安裝指南

Novell®
Sentinel Log Manager

1.1

July 08, 2010

www.novell.com

法律聲明

Novell, Inc. 不對本文件的內容或使用做任何表示或保證，且特別聲明不對任何特定用途的適銷性或適用性提供任何明示或默示的保證。此外，Novell, Inc. 有權隨時修訂本出版品或更改其內容，而無義務向任何個人或實體告知這類修訂或變更。

此外，Novell, Inc. 不對軟體做任何表示或保證，且特別聲明不對任何特定用途的適銷性或適用性提供任何明示或默示的保證。此外，Novell, Inc. 有權隨時變更部分或全部 Novell 軟體，而無義務向任何個人或實體告知這類變更。

此合約下提到的任何產品或技術資訊可能受美國出口管制法與其他國家 / 地區的貿易法的限制。您同意遵守所有出口管制規定，並同意取得出口、再出口或進口產品所需的一切授權或類別。您同意不出口或再出口至目前美國出口排除清單上所列之實體，或是任何美國出口法所指定之禁運或恐怖主義國家 / 地區。您同意不將交付產品用在禁止的核武、飛彈或生化武器等用途上。請參閱 Novell 國際貿易服務網頁 (http://www.novell.com/info/exports/)，以取得有關出口 Novell 軟體的詳細資訊。Novell 無需承擔您無法取得任何必要的出口核准之責任。

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

*線上文件：*若要存取本產品及其他 Novell 產品的最新線上文件，請參閱 Novell 文件網頁 (http://www.novell.com/documentation)。

Novell 商標

若要查看 Novell 商標，請參閱 Novell 商標和服務標誌清單 (http://www.novell.com/company/legal/trademarks/tmlist.html)。

協力廠商資料

所有的協力廠商商標均爲其各別擁有廠商的財產。

目錄

關於本指南

本指南提供對 Novell Sentinel Log Manager 及其安裝的綜覽。

使用對象

本指南適用於 Novell Sentinel Log Manager 管理員與終端使用者。

意見反應

我們希望得到您對本手冊以及本產品隨附之其他文件的意見和建議。您可以使用線上文件各頁底部的「使用者意見」功能，或造訪 Novell 文件的意見反應網站 (http://www.novell.com/documentation/feedback.html)，寫下您的意見。

其他文件

如需有關建立自己的外掛程式 (例如，JasperReports) 的詳細資訊，請造訪 Sentinel SDK 網頁 (http://developer.novell.com/wiki/index.php/Develop_to_Sentinel)。Sentinel Log Manager 報告外掛程式的建置環境與 Novell Sentinel 所記載的建置環境完全相同。

如需有關 Sentinel 文件的詳細資訊，請參閱 Sentinel 文件網站 (http://www.novell.com/documentation/sentinel61/index.html)。

如需有關設定 Sentinel Log Manager 的其他文件，請參閱 《*Sentinel Log Manager 1.1 管理指南*》。

連絡 Novell

- Novell 網站 (http://www.novell.com)
- Novell 技術支援 (NTS) (http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup)
- Novell 自助支援 (http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog)
- 修補程式下載網站 (http://download.novell.com/index.jsp)
- Novell 24x7 支援 (http://www.novell.com/company/contact.html)

- Sentinel TIDS (http://support.novell.com/products/sentinel)
- Sentinel 社群支援論壇 (http://forums.novell.com/novell-product-support-forums/sentinel/)

介紹

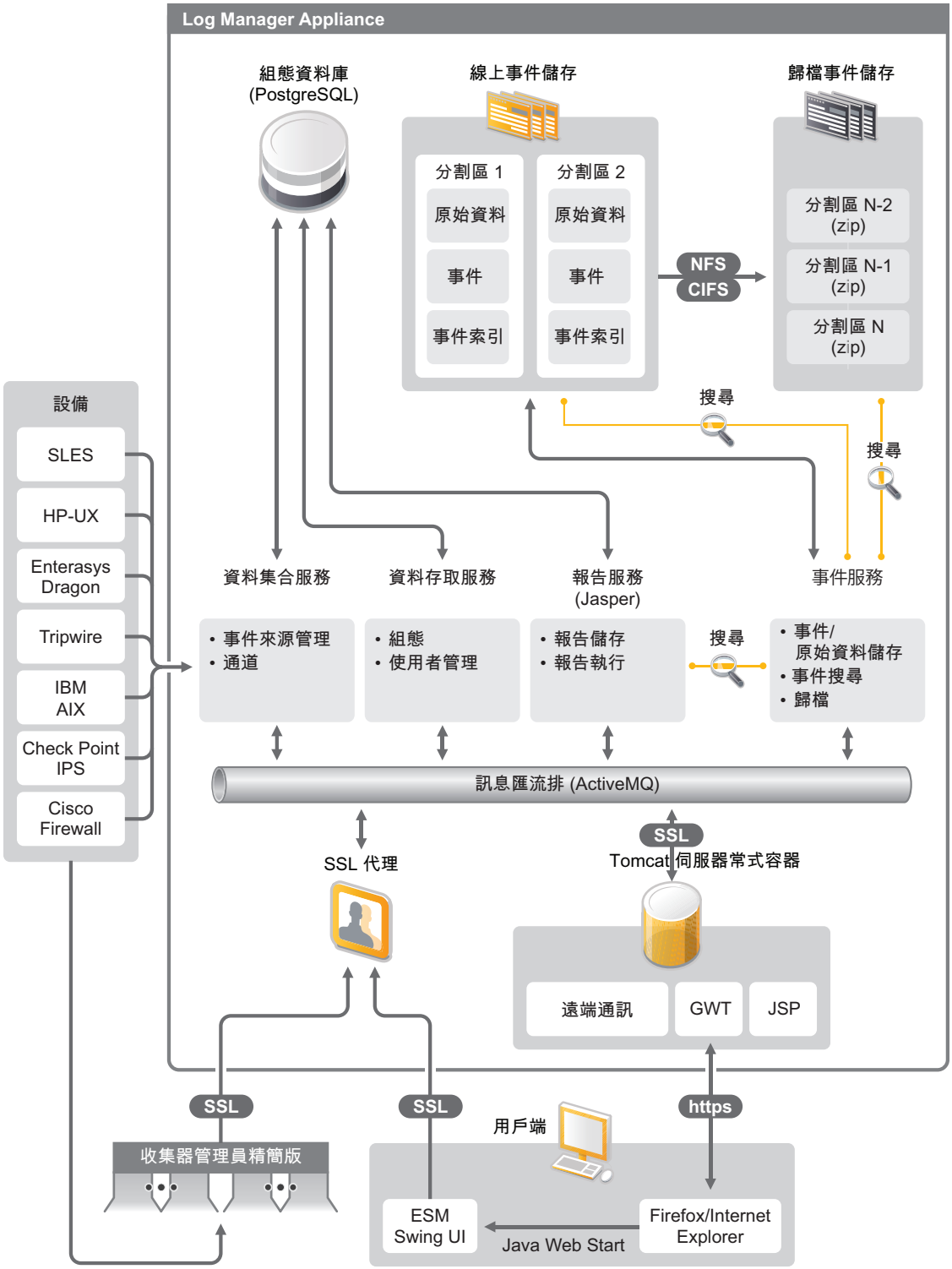
1

Novell Sentinel Log Manager 可從各種裝置和應用程式收集並管理資料，包括入侵偵測系統、防火牆、作業系統、路由器、Web 伺服器、資料庫、交換器、大型主機與防毒事件來源。Novell Sentinel Log Manager 對各種應用程式與裝置，提供高事件發生率處理、長期資料保留、規則型資料保留、區域性資料彙總，以及簡易搜尋及報告等功能。

1.1 產品綜覽

Novell Sentinel Log Manager 1.1 可爲組織提供靈活且可調整的記錄管理解決方案。Novell Sentinel Log Manager 是一種記錄管理解決方案，可以因應基本記錄收集與管理的挑戰，還可以提供專門降低管理風險的成本與複雜性，以及簡化法規遵循需求的完整解決方案。

圖 1-1 Novell Sentinel Log Manager 架構



Novell Sentinel Log Manager 有以下功能：

- 分散式搜尋能力不僅能讓客戶在本地 Sentinel Log Manager 伺服器上搜尋收集事件，而且還能從一個集中式主控台中的一或多個 Sentinel Log Manager 伺服器上搜尋收集事件
- 預先建立的法規遵循報表，可簡化產生法規遵循報表以進行稽核或鑑識分析的任務
- 客戶可以使用非專屬儲存技術，利用其現有基礎架構，進一步管理成本。
- 以瀏覽器爲基礎的使用者介面經過強化，可支援收集、儲存、報告及搜尋記錄資料等作業，進而大幅度簡化監看及管理任務。
- 透過新群組與使用者許可功能，細微且有效控制及自定資訊科技管理員，可增加 IT 基礎架構活動的透明度。

這一節包含下列資訊：

1.1.1 事件來源

Novell Sentinel Log Manager 可從產生記錄至 syslog、Windows 事件記錄、檔案、資料庫、SNMP、Novell Audit、Security Device Event Exchange (SDEE)、Check Point Open Platforms for Security (OPSEC) 以及其他儲存機制與通訊協定的事件來源收集資料。

如果有適合的連接器剖析來自這些事件來源的資料，Sentinel Log Manager 可支援所有事件來源。Novell Sentinel Log Manager 爲許多事件來源提供收集器。泛型事件收集器可從擁有適合連接器但無法辨識的事件來源中收集和處理資料。

您可以使用 「事件來源管理」介面，爲資料收集設定事件來源。

如需所支援事件來源的完整清單，請參閱第 2.6 節 「支援的事件來源」(第 19 頁)。

1.1.2 事件來源管理

「事件來源管理」介面可讓您輸入及設定 Sentinel 6.0 與 6.1 連接器與收集器。

您可以透過 「事件來源管理」視窗的即時檢視，執行以下任務：

- 使用 「組態」精靈新增或編輯事件來源的連接。
- 檢視事件來源連接的即時狀態。
- 將事件來源組態輸入至 「即時檢視」或從 「即時檢視」匯出事件來源組態。
- 檢視及設定隨 Sentinel 安裝的連接器與收集器。
- 從集中儲存機制輸入連接器與收集器，或將連接器與收集器匯出至集中儲存機制。
- 監看在設定之收集器與連接器間流通的資料。

- 檢視原始資料資訊。
- 設計、設定與建立「事件來源階層」的元件，以及使用這些元件執行必要動作。

如需詳細資訊，請參閱《*Sentinel 使用者指南* (http://www.novell.com/documentation/sentinel61/#admin)》的「事件來源管理」一節。

1.1.3 資料收集

Novell Sentinel Log Manager 可在連接器與收集器的幫助下，收集設定事件來源的資料。

收集器是一種程序檔，可將各種事件來源的資料剖析爲標準化 Sentinel 事件結構，或在某些情況下，收集其他形式外部資料來源的資料。部署每個收集器時都應該一併部署相容的連接器。連接器有助於 Sentinel Log Manager 收集器與事件或資料來源之間的連接。

Novell Sentinel Log Manager 可爲 syslog 與 Novell Audit 提供增強的網路型使用者介面支援，以輕鬆收集不同事件來源的記錄。

Novell Sentinel Log Manager 會使用各種連接方式收集資料：

- Syslog 連接器會自動接受及設定可透過「使用者資料包通訊協定」(UDP)、「傳輸控制通訊協定」(TCP) 或安全「輸送層系統」(TLS) 傳送資料的 syslog 資料來源。
- 稽核連接器會自動接受及設定啓用稽核的 Novell 資料來源。
- 檔案連接器會讀取記錄檔案。
- SNMP 連接器會接收 SNMP Trap。
- JDBC 連接器會讀取資料庫表格。
- WMS 連接器會存取桌上型電腦與伺服器的 Windows 事件記錄。
- SDEE 連接器會連接至支援 SDEE 通訊協定的設備，如 Cisco 設備。
- Check Point Log Export API (LEA) 連接器有助於 Sentinel 收集器與 Check Point 防火牆伺服器之間的整合。
- Sentinel Link 連接器會接受來自其他 Novell Sentinel Log Manager 伺服器的資料。
- 處理連接器會接受來自輸出事件記錄之自定程序的資料。

您也可以購買額外授權，來下載適用於 SAP 與大型主機作業系統的連接器。

若要取得授權，請致電 1-800-529-3400 或聯絡 Novell 技術支援 (NTS) (http://support.novell.com)。

如需有關設定連接器的詳細資訊，請參閱 Sentinel Content 網站 (http://support.novell.com/products/sentinel/sentinel61.html) 的連接器文件。

如需有關設定資料收集的詳細資訊，請參閱《*Sentinel Log Manager 1.1 管理指南*》中的「“設定資料收集”」。

附註：您必須一律下載及輸入最新版本的收集器與連接器。更新的收集器與連接器會定期發佈至 Sentinel 6.1 內容網站 (http://support.novell.com/products/sentinel/sentinel61.html)。連接器與收集器的更新包括修正、其他事件的支援以及效能改善。

1.1.4 收集器管理員

收集器管理員爲 Sentinel Log Manager 提供了靈活的資料收集點。依預設，Novell Sentinel Log Manager 會在安裝期間安裝收集器管理員。但是，您可以在網路中的適當位置，遠端安裝收集器管理員。這些遠端收集器管理員可執行連接器與收集器，並將收集的資料轉遞至 Novell Sentinel Log Manager 以進行儲存及處理。

如需有關安裝其他收集器管理員的詳細資訊，請參閱 「安裝其他收集器管理員」(第 47 頁)。

1.1.5 資料儲存

資料會從資料收集元件流向資料儲存元件。這些元件會使用檔案型資料儲存與索引系統來保留收集的設備記錄資料，並使用 PostgreSQL 資料庫來保留 Novell Sentinel Log Manager 組態資料。

資料會以壓縮格式儲存在伺服器檔案系統上，然後再儲存在設定位置以便長期儲存。您可在本地儲存資料，或將其儲存在遠端掛接的 SMB (CIFS) 或 NFS 共享上。根據在資料保留規則中設定的排程，本地與網路儲存位置中資料檔案會自動刪除

如果超過儲存位置特殊資料的資料保留時間限制，或者如果可用空間降到指定磁碟空間值以下，您可以設定資料保留規則以刪除該儲存位置的資料。

如需有關設定資料儲存的詳細資訊，請參閱《*Sentinel Log Manager 1.1 管理指南*》中的「“設定資料儲存”」。

1.1.6 搜尋與報告

搜尋與報告元件可協助您在本地與網路資料儲存以及索引系統中，搜尋及報告事件記錄資料。您可以使用一般方式搜尋儲存的事件資料，或者針對特定事件欄位 (如來源使用者名稱) 搜尋。您可以進一步精簡或過濾這些搜尋結果，並將其另存爲報表範本以供未來使用。

Sentinel Log Manager 隨附預先安裝的報表。您也可以上載其他報表。您可以按照排程或者在需要時執行報表。

如需有關預設報表清單的資訊，請參閱《*Sentinel Log Manager 1.1 管理指南*》中的「“報表”」。

如需有關搜尋事件和產生報表的資訊，請參閱《*Sentinel Log Manager 1.1 管理指南*》中的「“搜尋”」與「“報表”」。

1.1.7 Sentinel Link

可以使用「Sentinel 連結」將事件資料從某個 Sentinel Log Manager 轉遞到另一個 Sentinel Log Manager。透過由多個 Sentinel Log Manager 組成的階層式集合，可在多個地理位置維護完整的記錄，同時將較重要的事件轉遞到單一 Sentinel Log Manager 以執行集中搜尋與報告作業。

此外，Sentinel Link 可將重要事件轉遞到 Novell Sentinel (更完整的安全性資訊與事件管理 (SIEM) 系統)，以執行進階關連、事件補救與加入重要上下文資訊 (例如，伺服器重要性或來自身分管理系統的身分資訊) 等作業。

1.1.8 網路型使用者介面

Novell Sentinel Log Manager 隨附可設定及使用 Log Manager 的網路型使用者介面。使用者介面功能由網路伺服器與以 Java Web Start 爲基礎的圖形使用者介面所提供。所有使用者介面都會使用加密連線與伺服器通訊。

您可以使用 Novell Sentinel Log Manager Web 介面來執行下列任務：

- 搜尋事件
- 將搜尋準則儲存爲報告範本
- 檢視及管理報表
- 啓動「事件來源管理」介面，來爲 syslog 與 Novell 應用程式以外的資料來源設定資料收集。(僅限管理員)
- 設定資料轉遞 (僅限管理員)
- 爲遠端安裝下載 Sentinel 收集器管理員安裝程式 (僅限管理員)
- 檢視事件來源的狀態 (僅限管理員)
- 爲 syslog 與 Novell 資料來源設定資料收集 (僅限管理員)
- 設定資料儲存與檢視資料庫的狀態 (僅限管理員)
- 設定資料歸檔 (僅限管理員)
- 設定相關聯的動作，以傳送符合的事件資料到輸出通道 (僅限管理員)
- 管理使用者帳戶與許可 (僅限管理員)

1.2 安裝綜覽

您可以將 Novell Sentinel Log Manager 安裝爲裝置，或者安裝在現有 SUSE Linux Enterprise Server (SLES) 11 作業系統上。當將 Sentinel Log Manager 安裝爲裝置時，會將 Log Manager 伺服器安裝在 SLES 11 作業系統上。

依預設，Novell Sentinel Log Manager 會安裝以下元件：

- Sentinel Log Manager 伺服器
- 通訊伺服器
- 網路伺服器與網路型使用者介面
- 報告伺服器
- 收集器管理員

其中某些元件需要其他組態。

依預設，Novell Sentinel Log Manager 會安裝「收集器管理員」。如果您想要其他「收集器管理員」，可以在遠端機器上單獨予以安裝。如需詳細資訊，請參閱第 7 章 「安裝其他收集器管理員」(第 47 頁)。

系統需求

2

以下幾節說明 Novell Sentinel Log Manager 的硬體、作業系統、瀏覽器、支援的連接器以及事件來源相容性需求。

2.1 硬體需求

2.1.1 Sentinel Log Manager 伺服器

64 位元的 Intel Xeon 與 AMD Opteron 處理器支援 Novell Sentinel Log Manager，但 Itanium 處理器並不支援它。

附註：以下需求適用於 300 位元組的平均事件大小。

針對保持 90 天線上資料的生產系統，建議使用以下硬體需求：

表格 2-1 *Sentinel Log Manager 硬體需求*

需求	Sentinel Log Manager (500 EPS)	Sentinel Log Manager (2500 EPS)	Sentinel Log Manager (7500 EPS)
壓縮	最多 10:1	最多 10:1	最多 10:1
事件來源上限	最多 1000 個	最多 1000 個	最多 2000 個
事件發生率上限	500	2500	7500
CPU	一個 Intel Xeon E5450 3-GHz (4 核) CPU 或 兩個 Intel Xeon L5240 3-(雙核) CPU (共 4 核)	一個 Intel Xeon E5450 3-GHz (4 核) CPU 或 兩個 Intel Xeon L5240 3-(雙核) CPU (共 4 核)	兩個 Intel Xeon X5470 3.33-GHz (4 核) CPU (共 8 核)

需求	Sentinel Log Manager (500 EPS)	Sentinel Log Manager (2500 EPS)	Sentinel Log Manager (7500 EPS)
隨機存取記憶體 (RAM)	4 GB	4 GB	8 GB
儲存	2x 500 GB，7.2k RPM 磁碟機 (256 MB 快取的硬體 RAID，RAID 1)	2x 1 TB，7.2k RPM 磁碟機 (256 MB 快取的硬體 RAID，RAID 1)	6x 450 GB，15k RPM 磁碟機 (512 MB 快取的硬體 RAID，RAID 10)

附註：

- 一部機器可以包含多個事件來源。例如，Windows 伺服器可以包含兩個 Sentinel 事件來源，因爲您想要收集 Windows 作業系統的資料，還想收集該機器上主控之 SQL Server 資料庫的資料
- 您必須設定外部多磁碟機儲存網路區域 (SAN) 或網路附加儲存 (NAS) 的網路儲存位置。
- 建議的穩定狀態量爲最大授權 EPS 的 80%。Novell 建議您在達到此限制時，新增其他 Sentinel Log Manager 例項。

附註：事件來源上限不是硬限制，但卻是以 Novell 執行的效能測試爲基礎的建議值，且假設每個事件來源，每秒的平均事件發生率都較低 (低於 3 EPS)。較高的 EPS 率會導致可承受事件來源上限偏低。您可以使用公式 (事件來源上限) x (每個事件來源的平均 EPS) = 事件發生率上限，來得到特定平均 EPS 率或事件來源數的約略限制，只要事件來源數上限不超過上述限制即可。

2.1.2 收集器管理員伺服器

- ❑ 一個 Intel Xeon L5240 3-GHz (雙核 CPU)
- ❑ 256 MB RAM
- ❑ 10 GB 可用硬碟空間。

2.1.3 資料儲存需求預估

Sentinel Log Manager 可用於長時間保留原始資料，以符合法規及其他需求。Sentinel Log Manager 可使用壓縮來協助您有效使用本地與網路儲存空間。但是，在較長的時間內，儲存需求可能很重要。

若要克服大型儲存系統的成本限制問題，您可以使用具成本效益的資料儲存系統來長期儲存資料。磁帶型儲存系統是最常用且具成本效益的解決方案。不過，磁帶無法讓您隨機存取已存資料，但這項功能是執行快速搜尋所必需的。因此，對於儲存長期資料的需求必須採用混合方法。在此方法中，您需要搜尋的資料可於隨機存取儲存系統中獲得，而您需要保留但不需搜尋的資料會保存在具成本效益的替代物上，例如磁帶。如需使用此混合方法的指示，請參閱《*Sentinel Log Manager 1.1 管理指南*》中的「“使用順序存取儲存以長期儲存資料”」。

若要決定 Sentinel Log Manager 所需隨機存取儲存空間的量，請先預估您需要定期執行搜尋或執行報表之資料天數。您應該在本地 Sentinel Log Manager 機器上，或者在遠端「伺服器訊息區塊」(SMB) 通訊協定 (或 CIFS 通訊協定)、網路檔案系統 (NFS) 或 Sentinel Log Manager 的 SAN 上，擁有足夠的硬碟空間，以便於歸檔資料。

您還應該擁有超過需求下限的以下其他硬碟空間：

- 用於說明高於預期的資料速率。
- 用於將磁帶中的資料複製回 Sentinel Log Manager 中，以對歷程資料執行搜尋與報告。

使用以下公式，預估儲存資料所需的空間量：

- **事件資料儲存大小：**{ 天數 } x { 每秒事件量 (EPS)} x { 事件平均位元組大小 } x 0.000012 = 儲存所需 GB

  事件大小的範圍通常爲 300-1000 位元組。
- **原始資料儲存大小：**{ 天數 } x { 每秒事件量 (EPS)} x { 原始資料平均位元組大小 } x 0.000012 = 儲存所需 GB

  syslog 訊息通常的平均原始資料大小爲 200 位元組。
- **總儲存大小：**({ 事件平均位元組大小 } + { 原始資料平均位元組大小 }) x { 天數 } x { 每秒事件量 (EPS)} x 0.000012 = 儲存所需總 GB

附註：這些數目只是預估值，且取決於事件資料大小以及壓縮資料大小。

上述公式可計算將完全壓縮的資料儲存在外部儲存系統上所需的儲存空間下限。當本地儲存已滿時，Sentinel Log Manager 會壓縮資料，然後將其從本地 (部分壓縮) 移至外部 (完全壓縮) 儲存系統。因此，預估外部儲存空間需求對於資料保留來說是最重要的。若要改善最近使用資料的搜尋及報告效能，您可以增加超過 Sentinel Log Manager 硬體需求的本地儲存空間；但是，這並非必要。

您也可以使用上述公式，決定長期資料儲存系統 (如磁帶) 所需的儲存空間量。

2.1.4 虛擬環境

Sentinel Log Manager 在 VMware ESX 伺服器上受到廣泛測試及完全支援。虛擬環境中的效能結果可與實體機器測試所得結果不相上下。但是，虛擬環境應該提供與實體機器相同的建議記憶體、CPU、磁碟空間與輸入 / 輸出 (I/O)。

2.2 支援的作業系統

本節包含有關 Sentinel Log Manager 伺服器與遠端收集器管理員支援的作業系統的資訊：

- 第 2.2.1 節 「Sentinel Log Manager」(第 17 頁)
- 第 2.2.2 節 「收集器管理員」(第 18 頁)

2.2.1 Sentinel Log Manager

本節僅適用於您在現有作業系統上安裝 Sentinel Log Manager 時參考。

- ❑ 64 位元 SUSE Linux Enterprise Server 11。
- ❑ 高效能檔案系統。

  附註：ext3 檔案系統已完成所有 Novell 測試。

2.2.2 收集器管理員

您可以在以下作業系統上安裝其他收集器管理員：

- 「Linux」(第 18 頁)
- 「Windows」(第 18 頁)

Linux

- ❑ SUSE Linux Enterprise Server 10 SP2 (32 位元與 64 位元)
- ❑ SUSE Linux Enterprise Server 11 (32 位元和 64 位元)

Windows

- ❑ Windows Server 2003 (32 位元和 64 位元)
- ❑ Windows Server 2003 SP2 (32 位元和 64 位元)
- ❑ Windows Server 2008 (64 位元)

2.3 支援的瀏覽器

Sentinel Log Manager 介面已最佳化，可在以下支援的瀏覽器中，以 1280 x 1024 或更高解析度檢視：

- 第 2.3.1 節 「Linux」(第 18 頁)
- 第 2.3.2 節 「Windows」(第 18 頁)

2.3.1 Linux

- ❑ Mozilla Firefox 3.6

2.3.2 Windows

- ❑ Mozilla Firefox 3 (3.6 的效能最佳)
- ❑ Microsoft Internet Explorer 8 (8.0 的效能最佳)

Internet Explorer 8 的先決條件

- 如果將 「網際網路安全層級」設定爲 「高」，登入 Novell Sentinel Log Manager 之後，只會顯示空白頁面。若要解決此問題，請瀏覽至 *「工具」* > *「網際網路選項」* > *「安全性」索引標籤* > *「信任的網站」*。按一下 *「網站」*按鈕，將 Sentinel Log Manager 網站新增至信任的網站清單。
- 確保未選取 *「工具」* > *「相容性檢視」*選項。
- 如果未啓用 *「自動提示下載檔案」*選項，瀏覽器可能會封鎖檔案下載快顯。若要解決此問題，請瀏覽至 *「工具」* > *「網際網路選項」* > *「安全性」索引標籤* > *「自訂等級」*，然後向下捲動至下載部分，並選取 *「啓用」*來啓用 *「自動提示下載檔案」*選項。

2.4 支援的虛擬環境

- VMware ESX/ESXi 3.5/4.0 或更高
- VMPlayer 3 (僅適用於展示)
- Xen 3.1.1

2.5 支援的連接器

Sentinel Log Manager 支援 Sentinel 與 Sentinel RD 所支援的所有連接器。

- 稽核連接器
- Check Point LEA 處理連接器
- 資料庫連接器
- 資料產生器連接器
- 檔案連接器
- 處理連接器
- Syslog 連接器
- SNMP 連接器
- SDEE 連接器
- Sentinel Link 連接器
- WMS 連接器
- 大型主機連接器
- 服務通告協定 (Service Advertising Protocol, SAP) 連接器

附註：大型主機與服務通告協定 (Service Advertising Protocol, SAP) 連接器需要單獨授權。

2.6 支援的事件來源

Sentinel Log Manager 可支援各種裝置和應用程式，包括入侵偵測系統、防火牆、作業系統、路由器、Web 伺服器、資料庫、交換器、大型主機與防毒事件來源。根據處理資料的方式，即使用將事件的整個封包內容放入公用欄位中的泛型事件收集器，還是使用將資料剖析至個別欄位中的設備特定收集器，這些事件來源的資料經過剖析並標準化的層級會有所不同。

Sentinel Log Manager 支援以下事件來源：

- Cisco Firewall (6 與 7)
- Cisco Switch Catalyst 6500 系列 (CatOS 8.7)
- Cisco Switch Catalyst 6500 系列 (IOS 12.2SX)
- Cisco Switch Catalyst 5000 系列 (CatOS 4.x)
- Cisco Switch Catalyst 4900 系列 (IOS 12.2SG)
- Cisco Switch Catalyst 4500 系列 (IOS 12.2SG)
- Cisco Switch Catalyst 4000 系列 (CatOS 4.x)
- Cisco Switch Catalyst 3750 系列 (IOS 12.2SE)

- Cisco Switch Catalyst 3650 系列 (IOS 12.2SE)
- Cisco Switch Catalyst 3550 系列 (IOS 12.2SE)
- Cisco Switch Catalyst 2970 系列 (IOS 12.2SE)
- Cisco Switch Catalyst 2960 系列 (IOS 12.2SE)
- Cisco VPN 3000 (4.1.5、4.1.7 與 4.7.2)
- Extreme Networks Summit X650 (使用 ExtremeXOS 12.2.2 及較舊版本)
- Extreme Networks Summit X450a (使用 ExtremeXOS 12.2.2 及較舊版本)
- Extreme Networks Summit X450e (使用 ExtremeXOS 12.2.2 及較舊版本)
- Extreme Networks Summit X350 (使用 ExtremeXOS 12.2.2 及較舊版本)
- Extreme Networks Summit X250e (使用 ExtremeXOS 12.2.2 及較舊版本)
- Extreme Networks Summit X150 (使用 ExtremeXOS 12.2.2 及較舊版本)
- Enterasys Dragon (7.1 與 7.2)
- 通用事件收集器
- HP HP-UX (11iv1 與 11iv2)
- IBM AIX (5.2、5.3 與 6.1)
- Juniper Netscreen 系列 5
- McAfee Firewall Enterprise
- McAfee Network Security Platform (2.1、3.x 與 4.1)
- McAfee VirusScan Enterprise (8.0i、8.5i 與 8.7i)
- McAfee ePolicy Orchestrator (3.6 與 4.0)
- McAfee AV Via ePolicy Orchestrator 8.5
- Microsoft Active Directory (2000、2003 與 2008)
- Microsoft SQL Server (2005 與 2008)
- Nortel VPN (1750、2700、2750 與 5000)
- Novell Access Manager 3.1
- Novell Identity Manager 3.6.1
- Novell Netware 6.5
- Novell 模組化驗證服務 3.3
- Novell Open Enterprise Server 2.0.2
- Novell Privileged User Manager 2.2.1
- Novell Sentinel Link 1
- Novell SUSE Linux Enterprise Server
- Novell 支援網站 (http://download.novell.com/Download?buildid=RH_B5b3M6EQ~) 上可找到的 Novell eDirectory 8.8.3 (含 eDirectory 儀器使用修補程式)
- Novell iManager 2.7
- Red Hat Enterprise Linux
- Sourcefire Snort (2.4.5、2.6.1、2.8.3.2 與 2.8.4)
- Snare for Windows Intersect Alliance (3.1.4 與 1.1.1)

- ❑ Sun Microsystems Solaris 10
- ❑ Symantec AntiVirus Corporate Edition (9 與 10)
- ❑ TippingPoint Security Management System (2.1 與 3.0)
- ❑ Websense Web Security 7.0
- ❑ Websense Web Filter 7.0

附註：若要啓用 Novell iManager 與 Novell Netware 6.5 事件來源的資料收集，請針對每個事件來源，在「事件來源管理」介面中，新增收集器的例項及子連接器 (稽核收集器)。執行完此操作之後，這些事件來源會顯示在 *「Audit 伺服器」*索引標籤下的 Sentinel Log Manager Web 主控台中。

您可以從 Sentinel 6.1 內容網站 (http://support.novell.com/products/sentinel/sentinel61.html) 取得支援其他事件來源的收集器，或使用可在 Sentinel 外掛程式 SDK 網站 (http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel) 上使用之 SDK 外掛程式來建立它們。

在現有 SLES 11 系統上安裝 3

本節說明使用應用程式安裝程式，在現有 SUSE Linux Enterprise Server (SLES) 11 系統上安裝 Sentinel Log Manager 的程序。您可以使用多種方法來安裝 Sentinel Log Manager 伺服器：標準安裝程序、自定安裝程序或無訊息安裝程序 (安裝會在無使用者輸入的情況下執行，且使用預設值)。您還可以將 Sentinel Log Manager 安裝爲非根使用者。

如果您選擇自定安裝方法，可選擇使用授權金鑰安裝產品，同時選取驗證選項。除了資料庫驗證以外，您還可以爲 Sentinel Log Manager 設定 LDAP 驗證。當您針對 LDAP 驗證設定 Sentinel Log Manager 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。

如果您想要在部署中安裝多個 Sentinel Log Manager 伺服器，可以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。如需相關資訊，請參閱第 3.4 節 「靜音安裝」(第 26 頁)。

在您繼續安裝之前，請確保符合第 2 章 「系統需求」(第 15 頁) 中指定的最低需求。

3.1 開始之前

- ❑ 請確保您的硬體與軟體符合第 2 章 「系統需求」(第 15 頁) 中所述的最低需求。
- ❑ 以 hostname -f 指令傳回有效主機名稱的方法設定作業系統。
- ❑ 從 Novell 客戶服務中心 (https://secure-www.novell.com/center/ICSLogin/?%22https://secure-www.novell.com/center/regadmin/jsps/home_app.jsp%22) 取得您的授權金鑰，以安裝授權版本。
- ❑ 使用網路時間通訊協定 (NTP) 同步化時間。
- ❑ 安裝以下作業系統指令：
  - mount
  - umount
  - id
  - df
  - du
  - sudo
- ❑ 確定已在防火牆上開啓以下連接埠：

  TCP 8080、TCP 8443、TCP 61616、TCP 10013、TCP 1289、TCP 1468、TCP 1443 與 UDP 1514

3.2 標準安裝

標準安裝程序可使用所有預設選項以及 90 天試用版授權安裝 Sentinel Log Manager。

1. 從 Novell 下載網站下載並複製安裝檔案。
2. 以 root 身分登入要安裝 Sentinel Log Manager 的伺服器。
3. 指定下列指令，以從 tar 檔案擷取安裝檔案：

   ```
   tar xfz <install_filename>
   ```

   將 <*install_filename*> 取代爲安裝檔案的實際名稱。
4. 指定以下指令，執行 install-slm 程序檔，以安裝 Sentinel Log Manager：

   ```
   ./install-slm
   ```

   如果您想要將 Sentinel Log Manager 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，在無人管理的其他系統上安裝 Sentinel Log Manager。若要記錄您的安裝選項，請指定以下指令：

   ```
   ./install-slm -r responseFile
   ```
5. 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。
6. 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。

   安裝會建立 novell 群組與 novell 使用者 (如果它們不存在)。
7. 出現提示時，請指定要繼續標準安裝的選項。

   安裝會繼續使用安裝程式中包含的 90 天試用版授權金鑰。此授權金鑰可讓您在 90 天的試用期內使用完整的產品功能。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。
8. 指定管理員使用者的密碼。
9. 確認管理員使用者的密碼。

   安裝程式會選取 *「僅驗證資料庫」方法*，然後繼續安裝。

   Sentinel Log Manager 安裝完成，隨之啓動伺服器。安裝後，啓動所有服務可能會花費約 5-10 分鐘，因爲系統會執行一個單次的啓始化。等待這段時間結束，再登入伺服器。
10. 若要登入 Sentinel Log Manager 伺服器，請使用安裝輸出中指定的 URL。URL 類似於 https://10.0.0.1:8443/novelllogmanager。

    如需有關登入伺服器的詳細資訊，請參閱第 5 章 「登入網路介面」 (第 39 頁)。
11. 若要設定事件來源以將資料傳送至 Sentinel Log Manager，請參閱 《*Sentinel Log Manager 1.1 管理指南*》中的「“設定資料收集”」。

3.3 自訂安裝

如果您選擇自定安裝方法，可選擇使用授權金鑰安裝產品，同時選取驗證選項。除了資料庫驗證以外，您還可以爲 Sentinel Log Manager 設定 LDAP 驗證。當您針對 LDAP 驗證設定 Sentinel Log Manager 時，使用者可以使用 LDAP 目錄身分證明來登入伺服器。

如果在安裝過程中，您不針對 LDAP 驗證設定 Sentinel Log Manager，如有必要，可以在安裝後設定驗證。若要在安裝後設定 LDAP 驗證，請參閱《*Sentinel Log Manager 1.1 管理指南*》中的「"LDAP 驗證"」。

1. 從 Novell 下載網站下載並複製安裝檔案。
2. 以 root 身分登入要安裝 Sentinel Log Manager 的伺服器。
3. 指定下列指令，以從 tar 檔案擷取安裝檔案：

   ```
   tar xfz <install_filename>
   ```

   將 <*install_filename*> 取代爲安裝檔案的實際名稱。
4. 指定以下指令，執行 install-slm 程序檔，以安裝 Sentinel Log Manager：

   ```
   ./install-slm
   ```
5. 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。
6. 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。

   安裝會建立 novell 群組與 novell 使用者 (如果它們不存在)。
7. 出現提示時，請指定要繼續自定安裝的選項。
8. 當系統提示您指定授權金鑰選項時，請輸入 2，指定購買產品的授權金鑰。
9. 指定授權金鑰，然後按 Enter 鍵。

   如需有關授權金鑰的詳細資訊，請參閱《*Sentinel Log Manager 1.1 管理指南*》中的「"管理授權金鑰"」。
10. 指定管理員使用者的密碼。
11. 確認管理員使用者的密碼。
12. 指定資料庫管理員 (dbauser) 的密碼。
13. 確認資料庫管理員 (dbauser) 的密碼。
14. 您可以針對以下服務，在指定範圍內設定任何有效的連接埠號碼：
    - 網路伺服器
    - Java 訊息服務
    - 用戶端代理服務
    - 資料庫服務
    - 代辦內部閘道

    如果您想繼續使用預設連接埠，請輸入選項 6 以繼續自定安裝。
15. 指定選項，以透過外部 LDAP 目錄驗證使用者。
16. 指定 LDAP 伺服器的 IP 位址或主機名稱。

    預設值爲 localhost。但是，您不應該在與 Sentinel Log Manager 伺服器相同的機器上安裝 LDAP 伺服器。
17. 選取下列其中一個 LDAP 連線類型：
    - **SSL/TSL LDAP 連線：**在瀏覽器與伺服器之間建立安全連線，以進行驗證。輸入 1 以指定此選項。
    - **未加密的 LDAP 連線：**建立未加密的連線。輸入 2 以指定此選項。

18 指定 LDAP 伺服器連接埠號碼。預設的 SSL 連接埠爲 636，而預設的非 SSL 連接埠爲 389。

19 (條件) 如果您已選取 SSL/TSL LDAP 連線，請指定 LDAP 伺服器證書是否由知名的 CA 所簽署。

20 (條件) 如果您已指定 n，請指定 LDAP 伺服器證書的檔案名稱。

21 選取您是否想在 LDAP 目錄上執行匿名搜尋：

- **在 LDAP 目錄上執行匿名搜尋：**Sentinel Log Manager 伺服器可根據指定的使用者名稱，對 LDAP 目錄執行*匿名搜尋*，擷取對應 LDAP 使用者可辨識名稱 (DN)。輸入 1 以指定此方法。
- **不在 LDAP 目錄執行匿名搜尋：**輸入 2 以指定此選項。

22 (條件) 如果您已選取匿名搜尋，請指定搜尋屬性並移至步驟 25。

23 (條件) 如果您未在步驟 21 中選取匿名搜尋，請指定是否要使用 Microsoft Active Directory。

如果是 Active Directory，可選擇性地將值爲 userName@domainName 格式的 userPrincipalName 屬性，用於在搜尋 LDAP 使用者物件之前驗證使用者，而不需要輸入使用者 DN。

24 (條件) 如果您想針對 Active Directory 使用上述方法，請指定網域名稱。

25 指定 Base DN。

26 按 y 鍵以指定提供的選項正確，否則按 n 鍵並變更組態。

27 若要登入 Sentinel Log Manager 伺服器，請使用安裝輸出中指定的 URL。URL 類似於 https://10.0.0.1:8443/novelllogmanager。

如需有關登入伺服器的詳細資訊，請參閱第 5 章 「登入網路介面」(第 39 頁)。

3.4 靜音安裝

如果您需要在部署中安裝多個 Sentinel Log Manager 伺服器，無訊息或無人管理安裝 Sentinel Log Manager 很有用。在此類情況下，您可以在首次安裝期間記錄安裝參數，然後在其他所有伺服器上執行記錄的檔案。

1 從 Novell 下載網站下載並複製安裝檔案。

2 以 root 身分登入要安裝 Sentinel Log Manager 的伺服器。

3 指定下列指令，以從 tar 檔案擷取安裝檔案：

```
tar xfz <install_filename>
```

將 <*install_filename*> 取代爲安裝檔案的實際名稱。

4 指定以下指令，執行 install-slm 程序檔，以在無訊息模式下安裝 Sentinel Log Manager：

```
./install-slm -u responseFile
```

如需有關建立回應檔案的資訊，請參閱第 3.2 節 「標準安裝」(第 24 頁)。安裝會以回應檔案中儲存的值繼續。

5 若要登入 Sentinel Log Manager 伺服器，請使用安裝輸出中指定的 URL。URL 類似於 https://10.0.0.1:8443/novelllogmanager。

如需有關登入伺服器的詳細資訊，請參閱第 5 章 「登入網路介面」(第 39 頁)。

6 若要設定事件來源以將資料傳送至 Sentinel Log Manager，請參閱 《“Sentinel Log Manager 1.1 管理指南”》中的「“設定資料收集”」。

3.5 非 Root 安裝

如果您的組織規則不允許您以 root 身分執行 Sentinel Log Manager 的完整安裝，則可以其他使用者身分執行大多數安裝步驟。

1. 從 Novell 下載網站下載並複製安裝檔案。
2. 指定下列指令，以從 tar 檔案擷取安裝檔案：

   `tar xfz <install_filename>`

   將 <*install_filename*> 取代爲安裝檔案的實際名稱。
3. 以 root 身分登入要以 root 身分安裝 Sentinel Log Manager 的伺服器。
4. 請指定以下指令：

   `./bin/root_install_prepare`

   以根權限執行之指令清單會顯示出來。

   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，以變更爲新建立的非根 novell 使用者：novell：

   su novell
7. 請指定以下指令：

   `./install-slm`
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，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。
10. 系統會提示您指定安裝模式。
    - 如果您選取繼續標準安裝，請遵循第 3.2 節 「標準安裝」(第 24 頁) 中的步驟 8 到步驟 11。
    - 如果您選取繼續自定安裝，請遵循第 3.3 節 「自訂安裝」(第 24 頁) 中的步驟 8 到步驟 23。

    Sentinel Log Manager 安裝完成，且隨之啓動伺服器。
11. 指定以下指令，以變更爲 root 使用者：

    `su root`
12. 指定以下指令以完成安裝：

    ./bin/root_install_finish
13. 若要登入 Sentinel Log Manager 伺服器，請使用安裝輸出中指定的 URL。URL 類似於 https://10.0.0.1:8443/novelllogmanager。

    如需有關登入伺服器的詳細資訊，請參閱第 5 章 「登入網路介面」(第 39 頁)。

安裝裝置

4

Novell Sentinel Log Manager 裝置是一種準備好可以隨時執行的軟體裝置，建立於 SUSE Studio (結合強化的 SUSE Linux Enterprise Server (SLES) 11 作業系統與 Novell Sentinel Log Manager 軟體整合的更新服務) 上，可提供簡單且無接縫的使用者體驗，並可讓客戶利用現有投資。可以將軟體裝置安裝在硬體或虛擬環境中。

4.1 開始之前

- 確保符合硬體需求。如需詳細資訊，請參閱第 2.1 節 「硬體需求」(第 15 頁)。
- 從 Novell 客戶服務中心 (http://www.novell.com/center) 取得您的授權金鑰，以安裝授權版本。
- 從 Novell 客戶服務中心 (http://www.novell.com/center) 取得登錄碼，以登錄軟體更新。
- 使用網路時間通訊協定 (NTP) 同步化時間。
- (條件) 如果您計劃使用 VMware，請確定 VMware Converter 同時上載影像至 VMware ESX 伺服器，並將其轉換爲可在 ESX 伺服器上執行的格式。

4.2 使用的連接埠

請注意，Novell Sentinel Log Manager 裝置會使用以下連接埠進行通訊，其中一些已在防火牆上開啓：

4.2.1 在防火牆中開啓的連接埠

表格 4-1 *Sentinel Log Manager 使用的網路連接埠*

連接埠	描述
TCP 1289	用於 Novell Audit 連線。
TCP 289	針對 Novell Audit 連線，轉遞至 1289。

連接埠	描述
TCP 22	用於保護對 Sentinel Log Manager 裝置的外圍程序存取。
UDP 1514	用於 syslog 訊息。
UDP 514	針對 syslog 訊息，轉遞至 1514。
TCP 8080	用於 HTTP 通訊。Sentinel Log Manager 裝置也會將其用於更新服務。
TCP 80	針對 Sentinel Log Manager Web 伺服器，轉遞至 8080，以進行 HTTP 通訊。Sentinel Log Manager 裝置也會將其用於更新服務。
TCP 8443	用於 HTTPS 通訊。Sentinel Log Manager 裝置也會將其用於更新服務。
TCP 1443	用於 SSL 加密 syslog 訊息。
TCP 443	針對 Sentinel Log Manager Web 伺服器，轉遞至 8443，以進行 HTTPS 通訊。Sentinel Log Manager 裝置也會將其用於更新服務。
TCP 61616	用於收集器管理員與伺服器之間的通訊。
TCP 10013	由「事件來源管理」使用者介面 SSL 代理所用。
TCP 54984	由 Sentinel Log Manager 裝置管理主控台 (WebYaST) 所用。
TCP 1468	用於 syslog 訊息。

4.2.2 本地使用的連接埠

表格 4-2 *用於本地通訊的連接埠*

連接埠	描述
TCP 61617	用於 Web 伺服器與伺服器之間的內部通訊。
TCP 5556	與 internal_gateway_server 以及 internal_gateway 一起，在內部通訊的回路介面上使用。可將其用於代辦引擎與收集器管理員之間的內部通訊。
TCP 5432	用於 PostgreSQL 資料庫。依預設，您不需要開啓此連接埠。但是，如果您要使用 Sentinel SDK 來開發報表，則必須開啓此連接埠。如需詳細資訊，請參閱 Sentinel 外掛程式 SDK 網站 (http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel)。
兩個隨機選取的其他 TCP 連接埠	用於代辦引擎與收集器管理員之間的內部通訊。
TCP 8005	用於與 Tomcat 程序之間的內部通訊。
TCP 32000	用於代辦引擎與收集器管理員之間的內部通訊。

4.3 安裝 VMware 裝置

若要從 VMware ESX 伺服器執行裝置影像，請在伺服器上輸入並安裝裝置影像。

1 下載 VMware 裝置安裝檔案。

VMware 裝置正確檔案的檔名中含有 vmx 例如 Sentinel_Log_Manager_1.1.0.0_64_VMX.x86_64-0.777.0.vmx.tar.gz

2 建立可安裝裝置影像的 ESX 資料儲存。

3 以 Administrator 身分登入要安裝裝置的伺服器。

4 指定下列指令，以從安裝 VM Converter 的機器中解壓縮壓縮的裝置影像：

tar zxvf <*install_file*>

將 <*install_file*> 取代爲實際檔案名稱。

5 若要將 VMware 影像輸入至 ESX 伺服器，請使用 VMware Converter，然後遵照安裝精靈中畫面上的指示進行。

6 登入 ESX 伺服器機器。

7 選取裝置的輸入 VMware 影像，然後按一下 *「開啓電源」*圖示。

8 選取您選擇的語言，然後按一下 *「下一步」*。

9 選取鍵盤配置，然後按一下 *「下一步」*。

10 閱讀並接受「Novell SUSE Enterprise Server Software 授權合約」。

11 閱讀並接受「Novell Sentinel Log Manager 使用者授權合約」。

12 在「主機名稱」與「網域名稱」螢幕中，指定主機名稱與網域名稱。請確保選取 *「將主機名稱寫入 /etc/hosts」*選項。

13 選取「*下一步*」。儲存主機名稱組態。

14 請執行下列其中一個步驟：

- 若要使用目前網路連線設定，請在 *「網路組態 II」*螢幕中選取 *「使用下列組態」*。
- 若要變更網路連線設定，請選取 *「變更」*。

15 設定「時間與日期」，按一下 *「下一步」*，然後按一下 *「完成」*。

附註：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啓動 NTP：

```
rcntp restart
```

---

16 設定 Novell SUSE Enterprise Server root 密碼，然後按一下 *「下一步」*。

17 設定 root 密碼，然後按一下 *「下一步」*。

18 設定 Sentinel Log Manager admin 密碼與 dbauser 密碼，然後按一下 *「下一步」*。

19 選取「*下一步*」。儲存網路連線設定。

安裝會繼續，直到完成。將主控台中顯示的裝置 IP 位址記下來。

20 繼續進行第 4.6 節 「安裝裝置後的設定」(第 34 頁)。

4.4 安裝 Xen 裝置

1 下載 Xen 虛擬裝置安裝檔案，並將其複製到 /var/lib/xen/images。

Xen 虛擬裝置的正確檔名包含 xen。例如 Sentinel_Log_Manager_1.1.0.0_64_Xen.x86_64-0.777.0.xen.tar.gz

2 指定下列指令，來解壓縮檔案：

```
tar -xvzf <install_file>
```

將 <*install_file*> 取代爲安裝檔案的實際名稱。

3 變更爲新的安裝目錄。此目錄包含下列檔案：

- <*file_name*>.raw 影像檔案
- <*file_name*>.xenconfig 檔案

4 使用文字編輯器開啓 <*file_name*>.xenconfig 檔案。

5 按如下所示修改檔案：

在磁碟設定中，指定 .raw 檔案的完整路徑。

爲您的網路組態指定橋接器設定。例如 "bridge=br0" 或 "bridge=xenbr0"。

指定名稱與記憶體設定的值。

例如：

```
# -*- mode: python; -*-
name="Sentinel_Log_Manager_1.1.0.0_64"
memory=4096
disk=[ "tap:aio:/var/lib/xen/images/Sentinel_Log_Manager_1.1.0.0_64_Xen-
0.777.0/Sentinel_Log_Manager_1.1.0.0_64_Xen.x86_64-0.777.0.raw,xvda,w" ]
vif=[ "bridge=br0" ]
```

6 修改 <*filename*>.xenconfig 檔案之後，指定下列指令，來建立 VM：

xm create <*file_name*>.xenconfig

7 (選用) 若要驗證是否建立 VM，請指定下列指令：

xm list

VM 即會顯示在清單中。

例如，如果您已設定 .xenconfig 檔案中的 name=” Sentinel_Log_Manager_1.1.0.0_64”，則 VM 會以該名稱顯示。

8 若要開始安裝，請指定下列指令：

xm console <*vm name*>

將 <*vm_name*> 取代爲在 .xenconfig 檔案的名稱設定中指定的名稱，該名稱也是在步驟 7 中傳回的值。例如：

xm console Sentinel_Log_Manager_1.1.0.0_64

9 選取您選擇的語言，然後按一下 *「下一步」*。

10 選取鍵盤配置，然後按一下 *「下一步」*。

11 閱讀並接受「Novell SUSE Enterprise Server Software 授權合約」。

12 閱讀並接受「Novell Sentinel Log Manager 使用者授權合約」。

13 在「主機名稱」與「網域名稱」螢幕中，指定主機名稱與網域名稱。請確保選取 *「將主機名稱寫入 /etc/hosts」* 選項。

14 選取「 *下一步*」。儲存主機名稱組態。

15 請執行下列其中一個步驟：

- 若要使用目前網路連線設定，請在 *「網路組態 II」* 螢幕中選取 *「使用下列組態」*。
- 若要變更網路連線設定，請選取 *「變更」*。

16 設定「時間與日期」，按一下 *「下一步」*，然後按一下 *「完成」*

附註：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啓動 NTP：

```
rcntp restart
```

17 設定 Novell SUSE Enterprise Server root 密碼，然後按一下 *「下一步」*。

18 設定 Sentinel Log Manager admin 密碼與 dbauser 密碼，然後按一下 *「下一步」*。

安裝會繼續，直到完成。將主控台中顯示的裝置 IP 位址記下來。

19 繼續進行第 4.6 節 「安裝裝置後的設定」(第 34 頁)。

4.5 在硬體上安裝裝置

在硬體上安裝裝置之前，請確保已從支援網站下載並解壓縮裝置 ISO 磁碟影像，且在 DVD 上可用。

1 使用 DVD 光碟機中的 DVD 啓動實體機器。

2 使用安裝精靈的畫面上指示。

3 選取開機功能表中的頂端項目，來執行 Live DVD 裝置影像。

4 閱讀並接受「Novell SUSE Enterprise Server Software 授權合約」。

5 閱讀並接受「Novell Sentinel Log Manager 使用者授權合約」。

6 選取「 *下一步*」。

7 在「主機名稱」與「網域名稱」螢幕中，指定主機名稱與網域名稱。

請確保選取 *「將主機名稱寫入 /etc/hosts」* 選項。

8 選取 *「下一步」*。儲存主機名稱組態。

9 請執行下列其中一個步驟：

- 若要使用目前網路連線設定，請在「網路組態 II」螢幕中選取 *「使用下列組態」*。
- 若要變更網路連線設定，請選取 *「變更」*。

10 選取「 *下一步*」。儲存網路連線設定。

11 設定「時間與日期」，然後按一下 *「下一步」*。

附註：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啓動 NTP：

```
rcntp restart
```

12 設定 root 密碼，然後按一下 *「下一步」*。

13 設定 Sentinel Log Manager admin 密碼與 dbauser 密碼，然後按一下 *「下一步」*。

14 在主控台中輸入使用者名稱與密碼，以登入裝置。

使用者名稱的預設值爲 root，密碼的預設值爲 password。

15 若要在實體伺服器上安裝裝置，請執行下列指令：

```
/sbin/yast2 live-installer
```

安裝會繼續，直到完成。將主控台中顯示的裝置 IP 位址記下來。

16 繼續進行第 4.6 節 「安裝裝置後的設定」(第 34 頁)。

4.6 安裝裝置後的設定

若要登入裝置網路主控台並啓始化軟體：

1 開啓網頁瀏覽器並登入 https://*<IP 位址>*:*8443*。即會顯示 Sentinel Log Manager 網路頁面。

安裝完成且伺服器重新啓動之後，會在裝置主控台上顯示裝置的 IP 位址。

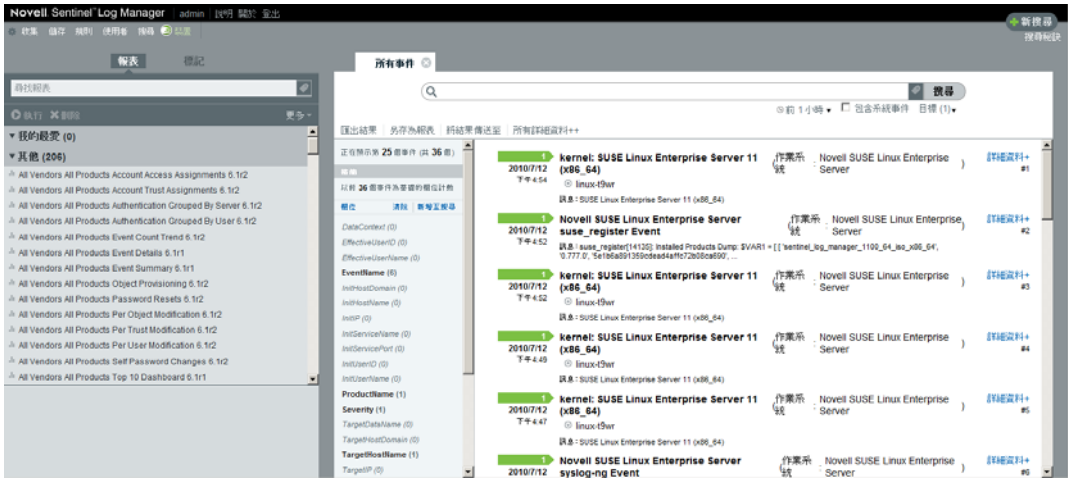
2 您可以設定資料儲存與資料收集的 Sentinel Log Manager 裝置。如需有關設定裝置的詳細資訊，請參閱《*Sentinel Log Manager 1.1 管理指南*》。

3 若要註冊以進行更新，請參閱第 4.8 節 「登錄以進行更新」(第 36 頁)。

4.7 設定 WebYaST

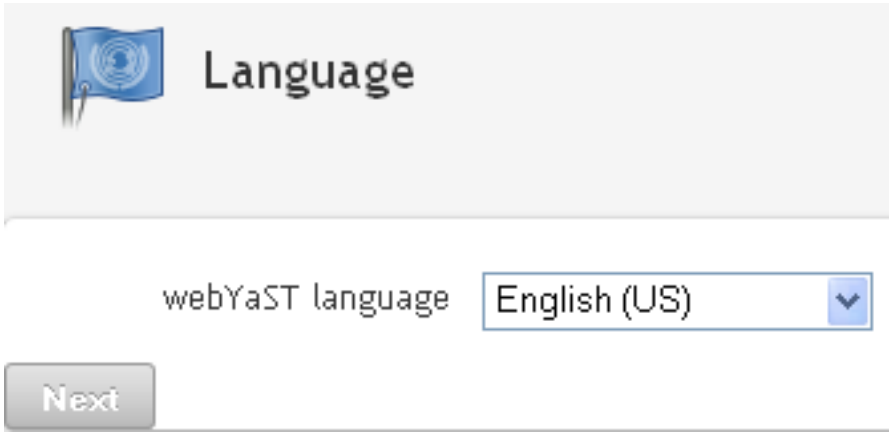
Novell Sentinel Log Manager 裝置使用者介面隨附 WebYaST。WebYaST 是一個網路型遠端主控台，可用來控制以 SUSE Linux Enterprise 爲基礎的裝置。您可以使用 WebYaST 存取、設定及監看 Sentinel Log Manager 裝置。下列程序簡要說明設定 WebYaST 的步驟。如需有關詳細組態的更多資訊，請參閱《WebYaST 使用者指南 (http://www.novell.com/documentation/webyast/)》。

1 登入 Sentinel Log Manager 裝置。

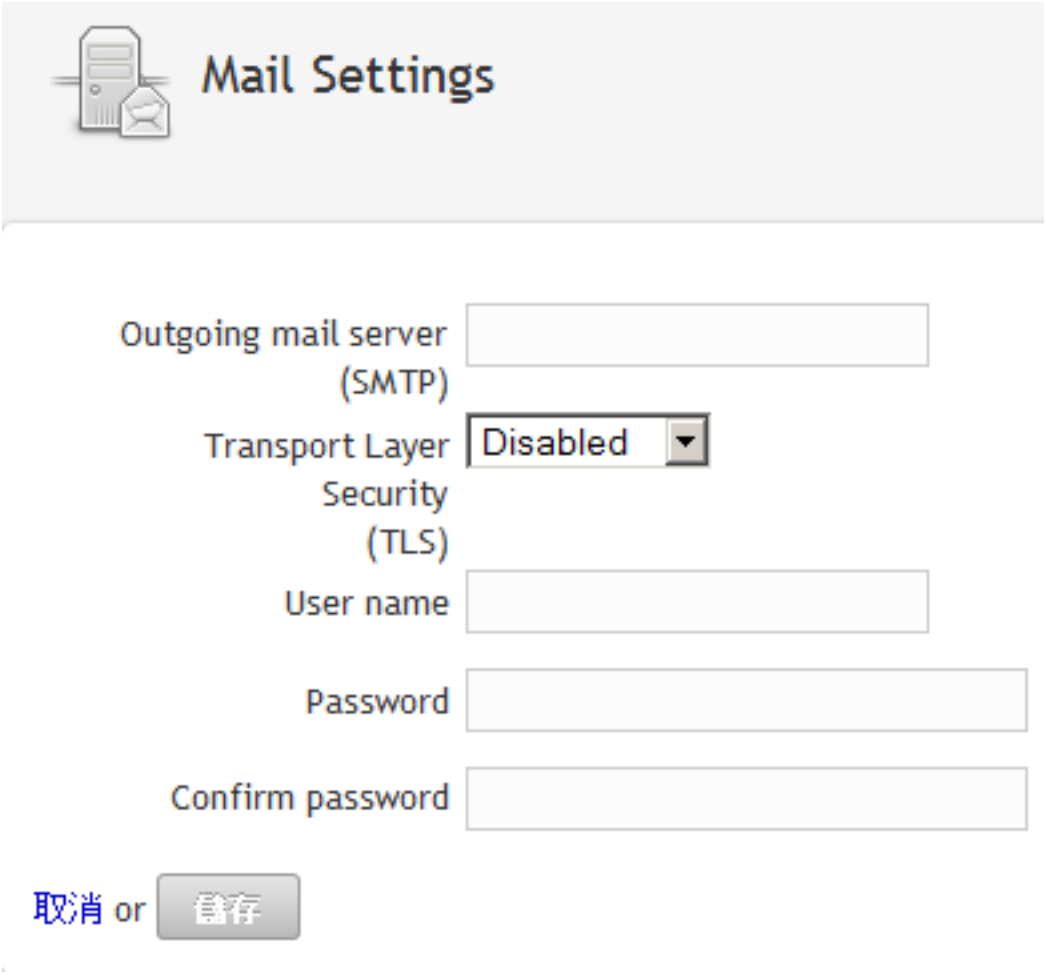


2 按一下 「*裝置*」。

3 指定系統的登入身分證明，然後按一下 「*登入*」



4 選取您選擇的語言，然後按一下 「*下一步*」



5 指定設定郵件伺服器的詳細資訊，然後按一下 「*儲存*」。

此時即顯示登錄頁面。

6 將 Sentinel Log Manager Server 設定爲接收更新，如第 4.8 節 「登錄以進行更新」 (第 36 頁) 中所述。

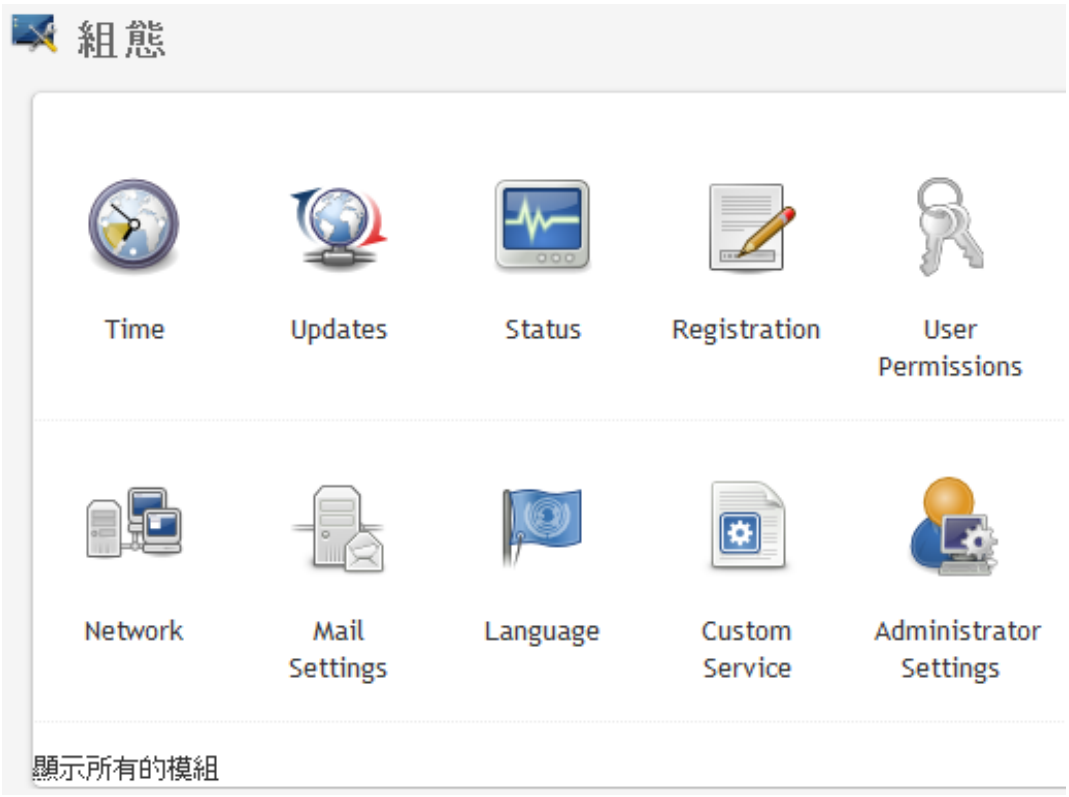
7 按一下 「*下一步*」完成初步設定。

4.8 登錄以進行更新

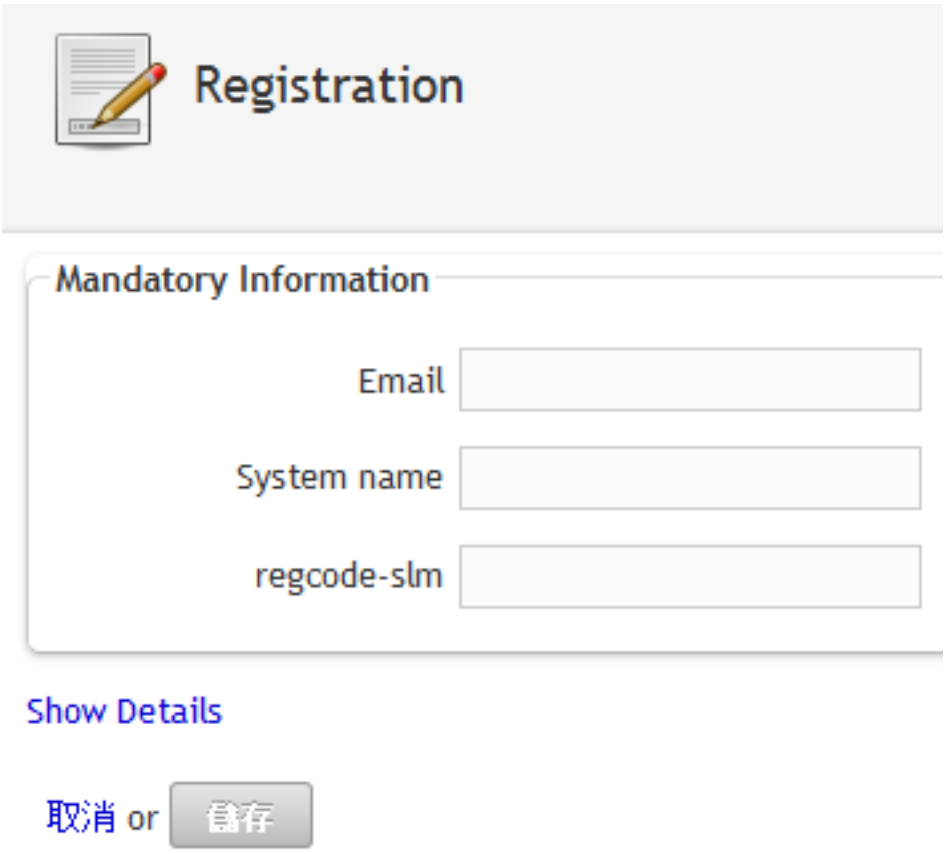
1 登入 Sentinel Log Manager 裝置。

即會顯示 Sentinel Log Manager 網路使用者介面。

2 按一下 「*裝置*」來啓動 WebYaST。


組態
Time
Updates
Status
Registration
User Permissions
Network
Mail Settings
Language
Custom Service
Administrator Settings
顯示所有的模組

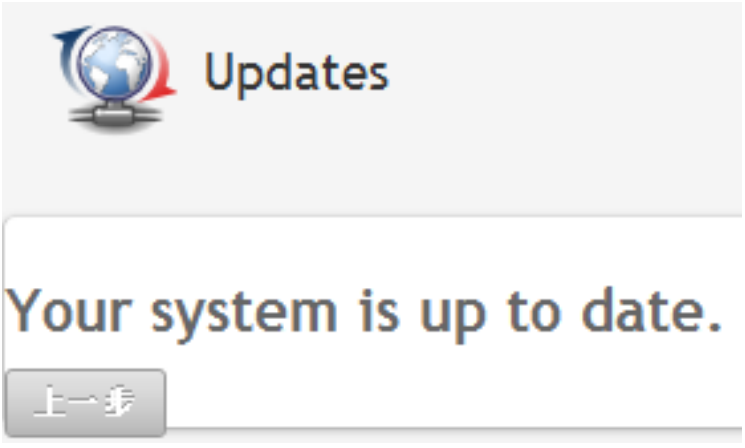
3 按一下 「*登錄*」。



4 指定裝置登錄碼。

5 按一下 *「儲存」*。

6 若要檢查是否有更新，請按一下 *「更新」*。
產生的頁面會指示是否有更新。



5 登入網路介面

安裝期間建立的管理員使用者可以登入網路介面，來設定並使用 Sentinel Log Manager：

1. 開啓支援的網頁瀏覽器。如需詳細資訊，請參閱第 2.3 節 「支援的瀏覽器」(第 18 頁)。
2. 指定 Novell Sentinel Log Manager 頁面的 URL (例如 https://10.0.0.1:8443/novelllogmanager)，然後按下 Enter 鍵。
3. (條件) 當您第一次登入 Sentinel Log Manager 時，系統會提示您是否接受證書。當您接受證書時，會顯示 Sentinel Log Manager 登入頁面。

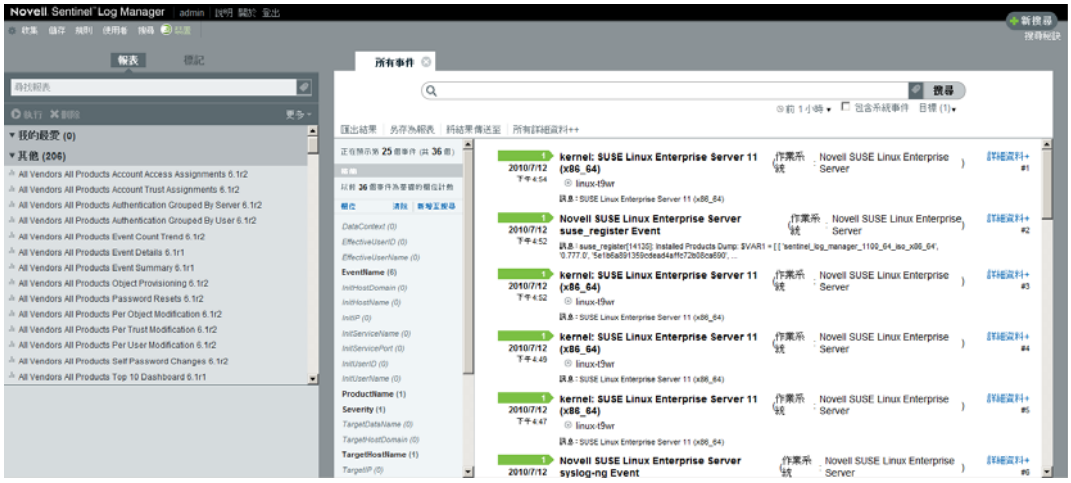
4 指定 Sentinel Log Manager 管理員的使用者名稱與密碼。

5 選取 Sentinel Log Manager 介面的語言。

Sentinel Log Manager 使用者介面有英文、葡萄牙文、法文、義大利文、德文、西班牙文、日文、繁體中文或簡體中文。

6 按一下 「*登入*」。

即會顯示 Novell Sentinel Log Manager 網路使用者介面。



升級 Sentinel Log Manager 6

您可以使用升級程序檔，將 Novell Sentinel Log Manager 從 1.0.0.4 或更高版本升級到 Sentinel Log Manager 1.1。

6.1 從 1.0 升級到 1.1

1. 如果您的 Sentinel Log Manager server 版本低於 1.0.0.4. 版，您必須先將其升級到 1.0.0.4 或更高版本。
2. 從 Novell 下載網站下載並複製安裝檔案。
3. 以 root 身分登入要安裝 Sentinel Log Manager 的伺服器。
4. 指定下列指令，以停止 Sentinel Log Manager 伺服器：

   ```
   <install_directory>/bin/server.sh stop
   ```

   例如 /opt/novell/sentinel_log_mgr_1.0_x86-64/bin/server.sh stop
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*> 取代爲安裝檔案的實際名稱。
6. 指定下列指令，以執行 install-slm 程序檔，來升級 Sentinel Log Manager：

   ```
   ./install-slm
   ```
7. 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。
8. 閱讀使用者授權，並輸入 yes 或 y，接受授權，然後繼續安裝。
9. 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。如果您按下 n 鍵，安裝會終止。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。

   會將現有 Sentinel Log Manager 1.0 安裝完整保留不動，以下狀況除外：

   - 如果 1.0 資料目錄 (例如 /opt/novell/sentinel_log_manager_1.0_x86-64/data) 與 1.1 資料目錄 (例如 /var/opt/novell/sentinel_log_mgr/data) 在相同檔案系統中，會將 <1.0>/data/eventuate 與 <1.0>/data/rawdata 子目錄移動到 1.1 位置，因爲通常 eventdata 與 rawdata 目錄都很大。如果 1.0 資料與 1.1 資料目錄在不同檔案系統中，會將 eventdata 與 rawdata 子目錄複製到 1.1 位置，而將 1.0 檔案保持完整不動。
   - 如果現有 1.0 資料目錄 (例如 /opt/novell/sentinel_log_mgr_1.0_x86-64) 在單獨掛接的檔案系統上，且包含 1.1 資料目錄 (/var/opt/novell/sentinel_log_mgr/data) 的檔案系統空間不足，您可以允許安裝程式將檔案系統從 1.0 位置重新掛接到 1.1 位置。也會更新 /etc/fstab 中的所有項目。如果您決定不允許安裝程式重新掛接現有檔案系統，則升級會結束。然後，您可以在檔案系統上爲 1.1 資料目錄建立足夠的空間。

10 當 Sentinel Log Manager 1.1 安裝成功且伺服器可以正常操作時，您必須指定下列指令，來手動移除 Sentinel Log Manager 1.0 目錄：

```
rm -rf /opt/novell/slm_1.0_install_directory
```

例如：

```
rm -rf /opt/novell/sentinel_log_mgr_1.0_x86-64
```

移除安裝目錄會永久刪除 Sentinel Log Manager 1.0 安裝

6.2 升級收集器管理員

1 以管理員身分登入 Sentinel Log Manager。

2 選取 *「收集」* > *「進階」*。

3 按一下「收集器管理員升級安裝程式」部分中的 *「下載安裝程式」*連結。

即會顯示視窗，其中包含開啓或將 scm_upgrade_installer.zip 檔案儲存在本地機器上的選項。儲存檔案。

4 將檔案複製到暫存位置。

5 解壓縮 .zip 檔案的內容。

6 根據您的作業軟體，以收集器管理員安裝擁有者的身分，執行下列其中一個升級檔案：

- 若要升級 Windows 收集器管理員，請執行 service_pack.bat。
- 若要升級 Linux 收集器管理員，請執行 service_pack.sh。

7 依照螢幕上的指示完成安裝。

8 重新啓動機器。

6.3 從 1.0 裝置移轉至 1.1 裝置

如果您已安裝 Sentinel Log Manager 1.0，並且要移轉至 Sentinel Log Manager 裝置 1.1，請按照如下所述的步驟，來移轉資料與組態

1 (條件) 如果安裝的 Sentinel Log Manager 版本低於 1.0 hotfix 4，請將其升級至 Sentinel Log Manager 1.0 hotfix 5，該版本是最新可用的 hotfix。從 Novell 修補程式下載網站 (http://download.novell.com/protected/Summary.jsp?buildid=VgZ3aerzjYc~) 下載 Hotfix。

附註：您必須是已註冊的使用者，才能下載修補程式。如果您尚未註冊，請按一下「註冊」，以在修補程式下載網站中建立使用者帳戶。

---

2 升級至 Sentinel Log Manager 1.1。如需詳細資訊，請參閱第 6.1 節 「從 1.0 升級到 1.1」 (第 43 頁)。

3 指定下列指令，以變更爲 novell 使用者：

```
su -novell
```

4 指定下列指令，以變更爲 /bin 目錄：

```
cd /opt/novell/sentinel_log_mgr/bin
```

5 指定下列指令，以完全備份 Sentinel Log Manager 1.1 資料與組態。

```
./backup_util.sh -m backup -c -e -l -r -s -w -f $APP_HOME/data/
<backupfilename>
```

將 <*backupfilename*> 取代爲檔案名稱，以儲存備份資料。

如需有關備份資料的詳細資訊，請參閱 “備份與還原資料”。

6 在個別機器上安裝 Sentinel Log Manager 裝置 1.1。如需詳細資訊，請參閱第 4 章 「安裝裝置」(第 29 頁)。

7 將包含備份資料的檔案複製到新安裝的 Sentinel Log Manager 1.1 裝置上。

8 請指定以下指令：

```
chown novell:novell <backfupfilename>
```

9 指定下列指令，以變更爲 /bin 目錄：

```
cd /opt/novell/sentinel_log_mgr/bin
```

10 指定下列指令，以完全還原從 Sentinel Log Manager 1.1 應用程式備份的資料：

```
./backup_util.sh -m restore -f $APP_HOME/data/<backupfilename>
```

如需詳細資訊，請參閱「“備份與還原資料”」。

安裝其他收集器管理員

7

收集器管理員可管理 Novell Sentinel Log Manager 的所有資料收集與資料剖析。依預設，Sentinel Log Manager 安裝程序會將收集器管理員安裝在 Sentinel Log Manager 伺服器上。但是，您可在分散式安裝中安裝多個收集器管理員。

7.1 開始之前

- 請確保您的硬體與軟體符合第 2 章 「系統需求」(第 15 頁) 中所述的最低需求。
- 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 Log Manager 伺服器上的訊息匯流排連接埠 (61616)。在您開始安裝 「收集器管理員」之前，請確保允許所有防火牆及其他網路設定透過此連接埠進行通訊。

7.2 其他收集器管理員的優勢

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。
- **可以從其他作業系統收集資料：**例如，您可以在 Microsoft Windows 上安裝收集器管理員，以透過 WMI 通訊協定收集資料。
- **檔案快取：**當您啓用檔案快取時，遠端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。

7.3 安裝其他收集器管理員

1. 以管理員身分登入 Sentinel Log Manager。
2. 選取 *「收集」> 「進階」*。
3. 按一下 「收集器管理員安裝程式」部分中的 *「下載安裝程式」*連結。

   即會顯示視窗，其中包含開啓或將 scm_installer.zip 檔案儲存在本地機器上的選項。儲存檔案。
4. 將檔案複製並解壓縮到您要安裝收集器管理員的位置。
5. 根據您的作業軟體，執行下列其中一個安裝檔案：
   - 若要在 Windows 系統上安裝收集器管理員，請執行 setup.bat。
   - 若要在 Linux 系統上安裝收集器管理員，請執行 setup.sh。

6 選取語言，然後按一下 *「確定」*。

即會顯示 InstallShield。

7 按一下「確定」。

8 閱讀並接受授權合約，然後按一下 *「下一步」*。

9 您可以使用預設安裝目錄，或瀏覽並選取目錄，然後按一下 *「下一步」*。

10 不變更預設訊息匯流排連接埠 (61616)，並指定通訊伺服器的主機名稱，然後按一下 *「下一步」*。

11 按一下 *「下一步」* 使用預設的自動記憶體組態 (256 百萬位元組)。

隨即顯示安裝摘要。

12 按一下 *「安裝」*。

13 指定收集器管理員的使用者名稱和密碼。

附註：會將使用者名稱與密碼儲存在 /etc/opt/novell/sentinel_log_mgr/config/activemqusers.properties 檔案中，該檔案位於 Sentinel Log Manager 伺服器上。

---

14 提示時，永久接受證書。

15 按一下 *「完成」* 以完成安裝。

16 重新啓動機器。

解除安裝 Sentinel Log Manager 8

本節介紹解除安裝 Novell Sentinel Log Manager 伺服器與收集器管理員的程序。

8.1 解除安裝裝置

如果您要保留任何 Log Manager 資料，則必須在解除安裝裝置之前備份資料，以便稍後可以還原資料。如需詳細資訊，請參閱《*Sentinel Log Manager 1.1 管理指南*》中的「“備份與還原資料”」。

如果您不需要保留任何資料，請使用下列程序來解除安裝裝置：

- **VMware ESX 裝置**：若虛擬機器專用來執行 Novell Sentinel Log Manager 而且您不需要保留任何資料，請刪除虛擬機器以解除安裝 Log Manager 虛擬裝置。
- **Xen 裝置**：若 Xen 虛擬機器專用來執行 Novell Sentinel Log Manager 而且您不需要保留任何資料，請刪除它以解除安裝 Log Manager 虛擬裝置。
- **硬體裝置**：若系統專用來執行 Novell Sentinel Log Manager 而且您不需要保留任何資料，請重新格式化硬碟以解除安裝實體機器上的 Log Manager。

8.2 從現有 SLES 11 系統解除安裝

1. 以 root 身分登入 Sentinel Log Manager 伺服器。
2. 若要執行解除安裝程序檔，請執行下列指令：

   ```
   /opt/novell/sentinel_log_mgr/setup/uninstall-slm
   ```
3. 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。

   會先停止 Sentinel Log Manager 伺服器，然後將其解除安裝。

8.3 解除安裝收集器管理員

本節介紹安裝在 Windows 或 Linux 機器上的 Sentinel 收集器管理員之解除安裝程序。

8.3.1 解除安裝 Linux 收集器管理員

1. 以 root 的身分登入。
2. 在安裝收集器管理員的機器中，瀏覽至下列位置：

   $ESEC_HOME/_unist

3 執行以下指令：

```
./uninstall.bin
```

4 選取語言，然後按一下 *「確定」*。

5 在 InstallShield 精靈中，按一下 *「下一步」*。

6 選取您要解除安裝的功能，然後按一下 *「下一步」*。

7 停止正在執行的所有 Sentinel Log Manager 應用程式，然後按一下 *「下一步」*。

8 按一下 *「解除安裝」*。

9 按一下 *「完成」*。

10 選取 *「重新啓動系統」*，然後按一下 *「完成」*。

8.3.2 解除安裝 Windows 收集器管理員

1 以管理員身分登入。

2 停止 Sentinel Log Manager 伺服器。

3 選取「開始」>「執行」。

4 指定下列項目：

```
%Esec_home%\_uninst
```

5 連按兩下 uninstall.exe 來執行它。

6 選取語言，然後按一下 *「確定」*。

即會顯示「Install Shield 精靈」。

7 按一下「下一步」。

8 選取您要解除安裝的功能，然後按一下 *「下一步」*。

9 停止正在執行的所有 Sentinel Log Manager 應用程式，然後按一下 *「下一步」*。

10 按一下 *「解除安裝」*。

11 按一下 *「完成」*。

12 選取 *「重新啓動系統」*，然後按一下 *「完成」*。

8.3.3 手動清理目錄

- 「Linux」(第 50 頁)
- 「Windows」(第 50 頁)

Linux

1 以 root 身分登入從中解除安裝收集器管理員的機器。

2 停止所有 Sentinel Log Manager 程序。

3 移除 /opt/novell/sentinel6 的內容

Windows

1 以管理員身分登入從中解除安裝收集器管理員的機器。

2 刪除 %CommonProgramFiles%\InstallShield\Universal 資料夾與該資料夾下的所有內容。

3 刪除 %ESEC_HOME% 資料夾。預設爲 C:\Program Files\Novell\Sentinel6。

安裝作業疑難排解

A

本節包含安裝期間可能發生的一些問題，以及解決問題的程序。

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 Log Manager。

若要解決此問題，請正確設定網路設定。驗證組態時，ifconfig 指令應傳回有效 IP 位址，而 hostname -f 指令應傳回有效主機名稱。

A.2 無法使用 SLES 11 上的 VMware Player 3 設定網路

當您嘗試使用 SLES 11 上的 VMware Player 3 設定網路時，可能會看到下列錯誤：

```
Jan 12 14:57:34.761: vmx| VNET: MACVNetPortOpenDevice: Ethernet0: can't open
vmnet device (No such device or address)
Jan 12 14:57:34.761: vmx| VNET: MACVNetPort_Connect: Ethernet0: can't open
data fd
Jan 12 14:57:34.761: vmx| Msg_Post: Error
Jan 12 14:57:34.761: vmx| [msg.vnet.connectvnet] Could not connect Ethernet0
to virtual network "/dev/vmnet0". More information can be found in the
vmware.log file.
Jan 12 14:57:34.761: vmx|[msg.device.badconnect] Failed to connect virtual
device Ethernet0.
Jan 12 14:57:34.761: vmx| --
```

該錯誤指示 VMX 檔案可能已由另一個 VM 開啓。若要解決此問題，您必須更新 VMX 檔案中的 MAC 位址，如下所述：

1. 在文字編輯器中開啓 VMX 檔案。
2. 從 ethernet0.generatedAddress 欄位複製 MAC 位址。
3. 從訪客作業系統中開啓 /etc/udev/rules.d/70-persistent-net.rules 檔案。
4. 註解化原始行，然後輸入 SUBSYSTEM 行，如下所述：

   ```
   SUBSYSTEM=="net", DRIVERS=="?*", ATTRS{address}==<MAC address>,
   NAME="eth0"
   ```

5. 將 <*MAC address*> 取代爲您在步驟 2 中複製的 MAC 位址步驟 2。
6. 儲存然後關閉該檔案。
7. 在 VMware Player 中開啓 VM。

A.3 升級安裝爲非根使用者而非 Novell 使用者的 Log Manager

如果您嘗試升級安裝爲非根使用者，而非 novell 使用者的 Novell Sentinel Log Manager 1.0 伺服器，升級程序會失敗。發生此問題的原因是，在 Sentinel Log Manager 1.0 安裝期間所設定的檔案權限性質。

若要升級安裝爲非根使用者，而非 novell 使用者的 Sentinel Log Manager 1.0 伺服器，請執行下列操作：

1. 建立 novell 使用者。
2. 將 Sentinel Log Manager 1.0 安裝的擁有權變更爲 novell:novell。

   ```
   chown -R novell:novell /opt/novell/<install_directory>
   ```

   將 <*install_directory*> 變更爲安裝目錄的名稱。例如，

   ```
   chown -R novell:novell /opt/novell/sentinel_log_mgr_1.0_x86-64
   ```
3. 將 config/esecuser.properties 中的 ESEC_USER 項目變更爲 novell。
4. 以 root 身分登入，然後升級爲 Sentinel Log Manager 1.1。如需有關升級的詳細資訊，請參閱第 6.1 節 「從 1.0 升級到 1.1」 (第 43 頁)。

Sentinel 術語

本節說明此文件中所使用的術語。

收集器
將事件關連化、分析並傳送至資料庫之前，會將分類法、入侵偵測和企業相關性用於資料流中，以剖析資料並提供更豐富之事件資料流的公用程式。

連接器
使用業界標準方法連接到資料來源以取得原始資料的公用程式。

資料保留
定義從 Sentinel Log Manager 伺服器刪除事件之前，事件保留之持續時間的規則。

事件來源
記錄事件的應用器或系統。

事件來源管理
ESM。可讓您使用 Sentinel 連接器與 Sentinel 收集器來管理和監控 Sentinel 與其事件來源之間連接的介面。

每秒事件數
EPS。測量網路從其安全性設備與應用程式產生資料之速度值。該值也是 Sentinel Log Manager 可以從安全性設備收集與儲存資料的速率。

整合器
允許 Sentinel 系統連線至其他外部系統的外掛程式。JavaScript 動作可以使用整合器與其他系統互動。

原始資料
由連接器接收並直接傳送至 Sentinel Log Manager 訊息匯流排，然後寫入 Sentinel Log Manager 伺服器磁碟的未處理事件。因爲儲存在裝置上之資料格式的原因，不同連接器上的原始資料會不一樣。