

SAP

Deployment Guide

UPDATED: 27 July 2023

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

These materials and all Progress® software products are copyrighted and all rights are reserved by Progress Software Corporation. The information in these materials is subject to change without notice, and Progress Software Corporation assumes no responsibility for any errors that may appear therein. The references in these materials to specific platforms supported are subject to change.

#1 Load Balancer in Price/Performance, 360 Central, 360 Vision, Chef, Chef (and design), Chef Habitat, Chef Infra, Code Can (and design), Compliance at Velocity, Corticon, Corticon.js, DataDirect (and design), DataDirect Cloud, DataDirect Connect, DataDirect Connect64, DataDirect XML Converters, DataDirect XQuery, DataRPM, Defrag This, Deliver More Than Expected, DevReach (and design), Driving Network Visibility, Flowmon, Inspec, Ipswitch, iMacros, K (stylized), Kemp, Kemp (and design), Kendo UI, Kinvey, LoadMaster, MessageWay, MOVEit, NativeChat, OpenEdge, Powered by Chef, Powered by Progress, Progress, Progress Software Developers Network, SequeLink, Sitefinity (and Design), Sitefinity, Sitefinity (and design), Sitefinity Insight, SpeedScript, Stylized Design (Arrow/3D Box logo), Stylized Design (C Chef logo), Stylized Design of Samurai, TeamPulse, Telerik, Telerik (and design), Test Studio, WebSpeed, WhatsConfigured, WhatsConnected, WhatsUp, and WS_FTP are registered trademarks of Progress Software Corporation or one of its affiliates or subsidiaries in the U.S. and/or other countries.

Analytics360, AppServer, BusinessEdge, Chef Automate, Chef Compliance, Chef Desktop, Chef Workstation, Corticon Rules, Data Access, DataDirect Autonomous REST Connector, DataDirect Spy, DevCraft, Fiddler, Fiddler Classic, Fiddler Everywhere, Fiddler Jam, FiddlerCap, FiddlerCore, FiddlerScript, Hybrid Data Pipeline, iMail, InstaRelinker, JustAssembly, JustDecompile, JustMock, KendoReact, OpenAccess, PASOE, Pro2, ProDataSet, Progress Results, Progress Software, ProVision, PSE Pro, Push Jobs, SafeSpaceVR, Sitefinity Cloud, Sitefinity CMS, Sitefinity Digital Experience Cloud, Sitefinity Feather, Sitefinity Thunder, SmartBrowser, SmartComponent, SmartDataBrowser, SmartDataObjects, SmartDataView, SmartDialog, SmartFolder, SmartFrame, SmartObjects, SmartPanel, SmartQuery, SmartViewer, SmartWindow, Supermarket, SupportLink, Unite UX, and WebClient are trademarks or service marks of Progress Software Corporation and/or its subsidiaries or affiliates in the U.S. and other countries. Java is a registered trademark of Oracle and/or its affiliates. Any other marks contained herein may be trademarks of their respective owners.

Please refer to the NOTICE.txt or Release Notes – Third-Party Acknowledgements file applicable to a particular Progress product/hosted service offering release for any related required third-party acknowledgements.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Table of Contents

1 Introduction **5**

1.1 Document Purpose 5

1.2 Prerequisites 5

2 Load Balancing SAP **7**

3 Configuring Virtual Services for SAP **10**

3.1 Ports 10

3.1.1 Persistence 10

3.1.2 SSL Acceleration 11

3.1.3 Certificates 13

3.1.3.1 Server Certificates 13

3.1.3.2 Reverse Proxy Client Certificates 13

3.1.3.3 Intermediate Certificates 13

4 Template **14**

5 Enable Subnet Originating Requests Globally **15**

6 Configure the Virtual Service for SAP CRM **16**

6.1 SAP CRM Offloaded 16

6.2 SAP CRM Reencrypted 18

7 Configure the Virtual Service for SAP Enterprise Portal **21**

7.1 SAP Enterprise Portal Offloaded 21

7.2 SAP Enterprise Portal Reencrypted 23

8 Configure the Virtual Services for SAP Business Objects **26**

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

8.1 SAP Business Objects Offloaded 26

8.2 SAP Business Objects Reencrypted 28

9 Additional Features **32**

References **33**

Last Updated Date **34**

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

1 Introduction

Kemp's LoadMaster family of purpose-built hardware and Virtual Appliances (Virtual LoadMaster) offer advanced Layer 4 and Layer 7 server load balancing, content switching, SSL Acceleration and a multitude of other advanced Application Delivery Controller (ADC) and optimization features.

Kemp's LoadMaster fully supports SAP's key solutions and has been certified by SAP. The LoadMaster efficiently distributes user traffic for the SAP workloads so that users get the best performance experience possible. Also, High Availability (HA) and high capacity scale-out deployments of the SAP solutions are complemented from the network technology side.

The entire Kemp LoadMaster product family, including the Virtual LoadMaster (VLM) supports SAP.

For more information about Kemp, visit www.kemptechnologies.com.

1.1 Document Purpose

This document is intended to provide technical guidance on how to configure the Kemp LoadMaster product to provide various Application Delivery network services for SAP application HTTP protocol-based client traffic to SAP backend application systems.

Clients to an SAP backend are typically:

- End users who are using different browser types to work interactively in SAP systems
- Other SAP and non-SAP applications connecting using web-services or RESTful Application Program Interfaces (APIs) to an SAP backend system for application integration scenarios

A particularly important use case of application integration is the integration of new SAP cloud-based solutions which SAP applications customers run in their own "on premise" data centers. This document was created from test experiences and results in a representative sample environment which is described later in the document. As this document is not intended to cover every possible deployment scenario, it may not address unique setup or requirements. The Kemp Support Team is available to provide solutions for scenarios which are not explicitly defined in this document.

1.2 Prerequisites

It is assumed that the reader is a network administrator or a person otherwise familiar with networking and general computer terminology. It is further assumed that the SAP environment has been set up and the Kemp LoadMaster has been installed. A network and an SAP administrator

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

should work together on details which need to be coordinated between network and application configurations.

Other LoadMaster documentation can be referred to as needed from http://www.kemptechnologies.com/documentation.

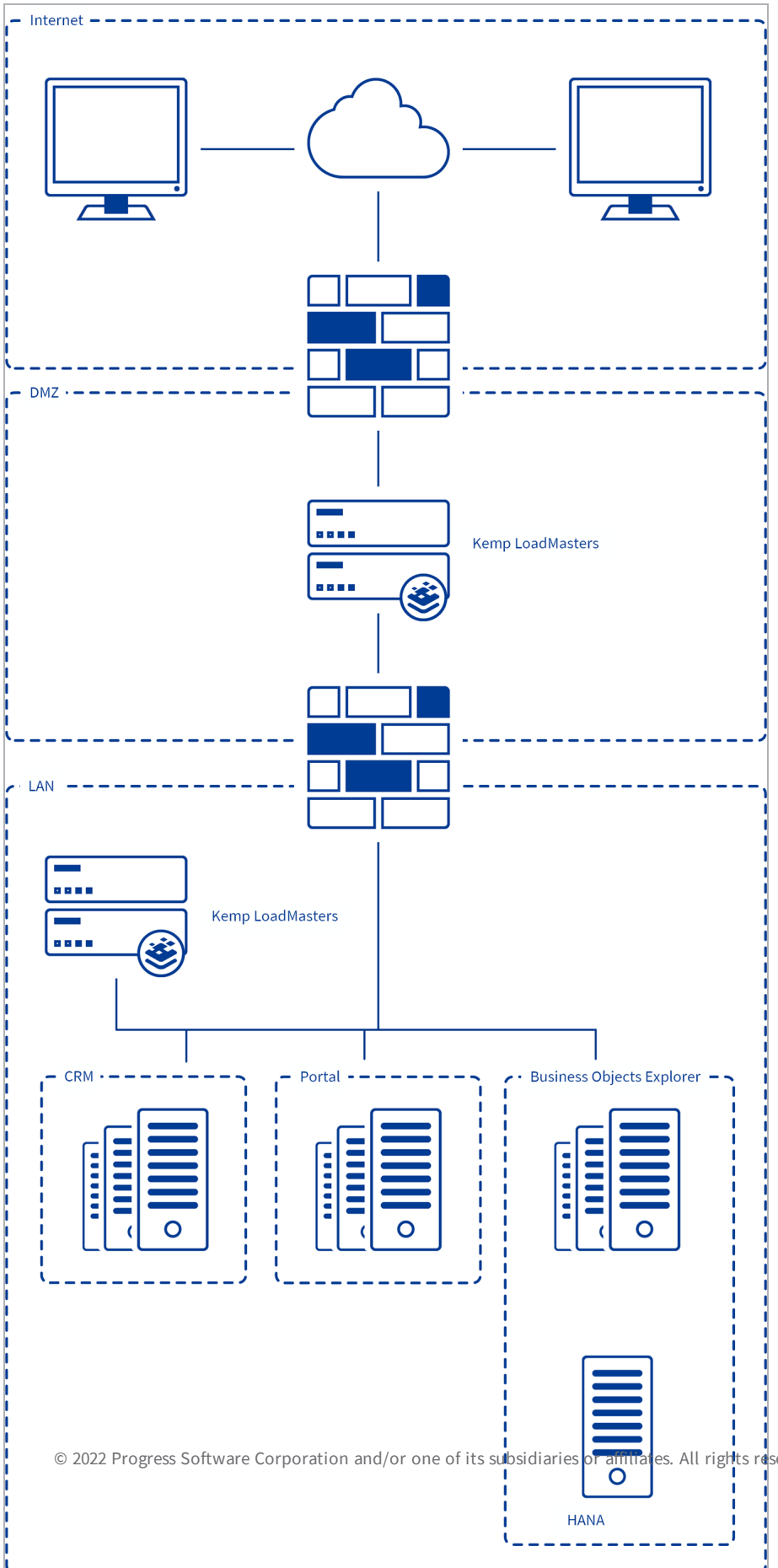
The minimum requirements which should be met before proceeding are as follows:

- LoadMaster firmware version 7.2.48 or above should be installed
- SAP applications should be installed and configured
- Internal and external DNS entries for the SAP applications should be configured
- Access to the LoadMaster Web User Interface (WUI) should be established

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

2 Load Balancing SAP

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.



© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Deploying a SAP environment can require multiple servers to provide High Availability (HA). Load balancing is necessary in this situation to distribute the traffic amongst these servers.

Kemp recommends the configuration as depicted in the above diagram**.** The SAP Customer Relationship Management (CRM) application is depicted as a representative of SAP Business Suite components, which run on the SAP NetWeaver ABAP platform. The SAP NetWeaver Portal is an example of a component running on the NetWeaver Java platform and the SAP Business Object Explorer is a representative of SAP's Business Intelligence (BI) solutions. The LoadMaster should be configured in analogous ways as described in this document for other SAP NetWeaver ABAP and Java and SAP BI solutions. If your configuration differs from the recommended configuration and there are issues deploying the LoadMaster, contact the local Kemp Support Team for assistance.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

3 Configuring Virtual Services for SAP

The below sections provide instructions and recommended configuration options for setting up a Kemp LoadMaster to work with the SAP NetWeaver-based and SAP BI solutions. For clarity, the following applications are used as representative examples:

- SAP CRM on the SAP NetWeaver-ABAP platform
- SAP Enterprise Portal on the NetWeaver-Java platform
- SAP Business Objects Explorer (BOE)

For an explanation of each of the fields mentioned, refer to the Web User Interface, Configuration Guide.

3.1 Ports

In some cases, the ports used for accessing SAP CRM are non-standard to provide better security. In general, all ports used by the SAP backend systems can be freely configured by the SAP application administrator. The standard HTTP 80 and HTTPS 443 ports for Internet-facing traffic are also supported and may be used during the configuration. However, the purpose of an ADC is to provide standard ports 80/443 for the Internet-facing traffic and route that traffic to non-standard ports used on the SAP backend systems as a passive security measure.

3.1.1 Persistence

Persistence provides client connections to the same SAP server node of a scaled out cluster deployment for each subsequent request to the Virtual Service.

Source IP Address Persistence

Source IP Address persistence can be used but take care before enabling it because:

- Clients from behind a Network Address Translation (NAT) device show up as a single IP address
- It can result in uneven connection distribution

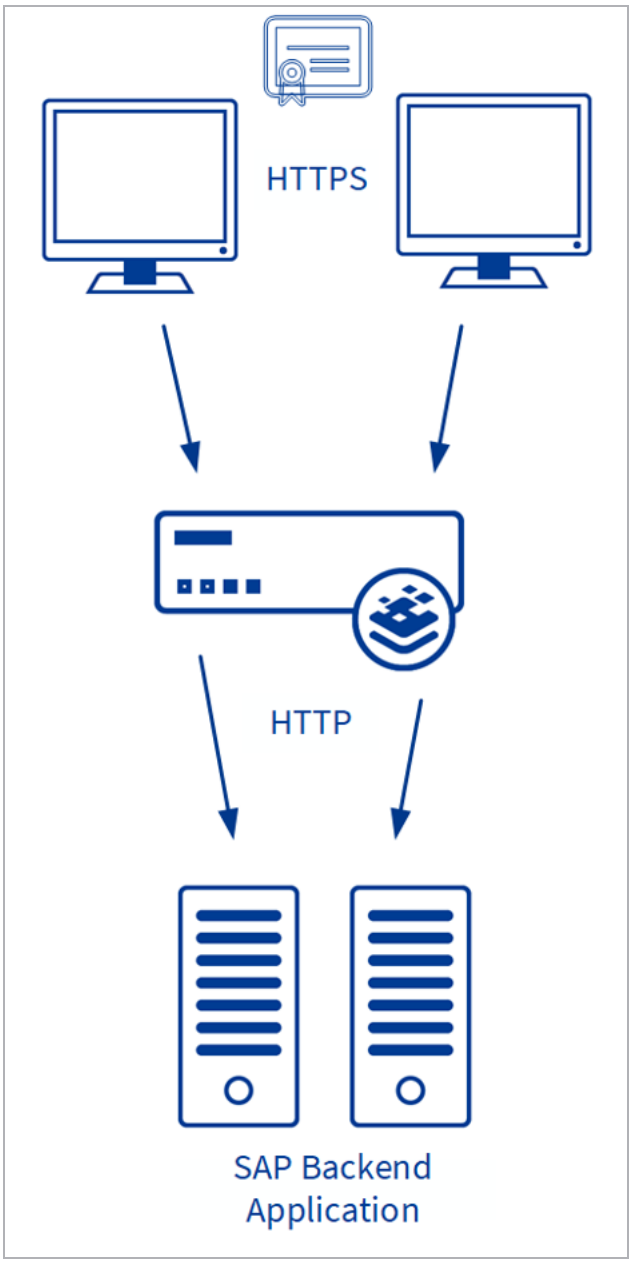
Cookie Persistence

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

If cookies are used, there is no negative impact. The name of the cookie does not have any specific requirements.

3.1.2 SSL Acceleration

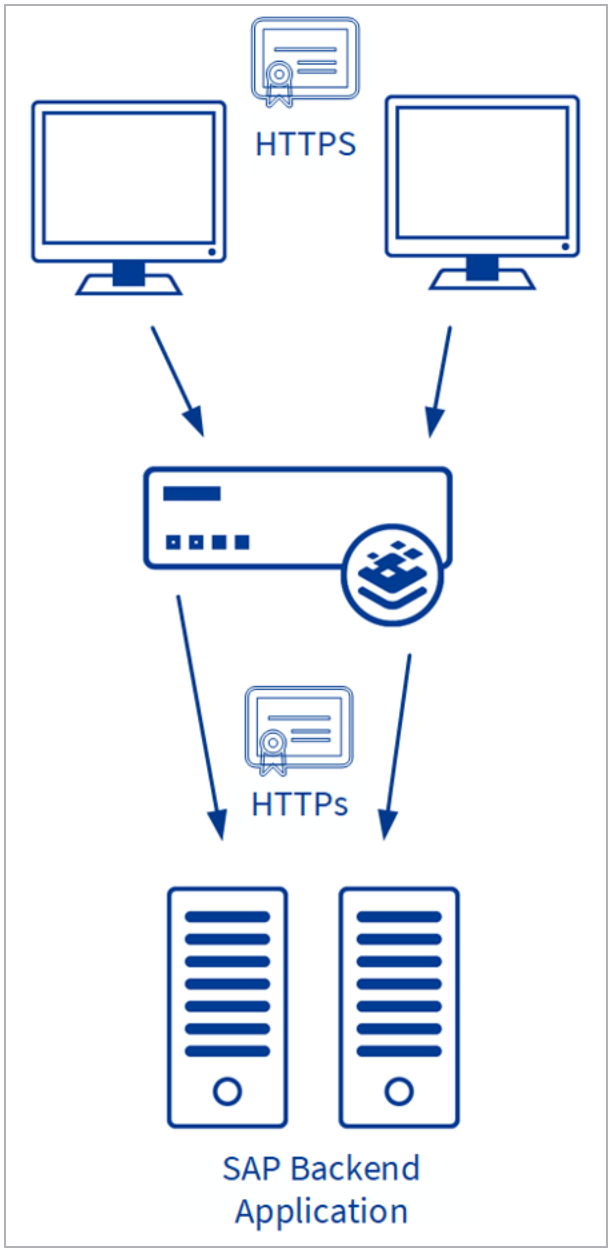
When **SSL Acceleration** is enabled on the Kemp LoadMaster there are two options that can be leveraged. The decision to choose which option is primarily determined by the corporate security policies within an organization.



SSL Offloading

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

This option will allow the LoadMaster to accept connections from the clients encrypted over HTTPS and then send the traffic to the SAP backend application un-encrypted over HTTP. In some environments this is not permitted due to the possible security risks.



SSL Reencrypt

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

This option allows the LoadMaster to accept connections from the clients encrypted over HTTPS and then re-encrypt the traffic over HTTPS before sending to the SAP backend application. This configuration typically provides the security requirements for most organizations.

3.1.3 Certificates

Certificates play a large part in the configuration of the SAP applications. Several certificate types will be used as part of this configuration and must be imported into the LoadMaster. More information about managing LoadMaster certificates can be found in the SSL Accelerated Services, Feature Description.

3.1.3.1 Server Certificates

In order to encrypt the traffic between the client and the LoadMaster, the necessary certificates must be installed. If the configuration is going to be encrypted traffic from end to end, the same certificates on the back end systems can be used for this purpose. These certificates can either be in .PEM or .PFX formats and are imported under **Certificates & Security > SSL Certificates** in the main menu of the LoadMaster WUI.

3.1.3.2 Reverse Proxy Client Certificates

This certificate is used to authenticate the LoadMaster to the backend systems. This certificate should be imported prior to the configuration of the LoadMaster Virtual Services. These certificates can either be in .PEM or .PFX formats and are imported under **Certificates & Security > SSL Certificates** in the main menu of the LoadMaster WUI.

3.1.3.3 Intermediate Certificates

These certificates are imported to allow the LoadMaster to trust the Certificate Authorities used in obtaining the Server and Client Certificates. These certificates are in Base64 format and are imported under **Certificates & Security > Intermediate Certs** in the main menu of the LoadMaster WUI.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

4 Template

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 on the Kemp Documentation page.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

5 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.

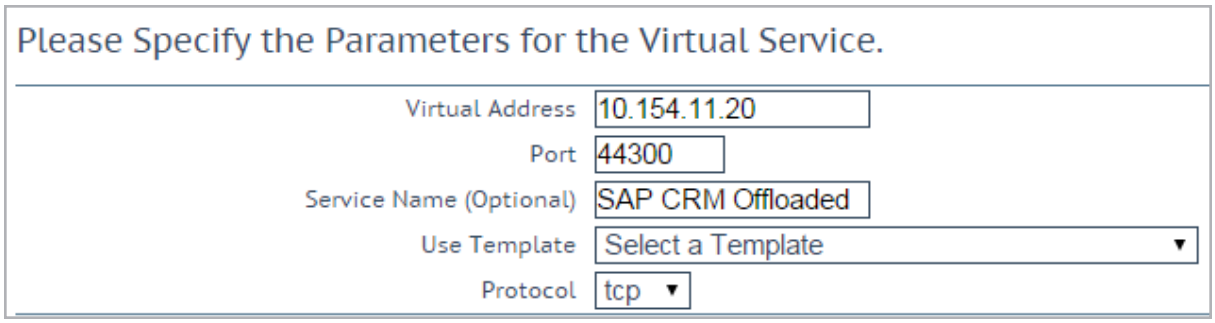
© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

6 Configure the Virtual Service for SAP CRM

6.1 SAP CRM Offloaded

To configure an offloaded Virtual Service for SAP CRM, follow the steps below:

1. In the main menu of the LoadMaster WUI, go to **Virtual Services > Add New**.



2. Enter a **Virtual Address**.
3. Enter **44300** in the **Port** field.

> The port may differ depending on SAP environment. To ensure you use the correct port, please consult with your SAP administrator.

4. Enter a recognisable **Service Name**, for example **SAP CRM Offloaded**.
5. Ensure that **tcp** is selected as the **Protocol**.
6. Click **Add This Virtual Service**.
7. Configure the settings as shown in the following table:

Section	Option	Value	Comment
Basic Properties	Service Type	HTTP/HTTPS	

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Section	Option	Value	Comment
Standard Options	Transparency	Disabled	
	Persistence Mode	Active Cookie	
	Persistence Timeout	8 Hours	
	Cookie name	Enter a unique cookie name.	Click **Set Cookie**.
	Scheduling Method	round robin	
	Idle Connection Timeout	1800	Click **Set Idle Timeout**.
SSL Properties	SSL Acceleration	Enabled	Click **OK**.
	Certificates	Select the certificate previously imported.	Click the **>** button to assign the certificate. *
	Require SNI hostname	Disabled	
	Supported Protocols	TLS1.1, TLS1.2, and TLS1.3 enabled	
	Client Certificates	No Client Certificates Required	
Real Servers	Real Server Check Method	HTTP Protocol	
	Use HTTP/1.1	Enable	
	HTTP Method	HEAD	

* Information about managing LoadMaster certificates can be found in the SSL Accelerated Services, Feature Description.

8. Add the Real Servers:

   a) Click the **Add New** button.

   b) Enter the **Real Server Address**.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

c) Enter the correct **Port**.

> Please use the IP Address and **Port** of the backend server.

> The **Forwarding method** and the **Weight** values are set, by default, to those shown in the diagram in the Real Servers section above. If required these settings may be altered.

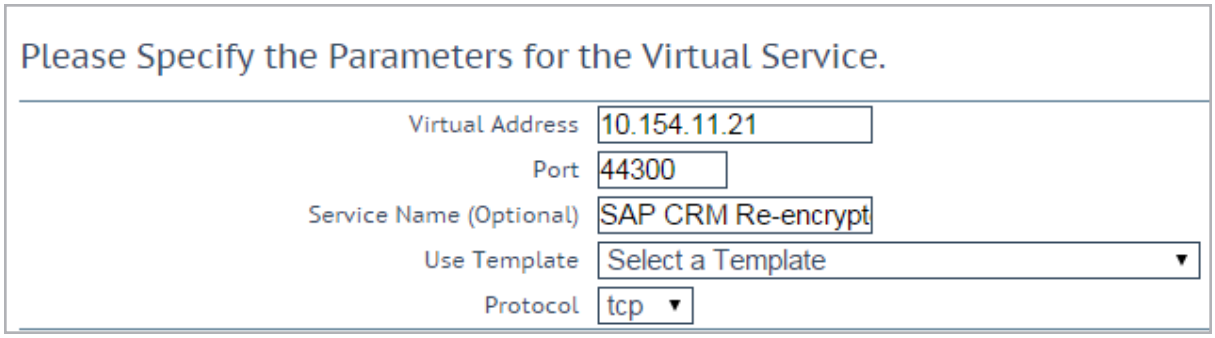
d) Click **Add this Real Server**. Click **OK** to close the pop-up message.

e) Repeat steps b) to d) above to add more Real Servers as needed, based on the environment.

6.2 SAP CRM Reencrypted

To configure a reencrypted Virtual Service for SAP CRM, follow the steps below:

1. In the main menu of the LoadMaster WUI, go to **Virtual Services > Add New**.



2. Enter a **Virtual Address**.
3. Enter **44300** in the **Port** field.

> The port may differ depending on SAP environment. To ensure you use the correct port, consult your SAP administrator.

4. Enter a recognisable **Service Name**, for example **SAP CRM Re-encrypted**.
5. Ensure that **tcp** is selected as the **Protocol**.
6. Click **Add This Virtual Service**.
7. Configure the settings as shown in the following table:

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Section	Option	Value	Comment
Basic Properties	Service Type	HTTP/HTTPS	
SSL Properties	SSL Acceleration	Enabled	
	Reencrypt	Enabled	
	Certificates	Select the certificate previously imported.	Click the **>** button to assign the certificate. *
	Require SNI hostname	Disabled	
	Supported Protocols	TLS1.1, TLS1.2, and TLS1.3 enabled	
	Client Certificates	No Client Certificates required	
Standard Options	Persistence Mode	Active Cooke	
	Persistence Timeout	8 Hours	
	Cookie name	Enter a unique cookie name.	Click **Set Cookie**.
	Idle Connection Timeout	1800	Click **Set Idle Timeout**.
Real Servers	Real Server Check Method	HTTPS Protocol	
	Use HTTP/1.1	Enabled	
	HTTP Method	HEAD	

* Information about managing LoadMaster certificates can be found in the SSL Accelerated Services, Feature Description.

8. Add the Real Servers:

   a) Click the **Add New** button.

   b) Enter the **Real Server Address**.

   c) Enter the correct **Port**.

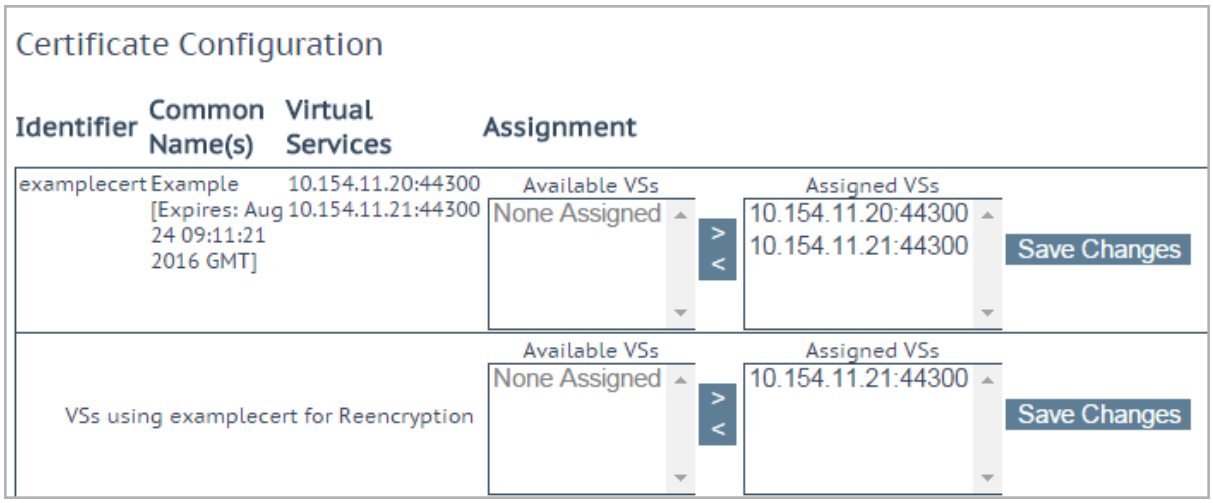
© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Please use the IP Address and Port of the backend server.

The **Forwarding method** and the **Weight** values are set, by default, to those shown in the above **Add New Real Server** screen. If required these settings may be altered.

d) Click **Add this Real Server**. Click **OK** to close the pop-up message.

e) Repeat the steps to add any additional Real Servers as needed.



9. Set the Reencryption Client Certificate to be used in the Virtual Service:

Reencyption client certificate is the client certificate the LoadMaster presents when connecting to an HTTPS Real Server. This is only needed if the Real Server requires it.

a) In the main menu of the LoadMaster WUI, go to **Certificates & Security > SSL Certificates**.

b) Click the **Reencryption Usage** button for the client certificate installed earlier.

c) Select the IP Address for the CRM Virtual Service and click the **>** button to move the IP address to the **Assigned VSs** box.

d) Click **Save Changes**.

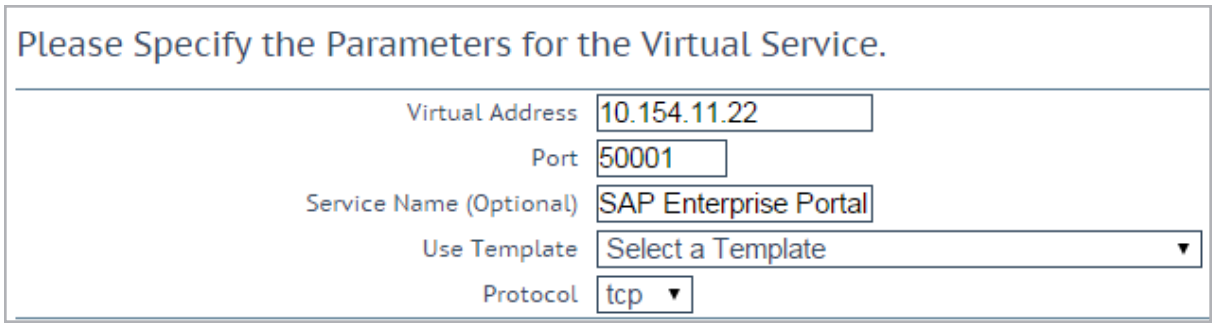
© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

7 Configure the Virtual Service for SAP Enterprise Portal

7.1 SAP Enterprise Portal Offloaded

To configure an offloaded Virtual Service for SAP Enterprise Portal, follow the steps below:

1. In the main menu of the LoadMaster WUI, go to **Virtual Services > Add New**.



2. Enter a **Virtual Address**.
3. Enter **50001** in the **Port** text box.

> The port may differ depending on the SAP Portal environment. To ensure you use the correct port, consult your SAP administrator.

4. Enter a recognisable **Service Name**, for example **SAP Enterprise Portal Offloaded**.
5. Ensure that **tcp** is set as the **Protocol**.
6. Click **Add This Virtual Service**.
7. Configure the settings as shown in the following table:

Section	Option	Value	Comment
Basic Properties	Service Type	HTTP/HTTPS	

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Section	Option	Value	Comment
Standard Options	Transparency	Disabled	
	Persistence Mode	Active Cookie	
	Persistence Timeout	8 Hours	
	Cookie name	Enter a unique cookie name.	Click **Set Cookie**.
	Idle Connection Timeout	1800	Click **Set Idle Timeout**.
SSL Properties	SSL Acceleration	Enabled	
	Certificates	Select the previously imported certificate.	Click the **>** button to assign the certificate. *
	Require SNI hostname	Disabled	
	Supported Protocols	TLS1.1, TLS1.2, and TLS1.3 enabled	
	Client Certificate	No Client Certificates required	
Real Servers	Real Server Check Method	HTTP Protocol	
	Use HTTP/1.1	Enabled	
	HTTP Method	HEAD	

* Information about managing LoadMaster certificates can be found in the SSL Accelerated Services, Feature Description.

8. Add the Real Servers:

   a) Click the **Add New** button.

   b) Enter the **Real Server Address**.

   c) Enter the correct **Port**.

   Please use the IP Address and Port of the backend server.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

> The **Forwarding method** and the **Weight** values are set, by default, to those shown in the above image. If required these settings may be altered.

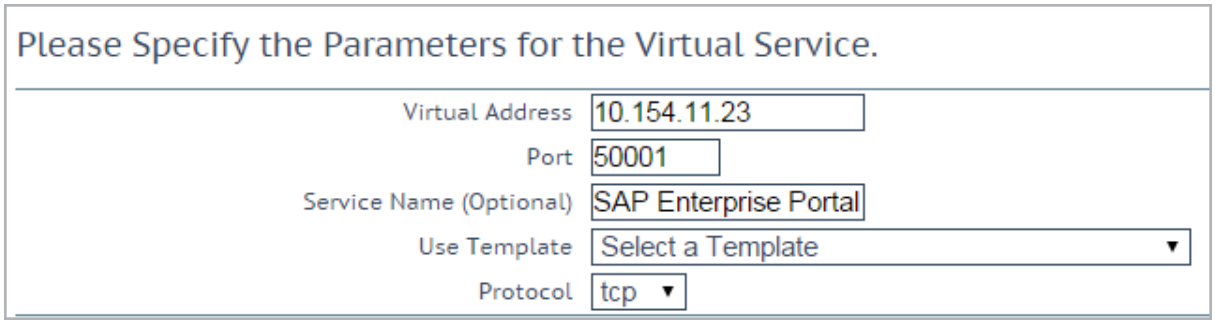
d) Click **Add this Real Server**. Click **OK** to close the pop-up message.

e) Repeat steps b) to d) above to add any additional Real Servers as needed, based on environment.

7.2 SAP Enterprise Portal Reencrypted

To configure a reencrypted Virtual Service for SAP Enterprise Portal, follow the steps below:

1. In the main menu of the LoadMaster WUI, go to **Virtual Services** > **Add New**.



2. Enter a **Virtual Address**.
3. Enter **50001** in the **Port** text box.

> The port may differ depending on the SAP Portal environment. To ensure you use the correct port, consult your SAP administrator.

4. Enter a recognisable **Service Name**, for example **SAP Enterprise Portal Reencrypt**.
5. Ensure that **tcp** is set as the **Protocol**.
6. Click **Add This Virtual Service**.
7. Configure the settings as shown in the following table:

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Section	Option	Value	Comment
Basic Properties	Service Type	HTTP/HTTPS	
SSL Properties	SSL Acceleration	Enabled	
	Reencrypt	Enabled	
	Certificates	Select the certificate previously imported.	Click the **>** button to assign the certificate. *
	Require SNI hostname	Disabled	
	Supported Protocols	TLS1.1, TLS1.2, and TLS1.3 enabled	
	Client Certificates	No Client Certificates required	
Standard Options	Persistence Mode	Active Cookie	
	Persistence Timeout	8 Hours	
	Cookie name	Enter a unique cookie name.	Click **Set Cookie**.
	Idle Connection Timeout	1800	Click **Set Idle Timeout**.
Real Servers	Real Server Check Method	HTTPS Protocol	
	Use HTTP/1.1	Enabled	
	HTTP Method	HEAD	

* Information about managing LoadMaster certificates can be found in the SSL Accelerated Services, Feature Description.

8. Add the Real Servers:

   a) Click the **Add New** button.

   b) Enter the **Real Server Address**.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

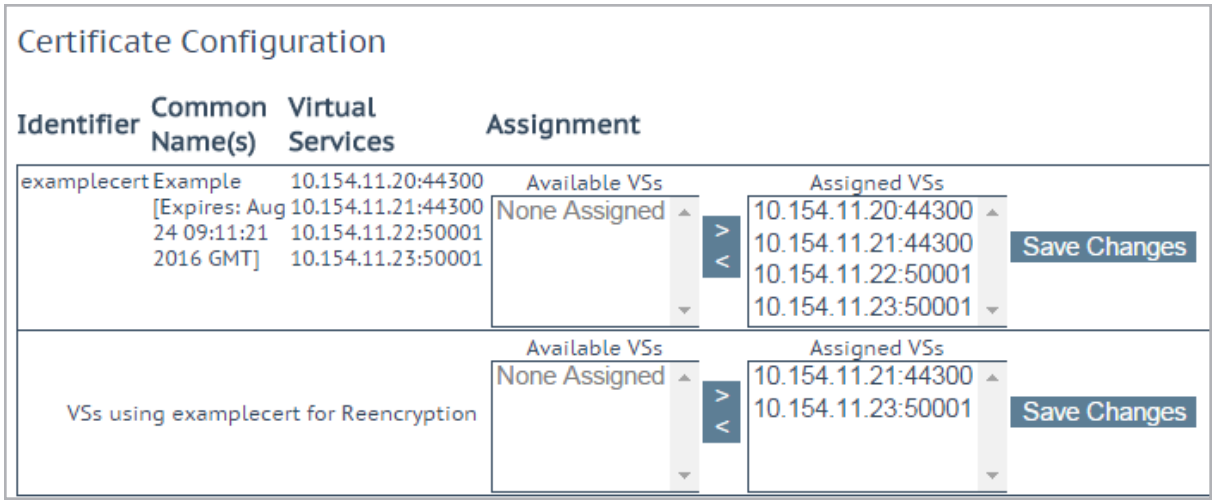
c) Enter the correct **Port**.

> Please use the IP Address and Port of the backend server.

> The **Forwarding method** and the **Weight** values are set, by default, to those shown in the above image. If required these settings may be altered.

d) Click **Add this Real Server**.

e) Repeat steps b) to d) above to add any additional Real Servers as needed, based on environment.



9. Set the Reencryption Client Certificate to be used in the Virtual Service:

> Reencyption Client Certificate is the client certificate the LoadMaster presents when connecting to an HTTPS Real Server. This is only needed if the Real Server requires it.

a) In the main menu of the LoadMaster WUI, go to **Certificates & Security > SSL Certificates**.

b) Click the **Reencryption Usage** button for the client certificate installed earlier.

c) Select the IP Address for the CRM Virtual Service and click the **>** button to move the IP address to the **Assigned VSs** box.

d) Click **Save Changes**.

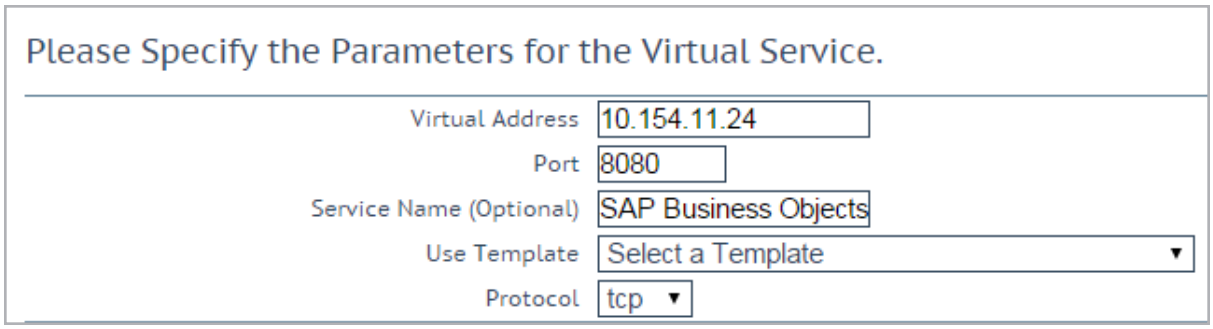
© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

8 Configure the Virtual Services for SAP Business Objects

8.1 SAP Business Objects Offloaded

To configure an offloaded Virtual Service for SAP Business Objects, follow the steps below:

1. In the main menu of the LoadMaster WUI, go to **Virtual Services > Add New**.



2. Enter a **Virtual Address**.
3. Enter **8080** in the **Port** text box.

> The port may differ depending on SAP BOE environment. To ensure you use the correct port, consult your SAP administrator.

4. Enter a recognisable **Service Name**, for example **SAP Business Objects Explorer Offloaded**.
5. Ensure that **tcp** is set as the **Protocol**.
6. Click **Add This Virtual Service**.
7. Configure the settings as shown in the following table:

Section	Option	Value	Comment
Standard Options	Transparency	Disabled	

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Section	Option	Value	Comment
	Persistence Mode	Active Cookie	
	Persistence Timeout	8 Hours	
	Cookie name	Enter a unique cookie name.	Click **Set Cookie**.
	Idle Connection Timeout	1800	Click **Set Idle Timeout**.
SSL Properties	SSL Acceleration	Enabled	
	Reencrypt	Disabled	
	Certificates	Select the certificate previously imported.	Click the **>** button to assign the certificate. Click **Set Certificates**. *
	Require SNI hostname	Disabled	
	Supported Protocols	TLS1.1, TLS1.2, and TLS1.3 enabled	While this workload may not support TLS1.3 yet, Kemp recommend enabling it for future proofing.
	Client Certificates	No Client Certificates required	
Real Servers	Real Server Check Method	HTTP Protocol	
	Use HTTP/1.1	Enabled	
	HTTP Method	HEAD	

* Information about managing LoadMaster certificates can be found in the SSL Accelerated Services, Feature Description.

8. Add the Real Servers:

   a) Click the **Add New** button.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

b) Enter the **Real Server Address**.

c) Enter the correct **Port**.

> Please use the IP Address and Port of the backend server.

> The **Forwarding method** and the **Weight** values are set, by default, to those shown in the above image. If required these settings may be altered.

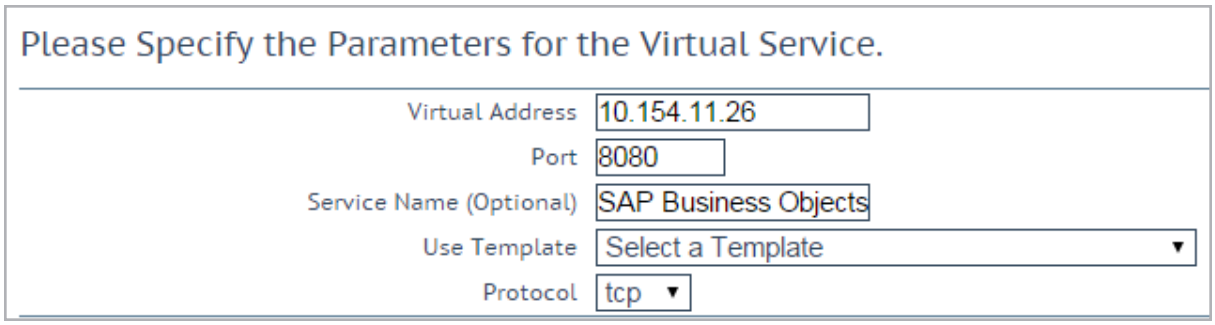
d) Click **Add this Real Server**.

e) Repeat steps b) to d) above to add any additional Real Servers as needed, based on the environment.

8.2 SAP Business Objects Reencrypted

To configure a reencrypted Virtual Service for SAP Business Objects, follow the steps below:

1. In the main menu of the LoadMaster WUI, go to **Virtual Services > Add New**.



2. Enter a **Virtual Address**.
3. Enter **8080** in the **Port** text box.

> The port may differ depending on SAP BOE environment. To ensure you use the correct port, consult your SAP administrator.

4. Enter a recognisable **Service Name**, for example **SAP Business Objects Explorer Re-encrypted**.
5. Ensure that **tcp** is set as the **Protocol**.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

6. Click **Add This Virtual Service**.

7. Configure the settings as shown in the following table:

Section	Option	Value	Comment
Standard Options	Transparency	Disabled	
	Persistence Mode	Active Cookie	
	Persistence Timeout	8 Hours	
	Cookie name	Enter a unique cookie name.	Click **Set Cookie**.
	Idle Connection Timeout	1800	Click **Set Idle Timeout**.
SSL Properties	SSL Acceleration	Enabled	
	Reencrypt	Enabled	
	Supported Protocols	TLS1.1, TLS1.2, and TLS1.3 enabled	
	Certificates	Select the previously imported certificate.	Click **>** to assign the certificate. Click **Set Certificates**. *
	Require SNI hostname	Disabled	
	Client Certificates	No Client Certificates required	
Real Servers	Real Server Check Method	HTTPS Protocol	
	Use HTTP/1.1	Enabled	
	HTTP Method	HEAD	

* Information about managing LoadMaster certificates can be found in the SSL Accelerated Services, Feature Description.

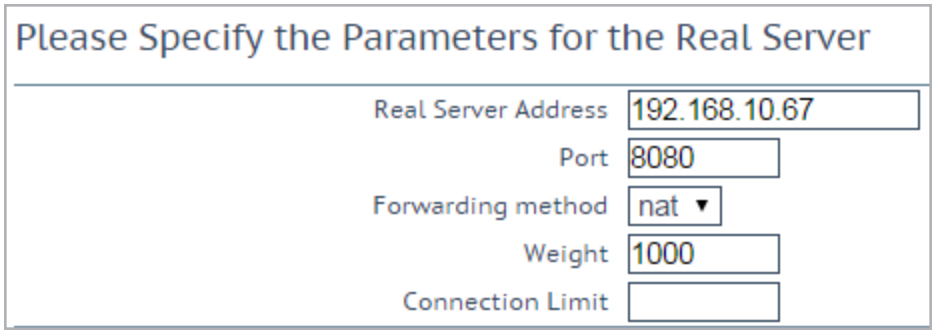
8. Expand the **Real Servers** section and set the following options:

   a) Select the **HTTPS Protocol** option in the health check drop-down menu.

   b) Select the **Use HTTP/1.1** check box.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

c) Select **HEAD** as the **HTTP Method**.



9. Add the Real Servers:

a) Click the **Add New** button.

b) Enter the **Real Server Address**.

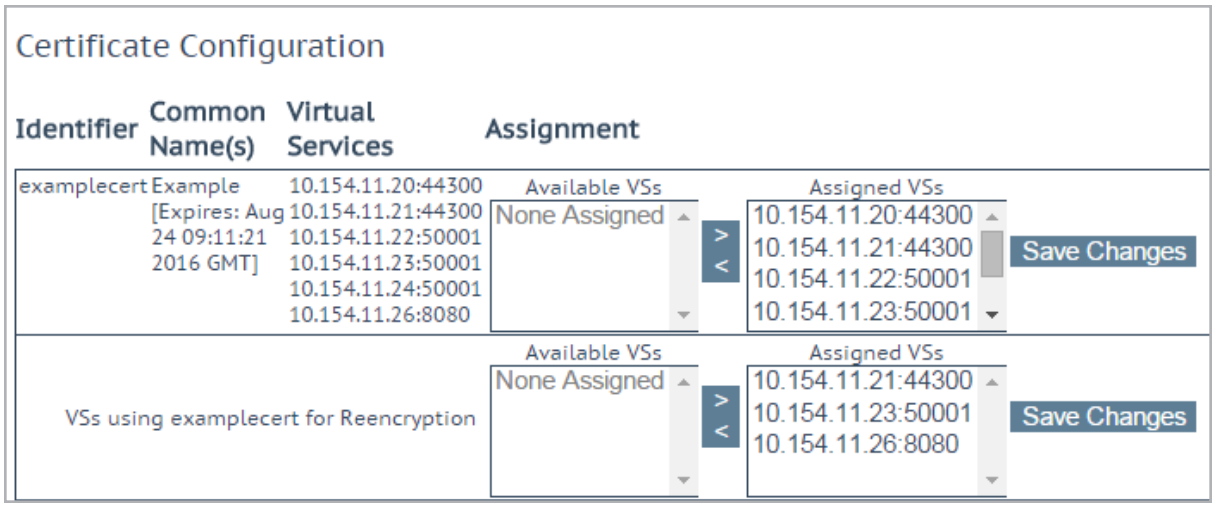
c) Enter the correct **Port**.

> Please use the IP Address and Port of the backend server.

> The **Forwarding method** and the **Weight** values are set, by default, to those shown in the above image. If required these settings may be altered.

d) Click **Add this Real Server**.

e) Repeat steps b) to d) above to add any additional Real Servers as needed, based on the environment.



© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

10. Set the Reencryption Client Certificate to be used in the Virtual Service:

> Reencyption Client Certificate is the client certificate the LoadMaster presents when connecting to an HTTPS real server. This is only needed if the real server requires it.

a) In the main menu of the LoadMaster WUI, go to **Certificates & Security > SSL Certificates**.

b) Click the **Reencryption Usage** button for the client certificate installed earlier.

c) Select the IP Address for the CRM Virtual Service and click the **>** button to move the IP address to the **Assigned VSs** box.

d) Click **Save Changes**.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

9 Additional Features

Additional Kemp 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 Kemp documentation web page: http://kemptechnologies.com/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.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

References

The following sources are referred to in this document:

Kemp website

www.kemptechnologies.com

Kemp Documentation page

http://kemptechnologies.com/documentation/

SSL Accelerated Services, Feature Description

Web User Interface (WUI), Configuration Guide

Web Application Firewall (WAF), Feature Description

Virtual Services and Templates, Feature Description

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Last Updated Date

This document was last updated on 27 July 2023.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.