

管理 vRealize Log Insight

2022 年 5 月 24 日

vRealize Log Insight 8.4

您可以从 VMware 网站下载最新的技术文档:

<https://docs.vmware.com/cn/>。

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

**威睿信息技术（中国）有
限公司**
北京办公室
北京市
朝阳区新源南路 8 号
启皓北京东塔 8 层 801
www.vmware.com/cn

上海办公室
上海市
淮海中路 333 号
瑞安大厦 804-809 室
www.vmware.com/cn

广州办公室
广州市
天河路 385 号
太古汇一座 3502 室
www.vmware.com/cn

版权所有 © 2022 VMware, Inc. 保留所有权利。 [版权和商标信息](#)

目录

管理 vRealize Log Insight 7

1 升级 vRealize Log Insight 8

vRealize Log Insight 升级途径 8

升级到最新版本的 vRealize Log Insight 8

升级到 vRealize Log Insight 8.1 9

升级到 vRealize Log Insight 8.0 10

2 管理 vRealize Log Insight 用户帐户 11

用户管理概览 11

基于角色的访问控制 12

使用筛选功能管理用户帐户 12

创建用户帐户 13

解除锁定用户帐户 14

为 vRealize Log Insight 配置通过 VMware Identity Manager 访问 Active Directory 组 15

将 Active Directory 组导入到 vRealize Log Insight 16

定义数据集 17

创建和修改角色 19

删除用户帐户或组 19

3 配置身份验证 21

启用通过 VMware Identity Manager 进行用户身份验证 21

启用通过 Active Directory 的用户身份验证 23

配置用于 Active Directory 的协议 24

4 配置 vRealize Log Insight 26

vRealize Log Insight 配置限制 27

添加日志筛选器配置 28

添加日志屏蔽配置 29

配置虚拟设备设置 30

配置 vRealize Log Insight 虚拟设备的根 SSH 密码 30

更改 vRealize Log Insight 虚拟设备的网络设置 31

增加 vRealize Log Insight 虚拟设备的存储容量 31

向 vRealize Log Insight 虚拟设备添加内存和 CPU 32

向 vRealize Log Insight 分配许可证 33

日志存储策略 34

管理系统通知 34

- 系统通知 34
 - 为 vRealize Log Insight 系统通知配置目标 38
- 添加 vRealize Log Insight 事件转发目标 40
 - 在交互式分析中使用日志管理筛选器 43
- 同步 vRealize Log Insight 虚拟设备上的时间 43
- 为 vRealize Log Insight 配置 SMTP 服务器 44
- 配置 Webhook 45
- 安装自定义 SSL 证书 46
 - 生成自签名证书 47
 - 生成证书签名请求 48
 - 请求来自证书颁发机构的签名 49
 - 连接证书文件 49
 - 上载已签名证书 50
 - 在 vRealize Log Insight 服务器和 Log Insight Agents 之间配置 SSL 连接 51
- 查看和移除 SSL 证书 54
- 更改 vRealize Log Insight Web 会话的默认超时期限。 54
- 保留和存档 55
 - 配置数据分区 55
 - 数据存档 56
 - vRealize Log Insight 存档文件的格式 57
 - 将 vRealize Log Insight 存档导入到 vRealize Log Insight 中 57
 - 将 Log Insight 存档导出为原始文本文件或 JSON 58
- 重新启动 vRealize Log Insight 服务 59
- 关闭 vRealize Log Insight 虚拟设备的电源 60
- 下载 vRealize Log Insight 支持包 60
- 加入或退出 VMware 客户体验改善计划 61
- 为 vRealize Log Insight 配置 STIG 合规性 62
- 为 vRealize Log Insight 激活 FIPS 63

5 管理 vRealize Log Insight 群集 64

- 向 vRealize Log Insight 集群添加工作线程节点 64
 - 部署 vRealize Log Insight 虚拟设备 64
 - 加入现有部署 67
- 从 vRealize Log Insight 群集中移除工作线程节点 68
- 使用集成负载均衡器 68
 - 启用集成负载均衡器 69
- 查询生产中群集检查的结果 70

6 配置、监控和更新 vRealize Log Insight 代理 72

- 集中式代理配置和代理组 72
 - 代理组配置合并 73

- 创建代理组 73
- 编辑代理组 74
- 将内容包代理组作为代理组添加 75
- 删除代理组 75
- 监控 vRealize Log Insight 代理的状态 76
- 从服务器中启用代理自动更新 77

7 监控 vRealize Log Insight 78

- 检查 vRealize Log Insight 虚拟设备的运行状况 78
- 监控发送日志事件的主机 79
- 配置报告非活动主机的系统通知 79

8 将 vRealize Log Insight 与 VMware 产品集成 81

- 将 vRealize Log Insight 连接到 vSphere 环境 82
 - vRealize Log Insight 用作 Syslog 服务器 83
 - 配置 ESXi 主机以将日志事件转发到 vRealize Log Insight 83
 - 修改 ESXi 主机配置以将日志事件转发到 vRealize Log Insight 85
 - vRealize Operations Manager 中的 vRealize Log Insight 通知事件 86
- 配置 vRealize Log Insight 以从 vCenter Server 实例中提取事件、任务和警报 87
- 将 vRealize Operations Manager 与 vRealize Log Insight 一起使用 87
 - 与 vRealize Operations Manager 集成的要求 87
 - 将 vRealize Log Insight 配置为向 vRealize Operations Manager 发送通知和衡量指标 89
 - 在 vRealize Operations Manager 中为 vRealize Log Insight 启用“在环境中启动” 91
 - 在 vRealize Operations Manager 中为 vRealize Log Insight 禁用“在环境中启动” 94
- 添加 DNS 搜索路径和域 95
- 移除 vRealize Log Insight 适配器 96
- 适用于 vRealize Log Insight 的 vRealize Operations Manager Content Pack 97

9 vRealize Log Insight 的安全注意事项 98

- 端口和外部接口 98
- vRealize Log Insight 配置文件 99
- vRealize Log Insight 公用密钥、证书和密钥库 100
- vRealize Log Insight 许可证和 EULA 文件 100
- vRealize Log Insight 日志文件 101
 - 为用户审核日志消息启用调试级别 103
 - vRealize Log Insight 中的审核日志 104
- vRealize Log Insight 用户帐户 104
- vRealize Log Insight 防火墙建议 105
- 安全更新和修补程序 106

10 备份、还原和灾难恢复 107

备份、还原和灾难恢复概览	107
使用静态 IP 地址和 FQDN	108
规划与准备	108
备份节点和集群	109
备份 Linux 或 Windows 代理	110
还原节点和集群	111
还原后更改配置	112
还原到相同主机	112
还原到其他主机	112
验证还原	115
灾难恢复	115

11 vRealize Log Insight 故障排除 116

无法在 Internet Explorer 上登录到 vRealize Log Insight	116
vRealize Log Insight 磁盘空间不足	117
存档数据的导入可能失败	117
使用虚拟设备控制台创建 vRealize Log Insight 的支持包	118
重置管理员用户密码	118
重置 Root 用户密码	119
无法向 vRealize Operations Manager 提交警示	120
使用 Active Directory 凭据无法登录	121
SMTP 无法在启用 STARTTLS 选项的情况下使用	121
由于无法验证 .pak 文件的签名，升级失败	122
升级失败并显示内部服务器错误	123
与 VMware 产品集成后第一条日志消息中缺少 vmw_object_id 字段	123

管理 vRealize Log Insight

《管理 vRealize Log Insight》提供了有关管理 VMware® vRealize™ Log Insight™ 的信息，包括如何管理用户帐户以及如何配置与其他 VMware 产品的集成。还包括有关管理产品安全和升级部署的信息。

本信息的目标读者为熟悉虚拟机技术和数据中心操作且具有丰富经验的 Windows 或 Linux 系统管理员。

升级 vRealize Log Insight

1

您可以将 vRealize Log Insight 从版本 8.3 或 8.2 升级到 8.4、从 8.2 升级到 8.3、从 8.1 升级到 8.2，以及从 4.8 或 8.0 升级到 8.1。要升级到 vRealize Log Insight 8.0 或更早版本，必须遵循增量升级途径。升级包括自动升级集群中的节点。

要下载 vRealize Log Insight 的 PAK 文件，请转到[下载 VMware vRealize Log Insight](#) 页面。

本章讨论了以下主题：

- [vRealize Log Insight 升级途径](#)
- [升级到最新版本的 vRealize Log Insight](#)
- [升级到 vRealize Log Insight 8.1](#)
- [升级到 vRealize Log Insight 8.0](#)

vRealize Log Insight 升级途径

要采用的升级途径取决于安装的 vRealize Log Insight 版本以及要升级到的版本。

您可以将 vRealize Log Insight 从版本 8.3 或 8.2 升级到 8.4、从 8.2 升级到 8.3、从 8.1 升级到 8.2，以及从 4.8 或 8.0 升级到 8.1。要升级到 vRealize Log Insight 8.0 或更早版本，必须执行增量升级。例如，要从版本 4.5 升级到 4.7，您需要对 4.5 应用 4.6 升级，然后再从 4.6 升级到 4.7。您必须升级到每个中间版本。

您还可以在 [VMware 产品互操作性列表](#) 站点上查看支持的升级途径。

升级到最新版本的 vRealize Log Insight

您可以将集群从 vRealize Log Insight 8.3 或 8.2 升级到 8.4、从 8.2 升级到 8.3、从 8.1 升级到 8.2，以及从 4.8 或 8.0 升级到 8.1。要将集群升级到 vRealize Log Insight 8.0 或更早版本，必须遵循增量途径。例如，要从版本 3.6 升级到 4.3，需先将 3.6 升级到 4.0，然后再从 4.0 升级到 4.3。

必须从主节点的 FQDN 升级 vRealize Log Insight。不支持使用集成负载均衡器 IP 地址进行升级。

在升级期间，先升级主节点，然后重新启动。将按顺序升级每个集群节点。您可以在[管理 > 集群](#)页上查看滚动升级的状态。如果配置了集成的负载均衡器，则会在集群节点之间迁移其 IP，因此，集群服务（包括 UI、API 和入站事件载入）将在滚动升级期间保持可用。更具体的详细信息会写入每个单独节点上的 `/storage/core/loginsight/var/upgrade.log` 文件中。在成功完成升级后，将发送系统通知。

如果在升级过程中遇到影响一个或多个节点的问题，则会将整个集群回滚到原始的正常工作版本。由于在开始升级后执行的配置更改可能不一致或无效，配置将恢复到在升级之前捕获的已知正常状态。不会丢失载入的任何事件。进度信息会写入每个单独节点上的 `/storage/core/loginsight/var/rollback.log` 文件中。在回滚完成后，将发送系统通知。在调查并修复问题后，您可以再次尝试进行升级。

在升级后，所有节点将置于已连接状态并恢复联机，即使它们在升级之前处于维护模式。

前提条件

- 确认您将正确的升级应用于 vRealize Log Insight 版本。有关支持的升级途径的详细信息，请参见 [vRealize Log Insight 升级途径](#)。
- 创建 vRealize Log Insight 虚拟设备的快照或备份副本。
- 为要升级到的版本获取一个 vRealize Log Insight 升级包 `.pak` 文件副本。
- 验证是否已以具有**编辑管理员**权限的用户身份登录到 vRealize Log Insight Web 用户界面。URL 格式为 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。
- 记下您进行升级并处于维护模式的任何节点。升级完成后，您必须将其从已连接状态恢复为维护模式。

步骤

- 1 导航到**管理**选项卡。
- 2 在“管理”下，单击**集群**。
- 3 单击**从 PAK 升级**，以上载 `.pak` 文件。
- 4 接受新 EULA 完成升级过程。

后续步骤

在主节点升级过程完成后，您可以查看其余升级过程，该过程是自动执行的。

查看发送给管理员的电子邮件，以确认升级成功完成。

在升级后，所有节点将恢复联机状态，即使它们在升级之前处于维护模式。根据需要，将这些节点恢复为维护模式。

升级到 vRealize Log Insight 8.1

您可以从 vRealize Log Insight 8.0 升级到 8.1，这两个版本均位于 Photon 操作系统上。您还可以从 SLES 操作系统上的 vRealize Log Insight 4.8 直接升级到 Photon 操作系统上的 vRealize Log Insight 8.1。

从 vRealize Log Insight 8.0 升级到 8.1

从 vRealize Log Insight 8.0 升级到 8.1 不会更改 vRealize Log Insight 虚拟设备的虚拟机架构。唯一的更改是在当前引导的根分区中（例如，从 SDA4 更改为 SDA3），这对用户体验没有任何影响。

如果升级到 vRealize Log Insight 8.1 失败，则不会进行自动回滚。但是，您可以手动进行回滚以恢复到之前的版本。有关详细信息，请参见 <https://kb.vmware.com/s/article/75150>。用户界面或 REST API 中没有变化。从命令行连接到 vRealize Log Insight 8.1 虚拟机并在其上工作时，您会看到基于 `systemd` 的信息，因为 Photon 基于 `systemd`。

从 vRealize Log Insight 4.8 升级到 8.1

从 vRealize Log Insight 4.8 升级到 8.1 与从 4.8 升级到 8.0 相似。有关详细信息，请参见 [升级到 vRealize Log Insight 8.0](#)。

有关升级到 vRealize Log Insight 8.1 的其他信息，请参见 [升级说明](#)。

有关升级过程的信息，请参见 [升级到最新版本的 vRealize Log Insight](#)。

升级到 vRealize Log Insight 8.0

您可以从 SLES 操作系统上的 vRealize Log Insight 4.8 升级到 Photon 操作系统上的 vRealize Log Insight 8.0。

从基于 SLES 的 vRealize Log Insight 4.8 升级到基于 Photon 的 vRealize Log Insight 8.0 与以前的升级有所不同，这是因为底层操作系统发生了变化。此升级将更改 vRealize Log Insight 虚拟设备中每个虚拟机的架构。

例如，考虑一个具有磁盘 SDA 的虚拟机，该虚拟机具有三个分区，分别用于引导 (SDA1)、交换 (SDA2) 和根 (SDA3)。分区 SDA3 的大小约为 16 GB，其中包含有关 SLES 的信息。从基于 SLES 的 vRealize Log Insight 4.8 升级到基于 Photon 的 vRealize Log Insight 8.0 时，将在 SDA3 中创建另一个分区，并将其平均分成两部分，每部分大小约为 8 GB：一部分用于 SLES (SDA3)，另一部分用于 Photon (SDA4)。SDA4 成为活动分区。SDA3 保持不活动状态，但包含用于 SLES 的有效 vRealize Log Insight 信息。在引导虚拟机时，您可以通过手动选择来引导 SDA3。

注 在从基于 SLES 的 vRealize Log Insight 4.8 升级到基于 Photon 的 vRealize Log Insight 8.0 之前，请确保根分区中具有足够的空间来进行升级。如果根分区较小，例如 8 GB，请将磁盘大小增加到 20 GB，以便根分区大小能够增加到 16 GB。对于根分区空间较小的每个节点，必须增加其磁盘大小。有关增加根分区大小的信息，请参见 <https://kb.vmware.com/s/article/76304>。

升级到基于 Photon 的 vRealize Log Insight 8.0 后：

- 用户界面或 REST API 中没有变化。
- 从命令行连接到 vRealize Log Insight 8.0 虚拟机并在其上工作时，您会看到基于 `systemd` 的信息，因为 SLES 基于 `initd`，而 Photon 基于 `systemd`。

有关升级到 vRealize Log Insight 8.0 的其他信息，请参见 [升级说明](#)。

有关升级过程的信息，请参见 [升级到最新版本的 vRealize Log Insight](#)。

管理 vRealize Log Insight 用户帐户

2

管理员可创建用户帐户和角色，以便提供访问 vRealize Log Insight Web 界面的权限。

仅拥有编辑管理员权限的用户才可以创建和编辑用户帐户。但是，没有编辑管理员权限的用户可以更改自己的电子邮件和帐户密码。

本章讨论了以下主题：

- 用户管理概览
- 基于角色的访问控制
- 使用筛选功能管理用户帐户
- 创建用户帐户
- 解除锁定用户帐户
- 为 vRealize Log Insight 配置通过 VMware Identity Manager 访问 Active Directory 组
- 将 Active Directory 组导入到 vRealize Log Insight
- 定义数据集
- 创建和修改角色
- 删除用户帐户或组

用户管理概览

系统管理员使用用户登录名、基于角色的访问控制、权限和数据集的组合来管理 vRealize Log Insight 用户。通过基于角色的访问控制，管理员可以管理用户以及他们能够执行的任务。

角色是执行特定任务所需的权限集。系统管理员在定义安全策略的过程中定义角色，并向用户授予角色。要更改与特定角色关联的权限和任务，系统管理员需要更新角色设置。更新的设置对与此角色关联的所有用户都生效。

- 要允许用户执行某项任务，系统管理员需授予该用户相应角色。
- 要阻止用户执行某项任务，系统管理员需撤销该用户的相应角色。

基于用户登录帐户管理每位用户的访问、角色和权限。可向每位用户授予多种角色和权限。

用户无法查看或访问特定对象，或无法执行特定操作，这是因为他们没有被授予相应权限。

基于角色的访问控制

通过基于角色的访问控制，系统管理员可以限制特定用户对日志的访问，并控制这些用户可以在登录后执行的任务。系统管理员可以将权限和角色与用户登录帐户相关联或从中撤销权限和角色。用户可以查看他们有权访问的所有仪表板，但仪表板和交互式分析中的数据将基于用户角色有权访问的数据集进行筛选。

用户

系统管理员可以通过向用户登录帐户授予权限和角色或从中撤销权限和角色，控制每个用户的访问和操作。

权限

权限控制在 vRealize Log Insight 中允许的操作。权限适用于 vRealize Log Insight 中的特定管理或用户任务。例如，可以授予**查看管理员**权限，以允许用户查看 vRealize Log Insight 管理设置。

数据集

数据集包含一组筛选器。可以使用数据集，通过将数据集与角色相关联，为用户提供对特定内容的访问。

角色

角色是可与用户关联的权限和数据集的集合。角色提供用于打包执行任务所需的所有权限的一种简便方法。可以为一个用户分配多个角色。

使用筛选功能管理用户帐户

您可以指定搜索筛选器以搜索一个或一组用户。

筛选是从**访问控制**页上的**用户和组**选项卡中完成的。要转到该页面，请在**管理**选项卡上，单击**管理**菜单下的**访问控制**，然后选择**用户和组**选项卡。

搜索文本框位于页面顶部附近，并包含按用户名筛选短语。

在您键入时，搜索功能将筛选结果以返回包含输入模式的用户名。例如，如果您具有 John_Smith、John_Doe 和 Helen_Jonson 用户名，在键入字母 **J** 时，搜索将返回所有包含该字母的用户名；对于此示例，将返回 John_Smith、John_Doe 和 Helen_Jonson。在继续键入字母时，将缩小搜索结果范围，以便与精确模式相匹配。对于此示例，在键入 **John_** 时，搜索将返回 John_Smith 和 John_Doe。

您可以按字段对搜索结果进行排序：域、身份验证、角色、电子邮件或 UPN。此外，您可以对搜索结果执行批量操作，例如删除多个用户。

创建用户帐户

被赋予超级管理员角色的用户可创建用户帐户来提供对 vRealize Log Insight Web 用户界面的访问权限。

前提条件

验证是否已具有**编辑管理员**权限的用户身份登录到 vRealize Log Insight Web 用户界面。URL 格式为 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

如果要创建使用 VMware Identity Manager 或 Active Directory 的用户帐户，请确认您已配置为支持这些身份验证类型。请参见[启用通过 VMware Identity Manager 进行用户身份验证](#)和[启用通过 Active Directory 的用户身份验证](#)。

步骤

- 1 导航到**管理**选项卡。
- 2 在“管理”下，单击**访问控制**。
- 3 单击**用户和组**。
- 4 单击**新建用户**。
- 5 执行以下操作之一：
 - 如果使用默认的内置身份验证，请输入用户名和电子邮件地址。
 - 如果使用 Active Directory 或 VMware Identity Manager 身份验证，请为用户帐户输入用户所属的域、用户名，以及电子邮件地址（可选）。
- 6 从右侧的**角色**列表中，选择一个或多个预定义或自定义的用户角色。

选项	描述
用户	用户可以访问 vRealize Log Insight 的完整功能。您可以查看日志事件，运行查询以搜索和筛选日志，将内容包导入到自己的用户空间中，添加警示查询，以及管理自己的用户帐户以更改密码或电子邮件地址。用户没有访问管理选项的权限，无法与其他用户共享内容，无法修改其他用户的帐户，也无法从商城安装内容包。但是，您可以将内容包导入到只有您自己可以看到的用户空间中。
仪表板用户	仪表板用户只能使用 vRealize Log Insight 的“仪表板”页面。
仅查看管理员	“查看管理员”用户可以查看管理员信息，具有完全用户访问权限，并且可以编辑共享内容。
超级管理员	“超级管理员”用户可以访问 vRealize Log Insight 的完整功能，可以管理 vRealize Log Insight，还可以管理所有其他用户的帐户。

7 单击保存。

- 对于内置身份验证，将在本地保存该信息。将向用户的电子邮件地址发送一封电子邮件，其中包含用于完成注册的链接。用户可以单击该链接，然后输入其帐户的密码。在用户完成注册帐户前，帐户状态为“挂起”。完成注册后，帐户状态为“活动”。

注 用户必须在收到注册电子邮件后的 24 小时内注册他们的帐户。如果用户没有这样做，其帐户将一直保持“挂起”状态，并且必须请求超级管理员用户解除锁定他们的帐户。有关详细信息，请参见[解除锁定用户帐户](#)。

- 通过 VMware Identity Manager 进行身份验证时，vRealize Log Insight 将验证用户的域是否已与某个组关联。如果该域不属于任一组，vRealize Log Insight 将验证该域是否已同与某个组关联的域建立了信任关系。如果已建立跨域信任关系，则用户可以登录到 vRealize Log Insight，且相应的用户帐户会被添加到[访问控制 > 用户和组](#)中的用户表。

解除锁定用户帐户

如果用户帐户由于未能在 24 小时内完成注册而处于挂起状态，或者该帐户处于锁定状态，超级管理员用户可以解除锁定该帐户。

超级管理员用户帐户永远不会被锁定。在以下任一情况下，其他用户帐户将被锁定：

- 用户在 15 分钟内连续三次输入错误的密码。
- 用户已有 35 天未登录到 vRealize Log Insight。只有在启用了密码策略限制时，此锁定条件才有效。
- 用户已有 60 天未更改密码。只有在启用了密码策略限制时，此锁定条件才有效。

有关启用密码策略限制的信息，请参见[vRealize Log Insight 配置 STIG 合规性](#)。

注 此过程将仅解除锁定使用默认的内置身份验证的帐户，而不会解除锁定使用 VMware Identity Manager 或 Active Directory 身份验证的帐户。

前提条件

验证是否已具有[编辑管理员](#)权限的用户身份登录到 vRealize Log Insight Web 用户界面。URL 格式为 <https://log-insight-host>，其中 *log-insight-host* 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

- 1 导航到[管理](#)选项卡。
- 2 在“管理”下，单击[访问控制](#)。
- 3 单击[用户和组](#)。
- 4 （可选）对于锁定的用户帐户，指向[状态](#)列中红色的锁图标，可了解该帐户被锁定的原因。
- 5 针对帐户的用户名单击铅笔图标。
- 6 如果尚未选中[重置密码](#)复选框，请将其选中。

7 单击**保存**。

结果

将向用户的电子邮件地址发送一封电子邮件，其中包含用于重置密码的链接。用户可以单击该链接，然后为其帐户输入新密码。

注 用户必须在收到电子邮件后的 24 小时内解除锁定他们的帐户。如果用户没有这样做，则必须请求超级管理员用户重新解除锁定他们的帐户。

为 vRealize Log Insight 配置通过 VMware Identity Manager 访问 Active Directory 组

您可以通过 VMware Identity Manager 单点登录身份验证在 vRealize Log Insight 中使用 Active Directory 组。必须为您的站点配置启用了 Active Directory 支持的 VMware Identity Manager 身份验证，并且必须启用了服务器同步。

您还必须将组信息导入到 vRealize Log Insight 中。

除了分配给单个用户的角色以外，VMware Identity Manager 用户还会继承分配给所属的任何组的角色。例如，管理员可以为组 A 分配**查看管理员**角色，并为某个用户分配**用户**角色。此外，也可以将该用户分配到组 A。当该用户登录时，用户将继承组角色，因而将同时拥有**查看管理员**和**用户**角色特权。

该组不是 VMware Identity Manager 本地组，而是与 VMware Identity Manager 同步的 Active Directory 组。

前提条件

- 确认您配置了 UPN 属性 (userPrincipalName)。可以通过 VMware Identity Manager 管理员界面的**身份和访问管理 > 用户属性**配置该属性。
- 验证是否已以具有**编辑管理员**权限的用户身份登录到 vRealize Log Insight Web 用户界面。URL 格式为 https://log-insight-host，其中，log-insight-host 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。
- 确认在 vRealize Log Insight 中配置了 VMware Identity Manager 支持。请参见[启用通过 VMware Identity Manager 进行用户身份验证](#)

步骤

- 1 导航到**管理**选项卡。
- 2 在“管理”下，单击**访问控制**。
- 3 单击**用户和组**。
- 4 滚动到目录组表，然后单击**新建组**。
- 5 从**类型**下拉菜单中选择 **VMware Identity Manager**。

将在**域**文本框中显示在配置 VMware Identity Manager 支持时指定的默认域名。

- 6 将域名更改为组的 Active Directory 名称。

- 7 输入要添加的组的名称。
- 8 从右侧的**角色**列表中，选择一个或多个预定义或自定义的用户角色。

选项	描述
用户	用户可以访问 vRealize Log Insight 的完整功能。您可以查看日志事件，运行查询以搜索和筛选日志，将内容包导入到自己的用户空间中，添加警示查询，以及管理自己的用户帐户以更改密码或电子邮件地址。用户没有访问管理选项的权限，无法与其他用户共享内容，无法修改其他用户的帐户，也无法从商城安装内容包。但是，您可以将内容包导入到只有您自己可以看到的用户空间中。
仪表板用户	仪表板用户只能使用 vRealize Log Insight 的“仪表板”页面。
仅查看管理员	“查看管理员”用户可以查看管理员信息，具有完全用户访问权限，并且可以编辑共享内容。
超级管理员	“超级管理员”用户可以访问 vRealize Log Insight 的完整功能，可以管理 vRealize Log Insight，还可以管理所有其他用户的帐户。

9 单击保存。

在进行身份验证时，vRealize Log Insight 将验证用户的域是否已与某个组关联。如果该域不属于任一组，vRealize Log Insight 将验证该域是否已同与某个组关联的域建立了信任关系。如果已建立跨域信任关系，则用户可以登录到 vRealize Log Insight，且相应的用户帐户会被添加到**访问控制 > 用户和组**中的用户表。

结果

属于您添加的组的用户可以使用其 VMware Identity Manager 帐户登录到 vRealize Log Insight，并拥有所属的组的权限级别。

将 Active Directory 组导入到 vRealize Log Insight

可以通过添加域组而不是单个域用户，允许用户登录 vRealize Log Insight。

如果在 vRealize Log Insight 中启用 AD 支持，请配置域名，并提供属于该域的一个绑定用户。vRealize Log Insight 使用绑定用户验证与 AD 域的连接，并验证是否存在 AD 用户和组。

您添加到 vRealize Log Insight 的 Active Director 组必须属于绑定用户的域，或者属于绑定用户的域信任的域。

Active Directory 用户除继承分配给单个用户的角色外，还会继承分配给其所属组的角色。例如，管理员可以将 GroupA 分配给角色**查看管理员**，并将用户 Bob 分配给角色**用户**。还可以将 Bob 分配给 GroupA。Bob 登录后，将会继承组角色并拥有**查看管理员**和**用户**两种角色的特权。

前提条件

- 验证是否已以具有**编辑管理员**权限的用户身份登录到 vRealize Log Insight Web 用户界面。URL 格式为 `https://log-insight-host`，其中，log-insight-host 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。
- 验证是否已配置 AD 支持。请参见[启用通过 Active Directory 的用户身份验证](#)

步骤

- 1 导航到**管理**选项卡。
- 2 在“管理”下，单击**访问控制**。
- 3 单击**用户和组**。
- 4 在“目录组”下面，单击**新建组**。
- 5 在**类型**下拉菜单中，单击“Active Directory”。

将在**域**文本框中显示在配置 Active Directory 支持时指定的默认域名。如果要添加默认域中的组，请勿修改域名。

- 6 （可选）如果要添加信任默认域的域中的组，请在**域**文本框中键入该信任域的名称。
- 7 输入要添加的组的名称。
- 8 从右侧的**角色**列表中，选择一个或多个预定义或自定义的用户角色。

选项	描述
用户	用户可以访问 vRealize Log Insight 的完整功能。您可以查看日志事件，运行查询以搜索和筛选日志，将内容包导入到自己的用户空间中，添加警示查询，以及管理自己的用户帐户以更改密码或电子邮件地址。用户没有访问管理选项的权限，无法与其他用户共享内容，无法修改其他用户的帐户，也无法从商城安装内容包。但是，您可以将内容包导入到只有您自己可以看到的用户空间中。
仪表板用户	仪表板用户只能使用 vRealize Log Insight 的“仪表板”页面。
仅查看管理员	“查看管理员”用户可以查看管理员信息，具有完全用户访问权限，并且可以编辑共享内容。
超级管理员	“超级管理员”用户可以访问 vRealize Log Insight 的完整功能，可以管理 vRealize Log Insight，还可以管理所有其他用户的帐户。

- 9 单击**保存**。

vRealize Log Insight 将验证指定域或信任域中是否存在该 AD 组。如果找不到组，将显示一个对话框，通知您 vRealize Log Insight 无法验证该组。可以保存组而不验证，或取消并更改组名称。

结果

属于您添加的 Active Directory 组的用户可以使用其域帐户登录到 vRealize Log Insight，并拥有所属的组的权限级别。

定义数据集

可以定义数据集，为用户提供特定内容的访问权限。

数据集不支持基于文本的限制。

前提条件

验证是否已具有**编辑管理员**权限的用户身份登录到 vRealize Log Insight Web 用户界面。URL 格式为 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

- 1 导航到**管理**选项卡。
- 2 在“管理”下，单击**访问控制**。
- 3 单击**数据集**。
- 4 单击**新建数据集**。
- 5 单击**添加筛选器**。
- 6 使用第一个下拉菜单选择在 vRealize Log Insight 中定义的字段以用于筛选。

例如，**hostname**。

该列表仅包含静态字段，并排除提取的字段、用户共享的字段、文本字段以及通过 `event_type` 筛选器创建的字段。

注 数字字段包含字符串字段所不包含的其他运算符 `=`、`>`、`<`、`>=` 和 `<=`。这些运算符执行数字比较。与使用字符串运算符相比，使用它们可生成不同的结果。例如，`response_time=02` 筛选器与包含值为 2 的 `response_time` 字段的事件匹配。`response_timecontains02` 筛选器没有相同的匹配项。

- 7 在第二个下拉菜单中选择要应用于在第一个下拉菜单中选择的字段的操作。
例如，选择 **contains**。**contains** 筛选器与完整令牌匹配：搜索字符串 `err` 不会将 `error` 作为匹配项返回。
- 8 在筛选器下拉菜单右侧的筛选器框中，输入要用作筛选器的值。
可以使用多个值。这些值之间的运算符是 **OR**。

注 如果在第二个下拉菜单中选择 **exists** 运算符，则此框不可用。

- 9 （可选）要添加更多筛选器，请单击**添加筛选器**。
- 10 （可选）要验证筛选器行为是否符合您的要求，请单击**在交互式分析中运行**，这会打开一个交互式分析窗口，其中将显示与您的筛选器匹配的数据。
- 11 单击**保存**。

后续步骤

将数据集与用户角色相关联。请参见**创建和修改角色**。



创建和修改角色

您可以创建自定义角色或修改预定义角色，以允许用户执行特定的任务和访问特定的内容。

前提条件

验证是否已以具有**编辑管理员**权限的用户身份登录到 vRealize Log Insight Web 用户界面。URL 格式为 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

- 1 导航到**管理**选项卡。
- 2 在“管理”下，单击**访问控制**。
- 3 单击**角色**。
- 4 单击**新建角色**或   以编辑现有角色。
在编辑超级管理员和用户角色之前，必须先克隆这些角色。
- 5 修改**名称**和**描述**文本框。
- 6 从“权限”列表选择一个或多个权限。

选项	描述
编辑管理员	可以编辑管理员信息和设置，如集群管理、访问控制、集成和内容包
查看管理员	可以查看管理员信息和设置，但不能进行任何更新
编辑共享	可以编辑共享内容、创建新警示以及编辑现有警示
分析	可以使用交互式分析、创建已提取字段、保存常用查询以及创建仪表板
仪表板	可以查看内容包和共享仪表板

- 7 （可选）从右侧的**数据集**列表中，选择要与用户角色相关联的数据集。
- 8 单击**保存**。

删除用户帐户或组

可以从 vRealize Log Insight 管理用户界面中删除用户帐户或组。

用户帐户和组分别列在“访问控制”页面上的不同表格中。您可以使用搜索筛选器来查找特定的用户帐户。删除组时，属于该组的所有用户都将失去该组为他们授予的特权。

前提条件

验证是否已以具有**编辑管理员**权限的用户身份登录到 vRealize Log Insight Web 用户界面。URL 格式为 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

- 1 导航到**管理**选项卡。
- 2 在“管理”下，单击**访问控制**。
- 3 单击**用户和组**。
- 4 选中要删除的用户名或组旁边的复选框。
- 5 要移除帐户或组，请单击“用户帐户”或“组”表顶部的 **X 删除**。

配置身份验证

3

可以在您的部署中使用几种身份验证方法。

身份验证方法包括本地身份验证、VMware Identity Manager 身份验证和 Active Directory 身份验证。您可以在同一部署中使用多种方法，然后用户选择在登录时使用的身份验证类型。

vRealize Log Insight 下载页面包含相应 VMware Identity Manager 版本的下载链接。VMware Identity Manager 包含以下功能。

- 目录集成，以便在现有的目录中对用户进行身份验证，例如，Active Directory 或 LDAP。
- 单点登录与也支持该功能的其他 VMware 产品集成在一起。
- 使用某些第三方身份提供程序的单点登录，例如，ADFS、Ping Federate，等等。
- 通过与第三方软件（如 RSA SecurID、Entrust 等）集成的双因素身份验证。包括使用 VMware Verify 的双因素身份验证。

本地身份验证是一个 vRealize Log Insight 组件。要使用这种身份验证，请创建一个存储在 vRealize Log Insight 服务器上的本地用户和密码。产品管理员必须启用 vRealize Log Insight 和 Active Directory。

本章讨论了以下主题：

- 启用通过 [VMware Identity Manager](#) 进行用户身份验证
- 启用通过 [Active Directory](#) 的用户身份验证

启用通过 VMware Identity Manager 进行用户身份验证

管理员启用 VMware Identity Manager 身份验证后，可以在 vRealize Log Insight 中使用该身份验证。

通过使用 VMware Identity Manager 身份验证，用户可以在使用相同 Identity Manager 的所有 VMware 产品中使用单点登录。

如果已同步 Active Directory 和 VMware Identity Manager 服务器，Active Directory 用户也可以通过 VMware Identity Manager 进行身份验证。请参见 VMware Identity Manager 文档，以了解有关同步的详细信息。

与 VMware Identity Manager 的集成只能由本地用户完成。在 VMware Identity Manager 中分配了租户管理员角色的 Active Directory 用户不符合与 vRealize Log Insight 集成的条件。

前提条件

验证是否已具有**编辑管理员**权限的用户身份登录到 vRealize Log Insight Web 用户界面。URL 格式为 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

- 1 导航到**管理**选项卡。
- 2 在“配置”下，单击**身份验证**。
- 3 选择**启用单点登录**。
- 4 在**主机**文本框中，输入用于验证用户身份的 VMware Identity Manager 实例的主机标识符。
例如，`company-name.vmwareidentity.com`。
- 5 在**API 端口**文本框中，指定用于连接到 VMware Identity Manager 实例的端口。默认值为 443。
- 6 （可选）输入 VMware Identity Manager 租户。只有在 VMware Identity Manager 中将租户模式配置为“路径中的租户”时，才需要输入该信息。
- 7 在**用户名**和**密码**文本框中指定 VMware Identity Manager 用户凭据。
在配置期间，仅使用一次该信息以在 VMware Identity Manager 上创建 vRealize Log Insight 客户端，而不会在 vRealize Log Insight 本地存储该信息。用户必须具有针对租户运行 API 命令的权限。
- 8 单击**测试连接**以验证连接是否正常工作。
- 9 如果 VMware Identity Manager 实例提供了不受信任的 SSL 证书，则会显示一个对话框，其中显示有该证书的详细信息。单击**接受**将证书添加到 vRealize Log Insight 集群中所有节点的信任库。
如果单击**取消**，则不会将该证书添加到信任库，并且与 VMware Identity Manager 实例的连接将失败。您必须接受证书才能成功连接。
- 10 在**重定向 URL 主机**下拉菜单中，选择要在重定向 URL 中用于在 VMware Identity Manager 上进行注册的主机名或 IP。
如果为集成负载均衡器定义了至少一个虚拟 IP，VMware Identity Manager 将重定向到选定的 VIP。如果未配置集成负载均衡器，则会改为使用主节点的 IP 地址。
- 11 选择是否为 Active Directory 用户启用通过 VMware Identity Manager 的登录支持。
如果 VMware Identity Manager 已与该 Active Directory 实例同步，则可以针对 Active Directory 用户使用该选项。
- 12 单击**保存**。
如果未测试连接，并且 VMware Identity Manager 实例提供的证书不受信任，请按照第 9 步中的说明进行操作。

启用通过 Active Directory 的用户身份验证

您可以让用户使用用于多种用途的通用密码，来通过 Active Directory 对用户进行身份验证，从而简化登录过程。

不支持通过 Active Directory 访问子域。只支持通过 VMware Identity Manager 进行此类访问。

前提条件

验证是否已具有**编辑管理员**权限的用户身份登录到 vRealize Log Insight Web 用户界面。URL 格式为 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

- 1 导航到**管理**选项卡。
- 2 在“配置”下，单击**身份验证**。
- 3 选择**启用 Active Directory 支持**。
- 4 在**默认域**文本框中，键入域名。

例如，**company-name.com**。

注 无法在“默认域”文本框中列出多个域。如果您指定的默认域被其他域信任，则 vRealize Log Insight 会使用默认域和绑定用户来验证信任域中的 Active Directory 用户和组。不支持通过 Active Directory 访问子域。

如果切换到已包含用户和组的其他域，现有用户和组的身份验证将会失败，并且现有用户保存的数据将会丢失。

- 5 如果您的域控制器按地理位置定位或具有安全性限制，请手动指定最接近此 vRealize Log Insight 实例的域控制器。

注 不支持负载均衡的 Active Directory 授权服务器。

- 6 输入属于默认域的绑定用户的凭据。
vRealize Log Insight 使用默认域和绑定用户来验证默认域中和信任默认域的域中的 AD 用户和组。
- 7 指定连接类型值。
此连接用于 Active Directory 身份验证。
- 8 单击**测试连接**以验证连接是否正常工作。
- 9 如果 Active Directory 服务器提供了不受信任的 SSL 证书，则会显示一个对话框，其中显示有该证书的详细信息。单击**接受**将证书添加到 vRealize Log Insight 群集中所有节点的信任库。

如果单击**取消**，则不会将该证书添加到信任库，并且与 Active Directory 服务器的连接将失败。您必须接受证书才能成功连接。

10 单击保存。

如果未测试连接，并且 Active Directory 服务器提供了不受信任的证书，请按照第 9 步中的说明进行操作。

后续步骤

为 Active Directory 用户和组授予访问当前 vRealize Log Insight 实例的权限。

配置用于 Active Directory 的协议

您可以配置连接至 Active Directory 时使用的协议。默认情况下，vRealize Log Insight 在连接到 Active Directory 时，会首先尝试 SSL LDAP，然后再尝试非 SSL LDAP（如果需要）。

如果要限制与某个特定协议的 Active Directory 通信，或者要更改尝试协议的顺序，必须在 vRealize Log Insight 虚拟设备中应用其他配置。

前提条件

- 验证是否拥有可登录 vRealize Log Insight 虚拟设备的 root 用户凭据。
- 要启用 SSH 连接，请验证是否已打开 TCP 端口 22。

步骤

- 1 与 vRealize Log Insight 虚拟设备建立 SSH 连接，然后以 root 用户身份登录。
- 2 导航到以下位置：/storage/core/loginsight/config
- 3 找到 [number] 最大的最新配置文件：/storage/core/loginsight/config/loginsight-config.xml#[number]
- 4 复制最新的配置文件：/storage/core/loginsight/config/loginsight-config.xml#[number]
- 5 增加 [number] 并保存到以下位置：/storage/core/loginsight/config/loginsight-config.xml#[number + 1]
- 6 打开文件进行编辑。
- 7 在 Authentication 部分中，添加与要应用的配置对应的行：

选项	描述
<code><ad-protocols value="LDAP" /></code>	针对使用非 SSL LDAP
<code><ad-protocols value="LDAPS" /></code>	仅针对使用 SSL LDAP
<code><ad-protocols value="LDAP,LDAPS" /></code>	针对首先使用 LDAP，然后使用 SSL LDAP。
<code><ad-protocols value="LDAPS,LDAP" /></code>	针对首先使用 LDAPS，然后使用非 SSL LDAP。

如果未选中任何协议，vRealize Log Insight 会尝试首先使用 LDAP，然后使用 SSL LDAP。

- 8 保存并关闭文件。

9 运行 `service loginsight restart` 命令。

配置 vRealize Log Insight

4

您可以配置和自定义 vRealize Log Insight 以更改默认设置、网络设置，并修改存储资源。还可以配置系统通知。

本章讨论了以下主题：

- vRealize Log Insight 配置限制
- 添加日志筛选器配置
- 添加日志屏蔽配置
- 配置虚拟设备设置
- 向 vRealize Log Insight 分配许可证
- 日志存储策略
- 管理系统通知
- 添加 vRealize Log Insight 事件转发目标
- 同步 vRealize Log Insight 虚拟设备上的时间
- 为 vRealize Log Insight 配置 SMTP 服务器
- 配置 Webhook
- 安装自定义 SSL 证书
- 查看和移除 SSL 证书
- 更改 vRealize Log Insight Web 会话的默认超时期限。
- 保留和存档
- 重新启动 vRealize Log Insight 服务
- 关闭 vRealize Log Insight 虚拟设备的电源
- 下载 vRealize Log Insight 支持包
- 加入或退出 VMware 客户体验改善计划
- 为 vRealize Log Insight 配置 STIG 合规性
- 为 vRealize Log Insight 激活 FIPS

vRealize Log Insight 配置限制

在配置 vRealize Log Insight 时，必须等于或低于支持的最大值。

表 4-1. vRealize Log Insight 最高配置

项目	最大值
节点配置	
CPU	16 个 vCPU
内存	32GB
存储设备 (vmdk)	2 TB - 512 字节
总可寻址存储	4 TB (+ 操作系统驱动器) 虚拟机磁盘 (VMDK) 上的最大总可寻址日志存储为 4 TB，每个 VMDK 的最大大小为 2 TB。您可以具有两个 2 TB 的 VMDK 或四个 1 TB 的 VMDK，以此类推。达到最大限制后，必须向外扩大集群的规模，而不是向现有虚拟机添加更多的磁盘。
Syslog 连接	750
集群配置	
节点	18 个 (1 个主节点 + 17 个工作线程节点)
虚拟 IP 地址	12
每节点载入速率	
每秒事件数	15,000 EPS
Syslog 消息长度	10 KB (文本字段)
数据获取 API HTTP POST 请求	16 KB (文本字段)；每个 HTTP Post 请求 4 MB
集成	
vRealize Operations Manager	1
vSphere vCenter Server	每个节点 15 个
Active Directory 域	1
电子邮件服务器	1
DNS 服务器	2
NTP 服务器	4
转发器	10
数据分区配置	
数据分区	5

添加日志筛选器配置

您可以通过添加相应配置来丢弃与所提供的筛选标准匹配的日志。

通过丢弃日志，您可以仅查看所需的日志，这样做具有成本效益，并且可以节省存储和提高性能。

注

- 日志筛选器配置仅适用于在创建并启用该配置后载入的日志。
- 日志筛选器配置仅适用于含有筛选标准中的静态字段的日志。

前提条件

验证是否已具有**编辑管理员**权限的用户身份登录到 vRealize Log Insight Web 用户界面。URL 格式为 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

- 1 导航到**管理**选项卡。
- 2 在“管理”下，单击**日志管理**，然后单击**日志筛选**。
- 3 单击 **+新建配置**。
- 4 输入日志筛选器配置的唯一名称。
- 5 选择字段和限制以定义要丢弃的日志。如果不选择筛选器，将丢弃所有日志。要查看筛选器的结果，请单击在**交互式分析中运行**。

运算符	描述
匹配	查找匹配字符串和通配符规范的字符串，其中 * 表示零个或多个字符，? 表示零个或任意单个字符。支持前缀和后缀通配。 例如， *test* 与 test123 或 my-test-run 等字符串匹配。
不匹配	排除匹配字符串和通配符规范的字符串，其中 * 表示零个或多个字符，? 表示零个或任意单个字符。支持前缀和后缀通配。 例如， test* 会排除 test123 ，但不会排除 mytest123 。 ?test* 会排除 test123 和 xtest123 ，但不会排除 mytest123 。
开头为	查找以指定字符串开头的字符串。 例如， test 找到 test123 或 test ，但不会找到 my-test123 。
不以下列字符开头	排除以指定字符串开头的字符串。 例如， test 筛选掉 test123 ，但不会排除 my-test123 。

- 6 日志筛选器配置在默认情况下处于启用状态。要禁用该配置，请单击**已启用**切换按钮。
- 7 单击**保存**。

结果

日志筛选器配置显示在**日志筛选**选项卡中，该选项卡包含有关丢弃筛选器及其是否已启用的信息。您可以通过单击**已启用**切换按钮来启用或禁用该配置。

添加日志屏蔽配置

您可以通过添加相应配置来屏蔽所有日志或与所提供的筛选标准匹配的日志中的敏感信息。

注

- 日志屏蔽配置仅适用于在创建并启用该配置后载入的日志。
- 日志屏蔽配置仅适用于含有 *FieldName* 字段和筛选标准中的静态字段的日志。

前提条件

验证是否已具有**编辑管理员**权限的用户身份登录到 vRealize Log Insight Web 用户界面。URL 格式为 `https://log-insight-host`，其中 *log-insight-host* 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

- 1 导航到**管理**选项卡。
- 2 在“管理”下，单击**日志管理**，然后单击**日志屏蔽**。
- 3 单击 **+新建配置**。
- 4 输入日志屏蔽配置的唯一名称。
- 5 在**字段名称**下拉菜单中，选择要在日志中屏蔽的字段。
- 6 在**选择器**文本框中，输入字段值的正则表达式选择器，以指示要屏蔽的字段部分。

您必须将此值表示为正则表达式中的捕获组。捕获组用圆括号 () 进行标识。您可以在选择器内包含多个捕获组。要屏蔽指定字段的所有内容，可将选择器设置为 `(.*)`。

- 7 在**掩码值**文本框中，输入一个值来替换指定字段中被屏蔽的内容，其默认值为空字符串。
- 8 单击 **+添加筛选器**以定义要屏蔽信息的日志。如果不添加筛选器，将屏蔽所有日志。要查看筛选器的结果，请单击在**交互式分析**中运行。

运算符	描述
匹配	查找匹配字符串和通配符规范的字符串，其中 * 表示零个或多个字符，? 表示零个或多个任意单个字符。支持前缀和后缀通配。 例如， <code>*test*</code> 与 <code>test123</code> 或 <code>my-test-run</code> 等字符串匹配。
不匹配	排除匹配字符串和通配符规范的字符串，其中 * 表示零个或多个字符，? 表示零个或多个任意单个字符。支持前缀和后缀通配。 例如， <code>test*</code> 会排除 <code>test123</code> ，但不会排除 <code>mytest123</code> 。 <code>?test*</code> 会排除 <code>test123</code> 和 <code>xtest123</code> ，但不会排除 <code>mytest123</code> 。

运算符	描述
开头为	查找以指定字符串开头的字符串。 例如， test 找到 test123 或 test ，但不会找到 my-test123 。
不以下列字符开头	排除以指定字符串开头的字符串。 例如， test 筛选掉 test123 ，但不会排除 my-test123 。

9 日志屏蔽配置在默认情况下处于启用状态。要禁用该配置，请单击**已启用**切换按钮。

10 单击**保存**。

结果

日志屏蔽配置显示在**日志屏蔽**选项卡中，该选项卡包含该配置是否已启用、应用该配置的日志等相关信息。您可以通过单击**已启用**切换按钮来启用或禁用该配置。

配置虚拟设备设置

您可以修改虚拟设备设置，包括存储容量和内存或 CPU 容量。

配置 vRealize Log Insight 虚拟设备的根 SSH 密码

默认情况下，与虚拟设备的 SSH 连接已禁用。您可以从 VMware Remote Console 或在部署 vRealize Log Insight 虚拟设备时配置根 SSH 密码。

作为最佳实践，请在部署 vRealize Log Insight .ova 文件时设置根 SSH 密码。有关详细信息，请参见[部署 vRealize Log Insight 虚拟设备](#)。

您还可以启用 SSH，并从 VMware Remote Console 设置根密码。

前提条件

验证 vRealize Log Insight 虚拟设备是否已部署且正在运行。

步骤

- 1 在 vSphere Client 清单中，单击 vRealize Log Insight 虚拟设备，然后打开**控制台**选项卡。
- 2 按照初始屏幕上指定的组合键转到命令行。
- 3 在控制台中，键入 **root**，然后按 Enter。将密码留空，然后按 Enter。

控制台中会显示以下消息：已请求密码更改。请选择新密码 (Password change requested. Choose a new password)。

- 4 将旧密码留空，然后按 Enter。
- 5 键入 root 用户的新密码，按 Enter，再次键入 root 用户的新密码，然后按 Enter。

密码必须至少包含 8 个字符，并且必须至少包括 1 个大写字母、1 个小写字母、1 个数字和 1 个特殊字符。同一字符不得重复四次以上。

结果

将显示以下消息：密码已更改 (Password changed)。

后续步骤

可以使用根密码与 vRealize Log Insight 虚拟设备建立 SSH 连接。

更改 vRealize Log Insight 虚拟设备的网络设置

您可以按照 <https://kb.vmware.com/s/article/87992> 中所述的步骤更改 vRealize Log Insight 虚拟设备的网络设置。

增加 vRealize Log Insight 虚拟设备的存储容量

随着需求的增长，您可以增加分配给 vRealize Log Insight 的存储资源。

可以通过向 vRealize Log Insight 虚拟设备添加新虚拟磁盘来增加存储空间。您可以根据需要添加任意数量的磁盘，但总可寻址存储最高为 4 TB（包含操作系统驱动器）。总存储可以是两个 2 TB 磁盘或四个 1 TB 磁盘等形式的组合。请参见 [vRealize Log Insight 配置限制](#)。

在 vRealize Log Insight 群集中，您必须向群集中的每个节点添加相同数量的存储。

前提条件

- 以具有修改环境中虚拟机硬件特权的用户身份登录到 vSphere Client。
- 安全地关闭 vRealize Log Insight 虚拟设备。请参见[关闭 vRealize Log Insight 虚拟设备的电源](#)

步骤

- 1 在 vSphere Client 清单中，右键单击 vRealize Log Insight 虚拟机并选择**编辑设置**。
- 2 在**硬件**选项卡上，单击**添加**。
- 3 选择**硬盘**，然后单击**下一步**。

4 选择**创建新的虚拟磁盘**，然后单击**下一步**。

a 键入磁盘容量。

vRealize Log Insight 最大支持 2 TB 虚拟硬盘。如果需要更多容量，可添加多个虚拟硬盘。

b 选择磁盘格式。

选项	描述
厚置备延迟置零	以默认的厚格式创建虚拟磁盘。创建虚拟磁盘时分配虚拟磁盘所需的空間。创建时不会擦除物理设备上驻留的数据，但是以后首次从虚拟设备写入后会按需要将其置零。
厚置备置零	创建支持群集功能（如 Fault Tolerance）的一种厚虚拟磁盘类型。在创建时为虚拟磁盘分配所需的空間。与平面格式相反，在创建虚拟磁盘时，会将物理设备上驻留的数据置零。创建这种格式的磁盘所需的时间可能会比创建其他类型的磁盘长。 尽可能创建厚置备置零磁盘，以获得更佳性能以及保证 vRealize Log Insight 虚拟设备的运行。
精简置备	创建精简格式的磁盘。使用此格式可节省存储空间。

c （必选）要选择数据存储，请浏览数据存储位置，然后单击**下一步**。

5 接受默认虚拟设备节点，然后单击**下一步**。

6 检查信息，然后单击**完成**。

7 单击**确定**保存更改并关闭对话框。

结果

在您打开 vRealize Log Insight 虚拟设备电源后，虚拟机会发现新虚拟磁盘并自动将其添加到默认数据卷。请先完全关闭虚拟机的电源。有关打开虚拟设备电源的信息，请参见 <https://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-6-pubs.html>。

小心 将磁盘添加到虚拟设备后，无法将其安全移除。从 vRealize Log Insight 虚拟设备移除磁盘可能会导致数据全部丢失。

向 vRealize Log Insight 虚拟设备添加内存和 CPU

在部署后，可以更改分配给 vRealize Log Insight 虚拟设备的内存和 CPU 量。

例如，如果环境中的事件数量增加，则可能需要调整资源分配。

前提条件

- 以具有修改环境中虚拟机硬件特权的用户身份登录到 vSphere Client。
- 安全地关闭 vRealize Log Insight 虚拟设备。请参见[关闭 vRealize Log Insight 虚拟设备的电源](#)

步骤

1 在 vSphere Client 清单中，右键单击 vRealize Log Insight 虚拟机并选择**编辑设置**。

- 2 在**硬件**选项卡上，单击**添加**。
- 3 根据需要调整 CPU 和内存量。
- 4 检查信息，然后单击**完成**。
- 5 单击**确定**保存更改并关闭对话框。

结果

打开 vRealize Log Insight 虚拟设备电源时，虚拟机将开始利用新资源。

向 vRealize Log Insight 分配许可证

只有使用有效许可证密钥才能使用 vRealize Log Insight。

从 VMware 网站下载 vRealize Log Insight 时，您可以获取一个评估许可证。此许可证的有效期是 60 天。评估许可证过期后，必须分配永久许可证才能继续使用 vRealize Log Insight。

vRealize Log Insight 操作系统实例 (Operating System Instance, OSI) 许可证模式将 OSI 定义为非虚拟化物理服务器或虚拟机上的单个操作系统安装。对于 vRealize Log Insight，OSI 也可以是一个由 IP 地址标识的系统，例如，虚拟化物理服务器、存储阵列或可生成日志消息的网络设备。

当某个主机、服务器或其他源停止向 vRealize Log Insight 发送日志时，“许可证”页面上的 OSI 计数在保留期限内将保持不变。保留期限基于许可证使用情况，其计算方式为过去三个月 OSI 计数的平均值。

您可以使用 vRealize Log Insight Web 用户界面的“管理”部分检查 vRealize Log Insight 许可状态并管理许可证。

作为解决方案互操作性的一部分，VMware NSX Standard、Advanced 或 Enterprise 版用户可以使用其 NSX 许可证密钥来许可 vRealize Log Insight。有关详细信息，请参阅 VMware NSX 文档。

前提条件

- 从 My VMware™ 中获取有效许可证密钥。
- 验证是否已以具有**编辑管理员**权限的用户身份登录到 vRealize Log Insight Web 用户界面。URL 格式为 `https://log-insight-host`，其中 *log-insight-host* 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

- 1 导航到**管理**选项卡。
- 2 在“管理”下，选择**许可证**。
- 3 在**许可证密钥**文本框中，输入您的许可证密钥，然后单击**设置密钥**。如果您具有 VMware NSX 许可证密钥，请在此处输入该密钥。
- 4 验证许可证状态是否为“活动”，以及许可证类型和过期日期是否正确。

日志存储策略

vRealize Log Insight 虚拟设备至少使用 100GB 的存储用于入站日志。

在导入到 vRealize Log Insight 的日志量达到存储限制时，将按照先入站先停用原则自动和定期停用旧日志消息。您可以在 vRealize Log Insight 虚拟设备中添加更多存储以增加存储限制。请参见[增加 vRealize Log Insight 虚拟设备的存储容量](#)。

要保留旧消息，可以启用 vRealize Log Insight 的存档功能。请参见[数据存档](#)。

由 vRealize Log Insight 存储的数据不可变。日志在导入后，无法移除，直到其自动停用。

管理系统通知

vRealize Log Insight 提供了有关 vRealize Log Insight 运行状况相关活动的内置系统通知，例如，当磁盘空间几乎用尽并且将要删除旧日志文件时便会发出通知。管理员可以配置系统通知的发送频率和目标。

系统通知用于告知您需要立即注意的严重问题、向您提供可能需要做出响应的警告，以及告知您系统活动正常。系统通知在升级期间会被挂起，而在所有其他时间都将起效。

管理员可以指定触发后发送通知的频率以及电子邮件的目标地址。有关 vRealize Log Insight 的系统通知也可以发送到第三方应用程序。

系统通知不同于用户定义的警示查询。有关警示查询的详细信息，请参见在[Log Insight 中添加警示查询以发送电子邮件通知](#)。

vRealize Log Insight 系统通知

vRealize Log Insight 为您提供两组有关系统运行状况的通知：适用于所有产品配置的常规通知，以及与基于集群的部署中的集群相关的通知。

以下各表列出并介绍了 vRealize Log Insight 的系统通知。

注 在本主题中，管理员用户是指与超级管理员角色相关联的用户，或与具有相应权限的角色相关联的用户，如[创建和修改角色](#)中所述。

常规系统通知

在发生可能需要管理干预的情况（包括存档失败或警示计划延迟）时，vRealize Log Insight 将会发出通知。

通知名称	描述
最旧的数据即将不可搜索	<p>vRealize Log Insight 预计根据预期可搜索数据大小、存储空间和当前载入速率开始停用虚拟设备存储中的旧数据。如果已配置存档，将会存档已停用的数据，如果未配置，则会删除。</p> <p>要解决该问题，请添加存储或调整保留通知阈值。有关详细信息，请参见配置 vRealize Log Insight 以发送运行状况通知。</p> <p>通知将在每次重新启动 vRealize Log Insight 服务后发送。</p>
存储库保留时间	<p>保留期是在 vRealize Log Insight 实例的本地磁盘上保留数据的时间长度。保留期是由系统可保留的数据量以及当前载入速率决定的。例如，如果每天收到 10 GB 数据（在编制索引后）并具有 300 GB 空间，则保留速率为 30 天。</p> <p>在达到存储限制时，将移除旧数据，以便为新载入的数据腾出空间。该通知告诉您，vRealize Log Insight 以当前载入速率存储的可搜索数据量何时超过虚拟设备上的可用存储空间。</p> <p>您可能在使用保留通知阈值设置的时间段结束前用完存储。请添加存储或调整保留通知阈值。</p>
已丢弃的事件	<p>vRealize Log Insight 无法载入所有入站日志消息。</p> <ul style="list-style-type: none"> ■ 如果 vRealize Log Insight 服务器跟踪发现丢弃了 TCP 消息，则会按以下方式发送系统通知： <ul style="list-style-type: none"> ■ 每天一次 ■ 每次手动或自动重新启动 vRealize Log Insight 服务时 ■ 电子邮件包含自上次通知电子邮件发送后丢弃的消息数量，以及自上次重新启动 vRealize Log Insight 后丢弃的消息总数。 <p>注 发送行中的时间由电子邮件客户端控制，并且以当地时区显示，而电子邮件正文则显示 UTC 时间。</p>
损坏索引段	<p>磁盘上的索引的一部分已损坏。损坏索引通常表示基础存储系统存在严重问题。索引的损坏部分将从服务查询中排除。损坏索引会影响新数据的载入。vRealize Log Insight 会在服务启动时检查索引的完整性。如果检测到损坏，vRealize Log Insight 会按以下方式发送系统通知：</p> <ul style="list-style-type: none"> ■ 每天一次 ■ 每次手动或自动重新启动 vRealize Log Insight 服务时
磁盘空间不足	<p>vRealize Log Insight 将用完分配的磁盘空间。vRealize Log Insight 很可能出现与存储相关的问题。</p>
存档空间将满	<p>NFS 服务器上用于存档 vRealize Log Insight 数据的磁盘空间将很快用完。如果在当前载入速率下 NFS 服务器可以保存的已存档数据量小于七天，则会发送系统通知。例如，如果您以 708.9 MB/天的磁盘消耗率进行存档，并且有 2000 MB 的空间，则您拥有约三天的容量，这小于阈值。在这种情况下，您将收到低于此容量的通知。</p>
总磁盘空间更改	<p>vRealize Log Insight 数据存储的总分区大小已减小。此通知通常表示底层存储系统中存在严重问题。当 vRealize Log Insight 检测到该情况时，会按以下方式发送此通知：</p> <ul style="list-style-type: none"> ■ 立即 ■ 每天一次
挂起的存档	<p>vRealize Log Insight 无法按预期方式存档数据。该通知通常表示您配置用于数据存档的 NFS 存储存在问题。</p>

通知名称	描述
分配的日志记录存储卷已达到最大日志记录存储容量的 75%	<p>已配置 vRealize Log Insight 以确保 STIG 合规性，并且分配的日志记录存储卷达到存储库最大日志记录存储容量的 75%。</p> <p>注 此通知按节点发送。</p>
许可证即将过期	vRealize Log Insight 的许可证即将过期。
许可证过期	vRealize Log Insight 的许可证已过期。
SSL 证书即将过期	vRealize Log Insight 集群的 SSL 证书将在 30 天后过期。
无法连接 AD 服务器	vRealize Log Insight 无法连接到配置的 Active Directory 服务器。
无法接管 High Availability IP 地址 [IP Address]，因为其他计算机已拥有它	<p>vRealize Log Insight 集群无法接管为集成负载均衡器 (Integrated Load Balancer, ILB) 配置的 IP 地址。出现此通知的最常见原因是同一网络中的其他主机拥有该 IP 地址，因此集群无法接管该 IP 地址。</p> <p>通过从当前拥有该 IP 地址的主机释放该 IP 地址，或者使用网络中可用的静态 IP 地址配置 Log Insight 集成负载均衡器，您可以解决此冲突。当更改 ILB IP 地址时，必须重新配置所有客户端以将日志发送到新的 IP 地址，或者发送到可解析为此 IP 地址的 FQDN/URL。您还必须从“vSphere 集成”页面取消配置与 vRealize Log Insight 集成的每个 vCenter Server，然后重新对其进行配置。</p>
由于节点故障太多，High Availability IP 地址 [IP Address] 不可用	<p>为集成负载均衡器 (ILB) 配置的 IP 地址不可用。在客户端尝试通过 ILB IP 地址或可解析为此 IP 地址的 FQDN/URL 将日志发送到 vRealize Log Insight 集群时，此 IP 地址将在客户端中显示为不可用。发出此通知的最常见原因是 vRealize Log Insight 集群中的大多数节点不正常、不可用或无法从主节点访问。另一个常见原因是尚未启用 NTP 时间同步，或者配置的 NTP 服务器彼此之间存在相当大的时间偏移。您可以尝试对 IP 地址执行 ping 操作（如果允许）以验证是否可以访问该地址，以确认该问题是否仍然存在。</p> <p>通过确保大多数集群节点正常且可访问，并启用与精确 NTP 服务器的 NTP 时间同步，可以解决此问题。</p>
vRealize Log Insight 节点之间的 High Availability IP 地址 [您的 IP 地址] 迁移次数太多	<p>在最近 10 分钟内，为集成负载均衡器 (ILB) 配置的 IP 地址的迁移次数太多。</p> <p>在正常操作下，IP 地址很少在 vRealize Log Insight 集群节点之间移动。但是，如果当前所有者节点重新启动或处于维护状态下，IP 地址可能移动。另一个原因可能是 Log Insight 集群节点之间未进行时间同步，而时间同步对于保证集群正常运行至关重要。对于后者，通过启用与精确 NTP 服务器的 NTP 时间同步，可以修复此问题。</p>
SSL 证书错误	<p>syslog 源已通过 SSL 启动到 vRealize Log Insight 的连接，但突然终止了该连接。此通知可能表示 syslog 源无法确认 SSL 证书的有效性。为了使 vRealize Log Insight 接受 SSL 上的 syslog 消息，需要具备一个由客户端验证的证书，且系统时钟必须进行同步。可能是 SSL 证书或者网络时间服务出现了问题。</p> <p>您可以验证 SSL 证书是否受 syslog 源信任、将源重新配置为不使用 SSL 或重新安装 SSL 证书。请参见配置 vRealize Log Insight 代理的 SSL 参数和安装自定义 SSL 证书。</p>
vCenter 收集失败	vRealize Log Insight 无法收集 vCenter 事件、任务和警报。要查找导致收集失败的确切错误，并了解当前是否正在进行收集，请查看 <code>/var/log/vmware/loginsight/plugins/vsphere/li-vsphere.log</code> 文件。

通知名称	描述
vCenter Kubernetes 服务事件收集失败	vRealize Log Insight 无法收集 vCenter Kubernetes 系统事件、任务和警报。要查找导致收集失败的确切错误，并了解当前是否正在进行收集，请查看 <code>/var/log/vmware/loginsight/plugins/vsphere/li-vsphere.log</code> 文件。
丢弃了事件转发器的事件	<p>由于连接或过载问题，转发器丢弃了事件。</p> <p>示例：</p> <pre>Log Insight Admin Alert: Event Forwarder Events Dropped This alert is about your Log Insight installation on https://<your_url> Event Forwarder Events Dropped triggered at 2016-08-02T18:41:06.972Z Log Insight just dropped 670 events for forwarder target 'Test', reason: Pending queue is full.</pre>
警示查询延迟	vRealize Log Insight 无法在配置的时间运行用户定义的警示。出现延迟的原因可能是，存在一个或多个用户定义的低效警示，或者未正确调整系统大小以满足载入和查询负载要求。
自动禁用警示	如果用户定义的警示已运行至少 10 次，并且平均运行时间超过一小时，则会将该警示视为低效警示，并将其禁用以免影响其他用户定义的警示。
低效的警示查询	如果用户定义的警示需要超过一小时才能完成，则会将该警示视为低效警示。
创建新用户或者用户首次登录	已配置 vRealize Log Insight 以确保 STIG 合规性，并且创建新用户或者 Active Directory 或 VMware Identity Manager 用户首次登录。

有关集群的系统通知

vRealize Log Insight 会发送有关集群拓扑更改的通知，包括添加新的集群成员或暂时性节点通信问题。

发送人	通知名称	描述
主节点	新工作线程节点需要批准	工作线程节点发送请求以加入集群。管理员用户必须批准或拒绝该请求。
主节点	已批准新工作线程节点	管理员用户已批准工作线程节点加入 vRealize Log Insight 集群的成员资格请求。
主节点	已拒绝新工作线程节点	管理员用户已拒绝工作线程节点加入 vRealize Log Insight 集群的成员资格请求。如果错误地拒绝了该请求，管理员用户可以从工作线程节点重新提出该请求，然后在主节点上批准该请求。
主节点	新添加的工作线程节点使节点数超出所支持的最大数量	由于添加新的工作线程节点，Log Insight 集群中的工作线程节点数超出支持的最大节点数。
主节点	允许的节点数超出，已拒绝新工作线程节点	用户尝试在集群中添加的节点超出允许的最大节点数，因此已拒绝该节点。

发送人	通知名称	描述
主节点	工作线程节点已断开连接	已将以前连接的工作线程节点从 vRealize Log Insight 集群断开连接。
主节点	工作线程节点已重新连接	已将工作线程节点重新连接到 vRealize Log Insight 集群。
主节点	工作节点已撤销	管理员用户已撤销工作线程节点成员资格，并且该节点不再属于 vRealize Log Insight 集群。
主节点	已拒绝未知工作线程节点	vRealize Log Insight 主节点已拒绝工作线程节点的请求，因为该工作线程节点对主节点而言为未知节点。如果工作线程节点是有效节点，并且应将其添加到集群，请登录到该工作线程节点，在 <code>/storage/core/loginsight/config/</code> 上移除其令牌文件和用户配置，然后在该工作线程节点上运行 <code>restart loginsight service</code> 。
主节点	工作线程节点已进入维护模式	工作线程节点已进入维护模式，管理员用户必须将该工作线程节点退出维护模式，然后它才能接收配置更改和处理查询。
主节点	工作线程节点已恢复运行	工作线程节点已退出维护模式并恢复提供服务。
工作线程节点	主节点出现故障或从工作线程节点断开连接	<p>发送通知的工作线程节点无法联系 vRealize Log Insight 主节点。此通知可能表明主节点出现故障，可能需要重新启动。如果主节点出现故障，则在主节点恢复联机之前，将无法配置集群，并且无法提交查询。工作线程节点继续采集消息。</p> <p>注 您可能会接收到许多此类通知，这是因为多个工作线程节点可能会分别检测到主节点故障，并发出通知。</p>
工作线程节点	主节点已连接到工作线程节点	发送通知的工作线程节点已重新连接到 vRealize Log Insight 主节点。

为 vRealize Log Insight 系统通知配置目标

作为管理员用户，您可以配置在触发系统通知时 vRealize Log Insight 执行的操作。

在发生重要系统事件时，vRealize Log Insight 会生成系统通知，例如，当磁盘空间几乎用完，vRealize Log Insight 必须开始删除或存档旧日志文件时。

管理员可以配置 vRealize Log Insight 以发送有关这些事件的电子邮件通知。管理员用户可在管理 UI 的 SMTP 配置页面的**发件人**文本框中配置系统通知电子邮件的发件人地址。请参见[为 vRealize Log Insight 配置 SMTP 服务器](#)。

管理员用户还可以向第三方应用程序发送通知。请参见[配置 Webhook](#)。

配置 vRealize Log Insight 以发送运行状况通知

管理员可以配置 vRealize Log Insight 以发送与其自身运行状况相关的通知。

如果无法传送电子邮件，您会在 Web 界面上收到错误通知。

前提条件

- 验证是否已以具有**编辑管理员**权限的用户身份登录到 vRealize Log Insight Web 用户界面。URL 格式为 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。
- 确认为 vRealize Log Insight 配置 SMTP 服务器。有关详细信息，请参见 [vRealize Log Insight 配置 SMTP 服务器](#)。

步骤

- 1 导航到**管理**选项卡。
- 2 在“配置”下，单击**常规**。
- 3 在“警示”标题下，设置系统通知。
 - a 在**系统通知电子邮件收件人**文本框中，键入要通知的电子邮件地址。
使用逗号分隔多个电子邮件地址。
 - b 选中**保留通知阈值**复选框，然后设置触发通知的阈值。
当在指定的时间段内系统可保存的数据量不足时，将会发送通知。此值基于当前的载入速率来计算。
- 4 单击**保存**。
- 5 单击**重新启动 Log Insight** 应用所做的更改。

为第三方产品配置 vRealize Log Insight 系统通知

管理员可以配置 vRealize Log Insight，以便向第三方应用程序发送与其自身运行状况相关的通知。

当出现重要系统事件时，例如，当磁盘空间几乎用尽，并且 vRealize Log Insight 必须开始删除旧日志文件时，vRealize Log Insight 会生成这些通知。

前提条件

验证是否已以具有**编辑管理员**权限的用户身份登录到 vRealize Log Insight Web 用户界面。URL 格式为 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

- 1 导航到**管理**选项卡。
- 2 在“配置”下，单击**常规**。

- 3 在“警示”标题下，设置系统通知。
 - a 在将 HTTP Post 系统通知发送到文本框中，键入要通知的 URL。
 - b （可选）确认已为环境正确配置了当容量降至低于复选框和相关阈值。
- 4 单击保存。

后续步骤

将 Webhook 配置为向第三方应用程序发送通知。有关详细信息，请参见配置 [Webhook](#)。

系统通知的 Webhook 格式

vRealize Log Insight Webhook 的格式取决于创建它的查询类型。系统通知、用户警示消息查询，以及从聚合用户查询生成的警示每个都有不同的 Webhook 格式。

您必须是 vRealize Log Insight 管理员，才能配置 vRealize Log Insight 以发送系统通知。

系统通知的 Webhook 格式

以下示例显示了系统通知的 vRealize Log Insight Webhook 格式。

```
{
  "AlertName": "Admin Alert: Worker node has returned to service (Host = 127.0.0.2)",
  "messages": [
    {
      "text": "This notification was generated from Log Insight node (Host = 127.0.0.2, Node Identifier = a31cad22-65c2-4131-8e6c-27790892a1f9). A worker node has returned to service after having been in maintenance mode. The Log Insight primary node reports that worker node has finished maintenance and exited maintenance mode. The node will resume receiving configuration changes and serving queries. The node is also now ready to start receiving incoming log messages."
    }
  ],
  "timestamp": 1458665320514, "fields": []
}
```

添加 vRealize Log Insight 事件转发目标

您可以配置 vRealize Log Insight 服务器以将传入事件转发到 syslog 或数据获取 API 目标。

使用事件转发可将筛选或标记的事件发送到一个或多个远程目标，例如 vRealize Log Insight 和/或 syslog。事件转发可用于支持现有的日志记录工具（例如 SIEM）以及整合不同网络（例如 DMZ 或 WAN）上的日志记录。

事件转发器可以是独立的，也可以是集群形式的，但事件转发器是与远程目标分离的实例。配置用于事件转发的实例也会在本地存储事件，并可用于查询数据。


在“已转发的事件”页面上用于创建筛选器的运算符与在“交互式分析”页面上用于创建筛选器的运算符不同。有关使用在交互式分析中运行菜单项预览事件筛选器结果的详细信息，请参见在交互式分析中使用日志管理筛选器。

前提条件

验证是否已以具有编辑管理员权限的用户身份登录到 vRealize Log Insight Web 用户界面。URL 格式为 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

验证目标可以处理转发的事件数。如果目标集群比转发实例小很多，可能会丢弃某些事件。

步骤

- 1 导航到**管理**选项卡。
- 2 在“管理”下，单击**日志管理**，然后单击**日志转发**。
- 3 单击  **新建目标**，然后提供以下信息。

选项	描述
名称	新目标的唯一名称。
主机	IP 地址或完全限定域名。 小心 转发循环是一种配置，在这种配置中，vRealize Log Insight 集群会向其自身或其他集群转发事件，之后目标集群又会将事件转发回原始集群。此类循环可能会为每个转发的事件创建无数个副本。vRealize Log Insight Web 界面不允许将事件配置为转发给自身。但是，vRealize Log Insight 无法阻止间接转发循环，例如 vRealize Log Insight 集群 A 将事件转发给集群 B，集群 B 又将相同的事件转发回集群 A。在创建转发目标时，请注意不要创建间接转发循环。
协议	<p>数据获取 API、syslog 或 RAW。默认值为数据获取 API (CFAPI)。</p> <p>当使用数据获取 API 转发事件时，事件的原始源会保留在源字段中。当使用 syslog 转发事件时，事件的原始源会丢失且接收器可以将消息源记录为 vRealize Log Insight 转发器的 IP 地址或主机名。使用 RAW 转发事件时，行为与 syslog 类似，但无法确保 syslog RFC 合规性。RAW 将完全按照接收事件的方式来转发事件，vRealize Log Insight 不会添加自定义 syslog 标头。此协议对于第三方目标非常有用，因为它们需要原始格式的 syslog 事件。</p> <p>注 根据在事件转发器上选定的协议，源字段的值可能有所不同：</p> <ul style="list-style-type: none"> a 对于数据获取 API，源是最初发送方（事件发生器）的 IP 地址。 b 对于 syslog 和 RAW，源是事件转发器的 vRealize Log Insight 实例 IP 地址。此外，消息文本包含指向最初发送方 IP 地址的 <code>_li_source_path</code>。
使用 SSL	您可以选择使用 SSL 保护数据获取 API 或 syslog 的连接。如果转发目标提供的 SSL 证书不受信任，您可以在测试或保存此配置时接受该证书。
标记	您可以选择添加带有预定义值的标记对。标记可使您更方便地查询事件。您可以采用逗号分隔的形式添加多个标记。

选项	描述
转发补充标记	您可以选择是否要转发 syslog 的补充标记。 补充标记是集群本身添加的标记，例如，“ vc_username ”或“ vc_vmname ”。可以将其与直接来自源的标记一起转发。在使用数据获取 API 时，将始终转发补充标记。
传输	选择 syslog 的传输协议。您可以选择“ UDP ”或“ TCP ”。

4 要控制转发的事件，请单击 添加筛选器。

选择字段和限制以定义所需的事件。只能将静态字段作为筛选器。如果不选择筛选器，将转发所有事件。通过单击在交互式分析中运行，可以查看所构建的筛选器的结果。

运算符	描述
匹配	查找匹配字符串和通配符规范的字符串，其中 * 表示零个或多个字符，? 表示零个或任意单个字符。支持前缀和后缀通配。 例如， *test* 与 test123 或 my-test-run 等字符串匹配。
不匹配	排除匹配字符串和通配符规范的字符串，其中 * 表示零个或多个字符，? 表示零个或任意单个字符。支持前缀和后缀通配。 例如， test* 会排除 test123 ，但不会排除 mytest123 。 ?test* 会排除 test123 和 xtest123 ，但不会排除 mytest123 。
开头为	查找以指定字符串开头的字符串。 例如， test 找到 test123 或 test ，但不会找到 my-test123 。
不以下列字符开头	排除以指定字符串开头的字符串。 例如， test 筛选掉 test123 ，但不会排除 my-test123 。

5 （可选）要修改以下转发信息，请单击显示高级设置。

选项	描述
端口	远程目标上向其发送事件的端口。将基于协议设置默认值。请勿更改，除非远程目标侦听其他端口。
工作线程数	要使用的同步出站连接数。设置的工作线程数越高，转发目标的网络延迟就越长，每秒转发的事件数也就越多。默认值为 8。

6 要验证您的配置，请单击测试。

7 如果转发目标提供了不受信任的 SSL 证书，则会显示一个对话框，其中显示有该证书的详细信息。单击接受将证书添加到 vRealize Log Insight 集群中所有节点的信任库。

如果单击取消，则不会将该证书添加到信任库中，并且与转发目标的连接将失败。您必须接受证书才能成功连接。

8 单击保存。

如果未测试配置，并且目标提供的证书不受信任，请按照第 7 步中的说明进行操作。

后续步骤

您可以编辑或克隆事件转发目标。如果编辑目标以更改事件转发器名称，则所有统计信息都将重置。

在交互式分析中使用日志管理筛选器

日志管理筛选器中使用的运算符与在交互式分析的筛选器中使用的运算符在名称上没有一一对应关系。但是，您可以选择为两种格式生成类似结果的运算符。

在使用**日志管理**页面的以下选项卡中的**在交互式分析中运行**菜单项时，这种差异是非常重要的：

- 日志屏蔽
- 日志筛选
- 日志转发
- 索引分区

例如，如果您的日志管理筛选器为**匹配 *foo***，并且您选择**在交互式分析中运行**菜单项，则交互式分析查询会将该日志管理筛选器视为等同于**匹配正则表达式 ^.*foo.* \$**，这可能不会匹配所有相同事件。

另一个例子是**匹配 foo**，在交互式分析上运行时，将其视为**包含 foo**。由于交互式分析功能还搜索关键字查询，因此，**包含 foo** 匹配的事件可能比**匹配 foo** 多。

您可以更改交互式分析使用的运算符以消除这些差异。

- 将**包含**运算符更改为**匹配正则表达式**。
- 将日志管理筛选器中出现的 ***** 更改为 **.***，并在筛选词前面添加 **.***。例如，将事件筛选器表达式**匹配 *foo*** 更改为**匹配正则表达式 .*foo.*** 以进行交互式分析。
- 对于事件筛选器中的**不匹配**运算符，您可以使用**匹配正则表达式**运算符以及正则表达式前向值。例如，**不匹配 *foo*** 相当于**匹配正则表达式 .*(?!foo).***。

同步 vRealize Log Insight 虚拟设备上的时间

必须将 vRealize Log Insight 虚拟设备上的时间与 NTP 服务器或在其中部署虚拟设备的 ESX/ESXi 主机上的时间同步。

时间对于 vRealize Log Insight 的核心功能很重要。

默认情况下，vRealize Log Insight 与预定义的公用 NTP 服务器列表同步时间。如果公用 NTP 服务器由于防火墙而无法访问，可以使用您公司的内部 NTP 服务器。如果没有 NTP 服务器可用，可以与在其中已部署 vRealize Log Insight 虚拟设备的 ESX/ESXi 主机同步时间。

前提条件

验证是否已具有**编辑管理员**权限的用户身份登录到 vRealize Log Insight Web 用户界面。URL 格式为 **https://log-insight-host**，其中 **log-insight-host** 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

- 1 导航到**管理**选项卡。
- 2 在“配置”下，单击**时间**。

- 3 从同步时间下拉菜单中，选择时间源。

选项	描述
NTP 服务器	将 vRealize Log Insight 虚拟设备上的时间与其中一个列出的 NTP 服务器同步。
ESX/ESXi 主机	将 vRealize Log Insight 虚拟设备上的时间与在其中部署虚拟设备的 ESX/ESXi 主机上的时间同步。

- 4 （可选）如果选择了 NTP 服务器同步，请列出 NTP 服务器地址，然后单击**测试**。

注 测试与 NTP 服务器的连接可能每台服务器最多需要 20 秒的时间。

- 5 单击**保存**。

为 vRealize Log Insight 配置 SMTP 服务器

可以配置 SMTP 以允许 vRealize Log Insight 发送电子邮件通知。

在 vRealize Log Insight 检测到重要系统事件时（例如，在虚拟设备上的存储容量达到设置的阈值时），将生成系统通知。

前提条件

验证是否已具有**编辑管理员**权限的用户身份登录到 vRealize Log Insight Web 用户界面。URL 格式为 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

- 1 导航到**管理**选项卡。
- 2 在“配置”下，单击 **SMTP**。
- 3 键入 SMTP 服务器地址和端口号。
- 4 如果 SMTP 服务器使用加密的连接，请选择加密协议。
- 5 在**发件人**文本框中，键入发送系统通知时要使用的电子邮件地址。
发件人地址会在系统通知电子邮件中显示为发件人地址。该地址无需是实际地址，可以是表示 vRealize Log Insight 特定实例的任何内容。例如，`loginsight@example.com`。
- 6 键入用户名和密码以在发送系统通知时使用 SMTP 服务器进行身份验证。
- 7 键入目标电子邮件，然后单击**发送测试电子邮件**以确认连接正常。
- 8 如果 SMTP 服务器提供了不受信任的 SSL 证书，则会显示一个对话框，其中显示有该证书的详细信息。单击**接受**将证书添加到 vRealize Log Insight 群集中所有节点的信任库。

如果单击**取消**，则不会将该证书添加到信任库，并且与 SMTP 服务器的连接将失败。您必须接受证书才能成功连接。

9 单击保存。

如果未测试连接，并且 SMTP 服务器提供的证书不受信任，请按照第 8 步中的说明进行操作。

配置 Webhook

您可以将 Webhook 配置为向远程 Web 服务器发送警示通知。Webhook 通过 HTTP POST/PUT 提供通知。

前提条件

验证是否已具有**编辑管理员**权限的用户身份登录到 vRealize Log Insight Web 用户界面。URL 格式为 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

- 1 导航到**管理**选项卡。
- 2 在“配置”下，单击 **Webhook**。
- 3 单击**新建 Webhook**。
- 4 在**名称**文本框中，输入 Webhook 的名称。
- 5 输入以下信息。

选项	描述
端点	选择要向其发送通知的端点，例如，Slack、Pager Duty 或自定义端点。根据所选的端点类型： <ul style="list-style-type: none"> ■ 用户界面提供其他输入选项。 ■ 用户界面使用预定义的模板填充 Webhook 负载，您可以根据需要自定义该模板。
Webhook URL	输入要将 Webhook 通知发布到的远程 Web 服务器的 URL。要验证该连接，请单击 测试警示 。 您可以输入以空格分隔的多个 Webhook URL。
集成密钥	如果选择 Pager Duty 端点，请输入 Webhook 请求的集成密钥。
高级设置	如果选择自定义端点，请输入其他信息，如内容类型、操作等。 内容类型 的默认值为 JSON， 操作 的默认值为 POST。您可以自定义这些选项，并在 自定义标头 下向请求添加其他标头。如果配置的远程 Web 服务器需要授权才能对 Webhook 通知执行 POST/PUT 操作，请在 授权用户 和 授权密码 文本框中输入用于进行服务器身份验证的用户名和密码。
Webhook 负载	此区域将根据您在 端点 下拉菜单中所做的选择自动进行填充。您可以自定义负载，即作为 POST/PUT Webhook 通知请求的一部分发送的正文模板。正文可采用 XML 或 JSON 格式。
参数	您可以使用参数列表构建 Webhook 负载。这些参数将在发送 Webhook 通知时替换为实际值。

6 单击保存。

安装自定义 SSL 证书

默认情况下，vRealize Log Insight 会在虚拟设备上安装自签名 SSL 证书。

当您连接到 vRealize Log Insight Web 用户界面时，自签名证书将生成安全警告。如果您不想使用自签名安全证书，可以安装自定义 SSL 证书。唯一需要自定义 SSL 证书的功能是通过 SSL 转发事件。如果您的集群设置已启用 ILB，请参见[启用集成负载均衡器](#)了解自定义 SSL 证书的特殊要求。

注 vRealize Log Insight Web 用户界面和 Log Insight Ingestion 协议 `cfapi` 使用相同的证书进行身份验证。

前提条件

- 验证您的自定义 SSL 证书是否符合以下要求。
 - CommonName 包含主节点的通配符或精确匹配或者虚拟 IP 地址的 FQDN。（可选）所有其他 IP 地址和 FQDN 均列为 `subjectAltName`。
 - 证书文件包含有效的私钥和证书链。
 - 私钥是通过 RSA 或 DSA 算法生成的。
 - 私钥未使用口令加密。
 - 如果该证书由一系列其他证书签名，则在要导入的证书文件中包括所有其他证书。
 - 证书文件中包括的私钥和所有证书都采用 PEM 编码。vRealize Log Insight 不支持采用 DER 编码的证书和私钥。
 - 证书文件中包括的私钥和所有证书都采用 PEM 格式。vRealize Log Insight 不支持采用 PFX、PKCS12、PKCS7 或其他格式的证书。
- 确认您将每个证书的整个正文按以下顺序连接到单个文本文件。
 - a 私钥 - `your_domain_name.key`
 - b 主要证书 - `your_domain_name.crt`
 - c 中间证书 - `DigiCertCA.crt`
 - d 根证书 - `TrustedRoot.crt`
- 确认您按以下格式包含每个证书的开头和结尾标记。

```
-----BEGIN PRIVATE KEY-----
(Your Private Key: your_domain_name.key)
-----END PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
(Your Primary SSL certificate: your_domain_name.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Intermediate certificate: DigiCertCA.crt)
```

```
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Root certificate: TrustedRoot.crt)
-----END CERTIFICATE-----
```

- 验证是否已以具有**编辑管理员**权限的用户身份登录到 vRealize Log Insight Web 用户界面。URL 格式为 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

1 生成自签名证书

您可以使用 OpenSSL 工具生成 Windows 或 Linux 自签名证书。

2 生成证书签名请求

可以使用适用于 Windows 的 OpenSSL 工具生成证书签名请求。

3 请求来自证书颁发机构的签名

向您选择的证书颁发机构发送证书签名请求，然后请求签名。

4 连接证书文件

将密钥和证书文件合并到 PEM 文件中。

5 上载已签名证书

可以上载已签名的 SSL 证书。

6 在 vRealize Log Insight 服务器和 Log Insight Agents 之间配置 SSL 连接

借助 SSL 功能，您可以通过摄取 API 安全流在 Log Insight Agents 和 vRealize Log Insight 服务器之间提供仅 SSL 连接。您还可以配置 Log Insight Agents 的各种 SSL 参数。

生成自签名证书

您可以使用 OpenSSL 工具生成 Windows 或 Linux 自签名证书。

前提条件

- 从以下位置下载相应的 OpenSSL 安装程序：<https://www.openssl.org/community/binaries.html>。使用下载的 OpenSSL 安装程序在 Windows 上进行安装。
- 编辑 `openssl.cnf` 文件来添加其他所需参数。确保 `[req]` 部分的 `req_extensions` 参数已定义。

```
[req]
.
.
req_extensions=v3_req #
```

- 为服务器的主机名或 IP 地址添加相应的使用者备用名称条目，例如 *server-01.loginsight.domain*。无法为主机名指定模式。

```
[v3_req]
.
.
subjectAltName=DNS:server-01.loginsight.domain
#subjectAltName=IP:10.27.74.215
```

步骤

- 1 创建文件夹以保存您的证书文件，例如 C:\Certs\LogInsight。
- 2 打开命令提示符并运行以下命令。

```
C:\Certs\LogInsight>openssl req -x509 -nodes -newkey 2048 -keyout server.key -out
server.crt -days 3650
```

OpenSSL 提示您提供证书属性，包括国家/地区、组织等。

- 3 输入 vRealize Log Insight 服务器的准确 IP 地址或主机名，或如果启用了负载平衡，请输入 vRealize Log Insight 群集地址。

此属性是唯一一个必须指定值的属性。

结果

创建了两个文件：server.key 和 server.crt。

- server.key 是新的 PEM 编码私钥。
- server.crt 是 server.key 签名的新 PEM 编码证书。

生成证书签名请求

可以使用适用于 Windows 的 OpenSSL 工具生成证书签名请求。

前提条件

- 安装 OpenSSL 工具。有关获取 OpenSSL 工具的信息，请参见 <http://www.openssl.org>。
- 编辑 openssl.cfg 文件来添加其他所需参数。确保 [req] 部分的 req_extensions 参数已定义。

```
[req]
.
.
req_extensions=v3_req #
```

- 为服务器的主机名或 IP 地址添加相应的使用者备用名称条目，例如 *server-01.loginsight.domain*。无法为主机名指定模式。

```
[v3_req]
.
.
subjectAltName=DNS:server-01.loginsight.domain
#subjectAltName=IP:10.27.74.215
```

步骤

- 1 创建文件夹以保存您的证书文件，例如 C:\Certs\LogInsight。

- 2 打开命令提示符，然后运行以下命令以生成私钥。

```
C:\Certs\LogInsight>openssl genrsa -out server.key 2048
```

- 3 通过运行以下命令生成证书签名请求。

```
C:\Certs\LogInsight>openssl req -new -key server.key -out server.csr
```

注 此命令以交互方式运行，并且会向您询问一些问题。您的证书颁发机构将交叉检查您的答案。您的答案必须与公司注册的相关法律文档相符。

- 4 按照屏幕上的说明进行操作，然后输入将合并到您的证书请求中的信息。

重要事项 在“公用名称”字段中，输入服务器的主机名或 IP 地址，例如 **mail.your.domain**。如果要包括所有子域，请输入 ***your.domain**。

结果

您的证书签名请求文件 `server.csr` 已生成和保存。

请求来自证书颁发机构的签名

向您选择的证书颁发机构发送证书签名请求，然后请求签名。

步骤

- ◆ 将 `server.csr` 文件提交到证书颁发机构。

注 请求证书颁发机构采用 PEM 格式对您的文件进行编码。

证书颁发机构会处理您的请求，然后将采用 PEM 格式编码的 `server.crt` 文件发送回给您。

连接证书文件

将密钥和证书文件合并到 PEM 文件中。

步骤

- 1 创建新的 `server.pem` 文件，然后在文本编辑器中打开该文件。

- 2 复制 `server.key` 文件的内容，然后将其粘贴在 `server.pem` 中，使用以下格式。

```
-----BEGIN RSA PRIVATE KEY-----
(Your Private Key: server.key)
-----END RSA PRIVATE KEY-----
```

- 3 复制从证书颁发机构收到的 `server.crt` 文件内容，然后使用以下格式将其粘贴在 `server.pem` 中。

```
-----BEGIN CERTIFICATE-----
(Your Primary SSL certificate: server.crt)
-----END CERTIFICATE-----
```

- 4 如果证书颁发机构为您提供中间证书或链接证书，请将这些中间证书或链接证书附加到公共证书文件的末尾，使用以下格式。

```
-----BEGIN RSA PRIVATE KEY-----
(Your Private Key: server.key)
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
(Your Primary SSL certificate: server.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Intermediate certificate: DigiCertCA.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Root certificate: TrustedRoot.crt)
-----END CERTIFICATE-----
```

- 5 保存 `server.pem` 文件。

上载已签名证书

可以上载已签名的 SSL 证书。

步骤

- 1 导航到**管理**选项卡。
- 2 在“配置”下，单击 **SSL 证书**。
- 3 浏览到您的自定义 SSL 证书，然后单击**打开**。
- 4 单击**保存**。
- 5 重新启动 vRealize Log Insight。

后续步骤

在 vRealize Log Insight 重新启动后，确认 ESXi 中的 syslog 源继续到达 vRealize Log Insight。

在 vRealize Log Insight 服务器和 Log Insight Agents 之间配置 SSL 连接

借助 SSL 功能，您可以通过摄取 API 安全流在 Log Insight Agents 和 vRealize Log Insight 服务器之间提供仅 SSL 连接。您还可以配置 Log Insight Agents 的各种 SSL 参数。

vRealize Log Insight 代理通过 TLSv.1.2 进行通信。为了符合安全准则，已禁用 SSLv.3/TLSv.1.0。

主要 SSL 功能

了解主要 SSL 功能可以帮助您正确配置 Log Insight Agents。

vRealize Log Insight 代理会存储证书，并在每次连接到特定服务器时使用这些证书验证服务器身份（首次连接除外）。如果无法确认服务器身份，vRealize Log Insight 代理会拒绝与服务器连接，并将相应错误消息写入日志。代理收到的证书存储在 cert 文件夹中。

- 对于 Windows，请转至 C:\ProgramData\VMware\Log Insight Agent\cert。
- 对于 Linux，请转至 /var/lib/loginsight-agent/cert。

当 vRealize Log Insight 代理与 vRealize Log Insight 服务器建立安全连接时，代理会检查从 vRealize Log Insight 服务器接收的证书的有效性。vRealize Log Insight 代理使用系统信任的根证书。

- Log Insight Linux Agent 从 /etc/pki/tls/certs/ca-bundle.crt 或 /etc/ssl/certs/ca-certificates.crt 加载信任的证书。
- Log Insight Windows Agent 使用系统根证书。

如果 vRealize Log Insight 代理已在本地存储自签名证书，但仍接收到带有相同公共密钥的其他有效自签名证书，则代理会接受新证书。如果重新生成的自签名证书使用相同的专用密钥，但具有不同的详细信息（如新的到期日期），则可以成功连接。否则，会拒绝连接。

如果 vRealize Log Insight 代理已在本地存储自签名证书，但仍接收到有效的 CA 签名证书，则 vRealize Log Insight 代理会无声替换新接受的证书。

如果 vRealize Log Insight 代理在拥有 CA 签名证书后接收到自签名证书，则 Log Insight 代理会拒绝接收。仅在首次连接 vRealize Log Insight 服务器时，vRealize Log Insight 代理才会接受来自该服务器的自签名证书。

如果 vRealize Log Insight 代理已在本地存储 CA 签名证书，但仍接收到由其他信任 CA 签名的有效证书，则代理会拒绝接收。您可以修改 vRealize Log Insight 代理的配置选项以接受新证书。请参见[配置 vRealize Log Insight 代理的 SSL 参数](#)。

vRealize Log Insight 代理通过 TLSv.1.2 进行通信。为了符合安全准则，已禁用 SSLv.3/TLSv.1.0。

强制使用仅 SSL 连接

您可以使用 vRealize Log Insight Web 用户界面将 vRealize Log Insight Agents 和数据获取 API 配置为仅允许通过 SSL 连接至服务器。

通常，可以通过 HTTP 在端口 9000 上以及通过 HTTPS 在端口 9543 上访问 vRealize Log Insight API。vRealize Log Insight 代理或自定义 API 客户端可以使用这两个端口。所有经过身份验证的请求都需要使用 SSL，但未经身份验证的请求（包括 vRealize Log Insight 代理载入流量）可以使用这两种方法来执行。您可以强制所有 API 请求使用 SSL 连接。该选项不限制 syslog 端口 514 流量，也不影响 vRealize Log Insight 用户界面，HTTP 端口 80 请求会继续重定向到 HTTPS 端口 443。

前提条件

验证是否已具有**编辑管理员**权限的用户身份登录到 vRealize Log Insight Web 用户界面。URL 格式为 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

- 1 导航到**管理**选项卡。
- 2 在“配置”下，单击 **SSL**。
- 3 在“API 服务器 SSL”下，选择**需要 SSL 连接**。
- 4 单击**保存**。

结果

vRealize Log Insight API 仅允许通过 SSL 连接至服务器。拒绝非 SSL 连接。

配置 vRealize Log Insight 代理的 SSL 参数

可以编辑 vRealize Log Insight 代理配置文件以更改 SSL 配置，添加可信根证书的路径以及确定该代理是否接受证书。

对 vRealize Log Insight Windows 和 Linux 代理应用此步骤。

前提条件

对于 vRealize Log Insight Linux 代理：

- 以 **root** 用户身份登录，或使用 `sudo` 运行控制台命令。
- 登录到已安装 vRealize Log InsightLinux 代理的 Linux 计算机，打开控制台，然后运行 `pgrep liagent` 以验证 vRealize Log Insight Linux 代理是否已安装且正在运行。

对于 vRealize Log Insight Windows 代理：

- 登录到已安装 vRealize Log InsightWindows 代理的 Windows 计算机，启动“服务”管理器以验证是否已安装 vRealize Log Insight 代理服务。

步骤

- 1 导航到包含 `liagent.ini` 文件的文件夹。

操作系统	路径
Linux	<code>/var/lib/loginsight-agent/</code>
Windows	<code>%ProgramData%\VMware\Log Insight Agent</code>

- 2 在任意文本编辑器中打开 `liagent.ini` 文件。
- 3 将以下键添加到 `liagent.ini` 文件的 `[server]` 部分。

键	描述
<code>ssl_ca_path</code>	<p>覆盖根证书颁发机构签名证书的默认存储路径，这些证书用于验证连接对等证书。</p> <p>为 <code>ssl_ca_path</code> 提供路径时，您将覆盖 Linux 和 Windows 代理的默认值。您可以使用其中连接了多个 PEM 格式的证书的文件，或者其中包含 PEM 格式的证书且证书名称采用 <code>hash.0</code> 形式的目录。（请参见 <code>x509</code> 实用程序的 <code>-hash</code> 选项。）</p> <p>Linux: 如果未指定任何值，代理将使用分配给 <code>LI_AGENT_SSL_CA_PATH</code> 环境变量的值。如果该值不存在，代理将尝试从 <code>/etc/pki/tls/certs/ca-bundle.crt</code> 文件或 <code>/etc/ssl/certs/ca-certificates.crt</code> 文件中加载受信任证书。</p> <p>Windows: 如果未指定任何值，代理将使用由 <code>LI_AGENT_SSL_CA_PATH</code> 环境变量指定的值。如果该值不存在，vRealize Log Insight Windows 代理将从 Windows 根证书存储中加载证书。</p>
<code>ssl_accept_any</code>	<p>定义 vRealize Log Insight 代理是否接受任何证书。可能的值为 <code>yes</code>、<code>1</code>、<code>no</code> 或 <code>0</code>。当值设置为 <code>yes</code> 或 <code>1</code> 时，代理将接受来自服务器的任何证书，并建立安全连接以发送数据。默认值为 <code>no</code>。</p>
<code>ssl_accept_any_trusted</code>	<p>可能的值为 <code>yes</code>、<code>1</code>、<code>no</code> 或 <code>0</code>。如果 vRealize Log Insight 代理已在本地存储由受信任证书颁发机构签名的证书，但仍接收到由其他受信任证书颁发机构签名的其他有效证书。如果值设置为 <code>yes</code> 或 <code>1</code>，则代理将接受新的有效证书。如果值设置为 <code>no</code> 或 <code>0</code>，则将拒绝证书并结束连接。默认值为 <code>no</code>。</p>
<code>ssl_cn</code>	<p>自签名证书的 Common Name。</p> <p>默认值为 VMware vCenter Log Insight。您可以将自定义 Common Name 定义为根据证书 Common Name 字段进行检查。</p> <p>vRealize Log Insight 代理会将接收到的证书的 Common Name 字段与 <code>[server]</code> 部分中的 <code>hostname</code> 键指定的主机名进行比较。如果它们不匹配，代理将根据 <code>liagent.ini</code> 文件中的 <code>ssl_cn</code> 键来检查 Common Name 文本框。如果值匹配，vRealize Log Insight 代理将接受证书。</p>

注 如果禁用 SSL，则会忽略这些键。

4 保存并关闭 `liagent.ini` 文件。

示例：配置

以下是 SSL 配置示例。

```
proto=cfapi
port=9543
ssl=yes
ssl_ca_path=/etc/pki/tls/certs/ca-bundle.crt
ssl_accept_any=no
ssl_accept_any_trusted=yes
ssl_cn=LOGINSIGHT
```

查看和移除 SSL 证书

您可以查看已接受的 SSL 证书，并将其添加到 vRealize Log Insight 群集中所有节点的信任库中。您也可以移除不再需要的证书。

前提条件

验证是否已以具有**编辑管理员**权限的用户身份登录到 vRealize Log Insight Web 用户界面。URL 格式为 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

- 1 导航到**管理**选项卡。
- 2 在“管理”下，选择**证书**。
- 3 执行以下操作之一：
 - 要查看有关证书的信息，请单击证书指纹右侧的信息图标。
 - 要移除证书，请选择证书，然后单击**删除**。或者，您可以单击每个证书指纹右侧的删除图标。

提示 可以使用提供的选项对证书进行排序和筛选。

更改 vRealize Log Insight Web 会话的默认超时期限。

默认情况下，为保证环境的安全，vRealize Log Insight Web 会话会在 30 分钟后过期。可以增加或减少超时持续时间。

注 更改超时期限仅适用于新创建的会话。

前提条件

验证是否已以具有**编辑管理员**权限的用户身份登录到 vRealize Log Insight Web 用户界面。URL 格式为 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

- 1 导航到**管理**选项卡。
- 2 在“配置”下，单击**常规**。
- 3 在“浏览器会话”窗格中，以分钟为单位指定超时值。
值 -1 会禁用会话超时。
- 4 单击**保存**。

保留和存档

您可以通过为不同类型的日志定义不同的保留期限，在数据分区中保留日志数据。例如，可以为包含敏感信息的日志定义较短的保留期限。您还可以将分区中的日志数据进行存档以延长保留时间。如果为数据分区启用存档，分区中的数据会在保留期限过后移动到 NFS 挂载。

配置数据分区

您可以将日志数据保留在设置有筛选器和保留期限的分区中。通过数据分区，您可以为不同类型的日志定义不同的保留期限。例如，包含敏感信息的日志可能需要较短的保留期限，如 5 天。您还可以将数据分区中的数据存档到 NFS 挂载，以长时间保留日志。

与某个数据分区的筛选标准相匹配的日志数据会在该分区中存储指定的保留期限。如果启用存档，数据会在保留期限过后移动到 NFS 存储。与任何定义的数据分区中的筛选标准均不匹配的日志会存储在默认分区中。此分区始终处于启用状态，并且会无期限地存储数据。您可以为默认分区修改保留期限和启用存档。

注 最多可创建五个数据分区。

前提条件

- 如果要为数据分区启用存档，请确认您有权访问符合以下要求的 NFS 分区。
 - NFS 分区必须允许客户机帐户的读取和写入操作。
 - 挂载不得要求身份验证。
 - NFS 服务器必须支持 NFS v3 或 v4。
 - 如果使用 Windows NFS 服务器，请允许未映射用户 UNIX 访问（通过 UID/GID）。
 有关存档的详细信息，请参见[数据存档](#)。
- 验证是否已以具有**编辑管理员**权限的用户身份登录到 vRealize Log Insight Web 用户界面。URL 格式为 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

- 1 导航到**管理**选项卡。
- 2 在“管理”下，单击**日志管理**，然后单击**索引分区**。

- 3 要查看默认分区的详细信息（如保留期限和存档位置），请单击名为**默认分区**的分区对应的编辑图标。要修改分区的详细信息，请单击编辑图标，然后按照步骤 7 至 9 进行操作。
- 4 要创建分区，请单击**新建分区**，然后按照步骤 5 至 9 进行操作。
- 5 在**分区名称**文本框中，输入数据分区的名称。
- 6 添加一个或多个筛选器以细化要存储在该数据分区中的日志。（可选）单击在**交互式分析中运行**，以预览筛选的日志结果。
- 7 在**保留期**文本框中，输入希望在该数据分区中保留日志的天数。如果希望无限期保留，请输入 0。
- 8 单击**存档位置**切换按钮以对分区中的日志数据进行存档。在文本框中，以 `nfs://servername<:port-number>/exportname` 格式输入要存储已存档数据的 NFS 位置。端口号默认为 2049。
单击**测试**以验证与 NFS 存储的连接。
- 9 单击**保存**。

注

- 数据分区在默认情况下处于启用状态。要禁用数据分区，请使用**索引分区**选项卡上该分区对应的切换按钮。
- 创建、修改和删除数据分区要求您在所有集群节点上重新启动 vRealize Log Insight。

在 vRealize Log Insight 重新启动后，确认 ESXi 中的 syslog 源继续到达 vRealize Log Insight。

结果

数据分区列在**索引分区**选项卡中，该选项卡包含有关分区是否已启用、筛选标准、保留期限、已用存储以及第一条日志载入时间的信息。您可以通过单击分区名称旁边的编辑图标来查看或修改分区详细信息。

数据存档

数据存档可保留可能会在保留期限过后从数据分区中移除的旧日志。vRealize Log Insight 可以将已存档的数据存储到 NFS 挂载。

注

- 数据存档发生在日志载入期间，如《vRealize Log Insight 入门》中的[事件生命周期的主要方面](#)中所述。
 - vRealize Log Insight 不会管理用于存档目的的 NFS 挂载。如果已启用系统通知，则 vRealize Log Insight 会在 NFS 挂载即将用尽空间或不可用时发送电子邮件。
 - 已存档的日志事件无法再进行搜索。如果要搜索已存档的日志，必须将其导入到 vRealize Log Insight 实例中。有关导入已存档的日志文件的信息，请参见[将 vRealize Log Insight 存档导入到 vRealize Log Insight 中](#)。
 - 请勿永久挂载 NFS 或更改 `/etc/fstab` 文件。vRealize Log Insight 会自行为您执行 NFS 挂载。
-

有关在数据分区中启用存档的信息，请参见[配置数据分区](#)。

vRealize Log Insight 存档文件的格式

vRealize Log Insight 以特定的格式存档数据。

vRealize Log Insight 将存档文件存储在 NFS 服务器上，并根据存档时间将其在分层目录中进行组织。例如，

```
/backup/2014/08/07/16/bd234b2d-df98-44ae-991a-e0562f10a49/data.blob
```

其中，/backup 是 NFS 位置，2014/08/07/16 是存档时间，bd234b2d-df98-44ae-991a-e0562f10a49 是存储日志文件的段 ID，而 data.blob 是段的已存档数据。

已存档数据 data.blob 是使用 vRealize Log Insight 内部编码的压缩文件。它包含段中存储的所有消息的原始内容以及时间戳、主机名、源和应用程序名称等静态字段。

可以将已存档数据导入到 vRealize Log Insight，将存档数据导出到原始文本文件，并从存档数据提取消息内容。请参见[将 Log Insight 存档导出为原始文本文件或 JSON](#)和[将 vRealize Log Insight 存档导入到 vRealize Log Insight 中](#)。

将 vRealize Log Insight 存档导入到 vRealize Log Insight 中

数据存档可保留可能会在保留期限过后从数据分区中移除的旧日志。请参见[数据存档](#)。可以使用命令行导入 vRealize Log Insight 中已存档的日志。

注 虽然 vRealize Log Insight 可以同时处理历史数据和实时数据，但还是建议您部署 vRealize Log Insight 的单独实例以处理导入的日志文件。

前提条件

- 验证是否拥有可登录 vRealize Log Insight 虚拟设备的 root 用户凭据。
- 确认您可以访问已在其中存档 vRealize Log Insight 日志的 NFS 服务器。
- 确认 vRealize Log Insight 虚拟设备具有足够磁盘空间来容纳已导入的日志文件。

虚拟设备上 /storage/core 分区中的最小可用空间必须是要导入的存档日志的约 10 倍。

步骤

- 1 与 vRealize Log Insight vApp 建立 SSH 连接，然后以 root 用户身份登录。
- 2 将共享文件夹挂载在存档数据所在的 NFS 服务器上。

3 要导入已存档的 vRealize Log Insight 日志的目录，请运行以下命令。

```
/usr/lib/loginsight/application/bin/loginsight repository import Path-To-Archived-Log-Data-Folder.
```

注

- 为避免修改要导入目录的时间戳，请确保从要导入的目录以外的目录中执行此命令。从要导入的目录中运行该命令会创建 `JavaClient.log` 文件并更新该目录的修改时间戳。
- 导入存档数据的过程可能需要很长时间，具体取决于所导入的文件夹的大小。

4 关闭 SSH 连接。

后续步骤

您可以搜索、筛选和分析已导入的日志事件。

将 Log Insight 存档导出为原始文本文件或 JSON

可以使用命令行将 vRealize Log Insight 存档导出为常规原始文本文件或 JSON 格式。

注 这是一个高级过程。在没有向后兼容性的更高版本的 vRealize Log Insight 中，命令语法和输出格式可能会发生更改。

前提条件

- 验证是否拥有可登录 vRealize Log Insight 虚拟设备的 root 用户凭据。
- 确认 vRealize Log Insight 虚拟设备具有足够磁盘空间来容纳所导出的文件。

步骤

- 1 与 vRealize Log Insight vApp 建立 SSH 连接，然后以 root 用户身份登录。
- 2 在 vRealize Log Insight vApp 上创建存档目录。

```
mkdir /archive
```

- 3 通过运行以下命令，将共享文件夹挂载到存档数据所在的 NFS 服务器上。

```
mount -t nfs
archive-fileshare:archive directory path /archive
```

- 4 检查 vRealize Log Insight vApp 上的可用存储空间。

```
df -h
```

- 5 将 vRealize Log Insight 存档导出为原始文本文件。

```
/usr/lib/loginsight/application/sbin/repo-exporter -d archive-file-directory
output-file
```

例如，

```
/usr/lib/loginsight/application/sbin/repo-exporter -d /archive/2014/08/07/16/bd234b2d-
df98-44ae-991a-e0562f10a49 /tmp/output.txt
```

- 6 将 vRealize Log Insight 存档消息内容导出为 JSON 格式。

```
/usr/lib/loginsight/application/sbin/repo-exporter -F -d archive-file-directory output-
file.
```

例如，

```
/usr/lib/loginsight/application/sbin/repo-exporter -F -d /archive/2014/08/07/16/bd234b2d-
df98-44ae-991a-e0562f10a49 /tmp/output.json
```

- 7 关闭 SSH 连接。

重新启动 vRealize Log Insight 服务

通过使用 Web 用户界面中的“管理”页面，可以重新启动 vRealize Log Insight。

小心 重新启动 vRealize Log Insight 将关闭所有活动的用户会话。将强制 vRealize Log Insight 实例的用户重新登录。

前提条件

验证是否已以具有**编辑管理员**权限的用户身份登录到 vRealize Log Insight Web 用户界面。URL 格式为 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

- 1 导航到**管理**选项卡。
- 2 在“管理”下，单击**集群**。
- 3 选择集群节点。
- 4 单击**重新启动主节点**，然后单击**重新启动**。

后续步骤

在 vRealize Log Insight 重新启动后，确认 ESXi 中的 syslog 源继续到达 vRealize Log Insight。

关闭 vRealize Log Insight 虚拟设备的电源

要避免在关闭 vRealize Log Insight 主节点或工作线程节点的电源时丢失数据，必须严格按照相应步骤顺序操作来关闭节点电源。

必须先关闭 vRealize Log Insight 虚拟设备的电源，然后再对该设备的虚拟硬件进行修改。

您可以使用 vSphere Client 中的**电源 > 关闭客户机**菜单选项来关闭 vRealize Log Insight 虚拟设备的电源。此外，还可以使用虚拟设备控制台，或者建立与 vRealize Log Insight 虚拟设备的 SSH 连接并运行相应命令。

前提条件

- 如果计划使用 SSH 连接到 vRealize Log Insight 虚拟设备，请验证 TCP 端口 22 是否已打开。
- 验证是否拥有可登录 vRealize Log Insight 虚拟设备的 root 用户凭据。

步骤

- 1 与 vRealize Log Insight vApp 建立 SSH 连接，然后以 root 用户身份登录。
- 2 要关闭 vRealize Log Insight 虚拟设备的电源，请运行 `shutdown -h now`。

后续步骤

可以安全地修改 vRealize Log Insight 虚拟设备的虚拟硬件。

下载 vRealize Log Insight 支持包

如果 vRealize Log Insight 由于出现问题未按预期运行，可以将日志和配置文件的副本以支持包的格式发送到 VMware 支持服务部门。

仅当 VMware 支持服务部门要求时，才有必要下载群集范围的支持包。您可以通过静态方式（占用节点上的磁盘空间）或流式（不占用节点上的磁盘空间，默认情况下会将包存储在您的启动计算机上）创建包。

支持包的存储位置取决于用于获取支持包的选项：

选项	支持包位置
API - POST appliance/vm-support-bundle	这是一个不包含本地文件的流式版本。
API - POST appliance/support-bundle	/tmp/ui-support/
Web 用户界面 - 静态支持包	/tmp/ui-support/
Web 用户界面 - 流式支持包	这是一个不包含本地文件的流式版本。
命令行 - scripts/loginsight-support	包将在当前目录中生成。

前提条件

验证是否已具有**编辑管理员**权限的用户身份登录到 vRealize Log Insight Web 用户界面。URL 格式为 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

- 1 导航到**管理**选项卡。
- 2 在“管理”下，单击**群集**。
- 3 在“支持”标题下，单击**下载支持包**。

vRealize Log Insight 系统会收集诊断信息，并以压缩 tarball 的形式将数据发送到您的浏览器。

- 4 选择创建包的方法。
 - 选择**静态支持包**可在本地创建包。创建包时，会占用节点上的磁盘空间。
 - 选择**流式支持包**可立即开始流式传输支持包。此方法不会占用节点上的磁盘空间。
- 5 单击**继续**。
- 6 在“文件下载”对话框中，单击**保存**。
- 7 选择要保存 tarball 存档的位置，然后单击**保存**。

后续步骤

您可以查看日志文件的内容，以检查是否存在错误消息。解决或关闭问题后，请删除过期的支持包，以节省磁盘空间。

加入或退出 VMware 客户体验改善计划

您可以在部署 vRealize Log Insight 后加入或退出 VMware 客户体验改善计划。

在安装 vRealize Log Insight 时，您可以选择是否参与客户体验改善计划。安装之后，您可以按照以下步骤加入或退出该计划。

前提条件

验证是否已具有**编辑管理员**权限的用户身份登录到 vRealize Log Insight Web 用户界面。URL 格式为 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

- 1 导航到**管理**选项卡。
- 2 在“配置”下，单击**常规**。
- 3 在“客户体验改善计划”窗格中，选中或清除**加入 VMware 客户体验改善计划**复选框。

选定后，该选项将激活该计划并向 `https://vmware.com` 发送数据。

4 单击保存。

为 vRealize Log Insight 配置 STIG 合规性

为提高安全性，您可以配置 vRealize Log Insight 以确保 STIG（安全技术实施指南）合规性。此配置包括 DoD（美国国防部）同意协议和其他密码策略限制。

启用 STIG 合规性后，vRealize Log Insight 会在以下情况下发送系统通知：

- 创建新用户或者 Active Directory 或 VMware Identity Manager 用户首次登录。
- 分配的日志记录存储卷达到了存储库最大日志记录存储容量的 75%。此通知按节点发送。

有关详细信息，请参见 [vRealize Log Insight 系统通知](#)。

前提条件

验证是否已具有 **编辑管理员** 权限的用户身份登录到 vRealize Log Insight Web 用户界面。URL 格式为 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

- 1 导航到 **管理** 选项卡。
- 2 在“配置”下，单击 **常规**。
- 3 在“安全技术实施指南”窗格中，执行相关操作：
 - 单击 **DoD 同意协议** 切换按钮，以便在用户登录 vRealize Log Insight 时显示强制性 DoD 同意协议。选择登录消息类型 - 在登录页面上显示一则简单的消息；在登录页面上包含一个复选框，登录前需选中该复选框以接受同意；或者显示一个同意对话框，该对话框中包含用于接受 DoD 同意协议的按钮。添加同意协议标题和描述。

启用 DoD 同意协议后，用户在登录时将可以看到其所选登录消息类型。

- 单击 **密码策略限制** 切换按钮，对用户帐户启用进一步的密码限制以及锁定帐户的其他规则。

如果启用了密码策略限制，会将以下额外规则应用于密码：

- 密码必须包含至少 15 个字符。
- 用户每 24 小时只能更改一次密码。
- 用户更改密码时，无法使用最近五次用过的密码。
- 用户更改密码时，新密码必须至少有八个字符与旧密码不同。

如果启用了密码策略限制，则在以下情况下将锁定用户帐户：

- 用户已有 35 天未登录到 vRealize Log Insight。
- 用户已有 60 天未更改密码。

注 超级管理员用户帐户永远不会被锁定。

4 单击保存。

为 vRealize Log Insight 激活 FIPS

为提高安全性，您可以配置 vRealize Log Insight 以确保 FIPS（联邦信息处理标准）合规性。这套标准描述了美国非军事政府机构以及与这些机构合作的美国政府承包商和供应商所采用的文档处理、加密算法和其他信息技术标准。激活 FIPS 后，vRealize Log Insight 会将 FIPS 140-2 标准与安全级别 1 结合使用，后者指定了用于保护敏感或重要数据的基本安全要求。

有关各个 VMware 产品对 FIPS 140-2 支持情况的信息，请参见 <https://www.vmware.com/security/certifications/fips.html>。

vRealize Log Insight 使用 Apache Thrift 进行节点间通信。激活 FIPS 时会自动启用通过 SSL 的 Thrift，这将使节点间通信更加安全。但是，在没有激活 FIPS 的情况下，也可以启用通过 SSL 的 Thrift。有关详细信息，请参见 <https://kb.vmware.com/s/article/82299>。

前提条件

验证是否已以具有**编辑管理员**权限的用户身份登录到 vRealize Log Insight Web 用户界面。URL 格式为 <https://log-insight-host>，其中 *log-insight-host* 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

- 1 导航到**管理**选项卡。
- 2 在“配置”下，单击**常规**。
- 3 在“FIPS 模式”窗格中，单击**激活 FIPS 模式**切换按钮以激活 FIPS。

小心 激活 FIPS 后，无法再将其停用。

4 单击保存。

结果

保存 FIPS 配置时，会重新引导所有节点。您必须等待几分钟才能再次使用 vRealize Log Insight。

管理 vRealize Log Insight 群集

5

您可以添加、移除和升级 vRealize Log Insight 群集的节点。

注 vRealize Log Insight 不支持 WAN 群集。当前版本的 vRealize Log Insight 不支持 WAN 群集（也称为地理群集、高可用性群集或远程群集）。群集中的所有节点都应该部署在同一个第 2 层 LAN 内。另外，[端口和外部接口](#)中所述的端口必须在节点之间打开才能正常通信。

本章讨论了以下主题：

- [向 vRealize Log Insight 集群添加工作线程节点](#)
- [从 vRealize Log Insight 群集中移除工作线程节点](#)
- [使用集成负载均衡器](#)
- [查询生产中群集检查的结果](#)

向 vRealize Log Insight 集群添加工作线程节点

部署 Log Insight 虚拟设备的新实例，然后将其添加到现有的 Log Insight 主节点中。

步骤

1 部署 vRealize Log Insight 虚拟设备

下载 vRealize Log Insight 虚拟设备。VMware 将 vRealize Log Insight 虚拟设备作为 .ova 文件进行分发。使用 vSphere Client 部署 vRealize Log Insight 虚拟设备。

2 加入现有部署

在部署和设置独立 vRealize Log Insight 节点后，可以部署新的 vRealize Log Insight 实例，然后将其添加到现有节点以形成 vRealize Log Insight 集群。

部署 vRealize Log Insight 虚拟设备

下载 vRealize Log Insight 虚拟设备。VMware 将 vRealize Log Insight 虚拟设备作为 .ova 文件进行分发。使用 vSphere Client 部署 vRealize Log Insight 虚拟设备。

前提条件

- 验证您是否拥有 vRealize Log Insight 虚拟设备 .ova 文件的副本。
- 验证您是否有权将 OVF 模板部署至清单。

- 验证您的环境是否拥有足够资源来满足 vRealize Log Insight 虚拟设备的最低要求。请参见[最低要求](#)。
- 确保已阅读并了解虚拟设备大小调整建议。请参见[调整 Log Insight 虚拟设备的大小](#)。

步骤

- 1 在 vSphere Client 中，选择文件 > 部署 OVF 模板。
- 2 按照部署 OVF 模板向导中的提示进行操作。
- 3 在“选择配置”页面上，根据要收集日志的环境的大小选择 vRealize Log Insight 虚拟设备的大小。

小型是生产环境的最低要求。

vRealize Log Insight 提供了预设虚拟机大小，您可以从中选择满足您环境载入要求的相应大小。这些预设是经过认证的计算和磁盘资源大小组合，但您可以在以后添加额外的资源。小型配置消耗最少的资源，同时保持受支持状态。超小型配置仅适用于演示目的。

预设大小	日志载入速率	虚拟 CPU	内存	IOPS	syslog 连接（活动的 TCP 连接）	每秒事件数
超小型	6 GB/天	2	4GB	75	20	400
小型	30 GB/天	4	8 GB	500	100	2000
中型	75 GB/天	8	16 GB	1000	250	5000
大型	225 GB/天	16	32GB	1500	750	15,000

可以使用 syslog 聚合器增加向 vRealize Log Insight 发送事件的 syslog 连接数。但是，每秒的最大事件数是固定的，并不取决于是否使用 syslog 聚合器。vRealize Log Insight 实例无法用作 syslog 聚合器。

注 如果选择**大型**，必须在部署后升级 vRealize Log Insight 虚拟机上的虚拟硬件。

- 4 在“选择存储”页面上，选择磁盘格式。
 - **厚置备延迟置零**以默认的厚格式创建虚拟磁盘。创建虚拟磁盘时分配虚拟磁盘所需的空間。创建时不会擦除物理设备上保留的数据，但是以后首次从虚拟设备写入时会按需要将其置零。
 - **厚置备置零**创建一种厚虚拟磁盘类型，可支持 Fault Tolerance 等群集功能。在创建时为虚拟磁盘分配所需的空間。与平面格式相反，创建虚拟磁盘时，会将物理设备上保留的数据置零。创建这种格式的磁盘所需的时间可能会比创建其他类型的磁盘长。

重要事项 尽可能使用厚置备置零磁盘部署 vRealize Log Insight 虚拟设备，以获得更佳性能以及保证虚拟设备的运行。

- **精简置备**创建精简格式的磁盘。磁盘会随其上保存的数据量增加而扩展。如果存储设备不支持厚置备磁盘或您希望节省 vRealize Log Insight 虚拟设备上的未使用磁盘空间，请使用精简置备磁盘部署虚拟设备。

注 不支持压缩 vRealize Log Insight 虚拟设备上的磁盘，并且该操作可能导致数据损坏或数据丢失。

- 5 （可选）在“选择网络”页面上，设置 vRealize Log Insight 虚拟设备的网络连接参数。您可以选择 IPv4 或 IPv6 协议。

如果不提供网络设置，如 IP 地址、DNS 服务器和网关信息，vRealize Log Insight 会使用 DHCP 设置这些设置。

小心 请勿指定超过两个域名服务器。如果指定超过两个域名服务器，将会忽略 vRealize Log Insight 虚拟设备中的所有已配置域名服务器。

使用以逗号分隔的列表指定域名服务器。

- 6 （可选）如果使用的不是 DHCP，则在“自定义模板”页面上设置网络属性。

如果要在双堆栈网络中运行虚拟机，请在“应用程序”下选中**优先使用 IPv6 地址**复选框。

小心 如果尽管您的网络支持 IPv6 但您仍希望使用纯 IPv4，那么请不要选中**优先使用 IPv6 地址**复选框。仅当您的网络支持双堆栈或纯堆栈 IPv6 时，才选中该复选框。

- 7 （可选）在“自定义模板”页面上，选择**其他属性**，然后为 vRealize Log Insight 虚拟设备设置根密码。

SSH 需要根密码。您还可以通过 VMware Remote Console 设置此密码。

- 8 按照提示完成部署。

有关部署虚拟设备的信息，请参见《部署 vApp 和虚拟设备用户指南》。

在打开虚拟设备电源后，将开始初始化进程。初始化进程需要几分钟时间完成。在进程结束时，将重新启动虚拟设备。

- 9 导航到**控制台**选项卡，然后验证 vRealize Log Insight 虚拟设备的 IP 地址。

IP 地址前缀	描述
https://	虚拟设备上的 DHCP 配置正确。
http://	虚拟设备上的 DHCP 配置失败。 a 关闭 vRealize Log Insight 虚拟设备的电源。 b 右键单击虚拟设备，然后选择 编辑设置 。 c 为虚拟设备设置静态 IP 地址。

后续步骤

- 如果要配置独立的 vRealize Log Insight 部署，请参见[配置新的 Log Insight 部署](#)。

vRealize Log InsightWeb 界面的网址为 `https://log-insight-host/`，其中 `log-insight-host` 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

加入现有部署

在部署和设置独立 vRealize Log Insight 节点后，可以部署新的 vRealize Log Insight 实例，然后将其添加到现有节点以形成 vRealize Log Insight 集群。

vRealize Log Insight 可以通过在集群中使用多个虚拟设备实例来进行扩展。集群能够实现载入吞吐量的线性扩展、提高查询性能，并实现高可用性载入。在集群模式下，vRealize Log Insight 会提供主节点和工作线程节点。主节点和工作线程节点均负责处理数据子集。主节点可以查询所有数据子集并聚合结果。您可能需要更多节点来支持站点需求。您可以在一个集群中使用 3 到 18 个节点。这意味着完全正常运行的集群必须至少具有三个正常节点。在较大集群中，必须有大多数节点处于正常状态。例如，如果包含六个节点的集群中有三个节点出现故障，则在移除故障节点之前，任何节点均无法完全正常运行。

前提条件

- 在 vSphere Client 中，记下工作 vRealize Log Insight 虚拟设备的 IP 地址。
- 确认知晓主 vRealize Log Insight 虚拟设备的 IP 地址或主机名。
- 确认拥有主 vRealize Log Insight 虚拟设备的管理员帐户。
- 确认 vRealize Log Insight 主节点和工作线程节点的版本已同步。请勿将旧版本的 vRealize Log Insight 工作线程添加到较新版本的 vRealize Log Insight 主节点。
- 必须将 vRealize Log Insight 虚拟设备上的时间与 NTP 服务器同步。请参见[同步 Log Insight 虚拟设备上的时间](#)。
- 有关支持的浏览器版本的信息，请参见《[vRealize Log Insight 发行说明](#)》。

步骤

- 1 使用受支持的浏览器导航到 vRealize Log Insight 工作线程的 Web 用户界面。
URL 格式为 `https://log_insight-host/`，其中，`log_insight-host` 是 vRealize Log Insight 工作线程节点虚拟设备的 IP 地址或主机名。
初始配置向导将打开。
- 2 单击**加入现有部署**。
- 3 输入 vRealize Log Insight 主节点的 IP 地址或主机名，然后单击**转到**。
工作线程节点会向 vRealize Log Insight 主节点发送加入现有部署的请求。
- 4 单击**单击此处访问“集群管理”**页面。
- 5 以管理员身份登录。
将加载“集群”页面。
- 6 单击**[允许]**。
工作线程节点加入现有部署，然后 vRealize Log Insight 开始在集群中运行。

后续步骤

- 根据需要，添加更多工作线程节点。该集群必须具有至少三个节点。

从 vRealize Log Insight 群集中移除工作线程节点


您可以从 vRealize Log Insight 群集中移除不再正常工作的工作线程节点。请勿从群集中移除正常工作的工作线程节点。

警告 移除节点将导致数据丢失。如果必须移除某个节点，首先确保已将其备份。避免在添加新节点后 30 分钟内移除节点。


前提条件

验证是否已以具有**编辑管理员**权限的用户身份登录到 vRealize Log Insight Web 用户界面。URL 格式为 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

- 1 导航到**管理**选项卡。
- 2 在“管理”下，单击**集群**。
- 3 在“工作线程”表中，找到所需的节点，单击暂停图标 ，然后单击**继续**。
现在，该节点处于维护模式。

注 处于维护模式的节点继续接收日志。

- 4 单击  移除节点。
vRealize Log Insight 会从群集中移除节点，然后发出电子邮件通知。
- 5 移除后，节点可以作为独立节点进行引导，也可以引导并加入集群。

使用集成负载均衡器

vRealize Log Insight 集成负载均衡器 (ILB) 支持 vRealize Log Insight 集群，并确保 vRealize Log Insight 接受入站载入流量，即使一些 vRealize Log Insight 节点变为不可用。也可配置多个虚拟 IP 地址。

注 不支持将外部负载均衡器用于 vRealize Log Insight，包括 vRealize Log Insight 集群。

最佳做法是 在所有部署中包含 ILB，包括单节点实例。将查询和载入流量发送到 ILB，以便将来根据需要轻松支持集群。ILB 在集群中的节点之间均衡流量，并最大限度减少管理开销。

ILB 确保 vRealize Log Insight 接受入站载入流量，即使一些 vRealize Log Insight 节点变为不可用。ILB 还可以把传入流量平均分摊到所有可用的 vRealize Log Insight 节点。同时使用 Web 用户界面和载入（通过 syslog 或数据获取 API）的 vRealize Log Insight 客户端通过 ILB 地址连接到 vRealize Log Insight。

ILB 要求所有 vRealize Log Insight 节点位于同一第 2 层网络上（例如，在同一交换机后面），或者能够以其他方式相互接收和发送 ARP 请求。必须设置 ILB IP 地址，以便任何 vRealize Log Insight 节点可以具有该地址并接收其流量。通常，这意味着 ILB IP 地址与 vRealize Log Insight 节点的物理地址位于同一子网中。在配置 ILB IP 地址之后，尝试从其他网络对其执行 ping，以确保它可访问。

为了简化将来的更改和升级，您可以将客户端指向解析为 ILB IP 地址的 FQDN，而不要直接指向 ILB IP 地址。

有关服务器直接返回配置

vRealize Log Insight 负载均衡器使用服务器直接返回 (DSR) 配置。在 DSR 中，所有入站流量通过 vRealize Log Insight 节点进行传输，该节点是当前负载均衡器节点。返回流量从 vRealize Log Insight 服务器直接发回到客户端，而无需通过负载均衡器节点进行传输。

多个虚拟 IP 地址

可以为集成负载均衡器配置多个虚拟 IP 地址 (vIP)。您也可以为每个 vIP 配置静态标记列表，以便从该 vIP 收到的每个日志消息均注释有配置的标记。

注 最佳做法是为 vRealize Log Insight 实例配置最多 12 个 vIP。

启用集成负载均衡器

在 vRealize Log Insight 集群上启用 vRealize Log Insight 集成负载均衡器 (ILB) 时，您必须配置一个或多个虚拟 IP 地址。

集成负载均衡器支持一个或多个虚拟 IP 地址 (vIP)。每个 vIP 在可用的 vRealize Log Insight 节点之间均衡入站载入和查询流量。最佳做法是，通过 vIP 将所有 vRealize Log Insight 客户端连接到节点，而不是直接连接到节点。

为了简化将来的更改和升级，您可以将客户端指向解析为 ILB IP 地址的 FQDN，而不要直接指向 ILB IP 地址。vSphere 和 vRealize Operations 集成以及警示消息将使用 FQDN（如果提供）。否则，它们使用 ILB IP 地址。vRealize Log Insight 可以将 FQDN 解析为给定 IP 地址，这意味着，您提供的 FQDN 值应该与 DNS 中定义的值相匹配。

前提条件

- 确认所有 vRealize Log Insight 节点和指定的集成负载均衡器 IP 地址在同一个网络上。
- 如果将 vRealize Log Insight 与 NSX 一起使用，请确认已在 NSX 逻辑交换机上禁用了 **启用 IP 发现** 选项。
- vRealize Log Insight 主节点和工作线程节点必须具有相同的证书。否则，配置为通过 SSL 连接的 vRealize Log Insight 代理将拒绝该连接。在将 CA 签名的证书上载到 vRealize Log Insight 主节点和工作线程节点时，请在证书生成请求期间将“公用名称”设置为 ILB FQDN（或 IP 地址）。请参见[生成证书签名请求](#)。
- 必须将 vRealize Log Insight 虚拟设备上的时间与 NTP 服务器同步。请参见[同步 Log Insight 虚拟设备上的时间](#)。

步骤

- 1 导航到**管理**选项卡。
- 2 在“管理”下，单击**集群**。
- 3 在“集成负载均衡器”部分中，选择**新建虚拟 IP 地址**，并输入用于集成负载均衡的虚拟 IP (VIP) 地址。
- 4 （可选）要配置多个虚拟 IP 地址，请单击**新建虚拟 IP 地址**，然后输入 IP 地址。可以选择输入 FQDN 和标记。
 - 每个 VIP 都应位于同一子网内（其中每个节点上至少有一个网络接口），且 VIP 必须是可用的（未被其他任何计算机使用）。
 - 使用标记您可以将含预定义值的字段添加到事件以简化查询。您可以采用逗号分隔的形式添加多个标记。通过 VIP 传入系统的所有事件均标有 VIP 标记。
 - 可以为 ILB VIP 配置一个静态标记（键=值）列表，这样，从该 VIP 接收到的每条日志消息都能以配置的标记进行注释。
- 5 （可选）要使 vRealize Log Insight 用户能够通过 FQDN 访问集群，请将客户端指向 FQDN，而不要直接指向配置的 ILB IP 地址。

为了简化将来的更改和升级，您可能希望将客户端指向可解析为 ILB IP 地址的 FQDN。您可以将客户端指向 FQDN，而不是直接指向 ILB IP 地址。

- 6 单击**保存**。

集成负载均衡器由 vRealize Log Insight 集群中的一个节点（声明作为该服务的前导者）管理。当前前导者由节点旁的文本 (ILB) 表示。

查询生产中群集检查的结果

生产中群集检查服务在每个节点上定期运行一组检查。可以使用 CLI 查询最新的生产中群集检查结果。

例如，该服务可确定群集是否正在运行并按预期配置，或是否存在与集成到其他系统有关的任何问题。下面列出其他检查内容。

- 多主机部署中是否配置了 NTP?
- 如果当前配置了 Active Directory，是否可以访问它?
- 如果当前配置了 Active Directory 身份验证，是否会发生该验证?
- 如果当前配置了 Active Directory，是否可以访问 Active Directory 主机和 Kerberos 主机?
- 系统是否运行在不受支持的双主机部署中?
- /tmp 中是否有足够的空间来执行升级?
- /storage/core 中是否有足够的空间来执行升级?
- localhost 是否正确置于 /etc/hosts 中?

步骤

- 1 在命令行处建立 SSH 到 vRealize Log Insight 虚拟设备的连接，然后以 **root** 用户身份登录。
- 2 在命令行中键入 `/usr/lib/loginsight/application/sbin/query-check-results.sh`，然后按 **Enter**。

配置、监控和更新 vRealize Log Insight 代理

6

您可以集中管理多个 vRealize Log Insight 代理的配置，监控其状态并启用自动更新。

本章讨论了以下主题：

- 集中式代理配置和代理组
- 监控 vRealize Log Insight 代理的状态
- 从服务器中启用代理自动更新

集中式代理配置和代理组

使用 vRealize Log Insight 服务器，您可以从应用程序用户界面内配置代理。代理定期轮询 vRealize Log Insight 服务器，以确定是否有可用的新配置。

可以将需要相同配置的代理分为一组。例如，可以将所有 vRealize Log Insight Windows 代理与 vRealize Log Insight Linux 代理分成不同的组。

在**所有代理**菜单中，将会自动列出内容包中的现有代理组。列出的代理与已安装的使用代理组的内容包（如 vSphere 内容包）相关。当您单击**我的内容**或**共享内容**时，用户创建的所有代理组都将显示在**内容包 > 自定义内容**下。

至少具有仅查看管理员角色的用户可以使用代理组模板导出内容包。

注

- 您不能多次使用同一个内容包模板。
- 内容包组是只读的。

内容包仅使用以 [winlog]、[filelog]、[journalldlog] 和 [parser] 开头的配置部分。其他部分不会作为内容包的一部分进行导出。内容包仅在 [winlog]、[filelog] 和 [parser] 部分下预留单行注释（即以 ; 开头的行）。

注 单个代理可以属于多个代理组，并从集中式代理配置中继承所有设置。

您可以按照**创建代理组**中的说明为所有代理组创建配置。如果通过集中式代理配置和其他配置的组合来配置代理，则代理配置是两个配置合并的结果。有关合并的更多信息，请参见**代理组配置合并**。

注 请尽可能使用代理组，除非需要，否则不要使用所有代理配置。

请参见使用 vRealize Log Insight 代理，了解有关配置代理，以及合并本地和服务器端配置的信息。

- [代理组配置合并](#)

在使用代理组的情况下，代理可以是多个组的一部分并且它们可以属于默认组“所有代理” - 启用集中式配置。

- [创建代理组](#)

可以创建一组使用相同参数配置的代理。

- [编辑代理组](#)

您可以编辑代理组的名称和描述，更改筛选器和编辑配置。

- [将内容包代理组作为代理组添加](#)

可以将定义为内容包一部分的代理组添加到活动组，并对该组应用代理配置。

- [删除代理组](#)

您可以删除代理组，将其从活动组列表中移除。

代理组配置合并

在使用代理组的情况下，代理可以是多个组的一部分并且它们可以属于默认组“所有代理” - 启用集中式配置。

服务器端出现合并 - 并且产生的配置与代理端配置合并。合并的配置是以下规则的结果。

- 单个组配置具有更高的优先级并且优先于“所有代理”组设置。
- “所有代理”组配置优先于本地配置。
- 您无法配置在除“所有代理”组外的其他组中具有相同名称的部分。但是，单个组中的部分具有更高的优先级。

注 为防止代理丢失，不能从服务器集中更改代理配置的 **hostname** 和 **port** 参数。

合并的配置存储在代理端 `liagent-effective.ini` 文件中。对于 Windows 系统，该文件存储在 `%ProgramData%\VMware\Log Insight Agent` 中；对于 Linux 系统，该文件存储在 `/var/lib/loginsight-agent/` 中。

创建代理组

可以创建一组使用相同参数配置的代理。

前提条件

验证是否已具有编辑管理员权限的用户身份登录到 vRealize Log Insight Web 用户界面。URL 格式为 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

- 1 导航到**管理**选项卡。

- 2 在“管理”下，单击**代理**。
- 3 在**所有代理**菜单中，在“刷新”按钮旁边的代理名称字段中打开下拉菜单，然后单击**新建组**。
- 4 为代理组提供唯一名称和描述，然后单击**新建组**。

将创建代理组，创建的代理组会显示在**所有代理**列表中，但是不会保存。

- 5 为代理组指定一个或多个筛选器。要创建筛选器，请指定字段名称、运算符和值。

筛选器可以包含通配符，如 * 和 ?。例如，您可以选择操作系统筛选器 contains，并指定 windows 值以列出配置的所有 Windows 代理。

- a 选择以下字段之一以进行筛选：

- IP 地址
- 主机名
- 版本
- 操作系统

- b 从下拉菜单中选择一个运算符，然后指定一个值。

运算符	描述
匹配	查找匹配指定字符串和通配符规范的字符串，其中 * 表示零个或多个字符，? 表示任何单个字符。支持前缀和后缀通配。 例如， *test* 与 test123 或 my-test-run 等字符串匹配。
不匹配	排除匹配指定字符串和通配符规范的字符串，其中 * 表示零个或多个字符，? 表示任何单个字符。支持前缀和后缀通配。 例如， test* 筛选掉 test123 ，但不会排除 mytest123 。 %test* 不会筛选掉 test123 ，但会排除 xtest123
开头为	查找以指定字符串开头的字符串。 例如， test 找到 test123 或 test ，但不会找到 my-test123 。
不以下列字符开头	排除以指定字符串开头的字符串。 例如， test 筛选掉 test123 ，但不会排除 my-test123 。

- 6 在“代理配置”区域中指定代理配置值，然后单击**保存新组**。

结果

下一个轮询间隔后将应用代理配置。

编辑代理组

您可以编辑代理组的名称和描述，更改筛选器和编辑配置。

前提条件

验证是否已以具有**编辑管理员**权限的用户身份登录到 vRealize Log Insight Web 用户界面。URL 格式为 <https://log-insight-host>，其中 *log-insight-host* 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

- 1 导航到**管理**选项卡。
- 2 在“管理”下，单击**代理**。
- 3 在**所有代理**菜单中，选择适当代理组的名称，然后单击铅笔图标即可对其编辑。
- 4 进行必要的更改。

要编辑的项目	操作
名称或描述	进行必要的更改，并单击 保存 。
筛选器或配置	进行必要的更改，并单击 保存组 。

将内容包代理组作为代理组添加

可以将定义为内容包一部分的代理组添加到活动组，并对该组应用代理配置。

前提条件

验证是否已具有**编辑管理员**权限的用户身份登录到 vRealize Log Insight Web 用户界面。URL 格式为 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

- 1 导航到**管理**选项卡。
- 2 在“管理”下，单击**代理**。
- 3 在**所有代理**菜单中，从“可用模板”列表中选择代理模板。
- 4 单击**复制模板**，将内容包代理组复制到活动组。
- 5 单击**复制**。
- 6 选择所需的筛选器，然后单击**保存新组**。

结果

内容包代理组就添加到了活动组中，并且根据您指定的筛选器配置好了代理。

删除代理组

您可以删除代理组，将其从活动组列表中移除。

前提条件

验证是否已具有**编辑管理员**权限的用户身份登录到 vRealize Log Insight Web 用户界面。URL 格式为 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

- 1 导航到**管理**选项卡。
- 2 在“管理”下，单击**代理**。
- 3 在**所有代理**菜单中，通过单击要删除的代理组名称旁边的 X 图标将其选中。
- 4 单击**删除**。

结果

代理组就从活动组中移除了。

监控 vRealize Log Insight 代理的状态

您可以监控 vRealize Log Insight Windows 和 Linux 代理的状态，并查看有关其运行状态的当前统计数据。

仅配置为通过 CFAPI 发送数据的代理显示在“代理”页面上。配置为通过 syslog 发送数据的代理与其他 syslog 源一起显示在“主机”页面上。如果协议从 CFAPI 更改为 syslog，则不会在“统计信息”页面上更新和显示统计信息，并且代理状态显示为“已断开连接”。在此处显示的数据每 30 秒从 LI 代理发送一次。vRealize Log Insight 最多可以显示 15,000 个代理的信息。

如果将协议从 CFAPI 更改为 syslog，统计信息将停止更新，并且不会再显示在代理页面上，同时代理状态会显示为已断开连接。这里显示的数据将每三十秒从 vRealize Log Insight 代理发送一次。

注 如果在代理配置中更改 vRealize Log Insight 服务器的主机 IP，代理将页面统计信息重置为零。

前提条件

确认您以具有**查看管理员**权限的用户身份登录到 vRealize Log Insight Web 用户界面。URL 格式为 <https://log-insight-host>，其中 *log-insight-host* 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

- 1 导航到**管理**选项卡。
- 2 在“管理”下，单击**代理**。

将会显示通过 CFAPI 发送数据的每个代理的状态信息。

Management										
System Monitor										
Cluster										
Access Control										
User Alerts										
Hosts										
Agents										
Event Forwarding										
License										

Agents										
All Agents										Enable auto-upda
EXPORT										Configurable only ⓘ 1 to 20 out
IP Addr...	Hostna...	Version	OS	Last Act...	Events ...	Events ...	Events ...	Uptime	Status	
1...	...	4.3.0.5052904	SUSE Linux Enterprise Server 11	Less than 1 minute ago	117,012	10	0	2 hours	Active	

后续步骤

可以使用“代理”页面中的信息来监控已安装的 vRealize Log Insight Windows 和 Linux 代理的运行状态。单击代理主机名可转到该主机的“交互式分析”页面。从 LI 代理中设置主机名参数后，如果使用默认 CFAP 协议并指向 Log Insight 实例，您可以打开“代理”统计信息页面，然后确认在代理列表中显示该代理以监控连接。您可以使用主机名列下面的链接导航到 Insight 代理页面，并检查来自上述代理的日志。

从服务器中启用代理自动更新

您可以从 vRealize Log Insight 服务器中为所有代理启用自动更新。

自动更新会将可用的最新更新应用于连接到服务器的所有代理。通过编辑代理的 `liagent.ini` 文件，可以禁用各个服务器的自动更新功能。有关详细信息，请参见使用 vRealize Log Insight 代理。

默认情况下，将为服务器禁用自动更新。

前提条件

代理必须处于活动状态，并且版本为 4.3 或更高版本。

步骤

- 1 导航到**管理**选项卡。
- 2 从左侧的菜单中，单击**代理**。
- 3 在“代理”页面上，单击**为所有代理启用自动更新**的切换控件。

结果

如果具有更新，则会更新连接到该服务器的代理。

监控 vRealize Log Insight

7

可以监控 vRealize Log Insight 虚拟设备以及将日志事件发送到 vRealize Log Insight 的主机和设备。

本章讨论了以下主题：

- 检查 vRealize Log Insight 虚拟设备的运行状况
- 监控发送日志事件的主机
- 配置报告非活动主机的系统通知

检查 vRealize Log Insight 虚拟设备的运行状况

检查 vRealize Log Insight 虚拟设备上的可用资源和活动查询，然后查看当前有关 vRealize Log Insight 运行的统计信息。

前提条件

验证是否已具有编辑管理员权限的用户身份登录到 vRealize Log Insight Web 用户界面。URL 格式为 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

- 1 导航到**管理**选项卡。
- 2 在“管理”下，单击**系统监控**。
- 3 如果 vRealize Log Insight 正在作为群集运行，请单击**显示下列项的资源**，然后选择要监控的节点。
- 4 单击“系统监控”页面上的按钮来查看您所需的信息。

选项	描述
资源	查看有关 vRealize Log Insight 虚拟设备上的 CPU、内存、IOPS（读取和写入活动）和存储使用情况的信息。 右侧的图表表示过去 24 小时的历史数据，并且每隔 5 分钟就会进行刷新。左侧的图表显示过去 5 分钟的信息，并且每隔 3 秒就会进行刷新。
活动查询	查看有关当前在 vRealize Log Insight 中处于活动状态的查询的信息。
统计信息	查看有关日志采集操作和速率的统计信息。 要查看更多详细的统计信息，请单击 显示高级统计信息 。

后续步骤

可以使用“系统监控”页面中的信息来管理 vRealize Log Insight 虚拟设备上的资源。

监控发送日志事件的主机

可以查看向 vRealize Log Insight 发送日志事件的所有主机和设备的列表，并对其进行监控。

主机表中的条目在上次载入的事件之后的三个月过期。

前提条件

验证是否已具有 **编辑管理员** 权限的用户身份登录到 vRealize Log Insight Web 用户界面。URL 格式为 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

- 1 导航到 **管理** 选项卡。
- 2 在“管理”下，单击 **主机**。

注 如果已将 vCenter Server 配置为发送事件和警报，但未将各个 ESXi 主机配置为发送日志，则“主机名”列会同时将 vCenter Server 和各个 ESXi 主机作为源列出，而不是仅列出 vCenter Server。

后续步骤

具有管理员特权的用户可以设置当主机处于非活动状态时发送的系统通知。有关详细信息，请参见 [配置报告非活动主机的系统通知](#)。

配置报告非活动主机的系统通知

vRealize Log Insight 包含一个内置通知，您可以通过此通知来了解哪些主机处于非活动状态的时间达到了指定的时间段。

您可以在“主机”屏幕上启用此通知并指定一个触发该通知的阈值。可以将此通知应用到所有主机或少数一些主机。

Hosts

☒ Inactive hosts notification.

Send alert listing hosts that are inactive for days of last received event ⓘ

The query will run every 1 hour and will only alert once for the defined threshold above.

☐ Inactive hosts notification whitelist ⓘ

前提条件

验证是否已具有**编辑管理员**权限的用户身份登录到 vRealize Log Insight Web 用户界面。URL 格式为 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

- 1 导航到**管理**选项卡。
- 2 在“管理”下，单击**主机**。

注 如果已将 vCenter Server 配置为发送事件和警报，但未将各个 ESXi 主机配置为发送日志，则“主机名”列会同时将 vCenter Server 和各个 ESXi 主机作为源列出，而不是仅列出 vCenter Server。

- 3 在**主机**页面上选择**非活动主机通知**，此时将显示一个表单，您可以从中配置应何时发送通知以及应针对哪些主机发送通知。
- 4 指定在发送通知之前主机应处于非活动状态的时间长度。

值的范围从 10 分钟到主机最大生存时间 (Time to Live, TTL) 周期（默认为三个月）。

例如

```
Send alert listing hosts that are inactive for 8 hours of last received event.
```

- 5 通过**非活动主机通知接受列表**设置，可以控制要对哪些主机进行监控以发送通知。如果未选择此设置，将对所有非活动主机发送通知。
 - 要对所有非活动主机发送通知，请清除该复选框。
 - 如要仅对部分非活动主机发送通知，请选择**非活动主机通知接受列表**，并通过以逗号分隔的列表来指定主机名。
- 6 单击**保存**。

结果

如果主机处于非活动状态的时间超过指定限制，将向在**配置 > SMTP 服务器**页上指定的地址发送系统通知。

将 vRealize Log Insight 与 VMware 产品集成



vRealize Log Insight 可以与其他 VMware 产品集成，以便使用事件和日志数据并为虚拟环境中出现的事件提供更佳可见性。

与 VMware vSphere 集成

vRealize Log Insight 管理员用户可以将 vRealize Log Insight 设置为每隔两分钟连接到 vCenter Server 系统，并从这些 vCenter Server 系统中收集事件、警报和任务数据。此外，vRealize Log Insight 还可以通过 vCenter Server 配置 ESXi 主机。请参见[将 vRealize Log Insight 连接到 vSphere 环境](#)。

与 VMware vRealize Operations Manager 集成

可以将 vRealize Log Insight 与 vRealize Operations Manager vApp 和 vRealize Operations Manager Installable 集成。与 Installable 版本集成需要对 vRealize Operations Manager 配置进行其他更改。有关配置 vRealize Operations Manager Installable 以与 vRealize Log Insight 集成的信息，请参见《Log Insight 入门指南》。

可以通过两种不同方法集成 vRealize Log Insight 和 vRealize Operations Manager。

通知事件

vRealize Log Insight 管理员用户可以设置 vRealize Log Insight 基于您创建的查询向 vRealize Operations Manager 发送通知事件。请参见[将 vRealize Log Insight 配置为向 vRealize Operations Manager 发送通知和衡量指标](#)。

在环境中启动

在环境中启动是 vRealize Operations Manager 中的一项功能，允许您通过 URL 在特定环境中启动外部应用程序。上下文由活动的 UI 元素和对象选择定义。在环境中启动可允许 vRealize Log Insight 适配器将菜单项添加到 vRealize Operations Manager 的自定义用户界面和 vSphere 用户界面中的许多不同视图中。请参见在[vRealize Operations Manager 中为 vRealize Log Insight 启用“在环境中启动”](#)。

注 通知事件不依赖于在环境中启动配置。即使不启用“在环境中启动”功能，您也可以将通知事件从 vRealize Log Insight 发送到 vRealize Operations Manager。

如果环境更改，vRealize Log Insight 管理员用户可以在 vRealize Log Insight 中更改、添加或删除 vSphere 系统，更改或删除向其发送警示通知的 vRealize Operations Manager 实例，以及更改用于连接到 vSphere 系统和 vRealize Operations Manager 的密码。

本章讨论了以下主题：

- 将 vRealize Log Insight 连接到 vSphere 环境
- 配置 vRealize Log Insight 以从 vCenter Server 实例中提取事件、任务和警报
- 将 vRealize Operations Manager 与 vRealize Log Insight 一起使用
- 适用于 vRealize Log Insight 的 vRealize Operations Manager Content Pack

将 vRealize Log Insight 连接到 vSphere 环境

在配置 vRealize Log Insight 以从 vSphere 环境中收集警报、事件和任务数据之前，必须将 vRealize Log Insight 连接到一个或多个 vCenter Server 系统。

vRealize Log Insight 可以从 vCenter Server 实例及其管理的 ESXi 主机中收集两种类型的数据。

- 事件、任务和警示是具有特殊含义的结构化数据。配置后，vRealize Log Insight 可从已注册的 vCenter Server 实例中提取事件、任务和警示。
- 日志包含可在 vRealize Log Insight 中分析的非结构化数据。ESXi 主机或 vCenter Server Appliance 实例可以通过 syslog 将其日志推送到 vRealize Log Insight。

前提条件

- 对于要达到的集成级别，请验证是否拥有具备在 vCenter Server 系统及其 ESXi 主机上执行必要配置所需足够特权的用户凭据。

集成级别	所需特权
事件、任务和警报集合	<ul style="list-style-type: none"> ■ 系统.查看
	<p>注 系统.查看是一种系统定义的权限。如果您添加了一个自定义角色但并不向其分配任何权限，则该角色创建为拥有如下三种系统定义权限的只读角色：系统.匿名、系统.查看和系统.读取。</p>
ESXi 主机上的 Syslog 配置	<ul style="list-style-type: none"> ■ 主机.配置.更改设置 ■ 主机.配置.网络配置 ■ 主机.配置.高级设置 ■ 主机.配置.安全配置文件和防火墙

注 必须在 vCenter Server 清单中配置顶层文件夹的权限，然后验证是否已选中传播到子项复选框。

- 确保知道 vCenter Server 系统的 IP 地址或域名。
- 验证是否已以具有编辑管理员权限的用户身份登录到 vRealize Log Insight Web 用户界面。URL 格式为 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

- 1 导航到**管理**选项卡。
- 2 在“集成”下，单击 **vSphere**。
- 3 输入 vCenter Server 的 IP 地址和服务帐户凭据，然后单击**测试连接**。
- 4 如果 vSphere 环境提供了不受信任的 SSL 证书，则会显示一个对话框，其中显示有该证书的详细信息。单击**接受**将证书添加到 vRealize Log Insight 群集中所有节点的信任库。

如果单击**取消**，则不会将该证书添加到信任库，并且与 vSphere 环境的连接将失败。您必须接受证书才能成功连接。
- 5 （可选）要注册另一个 vCenter Server，请单击**添加 vCenter Server**，然后重复步骤 3 到步骤 5。

注 请勿使用重复的名称或 IP 地址注册 vCenter Server 系统。vRealize Log Insight 不会检查重复的 vCenter Server 名称。必须验证已注册的 vCenter Server 系统列表是否不包含重复条目。

- 6 单击**保存**。

如果未测试连接，并且 vSphere 环境提供的证书不受信任，请按照第 4 步中的说明进行操作。

后续步骤

- 从您注册的 vCenter Server 实例中收集事件、任务和警报数据。请参见[配置 vRealize Log Insight 以从 vCenter Server 实例中提取事件、任务和警报](#)。
- 从 vCenter Server 管理的 ESXi 主机中收集 syslog 源。请参见[配置 ESXi 主机以将日志事件转发到 vRealize Log Insight](#)。

vRealize Log Insight 用作 Syslog 服务器

vRealize Log Insight 包括一个内置的 syslog 服务器，该服务器在 vRealize Log Insight 服务运行时一直保持活动状态。

Syslog 服务器可以侦听端口 514/TCP、1514/TCP 和 514/UDP，并载入发送自其他主机的日志消息。

Syslog 服务器载入消息后，可以近乎实时地在 vRealize Log Insight Web 用户界面中进行搜索。

vRealize Log Insight 可接受的最大 syslog 消息长度为 10 KB。

支持 syslog 格式 RFC-6587、RFC-5424 和 RFC-3164。

配置 ESXi 主机以将日志事件转发到 vRealize Log Insight

ESXi 主机或 vCenter Server Appliance 实例生成可在 vRealize Log Insight 中分析的非结构化日志数据。

使用 vRealize Log Insight 管理界面可在已注册的 vCenter Server 上配置 ESXi 主机，以便将 syslog 数据推送到 vRealize Log Insight。

小心 运行并行配置任务可能会在目标 ESXi 主机上导致错误 syslog 设置。验证没有任何其他管理用户正在配置您要配置的 ESXi 主机。

vRealize Log Insight 群集可以使用集成负载均衡器在群集的各个节点之间分配 ESXi 和 vCenter Server Appliance syslog 源。

有关在将 syslog 消息发送到 vRealize Log Insight 之前在 ESXi 主机上筛选这些消息的信息，请参见《vSphere 安装和设置》指南的“设置 ESXi”部分中的“在 ESXi 主机上配置日志筛选”主题。

有关从 vCenter Server Appliance 配置 syslog 源的信息，请参见[配置 vCenter Server](#) 以将日志事件转发到 vRealize Log Insight。

注 vRealize Log Insight 可以从 ESXi 主机版本 5.5 及更高版本接收 syslog 数据。

前提条件

- 验证管理 ESXi 主机的 vCenter Server 是否已在 vRealize Log Insight 实例中注册。或者，您可以在单个操作中注册 ESXi 主机并配置 vCenter Server。
- 验证是否拥有具备在 ESXi 主机上配置 syslog 所需足够特权的用户凭据。
 - 主机.配置.高级设置
 - 主机.配置.安全配置文件和防火墙

注 必须在 vCenter Server 清单中配置顶层文件夹的权限，然后验证是否已选中**传播到子项**复选框。

步骤

- 1 导航到**管理**选项卡。
- 2 在“集成”下，单击 **vSphere**。
- 3 在 vCenter Server 表中，找到管理要从中接收 syslog 源的 ESXi 主机的 vCenter Server 实例，然后单击**编辑**。
- 4 在打开的编辑视图中，选中**将 ESXi 主机配置为发送日志至 Log Insight** 复选框。
默认情况下，vRealize Log Insight 会配置所有可访问的版本 5.5 及更高版本的 ESXi 主机以通过 UDP 发送其日志。
- 5 （可选）要修改默认配置值，请单击**高级选项**。
 - 要更改所有 ESXi 主机的协议，请选择**配置所有 ESXi 主机**，选择一种协议，然后单击**确定**。
 - 要仅为特定 ESX 主机设置日志记录或更改选定 ESXi 主机的协议，请使用以下步骤：
 - a 选择**配置特定 ESXi 主机**。
 - b 从**按主机筛选**列表中选择一个或多个主机。
 - c 设置协议值。
 - d 单击**确定**。
- 6 （可选）如果使用群集，请打开**目标**文本框的下拉菜单，然后选择分配 syslog 源的负载均衡器的主机名或 IP 地址。
- 7 单击**保存**。

后续步骤

ESXi 主机配置显示在 vCenter Server 表的“ESXi 主机已配置”列中。如果已配置主机，您可以在“主机已配置”列中单击[查看详细信息](#)以查看配置的 ESXi 主机的详细信息。

修改 ESXi 主机配置以将日志事件转发到 vRealize Log Insight

ESXi 主机或 vCenter Server Appliance 实例生成可在 vRealize Log Insight 中分析的非结构化日志数据。

使用 vRealize Log Insight 管理界面可在已注册的 vCenter Server 上配置 ESXi 主机，以便将 syslog 数据推送到 vRealize Log Insight。

小心 运行并行配置任务可能会在目标 ESXi 主机上导致错误 syslog 设置。验证没有任何其他管理用户正在配置您要配置的 ESXi 主机。

设置初始配置后，您可以启用一个选项，以便定期查找并自动配置尚未配置的现有和新添加的 vSphere ESXi 主机。将使用当前配置的协议自动配置 ESXi 主机。

vRealize Log Insight 群集可以使用集成负载均衡器在群集的各个节点之间分配 ESXi 和 vCenter Server Appliance syslog 源。

有关在将配置的 syslog 消息发送到 vRealize Log Insight 之前在 ESXi 主机上筛选这些消息的信息，请参见《**vSphere 安装和设置**》指南中[设置 ESXi](#)部分的“在 ESXi 主机上配置日志筛选”主题。

有关从 vCenter Server Appliance 配置 syslog 源的信息，请参见[配置 vCenter Server 以将日志事件转发到 vRealize Log Insight](#)。

vRealize Log Insight 可以从 ESXi 主机版本 5.5 及更高版本接收 syslog 数据。

前提条件

- 验证管理 ESXi 主机的 vCenter Server 是否已在 vRealize Log Insight 实例中注册。
- 验证是否拥有具备在 ESXi 主机上配置 syslog 所需足够特权的用户凭据。
 - 主机.配置.高级设置
 - 主机.配置.安全配置文件和防火墙

注 必须在 vCenter Server 清单中配置顶层文件夹的权限，然后验证是否已选中[传播到子项](#)复选框。

步骤

- 1 导航到**管理**选项卡。
- 2 在“集成”下，单击 **vSphere**。
- 3 选中**将 ESXi 主机配置为发送日志至 Log Insight** 复选框。
- 4 单击**高级选项**。

- 5 要更改选定 ESXi 主机的协议，请使用以下步骤：
 - a 从**按主机筛选**列表选择一个或多个主机。
 - b 确认当前协议是您所需的协议，否则选择其他协议。
 - c 要启用通过当前配置的协议自动配置 ESXi 主机功能，请选择**自动配置所有 ESXi 主机**。启用后，vRealize Log Insight 会定期查找并配置尚未配置的现有和新添加的 vSphere ESXi 主机。
 - d 单击**配置**以开始配置选定的主机。将关闭 ESXi 对话框。
 - e 在消息对话框中，单击**确定**。
 - f 如果您更改了协议设置，请在关闭 **ESXi 配置**对话框后单击主窗口中的**保存**。
- 6 （可选）如果使用群集，您可以通过在 **vSphere 集成**页面上打开**目标**文本框的下拉菜单，然后选择负载平衡器的主机名或 IP 地址，来指定一个负载平衡器。

vRealize Operations Manager 中的 vRealize Log Insight 通知事件

可以配置 vRealize Log Insight 基于您创建的警示查询向 vRealize Operations Manager 发送通知事件。

在 vRealize Log Insight 中配置通知警示时，从 vRealize Operations Manager 中选择与通知事件相关联的资源。请参见在 [Log Insight 中添加警示查询以向 vRealize Operations Manager 发送通知事件](#)。

下面列出了显示通知事件的 vRealize Operations Manager UI 部分。

- 主页 > **建议仪表板** > **排名靠前的后代运行状况警示**小组件
- 主页 > **警示**选项卡
- 在包含事件通知小组件的所有自定义仪表板上

有关通知事件显示位置的其他信息，请参见 [VMware vRealize Operations Manager 文档中心](#)。

配置 vCenter Server 以将日志事件转发到 vRealize Log Insight

vSphere 集成从 vCenter Server 收集任务和事件，但不从每个 vCenter Server 组件收集低级别内部日志。这些日志由 vSphere 内容包使用。

vCenter Server 6.5 和更高版本的配置应当通过 vCenter Server Appliance 管理界面完成。有关如何转发来自 vCenter Server 的日志事件的详细信息，请参见有关将 vCenter Server Appliance 日志文件重定向到其他计算机的 [vSphere 文档](#)。

对于较低版本的 vSphere，虽然 vCenter Server Appliance 包含可用于路由日志的 syslog 守护进程，但首选方法是安装 vRealize Log Insight 代理。

有关安装 vRealize Log Insight 代理的信息，请参见[使用 vRealize Log Insight 代理](#)。

vSphere 内容包包含定义要从 vCenter Server 安装收集的特定日志文件的代理组。配置位于 `https://LogInsightServerFqdnOrIP/contentpack?contentPackId=com.vmware.vsphere`。

有关使用代理组的信息，请参见[集中式代理配置和代理组](#)。

有关 vCenter Server 日志文件位置的信息，请参见 <http://kb.vmware.com/kb/1021804> 和 <http://kb.vmware.com/kb/1021806>。

配置 vRealize Log Insight 以从 vCenter Server 实例中提取事件、任务和警报

事件、任务和警示是具有特殊含义的结构化数据。可以配置 vRealize Log Insight 以从一个或多个 vCenter Server 系统中收集警报、事件和任务数据。

使用管理 UI 配置 vRealize Log Insight 以连接到 vCenter Server 系统。通过使用 vSphere Web Services API 从 vCenter Server 系统中提取信息，这些信息在 vRealize Log Insight Web 用户界面中显示为 vSphere 内容包。

请注意，vSphere 6.5 提供了一个新的本机高可用性解决方案。有关高可用性和负载平衡器用法的详细信息，请参见 www.vmware.com 上提供的白皮书《VMware vSphere 6.5 的新增功能》。

注 vRealize Log Insight 仅可从 vCenter Server 5.5 及更高版本中提取警报、事件和任务数据。

前提条件

验证您是否拥有具有**系统.查看**特权的用户凭据。

注 必须在 vCenter Server 清单中配置顶层文件夹的权限，然后验证是否已选中**传播到子项**复选框。

步骤

- 1 导航到**管理**选项卡。
- 2 在“集成”下，单击 **vSphere**。
- 3 在 vCenter Server 表中，找到要从中收集数据的 vCenter Server 实例。
- 4 在打开的编辑视图中，选中**收集 vCenter Server 事件、任务和警报**复选框。
- 5 单击**保存**。

结果

vRealize Log Insight 会每两分钟便连接到 vCenter Server，并载入自上次成功轮询后的所有新信息。

后续步骤

- 使用 vSphere 内容包或自定义查询分析 vSphere 事件。
- 启用 vSphere 内容包警示或自定义警示。

将 vRealize Operations Manager 与 vRealize Log Insight 一起使用

与 vRealize Operations Manager 集成的要求

在将 vRealize Log Insight 与 vRealize Operations Manager 集成的过程中，必须指定 vRealize Log Insight 的凭据以便针对 vRealize Operations Manager 进行身份验证。

vRealize Operations Manager 既支持本地用户帐户，也支持多个 LDAP 源。vRealize Operations Manager 和 VMware Identity Manager 集成是由 vRealize Log Insight 管理员配置的。

如果您的部署在 vRealize Log Insight 中使用 VMware Identity Manager 集成，则 vRealize Operations Manager 集成页面上的 VMware Identity Manager 回退 URL（重定向 URL 主机）和目标字段应具有完全相同的值。

前提条件

验证集成用户帐户是否具有在 vRealize Operations Manager 中操作对象的权限。请参见[本地或 Active Directory](#) 用户帐户需具有的最低权限。

步骤

- ◆ 要确定本地用户帐户的用户名，请执行以下操作：
 - a 从 vRealize Operations Manager Web 界面中，选择**访问控制**。
 - b 标识或创建集成用户。“源类型”字段为**本地用户**。
 - c 记录**用户名**字段的值。在 vRealize Log Insight 管理用户界面中配置集成时，需指定此用户名。
- ◆ 要确定必须在 vRealize Log Insight 中提供的 LDAP 用户帐户的用户名格式，请按照下面的说明进行操作：
 - a 从 vRealize Operations Manager Web 界面中，选择**访问控制**。
 - b 标识或创建集成用户。记录**用户名**和**源类型**字段。例如，名为 **integration@example.com**、来自源 **Active Directory - ad** 的用户。
 - c 选择**身份验证源**。
 - d 标识与步骤 b 中的**源类型**对应的身份验证源。记录**源显示名称**字段。例如，“ad”。
 - e 在 vRealize Log Insight 管理用户界面中输入的用户名是步骤 3 和步骤 5 中的内容组合，形式为 **UserName@SourceDisplayName**。例如，**integration@example.com@ad**。

本地或 Active Directory 用户帐户需具有的最低权限

要将 vRealize Log Insight 与 vRealize Operations Manager 集成，必须指定 vRealize Log Insight 的凭据以便针对 vRealize Operations Manager 进行身份验证。要在 vRealize Operations Manager 中操作对象，用户帐户必须具有所需的权限。

如果为用户分配“在环境中启动”权限，用户还可以配置警示集成。请仅使用警示集成表中的信息分配警示集成权限。

表 8-1. 警示集成

操作	可选择的权限和对象
创建一个具有列出的权限的自定义角色。	1 系统管理-> Rest API a 所有其他 API，读取、写入 API b 对 API 的读取访问权限
为新的或现有的本地或 Active Directory 用户分配上述角色，并选择要分配的对象/对象层次结构。	1 适配器实例 -> vRealizeOpsMgrAPI [全选] 2 vSphere 主机和群集 [全选] 3 vSphere 网络连接 [全选] 4 vSphere 存储 [全选]

表 8-2. 在环境中启动集成

操作	可选择的权限和对象
创建一个具有列出的权限的自定义角色。	1 系统管理-> Rest API a 所有其他 API，读取、写入 API b 对 API 的读取访问权限 c 删除资源 2 系统管理 -> 配置 -> 管理资源关系 3 系统管理 -> 资源种类管理 a 创建 b 编辑 4 系统管理 -> 资源管理 a 创建 b 删除 c 读取 5 系统管理 -> 访问 -> 访问控制 -> 添加、编辑或删除角色。 注 vRealize Operations Manager 7.0 和更低版本需要使用该权限。
为新的或现有的本地或 Active Directory 用户分配上述角色，并选择要分配的对象/对象层次结构。	选择允许访问系统中的所有对象。

将 vRealize Log Insight 配置为向 vRealize Operations Manager 发送通知和衡量指标

可以将 vRealize Log Insight 配置为向 vRealize Operations Manager 发送警示通知和衡量指标。

可以将 vRealize Log Insight 与 vRealize Operations Manager vApp 和 vRealize Operations Manager Installable 集成。与 Installable 版本集成需要对 vRealize Operations Manager 配置进行其他更改。有关配置 vRealize Operations Manager Installable 以与 vRealize Log Insight 集成的信息，请参见《Log Insight 入门指南》。

通过将 vRealize Log Insight 警示与 vRealize Operations Manager 相集成，可以在单个用户界面中查看有关环境的所有信息。

可以将通知事件从多个 vRealize Log Insight 实例发送到单个 vRealize Operations Manager 实例。可以为每个 vRealize Operations Manager 实例的单个 vRealize Log Insight 实例启用“在环境中启动”。

vRealize Log Insight 使用 vRealize Operations Manager REST API 在 vRealize Operations Manager 中创建资源和关系以配置“在环境中启动”适配器。

前提条件

- 使用所需权限，在 vRealize Operations Manager 中创建集成用户帐户。有关详细信息，请参见 [与 vRealize Operations Manager 集成的要求](#)。
- 确保了解目标 vRealize Operations Manager 实例的 IP 地址或主机名。
- 验证是否已以具有[编辑管理员](#)权限的用户身份登录到 vRealize Log Insight Web 用户界面。URL 格式为 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

注 在运行配置了负载均衡器的 vRealize Operations Manager 集群的环境中，您可以使用负载均衡器 IP 地址（如果可用）。

步骤

- 1 导航到**管理**选项卡。
- 2 在“集成”下，选择 **vRealize Operations Manager**。
- 3 输入主节点或负载均衡器（如果已配置）的 IP 地址或主机名。使用 vRealize Operations Manager 用户凭据并单击**测试连接**。vRealize Log Insight 使用凭据将通知事件推送到 vRealize Operations Manager。确保配置的用户拥有使集成正常工作所需的最低权限。请参见[本地或 Active Directory 用户帐户需具有的最低权限](#)。
- 4 如果 vRealize Operations Manager 提供了不受信任的 SSL 证书，则会显示一个对话框，其中显示有该证书的详细信息。单击**接受**将证书添加到 vRealize Log Insight 集群中所有节点的信任库。

如果单击**取消**，则不会将该证书添加到信任库，并且与 vRealize Operations Manager 的连接将失败。您必须接受证书才能成功连接。

- 5 在 vRealize Operations Manager 窗格中，根据您的偏好选中相关的复选框：
 - 要向 vRealize Operations Manager 发送警示，请选择**启用警示集成**。
 - 要让 vRealize Operations Manager 打开 vRealize Log Insight 并查询对象日志，请选择**启用“在环境中启动”**。有关详细信息，请参见在 [vRealize Operations Manager 中为 vRealize Log Insight 启用“在环境中启动”](#)。
 - 要计算衡量指标并将其发送到 vRealize Operations Manager，请选择**启用衡量指标计算**。

- 6 单击**保存**。

如果未测试连接，并且 vRealize Operations Manager 提供的证书不受信任，请按照第 4 步中的说明进行操作。

后续步骤

- 请参见 vRealize Operations Manager UI 中的相关页面以查看 vRealize Log Insight 发送的通知事件。

在 vRealize Operations Manager 中为 vRealize Log Insight 启用“在环境中启动”

可以配置 vRealize Operations Manager 以显示与 vRealize Log Insight 相关的菜单项，并使用对象特定的查询启动 vRealize Log Insight。

可以将 vRealize Log Insight 与 vRealize Operations Manager vApp 和 vRealize Operations Manager Installable 集成。

要与 vApp 安装和 Installable（Windows、Linux）集成在一起，需要对 vRealize Operations Manager 配置进行其他更改。请参见 [vRealize Log Insight 文档](#) 中有关在 vRealize Operations Manager 6.x 及更高版本中安装 vRealize Log Insight 管理包（适配器）的主题。

注 在 vRealize Operations Manager 6.0 和更高版本中预装了 vRealize Log Insight 管理包，该管理包不需要进行配置更改。

从 vRealize Operations Manager 6.5 和更高版本开始，不再支持 vRealize Operations Manager Installable（Windows 版本）。

重要事项 vRealize Operations Manager 的一个实例仅支持 vRealize Log Insight 的一个实例的“在环境中启动”。由于 vRealize Log Insight 无法检查是否其他实例已在 vRealize Operations Manager 中注册，您可能会覆盖其他用户的设置。

前提条件

- 验证是否已以具有**编辑管理员**权限的用户身份登录到 vRealize Log Insight Web 用户界面。URL 格式为 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。
- 确保了解目标 vRealize Operations Manager 实例的 IP 地址或主机名。
- 确认您具有所需的用户凭据。请参见本地或 [Active Directory](#) 用户帐户需具有的最低权限。
- 如果使用的是 vRealize Operations Manager 6.5 或更高版本，请使用《vRealize Operations Manager 配置指南》的使用 vRealize Operations Manager 配置 vRealize Log Insight 中启用“在环境中启动”的步骤。

步骤

- 1 导航到**管理**选项卡。
- 2 在“集成”下，选择 **vRealize Operations Manager**。
- 3 输入 vRealize Operations Manager 主节点或负载均衡器（如果已配置）的 IP 地址或 FQDN，然后单击**测试连接**。

注 为了使用“在环境中启动”功能，必须为 vRealize Operations Manager 用户提供管理员特权。

- 4 单击**保存**。

结果

vRealize Log Insight 会配置 vRealize Operations Manager 实例。此操作可能需要几分钟的时间。

与 vRealize Log Insight 相关的项会在 vRealize Operations Manager 的菜单中显示。

后续步骤

从 vRealize Operations Manager 实例中启动 vRealize Log Insight 查询。请参见[在环境中启动 vRealize Log Insight](#)

在环境中启动 vRealize Log Insight

针对 vRealize Log Insight 启用“在环境中启动”时，将在 vRealize Operations Manager 中创建 vRealize Log Insight 资源。

资源标识符包含 vRealize Log Insight 实例的 IP 地址，vRealize Operations Manager 使用该资源标识符打开 vRealize Log Insight。

vRealize Operations Manager 6.5 和更高版本中的“在环境中启动”

有关启用“在环境中启动”的信息，请参见 [vRealize Operations Manager 信息中心](#)。

vRealize Operations Manager 6.4 和更低版本的 vSphere 用户界面中的“在环境中启动”

与 vRealize Log Insight 相关的“在环境中启动”选项显示在 vSphere 用户界面的操作下拉菜单中。可以使用这些菜单项打开 vRealize Log Insight，并搜索 vRealize Operations Manager 中对象的日志事件。

可用的“在环境中启动”操作取决于您在 vRealize Operations Manager 清单中选择对象。查询的时间范围限制在单击“在环境中启动”选项前的 60 分钟内。

表 8-3. vRealize Operations Manager UI 中的对象及其对应的“在环境中启动”选项和操作

在 vRealize Operations Manager 中选定的对象	操作下拉菜单中的“在环境中启动”选项	vRealize Operations Manager 中的操作	vRealize Log Insight 中的操作
环境	打开 vRealize Log Insight	打开 vRealize Log Insight。	vRealize Log Insight 将显示交互式分析选项卡。
vCenter Server	打开 vRealize Log Insight	打开 vRealize Log Insight。	vRealize Log Insight 将显示交互式分析选项卡。
数据中心	在 vRealize Log Insight 中搜索日志	打开 vRealize Log Insight，并传递选定数据中心对象下所有主机系统的资源名称。	vRealize Log Insight 将显示交互式分析选项卡，并执行查询来查找包含数据中心内主机的名称的日志事件。
群集	在 vRealize Log Insight 中搜索日志	打开 vRealize Log Insight，并传递选定群集对象下所有主机系统的资源名称。	vRealize Log Insight 将显示交互式分析选项卡，并执行查询来查找包含群集中主机的名称的日志事件。

表 8-3. vRealize Operations Manager UI 中的对象及其对应的“在环境中启动”选项和操作（续）

在 vRealize Operations Manager 中选定的对象	操作下拉菜单中的“在环境中启动”选项	vRealize Operations Manager 中的操作	vRealize Log Insight 中的操作
主机系统	在 vRealize Log Insight 中搜索日志	打开 vRealize Log Insight，并传递选定主机对象的资源名称。	vRealize Log Insight 将显示 交互式分析 选项卡，并执行查询来查找包含选定主机系统的名称的日志事件。
虚拟机	在 vRealize Log Insight 中搜索日志	打开 vRealize Log Insight，并传递选定虚拟机的 IP 地址和相关主机系统的资源名称。	vRealize Log Insight 将显示 交互式分析 选项卡，并执行查询来查找包含虚拟机 IP 地址和虚拟机所驻留的主机的名称的日志事件。

在**警示**选项卡上，如果选择一个警示并在上下文菜单中选择在 **Log Insight 中搜索日志**，则查询的时间范围将限制在触发该警示前的一小时内。例如，如果在 2:00 PM 触发警示，则 vRealize Log Insight 查询将显示在 1:00 PM 到 2:00 PM 之间发生的所有日志消息。这有助于识别可能触发警示的事件。

可以通过 vRealize Operations Manager 的衡量指标图表打开 vRealize Log Insight。vRealize Log Insight 所运行的查询的时间范围与衡量指标图表的时间范围相匹配。

注 如果虚拟设备的时间设置不同，则 vRealize Log Insight 和 vRealize Operations Manager 衡量指标图表中显示的时间可能有所不同。

vRealize Operations Manager 6.4 和更低版本用户界面中的“在环境中启动”

“在环境中启动”图标  显示在用户界面的多个页面上，但是，只能从显示 vRealize Log Insight 通知事件的页面启动 vRealize Log Insight：

- “警示概览”页面。
- vRealize Log Insight 通知警示的“警示摘要”页面。
- 仪表板上的“警示”小组件，如果选择了 vRealize Log Insight 通知警示。

在自定义用户界面上选择 vRealize Log Insight 通知事件后，可以在两个“在环境中启动”操作中进行选择。

表 8-4. vRealize Operations Manager UI 中的“在环境中启动”选项和操作

vRealize Operations Manager 中的“在环境中启动”选项	vRealize Operations Manager 中的操作	vRealize Log Insight 中的操作
打开 vRealize Log Insight	打开 vRealize Log Insight。	vRealize Log Insight 将显示 仪表板 选项卡并加载“vSphere 概览”仪表板。
在 vRealize Log Insight 中搜索日志	打开 vRealize Log Insight，并传递触发通知事件的查询的 ID。	vRealize Log Insight 将显示 交互式分析 选项卡，并执行触发通知事件的查询。

如果选择的警示不是源自 vRealize Log Insight，则“在环境中启动”菜单将包含在 **vRealize Log Insight 中搜索虚拟机和主机日志** 菜单项。如果选择此菜单项，则 vRealize Operations Manager 将打开 vRealize Log Insight，并传递触发警示的对象的标识符。vRealize Log Insight 将使用该资源标识符在可用日志事件中执行搜索。

双向在环境中启动

也可以从 vRealize Log Insight 到 vRealize Operations Manager 执行“在环境中启动”。

如果将 vRealize Log Insight 与 vRealize Operations Manager 集成，可以通过一个 vRealize Log Insight 事件执行在环境中启动，其方法是：选择该事件左侧的齿轮图标，然后通过选择相关选项在 vRealize Operations Manager 中查看。

有关从 vRealize Operations Manager 到 vRealize Log Insight 执行在环境中启动的信息，请参见 [在环境中启动 vRealize Log Insight](#)。

步骤

- 1 在 vRealize Log Insight 中，导航到**交互式分析**选项卡。
- 2 找到包含清单映射字段的事件，然后将鼠标悬停在该事件上。
- 3 单击齿轮图标，然后从 vRealize Operations Manager 的下拉菜单中选择**打开分析**。

将打开一个新浏览器选项卡，将您定向到与 vRealize Log Insight 集成的 vRealize Operations Manager 实例。在进行身份验证后，将定向到 vRealize Operations Manager 的**环境 > 分析**部分并选定对象。

注 如果多个 vRealize Log Insight 实例连接到同一个 vRealize Operations Manager 实例，则只有最后一个与 vRealize Operations Manager 集成的 vRealize Log Insight 实例具有在环境中启动功能。这也就是说，如果 vRealize Operations Manager 实例先前曾与 vRealize Log Insight 实例集成，则当其再与其他 vRealize Log Insight 实例集成时，在环境中启动功能将被覆盖。

在 vRealize Operations Manager 中为 vRealize Log Insight 禁用“在环境中启动”

可以从 vRealize Operations Manager 实例中卸载 vRealize Log Insight 适配器以从 vRealize Operations Manager 用户界面中移除与 vRealize Log Insight 相关的菜单项。

使用 vRealize Log Insight 的管理 UI 禁用“在环境中启动”。如果没有 vRealize Log Insight 的访问权限，或者在禁用与 vRealize Operations Manager 的连接之前已删除 vRealize Log Insight 实例，则可以从 vRealize Operations Manager 的管理 UI 取消注册 vRealize Log Insight。请参见 vRealize Operations Manager 管理门户中的“帮助”。

小心 vRealize Operations Manager 的一个实例仅支持 vRealize Log Insight 的一个实例的“在环境中启动”。如果在注册要禁用的实例后已注册 vRealize Log Insight 的另一个实例，则第二个实例会覆盖第一个实例的设置，且不会通知您。

前提条件

- 验证是否已以具有**编辑管理员**权限的用户身份登录到 vRealize Log Insight Web 用户界面。URL 格式为 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

- 1 导航到**管理**选项卡。
- 2 在“集成”下，选择 **vRealize Operations Manager**。
- 3 取消选中启用“在环境中启动”复选框。
- 4 单击**保存**。

结果

vRealize Log Insight 会配置 vRealize Operations Manager 实例以移除 vRealize Log Insight 适配器。此操作可能需要几分钟的时间。

添加 DNS 搜索路径和域

您可以添加 DNS 搜索路径和域来提高 vRealize Operations Manager 清单匹配。

当虚拟机标签和搜索域解析为将日志消息发送至 vRealize Log Insight 的主机的 IP 地址时，添加 DNS 搜索路径和域可提高匹配。例如，如果您在 vRealize Operations Manager 中有一个名为 `linux_01` 的虚拟机，并且主机名 `linux_01.company.com` 解析为 `192.168.10.10`，那么，添加搜索域可允许 vRealize Log Insight 识别和匹配该资源。

步骤

- 1 对 vRealize Log Insight 虚拟设备执行客户机关闭操作。
- 2 关闭虚拟机电源后，选择**编辑设置**。
- 3 选择 **vApp 选项**选项卡。
- 4 在 **vApp 选项 > 编写**中，单击**属性**。
- 5 查找 `vami.searchpath.VMware_vCenter_Log_Insight` 和 `vami.domain.VMware_vCenter_Log_Insight` 键。

如果这些键不存在，请创建这些键。

对于搜索路径键，请使用以下值：

- 类别为**网络属性**
- 标签为 **DNS 搜索路径**
- 键类 ID 为 **vami**
- 键实例 ID 为 **VMware_vCenter_Log_Insight**。
- 类型为**静态属性**、“字符串”和**用户可配置**。

对于域键，请使用相同的值，并用 **DNS 域** 替换 **标签**，用 **域** 替换 **键 ID**。

6 设置 DNS 搜索路径和域。例如 `ny01.acme.local`。

7 打开虚拟设备电源。

后续步骤

在 vRealize Log Insight 引导后，可以登录并查看 `/etc/resolv.conf` 文件的内容以验证 DNS 配置。您应在文件结尾看到搜索和域选项。

移除 vRealize Log Insight 适配器

在 vRealize Operations Manager 6.2 和更高版本的实例上启用“在环境中启动”时，vRealize Log Insight 将在 vRealize Operations Manager 实例上创建一个 vRealize Log Insight 适配器实例。

卸载 vRealize Log Insight 后，适配器实例仍保留在 vRealize Operations Manager 实例中。因此，“在环境中启动”菜单项继续在操作菜单中显示，并且指向不再存在的 vRealize Log Insight 实例。

要在 vRealize Operations Manager 中禁用“在环境中启动”功能，必须从 vRealize Operations Manager 实例中移除 vRealize Log Insight 适配器。

可以使用命令行实用程序 cURL 向 vRealize Operations Manager 发送 REST 调用。

注 仅当启用了“在环境中启动”时才需要执行这些步骤。

前提条件

- 验证是否已在您的系统上安装 cURL。请注意，此工具已预安装在 vRealize Operations Manager 虚拟设备中，因此这些步骤可以从此设备中使用 IP 地址 127.0.0.1 来执行。
- 确保了解目标 vRealize Operations Manager 实例的 IP 地址或主机名。
- 根据所拥有的 vRealize Operations Manager 许可证，验证是否具有移除管理包所需的最少凭据。请参见 [本地或 Active Directory 用户帐户](#) 需具有的最低权限。

步骤

- 1 在 cURL 中，在 vRealize Operations Manager 虚拟设备上运行以下查询以查找 vRealize Log Insight 适配器。

```
curl -k -u "admin" https://ipaddress/suite-api/api/adaptkinds/LogInsight/resourcekinds/LogInsightLogServer/resources
```

其中 *admin* 是管理员的登录名，*ipaddress* 是 vRealize Operations Manager 实例的 IP 地址（或主机名）。系统将提示您输入用户 *admin* 的密码。

从 cURL 输出中找到分配给 *identifier* 的 GUID 值：`<ops:resource creationTime="{TIMESTAMP}" identifier="{GUID}">`。可以在下面移除适配器实例的命令中使用此 GUID 值。

2 运行以下命令以移除 vRealize Log Insight 适配器。

```
curl -k -u "admin" -X DELETE https://ipaddress/suite-api/api/adapters/{GUID}
```

其中 *admin* 是管理员的登录名，*ipaddress* 是 vRealize Operations Manager 实例的 IP 地址（或主机名）。系统将提示您输入用户 *admin* 的密码。

结果

vRealize Log Insight 在环境中启动项已从 vRealize Operations Manager 的菜单中移除。有关在环境中启动的详细信息，请参见 vRealize Log Insight 产品帮助的“vRealize Log Insight 在环境中启动”主题。

适用于 vRealize Log Insight 的 vRealize Operations Manager Content Pack

适用于 vRealize Log Insight 的 vRealize Operations Manager Content Pack 包含可用于分析从 vRealize Operations Manager 实例重定向的所有日志的仪表板、已提取字段、已保存的查询和警示。

vRealize Operations Manager Content Pack 提供了一种分析从 vRealize Operations Manager 实例重定向的所有日志的方法。内容包中包含可向 vRealize Operations Manager 管理员提供诊断和故障排除功能的仪表板、查询和警示。仪表板根据 vRealize Operations Manager 的主要组件（如分析、UI 和适配器）进行分组以便更好地管理。可以启用各种警示来向管理员发送 vRealize Operations Manager 中的通知事件以及相关电子邮件。

可以从 [VMware Marketplace](#) 下载 vRealize Operations Manager Content Pack。

请参见[使用内容包](#)。

vRealize Log Insight 的安全注意事项

9

使用 vRealize Log Insight 功能可保护您的环境免受攻击。

本章讨论了以下主题：

- 端口和外部接口
- vRealize Log Insight 配置文件
- vRealize Log Insight 公用密钥、证书和密钥库
- vRealize Log Insight 许可证和 EULA 文件
- vRealize Log Insight 日志文件
- vRealize Log Insight 用户帐户
- vRealize Log Insight 防火墙建议
- 安全更新和修补程序

端口和外部接口

vRealize Log Insight 使用特定所需服务、端口和外部接口。

要查看有关 vRealize Log Insight 的端口和协议的信息，请参见 [VMware Ports and Protocols](#) 工具。

通信端口

vRealize Log Insight 使用 Ports and Protocols 工具中列出的通信端口和协议。所需端口的组织方式取决于：源、用户界面、集群间以及外部服务是否需要端口；或防火墙是否可以安全地阻止端口。某些端口仅在启用相应集成后才会使用。

注 vRealize Log Insight 不支持 WAN 集群（也称为地理集群、高可用性集群或远程集群）。集群中的所有节点都应该部署在同一个第 2 层 LAN 内。此外，还必须在节点之间打开通信端口才能正确交换信息。

vRealize Log Insight 网络流量拥有多个源。

管理员工作站

系统管理员用来远程管理 vRealize Log Insight 虚拟设备的计算机。

用户工作站

vRealize Log Insight 用户使用浏览器访问 vRealize Log Insight 的 Web 界面的计算机。

发送日志的系统

向 vRealize Log Insight 发送日志以供分析和搜索的端点。例如，端点包括 ESXi 主机、虚拟机或具有 IP 地址的任何系统。

Log Insight Agents

位于 Windows 或 Linux 计算机上，并通过 API 向 vRealize Log Insight 发送操作系统事件和日志的代理。

vRealize Log Insight 设备

任何 vRealize Log Insight 虚拟设备、vRealize Log Insight 服务所在的主节点或工作线程节点。设备的基础操作系统是 SUSE 11 SP3。

源发送数据所需的端口

必须为来自向 vRealize Log Insight 发送数据的源的网络流量打开这些端口，这适用于集群外部的连接以及在集群节点之间均衡负载的连接。

用户界面所需的端口

必须为需要使用 vRealize Log Insight 用户界面的网络流量打开这些端口，这适用于集群外部的连接以及在集群节点之间均衡负载的连接。

集群节点间所需的端口

为最大程度地保证安全，从工作线程节点访问网络时，应仅在 vRealize Log Insight 主节点上打开这些端口。这些端口为用于在集群节点之间均衡负载的源和 UI 流量的端口提供补充。

外部服务所需的端口

必须为从 vRealize Log Insight 集群节点到远程服务的出站网络流量打开这些端口。

vRealize Log Insight 配置文件

某些配置文件包含影响 vRealize Log Insight 安全性的设置。

注 root 帐户可访问所有与安全相关的资源。保护此帐户的安全对 vRealize Log Insight 的安全至关重要。

表 9-1. Log Insight 配置文件

文件	描述
/usr/lib/loginsight/application/etc/loginsight-config-base.xml	vRealize Log Insight 的默认系统配置。
/storage/core/loginsight/config/loginsight-config.xml# <i>number</i>	vRealize Log Insight 的（从默认值）修改的系统配置。

表 9-1. Log Insight 配置文件（续）

文件	描述
/usr/lib/loginsight/application/etc/jaas.conf	Active Directory 集成的配置。
/usr/lib/loginsight/application/etc/3rd_config/server.xml	Apache Tomcat 服务器的系统配置。
/storage/var/loginsight/apache-tomcat/conf/tomcat-users.xml	Apache Tomcat 服务器的系统配置。
/usr/lib/loginsight/application/3rd_party/apache-tomcat-*/conf/server.xml	Apache Tomcat 服务器的系统配置。
/usr/lib/loginsight/application/3rd_party/apache-tomcat-*/conf/tomcat-users.xml	Apache Tomcat 服务器的用户信息。

vRealize Log Insight 公用密钥、证书和密钥库

vRealize Log Insight 的公用密钥、证书和密钥库位于 vRealize Log Insight 虚拟设备上。

注 root 帐户可访问所有与安全相关的资源。保护此帐户的安全对 vRealize Log Insight 的安全至关重要。

- /usr/lib/loginsight/application/etc/public.cert
- /usr/lib/loginsight/application/etc/loginsight.pub
- /usr/lib/loginsight/application/etc/3rd_config/keystore
- /usr/lib/loginsight/application/etc/truststore
- /usr/lib/loginsight/application/3rd_party/apache-tomcat-*/conf/keystore

vRealize Log Insight 许可证和 EULA 文件

最终用户许可协议 (EULA) 和许可证文件位于 vRealize Log Insight 虚拟设备上。

注 root 帐户可访问所有与安全相关的资源。保护此帐户的安全对 vRealize Log Insight 的安全至关重要。

文件	位置
许可证	/usr/lib/loginsight/application/etc/license/loginsight_dev.dlf
许可证	/usr/lib/loginsight/application/etc/license/loginsight_cpu.dlf
许可证	/usr/lib/loginsight/application/etc/license/loginsight_osi.dlf
许可证密钥文件	/usr/lib/loginsight/application/etc/license/loginsight_license.bak
最终用户许可协议	/usr/lib/loginsight/application/etc/license/release/eula.txt

vRealize Log Insight 日志文件

这些文件包含系统消息，它们位于 vRealize Log Insight 虚拟设备上。

下表列出了每个文件及其用途。

如果您需要了解有关这些文件的日志轮换或日志存档的信息，请参见使用 vRealize Log Insight 代理中的 [vRealize Log Insight 代理支持的日志轮换方案](#) 以及管理 vRealize Log Insight 中的 [数据存档](#)。

文件	描述
/var/log/vmware/loginsight/alert.log	用于跟踪有关已触发的用户定义的警示的信息。
/var/log/vmware/loginsight/apache-tomcat/logs/*.log	用于跟踪来自 Apache Tomcat 服务器的事件。
/var/log/vmware/loginsight/cassandra.log	用于跟踪 Apache Cassandra 中的集群配置存储和复制。
/var/log/vmware/loginsight/plugins/vsphere/li-vsphere.log	用于跟踪与 vSphere Web Client 集成相关的事件。
/var/log/vmware/loginsight/loginsight_daemon_stdout.log	用于 vRealize Log Insight 守护进程的标准输出。
/var/log/vmware/loginsight/phonehome.log	用于跟踪有关发送至 VMware 的跟踪数据收集的信息（如果已启用）。
/var/log/vmware/loginsight/pi.log	用于跟踪数据库启动或停止事件。
/var/log/vmware/loginsight/runtime.log	用于跟踪与 vRealize Log Insight 相关的所有运行时信息。
/var/log/firstboot/stratavm.log	用于跟踪在 vRealize Log Insight 虚拟设备首次引导和配置时出现的事件。
/var/log/vmware/loginsight/systemalert.log	用于跟踪有关 vRealize Log Insight 发送的系统通知的信息。每个警示都列为 JSON 条目。
/var/log/vmware/loginsight/systemalert_worker.log	用于跟踪有关 vRealize Log Insight 工作线程节点发送的系统通知的信息。每个警示都列为 JSON 条目。
/var/log/vmware/loginsight/ui.log	用于跟踪与 vRealize Log Insight 用户界面相关的事件。
/var/log/vmware/loginsight/ui_runtime.log	用于跟踪与 vRealize Log Insight 用户界面相关的运行时事件。
/var/log/vmware/loginsight/upgrade.log	用于跟踪 vRealize Log Insight 升级期间出现的事件。
/var/log/vmware/loginsight/usage.log	用于跟踪所有查询。
/var/log/vmware/loginsight/vrops_integration.log	用于跟踪与 vRealize Operations Manager 集成相关的事件。
/var/log/vmware/loginsight/watchdog_log*	用于跟踪监视程序进程的运行时事件，该进程负责在 vRealize Log Insight 由于某些原因而关闭时将其重新启动。
/var/log/vmware/loginsight/api_audit.log	用于跟踪对 Log Insight 的 API 调用。
/var/log/vmware/loginsight/pattern_matcher.log	用于跟踪字段提取的模式匹配时间和超时。
/var/log/vmware/loginsight/audit.log	用于跟踪 vRealize Log Insight 的使用情况。有关详细信息，请参见 vRealize Log Insight 中的审核日志 。

与安全性相关的日志消息

ui_runtime.log 文件包含以下格式的用户审核日志消息。

- [2019-05-10 11:28:29.709+0000] ["https-jsse-nio-443-exec-9"/10.153.234.136
DEBUG] [com.vmware.loginsight.web.actions.misc.LoginActionBean] [User
login success: vIDM: SAM=myusername, Domain=vmware.com,
UPN=myusername@vmware.com]
- [2019-05-10 11:28:45.812+0000] ["https-jsse-nio-443-exec-3"/10.153.234.136
INFO] [com.vmware.loginsight.web.actions.misc.LoginActionBean] [User
logged out: vIDM: SAM=myusername, Domain=vmware.com,
UPN=myusername@vmware.com]
- [2019-05-10 11:28:29.709+0000] ["https-jsse-nio-443-exec-9"/10.153.234.136
DEBUG] [com.vmware.loginsight.web.actions.misc.LoginActionBean] [User
login success: Active Directory User: SAM=myusername,
Domain=vmware.com,UPN=myusername@vmware.com]
- [2019-05-10 11:28:45.812+0000] ["https-jsse-nio-443-exec-3"/10.153.234.136
INFO] [com.vmware.loginsight.web.actions.misc.LoginActionBean] [User
logged out: Active Directory User: SAM=myusername,
Domain=vmware.com,UPN=myusername@vmware.com]
- [2019-05-10 11:29:28.330+0000] ["https-jsse-nio-443-exec-6"/10.153.234.136
DEBUG] [com.vmware.loginsight.web.actions.misc.LoginActionBean] [User
login success: Local User: Name=myusername]
- [2019-05-10 11:29:47.078+0000] ["https-jsse-nio-443-exec-10"/
10.153.234.136 INFO]
[com.vmware.loginsight.web.actions.misc.LoginActionBean] [User logged out:
Local User: Name=myusername]
- [2019-05-10 11:29:23.559+0000] ["https-jsse-nio-443-exec-7"/10.153.234.136
WARN] [com.vmware.loginsight.web.actions.misc.LoginActionBean] [User login
failure: Bad username/password attempt (username: incorrectUser)]
- [2019-05-10 11:45:37.795+0000] ["https-jsse-nio-443-exec-7"/10.153.234.136
INFO] [com.vmware.loginsight.web.actions.settings.UsersActionBean]
[Created new user: Local User: Name=myusername]
- [2019-05-10 11:09:50.493+0000] ["https-jsse-nio-443-exec-6"/10.153.234.136
INFO] [com.vmware.loginsight.web.actions.settings.UsersActionBean]
[Created new user: vIDM: SAM=myusername, Domain=vmware.com,
UPN=myusername@vmware.com]
- [2019-05-10 11:47:05.202+0000] ["https-jsse-nio-443-exec-10"/
10.153.234.136 INFO]
[com.vmware.loginsight.web.actions.settings.UsersActionBean] [Created new
group: (directoryType= VIDM, domain=vmware.com, group=vidm_admin)]

```
■ [2019-05-10 11:58:11.902+0000] ["https-jsse-nio-443-exec-4"/10.153.234.136
INFO] [com.vmware.loginsight.web.actions.settings.UsersActionBean]
[Removed groups: [class
com.vmware.loginsight.database.dao.RBACADGroupDO<vidm/vmware.com/
vidm_admin>]]
```

某些日志在调试级别可用。有关为每个节点启用调试级别的信息，请参见[为用户审核日志消息启用调试级别](#)。

提示 如果您是管理员，则可以在不重新启动 vRealize Log Insight 服务的情况下修改日志记录级别。转到 http://<your_Log_Insight_host>/internal/config，更新相关日志的日志记录级别值，然后单击**保存**。例如：

```
<self-logging>
  <logger name="root" level="INFO" />
</self-logging>
```

您可以将日志记录级别更改为 OFF、FATAL、ERROR、WARN、INFO、DEBUG、TRACE 或 ALL。

注 vRealize Log Insight 集群中的每个节点都有其自身的 ui_runtime.log 文件。您可以通过检查节点的日志文件来监控集群。

为用户审核日志消息启用调试级别

您可以为用户审核日志消息启用调试级别，以将日志消息包含在 ui_runtime.log 文件中。

前提条件

确认您拥有登录 vRealize Log Insight 虚拟设备所需的 root 用户凭据。

步骤

- 1 导航到 /usr/lib/loginsight/application/etc/ 位置，然后在任意文本编辑器中打开配置文件 loginsight-config-base.xml。
- 2 对于名称为 UI_RUNTIME_FILE 的附加程序，请将 Threshold 参数值更新为 DEBUG：

```
<appenders>
  <appender name="UI_RUNTIME_FILE"
    class="com.vmware.loginsight.log4j.SafeRollingFileAppender">
    <param name="Threshold" value="DEBUG"/>
  </appender>
</appenders>
```

- 3 使用 DEBUG 登录级别为 LoginActionBean 添加一个新日志记录：

```
<loggers>
  <logger name="com.vmware.loginsight.web.actions.misc.LoginActionBean" level="DEBUG"
    appender="UI_RUNTIME_FILE" additivity="false"/>
</loggers>
```

- 4 保存并关闭 `loginsight-config-base.xml` 文件。
- 5 运行 `service loginsight restart` 命令以应用所做的更改。

提示 您还可以在不重新启动 vRealize Log Insight 服务的情况下为用户审核日志启用调试级别。有关详细信息，请参见 [vRealize Log Insight 日志文件](#)。

vRealize Log Insight 中的审核日志

审核日志可跟踪 vRealize Log Insight 的使用情况。

审核日志文件 `audit.log` 位于 `/var/log/vmware/loginsight/` 中。此文件将记录以下操作：

类别	记录的操作
用户身份验证	<ul style="list-style-type: none"> ■ 登录、注销和身份验证失败。
访问控制	<ul style="list-style-type: none"> ■ 创建、移除和修改用户、组、角色及数据集。
配置	<ul style="list-style-type: none"> ■ 创建和移除转发器、vSphere 和 vRealize Operations Manager 集成等。 ■ 更改配置值，如会话超时、SSL、SMTP 配置等。
内容包	<ul style="list-style-type: none"> ■ 安装、卸载和升级。 ■ 导入和导出。
仪表板和小组件	<ul style="list-style-type: none"> ■ 创建、移除和修改。 ■ 共享仪表板。
系统管理	<ul style="list-style-type: none"> ■ 配置代理并启用自动更新。 ■ 升级集群。 ■ 添加和移除证书与许可证。
警示	<ul style="list-style-type: none"> ■ 创建、移除和修改。
交互式分析	<ul style="list-style-type: none"> ■ 创建、移除和修改快照和已提取字段。

vRealize Log Insight 用户帐户

必须设置系统和 root 帐户才能管理 vRealize Log Insight。

vRealize Log Insight Root 用户

vRealize Log Insight 当前使用 root 用户帐户作为服务用户。未创建任何其他用户。

除非在部署期间已设置根密码属性，否则默认根密码为空。在首次登录到 vRealize Log Insight 控制台时，必须更改根密码。

在设置默认根密码之前，SSH 处于禁用状态。

根密码必须符合以下要求。

- 长度必须至少为 8 个字符

- 必须至少包含 1 个大写字母、1 个小写字母、1 个数字和 1 个特殊字符
- 同一字符不得重复四次

vRealize Log Insight 管理员用户

首次启动 vRealize Log Insight 虚拟设备时，vRealize Log Insight 会为其 Web 用户界面创建管理员用户帐户。

管理员的默认密码为空。在 vRealize Log Insight 初始配置期间，必须在 Web 用户界面中更改管理员密码。

Active Directory 支持

vRealize Log Insight 支持与 Active Directory 集成。配置后，vRealize Log Insight 可以针对 Active Directory 对用户进行身份验证或授权。

请参见启用通过 [Active Directory](#) 进行用户身份验证。

分配给默认用户的特权

vRealize Log Insight 服务用户拥有 root 特权。

Web 用户界面管理员用户仅具有 vRealize Log Insight Web 用户界面的管理员特权。

vRealize Log Insight 防火墙建议

要保护由 vRealize Log Insight 收集的敏感信息，请将一台或多台服务器置于受防火墙保护而不受其余内部网络干扰的管理网段上。

所需的端口

必须为来自向 vRealize Log Insight 发送数据的源的网络流量打开以下端口。

端口	协议
514/UDP, 514/TCP	Syslog
1514/TCP, 6514/TCP	Syslog-TLS (SSL)
9000/TCP	vRealize Log Insight 数据获取 API
9543/TCP	vRealize Log Insight 数据获取 API - TLS (SSL)

必须为需要使用 vRealize Log Insight UI 的网络流量打开以下端口。

端口	协议
80/TCP	HTTP
443/TCP	HTTPS

为最大程度地保证安全，从工作线程节点访问网络时，应仅在 vRealize Log Insight 主节点上打开以下端口集。

端口	协议
16520:16580/TCP	Thrift RPC
59778/TCP	log4j 服务器
12543/TCP	数据库服务器

安全更新和修补程序

vRealize Log Insight 虚拟设备使用 VMware Photon 3.0 作为客户机操作系统。

vRealize Log Insight 8.0 或更高版本附带 Photon 操作系统。Photon 比 vRealize Log Insight 4.8 或更早版本附带的 SLES 操作系统更安全。

VMware 发布了修补程序来解决维护版本中存在的安全问题。您可以从 [vRealize Log Insight 下载页面](#) 下载这些修补程序。

在将升级或修补程序应用到客户机操作系统之前，请考虑相应依赖关系。请参见 [端口和外部接口](#)。

备份、还原和灾难恢复

10

为防止代价昂贵的数据中心停机，请遵循以下关于执行 vRealize Log Insight 备份、还原和灾难恢复操作的最佳做法。

本章讨论了以下主题：

- 备份、还原和灾难恢复概览
- 使用静态 IP 地址和 FQDN
- 规划与准备
- 备份节点和集群
- 备份 Linux 或 Windows 代理
- 还原节点和集群
- 还原后更改配置
- 验证还原
- 灾难恢复

备份、还原和灾难恢复概览

VMware 提供全面、集成的业务连续性和灾难恢复 (BCDR) 解决方案产品组合，使您享受高可用性、数据保护和灾难恢复服务。

请阅读本文档中有关 vRealize Log Insight 组件（包括主节点、工作线程节点和转发器）的备份、还原和灾难恢复信息。

- 有关主节点和工作线程节点集群成员的信息（包括配置、日志数据和自定义），请参见[备份节点和集群](#)。
- 有关 Linux 或 Windows 代理本地配置的信息，请参阅[备份 Linux 或 Windows 代理](#)。

本文档中的信息不适用于以下工具和产品。您必须从多个资源获取关于这些工具和产品的信息。

- 用于备份、还原和灾难恢复的第三方工具。有关详细信息，请参见供应商文档。
- vSphere Data Protection、Site Recovery Manager 和 Veritas NetBackup。有关 VMware BCDR 解决方案的其他信息，请参见 <https://www.vmware.com/solutions/business-continuity-disaster-recovery-draas.html>。

- 与 vRealize Log Insight 相集成的产品的备份、还原和灾难恢复功能。
 - vRealize Operations Manager
 - vSphere Web Client 服务器
 - ESXi 主机

使用静态 IP 地址和 FQDN

可以使用静态 IP 地址和 FQDN 来避免备份、还原和灾难恢复操作期间的风险。

将静态 IP 地址用于 vRealize Log Insight 集群节点和负载均衡器

如果将静态 IP 地址用于 vRealize Log Insight 集群中的所有节点，就无需在 IP 地址更改时更新集群节点的 IP 地址。

vRealize Log Insight 包括每个集群节点配置文件中的所有节点 IP 地址，如[知识库文章 2123058](#)中所述与 vRealize Log Insight 集成的所有产品（ESXi、vSphere、vRealize Operations）使用集群主节点的完全限定域名（FQDN）或 IP 地址作为 syslog 目标。这些产品可以使用负载均衡器的 FQDN 或 IP 地址（如果配置了）作为 syslog 目标。静态 IP 地址可减少经常更新多个位置中的 syslog 目标 IP 地址的风险。

为负载均衡器提供静态 IP 地址以及可选的虚拟 IP 地址。当配置集成负载均衡器时，为虚拟 IP 地址提供可选的 FQDN。出于任何原因无法访问 IP 地址时，将使用 FQDN。

将 FQDN 用于 vRealize Log Insight 集群节点和工作线程节点

如果将 FQDN 用于 vRealize Log Insight 集群中的所有节点，可以节省还原和恢复后配置更改的时间，前提是同一 FQDN 可以在恢复站点上解析。

对于主节点（负载均衡器，如果使用），需使用完全可解析的 FQDN。否则，ESXi 主机将无法给 vRealize Log Insight 或任何远程目标提供 syslog 消息。

对于系统通知，vRealize Log Insight 使用 FQDN 主机名（如果可用）而非 IP 地址。

可以合理假设，只有底层 IP 地址在备份和还原或灾难恢复操作后发生了更改。使用 FQDN，就无需更改向 vRealize Log Insight 集群提供日志的所有外部设备上的 syslog 目标地址（主节点 FQDN 或内部负载均衡器 FQDN）。

验证来自 vRealize Log Insight 工作线程节点的加入请求是否使用 vRealize Log Insight 主节点的 FQDN。

每个节点上的配置文件中的主节点主机值基于发送加入请求的第一个工作线程节点所使用的值。对加入请求使用主节点的 FQDN 可防止在灾难恢复后对主节点主机值进行任何手动更改。否则，在所有已还原集群节点上的配置文件中更新主节点主机名之前，工作线程节点将无法重新加入主节点。

规划与准备

在实施备份、还原或灾难恢复过程之前，请查看此主题中的计划和准备信息。

备份、还原和灾难恢复计划中应包括下列建议。

测试备份操作

首先在测试或转储环境中执行备份、还原和灾难恢复操作的测试运行，然后再在实时生产设置上执行这些操作。

执行整个 vRealize Log Insight 群集的完全备份。不要依靠自动步骤来备份各个文件和配置。

确认修复

确认在执行备份、还原和灾难恢复操作之前执行了修复并且解决了警告和错误。备份、还原和灾难恢复工具通常提供可视化验证和步骤，以确保成功创建备份、还原和灾难恢复配置。

调度备份

根据群集配置，首次备份操作通常是执行完全备份。您应延长一些时间等待首次备份完成。后续备份可以为增量备份或完全备份，与首次备份操作相比其完成速度相对较快。

其他文档和工具

对于 vRealize Log Insight 备份、还原和灾难恢复工具，确认您遵循文档来分配资源。

对于第三方备份、还原和灾难恢复工具，确认您遵循下列工具特定的最佳做法和建议。

对于使用 VMware 产品部署的虚拟机，使用可以提供特殊功能和配置的其他工具来支持备份、还原和灾难恢复。

转发器和群集

针对转发器，请对主要 vRealize Log Insight 群集应用备份、还原和灾难恢复步骤。请参见[还原节点和集群](#)。

根据客户要求，您可能有一个或多个 vRealize Log Insight 转发器。此外，可以将转发器安装为独立节点或安装为群集。出于备份、还原和灾难恢复操作的目的，vRealize Log Insight 转发器与主 vRealize Log Insight 群集节点相同，处理方式也一样。

备份节点和集群

最佳做法是，设置计划的 vRealize Log Insight 节点和集群备份或复制。

前提条件

- 在执行备份或复制操作之前，验证源站点和目标站点上不存在任何配置问题。
- 验证集群资源分配未达到容量上限。

在具有合理载入和查询负载的配置中，内存和交换使用量在备份和复制操作期间可达到近 100% 的能力。由于内存存在实时环境中接近容量上限，因此内存高峰一部分是由 vRealize Log Insight 集群的使用量所导致。同时，调度备份和复制操作也会极大程度上造成内存高峰。

某些情况下，工作线程节点在重新连接到主节点前会暂时断开 1 至 3 分钟，可能的原因是高内存使用率。

- 通过执行以下一项或两项操作，降低 vRealize Log Insight 节点上的内存限制：
 - 通过 vRealize Log Insight 建议的配置分配额外的内存。
 - 在非高峰期间调度周期性备份。

步骤

- 1 通过使用与 vRealize Log Insight 服务器相同的步骤，启用对 vRealize Log Insight 转发器的定期备份或复制。
- 2 确认根据可用资源和客户的特定要求正确选择了备份频率和备份类型。
- 3 如果资源不是问题且如果工具提供支持，则启用并发集群节点备份以加速备份过程。
- 4 同时备份所有节点。

有关如何备份节点的信息，请参见 [vRealize Suite 文档](#) 中的备份、还原和灾难恢复部分。

后续步骤

监控 - 当正在进行备份时，确保检查 vRealize Log Insight 设置中的任何环境或性能问题。大多数备份、还原和灾难恢复工具都提供监控功能。

在备份过程中，检查生产系统中的所有相关日志，因为用户界面可能不会显示所有问题。

备份 Linux 或 Windows 代理

您可以在服务器端备份安装和配置信息以备份代理。无需单独备份代理节点。

代理通常安装在还用于其他某个应用程序或服务的 Linux 或 Windows 系统上，并且可能包括在现有的备份过程中。通过使用包含整个代理安装及其配置的计算机的完整文件级别或块级别备份，就足以进行恢复了。代理支持本地配置和服务器提供的配置。

如果完全从 vRealize Log Insight 服务器中配置代理，而没有在本地对 `liagent.ini` 配置文件进行任何更改，您可以完全避免创建代理安装备份。相反，可以执行全新的代理安装并检索服务器备份。

如果代理具有自定义本地配置，请备份 `liagent.ini` 文件，并在进行全新代理安装时还原该文件。如果使用代理节点并不仅仅是安装代理软件并且这些节点需要完全备份，请遵循与任何其他虚拟机相同的备份过程。

如果在（代理上的）客户端上执行了代理配置并且仅将代理节点用于在其上安装 vRealize Log Insight 代理软件，则只需对代理配置文件进行备份就已足够。

前提条件

确认在 vRealize Log Insight 服务器端具有代理配置。

步骤

- 1 备份 `liagent.ini` 文件。
- 2 使用备份文件替换已恢复代理或 Linux 或 Windows 计算机上的文件。

还原节点和集群

必须按特定顺序还原节点，某些还原场景可能需要手动更改配置。

根据用于还原的工具，您可以将虚拟机还原到相同主机、相同数据中心上的不同主机或目标远程数据中心上的不同主机。请参见[还原后更改配置](#)

前提条件

- 确认还原的节点处于已关闭电源状态。
- 确认集群实例已关闭电源，然后再将集群还原至新站点。
- 确认在恢复站点上使用相同 IP 地址和 FQDN 时无裂脑行为发生。
- 确认没有人在主站点上意外使用部分正在运行的集群。

步骤

- 1 先还原主节点，然后再还原工作线程节点。
- 2 以任意顺序还原工作线程节点。
- 3 （可选）还原转发器（如果已配置）。

确保先还原 vRealize Log Insight 服务器（集群设置中的主节点及所有工作线程节点），然后再还原转发器。

- 4 还原任意已恢复代理。

后续步骤

- 在还原 vRealize Log Insight 集群时，如果使用相同的 IP 地址，请确认所有已还原的节点 IP 地址和 FQDN 均与其原始的节点 IP 地址和 FQDN 相关联。

例如，以下方案失败。在包含节点 A、B 和 C 的三节点集群中，节点 A 使用 IP 地址 B 还原，节点 B 使用 IP 地址 C 还原，节点 C 使用 IP 地址 A 还原。

- 如果仅将相同 IP 地址用于部分已还原的节点，则请确认对于这些节点，所有还原的映像均与其原始 IP 地址相关联。
- 大多备份还原和灾难恢复工具会提供一个监控视图，用于查看还原操作的进度，了解还原操作是失败还是出现警告。对发现的所有问题采取适当的操作。
- 如果需要进行手动配置更改后才可以完全还原站点，请按照[还原后更改配置](#)中的准则执行操作。
- 成功还原后，抽查已还原的集群。

还原后更改配置

备份配置过程中应用的恢复目标和 IP 自定义决定了需要进行哪些手动配置更改。您必须对一个或多个 vRealize Log Insight 节点应用配置更改，之后还原的站点才能完全正常运行。

还原到相同主机

将 vRealize Log Insight 群集恢复到相同主机比较简单，可以通过任意工具执行。

前提条件

查看有关[规划与准备](#)的重要信息。

步骤

- 1 关闭现有群集电源，然后再开始还原操作。默认情况下，会将相同的 IP 地址和 FQDN 用于还原的群集节点。

- 2 （可选）为群集提供一个新名称。

在还原过程中，还原的版本会覆盖群集的原始副本，除非向虚拟机提供了新名称。

- 3 （可选）如果可能，确认用于生产环境的所有网络、IP 和 FQDN 设置均保留在已还原和恢复的站点中。

后续步骤

成功还原且进行健全性检查后，删除旧副本以节省资源，并防止在用户打开旧副本电源时发生意外裂脑情况。

还原到其他主机

执行到其他主机的还原时，必须在 vRealize Log Insight 集群上进行配置更改。

在 vRealize Log Insight 3.0 及更高版本中，不正式支持直接从设备控制台修改配置文件。有关如何使用 Web UI 界面修改这些文件的信息，请参见[知识库文章 2123058](#)。

这些配置更改特定于可与任何备份恢复工具配合使用的 vRealize Log Insight 内部版本。

恢复到其他主机需要在 vRealize Log Insight 集群上手动配置更改。您可以假定还原的 vRealize Log Insight 节点具有与从中执行备份的源节点不同的 IP 地址和 FQDN。

前提条件

查看有关[规划与准备](#)的重要信息。

步骤

- 1 列出分配给各个 vRealize Log Insight 节点的所有新 IP 地址和 FQDN。

2 使用[知识库文章 2123058](#) 中所述的步骤在主节点上进行以下配置更改。

- a 在 vRealize Log Insight 配置部分中，查找与以下各行内容类似的行。

```
<distributed overwrite-children="true">
  <daemon host="prod-es-vrli1.domain.com" port="16520" token="c4c4c6a7-f85c-4f28-
a48f-43aeea27cd0e">
    <service-group name="standalone" />
  </daemon>
  <daemon host="192.168.1.73" port="16520" token="a5c65b52-
aff5-43ea-8a6d-38807ebc6167">
    <service-group name="workernode" />
  </daemon>
  <daemon host="192.168.1.74" port="16520" token="a2b57cb5-
a6ac-48ee-8e10-17134ele462e">
    <service-group name="workernode" />
  </daemon>
</distributed>
```

该代码显示三个节点。第一个节点是主节点，显示 `<service-group name=standalone>`；其余两个节点是工作线程节点，显示 `<service-group name="workernode">`

- b 对于主节点，在新恢复的环境中，验证曾用于恢复前环境中的 DNS 条目是否可以重用。
- 如果 DNS 条目可以重用，则仅更新 DNS 条目以指向主节点的新 IP 地址。
 - 如果 DNS 条目不可重用，则将主节点条目替换为新 DNS 名称（指向新 IP 地址）。
 - 如果无法分配 DNS 名称，最后的选择是使用新 IP 地址更新配置条目。
- c 同时，更新工作线程节点 IP 地址以反映新 IP 地址。

- d 在相同配置文件中，确认具有表示 NTP、SMTP 以及数据库和 appender 部分的条目。

```
<ntp>
  <ntp-servers value="ntp1.domain.com, ntp2.domain.com" />
</ntp>

<smtp>
  <server value="smtp.domain.com" />
  <default-sender value="source.domain.com@domain.com" />
</smtp>

<database>
  <password value="xserttt" />
  <host value="vrli-node1.domain.com" />
  <port value="12543" />
</database>
```

- 如果配置的 NTP 服务器值在新环境中不再有效，则在 <ntp>...</ntp> 部分更新这些值。
- 如果配置的 SMTP 服务器值在新环境中不再有效，则在 <smtp>...</smtp> 部分更新这些值。
- 此外，还可以在 SMTP 部分更改 default-sender 值。可以更改为任意值，但最佳做法是此值应表示所发送电子邮件的来源。
- 在 <database>...</database> 部分，更改主机值以指向主节点的 FQDN 或 IP 地址。

- e 在相同的配置文件中，更新 vRealize Log Insight ILB 配置部分。

```
<load-balancer>
<leadership-lease-renewal-secs value="5" />
<high-availability-enabled value="true" />
<high-availability-ip value="10.158.128.165" />
<high-availability-fqdn value="LB-FQDN.eng.vmware.com" />
<layer4-enabled value="true" />
<ui-balancing-enabled value="true" />
</load-balancer>
```

- f 在 <load-balancer>...</load-balancer> 部分下，更新 high-availability-ip 值（如果不同于当前设置）。
- g 确保也更新负载均衡器的 FQDN。
- h 通过 **管理** 选项卡上的 **集群** 子选项卡从 Web UI 重新启动。对于列出的各个节点，选择相应主机名或 IP 地址以打开“详细信息”面板，然后单击 **“重新启动 Log Insight”**。
- 配置更改会自动应用于所有集群节点。
- i 在 vRealize Log Insight 服务启动后等待 2 分钟，以便在使其他工作线程节点联机之前有足够的时间让 Cassandra 服务启动。

后续步骤

确认为已还原 vRealize Log Insight 节点分配的 IP 地址和 FQDN 与从中执行备份的源 IP 地址和 FQDN 不同。

验证还原

必须确认所有已还原的 vRealize Log Insight 集群可以完全正常运行。

前提条件

在验证节点和集群配置之前，确认备份和还原过程已完成。

步骤

- 1 使用内部负载均衡器 (ILB) IP 地址或 FQDN（如果配置了）登录到 vRealize Log Insight。
- 2 导航到**管理**选项卡。
- 3 确认以下项：
 - a 确认各个集群节点都可以使用各自的 IP 地址或 FQDN 访问。
 - b 从集群页面确认集群节点的状态，并确保 ILB（如已配置）也处于活动状态。
 - c 确认 vSphere 集成。如有必要，请重新配置集成。如果 ILB 或者主节点 IP 地址或 FQDN 在恢复后发生了更改，需进行重新配置。
 - d 确认 vRealize Operations Manager 集成并再次重新配置（如果需要）。
 - e 确认所有内容包和 UI 功能均可正常运行。
 - f 确认 vRealize Log Insight 转发器和代理可以正常运行（如果配置了）。
- 4 确认 vRealize Log Insight 的其他关键功能可按预期运行。

后续步骤

对备份和恢复计划进行任何必要的调整，以解决在备份、还原和确认操作期间可能发现的问题。

灾难恢复

记录充分和测试良好的恢复计划对群集快速恢复工作状态至关重要。

针对灾难恢复进行虚拟机配置时，复制类型的选择十分关键。决定复制类型时，请考虑恢复点目标 (RPO)、恢复时间目标 (RTO) 以及成本和可扩展性。

在灾难恢复方案中，有时如果主要站点完全关闭，则您无法恢复到相同的站点。但是基于您选择的选项，要求采取一些手动步骤以使 vRealize Log Insight 群集完全还原并恢复到运行状态。

除非 vRealize Log Insight 群集完全关闭且不可访问，否则在将群集还原到新站点前请验证群集实例已关闭电源。

在断电或灾难期间，请尽快恢复 vRealize Log Insight 群集。

vRealize Log Insight 故障排除

11

在致电 VMware 支持服务之前，您可以解决与 vRealize Log Insight 管理相关的一些常见问题。

本章讨论了以下主题：

- 无法在 Internet Explorer 上登录到 vRealize Log Insight
- vRealize Log Insight 磁盘空间不足
- 存档数据的导入可能失败
- 使用虚拟设备控制台创建 vRealize Log Insight 的支持包
- 重置管理员用户密码
- 重置 Root 用户密码
- 无法向 vRealize Operations Manager 提交警示
- 使用 Active Directory 凭据无法登录
- SMTP 无法在启用 STARTTLS 选项的情况下使用
- 由于无法验证 .pak 文件的签名，升级失败
- 升级失败并显示内部服务器错误
- 与 VMware 产品集成后第一条日志消息中缺少 vmw_object_id 字段

无法在 Internet Explorer 上登录到 vRealize Log Insight

无法在 Internet Explorer 上进行 vRealize Log Insight 身份验证。

问题

vRealize Log Insight Web 客户端需要 LocalStorage 或 DOM 存储支持，但您的文件系统完整性级别禁止 Internet Explorer 使用 LocalStorage。控制台和调试程序显示错误 SCRIPT5：访问被拒绝 (SCRIPT5: Access is Denied)。

原因

vRealize Log Insight 无法访问 LocalStorage 或 DOM 存储支持。Internet Explorer 会将此存储数据保存在使用 CachePath 参数设置的文件夹中，名义上位于 %USERPROFILE%

\AppData\LocalLow\Microsoft\Internet Explorer\DOMstore 中。如果此文件夹的完整性级别不是“低”，则 Internet Explorer 将无法使用 LocalStorage。

解决方案

您可以使用以下命令来设置用户帐户的完整性级别。

```
icaccls %userprofile%\Appdata\LocalLow /t /setintegritylevel (OI)(CI)L
```

vRealize Log Insight 磁盘空间不足

如果使用小型虚拟磁盘，并且未启用存档，则 vRealize Log Insight 主节点或工作线程节点可能会出现磁盘空间不足问题。

问题

如果每分钟入站日志速率超出存储空间的 3%，或者 vRealize Log Insight 无法从存储中删除最旧的数据段，则 vRealize Log Insight 磁盘空间不足。

原因

在正常情况下，vRealize Log Insight 绝不会磁盘空间不足，因为它每分钟都会检查可用空间是否小于 3%。如果 vRealize Log Insight 虚拟设备上的可用空间下降至低于 3%，则旧数据段会停用。

如果启用了存档，vRealize Log Insight 会先将段存档，然后再将其标记为已存档并在将来停用。如果在旧分段存档和停用之前可用空间已满，则 vRealize Log Insight 会磁盘空间不足。

解决方案

验证数据存档位置是否可用以及是否具有足够的可用空间。请参见[数据存档](#)。

注 如果所有解决方案都不适用，请联系客户支持。

存档数据的导入可能失败

如果 vRealize Log Insight 虚拟设备磁盘空间不足，则存档数据的导入可能失败。

问题

vRealize Log Insight 存储库导入程序实用程序不检查 vRealize Log Insight 虚拟设备上的可用磁盘空间。因此，如果虚拟设备磁盘空间不足，则导入存档的日志可能失败。

解决方案

增加 vRealize Log Insight 虚拟设备的存储容量并再次开始导入。不过请注意，在失败之前成功导入的信息将会重复。

使用虚拟设备控制台创建 vRealize Log Insight 的支持包

如果无法访问 vRealize Log Insight Web 用户界面，可以使用虚拟设备控制台或在与 vRealize Log Insight 虚拟设备建立 SSH 连接后下载支持包。

前提条件

- 验证是否拥有可登录 vRealize Log Insight 虚拟设备的 root 用户凭据。
- 如果计划使用 SSH 连接到 vRealize Log Insight 虚拟设备，请验证 TCP 端口 22 是否已打开。

步骤

- 1 与 vRealize Log InsightvApp 建立 SSH 连接，然后以 root 用户身份登录。
- 2 要生成支持包，请运行 `loginsight-support`。

要生成支持包并仅包含在某一时间段内发生更改的文件，请执行带 `--days` 限制的 `loginsight-support` 命令。例如，`--days=1` 仅包含在 1 天内发生更改的文件。

结果

支持信息收集和保存在具有以下命名约定的 `*.tar.gz` 文件中：`loginsight-support-YYYY-MM-DD_HHMMSS.xxxxxx.tar.gz`，其中，`xxxxxx` 是 `loginsight-support` 进程运行的进程 ID。

后续步骤

可根据请求将支持包转发到 VMware 支持服务。

重置管理员用户密码

如果管理员用户忘记 Web 用户界面的密码，该帐户将无法访问。

前提条件

- 验证是否拥有可登录 vRealize Log Insight 虚拟设备的 root 用户凭据。
- 要启用 SSH 连接，请验证是否已打开 TCP 端口 22。

问题

如果 vRealize Log Insight 只有一个管理员用户，并且该管理员用户忘记密码，将无法管理应用程序。如果管理员用户是 vRealize Log Insight 的唯一用户，将无法访问整个 Web 用户界面。

原因

如果用户不记得其当前密码，vRealize Log Insight 不会为管理员用户提供用于重置其自己密码的用户界面。

注 可以登录的管理员用户可以重置其他管理员用户的密码。仅当所有管理员用户帐户的密码均未知时，才可重置管理员用户密码。

解决方案

- 1 与 vRealize Log Insight 虚拟设备建立 SSH 连接，然后以 root 用户身份登录。
- 2 运行重置管理员用户密码的脚本：

```
li-reset-admin-passwd.sh
```

该脚本会重置管理员用户密码，生成新密码，并在屏幕上显示该新密码。

后续步骤

使用新密码登录到 vRealize Log Insight Web 用户界面，然后更改管理员用户密码。

重置 Root 用户密码

如果忘记 root 用户的密码，将无法再建立 SSH 连接或使用 vRealize Log Insight 虚拟设备控制台。

由于各种原因您可能无法以 root 身份登录，其中包括：

- 您尚未更改默认密码。默认情况下，vRealize Log Insight 将 root 用户的密码设置为空，并禁用 SSH 访问。一旦设置了密码，即为 root 用户启用 SSH 访问。
- 在部署 vRealize Log Insight 虚拟设备时设置了 SSH 密钥。如果通过 OVF 指定了 SSH 密钥，则禁用密码身份验证。使用设置的 SSH 密钥登录或参见以下解决方案中的步骤。
- 您多次输入了错误的密码，现在暂时被锁定。在这种情况下，在锁定期限结束前，即使输入了正确的密码也无法登录。您可以等待锁定期限结束，或重新启动虚拟设备。

由于 vRealize Log Insight 虚拟设备位于 Photon OS 上，以下步骤介绍了如何重置 Photon OS 计算机上的 root 密码。

问题

如果无法建立 SSH 连接或使用 vRealize Log Insight 虚拟设备控制台，将无法完成某些管理任务，也无法重置管理员用户的密码。

解决方案

- 1 重新启动运行 Photon OS 的 vRealize Log Insight 虚拟机。
- 2 当 Photon OS 重新启动并显示初始屏幕时，立即输入字母 e 以转到 GNU GRUB 编辑菜单。

注 由于 Photon OS 重新引导速度很快，因此，您将不会有太多时间输入 e。在 vSphere 和 Workstation 中，您可能需要通过单击控制台窗口以使该控制台获得焦点，然后它才能接受键盘输入。

- 3 在 GNU GRUB 编辑菜单中，在以 linux 开头的行的结尾处，输入一个空格并添加以下代码：

```
rw init=/bin/bash
```

- 4 按 F10 打开命令提示符。

5 运行以下命令：

```
passwd
```

6 按照说明输入并重新输入符合 Photon OS 密码复杂性规则的新 root 密码。确保记住该密码。

7 当您看到指示密码已更新的消息时，运行以下命令：

```
umount /
```

8 运行下列命令。

```
reboot -f
```

注 必须包含 -f 选项才能强制重新引导。否则，内核将进入应急状态。

后续步骤

重新引导 vRealize Log Insight 后，验证您是否可以使用新 root 用户密码登录。

无法向 vRealize Operations Manager 提交警示

如果无法向 vRealize Operations Manager 发送警示事件，vRealize Log Insight 会通知您。vRealize Log Insight 每分钟都会重试发送警示，直到问题解决。

问题

当无法向 vRealize Operations Manager 提交警示时，vRealize Log Insight 工具栏中会显示红色叹号标志。

原因

连接问题阻止 vRealize Operations Manager vRealize Log Insight 向 vRealize Operations Manager 发送警示通知。

解决方案

- ◆ 单击红色图标打开错误消息列表，然后向下滚动以查看最新消息。
打开错误消息列表或问题解决后，红色标志会从工具栏中消失。
- ◆ 要修复 vRealize Operations Manager 存在的连接问题，请尝试以下操作。
 - 验证 vRealize Operations Manager vApp 是否未关闭。
 - 通过 vRealize Log Insight Web 用户界面 **管理** 选项卡的 **vRealize Operations Manager** 部分中的 **测试连接** 按钮验证是否可以连接到 vRealize Operations Manager。
 - 通过直接登录到 vRealize Operations Manager 验证是否拥有正确凭据。
 - 检查 vRealize Log Insight 和 vRealize Operations Manager 日志中与连接问题相关的消息。
 - 验证在 vRealize Operations Manager vSphere 用户界面中是否未筛选出任何警示。

使用 Active Directory 凭据无法登录

使用 Active Directory 凭据时，无法登录到 vRealize Log Insight Web 用户界面。

问题

使用 Active Directory 域用户凭据无法登录到 vRealize Log Insight，尽管管理员用户已将您的 Active Directory 帐户添加到 vRealize Log Insight。

原因

最常见的原因是密码过期、凭据不正确、连接问题或 vRealize Log Insight 虚拟设备和 Active Directory 时钟之间缺乏同步。

解决方案

- 确保您的凭据有效，密码未过期，并且 Active Directory 帐户未锁定。
- 如果未指定使用 Active Directory 进行身份验证的域，请确认您在最新 vRealize Log Insight 配置（位置：`/storage/core/loginsight/config/loginsight-config.xml#[number]`，其中 `[number]` 是最大值）中存储的默认域上拥有帐户。
- 找到 `[number]` 最大的最新配置文件：`/storage/core/loginsight/config/loginsight-config.xml#[number]`。
- 验证 vRealize Log Insight 是否已连接到 Active Directory 服务器。
 - 转到 vRealize Log Insight Web 用户界面的**管理**选项卡的**身份验证**部分，填写用户凭据，然后单击**测试连接**按钮。
 - 检查 vRealize Log Insight `/var/log/vmware/loginsight/runtime.log` 中与 DNS 问题相关的消息。
- 验证 vRealize Log Insight 和 Active Directory 时钟是否已同步。
 - 检查 vRealize Log Insight `/var/log/vmware/loginsight/runtime.log` 中与时钟偏移相关的消息。
 - 使用 NTP 服务器同步 vRealize Log Insight 和 Active Directory 时钟。

SMTP 无法在启用 STARTTLS 选项的情况下使用

配置已启用 STARTTLS 选项的 SMTP 服务器时，测试电子邮件失败。将 SMTP 服务器的 SSL 证书添加到 Java 信任库以解决该问题。

前提条件

- 验证是否拥有可登录 vRealize Log Insight 虚拟设备的 root 用户凭据。
- 如果计划使用 SSH 连接到 vRealize Log Insight 虚拟设备，请验证 TCP 端口 22 是否已打开。

步骤

- 1 与 vRealize Log Insight vApp 建立 SSH 连接，然后以 root 用户身份登录。
- 2 将 SMTP 服务器的 SSL 证书复制到 vRealize Log Insight vApp。
- 3 运行下列命令。

```
`/usr/java/jre-vmware/bin/keytool -import -alias certificate_name -file  
path_to_certificate -keystore /usr/java/jre-vmware/lib/security/cacerts`
```

注 通过使用位于键盘上与波形符同一个键上的反引号符号插入外引号。请勿使用单引号。

- 4 输入默认密码 **changeit**。
- 5 运行 `service loginsight restart` 命令。

后续步骤

导航到**管理 > SMTP**，然后使用**发送测试电子邮件**测试您的设置。请参见为 [vRealize Log Insight 配置 SMTP 服务器](#)

由于无法验证 .pak 文件的签名，升级失败

vRealize Log Insight 由于 .pak 文件已损坏、许可证已过期或者磁盘空间不足，升级失败。

问题

升级 vRealize Log Insight 失败，将显示错误消息升级失败。无法升级：无法验证 PAK 文件的签名。

原因

可能导致错误的原因如下：

- 上载的文件不是 .pak 文件。
- 上载的 .pak 文件不完整。
- vRealize Log Insight 的许可证已过期。
- vRealize Log Insight 虚拟设备根文件系统的磁盘空间不足。

解决方案

- ◆ 验证您是否正在上载 .pak 文件。
- ◆ 对 VMware 下载站点验证 .pak 文件的 md5sum。
- ◆ 验证 vRealize Log Insight 上是否已配置至少一个有效的许可证。
- ◆ 登录到 vRealize Log Insight 虚拟设备，并运行 `df -h` 以检查可用磁盘空间。

注 不要将文件放置在 vRealize Log Insight 虚拟设备根文件系统中。

升级失败并显示内部服务器错误

vRealize Log Insight 由于连接问题导致升级失败，并显示内部服务器错误。

问题

升级 vRealize Log Insight 失败，将显示错误消息升级失败。内部服务器错误。

原因

客户端和服务端之间出现连接问题。例如，当您尝试从 WAN 上的客户端升级时，会出现该问题。

解决方案

- ◆ 请从与服务器位于同一 LAN 的客户端升级 LI。

与 VMware 产品集成后第一条日志消息中缺少 vmw_object_id 字段

将 vRealize Log Insight 与 VMware 产品集成后，第一条日志消息中不包含 vmw_object_id 字段。

问题

将 vRealize Log Insight 与 vCenter Server 和 vRealize Operations Manager 集成后收到的第一条日志消息中不包含关联的 vmw_object_id 字段。在将 vRealize Operations Manager 对象指定为警示目标时，缺少的字段可能会影响警示传送机制。

注 确保也已将 vCenter Server 与 vRealize Operations Manager 集成。

解决方案

等待两分钟。您收到的下一条日志消息中将包含 vmw_object_id 字段。