Windows Server Hardening voor Cisco Unified Attendant Console Advanced Server

Inhoud

Overzicht
Firewallbeleid en groepsbeleid
Antivirussoftware
IP-brontrouting uitschakelen
Windows updates
Overige strengere eisen volgens het beleid van de onderneming

Overzicht

Dit document beschrijft een aantal configuratiewijzigingen die op een Cisco Unified Attendant Console Advanced-server (CUACA) kunnen worden aangebracht om de beveiliging ervan te verbeteren. Het proces om het Windows-systeem veiliger te maken, wordt Windows Verhardend genoemd. De onderstaande informatie kan als richtlijn worden gebruikt om uw Cisco Unified Attendant Console geavanceerde server(s) te verscherpen.

Firewallbeleid en groepsbeleid

Nadat de Windows server aan het domein is toegevoegd, kan het groepsbeleid naar Windows worden geduwd. Firewallbeleid en groepsbeleid op CUACA-server mogen de werking van de volgende services en poorten niet blokkeren of onderbreken:

- Windows Management Instrumentation (WMI)
- Distributed Transaction Coordinator (MDDTC) - alleen vereist als u SQL-replicatie/veerkracht gebruikt
- Berichtbus (MBUS) - open inkomende en uitgaande poorten 61616 en 61618 (alleen vereist als u SQL-replicatie/veerkracht gebruikt)
- exe - *bijvoorbeeld : C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Binn\sqlservr.exe*
- Poortnummers (gebruikt door CUAC):

Poortnummers	Poorttype
80	TCP
389	TCP
443	TCP
636	TCP
1433 en 1434	TCP
1859	TCP
1862	TCP
1863	TCP
1864	TCP
2748	TCP
5060	UDP
5061 en 5062	TCP
11859	TCP

61616	TCP
61618	TCP
49152 tot 65535	TCP
1025 tot 5000	TCP

Poortnummer	Gebruik
389	LDAP server gebruikt SSL niet en is niet ingesteld als de Global Catalog.
636	LDAP server gebruikt SSL en is niet ingesteld als de Global Catalog.
3268	LDAP server gebruikt SSL niet en is ingesteld als de Global Catalog.
3269	LDAP server gebruikt SSL en is ingesteld als de Global Catalog.

Raadpleeg de nieuwste beheers- en installatiehandleidingen voordat deze worden geïmplementeerd om de lijst met uitsluitingen te valideren.

Antivirussoftware

Installeer een anti-virussoftware op de Windows-server om deze te beveiligen tegen malware, virussen enz. Antivirus-toepassing vertraagt echter de CUACA server functionaliteit omdat het continue toegang tot een aantal mappen nodig heeft terwijl anti-virus ze scant. Daarom is het raadzaam de volgende bestanden en mappen toe te voegen als uitsluitingen van antivirussoftware:

Standaardmap	Bevat
\\DBData	Systeemconfiguratie-databases
\\Program Files\Cisco\	Software- en toepassingsspoorbestanden
\\Apache	Actieve MQ-map
\\Temp\Cisco\Trace	Cisco TSP-spoorbestanden
\%ALLUSERSPROFIEL%\Cisco\CUACA	Cisco-profiel

Dit zijn standaardlocaties die worden gebruikt door een CUACA-installateur. Indien de beheerder de locatie van deze mappen wijzigt of andere mappen gebruikt, dient de uitsluiting van het anti-virus dienovereenkomstig te worden gewijzigd.

Raadpleeg de nieuwste beheers- en installatiehandleidingen voordat deze worden geïmplementeerd om de lijst met uitsluitingen te valideren.

IP-brontrouting uitschakelen

IP Bron routing wordt tegenwoordig zelden gebruikt wanneer hackers het kunnen gebruiken om firewall te omzeilen en dus Cisco-services om het uit te schakelen.

Hieronder volgen de stappen om IP-brontrouting uit te schakelen:

- Regedit openen
- Stel deze waarden in of maak deze:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\

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

Naam waarde: Uitschakelen van IPSource-routing
Waarde type: REG_DWORD
Value: 2

- Sluit Regedit.

Windows updates

Cisco adviseert om Windows server gepatched te houden met de nieuwste Microsoft Windows en SQL Server updates en Service Packs. Automatische updates en automatische controles op updates moeten worden uitgeschakeld.

De automatische updates van Java worden niet ondersteund omdat ze soms falen en dit kan leiden tot onbruikbaar systeem. Kleine updates worden ondersteund.

Alle controles op updates en installatie van updates dienen buiten de productie te worden uitgevoerd. Na installatie start u het besturingssysteem van de server opnieuw op.

Overige strengere eisen volgens het beleid van de onderneming

De services van Cisco om Windows Server te onderbreken zoals vereist/beleid echter, moet de beheerder ervoor zorgen dat aan alle CUACA-vereisten wordt voldaan na het verharden. Raadpleeg de CUACA-handleiding voor uitgebreide informatie over de CUAC-vereisten en de CUAC-installatiehandleiding.