Fehlerbehebung: Umbrella Connector blockiert ein Active Directory-Dienstkonto

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie die Ursache dafür finden, dass ein Active Directory-Dienstkonto vom Umbrella Connector blockiert wird.

Überblick

Der Umbrella Connector-Dienst stellt WMI-Verbindungen zu den Ereignisprotokollen aller registrierten Domänencontroller (DC) her, die Teil desselben Umbrella-Standorts sind, um Anmeldeinformationen zu lesen. Diese Anmeldeereignisse werden analysiert und an alle virtuellen Appliances (VAs) am gleichen Umbrella-Standort hochgeladen. Die VA erstellt dann eine temporäre Benutzer-zu-IP-Zuordnung für diesen Benutzernamen/diese Quell-IP-Adresse. Es gibt einige Punkte, die erwähnenswert sind:

- Umbrella Insights kann jeweils nur einen angemeldeten Benutzer pro IP unterstützen.
- Das zuletzt verarbeitete Anmeldeereignis einer Quell-IP gewinnt

Da alle Anmeldeereignisse gleich sind, verfügt der Connector über eine hartcodierte Liste mit allgemeinen AD-Dienstkonten, deren Ereignisse ignoriert werden. In der Connector-Protokolldatei können Sie die Anmeldeereignisse dieser Konten sehen. Beispiele:

Ereignis von Benutzer auf Blacklist ignoriert: OpenDNS-Connector

Auf diese Weise wird verhindert, dass Dienstkonten (die wie Standardbenutzer Anmeldeereignisse in den Ereignisprotokollen der Sicherheitssicherheit des Rechenzentrums generieren) die Zuordnung von Benutzer zu IP des tatsächlich angemeldeten Benutzers überschreiben.

In großen Umgebungen können sie je nach Prozess/Anwendung, für die ein Dienstkonto verwendet wird, auch Tausende von Anmeldeereignissen pro Minute generieren. Dies ist auch eine zusätzliche Last für den Connector, die sich als Verzögerung zwischen der Benutzeranmeldung und der Anwendung der richtigen Richtlinie oder als korrekte, später verlorene Richtlinie manifestieren kann.

Liste der gesperrten Konten

- _vmware_user_
- Administrator
- ANONYM
- Anonyme Anmeldung
- ASPNET
- Lokaler Dienst
- McAfeeMVSUser
- MHControl
- Netzwerkservice
- Netzwerkanschluss
- OpenDNS-Connector
- peersyncsvc
- s-pcadmin
- SophosUpdateManager
- SophosUpdManager
- SVC-Altiris
- svc.iErstellen

Weitere Informationen

Sie können auch alle anderen Anmeldeereignisse des AD-Kontos von der Verarbeitung durch den Connector ausschließen. Anweisungen hierzu finden Sie in diesem Artikel:

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

Darüber hinaus gibt es AD-Gruppen, die von der AD-Synchronisierung des Connectors ausgeschlossen werden können. Diese Synchronisierung wird durchgeführt, um eine Liste von AD-Benutzern, -Computern und -Gruppen im Dashboard-Richtlinienbereich zu erstellen. Diese finden Sie hier:

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

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.