

Begrijp overkoepelende beleidsselectie waarbij meerdere organisaties betrokken zijn

Inhoud

[Inleiding](#)

[Overzicht](#)

[Beleidsselectie met één organisatie](#)

[Beleidsselectie met meerdere organisaties](#)

[Rapporteren met meerdere organisaties](#)

[Implicaties voor het huidige beleidsselectiegedrag](#)

[Speciale blokpagina's voor scenario's waarbij meerdere organisaties betrokken zijn](#)

[Geplande wijzigingen voor beleidsselectie waarbij meerdere organisaties betrokken zijn](#)

[Beleidsselectiegedrag](#)

[Rapportage voor alle betrokken organisaties](#)

Inleiding

Dit document beschrijft het beleid van meerdere overkoepelende organisaties die in bepaalde scenario's worden overwogen.

Overzicht

In bepaalde scenario's is het mogelijk om het beleid van meerdere Umbrella organisaties in overweging te nemen. Een voorbeeld hiervan is een roamingclient of mobiel apparaat voor één organisatie die verbinding maakt met het netwerk van een andere organisatie. In dit artikel wordt beschreven hoe het beleid momenteel in dit geval wordt gekozen en welke wijzigingen Umbrella van plan is aan te brengen om dit gedrag te verbeteren.

Beleidsselectie met één organisatie

Wanneer een DNS-query naar Umbrella wordt verzonden, is het mogelijk om meerdere identiteiten aan de query te koppelen. Een zoekopdracht van een roamingclient (RC) achter een beveiligd netwerk bevat bijvoorbeeld zowel de apparaat-ID van de RC als het IP-adres van het netwerk. Evenzo bevat een query van een virtueel toestel de site-ID, het interne netwerk, de AD-gebruiker en de AD-groep.

De identiteiten die in de query zijn opgenomen, zijn doorgaans allemaal gekoppeld aan één organisatie. In dit geval maakt het beleid dat wordt afgedwongen gebruik van de regels voor beleidsprioriteit die in onze documentatie zijn beschreven:

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

Kortom, Umbrella kent elk beleid een prioriteit toe op basis van zijn volgorde in het Dashboard, waarbij het hoogste beleid de hoogste prioriteit heeft. De overkoepelende oplossers kiezen het beleid met de hoogste prioriteit dat van toepassing is op ten minste één van de identiteiten in de zoekopdracht.

Organisatie A kan bijvoorbeeld het volgende beleid hebben gedefinieerd:

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

Het beleid van de roamingcomputer heeft een prioriteit van 2, terwijl het beleid van het netwerk een prioriteit van 1 heeft. Dus als een query binnenkomt van een zwervende computer die is aangesloten op een extern netwerk, wordt beleid 2 toegepast. Als de roamingcomputer echter is aangesloten op een van de netwerken van organisatie A, is beleid 1 van toepassing, omdat het beleid van het netwerk een hogere prioriteit heeft.

Beleidsselectie met meerdere organisaties

Dezelfde logica wordt toegepast wanneer er identiteiten van meerdere organisaties in de query zijn opgenomen. Omdat er echter meerdere organisaties bij betrokken zijn, is het de relatieve prioriteit van elk beleid dat wordt overwogen met betrekking tot de beleidslijst van elke organisatie.

Een voorbeeld verklaart dit het best. Organisatie A en Organisatie B hebben elk deze beleidsregels gedefinieerd in hun respectieve overkoepelende dashboards:

- **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

Een zwervende computer van organisatie A sluit zich vervolgens aan bij een netwerk dat behoort tot organisatie B. De DNS-query die naar Umbrella wordt verzonden, bevat dus het apparaat-ID van de organisatie A, en het IP-adres van het netwerk van organisatie B.

Met behulp van de logica voor een enkele organisatie krijgen we de prioriteiten voor het beleid van elke identiteit. De RC van Organisatie A krijgt beleid A2, dat een prioriteit van 2 heeft, terwijl het Netwerk van Organisatie B beleid B1 krijgt, dat een prioriteit van 1 heeft. Zo wordt het beleid voor het netwerk van organisatie B, beleid B1, toegepast.

Rapporteren met meerdere organisaties

Wanneer een query identiteiten van meerdere organisaties bevat, wordt de query alleen weergegeven in de rapporten voor de organisatie waarvan het beleid is geselecteerd. De rapporten voor die organisatie tonen ALLEEN de identiteiten die tot die organisatie behoren. Een organisatie heeft NOOIT zicht op de andere identiteiten in de query die bij andere organisaties horen.

Implicaties voor het huidige beleidsselectiegedrag

Door het beschreven beleidsselectiegedrag is het mogelijk dat een identiteit die bij een organisatie hoort, door het beleid van een andere organisatie wordt overschreven. Dit omvat alle beleidsfuncties, waaronder beveiliging en het blokkeren van inhoud, bestemmingslijsten, ontwerpen van blokpagina's en logboekinstellingen (met vermelding van de beperkingen op rapportage), met uitzondering van omleidingen van blokpagina's.

Speciale blokpagina's voor scenario's waarbij meerdere organisaties betrokken zijn

Vanaf 16 juli 2021, wanneer de Umbrella resolvers detecteren dat een zoekopdracht identiteiten van meerdere organisaties bevat, worden geblokkeerde zoekopdrachten omgeleid naar een speciale blokpagina. Deze blokkeerpagina informeert de gebruiker dat meer dan één organisatie

is gedetecteerd en dat de zoekopdracht dus mogelijk is geblokkeerd vanwege het beleid van een andere organisatie.

Geplande wijzigingen voor beleidsselectie waarbij meerdere organisaties betrokken zijn

Paraplu plannen over het veranderen van het gedrag van beleidsselectie wanneer meer dan één organisatie betrokken is. Toekomstige veranderingen zijn onder meer:

Beleidsselectiegedrag

Umbrella wijzigt het beleidsselectiegedrag zodat het beleid met de hoogste prioriteit voor elke organisatie wordt geselecteerd en gehandhaafd. Als een van deze beleidsregels de zoekopdracht blokkeert, wordt de zoekopdracht geblokkeerd. Hierdoor kunnen alle betrokken organisaties ervoor zorgen dat hun beleid niet wordt omzeild. Dit gedrag kan het best worden verklaard met behulp van een analogie:

De ouders van Alice zeggen dat haar individuele regels belangrijker zijn dan huisregels. Alice mag geen ijs eten, waar en wanneer dan ook.

Bob's ouders zeggen dat huisregels belangrijker zijn dan individuele regels. Ze laten geen pizza in hun huis toe, nooit.

Huidig model:

Alice gaat naar het huis van Bob. De huisregels van Bob zijn van toepassing en niet de individuele regels van Alice. Alice kan ijs eten, maar geen pizza. Bob's ouders krijgen een rapport dat zegt dat iemand een ijsje at in hun huis, maar het zegt niet dat het Alice bij naam was.

Voorgesteld model:

Alice gaat naar het huis van Bob. Bob's huisregels zijn van toepassing, en Alice's individuele regels zijn van toepassing. Alice heeft geen ijs of pizza. Bob's ouders krijgen een rapport dat zegt dat iemand pizza en ijs werd geweigerd, maar het zegt niet dat het Alice bij naam was.

Rapportage voor alle betrokken organisaties

Wanneer het beleidsselectiegedrag aanwezig is, zorgt Umbrella er bovendien voor dat alle vragen met betrekking tot identiteiten van meerdere organisaties worden opgenomen in de rapporten van alle betrokken organisaties. De rapporten bevatten ALLEEN identiteiten die tot die organisatie behoren - een bepaalde organisatie ziet NOOIT de identiteiten van een andere organisatie.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.