Risoluzione dei problemi relativi al blocco di un account del servizio Active Directory da parte di Umbrella Connector

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi relativi al blocco di un account del servizio Active Directory da parte di Umbrella Connector.

Panoramica

Il servizio Umbrella Connector consente di stabilire connessioni WMI ai registri eventi di qualsiasi controller di dominio registrato appartenente allo stesso sito Umbrella, al fine di leggere le informazioni sugli eventi di accesso. Questi eventi di accesso vengono quindi analizzati e caricati in tutte le appliance virtuali (VA) nello stesso sito Umbrella. La VA crea quindi un mapping utente-IP temporaneo per il nome utente/indirizzo IP di origine. Vi sono due punti che meritano di essere sottolineati:

- Umbrella Insights può supportare solo un utente connesso per IP alla volta
- Evento di accesso elaborato più di recente da un indirizzo IP di origine 'wins'

Poiché tutti gli eventi di accesso sono uguali, il connettore dispone di un elenco hardcoded di account di servizio Active Directory comuni i cui eventi vengono ignorati. È possibile visualizzare gli eventi di accesso di questi account selezionati nel file di registro del connettore. Ad esempio:

Evento da utente in blacklist ignorato: ApriConnettore_DNS

In questo modo si impedisce agli account di servizio, che come gli utenti standard generano eventi di accesso nei registri eventi di protezione del controller di dominio, di ignorare il mapping da utente a IP dell'utente effettivamente connesso.

In ambienti di grandi dimensioni, a seconda del processo/applicazione per cui viene utilizzato un account di servizio, possono inoltre generare migliaia di eventi di accesso al minuto. Si tratta inoltre di un carico aggiuntivo per il connettore, che può manifestarsi come un ritardo tra l'accesso dell'utente e l'applicazione del criterio corretto o un criterio corretto che viene successivamente perso.

Elenco di account bloccati

- _vmware_user_
- Amministratore
- ANONIMO
- Accesso anonimo
- ASPNET
- Servizio locale
- McAfeeMVSUser
- MHControl
- Servizio di rete
- netwrix
- ApriConnettore_DNS
- persyncsvc
- s-pcadmin
- SophosUpdateMgr
- SophosUpdMgr
- svc-altiris
- svc.iCreate

Ulteriori informazioni

È inoltre possibile escludere qualsiasi altro evento di accesso dell'account AD dall'elaborazione da parte del connettore. Per istruzioni, vedere questo articolo:

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

Esistono inoltre gruppi AD che possono essere esclusi dalla sincronizzazione AD del connettore, che viene eseguita per popolare l'area dei criteri del dashboard con un elenco di utenti, computer e gruppi AD. È possibile trovare qui:

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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).