

实验九：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



扫码看操作演示

四、实验需求

1、硬件

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）。

每个人分配网络运维实验室的服务器 1 台（预先安装 VMware vSphere ESXi）或提供云计算资源。

2、软件

Windows 操作系统，或 MacOS 操作系统。

安装 VirtualBox 或 VMware WorkStation Pro。

安装最新版本的浏览器，建议使用 Edge、Chrome 等。

3、网络

计算机使用固定 IP 地址接入局域网，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。

五、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。

六、实验环境

- 1、本实验需要 VM 1 台；
- 2、本实验 VM 配置信息如表 9-1 所示。

表 9-1 虚拟机配置信息

虚拟机配置	操作系统配置
虚拟机名称: Labs-Cloud-vRealize-Log-Insight	主机名: Labs-Cloud-vRealize-Log-Insight
内存: 4GB	IP 地址: 10.10.2.126
CPU: 2 颗	子网掩码: 255.255.255.0
虚拟磁盘: 20GB+40GB+512GB	网关: 10.10.2.1
网卡: 1 块	DNS: 10.10.3.70

七、实验内容步骤

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，选中资源池“Student-2024181999-学生姓名”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【NEXT】，如图 9-1 所示。

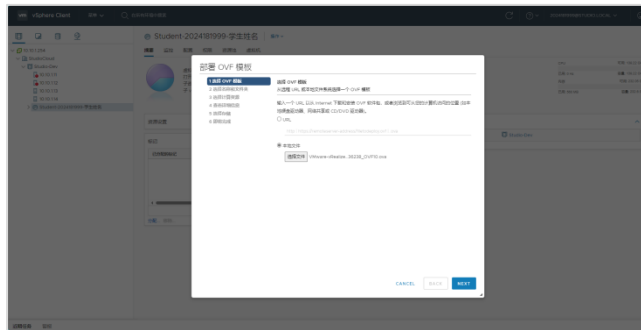


图 9-1 选择 OVF 模板

(4) 在向导的“2 选择名称和文件夹”中设置虚拟机名称为“Labs-Cloud-vRealize-Log-Insight”、选择虚拟机存放位置为“实验-学生姓名”文件夹，单击【NEXT】，如图 9-2 所示。

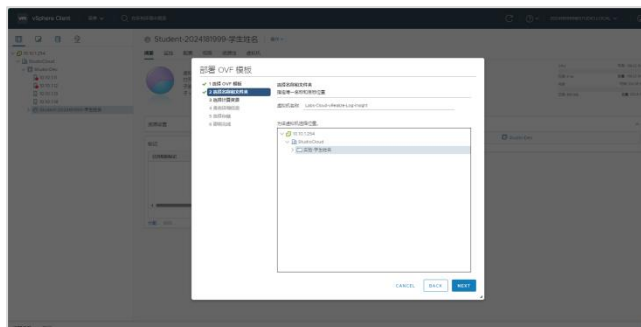


图 9-2 选择名称和文件夹

(5) 在向导的“3 选择计算资源”中选择资源池“Student-2024181999-学生姓名”，单击【NEXT】，如图 9-3 所示。

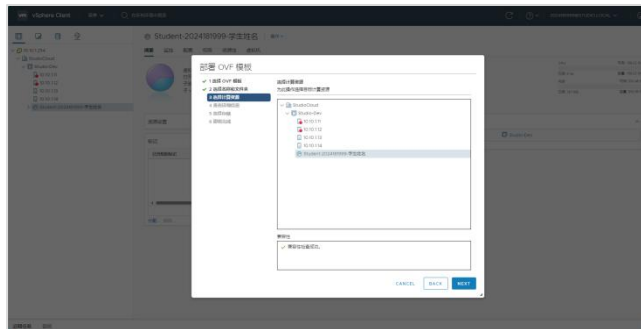


图 9-3 选择计算资源

(6) 在向导的“4 查看详细信息”验证模板详细信息，单击【NEXT】，如图 9-4 所示。

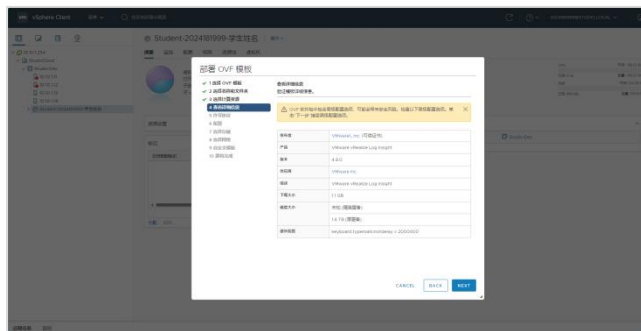


图 9-4 查看详细信息

(7) 在向导的“5 许可协议”中勾选“我接受所有许可协议”，单击【NEXT】，如图 9-5 所示。

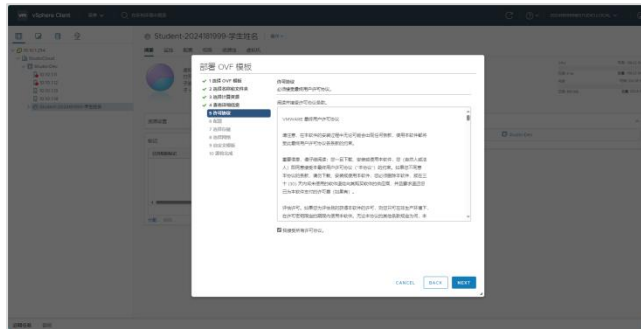


图 9-5 勾选许可协议

(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【NEXT】，如图 9-6 所示。

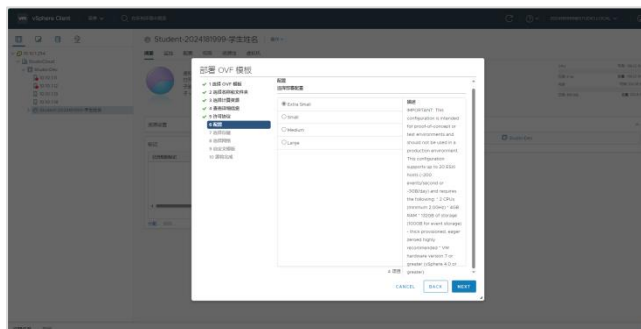


图 9-6 配置

(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【NEXT】，如图 9-7 所示。

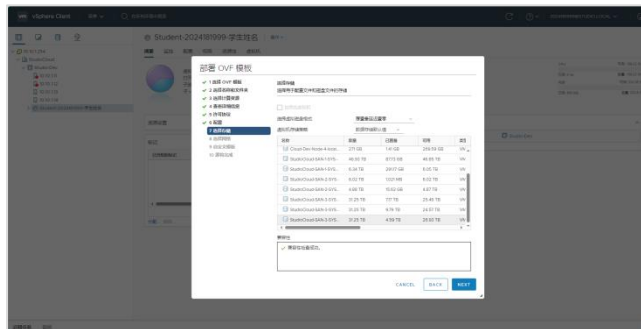


图 9-7 选择存储

(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【NEXT】，如图 9-8 所示。

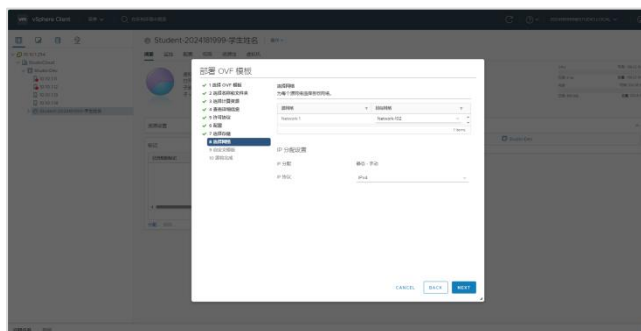


图 9-8 选择网络

(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“Labs-Cloud-vRealize-Log-Insight”，Network 1 IP Address 设置为“10.10.2.126”，Network 1 Netmask 设置为“255.255.255.0”，Default Gateway 设置为“10.10.2.1”，DNS 设置为“10.10.3.70”，并设置 Root Password，单击【NEXT】，如图 9-9 所示。

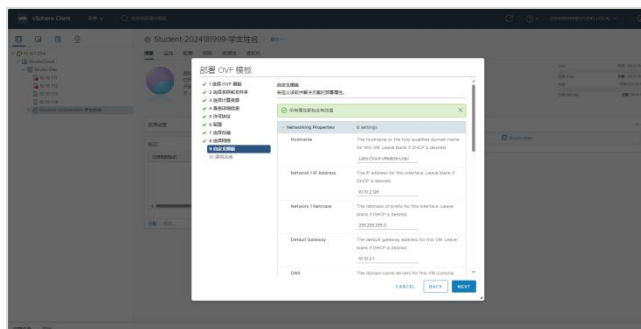


图 9-9 自定义模板

(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 9-10 所示。

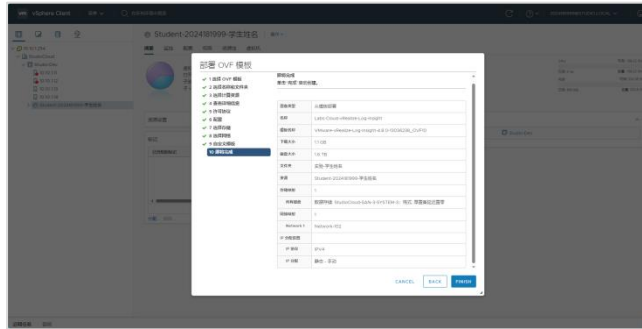


图 9-10 完成部署 OVF 模板

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://10.10.2.126>，单击【下一步】，如图 9-11 所示。

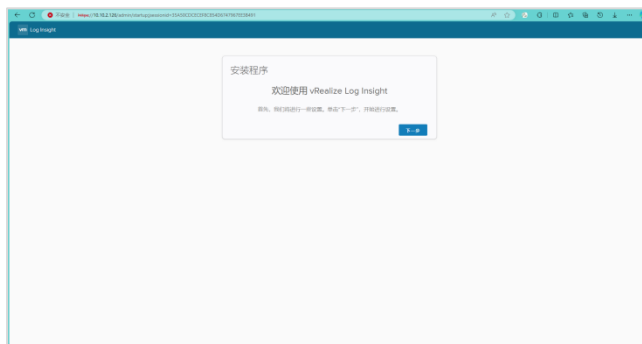


图 9-11 安装程序

(2) 选择部署类型，单击【启动新部署】，等待部署加载，如图 9-12 所示。

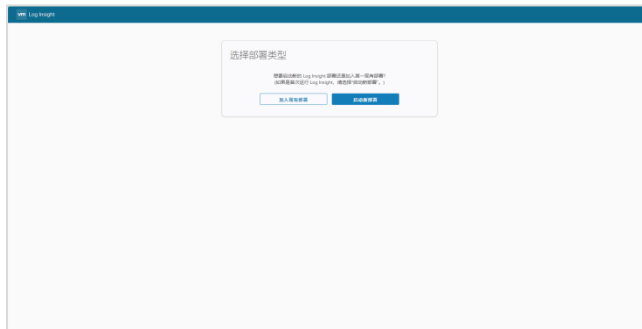


图 9-12 启动新部署

(3) 管理员用户初始化，为用户“admin”设置密码，单击【保存并继续】，如图 9-13 所示。

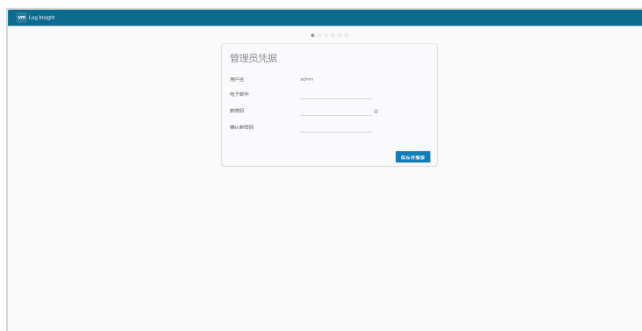


图 9-13 输入管理员凭据

(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】，如图 9-14 所示。

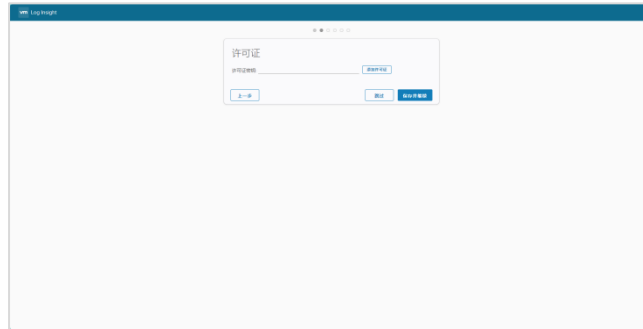


图 9-14 添加许可证

(5) 设置常规配置，单击【保存并继续】，如图 9-15 所示。



图 9-15 常规配置

(6) 配置 NTP 服务器，设置 NTP 服务器(逗号分隔)为“10.10.3.70”，单击【测试】，测试是否生效，单击【保存并继续】，如图 9-16 所示。



图 9-16 时间配置

(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，单击【保存并继续】，如图 9-17 所示。

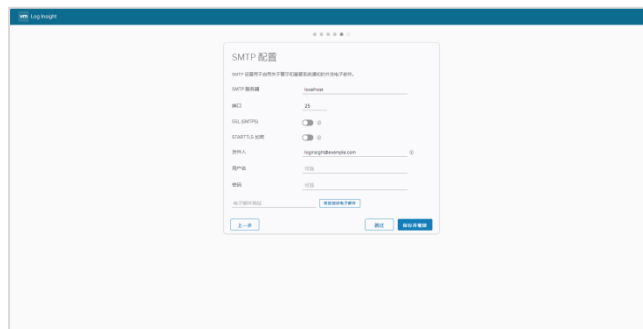


图 9-17 SMTP 配置

(8) 设置完成后，单击【完成】，完成系统初始化，如图 9-18 所示。

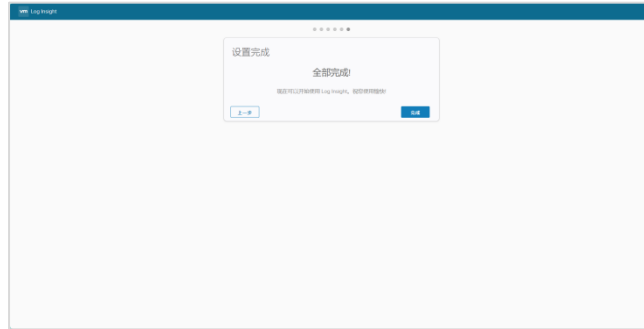


图 9-18 设置完成

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“10.10.2.120”，用户名为“administrator@labs.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 9-19、9-20、9-21 所示。



图 9-19 集成 vSphere

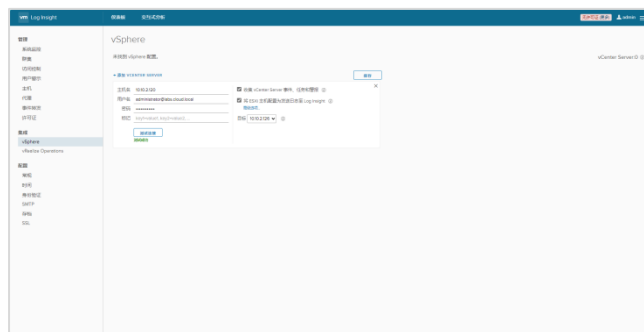


图 9-20 配置 vCenter Server

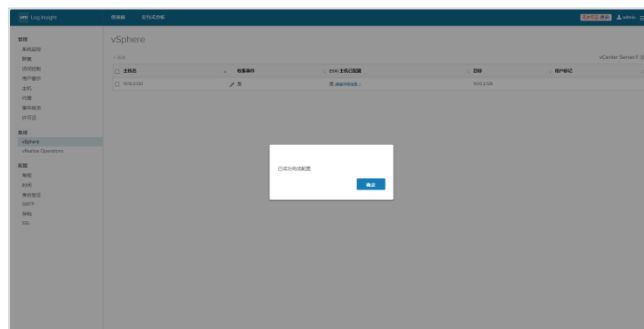


图 9-21 保存配置并配置 ESXi 主机

(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“10.10.2.125”，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 9-22、9-23 所示。

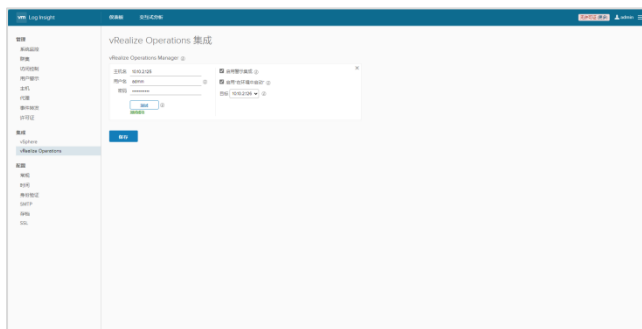


图 9-22 配置 vRealize Operations 集成

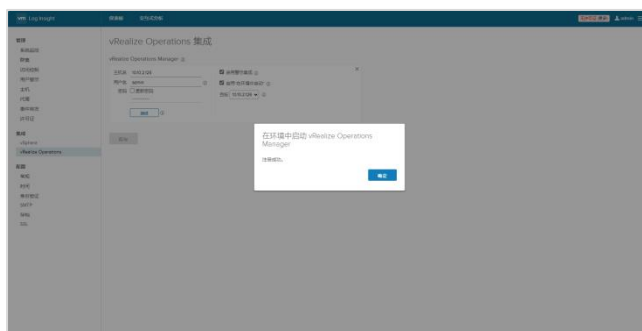


图 9-23 数据源注册成功

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 9-24 所示。

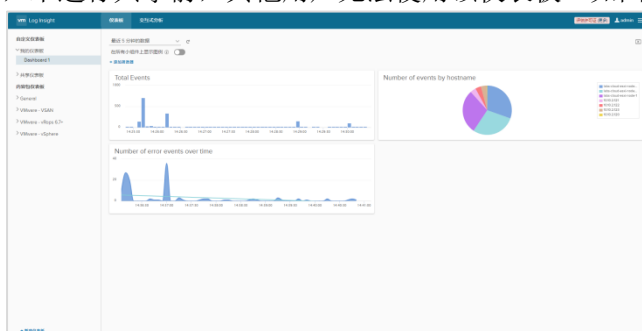


图 9-24 我的仪表板

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 9-25、9-26、9-27 所示。

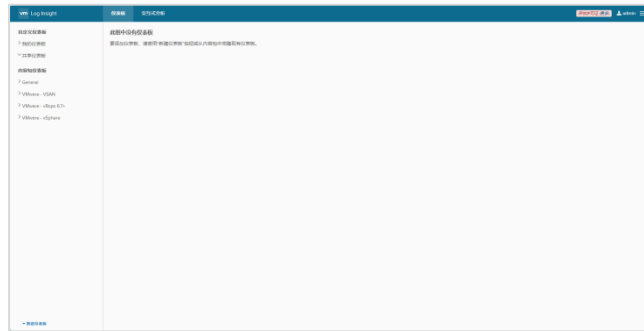


图 9-25 共享仪表盘

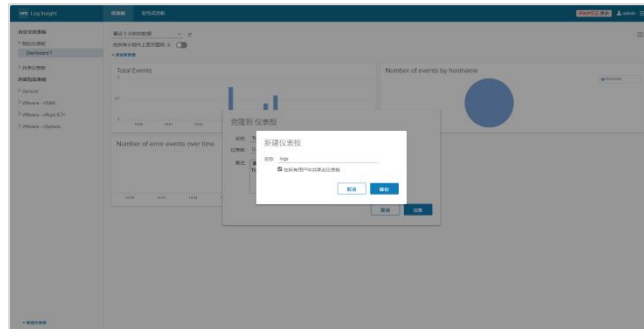


图 9-26 新建仪表盘

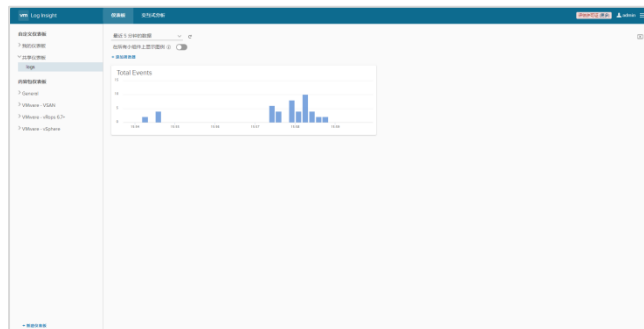


图 9-27 新建共享仪表盘

③ 内容包仪表板存放的是从内容包市场中导入的已经定义好的仪表板组件，不能进行修改，如图 9-28、9-29 所示。

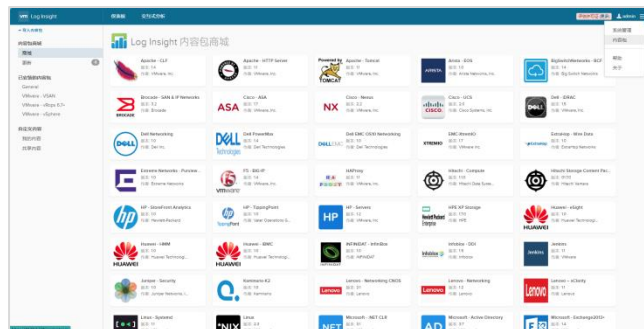


图 9-28 内容包商城

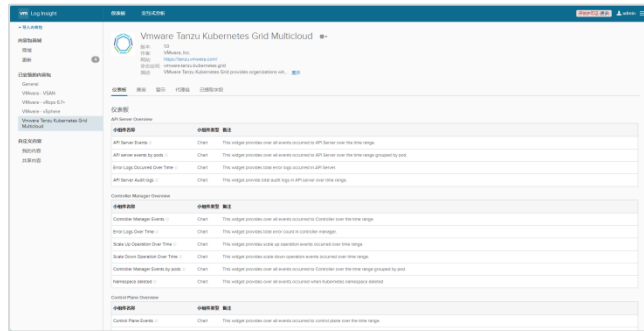


图 9-29 导入内容包

(2) 小组件的使用

① 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 2-5-7 所示。

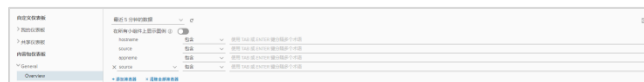


图 9-30 添加和删除筛选器

② 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，如图 9-31、9-32 所示。

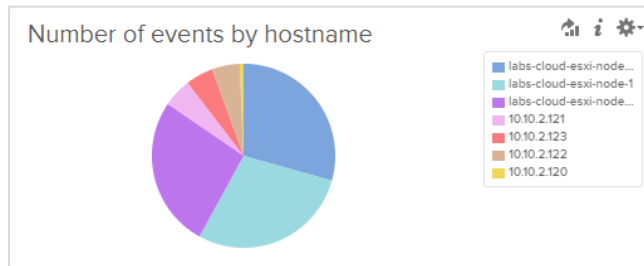


图 9-31 图表

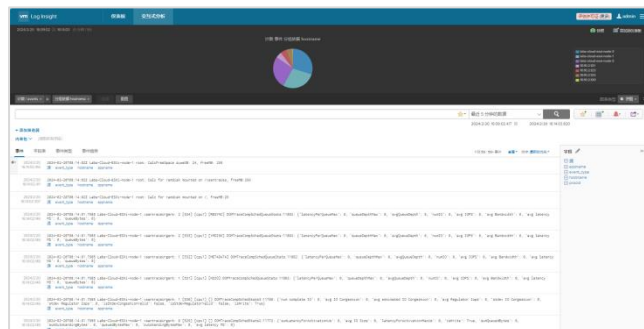


图 9-32 浏览日志

5、日志浏览与检索

(1) 按时间范围浏览和检索日志

① 以 vSphere 日志为例，在侧边栏中选择“VMware - vSphere”选项，选择一个仪表板子项，在左上角选择不同的时间范围浏览和检索其日志。如图 9-33、9-34 所示。

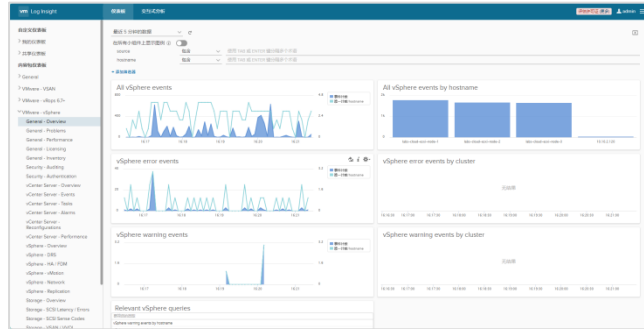


图 9-33 仪表板 1

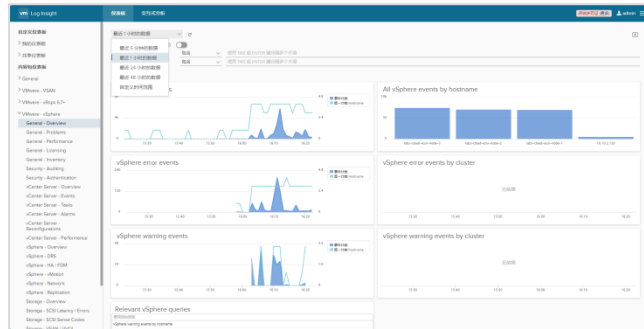


图 9-34 仪表板 2

② 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 9-35、9-36 所示。

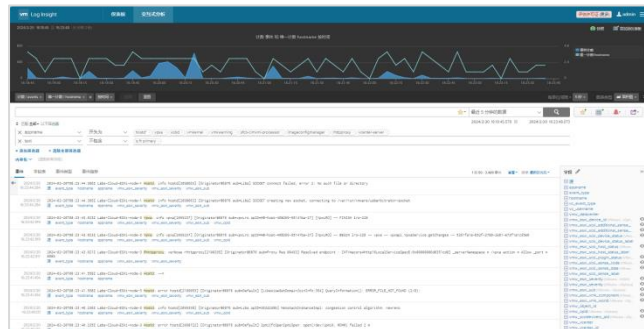


图 9-35 浏览日志 1

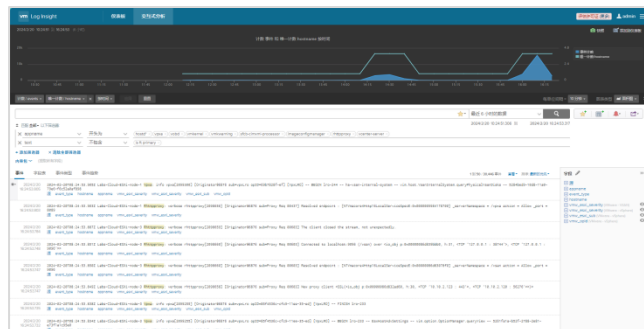


图 9-36 浏览日志 2

(2) 按字段运算检索日志

① 在交互式分析界面，单击“添加筛选器”，在搜索文本框下方的筛选器行中，使用第一个下拉菜单选择在 vRealize Log Insight 中定义的字段，此处选择“hostname”与“event_type”，在第二个下拉菜单选择“包含”与“为”，第三个下拉菜单填写“Labs-Cloud-ESXi-node-1”与“v4_921a00e9”，回车后，显示出含有相关字段的事件与图表。如图 9-37、9-38 所示。

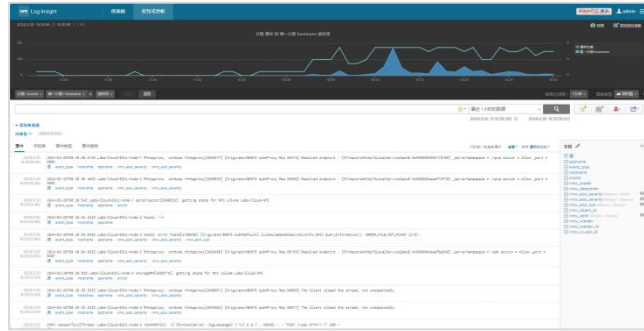


图 9-37 原日志

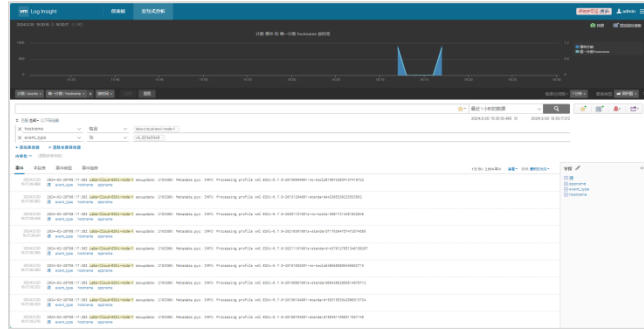


图 9-38 确定字段后的日志

② 除添加筛选器之外，可直接在图表下的搜索框中，对字段“Labs-Cloud-ESXi-node-1”进行检索，也可获取到其相关日志。如图 9-39 所示。

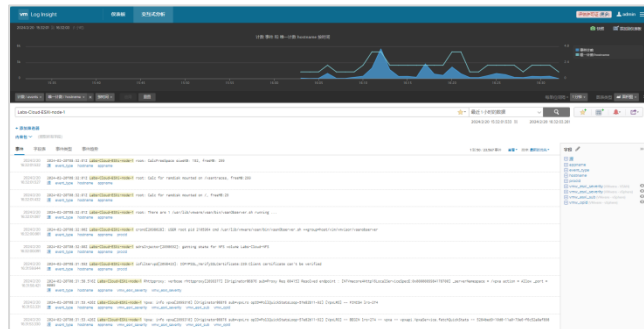


图 9-39 检索字段日志

(3) 分析日志事件类型和事件趋势

① 以“Labs-Cloud-ESXi-node-1”为例，分析其如图 9-40 之中的事件类型。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”、“Labs-Cloud-ESXi-node-1”的筛选器。如图 9-41 所示。

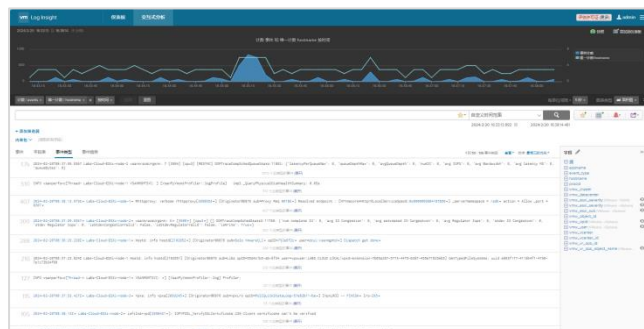


图 9-40 事件类型原图

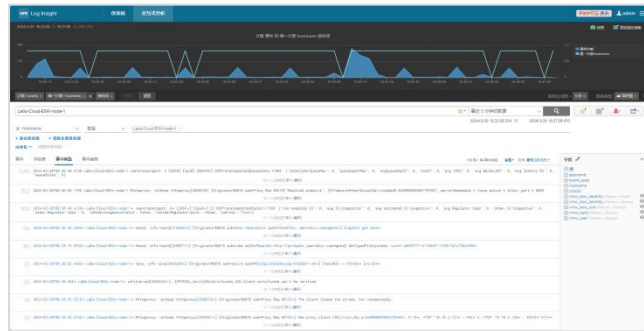


图 9-41 Labs-Cloud-ESXi-node-1 事件类型

② 分析其如图9-42之中的 Labs-Cloud-ESXi-node-1 的事件趋势。在交互式分析界面中，单击“事件趋势”子选项。然后在搜索框或者添加一个为“hostname”、“包含”、“Labs-Cloud-ESXi-node-1”的筛选器。如图 9-43 所示。

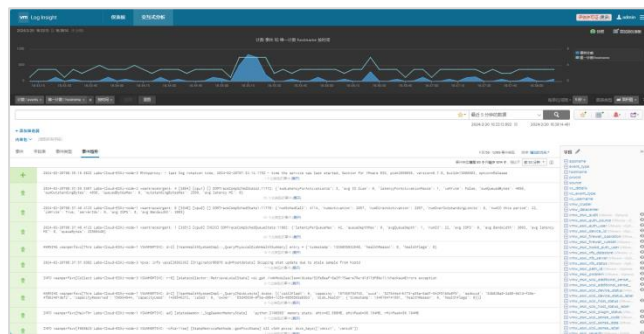


图 9-42 事件趋势

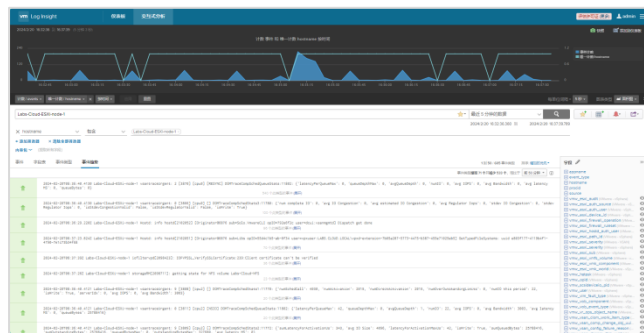


图 9-43 Labs-Cloud-ESXi-node-1 事件趋势

6、对数据中心进行日志分析

(1) 查看和管理数据中心日志

① 在侧边栏中选择“VMware - vSphere”选项，在最右侧显示的仪表板小组件中，查看和管理 vSphere 日志。在“VMware - vSphere”选项的子选项中，查看和管理 vSphere 的各项参数功能的数据和日志情况。如图 9-44、9-45 所示。

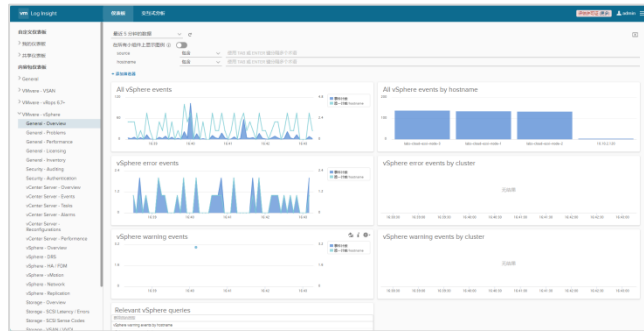


图 9-44 vSphere 仪表盘

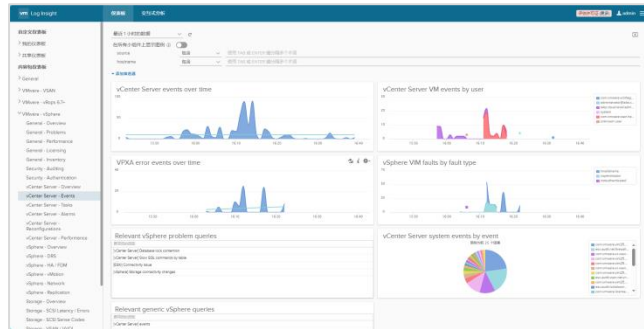


图 9-45 vCenter Server - Events 功能仪表盘

② 在左上角选择不同的时间范围，查看 vSphere 不同时间的日志情况。如图 9-46 所示。

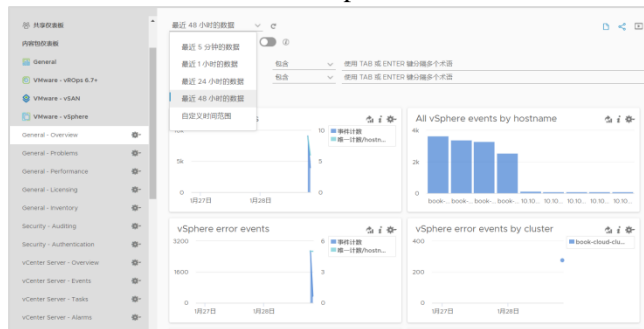


图 9-46 时段选择

(2) 向 vSphere 发送警示

① 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“VMware-vSphere 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 9-47、9-48、9-49 所示。

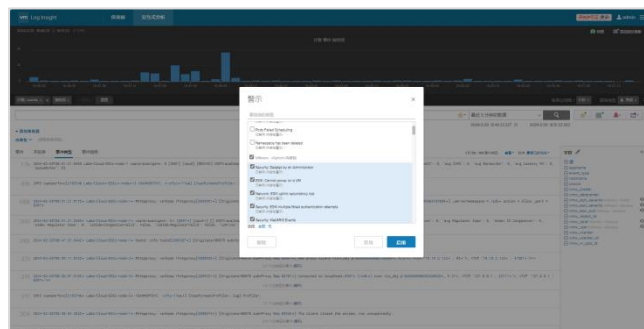


图 9-47 启用警示

点，学生现场进行演示和汇报讲解。

实验线上考：每个实验设置 5-10 个客观题。通过线上考核平台（课堂派）进行作答。

1、实验随堂查

本实验随堂查设置 3 个考核点，具体如下。

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

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。

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。

2、实验线上考

本实验线上考共 10 题，其中单选 3 题、多选 2 题、判断 3 题、填空 2 题。