

Umbrellaのアクティビティ検索レポートに表示されないActive Directoryユーザのトラブルシューティング

内容

[はじめに](#)

[解決方法](#)

[原因](#)

[アクティビティ検索で「ID」が取得される場所](#)

[追加情報](#)

はじめに

このドキュメントでは、Cisco Umbrellaのアクティビティ検索レポートについて説明します。[アクティビティ検索レポート](#)は、ユーザが作成しているすべてのDNSクエリをほぼライブで報告したものです。Cisco Umbrella [Active Directory\(AD\)統合](#)を設定している場合は、ADユーザがアクティビティ検索のID列に入力していることを確認できます。ただし、Identity列にユーザが表示されない場合があります。

解決方法

アクティビティ検索のID列にADユーザが直接表示されている必要があるが、表示されない場合、または表示されるADユーザが少数であっても予想したほど多くない場合は、次の点を確認してください。

1. サイトとActive Directory

- すべてのADコンポーネントをチェックして、報告されたエラーや問題がないことを確認します。コンポーネントのいずれかにグレー、オレンジ、または赤のステータスインジケータが表示された場合は、これらの詳細を取得してサポートチケット(umbrella-support@cisco.com)を開きます。
 - 影響を受けるユーザ (アクティビティ検索に表示されないユーザ) からの[診断テスト](#)
 - エラーメッセージが展開された仮想アプライアンス(VA)コンソールのスクリーンショット
 - ADコネクタの監査ログ

2. ログの設定

- すべてのポリシーの[詳細設定]で、ログの量に関するセクションが下部に表示されます。次のように設定できます。
 - すべての要求をログに記録
 - セキュリティイベントのみのログ
 - 要求をログに記録しない

- ポリシーが「セキュリティイベントのみログ」に設定されている場合は、クエリの数
が予想より少ないか、一部のユーザーからの結果がまったく表示されない理由を説明
できます。

LOGGING

☒ Log All Requests

☐ Log Only Security Events

Log and report on only those requests that match a security filter or integration, with no reporting on other requests.

☐ Don't Log Any Requests

Note: No requests will be reported or alerted on. Unreported events will still be logged anonymously and aggregated for research and threat intelligence purposes.

3. 正しいポリシーの優先順位

- ポリシーのリスト内でADユーザポリシーよりも高いネットワークIDに適用するポリ
シーがある場合、ネットワークIDポリシーが適用される可能性が高くなります。これは
、アクティビティ検索で、ネットワークが報告されたIDとして表示されることを意味
します。[ベストプラクティス](#)および[ポリシーの優先順位](#)については、Cisco
Umbrellaのドキュメントも確認してください。

原因

アクティビティ検索で「ID」が取得される場所

AD統合が期待どおりに動作していると仮定して、DNSクエリがUmbrellaに着信すると、次の情報
がクエリに渡されます。

- 内部IPアドレス
- AD IDハッシュ (ユーザ、ホスト、またはその両方)
- 出力IP
- クエリ中のドメイン

AD IDハッシュは、仮想アプライアンスによってクエリに追加され、仮想アプライアンスはその
情報と、ADコネクタからのログオンイベントに対応する内部IPアドレスを渡します。

次に、Cisco Umbrellaはこの情報を使用して、組織を特定し、適用するポリシーを決定します。
ADユーザに適用されるポリシーが存在せず、ネットワークまたはサイトに適用されるポリシーが
存在する場合、Cisco Umbrellaはそのアイデンティティを使用してポリシーを適用します。これ
は、クエリ、ID、および応答がアクティビティ検索で報告されると、報告されたポリシーをトリ
ガーしたIDを意味します。その他の情報は引き続き要求でタグ付けされるため、ADユーザを検
索して、ネットワークをIDとして報告するアクティビティを取得できます。さらに、アクティビ
ティ検索データをCSVファイルにエクスポートすると、クエリに関連付けられているすべての
ID情報が表示されます。

追加情報

それでもADユーザが表示されない場合は、サポート(umbrella-support@cisco.com)に連絡し、[診
断テストの結果](#)、および関連するADコネクタ監査ログを提示してください。

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。