



Balance network loads

ONTAP 9

NetApp
April 06, 2024

This PDF was generated from https://docs.netapp.com/us-en/ontap/networking/balance_network_loads_to_optimize_user_traffic_@cluster_administrators_only@_overview.html on April 06, 2024. Always check docs.netapp.com for the latest.

Table of Contents

- Balance network loads 1
 - Balance network overview 1
 - How DNS load balancing works 1
 - Create a DNS load balancing zone 1
 - Add or remove a LIF from a load balancing zone 2
 - Configure DNS services (ONTAP 9.8 and later) 3
 - Configure DNS services (ONTAP 9.7 and earlier) 6
 - Configure dynamic DNS services 9

Balance network loads

Balance network overview

You can configure your cluster to serve client requests from appropriately loaded LIFs. This results in a more balanced utilization of LIFs and ports, which in turn allows for better performance of the cluster.

DNS load balancing helps in selecting an appropriately loaded data LIF and balancing user network traffic across all available ports (physical, interface groups, and VLANs).

With DNS load balancing, LIFs are associated with the load balancing zone of an SVM. A site-wide DNS server is configured to forward all DNS requests and return the least-loaded LIF based on the network traffic and the availability of the port resources (CPU usage, throughput, open connections, and so on). DNS load balancing provides the following benefits:

- New client connections balanced across available resources.
- No manual intervention required for deciding which LIFs to use when mounting a particular SVM.
- DNS load balancing supports NFSv3, NFSv4, NFSv4.1, SMB 2.0, SMB 2.1, SMB 3.0, and S3.

How DNS load balancing works

Clients mount an SVM by specifying an IP address (associated with a LIF) or a host name (associated with multiple IP addresses). By default, LIFs are selected by the site-wide DNS server in a round-robin manner, which balances the workload across all LIFs.

Round-robin load balancing can result in overloading some LIFs, so you have the option of using a DNS load balancing zone that handles the host-name resolution in an SVM. Using a DNS load balancing zone, ensures better balance of the new client connections across available resources, leading to improved performance of the cluster.

A DNS load balancing zone is a DNS server inside the cluster that dynamically evaluates the load on all LIFs and returns an appropriately loaded LIF. In a load balancing zone, DNS assigns a weight (metric), based on the load, to each LIF.

Every LIF is assigned a weight based on its port load and CPU utilization of its home node. LIFs that are on less-loaded ports have a higher probability of being returned in a DNS query. Weights can also be manually assigned.

Create a DNS load balancing zone

You can create a DNS load balancing zone to facilitate the dynamic selection of a LIF based on the load, that is, the number of clients mounted on a LIF. You can create a load balancing zone while creating a data LIF.

Before you begin

The DNS forwarder on the site-wide DNS server must be configured to forward all requests for the load balancing zone to the configured LIFs.

The Knowledgebase article [How to set up DNS load balancing in Cluster-Mode](#) on the NetApp Support Site contains more information about configuring DNS load balancing using conditional forwarding.

About this task

- Any data LIF can respond to DNS queries for a DNS load balancing zone name.
- A DNS load balancing zone must have a unique name in the cluster, and the zone name must meet the following requirements:
 - It should not exceed 256 characters.
 - It should include at least one period.
 - The first and the last character should not be a period or any other special character.
 - It cannot include any spaces between characters.
 - Each label in the DNS name should not exceed 63 characters.

A label is the text appearing before or after the period. For example, the DNS zone named `storage.company.com` has three labels.

Step

Use the `network interface create` command with the `dns-zone` option to create a DNS load balancing zone.

If the load balancing zone already exists, the LIF is added to it. For more information about the command, see [ONTAP 9 commands](#).

The following example demonstrates how to create a DNS load balancing zone named `storage.company.com` while creating the LIF `lif1`:

```
network interface create -vserver vs0 -lif lif1 -home-node node1
-home-port e0c -address 192.0.2.129 -netmask 255.255.255.128 -dns-zone
storage.company.com
```

Add or remove a LIF from a load balancing zone

You can add or remove a LIF from the DNS load balancing zone of a virtual machine (SVM). You can also remove all the LIFs simultaneously from a load balancing zone.

Before you begin

- All the LIFs in a load balancing zone should belong to the same SVM.
- A LIF can be a part of only one DNS load balancing zone.
- Failover groups for each subnet must have been set up, if the LIFs belong to different subnets.

About this task

A LIF that is in the administrative down status is temporarily removed from the DNS load balancing zone. When the LIF returns to the administrative up status, the LIF is automatically added to the DNS load balancing zone.

Step

Add a LIF to or remove a LIF from a load balancing zone:

If you want to...	Enter...
Add a LIF	<pre>network interface modify -vserver vs1 -lif lif_name -dns-zone zone_name</pre> <p>Example:</p> <pre>network interface modify -vserver vs1 -lif data1 -dns -zone cifs.company.com</pre>
Remove a single LIF	<pre>network interface modify -vserver vs1 -lif lif_name -dns-zone none</pre> <p>Example:</p> <pre>network interface modify -vserver vs1 -lif data1 -dns -zone none</pre>
Remove all LIFs	<pre>network interface modify -vserver vs1 -lif * -dns-zone none</pre> <p>Example:</p> <pre>network interface modify -vserver vs0 -lif * -dns-zone none</pre> <p>You can remove an SVM from a load balancing zone by removing all the LIFs in the SVM from that zone.</p>

Configure DNS services (ONTAP 9.8 and later)

You must configure DNS services for the SVM before creating an NFS or SMB server. Generally, the DNS name servers are the Active Directory-integrated DNS servers for the domain that the NFS or SMB server will join.

About this task

Active Directory-integrated DNS servers contain the service location records (SRV) for the domain LDAP and domain controller servers. If the SVM cannot find the Active Directory LDAP servers and domain controllers, NFS or SMB server setup fails.

SVMs use the hosts name services ns-switch database to determine which name services to use and in which order when looking up information about hosts. The two supported name services for the hosts database are files and dns.

You must ensure that dns is one of the sources before you create the SMB server.



To view the statistics for DNS name services for the mgwd process and SecD process, use the Statistics UI.

Steps

1. Determine what the current configuration is for the hosts name services database. In this example, the hosts name service database uses the default settings.

```
vserver services name-service ns-switch show -vserver vs1 -database hosts
```

```
Vserver: vs1
Name Service Switch Database: hosts
Vserver: vs1 Name Service Switch Database: hosts
Name Service Source Order: files, dns
```

2. Perform the following actions, if required.

- a. Add the DNS name service to the hosts name service database in the desired order, or reorder the sources.

In this example, the hosts database is configured to use DNS and local files in that order.

```
vserver services name-service ns-switch modify -vserver vs1 -database hosts
-sources dns,files
```

- b. Verify that the name services configuration is correct.

```
vserver services name-service ns-switch show -vserver vs1 -database hosts
```

```
Vserver: vs1
Name Service Switch Database: hosts
Name Service Source Order: dns, files
```

3. Configure DNS services.

```
vserver services name-service dns create -vserver vs1 -domains
example.com,example2.com -name-servers 10.0.0.50,10.0.0.51
```



The `vserver services name-service dns create` command performs an automatic configuration validation and reports an error message if ONTAP is unable to contact the name server.

4. Verify that the DNS configuration is correct and that the service is enabled.

```
Vserver: vs1
Domains: example.com, example2.com Name Servers: 10.0.0.50, 10.0.0.51
Enable/Disable DNS: enabled Timeout (secs): 2
Maximum Attempts: 1
```

5. Validate the status of the name servers.

```
vserver services name-service dns check -vserver vs1
```

Vserver	Name Server	Status	Status Details
vs1	10.0.0.50	up	Response time (msec): 2
vs1	10.0.0.51	up	Response time (msec): 2

Configure dynamic DNS on the SVM

If you want the Active Directory-integrated DNS server to dynamically register the DNS records of an NFS or SMB server in DNS, you must configure dynamic DNS (DDNS) on the SVM.

Before you begin

DNS name services must be configured on the SVM. If you are using secure DDNS, you must use Active Directory-integrated DNS name servers and you must have created either an NFS or SMB server or an Active Directory account for the SVM.

About this task

The specified fully qualified domain name (FQDN) must be unique:

The specified fully qualified domain name (FQDN) must be unique:

- For NFS, the value specified in `-vserver-fqdn` as part of the `vserver services name-service dns dynamic-update` command becomes the registered FQDN for the LIFs.
- For SMB, the values specified as the CIFS server NetBIOS name and the CIFS server fully qualified domain name become the registered FQDN for the LIFs. This is not configurable in ONTAP. In the following scenario, the LIF FQDN is "CIFS_VS1.EXAMPLE.COM":

```
cluster1::> cifs server show -vserver vs1

                                Vserver: vs1
                                CIFS Server NetBIOS Name: CIFS_VS1
                                NetBIOS Domain/Workgroup Name: EXAMPLE
                                Fully Qualified Domain Name: EXAMPLE.COM
                                Organizational Unit: CN=Computers
Default Site Used by LIFs Without Site Membership:
                                Workgroup Name: -
                                Kerberos Realm: -
                                Authentication Style: domain
                                CIFS Server Administrative Status: up
                                CIFS Server Description:
                                List of NetBIOS Aliases: -
```



To avoid a configuration failure of an SVM FQDN that is not compliant to RFC rules for DDNS updates, use an FQDN name that is RFC compliant. For more information, see [RFC 1123](#).

Steps

1. Configure DDNS on the SVM:

```
vserver services name-service dns dynamic-update modify -vserver vserver_name
-is- enabled true [-use-secure {true|false} -vserver-fqdn
FQDN_used_for_DNS_updates
```

```
vserver services name-service dns dynamic-update modify -vserver vs1 -is
-enabled true - use-secure true -vserver-fqdn vs1.example.com
```

Asterisks cannot be used as part of the customized FQDN. For example, *.netapp.com is not valid.

2. Verify that the DDNS configuration is correct:

```
vserver services name-service dns dynamic-update show
```

Vserver	Is-Enabled	Use-Secure	Vserver FQDN	TTL
vs1	true	true	vs1.example.com	24h

Configure DNS services (ONTAP 9.7 and earlier)

You must configure DNS services for the SVM before creating an NFS or SMB server. Generally, the DNS name servers are the Active Directory-integrated DNS servers for the domain that the NFS or SMB server will join.

About this task

Active Directory-integrated DNS servers contain the service location records (SRV) for the domain LDAP and domain controller servers. If the SVM cannot find the Active Directory LDAP servers and domain controllers, NFS or SMB server setup fails.

SVMs use the hosts name services ns-switch database to determine which name services to use and in which order when looking up information about hosts. The two supported name services for the hosts database are files and dns.

You must ensure that dns is one of the sources before you create the SMB server.



To view the statistics for DNS name services for the mgwd process and SecD process, use the Statistics UI.

Steps

1. Determine what the current configuration is for the hosts name services database.

In this example, the hosts name service database uses the default settings.

```
vserver services name-service ns-switch show -vserver vs1 -database hosts
```

```
Vserver: vs1
Name Service Switch Database: hosts
Name Service Source Order: files, dns
```


2. Perform the following actions, if required.

- Add the DNS name service to the hosts name service database in the desired order, or reorder the sources.

In this example, the hosts database is configured to use DNS and local files in that order.

```
vserver services name-service ns-switch modify -vserver vs1 -database hosts  
-sources dns,files
```

- Verify that the name services configuration is correct.

```
vserver services name-service ns-switch show -vserver vs1 -database hosts
```

3. Configure DNS services.

```
vserver services name-service dns create -vserver vs1 -domains  
example.com,example2.com -name-servers 10.0.0.50,10.0.0.51
```



The `vserver services name-service dns create` command performs an automatic configuration validation and reports an error message if ONTAP is unable to contact the name server.

4. Verify that the DNS configuration is correct and that the service is enabled.

```
Vserver: vs1  
Domains: example.com, example2.com Name  
Servers: 10.0.0.50, 10.0.0.51  
Enable/Disable DNS: enabled Timeout (secs): 2  
Maximum Attempts: 1
```

5. Validate the status of the name servers.

```
vserver services name-service dns check -vserver vs1
```

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

Configure dynamic DNS on the SVM

If you want the Active Directory-integrated DNS server to dynamically register the DNS records of an NFS or SMB server in DNS, you must configure dynamic DNS (DDNS) on the SVM.

Before you begin

DNS name services must be configured on the SVM. If you are using secure DDNS, you must use Active Directory-integrated DNS name servers and you must have created either an NFS or SMB server or an Active

Directory account for the SVM.

About this task

The specified fully qualified domain name (FQDN) must be unique:

- For NFS, the value specified in `-vserver-fqdn` as part of the `vserver services name-service dns dynamic-update` command becomes the registered FQDN for the LIFs.
- For SMB, the values specified as the CIFS server NetBIOS name and the CIFS server fully qualified domain name become the registered FQDN for the LIFs. This is not configurable in ONTAP. In the following scenario, the LIF FQDN is "CIFS_VS1.EXAMPLE.COM":

```
cluster1::> cifs server show -vserver vs1

                                Vserver: vs1
                        CIFS Server NetBIOS Name: CIFS_VS1
NetBIOS Domain/Workgroup Name: EXAMPLE
        Fully Qualified Domain Name: EXAMPLE.COM
                Organizational Unit: CN=Computers
Default Site Used by LIFs Without Site Membership:
                                Workgroup Name: -
                                Kerberos Realm: -
                        Authentication Style: domain
CIFS Server Administrative Status: up
        CIFS Server Description:
        List of NetBIOS Aliases: -
```



To avoid a configuration failure of an SVM FQDN that is not compliant to RFC rules for DDNS updates, use an FQDN name that is RFC compliant. For more information, see [RFC 1123](#).

Steps

1. Configure DDNS on the SVM:

```
vserver services name-service dns dynamic-update modify -vserver vs1 -is-  
enabled true [-use-secure {true|false}] -vserver-fqdn  
FQDN_used_for_DNS_updates
```

```
vserver services name-service dns dynamic-update modify -vserver vs1 -is-  
enabled true - use-secure true -vserver-fqdn vs1.example.com
```

Asterisks cannot be used as part of the customized FQDN. For example, `*.netapp.com` is not valid.

2. Verify that the DDNS configuration is correct:

```
vserver services name-service dns dynamic-update show
```

Vserver	Is-Enabled	Use-Secure	Vserver FQDN	TTL
-----	-----	-----	-----	-----
vs1	true	true	vs1.example.com	24h

Configure dynamic DNS services

If you want the Active Directory-integrated DNS server to dynamically register the DNS records of an NFS or SMB server in DNS, you must configure dynamic DNS (DDNS) on the SVM.

Before you begin

DNS name services must be configured on the SVM. If you are using secure DDNS, you must use Active Directory-integrated DNS name servers and you must have created either an NFS or SMB server or an Active Directory account for the SVM.

About this task

The specified FQDN must be unique.



To avoid a configuration failure of an SVM FQDN that is not compliant to RFC rules for DDNS updates, use an FQDN name that is RFC compliant.

Steps

1. Configure DDNS on the SVM:

```
vserver services name-service dns dynamic-update modify -vserver vserver_name
-is-enabled true [-use-secure {true|false} -vserver-fqdn
FQDN_used_for_DNS_updates
```

```
vserver services name-service dns dynamic-update modify -vserver vs1 -is
-enabled true - use-secure true -vserver-fqdn vs1.example.com
```

Asterisks cannot be used as part of the customized FQDN. For example, *.netapp.com is not valid.

2. Verify that the DDNS configuration is correct:

```
vserver services name-service dns dynamic-update show
```

Vserver	Is-Enabled	Use-Secure	Vserver FQDN	TTL
-----	-----	-----	-----	-----
vs1	true	true	vs1.example.com	24h

Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.