Progress®
Kemp® LoadMaster®

Deployment Guide CyberArk

Generated on: 18 December 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 8

Enable Subnet Originating Requests Globally 8

Enable Check Persist Globally 9

Chapter 5: Virtual Services 11

Create the CyberArk PVWA Virtual Service 11

CyberArk PVWA Virtual Service Recommended Settings (optional) 12

Create the CyberArk PSM Virtual Services 14

CyberArk PSM Virtual Service Advanced Health Checking (optional) 15

CyberArk PSM Virtual Service Recommended Settings (optional) 16

1

Introduction

CyberArk Endpoint Privilege Manager blocks and contains attacks at the endpoint by enforcing least privilege thereby reducing the risk of data exfiltration. With the use of enforced, granular, least privileged policies and the ability to identify and block malicious applications, security teams can prevent ransomware.

The Progress Kemp LoadMaster delivers an exceptional, cost effective, and easy to use solution which by employing High Availability, Global Server Load Balancing (GSLB), intelligent load balancing, and intelligent server health checking can support an always-on application experience.

Related Links

For details, see the following topics:

- Document Purpose
- Intended Audience

Document Purpose

This document provides the recommended LoadMaster settings used when load balancing CyberArk. The Progress Support team is available to provide solutions for scenarios not explicitly defined. For further details, refer to the: LoadMaster Support and Learning Hub.

Intended Audience

This document is intended to be read by anyone who is interested in configuring the LoadMaster to optimize CyberArk.

2

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.

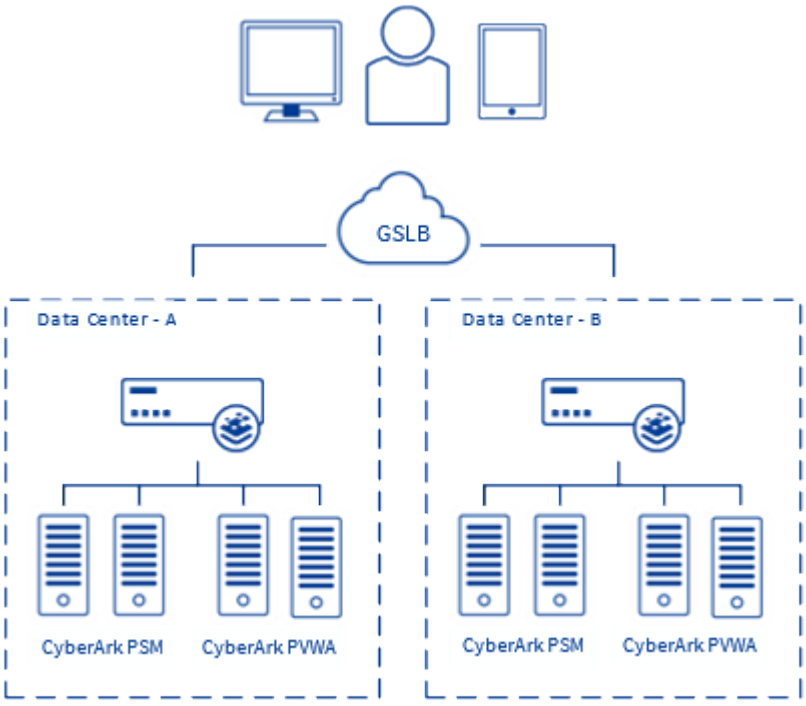
Download released templates from the following page: LoadMaster Templates.

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

3

Architecture

CyberArk consists of two server roles that are load balanced - Password Vault Web Access (PVWA) and Privileged Session Manager (PSM).



4

Configure the LoadMaster

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

Related Links

For details, see the following topics:

- Enable Subnet Originating Requests Globally
- Enable Check Persist 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.

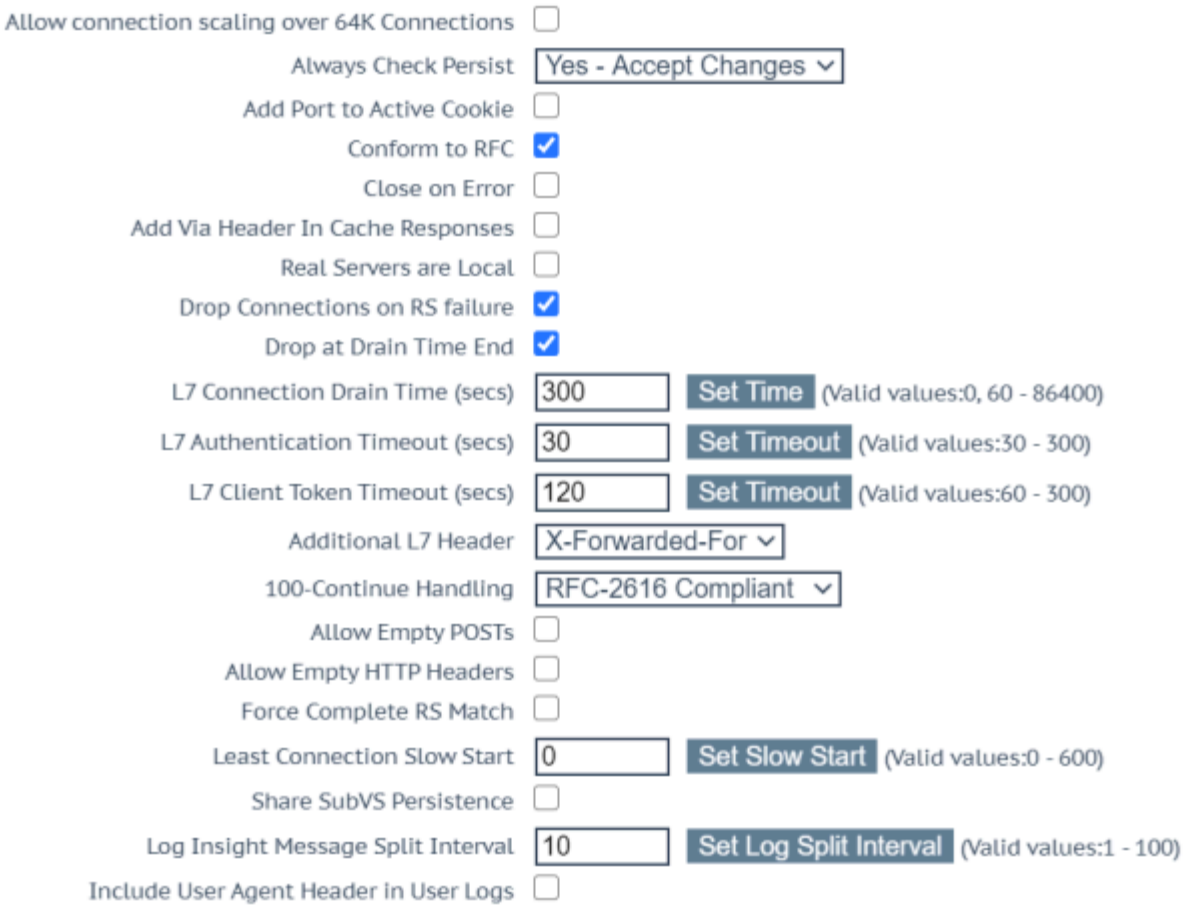
To enable **Subnet Originating Requests** globally, follow the steps below:

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.

Enable Check Persist Globally

It is recommended that you change the **Always Check Persist** option to **Yes – Accept Changes**. Use the following steps:

1. Go to **System Configuration > Miscellaneous Options > L7 Configuration**.



2. Click the **Always Check Persist** drop-down arrow and select **Yes – Accept Changes**.

5

Virtual Services

CyberArk consists of two components that can be load balanced and optimized depending on the environment in which it is deployed. CyberArk Password Vault Web Access (PVWA) and the CyberArk Privileged Session Manager (PSM) can leverage the Progress Kemp LoadMaster to provide the necessary high availability and failover to ensure an always-on application experience.

This step-by-step setup of Virtual Services (VSs) leverages the Progress Kemp application template for CyberArk.

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 Progress Kemp LoadMaster Application Programming Interface (API) and automation tools.

SSL/TLS certificates should be added before creating this Virtual Service. For further information on certificates, refer to the SSL Accelerated Services, Feature Description.

Related Links

For details, see the following topics:

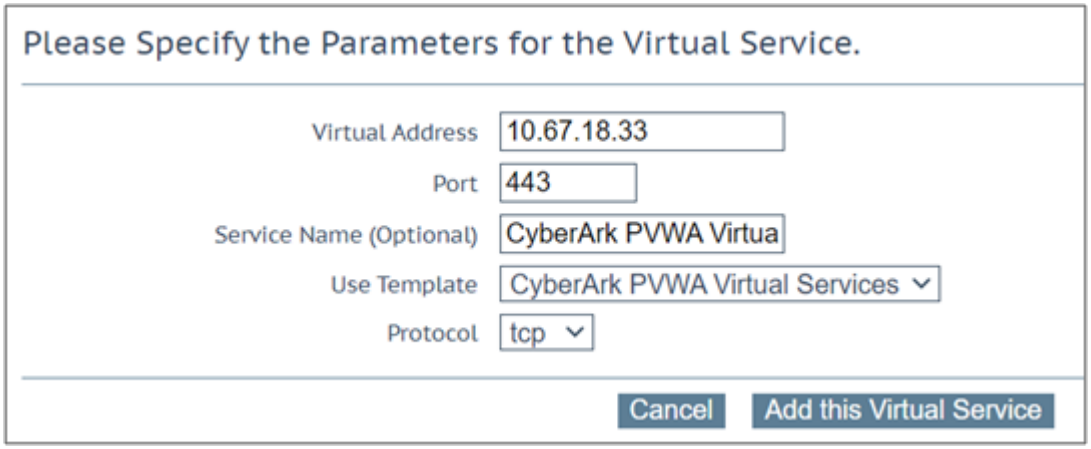
- Create the CyberArk PVWA Virtual Service
- Create the CyberArk PSM Virtual Services

Create the CyberArk PVWA Virtual Service

The following are the steps involved and the recommended settings to configure the CyberArk Password

Vault Web Access (PVWA) 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 **CyberArk PVWA Virtual Service** template in the **Use Template** drop-down list.
4. Click **Add this Virtual Service**.
5. Click **View/Modify Services** in left navigation.
6. Click **Modify** for the CyberArk PVWA Virtual Services on port 443.
7. Expand the **SSL Properties** section.
8. Select the certificate to use from **Available Certificates** and click the arrow (**>**) to move it to **Assigned Certificates**.
9. Expand the **Real Servers** section.
10. Click **Add New**.
11. Type the **Real Server Address**.
12. Click **Add This Real Server**.
13. Repeat these steps to add more Real Servers as needed.

CyberArk PVWA Virtual Service Recommended Settings (optional)

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

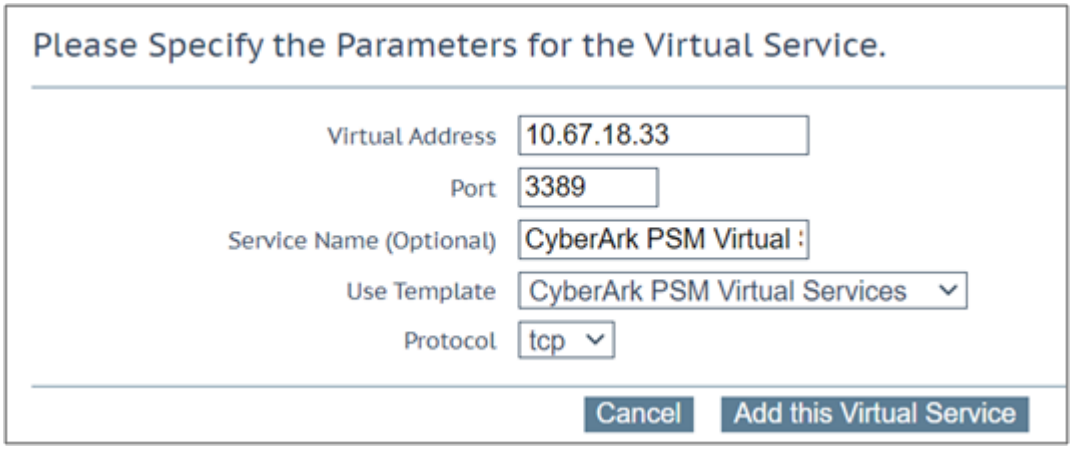
API Parameter	API Value	WUI Field Name	WUI Field Value
port	443	Port	443
prot	tcp	Protocol	tcp
VStype	http	Service Type	HTTP-HTTP/2-HTTPS
SubnetOriginating	1	Subnet Originating Requests	Enabled
Forcel7	1	Force L4	Disabled
Schedule	lc	Scheduling Method	least connection
Persist	src	Persistence Options	Source IP Address
PersistTimeout	1800	Timeout	30 Minutes
SSLAcceleration	1	SSL Acceleration	Enabled
SSLReencrypt	1	Reencrypt	Enabled
TLSType	3	Supported Protocols	TLS1.1, TLS1.2, and TLS1.3 (Enabled)
CipherSet	BestPractices	Cipher Set	BestPractices
CheckType	https	Real Server Check Method	HTTPS Protocol

API Parameter	API Value	WUI Field Name	WUI Field Value
CheckUseGet	1	HTTP Method	GET
CheckUrl	/psm/api/health	URL	/psm/api/health
CheckUse1.1	1	Use HTTP/1.1	Enabled
checkhost	<EnterYourHostname>	HTTP/1.1 Host	<EnterYourHostname>
checkpattern	PASS	Reply 200 Pattern	PASS

Create the CyberArk PSM Virtual Services

The following are the steps involved and the recommended settings to configure the CyberArk Privileged Session Manager (PSM) Virtual Service:

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



2. Type a valid **Virtual Address**.
3. Select the **CyberArk PSM Virtual Service** template in the **Use Template** drop-down list.
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.

CyberArk PSM Virtual Service Advanced Health Checking (optional)

This section outlines the steps to leverage the advanced health checking capabilities for CyberArk PSM. This capability will use HTTPS to determine the health of the service rather than the default RDP health check in the template. This will require an addition Virtual Service to be set up for health checking purposes only on TCP/443.

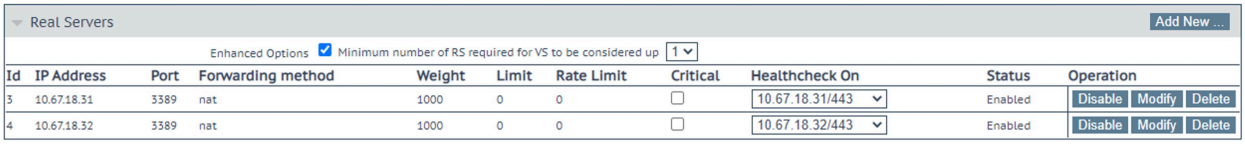
Note: Steps to enable advanced health checking on the CyberArk PSM server can be found here: Deploy PSM Health Check.

Create a Dedicated Health Check Virtual Service

1. In the main menu of the LoadMaster UI, go to **Virtual Services > Add New**.
2. Type a valid **Virtual Address**.
3. Enter **Port** 443.
4. Provide a **Service Name** such as **CyberArk PSM HealthCheck Virtual Service**.
5. Click **Add this Virtual Service**.
6. Expand **Real Servers**.
7. For **URL**, enter **/psm/api/health** and click **Set URL**.
8. Tick the box for **Use HTTP/1.1**.
9. For **HTTP/1.1 Host**, enter the Hostname of the PSM Servers and click **Set Host**.
10. Set **HTTP Method** to **GET**.
11. For **Reply 200 Pattern**, enter **PASS** and click **Set Pattern**.
12. Click **Add New**.
13. Type the **Real Server Address**.
14. Click **Add This Real Server**.
15. Repeat these steps to add more PSM Servers as needed.

Enable Enhanced Health Checking on the CyberArk PSM Virtual Service

1. Click **View/Modify Services** in left navigation.
2. Click **Modify** for the CyberArk PSM Virtual Services on port 3389.
3. Expand **Real Servers**.
4. Tick the box for **Enhanced Options**.



5. Under the **Healthcheck On** column select the matching IP address for each real server for port 443.

CyberArk PSM Virtual Service Recommended Settings (optional)

This table outlines the recommended settings that are set using the 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	3389	Port	3389
prot	tcp	Protocol	tcp
VStype	ts	Service Type	Remote Terminal
SubnetOriginating	1	Subnet Originating Requests	Enabled
Forcel7	1	Force L4	Disabled
Schedule	lc	Scheduling Method	least connection
Persist	rdp-src	Persistence Options	Terminal Service or Source IP

API Parameter	API Value	WUI Field Name	WUI Field Value
PersistTimeout	1800	Timeout	30 Minutes
IdleTimeout	1800	Idle Connection Timeout	30 Minutes
CheckType	rdp	Real Server Check Method	Remote Terminal Protocol
CheckPort	3389	Checked Port	3389