Progress®
Kemp® LoadMaster®

Deployment Guide Splunk

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 Splunk Virtual Services 9

Enable Subnet Originating Requests Globally 9

Splunk Virtual Service 10

Splunk HTTP (Redirect) Virtual Service 12

Splunk Syslog UDP Virtual Service 12

Chapter 5: References 14

1

Introduction

Splunk is an enterprise software that makes machine data accessible, usable and valuable to anyone. Splunk makes it simple to collect, analyse, and act upon the value of the data generated by an enterprise's technology infrastructure. Splunk helps users turn machine data into operational intelligence.

Such a powerful tool requires reliable and powerful support. The LoadMaster delivers an exceptional, cost-effective and easy to use solution that, by employing Adaptive Load Balancing, balances requests across Splunk servers.

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. For more information on HA please refer to: High Availability (HA), Feature Description.

Related Links

For details, see the following topics:

- Document Purpose
- Intended Audience

Document Purpose

This document provides guidance on how to deploy Splunk with a LoadMaster. The Progress Kemp 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 used by anyone deploying Splunk with a LoadMaster.

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.

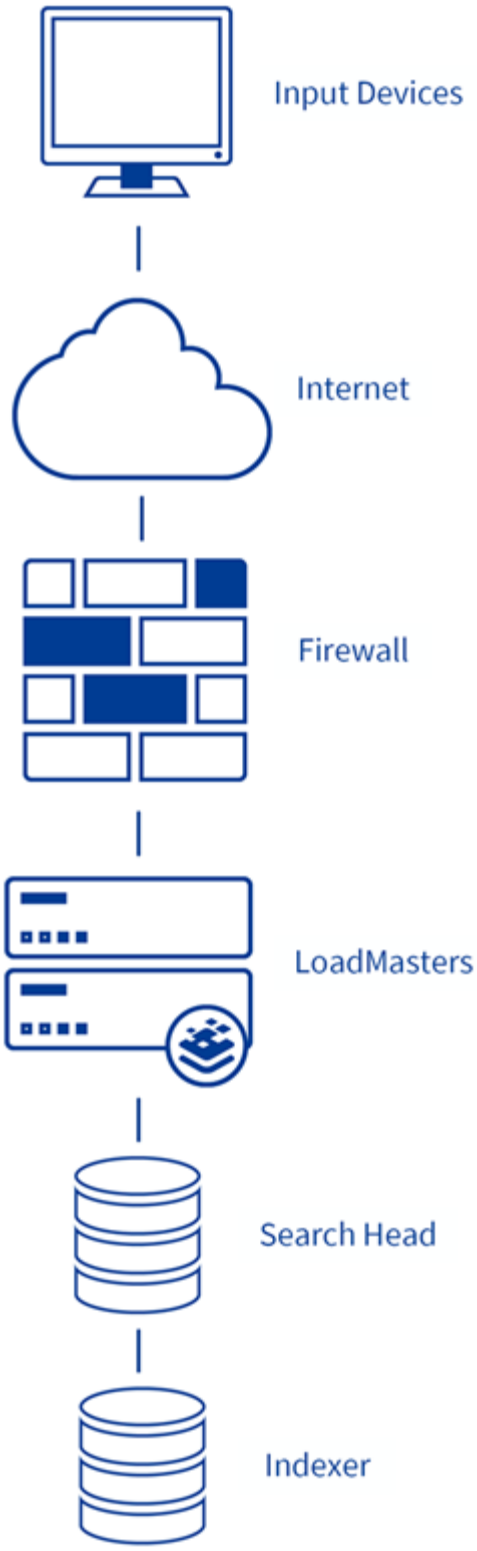
You can remove templates after use and this will not affect deployed services. If needed, you can make changes to any of the VS settings after using the template.

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


Input Devices
Internet
Firewall
LoadMasters
Search Head
Indexer

4

Configure Splunk Virtual Services

The environment in which Splunk is deployed determines which of the following setups should be used.

Related Links

For details, see the following topics:

- Enable Subnet Originating Requests Globally
- Splunk Virtual Service
- Splunk HTTP (Redirect) Virtual Service
- Splunk Syslog UDP Virtual Service

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.

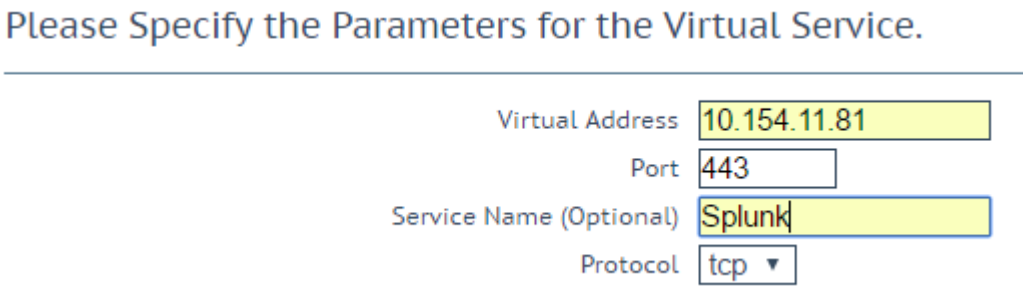
To enable **Subnet Originating Requests** globally, follow the steps below:

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.

Splunk Virtual Service

The following are the steps involved and the values required to configure Splunk Virtual Service:

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 **443** in the **Port** text box.
4. Enter a recognizable **Service Name**, for example **Splunk**.
5. Ensure **tcp** is selected as the **Protocol**.
6. Click **Add this Virtual Service**.
7. Enter the details shown in the following table:

   Users should note that clicking the **Set Redirect URL** button, automatically creates a redirect Virtual Service on Port **80**.

Section	Option	Value	Comment
Standard Options	Transparency	Deselected	
	Persistence Mode	None	
	Scheduling Method	Round robin	
SSL Properties	SSL Acceleration	Enabled Reencrypt	A wildcard certificate allows secure connections to be established with a request URL in the format of *.example.com. With this approach, a single certificate secures traffic for all clients in a multi-tenant environment.
	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.
	Cipher Set	Best Practices	For further information on cipher sets, please refer to the SSL Accelerated Services, Feature Description.
Advanced Properties	Content Switching	Disabled	
	Add HTTP Headers	Legacy Operation (X-ClientSide)	
	Redirect URL	https://%h%s	Click **Add HTTP Redirector**

Section	Option	Value	Comment
Real Servers	Real Server Check Method	HTTPS Protocol	
	Checked Port	8000	
	HTTP Method	HEAD	

8. Add the Real Servers:
   1. Click the **Add New** button.
   2. Enter the IP address of the **AX 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. An administrator can change these.

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

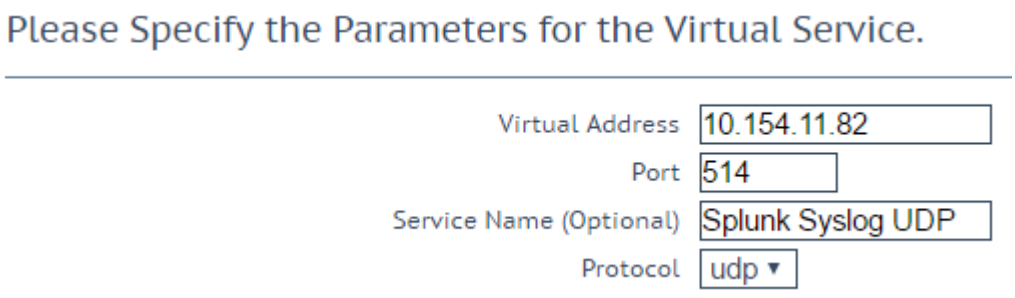
Splunk HTTP (Redirect) Virtual Service

1. This Virtual Service is automatically created when users click the **Set Redirect URL** button while configuring the **Splunk** Virtual Service in the Splunk Virtual Service section.

Splunk Syslog UDP Virtual Service

The following are the steps involved and the values required to configure the Splunk Syslog UDP Virtual Service:

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 **514** in the **Port** text box.
4. Enter a recognizable **Service Name**, for example **Splunk Syslog udp**.
5. Ensure **udp** is selected as the **Protocol**.
6. Click **Add this Virtual Service**.
7. Enter the details shown in the following table:

Section	Option	Value
Standard Options	Transparency	Enabled
	Persistence Mode	Source IP Address
	Prersistence Timeout	1 Minute
	Scheduling Method	Weighted round robin
Real Servers	Real Server Check Method	ICMP Ping

8. Add the Real Servers:
   1. Click the **Add New** button.
   2. Enter the IP address of the **AX Server**.
   3. Enter **514** 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. An administrator can change these.

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

5

References

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

Virtual Services and Templates, Feature Description.

High Availability (HA), Feature Description

SSL Accelerated Services, Feature Description