Windows Server durcissant pour l'Advanced Server de console de réception de Cisco Unified

Contenu

Aperçu

Ce document décrit plusieurs modifications de configuration qui peuvent être apportées sur un serveur avancé par console de réception de Cisco Unified (CUACA) afin de le rendre plus sécurisé. Le processus de faire le système Windows sécurisent davantage est connu comme durcissement de Windows. Les informations répertoriées ci-dessous peuvent être utilisées comme guide pour durcir vos serveurs avancés par console de réception de Cisco Unified.

Pare-feu et stratégies de groupe

Une fois que les Windows Server ont été ajoutés au domaine, des stratégies de groupe pourraient être poussées à Windows. Les stratégies et les stratégies de groupe de Pare-feu poussées au serveur CUACA ne devraient pas bloquer ou interrompre le fonctionnement des services et des ports suivants :

- Windows Management Instrumentation (WMI)
- Coordonnateur distribué de transaction (MDDTC) – seulement requis si utilisant la réplication/résilience SQL
- Le bus de message (MBUS) – ouvrez d'arrivée et les ports de sortie 61616 et 61618 (seulement requis si utilisant 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

Numéro de port	Utilisation
389	Le serveur LDAP n'utilise pas le SSL et n'est

	pas configuré comme catalogue global.
636	Le serveur LDAP utilise le SSL et n'est pas configuré comme catalogue global.
3268	Le serveur LDAP n'utilise pas le SSL et est configuré comme catalogue global.
3269	Le serveur LDAP utilise le SSL et est configuré comme catalogue global.

Référez-vous à la plus défunts gestion et guides d'installation avant l'implémentation pour valider la liste d'exclusions.

Logiciel antivirus

Installez un logiciel antivirus sur les Windows Server pour les maintenir sûrs du malware, des virus etc. Cependant, l'application d'antivirus ralentit la fonctionnalité de serveur CUACA pendant qu'elle a besoin de l'accès continu à peu de répertoires tandis que l'antivirus les balaye. Par conséquent on lui informe pour ajouter après des fichiers et dossiers comme exclusions sur le logiciel anti-virus :

Dossier par défaut	Contient
\ \ DBData	Bases de données de configuration système
\ \ fichiers de programme \ Cisco \	Fichiers de suivi de logiciel et d'application
\ \ Apache	Répertoire actif MQ
\ \ Temp \ Cisco \ suivi	Fichiers de suivi TSP de Cisco
\ \ %ALLUSERSPROFILE% \ Cisco \ CUACA	Cisco profilent

Ce sont des emplacements par défaut utilisés par l'installateur CUACA. Au cas où l'administrateur changerait l'emplacement de ces répertoires ou utilise quelques autres répertoires, des exclusions sur le besoin d'antivirus d'être changé en conséquence.

Référez-vous à la plus défunts gestion et guides d'installation avant l'implémentation pour valider la liste d'exclusions.

Désactiver le routage de la source IP

L'acheminement de source IP est rarement de nos jours utilisés cependant les pirates informatiques peut l'employer pour sauter le Pare-feu et par conséquent, des conseils de Cisco pour le désactiver.

Être suivent les étapes pour désactiver l'acheminement de source IP :

- Ouvrez Regedit
- Le positionnement ou créent ces valeurs :
  HKEY_LOCAL_MACHINE \ système \ CurrentControlSet \ services \ Tcpip \ paramètres \

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

Nom de valeur : DisableIPSourceRouting
Value type : REG_DWORD
Valeur : 2

- Clôturez Regedit.

Windows Update

Cisco informe pour maintenir des Windows Server corrigés avec plus défunt Microsoft Windows et des mises à jour et des Services Pack de Serveur SQL. Les mises à jour et l'automatique automatiques vérifie des mises à jour devraient être désactivés.

Des automatique-mises à jour de Javas ne sont pas prises en charge pendant qu'elles échouent parfois et ceci peut avoir comme conséquence le système inutilisable. Des mises à jour mineures sont prises en charge.

Tout vérifie des mises à jour et l'installation des mises à jour devrait être exécutée en dehors de la production. L'installation suivante redémarrent le SYSTÈME D'EXPLOITATION de serveur.

D'autres conditions requises durcissantes selon la stratégie de société

Les conseils de Cisco pour durcir des Windows Server selon la condition requise/stratégie cependant, administrateur doit s'assurer que toutes les exigences CUACA sont répondues après durcissement. Pour la connaissance détaillée sur des conditions requises CUACA, référez-vous au guide de conception CUACA et CUAC installent le guide.