Secure Accessサポートチームの基本的な情報のトラブルシューティングと収集

内容

はじめに

このドキュメントでは、Cisco Secure Access Support Team(ACS)と連携する際に収集する必要がある基本情報について説明します

前提条件

要件

次の項目に関する知識があることが推奨されます。

- シスコセキュアアクセス
- Cisco Secureクライアント
- Wiresharkとtcpdumpによるパケットキャプチャ

使用するコンポーネント

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

Cisco Secure Accessの使用中にシスコサポートチームに問い合わせる必要がある問題が発生したり、問題の基本的な調査を行って、ログを調べて問題を解決しようとする場合があります。この記事では、セキュアアクセスに関連する基本的なトラブルシューティングログの収集方法について説明します。すべての手順がすべてのシナリオに適用されるわけではないことに注意してください。

セキュアアクセス組織IDの検索

シスコのエンジニアがお客様のアカウントを見つけるには、セキュアアクセスダッシュボードへのログイン後にURLに記載されている組織IDを提供してください。

組織IDの検索手順：

1. sse.cisco.comにログインします。
2. 複数の組織がある場合は、適切な組織に切り替えます。
3. 組織IDは、次のパターンのURLで確認できます。
https://dashboard.sse.cisco.com/org/{7_digit_org_id}/overview

Cisco Secure Client Diagnostic and Reporting Tool(DART)

Cisco Secure Client Diagnostic and Reporting Tool(DART)は、Secure Clientパッケージとともにインストールされるツールで、ユーザエンドポイントに関する重要な情報の収集に役立ちます。

DARTバンドルによって収集される情報の例：

- ZTNAログ
– クライアントログとプロファイル情報の保護
– システム情報
– インストールされているその他のセキュアクライアントアドオンまたはプラグインログ

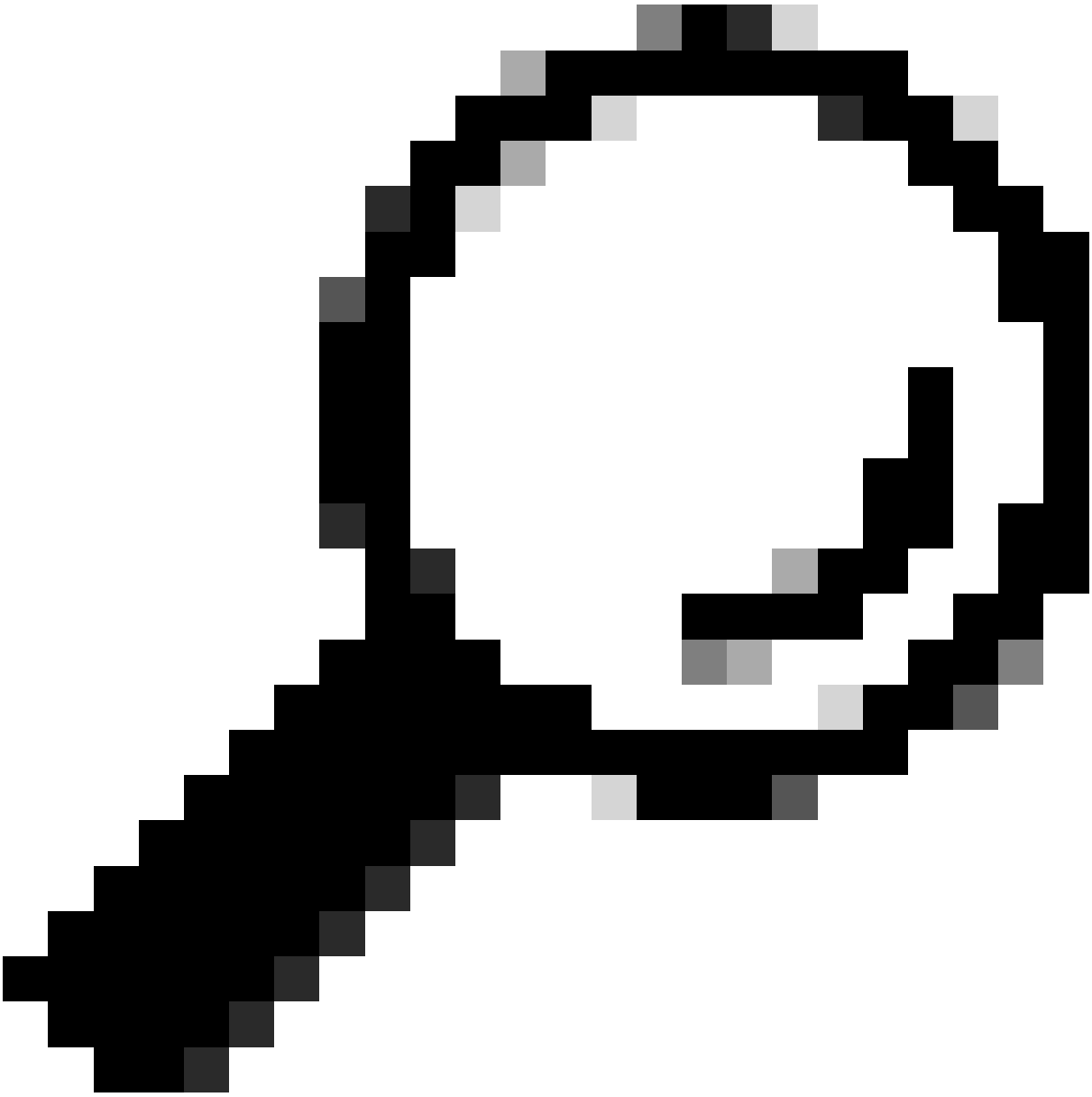
DARTの収集手順：

ステップ 1：DARTを起動します。

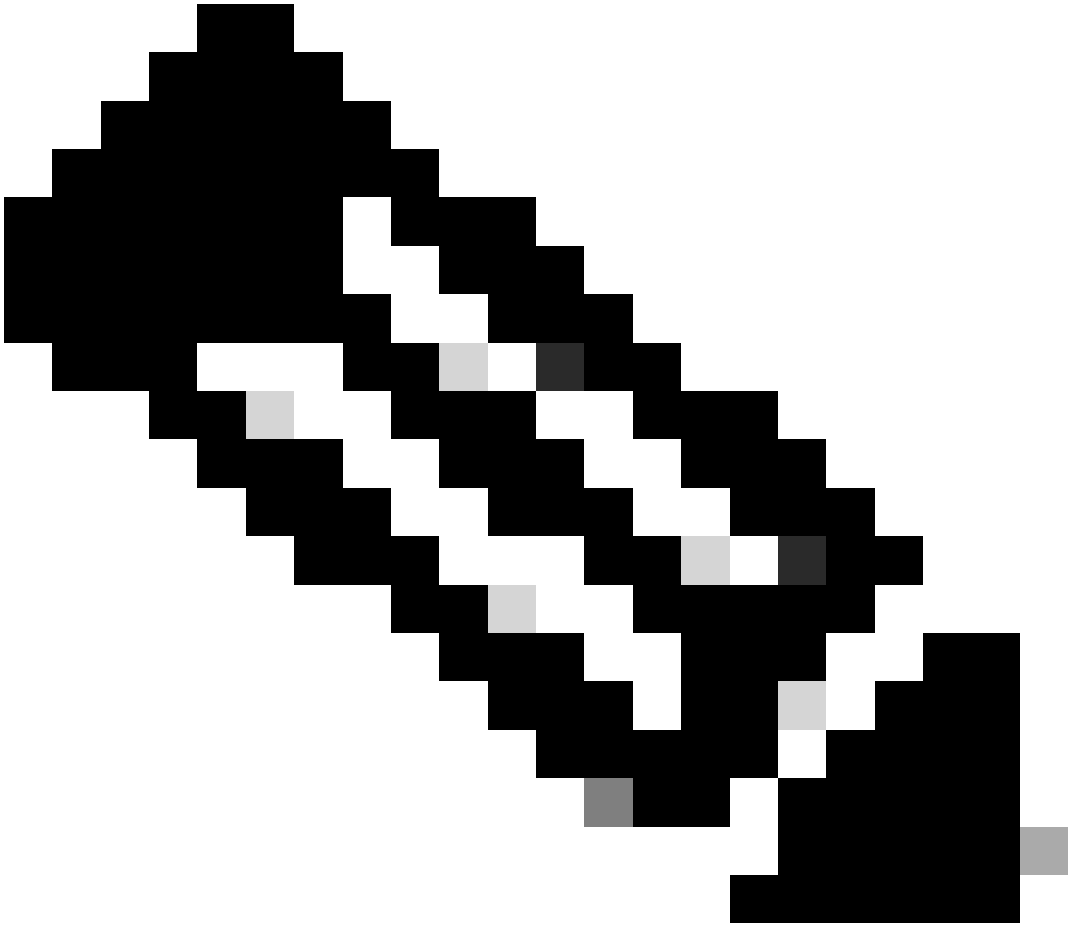
1. Windowsコンピュータの場合は、Cisco Secure Clientを起動します。
2. Linuxコンピュータの場合は、 **Applications** > **Internet** > **Cisco DART**または/opt/cisco/anyconnect/dart/dartuiを選択します。
3. Macコンピュータの場合は、Applications > Cisco > Cisco DARTを選択します。

ステップ 2：[統計]タブをクリックし、[詳細]をクリックします。

ステップ 3：デフォルトまたはカスタムバンドル作成を選択します。



ヒント：バンドルのデフォルト名はDARTBundle.zipで、ローカルデスクトップに保存されます。



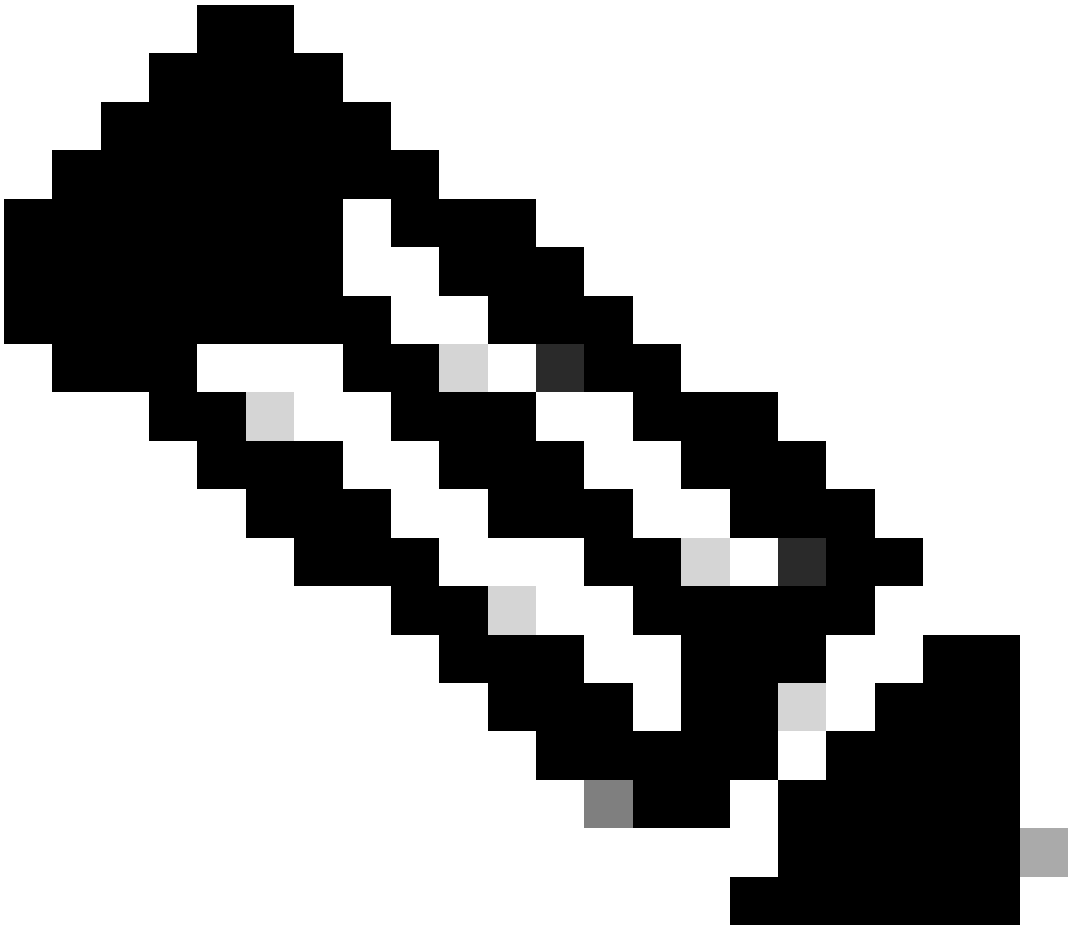
注：デフォルトを選択すると、DARTはバンドルの作成を開始します。[カスタム]を選択した場合は、ウィザードの指示に従って、ログ、設定ファイル、診断情報、およびその他のカスタマイズを指定します

HTTPアーカイブ(HAR)のキャプチャ

HARはさまざまなブラウザから収集できます。HARは次のような複数の情報を提供します。

1. HTTPS要求の復号化バージョン。
2. エラー・メッセージ、要求の詳細およびヘッダーに関する内部情報。
3. タイミング及び遅延情報
4. ブラウザベースの要求に関するその他の情報

HARキャプチャを収集するには、https://toolbox.googleapps.com/apps/har_analyzer/に記載されている手順を使用してください。



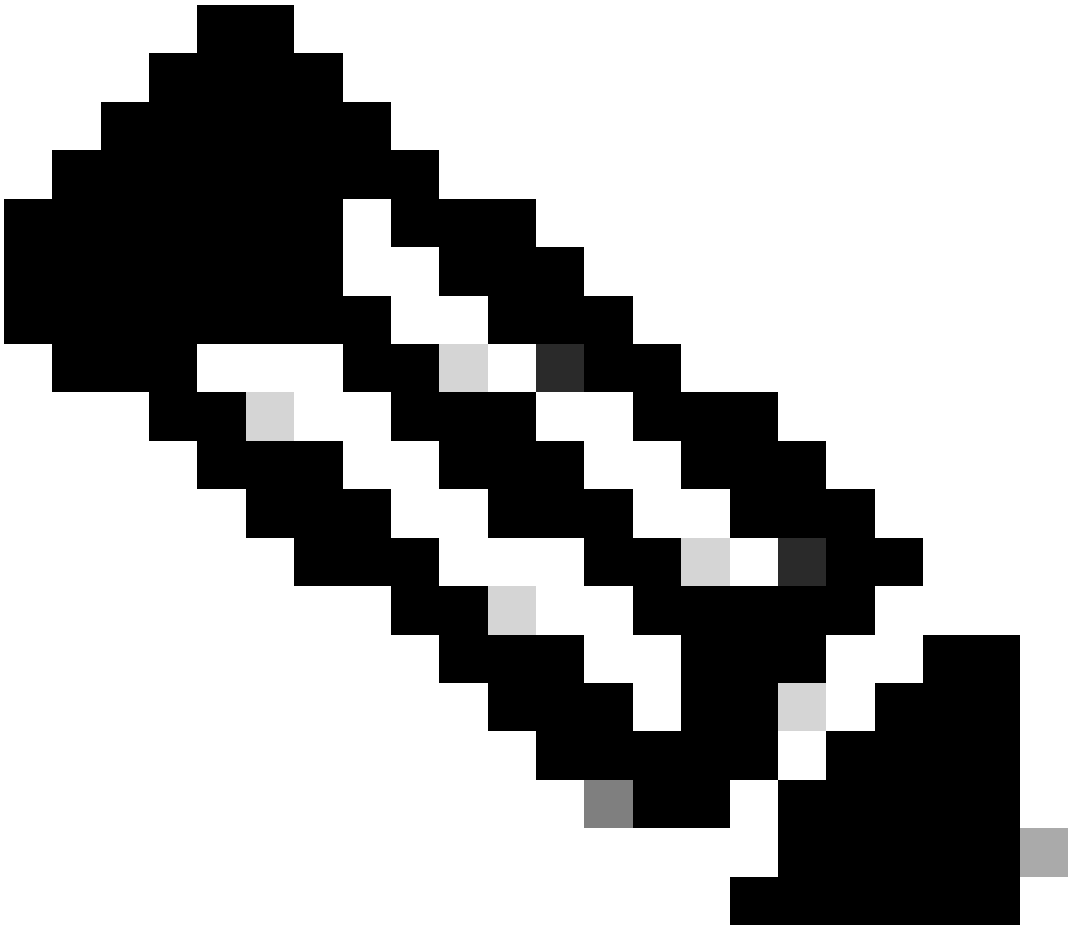
注：適切なデータを収集するには、ブラウザセッションを更新する必要があります

パケット キャプチャ

パケットキャプチャは、パフォーマンスの問題やパケット損失が検出されるシナリオ、またはネットワークの完全停止が検出されるシナリオで役立ちます。キャプチャを収集するための最も一般的なツールは、wiresharkおよび **tcpdump**です。または、Ciscoファイアウォールやルータなど、デバイス自体でpcapファイル形式を収集する組み込み機能。

エンドポイントで有用なパケットキャプチャを収集するには、次の情報を必ず収集してください。

1. セキュアクライアントアドオンを介して送信されるトラフィックをキャプチャするループバックインターフェイス。
2. パケットパスに関係する他のすべてのインターフェイス。
3. すべてのデータが収集されるように、最小限のフィルタを適用するか、まったくフィルタを適用しません。



注：ネットワークデバイスでキャプチャが収集される際、このアクティビティによるパフォーマンスの発生を避けるために、トラフィックの送信元と宛先でフィルタリングし、関連するポートとサービスだけにキャプチャを制限してください。

ポリシーのデバッグ出力

Policy debug outputは、Secure Accessによって保護されている場合にユーザーのブラウザから送信される診断出力です。この出力には、展開に関する重要な情報が含まれます。

1. 組織ID
2. 展開の種類
3. 接続されたプロキシ
4. パブリックおよびプライベートIPアドレス
5. トラフィックの送信元に関連するその他の情報。

ポリシーテストの結果を実行するには、保護されたエンドポイント(https://policy.test.sse.cisco.com/)からこのリンクにログインしてください。

ブラウザに証明書エラーメッセージが表示される場合は、セキュアアクセスルート証明書を信頼していることを確認してください。

セキュアアクセスのルート証明書をダウンロードするには：

セキュアアクセスに移動します Dashboard > Secure > Settings > Certificate > (Internet Destinations tab)

シスコサポートサービスリクエストへの結果のアップロード

サポートケースにファイルをアップロードするには、次の手順を実行します。

ステップ 1：SCMにログインします。

ステップ 2：ケースを表示および編集するには、リスト内のケース番号またはケースタイトルをクリックします。「ケースの概要」ページが開きます。

ステップ 3：Add Filesをクリックしてファイルを選択し、ケースの添付ファイルとしてアップロードします。SCM File Uploaderツールが表示されます。

ステップ 4：[アップロードするファイルを選択]ダイアログボックスで、アップロードするファイルをドラッグするか、内をクリックしてローカルマシンでアップロードするファイルを参照します。

ステップ 5：説明を追加して、すべてのファイルのカテゴリを指定するか、個別に指定します。

関連情報

- **シスコのテクニカルサポートとダウンロード**
- **セキュアアクセスに関するドキュメントおよびユーザガイド**

- **Cisco Secure Clientソフトウェアのダウンロード**

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。