Comprendre les événements/ID d'événement de fenêtre lus par un connecteur

Table des matières

Introduction

Ce document décrit les événements/ID d'événement de fenêtre lus par un connecteur par défaut.

Aperçu

Techniquement, l'appliance virtuelle Umbrella ne dispose que d'une visibilité sur l'adresse IP source à partir de laquelle elle reçoit une requête DNS. Afin qu'un utilisateur soit associé à la requête DNS, l'AV fonctionne en conjonction avec le connecteur, ce qui entraîne un mappage d'utilisateur à IP.

Le connecteur lit les événements avec des ID d'événements spécifiques à partir des journaux des événements de sécurité sur vos contrôleurs de domaine. Ces événements sont ensuite analysés et le nom d'utilisateur et l'adresse IP source sont envoyés à l'AV, qui crée alors un mappage entre cette adresse IP source et cet utilisateur.

Si ces événements ne sont pas audités par vos contrôleurs de domaine, le processus de mappage des VA ne peut pas se dérouler correctement. Cet article décrit exactement quel type d'ID d'événement le connecteur surveille par défaut.

EventID	Description
4624	L'événement 4624 documente chaque tentative réussie de connexion à l'ordinateur local, quel que soit le type de connexion, l'emplacement de l'utilisateur ou le type de compte.
528	L'événement 528 est consigné chaque fois qu'un compte se connecte à l'ordinateur local, sauf en cas de connexions réseau. L'événement 528 est consigné, que le compte utilisé pour la connexion soit un compte SAM local ou un compte de domaine.
540	L'événement 540 est consigné lorsqu'un utilisateur situé ailleurs sur le réseau se

	connecte à une ressource (telle qu'un dossier partagé) fournie par le service Serveur sur cet ordinateur.
4768	Cet événement est enregistré uniquement sur les contrôleurs de domaine et les instances de réussite et d'échec de cet événement sont enregistrées.
4769	Windows utilise cet ID d'événement pour les demandes de ticket de service réussies et en échec.

Si votre connecteur ne parvient pas à lire les événements directement à partir des journaux d'événements de sécurité du contrôleur de domaine, vous pouvez créer un ticket d'assistance avec Umbrella demandant que ce ticket soit remplacé par un abonnement WMI. Dans le cas d'abonnements WMI, le connecteur s'abonne à tous les événements répertoriés ci-dessus. En outre, le connecteur s'abonne également aux événements de fermeture de session avec des ID d'événement comme indiqué ci-dessous. Notez que par défaut, le connecteur ne lit pas ces événements de déconnexion à partir des journaux des événements de sécurité.

EventID	Description
538	L'événement 538 est consigné chaque fois qu'un utilisateur se déconnecte, que ce soit à partir d'une connexion réseau, d'une ouverture de session interactive ou d'un autre type d'ouverture de session (voir l'événement 528 pour un tableau des types d'ouverture de session).
4647	Cet événement signale la fin d'une session d'ouverture de session et peut être mis en corrélation avec l'événement d'ouverture de session 4624 à l'aide de l'ID d'ouverture de session.
4634	Cet événement signale également la fin d'une session d'ouverture de session et peut être mis en corrélation avec l'événement d'ouverture de session 4624 à l'aide de l'ID d'ouverture de session.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.