

Citrix XenApp and XenDesktop 7.x Deployment

<https://campus.barracuda.com/doc/41112214/>

Follow the steps in this guide to deploy the Barracuda Load Balancer ADC to increase the scalability and reliability of your Citrix XenApp and 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(s) 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 7.x with the Barracuda Load Balancer ADC, you need the following:

- Barracuda Load Balancer ADC version 5.1 or higher
- Citrix XenApp 7.x or XenDesktop 7.x
- Windows Server 2012 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 types of traffic that are 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 <i>and</i> CITRIX_HTTPS service.

Step 1. Configure the XenApp and XenDesktop Servers

Set up at least two Citrix XenApp and XenDesktop servers in a server group configuration and license both servers. Ensure that the Citrix Store Front is properly configured. HTTP is enabled 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

Step 2A. Create Citrix StoreFront Service

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

- The PORT RANGE service is not implemented for ICA StoreFront config. The display service will not have the service port range enabled because of this.
- Currently, ports are added as part of Response Body Rewrite Rules.
- The Auto ICA rule names should not be changed because the functionality may get distorted.

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.

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	<ul style="list-style-type: none"> • Testing Method: Simple HTTP • HTTP Method: HEAD • Test Target: /Citrix/StoreWeb • 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	<ul style="list-style-type: none"> • Testing Method: Simple HTTPS • HTTP Method: HEAD • Test Target: /Citrix/StoreWeb • 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	<ul style="list-style-type: none"> • Testing Method: Simple HTTP • HTTP Method: HEAD • Test Target: /Citrix/StoreWeb • Additional Headers: User-Agent: Barracuda Load Balancer ADC Server Monitor • Status Code: 200 • Test Delay: 30 Seconds

1. 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.
2. Click **Create**.

Note that Step 2B and Step 3 configuration is not required when clients connect XenApp servers

directly from the internal network.

Step 2B. Create Display Service

Name	Type	IP Address	Port	Session Timeout	Server Monitor
CITRIX_DISPLAY	TCPPROXY	VIP address for the Citrix service For example: 10.5.7.193	2598	0	Testing method: TCP PORT check

Specify these settings in the **Load Balancing** section:

1. For **Algorithm**, select **Weighted Round Robin**.
2. For **Persistence Type**, select **None**.

Step 3. Configure Citrix XenApp Server

After adding your Citrix XenApp servers to your service, you should configure Citrix Xen App/Desktop deployment settings for client to send XenApp traffic ADC to external users/internal users.

1. Navigate to **ADVANCED > System Configuration > StoreFront Settings**.
2. Specify the details for the following fields.
 1. **Secure Web Connection Service** - Select one of the service **CITRIX_HTTP/ CITRIX_HTTPS/CITRIX_INSTSSL** as the storefront secure web connection service.
 2. **ICA Display Service** - Select **CITRIX_DISPLAY** as the display service.
 3. **ICA Display Service Public IP** - The public IP of the display service when the service is configured on a private network on ADC.
 4. **ICA Address Search Pattern** - The IP address followed by this pattern in the ICA file that is used to persist the traffic to the Xen App/Desktop servers. The default value is **Address=**.
 5. **Dual ADC Storefront Configuration** - Select **No**.
3. Click **Save**

Step 4. Add the Real Servers

Add your Citrix servers to your services. Configure each Citrix server as follows:

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 5. 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 and XenDesktop 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 6. Verify Your Configuration

Go to the Citrix Store Front 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/StoreWeb

Next Steps

You can configure authentication and access control for your applications. For more information, see [Access Control](#).

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.