Risoluzione dei problemi e raccolta di informazioni di base per il team di supporto Secure Access

Sommario

Introduzione

Questo documento descrive le informazioni di base da raccogliere quando si lavora con il team di supporto Cisco Secure Access

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Secure Access
- Cisco Secure Client
- Acquisizione dei pacchetti tramite Wireshark e tcpdump

Componenti usati

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Quando si lavora su Cisco Secure Access, è possibile riscontrare problemi quando è necessario contattare il team di supporto Cisco o si desidera eseguire un'indagine di base sul problema e provare a esaminare i log per individuare la causa. In questo articolo viene descritto come raccogliere i log di risoluzione dei problemi di base relativi ad Accesso protetto. Si noti che non tutti i passaggi sono validi per tutti gli scenari.

Individua l'ID organizzazione di accesso sicuro

Per consentire al tecnico Cisco di individuare l'account, fornire l'ID organizzazione che si trova nell'URL una volta eseguito l'accesso al dashboard di accesso sicuro.

Passaggi per individuare l'ID organizzazione:

1. Accedi a sse.cisco.com
2. Se si dispone di più organizzazioni, passare a quella destra.
3. L'ID dell'organizzazione è disponibile nell'URL con il seguente schema: https://dashboard.sse.cisco.com/org/{7_digit_org_id}/overview

Strumento di diagnostica e reporting (DART) Cisco Secure Client

Cisco Secure Client Diagnostic and Reporting Tool (DART) è uno strumento installato con il pacchetto Secure Client che consente di raccogliere informazioni importanti sull'endpoint utente.

Esempio di informazioni raccolte dal bundle DART:

- Registri ZTNA
- Registri client sicuri e informazioni sul profilo
- System Information
- Altri plug-in o componenti aggiuntivi client sicuri installati in

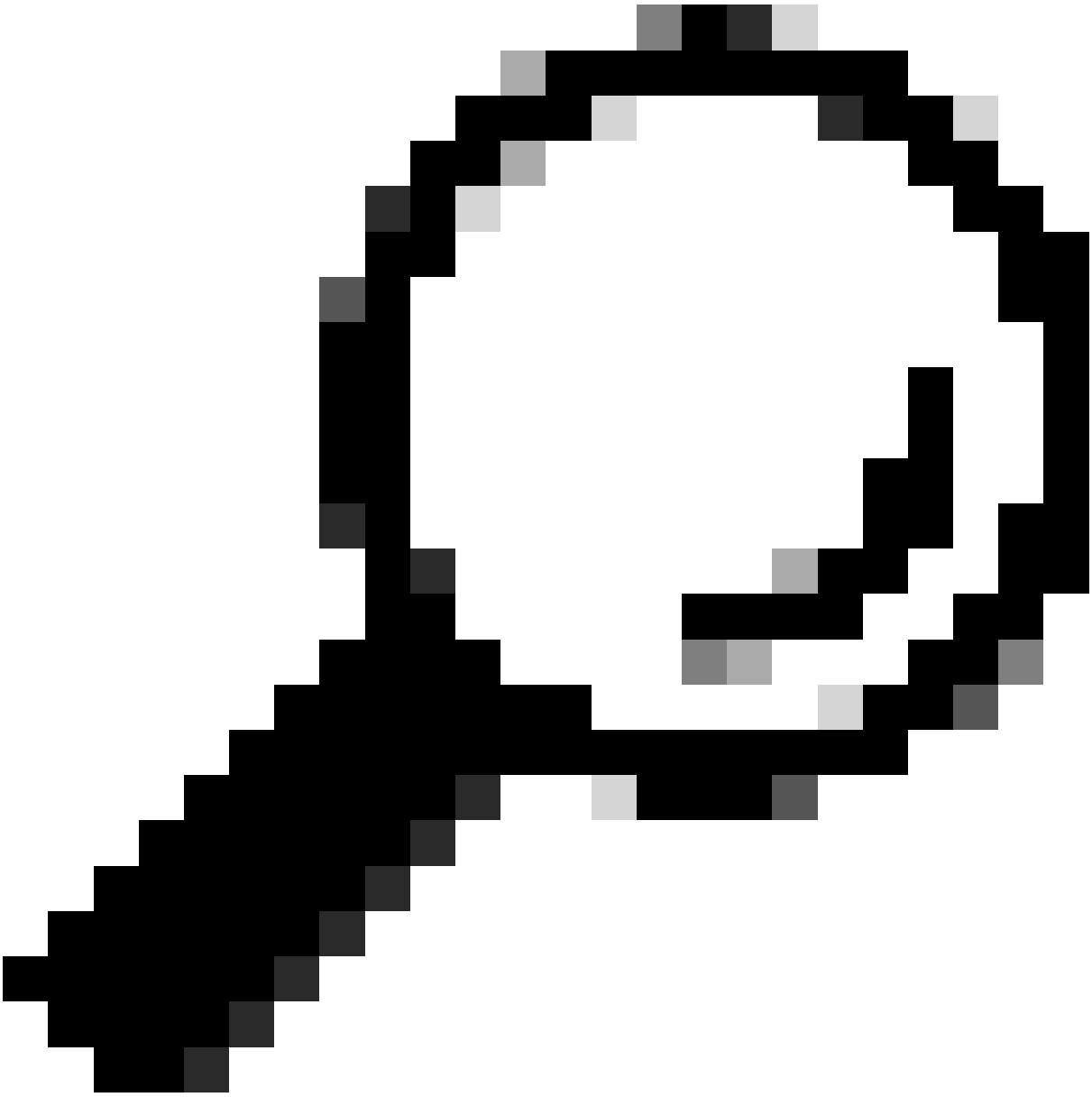
Istruzioni per la raccolta di DART:

Passaggio 1. Avviare DART.

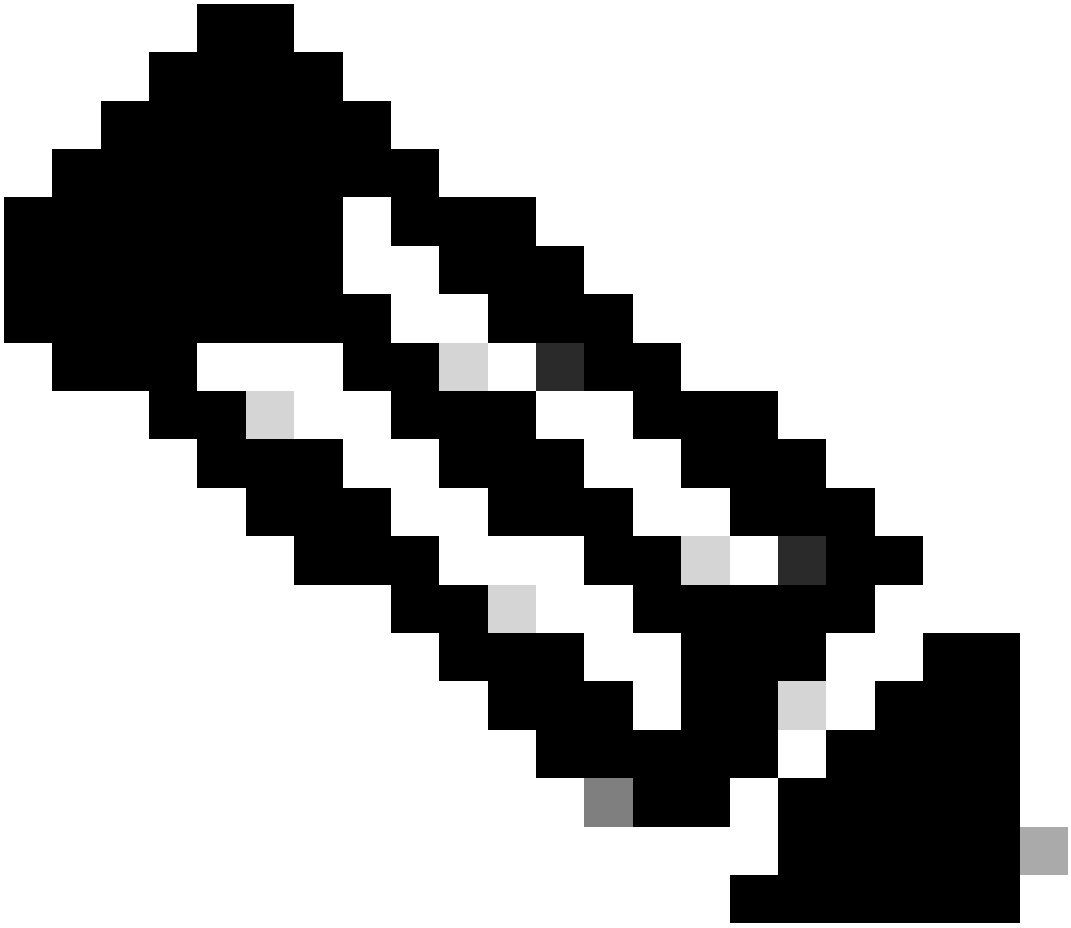
1. Per un computer Windows, avviare Cisco Secure Client.
2. Per un computer Linux, scegliere **Applications** > **Internet** > **Cisco DART**o /opt/cisco/anyconnect/dart/dartui.
3. Per un computer Mac, scegliere Applications > Cisco > Cisco DART.

Passaggio 2. Fare clic sulla scheda Statistiche e quindi su Dettagli.

Passaggio 3. Selezionate Default o Custom bundle creation.



Suggerimento: il nome predefinito del bundle è DARTBundle.zip e viene salvato sul desktop locale.



Nota: se si sceglie Predefinito, DART avvia la creazione del fascio. Se si sceglie Personalizzata, continuare la procedura guidata per specificare i registri, i file di preferenze, le informazioni di diagnostica e qualsiasi altra personalizzazione

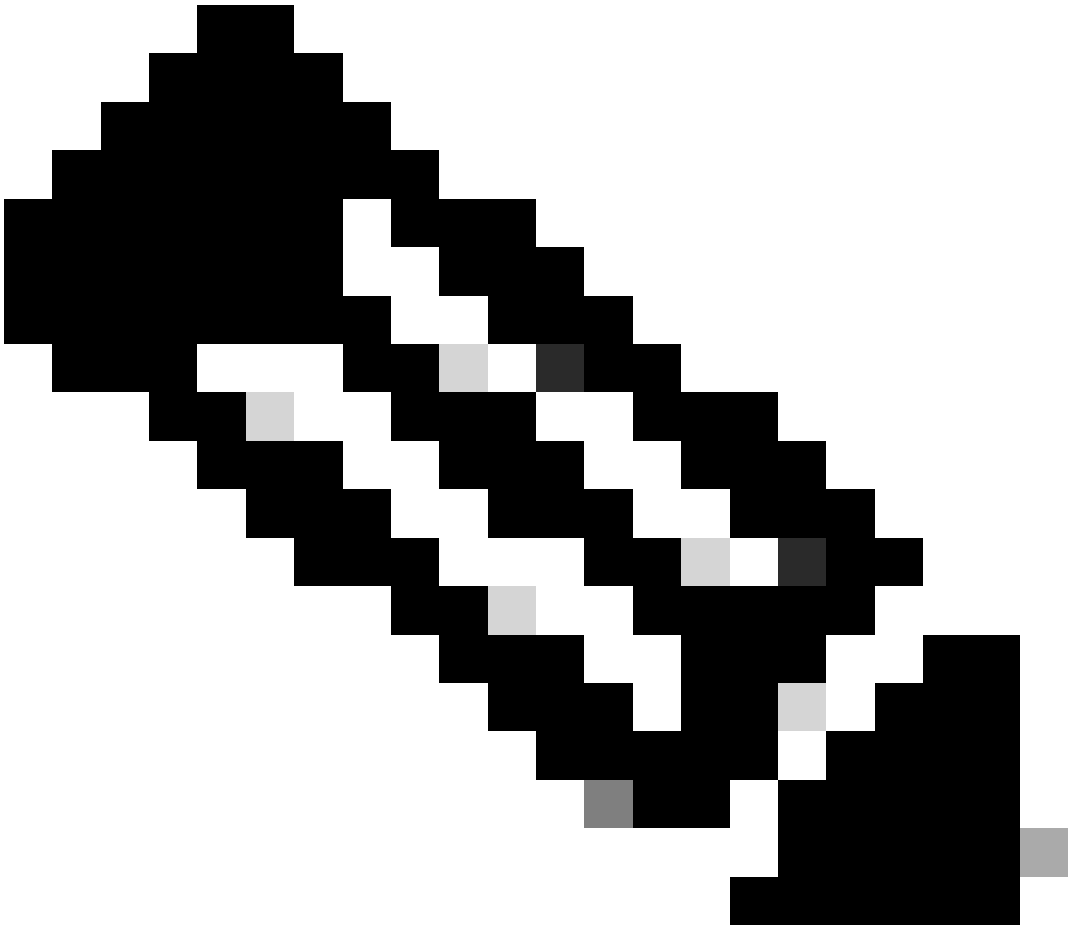
---

Acquisizioni HTTP Archive (HAR)

HAR può essere raccolto da diversi browser e fornisce più informazioni, tra cui:

1. Versione decrittografata delle richieste HTTPS.
2. Informazioni interne sui messaggi di errore, i dettagli della richiesta e le intestazioni.
3. Informazioni sui tempi e i ritardi
4. Altre informazioni varie sulle richieste basate su browser.

Per raccogliere le clip HAR, attenersi alla procedura descritta in questa fonte: https://toolbox.googleapps.com/apps/har_analyzer/



Nota: per raccogliere i dati corretti, è necessario aggiornare la sessione del browser

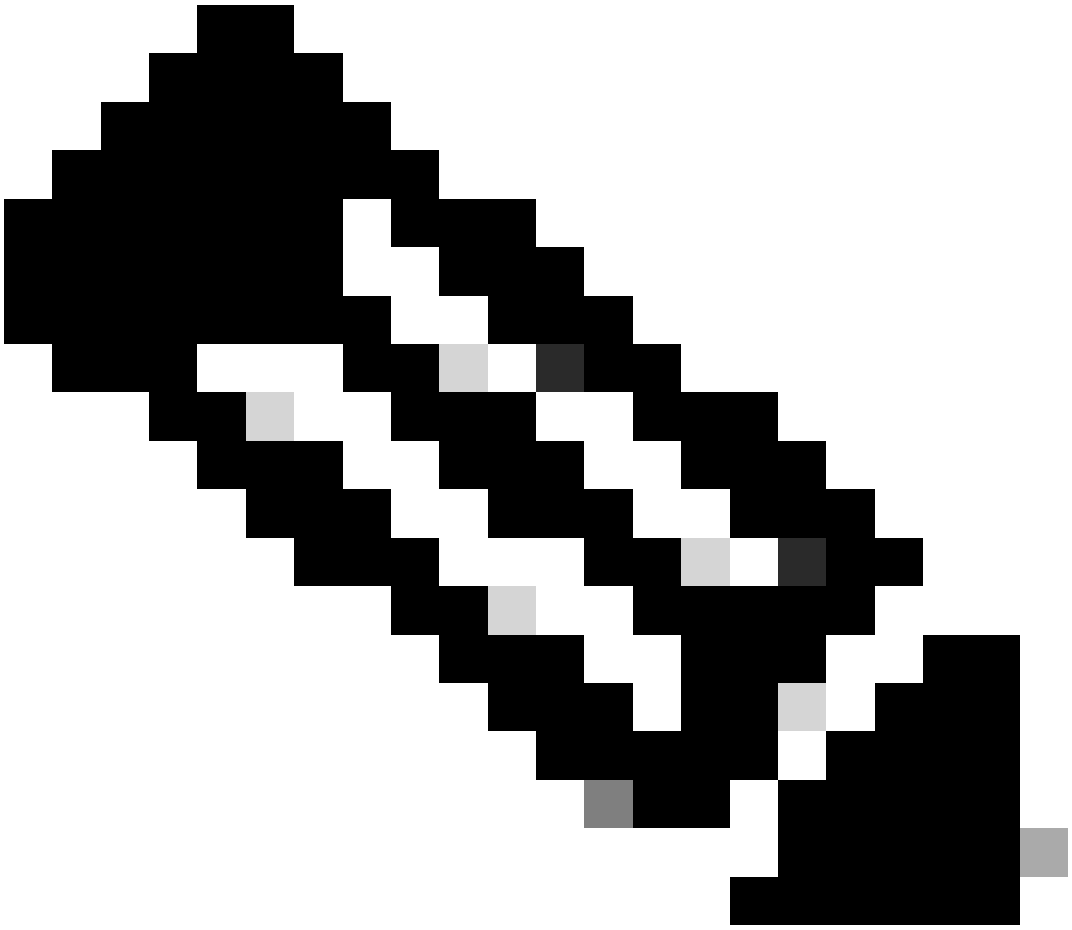
---

Acquisizioni pacchetti

L'acquisizione dei pacchetti è utile in uno scenario in cui viene rilevato un problema di prestazioni o la perdita di un pacchetto o l'interruzione totale della rete. Gli strumenti più comuni per la raccolta delle acquisizioni sono wireshark e **tcpdump**. Oppure una funzionalità incorporata per la raccolta di file in formato pcap all'interno del dispositivo stesso, ad esempio un Cisco Firewall o un router.

Per raccogliere utili acquisizioni di pacchetti su un endpoint, assicurarsi di includere:

1. Interfaccia di loopback per l'acquisizione del traffico inviato tramite i componenti aggiuntivi Secure Client.
2. Tutte le altre interfacce coinvolte nel percorso del pacchetto.
3. Applicare filtri minimi o nessun filtro per assicurarsi che tutti i dati siano raccolti.



> **Nota**: quando le clip vengono raccolte su un dispositivo di rete, accertati di filtrare in base all'origine e alla destinazione del traffico e di limitare le clip alle sole porte e ai servizi correlati, per evitare prestazioni causate da questa attività.

Output debug criteri

L'output di debug dei criteri è un output di diagnostica inviato tramite il browser utente quando protetto da Secure Access. include informazioni

critiche sulla distribuzione.

1. ID organizzazione
2. Tipo di distribuzione
3. Proxy connesso
4. Indirizzo IP pubblico e privato
5. Altre informazioni relative alla fonte del traffico.

Per eseguire i risultati del test dei criteri, accedere a questo collegamento da un endpoint protetto: https://policy.test.sse.cisco.com/

Assicurarsi di considerare attendibile il certificato radice di accesso sicuro se nel browser viene visualizzato un messaggio di errore del certificato.

Per Scaricare Il Certificato Radice Di Accesso Sicuro:

Passa ad accesso protetto Dashboard > Secure > Settings > Certificate > (Internet Destinations tab)

Caricamento Dei Risultati Nella Richiesta Del Servizio Di Supporto Cisco

È possibile caricare i file nella richiesta di assistenza eseguendo la procedura seguente:

Passaggio 1. Accedere a SCM.

Passaggio 2. Per visualizzare e modificare la richiesta, fare clic sul numero o sul titolo nell'elenco. Si apre la pagina Riepilogo della richiesta.

Passaggio 3. Per scegliere un file e caricarlo come allegato alla richiesta, fare clic su Add Files. Viene visualizzato lo strumento SCM File Uploader.

Passaggio 4. Nella finestra di dialogo Scegli file da caricare, trascinare i file che si desidera caricare o fare clic all'interno per cercare i file da caricare nel computer locale.

Passaggio 5. Aggiungere una descrizione e specificare una categoria per tutti i file o singolarmente.

Informazioni correlate

- **Supporto tecnico Cisco e download**
- **Documentazione e guida per l'utente di Secure Access**
- **Download del software Cisco Secure Client**

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).