

Compreender a seleção de políticas abrangentes que envolvem várias empresas

Contents

[Introdução](#)

[Overview](#)

[Seleção de política com uma única organização](#)

[Seleção de política com várias organizações](#)

[Emissão de Relatórios com Várias Organizações](#)

[Implicações para o Comportamento de Seleção de Política Atual](#)

[Páginas de bloco dedicadas para cenários envolvendo várias organizações](#)

[Alterações Planejadas para Seleção de Política envolvendo Várias Organizações](#)

[Comportamento de Seleção de Política](#)

[Geração de relatórios para todas as organizações envolvidas](#)

Introdução

Este documento descreve as políticas de várias organizações Umbrella que estão sendo consideradas em determinados cenários.

Overview

Em certos cenários, é possível considerar as políticas de várias organizações de guarda-chuva. Um exemplo disso seria um cliente de roaming ou dispositivo móvel para uma organização que se conecta à rede de uma organização diferente. Este artigo detalha como a política é escolhida atualmente neste caso e quais alterações a Umbrella pretende fazer a fim de melhorar este comportamento.

Seleção de política com uma única organização

Quando uma consulta DNS é enviada ao Umbrella, é possível que várias identidades sejam associadas à consulta. Por exemplo, uma consulta de um cliente de roaming (RC) por trás de uma rede protegida incluiria a ID do dispositivo do RC e o endereço IP da rede. Da mesma forma, uma consulta de um dispositivo virtual inclui a ID do local, a rede interna, o usuário do AD e o grupo do AD.

Normalmente, as identidades incluídas na consulta são todas associadas a uma única organização. Nesse caso, a política aplicada usa as regras de precedência de política detalhadas em nossa documentação:

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

Resumindo, o Umbrella atribui a cada política uma prioridade com base em sua ordem no Painel , com a política mais alta tendo a prioridade mais alta. Os resolvedores de Umbrella escolhem a política de prioridade mais alta que se aplica a pelo menos uma das identidades presentes na consulta.

Por exemplo, a Organização A pode ter estas políticas definidas:

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

A política do computador em roaming tem prioridade 2, enquanto a política da rede tem prioridade 1. Portanto, se uma consulta vier de um computador em roaming associado a uma rede externa, a Política 2 será aplicada. No entanto, se o computador em roaming ingressou em uma das redes da Organização A, a Política 1 será aplicada, pois a política da Rede tem uma prioridade mais alta.

Seleção de política com várias organizações

Essa mesma lógica é aplicada quando há identidades de várias organizações incluídas na

consulta. No entanto, como há várias organizações envolvidas, é a prioridade relativa de cada política que é considerada em relação à lista de políticas de cada organização.

Um exemplo explica isso melhor. Cada uma das organizações A e B tem essas políticas definidas em seus respectivos Umbrella 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.ping

Um Computador em Roaming da Organização A ingressa em uma Rede pertencente à Organização B. A consulta DNS enviada à Umbrella contém, portanto, a ID do dispositivo RC da Organização A e o endereço IP da Rede da Organização B.

Usando a lógica de uma única organização, obtemos as prioridades para a política de cada identidade. O RC da Organização A obtém a política A2, que tem uma prioridade 2, enquanto a Rede da Organização B obtém a política B1, que tem uma prioridade 1. Portanto, a política para a Rede da Organização B, a política B1, é aplicada.

Emissão de Relatórios com Várias Organizações

Quando uma consulta contém identidades de várias organizações, ela aparece apenas nos relatórios da organização cuja política foi selecionada. Os relatórios para essa organização mostram SOMENTE as identidades pertencentes a essa organização. Uma organização NUNCA tem visibilidade de outras identidades na consulta que pertencem a outras organizações.

Implicações para o Comportamento de Seleção de Política Atual

Devido ao comportamento de seleção de política descrito, é possível que uma identidade pertencente a uma organização possa ter sua política substituída pela política de outra organização. Isso inclui todos os recursos de política, incluindo bloqueio de segurança e conteúdo, listas de destino, designs de páginas bloqueadas e configurações de registro (observando as restrições em relatórios), com exceção de redirecionamentos de página bloqueada.

Páginas de bloco dedicadas para cenários envolvendo várias organizações

A partir de 16 de julho de 2021, quando os resolvedores do Umbrella detectam que uma consulta contém identidades de várias organizações, ela redireciona qualquer consulta bloqueada para uma página de bloqueio dedicada. Esta página de bloqueio informa ao usuário que mais de uma organização foi detectada e, portanto, que a consulta pode ter sido bloqueada devido à política de

outra organização.

Alterações Planejadas para Seleção de Política envolvendo Várias Organizações

Planos gerais para alterar o comportamento da seleção de políticas quando mais de uma organização estiver envolvida. As mudanças futuras incluem:

Comportamento de Seleção de Política

O Umbrella modifica o comportamento de seleção de política para que a política de prioridade mais alta de cada organização seja selecionada e aplicada. Em seguida, se alguma dessas políticas bloquear a consulta, ela será bloqueada. Isso permite que todas as empresas envolvidas garantam que suas políticas não sejam ignoradas. Esse comportamento pode ser melhor explicado usando uma analogia:

Os pais de Alice dizem que suas regras individuais são mais importantes do que as regras de casa. Alice não tem permissão para tomar sorvete, a qualquer hora, em qualquer lugar.

Os pais de Bob dizem que as regras de casa são mais importantes do que as regras individuais. Eles nunca deixam pizza em casa.

Modelo atual:

Alice vai para a casa de Bob. As regras da casa de Bob se aplicam e não as regras individuais de Alice. Alice pode tomar sorvete, mas não pizza. Os pais de Bob recebem um relatório que diz que alguém tomou sorvete em sua casa, mas não diz que foi Alice pelo nome.

Modelo proposto:

Alice vai para a casa de Bob. As regras da casa de Bob se aplicam, e as regras individuais de Alice se aplicam. Alice não tem sorvete nem pizza. Os pais de Bob recebem um relatório que diz que alguém teve a pizza e o sorvete negados, mas não diz que foi Alice pelo nome.

Geração de relatórios para todas as organizações envolvidas

Quando o comportamento de seleção de política está em vigor, o Umbrella também garante que quaisquer consultas envolvendo identidades de várias organizações sejam incluídas nos relatórios de todas as organizações envolvidas. Os relatórios SÓ incluem identidades pertencentes a essa organização - uma determinada organização NUNCA vê as identidades de outra organização.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.