IMPORTANT: This guide has been archived. While the content in this guide is still valid for the products and version listed in the document, it is no longer being updated and may refer to F5 or 3rd party products or versions that have reached end-of-life or end-of-support. See https://support.f5.com/csp/article/K11163 for more information.

# Deploying the BIG-IP LTM with IBM QRadar Logging

Welcome to the F5 deployment guide for IBM<sup>®</sup> Security QRadar<sup>®</sup> SIEM and Log Manager. This guide shows administrators how to configure the BIG-IP Local Traffic Manager (LTM) for Syslog event load balancing for IBM Security QRadar SIEM and Log Manager.

The BIG-IP LTM is capable of load balancing Syslog event messages. This is beneficial for environments that have more logs being generated than a single log server can collect. By deploying multiple QRadar log servers behind the BIG-IP system, the load of the log generating devices can be spread across multiple log collectors.

## Products and applicable versions

Product	Version
BIG-IP LTM	11.3 -12.1.1
IBM QRadar	7.1, 7.2.6
Document version	1.2 (see Document Revision History on page 7)

To provide feedback on this deployment guide or other F5 solution documents, contact us at solutionsfeedback@f5.com

# Contents

Why F5?	3
Prerequisites and configuration notes	3
Network topology	3
Configuring the BIG-IP LTM for QRadar SIEM and Log Manager	4
Viewing virtual server statistics	5
Viewing load balancing pool statistics	5
QRadar Configuration	6
DSM Installation	6
Viewing Log Events	6
Next Steps	6
Document Revision History	7

J.

## Why F5?

Scaling syslog services can become a manual task that involves the configuration and restart of multiple configuration files; an error prone set of procedures. By using BIG-IP Local Traffic Manager, you can realize the following benefits:

- Reduce configuration complexity by using a Virtual IP Address instead of hard-coding individual QRadar SIEM IP addresses,
- Increase uptime and percentage of log retention by managing failover through BIG-IP's health monitors,
- Ease scaling the configuration by reducing the effort required to add resources; simply add a new server to the BIG-IP load balancing pool.

### Prerequisites and configuration notes

The following are general prerequisites and configuration notes for this guide.

- > You must have the F5 BIG-IP system installed, licensed, and provisioned with Local Traffic Manager (LTM).
- > You must have management administrative access rights to the BIG-IP system.
- > You need an available IP address on the BIG-IP system's External VLAN for the virtual server
- > The QRadar Log collectors must be installed and accessible in an internal VLAN on the BIG-IP system.
- > You must have QRadar DSMs installed for each of the log server sources
- Make sure you are using the most recent version of this deployment guide, available at http://f5.com/pdf/deployment-guides/ibm-gradar-dg.pdf.

## Network topology

The following diagram shows the network topology of the configuration described in this guide



Figure 1: Logical configuration example

# Configuring the BIG-IP LTM for QRadar SIEM and Log Manager

Use the following tables for guidance on configuring the BIG-IP system for the IBM Security QRadar SIEM and Log Manager. These tables contains any non-default setting you should configure as a part of this deployment. Settings not contained in the table can be configured as applicable. For specific instructions on configuring individual objects, see the online help or product manuals.

BIG-IP object		Non-default se	ttings/Notes				
	Name	Type a unique name.					
Health Monitor (Local Traffic>Monitors)	Туре	TCP or UPD depending on which protocol your QRadar nodes are using					
	Interval	30					
	Timeout	91					
	Name	Type a unique name.					
	Health monitor	Add health monitor you created					
	Slow Ramp Time <sup>1</sup>	300					
Pool	Load Balancing Method	Least Connections (memb	per) recommended				
(Local Traffic>Pools)	Address	IP address of the QRadar no	bde				
	Service Port	<b>514</b> (514 is the default syslo implementation to use a non	g port, modify this port if you have configured your syslog -standard port)				
		Repeat Address and Port for	r all members				
		TCP profile if your QRadar nodes are using TCP					
		Name	Type a unique name.				
		Parent profile	TCP				
	Protocol (Profiles>Protocol)	UDP profile if your QRadar nodes are using UDP					
Profiles		Name	Type a unique name.				
(Local traffic>Proffies)		Parent profile	UDP				
		Datagram LB <sup>2</sup>	Enabled (optional)				
	Devoietence (Drefiles - Devoietence)	Name	Type a unique name.				
	reisistence (Fromes>reisistence)	Persistence Type	Source Address Affinity				
	Name	Type a unique name.					
	Destination Address	Type the IP address for the virtual server. This address is where the log sources will send their log events.					
	Service Port	<b>514</b> (514 is the default syslog port, modify this port if you have configured your syslog implementation to use a non-standard port)					
Virtual Server	Protocol	TCP or UPD depending on which protocol your QRadar nodes are using					
(Local Traffic>Virtual Servers)	VLAN and Tunnel Traffic	Select <b>Enabled on</b> , and then move the external VLAN (or the VLAN closest to the log server sources) to the <b>Selected</b> list.					
	Source Address Translation	None					
	Default Pool	Select the pool you created for the QRadar nodes					
	Default Persistence Profile	Select the persistence profile you created above					

<sup>1</sup> You must select Advanced from the Configuration list for these options to appear.

<sup>2</sup> Optional, only necessary if you want the system to load balance UDP traffic packet-by-packet

### Viewing virtual server statistics

You can easily monitor statistics for the virtual server. Once the log servers have started sending log events to the virtual server, these statistics will reflect the traffic utilization.

#### To view virtual server statics

- 1. On the Main tab, expand Local Traffic, and then click Virtual Servers.
- 2. From the list, click the name of the virtual server you just created.
- 3. On the menu bar, click **Statistics** to view a wide range of statistics for the virtual server.

## Viewing load balancing pool statistics

You can also monitor the traffic to each of the log servers. These statistics report the accumulated traffic in bits, packets, connections, and requests.

#### To view pool statics

- 1. On the Main tab, expand **Local Traffic**, and then click **Pools**.
- 2. From the list, click the name of the pool you just created.
- 3. On the menu bar, click Statistics to view a wide range of statistics for the pool.

In the following example, Pool member Q1-3 is actively receiving events.

Displa	y Options												
Statis	stics Type	Pools											
Data Format Normalized 💌													
Auto	Auto Refresh Disabled 💌 Refresh												
Comr	mon/ORada		Search Report Search									-	
1001111	non/artauai		Search Reser Search	Bits		Pack	(ets	(	Connections	;	Requests	Req	uest Queue
	Status	Pool/Member	Partition / Path	In	Out	1							
						m	Out	Current	Maximum	lotal	Total	Depth	Maximum Age
	0	QRadar	Common	560.6M	0	1.3M	Out 0	Current 0	Maximum 27	1 otal 335.0K	Total 0	Depth 0	Maximum Age 0
	•	QRadar Q1-1:514	Common Common	560.6M 0	0 0	т 1.3М 0	0 0	Current 0 0	Maximum 27 0	1 otal 335.0K 0	Total 0 0	Depth 0 0	Maximum Age 0 0
	•	QRadar Q1-1:514 Q1-2:514	Common Common Common	560.6M 0 0	0 0 0 0	1.3M 0 0	0 0 0 0	Current 0 0 0	Maximum 27 0 0	1 otal 335.0K 0 0	Total 0 0 0	Depth 0 0 0	Maximum Age 0 0 0

# **QRadar Configuration**

QRadar needs to be configured for the DSM that supports the BIG-IP system. This module is how QRadar interprets the log sentences. If the BIG-IP system is also load balancing logs from third party devices, the DSMs for those devices also need to be installed.

# **DSM** Installation

Refer to the IBM Security QRadar DSM Configuration guide for details on installing and updating the DSM installation.

# **Viewing Log Events**

To view log events, open the QRadar console, and then navigate to the Log Activity tab. From the **View** list select **Real time Streaming**. As the logs are received, QRadar will display them in order of arrival.

We	Welcome, admin [logou] Dashbaard Offenses Log Activity Network Activity Assets Reports Admin System Time: 15:17 Preferences Help										ar	
Sea	Search 🔻 Quick Searches 🔻 🍸 Add Filter 🚔 Save Criteria 🌘 Save Results 🔗 Cancel 🦴 False Positive Rules 🔻 Actions 🕈 Quick Filter 🔍									П	0	
										ſ		
	Viewing rear unite events View. Select An Option: View. Display: Default (Normalized)											
							_					
	Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port	Destination IP	Destina Port	Username	Magnitude	
	Information Message	System Notification-2 :: sipp1	1	15:17	Information	172.30.72.170	0	127.0.0.1	0	N/A		
	Information Message	System Notification-2 :: sipp1	1	15:17	Information	172.30.72.170	0	127.0.0.1	0	N/A		
	Information Message	System Notification-2 :: sipp1	1	15:17	Information	172.30.72.170	0	127.0.0.1	0	N/A		
	Information Message	System Notification-2 :: sipp1	1	15:17	Information	172.30.72.170	0	127.0.0.1	0	N/A		-

# **Next Steps**

The only additional required task is to adjust the configuration of all of the services you intended to deliver to the QRadar SIEM via syslog by changing the syslog destination server IP address to the BIG-IP's Virtual Server IP address. Ensure that your machines have a route to the BIG-IP Virtual IP address. For specific instructions, consult the appropriate documentation.

# **Document Revision History**

Version	Description	Date
1.0	New guide	07-09-2013
1.1	Corrected the product name to IBM Security QRadar SIEM and Log Manager	07-22-2013
1.2	Updated the applicable BIG-IP LTM and QRadar versions in Products and applicable versions on page 1.	02-14-2017

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc. Corporate Headquarters info@f5.com F5 Networks Asia-Pacific apacinfo@f5.com F5 Networks Ltd. Europe/Middle-East/Africa emeainfo@f5.com F5 Networks Japan K.K. f5j-info@f5.com **B** 

7

©2017 F5 Networks, Inc. All rights reserved. F5, F5 Networks, the F5 logo, and IT agility. Your way., are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com. Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, express or implied, claimed by F5. 0412