Softnext 中華數位科技

Action1

雲原生漏洞修補管理平台

簡易安裝手冊 2024

目錄

說明：Action1 安裝使用手冊的內容或更新，請以 Action1 官方網站 為依據

一 . Action 1 在幾分鐘內完成漏洞修補管理

Action1 是排名第一基於風險的漏洞修補管理平台，適用於分佈式企業網路，受到全球數千個組織的信賴。**Action1 有助於在單一解決方案中發現漏洞、確定優先級並進行修復，以防止安全漏洞和勒索軟體攻擊**。它可以自動修補第三方軟體和作業系統，確保持續的漏洞修補合規性並在安全漏洞被利用之前進行修復。

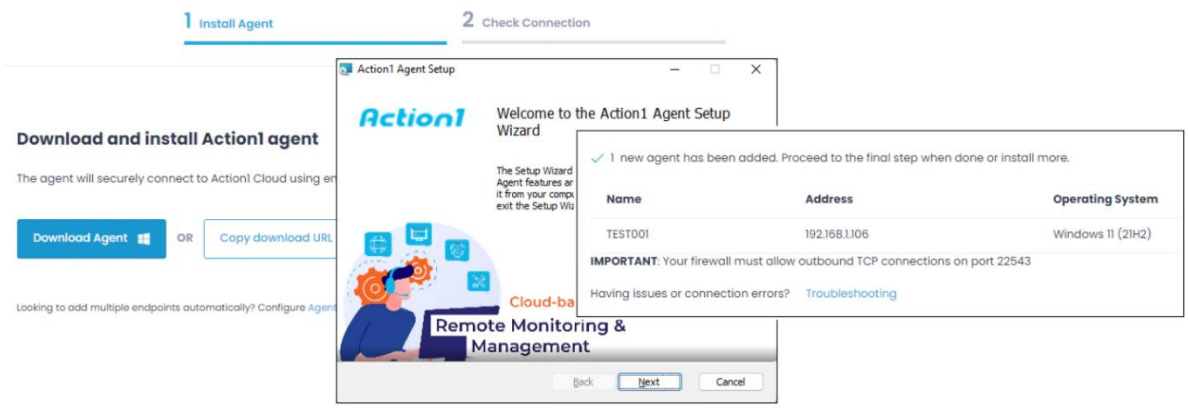
本快速入門指南展示如何在 5 分鐘內為第三方應用程式和作業系統啟用漏洞修補管理。

步驟 1：增加端點
步驟 2：手動檢查和部署漏洞修補
步驟 3：自動部署關鍵更新
步驟 4：產生漏洞修補合規性報告

步驟 1. 增加端點 (Add Endpoints)

在開始修補端點之前，需要安裝 Action1 Agent,它是一個微型應用程式，系統佔用空間非常小，除非端點需要修補或狀態更新，否則它會處於空閒狀態。

1. 導航到 **Endpoints** 並選擇 **Install Agents**。
2. 單擊 **Download Agent**。下載的設置,將給組織預先配置特定的連接參數
3. **安裝 Action1 Agent**。完成安裝嚮導步驟。在最後一步中，安裝程式(installer)將要求提升安裝代理的權限。
4. **檢查狀態(Check Status)**。返回到 Action1 控制台並單擊 **Next Step** ,以繼續 **Check Connection** 步驟以驗證連接。
5. 單擊 **“Finish”** 返回 **“Endpoints”** 並在其中查看新增加的 Agent 詳細信息。它將自動顯示所有系統信息，例如缺失的更新、已安裝的軟體和硬體詳細信息。

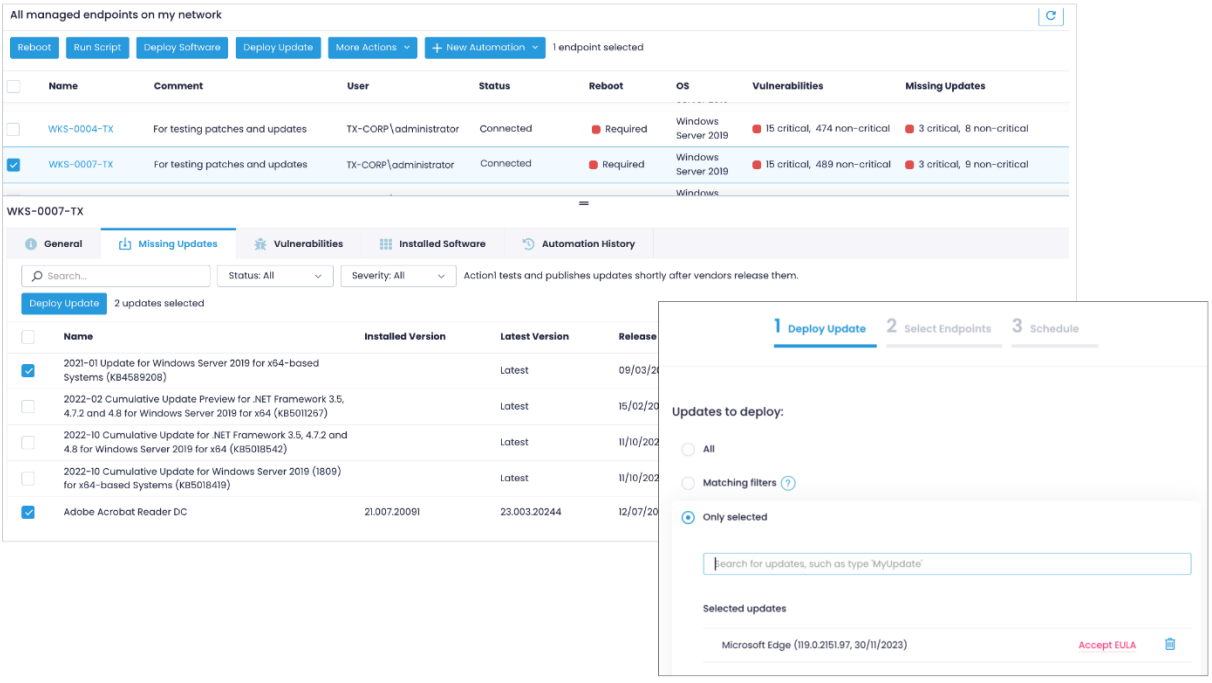


稍後可嘗試：要在多個端點上進行批量部署，請使用 **Action1 Deployer** 、**群組政策**或任何當前的遠端部署工具。

步驟 2.手動檢查和部署漏洞修補 (Manually Review and Deploy Patches)

所有端點信息，包括缺失的漏洞修補、已安裝的軟體和作業系統詳細資訊都會即時更新。無需安排定期掃描來了解是否缺少任何更新。

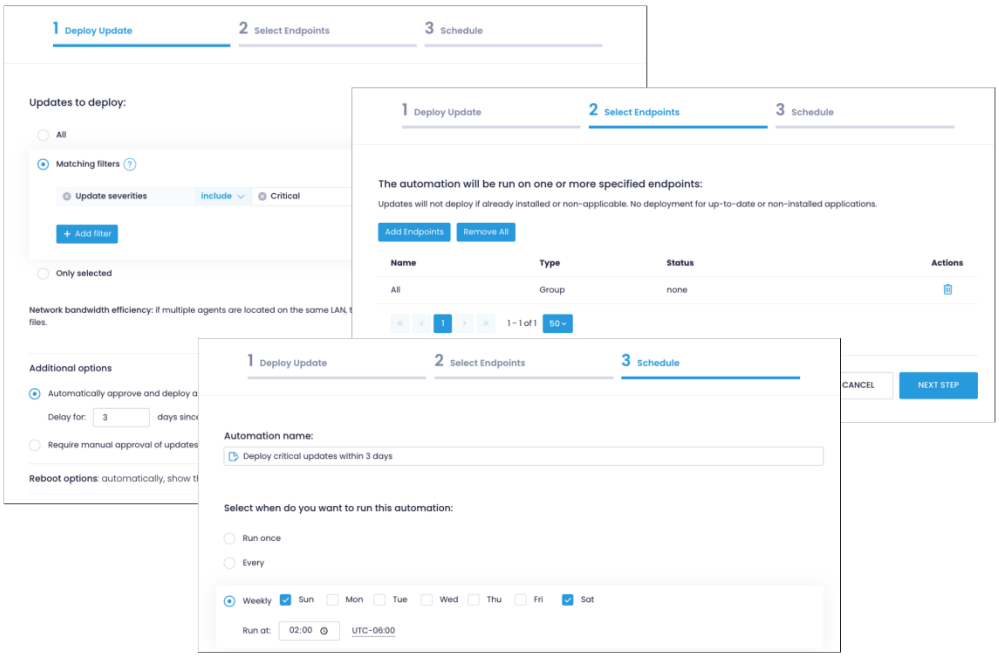
1. 在 **Endpoints** 部分中，單擊端點名稱(**endpoint name**)。
2. 單擊 **Missing Updates**(缺失更新)並選擇要部署的更新。作業系統和第三方應用程式的所有適合更新，以及更新類型和安全嚴重性都將顯示在一個視窗圖中。
3. 單擊 **Deploy Update**(部署更新)以啟動更新嚮導。它將預先填入 **Step1** 中選定更新的清單。
4. 根據需要調整 **Reboot Options**(重新啟動)選項。如果正在部署的任何更新需要重新啟動，則預設為使用者提供最多 **60 分鐘的時間**來保存其工作的資料。
5. 單擊 **Next Step 兩次**以查看 Step3 中的排程選項。出於測試目的保留預設的 **“Run Now(立即運行)”** ，然後單擊 **“Finish”** 。
6. Action1 將開始部署選定的更新並即時報告狀態。**稍後可嘗試：**查看**漏洞**視圖以修復漏洞。



步驟 3. 自動部署關鍵更新 (Automate Deployment of Critical Updates)

自動化漏洞修補(Patch)和漏洞管理例程，以確保端點的合規性，以下範例設定自動化，以在作業系統和應用程式發布 3 天後部署所有關鍵安全漏洞修補。

1. 導航 **Automations**，選擇 **New Automation** 並指定 **Deploy Update**。
2. 在「**Deploy Update**」步驟中，選擇「**Matching Filters**」。
3. 按一下「**Add filter**」，選擇 **Update severities,**」，然後選擇「**Critical.**」。
4. 在過濾器下方，按一下 “Additional options” ，選擇 “**自動核准並部署所有符合的更新 (Automatically approve and deploy all matching updates)**” ，然後輸入 **3** 天作為延遲參數。
5. 根據需要調整 **Reboot Options**，類似於上一個步驟。
6. 然後 **Add Endpoints** 以選擇端點或群組。
7. 在「**Schedule**」步驟中，定義自動化排程，例如每週、週日和週六凌晨 2 點。

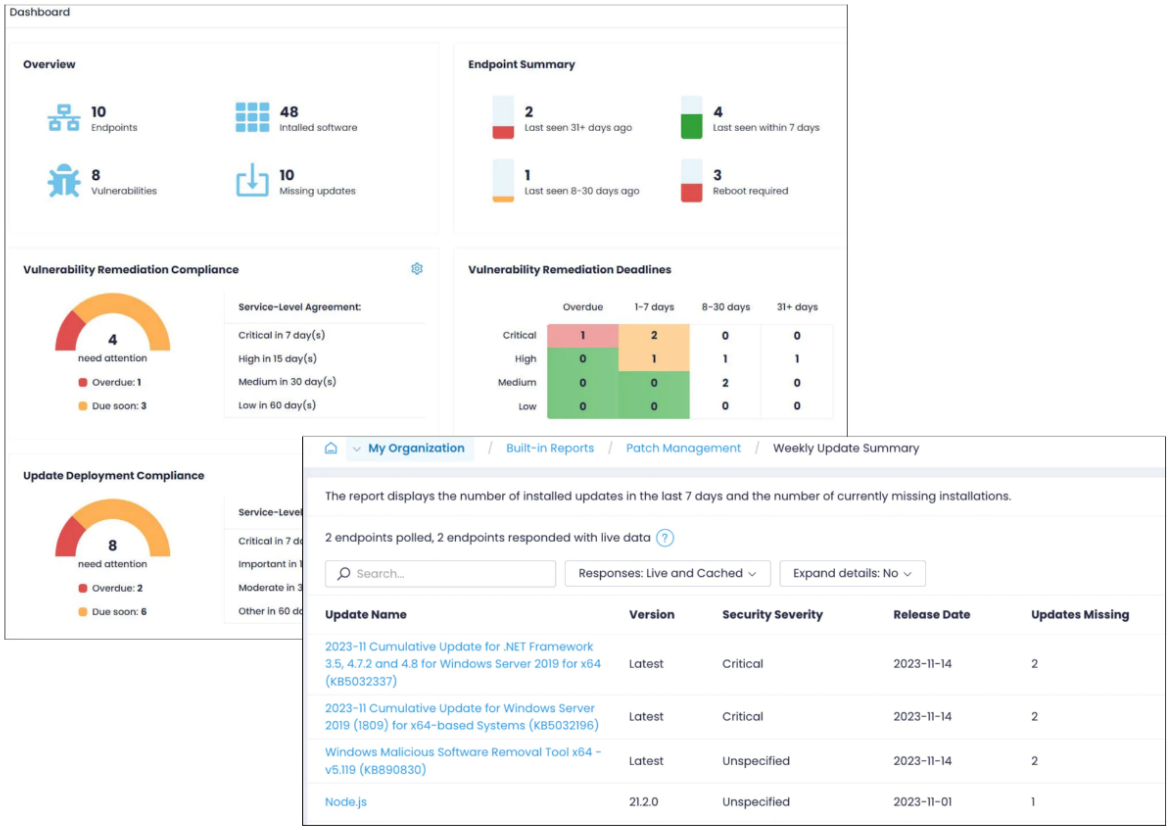


稍後可嘗試：建立另一個需要手動批准更新的政策，並使用 “Update Approval” 部分有選擇地批准或拒絕更新。另一種選擇是建立更廣泛的自動化,來自動涵蓋關鍵更新之外的更新。

步驟 4. 產生漏洞修補合規性報告 (Generate Patch Compliance Reports)

Action1 即時漏洞修補合規性儀表板和即時報告，可方便定期檢查安全狀況並協助合規性稽核。

1. 導航到 **Dashboard** 以導瞰端點健康狀態，包括漏洞修復合規性、等待部署、需要重新啟動的端點數量等。
2. 轉到**內建報告| 漏洞修補管理(Built-in Reports | Patch Management)**可產生有關每日和每週漏洞修補統計資訊、仍然缺失更新、需要重新啟動等的報告。
3. 點選**工具| 訂閱(Tools | Subscribe)**這些報告中的任何一個，即可按所需的排程表（例如每週透過電子郵件接收它們。）



下一步

Action1 附帶許多其他功能來簡化漏洞修補管理。一旦熟悉基礎知識，請探索以下步驟：

- **批量代理部署(Bulk agent deployment)**
  使用 **Action1 Deployer** 自動掃描 Active Directory 中的新電腦並部署 Agent 來修補所有電腦。前往 **Configuration | Agent Deployment** 部分。

- **建立端點群組(Create endpoint groups)**
  對組織進行細分，根據伺服器類型、部門、位置、作業系統版本等分配不同的政策。導航到 **Endpoints** 並單擊 **Create Group**。

- **已安裝軟體清單**(Inventory of installed software)
  前往 **“Installed Software”** 查看所有應用程式、其版本以及是否有可用的更新。

- **部署應用程式(Deploy applications)**
  遠端安裝和設定軟體儲存庫(**Software Repository**)中預先配置的數十個應用程式。選擇一個或多個端點，然後按一下「**Deploy to Endpoints**」即可開始。若要新增自訂應用程式，請前往 **Software Repository** 並按一下 **Add to Repository** 即可開始。

- **卸載應用程式(Uninstall applications)**
  手動或自動刪除不需要的或遺留的應用程式。選擇一個或多個端點，然後按一下卸載軟體(Uninstall Software)或建立卸載應用程式原則以簡化自動卸載。
- **運行腳本**(Run scripts)
  Action1 附帶**腳本庫(Script Library)**來執行遠端管理活動，例如阻止 Windows 功能更新、刪除臨時檔案等。還可以將自訂 PowerShell 腳本增加到**腳本庫**內。

二. Acton1 的要求

Action1 Web 控制台

- Web 瀏覽器：Chrome、Safari、Firefox、Internet Explorer 或 Microsoft Edge
- 必須啟用 JavaScript 和 cookie
- 連接 https://www.action1.com

Action1 部署程式 (Deployer)

- 作業系統：Windows 7 或更高版本
- 記憶體：至少 100 MB 可用物理記憶體，**50 MB 磁碟空間**
- 權限：對所有託管端點的管理存取 (對 \\admin$ 共享的寫入存取以及管理 Windows 服務的能力)、對服務所在伺服器的管理存取、對 Active Directory 的僅讀存取

Action1 Agents

- 作業系統： Windows 7 或以上
- 記憶體： **至少 50 MB 可用物理記憶體，10 MB 磁碟空間**
- Windows PowerShell： 2.0 或更高版本*

* 預設情況下，Windows PowerShell 從 Windows 7 開始可用，但需要在安裝正確服務包的早期版本的 Windows 中啟用。有關詳細信息，請參閱 Microsoft 文件：Windows PowerShell 系統要求和安裝 Windows PowerShell。

防火牆配置

有關端口和協定配置的信息，請參閱 防火牆配置。

防病毒白名單設置

為避免防病毒軟體阻止 Action1 服務，請在防病毒設置中將 Action1 檔案夾和以下檔案列入白名單：

- C:\Windows\Action1
- C:\Windows\Action1\action1_agent.exe
- C:\Windows\Action1\action1_remote.exe

三. 防火牆配置

Inbound 與 Outbound 連接說明

Action1 Agent 代理的設計在專門建立與 Action1 雲伺服器的連接 - 它始終是由 Agent 發起聯繫，而不是反向。因此，只需設置出站防火牆規則即可。儘管是單向啟動，但資料傳輸可以而且確實在兩個方向上發生：從 Agent 到伺服器，然後再返回。

當建立連接後，Agent 只需等待來自伺服器的指令。這些指示可能是執行政策或收集報告資料。伺服器在當使用者通過 Action1 控制台提示時或根據預設時間表發送這些指令。可把它想像成一個管弦樂隊：指揮（伺服器）發出指令，音樂家（Agent）等待並遵循這些指令。音樂家總是注意指揮的指示，而不是相反操作。

出站(Outbound)規則僅有一個例外：當同一本地網路上的 Action1 Agent 想要通過點對點 (P2P) 共享交換軟體包套件時。在這些情況下，Agent 將接受來自其對等方的入站(Inbound)連接。儘管這不是強制性的，但建議設置僅入站 LAN 防火牆規則以促進此類交換。

防火牆規則參考

有關應在系統中配置的 Port 和協定的完整說明，請參閱本節。建立防火牆規則以允許存取以下資源：

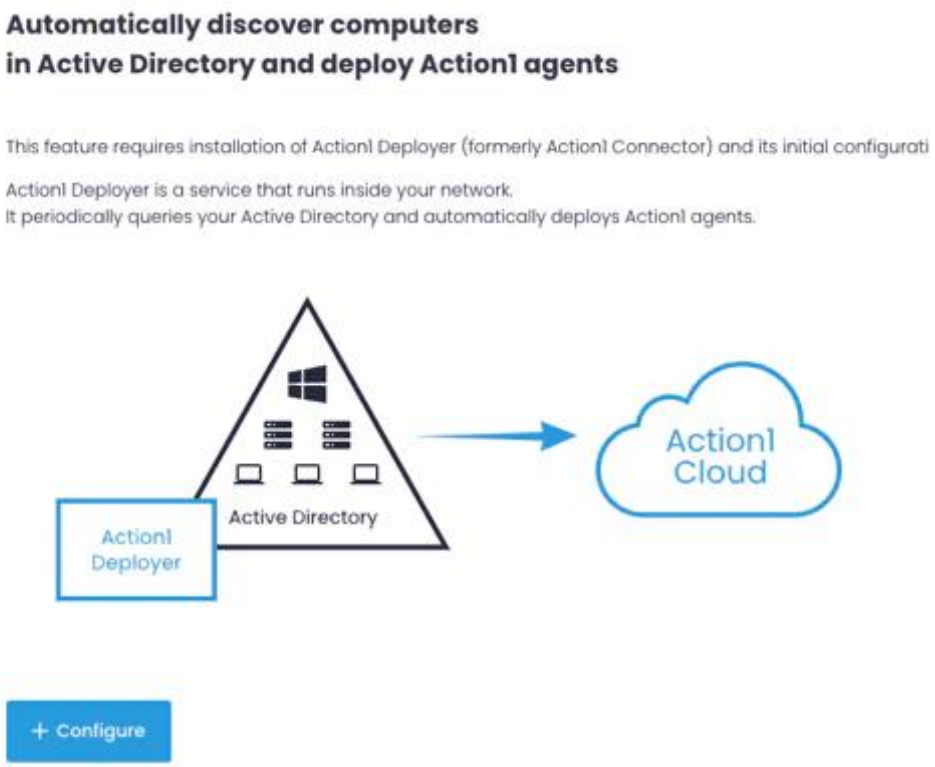
Resource	Type	Port & Protocol	Required for	Components
Action1 servers (server.action1.com): 54.210.188.13 54.227.102.112 3.210.54.212 3.213.90.174	Outbound	22543 TCP, TLS 1.2 over TCP	**(Required)** Connection to Action1 Cloud.	Agents, Deployer
	Outbound	135 RPC TCP	(Required) Connection to Action1 Cloud.	Deployer
	Outbound	139 SMB TCP	(Required) Connection to Action1 Cloud.	Deployer
	Outbound	445 SMB TCP	(Required) Connection to Action1 Cloud.	Deployer
	Outbound	389 LDAP TCP	(Required) Connection to Action1 Cloud.	Deployer
	Outbound	Randomly allocated high TCP ports (between 49152 - 65535) TCP	(Required) Connection to Action1 Cloud.	Deployer

Resource	Type	Port & Protocol	Required for	Components
Action1 Remote Desktop relay servers in North America: 34.203.184.16 52.205.66.134 52.200.246.160	Outbound	22543 TCP, TLS 1.2 over TCP	(**Required** - only for North America) 連線到 Action1 遠端桌面中繼伺服器。 這些伺服器位於北美，以確保該地區的用戶獲得流暢的遠端桌面體驗。	Agents
Managed endpoints (LAN only)	Inbound	22551 TCP/UDP, 6771 UDP	(**Recommended**) 推薦）交換下載的應用程式（P2P 文件共享）有助於最大限度地減少外部頻寬的使用。 該 port 應在託管端點上本地打開，以允許本地網路中 Agent 之間的連接。 如果不允許本地網路上 Agent 之間的入站通信，則 Agent 將不會在本地交換下載的應用程式，而是始終從雲中完整下載。	Agents
a1-backend-packages.s3.amazonaws.com	Outbound	443 HTTPS	部署應用程式和第三方漏洞修補管理。.	Agents
*.windowsupdate.com	Outbound	TCP, proprietary by Microsoft	Windows Update management.	Agents
*.mp.microsoft.com	Outbound	HTTPS/TLS 1.2	Windows Update management.	Agents
emdl.ws.microsoft.com	Outbound	HTTP	Windows Update management.	Agents
*.update.microsoft.com	Outbound	HTTPS/TLS 1.2	Windows Update management.	Agents
us-cdn.action1.com	Outbound	443 HTTPS	Deploying apps and 3rd party patch management.	Agents
eu-cdn.action1.com	Outbound	443 HTTPS	Deploying apps and 3rd party patch management.	Agents
Action1 Remote Desktop Console for North America: us.remote.app.action1.com	Outbound	443 HTTPS	(Required - only for North America) 連接到 Action1 遠端桌面控制台。這些伺服器位於北美，以確保該地區的用戶獲得流暢的遠端桌面體驗。	Action1 Console (web browser)

註： DNS 名稱中的*（星號）表示包括所有子網域。例如， *.example.com 將包括 example.com、child.example.com、grand.child.example.com 和所有其他可能的子網域。

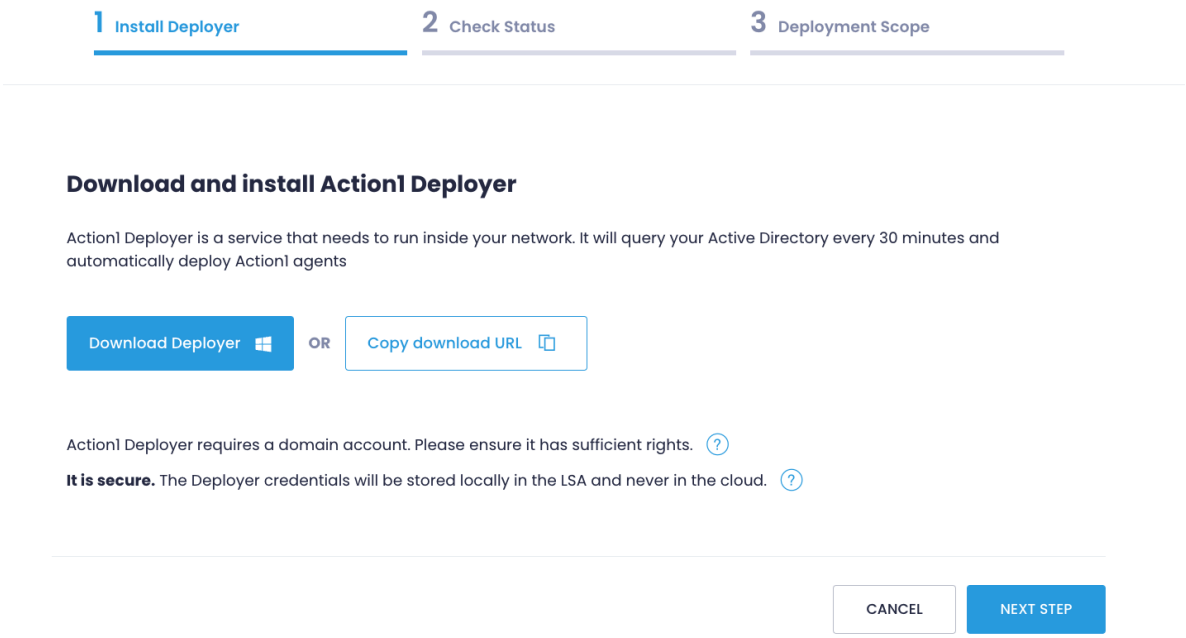
四 . Action1 Deployer 部署程式（推薦）

Action1 Deployer 能夠自動檢測網路端點、部署 Action1 Agent 並使它們保持最新狀態。Action1 Deployer 是一種在網路內部執行的管理服務，**可發現位於 Active Directory 網域或組織單位 (organizational unit (OU) 中的工作站和伺服器。**最重要的是，可以手動將工作組(workgroup)中的電腦增加到 Action1 Deployer 配置中。按照以下說明在您的環境中進行設置。



步驟 1. 安裝 Action1 Deployer 服務

1. 到 Configuration 部分中的 Agent Deployment 頁面並選擇+ Configure。
2. 在 Install Deployer 步驟中，下載安裝包或複制鏈接。安裝程式名稱是唯一的並顯示您的組織。Action1 Deployer 支持 32 位和 64 位系統。
3. 選擇正確的伺服器來安裝 Action1 Deployer 服務。由於此服務負責管理在遠端端點上執行的 Agent，因此該伺服器的 24/7 啟用服務至關重要。
4. 右鍵單擊 Deployer 安裝程式並以**管理員身份執行**。
5. 提供管理憑證(administrative credentials)。將用於在您的端點上自動部署 Action1 Agent。



所需權限

建議不要使用預設的 Administrator 帳戶，而是為 Action1 Deployer 服務**建立一個專用的網域帳戶 (Create a dedicated domain account)**。

- 該帳戶必須對 Active Directory 網域具有只讀存取權限 (read-only access)
- 該帳戶必須被授予登錄即服務權限(Logon as a service)（在本地電腦上）。安裝程式(installer)將嘗試將此權限授予指定帳戶。
- 該帳戶必須是 **Action1 Deployer 服務所在的伺服器上本地 Administrators 群組的成員**。可以手動將專用網域帳戶增加到本地管理員組。
- 該帳戶必須是**所有託管端點上本地管理員組的成員**。可以使用腳本或通過群組政策手動將專用網域帳戶增加到本地管理員組。請注意，帳戶本身不需要對 Active Directory 的任何網域管理權限，只需要本地權限。
- 如果排程發現駐留在工作組(workgroup)中的端點，請確保所有工作組電腦都使用具有相同密碼的相同本地使用者。Deployer 必須在這些憑証據下設置才能存取訪問工作組電腦。

如何為 Action1 Deployer 建立專用網域帳戶？

1. 在網域控制器(domain controller)上，啟動 **Active Directory 使用者和電腦**並導航到**網域\使用者(domain/Users)**。
2. 為 **Action1 Deployer 服務建立一個新使用者**，例如 *"Action1Deployer"*。

如何手動將 Action1 Deployer 服務帳號增加到本地 Administrators？

如果出於某種原因不想利用群組政策或出於測試目的安裝 Deployer 服務，請考慮**手動將服務帳戶增加到本地 Administrators 群組**。在要安裝 Action1 Deployer 服務的伺服器上以及它應該管理的端點上執行以下步驟。

1. 導航到**本地使用者和群組/群組(Local Users and Groups / Groups)**。
2. 找到**管理員(Administrators)群**組並選擇**增加到群組(Add to group)**。
3. 輸入服務帳戶名稱（例如，*domain\Action1Deployer*）。確保使用網域帳戶。

如何通過群組政策將 Action1 Deployer 服務帳戶增加到本地管理員？

如果您的基礎架構中有多個端點並希望自動化 Agent 交付過程，請利用群組政策(Group Policy)。

1. 在網域控制器上，啟動 **Active Directory 使用者和電腦(Active Directory Users and Computers)**並導航到你的網域。
2. 建立網域全局安全群組(domain global security group)，例如 *"Action1LocalAdmins"*，並使 *Action1Deployer* 成為該群組的成員。
3. 啟動**組政策管理控制台(Group Policy Management Console -GPMC)**。
4. 找到一個有效的網域政策（很可能是 **Default Domain Policy**）或建立一個新的群組政策物件，該物件適用於整個網域或僅適用於託管端點所需的 OU。
5. 右鍵單擊政策並選擇**編輯(Edit)**。
6. 導航到**電腦配置/政策/Windows 設置/安全設置/受限群組(Computer Configuration / Policies / Windows Settings / Security Settings / Restricted Group)**。
7. 右鍵單擊空白區域並選擇**增加群組(Add Group)**。指定專用於 Action1 Deployer 的群組的名稱(*Action1LocalAdmins)*。
8. 配置設置。在**該群組的成員(Members of this group)**部分中，單擊**增加(Add)**並選擇建立的帳戶 (*Action1Deployer)*。在 **This group is a member of** 部分中，單擊 **Add** 並選擇 **Administrators**。
9. 要應用這些更改，請在指令提示下執行 *"gpupdate /force"* 。

為什麼 Action1 Deployer 需要這些權限(permissions)？

需要本地**管理員(Administrators)的成員身份才能將可執行檔案複製到** *machinename**admin$**Action1* 檔案夾並在所有託管端點上配置名為 Action1 Update 的 Windows 服務。此服務將依次安裝和更新 Action1 Agent。

Action1 Deployer 不會將這些憑證發送到 Action1 Cloud 或 Deployer 安裝之外的任何其他地方。它們將被**存儲的唯一位置是由 Windows 作業系統以加密格式維護的本地服務控制管理器**(SCM)資料庫，並由 Windows 作業系統作為 LSA 機密存儲，並且永遠不會離開您的環境。

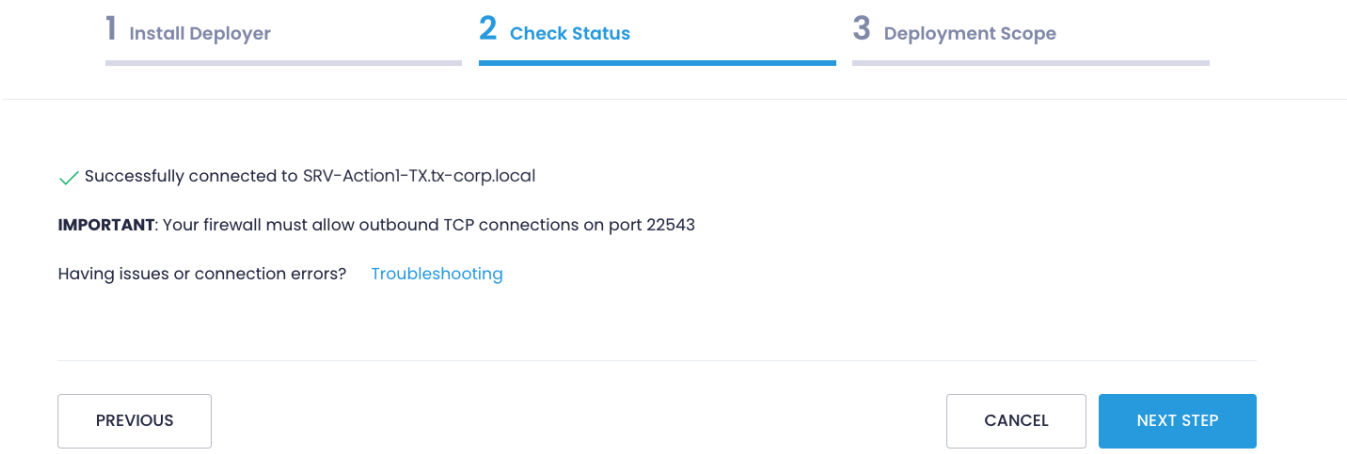
什麼是 LSA 機密？

本地安全機構 (Local Security Authority-LSA) 機密是一段資料，只能由在本地電腦上執行的 SYSTEM 帳戶程式取。其中一些機密是重啟後必須保留的憑證，它們以加密形式存儲在硬碟驅動器上。作為 LSA 機密存儲的憑證包括在電腦上配置的 Windows 服務（包括 Action1 Deployer 服務）的帳戶密碼。這是唯一存儲您的 Active Directory 密碼的地方。

步驟 2. 檢查狀態

1. 在 Action1 Deployer 根據系統類型將自身安裝到*%ProgramFiles%\Action1\Connector* 或 *%ProgramFiles(x86)%\Action1\Connector* 後，Action1 Deployer 將使用有關組織的嵌入式信息安全地連接到 Action1 Cloud，其中包括用於相互身份驗證的身份驗證證書和特定於的組織的私有加密密鑰。

2. 在 **Check Status** 步驟中，驗證 Action1 Deployer 是否已成功安裝並連接到 Action1 Cloud。



步驟 3. 配置部署範圍

繼續執行**部署範圍(Deployment Scope)**步驟以完成配置過程並開始使用 Action1。

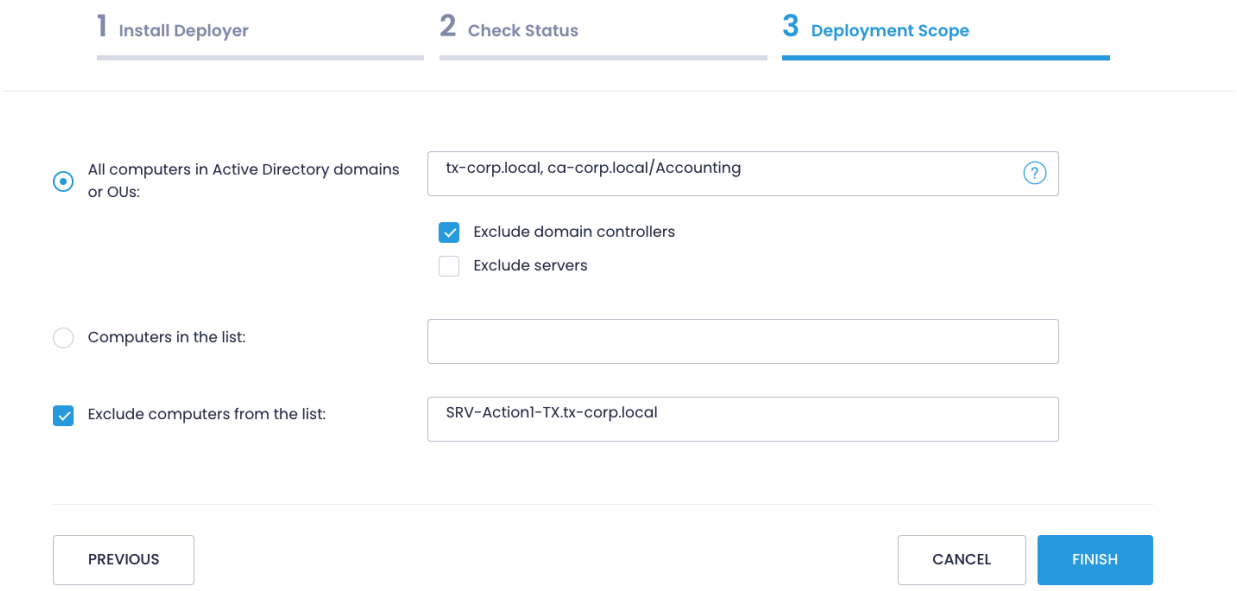
- **Active Directory 網域或 OU 中的所有電腦 (All computers in Active Directory domains or OUs**): 指定一個或多個網域或組織單位，以逗號分隔例如，*widgets.local*、*organization.com/Servers*)。可以選控制器或所有執行 Windows Server 作業系統的電腦。

- **列表中的電腦 (Computers in the list)** : 連接到 Action1 **特定電腦 (specific computers)**。請注意，可以發現位於工作組中的端點。提供電腦名稱，以逗號分隔。

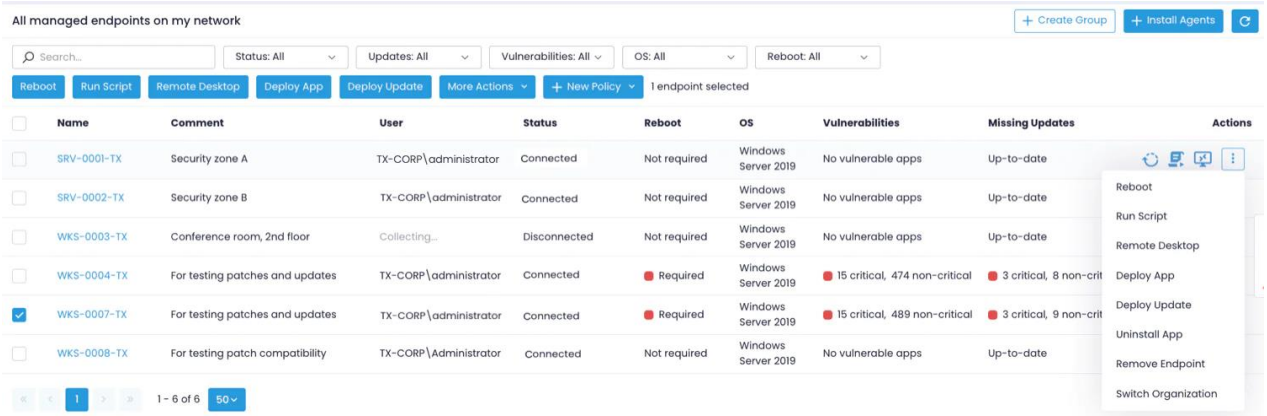
- 此外，**從列表中排除** 不應連接到 Action1 Cloud 的電腦。

怎麼執行的？

一旦指定部署範圍（例如 Active Directory 網域或電腦列表），Action1 部署程式服務將自動聯繫每台託管電腦，將 Action1 Agent 可執行檔案複製到 \\computername\admin$\Action1 檔案夾（其中本地映射到*%WinDir%\Action1*），然後建立並啟動 Action1 Agent 服務。繞過 Action1 部署程式，Action1 Agent 將連接到 Action1 Cloud，發現的設備將出現在**端點(Endpoints)**列表中。



如果您管理多個組織，應該為每個組織安裝 Action1 Deployer 並分別配置設定。



注意：要斷開端點與 Action1 Cloud 的連接，請在 **“端點(Endpoints)”**頁面上選擇刪除端點選項。

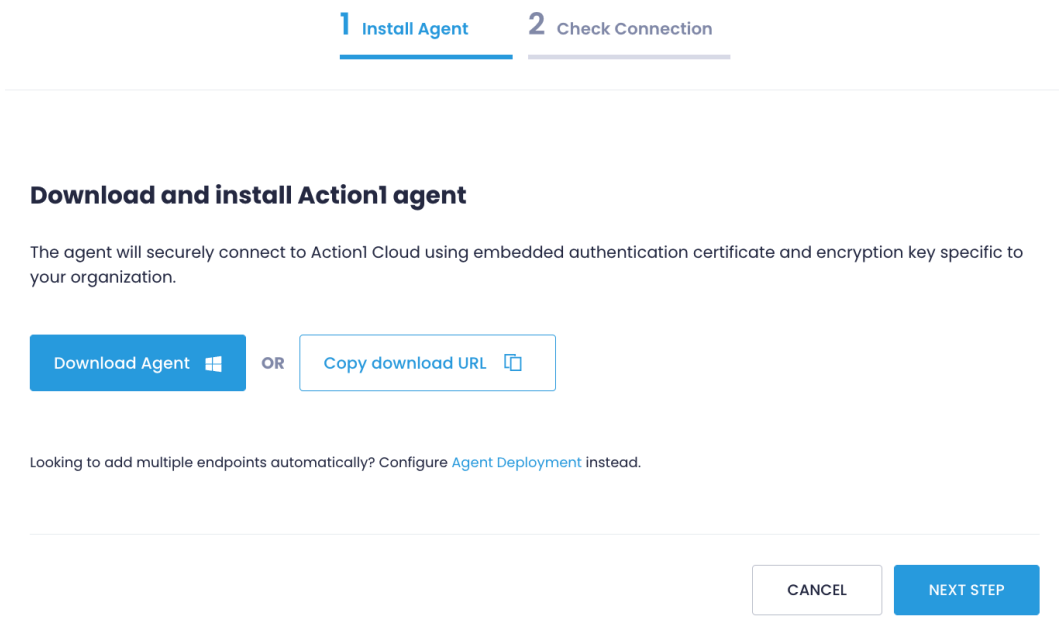
五．手動增加端點

如果不想 安裝 Action1 Deployer 服務，您可以手動連接端點。如果只想監控幾個業務關鍵端點，或者如果訂閱端點有限（例如，免費版本最多 100 個端點）並且還沒有準備好擴充，則此選項很方便。

在這種情況下，必須在要監控的端點上手動安裝 Action1 Agent。該 Agent 是一種非侵入式服務，以 **MSI 檔案的形式分發**。配置過程包括兩個步驟。首先，下載 MSI Agent 安裝程式，然後安裝 Agent 並驗證與 Action1 Cloud 的連接。

步驟 1. 下載 Action1 Agent 安裝程式

1. 導航到 Endpoints 並選擇 **Install Agents**。
2. 在 **“安裝 Agent (Install Agent s)”** 步驟中，**下載 Action1 Agent 安裝程式或複制 URL，如果您打算在另一台電腦機器上安裝 Agent**。安裝程式名稱是唯一的，表示您的 Action1 帳戶和組織。安裝程式支持 32 位和 64 位 Windows。



步驟 2. 安裝 Agent

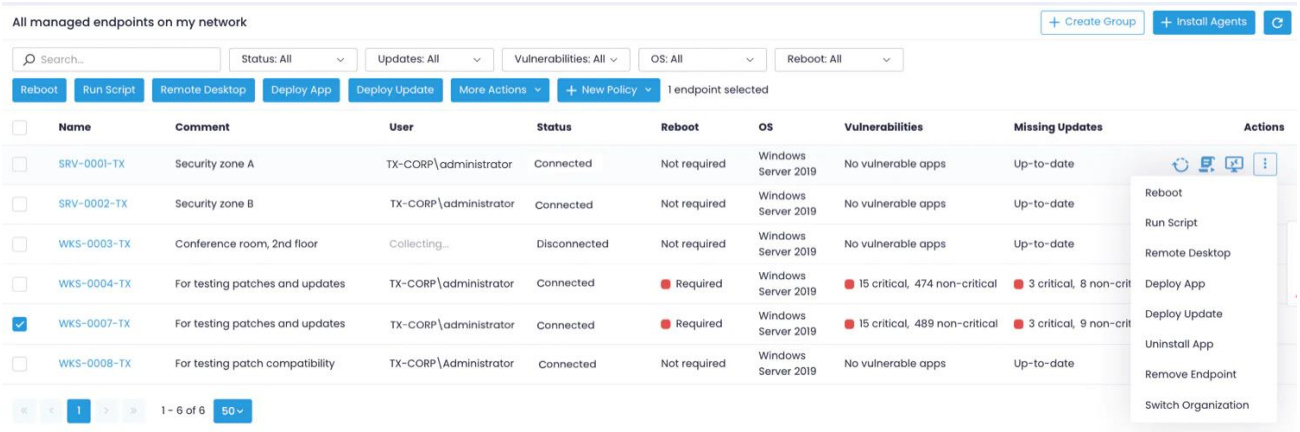
選擇以下選項之一：

- 安裝簡單（基於 UI）
- 無人值守安裝（無 UI）

簡易安裝（基於 UI）

將 Agent 安裝程式複製到每個託管端點並執行設置嚮導(setup wizard)。或者，您可以共享此安裝程式的鏈接並顯示端點所有者自行下載和啟動安裝程式。該 Agent 作為名為 Action1 Agent 的服務安裝在本地系統帳戶下的 ***%WinDir%\\Action1*** *檔案夾中*。

Action1 Agent 將使用有關組織的嵌入式信息安全地連接到 Action1 Cloud，這些信息包括 用於相互身份驗證的身份驗證證書和特定於組織的私有加密密鑰。執行的設備被增加到 **Endpoints** 中。選擇新端點旁邊的**操作(Actions)**並查看可用的管理操作，例如查看缺失的更新、啟動遠端桌面或重新啟動。



無人值守安裝(Unattended Installation)（無 UI）

要靜默安裝 Action1 Agent，請在要增加到 Action1 的每個端點上**以管理員身份執行(run as administrator)** *"msiexec /i "action1_agent(My_Organization).msi" /quiet"* 。

注意： Action1 Agent 支持機器範圍內的安裝，它需要管理權限才能成功。由於無人值守安裝模式不允許顯示任何使用者提示，因此在非提升權限下執行它會靜默失敗。
對於無人值守的卸載，請在要與 Action1 斷開連接的每個端點上執行指令 *"msiexec /uninstall "action1_agent(My_Organization).msi" /quiet"* 。

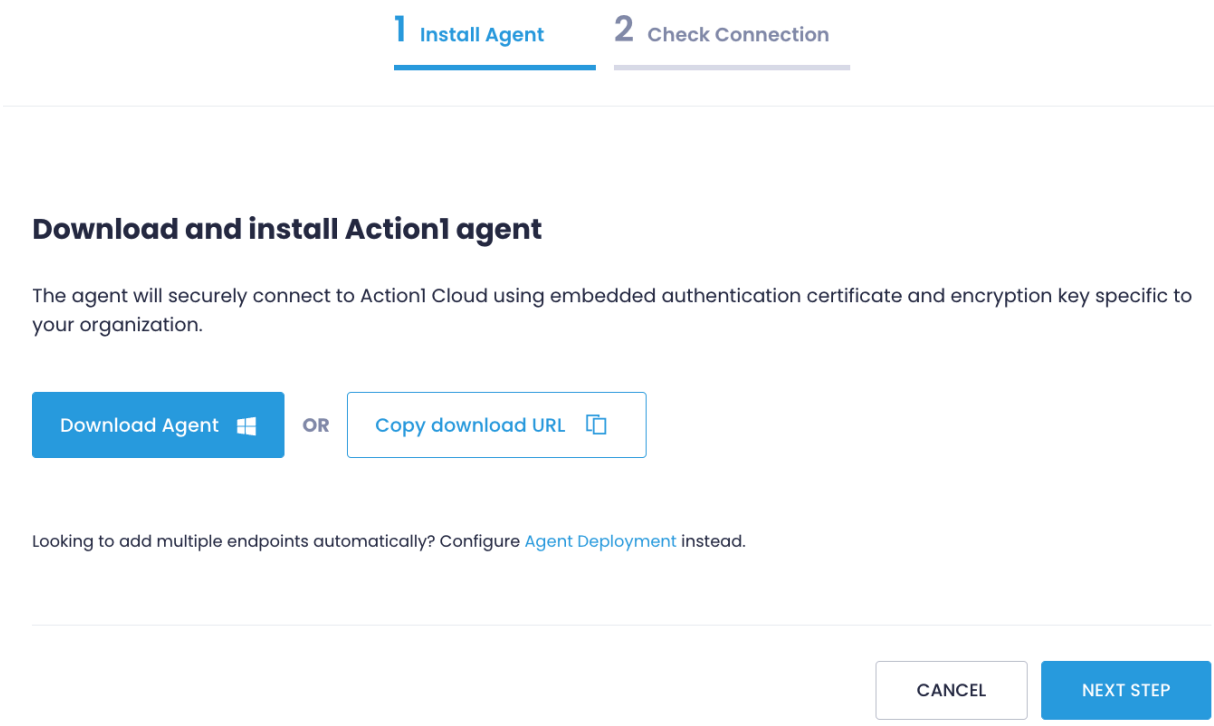
快速指南影片
https://www.action1.com/documentation/adding-endpoints-manually/

六 . 使用群組政策(Group Policy)安裝

GPO (Group Policy Object)軟體安裝是一種在多個工作站或伺服器上部署 Action1 Agent 的方法。

通過 GPO 軟體安裝交付 Action1 Agent

1. 導航到 Endpoints 並選擇 **Install Agents** 以下載 Action1 Agent 安裝程式。然後將其複製到 **網域控制器上的檔案夾中**，網路中的其他端點可以存取該檔案夾。



2. 啟動群**組政策管理控制台(Group Policy Management Console)**並向下點選到您的網域。

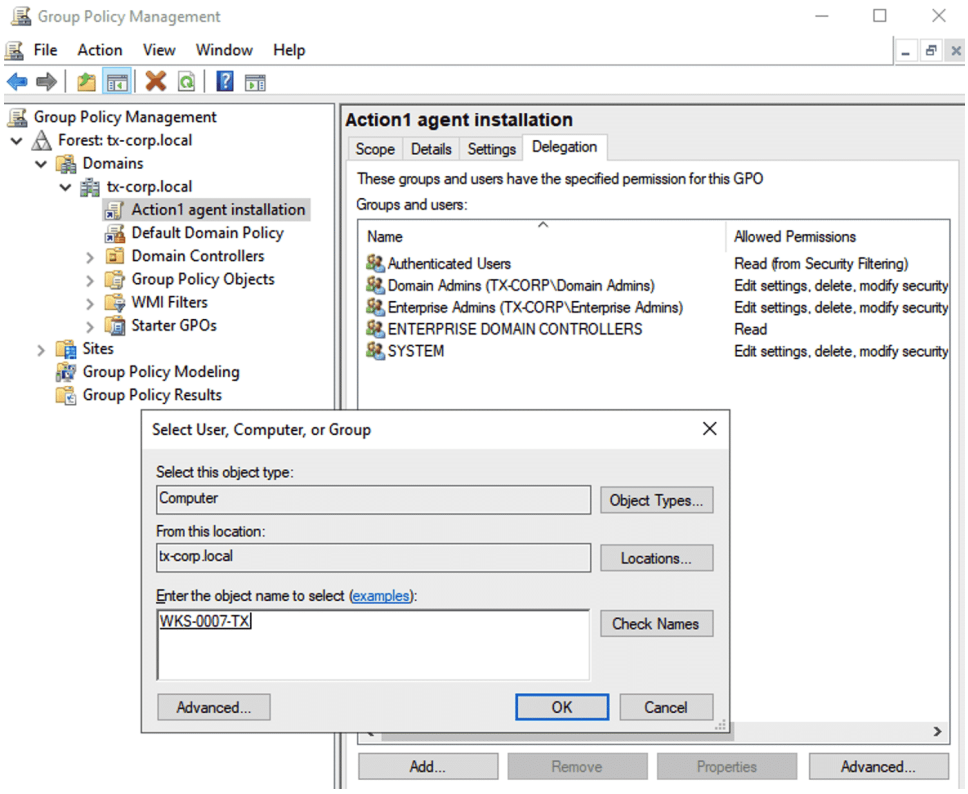
3. 右鍵單擊它並選擇在此**網域中建立 GPO，然後在此處連結(Link)**。

4. 為新的網域政策提供名稱，例如 *Action1 agent installation*。

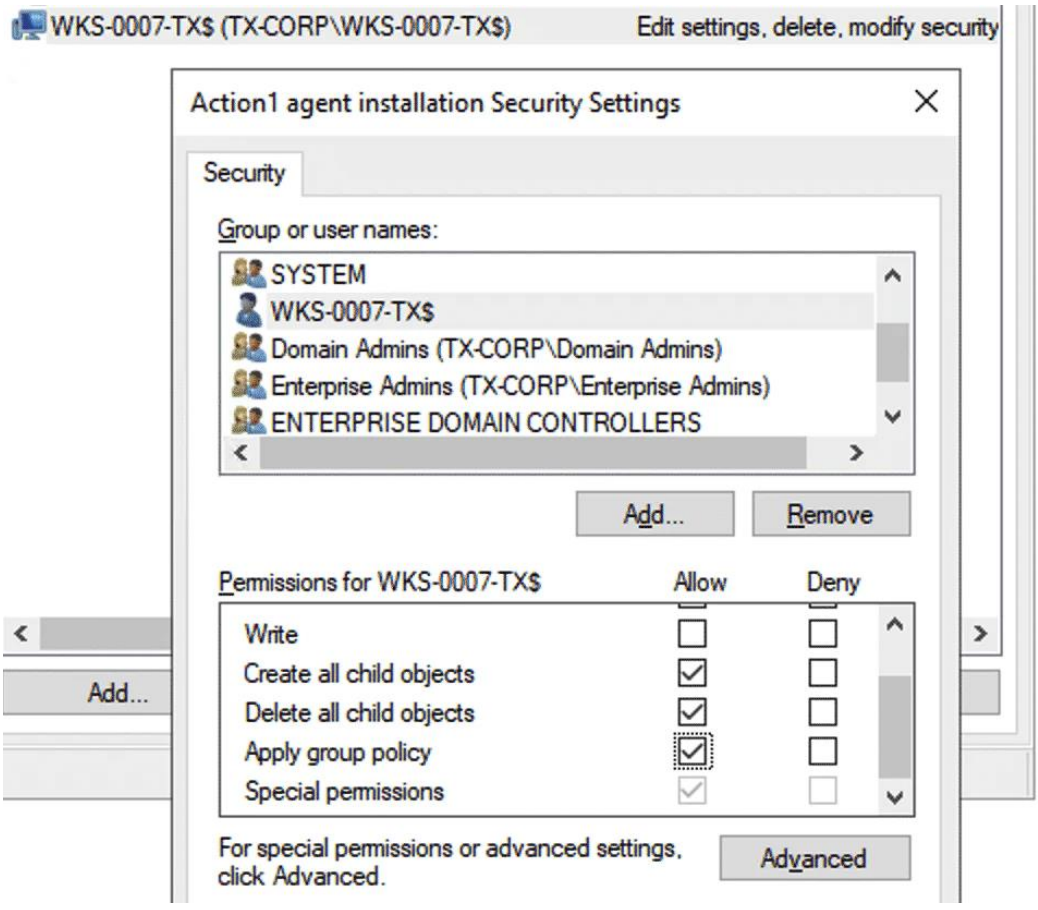
5. 在政策設置中，前往**委派(Delegation)選項**。選擇屏幕底部的**增加(Add)**。

6. 在**選擇使用者、電腦或組(Select User, Computer, or Group)視**窗中，將**物件類型(Object Types)**設置為 ***"電腦(Computer)"*** 。輸入電腦名稱並選擇 **"檢查名稱(Check Names)"** 以查找它。將新組的權限設置為 ***"編輯設置、刪除、修改安全性(Edit settings, delete, modify security)"*** 。

注意： 增加要安裝 Action1 Agent 程式的所有電腦。

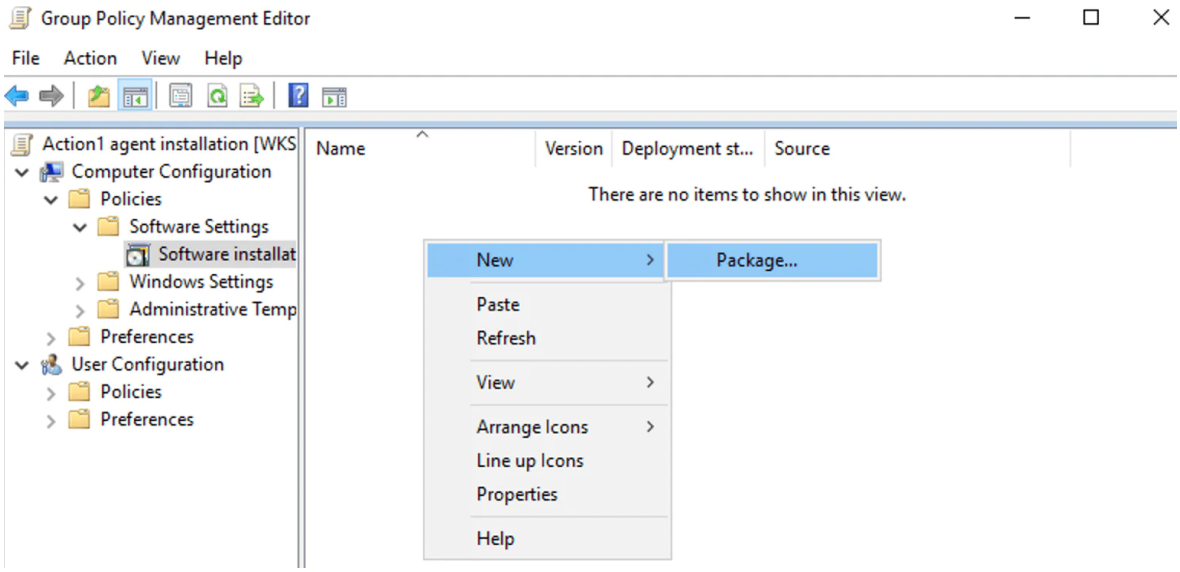


7. 選擇新組並指定 **Advanced**。在打開的對話框中，選擇電腦組並更新權限：將**應用群組政策 (Apply group policy)**設置為 *"允許(Allow)"*。

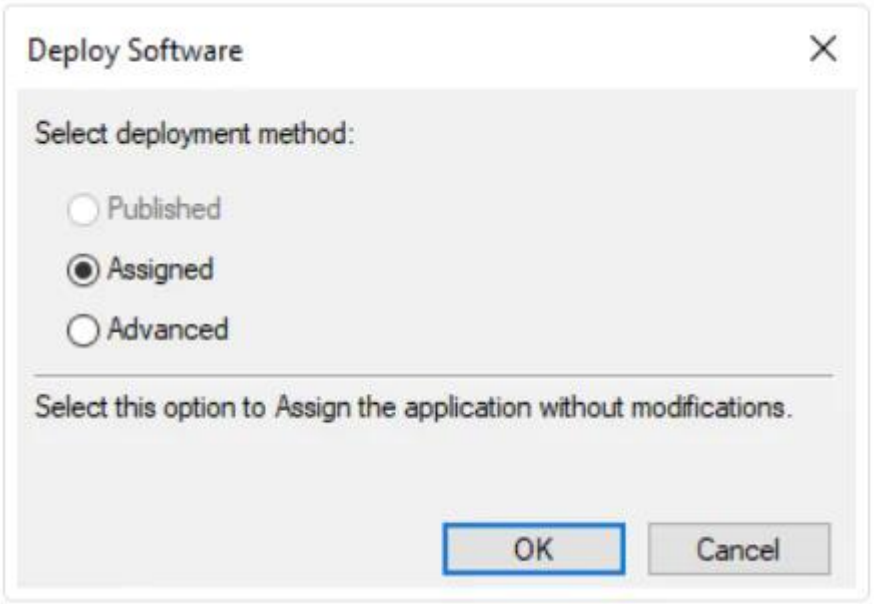


8. 右鍵單擊新建立的政策並選擇**編輯(Edit)**，然後繼續**電腦配置/政策/軟體設置(Computer Configuration / Policies / Software Settings)**。

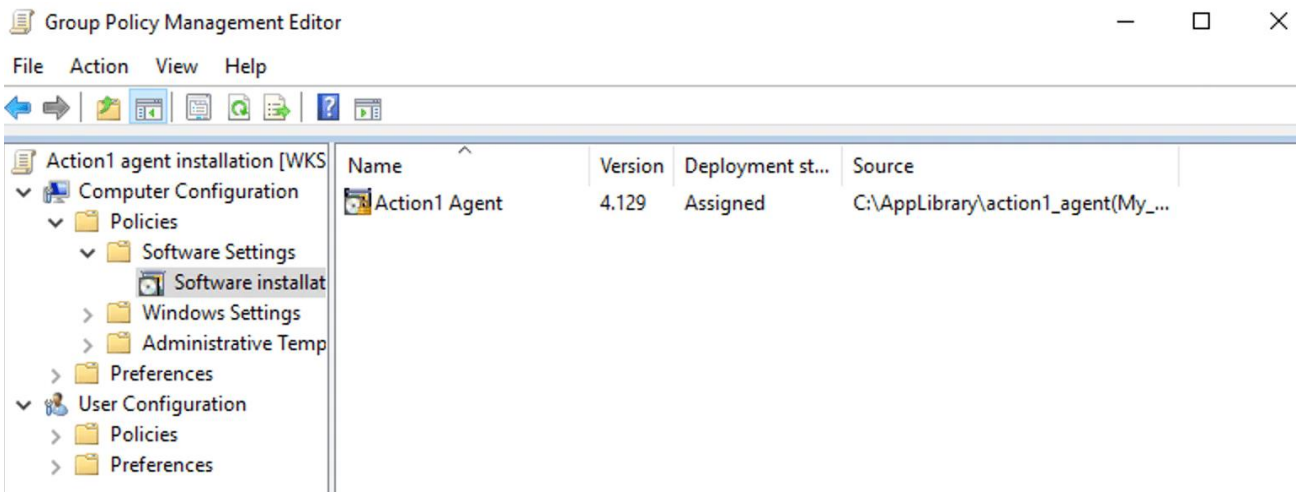
9. 在**軟體安裝 Software installation** 頁面上，右鍵單擊並選擇**新建/打包(New / Package)**。



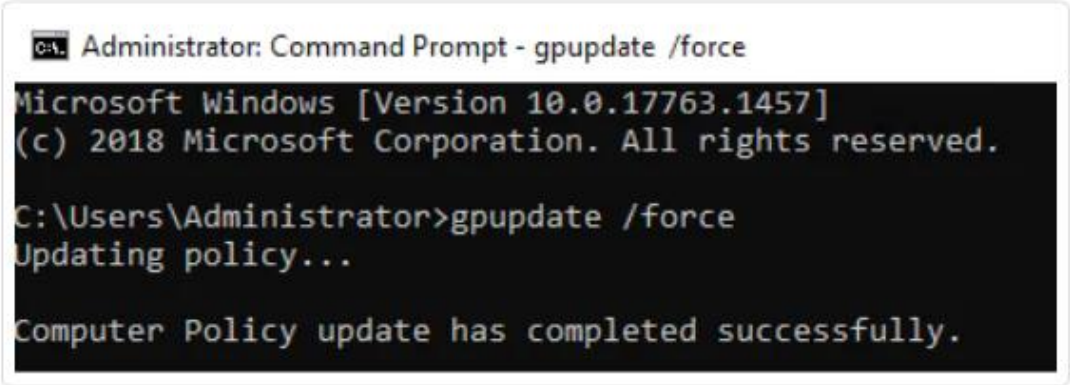
10. 選擇 Agent MSI 檔案。在打開的對話框中，將部署方法設置為 “已分配(Assigned)” 。



11. 新建立的安裝包將出現在列表中。



12. 在指令提示下，執行“gpupdate /force”。一旦重新啟動，Agent 將分發到受群組政策管理的所有端點和設備。



故障排除提示：

- 檢查 Internet 連接並確保**電腦配置/管理模板/系統/登錄/始終在電腦啟動和登錄時等待網路(Computer Configuration / Administrative Templates / System / Logon / Always wait for the network at computer startup and logon)** 設置為 *“已啟用”*。

- 增加**電腦配置/政策/管理模板/系統/組政策/指定啟動政策處理等待時間(Computer Configuration / Policies / Administrative Templates / System / Group Policy / Specify startup policy processing wait time)**下的超時值(timeout value)。

七. 故障排除

以下是我們的使用者通常遇到的最常見問題。

安裝(Installation)： 安裝錯誤最常見的原因是在沒**有管理權限**的情況下執行 Action1 Deployer 或 Agent 安裝程式。確保以管理員身份執行來啟動檔案。

部署(Deployment)： 查看 日誌 頁面以查看 Agent 部署和操作期間發生的錯誤。如果您不理解某些錯誤消息，請隨時聯繫我們的技術支持， 我們將為您提供幫助。

網路連接(Network connectivity)： 最常見的是，連接問題與防火牆設置拒絕連接有關。必須為**出站連接打開端口 22543 和 443；端口 22551 必須為入站連接打開**。您可能需要配置公司防火牆以允許這些連接。請隨時聯繫我們的技術支持以獲取網路配置方面的幫助。有關詳細信息，請參閱**防火牆配置。**

報告執行時間過長或未返回任何結果(Reports run too long or return no results)： 某些報告可能需要很長時間才能完成（有時需要數小時，具體取決於檔案和端點的數量）。您可以更新報告結果（無需重新執行）以在一段時間後查看最新結果。

不會產生警報(Alerts are not generated)： 確保您在電子郵件設置中將 Action1.Platform@action1.com 和 www.action1.com 電子郵件網域列入白名單。此外，為了防止您的收件箱溢出，如果一個警報規則每小時從一個端點產生超過 10 個警報，警報將被抑制（在這種情況下您會收到通知）。通過增加額外的過濾器來重新配置規則以降低警報觸發頻率。

有阻止 PowerShell 腳本的防病毒軟體？有時 Avast 和 AVG 等 AV 應用程式可以阻止 Action1 執行的 PS 腳本。為避免阻止，請在防病毒設置中將 Action1 檔案夾列入白名單。為此，在您的防病毒應用程式中，導航至**選單/設置/一般/例外(Menu / Settings / General / Exceptions)**並增加以下檔案和檔案夾：

- C:\Windows\Action1\scripts
- C:\Windows\Action1\action1_agent.exe
- C:\Windows\Action1\action1_remote.exe

Action1

雲原生漏洞修補管理平台

常見問題 Q&A

1. Action1 將哪些端點資料存儲在雲端？

Action1 維護的端點列表，其中包括電腦主機名稱、IP 地址和連接統計信息。出於效率目的，還會在雲中執行端點資料的短期暫存。

當執行查詢時，Action1 Cloud 會聯繫端點以查詢信息，將查詢結果暫存在雲端，，然後在 Web 控制台中顯示或通過電子郵件發送（排程查詢）。 之後，端點資料將從 Action1 Cloud 中永久刪除。因此，始終擁有來自端點的最新即時信息（而不是數小時甚至數天前收集的過時資料）。

當警報產生時，首先由 Agent 發送到 Action1 Cloud，然後 Action1 Cloud 將通過 SMTP 發送到您的電子郵件地址，然後刪除警報內容。Action1 還存儲一些診斷信息（見記錄） 7 天。如果希望比規定的時間更早刪除任何此類資料，請聯繫技術支持。

2. Action1 雲伺服器託管在哪裡？

Action1 雲伺服器目前託管在美國弗吉尼亞（Virginia）與德國法蘭克福(Frankfurt, Germany)資料中心的 Amazon Web Services 與德國法蘭克福的資料中心。如果您的組織受制於限制信任上述位置的任何本地資料隱私法規，請聯繫技術支持以討論您的要求。

3. Action1 Cloud 的安全性如何？

Action1 的設計是在充分利用 Amazon Web Services 最先進的內建安全機制和嚴格的內部流程，確保最高標準的客戶資料保護。例如，在內部使用多因子身份驗證、資料加密和基於需要知道的存取權限，確保組織中沒有任何人在任何時候都擁有“國王的鑰匙(keys to the kingdom)”。

Action1 Cloud 與 Action1 Agents 及 Deployer 之間的所有通信都通過最新版本的 SSL/TLS 協定進行，該協定具有相互身份驗證和加密功能，可提供針對竊聽、資料篡改甚至中間人攻擊的全面保護。

Action1 Agent 和 Deployer 分發包在下載時自動嵌入安全驗證信息（私有加密密鑰、驗證證書和客戶 ID），並且不會發生未經驗證或明文通信。自動代理(Agent)更新也可以免受 DNS 欺騙和其他復雜攻擊，因為每個下載的更新都經過完整性驗證，以確保來自可信來源。要了解有關安全架構和內部組織實踐的更多信息。

4. 為什麼不在 Action1 控制台中使用 SMS 進行多重身份驗證？

多因子身份驗證是為登錄過程帶來額外的安全層，當輸入憑證後，系統會提示提供一次性代碼。SMS 不再被認為是安全的，因為電話號碼所有權很容易被撤銷和侵犯。

在 Action1 中，我們建議使用 **Google Authenticator、Twilio Authy、Duo Mobile 或 Microsoft Authenticator 等身份驗證應用程式**。 此外，還可以利用發送到公司電子郵件的一次性代碼。 MFA 確保更高級別的保護，同時使您的組織符合資料安全標準。

5. Action1 Deployer 要求提供具有管理員權限的憑證 - 為什麼？

Action1 Deployer 僅使用管理員憑證來部署 Action1 更新服務，該服務又會在您的網路上部署 Agent。Action1 Deployer 永遠不會將這些憑證發送到 Action1 Cloud 或您的 Agent 上。

如果無法向 Action1 Deployer 提供管理憑證，可以使用其他部署選項，例如通過**群組政策 (Group Policy)、手動或批量安裝**。 如果您需要這方面的幫助，請參閱線上文檔(online documentation)或聯繫技術支持。

6. Action1 使用哪些 TCP/IP 端口？

Action1 Deployer 和 Action1 Agents 使用 **TCP Port 22543** 上的安全連接與 Action1 Cloud 通信，因此需要打開此 TCP Port 以進行直接出站連接（繞過任何代理伺服器-proxy servers）。**入站 Port 22551** 也應該打開以允許 2P2 檔案分發。 有關詳細信息，請參閱防火牆配置。

7. 每個客戶 Action1 支持多少個端點？

Action1 從一開始設計就是基於雲的技術，具有幾乎無限的可擴展性，以支持數百萬個端點。隨著更多 Agent 的推出，多層次架構會自動擴展。

8. 每個客戶有多少可用空間？

存儲配額取決於連接到 Action1 Cloud 的端點數量。**Action1 通常為每個端點保留 1 GB**。 例如，對於 100 個端點的許可證，我們將提供最多 100 GB 的空間來存儲軟體包(store packages)。如果需要額外的空間，請隨時與我們聯繫。我們可以延長存儲配額，但需要額外收費。

9. Action1 Agent 是否使用任何重要的系統資源？

Action1 Agent 是一個很小的可執行檔案（小於 6 MB），佔用的資源最少。除非啟用警報規則，否則它大部分時間都處於空閒狀態，等待您的查詢。

如果啟用警報，它會使用更多的 CPU、記憶體和磁碟資源，具體取決於啟用的警報規則的數量和這些規則的複雜性（例如應用於過濾器）。 通常，**它只使用大約 10-15 MB 的磁盤空間、30-50 MB 的記憶體，偶爾會消耗 1 個 CPU 來處理查詢和監視警報條件。**

10. 網路頻寬要求是什麼？

Action1 使用一種負載很小的高效通信協定。使用查詢時，使用的頻寬量取決於查詢輸出（返回的結果數）。**使用警報時，通常每個產生的警報消耗大約 5 KB**（並且可以產生固定數量的警報：目前設置為每個規則每小時 10 個警報）。

此外，還有一些與自動 Agent 更新相關的負載，這種情況時有發生。**每個端點每次更新大小大約為 6 MB**，並且隨著我們不斷改進服務的功能，它通常每月發生幾次。但是，如果使用 Action1 Deployer，**則可以大大減少更新負載。在這種情況下，更新僅從 Action1 Cloud 下載一次，然後通過本地網路自動分發給所有 Agent。**

11. 託管是以什麼為基礎的產品或服務？

Action1 是從一開始構建的，沒有使用除 Amazon Web Services 之外的任何第三方產品或服務。Action1 不在伺服器上託管任何第三方產品，也不使用任何第三方產品或服務。此外，作為一家技術公司，Action 的政策是絕不外包任何核心技術活動，包括開發、DevOps 或技術支持。

12. 為什麼不能只使用 PowerShell 腳本來完成相同的功能？

是的，幾乎可以通過使用腳本來完成一切。但是，在這種情況下必須考慮所有風險和維護成本，處理複雜性、可擴展性和可靠性問題。您幾乎可以在網上找到任何類型的腳本或實用程式，並自行承擔使用風險，並在管理憑證下運行。

隨著系統和流程的發展，還必須維護腳本。定期管理、解釋和自動分析腳本產生的資料，是一項非常繁瑣的任務，可能需要大量的管理框架（排程任務、加密資料存儲、電子郵件警報等）。

最重要的是，增加網路連接問題（您的所有端點是否 100% 在線？）以及自訂系統的一般可靠性和安全性。Action1 解決了這些問題，並通過統一的資料分析能力和高效的實時資料處理增加了很多附加值。