

Comprendere la selezione dei criteri Umbrella che coinvolge più organizzazioni

Sommario

[Introduzione](#)

[Panoramica](#)

[Selezione dei criteri con una singola organizzazione](#)

[Selezione criteri con più organizzazioni](#)

[Creazione di rapporti con più organizzazioni](#)

[Implicazioni per il comportamento di selezione dei criteri corrente](#)

[Pagine a blocchi dedicate per scenari che coinvolgono più organizzazioni](#)

[Modifiche pianificate per la selezione dei criteri che interessano più organizzazioni](#)

[Comportamento selezione criteri](#)

[Creazione di rapporti per tutte le organizzazioni coinvolte](#)

Introduzione

Questo documento descrive le politiche di più organizzazioni Umbrella prese in considerazione in alcuni scenari.

Panoramica

In alcuni scenari, è possibile prendere in considerazione le politiche di più organizzazioni Umbrella. Ad esempio, un client o un dispositivo mobile in roaming per un'organizzazione che si connette alla rete di un'altra organizzazione. Questo articolo spiega come la politica sia attualmente scelta in questo caso, e quali cambiamenti Umbrella intende fare per migliorare questo comportamento.

Selezione dei criteri con una singola organizzazione

Quando una query DNS viene inviata a Umbrella, è possibile associare più identità alla query. Ad esempio, una query di un client di roaming (RC) dietro una rete protetta includerebbe sia l'ID dispositivo della RC che l'indirizzo IP della rete. Analogamente, una query da un'appliance virtuale include l'ID sito, la rete interna, l'utente AD e il gruppo AD.

In genere, le identità incluse nella query sono tutte associate a una singola organizzazione. In questo caso, la regola applicata utilizza le regole di precedenza illustrate nella documentazione:

<https://docs.umbrella.com/deployment-umbrella/docs/policy-precedence>

In breve, Umbrella assegna a ogni criterio una priorità in base al suo ordine nel Dashboard , con il

criterio di livello superiore che ha la priorità più alta. I resolver Umbrella scelgono il criterio di priorità più alta che si applica ad almeno una delle identità presenti nella query.

Ad esempio, per l'organizzazione A possono essere definiti i seguenti criteri:

Subscription Properties - Login Events

Subscription name: Login Events

Description:

Destination log: Forwarded Events

Subscription type and source computers

Collector initiated Select Computers...
This computer contacts the selected source computers and provides the subscription.

Source computer initiated Select Computer Groups...
Source computers in the selected groups must be configured through policy or local configuration to contact this computer and receive the subscription.

Events to collect: Select Events...

User account (the selected account must have read access to the source logs):
Machine Account

Change user account or configure advanced settings: Advanced...

OK Cancel

mceclip0.png

Il criterio del computer in roaming ha priorità 2, mentre il criterio della rete ha priorità 1. Pertanto, se una query proviene da un computer in roaming che è collegato a una rete esterna, verrà applicato il criterio 2. Tuttavia, se il computer in roaming fosse collegato a una delle reti dell'organizzazione A, si applicherebbe il criterio 1, in quanto il criterio della rete ha una priorità più alta.

Selezione criteri con più organizzazioni

La stessa logica viene applicata quando nella query sono incluse identità provenienti da più organizzazioni. Tuttavia, poiché vi sono più organizzazioni coinvolte, è la priorità relativa di ogni politica che viene considerata rispetto all'elenco di politiche di ogni organizzazione.

Un esempio spiega meglio questo. L'organizzazione A e l'organizzazione B dispongono ognuna di questi criteri definiti nei rispettivi pannelli di controllo Umbrella:

- **Minimize Latency**
 - Makes sure that events are delivered by having minimal delay.
 - The appropriate choice if you collect alerts or critical events.
 - Uses push delivery mode, and sets a batch time-out of 30 seconds.

mceclip2.png

Un computer in roaming dell'organizzazione A viene quindi aggiunto a una rete appartenente all'organizzazione B. La query DNS inviata a Umbrella contiene quindi l'ID del dispositivo dell'organizzazione A e l'indirizzo IP della rete dell'organizzazione B.

Utilizzando la logica di una singola organizzazione, otteniamo le priorità per ogni politica di identità. Alla RC dell'organizzazione A viene assegnato il criterio A2, con priorità 2, mentre alla rete dell'organizzazione B viene assegnato il criterio B1, con priorità 1. Viene quindi applicato il criterio B1, relativo alla rete dell'organizzazione B.

Creazione di rapporti con più organizzazioni

Quando una query contiene identità provenienti da più organizzazioni, viene visualizzata solo nei report relativi all'organizzazione per la quale è stato selezionato il criterio. I rapporti per tale organizzazione mostrano SOLO le identità appartenenti a tale organizzazione. Un'organizzazione NON ha MAI la visibilità sulle altre identità della query che appartengono ad altre organizzazioni.

Implicazioni per il comportamento di selezione dei criteri corrente

A causa del comportamento di selezione dei criteri descritto, è possibile che i criteri di un'identità appartenente a un'organizzazione possano essere sostituiti dai criteri di un'altra organizzazione. Sono incluse tutte le funzionalità dei criteri, tra cui la protezione e il blocco del contenuto, gli elenchi di destinazione, la progettazione di pagine di blocco e le impostazioni di registrazione (con l'indicazione delle restrizioni relative alla creazione di report), ad eccezione dei reindirizzamenti delle pagine di blocco.

Pagine a blocchi dedicate per scenari che coinvolgono più organizzazioni

A partire dal 16 luglio 2021, quando i resolver Umbrella rilevano che una query contiene identità di più organizzazioni, reindirizza tutte le query bloccate a una pagina blocco dedicata. Questa pagina di blocco informa l'utente che sono state rilevate più organizzazioni e che pertanto la query potrebbe essere stata bloccata a causa dei criteri di un'altra organizzazione.

Modifiche pianificate per la selezione dei criteri che interessano

più organizzazioni

Umbrella prevede di modificare il comportamento della selezione dei criteri quando è coinvolta più di un'organizzazione. Le modifiche future includono:

Comportamento selezione criteri

Umbrella modifica il comportamento di selezione dei criteri in modo che venga selezionato e applicato il criterio con la priorità più alta per ogni organizzazione. Se uno di questi criteri blocca la query, la query viene bloccata. Ciò consente a tutte le organizzazioni coinvolte di garantire che le proprie policy non vengano ignorate. Questo comportamento può essere spiegato meglio usando un'analogia:

I genitori di Alice dicono che le sue regole individuali sono più importanti delle regole della casa. Ad Alice non è permesso mangiare il gelato, in qualsiasi momento e da nessuna parte.

I genitori di Bob dicono che le regole della casa sono più importanti delle regole individuali. Non permettono mai la pizza in casa loro.

Modello corrente:

Alice va a casa di Bob. Si applicano le regole di casa di Bob e non le regole individuali di Alice. Alice sa mangiare il gelato, ma non la pizza. I genitori di Bob ricevono un rapporto che dice che qualcuno ha mangiato del gelato in casa, ma non dice che si trattasse di Alice per nome.

Modello proposto:

Alice va a casa di Bob. Si applicano le regole di casa di Bob e le regole individuali di Alice. Alice non ha né gelato né pizza. I genitori di Bob ricevono un rapporto che dice che a qualcuno è stata negata la pizza e il gelato, ma non dice che si trattasse di Alice per nome.

Creazione di rapporti per tutte le organizzazioni coinvolte

Quando è in atto il comportamento di selezione dei criteri, Umbrella garantisce inoltre che qualsiasi query che coinvolga identità provenienti da più organizzazioni sia inclusa nei report di tutte le organizzazioni coinvolte. I rapporti includono SOLO le identità appartenenti a tale organizzazione - una determinata organizzazione non vede mai le identità di un'altra organizzazione.

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).