# 適用於Cisco整合應答主控台進階伺服器的Windows伺服器強化

## 目錄



#### 概觀

本檔案介紹可在思科整合應答主控台進階版(CUACA)伺服器上進行的一些組態變更，以確保其更安全。 使Windows系統更安全的過程稱為Windows強化。 下列資訊可作為強化思科整合應答主控台進階伺服器的指南。

#### 防火牆和組策略

將Windows伺服器新增到域後，可以將組策略推送到Windows。推送到CUACA伺服器的防火牆策略和組策略不應阻止或中斷以下服務和埠的工作：

- Windows Management Instrumentation(WMI)
- 分散式事務處理協調器(MDDTC) — 僅在使用SQL複製/恢復性時需要
- 消息匯流排(MBUS) — 開啟入站和出站埠61616和61618（僅在使用SQL複製/恢復時需要）
- exe - *例如：C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Binn\sqlservr.exe*
- 埠號（由CUAC使用）：

| 連接埠號碼 | 連線埠型別 |
|---|---|
| 80 | TCP |
| 389 | TCP |
| 443 | TCP |
| 636 | TCP |
| 1433和1434 | TCP |
| 1859 | TCP |
| 1862 | TCP |
| 1863 | TCP |
| 1864 | TCP |
| 2748 | TCP |
| 5060 | UDP |
| 5061和5062 | TCP |
| 11859 | TCP |
| 61616 | TCP |
| 61618 | TCP |
| 49152 - 65535 | TCP |
| 1025至5000 | TCP |

| 連線埠號碼 | 使用 |
|---|---|

| | |
|---|---|
| 389 | LDAP伺服器不使用SSL，並且未配置為全域性目錄。 |
| 636 | LDAP伺服器使用SSL，並且未配置為全域性目錄。 |
| 3268 | LDAP伺服器不使用SSL，而是配置為全域性目錄。 |
| 3269 | LDAP伺服器使用SSL並配置為全域性目錄。 |

在實施之前請參閱最新的管理和安裝指南，以驗證排除清單。

**防病毒軟體**

在Windows伺服器上安裝防病毒軟體，使其免受惡意軟體、病毒等攻擊。但是，防病毒應用程式會減慢CUACA伺服器的功能，因為它在防病毒掃描期間需要連續訪問幾個資料夾。因此，建議新增以下檔案和資料夾作為防病毒軟體的排除項：

| 預設資料夾 | 包含 |
|---|---|
| \\DBData | 系統配置資料庫 |
| \\Program Files\Cisco\ | 軟體和應用程式跟蹤檔案 |
| \\Apache | 活動MQ資料夾 |
| \\Temp\Cisco\Trace | Cisco TSP跟蹤檔案 |
| \\%ALLUSERSPROFILE%\Cisco\CUACA | 思科設定檔 |

這些是CUACA安裝程式使用的預設位置。如果管理員更改這些資料夾的位置或使用某些其他資料夾，則需要相應地更改防病毒例外。

在實施之前請參閱最新的管理和安裝指南，以驗證排除清單。

**禁用IP源路由**

IP源路由現在很少使用，但駭客可以使用它繞過防火牆，因此，思科建議禁用它。

以下是禁用IP源路由的步驟：

- 開啟Regedit
- 設定或建立以下值：
  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\

  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip6\Parameters\

  值名稱：禁用IPSourceRouting
  值型別：REG_DWORD
  值：2

- 關閉Regedit。

**Windows更新**

思科建議使用最新的Microsoft Windows和SQL Server更新以及Service Pack為Windows伺服器打補

丁。應禁用自動更新和自動檢查更新。

不支援Java自動更新，因為它們有時會失敗，這可能會導致系統不可用。支援次要更新。

所有對更新的檢查和更新安裝應在生產外部執行。安裝後，請重新啟動伺服器作業系統。

**根據公司政策的其他強化要求**

思科建議根據要求/策略強化Windows Server，但管理員需要確保在強化後滿足所有CUACA要求。有關CUACA要求的詳細資訊，請參閱CUACA設計手冊和CUAC安裝指南。