Progress®
Kemp® LoadMaster®

Deployment Guide Progress Application Server for OpenEdge

Generated on: 16 September 2024

Copyright

Visit the following page online to see Progress Software Corporation's current Product Documentation Copyright Notice/Trademark Legend: Product Documentation Copyright Notice & Trademarks | Progress

Table of Contents

Chapter 1: Introduction 4

Document Purpose 4

Intended Audience 5

Chapter 2: Template 6

Chapter 3: Architecture 7

Chapter 4: Configure the LoadMaster 9

Enable Subnet Originating Requests Globally 9

Chapter 5: Virtual Services 11

Create the PASOE HTTP Virtual Service 12

PASOE HTTP Source IP Virtual Service Recommended Settings (optional). 13

PASOE HTTP JSESSIONID Cookie Virtual Service Recommended Settings (optional). . . . 14

Create the PASOE HTTPS Offloaded Virtual Service 15

PASOE HTTPS Offloaded Source IP Virtual Service Recommended Settings (optional) . . . 16

PASOE HTTPS Offloaded JSESSIONID Cookie Virtual Service Recommended Settings (optional). 17

Create the PASOE HTTPS ReEncrypt Virtual Service 19

PASOE HTTPS ReEncrypt Source IP Virtual Service Recommended Settings (optional) . . 20

PASOE HTTPS ReEncrypt JSESSIONID Cookie Virtual Service Recommended Settings (optional). 21

1

Introduction

Introduction

Progress Application Server for OpenEdge (PASOE), built upon the industry standard Apache Tomcat web server, delivers an efficient, highly scalable, and secure application server. This innovative application server allows organizations to modernize experiences and limit security vulnerabilities.

The LoadMaster delivers an exceptional, cost effective, and easy to use solution which, by employing intelligent server health checking, optimized performance, security and automatic failover can support an always-on application experience for PASOE.

Related Links

- Document Purpose
- Intended Audience

Document Purpose

Document Purpose

This document provides the recommended LoadMaster settings used when providing high availability, optimization and security for PASOE. The Progress Kemp Support team is available to provide solutions for scenarios not explicitly defined. The Progress Kemp Support site can be found at: https://support.kemptechnologies.com.

Intended Audience

Intended Audience

This document is intended to be read by anyone who is interested in configuring the LoadMaster to optimize Progress Application Server for OpenEdge (PASOE).

2

Template

Template

Progress Kemp has developed a template containing our recommended settings for this workload. You can install this template to help create Virtual Services (VSs) because it automatically populates the settings. You can use the template to easily create the required VSs with the recommended settings. For some workloads, additional manual steps may be required such as assigning a certificate or applying port following. These steps are covered in the document, if needed.

You can remove templates after use and this will not affect deployed services. If needed, you can make changes to any of the VS settings after using the template.

Download released templates from the following page: LoadMaster Templates.

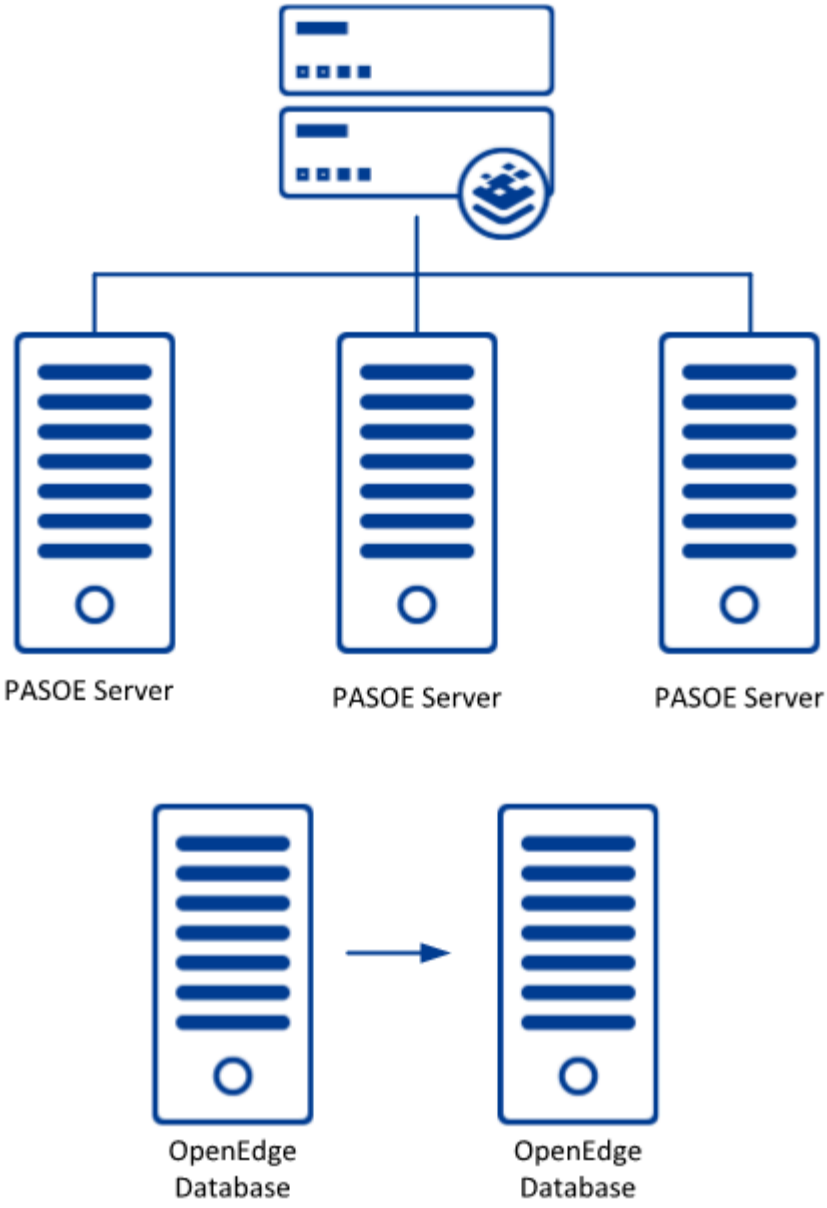
For more information and steps on how to import and use templates, refer to the Virtual Services and Templates, Feature Description.

3

Architecture

Architecture

PASOE deployments consist of 2 or more servers running the PASOE and a back-end database server (set up with High Availability recommended).


PASOE Server
PASOE Server
PASOE Server
OpenEdge Database
OpenEdge Database

4

Configure the LoadMaster

Configure the LoadMaster

Refer to the sections below for details on some recommended global settings.

Related Links

- Enable Subnet Originating Requests Globally

Enable Subnet Originating Requests Globally

Enable Subnet Originating Requests Globally

It is best practice to enable the **Subnet Originating Requests** option globally.

In a one-armed setup (where the Virtual Service and Real Servers are on the same network/subnet) **Subnet Originating Requests** is usually not needed. However, enabling **Subnet Originating Requests** should not affect the routing in a one-armed setup.

In a two-armed setup where the Virtual Service is on network/subnet A, for example, and the Real Servers are on network B, **Subnet Originating Requests** should be enabled on LoadMasters with firmware version 7.1-16 and above.



When **Subnet Originating Requests** is enabled, the Real Server sees traffic originating from 10.20.20.21 (LoadMaster eth1 address) and responds correctly in most scenarios.

With **Subnet Originating Requests** disabled, the Real Server sees traffic originating from 10.0.0.15 (LoadMaster Virtual Service address on **eth0**) and responds to **eth0** which could cause asymmetric routing.

When **Subnet Originating Requests** is enabled globally, it is automatically enabled on all Virtual Services. If the **Subnet Originating Requests** option is disabled globally, you can choose whether to enable **Subnet Originating Requests** on a per-Virtual Service basis.

To enable **Subnet Originating Requests** globally, follow the steps below:

1. In the main menu of the LoadMaster User Interface (UI), go to **System Configuration > Miscellaneous Options > Network Options**.
2. Select the **Subnet Originating Requests** check box.

5

Virtual Services

Virtual Services

This step-by-step setup of Virtual Services (VSs) leverages the Progress Kemp application template for Progress Application Server for OpenEdge (PASOE).

Note: Progress Application Server for OpenEdge (PASOE) can be published with different configuration options dependent on the customer requirements. In many cases if anonymous access or basic authentication is used for PASOE, using Source IP Persistence is supported. However, if Forms Based Authentication is leveraged for PASOE, Active Cookie Persistence is recommended.

Note: The PASOE template is using HTTP/HTTPS health checking along with the default PASOE default TCP port numbers. If enabled on the PASOE environment, OpenEdge Ping can be leveraged to provide more advanced health checking. This advanced health checking will be determined on how OpenEdge Ping is configured within PASOE environment.

The table in each section outlines the settings configured by the application template. You can use this information to manually configure Virtual Services or use the LoadMaster Application Programming Interface (API) and automation tools.

Note: This document assumes an SSL/TLS certificate has already been installed on the LoadMaster. For more information on adding SSL/TLS Certificates reference the SSL Accelerated Services, Feature Description.

Related Links

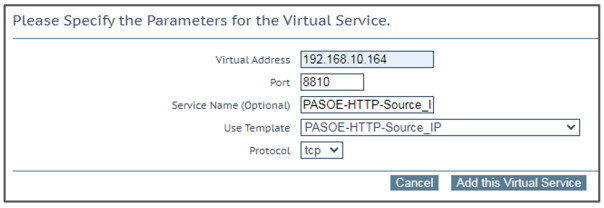
- Create the PASOE HTTP Virtual Service
- Create the PASOE HTTPS Offloaded Virtual Service
- Create the PASOE HTTPS ReEncrypt Virtual Service

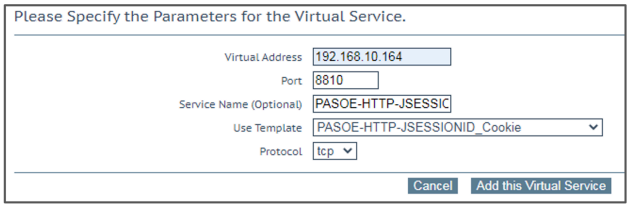
Create the PASOE HTTP Virtual Service

Create the PASOE HTTP Virtual Service

The following are the steps involved and the recommended settings to configure the PASOE HTTP Virtual Service.

1. In the main menu of the LoadMaster User Interface (UI), go to **Virtual Services > Add New**.





2. Type a valid **Virtual Address**.
3. Select the **PASOE-HTTP-Source_IP** or **PASOE-HTTP-JSESSIONID_Cookie** template in the **Use Template** drop-down list depending on what persistence method is required. (Refer to the note in the Virtual Services section for recommendations about the persistence method.)
4. Click **Add this Virtual Service**.
5. Expand the **Real Servers** section.
6. Click **Add New**.
7. Type the **Real Server Address**.
8. Click **Add This Real Server**.
9. Repeat these steps to add more Real Servers as needed.

Related Links

- PASOE HTTP Source IP Virtual Service Recommended Settings (optional)
- PASOE HTTP JSESSIONID Cookie Virtual Service Recommended Settings (optional)

PASOE HTTP Source IP Virtual Service Recommended Settings (optional)

PASOE HTTP Source IP Virtual Service Recommended Settings (optional)

This table outlines the recommended settings set using the Progress Kemp application template. You can use the API parameters and values with scripts and automation tools.

API Parameter	API Value	WUI Field Name	WUI Field Value
port	8810	Port	8810
prot	tcp	Protocol	tcp
VStype	http	Service Type	HTTP-HTTP/2-HTTPS
SubnetOriginating	1	Subnet Originating Requests	Enabled
Forcel7	1	Force L4	Disabled
Schedule	lc	Scheduling Method	least connection
Persist	src	Persistence Options	Source IP Address
PersistTimeout	360	Timeout	6 Minutes
CheckType	http	Real Server Check Method	HTTP Protocol
CheckUseGet	1	HTTP Method	GET

API Parameter	API Value	WUI Field Name	WUI Field Value
CheckPort	8810	Checked Port	8810

PASOE HTTP JSESSIONID Cookie Virtual Service Recommended Settings (optional)

PASOE HTTP JSESSIONID Cookie Virtual Service Recommended Settings (optional)

This table outlines the recommended settings set using the Progress Kemp application template. You can use the API parameters and values with scripts and automation tools.

API Parameter	API Value	WUI Field Name	WUI Field Value
port	8810	Port	8810
prot	tcp	Protocol	tcp
VStype	http	Service Type	HTTP-HTTP/2-HTTPS
SubnetOriginating	1	Subnet Originating Requests	Enabled
Forcel7	1	Force L4	Disabled
Schedule	lc	Scheduling Method	least connection
Persist	server-cookie	Persistence Options	Server Cookie
PersistTimeout	360	Timeout	6 Minutes

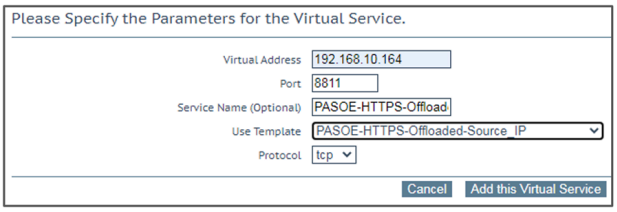
API Parameter	API Value	WUI Field Name	WUI Field Value
Cookie	JSESSIONID	Cookie Name	JSESSIONID
CheckType	http	Real Server Check Method	HTTP Protocol
CheckUseGet	1	HTTP Method	GET
CheckPort	8810	Checked Port	8810

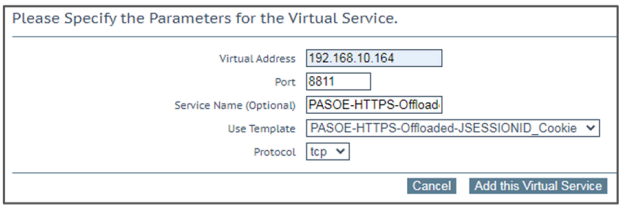
Create the PASOE HTTPS Offloaded Virtual Service

Create the PASOE HTTPS Offloaded Virtual Service

The following are the steps involved and the recommended settings to configure the PASOE HTTPS Offloaded Virtual Service.

1. In the main menu of the LoadMaster User Interface (UI), go to **Virtual Services > Add New**.





2. Type a valid **Virtual Address**.
3. Select the **PASOE-HTTPS-Offloaded-Source_IP** or **PASOE-HTTP-Offloaded-JSESSIONID_Cookie** template in the **Use Template** drop-down list depending on what persistence method is required. (Refer to the note in the Virtual Services section for recommendations about the persistence method.)
4. Click **Add this Virtual Service**.
5. Expand the **SSL Properties** section.
6. Select the certificate to use from **Available Certificates** and click the arrow (>) to move it to **Assigned Certificates**.
7. Expand the **Real Servers** section.
8. Click **Add New**.

9. Type the **Real Server Address**.
10. Click **Add This Real Server**.
11. Repeat these steps to add more Real Servers as needed.

Related Links

- PASOE HTTPS Offloaded Source IP Virtual Service Recommended Settings (optional)
- PASOE HTTPS Offloaded JSESSIONID Cookie Virtual Service Recommended Settings (optional)

PASOE HTTPS Offloaded Source IP Virtual Service Recommended Settings (optional)

PASOE HTTPS Offloaded Source IP Virtual Service Recommended Settings (optional)

This table outlines the recommended settings set using the Progress Kemp application template. You can use the API parameters and values with scripts and automation tools.

API Parameter	API Value	WUI Field Name	WUI Field Value
port	8811	Port	8811
prot	tcp	Protocol	tcp
VStype	http	Service Type	HTTP-HTTP/2-HTTPS
SubnetOriginating	1	Subnet Originating Requests	Enabled
Forcel7	1	Force L4	Disabled
Schedule	lc	Scheduling Method	least connection
Persist	src	Persistence Options	Source IP Address

API Parameter	API Value	WUI Field Name	WUI Field Value
PersistTimeout	360	Timeout	6 Minutes
SSLAcceleration	1	SSL Acceleration	Enabled
TLSType	1	Supported Protocols	TLS1.0, TLS1.1, TLS1.2, and TLS1.3 (Enabled)
CipherSet	BestPractices	Cipher Set	BestPractices
CheckType	http	Real Server Check Method	HTTP Protocol
CheckUseGet	1	HTTP Method	GET
CheckPort	8810	Checked Port	8810

PASOE HTTPS Offloaded JSESSIONID Cookie Virtual Service Recommended Settings (optional)

PASOE HTTPS Offloaded JSESSIONID Cookie Virtual Service Recommended Settings (optional)

This table outlines the recommended settings set using the Progress Kemp application template. You can use the API parameters and values with scripts and automation tools.

API Parameter	API Value	WUI Field Name	WUI Field Value
port	8811	Port	8811
prot	tcp	Protocol	tcp

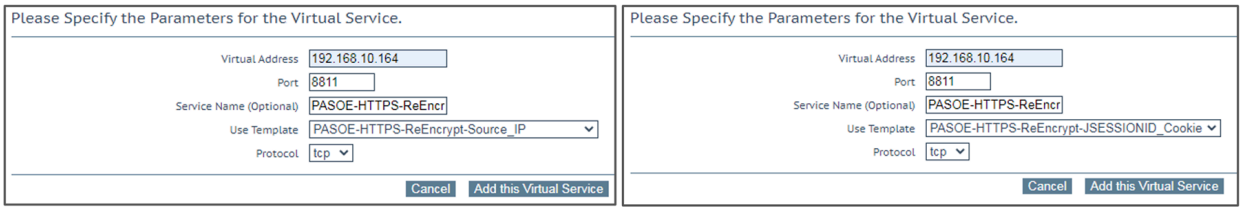
API Parameter	API Value	WUI Field Name	WUI Field Value
VStype	http	Service Type	HTTP-HTTP/2-HTTPS
SubnetOriginating	1	Subnet Originating Requests	Enabled
Forcel7	1	Force L4	Disabled
Schedule	lc	Scheduling Method	least connection
Persist	server-cookie	Persistence Options	Server Cookie
PersistTimeout	360	Timeout	6 Minutes
Cookie	JSESSIONID	Cookie Name	JSESSIONID
SSLAcceleration	1	SSL Acceleration	Enabled
TLSType	1	Supported Protocols	TLS1.0, TLS1.1, TLS1.2, and TLS1.3 (Enabled)
CipherSet	BestPractices	Cipher Set	BestPractices
CheckType	http	Real Server Check Method	HTTP Protocol
CheckUseGet	1	HTTP Method	GET
CheckPort	8810	Checked Port	8810

Create the PASOE HTTPS ReEncrypt Virtual Service

Create the PASOE HTTPS ReEncrypt Virtual Service

The following are the steps involved and the recommended settings to configure the PASOE HTTPS ReEncrypt Virtual Service.

1. In the main menu of the LoadMaster User Interface (UI), go to **Virtual Services > Add New**.



2. Type a valid **Virtual Address**.
3. Select the **PASOE-HTTPS-ReEncrypt-Source_IP** or **PASOE-HTTP- ReEncrypt -JSESSIONID_Cookie** template in the **Use Template** drop-down list depending on what persistence method is required. (Refer to the note in the Virtual Services section for recommendations about the persistence method.)
4. Click **Add this Virtual Service**.
5. Expand the **SSL Properties** section.
6. Select the certificate to use from **Available Certificates** and click the arrow (>) to move it to **Assigned Certificates**.
7. Expand the **Real Servers** section.
8. Click **Add New**.
9. Type the **Real Server Address**.
10. Click **Add This Real Server**.
11. Repeat these steps to add more Real Servers as needed.

Related Links

- PASOE HTTPS ReEncrypt Source IP Virtual Service Recommended Settings (optional)
- PASOE HTTPS ReEncrypt JSESSIONID Cookie Virtual Service Recommended Settings (optional)

PASOE HTTPS ReEncrypt Source IP Virtual Service Recommended Settings (optional)

PASOE HTTPS ReEncrypt Source IP Virtual Service Recommended Settings (optional)

This table outlines the recommended settings set using the Progress Kemp application template. You can use the API parameters and values with scripts and automation tools.

API Parameter	API Value	WUI Field Name	WUI Field Value
port	8811	Port	8811
prot	tcp	Protocol	tcp
VStype	http	Service Type	HTTP-HTTP/2-HTTPS
SubnetOriginating	1	Subnet Originating Requests	Enabled
Forcel7	1	Force L4	Disabled
Schedule	lc	Scheduling Method	least connection
Persist	src	Persistence Options	Source IP Address
PersistTimeout	360	Timeout	6 Minutes
SSLAcceleration	1	SSL Acceleration	Enabled
SSLReencrypt	1	Reencrypt	Enabled

API Parameter	API Value	WUI Field Name	WUI Field Value
TLSType	1	Supported Protocols	TLS1.0, TLS1.1, TLS1.2, and TLS1.3 (Enabled)
CipherSet	BestPractices	Cipher Set	BestPractices
CheckType	http	Real Server Check Method	HTTP Protocol
CheckUseGet	1	HTTP Method	GET
CheckPort	8811	Checked Port	8811

PASOE HTTPS ReEncrypt JSESSIONID Cookie Virtual Service Recommended Settings (optional)

PASOE HTTPS ReEncrypt JSESSIONID Cookie Virtual Service Recommended Settings (optional)

This table outlines the recommended settings set using the Progress Kemp application template. You can use the API parameters and values with scripts and automation tools.

API Parameter	API Value	WUI Field Name	WUI Field Value
port	8811	Port	8811
prot	tcp	Protocol	tcp
VStype	http	Service Type	HTTP-HTTP/2-HTTPS
SubnetOriginating	1	Subnet Originating Requests	Enabled

API Parameter	API Value	WUI Field Name	WUI Field Value
Forcel7	1	Force L4	Disabled
Schedule	lc	Scheduling Method	least connection
Persist	server-cookie	Persistence Options	Server Cookie
PersistTimeout	360	Timeout	6 Minutes
Cookie	JSESSIONID	Cookie Name	JSESSIONID
SSLAcceleration	1	SSL Acceleration	Enabled
SSLReencrypt	1	Reencrypt	Enabled
TLSType	1	Supported Protocols	TLS1.0, TLS1.1, TLS1.2, and TLS1.3 (Enabled)
CipherSet	BestPractices	Cipher Set	BestPractices
CheckType	http	Real Server Check Method	HTTP Protocol
CheckUseGet	1	HTTP Method	GET
CheckPort	8811	Checked Port	8811