ZENworks 2020 Update 2

新增功能參考

2021 年 **8** 月

法律聲明

如需法律聲明、商標、免責聲明、擔保聲明、出口與其他使用限制、美國政府限制的權利、專利政策與 FIPS 法規遵循的相關資訊，請參閱 https://www.novell.com/company/legal/。

目錄

關於本指南

本 《*ZENworks* 新增功能參考》介紹 ZENworks 2020 Update 2 版本中的新功能。本指南包含下列章節：

適用對象

本指南的適用對象為 ZENworks 管理員。

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。請使用線上文件每頁下方的 「對此主題提供意見」功能。

其他文件

也可以透過 ZENworks 的其他支援文件 (有提供 PDF 與 HTML 格式) 來瞭解與實作本產品。如需其他文件，請造訪 ZENworks 文件網站。

1 ZENworks 2020 Update 2 中的新增功能

以下章節介紹 ZENworks 2020 Update 2 中的新功能和增強功能：

平台支援

此版本支援下列新平台：

- CentOS (做為受管理裝置)
- macOS 11 (Big Sur) (做為受管理裝置)
- Android 11
- iOS 14
- SLES 15 SP2
  - SLES 15 SP2 (主要伺服器)
  - SLES 15 SP2 (受管理裝置 - 包括 SLES for SAP)
  - SLED 15 SP2 (受管理裝置)
- 新的 RHEL 和 Scientific Linux 平台
  - Scientific Linux 7.7 和 7.8
  - RHEL 7.8 和 8.2

安裝與升級

由於 ZENworks 的目標是採用更穩健、更靈活的架構，並與 Micro Focus 標準保持一致，因此 ZENworks 2020 Update 2 版本為安裝和升級程序引入了一些增強功能。此版本中引入的變更如下：

安裝 **Docker** 和 **Docker Compose**

在 Linux 主要伺服器上升級或安裝 ZENworks 2020 Update 2 之前，需要在該伺服器上安裝 Docker 和 Docker Compose。如需 Docker 的詳細資訊，請參閱 https://docs.docker.com/。

將伺服器資料移轉至新檔案路徑

在 Windows、Appliance 或 Linux 主要伺服器上升級至 ZENworks 2020 Update 2 後，之前位於 Novell 檔案路徑中的 ZENworks 伺服器資料 (例如 MSI、RPM、記錄和組態檔案) 將移至新 Micro Focus 檔案路徑。

例如，在 Linux 伺服器上，之前位於 /etc/opt/novell/zenworks 中的組態檔案現在位於 /etc/opt/microfocus/zenworks 中。同樣，在 Windows 伺服器上，之前位於 C:\Program Files (x86)\Novell\ZENworks\conf 中的組態檔案現在位於 C:\Program Files (x86)\Micro Focus\ZENworks\conf 中。

與 ZENworks 代理程式相關的檔案和資料仍將保留在舊 Novell 位置。

ZENworks 伺服器服務已更名

在 Windows、Appliance 或 Linux 主要伺服器上升級至 ZENworks 2020 Update 2 後，某些 ZENworks 伺服器服務 (例如 ZENServer、ZENLoader 和 ZENJoinProxy 服務) 將從 Novell 更名為 Micro Focus。例如，在 Linux 伺服器上，novell-zenserver.service 將更名為 microfocus-zenserver.service。

引入了一個新環境變數

對於 Windows 伺服器，引入了一個新環境變數 %ZENSERVER_HOME%，該變數同樣指向非預設路徑的伺服器安裝位置 (C:\Program Files(x86)\Micro Focus\ZENworks)。

TLS 版本

如果您全新安裝了 ZENworks 2020 Update 2，區域中預設會啟用 TLS 1.2，當您嘗試註冊 Microsoft.NET 版本早於 4.7 的裝置時，裝置註冊將會失敗，但會在裝置上安裝代理程式。

如果您要將現有區域升級至 ZENworks 2020 Update 2，則預設不會啟用 TLS 1.2。如果您要在區域中啟用 TLS 1.2，則某些功能可能無法依預期運作，並且請確定您在區域中的所有裝置上都安裝了 Microsoft.NET 4.7。

如果您已在區域中啟用 TLS 1.2，若要註冊裝置，應在裝置上安裝 Microsoft .NET 4.7。

取代主要伺服器

如需以第二部主要伺服器取代第一部主要伺服器，或以新主要伺服器取代現有主要伺服器的更多詳細資料，請參閱 《*ZENworks Disaster Recovery Reference*》 (ZENworks 災難備援參考) 中的 「*Replacing Primary Servers*」 (取代主要伺服器)。

將主要伺服器移轉至 **Appliance**

如需將現有主要伺服器 (Windows 或 Linux) 移轉至 Appliance 伺服器的程序的更多詳細資料，請參閱《*ZENworks Primary Server and Satellite Reference*》(ZENworks 主要伺服器和輔助伺服器參考) 中的「*Moving from a Windows or Linux Primary Server to Appliance*」(從 Windows 或 Linux 主要伺服器移轉至 Appliance)。

ZENworks Configuration Management

Windows 10 裝置管理

ZENworks 2020 Update 2 版本中新增了一些新功能，可讓您使用 Windows 10 裝置上的內建 MDM 代理程式來管理這些裝置的整個生命週期。為了應對超出 Windows 10 裝置功能範圍之外的使用情形，您還可以在使用 Windows 10 MDM 代理程式的裝置上部署 ZENworks 代理程式。

如需本節中所列各項功能的詳細資訊，請參閱 《Windows MDM Reference》 (Windows MDM 參考)。

新功能如下：

組態功能

您現在可以設定 Windows 通知服務 (WNS)，以將推播通知傳送至透過 Windows 新式管理功能管理的 Windows 裝置。

註冊功能

引入了下列註冊功能。

註冊方法：可以使用以下方法將 Windows 10 裝置註冊到 ZENworks。

- 佈建套件 (PPKG) 註冊
- 加入 Azure Active Directory (Azure AD)
- AutoPilot 註冊

部署 **ZENworks** 代理程式：現在，您可以在已使用 MDM 註冊模式註冊的 Windows 10 裝置上部署 ZENworks 代理程式。

設定使用條款：您可以將使用條款規則指定到裝置，以新增在使用 Azure AD Join 或 Auto Pilot 註冊功能註冊 Windows 10 裝置時，要在代理程式上顯示的使用條款內容。

管理功能

引入了下列管理功能：

部署 **Windows 10 MDM** 套裝軟體：現在，您可以將以下套裝軟體部署到 Windows 10 MDM 裝置：

附註：對這些套裝軟體的支援屬於實驗性支援，應該僅用於試用目的。

- 使用「Windows 10 MDM - 安裝 MSI」套裝軟體在 Windows 10 MDM 裝置上部署 Microsoft 安裝程式 (MSI) 套件。
- 使用 Windows 10 MDM CSP 套裝軟體配送組態服務提供者 (CSP)，以在 Windows 10 MDM 裝置上部署透過 CSP 提供的各種組態。

啟動快速任務：支援對 Windows 10 MDM 裝置執行以下快速任務：

- 刪除裝置
- 取消註冊裝置
- 淘汰裝置
- 取消淘汰裝置
- 遺失裝置
- 取消註冊裝置

其他功能

針對 Windows 10 MDM 功能引入的一些其他功能如下：

- Windows 10 裝置支援自動重整。
- CA 重建程序現在會向 Windows 10 MDM 裝置核發證書。
- MS Graph API 設定已更名為 Azure MDM 應用程式，需要進行重新設定才能利用此版本中引入的新增強功能。

開始使用新式管理

「行動裝置管理入門」頁面已翻新，現在還包含 Windows 10 MDM 裝置的註冊和管理功能。如需詳細資訊，請參閱《Modern Management Reference》(新式管理參考)。

ZENworks 影像

在 **WinPE** 上使用套裝軟體名稱還原影像：在 ZENworks 2020 Update 1 及更早版本上，WinPE 發行套件支援使用 IMG 指令透過提供影像名稱來還原影像，而該指令無法識別是否透過該指令傳遞了套裝軟體。從 ZENworks 2020 Update 2 開始，WinPE 發行套件上支援 IMG 套裝軟體指令。如需詳細資訊，請參閱 《Preboot Services and Imaging》 (開機前服務和影像) 指南。

讀取 **ZENworks** 影像資訊的新工具：zmginfo 工具可協助您收集有關影像的資訊。當您的內容儲存庫或共用路徑中有多個影像，而您需要收集每個影像的相關資訊時，可以使用此工具來節省時間。您可以使用 zmginfo 工具收集影像的基本資訊或完整資訊。管理員可以使用 zmginfo 建立套裝軟體 xml，這些檔案可做為套裝軟體輸入，用於將所有 linux 基本影像轉換為 winpe 基本影像。

如需詳細資訊，請參閱 《Preboot Services and Imaging》 (開機前服務和影像) 指南。

ZENworks Remote Management

從遠端控制具有活動 **RDP** 工作階段的裝置：現在，您可在具有作用中 RDP 工作階段的裝置上啟動遠端工作階段，就像一般遠端管理工作階段一樣。如需詳細資訊，請參閱 《Remote Management Reference》 (遠端管理參考) 指南。

錄製遠端管理工作階段 **(** 實驗性支援 **)**：可讓受管理裝置上的使用者錄製遠端管理工作階段。如需詳細資訊，請參閱 《Remote Management Reference》 (遠端管理參考) 指南。

行動裝置管理

對 **Android** 套裝軟體啟用裝置指定：為核准的 Google Play 商店 APP 建立的 Android 套裝軟體先前僅可指定給使用者，現在也可指定給裝置。如需詳細資訊，請參閱 《Mobile Management Reference》 (行動裝置管理參考)。

佈建系統 **APP**：使用套裝軟體功能，您可以在 Android 裝置上啟用或停用系統 APP。系統 APP 是裝置上已預先安裝的內建 APP。如需詳細資訊，請參閱 《Mobile Management Reference》 (行動裝置管理參考)。

開始使用新式管理：「行動裝置管理入門」頁面已翻新，現在還包含 Windows 10 MDM 裝置的註冊和管理功能。此外，此頁面上還包含與註冊和管理 Apple 及 Android 裝置相關的一些其他功能。如需詳細資訊，請參閱 《Modern Management Reference》 (新式管理參考)。

修改 **Android** 裝置記錄位置 Android 裝置上 ZENworks APP 記錄的位置已變為 Android/data/com.novell.zapp/files/Documents/zapp.log。若要共用這些記錄，您需要在 Android 裝置上部署 Files APP。

套裝軟體管理

「複製關係」工作流程中引入了新的失敗時繼續選項。如果在將關係從一部裝置複製到另一組物件時發生錯誤，針對其餘物件的操作仍將繼續。操作結束時將顯示錯誤的詳細資料，並會提供一個選項用於輸出操作詳細資料，以供進一步參考及採取相應措施。如需詳細資訊，請參閱 《Software Distribution Reference》 (軟體配送參考)。

其他

讓客戶可以使用 **puppet-agent** 套件的最新版本：以前，ZENworks 將 puppet-agent 套件做為版次的一部分提供，以便使用者可以使用 Puppet 規則。但是，由於 puppet-agent 版本會持續更新，因此在 ZENworks 發行後，使用者便無法使用 puppet-agent 套件的最新版本。從此版本開始，若要使 Puppet 規則在 ZENworks 2020 Update 2 及更新版本的 Linux 受管理裝置上生效，您需要確定裝置上已安裝 puppet-agent 套件。如需詳細資訊，請參閱《Configuration Policies Reference》(組態規則參考)。

ZENworks 中的安全性增強功能

此版本中引入了安全性增強功能，讓您即使在 DMZ 環境中也能安全地註冊裝置並與其通訊。

- 如果您全新安裝了 ZENworks 2020 Update 2，則所有主要伺服器上預設都會啟用該安全性設定。
- 如果您要升級主要伺服器，則預設將停用該安全性設定。
- 如果您已將新的主要伺服器新增至區域中，則在升級至 ZENworks 2020 Update 2 後，預設將啟用該安全性設定。

您需要執行以下 zman 指令來啟用該設定：

- 引入了 zman ssassc (Security-Set-Agent-Server-Secure-Communication)，可讓您啟用或停用針對 ZENworks 代理程式與 ZENworks 伺服器之間通訊的驗證。

如需此版本中引入的安全性增強功能的詳細資訊，請參閱《ZENworks Securing Devices Reference》(ZENworks 保護裝置安全參考)。

裝置註冊

預先核准裝置註冊

預先核准的裝置是管理員已核准要新增至區域中的裝置。此功能特別適合用於在大量註冊一組已知裝置時必須預先核准一些裝置的情況。您還可以使用此功能來允許對已知裝置進行重整 (如果需要)。

使用授權金鑰

ZENworks 代理程式可使用授權金鑰來授權自己註冊到區域，以及在安裝期間與伺服器進行任何通訊。

保障受管理裝置和 iOA 裝置註冊的安全

若要將更新的 iOA 代理程式或受管理裝置註冊到區域，您需要在裝置註冊期間指定授權金鑰，或確定裝置包含在預先核准的裝置清單中。

裝置通訊

使用 **OSP** 進行裝置通訊 **(** 包括 **ZCC** 登入 **)**

對於大部分功能，ZENworks 已改為使用 O-Auth 通訊協定來建立使用者身分。因此，產品中引入了名為 OSP 的新服務，用於登入 ZCC、進行服務間通訊，以及裝置與伺服器之間的通訊。

保護裝置、主要伺服器和輔助伺服器之間內容傳輸和收集的安全

引入此項新安全性功能後，將透過 SSL 在受管理裝置、主要伺服器和輔助伺服器之間進行端到端內容收集和傳輸。可以透過在 ZCC 中進行相應設定或使用新引入的 zman 指令來實現此目的。

保護裝置與主要伺服器或輔助伺服器之間的 **Web** 服務通訊的安全

為了進一步保護 ZENworks 代理程式與 ZENworks 主要伺服器和輔助伺服器之間的 Web 服務通訊的安全，此版本中針對 Web 服務呼叫引入了安全性增強功能。

Microsoft 資料加密規則磁碟機排除項

現在，當在受管理裝置上執行 Microsoft 資料加密規則時，可依該規則中的磁碟機類型將抽取式資料磁碟機排除在加密範圍之外。

反惡意程式碼

ZENworks 反惡意程式碼是 ZENworks Endpoint Security Management 的一個新元件，位於 ZENworks 控制中心的「安全性」分組之下。反惡意程式碼是一種壓縮解決方案，可保護受管理裝置免遭所有最新惡意程式碼的威脅。將反惡意程式碼代理程式部署到區域中的裝置上後，它會持續從反惡意程式碼雲端服務接收惡意程式碼簽名檔案更新，以便透過存取時掃描和隨選掃描來偵測惡意程式碼感染情況。系統會隔離受感染檔案，直至已將其殺毒。

如需本節中主題的詳細資訊，請參閱以下內容：

- 《ZENworks Endpoint Security Antimalware Reference》 (ZENworks Endpoint Security 反惡意程式碼參考)

防範惡意程式碼 **-** 入門頁面

安全性的入門頁面中包含一個額外的索引標籤式頁面，名為「防範惡意程式碼」。您可以使用此頁面做為設定、部署以及自訂 ZENworks 反惡意程式碼必須提供的所有功能的單一存取點。

反惡意程式碼更新授權

您需要有反惡意程式碼更新授權才能將反惡意程式碼規則部署到裝置。在試用模式下啟用端點安全性管理時，該授權會自動啟用，持續時間為整個試用期。

Windows 端點安全性規則

可使用四個新規則來管理反惡意程式碼的部署、自訂和連續性：

反惡意程式碼執行規則：這是基本規則，會在受管理裝置上安裝反惡意程式碼代理程式。必須部署此規則才能使用任何其他反惡意程式碼規則。該規則包含所有惡意程式碼掃描類型的組態，包括存取時掃描、完整掃描、快速掃描、外部裝置掃描，以及關聯式隨選掃描。規則還提供隔離行為設定，以及用於定義要排除在掃描範圍之外的內容的設定。

如果部署規則後最終使用者權限和通知的預設設定保持不變，最終使用者將有權在其端點上存取代理程式狀態主控台。在該主控台上，使用者可啟動自己的掃描、檢視掃描和代理程式更新狀態，以及接收受規則控制的代理程式活動的通知。

反惡意程式碼掃描排除項規則：反惡意程式碼具有掃描排除項，包括內建排除項，以及您可以新增至任何反惡意程式碼規則的自訂掃描排除項。如果還為相同裝置指定了其他反惡意程式碼規則，將根據裝置指定採用掃描排除項規則，這樣可透過更簡單的方式在區域中傳播掃描排除項。可以針對特定掃描類型啟用或停用排除項。

反惡意程式碼自訂掃描規則：如果懷疑有特定威脅或者要掃描受管理裝置上的具體位置，可使用自訂掃描規則更有針對性地掃描這些裝置上的本地磁碟機。自訂掃描規則有自己的排程，而反惡意程式碼執行規則不同，它使用為其設定的區域排程。

反惡意程式碼網路掃描規則：網路掃描規則也是一種更有針對性的掃描方法，但明確用於掃描網路磁碟上的資料夾和檔案。該規則也有自己的排程，並包含用於向網路位置進行驗證的額外設定。

反惡意程式碼安全性 **Dashlet**

安全性儀表板中預設包含四個新 dashlet，用於監控惡意程式碼威脅、惡意程式碼掃描，以及惡意程式碼簽名更新。

裝置惡意程式碼狀態：此 dashlet 顯示在所選偵測期間區域中個別裝置的惡意程式碼狀態。

裝置上次惡意程式碼掃描：此 dashlet 顯示區域中的裝置防禦惡意程式碼威脅的狀況。它預設顯示有關在指定期間對裝置執行的任何掃描類型的資訊。

惡意程式碼威脅排行榜：此 dashlet 顯示區域中排在前幾名的惡意程式碼威脅清單。預設會依據受感染裝置數顯示惡意程式碼威脅排行榜。

裝置惡意程式碼簽名版本：此 dashlet 顯示區域中的裝置上安裝的惡意程式碼簽名版本和反惡意程式碼代理程式版本清單。

裝置反惡意程式碼頁面

此頁面包含一個新索引標籤，選取某部裝置後可以存取該索引標籤。它提供選定裝置的惡意程式碼威脅的快照狀態、掃描排程以及隔離檔案資訊。您也可以在該裝置上對檔案執行特定的動作、啟動掃描，以及更新反惡意程式碼代理程式和惡意程式碼簽名版本。

惡意程式碼威脅詳細資料頁面

在裝置的「反惡意程式碼」頁面的「惡意程式碼威脅」區段中，按一下某個惡意程式碼威脅連結可存取此頁面。此頁面提供有關選定威脅的詳細資訊，以及已受該威脅感染的裝置的詳細資料。

反惡意程式碼快速任務

當在 ZENworks 控制中心的「裝置」分組中選取一或多部安裝了反惡意程式碼代理程式的裝置後，可在選定裝置上執行五個新的快速任務。其中包括以下快速任務：

- 啟動惡意程式碼掃描
- 更新惡意程式碼簽名
- 更新反惡意程式碼代理程式
- 還原惡意程式碼隔離區中的檔案
- 刪除惡意程式碼隔離區中的檔案

反惡意程式碼 **zac** 指令

反惡意程式碼隨附數個此元件特有的新 zac 指令。其中包括用於在裝置上啟動惡意程式碼掃描、檢查反惡意程式碼代理程式的惡意程式碼狀態、安裝、更新或移除代理程式、刪除隔離區中的檔案的指令，以及其他指令。

反惡意程式碼區域組態頁面

ZENworks 主組態頁面中的「安全性」分組中現在包含三個新的區域組態頁面。其中每個頁面都包含您可以自訂的預設設定。這些頁面如下：

反惡意程式碼代理程式排程：設定惡意程式碼掃描和惡意程式碼簽名更新的排程。您可以在裝置資料夾層級和裝置層級覆寫此排程。

反惡意程式碼代理程式通知：設定反惡意程式碼代理程式在受管理裝置上顯示的警示和通知。您可以在裝置資料夾層級和裝置層級覆寫這些設定。

反惡意程式碼組態：指定將 ZENworks 主要伺服器做為反惡意程式碼伺服器使用，為此必須進行手動設定，以部署反惡意程式碼元件。還可為反惡意程式碼代理程式設定維護排程。

隨選內容組態頁面

ZENworks 主組態頁面中的「套裝軟體」、「規則」和「內容」分組中現在包含這個新的區域組態頁面。可使用該頁面管理區域中內容配送的內容下載速率和內容快取大小，目前包括反惡意程式碼簽名檔案和反惡意程式碼代理程式更新。

反惡意程式碼服務狀態

現在，您可在 ZCC 的「診斷」頁面中存取反惡意程式碼服務狀態。

反惡意程式碼資料庫

ZENworks 2020 Update 2 中新增了反惡意程式碼資料庫。目的是透過 「反惡意程式碼」頁面和反惡意程式碼安全性 dashlet 為反惡意程式碼的監控功能提供資料。進行設定後，此資料庫會與 ZENworks 資料庫同步，因此它們的資料庫類型必須相同。例如：PostgreSQL、Microsoft SQL Server 或 Oracle。

可從 ZENworks 控制中心的 「安全性」下的 「防範惡意程式碼 - 入門」頁面設定反惡意程式碼資料庫。如果反惡意程式碼資料庫將設定為使用尚不存在的外部資料庫，可以透過 CLI 指令使用 setup.exe 檔案建立一個外部資料庫。