Progress®
Kemp® LoadMaster®

Deployment Guide FujiFilm Synapse

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 5
Document Purpose 6
Intended Audience 6

Chapter 2: Template 7

Chapter 3: Enable Subnet Originating Requests Globally 8

Chapter 4: Synapse Virtual Services Configuration 10
Create Fujifilm Synapse Virtual Services 10
Configure the Synapse HTTP Virtual Service 11
Configure the Synapse DICOM Virtual Service 12
Configure the Synapse External Virtual Service. 14

Chapter 5: Adaptive Agent Configuration 16

Chapter 6: Health Checking. 17

Chapter 7: Additional Features 18

Chapter 8: References 19

1

Introduction

Introduction

Synapse is Fujifilm's Picture Archiving and Communication System (PACS). It allows filmless diagnosis with high quality image processing. Synapse allows the archiving and distribution of vast amounts of image information from all modalities, managing it with a single system.

Such a powerful tool requires reliable and powerful support. The LoadMaster delivers an exceptional, cost-effective and easy to use solution which, by employing Adaptive Load Balancing, balances requests across Synapse. Synapse consists of the following servers:

- Database Server
- Windows Internet Information Server (IIS)
- Storage Server
- Digital Imaging and Communications in Medicine (DICOM) Server
- Hospital Information System (HIS) Server

When deployed as a pair, two LoadMasters give the security of High Availability (HA). HA allows two physical or virtual machines to become one logical device. Only one of these units is ever handling traffic at any particular moment. One unit is active and the other is a hot standby (passive). This provides redundancy and resiliency, meaning if one LoadMaster goes down for any reason, the hot standby can become active, therefore avoiding any downtime.

Related Links

- Document Purpose

- Intended Audience

Document Purpose

Document Purpose

This document is intended to provide guidance on how to deploy Synapse with a LoadMaster. The Progress Kemp Support Team is available to provide solutions for scenarios not explicitly defined.

Intended Audience

Intended Audience

This document is intended to be used by anyone deploying Synapse with a LoadMaster.

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

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.

4

Synapse Virtual Services Configuration

Synapse Virtual Services Configuration

Note: The LoadMaster uses Adaptive Agent Load Balancing to distribute the various requests received. The LoadMaster recognizes that requests received on different ports are different types of requests.

Refer to the following sections for step-by-step instructions on creating and configuring Fujifilm Synapse Virtual Services.

Related Links

- Create Fujifilm Synapse Virtual Services

Create Fujifilm Synapse Virtual Services

Create Fujifilm Synapse Virtual Services

When deploying Fujifilm Synapse, three Virtual Services must be configured.

Related Links

- Configure the Synapse HTTP Virtual Service
- Configure the Synapse DICOM Virtual Service

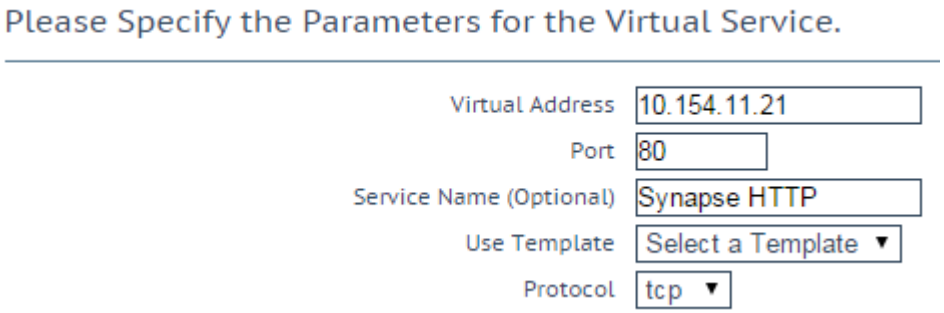
- Configure the Synapse External Virtual Service

Configure the Synapse HTTP Virtual Service

Configure the Synapse HTTP Virtual Service

The following are the steps involved and the values required to set up the first of the Fujifilm Synapse Virtual Services:

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



2. Enter a valid IP address in the **Virtual Address** text box.
3. Enter **80** in the **Port** text box.

Note: HTTP requests received on Port 80 and external (HTTPS) requests on Port 443 are distributed to their most available server in the same adaptive manner.

4. Enter a recognizable **Service Name**, for example **Synapse HTTP**.
5. Ensure **tcp** is selected as the **Protocol**.
6. Click **Add this Virtual Service**.
7. Configure the settings as recommended in the following table:

Section	Option	Value
Standard Options	Transparency	Disabled
	Subnet Originating Requests	Enabled
	Persistence Mode	Source IP Address
	Timeout	1 Hour
	Scheduling Method	resource based (adaptive)

Section	Option	Value
Advanced Properties	Add HTTP Headers	None
Real Servers	Real Server Check Method	HTTP Protocol

8. Add the Real Servers:
   1. Click the **Add New** button.
   2. Enter the **Real Server Address**.

      Note: This is the address of the backend server.

   3. Enter **80** as the **Port**.

      Note: The Real Server **Port** should match the Virtual Service **Port**.

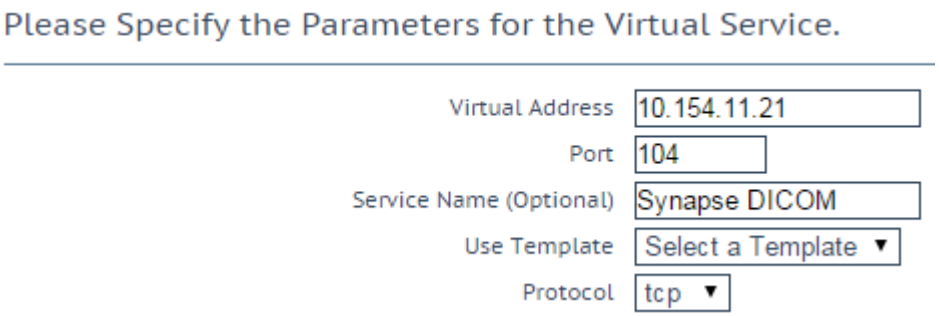
      Note: The **Forwarding method** and **Weight** values are set by default. These can be changed by an administrator.

   4. Click **Add this Real Server**. Click **OK** to the pop-up message.
   5. Repeat the steps above to add more Real Servers as needed, based on the environment.

Configure the Synapse DICOM Virtual Service

Configure the Synapse DICOM Virtual Service

1. The following are the steps involved and the values required to set up the second of the Fujifilm Synapse Virtual Services:
2. In the LoadMaster Web User Interface (WUI) main menu, go to **Virtual Services > Add New**.



3. Enter the same IP address in the **Virtual Address** text box as you did when setting up the Synapse HTTP Virtual Service in the Configure the Synapse HTTP Virtual Service section.
4. Enter **104** in the **Port** text box.

   Note: TCP connections on port 104 are recognized as DICOM requests and are forwarded to the

DICOM server which the LoadMaster determines is the most available based on processor and memory utilization.

5. Enter a recognizable **Service Name**, for example **Synapse DICOM**.
6. Ensure **TCP** is selected as the **Protocol**.
7. Click **Add this Virtual Service**.
8. Configure the settings as recommended in the following table:

Section	Option	Value
Basic Properties	Service Name	HTTP/HTTPS
Standard Options	Transparency	Disabled
	Subnet Originating Requests	Enabled
	Persistence Mode	Source IP Address
	Timeout	1 Hour
	Scheduling Method	resource based (adaptive)
Advanced Properties	Added HTTP Headers	None
Real Servers	Real Server Check Method	TCP Connection Only

9. Add the Real Servers:
   1. Click the **Add New** button.
   2. Enter the **Real Server Address**.

      Note: This is the address of the backend server.

   3. Enter **104** as the **Port**.

      Note: The Real Server **Port** should match the Virtual Service **Port**.

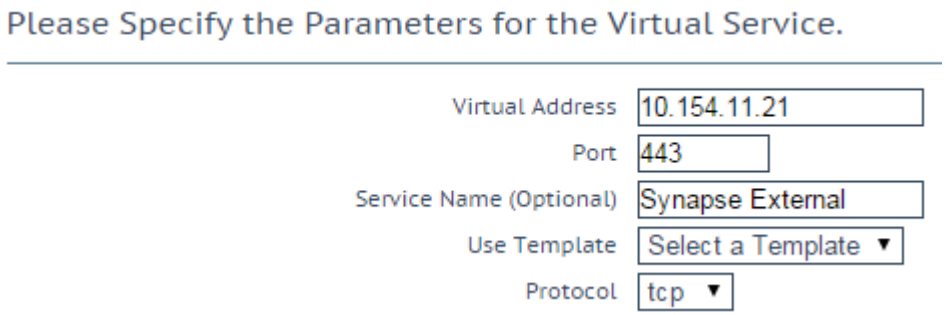
      Note: The **Forwarding method** and **Weight** values are set by default. These can be changed by an administrator.

   4. Click **Add this Real Server**. Click **OK** to the pop-up message.
   5. Repeat the steps above to add more Real Servers as needed, based on the environment.

Configure the Synapse External Virtual Service

Configure the Synapse External Virtual Service

1. The following are the steps involved and the values required to set up the third Fujifilm Synapse Virtual Service:
2. In the LoadMaster Web User Interface (WUI) main menu, go to **Virtual Services > Add New**.



3. Enter the same IP address in the **Virtual Address** text box as you did when setting up the Synapse HTTP and Synapse DICOM Virtual Services.
4. Enter **443** in the **Port** text box.

Note: HTTP requests received on Port 80 and external (HTTPS) requests on Port 443 are distributed to their most available server in the same adaptive manner.

5. Enter a recognizable **Service Name**, for example **Synapse External**.
6. Ensure **TCP** is selected as the **Protocol**.
7. Click **Add this Virtual Service**.
8. Configure the settings as recommended in the following table:

Section	Option	Value	Comments
SSL Properties	SSL Accelerationt	Enabled	Click **OK** to the pop-up that appears.
	Reencrypt	Enabled	
	Supported Protocols	TLS1.0; TLS1.1; TLS1.2; TLS1.3	While this workload may not support TLS1.3 yet, we recommend enabling it for future proofing.
	Require SNI hostname	Disabled	
	Client Certificates	No Client Certificates	

Section	Option	Value	Comments
		Required	
Standard Options	Subnet Originating Requests	Enabled	
	Persistence Mode	Source IP Address	
	Timeout	1 Hour	
	Scheduling Method	resource based (adaptive)	
Advanced Properties	Added HTTP Headers	None	
Real Servers	Real Server Check Method	HTTPS Protocol	

9. Add the Real Servers:
   1. Click the **Add New** button.
   2. Enter the **Real Server Address**.

      Note: This is the address of the backend server.

   3. Enter **443** as the **Port**.

      Note: The Real Server **Port** should match the Virtual Service **Port**.

      Note: The **Forwarding method** and **Weight** values are set by default. These can be changed by an administrator.

   4. Click **Add this Real Server**. Click **OK** to the pop-up message.
   5. Repeat the steps above to add more Real Servers as needed, based on the environment.

5

Adaptive Agent Configuration

Adaptive Agent Configuration

The configuration of Adaptive Agent is based on the requirements of the actual hardware and Operating System on which Synapse is running.

6

Health Checking

Health Checking

By sending heartbeat checks, the LoadMaster periodically ensures that each of the servers in a deployment is still running. As part of the heartbeat checks, on port 104 the LoadMaster opens a TCP connection to determine if the DICOM server on the Synapse server is still responding.

Note: The LoadMaster does not currently support DICOM Echo health checking.

The LoadMaster can also be configured to test the IIS service. The LoadMaster performs a check over HTTP to the web server. A particular URL to be reached is identified and a value (for example, DB-OK) set for LoadMaster to find. The LoadMaster calls the URL to determine if the database server is running successfully. If it is, the webpage returns a message containing the value. If not, an error message is returned. The LoadMaster can recognize this and looks for this value in every health check it performs.

7

Additional Features

Additional Features

Additional LoadMaster security and optimization features can be enabled for the deployment of SAP. The deployment steps and configuration settings of these features can be found in the documents which are listed in the References section of this document. These documents can be found on the Progress Kemp documentation web page: https://docs.progress.com/category/loadmaster-documentation

- **Edge Security Pack (ESP)** - A solution that provides edge security, SSO application integration and flexible authentication options is critical for optimal user experience and information security policy compliance.
- **Web Application Firewall (WAF)** - This enables secure deployment of web applications, preventing Layer 7 attacks while maintaining core load balancing services which ensures superior application delivery and security.
- **Content Caching** - The LoadMaster can cache static content that fits certain criteria (file extension, query string, caching headers, size, and so on). As long as the file meets these criteria it can be stored locally in the LoadMaster to avoid unnecessary requests to the Real Server to retrieve the file.
- **Intrusion Detection** – The LoadMaster's implementation of Intrusion Detection leverages Snort. Snort is an open source network intrusion prevention and detection system (IDS/IPS). Snort rules can be imported to the LoadMaster and applied to HTTP/HTTPS connections.

8

References

References

Unless otherwise specified, the following documents can be found at https://docs.progress.com/.

Virtual Services and Templates, Feature Description