



FortiADC - Server Load Balance General Deployment Guide

Version 5.4.0

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/support-and-training/training.html>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://fortiguard.com/>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



February 4, 2020

FortiADC 5.4.0 Server Load Balance General Deployment Guide

00-540-000000-20200204

TABLE OF CONTENTS

Change Log	4
Introduction	5
Server load balance	6
Server Load Balance overview	6

Change Log

Date	Change Description
12/2/2019	First release.

Introduction

This guide details the steps required to configure a Layer 7 load balance server in FortiADC. It covers the common concept for configuration of load balance profile, load balance method and load balance pool. For other optional features information, please also refer to the relevant deployment guide.

Server load balance

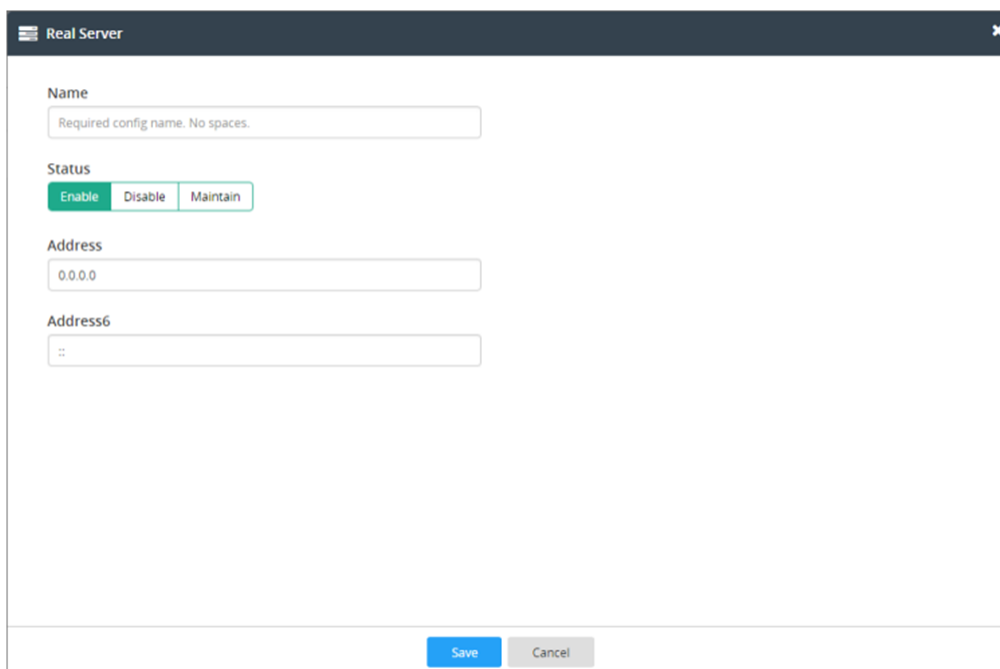
Server Load Balance overview

FortiADC provides two options for configuring virtual servers—Basic Mode and Advanced Mode. In this document we will provide a step by step example for you to deploy load balance based on Advanced mode.

Example

1. Configure a load-balance real server.

Go to **Server Load Balance > Real Server Pool**, and click the **Real Server tab**.



The screenshot shows the 'Real Server' configuration window in FortiADC. The window has a dark header with a hamburger menu icon, the text 'Real Server', and a close button (X). The main content area contains the following fields and controls:

- Name:** A text input field with a placeholder text 'Required config name. No spaces.'
- Status:** Three buttons: 'Enable' (highlighted in green), 'Disable', and 'Maintain'.
- Address:** A text input field containing '0.0.0.0'.
- Address6:** A text input field containing '::'.

At the bottom of the window, there are two buttons: 'Save' (highlighted in blue) and 'Cancel' (greyed out).

2. Configure a load-balance pool

Go to **Server Load Balance > Real Server Pool**, click the **Real Server Pool tab**.

- Set name, address type and Health Check as desired.
- If your real web server is using an http server, leave Real Server SSL Profile as NONE. If your real web server uses an https server, set Real Server SSL Profile as desired.

Then add pool members.

For all detailed setting please check CLI reference [config load-balance pool](#).

For Pool member weight, please see below:

Pool member weight	<p>Assigns relative preference among members—higher values are preferred and are assigned connections more frequently. The default is 1. The valid range is 1 to 256.</p> <p>All load balancing methods consider weight. Servers are dispatched requests proportional to their weight, relative to the sum of all weights.</p>
--------------------	--



The following example shows the effect of weight on Round Robin:
 RealServer1-weight: 1, RealServer2-weight: 2, RealServer3-weight: 3;
 If there are in total 60 connections coming to the virtual server, there should be 10 connections to RealServer1, 20 connections to RealServer2, 30 connections to RealServer3.

For other methods, weight functions as a tie-breaker. For example, with the Least Connection algorithm, requests are sent to the server with the least connections. If the number of connections is equal, the request is sent to the server with the greater weight.

Example

RealServer A, Weight 1, 1 connection

RealServer B, Weight 2, 1 connection

The next request is sent to RealServer B.

3. Config load-balance Method. The system includes predefined configuration objects for all supported load balancing methods, and there is no need to create additional configuration objects. You may choose to do so, however, for various reasons.

Go to **Server Load Balance > application resources**, click the **LB Method tab**.

☰
LB Method

Name

Type

For detailed settings please check the CLI reference [config load-balance method](#).

4. Configure a load-balance Profile.

A profile is a configuration object that defines how you want the FortiADC virtual server to handle traffic for specific protocols.

The system includes predefined configuration objects for all supported load balancing profile, and there is no need to create additional configuration objects. You may choose to do so, however, for various reasons.

Go to **Server Load Balance > application resources**, click the **Application Profile tab**.

Application Profile

Name
Required config name. No spaces.

Type
HTTP

Specifics

Client Timeout
50
Default: 50 Range: 1-3600 seconds

Server Timeout
50
Default: 50 Range: 1-3600 seconds

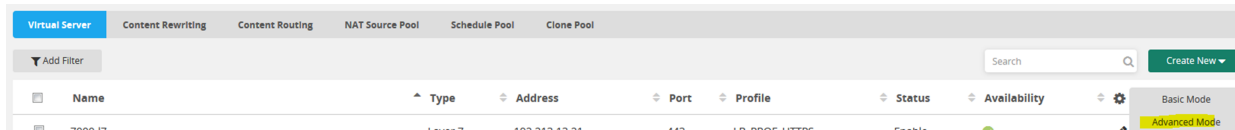
Connect Timeout
5
Default: 5 Range: 1-3600 seconds

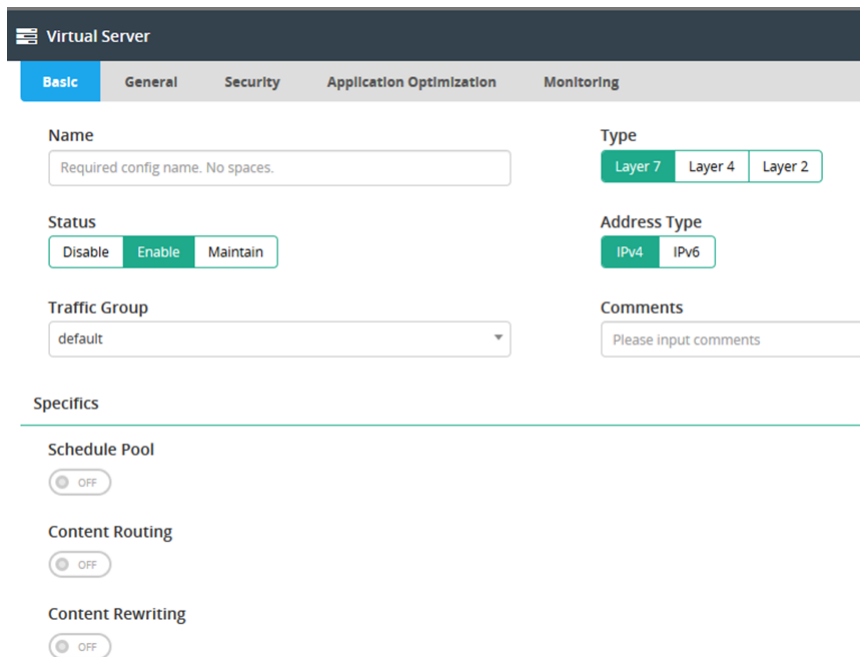
Queue Timeout
5

For all detail setting please check CLI reference [config load-balance profile](#).

5. Configure a load-balance virtual server

Go to **Server Load Balance > Virtual Server > Virtual Server tab**, click **Create New** button, select **Advanced Mode**.





For detailed settings please check CLI reference [config load-balance virtual-server](#). The document only provides the items that must be configured.

More information

For more information, see the following pages:

- Example for Layer 7 HTTPS virtual server

Please see “FortiADC Server Load Balance SSL Deployment Guide”:

<https://docs.fortinet.com/document/fortiadc/5.3.0/server-load-balance-ssl-deployment-guide>

- Example for Layer 4 virtual server

Please see “FortiADC SLB Layer 4 Deployment Guide”:

<https://docs.fortinet.com/document/fortiadc/5.3.0/server-load-balance-layer-4-deployment-guide/153989/introduction>

- Example: NAT46 (Layer 7 virtual servers)

<https://docs.fortinet.com/document/fortiadc/5.3.0/handbook/630669/using-source-pools>

- Example: NAT64 (Layer 7 virtual servers)

<https://docs.fortinet.com/document/fortiadc/5.3.0/handbook/630669/using-source-pools>

Other deployment guide for advanced features

- L7VS Content Rewriting Deployment Guide:
<https://docs.fortinet.com/document/fortiadc/5.2.0/fortiadcdseriesfortiadcl7vscontentrewritingdeploymentguide>
- L7VS Content Routing Deployment Guide:

<https://docs.fortinet.com/document/fortiadc/5.2.0/l7vs-content-routing-deployment-guide>

- L7VS with SSO Authentication Relay Deployment Guide:

<https://docs.fortinet.com/document/fortiadc/5.2.0/fortiadcseriesfortiadcl7vswithssoauthenticationrelaydeploymentguide>

- L7VS Kerberos Deployment Guide:

<https://docs.fortinet.com/document/fortiadc/5.2.0/fortiadcseriesfortiadcl7vskerberosdeploymentguide>

- L7SLB Virtual Server with AntiVirus Deployment Guide

<https://docs.fortinet.com/document/fortiadc/5.2.0/fortiadcseriesfortiadcl7slbvirtualserverwithantivirusdeploymentguide>



FORTINET[®]



Copyright© 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.