

複数の組織が関与する包括的なポリシー選択の理解

内容

[はじめに](#)

[概要](#)

[単一組織でのポリシー選択](#)

[複数の組織でのポリシー選択](#)

[複数組織でのレポート](#)

[現在のポリシー選択動作への影響](#)

[複数の組織が関与するシナリオ用の専用ブロックページ](#)

[複数の組織が関与するポリシー選択の計画的変更](#)

[ポリシー選択の動作](#)

[関連するすべての組織のレポート](#)

はじめに

このドキュメントでは、特定のシナリオで検討されている複数のUmbrella組織のポリシーについて説明します。

概要

特定のシナリオでは、複数のUmbrella組織のポリシーを考慮することが可能です。たとえば、ある組織が別の組織のネットワークに接続する場合のクライアントまたはモバイルデバイスのローミングが考えられます。この記事では、この場合のポリシーの選択方法と、この動作を改善するためにUmbrellaが行う変更について説明します。

単一組織でのポリシー選択

DNSクエリがUmbrellaに送信されると、複数のIDがクエリに関連付けられる可能性があります。たとえば、保護されたネットワークの背後にあるローミングクライアント(RC)からのクエリには、RCのデバイスIDとネットワークのIPアドレスの両方が含まれます。同様に、仮想アプライアンスからのクエリには、サイトID、内部ネットワーク、ADユーザ、およびADグループが含まれます。

通常、クエリに含まれるIDはすべて1つの組織に関連付けられます。この場合、適用されるポリシーは、次のドキュメントに記載されているポリシーの優先順位ルールを使用します。

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

つまり、Umbrellaは各ポリシーにダッシュボード内での順序に基づいて優先順位を割り当て（優

先度の高い順にポリシーの優先順位を並べ替える)、最上位のポリシーが最も高い優先順位になります。Umbrellaリゾルバは、クエリに含まれるIDの少なくとも1つに適用される最も高い優先順位のポリシーを選択します。

たとえば、組織Aでは次のポリシーが定義されています。

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

Roaming Computerのポリシーの優先度は2ですが、Networkのポリシーの優先度は1です。したがって、クエリが外部ネットワークに参加しているRoaming Computerから送信された場合は、ポリシー2が適用されます。ただし、Roaming ComputerがA社のネットワークのいずれかに参加している場合は、ネットワークのポリシーの優先度が高いため、ポリシー1が適用されます。

複数の組織でのポリシー選択

クエリに複数の組織のIDが含まれている場合も、同じロジックが適用されます。ただし、関係する組織が複数あるため、各組織のポリシーリストに関して考慮されるのは、各ポリシーの相対的な優先順位です。

次に例を示します。組織Aと組織Bはそれぞれ、それぞれのUmbrellaダッシュボードで次のポリシーを定義しています。

- **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

次に、組織Aからのローミングコンピュータが、組織Bに属するネットワークに参加します。したがって、Umbrellaに送信されるDNSクエリには、組織AのRCのデバイスIDと組織BのネットワークのIPアドレスが含まれます。

単一の組織のロジックを使用して、各IDのポリシーの優先順位を取得します。組織AのRCはポリシーA2を取得します。これは優先度が2で、組織BのネットワークはポリシーB1を取得します。ポリシーB1の優先度が1です。したがって、組織Bのネットワークに対するポリシーであるポリシーB1が適用されます。

複数組織でのレポート

クエリに複数の組織のIDが含まれている場合、ポリシーが選択された組織のレポートにのみクエリが表示されます。その組織のレポートには、その組織に属するIDのみが表示されます。組織は、他の組織に属するクエリ内の他のIDを表示することはできません。

現在のポリシー選択動作への影響

説明したポリシー選択動作により、ある組織に属するIDのポリシーが、別の組織のポリシーによって上書きされる可能性があります。これには、ブロックページのリダイレクトを除く、セキュリティとコンテンツブロッキング、宛先リスト、ブロックページの設計、ロギング設定（レポートに関する制限に注意）を含むすべてのポリシー機能が含まれます。

複数の組織が関与するシナリオ用の専用ブロックページ

2021年7月16日の時点で、Umbrellaリゾルバは、クエリに複数の組織からのIDが含まれていることを検出すると、ブロックされているすべてのクエリを専用のブロックページにリダイレクトします。このブロックページは、複数の組織が検出されたため、クエリが別の組織のポリシーによってブロックされた可能性があることをユーザに通知します。

複数の組織が関与するポリシー選択の計画的変更

Umbrellaでは、複数の組織が関与する場合にポリシー選択の動作を変更することを計画しています。今後の変更は次のとおりです。

ポリシー選択の動作

Umbrellaは、各組織で最も優先度の高いポリシーが選択および適用されるように、ポリシー選択動作を変更します。その後、これらのポリシーのいずれかがクエリをブロックすると、クエリがブロックされます。これにより、関係するすべての組織で、ポリシーがバイパスされないようにすることができます。この動作は、次の例を使用すると説明できます。

アリスの両親は、家のルールより自分のルールの方が大事だと言っている。アリスはいつでもどこでもアイスクリームを食べることは許されていない。

ボブの両親は家事のルールは個人のルールより大事だと言っている。彼らは家の中でピザを絶対に許さない。

現在のモデル:

アリスはボブの家に行く。ボブの家の規則は適用され、アリスの個々の規則は適用されません。アリスはアイスクリームを食べるが、ピザは食べられない。ボブの両親は、誰かが自分の家でアイスクリームを食べたと言うレポートを受け取ったが、それが名前でアリスだったとは言わない。

提案モデル:

アリスはボブの家に行く。ボブの家の規則が適用され、アリスの個々の規則が適用されます。アリスにはアイスクリームもピザもない。ボブの両親は、誰かがピザとアイスクリームを拒否されたというレポートを得るが、それは名前でアリスだったとは言わない。

関連するすべての組織のレポート

さらに、ポリシー選択の動作が実施されると、複数の組織のIDに関するクエリが、関係するすべての組織のレポートに含まれるようになります。レポートには、その組織に属するIDのみが含まれます。特定の組織が別の組織のIDを参照することはありません。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。