



GLOBAL SERVER LOAD BALANCING (GSLB) POWERED ZONE PREFERENCE

(A NetScaler GSLB and StoreFront solution)

Contents

Introduction	3
Solution.....	3
Deployment Topology	4
High-Level Request Flow	4
Configuration	5
Configuring the Load Balancing Virtual Server and the Services	5
Adding a Rewrite Policy and Action.....	8
Appendix A: Sample Deployment.....	11
BGL Site.....	11
CAM site	16
FTL site	21
Appendix B: Configuring GSLB entities, Servers, Services, Monitors, VPN Virtual Servers, and SSL Certificates	26

Introduction

In a distributed XenApp/XenDesktop deployment, StoreFront might not select an optimal datacenter when multiple equivalent resources are available from multiple datacenters. In such cases, StoreFront randomly selects a datacenter. It can send the request to any of the XenApp/XenDesktop servers in any datacenter, regardless of proximity to the client making the request.

Proximity-based GSLB might not choose the best site, because of a discrepancy caused by using the Local Domain Name Server (LDNS) to determine the client location. When clients make Domain Name System (DNS) requests, the requests are typically made to the respective LDNS server. Most LDNS servers are configured to perform recursive lookups, and therefore the NetScaler appliance does not receive the actual client IP address. It receives only the LDNS IP address. Internet service providers, such as AT&T, might have only one LDNS for a country. As a result, the datacenter might be chosen on the basis of an LDNS that is not in the user's geographical area, and it might not be the datacenter closest to the client.

Solution

Note: This enhancement is available with NetScaler release 11.0 build 65.x or later, StoreFront release 3.5 or later, and XenApp/XenDesktop release 7.7 or later.

With this enhancement, the client IP address is examined when an HTTP request arrives at the NetScaler Gateway appliance, and the real client IP address can be used to create the datacenter preference list that is forwarded to StoreFront. StoreFront uses this list to connect to the delivery controller closest to the client. StoreFront selects the optimal gateway VPN virtual server for the selected datacenter zone, adds this information to the ICA file, with appropriate IP addresses, and sends it to the client. If the NetScaler appliance is configured to insert the zone preference header, StoreFront 3.5 or later can use the information provided by the appliance to reorder the list of delivery controllers. Storefront then tries to launch applications hosted on the preferred datacenter's delivery controllers before trying to contact equivalent controllers in other datacenters.

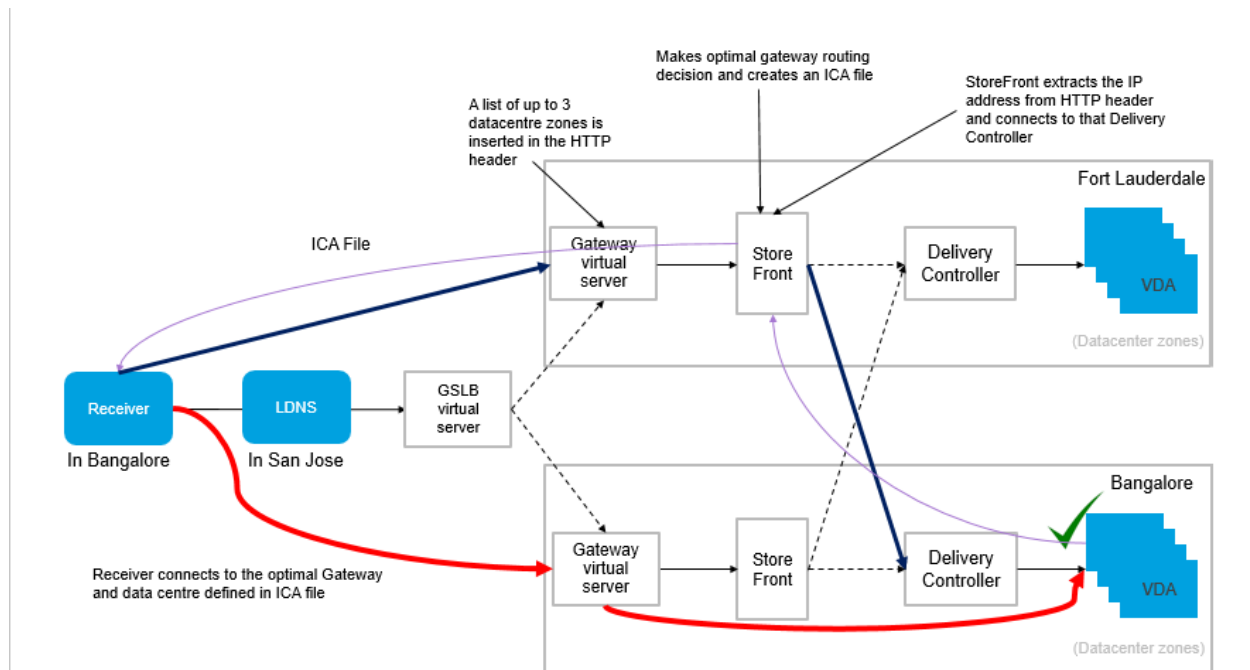
Notes:

1. Citrix recommends that when you deploy GSLB powered zone preference, you also create optimal gateway mappings between datacenters (zones) and NetScaler gateways. For information about configuring StoreFront, see <http://docs.citrix.com/en-us/storefront/3-5/sf-configure-ha.html>.
2. NetScaler Gateway must be set to clientless VPN (cVPN) or ICA Proxy mode. The sample deployment includes commands for cVPN mode. For information about configuring ICA Proxy mode, see https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/deploying-netscaler-gateway-in-ica-proxy-mode.pdf.

- The initial DNS query in a GSLB-Gateway setup is processed similar to a GSLB-LB setup. However, HTTP redirect persistence in a GSLB-Gateway persistence deployment functions as follows:
When the first request reaches a Gateway virtual server, the request is redirected to a site-specific URL by using HTTP 302 redirect. Because the URL is now site-specific, all further requests go directly on that site.

Deployment Topology

Some key components of this deployment are NetScaler and NetScaler Gateway appliances, and StoreFront and XenApp/XenDesktop servers. The following diagram shows how a user, who is logged on to Citrix Receiver to access his or her applications, is directed to the most optimal site on the basis of location.



High-Level Request Flow

Configure the Gateway to extract the client IP address and find the nearest datacenter:

- Create a non-addressable load balancing virtual server, with static proximity as the load balancing method, that creates a list of preferred datacenter zones. Configure the datacenter zones as back-end services and bind them to this virtual server.
- Create a rewrite policy with an action that causes the above virtual server to perform load balancing and insert the list of preferred services into an HTTP header.

3. Bind this policy to the Gateway VPN virtual server that acts on the incoming HTTP traffic.

When a request matches the policy:

4. The load balancing virtual server finds the closest datacenter to the client's IP address and prepares a datacenter zone preference, comma-separated list of up to three zones.
5. A new HTTP header, called "X-Citrix-ZonePreference," containing this list is inserted into the request sent to the StoreFront connected to the gateway VPN virtual server.
6. StoreFront extracts this list from the X-Citrix-ZonePreference header and uses it to connect to the appropriate datacenter zone.
7. Because Optimal Gateway Routing is configured, StoreFront selects the optimal gateway VPN virtual server for the connected datacenter, creates an ICA file with appropriate IP addresses, and sends it to the client. All HDX traffic from client to VDA then passes through the optimal gateway during the session.
8. When clients receive an ICA file, they connect to resources published in the nearest datacenter through the optimal gateway virtual server.

Configuration

A GSLB powered zone-preference setup requires a non-addressable load balancing server with services representing the datacenter zones. Also configure a rewrite action and policy, in addition to the other entities required in a typical GSLB-StoreFront setup.

The NetScaler command line and GUI steps for configuring the entities specific to the zone-preference are shown below. For information about configuring the other entities, see **Appendix B: Configuring GSLB entities, Servers, Services, Monitors, VPN Virtual Servers, and SSL Certificates**.

Configuring the Load Balancing Virtual Server and the Services

Create a non-addressable load balancing virtual server that uses the static proximity load balancing method, with round robin (the default) as the backup method. Add services to specify the datacenter zones, and bind them to the load balancing virtual server. The service IP address is just a placeholder for the zone that the service is representing. Bind monitors to the service, with each monitor monitoring a delivery controller for that zone. That is, the destination IP address in the monitor must be the delivery-controller IP address.

To configure a non-addressable load balancing virtual server by using the NetScaler command line

At the command prompt, type:

```
add lb vservers <name> <serviceType> <IPAddress> <port> -lbMethod <lbMethod>
```

To configure a non-addressable load balancing virtual server by using the NetScaler GUI

1. Navigate to **Traffic Management > Load Balancing > Virtual Servers**.
2. Add an HTTP virtual server.

Load Balancing Virtual Server

Basic Settings

Create a virtual server by specifying a name, an IP address, a port, and a protocol type. If an application is accessible from the Internet, the virtual server IP (VIP) address is a public IP address. If the application is accessible only from the local area network (LAN) or wide area network (WAN), the VIP is usually a private (ICANN non-routable) IP address. You can configure multiple virtual servers to receive client requests, thereby increasing the availability of resources to process client requests.

Name*

Protocol*

IP Address Type*

► More

To configure services to represent the datacenter zones by using the NetScaler command line

At the command prompt, type:

```
add service <name> <IP> <serviceType> <port> -monThreshold <positive_integer> -comment <string>
```

To configure services to represent the datacenter zones by using the NetScaler GUI

1. Navigate to **Traffic Management > Load Balancing > Services**.

2. Add an HTTP service.

Basic Settings

Service Name*

New Server Existing Server

Server*

Protocol*

Port*

Traffic Domain

Hash ID

Server ID

Cache Type*

Cacheable
 Enable Service
 Health Monitoring
 AppFlow Logging

Number of Active Connections

Comments

▲ Less

Note: The zone name (**Comments**) must be the same on StoreFront and XenApp/XenDesktop. For information about configuring the zone name on StoreFront, see <http://docs.citrix.com/en-us/storefront/3-5/sf-configure-ha.html>.

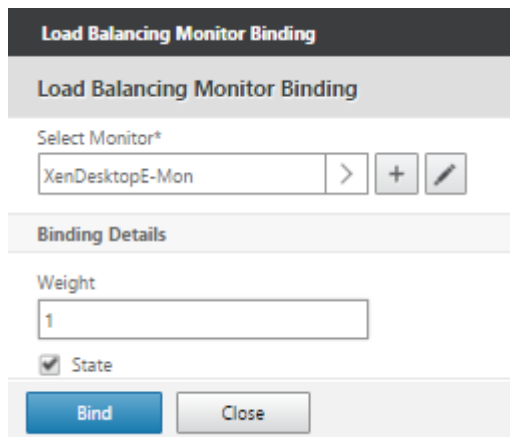
To bind a monitor to a service by using the NetScaler command line

At the command prompt, type:

bind service <name> -**monitorName** <string> -**weight** <positive_integer>

To bind a monitor to a service by using the NetScaler GUI

1. Navigate to **Traffic Management > GSLB > Services**.
2. Select a service and click **Edit**.
3. In **Advanced Settings**, click **Monitors** and bind a monitor to the service.



The screenshot shows the 'Load Balancing Monitor Binding' dialog box in the NetScaler GUI. It has a title bar 'Load Balancing Monitor Binding' and a subtitle 'Load Balancing Monitor Binding'. Below the subtitle is a 'Select Monitor*' section with a text input field containing 'XenDesktopE-Mon', a right arrow button, a plus button, and an edit button. Below that is a 'Binding Details' section with a 'Weight' input field containing '1' and a checked 'State' checkbox. At the bottom are 'Bind' and 'Close' buttons.

Note: The monitor IP address must match the desktop delivery controller (DDC) IP address. StoreFront might use the FQDN instead of the DDC IP address.

Adding a Rewrite Policy

Add a rewrite policy for incoming traffic, with an action that inserts the preferred zone description (ZoneName) into an HTTP header. The ZoneName is then used by StoreFront to send the request to the optimal VDA.

To configure a rewrite action and policy by using the NetScaler command line

At the command prompt, type:

```
add rewrite action <name> <type> <target> <stringBuilderExpr>  
add rewrite policy <name> <rule> <action>
```

To configure a rewrite action and policy by using the NetScaler GUI

1. Navigate to **AppExpert > Rewrite > Actions**.
2. Add the rewrite action.

Configure Rewrite Action

Configure Rewrite Action

Name
InsertZonePreferenceAction

Type
INSERT_HTTP_HEADER

Use this action type to insert a header.

Header Name*
X-Citrix-ZonePreference

Expression

Operators Saved Policy Expressions Frequently Used Expressions

`sys.vserver("ZonePreference").determine_services(description, ",")`

3. Navigate to **AppExpert > Rewrite > Policies**.
4. Add the rewrite policy.

Create Rewrite Policy

Name*

Action*

Log Action

Undefined-Result Action*

Expression*

TRUE

Comments

Appendix A: Sample Deployment

The following sample deployment shows the configuration on the NetScaler appliance and assumes that StoreFront and XenApp/XenDesktop are already configured at three sites: Bangalore (BGL), Cambridge (CAM), and Fort Lauderdale (FTL).

Note: This example is a complete GSLB StoreFront configuration that includes the entities configured for GSLB powered zone preference.

BGL Site

GSLB Site IP address - BGL site

```
add ns ip 203.0.113.1 255.255.255.255 -type GSLBsiteIP
```

SSL certificates for gateway virtual server

```
add ssl certKey Domain-CA -cert "/nsconfig/ssl/Domain-CA.cer"
```

```
add ssl certKey wildcard.domain.com -cert wildcard.domain.com -key  
wildcard.domain.com
```

LDAP authentication policy for gateway logon

```
add authentication ldapAction "domain.com LDAP" -serverIP  
192.168.1.100 -ldapBase "CN=Users,DC=domain,DC=com" -ldapBindDn  
"CN=administrator,CN=Users,DC=domain,DC=com" -ldapBindDnPassword  
Pa55word -encrypted -encryptmethod ENCMTHD_3 -ldapLoginName  
samAccountName -groupAttrName memberOf -subAttributeName CN
```

Policy to insert the HTTP X-Citrix-ZonePreference header into all traffic passing through the gateway virtual server

```
add policy expression InsertZonePreferenceExpression  
"sys.vserver(\"ZonePreference\").determine_services(description,  
\",\")"
```

```
add rewrite action InsertZonePreferenceAction insert_http_header X-  
Citrix-ZonePreference InsertZonePreferenceExpression
```

```
add rewrite policy InsertZonePreferencePolicy TRUE  
InsertZonePreferenceAction
```

Static proximity zone locations for ZonePreference virtual server

```
add location 192.0.0.1 192.0.0.255 "Europe.UK.FTL.*.*.*"  
add location 198.51.100.1 198.51.100.255 "NorthAmerica.US.CAM.*.*.*"  
add location 203.0.113.1 203.0.113.255 "Asia.India.BGL.*.*.*"
```

StoreFront server

```
add server StorefrontBGL 203.0.113.178
```

XD 7.8 servers

```
add server XenDesktopA 192.0.0.206  
add server XenDesktopB 192.0.0.207  
add server XenDesktopC 198.51.100.208  
add server XenDesktopD 198.51.100.209  
add server XenDesktopE 203.0.113.210  
add server XenDesktopF 203.0.113.211
```

ZonePreference services

Note: The zone name (comment) in the following command must be the same on StoreFront and XenApp/XenDesktop also.

```
add service FTL 192.0.0.2 HTTP 80 -monThreshold 1 -comment FTLZone  
add service CAM 198.51.100.2 HTTP 80 -monThreshold 1 -comment CAMZone  
add service BGL 203.0.113.2 HTTP 80 -monThreshold 1 -comment BGLZone
```

ZonePreference virtual server (non-addressable)

```
add lb vserver ZonePreference HTTP 0.0.0.0 0 -lbMethod STATICPROXIMITY
```

ZonePreference services to virtual server binding

```
bind lb vserver ZonePreference FTL  
bind lb vserver ZonePreference CAM  
bind lb vserver ZonePreference BGL
```

Monitors to check the connectivity to each XenDesktop Delivery Controller

Note: The monitor IP address in the following commands must match the Desktop Delivery Controller (DDC) IP address. StoreFront might use the FQDN instead of the DDC IP address.

```
add lb monitor XenDesktopA-Mon CITRIX-XD-DDC -destIP 192.0.0.206 -
destPort 80
```

```
add lb monitor XenDesktopB-Mon CITRIX-XD-DDC -destIP 192.0.0.207 -
destPort 80
```

```
add lb monitor XenDesktopC-Mon CITRIX-XD-DDC -destIP 198.51.100.208 -
destPort 80
```

```
add lb monitor XenDesktopD-Mon CITRIX-XD-DDC -destIP 198.51.100.209 -
destPort 80
```

```
add lb monitor XenDesktopE-Mon CITRIX-XD-DDC -destIP 203.0.113.210 -
destPort 80
```

```
add lb monitor XenDesktopF-Mon CITRIX-XD-DDC -destIP 203.0.113.211 -
destPort 80
```

XenDesktop monitors to ZonePreference service binding (a probe from at least 1 monitor should succeed for the service to be marked as UP)

```
bind service FTL -monitorName XenDesktopA-Mon -weight 1
```

```
bind service FTL -monitorName XenDesktopB-Mon -weight 1
```

```
bind service CAM -monitorName XenDesktopC-Mon -weight 1
```

```
bind service CAM -monitorName XenDesktopD-Mon -weight 1
```

```
bind service BGL -monitorName XenDesktopE-Mon -weight 1
```

```
bind service BGL -monitorName XenDesktopF-Mon -weight 1
```

ADNS Service for GSLB (This must be a public IP address)

```
add service aDNSsvc 203.0.113.1 ADNS 53
```

GSLB virtual server and sites

```
add gslb vserver gslbvsGlobal SSL -lbMethod STATICPROXIMITY -
backupLBMethod ROUNDROBIN
```

```
add gslb site FTL 192.0.0.1
```

```

add gslb site CAM 198.51.100.1
add gslb site BGL 203.0.113.1

# GSLB services representing a gateway virtual server at each zone
add gslb service gslbsvcFTL 192.0.0.14 SSL 443 -siteName FTL
add gslb service gslbsvcCAM 198.51.100.24 SSL 443 -siteName CAM
add gslb service gslbsvcBGL 203.0.113.54 SSL 443 -siteName BGL

# GSLB services to GSLB virtual server binding
bind gslb vserver gslbvsGlobal -serviceName gslbsvcFTL
bind gslb vserver gslbvsGlobal -serviceName gslbsvcCAM
bind gslb vserver gslbvsGlobal -serviceName gslbsvcBGL

# GSLB domain name
bind gslb vserver gslbvsGlobal -domainName gslb.domain.com -TTL 5

# Cookie recognition patterns for StoreFront NoRewrite policy
add policy patset SFCookies
bind policy patset SFCookies Csrftoken -index 1
bind policy patset SFCookies ASP.NET_SessionId -index 2
bind policy patset SFCookies CtxsPluginAssistantState -index 3
bind policy patset SFCookies CtxsAuthId -index 4

# Clientless access No Rewrite Policy
add vpn clientlessAccessProfile NoRewrite
set vpn clientlessAccessProfile NoRewrite -URLRewritePolicyLabel
ns_cvpn_default_url_label -ClientConsumedCookies SFCookies
add vpn clientlessAccessPolicy NoRewrite true NoRewrite

```

Gateway virtual server (This must be a public IP address)

```
add vpn vserver BGLGateway SSL 203.0.113.54 443
```

Gateway policies and actions

```
add vpn sessionAction NativeReceiver -sessTimeout 60 -
defaultAuthorizationAction ALLOW -icaProxy OFF -wiPortalMode NORMAL -
ntDomain ptd -clientlessVpnMode ON -clientlessModeUrlEncoding
TRANSPARENT -clientlessPersistentCookie ALLOW -storefronturl
"https://storefrontBGL.domain.com/Citrix/Roaming/Accounts"
```

Note: The URL in the following command must match the host base URL and receiver for web site in StoreFront.

```
add vpn sessionAction WebReceiver -sessTimeout 60 -
defaultAuthorizationAction ALLOW -SSO ON -ssoCredential PRIMARY -
homePage "https://storefrontBGL.domain.com/Citrix/StoreWeb" -icaProxy
OFF -wihome "https://storefrontBGL.domain.com/Citrix/StoreWeb" -
ntDomain domain -clientlessVpnMode ON -clientlessModeUrlEncoding
TRANSPARENT -clientlessPersistentCookie ALLOW
```

```
add vpn sessionPolicy WebReceiver "REQ.HTTP.HEADER User-Agent
NOTCONTAINS CitrixReceiver && REQ.HTTP.HEADER Referer EXISTS"
WebReceiver
```

```
add vpn sessionPolicy NativeReceiver "REQ.HTTP.HEADER User-Agent
CONTAINS CitrixReceiver && REQ.HTTP.HEADER X-Citrix-Gateway EXISTS"
NativeReceiver
```

```
set vpn parameter -clientSecurityLog ON -transparentInterception ON -
forceCleanup none -clientOptions all -clientConfiguration all
```

```
bind vpn vserver BGLGateway -staServer "http://xendesktop.domain.com"
```

```
bind vpn vserver BGLGateway -staServer "http://xendesktopf.domain.com"
```

```
bind vpn vserver BGLGateway -policy "domain.com LDAP" -priority 100
```

```
bind vpn vserver BGLGateway -policy WebReceiver -priority 10
```

```
bind vpn vserver BGLGateway -policy NativeReceiver -priority 20
```

```
bind vpn vserver BGLGateway -policy NoRewrite -priority 8 -
gotoPriorityExpression END -type REQUEST
```

```
bind vpn vserver BGLGateway -policy InsertZonePreferencePolicy -
priority 5 -gotoPriorityExpression END -type REQUEST
```

```
bind ssl vserver BGLGateway -certkeyName wildcard.domain.com
```

```
bind ssl vsrver BGLGateway -certkeyName Internet.Local-CA -CA -
ocspCheck Optional
```

CAM site

```
## GSLB Site IP address - CAM site
```

```
add ns ip 198.51.100.1 255.255.255.255 -type GSLBsiteIP
```

```
# SSL certificates for gateway virtual server
```

```
add ssl certKey Domain-CA -cert "/nsconfig/ssl/Domain-CA.cer"
```

```
add ssl certKey wildcard.domain.com -cert wildcard.domain.com -key
wildcard.domain.com
```

```
# LDAP authentication policy for gateway logon
```

```
add authentication ldapAction "domain.com LDAP" -serverIP
192.168.1.100 -ldapBase "CN=Users,DC=domain,DC=com" -ldapBindDn
"CN=administrator,CN=Users,DC=domain,DC=com" -ldapBindDnPassword
Pa55word -encrypted -encryptmethod ENCMTHD_3 -ldapLoginName
samAccountName -groupAttrName memberOf -subAttributeName CN
```

```
# Policy to insert the HTTP X-Citrix-ZonePreference header into all traffic passing through the
gateway virtual server
```

```
add policy expression InsertZonePreferenceExpression
"sys.vserver(\"ZonePreference\").determine_services(description,
\",\")"
```

```
add rewrite action InsertZonePreferenceAction insert_http_header X-
Citrix-ZonePreference InsertZonePreferenceExpression
```

```
add rewrite policy InsertZonePreferencePolicy TRUE
InsertZonePreferenceAction
```

```
# Static proximity zone locations for ZonePreference virtual server
```

```
add location 192.0.0.1 192.0.0.255 "Europe.UK.FTL.*.*.*"
```

```
add location 198.51.100.1 198.51.100.255 "NorthAmerica.US.CAM.*.*.*"
```

```
add location 203.0.113.1 203.0.113.255 "Asia.India.BGL.*.*.*"
```


StoreFront server

```
add server StorefrontCAM 198.51.100.178
```

XD 7.8 servers

```
add server XenDesktopA 192.0.0.206
add server XenDesktopB 192.0.0.207
add server XenDesktopC 198.51.100.208
add server XenDesktopD 198.51.100.209
add server XenDesktopE 203.0.113.210
add server XenDesktopF 203.0.113.211
```

ZonePreference services

Note: The zone name (comment) in the following command must be the same on StoreFront and XenApp/XenDesktop also.

```
add service FTL 192.0.0.2 HTTP 80 -monThreshold 1 -comment FTLZone
add service CAM 198.51.100.2 HTTP 80 -monThreshold 1 -comment CAMZone
add service BGL 203.0.113.2 HTTP 80 -monThreshold 1 -comment BGLZone
```

ZonePreference virtual server (non-addressable)

```
add lb vserver ZonePreference HTTP 0.0.0.0 0 -lbMethod STATICPROXIMITY
```

ZonePreference services to virtual server binding

```
bind lb vserver ZonePreference FTL
bind lb vserver ZonePreference CAM
bind lb vserver ZonePreference BGL
```

Monitors to check the connectivity of each XenDesktop Delivery Controller

Note: The monitor IP address in the following commands must match the Desktop Delivery Controller (DDC) IP address. StoreFront might use the FQDN instead of the DDC IP address.

```
add lb monitor XenDesktopA-Mon CITRIX-XD-DDC -destIP 192.0.0.206 -
destPort 80
```

```
add lb monitor XenDesktopB-Mon CITRIX-XD-DDC -destIP 192.0.0.207 -
destPort 80

add lb monitor XenDesktopC-Mon CITRIX-XD-DDC -destIP 198.51.100.208 -
destPort 80

add lb monitor XenDesktopD-Mon CITRIX-XD-DDC -destIP 198.51.100.209 -
destPort 80

add lb monitor XenDesktopE-Mon CITRIX-XD-DDC -destIP 203.0.113.210 -
destPort 80

add lb monitor XenDesktopF-Mon CITRIX-XD-DDC -destIP 203.0.113.211 -
destPort 80
```

XenDesktop monitors to ZonePreference service binding (a probe from at least 1 monitor should succeed for the service to be marked as UP)

```
bind service FTL -monitorName XenDesktopA-Mon -weight 1
bind service FTL -monitorName XenDesktopB-Mon -weight 1
bind service CAM -monitorName XenDesktopC-Mon -weight 1
bind service CAM -monitorName XenDesktopD-Mon -weight 1
bind service BGL -monitorName XenDesktopE-Mon -weight 1
bind service BGL -monitorName XenDesktopF-Mon -weight 1
```

ADNS Service for GSLB (This must be a public IP address)

```
add service aDNSsvc 198.51.100.1 ADNS 53
```

GSLB virtual server and sites

```
add gslb vserver gslbvsGlobal SSL -lbMethod STATICPROXIMITY -
backupLBMethod ROUNDROBIN

add gslb site FTL 192.0.0.1

add gslb site CAM 198.51.100.1

add gslb site BGL 203.0.113.1
```

GSLB services representing a gateway virtual server at each zone

```
add gslb service gslbsvcFTL 192.0.0.14 SSL 443 -siteName FTL
add gslb service gslbsvcCAM 198.51.100.24 SSL 443 -siteName CAM
```

```
add gslb service gslbsvcBGL 203.0.113.54 SSL 443 -siteName BGL
```

GSLB services to GSLB virtual server binding

```
bind gslb vserver gslbvsGlobal -serviceName gslbsvcFTL
```

```
bind gslb vserver gslbvsGlobal -serviceName gslbsvcCAM
```

```
bind gslb vserver gslbvsGlobal -serviceName gslbsvcBGL
```

GSLB domain name

```
bind gslb vserver gslbvsGlobal -domainName gslb.domain.com -TTL 5
```

Cookie recognition patterns for StoreFront NoRewrite policy

```
add policy patset SFCookies
```

```
bind policy patset SFCookies Csrftoken -index 1
```

```
bind policy patset SFCookies ASP.NET_SessionId -index 2
```

```
bind policy patset SFCookies CtxsPluginAssistantState -index 3
```

```
bind policy patset SFCookies CtxsAuthId -index 4
```

Clientless access No Rewrite Policy

```
add vpn clientlessAccessProfile NoRewrite
```

```
set vpn clientlessAccessProfile NoRewrite -URLRewritePolicyLabel  
ns_cvpn_default_url_label -ClientConsumedCookies SFCookies
```

```
add vpn clientlessAccessPolicy NoRewrite true NoRewrite
```

Gateway virtual server (This must be a public IP address)

```
add vpn vserver CAMGateway SSL 198.51.100.54 443
```

Gateway policies and actions

```
add vpn sessionAction NativeReceiver -sessTimeout 60 -  
defaultAuthorizationAction ALLOW -icaProxy OFF -wiPortalMode NORMAL -  
ntDomain ptd -clientlessVpnMode ON -clientlessModeUrlEncoding  
TRANSPARENT -clientlessPersistentCookie ALLOW -storefronturl  
"https://storefrontCAM.domain.com/Citrix/Roaming/Accounts"
```

Note: The URL in the following command must match the host base URL and receiver for web site in StoreFront.

```
add vpn sessionAction WebReceiver -sessTimeout 60 -
defaultAuthorizationAction ALLOW -SSO ON -ssoCredential PRIMARY -
homePage "https://storefrontCAM.domain.com/Citrix/StoreWeb" -icaProxy
OFF -wihome "https://storefrontCAM.domain.com/Citrix/StoreWeb" -
ntDomain domain -clientlessVpnMode ON -clientlessModeUrlEncoding
TRANSPARENT -clientlessPersistentCookie ALLOW
```

```
add vpn sessionPolicy WebReceiver "REQ.HTTP.HEADER User-Agent
NOTCONTAINS CitrixReceiver && REQ.HTTP.HEADER Referer EXISTS"
WebReceiver
```

```
add vpn sessionPolicy NativeReceiver "REQ.HTTP.HEADER User-Agent
CONTAINS CitrixReceiver && REQ.HTTP.HEADER X-Citrix-Gateway EXISTS"
NativeReceiver
```

```
set vpn parameter -clientSecurityLog ON -transparentInterception ON -
forceCleanup none -clientOptions all -clientConfiguration all
```

```
bind vpn vserver CAMGateway -staServer "http://xendesktopc.domain.com"
```

```
bind vpn vserver CAMGateway -staServer "http://xendesktopd.domain.com"
```

```
bind vpn vserver CAMGateway -policy "domain.com LDAP" -priority 100
```

```
bind vpn vserver CAMGateway -policy WebReceiver -priority 10
```

```
bind vpn vserver CAMGateway -policy NativeReceiver -priority 20
```

```
bind vpn vserver CAMGateway -policy NoRewrite -priority 8 -
gotoPriorityExpression END -type REQUEST
```

```
bind vpn vserver CAMGateway -policy InsertZonePreferencePolicy -
priority 5 -gotoPriorityExpression END -type REQUEST -
```

```
bind ssl vserver CAMGateway -certkeyName wildcard.domain.com
```

```
bind ssl vserver CAMGateway -certkeyName Internet.Local-CA -CA -
ocspCheck Optional
```

FTL site

GSLB Site IP address - FTL site

```
add ns ip 192.0.0.1 255.255.255.255 -type GSLBsiteIP
```

SSL certificates for gateway virtual server

```
add ssl certKey Domain-CA -cert "/nsconfig/ssl/Domain-CA.cer"
```

```
add ssl certKey wildcard.domain.com -cert wildcard.domain.com -key  
wildcard.domain.com
```

LDAP authentication policy for gateway logon

```
add authentication ldapAction "domain.com LDAP" -serverIP  
192.168.1.100 -ldapBase "CN=Users,DC=domain,DC=com" -ldapBindDn  
"CN=administrator,CN=Users,DC=domain,DC=com" -ldapBindDnPassword  
Pa55word -encrypted -encryptmethod ENCMTHD_3 -ldapLoginName  
samAccountName -groupAttrName memberOf -subAttributeName CN
```

Policy to insert the HTTP X-Citrix-ZonePreference header into all traffic passing through the gateway virtual server

```
add policy expression InsertZonePreferenceExpression  
"sys.vserver(\"ZonePreference\").determine_services(description,  
\",\")"  
  
add rewrite action InsertZonePreferenceAction insert_http_header X-  
Citrix-ZonePreference InsertZonePreferenceExpression  
  
add rewrite policy InsertZonePreferencePolicy TRUE  
InsertZonePreferenceAction
```

Static proximity zone locations for ZonePreference virtual server

```
add location 192.0.0.1 192.0.0.255 "Europe.UK.FTL.*.*.*"  
add location 198.51.100.1 198.51.100.255 "NorthAmerica.US.CAM.*.*.*"  
add location 203.0.113.1 203.0.113.255 "Asia.India.BGL.*.*.*"
```

StoreFront server

```
add server StorefrontFTL 192.0.0.178
```

XD 7.8 servers

```
add server XenDesktopA 192.0.0.206
add server XenDesktopB 192.0.0.207
add server XenDesktopC 198.51.100.208
add server XenDesktopD 198.51.100.209
add server XenDesktopE 203.0.113.210
add server XenDesktopF 203.0.113.211
```

ZonePreference services

Note: The zone name (comment) in the following command must be the same on StoreFront and XenApp/XenDesktop also.

```
add service FTL 192.0.0.2 HTTP 80 -monThreshold 1 -comment FTLZone
add service CAM 198.51.100.2 HTTP 80 -monThreshold 1 -comment CAMZone
add service BGL 203.0.113.2 HTTP 80 -monThreshold 1 -comment BGLZone
```

ZonePreference virtual server (non-addressable)

```
add lb vserver ZonePreference HTTP 0.0.0.0 0 -lbMethod STATICPROXIMITY
```

ZonePreference services to virtual server binding

```
bind lb vserver ZonePreference FTL
bind lb vserver ZonePreference CAM
bind lb vserver ZonePreference BGL
```

Monitors to check the connectivity of each XenDesktop Delivery Controller

Note: The monitor IP address in the following commands must match the Desktop Delivery Controller (DDC) IP address. StoreFront might use the FQDN instead of the DDC IP address.

```
add lb monitor XenDesktopA-Mon CITRIX-XD-DDC -destIP 192.0.0.206 -
destPort 80
add lb monitor XenDesktopB-Mon CITRIX-XD-DDC -destIP 192.0.0.207 -
destPort 80
```

```
add lb monitor XenDesktopC-Mon CITRIX-XD-DDC -destIP 198.51.100.208 -
destPort 80

add lb monitor XenDesktopD-Mon CITRIX-XD-DDC -destIP 198.51.100.209 -
destPort 80

add lb monitor XenDesktopE-Mon CITRIX-XD-DDC -destIP 203.0.113.210 -
destPort 80

add lb monitor XenDesktopF-Mon CITRIX-XD-DDC -destIP 203.0.113.211 -
destPort 80
```

XenDesktop monitors to ZonePreference service binding (a probe from at least 1 monitor should succeed for the service to be marked as UP)

```
bind service FTL -monitorName XenDesktopA-Mon -weight 1
bind service FTL -monitorName XenDesktopB-Mon -weight 1
bind service CAM -monitorName XenDesktopC-Mon -weight 1
bind service CAM -monitorName XenDesktopD-Mon -weight 1
bind service BGL -monitorName XenDesktopE-Mon -weight 1
bind service BGL -monitorName XenDesktopF-Mon -weight 1
```

ADNS Service for GSLB (This must be a public IP address)

```
add service aDNSsvc 192.0.0.1 ADNS 53
```

GSLB virtual server and sites

```
add gslb vserver gslbvsGlobal SSL -lbMethod STATICPROXIMITY -
backupLBMethod ROUNDROBIN

add gslb site FTL 192.0.0.1
add gslb site CAM 198.51.100.1
add gslb site BGL 203.0.113.1
```

GSLB services representing a gateway virtual server at each zone

```
add gslb service gslbsvcFTL 192.0.0.14 SSL 443 -siteName FTL
add gslb service gslbsvcCAM 198.51.100.24 SSL 443 -siteName CAM
add gslb service gslbsvcBGL 203.0.113.54 SSL 443 -siteName BGL
```

GSLB services to GSLB virtual server binding

```
bind gslb vserver gslbvsGlobal -serviceName gslbsvcFTL
bind gslb vserver gslbvsGlobal -serviceName gslbsvcCAM
bind gslb vserver gslbvsGlobal -serviceName gslbsvcBGL
```

GSLB domain name

```
bind gslb vserver gslbvsGlobal -domainName gslb.domain.com -TTL 5
```

Cookie recognition patterns for StoreFront NoRewrite policy

```
add policy patset SFCookies
bind policy patset SFCookies Csrftoken -index 1
bind policy patset SFCookies ASP.NET_SessionId -index 2
bind policy patset SFCookies CtxsPluginAssistantState -index 3
bind policy patset SFCookies CtxsAuthId -index 4
```

Clientless access No Rewrite Policy

```
add vpn clientlessAccessProfile NoRewrite
set vpn clientlessAccessProfile NoRewrite -URLRewritePolicyLabel
ns_cvpn_default_url_label -ClientConsumedCookies SFCookies
add vpn clientlessAccessPolicy NoRewrite true NoRewrite
```

Gateway virtual server (This must be a public IP address)

```
add vpn vserver FTLLGateway SSL 192.0.0.54 443
```

Gateway policies and actions

```
add vpn sessionAction NativeReceiver -sessTimeout 60 -
defaultAuthorizationAction ALLOW -icaProxy OFF -wiPortalMode NORMAL -
ntDomain ptd -clientlessVpnMode ON -clientlessModeUrlEncoding
TRANSPARENT -clientlessPersistentCookie ALLOW -storefronturl
"https://storefrontFTL.domain.com/Citrix/Roaming/Accounts"
```


Note: The URL in the following command must match the host base URL and receiver for web site in StoreFront.

```
add vpn sessionAction WebReceiver -sessTimeout 60 -
defaultAuthorizationAction ALLOW -SSO ON -ssoCredential PRIMARY -
homePage "https://storefrontFTL.domain.com/Citrix/StoreWeb" -icaProxy
OFF -wihome "https://storefrontFTL.domain.com/Citrix/StoreWeb" -
ntDomain domain -clientlessVpnMode ON -clientlessModeUrlEncoding
TRANSPARENT -clientlessPersistentCookie ALLOW
```

```
add vpn sessionPolicy WebReceiver "REQ.HTTP.HEADER User-Agent
NOTCONTAINS CitrixReceiver && REQ.HTTP.HEADER Referer EXISTS"
WebReceiver
```

```
add vpn sessionPolicy NativeReceiver "REQ.HTTP.HEADER User-Agent
CONTAINS CitrixReceiver && REQ.HTTP.HEADER X-Citrix-Gateway EXISTS"
NativeReceiver
```

```
set vpn parameter -clientSecurityLog ON -transparentInterception ON -
forceCleanup none -clientOptions all -clientConfiguration all
```

```
bind vpn vserver FTLGateway -staServer "http://xendesktop1.domain.com"
```

```
bind vpn vserver FTLGateway -staServer "http://xendesktopb.domain.com"
```

```
bind vpn vserver FTLGateway -policy "domain.com LDAP" -priority 100
```

```
bind vpn vserver FTLGateway -policy WebReceiver -priority 10
```

```
bind vpn vserver FTLGateway -policy NativeReceiver -priority 20
```

```
bind vpn vserver FTLGateway -policy NoRewrite -priority 8 -
gotoPriorityExpression END -type REQUEST
```

```
bind vpn vserver FTLGateway -policy InsertZonePreferencePolicy -
priority 5 -gotoPriorityExpression END -type REQUEST
```

```
bind ssl vserver FTLGateway -certkeyName wildcard.domain.com
```

```
bind ssl vserver FTLGateway -certkeyName Internet.Local-CA -CA -
ocspCheck Optional
```

Appendix B: Configuring GSLB entities, Servers, Services, Monitors, VPN Virtual Servers, and SSL Certificates

The NetScaler command line and GUI procedures for configuring a GSLB-StoreFront setup are as follows:

To configure a GSLB site and custom location by using the NetScaler command line

At the command prompt, type:

```
add gslb site <siteName> <siteIPAddress>
```

```
add location <IPfrom> <IPto> <preferredLocation>
```

To configure a GSLB site by using the NetScaler GUI

1. Navigate to **Traffic Management > GSLB > Sites**.
2. Add a GSLB site.

To configure a custom location by using the NetScaler GUI

1. Navigate to **AppExpert > Location**.
2. Create a custom entry or location file (static databases).

To configure a GSLB virtual server by using the NetScaler command line

At the command prompt, type:

```
add gslb vsrver <name> <serviceType> -lbMethod -backupLBMethod
```

To configure a GSLB service and bind it to a GSLB virtual server by using the NetScaler command line

At the command prompt, type:

```
add gslb service <serviceName> <IP> <serviceType> <port> -siteName  
bind gslb vsrver <name> -serviceName <string>
```

To configure a domain by using the NetScaler command line

At the command prompt, type:

```
set gslb vserver <name> -domainName <string>
```

To configure a GSLB virtual server, service, and domain by using the NetScaler GUI

1. Navigate to **Traffic Management > GSLB > Virtual Servers**.
2. Add a GSLB virtual server of type SSL.
3. Click **OK**.
4. In **Advanced Settings** select **Service**, and add or bind a service of type SSL.
5. Select **Domains**, and bind a domain to the virtual server.
6. Click **Done**.

To configure a VPN virtual server by using the NetScaler command line

At the command prompt, type:

```
add vpn vserver <name> SSL <IPAddress> <port>
```

To configure a VPN session policy by using the NetScaler command line

At the command prompt, type:

```
add vpn sessionPolicy <name> <rule> <action>
```

```
add vpn sessionAction <name> -sesTimeout <mins> -defaultAuthorizationAction ALLOW  
-SSO ON -ssoCredential PRIMARY -homePage <URL> -icaProxy OFF -wihome <URL> -  
ntDomain <string> -clientlessVpnMode ON -clientlessModeUrlEncoding TRANSPARENT -  
clientlessPersistentCookie ALLOW
```

To configure an SSL certificate by using the NetScaler command line

At the command prompt, type:

```
add ssl certkey <certkeyname> -cert <string> -key <string>
```

To configure a VPN virtual server and bind an SSL certificate and a policy by using the NetScaler GUI

1. Navigate to **NetScaler Gateway > Virtual Servers**.
2. Add a virtual server.
3. In **Certificates**, add or select a certificate to bind to this virtual server.

4. In **Policies**, add or select a policy to bind to this virtual server.
5. Click **Done**.

For information about configuring LDAP authentication on NetScaler Gateway, see <http://docs.citrix.com/en-us/netScaler-gateway/11/authentication-authorization/configure-ldap.html>

To configure a server by using the NetScaler command line

At the command prompt, type:

```
add server <name> <IPAddress>
```

To configure a server by using the NetScaler GUI

1. Navigate to **NetScaler Gateway > Servers**.
2. Add a server.

To configure an ADNS service by using the NetScaler command line

At the command prompt, type:

```
add service <name> <IP> ADNS <port>
```

To configure an ADNS service by using the NetScaler GUI

1. Navigate to **Traffic Management > Load Balancing > Services**.
2. Add an ADNS service.

To configure a CITRIX-XD-DDC monitor and bind it to a service by using the NetScaler command line

At the command prompt, type:

```
add lb monitor <monitorName> CITRIX-XD-DDC
```

```
bind service <name> -monitorName <string>
```

To configure a CITRIX-XD-DDC monitor by using the NetScaler GUI

1. Navigate to **Traffic Management > Load Balancing > Services**.
2. Add a CITRIX-XD-DDC monitor.

To bind a monitor to a service by using the NetScaler GUI

1. Navigate to **Traffic Management > GSLB > Services**.
2. Select a service and click **Edit**.
3. In **Advanced Settings**, click **Monitors** and bind a monitor to the service.

To add a pattern set and bind a pattern to it by using the NetScaler command line

At the command prompt, type:

```
add policy patset <name>
```

```
bind policy patset <name> <string> [-index <positive_integer>]
```

To add a pattern set by using the NetScaler GUI

1. Navigate to **AppExpert > Pattern Sets**.
2. Add a pattern set and insert a pattern.