NetIQ® Sentinel™

安裝與組態指南

2015 年 2 月

法律聲明

NetIQ Sentinel 受到以下美國專利號碼所保護：05829001。

本文和本文中所述軟體是根據授權合約或保密合約的條款提供，並受其規範。除非在此類授權合約或保密合約中明白指定，NETIQ CORPORATION 係「按現狀」提供本文和本文中所述軟體，不附任何明示或默示擔保，包括 (但不限於) 適售性之默示擔保或特定目的之適用性。有些州不允許在特定交易中免除明示或默示擔保；因此，您可能不適用此聲明。

基於明確性考量，任何模組、介面卡和其他類似的材料 (「模組」) 是依據一般使用者授權合約的條款和條件所授權，適用於相關或相互操作的 NetIQ 產品或軟體版本，存取、複製或使用某個模組即代表您同意受到這些條款的約束。若不同意一般使用者授權合約的條款，您就無法取得使用、存取或複製某個模組的授權，您必須銷毀所有模組的複本，並聯絡 NetIQ 瞭解進一步指示。

若未事先取得 NetIQ Corporation 書面許可，本文和本文中所述軟體不得出借、銷售或贈送 (除非法律另有規定)。除非在此類授權合約或保密合約中明白指定，若未事先取得 NetIQ Corporation 書面同意，本文和本文中所述軟體之任何部分皆不得重製、儲存在取回系統中或以任何形式或透過任何方式 (電子或機械) 轉送。本文中使用的部分公司、名稱和資料是基於說明用途，不代表真實的公司、個人或資料。

本文可能包含不正確的技術或錯字。此處提供的資訊會定期變更。這些變更會加入本文新版內容。NetIQ Corporation 隨時會對本文中所述軟體進行改進或變更。

美國政府限制的權利：若軟體或文件是由 (或代表) 美國政府或 (在任何層級的) 美國政府主要承包商或轉包商根據 48 C.F.R. 227.7202-4 (適用於國防部 (DOD) 採購)、48 C.F.R. 2.101 和 12.212 (適用於非國防部採購) 取得，美國政府對軟體和文件的權利 (包括其使用、修改、重製、發行、執行、顯示或揭露軟體或文件的權利) 皆受到授權合約中提供之商業授權權利和限制的全面規範。

目錄

關於本書和文件庫

《*安裝與組態指南*》提供了 NetIQ 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。

關於 NetIQ Corporation

我們是一家全球性企業軟體公司，著重於處理您環境中三個不斷出現的挑戰：變動、複雜性和風險，以及我們可以如何協助您進行控制。

我們的觀點

因應變動及管理複雜性和風險已不是新資訊

事實上，在您所面對的挑戰中，這些或許是最明顯的變數，可控制您是否可以安全地測量、監控及管理您的實體、虛擬和雲端運算環境。

更有效、更快速地啟用重要的業務服務

我們認為對 IT 組織提供最大控制權限，是提供及時服務交付並符合成本效益的唯一方式。隨著組織繼續推動革新，用來進行管理的技術也日益複雜，由變動及複雜性所帶來的壓力只會繼續提高。

經營理念

不只銷售軟體，而是銷售智慧型解決方案

為提供可靠的控制，我們會先確保已瞭解真實世界中與您類似的 IT 組織日常的操作方式。這是我們能夠開發出實際的智慧型 IT 解決方案的唯一方式，這些解決方案也已順利產生經過證明且可測量的成效。這比單純銷售軟體更有價值。

協助您成功是我們的目標

我們將您的成就視為我們的業務核心。從產品發想到部署，我們瞭解您需要能夠運作良好的 IT 解決方案，並與現有投資緊密結合；您需要持續的支援以及部署後訓練，並需要改與容易合作的對象往來。到了最後，您的成功就是我們的成就。

我們的解決方案

- 身分與存取治理
- 存取管理
- 安全性管理
- 系統與應用程式管理
- 工作量管理
- 服務管理

聯絡銷售支援

若有關於產品、價格及功能等方面的問題，請聯絡當地合作夥伴。如果您無法聯絡合作夥伴，請聯絡我們的銷售支援團隊。

全球：	www.netiq.com/about_netiq/officelocations.asp
美國和加拿大：	1-888-323-6768
電子郵件：	info@netiq.com
網站：	www.netiq.com

聯絡技術支援

若有關於特定產品的問題，請聯絡我們的技術支援團隊。

全球：	www.netiq.com/support/contactinfo.asp
北美與南美：	1-713-418-5555
歐洲、中東和非洲：	+353 (0) 91-782 677
電子郵件：	support@netiq.com
網站：	www.netiq.com/support

聯絡文件支援

我們的目標是提供符合您需求的文件。若您有任何改善建議，請按一下 HTML 文件版本任何頁面底部的 **「新增備註」**，HTML 文件版本的張貼網址是：www.netiq.com/documentation。您也可以將電子郵件寄至 Documentation-Feedback@netiq.com。我們重視您的意見並期待您提出建議。

聯絡線上使用者社群

Qmunity (NetIQ 線上社群) 是一個協同網路，將您與使用者和 NetIQ 專家連接起來。透過提供更多立即的資訊、有用資源的實用連結以及諮詢 NetIQ 專家的管道，Qmunity 協助確保您精通必要知識，以充分發揮您所仰賴之 IT 投資的全部潛力。如需詳細資訊，請造訪 http://community.netiq.com。

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。

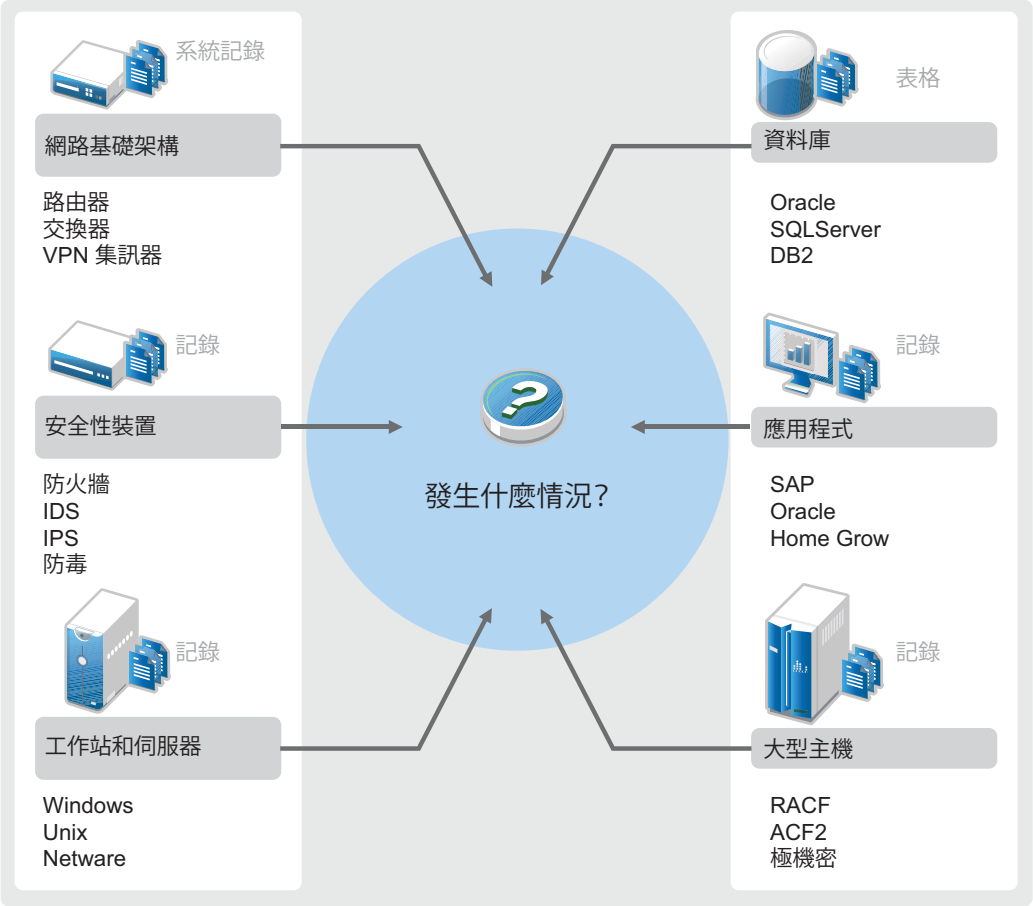
1 Sentinel 是什麼？

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。

1.1 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。眾多應用程式、資料庫、大型主機、工作站及伺服器等均會將事件記錄下來。安全裝置和網路基礎架構裝置也會包含 IT 環境中所有事件的記錄。

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。
- 記錄存放在筒倉中。
- 於記錄內產生的資訊數量。
- 必須要手動分析所有記錄才能判斷誰做了哪些動作。

為讓資訊具有實用性，您必須能執行下列動作：

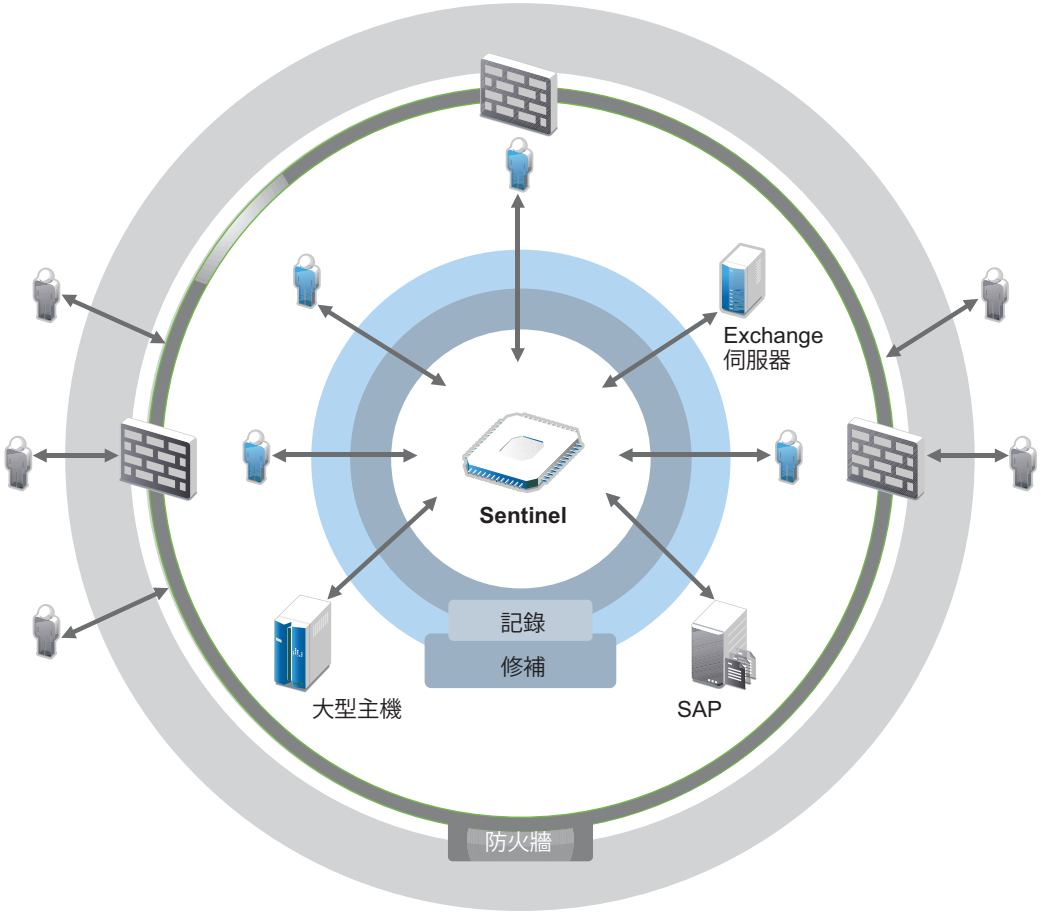
- 收集資料。
- 整合資料。
- 將不同的資料標準化到您可以輕鬆比較的事件中。
- 將事件對應至標準法規。
- 分析資料。
- 比對多個系統間的事件以判斷是否有安全問題。
- 當資料顯示異狀時傳送通知。
- 針對通知採取動作，以遵守公司規則。
- 產生報告以證明遵循法規。

在瞭解保護 IT 環境的難題後，您需要判斷如何一方面保護企業和使用者，另一方面從使用者權限著手規範，卻不致讓他們感到像心懷不軌的使用者一般，或加重其負擔以致於喪失生產力。Sentinel 能提供問題的解決方案。

1.2 Sentinel 提供的解決方案

Sentinel 能扮演企業安全性的中樞神經系統。它能提取整個基礎架構中的資料，包括應用程式、資料庫、伺服器及安全性裝置；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



解決方案運作時，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。如此一來，您可以判斷使用者行為及有效地進行監控。不論是內部人員或外部人員，您都能將人員採取的動作與人員連結在一起，使未授權的活動一目了然，避免對企業造成損害。

Sentinel 達成上述目標所採用的方式非常符合成本效益，其中結合：

- 提供單一解決方案來解決多種法規限制下的 IT 控管問題。
- 消彌網路環境中預期發生與實際發生之間的認知落差。
- 向稽核人員和執法人員證明，企業組織確實記錄、監控及報告安全控管事項。
- 提供立即可用的法規遵循監控和報告程式。
- 洞悉及掌握持續評估組織法規遵循與安全方案的達成狀況。

Sentinel 可將記錄收集、分析和報告程序自動化，以確保 IT 控制能有效支援威脅偵測與稽核要求。Sentinel 可提供安全性事件、法規遵循事件及 IT 控制的自動監控，因此當發生破壞安全性或未遵循法規的事件時，您將可立即採取行動。Sentinel 可讓您輕鬆地收集與環境有關的摘要資訊，以便將整體安全性狀態傳達給主要關係人。

2 Sentinel 如何運作

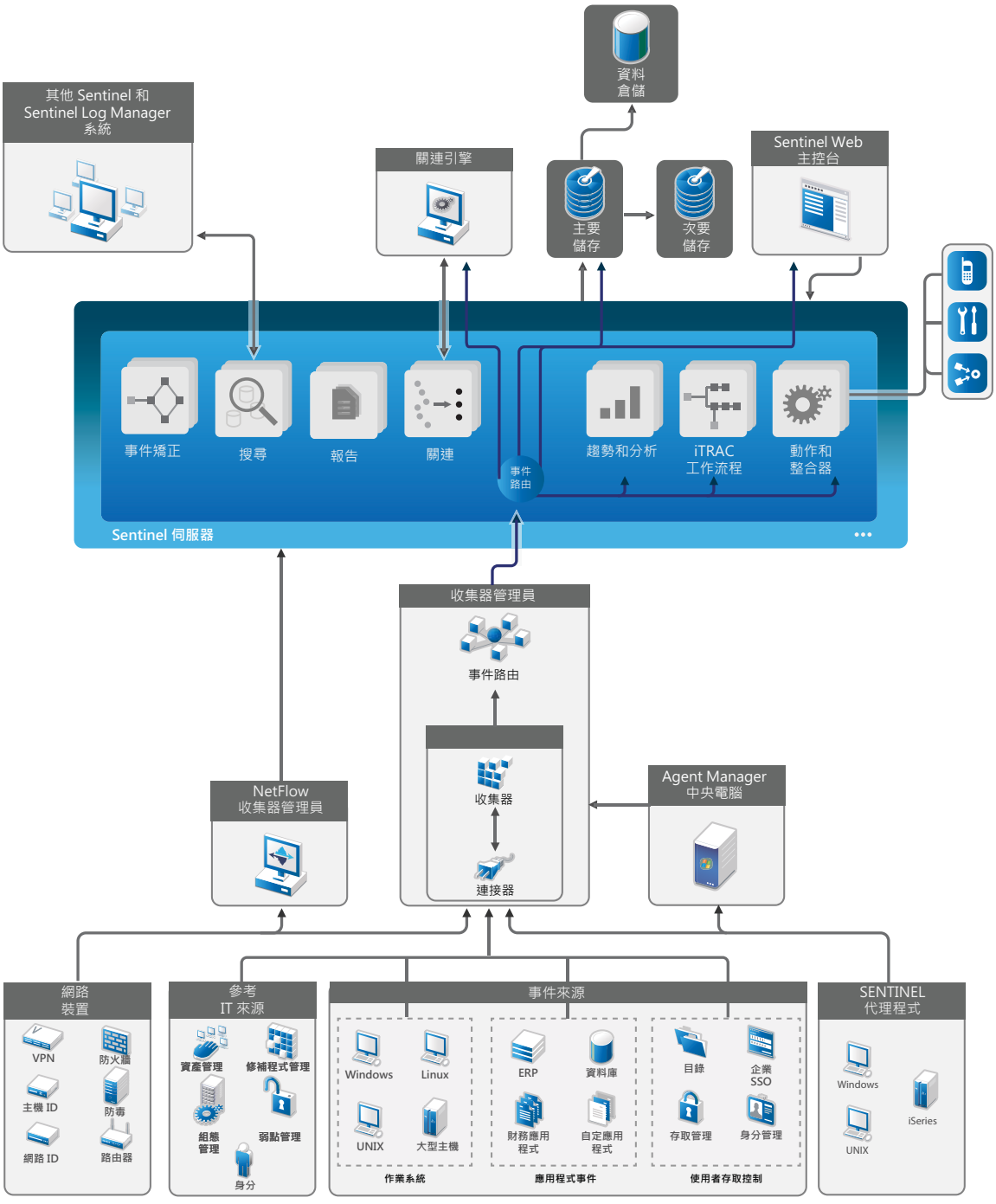
Sentinel 能持續管理 IT 環境中的安全性資訊和事件，提供全方位的監控解決方案。

Sentinel 進行下列動作：

- 從 IT 環境中各個不同的事件來源蒐集記錄、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，使其成為通用的格式。
- 透過彈性、可自訂的資料保留規則，將事件儲存在檔案式資料儲存中。
- 收集網路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。
- 使指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 的運作方式：

圖 2-1 Sentinel 架構



以下各節會詳細說明 Sentinel 元件：

- 第 2.1 節「事件來源」(第 21 頁)
- 第 2.2 節「Sentinel 事件」(第 21 頁)
- 第 2.3 節「收集器管理員」(第 22 頁)
- 第 2.4 節「代理程式管理員」(第 23 頁)

2.1 事件來源

Sentinel 會從 IT 環境內許多不同的來源收集安全性資訊和事件。這些來源稱為「事件來源」。網路中許多不同的項目都能成為事件來源。

安全性周邊：安全性裝置包括用來為環境建立安全性周邊的硬體和軟體，例如防火牆、IDS 和 VPN。

作業系統： 來自各種在網路中運作的作業系統的事件。

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。

應用程式事件：由安裝於網路中的應用程式所產生的事件。

使用者存取控制：由允許使用者存取公司資源的應用程式或裝置所產生的事件。

如需有關從事件來源收集事件的詳細資訊，請參閱「「設定無代理程式之資料收集」」。

2.2 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。將類別資訊 (分類) 新增至事件之後，您就可以輕鬆地在報告不同事件的系統之間比較各種事件；例如，驗證失敗。即時顯示、關連引擎、儀表板及後端伺服器是負責處理事件的程序。

一個事件含有 200 個以上的欄位。事件欄位分屬不同的類型，也具有不同的目的。諸如安全性、嚴重性、目的地 IP 及目的地連接埠等即為一些預先定義的欄位。可設定的欄位分為兩種：「保留欄位」是供 Sentinel 內部用來允許日後進行擴充之用的欄位；「客戶欄位」則是供客戶延伸之用的欄位。

重新命名欄位可重新訂定欄位的用途。欄位的來源可以來自外部。這表示它可以是由裝置或對應收集器明確設定的來源，此時稱為參考欄位。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，您可以將欄位定義為建置碼，以供含有做為事件目的地 IP 之資產的建置之用。例如，您可以利用事件目的地 IP，並透過使用客戶定義映射的映射服務來計算欄位。

2.2.1 映射服務

映射服務能讓您透過精密的機制，將企業相關性資料散播到整個系統中。此資料可在事件中新增參考資訊以提供相關資訊，讓分析者能進行最佳決策、撰寫更有用的報告，並寫出完善的關連規則。

您可以使用映射，將主機和身分詳細資料等額外資訊新增至從來源設備收到的事件，讓事件內容更為豐富。這類額外資訊可用來進行進階關連和報告。系統支援數種內建映射以及自訂的使用者定義映射。

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，使用收集器代碼中的 API 進行更新，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映射資料組態 UI 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收集器管理員並在本機套用。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。

2.2.2 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建立大量靜態映射。這項串流能力的價值與關鍵任務即時系統 (如 Sentinel) 格外相關，因為這類型的系統需要穩定、可預期、靈活，以及不受系統中任何暫時性負載干擾的資料移動。

2.2.3 入侵偵測 (映射服務)

Sentinel 提供交互參考事件資料簽名和弱點掃描器資料的能力。當嘗試入侵含有弱點的系統的攻擊發生時，系統會自動在第一時間通知使用者。這項作業是透過以下項目來完成的：

- Advisor 饋送
- 入侵偵測
- 弱點掃描
- 防火牆

Advisor 提供交互參考事件資料簽名和弱點掃描器資料的能力。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漏洞外掛程式。如需有關 Advisor 的詳細資訊，請參閱《*NetIQ Sentinel 管理指南*》中的「「偵測漏洞和入侵」」。

2.3 收集器管理員

收集器管理員可管理資料收集、監控系統狀態訊息，並視需要執行事件過濾。收集器管理員的主要功能包括以下所列：

- 轉換事件。
- 透過映射服務將業務關聯性新增至事件。
- 路由事件。
- 判斷即時、弱點、資產或非即時資料。
- 將狀態訊息傳送至 Sentinel 伺服器。

2.3.1 收集器

收集器能標準化並收集來自連接器的資訊。收集器是以 Javascript 所撰寫，可定義下列邏輯：

- 接收來自連接器的原始資料。
- 剖析及標準化資料。
- 將可重複的邏輯套用至資料。
- 將裝置特有的資料轉譯為 Sentinel 特有的資料。
- 格式化事件。
- 將經過標準化、剖析及格式化的資料傳遞至收集器管理員。
- 將裝置特有的事件進行過濾。

如需有關收集器的詳細資訊，請參閱 Sentinel 外掛程式網站。

2.3.2 連接器

連接器能提供事件來源和 Sentinel 系統間的連接。連接器會使用產業標準的通訊協定來取得像是 Syslog 的事件，例如使用 JDBC 從資料庫表格讀取事件，或使用 WMI 從 Windows 事件記錄檔讀取事件等等，藉以提供下列功能：

- 將原始事件資料從事件來源傳輸至收集器。
- 連接專用過濾。
- 連接錯誤處理。

2.4 代理程式管理員

代理程式管理員提供主機式資料收集，補足無代理程式之資料收集，可讓您：

- 存取無法從網路取得的記錄。
- 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

代理程式管理員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。如需有關代理程式管理員的詳細資訊，請參閱代理程式管理員文件。

2.5 NetFlow 收集器管理員

NetFlow 收集器管理員會收集路由器、交換器和防火牆等網路裝置的網路流程資料 (NetFlow、IPFIX 等)。網路流程資料可說明關於主機之間所有網路連接的基本資訊 (包括轉送的封包和位元組)，協助您以視覺方式呈現個別主機或整個網路的行為。

NetFlow 收集器管理員功能包括以下項目：

- 從支援網路裝置收集位元組、流程和封包等網路流程資料。
- 結集收集到的資料並傳送至 Sentinel 伺服器，以透過視覺方式分析在您環境中的網路活動。

如需有關以視覺方式呈現並分析網路流程資料的詳細資訊，請參閱《*NetIQ Sentinel 使用者指南*》中的「「視覺化並分析網路流程資料」」。

2.6 Sentinel 資料路由和儲存

Sentinel 可針對輪遞、儲存和解壓縮所收集的資料提供多種選項。依預設，Sentinel 會從收集器管理員接收兩個獨立但相關的資料流：剖析的事件資料和原始資料。原始資料會立即儲存在受保護的分割區中，以提供安全的辨識鏈。剖析的事件資料會根據您所定義的規則輪遞，您可以過濾這些資料、將其傳送至儲存、傳送至即時分析及輪遞至外部系統。傳送到儲存的所有事件資料會進一步對應到使用者定義的保留規則，這些規則決定要在其中放入資料的分割區，也定義清理規則，以依其保留及刪除資料。

Sentinel 的資料儲存基礎為三層結構：

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	分割區關閉之後，您可以將分割區備份至離線儲存，例如 Amazon Glacier 等等。必要時，您可以暫時重新輸入分割區以用於長期詳細分析。

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《*NetIQ Sentinel 管理指南*》中的「「設定資料儲存」」。

2.7 關連

單一事件或許相當細瑣，但在與其他事件相結合之後，它就能針對潛在性問題發出警告。Sentinel 會使用您建立並部署在關連引擎中的規則，建立這些事件的關連，然後採取適當的行動以解決這些問題。

關連會自動分析收到的事件資料流，找出值得注意的模式，進而為安全性事件管理貢獻可靠情報。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。如需詳細資訊，請參閱 《*NetIQ 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，您必須在關連引擎中部署規則。當發生符合規則準則的事件時，關連引擎會產生說明該模式的關連事件。如需詳細資訊，請參閱《「NetIQ Sentinel 使用者指南」》中的「*關連引擎*」。

2.8 安全性智慧

透過 Sentinel 中的關連功能，您可基於安全性、法規遵循或其他目的，輕鬆搜尋已知的活動模式。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，使分析師得以藉由自動化的統計引擎或手動解譯統計資料的視覺呈現來識別及分析偏離 (異常)。如需詳細資訊，請參閱 *《NetIQ Sentinel 使用者指南》*中的「「分析資料中的趨勢」」。

2.9 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，提供與問題報修系統的雙向整合。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《*NetIQ Sentinel 使用者指南*》中的「「設定事件」」。

2.10 iTrac 工作流程

iTRAC 工作流程的設計在於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。

您可以利用手動和自動化的步驟來建立工作流程。它支援如分支、以時間為基礎之提升及本地變數等進階功能，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 *《NetIQ Sentinel 使用者指南》*中的「「設定 iTRAC 工作流程」」。

2.11 動作與整合器

動作會在 Sentinel 中手動或自動執行某些動作類型，例如傳送電子郵件。透過手動執行事件、事件操作，以及關連規則，動作可由路由規則觸發。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《*NetIQ 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《*NetIQ Sentinel 管理指南*》中的「「設定整合器」」。

2.12 搜尋

Sentinel 提供執行事件搜尋的選項。您可搜尋在主要儲存或次要儲存位置中的資料。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《*NetIQ Sentinel 使用者指南*》中的「「執行搜尋」」。

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「《NetIQ Sentinel 管理指南》」中的 *「設定資料聯盟」*。

2.13 報告

Sentinel 提供針對收集的資料執行報告的能力。Sentinel 已預先封裝各種可自定報告。某些報告預留彈性空間，能讓您指定要顯示在結果中的欄。

您能執行報告、排程報告，以及利用電子郵件傳送 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與結果互動 (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 *《NetIQ Sentinel 使用者指南》*中的 「「報告」」。

2.14 身分追蹤

Sentinel 提供身分管理系統的整合架構，可追蹤每個使用者帳戶的身分，以及這些身分已執行的事件。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。透過顯示使用者啟動指定動作或受到動作影響的使用者相關資訊，事件回應次數獲得改善並可採用行為式分析。如需詳細資訊，請參閱《*NetIQ Sentinel 使用者指南*》中的 「「運用身分資訊」」。

2.15 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；同時在任何特殊類型的分析中進行系統的調整及最佳化以大幅提升效率，並提供將分析類型轉換至另一種類型的簡易方式以進行順暢的轉換。

Sentinel 中的事件調查通常會從接近即時的 Active Views 開始。雖然有進階工具可供使用，但 Active Views 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概略分析，並可以識別特定事件。在經過一段時間之後，您就可以針對特定資料類別 (例如從關聯性輸出) 增加已調整的過濾器。您可以將 Active Views 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建立的互動式搜尋傳送到報告範本，然後迅速建立報告以顯示適用於大量事件的相同資料，使資料的轉換更為簡易。

Sentinel 包含許多種這類用途的範本。某些範本適用於顯示特殊類型的資料，例如驗證資料或使用者建立，或者您也可以使用一般用途的範本，以互動方式自訂報告上的群組及欄位。

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完整支援。如需詳細資訊，請參閱 *《NetIQ Sentinel 使用者指南》*。

II 規劃 Sentinel 安裝

本節將向您說明安裝 Sentinel 之前的規劃考量。若您想要安裝的組態並未出現在下列各節，或有任何疑問，請聯絡 NetIQ 技術支援。

3 執行核對清單

使用下列核對清單來完成規劃、安裝及設定 Sentinel 的組態：

❒	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，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 31 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 35 頁)。
❒	檢閱收集器管理員和關連引擎的每秒事件 (EPS)，和 NetFlow 收集器管理員的每秒記錄 (RPS)。 判斷您需要安裝以改善效能和負載平衡的收集器管理員、關連引擎和 NetFlow 收集器管理員數目。	第 6.1 節 「分散式佈署的優點」 (第 37 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 59 頁)。
❒	確定已設定 Sentinel 伺服器上的時間。	第 17 章 「設定時間」 (第 91 頁)。
❒	安裝 Sentinel 時，預設會安裝 Sentinel 發行當時可以使用的 Sentinel 外掛程式。設定立即可用的外掛程式，以用於資料收集和報告。	第 19 章 「設定立即可用外掛程式」 (第 97 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 15 章 「安裝額外的收集器和連接器」 (第 85 頁)。
❒	視需求在環境中安裝其他收集器管理員和關連引擎。	第 12.4 節 「安裝收集器管理員和關連引擎」 (第 69 頁)。

4 瞭解授權資訊

Sentinel 平台包含各式各樣功能，而不同的客戶有不同的需求。NetIQ 提供不同的授權模式以滿足這些需求。

在 Sentinel 7.3 之前，基本的 Sentinel 平台分為兩個不同產品，即 Sentinel 和 Sentinel Log Manager。自 Sentinel 7.3 起，NetIQ 將這兩個產品結合為單一平台，以更佳方式提供新功能、修補程式、文件及支援，同時讓客戶得以選擇最符合其需求的解決方案功能。

Sentinel 平台提供兩大解決方案：

- **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 專注於安全性資訊和事件管理 (SIEM) 用例，如即時威脅偵測、警示及修補。
- **Sentinel for Log Management:** 適用於記錄管理用例的解決方案，如收集、儲存、搜尋、報告資料的能力。

  Sentinel for Log Management 7.3 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。若您要規劃升級至 Sentinel for Log Management 7.3，請詳見常見問答集 (FAQ)，可於以下網址取得 https://www.netiq.com/products/sentinel/frequently-asked-questions/slm122-to-slm73-upgrade-faqs.html。

NetIQ 為各個解決方案分別提供不同授權。取決於您的授權金鑰類型，將啟用其各別適用的解決方案。Sentinel 授權也取決於其他因素，如需要額外授權的 EPS、裝置許可及外掛程式。如需更多詳細資料，請參考您的使用者授權合約。

下表為各解決方案啟用之特定服務與功能：

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 ◆ 基本事件集合 ◆ 非事件資料集合 (資產、漏洞、身分識別) ◆ 剖析及標準化 ◆ 事件資料分類法 ◆ 內部網路位置映射 ◆ Netflow 集合與儲存 ◆ 即時 NetFlow 視覺效果 ◆ 基於事件的 NetFlow 視覺效果 ◆ 事件搜尋 (本地) ◆ 事件報告 ◆ 事件過濾 ◆ 即時事件視覺效果 ◆ 事件儲存 ◆ 資料保留規則 ◆ 事件儲存肯定認證 ◆ FIPS 啟用 ◆ 手動觸發動作 ◆ 事件的手動建立和管理 ◆ 事件動作和工作流程 ◆ iTRAC 工作流程	是	是
動作 ◆ 關連性觸發的活動 (僅適用於關連已啟用) ◆ 路由規則觸發的活動 (僅適用於規則已啟用) ◆ 手動觸發動作	是	是
路由規則 ◆ 事件路由 (外部) ◆ 路由規則觸發的動作 (僅適用於動作已啟用)	是	是
Sentinel Link	是	是
關聯性 ◆ 即時模式關連 ◆ 關連規則觸發的動作 (僅適用於動作已啟用) ◆ 警告分級 ◆ 警告儀表板	是	否

服務與功能	Sentinel Enterprise	Sentinel for Log Management
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
安全性智慧 • 異常規則 • 即時統計分析	是	否
即時統計分析	是	否
授權過期	從未：	從未：
EPS 限制	未設限	未設限

4.1 Sentinel 授權

本節提供各種 Sentinel 授權相關資訊。

- 第 4.1.1 節「試用版授權」(第 33 頁)
- 第 4.1.2 節「免費授權」(第 33 頁)
- 第 4.1.3 節「企業授權」(第 34 頁)

4.1.1 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 32 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 將依此調整過期日。

試用版授權過期後，系統將以基礎授權金鑰執行，啟用有限的功能，且事件率上限為 25 EPS。基礎授權又稱為免費授權。

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。

4.1.2 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。免費授權沒有過期日。

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：NetIQ 不提供 Sentinel 免費版本技術支援及產品更新。

4.1.3 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某些功能、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《NetIQ Sentinel 管理指南》中的 *「新增授權金鑰」*。

5 符合系統需求

Sentinel 執行可能會依環境需求而異，因此建議您先諮詢 NetIQ 諮詢服務或任何的 NetIQ Sentinel 合作夥伴，再決定 Sentinel 架構。

如需要建議硬體、支援作業系統、裝置平台及瀏覽器的資料，請參閱 NetIQ Sentinel 技術資訊網站。

5.1 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。請參閱 Sentinel 外掛程式網站中的連接器和收集器文件。

5.2 虛擬環境

Sentinel 在 VMware ESX 伺服器上受到廣泛測試及完全支援。在設定虛擬環境時，虛擬機器必須具備 2 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媲美的效能結果，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。

如需有關實體機器建議的詳細資訊，請參閱第 5 章 「符合系統需求」(第 35 頁)。

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。您可在 Sentinel 上放置多種載入。本章綜覽擴充 Sentinel 佈署時最重要的考量。NetIQ Services 或 NetIQ Partner Services 專業人員可與您共同合作，為您獨特的環境更周全地設計完整的系統。

6.1 分散式佈署的優點

依預設，Sentinel 伺服器包括下列元件：

- **收集者管理員：**收集器管理員為 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收集器管理員。
- **關連引擎：**關連引擎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。
- **NetFlow 收集器管理員：**NetFlow 收集器管理員會收集路由器、交換器和防火牆等網路裝置的網路流程資料 (NetFlow、IPFIX 等)。網路流程資料可說明關於主機之間所有網路連接的基本資訊 (包括轉送的封包和位元組)，協助您以視覺方式呈現個別主機或整個網路的行為。

重要：針對生產環境，NetIQ Corporation 建議設定分散式部署，因為如此可隔離不同電腦上的資料收集元件。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。

6.1.1 額外收集器管理員的優點

依預設，Sentinel 伺服器含有收集器管理員。不過，針對生產環境，分散式收集器管理員在收到大量資料時會提供更好的隔離。在這種情況下，分散式收集器管理員可能超載，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收集器管理員可提供多項優勢：

- **改善系統效能：**其他收集器管理員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：**如果收集器管理員與事件來源共存，則可對資源執行過濾、加密以及資料壓縮。
- **檔案快取：**其他收集器管理員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收集器管理員。這些遠端收集器管理員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。如需有關安裝額外收集器管理員的詳細資訊，請參閱第 12.4 節 「安裝收集器管理員和關連引擎」 (第 69 頁)。

附註：您不可在單一系統上安裝多個收集器管理員。您可在遠端系統上安裝其他收集器管理員，然後再將其連接到 Sentinel 伺服器。

6.1.2 增加關連引擎的優點

您可以在個別的伺服器上部署多個關連引擎，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？極高的環境，安裝多個關連引擎並重新部署部分規則到新的關連引擎會比較有利。多個關連引擎可隨著 Sentinel 系統加入更多資料來源或事件發生？提高時加以延伸。如需安裝其他關連引擎的相關資訊，請參閱 第 12.4 節 「安裝收集器管理員和關連引擎」 (第 69 頁).

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

6.1.3 額外 NetFlow 收集器管理員的優點

NetFlow 收集器管理員會收集網路裝置的網路流程資料。您應安裝額外 NetFlow 收集器管理員，而不是使用 Sentinel 伺服器上的 NetFlow 收集器管理員，以將系統資源釋出給其他重要功能，例如事件儲存和搜尋。

您可在以下情境中安裝額外的 NetFlow 收集器管理員：

- 在使用許多網路裝置及高速率網路流程資料的環境中，您可安裝多個 NetFlow 收集器管理員來分散負載。
- 如果您是在多重租用戶環境中，您應為每個租用戶安裝個別的 NetFlow 收集器管理員，以按租用戶收集不同的網路流程資料。

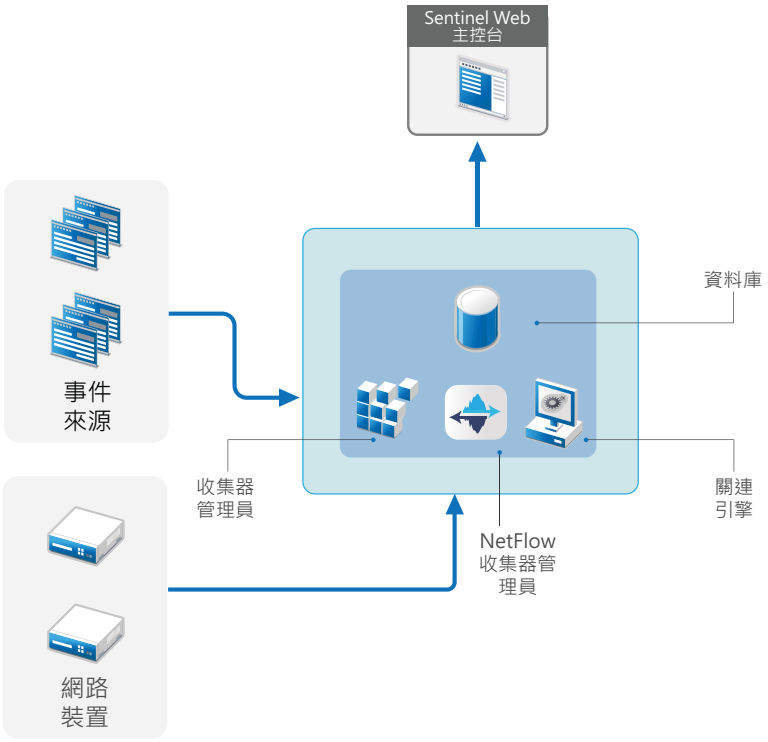
如需有關安裝額外 NetFlow 收集器管理員的詳細資訊，請參閱第 14 章 「NetFlow 收集器管理員安裝」 (第 83 頁)。

6.2 整合式佈署

最基本的佈署選項是整合式系統，在單一機器上包含所有 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、不斷變動的負載，以及不同元件間的細微資源衝突都可能引發效能問題。

重要：針對生產環境，NetIQ Corporation 建議設定分散式部署，因為如此可隔離不同電腦上的資料收集元件。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 6-1 整合式佈署

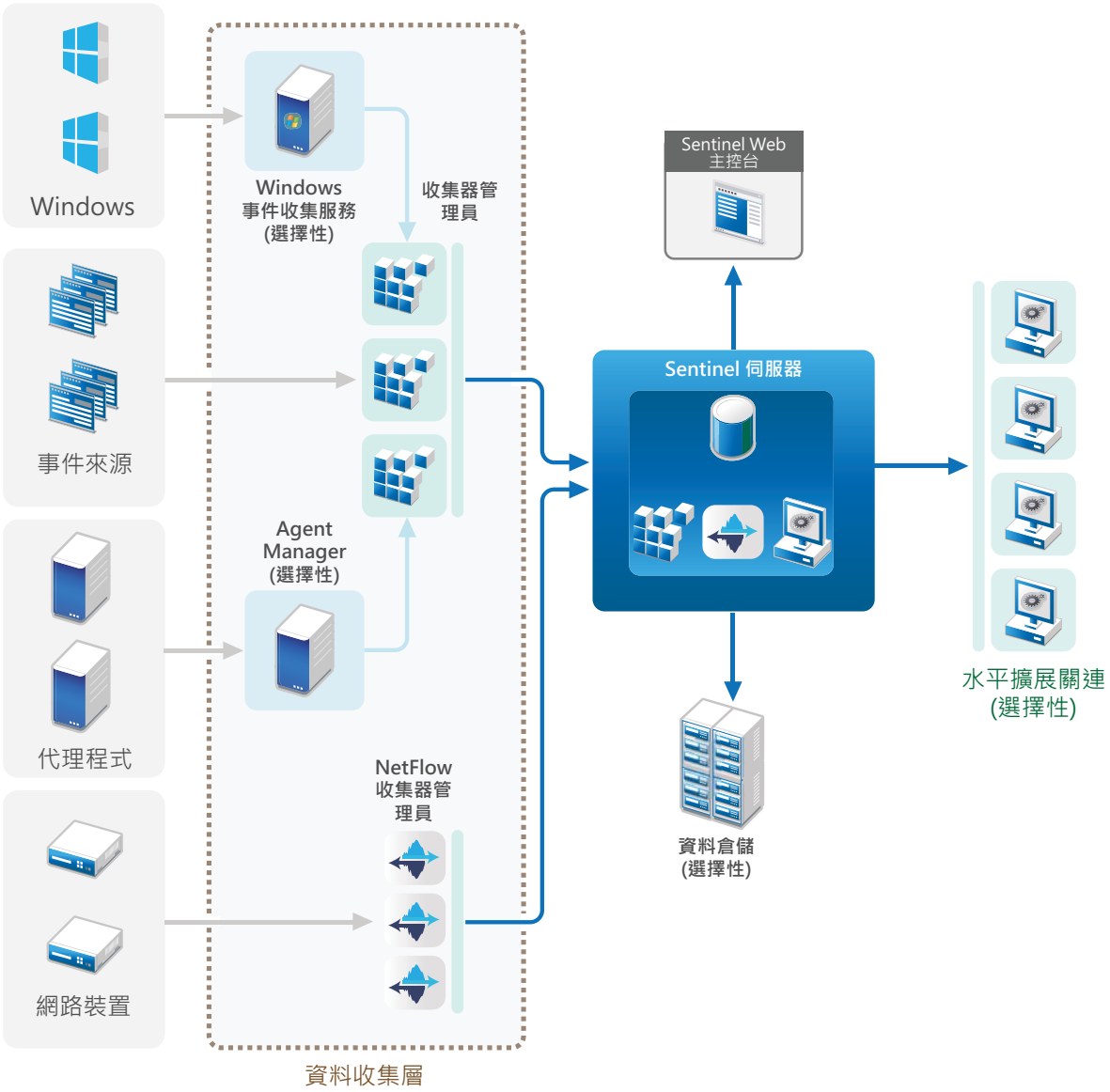


6.3 單層分散式佈署

單層佈署增加了監控 Windows 機器的能力，也可處理比整合式佈署更大的載入。資料集合和關連可透過新增從中央 Sentinel 伺服器卸載處理的收集器管理員、NetFlow 收集器管理員和關連引擎機器來擴充。除了處理事件載入、關連規則和網路流程資料，遠端收集器管理員、關連引擎和 NetFlow 收集器管理員也會將中央 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。

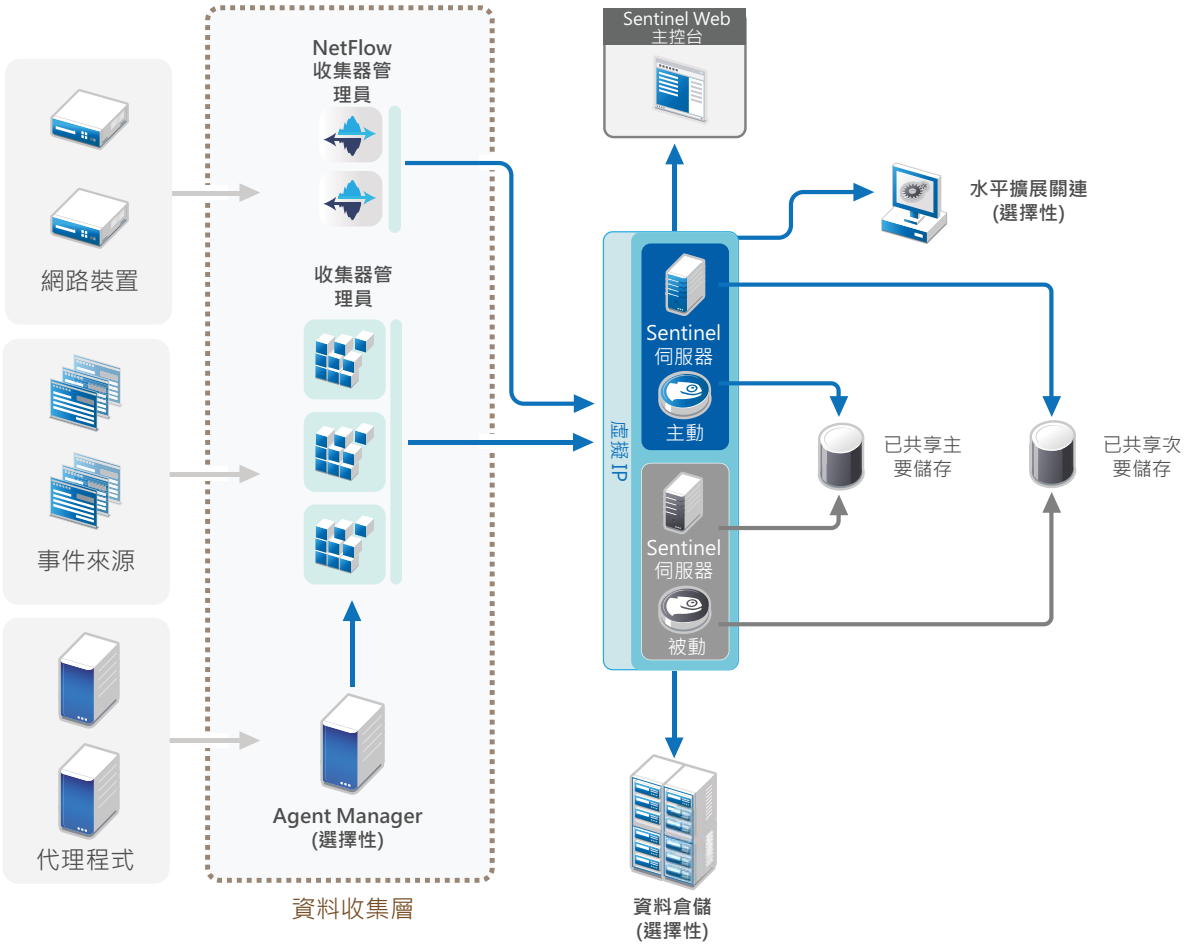
圖 6-2 單層分散式佈署



6.4 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 VI 部分「部署 Sentinel 以提供高可用性」(第 127 頁)。

圖 6-3 高可用性單層分散式佈署

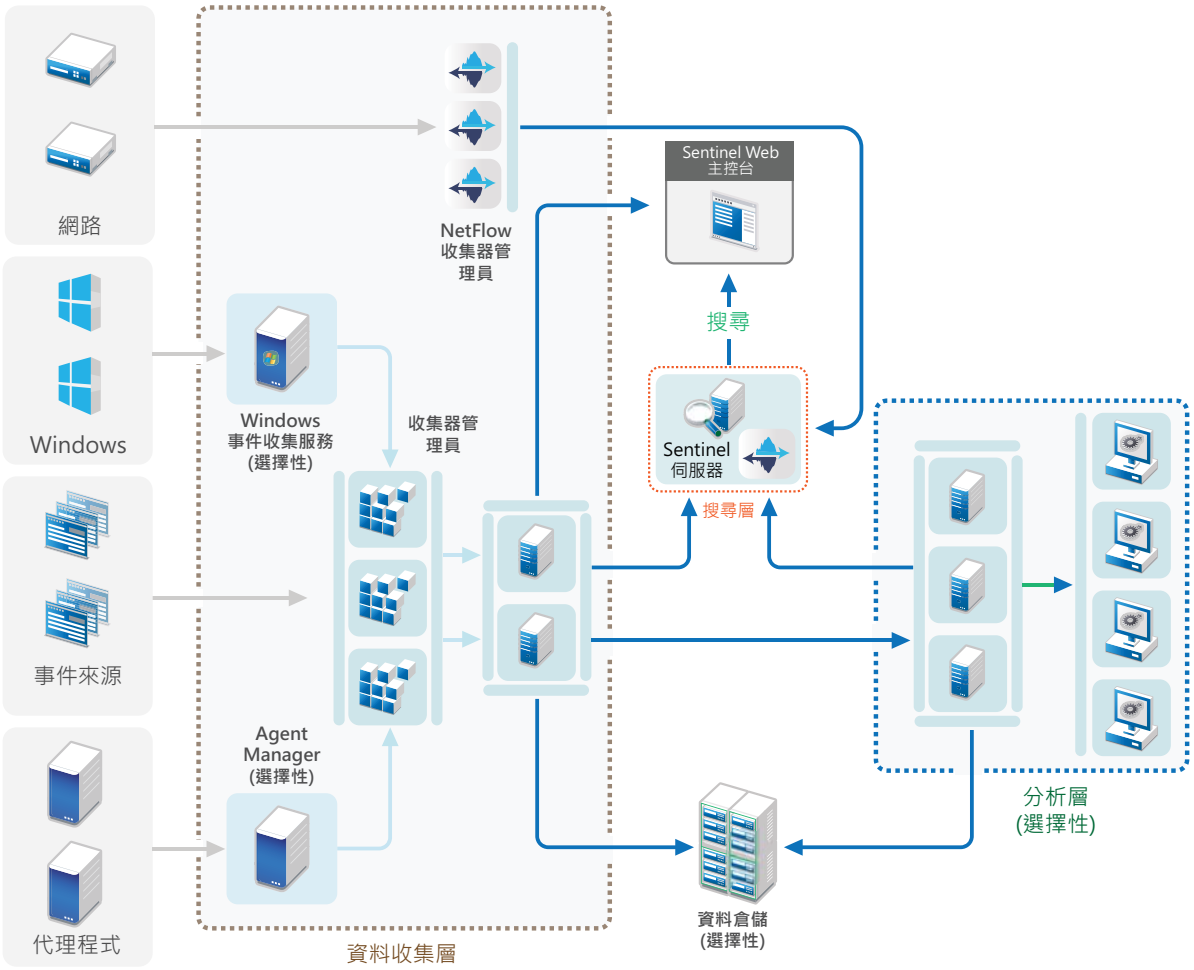


6.5 兩層和三層分散式佈署

此佈署可讓您超越單一中央 Sentinel 伺服器的載入處理能力，並利用 Sentinel Link 和 Sentinel 分散式搜尋功能共享多個 Sentinel 例項的處理載入。資料集合在多個 Sentinel 伺服器上為載入平衡，各有多個收集器管理員，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 分散式搜尋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，這個佈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。

網路流程資料會儲存在搜尋層級中，以方便從搜尋結果瀏覽至關聯式網路流量分析。

圖 6-4 兩層和三層分散式佈署



6.6 規劃資料儲存的分割區

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，以確保能進行適當的磁碟使用率計算。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，請參閱第 6.6.4 節「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」。

6.6.1 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「第 6.6.4 節「Sentinel 目錄結構」(第 44 頁)」詳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。

6.6.2 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，請參閱第 13.3.2 節「建立分割區」(第 80 頁)。

6.6.3 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)。

n. 分割區 v. 分割，製作 ... 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
暫存	/tmp	30 GB	作業系統和 Sentinel 暫存檔案的位置；將此隔離在不同的分割區上可保護應用程式資料，避免在失控程序填滿暫存空間時損壞。
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。

6.6.4 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
- 組態檔案位於 /etc/opt/novell/sentinel 目錄中
- 程序 ID (PID) 檔案位於 /var/run/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。

7 FIPS140-2 模式的部署考量因素

您也可以將 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 遠端收集器管理員、Sentinel 遠端關連引擎、Sentinel Web UI、Sentinel 控制中心和 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。

7.1 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 RHEL 6.3 提供的 NSS 加密模組是經過 FIPS 140-2 驗證。由 SLES 11 SP3 提供的 NSS 加密模組尚未正式經過 FIPS 140-2 驗證，但是我們目前正致力讓 SUSE 模組通過 FIPS 140-2 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 RHEL 6.2 FIPS 140-2 證書的相關資訊，請 參閱《{ *通過 FIPS 140-1 和 FIPS 140-2 驗證的加密模組*》。

7.1.1 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-4.9-1.el6.x86_64
- nss-sysinit-3.13.3-6.el6.x86_64
- nss-util-3.13.3-2.el6.x86_64
- nss-softokn-freebl-3.12.9-11.el6.x86_64
- nss-softokn-3.12.9-11.el6.x86_64
- nss-3.13.3-6.el6.x86_64
- nss-tools-3.13.3-6.el6.x86_64

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。

7.1.2 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：

- libfreebl3-3.13.1-0.2.1
- mozilla-nspr-4.8.9-1.2.2.1
- mozilla-nss-3.13.1-0.2.1
- mozilla-nss-tools-3.13.1-0.2.1

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。

7.2 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

  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 103 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 108 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。
- NetIQ 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 Sentinel 外掛程式的相關資訊，請參閱 Sentinel 外掛程式網站。若您想要針對其中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。

7.3 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。	第 7.4 節「部署情境」(第 47 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。	第 12.2.2 節「自訂安裝」(第 67 頁)。 第 12.3 節「執行靜默安裝」(第 68 頁) 第 20 章「在現有 Sentinel 安裝中啟用 FIPS 140-2 模式」(第 99 頁)
設定 Sentinel 外掛程式在 FIPS 140-2 模式中執行。	第 21.5 節「設定 Sentinel 外掛程式在 FIPS 140-2 模式中執行」(第 103 頁)。
將證書輸入 Sentinel FIPS KeyStore。	第 21.6 節「輸入證書到 FIPS Keystore 資料庫」(第 108 頁)

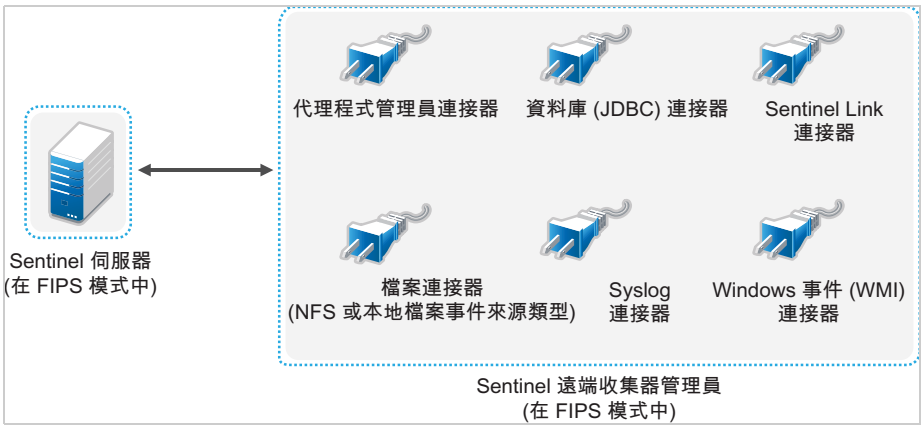
附註：NetIQ 強烈建議先將 Sentinel 系統備份，再開始轉換到 FIPS 模式。若因為某些原因造成伺服器必須回復到非 FIPS 模式，支援執行此動作的唯一方法是從備份還原。如需回復到非 FIPS 模式的相關資訊，請參閱「回復 Sentinel 到非 FIPS 模式」(第 108 頁)。

7.4 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。

7.4.1 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收集器管理員來收集。您可能會有一個以上的遠端收集器管理員。



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 99 頁)。

---

2 您的 Sentinel 遠端收集器管理員必須是以 FIPS 140-2 模式執行。

附註：若您的遠端收集器管理員 (新安裝或已升級) 是以非 FIPS 模式執行，您必須啟用遠端收集器管理員上的 FIPS。如需詳細資訊，請參閱「啟用遠端收集器管理員和關連引擎上的 FIPS 140-2 模式」(第 99 頁)。

---

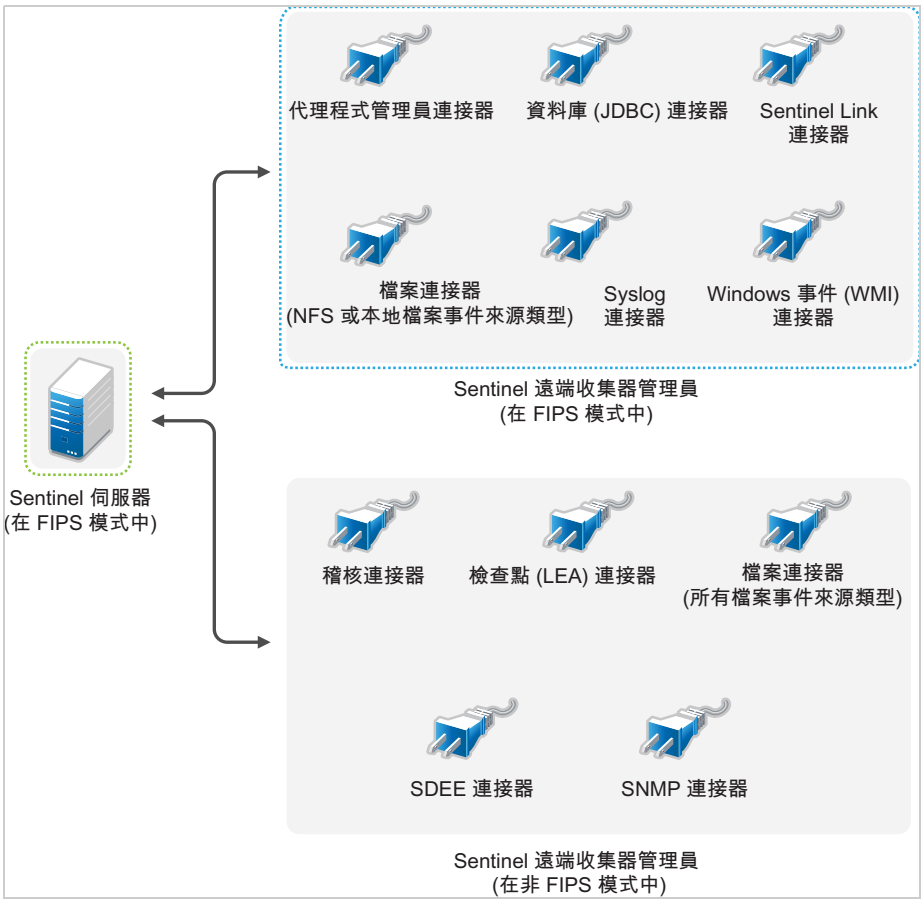
3 請確定 FIPS 伺服器和遠端收集器管理員可互相通訊。

4 將遠端關連引擎 (若有) 轉換為在 FIPS 模式中執行。如需詳細資訊，請參閱「啟用遠端收集器管理員和關連引擎上的 FIPS 140-2 模式」(第 99 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 103 頁)。

7.4.2 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。我們假設此環境與 Sentinel 伺服器相關，而且資料是透過遠端收集器管理員來收集。您可能會有一個以上的遠端收集器管理員。



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收集器管理員，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 模式的連接器和尚未支援 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 99 頁)。

---

2 請確定一個遠端收集器管理員是以 FIPS 140-2 模式執行，另一個遠端收集器管理員繼續以非 FIPS 模式執行。

2a 若您沒有已啟用 FIPS 140-2 模式的遠端收集器管理員，您必須在遠端收集器管理員上啟用 FIPS 模式。如需詳細資訊，請參閱「啟用遠端收集器管理員和關連引擎上的 FIPS 140-2 模式」(第 99 頁)。

2b 更新在非 FIPS 遠端收集器管理員上的伺服器證書。如需詳細資訊，請參閱「更新在遠端收集器管理員和關連引擎上的伺服器證書」(第 103 頁)。

3 確定兩個遠端收集器管理員能與已啟用 FIPS 140-2 的 Sentinel 伺服器通訊。

4 將遠端關連引擎 (若有) 轉換為在 FIPS 模式中執行。如需詳細資訊，請參閱「啟用遠端收集器管理員和關連引擎上的 FIPS 140-2 模式」(第 99 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 103 頁)。

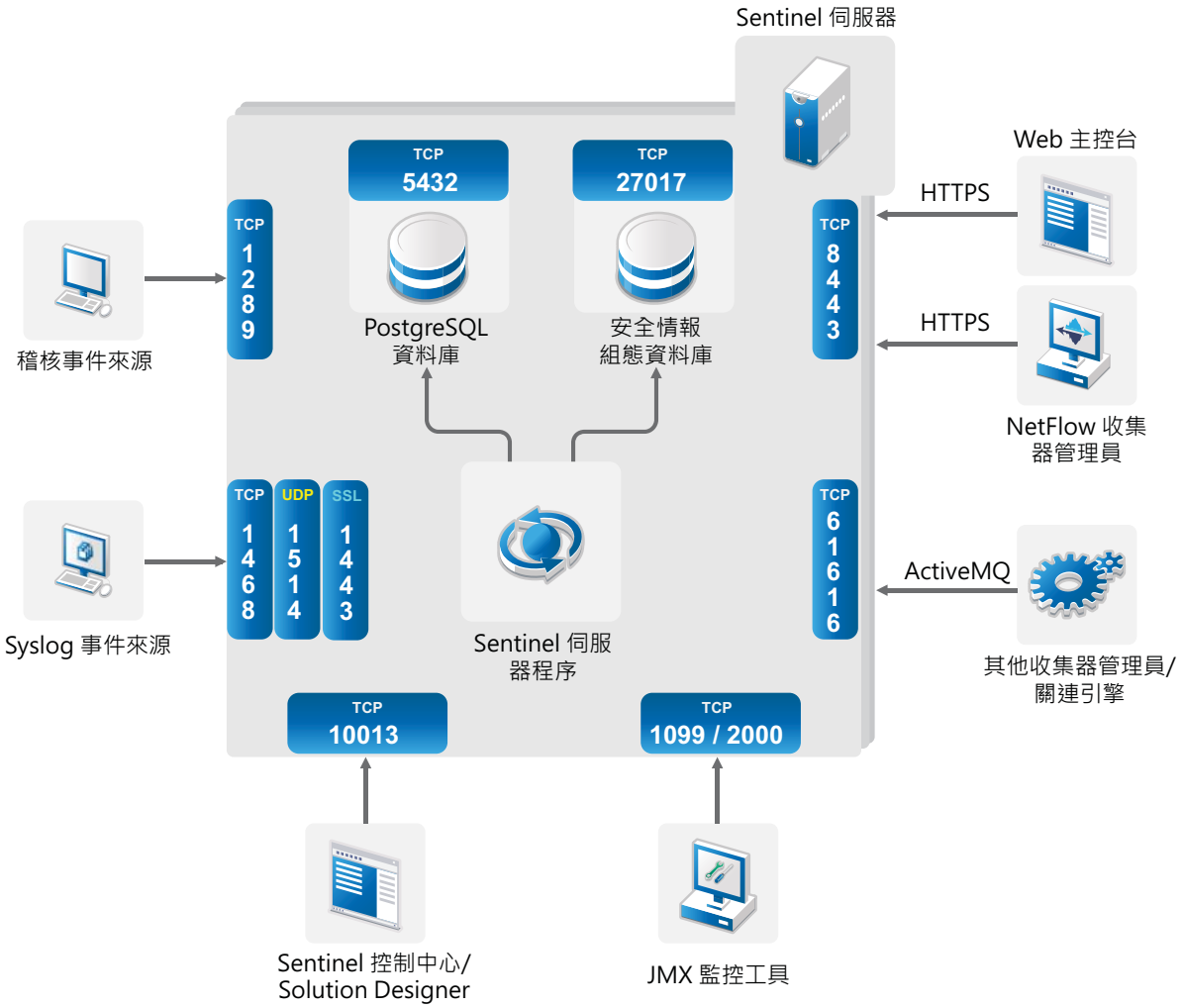
5a 部署在以 FIPS 模式執行的遠端收集器管理員上支援 FIPS 140-2 模式的連接器。

5b 部署在非 FIPS 遠端收集器管理員上不支援 FIPS 140-2 模式的收集器。

8 使用的連接埠

Sentinel 使用不同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。下圖說明 Sentinel 中使用的連接埠：

圖 8-1 *Sentinel 中使用的連接埠*



- 第 8.1 節「Sentinel 伺服器連接埠」(第 52 頁)
- 第 8.2 節「收集器管理員連接埠」(第 54 頁)
- 第 8.3 節「關連引擎連接埠」(第 54 頁)
- 第 8.4 節「NetFlow 收集器管理員連接埠」(第 55 頁)

8.1 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。

8.1.1 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 介面。
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。

8.1.2 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	選擇性	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。
UDP 1514	向內	選擇性	用於 syslog 訊息。
TCP 8443	向內	必要	用於 HTTPS 通訊和從 NetFlow 收集器管理員收到的連接。
TCP 1443	向內	選擇性	用於 SSL 加密 syslog 訊息。
TCP 61616	向內	選擇性	用於從收集器管理員和關連引擎收到的連接。
TCP 10013	向內	必要	用於 Sentinel 控制中心和 Solution Designer。
TCP 1468	向內	選擇性	用於 syslog 訊息。
TCP 10014	向內	選擇性	遠端收集器管理員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，遠端收集器管理員使用 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 URL (https://secure-www.novell.com/sentinel/download/advisor/)。

連接埠	方向	必要 / 選用	描述
TCP 8443	向外	選擇性	若使用了分散式搜尋，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。

8.1.3 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。
TCP 4984	向內	必要	由 Sentinel 裝置管理主控台 (WebYaST) 所用。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 NetIQ 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。

8.2 收集器管理員連接埠

收集器管理員使用以下連接埠與其他元件通訊。

8.2.1 網路連接埠

若要使 Sentinel 收集器管理員正常運作，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	選擇性	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。

8.2.2 收集器管理員裝置專用連接埠

除了上述連接埠之外，Sentinel 收集器管理員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	由 Sentinel 裝置管理主控台 (WebYaST) 所用。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	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	向外	必要	啟始網際網路上 NetIQ 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。

8.3 關連引擎連接埠

關連引擎使用以下連接埠與其他元件通訊。

8.3.1 網路連接埠

若要使 Sentinel 關連引擎正常運作，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	選擇性	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。

8.3.2 關連引擎裝置專用連接埠

除了上述連接埠之外，Sentinel 關連引擎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	由 Sentinel 裝置管理主控台 (WebYaST) 所用。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 NetIQ 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。

8.4 NetFlow 收集器管理員連接埠

NetFlow 收集器管理員使用以下連接埠與其他元件通訊：

連接埠	方向	必要 / 選用	描述
HTTPS 8443	向外	必要	啟始 Sentinel 伺服器的連接。
3578	向內	必要	用於從網路裝置接收網路流程資料。

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。

9.1 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。
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，請參閱第 12.2 節「執行互動式安裝」(第 65 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，然後使用檔案執行無人管理安裝。如需靜默安裝的其他資訊，請參閱第 12.3 節「執行靜默安裝」(第 68 頁)。

9.2 裝置安裝

裝置安裝會安裝 SLES 11 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
- 直接部署在硬體伺服器上的硬體裝置 Live DVD 影像

如需裝置安裝的其他資訊，請參閱第 13 章 「裝置安裝」(第 75 頁)。

III 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

Sentinel 安裝會在 Sentinel 伺服器上安裝下列元件：

- **Sentinel 伺服器程序：**這是 Sentinel 的主要元件。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。
- **Web 伺服器：**Sentinel 使用 Jetty 做為其 Web 伺服器，藉此確保連往 Sentinel Web 介面的連線安全無虞。
- **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：**儲存安全情報資料。
- **收集者管理員：**收集器管理員為 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收集器管理員。
- **NetFlow 收集器管理員：**NetFlow 收集器管理員會收集路由器、交換器和防火牆等網路裝置的網路流程資料 (NetFlow、IPFIX 等)。網路流程資料可說明關於主機之間所有網路連接的基本資訊 (包括轉送的封包和位元組)，協助您以視覺方式呈現個別主機或整個網路的行為。
- **關連引擎：**關連引擎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《*NetIQ 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。您可以從 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

Sentinel 的結構可靈活調整，若事件發生率可能很高，您可將元件配送到多部機器，以確保系統可達到最佳效能。針對生產環境，NetIQ Corporation 建議設定分散式佈署，因為可隔離不同機器上的資料收集元件，對於處理特殊圖文集和其他異常以提高系統穩定性是不可或缺的要素。如需詳細資訊，請參閱第 6.1 節「分散式佈署的優點」(第 37 頁)。

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 35 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 157 頁)。
- ❒ 若您計劃安裝授權版本，請向 NetIQ 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 51 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。
- ❒ **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

12 傳統安裝

本章節提供 Sentinel 各種安裝方法的相關資訊。

12.1 瞭解安裝選項

。/install-sentinel --help 會顯示以下選項：

選項	值	描述
--location	目錄	指定將 Sentinel 安裝在根目錄 (/) 之外的目錄。
-m, --manifest	檔案名稱	指定要使用的產品資訊清單檔案 (不使用預設的資訊清單檔案)。
--no-configure		指定不在安裝完成後設定產品。
-n, --no-start		指定不在安裝或組態完成後啟動或重新啟動 Sentinel。
-r, --recordunattended	檔名	指定檔案以記錄無人管理安裝所用的參數。
-u, --unattended	檔名	使用指定檔案中的參數，以將 Sentinel 安裝在無人管理的系統上。
-h, --help		顯示可在安裝 Sentinel 時使用的選項。
-l, --log-file	檔名	將記錄訊息記錄在檔案中。
--no-banner		隱藏標題頁訊息。
-q, --quiet		顯示較少訊息。
-v, --verbose		在安裝時顯示所有訊息。

12.2 執行互動式安裝

本節提供標準和自定安裝的相關資訊。

12.2.1 標準安裝

執行標準安裝的步驟如下：

1. 從 NetIQ 下載網站下載 Sentinel 安裝檔：
   1a. 在「**產品或技術**」欄位中，瀏覽並選取 **SIEM-Sentinel**。
   1b. 按一下「**搜尋**」。
   1c. 按一下 **Sentinel Evaluation** 的「**下載**」欄中的按鈕。
   1d. 按一下「**前往下載**」，然後指定客戶名稱和密碼。
   1e. 按一下「**下載**」，以取得您平台的安裝版本。
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 Web 介面，請在網頁瀏覽器中指定下列 URL：

```
https://<IP_Address_Sentinel_server>:8443.
```

<IP_Address_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。

12.2.2 自訂安裝

如果利用自定組態安裝 Sentinel，您可以指定授權金鑰、針對不同的使用者變更密碼，以及針對用來與內部元件互動的各個連接埠指定值。

1 從 NetIQ 下載網站下載 Sentinel 安裝檔：

   1a 在「**產品或技術**」欄位中，瀏覽並選取 **SIEM-Sentinel**。

   1b 按一下「**搜尋**」。

   1c 按一下 **Sentinel 7.2 Evaluation** 的「**下載**」欄中的按鈕。

   1d 按一下「**前往下載**」，然後指定客戶名稱和密碼。

   1e 按一下「**下載**」，以取得您平台的安裝版本。

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 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>`

4 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。

5 按下空格鍵，以完整讀取授權合約。

6 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。

7 指定 2 以執行 Sentinel 自定組態。

8 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。

9 指定管理員使用者 (admin) 的密碼，並再次確認密碼。

10 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。

11 指定應用程式使用者 (appuser) 的密碼，並再次確認密碼。

12 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。

13 變更連接埠後，請指定 7 來完成作業。

14 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。

15 ***若要在 FIPS 140-2 模式中啟用 Sentinel***，請按 y。

15a 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。

15b 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

15c 按照在「第 21 章 「以 FIPS 140-2 模式操作 Sentinel」(第 101 頁)」中提到的任務，完成 FIPS 140-2 模式組態。

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 Web 介面，請在網頁瀏覽器中指定下列 URL：

```
https://<IP_Address_Sentinel_server>:8443.
```

<IP_Address_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。

12.3 執行靜默安裝

如果您需要在部署中安裝多個 Sentinel 伺服器，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。您可以在利用標準組態或自定組態安裝 Sentinel 時記錄安裝參數。

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，請參閱第 12.2.1 節「標準安裝」(第 66 頁) 或第 12.2.2 節「自訂安裝」(第 67 頁)。

若要在 FIPS 140-2 模式中啟用 Sentinel，請確定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 NetIQ 下載網站下載安裝檔。

2 以 root 身分登入要安裝 Sentinel 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安裝 Sentinel：

```
./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。

5 **(條件式) 若選擇啟用 FIPS 140-2 模式，**按照在「第 21 章 「以 FIPS 140-2 模式操作 Sentinel」(第 101 頁)」中提到的任務，完成 FIPS 140-2 模式組態。

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。

12.4 安裝收集器管理員和關連引擎

Sentinel 預設安裝收集器管理員和關連引擎。針對生產環境，NetIQ Corporation 建議設定分散式佈署，因為可隔離不同機器上的資料收集元件，對於處理特殊圖文集和其他異常以提高系統穩定性是不可或缺的要素。如需有關安裝額外元件有何優點的詳細資訊，請參閱第 6.1 節 「分散式佈署的優點」(第 37 頁)。

重要：您必須在不同的系統上安裝其他收集器管理員或關連引擎。收集器管理員或關連引擎不得位於安裝 Sentinel 伺服器的相同系統上。

- 第 12.4.1 節 「安裝核對清單」(第 69 頁)
- 第 12.4.2 節 「安裝收集器管理員和關連引擎」(第 69 頁)
- 第 12.4.3 節 「新增收集器管理員或關連引擎的自定 ActiveMQ 使用者」(第 70 頁)

12.4.1 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 35 頁)。
- ❒ 使用網路時間通訊協定 (NTP) 同步化時間。
- ❒ 收集器管理員需要網路連接至 Sentinel 伺服器上的訊息匯流排連接埠 (61616)。在開始安裝收集器管理員之前，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。

12.4.2 安裝收集器管理員和關連引擎

1 在網頁瀏覽器中指定下列 URL 以啟動 Sentinel Web 介面：

```
https://<IP_Address_Sentinel_server>:8443.
```

<IP_Address_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收集器管理員或關連引擎：

針對收集器管理員：

```
./install-cm
```

針對關連引擎：

```
./install-ce
```

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 在出現提示時，指定 1 可繼續進行標準組態。

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。

將會顯示 Sentinel 伺服器證書。

13 指定收集器管理員或關連引擎的 ActiveMQ 使用者身分證明。

ActiveMQ 使用者身分證明儲存在 Sentinel 伺服器的 /<*install_dir*>/etc/opt/novell/sentinel/config/activemqusers.properties 檔案中。

14 當系統提示您接受證書時，請使用下列指令來驗證證書：

```
/opt/novell/sentinel/jre/bin/keytool -list -keystore
/etc/opt/novell/sentinel/config/.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。

15 若證書輸出與 Sentinel 伺服器證書相符，則接受證書。

16 輸入 yes 或 y 以啟用 Sentinel 中的 FIPS 140-2 模式，並繼續使用 FIPS 組態。

17 依提示繼續安裝，直到完成為止。

12.4.3 新增收集器管理員或關連引擎的自定 ActiveMQ 使用者

Sentinel 建議您使用遠端收集器管理員和關連引擎的預設 ActiveMQ 使用者名稱。然而，如果您安裝了多個遠端收集器管理員，並且想要個別加以識別，則可以建立新 ActiveMQ 使用者：

1 以具有安裝檔案存取權限的 Sentinel 使用者身分登入伺服器。

2 開啟 activemqgroups.properties 檔案。

該檔案位於 /<*install_dir*>/etc/opt/novell/sentinel/config/ 目錄中。

3 加入以逗號分隔的新 ActiveMQ 使用者名稱，如下所示：

針對收集器管理員，在收集器管理員區段加入新使用者。例如：

```
cm=collectormanager,cmuser1,cmuser2,...
```

針對關連引擎，在管理區段加入新使用者。例如：

```
admins=system,correlationengine,ceuser1,ceuser2,...
```

4 儲存然後關閉該檔案。

5 開啟 activemqusers.properties 檔案。

該檔案位於 /<*install_dir*>/etc/opt/novell/sentinel/config/ 目錄中。

6 針對在步驟 3 中建立的 ActiveMQ 使用者新增密碼。

密碼可以是任何隨機字串。例如：

針對收集器管理員使用者：

```
system=c7f34372ecd20d831cceb29e754e5ac9
collectormanager=1c51ae56
cmuser1=1b51de55
cmuser2=1a51ce57
```

針對關連引擎使用者：

```
system=c7f34372ecd20d831cceb29e754e5ac9
correlationengine=68790d7a
ceuser1=69700c6d
ceuser2=70701b5c
```

7 儲存然後關閉該檔案。

8 重新啟動 Sentinel 伺服器。

12.5 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。雖然安裝會順利地繼續進行，但 NetIQ Corporation 不支援 novell 使用者以外的非 root 安裝。

1 從 NetIQ 下載網站下載安裝檔。

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
收集者管理員	**預設位置：**./install-cm
	非預設位置：./install-cm --location=/foo
關連引擎	**預設位置：**./install-ce
	非預設位置：./install-cm --location=/foo
NetFlow 收集器管理員	**預設位置：**./install-netflow
	非預設位置：./install-netflow --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，請參閱第 12.2.1 節「標準安裝」(第 66 頁) 或第 12.2.2 節「自訂安裝」(第 67 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*>
收集者管理員	**預設位置：**./install-cm -u <*response_file*>
	非預設位置：./install-cm --location=/foo -u <*response_file*>
關連引擎	**預設位置：**./install-ce -u <*response_file*>
	非預設位置：./install-ce --location=/foo -u <*response_file*>
NetFlow 收集器管理員	**預設位置：**./install-netflow -u <*response_file*>
	非預設位置：./install-netflow --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「第 12.2.1 節「標準安裝」(第 66 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 7」中的步驟 14 到第 12.2.2 節「自訂安裝」(第 67 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 Web 介面，請在網頁瀏覽器中指定下列 URL：

```
https://<IP_Address_Sentinel_server>:8443.
```

<IP_Address_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。

13 裝置安裝

Sentinel 裝置是以 SUSE Studio 為基礎而建置的立即可用軟體裝置。這項裝置結合了強化的 SLES 作業系統和 Sentinel 軟體整合式更新服務，可讓客戶運用現有的投資，同時提供簡單而流暢的使用者經驗。安裝 Sentinel 裝置前，請先查看支援的 SLES 版本說明中的新功能和已知問題。

Sentinel 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 NetIQ Sentinel 技術資訊網站。

13.1 安裝 Sentinel ISO 裝置

本節提供利用 ISO 裝置影像安裝 Sentinel、收集器管理員和關連引擎的相關資訊。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)。

13.1.1 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：

- (條件式) 若您在空機硬碟上安裝 Sentinel ISO 裝置，請自支援網站下載裝置 ISO 磁碟影像，解壓縮檔案，並製作成 DVD。
- 確定您要安裝該 ISO 磁碟影像的系統包含至少 4.5 GB 記憶體以完成安裝。
- 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。

13.1.2 安裝 Sentinel

安裝 Sentinel ISO 裝置：

1. 至 NetIQ 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，並開啟。

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 選取開機功能表中的頂端項目，來執行 Live DVD 裝置影像。

安裝作業會先檢查可用的記憶體和磁碟空間。如果可用記憶體少於 2.5 GB，安裝作業即會自動終止。如果可用記憶體大於 2.5 GB 但少於 6.7 GB，安裝作業會顯示一則訊息，提示您記憶體少於建議的大小。若要繼續安裝，請輸入 y，若不想繼續，請輸入 n。

4 選取您選擇的語言，然後按一下**「下一步」**。

5 選取鍵盤組態，然後按一下**「下一步」**。

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

7 閱讀並接受「NetIQ Sentinel 使用者授權合約」。按「**下一步**」

8 在「主機名稱」與「網域名稱」頁面中，指定主機名稱與網域名稱。不選**指定主機名稱以回送 IP**。

9 按一下**「下一步」**。

10 選擇下列其中一個連接設定選項：

- 若要使用目前的網路連線設定，請在「網路組態 II」頁面中選取**「使用下列組態」**。
- 若要變更網路連線設定，請按一下**「變更」**，接著執行想要的變更。

11 按一下**「下一步」**。

12 設定「時間與日期」，然後按一下**「下一步」**。

若要在安裝之後變更 NTP 組態，請使用裝置指令行中的 YaST。您可以使用 WebYast 來變更時間與日期設定，而不是 NTP 組態。

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
```

13 設定 root 密碼，然後按一下**「下一步」**。

14 設定 Sentinel 管理員密碼，然後按一下**「下一步」**。

確定選取了**「將 Sentinel 裝置安裝至硬碟 (僅適用於「即時 DVD」影像)」**，以將裝置安裝到實體伺服器上。預設會選取此核取方塊。

若取消選取此核取方塊，裝置便不會安裝到實體伺服器上，而且只會以「即時 DVD」模式執行，前往步驟 21。

15 在 YaST2 即時安裝程式主控台上，選取**「下一步」**。

YaST2 即時安裝程式主控台會將裝置安裝到硬碟。YaST2 即時安裝程式主控台會重複部分先前的安裝步驟。

16 **「建議的分割」**螢幕會顯示建議的分割區設定。檢閱分割區設定，設定安裝 (若有需要)，然後選取**「下一步」**。只有在您熟悉在 SLES 中設定分割區時才修改這些設定。

您可使用螢幕上各種分割選項來設定分割區設定。如需關於設定分割區的詳細資訊，請參閱《*SLES 文件*》中的「使用 YaST 分割器」和第 6.6 節「規劃資料儲存的分割區」(第 42 頁)。

17 輸入根部密碼，然後選取**「下一步」**。

18 **「即時安裝設定」**螢幕會顯示選取的安裝設定。檢閱設定，設定各項設定 (若有需要)，然後選取**「安裝」**。

19 選取**「安裝」**以確認「安裝」。

請等待安裝完成。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。

20 選取「**確定**」將系統重新開機。

21 將主控台中顯示的裝置 IP 位址記下來。

22 在主控台中輸入根部使用者名稱與密碼，以登入裝置。

使用者名稱的預設值為 root，密碼的預設值為您在步驟 17 中設定的密碼。

23 繼續執行 第 13.3 節「安裝裝置後的組態」(第 79 頁)。

13.1.3 安裝收集器管理員和關連引擎

安裝收集器管理員或關連引擎的程序相同，不過您必須先從 NetIQ 下載網站下載相關 ISO 裝置檔案。

1 完成在 第 13.1.2 節「安裝 Sentinel」(第 75 頁) 中的步驟 1 至 步驟 13。

2 指定收集器管理員或關連引擎的下列組態：

- **Sentinel 伺服器的主機名稱或 IP 位址：**指定收集器管理員或關連引擎應連接之 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。
- **通訊通道使用者名稱：**指定通訊通道使用者名稱 (收集器管理員或關連引擎使用者名稱)。
- **通訊通道使用者密碼：**指定通訊通道使用者密碼。

  通訊通道使用者身分證明儲存在 Sentinel 伺服器的 /<*install_dir*>/etc/opt/novell/sentinel/config/activemqusers.properties 檔案中。

  若要驗證身分證明，請參見 activemqusers.properties 檔案中的下列文字行：

  針對收集器管理員：

  collectormanager=<*password*>

  在此範例中，collectormanager 為使用者名稱，而對應的值為密碼。

  針對關連引擎：

  correlationengine=<*password*>

  在此範例中，correlationengine 為使用者名稱，而對應的值為密碼。

- **將 Sentinel 裝置安裝至硬碟 (僅適用於「即時 DVD」影像)：**確定選取此核取方塊以將裝置安裝到實體伺服器上。

  若取消選取此核取方塊，裝置將不會安裝到實體伺服器上，而且只會以「即時 DVD」模式執行。

3 按一下「**下一步**」。

4 出現提示時，接受證書。

5 完成「第 13.1.2 節「安裝 Sentinel」(第 75 頁)」中的步驟 15 到步驟 20。

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 收集器管理員或關連引擎，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「第 13.1.2 節「安裝 Sentinel」(第 75 頁)」中的步驟 22 到步驟 23。

13.2 安裝 Sentinel OVF 裝置

本節提供安裝 Sentinel、收集器管理員和關連引擎做為 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。

13.2.1 安裝 Sentinel

安裝 Sentinel OVF 裝置：

1. 至 NetIQ 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. 選取您選擇的語言，然後按一下**「下一步」**。
6. 選取鍵盤配置，然後按一下**「下一步」**。
7. 閱讀並接受「 SUSE Linux Enterprise Server (SLES) 11 SP3 軟體授權合約」。
8. 閱讀並接受「NetIQ Sentinel 使用者授權合約」。
9. 在「主機名稱」與「網域名稱」頁面中，指定主機名稱與網域名稱。不選**指定主機名稱以回送 IP**。
10. 按一下**「下一步」**。儲存主機名稱組態。
11. 選擇下列其中一個網路連接選項：
    - 若要使用目前網路連線設定，請在「網路組態 II」頁面中選取**「使用下列組態」**，接著按**「下一步」**。
    - 若要變更網路連線設定，請選取**「變更」**並執行想要的變更，接著按**「下一步」**。

    如此即可儲存網路連線設定。
12. 設定時間和日期，接著按**「下一步」**。

    若要在安裝之後變更 NTP 組態，請使用裝置指令行中的 YaST。您可以使用 WebYast 來變更時間與日期，而不是 NTP 組態。

    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
13. 設定 root 密碼，然後按一下**「下一步」**。

    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 2.5 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。

    如果可用記憶體大於 2.5 GB 但少於 6.7 GB，安裝作業會顯示一則訊息，提示您記憶體少於建議的大小。當這則訊息出現時，請按**「下一步」**以繼續安裝。
14. 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。

15 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 Web 主控台。

13.2.2 安裝收集器管理員和關連引擎

在 VMware ESX 伺服器上安裝收集器管理員或關連引擎做為 OVF 裝置影像：

1 完成在 第 13.2.1 節「安裝 Sentinel」(第 78 頁) 中的步驟 1 至步驟 10。

2 指定收集器管理員應連接之 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 ActiveMQ 使用者名稱 (收集器管理員或關連引擎使用者名稱)。收集器管理員的預設使用者名稱為 collectormanager，關連引擎為 correlationengine。

5 指定 ActiveMQ 使用者的密碼。

ActiveMQ 使用者身分證明儲存在 Sentinel 伺服器的 /<*install_dir*>/etc/opt/novell/sentinel/config/activemqusers.properties 檔案中。

6 (選擇性) 若要驗證密碼，請參見 activemqusers.properties 中的下列文字行

針對收集器管理員：

```
collectormanager=<password>
```

在此範例中，collectormanager 為使用者名稱，而對應的值為密碼。

針對關連引擎：

```
correlationengine=<password>
```

在此範例中，correlationengine 為使用者名稱，而對應的值為密碼。

7 按一下**「下一步」**。

8 接受證書。

9 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 收集器管理員或 Sentinel 關連引擎，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。

13.3 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。

- 第 13.3.1 節「設定 WebYaST」(第 80 頁)
- 第 13.3.2 節「建立分割區」(第 80 頁)
- 第 13.3.3 節「登錄以進行更新」(第 81 頁)
- 第 13.3.4 節「使用 SMT 設定裝置」(第 81 頁)

13.3.1 設定 WebYaST

Sentinel 裝置使用者介面備有 WebYaST，其為用來控制以 SUSE Linux Enterprise 為基礎之裝置的 Web 式遠端主控台。您可以使用 WebYaST 存取、設定及監看 Sentinel 裝置。下列程序簡要說明設定 WebYaST 的步驟。如需更多有關詳細組態的資訊，請參閱《*WebYaST 使用者指南* (http://www.novell.com/documentation/webyast/)》。

1. 登入 Sentinel 裝置。
2. 按一下**「裝置」**。
3. 將 Sentinel Server 設定為接收更新，如第 13.3.3 節「登錄以進行更新」(第 81 頁) 中所述。
4. 按一下**「下一步」**完成初步設定。

13.3.2 建立分割區

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，請參閱第 6.6 節「規劃資料儲存的分割區」(第 42 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 控制中心：

   ```
   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
    ```

13.3.3 登錄以進行更新

您必須使用裝置更新通道來註冊 Sentinel 裝置，以接收修補程式更新。若要註冊此裝置，您必須先向 NetIQ 客戶服務中心取得裝置登錄碼或裝置啟用碼。

註冊裝置更新的步驟如下：

1. 登入 Sentinel 裝置。
2. 按一下**「裝置」**來啟動 WebYaST。
3. 按一下**「登錄」**。
4. 指定要接收更新的電子郵件 ID，接著再指定系統名稱和裝置登錄碼。
5. 按一下**「儲存」**。

13.3.4 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 NetIQ Customer Center 的套件代理系統，提供重要的 NetIQ Customer Center 功能。

- 「必要條件」(第 81 頁)
- 「設定裝置」(第 82 頁)
- 「升級裝置」(第 82 頁)

必要條件

- 取得適用於 Sentinel 的 NetIQ Customer Center 身分證明，並從 NetIQ 取得更新。如需關於取得身分證明的資訊，請聯絡 NetIQ Support。
- 確認已在您要安裝 SMT 的機器上，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》中的以下小節：
  - 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

如需使用 SMT 設定裝置的相關資訊，請參閱 SUSE Linux Enterprise 11 的 Subscription Management Tool (SMT) 一文。

若要啟用裝置儲存機制，請執行下列指令：

```
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
```

升級裝置

如需有關升級裝置的詳細資訊，請參閱第 25.3 節「使用 SMT 升級裝置」(第 123 頁)。

13.4 使用 WebYaST 停止和啟動伺服器

您可以使用 Web 介面來啟動和停止 Sentinel 伺服器，如下所示：

1. 登入 Sentinel 裝置。
2. 按一下**「裝置」**來啟動 WebYaST。
3. 按一下**「系統服務」**。
4. 若要停止 Sentinel 伺服器，請按一下**「停止」**。
5. 若要啟動 Sentinel 伺服器，請按一下**「啟動」**。

14 NetFlow 收集器管理員安裝

您必須在不同的電腦上安裝 NetFlow 收集器管理員，而不是在安裝了 Sentinel 伺服器、收集器管理員或關連引擎的電腦上。

14.1 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 35 頁)。
- ❒ 使用網路時間通訊協定 (NTP) 同步化時間。

14.2 安裝 NetFlow 收集器管理員

您可以使用下列其中一種方法來安裝 NetFlow 收集器管理員：

- **標準：**使用 NetFlow 組態的預設值。
- **自定：**可讓您自定 Sentinel 伺服器的連接埠號碼。

附註：

- 若要將網路流程傳送到 Sentinel 伺服器，您必須是管理員、屬於 NetFlow 提供者角色，或擁有傳送 NetFlow 的資料許可。
- 若您計劃安裝多個 NetFlow 收集器管理員，建議您為每個 NetFlow 收集器管理員建立一個新的使用者帳戶，以將網路流程資料傳送至 Sentinel。讓每個 NetFlow 收集器管理員擁有不同的使用者帳戶能進一步控制可將資料傳送至 Sentinel 的 NetFlow 收集器管理員。

若要安裝 NetFlow 收集器管理員：

1. 在網頁介面中指定下列 URL 以啟動 Sentinel Web 介面：

   `https://<IP_Address_Sentinel_server>:8443`

   <IP_Address_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 NetFlow 收集器管理員標題下方的 **「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. 在指令提示中，指定下列指令以擷取安裝檔案。

   `tar zxvf <install_filename>`

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

6 移至解壓縮安裝程式的目錄：

```
cd <directory_name>
```

7 指定下列指令以安裝 NetFlow 收集器管理員：

```
./install-netflow
```

8 指定要用於安裝作業的語言號碼，然後按 Enter。

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，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 指定您要進行「標準」或「自定」安裝。

12 指定應接收網路流程資料的 Sentinel 伺服器的主機名稱或 IP 位址。

13 (條件式) 若您選擇「自定」安裝，請指定 Sentinel 伺服器的連接埠號碼。

預設連接埠號碼為 8443。

14 指定驗證至 Sentinel 伺服器的使用者名稱和密碼。

附註：確定您指定的使用者身分證明擁有傳送 NetFlow 資料許可或管理權限。否則，若 NetFlow 收集器管理員將資料傳送至 Sentinel 伺服器時，當安裝完成時，驗證會失敗。

安裝完成。NetFlow 收集器管理員可能需要幾分鐘時間來建立到 Sentinel 伺服器的連接。

15 (選擇性) 若要判斷 NetFlow 收集器管理員安裝是否成功，請執行下列其中一個動作：

- 驗證 NetFlow 收集器管理員服務是否正在執行：

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

- 驗證 NetFlow 收集器管理員是否已與 Sentinel 伺服器建立連接：

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

- 驗證 NetFlow 收集器管理員是否顯示在 Sentinel Web 主控台中，按一下**「集合」** > **「NetFlow」**。

16 在您想要收集網路流程資料的裝置上，啟用網路流程流量轉遞。

啟用裝置上的 NetFlow 時，您必須指定 Sentinel 伺服器的 IP 位址和 NetFlow 收集器管理員用來從 NetFlow 啟用裝置接收資料的連接埠。預設連接埠號碼為 3578。如需詳細資訊，請參閱指定 NetFlow 啟用裝置文件。

15 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。

15.1 安裝收集器

安裝收集器的步驟如下：

1. 從 Sentinel 外掛程式網站下載所要的收集器。
2. 登入 Sentinel Web 介面，其位置為 https://<*IP address*>:8443 (8443 是 Sentinel 伺服器的預設連接埠)。
3. 按一下工具列中的 **「應用程式」**，接著按一下 **「應用程式」**。
4. 按一下 **「啟動控制中心」**以啟動 Sentinel 控制中心。
5. 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」**。
6. 瀏覽並選取在步驟 1 中下載的收集器檔案，接著按 **「下一步」**。
7. 遵循剩餘的提示，接著按一下 **「完成」**。

若要設定收集器，請參閱 Sentinel 外掛程式網站中特定收集器的文件。

15.2 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要的連接器。
2. 登入 Sentinel Web 介面，其位置為 https://<*IP address*>:8443 (8443 是 Sentinel 伺服器的預設連接埠)。
3. 按一下工具列中的 **「應用程式」**，接著按一下 **「應用程式」**。
4. 按一下 **「啟動控制中心」**以啟動 Sentinel 控制中心。
5. 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」**。
6. 瀏覽並選取在步驟 1 中下載的連接器檔案，接著按 **「下一步」**。
7. 遵循剩餘的提示，接著按一下 **「完成」**。

若要設定連接器，請參閱 Sentinel 外掛程式網站中特定連接器的文件。

16 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
  ```

- 驗證 Sentinel 服務是否正常運作：

  ```
  /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。

- 存取 Sentinel Web 介面：

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

     ```
     https://<IP_Address/DNS_Sentinel_server:8443>
     ```

     IP_Address/DNS_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。

17 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。

17.1 瞭解 Sentinel 中的時間

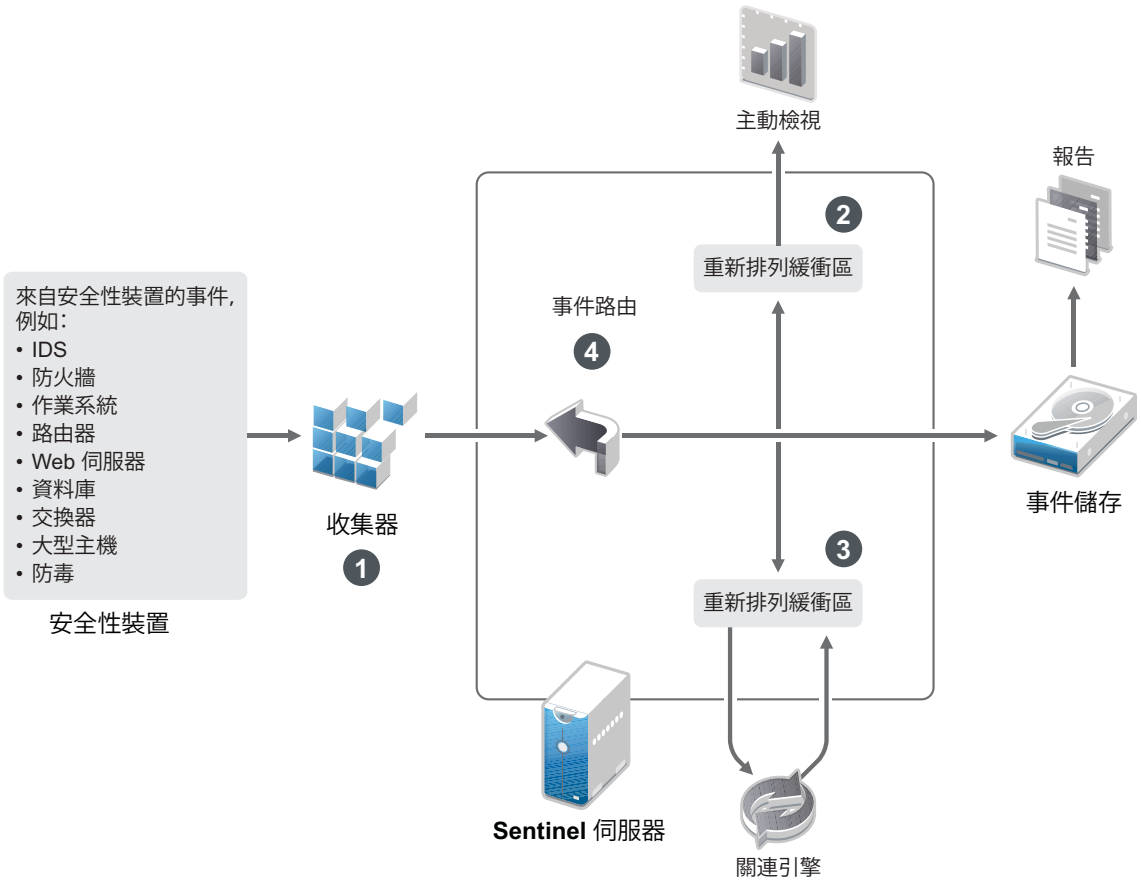
Sentinel 為分散式系統，由分散至整個網路的多個程序組成。此外，系統中還會有一些由事件來源造成的延遲。為了調和延遲的狀況，Sentinel 程序在處理事件之前，會將事件重新排列為以時間先後順序排列的資料流。

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，記錄自收集器管理員系統時間。
- **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 達成這項目標的方式：

圖 17-1 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. 通常是由主動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。時間戳記快 5 分鐘以上的事件不會出現在主動檢視中，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，讓關連引擎可依時間順序來處理。如果事件時間比伺服器快 30 秒，關連引擎便不會處理事件。
4. 如果事件時間比收集器管理員系統時間快 5 分鐘，Sentinel 會直接將事件路由到事件儲存，略過關連、主動檢視和等安全情報即時系統。

17.2 在 Sentinel 中設定時間

關連引擎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：

- 在收集器管理員上設定 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 會將收集器管理員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《*NetIQ 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。

17.3 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>
```

17.4 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，收集器管理員位在另一個時區中，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。

收集器和收集器管理員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。這項資訊會從收集器管理員傳送至 Sentinel 伺服器，且儲存在事件儲存中。收集器管理員和 Sentinel 伺服器所在的時區不會影響這個程序或儲存的資料。然而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。

18 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。

     管理員使用者是透過 Sentinel Web 主控台用來執行管理工作的身分，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。

19 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。

19.1 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 Web 介面，其位置為 https://<*IP address*>:8443 (8443 是 Sentinel 伺服器的預設連接埠)。
2. 按一下 **「外掛程式」** > **「目錄」**。

19.2 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 *《NetIQ Sentinel 管理指南》*中的 「收集和路由事件資料」。

19.3 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 《「NetIQ Sentinel 管理指南」》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 Web 主控台以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 《*NetIQ Sentinel 使用者指南*》中的 「「安裝及管理解決方案套件」」。

19.4 設定動作與整合器

如需設定立即可用外掛程式的相關資訊，請參閱 Sentinel 外掛程式網站上的特定外掛程式文件。

20 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。

20.1 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. 按照在「第 21 章 「以 FIPS 140-2 模式操作 Sentinel」(第 101 頁)」中提到的任務，完成 FIPS 140-2 模式組態。

20.2 啟用遠端收集器管理員和關連引擎上的 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，您必須啟用遠端收集器管理員和關連引擎上的 FIPS 140-2 模式。

要啟用遠端收集器管理員或關連引擎，以在 FIPS 140-2 模式中執行：

1. 登入遠端收集器管理員或關連引擎系統。
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. 按照在「第 21 章 「以 FIPS 140-2 模式操作 Sentinel」(第 101 頁)」中提到的任務，完成 FIPS 140-2 模式組態。

21 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。

21.1 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 108 頁)。

21.2 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 108 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>/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 108 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>/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 108 頁)。

5 重新啟動來源電腦上的 Sentinel 服務。

21.3 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 108 頁)。

3 以管理員職能的使用者身分登入 Sentinel Web 主控台，然後繼續設定 LDAP 驗證。

如需詳細資訊，請參閱《*NetIQ Sentinel 管理指南*》中的「「設定 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。

21.4 更新在遠端收集器管理員和關連引擎上的伺服器證書

要設定現有遠端收集器管理員和遠端關連引擎，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，將收集器管理員和關連引擎留在非 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 模式中的遠端收集器管理員可能無法與這樣的事件來源搭配運作。

若您不想啟用遠端收集器管理員或關連引擎上的 FIPS 140-2 模式，您必須複製最新的 Sentinel 伺服器證書到遠端系統，讓收集器管理員或關連引擎可以與 Sentinel 伺服器通訊。

要更新遠端收集器管理員或關連引擎上的 Sentinel 伺服器證書：

1. 登入遠端收集器管理員或關連引擎電腦。
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。

21.5 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。

21.5.1 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 108 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 伺服器或遠端收集器管理員，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

   遠端收集器管理員證書位置：/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。

21.5.2 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 108 頁)。
3. 繼續設定連接器。

21.5.3 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 108 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。

21.5.4 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 108 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 伺服器證書或遠端收集器管理員證書，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。

21.5.5 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 108 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 伺服器證書或遠端收集器管理員證書，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。

---

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 108 頁)。

21.5.6 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收集器管理員中，您必須從遠端收集器管理員機器複製 /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 108 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。

21.5.7 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 108 頁)。

3 繼續設定整合器例項。

21.5.8 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。

21.5.9 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 模式中安裝遠端收集器管理員，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 12.4 節「安裝收集器管理員和關連引擎」(第 69 頁)。

2 將非 FIPS 連接器指定部署到非 FIPS 遠端收集器管理員。

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 遠端收集器管理員上時，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 7.1 版本說明。

21.6 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。當 FIPS 140-2 模式已在 Sentinel 中啟用時，您無法使用 Sentinel 使用者介面上傳證書。您必須手動輸入證書到 FIPS KeyStore 資料庫。

針對使用部署到遠端收集器管理員的連接器的事件來源，您必須輸入證書到遠端收集器管理員的 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 伺服器或遠端收集器管理員上的任何暫存位置。

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 伺服器或遠端收集器管理員時，輸入 yes 或 y。

21.7 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。

- 第 21.7.1 節「回復 Sentinel 伺服器到非 FIPS 模式」(第 109 頁)
- 第 21.7.2 節「回復遠端收集器管理員或遠端關連引擎到非 FIPS 模式」(第 109 頁)

21.7.1 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。

21.7.2 回復遠端收集器管理員或遠端關連引擎到非 FIPS 模式

您可以回復遠端收集器管理員或遠端關連引擎到非 FIPS 模式。

要回復遠端收集器管理員或遠端關連引擎到非 FIPS 模式：

1. 登入遠端收集器管理員或遠端關連引擎系統。
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. 重新啟動遠端收集器管理員或遠端關連引擎。

V 升級 Sentinel

本節提供升級 Sentinel 和其他元件的相關資訊。

22 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 22-1 *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。	NetIQ 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

23 必要條件

23.1 Sentinel 在 FIPS 模式中的必要條件

若您已使用 JRE 7 更新 45 降級 Java 版本以解決用戶端和採 FIPS 模式執行的 Sentinel 之間的連線問題 (如 Sentinel 7.2.2 已知問題 所述)，則適用下列必要條件。

若任一 Sentinel 安裝目錄中包含符號連結，則 Sentinel 安裝程式將不會繼續升級。當您下載並安裝 JRE 7 更新 45 以降級 Java 版本時，JRE 資料夾會包含名為 man 的子資料夾，其包含符號連結。因此，您應刪除 man 資料夾以成功升級至 Sentinel 7.3 及更新版本。不過，若您已下載並安裝 JDK 7 更新 45 而非 JRE 7 更新 45，man 資料夾就不會包含符號連結，不必加以刪除。

刪除 man 資料夾：

1. 以 novell 使用者身分登入 Sentinel 伺服器。
2. 指定下列指令以變更目錄：

   cd /opt/novell/sentinel/jre/
3. 刪除 man 資料夾：

   rm -rf man

23.2 Sentinel 7.1.1 之前版本的必要條件

Sentinel 7.1.1 和更新版本包括 MongoDB 版本 2.4.1。MongoDB 2.4 必須移除資料庫中重複的使用者名稱。若您要升級 7.1.1 之前的 Sentinel 版本，請驗證是否有任何重複使用者，接著移除重複使用者。

請執行下列步驟以辨識重複的使用者：

1. 以 novell 使用者身分登入 Sentinel 7.1 或舊版伺服器。
2. 變更至以下目錄：

   ```
   cd opt/novell/sentinel/3rdparty/mongodb/bin
   ```
3. 執行下列指令以驗證重複的使用者：

   ```
   ./mongo --port 27017 --host "localhost"
   use analytics
   db.system.users.find().count()
   ```

   若 count 大於 1，就代表有重複的使用者。

請執行下列步驟以移除重複的使用者：

1. 執行下列指令以列出使用者：

   ```
   db.system.users.find().pretty()
   ```

   指令會一同列出使用者與重複的項目。清單中的第一位使用者是原始使用者。請保留第一位使用者，並刪除清單中其他人。

2. 執行下列指令以移除重複的使用者：

   ```
   db.system.users.remove({ _id : ObjectId("object_ID") })
   ```

3. 執行下列指令以驗證是否已移除重複的使用者：

   ```
   db.system.users.find().pretty()
   ```

4. 切換至資料庫管理員使用者：

   ```
   use admin
   ```

5. 重複步驟 1 至步驟 3 以驗證並移除管理員資料庫中重複的 dbausers。

24 升級 Sentinel 傳統安裝

24.1 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。

   如需備份資料的詳細資訊，請參閱《*NetIQ 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「《NetIQ Sentinel 管理指南》」中的 *「保留 XML 檔案自訂設定」*。

3. 從 NetIQ 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 控制中心清除 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 postgreSQL 舊檔案：

```
./delete_old_cluster.sh
```

14 (條件式) 若您要升級 Sentinel 7.1.1 或更早的版本，安裝程式不會預設移轉安全性智慧 (SI) 資料。若要從 Sentinel 7.1.1 或更早的版本移轉 SI 資料，請手動啟用 SI 資料移轉如下：

14a 切換至 novell 使用者。

```
su novell
```

14b 開啟 /etc/opt/novell/sentinel/config/server.xml 檔案。

14c 將下列內容新增至 BaseliningRuntime 元件區段：

```
<property name="baselining.migration.check">true</property>
```

14d 重新啟動 Sentinel 伺服器。

15 若要升級收集器管理員系統和關連引擎系統，請參閱第 24.3 節 「升級收集器管理員或關連引擎」(第 120 頁)。

24.2 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《*NetIQ 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「《NetIQ Sentinel 管理指南》」中的 *「保留 XML 檔案自訂設定」*。

3. 從 NetIQ 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 控制中心清除 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) 若您要升級 Sentinel 7.1.1 或更早的版本，安裝程式不會預設移轉安全性智慧 (SI) 資料。若要從 Sentinel 7.1.1 或更早的版本移轉 SI 資料，請手動啟用 SI 資料移轉如下：

16a 切換至 novell 使用者。

```
su novell
```

16b 開啟 /etc/opt/novell/sentinel/config/server.xml 檔案。

16c 將下列內容新增至 BaseliningRuntime 元件區段：

```
<property name="baselining.migration.check">true</property>
```

16d 重新啟動 Sentinel 伺服器。

24.3 升級收集器管理員或關連引擎

使用下列步驟升級收集器管理員和關連引擎：

1. 請將組態備份並建立 ESM 輸出。

   如需詳細資訊，請參閱《*NetIQ Sentinel 管理指南*》中的「「備份與還原資料」」。
2. 以管理員職能中的使用者身分登入 Sentinel Web 介面。
3. 選取**「下載」**。
4. 在「收集器管理員安裝程式」區段中，按一下**「下載安裝程式」**。

   即會顯示視窗，其中包含開啟或將檔案儲存在本地機器上的選項。
5. 儲存檔案。
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：

   針對收集器管理員：

   ```
   ./install-cm
   ```

   針對關連引擎：

   ```
   ./install-ce
   ```
9. 依照螢幕上的提示完成安裝。

25 升級 Sentinel 裝置

本章節中的程序將協助您升級 Sentinel 裝置、收集器管理員，以及關連引擎裝置。

25.1 使用 Zypper 升級裝置

若要使用 zypper 修補程式將裝置升級：

1. 請將組態備份，然後建立 ESM 輸出。如需詳細資訊，請參閱《*NetIQ 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「《NetIQ 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) 若您要升級 Sentinel 7.0.1 或更早的版本，請輸入 1 以接受將廠商從 Novell 變更為 NetIQ。
6. (條件式) 若您要升級 7.2 之前的 Sentinel 版本，安裝程式會顯示針對某些裝置套件解析相依性的訊息。請輸入 1 以解除安裝相依套件。
7. 輸入 Y 繼續。
8. 輸入 yes 接受授權合約。
9. 重新啟動 Sentinel 裝置。
10. 清除網頁瀏覽器快取以檢視 Sentinel 最新版本。
11. 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 控制中心清除 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。
12. (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。

    12a 切換至 novell 使用者。

    ```
    su novell
    ```

    12b 瀏覽至 bin 資料夾：

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

12c 使用下列指令刪除所有 postgreSQL 舊檔案：

```
./delete_old_cluster.sh
```

13 (條件式) 若您要升級 Sentinel 7.1.1 或更早的版本，安裝程式不會預設移轉安全性智慧 (SI) 資料。若要從 Sentinel 7.1.1 或更早的版本移轉 SI 資料，請手動啟用 SI 資料移轉如下：

13a 切換至 novell 使用者。

```
su novell
```

13b 開啟 /etc/opt/novell/sentinel/config/server.xml 檔案。

13c 將下列內容新增至 BaseliningRuntime 元件區段：

```
<property name="baselining.migration.check">true</property>
```

13d 重新啟動 Sentinel 伺服器。

附註：若要升級收集器管理員或關連引擎，請依照步驟 3 到步驟 9 的指示進行。

25.2 透過 WebYast 升級裝置

附註：您必須使用 zypper 指令行公用程式才可升級 Sentinel 7.2 之前版本的裝置，這是因為升級需要使用者互動才能完成。WebYaST 無法協助處理必要的使用者互動。如需關於使用 Zypper 升級裝置的詳細資訊，請參閱第 25.1 節「使用 Zypper 升級裝置」(第 121 頁).

---

1. 以管理員角色中的使用者身分登入 Sentinel 裝置。
2. 請將組態備份，然後建立 ESM 輸出。如需詳細資訊，請參閱《*NetIQ Sentinel 管理指南*》中的「「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「《NetIQ Sentinel 管理指南》」中的 *「保留 XML 檔案自訂設定」*。
4. **如果您想要升級 Sentinel 裝置**，請按一下**「裝置」**啟動 WebYaST。
5. **若您想升級收集器管理員或關連引擎裝置**，請將使用連接埠 4984 啟動 WebYaST 的收集器管理員或關連引擎電腦的 URL 指定為 https://*<IP_address>*:4984，其中 *<IP_address>* 是收集器管理員或關連引擎的 IP 位址。完成步驟 10 到步驟 7 的作業。
6. 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《*NetIQ Sentinel 管理指南*》中的「「備份與還原資料」」。
7. (條件式) 如果您還沒有註冊裝置以接收自動更新，請註冊。

   如需詳細資訊，請參閱第 13.3.3 節「登錄以進行更新」(第 81 頁)。

   若是尚未註冊的裝置，Sentinel 會顯示一個黃色警告，指出該裝置尚未註冊。
8. 若要檢查是否有更新，請按一下「**更新**」。

   可用的更新便會隨即顯示。
9. 選取並套用更新。

   更新可能需要數分鐘才會完成。更新成功後，就會顯示 WebYaST 登入頁面。

   裝置升級之前，WebYaST 會自動停止 Sentinel 服務。完成升級後，您必須以手動方式重新啟動服務。

10 使用 Web 介面重新啟動 Sentinel 服務。

如需詳細資訊，請參閱第 13.4 節「使用 WebYaST 停止和啟動伺服器」(第 82 頁)。

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 控制中心清除 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 postgreSQL 舊檔案：

```
./delete_old_cluster.sh
```

14 (條件式) 若您要升級 Sentinel 7.1.1 或更早的版本，安裝程式不會預設移轉安全性智慧 (SI) 資料。若要從 Sentinel 7.1.1 或更早的版本移轉 SI 資料，請手動啟用 SI 資料移轉如下：

14a 切換至 Novell 使用者：

```
su novell
```

14b 開啟 /etc/opt/novell/sentinel/config/server.xml 檔案。

14c 將下列內容新增至 BaseliningRuntime 元件區段：

```
<property name="baselining.migration.check">true</property>
```

14d 重新啟動 Sentinel 伺服器。

25.3 使用 SMT 升級裝置

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，請參閱第 13.3.4 節「使用 SMT 設定裝置」(第 81 頁)。

2 請將組態備份，然後建立 ESM 輸出。如需詳細資訊，請參閱《*NetIQ Sentinel 管理指南*》中的「「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「《NetIQ 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
```

26 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。

新的和更新的 Sentinel 外掛程式 (包括解決方案套件)，會經常上載至 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 部署 Sentinel 以提供高可用性

您可使用本附錄在主動 / 被動高可用性模式中安裝 NetIQ Sentinel，以允許 Sentinel 在硬體或軟體失敗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，請連絡 NetIQ 支援小組。

附註：只有 Sentinel 伺服器支援高可用性 (HA) 組態。不過，收集器和關連引擎仍可與 Sentinel HA 伺服器通訊。

27 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。

27.1 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。若存取權限嚴格受到限制 (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)，協力廠商系統就必須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，Sentinel 應使用虛擬 IP 設定)。

27.2 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。

附註：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。

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。

27.3 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。

27.4 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。

28 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：
  - SUSE Linux Enterprise Server (SLES) 11 SP3 作業系統
  - SUSE Linux Enterprise Server High Availability Extension (SLES HAE) 套件
  - Sentinel 軟體 (包括 HA rpm)
- ❒ **(條件式) 針對傳統 HA 安裝**，確定可以取得 Sentinel 安裝檔案 (TAR 檔案) 和包含有效授權的 SUSE Linux High Availability Extension (SLE HAE) ISO 影像。
- ❒ **(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>
     ```

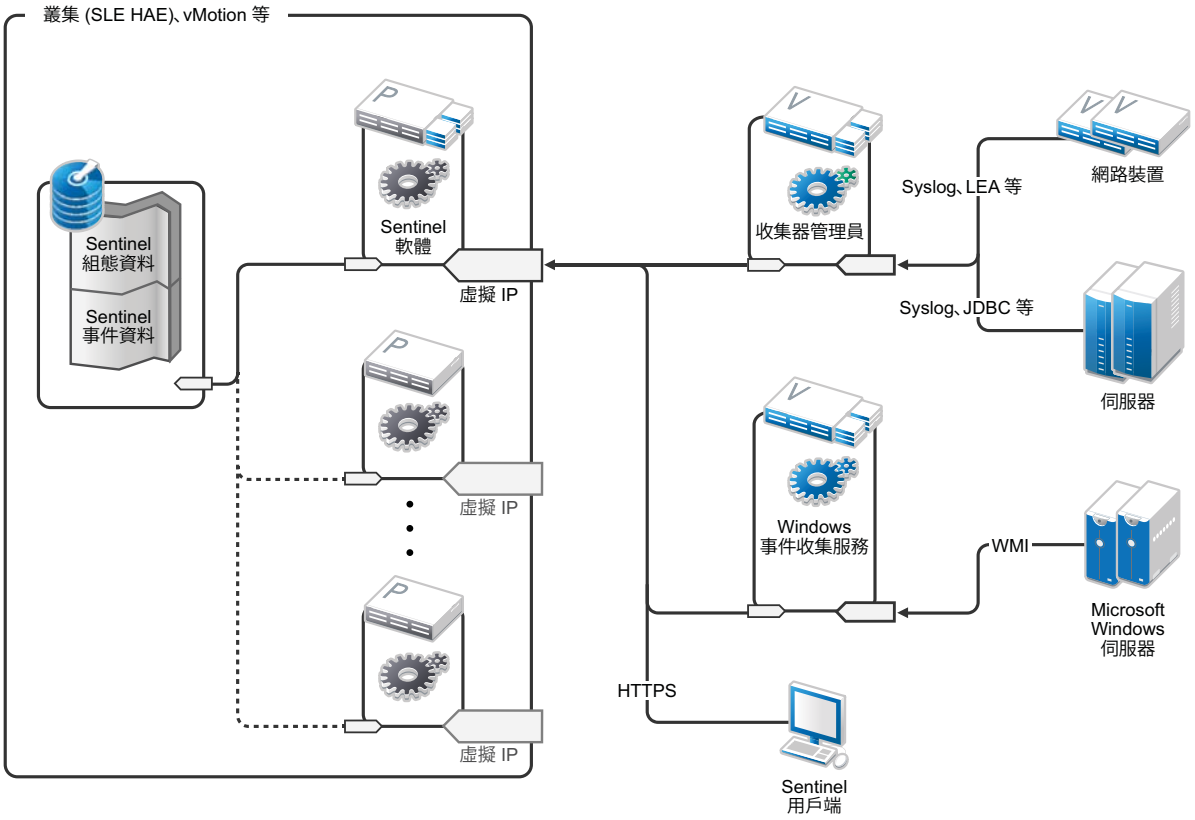
  2. 在 /etc/init.d/boot.local 檔案中新增下列行，確保電腦每次開機時都會自動載入監視程式驅動程式：

     ```
     /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 35 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 35 頁)」中指定的效能及大小特性要求。NetIQ 建議使用標準 SUSE Linux VM，設定為使用 iSCSI 目標做為共享儲存。
- ❒ 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。NetIQ 建議使用兩個 SUSE Linux VM。
- ❒ 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。NetIQ 建議使用專用 IP 位址連線至 iSCSI 目標。
- ❒ 請確保您擁有可在叢集中的節點之間移轉的虛擬 IP，以當成 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。NetIQ 建議簡單的單點傳播 IP 位址，但生產環境偏好多路廣播。

29 安裝和組態

本節說明在高可用性 (HA) 環境中安裝及設定 Sentinel 的步驟。

下圖代表主動 / 被動高可用性結構：



29.1 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 35 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 35 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 51 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」**。

NetIQ 建議使用下列組態：

- **(條件式) 針對傳統 HA 安裝：**
  - 兩個 SUSE Linux 11 SP3 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：**兩個 HA ISO 裝置的叢集節點虛擬機器。如需安裝 HA ISO 裝置的詳細資訊，請參閱第 13.1.2 節 「安裝 Sentinel」(第 75 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 SUSE Linux 和 SLE HAE 系統要求，以及 Sentinel 應用程式要求。
- 一個使用以 iSCSI 目標做為共享儲存所設定的 SUSE Linux 11 SP3 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。
  - 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 SUSE Linux 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，以進行內部叢集通訊。

29.2 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。

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：NetIQ 建議您設定共享儲存並在每個叢集節點上測試掛接共享儲存。不過，叢集組態將處理實際的儲存掛接。

NetIQ 建議使用下列程序來建立由 SUSE Linux VM 代管的 iSCSI 目標：

1. 連線至 storage03 (您在 啟始設定 期間建立的 VM)，接著啟動主控台工作階段。
2. 使用 dd 指令為 Sentinel 主要儲存建立任何所要大小的空白檔案：

   dd if=/dev/zero of=/localdata count=10240000 bs=1024
3. 建立填滿零的 10GB 檔案，複製自 /dev/zero pseudo-device 檔案。請參閱 dd 指令的資訊或主要頁面以取得指令行選項的詳細資料。
4. 重複步驟 1 到 3 以建立次要儲存的檔案：

   dd if=/dev/zero of=/networkdata count=10240000 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。

29.2.1 設定 iSCSI 目標

將檔案 localdata 和 networkdata 設定為 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。
6. 按一下 **「下一步」**，然後按一下 **「確定」**。
7. 在主螢幕上，選取 **「網路服務」** > **「iSCSI 目標」**。
8. 系統提示時，從 SUSE Linux 11 SP3 媒體安裝必要的軟體 (iscsitarget RPM)。
9. 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。
10. 按一下 **「全域」**，然後選取 **「無驗證」**，因為目前的 OCF Resource Agent for iSCSI 不支援驗證。
11. 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。

12 按一下「**新增**」以加入新的 LUN。

13 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。

14 重複步驟 12 和 13，並在此時加入 LUN 1 和 /networkdata。

15 保留其他選項的預設值。按一下「**確定**」，然後按一下「**下一步**」。

16 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。若系統要求重新啟動 iSCSI，按「接受」。

17 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。

29.2.2 設定 iSCSI 啟動器

使用下列程序來格式化裝置：

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。

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 系統提示時，從 SUSE Linux 11 SP3 媒體安裝必要的軟體 (open-iscsi 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)，選取「**無驗證**」，然後按一下「**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 在「**啟動**」下拉式清單中切換到自動，然後選取「**無驗證**」，然後按一下「**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 您應可在「系統檢視」中查看清單中的新硬碟 (例如 /dev/sdb 和 /dev/sdc)，他們的類型為 IET-VIRTUAL-DISK。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 ext3 主要分割區，但是不要將它掛接。確定已選取「請勿掛接分割區」選項。

19 檢閱將要進行的變更之後，依序選取「**下一步**」、「**完成**」。假設您在這個共享 iSCSI LUN 上建立一個大型分割區，您會取得一個 /dev/sdb1 分割區或類似的格式化磁碟 (參照以下 /dev/<SHARED1>)。

20 回到分割器，重複 /dev/sdc 的分割 / 格式化程序 (步驟 16-19)，或對應到次要儲存的任一區塊裝置。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) 若您執行的是傳統 HA 安裝**，請建立掛接點並依下列方式測試掛接本地分割區 (確切的裝置名稱可能會依指定實作而不同)：

```
# 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 取代每個叢集節點的節點 IP。

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 5 中使用不同的 IP 取代每個叢集節點的節點 IP。

29.3 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。

NetIQ 建議將 Sentinel 安裝至每個可代管它的叢集節點。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。

29.3.1 首次節點安裝

- 「傳統高可用性安裝」(第 137 頁)
- 「Sentinel HA 裝置安裝」(第 138 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
```

4 執行整個標準安裝，依需求設定產品。安裝程式會安裝二進位、資料庫和組態檔案。安裝程式也會設定登入身分證明、組態設定和網路連接埠。

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 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 指定選項以選取 Sentinel 組態類型。

3c 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/sentinel /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/
```

29.3.2 後續節點安裝

- 「傳統高可用性安裝」(第 139 頁)
- 「Sentinel HA 裝置安裝」(第 139 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
./install-sentinel --no-start --cluster-node --unattended=/tmp/install.props
cd /
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/sentinel
```

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。

29.4 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。

NetIQ 建議使用下列程序來設定 SUSE Linux 高可用性延伸，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 SLE HAE 文件安裝核心 SLE HAE 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
```

29.5 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。

NetIQ 建議針對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 SUSE Linux VM 上設定的 iSCSI 目標，以做為用於圍籬區隔用途的叢集分裂 (SBD) 裝置。

SBD 安裝程式

1. 連接至 storage03 並啟動主控台工作階段。使用 dd 指令建立任何所要大小的空白檔案：

   ```
   dd if=/dev/zero of=/sbd count=1024 bs=1024
   ```

2. 建立填滿零的 1MB 檔案，複製自 /dev/zero pseudo-device。
3. 從指令行或圖形使用者介面執行 YaST：/sbin/yast
4. 選取 **「網路服務」** > **「iSCSI 目標」**。
5. 按一下 **「目標」**，然後選取現有的目標。

6 選取 「**編輯**」。UI 將顯示可用 LUN (磁碟機) 的清單。

7 選取 「**新增**」以加入新的 LUN。

8 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。

9 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。

10 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)。若 DNS 尚未設定或無法使用，將每個主機的項目新增到列出每個 IP 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**」啟動選項和 「**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 1MB IET-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 執行指令 sleha-init。

11 當系統提示要繫結的網路位址時，請指定外部 NIC IP (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/<device id>，其中 <device id> 是您在以上找到的 ID (您可以使用定位鍵自動完成路徑)。

14 完成精靈並確定未回報任何錯誤。

15 啟動 YaST。

16 選取 「**高可用性**」>「**叢集**」(或在某些系統上只要 「叢集」)。

17 在左側方塊中，確定已選取 「**通訊通道**」。

18 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)。

19 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。

20 選取 「**完成**」以完成組態。

21 結束 YaST。

22 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**」啟動選項和「**無驗證**」)。

6 選取「**確定**」以結束 iSCSI 啟動器 工具。

7 執行以下指令：sleha-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 將 /etc/corosync/corosync.conf 手動從 node01 複製到 node02，或執行 node01 上的 csync2 -x -v，或透過 YaST 手動在 node02 上設定叢集。

2 執行 node02 上的 /etc/rc.d/openais start

(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。

3 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。

29.6 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。
- 儲存組態和事件中繼資料的 PostgreSQL 資料庫軟體。

NetIQ 建議針對資源組態使用下列內容：

NetIQ 提供一個 crm 程序檔協助叢集組態。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) 叢集產生的新資源可能會發生問題；若發生此問題，請在 node02 上執行 /etc/rc.d/openais restart。

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，以及共享儲存的裝置名稱，然後將會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 NetIQ 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。

29.7 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 Web 主控台中，在頂端功能表列按一下**「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

NetIQ 建議使用簡易 iSCSI 目標做為網路共享儲存位置，使用的組態與主要儲存大多相同。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：由於 NetIQ 建議在此解決方案中使用 iSCSI 目標，此目標將會掛接為目錄，以當成次要儲存使用。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 Web 主控台或執行指令：

```
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 Web 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。

NetIQ 建議使用必要資源的簡易版本，例如簡易的檔案系統資源代理程式，客戶可以視需要選擇使用更複雜的叢集資源，例如 cLVM (檔案系統的邏輯磁碟區版本)。

30 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。

30.1 必要條件

- 從 NetIQ 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 <watchdog driver name>
     ```

  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 <watchdog driver name>
     ```

30.2 升級傳統 Sentinel HA 安裝

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 <install_filename>
```

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
```

重複所有被動叢集節點的步驟 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 《「NetIQ 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 <install_filename>
```

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：

```
run 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
```

30.3 升級 Sentinel HA 裝置安裝

您可以使用 Zypper 修補程式，也可透過 WebYast 升級 Sentinel HA 裝置安裝。

- 第 30.3.1 節「使用 Zypper 升級 Sentinel HA 裝置」(第 147 頁)
- 第 30.3.2 節「透過 WebYast 升級 Sentinel HA 裝置」(第 148 頁)

30.3.1 使用 Zypper 升級 Sentinel HA 裝置

升級之前，您必須透過 WebYast 註冊所有裝置。如需詳細資訊，請參閱 第 13.3.3 節「登錄以進行更新」(第 81 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 下載 Sentinel HA 裝置的更新。

```
zypper -v patch -d
```

此指令下載裝置上已安裝套件的更新 (包括 Sentinel) 至 /var/cache/zypp/packages。

3b 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。

3c 下載更新之後，請使用下列指令安裝更新：

```
rpm -Uvh /var/cache/zypp/packages/sentinel_server_7000_x86_64-Updates/rpm/noarch/*.rpm /
var/cache/zypp/packages/sentinel_server_7000_x86_64-Updates/rpm/x86_64/*.rpm /var/cache/
zypp/packages/sentinel_server_7000_x86_64-Updates/rpm/i586/*.rpm --excludepath=/var/opt/
novell/
```

3d 執行下列程序檔以完成升級程序：

```
/var/adm/update-scripts/sentinel_server_ha_x86_64-update-<version>-overlay_files.sh
```

3e 升級完成之後，請重新啟動叢集堆疊。

```
rcopenais start
```

重複所有被動叢集節點的步驟 3。

4 升級主動叢集節點：

4a 請將組態備份，然後建立 ESM 輸出。

如需備份資料的詳細資訊，請參閱《*NetIQ 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 以管理員身分登入 Sentinel 裝置。

4d 若要升級 Sentinel 裝置，請按一下**「裝置」**啟動 WebYaST。

4e 若要檢查是否有更新，請按一下**「更新」**。

4f 選取並套用更新。

更新可能需要數分鐘才會完成。更新成功後，就會顯示 WebYaST 登入頁面。

裝置升級之前，WebYaST 會自動停止 Sentinel 服務。完成升級後，您必須以手動方式重新啟動服務。

4g 清除網頁瀏覽器快取以檢視 Sentinel 最新版本。

4h 升級完成之後，請重新啟動叢集堆疊。

```
rcopenais start
```

4i 執行下列指令以同步化組態檔案中的任何變更：

```
run 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
```

30.3.2 透過 WebYast 升級 Sentinel HA 裝置

升級之前，您必須透過 WebYast 註冊所有裝置。如需詳細資訊，請參閱 第 13.3.3 節「登錄以進行更新」(第 81 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存取性，並避免節點的圍籬區隔。

3b 將使用連接埠 4984 啟動 WebYaST 的被動叢集節點的 URL 指定為 https://<*IP_address*>:4984，其中 <*IP_address*> 是被動叢集節點的 IP 位址。以管理員身分登入 Sentinel 裝置。

3c 若要檢查是否有更新，請按一下**「更新」**。

3d 選取並套用更新。

更新可能需要數分鐘才會完成。更新成功後，就會顯示 WebYaST 登入頁面。

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 4。

4 升級主動叢集節點：

4a 請將組態備份，然後建立 ESM 輸出。

如需備份資料的詳細資訊，請參閱《*NetIQ 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 以管理員身分登入 Sentinel 裝置。

4d 若要升級 Sentinel 裝置，請按一下**「裝置」**啟動 WebYaST。

4e 若要檢查是否有更新，請按一下**「更新」**。

4f 選取並套用更新。

更新可能需要數分鐘才會完成。更新成功後，就會顯示 WebYaST 登入頁面。

裝置升級之前，WebYaST 會自動停止 Sentinel 服務。完成升級後，您必須以手動方式重新啟動服務。

4g 清除網頁瀏覽器快取以檢視 Sentinel 最新版本。

4h 升級完成之後，請重新啟動叢集堆疊。

```
rcopenais start
```

4i 執行下列指令以同步化組態檔案中的任何變更：

```
run 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
```

31 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。

31.1 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。*《NetIQ 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。

31.2 復原

31.2.1 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。

31.2.2 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。

31.2.3 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。「《NetIQ 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。

VII 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。

A.1 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。

A.2 無法針對已建立影像的收集器管理員或關連引擎建立 UUID

如果為收集器管理員伺服器建立影像 (例如使用 ZENworks Imaging 建立) 並將影像還原到其他機器，則 Sentinel 無法唯一識別收集器管理員的各個新例項。發生這個問題的原因在於重複的 UUID。

您必須在新安裝的收集器管理員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. 重新啟動收集器管理員。

   收集器管理員將自動產生 UUID。

A.3 在登入後，Internet Explorer 的 Web 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」**。

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。

B.1 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。
- ❒ 解除安裝收集器管理員和關連引擎 (若有)。
- ❒ 執行解除安裝後工作以完成 Sentinel 解除安裝。

B.2 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。

B.2.1 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：

   ```
   /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。

B.2.2 解除安裝收集器管理員和關連引擎

使用下列步驟解除安裝收集器管理員和關連引擎：

1 以 root 身分登入收集器管理員和關連引擎電腦。

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收集器管理員或遠端關連引擎。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，表示將完全移除收集器管理員或關連引擎以及所有相關資料。

4 輸入 y 以移除收集器管理員或關連引擎。

程序檔會先停止服務，然後再將服務完全移除。不過，收集器管理員和關連引擎圖示在 Web 介面中仍會以非使用中狀態顯示。

5 執行以下其他步驟，手動刪除 Web 介面中的收集器管理員和關連引擎：

收集者管理員：

1. 存取**「事件來源管理」>「即時檢視」**。
2. 在您要刪除的收集器管理員上按一下滑鼠右鍵，然後按一下**「刪除」**。

關連引擎：

1. 以管理員身分登入 Sentinel Web 介面。
2. 顯示**關連**的次目錄，接著選取要刪除的關連引擎。
3. 按一下**「刪除」**按鈕 (垃圾桶圖示)。

B.2.3 解除安裝 NetFlow 收集器管理員

使用下列步驟解除安裝 NetFlow 收集器管理員：

1 登入至 NetFlow 收集器管理員電腦。

附註：您必須使用與用來安裝 NetFlow 收集器管理員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 以解除安裝收集器管理員。

程序檔會先停止服務，然後再將服務完全解除安裝。

B.3 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。