Von einem Connector gelesene Fensterereignisse/Ereignis-IDs verstehen

Inhalt

Einleitung

In diesem Dokument wird beschrieben, welche Fensterereignisse/Ereignis-IDs standardmäßig von einem Connector gelesen werden.

Überblick

Die Umbrella Virtual Appliance (VA) hat technisch gesehen nur eine Übersicht darüber, von welcher Quell-IP-Adresse sie eine DNS-Abfrage empfängt. Damit ein Benutzer der DNS-Anforderung zugeordnet werden kann, arbeitet die VA mit dem Connector zusammen, wodurch eine Zuordnung von Benutzer zu IP erfolgt.

Der Connector liest Ereignisse mit bestimmten Ereignis-IDs aus den Sicherheitsereignisprotokollen auf den Domänencontrollern. Diese Ereignisse werden analysiert, und der Benutzername sowie die Quell-IP-Adresse werden an die VA gesendet, die dann eine Zuordnung zwischen der Quell-IP und dem Benutzer erstellt.

Wenn diese Ereignisse nicht von Ihren Domänencontrollern überprüft werden, kann die VAs-Zuordnung nicht ordnungsgemäß durchgeführt werden. In diesem Artikel wird genau umrissen, auf welche Art von Ereignis-IDs der Connector standardmäßig achtet.

Ereignis-ID	Beschreibung
4624	Ereignis 4624 dokumentiert jeden erfolgreichen Versuch, sich am lokalen Computer anzumelden, unabhängig von Anmeldetyp, Standort des Benutzers oder Kontoart.
528	Ereignis 528 wird protokolliert, wenn sich ein Konto beim lokalen Computer anmeldet, außer bei Netzwerkanmeldungen. Ereignis 528 wird protokolliert, unabhängig davon, ob es sich bei dem für die Anmeldung verwendeten Konto um ein lokales SAM-Konto oder ein Domänenkonto handelt.

540	Ereignis 540 wird protokolliert, wenn ein Benutzer an einer anderen Stelle im Netzwerk eine Verbindung mit einer Ressource herstellt (z. B. einem freigegebenen Ordner), die vom Serverdienst auf diesem Computer bereitgestellt wird.
4768	Dieses Ereignis wird nur auf Domänencontrollern protokolliert, und sowohl Erfolgs- als auch Fehlerinstanzen dieses Ereignisses werden protokolliert.
4769	Windows verwendet diese Ereignis-ID sowohl für erfolgreiche als auch für fehlgeschlagene Service-Ticket-Anfragen.

Wenn Ihr Connector Ereignisse nicht direkt aus den Sicherheitsereignisprotokollen des Domänencontrollers lesen kann, können Sie ein Support-Ticket mit Umbrella erstellen, in dem Sie darum bitten, dieses in ein WMI-Abonnement zu ändern. Im Fall von WMI-Abonnements werden vom Connector alle oben aufgeführten Ereignisse abonniert. Darüber hinaus abonniert der Connector auch Abmeldeereignisse mit EventIDs, wie unten beschrieben. Beachten Sie, dass der Connector diese Abmeldeereignisse standardmäßig nicht aus den Sicherheitsereignisprotokollen liest.

Ereignis-ID	Beschreibung
538	Ereignis 538 wird protokolliert, wenn sich ein Benutzer abmeldet, sei es über eine Netzwerkverbindung, eine interaktive Anmeldung oder einen anderen Anmeldetyp (eine Übersicht der Anmeldetypen finden Sie unter Ereignis 528).
4647	Dieses Ereignis signalisiert das Ende einer Anmeldesitzung und kann mithilfe der Anmelde-ID mit dem Anmeldeereignis 4624 korreliert werden.
4634	Dieses Ereignis signalisiert auch das Ende einer Anmeldesitzung und kann mithilfe der Anmelde-ID mit dem Anmeldeereignis 4624 korreliert werden.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.