Admin Partitioning

http://docs.citrix.com/content/docs/en-us/netscaler/11-1/admin-partition.html
Nov. 16, 2015

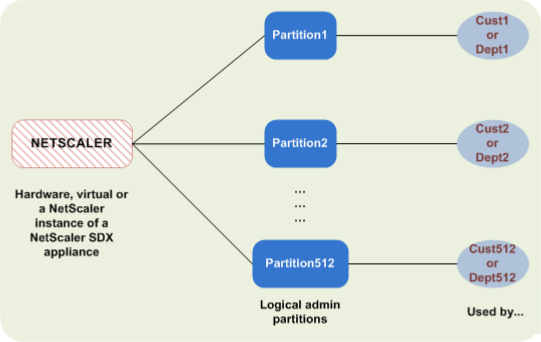
Admin Partitioning

Important

- The admin partitioning feature is provided from NetScaler 11.0 onwards. It is also provided as a separate enhancement release that is based on NetScaler 10.5 Build 52.11.

- Until specified otherwise, this documentation applies to NetScaler versions 11.0 and 10.5 Build 52.11.

A NetScaler appliance can be partitioned into logical entities called admin partitions, where each partition can be configured and used as a separate NetScaler appliance. The following figure shows the partitions of a NetScaler being used by different customers and departments:



For information on how admin partitions can benefit your business, see Benefits and Uses of Admin Partitions.

A partitioned NetScaler appliance has a single default partition and one or more admin partitions. The following table provides further details on the two partition types:

	Default Partition	Admin Partitions
Availability	The NetScaler ships with a single partition, which is called a default partition. The default partition is retained even after the NetScaler is partitioned.	Must be explicitly created as described in Partitioning a NetScaler.
Number of Partitions	One	A NetScaler appliance can have one or more (maximum of 512) admin partitions.
User Access and Roles	The default partition can be accessed and configured by all NetScaler users who are not associated with a *partition-specific* command policy. As always, the operations that a user can perform are restricted by the associated command policy.	Can be created only by NetScaler superusers who also specify the users for that partition. Only superusers and associated users of the partition can access and configure the admin partition. Note: Partition users do not have shell access.
	All files in a default partition are stored in the default NetScaler file structure.	All files in an admin partition are stored in directory paths that have the name of the admin partition. For example, the NetScaler configuration file (ns.conf) is stored in the */nsconfig/partitions/<partitionName>* directory. Other partition-specific files are stored in the */var/partitions/<partitionName>* directories. Some other paths in an admin partition:

File Structure	For example, the NetScaler configuration file is stored in the */nsconfig* directory and NetScaler logs are stored in the */var/log/* directory.	○ Downloaded files: */var/partitions/<partitionName>/download/* ○ Log files: */var/partitions/<partitionName>/log/* **Note:** Currently, logging is not supported at partition-level. Therefore, this directory is empty and all logs are stored in the */var/log/* directory. ○ SSL CRL certificate related files: */var/partitions/<partitionName>/netscaler/ssl*
Resources Available	All NetScaler resources.	NetScaler resources that are explicitly assigned to the admin partition.

Benefits and Uses of Admin Partitions

You can avail the following benefits by using admin partitions for your deployment:

- Allows delegation of administrative ownership of an application to the customer.
- Reduces the cost of ADC ownership without compromising on performance and ease-of-use.
- Safeguards from unwarranted configuration changes. In a non-partitioned NetScaler, authorized users of other application could intentionally or unintentionally change configurations that are required for your application. This could lead to undesirable behavior. This possibility is reduced in a partitioned NetScaler.
- Isolates traffic between different applications by the use of dedicated VLANs for each partition.
- Accelerates and allows to scale application deployments.
- Allows application-level or localized management and reporting.

Let us analyze a couple of cases to understand the scenarios in which you can use admin partitions.

Case 1 : Admin partitions used by an enterprise

Let us consider a scenario faced by a company named **Foo.com**.

- **Foo.com** has a single NetScaler ADC.
- There are five departments and each department has one application that requires to be deployed with the NetScaler.
- Each application must be managed independently by a different set of users or administrators.
- Other users must be restricted from accessing the configurations.
- The application or back-end must be able to share resources like IP addresses.
- The global IT department must be able to control NetScaler-level settings which must be common to all partitions.
- Applications must be independent of one another. An error in configuration of one application must not affec the other.

A non-partitioned NetScaler would not be able to satisfy these requirements. However, you can achieve all these requirements by partitioning a NetScaler.

Simply create a partition for each of the applications, assign the required users to the partitions, specify a VLAN for each partition, and define global settings on the default partition.

Case 2 : Admin partitions used by a service provider

Let us consider a scenario faced by a service provider named **BigProvider**:

- BigProvider has 5 customers: 3 small enterprises and 2 large enterprises.
- **SmallBiz**, **SmallerBiz**, and **StartupBiz** need only the most basic NetScaler functionality.
- **BigBiz** and **LargeBiz** are larger enterprises and have applications that attract a lot of traffic. They would like to use some of the more complex NetScaler functionality.

In a non-partitioned approach, the NetScaler administrator would typically use a NetScaler SDX appliance and provision a NetScaler instance for each customer.

This solution suits **BigBiz** and **LargeBiz** because their applications need the undiminished power of the entire non-partitioned NetScaler appliance. However, this solution might not be as cost effective for servicing **SmallBiz**, **SmallerBiz** , and **StartupBiz**.

Therefore, **BigProvider** decides on the following solution:

- Using a NetScaler SDX appliance to bring up dedicated NetScaler instances for **BigBiz** and **LargeBiz**.

- Using a single NetScaler which is partitioned into three partitions, one each for **SmallBiz**, **SmallerBiz**, and **StartupBiz**.

  The NetScaler administrator (superuser) creates an admin partition for each of these customers, specifies the users for the partitions, specifies the NetScaler resources for the partitions, and specifies the VLAN to be used by the traffic that is destined for each of the partitions.

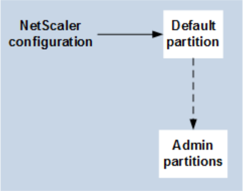
NetScaler Configurations Supported in Partitions

Depending on the NetScaler configuration and the partition in which the configuration is performed, NetScaler configurations can be categorized into the cases mentioned below.

Note

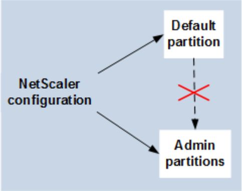
- Admin partitions cannot be set up on a NetScaler cluster. This means that a NetScaler cluster cannot be partitioned.
- Admin partitions cannot be set up on a NetScaler MPX-FIPS appliance.
- Case 3 lists the NetScaler features that are not supported in admin partitions.

Case 1 (global configurations). Configurations that can be performed ONLY in the default partition and which are available or impact all the admin partitions.



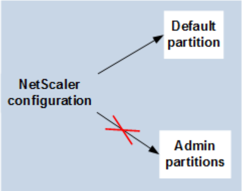
- Updates to built-in entities for monitors, TCP profiles, HTTP profiles, and so on.
- Updates to global parameters for syslog, nslog, weblog, content switching, IPSEC, SIP, DHCP, Surge protection, TCP buffering, and system collection.
- High availability (HA) configurations
- Interface and VLAN changes
- User configurations

Case 2 (partition-specific configurations). Configurations that can be performed independently in default and admin partitions. These configurations are applicable only to the partition in which they are performed.



- Getting traffic level statistics for a partition.
- Partition admin can update IP bindings for VLAN which is bound to that partition. But cannot update the interface bindings.
- Clearing NetScaler configurations.
- Feature-specific parameters for the following features: AppFlow, AppQoE, HTTP compression, DNS, TCP, HTTP, encryption, responder, rewrite, and SSL.
- Feature-specific configurations such as virtual servers, services, monitors, and so on.

Case 3: Configurations that cannot be performed on admin partitions. These features can be configured in the default partition, but there is no impact on admin partitions.



Note: Configurations that are supported on admin partitions for a particular release are marked as **Yes**.

		NetSCALER		

Group	Feature	10.5	NetScaler 11.0	NetScaler 11.1
Policy	Extensibility	No	Yes	Yes
LB	DBS AutoScale	No	Yes	Yes
LB	DNSSEC	No	No	No
LB	Diameter	No	No	Yes
LB	RTSP	No	No	No
LB	Sure Connect	No	Yes	Yes
LB	Autoscale Service Group	No	No	Yes
Manageability	RBA External Authentication	No	No	No
Manageability	RISE Cisco	No	No	No
Manageability	ACI-Cisco	No	No	Yes
Manageability	AppExpert	Yes	Yes	Yes
Manageability	HDX Insight	No	No	No
ManageabilityNo	Insight	No	No	No
VPN	Cloudbridge Connector	No	No	No
VPN	NetScaler Gateway or SSL VPN	No	No	No
VPN	SSL VPN ICA Proxy	No	No	No
VPN	Web Interface on NetScaler	No	No	No
SSL	SSL Profile	No	No	Yes
SSL	SSL-FIPS	No	No	No
SSL	External-HSM	No	No	No
Infra	Cache Re-direction	No	No	No
Infra	Integrated Caching (Restricted Feature)	No	Yes	Yes
Network	VXLAN	No	No	Yes
Network	Graceful Shutdown	No	Yes	Yes
Network	LSN	No	No	No
Network	v6 Ready Logo	No	No	Yes
Network	Vpath	No	No	Yes
LB	Datastream	No	Yes	Yes
Logging	Web logging	No	Yes	Yes
Network	L2 Param/L3 Param	No	Yes	Yes
Network	GRE Tunnel	No	No	Yes
LB	Scriptable Mirroring	No	Yes	Yes
LB	GSLB	No	Yes	Yes
Infra	Connection Mirroring	No	Yes	Yes
Infra	FEO	No	Yes	Yes
Infra	Nstrace	No	Yes	Yes
LB	SureConnect	No	Yes	Yes
LB	Priority Queuing	No	No	Yes
Network	HDOSP	No	No	Yes
Network	Netprofile (Restricted Feature)	No	No	Yes
Network	Networking (Restricted Feature)	No	No	Yes
Network	VRRP (Restricted Feature)	No	No	Yes
Logging	Audit Logging (Restricted Feature)	No	No	Yes
VPN	NetScaler Gateway	No	No	No
VPN	AAA-TM	No	Yes except RBA authentication feature.	Yes except RBA authentication feature
APPFW	Application Firewall	No	No	No
LB	TCP Buffering (Restricted Feature)	No	No	No
Policies	OCSP Responder	No	Yes	Yes
SSL	SSL-FIPS	No	No	No

Partitioning a NetScaler

Important

- Only superusers are authorized to create and configure admin partitions.
- Unless specified otherwise, configurations to set up an admin partition must be done from the default partition.

By partitioning a NetScaler appliance, you are in-effect creating multiple instances of a single NetScaler appliance. Each instance has its own configurations and the traffic of each of these partitions is isolated from the other by assigning each partition a dedicated VLAN or a shared VLAN.

A partitioned NetScaler has one default partition and the admin partitions that are created. To set up an admin partition, you must first create a partition with the relevant resources (memory, maximum bandwidth, and connections). Then, specify the users that can access the partition and the level of authorization for each of the users on the partition.

VLANs can be bound to a partition as a â€œDedicatedâ€• VLAN or a â€œSharedâ€• VLAN. Based on your deployment, you can bind a VLAN to a partition to isolate its network traffic from other partitions.

Dedicated VLAN â€“ A VLAN bound only to one partition with â€œSharingâ€• option disabled and must be a tagged VLAN. For example, in a client-server deployment, for security reasons a system administrator creates a dedicated VLAN for each partition on the server side.

Shared VLAN â€“ A VLAN bound (shared across) to multiple partitions with â€œSharingâ€• option enabled. For example, in a client-server deployment, if the system administrator does not have control over the client side network, a VLAN is created and shared across multiple partitions.

Important

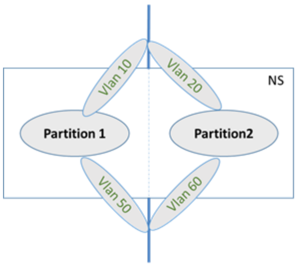
Citrix recommends you to bind a Dedicated or Shared VLAN to multiple partitions. You can bind only a tagged VLAN to a partition. If there are untagged VLANs, you must enable them as â€œSharedâ€• VLANs and then bind them to other partitions. This ensures that you control traffic packets (for example, LACP, LLDP, and xSTP packets) handled in the default partition. If you have already bound an untagged VLAN for a partition in 11.0, see â€œDeployment procedure for upgrading a sharable VLAN to NetScaler 11.1 softwareâ€• procedure.

VLAN Implementation

In a partitioned (multi-tenant) NetScaler appliance, a system administrator can isolate the traffic flowing to a particular partition or partitions by binding one or more VLANs to each partition. A VLAN can be dedicated to one partition or Shared across multiple partitions.

Dedicated VLANs

To isolate the traffic flowing into a partition, create a VLAN and associate it with the partition. The VLAN is then visible only to the associated partition, and the traffic flowing through the VLAN is classified and processed only in the associated partition.



To implement a dedicated VLAN for a particular partition, do the following.

1. Add a VLAN (V1).
2. Bind a network interface to VLAN as a tagged network interface.
3. Create a partition (P1).
4. Bind partition (P1) to the dedicated VLAN (V1).

To add a VLAN by using the command line interface

At the command prompt, type:

Adding a VLAN

```
add vlan <id>
```

Example

```
add vlan V1
```

To bind a VLAN by using the command line interface

At the command prompt, type:

Binding a VLAN

```
bind vlan <id> -ifnum <interface> -tagged
```

Example

```
bind vlan V1 â€“ifnum 1/8 -tagged
```

To create a partition by using the command line interface

At the command prompt, type:

Creating a Partion

```
Add ns partition <partition name> [-maxBandwidth <positive_integer>] [-maxConn
<positive_integer>] [-maxMemLimit <positive_integer>]
```

Example

```
Add ns partition P1 â€“maxBandwidth 200 â€“maxconn 50 â€“maxmemlimit 90

Done
```

To bind a partition to a VLAN by using the command line interface

At the command prompt, type:

Binding a Partition

```
bind partition <partition-id> -vlan <vlan>
```

Example

```
bind partition P1 â€“vlan V1
```

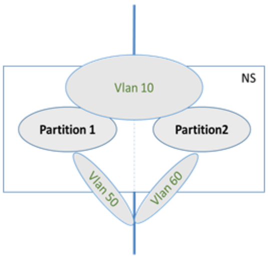
To configure a dedicated VLAN by using the NetScaler GUI

1. Navigate to **Configuration** > **System** > **Network** > **VLANs** and click **Add** to create a VLAN.
2. On the **Create VLAN** page, set the following parameters:
    a. VLAN ID
    b. Alias Name
    c. Maximum Transmission Unit
    d. Dynamic Routing
    e. IPv6 Dynamic Routing
    f. Partitions Sharing
3. In the **Interface Bindings** section, select one or more interfaces and bind it to the VLAN.
4. In the **IP Bindings** section, select one or more IP addresses and bind to the VLAN.
5. Click **OK** and **Done**.

Shared VLANs

In a shared VLAN configuration, each partition has a MAC address, and traffic received on the shared VLAN is classified by MAC address. Using a Layer3 VLAN is recommended, because it can restrict the subnet traffic.

The following diagram shows how a VLAN (VLAN 10) is shared across two partitions.



To deploy a shared VLAN configuration, do the following:

1. Create a VLAN with the sharing option â€˜enabledâ€™, or enable the sharing option on an existing VLAN. By default, the option is â€˜disabledâ€™.
2. Bind partition interface to shared VLAN.
3. Create the partitions, each with its own PartitionMAC address.
4. Bind the partitions to the shared VLAN.

To configure a shared VLAN by using the command line interface

At the command prompt, type one of the following commands to add a new VLAN or set the sharing parameter of an existing VLAN:

Configuring a Shared VLAN

```
add vlan <id> [-sharing (ENABLED | DISABLED)]

set vlan <id> [-sharing (ENABLED | DISABLED)]
```

Examples

```
add vlan V1 â€“sharing ENABLED

set vlan V1 â€“sharing ENABLED
```

To bind a partition to a Shared VLAN by using the command line interface

At the command prompt, type:

Binding a partition

```
bind partition <partition-id> -vlan <id>
```

Example

```
bind partition P1 â€“vlan
```

To create a shared partition by using the command line interface

At the command prompt, type:

Creating a Shared Partition

```
Add ns partition <partition name> [-maxBandwidth <positive_integer>] [-maxConn
<positive_integer>] [-maxMemLimit <positive_integer>] -partitionMAC<mac_addr>
```

Example

```
Add ns partition P1 â€“maxBandwidth 200 â€“maxconn 50 â€“maxmemlimit 90 -
partitionMAC<mac_addr

Done
```

To configure an existing partition as a shared partition by using the command line interface

At the command prompt, type:

Configuring an Existing Partition

```
set ns partition <partition name> [-partitionMAC<mac_addr>]
```

Example

```
set ns partition P1 â€“partitionMAC 22:33:44:55:66:77
```

To bind partitions to a shared VLAN by using the command line interface

At the command prompt, type:

bind partition <partition-id> -vlan <id>

bind partition <partition-id> -vlan <id>

Example

bind partition P1 â€“vlan V1

bind partition P2 â€“vlan V1

bind partition P3 â€“vlan V2

bind partition P4 â€“vlan V1

To configure Shared VLAN by using the NetScaler GUI

1. Navigate to **Configuration** > **System** > **Network** > **VLANs** and then select a VLAN profile and click **Edit** to set the partition sharing parameter.
2. On the **Create VLAN** page, select the **Partitions Sharing** checkbox.
3. Click **OK** and then **Done**.

Supporting VMACs on an SDX Platform

For shared VLAN to work in a partitioned deployment on a NetScaler SDX platform, you must log on to a Storage Virtualization Manager (SVM) appliance and assign each partition's MAC (VMAC) to a NetScaler VPX appliance.

Rate limits for an admin partition are as follows:

- **Maximum memory limit.** Must be configured as the memory that will be required for each admin partition. You must make sure that you set the appropriate value when creating the partition.

  Once an admin partition is created, the memory limit cannot be decreased. The memory limit can however be increased when required or more specifically, when there is execution failure due to insufficient memory in a partition; provided sufficient memory is available in the default partition.

  Note: From NetScaler 11.0 Build 64.x onwards, you can set the memory limit to a minimal value of 5 MB, when creating the admin partition. This setting can be useful for lighter deployments of the NetScaler appliance.

- **Maximum bandwidth.** The maximum bandwidth that can be used by an admin partition. This value must be limited to the appliance's licensed throughput. Otherwise, in effect, you are NOT limiting the bandwidth that can be used by the admin partition.

  It must be configured such that it accounts for the bandwidth that the application requires. If the application bandwidth exceeds the configured value, packets will be dropped. It accounts for incoming and outgoing packets.

  The maximum bandwidth can be increased or decreased when required.

  Note:
  - The default value is 10240 kbps, minimum value is 0, and maximum value is 4294967295 kbps.
  - Setting this parameter to its minimum value (0) means that you are not assigning any bandwidth to the partition. Traffic received for this partition will be dropped.
  - This is not the guaranteed bandwidth available for the admin partition. After a partition is configured with a maximum bandwidth value, the actual bandwidth assigned depends on the appliance's licensed throughput.

- **Maximum number of connections.** Must be configured such that it accounts for the maximum simultaneous flows expected within a partition. It is configured only on the client-side and not on the back-end server-side TCP connections. New connections cannot be established beyond this configured value.

  The maximum number of connections can be increased or decreased when required.

Note: When the bandwidth and number of connections crosses the threshold value, if SNMP is configured, traps will be sent with the relevant information.

Note

- After creating a partition, inform the users that the NetScaler configurations they perform will be isolated from users who are not members of the partition.
- Make sure the relevant users, command policies, VLANs, and bridgegroups are available on the NetScaler appliance.
- For deployments that have large size of NetScaler configuration and large quantum of traffic, Citrix advises that you increase the default values for the maximum memory limit, maximum bandwidth, and maximum number of connections.

To partition a NetScaler by using the command line interface

On the command prompt, do the following:

1. Create a partition and configure the NetScaler resources for that partition.

   add ns partition <partitionName> [-maxBandwidth <positive_integer>] [-maxConn <positive_integer>] [-maxMemLimit <positive_integer>]

   Note: Check the rate limiting content provided above for tips to update the maximum memory limit, maximum bandwidth, and maximum number of connections.
2. Associate the appropriate users with the partition.

   bind system user <name> -partitionName <string>
3. Specify the level of authorization for each user by associating one of the following command policies: *partition-operator, partition-read-only, partition-network, and partition-admin*.

   bind system user <name> <policyName> <priority>
4. Configure the VLAN through which traffic for this partition must be routed. You can use bridgegroups instead of VLANs to route the traffic.

   - Add the VLAN and bind the required interfaces to it.

     add vlan <id>

     bind vlan <id> -ifnum <interface>

     Note: When a VLAN is bound to an admin partition, its IP address bindings are lost. To make sure that the VLAN continues to have the IP address, create the IP address on the admin partition and then bind it to that VLAN.

   OR

   - Add the bridgegroup and bind the required VLANs to it.

     add bridgegroup <id>

     bind bridgegroup <id> -vlan <id>
5. Bind the VLAN or bridgegroup to the partition.

   bind ns partition <partitionName> -vlan <positive_ integer>

   OR

   bind ns partition <partitionName> -bridgegroup <positive_ integer>

   Note: Use the show vlan or the show bridgegroup command to view the partitions associated with that VLAN or bridgegroup.
6. Verify the configurations of the partition.

   show ns partition <partitionName>

   Note: You can also use the stat ns partition command to view partition configurations.

7. Save the configuration.

   ```
   save ns config
   ```

To partition a NetScaler by using the configuration utility

On the Configuration tab of the graphical user interface:

1. Navigate to System > Partition Administration, click Add and do the following:
   a. Create and configure the resources for the admin partition.
   b. Specify the VLANs or bridgegroups to be associated with the partition.
   c. Associate user(s) with the partition.
      Note: Make sure you bind users who are not yet associated with partition type command policies.
2. Navigate to System > User Administration, and to the partition user, bind the appropriate command policy. The command policy must be one of the `partition-` entries. The choice depends on the level of authorization you intend the user to have.
3. Save the configuration.

Configuring in a NetScaler Partition

Accessing a partitioned NetScaler is the same as accessing a non-partitioned NetScaler: through the NetScaler IP (NSIP) address or any other management IP address. As a user, after you provide your valid logon credentials, you are taken to the partition to which you are bound. Any configurations that you create are saved to that partition. If you are associated with more than one partition, you are taken to the first partition with which you were associated. If you want to configure entities on one of your other partitions, you must explicitly switch to that partition.

After accessing the appropriate partition, configurations that you perform are saved to that partition and are specific to that partition.

Note

- NetScaler superusers and other non-partition users are taken to the default partition.
- Users of all the 512 partitions can log in simultaneously.

Tip

To access a partitioned NetScaler appliance over HTTPS by using the SNIP (with management access enabled), make sure that each partition has the certificate of its partition administrator. Within the partition, the partition admin must do the following:

1. Add the certificate to the NetScaler.
   > **add ssl certKey** ns-server-certificate -**cert** ns-server.cert -**key** ns-server.key

2. Bind it to a service named "nskrpcs-<SNIP>-3009", where <SNIP> must be replaced with the SNIP address, in this case 100.10.10.1.
   > **bind ssl service** nskrpcs-100.10.10.1-3009 -**certkeyName** ns-server-certificate

To configure in a NetScaler partition by using the command line interface

1. Log on to the NetScaler appliance.

2. Check if you are in the correct partition. The command prompt displays the name of the currently selected partition.

   - If yes, skip to the next step.

   - If no, get a list of the partitions with which you are associated and switch over to the appropriate partition.

     - **show system user** <username>
     - **switch ns partition** <partitionName>

3. Now, you can perform the required configurations just as a non-partitioned NetScaler.

To configure in a NetScaler partition by using the configuration utility

1. Log on to the NetScaler appliance.

2. Check if you are in the correct partition. The top bar of the graphical user interface displays the name of the currently selected partition.

   - If yes, skip to the next step.

   - If no, navigate to **Configuration > System > Administrative Partitions > Partitions**, right-click the partition to which you want to switch, and select **Switch**.

3. Now, you can perform the required configurations just as a non-partitioned NetScaler.

Configuring an LACP Ethernet Channel on the Default Admin Partition

With Link Aggregation Control Protocol (LACP), you can combine multiple ports into a single, high-speed link (also called a channel). An LACP-enabled appliance exchanges LACP Data Units (LACPDU) over the channel.

There are three LACP configuration modes that you can enable in the default partition of a NetScaler appliance:

1. Active. A port in active mode sends LACPDUs. Link aggregation is formed if the other end of the Ethernet link is in the LACP active or passive mode.
2. Passive. A port in passive mode sends LACPDUs only when it receives LACPDUs. The link aggregation is formed if the other end of the Ethernet link is in the LACP active mode.
3. Disable. Link aggregation is not formed.

Note: By default, the link aggregation is disabled in the default partition of the appliance.

LACP exchanges LACPDU between devices connected by an Ethernet link. These devices are typically referred as an actor or partner.

A LACPDU data unit contains the following parameters:

- LACP Mode. Active, passive or disable.
- LACP timeout. The waiting period before timing out the partner or actor. Possible values: Long and Short. Default: Long.
- Port Key. To distinguish between the different channel. When key is 1, LA/1 is created. When key is 2, LA/2 is created. Possible values: Integer from 1 through 8. 4 through 8 is for cluster CLAG.
- Port Priority. Minimum value: 1. Maximum value: 65535. Default: 32768.
- System Priority. Uses this priority along with system MAC to form the system ID to uniquely identify the system during LACP negotiation with the partner. Sets system priority from 1 and 65535. The default value is set to 32768.
- Interface. Supports 8 interfaces per channel on NetScaler 10.1 appliance and supports 16 interfaces per channel on NetScaler 10.5 and 11.0 appliances.

After exchanging LACPDUs, the actor and partner negotiate the settings and decide whether to add the ports to the aggregation.

Configuring and Verifying LACP on a NetScaler appliance by using the command line interface

To configure and verify LACP on a NetScaler appliance by using the command line

1. Enable LACP on each interface.

At the command prompt, type:

```
set interface <Interface_ID> -lacpMode PASSIVE -lacpKey 1
```

When you enable LACP on an interface, the channels are dynamically created. Additionally, when you enable LACP on an interface and set lacpKey to 1, the interface is automatically bound to channel LA/1.

Note: When you bind an interface to a channel, the channel parameters take precedence over the interface parameters, so the interface parameters are ignored. If a channel was created dynamically by LACP, you cannot perform add, bind, unbind, or remove operations on the channel. A channel dynamically created by LACP is automatically deleted when you disable LACP on all interfaces of the channel.

2. Set the system priority.

At the command prompt, type:

```
set lacp -sysPriority <Positive_Integer>
```

3. Verify that LACP is working as expected.

```
show interface <Interface_ID>
```

```
show channel
```

```
show LACP
```

Note: In some versions of Cisco IOS, running the switchport trunk native vlan <VLAN_ID> command causes the Cisco switch to tag LACP PDUs. This causes the LACP channel between the Cisco switch and the NetScaler appliance to fail. However, this issue does not affect the static link aggregation channels configured in the above procedure.

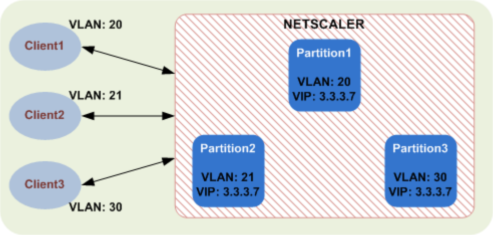
Use Case 1: Reusing the Same Identifier in Different Partitions

By using admin partitions, resource identifiers such as IP addresses and entity names can be reused in different partitions. This means that:

- You can use an IP address (for example, 3.3.3.7) as a virtual server IP address in different partitions.
- You can use the same name (for example, lbvserver1) for a virtual server in different partitions.

This is possible as each partition is associated with a different VLAN (or bridgegroup) and therefore traffic destined for different applications is segregated.

As shown in the following image, the virtual server IP address 3.3.3.7 is used in Partition1, Partition2, and Partition3.



Let us understand how the configurations must be performed.

Creating and configuring partitions that share the same IP address among virtual servers

1. **On default partition:** Log on to the NetScaler appliance as a super user and configure the three partitions as follows:

```
shell> ssh 10.102.29.60 -l nsroot
password: ******

> add ns partition Partition1
Done

> add ns partition Partition2
Done

> add ns partition Partition3
Done

> bind system user user1 -partitionName Partition1
Done

> bind system user user2 -partitionName Partition2
Done

> bind system user user3 -partitionName Partition3
Done

> bind system user user1 partition-admin 10
Done

> bind system user user2 partition-admin 20
Done

> bind system user user3 partition-admin 20
Done

> add vlan 20
Done

> bind vlan 20 -ifnum 2/1
Done

> add vlan 21
Done
```

```
> bind vlan 21 -ifnum 3/1
Done

> add vlan 30
Done

> bind vlan 30 -ifnum 4/1
Done

> bind ns partition Partition1 -vlan 20
Done

> bind ns partition Partition2 -vlan 21
Done

> bind ns partition Partition3 -vlan 30
Done
```

2. **On Partition1:** Log on to the NetScaler appliance as user1 and configure on Partition1.

```
shell> ssh 10.102.29.60 -l user1
password: *****

Partition1> add ns ip 3.3.3.2 255.255.255.0 -vServer DISABLED -type SNIP
Done

Partition1> add service s1 3.3.3.5 HTTP 80
Done

Partition1> add lb vserver lbvserver1 HTTP 3.3.3.7 80 -persistenceType NONE
Done

Partition1> bind lb vserver lbvserver1 s1
Done

Partition1> bind vlan 20 -IPAddress 3.3.3.2 255.255.255.0
Done
```

3. **On Partition2:** Log on to the NetScaler appliance as user2 and configure on Partition2.

```
shell> ssh 10.102.29.60 -l user2
password: *****

Partition2> add ns ip 5.5.5.3 255.255.255.0 -vServer DISABLED -type SNIP
Done

Partition2> add service s1 5.5.5.5 HTTP 80
Done

Partition2> add lb vserver lbvserver1 HTTP 3.3.3.7 80 -persistenceType NONE
Done

Partition2> bind lb vserver lbvserver1 s1
Done

Partition2> bind vlan 21 -IPAddress 5.5.5.3 255.255.255.0
Done
```

4. **On Partition3:** Log on to the NetScaler appliance as user3 and configure on Partition3.

```
shell> ssh 10.102.29.60 -l user3
password: *****

Partition3> add ns ip 6.6.6.3 255.255.255.0 -vServer DISABLED -type SNIP
Done

Partition3> add service s1 6.6.6.6 HTTP 80
Done

Partition3> add lb vserver lbvserver1 HTTP 3.3.3.7 80 -persistenceType NONE
Done
```

```
Partition3> bind lb vserver lbvserver1 s1
Done

Partition3> bind vlan 30 -IPAddress 6.6.6.3 255.255.255.0
Done
```

Use Case 2: Upgrading a Partition Deployment in a HA Setup

When upgrading NetScaler appliances in a high availability setup to software release 11.1, be sure to upgrade the secondary appliance first, and then upgrade the primary appliance.

Note: If you encounter any issues during the upgrade, roll back to version 11.0 for services managed by the NetScaler appliance.

> **Warning**
>
> Any customization within the partitioned appliance might cause an unexpected behavior during or after the upgrade process. This might lead to a configuration loss. Therefore, be sure to back up the running configuration of each admin partition and default partition before you begin the upgrade.

> **Important**
>
> The deployment described here is applicable when you have untagged VLANs passing through the port interface and bound to admin partitions.

There are two ways of implementing this deployment on a partitioned appliance.

1. Tagging few VLANs before deploying NetScaler 11.1
2. Enabling VLANs as "Shared" after deploying NetScaler 11.1

Tagging VLANs before deploying NetScaler 11.1

1. Before you begin the upgrade on the secondary appliance, make a few VLANs tagged members of the port interface. For example:
   >bind partition p1 - vlan 10
   > unbind vlan 10 -ifnum 1/2
   >Done
   > bind vlan 10 -ifnum 1/2 -tagged
   >Done
2. Access the secondary NetScaler appliance by entering its NSIP address in an SSH utility, such as PuTTY, and use the nsroot credentials to log on to the appliance.
3. From the command line interface of the appliance, type the "save configuration" command to save the existing configuration.
4. Switch to the shell prompt
   - *login as: username*
   - *Using keyboard-interactive authentication.*
   - *Password:*
   - *Last login: Wed Jun 24 14:59:16 2015 from 10.252.252.65*
   - *Done*
   - *shell*
   - *Copyright (c) 1992-20*
5. Run the following command to change to the default installation directory: *cd/var/nsinstall*
6. Run the following command to create a temporary subdirectory of the nsinstall directory:
   - *# mkdir x.xnsinstall* **Note**: The text x.x is used to name the NetScaler version for future configurations. For example, the directory for the installation files of NetScaler 11.1 will be called 11.1 nsinstall.
7. Change to the x.xnsinstall directory.
8. Download the installation package and documentation bundle, such as "ns-x.0-xx.x-doc.tgz", to the temporary directory created in Step 4. **Note:** Some builds do not have a documentation bundle. Installing the documentation is optional.
9. Click the **Documentation** tab from the GUI to access the documentation.
10. Before you run the install script, the files must be extracted and placed on the appliance. Use the following command to uncompress the bundle downloaded from Citrix website.

- *tar -zxvf ns-x.0-xx.x-doc.tgz where*
- *z = The file is a "gzipped" file*
- *x = Extract files*
- *v = Print the file names as they are extracted one by one*
- *f = Use the following tar archive for the operation*

11. Run the following command to install the downloaded software.
    - *# ./installns*   **Note:** If the appliance does not have sufficient disk space to install the new kernel files, the installation process performs an automatic cleanup of the flash drive.
12. After the installation process is completed you are prompted to restart the appliance. Press y to restart the appliance.
13. Upgrade the secondary appliance to release 11.1, and then perform a force failover to make the secondary appliance primary.
    - *> force failover*
14. Access the new secondary appliance (formerly the primary) by entering its NSIP address in an SSH utility, such as PuTTY, and use the nsroot credentials to log on to the appliance.
15. Repeat steps 3 through 13 to upgrade the current secondary appliance to release 11.1.
16. After the installation process is complete, you are prompted to restart the appliance. Press y to restart the appliance.
17. From the command line interface of the secondary appliance, type the following command to save the running configuration: save config
18. Run "save config" command to make the secondary appliance is the primary appliance.
19. Run "> force failover" command to make the secondary appliance is the primary appliance.
20. Verify the appliance is now the primary appliance.
21. After upgrading both the primary and secondary appliances, enable the tagged VLANs as "Shared". This is a preferred choice as you will not encounter a configuration loss during upgrade.

Enabling VLANs as "Shared" after NetScaler 11.1 deployment

This scenario is about untagged VLANs and how to enable it as shared for VLAN deployment from an earlier release to 11.1 release. This is a least preferred scenario as it involves configuration loss during the software upgrade.

1. Follow steps 2 to 20 of the previous procedure to upgrade the secondary appliance with NetScaler 11.1 software.
2. After you have upgraded the software on the secondary appliance, VLAN bindings to partitions are lost, and the configuration depends on the VLAN inside the partition during the upgrade process.
3. Now enable the untagged VLANs of any port interface "Shared" and bind the "Shared" VLAN to the partitions and configure the VLAN inside each partition. Note: Make sure you first enable the untagged VLANs as shared before you bind it to a partition.
    - *unbind partition p1 -vlan 10*
    - *Done*
    - *set vlan 10 -sharing enabled*
    - *Done*
    - *bind partition p1 -vlan 10*
    - *Done*
4. From the command line interface of the appliance, type "save config" command to save the configuration in all the affected partition and the default partition.
5. If the appliance is not a primary appliance, run the "> force failove" command to perform a force failover to ensure that the appliance is a primary appliance.
6. Upgrade the new secondary (formerly the primary) appliance with NetScaler 11.1 software and reboot it to synchronize its configuration from the primary appliance.
7. From the command line interface of the primary appliance, type the "save config" command to save the configuration in the primary appliance.
8. If the appliance is not a primary appliance, run the "> force failover" command to perform a force failover to ensure that the appliance is a primary appliance.
9. Verify that the appliance is a primary appliance.

FAQs

Where can I get the NetScaler configuration file for a partition?

The configuration file (*ns.conf*) for the default partition is available in the */nsconfig* directory. For admin partitions, the file is available in the */nsconfig/partitions/<partitionName>* directory.

How can I configure integrated caching in a partitioned NetScaler appliance?

Note: Integrated caching in admin partitions is supported from NetScaler 11.0 onwards.

To configure integrated caching (IC) on a partitioned NetScaler, after defining the IC memory on the default partition, the superuser can configure the IC memory on each admin partition such that the total IC memory allocated to all admin partitions does not exceed the IC memory defined on the default partition. The memory that is not configured for the admin partitions remains available for the default partition.

For example, if a NetScaler appliance with two admin partitions has 10 GB of IC memory allocated to the default partition, and IC memory allocation for the two admin partitions is as follows:

- Partition1: 4 GB
- Partition2: 3 GB

Then, the default partition has 10 - (4 + 3) = 3 GB of IC memory available for use.

Note: If all IC memory is used by the admin partitions, no IC memory is available for the default partition.

What is the scope for L2 and L3 parameters in admin partitions?

Note: Applicable from NetScaler 11.0 onwards.

On a partitioned NetScaler appliance, the scope of updating the L2 and L3 parameters is as follows:

- For L2 parameters that are set by using the "set L2Param" command, the following parameters can be updated only from the default partition, and their values are applicable to all the admin partitions:

  maxBridgeCollision, bdgSetting, garpOnVridIntf, garpReply, proxyArp, resetInterfaceOnHAfailover, and skip_proxying_bsd_traffic.

  The other L2 parameters can be updated in specific admin partitions, and their values are local to those partitions.

- For L3 parameters that are set by using the "set L3Param" command, all parameters can be updated in specific admin partitions, and their values are local to those partitions. Similarly, the values that are updated in the default partition are applicable only to the default partition.

How to enable dynamic routing in an admin partition?

Note: Dynamic routing in admin partitions is supported from NetScaler 11.0 onwards.

While dynamic routing (OSPF, RIP, BGP, ISIS, BGP+) is by default enabled on the default partition, in an admin partition, it must be enabled by using the following command:

> **set L3Param** -dynamicRouting ENABLED

Note: A maximum of 63 partitions can run dynamic routing (62 admin partitions and 1 default partition).

On enabling dynamic routing on an admin partition, a virtual router (VR) is created.

- Each VR maintains its own vlan0 which will be displayed as vlan0_<partition-name>.
- All unbound IP addresses that are exposed to ZebOS are bound to vlan0.
- The default VR (of the default partition) shows all the VRs that are configured.
- The default VR shows the VLANs that are bound to these VRs (except default VLANs).

Where can I find the logs for a partition?

NetScaler logs are not partition-specific. Log entries for all partitions must be stored in the */var/log/* directory.

How can I get auditlogs for an admin partition?

In a partitioned NetScaler, you cannot have specific log servers for a specific partition. The servers that are defined at the default partition are applicable across all admin partitions. Therefore, to view the audit logs for a specific partition, you will have to use the "show audit messages" command.

Note: The users of an admin partition do not have access to the shell and therefore are not able to access the log files.

How can I get web logs for an admin partition?

You can get the web logs for an admin partition as follows:

- **For NetScaler 11.0 and later versions**

  The web logging feature must be enabled on each of the partitions that require web logging. Using the NetScaler Web Logging (NSWL) client, the NetScaler retrieves the web logs for all the partitions with which the user is associated.

- **For versions prior to NetScaler 11.0**

  Web logs can be obtained only by nsroot and other superusers. Also, even though web logging is enabled on the default partition, the NetScaler Web Logging (NSWL) client fetches web logs for all the partitions.

To view the partition for each log entry, customize the log format to include the %P option. You can then filter the logs to view the logs for a specific partition.

How can I get the trace for an admin partition?

You can get the trace for an admin partition as follows:

- **For NetScaler 11.0 and later versions**

  In a partitioned NetScaler appliance, the nstrace operation can be performed on individual admin partitions. The trace files are stored in the */var/partitions/<partitionName>/nstrace/*directory.

  Note: You cannot get the trace of an admin partition by using the NetScaler GUI. You must use the NetScaler CLI.

- **For versions prior to NetScaler 11.0**

  The nstrace operation can only be performed on the default partition. Therefore, packet captures are available for the entire NetScaler system. To get partition-specific packet captures, use VLAN-ID based filters.

How can I get the technical support bundle specific to an admin partition?

To get the tech support bundle for a specific partition, you must execute the following command from the default partition:

```
> show techsupport -scope partition -partitionname <string>
```

Note: This command also gives system-specific information.