Citrix XenApp and XenDesktop 6.x Deployment

https://campus.barracuda.com/doc/41111558/

Follow the steps in this guide to deploy the Barracuda Load Balancer ADC to increase the scalability and reliability of your Citrix XenApp or XenDesktop deployment.

Terminology

Term	Definition
Fully Qualified Domain Name (FQDN)	The unique name for a specific computer or host that can resolve to an IP address (e.g., www.example.com).
Service	A combination of a virtual IP address and one or more TCP/UDP ports that the Barracuda Load Balancer ADC listens on. Traffic arriving on the specified port is directed to one of the real servers associated with a service.
VIP	Virtual IP address. In the Barracuda Load Balancer ADC deployment, the VIP address is added to the service on the Barracuda Load Balancer ADC.

Product Versions and Prerequisites

To deploy Citrix XenApp and XenDesktop 6.x with the Barracuda Load Balancer ADC, you must have the following:

- Barracuda Load Balancer ADC version 5.1 and above
- Citrix XenApp 6.x or Citrix XenDesktop 6.x
- Windows Server 2008 R2 or later

You must also complete the following tasks:

- Install your Barracuda Load Balancer ADC(s), connect to the web interface, and activate your subscription(s).
- To deploy Citrix XenApp and/or XenDesktop with high availability, you must cluster your Barracuda Load Balancer ADCs. For more information, see High Availability.

Barracuda Load Balancer ADC Service Options

On the Barracuda Load Balancer ADC, create services for the type of traffic that is supported by your Citrix servers. Depending on the traffic type, you can create Instant SSL, HTTP, or HTTPS services.

Scenario	Service Options
Citrix servers support traffic over HTTP only	Create the CITRIX_HTTP service.
Citrix servers support traffic over HTTPS only	Create the CITRIX_HTTPS service.
Citrix servers support traffic over HTTP and HTTPS	If you want to offload SSL to the ADC and redirect HTTP traffic to an HTTPS service, create the CITRIX_INSTSSL service, otherwise create a combination of the CITRIX_HTTP service *and* CITRIX_HTTPS service.

Step 1. Configure the Citrix Servers

When you are deploying Citrix XenApp or Citrix XenDesktop, set up at least two servers in a server group configuration and license both servers. Set up one server as the master and the other server as the support server. HTTP is configured by default. If you want to use HTTPS or Instant SSL, first make the appropriate changes to the internal and external access links.

Step 2. Create Services on the Barracuda Load Balancer ADC

Add services according to the type of traffic supported by your Citrix servers.

1. Log into the Barracuda Load Balancer ADC as the administrator.
2. If you want to create an HTTPS or Instant SSL service, go to the **BASIC > Certificates** page and import the same certificate you configured for the Citrix servers.
3. Go to the **BASIC > Services** page.
4. For each type of service that you add from Table 1, click **Add Service** and enter the values in the corresponding fields.

Table 1. Available Services

Name	Type	IP Address	Port	Session Timeout	Server Monitor
CITRIX_HTTP	HTTP	VIP address for the Citrix service For example: `10.5.7.193`	80	0	◦ **Testing Method:** Simple HTTP ◦ **HTTP Method:** HEAD ◦ **Test Target:** /CitrixAccess/auth/login.aspx ◦ **Additional Headers:** User-Agent: Barracuda Load Balancer ADC Server Monitor ◦ **Status Code:** 200 ◦ **Test Delay:** 30 Seconds

CITRIX_HTTPS	HTTPS	VIP address for the Citrix service For example: 10.5.7.193	443	0	◦ **Testing Method:** Simple HTTPS ◦ **HTTP Method:** HEAD ◦ **Test Target:** /CitrixAccess/auth/login.aspx ◦ **Additional Headers:** User-Agent: Barracuda Load Balancer ADC Server Monitor ◦ **Status Code:** 200 ◦ **Test Delay:** 30 Seconds
CITRIX_INSTSSL	INSTANT_SSL	VIP address for the Citrix service For example: 10.5.7.193	**Port**: 443 **HTTP Redirect Port**: 80	0	◦ **Testing Method:** Simple HTTP ◦ **HTTP Method:** HEAD ◦ **Test Target:** /CitrixAccess/auth/login.aspx ◦ **Additional Headers:** User-Agent: Barracuda Load Balancer ADC Server Monitor ◦ **Status Code:** 200 ◦ **Test Delay:** 30 Seconds

5. If your servers are configured in a cluster, specify these settings in the **Load Balancing** section:
    1. For **Algorithm**, select **Least Requests**.
    2. For **Persistence Type**, select **Cookie Insert**.
    3. Enter a name for the cookie and configure the cookie settings that appear.
    4. In the **Persistence Time** field, enter 1200.
6. Click **Create**.

Step 3. Add the Real Servers

Add your Citrix servers to your services. For each Citrix server:

1. On the **BASIC > Services** page, verify that the correct service for the server is displayed.
2. Click **Add Server**.
3. Enter the IP address and port of the server.
    - If you are adding the server to an CITRIX_HTTP or CITRIX_INSTSSL service, use **Port** 80.
    - If you are adding the server to an CITRIX_HTTPS service, use **Port** 443.
4. If the server is part of a cluster, specify whether it is a **Backup server** and enter its **Weight** for the load balancing algorithm.
5. If you are adding the server to an HTTPS service, enable SSL.
    1. Set **Servers uses SSL** to **On**. If you do not enable the server to use SSL, unencrypted traffic is passed to the server because the Barracuda Load Balancer ADC decrypts incoming traffic in order to maintain session persistence using HTTP cookies.
    2. Select the **Certificate** that you uploaded for the Citrix server.
6. Click **Create**.

Step 4. Configure DNS

Create an A record to point to the VIP address that you set on the Barracuda Load Balancer ADC for the Citrix XenApp service.

For example, if you want to use the name *citrix* and your domain is *barracuda.com*, your A record would appear as follows:

Name	IP Address
citrix.barracuda.com	10.5.7.193

Step 5. Verify Your Configuration

Go to the Citrix Access Site by using the name that you set in the A record, and verify that you can log in and use the applications.

For example: `citrix.barracuda.com`

Next Steps

You can configure authentication and access control for your applications. For more information, see Access Control.