

Cisco Unified Attendant Console Advanced ServerのWindows Serverの強化

内容

[概要](#)

[ファイアウォールとグループポリシー](#)

[アンチウイルスソフトウェア](#)

[IP ソース ルーティングを無効化](#)

[Windowsの更新](#)

[会社のポリシーに従ったその他の強化要件](#)

概要

このドキュメントでは、Cisco Unified Attendant Console Advanced(CUACA)サーバで設定を変更し、より安全な設定を行う方法について説明します。Windowsシステムをより安全にするプロセスは、Windowsの強化と呼ばれます。次に示す情報は、Cisco Unified Attendant Console Advancedサーバの強化ガイドとして使用できます。

ファイアウォールとグループポリシー

Windowsサーバをドメインに追加したら、グループポリシーをWindowsにプッシュできます。CUACAサーバにプッシュされるファイアウォールポリシーおよびグループポリシーは、次のサービスおよびポートの動作をブロックまたは中断してはなりません。

- Windows Management Instrumentation (WMI)
- 分散トランザクションコーディネーター(DDTC):SQLレプリケーション/復元力を使用する場合にのみ必要
- メッセージバス(MBUS) : 着信および発信ポート61616および61618を開きます (SQLレプリケーション/復元力を使用する場合のみ必要)
- exe -例 : *C:\Program Files\Microsoft SQL Server\MSSQL 10.MSSQLSERVER\MSSQL\Binn\sqlservr.exe*
- ポート番号 (CUACで使用) :

Port Numbers	ポート タイプ
80	TCP
389	TCP
443	TCP
636	TCP
1433 と 1434	TCP
1859	TCP
1862	TCP
1863	TCP
1864	TCP
2748	TCP
5060	UDP
5061 と 5062	TCP
11859	TCP
61616	TCP

61618	TCP
49152 ~ 65535	TCP
1025 ~ 5000	TCP

ポート番号	利用
389	LDAPサーバはSSLを使用せず、グローバルカタログとして設定されていません。
636	LDAPサーバはSSLを使用し、グローバルカタログとして設定されていません。
3268	LDAPサーバはSSLを使用せず、グローバルカタログとして設定されます。
3269	LDAPサーバはSSLを使用し、グローバルカタログとして設定されます。

除外リストを検証するには、[実装の前に最新の管理ガイド](#)およびインストールガイドを参照してください。

アンチウイルスソフトウェア

Windowsサーバにアンチウイルスソフトウェアをインストールして、マルウェアやウイルスなどから保護します。ただし、ウイルス対策アプリケーションでは、少数のフォルダに継続的にアクセスする必要があるため、CUACAサーバの機能が遅くなります。また、ウイルス対策アプリケーションによってスキャンされます。したがって、次のファイルとフォルダをウイルス対策ソフトウェアの除外として追加することをお勧めします。

既定のフォルダ	含む
\\DBData	システム構成データベース
\\プログラムFiles\Cisco\	ソフトウェアおよびアプリケーションのトレースファイル
\\Apache	アクティブMQフォルダ
\\Temp\Cisco\Trace	Cisco TSPトレースファイル
\\%ALLUSERSPROFILE%\Cisco\CUACA	シスコプロファイル

これらは、CUACAインストーラで使用されるデフォルトの場所です。管理者がこれらのフォルダの場所を変更したり、他のフォルダを使用する場合は、ウイルス対策の除外を適宜変更する必要があります。

除外リストを検証するには、[実装の前に最新の管理ガイド](#)およびインストールガイドを参照してください。

IP ソースルーティングを無効化

IPソースルーティングは現在ではほとんど使用されていませんが、ハッカーはそれをファイアウォールのバイパスに使用できるため、シスコデバイスはこれを無効にします。

IPソースルーティングを無効にする手順は、次のとおりです。

- Regeditを開く
- 次の値を設定または作成します。
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\

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

値の名前 : DisableIPSourceRouting

値の種類 : REG_DWORD

[Value] : 0

- regedit を閉じます。

Windowsの更新

シスコでは、Windowsサーバに最新のMicrosoft WindowsおよびSQL Serverのアップデートとサービスパックを適用し続けることを推奨しています。自動更新と更新の自動チェックを無効にする必要があります。

Javaの自動更新はサポートされていません。これは、システムが使用できなくなる可能性があるためです。マイナーアップデートがサポートされます。

アップデートおよびアップデートのインストールに関するすべてのチェックは、実稼働外に実行する必要があります。インストール後、サーバOSを再起動します。

会社のポリシーに従ったその他の強化要件

ただし、要件/ポリシーに従ってWindows Serverを強化するようにシスコからアドバイスを受けているため、管理者は、すべてのCUACA要件が強化された後に満たされていることを確認する必要があります。CUACA要件の詳細については、『CUACA設計ガイド』および『CUACインストールガイド』を参照してください。