

使用 vRealize Log Insight

2018 年 9 月 20 日

vRealize Log Insight 4.7



vmware®

您可以在 VMware 網站上找到最新的技術說明文件，網址為：

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

如果您對此文件有何想法，請將您的回應意見提交至：

docfeedback@vmware.com

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

Copyright © 2014–2018 VMware, Inc. 版權所有。 [版權和商標資訊](#)。

內容

vRealize Log Insight 4

1 使用 vRealize Log Insight 功能 5

[vRealize Log Insight Web 使用者介面概觀 7](#)

[搜尋和篩選記錄事件 7](#)

[使用互動式分析圖表分析記錄 18](#)

[動態欄位擷取 21](#)

[管理搜尋查詢 25](#)

[使用儀表板 28](#)

[使用內容套件 34](#)

[建立內容套件 39](#)

[vRealize Log Insight 中的警示查詢 49](#)

vRealize Log Insight

使用 *vRealize Log Insight* 主題提供有關使用 Web 使用者介面的資訊，其中包括下列程序：篩選和搜尋記錄訊息、執行分析與視覺化搜尋結果、使用警示查詢，以及以自訂查詢為基礎從記錄訊息動態擷取欄位。

本資訊主要提供給 vRealize Log Insight 的使用者使用。

使用 vRealize Log Insight 功能

vRealize Log Insight 可為 vCloud Suite 提供可擴充的記錄匯總與索引，其中包括具備近乎即時搜尋及分析功能的 vSphere 所有版本。

vRealize Log Insight 可收集、匯入以及分析記錄，以便針對與系統、服務以及應用程式相關的問題提供回答，並獲得重要見解。

高效能擷取

vRealize Log Insight 可以處理由記錄或機器產生的任何類型資料。其支援高輸送量速度和低延遲，並可透過 syslog 和擷取 API 接受資料。

擴充性

vRealize Log Insight 可以使用多個虛擬應用裝置執行個體來進行擴充。這能讓您線性擴充擷取輸送量、增進查詢效能，以及實現擷取的高可用性。在叢集模式下，vRealize Log Insight 會提供主節點和工作節點。主節點和工作節點負責資料子集。主節點和查詢節點可以查詢資料的所有子集，並彙總結果。

近乎即時的搜尋

可在數秒內搜尋 vRealize Log Insight 所擷取的資料。此外，可從具有相同低延遲的相同介面搜尋歷史資料。

vRealize Log Insight 可支援完整關鍵字查詢。關鍵字被定義為任意英數字元、連字號或底線字元。除完整關鍵字查詢之外，vRealize Log Insight 支援 Glob 查詢 (例如：erro? 或 vm*) 及以欄位為基礎的篩選 (例如：主機名稱與測試不相符*、IP 包含「10.64」)。此外，包含數值的記錄訊息欄位可用於定義選擇篩選器 (例如：CPU>80、10<執行緒<100 等)。

搜尋結果顯示為個別事件。每個事件都來自於單一來源，但是搜尋結果可能來自多個來源。您可以使用 vRealize Log Insight 相互關聯一或多個維度 (例如：時間和要求識別碼) 上的資料，從而提供整個堆疊的連貫視圖。透過此方式，根本原因分析會變得更為簡單。

Windows 和 Linux 代理程式

vRealize Log Insight 所含的代理程式會收集 Linux 和 Windows 機器上的事件和檔案。

智慧分組

vRealize Log Insight 使用一種新的機器學習技術。智慧分組可掃描傳入的非結構化資料，並根據問題類型將訊息分組歸類，以便您可以快速瞭解可能會跨越實體、虛擬以及混合雲環境的問題。

彙總

擷取自記錄資料的欄位可以用於彙總。這與 **GROUP-BY** 查詢在關聯式資料庫或 **Microsoft Excel** 的樞紐分析表中所提供的功能類似。不同之處在於：無需擷取、轉換以及載入 (ETL) 程序，並且

vRealize Log Insight 可擴充為任意的資料大小。

您可以產生資料的彙總視圖，並識別特定事件或錯誤，而不需存取多個系統和應用程式。例如，檢視重要的系統度量時，例如每分鐘錯誤的數目，您可以向下切入到特定時間範圍的事件，並檢查該環境中出現的錯誤。

執行階段欄位擷取

原始記錄資料並不是始終易於理解，您可能需要處理部分資料以識別對搜尋和彙總重要的欄位。

vRealize Log Insight 提供了執行階段欄位擷取來解決此問題。您可以透過提供規則運算式從資料中動態擷取任意欄位。擷取的欄位可用於選擇、投影和彙總，這與解析時所擷取之欄位的使用方式類似。

儀表板

您可以建立您想要密切監控之有用度量的儀表板。任何查詢都可以轉化為儀表板 **Widget**，並可在任意時間範圍內進行摘要。您可以選擇您系統在過去五分鐘、上一個小時或昨天的效能。您可以按小時檢視錯誤的明細，並觀察記錄事件中的趨勢。

安全性考量

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。

本章節討論下列主題：

- [vRealize Log Insight Web 使用者介面概觀](#)
- [搜尋和篩選記錄事件](#)
- [使用互動式分析圖表分析記錄](#)
- [動態欄位擷取](#)
- [管理搜尋查詢](#)
- [使用儀表板](#)

- [使用內容套件](#)
- [建立內容套件](#)
- [vRealize Log Insight 中的警示查詢](#)

vRealize Log Insight Web 使用者介面概觀

您可以存取的功能取決於用來登入 vRealize Log Insight Web 使用者介面的使用者帳戶。

儀表板索引標籤

儀表板索引標籤包含自訂儀表板和內容套件儀表板。在**儀表板**索引標籤上，您可以檢視環境中的記錄事件圖，或建立自訂的 Widget 集來存取對您最重要的資訊。

互動式分析索引標籤

在**互動式分析**索引標籤上，您可以搜尋和篩選記錄事件，並建立查詢來根據記錄事件中的時間戳記、文字、來源和欄位擷取事件。vRealize Log Insight 會顯示查詢結果圖。您可以儲存這些圖表，以便稍後在**儀表板**索引標籤上進行查閱。

內容套件

內容套件包含與特定產品或記錄集相關的儀表板、擷取之欄位、儲存之查詢和警示。您可以從 vRealize Log Insight Web 使用者介面右上方的下拉式功能表存取內容套件。

內容套件可由 vRealize Log Insight 使用者匯入或建立。請參閱 [使用內容套件](#)。

管理使用者介面

vRealize Log Insight 管理員可以管理使用者帳戶、設定儲存位置和封存、設定電子郵件通知的外寄 SMTP 伺服器，以及變更數項其他參數。管理 UI 的 URL 格式為 `https://log_insight-host/admin/`，其中 `log_insight-host` 是 vRealize Log Insight 虛擬應用裝置的 IP 位址或主機名稱。

搜尋和篩選記錄事件

您可以在**互動式分析**索引標籤上搜尋和篩選記錄事件。

您可以在搜尋文字方塊中輸入任何完整的關鍵字、glob 或片語，然後按一下**搜尋**來僅尋找包含指定關鍵字的事件。

您可以在 Web 使用者介面中的**儀表板**或**互動式分析**頁面中指定時間範圍。時間範圍在篩選時是內含的。

您可以搜尋符合特定欄位之特定值的記錄事件。在主搜尋欄位中使用引文將比對精確片語。在主搜尋欄位中輸入空格代表邏輯 AND 運算子。搜尋將僅使用完整 Token：搜尋「err」時不會找到「error」做為相符項。

您可以透過使用下拉式功能表和記錄事件清單上方的文字方塊來指定欄位搜尋準則 (或篩選器)。

在單資料列篩選器中，您可以使用逗點分隔的值來列出 **OR** 篩選器。例如，選取**主機名稱包含**並輸入 **127.0.0.1**，**127.0.0.2**。搜尋會傳回含有主機名稱 **127.0.0.1** 或 **127.0.0.2** 的事件。

備註 文字**包含**篩選器將每個以逗點分隔的值都視為一個完整的關鍵字。

具有使用內部查詢語言語法名稱 (例如，**from** 或 **in**) 之欄位的查詢均無法處理且不應使用。

透過為每個欄位建立一個新的篩選器資料列，您可以合併多個欄位篩選器。您可以切換套用至多資料列篩選器的運算子。

- 選取**全部**套用 **AND** 運算子。
- 選取**任何**套用 **OR** 運算子。

備註 無論切換值為何，單一篩選器資料列內以逗點分隔的值的運算子始終是 **OR**。

您可以在搜尋詞彙中使用 **glob**。例如，**vm*** 或 **vmw?re**。

- 使用 ***** 表示 0 個或更多字元
- 使用 **?** 表示一個字元。

備註 **glob** 不得用作搜尋詞彙的第一個字元。例如，您可以在篩選查詢中使用 **192.168.0.***，但不可使用 ***.168.0.0**。

事件類型分組

Log Insight 會使用機器學習來將類似事件歸為同一組。事件類型分組可以使疑難排解及根本原因分析更簡單。

在 Log Insight 中執行查詢時，結果數取決於查詢及時間範圍。查詢通常會傳回大量結果。機器學習會從 Log Insight 即將發生的事件中動態學習和調整模式。

事件類型索引標籤位於 [互動式分析] 頁面的搜尋列下方。按一下**事件類型**索引標籤後，您會看到已歸為同一組之類似事件的清單。

機器學習將分析事件並探索類似記錄訊息所包含的欄位類型。例如，這些類型可以是時間戳記、字串、**int**、十六進位及其他。這些探索到的類型將顯示為**事件類型**清單內的超連結。

機器學習探索到的每個類型表示一種新類型的欄位，稱為智慧欄位。智慧欄位的預設名稱遵循以下格式：**智慧欄位 - 類型 編號 [event_type]**。您可以變更智慧欄位的預設名稱。命名智慧欄位之後，它將如同其他欄位一樣，顯示在 [欄位] 區段下方。您可以重新命名或刪除智慧欄位，但不能修改其定義。

機器學習引進了新的靜態欄位，稱為 **event_type**。您可以將 **event_type** 用作篩選器，以在查詢中包括或從查詢中排除某些事件類型。

記錄事件中的資訊

vRealize Log Insight 可收集和分析機器產生的所有類型的記錄資料，包括應用程式記錄、網路追蹤、組態檔、訊息、效能資料及系統狀態傾印。

您可以將 vRealize Log Insight 與環境中的各項資源 (包括作業系統、應用程式、儲存區、防火牆、網路裝置) 連在一起，從而透過使用記錄分析實現企業級可見度。

已設定 vRealize Log Insight 並開始收集記錄時，您可以使用數種方式來擷取記錄資料，其中包括：

- **vSphere 整合** - vRealize Log Insight 可與 vSphere 整合，以自動從 vCenter Server 擷取事件以及從 ESXi 主機擷取記錄。
- **vRealize Operations Manager 整合** - vRealize Log Insight 可與 vRealize Operations Manager 整合，以在 vRealize Operations Manager 中啟用各種警示來傳送通知事件，並向管理員傳送電子郵件。
- **代理程式** - vRealize Log Insight 提供收集代理程式，可將檔案和事件記錄從 Linux 或 Windows 傳送到 vRealize Log Insight。
- **Syslog** - vRealize Log Insight 可透過 Syslog 從任何來源擷取資料。只需要將 vRealize Log Insight 伺服器設定為您的 Syslog 目的地。
- **Syslogd** —
- **CFAPI** - 事件以其原始格式傳送至 vRealize Log Insight (使用 cfapi)。透過 cfapi 傳送的事件不必遵循 Syslog 事件的準則，且不會加以修改以遵守 Syslog RFC。

每個事件均包含下列資訊。

類型	說明
時間戳記	事件發生的時間
來源	事件的來源。可以是 Syslog 訊息的建立者 (如 ESXi 主機) 或轉送站 (如 Syslog 彙總)。
Text	事件的原始文字。
欄位	從事件擷取的名稱值對。只有在代理程式使用 CFAPI 通訊協定時，才能將欄位傳遞至伺服器做為靜態欄位。

備註 vRealize Log Insight 不對來自其他 VMware 產品的記錄訊息內容負責。如果您對記錄內容有疑問，請連絡產生記錄訊息的產品團隊。

依時間範圍篩選記錄事件

您可以篩選記錄事件，以僅檢視特定期間的事件。

您可以在 Web 使用者介面中的儀表板或互動式分析頁面中指定時間範圍。時間範圍在篩選時是內含的。

先決條件

確認您已登入 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 從搜尋按鈕左側的下拉式功能表中，選取一個預先定義期間。

- 2 (選擇性) 若要設定時間範圍的起始點和最終點，請選取**自訂時間範圍**。

搜尋包含完整關鍵字的記錄事件

您可以搜尋包含完整關鍵字的記錄事件。關鍵字包含英數、連字號和底線字元。

先決條件

確認您已登入 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**互動式分析**索引標籤。
- 2 在搜尋文字方塊中，輸入您想要在記錄事件中搜尋的完整關鍵字，然後按一下**搜尋**按鈕。

包含指定完整關鍵字的記錄事件隨即出現在清單中。

您搜尋的字串會以黃色反白顯示。

下一個

您可以儲存目前查詢以在稍後進行載入。

依欄位運算搜尋記錄事件

您可以使用現有欄位清單來搜尋具有特定欄位值的記錄事件。

重要事項 vRealize Log Insight 針對完整、英數、連字號及底線字元建立索引。

先決條件

確認您已登入 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**互動式分析**索引標籤。
- 2 按一下**新增篩選器**。

- 3 在搜尋文字方塊下方的篩選器列中，使用第一個下拉式功能表來選取在 vRealize Log Insight 內定義的任何欄位。

例如，**主機名稱**。

清單包含在內容套件和自訂內容中靜態可用的所有已定義欄位。欄位按名稱排序，**文字**欄位除外。因為**文字**是參照訊息文字的特殊欄位，**文字**顯示在清單頂部，預設為選取狀態。

備註 數字欄位包含字串欄位中沒有的其他運算子：**=**、**>**、**<**、**>=** 和 **<=**。這些運算子可執行數字比較，並且使用它們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。

- 4 在搜尋文字方塊下方的篩選器列中，使用第二個下拉式功能表來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。

例如，選取**包含**。**包含**篩選器會比對完整 Token：搜尋「err」時不會找到「error」做為相符項。

- 5 在篩選器下拉式功能表右側的文字方塊中，輸入要用作篩選器的值。

您可以列出多個值，並以逗點分隔。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，則文字方塊無法使用。

- 6 (選擇性) 若要新增更多篩選器，請按一下**新增篩選器**。

切換按鈕顯示在篩選器列上方。

- 7 (選擇性) 對於多個篩選器列，請選取篩選器之間的運算子。

選項	說明
全部	選取以在篩選器列之間套用 AND 運算
任何	選取以在篩選器列之間套用 OR 運算

預設為選取**全部**。

- 8 按一下**搜尋**按鈕。

範例 1-1. 搜尋其名稱包含常用字串的主機群組

假定您有多部主機，其中一部主機的名稱為 **w1-stvc-205-prod3**，另有一部主機名為 **w1-stvc-206-prod5**。

若要找到這兩部主機的所有記錄，請建立下列查詢。

- 1 將搜尋文字方塊保留為空白。
- 2 定義篩選器。
 - a 從欄位下拉式功能表中選取**主機名稱**。
 - b 從運算子下拉式功能表選取**開頭為**。

c 在值文字方塊中輸入 **w1-stvc**。

或者，您可以使用**包含**運算子，但是接下來您必須在搜尋值中使用 **glob**。在此範例中，您必須在值文字方塊中輸入 **w1-stvc-***。

3 按一下**搜尋**按鈕。

下一個

您可以儲存目前查詢以在稍後進行載入。

搜尋在某事件前後或左右發生的事件


您可以搜尋記錄事件清單，找到在清單中某事件前後及左右發生的事件。

如果您想要進一步瞭解事件發生前後的環境狀態，您可以檢查周圍事件。

先決條件

確認您已登入 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 在**互動式分析**索引標籤上，找到清單中的事件。
- 2 在事件列的左側，按一下 ，然後選取**設定此事件的時間範圍**。
- 3 在 [從事件設定時間範圍] 對話方塊中，使用下拉式功能表選取時間範圍的期間和方向。
您可以從預先定義期間 (1 秒到 10 分鐘) 的清單中選取。
- 4 按一下**設定範圍**。

圍繞所選事件發生的事件會顯示在清單中。

備註 此作業會清除之前指定的所有搜尋參數和篩選器。

檢視內容中的事件


您可以檢視記錄事件的內容，並瀏覽在其之前及之後到達的記錄事件。


如果您想要進一步瞭解事件發生前後的環境狀態，您可以檢查周圍事件。

先決條件

確認您已登入 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 在**互動式分析**索引標籤上，找到清單中的事件。
- 2 在事件列的左側，按一下 ，然後選取**檢視內容中的事件**。

- 3 (選擇性) 向上或向下捲動到視窗邊緣，以載入更多事件。
- 4 (選擇性) 按一下紫色的時間戳記，以捲動回到反白顯示的訊息。
- 5 (選擇性) 若要新增篩選器，請在頂部按一下**新增篩選器**，或按一下反白顯示之事件內的欄位。
- 6 (選擇性) 新增或移除特定的事件類型，方法是指向某個事件，並按一下 .

分析事件趨勢

您可以分析記錄事件來瞭解趨勢和異常。

先決條件

確認您已登入 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**互動式分析**索引標籤。
- 2 透過使用搜尋文字方塊以及套用篩選器來建構並執行查詢。
- 3 在 [從事件設定時間範圍] 對話方塊中，使用下拉式功能表選取時間範圍的期間和方向。
- 4 按一下**事件趨勢**索引標籤。

vRealize Log Insight 將您的查詢與之前同一期間的查詢進行比較，並顯示結果。

清除所有篩選規則

您可以清除篩選及搜尋結果以檢視所有記錄事件的清單。

針對事件清單執行搜尋後，搜尋結果會一直保留在畫面上，直到您清除所有查詢。

先決條件

確認您已登入 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 在**互動式分析**索引標籤上，移除所有篩選器。
- 2 如果搜尋文字方塊中顯示文字，請將其刪除。
- 3 按一下**搜尋**按鈕。

搜尋查詢的範例

在 vRealize Log Insight 的**互動式分析**索引標籤上建立查詢時，您可以使用這些範例。

範例 1-2. 查詢 ESX/ESXi hostd 程序於昨天 9-10am 之間報告的所有活動訊號事件

重要事項 vRealize Log Insight 針對完整、英數、連字號及底線字元建立索引。

查詢 ESX/ESXi hostd 程序報告的所有活動訊號事件：

- 1 在搜尋文字方塊中，輸入 **heartbeat***。
- 2 定義篩選器。
 - a 從第一個下拉式功能表中選取**應用程式名稱**。
 - b 從第二個下拉式功能表中選取**包含**。
 - c 在值文字方塊中輸入 **hostd**。
- 3 定義時間範圍。
 - a 在**時間範圍**下拉式功能表中，選取**自訂**。
 - b 在第一個文字方塊中，輸入昨天的日期和 **9am**。
 - c 在第二個文字方塊中，輸入昨天的日期和 **10am**。
- 4 按一下**搜尋**按鈕。

範例 1-3. 搜尋其名稱包含常用字串的主機群組

假定您有多部主機，其中一部主機的名稱為 **w1-stvc-205-prod3**，另有一部主機名為 **w1-stvc-206-prod5**。

若要找到這兩部主機的所有記錄，請建立下列查詢。

- 1 1. 將搜尋文字方塊保留為空白。
- 2 定義篩選器。
 - a 從欄位下拉式功能表中選取**主機名稱**。
 - b 從運算子下拉式功能表選取**開頭為**。
 - c 在值文字方塊中輸入 **w1-stvc**。

或者，您可以使用**包含**運算子，但是接下來您必須在搜尋值中使用 **glob**。在此範例中，您必須在值文字方塊中輸入 **w1-stvc-***。

- 3 按一下**搜尋**按鈕。

範例 1-4. 查詢 vCenter Server 工作、事件和警示報告的所有錯誤

查詢 vCenter Server 工作、事件和警示報告的所有錯誤：

- 1 在搜尋文字方塊中，輸入 **error**。
- 2 定義篩選器。
 - a 從第一個下拉式功能表中選取 **vc_event_type**。
 - b 從第二個下拉式功能表中選取**存在**運算子。
- 3 按一下**搜尋**按鈕。

範例 1-5. 查詢 ESX/ESXi 報告的超過一秒的 SCSI 延遲

查詢 ESX/ESXi 報告的超過一秒的 SCSI 延遲：

- 1 在搜尋文字方塊中，輸入 **scsi latency "performance has"**。
- 2 定義篩選器。
 - a 從第一個下拉式功能表中選取 **vmw_vob_component**。
 - b 從第二個下拉式功能表中選取**包含**運算子。
 - c 在文字方塊中輸入 **scsiCorrelator**。
- 3 定義第二個篩選器。
 - a 從第一個下拉式功能表中選取 **vmw_latency_in_micros**。
 - b 從第二個下拉式功能表中選取 **>** 運算子。
 - c 在文字方塊中輸入 **1000000**。
- 4 按一下**搜尋**按鈕。

規則運算式的範例

您可以在文字方塊中輸入欄位值的規則運算式，以從記錄事件中擷取欄位。

輸入的運算式必須使用 **Java** 規則運算式語法。

表格 1-1. 字元運算子

規則運算式	說明
\	逸出特殊字元
\b	字邊界
\B	非字邊界
\d	一個數字
\D	一個非數字
\n	換行
\r	換行字元
\s	一個空格
\S	空白之外的任何字元
\t	索引標籤
\w	一個英數字元或底線字元
\W	一個非英數字元或底線字元

例如，如果您有字串 **1234-5678** 並套用了下列規則運算式

規則運算式	結果
\d	1
\d+	1234
\w+	1234
\S	1234-5678

表格 1-2. 限定詞運算子

規則運算式	說明
.	換行之外的任何字元
*	零個或更多字元 (儘可能長)
?	零個或一個字元 (或者儘可能短)
+	一個或多個
{<n>}	恰好是 <n> 次
{<n>,<m>}	<n> 到 <m> 次

例如，如果您有字串 **aaaaa** 並套用了下列規則運算式

規則運算式	結果
.	a
*	aaaaa
.*?	aaaaa
.{1}	a
.{1,2}	aa

表格 1-3. 組合運算子

規則運算式	說明
.	所有字元
.*?	所有字元，長度儘可能像之前一樣短

例如，如果您有字串 **a b 3 hi d hi** 並套用了下列規則運算式

規則運算式	結果
a.* hi	b 3 hi d
a .*? hi	b 3

表格 1-4. 邏輯運算子

規則運算式	說明
^	行開頭或在括弧內則非
\$	行結尾
()	封裝

表格 1-4. 邏輯運算子 (繼續)

規則運算式	說明
[]	括弧內的一個字元
	或
-	範圍
\A	字串開頭
\Z	字串結尾

例如，如果套用下列規則運算式

規則運算式	結果
(hello)?	包含 hello 或不包含 hello
(a b c)	a 或 b 或 c
[a-cp]	a 或 b 或 c 或 p
world\$	結尾為 world，不跟隨任何內容

表格 1-5. Lookahead 運算子

規則運算式	說明
?=	正 lookahead (包含)
?!=	負 lookahead (不包含)

例如，如果套用下列規則運算式

規則運算式	結果
is (?=\\w+\\w{2}) primary	is FT primary? false
opid=(?!WFU-1fecf8f9)\\S+	WFU-3c9bb994

表格 1-6. 其他規則運算式範例

規則運算式	說明
[xyz]	x、y 或 z
(info warn error)	info、warn 或 error
[a-z]	一個小寫字母
[^a-z]	非一個小寫字母
[a-z]+	一個或多個小寫字母
[a-z]*	零個或多個小寫字母
[a-z]?	零個或一個小寫字母
[a-z]{3}	恰好是三個小寫字母
[d]	一個數字
\\d+\$	一個或多個數字，後面跟隨訊息結尾
[0-5]	0 到 5 的其中一個數字

表格 1-6. 其他規則運算式範例 (繼續)

規則運算式	說明
\w	文字字元 (字母、數字或底線)
\s	空白
\S	空白之外的任何字元
[a-zA-Z0-9]+	一個或多個英數字元
([a-z] {2,} [0-9] {3,5})	兩個或多個字母，後面跟隨 3 到 5 個數字

使用互動式分析圖表分析記錄

互動式分析 頁面頂部的圖表可讓您針對查詢結果執行視覺化分析。

圖表代表了記錄搜尋查詢的圖形快照。您可以使用圖表下方的下拉式功能表來變更圖表類型。

您可以使用左側第一個下拉式功能表來控制圖表的彙總層級。依預設選取**計數**函數。

圖表類型

您可以選取不同的圖表類型，以變更資料在 **[互動式分析]** 頁面上視覺化的方式。

不同的圖表類型需要不同的彙總函數、分組依據欄位以及是否使用時間序列。圖表中最多可顯示 **2,000** 個最近的結果。

圖表類型	彙總函數	時間序列需求	分組依據欄位需求
直條圖	任何	時間序列	N/A
折線圖	任何	時間序列	N/A
區域圖	任何	時間序列	N/A
橫條圖	任何	非時間序列	至少一個欄位
圓形圖	計數或唯一計數	非時間序列	至少一個欄位
泡泡圖	任何	非時間序列	兩個欄位
量測計	計數	非時間序列	N/A
純量	計數	非時間序列	N/A
資料表	任何	任何	N/A

多功能圖表

您可以使用多功能圖表來比較不同範圍的變數。

如果想要比較不同類別的資料集，則可以使用多功能圖表為每個系列指派 **Y** 軸或 **X** 軸。每個軸均可放置於圖表的右側或左側。您可以交換功能，以便將其繪製時所在的 **Y** 軸左右互換。

例如，除按通道及層級分組之工作平均數以外，您可以繪製按通道及層級分組之事件計數的圖表。

彙總函數

vRealize Log Insight 提供多個彙總函數。

類型	欄位	說明
計數	僅事件	為特定查詢建立一個事件數目圖表。
唯一計數	任意欄位	為欄位建立一個唯一值的數目圖表。
下限	僅數字欄位	為欄位建立一個最小值圖表。
上限	僅數字欄位	為欄位建立一個最大值圖表。
平均值	僅數字欄位	為欄位建立一個平均值圖表。
標準差	僅數字欄位	為欄位值建立一個標準差圖表。
總計	僅數字欄位	為欄位建立一個值的總計圖表。
差異	僅數字欄位	為欄位值之間的差異建立圖表。

您可以修改檢視查詢結果的方式。

檢視	說明
依特定欄位值分組查詢結果	使用圖表下方的第二個下拉式功能表，依特定欄位值而非時間序列 (或加上時間序列) 來分組查詢結果。
檢視欄位的事件數	例如，每台主機的事件數，取消選取 事件序列 核取方塊，然後選取該欄位對應的核取方塊。
檢視針對隨時間變化的群組的堆疊橫條圖	選取 事件序列 核取方塊和該欄位核取方塊。

使用圖表

您可以變更圖表在**互動式分析**索引標籤上的外觀、將圖表新增至您的自訂儀表板，並管理儀表板圖表。

工作	程序
變更圖表的時間範圍	在 互動式分析 索引標籤上，使用 搜尋 按鈕左側的下拉式功能表來切換圖表中顯示的期間。
變更圖表的資料粒度	在 互動式分析 索引標籤上，使用右上方的按鈕，來切換圖表上呈現之各個點的不同時間範圍。可用的範圍取決於針對查詢指定的時間範圍。
在 互動式分析 索引標籤上載入儀表板圖表	在 儀表板 索引標籤上，找到圖表，按一下 在互動式分析中開啟圖示  。 時間範圍會設定為儀表板目前的時間範圍。您可以視需要修改此時間範圍。
將圖表儲存到自訂儀表板	<ol style="list-style-type: none"> 在互動式分析索引標籤的左上方，按一下新增到儀表板。或者，從搜尋按鈕右側的功能表中，選取將目前查詢新增到儀表板。 輸入一個名稱，從下拉式功能表中選取目的地儀表板，然後選取 Widget 類型，接著新增此 Widget 的相關資訊並按一下新增。
將查詢做為圖表儲存到自訂儀表板	<ol style="list-style-type: none"> 按一下搜尋按鈕旁的將目前查詢新增到儀表板。 輸入名稱，從下拉式功能表中選取目的地儀表板，確定 Widget 類型已設定為圖表，新增 Widget 的相關資訊，然後按一下新增。

工作	程序
將查詢做為欄位資料表儲存到自訂儀表板	<ol style="list-style-type: none"> 按一下搜尋按鈕旁的將目前查詢新增到儀表板。 輸入名稱，從下拉式功能表中選取目的地儀表板，確定 Widget 類型已設定為欄位資料表，新增 Widget 的相關資訊，然後按一下新增。
從自訂儀表板刪除 Widget	<ol style="list-style-type: none"> 在儀表板索引標籤上，選取包含要刪除 Widget 的自訂儀表板。 在 Widget 右上角，按一下其他動作圖示 ，並選取刪除。 在 [刪除 Widget] 對話方塊中，按一下刪除以確認。

變更互動式分析圖表的類型

您可以變更圖表中顯示的查詢結果的彙總和群組，透過圖形方式分析記錄事件。

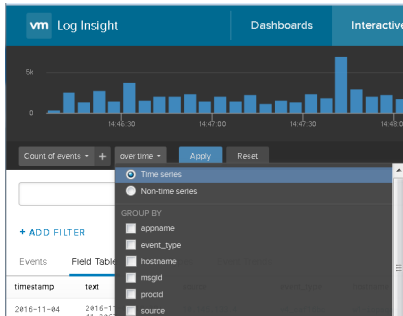
您可在圖表下方看到的下拉式功能表的數目取決於所選的彙總函數。

先決條件

確認您已登入 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

- 使用 [互動式分析] 圖表下方的下拉式功能表來變更彙總函數和群組類型。



- 若要檢視隨著時間變更的事件數，請選取**時間序列**按鈕。
- 若只要檢視事件值，請選取**非時間序列**按鈕，並至少選取一個欄位。

- 按一下**更新**。

範例 1-6. 互動式分析圖表中的彙總和群組

下表包含用於說明 vRealize Log Insight 圖表中的彙總和群組的範例。

表格 1-7. 互動式分析圖表中的彙總和群組範例

第一個下拉式功能表中的選擇	第二個下拉式功能表中的選擇	時間序列選擇	顯示在畫面上的文字	結果
計數	時間序列	時間序列	隨著時間變更的事件計數	該圖表顯示隨著時間變更的目前查詢的事件數之橫條圖。
平均值	vmw_op_latency (VMware - vSphere)	時間序列	隨著時間變更的 vmw_op_latency (VMware - vSphere) 平均值	該圖表顯示隨著時間變更的作業延遲平均值之折線圖。
計數	vmw_esx_problem <small>備註 依預設，不會顯示 vmw_esx_problem 欄位。您必須擷取 vmw_esx_problem 欄位並儲存查詢，以使 vmw_esx_problem 顯示在下拉式功能表中。</small>	非時間序列	依 vmw_esx_problem 分組的事件計數	該圖表顯示包含 vmw_esx_problem 欄位的事件數之橫條圖。
計數	時間序列、vmw_esx_problem	時間序列	隨著時間變更的依 vmw_esx_problem 分組的事件計數	該圖表顯示隨著時間變更的依 vmw_esx_problem 分組的堆疊橫條圖。

動態欄位擷取

在含大量記錄事件的大型環境中，您無法始終找到對您重要的資料欄位。

vRealize Log Insight 提供了執行階段欄位擷取來解決此問題。您可以透過提供規則運算式從資料中動態擷取任何欄位。請參閱[規則運算式的範例](#)。

備註 一般查詢的速度可能會非常慢。例如，如果您嘗試使用 `\(d+\)` 運算式來擷取欄位，查詢會傳回所有括弧中包含數字的記錄事件。確認您的查詢包含儘可能多的文字內容。例如，較好的欄位擷取查詢是 `Event for vm\(d+\)`。

您可以使用擷取的欄位來搜尋和篩選記錄事件清單，或在 [\[互動式分析\]](#) 圖表中彙總事件。

使用單鍵擷取來擷取欄位

除了輸入內容值來動態擷取欄位，您可以改用單鍵擷取功能。

單鍵擷取功能會填入與您在記錄事件中選取的欄位對應的所有內容值。

備註 單鍵擷取選項僅在 [\[事件\]](#) 索引標籤中提供。

先決條件

確認您已登入 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**互動式分析**索引標籤。

2 在記錄事件清單中，反白顯示代表您要擷取之欄位的文字。

動作功能表隨即出現在該事件存在的欄位名稱集上方。

3 按一下**擷取欄位**。

[欄位] 窗格中的預先內容值和內容值後會自動使用擷取反白顯示之欄位所需的內容填入。

4 (選擇性) 修改 [欄位] 窗格中的 [擷取的值] 規則運算式。

5 (選擇性) 修改 [欄位] 窗格中的 [內容前後] 規則運算式。

6 (選擇性) 按一下 **+** **新增其他內容** 以新增更多的關鍵字和篩選器。

您可以新增一或多個關鍵字並使用單一靜態欄位做為篩選器。

7 如果您是管理員使用者，請選取哪些使用者可以存取下拉式功能表中的欄位。

選項	說明
所有使用者	所有使用者都將會看到其事件和篩選器下拉式功能表中的欄位。
只有我	僅欄位的建立者可以看到其事件和篩選器下拉式功能表中的欄位。

8 (選擇性) 在 [欄位] 窗格上方，按一下 **i**，然後按一下**編輯**以將附註新增至此欄位。在**編輯附註**視窗中新增附註，然後按一下**確定**。

9 按一下**儲存**。

下一個

您可以使用擷取的欄位來搜尋和篩選記錄事件清單，或在 [互動式分析] 圖表中彙總事件。

您可以修改儲存的欄位定義或者在不需要時將其刪除。

修改擷取的欄位

您可以修改擷取的欄位之定義。

vRealize Log Insight 會為您在建立圖表、查詢或警示時使用的欄位建立複本。如果您修改欄位定義，使用該修改欄位的所有圖表、查詢和警示會隨之更新，以反映新定義。

一般使用者僅可以修改自己的內容。管理員使用者可以修改自己的內容及其共用內容。

內容套件欄位為唯讀。

先決條件

確認您已登入 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**互動式分析**索引標籤。

2 在 [欄位] 窗格的頂部，按一下**管理擷取的欄位** ，然後從清單中選取擷取的欄位。

3 修改值，然後按一下**更新**。

隨即出現對話方塊，顯示將受到更新欄位影響的內容清單。如果欄位在多個使用者之間共用，此對話方塊也會顯示受影響使用者的清單。

4 (選擇性) 在 [欄位] 窗格上方，按一下 **i**，然後按一下**編輯**以將附註新增至此欄位。在**編輯附註**視窗中新增附註，然後按一下**確定**。

5 按一下**更新**確認變更。

vRealize Log Insight 會更新使用您所修改之欄位的所有查詢、警示和圖表。

篩選擷取欄位的內容套件

您可以指定要從中擷取欄位的內容套件。這可以避免擷取不必要的欄位並提高效率。

您可以在 [互動式分析] 頁面上，從 [內容套件] 下拉式功能表選取內容套件。

複製擷取的欄位

您可以複製擷取的欄位。

當您想要從事件中擷取多個欄位時，請使用 [複製] 選項，此時兩個欄位會顯示在相似內容中。擷取欄位並儲存後，開啟已擷取欄位的定義並使用 [複製] 選項。重複欄位的定義與原始擷取欄位的定義完全相同。可以修改重複欄位的定義，以與您感興趣事件中的其他值相符。

一般使用者僅可以複製自己的內容。管理員使用者可以修改自己的內容及其共用內容。

先決條件

確認您已登入 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**互動式分析**索引標籤。

2 在 [欄位] 窗格的頂部，按一下**管理擷取的欄位** ，然後從清單中選取擷取的欄位。

3 按一下**複製**，建立欄位複本。

4 (選擇性) 修改 [欄位] 窗格中的 [擷取的值] 規則運算式。

5 (選擇性) 修改 [欄位] 窗格中的 [內容前後] 規則運算式。

6 (選擇性) 按一下 **+** **新增其他內容**以新增更多的關鍵字和篩選器。

您可以新增一或多個關鍵字並使用單一靜態欄位做為篩選器。

- 7 如果您是管理員使用者，請選取哪些使用者可以存取下拉式功能表中的欄位。

選項	說明
所有使用者	所有使用者都將會看到其事件和篩選器下拉式功能表中的欄位。
只有我	僅欄位的建立者可以看到其事件和篩選器下拉式功能表中的欄位。

- 8 按一下**儲存**。

下一個


您可以使用擷取的欄位來搜尋和篩選記錄事件清單，或在 [互動式分析] 圖表中彙總事件。

您可以修改儲存的欄位定義或者在不需要時將其刪除。

刪除擷取的欄位

您可以刪除不再需要之擷取的欄位。

vRealize Log Insight 會為您在建立 Widget、查詢或警示時使用的欄位建立複本。如果刪除用於 Widget、查詢或警示的欄位，則 vRealize Log Insight 為每個使用該欄位的 Widget、查詢或警示建立已刪除欄位的暫存複本。



您只能刪除名稱旁邊有**編輯此欄位**圖示  的欄位。一般使用者僅可以刪除自己的內容。管理員使用者可以刪除自己的內容及其共用內容。

內容套件欄位為唯讀。

先決條件

確認您已登入 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**互動式分析**索引標籤。
- 2 在 [欄位] 窗格頂部，按一下**管理擷取的欄位** ，然後將游標暫留在清單中的已擷取欄位上。
- 3 按一下 。
對話方塊會顯示使用您想要刪除之欄位的內容清單。如果您是管理員使用者且欄位由多個使用者共用，則對話方塊也會顯示受影響使用者的清單。
- 4 按一下**刪除**確認。

如果現有查詢中使用已刪除欄位，當您載入使用該已刪除欄位的查詢時，vRealize Log Insight 會建立欄位的暫存複本並顯示。

如果匯出內容包含暫存欄位，則 vRealize Log Insight 會在匯出的內容套件中建立欄位以避免使用暫存欄位。

管理搜尋查詢

您可以匯出查詢結果並與其他使用者共用您的查詢，還可以儲存、刪除、重新命名和載入現有的查詢。您可以建立查詢的快照，並將這些快照儲存到儀表板。


在 vRealize Log Insight 中儲存查詢

您可以在 vRealize Log Insight 中儲存目前查詢和時間範圍，以供稍後檢視。僅可從[互動式分析](#)頁面載入已儲存查詢。

先決條件

確認您已登入 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 在[互動式分析](#)索引標籤上，執行要儲存的查詢。
- 2 按一下，選取將目前查詢新增到我的最愛圖示 .
- 3 輸入名稱，然後按一下儲存。

備註 已儲存查詢包含固定時間範圍，且不會進行更新。透過儲存查詢，您可以在儲存時建立該時間範圍內提供之記錄訊息的快照。

查詢會新增至 [最常用查詢] 清單。

包括管理員在內的所有使用者都擁有已儲存查詢的個別清單。



在 vRealize Log Insight 中重新命名查詢

您可以變更已儲存在 vRealize Log Insight 中的查詢名稱。

先決條件

確認您已登入 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[互動式分析](#)索引標籤。
- 2 按一下 [最常用查詢] 圖示 .
- 3 指向要重新命名的查詢，然後按一下編輯此儲存查詢圖示 .
- 4 輸入新的名稱，然後按一下儲存。

在 vRealize Log Insight 中載入查詢

您可以從內容套件載入查詢或載入已儲存的查詢，以在 **互動式分析** 索引標籤上檢視。


已儲存查詢與儀表板項目是分隔的。這些查詢不會出現在任何自訂儀表板上。如果您想要檢視已儲存查詢，就必須載入它。

包括管理員在內的所有使用者都擁有已儲存查詢的個別清單。

先決條件

確認您已登入 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 **互動式分析** 索引標籤。
- 2 按一下 [最常用查詢] 圖示 .
- 3 在 [最常用查詢] 清單中，按一下要在 **互動式分析** 索引標籤上檢視的查詢。
查詢隨即會載入到 **互動式分析** 索引標籤上。查詢的時間範圍會顯示在事件清單上方。

下一個

您可以將查詢新增到儀表板、變更圖表的資料粒度，或將其他篩選套用到查詢結果。



從 vRealize Log Insight 刪除查詢

您可以從 vRealize Log Insight 刪除已儲存的查詢。

先決條件

確認您已登入 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 **互動式分析** 索引標籤。
- 2 從 **搜尋** 按鈕右側的下拉式功能表中，選取 **載入查詢**。
- 3 按一下 [最常用查詢] 圖示 .
- 4 在 [最常用查詢] 清單中，按一下您想要刪除之查詢旁的 .
- 5 按一下 **刪除** 確認。


共用目前查詢

您可以向同事傳送目前查詢的連結。

先決條件

確認您已登入 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 在**互動式分析**索引標籤上，執行要共用的查詢。
- 2 按一下  並選取**共用查詢**。
vRealize Log Insight 會建立並顯示縮短的查詢 URL。最後一次使用 URL 後會保留 93 天，才會刪除該 URL。
- 3 複製該 URL 並將其傳送到要共用的人員。


匯出目前查詢

您可以匯出記錄查詢的結果，以與其他系統共用或將其轉送給您的支援連絡人。

先決條件

確認您已登入 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 在**互動式分析**索引標籤上，執行要匯出的查詢。
- 2 按一下  並選取**匯出事件結果**。
- 3 選取儲存查詢的格式，然後按一下**匯出**。

功能表項目	說明
原始事件	選取以 TXT 格式儲存結果
JSON	選取以 JSON 格式儲存結果
CSV	選取以 CSV 格式儲存結果

建立查詢的快照



您可以在 vRealize Log Insight 中建立目前查詢和時間範圍的快照，以供快速檢視或儲存到儀表板。快照可以從 **[互動式分析]** 頁面建立。

快照會儲存您建立快照當時的時間範圍內可用的記錄訊息。建立快照後，按一下它可返回至建立快照時的查詢。如果想要儲存一或多個快照，請將它們新增到現有儀表板或建立新的儀表板。

先決條件

確認您已登入 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 在**互動式分析**索引標籤上，執行要儲存為快照的查詢。
- 2 按一下快照圖示。
快照隨即出現在畫面底部。
- 3 (選擇性) 變更查詢並建立更多快照。
快照隨即出現在畫面底部。
- 4 (選擇性) 在畫面底部，按一下  並選取**全部儲存至儀表板**。
 - a 選取現有儀表板或建立新的儀表板。
 - b 按一下**新增**。
快照隨即新增到選取或新的儀表板。
- 5 (選擇性) 按一下快照上的 "X" 可刪除快照。
- 6 (選擇性) 按一下  並選取**全部刪除**可刪除快照。

疑難排解 vRealize Log Insight 查詢結果

儀表板 Widget 旁或 [互動式分析] 頁面上的警告圖示，表示所顯示的資料可能存在問題。

當 vRealize Log Insight 必須處理大量記錄事件以提供準確結果時可能會發生此問題。有時，一小部分收集的記錄會因為未進行處理，而未包含在最終的結果中。根據目前的 vRealize Log Insight 負載及其必須為查詢處理的記錄數量，已處理的記錄數目和查詢結果可能會有所不同。

對於包含分組依據子句、涵蓋大量記錄或傳回數目相對大量結果的查詢，可能會顯示此行為。

您可以透過取代產生時間序列結果，而非單一值的查詢來解決此問題。此類型的查詢可產生更準確的結果，因為查詢處理不受記錄數量的影響。

使用儀表板

vRealize Log Insight 中的儀表板是圖表、欄位資料表和查詢清單 Widget 的集合。

自訂儀表板

自訂儀表板由 vRealize Log Insight 之目前執行個體的使用者建立。自訂儀表板以兩種類別加以組織：[我的儀表板] 和 [共用儀表板]。[共用儀表板] 對 vRealize Log Insight 執行個體的所有使用者可見。

[我的儀表板] 則為使用者特定。

一般使用者只能修改 [我的儀表板] 區段中的儀表板。

Admin 使用者可以修改 [我的儀表板] 區段中的儀表板和他們在 [共用儀表板] 區段中建立的儀表板。

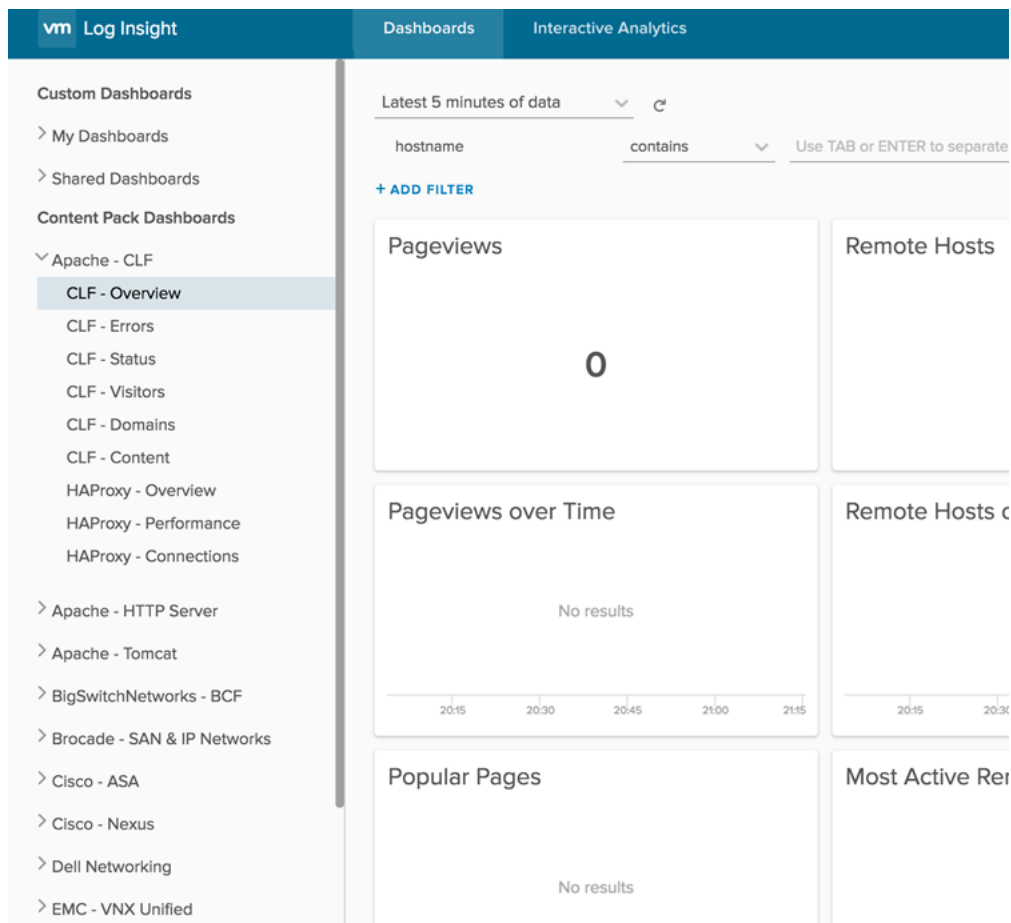
內容套件儀表板

內容套件儀表板隨內容套件一同匯入，並且對 vRealize Log Insight 執行個體的所有使用者都可見。

備註 內容套件儀表板為唯讀。您無法將其刪除或重新命名。但是，您可以將內容套件儀表板複製到自訂儀表板。您可以複製整個儀表板或個別 Widget。

若要檢視 vRealize Log Insight 執行個體中可用的儀表板，請按一下 vRealize Log Insight 使用者介面左上角的**儀表板**。出現的左窗格會列出您有權存取的所有儀表板，並依 [自訂儀表板] 和 [內容套件儀表板] 分組。按一下每個子群組旁的 >，可顯示相關聯的儀表板。您可以按一下群組名稱旁的 >，一次開啟一個儀表板群組。按一下另一個群組名稱旁的 >，可開啟新群組並關閉前一個群組。一次只能開啟一個群組。

若要檢視儀表板內容，請按一下左側清單中的儀表板名稱。



管理儀表板

您可以在 [自訂儀表板] 空間中新增、修改和刪除儀表板。

您無法修改內容套件儀表板和所下載的預先建立儀表板，但可以將這些儀表板複製到 [自訂儀表板] 空間並修改複製品。

重要事項 vRealize Log Insight 不會檢查您所儲存或複製的儀表板、查詢與警示是否有重複的名稱。當 vRealize Log Insight 儲存查詢時，顯示名稱不會是唯一的識別碼。因此，您可以儲存同名的多個圖表、警示和儀表板。為了方便擷取資料，儲存圖表、警示或儀表板時，請勿使用重複的名稱。

使用自訂儀表板

下表列出可用於建立或修改自訂儀表板的產品功能。

工作	程序
建立自訂儀表板。	在 儀表板 索引標籤上，選取 我的儀表板 ，然後按一下左下方的 新增儀表板 。
編輯自訂儀表板的名稱。	在 儀表板 索引標籤上，將游標指向儀表板名稱，接著按一下功能表圖示  ，然後選取 重新命名 。輸入新的名稱，然後按一下 儲存 。
刪除自訂儀表板。	在 儀表板 索引標籤上，將游標指向儀表板名稱，接著按一下功能表圖示  ，然後選取 刪除 。在確認對話方塊中，選取 刪除 。
將內容套件中的儀表板複製到自訂儀表板。	<ol style="list-style-type: none"> 在儀表板索引標籤上，選取內容套件，然後將游標指向您要複製的儀表板。 按一下功能表圖示 ，然後從下拉式功能表中選取複製。 輸入名稱，然後按一下儲存。 <p>如果您是管理員使用者，可以選取是否要與其他使用者共用儀表板。</p>
將圖表 Widget 新增到儀表板。	<ol style="list-style-type: none"> 在互動式分析索引標籤的左上方，按一下新增到儀表板。或者，從搜尋按鈕右側的功能表中，選取將目前查詢新增到儀表板。 輸入一個名稱，從下拉式功能表中選取目的地儀表板，然後選取 Widget 類型，接著新增此 Widget 的相關資訊並按一下新增。
將查詢清單 Widget 新增到儀表板。	請參閱 將查詢清單 Widget 新增到儀表板 。
將查詢新增到儀表板中的查詢清單 Widget。	請參閱 將查詢新增到儀表板中的查詢清單 Widget 。
將查詢新增到儀表板中的欄位資料表 Widget。	請參閱 將欄位資料表 Widget 新增到儀表板
將事件類型 Widget 新增到儀表板。	將事件類型 Widget 新增到儀表板
將事件趨勢 Widget 新增到儀表板。	將事件趨勢 Widget 新增到儀表板
從儀表板刪除 Widget。	<ol style="list-style-type: none"> 在儀表板索引標籤上，選取包含要刪除 Widget 的自訂儀表板。 在 Widget 右上角，按一下其他動作圖示 ，並選取刪除。 在 [刪除 Widget] 對話方塊中，按一下刪除以確認。

工作	程序
顯示所有 Widget 的時間同步化資料。	<p>依預設，您可以將滑鼠游標暫留在 Widget 中的指定資料點上，以顯示該點的圖例標籤。您也可以透過啟用顯示所有 Widget 的圖例的設定，以同時顯示所有 Widget 的圖例標籤，此設定適用於所有儀表板。此設定以 Cookie 為基礎，且會持續保留在瀏覽器工作階段中。</p> <ol style="list-style-type: none"> 1 在儀表板索引標籤上，選取一個儀表板。 2 在儀表板的左上角，將顯示所有 Widget 上的圖例切換設定為作用中。
對顯示警告符號的 Widget 進行疑難排解。	請參閱 疑難排解 vRealize Log Insight 查詢結果 。


將查詢清單 Widget 新增到儀表板

您可以透過建立查詢清單 Widget，將搜尋查詢清單儲存到自訂儀表板。

先決條件

確認您已登入 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 在**互動式分析**索引標籤上，執行要新增至儀表板的查詢。
- 2 按一下**將目前查詢新增到儀表板**圖示 。
- 3 從**儀表板**下拉式功能表中，選取要向其新增查詢的儀表板。
- 4 從**Widget 類型**下拉式功能表中，選取**查詢清單**。
- 5 從**查詢清單**下拉式功能表中，選取**新增查詢清單**，輸入清單的名稱，然後按一下**儲存**。
- 6 按一下**新增**。

查詢清單 Widget 會顯示在您指定的儀表板上。

下一個

您可以將查詢新增至已建立的查詢清單 Widget。請參閱 [將查詢新增到儀表板中的查詢清單 Widget](#)。

將查詢新增到儀表板中的查詢清單 Widget


查詢清單 Widget 提供從儀表板對一或多個已儲存查詢的快速存取。

您可以修改您的自訂查詢清單 Widget，以新增查詢。

先決條件

確認您已登入 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 在**互動式分析**索引標籤上，執行要新增至查詢清單 Widget 的查詢。
- 2 按一下**將目前查詢新增到儀表板**圖示 。
- 3 從**儀表板**下拉式功能表中，選取包含查詢清單 Widget 的儀表板。
- 4 從 **Widget 類型**下拉式功能表中，選取**查詢清單**。
- 5 從**查詢清單**下拉式功能表中，選取要向其新增查詢的 Widget 的名稱，然後按一下**儲存**。
- 6 按一下**新增**。

vRealize Log Insight 會將查詢新增至所選 Widget。

備註 查詢清單 Widget 使用訊息查詢。如果您在圖表 Widget 中使用相同的訊息查詢並選擇不存在於任何訊息中的分組依據欄位，則該圖表將不會顯示任何結果。


將欄位資料表 Widget 新增到儀表板

欄位資料表 Widget 提供從儀表板對一或多個已儲存欄位的快速存取。

先決條件

確認您已登入 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 在**互動式分析**索引標籤上，執行要新增至欄位資料表 Widget 的查詢。
- 2 按一下**將目前查詢新增到儀表板**圖示 。
- 3 從**儀表板**下拉式功能表中，選取要向其新增欄位資料表的儀表板。
- 4 從 **Widget 類型**下拉式功能表中，選取**欄位資料表**。
- 5 選取要包含在欄位資料表中的欄位。
- 6 按一下**新增**。

欄位資料表 Widget 會顯示在您指定的儀表板上。


將事件類型 Widget 新增到儀表板

事件類型 Widget 可讓您存取事件類型群組，其中系統會透過機器學習來建立事件類型，以將類似事件分組在一起。

先決條件

確認您已登入 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 在**互動式分析**索引標籤上，執行要新增至 **Widget** 的查詢。
- 2 按一下將目前查詢新增到儀表板圖示 。
- 3 從**儀表板**下拉式功能表中，選取要向其新增 **Widget** 的儀表板。
- 4 從 **Widget 類型**下拉式功能表中，選取 [事件類型]。
- 5 按一下**新增**。

Widget 會顯示在您指定的儀表板上。


將事件趨勢 **Widget** 新增到儀表板

事件趨勢 **Widget** 可讓您存取事件趨勢的相關資訊，這可用來分析指定期間內的趨勢。

先決條件

確認您已登入 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 在**互動式分析**索引標籤上，執行要新增至 **Widget** 的查詢。
- 2 按一下將目前查詢新增到儀表板圖示 。
- 3 從**儀表板**下拉式功能表中，選取要向其新增 **Widget** 的儀表板。
- 4 從 **Widget 類型**下拉式功能表中，選取 [事件趨勢]。
- 5 按一下**新增**。

Widget 會顯示在您指定的儀表板上。

使用圖表中的欄位值進行篩選

您可在包含圖表的儀表板、使用其欄位的不同儀表板和 [互動式分析] 中，將該圖表中的欄位值用作篩選器。

如果您發現圖表中的欄位值有問題，則可以快速將欄位值用作輸入，並跳到使用該欄位的其他儀表板。如果沒有其他儀表板使用該欄位，您可以將欄位值用作相同儀表板上的篩選器，或在 [互動式分析] 中執行該欄位值。

先決條件

確認您已登入 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 從**儀表板**下拉式功能表中，選取包含圖表 **Widget** 的儀表板。
- 2 在圖表 **Widget** 中，將游標暫留在圖表資料上即可檢視顯示為工具提示的欄位值。

- 3 按一下要用作篩選器的欄位值。

將值新增為篩選器功能表隨即顯示。

- 4 選取要將欄位值用作篩選器的位置。

選項	動作
互動式分析	[互動式分析] 頁面隨即開啟，並顯示圖表查詢的結果。將在步驟 3 中選取的欄位值用作篩選器。
此儀表板	將在步驟 3 中選取的欄位值用作相同儀表板上的篩選器。
其他儀表板	將在步驟 3 中選取的欄位值用作包含該欄位的其他儀表板上的篩選器。

使用內容套件

內容套件包含與特定產品或記錄集相關的儀表板、擷取之欄位、儲存之查詢和警示。

若要檢視在系統上載入的內容套件，請從 vRealize Log Insight 使用者介面右上角的下拉式功能表中選取內容套件。

若要檢視內容套件的內容，請按一下左側清單中的內容套件。

內容套件

[內容套件] 類別包含匯入的儀表板、擷取之欄位、查詢和警示集。依預設，會匯入一般內容套件和 VMware - vSphere 內容套件。

備註 內容套件儀表板為唯讀。您無法將其刪除或重新命名。但是，您可以將內容套件儀表板複製到自訂儀表板。您可以複製整個儀表板或個別 Widget。

自訂內容

[自訂內容] 類別包含在 vRealize Log Insight 目前執行個體中建立的儀表板、擷取之欄位和查詢。[我的內容] 區段包含目前登入的使用者的自訂內容。[共用內容] 區段包含 vRealize Log Insight 的所有使用者共用的內容。

僅 Admin 使用者可與其他使用者共用內容。僅 Admin 使用者可管理共用內容。

備註 您無法從 [自訂內容] 區段解除安裝內容。如果您要從 [自訂內容] 區段移除儲存的資訊，您必須刪除個別元素，如儀表板、查詢、警示和欄位。

安裝來自內容套件市集的內容套件

您可以安裝來自內容套件市集的內容套件，無需離開 vRealize Log Insight UI。

先決條件

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 從右上方的下拉式功能表中，選取**內容套件**。
- 2 在左側的**內容套件市集**下方按一下**市集**。
- 3 按一下您要安裝的內容套件。
- 4 選取同意授權合約條款的核取方塊。
- 5 按一下**安裝**。

安裝完成時，內容套件會顯示在左側的 [已安裝的內容套件] 清單上。

更新來自內容套件市集的已安裝內容套件

您可以從內容套件市集更新已安裝的內容套件，而無需離開 vRealize Log Insight。

備註 當來自內容套件的警示啟用時，警示將會複製到使用者的設定檔。使用者可修改複本的說明或條件。從在 4.0 中執行個體化的警示定義開始，更新內容套件、以及延伸其警示定義，將會更新或移除複本，以符合改善的內容套件。若要保留任何使用者修改，請先將其匯出為內容套件，等到更新之後，再重新匯入至使用者設定檔。

先決條件

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 從右上方的下拉式功能表中，選取**內容套件**。
- 2 從左側的功能表中選取**更新**，以檢視有可用更新的內容套件清單。
 - 若要更新單一內容套件，請按一下其圖示，以開啟資訊視窗。按一下**更新**，開始進行匯入。視內容套件而定，在匯入完成之後，您可能會看見進一步指示。若顯示這些指示，請依照設定步驟以成功完成升級。
 - 若要無訊息地以擱置的更新針對所有內容套件進行更新，請按一下**更新全部**。閱讀資訊快顯視窗中的指示，然後按一下**更新**繼續作業。升級之後，請按一下每個內容套件，以查看可在匯入後順利完成升級的後續設定步驟。如果您先前曾匯出內容套件以保存使用者修改，請將其重新匯入使用者設定檔中。

已更新的內容套件會顯示在左側的 [已安裝的內容套件] 清單中。

匯入內容套件

您可以匯入內容套件，以與 vRealize Log Insight 的其他執行個體交換使用者定義的資訊，或將舊版內容套件升級到較新版本。

您只能匯入 vRealize vRealize Log Insight 內容套件 (VLCP) 檔案。

備註 如果您匯入現有內容套件的新版本，並且該新版本包含已修改的欄位定義，則會更新使用已修改欄位的所有查詢、警示和圖表，以反映新定義。

當來自內容套件的警示啟用時，警示將會複製到使用者的設定檔。使用者可修改複本的說明或條件。從在 4.0 中執行個體化的警示定義開始，更新內容套件、以及延伸其警示定義，將會更新或移除複本，以符合改善的內容套件。若要保留任何使用者修改，請先將其匯出為內容套件，等到更新之後，再重新匯入至使用者設定檔。

您也可以從 VMware Solutions Exchange 下載內容套件，網址為 <https://marketplace.vmware.com>。在內容類型清單下方找到 vRealize Log Insight 內容套件，然後將其作為內容套件進行安裝

先決條件

- 如果您要使用「做為內容套件安裝」匯入方法，請確認您已使用具有**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。
- 如果您要使用「匯入至 [我的內容]」，您可以使用任何層級的權限登入 vRealize Log Insight Web 使用者介面。

程序

- 從右上方的下拉式功能表中，選取**內容套件**。
- 在左下角按一下**匯入內容套件**。
- 選取匯入方法。

選項	說明
做為內容套件安裝	內容會做為唯讀內容套件匯入，該內容套件對 vRealize Log Insight 執行個體的所有使用者可見。 備註 內容套件儀表板為唯讀。您無法將其刪除或重新命名。但是，您可以將內容套件儀表板複製到自訂儀表板。您可以複製整個儀表板或個別 Widget。
匯入到 [我的內容]	內容會做為自訂內容匯入到您的使用者空間，並且只有您能看見該內容。您可以編輯已匯入的內容，而無需複製。 備註 內容套件中繼資料 (如名稱、作者、圖示等) 不會在此模式下顯示。 一旦匯入到 [我的內容]，內容套件就無法做為套件解除安裝。如果要從 [我的內容] 移除內容套件，必須單獨移除其每個元素，如儀表板、查詢、警示和欄位。

一般使用者僅可將內容套件匯入其自己的使用者空間。

- 瀏覽您要匯入的內容套件，然後按一下**開啟**。

5 按一下匯入。

如果您已選取做為自訂內容匯入，則會出現對話方塊，讓您選取要匯入的內容。

6 (選擇性) 如果您已選取做為自訂內容匯入，請使用核取方塊選取要匯入的項目，然後再次按一下匯入。

備註 也會匯入用於已匯入的查詢、圖表和警示的欄位。

7 (選擇性) 針對某些內容套件，若您第一次匯入內容套件，您將會在匯入完成後看見彈出的設定指示。請依照這些指示完成內容套件的設定。

8 (選擇性) 針對某些內容套件，若您匯入內容套件作為升級，您將會在匯入完成後看見彈出的升級指示。請依照這些指示完成內容套件的設定。

匯入的內容套件隨即可供使用，並且會顯示在左側的 [內容套件] 或 [自訂內容] 清單中。

備註 依預設會停用已匯入的警示。請參閱[啟用警示查詢](#)。

匯出內容套件


您可以將自訂儀表板、儲存的查詢、警示和擷取的欄位匯出為內容套件，以便在 vRealize Log Insight 執行個體之間共用內容，或與社群上的 vRealize Log Insight 使用者共用內容。

內容套件會儲存為 vRealize vRealize Log Insight 內容套件 (VLCP) 檔案。

您匯出的查詢、圖表和警示中使用的所有欄位包含在已匯出的內容套件內。

如果匯出內容包含暫存欄位，則 vRealize Log Insight 會在匯出期間在內容套件中建立這些欄位。

程序

- 1 從右上方的下拉式功能表中，選取**內容套件**。
- 2 按一下要匯出的內容套件，然後從內容套件名稱旁的下拉式功能表  中選取**匯出**。
- 3 (選擇性) 選取要納入內容套件的內容。

備註 您無法取消選取用於為匯出所選取之儀表板、查詢或警示中的欄位。

4 在右側的文字欄位中，填寫內容套件的中繼資料。

選項	說明
名稱	將套件匯入 vRealize Log Insight 執行個體時，會顯示該名稱。內容套件檔案名稱是從 名稱 文字方塊衍生的。建議的格式為 <i>Vendor - Product</i> 。例如，VMware - vSphere。
版本	如果計劃升級此內容套件，請輸入版本。當您嘗試安裝 [內容套件] 清單中已存在的內容套件時，vRealize Log Insight 會顯示該版本。
命名空間	命名空間是內容套件的唯一識別碼。使用反向 DNS 命名，例如 com.companyname.contentpackname 。
作者	您可以輸入您的姓名或您公司的名稱。

選項	說明
網站	您可以提供與內容套件相關聯的網站連結。可檢視內容套件的所有使用者也可看到網站連結。
說明	您可以提供有關套件內容和用途的資訊。
圖示	您可以瀏覽顯示在內容套件名稱旁的圖示。 備註 圖示檔案格式必須為 PNG 或 JPG，並且其大小將擴充至 144 x 144 像素。

備註 只有透過使用**做為內容套件安裝**選項匯入內容套件時，此資料才可見。如果選擇匯入內容套件做為自訂內容，就無法檢視此資訊。

- 按一下**匯出**，瀏覽至要儲存檔案的位置，然後按一下**儲存**。

匯出的 VLCP 檔案將下載到所選的位置。

檢視有關內容套件元素的詳細資料

您可以直接從 [內容套件] 檢視開啟建立儀表板的查詢，或開啟欄位、查詢和警示的定義。

您可能想要將內容套件元素的定義用作自訂定義的範本。

程序

- 從右上方的下拉式功能表中，選取**內容套件**。
- 選取包含要檢閱之元素的内容套件。
- 按一下與要檢閱之元素類型相對應的按鈕。
例如，按一下**警示**以檢視內容套件包含的所有警示。
- 在元素清單中，按一下要檢閱之元素的名稱。

互動式分析頁面隨即開啟，並顯示與所選元素相對應的查詢。

下一個

您可以修改內容套件元素的查詢或定義，並將其儲存到您的自訂內容。

解除安裝內容套件

您可以解除安裝內容套件。解除安裝內容套件會移除自訂儀表板、已儲存的查詢、警示以及擷取的欄位。


內容套件會儲存為 vRealize vRealize Log Insight 內容套件 (VLCP) 檔案。

解除安裝內容套件會使其永久不可供使用者使用。透過先將內容套件匯出為 **VLCP** 檔案進行備份。請參閱[匯出內容套件](#)。

先決條件

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 從右上方的下拉式功能表中，選取**內容套件**。
- 2 按一下要解除安裝的內容套件，然後從內容套件名稱旁的下拉式功能表  中選取**解除安裝**。
- 3 按一下**解除安裝**。

內容套件即從 [已安裝內容套件] 清單中移除。

建立內容套件

任何 Log Insight 使用者都能建立針對私用或公用的內容套件。

內容套件是固定或唯讀的 vRealize Log Insight 外掛程式，可提供有關特定事件類型 (例如記錄訊息) 的預先定義知識。內容套件旨在以管理員、工程師、監控團隊和執行人員易於瞭解的格式提供有關特定事件集的知識。

內容套件提供了有關產品或應用程式健全狀況狀態的資訊。此外，內容套件還可協助您瞭解產品或應用程式的運作方式。

您可以透過使用 vRealize Log Insight 中的 [儀表板] 或 [互動式分析] 頁面，儲存內容套件資訊。內容套件資訊包括：

- 查詢 - 通常，一個內容套件會針對每個儀表板包含至少 3 個查詢和 3 個圖表 Widget，因此，總計超過 9 個查詢
- 欄位 - 內容套件應具備至少 20 個擷取的欄位
- 彙總
- 警示 - 每個內容套件包含至少 5 個警示
- 儀表板 - 每個內容套件中至少有 3 個儀表板
- 儀表板篩選 - 請參閱[搜尋和篩選記錄事件](#)
- 視覺化 - 請參閱[使用互動式分析圖表分析記錄](#)

依預設，vRealize Log Insight 出廠時隨附 VMware - vSphere 內容套件。您可以視需要匯入其他的內容套件。

內容套件術語

內容套件建立工作流程是以幾個概念和術語為基礎。您應該熟悉這些概念和術語，以便有效地建立和維護內容套件。

執行個體

僅 vRealize Log Insight 管理員可以將內容套件檔案匯入為內容套件。如果內容套件檔案匯入為內容套件，則無法進行編輯。

所有使用者可將內容套件檔案匯入使用者空間。如果您將內容套件檔案匯入使用者空間，則作業會選擇性地匯入 [我的內容] 下的物件。將內容套件匯入使用者空間時，您可以在 vRealize Log Insight 執行個體中編輯內容套件。如果要發佈或修改內容套件，您需要匯出的內容套件。

使用者

從自訂儀表板 (也稱為使用者空間，明確而言就是 [儀表板] 頁面上的 [我的儀表板] 或 [共用儀表板]) 下儲存的内容建立部分內容套件。由於可從自訂儀表板選擇性匯出物件，建議由 vRealize Log Insight 中獨立的使用者實體編寫每個個別內容套件，以確保每個內容套件有乾淨的使用者空間。

如需在 vRealize Log Insight 中建立使用者的相關資訊，請參閱《VMware vRealize Log Insight 管理指南》。

為建立的每個內容套件使用 vRealize Log Insight 中的獨立的內容套件作者使用者。

事件

在嘗試建立內容套件之前收集相關事件至關重要，以確保內容套件涵蓋產品或應用程式的所有相關事件。收集相關事件的一種常用方法是向品質保證和支援團隊索取，因為這些團隊通常可存取並瞭解常見事件。

在建立內容套件時嘗試產生事件會非常耗時，並會導致重要事件遺失。如果 QA 和支援團隊無法提供事件，您可以模擬事件，並在產品或應用程式事件已知並記錄的情況下使用這些事件。

收集適當的記錄後，必須將這些記錄擷取到 vRealize Log Insight。

作者

內容套件的作者需要滿足下列條件：

- 具備使用 VMware vRealize Log Insight 的經驗。
- 具備產品或應用程式的實際操作知識。
- 瞭解並可以產生最佳化規則運算式。
- 具備使用記錄偵錯多個產品或應用程式問題的經驗。
- 具備應對各種問題的支援背景。
- 具備之前 syslog 經驗的系統管理員背景。

工作流程

建立內容套件的建議方法是從 [互動式分析] 頁面開始查詢特定類型的事件 (如錯誤或警告)。查看查詢結果並視情況分析和擷取潛在欄位候選。大概瞭解事件類型和事件中提供的有用資訊，視情況建構和儲存相關查詢。對於反白顯示需要快速採取動作之問題的查詢，建立和儲存警示。儲存查詢時，使用篩選器將其從結果清單中移除，以顯示可能為新儲存查詢之潛在候選的其他事件。儲存所有相關查詢後，在 [儀表板] 頁面上以邏輯方式組織和顯示它們。

查詢

vRealize Log Insight 中的查詢可擷取和摘要事件。

您可以從 [互動式分析] 頁面建立和儲存查詢。查詢包含下列一或多項：

關鍵字	完整或全文檢索英數、連字號和/或底線比對。
Glob	完整或全文檢索英數、連字號和/或底線比對。
規則運算式	根據 Java 規則運算式進行複雜的字串模式比對。
欄位運算	套用到擷取之欄位的關鍵字、規則運算式和模式比對。
彙總	套用到一或多個結果子群組的函數。

vRealize Log Insight 支援下列查詢類型：

- 訊息。由關鍵字、規則運算式和/或欄位運算組成的查詢。
- 規則運算式或欄位。由關鍵字和/或規則運算式組成的查詢。
- 彙總。由函數、一或多個群組，以及任何數目的欄位組成的查詢。

您可以在 vRealize Log Insight 中定義自訂警示，並從任何類型的排定查詢觸發這些警示。

建立訊息查詢的最佳做法

建立訊息查詢的基本概念。

您可以使用搜尋列或輸入篩選器來輸入訊息查詢。

使用搜尋列可縮小 vRealize Log Insight 執行個體中事件的範圍。雖然您可以使用篩選器來取代搜尋列，但通常運用搜尋列會比運用對等的篩選器更易瞭解查詢。最佳做法是儘可能使用搜尋列，而不要使用對等的篩選器。

篩選器可讓您使用規則運算式、欄位、邏輯 **OR** 運算或是搜尋列和篩選器的查詢組合來建立查詢。

當您使用搜尋列和篩選器建立查詢時，適用下列最佳做法：

- 確認查詢不限於特定環境。公用內容套件必須對任何環境通用，這樣一來就不需要依賴環境特定資訊。環境特定資訊的範例包括來源、主機名稱以及可能的功能 (如果功能使用 *local**)。
- 建構查詢時，儘可能使用關鍵字，當關鍵字不足時，請使用 **Glob**，而當 **Glob** 不足時，再使用規則運算式。關鍵字查詢是耗費資源最少的查詢類型。**Glob** 是規則運算式的簡化版，是次耗費資源最少的查詢類型。規則運算式是耗費資源最多的查詢類型。
- 使用規則運算式或欄位時，儘可能提供多個關鍵字。如果規則運算式包含邏輯 **OR**，例如 *這個/那個*，請勿包含關鍵字。vRealize Log Insight 最適合在規則運算式之前執行關鍵字查詢，以將規則運算式的額外負荷降至最低。

欄位查詢

欄位提供了一種極佳的方法，可將結構新增至非結構化事件並允許操作資料的文字和視覺表示。

欄位是內容套件中最重要之項目之一，因為可透過包括彙總和篩選器在內的不同方式使用它們。彙總允許您將函數和群組套用至欄位。篩選器允許您在欄位上執行作業。

您必須擷取可能適用於查詢或彙總的記錄訊息的任意部分。欄位是一種規則運算式查詢，對複雜模式比對非常有用，因此，您無需瞭解、記住和掌握複雜的規則運算式。

欄位內容值	定義
值之前的 regex	包含儘可能多的關鍵字。如果此欄位空白或僅包含特殊字元，則值之後的 regex 必須包含關鍵字。
值之後的 regex	包含儘可能多的關鍵字。如果此欄位空白或僅包含特殊字元，則值之前的 regex 必須包含關鍵字。
名稱	僅使用英數字元。確保所有字元都為小寫，並使用底線而非空格，因為這樣會使欄位更易於檢視。請記住，內容套件欄位和使用者欄位的名稱可以相同，但內容套件欄位在欄位名稱右側有以括弧括起的命名空間。為內容套件欄位加上縮寫前置詞 (如 vmw_)，以避免產生混淆。
關鍵字搜尋詞彙	一或多個由空格隔開的關鍵字，這些關鍵字會出現在包含欄位的事件內。
篩選器	靜態欄位、運算子和可能的值，這些項目會出現在包含欄位的事件內。 篩選器常與 vRealize Log Insight 代理程式和標記搭配用於未包含關鍵字的事件。
資訊 ("i" 按鈕)	用來提供關於欄位的資訊，包括其代表的意義、可能傳回的值，並可能包括將值解讀為人類可理解資訊的易用對應。

最佳做法

除了組成欄位的各種元件外，還適用一些最佳做法。

- 僅為規則運算式模式建立欄位。如果可使用關鍵字查詢來查詢欄位或欄位僅傳回單一值，則使用關鍵字查詢，而非預先定義欄位。如果欄位僅傳回兩個值，則考慮建構個別查詢，而非擷取欄位。欄位可將結構新增至非結構化資料，並提供查詢事件之特定部分的方法。
- 僅為傳回事件總計一部分的規則運算式模式建立欄位。符合多數事件和/或傳回大量結果的欄位並非良好的欄位擷取候選。需要將規則運算式套用至大量事件，這會導致資源密集型作業。如果可能，新增其他關鍵字以減少傳回的結果數，並最佳化查詢。
- 如果欄位包含規則運算式語法內的關鍵字，則新增此類關鍵字做為沒有規則運算式語法時的篩選器。例如，如果欄位的值或內容包含規則運算式語法內的關鍵字 (如 *這個那個*)，則將此關鍵字新增為文字篩選器，以最佳化查詢 (如 *文字包含這個、那個*)。
- 建議在複雜規則運算式的前後內容中使用包含一或多個關鍵字的其他內容。
- 將其他內容新增到所有擷取的欄位，以最佳化查詢效能。

暫存欄位

暫存欄位是查詢的一部分，但不在 **vRealize Log Insight** 執行個體內全域儲存或做為已安裝內容套件的一部分進行儲存。

vRealize Log Insight 透過自動更新依賴所修改之欄位的查詢，減少建立暫存欄位的機會。

備註 如果刪除已儲存查詢所依賴之欄位，則已儲存查詢會包含一個暫存欄位。

當您在 [互動式分析] 頁面中執行已儲存查詢時，如果已儲存查詢中使用的某個欄位之欄位名稱右側包含命名空間「暫存」，您就會看到暫存欄位。

查詢要包含一或多個欄位。對於 vRealize Log Insight 中的已儲存查詢，修改欄位時也會修改在儲存查詢時使用的欄位定義。欄位修改包括

- 變更欄位值
- 變更值之前的 regex 和欄位值之後的 regex
- 變更欄位名稱
- 刪除欄位

匯出內容套件時，vRealize Log Insight 會將所有暫存欄位轉換為內容套件欄位。如果您在內容套件中看到暫存欄位，則可能查看的是連同暫存欄位一併匯出之舊產品版本的內容套件或手動編輯的內容套件。

如果有暫存欄位與現有擷取欄位同名，暫存欄位的結尾會顯示 {n}。例如，如果您有個名為 `product_test_field` 的欄位，在匯出期間也可能看到 `product_test_field {2}`。如果出現此現象，表示有暫存欄位存在。若要解決此問題，請選擇匯出對話方塊底部的**全部不選**選項，然後選取每個儀表板和/或警示，直到勾選包含 {n} 結尾的擷取欄位。前往這些儀表板和/或警示，然後編輯每個查詢。當您找到使用擷取欄位的查詢時，請變更篩選器或彙總以使用沒有 {n} 結尾的欄位、執行查詢，然後儲存查詢。針對使用 {n} 結尾的欄位的所有查詢完成上述步驟後，該欄位就不再會在匯出期間顯示。

彙總查詢

vRealize Log Insight 可讓您使用彙總查詢操縱事件的視覺表示。

彙總查詢由下列兩個屬性組成：

- 函數
- 群組

彙總查詢需要一個函數和至少一個群組。群組是內容套件的重要組成部分。函數和群組會影響圖表的顯示方式。

圖表中最多可顯示 2,000 個最近的結果。

橫條圖

依預設，vRealize Log Insight 的 [互動式分析] 頁面上的概觀圖表顯示隨著時間變更的事件計數。如果您同時使用計數函數和時間序列群組，則 vRealize Log Insight 會建立橫條圖。

如果您同時使用計數函數和單一欄位群組 (而非時間序列群組)，則 vRealize Log Insight 會建立橫條圖，並在圖表中按最高到最低的順序列出數量。

折線圖

除計數函數之外的所有函數都是數學函數。它們需要可在其中套用方程式的欄位。如果在欄位上執行數學函數並按時間序列分組，則 vRealize Log Insight 會建立折線圖。

堆疊圖

依預設，vRealize Log Insight 的 [互動式分析] 頁面上的概觀圖表表示隨著時間變更的事件計數。如果您將一個欄位新增至時間序列群組，則 vRealize Log Insight 會建立堆疊圖。

如果您使用按時間序列分組，再加上一個欄位，並使用除計數函數之外的任何函數，vRealize Log Insight 會建立堆疊折線圖。堆疊圖在嘗試尋找物件的異常時十分實用。

您必須以彙總查詢可能傳回的物件數為基礎，決定使用哪種類型的堆疊圖。顯示的物件越多，需要用於剖析和顯示資訊的資源也就越多。此外，色彩的數目是固定的，區分物件亦可能視傳回的物件數目而變得困難。一般而言，下列最佳做法較適用

- 如果每個長條中傳回的物件數均小於十，則您可能需要使用堆疊圖。
- 如果每個長條中傳回的物件數均介於或可能介於十到二十之間，則堆疊圖是較好的選擇。您必須考慮如何在內容套件中直覺地表示圖表。
- 如果每個長條中傳回的物件數均大於或可能大於二十，則不建議使用堆疊圖。

多色圖

如果使用多個欄位和時間序列來建立群組，則 vRealize Log Insight 會建立多色圖。該圖表包括兩種可交換的顏色。每次交換均表示新的時間範圍。多色圖表難於理解，因此，將此圖表包含在內容套件之前，請先考慮此圖表的價值。

當您按多個欄位進行分組時，請考慮使用非時間序列。移除時間序列會使橫條圖更易於理解。

如果多個欄位在指定時間範圍內非常重要，則您可以為每個欄位個別建立隨著時間範圍變更的多個圖表。然後您可以將這些圖表顯示在內容套件中儀表板群組的相同資料行中。

其他圖表

有數個其他類型的圖表可供使用，包括圓形圖、泡泡圖和資料表圖。若要使用這些圖表，需要特定查詢類型。如果這些圖表的選項可用，表示您已有正確的查詢。如果這些圖表的選項無法使用，請將游標暫留在要使用的圖表名稱上。快顯訊息會說明圖表類型所需的查詢類型。

訊息查詢

建構彙總查詢時，訊息查詢應僅傳回與彙總查詢相關的結果。這會讓分析變得更簡單，並確保結果僅顯示相關欄位。若要確保訊息查詢傳回與彙總查詢相同的結果，您必須使用 **exists** 運算子為彙總查詢中使用的每個欄位新增篩選條件。

變更圖表類型

如果要變更儀表板上 Widget 的圖表類型，請按一下 Widget 上的齒輪圖示，然後選取**編輯圖表類型**。如果要變更 Widget 類型，請儲存新的 Widget 並刪除舊 Widget。

警示

警示提供在發生特定類型的事件時觸發反應的方法。

vRealize Log Insight 支援兩種類型的警示

- 電子郵件
- vRealize Operations Manager

您僅可在使用者空間中儲存警示。依預設，會停用所有內容套件警示。如果建立啟用的警示並將其做為內容套件的一部分匯出，則會在內容套件中停用該警示。

內容套件不包含電子郵件及 **vRealize Operations Manager** 設定。並且您無法將這些設定新增到內容套件。

臨界值

臨界值對已觸發警示的數目設定限制。

瞭解臨界值的運作方式非常重要，以確保在啟用臨界值的情況下內容套件警示不會無意向使用者濫發。考慮使用臨界值時，必須記住下面兩個問題

- 觸發警示的頻率如何？**Log Insight** 帶有預先定義的頻率。警示僅針對指定臨界值時間範圍觸發一次。
- 檢查是否發生警示狀態的頻率如何？警示由查詢觸發。同查詢一樣，警示在目前版本中並非即時。對於每個臨界值時間範圍，會配置預先定義的查詢頻率。變更臨界值會變更查詢時間。

群組

建立電子郵件警示時，依可識別警示來源的欄位進行分組很重要。

警示傳送的電子郵件包含特定彙總查詢結果的資料表。您可以在 **[互動式分析]** 頁面上查看查詢的視覺呈現。

如果沒有唯一識別碼做為分組依據，您將無法知道結果是否與環境中的一或多個系統相關。您應按照主機名稱欄位 (而非來源欄位) 進行分組。您也可以新增唯一識別事件來源的任何欄位。

儀表板最佳做法

儀表板是內容套件的一部分。以下是一些建立儀表板時適用的最佳做法。

建立儀表板時，適用以下最佳做法

- 內容套件通常至少包含三個儀表板。最佳做法是從概觀儀表板開始，提供有關特定產品或應用程式事件的高階資訊。除了概觀儀表板之外，儀表板應以事件的邏輯群組為基礎建立。邏輯群組為產品特定或應用程式特定，但某些常見方法為效能、故障和稽核。同樣，建立元件 (如磁碟及控制器) 的儀表板也很常見。使用元件方法時，需要注意的是，此方法僅在可以建構查詢以從特定元件傳回結果時有效。如果這種方法不可用，建議使用邏輯方法。
- 命名儀表板時，使用一般名稱，避免新增產品特定或應用程式特定的名稱，除非以元件特定的方式使用。例如，在 **VMware - vSphere** 內容套件中，存在名為 **ESX/ESXi** 而非 **VMware ESX/ESXi** 的儀表板群組。
- 儀表板必須至少包含三個儀表板 **Widget**，最多包含六個儀表板 **Widget**。如果少於三個儀表板 **Widget**，則儀表板取得的資訊量很小。此外，具有多個僅包含有限數量儀表板 **Widget** 的儀表板，需要使用者在不同頁面之間切換，並且不以連貫方式提供資訊。

反之，儀表板中有超過六個儀表板 **Widget** 可能會帶來負面影響。您可能會收到過多資訊，令人混淆。過多 **Widget** 需要大量使用您的系統資源，因為每個 **Widget** 都是必須針對系統執行的查詢。

在儀表板中加入六個以上的儀表板 **Widget** 時，您必須分隔資訊並建立多個儀表板。如果儀表板 **Widget** 適用於一或多個儀表板，則在每個適用的儀表板中建立此 **Widget**。

儀表板篩選器

儀表板篩選器可用來向下切入到特定事件。篩選器的作用類似於 [互動式分析] 頁面上的篩選器，利用欄位向下切入。每個儀表板都應至少有一個儀表板篩選器，通常是主機名稱欄位，不過每個儀表板最多可以新增 5 個欄位。

特定儀表板上的大多數 **Widget** 都應使用新增的欄位，以便在使用儀表板篩選器時，大多數 **Widget** 都能傳回結果。儀表板篩選器的例子可包括嚴重性欄位、使用者欄位或甚至元件欄位。

備註 儀表板篩選器使用的欄位和運算子將儲存在匯出的內容套件中。匯出期間不會儲存儀表板篩選器使用的任何值，因為此值可能是環境特定的，並非所有環境皆通用。

儀表板 Widget

儀表板 **Widget** 可協助您視覺化資訊。

您可以在 vRealize Log Insight 中將數種類型的 **Widget** 新增到儀表板。這些包含：

- 圖表 **Widget**，包含事件的視覺表示，隨附已儲存查詢的連結。
- 查詢清單 **Widget**，包含已儲存查詢的標題連結。
- 欄位資料表 **Widget**，包含事件，其中每個欄位均代表一個資料行。
- 簡化的事件類型資料表 **Widget**，包含在單一群組中合併的類似事件。
- 簡化的事件趨勢資料表 **Widget**，顯示在查詢中找到的事件類型清單，依發生次數排序。您可以透過此方法快速查看查詢中頻繁發生的事件類型。

圖表

儀表板圖表 **Widget** 包含事件的視覺表示。您可將圖表示為橫條圖或折線圖，二者皆可顯示為堆疊圖。

可以使用多種方法來表示圖表：

- 圖表可以包含大量資訊。避免在單一系列中使用兩個以上的圖表 **Widget**。在少數情況下，可有效地使用三個圖表 **Widget**，但十分不建議使用三個以上的圖表 **Widget**。當決定圖表 **Widget** 是否可讀取時，請確保使用 vRealize Log Insight 支援的最小解析度 1024 x 768 像素。
- 如果除最後一系列的任意列具有單一圖表 **Widget**，請使該 **Widget** 為全寬
- 命名圖表 **Widget** 時，請使用描述性標題並避免隱密的欄位名稱。例如，擷取的欄位名為 `vmw_error_message`。將圖表稱為錯誤訊息計數，而非 `vmw_error_message` 計數
- 您可以儲存類似圖表並將其堆疊到儀表板群組的同一資料行中，以便進行視覺比較。例如：
 - 隨著時間變更的事件平均值 X + 隨著時間變更的事件最大值 X。考慮到使用不同的函數，圖表中 Y 軸的刻度可能會有所不同。
 - 按 X 分組的隨著時間變更的事件計數 + 按 Y 分組的隨著時間變更的事件計數。

查詢清單

儀表板查詢清單 **Widget** 包含預先定義查詢的一或多個連結。

可能會使用查詢清單 **Widget** 的原因如下

- 圖表 **Widget** 未提供有意義的值，但基礎查詢卻能提供。
- 要儲存複雜查詢，例如使用規則運算式的查詢。
- 要在儀表板群組內的相同基礎查詢上使用不同的彙總。

欄位資料表

欄位資料表，包含事件，其中每個欄位均代表一個資料行。

儀表板欄位資料表 **Widget** 以資料表格式包含特定查詢的最新事件，其中每個欄位均代表一個資料行。

出於以下原因，您可以使用欄位資料表 **Widget**。

- 查看特定查詢的最新事件。這對於變更管理或安全考量可能很有用。
- 僅查看特定查詢中所需的欄位。這對於限制事件輸出可能很有用。

內容套件匯入錯誤

匯入內容套件時，您可能會收到一些警告或錯誤訊息。

升級

您可能會收到升級訊息。這表示其他內容套件已安裝在具有相同命名空間的系統中。在此情況下，您可以升級並取代現有內容套件，或取消升級程序並保留現有內容套件。

格式無效

您可能會收到一則訊息，說明格式無效。這表示已手動編輯 **VLCP** 檔案且此檔案包含語法錯誤。必須先修正語法錯誤，然後才能匯入內容套件。

較新版本

此類型的訊息表示內容套件在更新版本的 **Log Insight** 中建立並且僅受其支援。在高於 **Log Insight 1.5** 版本的產品中，顯示此類型的訊息表示已手動編輯 **VLCP** 檔案。

無法辨識的版本

如果已手動編輯 **VLCP** 檔案且此檔案包含語法錯誤，您會看到此類型的訊息。您必須先修正語法錯誤，然後才能嘗試匯入內容套件。

備註 您不應手動編輯 **VLCP** 檔案。因此，找到並修正語法錯誤相當困難。

發佈內容套件的需求

當您建立並想要發佈內容套件時，請確定內容套件符合基本發佈需求。

您必須檢查內容套件需求和發佈需求。

內容套件需求

內容套件必須符合一些內容、品質和標準需求。

內容需求包括

- 最少三個儀表板
- 每個儀表板最少一個 (最好三個) 最多五個儀表板篩選器
- 每個儀表板最少三個儀表板 Widget
- 每個儀表板最多六個儀表板 Widget
- 每列最多三個儀表板 Widget
- 最少五個警示
- 最少二十個擷取的欄位

內容套件的品質需求如下

- 每個查詢至少有一個全文檢索關鍵字，並且最好有三個或以上的關鍵字
- 查詢不是以環境特定屬性 (例如來源、主機名稱或 *功能**) 為基礎
- 每個欄位至少有一個全文檢索關鍵字，並且最好有三個或以上的關鍵字
- 欄位特定於產品/應用程式，不會傳回其他產品/應用程式記錄的結果
- 每個儀表板 Widget 必須包含說明圖表內容及重要性的資訊/連結

建立內容套件的標準遵循下列規則

內容套件部分	格式
內容套件名稱格式	<i>Company - Product</i>
內容套件命名空間格式 (內容套件必須使用命名空間匯出)	<i>Ext.Domain.Product</i>
擷取的欄位格式	<i>Prefix_Field_Name</i> ，其中 <i>Prefix</i> 是公司名稱或公司縮寫。

發佈需求

發佈內容套件之前，請檢查套件是否符合發佈需求。使用開發人員中心上的內容套件發佈者來取得內容套件建議，並將要檢閱的版本上傳給 VMware。 <https://developercenter.vmware.com/web/loginsight>

發佈需求	說明
內容套件檔案格式	VLCP 檔案。
事件	驗證內容套件所需的適当事件。
概觀	內容套件的概觀，長度為一到兩個段落。
要點	三個要點，說明內容套件的價值。
說明	內容套件及其價值的說明，長度為兩到三個段落。
技術規格	說明最低系統需求，包括產品版本和組態，以及 Log Insight 版本和組態。此外還提供設定產品以登入 Log Insight 以及填入內容套件所需的所有指示。

發佈需求	說明
螢幕擷取畫面	三個或以上的螢幕擷取畫面，顯示包含真實資料的內容套件。
視訊 (選擇性)	示範內容套件如何帶入值。
白皮書 (選擇性)	如何設定產品或應用程式將記錄轉送給 vRealize Log Insight。

提交內容套件

提交在 VMware Solutions Exchange 上建立的內容套件。

先決條件

- 確認您的內容套件滿足[發佈內容套件的需求](#)。
- 如果您在 <http://solutionexchange.vmware.com> 上沒有帳戶，請按一下**註冊**並選取**合作夥伴**。填寫 [合作夥伴註冊申請] 表單並提交。如果您的登入申請已獲核准，您將會收到通知電子郵件。

程序

- 1 前往 <http://solutionexchange.vmware.com> 並按一下頁面右上角的**立即登入**。
- 2 輸入您的使用者名稱和密碼，然後按一下**立即登入**。
- 3 按一下**管理**並選擇**管理解決方案**，以新增或編輯解決方案。
- 4 按一下**新增解決方案**並填寫所需資訊。
頻繁使用**儲存草稿**按鈕以確保您不會遺失任何工作成果。
- 5 按一下**提交以供核准**。
您的解決方案將會傳送至 VMware Solution Exchange 聯盟團隊，以供檢閱和核准。

您將收到有關解決方案的核准狀態的電子郵件。

下一個

如需填寫解決方案清單的詳細資訊，請按一下頁面頂部的**合作夥伴專區**連結。如果您找不到所需資訊，請連絡 VSXAlliance@vmware.com 提出任何問題。

vRealize Log Insight 中的警示查詢

您可以將 vRealize Log Insight 設定為以排定的時間間隔執行特定的查詢。

如果符合查詢的事件數目超過了設定的臨界值，vRealize Log Insight 會傳送電子郵件或 Webhook 通知並在 vRealize Operations Manager 中觸發通知事件。

若要檢視可用警示的清單，請導覽至 [互動式分析] 頁面，然後從**搜尋**欄位旁的**建立和管理警示...**下拉式功能表中選取**管理警示...**。每個警示名稱的下方將出現該警示的狀態。

備註 警示查詢特定於使用者。您只能管理自己的警示。您必須獲指派為超級管理員角色，才能管理其他使用者警示。

vRealize Log Insight 中可建立的警示類型

您可以控制警示查詢執行的時間間隔，以及 vRealize Log Insight 傳送警示通知的條件 (選取一個警示類型後)。

任何相符項的警示	警示查詢會每隔 5 分鐘自動執行。如果最後 5 分鐘內至少有一個事件與查詢相符，則會觸發通知。
根據事件類型的警示	警示查詢會每隔 5 分鐘自動執行。看到指定的事件類型時會觸發通知。
根據自訂期間內事件數目的警示	<p>警示查詢的時間間隔取決於您的設定。根據您的設定，在最後 Y 分鐘內出現的相符事件數超過或少於 X 時觸發警示。</p> <p>觸發此類型的警示後，將對其期間的持續時間進行延期，以防止針對同一組事件發出重複的警示。如果希望在延期時啟用警示，您可以先停用再重新啟用警示。</p>
根據彙總查詢的警示	<p>如果分組中函數的值超出您定義的值，則彙總查詢警示會觸發通知。您可以在圖表中看到此情況，其中在您指定的期間內，圖表中至少有一個長條高於或低於設定的臨界值。</p> <p>可針對不視覺化 隨著時間變更的事件計數 的圖表設定此警示類型。</p>

內容套件警示

內容套件可包含警示查詢。vRealize Log Insight 中預設包括的 vSphere 內容套件包含數個預先定義的警示查詢。這些查詢會在下列情況下觸發警示：ESXi 主機停止傳送 syslog 資料，vRealize Log Insight 無法再從 vCenter Server 收集事件、工作和警示資料，或者警示狀態變更為紅色。您可以將這些警示查詢做為範本來建立特定於您環境的警示。

預設會停用所有的內容套件警示。

啟用 **vCenter Server: ESX/ESXi 停止記錄** 警示是一種比較好的做法，因為當您重新啟動 vRealize Log Insight 時，某些版本的 ESXi 主機可能會停止傳送 syslog 資料。此警示會監控 vCenter Server 事件 `esx.problem.vmsyslogd.remote.failure`，以偵測是否存在停止傳送 syslog 摘要的 ESXi 主機。如需有關 syslog 問題和解決方案的詳細資料，請參閱 [VMware ESXi 5.x 主機停止向遠端伺服器傳送 syslog \(2003127\)](#)。

您可以將下面的篩選器新增到警示查詢並將其儲存為新的警示，以僅偵測停止向 vRealize Log Insight 執行個體傳送摘要的 ESXi 主機：**vc_remote_host (VMware - vSphere)** 包含 *log-insight-hostname*。

內容套件警示查詢為唯讀。若要儲存對內容套件警示所做的變更，您必須將警示儲存到您的自訂內容。

- **新增警示查詢以傳送電子郵件通知**

您可以在 vRealize Log Insight 中設定警示查詢，以在記錄中顯示特定資料時傳送電子郵件通知。

- **關於使用 Webhook 傳送警示給協力廠商產品**

您可以使用 Webhook 傳送 vRealize Log Insight 使用者警示給協力廠商產品。

■ 檢視警示查詢

您可以檢視已建立的警示查詢，並檢查是否已啟用這些查詢的通知。

■ 修改警示查詢

您可以變更警示查詢的觸發器、啟用或停用查詢傳送的通知，或者變更通知方法 (電子郵件、Webhook，或傳送至 vRealize Operations Manager)。

■ 啟用警示查詢

停用警示查詢後，vRealize Log Insight 不會傳送電子郵件或 Webhook 通知，並且不會觸發 vRealize Operations Manager 通知事件。

■ 刪除警示查詢

當您不再需要警示查詢時，可以將其刪除。

新增警示查詢以傳送電子郵件通知

您可以在 vRealize Log Insight 中設定警示查詢，以在記錄中顯示特定資料時傳送電子郵件通知。

先決條件

- 確認您已登入 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。
- 確認管理員已將 SMTP 設定為啟用電子郵件通知。請參閱 [為 Log Insight 設定 SMTP 伺服器](#)。

程序

- 1 在 **互動式分析** 索引標籤上，針對要為其傳送通知的項目執行查詢。
- 2 從 **搜尋** 按鈕右側的 **建立或管理警示** 功能表中，按一下 ，然後選取 **從查詢建立警示**。
- 3 在 **[新增警示]** 對話方塊中，輸入警示的名稱，並提供觸發該警示之事件的簡短而有意義的說明。
警示名稱和說明包含在 vRealize Log Insight 傳送的電子郵件中。
- 4 選取 **電子郵件** 核取方塊，並輸入您想要 vRealize Log Insight 向其傳送通知的電子郵件地址。
使用逗點分隔多個地址。
- 5 設定警示臨界值。

警示類型	選擇
任何相符項	選取在 任何相符項 上選項。 每隔 5 分鐘執行一次查詢。
根據事件類型	選取 過去 <time period> 內第一次看到新的事件類型時 選項，然後從下拉式功能表中選取時間。 每隔 5 分鐘執行一次查詢。

警示類型	選擇
根據一段時間內的事件數目	選取第三個選項，然後使用下拉式功能表設定參數。 根據下拉式功能表中的選擇執行查詢。
根據圖表值	選取第四個選項，然後使用下拉式功能表設定參數。 備註 僅當您選取根據至少一個欄位分組事件時，此警示類型才可用。您無法針對僅視覺化時間序列的圖表建立此警示類型。 根據第二個下拉式功能表中的選擇執行查詢。

預覽圖表中的橙色行將顯示目前臨界值。

6 按一下儲存。

下一個

您可以啟用、停用或刪除已儲存的警示。

備註 警示查詢特定於使用者。您只能管理自己的警示。您必須獲指派為超級管理員角色，才能管理其他使用者警示。

關於使用 Webhook 傳送警示給協力廠商產品

您可以使用 Webhook 傳送 vRealize Log Insight 使用者警示給協力廠商產品。

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。

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

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。vRealize Log Insight 會重試失敗的要求。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。

您必須是 vRealize Log Insight 管理員才能建立系統通知。

新增警示查詢以傳送 Webhook 通知

您可以在 vRealize Log Insight 中設定警示查詢，以在記錄中顯示特定資料時將 Webhook 通知傳送到遠端 Web 伺服器。Webhook 會透過 HTTP POST 提供事件通知。

備註 伺服器可能會報告成功或失敗。vRealize Log Insight 會在失敗時重試。vRealize Log Insight 會將所有 HTTP/2xx 狀態碼回應視為成功。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。

先決條件

- 確認您已登入 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。
- 確認已將 Web 伺服器設定可接收 Webhook 通知。

程序

- 1 導覽至 **互動式分析** 索引標籤。
- 2 從 **搜尋** 按鈕右側的 **建立或管理警示** 功能表中，按一下 ，然後選取 **從查詢建立警示**。
- 3 在 **[新增警示]** 對話方塊中，輸入警示的名稱，並提供觸發該警示之事件的簡短而有意義的說明。
警示名稱和說明包含在 vRealize Log Insight 傳送的通知中。
- 4 選取 **Webhook** 核取方塊，並輸入您想要 vRealize Log Insight 向其傳送通知的 URL。
- 5 設定警示臨界值。

警示類型	選擇
任何相符項	選取 在任何相符項上 選項。 每隔 5 分鐘執行一次查詢。
根據事件類型	選取 過去 <time period> 內第一次看到新的事件類型時 選項，然後從下拉式功能表中選取時間。 每隔 5 分鐘執行一次查詢。
根據一段時間內的事件數目	選取第三個選項，然後使用下拉式功能表設定參數。 根據下拉式功能表中的選擇執行查詢。
根據圖表值	選取第四個選項，然後使用下拉式功能表設定參數。 備註 僅當您選取根據至少一個欄位分組事件時，此警示類型才可用。您無法針對僅視覺化時間序列的圖表建立此警示類型。 根據第二個下拉式功能表中的選擇執行查詢。

預覽圖表中的橙色行將顯示目前臨界值。

- 6 按一下 **儲存**。

下一個

您可以啟用、停用或刪除已儲存的警示。

備註 警示查詢特定於使用者。您只能管理自己的警示。您必須獲指派為超級管理員角色，才能管理其他使用者警示。

關於撰寫 vRealize Log Insight 警示的轉譯填充碼

填充碼是用於對應不同的 Webhook 格式。

vRealize Log Insight 會以自己的專有格式傳送 Webhook，而協力廠商解決方案希望傳入的 Webhook 可以是它們的專有格式。這表示協力廠商解決方案必須具備 vRealize Log Insight 格式的原生支援，或者需要能在 vRealize Log Insight 和協力廠商解決方案之間將 vRealize Log Insight 格式轉譯為協力廠商格式的填充碼。

下圖顯示使用者警示查詢和為其產生的 Webhook。您可以使用此資訊深入了解支援填充碼所需的對應。

圖 1-1 使用者定義的警示查詢

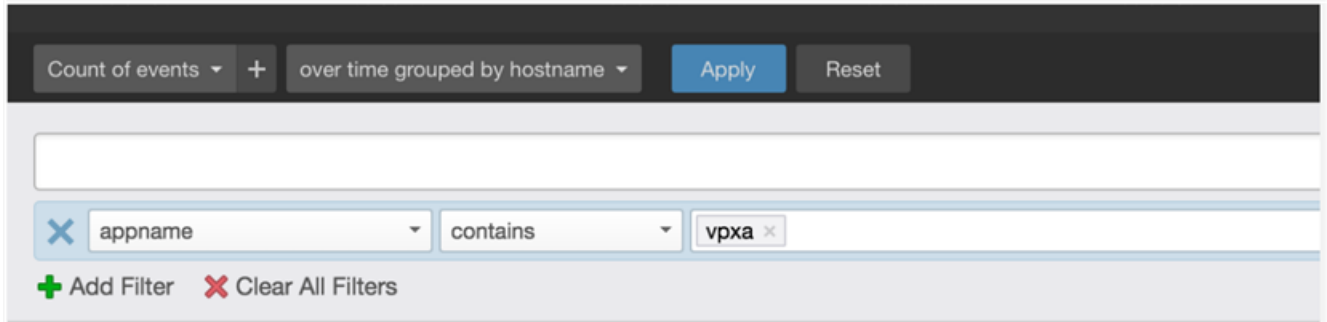


圖 1-2 使用者警示彙總查詢的 Webhook 輸出

```
{
  "AlertType":1,
  "AlertName":"ESXi Vpxa Alert",
  "SearchPeriod":300000,
  "HitCount":0.0,
  "HitOperator":2,
  "messages":[
    {
      "text":"2016-06-24T15:42:42.055Z esx01 Vpxa: [4845FB90 verbose 'VpxaHalCnxHostagent' opID=WFU-
dcfc2d3a] [WaitForUpdatesDone] Starting next WaitForUpdates() call to hostd",
      "timestamp":1451940578545,
      "fields":[
        {
          "name":"hostname",
          "content":"esx01"
        },
        {
          "name":"appname",
          "content":"vpxa"
        }
      ]
    },
    {
      "text":"2016-06-24T15:42:42.055Z esx02 Vpxa: [4845FB90 verbose 'vpxavpxaInvntVm' opID=WFU-
dcfc2d3a] [VpxaInvntVmChangeListener] Guest DiskInfo Changed",
      "timestamp":1451940561008,
      "fields":[
        {
          "name":"hostname",
          "content":"esx02"
        }
      ]
    }
  ]
}
```

```

        "name": "appname",
        "content": "vpxa"
    }
]
}
],
"HasMoreResults": false,
"Url": "https://10.11.12.13/s/8pgzq6",
"EditUrl": "https://10.11.12.13/s/56monr",
"Info": "This is an alert for all the 'ESXi Vpxa' messages",
"NumHits": 2
}

```

使用者警示訊息查詢的 Webhook 格式

vRealize Log Insight Webhook 所使用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。

當您傳送使用者警示訊息查詢所產生的警示給協力廠商程式時，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。

使用者警示訊息查詢 Webhook 格式

下列範例顯示使用者警示訊息查詢的 vRealize Log Insight Webhook 格式。

```

{
  "AlertType": 1,
  "AlertName": "Hello World Alert",
  "SearchPeriod": 300000,
  "HitCount": 0.0,
  "HitOperator": 2,
  "messages": [
    {
      "text": "hello world 1",
      "timestamp": 1451940578545,
      "fields": [
        {
          "name": "Field_1",
          "content": "Content 1"
        },
        {
          "name": "Field_2",
          "content": "Content 2"
        }
      ]
    },
    {
      "text": "hello world 2",
      "timestamp": 1451940561008,
      "fields": [
        {
          "name": "Field_1",
          "content": "Content 1_2"
        }
      ]
    }
  ]
}

```

```

        {
            "name": "Field_2",
            "content": "Content 2_2"
        }
    ]
}
],
"HasMoreResults": false,
"Url": "https://10.11.12.13/s/8pgzq6",
"EditUrl": "https://10.11.12.13/s/56monr",
"Info": "This is an alert for all the 'Hello World' messages",
"NumHits": 2
}

```

使用者警示彙總查詢的 Webhook 格式

vRealize Log Insight Webhook 所使用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。

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。

使用者警示彙總查詢的 Webhook 格式

```

{
    "AlertType": 2,
    "AlertName": "field_1 aggregated alert",
    "SearchPeriod": 300000,
    "HitCount": 2.0,
    "HitOperator": 2,
    "messages": [
        {
            "fields": [
                {
                    "name": "Field_1",
                    "content": "Content 1"
                }
            ]
        }
    ],
    "HasMoreResults": false,
    "Url": "https://10.11.12.13/s/r25g3s",
    "EditUrl": "https://10.11.12.13/s/n3gsed",
    "Info": null,
    "NumHits": 1
}

```

檢視警示查詢

您可以檢視已建立的警示查詢，並檢查是否已啟用這些查詢的通知。

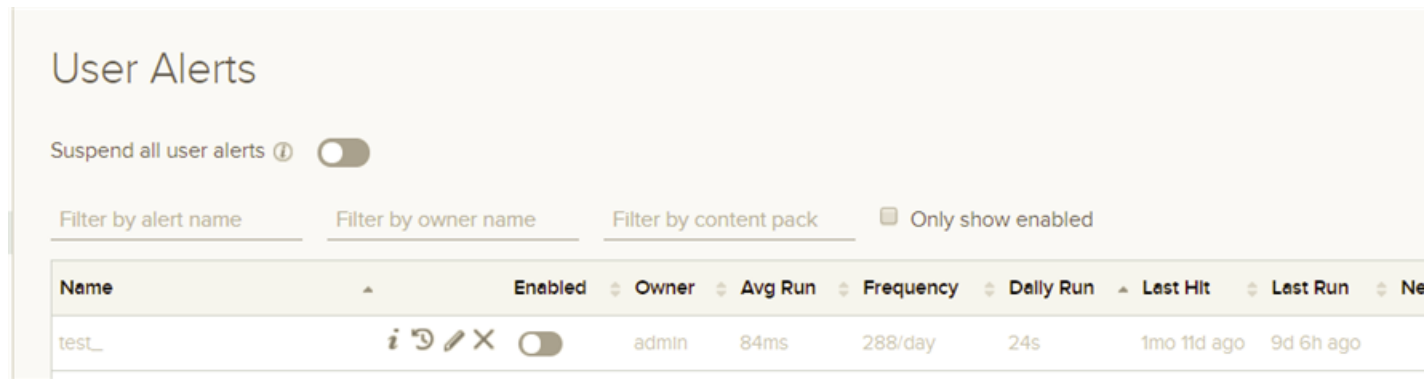
使用**使用者警示**視窗做為起點，以檢視和管理您以使用者身分建立的警示。在此視窗中，您可以監控警示的活動和檢視警示歷程，以及管理您的警示。您可以執行下列工作：

- 啟用或停用所有警示或個別警示
- 依警示名稱、擁有者名稱或內容套件進行警示的排序
- 變更警示的參數
- 刪除警示

使用工具提示說明進一步瞭解畫面上的每個圖示。

備註 警示查詢特定於使用者。您只能管理自己的警示。您必須獲指派為超級管理員角色，才能管理其他使用者警示。

圖 1-3 使用者警示



第一次命中發生之前，[上次命中時間] 欄中的值會保持為 **never**。

先決條件

確認您已登入 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 按一下組態下拉式功能表圖示 ，然後選取**管理**。
- 2 在左側功能表的 [管理] 區段中，按一下**使用者警示**。

您會看到所有警示查詢的清單。警示通知的狀態顯示在警示名稱下。

下一個

您可以按一下清單中的警示查詢，以修改其參數或刪除不再需要的查詢。

內容套件警示查詢為唯讀。若要儲存對內容套件警示所做的變更，您必須將警示儲存到您的自訂內容。

修改警示查詢

您可以變更警示查詢的觸發器、啟用或停用查詢傳送的通知，或者變更通知方法 (電子郵件、Webhook，或傳送至 vRealize Operations Manager)。

備註 警示查詢特定於使用者。您只能管理自己的警示。您必須獲指派為超級管理員角色，才能管理其他使用者警示。

內容套件警示查詢為唯讀。若要儲存對內容套件警示所做的變更，您必須將警示儲存到您的自訂內容。

您可以將變更同時套用至一或多個警示。

先決條件

- 確認您已登入 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。
- 確認管理員已將 SMTP 設定為啟用電子郵件通知。請參閱[為 Log Insight 設定 SMTP 伺服器](#)。
- 確認管理員已將 vRealize Log Insight 和 vRealize Operations Manager 之間的連線設定為啟用警示整合。請參閱[設定 Log Insight 以將通知事件傳送至 vRealize Operations Manager](#)。
- 如果您是使用 Webhook，請確認已將 Web 伺服器設定為接收 Webhook 通知。

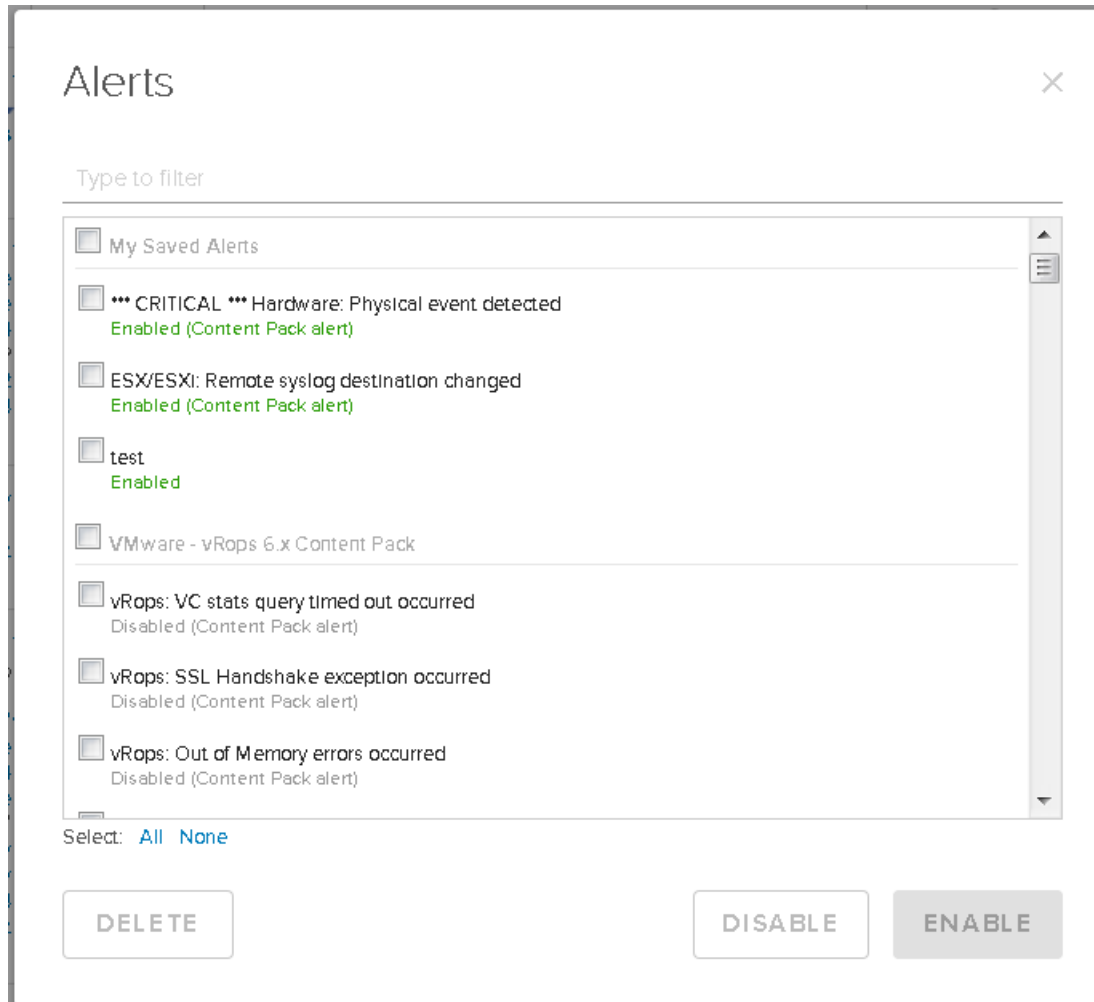
程序

- 1 導覽至[互動式分析](#)索引標籤。
- 2 從[搜尋](#)按鈕右側的[建立或管理警示](#)功能表中，按一下 ，然後選取[管理警示](#)。

- 3 在 [警示] 清單中，選取要修改的一或多個警示查詢，然後視需要變更查詢參數。

您可以輸入字串做為篩選器來尋找查詢。查詢會加上已啟用或已停用以及是否為內容套件查詢的標籤。

備註 如果取消選取所有通知選項，則警示查詢會停用。



- 4 儲存您的變更。

選項	說明
儲存	當您修改自己的警示時，會顯示此按鈕。
儲存到我的警示	當您修改共用警示或內容套件警示時，會顯示此按鈕。原始警示保持不變，而是將該警示的複本儲存到您的自訂內容。

啟用警示查詢

停用警示查詢後，vRealize Log Insight 不會傳送電子郵件或 Webhook 通知，並且不會觸發 vRealize Operations Manager 通知事件。

備註 警示查詢特定於使用者。您只能管理自己的警示。您必須獲指派為超級管理員角色，才能管理其他使用者警示。

警示查詢在下列條件下停用。


- 當您停用 [編輯警示] 對話方塊中的所有通知選項時。
- 當警示為內容套件的一部分時。

內容套件警示查詢為唯讀。若要儲存對內容套件警示所做的變更，您必須將警示儲存到您的自訂內容。

先決條件

- 確認您已登入 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。
- 確認管理員已將 SMTP 設定為啟用電子郵件通知。請參閱 [Log Insight 設定 SMTP 伺服器](#)。
- 確認管理員已將 vRealize Log Insight 和 vRealize Operations Manager 之間的連線設定為啟用警示整合。請參閱 [設定 Log Insight 以將通知事件傳送至 vRealize Operations Manager](#)。

程序

- 1 導覽至 **互動式分析** 索引標籤。
- 2 從 **搜尋** 按鈕右側的 **建立或管理警示** 功能表中，按一下 ，然後選取 **管理警示**。
- 3 在 [警示] 清單中，按一下您要啟用的一或多個警示查詢。
- 4 選取您想要啟用的通知選項，並提供必要參數。

選項	說明
電子郵件	在文字方塊中至少輸入一個電子郵件地址。使用逗點分隔多個地址。
Webhook	輸入您要 vRealize Log Insight 向其傳送通知的 URL。
傳送至 vRealize Operations Manager	選取與通知事件相關聯的 vRealize Operations Manager 資源，然後選取事件的嚴重度層級。

- 5 儲存您的變更。

選項	說明
儲存	當您修改自己的警示時，會顯示此按鈕。
儲存到我的警示	當您修改共用警示或內容套件警示時，會顯示此按鈕。原始警示保持不變，而是將該警示的複本儲存到您的自訂內容。

當警示查詢傳回與警示準則相符的結果時，vRealize Log Insight 會根據您的組態傳送通知。

範例 1-7. 從 VMware - vSphere 內容套件啟用警示

VMware - vSphere 內容套件包含多個預先定義的警示查詢，包括 **vCenter Server: ESX/ESXi 停止記錄** 警示。

啟用 **vCenter Server: ESX/ESXi 停止記錄** 警示是一種比較好的做法，因為當您重新啟動 vRealize Log Insight 時，某些版本的 ESXi 主機可能會停止傳送 syslog 資料。此警示會監控 vCenter Server 事件 `esx.problem.vmsyslogd.remote.failure`，以偵測是否存在停止傳送 syslog 摘要的 ESXi 主機。

- 1 在 **互動式分析** 索引標籤上，展開 **搜尋** 按鈕右側的下拉式功能表，然後選取 **管理警示**。
- 2 在 VMware - vSphere 內容套件下，按一下 **vCenter Server: ESX/ESXi 停止記錄**。
- 3 啟用電子郵件通知、Webhook 通知或 vRealize Operations Manager 通知事件。
- 4 按一下 **儲存至 [我的警示]**。

若要僅偵測停止向 vRealize Log Insight 執行個體傳送摘要的 ESXi 主機，您可以將下列篩選器新增到警示查詢：**vc_remote_host (VMware - vSphere)** 包含 `<log-insight-hostname>`，然後將新的查詢儲存到警示中。

如需關於 syslog 問題和解決方案的詳細資料，請參閱知識庫文章《VMware ESXi 5.x 主機停止向遠端伺服器傳送 syslog (2003127)》，位於 <https://kb.vmware.com/kb/2003127>。

刪除警示查詢



當您不再需要警示查詢時，可以將其刪除。

備註 警示查詢特定於使用者。您只能管理自己的警示。您必須獲指派為超級管理員角色，才能管理其他使用者警示。

先決條件

確認您已登入 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 **互動式分析** 索引標籤。
- 2 從 **搜尋** 按鈕右側的功能表，按一下  並選取 **管理警示**。
- 3 選取一或多個要刪除的警示，然後按一下 **刪除** 或刪除圖示 .
- 4 在 **刪除警示** 對話方塊中，選取 **刪除** 以確認動作。