Windows Server Hardening pour Cisco Unified Attendant Console Advanced Server

Contenu

Aperçu

Ce document décrit plusieurs modifications de configuration qui peuvent être apportées sur un serveur Cisco Unified Attendant Console Advanced (CUACA) afin de le rendre plus sécurisé. Le processus de sécurisation du système Windows est appelé renforcement de Windows. Les informations ci-dessous peuvent être utilisées comme guide pour renforcer votre ou vos serveurs Cisco Unified Attendant Console Advanced.

Politiques de pare-feu et de groupe

Une fois le serveur Windows ajouté au domaine, les stratégies de groupe peuvent être poussées vers Windows. Les stratégies de pare-feu et de groupe poussées vers le serveur CUACA ne doivent pas bloquer ou interrompre le fonctionnement des services et ports suivants :

- WMI (Windows Management Instrumentation)
- MDTC (Distributed Transaction Coordinator) - obligatoire uniquement si vous utilisez la réplication/résilience SQL
- Bus de messages (MBUS) - ports entrants et sortants ouverts 61616 et 61618 (requis uniquement si vous utilisez la réplication/résilience SQL)
- exe - *Par exemple : C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Binn\sqlservr.exe*
- Numéros de port (utilisés par CUAC) :

Numéros de port	Type de port
80	TCP
389	TCP
443	TCP
636	TCP
1433 et 1434	TCP
1859	TCP
1862	TCP
1863	TCP
1864	TCP
2748	TCP
5060	UDP
5061 et 5062	TCP
11859	TCP

61616	TCP
61618	TCP
49152 à 65535	TCP
1025 à 5000	TCP

Port number (numéro de port)	Utilisation
389	Le serveur LDAP n'utilise pas SSL et n'est pas configuré en tant que catalogue global.
636	Le serveur LDAP utilise SSL et n'est pas configuré en tant que catalogue global.
3268	Le serveur LDAP n'utilise pas SSL et est configuré en tant que catalogue global.
3269	Le serveur LDAP utilise SSL et est configuré en tant que catalogue global.

Reportez-vous aux derniers guides d'administration et d'installation avant la mise en oeuvre pour valider la liste des exclusions.

Logiciel antivirus

Installez un logiciel antivirus sur le serveur Windows pour le protéger des programmes malveillants, des virus, etc. Cependant, l'application antivirus ralentit la fonctionnalité du serveur CUACA car elle a besoin d'un accès continu à quelques dossiers pendant que l'antivirus les analyse. Il est donc conseillé d'ajouter les fichiers et dossiers suivants en tant qu'exclusions sur un logiciel antivirus :

Dossier par défaut	Contient
\\DBData	Bases de données de configuration système
\\Programme Files\Cisco\	Fichiers de suivi des logiciels et des applications
\\Apache	Dossier MQ actif
\\Temp\Cisco\Trace	Fichiers de suivi Cisco TSP
\\%ALLUSERSPROFILE%\Cisco\CUACA	Profil Cisco

Il s'agit des emplacements par défaut utilisés par le programme d'installation de CUACA. Si l'administrateur modifie l'emplacement de ces dossiers ou utilise d'autres dossiers, les exclusions sur les antivirus doivent être modifiées en conséquence.

Reportez-vous aux derniers guides d'administration et d'installation avant la mise en oeuvre pour valider la liste des exclusions.

Désactiver le routage de la source IP

Le routage IP Source est rarement utilisé de nos jours, mais les pirates peuvent l'utiliser pour contourner le pare-feu et, par conséquent, Cisco conseille de le désactiver.

Les étapes suivantes permettent de désactiver le routage IP Source :

- Ouvrir Regedit
- Définissez ou créez ces valeurs :
  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\

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

  Nom de la valeur : DésactiverRoutageSourceIPS
  Type de valeur : MOT_RÉG
  Valeur: 2

- Fermez Regedit.

Mises à jour Windows

Cisco recommande de conserver les correctifs Windows Server avec les mises à jour et Service Packs Microsoft Windows et SQL Server les plus récents. Les mises à jour automatiques et les vérifications automatiques des mises à jour doivent être désactivées.

Les mises à jour automatiques Java ne sont pas prises en charge car elles échouent parfois et cela peut entraîner l'inutilisable du système. Les mises à jour mineures sont prises en charge.

Toutes les vérifications des mises à jour et de l'installation des mises à jour doivent être exécutées en dehors de la production. Après l'installation, redémarrez le système d'exploitation du serveur.

Autres exigences de renforcement conformément à la politique de la société

Cisco conseille de renforcer Windows Server conformément aux exigences/politiques. Cependant, l'administrateur doit s'assurer que toutes les exigences CUACA sont satisfaites après le durcissement. Pour obtenir des informations détaillées sur les exigences CUACA, reportez-vous au guide de conception CUACA et au guide d'installation CUAC.