開始使用 vRealize Log Insight

2022 年 5 月 24 日

vRealize Log Insight 8.1

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

目錄

vRealize Log Insight 入門

《vRealize Log Insight 入門》提供有關部署和設定 VMware® vRealize™Log Insight™ 的資訊，其中包括如何調整 vRealize Log Insight 虛擬應用裝置的大小以接收記錄訊息。

請在您想要計劃或安裝部署時使用此資訊。此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 Linux 和 Windows 系統管理員而撰寫。

安裝 vRealize Log Insight 之前 1

若要在您的環境中開始使用 vRealize Log Insight，您必須部署 vRealize Log Insight 虛擬應用裝置並套用一些基本組態。

本章節討論下列主題：

- vRealize Log Insight 中支援的記錄檔和封存格式
- 安全性需求
- 產品相容性
- 最低需求
- 規劃您的 vRealize Log Insight 部署
- 調整 vRealize Log Insight 虛擬應用裝置的大小
- 整合 vRealize Log Insight 和 vRealize Operations Manager

vRealize Log Insight 中支援的記錄檔和封存格式

您可以使用 vRealize Log Insight 來分析非結構化或結構化記錄資料。

vRealize Log Insight 會接受來自下列來源的資料：

- 支援透過 Syslog 通訊協定傳送記錄串流的來源。
- 寫入記錄檔且可執行 vRealize Log Insight 代理程式的來源。
- 可使用 REST API 服務並透過 HTTP 或 HTTPS 來張貼記錄資料的來源。`https://<vRLI_host>/rest-api` 的 vRealize Log Insight 介面提供 API 說明文件。
- vRealize Log Insight 封存的歷史資料。

vSphere 記錄剖析器可讓您在 vRealize Log Insight 中匯入 vSphere 記錄服務包。

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。

在管理 vRealize Log Insight 中參閱將 Log Insight 封存匯入 vRealize Log Insight。

安全性需求

為了確保您的虛擬環境免遭外部攻擊，您必須遵守特定規則。

- 總是在受信任網路中安裝 vRealize Log Insight。
- 總是在安全位置中儲存 vRealize Log Insight 支援服務包。

IT 決策者、架構設計人員、管理員，以及必須熟悉 vRealize Log Insight 的安全性元件的其他人，都必須閱讀 管理 vRealize Log Insight 中的安全性主題。

這些主題可提供 vRealize Log Insight 安全性功能的簡要參考。主題包括產品外部介面、連接埠、驗證機制，以及安全性功能的組態和管理選項。

如需保護虛擬環境的相關資訊，請參閱《VMware vSphere 安全性指南》和 VMware 網站上的「安全中心」。

產品相容性

vRealize Log Insight 透過 syslog 通訊協定和 HTTP 收集資料，可連線至 vCenter Server 以收集事件、工作和警示資料，並能與 vRealize Operations Manager 進行整合以傳送通知事件和啟用在環境定義中啟動。請檢查《VMware vRealize Log Insight 版本說明》，以取得有關受支援產品版本的最新更新。

虛擬應用裝置部署

您必須使用 vSphere 部署 vRealize Log Insight 虛擬應用裝置。總是使用 vSphere Client 連線至 vCenter Server。在由 vCenter Server 5.0 或更新版本管理的 ESX/ESXi 主機版本 5.0 或更新版本上部署 vRealize Log Insight 虛擬應用裝置。

Syslog 摘要

vRealize Log Insight 會透過下列連接埠和通訊協定來收集和分析 Syslog 資料：

- 514/UDP
- 514/TCP
- 1514/TCP (SSL)

您必須設定環境元件 (如作業系統、應用程式、儲存區、防火牆和網路裝置)，以將其 syslog 摘要推送至 vRealize Log Insight。

API 摘要

vRealize Log Insight 擷取 API 會透過下列連接埠和通訊協定收集資料。

- 9000/TCP
- 9543/TCP (SSL)

vSphere 整合

您可以將 vRealize Log Insight 設定為提取在一或多個 vCenter Server 執行個體中發生的工作、事件和警示的資料。vRealize Log Insight 使用 vSphere API 連線至 vCenter Server 系統並收集資料。

您可以將 ESXi 主機設定為將 syslog 資料轉送給 vRealize Log Insight。

如需 vCenter Server 和 ESXi 特定版本的相容性資訊，請參閱 VMware 產品互通性對照表。

如需連線至 vSphere 環境的相關資訊，請參閱將 vRealize Log Insight 連線到 vSphere 環境。

vRealize Operations Manager 整合

可透過兩種獨立的方法整合 vRealize Log Insight 和 vRealize Operations Manager vApp 或 Installable。

vCenter Operations Manager 支援的所有版本均支援通知以及「在環境定義中啟動」。

- vRealize Log Insight 可將通知事件傳送給 vRealize Operations Manager。

  請參閱設定 vRealize Log Insight 以將通知事件傳送至 vRealize Operations Manager。

- vRealize Operations Manager 的 [在環境定義中啟動] 功能表可顯示與 vRealize Log Insight 相關的動作。

  請參閱在 vRealize Operations Manager 中啟用 vRealize Log Insight 的在環境定義中啟動。

最低需求

VMware 將 vRealize Log Insight 做為虛擬應用裝置以 OVA 檔案格式進行散佈。各種資源和應用程式必須適用於虛擬應用裝置才能成功執行。如需有關需求的最新資訊，請查看最新的版本說明。

虛擬硬體

您可以在部署 vRealize Log Insight 虛擬應用裝置期間，根據環境的擷取需求從預設組態大小中進行選取。預設是已經過認證的運算和磁碟資源大小組合，但您也可以在之後新增額外的資源。如下表所述，小型組態在維持支援時會耗用最少的資源。您也可以使用極小型組態，但這僅適合示範用途。

如需依據擷取需求的完整資源需求，請參閱調整 vRealize Log Insight 虛擬應用裝置的大小。

表 1-1. 小型組態的預設值

資源	最低需求
記憶體	8 GB
vCPU	4
儲存空間	530 GB

支援的瀏覽器

您可以使用下列其中一個瀏覽器連線到 vRealize Log Insight Web 使用者介面。更新版本的瀏覽器也適用於 vRealize Log Insight，但尚未經過驗證。

重要 您的瀏覽器中必須啟用 Cookie。

- Mozilla Firefox 45.0 及更高版本
- Google Chrome 51.0 及更高版本
- Safari 9.1 及更高版本
- Internet Explorer 11.0 及更高版本

備註

- Internet Explorer 文件模式必須設定為**標準模式**。不支援其他模式。
- **瀏覽器模式**：不支援相容性檢視。
- 若要在 vRealize Log Insight Web 用戶端上使用 Internet Explorer，Windows 本機儲存區完整性層級必須設為「低」。

帳戶密碼

類型	需求
根	除非您在部署 OVA 期間指定根密碼或使用客體自訂，否則 vRealize Log Insight 虛擬應用裝置上根使用者的預設認證為 **root/<blank>**。您首次存取 vRealize Log Insight 虛擬應用裝置主控台時，會提示您變更根帳戶密碼。 **備註** 在您設定根密碼之前，SSH 會停用。
使用者帳戶	在 vRealize Log Insight 3.3 和更新版本中建立的使用者帳戶需要強式密碼。密碼必須至少為 8 個字元，且必須包含一個大寫字元、一個小寫字元、一個數字和一個特殊字元。

整合需求

產品	需求
vCenter Server	若要從 vCenter Server 提取事件、工作和警示資料，必須針對該 vCenter Server 提供一組使用者認證。若要使用 vCenter Server 登錄和解除登錄 vRealize Log Insight，則至少需要**唯讀**角色。此角色必須於 vCenter Server 層級上進行設定，並傳播至子物件。若要設定 vCenter Server 所管理的 ESXi 主機，vRealize Log Insight 還需要其他權限。
vSphere ESXi	需要 vSphere ESXi 6.0 Update 1 或更新版本，才可建立 vRealize Log Insight 的 SSL 連線。
vRealize Operations Manager	若要在 vRealize Operations Manager 執行個體中啟用通知事件和在環境定義中啟動功能，您必須針對該 vRealize Operations Manager 執行個體提供使用者認證。

網路連接埠需求

下列網路連接埠必須可從外部進行存取。

連接埠	通訊協定
22/TCP	SSH
80/TCP	HTTP
443/TCP	HTTPS
514/UDP、514/TCP	Syslog
1514/TCP	僅限透過 SSL 的 Syslog 擷取
9000/TCP	vRealize Log Insight 擷取 API
9543/TCP	vRealize Log Insight 擷取 API (SSL)

規劃您的 vRealize Log Insight 部署

您可為 vRealize Log Insight 部署單一節點、單一叢集或具有轉送站的叢集。

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。

透過 vRealize Suite Lifecycle Manager 進行安裝

vRealize Suite Lifecycle Manager 會自動執行套件產品的安裝、組態、升級、修補、組態管理、偏離修復，以及健全狀況。您可以透過 vRealize Suite Lifecycle Manager 安裝 vRealize Log Insight，以取代使用 vRealize Log Insight 進行安裝。您必須使用 vRealize Suite Lifecycle Manager 1.2 版或更新版本，以及 vRealize Log Insight 4.5.1 或更新版本。如需詳細資訊，請參閱 vRealize Suite Lifecycle Manager 說明文件。

單一節點

基本 vRealize Log Insight 組態包含單一節點。記錄檔來源可以是應用程式、作業系統記錄檔、虛擬機器記錄檔、主機、vCenter Server、虛擬或實體交換器和路由器、儲存區硬體等。記錄資料流會直接透過來源上安裝的應用程式、Syslog 集訊器或 vRealize Log Insight 代理程式，使用 Syslog (UDP、TCP、TCP+SSL) 或 CFAPI (透過 HTTP 或 HTTPS 的 vRealize Log Insight 原生擷取通訊協定) 傳輸至 vRealize Log Insight 節點。

單一節點部署的最佳做法是使用 vRealize Log Insight 整合式負載平衡器 (ILB)，並將查詢和擷取流量傳送至 ILB。如此不會產生額外負荷，且未來若您想為部署新增節點和建立叢集時將可簡化設定程序。

最佳做法是，請勿針對生產環境使用單一節點。

叢集

生產環境通常需要使用叢集。叢集必須符合下列需求：

- 叢集中的所有節點應為相同大小且位於相同資料中心。
- 搭配叢集使用的 ILB 需要節點位於相同的 L2 網路。
- vRealize Log Insight 虛擬機器必須從 VMware NSX 分散式防火牆保護中排除。

這是因為叢集的虛擬 IP 會在「伺服器直接回傳模式」(LVS-DR) 中使用 Linux 虛擬伺服器，以進行負載平衡。「伺服器直接回傳」比透過單一叢集成員路由所有回應流量更有效率。但是，其形式類似於詐騙流量，因此會遭到 NSX 分散式防火牆封鎖。

調整叢集大小

vRealize Log Insight 單一叢集組態可包含三至十八個節點，且使用 ILB。叢集需要至少三個狀況良好的節點才能正確運作。

生產環境需要至少為中等大小的節點。如果您預期會使用大量的並行查詢，包括警示，請考慮使用大型節點。如需調整大小的相關資訊，請參閱調整 vRealize Log Insight 虛擬應用裝置的大小。

雖然 vRealize Log Insight 叢集中的節點最小數目為三個，如果有節點失敗，其中健全狀況良好的節點少於三個，叢集將不會完全正常運作。此外，叢集中健全狀況良好的節點數目必須大於叢集節點總數的一半。例如，如果您有六個節點的叢集，而其中三個節點無法使用，除非從叢集移除不具功能的節點，否則叢集無法完全正常運作。 不支援移除和重新引入叢集節點。

具有轉送站的叢集

具有轉送站組態的 vRealize Log Insight 叢集包含主要索引、儲存區，和一個由三至十八個使用 ILB 之節點所組成的查詢叢集。單一記錄訊息只會存在於主要叢集內的一個位置中，如同在單一叢集中的情況。

透過在遠端站台或叢集上新增多個轉送站叢集可擴充設計。每個轉送站叢集皆設定為將其所有記錄訊息轉送至主要叢集，使用者可連線至主要叢集，從而利用 CFAPI 在轉送路徑上進行壓縮並獲得彈性。設定為機櫃頂端 (Top-of-Rack) 的轉送站叢集可以設定較大的本機保留。

用於備援的交叉轉送

此 vRealize Log Insight 部署案例包含具有已延伸和已鏡像之轉送站的叢集。兩個主要叢集用於索引建立、儲存和查詢。每個資料中心各有一個主要叢集。每個叢集的前端皆有成對的專用轉送站叢集。所有機櫃頂端彙總的所有記錄來源集中在轉送站叢集上。您可在兩個保留叢集上獨立查詢相同的記錄。

vRealize Log Insight 整合式負載平衡器

若要在叢集中的節點間適當平衡流量，並盡可能減輕管理額外負荷，請針對所有部署使用整合式負載平衡器 (ILB)。這可確保即使在部分 vRealize Log Insight 節點無法使用時，仍可接受傳入擷取流量。

調整 vRealize Log Insight 虛擬應用裝置的大小

依預設，vRealize Log Insight 虛擬應用裝置會使用小型組態的預設值。

獨立部署

您可以變更應用裝置設定，以符合要在部署期間收集記錄的環境需求。

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，但您也可以在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。

大小調整根據下列假設而定。

- 每個虛擬 CPU 至少為 2 GHz。
- 每個 ESXi 主機每秒最多可傳送 10 則訊息，且訊息的平均大小為 170 位元組/訊息，大約相當於 150 MB/天/主機。

備註 對於大型安裝，您必須升級 vRealize Log Insight 虛擬機器的虛擬硬體版本。vRealize Log Insight 支援虛擬硬體版本 7 或更新版本。虛擬硬體版本 7 最多可支援 8 個虛擬 CPU。因此，如果您打算佈建 16 個虛擬 CPU，則必須將 ESXi 5.x 的虛擬硬體升級至版本 8 或更新版本。您可以使用 vSphere Client 來升級虛擬硬體。如果您想要將虛擬硬體升級為最新版，請閱讀並瞭解 VMware 知識庫文章 Upgrading a virtual machine to the latest hardware version (1010675) (將虛擬機器升級為最新硬體版本 (1010675)) 中的資訊。

叢集部署

為 vRealize Log Insight 叢集中的主要節點和工作節點使用中型組態或更大的組態。每秒事件數會以線性方式隨節點數增加。例如，在 3 到 18 節點的叢集中 (叢集必須具有至少三個節點)，18 節點叢集中的擷取為每秒 270,000 個事件 (EPS) 或每天 4 TB 的事件。

減小記憶體大小

在概念驗證或測試環境中，而非在生產環境中使用應用裝置的**超小型**版本。此組態最多可支援 20 個 ESXi 主機 (約 200 個事件/秒或約 3 GB/天)。

vRealize Log Insight 大小調整計算器

計算器可協助您決定 vRealize Log Insight 和網路與儲存區使用量的可用大小調整。此計算器僅提供指引。許多環境輸入為站台特定，因此計算器必須在某些區域中使用估計值。請參閱 https://www.vmware.com/go/loginsight/calculator。

備註 如果您在定義轉送站時所根據的文字欄位具有涉及規則運算式的複雜條件或多個條件 (例如「`text=~"Deleting the machine`」)，則 vRealize Log Insight 的整體效能可能會下降。在這些情況下，尤其是叢集上的整體負載較高時，可能會降低效能，且磁碟區塊可能會累積在叢集的每個節點上。

整合 vRealize Log Insight 和 vRealize Operations Manager

若要能夠在 vRealize Log Insight 和 vRealize Operations Manager 之間進行整合，這兩個產品都必須執行設定。

程序

1 將 vRealize Log Insight Management Pack 安裝到 vRealize Operations Manager 中。

在兩個產品之間使用「在環境定義中啟動」功能，需要 vRealize Log Insight Management Pack。可在 vRealize Operations Manager 下載檔案中或 VMware Solution Exchange 網站上取得 vRealize Log Insight Management Pack。

2 設定 vRealize Log Insight 以連線至 vRealize Operations Manager。

3 設定 vRealize Log Insight 警示以將資訊轉送到 vRealize Operations Manager。

請參閱《管理 vRealize Log Insight》中的〈將 vRealize Log Insight 設定為傳送通知事件至 vRealize Operations Manager〉。

4 啟用 vRealize Operations 的「在環境定義中啟動」以在 vRealize Log Insight 中查詢記錄。

請參閱《管理 vRealize Log Insight》中的〈在 vRealize Operations Manager 中為 vRealize Log Insight 啟用在環境定義中啟動〉。

事件的生命週期

2

瞭解 vRealize Log Insight 如何處理訊息和事件是有效使用 vRealize Log Insight 的關鍵。

記錄訊息或事件的生命週期具有多個階段，包括讀取、剖析、擷取、索引、警示、查詢應用程式、封存，以及刪除。

事件和訊息轉換會經歷下列階段。

1 事件產生於裝置上 (在 vRealize Log Insight 外部)。

2 提取事件，並使用下列方式之一傳送至 vRealize Log Insight：

- 藉由使用擷取 API 或 syslog 的 vRealize Log Insight 代理程式
- 透過使用 syslog 的第三方代理程式，例如 rsyslog、syslog-ng 或 log4j
- 藉由對擷取 API 的自訂寫入 (例如 log4j 附加器)
- 藉由對 syslog 的自訂寫入 (例如 log4j 附加器)

3 vRealize Log Insight 接收事件。

- 如果您使用整合式負載平衡器 (ILB)，則事件會導向至負責處理事件的單一節點。
- 如果事件遭到拒絕，用戶端會透過 UDP 捨棄、具有通訊協定設定的 TCP，或具有磁碟支援佇列的 CFAPI 來處理拒絕作業。
- 如果接受事件，則系統會通知用戶端。

4 透過 vRealize Log Insight 擷取管線傳遞事件；此時會發生下列步驟：

- 建立或更新關鍵字索引。索引會以專屬格式儲存在本機磁碟中。
- 將機器學習套用至叢集事件。
- 事件會以壓縮的專屬格式儲存在本機磁碟的值區中。

5 查詢事件。

- 將關鍵字和 Glob 查詢與關鍵字索引比對。
- 將 Regex 與壓縮事件比對。

6 將事件移至值區並封存。

- 當值區到達 0.5 GB，將會密封並封存。

7 刪除事件。

- 值區會依照 FIFO 順序刪除。

取得詳細資訊

如需詳細資訊，請參閱 VMware Technical Publications 影片

vRealize Log Insight 中的記錄事件生命週期。(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_horp849x/uiConfId/50138843/)

本章節討論下列主題：

事件生命週期的重要方面

隨著事件存留時間的增長，需要在事件生命週期期間留意一些事件儲存與管理的重要環節。

事件儲存

每個事件都儲存在單個磁碟上的值區中。使用值區時，請留意下列行為和特性。

- 值區的大小最多可能達到 0.5 GB。當值區達到 0.5 GB 時，會密封並排入佇列以進行封存。密封的值區完成封存後，就會標記為已封存。事件可同時保留在本機和封存檔上。
- 值區不會跨 vRealize Log Insight 節點複寫。當您遺失某個節點時，則會失去該節點上的資料。
- 所有值區均儲存在 `/storage/core` 磁碟分割上。
- 當 `/storage/core` 磁碟分割上的可用空間小於 3% 時，vRealize Log Insight 將會刪除舊值區。刪除會依照 FIFO 模式來進行。

備註 `/storage/core` 磁碟分割的狀態接近滿載是正常和預期情形。該磁碟分割應該永遠不會達到 100%，因為 vRealize Log Insight 會管理該磁碟分割。但是，請勿嘗試在該磁碟分割上儲存資料，因為它可能會干擾舊值區的刪除。

事件管理

當您安裝並設定您的產品時，先熟悉 vRealize Log Insight 事件和事件管理的下列特性和行為會很有幫助。

- 在本機上刪除事件後，除非使用命令列介面從封存檔中匯入該事件，否則無法再查詢該事件。
- 從 vRealize Log Insight 中刪除機器學習叢集的所有事件後，該叢集即會移除。
- vRealize Log Insight 會公平地將叢集中各節點間的所有傳入事件重新平衡。例如，即使明確地將某個節點傳送至事件，該節點也可能不是要擷取事件的節點。
- 事件中繼資料以專屬格式儲存在單個 vRealize Log Insight 節點上，而不是資料庫中。
- 事件可存在於本機的節點上，也可存在於封存檔上。

安裝 vRealize Log Insight 3

vRealize Log Insight 會做為虛擬應用裝置來提供，且必須部署在您的 vSphere 環境中。

檢閱調整 vRealize Log Insight 虛擬應用裝置的大小後，前往部署 vRealize Log Insight 虛擬應用裝置。不論您執行的是單一節點部署還是叢集化部署，請遵循本節所述的標準 OVF 部署程序。

備註 您可以使用 vRealize Suite Lifecycle Manager 1.2 或更新版本來安裝 vRealize Log Insight 4.5.1 及更新版本。如需詳細資訊，請參閱 vRealize Suite 說明文件。

本章節討論下列主題：

- 部署 vRealize Log Insight 虛擬應用裝置
- 開始新的 vRealize Log Insight 部署
- 加入現有部署

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，但您也可以在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 伺服器和閘道資訊)，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。 a 關閉 vRealize Log Insight 虛擬應用裝置的電源。 b 在虛擬應用裝置上按一下滑鼠右鍵，然後選取**編輯設定**。 c 設定虛擬應用裝置的靜態 IP 位址。

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。

開始新的 vRealize Log Insight 部署

完成虛擬應用裝置部署或從叢集中移除工作節點後，在首次存取 vRealize Log Insight Web 介面時，您必須完成初始組態步驟。

在初始組態期間修改的所有設定也可在管理 Web 使用者介面中找到。

如需在您參與客戶經驗改進計劃時，vRealize Log Insight 可能會收集並傳送至 VMware 的追蹤資料相關資訊，請參閱第 4 章 客戶經驗改進計劃。

必要條件

- 在 vSphere Client 中，記下 vRealize Log Insight 虛擬應用裝置的 IP 位址。如需有關尋找 IP 位址的資訊，請參閱部署 vRealize Log Insight 虛擬應用裝置。
- 確認您正在使用受支援的瀏覽器。請參閱最低需求。

- 確認您具有有效授權金鑰。您可以透過 My VMware™ (https://my.vmware.com/) 上的帳戶，要求取得評估授權金鑰或永久授權金鑰。
- 如果您想要使用本機、vCenter Server 或 Active Directory 認證整合 vRealize Log Insight 與 vRealize Operations Manager，請確認已在 vRealize Operations Manager 自訂使用者介面匯入這些使用者。如需有關如何設定 LDAP 的指示，請參閱 vRealize Operations Manager 說明文件。

程序

1 使用支援的瀏覽器導覽到 vRealize Log Insight 的 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。

初始組態精靈隨即開啟。

2 按一下**開始新的部署**。

3 設定 Admin 使用者的密碼，然後按一下**儲存並繼續**。

您可以提供 Admin 使用者的電子郵件地址。

4 輸入授權金鑰，按一下**新增授權金鑰**，然後按一下**儲存並繼續**。

5 在 [一般組態] 頁面上，輸入用來從 vRealize Log Insight 接收系統通知的電子郵件地址。

6 如果您要使用 Webhook 將通知傳送至 vRealize Operations Manager 或第三方應用程式，請在**將 HTTP Post 系統通知傳送至**文字方塊中輸入以空格分隔的 URL 清單。

7 (選擇性) 若要退出客戶經驗改進計劃，請取消選取**加入 VMware 客戶經驗改進計劃**選項。按一下**儲存並繼續**。

8 在 [時間組態] 頁面上，設定在 vRealize Log Insight 虛擬應用裝置上同步時間的方式，然後按一下**測試**。

選項	說明
NTP 伺服器 (建議)	依預設，vRealize Log Insight 設定為將時間與公用 NTP 伺服器同步。如果由於防火牆設定而無法存取外部 NTP 伺服器，則您可以使用組織的內部 NTP 伺服器。 使用逗點分隔多個 NTP 伺服器。
ESX/ESXi 主機	如果沒有可用的 NTP 伺服器，您可以將時間與已部署 vRealize Log Insight 虛擬應用裝置的 ESXi 主機同步。

9 按一下**儲存並繼續**。

10 (選擇性) 若要啟用傳出警示和系統通知電子郵件，請指定 SMTP 伺服器的內容。

若要驗證 SMTP 組態是否正確，請輸入有效的電子郵件地址，然後按一下**測試**。vRealize Log Insight 會將一封測試電子郵件傳送到您提供的地址。

11 (選擇性) 若要提供自訂 SSL 憑證，請以 PEM 格式將憑證檔案上傳至叢集。您也可以檢視現有憑證的詳細資料。

系統會將憑證新增至叢集中所有節點的信任存放區，並加以儲存以供日後使用。

如需自訂 SSL 憑證之必要條件的相關資訊，請參閱安裝自訂 SSL 憑證。

12 按一下**儲存並繼續**。

結果

vRealize Log Insight 程序重新啟動後，系統會將您重新導向至 vRealize Log Insight 的**儀表板**索引標籤。

後續步驟

- 導覽至**管理**索引標籤。從 **vSphere 整合**頁面中，將 vRealize Log Insight 設定為從 vCenter Server 執行個體提取工作、事件和警示，並將 ESXi 主機設定為將 Syslog 摘要傳送至 vRealize Log Insight。
- 將永久授權指派給 vRealize Log Insight。請參閱《管理 vRealize Log Insight》中的將永久授權指派給 Log Insight。
- 在 vRealize Operations Manager 中設定 vRealize Log Insight 介面卡，以啟用在環境定義中啟動。請參閱《vRealize Operations Manager 組態指南》中的〈使用 vRealize Operations Manager 設定 vRealize Log Insight〉。
- 安裝 vRealize Log Insight Windows 代理程式以從 Windows 事件通道、Windows 目錄和一般文字記錄檔收集事件。請參閱《使用 vRealize Log Insight 代理程式》中的安裝 Windows 代理程式。

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。

客戶經驗改進計劃

4

本產品參與 VMware 客戶經驗改進計劃 (CEIP)。

有關透過 CEIP 收集之資料的詳細資訊，以及 VMware 使用這些資料的目的，都將於信任與保證中心內闡述，網址：https://www.vmware.com/solutions/trustvmware/ceip.html。

若要參加或離開此產品的 CEIP，請參閱 管理 vRealize Log Insight 中的〈參加或離開 VMware 客戶經驗計劃〉。