Cisco Unified Attendant Console Advanced Server的Windows Server强化

目录

概述

本文档介绍可在Cisco Unified Attendant Console Advanced(CUACA)服务器上进行的几项配置更改，以使其更加安全。 使Windows系统更安全的过程称为Windows强化。 下面列出的信息可用作加强Cisco Unified Attendant Console高级服务器的指南。

防火墙和组策略

将Windows服务器添加到域后，组策略可以推送到Windows。推送到CUACA服务器的防火墙策略和组策略不应阻止或中断以下服务和端口的工作：

- Windows Management规范(WMI)
- 分布式事务协调器(MDDTC) — 仅在使用SQL复制/恢复时才需要
- 消息总线(MBUS) — 打开入站和出站端口61616和61618（仅在使用SQL复制/恢复时才需要）
- exe -*例如：C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Binn\sqlservr.exe*
- 端口号（由CUAC使用）：

端口号	端口类型
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 到 65535	TCP
1025 到 5000	TCP

端口号	使用

389	LDAP服务器不使用SSL，并且未配置为全局目录。
636	LDAP服务器使用SSL，未配置为全局目录。
3268	LDAP服务器不使用SSL，并配置为全局目录。
3269	LDAP服务器使用SSL，并配置为全局目录。

在实施之前，请参阅最新的《管理和安装指南》，以验证排除项列表。

防病毒软件

在Windows服务器上安装防病毒软件，以防恶意软件、病毒等。但是，防病毒应用程序会降低CUACA服务器功能，因为它需要在防病毒扫描时连续访问少数文件夹。因此，建议在防病毒软件中添加以下文件和文件夹作为例外项：

默认文件夹	包含
\\DBData	系统配置数据库
\\计划Files\Cisco\	软件和应用跟踪文件
\\Apache	活动MQ文件夹
\\Temp\Cisco\Trace	思科TSP跟踪文件
\\%所有用户配置文件%\Cisco\CUACA	思科简档

这些是CUACA安装程序使用的默认位置。如果管理员更改了这些文件夹的位置或使用某些其他文件夹，则需要相应地更改防病毒的排除项。

在实施之前，请参阅最新的《管理和安装指南》，以验证排除项列表。

禁用 IP 源路由

IP源路由现在很少使用，但黑客可以使用它绕过防火墙，因此思科建议禁用它。

以下是禁用IP源路由的步骤：

- 打开Regedit
- 设置或创建以下值：
  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\

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

  值名称：禁用IPSource路由
  值类型：REG_DWORD
  值：2

- 关闭Regedit。

Windows更新

思科建议使用最新的Microsoft Windows和SQL Server更新及Service Pack对Windows服务器进行修补。应禁用自动更新和自动检查更新。

不支持Java自动更新，因为它们有时会失败，这可能导致系统不可用。支持次要更新。

所有更新检查和更新安装都应在生产之外执行。安装后，请重新启动服务器操作系统。

根据公司策略的其他强化要求

但是，思科建议根据要求/策略强化Windows Server，管理员需要确保强化后满足所有CUACA要求。有关CUACA要求的详细信息，请参阅CUACA设计指南和CUAC安装指南。