ACOS 6.0.8

Configuring Application Delivery Partitions

December, 2025

Information in this document is subject to change without notice.

PATENT PROTECTION

A10 Networks, Inc. products are protected by patents in the U.S. and elsewhere. The following website is provided to satisfy the virtual patent marking provisions of various jurisdictions including the virtual patent marking provisions of the America Invents Act. A10 Networks, Inc. products, including all Thunder Series products, are protected by one or more of U.S. patents and patents pending listed at:
a10-virtual-patent-marking.

TRADEMARKS

A10 Networks, Inc. trademarks are listed at: a10-trademarks

CONFIDENTIALITY

This document contains confidential materials proprietary to A10 Networks, Inc. This document and information and ideas herein may not be disclosed, copied, reproduced or distributed to anyone outside A10 Networks, Inc. without prior written consent of A10 Networks, Inc.

DISCLAIMER

This document does not create any express or implied warranty about A10 Networks, Inc. or about its products or services, including but not limited to fitness for a particular use and non-infringement. A10 Networks, Inc. has made reasonable efforts to verify that the information contained herein is accurate, but A10 Networks, Inc. assumes no responsibility for its use. All information is provided "as-is." The product specifications and features described in this publication are based on the latest information available; however, specifications are subject to change without notice, and certain features may not be available upon initial product release. Contact A10 Networks, Inc. for current information regarding its products or services. A10 Networks, Inc. products and services are subject to A10 Networks, Inc. standard terms and conditions.

ENVIRONMENTAL CONSIDERATIONS

Some electronic components may possibly contain dangerous substances. For information on specific component types, please contact the manufacturer of that component. Always consult local authorities for regulations regarding proper disposal of electronic components in your area.

FURTHER INFORMATION

For additional information about A10 products, terms and conditions of delivery, and pricing, contact your nearest A10 Networks, Inc. location, which can be found by visiting www.a10networks.com.

Table of Contents

Getting Started

Each ACOS device includes a default partition called the shared partition; when you access and configure the device, you are making changes on the shared partition.

It is also possible to create additional partitions on the ACOS device, called Application Delivery Partitions (ADPs). These “private” partitions can provide aggregated networking and system services, application resources, and administrative and management capabilities.

There are two types of partitions that can be created to segment your ACOS device:

- Layer 3 Virtualization (L3V) partitions are network-enabled partitions.
- Service partitions (SvP) are non-network-enabled partitions.

The following topics are covered:

Overview

ACOS is initially provisioned with one partition (named *shared*). Additional partitions can be added to the device through CLI and GUI commands. An Application Delivery Partition (ADP) is a partition that is added to the device. An administrator account with root access has read-write privileges to all ACOS objects across all partitions. ADPs are also referred to as *Private Partitions*.

ACOS is also initially provisioned with one administrator account (named *admin*). The *admin* account has root access to the device ACOS. Additional administrator accounts can be added to the device. The accounts can be configured to provide full access to all partitions on the device or to restrict access to specific partitions.

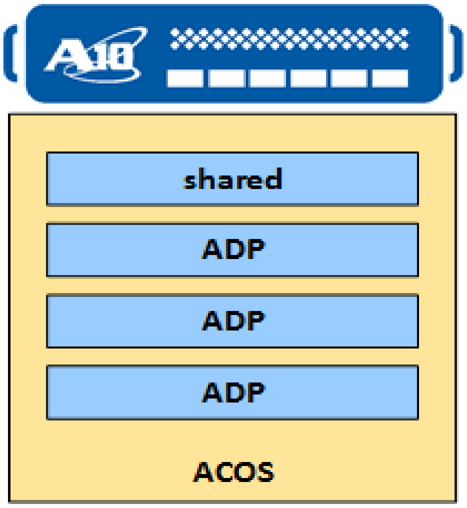
NOTE: Configuring administrator accounts is described in *Management Access and Security Guide*.

When ACOS is in its default state, all configurations run in the shared partition. Isolating configurations from each other, as if they are on multiple separate ACOS devices, requires the configuration of ADPs, as illustrated in (Figure 1).

An ACOS object that is configured in the shared partition is available to processes and users of all ADPs. An ACOS object that is created in a private partition is available only to processes and users in that partition. Partitioning is a method of logically segmenting an ACOS device to support separate systems for separate customers. Communication between partitions is through routed interfaces.

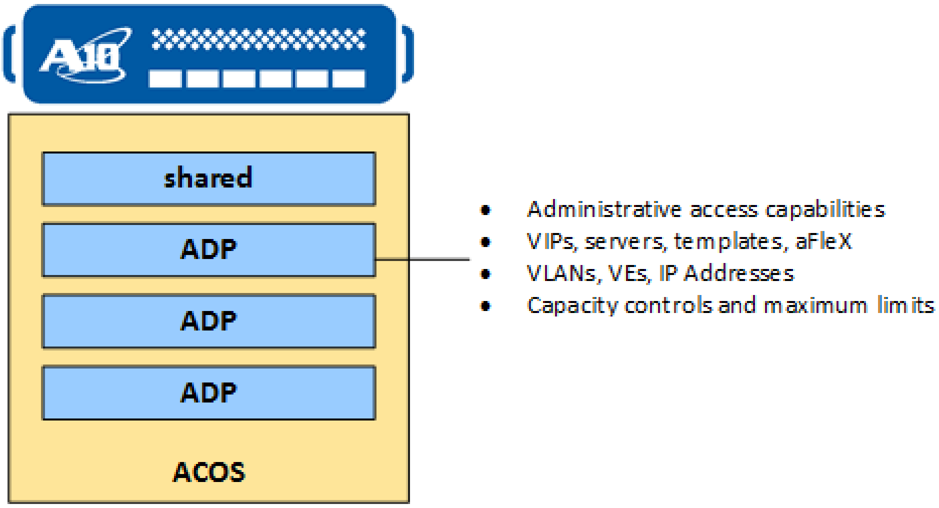
NOTE: For details on how to create administrator accounts, see the section “Overview of Administrator Accounts” in the *Management Access and Security Guide*.

Figure 1 : Application Delivery Partitions



Each partition may provide aggregated services, including networking, system, and application resources. Each partition can be administered and monitored separately (Figure 2).

Figure 2 : Partition Resources


shared
ADP
ADP
ADP
ACOS
Administrative access capabilities
VIPs, servers, templates, aFleX
VLANs, VEs, IP Addresses
Capacity controls and maximum limits

NOTE: Also see "Configuring Admin Access to Partitions" and "Configuring Partition Admin Accounts" in this document for additional information administrator accounts.

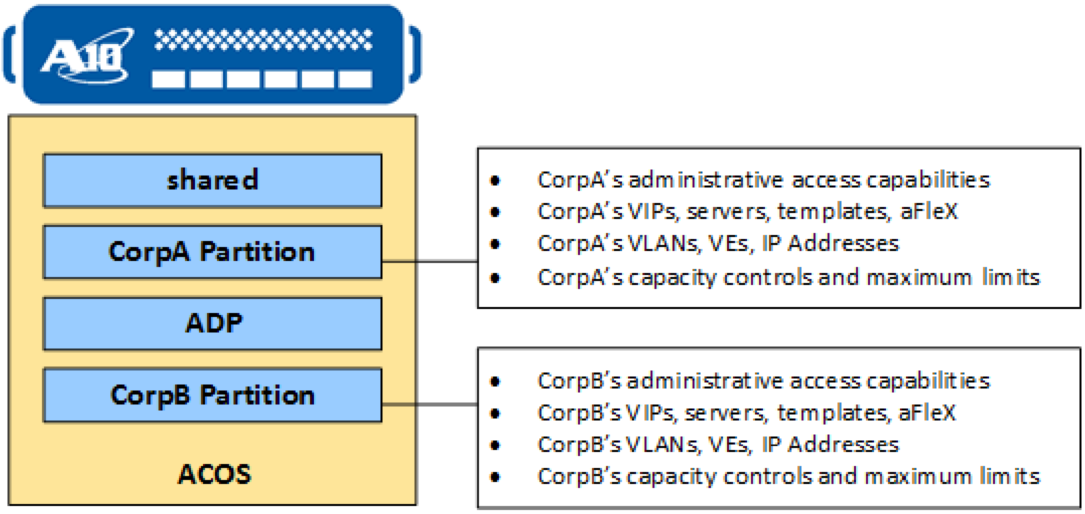
Partition Benefits

Partitioning allows the ACOS device to be logically segmented to support separate configurations for different customers. This provides isolation of configuration objects and isolates administration of these components.

For example, separate companies or separate departments within an enterprise may prefer to have their content isolated from other departments.

Figure 3 shows an example with a service provider hosting an ACOS device shared by two companies CorpA.com and CorpB.com. Each company has its own dedicated servers that they want to manage in entirety. The partition for CorpA.com contains CorpA.com's SLB resources. Likewise, the partition for CorpB.com contains CorpB.com's SLB resources.

Figure 3 : Example of Multiple Partitions


A10
shared
CorpA Partition
ADP
CorpB Partition
ACOS
CorpA's administrative access capabilities
CorpA's VIPs, servers, templates, aFleX
CorpA's VLANs, VEs, IP Addresses
CorpA's capacity controls and maximum limits
CorpB's administrative access capabilities
CorpB's VIPs, servers, templates, aFleX
CorpB's VLANs, VEs, IP Addresses
CorpB's capacity controls and maximum limits

Admins assigned to the partition for CorpA.com can add, modify, delete and save only those resources contained in CorpA.com's partition. Likewise, CorpB.com's admins can add, modify, delete and save only the resources in CorpB.com's partition.

NOTE: For more information about administrative roles, refer to Configuring Admin Access to Partitions.

Types of Partitions

This section describes each partition type.

The following topics are covered:

Shared Partition

Every ACOS device contains one shared partition. By default, this is the only partition on the device and cannot be deleted. If there are no additional partitions on the device, all configuration changes take place in the shared partition.

NOTE: If you create any L3V or Service partitions, you must explicitly switch to that partition for your configuration changes to take effect in the desired partition.

L3V Partitions

Partitions that provide Layer 3-7 support are referred to as L3V partitions. Each L3V partition can contain either SLB or CGN application resources, networking resources, and system resources. In essence, each L3V partition can operate as an independent ACOS device. An L3V partition can be created, configured and deleted by a root admin and configured by a partition admin.

The partition admin has access to configure all applications, network, and system resources within the partition.

NOTE: A partition admin account can be created in the L3V partition using the `admin` or `partition-admin` command. When the partition-admin command is used, the created user is valid even if the creator admin user is removed. For more information about `partition-admin` command, see the *Command Line Interface Reference* guide .

For system and network resources, the partition admin will depend on the root admin for configuration help.

NOTE:

- The L3V partition is not supported in transparent mode.
- For details on L3V partitions and supported resources, see Understanding L3V Partitions.

Service Partitions

Partitions that provide Layer 4-7 support are referred to as Service partitions, which can contain SLB application resources. A service partition can be created, configured and deleted by a root admin and configured by a partition admin. A service partition is created from the shared partition and accesses network resources from the shared partition.

The partition admin has access to configure all applications within the partition. For system and network resources, the partition admin will depend on the root admin for configuration help.

NOTE: For details on Service partitions and supported resources, see Understanding Service Partitions.

Working with Application Delivery Partitions

The following topics are covered:

Administering ADP Partitions

The following topics are covered:

Overview

To administer an ADP partition, you must have the appropriate privilege level. Only a “root administrator” can assign privileges to the partition admins. For details on configuring admin accounts and privileges, refer to Configuring Partition Admin Accounts.

Once within an ADP partition, if you only have read access, you will not be able to enter the config mode. You can use show commands only.

For example:

```
ACOS[partition1]> enable
Password:
ACOS[partition1]#
ACOS[partition1]# config
Permission denied: Insufficient privilege
```

Other than a "`root administrator`" a partition admin is only able to make configuration changes inside the partition for which they have privileges.

Configuring Admin Access to Partitions

Admins with Global Read/Write privileges (also known as "root admins") can configure other admin accounts, including partition admin accounts.

The following privilege levels are supported:

- Global privileges:
  - read
  - write
- Partition privileges:
  - Partition-enable-disable
  - Partition-read
  - Partition-write

Table 1 describes the privilege levels.

Table 1 : Admin Privilege Levels and Partition Access

Privilege Level	Access to Shared Partition	Access to L3V Partition
Global read	Read-only; unable to enter Global configuration mode.	Read-only; unable to enter Global configuration mode.
Global write	Read-Write; has access to all resources.	Read-Write; has access to all resources.
Partition-read	No access	Read-only; unable to enter Global configuration mode in the partition. All access is restricted to the partition to which the admin is assigned.
Partition-write	No access	Read-write for all resources in the partition. All access is restricted to the

Table 1 : Admin Privilege Levels and Partition Access

Privilege Level	Access to Shared Partition	Access to L3V Partition
		partition to which the admin is assigned.

Additional Administrative Capabilities

The following information highlights what administrators can or cannot do within an ADP partition:

- System and networking resources can be configured only by admins with Global write privileges. An admin with such privileges can configure system and networking resources for all partitions.
- An ADP partition can be configured and accessed only by the admins who are assigned to it, and by admins with Global read or Global write privileges.
- Admins assigned to an ADP partition can manage only the resources inside that partition.

Configuring Partition Admin Accounts

The partition admin accounts can be configured using the `admin` or `partition-admin` command. Although these commands are similar, when the `partition-admin` command is used, the created user is valid even if the creator admin user is removed. Also, the `partition-admin` command is supported only for L3V partition, Service Partitions are not supported.

This section describes the steps to configure admin account using the `admin` command.

NOTE: To configure an admin account for an L3V partition, follow the instructions in the *Management Access and Security Guide*.

The following example creates a new admin named “exampleadmin” with the password of “a10”. This is the default password if you choose not to specify a password here:

```
ACOS(config)# admin exampleadmin password a10
ACOS(config-admin:exampleadmin)#
```

These commands grant Partition-write privileges to the "exampleadmin" user for partition companyA:

```
ACOS(config-admin:exampleadmin)# privilege partition-write companyA
Modify Admin User successful!
ACOS(config-admin:exampleadmin)#
```

NOTE: To delete an admin account, see "Delete an Admin Account" in the *Management Access and Security Guide*.

Partition-Based Banners

Admins with the "write" or "write partition" access privilege level can configure the banner message displayed when the Privileged EXEC level of the CLI is accessed by a partition admin.

You may configure the default as a single or multiple lines.

NOTE: For details on configuring banners using the CLI or GUI, refer to "Configuring Basic System Parameters" in the *System Configuration and Administration Guide*.

Limiting Resources for Partitions Using Templates

Resource templates will help establish resource limits per partition. In this way, no one partition will monopolize all available resources. For details, refer to Resource Templates for L3V Partitions.

Enabling SLB or CGN in a Partition

The following topics are covered:

Overview

All ACOS devices, including physical devices (A10 Thunder Series and ACOS Series devices) and virtual devices (vThunders), support running both SLB and CGN on the same device, but in separate partitions. A partition can support either SLB or CGN, one of which must be explicitly enabled in that partition. Neither SLB nor CGN are enabled by default. When one is enabled, the other one is blocked.

NOTE: Service Partitions only support SLB.

Configuring Partition Type Using GUI

This section describes how to use the GUI to configure the application type in a partition.

Configuring Application Type in the Shared Partition

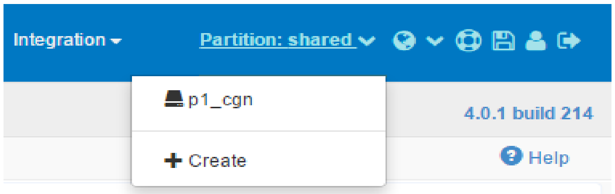
In the shared partition, there is no mechanism in the GUI to explicitly define the application type. Once you configure an SLB object, all CGN options will be blocked, or if you configure a CGN object then all SLB objects will be blocked.

Configuring Application Type in an L3V Partition

For L3V partitions, you can configure the application type when you create the partition.

1. Navigate to **System > Admin** and the click **Partitions** tab.
2. Click **Create** to create a new partition.
3. On the Create Partitions screen, specify the partition name, ID, and application type (ADC or CGN).
4. When the partition is created, use the **Partition** menu to switch to the new partition (“**p1-cgn**”).

NOTE: Observe that the name of the partition in the menu bar is changed from “**shared**” to “**p1_cgn**”.



Configuring Partition Type Using CLI

To configure the partition type from the CLI, use the **application-type** parameter in the partition creation command (**partition** or **service-partition**). For example, to create an L3V partition named “p1” and enable SLB in that partition:

```
ACOS(config)# partition p1 id 1 application-type adc
```

All CGN commands are blocked in partition p1. If you create an L3V partition without using the **application-type** parameter, then by default both SLB and CGN commands are available. Once an object for one application type is configured, the commands for the other application type are disabled.

When creating a Service partition, the **application-type** parameter is mandatory.

CGN Commands for CGN-Enabled Partitions

CGN-enabled partitions support a dedicated command set that parallels the commonly used SLB commands.

The following table provides a list of SLB commands and their CGN equivalents, ensuring smooth transition between application types.

Table 2 : SLB Commands and CGN Equivalents

SLB Commands	CGN Commands
slb server	**cgnv6 server**
slb virtual-server	**cgnv6 dns64-virtualserver**
slb service-group	**cgnv6 service-group**
slb template policy	**cgnv6 template-policy**
slb template dns	**cgnv6 template dns**
ip nat inside source static	**cgnv6 nat inside source static**
ip nat range-list	**cgnv6 nat range-list**

The CGN commands mirror the SLB commands and make CGN self-sufficient within a partition. As a result, CGN can be enabled independently without relying on SLB constructs. This allows both CGN and SLB to be configured and operated separately within the same partition.

Managing Partitions

The following topics are covered:

Switching To Another Partition

Admins with Read Write or Read Only privileges can select the partition to view. When an admin with one of these privilege levels logs in, the view is set to the shared partition by default, which means all resources are visible.

To change the view to an ADP partition, use either of the following methods.

GUI Configuration

On the title bar, select the **partition** from the Partition drop-down list.

You will be asked to confirm that you want to switch partitions.

CLI Configuration

Use the **active-partition** command at the Privileged EXEC level of the CLI. For example, if you are in the shared partition and you want to switch to companyA, use:

```
ACOS# active-partition companyA
Current active partition: companyA
ACOS[companyA]#
```

The name of the active partition is shown in the CLI prompt.

Deleting a Partition

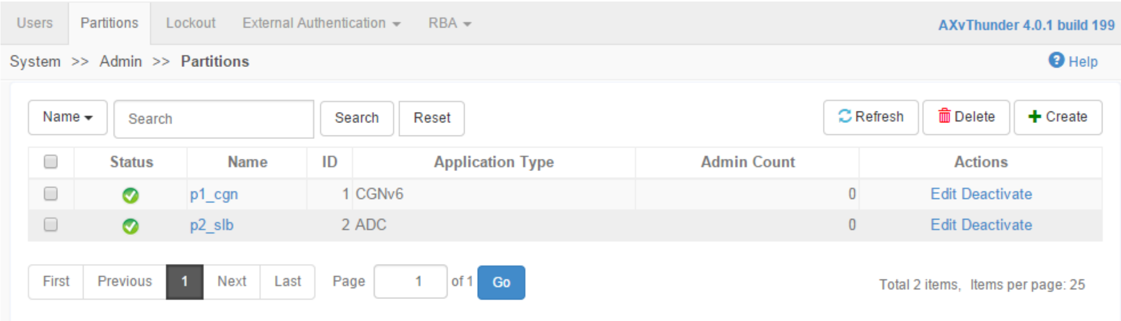
Only an admin with Read Write privileges can delete a partition. When a partition is deleted, all resources within the partition also are deleted.

When you delete a partition, resources associated with the partition are permanently deleted. This includes SSL certificates and keys, and aFleX scripts. These resources are deleted even if you reload or reboot without saving the configuration. In this case, the partition configuration is restored but the resources are still gone.

GUI Configuration

1. Navigate and expand over **System** in the menu bar, then click **Admin**.
2. Click **Partitions** tab.
3. For the partition you want to delete, select the **Deactivate** link in the Action column for that partition.

   When the partition is deactivated, the icon in the Status column should change to a red circle with an "**X**" in it.
4. After the partition is deactivated, click the checkbox next to the partition name, then click **Delete**.



□	Status	Name	ID	Application Type	Admin Count	Actions
□	✓	p1_cgn	1	CGNv6	0	Edit Deactivate
□	✓	p2_slb	2	ADC	0	Edit Deactivate

CLI Configuration

To delete a partition, use the commands shown in the example below:

```
ACOS(config)# no partition companyA id 1
Remove this partition and keep configurations on the disk? (y/n)y
ACOS(config)# delete partition companyA id 1
The operation will delete this partition permanently from all profiles
on disk.
This action is not recoverable. Continue? [yes/no]: yes
```

The **no partition** command unloads the partition but keeps the configuration on your system. Permanently deleting the partition and associated configuration requires the **delete partition** command.

Table 3 summarizes the CLI commands available to remove partitions or partition configurations.

Table 3 : Working with Private Partitions in the CLI

CLI Command	Description
no partition	Unload the specified partition from the running-configuration of the shared partition. To also remove the configuration from the startup configuration, use the **write memory** command after using the **no partition** command.
delete partition	Remove the specified partition and its associated configuration from the disk. The command is only valid on a partition that has already been unloaded with the **no partition** command.
erase	Erase the startup configuration file in the shared partition. Existing private partitions are preserved on the disk, and are loaded when the partition is configured again from the shared partition. See “erase” in the *Command Line Interface Reference* for more information.
system-reset	Reset the device back to its original factory settings. All startup configurations and private partition configurations are removed. See “system-reset” in the *Command Line Interface Reference* for more information.

Managing Partition Configurations

The following topics are covered:

Viewing Partition Configuration

Admins with Partition-write or Partition-read privileges can view resources in any partition.

Admins assigned to a partition can view the resources in the shared partition and in their own private partition but not in any other private partition.

To view the partitions configured on the device, use the **`show running-config partition`** command:

```
ACOS(config)# show running-config partition
!Section configuration: 96 bytes
!
partition p1-cgn id 1 application-type cgnv6
!
partition p2-slb id 2 application-type adc
!
!
end
```

You can specify a partition-name to view only the resources in the specified partition.

To view the running-config for all partitions, the shared, or a specific ADP partition on the system, use the **`show partition-config`** `{`**`all`** `|` **`shared`** `|` *`partition-name`*`}` command. You can specify a *`partition-name`* at the end of the command to view only the resources in the specified partition:

```
ACOS(config)# show partition-config p1
!
active-partition p1
!
end
```

Saving Partition Configuration

The following topics are covered:

Admins with Global write privileges can save resources in any partition. Admins with Partition-write privileges can save only the resources within their own partition.

To save the configuration on an ACOS device configured with private partitions, use one of the methods mentioned below.

GUI Configuration

1. To save the configuration in the GUI, click the **Save***icon* on the title bar.
2. The GUI automatically saves only the resources that are in the current partition view.

For example, if the partition view is set to the “**companyA**” L3V partition, only the resources in that partition are saved.

CLI Configuration

To save the configuration for the current partition, use the **write memory** [**all-partitions** | **partition** {**shared** | *part-name*}] command.

If you have multiple partitions and want to save the configuration changes for all of them with a single command, use the **all-partitions** command to save changes for all resources in all partitions:

CAUTION: Before saving all partitions or before a reload, reboot, or shutdown operation, a root admin should notify all partition admins to save their configurations. Saving all partitions without consent from the partition admins is not recommended.

The **all-partitions** and **partition** *partition-name* options are not applicable for admins with Partition-write privileges. Partition admins can only save their respective partitions. For these admins, the command syntax is the same as in previous releases. The options are available only to admins with Global Write privileges.

A configuration can be saved either to the default startup-config, the current, or a new configuration profile.

By default, when a new ADP partition is created, configuration changes made to this new ADP partition is saved according to the shared partition configuration.

Depending on the configuration profile and the partition being saved to, the following summarizes the usages of the **`write memory`** command in the context of saving partition configuration:

- Use the **`write memory`** command to save the running configuration to the startup-config or the current profile in the current partition.
- Use the **`write memory all-partitions`** command to save the running configuration to their respective startup-config or their current profiles of all partitions.
- Use the **`write memory`** <*`profile-name`*> command to save the running configuration to the new <*`profile-name`*> profile in the current partition.
- Use the **`write memory`** <*`profile-name`*> **`all-partitions`** command to save the running configuration to the new <*`profile-name`*> profile of all partitions.

Manually Synchronizing Configurations of All Partitions Between ACOS Devices

The `configure sync` command is used to manually synchronize the running-config and startup-config of all the partitions such as Shared Partition, L3V Partition, and Service Partition from one ACOS device to another ACOS device.

This feature is supported for the ACOS devices that are deployed in VRRP-A or non-VRRP-A environments.

For example, consider a scenario with Thunder devices T1 and T2 in a VRRP-A environment.

Configuration synchronization is permitted in the following scenarios:

- From T1 Shared partition to T2 Shared/L3V/Service partition

- From T1 all partitions including shared to T2 all partitions including shared partitions.
- From T1 L3V partition to and the same T2 L3V partition
- From T1 Service partition to the same T2 Service partition

NOTE: Only running and startup configurations are synchronized; while the device-specific configurations, such as interface configurations, are not synchronized.

For more information about configuration options, see configure sync in the ***Command Line Reference Guide***. For information on configuration objects that are included or not included in a manual synchronization, see the appropriate topic below

NOTE: Manual configuration is not necessary for running ACOS Virtual Chassis System (aVCS). For more information, see the Configuration Synchronization without Reload section in the Configuring ACOS Virtual Chassis Systems Guide.

For more information, see ***System Configuration and Administration Guide***.

Understanding L3V Partitions

This section provides information about L3V partitions.

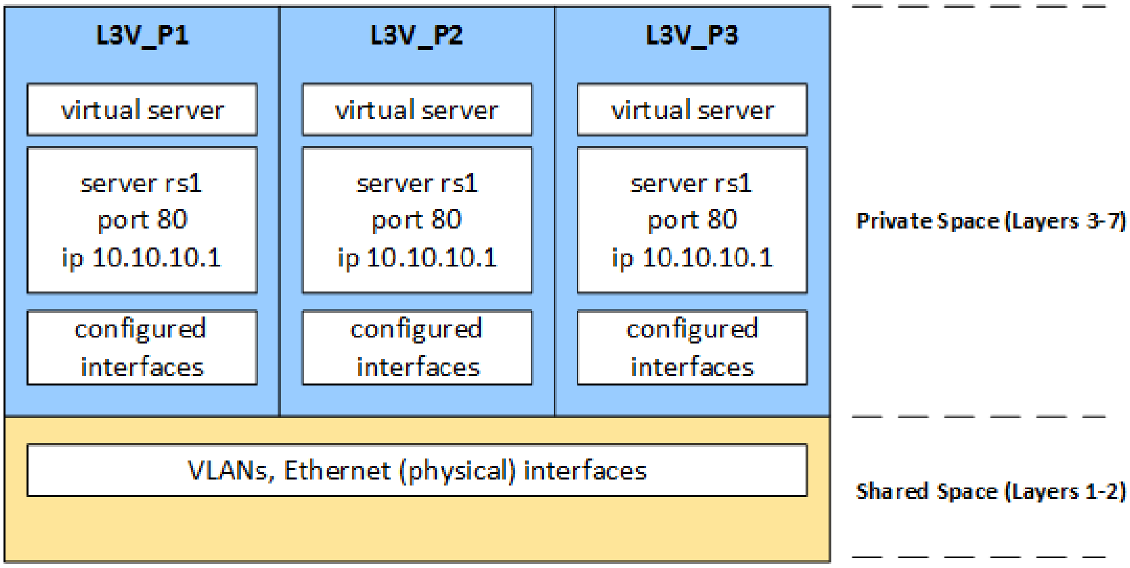
The following topics are covered:

Overview

L3V partitions provide a mechanism to segment a single ACOS device into multiple instances that behave independent of each other. Layer 3 Virtualization (L3V) in each partition allows admins with the proper privileges to configure and view network, SLB, and CGN resources.

Figure 4shows how an ACOS device can be carved into separate L3V partitions.

Figure 4 : L3V Partition Resources



L3V allows the ACOS device to split layer 2, 3, and 4-7 resources in multi-instance architecture enabling virtual segmentation for multi-client organizations. Specifically, in a corporation or at a service provider where many clients use the same load balancer, an administrator can create multiple L3V partitions and then control access to each organization's configuration or space. Each organization then can authenticate their own partition and configure their own devices as if they were a completely, separate organization.

ACOS devices provide support for multiple L3V partitions. The number of partitions they support are platform dependent.

Every configured device has one shared partition. By default, private partitions can access shared partition resources. A root admin can restrict access to shared partition resources. For example, a user with restricted access can log into a device with defined limited access to the shared partition.

Nothing within partitions is shared, unless an administrator allows users to share interfaces. When creating partitions, an administrator may allow users to share partitions or leave the shared partition blank. Users too can share interfaces, but are not required to.

Each partition has its own ARP table, and its own IPv4 and IPv6 route tables. They are completely separate from the ARP and IP route tables in other partitions.

After a network resource belongs to a partition, the resource does not appear in show command output except for the L3V partition and the partition to which the interface belongs. Likewise, statistics for the resource are not included in the statistics counters for other L3V partitions.

Untagged VLAN ports are exclusively owned by the shared or L3V partitions. Tagged VLAN ports can be shared across all the partitions by tagging them explicitly with unique VLAN IDs per partition.

The administrator may create partitions using CLI or GUI.

NOTE: For details on configuring partitions, refer to L3V Partition Configuration.

L3V Partition Requirements

Layer 3 resources must be unique within a given L3V partition. However, some types of Layer 3 resources can be the same in multiple partitions, as long as they remain unique within a given partition:

- VE number

NOTE: VE numbers must be unique and must match the VLAN ID in an L3V partition. If a VLAN ID already belongs to a shared or another L3V partition, do not re-use it.

- NAT pool

- Interface IP addresses
- IP addresses in source NAT pools
- Virtual server IP addresses (VIPs)

For example, multiple partitions can use a real server that has IP address 10.10.10.10, but a given partition can have only one instance of the server.

Each L3V partition supports a maximum of 2 loopback interfaces, with IDs 1-2. Loopback interface IDs 0-10 are valid in the shared partition.

L3V Partition Feature Support

The following topics are covered:

Features Configured at Global Configuration Level

The following features are configured at the global configuration level within an L3V partition:

- Hardware-based SYN cookies
- BGP instances per L3V partition
- Disable of Layer 3 forwarding between VLANs
- Source-IP connection-rate limiting
- DNS caching
- ICMP rate limiting
- Session filtering
- Global SLB options:
  - SLB peak-connection statistics (extended-stats)
  - SLB graceful shutdown

- SSL Insight
- Default compression block size for SLB
- Transparent TCP template
- Source NAT gateway for Layer 3
- Source NAT on VIP
- Reset stale session
- Application templates:
    - TCP
    - Source-IP persistence
    - Destination-IP persistence

NOTE: Also see L3V Partition Default SLB Templates.

Features Configured at Interface Configuration Level

The following features are configured at the interface configuration level within an L3V Partition

- IPv6 router advertisement and discovery
- ICMP rate limiting

L3V Partition Default SLB Templates

Partition-specific default server and port templates are supported.

- Real server
- Real port
- Virtual server
- Virtual port

Changes to a default server or port template in an L3V partition do not affect the default server or port templates in the shared partition or any other L3V partition.

Likewise, changes to a default server or port template in the shared partition do not affect the default server or port templates in L3V partitions.

NOTE: This behavior does not apply to feature templates such as HTTP, TCP, or source-IP persistence templates.

L3V Partition Configuration

This section provides information for configuring an L3V partition.

The following topics are covered:

L3V Partition Configuration Steps

The basic steps are summarized below:

1. Creating the partition.

   Each L3V partition must be configured with a unique identifier; this unique identifier is bound to the partition for the life of the partition. Only when the partition is deleted from the system can its partition ID can be re-used with the creation of a new partition.

2. Configuring admin accounts and assign them to partition.

   The partition admin accounts for L3V partition can be configured using the `admin` or `partition-admin` command. Although these commands are similar, when the `partition-admin` command is used, the created user is valid even if the creator admin user is removed. This command is supported in L3V partition only, Service Partition is not supported.

3. Configuring any SLB or CGN shared resources that you want to make available.

Configuration of SLB or CGN resources within an L3V partition can be perform ed by an admin with Partition-write privileges who is assigned to the partition.

NOTE: For details on a privileges, refer to Administering ADP Partitions.

4. Configure network and system connectivity resources, including interfaces, VLANs, and routing tables, for L3V partitions. Configuring additional admin accounts for the partition is also required.

NOTE: This document shows how to set up partitions and assign admins to them. The partition admins will be able to configure their own SLB or CGN, network, and system resources.

Understanding L3V Partition Profiles

The following topics are covered:

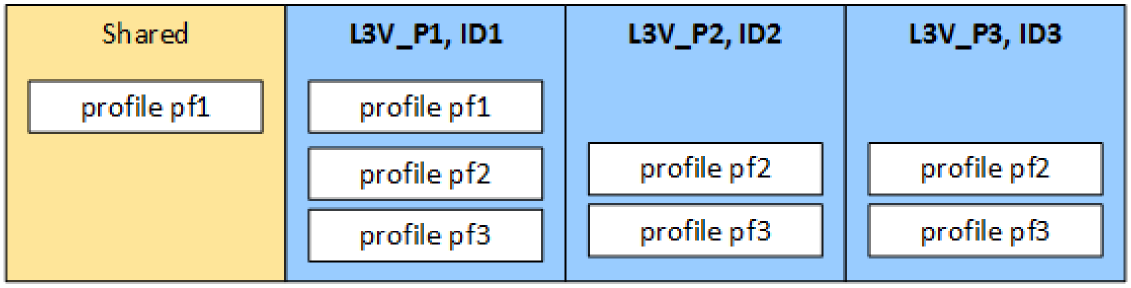
Overview

Each L3V partition has its own startup-config. An L3V partition administrator can save the running-config to a profile, using the **`write memory`** *`profile-name`* command.

Multiple configurations can be saved in each partition using this method (Figure 5); each configuration profile applies only to the L3V partition in which it was configured.

The startup-config profile in an L3V partition is not tied to the profile used in shared partition; this allows an L3V partition administrator to choose to use a configuration saved in a profile for that L3V partition that is independent of the configuration in use by the shared partition.

Figure 5 : Partition IDs and Profiles



Profiles

Profiles within an L3V partition can be dynamically loaded and unloaded. Using Partition IDs and Profiles as an example, suppose the active startup-config profile on partition p2 is "**pf3**," and you want to change this so that profile "**pf2**" becomes the active startup-config profile in partition p2:

1. Go to partition L3V_P2 and link the profile you want to be active (in this case, profile pf2) to the startup-config in that partition:

```
ACOS(config)# partition L3V_P2 id 2
ACOS(config-partition:L3V_P2)# active-partition L3V_P2
Current active partition: L3V_P2
ACOS[L3V_P2](config)# write memory pf2
ACOS[L3V_P2](config)# link startup-config pf2
```

2. Return to the shared partition.

```
ACOS[L3V_P2](config)# active-partition shared
ACOS(config)#
```

3. Unload the currently active profile in partition L3V_P2 (profile pf3):

```
ACOS(config)# no partition L3V_P2 id 2
Remove this partition and keep configurations on the disk? (y/n)y
ACOS(config)#
```

4. Use the `partition` command to load the new profile, which you linked to the startup-config in step 1.

```
ACOS(config)# partition L3V_P2 id 2
```

Creating L3V Partitions

The following topics are covered:

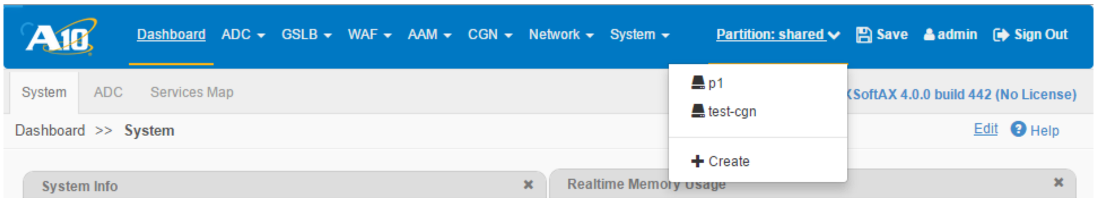
To create an L3V partition, use either of the following methods.

GUI Configuration

To create an L3V partition using the GUI:

1. From the top menu bar, select **Partition**, then select **Create**.

   In addition to the Create option, any existing L3V partitions are also shown.



2. On the Create Partitions screen, enter the partition name, partition ID, and application type.

NOTE: For more information about the application type, see Enabling SLB or CGN in a Partition.

3. Click **Create**. The new partition appears in the partition list.

NOTE: For more information about the fields in the GUI, refer to the GUI online help.

CLI Configuration

To create an L3V partition in the CLI, use the partition command.

For example, to create a partition named “**l3v-part-1**” with a partition ID of 3:

```
ACOS(config)# partition l3v-part-1 id 3
```

Each partition can be configured for either SLB or CGN applications, but not both. To specify, use the **`application-type`** parameter:

```
ACOS(config)# partition l3v-part-1 id 3 application-type adc
```

NOTE: For more information, see Enabling SLB or CGN in a Partition.

L3V Partition Configuration Examples

This section provides the configuration examples.

The following topics are covered:

Example 1: Simple L3V Partition Configuration

The following example shows how to create an L3V partition:

1. Create an L3V partition:

```
ACOS(config)# partition l3v1 id 1
ACOS(config-partition:l3v1)# exit
ACOS(config)#
```

2. Create the admin and assign privileges:

```
ACOS(config)# admin admin-l3v1 password test
ACOS(config-admin:admin-l3v1)# privilege partition-write l3v1
Modify Admin User successful!
ACOS(config-admin:admin-l3v1)# access axapi web cli
ACOS(config-admin:admin-l3v1)# enable
ACOS(config-admin:admin-l3v1)# exit
```

Alternatively, the admin for L3V can also be created using the `partition-admin` command:

```
ACOS[Partition_1234](config)# partition-admin padmin-l3v1 password
test
```

```
ACOS[Partition_1234](config-admin:padmin-l3v1)# privilege partition-write
Modify Admin User successful!
```

3. Now that the admin has been successfully created, log in to the partition using admin account:

```
login as: admin-l3v1
Using keyboard-interactive authentication.
Password:
Last login: Thu Aug 30 19:47:08 2012 from 192.168.33.157

ACOS system is ready now.

[type ? for help]

ACOS-Active[l3v1]> enable
Password:
ACOS-Active[l3v1]# config
ACOS-Active[l3v1](config)#
```

4. Configure the desired network and system resources.

   a. Configure a VLAN:

```
ACOS-Active[l3v1](config)# vlan 50
ACOS-Active[l3v1](config-vlan:50)# tagged ethernet 1
ACOS-Active[l3v1](config-vlan:50)# router-interface ve 50
ACOS-Active[l3v1](config-vlan:50)# exit
ACOS-Active[l3v1](config)# vlan 60
ACOS-Active[l3v1](config-vlan:60)# tagged ethernet 1
ACOS-Active[l3v1](config-vlan:60)# router-interface ve 60
ACOS-Active[l3v1](config-vlan:60)# exit
```

   b. Configure VEs:

```
ACOS-Active[l3v1](config)# interface ve 50
ACOS-Active[l3v1](config-if:ve50)# ip address 50.50.50.1 /24
ACOS-Active[l3v1](config-if:ve50)# exit
ACOS-Active[l3v1](config)# interface ve 60
ACOS-Active[l3v1](config-if:ve60)# ip address 60.60.60.1 /24
ACOS-Active[l3v1](config-if:ve60)# exit
```

c. Configure a server:

```
ACOS-Active[l3v1](config)# slb server s1-l3v 60.60.60.20
ACOS-Active[l3v1](config-real server)# port 80 tcp
ACOS-Active[l3v1](config-real server-node port)# exit
ACOS-Active[l3v1](config-real server)# exit
```

d. Configure a service-group:

```
ACOS-Active[l3v1](config)# slb service-group s1-80 tcp
ACOS-Active[l3v1](config-slb svc group)# member s1-l3v 80
ACOS-Active[l3v1](config-slb svc group-member:80)# exit
ACOS-Active[l3v1](config-slb svc group)# exit
```

e. Configure a VIP:

```
ACOS-Active[l3v1](config)# slb virtual-server vip1 50.50.50.15
ACOS-Active[l3v1](config-slb vserver)# port 80 tcp
ACOS-Active[l3v1](config-slb vserver-vport)# service-group s1-80
ACOS-Active[l3v1](config-slb vserver-vport)# exit
ACOS-Active[l3v1](config-slb vserver)# exit
```

5. View your running configuration. Since you have created an L3V partition, you can see and configure Layer 3 network resources, such as VLANs, VEs, and IP Addresses:

```
ACOS-Active[l3v1](config)# show running-config
!Current configuration: 596 bytes
!
!Configuration last updated at 20:03:00 PDT Thu Aug 30 2012
!
active-partition l3v1
vlan 50
 tagged ethernet 1
 router-interface ve 50
!
vlan 60
 tagged ethernet 1
 router-interface ve 60
!
!
```

```
interface ethernet 1
 mtu 9216
!
interface ve 50
 ip address 50.50.50.1 255.255.255.0
!
interface ve 60
 ip address 60.60.60.1 255.255.255.0


!
slb server s1-l3v 60.60.60.20
   port 80  tcp
!
slb service-group s1-80 tcp
    member s1-l3v 80
!
slb virtual-server vip1 50.50.50.15
   port 80  tcp
      name _50.50.50.15_TCP_80
      service-group s1-80
```

Example 2: Configuring Partition-Specific Layer 3 Resources

The following commands log onto the CLI and access partition dmz1, with the prerequisite that the admin and the partition for dmz1 have already been created:

```
login as: admin-dmz1
Welcome to ACOS
Using keyboard-interactive authentication.
Password:***
type ? for help]
ACOS[dmz1]> enable
ACOS[dmz1]# configure
ACOS[dmz1](config)#
```

The following commands configure Layer 3 resources for the partition:

```
ACOS[dmz1](config)# vlan 100
ACOS[dmz1](config-vlan:100)# tagged ethernet 1
ACOS[dmz1](config-vlan:100)# untagged ethernet 2
ACOS[dmz1](config-vlan:100)# router-interface ve 100
```

```
ACOS[dmz1](config-vlan:100)# exit
ACOS[dmz1](config)# interface ve 100
ACOS[dmz1](config-if:ve100)# ip address 20.20.1.1 255.255.255.0
ACOS[dmz1](config-if:ve100)# exit
ACOS[dmz1](config)# ip route 0.0.0.0 /0 20.20.101.50
```

The following command saves the configuration.

```
ACOS[dmz1](config)# write memory
Building configuration...
[OK]
```

The following commands log onto the CLI and access partition dmz2, with the prerequisite that the admin and partition for dmz2 have already been created:

```
login as: admin-dmz2
Welcome to ACOS
Using keyboard-interactive authentication.
Password:***
[type ? for help]
ACOS[dmz2]> enable
ACOS[dmz2]# configure
ACOS[dmz2](config)#
```

This command displays the list of Ethernet interfaces. Interfaces that belong exclusively to partition dmz1 are not included. Interface 1 is listed, since it is a tagged member of dmz1’s VLAN. Interface 2 is not listed, since it is an untagged member of dmz1’s VLAN. Likewise, dmz1’s VE is not listed.

```
ACOS[dmz2]# show interfaces brief
Port  Link  Dupl  Speed Trunk Vlan MAC             IP Address
IPs  Name
-------------------------------------------------------------------------
-----------
mgmt  Up    Full  100   N/A   N/A  001f.a001.d020  192.168.20.10/24
1
1     Up    Full  1000  N/A   Tag  001f.a002.0870  0.0.0.0/0
            0
3     Disb  None  None  None  1    001f.a002.0872  0.0.0.0/0
            0
4     Disb  None  None  None  1    001f.a002.0873  0.0.0.0/0
            0
```

```
5     Disb  None  None  None  1    001f.a002.0874  0.0.0.0/0
            0
6     Disb  None  None  None  1    001f.a002.0875  0.0.0.0/0
            0
7     Disb  None  None  None  1    001f.a002.0876  0.0.0.0/0
            0
8     Disb  None  None  None  1    001f.a002.0877  0.0.0.0/0
            0
9     Disb  None  None  None  1    001f.a002.78ec  0.0.0.0/0
            0
10    Disb  None  None  None  1    001f.a002.78ed  0.0.0.0/0
            0
11    Disb  None  None  None  1    001f.a002.78ee  0.0.0.0/0
            0
12    Disb  None  None  None  1    001f.a002.78ef  0.0.0.0/0
            0
```

The following commands configure Layer 3 resources for partition dmz2, and list the interfaces:

```
ACOS[dmz2](config)# vlan 200
ACOS[dmz2](config-vlan:200)# tagged ethernet 1
ACOS[dmz2](config-vlan:200)# untagged ethernet 3
ACOS[dmz2](config-vlan:200)# router-interface ve 200
ACOS[dmz2](config-vlan:200)# exit
ACOS[dmz2](config)# interface ve 200
ACOS[dmz2](config-if:ve200)# ip address 20.20.2.1 255.255.255.0
ACOS[dmz2](config-if:ve200)# exit
ACOS[dmz2](config)# ip route 0.0.0.0 /0 20.20.102.50
ACOS[dmz2](config)# show interfaces brief
Port  Link  Dupl  Speed Trunk Vlan MAC             IP Address
IPs  Name
-------------------------------------------------------------------------
-----------
mgmt  Up    Full  100   N/A   N/A  001f.a001.d020  192.168.20.10/24
1
1     Up    Full  1000  N/A   Tag  001f.a002.0870  0.0.0.0/0
0
3     Up    Full  1000  None  200  001f.a002.0871  0.0.0.0/0
0
```

```
4      Disb   None   None   None   1     001f.a002.0873   0.0.0.0/0
0
5      Disb   None   None   None   1     001f.a002.0874   0.0.0.0/0
0
6      Disb   None   None   None   1     001f.a002.0875   0.0.0.0/0
0
7      Disb   None   None   None   1     001f.a002.0876   0.0.0.0/0
0
8      Disb   None   None   None   1     001f.a002.0877   0.0.0.0/0
0
9      Disb   None   None   None   1     001f.a002.78ec   0.0.0.0/0
0
10     Disb   None   None   None   1     001f.a002.78ed   0.0.0.0/0
0
11     Disb   None   None   None   1     001f.a002.78ee   0.0.0.0/0
0
12     Disb   None   None   None   1     001f.a002.78ef   0.0.0.0/0
0
ve1    Up     N/A    N/A    N/A    200   001f.a002.0870   20.20.2.1/24
1
```

The following command saves the configuration.

```
ACOS[dmz2](config)# write memory
Building configuration...
[OK]
```

The following commands again log onto the CLI and access partition dmz1, and display the list of Ethernet interfaces. Ethernet 3 is not listed since it now belongs exclusively to partition dmz2.

```
login as: admin-dmz1
Welcome to ACOS
Using keyboard-interactive authentication.
Password:***
[type ? for help]
ACOS[dmz1]> enable
ACOS[dmz1]# show interfaces brief
Port   Link   Dupl   Speed Trunk Vlan MAC             IP Address
IPs   Name
```

```
-------------------------------------------------------------------------
-----------
mgmt  Up    Full  100   N/A   N/A  001f.a001.d020  192.168.20.10/24
1
1     Up    Full  1000  N/A   Tag  001f.a002.0870  0.0.0.0/0
0
2     Up    Full  1000  None  100  001f.a002.0871  0.0.0.0/0
0
4     Disb  None  None  None  1    001f.a002.0873  0.0.0.0/0
0
5     Disb  None  None  None  1    001f.a002.0874  0.0.0.0/0
0
6     Disb  None  None  None  1    001f.a002.0875  0.0.0.0/0
0
7     Disb  None  None  None  1    001f.a002.0876  0.0.0.0/0
0
8     Disb  None  None  None  1    001f.a002.0877  0.0.0.0/0
0
9     Disb  None  None  None  1    001f.a002.78ec  0.0.0.0/0
0
10    Disb  None  None  None  1    001f.a002.78ed  0.0.0.0/0
0
11    Disb  None  None  None  1    001f.a002.78ee  0.0.0.0/0
0
12    Disb  None  None  None  1    001f.a002.78ef  0.0.0.0/0
0
ve1   Up    N/A   N/A   N/A   100  001f.a002.0870  20.20.1.1/24
1
```

The following commands log onto the CLI with Read Write admin access, and display the list of Ethernet interfaces in the shared partition. All physical Ethernet interfaces are listed, including those belonging to individual partitions. The VEs belonging to other partitions are not listed.

```
login as: admin
Welcome to ACOS
Using keyboard-interactive authentication.
Password:***
[type ? for help]
ACOS> enable
```

```
ACOS# show interfaces brief
Port  Link  Dupl  Speed Trunk Vlan MAC             IP Address
IPs  Name
-------------------------------------------------------------------------
-----------
mgmt  Up    Full  100   N/A   N/A  001f.a001.d020  192.168.20.10/24
1
1     Up    Full  1000  None  Tag  001f.a002.0870  0.0.0.0/0
0
2     Up    Full  1000  None  100  001f.a002.0871  0.0.0.0/0
0
3     Up    Full  1000  None  200  001f.a002.0872  0.0.0.0/0
0
4     Disb  None  None  None  1    001f.a002.0872  0.0.0.0/0
0
5     Disb  None  None  None  1    001f.a002.0874  0.0.0.0/0
0
6     Disb  None  None  None  1    001f.a002.0875  0.0.0.0/0
0
7     Disb  None  None  None  1    001f.a002.0876  0.0.0.0/0
0
8     Disb  None  None  None  1    001f.a002.0877  0.0.0.0/0
0
9     Disb  None  None  None  1    001f.a002.78ec  0.0.0.0/0
0
10    Disb  None  None  None  1    001f.a002.78ed  0.0.0.0/0
0
11    Disb  None  None  None  1    001f.a002.78ee  0.0.0.0/0
0
12    Disb  None  None  None  1    001f.a002.78ef  0.0.0.0/0
0
```

Shared VLAN in L3V Partitions

The following topics are covered:

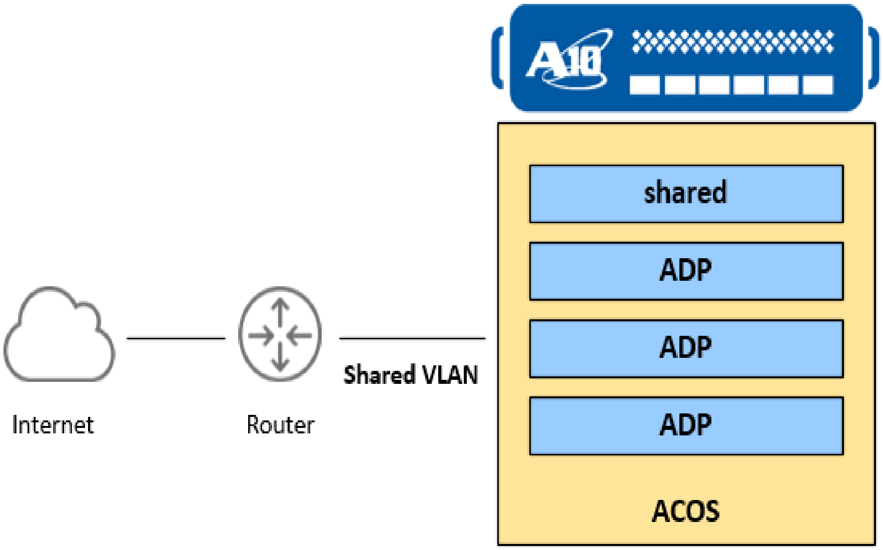
Overview

A virtual LAN or VLAN is any transmission area that is partitioned and secluded in a computer network at the data link layer.

In the latest release version of ACOS, starting with ACOS 4.1.4, the Shared VLAN Data Plane support is added for IPv4 and additionally for IPv6 as well.

This feature helps to limit the VLAN provisions and also minimize the configuration changes in the upstream router as administrators deploying multiple partitions on ACOS. To limit VLAN provisions and minimize configuration changes in the upstream router, configure a shared VLAN that is accessible from all partitions.

Figure 6 : Shared VLAN in L3V



For incoming and outgoing management traffic received on this interface, independent ACLs can be enabled in each partition (for this shared VLAN). Configure a shared VLAN across different partitions to support management applications and data traffic. The shared VLAN can only be created in the shared partition.

To support management applications as well as data traffic to VIP in partitions, the new commands for this feature are accessible once you have configured your partition(s) in the network partition level and configured your shared VLAN and data access.

1. Specify the interface to be bound to the partitions for management access.
2. Specify the source IP address allowed to establish management access to ACOS.
3. Configure your VLAN as a shared VLAN accessible from all partitions.

NOTE: A VE configured for shared VLAN management is limited to the following options: The option to enable or disable the interface, the ACL option and the name option. Only one IP address is allowed to be configured to match the allowable range provided.

Limitations

The following are the limitations or known issues of Shared VLAN feature in the L3V Partitions:

- It does not support IPv6 for management traffic.
- It supports L3V VIP.
- There is no support for Wildcard VIP.
- It is currently only applicable to Application Delivery Controller (ADC).
- The Multi-PU platforms are currently not supported.
- IPv6 address configuration for the shared VE interface is not allowed inside the L3V.
- Only one IPv4/IPv6 address is allowed on the shared VLAN interface inside the shared partition.
- Explicit default route must not be added in partitions.

NOTE: In case of default route learned from protocols running in the partition, explicit IP routes for the “Client Networks” must be added.

- Partition Follow feature must be configured for VRRP.

- There is no support for tunnel/tunneling, LIF (logical interface), and IPSec interface on shared VLAN.
- In shared partition, you must not configure VIP which is falling in `allowable-ip-range` assigned to partitions.
- You cannot remove the command `allowable-ip-range` while there are VIP/VE interfaces configured within the subnet.
- You cannot configure the command `allowable-ip-range` when the VIPs are already configured under the partition with matching subnet prefix.
- You cannot configure the non-matching subnet prefixes for the interface IP addresses in partitions using the shared VLAN feature.
- The shared VLAN cannot be removed while there are VE interfaces configured within a partition, using the shared VLAN.
- You can enable aVCS on the devices running on shared VLAN with the following mandatory specific configuration sequences:
  - The configurations for the shared VLAN as in the command `allowable-ip-range/allowable-ipv6-range` are device specific, whereas SLB virtual server configurations are common for master and blade.
  - You must configure the command `allowable-ip-range/allowable-ipv6-range` on both the devices, before enabling the aVCS on these devices.
  - If not followed properly, you may not be able to configure `allowable-ip-range/allowable-ipv6-range` on aVCS blade.
- You can utilize the management services from the L3V partition to networks reachable through the shared partition, only when the command `“ip mgmt-traffic all source-interface source-ip A.B.C.D”` is used.

NOTE: The representation of A.B.C.D must be either a shared VLAN management IP address or `mgmt-floating-ip-address`.

- You can utilize the management services from the L3V partition to networks reachable within the L3V partition work only without the config `"ip mgmt-traffic all source-interface source-ip A.B.C.D"`.
- The management services from the L3V partition cannot reach the networks from the shared partition and networks from the L3V partition at the same time.

- If the VIPS in L3V on the shared VLAN are configured with a route-map, then you must define the route-map in the shared partition. Otherwise, the redistribution for the VIPs fails in the shared partition, as it is unaware of the route-maps. Deny is the default operation of undefined route-maps.

Configuration

The following topics are covered:

GUI Configuration

This ACOS release does not support this feature in the GUI.

CLI Configuration

1. From the global configuration level, configure a VLAN.

```
ACOS(config)# vlan 100
ACOS(config-vlan:100)# untagged ethernet 1
ACOS(config-vlan:100-untagged ethernet 1)# router-interface ve 100
```

2. Set the VLAN as a shared VLAN accessible from all partitions using the following command:

```
ACOS(config-vlan:100)# shared-vlan
ACOS(config-vlan:100)# exit
```

3. Configure a partition, specify `shared-vlan` mode and the interface to be bound to the partition for management access (should already be configured) using the following command:

```
ACOS(config)# partition p1 id 1
ACOS(config-partition:p1)# shared-vlan
ACOS(config-partition:p1-shared-vlan)# vlan 100
```

4. Specify IP addresses allowed for the partition using the **`allowable-ip-range`** *`ip`*

address command, and the IP address for aVCS device management using the **mgmt-floating-ip-address** command:

```
ACOS(config-partition:p1-shared-vlan)# allowable-ip-range 1.3.4.0/24
ACOS(config-partition:p1-shared-vlan)# allowable-ip-range 2.3.4.0/24
ACOS(config-partition:p1-shared-vlan)# mgmt-floating-ip-address
1.3.4.100 vrid 0
```

NOTE: To use the shared VLAN in a VRRP/VCS deployment, it is mandatory to configure the **mgmt-floating-ip-address** option. Only the VRRP-A/VCS master will own the **mgmt-floating-ip-address** configuration. However, to use the shared VLAN feature, VRRP/VCS are not required.

5. Specify the **ipv6** address allowed for the partition using the **allowable-ipv6-range** *ipv6 address* command:

```
ACOS(config-partition:p1-shared-vlan)# allowable-ipv6-range 1111::/64
ACOS(config-partition:p1-shared-vlan)# allowable-ipv6-range 2222::/64
```

6. Repeat steps 2 and 3 for as many partitions as you wish to configure.

Redistribution of VIP Pools

The user can configure VIP in partition P1 within the subnet range for the **shared-vlan** feature. When the user configures VIP in a partition, the configured prefix is sent to share the partition. Protocols in the shared partition can redistribute these prefixes to upstream routers.

“**Ssh**” to **mgmt-floating-ip-address** lands in the specific partition of the active device in the group-id.

NOTE: The command **mgmt-floating-ip-address** is only applicable for **ipv4** and it is not supported for **ipv6**.

Shared VLAN Configuration Examples

The following shows an example of a shared VLAN configuration. In the configuration example below, the IPv4 address 80.1.1.0/24 is assigned to partition named “**one**”.

The subnet is matching the interface VE100 IP address configuration subnets. You are free to pick IP addresses in this range for management IP addresses. If 80.1.1.4 is used for management purposes, then this IP address can be configured on interface ve 100 within L3V partition “**one**.”

The **mgmt-floating-ip-address** is an optional configuration and is used in those scenarios where the user wants to have a single management address to configure both VRRP active and standby nodes in VCS environments.

NOTE: In a VRRP/VCS deployment, use the **affinity-vrrp-a-vrid** command to select the same node as the VRRP/VCS master. The VRID ID used in **affinity-vrrp-a-vrid** is the VRID ID that is also used with the **mgmt-floating-ip-address**.

```
vlan 100
untagged ethernet1
shared-vlan
router-interface ve 100

interface ve 100
ip address 80.1.1.1/24
ipv6 address 1111::3/64

vcs device 1
affinity-vrrp-a-vrid 10

partition one id 10
shared-vlan
vlan 100
mgmt-floating-ip-address 80.1.1.10 vrid 10
allowable-ip-range 80.1.1.0/24
allowable-ip-range 99.1.1.96/27
allowable-ipv6-range 1111::/64
allowable-ipv6-range 2222::/64
```

The following is a continuation of the example above. It shows the output given by the `show` command for partition “one.”

```
ACOS(config-partition:one)# show running-config
Interface ve 100
```

```
ip address 80.1.1.4/24
```

“**ssh**” to 80.1.1.4 results in landing to partition one.

In VCS scenarios, **ssh** to 80.1.1.10 results in landing to partition one of the active device in **vrrp group vr-id 10**.

```
Add partition configuration:
[one]#show running-config
interface ve 100
ip address 80.1.1.4 /24

ip nat pool pool1 80.1.1.2 80.1.1.3 netmask/32

ipv6 nat pool v6nat 5555::25 5555::25 netmask 64 vrid 1

slb virtual-server vip 99.1.1.96
port 5000 tcp

slb virtual-server vs1 1111::25
port 80 tcp
```

NOTE: You can configure VIP in partition P1 within the subnet range for the **shared-vlan** feature. Any VIP address configured in partition P1 inside the **allowable-ip-range** or **allowable-ipv6-range** cannot be configured with **vr-id** in its partition, because partitions using shared partition feature always use the **vr-id** follow feature in the partition.

Understanding Service Partitions

This section provides information about service partitions.

The following topics are covered:

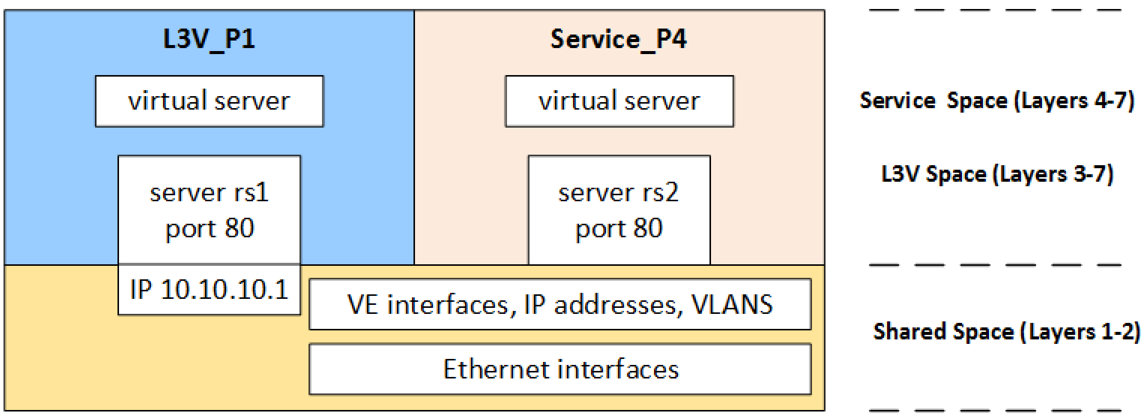
Overview

Service partitions provide Layer 4-7 support without direct access to system and networking resources. A service partition is configured within the shared partition. An administrator that has read and write privileges to all partitions can add VLANs, VEs, and assign IP addresses to the service partition. However, the configuration will be visible as part of the shared partition, not the service partition.

An administrator that can only access a service partition cannot add or remove any VLANs, VEs, and, IP addresses. The CLI and GUI also blocks service-only privileged administrators from creating any network resources. They must use the shared partition’s already defined network configurations to create VIPs, servers, and service-groups. These created servers, VIPs, service-groups, templates, and aFleX templates are independent of the shared partition but are on the same network. Since service partitions do not display network resources, partition administrators cannot remove them.

Figure 7 show how an ACOS device can be carved into separate service partitions.

Figure 7 : Service Partitions



Resources Contained in Service Partitions

The following types of resources can be contained in service partitions:

- Layer 4-7 (Application/SLB) resources:
  - Real servers
  - Virtual servers
  - Service groups
  - Templates
  - Health monitors
  - Certificates and keys
  - aFleX policies

A resource name can only be applied to one unit within the set of partitions that includes the shared partition and all service partitions.

For example, if a real server is named “**rs1**” in the shared partition, none of the service partitions can configure a different real server with the “**rs1**” label.

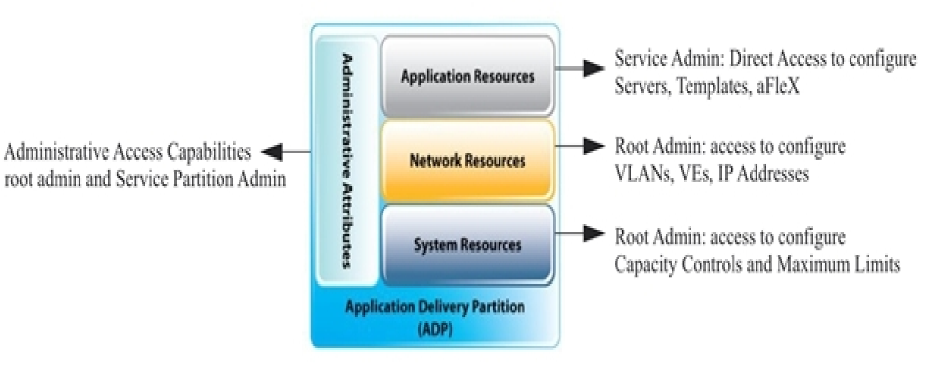
Service partitions depend on the shared partition for networking and system resources. The resources in the shared partition are not configurable by admins assigned to the service partition.

However, an admin who has read and write privileges to the shared partition can configure networking and system resources that affect the availability of resources accessible in the service partition.

Commands that create a private partition (L3V and Service) include parameters that provide a name and an ID number for the partition. Each private partition must be assigned a different ID number.

An ACOS device with service partitions provides the capabilities shown in Figure 8:

Figure 8 : Service Partition Capabilities


Administrative Access Capabilities
root admin and Service Partition Admin
Administrative Attributes
Application Resources
Network Resources
System Resources
Application Delivery Partition
(ADP)
Service Admin: Direct Access to configure
Servers, Templates, aFleX
Root Admin: access to configure
VLANs, VEs, IP Addresses
Root Admin: access to configure
Capacity Controls and Maximum Limits

Simple Service Partition Configuration

The following topics are covered:

Overview

To configure a service partition, log in using an admin account with Write privileges, and perform the steps described below:

1. Configuring partitions
2. Configuring admin accounts and assign them to partitions
3. Configuring SLB shared resources that you want to make available to multiple private partitions

NOTE: For information about configuring SLB resources, see the *Application Delivery and Server Load Balancing Guide*.

Configuring SLB resources within an ADP can be performed by an admin with partition-write privileges who is assigned to the partition.

NOTE: For details on administrative roles and privileges, refer to Administering ADP Partitions.

This document shows how to set up partitions and assign admins to them. The partition admins will be able to configure their own SLB resources.

However, you will need to configure connectivity resources such as interfaces, VLANs, routing, and so on. You also will need to configure any additional admin accounts for the partition.

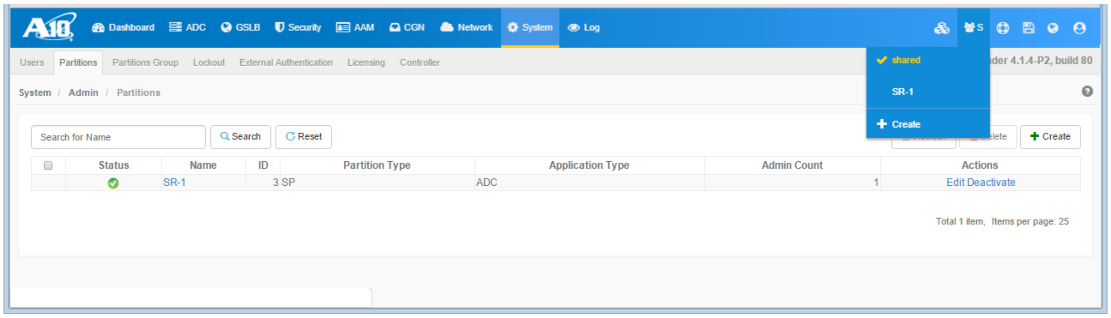
Creating Service Partitions

To create a service partition, use either of the following methods.

GUI Configuration

1. The GUI path that accesses the list of Partitions on the device is **System** > **Admin** > **Partitions**. Figure 9 displays the Create GUI panel that results from the partitions created in the Using the CLI section.

   Figure 9 : Partitions Panel (System > Admin > Partitions)



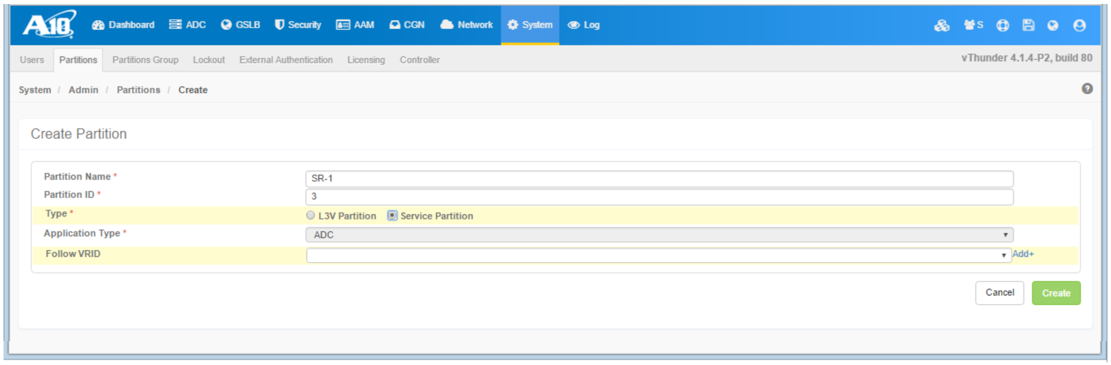
□	Status	Name	ID	Partition Type	Application Type	Admin Count	Actions
	✓	SR-1	3	SP	ADC	1	Edit Deactivate

Total 1 item, Items per page: 25

2. To create a Service Partition, click the Create button. The Type radio button selects the private partition type; this parameter is not editable after a partition

is created. Figure 10 displays the Create Partition panel that results in the creation of a Service partition.

Figure 10 : Create Partition panel



Create Partition

Partition Name * SR-1
Partition ID * 3
Type * ○ L3V Partition ● Service Partition
Application Type * ADC
Follow VRID

CLI Configuration

Service partitions are created with the service-partition command that is accessed through the global configuration level from the shared partition. A service partition’s parent partition is the partition where the service partition is created.

The command assigns an ID to the partition to ensure its configuration is consistent across devices in multi-device deployments. L3V and Service partition utilize the same ID number space. Each ID number assigned a private partition cannot be assigned to another partition of either type.

The show partition output displays information for all ADP partitions., including their name, ID number, ADP, type, and application type. The available-id option displays the partition ID numbers available to the device.

Example: Service Partition Configuration

The following subsections show additional service partition configuration examples.

1. Create the service partition:

```
ACOS(config)# service-partition SR-1 id 3 application-type adc
```

2. Create the admin and assign privileges. Assign the new admin read and write access for GUI and CLI.

```
ACOS(config-service-partition:SR-1)# admin ADMIN_SR-1 password test
ACOS(config-admin:ADMIN_SR-1)# privilege partition-write SR-1
Modify Admin User successful!
ACOS(config-admin:ADMIN_SR-1)# access web cli
ACOS(config-admin:ADMIN_SR-1)# exit
```

3. After creating the admin account, login to the partition using admin account. Open a new session by typing in information for the IP address:

```
login as: ADMIN_SR-1
Using keyboard-interactive authentication.
Password:
Last login: Thu Aug 30 19:46:54 2012 from 192.168.33.157
ACOS system is ready now.
[type ? for help]
ACOS[SR-1]>enable
Password:
ACOS[SR-1]#
ACOS[SR-1]# config
ACOS[SR-1](config)#
```

4. Configure the service partition for and ADC implementation with servers, service groups, and VIPs.

   a. Configure a server:

```
ACOS[SR-1](config)# slb server s1 20.20.20.25
ACOS[SR-1](config-real server)# port 80 tcp
ACOS[SR-1](config-real server-node port)# exit
ACOS[SR-1](config-real server)# exit
```

   b. Create service-groups:

```
ACOS[SR-1](config)# slb service-group s1-80 tcp
ACOS[SR-1](config-slb svc group)# member s1 80
ACOS[SR-1](config-slb svc group)# exit
```

   c. Create VIPs:

```
ACOS[SR-1](config)# slb virtual-server vip1 10.10.10.15
ACOS[SR-1](config-slb vserver)# port 80 http
ACOS[SR-1](config-slb vserver-vport)# service-group s1-80
```

5. Display the service partition configuration using the show running command. Service partitions only show Layer 4-7 configuration such as configuration of servers, service-groups, and VIPs. It does not display network resources, such as VLANs, VEs, or interfaces, since service partitions do not provide configurable network resources.

```
ACOS[SR-1](config)# show running-config
!Current configuration: 0 bytes
!Configuration last updated at 14:35:04 PDT Mon Jun 25 2018
!Configuration last saved at 10:52:29 PDT Mon Jun 25 2018
!
active-partition SR-1
!
!
slb server s1 10.10.20.20
  port 80 tcp
!
slb service-group s1-80 tcp
  member s1 80
!
slb virtual-server vip1 10.1.1.15
  port 80 http
    service-group s1-80
!
end
!Current config commit point for partition 3 is 0 & config mode is
classical-mode
ACOS[SR-1](config)#
```

Resource Templates for L3V Partitions

This section provides information about L3V partitions.

The following topics are covered:

Resource Templates

The following topics are covered:

Overview

Resource templates help you to define limits for application, network, and system resources in partitions enabled for Layer 3 Virtualization. Once defined, you can bind or unbind a resource template to a particular partition. You can also apply a sample template to multiple partitions. By default, Layer 3 partitions have the same resource limits as the shared partition. See the *Command Line Interface Reference*.

The current release allows you to ration resources to Layer 3 partitions. For example, you can specify the number of real servers a partition can access. Also for example, if the maximum number of real servers you specify is configured (no additional real servers can be configured), the ACOS device does not allow any additional GSLB service-IPs to be configured.

By configuring resource limits for individual Layer 3 partitions, you can ensure that no partition starves another partition of resources by monopolizing the available system resource quotas.

Resource Template Parameters

The following topics are covered:

You can configure the following types of resource templates for Layer 3 partitions:

Application Resources

Contains configuration parameters for application resources such as the number of health monitors, real servers, service groups, virtual servers, as well as a number of GSLB parameters, such as GSLB devices, GSLB sites, and GSLB zones. GSLB parameters are configurable on a per-partition basis (and thus non-configurable at the system level).

Network Resources

Contains configuration parameters for available network resources such as static ARPs, static IPv4 routes, static IPv6 routes, MAC addresses, and static neighbors.

System Resources

Contains configuration parameters for system resources such as limits for bandwidth, concurrent sessions, Layer 4 Connections Per Second (CPS), Layer 4 Session Limits, Layer 7 CPS, NAT CPS, SSL throughput, SSL CPS, and FW CPS.

Resource-accounting Parameter

The valid ranges and defaults for resource-accounting parameters differ depending on ACOS device model.

To view this information, enter the `show system resource-usage` command at the configuration level.

For details on the `show system resource-usage` command, see the *Command Line Interface Reference*.

Creating a System Resource Template

The following topics are covered:

Overview

The system resource limits that you configure in a default template are applied to all partitions, unless you explicitly apply a custom template to a partition. The “default” name should be reserved specifically for a non-custom partition template. Create a custom template to modify the limits for any application, network, or system resources from their default values.

GUI Configuration

The following topics are covered:

Creating a System Resource Template

The following general steps will help you create a System Resource Template:

1. Navigate to **System > Settings > Templates**.
2. Click **Create**.
3. In the name field, specify the name that will uniquely identify the template.
4. Configure the application, network, and system resource options. The online help will describe the available fields.
5. Click **OK**.

Deleting a System Resource Template

To delete a System Resource Template:

1. Unbind the template from network partitions. See Removing a Resource Template from a Partition.
2. Navigate to **System > Settings > Templates**.
3. This page displays a table of existing system resource templates. Select the checkbox of one or more system resource templates to delete.
4. Click **Delete**.

CLI Configuration

NOTE: For details on each CLI command used to configure a system resource template, see the **`system resource-accounting`** command in the *Command Line Interface Reference*.

The following general steps will help you create, use, or remove a custom resource template:

1. To create or modify a custom template, specify a unique name other than `default`. The following example shows creating a template named `ru-tmplt`.

```
ACOS(config)# system resource-accounting template ru-tmplt
ACOS(config-template:ru-tmplt)#
```

2. Within the template, specify the Application Resources, Network Resources, and System Resources you want to define from the appropriate sub-level.
3. To use your custom template, see Applying a System Resource Template to a Partition.

NOTE: Though partitions need to be bound to a template one at a time, several partitions may be bound to the same custom template.

To view your customized template containing the values for application, network, and system resources, use the `show running-config` command with appropriate filters, such as:

```
ACOS(config)# show running-config | sec resource-accounting template ru-tmplt
```

Assigning Resource Limits

The following topics are covered:

From the template configuration mode, you can modify any application, network, or system resource limits.

Application Resources

Use the **`app-resources`** command to enter the application resource limit configuration mode.

The following example shows you how to enter the application resources configuration mode. From this location, you can set values for the available application resources:

```
ACOS(config)# system resource-accounting template ru-tmplt
ACOS(config-template:ru-tmplt)# app-resources
ACOS(config-template:ru-tmplt-app-resour...)# gslb-zone-cfg max 10
ACOS(config-template:ru-tmplt-app-resour...)# health-monitor-cfg max 50
ACOS(config-template:ru-tmplt-app-resour...)# real-server-cfg max 100
ACOS(config-template:ru-tmplt-app-resour...)# service-group-cfg max 150
ACOS(config-template:ru-tmplt-app-resour...)# virtual-server-cfg max 250
```

NOTE: See "**`system resource-accounting template`**" in the *Command Line Interface Reference* for further information about the available parameters.

Network Resources

Use the **`network-resources`** command to enter the network resource limit configuration mode.

The following example shows you how to enter the network resources configuration mode. From this location, you can set values for the available network resources:

```
ACOS(config)# system resource-accounting template ru-tmplt
ACOS(config-template:ru-tmplt)# network-resources
ACOS(config-template:ru-tmplt-network-res...)# static-arp-cfg max 100
ACOS(config-template:ru-tmplt-network-res...)# static-ipv4-route-cfg max
1000
ACOS(config-template:ru-tmplt-network-res...)# static-ipv6-route-cfg max
2000
ACOS(config-template:ru-tmplt-network-res...)# static-mac-cfg max 200
ACOS(config-template:ru-tmplt-network-res...)# static-neighbor-cfg max 128
```

NOTE: See “**system resource-accounting template**” in the *Command Line Interface Reference* for further information about the available parameters.

System Resources

Use the **system-resources** command to enter the system resource limit configuration mode.

The following example shows you how to enter the system resources configuration mode. From this location, you can set values for the available system resources. Note that the **watermark-disable** optional keyword is used to disable the automatically-enabled watermark. However, the optional keyword, though available, is not used with the SSL throughput limit resource:

```
ACOS(config)# system resource-accounting template ru-tmplt
ACOS(config-template:ru-tmplt)# system-resources
ACOS(config-template:ru-tmplt-system-reso...)# bw-limit-cfg max 500
watermark-disable
ACOS(config-template:ru-tmplt-system-reso...)# concurrent-session-limit-
cfg max 3200
ACOS(config-template:ru-tmplt-system-reso...)# l4cps-limit-cfg max 2000
ACOS(config-template:ru-tmplt-system-reso...)# l7cps-limit-cfg max 4000
ACOS(config-template:ru-tmplt-system-reso...)# natcps-limit-cfg max 100000
ACOS(config-template:ru-tmplt-system-reso...)# ssl-throughput-limit-cfg
max 1000
ACOS(config-template:ru-tmplt-system-reso...)# sslcps-limit-cfg max 10000
```

NOTE: See “**system resource-accounting template**” in the *Command Line Interface Reference* for further information about the available parameters.

Applying a System Resource Template to a Partition

The following topics are covered:

Overview

If you create a custom system template, the template takes effect only after you attach it to an L3V partition. Attach the template to an L3V partition to override parameter values specified in the default template, if it exists.

Values from the default resource template are applied to L3V partitions that are not bound to a custom system template. Though a partition can be bound to only one template, multiple partitions may be bound to the same custom template.

NOTE: The template cannot be configured if resources utilized on the L3V partition exceed the system resource template limits. Additionally, while overwriting the template, the old template will be removed and the new template will be accepted only if the utilized resources are set below the threshold limits of the new template.

GUI Configuration

To apply a system resource template to a partition:

1. Navigate to **System > Admin > Partitions**.
2. Click the name of an existing partition from the partition drop-down menu at the top-right to access the partition configuration page, or click **Create** to create a new partition.
3. Select the **Resource Accounting** drop-down list to select from existing system resource templates.
4. Click **OK**.

CLI Configuration

Enter the `template` *`template-name`* command at the configuration level for the partition. The software will automatically check for the existence of the template before the template is successfully attached to a partition.

The following example shows applying a template to a partition. In this example, the template called `ru-tmplt` is being applied to a partition called `p55`:

```
ACOS(config)# partition p55 id 55
ACOS(config-partition:p55)# template
ACOS(config-partition:p55-template)# resource-accounting ru-tmplt
```

To verify that your template is applied to the partition called p55, use the `show running` command:

```
ACOS(config-partition)# show running-config | section partition p55
partition p55 id 55
   template
      resource-accounting ru-tmplt
```

Removing a Resource Template from a Partition

The following topics are covered:

Overview

To remove a link to a custom template from an existing partition, from the partition configuration level, issue the `no` form of the `template` command.

GUI Configuration

To unbind a System Resource Template:

1. Navigate to **System > Admin > Partitions**.
2. This page displays a table of existing partitions. Select an enabled partition from which to remove the resource accounting template.
3. Click **Edit** and then remove the **Resource Accounting** template from the drop-down menu.
4. Click **OK**.

CLI Configuration

To unbind all templates from a particular partition, issue the following commands, where "p55" refers to the name of the partition:

```
ACOS(config)# partition p55 id 55
(config-partition:p55)# no template
```

Or unbind a template from the template module:

```
ACOS(config)# partition p55 id 55
ACOS(config-partition:p55)# template
ACOS(config-partition:p55-template)# no resource-accounting ru-tmplt
```

When the custom template is removed from a partition, the default template values (from the default template that you have created) will be applied to the partition.

Resource Accounting Limit Scenario

Configuration of resource usages may fail in the event of contradictory resource limit conditions. Some scenarios are outlined below:

1. When attempting to bind a template to a partition, the software checks to see if the resources currently configured in the partition are within the new limits defined in the template, before it is bound to that partition. For example, if you have a partition called "p1" with 20 real servers, and a template called "t1" that has a limit of 10 real servers, when you attempt to bind template "t1" to partition "p1," an error claiming that this is an invalid configuration will be displayed.
2. When a particular resource limit is changed for a template which is already bound to a partition, the software performs a check for a contradictory configuration

scenario before the change is allowed. In this case, if template “t1” has a limit of 10 real servers and is bound to a partition “p1” with 8 real servers (which is within limits), when you attempt to change the limit in template “t1” to 5 real servers, you will not be allowed to do so because it contradicts the current configuration.

3. When a default template is defined, it gets applied to all the partitions that are not bound to a custom template. However, before the software assigns any values in the default template, it checks to make sure that the values in default template do not contradict any existing partition resource limits.
4. When you unbind a template from a partition, if a default template is configured, it gets applied to the partition. Before this happens, the software again checks for contradictory resource limits prior to unbinding the template.

Monitoring L3V Resource Templates

This section describes how to monitor resource templates using SNMP traps and Syslog messages.

The following topics are covered:

SNMP and Logging Thresholds for L3V Partition Resource Utilization

You can configure SNMP traps to be sent out when the configured threshold is reached for a particular system resource. This will show both the global system usage and the system usage per-partition.

NOTE: Both a Log message and a trap are generated when the configured threshold is crossed in either direction. The message will indicate if the current utilization if above or below the threshold.

GUI Configuration

This ACOS release does not support this feature in the GUI.

CLI Configuration

To set a threshold percentage for the network and application resource categories, use the `threshold` subcommands at your selected resource-accounting level:

The following example shows you how to configure the SNMP trap threshold for your application resources.

```
ACOS(config)# system resource-accounting template ru-tmplt
ACOS(config-template:ru-tmplt)# app-resources
ACOS(config-template:ru-tmplt-app-resour...)# threshold 10
```

Monitoring Resource Usage

This section describes the monitoring of resources allocated to a configuration.

The following topics are covered:

GUI Configuration

This ACOS release does not support this feature in the GUI.

CLI Configuration

To view the resource usage on a partition, use the `show resource-accounting` command. You can view utilization statistics for all partitions from the shared partition. When executing the command from an L3V partition, you can only view statistics for that partition. The command is not available from service partitions;

utilization statistics for the shared partitions includes resources used by all service partitions.

The following example uses the show resource-accounting command to display resource utilization on the shared partition.

```
ACOS(config)# show resource-accounting

Partition Shared

Resource Current Min-Guaranteed Max-allowed Utilization(%) Max-exceeded
Threshold-
exceeded Average Peak

Static Mac                0             0              500           0
           0                0               0            0

Static Arp                0             0              128           0
           0                0               0            0

Static Neighbor                0             0              128
0                0                0               0            0

V4 Static route                0             0             4000
0                0                0               0            0

V6 Static route                0             0             4000
0                0                0               0            0

Object Group Count                0             0             1000
  0                0                0               0            0

Object Group Clause Count                0             0            64000
         0                0                0               0            0

V4 ACL Lines Count                0             0            16000
  0                0                0               0            0

V6 ACL Lines Count                0             0            16000
  0                0                0               0            0
```

```
Real Servers                3             0             128           2
             0                0               0            3

Real Ports                4             0             256           1
           0                0               0            4

GSLB Sites                0             0             200           0
           0                0               0            0

GSLB Device                0             0             500           0
            0                0               0            0

GSLB Service IP                1             0             128
0                0                0               0            1

GSLB Service Port                0             0             256
 0                0                0               0            0

GSLB Zone                0             0             1000           0
          0                0               0            0

GSLB Service                0             0             2000           0
             0                0               0            0

GSLB Policy                0             0             2000           0
            0                0               0            0

GSLB IP List                0             0             200           0
             0                0               0            0

GSLB Template                0             0             200           0
              0                0               0            0

GSLB Geo-location               78             0          1000000
 0                0                0               0           78

GSLB Service-Group                0             0              200
  0                0                0               0            0
```

```
Service Group                4             0              128           3
              0                0               0            4

Virtual Server                1             0               64           1
               0                0               0            1

Health Monitor                0             0             1023           0
               0                0               0            0

L4 Session Count            0.00%         0.00%          100.00%
0                0                0           0.00%        0.00%

Concurrent Sessions                0             0          262.14K
   0                0                0               0            0

L4 CPS                0             0                0           0
       0                0               0            0

L7 CPS                0             0                0           0
       0                0               0            0

NAT CPS                0             0                0           0
        0                0               0            0

SSL CPS                0             0                0           0
        0                0               0            0
```

Inter-Partition Routing

This section describes how to configure inter-partition routing.

The following topics are covered:

Overview

ACOS enables you to configure static routes directly between an L3V partition and the shared partition. This capability is meaningful in case you lease different partitions to various customers. Traffic can now be routed from the shared partition to the VIP configured in an L3V partition and vice versa.

NOTE: Inter-partition routing is only provided for IPv4 addresses.

Enabling Inter-Partition Routing

The following are some common reasons for enabling inter-partition routing capabilities:

- To allow traffic to be redirected upstream from an L3V partition.
- To allow the shared partition to route traffic downstream to the real servers via the L3V partitions.
- To allow incoming traffic destined for a L3V partition with SLB information to bypass the shared partition (since it does not contain SLB configuration) and to be redirected to the L3V partition that is specified.
- To provide multiple L3V partitions, containing independent routing tables, with the ability to look up routing entries in the shared partition’s routing table (by treating the shared partition as the next hop within the device.)
- To operate in conjunction with VRRP-A for route lookups in the Forwarding Information Base (FIB) tables.

Requirements

This feature can be enabled successfully to route traffic between the shared and L3V partitions provided the following requirements are met:

- Inter-partition routing is only provided for IPv4 addresses. Currently, no IPv6 address support is provided.

- L3V partitions do not have duplicate IP Addresses across all partitions. If duplicate addresses are discovered, they will not be logged.
- If there are any overlapping real servers across partitions, NAT must be configured.
- Traffic must be received on the physical ingress port in the shared partition only.
- Static routes can forward traffic from the shared partition to VIP in an L3V partition.

Configuring Inter-Partition Routing

The following topics are covered:

Overview

The current release supports use of the CLI to configure this feature, with the prerequisite that partition **p1** has already been configured.

```
ACOS(config)# interface ethernet 4
ACOS(config-if:ethernet:4)# ip slb-partition-redirect
ACOS(config-if:ethernet:4)# exit
ACOS(config)# ip route 10.2.4.0 /24 partition p1
ACOS(config)# active-partition p1
ACOS[p69](config)# ip route 0.0.0.0 /0 partition shared
```

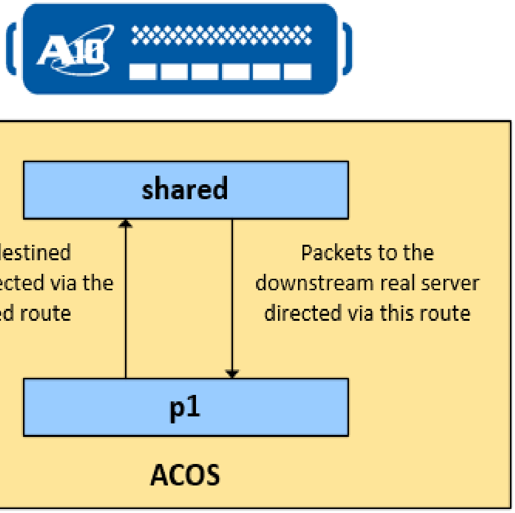
The **ip slb-partition-redirect** command enables the support on the ingress Ethernet data port that will receive the traffic addressed to the VIP in the L3V partition. Then, use the **ip route** command to add the static route whose destination is the network address configured in the L3V partition. Then, change the CLI session to the L3V partition (in this example, p69, and configure a static default route back to the shared partition.

Configuring Inter-Partition Routing in the Shared Partition

The following topics are covered:

Overview

Figure 11 : Inter-Partition Routing


shared
Packets destined upstream directed via the configured route
Packets to the downstream real server directed via this route
p1
ACOS

Shared partition config:

```
ip route 10.15.0.0 *24 partition p1
!
interface ve 21
ip address 10.11.0.1 /24
ip slb-partition-redirect
```

P1 config:

```
ip route 0.0.0.0 /24 partition shared
```

To enable inter-partition routing capabilities, there are two tasks that must be configured in the shared partition:

- Configure the specific route to the downstream real server via a L3V partition or to the VIPs in the L3V partition.
- Optionally, If you wish to enable forwarding of pass through (non-SLB) traffic, configure the ability to redirect traffic arriving on an incoming interface to be redirected to a L3V partition, bypassing the shared partition.

Specific Route/VIPs—Shared Partition to L3V Partition

Configured on the shared partition at the interface configuration level, the **`ip route`** command helps configure the specific route that will be used by the shared partition to communicate to the real server via an L3V partition or to the VIP in an L3V partition.

Packets destined for the downstream real server will be forwarded using this route:

In the following example, the default route to reach the real server (10.15.0.0) from the shared partition will traverse via an L3V partition (in this example, "partition p1"). Packets destined for the downstream real server will be directed using this route:

```
ACOS(config)# ip route 10.15.0.0 /24 partition p1
```

Verification

Verify your configuration using the **`show ip route`** command. In this output, you can see that the real server 10.15.0.0/24 is accessible "via partition p1":

```
ACOS(config)# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default

C       1.1.1.1/32 is directly connected, loopback 1
S       10.15.0.0/24 [1/0] via partition p1
C       219.247.8.0/24 is directly connected, ethernet 8
```

You can also verify your configuration using the **`show ip fib`** command. In this command, you see that "partition a" is the nexthop to the network address to which the VIP belongs, 10.15.0.0.

```
ACOS(config)# show ip fib
Prefix                 Next Hop        Interface       Distance   Index
------------------------------------------------------------------------
1.1.1.1 /32            0.0.0.0         loopback1       0
10.15.0.0 /24          partition p1    loopback1       0
```

```
219.247.8.0 /24        0.0.0.0          ethernet8       0
Total Routes = 3
```

IP SLB Partition Redirect Configuration

The **`ip slb-partition-redirect`** command is issued in the shared partition at the interface configuration level for traffic on the specified incoming interface. This traffic will be successfully redirected to the specified L3V partition that will process the packets. This command is meaningful for downstream routing of traffic.

The configuration is applied to the specified physical interface, virtual interface, or trunk at the interface configuration level.

In the following example, the **`ip slb-partition-redirect`** command will apply to the virtual interface (ve21) in the shared partition. The IP Address 10.11.0.1 /24 indicates the IP Address of the incoming virtual interface.

```
ACOS(config)# interface ve 21
ACOS(config-if:ve:21)# ip address 10.11.0.1 /24
ACOS(config-if:ve:21)# ip slb-partition-redirect
```

Verification

Verify your virtual interface configuration to see if you have successfully redirected traffic destined for the specified incoming interface downstream:

```
ACOS# show running-config interface ve 21
interface ve 21
 ip address 10.11.0.1 255.255.255.0
 ip slb-partition-redirect
```

Configuring Inter-Partition Routing in the L3V Partitions

The following topics are covered:

Overview

To enable inter-partition routing capabilities, there is one mandatory task and another optional ones that must be configured in the L3V partition:

- Configure the static default route to the shared partition.
- Optionally, configure SLB in the L3V partition, if you have not already done so.

NOTE: The current release does not provide support for outbound source NAT for pass through traffic.

Default Route—L3V Partition to the Shared Partition

Configured on the L3V partition at the interface configuration level, the **`ip route`** command helps configure the static route that will be used by the L3V partition to communicate with the shared partition.

Change the CLI session to the L3V partition, and configure a static default route back to the shared partition:

Packets destined upstream from the L3V partition will use the configured static route and will be sent out the specified outgoing interface:

Ensure that you have SLB running and VIPs configured in your L3V partition before you configure a static route to the VIP. Configure the default route to the shared partition from the L3V partition:

```
ACOS[a](config)# ip route 0.0.0.0 /0 partition shared
```

Verification

Verify your configuration using the **`show ip route`** command. Look at the route that shows that 0.0.0.0/0 is accessible “via partition shared”:

```
ACOS[a](config)# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default
```

```
Gateway of last resort is 127.1.0.0 to network 0.0.0.0

S*       0.0.0.0/0 [1/0] via partition shared
C        10.15.0.0/24 is directly connected, ve 22
```

Verify your configuration using the **show ip fib** command:

```
ACOS[a](config)# show ip fib
Prefix                 Next Hop        Interface       Distance
------------------------------------------------------------------------
0.0.0.0 /0             partition shared loopback1        0
10.15.0.0 /24          0.0.0.0         ve 22           0
Total Routes = 2
```

Verify your virtual interface configuration on ve22:

```
ACOS[a](config)# show running interface ve 22
interface ve 22
 ip address 10.15.0.1 255.255.255.0
```

Configuring SLB within an L3V Partition

The following topics are covered:

Configuration

To configure SLB in your L3V partition, use the following commands, configure the server, the associated port and protocol, the SLB service group, and the members of the group, the SLB virtual server, the associated port and protocol, the IP Address of the VIP, and service group for the virtual server.

```
ACOS[a](config)# active-partition a
ACOS[a](config)# slb server rs1 10.15.0.15
ACOS[a](config-real server)# port 80 tcp
ACOS[a](config-real server-node port)# exit
ACOS[a](config-real server)# exit
```

```
ACOS[a](config)# slb service-group sg1 tcp
ACOS[a](config-slb svc group)# member rs1 80
ACOS[a](config-slb svc group-member:80)# exit
ACOS[a](config-slb svc group)# exit
ACOS[a](config)# slb virtual-server vs1 10.15.0.101
ACOS[a](config-slb vserver)# port 80 http
ACOS[a](config-slb vserver-vport)# service-group sg1
ACOS[a](config-slb vserver-vport)# exit
ACOS[a](config-slb vserver)# exit
ACOS[a](config)# slb virtual-server vs2 10.15.0.102
ACOS[a](config-slb vserver)# port 80 tcp
ACOS[a](config-slb vserver-vport)# service-group sg1
ACOS[a](config-slb vserver-vport)#
```

Verification

Verify your partition SLB configuration using the **show run | sec slb** command and display the SLB configuration section:

```
ACOS[a](config)# show run | sec slb
slb server rs1 10.15.0.15
        port 80 tcp
slb service-group sg1 tcp
        member rs1 80
slb virtual-server vs1 10.15.0.101
        port 80 http
        service-group sg1
slb virtual-server vs2 10.15.0.102
        port 80 tcp
        service-group sg1
```

Having configured the static route in the L3V partition and the shared partition, and having configured SLB redirect capabilities on the shared partition, the inter-partition routing feature is now functional.

Contact Us