Protezione avanzata di Windows Server per Cisco Unified Attendant Console Advanced Server

Sommario

Panoramica

Questo documento descrive diverse modifiche alla configurazione che possono essere apportate su un server Cisco Unified Attendant Console Advanced (CUACA) per renderlo più sicuro. Il processo per rendere più sicuro il sistema Windows è noto come protezione avanzata di Windows. Le informazioni elencate di seguito possono essere utilizzate come guida per fortificare i server avanzati della console Cisco Unified Attendant.

Criteri firewall e di gruppo

Dopo aver aggiunto il server Windows al dominio, è possibile eseguire il push dei criteri di gruppo in Windows. I criteri firewall e i criteri di gruppo inviati al server CUACA non devono bloccare o interrompere il funzionamento dei servizi e delle porte seguenti:

- Strumentazione gestione Windows (WMI)
- Distributed Transaction Coordinator (MDTC) - obbligatorio solo se si utilizza la replica/resilienza SQL
- MBUS (Message Bus) - porte in entrata e in uscita aperte 61616 e 61618 (richiesto solo se si utilizza la replica/resilienza SQL)
- exe - *Ad esempio: C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Binn\sqlservr.exe*
- Numeri di porta (utilizzati da CUAC):

Numeri di porta	Tipo porta
80	TCP
389	TCP
443	TCP
636	TCP
1433 e 1434	TCP
1859	TCP
1862	TCP
1863	TCP
1864	TCP
2748	TCP
5060	UDP

5061 e 5062	TCP
11859	TCP
61616	TCP
61618	TCP
da 49152 a 65535	TCP
da 1025 a 5000	TCP

Numero porta	Utilizzo
389	Il server LDAP non utilizza SSL e non è configurato come catalogo globale.
636	Il server LDAP utilizza SSL e non è configurato come catalogo globale.
3268	Il server LDAP non utilizza SSL ed è configurato come catalogo globale.
3269	Il server LDAP utilizza SSL ed è configurato come catalogo globale.

Per convalidare l'elenco di esclusioni, consultare le Guide all'amministrazione e all'installazione più recenti prima dell'implementazione.

Software antivirus

Installare un software antivirus sul server Windows per proteggerlo da malware, virus e così via. Tuttavia, l'applicazione antivirus rallenta la funzionalità del server CUACA in quanto richiede l'accesso continuo a poche cartelle mentre l'antivirus le analizza. Si consiglia pertanto di aggiungere i seguenti file e cartelle come esclusioni dal software antivirus:

Cartella predefinita	Contiene
\\DBData	Database di configurazione del sistema
\\Programmi\Cisco\	File di traccia software e applicazioni
\\Apache	Cartella MQ attiva
\\Temp\Cisco\Trace	File di traccia Cisco TSP
\\%ALLUSERSPROFILE%\Cisco\CUACA	profilo Cisco

Si tratta delle posizioni predefinite utilizzate dal programma di installazione di CUACA. Nel caso in cui l'amministratore modifichi il percorso di queste cartelle o utilizzi altre cartelle, le esclusioni di antivirus devono essere modificate di conseguenza.

Per convalidare l'elenco di esclusioni, consultare le Guide all'amministrazione e all'installazione più recenti prima dell'implementazione.

Disabilita routing origine IP

Al giorno d'oggi il routing all'origine IP viene raramente utilizzato, ma gli hacker possono usarlo per ignorare il firewall e quindi, secondo i consigli di Cisco, per disabilitarlo.

Per disabilitare il routing dell'origine IP, effettuare le operazioni riportate di seguito.

- Apri Regedit

- Impostare o creare i valori seguenti:
  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\

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

  Nome valore: DisabilitaRoutingIPSource
  Tipo valore: REG_DWORD
  Valore: 2

- Chiudete Regedit.

Aggiornamenti di Windows

Cisco consiglia di installare patch per il server Windows con gli ultimi aggiornamenti di Microsoft Windows e SQL Server e i Service Pack. Gli aggiornamenti automatici e i controlli automatici per gli aggiornamenti devono essere disabilitati.

Gli aggiornamenti automatici Java non sono supportati poiché a volte si verificano errori e questo può rendere inutilizzabile il sistema. Sono supportati aggiornamenti di minore entità.

Tutti i controlli relativi agli aggiornamenti e all'installazione degli aggiornamenti devono essere eseguiti al di fuori della produzione. Dopo l'installazione, riavviare il sistema operativo del server.

Altri requisiti di protezione avanzata in base alla politica aziendale

Cisco consiglia di rafforzare Windows Server in base a requisiti/criteri. Tuttavia, l'amministratore deve accertarsi che tutti i requisiti CUACA siano soddisfatti dopo l'applicazione della protezione avanzata. Per informazioni dettagliate sui requisiti di CUACA, consultare la guida alla progettazione di CUACA e la guida all'installazione di CUAC.