Fehlerbehebung und Erfassung grundlegender Informationen für das Secure Access Support Team

Inhalt

Einleitung

In diesem Dokument werden die grundlegenden Informationen beschrieben, die bei der Arbeit mit dem Cisco Secure Access Support Team gesammelt werden müssen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Sicherer Zugriff von Cisco
- Cisco Secure Client
- Paketerfassung über Wireshark und tcpdump

Verwendete Komponenten

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Bei der Arbeit an Cisco Secure Access können Sie Probleme feststellen, wenn Sie das Cisco Support-Team kontaktieren müssen, oder wenn Sie eine grundlegende Untersuchung des Problems durchführen und versuchen möchten, die Protokolle zu durchsuchen und das Problem zu isolieren. In diesem Artikel wird erläutert, wie Sie die grundlegenden Fehlerbehebungsprotokolle für den sicheren Zugriff erfassen. Beachten Sie, dass nicht alle Schritte für jedes Szenario gelten.

ID der Organisation für sicheren Zugriff ermitteln

Damit Cisco Techniker nach Ihrem Konto suchen können, geben Sie Ihre Organisations-ID an, die Sie nach der Anmeldung beim Secure Access Dashboard unter der URL finden.

Schritte zum Suchen der Organisations-ID:

1. Melden Sie sich unter sse.cisco.com an.
2. Wenn Sie mehrere Organisationen haben, wechseln Sie zur rechten.
3. Die Organisations-ID befindet sich in der URL in diesem Muster: https://dashboard.sse.cisco.com/org/{7_digit_org_id}/overview

Cisco Secure Client Diagnostic and Reporting Tool (DART)

Das Cisco Secure Client Diagnostic and Reporting Tool (DART) ist ein Tool, das mit dem Secure Client-Paket installiert wird und dazu beiträgt, wichtige Informationen über das Benutzerendgerät zu erfassen.

Beispiel für Informationen, die vom DART-Paket gesammelt wurden:

- ZTNA-Protokolle
- Protokolle und Profilinformationen des sicheren Clients
- Systeminformationen
- Andere Secure Client Add-ons oder Plugins-Protokolle, die auf installiert sind

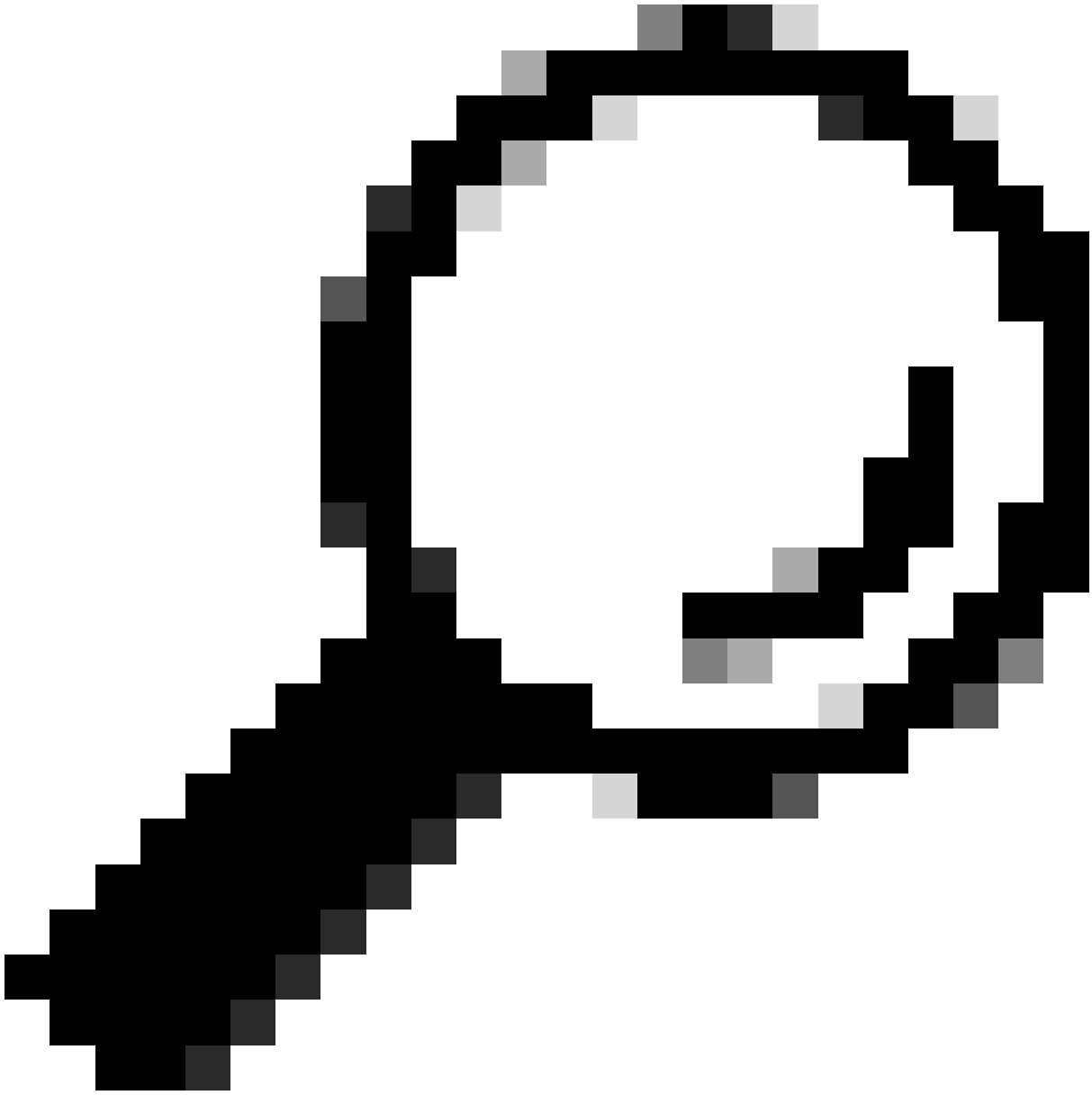
Hinweise zum Sammeln von DART:

Schritt 1: Starten Sie DART.

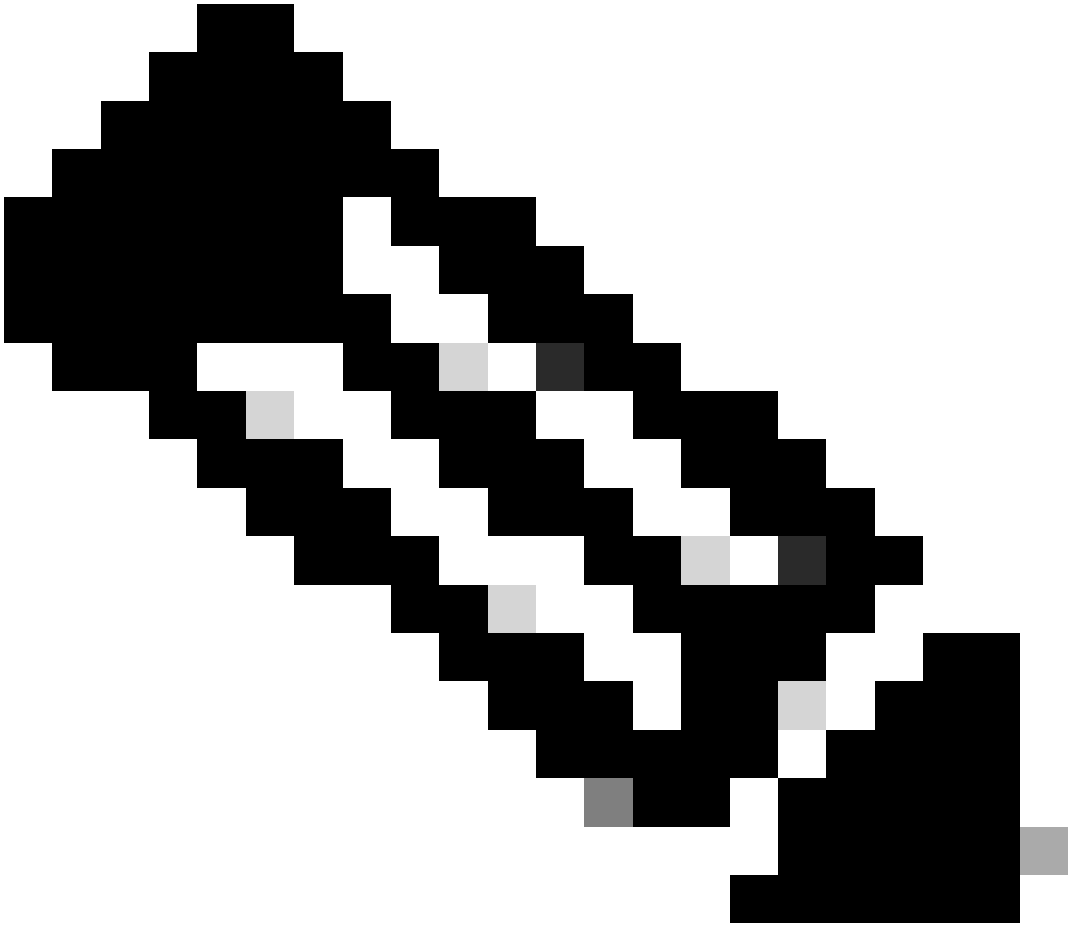
1. Starten Sie für einen Windows-Computer den Cisco Secure Client.
2. Wählen Sie für einen Linux-Computer **Applications** > **Internet** > **Cisco DART**oder /opt/cisco/anyconnect/dart/dartui.
3. Für einen Mac-Computer wählen Sie Applications > Cisco > Cisco DART.

Schritt 2: Klicken Sie auf die Registerkarte Statistik und anschließend auf Details.

Schritt 3: Wählen Sie Standardpaketerstellung oder benutzerdefinierte Bündelerstellung aus.



Tipp: Der Standardname für das Paket lautet DARTBundle.zip und wird auf dem lokalen Desktop gespeichert.



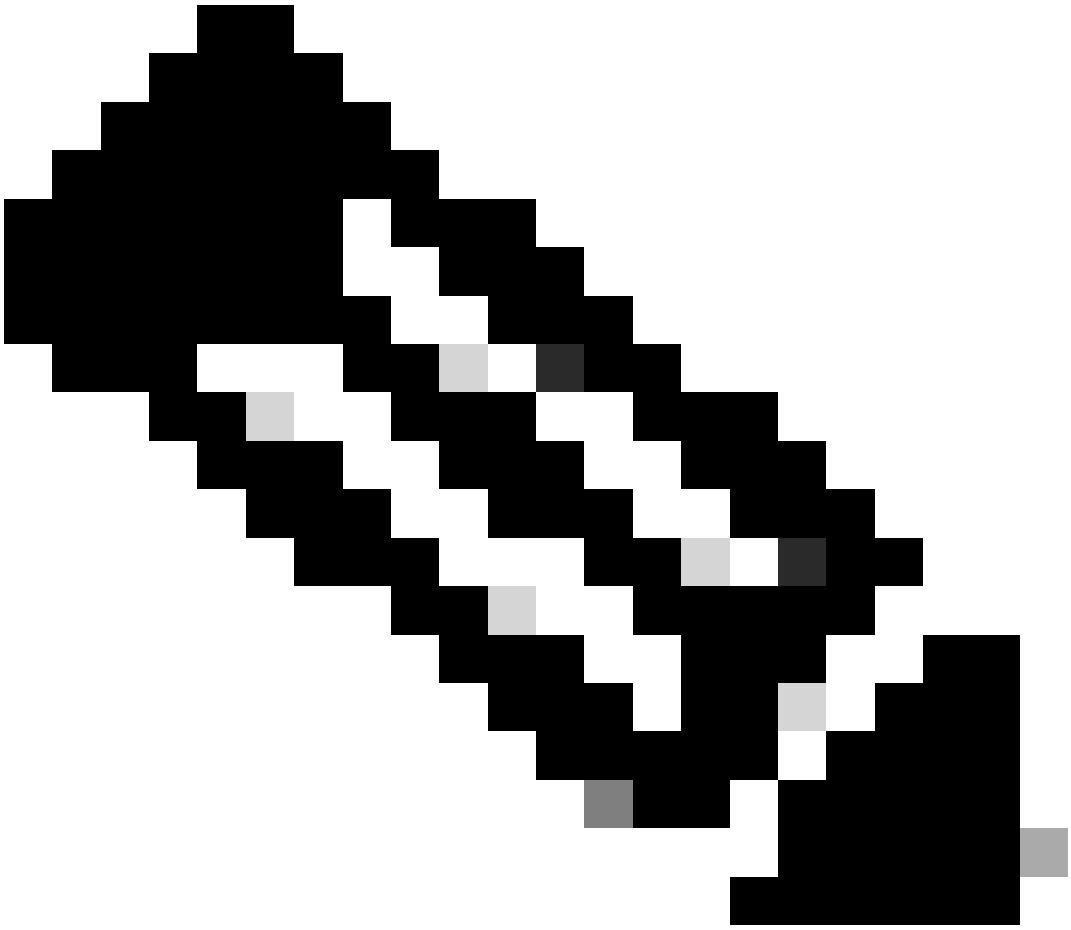
Hinweis: Wenn Sie Default (Standard) auswählen, beginnt DART mit der Erstellung des Pakets. Wenn Sie Benutzerdefiniert auswählen, fahren Sie mit den Aufforderungen des Assistenten fort, um Protokolle, Einstellungsdateien, Diagnoseinformationen und andere Anpassungen anzugeben.

HTTP-Archivierung (HAR) erfasst

HAR kann von verschiedenen Browsern gesammelt werden. Es stellt mehrere Informationen bereit, die Folgendes umfassen:

1. Entschlüsselte Version der HTTPS-Anforderungen.
2. Interne Informationen zu Fehlermeldungen, Anforderungsdetails und Headern.
3. Informationen zu Zeitablauf und Verzögerung
4. Sonstige Informationen zu browserbasierten Anfragen.

Zum Sammeln von HAR-Aufzeichnungen gehen Sie wie in dieser Quelle beschrieben vor: https://toolbox.googleapps.com/apps/har_analyzer/



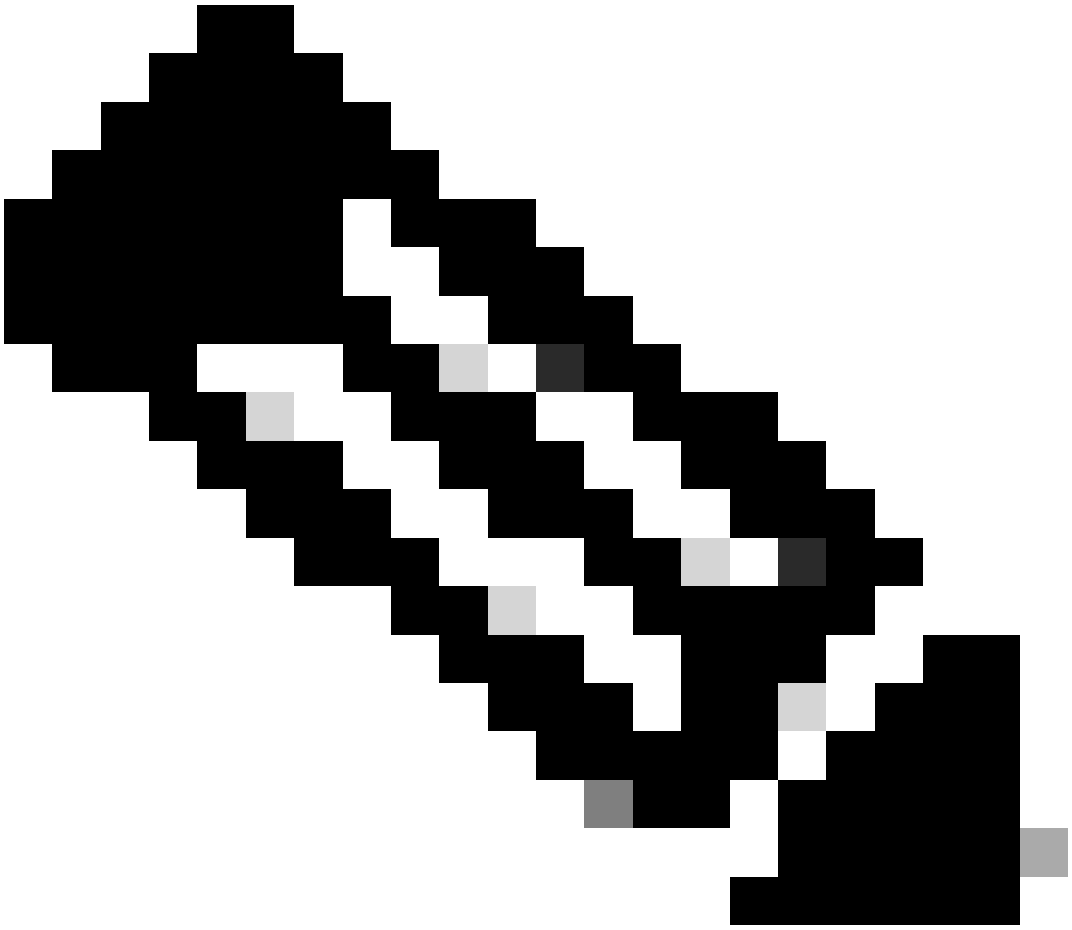
Hinweis: Sie müssen Ihre Browser-Sitzung aktualisieren, um die richtigen Daten zu sammeln.

Paketerfassung

Die Paketerfassung ist in einem Szenario nützlich, in dem ein Leistungsproblem oder ein Paketverlust erkannt wird oder bei dem ein Netzwerkausfall insgesamt auftritt. Die gängigsten Tools zum Sammeln von Aufnahmen sind wireshark und **tcpdump**. Oder eine integrierte Funktion zum Sammeln des PCAP-Dateiformats im Gerät selbst, z. B. eine Cisco Firewall oder ein Router.

Um nützliche Paketerfassungen auf einem Endpunkt zu sammeln, stellen Sie Folgendes sicher:

1. Loopback-Schnittstelle zur Erfassung von Datenverkehr, der über Secure Client-Add-ons gesendet wird
2. Alle anderen am Paketpfad beteiligten Schnittstellen.
3. Wenden Sie nur minimale oder gar keine Filter an, um sicherzustellen, dass alle Daten gesammelt werden.



Hinweis: Wenn Erfassungen auf einem Netzwerkgerät erfasst werden, müssen Sie nach Quelle und Ziel des Datenverkehrs filtern und die Erfassung auf zugehörige Ports und Services beschränken, um die durch diese Aktivität verursachte Leistung zu vermeiden.

Ausgabe von Richtliniendebugs

Bei der Ausgabe von Richtlinien-Debugging handelt es sich um eine Diagnoseausgabe, die über den Benutzerbrowser gesendet wird, wenn sie

durch Secure Access geschützt ist. Diese Datei enthält wichtige Informationen über die Bereitstellung.

1. Organisations-ID
2. Bereitstellungstyp
3. Angeschlossener Proxy
4. Öffentliche und private IP-Adresse
5. Weitere Informationen zur Quelle des Datenverkehrs.

Um die Richtlinientestergebnisse auszuführen, melden Sie sich über einen geschützten Endpunkt an: https://policy.test.sse.cisco.com/

Stellen Sie sicher, dass Sie dem Stammzertifikat für sicheren Zugriff vertrauen, wenn in Ihrem Browser eine Zertifikatfehlermeldung angezeigt wird.

So laden Sie das Stammzertifikat für sicheren Zugriff herunter:

Navigieren Sie zu Sicherer Zugriff Dashboard > Secure > Settings > Certificate > (Internet Destinations tab)

Ergebnisse in Cisco Support Service Request hochladen

Sie können Dateien wie folgt auf den Support hochladen:

Schritt 1: Melden Sie sich bei SCM an.

Schritt 2: Um das Ticket anzuzeigen und zu bearbeiten, klicken Sie in der Liste auf die Ticketnummer oder den Titel. Die Seite "Ticketübersicht" wird geöffnet.

Schritt 3: Klicken Sie auf Dateien hinzufügen, um eine Datei auszuwählen und als Anhang zum Ticket hochzuladen. Das System zeigt das SCM-Datei-Uploader-Tool an.

Schritt 4: Ziehen Sie im Dialogfeld Dateien zum Hochladen auswählen die Dateien, die Sie hochladen möchten, oder klicken Sie auf das Innere, um auf Ihrem lokalen Computer nach Dateien zum Hochladen zu suchen.

Schritt 5: Fügen Sie eine Beschreibung hinzu, und geben Sie eine Kategorie für alle Dateien oder einzeln an.

Zugehörige Informationen

- **Technischer Support und Downloads von Cisco**
- **Secure Access-Dokumentation und Benutzerhandbuch**
- **Software-Download für Cisco Secure Client**

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.