Solucionar problemas do Umbrella Connector que bloqueia uma conta de serviço do Active Directory

Contents

[Introdução](#)

[Overview](#)

[Lista de contas bloqueadas](#)

[Mais informações](#)

Introdução

Este documento descreve como solucionar o motivo pelo qual uma Conta de Serviço do Active Directory está bloqueada pelo Umbrella Connector.

Overview

O serviço Umbrella Connector faz conexões WMI com os logs de eventos de qualquer DC (controlador de domínio) registrado que faça parte do mesmo [Site de Umbrella](#), para ler informações de eventos de logon. Esses eventos de logon são analisados e carregados em todos os Virtual Appliances (VAs) no mesmo Umbrella Site. Em seguida, o VA cria um mapeamento de usuário para IP temporário para esse nome de usuário/endereço IP de origem. Há alguns pontos que valem a pena observar:

- O Umbrella Insights pode suportar apenas um usuário conectado por IP por vez
- O evento de logon processado mais recentemente de um IP de origem 'wins'

Como todos os eventos de logon são iguais, o conector tem uma lista codificada de contas de serviço comuns do AD cujos eventos são ignorados. Você pode ver eventos de logon dessas contas selecionados no arquivo de log do conector. Por exemplo:

Evento do usuário na lista negra ignorado: OpenDNS_Connector

Isso é feito para evitar que as contas de serviço (que, da mesma forma que os usuários padrão geram eventos de logon nos logs de eventos de segurança de DC) substituam o mapeamento de Usuário para IP do usuário realmente conectado.

Em ambientes grandes, dependendo do processo/aplicativo para o qual uma conta de serviço é usada, eles também podem gerar milhares de eventos de logon a cada minuto. Essa também é uma carga adicional para o conector, que pode se manifestar como um atraso entre o logon do usuário e a política correta que está sendo aplicada, ou uma política correta aplicada que é perdida posteriormente.

Lista de contas bloqueadas

- _usuário_vmware_
- Administrador
- ANÔNIMO
- Logon Anônimo
- ASPNET
- Serviço local
- McAfeeMVSUser
- MHControl
- Serviço de rede
- netwrite
- OpenDNS_Connector
- peersyncsvc
- s-pcadmin
- SophosUpdateMgr
- SophosUpdMgr
- svc-altiris
- svc.iCreate

Mais informações

Você também pode excluir qualquer outro evento de logon de conta do AD do processamento pelo conector. Consulte este artigo para obter instruções:

<https://support.umbrella.com/hc/en-us/articles/231266088>

Além disso, há grupos do AD que podem ser excluídos da Sincronização do AD do conector, que é executada para popular a área de política do Painel com uma lista de usuários, computadores e grupos do AD. Isso pode ser encontrado aqui:

<https://support.umbrella.com/hc/en-us/articles/115005206526>

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.