ACOS 6.0.7
Global Server Load Balancing Guide

March, 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

The following topics are covered:

Introduction

A10 Global Server Load Balancing (GSLB) refers to load balancing applications on ACOS devices and global networks, to direct users to multiple data centers. Each data center consists of server farms that provide users with fast response time and redundancy to protect against the failure of a complete data center. Each GSLB implementation falls under one of the categories:

- **DNS-Based GSLB:** Domain Name System technology is utilized to extend load balance to a global network.
- **IP-Based GSLB:** Route health injection advertises VIP availability throughout the network.

The following GSLB configuration advantages are provided with ACOS:

Provide data center fail-over to minimize downtime and ensure application availability.

- Optimize multi-site deployments.
- Maximize network access speed.
- Provide faster performance and improved user experience by directing users to the nearest site.
- Increase data center efficiency by using flexible policies to distribute traffic to multiple sites.

NOTE: GSLB is disabled by default and requires proper configuration to operate.

DNS-Based Protocol

The Domain Name System (DNS) is a distributed database of domain names, that uses the
Client-Server architecture. For example, a particular organization or website is assigned a domain name.

GSLB protocols decide what IP address must be sent for a DNS query. GSLB sites are geographically distributed and DNS servers run at each site as a service on ACOS device or instance. All Name Servers at the various sites involved are authoritative for the same domain(s). Each of the GSLB domains is a sub-domain for which a delegation is configured so that the GSLB Name Servers are authoritative and can use one of the various load balancing algorithms to decide which IP address to give out at any given time.

A delegation is created by adding a name-server record for the GSLB domain in the parent domain database files and a subsequent address record for the name-servers that are used for the delegation.

Controller and Devices

ACOS devices use the GSLB protocol to manage traffic between a controller and the accessible sites. The interval between protocol updates range from one second to five minutes (the default is 30 seconds). VIP information is sent asynchronously.

A GSLB controller administers protocol activities. The protocol must be enabled on the ACOS designated to perform controller functions.

The GSLB controller collects the following information from the accessible site load balancers:

- Virtual IP addresses & active servers
- Active-Round Delay Time (aRDT)
- Site session capacity statistics
- Connection load

- Connection count by site
- Number of active sessions

A GSLB Controller Group consists of multiple controllers, within a GSLB zone, whose service IP status and GSLB configurations are synchronized. GSLB Controller Groups provide redundancy that protects against the failure of an individual device. The ACOS device can automatically synchronize GSLB configurations and VIP-server status among multiple GSLB controllers for a GSLB zone.

Enabling the protocol on site devices within a GSLB configuration is operational for base configuration. Specific policy options and the default health checks require the protocol to be enabled.

When running GSLB in server mode, a VIP for the DNS is required; the configuration of a real server or service group is not required. When running GSLB in proxy mode, the real server and service group are required along with the VIP.

For additional information on DNS configuration for Server mode and Proxy mode see "*DNS Support*".chapter.

Configuring the GSLB Controller

1. Configure GSLB on the GSLB ACOS device with the GSLB Controller feature:
2. Configure health monitors for the DNS server proxy and the GSLB services to be load balanced.
3. Configure a GSLB policy as described in "Configuring Policies".

NOTE: Configuring GSLB policy can be skipped when using a default profile.

4. Configure services.
5. Configure sites.
6. Configure a zone.
7. Enable the GSLB protocol for the GSLB controller function (**`gslb protocol enable controller`** command).

Configuring GSLB Site ACOS Devices

GSLB deals with multiple sites. Each site has a unique IP address or IP addresses, management interfaces or VRRP interfaces. Each IP address is associated with a set of parameters. A site selection policy can be evaluated based on these parameters.

To configure GSLB on the site ACOS devices:

1. Configure SLB on the device.
2. Enable the GSLB protocol for the GSLB site device function. (**`gslb protocol enable device`** command)

See topic “gslb protocol” for a description of **`gslb protocol`** commands.

Dual Functionality

Two communicating ACOS devices in different sites, for example A and B, can each be deployed as both controller and normal device. Additional device is not required to act as a controller.

To configure GSLB on the site A and B ACOS devices:

1. Configure SLB on the device.
2. Enable the GSLB protocol for the GSLB site devices, use function. (**`gslb protocol enable device`** and **`gslb protocol enable controller`** commands).
3. Enable Virtual Server IP with UDP and HTTP services.
4. Configure health monitors for the DNS server to be proxies and the GSLB services to be load balanced.
5. Configure DNS proxies.
6. Configure a GSLB policy as described in “Configuring Policies”.
7. Configure services.
8. Configure sites.
9. Configure a zone.
10. Enable the GSLB protocol for the GSLB controller function (**`gslb protocol`**

enable controller command).

To perform the dual deployment configuration, run the following script for the Site A and Site B devices from the remote server through the GSLB controller device.

```
gslb protocol enable controller
!
gslb protocol enable device
slb virtual-server vip 35.193.67.127
port 53 udp
        gslb-enable
port 80 http
        aflex siteA
gslb service—ip SiteA-www 35.193.67.127
        health—check—protocol—disable
        health—check—disab1e
port 80 tcp
        health-check-protocol-disable
        health—check—disab1e
!
gslb service—ip SiteB—www 35.225.232.183
        health—check—protocol—disable
        health—check—disable
        port 80 tcp
                health-check-protocol-disable
                health—check—disable
!
gslb site SiteA
        slb-dev sitea 1.1.1.111
                vip-server SiteA-www
!
gslb site SiteB
        slb-dev siteB 2.2.2.222
                vip-server SiteB-www

gslb policy a101ab
        metric-order health-check geographic
        dns server srv mx naptr ns auto-ns auto-ptr
```

```
txt any authoritative cname

gslb zone gslb.a10demo.com
        policy a101ab
        dns-ns-record ns1.gslb.a10demo.com
        dns-ns-record ns2.gslb.a10demo.com
        service 80 www
                dns—a—record SiteA—www static
                dns—a—record SiteB—www static
```

Deployment

A10 GSLB deployments safeguard your network and support disaster recovery. This ensures
continuous availability of applications through the Application Delivery Controllers (ADCs). A10 GSLB balances the loads on the servers and ADCs across global data centers by directing client requests to the closest or high performance data centers, or to functioning data centers in the event of an outage.

The following topics are covered:

Modes

ACOS supports GSLB Server and Proxy modes to configure GSLB at different remote and controller sites.

The following topics are covered:

Server Mode

An ACOS device in server mode responds directly to queries for specific service IP addresses in the GSLB zone; the device also forwards other types of queries to the DNS server. In server mode, the ACOS device can reply with A, CNAME, MX, NAPTR, NS, PTR, SRV, and TXT records. For all other records, the ACOS device attempts proxy mode.

You can configure GSLB to use only the GSLB DNS server for all replies. When the configuration does not contain the applicable DNS record, the controller responds with a server failure message when it does not manage the FQDN.

An ACOS device becomes a GSLB ACOS device when you configure GSLB on the device and enable the GSLB protocol, for the controller function. The GSLB protocol uses port 4149. The protocol is registered on this port for both TCP and UDP.

The **dns server** command is a GSLB policy mode command that enables an ACOS device to act as a DNS server for specific service IPs in the GSLB zone to which the policy is applied. To configure DNS server mode on a device, apply a policy with a DNS server command to a zone or service on the device.

CLI Configuration

This command configures a policy to setup a device as a DNS server to use DNS TXT resource records to carry multiple pieces of DNS TXT data within one TXT record, then applies the policy to a service.

```
ACOS(config)# gslb policy kaibab
ACOS(config-policy:kaibab)# dns server txt
ACOS(config-policy:kaibab)# exit
ACOS(config)# gslb zone example.com
ACOS(config-zone:example.com)# service 80 www
ACOS(config-zone:example.com-service:www)# policy kaibab
ACOS(config-zone:example.com-service:www)# dns-txt-record obj-1 aaaa
ACOS(config-zone:example.com-service:www)# dns-txt-record obj-2 bbbb
ACOS(config-zone:example.com-service:www)# dns-txt-record obj-3 cccc
ACOS(config-zone:example.com-service:www)# exit
ACOS(config-zone:example.com)# show run | sec gslb
gslb policy kaibab
  dns server txt
gslb zone example.com
```

```
  service 80 www
    policy kaibab
    dns-txt-record obj-1 aaaa
    dns-txt-record obj-2 bbbb
    dns-txt-record obj-3 cccc
ACOS(config-zone:example.com)#
```

Proxy Mode

An ACOS device in proxy mode acts as a proxy for an external DNS server. In proxy mode, the ACOS device updates A and AAAA records in response to client requests and forwards requests for other record types to the external DNS server. DNS proxy is a DNS virtual service; its configuration is similar to that of an SLB service.

By default, a GSLB policy configures the device to act in DNS proxy mode. The **`no dns server`**
command disables DNS server mode within a policy where DNS server mode was previously enabled.

GUI Configuration

These steps describe the DNS proxy configuration process. For a description of SLB commands and processes, see the “ADC Command Line Interface Reference Guide” and the “Application Delivery and Server Load Balancing Guide”.

1. Configure a real server for the DNS server to be proxied (**`slb server`** command)
2. Configure a DNS port on the server (**`port`** command).
3. Enable health monitoring of the DNS service (**`health-check`** command).
4. Layer 3 health monitoring using the default Layer 3 health monitor is already enabled by default.
5. Configure a service group and add the DNS proxy (real server) (**`slb service-group`** command).
6. Add the DNS server to the service group (**`member`** command).
7. Configure a virtual server for the DNS proxy and bind it to the real server and service group (**`slb virtual-server`** command).

8. Add the DNS port (**`port`** command)
9. Bind the DNS port to the DNS proxy service group (**`service-group`** command)
10. Enable GSLB on the port (**`gslb-enable`** command)

NOTE: "Scenario 1: GSLB Proxy Mode" contains a DNS proxy configuration example.

GSLB Controller Groups

A GSLB Controller Group consists of multiple controllers, within a GSLB zone, whose service IP status and GSLB configurations are synchronized. GSLB Controller Groups provide redundancy that protects against the failure of an individual device.

Each group consists of member ACOS devices. Among the members, the group a Master which manages group synchronization. The Master device synchronizes GSLB configurations and VIP-server status among the GSLB controllers within the group. A group can contain up to 15 members. By default no primary members are defined.

On each GSLB controller, the configuration for a GSLB group includes a list of primary group members. Group member addresses, after they are configured on the Master device, are pushed to the other devices in the group. After the GSLB process starts on an ACOS device, the device joins the controller group by connecting to the primary group members to exchange group management traffic.

Controller groups provide a learning option that enables an ACOS device to learn IP addresses of member when they are added to the group. Learning is enabled by default.

This feature is different from the ACOS Series Virtual Chassis System (aVCS) feature. aVCS is used for multiple ACOS devices that serve as mutual backups within the same LAN.

Master Controller Election

Each GSLB controller in a controller group has a configurable priority value that ranges from 1 to 255. During master election, the GSLB controller with the highest priority is elected master for the group. If more than one controller has the highest

priority value, the controller with the highest last 4 bytes in its management interface MAC address is elected.

The master controller and the other controllers periodically send keepalive messages. If the other controllers stop receiving keepalive messages from the master controller, a new master is elected.

To designate a master controller for the GSLB group, set the priority of the desired ACOS device to a higher value than the other members. It is recommended that you make GSLB configuration changes for the group-wide parameters on the master. See GSLB Synchronization section for further information. The group synchronization feature pushes your configuration to the other group members.

GSLB Synchronization

The master controller synchronizes GSLB configurations and VIP server status among multiple controllers in a GSLB group. The master synchronizes the following GSLB configuration items when updating the configurations on other controllers:

- Service IPs
- Sites, including SLB-device parameters
- Zones, including services
- GSLB policies (only those that are used by services)
- SLB information for DNS proxy
- GSLB protocol settings
- Health Monitors (if configured using the GSLB option)
- Sticky Persistence

The following items are not synchronized:

- Geo-location files
- Black/white list files

The master controller sends the following status information to the other controllers:

- aRDT data
- Connection load data
- Virtual port status
- Virtual server status
- Device status

Until the configuration status reaches “FullSync”, by default directly changing GSLB configuration information. This can be edited directly on group members that are not the master. When multiple devices are configured differently, changes on the master overwrite changes on other group members when “FullSync” is reached.

After the configuration synchronization status reaches “FullSync”, directly changing the configuration on a member device is not supported and generates the error message “Operation denied by Group Master”.

- When a L3V network contains two or more controllers that use the same public NAT address, a GSLB group accepts only one controller as a group member. The ACOS GSLB controller rejects subsequent connection requests from the same external IP.
- In VRRP-A deployments, the GSLB configuration synchronizes with the active VRRP-A device, which then pushes the GSLB configuration changes to the VRRP-A standby device.
- The CLI prompt displays the ACOS device’s role within the GSLB group. Status indicator can be either “Master” or “Member”, as shown in these examples:

```
ACOS-Master(config)#
ACOS-Member(config)#
```

The group role indicator is disabled with the **`no terminal gslb-prompt`** command.

Synchronizing Additional Objects

Along with the default GSLB Synchronization, additional ACOS objects, such as, real servers, service-groups, health-monitors, virtual servers, and more can be configured for synchronization. These configured objects are synchronized from the master node to the member nodes.

NOTE: All the member nodes in the GSLB group must run the same software release version to ensure proper synchronization. This feature only works if all the devices are in the shared partition.

The synchronization of additional elements provides the following functionalities:

- **Shared configuration**: The additional configuration objects are considered as common or shared configurations. All the controller nodes have the exact same data.
- **Real-time Synchronization**: In case of any configuration change done on the master node, the same change is synchronized to all other controllers. Note that only the configuration objects mentioned in the `gslb sync-objects <object class>` will be synchronized during real-time synchronization. For example, if an object class, such as, health monitor is not specified in the `gslb sync-objects` on the master node, it will not be synchronized to the member. The master node does not wait for a response from each controller. A controller logs a failure message if it fails to process the sync command.
- **Full Synchronization when a new GSLB node joins**: When a new GSLB node joins the existing GSLB group, the master node pushes the entire default GSLB configuration objects and additional configured objects to the new node.
  - To enable full synchronization on member nodes, the `harmony-controller config-replace` command must be enabled.
  - The `force-full-sync` command forces GSLB to synchronize full application configuration and GSLB related files from the master node to all the member nodes.
  - During full synchronization, the master node also synchronizes the configuration from the `gslb protocol enable` command to the member node. To retain the configuration in the `gslb protocol enable` command on the member node, manually configure the `contoller/device` option in this command on the member node after the full synchronization completes.

  The new node replaces its configuration with the pushed configuration. Errors occurring during the synchronization are ignored and the remaining configuration is applied on the member nodes.

  Handling Synchronization Mode Mismatch

If the synchronization of objects on a member does not match with that of the GSLB group, the show log displays the following error:

```
ACOS(config-group:default)#show log
Aug 22 2024 18:12:23 Info  [GSLB_PROTOCOL]:GSLB Group default: member
10.1.1.1:4149 joined
Aug 22 2024 18:12:23 Info  [GSLB_PROTOCOL]:GSLB Group default: connected
Aug 22 2024 18:12:23 Info  [GSLB_PROTOCOL]:ERROR: GSLB group received
config with mismatch sync mode!
```

In such cases, GSLB removes the member and forces the group member to disable the group, correct the synchronization mode to match the master and then re-enable the GSLB group.

CLI Configuration

The **gslb sync-objects <objects>** on the master node synchronizes specified additional objects during GSLB synchronization. The following example indicates if slb virtual servers are getting synchronized to the GSLB members from the GSLB master.

```
gslb sync-objects slb.virtual-server
gslb sync-objects action enable
!
slb virtual-server VS1 190.165.10.70
  port 53 dns-tcp
    source-nat auto
!
harmony-controller config-replace enable
!
```

Limitations

• In case of a change of scope to GSLB dynamic synchronization, the changes are not applied to the existing configuration. The changes are only implemented to new configurations made after the changed scope.

• If a member fails to process the **gslb sync-objects** command, a failure rollback is not triggered in other nodes. Instead, the member logs a failure message.

• GSLB cluster does not detect out of synchronization cases between controller nodes.

• The synchronization only considers common ACOS objects. It does not support the synchronization of device-specific configuration. The network.vlan object lineage is currently not supported.

Configuring GSLB Controller Groups

Configure the GSLB controller groups parameters on the ACOS “Group Master” device and the secondary devices.

This following topics are covered:

Controller Group Parameters

The following is a list of configurable GSLB group parameters, accompanied with the command. The GSLB group command places the CLI in gslb-group configuration mode. All other commands in this section are accessed from gslb-group mode.

- **Group name:** Name of the GSLB controller group (`gslb group`)
- **Group state:** State of the group on the ACOS device. (`enable`)
- **DNS auto-mapping:** Maps group IP resources to IP addresses on the ACOS device. (`auto-map`)
- **DNS discover:** Discovers group members using DNS. (`dns-discover`)
- **DNS suffix:** DNS suffix used for DNS discovery. You can specify the suffix (name) that GSLB appends to the domain name when sending a dns-discover query. For example, for group name “group” and suffix “example.com”, strings are sent in the DNS discovery query as “group.example.com”. (`suffix`)

- **Priority:** Value used during master election for the group. Higher priority values are preferred over lower priority values. For example, priority value 200 is preferred over priority value 100. (`priority`)
- **Primary controller:** IP addresses of the other GSLB controllers to connect to within the group. You can specify up to 15 IP addresses. (`primary`)
- **Learning:** Allows the device to learn the IP addresses of additional group members from primary controllers (`learn`).
- **Automatic configuration save:** Automatically saves the configuration on a group member when the configuration is saved on the group's master controller. (`config-save`)
- **Automatic configuration merge following master takeover:** Automatically merges the previous master's configuration to the new master following takeover of the master role. (`config-merge`)
- **Configuration allowed on all group members:** Allows GSLB configuration to be performed on any group member. (`config-anywhere`)
- **Inherit configuration:** Allows a GSLB controller to acquire its GSLB configuration from another device. (`inherit`)
- **Standalone operation:** Allows this GSLB controller to operate independently of the group. (`standalone`)
- **Timeout:** Provides timeout (1-60 minutes) to complete the full synchronization between the master controller and member controllers by retrying synchronization if a full sync is not completed. (`sync-timeout`)

Configuring the Group Master

1. Configure the GSLB parameters that will be synchronized with the other controllers.

   For configuring additional ACOS objects for synchronization with other controllers, configure the **`gslb sync-objects <object>`** command.

2. Configure local GSLB parameters as applicable to your deployment.
3. Add the device to the GSLB controller group and change the group priority value to 255.
4. Enable the device's membership in the group.

Configuring the Secondary Devices

1. Add the device to the GSLB controller group. Set the priority to a value that is less than the master.
2. Enable the ACOS device's membership in the group.
3. Configure local GSLB parameters as applicable to your deployment.

Controller Group Configuration Example

These commands add a GSLB controller to the default GSLB group, enable the device's membership in the group, and display group information:

```
ACOS(config)# gslb group default
ACOS(config-gslb group:default)# enable
ACOS(config-gslb group:default)# primary 192.168.101.72

ACOS(config-gslb group:default)# show gslb group brief
                      Pri = Priority, Attrs = Attributes
                          D = Disabled, L = Learn
                          P = Passive, * = Master
Name                              Pri Attrs Master          Member
-------------------------------------------------------------------------------
---
default                           100 L     192.168.101.72  2

ACOS(config-gslb group:default)# show gslb group
                      Pri = Priority, Attrs = Attributes
                          D = Disabled, L = Learn
                          P = Passive, * = Master
Group: default, Master: 192.168.101.72
Member          ID       Pri Attrs  Status
-------------------------------------------------------------------------------
---
local           22e40d29 255 L*     OK
192.168.1.131   941a1229 100         Synced
192.168.1.132   ab301229 100 P       Synced
```

SSL Support

All the GSLB locations, termed as GSLB sites connect to a central node, GSLB controller, to communicate various information like site health, load, location, distance from client, and so on.
This controller is configured as a DNS device for the clients and based on the above information, the controller prioritizes the DNS response list and send it to client, guiding it to the right server.

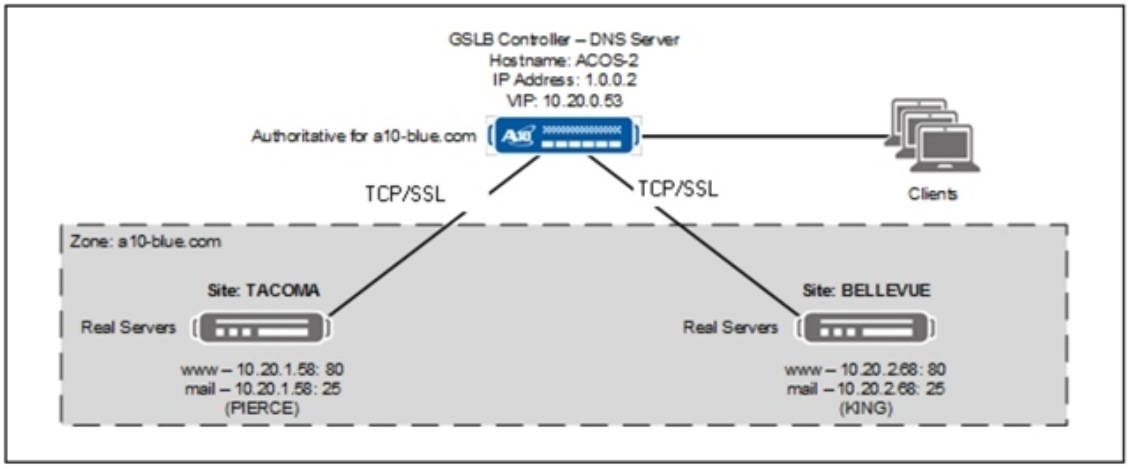
GSLB Protocol Connection between a GSLB Controller and GSLB site-device uses a TCP connection can be encrypted with SSL by default, and supports client/server certificates as a mechanism to identify and trust the GSLB peer. User can upload or generate SSL certificates using existing PKI infrastructure. This is also valid for GSLB group connections.

SSL support is provided over GSLB communication channel. ACOS supports importing SSL Certificate and Key through a text format file. A new SSL certificate and key processing support is available with existing PKI commands and the certification and key can be imported directly through the contents of the related files. Tenants can complete the operation through the command line.

The following limitations are valid for SSL support:

- There is no support for chain certificate and CRL configurations.
- Password protected keys are not supported.
- Web server certificate and key pair is set as global certificate and key pair by default.

Figure 1 : "Secure GSLB network



CLI Configuration

The following options are available for Secure GSLB configuration on ACOS CLI as a part of SSL support for GSLB:

- Use the following command to enable secure GSLB. This ACOS device can only connect to peer devices with SSL Secured GSLB. This is the default option.

```
ACOS(config)# gslb protocol secure enable
```

- Use this option to disable secure GSLB.

```
ACOS(config)# gslb protocol secure disable
```

- Use the following command to enable secure GSLB and revert to non-secure GSLB when site peer devices do not have Secure GSLB active.

```
ACOS(config)# gslb protocol secure enable-fallback
```

- To see SSL specific statistics, use:

```
ACOS(config)# show gslb statistics secure
```

The shared partitions have a per-partition configuration option and functions similar to any other L3V partition with these configurations.

If GSLB is configured per partition, it has priority over global configuration for that particular partition. By default it is set to **`use-global-config`**, to follow the behaviour configured globally under "**`gslb protocol secure`**" in shared partition.

For example, if global configuration has GSLB protocol secure disabled, and in a particular partition, the configuration has GSLB secure-attributes enabled, then this partition will have SSL enabled, and all other partitions will have SSL disabled.

Secure SSL Attributes Configuration

The following options are available to configure secure SSL attributes:

NOTE: When GSLB secure SSL behavior is changed, the established connections will not be affected. New connections will follow the updated behavior.
For GSLB group member "**`show gslb protocol`**" output will show “None” for "**`Secure Configuration`**" and "**`Current SSL State`**" as it is under Group Control.

- To configure secure attributes like SSL certificates and related configuration, use the command:
```
ACOS (config)# gslb secure-attributes
```
- To enable secure attributes configuration, use the command:
```
ACOS (config-secure-attributes)# enable
```
- Use the following command to enable attributes for secure GSLB and revert to non-secure GSLB when site peer devices do not have Secure GSLB active.
```
ACOS (config-secure-attributes)# enable-fallback
```
- To configure, certificate/key pair to be used for SSL handshake. This configuration is also per-partition.To configure secure attributes SSL certificate and SSL key name for secure GSLB, use the command:
```
ACOS (config-secure-attributes)# cert cert_ssl key ssl_1
```

NOTE: The **`cert`** (certificate) and **`key`** used in this configuration, must already exist on the box, which are configured using existing the PKI commands.(**`pki create cert`**, **`import cert`**, **`import key`**) IP security commands,

- Use this option to disable secure GSLB attributes.

```
ACOS(config)# gslb protocol secure disable
```

Partition Management

The ACOS device supports Global Server Load Balancing (GSLB) configuration within a maximum of 127 partitions. The shared partition and individual partitions can each have their own GSLB configuration parameters. To configure GSLB parameters for an individual partition, assign them to the same partition.

The following GSLB parameters cannot be configured for individual partitions; they are only configured globally and are effective within all ACOS device partitions:

1. GSLB system-wide settings: **`gslb system`**, **`gslb dns`**, **`gslb protocol`**, and **`gslb active-rdt`**
2. GSLB geo-locations (**`gslb geo-location`**)

GSLB parameter labels do not span partitions; zones in two partitions cannot use the same zone name.

For each partition, you can create one group, the “partition group”. Only one GSLB Group is supported to implement mapping. The following synchronization scenario is supported: from shared partition group to shared partition group. View and inheritance features are not supported in this release.

For additional information about L3V Partitions, see the *System Configuration and Administration Guide*.

In the actual deployment, NS1 and NS2 would be in different subnets (e.g. 10.100.x.x and 10.120.x.x).

Since the two sites will have local DNS servers and different subnets, we can use a geo-location mapping to reply to Main Campus requests with the Main Campus internal ADFS VIP and reply to South Campus requests with the South Campus internal ADFS VIP. Note that the source IP for the requests will be the IP of the local DNS server, so the geo-location config for each site should correspond with the subnet of the local DNS server. The metric-order for the Internal partition GSLB policy could begin with health-check and geo-location, whereas the metric-order for the DMZ partition GSLB policy could begin with health-check and admin IP.

IPv6 Support

IPv6 support has been provided for Global Server Load Balancing configurations that exclusively supported only IPv4 options. This feature helps in migration of GSLB network operations to IPv6. The following feature supports:

- IPv6 parity for GSLB
- GSLB Protocol Connection with IPv6
- GSLB Group connection with IPv6
- aRDT enhancement for IPv6

CLI Configuration

The `gslb protocol auto-detect` and `gslb protocol use-mgmt-port` commands function through API and CLI in GSLB configuration mode for a GSLB device with IPv6 address.

- To configure GSLB site SLB device with IPv6 address use the `gslb site command` as follows:

```
ACOS(config)# gslb site site1 slb-dev SLBDEV1 2001:db8:0:200::7
```

- To configure GSLB group primary device with IPv6 address, use:

```
ACOS(config)# gslb group group1 enable primary 2001:db8:0:200::1
```

```
ACOS(config)# gslb group default enable primary 2001:db8:0:200::1
priority 1
```

- To configure DNS discovery on GSLB group primary device with IPv6 address, use to resolve to IPv4 and IPv6.

```
[no] dns-discover [resolve-to-ipv4 | resolve-to-ipv6 | resolve-to-ipv4-
and-ipv6]
```

- To configure terminal with client IPv6 subnet mask for active RDT, use the new IPv6 mask under this context. The default is 128:

```
ACOS(config)# gslb site sitename
ACOS(config-gslb site:sitename)# active-rdt ipv6-mask 128
```

NOTE: To view IPv6 mask, use the command, `show gslb rdt controller active` command. The show commands have an IPv6 option, `show gslb samples rdt slb-device active ipv6 <ipv6_address>`, `show gslb samples rdt controller active ipv6 <ipv6_address>`To view GSLB statistics for SLB device, `show gslb slb-device`

aXAPI provides IPv6 compatibility support for GSLB configurations that previously supported only IPv4 options.

Configuration Example

Configure a GSLB site to IPv6 address in GSLB protocol mode.

Protocol:

```
gslb site ACOS
  slb-dev ipv6-ACOS 2001:206::2
```

Configure a GSLB group to IPv6 address in GSLB protocol mode.

Group:

```
gslb group default
  enable
  primary 172.16.204.3
  primary-ipv6 2001:204::3
  priority 255
```

aVCS

Typical aVCS deployments support a virtual chassis with multiple devices. Real-time configuration synchronization results in virtual chassis devices with identical GSLB configurations. This can result in multiple GSLB controllers tying for highest priority. In this case, the controller with the highest last 4 bytes in its management interface MAC address is elected group master.

NOTE: Configure all primary IPs instead of "floating-ip" when using "standalone" option for VCS topology.

GSLB groups synchronize configuration between ACOS devices. When a group is enabled and the GSLB configuration can be managed by the GSLB group, aVCS does not synchronize the GSLB
configuration to the vBlade. When the vMaster is not the same device as the GSLB group master, configuring GSLB in a member controller requires enabling the config-anywhere option in the GSLB group.

Cloud Computing Support

GSLB supports dynamic generation of a service IP based on the ACOS device hostname. When an SLB has an FQDN but lacks the associated IP address, the GSLB protocol provides for querying the DNS server for an A record or CNAME record to learn the device IP address. The GSLB ACOS device, or GSLB controller, can acquire the IP address of the device and apply it to the service-ip. This information is used to configure the SLB server (with hostname) as an ip-server or vip-server of a GSLB site. The IP address that appears in the A record or CNAME record becomes the SLB service-ip.

The feature supports IPv4 resource records and does not support IPv6 records.

The GSLB Cloud Computing Solution may be appropriate when using multiple web-based service providers to provide server load balancing services. It can allow you to shift from one web-based service provider to another to use services that cost less or that have better health metrics. When using a cloud-based SLB service provider for web-based services, the provider sends a CNAME record to access the cloud servers. The cloud servers can be dynamically imported into the ACOS device through the CNAME record in order to do GSLB.

The example below shows the generation of dynamic service-ip addresses by hostname via DNS. This can be accomplished using the following CLI configurations on an ACOS device:

1. Configure the cloud-based service provider number 1:

```
ACOS(config)# slb server www www.example2.com
ACOS(config-real server)# exit
```

2. Configure the cloud-based service provider number 2:

```
ACOS(config)# slb server mail mail.example2.com
ACOS(config-real server)# exit
```

3. Configure the cloud-based service provider number 3:

```
ACOS(config)# slb server www1 www1.example2.com
ACOS(config-real server)# exit
```

4. Configure three sites for each web-based service provider:

```
ACOS(config)# gslb site sanjose
ACOS(config-gslb site:sanjose)# slb-dev ACOS5200 192.168.1.2
ACOS(config-gslb site:sanjose-slb dev:ACO...)# exit
ACOS(config-gslb site:sanjose)# ip-server www
ACOS(config-gslb site:sanjose)# ip-server mail
ACOS(config-gslb site:sanjose)# ip-server www1
```

GSLB in Multi-PU Deployment

This section describes the features and configurations specific to GSLB in multi-PU platforms.

For the general multi-PU implementation details, see the *Application Delivery Controller Guide*.

The following topics are covered:

Features and Limitations

Supported Deployment and Topology on Multi-PU

- Server mode
- Proxy mode

- GSLB Controller Groups
- GSLB Site ACOS Devices

Limitations

- Only PU1 allows GSLB controller and devices, GSLB group between PU1 and PU2 is not supported.

Key Considerations

For the general multi-PU key considerations and traffic-flow, see *Application Delivery Controller Guide*.

- The GSLB session IDs are unique for each PU, where PU1 has an even GSLB session ID, and PU2 has an odd GSLB session ID.
- The PKI, certificate, and key are generated as a part of enrollment or renewal process and is executed on the PU1. This information is then copied to the PU2 during enrollment or renewal. The certificate serial number is unique for each PU.

CLI Configuration

This section describes the general CLI configuration guidelines for implementing GSLB in multi-PU platforms to ensure seamless traffic distribution across PU1 and PU2.

1. Configure the chassis application type using the **`chassis-application-type adc`** command.
2. Enable the odd-even IP NAT globally using the **`odd-even-nat-enable`** command for seamless traffic distribution across both PUs.
3. Configure IP NAT pools using the **`ip nat pool`** or **`ipv6 nat pool`** command to source NAT client traffic.
4. Configure client-side VLAN (or interface ethernet) with traffic distribution mode SIP using the **`traffic-distribution-mode`** command.
5. Configure server-side VLAN (or interface ethernet) with traffic distribution mode DIP using the **`traffic-distribution-mode`** command.
6. Configure the GSLB proxy or server mode.

For details on this configuration, see GUI Configuration or CLI Configuration

If you implement source NAT pool configuration, enable port splitting between PU1 and PU2 using the **system chassis-port-split** command.

7. Verify the configuration and view the show commands for traffic distribution.

CLI Configuration

This section provides the configuration example for GSLB in multi-PU platforms.

Application Type Configuration

```
ACOS(config)# chassis-application-type adc
```

SLB Global Configuration

```
ACOS(config)# slb common
ACOS (config-common)# odd-even-nat-enable
```

IP Address and Default Gateway Configuration

```
ACOS(config)# interface management
ACOS(config-if:management)# ip address 10.65.18.137 255.255.255.0
ACOS(config-if:management)# ip default-gateway 10.65.18.1
ACOS(config-if:management)# secondary-ip address 10.65.18.138
255.255.255.0
ACOS(config-if:management)# secondary-ip default-gateway 10.65.18.1
```

Interface and VLAN Configuration

```
ACOS(config)# interface ethernet 1
ACOS(config-if:ethernet:1)# speed-forced-40g
ACOS(config-if:ethernet:1)# enable
ACOS(config-if:ethernet:1)# lldp enable rx tx
ACOS(config-if:ethernet:1)# exit
ACOS(config)# vlan 10
ACOS(config-vlan:10)# tagged ethernet 1
ACOS(config-vlan:10)# router-interface ve 10
ACOS(config-vlan:10)# traffic-distribution-mode sip
ACOS(config-vlan:10)# exit
```

```
ACOS(config)# vlan 20
ACOS(config-vlan:20)# tagged ethernet 1
ACOS(config-vlan:20)# router-interface ve 20
ACOS(config-vlan:20)# traffic-distribution-mode dip
ACOS(config-vlan:20)# exit
```

IP Interface on VLAN Configuration

```
ACOS(config)# interface ve 10
ACOS(config-if:ve:10)# ip address 10.31.8.35 255.255.255.0
ACOS(config)# interface ve 20
ACOS(config-if:ve:20)# ip address 10.31.9.35 255.255.255.0
ACOS(config-if:ve:20)# exit
```

Common Configuration

```
ACOS(config)# system chassis-port-split enable
```

Source NAT Pool Configuration

```
ACOS(config)# ip nat pool snat1 10.31.9.48 10.31.9.63 netmask /24
ACOS(config)# ip nat pool snat2 10.31.9.64 10.31.9.79 netmask /24
```

GSLB Configuration

```
GSLB proxy mode config:
ACOS(config)# ip nat pool pool-odd-even 20.20.20.61 20.20.20.62 netmask
/24
ACOS(config)# slb server ACOS-11 10.10.0.53
ACOS(config-real server)# port 53 tcp
ACOS(config-real server-node port)# exit
ACOS(config-real server)# exit
ACOS(config)# slb service-group DNS-GP1 tcp
ACOS(config-slb svc group)# member ACOS-11 53
ACOS(config-slb svc group-member:53)# exit
ACOS(config-slb svc group)# exit
ACOS(config)# slb virtual-server DNS1 10.10.0.100
ACOS(config-slb vserver)# port 53 dns-tcp
ACOS(config-slb vserver-vport)# service-group DNS-GP1
ACOS(config-slb vserver-vport)# source-nat pool pool-odd-even
```

```
ACOS(config-slb vserver-vport)# gslb-enable
ACOS(config-slb vserver-vport)# exit
ACOS(config-slb vserver)# exit
```

Show Commands

This section describes the various show commands to view traffic statistics on GSLB multi-PU. All the GSLB module statistics are either aggregated as a single device (PU1+PU2) or displayed separately for PU1 and PU2. The following Show commands display the aggregated statistics:

- **show gslb service-ip**
- **show gslb site**
- **show gslb slb-device**
- **show gslb zone**
- **show gslb service-port**

For more information, see 'Show Commands' section under 'Global Server Load Balancing' in the *Command Line Interface Reference*.

The following is an example of a show command displaying aggregated GSLB counter details.

```
ACOS#show gslb service-ip
      P-Cnt = Count of Service Ports, Attrs = Attributes
      V = Is Virtual Server, D = Disabled
      P = GSLB Protocol,     L = Local Protocol
      M = Manually Health Check, * = Dynamic
Service-IP                                    IP/Desc         Attrs State
P-Cnt Hits
-------------------------------------------------------------------------
------------------------
site1::s2                                     20.20.20.21              Up
1     0
s2::rs-22                                     20.20.20.22     M        Up
4     2
```

GSLB Elements

The DNS distributed database is indexed by domain names, that reference a path in the domain database. A fully qualified domain name (FQDN) is an absolute domain name that is specified relative to the root and identifies a node explicitly, in terms of its location in the namespace hierarchy. GSLB data structures reference FQDNs within a DNS namespace.

The following topics are covered:

Basic Data Structures

GSLB protocol operates on data structures like zone, service, site, and service IP as follows:

- **Zones** – A GSLB zone is a DNS domain for GSLB. An ACOS device can be configured with one or more GSLB zones.

  Example: `mydomain.com` is a zone.

- **Services** – A service is an application, such as HTTP or FTP. Each service is given an FQDN with a zone managed by the GSLB. A zone may include the FQDN of multiple services,

  Example: `www.mydomain.com` is an FQDN where `www` is the HTTP service.

- **Sites** – A site is a server farm that is locally managed by an ACOS device that performs load balancing for the site. Each zone can contain one or more GSLB sites.

- **Service-IP** – A service-ip identifies a virtual server by its IP address and specifies the port that hosts the service provided by the server. The service-ip definition can also include health checks and an external IP address that facilitates access from outside of the internal network.
- **Policies** – A policy is a data structure that defines a set of metric settings and DNS options. After a policy is configured, it is applied to a zone or a service level within a zone. Zones and services use policies to manage client requests by selecting the best site and specifying DNS options for the request.

GSLB zones can be configured with the same domain on multiple partitions, facilitating independent policies for internal and external services for a domain. This also allows the same domain to be configured on different partitions, regardless of the mode each partition is running.

Policies, service groups, and service-IP names can be duplicated in different partitions, but they must be configured separately in each partition. The default GSLB policy is used globally and can only be configured in the shared partition. GSLB site configurations are unique and cannot be duplicated in different partitions.

FQDNs and FQDN Service Groups

The combination of a *service name* and *zone name* comprises a *fully-qualified domain name* (FQDN).

Example: The zone name “example.com” and service name combine to form the “www.example.com” FQDN.

You can configure all of a service’s parameters, including its site, service-IP, and zone membership. You can configure a service and all its required parameters.

An FQDN group combines multiple FQDNs (services) to provide a single point of contact for enabling or disabling services at multiple levels of granularity.

FQDN Service Groups Configuration describes the process of configuring FQDN Service Groups.

GSLB Elements Configuration

These sections describe GSLB Elements:

The following topics are covered:

FQDN String Creation

Zone Configuration

The `gslb zone` command places the device in zone configuration mode, which includes a command that associates a service to the zone. The command creates a zone when it references a zone not yet configured. gslb zone.

Example: This command creates a zone named a10-venus.com and places the device in zone configuration mode.

```
ACOS(config)# gslb zone a10-venus.com
ACOS(config-zone:a10-venus.com)#
```

Service Configuration

The `service` command, available in zone configuration mode, associates a service to the zone and places the device in zone-service configuration mode. The command specifies the port that accesses the service. Multiple services can be defined for a zone. See topic **`gslb zone`** in *Command Line Interface Reference*.

Commands are available in service configuration mode to configure a DNS records for the service, specify DNS traffic actions, enable health check parameters, and configure geo-location settings.

For every GSLB zone, ACOS creates a hidden service to handle NXDOMAIN cases. These services are included in the total GSLB zone service count.

Example: These commands create the www service for the previously created a1-venus.com zone and configure two DNS Address records for the service. The device remains in a10-venus.com-www service configuration after the commands.

```
ACOS(config-zone:a10-venus.com)# service 80 www
ACOS(config-zone:a10-venus.com-service:www)# dns-a-record 10.10.1.1 static
```

```
ACOS(config-zone:a10-venus.com-service:www)# dns-a-record 10.20.1.1 static
ACOS(config-zone:a10-venus.com-service:www)# exit
ACOS(config-zone:a10-venus.com)# exit
```

Example: The following example indicates the log error message received when GSLB zone service creation exceeds the total GSLB zone service limit.

```
ACOS-Active-vMaster[1/1]-gslb:Member(config:1-zone:example123.com)#service
80 www7982
Number of GSLB resources exceeds the current limit
```

Sites Configuration

The `gslb site` command places the device in site configuration mode, that includes commands that associate real servers and a service to the zone. The command creates a new zone when it references a zone that is not yet configured. See topic gslb site.

The `ip-server` command, available from site configuration mode, associates the real server at the specified IP address to the configuration mode site. See topic[no] ip-serverservice-ip.

The `slb-dev` command specifies an access IP address for the site and places the device in slb-dev configuration mode. Within this mode, commands are available that map virtual servers to the site and specifies access attributes to the device. See topic [no] slb-dev device-name [ip-addr].

The `vip-server` command adds the GSLB VIP server to the SLB device.

Example 1: This example creates the “oxygen” site and associates the static service-ip 10.10.1.1 with the site.

```
ACOS(config)# gslb service-ip red-1 10.10.1.1
ACOS(config-service-ip:red-1)# exit
ACOS(config)# gslb site oxygen
ACOS(config-gslb site:oxygen)# ip-server red-1
ACOS(config-gslb site:oxygen)# exit
```

The ip-server command references the name of a previously configured service-ip which, in

addition to the IP address of the real server, defines server implementation parameters within the site.

Example 2: This example creates the “nitrogen” site and associates a virtual server at named static virtual IP 10.10.1.5 with the site. This command includes a command that references an SLB that serves as the virtual server. SLB configuration is beyond the scope of this manual and covered in the ADC Configuration Guide.

```
ACOS(config)# gslb service-ip red-2 10.10.3.211
ACOS(config-service-ip:red-2)# exit
ACOS(config)# gslb site nitrogen
ACOS(config-gslb site:nitrogen)# slb-dev nitro-device 10.10.1.5
ACOS(config-gslb site:nitrogen-slb dev:ni...)# vip-server red-2
```

Service IPs Configuration

A Service IP identifies a virtual server by its IP address and specifies the port that hosts the service provided by the server. The service-ip definition can include health checks and an external IP address to facilitate access from outside the internal network.

The `gslb service-ip` command places the device in service-ip configuration mode. The command creates a service IP when it references one that is not yet configured. See topic gslb service-ip. The service-ip label is referenced by sites to associate servers to the site.

Example: This command creates the blue-1 named static service-ip 10.12.2.1

```
ACOS(config)# gslb service-ip blue-1 10.12.2.1
ACOS(config-service-ip:blue-1)# exit
```

- To assign an external IP address to the service, use the **`external-ip`** command. An external IP address is needed if the service IP address is an internal IP address that cannot be reached from outside the internal network.
- To configure a service port on the service, use the **`port`** command.
- To enable health monitoring of the service, use the **`health-check`** command.

Service-IP Parameters Configuration

These steps describe the process of configuring Service-IP parameters.

Step 1: Select a service-IP type

The following describe the Service IP types and their options

SLB direct-conn real server

The ACOS device you currently are configuring for GSLB is directly connected to the real server. Options include:

- Server – IP address of the server.
- Name – Name for the directly-connected server in the GSLB configuration.
- Health Monitor – Health monitor used to check the reachability and responsiveness of the service.

SLB self-service device

The ACOS device you currently are configuring for GSLB is also the ACOS device that is configured to perform SLB for the VIP that provides the service to clients. This is the VIP bound to a service group containing the real servers on which the service is located. Options include:

- VIP – Virtual IP address.
- Name – Name for the virtual server.
- Dev Name – Name for the SLB device (this device) in the GSLB configuration.
- Health Monitor – Health monitor for checking the reachability and responsiveness of the service.

SLB device

The service is load balanced by another ACOS device. Options include:

- Device Name – Name for the SLB device. (This name does not need to be the same as the hostname of the SLB device, although this is a handy way to simplify administration.)
- Device IP – IP address of the SLB device.
- VIP – VIP address.
- Name – Name for this SLB device in the GSLB configuration.

- Health Monitor – Health monitor for checking the reachability and responsiveness of the service.

Step 2: Configure DNS Records

Configure DNS records for the service. GSLB returns these records, when applicable, in response to DNS requests. You can configure the following types of records:

- MX – Mail Exchange record.
- CNAME – Canonical Name record.
- NS – Name Server record.
- SRV – Service Record.
- PTR – Pointer record.
- TXT – Text record.
- CAA – Certificate Authority Authorization record.

An Address (A) record for the service-IP is created automatically.

Step 3: Manually Configure Geo-location Entries (If Required)

A geo-location maps a range of client IP addresses to a description of the clients' geographic location. GSLB includes an IANA geo-location database, which is loaded by default.

Create a geo-location string name, then configure one of the following:

- Alias – Returns this alias for the geo-location.
- Action – To perform on DNS queries for the FQDN:
  - Forward Response – Forwards responses to the local DNS server, but does not forward queries to the Authoritative DNS server.
  - Forward Both – Forwards queries to the Authoritative DNS server, and forwards responses to the local DNS server.
  - Forward Query – Forwards queries to Authoritative DNS server; does not forward responses to local DNS server.
  - Drop – Drops DNS queries from the local DNS server.

- Ignore – Sends an empty response.
- Reject – Rejects DNS queries from the local DNS server and returns the "Refused" message in replies.

- Policy – Uses the selected GSLB policy instead of the policy used by the zone.

```
ACOS(config-policy:default)#
```

Types of IPs Used in GSLB Configuration

GSLB configurations include various scenarios where IP addresses are configured for a particular purpose. The following table lists the different nomenclature for IPs and details the configurations in which the IPs are implemented and used.

The following table displays the different types of IPs used in GSLB configuration.

Table 1 : Types of IPs, usage, and examples

Type of IP	Description	Configuration and sample	Usage

Static IP	This is a GSLB service-ip. It can be the IP address of the virtual server or the real server. It can be an IPv4 or IPv6 address.
	
	Users provide this IP. The IP address does not change.
		`gslb service-ip s1 1.1.1.1 port 53 udp`
		
		Example configuration:
		
		`gslb site site1 ip-server s1`
			The `ip-server` command binds the service-ip to the site. The IP is a local gslb service-ip or a local SLB real server IP owned by a local device. The static IP can also include an external IP address that facilitates access from outside of

Table 1 : Types of IPs, usage, and examples

Type of IP	Description	Configuration and sample	Usage
			the internal network.

Dynamic IP	This is the IP of the GSLB slb-device. This is the dynamic virtual IP server. It is created by the backend using the auto-detect feature.	`gslb site site1`
		`  slb-dev d1 10.1.1.1`
		`  auto-detect ip-and-port`
		fqdn vip-server - dynamic vip-server resolved from hostname slb-device. The following is an example configuration:
		`gslb site site1`
		`  slb-dev d1 Example Domain`
		`  auto-detect ip-and-port`
			Dynamically configures the interfaces based on the connected device name. The SLB device and FQDN is used to auto detect the dynamic virtual server IP address and port number. Reduces the need for manual configuration and speeds up deployment.

Named Static Virtual IP	The named static vip-server is a remote virtual IP resource on a remote slb-device corresponding to a locally defined GSLB service-ip object. It supports scaleout service-ip.	Example basic configuration:
		`slb site site1`
		`  slb-dev d1 10.1.1.1`
		`  vip-server s1`
		Example scaleout service-ip configuration:
			Processes client's requests and sends the response back through the SLB device to the

Table 1 : Types of IPs, usage, and examples

Type of IP	Description	Configuration and sample	Usage
		gslb site site1 slb-dev d1 10.1.1.1 vip-server s1 slb-dev d2 10.1.1.2 vip-server s1	client.
Fixed IP vip-server	The fixed IP vip-server is a remote virtual IP resource on a remote slb-device that may or may not be dynamic. It corresponds to a locally defined GSLB service-ip object.	gslb site site1 slb-dev d1 10.1.1.1 vip-server 10.1.1.100	Maps the SLB site to a globally configured GSLB service IP address.

FQDN Service Groups Configuration

An FQDN service group consists of multiple FQDNs Service groups simplify administration, by
providing a single location for enabling or disable services at any of the following levels of granularity

- Entire FQDN group (all zones in the group, and all their services)
- Individual sites (all services within the site)
- Individual FQDNs (individual services in individual zones)

The `gslb service-group` command places the device in service-group configuration mode. See topic gslb service-group.

Commands that are available in this mode include:

- Member — adds a specified service to the group. ([no] member service-name.zone-name)

- Persistent site — Implements site persistence for the group. ([no] persistent site [AGE][V4][V6])

  Example: These commands create an FQDN group called “example-group” and add an FQDN for GSLB services to it.

```
ACOS(config)# gslb service-group example-group
ACOS(config-svc group:example-group)# member www.example.com
ACOS(config-svc group:example-group)#
```

FQDN Partial Match Configuration

Currently, creating a wild card FQDN works when the exact octet DNS query matches. DNS FQDNs’ are more complex when they are generated from cloud-based applications.

Partial match support is based and built for cloud applications. The supported functions are:

- Starts-with
- Ends-with
- Contains

Let us consider www.dev.a10networks.com as an example.

- dev* is equivalent to starts-with. Any domain name which starts with dev will match the request
- *dev is equivalent to ends-with. Any domain name which ends with dev will match the request
- *dev* is equivalent to contains condition. Any domain name which contains dev will match the request

```
ACOS(config)# gslb service-ip test1 1.1.1.1
ACOS(config-service-ip:test1)# health-check-protocol-disable
ACOS(config-service-ip:test1)# health-check-disable
ACOS(config-service-ip:test1)# port 0 tcp
ACOS(config-service-ip:test1-port:tcp)# health-check-protocol-disable
ACOS(config-service-ip:test1-port:tcp)# health-check-disable
ACOS(config-service-ip:test1-port:tcp)# gslb site site1
```

```
ACOS(config-gslb site:site1)# ip-server test1
ACOS(config-gslb site:site1)# gslb policy server
ACOS(config-policy:server)# dns server authoritative
ACOS(config-policy:server)# gslb zone com
ACOS(config-zone:com)# policy server
ACOS(config-zone:com)# service 0 dev*
ACOS(config-zone:com-service:dev*)# dns-a-record test1 static
ACOS(config-zone:com-service:dev*)# service 1 *dev
ACOS(config-zone:com-service:*dev)# dns-a-record test1 static
ACOS(config-zone:com-service:*dev)# service 2 *dev*
ACOS(config-zone:com-service:*dev*)# dns-a-record test1 static
```

Implementation Examples

This section lists the GSLB configuration steps (Basic Configuration) and contains CLI commands that implement several GSLB scenarios.

The following topics are covered:

Basic Configuration

The basic GSLB configuration requires these steps:

The following topics are covered:

FQDN String Configuration

Create an FQDN string by configuring a zone and the service that corresponds to that string.

If a custom policy is required, create a GSLB policy to specify a set of metrics and DNS options.

To implement the custom policy, apply it to the zone or individual services.

(Optional) Configure an action to perform on DNS queries for the FQDN:

- Forward Response – Forwards responses to local DNS server; does not forward queries to Authoritative DNS server.
- Forward Both – Forwards queries to Authoritative DNS server; forwards responses to local DNS server.
- Forward Query – Forwards queries to Authoritative DNS server; does not forward responses to local DNS server.
- Drop – Drops DNS queries from local DNS server.
- Ignore – Sends an empty response.
- Reject – Rejects DNS queries from local DNS server; returns “Refused” message in replies.
- Enable or disable the service.

Site Configuration

Select a Site to configure with the FQDN.

If needed, apply a GSLB template to the FQDN configuration.

Configure the weight (bias) for the site, or use the default (1).

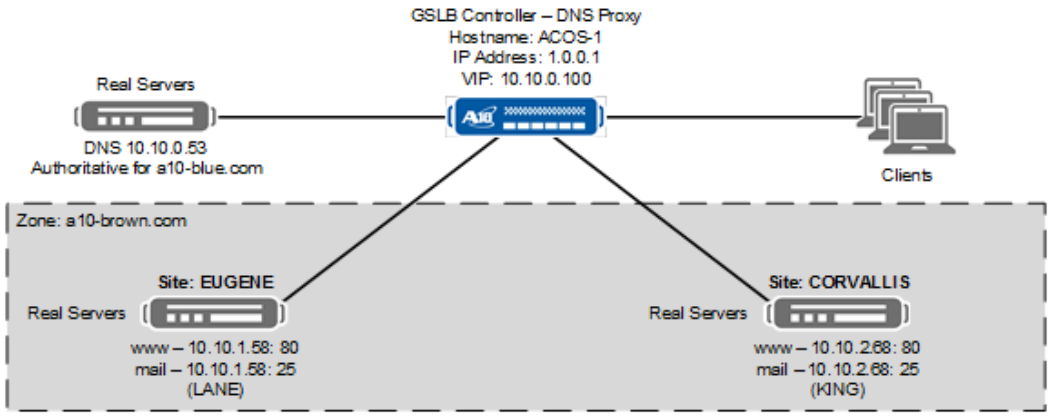
Service-IP Parameters Configuration

1. Select a service-IP type. Step 1: Select a service-IP type
2. Configure DNS Records. Step 2: Configure DNS Records
3. Manually configure Geo-Location entries. Step 3: Manually Configure Geo-location Entries (If Required)

Scenario 1: Proxy Mode

This scenario presents a GSLB Proxy Mode configuration, depicted in Figure 2, that requires these steps:

Figure 2 : Scenario 1: GSLB Proxy Mode



Device ACOS-1: Creating a VIP for DNS Queries

These commands create and enable the VIP for GSLB client DNS queries.

```
vThunder(config)# hostname ACOS-1
ACOS-1(config)# slb server ACOS-11 10.10.0.53
ACOS-1(config-real server)# port 53 tcp
ACOS-1(config-real server-node port)# exit
ACOS-1(config-real server)# exit
ACOS-1(config)# slb service-group DNS-GP1 tcp
ACOS-1(config-slb svc group)# member ACOS-11 53
ACOS-1(config-slb svc group-member:53)# exit
ACOS-1(config-slb svc group)# exit
ACOS-1(config)# slb virtual-server DNS1 10.10.0.100
ACOS-1(config-slb vserver)# port 53 dns-tcp
ACOS-1(config-slb vserver-vport)# service-group DNS-GP1
ACOS-1(config-slb vserver-vport)# gslb-enable
ACOS-1(config-slb vserver-vport)# exit
ACOS-1(config-slb vserver)# exit
ACOS-1(config)#
```

Device ACOS-1: Service IP Assignment

These commands associate two servers with GSLB labels that can be referenced by GSLB sites.

```
ACOS-1(config)# gslb service-ip LANE 10.10.1.58
```

```
ACOS-1(config-service-ip:LANE)# port 80 tcp
ACOS-1(config-service-ip:LANE-port:tcp)# exit
ACOS-1(config-service-ip:LANE)# port 25 tcp
ACOS-1(config-service-ip:LANE-port:tcp)# exit
ACOS-1(config-service-ip:LANE)# exit
ACOS-1(config)# gslb service-ip BENTON 10.10.2.68
ACOS-1(config-service-ip:BENTON)# port 80 tcp
ACOS-1(config-service-ip:BENTON-port:tcp)# exit
ACOS-1(config-service-ip:BENTON)# port 25 tcp
ACOS-1(config-service-ip:BENTON-port:tcp)# exit
ACOS-1(config-service-ip:BENTON)# exit
```

Device ACOS-1: GSLB Site

These commands create a GSLB site and binds the virtual servers to the site. ((missing or bad snippet)Sites Configuration).

```
ACOS-1(config)# gslb site EUGENE
ACOS-1(config-gslb site:EUGENE)# ip-server LANE
ACOS-1(config-gslb site:EUGENE)# exit
ACOS-1(config)# gslb site CORVALLIS
ACOS-1(config-gslb site:CORVALLIS)# ip-server BENTON
ACOS-1(config-gslb site:CORVALLIS)# exit
```

Device ACOS-1: GSLB Policy

These commands create a GSLB policy that, when applied, places the device in proxy mode for the specified zone. By default, policies place a zone in proxy mode.

```
ACOS-1(config)# gslb policy HELIUM
ACOS-1(config-policy:HELIUM)# exit
```

Device ACOS-1: GSLB Zone

These commands create a GSLB zone and implement two services within the zone. DNS address records are included for each zone. ((missing or bad snippet)FQDN String Creation).

```
ACOS-1(config)# gslb zone a10-brown.com
ACOS-1(config-zone:a10-brown.com)# policy HELIUM
ACOS-1(config-zone:a10-brown.com)# service 80 www
ACOS-1(config-zone:a10-brown.com-service:www)# dns-a-record LANE static
```

```
ACOS-1(config-zone:a10-brown.com-service:www)# dns-a-record BENTON
static
ACOS-1(config-zone:a10-brown.com-service:www)# exit
ACOS-1(config-zone:a10-brown.com)# service 25 mail
ACOS-1(config-zone:a10-brown.com-service:m...)# dns-a-record LANE static
ACOS-1(config-zone:a10-brown.com-service:m...)# dns-a-record BENTON
static
ACOS-1(config-zone:a10-brown.com-service:m...)# exit
ACOS-1(config-zone:a10-brown.com)# exit
```

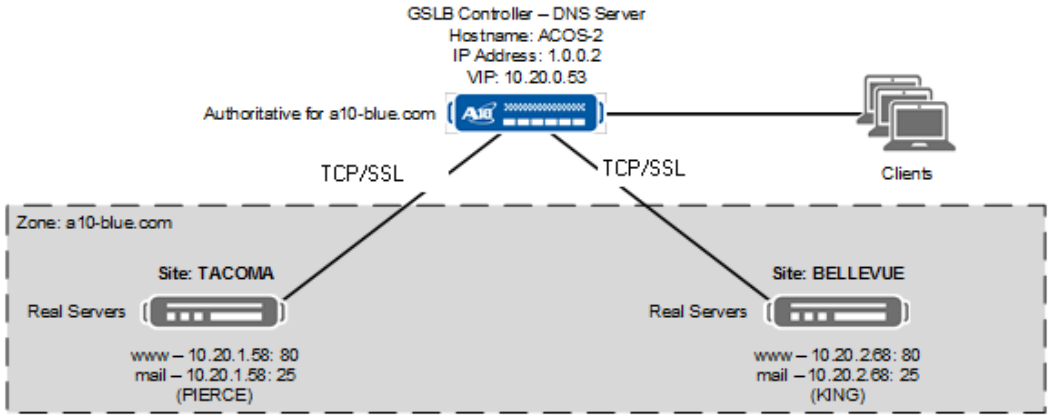
Device ACOS-1: Displaying the Configuration

```
ACOS-1(config)# show run | sec slb
slb server ACOS-11 10.10.0.53
  port 53 tcp
slb service-group DNS-GP1 tcp
  member ACOS-11 53
slb virtual-server DNS1 10.10.0.100
  port 53 dns-tcp
    gslb-enable
    service-group DNS-GP1
gslb service-ip LANE 10.10.1.58
  port 80 tcp
  port 25 tcp
gslb service-ip BENTON 10.10.2.68
  port 80 tcp
  port 25 tcp
gslb site EUGENE
  ip-server LANE
gslb site CORVALLIS
  ip-server BENTON
gslb policy HELIUM
gslb zone a10-brown.com
  policy HELIUM
  service 80 www
    dns-a-record BENTON static
    dns-a-record LANE static
  service 25 mail
    dns-a-record BENTON static
    dns-a-record LANE static
```

Scenario 2: Server Mode

This scenario is presents a GSLB Server Mode configuration, depicted in Scenario 2: GSLB Server Mode , requiring these steps:

Figure 3 : Scenario 2: GSLB Server Mode



Device ACOS-2: Creating a VIP for DNS Queries

These commands create and enable the VIP for GSLB client DNS queries.

```
vThunder(config)# hostname ACOS-2
ACOS-2(config)# slb virtual-server DNS2 10.20.0.53
ACOS-2(config-slb vserver)# port 53 dns-tcp
ACOS-2(config-slb vserver-vport)# gslb-enable
ACOS-2(config-slb vserver-vport)# exit
ACOS-2(config-slb vserver)# exit
```

Device ACOS-2: Service IP Assignment

These commands associate two servers with GSLB labels that can be referenced by GSLB sites.

```
ACOS-2(config)# gslb service-ip PIERCE 10.20.1.58
ACOS-2(config-service-ip:PIERCE)# port 80 tcp
ACOS-2(config-service-ip:PIERCE-port:tcp)# exit
ACOS-2(config-service-ip:PIERCE)# port 25 tcp
ACOS-2(config-service-ip:PIERCE-port:tcp)# exit
```

```
ACOS-2(config-service-ip:PIERCE)# exit
ACOS-2(config)# gslb service-ip KING 10.20.2.68
ACOS-2(config-service-ip:KING)# port 80 tcp
ACOS-2(config-service-ip:KING-port:tcp)# exit
ACOS-2(config-service-ip:KING)# port 25 tcp
ACOS-2(config-service-ip:KING-port:tcp)# exit
ACOS-2(config-service-ip:KING)# exit
```

Device ACOS-2: GSLB Site

These commands create two GSLB sites and bind the virtual servers to the sites. (Sites Configuration)

```
ACOS-2(config)# gslb site TACOMA
ACOS-2(config-gslb site:TACOMA)# ip-server PIERCE
ACOS-2(config-gslb site:TACOMA)# exit
ACOS-2(config)# gslb site BELLEVUE
ACOS-2(config-gslb site:BELLEVUE)# ip-server KING
ACOS-2(config-gslb site:BELLEVUE)# exit
```

Device ACOS-2: GSLB Policy

These command create a GSLB policy that, when applied, places the device in server mode for the specified zone.

```
ACOS-2(config)# gslb policy BORON
ACOS-2(config-policy:BORON)# dns server
ACOS-2(config-policy:BORON)# dns server authoritative
ACOS-2(config-policy:BORON)# exit
```

Device ACOS-2: GSLB Zone

These commands create a GSLB zone and implement two services within the zone. DNS address records are included for each zone ((missing or bad snippet)FQDN String Creation).

```
ACOS-2(config)# gslb zone a10-blue.com
ACOS-2(config-zone:a-blue.com)# policy BORON
ACOS-2(config-zone:a-blue.com)# service 80 www
ACOS-2(config-zone:a-blue.com-service:www)# dns-a-record PIERCE static
ACOS-2(config-zone:a-blue.com-service:www)# dns-a-record KING static
ACOS-2(config-zone:a-blue.com-service:www)# exit
ACOS-2(config-zone:a-blue.com)# service 25 mail
```

```
ACOS-2(config-zone:a-blue.com-service:mail)# dns-a-record PIERCE static
ACOS-2(config-zone:a-blue.com-service:mail)# dns-a-record KING static
ACOS-2(config-zone:a-blue.com-service:mail)# exit
ACOS-2(config-zone:a-blue.com)# exit
```

Device ACOS-2: Displaying the Configuration

```
ACOS-2(config)# show run | sec slb
slb virtual-server DNS2 10.20.0.53
  port 53 dns-tcp
    gslb-enable
gslb service-ip PIERCE 10.20.1.58
  port 80 tcp
  port 25 tcp
gslb service-ip KING 10.20.2.68
  port 80 tcp
  port 25 tcp
gslb site TACOMA
  ip-server PIERCE
gslb site BELLEVUE
  ip-server KING
gslb policy BORON
  dns server authoritative
gslb zone a10-blue.com
  policy BORON
  service 80 www
    dns-a-record KING static
    dns-a-record PIERCE static
  service 25 mail
    dns-a-record KING static
    dns-a-record PIERCE static
```

Scenario 3: Zone Owner Mode

This scenario presents a GSLB Zone Owner Mode configuration, as shown in Figure 4:

Figure 4 : Scenario 1: GSLB Proxy Mode

Device ADC01: Creates a VIP for DNS Queries

These commands create and enable the VIP for GSLB client DNS queries.

```
vThunder(config)# hostname ADC01
ADC01(config)# slb server ADC01 50.0.0.2
ADC01(config-real server)# port 80 tcp
ADC01(config-real server-node port)# exit
ADC01(config-real server)# port 443 tcp
ADC01(config-real server-node port)# exit
ADC01(config-real server)# exit
ADC01(config)# slb service-group sg_www443 tcp
ADC01(config-slb svc group)# member ADC01 80
ADC01(config-slb svc group-member:80)# exit
ADC01(config-slb svc group)# member ADC01 443
ADC01(config-slb svc group-member:443)# exit
ADC01(config-slb svc group)# exit
ADC01(config)# slb virtual-server GSLB_VIP 192.168.0.100
ADC01(config-slb vserver)# port 53 dns-udp
ADC01(config-slb vserver-vport)# gslb-enable
ADC01(config-slb vserver-vport)# exit
ADC01(config-slb vserver)# exit
ADC01(config)#
```

Device ADC01: Service IP Assignment

These commands associate two servers with GSLB labels that can be referenced by GSLB sites.

```
ADC01(config)# gslb service-ip VIP01 192.168.0.121
ADC01(config-service-ip:VIP01)# port 443 tcp
ADC01(config-service-ip:VIP01-port:tcp)# exit
ADC01(config-service-ip:VIP01)# port 80 tcp
ADC01(config-service-ip:VIP01-port:tcp)# exit
ADC01(config-service-ip:VIP01)# exit
```

Device ADC01: GSLB Site

These commands create a GSLB site and binds the virtual servers to the site.

```
ADC01(config)# gslb site DOMESTIC
ADC01(config-gslb site:DOMESTIC)# slb-dev A 10.23.14.130
ADC01(config-gslb site:DOMESTIC)# exit
ADC01(config)# gslb service-ip VIP01
```

```
ADC01(config-service-ip:VIP01)# exit
```

Device ADC01: GSLB Policy

These commands create a GSLB policy that, when applied, places the device in proxy mode for the specified zone. By default, policies place a zone in proxy mode.

```
ADC01(config)# gslb policy policy-zone
ADC01(config-policy:policy-zone)# dns server any authoritative zone-owner-mode
ADC01(config-policy:policy-zone)# exit
```

Device ADC01: GSLB Zone

These commands create a GSLB zone and implement two services within the zone. DNS address records are included for each zone.

```
ADC01(config)# gslb zone example.com
ADC01(config-zone:example.com)# policy policy-zone
ADC01(config-zone:example.com)# dns-a-record example.com a10@example.com expire 1200 refresh 200 retry 5 serial 123456
ADC01(config-zone:example.com)# service 443 www
ADC01(config-zone:example.com-service:www)# dns-a-record VIP01 static
ADC01(config-zone:example.com-service:www)# exit
ADC01(config-zone:example.com)# service 80 www80
ADC01(config-zone:example.com-service:www80)# dns-a-record VIP01 static
ADC01(config-zone:a10-brown.com-service:www80)# exit
ADC01(config-zone:example.com)# exit
```

Device ADC01: Displays the Configuration

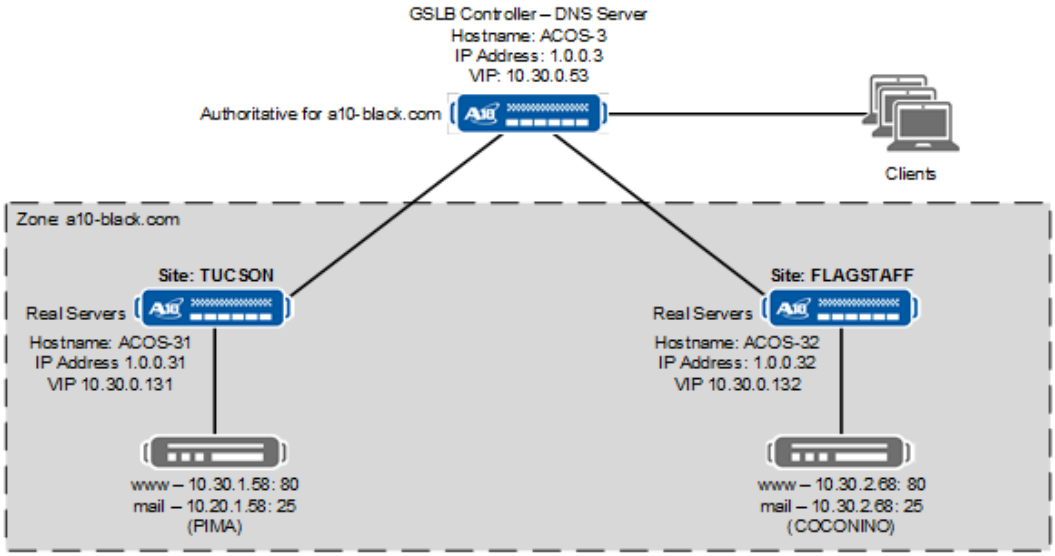
```
ADC01(config)# show run
```

```
slb server ADC01 50.0.0.2
  port 80 tcp
  port 443 tcp
!
slb service-group sg_www443 tcp
  member ADC01 80
  member ADC01 443
!
slb virtual-server GSLB_VIP 192.168.0.100
  port 53 dns-udp
    gslb-enable
!
gslb service-ip service-ip-VIP01 192.168.0.121
  port 443 tcp
  port 80 tcp
!
gslb service-ip VIP 192.168.0.124
!
gslb site DOMESTIC
  slb-dev A 10.23.14.130
!
gslb policy policy-zone
  dns server any authoritative zone-owner-mode
!
gslb zone example.com
  policy policy-zone
  dns-soa-record example.com a10@example.com expire 1200 refresh 200
retry 5 serial 123456
  service 443 www
    dns-a-record service-ip-VIP01 static
  service 80 www80
    dns-a-record service-ip-VIP01 static
!
!
end
```

Scenario 4: Controllers and Site Devices

This scenario presents a GSLB Server Mode configuration that includes one A10 device configured as a GSLB controller and two A10 devices configured as GSLB site devices, as depicted in Figure 5. The configuration requires these steps:

Figure 5 : Scenario 3: GSLB Server Mode – Controller and Devices



Device ACOS-3: Creating a VIP for DNS Queries

These commands create and enable the VIP for GSLB client DNS queries.

```
vThunder(config)# hostname ACOS-3
ACOS-3(config)# slb virtual-server DNS3 10.30.0.53
ACOS-3(config-slb vserver)# port 53 dns-tcp
ACOS-3(config-slb vserver-vport)# gslb-enable
ACOS-3(config-slb vserver-vport)# exit
ACOS-3(config-slb vserver)# exit
```

Device ACOS-3: Service IP Assignment

This code configures the service IP addresses.

```
ACOS-3(config)# gslb service-ip PIMA 10.30.0.131
ACOS-3(config-service-ip:PIMA)# port 80 tcp
```

```
ACOS-3(config-service-ip:PIMA-port:tcp)# exit
ACOS-3(config-service-ip:PIMA)# port 25 tcp
ACOS-3(config-service-ip:PIMA-port:tcp)# exit
ACOS-3(config-service-ip:PIMA)# exit
ACOS-3(config)# gslb service-ip COCONINO 10.30.0.132
ACOS-3(config-service-ip:COCONINO)# port 80 tcp
ACOS-3(config-service-ip:COCONINO-port:tcp)# exit
ACOS-3(config-service-ip:COCONINO)# port 25 tcp
ACOS-3(config-service-ip:COCONINO-port:tcp)# exit
ACOS-3(config-service-ip:COCONINO)# exit
```

Device ACOS-3: GSLB Site

For each site SLB device, enter the IP address of the ACOS device that provides SLB at the site. For the VIP server names, enter the named static virtual IP name as previously configured.

```
ACOS-3(config)# gslb site TUCSON
ACOS-3(config-gslb site:TUCSON)# slb-dev ACOS-31 10.30.0.131
ACOS-3(config-gslb site:TUCSON-slb dev:ACOS...)# vip-server PIMA
ACOS-3(config-gslb site:TUCSON-slb dev:ACOS...)# exit
ACOS-3(config-gslb site:TUCSON)# exit
ACOS-3(config)# gslb site FLAGSTAFF
ACOS-3(config-gslb site:FLAGSTAFF)# slb-dev ACOS-32 10.30.0.132
ACOS-3(config-gslb site:FLAGSTAFF-slb dev:A...)# vip-server COCONINO
ACOS-3(config-gslb site:FLAGSTAFF-slb dev:A...)# exit
ACOS-3(config-gslb site:FLAGSTAFF)# exit
```

Device ACOS-3: GSLB Policy

These command create a GSLB policy that, when applied, places the device in server mode for the specified zone.

```
ACOS-3(config)# gslb policy SODIUM
ACOS-3(config-policy:SODIUM)# dns server
ACOS-3(config-policy:SODIUM)# dns server authoritative
ACOS-3(config-policy:SODIUM)# exit
```

Device ACOS-3: GSLB Zone

These commands create a GSLB zone and implement two services within the zone. DNS address records are included for each zone (See “Creating an FQDN String” on

page 32.).

```
ACOS-3(config)# gslb zone a10-black.com
ACOS-3(config-zone:a10-black.com)# policy SODIUM
ACOS-3(config-zone:a10-black.com)# service 80 www
ACOS-3(config-zone:a10-black.com-service:www)# dns-a-record PIMA static
ACOS-3(config-zone:a10-black.com-service:www)# dns-a-record COCONINO
static
ACOS-3(config-zone:a10-black.com-service:www)# exit
ACOS-3(config-zone:a10-black.com)# service 25 mail
ACOS-3(config-zone:a10-black.com-service:mail)# dns-a-record PIMA static
ACOS-3(config-zone:a10-black.com-service:mail)# dns-a-record COCONINO
static
ACOS-3(config-zone:a10-black.com-service:mail)# exit
ACOS-3(config-zone:a10-black.com)# exit
```

Enabling GSLB Protocol on ACOS-3 as a Controller

```
ACOS-3(config)# gslb protocol enable controller
```

Devices ACOS-31 and ACOS-32: Configuring the GSLB Devices

These commands create and enable the VIP for GSLB client DNS queries on ACOS-31.

```
vThunder(config)# hostname ACOS-31
ACOS-31(config)# slb server SERVER-PIMA 10.30.1.58
ACOS-31(config-real server)# port 80 tcp
ACOS-31(config-real server-node port)# exit
ACOS-31(config-real server)# port 25 tcp
ACOS-31(config-real server-node port)# exit
ACOS-31(config-real server)# exit
ACOS-31(config)# slb service-group SG-PIMA-WWW tcp
ACOS-31(config-slb svc group)# member SERVER-PIMA 80
ACOS-31(config-slb svc group-member:80)# exit
ACOS-31(config-slb svc group)# exit
ACOS-31(config)# slb service-group SG-PIMA-MAIL tcp
ACOS-31(config-slb svc group)# member SERVER-PIMA 25
ACOS-31(config-slb svc group-member:25)# exit
ACOS-31(config-slb svc group)# exit
ACOS-31(config)# slb virtual-server VIP-31 10.30.0.131
ACOS-31(config-slb vserver)# port 80 tcp
ACOS-31(config-slb vserver-vport)# service-group SG-PIMA-WWW
```

```
ACOS-31(config-slb vserver-vport)# exit
ACOS-31(config-slb vserver)# port 25 tcp
ACOS-31(config-slb vserver-vport)# service-group SG-PIMA-MAIL
ACOS-31(config-slb vserver-vport)# exit
ACOS-31(config-slb vserver)# exit
```

Enabling GSLB Protocol on ACOS-31 as a Device

```
ACOS-31(config)# gslb protocol enable device
```

These commands create and enable the VIP for GSLB client DNS queries on ACOS-32.

```
vThunder(config)# hostname ACOS-32
ACOS-32(config)# slb server SERVER-COCONINO 10.30.2.68
ACOS-32(config-real server)# port 80 tcp
ACOS-32(config-real server-node port)# exit
ACOS-32(config-real server)# port 25 tcp
ACOS-32(config-real server-node port)# exit
ACOS-32(config-real server)# exit
ACOS-32(config)# slb service-group SG-COCONINO-WWW tcp
ACOS-32(config-slb svc group)# member SERVER-COCONINO 80
ACOS-32(config-slb svc group-member:80)# exit
ACOS-32(config-slb svc group)# exit
ACOS-32(config)# slb service-group SG-COCONINO-MAIL tcp
ACOS-32(config-slb svc group)# member SERVER-COCONINO 25
ACOS-32(config-slb svc group-member:25)# exit
ACOS-32(config-slb svc group)# exit
ACOS-32(config)# slb virtual-server VIP-32 10.30.0.132
ACOS-32(config-slb vserver)# port 80 tcp
ACOS-32(config-slb vserver-vport)# service-group SG-COCONINO-WWW
ACOS-32(config-slb vserver-vport)# exit
ACOS-32(config-slb vserver)# port 25 tcp
ACOS-32(config-slb vserver-vport)# service-group SG-COCONINO-MAIL
ACOS-32(config-slb vserver-vport)# exit
ACOS-32(config-slb vserver)# exit
```

Enabling GSLB Protocol on ACOS-32 as a Device

```
ACOS-32(config)# gslb protocol enable device
```

Scenario 5: Main Campus Basic Configuration

This scenario specifies a sample campus network. Different zones and partitions can be setup for each campus area: South Campus, North Campus, and so on.

Shared partition can be configured with:

- Management IP
- Interfaces and Trunks (Link Aggregation)
- aVCS
- VRRP-A and VRRP-A hello interfaces / VLANs
- GSLB protocol

The perimeter network or screened subnetwork called DMZ setup, can include the following
configurations:

- VLAN configuration
- VLAN interface configuration
- Routing configuration (for example, default route to upstream firewall)
- Source NAT pool
- Client SSL template
- Server SSL template
- Proxy Real Servers
- Proxy Service-group
- Public Proxy VIP
- GSLB VIP
- GSLB service IPs
- GSLB group
- GSLB sites
- GSLB policy
- GSLB zone

Internal zone includes the following configurations:

- VLAN configuration
- VLAN interface configuration
- Routing configuration (e.g. default route to upstream firewall)
- Source NAT pool
- Client SSL template
- Server SSL template
- Proxy real servers
- Proxy service-group
- Public proxy VIP
- GSLB VIP
- GSLB service IPs
- GSLB group
- GSLB sites
- GSLB policy
- GSLB zone

The South Campus can be configured with a similar setup except for the VRRP-A and aVCS
configuration. Other configuration options are user accounts, authentication options, logging, alerts, and more.

Each ACOS device can be configured with a shared or default screened subnetwork, and an Internal partition. This will ensure proper segmentation of DMZ and Internal traffic. The Internal partitions can use the same physical links to the existing switch or firewall infrastructure. The physical interfaces can be enabled in the shared partition, and then VLANs must be configured in each partition and tagged to the physical links that have been enabled in the shared partition. Optionally, The DMZ and Internal
partitions can "own" their physical interfaces. For example, this means that if the DMZ partition has tagged VLANs on Ethernet 1, the Internal partition cannot also tag on Ethernet 1. If this physical port ownership is desired, the interfaces must be enabled from within the desired partition instead of from the shared partition.

Example of enabling interfaces in the shared partitions and tagging VLANs in sub-network and Internal
partitions:

```
ACOS-Active-vMaster# config
ACOS-Active-vMaster(config:1)#int eth 6
ACOS-Active-vMaster(config:1-if:ethernet:6)#enable
This operation applied to device 1
ACOS-Active-vMaster(config:1-if:ethernet:6)#exit
ACOS-Active-vMaster(config:1)#act adfs-internal
Current active partition: adfs-internal
ACOS-Active-vMaster[adfs-internal-gslb:Master](config:1)#vlan 590
ACOS-Active-vMaster[adfs-internal-gslb:Master](config:1-vlan:590)#tagged
ethernet 6
This operation applied to device 1
ACOS-Active-vMaster[adfs-internal-gslb:Master](config:1-vlan:590)#exit
ACOS-Active-vMaster[adfs-internal-gslb:Master](config:1)#act adfs-dmz
Current active partition: adfs-dmz
ACOS-Active-vMaster[adfs-dmz-gslb:Master](config:1)#vlan 490
ACOS-Active-vMaster[adfs-dmz-gslb:Master](config:1-vlan:490)#tagged
ethernet 6
This operation applied to device 1
```

Example of DMZ partition owning Ethernet 6. Internal partition cannot use it now:

```
ACOS-Active-vMaster# config
-vMaster(config:1)#act adfs-dmz
Current active partition: adfs-dmz
ACOS-Active-vMaster[adfs-dmz-gslb:Master](config:1)#int eth 6
This operation applied to device 1
ACOS-Active-vMaster[adfs-dmz-gslb:Master](config:1-if:ethernet:6)#enable
This operation applied to device 1
ACOS-Active-vMaster[adfs-dmz-gslb:Master](config:1-if:ethernet:6)#vlan 490
ACOS-Active-vMaster[adfs-dmz-gslb:Master](config:1-vlan:490)#tagged
ethernet 6
This operation applied to device 1
ACOS-Active-vMaster[adfs-dmz-gslb:Master](config:1-vlan:490)#exit
ACOS-Active-vMaster[adfs-dmz-gslb:Master](config:1)#act adfs-internal
Current active partition: adfs-internal
ACOS-Active-vMaster[adfs-internal-gslb:Master](config:1)#vlan 590
```

```
ACOS-Active-vMaster[adfs-internal-gslb:Master](config:1-vlan:590)#tagged
ethernet 6
Interface is owned by another partition.
```

Scenario 6: Server Active/Standby Mode

This section provides configuration details for ACOS device with VRRP setup for both Active and Standby Mode. In this example, in the screened subnetwork, the shared partition uses the
administrator IP to always prefer the configured site. In the internal partition, they use static
geo-locations mapped to internal user subnets.

Use the command '`admin-preference`' to always prefer one site over another or by '`admin-ip`' to ensure that any record associated with a service at the preferred site is always selected.

This scenario presents a GSLB Server Active/Standby Mode configuration that includes one A10 device configured as a GSLB controller and A10 devices configured as GSLB site devices, as depicted in Scenario 3: GSLB Server Mode – Controller and Devices.

The following topics are covered:

SLB Setup

The SLB configuration setup is as follows:

This following topics are covered:

Open DNS Virtual Appliance and VRRP on vMaster Configuration

Client is configured to use an Open DNS Virtual Appliance as primary and secondary DNS server.

For ABC client, primary is at ABC and secondary is at DEF

If DEF client, primary is at DEF and secondary is at ABC

Client queries where is “`https://adfs.FPA.org`"

Internal Open-DNS (10.125.15.121 or 10.125.15.122 or 10.100.2.121 or 10.100.2.122) ”`FPA.org`" matches Open-DNS internal DNS forward policy

```
!
vrrp-a common
  device-id 1
  set-id 10
  enable
!
device-context 1
  vcs enable
!
device-context 2
  vcs enable
!
vcs floating-ip 10.202.1.100 255.255.255.0
!
vcs device 1
  priority 200
  interfaces management
  enable
!
vcs device 2
  priority 180
  interfaces management
  enable
!
```

Setup access list and warning

```
access-list 5 permit any log
!
```

```
banner login Warning: Access to this equipment is restricted. Unauthorized
use is prohibited. All connections are monitored.
!
authentication type local radius
!
monitor buffer-usage 711760
!
!
!
no terminal auto-size
terminal length 0
!
```

Setup DNS for Virtual IP address. Configure the Internal OpenDNS (10.125.15.121 or 10.125.15.122 or 10.100.2.121 or 10.100.2.122) for adfs.FPA.org. Client queries will be sent to these addresses.

```
ip dns primary 10.125.15.121
!
ip dns secondary 10.100.2.122
!
ip dns suffix FPA.org
!
vlan 1/580
  tagged ethernet 1
  router-interface ve 580
!
vlan 2/580
  tagged ethernet 1
  router-interface ve 580
!
```

Setup DMZ partition for internal sub-network and implement LLDP on ACOS device.

```
partition dmz id 10 application-type adc
!
partition inside id 20 application-type adc
!
lldp system-name CCC-MDF-3030S-01
lldp system-description CCC-MDF-3030S-01
lldp enable rx tx
lldp notification interval 30
```

```
!
device-context 1
  hostname CCC-MDF-3030S-01
!
device-context 2
  hostname IST-MDF-3030S-01
!
```

Configure all interfaces.

```
device-context 1
  interface management
    access-list 5 in
    ip address 10.202.1.101 255.255.255.0
    ip control-apps-use-mgmt-port
    ip default-gateway 10.202.1.1
    lldp enable rx tx
    lldp notification enable
!
device-context 2
  interface management
    access-list 5 in
    ip address 10.202.1.102 255.255.255.0
    ip control-apps-use-mgmt-port
    ip default-gateway 10.202.1.1
!
interface ethernet 1/1
  enable
!
interface ethernet 1/2
!
interface ethernet 1/3
!
interface ethernet 1/4
!
interface ethernet 1/5
!
interface ethernet 1/6
!
interface ethernet 1/7
!
```

```
interface ethernet 1/8
!
interface ethernet 1/9
  enable
  lldp enable rx tx
  lldp notification enable
!
interface ethernet 1/10
!
interface ethernet 1/11
  enable
  lldp enable rx tx
  lldp notification enable
!
interface ethernet 1/12
!
interface ethernet 2/1
  enable
!
interface ethernet 2/2
!
interface ethernet 2/3
!
interface ethernet 2/4
!
interface ethernet 2/5
!
interface ethernet 2/6
!
interface ethernet 2/7
!
interface ethernet 2/8
!
interface ethernet 2/9
!
interface ethernet 2/10
!
interface ethernet 2/11
!
interface ethernet 2/12
```

```
!
interface ve 1/580
  ip address 10.0.0.1 255.255.255.252
!
interface ve 2/580
  ip address 10.0.0.2 255.255.255.252
!
vrrp-a vrid 0
  device-context 1
    blade-parameters
      priority 200
  device-context 2
    blade-parameters
      priority 180
!
ip nat alg pptp enable
!
vrrp-a interface ethernet 1/1
  vlan 580
!
vrrp-a interface ethernet 2/1
  vlan 580
!
logging monitor information
!
logging console information
!
!
```

Controller Configuration

To setup the GSLB network, GSLB controller and devices must be configured:

1. Configure GSLB and SNMP parameters.

```
!
gslb protocol enable controller
!
gslb protocol enable device
!
snmp-server enable service
```

```
!
snmp-server location "4700 Research Way, Lakeland, FL 33805"
!
snmp-server view view 1.2.3 included
!
snmp-server group group v3 auth read view
!
!
end
```

2. View the current configuration commit to partition 0 in classical-mode configuration, using the `show running configuration` command:

```
Commit the current configuration commit to partition 0 in classical-
mode configuration
!Current configuration: 1650 bytes
!Configuration last updated at 13:58:18 EDT Wed Apr 18 2018
!Configuration last saved at 10:25:02 EDT Wed Apr 18 2018
!
active-partition dmz
!
!
access-list 99 permit any log
!
vlan 1/91
  tagged ethernet 9
  router-interface ve 91
  name dmz
!
vlan 2/91
  tagged ethernet 9
  router-interface ve 91
  name dmz
!
interface ethernet 1/9
  enable
!
interface ethernet 2/9
  name dmz
  enable
!
```

```
interface ve 1/91
  access-list 99 in
  ip address 10.200.240.198 255.255.255.0
!
interface ve 2/91
  access-list 99 in
  ip address 10.200.240.199 255.255.255.0
!
vrrp-a vrid 0
  floating-ip 10.200.240.200
  device-context 1
    blade-parameters
      priority 200
      tracking-options
        interface ethernet 9 priority-cost 40
        gateway 10.200.240.254 priority-cost 40
  device-context 2
    blade-parameters
      priority 180
      tracking-options
        interface ethernet 9 priority-cost 40
        gateway 10.200.240.254 priority-cost 40
!
```

3. Configure the NAT configuration for IP pool.

```
ip nat pool SNAT-POOL-DMZ 10.200.240.50 10.200.240.55 netmask /24
gateway 10.200.240.254 ip-rr
```

Configure the NAT to NAT IP in SNAT-Pool flow for unique 4-Tuple configuration.

```
ip nat pool 121.116.10.99 121.116.10.99 121.116.10.99 netmask /24 port-
overload
```

4. Setup the default IP route for each device or virtual instance.

```
device-context 1
  ip route 0.0.0.0 /0 10.200.240.254 1 description "default route"
!
device-context 2
  ip route 0.0.0.0 /0 10.200.240.254 1 description "default route"
!
```

5. Setup health monitoring and SLB server, service group, and client configurations.

```
health monitor TCP-80
  method tcp port 80
!
health monitor TCP-443
  method tcp port 443
!
health monitor gatewayhm1
  up-retry 3
  interval 2 timeout 1
!
slb template cipher TEMPLATE-CIPHER
  SSL3_RSA_DES_192_CBC3_SHA
  TLS1_RSA_AES_128_SHA priority 50
  TLS1_ECDHE_RSA_AES_128_SHA priority 80
  TLS1_ECDHE_RSA_AES_256_SHA priority 80
  TLS1_RSA_AES_128_GCM_SHA256
  TLS1_RSA_AES_256_GCM_SHA384
  TLS1_DHE_RSA_AES_128_SHA256 priority 70
  TLS1_DHE_RSA_AES_256_SHA256 priority 70
!
slb template server-ssl SERVER-SSL-ADFS.FPA.ORG-2020
  close-notify
  version 33 33
  use-client-sni
  template cipher TEMPLATE-CIPHER
!
slb server CCC-TESTA10-01 10.200.240.31
  port 80 tcp
!
slb server CCC-TESTA10-02 10.200.240.32
  port 80 tcp
!
slb server FPC-ADFSPROXY01 10.200.240.10
  port 443 tcp
!
slb server gateway1 10.200.240.254
  health-check gatewayhm1
!
slb service-group CCC-ADFSPROXY tcp
```

```
  member FPC-ADFSPROXY01 443
!
slb service-group dmz_test tcp
  member CCC-TESTA10-01 80
  member CCC-TESTA10-02 80
!
slb template client-ssl CLIENT-SSL-ADFS.FPA.ORG-2020
  chain-cert incommon-intermediate-2024
  cert adfs.FPA.org-2020
  key adfs.FPA.org-2020
  template cipher TEMPLATE-CIPHER
  disable-sslv3
  version 33 33
!
slb template persist cookie TEMPLATE-PERSIST-COOKIE
  expire 86400
!
slb template http TEMPLATE-HTTP-X-FORWARDED-FOR
  insert-client-ip X-Forwarded-For replace
!
slb template http TEMPLATE-HTTP-X-MS-FORWARDED-CLIENT-IP
  insert-client-ip X-MS-Forwarded-Client-IP
!
slb virtual-server VS-10.200.240.150-53 10.200.240.150
  description name "External GSLB"
  port 53 udp
    gslb-enable
!
```

6. Setup SLB virtual server.

```
slb virtual-server VS-10.200.240.201-443 10.200.240.201
  description "ADFS"
  port 80 http
    source-nat pool SNAT-POOL-DMZ
    service-group CCC-ADFSPROXY
    redirect-to-https
  port 443 https
    aflex aFlex-logging_clients
    source-nat pool SNAT-POOL-DMZ
    service-group CCC-ADFSPROXY
```

```
    template persist cookie TEMPLATE-PERSIST-COOKIE
    template http TEMPLATE-HTTP-X-MS-FORWARDED-CLIENT-IP
    template server-ssl SERVER-SSL-ADFS.FPA.ORG-2020
    template client-ssl CLIENT-SSL-ADFS.FPA.ORG-2020
!
```

Or

Create an IP NAT pool with "`port-overload`" and bind it to UDP virtual port.

```
ip nat pool 121.116.10.99 121.116.10.99 121.116.10.99 netmask /24 port-
overload
slb virtual-server nat1 60.1.1.62
  port 1 udp
    source-nat pool 121.116.10.99
    service-group sg1-udp
port 8080 tcp
    source-nat pool 121.116.10.99
service-group sg-tcp
```

7. Setup GSLB virtual server and service group as follows:

```
gslb service-ip VS-10.200.240.201-443 10.200.240.201
  external-ip 71.40.176.174
  port 443 tcp
!
gslb service-ip VS-10.100.99.201-443 10.100.99.201
  external-ip 71.40.181.225
  port 443 tcp
!
gslb group default
  enable
  primary 10.200.240.200
  priority 200
!
```

8. Associate the main zones or DMZs, DEF and ABC to the GSLB group.

```
gslb site DEF
  slb-dev DEF-10.100.99.198-DMZ 10.100.99.198
    vip-server VS-10.100.99.201-443
!
gslb site ABC
  slb-dev ABC-10.200.240.200-DMZ 10.200.240.200
```

```
    vip-server VS-10.200.240.201-443
!
gslb site DR
!
gslb policy GSLB-POLICY-ADFS-EXTERNAL
  admin-ip-enable
  admin-ip top-only
  no round-robin
  metric-order health-check admin-ip
  dns selected-only
  dns logging query
  dns server authoritative
!
```

9. Define the GSLB zone *gslb.FPA.org*

```
gslb zone gslb.FPA.org
  policy GSLB-POLICY-ADFS-EXTERNAL
  service 443 adfs
    dns-a-record 10.100.99.201 static admin-ip 180
    dns-a-record 10.200.240.201 static admin-ip 200
!
end
```

Reuse Port of NAT IP in SNAT-Pool Flow Unique 4-Tuple

The smart NAT instance of a NAT pool is assigned on a per port basis. The advantage of this is now, every destination server and port, we can go to 65K source port.

The source IP that is being is used is that of the interface IP. The maximum port usage is 41000 from 24000 to 65535 through “Source NAT auto failure", even though ACOS CLI guide says that the port usage is 45K from 2032 to 65535.

Use "SNAT + IP NAT pool" for high capacity of NAT port resources. Smart NAT supports up to 64K source ports per port instance. When you add one port under the same server, then the limit drops down to 32K source port per port. Therefore, as you add more ports, it will reduce the number of source ports per port. Reuse the same port if there is a unique 4-tuple. Used with unique 4 tuple socket. SNAT address and port remote socket.

The "`ip nat pool`" command will be changed to add the "`reuse-srcport`" option to support this feature. By default, this is disabled. Configure "`reuse-srcport`" to enable this feature.

```
vThunder(config)# ip nat pool test_pool 10.212.2.60 10.212.2.65 netmask/24
```

VRRP Interface on vBlade Configuration

Current configuration commit point for partition 1 is config mode is classical-mode.

1. Configure the management interface and VRRP interfaces on ACOS vBlade.

```
!Current configuration: 1664 bytes
!Configuration last updated at 13:58:18 EDT Wed Apr 18 2018
!Configuration last saved at 10:25:02 EDT Wed Apr 18 2018
!
active-partition inside
!
!
access-list 10 permit any log
!
no terminal auto-size
terminal width 0
!
vlan 1/514
  tagged ethernet 11
  router-interface ve 514
  name inside
!
vlan 2/514
  tagged ethernet 11
  router-interface ve 514
!
interface ethernet 1/11
  enable
!
interface ethernet 2/11
  enable
!
interface ve 1/514
  access-list 10 in
```

```
  ip address 10.125.14.198 255.255.255.0
!
interface ve 2/514
  name inside
  access-list 10 in
  ip address 10.125.14.199 255.255.255.0
!
```

2. Define VRRP interfaces for partition 1

```
vrrp-a vrid 0
  floating-ip 10.125.14.200
  device-context 1
    blade-parameters
      priority 200
      tracking-options
        interface ethernet 11 priority-cost 40
        gateway 10.125.14.254 priority-cost 40
  device-context 2
    blade-parameters
      priority 180
      tracking-options
        interface ethernet 11 priority-cost 40
        gateway 10.125.14.254 priority-cost 40
!
ip nat pool SNAT-POOL-INSIDE 10.125.14.50 10.125.14.55 netmask /24
gateway 10.125.14.254 ip-rr
!
device-context 1
  ip route 0.0.0.0 /0 10.125.14.254 1 description "default route"
!
device-context 2
  ip route 0.0.0.0 /0 10.125.14.254 1 description "default route"
!
health monitor TCP-443
  method tcp port 443
!
health monitor gatewayhm1
  up-retry 3
  interval 2 timeout 1
!
```

```
slb template cipher TEMPLATE-CIPHER
  SSL3_RSA_DES_192_CBC3_SHA
  TLS1_RSA_AES_128_SHA priority 50
  TLS1_ECDHE_RSA_AES_128_SHA priority 80
  TLS1_ECDHE_RSA_AES_256_SHA priority 80
  TLS1_RSA_AES_128_GCM_SHA256
  TLS1_RSA_AES_256_GCM_SHA384
  TLS1_DHE_RSA_AES_128_SHA256 priority 70
  TLS1_DHE_RSA_AES_256_SHA256 priority 70
!
slb template server-ssl SERVER-SSL-ADFS.FPA.ORG-2020
  close-notify
  version 33 33
  use-client-sni
  template cipher TEMPLATE-CIPHER
!
slb server CCC-ADFS01 10.125.15.9
  port 443 tcp
!
slb server gateway1 10.125.14.254
  health-check gatewayhm1
!
slb service-group CCC-ADFS tcp
  member CCC-ADFS01 443
!
slb template client-ssl CLIENT-SSL-ADFS.FPA.ORG-2020
  chain-cert incommon-intermediate-2024
  cert adfs.FPA.org-2020
  key adfs.FPA.org-2020
  template cipher TEMPLATE-CIPHER
  disable-sslv3
  version 33 33
!
slb template persist cookie TEMPLATE-PERSIST-COOKIE
  expire 86400
!
slb template http TEMPLATE-HTTP-X-FORWARDED-FOR
  insert-client-ip X-Forwarded-For replace
!
```

```
slb template http TEMPLATE-HTTP-X-MS-FORWARDED-CLIENT-IP
  insert-client-ip X-MS-Forwarded-Client-IP
!
slb virtual-server VS-10.125.14.175-53 10.125.14.175
  description "Internal GSLB"
  port 53 udp
    gslb-enable
!
slb virtual-server VS-10.125.14.224 10.125.14.224
  description "ADFS Layer 4 helper"
  port 80 http
    source-nat pool SNAT-POOL-INSIDE
    service-group CCC-ADFS
    redirect-to-https
  port 443 tcp
    source-nat pool SNAT-POOL-INSIDE
    service-group CCC-ADFS
!
slb virtual-server VS-10.125.14.225 10.125.14.225
  description "ADFS"
  port 80 http
    source-nat pool SNAT-POOL-INSIDE
    service-group CCC-ADFS
    redirect-to-https
  port 443 https
    aflex aFlex-logging_clients
    source-nat pool SNAT-POOL-INSIDE
    service-group CCC-ADFS
    template persist cookie TEMPLATE-PERSIST-COOKIE
    template http TEMPLATE-HTTP-X-MS-FORWARDED-CLIENT-IP
    template server-ssl SERVER-SSL-ADFS.FPA.ORG-2020
    template client-ssl CLIENT-SSL-ADFS.FPA.ORG-2020
!
```

GSLB Setup

The GSLB configuration setup is as follows for ADFS with Active site called ABC and Standby site called DEF.

1. Configure the named static service IP addresses for GSLB server IP address `71.40.176.174`:

```
!
gslb service-ip VS-10.200.240.201-443 10.200.240.201
  external-ip 71.40.176.174
  port 443 tcp
```

2. Configure the virtual service IP addresses for named static GSLB server IP address `71.40.176.225`:

```
!
gslb service-ip VS-10.100.99.201-443 10.100.99.201
  external-ip 71.40.181.225
  port 443 tcp
```

3. Configure the default IP addresses for GSLB group with primary service address 10.200.240.200:

```
!
gslb group default
  enable
  primary 10.200.240.200
  priority 200
```

4. Setup GSLB for the DEF site. Set active/standby mode on DEF by setting `admin-preference` priority:

```
!
gslb site DEF
  admin-preference 180
  slb-dev DEF-10.100.99.198-DMZ 10.100.99.198
    vip-server VS-10.100.99.201-443
```

5. Setup GSLB for the ABC site. ABC now has higher `admin-preference` priority:

```
!
gslb site ABC
  admin-preference 200
  slb-dev ABC-10.200.240.200-DMZ 10.200.240.200
    vip-server VS-10.200.240.201-443
```

NOTE: To confirm the Master selection, check the output of "`show gslb group`" command.

```
VMWS-ACOS-2-gslb:Member(config-group:default)# show gslb group
                      Pri = Priority, Attrs = Attributes
                          D = Disabled, L = Learn
                          P = Passive, * = Master
Group: default, Master: VMWS-ACOS-1 <-Now master
Member                            Sys-ID    Pri Attrs  Status      Address
-------------------------------------------------------------------------
---------
local                             d1a23459 180 L      OK
VMWS-ACOS-1                       4abc3929 200 PL*    Synced
10.10.50.11
```

6. Setup the disaster recovery site:

```
!
gslb site DR
!
gslb policy GSLB-POLICY-ADFS-EXTERNAL
  admin-ip-enable
  admin-ip top-only
  no round-robin
  metric-order health-check admin-preference
  dns selected-only
  dns logging query
  dns server authoritative
!
```

7. Configure the GSLB zone for `gslb.FPA.org`.

```
gslb zone gslb.FPA.org
  policy GSLB-POLICY-ADFS-EXTERNAL
  service 443 adfs
    dns-a-record 10.100.99.201 static
    dns-a-record 10.200.240.201 static
!
```

Scenario 7: Disaster Recovery Solution

A10 Networks ACOS GSLB technology provides site disaster recovery and failure protection. The GSLB controller monitors each active site in the GSLB domain to

verify the health of each site. If an active site fails the health check mechanism, the GSLB controller shifts application traffic to an alternate site dynamically.

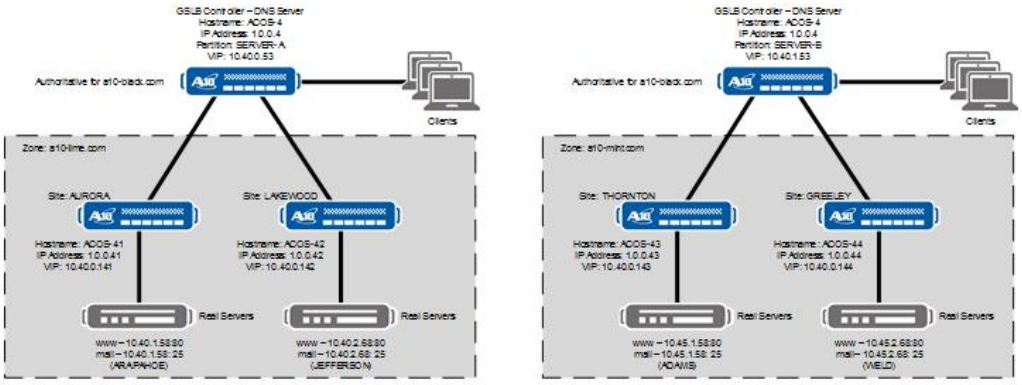
The fail-over is a transparent process to users connecting to a FQDN serviced by the A10 GSLB
controllers. The GSLB site fail-over process can also be accomplished manually in case of scheduled site maintenance. The operator can force traffic to an alternate site by a simple procedure.

The following topics are covered:

Disaster Recovery Setup

Following is an Active - Standby design in GSLB server mode. Each site has a GSLB controller and the GSLB controllers are authoritative for the delegated DNS zone.

Figure 6 : GSLB Disaster Recovery design



High-level overview of the GSLB Disaster Recovery setup is as follows:

- Users connecting to www.a10example.com:
  - Queries are sent to the local DNS server and the recursive lookup process continues to the root DNS servers.
  - The A10 GSLB controllers communicate using the GSLB protocol for health check monitors to verify site availability.
  - CNAME is used for delegation of the FQDN to the A10 GSLB controllers.
  - The Primary or the DR GSLB controller responds to the users with the Primary site HTTP VIP address if the Primary site is up.
- If the A10 GSLB controllers determine the Primary site is down:
  - The A10 GSLB controller responds with the HTTP VIP address of the DR site.
  - User traffic is directed to the DR site.
- When the GSLB Protocol determines the Primary site is up:
  - User traffic is directed to the Primary site.

Disaster Recovery Configuration

To configure the GSLB active and standby sites based on Figure 6 design:

- Enable the GSLB controller process for the GSLB protocol to exchange site health information.

```
ACOS(config)# <gslb protocol enable controller>
```

- If SLB is also combined with GSLB, enable the GSLB device.

```
ACOS(config)# <gslb protocol enable device>
```

- Enable the DNS VIP for a standalone DNS server, configure the port, and enable GSLB.

```
ACOS(config)# <slb virtual-server <name> <IP address>>
ACOS(config-slb vserver)# <port <number> < udp>
ACOS (config-slb vserver-vport)# <gslb-enable>
```

- Configure the named static Service IP address for each site. This is the SLB VIP address or remote host IP address the DNS VIP will respond with, to direct traffic to the site. Define the port and protocol.

```
ACOS(config)# <gslb service-ip <name> <IP address>>
ACOS(config-service-ip:PRI-GSLB-HTTP)# <port <number>  <udp or tcp>>
```

- Configure the GSLB controller for each site. Configure the site parameters and set the administrative preference to prefer Primary site for all traffic. The default administrative preference value is 100. Set the active site to a higher administrative value than the default value to prefer traffic over the DR site. Add the GSLB service VIP address to each site configuration.

```
ACOS(config)# <gslb site <name>>
ACOS(config-gslb site:name)# <slb-dev <name> <IP address>>
ACOS(config-gslb site:name-slb dev:name)# <admin-preference <0-255>>
ACOS(config-gslb site:name-slb dev:name)# <vip-server <GSLB VIP name>>.
```

- Configure the GSLB policy to determine how GSLB traffic will be distributed to each site. Enable the DNS attributes to respond with a single IP and be authoritative for the zone. Enable administrative-preference and disable round robin based on the active-standby design. Order the metrics for the desired GSLB behavior.

```
ACOS(config)# <gslb policy <name>>
ACOS(config-policy:name)# <dns selected-only 1>
ACOS(config-policy:name)# <dns server authoritative>
ACOS(config-policy:name)# <admin-preference>
ACOS(config-policy:name)# <no round-robin>
ACOS(configpolicy:name)# <metric-order admin-preference health-check>
```

- Enable the zone information for DNS query response for the FQDN zone. Bind the GSLB policy to the zone configuration. Enter the CNAME if it was used for zone delegation on the A10 GSLB controllers or enter the zone. Define the service prefix for the FQDN and associated service port.
  Configure the DNS A Record for each GSLB VIP address of each site which will return the HTTP VIP address with the DNS response.

```
ACOS(config)# <gslb zone <zone name>
ACOS(config-zone:zone-name)# <policy <name>>
ACOS(config-zone:zone-name)# <service <port number> <service prefix for
zone>>
ACOS(config-zone:zone-name.-service...)# <dns-a-record <GSLB VIP name>
<static>>
```

CLI Configuration

Configure GSLB with the following steps using the CLI for the illustrated GSLB Disaster Recovery design. The CNAME, *gslb.a10example.com*, is used for the zone,

www.a10example.com.

Primary Site Configuration

```
ACOS-PRI(config)# gslb protocol enable controller
ACOS-PRI(config)# gslb protocol enable device
ACOS-PRI(config)# slb virtual-server DNS-VIP 192.168.20.53
ACOS-PRI(config-slb vserver)# port 53 udp
ACOS-PRI(config-slb vserver-vport)# gslb-enable
ACOS-PRI(config)# gslb service-ip PRI-GSLB-HTTP 192.168.20.200
ACOS-PRI(config-service-ip:PRI-GSLB-HTTP)# port 80 tcp
ACOS-PRI(config)# gslb service-ip DR-GSLB-HTTP 192.168.40.200
ACOS-PRI(config-service-ip:DR-GSLB-HTTP)# port 80 tcp
ACOS-PRI(config)# gslb site Primary
ACOS-PRI(config-gslb site:Primary)# slb-dev PRI 192.168.20.125
ACOS-PRI(config-gslb site:Primary-slb dev:PRI)# admin-preference 200
ACOS-PRI(config-gslb site:Primary-slb dev:PRI)#vip-server PRI-GSLB-HTTP
ACOS-PRI(config)# gslb site DRsite
ACOS-PRI(config-gslb site:DRsite)# slb-dev DR 192.168.40.125
ACOS-PRI(config-gslb site:DRsite-slb dev:DR)# vip-server DR-GSLB-HTTP
ACOS-PRI(config)# gslb policy A10health
ACOS-PRI(config-policy:a10health)# dns selected-only-1
ACOS-PRI(config-policy:a10health)# dns server authoritative
ACOS-PRI(config-policy:a10health)# admin-preference
ACOS-PRI(config-policy:a10health)# no round-robin
ACOS-PRI(config-policy:a10health)# metric-order health-check admin-
preference
ACOS-PRI(config)# gslb zone gslb.a10example.com
ACOS-PRI(config-zone:gslb.a10example.)# policy A10health
ACOS-PRI(config-zone:gslb.a10example.)# service 80 www
ACOS-PRI(config-zone:gslb.a10example.-service...)# dns-a-record PRI-GSLB-
HTTP static
ACOS-PRI(config-zone:gslb.a10example.-service...)# dns-a-record DR-GSLB-
HTTP static
```

Primary and Disaster Recovery Site Configuration

The GSLB configuration example for both sites is as follows:

Figure 7 : GSLB design template configuration for Primary and Disaster Recovery Site

Primary Site:

```
ACOS-PRI#show running-configuration
!Current configuration: 508 bytes
!Configuration last updated at 00:28:05 GMT Sat Mar 24 2018
!Configuration last saved at 23:48:37 GMT Fri Mar 23 2018
!64-bit Advanced Core OS (ACOS) version 4.1.4, build 307 (Feb-12-2018,06:47)
!
hostname ACOS-PRI
!
interface management
 ip address 172.31.31.31 255.255.255.0
 enable
!
interface ethernet 1
 enable
 ip address 192.168.20.125 255.255.255.0
!
interface ethernet 2
 !
ip route 0.0.0.0 /0 192.168.20.154
!
slb server RS1 192.168.2.243
 port 80 tcp
!
slb service-group SG1 tcp
 member RS1 80
!
slb virtual-server DNS-VIP 192.168.20.53
 port 53 udp
  gslb-enable
!
slb virtual-server VS1 192.168.20.200
 port 80 http
  source-nat auto
  service-group SG1
!
gslb service-ip PRI-GSLB-HTTP 192.168.20.200
 port 80 tcp
!
gslb service-ip DR-GSLB-HTTP 192.168.40.200
 port 80 tcp
!
gslb site Primary
 slb-dev PRI 192.168.20.125
  admin-preference 200
  vip-server PRI-GSLB-HTTP
!
gslb site DRsite
 slb-dev DR 192.168.40.125
  vip-server DR-GSLB-HTTP
!
gslb policy A10health
 no geographic
 admin-preference
 no round-robin
 metric-order health-check admin-preference
 dns selected-only 1
 dns server authoritative
!
gslb zone gslb.a10example.com
 policy A10health
 service 80 www
  policy A10health
  dns-a-record DR-GSLB-HTTP static
  dns-a-record PRI-GSLB-HTTP static
!
gslb protocol enable controller
!
gslb protocol enable device
!
end
```

DR Site:

```
ACOS-DR#show running-configuration
!Current configuration: 362 bytes
!Configuration last updated at 00:46:37 GMT Sat Mar 24 2018
!Configuration last saved at 00:41:10 GMT Sat Mar 24 2018
!64-bit Advanced Core OS (ACOS) version 4.1.4, build 307 (Feb-12-2018,06:47)
!
hostname ACOS-DR
!
interface management
 ip address 172.31.31.32 255.255.255.0
!
interface ethernet 1
 enable
 ip address 192.168.40.125 255.255.255.0
!
interface ethernet 2
!
ip route 0.0.0.0 /0 192.168.40.154
!
slb server RS1 192.168.40.250
 port 80 tcp
!
slb service-group SG1 tcp
 member RS1 80
!
slb virtual-server DNS-VIP 192.168.40.53
 port 53 udp
  gslb-enable
!
slb virtual-server VS1 192.168.40.200
 port 80 http
  source-nat auto
  service-group SG1
!
gslb service-ip DR-GSLB-HTTP 192.168.40.200
 port 80 tcp
!
gslb service-ip PRI-GSLB-HTTP 192.168.20.200
 port 80 tcp
!
gslb site DRsite
 slb-dev DR 192.168.40.125
  vip-server DR-GSLB-HTTP
!
gslb site Primary
 slb-dev PRI 192.168.20.125
  admin-preference 200
  vip-server PRI-GSLB-HTTP
!
gslb policy A10health
 no geographic
 admin-preference
 no round-robin
 metric-order health-check admin-preference
 dns selected-only 1
 dns server authoritative
!
gslb zone gslb.a10example.com
 policy A10health
 service 80 www
  policy A10health
  dns-a-record DR-GSLB-HTTP static
  dns-a-record PRI-GSLB-HTTP static
!
gslb protocol enable controller
!
gslb protocol enable device
!
!
end
```

Metrics

Metrics that are assigned through policies assigned to GSLB sites.

The following topics are covered:

Metrics Management

GSLB metrics are implemented through enabling commands and managed by selecting the order by which the metrics are applied.

This following topics are covered:

Enabling and Disabling Metrics (CLI)

The Health-Check, Geographic, and Round-Robin metrics are enabled by default. All other metrics are disabled by default.

To enable a metric, enter the metric name at the configuration level for the policy. For example, to enable the Admin-Preference metric, enter the following commands:

```
ACOS(config)# gslb policy oxygen
ACOS(config-policy:oxygen)# admin-preference
```

To disable a GSLB metric, use the "no" form of the metric at the configuration level for the policy. For example, to disable the Health-Check metric, enter these commands:

```
ACOS(config)# gslb policy oxygen
ACOS(config-policy:oxygen)# no health-check
```

Configuration

ACOS devices use the GSLB protocol for GSLB management traffic. The protocol must be enabled on the GSLB controller.

GSLB does not need to be enabled on the site ACOS devices, but enabling it is recommended to collect site information that GSLB requires to generate the following metrics:

- Session-capacity
- aRDT
- Connection-Load
- Connection-count-by-site
- Num-Session

Enabling the GSLB protocol is required when using default health-check methods. However, when you modify default health checks, the GSLB protocol does not need to be enabled. (See Metrics Management.)

Changing Order

The metric order and the configuration of each metric are specified in a GSLB policy. Policies can be applied to GSLB zones and to individual services. The GSLB ACOS device has a default GSLB policy, named “default”, which is automatically applied to a zone or service.

Metric order does not apply to the Alias-Admin-Preference and Weighted-Alias metrics. When enabled, Alias-Admin-Preference always has high priority.

The **`metric-order`** command configures the precedence order of metrics in a GSLB policy (metric-order).

Descriptions

A GSLB policy consists of one or more metrics. These sections describe GSLB Metrics that are implemented through policies that are applied to zones and services.

This following topics are covered:

Weighted-IP

Weighted-IP – Service IP addresses with higher administratively assigned weights are used more often than service IP addresses with lower weights.

The Weighted-IP metric skews selection toward specific IP addresses. GSLB selects higher-weighted IP addresses more often than lower-weighted IP addresses.

If DNS caching is used, the cycle starts over if the cache aging timer expires.

Weighted-Site

Weighted-Site – Sites with higher administratively assigned weights are used more often than sites with lower weights. The Weighted-Site metric skews selection toward specific sites. GSLB selects higher-weighted sites more often than lower-weighted sites.

Example: if there are two sites (A and B), and A has weight 2 whereas B has weight 4, GSLB will select site B twice as often as site A. Specifically, GSLB will select site B the first 4 times, and will then select site A the next 2 times. This cycle then repeats: B is chosen 4 times, then A is chosen the next 2 times, then B is chosen the next 4 times, and so on.

If DNS caching is used, the cycle starts over if the cache aging timer expires.

Session Capacity

Session Capacity – Sites with more available sessions based on respective maximum Session-Capacity are preferred.

Active Servers

Active Servers – Sites with the most currently active servers are preferred.

Active-Round Delay Time (aRDT)

The Active-Round Delay Time (aRDT) is a metric to prefer sites with faster round-delay-times for DNS queries and replies between a site ACOS device and the GSLB local DNS.

This feature is beneficial to ensure:

- Faster page load times for clients across various regions: aRDT routes clients to the nearest data center with the lowest latency.
- Service availability in the event of a regional outage: aRDT instantly transfers traffic to the next best-performing data center.

You can configure aRDT at the following levels:

- GSLB Global Level aRDT Settings
- GSLB Policy Level aRDT Settings
- GSLB Site Level aRDT Settings

GSLB Global Level aRDT Settings

The aRDT can be configured globally using the `gslb active-rdt` command. This command affects all the policies and sites within the GSLB configuration.

The following options are available:

- Domain – Specifies the query domain used to measure the aRDT for a client. The site ACOS device sends queries for the domain name to a client's local DNS. An aRDT sample consists of the time between when the site's ACOS device sends a query and when it receives the response.

  You can configure only one aRDT domain. It is recommended to use a domain name that is likely to be in the cache of each client's local DNS. The default domain name is "google.com."

  The ACOS device averages multiple aRDT samples together to calculate a client's aRDT measurement. (See Track)

- ICMP - Use ICMP (Internet Control Message Protocol) to measure the aRDT.

- Interval – Specifies the number of seconds between queries. You can specify 1-16383 seconds. The default is 1.
- Port - Specifies the local port to send the probe packet. The default is 0 (no port).
- Retry – Specifies the number of times GSLB will resend a query if there is no response. You can specify 0-16. The default is 3.
- Sleep – Specifies the number of seconds GSLB stops tracking aRDT data for a client after a query fails. You can specify 1-300 seconds. The default is 3.
- Timeout – Specifies the number of milliseconds GSLB will wait for a reply before resending a query. You can specify 1-16383 milliseconds (ms). The default is 3000 ms.
- Track – Specifies the number of seconds during which the ACOS device collects samples for a client. You can specify 3-16383 seconds. The default is 60 seconds.

  The samples collected during the track time are averaged together. The averaged value is used as the aRDT measurement for the client.

CLI Configuration

These commands configure the domain and interval at the global level:

```
ACOS(config)# gslb active-rdt domain example.com
ACOS(config)# gslb active-rdt interval 50
```

GSLB Policy Level aRDT Settings

The GSLB policy-level aRDT settings allow for more granular control, enabling specific configurations for different GSLB policies using the **active-rdt enable** command. The policy should be bound to the GSLB zone to take effect.

The following options are available:

- Controller - Enables the active round-delay-time by controller.
- Difference - Specifies the difference between the round-delay-time (in milliseconds). The value can be 0-16383. The default is 0.
- Fail-break - Stops the RDT process if no valid round-trip delay measurements are available.

- Ignore ID - Exclude specific IP addresses from RDT consideration. This is typically used for filtering out known bad or unreliable IPs.
- Keep-tracking - Continues to monitor the client's RDT even after the required samples are collected.
- Limit - Specifies an upper limit on the RDT value (in milliseconds), preventing extremely high delays from skewing the results. The value can be 1-16383.
- Prefer DNS Sticky - Integrates DNS sticky with aRDT and uses DNS sticky if configured. Specify the mandatory difference value (in milliseconds 1-16383). This value represents the difference between the current best service IP and the previous best service IP. When this difference exceeds the specified value, the DNS sticky is updated with the current best IP. This means:
  - If there is no DNS sticky, the aRDT is used.
  - If DNS sticky is already present, continue using it if the difference is within the defined value. However, if the difference exceeds the defined value, update the DNS sticky to the new lowest aRDT value.
- Proto RDT - Enables the round-delay-time for the controller.
- Samples - Specifies the number of samples for round-delay-time. The samples can be 1-8, default is 5.
- Single Shot - Collects and uses only one RDT sample.
- Skip - Skips the DNS query if the required number of RDT samples hasn't been collected. The skip count can be 1-31, default is 3.
- Timeout - Specifies the timeout (in seconds) if round-delay-time samples are not ready. The timeout value can be 1-255, default is 3.
- Tolerance - Specifies the difference in percentage between the round-delay-time. The percentage is 0-100.

CLI Configuration

- These commands access the configuration level for GSLB policy "gslbp2" and enable the aRDT metric, using default settings:

```
ACOS(config)# gslb policy gslbp2
ACOS(config-policy:gslbp2)# active-rdt enable
```

- These commands access the configuration level for GSLB policy "gslbp3" and enable the aRDT metric with single-shot.

```
ACOS(config)# gslb policy gslbp3
ACOS(config-policy:gslbp3)# active-rdt single-shot
ACOS(config-policy:gslbp3)# active-rdt skip 3
```

  In this example, each site ACOS device will send a single DNS query to the GSLB domain's local DNS and wait 3 seconds (the default) for a reply. The site ACOS devices will then send their aRDT measurements to the GSLB ACOS device. However, if more than 3 site ACOS devices fail to send their aRDT measurements to the GSLB ACOS device, the ACOS device will not use the aRDT metric.

- These commands access the configuration level for GSLB policy "gslbp4" and exclude a set of IP addresses from aRDT polling using ignore ID.

```
ACOS(config)# gslb ip-list iplist1
ACOS(config-gslb ip-list)# ip 192.168.1.0 /24 id 3
ACOS(config-gslb ip-list)# ip 10.10.10.10 /32 id 3
ACOS(config)# gslb policy gslb4
ACOS(config-policy:gslbp4)# active-rdt ignore-id 3
```

- These commands access the configuration level for GSLB policy "gslbp5" and enable the aRDT metric with prefer-dns-sticky.

```
ACOS(config)# gslb policy gslbp5
ACOS(config-policy:gslbp5)# metric-order health-check active-rdt
ACOS(config-policy:gslbp5)# dns sticky /24
ACOS(config-policy:gslbp5)# active-rdt enable
ACOS(config-policy:gslbp5)# active-rdt prefer-dns-sticky difference 15
```

  In this example, site ACOS device checks for an existing DNS sticky record and examines the present sticky IP's delay.

  - If the delay is less than 15 milliseconds as compared to the lowest RDT value, the ACOS device will continue to use the current sticky IP.
  - If the delay between the current sticky IP and the lowest RDT value exceeds 15 milliseconds, the ACOS device changes to the new IP with the lowest RDT and updates the DNS sticky entry to this new IP.

GSLB Site Level aRDT Settings

The GSLB site-level aRDT settings provide customization for individual sites within the GSLB configuration. The following options are available:

- Aging-time – Specifies the maximum duration a stored aRDT result can be used. The average aRDT measurement is used until it expires. The duration can be 1-60 minutes, default is 10 minutes.
- Bind-geoloc – Stores the aRDT measurements on a per geo-location basis. Without this option, the measurements are stored on a per site-SLB device basis.
- Ignore-count – Specifies the ignore count if aRDT is out of range. The count can be 1-15, default is 5.
- IPv6-mask – Specifies the client IPv6 mask length, 1-128. The default is 128.
- Limit – Specifies the limit of valid RDT. The limit can be 1-16383, default is 16383 milliseconds.
- Mask – Based on the subnet mask or mask length, the entry can be a host address or a subnet address. The default is 32.
- Range-factor – Specifies the maximum percentage by which a new aRDT measurement can differ from the previous measurement. If the new measurement differs from the previous measurement by more than the allowed percentage, the new measurement is discarded, and the previous measurement is used again. The value can be 1-1000, default is 25.

  For example, if the range-factor is set to 25 (the default), a new measurement that has a value from 75% to 125% of the previous value can be used. A measurement that is less than 75% or more than 125% of the previous measurement cannot be used.

- Smooth-factor – Blends the new measurement with the previous one, to smoothen the measurements. The value can be 1-100, default is 10.

  For example, if the smooth-factor is set to 10 (the default), 10% of the new measurement is used, along with 90% of the previous measurement. Similarly, if the smooth-factor is set to 50, 50% of the new measurement is used, along with 50% of the previous measurement.

CLI Configuration

These commands configure aRDT aging time and limit at the site level:

```
ACOS(config)# gslb site example.com
ACOS(config-gslb site:example.com)# active-rdt aging-time 50
ACOS(config-gslb site:example.com)# active-rdt limit 115
```

For more information, see Command Line Interface Reference.

Single Sample (Single Shot)

To take a single sample and use that sample indefinitely, use the single-shot option. This option instructs each site ACOS device to send a single DNS query to the GSLB local DNS.

The single-shot option is useful if you do not want to frequently update the aRDT measurements. For example, if the GSLB domain's clients tend to remain logged on for long periods of time, using the single-shot option ensures that clients are not frequently sent to differing sites based on aRDT measurements.

The single-shot has the following additional options:

- timeout – Specifies the number of seconds each site ACOS device should wait for the DNS reply. If the reply does not arrive within the specified timeout, the site becomes ineligible for selection, in cases where selection is based on the aRDT metric. You can specify 1-255 seconds. The default is 3 seconds.
- skip – Specifies the number of site ACOS devices that can exceed their single-shot timeouts, without the aRDT metric itself being skipped by the GSLB ACOS device during site selection. You can skip from 1-31 sites. The default is 3.

Multiple Samples

To periodically retake aRDT samples, do not use the single-shot option. In this case, the ACOS device uses the averaged aRDT value based on the number of samples measured for the intervals.

For example, if you set aRDT to use 3 samples with an interval of 5 seconds, the aRDT is the average over the last 3 samples, collected in 5-second intervals. If you configure single-shot instead, a single sample is taken.

The number of samples can be 1-8. The default is 5 samples.

Store-By

By default, the GSLB ACOS device stores one aRDT measurement per site SLB device. Optionally, you can configure the GSLB ACOS device to store one measurement per geo-location instead. This option is configurable on individual GSLB sites. (See Changing aRDT Settings for a Site.)

Tolerance

Default measurement tolerance is 10 percent. If the aRDT measurements for more than one site are within 10 percent, GSLB ACOS device considers the sites to be equal in terms of aRDT. You can adjust the tolerance to any value from 0-100 percent.

Controller-Based Metrics

The device typically relies on GSLB site-based metrics, where the controller obtains metrics from site devices. GSLB Controller-Based metrics enable each GSLB controller to directly measure active-round delay time (aRDT or RDT) metric information as derived from its queries to the local DNS (LDNS) server and, optionally, the site GSLB devices. The device can be configured to calculate the response delay time by using ICMP packets through the `gslb active-rdt icmp` command.

Network topologies often include site devices that either require NAT to access local DNS servers or are isolated from the servers by firewalls. GSLB controllers cannot obtain valid site-based metrics from site devices in these topologies.

The GSLB controllers must be members of a GSLB Controller group, which is a data structure that synchronizes communications and designates a Master Controller among the members. The A10 GLOBAL SERVER LOAD BALANCING GUIDE describes the function and implementation of GSLB Controller groups.

GSLB Controller based metrics are not supported in IPv6 or L3V partition configurations.

Each location includes a GSLB controller that can access the client LDNS and its local site devices. Each GSLB Controller only queries its local site device and the originating LDNS server to derive the RDT metrics. The controllers send the metrics to the GSLB Master Controller. By default, the metric is based on the response time

between the controller and the LDNS server. An option is available that adds the response time between the controller and site device to the controller-LDNS response time.

Configuring GSLB Controller-Based Metrics (CLI Example)

These commands implement GSLB Controller-Based metrics. Configuring Controller-Based Metrics for the GUI implementation.

```
ACOS(config)# hostname ACOS-1
ACOS-1(config)# gslb service-ip NYE 10.1.1.10
ACOS-1(config-service-ip:NYE)# port 80 tcp
ACOS-1(config-service-ip:NYE-port:...)# exit
ACOS-1(config-service-ip:NYE)# exit
ACOS-1(config)# gslb service-ip WASHOE 20.1.1.20
ACOS-1(config-service-ip:WASHOE)# port 80 tcp
ACOS-1(config-service-ip:WASHOE-port...)# exit
ACOS-1(config-service-ip:WASHOE)# exit
```

These commands bind controllers to the GSLB sites (ACOS-1 to ELY and ACOS-2 to RENO).

```
ACOS-1(config)# gslb site ELY
ACOS-1(config-gslb site:ELY)# controller ACOS-1
ACOS-1(config-gslb site:ELY)# slb-dev d1 10.1.1.1
ACOS-1(config-gslb site:ELY-slb dev:d1)# vip-server NYE
ACOS-1(config-gslb site:ELY-slb dev:d1)# exit
ACOS-1(config-gslb site:ELY)# exit
ACOS-1(config)# gslb site RENO
ACOS-1(config-gslb site:RENO)# controller ACOS-2
ACOS-1(config-gslb site:RENO)# slb-dev d2 20.1.1.1
ACOS-1(config-gslb site:RENO-slb dev:d2)# vip-server WASHOE
ACOS-1(config-gslb site:RENO-slb dev:d2)# exit
ACOS-1(config-gslb site:RENO)#
```

These commands implement controller-based metrics on the GSLB policy named RHOMBUS

```
ACOS-1(config)# gslb policy RHOMBUS
ACOS-1(config-policy:RHOMBUS)# no round-robin
ACOS-1(config-policy:RHOMBUS)# dns active-only
ACOS-1(config-policy:RHOMBUS)# dns selected-only
ACOS-1(config-policy:RHOMBUS)# dns server
```

```
ACOS-1(config-policy:RHOMBUS)# active-rdt enable
ACOS-1(config-policy:RHOMBUS)# active-rdt controller
ACOS-1(config-policy:RHOMBUS)# active-rdt proto-rdt-enable
ACOS-1(config-policy:RHOMBUS)# exit
```

These commands enable controller-based metrics by applying the GSLB policy.

```
ACOS-1(config)# gslb zone a10-black.com
ACOS-1(config-zone:a10-black.com)# policy RHOMBUS
ACOS-1(config-zone:a10-black.com)# service 80 www
ACOS-1(config-zone:a10-black.com-service:www)# dns-a-record NYE static
ACOS-1(config-zone:a10-black.com-service:www)# dns-a-record WASHOE static
ACOS-1(config-zone:a10-black.com-service:www)# exit
ACOS-1(config-zone:a10-black.com)# exit
```

These commands enable the GSLB controller and configures the GSLB group.

```
ACOS-1(config)# gslb group g1
ACOS-1(config-group:g1)# enable
ACOS-1(config-group:g1)# primary 20.20.1.1
ACOS-1(config-group:g1)# gslb protocol enable controller
ACOS-1(config)#
```

Geo-Location

You can configure GSLB to prefer site VIPs for DNS replies that are geographically closer to the clients. For example, if a domain is served by sites in both the USA and Asia, you can configure GSLB to favor the USA site for USA clients while preferring the Asian site for Asian clients.

To configure geo-location:

- Leave the Geographic GSLB metric enabled; it is enabled by default.
- Load geo-location data. You can load geo-location data from a file or manually configure individual geo-location mappings.

Loading geo-location data from a file is simpler than manually configuring geo-location mappings, especially if you have more than a few GSLB sites.

The ACOS software includes an Internet Assigned Numbers Authority (IANA) database. The IANA database contains the geographic locations of the IP address

ranges and subnets assigned by the IANA. The IANA database is loaded on the ACOS device, and it is enabled by default.

CNAME Support

As an extension to geo-location support, you can configure GSLB to send a Canonical Name (CNAME) record instead of an Address record in DNS replies to clients. A CNAME record maps a domain name to an alias for that domain. For example, you can associate the following aliases with the domain “example.com”:

- www.example.co.cn
- mail.example.com
- ftp.example.com

Each of the aliases in the list above can be associated with a different geo-location:

If a client’s IP address is within the geo-location that is associated with `www.1.example.com`, then GSLB places a CNAME record for `www.1.example.com` in the DNS reply to that client.

To configure CNAME support:

- Configure geo-location as described above.
- In the GSLB policy, enable the following DNS options:
  - dns cname-detect (enabled by default)
  - dns geoloc-alias
- For individual services in the zone, configure the aliases and associate them with geo-locations.

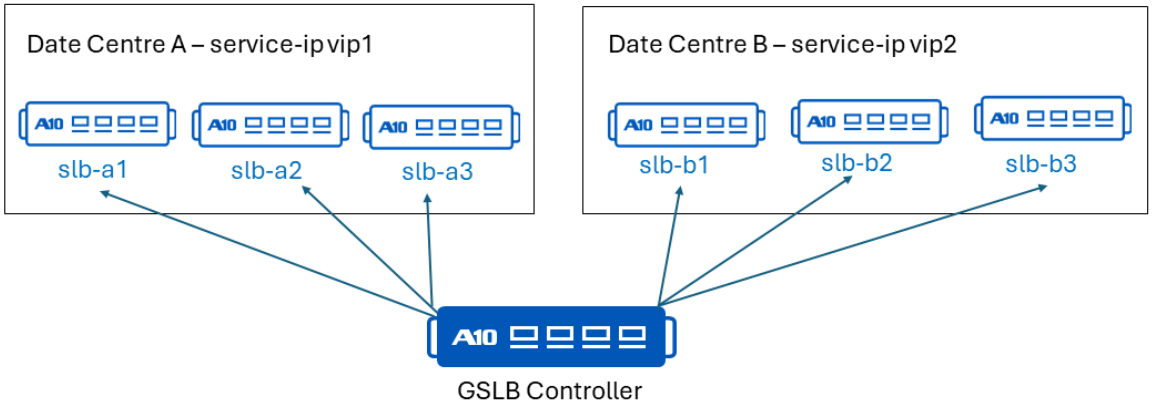
Connection Count by Site

Connection-Count-by-Site – Sites having service IPs with the lowest aggregated current connections are preferred. This metric is only supported for virtual IP servers (VIPs), specifically designed for scaleout clusters sharing the same VIP among multiple SLB devices. A named static virtual IP used as a scaleout service IP provides

support for multiple devices. It distributes network traffic across the multiple devices without making any interventions or changes to the network design.

The following configuration example indicates two sites; site_test1 and site_test2 hosting multiple devices. There are two GSLB service IPs vip1 and vip2. These are configured in the GSLB controller.

Figure 8 : Scaleout vip for multiple SLB devices



The three devices in site_test1 are bound to the same VIP, that is, vip1. Similarly, the three devices in site_test2 are bound to vip2. Within the zone testexample.com, both the virtual IPs are added as named static virtual IPs under a device. The metric is configured in test_policy1 and the policy is bound to the zone testexample.com.

```
!
gslb service-ip vip1 10.20.1.10
       port 80
gslb service-ip vip2 10.30.1.20
       port 80
!
gslb site site_test1
        slb-dev slb-a1 10.20.1.1
                vip-server vip1
        slb-dev slb-a2 10.20.1.2
                vip-server vip1
        slb-dev slb-a3 10.20.1.3
                vip-server vip1
!
gslb site site_test2
        slb-dev slb-b1 10.30.1.1
```

```
                vip-server vip2
        slb-dev slb-b2 10.30.1.2
                vip-server vip2
        slb-dev slb-b3 10.30.1.3
                vip-server vip2
!
gslb policy test_policy1
  dns-server
  connection-count-by-site enable
  metric-order connection-count-by-site
!
gslb zone testexample.com
       policy test_policy1
       service 80 www
            dns-a-record vip1 static
            dns-a-record vip2 static
!
gslb protocol status-interval 5
gslb protocol enable controller
!
```

The connection count by site metric works as follows:

1. To access www.testexample.com, the DNS query is sent to the configured DNS server for the IP address associated with www.testexample.com.
2. The DNS server (configured with GSLB zone testexample.com) responds with the IP addresses of vip1 (10.20.1.10) and vip2 (10.30.1.20).
3. The GSLB controller uses the test_policy1 to select either site_test 1 or site_test2. The record with the lowest connection count within the site is served on top. Accordingly, traffic is redirected to the site with the lower count.
4. The server processes the client's request and send the response back through the SLB device to the client.

Supported Features and Limitations

- The current connection metric is only supported for virtual IP servers bound under multiple SLB devices.
- The scaleout virtual IP servers must be restrictively used by only one site.

- A maximum of 16 SLB devices can share a service IP as a VIP server.
- The metric only considers the connection count of ports having active services.

Limitations

This feature has the following Health Check-related and other limitations:

- The health monitor health check function is not supported for scaleout service IPs configured as VIP servers.
- The GSLB Protocol health check stores the health status per SLB device at the port and service-level for scaleout virtual IPs. The service IP will indicate the 'UP' status if any of the devices in the scaleout cluster is up, and indicate the 'DOWN' status only if all the devices in the cluster are down. Connection count of virtual IP servers having services/ports with the DOWN status is not considered and displayed as 0 in the **`show gslb site curr-conn`** command.
- The current connection metrics is not calculated for service IP records used as IP servers directly under a site.
- Scaleout service IPs do not support virtual IP servers added as a dynamic server or as IP address (instead of name) under a device.
- The service-port overload feature is not supported.
- Configuring the `health-check-disable` command, along with `health-check-protocol-disable` command for shared scaleout virtual IPs and under their corresponding ports will mark the health status as ‘UP’ for the service and their corresponding ports, irrespective of the health status received from the GSLB protocol. The connection-count metric will be updated for the port and site aggregation, as received via the GSLB protocol.
- If the timestamp of the last received current connection count metric is older than twice the status-interval in GSLB protocol update duration, the current connection metric is considered as stale and not included in the aggregate port/site count.
- Scaleout service IP VIP servers will not display the 'disabled' state correctly in the `show gslb service-port` and `show gslb service-ip` commands.

Connection Load

Connection-Load – Sites that are not exceeding their thresholds for new connections are preferred.

Num Session

Num-Session – Sites that are not exceeding available Session-Capacity threshold compared to other sites are treated as having the same preference.

Admin Preference

Admin-Preference – The site with the highest administratively set preference is selected.

BW Cost

The BW-Cost metric selects sites based on bandwidth utilization on the site ACOS links.

To compare sites based on bandwidth utilization, the GSLB ACOS device sends SNMP GET requests for a specified MIB interface object, such as ifInOctets, to each site.

- If the SNMP object value is less than or equal to the site's configured bandwidth limit, the site is eligible for selection.
- If the SNMP object value is greater than the bandwidth limit configured for the site, then the site is ineligible.

The GSLB ACOS device sends the SNMP requests at regular intervals. Once a site is ineligible, the site can become eligible again at the next interval if the utilization is below the configured limit minus the threshold percentage.

To use the BW-Cost metric, an SNMP template must be configured and bound to each site. The GSLB SNMP template specifies the SNMP version and other information necessary to access the SNMP agent on the site ACOS device, and the Object Identifier (OID) of the MIB object to request.

In addition, the following BW-Cost parameters must be configured on each site:

- Bandwidth limit – The bandwidth limit specifies the maximum value of the requested MIB object for the site to be eligible for selection.
- Bandwidth threshold – For a site to regain eligibility when BW-Cost is being compared, the SNMP object's value must be below the threshold-percentage of the limit value.

For example, if the limit value is 80,000 and the threshold is 90 (percent), then the limit value must be 72,000 *or less*, for the site to become eligible again based on bandwidth cost. Once a site again becomes eligible, the SNMP object's value is again allowed to increase up to the bandwidth limit value (80,000 in this example).

Configuring Bandwidth Cost

To use the BW-Cost metric:

1. On the site ACOS devices, configure and enable SNMP.
2. On the GSLB ACOS device:
    a. Configure a GSLB SNMP template.
    b. Add the template to the GSLB site configuration.
    c. Optionally, set the bandwidth limit and threshold on the site. By default, the bandwidth limit is not set (unlimited).

Enable the BW-Cost metric in the GSLB policy. By default, the BW-Cost metric is disabled.

Configuring a GSLB SNMP Template (CLI Procedure)

The **`gslb template snmp`** command configures a GSLB SNMP template. This command adds the template and changes the CLI to the configuration level for the template, where the following template-related commands are available:

The **`version`** command specifies the SNMP version running on the site ACOS device.

The **`host`** command specifies the IP address of the site ACOS device.

The **`oid`** command specifies the interface MIB object to query on the site ACOS device. If the object is part of a table, append the table index to the end of the OID. Otherwise, the ACOS device will return an error.

The **community** command (SNMPv1 / SNMPv2c) specifies the community string required for authentication.

The **username** command (SNMPv3) specifies the SNMPv3 username required for access to the SNMP agent on the site ACOS device.

The **security-level** command specifies the SNMPv3 security level

no-auth – Authentication is not used and encryption (privacy) is not used. This is the default.

- **auth-no-priv** – Authentication is used but encryption is not used.
- **auth-priv** – Both authentication and encryption are used.

The **auth-proto** and **auth-key** commands are applicable in **auth-no-priv** or **auth-priv**. security levels. **Auth-proto** specifies the authentication protocol. **Auth-key** command specifies the authentication key.

The **priv-proto** and **priv-key** commands are applicable for **auth-priv**. security level. The **priv-proto** command specifies the privacy protocol used for encryption. The **priv-key** command specifies the encryption key.

The **context-engine-id** command specifies the SNMPv3 protocol engine ID running on the site ACOS device. The **context-name** command specifies an SNMPv3 collection of management information objects accessible by an SNMP entity. The **security-engine-id** command specifies the ID of the SNMPv3 security engine running on the site ACOS device.

The **interface** command specifies the SNMP interface ID.

The **interval** command specifies the amount of time between each SNMP GET to the site ACOS devices.

The **port** command specifies the port where site ACOS devices listen for SNMP requests from the GSLB ACOS device.

To apply a GSLB SNMP template to a GSLB site, use the **template** command at the configuration level for the site:

To configure the bandwidth limit and threshold on a site, use the **bw-cost limit** command at the site's configuration level

To enable the bandwidth cost metric in a GSLB policy, use the **bw-cost** command at the configuration level for the policy:

Use the **show gslb site** command to display BW-Cost data for a site.

Configuring SNMPv2c (CLI Example)

The following commands configure a GSLB SNMP template for SNMPv2c:

```
ACOS(config)# gslb template snmp snmp-1
ACOS(config-snmp:snmp-1)# version v2c
ACOS(config-snmp:snmp-1)# host 192.168.214.214
ACOS(config-snmp:snmp-1)# oid .1.3.6.1.2.1.2.2.1.16.12
ACOS(config-snmp:snmp-1)# community public
ACOS(config-snmp:snmp-1)# exit
ACOS(config)#
```

The following commands apply the SNMP template to a site and set the bandwidth limit and threshold:

```
ACOS(config)# gslb site usa
ACOS(config-gslb site:usa)# template snmp-1
ACOS(config-gslb site:usa)# bw-cost limit 100000 threshold 90
ACOS(config-gslb site:usa)# exit
ACOS(config)#
```

The following commands enable the BW-Cost metric in the GSLB policy:

```
ACOS(config)# gslb policy pol1
ACOS(config-policy:pol1)# bw-cost fail-break
ACOS(config-policy:pol1)# exit
ACOS(config)#
```

The following command displays BW-Cost data for the site:

```
ACOS# show gslb site usa bw-cost
                            U = Usable, TI = Time Interval
                                USGN = Unsigned, SN64 = Unsigned 64
                                CNTR = Counter,  CT64 = Counter 64
Site        Template    Current    Highest    Limit      U Type Len   Value
    TI
-------------------------------------------------------------------------------
------
```

```
usa         snmp-1      31091       142596      100000      Y CNTR    4
3355957308 3
ACOS#
```

Configuring SNMPv3 (CLI Example)

The following commands configure a GSLB SNMP template for SNMPv3. In this example, authentication and encryption are both used.

```
ACOS(config)# gslb template snmp snmp-2
ACOS(config-snmp:snmp-2)# security-level auth-priv
ACOS(config-snmp:snmp-2)# host 192.168.214.214
ACOS(config-snmp:snmp-2)# username read
ACOS(config-snmp:snmp-2)# oid .1.3.6.1.2.1.2.2.1.16.12
ACOS(config-snmp:snmp-2)# priv-proto des
ACOS(config-snmp:snmp-2)# auth-key 12345678
ACOS(config-snmp:snmp-2)# priv-key 12345678
ACOS(config-snmp:snmp-2)#
```

Least-Response

Least-Response – Service IP addresses with the fewest hits are preferred.

Admin-IP

Admin-IP – Sites are preferred based on administratively assigned weight.

Round-Robin

Round-Robin – Sites are selected in sequential order.

The ACOS device uses Round-Robin as a tie-breaker to select a site. This is true even if the Round-Robin metric is disabled in the GSLB policy.

Alias-Admin-Preference

The Alias-Admin-Preference metric selects the DNS CNAME record with the highest administratively set preference. This metric is similar to the Admin-Preference metric,

but applies only to DNS CNAME records.

The Alias Admin Preference metric, which selects the DNS CNAME record with the highest administratively set preference, can be used in DNS Proxy or DNS Server mode. Similarly, the Weighted Alias metric, which expresses a preference for higher-weighted CNAME records, can be used in DNS Proxy or DNS Server mode.

Some additional policy options are required in either mode.

- DNS proxy – Enable the geoloc-alias option. After GSLB retrieves the DNS response from the DNS answer, GSLB selects a DNS A record using IP metrics, and then tries to insert the DNS CNAME record into the answer based on geo-location settings. While inserting the CNAME record, if the Alias metrics are enabled, GSLB may remove some CNAME records and related service IPs.
- DNS server – If applicable, enable the backup-alias option. If there is no DNS A record to return, GSLB tries to insert all backup DNS CNAME records. During insertion, if Alias metrics are enabled, GSLB may remove some CNAME records. No DNS A records are returned.

This option also requires the dns-cname-record as-backup option on the service.

Configuring Alias Admin Preference

To configure the Alias Admin Preference metric:

1. At the configuration level for the GSLB service, assign an administrative preference to the DNS CNAME record for the service.
2. At the configuration level for the GSLB policy:
    a. Enable the Alias Admin Preference metric.
    b. Enable one or both of the following DNS options, as applicable to your deployment:
        i. DNS backup-alias
        ii. DNS geoloc-alias
3. If using the backup-alias option, use the dns-cname-record as-backup option on the service.

Configuring Alias Admin Preference (CLI Procedure)

1. To assign an administrative preference to the DNS CNAME record for a service, use the **admin-preference** command (gslb zone) at the service configuration level.
2. To enable the Alias Admin Preference metric, use the **alias-admin-preference** command (alias-admin-preference) at the policy configuration level

Weighted-Alias

The Weighted-Alias metric evaluates CNAME records. CNAME records with higher weight values have preference over CNAME records with lower weight values. This metric is similar to Weighted-IP, but applies only to DNS CNAME records.

Configuring Weighted Alias

To configure the Weighted Alias metric:

1. At the configuration level for the GSLB service, assign a weight to the DNS CNAME record for the service.
2. At the configuration level for the GSLB policy:
   a. Enable the Weighted Alias metric.
   b. Enable one or both of the following DNS options, as applicable to your deployment:
      i. DNS backup-alias
      ii. DNS geoloc-alias
3. If using the backup-alias option, use the dns-cname-record as-backup option on the service.

Configuring Weighted Alias (CLI Procedure)

1. To assign a weight to the DNS CNAME record for a service, use the **weight** command (gslb zone) at the service configuration level.
2. To enable the Weighted Alias metric, use the **weighted-alias** command (weighted-alias) at the policy configuration level.

GSLB Secure

To configure secure GSLB, use the following commands:

acos# gslb protocol secure disable / enable-fallback / enable

gslb secure-attributes

Configure the certificate for Secure GSLB. Use global configuration from GSLB master, using global command for GSLB protocol

- cert - Certificate for Secure GSLB
- enable - Enable Secure
- disable - Disable Secure
- enable - fallback Fall back to non-secure if fail
- use-global-config - Use global config under gslb protocol (default)

Provide SSL connection success/failure counters with reason codes if the SSL connection fails for any reason. Gslb protocol support for SSL handshake and also print decrypted info once SSL handshake is established successfully. Details will be provided in later stages of development. This per-partition configuration will have priority over global configuration.

Example:

If global configuration have Gslb protocol secure disable And in a particular partition, configuration have: GSLB secure-attributes. This particular partition will have ssl enabled, but all other partitions will have SSL disabled. CERT configuration under secure-attributes.

DNS Support

This section describes supported DNS functions.

The following topics are covered:

DNS Options

These sections describe DNS option functions.

The following topics are covered:

DNS Option Descriptions

DNS options provide additional control over the IP addresses that are listed in DNS replies to clients. The following DNS options can be set in GSLB policies

The cname-detect and external-ip options are enabled by default. All the other DNS options are disabled by default.

This following topics are covered:

DNS Action

The DNS action option enables GSLB to perform DNS actions specified in the service configurations.

The **`dns action`** command enables the active-only fail-safe option and returns a list of server IP addresses for failed servers.

DNS Active-only

By default, if all of the servers failed to pass the health check, then the GSLB controller would return an empty list to the client, rather than sending the list of IP addresses for the servers that had failed the health check.

You can configure the ACOS device to send the list of IP addresses (associated with servers that failed their health checks) back to the client. The feature can be enabled using the new dns active-only metric option.

In association with this feature, you can also designate one or more backup servers, and the IP addresses for these servers will be sent to the client in the event that all of the primary servers have failed. This behavior requires that you enable the dns backup-server feature within the GSLB policy, and that you specify the backup servers within the DNS A-record for the GSLB zone service.

To summarize, there are now two options:

- *active-only fail-safe* – A list of IP addresses for the servers that failed the health check are sent back to the client.
- *backup-server* – Designate one or more backup servers that can be returned to the client if the primaries should fail.

Configuring DNS Active-Only (CLI Example)

The **dns active-only fail-safe** command enables the active-only fail-safe option and returns a list of server IP addresses for failed servers (dns active-only).

These commands enable the DNS active-only fail-safe option within a GSLB policy, so a list of IP addresses are sent to the client for the servers that fail the health check.

```
ACOS(config)# gslb policy default
ACOS(config-policy:default)# dns active-only fail-safe
ACOS(config-policy:default)# exit
```

DNS Addition-MX

The DNS Addition-MX option appends MX records in the Additional section in replies for A records, when the device is configured for DNS proxy or cache mode.

DNS Auto-Mapping

An ACOS device acting as a GSLB controller can retrieve the data needed to build the DNS system by automatically returning DNS records by name. This GSLB Auto-Mapping feature reduces the required amount of DNS management work when deploying GSLB.

- This feature only works with GSLB wildcard service.
- There is no L3V support for SLB server or SLB virtual server.
- Names exceeding 20 characters must be changed to DNS domain, with labels separated by the '.' character.

With, GSLB Auto-mapping, the ACOS device automatically creates the service by taking the name of a system resource, or "module", and appending it to the front of a zone to create the service name (DNS name).

Once the servers and other network devices have been configured with basic information, auto-mapping enables the GSLB protocol to support DNS queries for the following modules (or system resources):

- SLB server
- SLB virtual server
- SLB device
- GSLB site
- GSLB service-IP
- GSLB Group
- Hostname

1. Select Config Mode > Service > GSLB.
2. Click the Site tab, and then click the Add button.
3. Scroll down and click the arrow button to expand the Options section.
   A window similar to the one shown below appears:
4. Select the Auto Map checkbox, if it is not already selected.
5. Click the Policy tab, and then click the Add button.
6. Scroll down and click the arrow button to expand the Auto Map section.
   A window similar to the one shown below appears:
7. By default, all modules (resources) are selected. You can select or clear the checkboxes to determine which “modules” or system resources for which the GSLB protocol will support DNS queries.
8. Either accept the default TTL value of 300 seconds, or enter a new time-to-live for

the modules.

9. Click OK to store your changes.

Configuring Auto-Mapping (CLI Procedure)

Configuring DNS Auto-mapping requires the following steps:

1. Configure DNS Auto-mapping at the zone level or system level.
2. Enable DNS Auto-mapping the zone and/or system level.

Configure DNS Auto-mapping at the System Level (CLI Procedure)

By default, system auto-mapping is disabled until you configure the modules. However, after system auto-mapping has been configured, the query name is the object's name.

The **`gslb system auto-map module`** command (global configuration level) configures auto-mapping.

By default, all modules are enabled in the policy.

Configure DNS Auto-mapping at the Zone Level (CLI Procedure)

The `dns auto-map` command configures auto-mapping for a zone level. This command enables creation of A and AAAA records for IP resources configured on the ACOS device. This option is useful for auto-mapping VIP addresses to service-IP addresses.

To receive a DNS response, the query name is in this format: `<obj-name>.<zone-name>`

Example: ,For a real server of *us-svr1*, and wildcard zone of *example.com*, the query name should be *us-svr1.example.com*

Configuring Auto-Mapping (CLI Example)

The following example configures a VIP called "WWW" at IP 192.168.1.100.

```
ACOS(config)# slb virtual-server WWW 192.168.1.100
ACOS(config-slb vserver)# port 80 http
ACOS(config-slb vserver-vport)# exit
ACOS(config-slb vserver)# exit
```

Next, the commands below configure a GSLB policy “auto-map”, for the zone “example.com”. A wildcard service IP is used. If a client sends a query for a host within the “example.com” zone (for example, an ACOS with the name "sj-acos"), then the full service name is “sj-acos.example.com”., and the GSLB protocol will respond to the client’s query by providing the management IP address and the IP address for the inbound data interface.

```
ACOS(config)# gslb policy auto-map
ACOS(config-policy:auto-map)# dns auto-map
ACOS(config-policy:auto-map)# gslb zone example.com
ACOS(config-zone:example.com)# service 80 *
ACOS(config-zone:example.com-service:*)# policy auto-map
```

DNS Backup Alias

The DNS dns backup-alias option returns the alias CNAME record configured for the service when GSLB does not receive an answer to a query for the service and no active DNS server exists. This option is valid in server mode or proxy mode.

The **dns backup-alias** command configures the DNS backup-alias option.

DNS Backup Server mode

The DNS backup-server option designates one or more backup servers that can be returned to the client if the primaries should fail. To designate one or more backup servers to be returned to the client if the primary servers fail, do the following:

1. Use the **dns backup-server** command to enable the backup server mode within the GSLB policy:
2. Specify the backup servers in the dns-a-record within the GSLB zone service with the **dns-a-record** command.

Configuring Backup Server Mode (CLI Example)

The commands below are used within a GSLB policy to specify that a backup server at IP 192.168.123.1 will be returned to the client, should the primary servers fail.

```
ACOS(config)# gslb policy default
ACOS(config-policy:default)# dns backup-server
ACOS(config-policy:default)# exit
ACOS(config)# gslb zone z1
ACOS(config-zone:z1)# service 80 http
```

```
ACOS(config-zone:z1-service:http)# dns-a-record 192.168.123.1 as-backup
ACOS(config-zone:z1-service:http)# exit
ACOS(config-zone:z1)# exit
```

DNS Cache

The DNS Cache option enables the GSLB ACOS device to cache DNS replies. The ACOS device uses information in the cached DNS entries to reply to subsequent client requests, as opposed to sending a new DNS request for every client query.

When this option is enabled, the ACOS device caches a DNS reply for the duration of the TTL in the reply when the aging time parameter is set to zero. To override the entry TTL, set the cache aging time to a value greater than zero.

The **dns cache** command configures the DNS cache option.

DNS CNAME detect

The DNS CNAME detect option enables CNAME response mode. When the ACOS device is in CNAME response mode, it applies the zone and service policy to the CNAME record instead of applying it to the address record. When CNAME response mode is disabled, the zone and service policy is applied to the address record.

The **dns cache** command configures the DNS cname-detect option.

DNS Sub-zone Delegation

GSLB sub-zone delegation allows you to delegate authority or responsibility for a portion of the DNS name space from the parent domain to a separate sub-domain which may reside on one or more remote servers and may be managed by someone other than the network administrator responsible for the parent zone.

By delegating responsibility for a sub-zone (or “sub-domain”), you are effectively dividing up the name space. This division allows for partitioning the responsibility for the DNS name space management.

For example, assume a San Jose-based company is expanding rapidly and decides to open an office in New York for its finance division. With the additional traffic generated by client DNS resolvers on the East Coast, the parent domain, (“example.com”) may no longer suffice. In this case, it might be helpful to add a

separate sub-zone (“finance.example.com”) for the New York office. Such a scenario is shown in Figure 9.

Figure 9 : Name space for finance division is delegated as new sub-zone

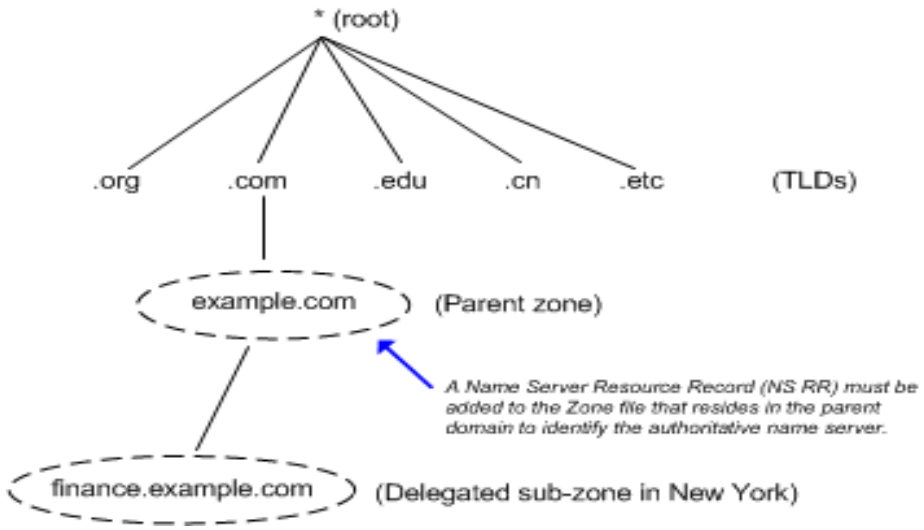


Figure 9 shows the root zone at the top of the DNS hierarchy. The figure also illustrates the following important points:

- The next level down are the Top Level Domains (TLDs), or the DNS servers responsible for managing the resource records for the “.com”, “.org” and other domains.
- The parent zone is located beneath the TLDs. It is at this level within the DNS structure that the organization’s main domain (“example.com”) is located.
- A separate sub-zone (“finance.example.com”), representing the New York office, has been delegated from the parent zone.

As this hypothetical sub-zone is branched off of the parent domain, it might be helpful to delegate responsibility for managing this new sub-zone to an IT administrator who is also located in New York.

Keep in mind that during the process of delegating authority for any sub-zone, an NS record must be added to the zone file within the authoritative name server for the parent zone. This must be done so that other DNS servers and clients will recognize the new server as being authoritative for the particular delegated sub-zone.

- Sub-zone delegation is enabled within a GSLB policy and applied at the zone level.
- When delegating a sub-zone, the GSLB ACOS device must be in server mode. The feature will not work with the GSLB ACOS device in proxy mode.
- Once a sub-zone has been delegated from the parent zone, client resolvers will send a query for the NS record, and the response from the GSLB ACOS device will have the NS record in the Authority section and the IP address in the Additional section of the full DNS response.

The ACOS device supports configuration of glue records. A glue record can be configured to prevent circular dependencies, which can occur if the name server is located in a sub-zone of the parent domain. Such a scenario can make it impossible for the client resolver to locate the IP for the name server, because it is located within a sub-zone of the parent domain. Configuring a glue record eliminates this problem by providing an address record that appears in the Additional section of the full DNS response, and this enables the client to find the name server.

The **dns delegation** command enables DNS subzone delegation.

Configuring DNS Sub-Zone Delegation (CLI Example #1)

The following command configures the GSLB policy, and places the GSLB ACOS device in server mode. The **delegation** command, which is also applied at the DNS level, enables the sub-zone delegation.

```
ACOS(config)# gslb policy delegate-1
ACOS(config-policy:delegate-1)# dns server
ACOS(config-policy:delegate-1)# dns delegation
ACOS(config-policy:delegate-1)# exit
```

The following command creates the sub-zone to be delegated. Note that this also requires the configuration of a wildcard service.

```
ACOS(config)# gslb zone sub.example.com
ACOS(config-zone:sub.example.com)# service 80 *
ACOS(config-zone:sub.example.com-service:*)# exit
ACOS(config-zone:sub.example.com)# exit
```

Alternatively, use these commands (instead of the previous gslb zone command block) to have the feature support DNSSEC by removing the “sub.” from the zone config. See the DDoS Mitigation Guide (for ADC) for information about DNS Security Extensions (DNSSEC).

```
ACOS(config)# gslb zone example.com
ACOS(config-zone:example.com)# service 80 *.sub
ACOS(config-zone:example.com-service:*.sub)# exit
```

The following command creates the NS record in the GSLB policy:

```
ACOS(config-zone:example.com)# dns-ns-record ns.finance.example.com
```

This command applies the delegation policy (delegate-1) at the zone level for the service group level:

```
ACOS(config-zone:example.com)# policy delegate-1
```

Configuring DNS Sub-Zone Delegation (CLI Example #2)

The following command configures the GSLB named static service IP “ns-ip-1” at IP 172.16.11.211 and disables the health check at the service IP level and at port 53 for UDP.

```
ACOS(config)# gslb service-ip ns-ip-1 172.16.11.211
ACOS(config-service-ip:ns-ip-1)# health-check-protocol-disable
ACOS(config-service-ip:ns-ip-1)# health-check-disable
ACOS(config-service-ip:ns-ip-1)# port 53 udp
ACOS(config-service-ip:ns-ip-1-port:udp)# health-check-protocol-disable
ACOS(config-service-ip:ns-ip-1-port:udp)# health-check-disable
ACOS(config-service-ip:ns-ip-1-port:udp)# exit
ACOS(config-service-ip:ns-ip-1)# exit
```

The following command configures the named static GSLB service IP “dc1-vip” at IP 10.10.10.10 and disables the health check at the service IP level and at port 80 for TCP.

```
ACOS(config)# gslb service-ip dc1-vip 10.10.10.10
ACOS(config-service-ip:dc1-vip)# health-check-protocol-disable
ACOS(config-service-ip:dc1-vip)# health-check-disable
ACOS(config-service-ip:dc1-vip)# port 80 tcp
ACOS(config-service-ip:dc1-vip-port:tcp)# health-check-protocol-disable
ACOS(config-service-ip:dc1-vip-port:tcp)# health-check-disable
ACOS(config-service-ip:dc1-vip-port:tcp)# exit
ACOS(config-service-ip:dc1-vip)# exit
```

The following command configures the GSLB named static service IP “ns-ip-1” at IP 172.16.10.203 and disables the health check at the service IP level and at port 80 for TCP.

```
ACOS(config)# gslb service-ip dc2-vip 172.16.10.203
ACOS(config-service-ip:dc2-vip)# health-check-protocol-disable
ACOS(config-service-ip:dc2-vip)# health-check-disable
ACOS(config-service-ip:dc2-vip)# port 80 tcp
ACOS(config-service-ip:dc2-vip-port:tcp)# health-check-protocol-disable
ACOS(config-service-ip:dc2-vip-port:tcp)# health-check-disable
ACOS(config-service-ip:dc2-vip-port:tcp)# exit
ACOS(config-service-ip:dc2-vip)# exit
```

The following commands configure a GSLB site called “dc1”. The site has an ACOS device, “dc1-acos” at named static virtual IP 10.10.10.50.

```
ACOS(config)# gslb site dc1
ACOS(config-gslb site:dc1)# slb-dev dc1-acos 10.10.10.50
ACOS(config-gslb site:dc1-slb dev:dc1-acos)# vip-server dc1-vip
ACOS(config-gslb site:dc1-slb dev:dc1-acos)# exit
ACOS(config-gslb site:dc1)# exit
```

The following commands configure a GSLB site called “dc2”. The site has an ACOS device, “dc2-acos” at named static virtual IP 172.16.10.50.

```
ACOS(config)# gslb site dc2
ACOS(config-gslb site:dc2)# slb-dev dc2-acos 172.16.10.50
ACOS(config-gslb site:dc2-slb dev:dc2-acos)# vip-server dc2-vip
ACOS(config-gslb site:dc2-slb dev:dc2-acos)# exit
ACOS(config-gslb site:dc2)# exit
```

The following commands configure a GSLB site called “dc5”. The site has an ACOS device, “dc5-ax” at named static virtual IP 172.16.11.50.

```
ACOS(config)# gslb site dc5
ACOS(config-gslb site:dc5)# slb-dev dc5-ax 172.16.11.50
ACOS(config-gslb site:dc5-slb dev:dc5-ax)# vip-server ns-ip-1
ACOS(config-gslb site:dc5-slb dev:dc5-ax)# exit
ACOS(config-gslb site:dc5)# exit
```

The following commands configure three GSLB policies: (1) the default GSLB policy, (2) GSLB policy “5” (for delegation), and (3) GSLB policy “dns-server”. The ACOS delegates authority for the sub-domain “sub.sub.example.com.jp” to nameserver "ns01.sub.sub.example.com.jp".

```
ACOS(config)# gslb policy default
ACOS(config-policy:default)# exit
ACOS(config)# gslb policy 5
```

```
ACOS(config-policy:5)# dns delegation
ACOS(config-policy:5)# dns server
ACOS(config-policy:5)# exit
ACOS(config)# gslb policy dns-server
ACOS(config-policy:dns-server)# dns server
ACOS(config-policy:dns-server)# exit
```

The following commands create the GSLB zone “sub.sub.example.com.jp” and creates a wildcard service within the zone. The GSLB policy “5”, created above, is assigned to the wildcard service, and an NS record is created for the name server, “ns01.sub.sub.example.com.jp”.

```
ACOS(config)# gslb zone sub.sub.example.com.jp
ACOS(config-zone:sub.sub.example.)# service 80 *
ACOS(config-zone:sub.sub.example.-servic...)# policy 5
ACOS(config-zone:sub.sub.example.-servic...)# dns-ns-record
ns01.sub.sub.example.com.jp
ACOS(config-zone:sub.sub.example.-servic...)# exit
```

The following commands are used within the same GSLB zone “sub.sub.example.com.jp” to creates a service for port 53 called “ns01”. The GSLB policy “dns-server”, created above, is assigned to the service, and an A record is created for “ns-ip-1” to return the associated Service-IP if the DNS is in server mode.

```
ACOS(config-zone:sub.sub.example.)# service 53 ns01
ACOS(config-zone:sub.sub.example.-service...)# policy dns-server
ACOS(config-zone:sub.sub.example.-service...)# dns-a-record ns-ip-1 static
ACOS(config-zone:sub.sub.example.-service...)# exit
ACOS(config-zone:sub.sub.example.)# exit
```

The following commands creates the GSLB zone “sub.example.com.jp” and enables the http service. Then, the policy “dns-server” is bound and A records are create for “dc1-vip” and “dc2-vip”.

```
ACOS(config)# gslb zone sub.example.com.jp
ACOS(config-zone:sub.example.com.)# service 80 www
ACOS(config-zone:sub.example.com.-service...)# policy dns-server
ACOS(config-zone:sub.example.com.-service...)# dns-a-record dc1-vip static
ACOS(config-zone:sub.example.com.-service...)# dns-a-record dc2-vip static
ACOS(config-zone:sub.example.com.-service...)# exit
ACOS(config-zone:sub.example.com.)# exit
```

The following command enables the GSLB and makes this ACOS device the GSLB controller.

```
ACOS(config)# gslb protocol enable controller
```

DNS External-IP

The DNS external-ip option configures the device to return the external IP address configured for a service IP. If this option is disabled, the internal address is returned instead.

The **dns external-ip** command configures the DNS external-ip option.

DNS External-SOA

The DNS external-soa option replaces the internal SOA record with an external SOA record to prevent external clients from gaining information that should only be available to internal clients. If this option is disabled, the internal address is returned.

The **dns external-soa** command configures the DNS external-soa option.

DNS Geoloc-Action

The DNS geoloc-action option performs the DNS traffic handling action specified for the client's geo-location. The action is specified as part of service configuration in a zone.

The **dns geoloc-action** command configures the DNS geoloc-action option.

DNS Geoloc-Alias

The DNS geoloc-alias option replaces the IP address with its alias configured on the GSLB ACOS device.

The **dns geoloc-alias** command configures the DNS geoloc-alias option.

DNS Geoloc-Policy

The DNS geoloc-policy option returns the alias name configured for the client's geo-location.

The **dns geoloc-policy** command configures the DNS geoloc-policy option.

Hints in DNS Responses

By default, the ACOS device places hints in the Additional Section of the DNS response. Hints are A or AAAA records that are sent in the response to a client's DNS request. These records provide a mapping between the host names and IP addresses.

You can disable the appearance of hints in a DNS response. In addition, you also can determine *where* in the DNS response the hints will appear.

Hints can appear in the following sections of a DNS response:

- None – Does not append hints in the DNS response
- Additional – Appends hints in the Additional Section (default)
- Answer – Appends hints in the Answer Section

This option applies to the following record types:

- NS
- MX
- SRV

Configuring DNS Response Hints (CLI Example)

The **dns hint** command (dns hint) specifies the Hint Record (or Glue Record) that appears in DNS replies sent from the GSLB ACOS device to a client's DNS request.

These commands configure the ACOS device to include the Hint Record in the Answer Section of the DNS response. One possible use is when the local DNS server has trouble parsing the Additional Section that appears in a full DNS reply.

```
ACOS(config)# gslb policy default
ACOS(config-policy:default)# dns hint answer
ACOS(config-policy:default)# exit
```

DNS IP-Replace

The DNS ip-replace option replaces the IP addresses with the set of addresses administratively assigned to the service in the zone configuration.

The **dns ip-replace** command configures the DNS external-soa option.

DNS IPv6

DNS ipv6 options enables support for IPv6 AAAA records.

- The **dns ipv6 mapping** command specifies the ACOS device response to IPv6 DNS query.
- The **dns ipv6 max** command configures the ACOS device to return AAAA and A records in the same response.
- The **dns ipv6 smart** command enables IPv6 return by query type.
- The command: **slb server** *<server_name> <FQDN>* **resolve-as-ipv6-address**. If the user prefers this hostname to be resolved to an IPv6 AAAA record, specify from CLI/GUI using a new option "**resolve-as-ipv6-address**" that hostname must be resolved to an IPv6 AAAA record. See IPv6 Support for AAAA and Dynamic Real Server for details.

DNS Logging

The following output options for GSLB logging are supported:

- Log *only* to the ACOS device's local logging buffer.
- Log *only* to remote log servers.

Remote Logging

Logging only to remote log servers is useful for deployments that experience high volumes of GSLB DNS traffic. Sending the logs for this activity to a group of remote servers prevents these messages from flooding the ACOS device's log.

- Logging only to remote log servers applies specifically to GSLB DNS logging, configurable globally and in individual GSLB policies.
- Logging templates are included in HA or VRRP-A configuration synchronization. They are not included in GSLB synchronization among GSLB groups.

Enabling DNS Logging for a GSLB Policy (Procedure)

To enable DNS logging for a GSLB policy:

1. Configure a logging group and logging template, if not already configured. Logging groups also are supported in previous releases. Beginning in ACOS 2.7.2-

P2, you also can use logging groups for GSLB. You can configure the logging group to receive log traffic over TCP or UDP, depending on which Layer 4 protocol the servers use to receive log traffic.

2. In the GSLB policy, enable DNS logging and specify the SLB logging group to use. By specifying a logging group, you enable remote logging and disable local logging, for GSLB DNS events.

Enabling DNS Logging for a GSLB Policy (CLI Example)

The following commands create a simple GSLB configuration that uses remote logging for DNS events handled by GSLB. In this simple deployment, client DNS requests for the IP address of "www.example.com" always receive the same IP address (192.1.1.190) in the DNS response from GSLB.

The policy in this example is set to run GSLB in DNS server mode. Logging of GSLB DNS events to remote logging servers is also supported for proxy mode. The syntax for the logging portion of the configuration is the same.

Logging Group Configuration (CLI Example)

These commands configure the logging group, which consist of the logging server, service group, and logging template.

```
ACOS(config)# slb server log-s1 10.1.1.20
ACOS(config-real server)# port 1514 tcp
ACOS(config-real server-node port)# exit
ACOS(config-real server)# exit
ACOS(config)# slb service-group log tcp
ACOS(config-slb svc group)# member log-s1 1514
ACOS(config-slb svc group-member:1514)# exit
ACOS(config-slb svc group)# exit
ACOS(config)# slb template logging log
ACOS(config-logging)# service-group log
ACOS(config-logging)# exit
```

GSLB Configuration (CLI Example)

These commands configure the DNS VIP that will intercept UDP DNS requests from clients:

```
ACOS(config)# slb virtual-server vip 10.1.1.190
ACOS(config-slb vserver)# port 53 udp
ACOS(config-slb vserver-vport)# gslb-enable
ACOS(config-slb vserver-vport)# exit
ACOS(config-slb vserver)# exit
```

These commands configure the named static service-IP and the site. This is the site that GSLB helps clients reach. The site SLB device that is load-balancing the server (192.1.1.190) is a Thunder device (192.1.1.100). The site SLB device's configuration is not shown.

```
ACOS(config)# gslb service-ip gs3 192.1.1.190
ACOS(config-service-ip:gs3)# port 80 tcp
ACOS(config-service-ip:gs3-port:tcp)# exit
ACOS(config-service-ip:gs3)# exit
ACOS(config)# gslb site ssl
ACOS(config-gslb site:ssl)# slb-dev thunder 192.1.1.100
ACOS(config-gslb site:ssl-slb dev:thunder)# vip-server gs3
ACOS(config-gslb site:ssl-slb dev:thunder)# exit
ACOS(config-gslb site:ssl)# exit
```

The following commands configure the GSLB policy. The `dns logging both template log` command enables logging of DNS events to remote logging servers and disables logging of the events to the local buffer.

```
ACOS(config)# gslb policy p1
ACOS(config-policy:p1)# dns server
ACOS(config-policy:p1)# dns logging both template log
ACOS(config-policy:p1)# exit
```

These commands configure the zone, "example.com" and service, "www". For this service, a static DNS Address (A) record is configured. Based on this configuration, GSLB responds to client queries for www.example.com with the IP address of service-IP "gs3".

```
ACOS(config)# gslb zone example.com
ACOS(config-zone:example.com)# policy p1
ACOS(config-zone:example.com)# service 80 www
ACOS(config-zone:example.com-service:www)# dns-a-record gs3 static
ACOS(config-zone:example.com-service:www)# exit
ACOS(config-zone:example.com)# exit
```

GSLB DNS Log Messages Sent to Remote Log Server

The following messages are sent to the remote logging server to indicate a DSN query from a client for www.example.com, and the response sent to the client:

```
May 30 17:22:16 10.1.1.180  QUERY Fwd 10.1.1.190 10.1.1.68 www.example.com
A 43617
May 30 17:22:16 10.1.1.180  RESP Server 10.1.1.190 10.1.1.68
www.example.com A 43617 0 0 1 [A,1,10,4,192.1.1.190]
```

Query Log

The first message logs the DNS query message intercepted by ACOS and forwarded to the GSLB DNS server. The message provides the following details:

- May 30 17:22:16 10.1.1.180 – Timestamp indicating the system time on the ACOS device when GSLB generated the message.
- QUERY – Type of DNS message.
- Fwd 10.1.1.190 – VIP address of the GSLB DNS server to which ACOS forwarded the request.
- If GSLB is running in DNS server mode, this is the GSBL DNS VIP configured on the same device.
- If GSLB is running in DNS proxy mode, this is the IP address of the external DNS server bound to by the DNS VIP.
- 10.1.1.68 – Client IP address (local DNS).
- www.example.com – The host for which the client is requesting the IP address.
- A – The type of query. In this example, this is a query for an IPv6 address (A).
- 43617 – DNS transaction ID.

Response Log

The second message logs the response to the client's DNS query.

- May 30 17:22:16 10.1.1.180 – Message timestamp.
- RESP – Type of message, in this case a DNS Response.
- Server – GSLB DNS mode, Proxy or Server.

- 10.1.1.190 – VIP address of the GSLB DNS server from which the response is sent.
- 10.1.1.68 – Client IP address (local DNS).
- www.example.com – The host for which the client is requesting the IP address.
- A – Type of record in the response. In this case, the response includes an IPv4 address record.
- 43617 – DNS transaction ID.
- 0 0 1 – Shows the following information:
- GSLB error code (Code 0 indicates success.)
- DNS reply code in header
- Answer count
- [A,1,10,4,192.1.1.190] – Content of the answer:
- A – Record type
- 1 – Class type
- 10 – TTL
- 4 – Data length
- 192.1.1.190 – DNS VIP address of the GSLB DNS server (or proxy, if proxy mode is used)

Local Logging

Logging can be done to the local server. However, local logging is not recommended for deployments that experience high volumes of GSLB DNS traffic as it can over utilize memory and CPU and impact the disk capacity and available resources.

Local logging is disabled by default. To enable local logging:

1. Configure acos-events with the related lineage.

```
ACOS(config)#acos-events message-id gslb all
ACOS(config-log-msg:all)#property log-route local-only
```

2. Enable GSLB logging to log both, DNS queries and responses.

```
ACOS(config)#gslb dns logging both
```

NOTE: The `acos-events rate-limit-local` command configures the limit for local logging, which is set to `<0-100>`.

DNS Proxy

GSLB does not have a separately configurable “proxy” option. The proxy option is automatically enabled when you configure the DNS proxy as part of GSLB configuration.

Support for DNS CNAME Records

This feature enhances GSLB to reply to GSLB DNS requests with load-balanced CNAMEs records. When the feature is enabled, a CNAME record is associated with a hostname server through a policy assignment. The ACOS device can then monitor the record’s status through a port-level or server-level health check.

The feature is defined on a GSLB policy basis. When the policy is assigned to a GSLB zone, the feature is implemented for DNS server CNAME records that are managed within the zone

Configuring DNS CNAME Load Balancing (CLI Example)

The following configuration implements the DNS CNAME records feature.

1. This code associates a pre-configured Health Monitors (HMONITOR-1) to DNS servers accessed from the GSLB zone. This code does not include the configuration of the HMONITOR-1 Health Monitor.

```
ACOS(config)# slb server s1 www1.example.com
ACOS(config-real server)# health-check HMONITOR-1
ACOS(config-real server)# exit
ACOS(config)# slb server s2 www2.example.com
ACOS(config-real server)# port 80 tcp
ACOS(config-real server-node port)# health-check HMONITOR-1
ACOS(config-real server-node port)# exit
ACOS(config-real server)# exit
```

2. This code configures the policy for replying to CNAME records. The other policy commands filter CNAME records that are DOWN and enable the return of a single CNAME record.

```
ACOS(config)# gslb policy OXYGEN
ACOS(config-policy:OXYGEN)# dns server cname
```

```
ACOS(config-policy:OXYGEN)# dns active-only
ACOS(config-policy:OXYGEN)# dns selected-only 1
ACOS(config-policy:OXYGEN)# exit
```

3. This code implements the CNAME reply policy to the zone that accesses the DNS servers.

```
ACOS(config)# gslb zone a10africa.com
ACOS(config-zone:a10africa.com)# policy OXYGEN
ACOS(config-zone:a10africa.com)# service 80 www
ACOS(config-zone:a10africa.com-service:www)# dns-cname-record
www1.example.com
ACOS(config-zone:a10africa.com-service:www)# dns-cname-record
www2.example.com
ACOS(config-zone:a10africa.com-service:www)# exit
ACOS(config-zone:a10africa.com)# exit
```

DNS Selected-only

The DNS selected-only option configures the device to return only the selected IP addresses.

The **dns selected-only** command enables return of only selected IP addresses. The command specifies a limit of records that can be returned after a record is selected. When the number of records exceed the configured value, GSLB ignores this configuration.

DNS Server

The DNS Server options enables the GSLB ACOS device to act as a DNS server for specific service IPs in the GSLB zone. When this setting is enabled, the ACOS device responds directly to address queries for specific service IP addresses in the GSLB zone. The ACOS device still forwards other types of queries to the DNS server.

In DNS Server mode, the `dns cname-detect` command is not required. When a client requests a configured alias name, GSLB applies the policy to the CNAME records. The **dns server** command is not valid with the **dns ip-replace** command. They are mutually exclusive.

DNS Server mode requires the enalbing of the **static** option on the individual service IP. (To configure the service IP addresses, use the **service-ip** command at the configuration level for the service.

The **dns server** command configures the DNS external-ip option. (missing or bad snippet)**Command Line Reference** Guide.

DNS Sticky

The DNS Sticky options sends the same service IP address to a client for all requests from that client for the service address.

The **dns sticky** command programs the device to send the same service IP address to a client for all requests from that client for the service address. Sticky DNS ensures that, during the aging-time, a client is always directed to the same site.

DNS Sticky with ECS

EDNS client subnet (ECS) is a mechanism used to encapsulate a client's real source IP address within a DNS query or HTTP payload. This helps you to protect the client's real source IP by masking it. Sticky DNS ensures that, a client is always directed to the same IP during the aging-time.

In ACOS 6.0.6 sticky sessions with ECS are supported in GSLB. DNS sticky with ECS uses client's subnet information to direct traffic to the nearest data center by the routing requests with the lowest latency.

The DNS sticky with ECS has the following conditions:

- DNS Sticky and ECS match - If a matching session exists in the DNS sticky table, resolve the clients request using DNS Sticky and ECS information.
- No session match (DNS sticky/ECS) - If no matching session is based on DNS sticky or ECS, resolve the query based on metric order and create a session with minimum subnet of /24 for IPv4 and /112 for IPv6.
- No ECS - If ECS information is not available, resolve the query using Local DNS Server (LDNS) information and create a sticky session.
- aRDT behavior - aRDT always uses LDNS information to update the statistics summary in the table.

Limitations

- GSLB service groups are not supported for sticky sessions.
- Local DNS (LDNS) and ECS subnet information rarely match, if they do the default match will align with the first session created.
- Sticky session matching with ECS requires an exact match irrespective of LDNS or ECS lookup.
- The existing sticky subnet mask configuration applies only to LDNS sessions and not to EDNS.

DNS TTL Override

GSLB ensures that DNS replies to clients contain the optimal set of IP addresses based on current network conditions. However, if the DNS TTL value assigned to the Address records is long, the local DNS servers used by clients might cache the replies for a long time and send those stale replies to clients. Thus, even though the GSLB ACOS device has current information, clients might receive outdated information.

To ensure that the clients' local DNS servers do not cache the DNS replies for too long, you can configure the GSLB ACOS device to override the TTL values of the Address records in the DNS replies before sending the replies to clients.

The TTL of the DNS reply can be overridden in two different places in the GSLB configuration:

1. If a GSLB policy is assigned to the individual service, the TTL set in that policy is used.
2. If no policy is assigned to the individual service, but the TTL is set in the zone, then the zone's TTL setting is used.

By default, the TTL override is not set in either of these places.

In DNS server mode, the DNS response from the ACOS device includes an IP TTL (maximum number of Layer 3 hops), with a default value equal to 255. This IP TTL can be configured using the following CLI command: **`gslb system ip-ttl`**.

The **`dns ttl`** command programs the ACOS device to change the TTL of each DNS record contained in DNS replies received from the DNS for which the ACOS device is a proxy.

IPv6 Support for AAAA and Dynamic Real Server

An SLB server configured with a hostname gets resolved to an IPv6 address when the DNS server has only a AAAA record for the hostname. When user configures a dynamic server using hostname, such as **slb server** *server-name* **detail** for FQDN, ACOS only sends an authentication query.

If the user prefers this hostname to be resolved to an IPv6 AAAA record, specify from CLI or GUI using a new option "**resolve-as-ipv6-address**" that hostname must be resolved to an IPv6 AAAA record. By default when no such option is entered, it will be IPv4 address.

CLI Configuration Command

Use the following command to resolve hostname to an IPv6 AAAA record, specify from CLI using a new option "**resolve-as-ipv6-address**"

```
ACOS (config)# slb server rs1 www.google.co m resolve-as-ipv6-address.
```

To check if the configuration is working, use the command: **show slb server both detail**. The "**show slb server** <*server_name*> FQDN **detail**" command now displays all additional IPv6 related server and statistical parameters.

GUI Configuration

An optional setting for "IPv6 address resolution" under **FQDN name** parameter is available in
ADC > SLB > Servers > Create page**. I**f the server is configured with hostname instead of an IP address, this option is supported in fast path and slow path.

DNS Options Preference

If more than one of the following options are enabled, GSLB uses them in the order listed

The following topics are covered:

GSLB does not have a separately configurable “proxy” option. The proxy option is automatically enabled when you configure the DNS proxy as part of GSLB configuration.

The site address selected by the first option that is applicable to the client and requested service is used.

DNS Records

These sections describe DNS records functions:

This following topics are covered:

Append NS Records in DNS Authority Section

GSLB supports name server (NS) records in the Authority Section of the DNS response. When this feature is enabled, the GSLB ACOS device (running in server mode) will include all NS records in the Authority Section of the DNS response that is sent to the client. By providing additional NS information, this feature can be helpful if one or more of the name servers becomes unavailable.

To append all Name Server (NS) Resource Records (RR) in the Authority Section of a DNS reply from a GSLB ACOS device in server mode, use the **`fdns server authoritative ns-list`** command at the **`gslb policy`** configuration level.

Support for DNS TXT Records

The TXT record is a type of DNS resource record, similar to an A record or a CNAME record, but it has typically been used to carry machine-readable data, opportunistic encryption, Sender Policy Framework (SPF), Domain Keys, and DNS-SD. (Refer to RFC 1464 for further details on uses for TXT resource records.)

GSLB supports the ability to use DNS TXT resource records for the following purposes:

- Perform Add/Delete/Find operations, based on a DNS TXT record
- Support multiple DNS TXT records for each service
- Carry multiple pieces of DNS TXT data within one TXT record
- Support DNS TXT/ANY query in server mode
- Support GSLB debug functions

The maximum length of a DNS TXT record data is 2048 characters.

NOTE: Use quotation marks when entering text strings that contain spaces. If a text string is entered without using quotation marks, this will cause the content to be split into different sections of the record.

Configuring DNS TXT Records (CLI Procedure)

The `dns server txt` command configures the device to use DNS TXT resource records to carry multiple pieces of DNS TXT data within one TXT record,

Then use the `dns-txt-record` command at the service config level within a GSLB zone:

The ACOS device has a special handler that enables you to enter non-printable characters that the CLI does not support.

Displaying DNS TXT Records (CLI Procedure)

To display the DNS TXT Records, use the `show gslb service dns-txt-record` command.

To display the DNS TXT switch, use the `show gslb policy` command.

Multi-Match Rule-Based DNS Resolution

The following sections provide information on Multi-Match Rule-Based DNS Resolution.

The following topics are covered:

Overview

Multi-match rule-based DNS Resolution allows you to redirect the incoming DNS client queries to a target zone service (within the same zone) based on specific conditions, such as the domain name, the client's source IP, and the health status of services or servers.

This feature is useful in the following scenarios where you need granular control to manage and distribute DNS traffic based on certain conditions:

- To ensure high availability by resolving DNS queries to appropriate servers or sites based on their current health status, avoiding servers or sites that are down or partially operational.
- To implement traffic management policies based on the source of DNS queries i.e., client IP addresses. For example, direct internal client queries to local servers and route external queries to a different set of servers.

This rule-based DNS resolution thus provides granular control over DNS query management and helps improve the availability and reliability of services across distributed environments. To implement multi-match rule-based DNS resolution, you need to configure the **service-matching-rules** command.

Service Matching Rules

The **service-matching-rules** command allows you to configure rules in a GSLB zone to redirect DNS queries to a target service when certain conditions are met.

When a client DNS query is received, if it matches all the conditions specified in a service matching rule, the query is redirected to the configured target service of the matched rule (under the same zone). The policies and configurations of the new target service are then used to process the query.

Consider the following example configuration:

```
gslb service-matching-rules zone a10.com
 rule 1
   domain-name equals www.in-example.com
   health-state slb-server dc1-link-1a Down
```

```
service www-example-service
```

Here, rule *1* is configured under the zone *a10.com*. In this rule, the DNS queries are redirected to the *www-example-service* service only when the following conditions are met:

- The domain name matches *wwwin-example.com*.
- The *dc1-link-1a* SLB server is in Down state.

This rule ensures that the traffic is routed to the target service based on the health status of the SLB server.

The following options can be configured as conditions using the **service-matching-rules** command:

- **domain-name** – Check if the DNS query name matches the specified domain name. You can use one of the following match options:
  - **equals** *string* – Matches if the domain name completely matches the specified string.
  - **contains** *string* – Matches if the specified string appears anywhere within the domain name.
  - **starts-with** *string* – Matches if the domain name starts with the specified string.
  - **ends-with** *string* – Matches if the domain name ends with the specified string.
- **health-state** – Check the health state of the specified object.

  You can check one of the following objects and its corresponding states:
  - **gslb-site** – Check the health state of the GSLB site by specifying the options **AllUp**, **AllUp-or-PartUp**, **Down-or-PartUp**, or **Down** that allow you to verify if all the components of the specified GSLB site are in Up state, Down state, or partially Up state.
  - **gslb-service-ip** - Check the health state of the GSLB service IP. You can verify if the specified GSLB service IP is in Up state (**Up**) or Down state (**Down**).
  - **slb-server** - Check the health state of the SLB server. You can verify if the specified SLB server is in Up state (**Up**) or Down state (**Down**).

- **source-addr** *{ A.B.C.D/nn | A:B:C:D:E:F:G:H/nn }* – Check if the client source IP address falls within the specified IPv4 or IPv6 subnet.

Additionally, you can configure the **hitcount-enable** parameter to enable the hit count for rule matching. For viewing and clearing the hit count, see Show and Clear Commands.

Key Considerations

Consider the following points while configuring service matching rules in GSLB zones:

- A rule must contain at least one condition and a target service, else it is considered invalid.
- A maximum of 500 service matching rules can be configured for one GSLB zone.
- The rules are matched sequentially, starting with rule 1 and ending with rule 500.
- A maximum of four health-state statements can be defined in a single service matching rule.
- Ensure that the target zone service exists within the same zone as the rule; it cannot cross zones.

NOTE: If no rules are matched or no service-matching rules are configured, ACOS processes DNS queries as usual.

Example Configurations

Example 1

```
rule 1
 domain-name equals www.example.com
 health-state gslb-site a10-dc2 Down-or-PartUp
 health-state slb-server link-1b Down
 service example-service1
```

In this rule, the DNS queries are redirected to the *example-service1* service only when the following conditions are met:

- The domain name matches *www.example.com*
- The *a10-dc2 GSLB* site is either in Down state or is in partially Up state.

- The *link-1b* SLB server is in Down state.

Example 2

```
rule 2
 domain-name contains example
 source-addr 7.7.7.64/26
 health-state gslb-site a10-dc1 AllUp-or-PartUp
 service example-service2
```

In this rule, the DNS queries are redirected to the *example-service2* service only when the following conditions are met:

- The domain name contains the string *example*.
- The DNS query originates from the IP range *7.7.7.64/26*.
- The *a10-dc1* GSLB site is either in Up state or partially Up state.

CLI Configuration

- To implement multi-match rule-based DNS resolution, you need to define service-matching rules in a GSLB zone. Use the service-matching-rules command to define the rules as shown below:

```
ACOS(config)# gslb service-matching-rules zone a10.com
ACOS(config-service-matching-rules:a10.com)# rule 1
ACOS(config-service-matching-rules:a10.co...)# domain-name equals
www.a10.com
ACOS(config-service-matching-rules:a10.co...)# source-addr 10.214.6.0/24
ACOS(config-service-matching-rules:a10.co...)# health-state gslb-site
a10-dc1 AllUp-or-PartUp
ACOS(config-service-matching-rules:a10.co...)# health-state gslb-
service-ip a10-rs1 Up
ACOS(config-service-matching-rules:a10.co...)# health-state slb-server
a10-dc1-link-1b Up
ACOS(config-service-matching-rules:a10.co...)# service www-view-cl1
ACOS(config-service-matching-rules:a10.co...)# exit
ACOS(config-service-matching-rules:a10.com)# rule 2
```

```
ACOS(config-service-matching-rules:a10.co...)# domain-name equals
www.a10.com
ACOS(config-service-matching-rules:a10.co...)# source-addr 10.214.6.0/24
ACOS(config-service-matching-rules:a10.co...)# health-state gslb-site
a10-dc1 Down
ACOS(config-service-matching-rules:a10.co...)# health-state gslb-site
a10-dc2 AllUp-or-PartUp
ACOS(config-service-matching-rules:a10.co...)# health-state slb-server
a10-dc1-link-1b Down
ACOS(config-service-matching-rules:a10.co...)# service www-view-cl2
```

In the above example configuration, service matching rules are created within the GSLB zone *a10.com*. If the conditions from rule *1* match, the DNS query is redirected to *www-view-cl1*. Else, if the conditions from rule *2* match, the query is redirected to *www-view-cl2*.

- To delete a particular service matching rule from the GSLB zone:

```
ACOS(config)# gslb service-matching-rules zone a10.com
ACOS(config-service-matching-rules:a10.com...)# no rule 2
```

After executing this command, rule *2* will be removed from the *a10.com* GSLB zone.

NOTE: If a GSLB zone is removed, all configured service-matching rules within that zone are also removed.

- To enable the hit count for rule matching within a GSLB zone, configure the **hitcount-enable** parameter:

```
ACOS(config)# gslb service-matching-rules zone a10.com
ACOS(config-service-matching-rules:a10.com...)# hitcount-enable
```

Show and Clear Commands

- To view the service matching rules configured in a specified zone, use the following command:

```
ACOS(config)# show gslb zone <zone-name> service-matching-rules
```

Example:

```
ACOS(config)# show gslb zone a10.com service-matching-rules
```

```
GSLB Zone a10.com:
Rule matching enabled, Hit count disabled
Total number of Valid SMRules: 2
Rule Target-Service       Hit
-------------------------------------------------------------------------
---------
1    www-view-cl1         0
2    www-view-cl2         0
```

- To view the service matching rules for all available zones, use the following command:

```
ACOS(config)# show gslb zone service-matching-rules
```

Example:

```
ACOS(config)# show gslb zone service-matching-rules
GSLB Zone a10.com:
Rule matching enabled, Hit count enabled
Total number of Valid SMRules: 2
Rule Target-Service      Hit
-------------------------------------------------------------------------
---
1    www-view-cl1         7
2    www-view-cl2         0
GSLB Zone google.com:
No service-matching-rules configured.
```

- To clear the service matching rule hit count for the specified GSLB zone, use the following command:

```
ACOS(config)# clear gslb zone <zone-name> service-matching-rules
```

- To clear the service matching rule hit count for all GSLB zones, use the following command:

```
ACOS(config)# clear gslb zone all service-matching-rules
```

For more information on show and clear commands, see the *Command Line Interface Reference guide*.

Geo-Location Mappings

A geo-location mapping consists of a geo-location name and an IP address or IP range.

- If you manually map a geo-location to an GSLB site, GSLB uses the mapping.
- If no geo-location is configured for a GSLB site, GSLB automatically maps the service-ip to a geo-location in the loaded geo-location database.
- If a service-ip cannot be mapped to a geo-location, GSLB maps the site ACOS device to a geo-location.
- If more than one geo-location matches a client's IP address, the most specific match is used. For example, if a client is in the same city as a site ACOS, that site will be preferred. If the client and site are in the same state but in different cities, the site in that state will be preferred.

Only one database can be active. If you load more than one database, the most-recently loaded one becomes the active one, and the older database is no longer used. Data from the older database is not merged into the new database. Using the "load" command to load a new database will synchronize the start-up configuration among all GSLB group members.

There is full parity in the synchronization, so the process works in reverse also. Unloading a geo-location database from a configuration, or deleting a geo-location database, will remove that database from all GSLB group members.

The following topics are covered:

Loading or Configuring Geo-Location Mappings

You can manually or automatically load and configure Geo-Location Mappings. This section has the following sub-topics:

The following topics are covered:

Geo-Location Database Files

You can load the geo-location database (which contains the geo-location mappings) from one of the following types of files:

Internet Assigned Numbers Authority (IANA) database – The IANA database contains geographic locations of IP address ranges and subnets assigned by the IANA. This database is loaded by default.

Custom database in CSV format – You can load a custom geo-location database from a file in comma-separated-values (CSV) format. However, before loading the file, you must first configure a CSV template on the ACOS device because the data in the file is formatted by the template.

Geo-Location Database File Example

An example of a database file is shown below. Each paragraph is actually a single line in the file, but they are displayed here in multiple lines due to the limited width of the page. (Note that lines in the database file should not have spaces between the paragraphs. This was done to improve readability.)

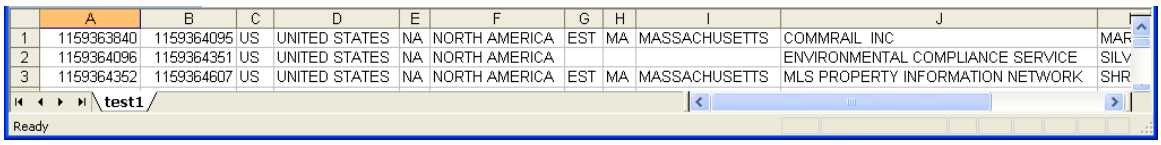
```
"119363840","11936409","US","UNITED STATES","NA","NORTH
AMERICA","EST","MA","MASSACHUSETTS", "COMMRAIL
INC","MARLBOROUGH","MIDDLESEX","42.3495","-71.5482"

"1159364096","1159364351","US","UNITED STATES","NA","NORTH
AMERICA","","","","ENVIRONMENTAL COMPLIANCE
SERVICE","SILVER","","32.0708","-100.682"

"1159364352","1159364607","US","UNITED STATES","NA","NORTH
AMERICA","EST","MA","MASSACHUSETTS", "MLS PROPERTY INFORMATION
NETWORK","SHREWSBURY","WORCESTER","42.2959","-71.7134"
...
```

The example above shows how the CSV file appears when displayed in a text editor. If the same data were displayed in a spreadsheet application, it would appear like CSV File in Spreadsheet Application below.

Figure 10 : CSV File in Spreadsheet Application



	A	B	C	D	E	F	G	H	I	J	
1	1159363840	1159364095	US	UNITED STATES	NA	NORTH AMERICA	EST	MA	MASSACHUSETTS	COMMRAIL INC	MAR
2	1159364096	1159364351	US	UNITED STATES	NA	NORTH AMERICA				ENVIRONMENTAL COMPLIANCE SERVICE	SILV
3	1159364352	1159364607	US	UNITED STATES	NA	NORTH AMERICA	EST	MA	MASSACHUSETTS	MLS PROPERTY INFORMATION NETWORK	SHR

test1

Ready

The database file can contain more types of information (fields, or columns) than are required for the GSLB database. When you load the CSV file into the geo-location database, the CSV template on the ACOS device filters the file to extract the required data, while ignoring the rest of the data. In the example below, only the fields shown in bold type will be extracted and placed into the geo-location database:

```
"1159363840","1159364095","US","UNITED STATES","NA","NORTH
AMERICA","EST","MA","MASSACHUSETTS","COMMRAIL
INC","MARLBOROUGH","MIDDLESEX","42.3495","-71.5482"
```

These fields contain the following information:

```
From IP address (starting IP address in range), To IP address (ending IP
address in range, or subnet mask), Continent, Country
```

The IP addresses in this example are in bin4 format. Dotted decimal format (for example: 69.26.125.0) is also supported. If you use bin4 format, the ACOS device automatically converts the addresses into dotted decimal format when you load the database into GSLB.

Creating and Loading a Custom Geo-Location Database

To create and load a custom geo-location database:

1. Prepare the database file. (This step requires an application that can save to text for CSV format, and it cannot be performed on the ACOS device.)
2. Configure a CSV template on the ACOS device. The CSV template specifies the field positions (or columns) in the database that should be extracted, such as IP address and location information.
3. Import the CSV file onto the ACOS device.

4. Load the CSV file.
5. Display the geo-location database.

1. Select Config Mode > Service > GSLB.
2. On the menu bar, select Geo-location > Import.
3. In the Template section, enter a name for the template.
4. If the CSV file uses a character other than a comma to delimit fields, enter the delimiter character in the Delimiter field. You want the CSV template to use the same delimiter that has been used in the database file you will be loading.
5. In each data field, indicate the field's position (or column) in the CSV file. For example, if the destination IP address or subnet is listed in the CSV file in the fourth column, enter "4" in the IP-To field.
6. Click Add.

1. Select Config Mode > Service > GSLB, if not already selected.
2. On the menu bar, select Geo-location > Import, if not already selected..
3. In the File section, select the file transfer protocol.
4. Enter the filename and the access parameters required to copy the file from the remote server.
5. Click Add.

1. Select Config Mode > Service > GSLB, if not already selected.
2. On the menu bar, select Geo-location > Import, if not already selected..
3. In the Load/Unload section, enter the name of the geo-location database in the file field.
4. In the Template field, enter the name of the template to use for formatting the data.

Configuring the CSV Template (CLI Procedure)

On the ACOS device, you must configure a CSV template for the database file. When you load the file into GSLB, the ACOS device uses the template to extract the data and load it into the GSLB database.

1. Use the **gslb template csv** command to create the template.
2. Use the **field** command to identify the field positions for the geo-location data:
3. If the CSV file does not use commas to delimit fields, use the **delimiter** command to specify the delimiter.

CSV File Field Delimiters

CSV file fields must be separated by a delimiter. By default, the ACOS device interprets commas as delimiters. When configuring a CSV template on the ACOS device, the delimiter can be set to any valid ASCII character.

Importing the CSV File (CLI Procedure)

To import the CSV file onto the ACOS device, use the **import geo-location** command at the Privileged EXEC or global configuration level of the CLI:**period** *num*]

You can enter the entire URL on the command line or press Enter to display a prompt for each part of the URL.If you enter the entire URL and a password is required, you will still be prompted for the password. To enter the entire URL:

- tftp://*host/file*
- ftp://[*user*@]*host*[:*port*]/*file*
- scp://[*user*@]*host/file*
- disk:*path*
- sftp://[*user*@]*host/file*

(For information about the **use-mgmt-port** option, see the “Using the Management Interface as the Source for Management Traffic” chapter in the *System Configuration and Administration Guide*.)

Loading the CSV File Data into the Geo-Location Database (CLI Procedure)

To load the CSV file, use the **gslb geo-location** command at the global configuration level of the CLI:

Use the file name you specified when you imported the CSV file, and the name of the CSV template to be used for extracting data from the file.

To display information about CSV files as they are being loaded, use the **show gslb geo-location** command.

Converting IP Addresses into bin4 Format (Procedure)

If you want to use bin4 format in the CSV file, here is how to convert an IP address from dotted-decimal format to bin4 format:

1. Convert each node into Hex.
2. Convert the resulting Hex number into decimal.
3. Enter the decimal number into the database file.

Here is an example for IP address 192.0.2.18, the first IP address in the example CSV file:

Dotted Decimal	Hex of Each Node	Combined Hex	Decimal
192.0.2.18	C0.00.02.12	C0000212	3221226002

Manual Configuration

To manually configure a geo-location mapping:

1. Configure each geographic location (geo-location) as a named range of client IP addresses. You can configure geo-locations globally and within individual GSLB policies.

   To configure a geo-location, use the `gslb geo-location` command at the global configuration level or at the configuration level for the GSLB policy:

2. Associate a site with a geo-location name, using the `geo-location` command at the configuration level for the site:

If you configure geo-locations globally and at the configuration level for individual sites, and a client IP address matches both a globally configured geo-location and a geo-location configured on a site, the globally configured geo-location is used by default. To configure the GSLB ACOS device to use geo-locations configured on individual sites instead, use the geo-location match-first policy command at the configuration level for the policy.

Displaying the Geo-Location Database (CLI Procedure)

1. Select Config Mode > Service > GSLB.
2. On the menu bar, select Geo-location > Find.

To display the geo-location database, use the **show gslb geo-location** command:

To search for an entry in the geo-location database that is based on client IP address, use the **show gslb geo-location** command.

Displaying the Geo-Location Database (CLI Example)

The commands in this example load a custom geo-location database from a CSV file called “test.csv”, and then display the database. The test.csv file is shown in Geo-Location Database File Example.

First, the following commands configure the CSV template:

```
ACOS(config)# gslb template csv test1-template
ACOS(config-gslb template csv)# field 1 ip-from
ACOS(config-gslb template csv)# field 2 ip-to-mask
ACOS(config-gslb template csv)# field 5 continent
ACOS(config-gslb template csv)# field 3 country
ACOS(config-gslb template csv)# exit
```

The following command imports the file onto the ACOS device:

```
ACOS(config)# import geo-location test1.csv
ftp://1.0.0.100/BaseConfig/Test1.csv
User name []?admin2
Password []?*******
Done.
```

The following commands initiate loading the data from the CSV file into the geo-location database, and display the status of the load operation:

```
ACOS(config)# gslb system geo-location load test1.csv test1-template
ACOS(config)# show gslb geo-location file
                Per = Percentage of loading, Err/W = Error or Warning
                T = T(Template)/B(Built-in)

Filename                T Template              Per  Lines    Success
Err/W
-------------------------------------------------------------------------
-----
```

```
iana*                    B                          100% 77        77        0
test1.csv                T test1-template           100% 5         5         0

ACOS(config)#
```

The following command displays the geo-location database extracted from the CSV file.

```
ACOS(config)# show gslb geo-location db NA
                  Last = Last Matched Client, Hits = Count of Client
matched
                  Sub = Count of Sub Geo-location
                  T = Type, P-Name = Policy name
                    G(global)/P(policy), S(sub)/R(sub range)
                    M(manually config)/B(built-in)

Geo-location: NA
From             To/Mask         Last             Hits      Sub    T    P-Name
-------------------------------------------------------------------------------
-----
                                                  0         1      G

ACOS(config)#
```

Geo-Location Overlap

The geo-location overlap option searches the geo-location database for the “match best” instead of searching the database using the “match first” algorithm. This behavior may be helpful if you suspect that more than one host has been mapped to a single public IP address.

The following topics are covered:

Database Background

When configuring GSLB on the ACOS device, a geo-location file containing mappings between geographic regions and IP addresses is imported onto the ACOS device. For example, the IANA database is pre-installed on the ACOS device prior to shipping, and it contains thousands of entries mapping geographic regions to IP address ranges.

In addition, third-party companies sell geo-location databases, and some of these databases may contain millions of mappings between geographic regions and ranges of IP addresses. As with the IANA database files, these files can also be imported into the ACOS device's global database.

Geo-location information can also be *manually* configured on the ACOS device at the GSLB policy level.

A GSLB policy is typically created for each GSLB zone, so you could, for example, have separate zones for a company that has offices in New York and San Jose. Each of these GSLB zones might have its own geo-location file, with each file containing highly granular information that maps IP addresses and local regions.

When configuring geo-location for a GSLB zone, you will need to use the match first command to decide whether to search the Global database (containing the IANA file) or if you would prefer to search the GSLB Policy database.

The match first command determines which of the two geo-location databases will be used to parse incoming DNS requests from clients. That is, it allows you to decide whether the Global database or GSLB Policy database will be searched.

Once this configuration decision has been made, then the next thing that you need to do is decide if you want to enable the geo-location overlap command.

The geo-location overlap command is disabled by default because it tends to tax the ACOS processors.

The default behavior for the ACOS device is to use the match first algorithm (not to be confused with the match first option described above), is to scan the geo-location database for the first IP address that matches the client's Source IP.

In contrast, the geo-location overlap option uses match best algorithm, meaning the entire geo-location file must be scanned in order to locate the optimal response to send back to the client. This is very demanding on the ACOS CPU.

Geo-Location Overlap Usage

The geo-location overlap option is recommended for situations in which the public IP address is not unique and the same IP address may be associated with different hosts. While it is unlikely that the IANA geo-location file would contain such errors, the Internet is a dynamic place and information can become stale and/or inaccurate. In particular, this situation might happen if users are careless about the way they manually add IP addresses to the GSLB policies. A user might have many GSLB zones and each zone might have many geo-location files, so it is possible that some IP address ranges may overlap.

For example, if a company has a site in New York and San Jose:

- New York IP range is 1.1.1.1 – 1.1.1.9
- San Jose IP range is 1.1.1.1 – 1.1.1.3

In this situation, there exists an overlap in the IP address from 1.1.1.1 to 1.1.1.3.

To remedy this confusing situation, one can enable the geo-location overlap option to cause the ACOS device to search the geo-location database for the match best (or longest matching IP address).

However, if the geo-location overlap option is disabled, then the ACOS device will revert to its default behavior, which is to use the match first algorithm to check the client's IP address against the database and then use the first IP address-region mapping discovered when parsing the database.

1. Select Config Mode > Service > GSLB.
2. Click the Policy tab, and then click the Add button.
3. Enter a name for the GSLB policy in the Name field.
4. Click the Geo-location arrow to expand the menu.
5. In the Match Best Entry section, select the desired checkboxes. By default, the Global and Policy checkboxes are clear, meaning the overlap feature is disabled (and the match first approach is used).

6. To enable the overlap behavior, select one or both checkboxes in the Match Best Entry area. Your options are:
   - Global – Enabling this option will search the global database (such as IANA) for the longest matching and most-specific address.
   - Policy – Enabling this option will search the GSLB policy database for the longest matching and most-specific address.
7. When finished, click OK to save your changes.

   If you believe your manually-configured geo-location databases may have two or more domains tied to the same IP address, you can use the **geo-location-match overlap** command at the GSLB policy configuration level of the CLI to enable geo-location overlap.

   The following command enables geo-location overlap at the GSLB policy level. The overlap option is used to enable match best behavior for the geo-location database within the default GSLB policy. By enabling this behavior, the match first algorithm will not be used, and instead the ACOS device will attempt to find the best match by searching for the longest string that matches the source IP address in the client's request.

```
ACOS(config)# gslb policy default
ACOS(config-gslb policy)# geo-location-match overlap policy
ACOS(config-gslb policy)# exit
```

Overlap Implementation Example

GSLB geo-location when GSLB is configured in multiple partitions when all partitions use geo-location with overlapping client subnets.

GSLB allows only a single Geo-database in shared partition.

If there are 3 partitions and all 3 partitions have GSLB enabled:

- Partition1 admin wants to setup Datacenter in GeoLoc1 for all clients coming from IP1 (192.168.0.0/20) and Datacenter in GeoLoc2 for IP2 (192.168.16.0/20)
- Partition2 admin wants to setup Datacenter in GeoLoc3 for all clients coming from IP3 (192.168.0.0./19)

- Partition3 admin wants to prefer Datacenter in GeoLoc4 for all clients coming from IP Group (192.168.0.1 - 192.168.1.123)

Step 1: Configure Custom Geo-locations

1. In shared partition:

```
gslb service-ip vip1 1.1.1.1
  health-check-protocol-disable
  health-check-disable
  port 80 tcp
    health-check-protocol-disable
    health-check-disable
!
gslb service-ip vip2 2.2.2.2
  health-check-protocol-disable
  health-check-disable
  port 80 tcp
    health-check-protocol-disable
    health-check-disable
!
gslb service-ip vip3 3.3.3.3
  health-check-protocol-disable
  health-check-disable
  port 80 tcp
    health-check-protocol-disable
    health-check-disable
!
gslb geo-location test
  ip 55.0.0.0 mask 255.255.255.0
!
gslb geo-location test2
  ip 55.0.0.0 mask 255.255.255.128
!
gslb geo-location test3
  ip 55.0.0.0 mask 255.255.240.0
!
gslb site UK
  geo-location test
  ip-server vip1
!
```

```
gslb site HK
  ip-server vip2
!
gslb site VA
  ip-server vip3
!
```

Set up Policy Based Geo-location

```
gslb policy policy1
  no round-robin
  metric-order health-check geographic
  dns server any authoritative
  geo-location test
    ip 55.0.0.0 mask /24
  geo-location-match match-first policy
!
gslb zone test.com
  service 80 test
    policy policy1
    dns-a-record vip1 static
    dns-a-record vip2 static
    dns-a-record vip3 static
!

active-partition part1
!
gslb service-ip vip1 1.1.1.1
  health-check-protocol-disable
  health-check-disable
  port 80 tcp
    health-check-protocol-disable
    health-check-disable
!
gslb service-ip vip2 2.2.2.2
  health-check-protocol-disable
  health-check-disable
  port 80 tcp
    health-check-protocol-disable
    health-check-disable
```

```
!
gslb service-ip vip3 3.3.3.3
  health-check-protocol-disable
  health-check-disable
  port 80 tcp
    health-check-protocol-disable
    health-check-disable
!
gslb site UK
  ip-server vip1
!
gslb site HK
  geo-location test2
  ip-server vip2
!
gslb site VA
  ip-server vip3
!
gslb policy policy1
  no round-robin
  metric-order health-check geographic
  dns server any authoritative
  geo-location test2
    ip 55.0.0.0 mask /25
  geo-location-match match-first policy
!
gslb zone test.com
  service 80 test2
    policy policy1
    dns-a-record vip1 static
    dns-a-record vip2 static
    dns-a-record vip3 static

active-partition part2
!
!
interface ethernet 4
  enable
  ip address 55.0.0.222 255.255.255.0
!
```

```
!
slb virtual-server vip555 55.0.0.210
  port 53 udp
    gslb-enable
    use-rcv-hop-for-resp
!
gslb service-ip vip1 1.1.1.1
  health-check-protocol-disable
  health-check-disable
  port 80 tcp
    health-check-protocol-disable
    health-check-disable
!
gslb service-ip vip2 2.2.2.2
  health-check-protocol-disable
  health-check-disable
  port 80 tcp
    health-check-protocol-disable
    health-check-disable
!
gslb service-ip vip3 3.3.3.3
  health-check-protocol-disable
  health-check-disable
  port 80 tcp
    health-check-protocol-disable
    health-check-disable
!
gslb site UK
  ip-server vip1
!
gslb site HK
  ip-server vip2
!
gslb site VA
  geo-location test3
  ip-server vip3
!
gslb policy policy1
  no round-robin
  metric-order health-check geographic
```

```
  dns server any authoritative
  geo-location test3
    ip 55.0.0.0 mask /20
  geo-location-match match-first policy
!
gslb zone test.com
  service 80 test3
    policy policy1
    dns-a-record vip1 static
    dns-a-record vip2 static
    dns-a-record vip3 static
!
```

Access Control

You can control access to a VIP based on the geo-location of the client. You can configure the ACOS device to perform one of the following actions for traffic from a client, depending on the location of the client:

- Drop the traffic
- Reset the connection
- Send the traffic to a specific service group (if configured using a black/white list)

The ACOS device determines a client's location by looking up the client's subnet in the geo-location database used by Global Server Load Balancing (GSLB).

This feature requires you to load a geo-location database, but does not require any other configuration of GSLB. Instead, SLB features are used along with the IANA database. The ACOS system image includes the Internet Assigned Numbers Authority (IANA) database. By default, the IANA database is not loaded but you can easily load it, as described in the configuration procedure later in this section.

This following topics are covered:

Using a Class List

This section show how to configure geo-location-based VIP access using a class list.

Geo-location-based VIP access works only if the class list is imported as a file. The CLI does not support configuration of class-list entries for this application.

Class List Example (CLI Example)

The following class list maps client geo-locations to limit IDs (LIDs), which specify the maximum number of concurrent connections allowed for clients in the geo-locations.

```
L US 1
L US.CA 2
L US.CA.SJ 3
```

The following commands import the class list onto the ACOS device, configure a policy template, and bind the template to a virtual port. The connection limits specified in the policy template apply to clients who send requests to the virtual port.

This example assumes the following:

- default geo-location database (iana) is already loaded (gslb system geo-location load).
- the c-share class list was previously created

```
ACOS(config)# slb template policy pclass
ACOS(config-policy)# class-list c-share
ACOS(config-policy-class-list:c-share)# lid 1
ACOS(config-policy-class-list:c-share-li...)# conn-limit 4
ACOS(config-policy-class-list:c-share-li...)# exit
ACOS(config-policy-class-list:c-share)# lid 2
ACOS(config-policy-class-list:c-share-li...)# conn-limit 2
ACOS(config-policy-class-list:c-share-li...)# exit
ACOS(config-policy-class-list:c-share)# lid 3
ACOS(config-policy-class-list:c-share-li...)# conn-limit 1
ACOS(config-policy-class-list:c-share-li...)# exit
ACOS(config-policy-class-list:c-share)# exit
ACOS(config-policy)# geo-location overlap
```

```
ACOS(config-policy)# exit
ACOS(config)# slb virtual-server vip1 10.1.1.155
ACOS(config-slb vserver)# port 80 http
ACOS(config-slb vserver-vport)# template policy pclass
ACOS(config-slb vserver-vport)# exit
ACOS(config-slb vserver)# exit
```

The **show slb geo-location statistics** command verifies operation of the policy.

Using a Black/White List

To configure geo-location-based access control for a VIP:

1. Configure a black/white list. You can configure the list using a text editor on a PC or enter it directly into the GUI. If you configure the list using a text editor, import the list onto the ACOS device.
2. Configure an SLB policy (PBSLB) template. In the template, specify the black/white list name, and the actions to perform for the group IDs in the list.
3. Load a geo-location database, if one is not already loaded.
4. Apply the policy template to the virtual port for which you want to control access.

Configuring the Black/White List (Procedure)

You can configure black/white lists in either of the following ways:

- Remote option – Use a text editor on a PC, then import the list onto the ACOS device.
- Local option – Enter the black/white list directly into a management GUI window.

With either method, the syntax is the same. The black/white list must be a text file that contains entries (rows) in the following format:

```
L "geo-location" group-id  #conn-limit
```

The “L” indicates that the client’s location will be determined using information in the geo-location database.

The *geo-location* is the string in the geo-location database that is mapped to the client’s IP address; for example, “US”, “US.CA”, or “US.CA.SanJose”.

The *group-id* is a number from 1 to 31 that identifies a group of clients (geo-locations) in the list. The default group ID is 0, which means no group is assigned. On the ACOS device, the group ID specifies the action to perform on client traffic.

The *#conn-limit* specifies the maximum number of concurrent connections allowed from a client. The # is required only if you do not specify a group ID. The connection limit is optional. For simplicity, the examples in this section do not specify a connection limit.

Here is a simple example of a black/white list for this feature:

```
L "US"          1
L "US.CA"       2
L "JP"          3
```

1. Select Config Mode > Service > PBSLB.
2. Click New.
   - To import the list:
     - Leave Remote selected.
     - Enter a name for the list in the Name field.
     - Enter the hostname or IP address in the Host field.
     - Enter the file path and name in the Location field.
   - To enter the file directly into the GUI:
     - Select Local.
     - Type the list into the Definition field.
3. Click OK.

1. Select Config Mode > Service > Template.
2. On the menu bar, select Application > PBSLB Policy.
3. Click Add.
4. In the Name field, enter a name for the template.
5. From the drop-down list below the Name field, select the black/white list.
6. Select a group ID from the Group ID drop-down list.
7. Select one of the following from the Action drop-down list.

- Drop – Drops new connections until the number of concurrent connections on the virtual port falls below the port's connection limit. (The connection limit is set in the black/white list.)
- Reset – Resets new connections until the number of concurrent connections on the virtual port falls below the connection limit.
- *service-group-name* – Each of the service groups configured on the ACOS device is listed.
- create – This option displays the configuration sections for creating a new service group.

8. Optionally, enable logging. (The ACOS device uses the same log rate limiting and load balancing features for PBSLB logging as those used for ACL logging. See the "Log Rate Limiting" section in the "Basic Setup" chapter of the *System Configuration and Administration Guide*.)
9. Click Add.
10. Repeat through for each group ID.
11. Click OK.

1. Select Config Mode > Service > GSLB.
2. On the menu bar, select Geo-location > Import.
3. In the Load/Unload section, enter "iana" in the File field. Leave the Template field blank.
4. Click Add.

NOTE: If preferred, you can import a custom geo-location database instead. For information, see Loading or Configuring Geo-Location Mappings.

1. Select Config Mode > Service > SLB.
2. On the menu bar, select Virtual Server.
3. Select the virtual server or click Add to configure a new one.
4. If you are configuring a new VIP, enter the name and IP address for the server.
5. In the Port section, select the port and click Edit, or click Add to add a new port. The Virtual Server Port page appears.

6. Select the policy template from the PBSLB Policy Template drop-down list.
7. Click OK.
8. Click OK again to finish the changes and redisplay the virtual server list.

1. Import a black/white list onto the ACOS device with the **bw-list** command.
2. To configure a PBSLB template, use the **slb template policy** commands:

   The command creates the template and changes the CLI to the configuration for the template, where the **bw-list name** and **bw-list id** PBSLB-related commands are available.
3. Load a geo-location database with the **gslb system geo-location load** command.
4. To apply a policy template to a virtual port, use the **template policy** command in configuration mode

Displaying and Clearing SLB Geo-Location Information (CLI Procedure)

To display SLB geo-location information, use the **show slb geo-location** command.

To clear SLB geo-location statistics, use the **clear slb geo-location** command.

Black/White List Example (CLI Example)

The following commands configure a policy template named “geoloc” and add a black/white list to it. The template is configured to drop traffic from clients in the geo-location mapped to group 1 in the list.

The black/white list can either be imported or by selecting **ADC >> BW-Lists** in the GUI. Refer to the DDos Mitigation Guide (DMG) for additional information about black/white lists.

```
ACOS(config)# slb template policy geoloc
ACOS(config-policy)# bw-list name geolist
ACOS(config-policy)# bw-list id 1 drop
ACOS(config-policy)# exit
```

The following commands apply the policy template to port 80 on virtual server “vip1”:

```
ACOS(config)# slb virtual-server vip1
ACOS(config-slb vserver)# port 80 http
ACOS(config-slb vserver-vport)# template policy geoloc
```

```
ACOS(config-slb vserver-vport)# show slb geo-location

                          M = Matched or Level, ID = Group ID
                          Conn = Connection number, Last = Last Matched IP
                            v = Exact Match, x = Fail
  Virtual Port: vip/80, geolist
-------------------------------------------------------------------------------
-----
 Max Depth: 1
   Success: 1
Geo-location                 M  ID Permit    Deny      Conn      Last
-------------------------------------------------------------------------------
-----
US                           x  1  0         0         0
-------------------------------------------------------------------------------
-----
     Total: 1
ACOS(config-slb vserver-vport)# exit
ACOS(config-slb vserver)# exit
```

Full-Domain Checking

By default, when a client requests a connection, the ACOS device checks the connection count only for the specific geo-location level of the client. If the connection limit for that specific geo-location level has not been reached, then the client's connection is permitted. Likewise, the permit counter is incremented only for that specific geo-location level.

Table 2 shows an example set of geo-location connection limits and current connections.

Table 2 : Geo-Location connection limit example

Geo-Location	Connection Limit	Current Connections
US	100	100
US.CA	50	37
US.CA.SanJose	20	19

Using the default behavior, the connection request from the client at US.CA.SanJose is allowed even though CA has reached its connection limit. Likewise, a connection request from a client at US.CA is allowed. However, a connection request from a client whose location match is simply “US” is denied.

After these three clients are permitted or denied, connection permit and deny counters are updated.

US – Deny counter is incremented by 1.

US.CA – Permit counter is incremented by 1.

US.CA.SanJose – Permit counter is incremented by 1.

This following topics are covered:

Configuring Full-Domain Checking

When full-domain checking is enabled, the ACOS device checks the current connection count not only for the client’s specific geo-location, but for all geo-locations higher up in the domain tree.

Based on full-domain checking, all three connection requests from the clients in the example above are denied. This is because the US domain has reached its connection limit. Likewise, the counters for each domain are updated as follows:

- US – Deny counter is incremented by 1.
- US.CA – Deny counter is incremented by 1.

To enable full-domain checking for geo-location-based connection limiting, use the **`geo-location full-domain-tree`** command at the configuration level for the PBSLB template.

It is recommended to enable or disable this option before enabling GSLB. Changing the state of this option while GSLB is running can cause the related statistics counters to be incorrect.

Enabling PBSLB Statistics Counter Sharing

Statistic counters can be shared by all virtual servers and virtual ports using a PBSLB template. This option causes the following counters to be shared by virtual servers and virtual ports using the template:

- Permit
- Deny
- Connection number
- Connection limit

To enable the share option, use the **`geo-location share`** command at the configuration level for the PBSLB policy template. It is recommended to enable or disable this option before enabling GSLB. Changing the state of this option while GSLB is running can cause the related statistics counters to be incorrect.

Gateway Health Monitoring

To simplify health monitoring of a GSLB site, you can use a gateway health check. A gateway health check is a Layer 3 health check (ping) sent to the gateway router for an SLB site. If a site's gateway router fails a health check, it is likely that none of the services at the site can be reached. GSLB stops using the site until it begins to pass gateway health checks again.

In most cases, an ICMP health check is sufficient; use the default ICMP health check or configure a custom one. For more detailed health analysis, use an external health check. For example, use a script to get SNMP information from the gateway, and base the gateway's health status on the retrieved information.

The following topics are covered:

Default Health Monitors

The default health monitor for a service is the default Layer 3 health monitor (ICMP ping). The default health monitor for a service port is the default TCP or UDP monitor, depending on the transport protocol.

By default, if the GSLB protocol is enabled and can reach the service, health checking is performed over the GSLB protocol. Otherwise, health checking is performed using standard network traffic instead. Optionally, you can disable use of the GSLB protocol for health checking, on individual service-IPs.

Health-Check Precedence

Health checking for a GSLB service can be performed at the following levels.

1. Gateway health check
2. Port health check
3. IP health check (Layer 3 health check of service IP)

Disabling a Gateway Health-Check

On the GSLB controller, you can disable gateway health checking at the SLB-device or service configuration level. This does not affect health checks configured for individual virtual servers and service ports at the site.

To disable gateway health checking at the SLB-device configuration level, use the **`no gateway health-check`** command. After entering this command, the SLB device stops accepting gateway status information.

Gateway Health Check Configuration

To configure gateway health checking for a GSLB site:

Configure the health monitor, unless you plan to use the default ICMP health monitor.

On the SLB device at the site, create an SLB real server configuration with the gateway router's IP address. If you configured a custom health check, make sure to apply it to the real server.

On the GSLB controller, specify the site's gateway IP address in the SLB-device configuration for the site.

The following topics are covered:

Display Health Status Site Gateway

To display the health status for a site gateway, use the **show gslb slb-device** command:

Configuring a Site with a Single Gateway Link (CLI Example)

On the site ACOS device, this command configures a real server for the gateway. The default ICMP health method is used.

```
Site-ACOS(config)# slb server acos-site 1.1.1.1
Site-ACOS(config-real server)# exit
```

On the GSLB controller, the following commands enable gateway health checking for site device “site-acos”:

```
GSLB-ACOS(config)# gslb site remote
GSLB-ACOS(config-gslb site:remote)# slb-dev site-acos 10.1.1.1
GSLB-ACOS(config-gslb site:remote-slb dev:site...)# gateway 1.1.1.1
GSLB-ACOS(config-gslb site:remote-slb dev:site...)# exit
GSLB-ACOS(config-gslb site:remote)# exit
```

The following command displays the gateway health status for GSLB sites:

```
GSLB-ACOS(config)# show gslb slb-device
         Attrs = Attributes, APF = Administrative Preference
         Sesn-Num/Uzn = Number/Utilization of Available Sessions
         GW = Gateway Status, IPCnt = Count of Service-IPs
             P = GSLB Protocol, L = Local Protocol
Device               IP              Attrs APF Sesn-Num    Uzn GW   IPCnt
-------------------------------------------------------------------------
-----
local:self           127.0.0.1             100 0            0%       0
local:self2          127.0.0.1             100 0            0%       0
local:self3          127.0.0.1             100 0            0%       2
remote:site-acos      10.1.1.1             100 0            0%  UP   0

GSLB-ACOS(config)#
```

In this example, the gateway health status for SLB-device configuration “site-acos” on the “remote” site is Up.

Multiple Gateway Links Configuration

For sites with multiple gateways, create a separate real server for each gateway on the site ACOS device. On the GSLB controller, create a separate SLB-device configuration for each gateway (real server). In each SLB-device configuration, specify only service IPs that can be reached by the gateway defined by the SLB device.

For a service IP that can be reached on any of multiple links, create a separate SLB-device configuration, *without* using the gateway option. The gateway health status for this SLB-device will be Down only if all the gateway health checks performed for the other SLB-device configurations for the site fail.

1. On the site ACOS device—To create the gateway router, navigate to the real server configuration page. Enter a name and the gateway IP address. Do not add any ports.
2. On the GSLB controller—To specify the site's gateway IP address, navigate to the site configuration page. From this page, navigate to the SLB-Device configuration page and enter the gateway IP address in the Gateway field.

   Configuring a Site with Multiple Gateway Links (CLI Procedure)

3. On the site ACOS device – To create the gateway router, use the slb server command at the global configuration level of the CLI on the site ACOS device:

   To use the default Layer 3 health monitor, no further configuration is needed on the site ACOS device. When using a custom ICMP monitor, configure the monitor, then use the **`health-check`** command at the configuration level for the real server (gateway):

4. On the GSLB controller — To specify the site's gateway IP address, use the **`gateway`** command at the configuration level for the SLB device, within the site configuration:

   Configuring a Site with Multiple Gateway Links (CLI Example)

   On the site ACOS device, the following commands configure real servers for each of two gateway links. The default ICMP health method is used for each link.

```
Site-ACOS(config)# slb server gate-1 2.2.2.1
Site-ACOS(config-real server)# exit
Site-ACOS(config)# slb server gate-2 3.3.3.1
```

```
Site-ACOS(config-real server)# exit
Site-ACOS(config)#
```

On the GSLB controller, these commands enable gateway health checking for each of the site's links. A unique SLB-device name is used for each link, even though both links are for the same SLB device (20.1.1.1).

```
GSLB-ACOS(config)# gslb site remote-line1
GSLB-ACOS(config-gslb site:remote-line1)# slb-dev site-acos-lnk1
20.1.1.1
GSLB-ACOS(config-gslb site:remote-line1-slb de...)# gateway 2.2.2.1
GSLB-ACOS(config-gslb site:remote-line1-slb de...)# exit
GSLB-ACOS(config-gslb site:remote-line1)# exit
GSLB-ACOS(config)# gslb site remote-line2
GSLB-ACOS(config-gslb site:remote-line2)# slb-dev site-acos-lnk2
20.1.1.1
GSLB-ACOS(config-gslb site:remote-line2-slb de...)# gateway 3.3.3.1
GSLB-ACOS(config-gslb site:remote-line2-slb de...)# exit
GSLB-ACOS(config-gslb site:remote-line2)# exit
```

If the same *services* can be reached through either link, an additional SLB-device configuration is required:

```
GSLB-ACOS(config)# gslb site remote-link-both
GSLB-ACOS(config-gslb site:remote-link-both)# slb-dev site-acos-lnkboth
20.1.1.1
GSLB-ACOS(config-gslb site:remote-link-both-sl...)# exit
GSLB-ACOS(config-gslb site:remote-link-both)# exit
```

No gateway is specified in the SLB-device configuration. The gateway health status will be Up unless the health checks for 2.2.2.1 *and* 3.3.3.1 both fail.

Multiple-Port Health Monitoring

GSLB supports multiple-port health checks for service IPs. When using multiple-port health check for a service IP, the service IP is marked Up if *any* port passes the health check; all ports are not required to pass the health check.

To configure a multiple-port health check, use the **health-check-port** command at the configuration level for the service IP. You can specify up to 64 ports.

Applying a health monitor is required only if you do not plan to use the default health monitors. (See Multiple-Port Health Monitoring.)

Configuring Multiple-Port Health Monitoring (CLI Example)

The following commands apply a custom HTTP health monitor to named static service IP “gslb-srvc2”. The commands utilize a health monitor (http) whose configuration is not included in the example.

```
ACOS(config)# gslb service-ip gslb-srvc2 192.168.20.99
ACOS(config-service-ip:gslb-srvc2)# port 80 tcp
ACOS(config-service-ip:gslb-srvc2-port:tcp)# health-check http
ACOS(config-service-ip:gslb-srvc2-port:tcp)# exit
ACOS(config-service-ip:gslb-srvc2)# port 8080 tcp
ACOS(config-service-ip:gslb-srvc2-port:tcp)# health-check http
ACOS(config-service-ip:gslb-srvc2-port:tcp)# exit
ACOS(config-service-ip:gslb-srvc2)# port 8081 tcp
ACOS(config-service-ip:gslb-srvc2-port:tcp)# health-check http
ACOS(config-service-ip:gslb-srvc2-port:tcp)# exit
ACOS(config-service-ip:gslb-srvc2)# exit
```

The following commands enable a multi-port health check for the HTTP service “www” on service IP “gslb-srvc2” in GSLB zone “abc.com”:

```
ACOS(config)# gslb zone abc.com
ACOS(config-zone:abc.com)# service 15 www
ACOS(config-zone:abc.com-service:www)# health-check-port 80
ACOS(config-zone:abc.com-service:www)# health-check-port 8080
ACOS(config-zone:abc.com-service:www)# health-check-port 8081
ACOS(config-zone:abc.com-service:www)# exit
ACOS(config-zone:abc.com)# service 15 www
ACOS(config)# exit
```

Health Monitoring of Individual Service Ports

GSLB provides the ability to monitor the health of individual services running on a server port. A real port or service port under GSLB service IP can contain multiple services per application, such as, HTTP or FTP. Health Monitoring can be configured to check the health status of these individual services.

For instance, let's consider a particular service on a server port, like HTTP, is down. Then, only the HTTP service will be marked down. However, other health services on the same port, say FTP service will continue to function and receive the traffic. As the health check operates at the service level, the other active services on the same port continue to process the traffic they receive.

This feature can be implemented in the scenarios where:

- A single server port hosts multiple services and their health needs to be monitored individually to ensure service availability.
- A specific service experiencing issues is redirected to the backup location, while the other services continue to operate seamlessly.
- The GSLB controller can distribute traffic based on the health status of individual services to provide uninterrupted user experience.

The following topics are covered:

Key Considerations

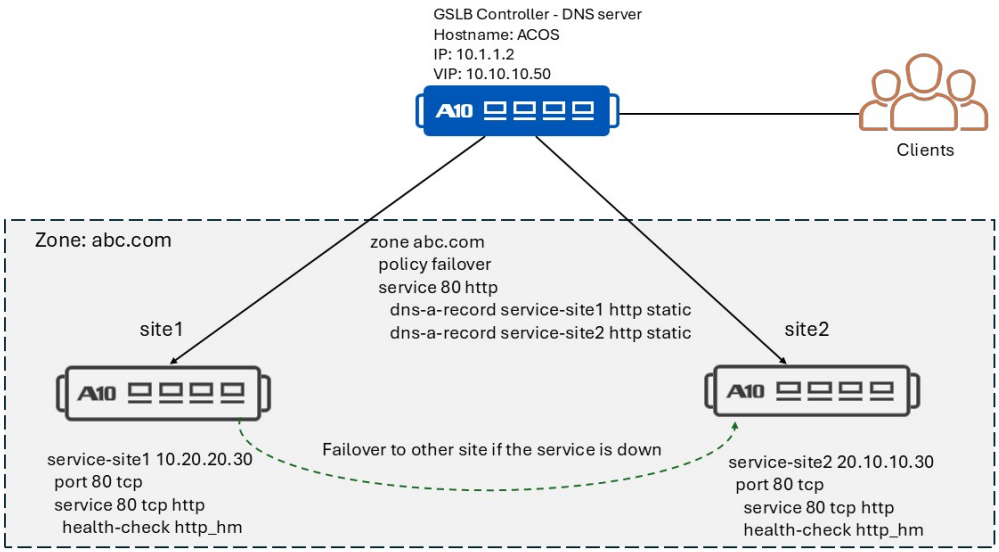
This section lists the key considerations to configure health checks for individual service ports and a failover mechanism in case the service ports fail the health check.

- Configure the real port (base port) or GSLB service IP port before configuring the service port.
- Configure the custom global health monitor first. Then, bind the custom health monitor to the individual service port.
- To configure failover across sites based on the service port health check, ensure that the port number and individual service name defined in the SLB server and/or GSLB service IP matches the service port number and individual service names defined in the associated GSLB zone.
- The same port with different protocols, such as, UDP or TCP cannot share the same service label.

Deployment

The following figure depicts the configuration of health checks for service ports across **site1** and **site2** and the resultant failover when the http service on **site1** is down and the same service on **site2** is up.

Figure 11 : Failover if service is down



CLI Configuration

This section describes the CLI configuration guidelines and examples for configuring health checks for service ports. The configuration indicates the identical ports and service ports in two sites with an associated health monitor. This configuration ensures that if the service port in one site is down, DNS traffic fails over to the same active service in another site.

1. Configure health monitor at the global configuration level. Define the health method object, assign the health monitor to the service port, and specify the action or response code expected.

```
ACOS(config)#health monitor http_hm
ACOS(config-health:monitor)#method http port 80 expect UP url GET /
```

   In this example, the http_hm monitors the health status of the HTTP service on port 80 and expects the UP status from the root URL “/”. If the status is not UP, the port is marked as down, and its service will failover.

2. Configure real servers and real ports. Configure services within real ports. Add

labels for services. Bind the configured health monitor to the individual service on the real port.

```
ACOS(config)#slb server rs1 10.10.10.11
ACOS(config-real server)#port 80 tcp
ACOS(config-real server-node port)#health-check http_hm
ACOS(config-real server-node port)#exit
ACOS(config-real server)#exit
ACOS(config)#slb server rs2 10.10.10.12
ACOS(config-real server)#port 80 tcp
ACOS(config-real server)#service 80 tcp http
ACOS(config-real server-node service)#health-check http_hm
```

In this example, the rs1 real server has the base port 80 tcp, which is bound to health check http_hm and the rs2 real server has the base port 80 tcp, service port 80 tcp http, which is also bound to health check http_hm.

3. Configure a virtual server, virtual port, and enable Global Server Load Balancing.

```
ACOS(config)#slb virtual-server vs1 10.10.10.50
ACOS(config-slb vserver)#port 53 dns-udp
ACOS(config-slb vserver-vport)#gslb-enable
```

4. Configure GSLB service IPs, ports, and service ports. Ensure that the port numbers and service port labels are matching to ensure a successful failover. Bind the configured health monitors to the service ports.

```
ACOS(config)#gslb service-ip service-site1 10.20.20.30
ACOS(config-service-ip:service-site1)#port 80 tcp
ACOS(config-service-ip:service-site1-port...)#service 80 tcp http
ACOS(config-service-ip:service-site1-service...)#health-check http_hm
ACOS(config-service-ip:service-site1-port...)#health-check-protocol-
disable
ACOS(config-service-ip:service-site1-port...)#exit
ACOS(config-service-ip:service-site1)#service 80 tcp ftp
ACOS(config-service-ip:service-site1-service...)#health-check http_hm
ACOS(config-service-ip:service-site1)#exit

ACOS(config)#gslb service-ip service-site2 20.10.10.30
ACOS(config-service-ip:service-site2)#port 80 tcp
ACOS(config-service-ip:service-site2-port...)#service80 tcp http
```

```
ACOS(config-service-ip:service-site2-service...)#health-check http_hm
ACOS(config-service-ip:service-site2-service...)#health-check-
protocol-disable
ACOS(config-service-ip:service-site2-service...)#exit
ACOS(config-service-ip:service-site2)#service 80 tcp ftp
ACOS(config-service-ip:service-site2-service...)#health-check http_hm
```

5. Configure GSLB settings.

```
ACOS(config)#gslb protocol enable controller
ACOS(config)#gslb protocol enable device
ACOS(config)#gslb protocol status-interval 5
```

6. Configure GSLB sites.

```
ACOS(config)#gslb site site1
ACOS(config-gslb site:site1)#slb-dev s1 10.20.20.1
ACOS(config-gslb site:site1-slb dev:s1)#vip-server service-site1
ACOS(config-gslb site:site1-slb dev:s1)#exit

ACOS(config)#gslb site site2
ACOS(config-gslb site:site2)#slb-dev s2 20.10.10.2
ACOS(config-gslb site:site2-slb dev:s2)#vip-server service-site2
```

7. Configure a GSLB policy with the following settings.

```
ACOS(config)#gslb policy failover
ACOS(config-policy:failover)#metric-order health-check
ACOS(config-policy:failover)# dns active-only
ACOS(config-policy:failover)#dns server
```

The `dns-server` command enables the ACOS device to act as a DNS server. The `dns-active only` command checks for an active service to serve DNS records. The health check metric ensures that the health status of services is being monitored.

8. Configure a GSLB zone. Bind the configured policy. Add the base port and service labels matching the ones defined under port configuration or GSLB service IP configuration.

```
ACOS(config)#gslb zone abc.com
ACOS(config-zone:abc.com)#policy failover
ACOS(config-zone:abc.com)#service 80 http
```

```
ACOS(config-zone:abc.com-service:http)#dns-a-record service-site1 http
static
ACOS(config-zone:abc.com-service:http)#dns-a-record service-site2 http
static
```

As per the above configuration, if the client sends a dig request to the abc.com zone, both, **service-site 1** and **service-site 2** will be seen as available to serve requests. If the http service on **site1** goes down, the health check will indicate the status. In this case, only the active service on **site 2** will be seen. Based on the configuration in the failover policy, as `dns-active-only` will check for active services to process requests, the traffic will failover to **site 2**. In the meanwhile, the other active services under port 80 in **site1**, such as, ftp, will continue to serve DNS requests.

Show Command

The **`show gslb site`** command displays the status of ports. The following example indicates the state of the various services.

```
ACOS#show gslb site Site1
Site         Device/server    VIP       Service           State
  Hits
-------------------------------------------------------------------------
-------------
Site1        Device1 (device) 2.1.1.10                    AllUp
  20
             1.2.2.2                    80:TCP:http       Up

                                        53:UDP:dns        Up

                              2.1.1.11  80:TCP:ftp        Up
  0
             serverB (server)                             Up
  10
             3.1.1.10                   80:TCP:http       Up
                                        53:UDP            Up
                                        80:TCP:ftp        Down
  0
```

Limitations

Configuring health checks for individual service ports has the following limitations:

- Does not support dynamic real servers and SLB server port range.
- Does not support GSLB protocol health check.
- The `show slb server` command does not show ports with service labels.
- The SLB server service port label can only be used with GSLB.

Application Groups

The following topics are covered:

Site persistence

Service groups can be configured for persistence and dependency when clients request different services, such as POP, IMAP, and SMTP. With site persistence, requests for different services from the same client will be directed to the same server site. Configuring dependency creates failover grouping. When one service is down on a site, the site is flagged as down for all services.

When persistence is enabled, ACOS ensures that requests for different services are sent to the same site.You configure application groups so that certain services are grouped together. When a client requests those services, they are always directed to the same site. For example, if a user requests the WWW service, and then later requests the Secure WWW service, then persistence ensures that both requests go to the same site.

Configuring dependency ensures that when one service is down on a site, ACOS marks all services as unusable for that site. Client traffic is then redirected to a site where persistence can be maintained for all services. For example, a service group may consistent of email protocols. If POP service is down, then all other services, such as IMAP and SMTP, are also marked as down.

Persistence and dependency can be configured individually or together. In both cases, a service should be configured in only one service-group.

Configuring Persistence and Dependency

To configure GSLB application groups with persistence and failover dependency, do the following:

1. Configure the virtual servers or services with the appropriate port and protocol.
2. Define the GSLB data centers or sites.
    a. Configure the devices in the data centers, as well as the virtual servers or services in the data centers.
3. Configure the applications and logical components in the system, such as the FQDN.
4. Group the defined applications together and then enable persistence and dependency

Configuring Persistence and Dependency (CLI Procedure)

To configure GSLB application groups with persistence and failover dependency, enter the following commands at the GSLB service-group configuration level:

```
persistent site
dependency site
```

The “persistent site” command can specify an IPv4 mask, IPv6 mask length, or aging-time that determines the period after which persistence is no longer maintained to a server when there is no traffic from the client (default aging-time is 5 minutes). Aging time is refreshed when the site receives a request from the client.

Configuring Persistence and Dependency (CLI Example)

This example configures two GSLB sites, one for New York and one for San Francisco. These sites will support the WWW and Secure WWW applications. Persistence and dependency are configured for these GSLB sites.

1. These commands configure GSLB data centers in New York and San Francisco. The virtual servers are grouped into data centers. Each data center has four servers with port 80 configured (vip1 - vip4), and four servers with port 443 configured (vip5 - vip8). The sites reference the servers through GSLB service-ip assignments that are not included in the example (gslb service-ip).

```
ACOS(config)# gslb site NY
ACOS(config-gslb site:NY)# slb-dev NY-slb-device1 11.11.11.11
ACOS(config-gslb site:NY-slb dev:NY-slb-d...)# vip-server vip1
ACOS(config-gslb site:NY-slb dev:NY-slb-d...)# vip-server vip2
ACOS(config-gslb site:NY-slb dev:NY-slb-d...)# vip-server vip5
ACOS(config-gslb site:NY-slb dev:NY-slb-d...)# vip-server vip6
ACOS(config-gslb site:NY-slb dev:NY-slb-d...)# exit
```

```
ACOS(config-gslb site:NY)# exit
ACOS(config)# gslb site SF
ACOS(config-gslb site:SF)# slb-dev SF-slb-device1 12.12.12.12
ACOS(config-gslb site:SF-slb dev:SF-slb-d...)# vip-server vip3
ACOS(config-gslb site:SF-slb dev:SF-slb-d...)# vip-server vip4
ACOS(config-gslb site:SF-slb dev:SF-slb-d...)# vip-server vip7
ACOS(config-gslb site:SF-slb dev:SF-slb-d...)# vip-server vip8
ACOS(config-gslb site:SF-slb dev:SF-slb-d...)# exit
ACOS(config-gslb site:SF)# exit
```

2. These commands define the www.example.com and secure.example.com FQDNs. They assign the WWW service to virtual servers 1 through 4, and the Secure WWW service to virtual servers 5 through 8.

```
ACOS(config)# gslb zone example.com
ACOS(config-zone:example.com)# service 80 www
ACOS(config-zone:example.com-service:www)# dns-a-record vip1 static
ACOS(config-zone:example.com-service:www)# dns-a-record vip2 static
ACOS(config-zone:example.com-service:www)# dns-a-record vip3 static
ACOS(config-zone:example.com-service:www)# dns-a-record vip4 static
ACOS(config-zone:example.com-service:www)# exit
ACOS(config-zone:example.com)# service 443 secure
ACOS(config-zone:example.com-service:sec...)# dns-a-record vip5 static
ACOS(config-zone:example.com-service:sec...)# dns-a-record vip6 static
ACOS(config-zone:example.com-service:sec...)# dns-a-record vip7 static
ACOS(config-zone:example.com-service:sec...)# dns-a-record vip8 static
ACOS(config-zone:example.com-service:sec...)# exit
ACOS(config-zone:example.com))# exit
```

3. The next commands group the applications (WWW and Secure WWW) together and configure dependency for failover grouping, as well as persistence with an aging-time of 10 minutes.

```
ACOS(config)# gslb service-group website
ACOS(config-svc group:website)# member www.example.com
ACOS(config-svc group:website)# member secure.example.com
ACOS(config-svc group:website)# persistent site aging-time 10
ACOS(config-svc group:website)# dependency site
ACOS(config-svc group:website)# exit
```

Configuring GSLB through the GUI

This chapter provides configuration examples for Global Server Load Balancing (GSLB). These examples implement a basic GSLB deployment. The examples assume that the default GSLB policy is used, without any changes to the policy settings.

Steps consist of an action and the resulting GUI response. For example, the following line instructs the user to select ADC >> SLB from the main menu, which opens the SLB Virtual Server Roster panel in the GUI:

- Select ADC >> SLB (primary menu)
- Open SLB Virtual Server Roster

The following topics are covered:

Proxy Mode (Scenario 1)

Scenario 1: Proxy Mode for the description and equivalent CLI implementation.

Changing the Hostname

1. Select **System >> Settings (primary menu)** Open Access Control panel.
2. Select DNS (secondary menu Open Configure DNS panel.
   - Data Entry: Open Configure DNS panel.
   - Hostname: ACOS-1
3. Click **Update DNS**.

Creating the VIP

1. Create the SLB Servers by clicking **ADC >> SLB (primary menu)**, open SLB Virtual

Server roster.

2. Select Servers (secondary menu) Open SLB Servers Roster.
3. Click **Create** and add the following information.
   - Data Entry: Create Server panel
   - Name: ACOS-11
   - Host: 10.10.0.53
   - Port Section: Click **Create** Open Update Port panel.
   - Data Entry: Update Port panel
   - Port Number: 53
   - Protocol: TCP
4. Click **Create** Return to SLB Servers Roster.
5. Select Service Groups (secondary menu). Open Service Groups roster.
6. Click **Create**. Open Create Service Group panel.
   - Data Entry: Create Service Group panel
   - Name: DNS-GP1
   - Protocol: TCP
   - Member section: Click Create button Open Create Member panel
   - Data Entry: Create Member panel
   - Choose Creation Type: (Existing Server) Existing Server
   - Server: (drop down) ACOS-11
   - Port: 53
7. Click **Create**. Returns to Update Service Group panel.
8. Select Virtual-Servers (secondary menu). Open SLB Virtual Servers roster.
9. Click **Create**. Open SLB Create Virtual Server panel.
   - Data Entry: SLB Create Virtual Server panel
   - Name: DNS1

- IP Address: 10.10.0.100
- Virtual Port section: Click Create button Opens SLB Create Virtual Port panel
- Data Entry: SLB Create Virtual Port panel
- Protocol: dns-tcp
- Port: 53
- Service Group: (Drop Down): DNS-GRP1
- Expand General Fields section
- Data Entry: General Fields section
- GSLB Enable: (checkbox) select

10. Click **Create**. Return to SLB Update Virtual Server panel.
11. Click **Update**. Return to SLB Virtual Servers roster.

Configuring GSLB Service IP (LANE)

1. Select **GSLB >> Service IPs**, Open GSLB Service IP Roster.
2. Click **Create** to open GSLB Create Service IP panel.
   - Data Entry: GSLB Create Service IP panel
   - Service IP Name: LANE
   - IP Address: 10.10.1.58
   - Service IP Ports section: Click Create button Opens GSLB Create Service IPs Ports panel
   - Data Entry: GSLB Create Service IPs Ports panel
   - Port: 80
   - Protocol: TCP
3. Click **Create** to return to GSLB Create Service IPs panel.
   - Service IP Ports section: Click Create button . This opens GSLB Create Service IPs Ports panel
   - Data Entry: Create Service IPs panel

- Port: 25
- Protocol: TCP

4. Click **Create**. Return to GSLB Create Service IPs panel.
5. Click **Update**. Return to GSLB Service IP Roster.

Configuring GSLB Service IP (BENTON)

1. Click Create. Open GSLB Create Service IP panel.
   - Data Entry: Create Service IP panel
   - Service IP Name: BENTON
   - IP Address: 10.10.2.68
   - Service IP Ports section: Click Create button Opens GSLB Create Service IPs Ports panel
   - Data Entry: Create Service IPs Ports panel
   - Port: 80
   - Protocol: TCP
2. Click **Create**. Return to GSLB Create Service IPs panel
3. Click **Create**. Opens GSLB Create Service IPs Ports panel.
   - Service IP Ports section: Click Create. Opens GSLB Create Service IPs Ports panel.
   - Data Entry: Create Service IPs panel
   - Port: 25
   - Protocol: TCP
4. Click **Create**. Return to GSLB Create Service IPs panel.
5. Click **Update**. Return to GSLB Service IP Roster.

Configuring GSLB Sites (EUGENE and CORVALLIS)

1. Select **GSLB >> Sites**. Open GSLB Sites Roster
2. Click **Create.** Open GSLB Create Sites panel.

- Data Entry: GSLB Sites panel
- Name: EUGENE
- IP Server (drop down): LANE – Click Add button

3. Click **Create**. Returns to GSLB Sites Roster
4. Click **Create**. Open GSLB Create Sites panel.
   - Data Entry: GSLB Sites panel
   - Name: CORVALLIS
   - IP Server (drop down): BENTON – Click Add button.
5. Click **Create**. Returns to GSLB Sites Roster

Configuring GSLB Policy (HELIUM)

1. Select **GSLB >> Policies**. Opens GSLB Policies Roster.
2. Click **Create**. Opens GSLB Create Policies panel.
   - Data Entry: GSLB Create Policies panel
   - Name: HELIUM
   - Expand DNS Options section
   - Data Entry: GSLB Create Policies panel
   - Server Mode: (checkbox) de-select
3. Click **Create**. Returns to GSLB Policies Roster

Creating GSLB FQDN (www.a10-brown.com)

1. Select **GSLB >> FQDN**. Opens GSLB FQDNs Roster.
2. Click **Create**. Opens GSLB Create FQDNs panel.
   - Data Entry: GSLB Create FQDNs panel
   - GSLB Zone: a10-brown.com
   - Service: www
   - Zone Policy: (drop down) HELIUM
   - Port: 80
3. Click **Create**. Returns to GSLB FQDNs Roster

Creating GSLB FQDN (mail.a10-brown.com)

1. Click **Create**. Opens GSLB Create FQDNs panel.
   - Data Entry: GSLB Create FQDNs panel
   - Existing Zone: a10-brown.com
   - Service: mail
   - Port: 25
2. Click **Create**. Returns to GSLB FQDNs Roster.

Configuring GSLB FQDN DNS Records (www.a10-brown.com)

1. Expand a10-brown.com (zone column) Reveals FQDNs for a10-brown.com zone.
2. Click **Edit** text on www.a10-brown.com. Opens GSLB Update FQDNs panel.
   - DNS Records section: Click Create button Opens GSLB Create DNS Record panel
   - Data Entry: GSLB Create DNS Record panel
   - Record Type: (Drop-Down) Service A
   - Service IP Name: (Drop-Down) LANE
   - Static: (checkbox) select
3. Click **Create**. Returns to GSLB Update FQDNs panel.
   - DNS Records section: Click Create button Opens GSLB Create DNS Record panel
   - Data Entry: GSLB Create DNS Record panel
   - Record Type: (Drop-Down) Service A
   - Service IP Name: (Drop-Down) BENTON
   - Static: (checkbox) select
4. Click **Create**. Returns to Update GSLB FQDNs Roster
5. Click **Update**. Returns to GSLB FQDNs Roster.

Configuring GSLB FQDN DNS Records (mail.a10-brown.com)

1. Expand a10-brown.com (zone column). Reveals FQDNs for a10-brown.com zone.

2. Click **Edit** text on mail.a10-brown.com. Opens GSLB Update FQDNs panel.
   - DNS Records section: Click Create. Opens GSLB Create DNS Record panel.
   - Data Entry: GSLB Create DNS Record panel
   - Record Type: (Drop-Down) SERVICE A
   - Service IP Name: (Drop-Down) LANE
   - Static: (checkbox) select
3. Click **Create**. Returns to GSLB Update FQDNs panel.
   - DNS Records section: Click Create button Opens GSLB Create DNS Record panel
   - Data Entry: GSLB Create DNS Record panel
   - Record Type: (Drop-Down) SERVICE A
   - Service IP Name: (Drop-Down) BENTON
   - Static: (checkbox) select
4. Click **Create**. Returns to GSLB FQDNs Roster.
5. Click **Update**. Returns to GSLB FQDNs Roster.

Server Mode Group (Scenario 2)

Scenario 2: Server Mode for the description and equivalent CLI implementation.

Changing the Hostname

1. Select **System >> Settings (primary menu)**. Open Access Control panel.
2. Select DNS (secondary menu). Open Configure DNS panel.
   - Data Entry: Open Configure DNS panel
   - Hostname: ACOS-2
3. Click **Update DNS**.

Creating the VIP

1. SLB Service Group configuration, required in step 4, is not featured in this

example. Refer to the ADC Configuration Guide.

2. Select **ADC >> SLB** (primary menu). Open SLB Virtual Server Roster.
3. Select Virtual-Servers (secondary menu). Open SLB Virtual Servers roster.
4. Click **Create**. Open SLB Create Virtual Server panel.
   - Data Entry: SLB Create Virtual Server panel
   - Name: DNS2
   - IP Address: 10.20.0.53
   - Virtual Port section: Click Create button Opens SLB Create Virtual Port panel
   - Data Entry: SLB Create Virtual Port panel
   - Protocol: dns-tcp
   - Port: 53
   - Service Group: (Drop Down): DNS-GROUP
5. Expand **General Fields** section.
   - Data Entry: General Fields section
   - GSLB Enable: (checkbox) select
6. Click **Create**. Return to SLB Update Virtual Server panel.
7. Click **Update**. Return to SLB Virtual Servers roster.

Configuring GSLB Service IP (PIERCE)

1. Select **GSLB >> Service IPs**. Open GSLB Service IP Roster.
2. Click **Create**. Open GSLB Create Service IP panel.
   - Data Entry: GSLB Create Service IPs panel
   - Service IP Name: PIERCE
   - IP Address: 10.20.1.58
   - Service IP Ports section: Click Create button Opens GSLB Create Service IPs Ports panel
   - Data Entry: GSLB Create Service IPs Ports panel

- Port: 80
- Protocol: TCP

3. Click **Create**. Return to GSLB Create Service IPs panel.
   - Service IP Ports section: Click Create button Opens GSLB Create Service IPs Ports panel.
   - Data Entry: Create Service IPs panel
   - Port: 25
   - Protocol: TCP
4. Click **Create**. Return to GSLB Create Service IPs panel.
5. Click **Update**. Return to GSLB Service IP Roster.

Configuring GSLB Service IP (KING)

1. Click **Create**. Open GSLB Create Service IP panel.
   - Data Entry: Create Service IP panel
   - Service IP Name: KING
   - IP Address: 10.20.2.68
   - Service IP Ports section: Click Create button Opens GSLB Create Service IPs Ports panel
   - Data Entry: Create Service IPs Ports panel
   - Port: 80
   - Protocol: TCP
2. Click **Create**. Return to GSLB Create Service IPs panel.
   - Service IP Ports section: Click Create button Opens GSLB Create Service IPs Ports panel
   - Data Entry: Create Service IPs panel
   - Port: 25
   - Protocol: TCP
3. Click **Create**. Return to GSLB Create Service IPs panel.
4. Click **Update**. Return to GSLB Service IP Roster.

Configuring GSLB Sites (TACOMA and BELLEVUE)

1. Select **GSLB >> Sites**. Open GSLB Sites Roster.
2. Click **Create**. Open GSLB Create Sites panel.
   - Data Entry: GSLB Sites panel
   - Name: TACOMA
   - IP Server (drop down): PIERCE – Click Add button
   - Click Create button Returns to GSLB Sites Roster
   - Click Create button Open GSLB Create Sites panel
   - Data Entry: GSLB Sites panel
   - Name: BELLEVUE
   - IP Server (drop down): KING – Click Add button
3. Click **Create**. Returns to GSLB Sites Roster.

Configuring GSLB Policy (BORON)

1. Select **GSLB >> Policies**. Opens GSLB Policies Roster
2. Click **Create**. Opens GSLB Create Policies panel.
   - Data Entry: GSLB Create Policies panel
   - Name: BORON
   - Expand DNS Options section
   - Data Entry: GSLB Create Policies panel
   - Server Mode: (checkbox) select
   - Authoritative Mode: (checkbox) select
3. Click **Create**. Returns to GSLB Policies Roster.

Creating GSLB FQDN (www.a10-blue.com)

1. Select **GSLB >> FQDN**. Opens GSLB FQDNs Roster.
2. Click **Create**. Opens GSLB Create FQDNs panel.

- Data Entry: GSLB Create FQDNs panel
- GSLB Zone: a10-blue.com
- Service: www
- Zone Policy: (drop down) BORON
- Port: 80

3. Click **Create**. Returns to GSLB FQDNs Roster

Creating GSLB FQDN (mail.a10-blue.com)

1. Click **Create**. Opens GSLB Create FQDNs panel.
   - Data Entry: GSLB Create FQDNs panel
   - Existing Zone: (drop down) a10-blue.com
   - Service: mail
   - Port: 25
2. Click **Create**. Returns to GSLB FQDNs Roster.

Configuring GSLB FQDN DNS Records (www.a10-blue.com)

1. Expand a10-blue.com (zone column) Reveals FQDNs for a10-blue.com zone.
2. Click **Edit** text on www.a10-blue.com Opens GSLB Update FQDNs panel.
   - DNS Records section: Click Create button Opens GSLB Create DNS Record panel.
   - Data Entry: GSLB Create DNS Record panel
   - Record Type: (Drop-Down) Service A
   - Service IP Name: (Drop-Down) PIERCE
   - Static: (checkbox) select
3. Click **Create**. Returns to GSLB Update FQDNs panel.
   - DNS Records section: Click Create button Opens GSLB Create DNS Record panel
   - Data Entry: GSLB Create DNS Record panel
   - Record Type: (Drop-Down) Service A

- Service IP Name: (Drop-Down) KING
- Static: (checkbox) select

4. Click **Create**. Returns to Update GSLB FQDNs Roster.
5. Click **Update**. Returns to GSLB FQDNs Roster.

Configuring GSLB FQDN DNS Records (mail.a10-blue.com)

1. Expand a10-blue.com (zone column) Reveals FQDNs for a10-blue.com zone
2. Click **Edit** text on mail.a10-blue.com Opens GSLB Update FQDNs panel.
   - DNS Records section: Click Create button Opens GSLB Create DNS Record panel.
   - Data Entry: GSLB Create DNS Record panel
   - Record Type: (Drop-Down) SERVICE A
   - Service IP Name: (Drop-Down) PIERCE
   - Static: (checkbox) select
3. Click **Create**. Returns to GSLB Update FQDNs panel.
   - DNS Records section: Click Create. Opens GSLB Create DNS Record panel.
   - Data Entry: GSLB Create DNS Record panel
   - Record Type: (Drop-Down) SERVICE A
   - Service IP Name: (Drop-Down) KING
   - Static: (checkbox) select
4. Click **Create**. Returns to GSLB FQDNs Roster.
5. Click **Update**. Returns to GSLB FQDNs Roster.

Controllers and Devices (Scenario 3)

Scenario 4: Controllers and Site Devices for the scenario description and equivalent CLI implementation.

Changing the Hostname

1. Select **System >> Settings** (primary menu). Open Access Control panel.

2. Select **DNS** (secondary menu). Open Configure DNS panel.
   - Data Entry: Open Configure DNS panel
   - Hostname: ACOS-3
3. Click **Update DNS**.

Creating the VIP

1. SLB Service Group configuration, required in step 4, is not featured in this example. Refer to the ADC Configuration Guide.
2. Select **ADC >> SLB** (primary menu). Open SLB Virtual Server Roster.
3. Select Virtual-Servers (secondary menu). Open SLB Virtual Servers roster.
4. Click **Create**. Open SLB Create Virtual Server panel.
   - Data Entry: SLB Create Virtual Server panel
   - Name: DNS3
   - IP Address: 10.30.0.53
   - Virtual Port section: Click Create button Opens SLB Create Virtual Port panel
   - Data Entry: SLB Create Virtual Port panel
   - Protocol: dns-tcp
   - Port: 53
   - Service Group: (Drop Down): DNS-GROUP
5. Expand **General Fields** section.
   - Data Entry: General Fields section
   - GSLB Enable: (checkbox) select
6. Click **Create**. Return to SLB Update Virtual Server panel.
7. Click **Update**. Return to SLB Virtual Servers roster.

Configuring GSLB Service IP (PIMA)

1. Select **GSLB >> Service IPs**. Open GSLB Service IP Roster.
2. Click **Create**. Open GSLB Create Service IP panel.

- Data Entry: GSLB Create Service IPs panel.
- Service IP Name: PIMA
- IP Address: 10.20.1.58
- Service IP Ports section: Click Create button Opens GSLB Create Service IPs Ports panel
- Data Entry: GSLB Create Service IPs Ports panel
- Port: 80
- Protocol: TCP

3. Click **Create**. Return to GSLB Create Service IPs panel.
   - Service IP Ports section: Click Create button Opens GSLB Create Service IPs Ports panel
   - Data Entry: Create Service IPs panel
   - Port: 25
   - Protocol: TCP
4. Click **Create**. Return to GSLB Create Service IPs panel.
5. Click **Update**. Return to GSLB Service IP Roster.

Configuring GSLB Service IP (COCONINO)

1. Click **Create**. Open GSLB Create Service IP panel.
   - Data Entry: Create Service IP panel
   - Service IP Name: COCONINO
   - IP Address: 10.20.2.68
   - Service IP Ports section: Click Create button Opens GSLB Create Service IPs Ports panel
   - Data Entry: Create Service IPs Ports panel
   - Port: 80
   - Protocol: TCP
2. Click **Create**. Return to GSLB Create Service IPs panel.
3. Click **Create**. Opens GSLB Create Service IPs Ports panel.

- Service IP Ports section: Click Create button Opens GSLB Create Service IPs Ports panel
- Data Entry: Create Service IPs panel
- Port: 25
- Protocol: TCP

4. Click **Create**. Return to GSLB Create Service IPs panel.
5. Click **Update.** Return to GSLB Service IP Roster.

Configuring GSLB Sites (TUCSON and FLAGSTAFF)

1. Select **GSLB >> Sites**. Open GSLB Sites Roster.
2. Click **Create**. Open GSLB Create Sites panel.
   - Data Entry: GSLB Sites panel
   - Name: TUCSON
   - SLB Devices section: Click Create button Open Create SLB Device pane
   - Data Entry: Create SLB Device panel
   - Device Name: ACOS-31
   - IP Address 10.30.0.131
   - VIP Server LIst: (drop down) PIMA – Click Add button
3. Click **Create**. Returns to GSLB Sites Roster.
4. Click **Create**. Open GSLB Create Sites panel.
   - Data Entry: GSLB Sites panel
   - Name: FLAGSTAFF
   - SLB Devices section: Click Create button Open Create SLB Device pane
   - Data Entry: Create SLB Device panel
   - Device Name: ACOS-32
   - IP Address 10.30.0.132
   - VIP Server LIst: (drop down) COCONINO – Click Add button
5. Click **Create**. Returns to GSLB Sites Roster.

Configuring GSLB Policy (SODIUM)

1. Select **GSLB >> Policies**. Opens GSLB Policies Roster.
2. Click **Create**. Opens GSLB Create Policies panel.
   - Data Entry: GSLB Create Policies panel
   - Name: SODIUM
   - Expand DNS Options section
   - Data Entry: GSLB Create Policies panel
   - Server Mode: (checkbox) select
   - Authoritative Mode: (checkbox) select
3. Click **Create**. Returns to GSLB Policies Roster.

Creating GSLB FQDN (www.a10-black.com)

1. Select **GSLB >> FQDN**. Opens GSLB FQDNs Roster.
2. Click **Create**. Opens GSLB Create FQDNs panel.
   - Data Entry: GSLB Create FQDNs panel
   - GSLB Zone: a10-black.com
   - Service: www
   - Zone Policy: (drop down) SODIUM
   - Port: 80
3. Click **Create**. Returns to GSLB FQDNs Roster.

Creating GSLB FQDN (mail.a10-black.com)

1. Click **Create**. Opens GSLB Create FQDNs panel.
   - Data Entry: GSLB Create FQDNs panel
   - Existing Zone: (drop down) a10-black.com
   - Service: mail
   - Port: 25
2. Click **Create**. Returns to GSLB FQDNs Roster.

Configuring GSLB FQDN DNS Records (www.a10-black.com)

1. Expand a10-black.com (zone column) Reveals FQDNs for a10-black.com zone
2. Click **Edit** text on www.a10-black.com Opens GSLB Update FQDNs panel.
   - DNS Records section: Click Create button Opens GSLB Create DNS Record panel
   - Data Entry: GSLB Create DNS Record panel
   - Record Type: (Drop-Down) Service A
   - Service IP Name: (Drop-Down) PIMA
   - Static: (checkbox) select
3. Click **Create**. Returns to GSLB Update FQDNs panel.
   - DNS Records section: Click Create button Opens GSLB Create DNS Record panel
   - Data Entry: GSLB Create DNS Record panel
   - Record Type: (Drop-Down) Service A
   - Service IP Name: (Drop-Down) COCONINO
   - Static: (checkbox) select
4. Click **Create**. Returns to Update GSLB FQDNs Roster.
5. Click **Update**. Returns to GSLB FQDNs Roster.

Configuring GSLB FQDN DNS Records (mail.a10-black.com)

1. Expand a10-black.com (zone column). Reveals FQDNs for a10-black.com zone.
2. Click **Edit** text on mail.a10-black.com. Opens GSLB Update FQDNs panel.
   - DNS Records section: Click Create button Opens GSLB Create DNS Record panel.
   - Data Entry: GSLB Create DNS Record panel
   - Record Type: (Drop-Down) SERVICE A
   - Service IP Name: (Drop-Down) PIMA
   - Static: (checkbox) select
3. Click **Create**. Returns to GSLB Update FQDNs panel.

- DNS Records section: Click Create button Opens GSLB Create DNS Record panel
- Data Entry: GSLB Create DNS Record panel
- Record Type: (Drop-Down) SERVICE A
- Service IP Name: (Drop-Down) COCONINO
- Static: (checkbox) select

4. Click **Create**. Returns to GSLB FQDNs Roster.

Enabling the GSLB Protocol

Select GSLB >> Global Opens GSLB Update Global (System) Panel

Select Protocol Opens GSLB Update Global (Protocol) panel

Data Entry: Update GSLB Global (Protocol) panel

Enable as GSLB controller: (checkbox) select

Click Update GSLB Global Protocol button

Device ACOS-31: Changing the Hostname

1. Select **System >> Settings** (primary menu). Open Access Control panel.
2. Select DNS (secondary menu). Open Configure DNS panel.
   - Data Entry: Open Configure DNS panel
   - Hostname: ACOS-31
3. Click **Update DNS**.

Device ACOS-31: Creating the VIP

1. Select **ADC >> SLB** (primary menu). Open SLB Virtual Server roster.
2. Select Servers (secondary menu). Open SLB Servers Roster.
3. Click **Create**. Open Create Server panel.
   - Data Entry: Create Server panel
   - Name: ACOS-31P
   - Host: 10.1.1.58

- Port Section: Click Create button Open Update Port panel
- Data Entry: Update Port panel
- Port Number: 53
- Protocol: TCP

4. Click **Create**.
5. Create Service group. Select Service Groups (secondary menu). Open Service Groups roster.
6. Click **Create**. Open Create Service Group panel.
   - Data Entry: Create Service Group panel
   - Name: DNS-31P
   - Protocol: TCP
   - Member section: Click Create button Open Create Member panel
   - Data Entry: Create Member panel
   - Choose Creation Type: (Radio button) Existing Server
   - Server: (drop down) ACOS-31P
   - Port: 53
7. Click **Create**. Returns to Update Service Group panel
8. Create virtual server. Select Virtual-Servers (secondary menu). Open SLB Virtual Servers roster.
9. Click **Create**. Open SLB Create Virtual Server panel.
   - Data Entry: SLB Create Virtual Server panel
   - Name: DNS-31
   - IP Address: 10.40.0.141
   - Virtual Port section: Click Create button Opens SLB Create Virtual Port panel
   - Data Entry: SLB Create Virtual Port panel
   - Protocol: dns-tcp

- Port: 53
- Service Group: (Drop Down): DNS-GROUP

10. Expand **General Fields** section.
    - Data Entry: General Fields section
    - GSLB Enable: (checkbox) select
11. Click **Create**. Return to SLB Update Virtual Server panel.
12. Click **Update**. Return to SLB Virtual Servers roster.

Device ACOS-31: Enabling the GSLB Protocol

1. Select **GSLB >> Global**. Opens GSLB Update Global (System) Panel.
2. Select Protocol Opens GSLB Update Global (Protocol) panel.
    - Data Entry: Update GSLB Global (Protocol) panel
    - Enable as site device: (checkbox) select
3. Click **Update**.

Device ACOS-32: Changing the Hostname

1. Select **System >> Settings** (primary menu). Open Access Control panel
2. Select DNS (secondary menu). Open Configure DNS panel.
    - Data Entry: Open Configure DNS panel
    - Hostname: ACOS-32
3. Click **Update DNS**.

Device ACOS-32: Creating the VIP

1. SLB Service Group configuration, required in step 4, is not featured in this example. Refer to the ADC Configuration Guide.
2. Create the SLB Server, **ADC >> SLB** (primary menu.) Open SLB Virtual Server roster.
3. Select Servers (secondary menu). Open SLB Servers Roster.
4. Click **Create**. Open Create Server panel.

- Data Entry: Create Server panel
- Name: ACOS-32P
- Host: 10.1.2.68
- Port Section: Click Create button Open Update Port panel
- Data Entry: Update Port panel
- Port Number: 53
- Protocol: TCP

5. Click **Create**.
6. Creating the SLB Service Group, select Service Groups (secondary menu). Open Service Groups roster.
7. Click **Create**. Open Create Service Group panel.
   - Data Entry: Create Service Group panel
   - Name: DNS-32P
   - Protocol: TCP
   - Member section: Click Create button Open Create Member panel
   - Data Entry: Create Member panel
   - Choose Creation Type: (Radio button) Existing Server
   - Server: (drop down) ACOS-32P
   - Port: 53
8. Click **Create**. Returns to Update Service Group panel.
9. Creating the SLB Virtual Server, select Virtual-Servers (secondary menu) Open SLB Virtual Servers roster.
10. Click **Create**. Open SLB Create Virtual Server panel.
    - Data Entry: SLB Create Virtual Server panel
    - Name: DNS-32
    - IP Address: 10.40.0.142
    - Virtual Port section: Click Create button Opens SLB Create Virtual Port panel

- Data Entry: SLB Create Virtual Port panel
- Protocol: dns-tcp
- Port: 53
- Service Group: (Drop Down): DNS-32P

11. Expand **General Fields** section.
    - Data Entry: General Fields section
    - GSLB Enable: (checkbox) select
12. Click **Create**. Return to SLB Update Virtual Server panel.

Device ACOS-32: Enabling the GSLB Protocol

1. Select **GSLB >> Global**. Opens GSLB Update Global (System) Panel.
2. Select Protocol. Opens GSLB Update Global (Protocol) panel.
    - Data Entry: Update GSLB Global (Protocol) panel
    - Enable as site device: (checkbox) select
3. Click **Update**.

Configuring Controller-Based Metrics

Configuring GSLB Controller-Based Metrics (CLI Example) for the scenario description and equivalent CLI implementation.

Changing the Hostname

1. Select System >> Settings (prmary menu). Open Access Control panel
2. Select DNS (secondary menu) Open Configure DNS panel.
    - Data Entry: Open Configure DNS panel
    - Hostname: ACOS-1
    - IP Address: 10.10.1.58
3. Click **Update DNS**.

Configuring GSLB Service IPs (NYE and WASHOE)

1. Select **GSLB >> Service IPs**. Open GSLB Service IP Roster.
2. Click **Create**. Open GSLB Create Service IP panel.
   - Data Entry: Create Service IP panel
   - Service IP Name: NYE
   - IP Address: 10.1.1.10
   - Service IP Ports section: Click Create button Opens GSLB Create Service IPs Ports panel
   - Data Entry: Create Service IPs Ports panel
   - Port: 80
   - Protocol: TCP
3. Click **Create**. Return to GSLB Create Service IPs panel.
4. Click **Update**. Return to GSLB Service IP Roster.
5. Click **Create**. Open GSLB Create Service IP panel.
   - Data Entry: Create Service IP panel
   - Service IP Name: WASHOE
   - IP Address: 20.1.1.20
   - Service IP Ports section: Click Create button Opens GSLB Create Service IPs Ports panel
   - Data Entry: Create Service IPs Ports panel
   - Port: 80
   - Protocol: TCP
6. Click **Create**. Return to GSLB Create Service IPs panel.
7. Click **Update**. Return to GSLB Service IP Roster.

Configuring GSLB Sites (ELY and RENO)

1. Select **GSLB >> Sites**. Open GSLB Sites Roster.
2. Click **Create**. Open GSLB Create Sites panel.

- Data Entry: GSLB Sites panel
- Name: ELY
- IP Server (drop down): NYE – Click Add button
- Click Create button Returns to GSLB Sites Roster
- Click Create button Open GSLB Create Sites panel
- Data Entry: GSLB Sites panel
- Name: RENO
- IP Server (drop down): WASHOE – Click Add button

3. Click **Create**. Returns to GSLB Sites Roster.

Configuring GSLB Policy (RHOMBUS)

1. Select **GSLB >> Policies**. Opens GSLB Policies Roster.
2. Click **Create**. Opens GSLB Create Policies panel.
   - Data Entry: GSLB Create Policies panel
   - Name: default
   - Round Robin: (checkbox) de-select
   - Metrics – Active RDT: (checkbox) select
   - Expand Active RDT section
   - Data Entry: Active RDT section
   - Controller: (checkbox) select
   - Enable RDT to Controller: (checkbox) select
3. Expand **DNS Options** section.
   - Data Entry: GSLB Create Policies panel
   - Server Mode: (checkbox) select
   - Only Keep Active Servers: (checkbox) select
   - Only Keep Selected Servers: (checkbox) select
   - Answer Number: 1
4. Click **Create**. Returns to GSLB Policies Roster.

Creating GSLB FQDN (www.a10-lime.com)

1. Select **GSLB >> FQDN**. Opens GSLB FQDNs Roster.
2. Click **Create**. Opens GSLB Create FQDNs panel.
   - Data Entry: GSLB Create FQDNs panel
   - GSLB Zone: a10-lime.com
   - Service: www
   - Zone Policy: (drop down) RHOMBUS
   - Port: 80
3. Click **Create**. Returns to GSLB FQDNs Roster.

Configuring GSLB FQDN (www.a0-black.com)

1. Expand a10-lime.com (zone column). Reveals FQDNs for a10-lime.com zone.
2. Click **Edit** text on www.a10-lime.com. Opens GSLB Update FQDNs panel.
   - DNS Records section: Click Create button Opens GSLB Create DNS Record panel
   - Data Entry: GSLB Create DNS Record panel
   - Record Type: (Drop-Down) SERVICE A
   - Service IP Name: (Drop-Down) NYE
   - Static: (checkbox) select
3. Click **Create**. Returns to GSLB Update FQDNs panel.
   - DNS Records section: Click Create button Opens GSLB Create DNS Record panel
   - Data Entry: GSLB Create DNS Record panel
   - Record Type: (Drop-Down) Service A
   - Service IP Name: (Drop-Down) WASHOE
   - Static: (checkbox) select
4. Click **Create**. Returns to GSLB Update FQDNs panel.
5. Click **Update**. Returns to GSLB FQDNs Roster.

Enabling the GSLB Protocol

1. Select **GSLB >> Global**. Opens GSLB Update Global (System) Panel.
2. Select Protocol (secondary menu) Opens GSLB Update Global (Protocol) panel.
   - Data Entry: Update GSLB Global (Protocol) panel
   - Enable as GSLB controller: (checkbox) select
3. Click **Update**.

Contact Us