Entender Eventos de Janela/EventIDs Lidos por um Conector

Contents

Introdução

Este documento descreve quais eventos de janela/IDs de evento são lidos por um conector por padrão.

Overview

Tecnicamente, o Umbrella Virtual Appliance (VA) só tem visibilidade do endereço IP de origem do qual recebe uma consulta DNS. Para que um usuário seja associado à solicitação DNS, o VA trabalha em conjunto com o conector, o que resulta em um mapeamento de usuário para IP.

O conector lê eventos com IDs de evento específicas dos Logs de eventos de segurança nos controladores de domínio. Esses eventos são analisados e o nome de usuário e o endereço IP de origem são enviados para o VA, que cria um mapeamento entre esse IP de origem e o usuário.

Se esses eventos não estiverem sendo auditados pelos controladores de domínio, o processo de mapeamento de VAs não poderá ocorrer corretamente. Este artigo descreve exatamente que tipo de IDs de evento o conector observa por padrão.

ID do Evento	Descrição
4624	O evento 4624 documenta toda e qualquer tentativa bem-sucedida de fazer logon no computador local, independentemente do tipo de logon, local do usuário ou tipo de conta.
528	O evento 528 é registrado sempre que uma conta se conecta ao computador local, exceto no caso de logons de rede. O evento 528 será registrado se a conta usada para logon for uma conta SAM local ou uma conta de domínio.
540	O evento 540 é registrado quando um usuário em qualquer lugar da rede se conecta a um recurso (como uma pasta compartilhada) fornecido pelo serviço

	Servidor neste computador.
4768	Este evento está conectado somente aos controladores de domínio e as instâncias de êxito e falha deste evento estão registradas.
4769	O Windows usa essa ID de evento para solicitações de tíquete de serviço bem-sucedidas e com falha.

Se o seu conector não puder ler eventos diretamente dos Logs de Eventos de Segurança do controlador de domínio, você poderá emitir um tíquete de suporte com o Umbrella solicitando que isso seja alterado para a assinatura WMI. No caso de assinaturas WMI, o conector se inscreve em todos os eventos listados acima. Além disso, o conector também se inscreve para eventos de logoff com EventIDs, conforme mencionado abaixo. Observe que, por padrão, o conector não lê esses eventos de logoff dos Logs de eventos de segurança.

ID do Evento	Descrição
538	O evento 538 é registrado sempre que um usuário faz logoff, seja de uma conexão de rede, logon interativo ou outro tipo de logon (consulte o evento 528 para obter um gráfico dos tipos de logon).
4647	Esse evento sinaliza o término de uma sessão de logon e pode ser correlacionado ao evento de logon 4624 usando a ID de logon.
4634	Esse evento também sinaliza o término de uma sessão de logon e pode ser correlacionado ao evento de logon 4624 usando a ID de logon.

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.