步驟 2. IISLockdown

IISLockdown 工具可以協助您自動化特定的安全性步驟。IISLockdown 可以大為減少 Windows 2000 Web 伺服器的弱點。讓您可以挑選特定類型的伺服器角色，然後使用自訂範本來改善該特定伺服器的安全性。此範本可以停用或保護各種功能的安全。此外，IISLockdown 會安裝 URLScan ISAPI 篩選器。URLScan 可以讓網站系統管理員根據系統管理員控制的一組規則來限制伺服器可處理的 HTTP 要求種類。藉由封鎖特定 HTTP 要求，URLScan 篩選器可以預防具有潛在危害的要求傳到伺服器，進而造成損害。

在此步驟中，您要：

- 安裝並執行 IISLockdown
- 安裝並設定 URLScan

安裝並執行 IISLockdown

IISLockdown 可以由網際網路從 Microsoft 網站下載，此網站位於 http://download.microsoft.com/download/iis50/Utility/2.1/NT45XP/EN-US/iislockd.exe。

將 IISlockd.exe 儲存在本機資料夾中。IISlockd.exe 是 IISLockdown 精靈，並非安裝程式。藉由再次執行 IISlockd.exe，可以還原所做的任何變更。

如果要鎖定管理 ASP.NET 網頁的 Windows 2000 電腦，請在 IISLockdown 工具提示時選取動態 Web 伺服器範本。在選取動態 Web 伺服器時，IISLockdown 會執行下列各項動作：

- 停用下列不安全的網際網路服務：
  - 檔案傳輸通訊協定 (FTP)
  - 電子郵件服務 (SMTP)
  - 新聞服務 (NNTP)
- 藉由對應下列副檔名到 404.dll 而停用指令碼對應：
  - 索引伺服器
  - Web 介面 (.idq、.htw、.ida)
  - 伺服器端包含檔案 (.shtml、.shtm、.stm)
  - 網際網路資料連接器 (.idc)
  - .HTR 指令碼 (.htr)、網際網路列印 (.printer)
- 移除下列虛擬目錄：IIS 範例、MSADC、IISHelp、Scripts 及 IISAdmin。
- 限制匿名存取系統公用程式及使用 Web 權限寫入 Web 內容目錄的能力。
- 停用 Web Distributed Authoring and Versioning (WebDAV)。

安裝 URLScan ISAPI 篩選器。

注意 如果您並非使用典型的 ASP，請勿使用靜態 Web 伺服器範本。此範本會移除 ASP.NET 網頁所需的基本功能，例如支援 POST 命令。 記錄檔

IISLockdown 會建立兩份報告，列出已經套用的變更： •

%windir%\system32\inetsrv\oblt-rep.log。此報告含有高階資訊。 •

%windir%\system32\inetsrv\oblt-log.log。此報告含有低階細節，例如哪些程式檔案設定為拒絕存取控制項目 (ACE)，以防止匿名網際網路使用者帳戶存取這些檔案。此記錄檔也可以用來支援 IISLockdown 復原

變更功能 Web 匿名使用者及 Web 應用程式群組

IISLockdown 建立 Web Anonymous Users 群組及 Web Application 群組Web Anonymous Users 群組包含 IUSR_MACHINE 帳戶Web Application 群組包含 IWAM_MACHINE 帳戶。根據這些群組來指派權限給系統工具及內容目錄，而不是直接指派給 IUSR 及 IWAM 帳戶。藉由檢視 IISLockdown 記錄檔 %windir%\system32\inetsrv\oblt-log.log可以檢視特定權限 404.dll

IISLockdown 會安裝 404.dll用來對應禁止用戶端執行的副檔名。如需詳細資訊，請參閱 <步驟 12：指令碼對應 URLScan

如果安裝 URLScan ISAPI 篩選器做為 IISLockdown 的一部份URLScan 設定會與執行 IISLockdown 時選取的伺服器角色整合在一起。例如，如果選擇靜態 Web 伺服器URLScan 會封鎖 POST 命令。 復原 IISLockdown 變更

若要復原 IISLockdown 執行的變更，請再次執行 IISLockd.exe如此會移除 URLScan ISAPI 篩選器。如需詳細資訊，請參閱本指南How To使用 URLScan一節中的<移除 URLScan 其他資訊

如需有關 IISLockdown 工具的詳細資訊，請參閱下列文件： •

如需有關執行 IISLockdown 的詳細資訊，請參閱本指南How To一節中的How To使用 IISLockdown.exe •

如需有關疑難排解 IISLockdown 的詳細資訊，請參閱Microsoft 知識庫文件325864How To: Install and Use the IIS Lockdown Wizard (最常見的問題是在執行 IISLockdown 之後意外收到 404 File Not Found (找不到檔案) 錯誤訊息)。 •

如需有關自動化 IISLockdown 的詳細資訊，請參閱Microsoft 知識庫文件310725How To: Run the IIS Lockdown Wizard Unattended in IIS

安裝和設定 URLScan

雖然可以個別下載和安裝 URLScan但在執行 IISLockdown 時就會安裝 URLScan

- 安裝 URLScan 而不執行 IISLockdown

1. 從 http://download.microsoft.com/download/iis50/Utility/2.1/NT45XP/EN-US/iislockd.exe 下載 IISlockd.exe
2. 執行下列命令以擷取 URLScan 安裝程式：

iislockd.exe /q /c

URLScan 封鎖包含不安全字元的要求 (例如已經用來利用弱點的字元，如目錄周遊所用的..)URLScan 在 %windir%\system32\inetsrv\urlscan 目錄中記錄含有這些字元的要求。

可以使用 .ini 檔案 %windir%\system32\inetsrv\urlscan\urlscan.ini 中的設定值來設定 URLScan

除了封鎖惡意要求之外，還可以在要求抵達 ASP.NET 之前使用 URLScan 防禦伺服器而免於拒絕服務攻擊。如果要執行這項操作，請在 URLScan.ini 檔案中以 MaxAllowedContentLength、MaxUrl 及 MaxQueryString 引數設定其限制。如需詳細資訊，請參閱本指南How To一節中的How To使用 URLScan 復原 URLScan 變更

沒有自動化的作業可以移除 URLScan□如果 URLScan 發生問題，可以從 IIS 加以移除，或藉由記錄遭到拒絕的要求來解析問題。如果要執行這項操作，請在 URLScan .ini 檔案中使用選項 RejectResponseUrl=/~* □

如需有關如何移除 ISAPI 篩選器的詳細資訊，請參閱本單元稍後的＜步驟 13□ISAPI 篩選器＞。 其他資訊

如需有關 URLScan 工具的詳細資訊，請參閱下列文件：

・如需有關執行 URLScan的詳細資訊，請參閱本指南□How To□一節中的□How To□使用 URLScan□□

・如需有關 URLScan 設定及 URLScan.ini 檔案設定的詳細資訊，請參閱□Microsoft 知識庫」文件 326444 □How To: Configure the URLScan Tool□□

From:
https://net.nthu.edu.tw/netsys/ - **網路系統組**

Permanent link:
https://net.nthu.edu.tw/netsys/security:guideline:web_server_windows_step2

Last update: **2009/06/01 09:40**