Secureworks

LogVault2, LogVault2 Plus Managed Service Installation Guide

Last Updated: September 2017

Secureworks

Copyright

Secureworks

Table of Contents

Secureworks

Document History

Document Revision #	Date Created:	Comments:
1.0	2017/09/25	Converted document to new format
1.1	2017/09/29	Merged LogVault2 and LogVault2 Plus documentation into a single document

Documentation update requests

To request modifications or notify the author of errors in this document, please notify your Secureworks representative. During initial implementation, notify your Provisioning Engineer. After initial implementation, please notify the Secureworks CTOC through a portal ticket.

Secureworks

Introduction

The LogVault2 log management appliances will receive/request logs from the contracted log retention hosts/devices for retention purposes. For security and health purposes, the LogVault2 appliance will be configured to send application alerts and OS logs via syslog to the Secureworks CTA or Log Collector appliances.

The LogVault2 OS logs are filtered and correlated in real-time for various security event observations, including login failures when local accounts are utilized.

Please follow the instructions below to configure the appliance(s) for Securworks management and monitoring services; keeping in mind the “syslog_IP” may be the IP address of the Secureworks CTA or Log Collector.

Terminology (Acronyms)

- **Secureworks CTA** – This device receives logs from many sources. It filters and correlates the logs, and then forwards correlated security events over an encrypted channel to the Secureworks Security Operations Centers (SOCs) for analysis.
- **Secureworks Log Collectors** – This device can receive logs from many sources, performs de-duplication, filters, correlates, and then forwards logs to the Secureworks CTA.
- **LMI –** Log Management Intelligence

Product Documentation

LogVault2 leverages TIBCO LogLogic Log Management Intelligence (LMI) technology. Vendor documentation may be found at the below location. Please speak with your implementation representatives to determine which version will be utilized for your LogVault2 deployment.

https://docs.tibco.com/products/tibco-loglogic-log-management-intelligence

System Specifications

Feature	LogVault2 PowerEdge R630	LogVault2 Plus PowerEdge R730xd
Form factor	1U rack	2U rack
Rack Support	Dell ReadyRails	Dell ReadyRails
Power Supplies	Hot-plug redundant power supplies (495W Platinum)	Hot-plug redundant power supplies (750W Platinum)
Heat Dissipation	1908 BTU/hr maximum (redundant, 495W power supply)	2891 BTU/hr maximum (redundant, 750W power supply)
Voltage	100–240 V AC, autoranging, 50/60 Hz	100–240 V AC, autoranging, 50/60 Hz
Hard Drives	5x 1TB 7.2K RPM SATA 6Gbps 2.5in (RAID5)	12x 4TB 7.2K RPM SATA 6Gbps 3.5in (RAID6)
RAID Controller	PERC H730P	PERC H730P
Memory	16GB (2x 8GB) RDIMM, 2400 MT/s, Dual Rank, X4 Data Width	256GB (8x 32GB) RDIMM, 2400 MT/s, Dual Rank, X4 Data Width
Processor	2x E5-2623 v3, 3.0GHz - 4 Cores	2x E5-2680 v4, 2.4GHz - 14 Cores
Embedded NIC	Broadcom 5720 Quad Port 1Gb Network Daughter Card; management interface	Broadcom 5720 Quad Port 1Gb Network Daughter Card; management interface
Ship Weight	60 lbs, 27.2kg	80 lbs, 36.5kg
Dimensions	H: 4.28 cm (1.68 in.) W: 48.23 cm (18.98 in.) D: 70.05 cm (27.57 in.)	H: 8.73 cm (3.44 in), W: 44.40 cm (17.49 in), D: 68.40 cm (26.92 in)
Includes	1x 10ft Cat5E Straight-through cable	1x 10ft Cat5E Straight-through cable

Secureworks

Prerequisite Information

Authentication Integration

Secureworks recommends integrating the LogVault2 appliance(s) with your Active Directory environment. This allows you full control over who from your organization has access to the system(s). With access, users will be able to execute raw log searches, run and view reports, and check device logging status.

To integrate your LogVault2 appliance(s) with Active Directory, please provide the following:

- LDAP/Active Directory Servers
  - Server Hostname
  - Server IP
  - Windows 2003 Domain
  - Windows NT Domain
- LDAP/Active Directory Service Account
  - username = swrxloglogic
  - password = <generate_password>
- Active Directory Security Group for User Authentication
  - Define a LogLogic Report Admins security group for binding user authentication. The security group can be anywhere in your AD tree you desire with any name you desire. In our below example, we used the group name "LogLogic Report Admins".
  - Once you have defined the security group, collect the DN information for the security group and add the service account that was created to the security group so authentication can be tested by your Provisioning Engineer.
  - **Example**: CN=LogLogic Report Admins,CN=Users,DC=example,DC=com

Secureworks

Email Integration

Secureworks recommends integrating your LogVault2 device(s) with an SMTP Relay server. This integration allows the LogVault2 device(s) to email reports or notifications to your internal users.

To enable this feature, please provide your Secureworks implementation engineer with the below information.

- Internal SMTP Server for Report Delivery
  - Server Hostname
  - Server IP

IP Address Information

This section provides the appliance requirements for management IP address allocation and assignment. LogVault2 and LogVault2 Plus may have different IP requirements, please reference the appropriate section for your deployment.

LogVault2

The Secureworks LogVault2 appliance consists of three unique hosts with each needing an IP address for communication and management purposes. Please provide IP information for each of the following.

IMPORTANT NOTE: THE THREE UNIQUE HOSTS SHARE THE SAME PHYSICAL INTERFACE; ALL THREE MANAGEMENT IPS MUST BE ON THE SAME SUBNET

iDrac IP	__.__.__.__	**Common Netmask**	__.__.__.__
ESXi IP	__.__.__.__	**Common Gateway**	__.__.__.__
LMI IP	__.__.__.__	**Common DNS**	__.__.__.__

LogVault2 Plus

The Secureworks LogVault2 Plus appliance consists of three or more unique hosts with each needing an IP address for communication and management purposes. Your implementation team will discuss and determine how many LMI instances you may need for your deployment.

IMPORTANT NOTE: THESE UNIQUE HOSTS SHARE THE SAME PHYSICAL INTERFACE; ALL MANAGEMENT IPS MUST BE ON THE SAME SUBNET

iDrac IP	__.__.__.__	**Common Netmask**	__.__.__.__
ESXi IP	__.__.__.__	**Common Gateway**	__.__.__.__
LMI #1 IP	__.__.__.__	**Common DNS**	__.__.__.__
LMI #2 IP (if applicable)	__.__.__.__		
LMI #3 IP (if applicable)	__.__.__.__		
LMI #4 IP (if applicable)	__.__.__.__		

Secureworks

Requirements

This section provides information on requirements for deploying and implementing LogVault2 device(s).

Required Network Connectivity

For ease of operation, Secureworks recommends to place the LogVault2 device(s) on the same subnet as your CTA Inspector/LogCollector. If this is not possible, ensure the below network access items are permitted to enable Secureworks to monitor and manage the LogVault2 device(s).

Source	Destination	Port/Protocol	Reason
Secureworks CTA	iDRAC; ESXi; LMI	ICMP; TCP/22; TCP/443	Management connectivity
Secureworks CTA	ESXi	TCP/902; TCP/5900; TCP/427	Additional ESXi management connectivity
Secureworks CTA	iDRAC	TCP/623; TCP/5900; UDP/623	Additional iDRAC management connectivity
Secureworks CTA	LMI	TCP/514; UDP/514; TCP/8080; UDP/4514; TCP/14514	Additional LMI connectivity
iDRAC; ESXi; LMI	Secureworks CTA	UDP/514; TCP/514; TCP/1470; UDP/123*	Application and System log monitoring; Time synchronization
iDRAC; ESXi; LMI	Internal_DNS	UDP/53	Hostname resolution
LMI	Domain Controller	TCP/389; TCP/636	LDAP
LMI	SMTP Relay	TCP/25	Report notification/delivery
Client_Workstations*	LMI	TCP/443	WebUI Access

*__NTP__ – If desired, you may utilize an internal NTP server instead of the CTA

*__Client_Workstations__ – For users to utilize the LogVault2 WebUI (LMI) to review raw log data or run reports

Supplemental Network Connectivity

The below network access items may or may not be required, depending on the log sources you wish to retain data. If need further assistance with identifying required ports and protocols, please reach out to your implementation representatives.

Source	Destination	Port/Protocol	Reason
Logging Source; LMI	LMI; Logging Source	TCP/20; TCP/21; TCP/22	Logging via FTP or SCP file pull
LMI	Logging Source	TCP/1433; TCP/3306	Database connections
LMI	Logging Source	TCP/18184; TCP/18210	Check Point OPSEC
Logging Source	LMI	UDP/162	SNMP Traps
LMI	Logging Source	TCP/8302	Cisco Firepower/Sourcefire logging
LMI	LMI	TCP/443	If using a centralized management station

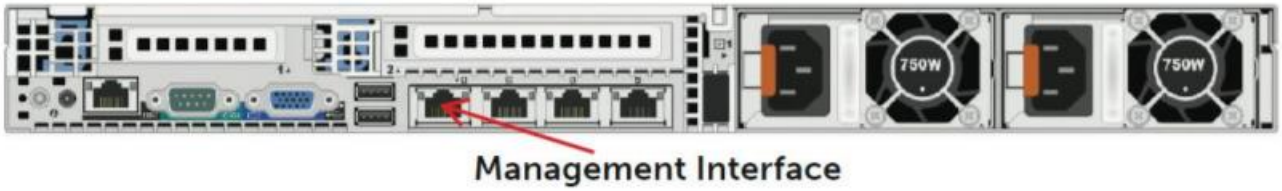
Secureworks

Hardware Installation

LogVault2

Please reference the '**System Specifications**' section for more information on hardware specifications.

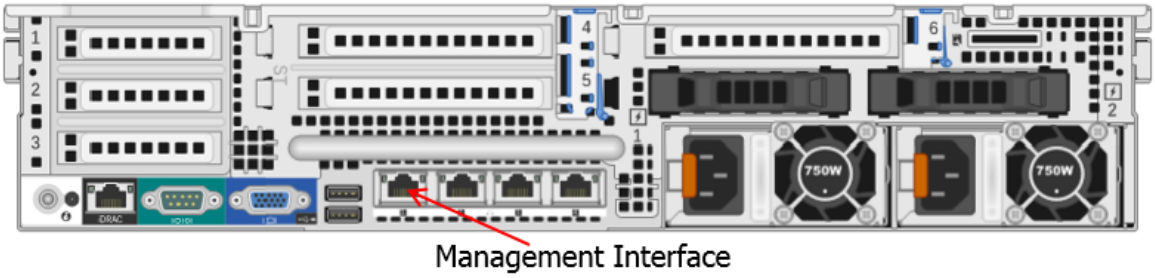
1. Rack the appliance in a 4 post rack per the Dell ReadyRails Instructions included with the rail kit.
2. Connect the included power cable(s) to the appliance.
3. Connect the Management interface of the appliance to the network. This will be the left most network interface when looking at the back of the device. No other interfaces are required. All three IP addresses will be associated with this one interface.
4. Power on the device.
5. Configure the iDRAC's management IP address.
    a. Reference section '**Remote Connectivity through the iDRAC'** to complete this task.
6. Notify your Secureworks implementation team that the LogVault2 appliance is on the network.



LogVault2 Plus

Please reference the '**System Specifications**' section for more information on hardware specifications.

1. Rack the appliance in a 4 post rack per the Dell ReadyRails Instructions included with the rail kit.
2. Connect the included power cable(s) to the appliance.
3. Connect the Management interface of the appliance to the network. This will be the left most network interface when looking at the back of the device. No other interfaces are required. All three IP addresses will be associated with this one interface.
4. Power on the device.
5. Configure the iDRAC's management IP address.
    a. Reference section '**Remote Connectivity through the iDRAC'** to complete this task.
6. Notify your Secureworks implementation team that the LogVault2 Plus appliance is on the network.



Secureworks

Remote Connectivity through the iDRAC

Remote access to the appliance will be provided to the Secureworks Engineer through the iDRAC interface of the appliance. Once you have connected the on-board management port, you may configure the iDRAC through the front LCD panel or through the BIOS with monitor and keyboard.

IMPORTANT NOTE: FOR LOGVAULT2 PLUS, YOU MUST CONFIGURE THE IDRAC THROUGH BIOS

Configuration through the front panel

1. From the front panel, press the ☑ button, and select "**Setup**" by using the arrow buttons to move the cursor.
2. Pressing the ☑ button again will confirm your selection.
3. Select "**iDRAC**" to access the iDRAC configuration options.
4. Using the arrow buttons, select "**Static IP**" to configure a Static IP address on the iDRAC interface.
5. Configure the Static IP Address for the iDRAC interface using the three buttons. Select the digit you want to change by using the arrow buttons. Once selected, press the ☑ button to edit the digit using the arrow buttons to move up or down. Confirm your choice by pressing the ☑ button a second time.
6. On the next screen, you will be asked to configure the subnet mask for the iDRAC interface, followed by the Gateway for the iDRAC interface.
7. Select "**No**" when prompted to setup the DNS.
8. Once complete, select "**Yes**" to Save your configuration.
9. Lastly**, contact your Secureworks Project Manager** so they may validate connectivity and schedule the next steps.

Configuration through the BIOS

1. As the system boots, when prompted press the "**F2**" key to select the System Setup menu.
2. Using the arrow keys, select the "**iDRAC Settings**" option.
3. Next, select the "**Network**" option.
4. On the iDRAC Settings screen, scroll down to "**IPV4 SETTINGS**" to edit your desired iDRAC IP Address, Subnet mask, and Gateway Address.
5. Once complete, select the "**Back**" button to return to the previous screen.
6. Select "**Finish**" to confirm you have finished making changes to the iDRAC interface.
7. Select "**Yes**" to save your changes.
8. You will receive confirmation your changes have been saved. Press "**OK**" to continue.
9. From here, select "**Finish**" or press the ESC key to exit out of the System Setup menu.
10. Select "**Yes**" to confirm your exit of the menu. The device will now continue to boot to the OS.
11. Lastly, **contact your SecureWorks Project Manager** so they may validate connectivity and schedule the next steps.