

여러 조직과 관련된 Umbrella 정책 선택 이해

목차

[소개](#)

[개요](#)

[단일 조직에서의 정책 선택](#)

[여러 조직에서 정책 선택](#)

[복수 조직 보고](#)

[현재 정책 선택 행동에 대한 의미](#)

[여러 조직 관련 시나리오의 전용 차단 페이지](#)

[여러 조직과 관련된 정책 선택을 위한 계획된 변경 사항](#)

[정책 선택 동작](#)

[모든 관련 조직에 대한 보고](#)

소개

이 문서에서는 특정 시나리오에서 고려되는 여러 Umbrella 조직의 정책을 설명합니다.

개요

특정 시나리오에서는 여러 Umbrella 조직의 정책을 고려할 수 있습니다. 예를 들면 한 조직이 다른 조직의 네트워크에 연결하는 로밍 클라이언트 또는 모바일 장치가 될 수 있습니다. 이 문서에서는 현재 이 사례에서 정책이 어떻게 선택되었는지, 그리고 Umbrella가 이러한 행동을 개선하기 위해 어떤 변화를 의도하는지 자세히 설명합니다.

단일 조직에서의 정책 선택

DNS 쿼리를 Umbrella로 보내면 여러 ID를 쿼리에 연결할 수 있습니다. 예를 들어, 보호되는 네트워크 뒤에 있는 RC(Roaming Client)의 쿼리에는 RC의 디바이스 ID와 네트워크의 IP 주소가 모두 포함됩니다. 마찬가지로, 가상 어플라이언스의 쿼리에는 사이트 ID, 내부 네트워크, AD 사용자 및 AD 그룹이 포함됩니다.

일반적으로 쿼리에 포함된 ID는 모두 단일 조직과 연결됩니다. 이 경우 적용된 정책은 Cisco 문서에 설명된 정책 우선 순위 규칙을 사용합니다.

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

간단히 말해, Umbrella는 Dashboard(대시보드)의 순서에 따라 각 정책에 우선순위를 지정하며, 가장 높은 우선순위의 정책이 적용됩니다. Umbrella 확인자는 쿼리에 있는 ID 중 하나 이상에 적용되는 가장 높은 우선 순위 정책을 선택합니다.

예를 들어 조직 A에 다음과 같은 정책이 정의될 수 있습니다.

Subscription name:

Description:

Destination log:

Subscription type and source computers

☒ Collector initiated

This computer contacts the selected source computers and provides the subscription.

☐ Source computer initiated

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:

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

Change user account or configure advanced settings:

mceclip0.png

로밍 컴퓨터 정책의 우선 순위는 2이고 네트워크 정책의 우선 순위는 1입니다. 따라서 외부 네트워크에 연결된 로밍 컴퓨터에서 쿼리가 들어오는 경우 정책 2가 적용됩니다. 그러나 로밍 컴퓨터가 조직 A의 네트워크 중 하나에 가입된 경우 네트워크 정책의 우선순위가 더 높으므로 정책 1이 적용됩니다.

여러 조직에서 정책 선택

쿼리에 포함된 여러 조직의 ID가 있는 경우에도 동일한 논리가 적용됩니다. 그러나 여러 조직이 관련되어 있으므로 각 조직의 정책 목록과 관련하여 고려되는 것은 각 정책의 상대적 우선 순위입니다.

한 가지 예가 이를 가장 잘 설명합니다. 조직 A와 조직 B는 각각 해당 Umbrella 대시보드에 다음과 같은 정책이 정의되어 있습니다.

- **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

그러면 조직 A의 로밍 컴퓨터가 조직 B에 속한 네트워크에 조인합니다. 따라서 Umbrella로 전송된 DNS 쿼리에는 조직 A의 RC 장치 ID 및 조직 B의 네트워크 IP 주소가 포함됩니다.

단일 조직에 대한 논리를 사용하여 각 ID의 정책에 대한 우선순위를 가져옵니다. 조직 A의 RC는 우선 순위가 2인 정책 A2를 가져오고, 조직 B의 네트워크는 우선 순위가 1인 정책 B1을 가져옵니다. 따라서 조직 B의 네트워크에 대한 정책인 정책 B1이 적용됩니다.

복수 조직 보고

쿼리에 여러 조직의 ID가 포함된 경우 쿼리는 정책이 선택된 조직에 대한 보고서에만 나타납니다. 해당 조직에 대한 보고서에서는 해당 조직에 속한 ID만 표시합니다. 조직은 다른 조직에 속한 쿼리의 다른 ID를 볼 수 없습니다.

현재 정책 선택 행동에 대한 의미

설명된 정책 선택 동작으로 인해 한 조직에 속한 ID가 다른 조직의 정책에 의해 정책을 재정의할 수 있습니다. 여기에는 보안 및 콘텐츠 차단, 대상 목록, 차단 페이지 설계, 로깅 설정(보고에 대한 제한 사항 참고)을 비롯한 모든 정책 기능이 포함됩니다(차단 페이지 리디렉션 제외).

여러 조직 관련 시나리오의 전용 차단 페이지

2021년 7월 16일을 기준으로 Umbrella 확인기에서 쿼리에 여러 조직의 ID가 포함되어 있음을 감지하면 차단된 모든 쿼리를 전용 차단 페이지로 리디렉션합니다. 이 차단 페이지는 두 개 이상의 조직이 탐지되었으므로 다른 조직의 정책으로 인해 쿼리가 차단되었을 수 있음을 사용자에게 알립니다.

여러 조직과 관련된 정책 선택을 위한 계획된 변경 사항

Umbrella는 두 개 이상의 조직이 관련되어 있을 때 정책 선택의 행동을 변경하는 것에 대해 계획합니다. 향후 변경 사항은 다음과 같습니다.

정책 선택 동작

Umbrella는 각 조직에 대해 우선순위가 가장 높은 정책이 선택되고 시행되도록 정책 선택 동작을 수정합니다. 그런 다음 이러한 정책 중 하나라도 쿼리를 차단할 경우 쿼리가 차단됩니다. 따라서 관련된 모든 조직에서 정책이 우회되지 않도록 할 수 있습니다. 이 동작은 다음과 같은 비유를 사용하여 가장 잘 설명할 수 있습니다.

앨리스의 부모는 집안의 규칙보다 자신의 개별 규칙이 더 중요하다고 말한다. 앨리스는 언제 어디서나 아이스크림을 먹을 수 없습니다.

밥의 부모들은 집안의 규칙이 개인의 규칙보다 더 중요하다고 말한다. 그들은 집안에서 피자를 절대 허용하지 않습니다.

현재 모델:

앨리스는 밥의 집으로 가요. Bob의 집 규칙은 Alice의 개별 규칙이 아니라 적용됩니다. 앨리스는 피자가 아니라 아이스크림을 먹을 수 있어요. 밥의 부모는 누가 집에서 아이스크림을 먹었다는 제보를 받지만, 앨리스라는 이름은 적혀있지 않다.

제안 모델:

앨리스는 밥의 집으로 가요. Bob의 집 규칙이 적용되고 Alice의 개별 규칙이 적용됩니다. 앨리스는 아이스크림도 피자도 없다. 밥의 부모는 피자과 아이스크림이 거부되었다는 보고를 받지만, 앨리스라는 이름은 적혀있지 않습니다.

모든 관련 조직에 대한 보고

정책 선택 동작이 실행될 때 Umbrella는 또한 여러 조직의 ID와 관련된 모든 쿼리가 관련된 모든 조직의 보고서에 포함되도록 합니다. 보고서에는 해당 조직에 속한 ID만 포함됩니다. 지정된 조직에는 다른 조직의 ID가 표시되지 않습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.