Novell Sentinel Log Manager 1.1 版本說明

2010 年 7 月 08 日

Novell

Novell Sentinel Log Manager 可從各種裝置和應用程式收集資料，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 對許多應用程式與裝置，提供高事件發生率處理、長期資料保留、區域性資料彙總，以及簡易搜尋及報告等功能。

1 Sentinel Log Manager 1.1 的最新消息

1.1 職能

管理員現在可以建立職能，並指定給任何數目的使用者。您可以爲每個職能指定一組不同的許可，而屬於該職能的使用者則會繼承所屬職能的許可。

Sentinel Log Manager 包含數個具有必要許可的預設職能。但是，您可以根據個人需求修改許可及建立其他職能。

如需有關群組許可的詳細資訊，請參閱《*Novell Sentinel Log Manager 1.1 管理指南*》中的「*"設定使用者和職能"*」(http://www.novell.com/documentation/novelllogmanager11/log_manager_admin/?page=/documentation/novelllogmanager11/log_manager_admin/data/bjxveru.html)」。

1.2 分散式搜尋

「分散式搜尋」功能不僅能讓您搜尋本地 Sentinel Log Manager 伺服器上的事件，也能搜尋散佈全球的其他 Sentinel Log Manager 伺服器上的事件。當您設定好分散式搜尋組態，將多個伺服器與本地伺服器 (搜尋啓使者) 連結在一起之後，便可以在本地伺服器中執行搜尋，也可選擇指示搜尋引擎也在連結的伺服器上執行搜尋。搜尋結果中會取回並顯示所有選取伺服器上的符合事件。搜尋結果中的每個事件都會顯示取回事件的來源伺服器上的資訊。

系統加強了匯出搜尋結果、傳送搜尋結果至動作以及取回原始資料事件，以利用這個新功能。另外還加強了報表功能以使用相同的基礎搜尋引擎，如此報表才能包含來自多個 Sentinel Log Manager 伺服器的資料。

如需有關分散式搜尋的詳細資訊，請參閱《*Novell Sentinel Log Manager 1.1 管理指南*》中的「"在分散式環境中搜尋和報告事件" (http://www.novell.com/documentation/novelllogmanager11/log_manager_admin/?page=/documentation/novelllogmanager11/log_manager_admin/data/bp5lx14.html)」。

1.3 標記

「標記」功能可讓您建立並指定一或多個可搜尋標記屬性至「事件管理系統」(ESM) 節點 (如事件來源、事件來源伺服器、「收集器管理員」和「收集器外掛程式」)，也可以指定至報表。所有來自這些 ESM 節點的事件也都會加上標記。利用標記功能，您可以建立這些 ESM 節點、事件本身以及報表的邏輯群組。

您可以根據事件所套用的標記來搜尋事件，然後根據事件來源及報表所擁有的標記來進行過濾。

Sentinel Log Manager 包含部分預設標記；但您可以根據個人需求來建立新的標記。

如需有關標記的詳細資訊，請參閱《*Novell Sentinel Log Manager 1.1 管理指南*》中的「"設定標記" (http://www.novell.com/documentation/novelllogmanager11/log_manager_admin/?page=/documentation/novelllogmanager11/log_manager_admin/data/bp62o80.html)」。

1.4 裝置

Sentinel Log Manager 裝置是一個準備就緒的軟體裝置，它將 Novell SUSE Linux Enterprise Server (SLES) 11 作業系統和 Novell Sentinel Log Manager 軟體與更新服務結合在一起。此裝置提供以瀏覽器爲主的加強型使用者介面，此介面支援從各種裝置、應用程式和通訊協定收集、儲存、報表製作和搜尋記錄資料等功能。

Sentinel Log Manager 1.1 裝置提供下列使用格式：

- VMware 裝置影像
- Xen 裝置影像
- 直接部署在硬體伺服器上的硬體裝置 Live DVD 影像

附註：Sentinel Log Manager 1.0 使用者可以遵循《*Novell Sentinel Log Manager 1.1 安裝指南*》第 6.4 節「"從 1.0 裝置移轉至 1.1 裝置" (http://www.novell.com/documentation/novelllogmanager11/log_manager_install/?page=/documentation/novelllogmanager11/log_manager_install/data/bq9ckex.html)」中的指示，將其安裝移轉至 Sentinel Log Manager 1.1 裝置。

如需有關 Sentinel Log Manager 裝置安裝的詳細訊息，請參閱《*Novell Sentinel Log Manager 1.1 安裝指南* (http://www.novell.com/documentation/novelllogmanager11/log_manager_install/?page=/documentation/novelllogmanager11/log_manager_install/data/bookinfo.html)》中的「“安裝裝置”」。

1.5 LDAP 驗證的加強功能

- 新的使用者介面位於「*使用者*」索引標籤下，可設定 Sentinel Log Manager 伺服器進行 LDAP 驗證。
- 您可以選擇是否要使用匿名搜尋的方式在 LDAP 目錄上執行 LDAP 驗證。

如需有關 LDAP 驗證的詳細資訊，請參閱《*Novell Sentinel Log Manager 1.1 管理指南*》中的「“LDAP 驗證” (http://www.novell.com/documentation/novelllogmanager11/log_manager_admin/?page=/documentation/novelllogmanager11/log_manager_admin/data/bpfef67.html)」。

1.6 報表的增強功能

報表已經過增強，可讓您向下切入至組成報表的事件。此向下切入選項可讓您以產生報表所使用的相同查詢和時間框架來啓動搜尋，所以使用者就可以檢視用來產生報表的事件詳細資訊。

您可以同時輸出多個報表定義和報表結果，也可以同時從報表定義輸出 zip 檔或「收集器套件」檔輸入多個報表定義。

如需有關這些加強功能的詳細資訊，請參閱《*Novell Sentinel Log Manager 1.1 管理指南*》中的「“報表” (http://www.novell.com/documentation/novelllogmanager11/log_manager_admin/?page=/documentation/novelllogmanager11/log_manager_admin/data/bjxdi87.html)」。

此版本加入新的報表範本，也更新了現有的報表範本；其中也刪除了數個已不再使用的報表範本。如需有關可用報表範本的詳細資訊，請參閱《*Novell Sentinel Log Manager 1.1 管理指南*》中的「“Sentinel Log Manager 報表” (http://wwwtest.provo.novell.com/documentation/novelllogmanager11/log_manager_admin/index.html?page=/documentation/novelllogmanager11/log_manager_admin/data/bl5jfoz.html)」。

1.7 資料還原

新的資料還原功能可以還原舊的、遺失的或已刪除的事件資料。您也可以針對還原的事件資料執行搜尋。

新的「*資料還原*」區段已加入「*儲存*」>「*組態*」使用者介面中。您可以選取特定的事件分割區來還原事件資料，並設定還原的事件分割區將於何時再次過期。

如需有關資料還原的詳細資訊，請參閱《*Novell Sentinel Log Manager 1.1 管理指南*》中「“設定資料儲存” (http://www.novell.com/documentation/novelllogmanager11/log_manager_admin/?page=/documentation/novelllogmanager11/log_manager_admin/data/)」的「*還原事件資料*」。

2 Sentinel Log Manager 1.0.0.5 的最新消息

2.1 Sentinel Log Manager 的 500 EPS 版本

Novell Sentinel Log Manager 現在已有 500 EPS (每秒事件數) 的版本。500 EPS 版本適合僅有一部 Sentinel Log Manager 伺服器，且其中事件率較低的小型佈署。在大型佈署中，此版本也可用於回報至另一部 Sentinel 或 Sentinel Log Manager 伺服器的低容量節點。

2.2 新的使用者授權合約

此版本中已更新使用者授權合約 (EULA) 條款。您必須接受新的條款才能繼續套用最新的修補程式。EULA 中的部分變更爲：

- Novell Sentinel Log Manager 現在已有 500 EPS 的版本。
- 「非生產例項」的定義已更新
- 「第一類設備」的定義已更新

3 系統需求

Sentinel Log Manager 1.0 發行後，系統需求並沒有重大變更。

如需有關硬體需求、支援的作業系統、瀏覽器和事件來源的詳細資訊，請參閱 《*Novell Sentinel Log Manager 1.1 安裝指南* (http://www.novell.com/documentation/novelllogmanager11/log_manager_install/?page=/documentation/novelllogmanager11/log_manager_install/data/bookinfo.html)》。

4 安裝 Novell Sentinel Log Manager 1.1

若要安裝 Novell Sentinel Log Manager 1.1，請參閱 《*Sentinel Log Manager 1.1 安裝指南* (http://www.novell.com/documentation/novelllogmanager11/log_manager_install/?page=/documentation/novelllogmanager11/log_manager_install/data/bookinfo.html)》。

5 Sentinel Log Manager 1.1 中修正的問題

錯誤編號	描述
617478	您現在可以將 「入侵偵測系統」的前 10 大報表建立爲 *「裝置攻擊名稱」*欄位，此報表目前也包含在 「事件」欄位中。
609811	現在使用者密碼變更時，*「目標使用者名稱」*和 *「啓始者 IP」*欄位會正常填入數值。
609814	現在使用者登入 Sentinel Log Manager 時，*「啓始者 IP」*欄位會正常填入數值。
607143	此版本中已建立可用來對內部事件執行稽核的新報表。
606861	您現在可以對包含大寫字元的事件執行萬用字元搜尋。

錯誤編號	描述
592503	現在您在 *「精簡」*面板中新增的額外搜尋查詢會顯示適當的結果。
587831	現在將 *CustomerVar22* 欄位加入爲要顯示的額外欄位時，*「精簡」*面板會顯示該欄位的事件計數。
567082	密碼中具有非標準字元的使用者現在可以正常登入網路使用者介面和 ESM 介面。
565777	「信任管理」報表現在包含移除使用者帳戶時所產生的 DEASSOC_TRUST 事件。
526062	網路使用者介面中的 *「組態」*連結現在已由齒輪圖示所取代，表示圖示旁邊的連結就是組態連結。
524575	現在所有的 JavaScript 快顯視窗 (如「搜尋秘訣」、「執行」和「刪除」) 都能在法語、西班牙語、義大利語的 Internet Explorer 8 中正常出現。
503808	現在第一次將 Sentinel Log Manager 安裝於先前從未安裝過 Sentinel Log Manager 的伺服器時，ESM 可以正常啓動。
545436	現在內部稽核欄位 (如「啓始使用者名稱」、「啓始 IP」和「目標使用者名稱詳細資料」) 會填入適當數值，並且會顯示在搜尋結果中。

6 已知問題

錯誤編號	描述
620681	**問題：**在 ESM 中，收集器節點會在伺服器重新啓動期間不正確地設爲停止狀態。不過，這是偶發的問題。 **解決方式：**重新啓動伺服器後，登入 ESM 並且確定應該要執行的收集器已設爲開始狀態。

620100	**問題：**舊版收集器無法用於遠端收集器管理員。
	
	解決方式：修改遠端收集器管理員機器中的 ESEC_HOME/config/collector_mgr.xml 檔案。
	
	1. 在任一編輯器中開啓 ESEC_HOME/config/collector_mgr.xml 檔案。
	2. 變更下列各行：
	
	`<property name="workbench.home">..</property>`
	`<property name="properties.file">../config/`
	`collector_mgr.properties</property>`
	`<property name="esecurity.home">..</property>`
	
	變更爲
	
	`<property name="workbench.home">${user.dir}/..</property>`
	`<property name="properties.file">../config/`
	`collector_mgr.properties</property>`
	`<property name="esecurity.home">${user.dir}/..</property>`
	
	3. 重新啓動遠端收集器管理員服務。

錯誤編號	描述
617318	**問題：**在您將舊版的 Sentinel Log Manager 升級至 Sentinel Log Manager 1.1 後，*「另存爲報表」* > *「視覺化」*下拉式清單應該只包含報表範本。但是，如果在升級前正在使用部分收集器專用的報表，則升級過程中可能不會刪除這些報表，因此可能還是會出現在 *「視覺化」*清單中。 **解決方式：**這個問題發生的原因，是因爲升級過程中，沒有自動升級清單中顯示的收集器專用報表。請從 Sentinel 6.1 內容網站 (http://support.novell.com/products/sentinel/sentinel61.html) 下載更新的收集器套件，然後使用 Sentinel Log Manager 報表上載選項來上載套件。
617663	**問題：**當您在 *「收集」* > *「事件來源伺服器」*頁面上同時修改事件來源中一個以上的欄位時，在按一下 *「儲存」*以重新整理頁面後，只有一個欄位會更新，其他欄位會顯示舊的值。 **解決方式：**每次變更一個欄位的值。在修改每個欄位後，按一下 *「儲存」*。
617477	**問題：**由於系統不允許單純的 NOT 準則查詢，所以在搜尋結果中的事件欄位上按一下 alt+left 以在空白查詢中加入 NOT 子句的功能將無法正常運作。 **解決方式：**如果您以 sev:[0 TO 5] 查詢而不是空白查詢開始搜尋的話，alt+left 點擊的功能便可正常運作。兩種查詢所取回的事件將會是相同的。
618294	**問題：**「主要」欄位爲空時，「事件摘要」、「前 10 大報表」和「前 10 儀表板」基礎報表會顯示包含 -0- 的事件而不顯示空值。 **解決方式：**對於「事件摘要」和「前 10 大報表」，請不要選取沒有資料 (爲空) 的「主要」欄位。對於「前 10 儀表板」報表，請忽略 X 軸中數值爲 -0- 欄位的圖形。
617103	**問題：**執行大型報表並且已設定 NFS 歸檔時，server_wrapper.log 檔案中會記錄例外。 **解決方式：**請在 EPS 最低時 (例如，晚間或是週末) 執行大型報表。在本地儲存 RAID 陣列中加入更多磁碟可能也有幫助。
614686	**問題：**在具有大約 2 億個事件的系統上執行大型報表時，搜尋查詢會逾時，且會記錄例外。 **解決方式：**避免在執行大規模搜尋時執行大型報表。
613960	**問題：**遠端收集器管理員 Installshield 精靈顯示 Sentinel 6.1 而不是 Sentinel Log Manager。 **解決方式：**無。這是使用者介面問題。
608905	**問題：**在您新增授權金鑰後，Sentinel Log Manager 使用者介面不會提示您重新啓動 Sentinel 服務，且無法正常執行某些操作。 **解決方式：**請在新增授權金鑰後重新啓動 Sentinel Log Manager 伺服器。
606567	**問題：**在裝置上，系統會以每兩分鐘的頻率，將平台版本透過核心訊息記錄到 syslog，位置在 /var/log/messages。 **解決方式：**作業系統送出這些訊息是爲了將其版本通知 Sentinel Log Manager。如果基於某些原因，這些訊息對您造成問題，請停用 wtmpmon 程序檔以避免產生這些訊息。
593435	**問題：**如果 Sentinel Log Manager 1.1 被移動到路徑中含有空格的基礎目錄，則 Sentinel Log Manager 伺服器將不會正常運作。例如，/home/user/Sentinel Log Manager。 **解決方式：**請確保目錄的路徑中不包含空格。

錯誤編號	描述
560966	**問題：**設定檔案連接器時，當您按一下 *「瀏覽」*來新增事件來源時，檔案瀏覽器不會出現，且控制中心記錄檔案中會記錄例外。 **解決方式：**請不要使用 *「瀏覽」*按鈕，而改以指定想要的檔案路徑，或將其複製 / 貼上至欄位中。
577073	在具有大約 3000 個事件來源的情況下，當原始資料分割狀態由開啓變更爲記錄時，EPS 率會下降爲 0。 **解決方式：**安裝額外的 Sentinel Log Manager 例項，使每個例項的總事件來源數低於「系統需求」中列出的建議裝置限制。如需詳細資訊，請參閱《*Novell Sentinel Log Manager 1.1 安裝指南*》中的「"系統需求" (http://www.novell.com/documentation/novelllogmanager11/log_manager_install/?page=/documentation/novelllogmanager11/log_manager_install/data/bjx8zq7.html)」。
617350	**問題：**安裝修補更新時，WebYaST 會報告 DBus.Error.LimitsExceeded 錯誤。 **解決方式：**重新啓動 yastws 服務： `/etc/init.d/yastws restart` 或者在「控制台」中按一下 *「重新開機」*以重新啓動機器。
607684	**問題：**當您從 ISO 裝置影像 (如以 Live CD/DVD 執行 ISO) 將機器開機時，如果您透過 WebYast > 「更新」執行修補更新，則系統會進入無回應的狀態。 **解決方式：**將 Live DVD 安裝至硬體，再執行修補更新。
609187	**問題：**在具有超過一百萬個事件的系統上，在您啓始報表產生並按一下 *「取消」*來取消報表產生後，報表產生會持續作用且無法取消。 **解決方式：**無。
593788	**問題：**在安裝後，Sentinel Log Manager 需要大約 5 分鐘才能第一次登入網路使用者介面。 **解決方式：**無。
510824	**問題：**在您按一下個別搜尋結果的 *「詳細資料 ++」*連結後，前 25 個事件的 *「所有詳細資料 ++」*和 *「所有詳細資料 --」*連結不會正常運作。 **解決方式：**無。
548515	**問題：**Sentinel Log Manager 中的範例報表會顯示在 Sentinel Log Manager 中不可用的使用者資料 (如全名、部門和工作人員 ID)。 **解決方式：**無。
509549	**問題：**在具有超過 75000 個事件的「搜尋結果」頁面中，當您向下捲動以檢視事件時，捲軸不會在捲動的點停止，而會不斷改變位置。 **解決方式：**無。
615572	**問題：**Sentinel Log Manager 可讓您在編輯目標伺服器詳細資料時變更其 IP 位址，且不會顯示訊息通知您指定的 IP 位址不同。 **解決方式：**無。

錯誤編號	描述
545436	**問題：**當您停止收集器時，事件記錄中會產生兩次 stopcollector 內部事件。所產生的第二個 stopcollector 不會顯示正確的「啓始使用者名稱」、「啓始 IP」和「目標使用者名稱詳細資料」事件欄位值。 **解決方式：**無。

7 文件

更新文件與版本說明可至 Sentinel Log Manager 文件網站 (http://www.novell.com/documentation/novelllogmanager11/) 下載。

8 法律聲明

Novell, Inc. 對本文件的內容與使用不做任何陳述或保證，對本產品在任何特定用途的適銷性與適用性上，亦不做任何明示或默示的保證。此外，Novell, Inc. 保留隨時修改本出版品及其內容的權利，進行此類修正或更動時，亦毋需另行通知任何人士或公司組織。

此外，Novell, Inc. 對軟體不做任何陳述或保證，對本產品在任何特定用途的適銷性與適用性上，亦不做任何明示或默示的保證。此外，Novell, Inc. 保留隨時修改任何或全部 Novell 軟體的權利，進行此類更動時，亦毋需通知任何人士或公司。

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。

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)。

所有的協力廠商商標均爲其各別擁有廠商的財產。