Informazioni sugli eventi/ID evento di Windows letti da un connettore

Sommario

Introduzione

In questo documento vengono descritti gli eventi e gli ID evento che vengono letti da un connettore per impostazione predefinita.

Panoramica

Tecnicamente, Umbrella Virtual Appliance (VA) ha solo la visibilità dell'indirizzo IP di origine da cui riceve una query DNS. Affinché un utente venga associato alla richiesta DNS, VA opera insieme al connettore che determina l'esecuzione di un mapping da utente a IP.

Il connettore legge gli eventi con ID specifici dai registri eventi di protezione nei controller di dominio. Questi eventi vengono quindi analizzati e il nome utente e l'indirizzo IP di origine vengono inviati all'amministratore di sistema, che crea quindi un mapping tra l'IP di origine e l'utente.

Se questi eventi non vengono controllati dai controller di dominio, il processo di mapping dei VA non può essere eseguito correttamente. In questo articolo viene descritto esattamente il tipo di ID di evento che il connettore cerca per impostazione predefinita.

IDEvento	Descrizione
4624	L'evento 4624 documenta ogni tentativo riuscito di accedere al computer locale, indipendentemente dal tipo di accesso, dalla posizione dell'utente o dal tipo di account.
528	L'evento 528 viene registrato ogni volta che un account accede al computer locale, tranne nel caso di accessi alla rete. L'evento 528 viene registrato sia che l'account utilizzato per l'accesso sia un account SAM locale o un account di dominio.
540	L'evento 540 viene registrato quando un utente in un altro punto della rete si connette a una risorsa, ad esempio una cartella condivisa, fornita dal servizio

	Server nel computer.
4768	Questo evento viene registrato solo nei controller di dominio e vengono registrate sia le istanze riuscite che quelle non riuscite di questo evento.
4769	Questo ID evento viene utilizzato sia per le richieste di ticket di servizio riuscite che per quelle non riuscite.

Se il connettore non è in grado di leggere gli eventi direttamente dai registri eventi protezione del controller di dominio, è possibile generare un ticket di supporto con Umbrella che richiede la modifica in sottoscrizione WMI. Nel caso di sottoscrizioni WMI, il connettore sottoscrive tutti gli eventi elencati in precedenza. Inoltre, il connettore sottoscrive anche eventi di disconnessione con EventID, come indicato di seguito. Si noti che, per impostazione predefinita, il connettore non legge questi eventi di disconnessione dai registri eventi protezione.

IDEvento	Descrizione
538	L'evento 538 viene registrato ogni volta che un utente si disconnette, da una connessione di rete, da un accesso interattivo o da un altro tipo di accesso (vedere l'evento 528 per un grafico dei tipi di accesso).
4647	Questo evento segnala la fine di una sessione di accesso e può essere correlato all'evento di accesso 4624 utilizzando l'ID di accesso.
4634	Questo evento segnala anche la fine di una sessione di accesso e può essere correlato all'evento di accesso 4624 utilizzando l'ID di accesso.

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).