



Configure IPspaces (cluster administrators only)

ONTAP 9

NetApp
May 17, 2023

This PDF was generated from https://docs.netapp.com/us-en/ontap/networking/configure_ipspaces_@cluster_administrators_only@_overview.html on May 17, 2023. Always check docs.netapp.com for the latest.

Table of Contents

- Configure IPspaces (cluster administrators only)..... 1
 - Overview 1
 - Example of using IPspaces 1
 - Standard properties of IPspaces 3
 - Create IPspaces..... 4
 - Display IPspaces 5
 - Delete an IPspace 6

Configure IPspaces (cluster administrators only)

Overview

IPspaces enable you to configure a single ONTAP cluster so that it can be accessed by clients from more than one administratively separate network domain, even if those clients are using the same IP address subnet range. This allows for separation of client traffic for privacy and security.

An IPspace defines a distinct IP address space in which storage virtual machines (SVMs) reside. Ports and IP addresses defined for an IPspace are applicable only within that IPspace. A distinct routing table is maintained for each SVM within an IPspace; therefore, no cross-SVM or cross-IPspace traffic routing occurs.



IPspaces support both IPv4 and IPv6 addresses on their routing domains.

If you are managing storage for a single organization, then you do not need to configure IPspaces. If you are managing storage for multiple companies on a single ONTAP cluster, and you are certain that none of your customers have conflicting networking configurations, then you also do not need to use IPspaces. In many cases, the use of storage virtual machines (SVMs), with their own distinct IP routing tables, can be used to segregate unique networking configurations instead of using IPspaces.

Example of using IPspaces

A common application for using IPspaces is when a Storage Service Provider (SSP) needs to connect customers of companies A and B to an ONTAP cluster on the SSP's premises and both companies are using the same private IP address ranges.

The SSP creates SVMs on the cluster for each customer and provides a dedicated network path from two SVMs to company A's network and from the other two SVMs to company B's network.

This type of deployment is shown in the following illustration, and it works if both companies use non-private IP address ranges. However, the illustration shows both companies using the same private IP address ranges, which causes problems.



Both companies use the private IP address subnet 10.0.0.0, causing the following problems:

- The SVMs in the cluster at the SSP location have conflicting IP addresses if both companies decide to use the same IP address for their respective SVMs.
- Even if the two companies agree on using different IP addresses for their SVMs, problems can arise.
- For example, if any client in A's network has the same IP address as a client in B's network, packets destined for a client in A's address space might get routed to a client in B's address space, and vice versa.
- If the two companies decide to use mutually exclusive address spaces (for example, A uses 10.0.0.0 with a network mask of 255.128.0.0 and B uses 10.128.0.0 with a network mask of 255.128.0.0), the SSP needs to configure static routes on the cluster to route traffic appropriately to A's and B's networks.
- This solution is neither scalable (because of static routes) nor secure (broadcast traffic is sent to all interfaces of the cluster). To overcome these problems, the SSP defines two IPspaces on the cluster—one for each company. Because no cross-IPspace traffic is routed, the data for each company is securely routed to its respective network even if all of the SVMs are configured in the 10.0.0.0 address space, as

shown in the following illustration:



Additionally, the IP addresses referred to by the various configuration files, such as the `/etc/hosts` file, the `/etc/hosts.equiv` file, and the `/etc/rc` file, are relative to that IPspace. Therefore, the IPspaces enable the SSP to configure the same IP address for the configuration and authentication data for multiple SVMs, without conflict.

Standard properties of IPspaces

Special IPspaces are created by default when the cluster is first created. Additionally, special storage virtual machines (SVMs) are created for each IPspace.

Two IPspaces are created automatically when the cluster is initialized:

- "Default" IPspace

This IPspace is a container for ports, subnets, and SVMs that serve data. If your configuration does not need separate IPspaces for clients, all SVMs can be created in this IPspace. This IPspace also contains the cluster management and node management ports.

- "Cluster" IPspace

This IPspace contains all cluster ports from all nodes in the cluster. It is created automatically when the cluster is created. It provides connectivity to the internal private cluster network. As additional nodes join the cluster, cluster ports from those nodes are added to the "Cluster" IPspace.

A "system" SVM exists for each IPspace. When you create an IPspace, a default system SVM of the same name is created:

- The system SVM for the "Cluster" IPspace carries cluster traffic between nodes of a cluster on the internal private cluster network.

It is managed by the cluster administrator, and it has the name "Cluster".

- The system SVM for the "Default" IPspace carries management traffic for the cluster and nodes, including the intercluster traffic between clusters.

It is managed by the cluster administrator, and it uses the same name as the cluster.

- The system SVM for a custom IPspace that you create carries management traffic for that SVM.

It is managed by the cluster administrator, and it uses the same name as the IPspace.

One or more SVMs for clients can exist in an IPspace. Each client SVM has its own data volumes and configurations, and it is administered independently of other SVMs.

Create IPspaces

IPspaces are distinct IP address spaces in which storage virtual machines (SVMs) reside. You can create IPspaces when you need your SVMs to have their own secure storage, administration, and routing.

About this task

There is a cluster-wide limit of 512 IPspaces. The cluster-wide limit is reduced to 256 IPspaces for clusters that contain nodes with 6 GB of RAM or less for platforms such as FAS2220 or FAS2240. See the Hardware Universe to determine whether additional limits apply to your platform.

[NetApp Hardware Universe](#)



An IPspace name cannot be "all" because "all" is a system-reserved name.

Step

Create an IPspace:

```
network ipspace create -ipspace ipspace_name
```

`ipspace_name` is the name of the IPspace that you want to create. The following command creates the IPspace `ipspace1` on a cluster:

```
network ipspace create -ipspace ipspace1
```

After you finish

If you create an IPspace in a cluster with a MetroCluster configuration, IPspace objects must be manually replicated to the partner clusters. Any SVMs that are created and assigned to an IPspace before the IPspace is replicated will not be replicated to the partner clusters.

Broadcast domains are created automatically in the "Default" IPspace and can be moved between IPspaces using the following command:

```
network port broadcast-domain move
```

For example, if you want to move a broadcast domain from "Default" to "ips1", using the following command:

```
network port broadcast-domain move -ipspace Default -broadcast-domain  
Default -to-ipspace ips1
```

Display IPspaces

You can display the list of IPspaces that exist in a cluster, and you can view the storage virtual machines (SVMs), broadcast domains, and ports that are assigned to each IPspace.

Step

Display the IPspaces and SVMs in a cluster:

```
network ipspace show [-ipspace ipspace_name]
```

The following command displays all of the IPspaces, SVMs, and broadcast domains in the cluster:

```

network ipspace show
IPspace      Vserver List      Broadcast Domains
-----
Cluster
Default      Cluster            Cluster
vs1, cluster-1
ipspace1     vs3, vs4, ipspace1  Default
bcast1

```

The following command displays the nodes and ports that are part of IPspace ipspace1:

```

network ipspace show -ipspace ipspace1
IPspace name: ipspace1
Ports: cluster-1-01:e0c, cluster-1-01:e0d, cluster-1-01:e0e, cluster-1-02:e0c, cluster-1-02:e0d, cluster-1-02:e0e
Broadcast Domains: Default-1
Vservers: vs3, vs4, ipspace1

```

Delete an IPspace

If you no longer need an IPspace, you can delete it.

Before you begin

There must be no broadcast domains, network interfaces, or SVMs associated with the IPspace you want to delete.

The system-defined "Default" and "Cluster" IPspaces cannot be deleted.

Step

Delete an IPspace:

```

network ipspace delete -ipspace ipspace_name

```

The following command deletes IPspace ipspace1 from the cluster:

```

network ipspace delete -ipspace ipspace1

```


Copyright information

Copyright © 2023 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.