and later versions do not support host name resolution through the cluster SVM for NFS export rule processing (that is, a single central DNS configuration for all SVMs in a cluster). Starting in 8.2.1, host name queries for export policy rules were moved from clusterwide DNS to the individual SVM to increase reliability and stability in host lookups. This change affects export policy rules that make use of host names, as well as domains, in the client match.

Note: Host name resolution through LDAP and NIS is currently not supported.

Upgrade Considerations

Starting in clustered Data ONTAP 8.2.2P2, host name resolution leveraging DNS tries the data SVM first and then falls back to the cluster name server if the data SVM DNS server cannot resolve the host name. However, in clustered Data ONTAP 8.3 and later, the cluster SVM is never used for DNS lookups. Therefore, DNS should always be configured for use with the data SVM. To avoid latency in lookups and potential failures, make sure that all host names that are specified in netgroups or export policy rules can be resolved (both forward and reverse) in the data SVM DNS server.

Note: When upgrading from 8.2.x to 8.3.x, all host name resolution is performed at the SVM level and never falls back to the cluster SVM DNS configuration. Thus, exports that rely on the cluster SVM experience failures.

Best Practice 2: Using Local Hosts When Upgrading from Clustered Data ONTAP 8.2.x to 8.3.x

If you intend to upgrade a cluster from 8.2.x or earlier to 8.3.x and local host names are being used in data SVMs, make sure that the host names and IP addresses exist in both the cluster admin SVM and the data SVMs. This step reduces the chance of having outages. Ideally, these host names are sourced from DNS rather than from local files.

4.2 Netgroups

Netgroups are supported for use with files, NIS, and LDAP in all versions of clustered Data ONTAP systems. NetApp recommends that netgroups use LDAP for security and scalability. When using netgroups, NetApp highly recommends leveraging the netgroup.byhost functionality (available in clustered Data ONTAP 8.2.3 and later) for faster lookups and, thus, better performance. For information about configuring netgroups and netgroup.byhost maps in LDAP, see TR-4073: Secure Unified Authentication.

4.3 User and Group Information

User and group information (such as UID/GID) can be stored in files, NIS, or LDAP in all versions of clustered Data ONTAP. In Data ONTAP 8.3 and later, users and groups can leverage different name service databases in the same SVM (such as local files for groups, LDAP for users).

Example:

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

NetApp recommends that users and groups use LDAP for security and scalability, because LDAP can provide encrypted lookups and supports use with more servers than an NIS configuration.

Limits

As local users and groups are created, the replicated database tables that make the clustered Data ONTAP operating system run properly grow in size and memory allocation. If these databases grow to the point of memory exhaustion when reading/writing the tables, cluster outages can occur. Therefore, clustered Data ONTAP 8.2.3 and later introduced a hard limit on local users and groups. This limit is clusterwide and affects all SVMs.

Best Practice 3: Local UNIX Users and Groups

In versions earlier than the clustered Data ONTAP 8.2.3 operating system, there was no hard limit on local users and groups. However, that does not mean that there is no actual limit. NetApp highly recommends not exceeding the local UNIX user and group limits as defined in Table 3 when using clustered Data ONTAP operating system versions earlier than 8.2.3.

Note: This limit is for local UNIX users and groups. Local CIFS users and groups (`vserver cifs users-and-groups`) have an independent limit and are not affected by this limit.

Table 3) Limits on local users and groups in clustered Data ONTAP.

Local UNIX User Limit in 8.3 (Default and Maximum)	Local UNIX Group Limit in 8.3 (Default and Maximum)
32,768 (default) 65,536 (maximum)	32,768 (default) 65,536 (maximum)

As previously mentioned, the local UNIX user and group limits are clusterwide and affect clusters with multiple SVMs. Thus, if a cluster has four SVMs, then the maximum number of users in each SVM must add up to the maximum limit set on the cluster.

For example:

- SVM1 has 2,000 local UNIX users.
- SVM2 has 40,000 local UNIX users.
- SVM3 has 20 local UNIX users.
- SVM4 would then have 23,516 local UNIX users available to create.

Any UNIX user or group creation attempted beyond the limit results in an error message.

Example:

```
cluster::> unix-group create -vserver SVM -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.
```

The limits are controlled by the following commands at the advanced privilege level:

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

Upgrade Considerations

When upgrading to a Data ONTAP version with the hard limits set, there is no check for existing users and groups. Therefore, if the limit is already exceeded on the cluster, the upgrade succeeds, but no new users and groups can be created. Also, if problems occur while the limit is exceeded, support issues might arise (for example, support deems your configuration as “unsupported”). Reducing the number of users and groups to below the limits is highly recommended. You can take this action before or after upgrades.

5 Best Practices

5.1 Differences Between 8.2.x and 8.3.x

The clustered Data ONTAP 8.2.x and 8.3.x operating systems have major architectural differences with regard to name services. The following section covers those differences and how they pertain to best practices in NAS environments.

Name Services in Clustered Data ONTAP 8.2.x and Earlier

Versions earlier than and including clustered Data ONTAP 8.2.x operating systems used two different mechanisms for name services. At the SVM level, the security daemon (SecD) was used to query all name services. However, the clusterwide name services configurations were performed by using a unified interface that leveraged standard libraries at the BSD level in the operating system. As a result, the cluster and SVMs used different methods to resolve host names, query name servers (such as Active Directory), and so on. Therefore, functionality such as local host name resolution was not supported at the SVM level of granularity.

Name Services in Data ONTAP 8.3 and Later

In Data ONTAP 8.3 systems and later versions, name services were moved to a converged infrastructure leveraging the same standardized unified interface for all name service requests, on both a clusterwide and an SVM level.

Most Notable Differences

Because of the change in name service architecture to one of a more converged nature, the following differences are most notable between clustered Data ONTAP 8.2.x and 8.3 operating systems:

- Name service configuration (new name services commands)
- Support for local host names per SVM
- Unified interface used for all name services
- Local UNIX user and group hard limits
- Netgroup load commands with hard limits for file sizes
- IPv6 support for DNS load balancer
- Ability to configure data LIFs to participate in on-box DNS but not act as DNS servers (send-soa)
- NIS and DNS statistics
- getXXbyYY functionality

5.2 Name Service (ns-switch) and Name Mapping (nm-switch)

The following section covers best practices for name service (ns-switch) and name mapping (nm-switch) configuration in clustered Data ONTAP operating systems.

What Is ns-switch?

Ns-switch is the *name service* switch. This controls which name service sources are used and the order in which the name service sources are used by the SVM for user/group, host, namemap, and netgroup lookups. In operating systems running clustered Data ONTAP 8.2.x and earlier, this was controlled with the `vserver` command. In versions of Data ONTAP 8.3.x and later, this is handled with the `name-service` command.

Example of clustered Data ONTAP 8.2.x ns-switch:

```
cluster82::> vserver modify -vserver SVM -ns-switch
    nis  file ldap
```

Example of Data ONTAP 8.3.x ns-switch:

```
cluster83::> name-service ns-switch modify -vserver SVM -database
    group    hosts    namemap  netgroup passwd
```

What Is nm-switch?

Nm-switch is the *name mapping* switch. This controls which name mapping source is used by the SVM for mapping UNIX users to Windows users and vice versa. This only applies to multiprotocol environments. Name mapping rules can exist in local tables in the cluster or on LDAP servers. In clustered Data ONTAP 8.2.x operating systems and earlier versions, this was controlled with the `vserver` command. In versions of Data ONTAP 8.3.x and later, this is handled with the `name-service` command, which is located in the `vserver services` command directory.

Example of clustered Data ONTAP 8.2.x nm-switch:

```
cluster82::> vserver modify -vserver SVM -nm-switch
    file ldap
```

Example of Data ONTAP 8.3.x nm-switch:

```
cluster83::> name-service ns-switch modify -vserver SVM -database namemap -sources
    files ldap
```

5.3 Name Server Configuration Best Practices

The following section covers name server best practices for use with clustered Data ONTAP.

What Is a Name Server?

A name server is any external server that provides a database for name services. Name servers can include, but are not limited to:

- DNS
- LDAP
- NIS

Name Server Transport Information

Because name servers are external servers, they leverage standard network transport protocols and are subject to the same issues to which any protocol running over an Ethernet network is subject, such as latency, retransmissions, and so on.

UDP or TCP?

Some name servers can leverage both TCP and/or UDP for network transport, such as DNS. DNS uses UDP by default. However, in the Data ONTAP 8.3 operating system, if a DNS response packet is greater than 512 bytes, then TCP is used to retrieve the remaining information.

Table 4) Name service transport protocols.

Service	Transport
NIS	UDP with the management gateway (mgwd) TCP with the security daemon (SecD)
LDAP	TCP
DNS	UDP by default; falls back on TCP

UDP is short for User Datagram Protocol and is generally regarded as the lesser of the two protocols because of its unreliability and limitations. TCP is short for Transmission Control Protocol and is used when a network connection requires a method to guarantee that a packet arrived between two networked entities. Most name servers use TCP for their transport. However, DNS servers still make use of UDP calls for host name lookups because it does provide some advantages over TCP, such as speed and lack of a need for a complete network conversation (that is, no retransmissions).

Best Practice 4: UDP Consideration for DNS

As a best practice, verify that UDP is enabled on the DNS server when possible. UDP does not face the same connection limits that TCP does. A majority of DNS requests are handled by UDP and use TCP only when they are too large to accommodate. TCP is considered a secondary protocol for DNS requests. In earlier versions of clustered Data ONTAP (prior to 8.3), the cluster firewall could actually block TCP connections if flooded with a number of DNS calls, such as with a misconfigured LDAP client. See bug 772638 for details.

In the clustered Data ONTAP 8.2.3 operating system, UDP support for DNS was added for host name lookups. Both UDP and TCP can be used for DNS lookups in 8.2.3 and later. UDP is used for smaller lookups, and TCP is used if the UDP response is truncated because of the size of the response.

It is possible to control the use of UDP or TCP for NFS exports through the NFS server option `-name-service-lookup-protocol` in 8.3.1 and later. The default setting is UDP, and NetApp does not recommend changing it.

```
[-name-service-lookup-protocol {TCP|UDP}] - Set the Protocol Used for Name Services Lookups
This optional parameter specifies the protocol to use for doing name service lookups. The allowed
values are TCP and UDP. The default setting is UDP.
```

Why This Matters

In 8.2.2 and earlier, if a DNS server uses TCP for host name lookups, these connections are not reused by the clustered Data ONTAP operating system. Therefore, a large number of host names in export policies and rules could result in a TCP flood to DNS, which could cause firewalls to treat these as rogue clients and block DNS connections and/or DNS lookups to be delayed, thus causing NFS exports to time out.

In rare cases, the clustered Data ONTAP firewall would need to be disabled to prevent blocking of DNS requests. This would need to be done if the EMS message of `ipfilter.ReachedMaxStates` is seen in `event log show`.

Example of the EMS:

```
cluster::> event route show -messagename ipfilter.ReachedMaxStates
                                     Message Name: ipfilter.ReachedMaxStates
                                         Severity: NOTICE
                                 Corrective Action: (NONE)
                                       Description: This message occurs when the ipfilter firewall
fails to create a new dynamic state entry for a 'keep-state' rule because the number of dynamic
state entries has reached the maximum allowed value of 4013. The 'keep-state' rule is used by the
firewall to keep track of whether a connection is established. States are maintained by firewall
for TCP, UDP, and ICMP packets. This message occurs at most once every 60 seconds; it lists the
most recent connections to reach the limit.
                                Supports SNMP trap: false
                                      Destinations: -
            Number of Drops Between Transmissions: 0
Dropping Interval (Seconds) Between Transmissions: 0
```

To disable the firewall:

```
cluster::> firewall modify -node [nodename] -enabled false
```

Ideally, the firewall should stay disabled only until the root cause of the ipfilter error is resolved. Contact NetApp Technical Support if you encounter this message.

Best Practice 5: Recommended Data ONTAP Version for Name Services

Any clustered Data ONTAP operating system implementation making use of name services for NAS connectivity should ideally run the latest available operating system version, but at a bare minimum, no earlier than 8.2.3P3. Be sure to keep in mind the architecture changes between 8.2.x and 8.3.x when upgrading.

Changing Name Service Lookup Transport Protocols for NFS Exports

In versions of Data ONTAP 8.3 and later, a new NFS server option was added in admin mode that allows changing of the protocol that is used for name service lookups. The default is set to UDP and should be left as UDP unless necessary and under NetApp Support's guidance.

Example of changing the name service lookup protocol:

```
cluster83::> nfs server modify -vserver SVM -name-service-lookup-protocol
    tcp udp
```

LAN Versus WAN

Enterprise NAS environments often have sites at locations across the globe. In many cases, these sites are smaller and do not have resources such as name service servers local to the site. In these scenarios, it is important to make certain that WAN latencies to name service servers do not exceed 2 seconds (2000ms) for name services. For information about viewing latencies for name services, see the section in this document covering name service statistics.

Best Practice 6: Best Practice for Name Services over a WAN

It is a best practice to determine that a name service server is local to any site where NAS access is desired or at least at a site close enough to prevent latencies over a WAN from exceeding 2 seconds.

Note: If using a WAN is required, enable latency monitoring for best results.

General Name Server Best Practices

The following provides a general list of name server best practices for the best possible resiliency and performance for name servers.

Best Practice 7: General Name Server Best Practices

- Always configure multiple servers for redundancy and load balancing.
- Verify that all name servers are in sync.
- Verify that forward and reverse lookup records exist for all hosts, including name servers.
- Verify that name servers are not overloaded (CPU, RAM, network connections, and so on) and can handle the load generated by clustered Data ONTAP storage needs.
- Avoid using virtual machines for production name servers when possible.
- If using virtual machines for name servers, do not host them on NFS datastores that are dependent on those name servers.
- Never specify name services on SVMs (ns-switch, nm-switch) that are not configured with functional name service servers and configurations.

Note: Misconfiguration of name services on SVMs can result in hangs, particularly with NFSv4.x, because the SVM attempts to use the services in the list to resolve nonexistent UID/GID mappings. If no servers are configured but external name services are specified (such as LDAP or NIS), requests for name lookups run indefinitely, and commands such as `ls` appear to hang.

5.4 Name Service Statistics

In versions of Data ONTAP 8.3 and later, new NIS and DNS statistics were added to collect information about requests. These statistics apply only to requests made during data access. These commands are available at the advanced privilege level. In the following output, pay specific attention to the round-trip delay time (RTT) for clues as to which connected name service servers might be experiencing slow responses. Additionally, pay attention to the number of errors or timeouts seen. Although these are not indicative of problems on their own (because host name lookup errors can be natural in large environments), they can be an indication of systemic issues. Incrementing counters over short time periods can suggest that there is an issue with a name server and can justify further investigation.

If some servers seem to be experiencing a high RTT or a large number of query errors, timeouts, and so on, then those servers should be investigated and potentially removed from rotation in the SVM's DNS configuration (using `dns modify`) until the problem is addressed.

Note: These statistics are available only in the Data ONTAP 8.3 operating system and later versions.

Example of DNS statistics:

```
cluster83::*> dns show-statistics -node node1 -vserver SVM

Node: node1

          Name     Average   Minimum   Maximum    Total      Num  Host Not  Timed     Num
Vserver   Server  RTT (us)  RTT (us)  RTT (us)  RTT (s)  Queries     Found    Out  Errors
--------  ------  --------  --------  --------  -------  -------  --------  -----  ------
NAS       10.228.225.120
                      5517       913    103789        2      390        64      0       0
```

Example of NIS statistics:

```
cluster83::*> nis show-statistics -node node1 -vserver SVM

Node: node1

        NIS     Number of    Total   Minimum   Maximum   Average    Number of  Entry Not
Vserver Server YP Lookups  RTT (s)  RTT (us)  RTT (us)  RTT (us)  Retransmits      Found
------  ------ ----------  -------  --------  --------  --------  -----------  ---------
NAS     10.228.225.120  0        0         0         0         0            0          0
```

Additionally, both clustered Data ONTAP 8.2.x and 8.3 offer SecD statistics at the diag privilege level to give information about server connections, failures, and so on.

Example of SecD connection statistics:

```
cluster::*> diag secd connections show -node node2 -vserver SVM
[ Cache: LSA/domain.netapp.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: 10.228.225.120 (2k8-dc-1.domain.netapp.com)
              Connected through the 10.63.21.9 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.netapp.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: 10.228.225.120 (2k8-dc-1.domain.netapp.com)
              Connected through the 10.63.21.9 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: 10.228.225.120 (10.228.225.120)
              Connected through the 10.63.21.9 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)
```

External Services Statistics

In ONTAP 9, new counter manager values for external services were added.

DNS External Statistics

ONTAP 9 adds a set of DNS-specific counters in counter manager. This set of statistics is available at advanced privilege. The objects are:

```
external_service_op
external_service_op_error
external_service_server
```

These counters aggregate the statistics from DNS.

To leverage the statistics, you must start the statistics gathering job. Use a pipe symbol (|) to include multiple objects in the capture:

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

After the gathering interval completes, stop the statistics:

```
::*> statistics stop
Statistics collection is being stopped for sample-id: sample_91613
```

To view the statistics:

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

Sample output of the statistics gathered for external_service_op:

```
Object: external_service_op
Instance: SVM1:DNS:Query:10.193.67.181
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:10.193.67.181
    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                                 10.193.67.181
    server_name                                                     -
    service_name                                                  DNS
    vserver_name                                                 SVM1
    vserver_uuid                                  05e7ab78-2d84-11e6-a796-
                                                          00a098696ec7
```


Sample output of the statistics gathered for external_service_op_error:

```
Object: external_service_op_error
Instance: SVM1:DNS:Query:NXDOMAIN:10.193.67.181
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:10.193.67.181
    last_modified_time                      Thu Jun 30 09:46:14 2016
    node_name                                                node-01
    operation_name                                         DNS Query
    server_ip_address                                  10.193.67.181
    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:10.193.67.181
    last_modified_time                      Thu Jun 30 10:10:20 2016
    node_name                                                node-02
    operation_name                                         DNS Query
    server_ip_address                                  10.193.67.181
    server_name                                                    -
    service_name                                                 DNS
    vserver_name                                                SVM1
    vserver_uuid                           05e7ab78-2d84-11e6-a796-
                                                           00a098696ec7
```

LDAP/NIS/Active Directory External Statistics

ONTAP 9 also adds a new counter in counter manager that shows statistics specific to LDAP, NIS, and Active Directory. This is available at diag privilege. The object is:

```
secd_external_service_op
```

To leverage the statistics, you must start the statistics gathering job. Use a pipe symbol (|) to include multiple objects in the capture:

```
::*> statistics start –object secd_external_service_op
```

After the gathering interval completes, stop the statistics:

```
::*> statistics stop
Statistics collection is being stopped for sample-id: sample_91613
```

To view the statistics:

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

Because the output of these statistics can be extensive, no examples are shown here.

5.5 Diagnosing Name Service Outages

The following sections give some tips on how to diagnose name service outages.

Common Causes of Name Service Outages

Some common causes of high RTT or incrementing errors include:

- Slow LAN or WAN links
- Name service servers that must travel great distances to the clients and storage system
- Network disconnects/drops/outages
- Busy or overloaded name service servers (for example, too many TCP connections, CPU maxed out, not enough servers to balance load)
- Firewall rules blocking TCP or UDP connections to name services

Common Symptoms of Name Service Outages

- Slow or failing user and group name resolution
- Permission/mount/CIFS share access issues
- Slow or hanging listing of NFSv4 files
- Errors in logs concerning DNS or SecD processes (`event log show` on the cluster)

Best Practice 8: General Name Service Best Practice: Number of Name Service Servers

It is a best practice to have multiple name service servers that are on fast Ethernet connections for all name service servers (such as LDAP, DNS, NIS, Active Directory, and so on). Multiple servers provide redundancy and load balancing and eliminate single points of failure in NAS environments.

Name Server Timeouts

The following table shows the various timeouts for name services in the clustered Data ONTAP operating system.

Table 5) Name service timeouts.

Name Service Timeout Type	Timeout (Clustered Data ONTAP)
LDAP server bind	5 seconds (nonconfigurable)
LDAP queries	3 seconds (default); 10 seconds (maximum)
SecD RPC call	23 seconds (nonconfigurable)
DNS query	2 seconds (default); 5 seconds (maximum)
SecD server connection	1 second ping response (nonconfigurable)
“Bad” DNS server cache	10 minutes (nonconfigurable)

Name Servers Hosted in Virtual Machines

In some cases, name servers (for example, DNS and LDAP) are hosted on virtual machines running in virtualized environments such as ESXi, Hyper-V, and so on. This configuration is perfectly fine, but you should also consider the following:

- Name servers on VMs should always have dedicated resources (RAM, CPU, and so on) allocated to their operating systems so that the name servers can respond appropriately.
- Name servers on datastores should not have interdependencies on the devices that they intend to service. For example, if a VM that serves DNS is hosted on an NFS datastore that requires DNS for proper export policy client resolution, that datastore should not be hosted on the same storage that has the dependency on the DNS server.
- For NFS datastores that host VMs with critical servers, such as name servers, it is a best practice to employ a dedicated export policy rule that uses local host entries (8.3 and later) or IP addresses to remove DNS dependency on those exports.

Ypbind

ONTAP 9 introduces a cluster-level command that allows administrators to stop/start ypbind from the CLI. The new command set is under `vserver services name-service ypbind`:

```
  restart                     *restart ypbind
  start                       *Start ypbind
  status                      *Current ypbind status
  stop                        *Stop ypbind
```

5.6 User and Group Best Practices

Limits

In the clustered Data ONTAP operating system, there are limits to the number of users and groups allowed locally on a system. Table 6 covers these limits.

Best Practice 7: Local Users and Group Considerations in Versions Earlier than Data ONTAP 8.3

Clustered Data ONTAP versions earlier than 8.3 did not limit local users and groups, which proved to be problematic for cluster operability. The following values are maximum values tested before the cluster began exhibiting issues and should be used as guidance for all clustered Data ONTAP versions.

Table 6) User and group limits in clustered Data ONTAP, non-scaled mode.

Limit	7-Mode	Data ONTAP 8.3.x (Clustered, non-scaled mode)
Number of characters per user and group (that is, length of name)	32 characters	64 characters
Limits for file size for -load-from-uri (netgroup, unix-user, unix-group)	N/A	UNIX users: 2.5MB UNIX groups: 1MB Netgroups: 5MB If the limit is exceeded, the load fails.
Clusterwide limit on local UNIX users and groups and members	N/A	UNIX users: 32,768 (default); 65,536 (maximum) UNIX groups and members: 32,768 (default); 65,536 (maximum)
UNIX groups single line limit (-load-from-uri)	N/A	32,768 characters
Name mapping rule limits	N/A	1,024 per SVM

Scaled Mode/File-Only Mode

Scaled mode/file-only mode for local users and groups in ONTAP 9.1 allows storage administrators to expand the limits of local users and groups by enabling a **diag-level** name service option and then using the load-from-uri functionality to load files into the cluster to provide higher numbers of users and groups. Scaled mode/file-only mode also can add performance improvements to name service lookups, because there is no longer a need to have external dependencies on name service servers, networks, and so on. However, this performance comes at the expense of ease of management of the name services, because file management adds overhead to the storage management and introduces more potential for human error. Additionally, local file management must be done per cluster, adding an extra layer of complexity.

Best Practice 8: Using File-Only Mode for Local UNIX Users and Groups

Be sure to evaluate your options at length and make the appropriate decision for your environment and consider file-only mode only if you require a name service environment that needs more than 64k users/groups.

For more information on file-only mode for UNIX users and groups, see TR-4067: NFS Best Pracrice and Implementation Guide.

Table 6) User and group limits in clustered Data ONTAP, scaled/file-only mode.

Data ONTAP 9.1 (Clustered, scaled/file-only mode; per-SVM)
Passwd file size (users): 10MB* Group file size: 25MB* **group and passwd file sizes can be overridden with `-skip-file-size-check` but larger file sizes have not been tested* Users: 400K Groups: 15k Group memberships: 3000k SVMs: 6

5.7 Host Name Resolution Best Practices

The following section covers host name resolution best practices in the clustered Data ONTAP operating system.

Dynamic DNS (DDNS) Support

Clustered Data ONTAP 8.3.1 introduced support for dynamic DNS (DDNS). DDNS is a DNS feature that provides IP addresses and host names dynamically in environments that incur frequent changes to IP addresses, such as in environments that make use of the Dynamic Host Configuration Protocol (DHCP). DDNS allows storage administrators to spend less time administering DNS records and spend more time managing their storage. Data ONTAP dynamically maintains DNS records.

Terminology for DNS can be found in the appendix of this document.

How DDNS Updates

In clustered Data ONTAP, DDNS updates occur on a 30-minute scheduled interval by way of a job running in the background. The job is managed by mgwd and simply calls a BSD-based `nsupdate` command to the node on which it is running.

To see these jobs, run the following command:

```
cluster::> job show -name "DNS Update Job"
                           Owning
Job ID Name                Vserver    Node           State
------ ------------------- ---------- -------------- ----------
5707   DNS Update Job      cluster    node-01        Running
       Description: Dynamic DNS Update
```

Job failures are logged in the corresponding node's mgwd log. The mgwd log can be viewed using the cluster SPI web interface.

DDNS Support Considerations in Clustered Data ONTAP 8.3.1

The following is a list of DDNS feature considerations in clustered Data ONTAP 8.3.1. Many features will be added in future releases. DDNS is configured at the SVM level and is disabled by default.

- IPv4 is supported for DDNS in 8.3.1 and later. ONTAP 9 adds IPv6 support for DDNS.
- DDNS is supported for data SVMs only; there is no support for cluster or admin SVMs.
- Per-LIF DDNS is supported.
- The NAS (CIFS, NFS) protocol is supported only on data LIFs; there is no iSCSI or management LIF support (data protocol = none).
- The ability to change time to live (TTL) is supported; the default is 24 hours.
- DDNS is not supported for use with on-box DNS.
- The default FQDN to which to register is the SVM name. If the SVM is not already an FQDN, then the DNS domain name specified in the DNS configuration of the SVM is appended to the SVM name.
- The first name configured in the DNS client configuration is used:
  - Example: An SVM named `vs1` with a DNS domain name of `domain.com` becomes `vs1.domain.com` in DDNS.
  - Alternatively, storage administrators can configure a custom FQDN through a command-line option.
- When you use a custom FQDN, only NFS traffic uses that FQDN. CIFS traffic uses the FQDN that is assigned to the CIFS server.
- DDNS update triggers on DNS client configuration changes, such as domain or DNS server modifications.
- Manual DDNS updates can be triggered through the CLI.
- DDNS has retry mechanisms in place in case of failure to update records.
- Secure DDNS updates are supported for GSS-TSIG as per RFC-3645:
  - Updates are supported only with Active Directory or Kerberos; a CIFS server is required.
- Statistics for DDNS are available through the counter manager.

DDNS Commands

The following covers commands to be used with DDNS in clustered Data ONTAP.

Commands available at the admin level:

```
cluster::> dns dynamic-update
    modify show
```

Commands available at the advanced level:

```
cluster::*> dns dynamic-update
    modify              prepare-to-downgrade record
    show
```

Example of a `show` command:

```
cluster ::*> dns dynamic-update show
Vserver         Is-Enabled Use-Secure Domain Name              TTL
--------------- ---------- ---------- ------------------------ -------
NAS             false      false      -                        24h
TRUST           false      false      -                        24h
2 entries were displayed.
```


Options available for DDNS configuration:

```
cluster::*> dynamic-update modify -vserver NAS ?
  (vserver services name-service dns dynamic-update modify)
  [[-is-enabled] {true|false}]                    Is Dynamic DNS Update Enabled?
  [ -use-secure {true|false} ]                    Use Secure Dynamic Update?
  [ -domain-name <text> ]                         FQDN to Be Used for DNS Updates
  [ -ttl <[<integer>h][<integer>m][<integer>s]> ]  *Time to Live for DNS Updates
```

Commands (advanced) for viewing DDNS statistics (provided by the counter manager):

```
cluster ::*> statistics start -vserver NAS -object ddns_update
Statistics collection is being started for sample-id: sample_23248

cluster::*> statistics stop -sample-id sample_23248
Statistics collection is being stopped for sample-id: sample_23248

cluster::*> statistics show -object ddns_update

Object: ddns_update
Instance: 5
Start-time: 5/20/2015 12:59:28
End-time: 5/20/2015 13:00:05
Elapsed-time: 37s
Vserver: NAS

    Counter                                                     Value
    -------------------------------- --------------------------------
    bulk_update_fail                                                2
    bulk_update_pass                                                0
    fail                                                            2
    forward_record_sent                                             2
    instance_name                                                   5
    lif_update_fail                                                 0
    lif_update_pass                                                 0
    manual_update_fail                                              0
    manual_update_pass                                              0
    node_name                                                  node01
    pass                                                            0
    process_name                                                    -
    retry_attempts                                                  0
    reverse_record_sent                                             0
    total                                                           2
    vserver_name                                                  NAS
16 entries were displayed.
```

The appendix of this document contains a table of Data ONTAP operating in 7-Mode DDNS commands mapped to clustered Data ONTAP equivalents.

Known DNS Issues

This is a list of some known DNS issues in ONTAP. This list is intended to help avoid scenarios that could cause problems, but is not comprehensive.

- ONTAP 9 introduces a new “bad” DNS caching mechanism. If a DNS server request experiences a timeout, the DNS server gets marked as “bad” for 10 minutes and is not used during this time period. The cache is flushed when DNS configuration is modified using “dns modify.” This timeout value is not modifiable.
- Currently, clustered Data ONTAP supports only the use of DNS or local files for host name mappings. LDAP and NIS are not supported for host names.
- Local file host names for SVMs are supported only in versions of Data ONTAP 8.3 and later.
- If DNS records do not have forward and reverse lookups, lookups for access in exports might fail.
- If DNS records have only an IPv4 (A) or IPv6 (AAAA) record, then a partial failure might occur in versions of clustered Data ONTAP earlier than 8.2.3P3 and 8.3.1.
- If using fully qualified domain names (FQDNs) in host names, netgroups, and so on, RFC-1535 states that it is best to append a dot (.) to the end of the FQDN to denote an “absolute rooted” FQDN. For example: *hostname.netapp.com.* For more information, see the section about rooted vs. nonrooted FQDNs.
- In versions earlier than clustered Data ONTAP 8.2.3P3 and 8.3.1, host name lookups would attempt to find both A and AAAA records for a host name. This could cause partial failures and host name lookup latency, particularly for NFS exports.
- In rare cases, on-box DNS may respond with a time to live (TTL) of 24 hours, particularly during LIF migrations (manual or automatic during storage failover events). In those cases, the DNS server will store the record in negative cache (as in, don’t use this LIF) until the DNS server cache is purged or the expiration time is reached. This issue is covered in bug 1027140 and is resolved in ONTAP versions listed in the public bug report. For information on flushing DNS server caches, please review the associated server’s documentation.

Best Practice 9: General DNS/Host Name Mapping Best Practices

- Use only relevant DNS search domains in DNS configurations for fast DNS lookups.
- Have multiple DNS servers with replicating databases (such as Active Directory DNS) to avoid single points of failure.
- Verify that local and/or the fastest DNS servers are listed first.
- Remove DNS servers undergoing maintenance to avoid timeouts from slow access.
- Verify that all DNS servers contain the same information.
- Make sure that all host names in DNS have IPv4 (A) and IPv6 (AAAA) records, even if IPv4 or IPv6 is not in use in the environment in clustered Data ONTAP versions earlier than 8.2.3P3. This is because clustered Data ONTAP does an IPv6 lookup in earlier releases, even if IPv6 is not present.
- If you use DDNS, make sure that the FQDN specified for updates is the intended FQDN.
- In clustered Data ONTAP versions prior to 8.2.3P3 and 8.3.1, disable IPv6 lookups if IPv6 is not in use in the environment.

Note: IPv6 is disabled by default.

```
cluster::> network options ipv6 show
                      IPv6 Enabled: false
```


5.8 Netgroup Best Practices

The following shows a list of general netgroup best practices for use with any netgroup implementation.

Best Practice 10: General Netgroup Best Practices

- Use the same netgroup configuration across sources.
- Leverage netgroup.byhost mapping when using netgroups with LDAP.
- Leave blank the “domain” and “user” parts of netgroup triples. NetApp supports only host-based netgroup entries (for example, host name).
- Verify that forward and reverse DNS entries exist for host names in netgroups.
- Clean up netgroups periodically to eliminate stale entries to speed up access.

Limits

The following table covers the limits for netgroups in versions of the Data ONTAP 8.3 and later operating system. Clustered Data ONTAP versions earlier than 8.3 did not enforce hard limits, but the limits in Table 7 should be honored in those versions for stability in the cluster.

Table 7) Netgroup limits in clustered Data ONTAP.

Limit	7-Mode	Data ONTAP 8.3.x (Clustered)
Nesting limit for netgroups	1,000	1,000
Limits for file size for -load-from-uri (netgroup, unix-user, unix-group)	N/A	UNIX users: 2.5MB UNIX groups: 1MB Netgroups: 5MB
Single netgroup line limit (local file)	4,096	4,096
Number of NIS servers	No limit	10
Line limit for NIS databases (NIS maps): external NIS servers	1,024	1,024 (8.3 and later; no limit prior to 8.3)

Best Practice 11: NIS Limit Considerations When Upgrading from Clustered Data ONTAP 8.2.x to 8.3.x

Because some limits change between 8.2.x and 8.3.x, it is important to closely review this document for limit differences and make sure that the cluster is in compliance with those limits prior to upgrading to 8.3.x. This helps make sure that no name service–related outages take place after upgrade. The NIS limit of 1,024 characters is a standard limit for most NIS servers.

Multiple DNS Search Domains

In the clustered Data ONTAP operating system, it is possible to configure SVMs to use multiple DNS search domains for host name resolution. However, doing this can cause issues with export policy rules because DNS host name resolution can take a considerable amount of time traversing multiple DNS domains if the first name in the list is not valid for the host.

Best Practice 12: Multiple DNS Search Domains Best Practices

- Use only the search domains applicable to an environment in the configuration. If possible, use only one search domain.
- If multiple search domains are needed, verify that the most commonly used DNS search domain is listed first in the DNS configuration.
- Verify that all DNS servers properly forward to the DNS zones listed in the configuration to avoid failures in host name resolution.
- When possible, use fully qualified domain names (FQDNs) in netgroups, export policies, and so on so that the cluster does not try to resolve a host name with the search domain list.
- Avoid using DNS aliases (such as CNAMEs) in netgroups. CNAMEs do not work well in netgroups because DNS can return an A record instead of a CNAME, and access could be denied, or, at the very least, latency in lookups could be seen. Use only A records if using host names in netgroups. In future releases of clustered Data ONTAP 8.3.x and later, netgroups no longer are expanded to IP addresses, so CNAME records are always denied access.
- Verify that PTR/reverse lookup records exist in DNS. This is a requirement for fully functional export policy rule name resolution. For information about how to do this, see the appendix in this document.

Rooted vs. Nonrooted FQDNs

RFC-1535 states there is a difference in FQDNs depending on how the name is specified. From the RFC:

```
Current Domain Name Server clients are designed to ease the burden of remembering IP dotted quad
addresses.  As such they translate human-readable names into addresses and other resource
records.  Part of the translation process includes understanding and dealing with hostnames that
are not fully qualified domain names (FQDNs).

An absolute "rooted" FQDN is of the format {name}{.} A non "rooted" domain name is of the format
{name}

A domain name may have many parts and typically these include the host, domain, and type.
Example:  foobar.company.com or fooschool.university.edu.
```

In clustered Data ONTAP, rooted FQDNs (FQDNs with the trailing dot) are handled in an efficient manner for scenarios where entries do not exist in DNS servers. When a rooted FQDN is used, the trailing dot is dropped (DNS only), and the cluster looks the FQDN up “as is” and only tries the lookup once. FQDNs are tried “as is” only if configured as rooted FQDNs (with the trailing dot). If the entry has no trailing dot and the FQDN is not found in DNS, the search domains are added to the FQDN, and DNS is queried with this combined name until all search domains are tried or a match is found.

In clustered Data ONTAP versions prior to 8.2.4 and 8.3.2, a nonrooted FQDN attempts to resolve “as is” first, and then the cluster attempts to append the search domains to the end of the FQDN. For example, a nonrooted FQDN might look like this:

```
hostname.netapp.com
```

If the search domains in the DNS configuration include “netapp.com” and others, then the retried lookup would look like this:

```
hostname.netapp.com.netapp.com
```

The cluster then cycles through all search domains, which adds unnecessary latencies to failed records. Using a rooted FQDN prevents this behavior.

In versions of clustered Data ONTAP after 8.2.4 and 8.3.2, the behavior of short names is to try to append the domains to the short name first, then to try the “as is” record. Therefore, it is preferable to leverage the rooted FQDN logic whenever possible.

In the event of a SERVFAIL error or DNS server timeout, the next server is tried.

Netgroups and DHCP/Dynamic DNS

In some scenarios, host names are granted IP address leases from servers running Dynamic Host Configuration Protocol (DHCP) and/or dynamic DNS (DDNS).

What Is DHCP?

DHCP is a protocol that automatically provides IP addresses to clients and servers based on a lease model. This is done both for ease of management and for the ability to work around IP number limitations.

What Is DDNS?

DDNS is a method that allows the name server to automatically update the DNS records for clients and servers. It is often used in conjunction with DHCP to allow automation of host name resolution to help reduce management and administration overhead. Support for DDNS in clustered Data ONTAP was added in 8.3.1. For more information, see the corresponding section in this document.

Why Does This Affect Netgroups?

When a netgroup is created, it’s done by adding a static host name or IP address. Because of the nature of DHCP and DDNS, using IP addresses in netgroups is a nonstarter. Thus, host names must be used, and DNS lookups would be leveraged by clustered Data ONTAP when attempting to resolve netgroup members for export policy rule verification. Clustered Data ONTAP makes heavy use of caching to improve overall NAS performance, so when a netgroup member’s IP address changes through DCHP/DDNS, the cluster does not update with that new information until a cache is refreshed. Cache refresh times are covered in this document and can be adjusted, and caches can be manually flushed.

Note: Manually flushing caches requires the caches to repopulate, which could take a while and/or create a situation in which a flood of requests eats up resources and prevents access.

Which Caches Need to Be Flushed to Clear Out Netgroups?

Three caches contain netgroup information:

- Security daemon (SecD)
- Management gateway (mgwd)
- NAS layer

Most caches can't be flushed at a granular level; they can be flushed only en masse. SecD is the only cache that can be flushed on a per-netgroup basis.

How Netgroups Cache Entries in Clustered Data ONTAP 8.3.x and Later

In clustered Data ONTAP 8.3, netgroup processing moved to a more standard model, as opposed to leveraging just SecD to expand netgroups. However, this did not mean that SecD was taken entirely out of the loop. SecD is still used to connect to name services servers, as well as cache netgroups that have been expanded. In particular, if using netgroups without leveraging netgroup.byhost functionality, there are multiple caches to consider, as well as multiple cache ages.

For instance, the netgroup cache found in mgwd (using `vserver netgroup cache` commands) refreshes after an hour. What this means is that the netgroup cache contacts SecD to check and see if any changes have been made to the SecD cache if netgroups are hosted by LDAP.

However, the SecD cache refreshes after 24 hours, which means, effectively, that the netgroup cache in mgwd does not refresh for 24 hours when considering netgroups that have added or removed members.

A key indication that a netgroup cache is using the SecD cache is in the `vserver netgroup cache show` command. Notice in the following example that the "hosts in netgroup" has an entry, but no addresses have been resolved.

```
cluster::*> export-policy netgroup cache show -vserver SVM -netgroup testnetgroup

                                  Vserver: SVM
                      Name of the Netgroup: testnetgroup
                                 Record ID: 3
                    State of the Cache Entry: ready
      Total Number of Hosts in the Netgroup: 1
            Number of IP Addresses Resolved: 0
                  Number of Hosts Not Found: 0
                         Expansion Duration: 0:0:3
                      Is Entry Refreshing?: false
                         Next Refresh Time: Tue Jun 28 17:25:06 2016
                Time Removed from the Queue: Tue Jun 28 16:55:06 2016
Are Netgroup-by-host Based Lookups Working?: false
              Number of Cached IP Addresses: 0
              Number of Member IP Addresses: -
             Number of Pending IP Addresses: -
```

The netgroup cache in mgwd keeps refreshing every hour, but contacts SecD to verify if it contains the netgroup members in cache to avoid having to refer to external servers. Only when the SecD cache flushes the entry does the cache truly refresh.

The SecD cache entries can be verified using diag privilege-level commands to view how many active cache entries exist, as well as dumping the existing cache entries to the SecD log file located in `/mroot/etc/mlog` of the specified node.

To view the cache entries:

```
::*> diag secd cache show-config -node node3 -cache-name ldap-netgroupname-to-members
Current Entries: 1
    Max Entries: 512
Entry Lifetime: 86400
```


To dump the cache entries to the log file:

```
::*> diag secd cache dump -node node3 -vserver SVM -cache-name ldap-netgroupname-to-members
The cache was successfully dumped to the SecD log file; see the file secd.log in the standard log
directory
```

From there, review the secd.log file:

```
00000a6f.000f7de0 0185e614 Wed Jun 29 2016 09:11:58 -04:00 [kern_secd:info:88335] .--------------
------------------------------------------------------------.
00000a6f.000f7de1 0185e614 Wed Jun 29 2016 09:11:58 -04:00 [kern_secd:info:88335]
|           Dumping cache 'LdapNetgroupNameToMembers' for vserver 7            |
00000a6f.000f7de2 0185e614 Wed Jun 29 2016 09:11:58 -04:00 [kern_secd:info:88335] |--------------
------------------------------------------------------------'
00000a6f.000f7de3 0185e614 Wed Jun 29 2016 09:11:58 -04:00 [kern_secd:info:88335]  VserverId 7
00000a6f.000f7de4 0185e614 Wed Jun 29 2016 09:11:58 -04:00 [kern_secd:info:88335]  NetGroupName
testnetgroup
00000a6f.000f7de5 0185e614 Wed Jun 29 2016 09:11:58 -04:00 [kern_secd:info:88335]  Members:
00000a6f.000f7de6 0185e614 Wed Jun 29 2016 09:11:58 -04:00 [kern_secd:info:88335] |--------------
------------------------------------------------------------.
00000a6f.000f7de7 0185e614 Wed Jun 29 2016 09:11:58 -04:00 [kern_secd:info:88335]
|            End of cache 'LdapNetgroupNameToMembers' for vserver 7            |
00000a6f.000f7de8 0185e614 Wed Jun 29 2016 09:11:58 -04:00 [kern_secd:info:88335] '--------------
------------------------------------------------------------'
```

Note: In the preceding example, the cache showed no members. However, the netgroup had recently been populated with members, so the cache was stale at that point.

If a netgroup has been recently modified (as in members added or removed) and the desired access has not been seen, the netgroup cache can be flushed en masse for the SVM with the following command:

```
::> export-policy cache flush -vserver SVM -cache netgroup
```

Clearing Out All Netgroup Cache Entries

The following steps show how to clear out all netgroup cache entries manually. This should be done only when needed, such as when loading a new netgroup file from URI.

Mgwd caches:

Netgroup caches in mgwd are flushed as a whole (in clustered Data ONTAP 8.2.3 and later):

```
cluster::> export-policy cache flush -vserver <vserver> -cache netgroup
```

Note: This flushes all entries in netgroup and SecD caches. Use this command only when necessary.

Note: This command must be issued from the node that owns the cache by logging in to a management LIF local to that node.

In addition to the preceding, there are commands at the diag privilege (8.3.1 and later) that allow control of the netgroup cache attributes in mgwd, as well as the ability to manage the host to IP cache. This command set allow allows storage administrators to adjust the journal (logging) level for exports to assist in troubleshooting efforts.

```
cluster::*> diag exports mgwd ?
  host-to-ip-cache>           *The host-to-ip-cache directory
  journal>                    *Manage NFS exports journal settings
  netgroup-cache>             *The netgroup-cache directory
```


SecD caches:

To clear out the SecD caches (all clustered Data ONTAP releases):

```
cluster::> set diag

cluster::*> diag secd cache clear -node <node> -vserver <vserver> -cache-name netgroup-ip
-entry <netgroup>

cluster::*> diag secd cache clear -node <node> -vserver <vserver> -cache-name netgroup-host
-entry <netgroup>
```

Note: If you used the command to flush mgwd caches, then this step is unnecessary, because the previous command clears mgwd and SecD caches.

NAS layer caches:

The NAS layer contains positive and negative cache entries for hosts in export policies. These caches are flushed on a per-node basis and can be flushed on a per-host basis.

```
cluster::> set diag

cluster::*> diag exports nblade access-cache flush -node <node> -policy <export-policy> -vserver
<vserver> -address <hostIP>
```

To check hosts for export policy access, use the following command (available in 8.2.3 and later):

```
cluster::*> vserver export-policy check-access -vserver SVM -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
```

You can also modify the NFS export policy access cache attributes in the NAS layer that control the refresh intervals of access caches. To see the default values, you have to go into diag privilege.

```
cluster::> set diag
cluster ::*> diag exports nblade access-cache attributes show

         Refresh Period for Positive Entries  (secs): 3600
   Max Refresh Interval for Positive Entries  (secs): 1800
   Min Refresh Interval for Positive Entries (msecs): 180
         Refresh Period for Negative Entries  (secs): 3600
   Max Refresh Interval for Negative Entries  (secs): 1800
   Min Refresh Interval for Negative Entries (msecs): 1800
                TTL for Entries with Failure  (secs): 5
                          Harvest Timeout  (secs): 86400
                  Max Outstanding RPCs to Mgwd: 64
```

Note: For more information about the values, use "`man diag exports nblade access-cache attributes modify`."

To modify these refresh intervals:

```
cluster ::*> man diag exports nblade access-cache attributes modify ?
  [[-refresh-period-positive] {300..86400}]        *Refresh Period for Positive Entries(secs)
  [ -max-refresh-interval-positive {150..43200} ]  *Max Refresh Interval for Positive
Entries(secs)
  [ -min-refresh-interval-positive {1..10000} ]    *Min Refresh Interval for Positive
Entries(msecs)
  [ -ttl-failure-time {1..60} ]                    *TTL for Entries with Failure(secs)
  [ -max-outstanding-calls {64..1024} ]            *Max Outstanding RPCs to Mgwd
  [ -refresh-period-negative {60..86400} ]         *Refresh Period for Negative Entries(secs)
  [ -max-refresh-interval-negative {30..43200} ]   *Max Refresh Interval for Negative
Entries(secs)
  [ -min-refresh-interval-negative {1..10000} ]    *Min Refresh Interval for Negative
Entries(msecs)
  [ -harvest-timeout {60..2592000} ]               *Harvest Timeout(secs)
```

How netgroup.byhost Works

The following describes how netgroup.byhost operations work in the clustered Data ONTAP operating system at a high level.

1. First, a mount request arrives from an IP address.
2. A reverse lookup is performed by using the SVM's DNS configuration to retrieve the FQDN.
   - A PTR record is highly recommended for all hosts that use NAS. PTR records enable CIFS to leverage Kerberos and allow export policies and rules to be resolved properly and efficiently.
3. After the FQDN (for example, *hostname.domainname.com*) is retrieved, the netgroup.byhost database (LDAP or NIS; local files are not supported for netgroup.byhost yet) is searched with the following, in order:
   - *hostname.domainname.com.**
   - *hostname.** (if the NFS setting `netgroup-dns-domain-search` is enabled and the DNS domain search is listed properly in the DNS configuration)
   - IP address
     - If reverse lookup fails, we go directly to this step
   - Wildcard search *.* (last resort)
4. If the host cannot be found in the netgroup.byhost map, the client is not granted access. Starting in clustered Data ONTAP 8.2.2P2 (and subsequent 8.2.x releases), host name resolution leveraging DNS tries the data SVM first and then falls back to the cluster name server if the data SVM DNS server cannot resolve the host name. In clustered Data ONTAP 8.3 and later, only the data SVM is used for DNS lookups. As a result, make sure that all host names specified in netgroups and/or export policy rules can be resolved (both forward and reverse) in the data SVM DNS server to avoid latency in lookups and potential failures if the cluster SVM does not have DNS specified and/or cannot resolve to the same DNS servers as the data SVM.

Note: For more information about netgroup.byhost, see the section in this document about the subject.

Local Files

This section covers local files for use as a name service. In the clustered Data ONTAP operating system, local files are entries in the replicated database (such as `unix-users`, `unix-groups`, and so on) that replace flat files seen in 7-Mode (such as `/etc/passwd`, `/etc/group`, and so on), which allows a cluster to have current information about all member nodes.

Line Length Limitations

Netgroup files in the clustered Data ONTAP operating system have limitations for line lengths and the number of nested netgroups. This information is covered in the limits section of the netgroup best practices.

Typo Handling

When using the `-load-from-uri` functionality in the clustered Data ONTAP operating system to import netgroups into the cluster locally, great care must be taken so that no typos exist in the file to prevent access issues. Starting in the clustered Data ONTAP 8.2.3 version, the system checks the file for you prior to uploading and warns about potential typo errors. Typos in netgroup files can cause access issues, such as denying access to clients that should have access. This can affect local and remote netgroup host resolution. Running the Recommended Data ONTAP Version for Name Services can help avoid scenarios like these.

Loading Netgroups from URI

When loading netgroups from URI to a local file on the cluster, the netgroup caches are not flushed out automatically. As a result, if a host name or IP is already in the cache (positive or negative) and the netgroup file is changed to reflect that particular host name or IP, the change does not take effect until the cache is manually flushed or refreshes on its own. Keep in mind that manually flushing caches requires the caches to repopulate, which could take a while and/or create a situation in which a flood of requests eats up resources and prevents access. Therefore, it is best to make this sort of change in a maintenance window. For more information about which caches store netgroup information, see the cache tunables section of this document. Remember that there are file size limits for loading files from URI.

Local File Sync Issues

In rare cases, local file entries might be out of sync with entries in the cluster's RDB. For instance, if a netgroup file was loaded recently and something happened during the load of the entries, then the netgroups in the cluster may not properly represent what was in the local file that was loaded.

Each time a file is loaded, it gets assigned a file version. Each time RDB is updated, it gets assigned the same version number as the file. To check if the versions are in sync, use the following command at diag privilege:

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


To rectify file version mismatches, use the following command in diag privilege:

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

Netgroups in External Name Services

The following table shows the recommended number of hosts in a netgroup correlated with the number of SVMs. These recommended limits are primarily in place for versions of clustered Data ONTAP 8.2.x and earlier, because they improve performance and prevent access issues. These issues are not present in versions of Data ONTAP 8.3 and later, which are the recommended versions for customers wanting to use larger netgroups.

Note: If a netgroup name is malformed and no other name service exists with the netgroup entry, then access may be denied to clients. Be sure to check your netgroups to make sure that there are no issues with the netgroup names or members.

Table 8) Recommended maximum netgroup sizes.

Number of SVMs	Recommended Maximum Number of Hosts in Netgroup
3 to 5	100,000
5 to 50	10,000
50 and above	1,000–5,000

About NIS Objects and Attributes in LDAP

NIS object types in LDAP are determined by way of the `objectClass` attribute. The `objectClass` attribute set on an object determines how clustered Data ONTAP and other LDAP clients query LDAP for netgroup-related objects. For netgroups, the `nisNetgroup` object class is used by default.

Table 9) Object class types for NIS objects in Active Directory.

Object Class	Used For	NIS Attributes Used
nisMap	NIS maps	nisMapName
nisNetgroup	Netgroups	nisMapName nisNetgroupTriple
nisObject	Netgroups Netgroup.byhost entries	nisMapEntry nisMapName

NIS Object Terminology

The following section describes terminology that defines specific aspects of NIS objects.

Table 5) NIS object terminology.

Term	Definition
NIS map	NIS maps were designed to centralize and replace common files found in the /etc directory of Linux and UNIX clients. Clustered Data ONTAP currently supports the following NIS map types: passwd.byname and passwd.byuid group.byname and group.bygid netgroup netgroup.byhost (as of 8.2.3) Host name resolution in NIS is not currently supported. For more information about NIS maps, see http://docs.oracle.com/cd/E19683-01/817-4843/anis1-24268/index.html.
Netgroup	A netgroup is a set of (host,user,domain) triples (also known as tuples) used for permission and export access checking. Clustered Data ONTAP currently supports only hosts in netgroup entries. For more information about netgroups, see http://linux.die.net/man/5/netgroup and http://www.freebsd.org/cgi/man.cgi?query=netgroup&sektion=5.
Triple	A netgroup triple (tuple) refers to the series of entries in a netgroup file consisting of (host,user,domain). A valid triple used in clustered Data ONTAP consists of (host,,). Host names used in netgroup triples require DNS resolution in clustered Data ONTAP. For best results in netgroup translation, see the name services best practices in TR-4067.
Netgroup.byhost	Netgroup.byhost entries are used to speed up netgroup lookups by querying the name service for the group membership by host rather than querying the entire netgroup. For netgroups with many entries, this can reduce lookup time drastically and improve performance.

Netgroup.byhost

As mentioned previously, netgroup.byhost entries are used to speed up netgroup lookups by querying NIS and LDAP for the group membership by host rather than querying the entire netgroup. The following section covers netgroup.byhost in greater detail.

Netgroup.byhost Support

Netgroup.byhost entries can vastly speed up netgroup entry lookup by allowing the cluster to avoid needing to query every entry in a netgroup for access and instead allowing the name server to efficiently look up the single host. In large environments with netgroups that have many entries, this can drastically speed up the time for lookups and avoid access issues caused by timeouts on queries. Support for netgroup.byhost was added to versions of clustered Data ONTAP 8.2.3 and later.

Note: Netgroup.byhost is enabled by default for NIS servers. No configuration change is needed. Netgroup.byhost in LDAP may require configuration changes, depending on the existing schema.

Best Practice 13: Netgroup.byhost Considerations

When using netgroup.byhost, the following must be in place to achieve the desired access results for hosts:

- Forward and reverse DNS records for host names
- Host triple entry in netgroup file (for example, host,,)
- Netgroup specification for the host's netgroup.byhost entry

Note: NetApp highly recommends netgroup.byhost functionality for large environments with large netgroups. "Large netgroups" in this case are defined in Table 8) Recommended maximum netgroup sizes.

Note: The netgroup.byhost and netgroup entries *must* be in sync to allow access to work properly.

Enabling netgroup.byhost Support for LDAP in the Clustered Data ONTAP Operating System

Netgroup.byhost support is not enabled by default in the clustered Data ONTAP operating system. Several options in the LDAP client configuration would need to be modified:

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

DN and scope are used to specify the filters desired for netgroup.byhost functionality. For more information, see the administration guides for your release of clustered Data ONTAP. Keep in mind that support for this feature applies only to versions of clustered Data ONTAP 8.2.3 and later. For examples of this, see TR-4073: Secure Unified Authentication.

NIS Netgroup Strict (nfs.netgroup.strict)

In 7-Mode, the option `nfs.netgroup.strict` allowed the ability to control whether or not a netgroup entry required the @ sign to make sure that Data ONTAP recognized the netgroup as a netgroup.

Best Practice 14: Netgroup Definition in Export Policy Rules

In clustered Data ONTAP, there currently is no equivalent to this option. All netgroups in export policy rules must be designated with the @ sign to be recognized as netgroups.

LDAP Netgroups

It is possible to leverage netgroup functionality in LDAP as opposed to NIS. Netgroups give storage administrators control of access to a series of hosts using a group, rather than needing to create a number of different rules per host. Using LDAP as an NIS server is covered in RFC-2307.

LDAP Netgroup Optimization

LDAP servers can be optimized to allow faster lookups from storage systems running the clustered Data ONTAP operating system. The following covers some general best practices that can be used. For specific best practices or steps to implement these best practices, contact the LDAP vendor.

Best Practice 15: LDAP Optimization

- Use LDAP servers that have fast WAN or LAN connections.
- Load balance LDAP servers to alleviate CPU, memory, and network pressure.
- Verify that LDAP servers have service records (SRVs) in DNS. Microsoft Active Directory does this by default for all LDAP servers that are also domain controllers.
- When the LDAP server database is extremely large, employ DN filtering through the base, user, group, and netgroup DN settings. Keep in mind that large is a subjective term and depends on factors such as network, LDAP server load, number of objects, and so on.
  - Searching LDAP at a lower level of the folder structure speeds up queries.
  - If possible, try reducing the number of objects by deleting unused users, groups, and so on.
- If attempting to use multiple domains in an Active Directory forest for querying UNIX objects in LDAP, consider using global catalog LDAP searches. LDAP referrals are currently not supported in Data ONTAP.
- Verify that all LDAP servers contain accurate and complete information in each object's schema attributes. For instance, every user should have a GID number assigned.
- Verify that all LDAP servers have a consistent copy of the schema. Active Directory does this by default on a 15-minute replication interval.
- Monitor the server's CPU, memory usage, and so on so that the server is not overworked.
- Remove slow or misbehaving LDAP servers from the client configuration as soon as possible to correct any issues.
- Always remove LDAP servers undergoing maintenance from the configuration.

Note: For details about LDAP referrals, global catalog searches, and other LDAP configurations, see TR-4073: Secure Unified Authentication.

Clustered Data ONTAP Operating System Interaction with Active Directory LDAP for Netgroups

In the LDAP client schemas provided in the clustered Data ONTAP operating system (for example, AD-IDMU, RFC-2307, and so on), the following attributes control lookups for netgroups and their members:

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

Starting in versions of clustered Data ONTAP 8.2.3, the following attributes are provided for netgroup.byhost support:

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

LDAP client schemas can be modified to change the default attributes only if the default schemas are copied into new schemas. Default schemas in clustered Data ONTAP are read only. For more information about default schemas, see the section in this document about LDAP schemas.

When Windows Server for NIS is installed in Active Directory, the container `DefaultMigrationContainer30` is created. This container is the default container to which NIS netgroups are migrated by default. To use a different container, create a new OU or container to host this information and specify it in your migrations.

The Active Directory schema has the following schema attributes added by default in Windows 2008 and later (default attributes used by clustered Data ONTAP are in bold):

```
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
```

Creating Netgroups in AD-Based LDAP

Active Directory netgroups can be controlled by using the utilities nis2ad and nismap or by using GUI tools such as ADSI Edit.

Nis2ad allows migration of existing maps from NIS to AD or the ability to create NIS maps from a local file. This utility is included in the identity management for UNIX feature in Windows 2008 and later. However, it generally is not needed unless you are creating new NIS maps outside of the default "netgroup" NIS map created by IDMU.

The nismap command allows granular management of NIS maps in addition to what nis2ad provides.

When identity management for UNIX is installed with server for NIS, a Windows MMC is created to view and manage server for NIS. The server for NIS MMC cannot be used to create or delete NIS maps, however. For examples, see TR-4073: Secure Unified Authentication.

Third-Party Schema Extensions

Active Directory provides an LDAP back end for use with directory services in Microsoft Windows. It also provides additional schema extensions to allow Active Directory to act as a UNIX identity management server. There are free schema extensions, such as services for UNIX (Windows 2003 and earlier) and identity management for UNIX (Windows 2003R2 and later), that allow LDAP clients to bind and search for UNIX attributes. Clustered Data ONTAP provides default read-only schemas for AD-SFU, AD-IDMU, and RFC-2307 schema types to help make the configuration simpler.

In addition to Microsoft Active Directory's integrated tools, there are third-party tools, such as Centrify's Vintela application suite, that extend the schema and provide a GUI for management. Data ONTAP supports any and all schema extensions that comply with RFC-2307 standards. To use third-party schema extensions with Data ONTAP, consult the vendor's product documentation on which schema attributes are leveraged and modify the client schema in Data ONTAP accordingly. TR-4073: Secure Unified Authentication covers how to create custom LDAP schemas for use with third-party vendors. The same general best practices for LDAP servers apply regardless of who is providing the schema.

Displaying Netgroup Caches

In addition to being able to flush various caches, Data ONTAP 8.3 and later versions offer the capability to display netgroup caches as well as check netgroup membership.

To view netgroup caches:

```
cluster ::> vserver export-policy netgroup cache show ?
  [ -instance | -fields <fieldname>, ... ]
    -vserver <vserver name>                                  Vserver
  [[-netgroup] <text>]                                       Name of the Netgroup
  [ -record-id <integer> ]                                   Record ID
  [ -is-getting-hosts {true|false} ]                         Hosts Being Retrieved
  [ -is-ready {true|false} ]                                 Is Ready to Be Used
  [ -is-notfound {true|false} ]                              Is Not Found
  [ -is-pending-notfound {true|false} ]                      Is Pending Not Found
  [ -is-wildcard {true|false} ]                              Is Wildcard
  [ -is-pending-wildcard {true|false} ]                      Is Pending Wildcard
  [ -is-abandoned {true|false} ]                             Is Abandoned
  [ -member-count <integer> ]                                Count of Members
  [ -hosts-count <integer> ]                                 Count of Hosts
  [ -pending-addresses-count <integer> ]                     Count of Addresses Pending
  [ -pending-hosts-dropped <integer> ]                       Count of Hosts Not Found in Pending
  [ -retries-on-queue <integer> ]                            Count of Times Retried in the Queue
  [ -expanded-duration <[[<hours>:]<minutes>:]<seconds>> ]   How Long it Took to Expand Netgroup
  [ -pending-hosts-resolved <integer> ]                      Count of Hosts Already Resolved
```

To check netgroup membership:

```
cluster::> vserver export-policy netgroup check-membership ?
    -vserver <vserver name>   Vserver
   [-netgroup] <text>         Name of the Netgroup
   [-client-ip] <IP Address>  Client Address
```


To view a queue of unresolved netgroups:

```
cluster::> vserver export-policy netgroup queue show ?
  [ -instance | -fields <fieldname>, ... ]
  [ -vserver <vserver name> ]                  Vserver
  [ -netgroup <text> ]                         Name of the Netgroup
  [ -queue-state {active|register|retry} ]     State of Entry in the Queue
  [ -record-id <integer> ]                     Record ID
  [ -is-getting-hosts {true|false} ]           Hosts Being Retrieved
  [ -is-ready {true|false} ]                   Is Ready to Be Used
  [ -is-notfound {true|false} ]                Is Not Found
  [ -is-pending-notfound {true|false} ]        Is Pending Not Found
  [ -is-wildcard {true|false} ]                Is Wildcard
  [ -is-pending-wildcard {true|false} ]        Is Pending Wildcard
  [ -is-abandoned {true|false} ]               Is Abandoned
  [ -member-count <integer> ]                  Count of Members
  [ -hosts-count <integer> ]                   Count of Hosts
  [ -pending-addresses-count <integer> ]       Count of Addresses Pending
  [ -pending-hosts-dropped <integer> ]         Count of Hosts Not Found in Pending
  [ -retries-on-queue <integer> ]              Count of Times Retried in the Queue
  [ -age <[[<hours>:]<minutes>:]<seconds>> ]   Age of Entry in the Queue
  [ -pending-hosts-resolved <integer> ]        Count of Hosts Already Resolved in Pending
```

General Netgroup Best Practices for External Servers

The following are general best practices for use with netgroups hosted on external servers.

Best Practice 16: General Netgroup Best Practices for External Servers (Such as LDAP or NIS)

- Use multiple name service servers for redundancy.
- Verify that servers in the configuration contain the same information.
- Remove servers from the list when undergoing maintenance.
- Enable LDAP netgroup.byhost mappings when possible (available in 8.2.3 and later).
- Verify that forward and reverse (PTR) DNS records exist for all hosts in netgroups. This is a necessary requirement for fully functional host name/export policy name resolution. For information about how to do this, see the appendix in this document.
- When loading netgroups from a file, be prepared to either wait for the cache to refresh organically or manually flush caches.
- When using DHCP and/or DDNS, netgroup caches might need to be manually flushed to reflect accurate host-ip information in netgroup caches.
- To secure LDAP binds and searches, consider using LDAP signing and sealing, which is available as of ONTAP 9.0. For more information, see TR-4073: Secure Unified Authentication.

5.9 Export Policy and Rule Best Practices

Preupgrade Considerations

Starting in clustered Data ONTAP 8.2.2P2, changes were made to the way export policy rules handled unresolvable host names. Therefore, it is imperative to make sure that all host names in export policy rules and netgroups can be resolved in DNS. If host names cannot be resolved from the SVM, then mount failures or hangs could occur after upgrading to clustered Data ONTAP 8.2.2P2 and later. The following section covers how to test DNS lookups in clustered Data ONTAP 8.2.x and earlier.

Best Practice 17: Export Policy and Rule Best Practices

- If using host names in export policy rules or in netgroups, make sure that all host names resolve in DNS (forward and reverse lookup).
- Avoid using short names. Fully qualified domain names (FQDNs) are much faster to resolve and result in better export policy rule evaluation performance. In some instances, short names that do not resolve can cause outages for other export rules, because a failure prevents evaluation of other rules in Data ONTAP versions later than 8.2.3.
- Never use CNAMEs. At best, export evaluation is slow. At worst, access is denied to hosts that should be allowed access.
- Avoid making frequent changes to export policy rules if possible. Each change requires the cache to be repopulated, which means that the cluster needs to spend time and resources on that function. This can add latency to access requests.
- If using large netgroups or a large number of host names in export policy rules (that is, thousands of hosts), be sure that all hosts resolve properly in DNS and that FQDNs or IP addresses are used.
- If netgroups/host names see a large amount of churn (that is, things change often), then make sure the appropriate caches are set accordingly to reflect that. For more information, see the section about cache tunables in this document.

Predeployment

Prior to rolling out an export policy and rule set, be sure to check all hosts and netgroups being used so that they have proper name resolution in DNS and the netgroup lookups work properly.

Versions of Clustered Data ONTAP 8.2.x and Earlier

In versions earlier than the Data ONTAP 8.3 operating system, the `diag secd` command set (diag privilege) could be used to query netgroups for host name resolution and membership information.

To test name resolution:

```
cluster::*> diag secd dns
    forward-lookup srv-lookup
```

Example:

```
cluster::*> diag secd dns forward-lookup -node node1 -vserver SVM -hostname centos65
10.228.225.140
```

Note: Keep in mind that in versions earlier than Data ONTAP 8.3, local host names are not supported per SVM. DNS must be used for host name resolution.

Also, test pings to see if they succeed in returning an IP address:

```
cluster::> net ping -lif [data_lif] -vserver [SVM]  -destination [hostname] -show-detail true
```

If a name cannot resolve, the cluster returns an error:

```
ping: cannot resolve hostname.netapp.com: Host name lookup failure
```

Querying netgroups:

```
cluster82::*> diag secd netgroup
    cache-locks             check-membership        query-netgroup-by-host
    show-host-addresses     show-hosts              show-triples
```

Example (netgroup.byhost):

```
cluster82::*> diag secd netgroup query-netgroup-by-host -node node1 -vserver SVM -netgroup-name
netgroup2 -address 10.228.225.140
Host IP  : 10.228.225.140
Hostname : centos65.domain.netapp.com
Netgroup : netgroup2
Member   : yes
```

Example (regular netgroup):

```
cluster82::*> diag secd netgroup show-hosts -node node1 -vserver SVM -netgroup-name testnetgroup
centos65
sles11
suse11
```

The Data ONTAP 8.3.x Operating System

The Data ONTAP 8.3 operating system introduced the command `getXXbyYY` (advanced privilege) for use with name service lookups. The `diag secd` commands used for netgroup resolution were deprecated and are no longer supported. See the section detailing changes between clustered Data ONTAP 8.2.x and 8.3 operating systems for more information.

Example of `diag secd` command that is no longer supported in 8.3:

```
cluster83::*> diag secd netgroup show-hosts -node node1 -vserver SVM -netgroup-name netgroup2

This command is not supported in this release.
```

Clustered Data ONTAP uses standard libc functions for name services in versions 8.3 and later. The following getXXbyYY standard calls are available at the cluster shell of clustered Data ONTAP.

Table 6) List of supported getXXbyYY functions in clustered Data ONTAP 8.3 and later.

Function	What It Does
Getaddrinfo	Gets the IP address information by using the host name.
Getgrbygid	Gets the group members by using the group identifier, or GID.
Getgrbyname	Gets the group members by using the group name.
Getgrlist	Gets the group list by using the user name.
Gethostbyaddr	Gets the host information from the IP address.
Gethostbyname	Gets the IP address information from the host name.
Getnameinfo	Gets the name information by using the IP address.
Getpwbyname	Gets the password entry by using the user name.
Getpwbyuid	Gets the password entry by using the user identifier, or UID.
Netgrp	Checks if a client is part of a netgroup.
Netgrpbyhost	Checks if a client is part of a netgroup using netgroup-by-host query.

Querying All Members of a Netgroup

Prior to clustered Data ONTAP 8.3, it was possible to query a netgroup and print all members to the screen from the cluster shell. This was done by using the following diag secd netgroup commands, available at diag privilege level:

```
diag secd netgroup show-triples
diag secd netgroup show-hosts
diag secd netgroup show-host-addresses
```

Because netgroups and DNS have been moved out of SecD, these commands have been deprecated. There currently is no way to query for all netgroup members (hosts, triples, or IP addresses) from the cluster shell. Workarounds include querying netgroups outside of the cluster or contacting NetApp Technical Support and referencing bug 880614.

Example of netgroup lookup by using getXXbyYY:

```
cluster83::*> getxxbyyy netgrpbyhost -node node1 -vserver SVM -netgroup netgroup2 -clientIP
10.228.225.140
  (vserver services name-service getxxbyyy netgrpbyhost)
Netgroup.byhost not enabled in all the configured sources
Hostname resolved to: centos65.domain.netapp.com
```

Example of user lookup by using getXXbyYY:

```
cluster83::*> getxxbyyy getpwbyuid -node node1 -vserver SVM -userID 1107
  (vserver services name-service getxxbyyy getpwbyuid)
pw_name: ldapuser2
pw_passwd:
pw_uid: 1107
pw_gid: 10005
pw_gecos: ldapuser
pw_dir: /home/CDOT/ldapuser
pw_shell: /bin/sh
```

Troubleshooting Using getXXbyYY

The `getXXbyYY` command also has a flag that allows an admin to show what name service source is being used during a request. This is useful to troubleshoot issues.

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

In addition, there is a hidden flag that provides more granularity of the name services used called `show-granular-err`.

Example of user lookup by using getXXbyYY with troubleshooting flags provided:

```
cluster83::*> getxxbyyy getpwbyname -node node1 -vserver NAS -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: /home/root
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
```

In the following examples, we can see what name service sources failed during a lookup.

Example of failed user and group lookup using getXXbyYY with troubleshooting flags provided:

```
cluster83::*> getxxbyyy getgrbyname -node node1 -vserver NAS -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


cluster83::*> getxxbyyy getpwbyname -node node1 -vserver NAS -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
```


Postdeployment

After deploying export policies and rules, be sure to check client access by using the new command `export-policy check-access`, available in versions of clustered Data ONTAP 8.2.3 and later.

Export Policy Rule Access Verification (exportfs -c)

The ability to check access to specific clients was added to clustered Data ONTAP versions starting with 8.2.3. This functionality in 7-Mode was known as `exportfs -c`. In the clustered Data ONTAP operating system, the command is now `vserver export-policy check-access`:

```
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.
```

Example of export-policy check-access:

```
cluster::*> vserver export-policy check-access -vserver SVM -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.
```

5.10 Cache Tunables

The following section covers the refresh times and tunables for caches in clustered Data ONTAP.

Caches for Name Services

The clustered Data ONTAP operating system provides a number of caches for name services to help improve performance. However, these caches need to be refreshed from time to time so that information is correct and current. For example, if a user's credentials are cached and group membership is changed, the cluster needs to retrieve the new group membership so that appropriate access is granted or denied.

Caches for name services live in a number of places in the clustered Data ONTAP operating system. The following tables show different caches and their time to live (TTL), as well as the recommended best practice for large NAS environments.

Note: Every environment is different. If there is a large amount of churn in an environment (for example, netgroups changing often), then cache ages need to be refreshed at a more normal interval. NetApp recommends testing for all environments to enable the desired results.

Mgwd Caches

Mgwd caches information about exports and netgroup host name resolution. The only caches that are configurable in mgwd currently are for netgroups. These caches are managed at the diag privilege level with the `diag exports mgwd` command. The recommended refresh time for the netgroup cache of 12 hours is set because netgroups do not generally see a lot of churn. However, if netgroups in an environment do change frequently, then leave the values as the defaults.

Table 7) Mgwd cache ages.

Cache Name	Default Refresh Period (in Seconds)	Recommended Refresh Period (in Seconds)
Netgroup cache	3,600	43,200
Host to IP cache	1,800	43,200

NAS Layer Caches

The following describes the layers used at the NAS layer in the clustered Data ONTAP operating system. For more information about the NAS layer, see the corresponding section in this document. Cache changes are made at the diag privilege level. With any diag command, use caution.

Export Caches

Export caches are managed with `diag exports nblade access-cache attributes` commands.

```
DESCRIPTION

The diag exports nblade access-cache attributes modify command is used to modify various refresh
periods related to the access cache in the kernel. Modification to these values from any node
will update the refresh periods on all the nodes in the cluster. The modified values also persist
across reboots. See diag exports nblade access-cache attributes show for a description of what
the refresh periods mean.

When the refresh time is modified, by default the max refresh will set to half of the refresh
time and the min refresh will be set to (refresh time/20000). The 20000 number is so that a
maximum of 20000 clients can be refreshed in one refresh interval.
```

The following caches affect export policies and rules:

- **Access refresh.** This is the amount of time a positive or negative export access attempt is kept in cache.
- **Maximum refresh time.** This specifies the maximum refresh period at which refreshes are sent to the management gateway (mgwd).
- **Minimum refresh time.** This specifies the minimum refresh period at which refreshes are sent to the management gateway (mgwd).
- **TTL failure time.** This specifies the refresh period at which the access cache entries that reach a transient failure are refreshed.
- **Maximum outstanding calls.** This is the maximum number of outstanding access calls waiting in queue.

Export Policy Rule Caching

In 7-Mode, export policy rules were cached based on the following NFS options:

```
nfs.export.harvest.timeout
nfs.export.neg.timeout
nfs.export.pos.timeout
nfs.export.resolve.timeout
```

These options do not currently exist in the clustered Data ONTAP operating system. In addition, 7-Mode allowed `exportfs` commands to be used to clear export caches. In the clustered Data ONTAP operating system, `exportfs` currently does not exist, but caches are flushed each time an export policy rule is updated. The cache is stored at the NAS layer and refreshes every hour if no export rule changes are made. The management gateway in the clustered Data ONTAP operating system caches host name to IP resolution (1 minute TTL) and resolved netgroups (1 hour TTL). Versions of Data ONTAP 8.3 and later introduced a command to manually flush the export policy caches as well as other related caches.

Flushing Export Policy Caches

In versions earlier than Data ONTAP 8.3.1 and 8.2.3, export policy caches could be flushed only by making changes to export policy rules. Now, the clustered Data ONTAP operating system offers a set of commands to allow manual flushing of export caches without needing to change existing policies. This command set is similar to `exportfs -f`, available in Data ONTAP operating in 7-Mode, and is done on a per-node, per-SVM basis. However, only the access cache can be flushed from any node in the cluster. The other caches must be flushed from a local management LIF.

```
cluster::> vserver export-policy cache flush -vserver SVM -node node1 -cache
    all       access    host      id        name      netgroup  showmount
```

Note: Never flush caches when name service servers are unavailable or experiencing higher than normal latencies. Doing so could cause client disruptions as the caches attempt to repopulate. For information about how to evaluate name service response times, see the section in this document regarding name service statistics.

Following is a table of the different caches and their refresh times.

Table 8) Cache for client IP addresses and matching export rules.

Cache Name	Type of Information	Refresh Time (in Minutes)
Access	All export policy rules	60
Name	Name to UID	1
ID	ID to credentials	1
Host	Host to IP	1
Netgroup	Netgroup to IP	60
Showmount	Export paths	1

Credential Caches

NAS layer credential caches cannot be modified through the cluster shell at this time, but they can be flushed and viewed with the `diag nblade credentials` command, which is at the diag privilege level.

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

NetApp does not recommend modifying this refresh time unless required. Need for modifying these values would be determined through support cases. Additionally, flushing the cache should be done only when necessary, because it can cause latency to access and outages as the cache gets repopulated.

NFS/Name Service Database (NSDB) Caches

In addition to NAS layer caches, ONTAP has the concept of NFS caches when name services are involved, particularly when using the extended goups option. Rather than constantly needing to reach out to name service servers (such as NIS or LDAP) and fetch credentials, the NSDB cache will keep NFS credentials for 30 minutes. The NSDB cache can also be cleared starting in ONTAP 8.3.1 with the **diag privilege** command `diag nblade nfs nsdb-cache clear`. Starting in ONTAP 9.0, the cache can be viewed with `diag nblade nfs nsdb-cache show`.


```
cluster::> set diag
cluster::*> diag nsdb-cache show -node node3 -vserver SVM -unix-user-name nfs_user
  (diag nblade nfs nsdb-cache show)

           Node: node3
        Vserver: SVM
  Unix user name: nfs_user
   Creation time: 2146204100
Last Access time: 2146261100
  Number of hits: 19
```

NAS Layer Cache Age Recommendations

For the NAS layer access caches that are modifiable through the cluster shell, the following table covers the recommended refresh times.

Table 9) NAS layer cache ages.

Cache Name	Default Refresh (in Seconds)*	Recommended Refresh (in Seconds)*
Access refresh	3,600	18,000
Maximum refresh time	1,800	18,000
Minimum refresh time	180ms	900ms
TTL failure time	5	5
Maximum outstanding calls	65 calls	65 calls
Credential cache	1,200 (8.2.2 and earlier) 7,200 (8.2.x) Positive TTL: 86400 (8.3.1 and later) Negative TTL: 7,200 (8.3.1 and later)	1,200 (8.2.2 and earlier) 7,200 (8.2.3 and later) Positive TTL: 86400 (8.3.1 and later) Negative TTL: 7,200 (8.3.1 and later)
NSDB Cache	30 minutes	N/A (not modifiable)

Note: *Seconds unless designated otherwise.

NAS Layer Cache Modification

In clustered Data ONTAP, it is possible to modify the refresh times for a number of NAS-related caches. Some caches, however, cannot be modified or can be modified only at the bootarg or systemshell levels. This applies mainly to clustered Data ONTAP versions earlier than 8.3.x.

To modify the NAS layer caches in versions earlier than 8.3.x, contact NetApp technical support.

To modify the NAS layer caches in 8.3.x and later, use the following command in diag privilege level:

```
cluster::> set diag
cluster::*> diag exports nblade access-cache attributes modify -access-refresh [3600] -max-
refresh-time [1800] -min-refresh-time [180] -ttl-failure-time [5] -max-outstanding-calls [64]
```

SecD Caches

SecD is another area in the clustered Data ONTAP operating system that caches information retrieved from name services, such as user and group information, name service server connections, and so on. DNS is not currently cached in SecD, however. SecD caches are managed at a diag privilege level. Most of these caches age out after 24 hours.

The following caches are available for configuration and querying:

```
cluster::*> diag secd cache show-config -node node1 -cache-name
    ad-to-netbios-domain       netbios-to-ad-domain
    ems-delivery               ldap-groupid-to-name
    ldap-groupname-to-id       ldap-userid-to-creds
    ldap-userid-to-name        ldap-username-to-creds
    log-duplicate              name-to-sid
    sid-to-name                nis-groupid-to-name
    nis-groupname-to-id        nis-userid-to-creds
    nis-username-to-creds      nis-group-membership
    netgroup-ip                schannel-key
    lif-bad-route-to-target    username-to-creds
    ad-sid-to-local-membership netgroup-host
```

Note: Any time a cache is modified on a node, it should be modified on every node in a cluster.

Modifying caches can alter NAS behavior. More aggressive caches can mean more load on the system for cache refreshes. Less aggressive caches can lead to inconsistencies in name service requests (that is, hosts removed from the netgroup remain in cache until flushed).

To adjust a secd cache, use the following command:

```
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 node1 -cache-name netgroup-host -life-time 3600
```

Example of viewing the cache configuration:

```
cluster::*> diag secd cache show-config -node node1 -cache-name netgroup-host
Current Entries: 0
    Max Entries: 1024
 Entry Lifetime: 3600
```

Note: SecD cache changes are persistent across reboots.

Table 10) SecD cache ages.

Cache Name	Default Refresh Time	Recommended Refresh Time
ad-to-netbios-domain	0	0
ad-sid-to-local-membership	86,400	86,400
ems-delivery	300	300
groupname-to-info*	86,400	86,400
ldap-groupid-to-name	86,400	86,400
ldap-groupname-to-id	86,400	86,400
ldap-groupname-to-info-batch*	86,400	86,400
ldap-netgroupname-to-members*	86,400	86,400
ldap-username-to-info-batch*	86,400	86,400
ldap-userid-to-creds	86,400	86,400
ldap-userid-to-name	86,400	86,400
ldap-username-to-creds	86,400	86,400
lif-bad-route-to-target	14,400	14,400
log-duplicate	300	300
name-to-sid	86,400	86,400
netbios-to-ad-domain	0	0
netgroup-host	3,600	3,600
netgroup-ip	3,600	3,600
nis-groupid-to-name	86,400	86,400
nis-group-membership	86,400	86,400
nis-groupname-to-id	86,400	86,400
nis-userid-to-creds	86,400	86,400
nis-username-to-creds	86,400	86,400
schannel-key	0	0
sid-to-name	86,400	86,400
username-to-creds	86,400	86,400
username-to-info*	86,400	86,400

Note: * Denotes cache in versions of Data ONTAP 8.3 and later.

Note: NetApp recommends not changing SecD caches without guidance from NetApp Support.

Note: Cache values might vary depending on how aggressively the caches need to be refreshed.

Appendix

The following section covers topics that are not included in the main sections of this technical report. This includes troubleshooting, useful commands, and other topics. This section is subject to change over the lifespan of this document and does not cover all use cases.

DNS Terminology

The following table is intended to define commonly used DNS terminology.

Table 11) Common DNS terminology.

Term	Meaning
A	Resource record for IPv4 addresses performing host name–to-IP resolution.
AAAA	Resource record for IPv6 addresses performing host name–to-IP resolution.
DAD	Duplicate address detection.
DDNS	Dynamic DNS: dynamic updates of DNS records.
DNS	Domain Name System: maps host names to IP addresses and vice versa.
FQDN	Fully qualified domain name: host name appended with DNS suffix; for example, host.domain.com is an FQDN.
PTR	Pointer record for IP-to–host name resolution.
RR	DNS resource record.
SOA	Start of authority record: designates which DNS server is the authoritative source for records.
TTL	Time to live: how long a DNS record remains in the cache before being updated.

DDNS 7-Mode to Clustered Data ONTAP Command Map

The following table lists DDNS commands for 7-Mode and clustered Data ONTAP.

Table 12) DDNS command map.

7-Mode Command	Clustered Data ONTAP Command
`options dns.update.enable off`	`vserver services name-service dns dynamic-update modify -vserver <vserver-name> is-enabled false`
`options dns.update.enable on`	`vserver services name-service dns dynamic-update modify -vserver <vserver-name> is-enabled true`

`options dns.update.enable secure`	`vserver services name-service dns dynamic-update modify -vserver <vserver-name> is-enabled true`
	
	`vserver services name-service dns dynamic-update modify -vserver <vserver-name> use-secure true`

`options dns.update.ttl`	`vserver services name-service dns dynamic-update modify -vserver <vserver-name> ttl (available only in advanced mode)`
`ifconfig <interface> <ip-address> no_ddns`	`network interface modify -vserver <vserver-name> -lif <lif-name> is-dns-update-enabled <true/false>`

Query Host Names from Clients to Test for DNS Entries

As per best practices for host names in netgroups, any host name should be able to resolve to DNS with forward and reverse lookups. To test this functionality, two main tools can be used: dig (domain information groper) and nslookup (name service lookup):

- Dig man pages
- Nslookup man pages

You can find a list of DNS error types in RFC-2929.

Dig Examples

Dig example: forward lookup of host name:

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

; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.30.rc1.el6_6.1 <<>> centos64.domain.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.domain.com. IN  ANY

;; ANSWER SECTION:
centos64.domain.com. 3600 IN A    10.228.225.140

;; Query time: 0 msec
;; SERVER: 10.228.225.120#53(10.228.225.120)
;; WHEN: Mon Apr 13 16:06:33 2015
;; MSG SIZE  rcvd: 67
```

Dig example: reverse lookup:

```
# dig -x 10.228.225.140

; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.30.rc1.el6_6.1 <<>> -x 10.228.225.140
;; 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:
;140.225.228.10.in-addr.arpa.   IN      PTR

;; ANSWER SECTION:
140.225.228.10.in-addr.arpa. 3600 IN    PTR     centos64.domain.com.

;; Query time: 0 msec
;; SERVER: 10.228.225.120#53(10.228.225.120)
;; WHEN: Mon Apr 13 16:08:19 2015
;; MSG SIZE  rcvd: 92
```


Dig example: SRV record:

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

; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.30.rc1.el6_6.1 <<>> _ldap._tcp.domain.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.domain.com. IN        SRV

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

;; ADDITIONAL SECTION:
2k8-dc-1.domain.com. 3600 IN A    10.228.225.120
2k8-dc-1.domain.com. 3600 IN AAAA fd20:8b1e:b255:8599:5457:61d9:fc87:423f

;; Query time: 1 msec
;; SERVER: 10.228.225.120#53(10.228.225.120)
;; WHEN: Mon Apr 13 16:01:34 2015
;; MSG SIZE  rcvd: 150
```

Dig example: nonexistent record:

```
# dig fail.domain.com

; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.30.rc1.el6_6.1 <<>> fail.domain.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.domain.com.               IN      A

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

;; Query time: 132 msec
;; SERVER: 10.228.225.120#53(10.228.225.120)
;; WHEN: Mon Apr 13 16:02:21 2015
;; MSG SIZE  rcvd: 85
```


Nslookup Examples

Nslookup example: forward lookup:

```
# nslookup -type=any centos64.domain.com.
Server:         10.228.225.120
Address:        10.228.225.120#53

Name:   centos64.domain.com
Address: 10.228.225.140
```

Nslookup example: reverse lookup:

```
# nslookup -type=ptr 10.228.225.140
Server:         10.228.225.120
Address:        10.228.225.120#53

140.225.228.10.in-addr.arpa     name = centos64.domain.com.
```

Nslookup example: SRV record:

```
# nslookup -type=srv _ldap._tcp.domain.com
Server:         10.228.225.120
Address:        10.228.225.120#53

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

Nslookup example: nonexistent record:

```
# nslookup -type=any fail.domain.com
Server:         10.228.225.120
Address:        10.228.225.120#53

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

For more examples, see the following pages:

- Dig examples
- Nslookup examples

References

- TR-3580: NFSv4 Enhancements and Best Practices Guide: Data ONTAP Implementation
- TR-4073: Secure Unified Authentication
- TR-4182: Ethernet Storage Best Practices for Clustered Data ONTAP Configurations
- TR-4191: Best Practices Guide for Clustered Data ONTAP 8.2.x and 8.3 Windows File Services
- TR-4211: NetApp Storage Performance Primer for Clustered Data ONTAP 8.2
- TR-4523: DNS Load Balancing in ONTAP
- TR-4557: NetApp FlexGroup Technical Overview

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.