实验06-vRealize Log Insight

一、实验目的

- 1、了解vRealize Log Insight;
- 2、掌握 vRealize Log Insight 的部署与配置;
- 3、掌握 vRealize Log Insight 的基本应用。

二、实验学时

2学时

三、实验类型

设计性

四、实验任务

- 1、完成 vRealize Log Insight 的部署;
- 2、完成对 vRealize Log Insight 的基本使用;
- 3、完成使用 vRealize Log Insight 对数据中心进行日志分析。

五、实验环境

1、硬件

本实验基于实验教学中心网络运维实验室服务器集群开展,每个实验小组分配集群中的1台物 理服务器作为实验基础平台,提供云计算资源。每个人配备计算机1台。(学生可根据自身情况 使用个人计算机)。

2、软件

Windows 操作系统,或 MacOS 操作系统。 安装最新版本的浏览器,建议使用 Edge、Chrome 等。

3、网络

计算机使用无线网络接入局域网,能够访问实验教学中心网络运维实验室服务器集群,并支持 对互联网的访问。

4、工具

需要预先下载 VMware vRealize Log Insight 4.8 的 ISO 文件。

六、实验内容步骤

1、本实验需要VM1台;

2、本实验VM 配置信息如表 6-1 所示。

虚拟机配置	操作系统配置
虚拟机名称:Cloud-M1-vRLI	主机名: Cloud-M1-vRLI
内存:4GB(默认)	IP地址: 172.16.125.87
CPU:2颗(默认)	子网掩码: 255.255.255.0
虚拟磁盘:20GB+40GB+512MB(默认)	网关: 172.16.125.1
网卡:1块	DNS: 8.8.8.8
虚拟机名称: Cloud-M1-vRLI 内存: 4GB(默认) CPU: 2颗(默认) 虚拟磁盘: 20GB+40GB+512MB(默认) 网卡: 1块	主机名: Cloud-M1-vRLI IP地址: 172.16.125.87 子网掩码: 255.255.255.0 网关: 172.16.125.1 DNS: 8.8.8.8

1、部署 vRealize Log Insight

(1) 软件获取

vRealize Log Insight 可通过 VMware 官网获取评估版,下载地址为 https://customerconnect. vmware.com/downloads/#all_products,本实验所使用的版本为 VMware-vRealize-Log-Insight-4.8.0-13036238_OVF10.ova。

(2) 平台准备

本任务在前期项目完成的基础上开展,需完成虚拟化平台的建设。

(3) 在 vSphere Web Client 控制台中,选中主机资源右击,选择【部署 OVF 模板】弹出向导框,在向导的"1选择 OVF 模板"中选择"本地文件",单击【选择文件】,选择"VMware-vRealize-Log-Insight-4.8.0-13036238_OVF10.ova"文件,单击【下一页】,如图 6-1 所示。



图 6-1 导入本地文件

(4)在向导的"2选择名称和文件夹"中设置虚拟机名称、选择虚拟机存放位置,单击【下一页】,如图 6-2 所示。

── vSphere Client Q 在所有环境中搜索						
	🔋 172.16.125.63 : 黒作					
Image: Weight of the second	部署 OVF 模板	选择名称和文件夹 ^{描定唯一名称和目标位置}		>	<	ŵ
 Class-Cloud-OPs 172.16.125.63 	1 选择 OVF 模板	虚拟机名称: Clou	d-M1-vRLI			
	 选择名称和文件夹 3 选择计算资源 	为该虚拟机选择位置。 ~ 限 172.16.125.66				
	4 查看详细信息	 Class-Cloud-Datacent Folder-2025M1 	er			
	 5 选择存储 6 即将完成 					
					#	
					N(R) Xeon(R) CPU E5-2620 v4	
				取満 上一页 下一页		
へ 近期任务 警报						
任务名称 Y 对象 Y	状态 マ 详細信息	▼ 启动者	▼ 排队时间 ▼ 开始时间	↓ ▼ 完成时间 ▼ 服务部	1	Υ

图 6-2 设置虚拟机名称和存储位置

(5) 在向导的"3选择计算资源"中选择主机的计算资源,单击【下一页】,如图6-3所示。

 ● 172.16.125.63 :=* ● 172.16.125.63 :=* ● 172.16.125.63 :=* ● 187.60.00 Obtacher ● 197.16.125.63 :=* ● 197.16.125.125.125 :=* 	────────────────────────────────────				C 2025M1@CLASS.CLOUD.LOCAL	~ © ?~
Image: Comparison of the compariso	<	. 172.16.125.63				
第音性 ・	Image: Construction of the state of th	 部署 OVF 模板 1 法様 OVF 模板 2 法様 4 法様 4 法様 4 法様 4 法様 4 法様 4 法様 7 法様 6 影 4 法様 7 徒 5 法核 6 影 4 法様 7 徒 6 影 4 先後 5 法 5 法 5 法 5 法 5 法 5 法 5 法 5 法 5 法 5	选择计算资源 为选择的题程标计算资源 → Ⅲ Class-Cloud-Datacenter → □ Class-Cloud-OPs □ 17216.125.63		×	©
	▲ 近期任务 薯蓣		業容性 ✓ 兼容性检查成功、 ○ ユールマロママママママ あいいろんんし、(5) ○ ユールマロマママママママママママママママママママママママママママママママママママ	報編 上一页	м(R) Xeon(R) CPU E5-2620 v4	٠

图 6-3 选择计算资源

(6) 在向导的"4查看详细信息"验证模板详细信息,单击【下一页】。

(7) 在向导的"5许可协议"中勾选"我接受所有许可协议",单击【下一页】。

(8) 在向导"6 配置"中根据实际需要选择部署配置,本次实验勾选"Extra Small"部署配置,单击【下一页】,如图 6-4 所示。

── vSphere Client Q 在所有环境中搜索			C	^O 2025M1@CLASS.CLOUD.LOCAL ∽	⊕ ?×
<	🗒 172.16.125.63 🛛 : 🛤				
	部署 OVF 模板	配置 选择部署配置	描述	×	¢.
> 172.16.125.63	2 选择名称和文件夹	Small Medium	IMPORTANT: This configuration is intended for proof-of-concept or test environments and should not be used in a production		
	 3 选择计算资源 4 查看详细信息 	OLarge	environment. This configuration supports up to 20 ESXi hosts (-200 events/second or ~3GB/day)		
	5 许可协议 6 配 置		and requires the following: * 2 CPUs (minimum 2.0GHz) * 4GB RAM * 132GB of storage (100GB for event storage) - thick provisioned,		
	7 选择存储 8 选择网络		eager zeroed highly recommended * VM hardware version 7 or greater (vSphere 4.0 or greater)		
	9 自定义模板			•• H(R) Xeon(R) CPU E5-2620 v4	
	10 周期受起。	4 项			
			取満 上一页 下一页		
▲ 近期任务 警报					
任务名称 Y 对象 Y	状态 マ 詳細信息	间组成代 Y 间绝缘数 Y 高街道 Y	↓ ▼ 完成时间 ▼ 服务	25	T I

图 6-4 部署配置

(9) 在向导"7选择存储"中选择用于配置文件和磁盘文件的存储,选择虚拟磁盘格式为"厚置备延迟置零",并进行兼容性检查,单击【下一页】,如图 6-5 所示。

── vSphere Client Q 在所有环境中搜索			9 0 ×
·	🗄 172.16.125.63 📄 : 🕸 🕅		
III BP ■ Ø ✓ III 172.16.125.66	部署 OVF 模板	选择存储 ×	ø
 Class-Cloud-Datacenter Class-Cloud-OPs 172.16.125.63 	1 选择 OVF 模板	2017年11月1日 1) 加賀山本(本)(1) - 新賀山(新山) - 新田山大(市)(1) - 新賀山(新山) - 新田山大(市)(1) - 新賀山(新山) - 新田山大(市)(1) - 新賀山(新山) - 新山大(市)(1) - 新田山大(市)(1) - 新田山大(1) - 新田山 - 新田山大(1) - 新田山 - 新田山 - 新田山	
	2 选择名称和文件夹	▲ 對机序確循端	
	3 选择计算资源	白府 Y 存稿第合性 Y 自日 Y 已回 Y 可回 Y 英型 ○ <t< td=""><td></td></t<>	
	4 查查详细信息 5 法可协议	Image: Construction Lot 10 9.09 VG Lot 11 D VMP Image: Construction L82 TB 941.46 GB 921.29 GB VMP	
	6 配置	(123月) 毎次川田銀 10 ∨ 2 刈	
	7 选择存储		
	8 选择网络		
	9 自定义模板	蒙容性 √ 蒙容性检查成功。 ((R) Xeon(R) CPU E5-2620 v4	
	10 即将完成		
		取得 正一页 下一页	
▲ 近期任务 警报			
任务名称 T 对象 T	状态 マ 詳細信息	▼ 自动者 Y 現私的 Y 現私的 ↓ Y 完成的 Y 原気器	т 🔍

图 6-5 选择存储

(10) 在向导 "8 选择网络"中,为每个源网络选择目标网络,选择 IP 协议为 "IPv4",单击 【下一页】。

(11)在向导"9 自定义模板"中自定义该软件解决方案的部署属性,设置 Hostname、IP地址、子网掩码、默认网关、DNS和 root密码,Hostname 设置为"Cloud-M1-vRLI",
 Network 1 IP Address 设置为"172.16.125.87",Network 1 Netmask 设置为

"255.255.255.0",Default Gateway 设置为"172.16.125.1",DNS 设置为"8.8.8.8",并设置 Root Password,单击【下一页】。

── vSphere Client Q 在所有环境中搜索					
<	📜 172.16.125.63 🛛 : 🛤				
	部署 OVF 模板	自定义模板 ^{自定义该软件解决方案的部署属性。}		×	Ø
 Class-Cloud-OPs 	1 选择 OVF 模板	所有属性都包含有效值	(
> 172.16.125.63	2 选择名称和文件夹	✓ Networking Properties	8 设置		
	3 选择计算资源	Hostname	The hostname or the fully qualified domain name for this VM. Leave blank if DHCP is desired. Cloud-M1-vRLI		
	 4 查看详细信息 5 许可协议 	Network 1 IP Address	The IP address for this interface. Leave blank if DHCP is desired. 172.16.125.87		
	6 配置	Network 1 Netmask	The netmask or prefix for this interface. Leave blank if DHCP is desired.		
	7 选择存储	Default Gateway	255,255,255,0 The default gateway address for this VM. Leave blank if DHCP is		
	8 选择网络 9 自会义模板		desired. 172.16.125.1		
	10 即時完成	DNS	The domain name servers for this VM (comma separated). Leave blank if DHOP is desired. WARNING: Do not specify more than two DNS entries will be configured! 8.8.8.8	H(R) Xeon(R) CPU E5-2620 v4	
		DNS searchoath	The domain name server searchoath for this VM (comma or soace 取論 上一只 下一	页 页	
▲ 近期任务 警报					



(12) 在向导"10即将完成"中,检查信息并单击【完成】,等待创建结束,如图 6-7 所示。

────────────────────────────────────	C & 2025MI@CLASS	s.cloud.local v 😨 🕐 v
(1)	□ 172.16.125.63 : ■ * 減要 监控 配置 权限 虚拟机 资源地 数据存储 网络 更新	
 ○ [27 12:12:565 > ☐ Class-Cloud-Datacenter > ☐ Class-Cloud-OPs > ☐ 172:16:125:63 	主机详细信息 ** Hypervisor: V/Mware ESX0, 8.0.2, 233054 6 ** 型号: System x3650 MM5: [8871AC1]) MR建築型: Intel(P) Xen(P) CPU ES-2620 MR: 5 成期: 5 成期: 5 成期: 5 成期: 2.84 GB ZH 第 2.35 GB ZH MR: 5 成期: 5 成期: 5 成期: 5.33 TB 智識 東電新計量系 東電新計量系 東電新計量系 東電新計量系	٢
	配置 詳 相关対象 提供 除哪座置文件 ESX1-8.0U2b-23305546-standard CPU 32.CPU(s) x Intel(F) Xeon(R) CPU vSphere HA tk况 ? 不用用 PA PA Fault Tolerance 不受支持 DF 63.9 GB Fault Tolerance 不受支持 近 R EVC 極式 第用 近 R PA	¥
ビリック どう どう どう どう どう どう どうしょう どう どうしょう どうしょう どうしょう どうしょう いっぽう いっぽう いっぽう いっぽう いっぽう いっぽう いっぽう いっぽ		
任务名称 Y 对象 Y	358 マ 単品品を マ 自由者 マ 同日本 マ 日本 本 市 市 2 (11) マ 単語)	т
部署 OVF 模板	34% ① 正在類規準期間配置 CLASS CLOUD LOCAL/byraxd evt 11業秒 2025/03/01 09:54:50 172.16.125.66 ension-9.3419:22b-8a74-4867-94 26-22740586-339	
导入 OVF 软件包 172.16.125.63	■ 15% ② class.cloud.local/2025M1 91 笼秒 2025/03/01 09:43:49 12216.125.66	
管理列 全部 > 更多任务		3 項

图 6-7 导入虚拟机

2、初始化安装 vRealize Log Insight

(1)创建完成后,启动虚拟机进行初始化安装。浏览器访问 https://172.16.125.87,弹出欢 迎界面,单击【下一步】。

(2) 选择部署类型,单击【启动新部署】,等待部署加载,如图6-7所示。

vm Log Insight		
	选择部署类型	
	想要启动新的 Log Insight 部署还是加入某一现有部署? (如果是首次运行 Log Insight,请选择"启动新部署"。)	
	加入现有邮晋启动新邮晋	
	图 6-7 启动新部署	

- (3) 管理员用户初始化,为用户 "admin" 设置密码,电子邮件选填,单击【保存并继续】。
- (4) 添加许可证密钥,单击【添加许可证】,添加完成后,单击【保存并继续】。

vm Log Insight		
	许可证	
	许可证密明:	源加许可证
	上一步	劉过保存并摧矣

图 6-8 添加许可证

💡 提醒:此处需添加许可证,否则无法看到日志视图。也可先跳过,部署完成后再添加。

(5)设置常规配置(选填),单击【保存并继续】。

vm Log Insight
常规配置
输入系统通知应发送到的电子部件地址列表(以逗号分隔),发生重要系统事件时会生成此关握如 da, 当 Log Insight 由于確全已满而要开始检测出发现时,
系統遭知电子邮件收件人以但号分隔的电子邮件
将 HTTP Post 系统通知觉送到 以应格分隔的 URL
案户体验提升计划
VAnsare 報告体設施計计包「CEEP 1件時 VAnsare 提供信托信息」以著助 VAnsare 改进产品和服务, 就為问 置。并非確認以OPU/UEES力試算用使用我们的产品,代力 CEP お子, VAnsare 合规的回应的目的 VAnsare PFI回道如同。J型的皮革并不是通知或不是通知的正式和Table VAnsare 使用此改善或的目的。我们回应任与这些情况。此意不不得于进制个人 自己。 本支通1 CEP 形式表达就成, VAnsare 使用此改善或的目的。我们回应任与你可能用我们的工作。 用实达到Wansare Can Call Sol Ling VAnsare 使用此改善通知。VAnsare 产品的 CEP。 语言 IEIS中的发送后。它们以通知LA或进出的 VAnsare 产品的 CEP。请取 语下面已选中的发送后。如何以通知LA或进出的 VAnsare 产品的 CEP。 LL一多 在存开推放

图 6-9 常规配置

(6)配置 NTP 服务器,此处设置 NTP 服务器(逗号分隔)为"ntp.aliyun.com",单击【测试】,测试是否生效,单击【保存并继续】。

vmr. Log Insight		
- Cog maight		
	时间 配置	
	指定要与之同步的 NTP 服务器	刘表成者选择与 ESXI 主机同步时间。
	浏览器时间	2025年3月1日 上午10:54:42 UTC+08:00
	服务器时间	2025年3月1日上午10:54:41 UTC+08:00 注意 服务器时间股限间线器的时区显示
	服务器时间同步对象	NTP 服务器 (建议) \vee
	NTP 服务器 (逗号分隔)	nte.aliyun.com
		謝試 注意 町全部営業を削款 20 秒 市本がいたのの 日間初
	上—歩	說过 保存并继续
	冬] 6-10 配置NTP

(7)设置 SMTP,用于启用关于警示和重要系统通知的外发电子邮件(选填),单击【保存并继续】。

(8) 设置完成后,单击【完成】,完成系统初始化

vm Log Insight		
	0 0 0 0 0	
	设置完成	
	全部完成!	
	现在可以开始使用 Log Insight。祝您使用愉快!	
	F−#	

图 6-11 设置完成

3、集成数据源

(1) 与 vSphere 集成

系统初始化完成后,单击"配置vSphere集成",界面跳转至"vSphere",填写vCenter Server 的主机名为"172.16.125.87",用户名为"administrator@class.cloud.local"及密

码。勾选"收集 vCenterServer 事件、任务和警报"、"将 ESXI 主机配置为发送日志至 Log Insight",单击【测试连接】,对其进行连接测试。出现"测试成功"字样后,单击【保存】, 配置 ESXi 主机,配置完成后,单击【确定】,如图 -12、6-13、6-14 所示。



图 6-12



图 6-13 配置集成vSphere

vm Log Insight	仪表板 交互式分析				无拚可证(更多) 💄 adn	ⁿⁱⁿ ≡
管理 系统监控 群集	vSphere × ^{服除}				vCenter Serv	er:1 @
访问控制	□ 主机名	、 收集事件	○ ESXI 主机已配置	⇒ 目标	⇒ 用户标记	
主机	172.16.125.80	/ 是	是 (查看详细编显)	172.16.125.87		
代理						
事件转发						
许可证						
集成						
vSphere						
vRealize Operations						
配置		Ed	动完成配置			
常规			确定			
时间。						
SMTP						
存档						
SSL						
						<u> </u>

图 6-14

(2) 与 vRealize Operations 集成

选择左侧的"集成"选项卡中"vRealize Operations",界面跳转至"vRealize Operations集成",填写 vRealize Operations Manager 的主机名为"172.16.125.86",用户名为"admin" 及密码。勾选"启用警示集成"、"启用"在环境中启动"",单击【测试】,对其进行连接测试。 显示"测试成功"字样后,单击【保存】,注册 vRealize Operations 数据源,注册数据源成功 后,单击【确定】,如图 6-15、6-16 所示。

图 6-15 集成vRealize Operations

vm Log Insight	仪表板 交互式分析	无许可证(更多) 💄 admin 🚍
日本 本成二定 不定 不定 不定 本の の の の の の の の の の の の の の	vRealize Operations 集成 vRealize Operations Manager ① 世报 172912580 回時 在环境中启动 vRealize Operations max ② 正在环境中启动 vRealize Operations Manager 建册率功. 建	
#481 SSL		K

图 6-16 注册成功

4、使用日志分析仪表板

(1) 管理仪表板

①在自定义仪表板中,有"我的仪表板"和"共享仪表板"两种。用户仪表板存放每个独立用 户的仪表板组件,未进行共享前,其他用户无法使用该仪表板。如图 6-17 所示。

vm Log Insight	仪表版 交互式分析	上 admin 😑
白定义仪表板 [◇] 我的仪表板 Deshboard 1	最近5分钟的数据 ✓ で 在所有小组件上显示磁例 ① ● + 通貨券28	E
> 共享化型版 PJ容信0/发展 > Apache - CLF > General > VMware - VSAN > VMware - vRops 6.7- > VMware - vSphere	Total Events	 € doud m1 + so 1 € doud m1 + so 2 € 725 50 38
- 100.015		

图 6-17 我的仪表板

②共享仪表板中默认没有组件,要想将加入组件,要使用"新建仪表板"按钮或从内容包中克 隆现有仪表板。共享仪表板中的组件,对所有的用户都是开放的。用户可对共享仪表板中的组 件进行添加、修改和删除等操作,如图 6-18 所示。



图 6-18 共享仪表板

③内容包仪表板存放的是从内容包商城中导入的已经定义好的仪表板组件,不能进行修改,可 以克隆到我的仪表板中。

(2) 小组件的使用

④在各个仪表板中可通过添加和删除筛选器来精确查找日志。如图 6-23 所示





⑤通过单击图表组件的右上角的"在交互式分析中打开"的图标,可详细查看与其相关的日志 情况,如 6-24 图所示。

vm Log Insight	仪表板	交互式分析			🔺 admin 😑		
		计数 事件 分组族语 hostname		◎ ₩55	□ 第加3000000 ¹		
				cloud m1-exxi-3 cloud m1-exxi-2 cloud m1-exxi-1 172-16.125.81 172-16.125.83 172-16.125.83			
计数 / events + 分担依据 hostname +				图表	·····································		
		★ 報道	£5分钟的数据 🗸 🍳	* I 🖬 I	. - C*-		
		20	2025/3/1 17:35:06.716 到 2025/3/1 17:40:0	9.605			
+ 添加等迭器 中変数 ~ (将取((本文型)							
中 件 子段表 甲件类型 甲件趋势		1]	1 50 / 50+事件 查看* 排序:最新的优先*	宇段	44		
2025/3/1 2025-03-01T09:40:07.565Z Cla 17:40:06.715 遼 event_type hostname ap	oud-M1-ESXi-3 Ho pname vmw_esxL	sstd: info hostd[20086443][Originator96676 sub⊔lbs] SOCKET connect failed, error 2: No such file or directory _seventyvmw_ebd_seventyvmw_ebd_sub		appname			
200531 2825-8-81789-48-07.5622 (loud-mr-ESNi-3 Hostsi info hostsi(2886640) (Driginator46876 submiles) SODRET creating new socket, connecting to /var/run/wmare/usbarbitrator-socket 274005371 🕱 ever_type hostmane approace wmw_sast_everby wmw_sast_everby wmw_sast_everby mm_sast_everby wmw_sast_everby wmw_sast_everby							
2025/31 2825-0-01191-4-07.0452 (Coud-01-5321-2 Rhtsports): verbase rhttsports/2107878] [Originator48076 sub-Proxy Reg 09051] Consected to localhost:8889 (ryss) over <io.dbj <br="" h:19,="" p:0x00080074004458,=""></io.dbj> Cloud-01-5321-2 Rhtsports/2107878] [Originator48076 sub-Proxy Reg 09051] Consected to localhost:8889 (ryss) over <io.dbj <br="" h:19,="" p:0x00080074004458,=""></io.dbj> Cloud-01-5321-2 Rhtsports/2107878] [Originator48076 sub-Proxy Reg 09051] Consected to localhost:8889 (ryss) over <io.dbj <br="" h:19,="" p:0x00080074004458,=""></io.dbj> Cloud-01-5321-2 Rhtsports/2107878] [Originator48076 sub-Proxy Reg 09051] Consected to localhost:8889 (ryss) over <io.dbj <br="" h:19,="" p:0x0080074004458,=""></io.dbj> Cloud-01-5321-2 Rhtsports/2107878] [Originator48076 sub-Proxy Reg 09051] Consected to localhost:8889 (ryss) over <io.dbj <br="" h:19,="" p:0x008007404458,=""></io.dbj>							
202501 222-83-01769-40.07.852 Cloud-MI-ESG-2 Rhttpproy: verbose rhttpproy[208670] [Driginator68576 sub=Proy Reg 80837] Resolved endpoint : [UTmacore=Http1ExccalServiceSpecE:bn80000867ac233a0] _serverHamsspace = /upua action = Allow _port = 8089 (202505) 202-83-01769-401, portuge = Approx = Allow _port = 8089 (202505) 202-83-01769-401, portuge = Approx = Allow _port = 8089 (202505) 202-83-01769-401, portuge = Approx = Allow _port = 8089 (202505) 202-83-01769-401, portuge = Approx = Allow _port = 8089 (202505) 202-83-01769-401, portuge = Allow _port = 8089 (202505) 202-83-01769-401, po							
2025/3/1 2025-03-01709:40:07.036Z C10 17:40:06:501 遼 event_type hostname app	oud-M1-ESXi-2 Rh pname vmw_esxl	ittppray: verbase rhttppray[2008672][Originator#6876 sub=Pray Req 00057] New pray client <5L(<io,dbj 1172.16.125.82="" 443'="" :="" <to*="" h:18,="" p:0x000000007e276c0,="">, <to* 11<br="">_seventy vmm_stat_seventy</to*></io,dbj>	/2.16.125.80 : 36954'>>)>				
2025/3/1 2025-03-01T09:40:07.032Z C10 17:40:06.498 # event_type hostname ap	202543- 2025-63-017891-69-07.8322 Cloud-MT-ESGI-2 Vpa: info vps2[209220] [Originator068376 sub-vpatro egit=PollQuickStataLoop-Stel2b11-e3] [VpuLR0] FNUSH Iro-4834 [74:00:488] 🦉 ever_type hommen vmu_exct_seventy vmu_exct_sev						
2023/21 2825-82-91785-46-87.822 Cloud-M1-65G-2 You: info you(289228) [Originetre8886 sub-mpc/ro qs10#01]QuidStatsLoop-51862811-e3] [YpuR0] 88GIN Iro-4834 ypug							
2025/3/1 2025-03-01T09:40:07.347Z C10 17:40:06.497	202551 2825-49-41189:49-67.3472 Cloud-MI-ESXI-1 Vpaz: info vpaZ2892321 [Originatur68476 aub-vpar.co.gotDe+01[QuickStates.cop=51e82b11-56] [VpuLR0] FDdSH [ro=4646 [724006-877 🚆 evert.pps hotmane opprane vmic.eox_severty vmic						
2025/3/1 2025-03-01709:40:07.347Z Clo 17:40:06.497 遼 event_type hostname app	oud-M1-ESXi-3 Vp pname vmw_esxL	xa: info ypa[209212] [Originator06876 sub-upuro opDT#011QuickStatsLoop-57682611-5d] [YpuR0] 865DY lro-6449 ypxa ypxapi YpuAService.fetchQuickStats 528609 Lewenty vmuLeoLLewenty vmuLeoLLeub vmuLopd	74-3950-09a8-4529-89fd75b85f12				
2025/3/1 2025-03-01T09:40:06.4822 C10 17:40:06.497	oud-M1-ESXi-1 Vp pname vmw_esxL	xa: info vpud(20091031] [Originator#8876 sub-vputro op]D=follQuickStatuLoop=57682b11-31] [VpuLRO] FDNSH lro=5883 _seventyvmm_excl_soventyvmm_excl_sobvmm_expd					

图 6-24 交互式分析

5、日志浏览与检索

(1) 按时间范围浏览和检索日志

选择仪表板图表组件,在交互式分析界面中打开,对图表组件进行不同时间范围的日志查看和 检索。如图 6-25 所示。

vm Log Insight 仪表板 交互式分析				🔺 admin 😑		
2005/31 114416 近 10.74417 (6.795) 计数 事件 f3 略一计数 hostname 18时间			⊘ ₩∰	175.1015(K)38482		
	1645 1700 1715	17:30	1.3 ■ 容件计数 ■ 龍一計数/hostname 2.4			
计我/events - 論—计我/hostnume - x 的时间 - 白河 田田			·····································	▲ 爾德國 - ▲		
h	▼ 最近6小时的数据	_~ ଦ	*	. - 🖆 -		
	最近 5 分钟的数据 最近 1 小时的数据 最近 6 小时的数据 最近 24 小时的数据	2025/3/1 17:44:	17.406			
事件 予約束 専作規型 専作規型 専作規算 200531 2825-87-81789.44.87.3742 Claub-91-4534-3 MARKE info hosts[2898648] [OriginstarM8876 sub-Lib2] 500ET connect failed, error 2: No such file or directory	最近 48 小时的数据 最近 7 天的数据	2. 最新的优先 *	字段 //	⇒		
(V4400.27) @ eer_type hostname sponse wm_ext_levery wm_est_levery mm_est_levery mm_est_levery 200501 2025-83-019914-89, 5922 (load-t-554-3) 586364 in hosts(20958449) [Druginster/6859 sub-Lib3] 500ET creating new socket, connecting to /ver/run/vmere/usbarbitrator-socket (V4400.27) @ evertype hostname sponse wm_est_levery mm_ext_levery wm_ext_levery mm_ext_levery.	自定义时间范围		event_type hostname vmw_esxi_severity (VMws vmw_esxi_severity (VMws	re - VSAN) O		
200501 2025-03-01195/44/06.4822 Cloud-M1-ESXi-1 1964: info vpsc[2009302] [Originator96878 sub-vpsc/ro opDimPollQuickStats.cop-37682811-68] [Vpsc.80] FINISH Iro-4902 0/400400 🕱 everpps hotemane appener vmc_escl_everby vmc_escl_everb						
200501 2825-43-41193-41-87.342 (Lood-M-ESK)-3 (www.:sefo-spool/2092121) (Draginator#8816 sub-ryou.co optio=foll0uicidStateLoop-31e82011-35) (VpuLRI) -+ FINISH Iro-4949 (FANDS-803 🗿 ever_type footmame approxime vmu_excl_seventy						
200501 2825-83-81789:44-84.882 Cloud-91-85X1-1 1988: info yps2(2897882) [Originstor8878 sub-yps1/or op10+PollQuickStats.cop-37682811-b8] [Op4.R] 8801N 1ro-4982 ypsa ypsapi. Vps58rvice. fetchQuickStats 52857fbe-888e-9686-968e-858a781c7829						
200531 222-03-01789:44:07.0222 Cloud-M1-25X1-2 1990: info ypus(20092113) [Originator06816 sub-pputro optD#PollQuickStatsLoop-37682011-37] [VpusR0] FINISH Iro-4642 (7.4400.63) 🗃 everLype bozzame appname wmw_eol_seventy wmw_eol_se						
202531 223-03-01109-44:07.3452 Cloud-M1-ESG1-3 1908: info-spac209022222 (Originator68016 sub-space optD=PollQuickStatsLoop-Ste22011-352 [VpsLR0] 8002N lro-4449 spac space	528069f4-3950-09a8-4529-89fd7	5b85f12				
202531 2225-03-01709-04:07.0222 Cloud-MT-ESGL-2 1900: info-pps200921713 [Originator06076 sub-ppiro optD=PollQuickStatsLoop-Stel2011-5f] [VpuL00] 8602N lro-6442 vpua vpuaji.VpuService.fetchQuickStats 12400.038 🚆 even_type hostmane approare wmw_escl_seventy wmw_escl_	5257d175-7487-1877-ab78-4ce18	119861e				
2005/31 2825-83-81789:44:86.4782 (Daud-MH-SSG-) Mittgoroup: vertose rhttpprop(288868) [Originstor66876 sub-Provy Reg 18272] Resolved endpoint : [DM/Macore4Http16.ocalServiceSpecE:b000008aF6d3a698] _serverNames	pace = /vpxa action = Allow _p	ort = 8089		-		

图 6-25 时间范围日志

(2) 按字段运算检索日志

在交互式分析界面,单击"添加筛选器",使用筛选器筛选字段日志,如图 6-26 所示。

Vm Log Insight 校表版 交互式分析	上 admin 😑
2025/01 (7:53-44 回 (7:58-48) (5)(行)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)	
	15 15
計載/events・ 唯一計載/hostname・x 第23周・ 印用 監査	1位间隔 = 5秒 • 图表类型 🖬 兩時週 • 🏦
★ 最近 5 分钟の激調 <	۹ 🚽 👷 ا 📷 ا 🜲 ا 🖄 ا
CRE全部・UTRABA 2025/31/17/534844 2025/31/17/5488 2025/31/17/5 2025/31/17/5488 2025/31/17/5488 2025/31/17/5488 2025/31/17/548 2025/31/17/548 2025/31/17/548 2025/31/17/548 2025/31/17/548 2025/31/17/548 2025/31/17/548 2025/31/17/548 2025/31/17/548 2025/31/17/548 2025/31/17/548	58-48143
An text	
## apache_cf_remote_user (Apache - CLF) 111501200平日 単音・旧木 豊新放気・	宇段 🖉 🕨
epache_df_url_fletype (Apache - CLF) apache_df_url_fletype (Apache - CLF) apache_df_user_egen_browser (Apache - CLF)	 ■ 源 ■ appname
apache_df_user_agent_browser_version (Apache - CLF) y12088665 [Originator86876 sub=Prany Req 00726] Resolved endpoint : [NTVmacore=Wttp16LocalServiceSpecE:8nd0000052667865100]_serverNamespace = /s6k action = Allow _port = 8307	even_type hostname vmw_esxi_device_id (\/Mware - vSph
apache_df_user_ogent_os_version(Apache - CLF) ar: 5544: Otacking disconnected filters for timeouts apache_bitm_engre_mission(Apache_CLF) toront toront	vmw_esxi_scs_additione_senseO vmw_esxi_scs_device_status (vMwO vmw_esxi_scs_device_status label
202501 222-43-01105.81.37.0172 Cloud-m-LSX12 inkernal: cpu1:2097680/DWFilter: 5564: CHecking disconnected filters for timeouts 7558/8577 generype homeme sphame symme semuces.unk.unk.unk.component	vmw_esxi_scsi_host_status (\/\/www vmw_esxi_scsi_host_status_label vmw_esxi_scsi_plugin_status (\/\/w
2025/31 2825-087-01109:58:37.3492 Cloud-M1-ESXI-3 Mitsparany: verbose rhttspravy(2866655) [Originator66376 sub=Provy Req 09212] Resolved endpoint : [UTVmacore=Http16LocalServiceSpecE:Bu000005266786160]_serverNamespace = /upus action = Allow _port = 8869 UTSR/0.90	vmw_esxi_scsi_sense_code (\//wwwO vmw_esxi_scsi_sense_data (\//wwwO vmw_esxi_scsi_sense_label
2025-01 2023-087095-181:86.6512 (20ud-m1-E5X1-2 Media):> 75838.3538 ∰ event_type incomme approame	vmw_esxi_severity (Vi/were - VSAN) vmw_esxi_severity (Vi/were - vSphere) vmw_esxi_sub (Vi/were - vSphere)
2005.01 2825-08-08109-58-36.4512 (Doud-MI-ESKI-2 Messá: error hosta(245468) [Originetor96876 sub-default] [LikewiseGetDomainJointInfo:354] QueryInformation(): EMBOR_FILE_NOT_FOUND (2/8): T558:35:38 🗶 exec_type hostmama appearma mun_ese_typeerty mun_ese_type	vmw_esxi_vmk_component (VMwarO vmw_esxi_vmk_world (VMware - vSpO vmw_opid (VMware - vSphere) vmw_opid(VMware - vSphere)
2025-01 2825-83-01789 58-37.0452 Cloud-m-E5Xi-3 Hostof:> 7.5838.029 ፹ even_type hostrame approare	vmw_user (VMwere - vSphere)
2005/31 2225-01-01191-34:27.4682 (Doub-M-1531:-) MARE: error hosts(245459) [Originator46876 sub-Offmult] [LikewiseGetdomainJoin[hfo:354] QueryInformation[): EMON_FILE_NOT_FOLD (2/0): 758352:09 🦉 over_type hotoama apprame wmm_esst_eventy wmm_esst_eventy wmm_esst_eventy	

- 图 6-26 筛选器检索
- (3)分析日志事件类型和事件趋势
- ① 在交互式分析界面中,单击"事件类型"子选项。然后在搜索框或者添加一个为 "hostname"、"包含"、"Cloud-M1-ESXi-2"的筛选器。如图 6-33 所示。

vm Log Insight 仪法版 女互式分析	💄 admin 😑
2025/341 1802201 影 1807/03	🖸 1455 🖬 WALLEN (1881
计数 事件 和 唑一计数 hostname 授时间	
	12 事件計載 電 一計数Thotanueme 0.6
は数/worse # 計数/hoorsene - x 時時间 - D 動産	间隔 = 5秒 • 图表类型 🖬 面积图 • 🌲
cloud-mi-ess/2	
	2.264
Andra Results Results Results Results and Andra	J3.204
+添加消益器 × 活致全部消益器	
内音包 (20%所有字段)	
## 字段表 ●### ##信節 1月47.47.#### 1月47.47.#### 1月47.47.##### 1月47.47.##### 1月47.47.#####	宇段 🆉 🙌
510 2023-03-01118-06-44.2557 - Cloud-MT-ESK1-2+ vsentrecorpent: 5+ [27285+] [qu1+] [BESINC-] DOMTrecoCopyCologRevolutes+11822+; ('latencyPerQuantmat': 8, 'augUnualbeth*at': 8, 'augUnualbeth*i: 8, 'augUnua	appname event_type hostname
100 2023-02-01116:86:44.289* - (Lood-MI-ESE-2+ valentraceurgent: 6+ [27281+] [coul-] [] DOMTraceCompEdedStat3:11788: ('num compLete 10': 0+, 'arg 10 Congestion': 0, 'arg estimated 10 Congestion': 0, 'arg Regulator Iops': 0+, 'isteeventurgent: 6+, 'isteeventurgent:	source vmw_esxi_device_id (\Mwsre - vSph O vmw_esxi_scsi_additional_sense
50 2015-03-01110:061-04-251-2- vantraceurgent: 9+ [272327+] [gud+] [00154-] D0MTraceConpEcheRQueeNEstats:11882; ('llatencyPerQueeNest': 256329+, 'ausubleptMax': 84+, 'augQueeNesth': 8+, 'augQueeNesth': 8+, 'augIOST: 8, 'aug Endedth': 8+, 'aug Latency MS': 8, 'augustiest: 19993356888+) S9 (CONTRACEURGENE)	vmw_esxi_scsi_additional_senseO vmw_esxi_scsi_device_status (VMwO vmw_esxi_scsi_device_status_label
45 2025-03-01110:06:37.0492 * Cloud-MT-ESXi-2* Rhttproxy: verbose rhttproxy(2006072+) [Originator06076 add=Proxy Req 00075+] Resolved explorint : [UTmacore=Wttp1EcoalServiceSpecE:bn000000020a233a0+]_serverNamespace = /vpma+ action = Allowport = 8685+ 	e vmw_esxi_scs_host_status (vMwar 0 vmw_esxi_scs_host_status_label vmw_esxi_scsi_plugin_status (vMw 0 vmw esxi_scsi_plugin_status (vMw 0
26 2025-03-01110:05:34.4042* Cloud-M1-E5Xi-2* Vpxa: info vpxa[2095218*] [OriginatorNdAT6 sub-vpx1r0 opID+08-host-1402455-1605072*=4*] [Vpx1x0] FINISH* Ino-4852* 20 4 (SUBERSPIR (BF)	vmw_esxi_scsi_sense_data (v1/wer ④ vmw_esxi_scsi_sense_label vmw_esxi_scsi_sense_label
24 2025-03-01110:06.562+ Cloud-M1-E5Ki-2+ storage894-[2058710+]: getting state for WES volume Cloud-M1-HFS 24个公共进行第一(展行)	vmw_esxl_severity (VMware - vSphere) vmw_esxl_sub (VMware - vSphere) vmw_esxl_uptime (VMware - vSphere)
2() 2015-01-01116-06-44.251- Cloud-MI-251-2- vantraceurgent: 7- [17219-] [goul-] [] DOMYaccousticedStatiz111772: ('semiatencyforActivationUs': 1072919685-, 'avg 10 Size': 0-, 'latencyforActivationUsus': 250220-, 'istrite': Trva-, 'sempenedBytes': 114438726-, 'avg-10 Size': 0-, 'latencyforActivationUsus': 250220-, 'istrite': Trva-, 'sempenedBytes': 2001251-, 'avg-10 Size': 0-, 'latencyforActivationUsus': 250220-, 'istrite': Trva-, 'sempenedBytes': 2001251-, 'avg-10 Size': 0-, 'latencyforActivationUsus': 250220-, 'istrite': Trva-, 'sempenedBytes': 2001251-, 'avg-10 Size': 0-, 'latencyforActivationUsus': 250220-, 'istrite': Trva-, 'sempenedBytes': 2001251-, 'avg-10 Size': 0-, 'latencyforActivationUsus': 250220-, 'istrite': Trva-, 'sempenedBytes': 2001251-, 'avg-10 Size': 0-, 'latencyforActivationUsus': 250220-, 'istrite': Trva-, 'sempenedBytes': 2001251-, 'avg-10 Size': 0-, 'latencyforActivationUsus': 250220-, 'istrite': Trva-, 'sempenedBytes': 2001251-, 'avg-10 Size': 0-, 'latencyforActivationUsus': 250220-, 'istrite': Trva-, 'sempenedBytes': 2001251-, 'avg-10 Size': 0-, 'latencyforActivationUsus': 250220-, 'latencyforActivationUsus': 250220-	
2() 205-09-01710-06-44,2597+ Cloud-MI-ESG-2+ vasatraceurgent: 6+ (27237+) [cpu8+] [] DOMTraceCoupEchedStats1:11778: ('numEchedStal1: 429426+, 'numEchedStal1: 429426+, 'numEchedStal2: 429426+, 'num	tymw_opid (VMware - vSphere) vmw_scsideviceio_pid (VMware - vSp vmw_task_status (VMware - vSphere)
2 2023-03-01110-05.46.4972 • Cloud-MI-ESX:-2+ Hostd: info hostd(2008658-1 [Originator98876 ad=Golo.VmareCLI opt]0+0678831c+ user=doui:vsamgetd+] Dispetch list done+	VMW_USER (VMware - vSphere) Vmw_vc_managed_host_id (VMware Vmw_vc_task_method (VMware - vSp
A A ALLANDON (A ANTI)	· · · · · · · · · · · · · · · · · · ·

图 6-27 事件类型

② 分析其如图 6-34 之中的 Cloud-M1-ESXi-2 事件趋势。在交互式分析界面中,单击"事件趋势"子选项。添加筛选器,如图 6-28 所示。

vm Log Insight 仪表版 交互式分析		🛓 admin 😑
2025-31 180357 目 180964 合分(F66)) 计数事件 和 唯一计数 hostname 按时间	O tess	🖬 iatosikkasik
224	4 ■ 第件計数 ■ 唯一計数/hostname 2	
注意 Zeverts 第一十歳 / hottmane × 約3回。 二 単直 年前の 2015 3 / hottmane × 約3回。 二 単位の 2015 3 / hottmane × 約3回。 2015 3 / hottmane × 約3回。 2015 3 / hottmane × 2015 3 / hottmane	3)% = 5∯ • <u>NR##</u>	▲ 1997- ×
X event_type 不为 (w_1,5102856 ·)(W_1,8835004 ·) * 原加時各書 × 清除全部件各書		
内着型 (回初所行中四) 毎件 字段表 毎件独型 1月1.1年(中四) 日末 運動(25,5) 単一 年(15,5) 日本 日本 第二 年(15,5) 日本 日本 第二 日本 日本 日本 日本 第二 日本 日本 日本 日本 第二 日本 日本 日本 日本 日本 日本 日本 日本 日本	字段 🖉	₩
2025-03-01T10 08:38.5852 Cloud-MT-ESXi-3 vekernel: cpu3:200763400vFilter: 5964: Checking disconnected filters for timeouts 3 今点共同記事件 個明	event_type hostname source vmw_esxl_vmk_compoi vmw_esxl_vmk_world (v	ient (VMwer O Mwere - vSp O

图 6-28 事件趋势

- (2) 向 vSphere 发送警示
- 在交互式分析界面中选择"创建或管理警示"图标,选择"管理警示",勾选"VMwarevSphere内容包",单击【启用】,使用预定义警示,根据需要勾选,本次实验勾选并设置电 子邮件,单击【启用】,单击"x"退出,向vSphere发送警示通知。如图6-29、6-30、6-31所示。

vm Log Insight								💄 admin	
2025/3/1 18:03:57 등) 18:09:04 (6 중1한 6 원)								o tes el susta	
1.2 1.2 1.60+00 18:00+15 18:00+30 1				fen inden inden inden in	0200 18-0215 18-02200 18-0	18 180800 180815 180820 180		寧件計數 唯一计数/hostname	
计数 / events + 唯一计数 / hostname + × 按照				警示	×				
	-#1-E5X1-3 vek	(v4_5%285%) (v4_ (v4_2bed964e) ernel: cpu3;2097634)	DFilter: SE4: Owoking discons	EVERSION/EX Security Security (Security Security Secure Security Secure Security Security Security Security Security Sec	be consided	★・ 単近5 分钟的数据 2025/3118-0357446 31 31311 (1日の次回 15311、1日の次回 単の次回講師1今7349 五十、回して	2025/3/1 10:05:04-406 2025/3/1 10:05:04-406 800:05:05 800:05:05 90	rie Jype Inte sel_vmic_component (Mase Sel_vmic_world (Masee visit)	*
					202				•

图 6-29 启用警示

vm Log Insight 仪表板 交互式分析			🛓 admin 😑
202531 180357 5; 180904 (6.5)(6.6))			o ve 🖬 izuzikan
24			■ 寄梓計載 ■ 唯一計載/hostriame
nadezo indens	decon 1886-18 1886-10 1886-85 1886-20 1886-189 1886-20 1886-20 1886-20 聲示 X		≅= 5 秒 • 图表发型 ▲ 面积图 • ▲
	启用警示 格局用以下警示并保存到"我的警示": ESX: Cannot power on a VM Network: ESX uplink redundancy lost Security: ESX uplink redundancy lost Security: WebMKS Events ESX: License has expired	★ 単近 5 分钟的旅游 Q 2025-31 1803.57446 別 2025-31 1805-044	
事件 字段表 事件独型 事件趋势	ESX: Unsuccessful authentication vCenter Server: DRS imbalance detected and could not be corrected	1到1/1事件按照 排來 增加的优先 * 5	₽段 ℓ →
2023-93-911118:08:38.9852 Cloud-M1-ESU-3 velormel: qual:2007E43[0VFilter: 5964: Decking discon	□ 电子邮件 以坦告分隔的电子邮件抽址 □ Webhook 以包括分隔的 URL □ 发送到 vRealize Operations Manager	₩10000000111111000支入110027111100000000000000000000000000000	si appname jevent, type ji outrame ji outrame ji vmv_sexLvmk_component (Viker Ø vmv_sexLvmk_world (Viker Ø

图 6-30 启用警示

		👗 admin 🚍
	○ 保存成功	
2.4 1.3 1.2 Ledvoo 112-bits 112-bit	警示 x ^{要实现的快型}	2.4 1.2 1.3 1.4 1.4 1.4 1.4 1.4 1.4 1.4 1.4
 添加算器器 ×清整全部装置 内容包 < (0500/F87590) 	- ESAT Lafinot polier on a vixi 문화(中語句句) - ESX: Hå koleted events by hostname 문화(中語句句句)	
事件 字段表 単件地型 単件地算 2025-03-01716 88 3852 Cloud-01-635(-3 veloanel: cpu3.2097634)D97315er: 5964: Owoking discommendation (Cloud) (Cl	SER Librate has expired SER installed SER installed SER installed SER installed SER installed SER installed X	1511 1 年4年8日 初示 第2000分5 * 学校 * ** マロルの回答 1 4 行政を支 た、防止于 低 50 分岐 * ① ロのの回答 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
	Electronic State	B mm_dmd_mm_dmd()/hom-+().

6-31 启用警示

七、实验讲解

本实验配置讲解视频,访问课程学习平台。

八、实验考核

实验考核为【实验随堂查】。

实验随堂查:每个实验设置3-5考核点,学生现场进行演示和汇报讲解。

1、考核点

考核点1:完成vRealize Log Insight的部署,能够访问到vRealize Log Insight系统。(40分)

考核点2:集成 vRealize Operations 和 vSphere 数据源,并要求仪表板中的 VMware - VSAN 仪表板能够正常显示数据。(30分)

考核点3:在交互式分析界面通过添加筛选器查看数据中心之中Labs-Cloud-ESXi-node-1的日志事件。(30分)

2、考核方式

以实验小组为单位进行考核,每个小组由1位同学进行实验成果汇报,小组其他成员回答教师 提问。根据汇报和答疑情况,对小组成员进行逐一打分。

由教师进行评分。