Windows Server Hardening para Cisco Unified Attendant Console Advanced Server

Contents

Overview

Este documento descreve várias alterações de configuração que podem ser feitas em um servidor Cisco Unified Attendant Console Advanced (CUACA) para torná-lo mais seguro. O processo de tornar o sistema Windows mais seguro é conhecido como Windows Hardening. As informações listadas abaixo podem ser usadas como um guia para fortalecer os servidores avançados do console Cisco Unified Attendant.

Políticas de firewall e grupo

Depois que o servidor Windows tiver sido adicionado ao domínio, as políticas de grupo poderão ser enviadas para o Windows. As políticas de firewall e as políticas de grupo enviadas para o servidor CUACA não devem bloquear ou interromper o funcionamento dos seguintes serviços e portas:

- Windows Management Instrumentation (WMI)
- Coordenador de Transações Distribuídas (MDTC) - necessário somente se estiver usando replicação/resiliência SQL
- Barramento de Mensagens (MBUS - Message Bus) - portas de entrada e saída abertas 61616 e 61618 (necessário somente se estiver usando replicação/resiliência SQL)
- exe - *Por exemplo: C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Binn\sqlservr.exe*
- Números de porta (usados pelo CUAC):

Números da porta	Tipo de 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
49152 a 65535	TCP
1025 a 5000	TCP

número da porta	Uso
389	O servidor LDAP não usa SSL e não está configurado como o catálogo global.
636	O servidor LDAP usa SSL e não está configurado como o catálogo global.
3268	O servidor LDAP não usa SSL e está configurado como o catálogo global.
3269	O servidor LDAP usa SSL e é configurado como o Catálogo Global.

Consulte os Guias de Administração e Instalação mais recentes antes da implementação para validar a lista de exclusões.

Software antivírus

Instale um software antivírus no servidor Windows para mantê-lo protegido contra malware, vírus, etc. No entanto, o aplicativo antivírus retarda a funcionalidade do servidor CUACA, pois ele precisa de acesso contínuo a poucas pastas enquanto o antivírus os examina. Portanto, é aconselhável adicionar os seguintes arquivos e pastas como exclusões em softwares antivírus:

Pasta padrão	Contém
\\DBData	Bancos de dados de configuração do sistema
\\Programa Files\Cisco\	Arquivos de rastreamento de software e aplicativos
\\Apache	pasta MQ ativa
\\Temp\Cisco\Trace	Arquivos de rastreamento do Cisco TSP
\\%ALLUSERSPROFILE%\Cisco\CUACA	perfil da Cisco

Estes são os locais padrão usados pelo instalador do CUACA. Caso o administrador altere o local dessas pastas ou use outras pastas, as exclusões de antivírus precisam ser alteradas de acordo.

Consulte os Guias de Administração e Instalação mais recentes antes da implementação para validar a lista de exclusões.

Desabilite o roteamento do origem de IP

O roteamento de origem de IP raramente é usado atualmente, mas os hackers podem usá-lo para ignorar o firewall e, portanto, aconselhá-lo a desativá-lo.

A seguir estão as etapas para desativar o roteamento de origem IP:

- Abrir Regedit

- Defina ou crie estes valores:
  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\

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

  Nome do valor: DesativarRoteamentoOrigemIPS
  Tipo de valor: REG_DWORD
  Valor: 2

- Feche o Regedit.

Atualizações do Windows

A Cisco aconselha manter o servidor Windows corrigido com as atualizações mais recentes do Microsoft Windows e SQL Server e Service Packs. As atualizações automáticas e as verificações automáticas de atualizações devem ser desativadas.

As atualizações automáticas de Java não são suportadas porque, às vezes, elas falham e isso pode resultar em sistema inutilizável. Há suporte para pequenas atualizações.

Todas as verificações de atualizações e instalação de atualizações devem ser executadas fora da produção. Após a instalação, reinicie o SO do servidor.

Outros requisitos de proteção conforme a política da empresa

A Cisco aconselha a fortalecer o Windows Server de acordo com a exigência/política, no entanto, o administrador precisa certificar-se de que todos os requisitos do CUACA sejam atendidos após o fortalecimento. Para obter informações detalhadas sobre os requisitos do CUACA, consulte o guia CUACA Design e o guia CUAC Install.