Probleemoplossing en verzameling van basisinformatie voor het Secure Access Support Team

Inhoud

Inleiding

Dit document beschrijft de basisinformatie die moet worden verzameld tijdens het werken met Cisco Secure Access Support Team

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco beveiligde toegang
- Cisco Secure-client
- Packet Captures via Wireshark en tcpdump

Gebruikte componenten

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Tijdens het werken aan Cisco Secure Access kunt u problemen tegenkomen waar u contact moet opnemen met Cisco Support Team of basisonderzoek naar het probleem wilt uitvoeren en proberen de logbestanden te doorlopen en het probleem op te lossen. Dit artikel gaat verder op hoe u de basislogboeken voor probleemoplossing met betrekking tot Secure Access kunt verzamelen. Houd er rekening mee dat niet alle stappen op elk scenario van toepassing zijn.

Identificatie van beveiligde toegangsorganisaties zoeken

Geef uw organisatie-ID op die in de URL kan worden gevonden zodra u bent aangemeld bij het Secure Access Dashboard, zodat Cisco Engineer uw account kan vinden.

Stappen om organisatie-ID te vinden:

1. Aanmelden op sse.cisco.com
2. Als je meerdere organisaties hebt, switch je naar rechts.
3. De organisatie-ID kan in de URL in dit patroon worden gevonden:
https://dashboard.sse.cisco.com/org/{7_digit_org_id}/overview

Cisco Secure Client-diagnostische en -rapportagetool (DART)

Cisco Secure Client Diagnostic and Reporting Tool (DART) is een tool dat is geïnstalleerd met het Secure Client-pakket en helpt bij het verzamelen van belangrijke informatie over het gebruikerseindpunt.

Voorbeeld van informatie verzameld door DART bundel:

- ZTNA-logs
- Beveiligde clientlogs en profielinformatie
- Systeeminformatie
- Andere Secure Client Add-ons of Plugins-logbestanden die zijn geïnstalleerd op

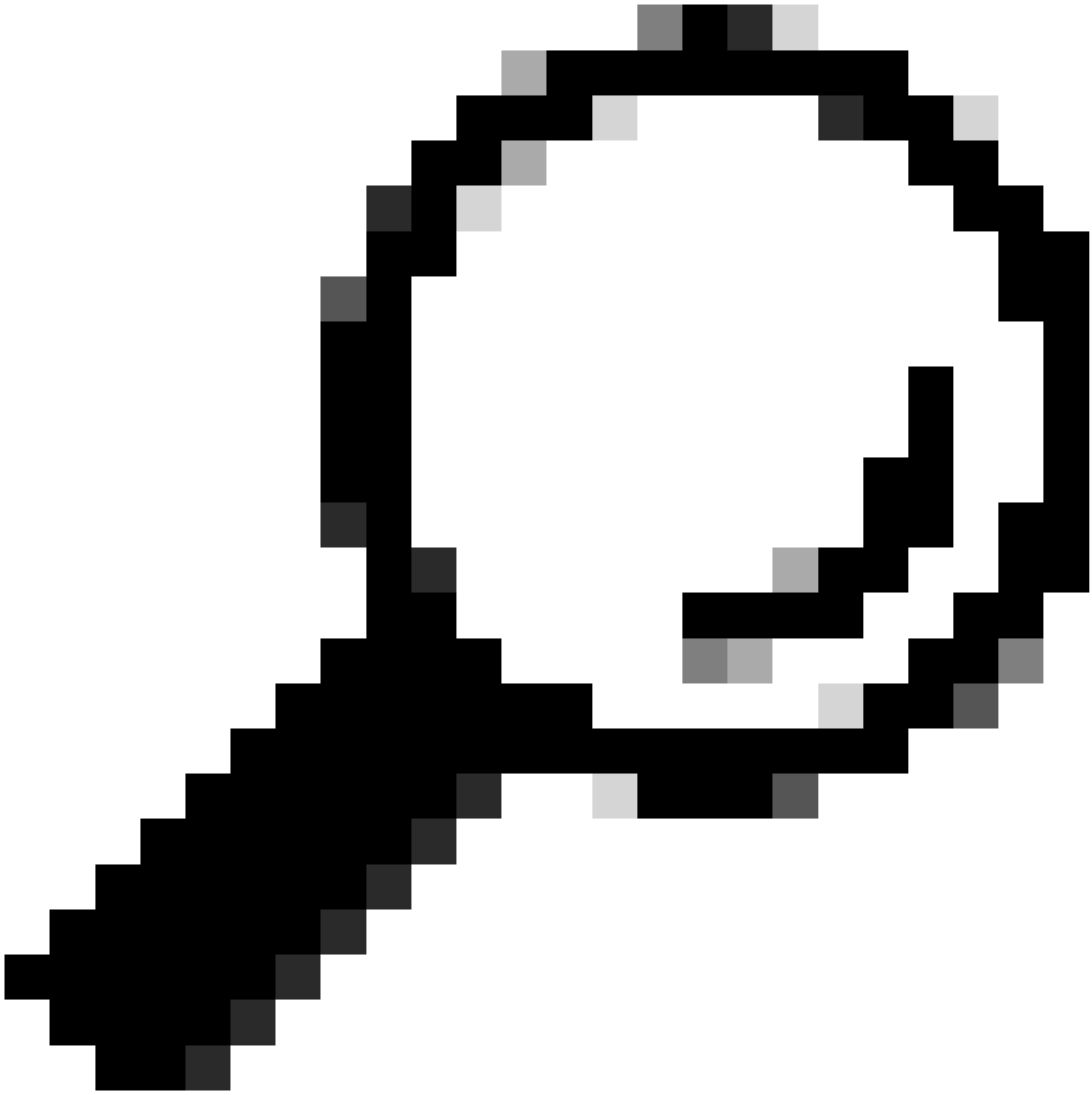
Instructies voor het verzamelen van DART:

Stap 1. Start DART.

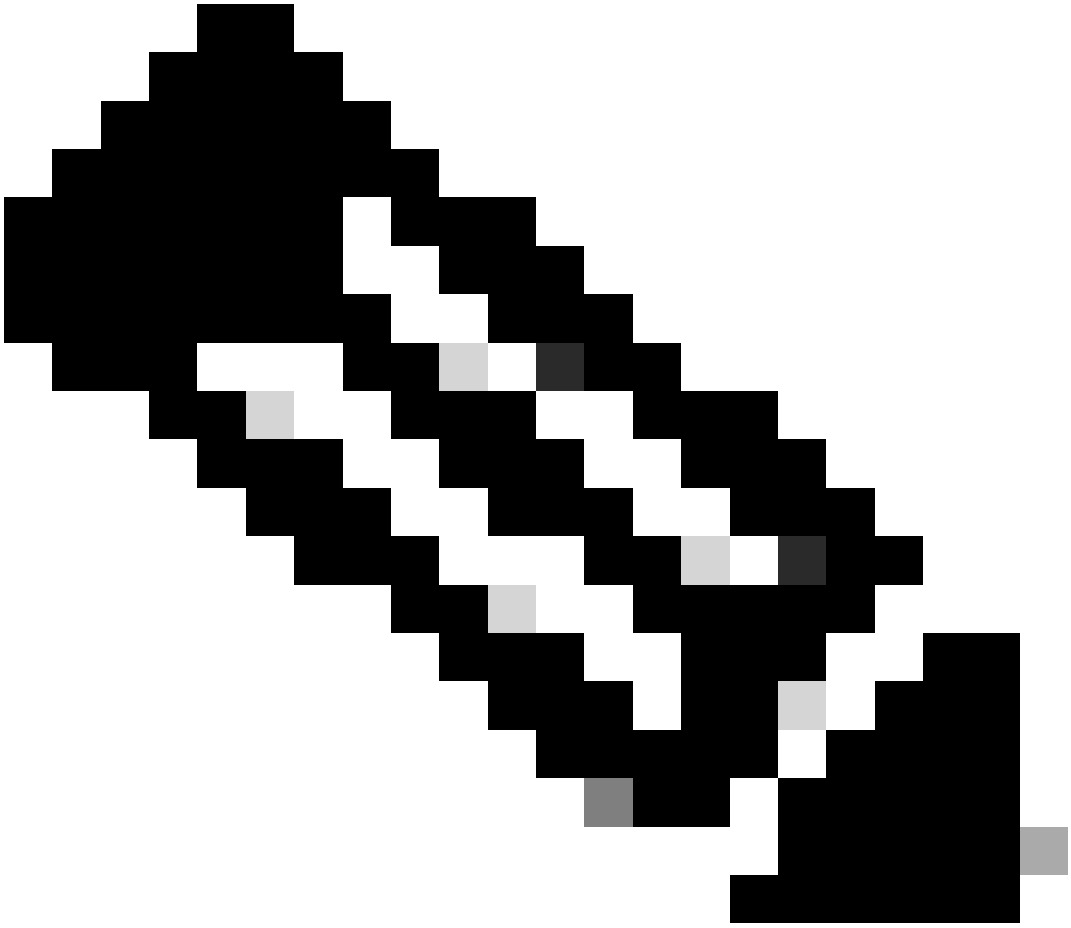
1. Start voor een Windows-computer de Cisco Secure-client.
2. Kies voor een Linux-computer **Applications** > **Internet** > **Cisco DART**of /opt/cisco/anyconnect/dart/dartui.
3. Voor een Mac-computer, kies Applications > Cisco > Cisco DART.

Stap 2. Klik op het tabblad Statistieken en klik vervolgens op Details.

Stap 3. Kies Standaard of Aangepaste bundel creatie.



Tip: de standaardnaam voor de bundel is DARTBundle.zip, en het wordt opgeslagen op de lokale desktop.



Opmerking: Als u Standaard hebt gekozen, begint DART met het maken van de bundel. Als u Aangepast hebt gekozen, gaat u verder met de wizard vraagt om logbestanden, voorkeurbestanden, diagnostische informatie en andere aanpassingen op te geven

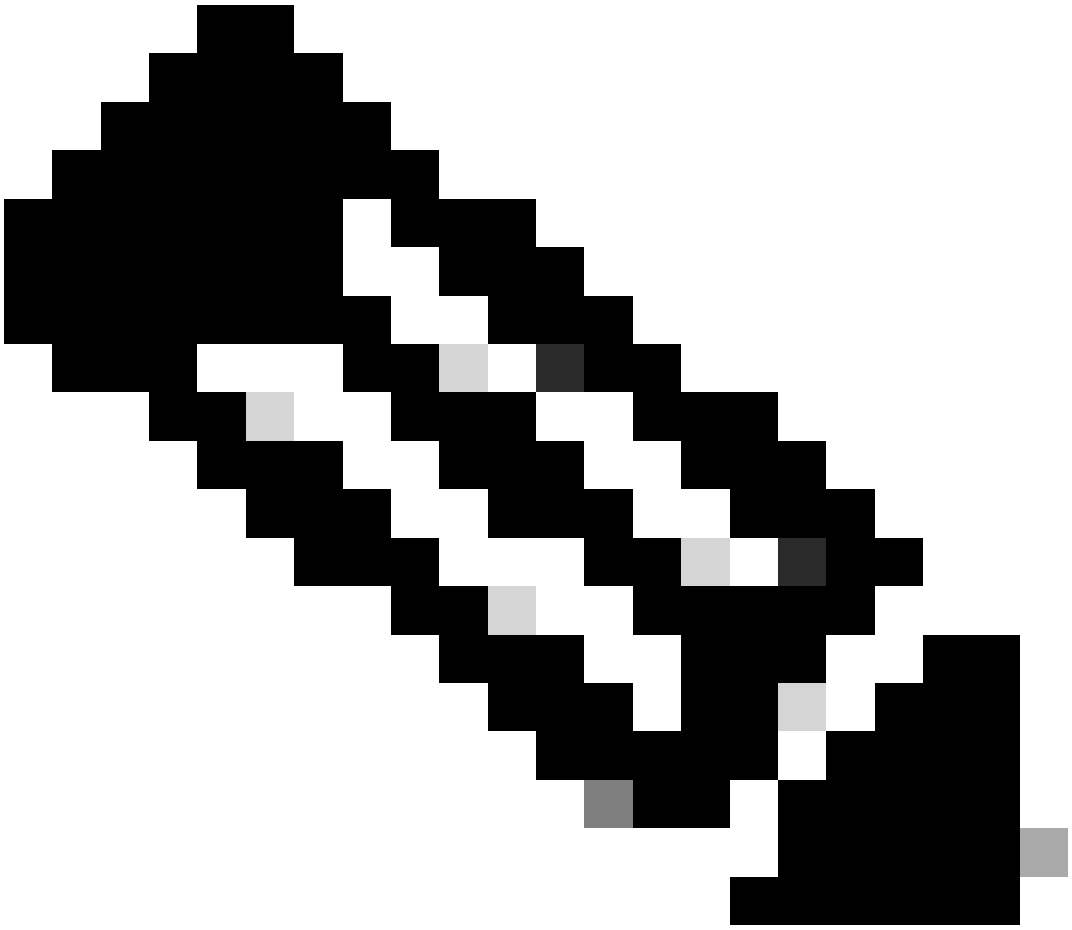
---

HTTP-archiefbestand (HAR) neemt

HAR kan worden verzameld uit verschillende browsers. het biedt meerdere informatie, waaronder:

1. Gedecrypteerde versie van de HTTPS-verzoeken.
2. Interne informatie over foutmeldingen, aanvraagdetails en kopregels.
3. Informatie over timing en vertraging
4. Overige informatie over op browser gebaseerde verzoeken.

Om HAR Captures te verzamelen gebruikt u de stappen die in deze bron worden beschreven: https://toolbox.googleapps.com/apps/har_analyzer/



Opmerking: U moet uw browsersessie verversen om de juiste gegevens te verzamelen

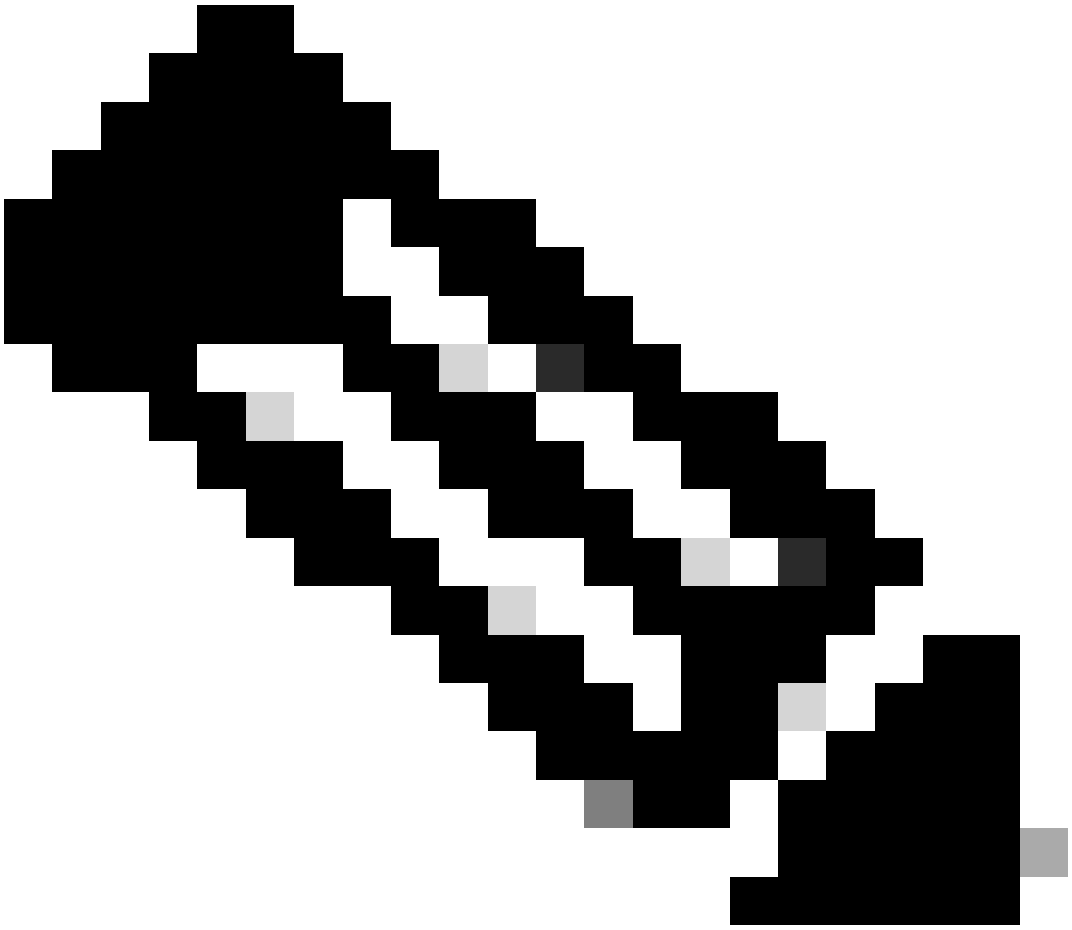
---

PacketCapture

Packet Captures is nuttig in een scenario waar een prestatiekwestie of een pakketverlies wordt gedetecteerd, of een totale stroomonderbreking voor het netwerk. De meest gebruikelijke gereedschappen om opnamen te verzamelen zijn wireshark en **tcpdump**. Of een ingebouwde mogelijkheid om cap-bestanden te verzamelen in het apparaat zelf, zoals een Cisco-firewall of router.

Om nuttige pakketopnamen op een eindpunt te verzamelen, dient u het volgende te vermelden:

1. Loopback-interface om verkeer op te nemen dat via beveiligde clientinvoegtoepassingen wordt verzonden.
2. Alle andere interfaces die betrokken zijn bij pakketpad.
3. Pas minimale filters toe, of helemaal geen filters om er zeker van te zijn dat alle gegevens worden verzameld.



Opmerking: wanneer opnamen worden verzameld op een netwerkapparaat, zorg er dan voor dat u filtert op de bron en de bestemming van het verkeer en beperk de opnamen tot alleen verwante poorten en services om te voorkomen dat prestaties door deze activiteit worden veroorzaakt.

Debuguitvoer beleid

Policy debug-uitvoer is een diagnostische uitvoer die via de gebruikersbrowser wordt verzonden wanneer deze wordt beveiligd door Secure Access. Dit bevat belangrijke informatie over de implementatie.

1. Organisatie-ID
2. Type uitzetting
3. Verbonden proxy
4. Publiek en privé IP-adres
5. Overige informatie over de bron van het verkeer.

Om de testresultaten van het beleid uit te voeren, meldt u zich aan bij deze link vanaf een beveiligd eindpunt: https://policy.test.sse.cisco.com/

Zorg ervoor dat u vertrouwt op het Secure Access Root Certificate als er een certificaatfoutmelding wordt weergegeven in uw browser.

U kunt als volgt Secure Access Root Certificate downloaden:

Navigeren naar beveiligde toegang Dashboard > Secure > Settings > Certificate > (Internet Destinations tab)

Resultaten uploaden naar Cisco-serviceaanvraag voor ondersteuning

U kunt bestanden uploaden naar de Support case via de volgende stappen:

Stap 1. Log in op SCM.

Stap 2. Klik om de case te bekijken en te editen op het casenummer of de casetitel in de lijst. De overzichtspagina van de case wordt geopend.

Stap 3. Klik op Add Files om een bestand te kiezen en het als een bijlage naar de case te uploaden. Het systeem toont het SCM File Uploader-gereedschap.

Stap 4. In het dialoogvenster Bestanden kiezen om te uploaden, sleept u de bestanden die u wilt uploaden of klikt u binnen om door uw lokale machine te bladeren voor het uploaden van bestanden.

Stap 5. Voeg een beschrijving toe en specificeer een categorie voor alle bestanden, of afzonderlijk.

Gerelateerde informatie

- **Cisco Technical Support en downloads**
- **Secure Access-documentatie en gebruikershandleiding**
- **Cisco Secure-clientsoftware downloaden**

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.