Sentinel™

安裝與組態指南

2018 年 7 月

法律聲明

有關 NetIQ 法律聲明、免責聲明、擔保聲明、出口或其他限制、美國政府限制權限、專利政策及 FIPS 法規遵循的相關資訊，請參閱 http://www.netiq.com/company/legal/。

Copyright © 2018 NetIQ Corporation.版權所有。

如需 NetIQ 註冊商標相關資訊，請參閱 http://www.netiq.com/company/legal/。所有的協力廠商商標均為其個別擁有廠商的財產。

關於本書和文件庫

《*安裝與組態指南*》提供了 Sentinel 的介紹，並說明如何安裝及設定 Sentinel。

預定對象

本指南適用於 Sentinel 管理員和顧問。

文件庫其他資訊

文件庫提供下列資訊資源：

管理指南

提供管理 Sentinel 部署所需的管理資訊和任務。

使用者指南

提供 Sentinel 相關概念性資訊。本書也提供使用者介面綜覽，以及許多任務的逐步指導。

瞭解 Sentinel

本節提供 Sentinel 相關詳細資訊，以及 Sentinel 如何為您的組織提供事件管理解決方案。

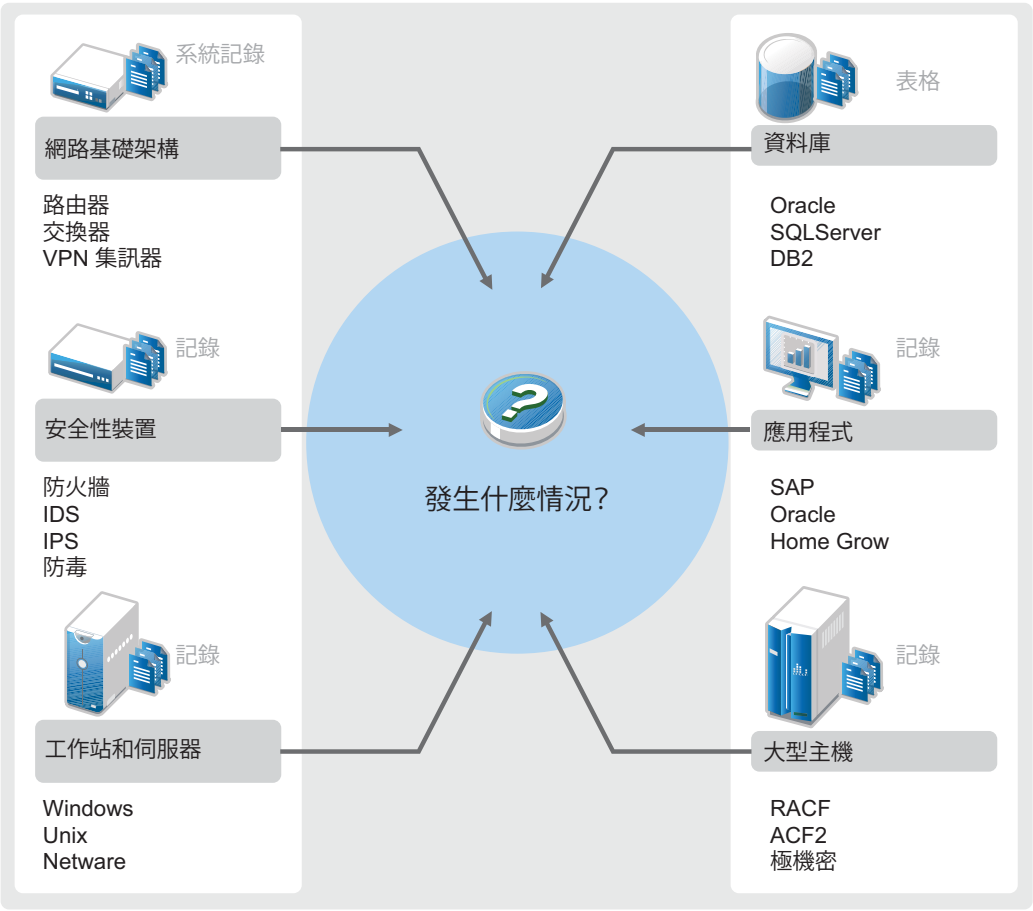
1 Sentinel 是什麼？

Sentinel 是一款安全資訊和事件管理 (SIEM) 解決方案，同時也是一款法規遵循監控解決方案。Sentinel 能自動監控最複雜的 IT 環境，並且提供保護 IT 環境所需的安全措施。

保護 IT 環境的難題

環境的複雜度使 IT 環境的保護成為一項難題。一般而言，您的 IT 環境中有許多應用程式、資料庫、大型主機、工作站與伺服器，這些實體全部會產生事件的記錄。您的安全裝置與網路基礎架構裝置也可能產生您 IT 環境中各種事件的記錄。

圖 1-1 環境中發生的事件



挑戰因為下列情況而升溫：

- IT 環境中的裝置太繁雜。

- 記錄以不同格式寫成。
- 記錄會儲存在不同的位置中。
- 在記錄檔案中擷取的資料量相當大。
- 若不經過手動分析記錄檔案，便無法判斷事件觸發情況。

為讓記錄中的資訊發揮效用，您必須能執行下列動作：

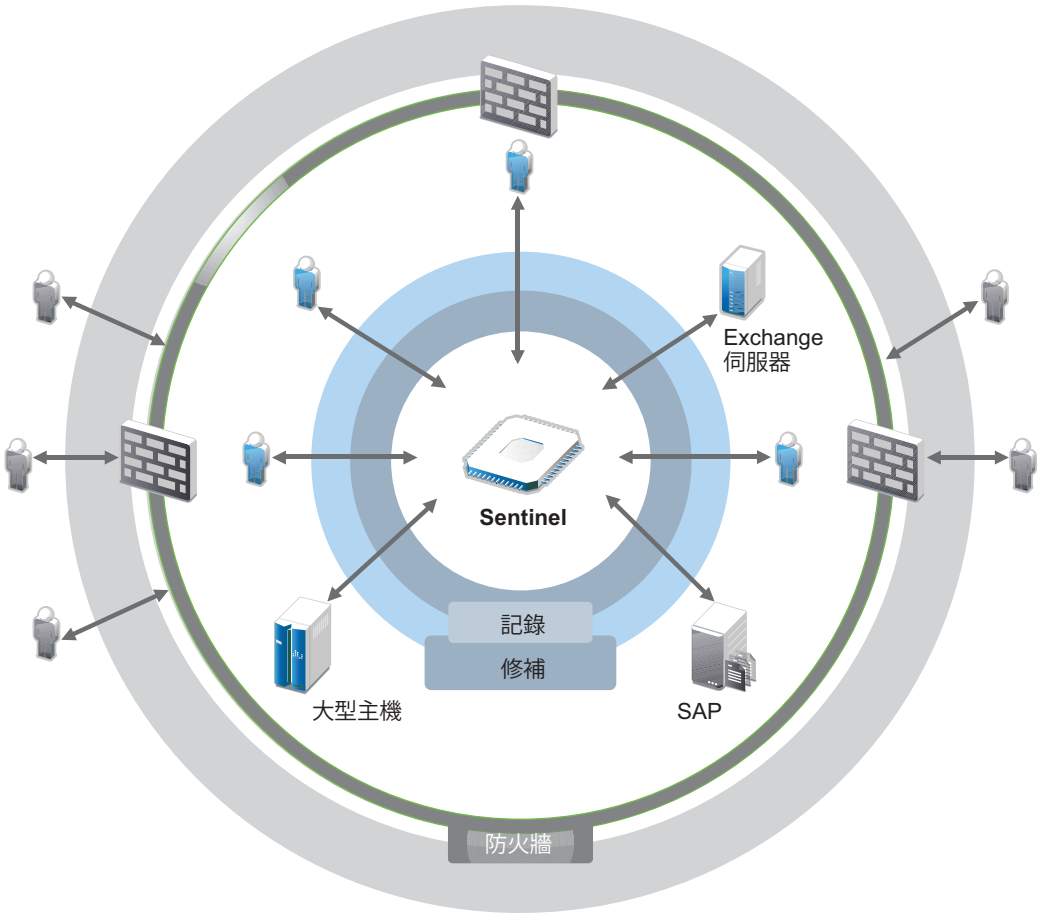
- 收集資料。
- 整合資料。
- 將不同的資料標準化到您可以輕鬆比較的事件中。
- 將事件對應至標準法規。
- 分析資料。
- 比對多個系統間的事件以判斷是否有安全問題。
- 當資料未遵循規範時傳送通知。
- 針對通知採取動作，以遵守公司規則。
- 產生報告以證明遵循法規。

在您瞭解保護 IT 環境所面臨的挑戰後，您必須決定如何在不影響使用者體驗的情況下，保護企業與使用者。Sentinel 能提供問題的解決方案。

Sentinel 提供的解決方案

Sentinel 能扮演企業安全性的中樞神經系統。其能收集整個基礎架構中的資料，包括應用程式、資料庫、伺服器、儲存裝置及安全性裝置。它能分析資料並產生關連，讓您可以自動或手動對資料執行動作。

圖 1-2 Sentinel 提供的解決方案



有了 Sentinel，您可以得知 IT 環境內於任何指定時間點發生的事件，也能將針對資源採取的動作與採取動作的人員連結在一起。這可讓您決定使用者行為，並有效地監控活動來防止惡意行為。

Sentinel 達成方式如下：

- 提供單一解決方案解決多種安全標準之間的 IT 控管問題。
- 消弭 IT 環境中預期發生與實際發生之間的落差。
- 幫助您符合安全標準。
- 提供立即可用的法規遵循監控和報告程式。

Sentinel 可自動化記錄收集、分析和報告程序，以確保 IT 控制能有效支援威脅偵測與稽核要求。Sentinel 也提供安全性事件、法規遵循事件及 IT 控制等作業的自動化監控。如果有安全缺口或不遵循法規的事件，其允許您立即採取動作。Sentinel 也允許收集您環境的摘要資訊，並與重要的利益相關者共享。

2 Sentinel 如何運作

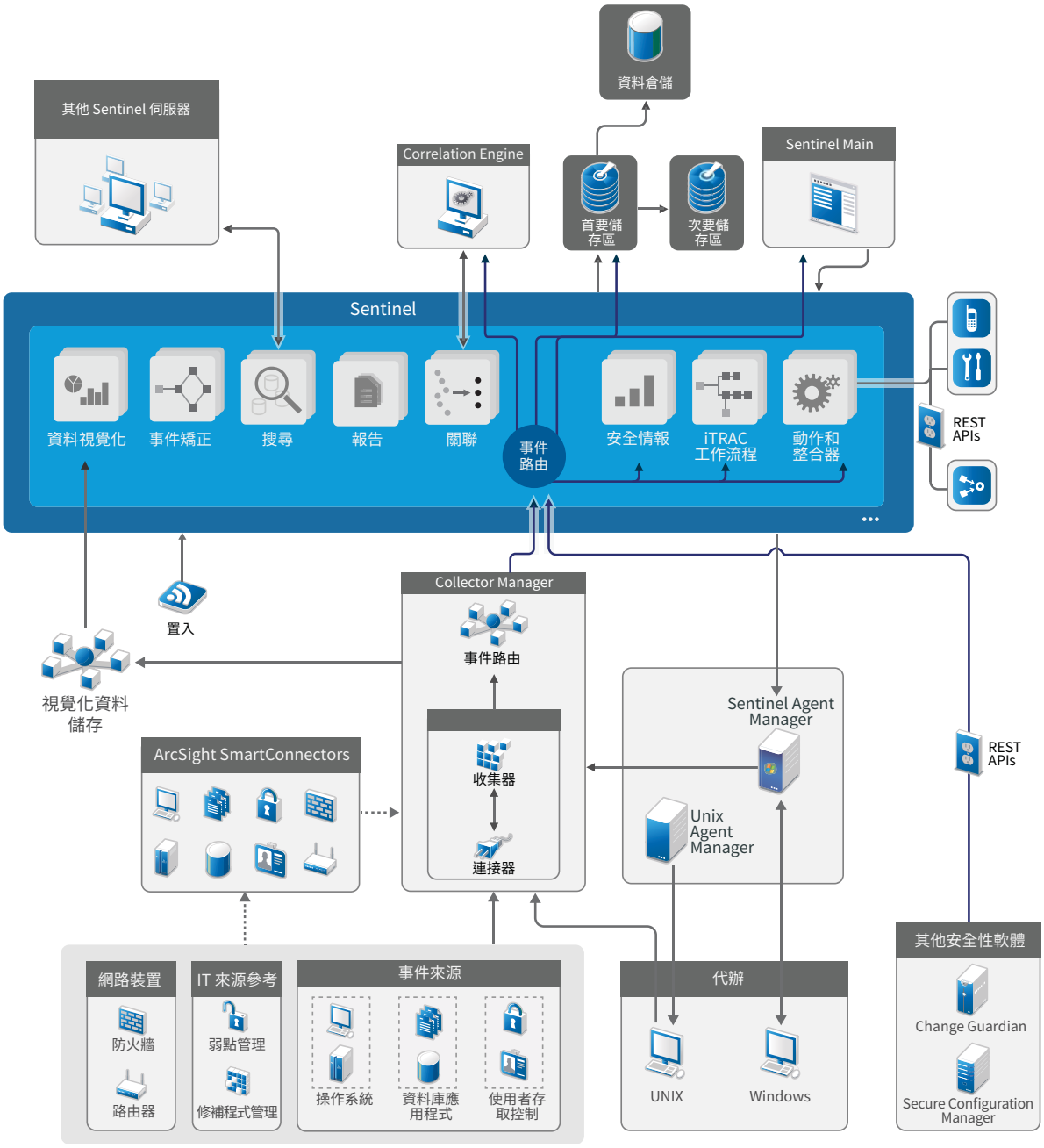
Sentinel 能持續管理 IT 環境中的安全性資訊和事件，提供全方位的監控解決方案。

Sentinel 進行下列動作：

- 從 IT 環境中各個不同的來源收集記錄、事件及安全性資訊。
- 將收集來的記錄、事件及安全性資訊標準化，使其成為標準的 Sentinel 格式。
- 在具有彈性且可自定之資料保留規則的檔案式資料儲存或 Hadoop 式可擴充儲存中儲存事件。
- 收集 IP 流程資料並協助您詳細監看網路活動。
- 提供以階層方式連結多個 Sentinel 系統的能力，包括 Sentinel Log Manager。
- 能讓您搜尋本地 Sentinel 伺服器上的事件，也能搜尋散佈全球的其他 Sentinel 伺服器上的事件。
- 執行能讓您定義基線的統計分析，接著再比對基線和發生的事件，以判斷是否有潛藏的問題。
- 使特定期間內一組類似或可比較的事件相互關連，以判斷出模式。
- 將事件 (event) 組織為事件 (incident)，以獲得有效的回應管理和追蹤能力。
- 提供以即時和歷程事件為基礎的報告。

下圖說明 Sentinel 如何與傳統儲存搭配運作，為您提供資料儲存選項：

圖 2-1 Sentinel 架構



以下各節會詳細說明 Sentinel 元件：

- 「事件來源」(第 21 頁)
- 「Sentinel 事件」(第 21 頁)
- 「Collector Manager」(第 23 頁)
- 「ArcSight SmartConnectors」(第 24 頁)
- 「Agent Manager」(第 24 頁)
- 「Sentinel 資料路由和資料儲存」(第 24 頁)

事件來源

Sentinel 會從 IT 環境內的各種來源收集安全性資訊和事件。這些來源稱為「事件來源」。一般而言，以下為您網路的事件來源：

安全性周邊： 安全裝置，包括為您的環境建立安全週邊的硬體與軟體，例如防火牆、入侵偵測系統 (IDS) 及虛擬私有網路 (VPN)。

作業系統： 在網路中執行的各種作業系統。

參考 IT 來源： 用來維護及追蹤資產、修補程式、組態及弱點的軟體。

應用程式： 安裝在網路中的各種應用程式。

使用者存取控制： 允許使用者存取公司資源的應用程式或裝置。

如需從事件來源收集事件的詳細資訊，請參閱《「 Sentinel 管理指南」》中的「*收集與路由事件資料*」。

Sentinel 事件

Sentinel 會從設備接收資料，將此資訊標準化成稱為事件的結構、將事件分類，然後傳送事件以進行處理。

事件代表協力廠商安全性裝置、網路或應用程式裝置，或內部 Sentinel 來源向 Sentinel 報告的標準化記錄。事件具有數種類型：

- 外部事件 (從安全性裝置接收的事件)，例如：
  - 入侵偵測系統 (IDS) 偵測到的攻擊
  - 由作業系統報告的成功登入
  - 客戶定義的情況，例如使用者存取檔案
- 內部事件 (Sentinel 產生的事件)，包括：
  - 已停用的關連規則
  - 資料庫已滿

Sentinel 將類別資訊 (分類) 新增至事件，可輕鬆地在以不同方式報告事件的系統之間比較事件。即時顯示、Correlation Engine、儀表板及後端伺服器是負責處理事件的程序。

事件包含超過 200 個欄位；事件欄位有不同的類型及不同的用途。諸如安全性、嚴重性、目的地 IP 位址及目的地連接埠等即為一些預先定義的欄位。

有兩組可設定的欄位：

- 保留的欄位：供 Sentinel 內部使用，以允許在未來擴充功能。
- 客戶欄位：供客戶使用以允許自定。

欄位來源可以是外部或參考的：

- 外部欄位的值可依裝置或對應的收集器明確地設定。例如，您可以將欄位定義為建置碼，以供含有做為事件目的地 IP 位址之資產的建置之用。
- 透過映射服務，參考欄位的值能以一或多個其他欄位之函數的形式加以運算。例如，您可以利用事件目的地 IP 位址，並透過使用客戶定義映射的映射服務來計算欄位。

- 「映射服務」(第 22 頁)
- 「串流映射」(第 22 頁)
- 「入侵偵測」(第 22 頁)

映射服務

映射服務會將業務相關性資料在整個系統中傳播。此資料可使用參考資訊讓事件更豐富。

您可以使用映射，將主機和身分資訊等額外資訊新增至從來源裝置收到的事件，讓事件內容更為豐富。Sentinel 可使用此額外的資訊進行進階的關連與報告。Sentinel 支援數個內建映射，以及自定的使用者定義映射。

在 Sentinel 中定義的映射會以兩種方式儲存：

- 內建映射會儲存在資料庫中，進行內部更新，並自動匯出至映射服務。
- 自訂映射會以 CSV 檔案格式儲存，並在檔案系統中或透過使用映射資料組態使用者介面進行更新，然後由映射服務載入。

在這兩種情況中，CSV 檔案都會保留在 Sentinel 中央伺服器中，但映射的變更會分散到每個 Collector Manager 並在本機套用。這種分散式處理方式可確保映射活動不會造成主伺服器超載。

串流映射

映射服務採用動態更新模型，能將某一點的映射串流至另一個點，避免在動態記憶體中累積大量靜態映射。這與如 Sentinel 等關鍵任務且即時的系統有關，這類系統需要資料移動方式是穩定、可預測且敏捷，但與系統的任何暫時性負載無關。

入侵偵測

Sentinel 提供交互參考事件資料簽名和弱點掃描器資料的能力。當發現有弱點的系統遭受入侵時，Sentinel 會立即自動通知使用者。Sentinel 透過下列功能達成：

- Advisor 饋送
- 入侵偵測

- 弱點掃描
- 防火牆

Advisor 饋送包含與漏洞和威脅有關的資訊，以及經過標準化的事件簽名和弱點外掛程式。此外也能夠在事件資料簽名和弱點掃描器資料之間進行交互參考。如需有關 Advisor 饋送的詳細資訊，請參閱《「 Sentinel 管理指南 」》中的「*偵測弱點和入侵*」。

Collector Manager

Collector Manager 可管理資料收集、監控系統狀態訊息，並執行事件篩選。Collector Manager 的主要功能包括以下所列：

- 使用連接器收集資料。
- 剖析及標準化使用收集器收集的資料。

收集器

收集器會從連接器收集資訊並予以標準化。其可執行的功能如下：

- 接收來自連接器的原始資料。
- 剖析及標準化資料：
  - 將事件來源特有的資料轉譯為 Sentinel 特有的資料。
  - 以 Sentinel 可讀取的格式變更事件中的資訊，讓事件更加豐富。
  - 事件的事件-來源特有過濾。
- 透過映射服務將業務相關性新增至事件：
  - 將事件映射至身分。
  - 將事件映射至資產。
- 路由事件。
- 將經過標準化、剖析及格式化的資料傳遞至 Collector Manager。
- 將狀態訊息傳送至 Sentinel 伺服器。

如需關於收集器的詳細資訊，請參閱 Sentinel 外掛程式網站。

連接器

連接器能提供事件來源和 Sentinel 系統間的連接。

連接器提供下列功能：

- 將原始事件資料從事件來源傳輸至收集器。
- 連接特定的過濾。
- 連接錯誤處理。

ArcSight SmartConnectors

Sentinel 可使用 ArcSight SmartConnector 從 Sentinel 未直接支援的各種事件來源類型收集事件。SmartConnector 會從支援的裝置收集事件、將事件標準化為一般事件格式 (CEF)，並透過 Syslog 連接器將其轉送至 Sentinel。接著，連接器會將事件轉送至 Universal Common Event Format Collector，以進行剖析。

如需關於透過 SmartConnector 設定 Sentinel 的詳細資訊，請參閱 Sentinel 外掛程式網站上的「Universal Common Event Format Collector」文件。

Agent Manager

Agent Manager 提供主機式資料收集，補足無代理程式之資料收集，可讓您執行下列任務：

- 存取不供整個網路使用的記錄檔。
- 在受到嚴密控制的網路環境中操作。
- 透過限制重要伺服器上的攻擊表面，改善安全性情況。
- 在網路中斷期間增強資料收集的可靠性。

Agent Manager 允許您部署代理程式、管理代理程式組態，並擔任 Sentinel 事件流程的集合點。如需有關 Agent Manager 的詳細資訊，請參閱 Agent Manager 文件。

Sentinel 資料路由和資料儲存

Sentinel 針對路由、儲存和解壓縮所收集的資料提供多種選項。依預設，Sentinel 會從 Collector Manager 接收剖析過的事件資料與原始資料。Sentinel 會儲存原始資料，以提供安全的證據鏈，並根據您定義的規則，路由已剖析的事件資料。您可以過濾已剖析的事件資料、將其傳送至儲存位置或進行即時分析，並路由到外部系統。Sentinel 會進一步符合所有傳送至儲存裝置至使用者定義保留原則的事件資料。當事件資料應從系統刪除時，保留原則會控制刪除程序。

根據每秒事件量 (EPS) 率和部署需求，您可以選擇使用傳統檔案式資料儲存或 Hadoop 式可擴充儲存作為資料儲存選項。如需詳細資訊，請參閱「資料儲存考量」(第 39 頁)。

事件視覺化

Sentinel 提供事件視覺化功能，以圖表、表格和圖說對應方式來呈現資料。這些視覺化可簡化對大量事件進行視覺化和分析的工作，包括 IP 流程事件。您也可以建立自己的視覺化和儀表板。

在使用可擴充儲存的 Sentinel 中，依預設會提供事件視覺化功能。在傳統儲存設定中，只有在已啟用視覺化資料儲存庫 (Elasticsearch) 來儲存資料及編製其索引時，才可使用事件視覺化。如需關於啟用 Elasticsearch 的詳細資訊，請參閱「設定視覺化資料儲存庫」(第 41 頁)。

關連

單一事件看起來可能不重要，但與其他事件結合時，可能會警告您有潛在的問題。Sentinel 能藉由使用您建立及部署於 Correlation Engine 中的規則，協助您將這類型的事件相互關連，並採用適當的動作來緩和所有問題。

關連性會自動分析收到的事件資料流，以找出所需的模式，為安全性事件管理增加智慧。您可使用關連來定義規則以識別嚴重威脅和複雜的攻擊模式，以便您按優先順序來處理事件並進行有效的事件管理和回應作業。如需關連的詳細資訊，請參閱《「 Sentinel 使用者指南」》中的「*使事件資料相關連*」。

若要根據關連規則監控事件，您必須在 Correlation Engine 中部署規則。當發生符合規則準則的事件時，Correlation Engine 會產生說明該模式的關連事件。如需詳細資訊，請參閱《「 Sentinel 使用者指南」》中的「*Correlation Engine*」。

安全性智慧

Sentinel 的關連功能讓您能夠尋找活動的已知模式，您可以針對安全性、遵循法規或任何其他理由來分析該模式。安全性智慧功能會找出異常的活動，這些活動可能是惡意的，但卻不符合任何已知的模式。

Sentinel 中的安全性智慧功能著重於統計分析時間序列資料，使分析師得以藉由可人工解讀的自動化統計引擎或以視覺呈現的統計資料來識別及分析異常。如需詳細資訊，請參閱「《 Sentinel 使用者指南》」中的「*分析資料中的趨勢*」。

事件矯正

Sentinel 提供自動的事件回應管理系統，可讓您將追蹤、提報和回應事件與違反規則的程序作成記錄並形式化。此外也能夠與疑難票證系統主行雙向整合。Sentinel 可讓您即時回應，以有效率的方式解決事件。如需詳細資訊，請參閱《「 Sentinel 使用者指南」》中的「*設定事件*」。

iTrac 工作流程

iTRAC 工作流程提供簡單而彈性的解決方案，以供自動化及追蹤企業的事件回應程序。iTRAC 運用 Sentinel 的內部事件系統來追蹤從識別 (透過關連規則或手動識別) 到解決等各階段的安全性問題或系統問題。

您可以使用手動與自動步驟建立流程。iTrac 工作流程支援進階功能，例如分支、以時間為基準的提升，以及本機變數。並且整合外部程序檔和外掛程式，讓您可以與協力廠商系統進行彈性的互動。全方位的報告可讓管理員瞭解及微調事件回應程序。如需詳細資訊，請參閱「《 Sentinel 使用者指南》」中的「*設定 iTRAC 工作流程*」。

動作與整合器

「動作」能執行某些類型的手動或自動作業，例如傳送電子郵件。您可以透過路由規則、手動執行事件或事件操作，以及關連規則，來觸發動作。Sentinel 會提供預先設定的動作清單。您可以使用預設動作，然後依需求重新設定，或可加入新動作。如需詳細資訊，請參閱《「 Sentinel 管理指南」》中的*「設定動作」*。

動作可自行執行，或可使用透過整合器外掛程式設定的整合器例項執行。整合器外掛程式延伸了 Sentinel 矯正動作的功能和性能。整合器提供連接到外部系統 (例如 LDAP、SMTP 或 SOAP 伺服器) 執行動作的能力。如需詳細資訊，請參閱《「 Sentinel 管理指南」》中的「*設定整合器*」。

搜尋

Sentinel 提供執行事件搜尋的選項。運用需要的組態，您也可搜尋 Sentinel 產生的系統事件，並檢視該事件的原始資料。如需詳細資訊，請參閱「《 Sentinel 使用者指南》」中的*「搜尋事件」*。

您也可以搜尋分散至不同地理位置的 Sentinel 伺服器。如需詳細資訊，請參閱「《 Sentinel 管理指南》」中的*「設定資料聯盟」*。

報告

Sentinel 讓您能針對收集而得的資料進行報表分析。Sentinel 已預先封裝各種可自定報告。某些報告是可設定的，能讓您指定要顯示在結果中的欄。

您可以執行、排程及以電子郵件傳送 PDF 格式的報告。您也能以搜尋的形式執行任何報告，然後再像操作搜尋一般採用結果 (例如，使搜尋結果更精簡或針對結果執行動作)。您也可以針對散佈在不同地理位置的 Sentinel 伺服器執行報告。如需詳細資訊，請參閱「《 Sentinel 使用者指南》」中的*「報告」*。

身分追蹤

Sentinel 提供了整合架構供識別管理系統，追蹤每個使用者帳戶的身分，以及這些身分執行的事件。Sentinel 可提供使用者資訊，例如聯絡資訊、使用者帳戶、最近的驗證事件、最近的存取事件、許可變更等等。Sentinel 透過顯示啟始特定動作的使用者及動作所影響的使用者其相關資訊，來改善事件回應時間並啟用以行為為基準的分析。如需詳細資訊，請參閱《「 Sentinel 使用者指南」》中的「*運用身分資訊*」。

事件分析

Sentinel 提供一組強大的工具，協助您輕鬆地尋找及分析關鍵事件資料。Sentinel 會將系統最佳化以提升任何類型分析的效率，並提供方法將某種類型的分析輕鬆地轉換成另一種類型，以進行順暢的轉換。

Sentinel 中的事件調查通常會從接近即時的事件檢視開始。雖然有進階工具可供使用，但事件檢視仍會顯示已過濾的事件資料流和摘要圖表，供您進行事件趨勢和事件資料的簡易快速分析，並識別特定事件。在經過一段時間之後，您就可以針對特定資料類別 (例如從關連性輸出) 增加已調整的過濾器。您可以將事件檢視做為儀表板使用，顯示完整的操作及安全性狀態。

然後使用互動式搜尋來執行事件的詳細分析。這可讓您快速且輕鬆地搜尋及尋找與特定查詢有關的資料，例如特定使用者或特殊系統的活動。您可以按一下事件資料或使用左邊的精簡窗格，快速搜尋相關的特定事件進行深入分析。

在分析數百個事件時，Sentinel 的報告功能可提供事件配置的自訂控制，並顯示大量的資料。Sentinel 可讓您將「搜尋」介面中累積的互動搜尋傳輸到報告範本，輕鬆地進行此轉換。這會立即建立顯示相同資料的報告，但報告採用更適合大量事件的格式。

Sentinel 包含許多種這類用途的報告範本。報告範本有兩種：

- 經微調可顯示特定類型資訊 (例如驗證資料或使用者建立) 的範本。
- 一般用途範本，允許您以互動的方式在報告上自訂群組與欄。

在經過一段時間後，您就可開發出常用的過濾器和報告以簡化您的工作流程。Sentinel 提供儲存這類資料並將其分送至組織內人員的支援。如需詳細資訊，請參閱*《Sentinel 使用者指南》*。

規劃 Sentinel 安裝

以下幾章將指導您規劃安裝 Sentinel。若您想要安裝的組態並未出現在下列各章，或有任何疑問，請聯絡 技術支援。

3 執行核對清單

使用下列核對清單規劃、安裝及設定 Sentinel。

如果您要從上一版的 Sentinel 升級，請不要使用此核對清單。若需有關升級的詳細資訊，請參閱 第 V 部分「升級 Sentinel」(第 135 頁)。

❒	任務	請參閱
❒	檢閱產品架構資訊，以瞭解 Sentinel 元件。	第 I 部分「瞭解 Sentinel」(第 13 頁)。
❒	檢閱 Sentinel 授權資訊，判斷您需要使用 Sentinel 試用版授權或企業授權。	第 4 章「瞭解授權資訊」(第 33 頁)。
❒	評估環境以決定硬體組態。確定安裝 Sentinel 和其元件的電腦符合指定要求。	第 5 章「符合系統需求」(第 37 頁)。
❒	根據每秒事件量 (EPS) 判斷您的環境所適用的部署類型。 判斷您需要安裝以改善效能和負載平衡的 Collector Manager 和 Correlation Engine 數目。	第 6 章「部署考量因素」(第 39 頁)。
❒	檢閱 Sentinel 版本說明，以瞭解新功能和已知的問題。	Sentinel 版本說明
❒	安裝 Sentinel。	第 III 部分「安裝 Sentinel」(第 67 頁)。
❒	設定 Sentinel。	第 IV 部分「設定 Sentinel 的組態」(第 107 頁)。
❒	Sentinel 包含立即可用的關連規則。部份關連規則預設為在規則觸發時執行傳送電子郵件的動作，例如通知安全性管理員動作。因此，您必須透過設定SMTP整合器以及傳送電子郵件動作，來設定 Sentinel 伺服器中的郵件伺服器設定。	Sentinel 外掛程式網站上的 SMTP 整合器和「傳送電子郵件」動作文件。
❒	視需求在環境中安裝其他收集器和連接器。	第 16 章「安裝額外的收集器和連接器」(第 103 頁)。
❒	視需求在環境中安裝其他 Collector Manager 和 Correlation Engine。	第 III 部分「安裝 Sentinel」(第 67 頁)。

4 瞭解授權資訊

Sentinel 包含各式各樣的功能以因應許多客戶的各種需求。您可以選擇符合您需求的授權模型。

Sentinel 平台提供下列兩種授權模型：

- **Sentinel Enterprise：** 具完整功能的解決方案，可使用所有核心即時視覺分析功能及許多額外功能。Sentinel Enterprise 著重於 SIEM 使用案例，例如即時威脅偵測、警示和矯正。
- **Sentinel for Log Management：** 記錄管理使用案例的解決方案，例如收集、儲存、搜尋和報告資料。

  Sentinel for Log Management 相較於 Sentinel Log Manager 1.2.2 功能提供了重大升級；在某些情況下，針對架構重要部分進行了修改。若要規劃升級至 Sentinel for Log Management，請參閱 Sentinel 常見問題頁面。

根據您購買的解決方案與附加產品，您可以購買適當的授權金鑰與授權，以啟用 Sentinel 內的適當功能。雖然授權金鑰與授權掌控了產品功能與下載的基本存取權，但您仍應參閱您購買合約與使用者授權合約中其他的條款與條件。

下表為各解決方案可用的特定服務與功能：

表格 4-1 *Sentinel 服務與功能*

服務與功能	Sentinel Enterprise	Sentinel for Log Management
核心功能 ◆ 事件集合、剖析、標準化和分類法分類 ◆ 非事件資料集合 (資產資料、弱點資料和使用者身分資料) ◆ 內部網路位置映射 ◆ 具有保留規則和不可否認性的事件儲存 ◆ 傳統儲存 (內部和外部) 的事件路由 ◆ 事件搜尋和視覺化 ◆ IP 流程收集、儲存和視覺化 ◆ 報告 ◆ 聯邦資訊處理標準?物 140-2 (FIPS 140-2) 促進 ◆ 手動觸發的動作 ◆ 事件的手動建立和管理	是	是
Sentinel Link	是	是
資料同步	是	是
自歸檔還原事件資料	是	是
資料聯盟 (分散式搜尋)	是	是

服務與功能	Sentinel Enterprise	Sentinel for Log Management
入侵偵測 (Advisor)*	是	是
可擴充儲存	是	是
關連 • 即時事件模式關連 • 關連規則觸發的動作 • 警示分級 • 警示視覺化	是	否
安全性智慧 • 異常規則 • 即時統計分析	是	否

*Advisor 是由 Security Nexus 提供技術支援的附加服務。您必須購買額外授權才能使用此服務。

Sentinel 授權

本節提供各種類型的 Sentinel 授權相關資訊。

- 「試用版授權」(第 34 頁)
- 「免費授權」(第 35 頁)
- 「企業授權」(第 35 頁)

試用版授權

預設的試用版授權可讓您在特定試用期間內使用所有 Sentinel Enterprise 功能，以及無限制的 EPS (視您的硬體性能而定)。如需有關 Sentinel Enterprise 功能的詳細資訊，請參閱 表格 4-1 「Sentinel 服務與功能」 (第 33 頁)。

系統的過期日會以系統中最舊的資料為基準。若您將舊事件還原至您的系統，Sentinel 將依此更新過期日。

試用版授權過期後，Sentinel 將以基本、免費授權執行，啟用有限的功能，且事件率上限為 25 EPS。僅適用於具有傳統儲存設定 Sentinel 的情況。

在可擴充儲存部署中，試用版授權過期後，Sentinel 將不再儲存事件和原始資料。

在您升級至企業授權後，Sentinel 將完整還原所有功能。為了避免造成功能中斷，請務必在試用版授權過期之前將系統升級為企業授權。

免費授權

免費授權可讓您使用有限的功能，且事件率上限為 25 EPS。免費授權僅適用於具有傳統儲存的 Sentinel。

免費授權可讓您收集和儲存事件。當事件率超過上限 25 EPS，Sentinel 將儲存接收到的事件，但不會在搜尋結果或報告中顯示這些事件的詳細資料。Sentinel 將以OverEPSLimit標記這些事件。

免費授權不提供即時功能。您可升級至企業授權以還原所有功能。

附註： 免費版的 Sentinel 未提供技術支援和產品更新。

企業授權

在購買 Sentinel 時，您會透過客戶入口網站收到授權金鑰。授權金鑰可讓您啟用功能、資料收集率及事件來源等，須視您購買的授權而定。授權金鑰可能並未執行其他的授權條件，因此請仔細閱讀您的授權合約。

若要變更您的授權，請聯絡帳戶管理員。

您可於安裝時或之後任何時間新增企業授權金鑰。若要新增授權金鑰，請參閱《「 Sentinel 管理指南」》中的「*新增授權金鑰*」。

5 符合系統需求

Sentinel 執行可依 IT 環境需求而異，因此您應先聯絡 諮詢服務或任何的 Sentinel 合作夥伴，再決定適合您環境的 Sentinel 結構。

如需關於建議硬體、受支援的作業系統、應用裝置平台和瀏覽器，請參閱 Sentinel 技術資訊網站。

連接器和收集器系統需求

每部連接器和收集器都有自己的系統需求和支援的平台。在 Sentinel 外掛程式網站上參閱連接器和收集器文件。

虛擬環境

VMware ESX 伺服器支援 Sentinel。在設定虛擬環境時，虛擬機器必須具備兩個以上的 CPU。為了在 ESX 上或任意其他虛擬環境中，實現能與實體機器測試結果相同的效能結果，虛擬環境應根據建議的實體機器要求，提供同樣的記憶體、CPU、磁碟空間及 I/O。

如需關於實體機器的建議，請參閱 Sentinel 技術資訊網站。

6 部署考量因素

Sentinel 擁有可擴充結構，可擴大以處理您需要放置其中的載入。本章綜覽擴充 Sentinel 佈署時最重要的考量。 技術支援或 合作夥伴服務專業人員會與您一起設計出適合您 IT 環境的 Sentinel 系統。

資料儲存考量

您可以根據 EPS 率，選擇使用傳統儲存或可擴充儲存來儲存 Sentinel 資料並為其編製索引。您的 Sentinel 部署視您選擇使用的資料儲存選項而定。

表格 6-1 *傳統儲存和可擴充儲存比較*

傳統儲存	可擴充儲存
根據預設，會在檔案式傳統儲存中儲存資料，並在 Sentinel 伺服器本機上編製索引。	在 Hadoop 式可擴充儲存中儲存資料，並使用可擴充分散式索引機制編製資料索引。
除了檔案式資料儲存以外，您也可以選擇在「視覺化資料儲存庫」中進行事件的儲存和索引編製，以使用資料視覺化功能。如需詳細資訊，請參閱「設定視覺化資料儲存庫」(第 41 頁)。	
無縫擴展到約 20000 EPS。此外，必須新增額外 Sentinel 伺服器才能擴充至更高的 EPS。	無縫擴充至非常高的 EPS，例如每秒 1 百萬個事件。
資料集合會跨數部 Sentinel 伺服器負載平衡。因此，資料會分散在不同的 Sentinel 伺服器中，且可個別管理。	資料集合會由單一 Sentinel 伺服器管理。因此，資料管理和資源管理集中於單一 Sentinel 伺服器。
將資料標記為與租用戶相關，但未在磁碟上因此進行分隔。	將資料標記為與租用戶相關，且在磁碟上因此進行分隔。
必須手動或使用昂貴的儲存機制 (例如 SAN 磁碟) 完成資料複製和可用性。	由於 Hadoop 在一般硬體上執行，因此資料複製和可用性具成本效益。

傳統儲存規劃

檔案式資料儲存有三層結構：

線上儲存	主要儲存，先前又稱本地儲存。	最佳化快速寫入和快速取回。儲存最近收集到的事件資料，和最常搜尋到的事件資料。
	次要儲存，先前又稱網路儲存。(optional)	最佳化以縮小在較便宜儲存上的空間使用，同時仍支援快速取回。Sentinel 會將資料分割區自動移轉到次要儲存。
	附註： 您可選擇使用次要儲存。資料保留規則、搜尋和報告會在事件資料分割區上作業，不論是存在於主要或次要儲存 (或兩者皆是) 上。	
離線儲存	歸檔儲存	分割區關閉時，您可以將分割區備份至任何檔案儲存服務，例如 Amazon Glacier。只要有需要，您都能暫時重新匯入分割區以供長期鑑識分析使用。

您也可以使用資料同步規則，設定 Sentinel 將事件資料和事件資料摘要擷取到外部資料庫。如需詳細資訊，請參閱「《 Sentinel 管理指南》」中的*「設定資料同步化」*。

安裝 Sentinel 時，您必須將主要儲存的磁碟分割區掛接在將安裝 Sentinel 的位置上，預設位在 /var/opt/novell 目錄。

在 /var/opt/novell/sentinel 目錄下的整個目錄結構必須位在單一磁碟分割區上，以確保能進行正確的磁碟使用量計算。否則，自動資料管理能力可能會過早刪除事件資料。如需有關 Sentinel 目錄結構的詳細資訊，請參閱「Sentinel 目錄結構」(第 44 頁)。

最佳作法是確認此資料目錄所在儲存位置，與可執行檔、組態和作業系統檔案位在不同的磁碟分割區上。分開儲存變數資料的優點包括易於備份檔案組合，也更容易復原損壞，並可在磁碟分割區滿載時提供額外加強。如此也能提升系統的整體效能，因為越小的檔案系統效率也越高。如需詳細資訊，請參閱「磁碟分割」。

附註： ext3 檔案系統中有檔案儲存的限制，讓目錄中的檔案或子目錄不能超過 32000 個。如果您會有大量的保留原則或是將長期保留資料 (例如一年)，您可以使用 XFS 檔案系統。

在傳統安裝中使用分割區

在傳統安裝上，您可以在安裝 Sentinel 前修改作業系統的磁碟分割區配置。管理員應依據「「Sentinel 目錄結構」(第 44 頁)」所述的目錄結構在適當的目錄中建立需要的分割區，並加以掛接。在執行安裝程式時，系統會將 Sentinel 安裝在預先建立的目錄中，使安裝作業得以涵蓋多個分割區。

附註：

- 在執行安裝程式時，您可以使用「--location」選項，指定非預設目錄的最上層位置來儲存檔案。傳遞至 --location 選項的值會加在目錄路徑的前面。例如，如果您指定 --location=/foo，資料目錄將會是 /foo/var/opt/novell/sentinel/data，而組態目錄將會是 /foo/etc/opt/novell/sentinel/config。
- 請勿將檔案系統連結 (如軟連結) 用於「--location」選項。

在裝置安裝中使用分割區

如果您使用的是 DVD ISO 裝置格式，您可在安裝期間依照 YaST 畫面中的指示設定裝置檔案系統的分割。例如，您可以為 /var/opt/novell/sentinel 掛接點建立不同的分割區，以將所有資料放在不同的分割區上。不過，若是其他裝置格式，您只能在安裝後才設定分割。您可以透過使用 SuSE YaST 系統設定工具來新增分割區並將目錄移至新的分割區。如需在安裝後才建立分割區的詳細資訊，請參閱「建立傳統儲存的分割區」(第 100 頁)。

分割區配置最佳實務

許多組織對於任何已安裝的系統都擁有自己記錄的最佳實務分割區配置規劃。以下分割區提案可用來引導尚未定義任何政策，並考慮採用 Sentinel 特定檔案系統用途的組織。一般來說，Sentinel 支援檔案系統階層標準 (如適用)。

分割區	裝置點	大小	附註
Root	/	100 GB	包含作業系統檔案和 Sentinel 二進位/組態。
開機	/boot	150 MB	開機分割區
主要儲存	/var/opt/novell/sentinel	以系統調整大小資訊計算。	這個區域將包含 Sentinel 收集的主要資料，加上其他變數資料，例如記錄檔案。這個分割區將與其他系統共享。
次要儲存	位置會依據儲存類型、NFS、CIFS 或 SAN。	以系統調整大小資訊計算。	這是次要儲存區域，可依顯示方式在本地或遠端掛接。
歸檔儲存	遠端系統	以系統調整大小資訊計算。	這個儲存用於歸檔資料。

設定視覺化資料儲存庫

Sentinel 提供可顯示圖表、表格和映射中資料的事件視覺化。這些視覺化可簡化對大量事件進行視覺化和分析的工作。您也可以建立自己的視覺化和儀表板。

Sentinel 可利用瀏覽器式分析和搜尋儀表板 Kibana，協助您搜尋事件並將其視覺化。Kibana 可從視覺化資料儲存庫 (Elasticsearch) 存取資料，以將事件顯示在儀表板中。根據預設，Sentinel 會包含僅儲存警示並為其編製索引的 Elasticsearch 節點。您必須啟用事件視覺化，才能在 Elasticsearch 中儲存事件及編製其索引。

當您啟用 Elasticsearch 以儲存資料及編製其索引時，Sentinel 只會為視覺化所需的特定事件欄位編製索引，並將已編製索引的欄位儲存在 Elasticsearch 中。Sentinel 每天都會建立專屬索引，並使用 UTC 時區 (午夜到午夜) 以計算索引日期。索引名稱格式為 security.events.normalized_yyyyMMdd。例如，索引 security.events.normalized_20160101 包含事件時間為 2016 年 1 月 1 日的所有事件。

設定視覺化資料儲存庫時須執行下列作業：

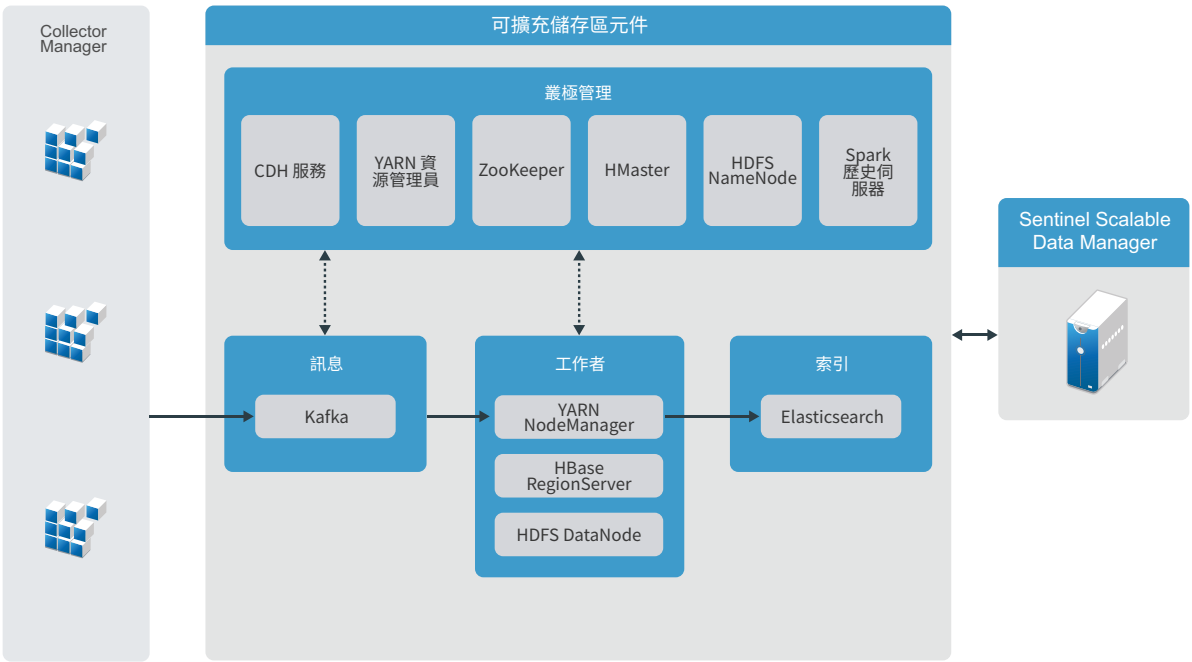
- **在叢集模式下安裝 Elasticsearch 節點：** 根據預設，Sentinel 會包含一個 Elasticsearch 節點。若要讓 Sentinel 伺服器達到最佳效能和穩定性，您必須在叢集模式下安裝更多 Elasticsearch 節點。如需詳細資訊，請參閱第 12 章 「安裝和設定 Elasticsearch」(第 73 頁)。
- **啟用事件視覺化：** 依預設會停用事件視覺化。若要啟用事件視覺化，請參閱第 20 章 「啟用事件視覺化」(第 115 頁)。
- **效能調整：** Sentinel 會自動設定特定的 Elasticsearch 設定，以達到最佳效能。您可以視需要自訂這些設定。例如，您可以修改要讓 Elasticsearch 編製索引的事件欄位。如需詳細資訊，請參閱「Elasticsearch 的效能調整」(第 78 頁)。

可擴充儲存規劃

Sentinel 會使用 Cloudera Distribution Including Apache Hadoop (CDH) 架構來儲存和管理大型資料。針對編製事件索引，Sentinel 使用 Elastic 所提供可擴充且分散式的索引引擎 Elasticsearch。

下圖說明可擴充儲存中使用的各種元件：

圖 6-1 *可擴充儲存架構*



- **訊息:** Sentinel 使用 Apache Kafka 做為可擴充訊息系統，可接收來自 Collector Manager 的標準化事件和原始資料。Collector Manager 會將原始資料和事件資料傳送至 Kafka 叢集。

  依預設，Sentinel 會建立下列 Kafka 主題：

  - **security.events.normalized：** 儲存所有已處理和標準化的事件資料，包括系統產生的事件和內部事件。

- **security.events.raw：** 儲存來自事件來源的所有原始資料。

事件和原始資料會遵循 Apache Avro 綱要。如需詳細資訊，請參閱 Apache Avro 文件。您可以在 /etc/opt/novell/sentinel/scalablestore 目錄中取得綱要檔案。

- **工作者：** 此節點代管即時處理和儲存工作。Apache Spark可即時進行大規模資料處理，例如根據租用戶 ID 分離事件，要求大量資料和儲存資料至記錄系統 (SOR) 和可調整索引。

  Apache HBase是分散式且可擴充的Hadoop式資料儲存。針對標準化事件和原始資料做為SOR使用，且依租用戶 ID 分隔。

  根據租用戶 ID，Sentinel 會為每個租用戶建立個別名稱空間。例如，預設租用戶的名稱空間為 1。在每個名稱空間下，Sentinel 會根據事件時間建立下列表格並儲存資料。

  - ***<tenant_ID>*:security.events.normalized:** 儲存所有已處理和標準化的事件資料，包括系統產生的事件和內部事件。
  - ***<tenant_ID>*:security.events.raw:** 儲存來自事件來源的所有原始資料。
- **叢集管理:** 此節點代管所有主檔案系統物件和叢集管理服務。Apache ZooKeeper 可做為維護組態資訊、命名服務、提供分散式同步化和提供群組服務的集中式服務。
- **編輯索引：** Sentinel 使用 Elasticsearch 做為索引事件的可擴充和分散式索引引擎。您可以從 Elasticsearch 存取資料，以進行事件搜尋和視覺化。

  Sentinel 每天都會建立專屬索引，並使用 UTC 時區 (午夜到午夜) 以計算索引日期。索引名稱格式為 security.events.normalized_yyyyMMdd。例如，索引 security.events.normalized_20160101 包含事件時間為 2016 年 1 月 1 日的所有事件。為了提供最佳效能，Sentinel 只會編製某些特定事件欄位的索引。您可以修改要讓 Elasticsearch 編製索引的事件欄位。如需詳細資訊，請參閱「Elasticsearch 的效能調整」(第 78 頁)。

可擴充儲存組態

啟用可擴充儲存時，Sentinel 伺服器會將使用者介面精簡為僅用於某些 Sentinel 功能，如資料收集、關連、事件路由、搜尋和視覺化事件，以及執行某些管理活動。Sentinel 的精簡功能版本稱為 Sentinel Scalable Data Manager (SSDM)。如需其他 Sentinel 功能 (例如，安全情報、基本搜尋和報告)，您必須安裝具有傳統儲存的 Sentinel 個別例項，並使用 Sentinel Link 將特定事件資料從 SSDM 路由至 Sentinel。

下列清單會列出 SSDM 中無法使用的服務和功能資訊：

- 報告
- 安全情報
- 搜尋期間執行事件操作
- 測試關連規則
- 事件的建立和管理
- 手動執行事件上的動作
- 資料同步
- iTRAC 工作流程
- 針對觸發關連事件的事件進行鑑識分析
- 檢視 Secure Configuration Manager 和 Change Guardian 事件的事件附件

啟用可擴充儲存是無法還原的一次性組態。如果您要停用可擴充儲存並切換至傳統儲存，您必須重新安裝 Sentinel。

下列核對清單提供設定可擴充儲存時，需要執行之任務的相關高階資訊：

表格 6-2 *可擴充儲存組態核對清單*

	任務	請參閱
❒	檢閱部署資訊以瞭解部署具有可擴充儲存的 Sentinel 部署時，所需的項目。	「具有可擴充儲存的三層部署」(第 49 頁)
❒	檢閱先決條件並完成所有必要任務。	第 13 章「安裝和設定可擴充儲存」(第 81 頁)。
❒	啟用可擴充儲存。 您可以在安裝期間或後續安裝工作中，啟用可擴充儲存。 若要升級安裝程式，您可以先升級 Sentinel，再啟用可擴充儲存。	若要在安裝期間啟用可擴充儲存，請執行 Sentinel 自定安裝。請參閱「Sentinel Server 自定安裝」(第 86 頁)。 若要在後續安裝工作或後續升級工作中啟用可擴充儲存，請參閱《 Sentinel 管理指南》中的*「在後續安裝工作中啟用可擴充儲存」*。
❒	透過 Sentinel 設定 CDH 元件和 Elasticsearch。	《 Sentinel 管理指南》中的*「設定可擴充儲存」*。

Sentinel 目錄結構

依預設，Sentinel 目錄位於下列位置：

- 資料檔案位於 /var/opt/novell/sentinel/data 與 /var/opt/novell/sentinel/3rdparty 目錄。
- 可執行檔和程式庫儲存在 /opt/novell/sentinel 目錄中.
- 記錄檔案位於 /var/opt/novell/sentinel/log 目錄中。
- 暫存檔案位於 /var/opt/novell/sentinel/tmp 目錄中。
- 組態檔案位於 /etc/opt/novell/sentinel 目錄中。
- 程序 ID (PID) 檔案位於 /home/novell/sentinel/server.pid 目錄中。

  管理員能使用 PID 來識別 Sentinel 伺服器的父代程序，以及監控或終止程序。

分散式佈署的優點

依預設，Sentinel 伺服器包括下列元件：

- **Collector Manager:** Collector Manager 為 Sentinel 提供了靈活的資料收集點。
- **Correlation Engine:** Correlation Engine 處理來自即時事件資料流的事件，以決定他們是否應觸發任何關連規則。
- **Elasticsearch：** 用來儲存資料和為其編製索引的選用資料儲存元件。根據預設，Sentinel 會包含一個 Elasticsearch 節點。如果您預期會有超過 2500 的大量 EPS，則必須在叢集中部署更多 Elasticsearch 節點。

重要： 在生產環境中，您應設定分散式部署，因為這樣可將資料收集元件隔離到個別電腦上；如想在處理流量突增和其他異常情況時維持最高的系統穩定性，這項做法相當重要。

本節說明分散式佈署的優點。

- 「額外 Collector Manager 的優點」(第 45 頁)
- 「增加 Correlation Engine 的優點」(第 45 頁)

額外 Collector Manager 的優點

依預設，Sentinel 伺服器含有 Collector Manager。不過，針對生產環境，分散式 Collector Manager 在收到大量資料時會提供更好的隔離。在這種情況下，分散式 Collector Manager 可能超載，但是 Sentinel 伺服器仍將會回應使用者要求。

在分散式網路中安裝多個 Collector Manager 可提供下列優勢：

- **改善系統效能：** 其他 Collector Manager 可以剖析及處理分散式環境中的事件資料，進而提高系統效能。
- **其他資料安全性與降低的網路頻寬需求：** 如果 Collector Manager 與事件來源共存，則可對資源執行過濾、加密以及資料壓縮。
- **檔案快取：** 其他 Collector Manager 可以在伺服器暫時忙於歸檔事件或處理事件中特殊圖文集的情況下，快取大量資料。此功能對於本身不支援事件快取的通訊協定 (例如，Syslog) 是一項優點。

您可在網路中合適的位置安裝其他 Collector Manager。這些遠端 Collector Manager 會執行連接器和收集器，並將收集的資料轉遞到 Sentinel 伺服器進行儲存和處理。如需有關安裝額外 Collector Manager 的詳細資訊，請參閱第 III 部分「安裝 Sentinel」(第 67 頁)。

附註： 您不可在單一系統上安裝多個 Collector Manager。您可在遠端系統上安裝其他 Collector Manager，然後再將其連接到 Sentinel 伺服器。

增加 Correlation Engine 的優點

您可以在個別的伺服器上部署多個 Correlation Engine，不需要複寫組態或新增資料庫。對於使用大量關連規則或事件發生率極高的環境，安裝多個 Correlation Engine 並重新部署部分規則到新的 Correlation Engine 會比較有利。多個 Correlation Engine 可隨著 Sentinel 系統加入更多資料來源或事件發生率提高時加以延伸。如需安裝其他 Correlation Engine 的相關資訊，請參閱 第 III 部分「安裝 Sentinel」(第 67 頁)。

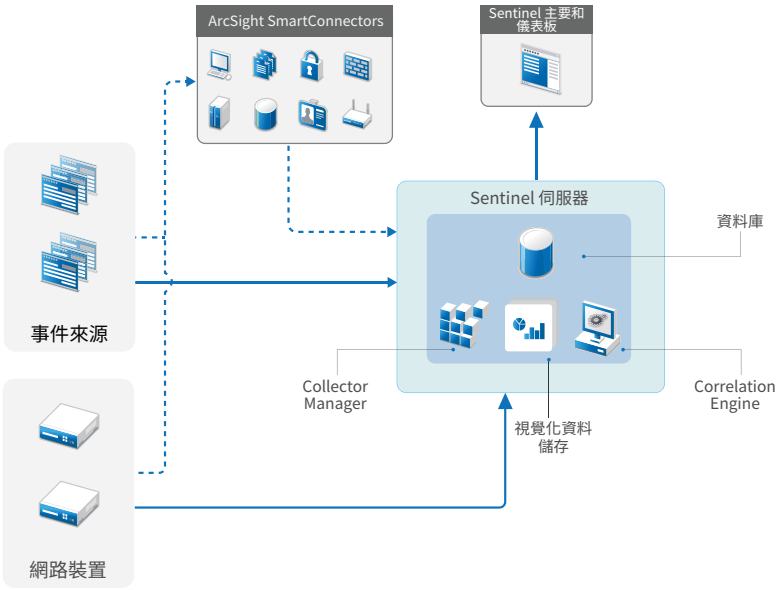
附註： 您不可在單一系統上安裝多個 Correlation Engine。您可在遠端系統上安裝其他 Correlation Engine，然後再將其連接到 Sentinel 伺服器。

整合式佈署

最基本的佈署選項是整合式系統，在單一電腦上包含所有 Sentinel 元件。全方位部署僅適用於系統負載較低且不需監控 Windows 電腦的情況。在許多環境中，無法預期且不斷變動的負載，以及元件間的資源衝突都可能引發效能問題。

重要： 在生產環境中，您應設定分散式部署，因為這樣可將資料收集元件隔離到個別電腦上；如想在處理流量突增和其他異常情況時維持最高的系統穩定性，這項做法相當重要。

圖 6-2 整合式佈署

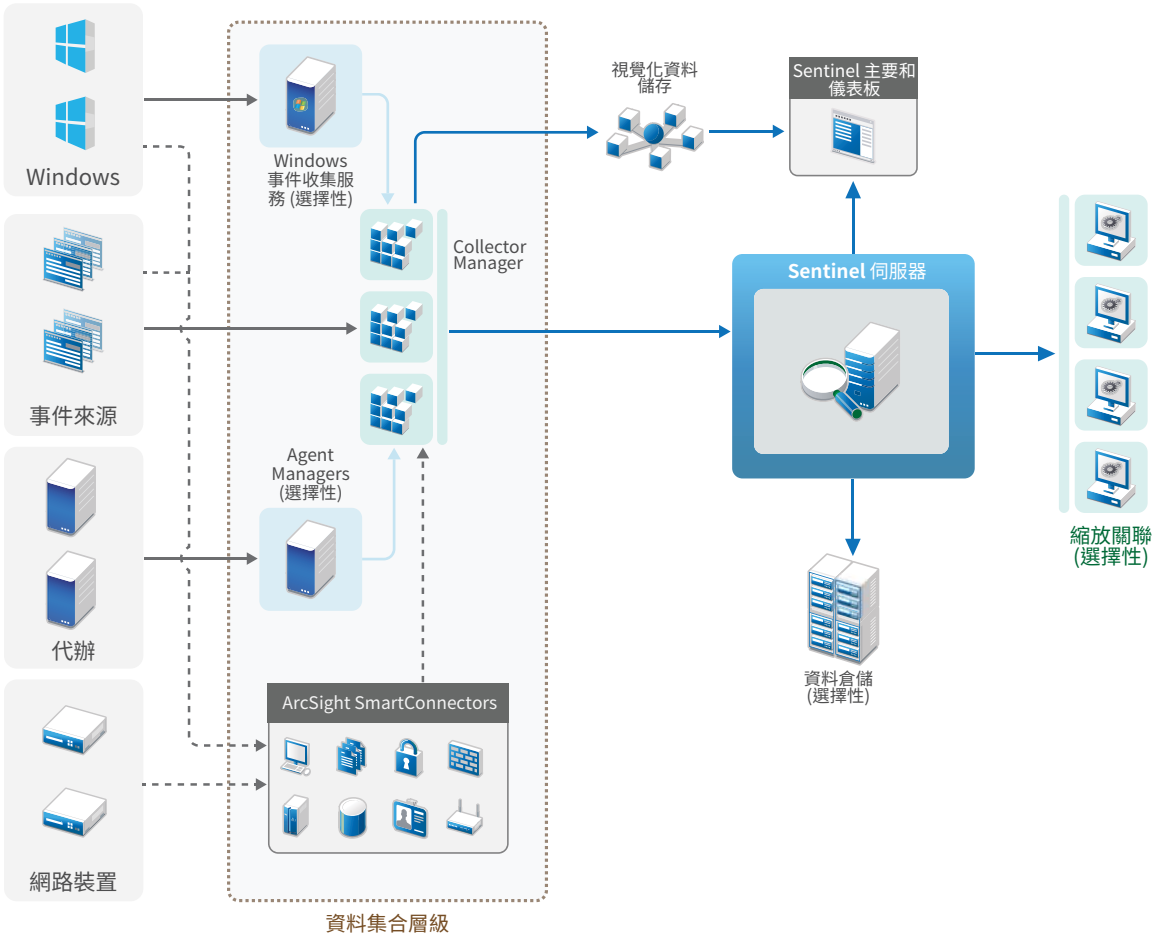


單層分散式佈署

單層佈署增加了監控 Windows 電腦的能力，也可處理比整合式佈署更大的負載。您可以新增 Collector Manager 和 Correlation Engine 電腦以分攤中央 Sentinel 伺服器的處理負載，進而向外擴充資料收集與關連的範圍。除了處理事件載入和關連規則，遠端收集器管理員和關連引擎也會將中央 Sentinel 伺服器上的資源釋出，以服務其他要求，例如事件儲存和搜尋。隨著系統上的載入提高，中央 Sentinel 伺服器最終將會成為瓶頸，您需要包含更多層級的佈署，以進一步擴充。

或者，您可以設定 Sentinel 將事件資料複製至資料倉儲，這對將自定報告、分析和其他處理卸載至另一個系統很實用。

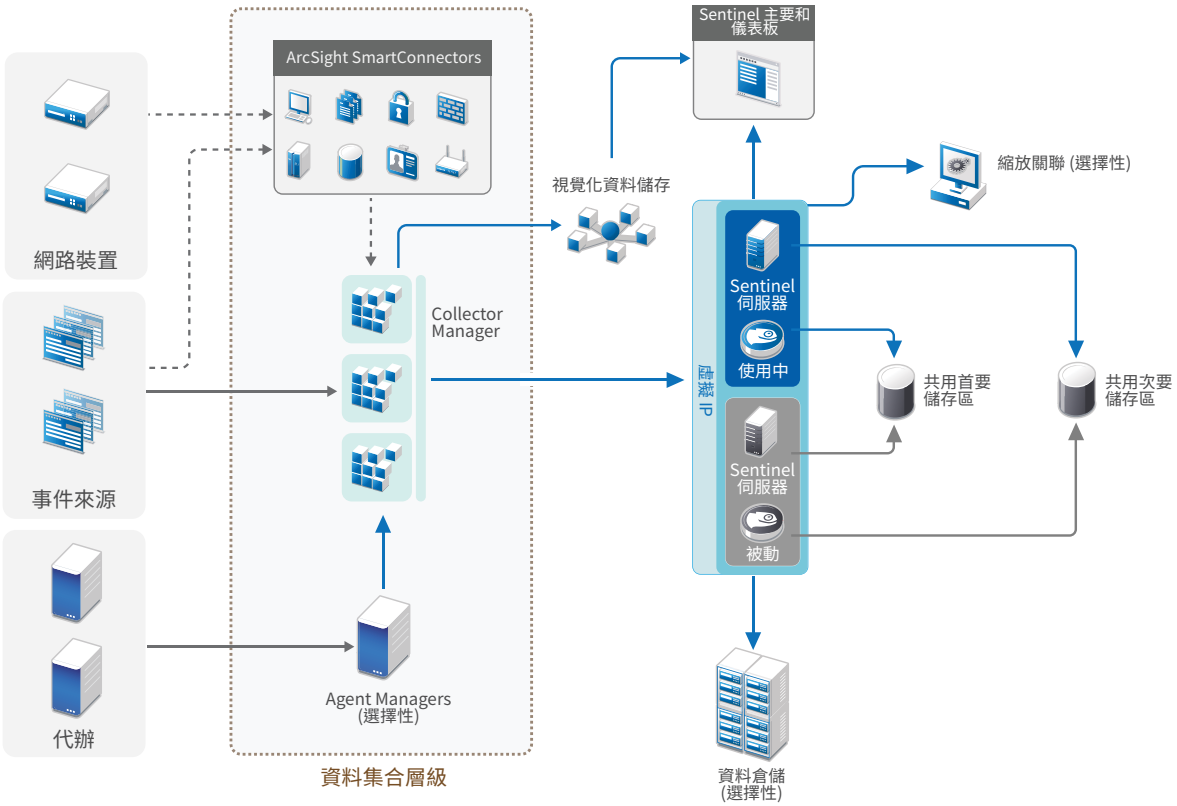
圖 6-3 單層分散式佈署



高可用性單層分散式佈署

單層分散式佈署顯示可如何將其轉變成包含容錯移轉備援的高可用性系統。如需有關以高可用性部署 Sentinel 的詳細資訊，請參閱第 VII 部分「部署 Sentinel 以提供高可用性」(第 171 頁)。

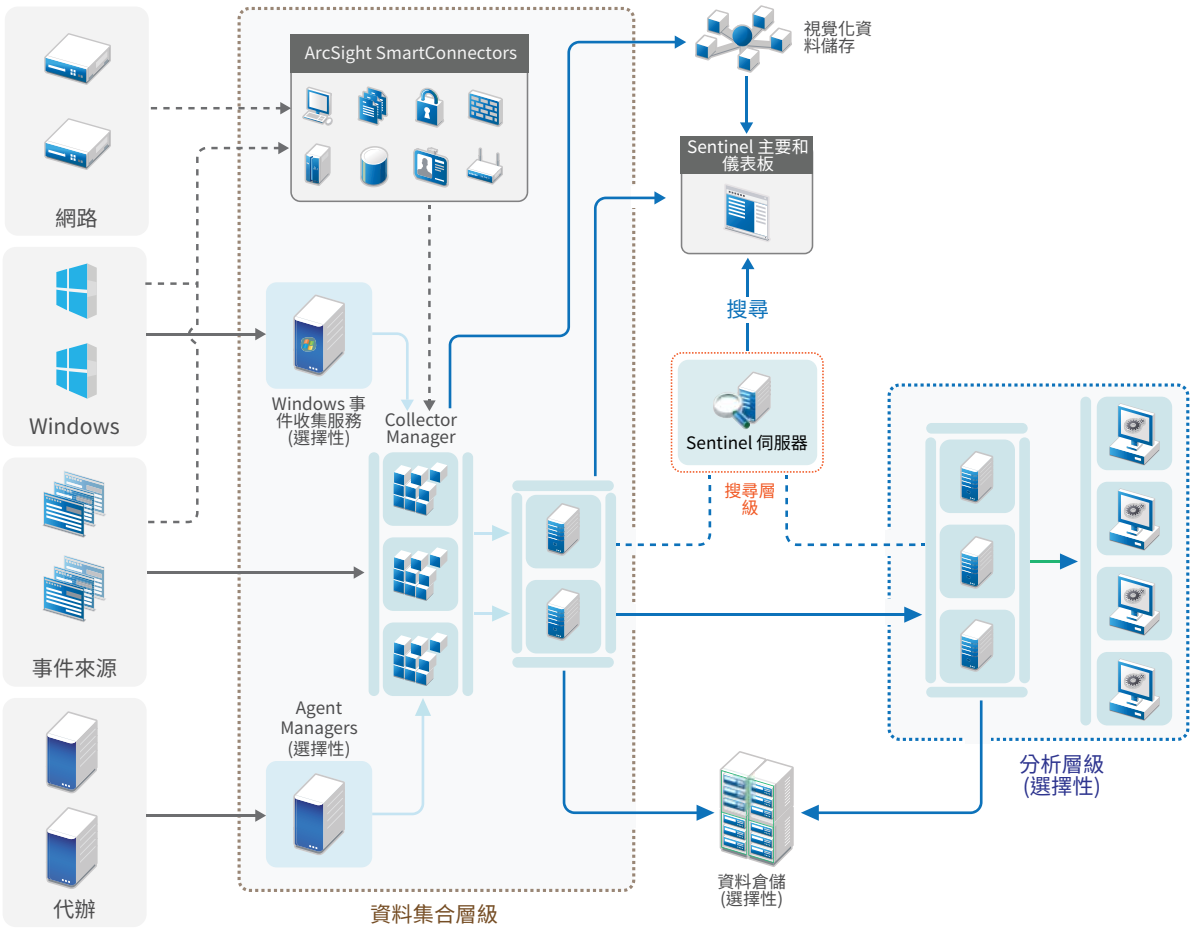
圖 6-4 高可用性單層分散式佈署



兩層和三層分散式佈署

這些佈署可讓您超越單一中央 Sentinel 伺服器的負載處理能力，並利用 Sentinel Link 和 Sentinel 資料聯盟共享多個 Sentinel 例項的處理負載。資料集合在多個 Sentinel 伺服器上為載入平衡，各有多個 Collector Manager，如資料集合層級所示。如果您要執行事件關連或安全情報，您可選擇使用 Sentinel Link 將資料轉遞至分析層級。搜尋層級提供便利的單一存取點，可使用 Sentinel 資料聯盟來搜尋在所有其他層級中的各個系統。由於搜尋申請會跨多個 Sentinel 例項聯盟，這個部署也包含搜尋載入平衡屬性，適合用於擴充以處理繁重的搜尋載入。

圖 6-5 兩層和三層分散式佈署



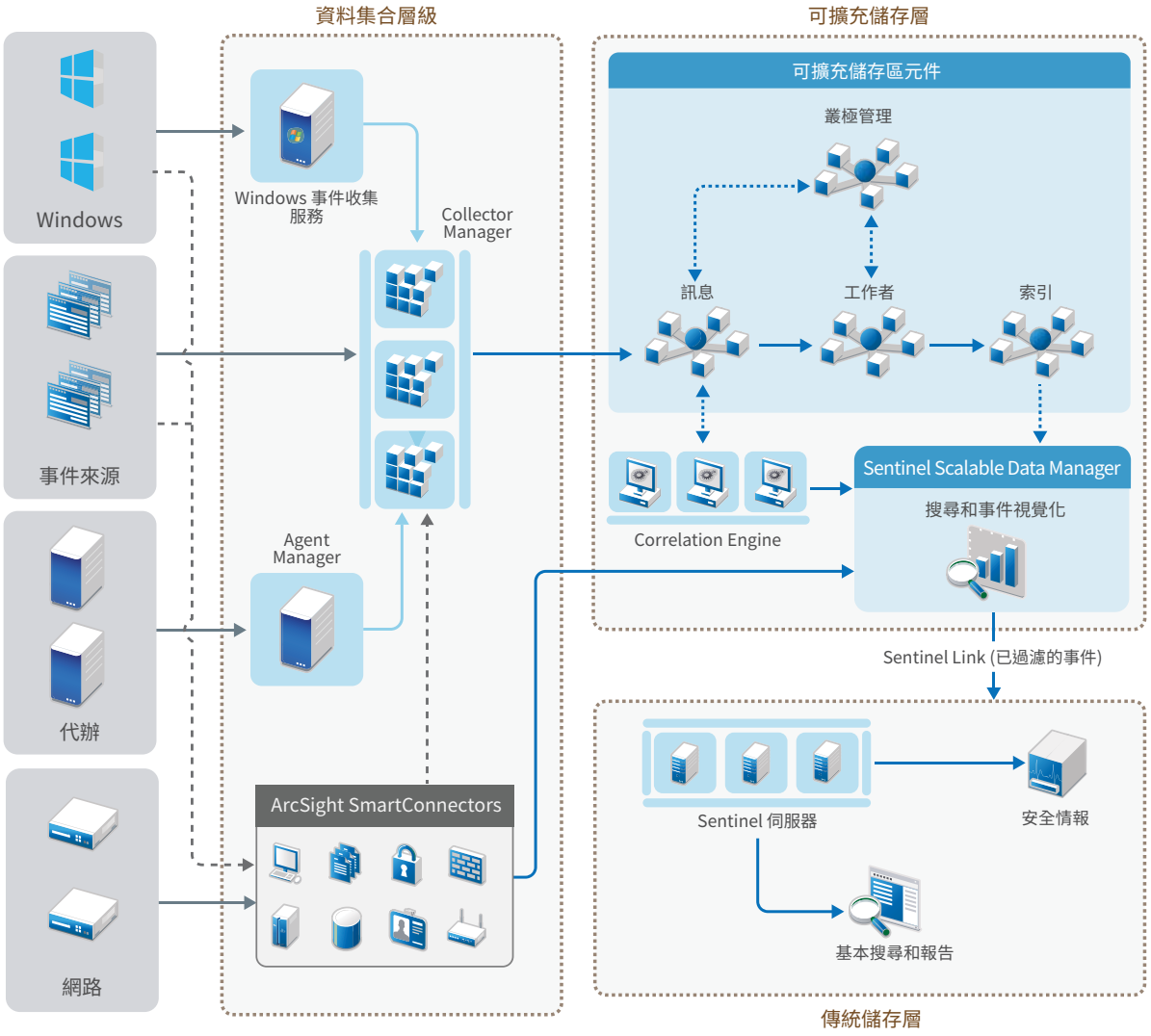
具有可擴充儲存的三層部署

針對您不想要讓事件分散在多部 Sentinel 伺服器中，和在多個例項中具有重複組態設定的大型資料儲存和資料處理需求，您可以設定具有可擴充儲存的三層分散式部署。此部署可透過使用具有可擴充儲存的單一 Sentinel 伺服器，而非使用多部 Sentinel 伺服器，讓您儲存和管理大型資料。

您可以使用設定可擴充式儲存設定新的 Sentinel 伺服器或升級您現有的 Sentinel 伺服器來啟用可擴充儲存。

根據您要使用的 Sentinel 功能，您可以決定如何設定 Sentinel 部署。

圖 6-6 可擴充儲存的三層部署



此部署包括下列層級：

- **資料集合層：** 適用於收集來自大範圍事件來源的事件。或者，若您想要使用傳統儲存 Sentinel 保留現有的資料收集設定，且仍使用可擴充儲存功能，您可以使用 data_uploader.sh 程序檔將想要的事件直接從傳統儲存轉送至可擴充儲存。如需詳細資訊，請參閱第 32 章 「將資料移轉至可擴充儲存」(第 163 頁)。
- **可擴充儲存層：** 針對儲存、索引和分析大量資料。在此層中的 SSDM 伺服器讓您可以管理資料集合和關連，並提供其他 SSDM 功能。若要使用 SSDM 中沒有的 Sentinel 功能，您可以設定傳統儲存層。您也可以轉遞集合資料至任何其他 SIEM 系統，或允許其他業務智慧工具查詢資料，或使用廣泛支援的 Hadoop、Kafka、Spark 和 Elasticsearch API，直接在您的 Hadoop 配送上執行分析。

- **傳統儲存層：** 若是 Sentinel 功能，例如安全情報、普通搜尋和報告，您必須安裝具有傳統儲存的 Sentinel 個別例項。您可以設定事件路由規則，使用 Sentinel 連結將想要的事件從 SSDM 轉遞至 Sentinel。

  您可以使用傳統儲存層中的任何 Sentinel 伺服器執行搜尋和報告。另一選項是您可以設定個別搜尋層，針對傳統儲存層中所有 Sentinel 伺服器的搜尋和報告，提供方便的單一存取點。針對在可擴充儲存中搜尋事件，請使用 SSDM 中的搜尋選項。

如需有關安裝和設定可擴充儲存的詳細資訊，請參閱第 13 章 「安裝和設定可擴充儲存」(第 81 頁)。

7 FIPS140-2 模式的部署考量因素

您也可以選擇性地將 Sentinel 設定為使用 Mozilla Network Security Services (NSS)，這是經過 FIPS 140-2 驗證的加密提供者，可處理其內部加密和其他功能。執行此操作的目的是確保 Sentinel 為「FIPS 140-2 inside」並符合美國聯邦採購規定和標準。

啟用 Sentinel FIPS 140-2 模式後，Sentinel 伺服器、Sentinel 遠端 Collector Manager、Sentinel 遠端 Correlation Engine、Sentinel 主要介面、Sentinel Control Center 和 Sentinel Advisor 服務之間的通訊一律都會使用經過 FIPS 140-2 驗證的加密措施。

重要： 只有 Sentinel 可支援 FIPS 模式。如果作業系統處於 FIPS 模式，則不支援 Sentinel。

在 Sentinel 中執行 FIPS

Sentinel 使用由作業系統提供的 Mozilla NSS 文件庫。Red Hat Enterprise Linux (RHEL) 和 SUSE Linux Enterprise Server (SLES) 使用不同的 NSS 套件組合。

由RHEL6.3或更新版本提供的NSS加密模組是經過FIPS140-2驗證。包含在SLES11中的NSS加密模組尚未正式經過FIPS140-2驗證，但是我們目前正致力讓SUSE模組通過FIPS140-2驗證。此驗證一旦可以使用，預期不需要進行任何 Sentinel 變更即可在 SUSE 平台上提供 'FIPS 140-2 Inside'。

如需有關 RHEL FIPS 140-2 驗證的詳細資訊，請參閱 https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/2711 和 https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/1837。

RHEL NSS 套件

Sentinel 必須有以下 64 位元 NSS 套件才能支援 FIPS 140-2 模式：

- nspr-*
- nss-sysinit-*
- nss-util-*
- nss-softokn-freebl-*
- nss-softokn-*
- nss-*
- nss-tools-*

若未安裝其中任一套件，請務必在 Sentinel 中啟用 FIPS 140-2 模式前完成安裝。

SLES NSS 套件

Sentinel 必須有以下 64 位元 NSS 套件才能支援 FIPS 140-2 模式：

- libfreebl3-*
- mozilla-nspr-*
- mozilla-nss-*
- mozilla-nss-tools-*

若未安裝其中任一套件，請務必在 Sentinel 中啟用 FIPS 140-2 模式前完成安裝。

Sentinel 中已啟用 FIPS 的元件

下列 Sentinel 元件提供 FIPS 140-2 支援：

- 所有 Sentinel 平台元件都已更新，可支援 FIPS 140-2 模式。
- 以下支援加密的 Sentinel 外掛程式都已更新，可支援 FIPS 140-2 模式：
  - Agent Manager Connector 2011.1r1 和更新版本
  - Database (JDBC) Connector 2011.1r2 和更新版本
  - File Connector 2011.1r1 和更新版本 (只有在檔案事件來源類型是本機或 NFS 時)。
  - LDAP Integrator 2011.1r1 和更新版本
  - Sentinel Link Connector 2011.1r3 和更新版本
  - Sentinel Link 整合器 2011.1r2 和更新版本
  - SMTP Integrator 2011.1r1 和更新版本
  - Syslog Connector 2011.1r2 和更新版本
  - Windows Event (WMI) Connector 2011.1r2 和更新版本
  - Check Point (LEA) Connector 2011.1r2 和更新版本
  - Syslog Integrator 2011.1r1 和更新版本

  如需設定這些 Sentinel 外掛程式以在 FIPS 140-2 模式中執行的相關資訊，請參閱「設定 Sentinel 外掛程式在 FIPS 140-2 模式中執行」(第 125 頁)。

以下支援選用加密的 Sentinel 連接器在本文發行當時尚未更新，無法支援 FIPS 140-2 模式。不過，您可以繼續使用這些連接器收集事件。如需在 FIPS 140-2 模式中使用這些連接器搭配 Sentinel 的相關資訊，請參閱「在 FIPS 140-2 模式中使用非 FIPS 啟用的連接器搭配 Sentinel」(第 131 頁)。

- Cisco SDEE Connector 2011.1r1
- File Connector 2011.1r1 - CIFS 和 SCP 功能包括加密，將無法在 FIPS 140-2 模式中運作。
- Audit Connector 2011.1r1
- SNMP Connector 2011.1r1

以下支援 SSL 的 Sentinel Integrator 在本文發行當時尚未更新，無法支援 FIPS 140-2 模式。不過，當這些 Integrator 在 FIPS 140-2 模式中搭配 Sentinel 使用時，您可以繼續使用未加密的連接。

- Remedy Integrator 2011.1r1 或更新版本
- SOAP Integrator 2011.1r1 或更新版本

未在以上列出的其他 Sentinel 外掛程式並未使用加密，不會受到在 Sentinel 中啟用 FIPS 140-2 模式影響。您不需要執行任何其他步驟就可以在 FIPS 140-2 模式中搭配 Sentinel 使用。

如需關於 Sentinel 外掛程式的詳細資訊，請參閱 Sentinel 外掛程式網站。若您想要針對任何一個尚未更新的外掛程式申請提供 FIPS 支援，請使用 Bugzilla 提交申請。

受 FIPS 模式影響的資料連線

如果 Sentinel 處於 FIPS 140-2 模式，則無法建立對 Microsoft SQL Server 的加密連線。這項考量會影響到下列類型的 Sentinel 作業：

- SQL Server 的資料同步原則
- 與 Agent Manager 資料庫通訊的 Sentinel 伺服器
- 資料庫連接器從 SQL Server 收集資料

執行核對清單

下表提供設定 Sentinel 以在 FIPS 140-2 模式中操作的必要任務綜覽。

任務	如需詳細資訊，請參閱...
規劃部署。	「部署情境」(第 55 頁)。
判斷您在 Sentinel 安裝期間是否需要啟用 FIPS 140-2 模式，或是您想在日後啟用。 若要在安裝期間在 FIPS 140-2 模式中啟用 Sentinel，您需要在安裝程序期間選取「自定」或「靜默」安裝方法。	「Sentinel Server 自定安裝」(第 86 頁)。 「執行靜默安裝」(第 90 頁) 第 23 章「在現有 Sentinel 安裝中啟用 FIPS 140-2 模式」(第 121 頁)
設定 Sentinel 外掛程式在 FIPS 140-2 模式中執行。	「設定 Sentinel 外掛程式在 FIPS 140-2 模式中執行」(第 125 頁)。
將證書輸入 Sentinel FIPS KeyStore。	「輸入證書到 FIPS Keystore 資料庫」(第 131 頁)

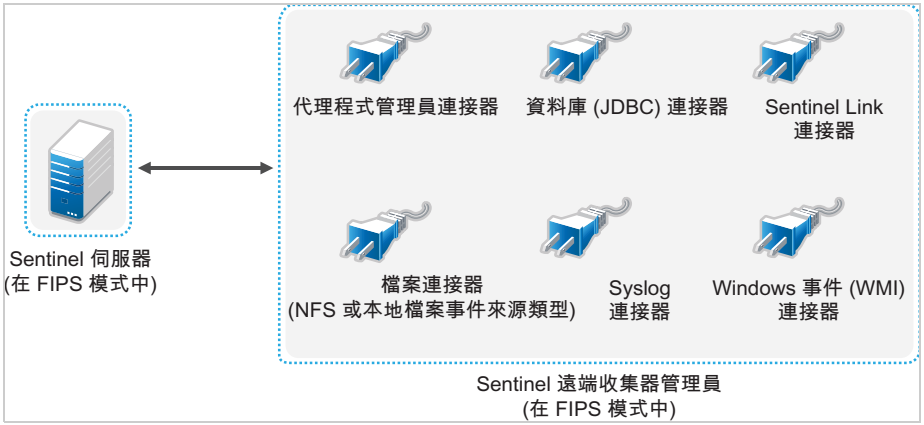
附註： 開始轉換至 FIPS 模式之前，請先備份 Sentinel 系統。如果伺服器日後必須回復成非 FIPS 模式，則唯一支援這麼做的方法是從備份還原。如需回復到非 FIPS 模式的相關資訊，請參閱「回復 Sentinel 到非 FIPS 模式」(第 131 頁)。

部署情境

本節提供在 FIPS 140-2 模式中 Sentinel 部署情境的相關資訊。

情境 1：在 FIPS 140-2 完整模式中的資料收集

在此情境中，資料收集只透過支援 FIPS 140-2 模式的連接器來完成。我們假設此環境與 Sentinel 伺服器相關，而且資料是透過遠端 Collector Manager 來收集。您可能會有一個以上的遠端 Collector Manager。



只有在您的環境使用支援 FIPS 140-2 模式的連接器收集事件來源的資料時，您才必須執行下列程序。

1 您的 Sentinel 伺服器必須是 FIPS 140-2 模式。

附註： 若您的 Sentinel 伺服器 (新安裝或已升級) 是在非 FIPS 模式，您必須啟用 Sentinel 伺服器上的 FIPS。如需詳細資訊，請參閱「啟用 Sentinel 伺服器在 FIPS 140-2 模式中執行」(第 121 頁)。

---

2 您的 Sentinel 遠端 Collector Manager 必須是以 FIPS 140-2 模式執行。

附註： 若您的遠端 Collector Manager (新安裝或已升級) 是以非 FIPS 模式執行，您必須啟用遠端 Collector Manager 上的 FIPS。如需詳細資訊，請參閱「啟用遠端 Collector Manager 和 Correlation Engine 上的 FIPS 140-2 模式」(第 122 頁)。

---

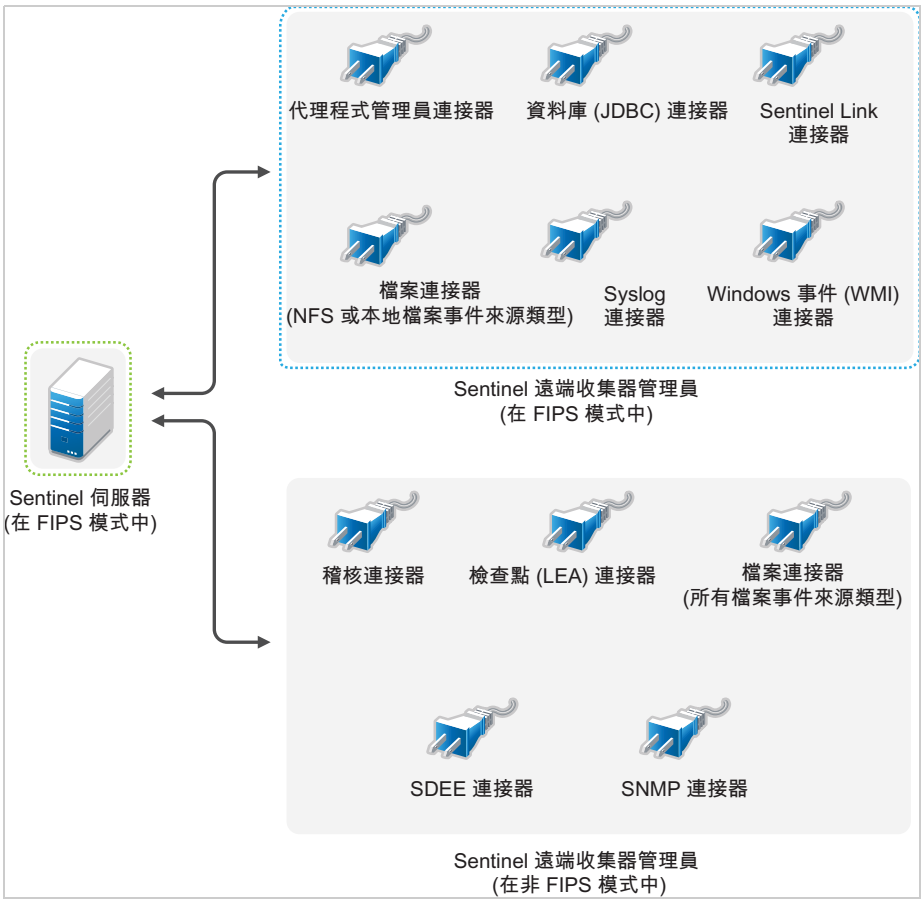
3 請確定 FIPS 伺服器和遠端 Collector Manager 可互相通訊。

4 若有遠端 Correlation Engine，請將其轉換為在 FIPS 模式中執行。如需詳細資訊，請參閱「啟用遠端 Collector Manager 和 Correlation Engine 上的 FIPS 140-2 模式」(第 122 頁)。

5 設定 Sentinel 外掛程式在 FIPS 140-2 模式中執行。如需詳細資訊，請參閱「設定 Sentinel 外掛程式在 FIPS 140-2 模式中執行」(第 125 頁)。

情境 2：在 FIPS 140-2 部分模式中的資料收集

在此情境中，資料收集是透過使用支援 FIPS 140-2 模式的連接器和不支援 FIPS 140-2 模式的連接器來完成。我們假設資料是透過遠端 Collector Manager 所收集。您可能會有一個以上的遠端 Collector Manager。



為因應使用支援和不支援 FIPS 140-2 模式的連接器進行資料收集，建議您使用兩個遠端 Collector Manager，一個以 FIPS 140-2 模式執行支援 FIPS 的連接器，另一個以非 FIPS (正常) 模式執行不支援 FIPS 140-2 模式的連接器。

若您的環境使用支援 FIPS 140-2 模式的連接器和未支援 FIPS 140-2 模式的連接器來收集事件來源的資料時，您必須執行下列程序。

1 您的 Sentinel 伺服器必須是 FIPS 140-2 模式。

附註： 若您的 Sentinel 伺服器 (新安裝或已升級) 是在非 FIPS 模式，您必須啟用 Sentinel 伺服器上的 FIPS。如需詳細資訊，請參閱「啟用 Sentinel 伺服器在 FIPS 140-2 模式中執行」(第 121 頁)。

---

2 請確定一個遠端 Collector Manager 是以 FIPS 140-2 模式執行，而另一個遠端 Collector Manager 繼續以非 FIPS 模式執行。

2a 若您沒有已啟用 FIPS 140-2 模式的遠端 Collector Manager，您必須在遠端 Collector Manager 上啟用 FIPS 模式。如需詳細資訊，請參閱「啟用遠端 Collector Manager 和 Correlation Engine 上的 FIPS 140-2 模式」(第 122 頁)。

2b 更新在非 FIPS 遠端 Collector Manager 上的伺服器證書。如需詳細資訊，請參閱「更新在遠端 Collector Manager 和 Correlation Engine 上的伺服器證書」(第 125 頁)。

3 確定兩個遠端 Collector Manager 能與已啟用 FIPS 140-2 的 Sentinel 伺服器通訊。

4 若有遠端 Correlation Engine，將其設定為在 FIPS 140-2 模式中執行。如需詳細資訊，請參閱「啟用遠端 Collector Manager 和 Correlation Engine 上的 FIPS 140-2 模式」(第 122 頁)。

5 設定 Sentinel 外掛程式在 FIPS 140-2 模式中執行。如需詳細資訊，請參閱「設定 Sentinel 外掛程式在 FIPS 140-2 模式中執行」(第 125 頁)。

5a 部署在以 FIPS 模式執行的遠端 Collector Manager 上支援 FIPS 140-2 模式的連接器。

5b 部署在非 FIPS 遠端 Collector Manager 上不支援 FIPS 140-2 模式的收集器。

8 使用的連接埠

Sentinel 使用各種的連接埠來與其他元件進行外部通訊。依預設，在安裝裝置時，防火牆上的連接埠會處於開啟狀態。然而在進行傳統安裝時，您必須設定即將安裝 Sentinel 的作業系統，以在防火牆上開啟連接埠。

Sentinel 伺服器連接埠

Sentinel 伺服器使用下列連接埠進行內部和外部通訊。

本地連接埠

Sentinel 使用下列連接埠來與資料庫和其他內部程序進行內部通訊：

連接埠	描述
TCP 27017	用於安全性智慧組態資料庫。
TCP 28017	用於安全性智慧資料庫的 Web 主控台。
TCP 32000	在包裝函式程序和伺服器程序之間進行內部通訊時使用。
TCP 9200	用於以 REST 和警示編列索引服務溝通。
TCP 9300	用於以其原生協定和警示編列索引服務溝通。

網路連接埠

若要使 Sentinel 正常運作，請確認已在防火牆上開啟下列連接埠：

連接埠	方向	必要/選用	描述
TCP 5432	向內	選用。依預設，此連接埠只在迴路介面上監聽。	用於PostgreSQL資料庫。依預設，您不需要開啟此連接埠。不過，當使用 Sentinel SDK 開發各種報告時，您必須開啟此連接埠。如需詳細資訊，請參閱 Sentinel 外掛程式 SDK。
TCP 1099 和 2000	向內	必要	監控工具使用這兩個連接埠來利用 Java Management Extensions (JMX) 連接 Sentinel 伺服器程序。
TCP 1289	向內	選擇性	用於 Audit 連線。

連接埠	方向	必要/選用	描述
UDP 1514	向內	選擇性	用於 syslog 訊息。
TCP 8443	向內	必要	用於 HTTPS 通訊。
TCP 1443	向內	選擇性	用於 SSL 加密 syslog 訊息。
TCP 61616	向內	選擇性	用於從 Collector Manager 和 Correlation Engine 收到的連接。
TCP 10013	向內	必要	用於 Sentinel Control Center 和 Solution Designer。
TCP 1468	向內	選擇性	用於 syslog 訊息。
TCP 10014	向內	選擇性	遠端 Collector Manager 會使用此連接埠來透過 SSL 代理連接伺服器。然而，這是少見的狀況。依預設，遠端 Collector Manager 使用 SSL 連接埠 61616 來連接伺服器。
TCP 443	向外	選擇性	若使用了 Advisor，連接埠會啟始 Advisor 服務的連接，透過網際網路連到 Advisor 更新頁面。
TCP 8443	向外	選擇性	若使用了資料聯盟，連接埠會啟始其他 Sentinel 系統的連接，以執行分散式搜尋。
TCP 389 或 636	向外	選擇性	若使用了 LDAP 驗證，連接埠會啟始 LDAP 伺服器的連接。
TCP/UDP 111 和 TCP/UDP 2049	向外	選擇性	若次要儲存設定為使用 NFS。
TCP 137、138、139、445	向外	選擇性	若次要儲存設定為使用 CIFS。
TCP JDBC (資料庫相依)	向外	選擇性	若採用了資料同步，連接埠會使用 JDBC 啟始目標資料庫的連接。在目標資料庫上使用的是相依連接埠。
TCP 25	向外	選擇性	啟始電子郵件伺服器的連接。
TCP 1290	向外	選擇性	當 Sentinel 將事件傳送到其他 Sentinel 系統時，此連接埠會啟始該系統的 Sentinel Link 連接。
UDP 162	向外	選擇性	當 Sentinel 傳送事件到接收 SNMP 設陷的系統時，連接埠會傳送封包到接收器。
UDP 514 或 TCP 1468	向外	選擇性	當 Sentinel 將事件傳送到接收 Syslog 訊息的系統時，便會使用此連接埠。若連接埠為 UDP，便會傳送封包到接收器。若連接埠為 TCP，便會啟始接收器的連接。
TCP 9443	向內	選擇性	此連接埠允許 Sentinel 系統從其他 SIEM 軟體接收事件，例如 Change Guardian 和 Secure Configuration Manager。

Sentinel 伺服器裝置專用連接埠

除了上述連接埠之外，裝置的下列連接埠也會開啟。

連接埠	方向	必要/選用	描述
TCP 22	向內	必要	用於保護對 Sentinel 裝置的外圍程序存取。

連接埠	方向	必要/選用	描述
TCP 4984	向內	必要	Sentinel 裝置也會將其用於更新服務。
TCP 289	向內	選擇性	針對 Audit 連線，轉遞至 1289。
TCP 443	向內	選擇性	轉遞至 8443 以進行 HTTPS 通訊。
UDP 514	向內	選擇性	針對 syslog 訊息，轉遞至 1514。
TCP 1290	向內	選擇性	允許透過 SuSE 防火牆進行連接的 Sentinel Link 連接埠。
UDP 和 TCP 40000 - 41000	向內	選擇性	設定資料集合伺服器 (例如 syslog) 時使用的連接埠。依預設，Sentinel 不會在這些連接埠上進行監聽。
TCP 443 或 80	向外	必要	啟始網際網路上 裝置軟體更新儲存機制或網路上 Subscription Management Tool 服務的連接。
TCP 80	向外	選擇性	啟始 Subscription Management Tool 的連接。
TCP 7630	向內	必要	由 High Availability Web Konsole (Hawk) 所使用。
TCP 9443	向內	必要	由 Sentinel 裝置管理主控台所使用。
TCP 1098 和 2000	向內	必要	監控工具使用這兩個連接埠來利用 Java Management Extensions (JMX) 連接 Sentinel 伺服器程序。

Collector Manager 連接埠

Collector Manager 使用以下連接埠與其他元件通訊。

網路連接埠

若要使 Sentinel Collector Manager 正常運作，請確認已在防火牆上開啟下列連接埠：

連接埠	方向	必要/選用	描述
TCP 1289	向內	選擇性	用於 Audit 連線。
UDP 1514	向內	選擇性	用於 syslog 訊息。
TCP 1443	向內	選擇性	用於 SSL 加密 syslog 訊息。
TCP 1468	向內	選擇性	用於 syslog 訊息。
TCP 1099 和 2000	向內	必要	監控工具使用這兩個連接埠來利用 Java Management Extensions (JMX) 連接 Sentinel 伺服器程序。
TCP 61616	向外	必要	啟始 Sentinel 伺服器的連接。
TCP 8443	向外	必要	啟始 Sentinel Web 伺服器連接埠的連接。 只在安裝和設定 Collector Manager 時，將此連接埠打開。

Collector Manager 裝置專用連接埠

除了上述連接埠之外，Sentinel Collector Manager 裝置上的下列連接埠也會開啟。

連接埠	方向	必要/選用	描述
TCP 22	向內	必要	用於保護對 Sentinel 裝置的外圍程序存取。
TCP 4984	向內	必要	Sentinel 裝置也會將其用於更新服務。
TCP 289	向內	選擇性	針對 Audit 連線，轉遞至 1289。
UDP 514	向內	選擇性	針對 syslog 訊息，轉遞至 1514。
TCP 1290	向內	選擇性	這是允許透過 SuSE 防火牆進行連接的 Sentinel Link 連接埠。
UDP 和 TCP 40000 - 41000	向內	選擇性	當設定資料收集伺服器 (例如 syslog) 時使用。依預設，Sentinel 不會在這些連接埠上進行監聽。
TCP 443	向外	必要	啟始網際網路上 裝置軟體更新儲存機制或網路上 Subscription Management Tool 服務的連接。
TCP 80	向外	選擇性	啟始 Subscription Management Tool 的連接。
TCP 9443	向內	必要	由 Sentinel 裝置管理主控台所使用。
TCP 1098 和 2000	向內	必要	監控工具使用這兩個連接埠來利用 Java Management Extensions (JMX) 連接 Sentinel 伺服器程序。

Correlation Engine 連接埠

Correlation Engine 使用以下連接埠與其他元件通訊。

網路連接埠

若要使 Sentinel Correlation Engine 正常運作，請確認已在防火牆上開啟下列連接埠：

連接埠	方向	必要/選用	描述
TCP 1099 和 2000	向內	必要	監控工具使用這兩個連接埠來利用 Java Management Extensions (JMX) 連接 Sentinel 伺服器程序。
TCP 61616	向外	必要	啟始 Sentinel 伺服器的連接。
TCP 8443	向外	必要	啟始 Sentinel Web 伺服器連接埠的連接。 只在安裝和設定 Correlation Engine 時將此連接埠打開。

Correlation Engine 裝置專用連接埠

除了上述連接埠之外，Sentinel Correlation Engine 裝置上的下列連接埠也會開啟。

連接埠	方向	必要/選用	描述
TCP 22	向內	必要	用於保護對 Sentinel 裝置的外圍程序存取。
TCP 4984	向內	必要	Sentinel 裝置也會將其用於更新服務。
TCP 443	向外	必要	啟始網際網路上 裝置軟體更新儲存機制或網路上 Subscription Management Tool 服務的連接。
TCP 80	向外	選擇性	啟始 Subscription Management Tool 的連接。
TCP 9443	向內	必要	由 Sentinel 裝置管理主控台所使用。
TCP 1098 和 2000	向內	必要	監控工具使用這兩個連接埠來利用 Java Management Extensions (JMX) 連接 Sentinel 伺服器程序。

可擴充儲存連接埠

若要讓 SSDM 透過 CDH 和 Elasticsearch 成功進行通訊，除了 Cloudera 需要的連接埠和Sentinel 伺服器連接埠一節中所列的連接埠以外，請確定您在可擴充儲存組態期間指定的連接埠都在防火牆上開放。

9 安裝選項

您可以執行 Sentinel 傳統安裝或安裝此裝置。本章節提供兩個安裝選項的相關資訊。

傳統安裝

傳統安裝會使用應用程式安裝程式將 Sentinel 安裝在現有作業系統上。您可以使用下列方式來安裝 Sentinel：

- **互動：** 安裝作業進行時會要求使用者輸入。在安裝期間，您可以將安裝選項 (使用者輸入或預設值) 記錄到檔案，日後可用來進行靜默安裝。您可以執行標準安裝或自定安裝。

標準安裝	自訂安裝
使用組態的預設值。唯一需要使用者輸入的項目為密碼。	提示您指定組態設定的值。您可以選取預設值或指定需要的值。
使用預設的試用版金鑰安裝。	可讓您利用預設的試用版授權金鑰或有效的授權金鑰進行安裝。
可讓您指定管理員密碼，並將此密碼作為 dbauser 與 appuser 的預設密碼。	可讓您指定管理員密碼。針對 dbauser 與 appuser，您可以指定新的密碼或使用管理員密碼。
安裝所有元件的預設連接埠。	可讓您為不同的元件指定連接埠。
在非 FIPS 模式中安裝 Sentinel。	可讓您在 FIPS 140-2 模式中安裝 Sentinel。
使用傳統儲存來儲存原始資料和事件。	可讓您使用可擴充儲存來儲存原始資料和事件。
利用內部資料庫驗證使用者。	提供除了資料庫驗證以外，為 Sentinel 設定 LDAP 驗證的選項。當您針對 LDAP 驗證設定 Sentinel 時，使用者可以使用其 Novell eDirectory 或 Microsoft Active Directory 身分證明來登入伺服器。

  如需互動式安裝的其他資訊，請參閱「執行互動式安裝」(第 85 頁)。

- **靜默：** 如果您想要在部署中安裝多個 Sentinel 伺服器，可以於標準或自定安裝期間在組態檔案中記錄安裝選項，然後使用檔案執行靜默安裝。如需靜默安裝的其他資訊，請參閱「執行靜默安裝」(第 90 頁)。

裝置安裝

裝置安裝會安裝 SLES 12 SP3 64 位元作業系統和 Sentinel 兩者。

Sentinel 裝置提供下列使用格式：

- OVF 裝置影像
- ISO 裝置映像

如需有關裝置安裝的詳細資訊，請參閱第 15 章 「裝置安裝」(第 95 頁)。

安裝 Sentinel

本節提供安裝 Sentinel 和其他元件的相關資訊。

10 安裝綜覽

預設 Sentinel 安裝會在 Sentinel 伺服器中安裝下列元件：

- **Sentinel 伺服器 和 Web 伺服器處理：** Sentinel 伺服器程序處理來自 Sentinel 其他元件的要求，並允許系統順利運作。Sentinel 伺服器程序處理各種要求，例如篩選資料、處理搜尋查詢及管理包括使用者驗證和授權的管理任務。

  Sentinel Web 伺服器允許安全連線至 Sentinel 主介面。
- **PostgreSQL 資料庫：** Sentinel 有一個內建資料庫，可儲存 Sentinel 組態資訊、資產和??資料、身分資訊、事件和工作流程狀態等等。
- **MongoDB 資料庫：** 儲存安全情報和警示資料。
- **Elasticsearch：** 為事件和警示編製索引以便搜尋和視覺化。
- **Collector Manager:** Collector Manager 為 Sentinel 提供了靈活的資料收集點。依預設，Sentinel 安裝程式會在安裝期間安裝 Collector Manager。
- **Elasticsearch：** 用來儲存資料和為其編製索引的選用資料儲存元件。根據預設，Sentinel 會包含一個 Elasticsearch 節點。如果您預期會有超過 2500 的大量 EPS，則必須在叢集中部署更多 Elasticsearch 節點。
- **Correlation Engine:** Correlation Engine 處理來自即時事件資料流的事件，以決定他們是否應觸發任何關連規則。
- **Advisor：** Advisor 係由 Security Nexus 提供技術支援，為選擇性資料訂閱服務，會針對入侵偵測與預防系統的即時事件以及企業??掃描結果，提供裝置層級的關連。如需有關 Advisor 的詳細資訊，請參閱《「 Sentinel 管理指南」》中的「*偵測漏洞和入侵*」。
- **Sentinel 外掛程式：** Sentinel 支援各種可擴充與增強系統功能的外掛程式。系統中會預安裝其中的一些外掛程式。您可從 Sentinel 外掛程式網站下載其他外掛程式和更新。Sentinel 外掛程式包含以下各項：
  - 收集器
  - 連接器
  - 關連規則與動作
  - 報告
  - iTRAC 工作流程
  - 解決方案套件

11 安裝核對清單

在開始安裝之前，請確認您已完成下列工作：

- ❒ 確認硬體和軟體符合「第 5 章 「符合系統需求」(第 37 頁)」所列示的系統需求。
- ❒ 若已有舊版 Sentinel 安裝，請確認已清除舊版安裝的所有檔案或系統設定。如需詳細資訊，請參閱附錄 B 「解除安裝」(第 211 頁)。
- ❒ 若您計劃安裝授權版本，請向 客戶服務中心取得授權金鑰。
- ❒ 確認已在防火牆開啟「第 8 章 「使用的連接埠」(第 59 頁)」所列示的連接埠。
- ❒ 為讓 Sentinel 安裝程式正常運作，系統必須能夠傳回主機名稱或有效 IP 位址。若要進行這項操作，請將主機名稱新增至 /etc/hosts 檔案中含有 IP 位址的文字行，接著再輸入 hostname -f 以確認主機名稱能正確顯示。
- ❒ 使用網路時間通訊協定 (NTP) 同步化時間。
- ❒ 如果您計劃部署具有可擴充儲存組態的 Sentinel，請確定您已安裝 CDH 和 Elasticsearch。如需有關部署具有可擴充儲存之 Sentinel 的詳細資訊，請參閱「安裝和設定可擴充儲存」(第 81 頁)。
- ❒ **在 RHEL 系統上：** 為取得最佳效能，記憶體設定必須正確設定以適用於 PostgreSQL 資料庫。SHMMAX 參數必須大於或等於 1073741824。

  若要設定適當的參數，請在 /etc/sysctl.conf 檔案中附加下列資訊：

  ```
  # for Sentinel Postgresql
  kernel.shmmax=1073741824
  ```

- ❒ **針對傳統安裝：**

  Sentinel 伺服器的作業系統必須至少包含 SLES 伺服器或 RHEL 6 伺服器的基底伺服器元件。Sentinel 必須具備下列 RPM 的 64 位元版本：

  - bash
  - bc
  - coreutils
  - gettext
  - glibc
  - grep
  - libgcc
  - libstdc
  - lsof
  - net-tools
  - openssl
  - python-libs
  - sed
  - zlib

- **對於使用傳統儲存的 Sentinel：**

  若要檢視事件視覺化，請新增 /etc/sysctl.conf 檔案中的 vm.max_map_count=262144 內容來設定虛擬記憶體。

12 安裝和設定 Elasticsearch

如需事件的可擴充和分散式索引，您必須在叢集節點中安裝 Elasticsearch。為 Sentinel 安裝的 Elasticsearch 叢集只能用於編製 Sentinel 資料的索引。

必要條件

安裝 Elasticsearch 前，請完成下列先決條件：

- 根據您的 EPS 率，使用 Sentinel 的技術資訊頁面中建議的節點數目和複本數目，在叢集模式下部署·Elasticsearch。
- 透過在 /etc/security/limits.conf 檔案中新增下列內容，設定檔案描述子：

  elasticsearch hard nofile 65536

  elasticsearch soft nofile 65536

  elasticsearch soft as unlimited

  附註： 您完成上方的前置作業後，執行 sysctl -p 指令以重新載入對檔案作出的變更。

安裝和設定 Elasticsearch

您必須在 Elasticsearch 叢集的每個節點上安裝 Elasticsearch 和所需的外掛程式。

若要安裝和設定 Elasticsearch：

1. 安裝 Elasticsearch 支援的 JDK 版本。
2. 下載認證版本的 Elasticsearch RPM。如需關於認證版本和下載 URL 的詳細資訊，請參閱 Sentinel 技術資訊頁面。
3. 安裝 Elasticsearch：

   rpm -i elasticsearch-<*版本*>.rpm
4. 完成 RPM 後續安裝工作指示畫面中所述的任務。
5. 確定 Elasticsearch 使用者具有 Java 的存取權。
6. 透過更新或新增下列資訊，設定 /etc/elasticsearch/elasticsearch.yml 檔案：

內容和值	附註
cluster.name: <*Elasticsearch 叢集名稱*>	您必須針對所有節點指定相同的叢集名稱。
node.name: <*節點名稱*>	每個節點的節點名稱都必須唯一。
network.host: _<*networkInterface*>:ipv4_	
discovery.zen.ping.unicast.hosts：[<Sentinel 伺服器中 elasticsearch 節點的 FQDN>、<*elasticsearch node1 的 FQDN*>、<*elasticsearch node2 的 FQDN*>，依此類推]	
thread_pool.bulk.queue_size: 300	
thread_pool.search.queue_size: 10000	當搜尋佇列大小達到上限，Elasticsearch 會丟棄任何佇列內等待中的搜尋要求。 您可以根據以下計算，增加搜尋佇列大小： threadpool.search.queue_size = 每位使用者針對儀表板的小工具查詢平均數 x 分區數 (每天索引) x 天數 (搜尋期間)
index.codec: best_compression	
path.data: ["/<*es1*>", "/<*es2*>"]	在多個獨立磁碟或位置中分散資料以降低磁碟 I/O 延遲。 針對儲存 Elasticsearch 資料設定多個路徑。例如 /es1、/es2 等。 為了取得最佳效能和管理性，請將每個路徑掛接至個別實體磁碟 (JBOD)。

7 更新 /etc/elasticsearch/jvm.options 檔案中預設的 Elasticsearch 堆積大小。

堆積大小必須是伺服器記憶體的 50%。例如，在 24 GB 的 Elasticsearch 節點上會配置 12 GB 作為堆積大小以提供最佳效能。

8 針對每個 Elasticsearch 叢集節點重複所有上述步驟。

9 在 Sentinel 伺服器 Elasticsearch 節點中，依照下列方式設定 /etc/opt/novell/sentinel/3rdparty/elasticsearch/elasticsearch.yml：

9a 確定 elasticsearch.yml 檔案中的 cluster.name 和 discovery.zen.ping.unicast.hosts 值與外部 Elasticsearch 節點中的 elasticsearch.yml 檔案相同。

9b 在 network.host 內容中指定 localhost IP 位址，並於其後指定本機 Elasticsearch 節點的 IP 位址，如下所示：

network.host: ["127.0.0.1","<*Sentinel 中 Elasticsearch 節點的 IP 位址*>"]

10 (條件式) 對於使用傳統儲存的 Sentinel，將外部 Elasticsearch 節點 IP 位址新增至 /etc/opt/novell/sentinel/config/elasticsearch-index.properties 檔案中的 ServerList 內容。

例如：ServerList=<*Elasticsearch IP1*>:<*Port*>,<*Elasticsearch IP2*>:<*Port*>

11 重新啟動 Sentinel：

rcsentinel restart

12 重新啟動每個 Elasticsearch 節點：

/etc/init.d/elasticsearch start

13 若要讓 Sentinel 伺服器達到最佳效能和穩定性，請將 Sentinel 伺服器中的 Elasticsearch 節點設定為專用 master-eligible 節點，讓所有事件視覺化資料在外部 Elasticsearch 節點中編製索引：

13a 以 novell 使用者身分登入 Sentinel 伺服器。

13b 確定所有現有的警示資料皆已移至外部 Elasticsearch 節點。

13c 開啟 /etc/opt/novell/sentinel/3rdparty/elasticsearch/elasticsearch.yml 檔案並新增下列資訊：

```
node.master: true
node.data: false
node.ingest: false
search.remote.connect: false
```

13d 重新啟動 Elasticsearch：

rcsentinel stopSIdb

rcsentinel startSIdb

14 繼續執行 「保護 Elasticsearch 中的資料」(第 75 頁)。

保護 Elasticsearch 中的資料

Elasticsearch 叢集節點可供多種不同的用戶端存取，例如：

- Sentinel：用以擷取和顯示「事件視覺化」儀表板中的事件資料。
- 在YARNNodeManager節點中執行的Spark工作：用以執行從Kafka所接收事件的大量索引編製。(適用於 SSDM)
- Collector Manager：用以對使用傳統儲存的 Sentinel 中的事件執行大量索引編製。
- 其他外部用戶端：用以執行自訂作業，例如自訂分析。

Sentinel 針對 Elasticsearch 提供了名為 **elasticsearch-security-plugin** 的安全性外掛程式，用以驗證 Elasticsearch 及授與其存取權。

此外掛程式會根據用戶端的連線方式，使用 SAML 記號或白名單進行驗證：

- 當用戶端連同要求傳送 SAML 記號時，此外掛程式會對 Sentinel 驗證伺服器驗證記號。驗證成功時，此外掛程式只會允許存取用戶端已獲授權的篩選事件。

  例如，「事件視覺化」儀表板 (用戶端) 只會顯示 Elasticsearch 中可供經過授權的使用者角色檢視的事件。

  如需角色和權限的相關資訊，請參閱 *Sentinel 管理指南*中的「建立角色」。
- 當用戶端無法傳送 SAML 記號時，此外掛程式會檢查其合法用戶端的白名單。驗證成功時，此外掛程式會允許存取所有事件，而不加以篩選。
- 當用戶端未傳送有效的 SAML 記號或未經白名單的允許時，此外掛程式會將其視為不合法的用戶端，而拒絕用戶端的存取。

本節提供安裝和設定 Elasticsearch 安全性外掛程式的相關資訊：

- 「安裝 Elasticsearch 安全性外掛程式」(第 76 頁)
- 「為其他 Elasticsearch 用戶端提供安全存取權」(第 77 頁)
- 「更新 Elasticsearch 外掛程式組態」(第 78 頁)

安裝 Elasticsearch 安全性外掛程式

您必須在 Elasticsearch 叢集的每個節點中和 Sentinel 所包含的 Elasticsearch 節點中安裝 Elasticsearch 安全性外掛程式。

若要在 Sentinel 所包含的 Elasticsearch 節點上安裝 elasticsearch-security-plug-in：

1. 登入 Sentinel Main 或 SSDM 伺服器。
2. 依照下列方式設定 JAVA_HOME 環境變數的路徑：

   ```
   export JAVA_HOME=/<Sentinel_installation_path>/opt/novell/sentinel/jdk/
   ```

3. 安裝外掛程式：

   對於 Linux，請以執行 Elasticsearch 的使用者身分登入，並執行下列指令：

   ```
   <sentinel_installation_path>/opt/novell/sentinel/3rdparty/elasticsearch/bin/elasticsearch-plugin install file://localhost/<Sentinel_installation_path>/etc/opt/novell/sentinel/scalablestore/elasticsearch-security-plugin*.zip --verbose
   ```

   出現是否要繼續安裝的提示時，請輸入 y。

4. (條件式) 如果 Elasticsearch 未在預設 HTTP 連接埠 (9200) 上接聽，則您必須在 <Sentinel_installation_path>/opt/novell/sentinel/3rdparty/elasticsearch/plugins/elasticsearch-security-plugin/elasticsearch-ip-whitelist.txt 檔案的每個項目中更新 Elasticsearch 連接埠號碼。

   如需詳細資訊，請參閱「使用白名單為 Elasticsearch 用戶端提供存取權」(第 77 頁)。

5. 使用下列指令重新啟動 Sentinel 中的索引服務：

   ```
   rcsentinel stopSIdb
   rcsentinel startSIdb
   ```

若要在外部 Elasticsearch 節點上安裝 elasticsearch-security-plug-in：

在 Elasticsearch 叢集中的每個節點上執行下列步驟：

1. 登入 Sentinel Main 或 SSDM 伺服器。
2. 將 <Sentinel_installation_path>/etc/opt/novell/sentinel/scalablestore/elasticsearch-security-plugin*.zip 檔案複製到 Elasticsearch 叢集中每個節點上的暫存位置。
3. 安裝外掛程式：

   對於 Linux，請以執行 Elasticsearch 的使用者身分登入，並執行下列指令：

   ```
   <elasticsearch_install_directory>/bin/elasticsearch-plugin install file://localhost/<full path of elasticsearch-security-plugin*.zip file> --verbose
   ```

   出現是否要繼續安裝的提示時，請輸入 y。

4. (條件式) 如果 Elasticsearch 未在預設 HTTP 連接埠 (9200) 上接聽，則您必須在 <elasticsearch_install_directory>/plugins/elasticsearch-security-plugin/elasticsearch-ip-whitelist.txt 檔案的每個項目中更新 Elasticsearch 連接埠號碼。

如需詳細資訊，請參閱「使用白名單為 Elasticsearch 用戶端提供存取權」(第 77 頁)。

5 重新啟動 Elasticsearch。

為其他 Elasticsearch 用戶端提供安全存取權

根據預設，信任的用戶端如 SSDM 伺服器 (適用於「事件視覺化」儀表板) 和 YARN NodeManagers、Sentinel 伺服器 (適用於「事件視覺化」儀表板) 和 RCM，皆可存取 Elasticsearch。如果您想要使用其他 Elasticsearch 用戶端，您必須使用 SAML 記號或白名單為這些用戶端提供安全存取權。

使用 SAML 記號為 Elasticsearch REST 用戶端提供存取權

如果您要使用 REST 用戶端來存取 Elasticsearch，您可以在要求標題中包含 SAML 記號，如下所示：

1 從 Sentinel 驗證伺服器取得 SAML 記號。如需詳細資訊，請參閱 Sentinel 中提供的 REST API 文件。

按一下「說明」>「API」>「教學課程」>「API 安全性」>「取得 SAML 記號 (登入)」。

2 在後續的REST要求中使用SAML記號：在REST用戶端所提出之每個要求的「授權」標題中包含 SAML 記號。將標題名稱指定為授權，並將標題值指定為在步驟 1 中取得的 <*SAML 記號*>。

使用白名單為 Elasticsearch 用戶端提供存取權

根據預設，Sentinel 會在白名單中自動填入信任的 Elasticsearch 用戶端 IP 位址，例如 SSDM 伺服器 (適用於「事件視覺化」儀表板) 和 YARN NodeManagers、Sentinel 伺服器 (適用於「事件視覺化」儀表板) 和 RCM。Elasticsearch 安全性外掛程式會為白名單中所列的所有用戶端授與 Elasticsearch 的存取權。

若要為未傳送有效 Sentinel 記號的其他用戶端提供存取權，您必須以 IP 位址:連接埠的格式，將用戶端的 IP 位址和 Elasticsearch 伺服器的 HTTP 連接埠號碼新增至白名單。您必須確定您在白名單中新增的外部用戶端是合法且可信任的，以防止任何未經授權的存取。

如果要更新白名單：

1 以執行 Elasticsearch 的使用者身分，登入 Sentinel 伺服器或 Elasticsearch 節點。

2 在下列檔案中新增項目 <Elasticsearch_Client_IP>:<Target_Elasticsearch_HTTP_Port>：

- <Sentinel_installation_path>/opt/novell/sentinel/3rdparty/elasticsearch/plugins/elasticsearch-security-plugin/elasticsearch-ip-whitelist.txt (適用於 Sentinel 中包含的 Elasticsearch 節點)。
- <elasticsearch_install_directory>/plugins/elasticsearch-security-plugin/elasticsearch-ip-whitelist.txt (適用於外部 Elasticsearch 節點)。

如果有多個項目，請將每個項目新增於不同行，並儲存檔案。

3 在 Elasticsearch 叢集的每個節點中重複上述步驟。

更新 Elasticsearch 外掛程式組態

如果您修改了可擴充儲存元件的 IP 位址/主機名稱和連接埠號碼，或是 Elasticsearch 版本和連接埠號碼，則必須對 Elasticsearch 外掛程式組態檔案進行相對應的更新。

在 Elasticsearch 叢集的每個節點上執行下列步驟：

1. 以執行 Elasticsearch 的使用者身分登入 Elasticsearch 節點。
2. (條件式) 如果您修改了 YARN NodeManager IP 位址、SSDM 或 Sentinel 伺服器 IP 位址、RCM IP 位址或 Elasticsearch 連接埠號碼，請對白名單進行相對應的更新，以確定 Elasticsearch 安全性外掛程式會為 Elasticsearch 用戶端授與存取權。

   如果您要在 HA 模式下設定 SSDM 或 Sentinel，請為 HA 叢集的每個主動節點和被動節點新增實體 IP 位址項目。

   如果您為 HA 叢集的任何節點修改了實體 IP 位址，或是將新的節點新增至 HA 叢集，請使用已修改或新增之節點的實體 IP 位址更新白名單。

   如需詳細資訊，請參閱「使用白名單為 Elasticsearch 用戶端提供存取權」(第 77 頁)。
3. (條件式) 如果您修改了 SSDM IP 位址、Sentinel 伺服器 IP 位址或 Web 伺服器連接埠號碼，請更新下列檔案中的 authServer.host 和 authServer.port 內容，並重新啟動 Elasticsearch：
   - <Sentinel_installation_path>/opt/novell/sentinel/3rdparty/elasticsearch/plugins/elasticsearch-security-plugin/plugin-configuration.properties (適用於 Sentinel 中包含的 Elasticsearch 節點)。
   - <elasticsearch_install_directory>/plugins/elasticsearch-security-plugin/plugin-configuration.properties (適用於外部 Elasticsearch 節點)。

   如果您要在 HA 模式中設定 SSDM 或 Sentinel，請將 authServer.host 內容設定為 HA 叢集的虛擬 IP 位址。

   如果您修改了 HA 叢集的虛擬 IP 位址，請將 authServer.host 內容更新為已修改的虛擬 IP 位址。
4. (條件式) 如果您將 Elasticsearch 升級至新版本，請更新下列檔案中的 elasticsearch.version 內容，並重新啟動 Elasticsearch：
   - /opt/novell/sentinel/3rdparty/elasticsearch/plugins/elasticsearch-security-plugin/plugin-descriptor.properties (適用於 Sentinel 中包含的 Elasticsearch 節點)。
   - <elasticsearch_install_directory>/plugins/elasticsearch-security-plugin/plugin-descriptor.properties (適用於外部 Elasticsearch 節點)。

Elasticsearch 的效能調整

Sentinel 會自動設定下表所說明的 Elasticsearch 設定。您可以視需要自訂 Elasticsearch 設定。

若要自訂預設設定：

對於傳統儲存： 開啟 /etc/opt/novell/sentinel/config/elasticsearch-index.properties 檔案，並視需要更新表格中所列的內容。

對於可擴充儲存： 在 SSDM 的首頁中，按一下「**儲存**」>「**可擴充儲存**」>「**進階內容**」>「**Elasticsearch**」。

表格 12-1 Elasticsearch 內容

內容	預設值	附註
elasticsearch.events.lucenefilter (選用)		指定僅將特定事件傳送至 Elasticsearch 進行索引編製的篩選器。例如：如果您將值指定為 sev:[3-5]，則只會將嚴重性值介於 3 和 5 之間的事件傳送至 Elasticsearch。
index.fields	id,dt,rv171,msg,ei,evt,xdastaxname,xdasoutcomename,sev,vul,rv32,rv39,rv159,dhn,dip,rv98,dp,fn,rv199,dun,tufname,rv84,rv158,shn,sip,rv76,sun,iufname,sp,iudep,rv198,rv62,st,tid,srcgeo,destgeo,obsgeo,rv145,estz,estzmonth,estzdiy,estzdim,estzdiw,estzhour,estzmin,rv24,tudep,pn,xdasclass,xdasid,xdasreg,xdasprov,iuident,tuident	指出您要讓 Elasticsearch 編製索引的事件欄位。
es.num.shards	5	指出每個索引的主要分區數。 您可以在分區大小超過 50 GB 時增加此預設值。
es.num.replicas	1	指出每個主要分區應有的複本分區數。 考量到容錯移轉和高可用性的需求，建議至少應為 2 個節點叢集。

重新部署 Elasticsearch 安全性外掛程式

在下列情況下，您必須重新部署，也就是在 Sentinel 中包含的 Elasticsearch 節點和外部 Elasticsearch 節點中解除安裝 Elasticsearch 安全性外掛程式，再加以重新安裝：

- 新增或修改遠端 Collector Manager IP 位址。
- 解除安裝遠端 Collector Manager。
- 啟用可擴充儲存後續安裝。

若要重新部署 Elasticsearch 安全性外掛程式：

1. 以執行 Elasticsearch 的使用者身分，登入 Sentinel 伺服器或 Elasticsearch 節點。
2. 使用下列指令解除安裝外掛程式：
   - 對於 Sentinel 中包含的 Elasticsearch：<Sentinel_installation_path>/opt/novell/sentinel/3rdparty/elasticsearch/bin/elasticsearch-plugin remove file://localhost/<Sentinel_installation_path>/etc/opt/novell/sentinel/scalablestore/elasticsearchsecurity-plugin
   - 對於外部 Elasticsearch：<elasticsearch_install_directory> remove file://localhost/etc/opt/novell/sentinel/scalablestore/elasticsearchsecurity-plugin

3 重新安裝外掛程式：

- 對於 Sentinel 中包含的 Elasticsearch：<Sentinel_installation_path>/opt/novell/sentinel/3rdparty/elasticsearch/bin/elasticsearch-plugin install file://localhost/<Sentinel_installation_path>/etc/opt/novell/sentinel/scalablestore/elasticsearchsecurity-plugin
- 對於外部 Elasticsearch：<elasticsearch_install_directory>/bin/elasticsearch-plugin install file://localhost/etc/opt/novell/sentinel/scalablestore/elasticsearchsecurity-plugin

4 使用下列指令重新啟動 Elasticsearch：

- 對於 Sentinel 中包含的 Elasticsearch 節點：

  ```
  rcsentinel stopSIdb
  rcsentinel startSIdb
  ```

- 對於外部 Elasticsearch 節點：

  sudo systemctl restart elasticsearch.service

13 安裝和設定可擴充儲存

請完成下表所列的先決條件，以設定可擴充儲存做為 Sentinel 的資料儲存選項：

表格 13-1 *啟用可擴充儲存的先決條件*

❒	任務	請參閱
❒	根據所需EPS率和複本數，判斷需要設定的Hadoop分配叢集數和 Elasticsearch 叢集節點數。 判斷 CDH 和 Elasticsearch 的認證版本。	Sentinel 技術資訊。
❒	CDH、Elasticsearch 和 Sentinel 都具有自己的平台支援矩陣。請檢閱每個產品的平台支援矩陣，並判斷要使用的平台。 對於 Elasticsearch 建議使用 RPM 安裝，因為 RPM 包含 init 程序檔。這會將 Elasticsearch 安裝為服務，並讓其在重新開機和升級期間自動停止和啟動，且不會覆寫組態檔案。 SLES 11 不支援 Elasticsearch RPM 安裝。因此，請判斷適合 Elasticsearch 的平台。	CDH 支援 Cloudera 文件內的矩陣。 Elasticsearch 支援 Elasticsearch 文件內的矩陣。 Sentinel 支援矩陣。
❒	在叢集模式中安裝和設定 CDH。	「安裝和設定 CDH」(第 81 頁)。
❒	在叢集模式中安裝和設定 Elasticsearch。	「安裝和設定 Elasticsearch」(第 73 頁)。
❒	在 Sentinel 中啟用可擴充儲存。	「啟用可擴充儲存」(第 83 頁)

安裝和設定 CDH

本節提供安裝和設定CDH時，Sentinel所需特定設定的相關資訊。如需有關CDH安裝和組態的詳細資訊，您必須參閱 Cloudera 文件的認證版本。

Sentinel 可與 CDH 的免費版本 Cloudera Express 搭配運作。Sentinel 也可與 Cloudera Enterprise 搭配運作。該版本需要向 Cloudera 購買授權，且包括 Cloudera Express 版本無法使用的數種功能。如果您選擇從 Cloudera Express 開始，而之後發現需要 Cloudera Enterprise 所提供的功能，則可以在向 Cloudera 購買授權後升級叢集。

必要條件

安裝 CDH 前，您必須根據下列先決條件設定主機：

- 完成 Cloudera 文件中所述的先決條件。
- 使用 ext4 或 XFS 檔案系統以獲取更佳效能。
- CDH需要預設不會安裝的某些作業系統套件。因此，您必須掛接各自的作業系統DVD。Cloudera 安裝指示會指引您要安裝的套件。
- 針對 SLES 作業系統，CDH 需要 python-psycopg2 套件。安裝 python-psycopg2 套件。如需詳細資訊，請參閱 openSUSE 文件。
- 如果您正在使用虛擬機器，建立虛擬機器節點時，請在檔案系統上保留所需的磁碟空間。例如，在 VMware 中，您可以使用完整佈建。
- 請確定 Sentinel 和 CDH 叢集節點位於相同的時區中。
- 透過新增下列項目，在 /etc/sysctl.conf 檔案中將所有主機的交換性設定為 1：

  ```
  vm.swappiness=1
  ```

  若要立即套用此設定，請執行下列指令：

  ```
  sysctl -p
  ```

- CDH中的JDK版本必須至少與Sentinel中使用的JDK版本相同。如果CDH中提供的JDK版本低於 Sentinel JDK，您必須遵循指示以手動安裝 JDK，而非安裝 CDH 儲存機制中提供的 JDK。

  在使用manage_spark_jobs.sh程序檔以在YARN提交Sparks工作時，JRKRPM安裝發生問題，請使用歸檔二進位檔案 (.tar.gz) 安裝 JDK。

  如要判斷 Sentinel 內使用的 JDK 版本，請參閱 Sentinel 版本說明。

安裝和設定 CDH

安裝 CDH 的認證版本。如需關於 CDH 認證版本詳細資訊，請參閱 Sentinel 技術性資訊頁面。請參閱 Cloudera 文件的認證版本以取得安裝指示。

安裝 CDH 時，請執行下列作業：

- (條件式) 如果安裝程序在安裝內嵌式 PostgreSQL 資料庫時失敗，請執行以下步驟：

  ```
  mkdir -p /var/run/postgresql
  ```

  ```
  sudo chown cloudera-scm:cloudera-scm /var/run/postgresql
  ```

- 在「**選取儲存機制**」視窗中選擇軟體安裝類型時，請確定已選取「**使用包裹**」，並在「**其他包裹**」中選取「Kafka」。
- 新增服務時，請確定您已啟用下列服務：
  - Cloudera Manager
  - ZooKeeper
  - HDFS
  - HBase
  - YARN

- Spark
- Kafka

附註： 您必須在相同的節點上安裝Spark歷程伺服器和HDFSNameNode，以取得系統可靠性。如需可擴充儲存架構的資訊，請參閱「可擴充儲存規劃」(第 42 頁)。

啟用以上服務時，請設定以下項目為高可用性：

- HBase HMaster
- HDFS NameNode
- YARN ResourceManager

- (條件式) 如果安裝程式因找不到 Java 路徑而無法部署用戶端組態，請開啟新瀏覽器工作階段並手動更新 Java 路徑，如下所示：

  按一下「**主機**」>「**所有主機**」>「**組態**」，並在「**Java 主目錄**」欄位中指定正確的路徑。

啟用可擴充儲存

您可以在安裝 Sentinel 期間或後續安裝工作中啟用可擴充儲存。在安裝期間啟用可擴充儲存時，Sentinel 會以預設值設定 CDH 元件。某些組態為永久組態且無法變更。例如，Kafka 主題分割區的預設數字為 9，且您無法變更此值。

如果您想要變更預設值，則必須在安裝 Sentinel 後啟用可擴充儲存，然後視需要設定 CDH 元件的組態。

針對傳統安裝，您可以在安裝 Sentinel 期間或安裝 Sentinel 後啟用可擴充儲存。針對裝置安裝，您只能在安裝後啟用可擴充儲存。

若要升級安裝程式，您可以先升級 Sentinel，再啟用可擴充儲存。

繼續啟用可擴充儲存前，請備妥 Kafka、HDFS NameNode、YARN NodeManager、ZooKeeper 和 Elasticsearch 節點的 IP 位址清單或主機名稱和連接埠號碼。啟用可擴充儲整時，您會需要此資訊。

若要在安裝 Sentinel 期間啟用可擴充儲存，請參閱「Sentinel Server 自定安裝」(第 86 頁)。

若要在安裝或升級 Sentinel 後啟用可擴充儲存，請參閱「《 Sentinel 管理指南》」中的*「在後續安裝工作中啟用可擴充儲存」*。

14 傳統安裝

本章節提供 Sentinel 各種安裝方法的相關資訊。

執行互動式安裝

本節提供標準和自訂安裝的相關資訊。

Sentinel Server 標準安裝

執行標準安裝的步驟如下：

1. 從 下載網站下載 Sentinel 安裝檔案：
2. 在指令行指定下列指令來解壓縮安裝檔案。

   `tar zxvf <install_filename>`

   將 *<install_filename>* 取代為安裝檔案的實際名稱。
3. 移至解壓縮安裝程式的目錄：

   `cd <directory_name>`
4. 指定下列指令以安裝 Sentinel：

   `./install-sentinel`

   或

   如果您想要將 Sentinel 安裝在多個系統上，可以在檔案中記錄安裝選項。您可以使用此檔案在其他系統上進行無人管理安裝。若要記錄您的安裝選項，請指定以下指令：

   `./install-sentinel -r <response_filename>`
5. 指定要用於安裝作業的語言號碼，然後按 Enter。

   使用者授權合約會以選取的語言顯示。
6. 按下空格鍵，以完整讀取授權合約。
7. 輸入 yes 或 y，接受授權，並且繼續安裝作業。

   安裝作業會利用幾秒鐘的時間來載入安裝套件，以及提示您指定組態類型。
8. 在出現提示時，指定 1 可繼續進行標準組態。

安裝會繼續使用安裝程式中包含預設的試用版授權金鑰。在試用期間或試用期結束後，您可以隨時以購買的授權金鑰取代試用版授權。

9 指定管理員使用者 (admin) 的密碼。

10 再次確認密碼。

此密碼用於 admin、dbauser 及 appuser。

Sentinel 安裝完成，且隨之啟動伺服器。由於系統會執行一次性的啟始化，因此在安裝完成後所有服務都需要幾分鐘的時間才能啟動。請等待安裝完成後再登入伺服器。

若要存取 Sentinel 主要介面，請在網頁瀏覽器中指定下列 URL：

`https://IP_AddressOrDNS_Sentinel_server:8443/sentinel/views/main.html`

其中 *IP_AddressOrDNS_Sentinel_server* 是 Sentinel 伺服器的 IP 位址或 DNS 名稱，*8443* 是 Sentinel 伺服器的預設連接埠。

Sentinel Server 自定安裝

如果您正在以自定組態安裝 Sentinel，則可以透過指定授權金鑰、設定不同的密碼和指定不同的連接埠等，自定 Sentinel 安裝。

1 如果您想要啟用可擴充儲存，請完成第 13 章 「安裝和設定可擴充儲存」(第 81 頁)中指定的先決條件。

2 從 下載網站下載 Sentinel 安裝檔案：

3 在指令行指定下列指令來解壓縮安裝檔案。

```
tar zxvf <install_filename>
```

將 *<install_filename>* 取代為安裝檔案的實際名稱。

4 在解壓縮之目錄的根目錄中指定下列指令以安裝 Sentinel：

```
./install-sentinel
```

或

如果您想要使用此自定組態將 Sentinel 安裝在多個系統上，可以在檔案中記錄安裝選項。您可以使用此檔案在其他系統上進行無人管理安裝。若要記錄您的安裝選項，請指定以下指令：

```
./install-sentinel -r <response_filename>
```

5 指定要用於安裝作業的語言號碼，然後按 Enter。

使用者授權合約會以選取的語言顯示。

6 按下空格鍵，以完整讀取授權合約。

7 輸入 yes 或 y，接受授權合約，並且繼續安裝作業。

安裝作業會利用幾秒鐘的時間來載入安裝套件，以及提示您指定組態類型。

8 指定 2 以執行 Sentinel 自訂組態。

9 輸入 1 以使用預設的試用版授權金鑰

或

輸入 2 以輸入購買的 Sentinel 授權金鑰。

10 指定管理員使用者 (admin) 的密碼，並再次確認密碼。

11 指定資料庫使用者 (dbauser) 的密碼，並再次確認密碼。

dbauser 帳戶是 Sentinel 用來與資料庫互動的身分。您在此處輸入的密碼可用來執行資料庫維護工作，包括在忘記或遺失管理員密碼時重設管理員密碼。

12 指定應用程式使用者 (appuser) 的密碼，並再次確認密碼。

13 藉由輸入需要的號碼再指定新的連接埠號碼，變更 Sentinel 服務的連接埠指定。

14 變更連接埠後，請指定 7 來完成作業。

15 輸入 1 ，僅以內部資料庫來驗證使用者。

或

如果您已在網域中設定 LDAP 目錄，請輸入 2 以利用 LDAP 目錄驗證來驗證使用者。

預設值為 1。

16 ***若要在 FIPS 140-2 模式中啟用 Sentinel***，請輸入 y。

16a 指定 KeyStore 資料庫的增強式密碼，並再次確認密碼。

附註： 密碼長度必須至少為七個字元。密碼必須包含至少三項下列字元類型：數字、ASCII 小寫字母、ASCII 大寫字母、ASCII 非英數字元以及非 ASCII 字元。

若 ASCII 大寫字母是第一個字元或最後一個字元是數字，則不列入計算。

16b 若想要將外部證書插入 KeyStore 資料庫以建立信任，請按 y，然後指定證書檔案的路徑。如不需要，請按 n

16c 按照在「第 24 章 「以 FIPS 140-2 模式操作 Sentinel」(第 123 頁)」中提到的任務，完成 FIPS 140-2 模式組態。

17 ***如果您想要啟用可擴充儲存***，請輸入 yes 或 y 以啟用可擴充儲存。

重要： 啟用可擴充儲存後，除非重新安裝 Sentinel，否則您無法回復組態。

17a 指定可擴充儲存元件的 IP 位址或主機名稱和連接埠號碼。

17b (條件式) 如果您想要結束可擴充儲存組態並繼續安裝 Sentinel，請輸入 no 或 n。

17c Sentinel 安裝完成後，請完成「可擴充儲存的後續安裝設定」(第 87 頁)一節中說明的可擴充儲存設定。

Sentinel 安裝完成，且隨之啟動伺服器。由於系統會執行一次性的啟始化，因此在安裝完成後所有服務都需要幾分鐘的時間才能啟動。請等待安裝完成後再登入伺服器。

若要存取 Sentinel 主要介面，請在網頁瀏覽器中指定下列 URL：

`https://IP_AddressOrDNS_Sentinel_server:8443/sentinel/views/main.html`

其中 *<IP_AddressOrDNS_Sentinel_server>* 是 Sentinel 伺服器的 IP 位址或 DNS 名稱，*8443* 是 Sentinel 伺服器的預設連接埠。

可擴充儲存的後續安裝設定

1 登入 SSDM 伺服器。

2 清除瀏覽器快取，以檢視您已安裝的 Sentinel 版本。

3 若要檢視事件和警示，請將 SSDM 中包含的 Elasticsearch 節點新增至您為可擴充儲存設定的 Elasticsearch 叢集：

在本機 Elasticsearch 節點中，開啟 /etc/opt/novell/sentinel/3rdparty/elasticsearch/elasticsearch.yml 檔案並新增下列資訊：

- cluster.name: <*Elasticsearch 叢集名稱*>
- node.name: <*節點名稱*>
- discovery.zen.ping.unicast.hosts: ["<*elasticsearch 節點 1 的 FQDN*>", "<*elasticsearch 節點 2 的 FQDN*>", 等"]

在所有外部 Elasticsearch 節點中，開啟 /etc/elasticsearch/elasticsearch.yml 並更新

discovery.zen.ping.unicast.hosts: ["<*elasticsearch 節點 1 的 FQDN*>", "<*elasticsearch 節點 2 的 FQDN*>", 等"]

附註： 請確定外部 Elasticsearch 節點中的本機 elasticsearch.yml 檔案和 elasticsearch.yml 檔案中的參數值是相同的 (network.host 和 node.name 除外)，因為這些值是節點的唯一值。

---

4 使用下列指令重新啟動索引服務：

```
rcsentinel stopSIdb
rcsentinel startSIdb
```

5 依照以下幾節的說明完成可擴充儲存設定：

- 「保護 Elasticsearch 中的資料」(第 75 頁)
- *Sentinel 管理指南*中的效能調整指引
- *Sentinel 管理指南*中的處理資料

Collector Manager 與 Correlation Engine 安裝

Sentinel 預設安裝 Collector Manager 和 Correlation Engine。在生產環境中，請設定分散式部署，因為這樣可將資料收集元件隔離到個別機器上；如想在處理流量突增和其他異常情況時維持最高的系統穩定性，這項做法相當重要。如需有關安裝額外元件有何優點的詳細資訊，請參閱「分散式佈署的優點」(第 44 頁)。

重要： 您必須在不同的系統上安裝其他 Collector Manager 或 Correlation Engine。Collector Manager 或 Correlation Engine 不得位於安裝 Sentinel 伺服器的相同系統上。

安裝核對清單: 在開始安裝之前，請確認您已完成下列工作。

- 確認硬體和軟體符合最低需求。如需詳細資訊，請參閱第 5 章「符合系統需求」(第 37 頁)。
- 使用網路時間通訊協定 (NTP) 同步化時間。
- Collector Manager 需要網路連接至 Sentinel 伺服器上的訊息匯流排連接埠 (61616)。在開始安裝 Collector Manager 之前，請務必允許所有防火牆及其他網路設定透過此連接埠進行通訊。

若要安裝 Collector Manager 或 Correlation Engine，請使用下列步驟：

1 在網頁瀏覽器中指定下列 URL 以啟動 Sentinel 主要介面：

```
https://IP_AddressOrDNS_Sentinel_server:8443/sentinel/views/main.html
```

其中 <*IP_AddressOrDNS_Sentinel_server*> 是 Sentinel 伺服器的 IP 位址或 DNS 名稱，*8443* 是 Sentinel 伺服器的預設連接埠。

使用在 Sentinel 伺服器安裝期間指定的使用者名稱和密碼登入。

2 按一下工具列中的「下載」。

3 按一下所需安裝之下的「下載安裝程式」。

4 按一下「儲存檔案」以將安裝程式儲存在需要的位置。

5 指定下列指令來解壓縮安裝檔案。

```
tar zxvf <install_filename>
```

將 *<install_filename>* 取代為安裝檔案的實際名稱。

6 移至解壓縮安裝程式的目錄。

7 指定下列指令以安裝 Collector Manager 或 Correlation Engine：

針對 Collector Manager：

```
./install-cm
```

針對 Correlation Engine：

```
./install-ce
```

或

如果您想要將 Collector Manager 或 Correlation Engine 安裝在多個系統上，您可以在檔案中記錄安裝選項。您可以使用此檔案在其他系統上進行無人管理安裝。若要記錄您的安裝選項，請指定以下指令：

針對 Collector Manager：

```
./install-cm -r <response_filename>
```

針對 Correlation Engine：

```
./install-ce -r <response_filename>
```

8 指定要用於安裝作業的語言號碼。

使用者授權合約會以選取的語言顯示。

9 按下空格鍵，以完整讀取授權合約。

10 輸入 yes 或 y，接受授權合約，並且繼續安裝作業。

安裝作業會利用幾秒鐘的時間來載入安裝套件，以及提示您指定組態類型。

11 出現提示時，請指定適當的選項繼續進行標準或自定組態。

12 輸入預設的通訊伺服器主機名稱或安裝 Sentinel 之機器的 IP 位址。

13 (條件式) 如果您已選用自定組態，請指定下列項目：

13a Sentinel 伺服器通訊通道連接埠號碼。

13b Sentinel Web 伺服器連接埠號碼。

14 當提示接受證書時，請在 Sentinel 伺服器中執行下列指令來驗證證書：

針對 FIPS 模式：

```
/opt/novell/sentinel/jdk/jre/bin/keytool -list -keystore
/etc/opt/novell/sentinel/config/.activemqkeystore.jks
```

針對非 FIPS 模式：

```
/opt/novell/sentinel/jdk/jre/bin/keytool -list -keystore
/etc/opt/novell/sentinel/config/nonfips_backup/.activemqkeystore.jks
```

將證書輸出與 步驟 12 中顯示的 Sentinel 伺服器證書互相比對。

附註： 如果證書不符合，安裝便會停止。再次執行安裝並檢查證書。

15 若證書輸出與 Sentinel 伺服器證書相符，則接受證書。

16 指定管理員角色中任何使用者的身分證明。輸入使用者名稱與密碼。

17 (條件式) 如果您已選用自訂組態，請輸入 yes 或 y 來啟用 Sentinel 中的 FIPS 140-2 模式，並繼續 FIPS 組態。

18 (條件式) 如果您的環境使用多因素或增強式驗證，您必須提供 Sentinel 用戶端 ID 和 Sentinel 用戶端密碼。如需有關驗證方法的詳細資訊，請參閱《*Sentinel 管理員指南*》中的「「驗證方法」」。

若要取回 Sentinel 用戶端 ID 和 Sentinel 用戶端密碼，請前往以下 URL：

https://*主機名稱*:*連接埠*/SentinelAuthServices/oauth/clients

其中：

- *主機名稱*是 Sentinel 伺服器的主機名稱。
- *連接埠*是 Sentinel 使用的連接埠 (通常是 8443)。

指定 URL 使用您目前的 Sentinel 工作階段取回 Sentinel 用戶端 ID 和 Sentinel 用戶端密碼。

19 (條件式) 如果您已啟用事件視覺化，則必須將 Collector Manager 新增至 Elasticsearch 白名單。如需詳細資訊，請參閱「使用白名單為 Elasticsearch 用戶端提供存取權」(第 77 頁)。

20 依提示繼續安裝，直到完成為止。

執行靜默安裝

如果您需要在部署中安裝多個 Sentinel 伺服器、Collector Manager 或 Correlation Engine，靜默安裝或無人管理安裝很有用。在此類情況下，您可以在互動安裝期間記錄安裝參數，然後在其他伺服器上執行記錄的檔案。

若要執行靜默安裝，請確認您已將安裝參數記錄在檔案中。如需建立回應檔案的相關資訊，請參閱「Sentinel Server 標準安裝」(第 85 頁) 或 「Sentinel Server 自定安裝」(第 86 頁) 與 「Collector Manager 與 Correlation Engine 安裝」(第 88 頁)。

若啟用 FIPS 140-2 模式，請確保回應檔案包含下列參數：

- ENABLE_FIPS_MODE
- NSS_DB_PASSWORD

若要執行靜默安裝，步驟如下：

1 從 下載網站下載安裝檔案：

2 請以 root 身分登入您要安裝 Sentinel、Collector Manager 或 Correlation Engine 的伺服器。

3 指定下列指令，以從 tar 檔案擷取安裝檔案：

```
tar -zxvf <install_filename>
```

將 *<install_filename>* 取代為安裝檔案的實際名稱。

4 指定下列指令以在靜默模式下執行安裝：

針對 Sentinel 伺服器：

./install-sentinel -u <*response_file*>

針對 Collector Manager：

./install-cm -u <*response_file*>

針對 Correlation Engine：

./install-ce -u <*response_file*>

系統將會利用儲存在回應檔案中的值繼續進行安裝。

如果您已安裝 Sentinel 伺服器，由於系統會執行一次性的啟始化，因此在安裝完成後會需要幾分鐘的時間才能啟動所有服務。請等待安裝完成後再登入伺服器。

5 **(條件式) 如果您針對 Sentinel 伺服器已選擇啟用 FIPS 140-2 模式，** 按照在「第 24 章 「以 FIPS 140-2 模式操作 Sentinel」(第 123 頁)」中提到的任務，完成 FIPS 140-2 模式組態。

以非 root 使用者安裝 Sentinel

若您的組織規則不允許以 root 使用者身分執行完整 Sentinel 安裝，您可以使用非 root 使用者身分來安裝 Sentinel；也就是 novell 使用者。在此類型的安裝作業中，有幾個步驟是以 root 使用者的身分執行，接著您需要以 root 使用者建立的 novell 使用者身分來繼續安裝 Sentinel。最後，root 使用者會完成安裝。

以非 root 使用者身分安裝 Sentinel 時，您應以 novell 使用者身分安裝 Sentinel。Novell 使用者以外的非根安裝不受支援，但安裝仍可繼續執行。

附註： 在現有的非預設目錄中安裝 Sentinel 時，請確定 Novell 使用者具備該目錄的擁有權權限。指定下列指令以在靜默模式指派擁有權權限：

chown novell:novell <*non-default installation directory*>

---

1 從 下載網站下載安裝檔案：

2 在指令行指定下列指令，以從 tar 檔案擷取安裝檔案：

tar -zxvf <*install_filename*>

將 <*install_filename*> 取代為安裝檔案的實際名稱。

3 以 root 身分登入要以 root 身分安裝 Sentinel 的伺服器。

4 請指定以下指令：

./bin/root_install_prepare

以 root 權限執行之指令清單會顯示出來。如果您想要讓非 root 使用者將 Sentinel 安裝在非預設位置，請在指令中指定 --location 選項。例如：

./bin/root_install_prepare --location=/foo

傳遞至 --location 選項的 foo 值會加在目錄路徑的前面。

如此還會建立 novell 群組與 novell 使用者 (如果它們不存在)。

5 接受指令清單。

即會執行顯示的指令。

6 指定以下指令，以變更為新建立的非 root 使用者；即為 novell：

su novell

7 (條件式) 若要進行互動安裝：

7a 根據您要安裝的元件來指定適當的指令：

元件	指令
Sentinel 伺服器	**預設位置:** ./install-sentinel
	非預設位置： ./install-sentinel --location=/foo
Collector Manager	**預設位置:** ./install-cm
	非預設位置： ./install-cm --location=/foo
Correlation Engine	**預設位置:** ./install-ce
	非預設位置： ./install-cm --location=/foo

7b 繼續執行步驟 9。

8 (條件式) 若要執行靜默安裝，請確認您已將安裝參數記錄在檔案中。如需建立回應檔案的相關資訊，請參閱「Sentinel Server 標準安裝」(第 85 頁)或「Sentinel Server 自定安裝」(第 86 頁)。

若要進行靜默安裝：

8a 根據您要安裝的元件來指定適當的指令：

元件	指令
Sentinel 伺服器	**預設位置:** ./install-sentinel -u <*response_file*>
	非預設位置 ./install-sentinel --location=/foo -u <*response_file*>
Collector Manager	**預設位置:** ./install-cm -u <*response_file*>
	非預設位置： ./install-cm --location=/foo -u <*response_file*>
Correlation Engine	**預設位置:** ./install-ce -u <*response_file*>
	非預設位置： ./install-ce --location=/foo -u <*response_file*>

系統將會利用儲存在回應檔案中的值繼續進行安裝。

8b 繼續執行步驟 12。

9 指定要用於安裝作業的語言號碼。

使用者授權合約會以選取的語言顯示。

10 閱讀使用者授權，並輸入 yes 或 y，接受授權，然後繼續安裝。

安裝會開始安裝所有 RPM 封裝。此安裝可能需要數秒鐘完成。

11 系統會提示您指定安裝模式。

- 若您選擇繼續進行標準組態，請繼續執行「「Sentinel Server 標準安裝」(第 85 頁)」中的步驟 8到步驟 10。
- 若您選擇繼續進行自定組態，請繼續執行「步驟 8」中的步驟 15到「Sentinel Server 自定安裝」(第 86 頁)。

12 以 root 使用者身分登入，並指定下列指令以完成安裝：

```
./bin/root_install_finish
```

Sentinel 安裝完成，且隨之啟動伺服器。由於系統會執行一次性的啟始化，因此在安裝完成後所有服務都需要幾分鐘的時間才能啟動。請等待安裝完成後再登入伺服器。

若要存取 Sentinel 主要介面，請在網頁瀏覽器中指定下列 URL：

https://*IP_AddressOrDNS_Sentinel_server*:*8443*/sentinel/views/main.html

其中 *IP_AddressOrDNS_Sentinel_server* 是 Sentinel 伺服器的 IP 位址或 DNS 名稱，*8443* 是 Sentinel 伺服器的預設連接埠。

15 裝置安裝

Sentinel 應用裝置是以 Micro Focus 通用裝置架構為基礎，且處於準備執行狀態的軟體應用裝置。這項應用裝置結合了強化的 SLES 12 SP3 作業系統，以及 Sentinel 軟體整合式更新服務，可讓您運用現有的投資，同時提供簡單而流暢的使用者經驗。Sentinel 應用裝置提供 Web 式使用者介面，用於設定及監控應用裝置。

Sentinel 應用裝置影像已封裝為 ISO 和 OVF 格式，可部署至虛擬環境。如需要支援的虛擬化平台相關資訊，請參閱 Sentinel 技術資訊網站。

必要條件

確保您將以 ISO 裝置安裝的環境符合以下必要條件：

- 安裝 Sentinel 應用裝置之前，請先查看支援的 SLES 版本說明中的新功能和已知問題。
- (條件式) 若您在空機硬碟上安裝 Sentinel ISO 應用裝置，請自支援網站下載應用裝置 ISO 磁碟影像，並製作成 DVD。
- 確定硬碟空間最少有 50 GB，方便安裝程式提出自動分割區提案。
- 確定系統符合 4GB 記憶體空間的最低安裝需求。如果記憶體空間小於 4 GB，則安裝程序將會失敗。如果記憶體空間大於 4 GB，但少於所建議的 24 GB，則安裝作業會顯示一則訊息，提示您記憶體空間少於建議的大小。

安裝 Sentinel ISO 裝置

本節提供利用 ISO 裝置影像安裝 Sentinel、Collector Manager 和 Correlation Engine 的相關資訊。影像格式可讓您產生完整磁碟影像格式，利用可開機的 ISO DVD 影像部署至硬體，不論其為實體(空機) 或虛擬 (在監管程式中解除安裝的虛擬機器)。

安裝 Sentinel

安裝 Sentinel ISO 裝置：

1. 至 下載網站下載 ISO 虛擬裝置影像。
2. (條件式) 若您使用的是監管程式：

使用 ISO 虛擬裝置影像設定虛擬機器，然後將虛擬機器開啟。

或

將 ISO 影像複製至 DVD，使用 DVD 設定虛擬機器，接著開啟。

3 (條件式) 若您在空機硬體上安裝 Sentinel 裝置：

3a 使用 DVD 光碟機中的 DVD 啟動實體機器。

3b 請遵照安裝精靈畫面上的指示。

3c 選取**安裝 Sentinel 伺服器 <*版本*>**

4 選取您所選擇的語言。

5 選取鍵盤配置。

6 按**下一步**。

7 閱讀並接受「 SUSE Enterprise Server Software 授權合約」。按「**下一步**」

8 閱讀並接受 Sentinel 伺服器裝置授權合約。按「**下一步**」

9 設定 Sentinel 應用裝置密碼、NTP 組態和時區。

設定 vaadmin 使用者身分證明，以登入·Sentinel 應用裝置管理主控台。

附註： 安裝後，您可以透過以下方式變更 NTP 組態和時區：

- 移至指令提示字元視窗，並輸入 yast->網路服務->NTP 組態
- 移至 Sentienl 應用裝置管理主控台，按一下**「時間」**

如果安裝之後，沒有立即同步顯示時間，請執行下列指令來重新啟動 NTP：

```
rcntp restart
```

---

10 在 Sentinel 伺服器裝置的「網路設定」頁面上，指定主機名稱和網域名稱。選取**「靜態 IP 位址」**或**「DHCP IP 位址」**。

11 按**下一步**。

12 (條件式) 如果您在步驟 10 中選取了**「靜態 IP 位址」**，請指定網路連線設定。

13 按一下**「下一步」**。

14 設定 Sentinel 使用者管理密碼，然後按一下**「下一步」**。

裝置隨即安裝。

15 將主控台中顯示的裝置 IP 位址記下來。

16 以根使用者身分登入主控台，以登入應用裝置。

以根使用者身分輸入使用者名稱，並輸入您在 步驟 9 中設定的密碼。

17 繼續執行 「安裝裝置後的組態」(第 99 頁)。

安裝 Collector Manager 和 Correlation Engine

Collector Manager 或 Correlation Engine 的安裝程序與 Sentinel 類似，但您必須先從下載網站下載適當 ISO 應用裝置檔案。

1 完成在 「安裝 Sentinel」(第 95 頁) 中的步驟 1 至步驟 13。

安裝作業會檢查可用的記憶體和磁碟空間。如果可用的記憶體少於 1 GB，安裝作業便不會讓您繼續進行安裝，因此「下一步」按鈕會變成灰色的。

2 指定 Collector Manager 或 Correlation Engine 的下列組態：

- **Sentinel 伺服器的主機名稱或 IP 位址：** 指定 Collector Manager 或 Correlation Engine 應連接之 Sentinel 伺服器的主機名稱或 IP 位址。
- **Sentinel 通訊通道連接埠：** 指定 Sentinel 伺服器通訊通道連接埠號碼。預設連接埠號碼為 61616。
- **Sentinel Web 伺服器連接埠：** 指定 Sentinel Web 伺服器連接埠。預設埠為 8443。
- **具有管理員角色的使用者名稱：** 指定管理員角色中任何使用者的使用者名稱。
- **具有管理員角色之使用者的密碼：** 指定您已在上述欄位中所指定之使用者名稱的密碼。

3 (條件式) 如果您的環境使用多因素或增強式驗證，您必須提供 Sentinel 用戶端 ID 和 Sentinel 用戶端密碼。如需有關驗證方法的詳細資訊，請參閱*《Sentinel 管理員指南》*中的「「驗證方法」」。

若要取回 Sentinel 用戶端 ID 和 Sentinel 用戶端密碼，請前往以下 URL：

https://*主機名稱*.*連接埠*/SentinelAuthServices/oauth/clients

其中：

- *主機名稱*是 Sentinel 伺服器的主機名稱。
- *連接埠*是 Sentinel 使用的連接埠 (通常是 8443)。

指定 URL 使用您目前的 Sentinel 工作階段取回 Sentinel 用戶端 ID 和 Sentinel 用戶端密碼。

4 按一下「下一步」。

5 出現提示時，接受證書。

6 將主控台中顯示的裝置 IP 位址記下來。

視您選擇安裝的項目而定，主控台會顯示訊息指出此裝置是 Sentinel Collector Manager 或 Correlation Engine，並附上 IP 位址。主控台也會顯示 Sentinel 伺服器使用者介面 IP 位址。

7 完成「「安裝 Sentinel」(第 95 頁)」中的步驟 16到步驟 17。

安裝 Sentinel OVF 裝置

本節提供安裝 Sentinel、Collector Manager 和 Correlation Engine 做為 OVF 裝置影像的相關資訊。

OVF 格式是標準虛擬機器格式，由監管程式直接或透過簡單轉換支援。Sentinel 以兩個認證的監管程式支援 OVF 裝置，但您也可使用其他監管程式。

- 「安裝 Sentinel」(第 97 頁)
- 「安裝 Collector Manager 和 Correlation Engine」(第 98 頁)

安裝 Sentinel

安裝 Sentinel OVF 裝置：

1 至 下載網站下載 OVF 虛擬裝置影像。

2 在您的監管程式管理主控台中以新的虛擬機器輸入OVF影像檔。若出現提示，請允許監管程式將 OVF 影像轉換為原生格式。

3 檢視已配置給您新的虛擬機器的虛擬硬體資源，確保其符合 Sentinel 必要條件。

4 開啟虛擬機器。

5 選取您所選擇的語言。

6 選取鍵盤配置。

7 按下一步。

8 閱讀並接受「 SUSE Enterprise Server Software 授權合約」。按「下一步」。

9 閱讀並接受 Sentinel 伺服器裝置授權合約。按「下一步」。

10 設定 Sentinel·應用裝置密碼、NTP 組態和時區。

設定 vaadmin 使用者身分證明，以登入·Sentinel 應用裝置管理主控台。

附註： 安裝後，您可以透過以下方式變更 NTP 組態和時區：

- 移至指令提示字元視窗，並輸入 yast->網路服務->NTP 組態
- 移至 Sentienl 應用裝置管理主控台，按一下「**時間**」

如果安裝之後，沒有立即同步顯示時間，請執行下列指令來重新啟動 NTP：

```
rcntp restart
```

---

11 在 Sentinel 伺服器裝置的「網路設定」頁面上，指定主機名稱和網域名稱。選取「**靜態 IP 位址**」或「**DHCP IP 位址**」。

12 按下一步。

13 (條件式) 如果您在步驟 11 選取了「**靜態 IP 位址**」，請指定網路連線設定。

14 按下一步。

15 設定 Sentinel 管理員密碼，然後按一下「下一步」。

由於系統會執行一次性的啟始化，因此在安裝完成後所有服務都需要幾分鐘的時間才能啟動。請等待安裝完成後再登入伺服器。

16 將主控台中顯示的裝置 IP 位址記下來。以相同的 IP 位址存取 Sentinel 主要介面。

安裝 Collector Manager 和 Correlation Engine

在 VMware ESX 伺服器上安裝 Collector Manager 或 Correlation Engine 做為 OVF 裝置影像：

1 完成在 「安裝 Sentinel」(第 97 頁) 中的步驟 1 至步驟 14。

安裝作業會檢查可用的記憶體和磁碟空間。如果可用的記憶體少於 1 GB，安裝作業便不會讓您繼續進行安裝，因此「下一步」按鈕會變成灰色的。

2 指定 Collector Manager 應連接之 Sentinel 伺服器的主機名稱/IP 位址。

3 指定通訊伺服器連接埠號碼。預設的埠是 61616。

4 指定管理員角色中任何使用者的身分證明。輸入使用者名稱與密碼。

5 (條件式) 如果您的環境使用多因素或增強式驗證，您必須提供 Sentinel 用戶端 ID 和 Sentinel 用戶端密碼。如需有關驗證方法的詳細資訊，請參閱*《Sentinel 管理員指南》*中的「「驗證方法」」。

若要取回 Sentinel 用戶端 ID 和 Sentinel 用戶端密碼，請前往以下 URL：

https://*主機名稱.連接埠*/SentinelAuthServices/oauth/clients

其中：

- *主機名稱*是 Sentinel 伺服器的主機名稱。
- *連接埠*是 Sentinel 使用的連接埠 (通常是 8443)。

指定 URL 使用您目前的 Sentinel 工作階段取回 Sentinel 用戶端 ID 和 Sentinel 用戶端密碼。

6 按**下一步**。

7 接受證書。

8 按「**下一步**」以完成安裝。

安裝完成時，視您選擇安裝的項目而定，安裝程式會顯示訊息指出此裝置是 Sentinel Collector Manager 或 Sentinel Correlation Engine，並附上 IP 位址。這則訊息也會顯示 Sentinel 伺服器使用者介面 IP 位址。

安裝裝置後的組態

安裝 Sentinel 之後，您需要執行其他裝置組態，才能正常運作。

- 「登錄以進行更新」(第 99 頁)
- 「建立傳統儲存的分割區」(第 100 頁)
- 「設定可擴充儲存」(第 101 頁)
- 「使用 SMT 設定裝置」(第 101 頁)

登錄以進行更新

您必須使用應用裝置更新通道來註冊 Sentinel 應用裝置，以接收 Sentinel 和作業系統的最新更新。若要註冊此裝置，您必須先向 客戶服務中心取得裝置登錄碼或裝置啟用碼。

使用 Sentinel 應用裝置管理主控台註冊

如果您使用 SLES 12 SP3，則可以使用 Sentinel 應用裝置管理主控台來註冊更新。

1 透過下列其中一種方式來啟動 Sentinel 應用裝置：

- 登入 Sentinel，按一下**Sentinel Main** > **應用裝置**。
- 在您的網頁瀏覽器中指定下列 URL：https://<IP_address>:9443.

2 以 vaadmin 或 根使用者身分登入。

3 按一下**線上更新** > **立即註冊**。

4 在**電子郵件**欄位中，指定要接收更新的電子郵件 ID。

5 在**啟用碼**欄位中，輸入註冊碼。

6 按一下**註冊** 以完成註冊程序。

使用指令進行註冊

如果您使用 SLES 11 SP4 或 SLES 12 SP3，您可以使用指令進行註冊。

若要註冊以進行更新

1. 以根使用者身分登入 Sentinel 伺服器。
2. 指定下列指令：
   - 若要註冊伺服器，請指定：suse_register -a regcode-sentinel="<*registration_code*>" -a email="<*email_ID*>"
   - 若要註冊 Collector Manager，請指定：suse_register -a regcode-sentinel-collector="<*registration_code*>" -a email="<*email_ID*>"
   - 若要註冊 Correlation Engine，請指定：suse_register -a regcode-sentinel-correlation ="<*registration_code*>" -a email="<*email_ID*>"
   - 若要註冊高可用性的 Sentinel，請指定：suse_register -a regcode-sentinel-ha ="<*registration_code*>" -a email="<*email_ID*>"

   針對電子郵件參數，請指定您想接收更新的電子郵件 ID。

建立傳統儲存的分割區

本節中的資訊僅適用於您想要使用傳統儲整做為資料儲存選擇的情況。

最佳實務為確定您建立不同的分割區，以在不同的分割區上儲存除了可執行檔、組態和作業系統檔案檔案之外的 Sentinel 資料。分開儲存變數資料的優點包括易於備份檔案組合，也更容易復原損壞，並可在磁碟分割區滿載時提供額外加強。如需關於規劃分割區的詳細資訊，請參閱「傳統儲存規劃」(第 40 頁)。您可以在裝置中新增分割區，並使用 YaST 工具將目錄移至新的分割區中。

使用以下程序來建立新的分割區，並將資料檔案從目錄移至新建立的分割區：

1. 以 root 身分登入 Sentinel。
2. 執行以下指令以停止裝置上的 Sentinel：

   /etc/init.d/sentinel stop
3. 指定下列指令，以變更為 novell 使用者：

   su -novell
4. 將 /var/opt/novell/sentinel 目錄中的內容移至暫時位置。
5. 變更為 root 使用者。
6. 輸入以下指令以存取 YaST2 Control Center：

   ```
   yast
   ```
7. 選取「**系統**」>「**分割器**」。
8. 閱讀警告並選取「**是**」以新增未使用的分割區。

   如需關於建立分割區的詳細資訊，請參閱《*SLES 11 文件*》中的「使用 YaST 分割器」。
9. 將新分割區掛接於 /var/opt/novell/sentinel/。
10. 指定下列指令，以變更為 novell 使用者：

    su -novell
11. 將暫時位置中的資料目錄內容 (儲存於步驟 4) 移回新分割區中的 /var/opt/novell/sentinel/。
12. 執行以下指令以重新啟動 Sentinel 裝置：

    /etc/init.d/sentinel start

設定可擴充儲存

若要啟用和設定可擴充儲存做為資料儲存選擇，請參閱「《 Sentinel 管理指南》」中的*「設定可擴充儲存」*。

使用 SMT 設定裝置

若您所處的安全環境必須在無直接網際網路存取的狀態下執行裝置，您可以使用 Subscription Management Tool (SMT) 來設定裝置，並得以在 Sentinel 的最新版本發行時將裝置升級至最新版本。SMT 為一種整合 Customer Center 的套件代理系統，提供重要的 Customer Center 功能。

先決條件

透過 SMT 設定裝置前，請確定您符合下列先決條件：

- 取得 Customer Center 身分證明以取得 Sentinel 更新。如需關於取得身分證明的詳細資訊，請聯絡技術支援。
- 請確定已在要安裝 SMT 的電腦上，將 SLES 11 SP3 與下列套件一併安裝：
  - htmldoc
  - perl-DBIx-Transaction
  - perl-File-Basename-Object
  - perl-DBIx-Migration-Director
  - perl-MIME-Lite
  - perl-Text-ASCIITable
  - yum-metadata-parser
  - createrepo
  - perl-DBI
  - apache2-prefork
  - libapr1
  - perl-Data-ShowTable
  - perl-Net-Daemon
  - perl-Tie-IxHash
  - fltk
  - libapr-util1
  - perl-PIRPC
  - apache2-mod_perl
  - apache2-utils
  - apache2
  - perl-DBD-mysql

- 安裝 SMT 並設定 SMT 伺服器。如需詳細資訊，請參閱 SMT 文件中的下列章節：
  - SMT 安裝
  - SMT 伺服器組態
  - 使用 SMT 執行鏡像複製安裝並更新儲存機制
- 在裝置電腦上安裝 wget 公用程式。

設定裝置

請執行下列步驟以透過 SMT 設定裝置：

1. 透過在 SMT 伺服器中執行下列指令，啟用裝置儲存機制：

   smt-repos -e Sentinel-Server-7.0-Updates sle-11-x86_64

   smt-repos -e Sentinel-Collector-Manager-7.0-Updates sle-11-x86_64

   smt-repos -e Sentinel-Correlation-Engine-7.0-Updates sle-11-x86_64
2. 透過執行「SMT 文件」中「將用戶端設定為使用 SMT」一節中的步驟，透過 SMT 設定裝置。

升級裝置

如需有關升級裝置的詳細資訊，請參閱「升級 Sentinel」(第 147 頁)。

16 安裝額外的收集器和連接器

依預設，當您安裝 Sentinel 時，會一併安裝所有發行的收集器和連接器。若要安裝在 Sentinel 發行之後發行的新收集器和連接器，請使用以下各節中的資訊。

- 「安裝收集器」(第 103 頁)
- 「安裝連接器」(第 103 頁)

安裝收集器

安裝收集器的步驟如下：

1. 從 NetIQ 下載網站下載所需的收集器。
2. 從 **Sentinel 主畫面**，按一下**管理員**下拉式清單，接著再按一下**應用程式**。
3. 按一下「**啟動 Control Center**」以啟動 Sentinel Control Center。
4. 在工具列中按一下「**事件來源管理**」>「**即時檢視**」，接著按一下「**工具**」>「**輸入外掛程式**」。
5. 瀏覽並選取在步驟 1中下載的收集器檔案，接著按「**下一步**」。
6. 遵循剩餘的提示，接著按一下「**完成**」。

如要設定收集器，請在 Sentinel 外掛程式網站上參閱指定收集器的文件。

安裝連接器

安裝連接器的步驟如下：

1. 從 Sentinel 外掛程式網站下載所需的連接器。
2. 從 **Sentinel 主畫面**，按一下**管理員**下拉式清單，接著再按一下**應用程式**。
3. 按一下「**啟動 Control Center**」以啟動 Sentinel Control Center。
4. 在工具列中選取「**事件來源管理**」>「**即時檢視**」，接著按一下「**工具**」>「**輸入外掛程式**」。
5. 瀏覽並選取在步驟 1中下載的連接器檔案，接著按「**下一步**」。
6. 遵循剩餘的提示，接著按一下「**完成**」。

如要設定連接器，請在 Sentinel 外掛程式網站上參閱指定連接器的文件。

17 驗證安裝

您可執行以下其中一項來判斷安裝是否成功：

- 驗證 Sentinel 版本：

  ```
  /etc/init.d/sentinel version
  ```

- 確認 Sentinel 服務已啟動且在執行中，並在 FIPS 或非 FIPS 模式中運作：

  ```
  /etc/init.d/sentinel status
  ```

- 驗證 Web 服務是否正常運作：

  ```
  netstat -an |grep 'LISTEN' |grep <HTTPS_port_number>
  ```

  預設連接埠號碼為 8443。

- 啟動 Sentinel：

  1. 啟動支援的網頁瀏覽器。
  2. 指定 Sentinel 的 URL：

     ```
     https://IP_AddressOrDNS_Sentinel_server:8443
     ```

     其中 *IP_AddressOrDNS_Sentinel_server* 是 Sentinel 伺服器的 IP 位址或 DNS 名稱，*8443* 是 Sentinel 伺服器的預設連接埠。
  3. 在安裝期間使用管理員名稱和密碼登入。預設使用者名稱為 admin。

IV 設定 Sentinel 的組態

本節提供設定 Sentinel 的組態和立即可用外掛程式的相關資訊。

18 設定時間

事件時間在 Sentinel 的處理程序中是非常關鍵的一環。對於報告、稽核和即時處理來說，它也是不可或缺的要素。本節提供瞭解 Sentinel 中的時間、如何設定時間以及處理時區的相關資訊。

瞭解 Sentinel 中的時間

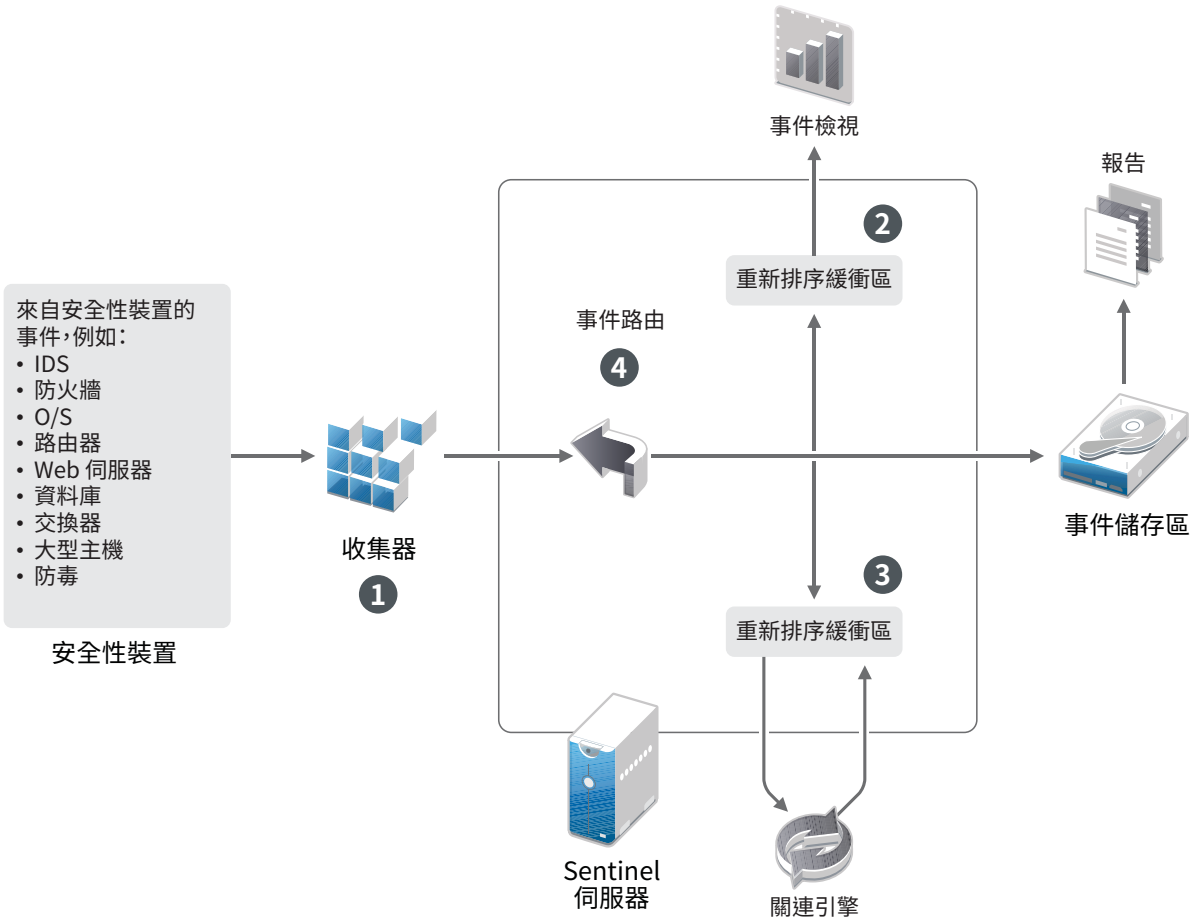
Sentinel 為分散式系統，由分散至整個網路的多個程序組成。此外，系統中還會有一些由事件來源造成的延遲。為了調和延遲的狀況，Sentinel 程序在處理事件之前，會將事件重新排列為以時間先後順序排列的資料流。

每個事件有三個時間欄位：

- **事件時間:** 這是所有分析引擎、搜尋、報告等所使用的事件時間。
- **Sentinel 程序時間：** Sentinel 收集裝置資料的時間，記錄自 Collector Manager 系統時間。
- **觀察者事件時間：** 裝置放入資料的時戳。資料不一定都會包含可靠的時戳，而且可能相當不同於 Sentinel 程序時間。例如，當裝置依批次傳送資料時。

下圖說明 Sentinel 如何在傳統儲存設定中完成此作業：

圖 18-1 Sentinel 時間



1. 依預設，系統會將事件時間設定為 Sentinel 程序時間。不過，理想的方式是將事件時間設為觀察者事件時間 (如有，而且可靠)。若可取得正確的裝置時間，而且已經過收集器正確剖析，最好是將資料收集設成「信任事件來源時間」。收集器可將事件時間設為觀察者事件時間。
2. 通常是由事件檢視來處理事件時間與伺服器時間差距 (包含過去和未來) 在 5 分鐘內的事件。事件時間超過未來 5 分鐘的事件不會顯示在事件檢視中，但系統會將事件插入事件儲存中。時間戳記快 5 分鐘以上以及小於 24 小時的事件仍會出現在圖表中，但不會出現在該圖表的事件資料中。您必須進行下探式操作以從事件儲存擷取這些事件。
3. 事件會以 30 秒間隔排序，讓 Correlation Engine 可依時間順序來處理。如果事件時間比伺服器快 30 秒，Correlation Engine 便不會處理事件。
4. 如事件時間比起 Collector Manager 的系統時間快上 5 秒，Sentinel 會直接將事件導向至事件儲存區，並繞過即時處理系統如 Correlation Engine 和安全情報。

在 Sentinel 中設定時間

Correlation Engine 會處理以時間先後順序排列的事件資料流，同時也會偵測事件中的模式和資料流中的暫時模式。不過，有時候產生事件的設備不會在其記錄訊息中包含時間。

若要設定與 Sentinel 一致的時間，您有兩個選擇：

- 在 Collector Manager 上設定 NTP，並取消選取事件來源管理員之事件來源中的「**信任事件來源時間**」。Sentinel 會將 Collector Manager 當做事件的時間來源。
- 選取事件來源管理員之事件來源中的「**信任事件來源時間**」。Sentinel 會將記錄訊息的時間當做正確的時間。

若要在事件來源上變更此項設定：

1. 登入事件來源管理。

   如需詳細資訊，請參閱《「 Sentinel 管理指南」》中的「*存取事件來源管理*」。
2. 以滑鼠右鍵按一下要變更時間設定的事件來源，接著選取「**編輯**」。
3. 選取或取消選取「**一般**」索引標籤底部的「**信任事件來源時間**」選項。
4. 按一下「**確定**」儲存變更。

設定事件的延遲時間限制

當 Sentinel 接收來自事件來源的事件時，產生事件和 Sentinel 處理事件的時間之間可能包含延遲。Sentinel 在不同的分割區中儲存事件時會有大量延遲。若有許多事件長期延遲，可能表示事件來源未正確設定。這也可能造成系統在嘗試處理延遲的事件時降低 Sentinel 效能。由於延遲的事件可能是由於設定錯誤所造成，建議不要儲存起來，Sentinel 可讓您設定所收到事件可接受的延遲限制。事件路由會捨棄超過延遲限制的事件。在 configuration.properties 檔案中指定在下列內容中的延遲限制：

```
esecurity.router.event.delayacceptthreshold = <time in milliseconds>
```

您也可使用定期登入 Sentinel 伺服器記錄檔案的清單，當中會顯示事件接收延遲超過指定限定值的事件來源。若要記錄此資訊，請在 configuration.properties 檔案的下列內容中指定限定值：

```
sentinel.indexedlog.eventdelay.reportthreshold= <time in milliseconds>
```

處理時區

在分散式環境中處理時區是相當複雜的工作。例如，您的事件來源可能位在某個時區中，Collector Manager 位在另一個時區中，後端的 Sentinel 伺服器又位在另一個時區中，而檢視資料的用戶端則位在其他時區中。當您加入如日光節約時間等考量及許多不報告所在時區的事件來源 (如所有 Syslog 來源) 時，便需要處理許多可能的問題。Sentinel 的彈性能讓您在事件發生時適當地呈現時間，也能讓您將事件與來自其他位在相同或相異時區之來源的事件做比較。

一般來說，事件來源報告時間戳記的方式可分為三種情境：

- 事件來源報告 UTC 時間。例如，所有標準的 Windows 事件記錄檔事件一律報告 UTC 時間。
- 事件來源報告本地時間，但一律會在時間戳記中加上時區。例如，任何遵循使時間戳記結構化之 RFC3339 的事件來源均會加入時區以做為偏移；其他來源則會報告詳細的時區 ID (如 Americas/New York) 或簡短的時區 ID (如 EST)，由於衝突和解析不當等因素，這可能會造成問題。
- 事件來源報告本地時間，但未加入時區。很遺憾，最普遍的 Syslog 格式遵循此模式。

對於第一種情境，您一律可以計算事件發生時的絕對 UTC 時間 (假設時間同步化通訊協定正在使用中)，因此可以輕易地將事件時間與世界中的其他事件來源做比較。不過您不能自動判斷事件發生時的本地時間。有鑑於此，Sentinel 允許客戶在事件來源管理員中編輯事件來源節點，以利用手動的方式設定事件來源的時區，以及指定適當的時區。這項資訊不會影響「設備事件時間」或「事件時間」的計算，但系統會將其放置在「觀察者時區」欄位中，並且用來計算各個「觀察者時區」欄位 (如「觀察者時區小時」)。這些欄位一律以本地時間來表示。

對於第二種情境，如果系統使用詳細時區ID或偏移，您除了可以轉換為UTC以取得絕對規範化UTC時間 (儲存在「設備事件時間」中) 之外，還能計算本地時間「觀察者時區」欄位。但如果使用簡短時區 ID，可能會造成某些衝突。

第三種情境需要所有受影響來源的管理員手動設定事件來源時區，Sentinel 才能正確計算 UTC 時間。如果您未藉由編輯事件來源管理員的事件來源節點來指定正確的時區，「設備事件時間」(或甚至「事件時間」) 可能會是錯誤的。此外，「觀察者時區」和相關的欄位也可能會是錯誤的。

一般來說，指定類型之事件來源 (如 Microsoft Windows) 的收集器都知道事件來源呈現時間戳記的方式，因此都能隨著調整。除非您知道事件來源報告是以本地時間為準且一律在時間戳記中加上時區，否則在事件來源管理員中針對所有事件來源節點手動設定時區會是放諸四海皆準的規則。

收集器和 Collector Manager 是負責處理時間戳記之事件來源呈現的裝置。「設備事件時間」和「事件時間」是以 UTC 的格式儲存，而事件來源的「觀察者時區」欄位則是以設定為本地時間的字串格式儲存。這項資訊會從 Collector Manager 傳送至 Sentinel 伺服器，且儲存在事件儲存中。Collector Manager 和 Sentinel 伺服器所在的時區不會影響這個程序或儲存的資料。不過，當用戶端在網頁瀏覽器中檢視事件時，由於系統會依據網頁瀏覽器將 UTC 事件時間轉換為本地時間，因此在將所有事件呈現給用戶端時是以本地時區為準。如果使用者想要查看來源的本地時間，他們能查驗「觀察者時區」欄位以取得詳細資料。

19 保護 Elasticsearch 中的資料

Sentinel 可利用瀏覽器式分析和搜尋儀表板 Kibana，協助您視覺化儀表板中的事件和警示。Sentinel 可在 Elasticsearch 中儲存警示並編製其索引。您也可以將 Sentinel 設定為在 Elasticsearch 中儲存事件並編製其索引，以運用事件視覺化功能。Sentinel 儀表板會從 Elasticsearch 存取資料，以將事件和警示顯示在儀表板中。若要確保儀表板只會顯示使用者角色有權檢視的資料，並防止 Elasticsearch 中出現未經授權的資料存取，您必須安裝 Elasticsearch 安全性外掛程式。如需詳細資訊，請參閱「保護 Elasticsearch 中的資料」(第 75 頁)。

20 啟用事件視覺化

在可擴充儲存設定中，依預設會提供事件視覺化功能。在傳統儲存設定中，只有在已啟用視覺化資料儲存庫 (Elasticsearch) 來儲存資料及編製其索引時，才可使用事件視覺化。

必備條件

若要在生產環境中進行事件的可擴充和分散式索引編製，您必須在叢集模式下設定更多 Elasticsearch 節點。若要在叢集模式下安裝和設定 Elasticsearch，請參閱「安裝和設定 Elasticsearch」(第 73 頁)。

啟用事件視覺化

若要啟用事件視覺化：

1. 以 Novell 使用者身分登入 Sentinel 伺服器。
2. 開啟 /etc/opt/novell/sentinel/config/configuration.properties 檔案。
3. 將 eventvisualization.traditionalstorage.enabled 設定為 true。
4. 在數分鐘後重新整理使用者介面，以檢視事件視覺化。

   您現在應可看到所有在「**我的 Sentinel**」使用者介面中啟用的儀表板。請啟動任何儀表板 (例如「威脅搜尋」儀表板)，然後按一下「**搜尋**」。儀表板會顯示在過去 1 小時內產生的所有事件。
5. (選用) 事件視覺化儀表板只會顯示在您啟用事件視覺化後處理的事件。若要檢視檔案式儲存中顯示的現有事件，您必須將資料從檔案式儲存移轉至 Elasticsearch。如需詳細資訊，請參閱第 33 章 「將資料移轉至 Elasticsearch」(第 167 頁)。

附註： 啟用或停用事件視覺化會產生例外狀況，因為這時會重新啟動 Sentinel 索引服務。這是預期中的例外狀況，您可加以忽略。

---

21 在安裝後修改組態

在安裝 Sentinel 之後，如果您想要輸入有效的授權金鑰、變更密碼或修改任何已指定的連接埠，可以執行 configure.sh 程序檔來加以修改。該程序檔可在 /opt/novell/sentinel/setup 資料夾中取得。

1. 使用下列指令將 Sentinel 關機：

   rcsentinel 停止

2. 在指令行中指定下列指令以執行 configure.sh 程序檔：

   ```
   ./configure.sh
   ```

3. 指定 1 可執行 Sentinel 標準組態；指定 2 可執行 Sentinel 自定組態。
4. 按下空格鍵，以完整讀取授權合約。
5. 輸入 yes 或 y，接受授權合約，並且繼續安裝作業。

   安裝作業會利用幾秒鐘的時間來載入安裝套件。
6. 輸入 1 以使用預設的試用版授權金鑰

   或

   輸入 2 以輸入購買的 Sentinel 授權金鑰。
7. 決定是否要保留 admin 管理員使用者現有的密碼。
   - 如果您想要保留現有的密碼，請輸入 1 並繼續進行步驟 8。
   - 如果您想要變更現有的密碼，請輸入 2 並指定新密碼、確認密碼，接著再繼續進行步驟 8。

     admin 使用者是用於透過 Sentinel 主要介面執行管理任務的身分，包括建立其他使用者帳戶在內。
8. 決定是否要保留 dbauser 資料庫使用者現有的密碼。
   - 如果您想要保留現有的密碼，請輸入 1 並繼續進行步驟 9。
   - 如果您想要變更現有的密碼，請輸入 2 並指定新密碼、確認密碼，接著再繼續進行步驟 9。

   dbauser 帳戶是 Sentinel 用來與資料庫互動的身分。您在此處輸入的密碼可用來執行資料庫維護工作，包括在忘記或遺失管理員密碼時重設管理員密碼。
9. 決定是否要保留 appuser 應用程式使用者現有的密碼。
   - 如果您想要保留現有的密碼，請輸入 1 並繼續進行步驟 10。
   - 如果您想要變更現有的密碼，請輸入 2 並指定新密碼、確認密碼，接著再繼續進行步驟 10。

     appuser 帳戶是 Sentinel java 程序用來建立連接並與資料庫互動的內部身分。您在此輸入的密碼可用來執行資料庫工作。
10. 藉由輸入需要的號碼再指定新的連接埠號碼，變更 Sentinel 服務的連接埠指定。
11. 變更連接埠後，請指定 7 來完成作業。
12. 輸入 1 ，僅以內部資料庫來驗證使用者。

    或

    如果您已在網域中設定 LDAP 目錄，請輸入 2 以利用 LDAP 目錄驗證來驗證使用者。

    預設值為 1。

22 設定立即可用外掛程式

Sentinel 將會預先安裝，並包含 Sentinel 發行時可用的預設 Sentinel 外掛程式。

本節提供如何設定立即可用外掛程式的相關資訊。

檢視預先安裝的外掛程式

您可檢視預先安裝在 Sentinel 內的外掛程式清單。您也可以查看外掛程式版本和其他中繼資料，這可協助您判斷您是否擁有最新版本的外掛程式。

檢視您 Sentinel 伺服器中安裝的外掛程式：

1. 以管理員身分登入 Sentinel 主要介面，其位置為 https://<*IP 位址*>:8443 (8443 是 Sentinel 伺服器的預設連接埠)。
2. 按一下「**外掛程式**」>「**目錄**」。

設定資料集合

如需針對資料收集設定 Sentinel 的詳細資訊，請參閱「《 Sentinel 管理指南》」中的*收集和路由事件資料*。

設定解決方案套件

Sentinel 隨附各式各樣立即可用的內容，可以符合您的各種分析需求。此內容大部分來自預先安裝的 Sentinel 核心解決方案套件和 ISO 27000 系列的解決方案套件。如需詳細資訊，請參閱《「 Sentinel 使用者指南」》中的「*使用解決方案套件*」。

解決方案套件可將內容分類及分組成各種控制項或規則組，並且將其視為一個單位。解決方案套件會預先安裝各種控制項以提供您立即可用的內容，不過您必須使用 Sentinel 主要介面正式執行或測試這些控制項。

如果您需要精確數據以確認您的 Sentinel 執行依設計進行運作，您可以使用解決方案套件內建的正式證明程序。此證明程序可執行並測試解決方案套件控制項，就如同您從任何其他解決方案套件執行及測試控制項一樣。此程序中的執行者及測試者將證明工作已確實完成，接下來這些證明會成為稽核線索的一部分，用於檢測特殊控制項已正確進行部署。

您可以使用解決方案管理員來執行證明程序。如需執行及測試控制項的詳細資訊，請參閱《「 Sentinel 使用者指南」》中的「*安裝及管理解決方案套件*」。

設定動作與整合器

如需關於設定立即可用外掛程式的詳細資訊，請參閱可在 Sentinel 外掛程式網站上取得的指定外掛程式文件。

23 在現有 Sentinel 安裝中啟用 FIPS 140-2 模式

本章提供在現有 Sentinel 安裝中啟用 FIPS 140-2 模式的相關資訊。

附註： 這些指示假設 Sentinel 已安裝在 /opt/novell/sentinel 目錄。指令必須以 novell 使用者的身分執行。

啟用 Sentinel 伺服器在 FIPS 140-2 模式中執行

要啟用 Sentinel 伺服器在 FIPS 140-2 模式中執行：

1. 登入 Sentinel 伺服器。
2. 切換為 novell 使用者 (su novell)。
3. 瀏覽至 Sentinel bin 目錄。
4. 執行 convert_to_fips.sh 程序檔並遵循畫面上的指示。
5. (條件式) 如果您的環境使用多因素或增強式驗證，您必須執行 create_mfa_fips_keys.sh 程序檔，然後依照畫面上的指示。

   附註： 當執行程序檔時，需要 NSS 資料庫的密碼。

6. (條件式) 如果您的環境使用多因素或增強式驗證，您必須提供 Sentinel 用戶端 ID 和 Sentinel 用戶端密碼。如需有關驗證方法的詳細資訊，請參閱*《Sentinel 管理員指南》*中的「「驗證方法」」。

   若要取回 Sentinel 用戶端 ID 和 Sentinel 用戶端密碼，請前往以下 URL：

   https://*主機名稱*:*連接埠*/SentinelAuthServices/oauth/clients

   其中：

   - *主機名稱*是 Sentinel 伺服器的主機名稱。
   - *連接埠*是 Sentinel 使用的連接埠 (通常是 8443)。

   指定 URL 使用您目前的 Sentinel 工作階段取回 Sentinel 用戶端 ID 和 Sentinel 用戶端密碼。
7. 重新啟動 Sentinel 伺服器。
8. 按照在「第 24 章 「以 FIPS 140-2 模式操作 Sentinel」(第 123 頁)」中提到的任務，完成 FIPS 140-2 模式組態。

啟用遠端 Collector Manager 和 Correlation Engine 上的 FIPS 140-2 模式

若您想要使用經過 FIPS 核准的通訊，搭配在 FIPS 140-2 模式中執行的 Sentinel 伺服器，您必須啟用遠端 Collector Manager 和 Correlation Engine 上的 FIPS 140-2 模式。

要啟用遠端 Collector Manager 或 Correlation Engine，以在 FIPS 140-2 模式中執行：

1. 登入遠端 Collector Manager 或 Correlation Engine 系統。
2. 切換為 novell 使用者 (su novell)。
3. 瀏覽至 bin 目錄。預設值位置是 /opt/novell/sentinel/bin。
4. 執行 convert_to_fips.sh 程序檔並遵循畫面上的指示。
5. 重新啟動 Collector Manager 或 Correlation Engine。
6. 按照在「第 24 章 「以 FIPS 140-2 模式操作 Sentinel」(第 123 頁)」中提到的任務，完成 FIPS 140-2 模式組態。

24 以 FIPS 140-2 模式操作 Sentinel

本章節提供在 FIPS 140-2 模式中設定及操作 Sentinel 的相關資訊。

在 FIPS 140-2 模式中設定 Advisor 服務

Advisor 使用安全的 HTTPS 連接，以從 Advisor 伺服器下載其饋送。伺服器用來進行安全通訊的證書需要加進 Sentinel FIPS KeyStore 資料庫。

要驗證成功登錄資源管理資料庫：

1. 從 Advisor 伺服器下載證書，然後將檔案另存為 advisor.cer。
2. 輸入 Advisor 伺服器證書到 Sentinel FIPS KeyStore。

   如需關於輸入證書的詳細資訊，請參閱 「輸入證書到 FIPS Keystore 資料庫」(第 131 頁)。

在 FIPS 140-2 模式中設定分散式搜尋

本節提供有關在 FIPS 140-2 模式中設定分散式搜尋的資訊。

情境 1：來源和目標 Sentinel 伺服器都在 FIPS 140-2 模式中

要允許在 FIPS 140-2 模式中執行跨多個 Sentinel 伺服器的分散式搜尋，您需要將用於安全通訊的證書新增至 FIPS KeyStore。

1. 登入分散式搜尋來源電腦。
2. 瀏覽到證書目錄：

   cd <*sentinel_install_directory*>/config
3. 複製來源證書 (sentinel.cer) 到目標電腦上的暫存位置。
4. 輸入來源證書到目標 Sentinel FIPS KeyStore。

   如需關於輸入證書的詳細資訊，請參閱 「輸入證書到 FIPS Keystore 資料庫」(第 131 頁)。
5. 登入分散式搜尋目標電腦。
6. 瀏覽到證書目錄：

```
cd /etc/opt/novell/sentinel/config
```

7 複製目標證書 (sentinel.cer) 到來源電腦上的暫存位置。

8 輸入目標系統證書到來源 Sentinel FIPS KeyStore。

9 重新啟動來源和目標電腦上的 Sentinel 服務。

情境 2：來源 Sentinel 伺服器在非 FIPS 模式中，目標 Sentinel 伺服器是在 FIPS 140-2 模式中

您必須將來源電腦上的 Web 伺服器 KeyStore 轉換成證書格式，然後將證書輸出到目標電腦。

1 登入分散式搜尋來源電腦。

2 以證書 (.cer) 格式建立 Web 伺服器 KeyStore：

```
<sentinel_install_directory>/jdk/jre/bin/keytool -export -alias webserver -keystore
<sentinel_install_directory>/config/.webserverkeystore.jks -storepass password -file
<certificate_name.cer>
```

3 複製分散式搜尋來源證書 (Sentinel.cer) 到分散式搜尋目標電腦上的暫存位置。

4 登入分散式搜尋目標電腦。

5 輸入來源證書到目標 Sentinel FIPS KeyStore。

如需關於輸入證書的詳細資訊，請參閱「輸入證書到 FIPS Keystore 資料庫」(第 131 頁)。

6 重新啟動目標電腦上的 Sentinel 服務。

情境 3：來源 Sentinel 伺服器在 FIPS 模式中，目標 Sentinel 伺服器是在非 FIPS 模式中

1 登入分散式搜尋目標電腦。

2 以證書 (.cer) 格式建立 Web 伺服器 KeyStore：

```
<sentinel_install_directory>/jdk/jre/bin/keytool -export -alias webserver -keystore
<sentinel_install_directory>/config/.webserverkeystore.jks -storepass password -file
<certificate_name.cer>
```

3 將證書複製到分散式搜尋來源電腦上的暫存位置。

4 輸入目標證書到來源 Sentinel FIPS KeyStore。

如需關於輸入證書的詳細資訊，請參閱「輸入證書到 FIPS Keystore 資料庫」(第 131 頁)。

5 重新啟動來源電腦上的 Sentinel 服務。

在 FIPS 140-2 模式中設定 LDAP 驗證

要為在 FIPS 140-2 模式中執行的 Sentinel 伺服器設定 LDAP 驗證：

1 從 LDAP 管理員取得 LDAP 伺服器證書，或者您可以使用指令。例如，

```
openssl s_client -connect <LDAP server IP>:636
```

然後將傳回的文字 (介於 (但不含) BEGIN 和 END 行之間) 複製到檔案。

2 輸入 LDAP 伺服器證書到 Sentinel FIPS KeyStore。

如需關於輸入證書的詳細資訊，請參閱「輸入證書到 FIPS Keystore 資料庫」(第 131 頁)。

3 以管理員角色中的使用者身分導覽至 **Sentinel 主要介面**，然後繼續設定 LDAP 驗證。

如需詳細資訊，請參閱 *Sentinel 管理指南*中的「對單一 LDAP 伺服器或網域進行 LDAP 驗證」。

附註： 您也可以執行在 /opt/novell/sentinel/setup 目錄中的 ldap_auth_config.sh 程序檔，為在 FIPS 140-2 模式中執行的 Sentinel 伺服器設定 LDAP 驗證。

更新在遠端 Collector Manager 和 Correlation Engine 上的伺服器證書

要設定現有遠端 Collector Manager 和遠端 Correlation Engine，以與在 FIPS 140-2 模式中執行的 Sentinel 伺服器通訊，您可以在 FIPS 140-2 模式中轉換遠端系統，或是將 Sentinel 伺服器證書更新到遠端系統，將 Collector Manager 和 Correlation Engine 留在非 FIPS 模式。如果事件來源不支援 FIPS 或必須使用其中一個尚未啟用 FIPS 的 Sentinel 連接器，則 FIPS 模式中的遠端 Collector Manager 可能無法與這樣的事件來源搭配運作。

若您不想啟用遠端 Collector Manager 或 Correlation Engine 上的 FIPS 140-2 模式，您必須複製最新的 Sentinel 伺服器證書到遠端系統，讓 Collector Manager 或 Correlation Engine 可以與 Sentinel 伺服器通訊。

要更新遠端 Collector Manager 或 Correlation Engine 上的 Sentinel 伺服器證書：

1. 登入遠端 Collector Manager 或 Correlation Engine 電腦。
2. 切換為 novell 使用者 (su novell)。
3. 瀏覽至 bin 目錄。預設值位置是 /opt/novell/sentinel/bin。
4. 執行 updateServerCert.sh 程序檔並遵循畫面上的指示。

設定 Sentinel 外掛程式在 FIPS 140-2 模式中執行

本節提供設定各種 Sentinel 外掛程式在 FIPS 140-2 模式中執行的相關資訊。

附註： 這些指示是以您已將 Sentinel 安裝於 /opt/novell/sentinel 目錄的假設為基礎提供。請以 novell 使用者身分執行所有指令。

- 「代理程式管理員連接器」(第 126 頁)
- 「資料庫 (JDBC) 連接器」(第 126 頁)
- 「Sentinel Link 連接器」(第 127 頁)
- 「Syslog 連接器」(第 127 頁)
- 「Windows 事件 (WMI) 連接器」(第 128 頁)
- 「Sentinel Link 整合器」(第 129 頁)
- 「LDAP Integrator」(第 129 頁)
- 「SMTP Integrator」(第 130 頁)
- 「Syslog Integrator」(第 130 頁)
- 「在 FIPS 140-2 模式中使用非 FIPS 啟用的連接器搭配 Sentinel」(第 131 頁)

代理程式管理員連接器

只有在設定代理程式管理員事件來源伺服器的網路設定時選取了「**已加密 (HTTPS)**」選項，才需要遵循以下程序。

要設定代理程式管理員連接器在 FIPS 140-2 模式中執行：

1. 新增或編輯代理程式管理員事件來源伺服器。繼續完成組態畫面，直到顯示「安全性」視窗為止。如需詳細資訊，請參閱《*代理程式管理員連接器指南*》。
2. 選取「*用戶端驗證類型*」欄位其中一個選項。用戶端驗證類型會判斷 SSL 代理程式管理員事件來源伺服器的嚴格程度，用以驗證嘗試傳送資料的代理程式管理員事件來源的身分。
   - **開啟：** 允許來自代理程式管理員代理程式的所有SSL連接。無法執行任何用戶端證書驗證。
   - **嚴格：** 驗證證書為有效的 X.509 證書，並檢查用戶端證書受到事件來源伺服器信任。新來源必須特定新增到 Sentinel (這可避免不受約束的來源傳送未授權資料)。

     針對「**嚴格**」選項，您必須將每個新代理程式管理員用戶端的證書輸入 Sentinel FIPS KeyStore。當 Sentinel 在 FIPS 140-2 模式中執行時，您無法使用事件來源管理 (ESM) 介面輸入用戶端證書。

     如需關於輸入證書的詳細資訊，請參閱 「輸入證書到 FIPS Keystore 資料庫」(第 131 頁)。

附註： 在 FIPS 140-2 模式中，代理程式管理員事件來源伺服器使用 Sentinel 伺服器金鑰組；不需要輸入伺服器金鑰組。

---

3. 若代理程式已啟用伺服器驗證，代理程式必須另外設定信任 Sentinel 伺服器或遠端 Collector Manager，視連接器部署位置而定。

   Sentinel 伺服器證書位置： /etc/opt/novell/sentinel/config/sentinel.cer

   遠端 Collector Manager 證書位置： /etc/opt/novell/sentinel/config/rcm.cer

---

附註： 使用由證書管理中心 (CA) 數位簽名的自訂證書時，代理程式管理員代理程式必須信任相關的證書檔案。

資料庫 (JDBC) 連接器

設定資料庫連接時，只有在您已選取 *SSL* 選項時才需要遵循以下程序。

要設定資料庫連接器在 FIPS 140-2 模式中執行：

1. 設定連接器之前，請從資料庫伺服器下載證書，然後另存為 database.cert 檔案到 Sentinel 伺服器的 /etc/opt/novell/sentinel/config 目錄。

   如需詳細資訊，請參閱個別資料庫文件。
2. 輸入證書到 Sentinel FIPS KeyStore。

   如需關於輸入證書的詳細資訊，請參閱 「輸入證書到 FIPS Keystore 資料庫」(第 131 頁)。
3. 繼續設定連接器。

Sentinel Link 連接器

只有在設定 Sentinel Link 事件來源伺服器的網路設定時選取了「已加密 (HTTPS)」選項，才需要遵循以下程序。

要設定 Sentinel Link 連接器在 FIPS 140-2 模式中執行：

1. 新增或編輯 Sentinel Link 事件來源伺服器。繼續完成組態畫面，直到顯示「安全性」視窗為止。如需詳細資訊，請參閱《*Sentinel Link 連接器指南*》。
2. 選取「*用戶端驗證類型*」欄位其中一個選項。用戶端驗證類型會判斷 SSL Sentinel Link 事件來源伺服器的嚴格程度，用以驗證嘗試傳送資料的 Sentinel Link 事件來源 (Sentinel Link 整合器) 的身分。
   - **開啟：** 允許所有來自用戶端的 SSL 連結 (Sentinel Link 整合器)。無法執行任何整合器證書驗證。
   - **嚴格：** 驗證整合器證書為有效的 X.509 證書，並檢查整合器證書受到事件來源伺服器信任。如需詳細資訊，請參閱個別資料庫文件。

     針對「嚴格」選項：

     - 若 Sentinel Link 整合器是在 FIPS 140-2 模式中，您必須從 Sentinel 寄件者機器複製 /etc/opt/novell/sentinel/config/sentinel.cer 檔案到 Sentinel 接收器機器。輸入此證書到 Sentinel FIPS KeyStore 接收器。

       附註： 使用由證書管理中心 (CA) 數位簽名的自訂證書時，您必須輸入相關的自定證書檔案。

     - 若 Sentinel Link 整合器是在非 FIPS 模式中，您必須輸入自定 整合器證書到 Sentinel FIPS KeyStore 接收器。

       附註： 若寄件者是 Sentinel Log Manager (在非 FIPS 模式中)，接收器是在 FIPS 140-2 模式中的 Sentinel，寄件者上要輸入的伺服器證書是來自 Sentinel 接收器機器的 /etc/opt/novell/sentinel/config/sentinel.cer 檔案。

     當 Sentinel 在 FIPS 140-2 模式中執行時，您無法使用事件來源管理 (ESM) 介面輸入用戶端證書。如需關於輸入證書的詳細資訊，請參閱 「輸入證書到 FIPS Keystore 資料庫」(第 131 頁)。

附註： 在 FIPS 140-2 模式中，Sentinel Link 事件來源伺服器使用 Sentinel 伺服器金鑰組。不需要輸入伺服器金鑰組。

Syslog 連接器

只有在設定 Syslog 事件來源伺服器的網路設定時選取了「SSL」協定，才需要遵循以下程序。

要設定 Syslog 連接器在 FIPS 140-2 模式中執行：

1. 新增或編輯 Syslog 事件來源伺服器。繼續完成組態畫面，直到顯示「網路」視窗為止。如需詳細資訊，請參閱《*Syslog 連接器指南*》。
2. 按一下「設定」。

3 選取「*用戶端驗證類型*」欄位其中一個選項。用戶端驗證類型會判斷 SSL Syslog 事件來源伺服器的嚴格程度，用以驗證嘗試傳送資料的 Syslog 事件來源的身分。

- **開啟：** 允許所有來自用戶端的 SSL 連接 (事件來源)。無法執行任何用戶端證書驗證。
- **嚴格：** 驗證證書為有效的 X.509 證書，並檢查用戶端證書受到事件來源伺服器信任。新來源必須特定新增到 Sentinel (這可避免不受約束的來源傳送資料到 Sentinel)。

  針對「嚴格」選項，您必須將 Syslog 用戶端的證書輸入 Sentinel FIPS KeyStore。

  當 Sentinel 在 FIPS 140-2 模式中執行時，您無法使用事件來源管理 (ESM) 介面輸入用戶端證書。

  如需關於輸入證書的詳細資訊，請參閱 「輸入證書到 FIPS Keystore 資料庫」(第 131 頁)。

附註： 在 FIPS 140-2 模式中，Syslog 事件來源伺服器使用 Sentinel 伺服器金鑰組。不需要輸入伺服器金鑰組。

4 若 syslog 用戶端已啟用伺服器驗證，用戶端必須信任 Sentinel 伺服器證書或遠端 Collector Manager 證書，視連接器部署位置而定。

Sentinel 伺服器證書檔案位在 /etc/opt/novell/sentinel/config/sentinel.cer。

遠端收集器管理員證書檔案位在 /etc/opt/novell/sentinel/config/rcm.cer。

附註： 使用由證書管理中心 (CA) 數位簽名的自訂證書時，該用戶端必須信任相關的證書檔案。

Windows 事件 (WMI) 連接器

要設定 Windows 事件 (WMI) 連接器在 FIPS 140-2 模式中執行：

1 新增或編輯 Windows 事件連接器。繼續完成組態畫面，直到顯示「安全性」視窗為止。如需詳細資訊，請參閱《*Windows 事件 (WMI) 連接器指南*》。

2 按一下「設定」。

3 選取「*用戶端驗證類型*」欄位其中一個選項。用戶端驗證類型會判斷 Windows 事件連接器的嚴格程度，用以驗證嘗試傳送資料的用戶端 Windows 事件收集服務 (WECS) 的身分。

- **開啟：** 允許所有來自用戶端 WECS 的 SSL 連接。無法執行任何用戶端證書驗證。
- **嚴格：** 驗證證書為有效的X.509證書，並檢查用戶端WECS證書是由CA簽名。新來源必須特定新增 (這可避免不受約束的來源傳送資料到 Sentinel)。

  針對「嚴格」選項，您必須將用戶端 WECS 的證書輸入 Sentinel FIPS KeyStore。當 Sentinel 在 FIPS 140-2 模式中執行時，您無法使用事件來源管理 (ESM) 介面輸入用戶端證書。

  如需關於輸入證書的詳細資訊，請參閱 「輸入證書到 FIPS Keystore 資料庫」(第 131 頁)。

附註： 在 FIPS 140-2 模式中，Windows 事件來源伺服器使用 Sentinel 伺服器金鑰組。不需要輸入伺服器金鑰組。

4 若 Windows 用戶端已啟用伺服器驗證，用戶端必須信任 Sentinel 伺服器證書或遠端Collector Manager 證書，視連接器部署位置而定。

Sentinel 伺服器證書檔案位在 /etc/opt/novell/sentinel/config/sentinel.cer。

遠端 Collector Manager 證書檔案位在 /etc/opt/novell/sentinel/config/rcm.cer。

附註： 使用由證書管理中心 (CA) 數位簽名的自訂證書時，該用戶端必須信任相關的證書檔案。

5 若您要自動同步事件來源或使用 Active Directory 連接填入事件來源的清單，您必須輸入 Active Directory 伺服器證書到 Sentinel FIPS KeyStore。

如需關於輸入證書的詳細資訊，請參閱「輸入證書到 FIPS Keystore 資料庫」(第 131 頁)。

Sentinel Link 整合器

只有在設定 Sentinel Link 整合器的網路設定時選取了「已加密 (HTTPS)」選項，才需要遵循以下程序。

要設定 Sentinel Link 整合器在 FIPS 140-2 模式中執行：

1 當 Sentinel Link 整合器在 FIPS 140-2 模式中時，必須強制進行伺服器驗證。在設定整合器例項之前，將 Sentinel Link 伺服器證書輸入 Sentinel FIPS KeyStore：

- **若 Sentinel Link 連接器是在 FIPS 140-2 模式中**：

  若連接器是部署在 Sentinel 伺服器中，您必須從 Sentinel 接收器機器複製 /etc/opt/novell/sentinel/config/sentinel.cer 檔案到 Sentinel 寄件者機器。

  若連接器是部署在遠端 Collector Manager 中，您必須從遠端 Collector Manager 機器複製 /etc/opt/novell/sentinel/config/rcm.cer 檔案到 Sentinel 接收器機器。

  輸入此證書到 Sentinel FIPS KeyStore 寄件者。

  附註： 使用由證書管理中心 (CA) 數位簽名的自訂證書時，您必須輸入相關的自定證書檔案。

- 若 Sentinel Link 連接器是在非 FIPS 模式中：

  將自定 Sentinel Link 伺服器證書輸入 Sentinel 寄件者 FIPS KeyStore。

  附註： 當 Sentinel Link 整合器是在 FIPS 140-2 模式中，而且 Sentinel Link 連接器是在非 FIPS 模式中，請使用連接器上的自定伺服器金鑰組。請勿使用內部伺服器金鑰組。

如需關於輸入證書的詳細資訊，請參閱「輸入證書到 FIPS Keystore 資料庫」(第 131 頁)。

2 繼續設定整合器例項。

附註： 在 FIPS 140-2 模式中，Sentinel Link 整合器使用 Sentinel 伺服器金鑰組。不需要輸入整合器金鑰組。

LDAP Integrator

要設定 LDAP Integrator 在 FIPS 140-2 模式中執行：

1 設定 Integrator 例項之前，請從 LDAP 伺服器下載證書，然後另存為 ldap.cert 檔案到 Sentinel 伺服器的 /etc/opt/novell/sentinel/config 目錄。

例如，使用

```
openssl s_client -connect <LDAP server IP>:636
```

然後將傳回的文字 (介於 (但不含) BEGIN 和 END 行之間) 複製到檔案。

2 輸入證書到 Sentinel FIPS KeyStore。

如需關於輸入證書的詳細資訊，請參閱 「輸入證書到 FIPS Keystore 資料庫」(第 131 頁)。

3 繼續設定整合器例項。

SMTP Integrator

SMTP Integrator 支援版本 2011.1r2 和更新版本的 FIPS 140-2。不需要變更任何組態。

Syslog Integrator

只有在設定 Syslog Integrator 的網路設定時選取「已加密 (SSL)」選項的情況下，才需要執行下列程序。

若要將 Syslog Integrator 設定為在 FIPS 140-2 模式中執行：

1 當 Syslog Integrator 在 FIPS 140-2 模式中時，必須強制進行伺服器驗證。設定整合器例項前，請將 Syslog 伺服器證書輸入 Sentinel FIPS 金鑰儲存區：

- **如果 Syslog Integrator 在 FIPS 140-2 模式中：** 如果連接器是部署在 Sentinel 伺服器中，您必須將 /etc/opt/novell/sentinel/config/sentinel.cer 檔案從 Sentinel 接收器伺服器複製到 Sentinel 寄件者伺服器。

  如果連接器是部署在遠端 Collector Manager 中，您必須將 /etc/opt/novell/sentinel/config/rcm.cer 檔案從遠端 Collector Manager 接收器電腦複製到 Sentinel 接收器電腦。

  輸入此證書到 Sentinel FIPS KeyStore 寄件者。

  附註： 使用由證書管理中心 (CA) 數位簽名的自訂證書時，您必須輸入相關的自定證書檔案。

- **如果 Syslog Connector 在非 FIPS 模式中：** 您必須將自定 Syslog 伺服器證書輸入 Sentinel FIPS 金鑰儲存區寄件者。

  附註： 當 Syslog Integrator 在 FIPS 140-2 模式中，且 Syslog Connector 在非 FIPS 模式中時，請使用連接器上的自定伺服器金鑰組。請勿使用內部伺服器金鑰組。

要輸入證書到 FIPS KeyStore 資料庫：

1. 複製證書檔案到 Sentinel 伺服器或遠端 Collector Manager 上的任何暫存位置。
2. 移至 /opt/novell/sentinel/bin 目錄。
3. 執行下列指令以將證書輸入 FIPS 金鑰儲存區資料庫，並遵循畫面上的指示：

   ```
   ./convert_to_fips.sh -i <certificate file path>
   ```

4. 系統提示重新啟動 Sentinel 伺服器或 Collector Manager 時，輸入 yes 或 y。

2 繼續設定整合器例項。

附註： 在 FIPS 140-2 模式中，Syslog Integrator 會使用 Sentinel 伺服器金鑰組。您不需要輸入整合器金鑰組。

在 FIPS 140-2 模式中使用非 FIPS 啟用的連接器搭配 Sentinel

本節提供如何在 FIPS 140-2 模式中使用非 FIPS 啟用的連接器搭配 Sentinel 伺服器的相關資訊。若您有不支援 FIPS 的來源，或您想要在環境中收集來自非 FIPS 連接器的事件，建議採用此方法。

如果要在 FIPS 140-2 模式中使用非 FIPS 連接器搭配 Sentinel：

1. 在非 FIPS 模式中安裝 Collector Manager，以連接到在 FIPS 140-2 模式中的 Sentinel 伺服器。

   如需詳細資訊，請參閱第 III 部分「安裝 Sentinel」(第 67 頁)。
2. 將非 FIPS 連接器指定部署到非 FIPS 遠端 Collector Manager。

附註： 當非 FIPS 連接器 (例如稽核連接器和檔案連接器) 部署在連接到在 FIPS 140-2 模式中的 Sentinel 伺服器之非 FIPS 遠端 Collector Manager 上時，有一些已知的問題。如需這些已知問題的相關資訊，請參閱 Sentinel 版本說明。

輸入證書到 FIPS Keystore 資料庫

您必須插入證書到 Sentinel FIPS KeyStore 資料庫，才能從擁有這些證書的元件建立安全的 (SSL) 通訊到 Sentinel。啟用 FIPS 140-2 模式時，您無法使用 Sentinel 使用者介面來上傳身分證明。您必須手動輸入證書到 FIPS KeyStore 資料庫。

針對使用部署到遠端 Collector Manager 的連接器的事件來源，您必須輸入證書到遠端 Collector Manager 的 FIPS KeyStore 資料庫，不是輸入到集中式 Sentinel 伺服器。

要輸入證書到 FIPS KeyStore 資料庫：

1. 複製證書檔案到 Sentinel 伺服器或遠端 Collector Manager 上的任何暫存位置。
2. 瀏覽至 Sentinel bin 目錄。預設值位置是 /opt/novell/sentinel/bin。
3. 執行以下指令，輸入證書到 FIPS KeyStore 資料庫，然後依照畫面上的指示執行：

   ```
   ./convert_to_fips.sh -i <certificate file path>
   ```
4. 系統提示重新啟動 Sentinel 伺服器或遠端Collector Manager 時，輸入 yes 或 y。

回復 Sentinel 到非 FIPS 模式

本節提供如何回復 Sentinel 和其元件到非 FIPS 模式的相關資訊。

- 「回復 Sentinel 伺服器到非 FIPS 模式」(第 131 頁)
- 「回復遠端 Collector Manager 或遠端 Correlation Engine 到非 FIPS 模式」(第 132 頁)

回復 Sentinel 伺服器到非 FIPS 模式

只有在您已將 Sentinel 伺服器備份，再轉換為在 FIPS 140-2 模式中執行時，您才可以將 Sentinel 伺服器從在 FIPS 140-2 模式中執行回復成在非 FIPS 模式中執行。

附註： 當您回復 Sentinel 伺服器到非 FIPS 模式時，您會遺失在轉換為執行 FIPS 140-2 模式之後的事件、事件資料和對 Sentinel 伺服器進行的組態變更。Sentinel 系統將會回存到非 FIPS 模式的上次還原點。請先將目前的系統備份，再回復到非 FIPS 模式，以便將來使用。

要回復 Sentinel 伺服器到非 FIPS 模式：

1. 以根使用者身分登入 Sentinel 伺服器。
2. 切換至 novell 使用者。
3. 瀏覽至 Sentinel bin 目錄。預設值位置是 /opt/novell/sentinel/bin。
4. 執行下列指令以回復 Sentinel 伺服器到非 FIPS 模式，並遵循畫面上的指示：

   ./backup_util.sh -f *<backup_file_name.tar.gz>* -m 'restore'

   例如，若 non-fips20130124191111359034887.tar.gz 是備份檔案，請執行以下指令：

   ./backup_util.sh -f non-fips20130124191111359034887.tar.gz -m 'restore'
5. 重新啟動 Sentinel 伺服器。

回復遠端 Collector Manager 或遠端 Correlation Engine 到非 FIPS 模式

您可以回復遠端 Collector Manager 或遠端 Correlation Engine 到非 FIPS 模式。

要回復遠端 Collector Manager 或遠端 Correlation Engine 到非 FIPS 模式：

1. 登入遠端 Collector Manager 或遠端 Correlation Engine 系統。
2. 切換為 novell 使用者 (su novell)。
3. 瀏覽至 bin 目錄。預設值位置是 /opt/novell/sentinel/bin。
4. 執行 revert_to_nonfips.sh 程序檔並遵循畫面上的指示。
5. 重新啟動遠端 Collector Manager 或遠端 Correlation Engine。

25 新增同意標題頁

Sentinel 可讓您在登入之前顯示同意標題頁。您可以依據需求指定標題頁的內容。在新增同意標題頁後，您在每次登入 Sentinel 時都必須接受同意標題頁中的條款。

若要新增同意標題頁：

1. 以 novell 使用者身分登入 Sentinel 伺服器。
2. 瀏覽至 /<Sentinel_installation_path>/var/opt/novell/sentinel/3rdparty/jetty/webapps/ROOT/siemdownloads。
3. 新增名為 USER_AGREEMENT.txt 的文字檔。
4. 輸入使用者合約文字。
5. 儲存檔案。
6. 啟動 Sentinel 以檢視同意標題頁。

Sentinel 此時會在登入畫面上顯示同意標題頁。

附註： 在升級 Sentinel 之前，您必須手動備份 USER_AGREEMENT.txt 檔案。

V 升級 Sentinel

本節提供升級 Sentinel 和其他元件的相關資訊。

26 執行核對清單

在升級 Sentinel 之前，請檢閱下列核對清單以確定能順利升級：

表格 26-1 *執行核對清單*

❒	任務	請參閱
❒	確定安裝 Sentinel 和其元件的電腦符合指定要求。	Sentinel 技術資訊網站
❒	檢閱支援的作業系統版本說明以瞭解已知問題。	SUSE 版本說明
❒	檢閱 Sentinel 版本說明，以查看新功能並瞭解已知的問題。	Sentinel 版本說明
❒	完成「先決條件」中所提及的任務。	第 27 章 「必要條件」(第 139 頁)

27 必要條件

儲存自定組態資訊

儲存 server.conf 檔案設定

如果已在 server.conf 檔案中設定任何自定組態參數值，在升級前，請先將這些值儲存在另外的檔案中。

若要儲存您的自定組態資訊：

1. 使用 novell 使用者身分登入 Sentinel 伺服器，然後瀏覽至 /etc/opt/novell/sentinel/config/ 目錄。
2. 建立名為 server-custom.conf 的組態檔，並將您的自定組態參數新增至這個檔案。

Sentinel 會在升級期間將儲存的自定組態套用至這些組態檔。

儲存 jetty-ssl 檔案設定

Sentinel 8.1 包含 Jetty 的更新版本。Jetty 的更新版本包含本身檔案結構的變更。

如果您已在之前版本的 Sentinel 中修改 /etc/opt/novell/sentinel/3rdparty/jetty/jetty-ssl.xml 檔案 (例如移除任何加密)，請先將這些變更儲存在個別的檔案中，然後再升級 Sentinel。

Sentinel 升級完成後，請將這些變更複製到 /etc/opt/novell/sentinel/3rdparty/jetty/jetty-ssl-context.xml 檔案，然後重新啟動 Sentinel。

延長事件關聯資料的保留期間

從 Sentinel 7.4.4 開始，事件關聯資料的保留期間預設為 14 天。如果您即將從早於 7.4.4 版的 Sentinel 進行升級，則您為事件關聯資料設定的保留期間將會在升級之後被覆寫為 14 天。若要避免此情況，您可以透過在 configuration.properties 檔案中新增內容，來將保留期間設定為您要的值。如需詳細資訊，請參閱 *《Sentinel 管理員指南》*中的「「設定事件關聯資料的保留期間」」。

預先升級 SSDM 組態

升級程序將會更新 Spark 應用程式的相關檔案。若要使用更新的檔案，您必須重新啟動 Spark 工作並重設 Kafka 主題上的所有 Spark 檢查點。若要避免因重設 Kafka 主題檢查點而遺失資料，您必須先暫停將資料從 Collector Manager 轉遞至 Kafka，然後再升級 SSDM。資料轉遞暫停後，資料將會儲存在 Collector Manager，直到恢復資料轉遞。當 Spark 應用程式處理好在轉遞暫停前轉遞至 Kafka 的資料時，檢查點即可安全地進行重設，而不會遺失任何資料。

若要暫停從 Collector Manager 轉遞事件至 Kafka：

1. 在 Sentinel 主要介面上，按一下「**儲存**」>「**可擴充儲存**」>「**進階組態**」>「**Kafka**」。
2. 加入下列內容並將其設定為 true：

   pause.events.tokafka
3. 按一下「**儲存**」。

Change Guardian 整合

Sentinel 與 Change Guardian 4.2 以上版本相容。若要接收來自 Change Guardian 的事件，您必須先將 Change Guardian 伺服器、代理程式和規則編輯器升級至 4.2 或更新版本，以確定升級後 Sentinel 會繼續接收來自 Change Guardian 的事件。

28 升級 Sentinel 傳統安裝

升級 Sentinel

使用下列步驟升級 Sentinel 伺服器：

1. 請將組態備份，然後建立 ESM 輸出。

   如需詳細資訊，請參閱《「 Sentinel 管理指南」》中的「*備份與還原資料*」。

2. (條件式) 若您已在server.xml，collector_mgr.xml，或correlation_engine.xml檔案中自訂組態設定，請確保您已建立以 obj-元件 id 命名的適當內容檔案，以確保在升級後保留自訂組態設定。若需要更多資訊，請參閱「《 Sentinel 管理指南》」中的「*保留 XML 檔案自訂設定*」。

3. 從下載網站下載最新的安裝程式。

4. 以 root 身分登入要升級 Sentinel 的伺服器。

5. 指定下列指令，以從 tar 檔案擷取安裝檔案：

   ```
   tar xfz <install_filename>
   ```

   將 *<install_filename>* 取代為安裝檔案的實際名稱。

6. 變更至擷取安裝檔案的目錄。

7. 指定下列指令以升級 Sentinel：

   ```
   ./install-sentinel
   ```

8. 若要繼續使用您選擇的語言，請選取語言旁指定的數字。

   使用者授權合約會以選取的語言顯示。

9. 閱讀使用者授權後輸入 yes 或 y，接受授權，然後繼續安裝。

10. 安裝程序檔偵測到已存在產品的較舊版本，並會提示您指定是否要升級該產品。若要繼續升級，請按下 y 鍵。

    安裝會開始安裝所有 RPM 封裝。此安裝可能需要數秒鐘完成。

11. 清除網頁瀏覽器快取以檢視 Sentinel 最新版本。

12. 清除用戶端電腦上的 Java 網頁啟動快取，以使用最新版本的 Sentinel 應用程式。

    您可以使用 javaws -clearcache 指令或使用 Java Control Center 清除 Java 網頁啟動快取。如需詳細資訊，請參閱 http://www.java.com/en/download/help/plugin_cache.xml。

13 (條件式) 若 PostgreSQL 資料庫已升級至主要版本 (例如，8.0 至 9.0 或 9.0 至 9.1)，請清除 PostgreSQL資料庫中的舊版PostgreSQL檔案。如需PostgreSQL資料庫是否已升級的詳細資訊，請參閱 Sentinel 版本說明。

13a 切換至 novell 使用者。

```
su novell
```

13b 瀏覽至 bin 資料夾：

```
cd /opt/novell/sentinel/3rdparty/postgresql/bin
```

13c 使用下列指令刪除所有舊版的 PostgreSQL 檔案：

```
./delete_old_cluster.sh
```

14 若要升級 Collector Manager 系統和 Correlation Engine 系統，請參閱「升級 Collector Manager 或 Correlation Engine」(第 144 頁)。

15 (條件式) 如果您要使用 Kerberos 驗證，請在 Java Runtime Environment 中啟用 AES256，因為 java資料夾在升級期間會取代為預設檔案。若要在Java Runtime Environment中啟用AES256，請完成下列步驟：

15a 從下列位置下載 Java Cryptography Extension (JCE) 8：http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html

15b 將兩個 *.jar 檔案解壓縮並複製到 /opt/novell/sentinel/jdk/jre/lib/security 目錄。

15c (條件式) 如果您要在 HA 環境中執行 Sentinel，請在叢集中的所有節點上重複這些步驟。

15d 重新啟動 Sentinel。

以非 root 使用者升級 Sentinel

如果組織規則不允許您以 root 身分執行 Sentinel 的完整升級，您能以其他使用者的身分升級 Sentinel。在此類型的升級作業中，有幾個步驟是以 root 使用者的身分執行，接著您需要以 root 使用者建立的其他使用者來繼續升級 Sentinel。

1 請將組態備份，然後建立 ESM 輸出。

如需備份資料的詳細資訊，請參閱《「 Sentinel 管理指南」》中的「*備份與還原資料*」。

2 (條件式) 若您已在server.xml，collector_mgr.xml，或correlation_engine.xml檔案中自訂組態設定，請確保您已建立以 obj-元件 id 命名的適當內容檔案，以確保在升級後保留自訂組態設定。如需詳細資訊，請參閱「《 Sentinel Administration Guide》」(NetIQ Sentinel 管理指南)中的*Backing Up and Restoring Data*(備份與還原資料)。

3 從 下載網站下載安裝檔案。

4 在指令行指定下列指令，以從 tar 檔案擷取安裝檔案：

```
tar -zxvf <install_filename>
```

將 *<install_filename>* 取代為安裝檔案的實際名稱。

5 以 root 身分登入要升級 Sentinel 的伺服器。

6 從 Sentinel 安裝檔擷取 squashfs RPM。

7 在 Sentinel 伺服器上安裝 squashfs。

```
rpm -Uvh <install_filename>
```

8 指定以下指令，以變更為新建立的非 root novell 使用者：novell：

su novell

9 (條件式) 若要進行互動升級：

9a 請指定以下指令：

```
./install-sentinel
```

若要將 Sentinel 升級在非預設位置，請在指令中指定 --location 選項。例如：

```
./install-sentinel --location=/foo
```

9b 繼續執行步驟 11。

10 (條件式) 若要進行靜默升級，請指定下列指令：

```
./install-sentinel -u <response_file>
```

系統將會利用儲存在回應檔案中的值繼續進行安裝。Sentinel 升級已完成。

11 指定要用於升級作業的語言號碼。

使用者授權合約會以選取的語言顯示。

12 閱讀使用者授權，並輸入 yes 或 y，接受授權，然後繼續升級。

升級會開始安裝所有 RPM 封裝。此安裝可能需要數秒鐘完成。

13 清除網頁瀏覽器快取以檢視 Sentinel 最新版本。

14 清除用戶端電腦上的 Java 網頁啟動快取，以使用最新版本的 Sentinel 應用程式。

您可以使用 javaws -clearcache 指令或使用 Java Control Center 清除 Java 網頁啟動快取。如需詳細資訊，請參閱 http://www.java.com/en/download/help/plugin_cache.xml。

15 (條件式) 若 PostgreSQL 資料庫已升級至主要版本 (例如，8.0 至 9.0 或 9.0 至 9.1)，請清除 PostgreSQL資料庫中的舊版PostgreSQL檔案。如需PostgreSQL資料庫是否已升級的詳細資訊，請參閱 Sentinel 版本說明。

15a 切換至 novell 使用者。

```
su novell
```

15b 瀏覽至 bin 資料夾：

```
cd /opt/novell/sentinel/3rdparty/postgresql/bin
```

15c 使用下列指令刪除所有 postgreSQL 舊檔案：

```
./delete_old_cluster.sh
```

16 (條件式) 如果您要使用 Kerberos 驗證，請在 Java Runtime Environment 中啟用 AES256，因為 java資料夾在升級期間會取代為預設檔案。若要在Java Runtime Environment中啟用AES256，請完成下列步驟：

16a 從下列位置下載 Java Cryptography Extension (JCE) 8：http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html

16b 將兩個 *.jar 檔案解壓縮並複製到 /opt/novell/sentinel/jdk/jre/lib/security 目錄。

16c (條件式) 如果您要在 HA 環境中執行 Sentinel，請在叢集中的所有節點上重複這些步驟。

16d 重新啟動 Sentinel。

升級 Collector Manager 或 Correlation Engine

使用下列步驟升級 Collector Manager 和 Correlation Engine：

1. 請將組態備份並建立 ESM 輸出。

   如需詳細資訊，請參閱「《 Sentinel Administration Guide》」(NetIQ Sentinel 管理指南) 中的*Backing Up and Restoring Data*(備份與還原資料)。
2. 以管理員角色中的使用者身分導覽至 **Sentinel 主要介面**。
3. 選取「**下載**」。
4. 在「Collector Manager 安裝程式」區段中，按一下「**下載安裝程式**」。
5. 將安裝程式檔案儲存到各自的 Collector Manager 或 Correlation Engine 伺服器。
6. 將檔案複製到暫存位置。
7. 解壓縮檔案的內容。
8. 執行以下程序檔：

   針對 Collector Manager：

   ```
   ./install-cm
   ```

   針對 Correlation Engine：

   ```
   ./install-ce
   ```
9. 依照螢幕上的提示完成安裝。
10. (條件式) 若要自定安裝，請執行下列指令將 Sentinel 伺服器、Collector Manager 與 Correlation Engine 之間的組態同步化：

    ```
    /opt/novell/sentinel/setup/configure.sh
    ```

升級作業系統

此 Sentinel 版本包括可在作業系統升級程序期間使用的指令集。這些指令可確定 Sentinel 在升級作業系統後是否正常運作。

附註： 升級作業系統前，您必須先升級 Sentinel。

請使用下列步驟升級作業系統：

1. 在要升級作業系統的 Sentinel 伺服器上，請以下列其中一個身分登入：
   - root 使用者
   - 非 root 使用者
2. 開啟指令提示，並將目錄變更為解壓縮 Sentinel 安裝檔案的目錄。
3. 停止 Sentinel 服務：

   rcsentinel stop
4. (條件式) 如果 Sentinel 在作業系統升級前處於 FIPS 模式，則 NSS 資料庫檔案必須透過執行下列指令來手動進行升級：

   certutil -K -d sql:/etc/opt/novell/sentinel/3rdparty/nss -X

請依照畫面上的指示升級 NSS 資料庫。

請給予 Novell 使用者可存取以下檔案的完整權限：

```
cert9.db
key4.db
pkcs11.txt
```

5 升級作業系統。

6 (條件式) 如果您使用 Mozilla Network Security Services (NSS) 3.29，則不會安裝兩個相依的 RPM 檔案 libfreebl3-hmac 和 libsoftokn3-hmac。請手動安裝下列 RPM 檔案：libfreebl3-hmac and libsoftokn3-hmac。

7 (條件式) 針對 RHEL 7。*x*，執行以下指令，檢查 RPM 資料庫中是否有任何錯誤：

rpm -qa --dbpath <*install_location*>/rpm | grep novell

例子：# rpm -qa --dbpath /custom/rpm | grep novell

7a 若有任何錯誤，執行以下指令以修復錯誤：

rpm --rebuilddb --dbpath <*install_location*>/rpm

例子：# rpm --rebuilddb --dbpath /custom/rpm

7b 執行步驟 7 提及的指令以確保沒有錯誤。

8 針對下列項目重複此程序：

- Collector Manager
- Correlation Engine
- NetFlow Collector Manager

9 重新啟動 Sentinel 服務：

rcsentinel restart

此步驟不適用於 Sentinel HA。

29 升級 Sentinel 裝置

本章中的程序將引導您完成 Sentinel 裝置的升級。您可以選擇僅升級 Sentinel 而不升級 SLES 作業系統，或同時升級 Sentinel 和 SLES 作業系統。由於 8.2 Sentinel 裝置包含 SLES 12 SP3，因此 SLES 11 更新通道現已淘汰，且將在 SUSE 結束對 SLES 11 的一般支援時移除。因此，您應升級至 Sentinel 8.2 應用裝置，其中包含SLES12SP3作業系統，以繼續接收作業系統更新。您必須在升級作業系統前，先升級 Sentinel。

升級 Sentinel

透過應用裝置更新通道升級 Sentinel

您可以使用 Zypper 來升級 Sentinel。Zypper 是指令行套件管理員，可讓您執行裝置的互動升級。在需要使用者互動才可完成升級的例項中 (例如使用者授權合約更新)，您必須使用 Zypper 來升級 Sentinel 裝置。

若要透過應用裝置更新通道來升級應用裝置：

1. 請將組態備份，然後建立 ESM 輸出。

   如需詳細資訊，請參閱「《 Sentinel Administration Guide》」(NetIQ Sentinel 管理指南) 中的*Backing Up and Restoring Data*(備份與還原資料)。

2. (條件式) 若您已在server.xml，collector_mgr.xml，或correlation_engine.xml檔案中自訂組態設定，請確保您已建立以 obj-元件 id 命名的適當內容檔案，以確保在升級後保留自訂組態設定。若需要更多資訊，請參閱「《 Sentinel 管理指南》」中的*「保留 XML 檔案自訂設定」*。

3. 以 root 使用者的身分登入裝置主控台。

4. 執行以下指令：

   ```
   /usr/bin/zypper patch
   ```

5. (條件式) 如果安裝程式顯示您必須解決 OpenSSH 套件相依性的訊息，請輸入適合的選項以降級 OpenSSH 套件。

6. (條件式) 如果安裝程式顯示表示 ncgOverlay 架構中變更的訊息，請輸入適合的選項以接受架構變更。

7. (條件式) 如果安裝程式顯示您必須解決某些裝置套件相依性的訊息，請輸入適合的選項以解除安裝相依套件。

8. 輸入 Y 繼續。

9. 輸入 yes 接受授權合約。

10 重新啟動 Sentinel 裝置。

11 (條件式) 如果 Sentinel 安裝在自定連接埠，或者 Collector Manager 或 Correlation Engine 為 FIPS 模式，請執行下列指令：

```
/opt/novell/sentinel/setup/configure.sh
```

12 清除網頁瀏覽器快取以檢視 Sentinel 最新版本。

13 清除用戶端電腦上的 Java 網頁啟動快取，以使用最新版本的 Sentinel 應用程式。

您可以使用 javaws -clearcache 指令或使用 Java Control Center 清除 Java 網頁啟動快取。如需詳細資訊，請參閱 http://www.java.com/en/download/help/plugin_cache.xml。

14 (條件式) 若 PostgreSQL 資料庫已升級至主要版本 (例如，8.0 至 9.0 或 9.0 至 9.1)，請清除 PostgreSQL資料庫中的舊版PostgreSQL檔案。如需PostgreSQL資料庫是否已升級的詳細資訊，請參閱 Sentinel 版本說明。

14a 切換至 novell 使用者。

```
su novell
```

14b 瀏覽至 bin 資料夾：

```
cd /opt/novell/sentinel/3rdparty/postgresql/bin
```

14c 使用下列指令刪除所有 postgreSQL 舊檔案：

```
./delete_old_cluster.sh
```

15 (條件式) 若要升級 Collector Manager 或 Correlation Engine，請依照 步驟 3 到 步驟 11 的指示進行。

16 (條件式) 如果您要使用 Kerberos 驗證，請在 Java Runtime Environment 中啟用 AES256，因為 java資料夾在升級期間會取代為預設檔案。若要在Java Runtime Environment中啟用AES256，請完成下列步驟：

16a 從下列位置下載 Java Cryptography Extension (JCE) 8：http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html

16b 將兩個 *.jar 檔案解壓縮並複製到 /opt/novell/sentinel/jdk/jre/lib/security 目錄。

16c 重新啟動 Sentinel。

17 (條件式) 如果您要在 HA 環境中執行 Sentinel，請在叢集中的所有節點上重複這些步驟。

18 (條件式) 若要升級作業系統，請參閱「升級作業系統」(第 149 頁)。

19 重新啟動 Sentinel。

使用 SMT 升級 Sentinel

若您所處的安全環境必須在無直接網際網路存取狀態下執行裝置，則可以使用 Subscription Management Tool (SMT) 來設定裝置，並得以將裝置升級至最新的可用版本。

1 請確認已使用 SMT 設定裝置。

如需詳細資訊，請參閱「使用 SMT 設定裝置」(第 101 頁)。

2 請將組態備份，然後建立 ESM 輸出。

如需詳細資訊，請參閱「《 Sentinel Administration Guide》」(NetIQ Sentinel 管理指南) 中的*Backing Up and Restoring Data*(備份與還原資料)。

3 (條件式) 若您已在server.xml，collector_mgr.xml，或correlation_engine.xml檔案中自訂組態設定，請確保您已建立以 obj-元件 id 命名的適當內容檔案，以確保在升級後保留自訂組態設定。若需要更多資訊，請參閱「《 Sentinel 管理指南》」中的*「保留 XML 檔案自訂設定」*。

4 以 root 使用者的身分登入裝置主控台。

5 重新整理升級的儲存機制：

```
zypper ref -s
```

6 檢查裝置是否已啟用，以便進行升級：

```
zypper lr
```

7 (選擇性) 檢查裝置可用的更新：

```
zypper lu
```

8 (選擇性) 檢查包含裝置可用更新的套件：

```
zypper lp -r SMT-http_<smt_server_fqdn>:<package_name>
```

9 更新裝置：

```
zypper up -t patch -r SMT-http_<smt_server_fqdn>:<package_name>
```

10 重新啟動裝置。

```
rcsentinel restart
```

11 (條件式) 如果 Sentinel 安裝在自定連接埠，或者 Collector Manager 或 Correlation Engine 為 FIPS 模式，請執行下列指令：

```
/opt/novell/sentinel/setup/configure.sh
```

12 (條件式) 若要升級 Collector Manager 或 Correlation Engine，請依照 步驟 4 到 步驟 11 的指示進行。

13 (條件式) 如果您要使用 Kerberos 驗證，請在 Java Runtime Environment 中啟用 AES256，因為 java資料夾在升級期間會取代為預設檔案。若要在Java Runtime Environment中啟用AES256，請完成下列步驟：

13a 從下列位置下載 Java Cryptography Extension (JCE) 8：http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html

13b 將兩個 *.jar 檔案解壓縮並複製到 /opt/novell/sentinel/jdk/jre/lib/security 目錄。

13c 重新啟動 Sentinel。

14 (條件式) 如果您要在 HA 環境中執行 Sentinel，請在叢集中的所有節點上重複這些步驟。

15 (條件式) 若要升級作業系統，請參閱「升級作業系統」(第 149 頁)。

16 重新啟動 Sentinel。

升級作業系統

您必須在升級 Sentinel 之後升級作業系統。升級作業系統後，您必須設定應用裝置，才能使用新的 Sentinel 應用裝置管理員功能。Sentinel 應用裝置管理員提供簡單的 Web 式使用者介面，可協助您設定並管理應用裝置。此功能會取代現有的 WebYast 功能。

若要升級作業系統，請設定裝置：

1. 升級 Sentinel。如需詳細資訊，請參閱 「升級 Sentinel」(第 147 頁)。
2. 停止 Sentinel 服務：

   rcsentinel stop
3. (條件式) 如果 Sentinel 在作業系統升級前處於 FIPS 模式，則 NSS 資料庫檔案必須透過執行下列指令來手動進行升級：

   certutil -K -d sql:/etc/opt/novell/sentinel/3rdparty/nss -X

   請依照畫面上的指示升級 NSS 資料庫。

   請給予 Novell 使用者可存取以下檔案的完整權限：

   ```
   cert9.db
   key4.db
   pkcs11.txt
   ```
4. (條件式) 如果您使用 Mozilla Network Security Services (NSS) 3.29，則不會安裝兩個相依的 RPM 檔案 libfreebl3-hmac 和 libsoftokn3-hmac。請手動安裝下列 RPM 檔案：libfreebl3-hmac and libsoftokn3-hmac。
5. 從 Micro Focus Patch Finder 網站下載 SLES 12 SP3 安裝程式和升級後公用程式。如果使用 Sentinel HA，請同時下載 SLES 12 SP3 HA 檔案。
6. 依照安裝提示來更新作業系統：如果使用 Sentinel HA，當提示要安裝其他附加產品時，請選取您要下載 SLES 12 SP3 HA 檔案的位置，然後繼續升級。

   如需關於升級至 SLES 12 SP3 的詳細資訊，請參閱 SLES 文件。
7. 在升級程序期間，SLES 會將 /etc/sysctl.conf 檔案重新命名為 /etc/sysctl.conf.rpmsave 作為備份，並建立 new /etc/sysctl.conf 檔案。升級後，請將 /etc/sysctl.conf.rpmsave 檔案的內容複製到 /etc/sysctl.conf 檔案。請開啟 sysctl.conf 檔案並搜尋 # Added by sentinel vm.max_map_count。請將此設定移至下一行，如下：

   將

   ```
   net.core.wmem_max = 67108864# Added by sentinel vm.max_map_count : 65530
   vm.max_map_count = 262144
   ```

   變更為

   ```
   net.core.wmem_max = 67108864
   # Added by sentinel vm.max_map_count : 65530
   vm.max_map_count = 262144
   ```
8. (條件式) 如果使用 Sentinel HA，請完成下列章節所提到的步驟：
   - 「設定 iSCSI 目標」(第 198 頁)
   - 「設定 iSCSI 啟動器」(第 198 頁)
   - 「設定 HA 叢集」(第 199 頁)
9. 若要設定應用裝置，請從指令提示字元視窗執行升級後公用程式：

   9a 將檔案解壓縮：

   tar -xvf *<post upgrade utility installer filename>*.tar.gz

   9b 切換到解壓縮公用程式的目錄：

   cd *<post upgrade utility installer filename>*

   9c 若要設定應用裝置，請執行下列指令碼：

。/appliance_SLESISO_post_upgrade.sh

附註： 請勿從遠端執行此指令碼，由於此指令碼將重設網路設定。

9d 依照螢幕上的指示完成設定。

此指令碼將重新設定已安裝的套件，並設定用於管理應用裝置的套件。

10 使用您現有的註冊代碼，再次註冊更新以便接收 Sentinel 與最新的作業系統更新。如需詳細資訊，請參閱 「登錄以進行更新」(第 99 頁)。

30 升級後組態

本章包含升級後組態。

保護 Elasticsearch 中的資料

Sentinel 可利用瀏覽器式分析和搜尋儀表板 Kibana，協助您視覺化儀表板中的事件和警示。Sentinel 可在 Elasticsearch 中儲存警示並編製其索引。您也可以將 Sentinel 設定為在 Elasticsearch 中儲存事件並編製其索引，以運用事件視覺化功能。Sentinel 儀表板會從 Elasticsearch 存取資料，以將事件和警示顯示在儀表板中。若要確保儀表板只會顯示使用者角色有權檢視的資料，並防止 Elasticsearch 中出現未經授權的資料存取，您必須安裝 Elasticsearch 安全性外掛程式。如需詳細資訊，請參閱「保護 Elasticsearch 中的資料」(第 75 頁)。

設定事件視覺化

Sentinel 提供可顯示圖表、表格和映射中資料的事件視覺化。這些視覺化可簡化對大量資料進行視覺化和分析的工作，例如事件、IP 流程事件和警示。您也可以建立自己的視覺化和儀表板。

Sentinel 可利用瀏覽器式分析和搜尋儀表板 Kibana，協助您搜尋事件並將其視覺化。Kibana 可從視覺化資料儲存庫 (Elasticsearch) 存取資料，以將事件顯示在儀表板中。根據預設，Sentinel 會包含一個 Elasticsearch 節點。您必須啟用事件視覺化，才能在 Elasticsearch 中儲存事件及編製其索引。如需詳細資訊，請參閱「設定視覺化資料儲存庫」(第 41 頁)。

附註： 某些使用 Kibana 的 Sentinel 儀表板在您升級至 Sentinel 8.2 之後並不會載入。之所以發生此問題，是因為 Sentinel 8.2 中的 Elasticsearch 和 Kibana 版本已升級，因此現有的 Kibana 索引檔案與已升級的 Elasticsearch 和 Kibana 版本不相容。若要修正此問題，您必須手動刪除現有的 Kibana 索引檔案，並重新建立新的 Kibana 索引檔案。如需詳細資訊，請參閱知識庫文章 7022736。

設定 IP 流程資料收集

Sentinel 現在已可使用 ArcSight SmartConnectors，藉由收集 IP 流程資料和 NetFlow 資料協助您監看企業網路。SmartConnectors 會以事件的形式收集 IP 流程資料，而讓您能夠：

- 使用現有的 Collector Manager 收集 IP 流程資料。您無須再以 NetFlow Collector Manager 來收集 NetFlow 資料。
- 在多種 Sentinel 領域中使用 IP 流程資料，例如視覺化、事件路由、資料聯盟、報告和關連。
- 對 IP 流程資料套用資料保留原則，讓您能夠在所需的期間內儲存這項資料。

在升級 Sentinel 之後，您可以繼續使用 NetFlow 功能，或選擇設定 IP 流程資料收集。不過，隨著 IP 流程資料收集和視覺化功能的推出，先前可用的 NetFlow 功能 (包括 NetFlow 檢視) 現已淘汰，且將在未來移除以提升使用者體驗。

在您啟用 IP 流程資料收集後：

- 系統會以事件的形式收集 IP 流程資料，因此會將其計入 EPS 計數中。
- 您將失去任何在啟用 IP 流程之前收集到的 NetFlow 資料。淘汰的 NetFlow 系統最多會保留 3 天。您可以視需要保留 IP 流程事件，沒有天數限制。
- 您無法將在 IP 流程啟用之前收集到的 NetFlow 資料，移轉至 IP 流程功能中。
- 除非您重新安裝 Sentinel，否則將無法回復設定。
- 您將會登出 Sentinel Main，且必須重新登入。

若要設定 IP 流程資料收集：

1. 安裝並設定 ArcSight SmartConnector。在設定時，請確實設定用來收集 IP 流程資料的相關 SmartConnector。

   如需關於設定 SmartConnector 的詳細資訊，請參閱 Sentinel 外掛程式網站上的「一般通用 CEF 收集器」文件。
2. 在「**Sentinel Main**」>「**收集**」>「**IP 流程**」中選取「**收集 IP 流程資料**」，然後按一下「**啟用**」。

附註： 由於 IP 流程事件現在會傳送至 Collector Manager，您已無須再使用 NetFlow Collector Manager。因此，您可以解除安裝任何現有的 NetFlow Collector Manager。如需詳細資訊，請參閱「解除安裝 NetFlow Collector Manager」(第 212 頁)。

Sentinel Scalable Data Manager 的升級後組態

- 「安裝 Elasticsearch 安全性外掛程式」(第 155 頁)
- 「在 YARN 上更新 Spark 應用程式」(第 155 頁)
- 「啟用 Sentinel 功能」(第 156 頁)
- 「在 Sentinel Scalable Data Manager 中更新儀表板和視覺化」(第 156 頁)

安裝 Elasticsearch 安全性外掛程式

除了 Elasticsearch 節點以外，Sentinel 現在依預設也會包含本機 Elasticsearch 節點，以用於資料視覺化。因此，您必須為本機 Elasticsearch 安裝 Elasticsearch 外掛程式。如需詳細資訊，請參閱「安裝 Elasticsearch 安全性外掛程式」(第 76 頁)。

在 Sentinel 中使用的 Elasticsearch 和 Kibana 升級時，您必須重新部署現有 Elasticsearch 節點中所有的 Elasticsearch 安全性外掛程式。如需關於重新部署 Elasticsearch 安全性外掛程式的詳細資訊，請參閱「重新部署 Elasticsearch 安全性外掛程式」(第 79 頁)。

在 YARN 上更新 Spark 應用程式

在升級 Sentinel 期間，部分 Spark 應用程式檔案也會隨之更新。您必須透過執行以下步驟，重新提交 Spark 應用程式和這些更新檔案：

1 以Novell使用者的身分登入SSDM伺服器，並將檔案複製到安裝HDFS NameNode的Spark歷程伺服器中：

cd /etc/opt/novell/sentinel/scalablestore

scp SparkApp-*.jar avroevent-*.avsc avrorawdata-*.avsc spark.properties log4j.properties manage_spark_jobs.sh root@<*hdfs_node*>:<*destination_directory*>

其中 <*destination_directory*> 是您要放置所複製檔案的任一目錄。此外，請確定 hdfs 使用者有存取此目錄的完整權限。

2 以 root 使用者的身分登入 <*hdfs_node*> 伺服器，並將所複製檔案的擁有權變更為 hdfs 使用者：

cd <*destination_directory*>

chown hdfs SparkApp-*.jar avroevent-*.avsc avrorawdata-*.avsc spark.properties log4j.properties manage_spark_jobs.sh

指定可執行權限給 manage_spark_jobs.sh 程序檔。

3 請確定 Spark 工作已完成所有資料的處理：

移至 YARN 的 ResourceManager Web 使用者介面，並檢視每個 Sentinel Spark 應用程式。當所有資料都已從 Kafka 完成處理時，Spark Streaming 應用程式資料將會顯示輸入率降至零。

4 執行下列指令以停止資料處理：

。/manage_spark_jobs.sh stop

5 清除資料處理檢查點：

```
sudo -u hdfs hadoop fs -rm -R -skipTrash  /spark/checkpoint
```

其中 /spark/checkpoint 是檢查點目錄。

6 執行下列程序檔以重新提交 Spark 工作：

。/manage_spark_jobs.sh start

上述指令會需要點時間來完成提交程序。

7 (選擇性) 執行下列指令可確認已提交的 Spark 工作狀態：

。/manage_spark_jobs.sh status

8 繼續將事件轉遞至 Kafka，以讓 Spark 開始處理事件：

8a 在 Sentinel 主要介面上，按一下「**儲存**」>「**可擴充儲存**」>「**進階組態**」>「**Kafka**」。

8b 將下列內容設定為 false：

pause.events.tokafka

8c 按一下「**儲存**」。

啟用 Sentinel 功能

當您從 SSDM 8.0 *x.x* 進行升級時，在 Sentinel 8.1 和更新版本中新增的部分 Sentinel 功能預設為無法使用。您必須在 /etc/opt/novell/sentinel/config/ui-configuration.properties 檔案中手動啟用這些功能。

1. 以 Novell 使用者身分登入 Sentinel 伺服器。
2. 開啟 /etc/opt/novell/sentinel/config/ui-configuration.properties 檔案。
3. 將下列內容變更為 false：

```
alerts.hideUI
solutionDesigner.launcher.hideUI
correlation.hideUI
scc.configurations.solutionPacks.hideUI
people.hideUI
permission.knowledgeBase.hideUI
scc.menuBarItem.toolsMenu.hideUI
scc.toolBarItem.peopleBrowser.hideUI
integration.hideUI
```

4. 重新整理 Sentinel 瀏覽器。

在 Sentinel Scalable Data Manager 中更新儀表板和視覺化

您必須在升級 SSDM 後更新儀表板和視覺化，以套用最新版儀表板和視覺化中所包含的加強功能。

升級 SSDM時，依預設不會更新儀表板和視覺化。不過，您可以在升級後手動更新這些項目。您可以透過刪除現有儀表板和視覺化，並執行可安裝最新儀表板和視覺化的 load_kibana_data.sh 程序檔，更新儀表板和視覺化。

重要： 更新儀表板和視覺化時，您已在儀表板和視覺化中完成的自定將遺失。

若要更新儀表板和視覺化：

1. 登入 SSDM Web 介面，並移至「事件視覺化」。
2. 在「事件視覺化」中，移至「**設定**」>「**物件**」>「**儀表板**」。
3. 選取要更新的儀表板，並按一下「**刪除**」。
4. 按一下「**視覺化**」。選取要更新的視覺化，並按一下「**刪除**」。
5. 登出 SSDM Web 介面。
6. 以 novell 使用者身分登入 SSDM 伺服器。
7. 移至 /opt/novell/sentinel/bin 目錄。
8. 使用下列指令執行 load_kibana_data.sh：

   。/load_kibana_data.sh http://<ip address>:<port>> <alerts/events/misc>

   例如：

   。/load_kibana_data.sh http://127.0.0.1:9200 alerts

。/load_kibana_data.sh http://127.0.0.1:9200 events

9 登入 SSDM Web 介面，並移至「事件視覺化」以檢視更新的儀表板和視覺化。

新增 JDBC DB2 驅動程式

升級至 Sentinel 後，加入正確的 JDBC 驅動程式，並執行下列步驟為其進行資料收集和資料同步化設定：

1 在 /opt/novell/sentinel/lib 資料夾中為您的 DB2 資料庫版本複製正確的 IBM DB2 JDBC 驅動程式版本 (db2jcc-*.jar)。

2 確定為驅動程式檔案設定了必要的擁有權和許可。

3 針對資料收集設定此驅動程式。如需詳細資訊，請參閱資料庫連接器文件。

在 Sentinel 裝置中設定資料同盟屬性

升級 Sentinel 裝置後請執行下列程序，讓資料同盟在已設定兩個以上 NIC 的環境中不會顯示任何錯誤：

1 在授權要求者伺服器中，在 /etc/opt/novell/sentinel/config/configuration.properties 檔案中新增以下內容，如下所示：

sentinel.distsearch.console.ip=<授權要求者的 IP 位址之一>

2 在資料來源伺服器中，新增以下檔案內容：/etc/opt/novell/sentinel/config/configuration.properties：

sentinel.distsearch.target.ip=<資料來源的 IP 位址之一>

3 重新啟動 Sentinel：

rcsentinel restart

4 登入授權要求者伺服器並按一下「整合」。 若您想新增的資料來源已存在，請使用您在步驟 2 中指定的 IP 位址之一來刪除並再次新增。

同樣地，使用您在步驟 1 中指定的 IP 位址新增授權要求者。

註冊 Sentinel 裝置以進行更新

如果您已升級作業系統，則必須重新註冊 Sentinel 應用裝置，以接收 Sentinel 和作業系統的最新更新。您可以使用現有的註冊金鑰重新註冊，以進行更新。若要註冊應用裝置，請參閱 「登錄以進行更新」(第 99 頁)。

針對資料同步化更新外部資料庫

從 Sentinel 8.x 開始，Message (msg) 事件欄位的大小已從 4000 個字元增加至 8000 個字元，以在欄位中容納更多資訊。

如果您已在之前版本中建立資料同步化規則，將 Message (msg) 事件欄位同步化至外部資料庫，則必須依此在外部資料庫中增加適合對應欄的大小。

附註： 上述步驟僅適用於將 Sentinel 之前版本升級至 8.x 版的情況。

以多因素驗證模式下重新驗證 Sentinel

當您以 MFA 模式升級 Sentinel 伺服器時，現有的 NetFlow Collector Manager 並不會自動重新對 Sentinel 伺服器進行重新驗證。您必須執行下列步驟，以手動方式將 NetFlow Collector Manager 重新驗證至 Sentinel 伺服器。

以 MFA 模式重新驗證 Sentinel：

1. 登入至 NetFlow Collector Manager 電腦。
2. 移至 /opt/novell/sentinel/setup。
3. 執行 configure.sh 程序檔。

   系統會提示您登入 Sentinel 伺服器。
4. 指定您的 LDAP 使用者名稱和密碼。
5. 提供 Sentinel 用戶端 ID 和 Sentinel 用戶端密碼。

   若要取回 Sentinel 用戶端 ID 和 Sentinel 用戶端密碼，請前往以下 URL：

   https://Sentinel_FQDN:port/SentinelAuthServices/oauth/clients

   其中：

   - Sentinel_FQDN 是 Sentinel 伺服器的完整網域名稱。

     例如 abc.netiq.com

     其中，abc 是 Sentinel 伺服器主機名稱，而 netiq.com 是網域名稱。
   - 連接埠是 Sentinel 使用的連接埠 (通常是 8443)。

   指定 URL 使用您目前的 Sentinel 工作階段取回 Sentinel 用戶端 ID 和 Sentinel 用戶端密碼。

31 升級 Sentinel 外掛程式

Sentinel 的升級安裝不會升級外掛程式，除非特定外掛程式與 Sentinel 最新版本不相容。

新推出且已更新的 Sentinel 外掛程式 (包括解決方案套件) 會不時上傳至 Sentinel 外掛程式網站。若要取得外掛程式的最新錯誤修正、文件更新和加強，請下載並安裝外掛程式最近的版本。如需安裝外掛程式的詳細資訊，請參閱特定外掛程式的文件。

VI 從傳統儲存移轉資料

從使用傳統儲存的 Sentinel 移轉資料，可讓您有效率地運用現有 Sentinel 資料和您花費在此的時間。若要從使用傳統儲存的 Sentinel 移轉資料，來源與目標 Sentinel 伺服器的 Sentinel 版本必須相同。例如，如果您要將資料從 Sentinel 8.1 (來源) 移轉至 Sentinel 8.2 (目標)，您必須先將 Sentinel 8.1 升級至 Sentinel 8.2，然後再開始進行資料移轉程序。

本節提供將現有資料移轉至所需之資料儲存元件的相關資訊。

32 將資料移轉至可擴充儲存

您可能有單一 Sentinel 伺服器或多個 Sentinel 伺服器使用傳統儲存。您需要遵循的資料移轉程序，會根據您要如何設定和維護 Sentinel 部署而定。

表格 32-1 *適用您 Sentinel 部署的資料移轉程序*

Sentinel 部署	移轉程序
您有單一 Sentinel 伺服器，而您計劃將現有 Sentinel 伺服器升級至可擴充儲存。	您只需要在升級 Sentinel 伺服器並啟用可擴充儲存時，將事件資料和原始資料從傳統儲存移轉至可擴充儲存即可。 如需詳細資訊，請參閱第 34 章「移轉資料」(第 169 頁)。
您有使用傳統儲存的單一 Sentinel 伺服器，而您想安裝另一個 Sentinel 伺服器以使用可擴充儲存，如此一來，您可以使用 Sentinel 中的所有功能。	使用備份與還原公用程式，將資料從使用傳統儲存的 Sentinel 伺服器移轉至使用可擴充儲存的 Sentinel。 如需使用備份與還原公用程式的詳細資訊，請參閱「《Sentinel Administration Guide》」(NetIQ Sentinel 管理指南) 中的*Backing Up and Restoring Data*(備份與還原資料)。
您擁有多層級設定，而其中有多個 Sentinel 伺服器，您計劃安裝新的 Sentinel 伺服器，或使用其中一個現有伺服器來使用可擴充儲存。那麼除了移轉事件資料和原始資料外，您還需要移轉組態資料。	在多層級設定中，您可以識別具有您大部分資料的其中一個傳統 Sentinel 伺服器，然後使用備份和還原公用程式來移轉資料。 如果您需要從其餘 Sentinel 伺服器備份資料，您必須使用不同方法 (將於此節中稍後說明) 來從這些伺服器移轉組態資料、事件資料和原始資料。您也必須手動重新建立部份組態。 您無法使用備份和還原公用程式從多個伺服器移轉資料，因為進行還原時，公用程式會覆寫現有資料。例如，如果您已從伺服器 A 還原資料，然後您試圖從伺服器 B 還原資料，則此公用程式會覆寫已從伺服器 A 還原的資料。 因此，若要了解涉及的資料移轉程序，以相同順序遵循下列幾節中提供的指示： ◆ 可以移轉的資料 ◆ 移轉組態資料 ◆ 移轉資料 ◆ 移轉警示和 NetFlow 資料 ◆ 更新 Sentinel 用戶端 ◆ 輸入 ESM 組態

可以移轉的資料

您可以移轉事件資料、原始資料和部分組態資料。您必須手動重新建立無法移轉的其餘組態。

表格 32-2 *可以移轉的組態和需要重新建立的組態*

可以移轉的組態	需要重新建立的組態
◆ 關連規則 ◆ 動作 ◆ 映射 ◆ 過濾器 ◆ 威脅摘要 ◆ ESM 組態 ◆ 知識庫資料除外的警示 ◆ NetFlow	◆ 租用戶、角色、使用者和 LDAP 組態 ◆ 事件和警示路由規則 ◆ 資料和警示保留規則 ◆ 狀態畫面 ◆ 即時檢視 ◆ 身分資訊 ◆ 饋送組態 ◆ 動作和整合器外掛程式組態 ◆ 保全性組態

移轉組態資料

移轉事件資料之前，您必須先將組態資料移轉至 Sentinel 目標伺服器。您可以使用 Solution Designer 和事件來源管理 (ESM) 中的輸出和輸入選項，來備份部分組態資料。您必須手動重新建立其餘無法備份或輸出的組態資料。

- 「備份來源伺服器上的資料」(第 164 頁)
- 「還原目標伺服器上的資料」(第 165 頁)

備份來源伺服器上的資料

您必須使用 Sentinel 中的各種選項來備份必要的資料。

- 「使用解決方案套件」(第 165 頁)
- 「使用 ESM 中的輸出組態選項」(第 165 頁)

使用解決方案套件

使用 Solution Designer 備份來源伺服器上的以下組態：

表格 32-3 *組態資料*

	資料	附註
❒	關連規則	為每個 Correlation Engine 建立個別控制項，如此一來，您可以將規則分別移轉至特定的 Correlation Engine。
❒	動作	您可以只備份 JavaScript 動作，不要備份如動態清單等舊版動作，並且建立事件。
❒	事件強化	Sentinel 也會備份事件欄位的相關聯映射。因此，您無須在還原事件強化資料後重新建立相關聯映射。
❒	過濾器	備份所有自訂過濾器。
❒	新聞來源	解決方案套件僅會備份「饋送」外掛程式，而不會備份外掛程式組態。

如需關於在 Solution Designer 中備份資料的資訊，請參閱*《Sentinel 管理指南》*中的「「建立解決方案套件」」。

使用 ESM 中的輸出組態選項

使用 ESM 中的輸出組態選項來備份您的資料收集組態。如需詳細資訊，請參閱「《Sentinel 管理指南》」中的*「輸出組態」*。

還原目標伺服器上的資料

- 「從解決方案套件安裝組態資料」(第 165 頁)
- 「手動重新建立組態」(第 165 頁)

從解決方案套件安裝組態資料

使用 Solution Designer 輸入您在來源伺服器上備份的組態資料。如需詳細資訊，請參閱「《Sentinel 使用者指南》」中的*「從解決方案套件安裝內容」*。

重新命名過濾器、動作和關連規則等物件的所有重複名稱。依預設，您在目標伺服器上輸入過濾器時，所有過濾器皆為公用。手動重新指派每個過濾器的許可。

手動重新建立組態

除了從來源伺服器輸入的組態資料外，您必須手動重新建立所有其他組態。如需關於必須手動重新建立的組態詳細資訊，請參閱表格 32-2 「可以移轉的組態和需要重新建立的組態」 (第 164 頁)。

移轉事件資料和原始資料

若要移轉事件資料和原始資料，請參閱移轉資料。

移轉警示和 NetFlow 資料

您可以使用備份和還原公用程式來將警示和 NetFlow 資料從來源伺服器移轉到目標伺服器。針對警示，此公用程式會還原觸發警示的事件。但是，公用程式不會還原相關聯的關連規則和知識庫資訊。

使用以下指令來備份與還原警示和 NetFlow 資料：

```
For backing up:
./backup_util.sh -i

For restore:
./backup_util.sh -m restore -f <backup_file_path>
```

針對警示和 NetFlow 資料，您可以選擇覆寫或附加現有資料。選擇需要的選項。

雖然上述指令會備份和還原安全情報資料，但您無法使用這些資料，因為在 SSDM 中無法使用安全情報。

如需使用備份與還原公用程式的詳細資訊，請參閱「《 Sentinel Administration Guide》」(NetIQ Sentinel 管理指南) 中的*Backing Up and Restoring Data*(備份與還原資料)。

更新 Sentinel 用戶端

您必須更新所有現有的 Collector Manager、Correlation Engines 和 NetFlow Collector Manager 組態，以使得這些組態可與目標 Sentinel 伺服器通訊。如需詳細資訊，請參閱「《 Sentinel 管理指南》」中的*「更新 Sentinel 用戶端」*。

附註： 雖然您已經移轉來源伺服器上的事件資料，但您必須再次執行資料移轉程序檔，才可將可能在此資料移轉程序期間或之後收到的所有資料移轉出去。如需詳細資訊，請參閱第 34 章 「移轉資料」 (第 169 頁)。

輸入 ESM 組態

使用 ESM 使用者介面中的「輸入組態」選項，輸入您在來源伺服器上使用的資料收集組態。如需詳細資訊，請參閱「《 Sentinel 管理指南》」中的*「輸入組態」*。

33 將資料移轉至 Elasticsearch

根據預設，Sentinel 會在檔案式傳統儲存中儲存資料，並在 Sentinel 伺服器本機上為資料編製索引。當您啟用事件視覺化時，Sentinel 除了在檔案式傳統儲存中儲存資料及編製其索引以外，也會在 Elasticsearch 中執行這些作業。儀表板只會顯示在您啟用事件視覺化後處理的事件。若要檢視檔案式儲存中顯示的現有事件，您必須將資料從檔案式儲存移轉至 Elasticsearch。若要將資料移轉至 Elasticsearch，請參閱第 34 章「移轉資料」(第 169 頁)。

34 移轉資料

您可以使用 data_uploader.sh 程序檔將資料移轉至下列其中一個資料儲存元件：

- **Kafka：** 您可以將事件和原始資料移轉至 Kafka。分別為事件資料和原始資料執行程序檔。程序檔會將資料移轉至 Kafka 主題。

  您可以指定自訂作業，例如在移轉期間壓縮檔案、以批次方式傳送資料等。若要指定這些自訂項目，請建立內容檔案，並以索引鍵值的格式新增必要的內容。例如，您可以新增以下內容：

  compression.type=lz4

  batch.size=20000

  如需關於 Kafka 內容的詳細資訊，請參閱《Kafka 文件》。請設定內容與其中的值，因為程序檔不會驗證這些內容。

  附註： 請確定 Sentinel 伺服器能夠將所有 Kafka 代理程式解析為整個 Kafka 叢集的有效 IP 位址。如果 DNS 未設定為啟用此功能，請將 Kafka 代理程式主機名稱新增至 Sentinel 伺服器的 /etc/hosts 檔案中。

- **Elasticsearch：** 您只能將事件資料移轉至 Elasticsearch。在移轉資料之前，請確定您已啟用事件視覺化。如需詳細資訊，請參閱「啟用事件視覺化」(第 115 頁)。

程序檔會依據您指定的日期範圍 (開始與結束) 傳輸資料。當您執行程序檔時，程序檔會顯示您為了起始資料移轉所應指定的必要和選用參數，以及有關所需的資料儲存元件要使用之相關內容的資訊。

程序檔必須以 Novell 使用者的身分執行。因此，請確定 Novell 使用有適當的權限，可使用您指定的資料目錄和任何檔案。根據預設，程序檔會從主要儲存位置移轉資料。如果您要從次要儲存位置移轉資料，請在執行程序檔時，指定次要儲存位置的適當路徑。

若要移轉資料：

1. 以 Novell 使用者身分登入 Sentinel 伺服器。
2. 執行以下程序檔：

   /opt/novell/sentinel/bin/data_uploader.sh
3. 依照畫面上的指示，並以必要的參數再次執行程序檔。

移轉資料的保留期間與目標伺服器上設定的相同。

完成資料移轉後，程序檔會記錄狀態，如分割區已成功移轉、分割區移轉失敗和移轉的事件數等。對於其日期是昨天和今天的分割區，資料傳輸狀態將會顯示 IN_PROGRESS，表示事件可能會較慢傳入。

如果資料移轉失敗，或分割區的資料移轉狀態持續指出 IN_PROGRESS，請重新執行程序檔。當您重新執行程序檔時，程序檔會先檢查狀態檔，以了解有多少分割區已移轉，然後僅繼續移轉剩餘的分割區。程序檔會將記錄保留在 /var/opt/novell/sentinel/log/data_uploader.log 目錄中，以便進行疑難排解。

VII 部署 Sentinel 以提供高可用性

本節提供如何在主動/被動高可用性模式中安裝 Sentinel 的相關資訊，這可讓 Sentinel 在硬體或軟體故障時容錯移轉到備援叢集節點。如須在您 Sentinel 環境中執行高可用性和災難復原的詳細資訊，請聯絡 技術支援小組。

附註： 只有 Sentinel 伺服器支援高可用性 (HA) 組態。不過，Collector Manager 和 Correlation Engine 仍可與 Sentinel HA 伺服器通訊。

35 概念

高可用性代表一種設計方式，目的是維持系統實際可行的最高可用性，希望可減少造成停機時間的原因 (例如系統故障及維護)，並縮短偵測到確實發生的停機時間事件並從中復原的時間。實務上，自動化代表為提高可用性，偵測到停機時間事件並快速從中復原是必要的。

如需有關高可用性的詳細資訊，請參閱 SUSE 高可用性指南。

外部系統

Sentinel 是複雜的多層應用程式，仰賴各種服務也提供多樣的服務，並整合多個外部協力廠商系統來進行資料收集、資料共享和事件矯正。大部分高可用性解決方案允許實作者宣告必須為高可用性的服務之間的相依性，但這只適用於在叢集本身執行的服務。Sentinel 的外部系統 (例如事件來源) 必須分開設定，以依組織規定提供使用，而且也必須設定為可正確處理一段時間無法使用 Sentinel 的情況，例如容錯移轉事件。如果存取權限受到嚴格限制 (例如使用驗證工作階段來傳送和/或接收協力廠商系統和 Sentinel 之間的資料)，則必須將協力廠商系統設定為接受來自任何叢集節點的工作階段或啟始其工作階段 (根據此目的，您應透過虛擬 IP 位址設定 Sentinel)。

共享儲存

所有高可用性叢集需要某種形式的共享儲存，方便應用程式資料在原始節點發生故障時，快速移至其他叢集節點。儲存本身必須為高可用性；這通常是透過使用連接至使用光纖通道網路之叢集節點的儲存區域網路 (SAN) 技術達成。其他系統使用網路附加儲存 (NAS)、iSCSI 或允許遠端掛接共享儲存的其他技術。共享儲存的基本要求為叢集可以完整將儲存從失敗的叢集節點移至新的叢集節點。

Sentinel 有兩個基本方法可以用於共享儲存。第一個方法是找出在分享儲存上的所有元件 (應用程式二進位檔、組態和事件資料)。進行容錯移轉時，儲存會從主要節點卸載並移至備份節點；備份節點會從共享儲存載入整個應用程式和組態。第二個方法會將事件資料儲存在共享儲存上，但是應用程式二進位檔和組態會放置在每個叢集節點上。進行容錯移轉時，只有事件資料會移到備份節點。

每個方法各有其優缺點，但是第二個方法允許 Sentinel 安裝使用符合 FHS 規定的標準安裝路徑、允許驗證 RPM 封裝，也允許軟修補和重新組態以縮短停機時間。

此解決方案將向您介紹一個範例，引導您瞭解安裝到使用 iSCSI 共享儲存之叢集的程序，並找到每個叢集節點上的應用程式二進位檔和組態。

服務監控

任何高可用性環境的一個重要元素是以一致的可靠方式來監控必須為高可用性的資源以及其所依賴的任何資源。SLE HAE使用名為資源代理程式的元件來執行此監控，資源代理程式的工作是提供每個資源的狀態，再加上 (必要時) 啟動或停止該資源。

資源代理程式必須為監控的資源提供可靠的狀態，才能避免不必要的停機時間。誤報 (資源被視為故障，但事實上可自行復原) 可能在非實際必要時導致服務移轉 (和相關的停機時間)，誤判異常 (資源代理程式回報某資源運作正常，但事實上並無法運作) 可能造成無法正常使用服務。從另一方面來說，外部監控服務並不容易，例如 Web 服務連接埠可能會回應簡單的 Ping，但可能無法在發出真正的查詢時提供正確的資料。在許多情況下，自我測試功能必須內建到服務本身，以提供確實正確的評量。

此解決方案為 Sentinel 提供基本的 OCF 資源代理程式，可監控重要硬體、作業系統或 Sentinel 系統故障。此時，Sentinel 的外部監控能力是根據 IP 連接埠探測，有可能會出現誤報和誤判異常。我們計劃持續改善 Sentinel 和資源代理程式，以提高此元件的準確性。

圍籬區隔

在高可用性叢集中，重要服務會隨時受到監控，並在失敗時自動在其他節點上重新啟動。不過，若主要節點發生通訊問題，此自動化可能產生問題；在該節點上執行的服務可能看起來已失敗，但實際上仍繼續執行，並寫入資料到共享儲存。若在此時於備份節點上啟動新的服務組合，很容易就會造成資料損毀。

叢集使用合稱為圍籬區隔的各種技術來防止發生此情況，包括電腦分裂偵測器 (SBD) 和 Shoot The Other Node In The Head (STONITH)。主要是為了防止共享儲存上的資料損毀。

36 系統需求

在配置叢集資源以支援高可用性 (HA) 安裝時，請考量下列要求：

- ❒ (條件式) 針對 HA 裝置安裝，確定可以取得包含有效授權的 Sentinel HA 裝置。Sentinel HA 裝置是 ISO 裝置，包括下列套件：
  - 作業系統：SLES 12 SP3
  - SLES 高可用性延伸 (SLES HAE) 套件
  - Sentinel 軟體 (包括 HA rpm)
- ❒ (條件式) 針對傳統 HA 安裝，請確定您可取得下列項目：
  - 作業系統：SLES 11 SP4 或 SLES 12 SP1 或更新版本
  - 具有有效授權的 SLES HAE ISO 影像
  - Sentinel 安裝程式 (TAR 檔案)
- ❒ (條件式) 若您正在使用 SLES 作業系統 (內含核心版本 3.0.101 或更新版本)，您必須在電腦上手動載入監視程式驅動程式。要尋找電腦硬體的相關監視程式驅動程式，請聯絡您的硬體廠商。要載入監視程式驅動程式，請執行下列動作：
  1. 在指令提示中，執行下列指令以在目前工作階段中載入監視程式驅動程式：

     ```
     /sbin/modprobe -v --ignore-install <watchdog driver name>
     ```

  2. 在 /etc/init.d/boot.local 檔案中新增下列行，確保電腦每次開機時都會自動載入監視程式驅動程式：

     ```
     /sbin/modprobe -v --ignore-install <watchdog driver name>
     ```

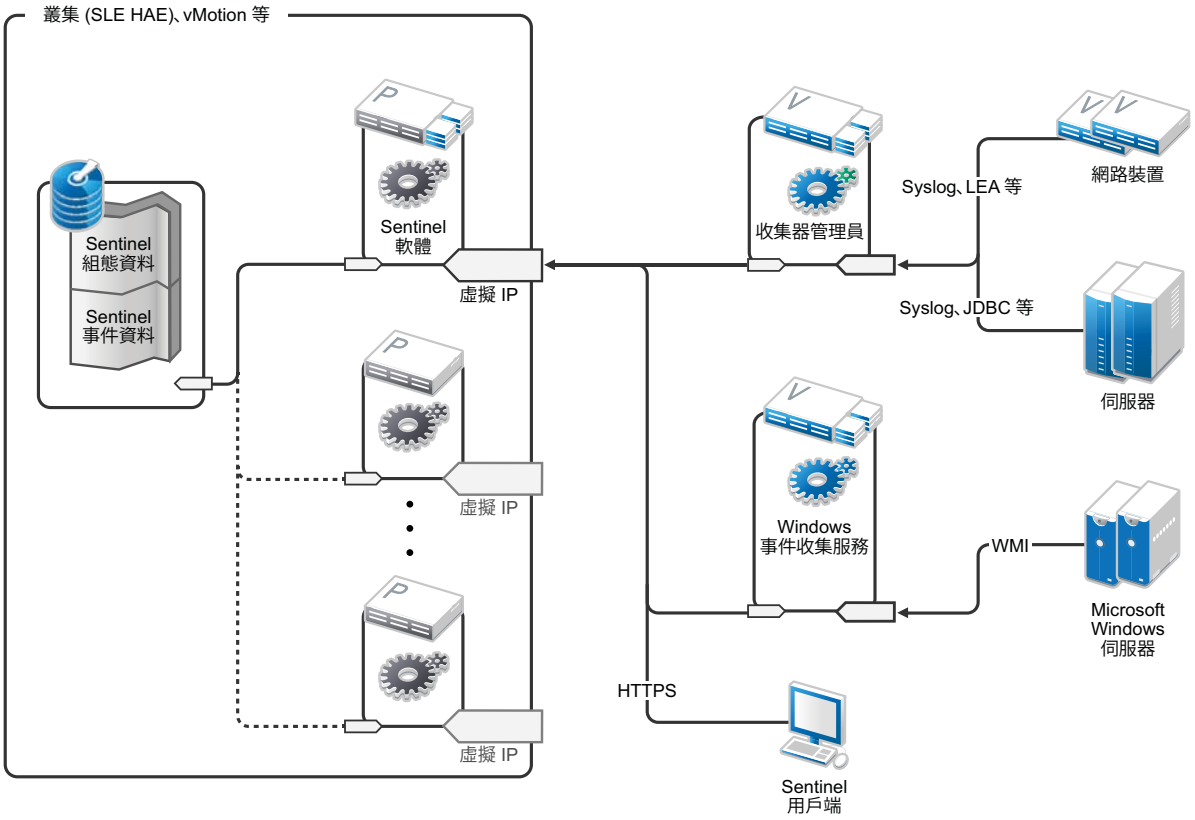
- ❒ 確保代管 Sentinel 服務的每個叢集節點符合在「第 5 章 「符合系統需求」(第 37 頁)」中指定的要求。
- ❒ 請確保 Sentinel 資料和應用程式有充分的共享儲存可以使用。
- ❒ 在進行容錯移轉時，確定您使用可在節點之間移轉的服務虛擬 IP 位址。
- ❒ 確保您的共享儲存裝置符合在「第 5 章 「符合系統需求」(第 37 頁)」中指定的效能及大小特性要求。請使用將 iSCSI 目標設定為共用儲存的標準 SLES 虛擬機器。

  若是 iSCSI，您應使用硬體支援的最大訊息傳輸單元 (MTU)。最大訊息傳輸單元有助提升儲存效能。若儲存的延遲和頻寬低於建議，Sentinel 可能發生問題。
- ❒ 確保您至少擁有兩個符合資源要求的節點，以在客戶環境中執行 Sentinel。建議使用兩個 SLES 虛擬機器。
- ❒ 請確保您建立一個讓叢集節點與共享儲存通訊的方法，例如 SAN (儲存區域網路) 的光纖通道。請使用專用 IP 位址連線至 iSCSI 目標。
- ❒ 請確定您擁有可在叢集中的節點之間移轉的虛擬 IP 位址，以做為 Sentinel 的外部 IP 位址。
- ❒ 請確保您每個叢集節點至少擁有一個用於內部叢集通訊的 IP 位址。您可以使用簡單的單點傳播 IP 位址，但在生產環境中則通常應使用多點傳播。

37 安裝和組態

本章提供在高可用性 (HA) 環境中安裝及設定 Sentinel 的步驟。

下圖代表主動/被動 HA 結構。



啟始設定

按照對 Sentinel 和本地客戶要求的各項規定來設定電腦硬體、網路硬體、儲存硬體、作業系統、使用者帳戶和其他基本系統資源。測試系統以確保運作正常、穩定。

使用下列核對清單來引導您完成啟始設定及組態。

	核對清單項目
❑	每個叢集節點的 CPU、RAM 和磁碟空間特性必須根據預期的事件發生?，符合在「第 5 章 「符合系統需求」(第 37 頁)」中定義的系統要求。
❑	儲存節點的磁碟空間和輸入/輸出特性必須根據預期的事件發生?和主要和次要儲存的資料保留政策，符合在「第 5 章 「符合系統需求」(第 37 頁)」中定義的系統要求。
❑	若您想要將作業系統防火牆設定為限制存取 Sentinel 和叢集，請參閱第 8 章 「使用的連接埠」(第 59 頁)，根據本地組態以及將傳送事件資料的來源，瞭解必須提供哪些連接埠的詳細資料。
❑	確保所有叢集節點的時間均已同步化。您可使用 NTP 或類似技術來達到此目的。
❑	◆ 此叢集需要可靠的主機名稱解析。將所有內部叢集主機名稱輸入 /etc/hosts 檔案，以在 DNS 失效時確保叢集連貫性。 ◆ 確保您並未將主機名稱指派至回送 IP 位址。 ◆ 在安裝作業系統期間，設定主機名稱及網域名稱時，取消選取「**指定主機名稱為回送 IP**」。

您可以使用下列組態：

- (條件式) 針對傳統 HA 安裝：
  - 兩部執行 SLES 11 SP4 或 SLES 12 SP1 或更新版本的叢集節點 VM。
  - (條件式) 若您需要 GUI 組態，您可安裝 X Windows。將開機程序檔設定為在缺少 X 的情況下啟動 (runlevel 3)，以便您僅在需要時啟動它們。
- (條件式) 針對 HA 裝置安裝：兩部 HA ISO 裝置式叢集節點虛擬機器。如需安裝 HA ISO 裝置的詳細資訊，請參閱「安裝 Sentinel」(第 95 頁)。
- 節點將會有一個用於外部存取的 NIC，以及一個用於 iSCSI 通訊的 NIC。
- 使用允許透過 SSH 或類似功能進行遠端存取的 IP 位址設定外部 NIC。針對此範例，我們將使用 172.16.0.1 (node01) 和 172.16.0.2 (node02)。
- 每個節點應有足夠的磁碟提供作業系統、Sentinel 二進位檔和組態資料、叢集軟體、暫存空間等使用。請參閱 SLES 和 SLES HAE 系統要求，以及 Sentinel 應用程式要求。
- 一部執行 SLES 11 SP4 或 SLES 12 SP1 或更新版本的虛擬機器，其使用 iSCSI Target 來設定共享儲存
  - (條件式) 若您需要 GUI 組態，您可安裝 X Windows。將開機程序檔設定為在缺少 X 的情況下啟動 (runlevel 3)，以便您僅在需要時啟動它們。
  - 系統將會有兩個 NIC：一個用於外部存取，一個用於 iSCSI 通訊。
  - 使用允許透過 SSH 或類似功能進行遠端存取的 IP 位址設定外部 NIC。例如：172.16.0.3 (storage03)。
  - 系統應有足夠的空間提供作業系統、暫存空間、可放置 Sentinel 資料共享儲存的大磁碟區以及提供 SBD 分割區使用的小空間。請參閱 SLES 系統要求和 Sentinel 事件資料儲存要求。

附註： 在生產叢集中，您可以在個別的 NIC (可能有多個，以供備援) 上使用內部非路由式 IP 位址，以進行內部叢集通訊。

共享儲存設定

設定您的共享儲存，並確定您可在每個叢集節點上進行掛接。若您使用 FibreChannel 以及 SAN，您可能必須提供實體連線以及額外組態。Sentinel 使用此共享儲存來儲存資料庫及事件資料。確保共享儲存根據預期事件速率和資料保留規則來適當設定大小。

請考量下列共享儲存設定範例：

一般實作可能透過光纖通道使用附加到所有叢集節點的快速 SAN (儲存區域網路)，包含可儲存本地事件資料的大型 RAID 陣列。個別的 NAS 或 iSCSI 節點可能會用於速度較慢的次要儲存。只要叢集節點可以將主要儲存掛接為正常區塊裝置，解決方案就可以進行使用。次要儲存也可以掛接為區塊裝置，也可以是 NFS 或 CIFS 磁碟區。

附註： 請設定您的共用儲存，並測試是否可將其掛接在每個叢集節點上。不過，叢集組態將處理實際的儲存掛接。

請執行下列程序以建立 SLES 虛擬機器代管的 iSCSI 目標：

1. 連線至 storage03 (您在啟始設定期間建立的虛擬機器)，並啟動主控台工作階段。
2. 執行下列指令為 Sentinel 主要儲存建立任何所需大小的空白檔案：

   dd if=/dev/zero of=/localdata count=<*檔案大小*> bs=<*位元大小*>

   例如，執行下列指令可建立充滿從 /dev/zero 虛擬裝置複製之 0 的 20 GB 檔案：

   dd if=/dev/zero of=/localdata count=20480000 bs=1024
3. 重複步驟 1 和 2 以相同方式為次要儲存建立檔案。

   例如，針對次要儲存執行下列指令：

   dd if=/dev/zero of=/networkdata count=20480000 bs=1024

附註： 在此範例中，您建立了兩個大小和效能特性均相同的檔案來代表兩個磁碟。針對生產部署，您可在快速 SAN (儲存區域網路) 上建立主要儲存，並將次要儲存放在較慢的 iSCSI、NFS 或 CIFS 磁碟區上。

執行下列章節提供的步驟以設定 iSCSI 目標和啟動器裝置：

- 「設定 iSCSI 目標」(第 179 頁)
- 「設定 iSCSI 啟動器」(第 181 頁)

設定 iSCSI 目標

執行下列程序以設定 localdata 和 networkdata 檔案做為 iSCSI 目標。

如需有關設定 iSCSI 目標的詳細資訊，請參閱 SUSE 文件中的「透過 YaST 建立 iSCSI 目標」。

1. 從指令行執行 YaST (或可依偏好使用圖形使用者介面)：/sbin/yast
2. 選取「**網路裝置**」>「**網路設定**」。
3. 確認已選取「**綜覽**」索引標籤。
4. 選取顯示清單的第二個 NIC，然後使用定位鍵往前到「編輯」，然後按下 Enter 鍵。
5. 在「**位址**」索引標籤上，指定靜態 IP 位址 10.0.0.3。這將成為內部 iSCSI 通訊 IP 位址。

6 按一下「下一步」，然後按一下「確定」。

7 (條件式) 在主要畫面上：

- 如果您正在使用 SLES 11 SP4，選取「網路服務」>「iSCSI 目標」。
- 如果您正在使用 SLES 12 SP1 或更新版本，選取「網路服務」>「iSCSI LIO 目標」。

附註： 如果您找不到此選項，請移至「軟體」>「軟體管理」>「iSCSI LIO 伺服器」，並安裝 iSCSI LIO 套件。

---

8 (條件式) 如果顯示提示，請安裝所需軟體：

- 如果是 SLES 11 SP4：iscsitarget RPM
- 如果是 SLES 12 SP1 或更新版本：iscsiliotarget RPM

9 (條件式) 如果您正在使用 SLES 12 SP1 或更新版本，請針對叢集中的所有節點執行下列步驟：

9a 執行下列指令以開啟包含 iSCSI 啟動器名稱的檔案：

cat /etc/iscsi/initiatorname.iscsi

9b 記下將用於設定 iSCSI 啟動器的啟動器名稱：

例如：

InitiatorName=iqn.1996-04.de.suse:01:441d6988994

設定 iSCSI 目標用戶端設定時，將使用這些啟動器名稱。

10 按一下「服務」，選取「開機時」選項，以確定服務會在作業系統開機時啟動。

11 選取「全域」索引標籤，取消選取「無驗證」以啟用驗證，然後指定內送和外送驗證的必要證書。

系統預設會啟用「無驗證」選項。不過，您應啟用驗證以確保組態的安全性。

12 按一下「目標」，然後按一下「新增」以加入新目標。

iSCSI 目標將會自動產生一個 ID，然後提出可用 LUN (磁碟機) 的空白清單。

13 按一下「新增」以加入新的 LUN。

14 將 LUN 數目設為 0，然後瀏覽「路徑」對話方塊 (在 Type=fileio 底下)，再選取您建立的 /localdata 檔案。若您有專用的儲存磁碟，請指定一個區塊裝置，例如 /dev/sdc。

15 重複步驟 13 和 14，並在此時新增 LUN 1 和選取 /networkdata。

16 (條件式) 如果您正在使用 SLES 11 SP4，請執行下列步驟：

16a 保留其他選項的預設值，按一下「確定」，然後按「下一步」。

16b (條件式) 如果您已在步驟 11 中啟用驗證，請提供驗證身分證明。

選取用戶端，選取「Edit Auth」(編輯驗證)>「Incoming Authentication」(內送驗證)，並指定使用者名稱和密碼。

17 (條件式) 如果您正在使用 SLES 12 SP1 或更新版本，請執行下列步驟：

17a 保留其他選項的預設值，並按「下一步」。

17b 按一下「新增」。當系統提示用戶端名稱時，請指定您在步驟 9 中複製的啟動器名稱。透過指定啟動器名稱，重複此步驟以新增所有用戶端名稱。

「用戶端清單」中將顯示用戶端名稱清單。

17c (條件式) 如果您已在步驟 11 中啟用驗證，請提供驗證身分證明。

選取用戶端，選取「編輯驗證」>「內送驗證」，並指定使用者名稱和密碼。請針對所有用戶端重複此步驟。

18 再按一下「下一步」選取預設驗證選項，然後按一下「完成」以結束組態。如果系統提示重新啟動 iSCSI，請按一下「接受」。

19 結束 YaST。

附註： 此程序公開在 IP 位址 10.0.0.3 的伺服器上的兩個 iSCSI 目標。請在每個叢集節點確保該伺服器能夠掛接本機資料共享儲存裝置。

設定 iSCSI 啟動器

請執行下列程序以格式化 iSCSI 啟動器裝置。

如需有關設定 iSCSI 啟動器的詳細資訊，請參閱 SUSE 文件中的「設定 iSCSI 啟動器」。

1 連接到其中一個叢集節點 (node01)，然後啟動 YaST。

2 選取「**網路裝置**」>「**網路設定**」。

3 確認已選取「**綜覽**」索引標籤。

4 選取顯示清單的第二個 NIC，然後使用定位鍵往前到「編輯」，然後按下 Enter 鍵。

5 按一下「**位址**」，指定靜態 IP 位址 10.0.0.1。這將成為內部 iSCSI 通訊 IP 位址。

6 選取「**下一步**」，然後按一下「**確定**」。

7 按一下「**網路服務**」>「**iSCSI 啟動器**」。

8 如果顯示提示，請安裝需求的軟體 (iscsiclient RPM)。

9 按一下「**服務**」，選取「**開機時**」選項，以確定 iSCSI 服務會在開機時啟動。

10 按一下「**已探查目標**」，然後選取「**探查**」。

11 指定 iSCSI 目標 IP 位址 (10.0.0.3)。

(條件式) 如果您已在「設定 iSCSI 目標」(第 179 頁)的步驟 11 中啟用驗證，請取消選取「**無驗證**」。在「**外送驗證**」欄位中，輸入您在 iSCSI 目標組態期間設定的使用者名稱和密碼。

按**下一步**。

12 選取包含 IP 位址 10.0.0.3 的已探查 iSCSI 目標，然後選取「**登入**」。

13 請執行以下步驟：

13a 在「**啟動**」下拉式功能表中，切換至「自動」。

13b (條件式) 如果您已啟用驗證，請取消選取「**無驗證**」。

「**外送驗證**」區段中應該會顯示您已在步驟 11 中指定的使用者名稱和密碼。如果未顯示這些身分證明，請在此區段中輸入該身分證明。

13c 按**下一步**。

14 切換到「**連接的目標**」索引標籤，以確定我們已連接到目標。

15 結束組態。如此一來 iSCSI 目標應可掛接到叢集節點上，成為區塊裝置。

16 在 YaST 主功能表，選取「**系統**」>「**分割器**」。

17 在「系統檢視」中，您應該會在清單中看到下列類型的新硬碟 (例如 /dev/sdb 和 /dev/sdc)：

- 在 SLES 11 SP4 中：IET-VIRTUAL-DISK
- 在 SLES 12 SP1 或更新版本中：LIO-ORG-FILEIO

使用定位鍵移至清單中的第一個硬碟 (此應為主要儲存)，選取該硬碟，然後按 Enter 鍵。

18 選取「新增」以加入新的分割區到空白磁碟。將磁碟格式化為 主要分割區，但是不要將它掛接。請確定已選取「請勿掛接分割區」選項。

19 檢閱將要進行的變更後，請選取「下一步」，然後選取「完成」。

格式化的磁碟 (例如 /dev/sdb1) 現在應該已準備就緒。此程序的下列步驟中將其稱為 /dev/<SHARED1>。

20 再次移至「分割器」，並針對 /dev/sdc 或對應到次要儲存的任一區塊裝置，重複分割/格式化程序 (步驟 16-19)。這應可產生一個 /dev/sdc1 分割區或類似的格式化磁碟 (參照以下 /dev/<NETWORK1>)。

21 結束 YaST。

22 (條件式) 如果您正在執行傳統 HA 安裝，請建立掛接點並測試掛接本地分割區 (確切的裝置名稱可能會依特定實作而異)，如下所示：

```
# mkdir /var/opt/novell
# mount /dev/<SHARED1> /var/opt/novell
```

您應可在新分割區上建立檔案，並可在分割區任何掛接位置查看檔案。

23 (條件式) 若您執行的是傳統 HA 安裝，要卸載：

```
# umount /var/opt/novell
```

24 (條件式) 針對 HA 裝置安裝，請重複步驟 1-15 來確保每個叢集節點都可掛接本機共享儲存。在步驟 5 中使用不同的 IP 位址取代每個叢集節點的節點 IP 位址。

25 (條件式) 針對傳統 HA 裝置安裝，請重複步驟 1-15、22 和 23 來確保每個叢集節點都可掛接本機共享儲存。在步驟 6 中使用不同的 IP 位址取代每個叢集節點的節點 IP 位址。

Sentinel 安裝

安裝 Sentinel 的選項有兩種：將 Sentinel 每個部分安裝到共享儲存上 (使用 --location 選項將 Sentinel 安裝重改方向到您掛接共享儲存的位置) 或只將變數應用程式資料安裝於共享儲存。

將 Sentinel 安裝至每個可裝載 Sentinel 的叢集節點。在您初次安裝 Sentinel 後，您必須執行完整安裝，包括應用程式二進位檔案、組態以及所有資料儲存。針對在其他叢集節點上的後續安裝，您僅須安裝應用程式。當您掛接共享儲存後，Sentinel 資料即可供使用。

首次節點安裝

- 「傳統高可用性安裝」(第 182 頁)
- 「Sentinel HA 裝置安裝」(第 183 頁)

傳統高可用性安裝

1 連接到其中一個叢集節點 (node01) 並開啟主控台視窗。

2 下載 Sentinel 安裝程式 (tar.gz 檔案)，並將它儲存在叢集節點的 /tmp 中。

3 執行以下步驟以開始安裝：

3a 執行以下指令：

mount /dev/<SHARED1> /var/opt/novell

cd /tmp

tar -xvzf sentinel_server*.tar.gz

cd sentinel_server*

。/install-sentinel --record-unattended=/tmp/install.props

3b 系統提示選取組態方法時，指定 2 以選取自定組態。

4 執行安裝程序，適當地設定產品。

5 啟動 Sentinel 並測試基本功能。您可以使用標準外部叢集節點 IP 位址存取產品。

6 將 Sentinel 關機並使用下列指令卸下共享儲存：

```
rcsentinel stop
```

```
umount /var/opt/novell
```

此步驟會移除自動啟動程序檔，方便叢集管理產品。

```
cd /
```

```
insserv -r sentinel
```

Sentinel HA 裝置安裝

Sentinel HA 裝置包括已安裝和已設定的 Sentinel 軟體。要設定 HA 的 Sentinel 軟體，請執行下列步驟：

1 連接到其中一個叢集節點 (node01) 並開啟主控台視窗。

2 導覽至以下目錄：

```
cd /opt/novell/sentinel/setup
```

3 記錄組態：

3a 執行下列指令：

```
./configure.sh --record-unattended=/tmp/install.props --no-start
```

這個步驟記錄在 install.props 檔案中的組態，使用 install-resources.sh 程序檔設定叢集資源時需要用到。

3b 系統提示選取組態方法時，指定 2 以選取自定組態。

3c 系統提示輸入密碼時，請指定 2 以輸入新密碼。

若您指定 1，install.props 檔案不會儲存密碼。

4 使用下列指令將 Sentinel 關機：

```
rcsentinel stop
```

此步驟會移除自動啟動程序檔，方便叢集管理產品。

```
insserv -r sentinel
```

5 使用下列指令將 Sentinel 資料夾移至共享儲存。此移動可讓節點透過共享儲存利用 Sentinel 資料夾。

```
mkdir -p /tmp/new
```

```
mount /dev/<SHARED1> /tmp/new
```

```
mv /var/opt/novell/* /tmp/new
```

```
umount /tmp/new/
```

6 使用下列指令驗證將 Sentinel 資料夾移動至共享儲存：

```
mount /dev/<SHARED1>  /var/opt/novell/
umount /var/opt/novell/
```

後續節點安裝

- 「傳統高可用性安裝」(第 184 頁)
- 「Sentinel HA 裝置安裝」(第 184 頁)

重複在其他節點上安裝：

啟始的 Sentinel 安裝程式會建立一個使用者帳戶，以供產品使用，該產品會在安裝當時使用下一個可用的使用者 ID。採用無人管理安裝模式的後續安裝將嘗試使用相同的使用者 ID 來建立帳戶，但確實可能發生衝突 (若叢集節點在安裝當時並不完全相同)。強烈建議您採取以下其中一個動作：

- 同步化所有叢集節點的使用者帳戶資料庫 (手動透過 LDAP 或類似功能)，確定在進行後續安裝已完成同步化。此時，安裝程式將偵測到使用者帳戶的存在，並使用現有帳戶。
- 注意後續無人管理安裝的輸出，若無法使用相同的使用者 ID 來建立使用者帳戶，系統將會發出警告。

傳統高可用性安裝

1 連接到每個額外的叢集節點 (node02) 並開啟主控台視窗。

2 執行以下指令：

```
cd /tmp
scp root@node01:/tmp/sentinel_server*.tar.gz .
scp root@node01:/tmp/install.props .
tar -xvzf sentinel_server*.tar.gz
cd sentinel_server*
./install-sentinel --no-start --cluster-node --unattended=/tmp/install.props
insserv -r sentinel
```

Sentinel HA 裝置安裝

1 連接到每個額外的叢集節點 (node02) 並開啟主控台視窗。

2 執行下列指令：

```
insserv -r sentinel
```

3 停止 Sentinel 服務。

```
rcsentinel stop
```

4 移除 Sentinel 目錄。

```
rm -rf /var/opt/novell/*
```

在此程序結束時，Sentinel 應會安裝在所有節點上，但能夠正常運作的可能只有第一個節點，直到各個金鑰都已同步化為止，這可在我們設定叢集資源時完成。

叢集安裝

您必須僅針對高可用性 (HA) 安裝來安裝叢集軟體。Sentinel HA 裝置包括叢集軟體，不需要手動安裝。

請使用下列程序來設定 SLES 高可用性延伸功能，包括 Sentinel 特定的資源代理程式重疊：

1. 在每個節點上安裝叢集軟體。
2. 使用叢集管理員註冊每個節點。
3. 驗證每個節點都顯示在叢集管理主控台中。

   附註： Sentinel 的 OCF 資源代理程式是一個簡單的外圍程序程序檔，可執行各種檢查來驗證 Sentinel 是否正常運作。若您不使用 OCF 資源代理程式來監控 Sentinel，您必須為本地叢集環境開發類似的監控解決方案。若要開發您專屬的資源代理程式，請檢閱現有的資源代理程式，它儲存於 Sentinel 下載套件中的 Sentinelha.rpm 檔案內。

   ---

4. 根據SLEHAE文件安裝核心SLEHAE軟體。如需安裝SLES附加產品的詳細資訊，請參閱《部署指南》。
5. 在所有叢集節點上重複步驟 4。附加產品將安裝核心叢集管理和通訊軟體，以及用來監控叢集資源的許多資源代理程式。
6. 安裝額外 RPM 來提供額外的 Sentinel 特定叢集資源代理程式。高可用性 RPM 可在儲存於預設 Sentinel 下載中的 novell-Sentinelha-<*Sentinel_version*>*.rpm 檔案中找到，您必須將其解除封裝才能安裝產品。
7. 在每個叢集節點上，將 novell-Sentinelha-<*Sentinel_version*>*.rpm 檔案複製到 /tmp 目錄，然後執行下列指令：

```
cd /tmp

rpm -i novell-Sentinelha-<Sentinel_version>*.rpm
```

磁簇組態

您必須設定叢集軟體才能將每個叢集節點註冊為叢集的成員。做為此組態的一部份，您也可以設定圍籬區隔以及關閉其他節點 (STONITH) 資源以確保叢集一致性。

重要： 此區段的程序使用rcopenais和openais指令，配合SLES 11 SP4才能使用。若是SLES 12 SP2和更新版本，請使用 systemctl pacemaker.service 指令。

例如，針對 /etc/rc.d/openais start 指令，請使用 systemctl start pacemaker.service 指令。

請為叢集組態使用下列程序：

針對此解決方案，您必須使用私人 IP 位址進行內部叢集通訊，並使用單點傳播來降低向網路管理員申請多路廣播位址的要求。您必須使用在代管共享儲存的相同SLES虛擬機器上設定的iSCSI目標，以做為用於圍籬區隔用途的電腦分裂偵測 (SBD) 裝置。

SBD 安裝程式

1 連接至 storage03 並啟動主控台工作階段。執行下列指示以建立任何所需大小的空白檔案：

dd if=/dev/zero of=/sbd count=<*檔案大小*> bs=<*位元大小*>

例如，執行下列指令可建立充滿從 /dev/zero 虛擬裝置複製之 0 的 1 MB 檔案：

```
dd if=/dev/zero of=/sbd count=1024 bs=1024
```

2 從指令行或圖形使用者介面執行 YaST：/sbin/yast

3 選取「**網路服務**」>「**iSCSI 目標**」。

4 按一下「**目標**」，然後選取現有的目標。

5 選取「**編輯**」。UI 將顯示可用 LUN (磁碟機) 的清單。

6 選取「**新增**」以加入新的 LUN。

7 將 LUN 數目設為 2。瀏覽「**路徑**」對話方塊並選取您建立的 /sbd 檔案。

8 保留其他選項的預設值，然後依序選取「**確定**」、「**下一步**」，再按一下「**下一步**」以選取預設驗證選項。

9 按一下「**完成**」以結束組態。視需要重新啟動服務。結束 YaST。

附註： 以下步驟要求每個叢集節點都能解析所有其他叢集節點的主機名稱 (若無法解析，檔案同步服務 csync2 將失敗)。如果尚未設定或無法使用 DNS，請將每個主機的項目新增到列出每個 IP 位址和其主機名稱的 /etc/hosts 檔案 (如主機名稱指令所回報)。此外，請確保您並未將主機名稱指派至回送 IP 位址。

執行以下步驟以公開在 IP 位址 10.0.0.3 的伺服器上 SBD 服務的 iSCSI 目標 (storage03)。

節點組態

連接到叢集節點 (node01) 並開啟主控台視窗：

1 執行 YaST。

2 開啟「**網路服務**」>「**iSCSI 啟動器**」。

3 選取「**連接的目標**」，然後選取您在以上設定的 iSCSI 目標。

4 選取「**登出**」選項並登出該目標。

5 切換到「**已探查目標**」索引標籤，選取「**目標**」，並再次登入，以重新整理裝置的清單 (保留「**自動**」啟動選項並取消選取「**無驗證**」)。

6 選取「**確定**」以結束 iSCSI 啟動器 工具。

7 開啟「**系統**」>「**分割器**」，並將SBD裝置辨識別為1MBIET-VIRTUAL-DISK。它將列示為**/dev/sdd** 或類似名稱，請記下是哪個。

8 結束 YaST。

9 執行指令 ls -l /dev/disk/by-id/ 並記下連接到您在以上找到的裝置名稱的裝置 ID。

10 (條件式) 執行下列其中一個指令：

- 如果您正在使用 SLES 11 SP4：

  sleha-init

- 如果您正在使用 SLES 12 SP1 或更新版本：

  ha-cluster-init

11 當系統提示要繫結的網路位址時，請指定外部 NIC IP 位址 (172.16.0.1)。

12 接受預設多點廣播位址和連接埠。我們會在稍後置換。

13 輸入 y 以啟用 SBD，然後指定 /dev/disk/by-id/<裝置 id>，其中 <裝置 id> 是您在上述步驟中找到的 ID (您可以使用定位鍵自動完成路徑)。

14 (條件式) 在出現下列提示時，輸入 N：

```
Do you wish to configure an administration IP? [y/N]
```

若要設定管理 IP 位址，請在「資源組態」(第 189 頁)期間提供虛擬 IP 位址。

15 完成精靈並確定未回報任何錯誤。

16 啟動 YaST。

17 選取「**高可用性**」>「**叢集**」(或在某些系統上只要「叢集」)。

18 在左側方塊中，確定已選取「**通訊通道**」。

19 使用定位鍵移至組態的第一行，然後將「**udp**」選項變更成「**udpu**」(這會停用多點傳播並選取單點傳播)。

20 選取以「**新增成員位址**」，指定此節點 (172.16.0.1)，然後重複並新增其他叢集節點：172.16.0.2。

21 選取「**完成**」以完成組態。

22 結束 YaST。

23 執行指令 /etc/rc.d/openais 重新啟動，以使用新的同步協定重新啟動叢集服務。

連接到每個額外的叢集節點 (node02) 並開啟主控台視窗：

1 執行 YaST。

2 開啟「**網路服務**」>「**iSCSI 啟動器**」。

3 選取「**連接的目標**」，然後選取您在以上設定的 iSCSI 目標。

4 選取「**登出**」選項並登出該目標。

5 切換到「**已探查目標**」索引標籤，選取「**目標**」，並再次登入，以重新整理裝置的清單 (保留「**自動**」啟動選項並取消選取「**無驗證**」)。

6 選取「**確定**」以結束 iSCSI 啟動器 工具。

7 (條件式) 執行下列其中一個指令：

- 如果您正在使用 SLES 11 SP4：

  sleha-join

- 如果您正在使用 SLES 12 SP1 或更新版本：

  ha-cluster-join

8 輸入第一個叢集節點的 IP 位址。

(條件式) 若叢集未正確啟動，請執行下列步驟：

1 執行指令 crm status，以確認節點是否已聯結。如果節點未聯結，請重新啟動叢集中的所有節點。

2 將 /etc/corosync/corosync.conf 檔案從 node01 手動複製到 node02，或針對 node01 執行 csync2 -x -v，或透過 YaST 針對 node02 手動設定叢集。

3 (條件式) 如果您在步驟 1 中執行的 csync2 -x -v 指令無法同步化所有檔案，請執行下列程序：

3a 清除所有節點上 /var/lib/csync2 目錄中的 csync2 資料庫。

3b 更新所有節點上的 csync2 資料庫以符合檔案系統，但不將任何項目標示為需要同步化至其他伺服器：

csync2 -clr /

3c 在主動節點上，執行下列作業：

3c1 找出主動節點與被動節點之間的所有差異，並將這些差異標示為要同步化：

csync2 -TUXI

3c2 重設資料庫，以強制主動節點覆寫任何衝突：

csync2 -fr /

3c3 啟動對所有其他節點的同步化：

csync2 -xr /

3d 在所有節點上，確認所有檔案均已同步化：

csync2 -T

此指令只會列出未同步化的檔案。

4 針對 node02 執行下列指令：

SLES 11 SP4：

/etc/rc.d/openais start

SLES 12 SP1 或更新版本：

systemctl start pacemaker.service

(條件式) 若 xinetd 服務未正確新增新的 csync2 服務，則程序檔將不會正確執行。xinetd 為必要服務，以便其他節點往下同步叢集組態檔案到此節點。若您看到 csync2 run failed 等錯誤，就可能發生了此問題。

若要解決此問題，請執行 kill -HUP `cat /var/run/xinetd.init.pid 指令，然後重新執行 sleha-join 程序檔。

5 在每個叢集節點上執行crm_mon以驗證叢集正常執行。您也可以使用「hawk」這個Web主控台來驗證叢集。預設登入名稱為 hacluster，密碼則為 linux。

(條件式) 根據您的環境而定，請執行下列任務來修改額外參數：

1 為確保您雙節點叢集中的單一節點故障時不會意外停止整個叢集，請將全域叢集選項 no-quorum-policy 設定為 ignore：

crm configure property no-quorum-policy=ignore

附註： 若您的叢集包含兩個以上的節點，請勿設定此選項。

---

2 為確保資源管理員允許資源原地執行並移動，請將全域叢集選項 default-resource-stickiness 設定為 1：

crm configure property default-resource-stickiness=1。

資源組態

SLE HAE 預設提供資源代理程式。若您不想使用 SLE HAE，您必須使用替代技術監控這些額外資源：

- 檔案系統資源，對應到該軟體使用的共享儲存。
- IP 位址資源，對應到可用來存取服務的虛擬 IP 位址。
- 儲存組態和事件中繼資料的 PostgreSQL 資料庫軟體。

請為資源組態使用下列程序：

crm 程序檔可協助您進行叢集設定。此程序檔會從安裝 Sentinel 時產生的無人管理的安裝程式檔案擷取相關的組態變更。若您未產生此安裝程式檔案，或您想要變更資源的組態，您可以依此使用下列程序來編輯程序檔。

1 連接至您安裝 Sentinel 的原始節點。

附註： 這必須是您在其上執行完整 Sentinel 安裝的節點.

2 編輯程序檔以讓它如下所示，其中 <SHARED1> 是您先前建立的共用磁碟區：

```
mount /dev/<SHARED1> /var/opt/novell

cd /usr/lib/ocf/resource.d/novell

./install-resources.sh
```

3 (條件式) 您可能會遇到叢集中出現新資源的問題。如果您遇到此問題，請在 node02 上執行下列指令：

SLES 11 SP4：

/etc/rc.d/openais start

SLES 12 SP1：

systemctl start pacemaker.service

4 install-resources.sh 程序檔將提示您輸入幾個值，也就是您想要其他人用來存取 Sentinel 的虛擬 IP 位址，以及共享儲存的裝置名稱，然後將自動建立要求的叢集資源。請注意，程序檔要求已先掛接共享磁碟區，並要求在安裝 Sentinel 期間建立的無人管理的安裝檔案必須存在 (/tmp/install.props)。您只需要在第一個已安裝的節點上執行此程序檔；所有相關組態檔案將會自動同步到其他節點。

5 若您的環境與此 建議的解決方案不同，您可以編輯 resources.cli 檔案 (在相同目錄中)，然後修改其中的原始定義。例如，建議解決方案使用簡易的檔案系統資源；您可能想要使用能支援叢集 cLVM 的資源。

6 執行外圍程序的程序檔之後，您可以發出 crm status 指令，輸出應如下所示：

```
crm status
```

```
Last updated: Thu Jul 26 16:34:34 2012
Last change: Thu Jul 26 16:28:52 2012 by hacluster via crmd on node01
Stack: openais
Current DC: node01 - partition with quorum
Version: 1.1.6-b988976485d15cb702c9307df55512d323831a5e
2 Nodes configured, 2 expected votes
5 Resources configured.
```

```
Online: [ node01, node02 ]
stonith-sbd    (stonith:external/sbd):    Started node01
 Resource Group: sentinelgrp
     sentinelip    (ocf::heartbeat:IPaddr2):    Started node01
     sentinelfs    (ocf::heartbeat:Filesystem):    Started node01
     sentineldb    (ocf::novell:pgsql):    Started node01
     sentinelserver    (ocf::novell:sentinel):    Started node01
```

7 此時，應在叢集中設定相關的 Sentinel 資源。例如，透過執行 crm 狀態，您可以在叢集管理工具中查看其設定和群組方式。

次要儲存組態

執行下列步驟以設定次要儲存，以便 Sentinel 將事件分割區移轉到較不耗費資源的儲存：

附註： 此程序為選擇性，而次要儲存不必像您設定系統其他部分那樣必須為高可用性。您可使用任何目錄，無論是否從 SAN、NFS 或 CIFS 磁碟區掛接。

---

1 在 Sentinel 主要介面的頂端功能表列中，按一下「**儲存**」。

2 選取「**組態**」。

3 在未設定的次要儲存下選取一個選項按鈕

請使用簡易 iSCSI 目標作為網路共用儲存位置，使用的組態與主要儲存大致相同。在您的線上環境中，您的儲存科技可能會有所不同。

使用以下程序設定 Sentinel 所使用的次要儲存：

附註： 就 iSCSI 目標而言，目標將會掛接為次要儲存的目錄。您必須使用類似設定主要儲存檔案系統的方式，將掛接設定為檔案系統資源。由於沒有其他可能的變化，因此這不會自動設定為資源安裝程序檔的一部份。

---

1 檢閱上述步驟以判斷建立做為次要儲存使用的分割區(/dev/<NETWORK1>，或像是/dev/sdc1)。若有需要，請建立一個可掛接分割區的空白目錄 (例如 /var/opt/netdata)。

2 將網路檔案系統設定為叢集資源：使用 Sentinel 主要介面或執行指令：

```
crm configure primitive sentinelnetfs ocf:heartbeat:Filesystem params device="/dev/<NETWORK1>"
directory="<PATH>" fstype="ext3" op monitor interval=60s
```

其中/dev/<NETWORK1>是在上述「共享儲存設定」區段中建立的分割區，<PATH>是可掛接的任何本地目錄。

3 將新資源加進受管理資源的群組：

```
crm resource stop sentinelgrp
crm configure delete sentinelgrp
crm configure group sentinelgrp sentinelip sentinelfs sentinelnetfs sentineldb sentinelserver
crm resource start sentinelgrp
```

4 您可以連接到目前代理資源的節點 (使用 crm status 或 Hawk)，並確定次要儲存已正確掛接 (使用 mount 指令)。

5 登入 Sentinel 主要介面。

6 選取「**儲存**」，然後選取「**組態**」，再選取未設定的「次要儲存」底下的「**SAN (本地掛接)**」。

7 輸入次要儲存掛接的路徑位置，例如 /var/opt/netdata。

請使用必要資源的簡易版，例如簡易的檔案系統資源代理程式。必要時，您可以選擇使用更多複雜的叢集資源，例如 cLVM (檔案系統的邏輯磁碟區版本)。

38 設定 Sentinel HA 為 SSDM

本章節會提供設定 Sentinel HA 安裝為 SSDM的訊息。這些指示同時適用於傳統安裝和裝置安裝。

如要設定 Sentinel HA 安裝為 SSDM：

1. 安裝並設定 Sentinel 可調整儲存。如需詳細資訊，請參閱第 13 章 「安裝和設定可擴充儲存」 (第 81 頁)。
2. 啟用在主動節點上的可調整儲存。如需詳細資訊，請參閱「《 Sentinel 管理指南》」中的*「在後續安裝工作中啟用可擴充儲存」*。
3. 在主動節點上執行以下命令：

   csync2 -x -v

   此步驟會將 SSDM 組態同步至所有被動節點。
4. (條件式) 如果您在步驟 3 中執行的 csync2 -x -v 指令無法同步化所有檔案，請執行下列步驟：

   4a 針對所有節點清除 csync2 資料庫 (在 /var/lib/csync2 目錄中)。

   4b 針對所有伺服器執行下列指令以將 csync2 資料庫更新為與檔案系統相符，但不標示需要同步化至其他伺服器的任何項目：

   csync2 -clr /

   4c 執行下列指令以尋找授權伺服器和遠端伺服器之間的所有差異，並針對同步化進行標示：

   csync2 -TUXI

   4d 執行下列指令重設資料庫，以針對任何衝突強制套用目前伺服器中的內容：

   csync2 -fr /

   4e 執行下列指令以開始同步化至所有其他伺服器：

   csync2 -xr /

   4f 執行下列指令以驗證所有檔案是否都已同步化：

   csync2 -T

   如果同步化成功，此指令便不會列出任何檔案。

39 以高可用性升級 Sentinel

當您在高可用性環境下升級 Sentinel 時，請先升級叢集中的被動節點，再升級主動叢集節點。

必要條件

- 從下載網站下載最新的安裝程式。
- 若您正在使用 SLES 作業系統 (內含核心版本 3.0.101 或更新版本)，您必須在電腦中手動載入監視程式驅動程式。要尋找電腦硬體的相關監視程式驅動程式，請聯絡您的硬體廠商。要載入監視程式驅動程式，請執行下列動作：
  1. 在指令提示中，執行下列指令以在目前工作階段中載入監視程式驅動程式：

     /sbin/modprobe -v --ignore-install <*監視程式驅動程式名稱*>
  2. 將下行新增至 /etc/init.d/boot.local 檔案以確定電腦可在每次開機時自動載入監視程式驅動程式：

     /sbin/modprobe -v --ignore-install <*監視程式驅動程式名稱*>

升級傳統 Sentinel HA 安裝

本節提供升級傳統 Sentinel 安裝，以及在傳統 Sentinel 安裝中升級作業系統的相關資訊。

重要： 此區段的程序使用rcopenais和openais指令，配合SLES 11 SP4才能使用。若是SLES 12 SP2和更新版本，請使用 systemctl pacemaker.service 指令。

例如，針對 /etc/rc.d/openais start 指令，請使用 systemctl start pacemaker.service 指令。

升級 Sentinel HA

1 啟用叢集上的維護模式：

crm configure property maintenance-mode=true

維護模式可助您在更新 Sentinel 時避免對執行叢集資源造成任何干擾。您可以從任何叢集節點執行此指令。

2 驗證維護模式是否為使用中：

crm status

叢集資源應以不受管理的狀態顯示。

3 升級被動叢集節點：

3a 停止叢集堆疊：

rcopenais stop

停止叢集堆疊可確保維持叢集資源的存取性，並避免節點的圍籬區隔。

3b 以 root 身分登入要升級 Sentinel 的伺服器。

3c 從目標檔案擷取安裝檔案：

tar xfz <*安裝檔名*>

3d 在您擷取安裝檔案的目錄中執行以下指令：

。/install-sentinel --cluster-node

3e 升級完成之後，請重新啟動叢集堆疊：

rcopenais start

針對所有被動叢集節點重複步驟 3。

3f 請移除自動啟動程序檔，方便叢集管理產品。

cd /

insserv -r sentinel

4 升級主動叢集節點：

4a 請將組態備份，然後建立 ESM 輸出。

如需詳細資訊，請參閱《「 Sentinel 管理指南」》中的「*備份與還原資料*」。

4b 停止叢集堆疊：

rcopenais stop

停止叢集堆疊可確保維持叢集資源的存取性，並避免節點的圍籬區隔。

4c 以 root 身分登入要升級 Sentinel 的伺服器。

4d 執行下列指令，以從目標檔案擷取安裝檔案：

tar xfz <*安裝檔名*>

4e 在您擷取安裝檔案的目錄中執行以下指令：

。/install-sentinel

4f 升級完成之後，請啟動叢集堆疊：

rcopenais start

4g 請移除自動啟動程序檔，方便叢集管理產品。

cd /

insserv -r sentinel

4h 執行下列指令以同步化組態檔案中的任何變更：

csync2 -x -v

5 停用叢集上的維護模式：

crm configure property maintenance-mode=false

您可以從任何叢集節點執行此指令。

6 驗證維護模式是否為非使用中：

crm status

叢集資源應以已啟動的狀態顯示。

7 (選擇性) 驗證 Sentinel 升級是否成功：

```
rcsentinel version
```

升級作業系統

本節提供如何將作業系統升級至主要版本的相關資訊，例如在 Sentinel HA 叢集中從 SLES 11 升級至 SLES 12。升級作業系統時，您必須執行某些組態任務，以確定 Sentinel HA 在升級作業系統後是否正常運作。

請執行下列章節中所述的步驟：

- 「升級作業系統」(第 197 頁)
- 「設定 iSCSI 目標」(第 198 頁)
- 「設定 iSCSI 啟動器」(第 198 頁)
- 「設定 HA 叢集」(第 199 頁)

升級作業系統

若要升級作業系統：

1 以 root 使用者身分登入 Sentinel HA 叢集中的任何節點。

2 執行下列指令以針對叢集啟用維護模式：

```
crm configure property maintenance-mode=true
```

維護模式可協助您在升級作業系統時避免對執行中叢集資源造成任何干擾。

3 執行下列指令以驗證維護模式是否為使用中：

```
crm status
```

叢集資源應以不受管理的狀態顯示。

4 請確定您已針對所有叢集節點將 Sentinel 升級至 8.2 或更新版本。

5 請確定已透過 SLES 和 SLESHA 註冊叢集中的所有節點。

6 執行下列步驟以升級被動叢集節點上的作業系統：

6a 執行下列指令以停止叢集堆疊：

```
rcopenais stop
```

停止叢集堆疊可確保維持叢集資源的不可存取性，並避免節點的圍籬區隔。

6b 升級作業系統。如需詳細資訊，請參閱升級作業系統。

7 針對所有被動節點，重複步驟 6 以升級作業系統。

8 針對主動節點，重複步驟 6 以升級其作業系統。

9 重複步驟 6b 以升級共享儲存上的作業系統。

10 請確定叢集中所有節點上的作業系統都已升級至 SLES12 SP3。

設定 iSCSI 目標

若要設定 iSCSI 目標：

1. 在共享儲存上，檢查是否已安裝 iSCSI LIO 套件。如果尚未安裝該套件，請移至 YaST2 軟體管理，並安裝 iSCSI LIO 套件 (iscciliotarget RPM)。
2. 針對叢集中的所有節點執行下列步驟：
   2a 執行下列指令以開啟包含 iSCSI 啟動器名稱的檔案：

   ```
   cat /etc/iscsi/initiatorname.iscsi
   ```

   2b 記下將用於設定 iSCSI 啟動器的啟動器名稱：

   例如：

   ```
   InitiatorName=iqn.1996-04.de.suse:01:441d6988994
   ```

   設定 iSCSI 目標用戶端設定時，將使用這些啟動器名稱。
3. 按一下「**服務**」，並選取「**開機時**」選項，以確定服務會在作業系統開機時啟動。
4. 選取「**全域**」索引標籤，取消選取「**無驗證**」以啟用驗證，然後指定內送和外送驗證的使用者名稱和密碼。

   系統預設會啟用「**無驗證**」選項。不過，您應啟用驗證以確保組態的安全性。
5. 按一下「**目標**」，並按一下「**新增**」以新增目標。
6. 按一下「**新增**」以加入新的 LUN。
7. 將 LUN 數目保留為 0，瀏覽「**路徑**」對話方塊 (在 Type=fileio 底下)，並選取您建立的 /localdata 檔案。若您有專用的儲存磁碟，請指定一個區塊裝置，例如 /dev/sdc。
8. 重複步驟 6 和 7，並在此時新增 LUN 1 和選取 /networkdata。
9. 重複步驟 6 和 7，並在此時新增 LUN 2 和選取 /sbd。
10. 保留其他選項的預設值。按**下一步**。
11. 按一下「**新增**」。當系統提示用戶端名稱時，請指定您在步驟 2 中複製的啟動器名稱。透過指定啟動器名稱，重複此步驟以新增所有用戶端名稱。

    「用戶端清單」中將顯示用戶端名稱清單。
12. (條件式) 如果您已在步驟 4 中啟用驗證，請提供您在已步驟 4 中指定的驗證身分證明。

    選取用戶端，選取「**編輯驗證**」>「**內送驗證**」，並指定使用者名稱和密碼。請針對所有用戶端重複此步驟。
13. 再按「**下一步**」以選取預設驗證選項，然後按一下「**完成**」以結束組態。如果顯示提示，請重新啟動 iSCSI。
14. 結束 YaST。

設定 iSCSI 啟動器

若要設定 iSCSI 啟動器：

1. 連接到其中一個叢集節點 (node01)，然後啟動 YaST。
2. 按一下「**網路服務**」>「**iSCSI 啟動器**」。
3. 如果顯示提示，請安裝需求的軟體 (iscsiclient RPM)。
4. 按一下「**服務**」，並選取「**開機時**」選項，以確定 iSCSI 服務會在開機時啟動。

5 按一下「已探查目標」。

附註： 如果顯示任何現有 iSCSI 目標，請刪除這些目標。

選取「探查」以新增 iSCSI 目標。

6 指定 iSCSI 目標 IP 位址 (10.0.0.3)。

(條件式) 如果您已在「設定 iSCSI 目標」(第 198 頁)的步驟 4 中啟用驗證，請取消選取「無驗證」。在「外送驗證」區段中，輸入設定 iSCSI 目標時指定的驗證身分證明。

按下一步。

7 選取包含 IP 位址 10.0.0.3 的已探查 iSCSI 目標，並選取「登入」。

8 請執行以下步驟：

8a 在「啟動」下拉式功能表中，切換至「自動」。

8b (條件式) 如果您已啟用驗證，請取消選取「無驗證」。

「外送驗證」區段中應該會顯示您已指定的使用者名稱和密碼。如果未顯示這些身分證明，請在此區段中輸入該身分證明。

8c 按下一步。

9 切換到「連接的目標」索引標籤，以確定您已連接到目標。

10 結束組態。如此一來 iSCSI 目標應可掛接到叢集節點上，成為區塊裝置。

11 在 YaST 主功能表，選取「系統」>「分割器」。

12 在「系統檢視」中，您應該會在清單中看到 LIO-ORG-FILEIO 類型的新硬碟 (例如 /dev/sdb 和 /dev/sdc)，以及格式化的磁碟 (例如 /dev/sdb1 或 /dev/<SHARED1)。

13 針對所有節點重複步驟 1 到 12。

設定 HA 叢集

若要設定 HA 叢集：

1 啟動 YaST2，並移至「高可用性」>「叢集」。

2 如果顯示提示，請安裝 HA 套件並解決相依性問題。

安裝 HA 套件後，便會顯示叢集通訊通道。

3 請確定已針對「傳輸」選項選取「單點傳播」。

4 選取「新增成員位址」，並指定節點 IP 位址，然後重複此動作以新增所有其他叢集節點 IP 位址。

5 請確定已選取「自動產生節點 ID」。

6 請確定已針對所有節點啟用 HAWK 服務。如果尚未啟用，請執行下列指令以將其啟用：

```
service hawk start
```

7 執行以下指令：

```
ls -l /dev/disk/by-id/
```

隨即顯示 SBD 分割區 ID。例如，scsi-1LIO-ORG_FILEIO:33caaa5a-a0bc-4d90-b21b-2ef33030cc53。

複製 ID。

8 開啟 sbd 檔案 (/etc/sysconfig/sbd)，並將 SBD_DEVICE ID 變更為您在步驟 7 中複製的 ID。

9 執行下列指令以重新啟動 pacemaker 服務：

rcpacemaker restart

10 執行下列指令以移除自動啟動程序檔，方便叢集管理產品。

cd /

insserv -r sentinel

11 針對所有叢集節點重複步驟 1 到 10。

12 執行下列指令以同步化組態檔案中的任何變更：

csync2 -x -v

13 執行下列指令以針對叢集停用維護模式：

crm configure property maintenance-mode=false

您可以從任何叢集節點執行此指令。

14 執行下列指令以驗證維護模式是否為非使用中：

crm status

叢集資源應以已啟動的狀態顯示。

升級 Sentinel HA 裝置安裝

您可以使用 Zypper 修補程式來升級 Sentinel HA 裝置安裝。

重要： 此區段的程序使用rcopenais和openais指令，配合SLES 11 SP4才能使用。若是SLES 12 SP2和更新版本，請使用 systemctl pacemaker.service 指令。

例如，針對 /etc/rc.d/openais start 指令，請使用 systemctl start pacemaker.service 指令。

- 「使用 Zypper 升級 Sentinel HA 裝置」(第 200 頁)

使用 Zypper 升級 Sentinel HA 裝置

升級之前，您必須透過 Sentinel 裝置管理員註冊所有裝置節點。如需詳細資訊，請參閱 「登錄以進行更新」(第 99 頁)。若未註冊裝置，Sentinel 會顯示黃色警告。

1 啟用叢集上的維護模式。

crm configure property maintenance-mode=true

維護模式可協助您在更新 Sentinel 軟體時避免對執行叢集資源造成任何干擾。您可以從任何叢集節點執行此指令。

2 驗證維護模式是否為使用中。

crm status

叢集資源應以不受管理的狀態顯示。

3 升級被動叢集節點：

3a 停止叢集堆疊。

rcopenais stop

停止叢集堆疊可確保維持叢集資源的不可存取性，並避免節點的圍籬區隔。

3b 下載 Sentinel HA 裝置的更新。

zypper -v patch

3c (條件式) 如果安裝程式顯示您必須解決 OpenSSH 套件相依性的訊息，請輸入適合的選項以降級 OpenSSH 套件。

3d (條件式) 如果安裝程式顯示表示 ncgOverlay 架構中變更的訊息，請輸入適合的選項以接受架構變更。

3e (條件式) 如果安裝程式顯示您必須為某些裝置套件解析相依性的訊息，請輸入適當的選項以解除安裝相依套件。

3f 升級完成之後，請啟動叢集堆疊。

rcopenais start

4 重複所有被動叢集節點的步驟 3。

5 升級主動叢集節點：

5a 請將組態備份，然後建立 ESM 輸出。

如需備份資料的詳細資訊，請參閱《「 Sentinel 管理指南」》中的「*備份與還原資料*」。

5b 停止叢集堆疊。

rcopenais stop

停止叢集堆疊可確保維持叢集資源的不可存取性，並避免節點的圍籬區隔。

5c 下載 Sentinel HA 裝置的更新。

zypper -v patch

5d (條件式) 如果安裝程式顯示您必須解決 OpenSSH 套件相依性的訊息，請輸入適合的選項以降級 OpenSSH 套件。

5e (條件式) 如果安裝程式顯示表示 ncgOverlay 架構中變更的訊息，請輸入適合的選項以接受架構變更。

5f (條件式) 如果安裝程式顯示您必須為某些裝置套件解析相依性的訊息，請輸入適當的選項以解除安裝相依套件。

5g 升級完成之後，請啟動叢集堆疊。

rcopenais start

5h 執行下列指令以同步化組態檔案中的任何變更：

csync2 -x -v

6 停用叢集上的維護模式。

crm configure property maintenance-mode=false

您可以從任何叢集節點執行此指令。

7 驗證維護模式是否為非使用中。

crm status

叢集資源應以已啟動的狀態顯示。

8 (選擇性) 驗證 Sentinel 升級是否成功：

rcsentinel version

9 (條件式) 若要升級作業系統，請參閱「升級作業系統」(第 149 頁)。

40 備份與復原

本文中說明的高可用性容錯移轉叢集提供了備援的層級，因此，若叢集中的某個節點上的服務失敗，此服務將自動容錯移轉，並在叢集中的其他節點上復原。當發生此類事件時，請務必將失敗的節點回復到運作狀態，讓系統中的備援可以復原並在再次失敗時受到保護。本節說明在多種失敗情況下復原失敗節點的相關資訊。

備份

當如同本文中說明的高可用性容錯移轉叢集提供了備援層時，請務必繼續為組態和資料定期進行傳統備份，這些內容若遺失或損毀並不易復原。「《 Sentinel 管理指南」》中的*「備份及回存資料」*一節說明如何使用 Sentinel 的內建工具來建立備份。這些工具應在叢集的使用中節點上使用，因為叢集中的被動節點將無法存取共享儲存裝置。可以改為使用其他可用的商業備份工具，而且對他們可以使用的節點可能會有不同的要求。

復原

暫時失敗

若失敗只是暫時失敗，也未對應用程式和作業系統軟體和組態造成任何明顯損毀，那麼直接清除暫時失敗 (例如將節點重新開機) 即可將節點回存到操作狀態。叢集管理使用者介面可用來讓執行中的服務在必要時錯誤回復到原始叢集節點。

節點損毀

若失敗造成應用程式或作業系統軟體或目前存在於節點儲存系統中的組態損毀，損毀的軟體將需要重新安裝。重複本文先前所述將節點新增到叢集的步驟，將可回存節點到操作狀態。叢集管理使用者介面可用來讓執行中的服務在必要時錯誤回復到原始叢集節點。

叢集資料組態

若資料損毀是以共享儲存裝置無法復原的方式發生在共享儲存裝置上，這將造成會影響到整個叢集的損毀，進而無法使用本文中所述之高可用性容錯移轉叢集自動復原。「《 Sentinel 管理指南」》中的*「備份及回存資料」*一節說明如何使用 Sentinel 的內建工具從備份回存。這些工具應在叢集的使用中節點上使用，因為叢集中的被動節點將無法存取共享儲存裝置。可以改為使用其他可用的商業備份和回存工具，而且對他們可以使用的節點可能會有不同的要求。

VIII 附錄

A 疑難排解

本節包含一些可能會在安裝期間發生的問題，以及解決問題的動作。

由於不正確的網路組態導致安裝失敗

第一次開機時，如果安裝程式發現網路設定不正確，即會顯示錯誤訊息。如果網路無法使用，便無法在裝置上安裝 Sentinel。

若要解決此問題，請正確設定網路設定。若要驗證組態，請使用 ifconfig 指令來傳回有效的 IP 位址，以及使用 hostname -f 指令來傳回有效的主機名稱。

無法針對已建立影像的 Collector Manager 或 Correlation Engine 建立 UUID

如果為 Collector Manager 伺服器建立影像 (例如使用 ZENworks Imaging 建立) 並將影像還原到其他機器，則 Sentinel 無法唯一識別 Collector Manager 的各個新例項。發生這個問題的原因在於重複的 UUID。

您必須在新安裝的 Collector Manager 系統上執行以下步驟，才能產生新的 UUID：

1. 刪除位於 /var/opt/novell/sentinel/data 資料夾中的 host.id 或 sentinel.id。
2. 重新啟動 Collector Manager。

   Collector Manager 將自動產生 UUID。

在登入後，Internet Explorer 的 Sentinel 主要介面為空白

如果網際網路保全性層級設為「高級」時，在登入 Sentinel 之後會出現空白頁面，而且瀏覽器會封鎖檔案下載快顯視窗。如果要解決此問題，您需要先將保全性層級設為「中高級」，然後變更「自定」層級，如下所示：

1. 請瀏覽至「**工具**」>「**網際網路選項**」>「**安全性**」，然後將安全性層級設為「**中高級**」。
2. 確保未選取「**工具**」>「**相容性檢視**」選項。
3. 請瀏覽至「**工具**」>「**網際網路選項**」>「**保全性**」索引標籤 >「**自定層級**」，然後向下捲動至「**下載**」區段，並在「**自動提示下載檔案**」選項下方選取「**啟用**」。

Sentinel 無法在 Windows Server 2012 R2 的 Internet Explorer 11 中啟動

當您使用 Windows Server 2012 R2 時，Sentinel 會因為 Internet Explorer 11 的預設安全性組態，而無法在 Internet Explorer 11 中啟動。您必須先手動將 Sentinel 新增至信任的網站清單，再啟動 Sentinel。

將 Sentinel 新增至信任的網站清單

1. 開啟 Internet Explorer 11。
2. 按一下「**設定**」圖示 >「**網際網路選項**」>「**安全性**」索引標籤 >「**信任的網站**」>「**網站**」
3. 將 Sentinel 主機新增至信任的網站清單。

Sentinel 無法使用預設 EPS 授權執行本地報告

如果您的環境具有預設的 25 EPS 授權，當您執行報告時，報告將會失敗，並出現下列錯誤：分散式搜尋功能的授權已過期

若要執行如 Sentinel 相同的 JVM 的報告，請完成下列步驟：

1. 登入 Sentinel 伺服器並開啟 /etc/opt/novell/sentinel/config/obj-component.JasperReportingComponent.properties 檔案。
2. 找出 reporting.process.oktorunstandalone 內容。
3. (條件式) 如果該內容不在檔案中，請加以新增。
4. 將該內容設定為 false。例如：

   reporting.process.oktorunstandalone=false
5. 重新啟動 Sentinel。

在 Sentinel High Availability 裡，當您將主動節點轉換成 FIPS 140-2 模式後，您需要手動開啟同步

問題： 在 Sentinel HA 裡，當您將主動節點轉換成 FIPS 140-2 模式，將被動節點轉換成 FIPS 140-2 模式的同步無法完全執行。您必須手動啟動同步。

解決方式： 透過下列方式將所有被動節點手動同步至 FIP 140-2 模式：

1. 在主動節點上使用 root 使用者身分登入。
2. 開啟 /etc/csync2/csync2.cfg 檔案。
3. 變更下行：

   include /etc/opt/novell/sentinel/3rdparty/nss/*;

   to

   include /etc/opt/novell/sentinel/3rdparty/nss;
4. 儲存 csync2.cfg 檔案。
5. 執行下列指令手動啟動同步化：

   csync2 -x -v

Sentinel 主要介面在轉換至 Sentinel 可擴充資料管理員後，顯示空白頁面

問題： 在您啟用 SSDM 後，登入 Sentinel Main 時，瀏覽器會顯示空白頁面。

解決方式： 請關閉您的瀏覽器，然後再次登入 Sentinel 主要介面。此問題僅會發生一次，發生在您啟用 SSDM 後第一次登入 Sentinel 主要介面的時候。

當編輯某些已儲存搜尋時，排程頁面中的「事件欄位」面板遺失

問題： 當編輯從 Sentinel 7.2 升級至新版的已儲存搜尋時，用於在搜尋報告 CSV 中指定輸出欄位的「事件欄位」面板在排程頁面中遺失。

解決方式： 在升級 Sentinel 後，重新建立並重新編程搜尋以在排程頁面中檢視「事件欄位」面板。

當您使用預設引發計數搜尋來搜尋已部署規則的事件時，Sentinel 不會傳回任何關連事件

問題： 在規則的「關連摘要」頁面中按一下「活動統計資料」面板上「引發計數」旁的圖示，當您搜尋在規則已部署或已啟用後產生的所有關連事件時，Sentinel 不會傳回任何關連事件。

解決方式： 將「事件搜尋」頁面中「從」欄位中的值變更至比欄位中填入時間更早的時間，然後再按一下「搜尋」。

重新產生基線時，安全情報儀表板會顯示無效的基線期間

問題： 在安全情報基線重新產生期間，基線的開始和結束日期錯誤並顯示 1/1/1970。

解決方式： 基線重新產生完成後，即會更新正確日期。

若單一分割區中有大量事件，則執行搜尋時，Sentinel 伺服器會關閉

問題： 若單一分割區中有大量已編製索引的事件，當您執行搜尋時，Sentinel 伺服器會關閉。

解決方式： 建立保留規則，讓一天內至少有兩個分割區開啟。有一個以上的分割區開啟可協助減少在分割區中已編製索引的事件數目。

您可以建立根據 estzhour 欄位過濾事件的保留規則，該欄位會追蹤當天的時間。因此，您可使用 estzhour:[0 TO 11] 做為過濾器來建立一個保留規則，然後使用 estzhour:[12 TO 23] 做為過濾器來建立另一個保留規則。

如需詳細資訊，請參閱「《 Sentinel 管理指南》」中的*「設定資料保留規則」*。

在已升級 Sentinel 裝置安裝上使用 report_dev_setup.sh 程序檔設定防火牆例外的 Sentinel 連接埠時發生錯誤

問題： 當您使用 report_dev_setup.sh 程序檔設定防火牆例外的 Sentinel 連接埠時，Sentinel 會顯示錯誤。

解決方式： 若要設定防火牆例外的 Sentinel 連接埠，請執行下列操作：

1. 開啟 /etc/sysconfig/SuSEfirewall2 檔案。
2. 變更下行：

   FW_SERVICES_EXT_TCP=" 443 8443 4984 22 61616 10013 289 1289 1468 1443 40000:41000 1290 1099 2000 1024 1590"

   至

   FW_SERVICES_EXT_TCP=" 443 8443 4984 22 61616 10013 289 1289 1468 1443 40000:41000 1290 1099 2000 1024 1590 5432"
3. 重新啟動 Sentinel。

B 解除安裝

本附錄提供解除安裝 Sentinel 及解除安裝後工作的相關資訊。

解除安裝核對清單。

使用以下核對清單解除安裝 Sentinel：

- ❒ 解除安裝 Sentinel 伺服器。
- ❒ 解除安裝 Collector Manager 和 Correlation Engine (若有)。
- ❒ 執行解除安裝後工作以完成 Sentinel 解除安裝。

解除安裝 Sentinel

您可以使用解除安裝程序檔來協助您移除 Sentinel 安裝。在執行新安裝前，請執行以下所有步驟以確保前次安裝所留下的檔案或系統設定均已清除。

警告： 這些指示包括修改作業系統設定和檔案。如果不知道如何修改這些系統設定和檔案，請聯絡您的系統管理員。

解除安裝 Sentinel 伺服器

使用下列步驟解除安裝 Sentinel 伺服器：

1. 以 root 身分登入 Sentinel 伺服器。

   附註： 如果安裝是以 root 身分執行，您將無法以非 root 身分解除安裝 Sentinel 伺服器。不過，如果安裝是由非 root 身分的使用者執行，則非 root 身分的使用者就可解除安裝 Sentinel 伺服器。

   ---

2. 存取以下目錄：

   `<sentinel_installation_path>/opt/novell/sentinel/setup/`

3. 執行以下指令：

   `./uninstall-sentinel`

4. 當系統提示您再次確認是否要繼續解除安裝時，請按下 y 鍵。

   程序檔會先停止服務，然後再將服務完全移除。

解除安裝 Collector Manager 和 Correlation Engine

使用下列步驟解除安裝 Collector Manager 和 Correlation Engine：

1 以 root 身分登入 Collector Manager 和 Correlation Engine 電腦。

附註： 如果安裝是以 root 使用者執行，您將無法以非 root 使用者解除安裝遠端 Collector Manager 或遠端 Correlation Engine。不過，如果安裝是由非 root 使用者完成，則非 root 使用者的使用者就可解除安裝。

2 移至下列位置：

```
/opt/novell/sentinel/setup
```

3 執行以下指令：

```
./uninstall -sentinel
```

程序檔會顯示警告，表示將完全移除 Collector Manager 或 Correlation Engine 以及所有相關資料。

4 輸入 y 以移除 Collector Manager 或 Correlation Engine。

程序檔會先停止服務，然後再將服務完全移除。不過，Collector Manager 和 Correlation Engine 圖示在 Sentinel 主要介面中仍會以非使用中狀態顯示。

5 (條件式) 如果您已啟用事件視覺化，則必須重新部署 Elasticsearch 安全性外掛程式。如需詳細資訊，請參閱「重新部署 Elasticsearch 安全性外掛程式」(第 79 頁)。

6 執行下列其他步驟，以手動刪除 Sentinel 主要介面中的 Collector Manager 和 Correlation Engine：

Collector Manager:

1. 存取「**事件來源管理**」>「**即時檢視**」。
2. 在您要刪除的 Collector Manager 上按一下滑鼠右鍵，然後按一下「**刪除**」。

Correlation Engine:

1. 以管理員身分導覽至 **Sentinel 主要介面**。
2. 顯示**關連**的次目錄，接著選取要刪除的 Correlation Engine。
3. 按一下「**刪除**」按鈕 (垃圾桶圖示)。

解除安裝 NetFlow Collector Manager

使用下列步驟解除安裝 NetFlow Collector Manager：

1 登入至 NetFlow Collector Manager 電腦。

附註： 您必須使用與用來安裝 NetFlow Collector Manager 相同的使用者許可登入。

2 變更至以下目錄：

```
/opt/novell/sentinel/setup
```

3 執行以下指令：

```
./uninstall -sentinel
```

4 輸入 y 以解除安裝 Collector Manager。

程序檔會先停止服務，然後再將服務完全解除安裝。

解除安裝後的工作

解除安裝 Sentinel 伺服器時並不會從作業系統移除 Sentinel 管理員使用者。您必須手動移除該使用者。

在解除安裝 Sentinel 之後，某些系統設定仍會存留下來。在執行 Sentinel 的全新安裝前，您應該移除這些設定，特別是當 Sentinel 的解除安裝作業發生錯誤時。

若要手動清除 Sentinel 系統設定：

1 以 root 身分登入。

2 確認所有 Sentinel 程序都已停止。

3 移除 /opt/novell/sentinel (或任何安裝 Sentinel 軟體之位置) 的內容。

4 確定沒有人以「Sentinel 管理員」作業系統使用者的身分 (依預設為 novell) 登入，接著移除使用者、主目錄及群組。

userdel -r novell

groupdel novell

5 重新啟動作業系統。