

# 管理 vRealize Log Insight

2022 年 5 月 24 日

vRealize Log Insight 8.3

您可以在 VMware 網站上找到最新的技術文件，網址如下：

<https://docs.vmware.com/tw/>

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

Copyright © 2022 VMware, Inc. 保留所有權利。 [版權與商標資訊](#)。

# 目錄

## 管理 vRealize Log Insight 7

### 1 升級 vRealize Log Insight 8

- vRealize Log Insight 升級路徑 8
- 升級至 vRealize Log Insight 8.3 或更早版本 8
- vRealize Log Insight 8.1 升級 9
- vRealize Log Insight 8.0 升級 10

### 2 管理 vRealize Log Insight 使用者帳戶 11

- 使用者管理概觀 11
- 角色型存取控制 12
- 使用篩選來管理使用者帳戶 12
- 建立使用者帳戶 12
- 解除鎖定使用者帳戶 14
- 為 vRealize Log Insight 設定 VMware Identity Manager 對 Active Directory 群組的存取權 15
- 將 Active Directory 群組匯入至 vRealize Log Insight 16
- 定義資料集 17
- 建立和修改角色 18
- 刪除使用者帳戶或群組 19

### 3 設定驗證 21

- 透過 VMware Identity Manager 啟用使用者驗證 21
- 透過 Active Directory 啟用使用者驗證 23
- 設定通訊協定以用於 Active Directory 24

### 4 設定 vRealize Log Insight 26

- vRealize Log Insight 組態限制 26
- 設定資料磁碟分割 28
- 進行虛擬應用裝置設定 28
  - 設定 vRealize Log Insight 虛擬應用裝置的根 SSH 密碼 28
  - 變更 vRealize Log Insight 虛擬應用裝置的網路設定 29
  - 增加 vRealize Log Insight 虛擬應用裝置的儲存容量 29
  - 將記憶體和 CPU 新增到 vRealize Log Insight 虛擬應用裝置 30
- 將授權指派給 vRealize Log Insight 31
- 記錄儲存區原則 32
- 管理系統通知 32
  - 系統通知 32

設定 vRealize Log Insight 系統通知的目的地	36
新增 vRealize Log Insight 事件轉送目的地	39
在互動式分析中使用事件轉送篩選器	41
同步 vRealize Log Insight 虛擬應用裝置的時間	42
為 vRealize Log Insight 設定 SMTP 伺服器	42
安裝自訂 SSL 憑證	43
產生自我簽署的憑證	45
產生憑證簽署要求	46
從憑證授權機構要求簽章	47
串連憑證檔案	47
上傳已簽署憑證	48
設定 vRealize Log Insight 伺服器與 Log Insight Agents 之間的 SSL 連線	48
檢視和移除 SSL 憑證	51
變更 vRealize Log Insight Web 工作階段的預設逾時期間	52
封存	52
在 vRealize Log Insight 中啟用或停用資料封存	52
vRealize Log Insight 封存檔的格式	54
將 vRealize Log Insight 封存檔匯入 vRealize Log Insight	54
將 Log Insight 封存檔匯出為原始文字檔或 JSON	55
重新啟動 vRealize Log Insight 服務	56
關閉 vRealize Log Insight 虛擬應用裝置的電源	57
下載 vRealize Log Insight 支援服務包	57
加入或退出 VMware 客戶經驗改進計劃	58
設定 vRealize Log Insight 的 STIG 合規性	59
啟用 vRealize Log Insight 的 FIPS 模式	59

## 5 管理 vRealize Log Insight 叢集 61

將工作節點新增到 vRealize Log Insight 叢集	61
部署 vRealize Log Insight 虛擬應用裝置	61
加入現有部署	63
從 vRealize Log Insight 叢集中移除工作節點	65
使用整合式負載平衡器	65
啟用整合式負載平衡器	66
查詢生產中叢集檢查的結果	67

## 6 設定、監控及更新 vRealize Log Insight 代理程式 69

集中式代理程式組態和代理程式群組	69
代理程式群組組態合併	70
建立代理程式群組	70
編輯代理程式群組	72
將內容套件代理程式群組新增為代理程式群組	72

刪除代理程式群組 73

監控 vRealize Log Insight 代理程式的狀態 73

從伺服器啟用代理程式自動更新 74

## 7 監控 vRealize Log Insight 75

檢查 vRealize Log Insight 虛擬應用裝置的健全狀況 75

監控傳送記錄事件的主機 76

設定系統通知以報告相關的非作用中主機 76

## 8 整合 vRealize Log Insight 與 VMware 產品 78

將 vRealize Log Insight 連線到 vSphere 環境 79

vRealize Log Insight 做為 Syslog 伺服器 80

設定 ESXi 主機將記錄事件轉送到 vRealize Log Insight 80

修改 ESXi 主機組態以便將記錄事件轉送至 vRealize Log Insight 82

vRealize Operations Manager 中的 vRealize Log Insight 通知事件 83

將 vRealize Log Insight 設定為從 vCenter Server 執行個體提取事件、工作和警示 84

搭配使用 vRealize Operations Manager 與 vRealize Log Insight 84

與 vRealize Operations Manager 整合的需求 85

設定 vRealize Log Insight，以將通知和度量傳送至 vRealize Operations Manager 86

在 vRealize Operations Manager 中為 vRealize Log Insight 啟用在環境定義中啟動 88

在 vRealize Operations Manager 中為 vRealize Log Insight 停用在環境定義中啟動 91

新增 DNS 搜尋路徑和網域 92

移除 vRealize Log Insight 介面卡 93

適用於 vRealize Log Insight 的 vRealize Operations Manager 內容套件 94

## 9 vRealize Log Insight 安全性考量 95

連接埠與外部介面 95

vRealize Log Insight 組態檔 96

vRealize Log Insight 公開金鑰、憑證和金鑰儲存區 97

vRealize Log Insight 授權和 EULA 檔案 97

vRealize Log Insight 記錄檔 98

為使用者稽核記錄訊息啟用偵錯層級 100

vRealize Log Insight 中的稽核記錄 100

vRealize Log Insight 使用者帳戶 101

vRealize Log Insight 防火牆建議 102

安全性更新和修補程式 102

## 10 備份、還原與災難復原 104

備份、還原和災難復原概觀 104

使用靜態 IP 位址和 FQDN 105

規劃和準備 105

備份節點和叢集	106
備份 Linux 或 Windows 代理程式	107
還原節點和叢集	108
還原後變更組態	108
還原至相同主機	109
還原至不同主機	109
確認還原	112
災害復原	112

## 11 疑難排解 vRealize Log Insight 113

無法在 Internet Explorer 上登入 vRealize Log Insight	113
vRealize Log Insight 磁碟空間不足	114
匯入封存資料可能會失敗	114
使用虛擬應用裝置主控台建立 vRealize Log Insight 支援服務包	114
重設 Admin 使用者密碼	115
重設根使用者密碼	116
無法將警示傳遞到 vRealize Operations Manager	117
無法使用 Active Directory 認證登入	118
啟用了 STARTTLS 選項時 SMTP 無法運作	118
升級失敗，因為無法驗證 .pak 檔案的簽章	119
升級失敗並顯示內部伺服器錯誤	120
與 VMware 產品整合後，第一個記錄訊息中遺失 vmw_object_id 欄位	120

# 管理 vRealize Log Insight

《管理 vRealize Log Insight》提供關於管理 VMware® vRealize™ Log Insight™ 的資訊，包括如何管理使用者帳戶以及如何設定與其他 VMware 產品的整合。其也包含關於管理產品安全性和升級您部署的資訊。

該資訊是針對熟悉虛擬機器技術和資料中心作業且富有經驗的 Windows 或 Linux 系統管理員而撰寫。

# 升級 vRealize Log Insight

# 1

您可以將 vRealize Log Insight 從 8.2 升級至 8.3 版、從 8.1 升級至 8.2，以及從 4.8 或 8.0 升級到 8.1。若要升級至 vRealize Log Insight 8.0 或更早版本，您必須採用漸進式升級。升級包括自動升級叢集中的節點。

若要下載 vRealize Log Insight 的 PAK 檔案，請前往[下載 VMware vRealize Log Insight](#) 頁面。

本章節討論下列主題：

- [vRealize Log Insight 升級路徑](#)
- [升級至 vRealize Log Insight 8.3 或更早版本](#)
- [vRealize Log Insight 8.1 升級](#)
- [vRealize Log Insight 8.0 升級](#)

## vRealize Log Insight 升級路徑

系統所遵循的升級路徑取決於已安裝的 vRealize Log Insight 版本，以及您所要升級的目標版本。

您可以將 vRealize Log Insight 從 8.2 升級至 8.3 版、從 8.1 升級至 8.2，以及從 4.8 或 8.0 升級到 8.1。升級至 vRealize Log Insight 8.0 或更早版本必須漸進式執行。例如，若要從 4.5 版升級到 4.7 版，則需要將 4.6 版升級套用至 4.5 版，然後從 4.6 版升級至 4.7 版。您必須升級至每個中繼版本。

您也可以[在 VMware 產品互通性對照表網站](#)上檢視支援的升級路徑。

## 升級至 vRealize Log Insight 8.3 或更早版本

您可以將叢集從 8.2 升級至 vRealize Log Insight 8.3 版、從 8.1 升級至 8.2、從 4.8 或 8.0 升級至 8.1。您必須將叢集漸進式升級至 4.0 版或更新版本，最高可至 8.0 版。例如，若要從 3.6 版升級至 4.3 版，請對 3.6 套用 4.0 升級，然後從 4.0 版升級至 4.3。

vRealize Log Insight 升級必須透過主要節點的 FQDN 完成。不支援使用整合式負載平衡器 IP 位址進行升級。

在升級期間，系統會先升級主要節點並重新啟動。每個叢集節點會依序升級。您可以在[管理員 > 叢集](#)頁面上看到漸進式升級的狀態。如果已設定整合負載平衡器，其 IP 會在叢集節點間移轉，使得叢集服務，包括 UI、API 和傳入事件的擷取，可在整個漸進式升級中保持可用。低層級詳細資料會寫入至每個個別節點上的檔案 `/storage/core/loginsight/var/upgrade.log`。升級成功完成時會傳送系統通知。



如果在升級程序期間遇到影響一或多個節點的問題，則整個叢集會復原到原始正常運作的版本。因為在升級開始之後執行的設定變更可能會不一致或無效，所有設定會還原為升級之前擷取的已知良好狀態。您不會遺失擷取的任何事件。進度會寫入至每個個別節點上的檔案 `/storage/core/loginsight/var/rollback.log`。復原完成時會傳送系統通知。調查並修正問題之後，您可以重試升級。

即便所有節點在升級之前處於維護模式，升級後都會處於連線狀態並上線。

#### 必要條件

- 確認您是否已將正確的升級套用至 vRealize Log Insight 版本。如需支援升級路徑的詳細資訊，請參閱 [vRealize Log Insight 升級路徑](#)。
- 建立 vRealize Log Insight 虛擬應用裝置的快照或備份複本。
- 取得您要升級的目標版本之 vRealize Log Insight 升級服務包 `.pak` 檔案的複本。
- 確認您已做為具有**編輯管理員**權限的使用者身分登入 vRealize Log Insight Web 使用者介面。URL 格式為 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虛擬應用裝置的 IP 位址或主機名稱。
- 記下您要升級且處於維護模式的任何節點。升級完成後，您必須將其從已連線狀態移至維護模式。

#### 程序

- 1 導覽至**管理**索引標籤。
- 2 在 [管理] 下，按一下**叢集**。
- 3 按一下從 **PAK 升級**以上傳 `.pak` 檔案。
- 4 接受新的使用者授權合約即完成升級程序。

#### 後續步驟

主要節點升級程序完成之後，您可以檢視其餘的自動升級程序。

檢查傳送給 Admin 的電子郵件，以確認升級已成功完成。

升級後，即便所有節點在升級之前處於維護模式仍會上線。您可視需要將這些節點移回維護模式。

## vRealize Log Insight 8.1 升級

您可以從 vRealize Log Insight 8.0 升級至 8.1，兩個版本均位於 Photon 作業系統。您也可以直接將 SLES 作業系統上的 vRealize Log Insight 4.8 升級至 Photon 作業系統上的 vRealize Log Insight 8.1。

### 從 vRealize Log Insight 8.0 升級至 8.1

從 vRealize Log Insight 8.0 升級至 8.1 不會變更 vRealize Log Insight 虛擬應用裝置的虛擬機器架構。唯一的變更是在目前開機的根磁碟分割，例如從 SDA4 到 SDA3，這對使用者體驗沒有任何影響。

如果升級至 vRealize Log Insight 8.1 失敗，則不會發生自動回復。不過，您可以進行手動回復來還原為舊版。如需詳細資訊，請參閱 <https://kb.vmware.com/s/article/75150>。使用者介面或 REST API 沒有任何變更。當您從命令列連線至 vRealize Log Insight 8.1 虛擬機器並開始進行作業時，您會看到以 `systemd` 型資訊，因為 Photon 是以 `systemd` 為基礎。

## 從 vRealize Log Insight 4.8 升級至 8.1

從 vRealize Log Insight 4.8 升級至 8.1 類似於從 4.8 升級至 8.0。如需詳細資訊，請參閱 [vRealize Log Insight 8.0 升級](#)。

如需升級至 vRealize Log Insight 8.1 的相關資訊，請參閱 [升級通知](#)。

如需升級程序的相關資訊，請參閱 [升級至 vRealize Log Insight 8.3 或更早版本](#)。

## vRealize Log Insight 8.0 升級

您可以將 SLES 作業系統上的 vRealize Log Insight 4.8 升級至 Photon 作業系統上的 vRealize Log Insight 8.0。

從 SLES 式 vRealize Log Insight 4.8 升級至 Photon 式 vRealize Log Insight 8.0 與先前的升級不同，因為基礎作業系統有所變更。此升級會變更 vRealize Log Insight 虛擬應用裝置中每個虛擬機器的架構。

例如，請考慮虛擬機器具有磁碟 SDA，其中有三個磁碟分割，用於開機 (SDA1)、交換 (SDA2) 和根 (SDA3)。磁碟分割 SDA3 的大小約為 16 GB，並且包含 SLES 的相關資訊。從 SLES 式的 vRealize Log Insight 4.8 升級至 Photon 式的 vRealize Log Insight 8.0 會在 SDA3 中建立另一個磁碟分割，並將其平均分割為兩個部分，每個部分的大小約為 8 GB - 一個用於 SLES (SDA3)，另一個則用於 Photon (SDA4)。SDA4 成為作用中的磁碟分割。SDA3 保持非作用中，但會包含 SLES 的有效 vRealize Log Insight 資訊。您可以在將虛擬機器開機時手動選取 SDA3 以將其開機。

---

**備註** 從以 SLES 為基礎的 vRealize Log Insight 4.8 升級至以 Photon 為基礎的 vRealize Log Insight 8.0 之前，請先確定根磁碟分割有足夠的空間可進行升級。如果根磁碟分割的大小不足 (例如，8 GB)，請將磁碟大小增加到 20 GB，使根磁碟分割大小增加到 16 GB。您必須為根磁碟分割空間較少的每個節點增加磁碟大小。如需增加根磁碟分割大小的相關資訊，請參閱 <https://kb.vmware.com/s/article/76304>。

升級至 Photon 式 vRealize Log Insight 8.0 之後：

- 使用者介面或 REST API 沒有任何變更。
  - 當您從命令列連線至 vRealize Log Insight 8.0 虛擬機器並開始進行作業時，您會看到以 `systemd` 為基礎的資訊，因為 SLES 是以 `initd` 為基礎，而 Photon 則是以 `systemd` 為基礎。
- 

如需升級至 vRealize Log Insight 8.0 的相關資訊，請參閱 [升級通知](#)。

如需升級程序的相關資訊，請參閱 [升級至 vRealize Log Insight 8.3 或更早版本](#)。

# 管理 vRealize Log Insight 使用者帳戶

## 2

管理員可建立使用者帳戶和角色，以提供對 vRealize Log Insight Web 介面的存取權。

只有具備編輯管理員權限的使用者才能建立和編輯使用者帳戶。但是，使用者無需編輯管理員權限就可變更其自己的電子郵件和帳戶密碼。

本章節討論下列主題：

- 使用者管理概觀
- 角色型存取控制
- 使用篩選來管理使用者帳戶
- 建立使用者帳戶
- 解除鎖定使用者帳戶
- 為 vRealize Log Insight 設定 VMware Identity Manager 對 Active Directory 群組的存取權
- 將 Active Directory 群組匯入至 vRealize Log Insight
- 定義資料集
- 建立和修改角色
- 刪除使用者帳戶或群組

## 使用者管理概觀

系統管理員結合使用使用者登入、角色型存取控制、權限和資料集，管理 vRealize Log Insight 使用者。角色型存取控制可讓管理員管理使用者及其可執行的工作。

角色是指執行特定工作所需的一組權限。系統管理員在定義安全性原則時定義角色，並將角色授與使用者。若要變更與特定角色相關聯的權限和工作，系統管理員需要更新角色設定。更新後的設定可用於與此角色相關聯的所有使用者。

- 若要允許使用者執行某項工作，系統管理員會將該角色授與該使用者。
- 若要阻止使用者執行某項工作，系統管理員會撤銷該使用者的角色。

每個使用者之存取、角色和權限的管理是以其使用者登入帳戶為基礎的。每個使用者可擁有多個角色和權限。

無法檢視或存取某些物件，或者無法執行某些作業的使用者，是因為未獲得執行這些動作的權限。

## 角色型存取控制

角色型存取控制會讓系統管理員限制對特定使用者的記錄存取權，並控制這些使用者登入後可執行的工作。系統管理員可以使用或從使用者登入帳戶中關聯或撤銷權限和角色。使用者可以查看其有權存取的所有儀表板，但儀表板和互動式分析中的資料會根據使用者角色有權存取的資料集進行篩選。

### 使用者

系統管理員可以透過將權限和角色授與使用者登入帳戶，或從使用者登入帳戶撤銷權限和角色，來控制每位使用者的存取權和動作。

### 權限

權限會控制 vRealize Log Insight 中允許的動作。權限會套用至 vRealize Log Insight 中的特定管理或使用者工作。例如，您可以授與**檢視管理**權限，以允許使用者檢視 vRealize Log Insight 管理設定。

### 資料集

資料集由一組篩選器組成。您可以將資料集與角色相關聯，以使用資料集為使用者提供對特定內容的存取權。

### 角色

角色即為可與使用者相關聯的權限和資料集的集合。角色提供了封裝執行工作所需之所有權限的便利方法。可為一個使用者指派多個角色。

## 使用篩選來管理使用者帳戶

您可以透過指定搜尋篩選來搜尋使用者或一組使用者。

您可透過**存取控制**頁面上的**使用者和群組**索引標籤來完成篩選。若要移至頁面，請在**管理**索引標籤上，按一下**管理**功能表下的**存取控制**，然後選取**使用者和群組**索引標籤。

搜尋文字方塊位於頁面的頂部附近，且包含字詞依照使用者名稱篩選。

搜尋功能會在您輸入時篩選結果，並傳回包含輸入模式的使用者名稱。例如，如果您擁有的使用者名為 John\_Smith、John\_Doe 和 Helen\_Jonson，當您輸入字母 **J** 時，搜尋會傳回所有包含該字母的使用者名稱，例如 John\_Smith、John\_Doe 和 Helen\_Jonson。若繼續輸入字母，則系統會縮小搜尋結果以符合確切模式。例如，當您輸入 **John\_** 時，搜尋會傳回 John\_Smith 和 John\_Doe。

您可以依下列欄位來排序搜尋結果：網域、驗證、角色、電子郵件或 UPN。此外，您可以在搜尋結果上執行大量動作，例如刪除多個使用者。

## 建立使用者帳戶

具有超級管理員角色的使用者可以建立使用者帳戶，以提供對 vRealize Log Insight Web 使用者介面的存取權。

## 必要條件

確認您已做為具有**編輯管理員**權限的使用者身分登入 vRealize Log Insight Web 使用者介面。URL 格式為 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虛擬應用裝置的 IP 位址或主機名稱。

如果您要建立使用這些驗證類型的使用者帳戶，請確認您已設定 VMware Identity Manager 或 Active Directory 支援。請參閱 [透過 VMware Identity Manager 啟用使用者驗證](#) 和 [透過 Active Directory 啟用使用者驗證](#)。

## 程序

- 1 導覽至**管理索引標籤**。
- 2 在 [管理] 下，按一下**存取控制**。
- 3 按一下**使用者和群組**。
- 4 按一下**新增使用者**。
- 5 執行下列其中一項作業：
  - 如果您要使用預設的內建驗證，請輸入使用者名稱和電子郵件地址。
  - 如果您要使用 Active Directory 或 VMware Identity Manager 驗證，請輸入使用者所屬的網域、使用者名稱，並選擇性地輸入使用者名稱帳戶的電子郵件地址。
- 6 在右側的**角色清單**中，選取一或多個預先定義或自訂使用者角色。

選項	說明
<b>使用者</b>	使用者可存取 vRealize Log Insight 的完整功能。您可以檢視記錄事件、執行查詢以搜尋和篩選記錄、將內容套件匯入其自己的使用者空間、新增警示查詢，以及管理您自己的使用者帳戶以變更密碼或電子郵件地址。無權存取管理選項的使用者不能與其他使用者共用內容、不能修改其他使用者的帳戶，並且不能從市集安裝內容套件。但是，可以將內容套件匯入只有您自己可以看見的使用者空間。
<b>儀表板使用者</b>	儀表板使用者只能使用 vRealize Log Insight 的 [儀表板] 頁面。
<b>僅檢視管理員</b>	檢視管理員使用者可以檢視管理員資訊、擁有完整使用者存取權，並且可以編輯共用內容。
<b>超級管理員</b>	超級管理員使用者可以存取 vRealize Log Insight 的完整功能、管理 vRealize Log Insight 以及所有其他使用者的帳戶。

- 7 按一下**儲存**。
  - 內建驗證的資訊會儲存在本機上。包含完成登錄連結的一封電子郵件隨即會傳送至使用者的電子郵件地址。使用者可以按一下連結，並輸入其帳戶的密碼。在使用者登錄其帳戶之前，帳戶狀態為擱置中。登錄後，帳戶狀態為作用中。

**備註** 使用者必須在收到登錄電子郵件的 24 小時內登錄其帳戶。如果沒有這麼做，其帳戶狀態會保持擱置中，且必須要求超級管理員使用者解除鎖定其帳戶。如需詳細資訊，請參閱[解除鎖定使用者帳戶](#)。

- 為使用 VMware Identity Manager 進行驗證，vRealize Log Insight 會驗證使用者的網域是否連結至群組。如果網域不屬於群組，vRealize Log Insight 會驗證該網域是否已與群組相關聯的網域建立信任。如果已建立跨網域信任，則使用者可以登入 vRealize Log Insight，而對應的使用者帳戶會新增至**存取控制 > 使用者和群組**的使用者表格。

## 解除鎖定使用者帳戶

如果使用者帳戶因無法在 24 小時內登錄而處於擱置中狀態，或者帳戶處於鎖定狀態，則超級管理員使用者可以解除鎖定該帳戶。

超級管理員使用者帳戶永遠不會遭到鎖定。其他使用者帳戶會在下列任一情況下鎖定：

- 使用者在 15 分鐘內連續輸入錯誤的密碼三次。
- 使用者未登入 vRealize Log Insight 達 35 天。此鎖定條件僅在已啟用密碼原則限制時有效。
- 使用者未變更其密碼達 60 天。此鎖定條件僅在已啟用密碼原則限制時有效。

如需啟用密碼原則限制的相關資訊，請參閱[設定 vRealize Log Insight 的 STIG 合規性](#)。

---

**備註** 此程序只會解除鎖定使用預設的內建驗證的帳戶，而非使用 VMware Identity Manager 或 Active Directory 驗證的帳戶。

---

### 必要條件

確認您已做為具有**編輯管理員**權限的使用者身分登入 vRealize Log Insight Web 使用者介面。URL 格式為 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虛擬應用裝置的 IP 位址或主機名稱。

### 程序

- 1 導覽至**管理**索引標籤。
- 2 在 [管理] 下，按一下**存取控制**。
- 3 按一下**使用者和群組**。
- 4 (選擇性) 對於鎖定的使用者帳戶，請指向**狀態**欄中的紅色鎖定圖示，以瞭解帳戶遭到鎖定的原因。
- 5 針對該帳戶的使用者名稱按一下鉛筆圖示。
- 6 選取**重設密碼**核取方塊 (如果尚未選取)。
- 7 按一下**儲存**。

### 結果

包含重設密碼連結的一封電子郵件隨即會傳送至使用者的電子郵件地址。使用者可以按一下連結，並輸入其帳戶的新密碼。

---

**備註** 使用者必須在收到該電子郵件的 24 小時內解除鎖定其帳戶。如果沒有這麼做，則必須再次要求超級管理員使用者解除鎖定其帳戶。

---

## 為 vRealize Log Insight 設定 VMware Identity Manager 對 Active Directory 群組的存取權

您可以使用 Active Directory 群組搭配 vRealize Log Insight 來通過 VMware Identity Manager 單一登入驗證。您的站台必須設定為使用針對 Active Directory 支援啟用的 VMware Identity Manager 驗證，且必須具備伺服器同步化。

您也必須將群組資訊匯入至 vRealize Log Insight。

VMware Identity Manager 使用者除了繼承指派給個別使用者的角色之外，還繼承指派給使用者所屬之任意群組的角色。例如，管理員可將群組 A 指派給**檢視管理員**角色，將使用者指派給**使用者**角色。還可以將同一位使用者指派給群組 A。當使用者登入時，便會繼承具有**檢視管理員**和**使用者**角色權限的群組角色。

此群組不是 VMware Identity Manager 本機群組，而是與 VMware Identity Manager 同步化的 Active Directory 群組。

### 必要條件

- 確認您已設定 UPN 屬性 (userPrincipalName) 屬性。可以透過 VMware Identity Manager 管理員介面來設定，位於**身分識別與存取管理 > 使用者屬性**中。
- 確認您已做為具有**編輯管理員**權限的使用者身分登入 vRealize Log Insight Web 使用者介面。URL 格式為 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虛擬應用裝置的 IP 位址或主機名稱。
- 確認您已在 vRealize Log Insight 中設定 VMware Identity Manager 支援。請參閱[透過 VMware Identity Manager 啟用使用者驗證](#)

### 程序

- 1 導覽至**管理索引標籤**。
- 2 在 [管理] 下，按一下**存取控制**。
- 3 按一下**使用者和群組**。
- 4 捲動至 [目錄群組] 表格，然後按一下**新增群組**。
- 5 從**類型**下拉式功能表中選取 **VMware Identity Manager**。

您在設定 VMware Identity Manager 支援時指定的預設網域名稱，會出現在**網域**文字方塊中。

- 6 將網域名稱變更為群組的 Active Directory 名稱。
- 7 輸入要新增之群組的名稱。



8 在右側的**角色清單**中，選取一或多個預先定義或自訂使用者角色。

選項	說明
<b>使用者</b>	使用者可存取 vRealize Log Insight 的完整功能。您可以檢視記錄事件、執行查詢以搜尋和篩選記錄、將內容套件匯入其自己的使用者空間、新增警示查詢，以及管理您自己的使用者帳戶以變更密碼或電子郵件地址。無權存取管理選項的使用者不能與其他使用者共用內容、不能修改其他使用者的帳戶，並且不能從市集安裝內容套件。但是，可以將內容套件匯入只有您自己可以看見的使用者空間。
<b>儀表板使用者</b>	儀表板使用者只能使用 vRealize Log Insight 的 [儀表板] 頁面。
<b>僅檢視管理員</b>	檢視管理員使用者可以檢視管理員資訊、擁有完整使用者存取權，並且可以編輯共用內容。
<b>超級管理員</b>	超級管理員使用者可以存取 vRealize Log Insight 的完整功能、管理 vRealize Log Insight 以及所有其他使用者的帳戶。

9 按一下**儲存**。

為進行驗證，vRealize Log Insight 會驗證使用者的網域是否連結至群組。如果網域不屬於群組，vRealize Log Insight 會驗證該網域是否已與群組相關聯的網域建立信任。如果已建立跨網域信任，則使用者可以登入 vRealize Log Insight，而對應的使用者帳戶會新增至**存取控制 > 使用者和群組**的使用者表格。

#### 結果

屬於您新增之群組的使用者可以使用其 VMware Identity Manager 帳戶登入 vRealize Log Insight，並擁有與他們所屬群組相同層級的權限。

## 將 Active Directory 群組匯入至 vRealize Log Insight

除了新增個別網域使用者，您可以新增網域群組以允許使用者登入 vRealize Log Insight。

在 vRealize Log Insight 中啟用 AD 支援時，可設定網域名稱並提供屬於該網域的繫結使用者。vRealize Log Insight 會使用該繫結使用者來驗證與 AD 網域的連線，並確認 AD 使用者和群組是否存在。

您新增到 vRealize Log Insight 的 Active Director 群組必須屬於繫結使用者的網域，或屬於繫結使用者的網域所信任的網域。

Active Directory 使用者除了繼承指派給個別使用者的角色之外，還繼承指派給使用者所屬之任意群組的角色。例如，管理員可將 GroupA 指派給**檢視管理員**角色，將使用者 Bob 指派給**使用者**角色。也可將 Bob 指派至 GroupA。Bob 登入時，會繼承群組角色並同時擁有**檢視管理員**和**使用者**角色的權限。

#### 必要條件

- 確認您已做為具有**編輯管理員**權限的使用者身分登入 vRealize Log Insight Web 使用者介面。URL 格式為 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虛擬應用裝置的 IP 位址或主機名稱。
- 確認您已設定 AD 支援。請參閱[透過 Active Directory 啟用使用者驗證](#)



## 程序

- 1 導覽至**管理**索引標籤。
- 2 在 [管理] 下，按一下**存取控制**。
- 3 按一下**使用者和群組**。
- 4 在 [目錄群組] 下，按一下**新增群組**。
- 5 按一下**類型**下拉式功能表中的 Active Directory。

您在設定 Active Directory 支援時指定的預設網域名稱，會出現在**網域**文字方塊中。如果您要從此預設網域新增群組，請勿修改網域名稱。

- 6 (選擇性) 如果想要從信任此預設網域的網域新增群組，請在**網域**文字方塊中輸入信任網域的名稱。
- 7 輸入要新增之群組的名稱。
- 8 在右側的**角色**清單中，選取一或多個預先定義或自訂使用者角色。

選項	說明
<b>使用者</b>	使用者可存取 vRealize Log Insight 的完整功能。您可以檢視記錄事件、執行查詢以搜尋和篩選記錄、將內容套件匯入其自己的使用者空間、新增警示查詢，以及管理您自己的使用者帳戶以變更密碼或電子郵件地址。無權存取管理選項的使用者不能與其他使用者共用內容、不能修改其他使用者的帳戶，並且不能從市集安裝內容套件。但是，可以將內容套件匯入只有您自己可以看見的使用者空間。
<b>儀表板使用者</b>	儀表板使用者只能使用 vRealize Log Insight 的 [儀表板] 頁面。
<b>僅檢視管理員</b>	檢視管理員使用者可以檢視管理員資訊、擁有完整使用者存取權，並且可以編輯共用內容。
<b>超級管理員</b>	超級管理員使用者可以存取 vRealize Log Insight 的完整功能、管理 vRealize Log Insight 以及所有其他使用者的帳戶。

- 9 按一下**儲存**。

vRealize Log Insight 會確認您指定的網域或信任的網域中是否存在 AD 群組。如果找不到該群組，系統會顯示對話方塊，通知您 vRealize Log Insight 無法驗證該群組。您可以儲存群組而不驗證，或取消以更正群組名稱。

## 結果

屬於您新增之 Active Directory 群組的使用者可以使用其網域帳戶登入 vRealize Log Insight，並擁有與其所屬群組相同層級的權限。

## 定義資料集

您可以定義資料集以向使用者提供特定內容的存取權。

資料集不支援文字型限制。

## 必要條件

確認您已做為具有**編輯管理員**權限的使用者身分登入 vRealize Log Insight Web 使用者介面。URL 格式為 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虛擬應用裝置的 IP 位址或主機名稱。

## 程序

- 1 導覽至**管理索引標籤**。
- 2 在 [管理] 下，按一下**存取控制**。
- 3 按一下**資料集**。
- 4 按一下**新增資料集**。
- 5 按一下**新增篩選器**。
- 6 使用第一個下拉式功能表選取 vRealize Log Insight 中所定義的欄位，據以進行篩選。

例如，**主機名稱**。

該清單僅包含靜態欄位並排除已擷取、使用者共用的欄位和文字欄位，以及透過 `event_type` 篩選器建立的欄位。

---

**備註** 數值欄位包含字串欄位中沒有的其他運算子：`=`、`>`、`<`、`>=` 和 `<=`。這些運算子可比較數值。使用這些運算子與使用字串運算子得到的結果會有所不同。例如，篩選器 `response_time=02` 會將包含 `response_time` 欄位的事件與值 2 相比對。篩選器 `response_time 包含 02` 沒有相同的相符項。

---

- 7 使用第二個下拉式功能表選取要套用到在第一個下拉式功能表中選取之欄位的運算。
  - 8 在篩選器下拉式功能表右側的篩選器方塊中，輸入要做為篩選器的值。
- 您可以使用多個值。這些值之間的運算子為 `OR`。

---

**備註** 如果在第二個下拉式功能表中選取**存在**運算子，則無法使用此方塊。

---

- 9 (選擇性) 若要新增更多篩選器，請按一下**新增篩選器**。
- 10 (選擇性) 若要確認篩選行為符合您的需要，請按一下**在互動式分析中執行**，這會開啟互動式分析視窗，其中包含與您的篩選器相符的資料。
- 11 按一下**儲存**。

## 後續步驟

將資料集與使用者角色相關聯。請參閱[建立和修改角色](#)。



## 建立和修改角色

您可以建立自訂角色或修改預先定義的角色，以允許使用者執行特定工作或存取特定內容。

### 必要條件

確認您已做為具有**編輯管理員**權限的使用者身分登入 vRealize Log Insight Web 使用者介面。URL 格式為 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虛擬應用裝置的 IP 位址或主機名稱。

### 程序

- 1 導覽至**管理索引標籤**。
- 2 在 [管理] 下，按一下**存取控制**。
- 3 按一下**角色**。
- 4 按一下**新增角色**或   來編輯現有角色。

您必須先複製「超級管理員」和「使用者」角色，然後才能加以編輯。

- 5 修改**名稱**和**說明文字**方塊。
- 6 從 [權限] 清單中選取一或多個權限。

選項	說明
編輯 Admin	可以編輯 Admin 資訊和設定
檢視 Admin	可以檢視 Admin 資訊和設定
編輯共用	可以編輯共用內容
分析	可以使用「互動式分析」
儀表板	可以檢視「儀表板」

- 7 (選擇性) 從右側的**資料集**清單中，選取要與使用者角色相關聯的資料集。
- 8 按一下**儲存**。

## 刪除使用者帳戶或群組

您可以從 vRealize Log Insight 管理使用者介面刪除使用者帳戶或群組。

使用者帳戶和群組會列於 [存取控制] 頁面上的個別表格中。您可以使用搜尋篩選器來尋找特定的使用者帳戶。刪除群組時，屬於該群組的所有使用者會失去群組對其授與的權限。

### 必要條件

確認您已做為具有**編輯管理員**權限的使用者身分登入 vRealize Log Insight Web 使用者介面。URL 格式為 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虛擬應用裝置的 IP 位址或主機名稱。

### 程序

- 1 導覽至**管理索引標籤**。
- 2 在 [管理] 下，按一下**存取控制**。

- 3 按一下**使用者和群組**。
- 4 選取欲刪除之使用者名稱或群組旁的核取方塊。
- 5 若要移除帳戶或群組，請按一下 [使用者帳戶] 或 [群組] 表格上方的 **X 刪除**。

您可以使用多種驗證方法來搭配您的部署。

驗證方法包括本機驗證、VMware Identity Manager 驗證和 Active Directory 驗證。您可以在相同部署中使用多個方法，然後使用者可以選取要在登入時使用的驗證類型。

vRealize Log Insight 的下載頁面包括適當 VMware Identity Manager 版本的下載連結。VMware Identity Manager 包含下列功能。

- 可對現有目錄 (例如 Active Directory 或 LDAP) 驗證使用者的目錄整合。
- 與其他也支援 Single Sign-On 功能的 VMware 產品進行 Single Sign-On 整合。
- 可與數個第三方身分識別提供者 (例如 ADFS、Ping Federate 和其他等) 進行 Single Sign-On。
- 透過與第三方軟體整合 (例如 RSA SecurID、Entrust 和其他等) 以提供雙因素驗證。包含使用 VMware Verify 的雙重要素驗證。

本機驗證是 vRealize Log Insight 的元件。若要加以使用，您必須建立儲存在 vRealize Log Insight 伺服器上的本機使用者和密碼。產品管理員必須啟用 vRealize Log Insight 和 Active Directory。

本章節討論下列主題：

- [透過 VMware Identity Manager 啟用使用者驗證](#)
- [透過 Active Directory 啟用使用者驗證](#)

## 透過 VMware Identity Manager 啟用使用者驗證

經管理員啟用後，VMware Identity Manager 驗證可與 vRealize Log Insight 搭配使用。

透過 VMware Identity Manager 驗證，使用者將可對所有使用相同 Identity Manager 的 VMware 產品使用 Single Sign-On。

當 Active Directory 與 VMware Identity Manager 伺服器已進行同步時，Active Directory 使用者也可以透過 VMware Identity Manager 驗證。如需同步的詳細資訊，請參閱 VMware Identity Manager 說明文件。

與 VMware Identity Manager 的整合僅能對本機使用者進行。受指派 VMware Identity Manager 中租用戶管理員角色的 Active Directory 使用者不符合與 vRealize Log Insight 整合的資格。

## 必要條件

確認您已做為具有**編輯管理員**權限的使用者身分登入 vRealize Log Insight Web 使用者介面。URL 格式為 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虛擬應用裝置的 IP 位址或主機名稱。

## 程序

- 1 導覽至**管理索引**標籤。
- 2 在 [組態] 下，按一下**驗證**。
- 3 選取**啟用 Single Sign-On**。
- 4 在**主機**文字方塊中，輸入 VMware Identity Manager 執行個體用來驗證使用者的主機識別碼。  
例如 `company-name.vmwareidentity.com`。
- 5 在 **API 連接埠**文字方塊中，指定用來連線至 VMware Identity Manager 執行個體的連接埠。預設值為 443。
- 6 選擇性地輸入 VMware Identity Manager 承租人。只有在 VMware Identity Manager 中的承租人模式設定為 `tenant-in-path` 時，才需要此項目。
- 7 在**使用者名稱和密碼**文字方塊中指定 VMware Identity Manager 使用者認證。  
這項資訊只會在 VMware Identity Manager 上建立 vRealize Log Insight 用戶端的設定期間使用一次，且不會儲存在 vRealize Log Insight 的本機上。使用者必須具有對承租人執行 API 命令的權限。
- 8 按一下**測試連線**，以確認連線可運作。
- 9 如果 VMware Identity Manager 執行個體提供了不受信任的 SSL 憑證，則會有對話方塊顯示憑證的詳細資料。按一下**接受**，將憑證新增至 vRealize Log Insight 叢集中所有節點的信任存放區。  
如果您按一下**取消**，則憑證不會新增至信任存放區，且與 VMware Identity Manager 執行個體的連線將會失敗。您必須接受憑證才能成功連線。
- 10 在**重新導向 URL 主機**下拉式功能表中，選取要在 [重新導向 URL] 中用於在 VMware Identity Manager 登錄的主機名稱或 IP。  
如果為整合式負載平衡器至少定義了一個虛擬 IP，VMware Identity Manager 將會重新導向至選取的 VIP。如果未設定整合式負載平衡器，則會改用主要節點的 IP 位址。
- 11 選取是否要允許 Active Directory 使用者透過 VMware Identity Manager 進行登入的支援。  
當 VMware Identity Manager 與 Active Directory 執行個體同步化時，則可以為 Active Directory 使用者使用此選項。
- 12 按一下**儲存**。  
如果您並未測試連線，且 VMware Identity Manager 執行個體提供的憑證不受信任，請依照步驟 9 中的指示操作。

## 透過 Active Directory 啟用使用者驗證

您可以透過 Active Directory 來驗證使用者，讓使用者將一個通用密碼用於多種用途，簡化登入程序。

不支援透過 Active Directory 的子網域存取。此類型的存取僅支援透過 VMware Identity Manager。

### 必要條件

確認您已做為具有**編輯管理員**權限的使用者身分登入 vRealize Log Insight Web 使用者介面。URL 格式為 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虛擬應用裝置的 IP 位址或主機名稱。

### 程序

- 1 導覽至**管理索引標籤**。
- 2 在 [組態] 下，按一下**驗證**。
- 3 選取**啟用 Active Directory 支援**。
- 4 在**預設網域**文字方塊中，輸入網域名稱。

例如，`company-name.com`。

---

**備註** 您不能在預設網域文字方塊中列出多個網域。如果您指定的預設網域受其他網域信任，則 vRealize Log Insight 會使用預設網域和繫結使用者來驗證信任網域中的 Active Directory 使用者和群組。不支援使用 Active Directory 的子網域存取。

如果您切換至已包含使用者和群組的不同網域，則針對現有使用者和群組的驗證會失敗，且現有使用者儲存的資料會遺失。

---

- 5 如果您具有地理定位或安全管制的網域控制站，請手動指定最接近此 vRealize Log Insight 執行個體的網域控制站。

---

**備註** 不支援負載平衡的 Active Directory 授權伺服器。

---

- 6 輸入屬於預設網域之繫結使用者的認證。

vRealize Log Insight 會使用預設網域和繫結使用者來驗證預設網域及信任該預設網域之網域中的 AD 使用者和群組。

- 7 指定連線類型的值。

此連線會用於 Active Directory 驗證。

- 8 按一下**測試連線**，以確認連線可運作。

- 9 如果 Active Directory 伺服器提供了不受信任的 SSL 憑證，則會有對話方塊顯示憑證的詳細資料。按一下**接受**，將憑證新增至 vRealize Log Insight 叢集中所有節點的信任存放區。

如果您按一下**取消**，則憑證不會新增至信任存放區，且與 Active Directory 伺服器的連線將會失敗。您必須接受憑證才能成功連線。

## 10 按一下儲存。

如果您並未測試連線，且 Active Directory 伺服器提供的憑證不受信任，請依照步驟 9 中的指示操作。

### 後續步驟

將權限授與 Active Directory 使用者和群組，以存取 vRealize Log Insight 的目前執行個體。

## 設定通訊協定以用於 Active Directory

您可以設定連線至 Active Directory 時要使用的通訊協定。依預設，當 vRealize Log Insight 連線到 Active Directory 時，會先嘗試 SSL LDAP，然後才是非 SSL LDAP (如有必要)。

如果想要限制 Active Directory 與某個特定通訊協定的通訊，或想要變更嘗試通訊協定的順序，您必須在 vRealize Log Insight 虛擬應用裝置中套用其他組態。

### 必要條件

- 確認您具有根使用者認證以登入 vRealize Log Insight 虛擬應用裝置。
- 若要啟用 SSH 連線，請確認 TCP 連接埠 22 為開啟狀態。

### 程序

- 1 建立與 vRealize Log Insight 虛擬應用裝置的 SSH 連線並以根使用者身分登入。
- 2 導覽到下列位置：`/storage/core/loginsight/config`
- 3 找出最新組態檔，其中 [number] 為最大：`/storage/core/loginsight/config/loginsight-config.xml#[number]`
- 4 複製最新組態檔：`/storage/core/loginsight/config/loginsight-config.xml#[number]`
- 5 增加 [number] 並儲存至下列位置：`/storage/core/loginsight/config/loginsight-config.xml#[number + 1]`
- 6 開啟檔案進行編輯。
- 7 在 Authentication 區段中，新增與想要套用之組態對應的行：

選項	說明
<code>&lt;ad-protocols value="LDAP" /&gt;</code>	明確使用不具有 SSL 的 LDAP
<code>&lt;ad-protocols value="LDAPS" /&gt;</code>	明確使用僅具有 SSL 的 LDAP
<code>&lt;ad-protocols value="LDAP,LDAPS" /&gt;</code>	明確先使用 LDAP，然後使用具有 SSL 的 LDAP。
<code>&lt;ad-protocols value="LDAPS,LDAP" /&gt;</code>	明確先使用 LDAPS，然後使用不具有 SSL 的 LDAP

當您未選取通訊協定時，vRealize Log Insight 會嘗試先使用 LDAP，然後使用具有 SSL 的 LDAP。

- 8 儲存並關閉該檔案。



9 執行 `service loginsight restart` 命令。

# 設定 vRealize Log Insight

# 4

您可以設定和自訂 vRealize Log Insight 以變更預設設定、網路設定，以及修改儲存資源。您也可以設定系統通知。

本章節討論下列主題：

- vRealize Log Insight 組態限制
- 設定資料磁碟分割
- 進行虛擬應用裝置設定
- 將授權指派給 vRealize Log Insight
- 記錄儲存區原則
- 管理系統通知
- 新增 vRealize Log Insight 事件轉送目的地
- 同步 vRealize Log Insight 虛擬應用裝置的時間
- 為 vRealize Log Insight 設定 SMTP 伺服器
- 安裝自訂 SSL 憑證
- 檢視和移除 SSL 憑證
- 變更 vRealize Log Insight Web 工作階段的預設逾時期間
- 封存
- 重新啟動 vRealize Log Insight 服務
- 關閉 vRealize Log Insight 虛擬應用裝置的電源
- 下載 vRealize Log Insight 支援服務包
- 加入或退出 VMware 客戶經驗改進計劃
- 設定 vRealize Log Insight 的 STIG 合規性
- 啟用 vRealize Log Insight 的 FIPS 模式

## vRealize Log Insight 組態限制

設定 vRealize Log Insight 時，您必須保持或低於支援上限。

表 4-1. vRealize Log Insight 組態上限

項目	上限
<b>節點組態</b>	
CPU	16 個 vCPU
記憶體	32 GB
儲存裝置 (vmdk)	2 TB - 512 位元組
可定址儲存區總計	4 TB (+ 作業系統磁碟機) 虛擬機器磁碟 (VMDK) 的可定址記錄儲存區上限為 4 TB，每一個磁碟的大小上限為 2 TB。您可以配置兩個 2 TB 的 VMDK，或是四個 1 TB 的 VMDK，以此類推。在達到上限時，您必須向外延展叢集的規模大小，而不是在現有的虛擬機器新增更多磁碟。
Syslog 連線	750
<b>叢集組態</b>	
節點	18 (1 個主要節點 + 17 個工作節點)
虛擬 IP 位址	12
<b>每節點擷取數</b>	
每秒事件數	15,000 eps
Syslog 訊息長度	10 KB (文字欄位)
擷取 API HTTP POST 要求	16 KB (文字欄位)；每 HTTP Post 要求 4 MB
<b>整合</b>	
vRealize Operations Manager	1
vSphere vCenter Server	每個節點 15 個
Active Directory 網域	1
電子郵件伺服器	1
DNS 伺服器	2
NTP 伺服器	4
轉送站	10
<b>資料磁碟分割組態</b>	
資料磁碟分割	5

## 設定資料磁碟分割

您可以利用篩選器和保留期間將記錄資料保留在磁碟分割中。資料磁碟分割可讓您針對不同類型的記錄定義不同的保留期間。例如，包含敏感資訊的記錄可能需要的保留期間較短，例如五天。

與資料磁碟分割篩選準則相符的記錄資料會儲存在指定保留期間的磁碟分割中。與任何已定義資料磁碟分割中的篩選準則不相符的記錄會儲存在預設的磁碟分割中。此磁碟分割一律會啟用並儲存無限長時間的資料。您可以修改預設磁碟分割的保留期間。

---

**備註** 您最多可以建立 5 個資料磁碟分割。

---

### 必要條件

確認您已做為具有**編輯管理員**權限的使用者身分登入 vRealize Log Insight Web 使用者介面。URL 格式為 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虛擬應用裝置的 IP 位址或主機名稱。

### 程序

- 1 導覽至**管理索引標籤**。
- 2 在 [管理] 下方，按一下**磁碟分割**。  
此頁面中會列出現有的資料磁碟分割。針對每個資料磁碟分割，系統會顯示磁碟分割是否已啟用、篩選準則、保留期間、已使用的儲存空間，以及擷取第一筆記錄的時間等相關資訊。
- 3 按一下**新增磁碟分割**。
- 4 在**磁碟分割名稱**文字方塊中，輸入資料磁碟分割的名稱。
- 5 新增一或多個篩選器，以縮小要儲存在資料磁碟分割中的記錄。您可以選擇性地按一下在**互動式分析中執行**，以預覽已篩選的記錄結果。
- 6 在**保留期間**文字方塊中，輸入要在資料磁碟分割中保留記錄的天數。輸入 0 則不會限制保留期間。
- 7 使用**已啟用**切換按鈕，以啟用或停用資料磁碟分割。
- 8 按一下**儲存**。

## 進行虛擬應用裝置設定

您可以修改虛擬應用裝置設定，包括儲存區容量以及記憶體或 CPU 容量。

### 設定 vRealize Log Insight 虛擬應用裝置的根 SSH 密碼

與虛擬應用裝置的 SSH 連線預設為停用狀態。您可以從 VMware Remote Console 或在您部署 vRealize Log Insight 虛擬應用裝置時設定根 SSH 密碼。

最佳做法是在部署 vRealize Log Insight .ova 檔案時設定根 SSH 密碼。如需詳細資訊，請參閱[部署 vRealize Log Insight 虛擬應用裝置](#)。

您也可以從 VMware Remote Console 啟用 SSH 並設定根密碼。

### 必要條件

確認 vRealize Log Insight 虛擬應用裝置已部署並正在執行中。

### 程序

- 1 在 vSphere Client 詳細目錄中，按一下 vRealize Log Insight 虛擬應用裝置，然後開啟**主控台**索引標籤。
- 2 依照啟動顯示畫面上指定的組合鍵，前往命令列。
- 3 在主控台中，輸入 `root`，然後按 Enter。將密碼保留空白，然後按 Enter。

主控台中將顯示以下訊息：要求變更密碼。選擇新密碼。

- 4 將舊密碼保留空白，然後按 Enter。
- 5 輸入根使用者的新密碼，按 Enter，再次輸入根使用者的新密碼，然後按 Enter。

密碼必須至少由 8 個字元組成，並且必須至少包括一個大寫字母、一個小寫字母、一個數字和一個特殊字元。不得重複使用同一字元超過四次。

### 結果

此時將顯示以下訊息：密碼已變更。

### 後續步驟

您可以使用根密碼來建立與 vRealize Log Insight 虛擬應用裝置的 SSH 連線。

## 變更 vRealize Log Insight 虛擬應用裝置的網路設定

您可以依照 <https://kb.vmware.com/s/article/87992> 中所述的步驟來變更 vRealize Log Insight 虛擬應用裝置的網路設定。

## 增加 vRealize Log Insight 虛擬應用裝置的儲存容量

您可以隨自身需求的增長來增加配置給 vRealize Log Insight 的儲存資源。

向 vRealize Log Insight 虛擬應用裝置新增虛擬磁碟來增加儲存空間。您可以視需要新增磁碟，可定址儲存區總計最多達 4 TB (加上 OS 磁碟機)。總計可以是兩個 2 TB 磁碟或四個 1 TB 磁碟的組合，依此類推。請參閱 [vRealize Log Insight 組態限制](#)。

在 vRealize Log Insight 叢集中，您必須將相同數量的儲存區新增至叢集中的每個節點。

### 必要條件

- 以擁有修改環境中虛擬機器硬體權限的使用者身分登入 vSphere Client。
- 安全地關閉 vRealize Log Insight 虛擬應用裝置。請參閱[關閉 vRealize Log Insight 虛擬應用裝置的電源](#)

## 程序

- 1 在 vSphere Client 詳細目錄中的 vRealize Log Insight 虛擬機器上按一下滑鼠右鍵，然後選取**編輯設定**。
- 2 在**硬體索引**標籤上，按一下**新增**。
- 3 選取**硬碟**，然後按**下一步**。
- 4 選取**建立新的虛擬磁碟**，然後按**下一步**。

- a 輸入磁碟容量。

vRealize Log Insight 支援最多 2 TB 的虛擬硬碟。如果您需要更多容量，請新增多個虛擬硬碟。

- b 選取磁碟格式。

選項	說明
完整佈建消極式歸零	以預設的完整格式建立虛擬磁碟。虛擬磁碟所需的空間會在虛擬磁碟建立時進行配置。建立過程中不會清除實體裝置上的資料，但之後首次從虛擬應用裝置寫入後，可依需要將這些資料歸零。
完整佈建積極式歸零	建立一種支援叢集功能 (例如 Fault Tolerance) 的完整虛擬磁碟。虛擬磁碟所需的空間會在建立時進行配置。與一般格式相反，建立虛擬磁碟時，會將實體裝置上的資料歸零。建立此類格式的磁碟所需的時間可能會比建立其他類型的磁碟久得多。 儘可能建立完整佈建積極式歸零磁碟，以便 vRealize Log Insight 虛擬應用裝置效能更佳及運作更順暢。
精簡佈建	以精簡格式建立磁碟。使用此格式可節省儲存空間。

- c (必要) 若要選取資料存放區，請瀏覽至資料存放區位置，然後按**下一步**。

- 5 接受預設虛擬裝置節點，然後按**下一步**。
- 6 檢閱資訊，然後按一下**完成**。
- 7 按一下**確定**，儲存變更並關閉對話方塊。

## 結果

開啟 vRealize Log Insight 虛擬應用裝置的電源時，虛擬機器會探索新的虛擬磁碟，並自動將其新增到預設的資料磁碟區。請先完全關閉虛擬機器的電源。如需開啟虛擬應用裝置電源的相關資訊，請參閱 <https://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-6-pubs.html>。

**注意** 將磁碟新增到虛擬應用裝置後，便無法將其安全移除。從 vRealize Log Insight 虛擬應用裝置移除磁碟可能會導致整體資料遺失。

## 將記憶體和 CPU 新增到 vRealize Log Insight 虛擬應用裝置

您可以在部署後變更為 vRealize Log Insight 虛擬應用裝置配置的記憶體和 CPU 數量。

例如，如果環境中的事件數目增加，您可能需要調整資源配置。

### 必要條件

- 以擁有修改環境中虛擬機器硬體權限的使用者身分登入 vSphere Client。
- 安全地關閉 vRealize Log Insight 虛擬應用裝置。請參閱[關閉 vRealize Log Insight 虛擬應用裝置的電源](#)

### 程序

- 1 在 vSphere Client 詳細目錄中的 vRealize Log Insight 虛擬機器上按一下滑鼠右鍵，然後選取**編輯設定**。
- 2 在**硬體**索引標籤上，按一下**新增**。
- 3 視需要調整 CPU 和記憶體數量。
- 4 檢閱資訊，然後按一下**完成**。
- 5 按一下**確定**，儲存變更並關閉對話方塊。

### 結果

開啟 vRealize Log Insight 虛擬應用裝置電源時，虛擬機器將開始利用新的資源。

## 將授權指派給 vRealize Log Insight

您只能透過有效的授權金鑰使用 vRealize Log Insight。

當您從 VMware 網站下載 vRealize Log Insight 時，會取得一個評估授權。此授權的有效期為 60 天。當評估授權到期時，您必須指派一個永久授權才能繼續使用 vRealize Log Insight。

vRealize Log Insight 作業系統執行個體 (OSI) 授權模式會將 OSI 定義為在非虛擬化實體伺服器或虛擬機器上作業系統的單一安裝。針對 vRealize Log Insight，OSI 也可以是透過 IP 位址識別的單一系統，例如可產生記錄訊息的虛擬化實體伺服器、儲存區陣列或網路裝置。

當主機、伺服器或其他來源停止將記錄傳送至 vRealize Log Insight 時，[授權] 頁面上的 OSI 計數在保留期間將保持不變。保留期間會根據授權使用來計算過去三個月內 OSI 計數的平均值。

您可以使用 vRealize Log Insight Web 使用者介面的 [管理] 區段檢查 vRealize Log Insight 授權狀態並管理您的授權。

作為解決方案互通性的一部分，VMware NSX 使用者的 Standard、Advanced 或 Enterprise 版本可使用其 NSX 授權金鑰來授權 vRealize Log Insight。如需詳細資訊，請參閱 VMware NSX 說明文件。

### 必要條件

- 從 My VMware™ 取得有效的授權金鑰。
- 確認您已做為具有**編輯管理員**權限的使用者身分登入 vRealize Log Insight Web 使用者介面。URL 格式為 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虛擬應用裝置的 IP 位址或主機名稱。

### 程序

- 1 導覽至**管理**索引標籤。

- 2 在 [管理] 下，選取**授權**。
- 3 在**授權金鑰**文字方塊中，輸入您的授權金鑰並按一下**設定金鑰**。如果您有 VMware NSX 授權金鑰，請在此處輸入。
- 4 確認授權狀態為 [作用中] 且授權類型和到期日期正確。

## 記錄儲存區原則

vRealize Log Insight 虛擬應用裝置至少使用 100 GB 的儲存區來儲存傳入記錄。

如果匯入 vRealize Log Insight 的記錄數量達到儲存區限制，則會根據先匯入先淘汰的原則定期自動淘汰舊的記錄訊息。您可以透過將更多儲存區新增至 vRealize Log Insight 虛擬應用裝置來提高儲存區限制。請參閱[增加 vRealize Log Insight 虛擬應用裝置的儲存容量](#)。

若要保留舊訊息，您可以啟用 vRealize Log Insight 的封存功能。請參閱在 [vRealize Log Insight 中啟用或停用資料封存](#)。

由 vRealize Log Insight 儲存的資料不可變。匯入記錄之後，便無法將其移除，直到它自動淘汰。

## 管理系統通知

vRealize Log Insight 會提供與 vRealize Log Insight 健全狀況有關之活動的內建系統通知，例如當磁碟空間已幾乎用盡且將要刪除舊的記錄檔時。管理員可以設定傳送系統通知的頻率和位置。

系統通知會告知您需要立即注意的嚴重問題、為您提供可能需要回應的警告，以及告知您一般系統活動。升級過程中會暫停系統通知，但該功能在其他所有時間內皆有效。

管理員可以指定觸發時傳送通知的頻率和傳送的電子郵件地址。系統也可以將與 vRealize Log Insight 相關的系統通知傳送至第三方應用程式。

系統通知與使用者定義的警示查詢不同。如需警示查詢的詳細資訊，請參閱在 [Log Insight 中新增警示查詢以傳送電子郵件通知](#)。

## vRealize Log Insight 系統通知

vRealize Log Insight 可為您提供有關系統健全狀況的兩組通知：適用於所有產品組態的一般通知，以及與叢集式部署之叢集相關的通知。

下表列出並說明 vRealize Log Insight 的系統通知。

### 一般系統通知

vRealize Log Insight 會發出可能需要管理介入情況的相關通知，這些情況包括封存失敗或警示排程延遲。



通知名稱	說明
最舊的資料即將無法搜尋	<p>vRealize Log Insight 將根據可搜尋資料的預期大小、儲存空間和目前擷取速率，從虛擬應用裝置儲存區淘汰舊資料。如果已設定封存，系統會封存已轉出的資料；如果未設定封存，則會刪除這些資料。</p> <p>若要解決此問題，請新增儲存區或調整保留通知臨界值。如需詳細資訊，請參閱<a href="#">設定 vRealize Log Insight 以傳送健全狀況通知</a>。</p> <p>每次重新啟動 vRealize Log Insight 服務後，都會傳送此通知。</p>
存放庫保留時間	<p>保留期間是指資料保留在 vRealize Log Insight 執行個體之本機磁碟上的時間長度。保留期間由系統可保存的資料量以及目前的擷取速率決定。例如，如果您一天收到 10 GB 的資料 (建立索引後)，且您擁有 300 GB 的空間，則保留率為 30 天。</p> <p>當您達到儲存區限制時，系統將會移除舊資料，以便將空間提供給新擷取的資料使用。此通知會在 vRealize Log Insight 依目前的擷取速率可儲存的可搜尋資料量超過虛擬應用裝置上可用的儲存空間時告知您。</p> <p>您可能在使用 <b>保留通知臨界值</b> 設定的期間之前用盡儲存空間。新增儲存區或調整保留通知臨界值。</p>
已捨棄事件	<p>vRealize Log Insight 無法擷取所有傳入記錄訊息。</p> <ul style="list-style-type: none"> <li>■ 如果丟棄 vRealize Log Insight 伺服器追蹤的任何 TCP 訊息，系統通知會按照如下方式傳送： <ul style="list-style-type: none"> <li>■ 一天一次</li> <li>■ 每次手動或自動重新啟動 vRealize Log Insight 服務時</li> </ul> </li> <li>■ 電子郵件包含自上次傳送通知電子郵件以來丟棄的訊息數目以及自上次重新啟動 vRealize Log Insight 以來丟棄的訊息總數。</li> </ul> <p><b>備註</b> 寄件日期行中的時間由電子郵件用戶端進行控制，並處於當地時區，而電子郵件內文則顯示 UTC 時間。</p>
索引值區損毀	<p>部分磁碟上索引已損毀。索引損毀通常表示基礎儲存區系統有嚴重問題。索引的損毀部分將排除在服務查詢之外。損毀的索引會影響新資料的擷取。服務啟動時，vRealize Log Insight 會檢查索引的完整性。如果偵測到損毀情況，vRealize Log Insight 會按照如下方式傳送系統通知：</p> <ul style="list-style-type: none"> <li>■ 一天一次</li> <li>■ 每次手動或自動重新啟動 vRealize Log Insight 服務時</li> </ul>
磁碟空間不足	<p>vRealize Log Insight 即將耗盡配置的磁碟空間。vRealize Log Insight 最有可能遇到與儲存區相關的問題。</p>
封存空間即將滿載	<p>NFS 伺服器上用於封存 vRealize Log Insight 資料的磁碟空間即將耗盡。如果 NFS 伺服器能以目前擷取速率保存的封存資料量少於七天，則會傳送系統通知。例如，如果您以每天 708.9 MB 的磁碟耗用率來進行封存，且您有 2000 MB 的空間，則您有大約三天的容量，而這低於臨界值。在此情況下，您將收到低於此容量的通知。</p>
磁碟空間總計變更	<p>vRealize Log Insight 資料儲存區的磁碟分割大小總計已減少。這個通知一般表示基礎儲存區系統中存在嚴重問題。當 vRealize Log Insight 偵測到上述情況時，將會按照如下方式傳送此通知：</p> <ul style="list-style-type: none"> <li>■ 立即</li> <li>■ 一天一次</li> </ul>
擱置中封存	<p>vRealize Log Insight 無法如預期般封存資料。此通知通常表示為資料封存設定的 NFS 儲存區存在問題。</p>

通知名稱	說明
已配置的記錄檔記錄儲存磁碟區已達到記錄檔記錄儲存容量上限的 75%。	vRealize Log Insight 已設定為確保 STIG 合規性，並且已配置的記錄檔記錄儲存磁碟區已達到存放庫的記錄檔記錄儲存容量上限的 75%。 <b>備註</b> 此通知會針對每個節點傳送。
授權即將到期	vRealize Log Insight 的授權即將到期。
授權已到期	vRealize Log Insight 的授權已到期。
SSL 憑證即將到期	vRealize Log Insight 叢集的 SSL 憑證將在 30 天後到期。
無法連線到 AD 伺服器	vRealize Log Insight 無法連線至設定的 Active Directory 伺服器。
無法接管 High Availability IP 位址 [IP Address]，因為它已經由其他機器保留	vRealize Log Insight 叢集無法接管針對整合式負載平衡器 (ILB) 設定的 IP 位址。此通知的最常見原因是相同網路內的其他主機已保留該 IP 位址，因此叢集無法接管該 IP 位址。 從目前保留該 IP 位址的主機釋放該 IP 位址，或為 Log Insight 整合式負載平衡器設定網路中可用的靜態 IP 位址，可以解決此衝突。變更 ILB IP 位址時，您必須重新設定所有用戶端，藉此將記錄傳送至新 IP 位址或是解析為此 IP 位址的 FQDN/URL。您也必須從 [vSphere 整合] 頁面中取消設定每個與 vRealize Log Insight 整合的 vCenter Server，然後再重新設定。
由於存在太多節點故障，High Availability IP 位址 [IP Address] 無法使用。	針對整合式負載平衡器 (ILB) 設定的 IP 位址無法使用。對於嘗試透過 ILB IP 位址或解析為此 IP 位址的 FQDN/URL，將記錄傳送到 vRealize Log Insight 叢集的用戶端而言，其將顯示為無法使用。此通知的最常見原因是 vRealize Log Insight 叢集中的大多數節點狀況不良、無法使用或無法從主節點連線。另一個常見原因是 NTP 時間同步化尚未啟用，或設定的 NTP 伺服器之間具有明顯的時間偏離。您可以嘗試對 IP 位址執行 Ping 動作 (如果允許) 並驗證它是否無法連線，以確認問題是否仍然存在。 若要解決此問題，請確保大多數叢集節點狀況良好且可連線，並為準確的 NTP 伺服器啟用 NTP 時間同步化。
vRealize Log Insight 節點之間有太多次 High Availability IP 位址 [您的 IP 位址] 移轉	針對整合式負載平衡器 (ILB) 設定的 IP 位址在過去 10 分鐘內已移轉太多次。 在一般運作情況下，IP 位址很少在 vRealize Log Insight 叢集節點之間移動。不過，如果目前的擁有者節點重新啟動或置於維護模式，IP 位址可能會移動。另一個原因可能是 Log Insight 叢集節點之間缺少時間同步化，這是叢集正常運作的必要條件。若要解決後者的問題，請對準確的 NTP 伺服器啟用 NTP 時間同步化。
SSL 憑證錯誤	Syslog 來源已透過 SSL 起始與 vRealize Log Insight 的連線，但突然終止該連線。此通知可能表示 Syslog 來源無法確認 SSL 憑證是否有效。若要使 vRealize Log Insight 透過 SSL 接受 Syslog 訊息，需要具有由用戶端驗證的憑證，並且必須同步系統的時脈。SSL 憑證或網路時間服務可能存在問題。 您可以驗證 SSL 憑證是否受 syslog 來源信任，將來源重新設定為不使用 SSL，或重新安裝 SSL 憑證。請參閱 <a href="#">設定 vRealize Log Insight 代理程式 SSL 參數</a> 和 <a href="#">安裝自訂 SSL 憑證</a> 。
vCenter 收集失敗	vRealize Log Insight 無法收集 vCenter 事件、工作和警示。若要尋找導致收集失敗的確切錯誤並查看收集目前是否運作，請查看 <code>/var/log/vmware/loginsight/plugins/vsphere/li-vsphere.log</code> 檔案。

通知名稱	說明
vCenter Kubernetes 服務事件收集失敗	vRealize Log Insight 無法收集 vCenter Kubernetes 系統事件、工作和警示。若要尋找導致收集失敗的確切錯誤並查看收集目前是否運作，請查看 <code>/var/log/vmware/loginsight/plugins/vsphere/li-vsphere.log</code> 檔案。
已捨棄事件轉送站的事件	轉送站因連線或超載問題而捨棄事件。 範例： <pre>Log Insight Admin Alert: Event Forwarder Events Dropped This alert is about your Log Insight installation on https://&lt;your_url&gt;  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>
排程之後的警示查詢	vRealize Log Insight 無法在其設定的時間執行使用者定義的警示。延遲的原因可能是一或多個無效率的使用者定義警示，或未針對擷取和查詢負載正確設定系統大小。
自動停用的警示	如果使用者定義的警示已執行至少 10 次且平均執行時間超過一小時，則系統會將該警示視為無效率並將其停用，避免影響其他使用者定義的警示。
無效率的警示查詢	如果使用者定義的警示需要超過一小時的時間才能完成，則系統會將該警示視為無效率。
新使用者已建立，或是第一次登入的使用者	vRealize Log Insight 已設定為確保 STIG 合規性以及新使用者已建立或 Active Directory 或是 VMware Identity Manager 使用者第一次登入。

## 叢集的系統通知

vRealize Log Insight 會傳送與叢集拓撲變更相關的通知，包括新增叢集成員或暫時性節點通訊問題。

傳送者	通知名稱	說明
主要節點	需要對新工作節點進行核准	工作節點正在傳送加入叢集的要求。管理員使用者必須核准或拒絕該要求。
主要節點	新工作節點已獲核准	管理員使用者已核准來自工作節點之加入 vRealize Log Insight 叢集的成員資格要求。
主要節點	新工作節點已遭拒絕	管理員使用者已拒絕來自工作節點之加入 vRealize Log Insight 叢集的成員資格要求。如果要求誤遭拒絕，管理員使用者可從工作節點重新放置要求，然後在主要節點上核准。
主要節點	由於工作節點的原因，已超過支援的節點數上限	由於新工作節點的原因，Log Insight 叢集中的工作節點數已超過支援的數量上限。
主要節點	超過允許的節點數，新工作節點遭拒	管理員使用者嘗試新增到叢集的節點數超過允許的節點數上限，因此節點遭拒。

傳送者	通知名稱	說明
主要節點	工作節點已中斷連線	先前連線的工作節點已從 vRealize Log Insight 叢集中斷連線。
主要節點	工作節點已重新連線	工作節點已重新連線至 vRealize Log Insight 叢集。
主要節點	工作節點由 Admin 撤銷	管理員使用者已撤銷工作節點成員資格，且節點不再屬於 vRealize Log Insight 叢集。
主要節點	未知工作節點遭拒	由於工作節點是主要節點未知的節點，因此 vRealize Log Insight 主要節點已拒絕來自該工作節點的要求。如果工作是有效的節點且應新增到叢集，請登入工作節點，移除其 Token 檔案和使用者組態 (位於 <code>/storage/core/loginsight/config/</code> 中)，然後在工作節點上執行 <code>restart loginsight service</code> 。
主要節點	工作節點已進入維護模式	工作節點已進入維護模式，管理員使用者必須先將工作節點從維護模式中移除，然後此節點才可接收組態變更和提供查詢。
主要節點	工作節點已返回到服務模式	工作節點已結束維護模式並返回到服務模式。
工作節點	主要節點故障或與工作節點中斷連線	傳送通知的工作節點無法連線到 vRealize Log Insight 主要節點。此通知可能表示主要節點故障，且可能需要重新啟動。如果主要節點故障，則無法設定叢集且無法提交查詢，直到此節點再次上線為止。工作節點將繼續擷取訊息。
<b>備註</b> 您可能會收到大量此類通知，因為許多工作節點可能會獨立偵測主要節點故障並發出通知。		
工作節點	主要節點已連線到工作節點	傳送通知的工作節點已重新連線到 vRealize Log Insight 主要節點。

## 設定 vRealize Log Insight 系統通知的目的地

管理員使用者可以設定觸發系統通知時 vRealize Log Insight 所採取的動作。

vRealize Log Insight 會在發生重要系統事件 (例如，磁碟空間幾乎已用盡且 vRealize Log Insight 必須開始刪除或封存舊的記錄檔) 時產生系統通知。

管理員可以設定 vRealize Log Insight 以傳送有關那些事件的電子郵件通知。管理員使用者可在管理 UI 之 SMTP 組態頁面上的**寄件者**文字方塊中設定系統通知電子郵件的寄件地址。請參閱[vRealize Log Insight 設定 SMTP 伺服器](#)。

管理員使用者也可以向第三方應用程式傳送通知。請參閱[關於使用 Webhook 傳送系統通知給協力廠商產品](#)。

## 設定 vRealize Log Insight 以傳送健全狀況通知

管理員可將 vRealize Log Insight 設定為傳送與其自身健全狀況相關的通知。

如果無法傳遞電子郵件訊息，您會在 Web 介面上收到錯誤通知。

### 必要條件

- 確認您已做為具有**編輯管理員**權限的使用者身分登入 vRealize Log Insight Web 使用者介面。URL 格式為 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虛擬應用裝置的 IP 位址或主機名稱。
- 確認已針對 vRealize Log Insight 設定 SMTP 伺服器。如需詳細資訊，請參閱 [vRealize Log Insight 設定 SMTP 伺服器](#)。

### 程序

- 1 導覽至**管理**索引標籤。
- 2 在 [組態] 下，按一下**一般**。
- 3 在 [警示] 標頭下，設定系統通知。
  - a 在**將系統通知透過電子郵件傳送至**文字方塊中，輸入要接收通知的電子郵件地址。  
使用逗點分隔多個電子郵件地址。
  - b 選取**保留通知臨界值**核取方塊，並設定用於觸發通知的臨界值。  
系統針對指定期間可保留的資料量不足時便會傳送通知。系統會根據目前的擷取速率來計算此值。
- 4 按一下**儲存**。
- 5 按一下**重新啟動 Log Insight** 以套用變更。

## 設定協力廠商產品的 vRealize Log Insight 系統通知

管理員可將 vRealize Log Insight 設定為傳送與其自身健全狀況相關的通知給協力廠商應用程式。

vRealize Log Insight 會在發生重要系統事件 (例如，磁碟空間幾乎已用盡且 vRealize Log Insight 必須開始刪除舊的記錄檔) 時產生這些通知。

### 必要條件

確認您已做為具有**編輯管理員**權限的使用者身分登入 vRealize Log Insight Web 使用者介面。URL 格式為 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虛擬應用裝置的 IP 位址或主機名稱。

### 程序

- 1 導覽至**管理**索引標籤。
- 2 在 [組態] 下，按一下**一般**。

### 3 在 [警示] 標頭下，設定系統通知。

- a 在將 HTTP Post 系統通知傳送至文字方塊中，輸入要接收通知的 URL。
- b (選擇性) 確認已為您的環境正確設定當容量低於以下值時傳送通知核取方塊與相關聯的臨界值。

### 4 按一下儲存。

#### 後續步驟

使用通知的 Webhook 輸出，建立填充碼以對應 vRealize Log Insight Webhook 格式和協力廠商應用程式所使用的格式。

#### 關於使用 Webhook 傳送系統通知給協力廠商產品

您可以使用 Webhook 傳送 vRealize Log Insight 系統通知給協力廠商產品。

vRealize Log Insight 使用 Webhook 透過 HTTP POST 傳送警示給其他應用程式。vRealize Log Insight 會以自己的專有格式傳送 Webhook，但是協力廠商解決方案希望傳入的 Webhook 是他們自己的專有格式。若要使用以 vRealize Log Insight Webhook 傳送的資訊，協力廠商應用程式必須具備 vRealize Log Insight 格式的原生支援，或者您必須使用填充碼在 vRealize Log Insight 格式和協力廠商所用格式之間建立對應。填充碼會將 vRealize Log Insight 格式轉譯或對應至不同格式。

vRealize Log Insight Webhook 實作會向遠端伺服器發出輸出 HTTP 要求。伺服器可能會報告成功或失敗，且 vRealize Log Insight 會在失敗時重試。所有 HTTP/2xx 狀態碼回應會視為成功，而所有其他回應 (包括逾時或拒絕連線)，則會視為失敗且將於稍後重試。

使用訊息查詢建立的警示、使用彙總查詢建立的警示以及系統通知皆有其自己的 Webhook 格式。

支援 HTTP 基本驗證。請使用 `{{https://username:password@hostname/path}}` 的格式在 URL 中內嵌認證

#### 系統通知的 Webhook 格式

vRealize Log Insight Webhook 的格式取決於其建立來源的查詢類型。系統通知、使用者警示訊息查詢和產生自彙總使用者查詢的警示各有不同的 Webhook 格式。

您必須是 vRealize Log Insight 管理員才能將 vRealize Log Insight 設定為傳送系統通知。

當您傳送系統通知給協力廠商程式時，您必須撰寫填充碼，讓協力廠商程式的格式能夠了解 vRealize Log Insight 資訊。

#### 系統通知的 Webhook 格式

下列範例顯示系統通知的 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 master 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":[]
  }
]
}

```

## 新增 vRealize Log Insight 事件轉送目的地

您可以將 vRealize Log Insight 伺服器設定為將傳入事件轉送到 syslog 或擷取 API 目標。

使用事件轉送將所篩選或標記的事件傳送至一或多個遠端目的地，例如 vRealize Log Insight、Syslog 或同時傳送至兩者。事件轉送可用於支援現有的記錄工具 (如 SIEM) 以及透過不同網路 (如 DMZ 或 WAN) 整併記錄。

事件轉送站可以是獨立，也可以是叢集化的，但事件轉送站是與遠端目的地不同的執行個體。針對事件轉送設定的執行個體也會在本機儲存事件，且可用於查詢資料。

您在轉送事件頁面上用於建立篩選器的運算子，與您在互動式分析頁面上使用的篩選器不同。如需使用在 [互動式分析中執行功能表項目來預覽事件篩選結果的詳細資訊](#)，請參閱在 [互動式分析中使用事件轉送篩選器](#)。

### 必要條件

確認您已做為具有**編輯管理員**權限的使用者身分登入 vRealize Log Insight Web 使用者介面。URL 格式為 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虛擬應用裝置的 IP 位址或主機名稱。

確認目的地可處理轉送的事件數。如果目的地叢集比轉送執行個體小許多，則可能會捨棄部分事件。

### 程序

- 1 導覽至**管理索引標籤**。
- 2 在 [管理] 下，按一下**事件轉送**。



### 3 按一下 新增目的地，並提供下列資訊。

選項	說明
名稱	新目的地的唯一名稱。
主機	IP 位址或完整網域名稱。  <b>注意</b> 轉送迴圈是 vRealize Log Insight 叢集將事件轉送給自己或其他叢集，然後將事件轉送回原始叢集的組態。此類迴圈可能會為每個轉送事件建立數目無限的複本。vRealize Log Insight Web 介面無法讓您將事件設定為轉送給事件本身。但 vRealize Log Insight 無法避免間接轉送迴圈，例如 vRealize Log Insight 叢集 A 轉送給叢集 B，而 B 將相同事件轉送回 A。建立轉送目的地時，請小心不要建立間接轉送迴圈。
通訊協定	擷取 API、Syslog 或 RAW。預設值為擷取 API (CFAPI)。 使用擷取 API 轉送事件時，事件的原始來源會保留在 [來源] 欄位中。使用 Syslog 轉送事件時，事件的原始來源會遺失，接收器會將訊息的來源記錄為 vRealize Log Insight 轉送站的 IP 位址或主機名稱。使用 RAW 轉送事件時的行為類似於 Syslog，但不一定會符合 Syslog RFC。RAW 會以接收事件的相同方式來轉送事件，而不會有 vRealize Log Insight 新增的自訂 Syslog 標頭。此通訊協定可用於第三方目的地，因為這些目的地預期 Syslog 事件會採用其原始格式。  <b>備註</b> 視事件轉送站上選取的通訊協定而定，來源欄位的值可能會有所不同： a 對於擷取 API，來源是初始寄件者 (事件建立者) 的 IP 位址。 b 對於 Syslog 和 RAW，來源是事件轉送站的 vRealize Log Insight 執行個體 IP 位址。此外，訊息文字包含指向初始寄件者 IP 位址的 <code>_li_source_path</code> 。
使用 SSL	您可以選擇性地為擷取 API 或 Syslog 使用 SSL 保護連線。如果轉送目的地所提供的 SSL 憑證不受信任，您可以在測試或儲存此組態時接受憑證。
標籤	您可以選擇性地新增具有預先定義值的標籤配對。標籤可讓您更輕鬆地查詢事件。您可以新增多個以逗點分隔的標籤。
轉送互補標籤	您可以選取是否要轉送 Syslog 的互補標籤。 互補標籤是由叢集本身新增的標籤，例如「vc_username」或「vc_vmname」。這些標籤可以連同直接從來源傳入的標籤一起轉送。使用擷取 API 時，系統一律會轉送互補標籤。
傳輸	選取 Syslog 的傳輸通訊協定。您可以選取 UDP 或 TCP。

### 4 若要控制轉送的事件，請按一下 新增篩選器。

選取用於定義所需事件的欄位和限制。只有靜態欄位可用作篩選器。如果您未選取任何篩選器，將轉送所有事件。您可以透過按一下在 **互動式分析** 中執行，看到您所建立之篩選器的結果。

運算子	說明
符合	尋找符合字串和萬用字元規格的字串，其中 * 表示零或多個字元，? 表示零或任何單一字元。支援前置詞和後置詞萬用字元。 例如， <code>*test*</code> 會比對如 <code>test123</code> 或 <code>my-test-run</code> 的字串。
不符合	排除符合字串和萬用字元規格的字串，其中 * 表示零或多個字元，? 表示零或任何單一字元。支援前置詞和後置詞萬用字元。 例如， <code>test*</code> 會排除 <code>test123</code> ，而非 <code>mytest123</code> 。 <code>?test*</code> 會排除 <code>test123</code> 和 <code>xtest123</code> ，而非 <code>mytest123</code> 。



運算子	說明
開頭為	尋找以指定字元字串開頭的字串。 例如， <code>test</code> 會找到 <code>test123</code> 或 <code>test</code> ，而非 <code>my-test123</code> 。
開頭非	排除以指定字元字串開頭的字串。 例如， <code>test</code> 會篩選掉 <code>test123</code> ，而非 <code>my-test123</code> 。

- 5 (選擇性) 若要修改下列轉送資訊，請按一下**顯示進階設定**。

選項	說明
連接埠	在遠端目的地上，事件將傳送到的連接埠。系統會根據通訊協定來設定預設值。除非遠端目的地接聽不同的連接埠，否則請勿進行變更。
工作計數	欲使用的同時外寄連線數。針對已轉送目的地之較高網路延遲以及每秒已轉送事件的較高數目，設定較高的工作計數。預設值為 8。

- 6 若要驗證組態，請按一下**測試**。

- 7 如果轉送目的地提供了不受信任的 SSL 憑證，則會有對話方塊顯示憑證的詳細資料。按一下**接受**，將憑證新增至 vRealize Log Insight 叢集中所有節點的信任存放區。

如果您按一下**取消**，則憑證不會新增至信任存放區，且與轉送目的地的連線將會失敗。您必須接受憑證才能成功連線。

- 8 按一下**儲存**。

如果您並未測試組態，且目的地提供的憑證不受信任，請依照步驟 7 中的指示操作。

#### 後續步驟

您可以編輯或複製事件轉送目的地。如果您對目的地進行編輯以變更事件轉送站名稱，所有的統計資料將會重設。

## 在互動式分析中使用事件轉送篩選器

用於事件篩選的運算子與用於互動式分析篩選器中的運算子並未按名稱一對一對應。不過，您可以針對兩種格式選取產生類似結果的運算子。

當您從**事件轉送**頁面使用在**互動式分析**中執行功能表項目時，此差異非常重要。例如，如果您有符合 `*foo*` 的事件轉送篩選器，並從事件篩選器頁面選取在**互動式分析**中執行功能表項目，則互動式分析查詢即相當於符合 `regex^.*foo.* $`，這可能不會比對所有相同事件。

另一個範例為符合 `foo`，這在互動式分析上執行時將視為包含 `foo`。由於互動式分析功能也會搜尋關鍵字查詢，因此包含 `foo` 可能會比符合 `foo` 符合更多的事件。

您可以變更互動式分析使用的運算子以解決這些差異。

- 將**包含**運算子變更為**符合 regex**。
- 將事件轉送篩選器中出現的 `*` 變更為 `.`，並將篩選器詞彙加上前置詞 `.`。例如，將變更事件篩選器運算式符合 `*foo*` 變更為符合 `regex.*foo.*`，以用於互動式分析。

- 針對事件篩選器中的**不符合**運算子，您可以將**符合 regex** 運算子與 regex look ahead 值搭配使用。  
例如，**不符合 \*foo\*** 相當於**符合 regex**。\*(?!foo).\*

## 同步 vRealize Log Insight 虛擬應用裝置的時間

您必須將 vRealize Log Insight 虛擬應用裝置的時間與已部署該虛擬應用裝置的 NTP 伺服器或 ESX/ESXi 主機的時間同步。

時間對於 vRealize Log Insight 的核心功能來說很重要。

依預設，vRealize Log Insight 會與一系列預先定義的公用 NTP 伺服器同步時間。如果公用 NTP 伺服器因防火牆而無法存取，您可以使用公司內部的 NTP 伺服器。如果 NTP 伺服器無法使用，您可以與已部署 vRealize Log Insight 虛擬應用裝置的 ESX/ESXi 主機同步時間。

### 必要條件

確認您已做為具有**編輯管理員**權限的使用者身分登入 vRealize Log Insight Web 使用者介面。URL 格式為 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虛擬應用裝置的 IP 位址或主機名稱。

### 程序

- 1 導覽至**管理索引標籤**。
- 2 在 [組態] 下，按一下**時間**。
- 3 從**同步時間基準**下拉式功能表中，選取時間來源。

選項	說明
NTP 伺服器	將 vRealize Log Insight 虛擬應用裝置的時間與所列的其中一個 NTP 伺服器的時間同步。
ESX/ESXi 主機	將 vRealize Log Insight 虛擬應用裝置的時間與已部署該虛擬應用裝置的 ESX/ESXi 主機的時間同步。

- 4 (選擇性) 如果您選取了 NTP 伺服器同步化，請列出 NTP 伺服器位址，然後按一下**測試**。

**備註** 測試一部 NTP 伺服器的連線可能最多需要 20 秒的時間。

- 5 按一下**儲存**。

## 為 vRealize Log Insight 設定 SMTP 伺服器

您可以設定 SMTP 以允許 vRealize Log Insight 傳送電子郵件通知。

當 vRealize Log Insight 偵測到重要系統事件 (例如，虛擬應用裝置上的儲存容量已達到您設定的臨界值) 時，即會產生系統通知。

### 必要條件

確認您已做為具有**編輯管理員**權限的使用者身分登入 vRealize Log Insight Web 使用者介面。URL 格式為 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虛擬應用裝置的 IP 位址或主機名稱。

### 程序

- 1 導覽至**管理索引**標籤。
- 2 在 [組態] 下，按一下 **SMTP**。
- 3 輸入 SMTP 伺服器位址和連接埠號碼。
- 4 如果 SMTP 伺服器使用加密連線，請選取加密通訊協定。
- 5 在**傳送者**文字方塊中，輸入傳送系統通知時要使用的電子郵件地址。  
**傳送者**地址在系統通知電子郵件中顯示為 [寄件者] 地址。此地址不需要是真實的地址，可以為代表 vRealize Log Insight 之特定執行個體的地址。例如，`loginsight@example.com`。
- 6 輸入在傳送系統通知時要透過 SMTP 伺服器進行驗證的使用者名稱和密碼。
- 7 輸入目的地電子郵件，並按一下**傳送測試電子郵件**以驗證連線。
- 8 如果 SMTP 伺服器提供了不受信任的 SSL 憑證，則會有對話方塊顯示憑證的詳細資料。按一下**接受**，將憑證新增至 vRealize Log Insight 叢集中所有節點的信任存放區。  
 如果您按一下**取消**，則憑證不會新增至信任存放區，且與 SMTP 伺服器的連線將會失敗。您必須接受憑證才能成功連線。
- 9 按一下**儲存**。  
 如果您並未測試連線，且 SMTP 伺服器提供的憑證不受信任，請依照步驟 8 中的指示操作。

## 安裝自訂 SSL 憑證

依預設，vRealize Log Insight 會在虛擬應用裝置上安裝自我簽署的 SSL 憑證。

當您連線至 vRealize Log Insight Web 使用者介面時，自我簽署的憑證會產生安全警告。如果您不想使用自我簽署的安全性憑證，可以安裝自訂 SSL 憑證。唯一要求使用自訂 SSL 憑證的功能是透過 SSL 的事件轉送。如果您具有在啟用 ILB 的情況下設定的叢集，請參閱**啟用整合式負載平衡器**瞭解自訂 SSL 憑證的特定需求。

---

**備註** vRealize Log Insight Web 使用者介面及 Log Insight 擷取通訊協定 `cfapi` 使用相同的憑證進行驗證。

---

### 必要條件

- 確認您的自訂 SSL 憑證滿足下列需求。
  - CommonName 包含主要節點或虛擬 IP 位址的 FQDN 的萬用字元或完全相符項目。所有其他 IP 位址和 FQDN 會選擇性地列為 subjectAltName。

- 憑證檔案包含有效的私密金鑰和有效的憑證鏈結。
- 私密金鑰由 RSA 或 DSA 演算法產生。
- 不會透過複雜密碼加密私密金鑰。
- 如果憑證由一系列其他憑證簽署，則所有其他憑證將包含在您要匯入的憑證檔案中。
- 憑證檔案中的私密金鑰和所有憑證均採用 PEM 編碼。vRealize Log Insight 不支援 DER 編碼的憑證和私密金鑰。
- 憑證檔案中的私密金鑰和所有憑證都是 PEM 格式。vRealize Log Insight 不支援 PFX、PKCS12、PKCS7 或其他格式的憑證。
- 確保按下列順序將每個憑證的整個本文串連到單一文字檔。
  - a 私密金鑰 - *your\_domain\_name.key*
  - b 主要憑證 - *your\_domain\_name.crt*
  - c 中繼憑證 - *DigiCertCA.crt*
  - d 根憑證 - *TrustedRoot.crt*
- 確保以下列格式包含每個憑證的開始和結束標籤。

```

-----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-----

```

- 確認您已做為具有**編輯管理員**權限的使用者身分登入 vRealize Log Insight Web 使用者介面。URL 格式為 `https://log-insight-host`，其中 *log-insight-host* 是 vRealize Log Insight 虛擬應用裝置的 IP 位址或主機名稱。

## 程序

### 1 產生自我簽署的憑證

您可以使用 OpenSSL 工具產生適用於 Windows 或 Linux 的自我簽署的憑證。

### 2 產生憑證簽署要求

使用適用於 Windows 的 OpenSSL 工具產生憑證簽署要求。

### 3 從憑證授權機構要求簽章

將您的憑證簽署要求傳送到您選擇的憑證授權機構並申請簽章。

#### 4 串連憑證檔案

將您的金鑰與憑證檔案合併為一個 PEM 檔案。

#### 5 上傳已簽署憑證

您可以上傳已簽署的 SSL 憑證。

#### 6 設定 vRealize Log Insight 伺服器與 Log Insight Agents 之間的 SSL 連線

SSL 功能可讓您透過擷取 API 的安全流量在 Log Insight Agents 和 vRealize Log Insight 伺服器之間提供僅使用 SSL 進行的連線。您還可以設定 Log Insight Agents 的各種 SSL 參數。

## 產生自我簽署的憑證

您可以使用 OpenSSL 工具產生適用於 Windows 或 Linux 的自我簽署的憑證。

#### 必要條件

- 從 <https://www.openssl.org/community/binaries.html> 下載針對 OpenSSL 的適當安裝程式。使用已下載的 OpenSSL 安裝程式，將其安裝在 Windows 上。
- 編輯 `openssl.cnf` 檔案以新增其他必要參數。確保 `[req]` 區段已定義 `req_extensions` 參數。

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

- 為伺服器的主機名稱或 IP 位址新增適當的 [主體別名] 項目，例如 `server-01.loginsight.domain`。您無法為此主機名稱指定模式。

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

#### 程序

- 1 建立一個資料夾以儲存您的憑證檔案，例如 `C:\Certs\LogInsight`。
- 2 開啟命令提示字元並執行下列命令。

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

OpenSSL 會提示您提供憑證內容，包括國家/地區、組織等等。

- 3 如果已啟用負載平衡，請輸入 vRealize Log Insight 伺服器的確切 IP 位址或主機名稱，或輸入 vRealize Log Insight 叢集位址。

此內容為唯一一個指定值時的必填項目。

## 結果

系統會建立兩個檔案：`server.key` 和 `server.crt`。

- `server.key` 是新的 PEM 編碼私密金鑰。
- `server.crt` 是由 `server.key` 簽署的新 PEM 編碼憑證。

## 產生憑證簽署要求

使用適用於 Windows 的 OpenSSL 工具產生憑證簽署要求。

### 必要條件

- 安裝 OpenSSL 工具。如需取得 OpenSSL 工具的相關資訊，請參閱 <http://www.openssl.org>。
- 編輯 `openssl.cfg` 檔案以新增其他必要參數。確保 `[req]` 區段已定義 `req_extensions` 參數。

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

- 為伺服器的主機名稱或 IP 位址新增適當的 [主體別名] 項目，例如 `server-01.loginsight.domain`。您無法為此主機名稱指定模式。

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

### 程序

- 1 建立一個資料夾以儲存您的憑證檔案，例如 `C:\Certs\LogInsight`。
- 2 開啟命令提示字元，然後執行以下命令來產生私密金鑰。

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

- 3 透過執行以下命令來建立憑證簽署要求。

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

**備註** 此命令會以互動方式執行，並向您詢問各種問題。憑證授權機構會反覆查對您的回答。您的回答必須與您公司註冊之相關法律文件相符。

- 4 遵循畫面指示，然後輸入將併入憑證要求的資訊。

**重要** 在 [一般名稱] 欄位中，輸入您伺服器的主機名稱或 IP 位址，例如 `mail.your.domain`。如果想要加入所有子網域，則輸入 `*your.domain`。

## 結果

系統會產生並儲存憑證簽署要求檔案 `server.csr`。

## 從憑證授權機構要求簽章

將您的憑證簽署要求傳送到您選擇的憑證授權機構並申請簽章。

### 程序

- ◆ 將您的 `server.csr` 檔案提交給憑證授權機構。

---

**備註** 向憑證授權機構要求對您的檔案以 PEM 格式進行編碼。

---

憑證授權機構將處理您的要求並傳回一個以 PEM 格式編碼的 `server.crt` 檔案。

## 串連憑證檔案

將您的金鑰與憑證檔案合併為一個 PEM 檔案。

### 程序

- 1 建立一個新的 `server.pem` 檔案並在文字編輯器中將其開啟。
- 2 複製 `server.key` 檔案的內容並使用以下格式將其貼到 `server.pem` 中。

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

- 3 複製從憑證授權機構接收的 `server.crt` 檔案內容，然後使用以下格式將其貼到 `server.pem` 中。

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

- 4 如果憑證授權機構為您提供了一個中繼或鏈結憑證，請以下列格式將此中繼或鏈結憑證附加到公開憑證檔案的結尾。

```
-----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 儲存 `server.pem` 檔案。

## 上傳已簽署憑證

您可以上傳已簽署的 SSL 憑證。

### 程序

- 1 導覽至**管理**索引標籤。
- 2 在 [組態] 下，按一下 **SSL 憑證**。
- 3 瀏覽至自訂 SSL 憑證，然後按一下**開啟**。
- 4 按一下**儲存**。
- 5 重新啟動 vRealize Log Insight。

### 後續步驟

vRealize Log Insight 重新啟動之後，請確認 ESXi 的 syslog 摘要會繼續送達 vRealize Log Insight。

## 設定 vRealize Log Insight 伺服器與 Log Insight Agents 之間的 SSL 連線

SSL 功能可讓您透過擷取 API 的安全流量在 Log Insight Agents 和 vRealize Log Insight 伺服器之間提供僅使用 SSL 進行的連線。您還可以設定 Log Insight Agents 的各種 SSL 參數。

已停用讓 vRealize Log Insight 代理程式無法透過 TLSv.1.2、SSLv.3/TLSv.1.0 進行通訊，以符合安全性準則。

### 主要 SSL 功能

瞭解主要 SSL 功能可協助您正確設定 Log Insight Agents。

vRealize Log Insight 代理程式可儲存憑證，並在與特定伺服器的所有 (除了第一次) 連線期間將憑證用於驗證伺服器的身分。如果無法確認伺服器的身分，vRealize Log Insight 代理程式會拒絕與伺服器連線並將適當的錯誤訊息寫入記錄。代理程式接收的憑證將儲存於 cert 資料夾。

- 對於 Windows，請前往 C:\ProgramData\VMware\Log Insight Agent\cert。
- 對於 Linux，請前往 /var/lib/loginsight-agent/cert。

當 vRealize Log Insight 代理程式建立與 vRealize Log Insight 伺服器的安全連線時，代理程式會檢查從 vRealize Log Insight 伺服器接收的憑證的有效性。vRealize Log Insight 代理程式使用系統信任的根憑證。

- Log Insight Linux Agent 從 /etc/pki/tls/certs/ca-bundle.crt 或 /etc/ssl/certs/ca-certificates.crt 載入受信任的憑證。
- Log Insight Windows Agent 使用系統根憑證。

如果 vRealize Log Insight 代理程式已本機儲存自我簽署的憑證，但是接收了另一個含相同公開金鑰的有效自我簽署的憑證，則代理程式將接受新憑證。使用含不同詳細資料 (例如，新的到期日期) 的相同私密金鑰重新產生自我簽署的憑證時，可能會發生此情況。否則，連線將遭拒。

如果 vRealize Log Insight 代理程式已本機儲存自我簽署的憑證，但接收了有效的 CA 簽署憑證，則 vRealize Log Insight 代理程式會以無訊息方式取代新接受的憑證。



如果 vRealize Log Insight 代理程式已經擁有 CA 簽署憑證，又接收自我簽署的憑證，則 Log Insight 代理程式會拒絕它。僅在第一次與伺服器連線時，vRealize Log Insight 代理程式接受從 vRealize Log Insight 伺服器接收的自我簽署的憑證。

如果 vRealize Log Insight 代理程式已本機儲存 CA 簽署憑證，但接收另一個受信任 CA 簽署的有效憑證，代理程式將拒絕它。您可以修改 vRealize Log Insight 代理程式的組態選項以接受新憑證。請參閱 [設定 vRealize Log Insight 代理程式 SSL 參數](#)。

已停用讓 vRealize Log Insight 代理程式無法透過 TLSv.1.2. SSLv.3/TLSv.1.0 進行通訊，以符合安全性準則。

## 強制執行僅使用 SSL 的連線

您可以使用 vRealize Log Insight Web 使用者介面將 vRealize Log Insight Agents 和擷取 API 設定為僅允許使用 SSL 連線到伺服器。

vRealize Log Insight API 一般可在連接埠 9000 透過 HTTP，以及在連接埠 9543 透過 HTTPS 連接。這兩個連接埠都可供 vRealize Log Insight 代理程式或自訂 API 用戶端使用。所有驗證要求都需要 SSL，但未經驗證的要求 (包括 vRealize Log Insight 代理程式擷取流量) 都可使用這兩個連接埠執行。您可以強制所有 API 要求使用 SSL 連線。由於 HTTP 連接埠 80 要求可繼續重新導向至 HTTPS 連接埠 443，因此該選項不會限制 Syslog 連接埠 514 的流量，也不會影響 vRealize Log Insight 使用者介面。

### 必要條件

確認您已做為具有**編輯管理員**權限的使用者身分登入 vRealize Log Insight Web 使用者介面。URL 格式為 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虛擬應用裝置的 IP 位址或主機名稱。

### 程序

- 1 導覽至**管理索引**標籤。
- 2 在 [組態] 下，按一下 **SSL**。
- 3 在 [API 伺服器 SSL] 下，選取**需要 SSL 連線**。
- 4 按一下**儲存**。

### 結果

vRealize Log Insight API 僅允許使用 SSL 連線到伺服器。非 SSL 連線會遭到拒絕。

## 設定 vRealize Log Insight 代理程式 SSL 參數

您可以編輯 vRealize Log Insight 代理程式組態檔以變更 SSL 組態、將路徑新增至受信任的根憑證，並指定代理程式是否接受憑證。

此程序適用於 Windows 和 Linux 適用的 vRealize Log Insight 代理程式。

### 必要條件

對於 vRealize Log Insight Linux 代理程式：

- 以**根使用者**身分登入，或使用 `sudo` 執行主控台命令。

- 登入安裝有 vRealize Log Insight Linux 代理程式的 Linux 機器，開啟主控台並執行 `pgrep liagent`，以確認 vRealize Log Insight Linux 代理程式已安裝且正在執行。

對於 vRealize Log Insight Windows 代理程式：

- 登入已安裝 vRealize Log Insight Windows 代理程式的 Windows 機器，然後啟動服務管理員以確認 vRealize Log Insight 代理程式服務已安裝。

## 程序

- 1 導覽到包含 `liagent.ini` 檔案的資料夾。

作業系統	路徑
Linux	<code>/var/lib/loginsight-agent/</code>
Windows	<code>%ProgramData%\VMware\Log Insight Agent</code>

- 2 在任一文字編輯器中開啟 `liagent.ini` 檔案。
- 3 將以下索引鍵新增到 `liagent.ini` 檔案的 `[server]` 區段。

索引鍵	說明
<code>ssl_ca_path</code>	<p>覆寫根憑證授權機構簽署憑證的預設儲存區路徑，其用於驗證連線對等憑證。</p> <p>為 <code>ssl_ca_path</code> 提供路徑時，您會覆寫 Linux 和 Windows 代理程式的預設值。您可以使用一個檔案，其中採用 PEM 格式的多個憑證已串連，或使用一個目錄，其中包含的憑證採用 PEM 格式且名稱格式為 <code>hash.0</code>。(請參閱 <code>x509</code> 公用程式的 <code>-hash</code> 選項。)</p> <p><b>Linux：</b>如果沒有指定值，代理程式會使用指派給 <code>LI_AGENT_SSL_CA_PATH</code> 環境變數的值。如果該值不存在，代理程式會嘗試從 <code>/etc/pki/tls/certs/ca-bundle.crt</code> 檔案或從 <code>/etc/ssl/certs/ca-certificates.crt</code> 檔案載入受信任的憑證。</p> <p><b>Windows：</b>如果沒有指定值，代理程式會使用 <code>LI_AGENT_SSL_CA_PATH</code> 環境變數指定的值。如果該值不存在，vRealize Log Insight Windows 代理程式會從 Windows 根憑證存放區載入憑證。</p>
<code>ssl_accept_any</code>	<p>定義 vRealize Log Insight 代理程式是否接受任何憑證。可能的值為 <code>yes</code>、<code>1</code>、<code>no</code> 或 <code>0</code>。當該值設為 <code>yes</code> 或 <code>1</code> 時，代理程式會接受來自伺服器的任何憑證，並建立用於傳送資料的安全連線。預設值為 <code>no</code>。</p>

索引鍵	說明
ssl_accept_any_trusted	可能的值為 yes、1、no 或 0。如果 vRealize Log Insight 代理程式具有本機儲存的受信任憑證授權機構簽署的憑證，並收到由另一受信任憑證授權機構所簽署的有效憑證，則會檢查組態選項。如果該值設為 yes 或 1，則代理程式會接受新的有效憑證。如果該值設為 no 或 0，則會拒絕憑證並終止連線。預設值為 no。
ssl_cn	自我簽署憑證的 Common Name。 預設值為 VMware vCenter Log Insight。您可以對照憑證 Common Name 欄位來定義要檢查的自訂 Common Name。vRealize Log Insight 代理程式會將所收到憑證的 Common Name 欄位與 [server] 區段中為 hostname 索引鍵指定的主機名稱進行比較。如果兩者不相符，代理程式會對照 liagent.ini 檔案中的 ssl_cn 索引鍵來檢查 Common Name 文字欄位。如果該值相符，則 vRealize Log Insight 代理程式會接受憑證。

**備註** 如果停用 SSL，則會忽略這些索引鍵。

#### 4 儲存並關閉 liagent.ini 檔案。

#### 範例：組態

SSL 組態的範例如下。

```
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
```

## 檢視和移除 SSL 憑證

您可以檢視已接受並新增至 vRealize Log Insight 叢集中所有節點之信任存放區的 SSL 憑證。您也可以移除不再需要的憑證。

#### 必要條件

確認您已做為具有**編輯管理員**權限的使用者身分登入 vRealize Log Insight Web 使用者介面。URL 格式為 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虛擬應用裝置的 IP 位址或主機名稱。

#### 程序

- 1 導覽至**管理**索引標籤。
- 2 在 [管理] 下，選取**憑證**。

### 3 執行下列其中一項作業：

- 若要檢視憑證的相關資訊，請按一下憑證指紋右側的資訊圖示。
- 若要移除憑證，請選取憑證，然後按一下刪除。或者，您可以按一下每個憑證指紋右側的刪除圖示。

---

**提示** 您可以使用提供的選項來排序和篩選憑證。

---

## 變更 vRealize Log Insight Web 工作階段的預設逾時期間

依預設，為保護您環境的安全，vRealize Log Insight Web 工作階段將在 30 分鐘後到期。您可以增加或減少此逾時持續時間。

---

**備註** 在逾時期間內的變更僅適用於新建立的工作階段。

---

### 必要條件

確認您已做為具有**編輯管理員**權限的使用者身分登入 vRealize Log Insight Web 使用者介面。URL 格式為 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虛擬應用裝置的 IP 位址或主機名稱。

### 程序

- 1 導覽至**管理索引標籤**。
- 2 在 [組態] 下，按一下**一般**。
- 3 在 [瀏覽器工作階段] 窗格中，指定逾時值 (以分鐘為單位)。  
值 -1 會停用工作階段逾時。
- 4 按一下**儲存**。

## 封存

如果您想要長時間保留記錄，您可以設定 vRealize Log Insight 以封存記錄資料。

### 在 vRealize Log Insight 中啟用或停用資料封存

資料封存可保留因儲存區限制而可能會從 vRealize Log Insight 虛擬應用裝置中移除的舊記錄。vRealize Log Insight 可以將封存資料儲存至 NFS 掛接。

vRealize Log Insight 會在一系列 0.5 GB 值區中收集和儲存磁碟上的記錄。值區包含壓縮記錄檔和索引。值區包含執行特定時間範圍內的查詢所需的一切內容。當值區大小超過 0.5 GB 時，vRealize Log Insight 會停止寫入、關閉值區中的所有檔案，並密封值區。

封存資料時，vRealize Log Insight 會在密封值區時，將原始壓縮記錄檔從值區複製到 NFS 掛接。無法追溯封存未啟用資料封存時所密封的值區。

封存匯出內建立的路徑所使用的格式為 `year/month/day/hour/bucketuuid/data.blob`，並會使用最初在 UTC 中建立值區時的時間戳記。

**備註** vRealize Log Insight 並不管用用於封存用途的 NFS 掛接。如果已啟用系統通知，vRealize Log Insight 會在 NFS 掛接空間即將不足或無法使用時傳送電子郵件。如果 NFS 掛接沒有足夠的可用空間，或無法使用的時間超過虛擬應用裝置的保留期間，vRealize Log Insight 會停止擷取新資料。NFS 掛接具有足夠的可用空間、狀態變為可用或停用封存時，其會再次開始擷取資料。

請勿永久掛接 NFS，或變更 `/etc/fstab` 檔案。vRealize Log Insight 本身會為您執行 NFS 掛接。

#### 必要條件

- 確認您可以存取滿足下列要求的 NFS 磁碟分割。
  - NFS 磁碟分割必須允許客體帳戶的讀取和寫入作業。
  - 掛接不需要驗證。
  - NFS 伺服器必須支援 NFS v3 或 v4。
  - 如果使用 Windows NFS 伺服器，則允許未對應的使用者 UNIX 存取 (透過 UID/GID)。
- 確認您已做為具有**編輯管理員**權限的使用者身分登入 vRealize Log Insight Web 使用者介面。URL 格式為 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虛擬應用裝置的 IP 位址或主機名稱。

#### 程序

- 1 導覽至**管理索引標籤**。
- 2 在 [組態] 下，按一下**封存**。
- 3 選取**啟用資料封存**，然後輸入 NFS 磁碟分割的路徑 (其中，記錄將以 `nfs://servername<:port-number>/exportname` 格式封存)。  
 連接埠號碼預設為 2049。
- 4 按一下**測試**以驗證連線。
- 5 按一下**儲存**。

#### 結果

**備註** 資料封存可保留本應因儲存區限制而已從 vRealize Log Insight 虛擬應用裝置中移除的記錄事件。無法再搜尋從 vRealize Log Insight 虛擬應用裝置移除但已封存的記錄事件。如果您想要搜尋封存記錄檔，則必須將其匯入 vRealize Log Insight 執行個體。如需關於匯入封存記錄檔的詳細資訊，請參閱[將 vRealize Log Insight 封存檔匯入 vRealize Log Insight](#)。

#### 後續步驟

vRealize Log Insight 重新啟動之後，請確認 ESXi 的 syslog 摘要會繼續送達 vRealize Log Insight。

## vRealize Log Insight 封存檔的格式

vRealize Log Insight 將資料封存為特定格式。

vRealize Log Insight 將封存檔儲存在 NFS 伺服器上，並根據封存時間在階層目錄中對其進行組織整理。例如，

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

其中 /backup 為 NFS 位置，2014/08/07/16 為封存時間，bd234b2d-df98-44ae-991a-e0562f10a49 為值區識別碼，data.blob 為值區的封存資料。

封存資料 data.blob 是採用 vRealize Log Insight 內部編碼的壓縮檔。它包含值區中儲存之所有訊息的原始內容，以及靜態欄位 (如時間戳記、主機名稱、來源和應用程式名稱)。

您可以將封存資料匯入 vRealize Log Insight、將封存資料匯出為原始文字檔，以及從封存資料中擷取訊息內容。請參閱[將 Log Insight 封存檔匯出為原始文字檔或 JSON](#) 及[將 vRealize Log Insight 封存檔匯入 vRealize Log Insight](#)。

## 將 vRealize Log Insight 封存檔匯入 vRealize Log Insight

資料封存可保留因儲存區限制而可能會從 vRealize Log Insight 虛擬應用裝置中移除的舊記錄。請參閱[在 vRealize Log Insight 中啟用或停用資料封存](#)。您可以使用命令列匯入已封存在 vRealize Log Insight 中的記錄檔。

---

**備註** 雖然 vRealize Log Insight 可以同時處理歷史資料和即時資料，但仍然建議您單獨部署一個 vRealize Log Insight 執行個體，用於處理匯入的記錄檔。

---

### 必要條件

- 確認您具有根使用者認證以登入 vRealize Log Insight 虛擬應用裝置。
- 確認您具有已封存 vRealize Log Insight 記錄檔之 NFS 伺服器的存取權。
- 確認 vRealize Log Insight 虛擬應用裝置具有足夠的磁碟空間來容納匯入的記錄檔。

虛擬應用裝置上的 /storage/core 磁碟分割的最小可用空間，必須約等於要匯入之封存記錄檔大小的 10 倍。

### 程序

- 1 建立與 vRealize Log Insight vApp 的 SSH 連線並以根使用者身分登入。
- 2 將共用資料夾掛接到封存資料所在的 NFS 伺服器。

- 3 若要匯入已封存 vRealize Log Insight 記錄檔的目錄，請執行下列命令。

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

#### 備註

- 為了避免修改要匯入目錄的時間戳記，請確保從您要匯入的目錄以外的目錄中執行此命令。從您要匯入的目錄中執行該命令會建立 `JavaClient.log` 檔案並更新該目錄的修改時間戳記。
- 匯入封存的資料可能需要很長時間，具體視已匯入資料夾的大小而定。

- 4 關閉 SSH 連線。

#### 後續步驟

您可以搜尋、篩選和分析已匯入的記錄事件。

## 將 Log Insight 封存檔匯出為原始文字檔或 JSON

您可以使用命令列將 vRealize Log Insight 封存檔匯出為一般原始文字檔或 JSON 格式。

**備註** 這是進階程序。命令語法和輸出格式在更新版本的 vRealize Log Insight 中可能會發生變更，不具有回溯相容性。

#### 必要條件

- 確認您具有根使用者認證以登入 vRealize Log Insight 虛擬應用裝置。
- 確認 vRealize Log Insight 虛擬應用裝置具有足夠的磁碟空間來容納匯出的檔案。

#### 程序

- 1 建立與 vRealize Log Insight vApp 的 SSH 連線並以根使用者身分登入。
- 2 在 vRealize Log Insight vApp 上建立封存目錄。

```
mkdir /archive
```

- 3 執行下列命令，將共用資料夾掛接在封存資料所在的 NFS 伺服器上。

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

- 4 檢查 vRealize Log Insight vApp 上的可用儲存空間。

```
df -h
```

## 5 將 vRealize Log Insight 封存檔匯出為原始文字檔。

```
/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 將 vRealize Log Insight 封存訊息內容匯出為 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 關閉 SSH 連線。

# 重新啟動 vRealize Log Insight 服務

您可以使用 Web 使用者介面中的 [管理] 頁面重新啟動 vRealize Log Insight。

**注意** 重新啟動 vRealize Log Insight 會關閉所有作用中使用者工作階段。vRealize Log Insight 執行個體的使用者會強制重新登入。

### 必要條件

確認您已做為具有**編輯管理員**權限的使用者身分登入 vRealize Log Insight Web 使用者介面。URL 格式為 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虛擬應用裝置的 IP 位址或主機名稱。

### 程序

- 1 導覽至**管理索引標籤**。
- 2 在 [管理] 下，按一下**叢集**。
- 3 選取叢集節點。
- 4 按一下**重新啟動主要**，然後按一下**重新啟動**。

### 後續步驟

vRealize Log Insight 重新啟動之後，請確認 ESXi 的 syslog 摘要會繼續送達 vRealize Log Insight。



## 關閉 vRealize Log Insight 虛擬應用裝置的電源

為避免關閉 vRealize Log Insight 主要節點或工作節點的電源時發生資料遺失，您必須嚴格遵循步驟順序關閉節點電源。

您必須先關閉 vRealize Log Insight 虛擬應用裝置電源，然後才能變更應用裝置的虛擬硬體。

您可以透過 vSphere Client 中的功能表選項**電源 > 關閉客體**來關閉 vRealize Log Insight 的虛擬應用裝置電源。您也可以使用虛擬應用裝置主控台，或是建立與 vRealize Log Insight 虛擬應用裝置的 SSH 連線，並執行命令。

### 必要條件

- 如果您計劃使用 SSH 連線到 vRealize Log Insight 虛擬應用裝置，請確認 TCP 連接埠 22 已開啟。
- 確認您具有根使用者認證以登入 vRealize Log Insight 虛擬應用裝置。

### 程序

- 1 建立與 vRealize Log Insight vApp 的 SSH 連線並以根使用者身分登入。
- 2 若要關閉 vRealize Log Insight 虛擬應用裝置電源，請執行 `shutdown -h now`。

### 後續步驟

您可以放心地修改 vRealize Log Insight 虛擬應用裝置的虛擬硬體。

## 下載 vRealize Log Insight 支援服務包

如果 vRealize Log Insight 因出現問題而無法如預期運作，您可以透過支援服務包的形式，將記錄檔和組態檔的複本傳送到 VMware 支援服務。

只有在 VMware 支援服務要求時才需要下載全叢集的支援服務包。您可以使用靜態 (使用節點上的磁碟空間) 或串流 (不使用節點上的磁碟空間) 的方式建立服務包，並依預設在起始機器時儲存服務包。

支援服務包的儲存位置取決於您用來取得支援服務包的選項：

選項	支援服務包位置
API - POST appliance/vm-support-bundle	這是不含本機檔案的串流版本。
API - POST appliance/support-bundle	/tmp/ui-support/
Web 使用者介面 - 靜態支援服務包	/tmp/ui-support/
Web 使用者介面 - 串流支援服務包	這是不含本機檔案的串流版本。
命令列 - scripts/loginsight-support	在目前的目錄中產生服務包。

### 必要條件

確認您已做為具有**編輯管理員**權限的使用者身分登入 vRealize Log Insight Web 使用者介面。URL 格式為 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虛擬應用裝置的 IP 位址或主機名稱。

### 程序

- 1 導覽至**管理**索引標籤。
- 2 在 [管理] 下，按一下**叢集**。
- 3 在 [支援] 標頭下，按一下**下載支援服務包**。

vRealize Log Insight 系統會收集診斷資訊，並 將資料以壓縮的 tarball 形式傳送至您的瀏覽器。

- 4 選擇要建立服務包的方法。

- 選取**靜態支援服務包**以在本機建立服務包。建立服務包會耗用節點上的磁碟空間。
- 選取**串流支援服務包**以立即開始串流支援服務包。此方法不會使用節點上的磁碟空間。

- 5 按一下**繼續**。
- 6 在 [檔案下載] 對話方塊中，按一下**儲存**。
- 7 選取您要儲存 tarball 封存的位置，然後按一下**儲存**。

### 後續步驟

您可以檢閱記錄檔內容查看錯誤訊息。解決或關閉問題後，刪除過期的支援服務包以節省磁碟空間。

## 加入或退出 VMware 客戶經驗改進計劃

在部署 vRealize Log Insight 之後，您可以加入或退出 VMware 客戶經驗改進計劃

在安裝 vRealize Log Insight 時，您可以選擇是否要參與客戶經驗改進計劃。安裝之後，您可以透過下列步驟來加入或退出計劃。

### 必要條件

確認您已做為具有**編輯管理員**權限的使用者身分登入 vRealize Log Insight Web 使用者介面。URL 格式為 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虛擬應用裝置的 IP 位址或主機名稱。

### 程序

- 1 導覽至**管理**索引標籤。
- 2 在 [組態] 下，按一下**一般**。
- 3 在 [客戶經驗改進計劃] 窗格中，選取或清除**加入 VMware 客戶經驗改進計劃**核取方塊。

選取後，即會啟動計畫並傳送資料至 `https://vmware.com`。

- 4 按一下**儲存**。

## 設定 vRealize Log Insight 的 STIG 合規性

您可以設定 vRealize Log Insight 以確保 STIG (安全性技術實作指南) 合規性，以獲得更好的安全性。此組態包括 DoD (國防部) 同意協定和其他密碼原則限制。

### 必要條件

確認您已做為具有**編輯管理員**權限的使用者身分登入 vRealize Log Insight Web 使用者介面。URL 格式為 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虛擬應用裝置的 IP 位址或主機名稱。

### 程序

- 1 導覽至**管理索引**標籤。
- 2 在 [組態] 下，按一下**一般**。
- 3 在 [安全性技術實作指南] 窗格中，執行相關的動作：
  - 按一下 **DoD 同意協定** 切換按鈕，以在使用者登入 vRealize Log Insight 時顯示強制 DoD 同意協定。選取登入訊息類型：登入頁面上的簡單訊息、在登入前接受同意的登入頁面，或是包含接受 DoD 同意協定按鈕的同意對話方塊。新增同意標題和說明。  
當 DoD 同意協定啟用時，使用者會在登入時看到選取的登入訊息類型。
  - 按一下 **密碼原則限制** 切換按鈕，以啟用使用者帳戶的進一步密碼限制，以及鎖定帳戶的額外規則。  
如果已啟用密碼原則限制，則會將下列額外的規則套用至密碼：
    - 密碼必須包含至少 15 個字元。
    - 使用者在 24 小時內僅能變更其密碼一次。
    - 當使用者變更其密碼時，無法使用最後五個密碼。
    - 當使用者變更其密碼時，新密碼中至少必須有八個字元與舊密碼不同。
 如果已啟用密碼原則限制，則在下列情況下會鎖定使用者帳戶：
    - 使用者未登入 vRealize Log Insight 達 35 天。
    - 使用者未變更其密碼達 60 天。

---

**備註** 超級管理員使用者帳戶永遠不會遭到鎖定。

---

- 4 按一下**儲存**。

## 啟用 vRealize Log Insight 的 FIPS 模式

您可以設定 vRealize Log Insight 以確保落實 FIPS (聯邦資訊處理標準)，藉此提升安全性。這組標準涵蓋檔案處理、加密演算法，以及其他資訊技術標準，適用於美國的非軍事政府機構，以及與政府承包商和供應商合作的代理機構。當您啟動 FIPS 時，vRealize Log Insight 會使用安全性層級 1 的 FIPS 140-2 標準，這是指定用於保護敏感或重要資料的基本安全標準。

如需不同 VMware 產品如何支援 FIPS 140-2 的相關資訊，請參閱 <https://www.vmware.com/security/certifications/fips.html>。

vRealize Log Insight 使用 Apache Thrift 進行節點到節點的通訊。啟用 FIPS 會自動透過 SSL 啟用 Thrift，讓這個通訊更安全。但您無需啟用 FIPS 也可以透過 SSL 啟用 Thrift。如需詳細資訊，請參閱 <https://kb.vmware.com/s/article/82299>。

#### 必要條件

確認您已做為具有**編輯管理員**權限的使用者身分登入 vRealize Log Insight Web 使用者介面。URL 格式為 <https://log-insight-host>，其中 *log-insight-host* 是 vRealize Log Insight 虛擬應用裝置的 IP 位址或主機名稱。

#### 程序

- 1 導覽至**管理**索引標籤。
- 2 在 [組態] 下，按一下**一般**。
- 3 在 FIPS 模式窗格中，按一下**啟用 FIPS 模式**切換按鈕以啟動 FIPS。

---

**注意** FIPS 一旦啟動便無法停用。

---

- 4 按一下**儲存**。

#### 結果

當您儲存 FIPS 設定時，所有節點都會重新開機。您必須等待幾分鐘，才能再次使用 vRealize Log Insight。

# 管理 vRealize Log Insight 叢集

# 5

您可以新增、移除及升級 vRealize Log Insight 叢集的節點。

**備註** vRealize Log Insight 不支援 WAN 叢集。vRealize Log Insight 的目前版本不支援 WAN 叢集 (也稱為地理叢集、高可用性叢集或遠端叢集)。應將叢集中的所有節點部署在相同 Layer 2 LAN 中。此外，必須在節點之間開啟 [連接埠與外部介面](#) 中所述的連接埠才能進行正常通訊。

本章節討論下列主題：

- 將工作節點新增到 vRealize Log Insight 叢集
- 從 vRealize Log Insight 叢集中移除工作節點
- 使用整合式負載平衡器
- 查詢生產中叢集檢查的結果

## 將工作節點新增到 vRealize Log Insight 叢集

部署 Log Insight 虛擬應用裝置的新執行個體，然後將其新增到現有的 Log Insight 主要節點。

### 程序

#### 1 部署 vRealize Log Insight 虛擬應用裝置

下載 vRealize Log Insight 虛擬應用裝置。VMware 將 vRealize Log Insight 虛擬應用裝置做為 .ova 檔案進行散佈。使用 vSphere Client 部署 vRealize Log Insight 虛擬應用裝置。

#### 2 加入現有部署

部署並設定獨立 vRealize Log Insight 節點後，您可以部署新的 vRealize Log Insight 執行個體並將其新增到現有節點，以組成 vRealize Log Insight 叢集。

## 部署 vRealize Log Insight 虛擬應用裝置

下載 vRealize Log Insight 虛擬應用裝置。VMware 將 vRealize Log Insight 虛擬應用裝置做為 .ova 檔案進行散佈。使用 vSphere Client 部署 vRealize Log Insight 虛擬應用裝置。

### 必要條件

- 確認您有 vRealize Log Insight 虛擬應用裝置 .ova 檔案的複本。
- 請確認您擁有將 OVF 範本部署到詳細目錄的權限。

- 確認您的環境具有足夠資源，可滿足 vRealize Log Insight 虛擬應用裝置的最低需求。請參閱[最低需求](#)。
- 確認您已閱讀並瞭解虛擬應用裝置大小調整的建議。請參閱[調整 Log Insight 虛擬應用裝置的大小](#)。

#### 程序

- 1 在 vSphere Client 中，選取**檔案 > 部署 OVF 範本**。
- 2 遵循**部署 OVF 範本精靈**中的提示。
- 3 在 [選取組態] 頁面上，依據您計畫從中收集記錄的環境大小，選取 vRealize Log Insight 虛擬應用裝置的大小。

**小型**是生產環境的最低需求。

vRealize Log Insight 提供了可供您選擇的預設 VM (虛擬機器) 大小，以符合您環境的擷取需求。這些預設是已經過認證的運算和磁碟資源大小組合，但您也可以之後新增額外的資源。小型組態會耗用最少的資源，但仍可維持受支援狀態。額外的小型組態僅適用於示範。

預設大小	記錄擷取速率	虛擬 CPU	記憶體	IOPS	Syslog 連線 (作用中 TCP 連線)	每秒事件數
超小型	6 GB/天	2	4 GB	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	32 GB	1500	750	15,000

您可以使用 syslog 彙總工具來增加用於將事件傳送至 vRealize Log Insight 的 syslog 連線數。但是，每秒最大事件數已固定，不取決於是否使用 syslog 彙總工具。無法將 vRealize Log Insight 執行個體用作 syslog 彙總工具。

**備註** 如果選取**大型**，您必須在部署後升級 vRealize Log Insight 虛擬機器上的虛擬硬體。

- 4 在 [選取儲存區] 頁面上，選取磁碟格式。
  - **完整佈建消極式歸零**以預設的完整格式建立虛擬磁碟。虛擬磁碟所需的空間會在建立時加以配置。建立過程中不會清除實體裝置上保留的資料，但之後首次從虛擬應用裝置寫入時，可依需要將這些資料歸零。
  - **完整佈建積極式歸零**會建立一種完整佈建虛擬磁碟類型，可支援 Fault Tolerance 等叢集功能。在建立時會為虛擬磁碟配置所需的空間。與一般格式相反，建立虛擬磁碟時會將實體裝置上保留的資料歸零。建立此類格式的磁碟所需的時間可能會比建立其他類型的磁碟久得多。

**重要** 儘可能使用完整佈建積極式歸零磁碟部署 vRealize Log Insight 虛擬應用裝置，以便虛擬應用裝置實現更佳效能及作業。

- **精簡佈建**以精簡格式建立磁碟。磁碟會在其中儲存的資料量增加時隨之擴充。如果您的儲存裝置不支援完整佈建磁碟或者您想要節省 vRealize Log Insight 虛擬應用裝置上未使用的磁碟空間，請使用精簡佈建磁碟部署虛擬應用裝置。

**備註** 不支援在 vRealize Log Insight 虛擬應用裝置上壓縮磁碟，這樣可能會導致資料損毀或遺失。

- 5 (選擇性) 在 [選取網路] 頁面上，設定 vRealize Log Insight 虛擬應用裝置的網路參數。您可以選取 IPv4 或 IPv6 通訊協定。

若未提供網路設定 (如 IP 位址、DNS 伺服器 and 閘道資訊)，則 vRealize Log Insight 會使用 DHCP 進行相關設定。

**注意** 請勿指定兩個以上的網域名稱伺服器。如果指定兩個以上的網域名稱伺服器，則 vRealize Log Insight 虛擬應用裝置中將忽略所有已設定的網域名稱伺服器。

使用以逗點分隔的清單來指定網域名稱伺服器。

- 6 (選擇性) 在 [自訂範本] 頁面上，如果您沒有使用 DHCP，請設定網路內容。

在 [應用程式] 下，如果您想要在雙重堆疊網路中執行虛擬機器，請選取**優先使用 IPv6 位址**核取方塊。

**注意** 如果您想要使用純 IPv4 (即使您的網路支援 IPv6)，請勿選取**優先使用 IPv6 位址**核取方塊。僅在您的網路有 IPv6 的雙重堆疊或純堆疊支援時，才適合選取此核取方塊。

- 7 (選擇性) 在 [自訂範本] 頁面上，選取**其他內容**，並設定 vRealize Log Insight 虛擬應用裝置的根密碼。

SSH 必須具備根密碼。您也可以透過 VMware Remote Console 設定此密碼。

- 8 依照提示完成部署。

如需部署虛擬應用裝置的相關資訊，請參閱《部署 vApp 及虛擬應用裝置使用者指南》。

開啟虛擬應用裝置的電源後，初始化程序隨即開始。初始化程序需要幾分鐘的時間才能完成。程序結束時，虛擬應用裝置會重新啟動。

- 9 導覽至主控台索引標籤，然後確認 vRealize Log Insight 虛擬應用裝置的 IP 位址。

IP 位址首碼	說明
https://	虛擬應用裝置上的 DHCP 組態正確。
http://	虛擬應用裝置上的 DHCP 組態失敗。 <ul style="list-style-type: none"> <li>a 關閉 vRealize Log Insight 虛擬應用裝置的電源。</li> <li>b 在虛擬應用裝置上按一下滑鼠右鍵，然後選取<b>編輯設定</b>。</li> <li>c 設定虛擬應用裝置的靜態 IP 位址。</li> </ul>

#### 後續步驟

- 如果想要設定獨立的 vRealize Log Insight 部署，請參閱[設定新的 Log Insight 部署](#)。

vRealize Log Insight Web 介面位於 `https://log-insight-host/`，其中 `log-insight-host` 是 vRealize Log Insight 虛擬應用裝置的 IP 位址或主機名稱。

## 加入現有部署

部署並設定獨立 vRealize Log Insight 節點後，您可以部署新的 vRealize Log Insight 執行個體並將其新增到現有節點，以組成 vRealize Log Insight 叢集。



vRealize Log Insight 可以使用叢集中的多個虛擬應用裝置執行個體來進行擴充。叢集可線性擴充擷取輸送量、提升查詢效能，並允許高可用性擷取。在叢集模式下，vRealize Log Insight 會提供主要節點和工作節點。主要節點和工作節點負責資料子集。主要節點可以查詢資料的所有子集，並彙總結果。您可能需要更多節點來支援站台的需求。您可以使用叢集中的三至十八個節點。這表示完全正常運作的叢集必須有至少三個健全狀況良好的節點。大型叢集中的大多數節點必須健全狀況良好。例如，如果六個節點的叢集有三個節點失敗，直到移除失敗的節點之前，沒有節點會完全正常運作。

#### 必要條件

- 在 vSphere Client 中，記下工作 vRealize Log Insight 虛擬應用裝置的 IP 位址。
- 確認您知道主要 vRealize Log Insight 虛擬應用裝置的 IP 位址或主機名稱。
- 確認您具有主要 vRealize Log Insight 虛擬應用裝置的管理員帳戶。
- 確認 vRealize Log Insight 主要節點和工作節點的版本處於同步狀態。請勿將舊版 vRealize Log Insight 工作節點新增到較新版本的 vRealize Log Insight 主要節點。
- 您必須同步 vRealize Log Insight 虛擬應用裝置與 NTP 伺服器上的時間。請參閱[同步 Log Insight 虛擬應用裝置上的時間](#)。
- 如需支援的瀏覽器版本的相關資訊，請參閱[vRealize Log Insight 版本說明](#)。

#### 程序

- 1 使用支援的瀏覽器導覽到 vRealize Log Insight 工作的 Web 使用者介面。

URL 格式為 `https://log_insight-host/`，其中 `log_insight-host` 是工作 vRealize Log Insight 虛擬應用裝置的 IP 位址或主機名稱。

初始組態精靈隨即開啟。

- 2 按一下**加入現有部署**。
- 3 輸入 vRealize Log Insight 主要節點的 IP 位址或主機名稱，然後按一下**執行**。  
工作會將要求傳送到 vRealize Log Insight 主要節點以加入現有部署。
- 4 按一下**按一下這裡以存取 [叢集管理] 頁面**。
- 5 以管理員身分登入。  
隨即載入 [叢集] 頁面。
- 6 按一下**允許**。

工作節點會加入現有部署，並且 vRealize Log Insight 將開始在叢集中運作。

#### 後續步驟

- 視需要新增更多工作節點。叢集必須具有至少三個節點。



## 從 vRealize Log Insight 叢集中移除工作節點


您可以從 vRealize Log Insight 叢集移除不再正確運作的工作節點。請勿從叢集中移除正常運作的工作節點。

**警告** 移除節點會導致資料遺失。如果必須移除節點，請確保已首先備份此節點。避免在新增新節點的 30 分鐘內移除節點。


### 必要條件

確認您已做為具有**編輯管理員**權限的使用者身分登入 vRealize Log Insight Web 使用者介面。URL 格式為 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虛擬應用裝置的 IP 位址或主機名稱。

### 程序

- 1 導覽至**管理**索引標籤。
- 2 在 [管理] 下，按一下**叢集**。
- 3 在工作資料表中，找到您想要的節點，按一下暫停圖示 ，然後按一下**繼續**。  
節點現在處於維護模式。

**備註** 處於維護模式的節點將繼續接收記錄。

- 4 按一下  移除節點。  
vRealize Log Insight 會從叢集中移除節點並送出一個電子郵件通知。
- 5 一旦移除，節點可做為獨立節點來啟動，或啟動並加入叢集。

## 使用整合式負載平衡器

vRealize Log Insight 整合式負載平衡器 (ILB) 支援 vRealize Log Insight 叢集，且能確保即便在部分 vRealize Log Insight 節點無法使用時，vRealize Log Insight 仍可接受傳入擷取流量。您也可以設定多個虛擬 IP 位址。

**備註** 不支援將外部負載平衡器用於 vRealize Log Insight，包括 vRealize Log Insight 叢集。

最佳做法是 在所有部署中加入 ILB，包括單一節點執行個體。請將查詢和擷取流量傳送至 ILB，以便必要時在未來能夠輕鬆支援叢集。ILB 可平衡叢集中各節點間的流量，並盡可能減輕管理額外負荷。

ILB 可確保即便在部分 vRealize Log Insight 節點無法使用時，vRealize Log Insight 仍可接受傳入擷取流量。此外，ILB 會在可用的 vRealize Log Insight 節點之間公平地平衡傳入流量。使用 Web 使用者介面和擷取 (透過 Syslog 或擷取 API) 的 vRealize Log Insight 用戶端，將透過 ILB 位址連線到 vRealize Log Insight。

ILB 要求所有 vRealize Log Insight 節點都位於相同的第 2 層網路上 (例如位於同一交換器的後方)，或者可以相互接收和傳送 ARP 要求。必須設定 ILB IP 位址，以便任何 vRealize Log Insight 節點都可以擁有該位址並接收其流量。通常，這意味著 ILB IP 位址將與 vRealize Log Insight 節點的實體位址位於相同的子網路中。設定 ILB IP 位址後，可嘗試從不同的網路對其執行 Ping 動作以確保該位址可連線。

若要簡化未來的變更和升級，您可以將用戶端指向解析為 ILB IP 位址的 FQDN，而非直接指向 ILB IP 位址。

## 關於 Direct Server Return 組態

vRealize Log Insight 負載平衡器使用 Direct Server Return (DSR) 組態。在 DSR 中，所有傳入流量都會通過 vRealize Log Insight 節點，該節點即為目前的負載平衡器節點。傳回流量會從 vRealize Log Insight 伺服器直接傳送回用戶端，而無需經過負載平衡器節點。

## 多個虛擬 IP 位址

您可以針對整合式負載平衡器設定多個虛擬 IP 位址 (VIP)。還可以為每個 VIP 設定靜態標籤清單，以便從 VIP 接收的每個記錄訊息都使用設定的標籤加以註釋。

---

**備註** 最佳做法是為 vRealize Log Insight 執行個體設定最多 12 個 VIP。

---

## 啟用整合式負載平衡器

在 vRealize Log Insight 叢集上啟用 vRealize Log Insight 整合式負載平衡器 (ILB) 時，您必須設定一或多個虛擬 IP 位址。

整合式負載平衡器支援一或多個虛擬 IP 位址 (VIP)。每個 VIP 會在可用的 vRealize Log Insight 節點之間平衡傳入擷取和查詢流量。這是將所有 vRealize Log Insight 用戶端透過 VIP 連線而不直接連線至節點的最佳做法。

若要簡化未來的變更和升級，您可以將用戶端指向解析為 ILB IP 位址的 FQDN，而非直接指向 ILB IP 位址。vSphere 和 vRealize Operations 整合及警示訊息會使用 FQDN (如果提供)，否則它們會使用 ILB IP 位址。vRealize Log Insight 可將 FQDN 解析為指定的 IP 位址，這表示您提供的 FQDN 值應與 DNS 中定義的值相符。

### 必要條件

- 確認所有 vRealize Log Insight 節點以及指定的整合式負載平衡器 IP 位址位於相同的網路中。
- 如果您正在使用 vRealize Log Insight 搭配 NSX，請確認 NSX 邏輯交換器上已停用**啟用 IP 探索**選項。
- vRealize Log Insight 主要節點和工作節點必須具有相同的憑證。否則，設定為透過 SSL 進行連線的 vRealize Log Insight 代理程式會拒絕連線。將 CA 簽署憑證上傳到 vRealize Log Insight 主要節點和工作節點時，請在憑證產生要求期間將 [一般名稱] 設定為 ILB FQDN (或 IP 位址)。請參閱 [產生憑證簽署要求](#)。
- 您必須同步 vRealize Log Insight 虛擬應用裝置與 NTP 伺服器上的時間。請參閱 [同步 Log Insight 虛擬應用裝置上的時間](#)。

## 程序

- 1 導覽至**管理**索引標籤。
- 2 在 [管理] 下，按一下**叢集**。
- 3 在 [整合式負載平衡器] 區段中，選取**新增虛擬 IP 位址**，然後輸入用於整合式負載平衡的虛擬 IP (vIP) 位址。
- 4 (選擇性) 若要設定多個虛擬 IP 位址，請按一下**新增虛擬 IP 位址**並輸入 IP 位址。您可以選擇輸入 FQDN 和標籤。
  - 每個 vIP 都應與每個節點上的至少一個網路介面位於同一子網路中，並且 vIP 必須可用 (未由任何其他機器使用)。
  - 標籤可讓您將具有預先定義值的欄位新增至事件，以進行更輕鬆的查詢。您可以新增多個以逗點分隔的標籤。所有透過 vIP 進入系統的事件均標有 vIP 標籤。
  - 您可以為 ILB vIP 設定靜態標籤 (機碼=值) 清單，以便從 vIP 收到的每則記錄訊息都使用所設定的標籤加以註釋。
- 5 (選擇性) 若要讓 vRealize Log Insight 使用者可透過 FQDN 存取叢集，請將用戶端指向 FQDN，而非直接指向已設定的 ILB IP 位址。

您可以讓用戶端指向解析為 ILB IP 位址的 FQDN，以便簡化未來的變更和升級。您可以讓用戶端指向 FQDN，而非直接指向 ILB IP 位址。

- 6 按一下**儲存**。

整合式負載平衡器由 vRealize Log Insight 叢集中的一個節點管理，宣告該服務的前置字元。目前的前置字元由節點旁的文字 (ILB) 表示。

## 查詢生產中叢集檢查的結果

生產中叢集檢查服務會在每個節點上定期執行眾多檢查。您可以使用 CLI 查詢生產中叢集檢查的最新結果。

例如，服務可判定叢集是否正在執行且是否按預期設定，或與其他系統的整合中是否存在任何問題。下方列出了其他檢查。

- 是否已在多主機部署中設定 NTP？
- 是否可以連線到 Active Directory (如果目前已設定)？
- 是否可以進行 Active Directory 驗證 (如果目前已設定)？
- 是否可以連線到 Active Directory 主機和 Kerberos 主機 (如果目前已設定 Active Directory)？
- 系統是否正在不受支援的雙主機部署中執行？
- /tmp 中是否有執行升級所需的足夠空間？
- /storage/core 中是否有執行升級所需的足夠空間？
- localhost 是否已正確放置在 /etc/hosts 內？

## 程序

- 1 在命令列中，建立與 vRealize Log Insight 虛擬應用裝置的 SSH 連線，並以根使用者身分登入。
- 2 在命令列中，輸入 `/usr/lib/loginsight/application/sbin/query-check-results.sh`，然後按下 **Enter**。

# 設定、監控及更新 vRealize Log Insight 代理程式

# 6

您可以集中管理多個 vRealize Log Insight 代理程式的組態、監控其狀態，以及啟用自動更新。

本章節討論下列主題：

- 集中式代理程式組態和代理程式群組
- 監控 vRealize Log Insight 代理程式的狀態
- 從伺服器啟用代理程式自動更新

## 集中式代理程式組態和代理程式群組

您可以使用 vRealize Log Insight 伺服器，從應用程式使用者介面內設定代理程式。代理程式會定期輪詢 vRealize Log Insight 伺服器，以判定新的組態是否可用。

您可以將需要相同組態的代理程式歸為一組。例如，您可以將所有 vRealize Log Insight Windows 代理程式歸為一組，以區別於 vRealize Log Insight Linux 代理程式。

在**所有代理程式**功能表中，系統會自動列出內容套件中的現有代理程式群組。列出的代理程式與您已安裝（例如，vSphere 內容套件）並使用代理程式群組的內容套件相關。當您按一下**我的內容**或**共用內容**時，所有使用者建立的代理程式群組都會顯示在**內容套件 > 自訂內容**下方。

至少具有僅限檢視管理員角色的使用者可以使用代理程式群組範本匯出內容套件。

---

### 備註

- 您不能多次使用相同的內容套件範本。
- 內容套件群組為唯讀。

---

內容套件中僅使用以 [winlog]、[filelog]、[journalldlog] 和 [parser] 開頭的組態區段。其他區段將不會匯出為內容套件的一部分。只有 [winlog]、[filelog] 和 [parser] 區段下的單行註解（以 、 開頭的行）會保留在內容套件中。

---

**備註** 單一代理程式可以屬於多個代理程式群組，且會繼承集中式代理程式組態的所有設定。

---

您可以建立〈所有代理程式〉群組的組態，如[建立代理程式群組](#)中所述。如果代理程式是從集中式代理程式組態和其他組態的組合進行設定，則代理程式組態會是合併這兩個組態的結果。如需合併的詳細資訊，請參閱[代理程式群組組態合併](#)。

---

**備註** 請盡可能使用代理程式群組，除非有需要，否則請避免使用〈所有代理程式〉組態。

---

請參閱使用 vRealize Log Insight 代理程式以取得設定代理程式，以及合併本機和伺服器端組態的相關資訊。

- [代理程式群組組態合併](#)

有了代理程式群組，代理程式可以是多個群組的一部分，也可以屬於預設群組所有代理程式，從而實現集中式組態。

- [建立代理程式群組](#)

您可以為使用相同參數所設定的代理程式建立群組。

- [編輯代理程式群組](#)

您可以編輯代理程式群組的名稱和說明、變更篩選器以及編輯組態。

- [將內容套件代理程式群組新增為代理程式群組](#)

您可將已定義為內容套件一部分的代理程式群組新增至作用中群組，並將代理程式組態套用至該群組。

- [刪除代理程式群組](#)

您可以刪除代理程式群組，以將其從作用中群組清單中移除。

## 代理程式群組組態合併

有了代理程式群組，代理程式可以是多個群組的一部分，也可以屬於預設群組所有代理程式，從而實現集中式組態。

合併發生在伺服器端，產生的組態會與代理程式端的組態合併。合併的組態是根據下列規則產生的。

- 個別群組組態具有較高的優先順序，會覆寫 [所有代理程式] 群組設定。
- [所有代理程式] 群組組態會覆寫本機組態。
- 您無法以相同名稱設定不同群組中的區段，[所有代理程式] 群組除外。但是，個別群組中的區段具有較高的優先順序。

---

**備註** 為防止代理程式遺失，請勿從伺服器集中變更代理程式組態的 **hostname** 和 **port** 參數。

---

合併的組態會儲存在代理程式端的 `liagent-effective.ini` 檔案中。若為 Windows 系統，該檔案儲存在 `%ProgramData%\VMware\Log Insight Agent` 中，若為 Linux 系統，則儲存在 `/var/lib/loginsight-agent/` 中。

## 建立代理程式群組

您可以為使用相同參數所設定的代理程式建立群組。

## 必要條件

確認您已做為具有**編輯管理員**權限的使用者身分登入 vRealize Log Insight Web 使用者介面。URL 格式為 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虛擬應用裝置的 IP 位址或主機名稱。

## 程序

- 1 導覽至**管理索引**標籤。
- 2 在 [管理] 下，按一下**代理程式**。
- 3 在**所有代理程式**功能表中，開啟 [重新整理] 按鈕旁邊的代理程式名稱欄位中的下拉式功能表，然後按一下**新增群組**。
- 4 為該代理程式群組提供唯一名稱和說明，然後按一下**新增群組**。

代理程式群組隨即建立並顯示於**所有代理程式**清單中，但並未儲存。

- 5 為代理程式群組指定一或多個篩選器。若要建立篩選器，請指定欄位名稱、運算子和值。

篩選器可以包含萬用字元，例如 \* 和 ?。例如，您可以選取作業系統篩選器 `contains`，並指定值 `windows` 來識別所有 Windows 代理程式以進行設定。

- a 選擇下列其中一個欄位以進行篩選：

- IP 位址
- 主機名稱
- 版本
- 作業系統

- b 從下拉式功能表中選取運算子，然後指定值。

運算子	說明
符合	尋找符合指定字串和萬用字元規格的字串，其中 * 表示零或更多字元和 ? 表示任何單一字元。支援前置詞和後置詞萬用字元。 例如， <code>*test*</code> 會比對如 <code>test123</code> 或 <code>my-test-run</code> 的字串。
不符合	排除符合指定字串和萬用字元規格的字串，其中 * 表示零或更多字元和 ? 表示任何單一字元。支援前置詞和後置詞萬用字元。 例如， <code>test*</code> 會篩選掉 <code>test123</code> ，但不會排除 <code>mytest123</code> 。 <code>%Test*</code> 不會篩選掉 <code>test123</code> ，但會排除 <code>xtest123</code>
開頭為	尋找以指定字元字串開頭的字串。 例如， <code>test</code> 會找到 <code>test123</code> 或 <code>test</code> ，而非 <code>my-test123</code> 。
開頭非	排除以指定字元字串開頭的字串。 例如， <code>test</code> 會篩選掉 <code>test123</code> ，而非 <code>my-test123</code> 。

- 6 在 [代理程式組態] 區域指定代理程式組態值，然後按一下**儲存新的群組**。

## 結果

下一個輪詢間隔後會套用此代理程式組態。

## 編輯代理程式群組

您可以編輯代理程式群組的名稱和說明、變更篩選器以及編輯組態。

### 必要條件

確認您已做為具有**編輯管理員**權限的使用者身分登入 vRealize Log Insight Web 使用者介面。URL 格式為 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虛擬應用裝置的 IP 位址或主機名稱。

### 程序

- 1 導覽至**管理**索引標籤。
- 2 在 [管理] 下，按一下**代理程式**。
- 3 在**所有代理程式**功能表中，選取適當代理程式群組的名稱，然後按一下鉛筆圖示來編輯該名稱。
- 4 做出變更。

要編輯的項目	動作
名稱或說明	請進行必要的變更，然後按一下 <b>儲存</b> 。
篩選器或組態	請進行必要的變更，然後按一下 <b>儲存群組</b> 。

## 將內容套件代理程式群組新增為代理程式群組

您可將已定義為內容套件一部分的代理程式群組新增至作用中群組，並將代理程式組態套用至該群組。

### 必要條件

確認您已做為具有**編輯管理員**權限的使用者身分登入 vRealize Log Insight Web 使用者介面。URL 格式為 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虛擬應用裝置的 IP 位址或主機名稱。

### 程序

- 1 導覽至**管理**索引標籤。
- 2 在 [管理] 下，按一下**代理程式**。
- 3 在**所有代理程式**功能表中，選取適用於 [可用範本] 清單的代理程式範本。
- 4 按一下**複製範本**將內容套件代理程式群組複製到作用中群組。
- 5 按一下**複製**。
- 6 選取所需的篩選器，然後按一下**儲存新的群組**。



## 結果

內容套件代理程式群組即新增到作用中群組，且將根據您所指定的篩選器來設定代理程式。

## 刪除代理程式群組

您可以刪除代理程式群組，以將其從作用中群組清單中移除。

### 必要條件

確認您已做為具有**編輯管理員**權限的使用者身分登入 vRealize Log Insight Web 使用者介面。URL 格式為 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虛擬應用裝置的 IP 位址或主機名稱。

### 程序

- 1 導覽至**管理索引標籤**。
- 2 在 [管理] 下，按一下**代理程式**。
- 3 在**所有代理程式**功能表中，選取要刪除之代理程式群組的名稱，然後按一下其名稱旁的 X 圖示。
- 4 按一下**刪除**。

## 結果

代理程式群組即從作用中群組中移除。

## 監控 vRealize Log Insight 代理程式的狀態

您可以監控 vRealize Log Insight Windows 和 Linux 代理程式的狀態，並檢視有關其作業的目前統計資料。

只有已設定為透過 CFAPI 傳送資料的代理程式才會顯示於 [代理程式] 頁面上。設定為透過 syslog 傳送資料的代理程式會與其他 syslog 來源一起顯示於 [主機] 頁面上。如果通訊協定從 CFAPI 變更為 syslog，則 [統計資料] 頁面將不會更新和顯示統計資料，且代理程式狀態會顯示為「已中斷連線」。該處顯示的資料每隔 30 秒會從 LI 代理程式傳送。vRealize Log Insight 最多可顯示 15,000 個代理程式的相關資訊。

如果您將通訊協定從 CFAPI 變更為 Syslog，則 [代理程式] 頁面上的統計資料將停止更新和顯示，且代理程式狀態會顯示為已中斷連線。該處顯示的資料每隔 30 秒會從 vRealize Log Insight 代理程式傳送。

---

**備註** 如果您在代理程式組態中變更 vRealize Log Insight 伺服器的主機 IP，則代理程式會將頁面統計料重設為零。

---

### 必要條件

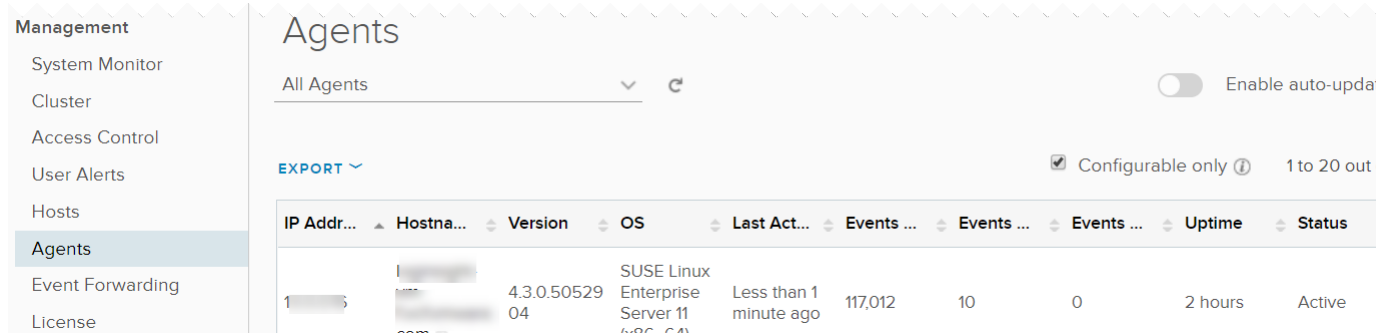
確認您已使用具有**檢視管理員**權限的使用者身分登入 vRealize Log Insight Web 使用者介面。URL 格式為 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虛擬應用裝置的 IP 位址或主機名稱。

### 程序

- 1 導覽至**管理索引標籤**。

## 2 在 [管理] 下，按一下代理程式。

使用 CFAPI 傳送資料之每個代理程式的狀態資訊隨即顯示。



### 後續步驟

您可以使用 [代理程式] 頁面中的資訊來監控安裝之 vRealize Log Insight Windows 和 Linux 代理程式的作業。按一下代理程式主機名稱以前往該主機的 [互動式分析] 頁面。在從 LI 代理程式設定主機名稱參數後，如果您使用預設的 CFAPI 通訊協定並將其指向 Log Insight 執行個體，您便可以藉由開啟 [代理程式統計資料] 頁面並確認該代理程式有出現在代理程式清單中，來監控連線。您可以使用 [主機名稱] 資料行下面的連結來導覽至 [Insight 代理程式] 頁面，並檢查來自上述代理程式的記錄。

## 從伺服器啟用代理程式自動更新

您可以從 vRealize Log Insight 伺服器啟用所有代理程式的自動更新。

自動更新會將最新的可用更新套用至連線至伺服器的所有代理程式。您可以透過編輯代理程式的 `liagent.ini` 檔案，停用個別伺服器的自動更新功能。如需詳細資訊，請參閱使用 vRealize Log Insight 代理程式。

伺服器的自動更新預設為停用。

### 必要條件

代理程式必須處於作用中狀態，且必須是 4.3 版或更新版本。

### 程序

- 1 導覽至管理索引標籤。
- 2 按一下左側功能表中的代理程式。
- 3 在 [代理程式] 頁面上，按一下為所有代理程式啟用自動更新的切換控制。

### 結果

有可用的更新時，連線至此伺服器的代理程式即會進行更新。

# 監控 vRealize Log Insight

# 7

您可以監控 vRealize Log Insight 虛擬應用裝置和傳送記錄事件至 vRealize Log Insight 的主機與裝置。

本章節討論下列主題：

- [檢查 vRealize Log Insight 虛擬應用裝置的健全狀況](#)
- [監控傳送記錄事件的主機](#)
- [設定系統通知以報告相關的非作用中主機](#)

## 檢查 vRealize Log Insight 虛擬應用裝置的健全狀況

您可以檢查 vRealize Log Insight 虛擬應用裝置上的可用資源和作用中查詢，以及檢視 vRealize Log Insight 作業的目前統計資料。

### 必要條件

確認您已做為具有**編輯管理員**權限的使用者身分登入 vRealize Log Insight Web 使用者介面。URL 格式為 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虛擬應用裝置的 IP 位址或主機名稱。

### 程序

- 1 導覽至**管理索引標籤**。
- 2 在 [管理] 下，按一下**系統監視器**。
- 3 如果 vRealize Log Insight 正在做為叢集執行，請按一下**顯示下列各項的資源**，並選擇您想要監控的節點。

- 4 按一下 [系統監視器] 頁面上的按鈕，可檢視所需資訊。

選項	說明
資源	檢視 vRealize Log Insight 虛擬應用裝置上的 CPU、記憶體、IOPS (讀取和寫入活動) 與儲存區使用量的相關資訊。 位於右側的圖表示過去 24 小時的歷史資料，每隔 5 分鐘重新整理一次。位於左側的圖表顯示過去 5 分鐘的資訊，每隔 3 秒鐘重新整理一次。
作用中查詢	檢視 vRealize Log Insight 中目前作用中查詢的相關資訊。
統計資料	檢視記錄擷取作業和速率的統計資料。 若要檢視更詳細的統計資料，請按一下 <b>顯示進階統計資料</b> 。

#### 後續步驟

您可以使用 [系統監視器] 頁面中的資訊來管理 vRealize Log Insight 虛擬應用裝置上的資源。

## 監控傳送記錄事件的主機

您可以檢視所有將記錄事件傳送到 vRealize Log Insight 並對其進行監控之主機和裝置的清單。

主機表格中的項目會在最後一個擷取事件之後的三個月到期。

#### 必要條件

確認您已做為具有**編輯管理員**權限的使用者身分登入 vRealize Log Insight Web 使用者介面。URL 格式為 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虛擬應用裝置的 IP 位址或主機名稱。

#### 程序

- 1 導覽至**管理索引標籤**。
- 2 在 [管理] 下，按一下**主機**。

**備註** 如果您已將 vCenter Server 設定為傳送事件和警示，但是未將個別 ESXi 主機設定為傳送記錄，則 [主機名稱] 資料行會同時列出 vCenter Server 和個別 ESXi 主機做為來源，而非僅僅列出 vCenter Server。

#### 後續步驟

具有管理員權限的使用者可以設定當主機處於非作用中時傳送的系統通知。如需詳細資訊，請參閱[設定系統通知以報告相關的非作用中主機](#)。

## 設定系統通知以報告相關的非作用中主機

vRealize Log Insight 包含內建的通知，您可以用來瞭解哪些主機處於非作用中狀態已達指定的時間。

您可以從 [主機] 畫面啟用通知，並指定觸發通知的臨界值。您可以將它套用至所有主機或較少的主機清單。

## 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 ⓘ

**SAVE** **RESET TO DEFAULTS...**

### 必要條件

確認您已做為具有**編輯管理員**權限的使用者身分登入 vRealize Log Insight Web 使用者介面。URL 格式為 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虛擬應用裝置的 IP 位址或主機名稱。

### 程序

- 1 導覽至**管理索引標籤**。
- 2 在 [管理] 下，按一下**主機**。

**備註** 如果您已將 vCenter Server 設定為傳送事件和警示，但是未將個別 ESXi 主機設定為傳送記錄，則 [主機名稱] 資料行會同時列出 vCenter Server 和個別 ESXi 主機做為來源，而非僅僅列出 vCenter Server。

- 3 在**主機**頁面上選取**非作用中主機通知**，以顯示用來設定應於何時以及對哪些主機傳送通知的表單。
- 4 指定傳送通知之前主機應處於非作用中狀態的時間長度。

值的範圍可以從 10 分鐘到主機存留時間 (TTL) 期間的上限 (預設值為三個月)。

例如

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

- 5 您可以使用**非作用中主機通知接受清單**設定來控制要監控以進行通知的主機。未選取此設定時，系統會對所有非作用中主機傳送通知。
  - 若要針對所有非作用中主機傳送通知，請清除該核取方塊。
  - 若要讓通知僅針對部分非作用中主機傳送，選取**非作用中主機通知接受清單**，然後以逗號分隔的清單指定主機名稱。
- 6 按一下**儲存**。

### 結果

當主機處於非作用中時間超過指定的限制時，系統通知會傳送至**組態 > SMTP 伺服器**頁面上指定的位址。

# 整合 vRealize Log Insight 與 VMware 產品



vRealize Log Insight 可與其他 VMware 產品整合，以使用事件和記錄資料，並能讓您更好地瞭解虛擬環境中發生的事件。

## 與 VMware vSphere 整合

vRealize Log Insight 管理員使用者可以設定 vRealize Log Insight 以 2 分鐘的時間間隔連線到 vCenter Server 系統，並從這些 vCenter Server 系統收集事件、警示和工作資料。此外，vRealize Log Insight 可以透過 vCenter Server 設定 ESXi 主機。請參閱[將 vRealize Log Insight 連線到 vSphere 環境](#)。

## 與 VMware vRealize Operations Manager 整合

您可以將 vRealize Log Insight 與 vRealize Operations Manager vApp 和 vRealize Operations Manager Installable 整合。與 Installable 版本整合需要對 vRealize Operations Manager 組態進行其他變更。如需將 vRealize Operations Manager Installable 設定為與 vRealize Log Insight 整合的相關資訊，請參閱《Log Insight 入門指南》。

vRealize Log Insight 和 vRealize Operations Manager 可以透過兩種獨立方法整合。

### 通知事件

vRealize Log Insight 管理員使用者可以設定 vRealize Log Insight 以您建立的查詢為基礎將通知事件傳送到 vRealize Operations Manager。請參閱[設定 vRealize Log Insight，以將通知和度量傳送至 vRealize Operations Manager](#)。

### 在環境定義中啟動

在環境定義中啟動是 vRealize Operations Manager 的功能，可讓您在特定環境中透過 URL 啟動外部應用程式。環境由作用中 UI 元素及物件選擇定義。在環境定義中啟動可讓 vRealize Log Insight 介面卡將功能表項目新增到自訂使用者介面及 vRealize Operations Manager vSphere 使用者介面內的多個不同檢視中。請參閱在[vRealize Operations Manager 中為 vRealize Log Insight 啟用在環境定義中啟動](#)。

**備註** 通知事件不取決於在環境定義中啟動的組態。即使您不啟用在環境定義中啟動功能，您也可以將通知事件從 vRealize Log Insight 傳送到 vRealize Operations Manager。

如果環境發生變更，vRealize Log Insight 管理員使用者可以從 vRealize Log Insight 變更、新增或移除 vSphere 系統，變更或移除接收警示通知的 vRealize Operations Manager 執行個體，並變更用於連線 vSphere 系統及 vRealize Operations Manager 的密碼。

本章節討論下列主題：

- 將 vRealize Log Insight 連線到 vSphere 環境
- 將 vRealize Log Insight 設定為從 vCenter Server 執行個體提取事件、工作和警示
- 搭配使用 vRealize Operations Manager 與 vRealize Log Insight
- 適用於 vRealize Log Insight 的 vRealize Operations Manager 內容套件

## 將 vRealize Log Insight 連線到 vSphere 環境

設定 vRealize Log Insight 從 vSphere 環境收集警示、事件及工作資料之前，您必須將 vRealize Log Insight 連線到一或多個 vCenter Server 系統。

vRealize Log Insight 可從 vCenter Server 執行個體及其管理的 ESXi 主機中收集兩種類型的資料。

- 事件、工作和警示為具有特定涵義的結構化資料。設定完成後，vRealize Log Insight 會從已登錄的 vCenter Server 執行個體提取事件、工作和警示。
- 記錄包含可在 vRealize Log Insight 中分析的非結構化資料。ESXi 主機或 vCenter Server Appliance 執行個體可透過 syslog 將記錄推送到 vRealize Log Insight。

### 必要條件

- 對於要達到的整合層級，請確認您的使用者認證具有足夠的權限來執行 vCenter Server 系統及其 ESXi 主機的必要組態。

整合層級	所需權限
事件、工作和警示收集	<ul style="list-style-type: none"> <li>■ 系統.檢視</li> </ul>
<p><b>備註</b> 系統.檢視是系統定義的權限。當您新增自訂角色，且未將任何權限指派給該角色時，角色會建立為唯讀角色，並具有三種系統定義的權限：系統.匿名、系統.檢視，以及系統.讀取。</p>	
ESXi 主機的 Syslog 組態	<ul style="list-style-type: none"> <li>■ 主機.組態.變更設定</li> <li>■ 主機.組態.網路組態</li> <li>■ 主機.組態.進階設定</li> <li>■ 主機.組態.安全性設定檔和防火牆</li> </ul>

**備註** 您必須設定 vCenter Server 詳細目錄內的頂層資料夾的權限，並確認已選取**散佈到子系核取方塊**。

- 確認您知道 vCenter Server 系統的 IP 位址或網域名稱。
- 確認您已做為具有**編輯管理員**權限的使用者身分登入 vRealize Log Insight Web 使用者介面。URL 格式為 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虛擬應用裝置的 IP 位址或主機名稱。



## 程序

- 1 導覽至**管理**索引標籤。
- 2 在 [整合] 下，按一下 **vSphere**。
- 3 輸入 vCenter Server 的 IP 位址和服務帳戶認證，然後按一下**測試連線**。
- 4 如果 vSphere 環境提供了不受信任的 SSL 憑證，則會有對話方塊顯示憑證的詳細資料。按一下**接受**，將憑證新增至 vRealize Log Insight 叢集中所有節點的信任存放區。  
  
如果您按一下**取消**，則憑證不會新增至信任存放區，且與 vSphere 環境的連線將會失敗。您必須接受憑證才能成功連線。
- 5 (選擇性) 若要登錄其他 vCenter Server，請按一下**新增 vCenter Server**，然後重複步驟 3 至 5。

---

**備註** 請勿使用重複名稱或 IP 位址登錄 vCenter Server 系統。vRealize Log Insight 不會檢查是否有重複 vCenter Server 名稱。您必須確認已登錄的 vCenter Server 系統清單不包含重複項目。

---

- 6 按一下**儲存**。

如果您並未測試連線，且 vSphere 環境提供的憑證不受信任，請依照步驟 4 中的指示操作。

## 後續步驟

- 從已登錄的 vCenter Server 執行個體收集事件、工作和警示資料。請參閱[將 vRealize Log Insight 設定為從 vCenter Server 執行個體提取事件、工作和警示](#)。
- 從 vCenter Server 管理的 ESXi 主機收集 Syslog 摘要。請參閱[設定 ESXi 主機將記錄事件轉送到 vRealize Log Insight](#)。

## vRealize Log Insight 做為 Syslog 伺服器

vRealize Log Insight 包含執行 vRealize Log Insight 服務時一直處於作用中的內建 Syslog 伺服器。

Syslog 伺服器接聽連接埠 514/TCP、1514/TCP 和 514/UDP，並且已經準備好擷取從其他主機傳送的記錄訊息。對於 Syslog 伺服器所擷取的訊息，可在 vRealize Log Insight Web 使用者介面中進行近乎即時的搜尋。vRealize Log Insight 接受的最大 Syslog 訊息長度為 10 KB。

支援 Syslog 格式 RFC-6587、RFC-5424 和 RFC-3164。

## 設定 ESXi 主機將記錄事件轉送到 vRealize Log Insight

ESXi 主機或 vCenter Server Appliance 執行個體產生可在 vRealize Log Insight 中分析的非結構化記錄資料。

您可以使用 vRealize Log Insight 管理介面在已登錄的 vCenter Server 上設定 ESXi 主機，以將 syslog 資料推送到 vRealize Log Insight。

---

**注意** 執行平行組態工作可能會導致目標 ESXi 主機上的 syslog 設定不正確。確認沒有其他的管理使用者正在設定您要設定的 ESXi 主機。

---



vRealize Log Insight 叢集可使用整合式負載平衡器在叢集的個別節點之間散佈 ESXi 和 vCenter Server Appliance Syslog 摘要。

如需在將訊息傳送至 vRealize Log Insight 前在 ESXi 主機上篩選 syslog 訊息的相關資訊，請參閱《vSphere 安裝和設定》指南的「[設定 ESXi](#)」一節中的「[在 ESXi 主機上設定記錄篩選](#)」主題。

如需從 vCenter Server Appliance 設定 syslog 摘要的相關資訊，請參閱[設定 vCenter Server 以將記錄事件轉送到 vRealize Log Insight](#)。

---

**備註** vRealize Log Insight 可接收來自 ESXi 主機 5.5 版及更新版本的 syslog 資料。

---

#### 必要條件

- 確認管理 ESXi 主機的 vCenter Server 已向 vRealize Log Insight 執行個體登錄。或者，您可以登錄 ESXi 主機，並在單一作業中設定 vCenter Server。
- 確認您的使用者認證具有足夠的權限在 ESXi 主機上設定 syslog。
  - **主機.組態.進階設定**
  - **主機.組態.安全性設定檔和防火牆**

---

**備註** 您必須設定 vCenter Server 詳細目錄內的頂層資料夾的權限，並確認已選取**散佈到子系核取方塊**。

---

#### 程序

- 1 導覽至**管理**索引標籤。
- 2 在 [整合] 下，按一下 **vSphere**。
- 3 在 vCenter Server 資料表中，針對要從中接收 syslog 摘要的 ESXi 主機，找到管理該主機的 vCenter Server 執行個體，然後按一下**編輯**。
- 4 在開啟的編輯視圖中，選取將 **ESXi 主機設定為傳送記錄至 Log Insight** 核取方塊。

依預設，vRealize Log Insight 會設定所有可連線的 5.5 版及更新版本的 ESXi 主機，以透過 UDP 傳送記錄。

- 5 (選擇性) 若要修改預設組態值，請按一下**進階選項**。
  - 若要變更所有 ESXi 主機的通訊協定，請選取**設定所有 ESXi 主機**，選取通訊協定，然後按一下**確定**。
  - 若僅要設定特定的 ESX 主機記錄或變更所選 ESXi 主機的通訊協定，請使用下列步驟：
    - a 選取**設定特定 ESXi 主機**。
    - b 從**依主機篩選**清單中，選取一或多個主機。
    - c 設定通訊協定值。
    - d 按一下**確定**。
- 6 (選擇性) 如果您使用的是叢集，請開啟**目標文字方塊**的下拉式功能表，然後選取散佈 Syslog 摘要之負載平衡器的主機名稱或 IP 位址。

## 7 按一下儲存。

### 後續步驟

ESXi 主機組態會顯示在 ESXi 主機所設定的 vCenter Server 資料表資料行中。如果主機已完成設定，您可以在主機所設定的資料行中按一下**檢視詳細資料**，以檢視所設定 ESXi 主機的詳細資訊。

## 修改 ESXi 主機組態以便將記錄事件轉送至 vRealize Log Insight

ESXi 主機或 vCenter Server Appliance 執行個體產生可在 vRealize Log Insight 中分析的非結構化記錄資料。

您可以使用 vRealize Log Insight 管理介面在已登錄的 vCenter Server 上設定 ESXi 主機，以將 syslog 資料推送到 vRealize Log Insight。

**注意** 執行平行組態工作可能會導致目標 ESXi 主機上的 syslog 設定不正確。確認沒有其他的管理使用者正在設定您要設定的 ESXi 主機。

設定初始組態後，您可以啟用適當選項，以定期尋找並自動設定尚未設定的現有和新增的 vSphere ESXi 主機。系統會使用目前設定的通訊協定自動設定 ESXi 主機。

vRealize Log Insight 叢集可使用整合式負載平衡器在叢集的個別節點之間散佈 ESXi 和 vCenter Server Appliance Syslog 摘要。

如需在將設定的訊息傳送至 vRealize Log Insight 前在 ESXi 主機上篩選 Syslog 訊息的相關資訊，請參閱《vSphere 安裝和設定》指南的〈[設定 ESXi](#)〉一節中的「在 ESXi 主機上設定記錄篩選」主題。

如需從 vCenter Server Appliance 設定 syslog 摘要的相關資訊，請參閱[設定 vCenter Server 以將記錄事件轉送到 vRealize Log Insight](#)。

vRealize Log Insight 可接收來自 ESXi 主機 5.5 版及更新版本的 syslog 資料。

### 必要條件

- 確認管理 ESXi 主機的 vCenter Server 已向 vRealize Log Insight 執行個體登錄。
- 確認您的使用者認證具有足夠的權限在 ESXi 主機上設定 syslog。
  - **主機.組態.進階設定**
  - **主機.組態.安全性設定檔和防火牆**

**備註** 您必須設定 vCenter Server 詳細目錄內的頂層資料夾的權限，並確認已選取**散佈到子系核取方塊**。

### 程序

- 1 導覽至**管理索引標籤**。
- 2 在 [整合] 下，按一下 **vSphere**。
- 3 選取將 **ESXi 主機設定為傳送記錄至 Log Insight** 核取方塊。
- 4 按一下**進階選項**。

- 5 若要變更所選 ESXi 主機的通訊協定，請使用下列步驟：
  - a 從**依主機篩選**清單中，選取一或多個主機。
  - b 確認目前的通訊協定是否符合您所需，否則請選取其他通訊協定。
  - c 若要以目前設定的通訊協定啟用 ESXi 主機的自動組態，請選取**自動設定所有 ESXi 主機**。啟用時，vRealize Log Insight 會定期尋找並設定尚未設定的現有和新增的 vSphere ESXi 主機。
  - d 按一下**設定**以開始設定選取的主機。ESXi 對話方塊隨即關閉。
  - e 在訊息對話方塊中按一下**確定**。
  - f 如果您變更通訊協定設定，請在關閉 **ESXi 組態**對話方塊後，按一下主視窗中的**儲存**。
- 6 (選擇性) 如果您使用的是叢集，則可以透過開啟 **vSphere 整合**頁面上**目標文字方塊**的下拉式功能表，並選取負載平衡器的主機名稱或 IP 位址來指定負載平衡器。

## vRealize Operations Manager 中的 vRealize Log Insight 通知事件

您可以設定 vRealize Log Insight 以您建立的警示查詢為基礎將通知事件傳送到 vRealize Operations Manager。

在 vRealize Log Insight 中設定通知警示時，可在 vRealize Operations Manager 中選取與此通知事件相關聯的資源。請參閱在 [Log Insight 中新增警示查詢以將通知事件傳送到 vRealize Operations Manager](#)。

以下列出會顯示通知事件之 vRealize Operations Manager UI 的區段。

- 首頁 > **建議儀表板** > **子代的首要健全狀況警示** Widget
- 首頁 > **警示索引**標籤
- 在所有包含具有通知事件之 Widget 的自訂儀表板上

如需有關通知事件出現位置的其他資訊，請參閱 [VMware vRealize Operations Manager 說明文件中心](#)。

## 設定 vCenter Server 以將記錄事件轉送到 vRealize Log Insight

vSphere 整合從 vCenter Server 收集工作和事件，但不會從每個 vCenter Server 元件收集低層級的內部記錄。vSphere 內容套件會利用這些記錄。

vCenter Server 6.5 和更新版本應透過 vCenter Server Appliance Management 介面進行設定。如需更多關於如何從 vCenter Server 轉送記錄檔事件的資訊，請參閱關於重新導向 vCenter Server Appliance 記錄檔至另一部機器的 vSphere 說明文件。

針對較早版本的 vSphere，雖然 vCenter Server Appliance 包含可用來路由記錄檔的 Syslog 精靈，但偏好的方法仍是安裝 vRealize Log Insight 代理程式。

如需安裝 vRealize Log Insight 代理程式的相關資訊，請參閱使用 vRealize Log Insight 代理程式。

vSphere 內容套件包含定義從 vCenter Server 安裝收集特定記錄檔的代理程式群組。可在 <https://LogInsightServerFqdnOrIP/contentpack?contentPackId=com.vmware.vsphere> 查看此組態。

如需使用代理程式群組的相關資訊，請參閱[集中式代理程式組態和代理程式群組](#)。

如需 vCenter Server 記錄檔位置的相關資訊，請參閱 <http://kb.vmware.com/kb/1021804> 和 <http://kb.vmware.com/kb/1021806>。

## 將 vRealize Log Insight 設定為從 vCenter Server 執行個體提取事件、工作和警示

事件、工作和警示為具有特定涵義的結構化資料。您可以將 vRealize Log Insight 設定為從一或多個 vCenter Server 系統收集警示、事件及工作資料。

您可以使用管理 UI 將 vRealize Log Insight 設定為連線到 vCenter Server 系統。資訊係使用 vSphere Web Services API 從 vCenter Server 擷取，並在 vRealize Log Insight Web 使用者介面中顯示為 vSphere 內容套件

請注意，vSphere 6.5 有新的原生高可用性解決方案。如需有關 HA 和使用負載平衡器的詳細資訊，請參閱可在 [www.vmware.com](http://www.vmware.com) 上取得的白皮書《VMware vSphere 6.5 中的新功能》。

---

**備註** vRealize Log Insight 只能從 vCenter Server 5.5 及更新版本提取警示、事件及工作資料。

---

### 必要條件

確認您擁有具有**系統檢視**權限的使用者認證。

---

**備註** 您必須設定 vCenter Server 詳細目錄內的頂層資料夾的權限，並確認已選取**散佈到子系核取方塊**。

---

### 程序

- 1 導覽至**管理索引**標籤。
- 2 在 [整合] 下，按一下 **vSphere**。
- 3 在 vCenter Server 資料表中，找到要從中收集資料的 vCenter Server 執行個體。
- 4 在開啟的編輯視圖中，選取**收集 vCenter Server 事件、工作和警示**核取方塊。
- 5 按一下**儲存**。

### 結果

vRealize Log Insight 將每隔 2 分鐘連線到 vCenter Server，並擷取自上次成功輪詢後的所有新資訊。

### 後續步驟

- 使用 vSphere 內容套件或自訂查詢分析 vSphere 事件。
- 啟用 vSphere 內容套件警示或自訂警示。

## 搭配使用 vRealize Operations Manager 與 vRealize Log Insight

## 與 vRealize Operations Manager 整合的需求

在將 vRealize Log Insight 與 vRealize Operations Manager 整合的程序中，您必須指定 vRealize Log Insight 的認證以針對 vRealize Operations Manager 進行驗證。

vRealize Operations Manager 支援本機使用者帳戶和多個 LDAP 來源。vRealize Operations Manager 和 VMware Identity Manager 整合皆由 vRealize Log Insight 管理員設定。

如果您的部署在 vRealize Log Insight 中使用 VMware Identity Manager 整合，則 VMware Identity Manager 後援 URL (重新導向 URL 主機) 和 vRealize Operations Manager 整合頁面上的目標欄位應該具有完全相同的值。

### 必要條件

確認整合使用者帳戶具有操縱 vRealize Operations Manager 中物件的權限。請參閱[本機或 Active Directory 使用者帳戶所需的最低權限](#)。

### 程序

- ◆ 決定本機使用者帳戶的使用者名稱：
  - a 從 vRealize Operations Manager Web 介面中，選取**存取控制**。
  - b 識別或建立整合使用者。[來源類型] 欄位為**本機使用者**。
  - c 記下**使用者名稱**欄位的值。在 vRealize Log Insight 管理使用者介面中設定整合時，請指定此使用者名稱。
- ◆ 若要決定必須在 vRealize Log Insight 中提供之 LDAP 使用者帳戶的使用者名稱格式，請遵循下列指示：
  - a 從 vRealize Operations Manager Web 介面中，選取**存取控制**。
  - b 識別或建立整合使用者。記下**使用者名稱**和**來源類型**欄位。例如，來自來源 **Active Directory - AD** 的名為 **integration@example.com** 的使用者。
  - c 選取**驗證來源**。
  - d 識別與步驟 b 中的**來源類型**相對應的驗證來源，並記下**來源顯示名稱**欄位。例如，「ad」。
  - e 在 vRealize Log Insight 管理使用者介面內輸入的使用者名稱是步驟 3 和步驟 5 組合而來，格式為 **UserName@SourceDisplayName**。例如，integration@example.com@ad。

### 本機或 Active Directory 使用者帳戶所需的最低權限

若要將 vRealize Log Insight 與 vRealize Operations Manager 整合，您必須指定適用於 vRealize Log Insight 的認證，以對 vRealize Operations Manager 進行驗證。若要操縱 vRealize Operations Manager 中的物件，使用者帳戶必須具有所需權限。

如果您指派「在環境定義中啟動」的權限給使用者，該使用者也可以設定警示整合。使用警示整合表格中的資訊可以僅指派警示整合的權限。

表 8-1. 警示整合

動作	要選取的權限和物件
使用下方列出的權限建立自訂角色。	<ol style="list-style-type: none"> <li>1 管理 -&gt; Rest API <ol style="list-style-type: none"> <li>a 所有其他讀取、寫入 API</li> <li>b 讀取對 API 的存取</li> </ol> </li> </ol>
將上述角色指派給本機或 Active Directory 使用者 (新的或現有的) 並選取要指派的物件/物件階層。	<ol style="list-style-type: none"> <li>1 介面卡執行個體 -&gt; vRealizeOpsMgrAPI [全部勾選]</li> <li>2 vSphere 主機和叢集 [全部勾選]</li> <li>3 vSphere 網路 [全部勾選]</li> <li>4 vSphere 儲存區 [全部勾選]</li> </ol>

表 8-2. 在環境定義中啟動整合

動作	要選取的權限和物件
使用下方列出的權限建立自訂角色。	<ol style="list-style-type: none"> <li>1 管理 -&gt; Rest API <ol style="list-style-type: none"> <li>a 所有其他讀取、寫入 API</li> <li>b 讀取對 API 的存取</li> <li>c 刪除資源</li> </ol> </li> <li>2 管理 -&gt; 組態 -&gt; 管理資源關聯性</li> <li>3 管理 -&gt; 資源種類管理 <ol style="list-style-type: none"> <li>a 建立</li> <li>b 編輯</li> </ol> </li> <li>4 管理 -&gt; 資源管理 <ol style="list-style-type: none"> <li>a 建立</li> <li>b 刪除</li> <li>c 讀取</li> </ol> </li> <li>5 管理 -&gt; 存取 -&gt; 存取控制 -&gt; 新增、編輯或刪除角色。</li> </ol> <p><b>備註</b> vRealize Operations Manager 7.0 版和更早版本需要此權限。</p>
將上述角色指派給本機或 Active Directory 使用者 (新的或現有的) 並選取要指派的物件/物件階層。	選取允許存取系統中的所有物件。

## 設定 vRealize Log Insight，以將通知和度量傳送至 vRealize Operations Manager

您可以將 vRealize Log Insight 設定為傳送警示通知和度量至 vRealize Operations Manager。

您可以將 vRealize Log Insight 與 vRealize Operations Manager vApp 和 vRealize Operations Manager Installable 整合。與 Installable 版本整合需要對 vRealize Operations Manager 組態進行其他變更。如需將 vRealize Operations Manager Installable 設定為與 vRealize Log Insight 整合的相關資訊，請參閱《Log Insight 入門指南》。

將 vRealize Log Insight 警示和 vRealize Operations Manager 整合可讓您在單一使用者介面中檢視您環境的所有相關資訊。

您可以將通知事件從多個 vRealize Log Insight 執行個體傳送至單一 vRealize Operations Manager 執行個體。您可以為每個 vRealize Operations Manager 執行個體的單一 vRealize Log Insight 執行個體啟用環境定義中啟動。

vRealize Log Insight 可使用 vRealize Operations Manager REST API 在 vRealize Operations Manager 中建立資源和關係，以設定在環境定義中啟動介面卡。

#### 必要條件

- 使用所需的權限在 vRealize Operations Manager 中建立整合使用者帳戶。如需詳細資訊，請參閱 [與 vRealize Operations Manager 整合的需求](#)。
- 確認您知道目標 vRealize Operations Manager 執行個體的 IP 位址或主機名稱。
- 確認您已做為具有**編輯管理員**權限的使用者身分登入 vRealize Log Insight Web 使用者介面。URL 格式為 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虛擬應用裝置的 IP 位址或主機名稱。

---

**備註** 在執行具有已設定負載平衡器之 vRealize Operations Manager 叢集的環境中，您可以使用負載平衡器 IP 位址 (如果可用)。

---

#### 程序

- 1 導覽至**管理索引**標籤。
- 2 在 **[整合]** 下，選取 **vRealize Operations Manager**。
- 3 輸入主要節點或負載平衡器的 IP 位址或主機名稱 (如果已設定)。使用 vRealize Operations Manager 使用者認證，然後按一下**測試連線**。vRealize Log Insight 會使用認證，將通知事件推送至 vRealize Operations Manager。確保設定的使用者具有執行整合所需的最低權限。請參閱**本機或 Active Directory 使用者帳戶所需的最低權限**。
- 4 如果 vRealize Operations Manager 提供了不受信任的 SSL 憑證，則會有對話方塊顯示憑證的詳細資料。按一下**接受**，將憑證新增至 vRealize Log Insight 叢集中所有節點的信任存放區。

如果您按一下**取消**，則憑證不會新增至信任存放區，且與 vRealize Operations Manager 的連線將會失敗。您必須接受憑證才能成功連線。

- 5 在 vRealize Operations Manager 窗格中，根據您的喜好設定選取相關的核取方塊：
  - 若要將警示傳送至 vRealize Operations Manager，請選取**啟用警示整合**。
  - 若要讓 vRealize Operations Manager 開啟 vRealize Log Insight 並查詢物件記錄，選取**啟用在環境定義中啟動**。如需詳細資訊，請參閱在 [vRealize Operations Manager 中為 vRealize Log Insight 啟用在環境定義中啟動](#)。
  - 若要計算並傳送度量至 vRealize Operations Manager，選取**啟用度量計算**。

- 6 按一下**儲存**。

如果您並未測試連線，且 vRealize Operations Manager 提供的憑證不受信任，請依照步驟 4 中的指示操作。



## 後續步驟

- 請參閱 vRealize Operations Manager UI 中的相關頁面，以檢視 vRealize Log Insight 所傳送的通知事件。

## 在 vRealize Operations Manager 中為 vRealize Log Insight 啟用在環境定義中啟動

您可以將 vRealize Operations Manager 設定為顯示與 vRealize Log Insight 相關的功能表項目，並透過物件特定查詢啟動 vRealize Log Insight。

您可以將 vRealize Log Insight 與 vRealize Operations Manager vApp 和 vRealize Operations Manager Installable 整合。

要與 vApp 安裝和 Installable (Windows、Linux) 整合，必須對 vRealize Operations Manager 組態進行額外的變更。請至 [vRealize Log Insight 說明文件](#)，參閱關於在 vRealize Operations Manager 6.x 及更新版本中安裝 vRealize Log Insight Management Pack (Adapter) 的主題。

---

**備註** vRealize Log Insight Management Pack 已預先安裝於 vRealize Operations Manager 6.0 及更新版本中，且不需進行組態變更。

---

vRealize Operations Manager Installable (Windows 版本) 在 vRealize Operations Manager 6.5 和更新版本中不再受到支援。

---

**重要** 一個 vRealize Operations Manager 執行個體僅支援一個 vRealize Log Insight 執行個體的在環境定義中啟動功能。由於 vRealize Log Insight 不會檢查其他執行個體是否已向 vRealize Operations Manager 登錄，因此您可能會覆寫其他使用者的設定。

---

### 必要條件

- 確認您已做為具有**編輯管理員**權限的使用者身分登入 vRealize Log Insight Web 使用者介面。URL 格式為 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虛擬應用裝置的 IP 位址或主機名稱。
- 確認您知道目標 vRealize Operations Manager 執行個體的 IP 位址或主機名稱。
- 確認您擁有必要的使用者認證。請參閱[本機或 Active Directory 使用者帳戶所需的最低權限](#)。
- 如果您使用的是 vRealize Operations Manager 6.5 或更新版本，請參閱《vRealize Operations Manager 組態指南》並使用〈使用 vRealize Operations Manager 設定 vRealize Log Insight〉中的啟用在環境定義中啟動程序。

### 程序

- 1 導覽至管理索引標籤。
- 2 在 [整合] 下，選取 **vRealize Operations Manager**。



- 輸入 vRealize Operations Manager 主要節點或負載平衡器的 IP 位址或 FQDN (如果已設定)，然後按一下**測試連線**。

**備註** 如需「在環境定義中啟動」功能，您必須提供具有管理員權限的 vRealize Operations Manager 使用者。

- 按一下**儲存**。

#### 結果

vRealize Log Insight 將設定 vRealize Operations Manager 執行個體。此作業可能需要幾分鐘的時間。與 vRealize Log Insight 相關的項目會顯示在 vRealize Operations Manager 的功能表中。

#### 後續步驟

從 vRealize Operations Manager 執行個體啟動 vRealize Log Insight 查詢。請參閱 [vRealize Log Insight 在環境定義中啟動](#)

### vRealize Log Insight 在環境定義中啟動

針對 vRealize Log Insight 啟用在環境定義中啟動時，會在 vRealize Operations Manager 中建立 vRealize Log Insight 資源。

資源識別碼包含 vRealize Log Insight 執行個體的 IP 位址，vRealize Operations Manager 會使用該識別碼來開啟 vRealize Log Insight。

#### vRealize Operations Manager 6.5 和更新版本中的「在環境定義中啟動」

如需啟用在環境定義中啟動的相關資訊，請參閱 [vRealize Operations Manager 資訊中心](#)。

#### vRealize Operations Manager 6.4 和較舊版本的 vSphere 使用者介面中的「在環境定義中啟動」

與 vRealize Log Insight 相關的在環境定義中啟動選項顯示在 vSphere 使用者介面的**動作**下拉式功能表中。您可以使用這些功能表項目來開啟 vRealize Log Insight，並從 vRealize Operations Manager 中的物件搜尋記錄事件。

可用的在環境定義中啟動之動作取決於您在 vRealize Operations Manager 詳細目錄中選取的物件。在按一下在環境定義中啟動選項之前，查詢的時間範圍限制為 60 分鐘。

表 8-3. vRealize Operations Manager UI 中的物件及其對應的在環境定義中啟動選項和動作

vRealize Operations Manager 中選取的物件	動作下拉式功能表中的在環境定義中啟動選項	vRealize Operations Manager 中的動作	vRealize Log Insight 中的動作
環境	開啟 vRealize Log Insight	開啟 vRealize Log Insight。	vRealize Log Insight 顯示 <b>互動式分析</b> 索引標籤。
vCenter Server	開啟 vRealize Log Insight	開啟 vRealize Log Insight。	vRealize Log Insight 顯示 <b>互動式分析</b> 索引標籤。

表 8-3. vRealize Operations Manager UI 中的物件及其對應的在環境定義中啟動選項和動作 (續)


vRealize Operations Manager 中選取的物件	動作下拉式功能表中的在環境定義中啟動選項	vRealize Operations Manager 中的動作	vRealize Log Insight 中的動作
資料中心	搜尋 vRealize Log Insight 中的記錄	開啟 vRealize Log Insight 並傳遞所選資料中心物件下所有主機系統的資源名稱。	vRealize Log Insight 顯示 <b>互動式分析</b> 索引標籤，並執行查詢以尋找包含資料中心內主機之名稱的記錄事件。
叢集	搜尋 vRealize Log Insight 中的記錄	開啟 vRealize Log Insight 並傳遞所選叢集物件下所有主機系統的資源名稱。	vRealize Log Insight 顯示 <b>互動式分析</b> 索引標籤，並執行查詢以尋找包含叢集內主機之名稱的記錄事件。
主機系統	搜尋 vRealize Log Insight 中的記錄	開啟 vRealize Log Insight 並傳遞所選主機物件的資源名稱。	vRealize Log Insight 顯示 <b>互動式分析</b> 索引標籤，並執行查詢以尋找包含所選主機系統之名稱的記錄事件。
虛擬機器	搜尋 vRealize Log Insight 中的記錄	開啟 vRealize Log Insight 並傳遞所選虛擬機器的 IP 位址以及相關主機系統的資源名稱。	vRealize Log Insight 顯示 <b>互動式分析</b> 索引標籤，並執行查詢以尋找包含虛擬機器 IP 位址及虛擬機器所在主機之名稱的記錄事件。

在**警示索引標籤**上，如果選取警示並從內部快顯功能表中選取**搜尋 Log Insight 中的記錄**，則查詢的時間範圍限制為警示觸發之前的一小時。例如，如果警示在 2:00 PM 觸發，則 vRealize Log Insight 中的查詢將顯示 1:00 PM 與 2:00 PM 之間發生的所有記錄訊息。這樣可以協助您識別可能已觸發警示的事件。

您可以從 vRealize Operations Manager 中的度量圖開啟 vRealize Log Insight。vRealize Log Insight 執行的查詢的時間範圍與度量圖的時間範圍相符。

**備註** 如果虛擬應用裝置的時間設定不同，則您在 vRealize Log Insight 中看到的時間與 vRealize Operations Manager 度量圖的時間可能不同。

#### vRealize Operations Manager 6.4 和較舊版本使用者介面中的「在環境定義中啟動」

在環境定義中啟動圖示  顯示於使用者介面的多個頁面上，但您僅可從顯示 vRealize Log Insight 通知事件的頁面啟動 vRealize Log Insight。

- [警示概觀] 頁面。
- vRealize Log Insight 通知警示的 [警示摘要] 頁面。
- 選取 vRealize Log Insight 通知警示時，儀表板上的警示 Widget。

選取自訂使用者介面中的 vRealize Log Insight 通知事件時，您可於兩個在環境定義中啟動動作之間進行選擇。

表 8-4. vRealize Operations Manager UI 中的在環境定義中啟動選項和動作

vRealize Operations Manager 中的在環境定義中啟動選項	vRealize Operations Manager 中的動作	vRealize Log Insight 中的動作
開啟 vRealize Log Insight	開啟 vRealize Log Insight。	vRealize Log Insight 顯示 <b>儀表板</b> 索引標籤，然後載入 vSphere 概觀儀表板。
搜尋 vRealize Log Insight 中的記錄	開啟 vRealize Log Insight 並傳遞已觸發通知事件之查詢的識別碼。	vRealize Log Insight 顯示 <b>互動式分析</b> 索引標籤，並執行已觸發通知事件的查詢。

選取不是源自 vRealize Log Insight 的警示時，[在環境定義中啟動] 功能表包含**搜尋 vRealize Log Insight 中的虛擬機器和主機記錄**功能表項目。如果選取此功能表項目，vRealize Operations Manager 將開啟 vRealize Log Insight 並傳遞已觸發警示之物件的識別碼。vRealize Log Insight 會使用資源識別碼在可用的記錄事件中執行搜尋。

## 雙向在環境定義中啟動

「在環境定義中啟動」也可以從 vRealize Log Insight 執行到 vRealize Operations Manager。

如果將 vRealize Log Insight 與 vRealize Operations Manager 整合，則可透過選取 vRealize Log Insight 事件左側的齒輪圖示並選取要在 vRealize Operations Manager 中檢視的選項，從該事件執行在環境定義中啟動。

如需從 vRealize Operations Manager 到 vRealize Log Insight 的在環境定義中啟動的相關資訊，請參閱 [vRealize Log Insight 在環境定義中啟動](#)。

### 程序

- 1 在 vRealize Log Insight 中，導覽至**互動式分析**索引標籤。
- 2 找到包含詳細目錄對應欄位的事件，並將游標暫留在事件上。
- 3 按一下齒輪圖示，然後從 vRealize Operations Manager 的下拉式功能表中選取**開啟分析**。

新的瀏覽器索引標籤隨即開啟，並將您導向到與 vRealize Log Insight 整合的 vRealize Operations Manager 執行個體。您在驗證後，會立即導向到 vRealize Operations Manager 的**環境 > 分析**區段，並會選取物件。

**備註** 當多個 vRealize Log Insight 執行個體連線至同一 vRealize Operations Manager 執行個體時，僅最後一個與 vRealize Operations Manager 整合的 vRealize Log Insight 執行個體具有在環境定義中啟動功能。這還表示只要 vRealize Log Insight 執行個體與先前同其他 vRealize Log Insight 執行個體進行整合的 vRealize Operations Manager 執行個體整合，就會覆寫在環境定義中啟動功能。

## 在 vRealize Operations Manager 中為 vRealize Log Insight 停用在環境定義中啟動

您可以從 vRealize Operations Manager 執行個體解除安裝 vRealize Log Insight 介面卡，以從 vRealize Operations Manager 使用者介面移除與 vRealize Log Insight 相關的功能表項目。

您可以使用 vRealize Log Insight 的管理 UI 停用在環境定義中啟動功能。如果您不具有 vRealize Log Insight 的存取權或者如果 vRealize Log Insight 執行個體在與 vRealize Operations Manager 的連線停用之前就已刪除，則可以從 vRealize Operations Manager 的管理 UI 中解除登錄 vRealize Log Insight。請參閱 vRealize Operations Manager 管理入口網站中的說明。

**注意** 一個 vRealize Operations Manager 執行個體僅支援一個 vRealize Log Insight 執行個體的在環境定義中啟動功能。在您登錄想要停用的執行個體後，如果其他 vRealize Log Insight 執行個體也已登錄，則第二個執行個體會在未通知您的情況下覆寫第一個執行個體的設定。

#### 必要條件

- 確認您已做為具有**編輯管理員**權限的使用者身分登入 vRealize Log Insight Web 使用者介面。URL 格式為 `https://log-insight-host`，其中 `log-insight-host` 是 vRealize Log Insight 虛擬應用裝置的 IP 位址或主機名稱。

#### 程序

- 1 導覽至**管理索引標籤**。
- 2 在 [整合] 下，選取 **vRealize Operations Manager**。
- 3 取消選取**啟用在環境定義中啟動核取方塊**。
- 4 按一下**儲存**。

#### 結果

vRealize Log Insight 會設定 vRealize Operations Manager 執行個體以移除 vRealize Log Insight 介面卡。此作業可能需要幾分鐘的時間。

## 新增 DNS 搜尋路徑和網域

新增 DNS 搜尋路徑和網域可改善 vRealize Operations Manager 詳細目錄比對。

在虛擬機器標籤和搜尋網域解析為傳送記錄訊息至 vRealize Log Insight 的主機之 IP 位址時，新增 DNS 搜尋路徑和網域可改善比對。例如，如果您在 vRealize Operations Manager 中有名為 `linux_01` 的虛擬機器，並且主機名稱 `linux_01.company.com` 解析為 `192.168.10.10`，則新增搜尋網域會允許 vRealize Log Insight 辨識和比對該資源。

#### 程序

- 1 對 vRealize Log Insight 虛擬應用裝置執行客體關閉。
- 2 虛擬機器關閉電源後，選取**編輯設定**。
- 3 選取 **vApp 選項索引標籤**。
- 4 在 **vApp 選項 > 撰寫中**，按一下**內容**。
- 5 尋找 `vami.searchpath.VMware_vCenter_Log_Insight` 和 `vami.domain.VMware_vCenter_Log_Insight` **金鑰**。

如果金鑰不存在，請建立金鑰。

針對搜尋路徑金鑰，請使用下列值：

- 類別為網路內容
- 標籤為 DNS 搜尋路徑
- 金鑰類別識別碼為 vami
- 金鑰執行個體識別碼 為 VMware\_vCenter\_Log\_Insight。
- 類型為靜態內容、字串和使用者可設定。

針對網域金鑰，請使用相同的值，將標籤取代為 DNS 網域，以及將金鑰識別碼取代為網域。

6 設定 DNS 搜尋路徑和網域。例如，ny01.acme.local。

7 開啟虛擬應用裝置的電源。

#### 後續步驟

vRealize Log Insight 開機後，您可以透過登入並檢視 `/etc/resolv.conf` 檔案的內容來驗證 DNS 組態。您應該會在該檔案的結尾附近看到搜尋和網域選項。

## 移除 vRealize Log Insight 介面卡

在 vRealize Operations Manager 6.2 及更新版本執行個體上啟用在環境定義中啟動時，vRealize Log Insight 會在 vRealize Operations Manager 執行個體上建立 vRealize Log Insight 介面卡的執行個體。

當您解除安裝 vRealize Log Insight 時，介面卡的執行個體將保留在 vRealize Operations Manager 執行個體中。因此，在環境定義中啟動功能表項目會繼續顯示在動作功能表中，並指向不再存在的 vRealize Log Insight 執行個體。

若要在 vRealize Operations Manager 中停用在環境定義中啟動功能，您必須從 vRealize Operations Manager 執行個體中移除 vRealize Log Insight 介面卡。

您可以使用命令列公用程式 cURL 將 REST 呼叫傳送到 vRealize Operations Manager。

---

**備註** 僅當在環境定義中啟動啟用時才需要這些步驟。

---

#### 必要條件

- 確認您的系統上安裝了 cURL。請注意，此工具預先安裝在 vRealize Operations Manager 虛擬應用裝置，並可使用 IP 位址 127.0.0.1 在應用裝置上執行步驟。
- 確認您知道目標 vRealize Operations Manager 執行個體的 IP 位址或主機名稱。
- 根據所擁有的 vRealize Operations Manager 授權，確認您具有移除管理套件所需的最低認證。請參閱 [本機或 Active Directory 使用者帳戶所需的最低權限](#)。

## 程序

- 1 在 cURL 中，於 vRealize Operations Manager 虛擬應用裝置上執行下列查詢，找到 vRealize Log Insight 介面卡。

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

其中 *admin* 為管理員登入名稱，*ipaddress* 為 vRealize Operations Manager 執行個體的 IP 位址 (或主機名稱)。系統會提示您輸入以下使用者的密碼：*admin*。

從 cURL 輸出中尋找指派給以下識別碼的 GUID 值：<ops:resource creationTime="{TIMESTAMP}" identifier="{GUID}">。您可以在移除介面卡執行個體的以下命令中使用此 GUID 值。

- 2 執行下列命令移除 vRealize Log Insight 介面卡。

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

其中 *admin* 為管理員登入名稱，*ipaddress* 為 vRealize Operations Manager 執行個體的 IP 位址 (或主機名稱)。系統會提示您輸入以下使用者的密碼：*admin*。

## 結果

vRealize Log Insight 在環境定義中啟動項目將從 vRealize Operations Manager 的功能表中移除。如需在環境定義中啟動的詳細資訊，請參閱 vRealize Log Insight 產品中說明的「vRealize Log Insight 在環境定義中啟動」主題。

## 適用於 vRealize Log Insight 的 vRealize Operations Manager 內容套件

適用於 vRealize Log Insight 的 vRealize Operations Manager 內容套件包含儀表板、擷取的欄位、已儲存的查詢以及警示，用於分析自 vRealize Operations Manager 執行個體重新導向的所有記錄。

vRealize Operations Manager 內容套件提供了一種方式來分析所有自 vRealize Operations Manager 執行個體重新導向之記錄。此內容套件包含儀表板、查詢和警示，可為 vRealize Operations Manager 管理員提供診斷和疑難排解功能。儀表板是根據 vRealize Operations Manager 的主要元件 (如分析、UI 和介面卡) 進行分組，以提供更好的管理能力。您可以啟用各種警示來傳送 vRealize Operations Manager 中的通知事件，並以電子郵件通知管理員。

您可以從 [VMware Marketplace](#) 下載 vRealize Operations Manager 內容套件。

請參閱[使用內容套件](#)。

# vRealize Log Insight 安全性考量

# 9

使用 vRealize Log Insight 功能可保護您的環境以免於攻擊。

本章節討論下列主題：

- [連接埠與外部介面](#)
- [vRealize Log Insight 組態檔](#)
- [vRealize Log Insight 公開金鑰、憑證和金鑰儲存區](#)
- [vRealize Log Insight 授權和 EULA 檔案](#)
- [vRealize Log Insight 記錄檔](#)
- [vRealize Log Insight 使用者帳戶](#)
- [vRealize Log Insight 防火牆建議](#)
- [安全性更新和修補程式](#)

## 連接埠與外部介面

vRealize Log Insight 使用所需的特定服務、連接埠和外部介面。

如需檢視 vRealize Log Insight 的連接埠和通訊協定的相關資訊，請參閱 [VMware Ports and Protocols 工具](#)。

## 通訊連接埠

vRealize Log Insight 會使用 [Ports and Protocols] 工具中列出的通訊連接埠和通訊協定。所需連接埠會根據其是否為來源、使用者介面、叢集之間、外部服務所必需，或防火牆是否可以安全封鎖來進行組織整理。某些連接埠僅在您啟用對應的整合時才會使用。

---

**備註** vRealize Log Insight 並不支援 WAN 叢集 (又稱地理叢集、高可用性叢集或遠端叢集)。應將叢集中的所有節點部署在相同 Layer 2 LAN 中。此外，必須在節點之間開啟通訊連接埠，以進行適當的資訊交換。

---

vRealize Log Insight 網路流量有多個來源。

### 管理員工作站



系統管理員用於遠端管理 vRealize Log Insight 虛擬應用裝置的機器。

### 使用者工作站

vRealize Log Insight 使用者在其上使用瀏覽器存取 vRealize Log Insight Web 介面的機器。

### 傳送記錄的系統

將記錄傳送至 vRealize Log Insight 以進行分析和搜尋的端點。例如，端點包括 ESXi 主機、虛擬機器或具有 IP 位址的任何系統。

### Log Insight Agents

位於 Windows 或 Linux 機器並且會透過 API 將作業系統事件和記錄傳送至 vRealize Log Insight 的代理程式。

### vRealize Log Insight 應用裝置

vRealize Log Insight 服務所在的任何 vRealize Log Insight 虛擬應用裝置、主要節點或工作節點。應用裝置的基礎作業系統為 SUSE 11 SP3。

## 來源傳送資料所需的連接埠

必須對來自傳送資料至 vRealize Log Insight 來源的網路流量，同時對來自叢集外部的連線以及叢集節點之間的負載平衡連線開放這些連接埠。

## 使用者介面所需的連接埠

這些連接埠必須向需要使用 vRealize Log Insight 使用者介面的網路流量開放，包括叢集外部的連線，以及叢集節點之間的負載平衡連線。

## 叢集節點之間所需的連接埠

這些連接埠只能在 vRealize Log Insight 主要節點上針對從工作節點存取網路而開啟，以取得最大的安全性。這些是除了用在叢集節點之間負載平衡的來源和 UI 流量的連接埠以外的連接埠。

## 外部服務所需的連接埠

必須對從 vRealize Log Insight 叢集節點到遠端服務的輸出網路流量開放這些連接埠。

## vRealize Log Insight 組態檔

某些組態檔包含會影響 vRealize Log Insight 安全性的設定。

---

**備註** 根帳戶可存取所有安全性相關的資源。保護此帳戶對 vRealize Log Insight 的安全性來說很重要。

---



表 9-1. Log Insight 組態檔

檔案	說明
/usr/lib/loginsight/application/etc/loginsight-config-base.xml	vRealize Log Insight 的預設系統組態。
/storage/core/loginsight/config/loginsight-config.xml#number	vRealize Log Insight 已修改 (從預設) 的系統組態。
/usr/lib/loginsight/application/etc/jaas.conf	Active Directory 整合的組態。
/usr/lib/loginsight/application/etc/3rd_config/server.xml	Apache Tomcat 伺服器的系統組態。
/storage/var/loginsight/apache-tomcat/conf/tomcat-users.xml	Apache Tomcat 伺服器的系統組態。
/usr/lib/loginsight/application/3rd_party/apache-tomcat-*/conf/server.xml	Apache Tomcat 伺服器的系統組態。
/usr/lib/loginsight/application/3rd_party/apache-tomcat-*/conf/tomcat-users.xml	Apache Tomcat 伺服器的使用者資訊。

## vRealize Log Insight 公開金鑰、憑證和金鑰儲存區

vRealize Log Insight 的公開金鑰、憑證和金鑰儲存區位於 vRealize Log Insight 虛擬應用裝置上。

**備註** 根帳戶可存取所有安全性相關的資源。保護此帳戶對 vRealize Log Insight 的安全性來說很重要。

- /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 授權和 EULA 檔案

使用者授權合約 (EULA) 和授權檔案位於 vRealize Log Insight 虛擬應用裝置上。

**備註** 根帳戶可存取所有安全性相關的資源。保護此帳戶對 vRealize Log Insight 的安全性來說很重要。

檔案	位置
授權	/usr/lib/loginsight/application/etc/license/loginsight_dev.dlf
授權	/usr/lib/loginsight/application/etc/license/loginsight_cpu.dlf
授權	/usr/lib/loginsight/application/etc/license/loginsight_osi.dlf
授權金鑰檔案	/usr/lib/loginsight/application/etc/license/loginsight_license.bak
使用者授權合約	/usr/lib/loginsight/application/etc/license/release/eula.txt

## vRealize Log Insight 記錄檔

包含系統訊息的檔案位於 vRealize Log Insight 虛擬應用裝置上。

下表列出每個檔案及其用途。

如果您需要記錄輪替，或這些檔案的封存記錄檔的相關資訊，請參閱使用 vRealize Log Insight 代理程式中的 [vRealize Log Insight 代理程式所支援的記錄輪替配置](#) 和管理 vRealize Log Insight 中的在 [vRealize Log Insight 中啟用或停用資料封存](#)。

檔案	說明
/storage/var/loginsight/alert.log	用於追蹤已觸發的使用者定義的警示的相關資訊。
/storage/var/loginsight/apache-tomcat/logs/*.log	用於追蹤 Apache Tomcat 伺服器中的事件。
/storage/var/loginsight/cassandra.log	用於追蹤 Apache Cassandra 中的叢集組態儲存和複寫。
/storage/var/loginsight/plugins/vsphere/li-vsphere.log	用於追蹤與 vSphere Web Client 整合相關的事件。
/storage/var/loginsight/loginsight_daemon_stdout.log	用於 vRealize Log Insight 精靈的標準輸出。
/storage/var/loginsight/phonehome.log	用於追蹤傳送至 VMware 的追蹤資料收集 (如果已啟用) 的相關資訊。
/storage/var/loginsight/pi.log	用於追蹤資料庫啟動或停止事件。
/storage/var/loginsight/runtime.log	用於追蹤與 vRealize Log Insight 相關的所有執行階段資訊。
/var/log/firstboot/stratavm.log	用於追蹤首次開機時發生的事件以及 vRealize Log Insight 虛擬應用裝置的組態。
/storage/var/loginsight/systemalert.log	用於追蹤 vRealize Log Insight 傳送的系統通知的相關資訊。每個警示都列示為 JSON 項目。
/storage/var/loginsight/systemalert_worker.log	用於追蹤 vRealize Log Insight 工作節點傳送的系統通知的相關資訊。每個警示都列示為 JSON 項目。
/storage/var/loginsight/ui.log	用於追蹤與 vRealize Log Insight 使用者介面相關的事件。
/storage/var/loginsight/ui_runtime.log	用於追蹤與 vRealize Log Insight 使用者介面相關的執行階段事件。
/storage/var/loginsight/upgrade.log	用於追蹤 vRealize Log Insight 升級期間發生的事件。
/storage/var/loginsight/usage.log	用於追蹤所有查詢。
/storage/var/loginsight/vrops_integration.log	用於追蹤與 vRealize Operations Manager 整合相關的事件。
/storage/var/loginsight/watchdog_log*	用於追蹤監視程式程序的執行階段事件，該程序負責在 vRealize Log Insight 由於某些原因關閉的情況下將其重新啟動。
/storage/var/loginsight/api_audit.log	用來追蹤對 Log Insight 的 API 呼叫。
/storage/var/loginsight/pattern_matcher.log	用來追蹤欄位擷取的模式比對時間和逾時。
/storage/var/loginsight/audit.log	用於追蹤 vRealize Log Insight 的使用方式。如需詳細資訊，請參閱 <a href="#">vRealize Log Insight 中的稽核記錄</a> 。

## 與安全性相關的記錄檔訊息

ui\_runtime.log 檔案包含下列格式的使用者稽核記錄訊息。

- [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>]]

### 備註

- 某些記錄檔可在偵錯層級中取得。如需為每個節點啟用偵錯層級的相關資訊，請參閱[為使用者稽核記錄訊息啟用偵錯層級](#)。
- vRealize Log Insight 叢集中的每個節點都有自己的 `ui_runtime.log` 檔案。您可以檢查節點的記錄檔以監控叢集。

## 為使用者稽核記錄訊息啟用偵錯層級

您可以為使用者稽核記錄訊息啟用偵錯層級，以在 `ui_runtime.log` 檔案中包含記錄訊息。

### 必要條件

確認您具有根使用者認證以登入 vRealize Log Insight 虛擬應用裝置。

### 程序

- 1 導覽至位置 `/usr/lib/loginsight/application/etc/`，並在任何文字編輯器中開啟組態檔 `loginsight-config-base.xml`。
- 2 對於名稱為 `UI_RUNTIME_FILE` 的附加器，將 `Threshold` 參數的值更新為 `DEBUG`：

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

- 3 以 `DEBUG` 登入層級為 `LoginActionBean` 新增新的記錄器：

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

- 4 儲存並關閉 `loginsight-config-base.xml` 檔案。
- 5 執行 `service loginsight restart` 命令以套用變更。

## vRealize Log Insight 中的稽核記錄

稽核記錄會追蹤 vRealize Log Insight 的使用方式。

稽核記錄檔 `audit.log` 位於 `/storage/var/loginsight/`。此檔案會記錄下列動作：

類別	記錄的動作
使用者驗證	<ul style="list-style-type: none"> <li>■ 登入、登出和驗證失敗。</li> </ul>
存取控制	<ul style="list-style-type: none"> <li>■ 建立、移除和修改使用者、群組、角色和資料集。</li> </ul>
組態	<ul style="list-style-type: none"> <li>■ 建立和移除轉送站、vSphere 和 vRealize Operations Manager 整合等。</li> <li>■ 變更組態值，例如工作階段逾時、SSL、SMTP 配置等。</li> </ul>
內容套件	<ul style="list-style-type: none"> <li>■ 安裝、解除安裝和升級。</li> <li>■ 匯入和匯出。</li> </ul>
儀表板和 Widget	<ul style="list-style-type: none"> <li>■ 建立、移除和修改。</li> <li>■ 共用儀表板。</li> </ul>
管理	<ul style="list-style-type: none"> <li>■ 設定代理程式並啟用自動更新。</li> <li>■ 升級叢集。</li> <li>■ 新增和移除憑證和授權。</li> </ul>
警示	<ul style="list-style-type: none"> <li>■ 建立、移除和修改。</li> </ul>
互動式分析	<ul style="list-style-type: none"> <li>■ 建立、移除和修改快照及擷取的欄位。</li> </ul>

## vRealize Log Insight 使用者帳戶

您必須設定系統和根帳戶，才能管理 vRealize Log Insight。

### vRealize Log Insight 根使用者

vRealize Log Insight 目前使用根使用者帳戶做為服務使用者。未建立其他使用者。

除非在部署期間設定根密碼內容，否則預設根密碼為空白。當您首次登入 vRealize Log Insight 主控台時，必須變更根密碼。

設定預設根密碼之前，SSH 處於停用狀態。

根密碼必須滿足下列要求。

- 長度必須至少為 8 個字元
- 必須至少包含一個大寫字母、一個小寫字母、一個數字和一個特殊字元
- 同一字元不得重複使用四次

### vRealize Log Insight Admin 使用者

當您首次啟動 vRealize Log Insight 虛擬應用裝置時，vRealize Log Insight 會針對其 Web 使用者介面建立 Admin 使用者帳戶。

Admin 的預設密碼為空白。初始設定 vRealize Log Insight 期間，您必須在 Web 使用者介面中變更 Admin 密碼。

## Active Directory 支援

vRealize Log Insight 支援與 Active Directory 整合。設定後，vRealize Log Insight 即可根據 Active Directory 驗證或授權給使用者。

請參閱[透過 Active Directory 啟用使用者驗證](#)。

## 指派給預設使用者的權限

vRealize Log Insight 服務使用者具有根權限。

Web 使用者介面 Admin 使用者只有 vRealize Log Insight Web 使用者介面的管理員權限。

## vRealize Log Insight 防火牆建議

為保護 vRealize Log Insight 收集的機密資訊，請將伺服器置於受防火牆保護的管理網路區段，而非內部網路的其餘部分。

## 必要連接埠

下列連接埠必須向將資料傳送到 vRealize Log Insight 的來源的網路流量開啟。

連接埠	通訊協定
514/UDP、514/TCP	Syslog
1514/TCP、6514/TCP	Syslog-TLS (SSL)
9000/TCP	vRealize Log Insight 擷取 API
9543/TCP	vRealize Log Insight 擷取 API - TLS (SSL)

下列連接埠必須向需使用 vRealize Log Insight UI 的網路流量開啟。

連接埠	通訊協定
80/TCP	HTTP
443/TCP	HTTPS

下列連接埠集只能在 vRealize Log Insight 主要節點上針對從工作節點存取網路而開啟，以取得最大的安全性。

連接埠	通訊協定
16520:16580/TCP	Thrift RPC
59778/TCP	log4j 伺服器
12543/TCP	資料庫伺服器

## 安全性更新和修補程式

vRealize Log Insight 虛擬應用裝置會以 VMware Photon 3.0 作為客體作業系統。

vRealize Log Insight 8.0 或更新版本隨附於 Photon 作業系統。Photon 較隨附 vRealize Log Insight 4.8 或更舊版本的 SLES 作業系統更安全。

VMware 會發行修補程式以處理維護版本中的安全性問題。您可以從 [vRealize Log Insight 下載頁面](#) 下載這些修補程式。

將升級或修補程式套用到客體作業系統之前，請考慮相依性。請參閱 [連接埠與外部介面](#)。

# 備份、還原與災難復原

# 10

為避免發生代價高昂的資料中心停機，請在執行 vRealize Log Insight 備份、還原以及災難復原作業時遵循這些最佳做法。

本章節討論下列主題：

- 備份、還原和災難復原概觀
- 使用靜態 IP 位址和 FQDN
- 規劃和準備
- 備份節點和叢集
- 備份 Linux 或 Windows 代理程式
- 還原節點和叢集
- 還原後變更組態
- 確認還原
- 災害復原

## 備份、還原和災難復原概觀

VMware 提供的全面且經整合的業務持續性以及災難復原 (BCDR) 解決方案組合，可提供高可用性、資料保護以及災難復原。

將此文件中的備份、還原和災難復原資訊用於 vRealize Log Insight 元件，包括主要節點、工作節點和轉送站。

- 如需主要節點和工作叢集成員的相關資訊 (包括組態、記錄資料和自訂)，請參閱[備份節點和叢集](#)。
- 如需 Linux 或 Windows 代理程式本機組態的相關資訊，請參閱[備份 Linux 或 Windows 代理程式](#)。

本文件中的資訊不適用於下列工具和產品。您必須從多個資源取得這些工具和產品的資訊。

- 用於備份、還原和災難復原的第三方工具。如需詳細資訊，請參閱廠商說明文件。
- vSphere Data Protection、Site Recovery Manager 和 Veritas NetBackup。如需 VMware BCDR 解決方案的其他資訊，請參閱 <https://www.vmware.com/solutions/business-continuity-disaster-recovery-draas.html>。



- 與 vRealize Log Insight 整合之產品的備份、還原和災難復原功能。
  - vRealize Operations Manager
  - vSphere Web Client 伺服器
  - ESXi 主機

## 使用靜態 IP 位址和 FQDN

您可以使用靜態 IP 位址和 FQDN，以在備份、還原和災難復原作業期間避免風險。

### vRealize Log Insight 叢集節點和負載平衡器的靜態 IP 位址

如果您針對 vRealize Log Insight 叢集中的所有節點均使用靜態 IP 位址，在 IP 位址變更時，您無需更新叢集節點的 IP 位址。

vRealize Log Insight 包含[知識庫文章 2123058](#) 所述每個叢集節點組態檔中的所有節點 IP 位址

與 vRealize Log Insight (ESXi、vSphere、vRealize Operations) 整合的所有產品均使用叢集主要節點的完整網域名稱 (FQDN) 或 IP 位址做為 Syslog 目標。若已設定，這些產品可以使用負載平衡器的 FQDN 或 IP 位址做為 Syslog 目標。靜態 IP 位址減少了在多個位置中不斷更新 syslog 目標 IP 位址的風險。

為負載平衡器提供靜態 IP 位址和選用的虛擬 IP 位址。設定整合式負載平衡器時，會針對虛擬 IP 位址提供選用 FQDN。因任何原因無法連線 IP 位址時，便會使用 FQDN。

### vRealize Log Insight 叢集節點和工作節點的 FQDN

針對 vRealize Log Insight 叢集中的所有節點使用 FQDN 時，假設可在復原站台上解析相同的 FQDN，則可節省還原後組態變更和復原後組態變更的時間。

對於主要節點 (當使用負載平衡器時)，需要完全可解析的 FQDN。否則，ESXi 主機無法將 Syslog 訊息餽送至 vRealize Log Insight 或任何遠端目標。

針對系統通知，vRealize Log Insight 會使用 FQDN 主機名稱 (如果可用)，而非 IP 位址。

您可以合理假設在執行備份、還原或災難復原作業後，只有基礎 IP 位址會變更。使用 FQDN 便無需將記錄饋送至 vRealize Log Insight 叢集的所有外部裝置上變更 Syslog 目標位址 (主要節點 FQDN 或內部負載平衡器 FQDN)。

確認來自 vRealize Log Insight 工作節點的加入要求使用 vRealize Log Insight 主要節點的 FQDN。

每個節點上組態檔中的主要節點主機值，是以傳送加入要求之第一個工作節點所使用的值為基礎。為加入要求使用主要節點的 FQDN 可防止在災難復原後對主要節點主機值進行任何手動變更。否則，工作節點將無法重新加入主要節點，直到在所有還原的叢集節點上更新組態檔中的主要節點主機名稱。

## 規劃和準備

實作備份、還原或災難復原步驟前，請檢閱本主題中的規劃和準備資訊。

應將下列建議納入備份、還原以及災難復原計劃中。

## 測試備份作業

請先在測試或暫存環境中對備份、還原以及災難復原作業執行測試，然後再以即時生產設定執行這些作業。

對整個 vRealize Log Insight 叢集執行完整備份。請勿依賴自動程序來備份個別檔案和組態。

## 確認修正

請先確認修正已實作，且警告和錯誤已得到解決，然後再執行備份、還原以及災難復原作業。備份、還原以及災難復原工具通常會提供視覺化驗證和步驟，以確保已成功建立備份、還原以及災難復原組態。

## 排程備份

視叢集組態而定，第一次備份作業通常為完整備份。您應為第一次備份預留較長時間，供其完成作業。相較於第一次備份作業，後續備份 (可以是增量或完整備份) 會相對較快完成。

## 其他說明文件和工具

請確認您遵循說明文件的內容，為 vRealize Log Insight 備份、還原以及災難復原工具配置資源。

請確認您遵循適用於第三方備份、還原以及災難復原工具的工具特定最佳做法和建議。

對於使用 VMware 產品部署的虛擬機器，請使用可提供特殊功能和組態的其他工具，以支援備份、還原以及災難復原。

## 轉送站和叢集

對於轉送站，請針對主要 vRealize Log Insight 叢集套用備份、還原以及災難復原步驟。請參閱 [還原節點和叢集](#)。

根據客戶需求，您可能需要擁有單一或多個 vRealize Log Insight 轉送站。此外，轉送站可做為獨立節點或叢集安裝。在備份、還原以及災難復原作業中，vRealize Log Insight 轉送站與主要 vRealize Log Insight 叢集節點相同，且處理方式相同。

## 備份節點和叢集

最佳做法是為 vRealize Log Insight 節點和叢集設定排程的備份或複寫。

### 必要條件

- 執行備份或複寫作業之前，請先確認來源和目標站台上沒有組態問題存在。
- 確認叢集資源配置未達到最大容量。

在具有合理擷取和查詢負載的組態中，記憶體和交換使用量在備份和複寫作業期間幾乎可達到 100% 容量。由於即時環境中記憶體容量幾乎已滿，因此有一部分記憶體突然增加是由於 vRealize Log Insight 叢集使用量所造成。此外，排定的備份和複寫作業可明顯導致記憶體突然增加。

在某些情況下，工作節點會先暫時中斷連線 1 到 3 分鐘，然後再重新加入主要節點，這可能是因記憶體使用量較高所造成。

- 執行下列一或兩項作業來減少 vRealize Log Insight 節點上的記憶體節流。
  - 在 vRealize Log Insight 建議的組態上配置額外的記憶體。
  - 排程在離峰時間執行週期性備份。

#### 程序

- 1 使用與用於 vRealize Log Insight 伺服器相同的程序，啟用 vRealize Log Insight 轉送站的定期備份或複寫。
- 2 確認已根據可用的資源和客戶特定需求適當選取備份頻率和備份類型。
- 3 如果資源不是問題所在且受工具支援，請啟用並行叢集節點備份以加速備份程序。
- 4 同時備份所有節點。

如需如何備份節點的相關資訊，請參閱《vRealize Suite 說明文件》中的〈[備份、還原與災難復原](#)〉一節。

#### 後續步驟

監控 - 備份進行中時，請檢查 vRealize Log Insight 設定中是否存在任何環境或效能問題。大多數備份、還原和災難復原工具均提供監控功能。

在備份程序期間，請檢查生產系統上的所有相關記錄，因為使用者介面可能不會顯示所有問題。

## 備份 Linux 或 Windows 代理程式

您可以透過將安裝和組態資訊備份在伺服器端的方式來備份代理程式。不需要單獨備份代理程式節點。

代理程式安裝所在的 Linux 或 Windows 系統通常也會用於某些其他應用程式或服務，且可能包含在現有的備份程序中。包含整體代理程式安裝及其組態的完整檔案層級或區塊層級機器備份，即足以供復原使用。代理程式同時支援本機和伺服器提供的組態。

如果代理程式完全是從 vRealize Log Insight 伺服器進行設定，而未對 `liagent.ini` 組態檔進行任何本機變更，則您完全不需要建立代理程式安裝的備份。您可以改為執行代理程式的全新安裝，並擷取伺服器備份。

如果代理程式具有自訂本機組態，請備份 `liagent.ini` 檔案，並將其與代理程式的全新安裝一併還原。如果您將代理程式節點不僅僅用於安裝代理程式軟體，且如果這些節點需要完整備份，請遵循與任何其他虛擬機器相同的備份程序。

如果代理程式組態是在用戶端 (在代理程式上) 上設定，且如果代理程式節點僅用於安裝 vRealize Log Insight 代理程式軟體，則備份代理程式組態檔便已足夠。

#### 必要條件

確認代理程式組態位於 vRealize Log Insight 伺服器端上。

#### 程序

- 1 備份 `liagent.ini` 檔案。

- 2 使用備份檔案取代已復原代理程式或者 Linux 或 Windows 機器上的檔案。

## 還原節點和叢集

必須按特定順序還原節點，某些還原案例可能需要手動變更組態。

根據還原所使用的工具，您可以將虛擬機器還原至相同主機、相同資料中心上的不同主機或目標遠端資料中心上的不同主機。請參閱[還原後變更組態](#)

### 必要條件

- 確認已還原的節點處於電源已關閉狀態。
- 確認在將叢集還原至新站台之前，已關閉叢集執行個體的電源。
- 確認當復原站台上使用相同的 IP 位址和 FQDN 時，未發生核心分裂行為。
- 確認沒有有人在主要站台上意外使用部分運作的叢集。

### 程序

- 1 請先還原主要節點，再還原工作節點。
- 2 以任意順序還原工作節點。
- 3 (選擇性) 還原轉送站 (若已設定)。

確保在還原轉送站前，已還原 vRealize Log Insight 伺服器 (叢集設定中的主要節點和所有工作節點)。

- 4 還原任何已復原的代理程式。

### 後續步驟

- 還原 vRealize Log Insight 叢集時，如果使用相同的 IP 位址，請確認所有已還原的節點 IP 位址和 FQDN 與其原始對應項目相關聯。

例如，下列案例會失敗。在具有節點 A、B 和 C 的三節點叢集中，節點 A 使用 IP 位址 B 還原，節點 B 使用 IP 位址 C 還原，節點 C 使用 IP 位址 A 還原。

- 如果相同 IP 位址僅用於已還原節點的子集，請確認針對這些節點，所有已還原映像都與其原始 IP 位址相關聯。
- 大多數備份還原和災難復原工具提供用於觀看還原作業進度的監控檢視，以便發現故障或警告。對任何已識別的問題採取適當的動作。
- 如果站台完全還原之前需要手動組態變更，請遵循[還原後變更組態](#)中的準則。
- 成功完成還原後，對已還原的叢集執行快速檢查。

## 還原後變更組態

備份組態期間套用的復原目標和 IP 自訂決定需要進行哪些手動組態變更。您必須先將組態變更套用至一或多個 vRealize Log Insight 節點，還原的站台才能變為完全正常運作。

## 還原至相同主機

將 vRealize Log Insight 叢集復原至相同主機很簡單，且可透過任何工具執行。

### 必要條件

檢閱有關[規劃和準備](#)的重要資訊。

### 程序

- 1 先關閉現有叢集的電源，然後再開始還原作業。依預設，會將相同的 IP 位址和 FQDN 用於已還原的叢集節點。
- 2 (選擇性) 提供叢集的新名稱。  
在還原過程中，除非為虛擬機器提供新名稱，否則會使用已還原的版本覆寫叢集的原始複本。
- 3 (選擇性) 如果可能，請確認還原及復原的站台中已保留用於生產環境的所有網路、IP 及 FQDN 設定。

### 後續步驟

成功還原並進行例行性檢查之後，請刪除舊複本以保留資源，並防止使用者開啟舊複本電源時可能發生的意外核心分裂情況。

## 還原至不同主機

執行至不同主機的還原作業時，必須在 vRealize Log Insight 叢集上進行組態變更。

vRealize Log Insight 3.0 和更新版本未正式支援直接從應用裝置主控台修改組態檔。如需如何使用 Web UI 介面修改這些檔案的相關資訊，請參閱[知識庫文章 2123058](#)。

這些組態變更特定於可與任何備份復原工具搭配使用的 vRealize Log Insight 組建版本。

復原至不同主機需要對 vRealize Log Insight 叢集進行手動組態變更。您可以假設已還原的 vRealize Log Insight 節點具有與從中進行備份的來源對應項目不同的 IP 位址及 FQDN。

### 必要條件

檢閱有關[規劃和準備](#)的重要資訊。

### 程序

- 1 列出已指派給每個 vRealize Log Insight 節點的所有新的 IP 位址及 FQDN。

## 2 使用知識庫文章 2123058 所述的步驟對主要節點進行下列組態變更。

- a 在 vRealize Log Insight 組態區段中，尋找與下列命令行類似的命令行。

```
<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>
```

程式碼將顯示三個節點。第一個節點為主要節點，會顯示 `<service-group name=standalone>`，其餘兩個節點為工作節點，會顯示 `<service-group name="workernode">`。

- b 對於主要節點，在新復原的環境中，確認復原前環境中所使用的 DNS 項目是否可以重複使用。
- 如果 DNS 項目可以重複使用，只需要將該 DNS 項目更新為指向主要節點的新 IP 位址。
  - 如果 DNS 項目無法重複使用，請使用新的 DNS 名稱 (指向新的 IP 位址) 取代主要節點項目。
  - 如果無法指派 DNS 名稱，最後的選擇是用新的 IP 位址更新組態項目。
- c 同時更新工作節點 IP 位址以反映新的 IP 位址。

- d 在相同組態檔中，確認擁有代表 NTP、SMTP 以及 [資料庫] 和 [附加器] 區段的項目。

```
<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>
```

- 如果所設定的 NTP 伺服器值在新環境中不再有效，請在 <ntp>...</ntp> 區段中更新這些值。
- 如果所設定的 SMTP 伺服器值在新環境中不再有效，請在 <smtp>...</smtp> 區段中更新這些值。
- 可以選擇變更 SMTP 區段中的 default-sender 值。該值可以為任意值，但是適合的做法是，代表傳送電子郵件的來源。
- 在 <database>...</database> 區段中，將主機值變更為指向主要節點 FQDN 或 IP 位址。

- e 在相同組態檔中，更新 vRealize Log Insight ILB 組態區段。

```
<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> 區段下，如果 high-availability-ip 值與目前設定不同，請進行更新。
- g 確保同時更新負載平衡器的 FQDN。
- h 透過管理索引標籤上的叢集索引標籤從 Web UI 重新啟動。對於列出的每個節點，選取其主機名稱或 IP 位址以開啟詳細資料面板，然後按一下 **重新啟動 Log Insight**。
- 組態變更會自動套用到所有叢集節點。
- i vRealize Log Insight 服務啟動後，請等待 2 分鐘，讓 Cassandra 服務在其他工作節點上線前有足夠的時間啟動。

## 後續步驟

確認已為還原的 vRealize Log Insight 節點指派與從中進行備份的來源對應項目不同的 IP 位址及 FQDN。

## 確認還原

您必須確認所有已還原的 vRealize Log Insight 叢集均完全正常運作。

### 必要條件

在確認節點和叢集組態之前，請先確認備份和還原程序已完成。

### 程序

- 1 使用內部負載平衡器 (ILB) IP 位址或 FQDN (若已設定) 登入 vRealize Log Insight。
- 2 導覽至**管理索引標籤**。
- 3 確認下列各項：
  - a 確認您可使用各自的 IP 位址或 FQDN 存取所有個別叢集節點。
  - b 在叢集頁面上確認叢集節點的狀態，並確保 ILB (如果已設定) 亦處於作用中狀態。
  - c 確認 vSphere 整合。如有需要，可重新設定整合。復原後，若 ILB 或主要節點的 IP 位址或 FQDN 變更，則需要重新設定。
  - d 確認 vRealize Operations Manager 整合並在需要時再次重新設定。
  - e 確認所有內容套件及 UI 功能均正確運作。
  - f 確認 vRealize Log Insight 轉送站和代理程式正常運作 (若已設定)。
- 4 確認 vRealize Log Insight 的其他主要功能均如預期正常運作。

## 後續步驟

對您的備份和復原計劃進行任何必要的調整，以解決在備份、還原和確認作業期間可能會識別出的任何問題。

## 災害復原

完整記錄並經充分測試的復原計劃對於將叢集快速返回到工作狀態至關重要。

為災難復原設定虛擬機器時，複寫類型的選擇非常關鍵。決定複寫類型時，請考量復原點目標 (RPO)、復原時間目標 (RTO) 以及成本和擴充性。

在災難復原案例中，如果主要站台完全關閉，有時無法還原至相同站台。但根據您選擇的選項，若要将 vRealize Log Insight 叢集完全還原並返回至執行中狀態，則需要執行一些手動步驟。

除非 vRealize Log Insight 叢集完全關閉且無法存取，否則請確認在將叢集還原至新站台之前，已關閉叢集執行個體的電源。

在中斷或災難期間，儘快復原 vRealize Log Insight 叢集。



# 疑難排解 vRealize Log Insight

# 11

呼叫 VMware 支援服務之前，您可以解決與 vRealize Log Insight 管理相關的常見問題。

本章節討論下列主題：

- 無法在 Internet Explorer 上登入 vRealize Log Insight
- vRealize Log Insight 磁碟空間不足
- 匯入封存資料可能會失敗
- 使用虛擬應用裝置主控台建立 vRealize Log Insight 支援服務包
- 重設 Admin 使用者密碼
- 重設根使用者密碼
- 無法將警示傳遞到 vRealize Operations Manager
- 無法使用 Active Directory 認證登入
- 啟用了 STARTTLS 選項時 SMTP 無法運作
- 升級失敗，因為無法驗證 .pak 檔案的簽章
- 升級失敗並顯示內部伺服器錯誤
- 與 VMware 產品整合後，第一個記錄訊息中遺失 vmw\_object\_id 欄位

## 無法在 Internet Explorer 上登入 vRealize Log Insight

Internet Explorer 上的 vRealize Log Insight 驗證會失敗。

### 問題

vRealize Log Insight Web 用戶端需要 LocalStorage 或 DOM 儲存支援，但您的檔案系統完整性層級禁止 Internet Explorer 使用 LocalStorage。主控台和偵錯工具顯示錯誤 SCRIPT5：拒絕存取。

### 原因

vRealize Log Insight 無法存取 LocalStorage 或 DOM 儲存支援。Internet Explorer 會將此儲存區資料保存在以 CachePath 參數設定的資料夾中，其位置是 %USERPROFILE%\AppData\LocalLow\Microsoft\Internet Explorer\DOMstore。如果此資料夾的完整性層級不是「低」，Internet Explorer 就無法使用 LocalStorage。

## 解決方案

您可以使用下列命令設定使用者帳戶的完整性層級。

```
icacls %userprofile%\Appdata\LocalLow /t /setintegritylevel (OI)(CI)L
```

## vRealize Log Insight 磁碟空間不足

如果您使用小型虛擬磁碟且未啟用封存，vRealize Log Insight 主要節點或工作節點的磁碟空間可能會不足。

### 問題

如果每分鐘傳入記錄的速率超過儲存空間的 3%，或者 vRealize Log Insight 無法刪除儲存區中最舊的值區，則 vRealize Log Insight 磁碟空間會不足。

### 原因

在正常狀況下，vRealize Log Insight 磁碟空間永遠不會不足，因為它每隔一分鐘會檢查可用空間是否小於 3%。如果 vRealize Log Insight 虛擬應用裝置上的可用空間下降到 3% 以下，則會淘汰舊的資料貯體。

如果啟用了封存，vRealize Log Insight 會先封存貯體，然後再將其標記為已封存並在將來淘汰。如果可用空間在封存和淘汰舊的貯體之前就已填滿，則 vRealize Log Insight 磁碟空間會不足。

### 解決方案

請驗證資料封存位置是否可用，以及是否有足夠的可用空間。請參閱 [在 vRealize Log Insight 中啟用或停用資料封存](#)。

---

**備註** 如果所有解決方案都不適用，請連絡客戶支援。

---

## 匯入封存資料可能會失敗

如果 vRealize Log Insight 虛擬應用裝置的磁碟空間不足，匯入封存資料可能會失敗。

### 問題

vRealize Log Insight 存放庫匯入公用程式並不會檢查 vRealize Log Insight 虛擬應用裝置上的可用磁碟空間。因此，如果虛擬應用裝置的磁碟空間不足，匯入已封存記錄可能會失敗。

### 解決方案

請在增加 vRealize Log Insight 虛擬應用裝置的儲存區容量後，再重新開始匯入。請注意，在失敗前已成功匯入的資訊將會重複。

## 使用虛擬應用裝置主控台建立 vRealize Log Insight 支援服務包

如果您無法存取 vRealize Log Insight Web 使用者介面，則可以使用虛擬應用裝置主控台或在建立與 vRealize Log Insight 虛擬應用裝置的 SSH 連線之後，下載支援服務包。

### 必要條件

- 確認您具有根使用者認證以登入 vRealize Log Insight 虛擬應用裝置。
- 如果您計劃使用 SSH 連線到 vRealize Log Insight 虛擬應用裝置，請確認 TCP 連接埠 22 已開啟。

### 程序

- 1 建立與 vRealize Log Insight vApp 的 SSH 連線並以根使用者身分登入。
- 2 若要產生支援服務包，請執行 `loginsight-support`。

若要產生支援服務包並僅包含特定時段內變更的檔案，請執行包含 `--days` 限制的 `loginsight-support` 命令。例如，`--days=1` 將僅包含 1 日內變更的檔案。

### 結果

此時，會收集支援資訊並將其儲存至具有下列命名慣例的 `*.tar.gz` 檔案：`loginsight-support-YYYY-MM-DD_HHMMSS.xxxxx.tar.gz`，其中 `xxxxx` 是 `loginsight-support` 程序藉以執行的程序識別碼。

### 後續步驟

根據要求，將支援服務包轉寄給 VMware 支援服務。

## 重設 Admin 使用者密碼

如果 Admin 使用者忘記了 Web 使用者介面的密碼，則帳戶將無法連線。

### 必要條件

- 確認您具有根使用者認證以登入 vRealize Log Insight 虛擬應用裝置。
- 若要啟用 SSH 連線，請確認 TCP 連接埠 22 為開啟狀態。

### 問題

如果 vRealize Log Insight 只有一個 Admin 使用者且該 Admin 使用者忘記了密碼，則無法管理應用程式。如果 Admin 使用者是 vRealize Log Insight 的唯一使用者，則將無法存取整個 Web 使用者介面。

### 原因

如果使用者不記得其目前的密碼，vRealize Log Insight 即不會提供 Admin 使用者的使用者介面讓他們重設自己的密碼。

---

**備註** 可登入的 Admin 使用者可以重設其他 Admin 使用者的密碼。僅當所有 Admin 使用者帳戶的密碼未知時才重設 Admin 使用者密碼。

---

### 解決方案

- 1 建立與 vRealize Log Insight 虛擬應用裝置的 SSH 連線並以根使用者身分登入。

## 2 執行重設 Admin 使用者密碼的指令碼：

```
li-reset-admin-passwd.sh
```

指令碼會重設 Admin 使用者密碼，然後產生一個新密碼並將其顯示在畫面上。

### 後續步驟

使用新密碼登入 vRealize Log Insight Web 使用者介面並變更 Admin 使用者密碼。

## 重設根使用者密碼

如果您忘記了根使用者的密碼，則無法再建立 SSH 連線或使用 vRealize Log Insight 虛擬應用裝置的主控制台。

由於各種原因，您可能無法以根使用者身分登入，其中包括：

- 您未變更預設密碼。依預設，vRealize Log Insight 會為根使用者設定空白密碼，且會停用 SSH 存取。密碼設定後，即可為根使用者啟用 SSH 存取。
- 您可在 vRealize Log Insight 虛擬應用裝置部署期間設定 SSH 金鑰。如果 SSH 金鑰是透過 OVF 指定的，將會停用密碼驗證。請使用設定的 SSH 金鑰登入或查看下方的解決方案步驟。
- 您已多次輸錯密碼，現已暫時被鎖定。在此情況下，即使輸入正確的密碼，也無法在鎖定期間結束前登入。您可等待鎖定期間結束或重新啟動虛擬應用裝置。

由於 vRealize Log Insight 虛擬應用裝置位於 Photon OS 上，下列步驟說明如何在 Photon OS 機器上重設根密碼。

### 問題

如果您無法建立 SSH 連線或使用 vRealize Log Insight 虛擬應用裝置的主控制台，則無法完成部分管理工作，也無法重設 Admin 使用者的密碼。

### 解決方案

- 1 重新啟動正在執行 Photon OS 的 vRealize Log Insight 虛擬機器。
- 2 當 Photon OS 重新開機且顯示啟動顯示畫面時，立即輸入字母 `e` 以移至 GNU GRUB 編輯功能表。

**備註** 由於 Photon OS 會快速重新開機，因此您將必須在短時間內輸入 `e`。在 vSphere 和 Workstation 中，您可能必須先按一下主控台視窗讓主控台進入焦點後，它才會接受您的鍵盤輸入。

- 3 在 GNU GRUB 編輯功能表中，在以 `linux` 開頭的行結尾，輸入空格並新增下列程式碼：

```
rw init=/bin/bash
```

- 4 按 F10 以開啟命令提示字元。
- 5 執行下列命令：

```
passwd
```

- 6 依照指示輸入及重新輸入符合 Photon OS 密碼複雜性規則的新根密碼。請務必記住密碼。
- 7 當您看到訊息指出密碼已更新時，請執行下列命令：

```
umount /
```

- 8 執行下列命令。

```
reboot -f
```

---

**備註** 您必須包含 `-f` 選項，才能強制重新開機。否則，核心會進入緊急狀態。

---

#### 後續步驟

vRealize Log Insight 重新開機後，請驗證您是否能使用新的根使用者密碼登入。

## 無法將警示傳遞到 vRealize Operations Manager

如果警示事件無法傳送到 vRealize Operations Manager，vRealize Log Insight 會通知您。vRealize Log Insight 會每分鐘都重試傳送警示，直到問題解決為止。

#### 問題

當警示無法傳遞到 vRealize Operations Manager 時，vRealize Log Insight 工具列中會顯示一個帶有驚嘆號的紅色符號。

#### 原因

連線問題會阻止 vRealize Operations Manager vRealize Log Insight 將警示通知傳送到 vRealize Operations Manager。

#### 解決方案

- ◆ 按一下紅色圖示開啟錯誤訊息清單，然後向下捲動檢視最新訊息。  
開啟錯誤訊息清單或問題已解決時，紅色符號會從工具列中消失。
- ◆ 若要修正 vRealize Operations Manager 的連線問題，請嘗試以下作業。
  - 確認 vRealize Operations Manager vApp 未關閉。
  - 確認您可透過**測試連線**按鈕連線至 vRealize Operations Manager，該按鈕位於 vRealize Log Insight Web 使用者介面之**管理**索引標籤的 **vRealize Operations Manager** 區段。
  - 透過直接登入 vRealize Operations Manager 確認您擁有正確的認證。
  - 檢查 vRealize Log Insight 和 vRealize Operations Manager 記錄檔查看與連線問題相關的訊息。
  - 確認在 vRealize Operations Manager vSphere 使用者介面中未篩選出任何警示。

## 無法使用 Active Directory 認證登入

使用 Active Directory 認證時，無法登入 vRealize Log Insight Web 使用者介面。

### 問題

儘管管理員已將您的 Active Directory 帳戶新增至 vRealize Log Insight，您還是無法使用 Active Directory 網域使用者認證登入 vRealize Log Insight。

### 原因

最常見的原因為密碼過期、認證錯誤、連線問題或 vRealize Log Insight 虛擬應用裝置與 Active Directory 的時鐘之間缺少同步。

### 解決方案

- 請確認您的認證有效、密碼尚未過期，並且 Active Directory 帳戶未鎖定。
- 如果您尚未指定要與 Active Directory 驗證搭配使用的網域，請確認您將預設網域上的帳戶儲存在位於 `/storage/core/loginsight/config/loginsight-config.xml#[number]` (其中 `[number]` 為最大) 的最新 vRealize Log Insight 組態中。
- 找出最新組態檔：`/storage/core/loginsight/config/loginsight-config.xml#[number]`，其中 `[number]` 為最大。
- 確認 vRealize Log Insight 可連線至 Active Directory 伺服器。
  - 前往 vRealize Log Insight Web 使用者介面之**管理**索引標籤的**驗證**區段，填寫您的使用者認證，然後按一下**測試連線**按鈕。
  - 如需與 DNS 問題相關的訊息，請查看 vRealize Log Insight `/storage/var/loginsight/runtime.log`。
- 確認 vRealize Log Insight 與 Active Directory 時鐘保持同步。
  - 如需與時鐘誤差相關的訊息，請查看 vRealize Log Insight `/storage/var/loginsight/runtime.log`。
  - 使用 NTP 伺服器以同步 vRealize Log Insight 和 Active Directory 的時鐘。

## 啟用了 STARTTLS 選項時 SMTP 無法運作

如果在啟用了 STARTTLS 選項時設定 SMTP 伺服器，則測試電子郵件會失敗。將 SMTP 伺服器的 SSL 憑證新增到 Java 信任存放區可解決此問題。

### 必要條件

- 確認您具有根使用者認證以登入 vRealize Log Insight 虛擬應用裝置。
- 如果您計劃使用 SSH 連線到 vRealize Log Insight 虛擬應用裝置，請確認 TCP 連接埠 22 已開啟。

## 程序

- 1 建立與 vRealize Log Insight vApp 的 SSH 連線並以根使用者身分登入。
- 2 將 SMTP 伺服器的 SSL 憑證複製到 vRealize Log Insight vApp。
- 3 執行下列命令。

```
`/usr/java/jre-vmware/bin/keytool -import -alias certificate_name -file
path_to_certificate -keystore /usr/java/jre-vmware/lib/security/cacerts`
```

**備註** 使用鍵盤上波狀符號所在之按鍵上的倒單引號符號插入外引號。請勿使用單引號。

- 4 輸入預設密碼 **changeit**。
- 5 執行 `service loginsight restart` 命令。

## 後續步驟

導覽到**管理 > Smtip** 並使用**傳送測試電子郵件**測試您的設定。請參閱為 [vRealize Log Insight 設定 SMTP 伺服器](#)

## 升級失敗，因為無法驗證 .pak 檔案的簽章

vRealize Log Insight 升級失敗，因為 .pak 檔案損毀，授權已到期或磁碟空間不足。

### 問題

升級 vRealize Log Insight 失敗，並顯示錯誤訊息：升級失敗。無法升級：無法驗證 PAK 檔案的簽章。

### 原因

由於下列原因出現錯誤：

- 上傳的檔案並非 .pak 檔案。
- 上傳的 .pak 檔案不完整。
- vRealize Log Insight 的授權已到期。
- vRealize Log Insight 虛擬應用裝置根檔案系統沒有足夠的磁碟空間。

### 解決方案

- ◆ 確認您上傳的是 .pak 檔案。
- ◆ 對照 VMware 下載網站確認 .pak 檔案的 md5sum。
- ◆ 確認已至少在 vRealize Log Insight 上設定一個有效的授權。
- ◆ 登入 vRealize Log Insight 虛擬應用裝置，然後執行 `df -h` 以檢查可用的磁碟空間。

**備註** 請勿將檔案置於 vRealize Log Insight 虛擬應用裝置根檔案系統之中。

## 升級失敗並顯示內部伺服器錯誤

vRealize Log Insight 升級失敗，並顯示由於連線問題導致發生內部伺服器錯誤。

### 問題

升級 vRealize Log Insight 失敗，並顯示錯誤訊息：升級失敗。內部伺服器錯誤。

### 原因

用戶端和伺服器之間出現連線問題。例如，當您嘗試從 WAN 上的用戶端進行升級。

### 解決方案

- ◆ 從與伺服器相同的 LAN 上的用戶端升級 LI。

## 與 VMware 產品整合後，第一個記錄訊息中遺失 vmw\_object\_id 欄位

與 vRealize Log Insight VMware 產品整合後，第一個記錄訊息中未包含 vmw\_object\_id 欄位。

### 問題

您在整合 vRealize Log Insight 與 vCenter Server 和 vRealize Operations Manager 後接收的第一個記錄訊息不會包含相關聯的 vmw\_object\_id 欄位。將 vRealize Operations Manager 物件指定為警示目標時，遺漏此欄位可能會影響到警示傳遞機制。

---

**備註** 請確定 vCenter Server 也已與 vRealize Operations Manager 整合。

---

### 解決方案

請等待兩分鐘。您收到的下一個記錄訊息將會包含 vmw\_object\_id 欄位。