# أستكشاف الأخطاء وإصلاحها وتجميع المعلومات الأساسية لفريق دعم الوصول الآمن

## المحتويات


المقدمة

المتطلبات الأساسية

- المتطلبات
- المكونات المستخدمة

معلومات أساسية

تحديد موقع معرف مؤسسة الوصول الآمن

أداة Cisco Secure Client Diagnostic and Reporting Tool (DART)

تمكين سجلات تصحيح الأخطاء للوحدات النمطية ZTNA و SWG

- تمكين سجلات تصحيح الأخطاء لـ ZTNA
- تمكين سجلات تصحيح الأخطاء لـ SWG
- تمكين سجلات تصحيح الأخطاء لـ DUO

تجميع سجلات KDF لـ ZTNA و SWG، وحدات DNS (في Windows)

- المتطلبات الأساسية

التقاط أرشيف HTTP (HAR)

عمليات التقاط الحزم

اخراج تصحيح أخطاء النهج

الأوامر الشائعة لاستكشاف أخطاء النفق من موقع الى موقع واصلاحها

أوامر شائعة لاستكشاف أخطاء موصل المواردواصلاحها

تحميل النتائج الى طلب خدمة الدعم من Cisco

معلومات ذات صلة


## المقدمة

يصف هذا المستند المعلومات الأساسية التي يلزم تجميعها أثناء العمل مع فريق دعم الوصول الآمن من Cisco

## المتطلبات الأساسية

### المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- Cisco Secure Access
- Cisco Secure Client

- يلتقط الحزمة من خلال Wireshark و tcpdump

### المكونات المستخدمة

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

## معلومات أساسية

أثناء العمل على Cisco Secure Access، يمكنك مواجهة المشاكل حيث تحتاج إلى الاتصال بفريق دعم Cisco، أو ترغب في إجراء تحقيق أساسي للمشكلة ومحاولة المرور عبر السجلات وإدخال المشكلة. توضح هذه المقالة كيفية تجميع سجلات أستكشاف الأخطاء وإصلاحها الأساسية المتعلقة بالوصول الآمن. لاحظ أن ليس كل الخطوات تنطبق على كل سيناريو.

## تحديد موقع معرف مؤسسة الوصول الآمن

لتحديد موقع حسابك من قبل مهندس Cisco، قم بتوفير معرف مؤسستك الذي يمكن العثور عليه في عنوان URL بمجرد تسجيل دخولك إلى لوحة معلومات الوصول الآمن.

خطوات تحديد موقع معرف المؤسسة:

1. تسجيل الدخول إلى sse.cisco.com
2. إذا كان لديك عدة مؤسسات، فعليك التبديل إلى المؤسسات المناسبة.
3. يمكن العثور على معرف المؤسسة في عنوان URL في هذا النمط:
https://dashboard.sse.cisco.com/org/{7_digit_org_id}/قمة قرظن

## أداة Cisco Secure Client Diagnostic and Reporting Tool (DART)

أداة Cisco Secure Client Diagnostic and Reporting Tool (DART) هي أداة يتم تثبيتها مع حزمة Secure Client، تساعد على تجميع معلومات مهمة حول نقطة نهاية المستخدم.

مثال للمعلومات التي تم تجميعها بواسطة حزمة DART:

- سجلات ZTNA
- تأمين سجلات العميل ومعلومات ملف التعريف
- معلومات النظام
- سجلات ملحقات أو ظائف إضافية أخرى مؤمنة للعملاء مثبتة على

إرشادات تجميع DART:

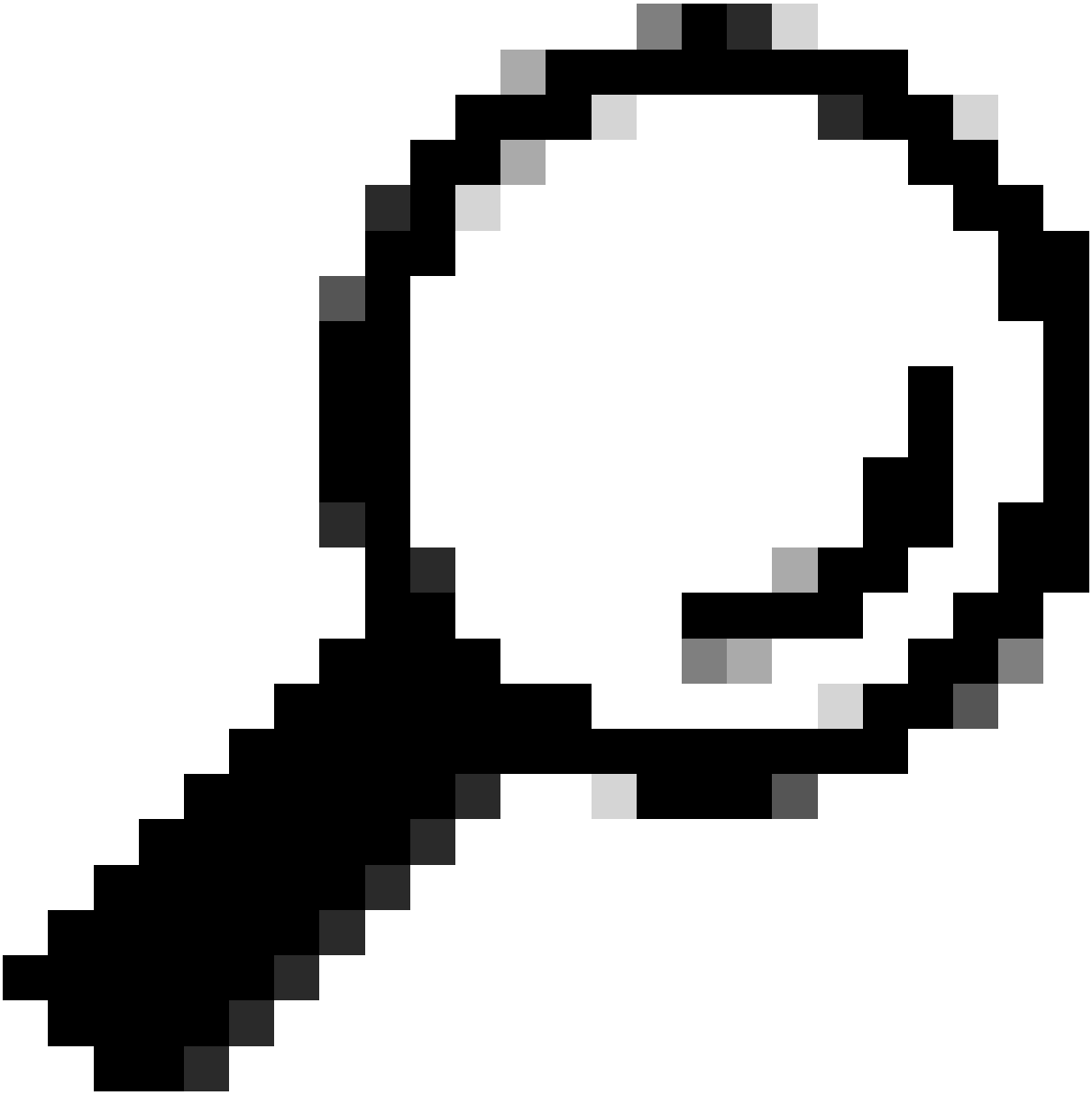
الخطوة 1. بدء تشغيل DART.

1. لكمبيوتر Windows، قم بتشغيل Cisco Secure Client.
2. بالنسبة لكمبيوتر Linux، أختر **Applications** > **Internet** > **Cisco DART**أو /opt/cisco/anyconnect/dart/dartui.
3. لكمبيوتر Mac، أخترApplications > Cisco > Cisco DART.

الخطوة 2. انقر فوق علامة التبويب "إحصائيات" ثم انقر فوق "تفاصيل".

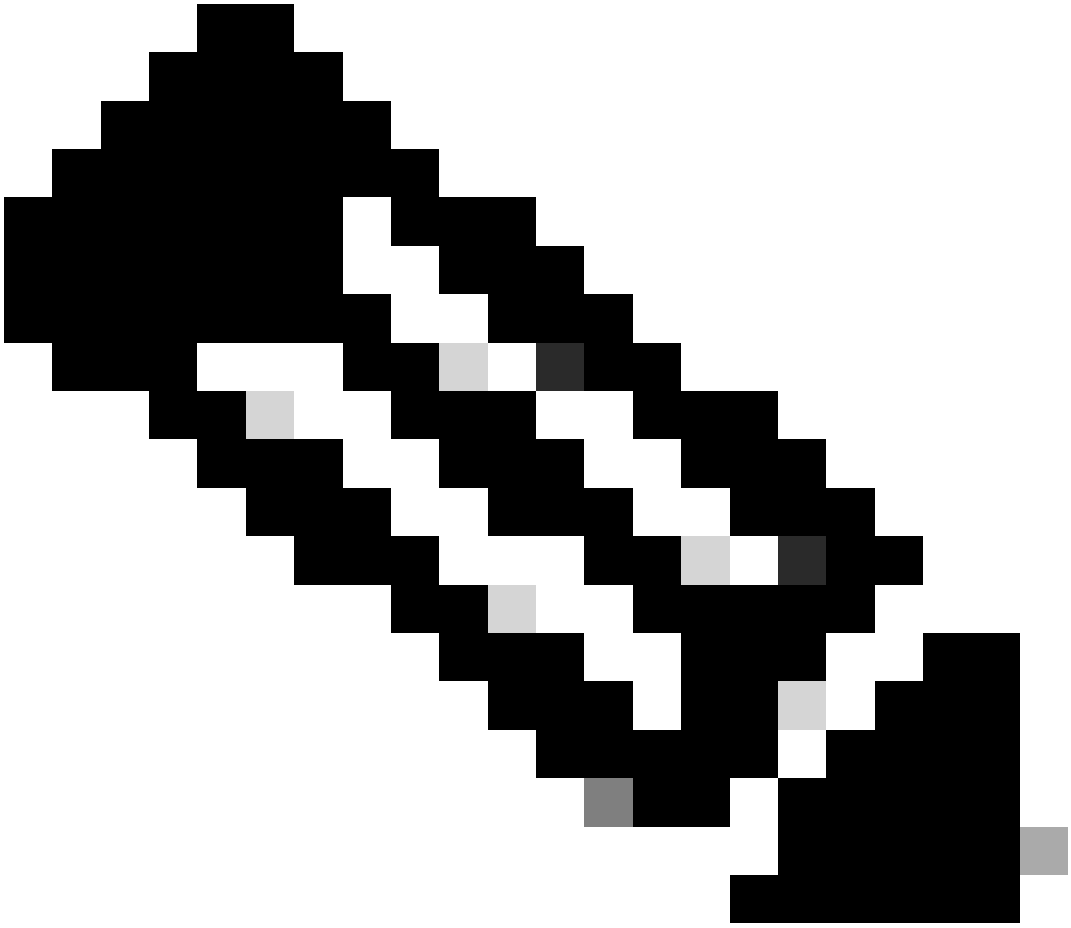
الخطوة 3. أختر إنشاء الحزمة الافتراضية أو المخصصة.

---



تلميح: الاسم الافتراضي للحزمة هو DARTBundle.zip، ويتم حفظه إلى سطح المكتب المحلي.

---



ملاحظة: إذا أخترت الافتراضي، يبدأ DART في إنشاء الحزمة. إذا أخترت مخصص، قم بمتابعة مطالبات المعالج لتحديد السجلات وملفات التفضيلات ومعلومات التشخيص وأي تخصيصات أخرى

## تمكين سجلات تصحيح الأخطاء للوحدات النمطية ZTNA و SWG

في بعض السيناريوهات يتطلب فريق دعم السيناريوهات تمكين سجلات مستوى التتبع وأ تصحيح الأخطاء من أجل تحديد المشاكل الأكثر تعقيدا.

أكمل الخطوات الواردة في هذا القسم لتمكين تصحيح الأخطاء لكل وحدة نمطية.

### تمكين سجلات تصحيح الأخطاء ل ZTNA

الخطوة 1. قم بإنشاء ملف json باسم logconfig.json

الخطوة 2. أدخل هذا النص داخل الملف

```
{ "global": "DBG_TRACE" }
```

الخطوة 3. ضع الملف في الدليل الصحيح استنادا إلى نظام التشغيل

- Windows: C:\ProgramData\Cisco\CiscoSecure Client\ZTA
- نظام التشغيل MacOS: /opt/cisco/secureclient/zta

الخطوة 4. قم بإعادة تشغيل وحدة ZTNA النمطية أو Cisco Secure Client لتأثير السجلات.

## تمكين سجلات تصحيح الأخطاء ل SWG

الخطوة 1. أنشئ ملف json باسم SWGConfigOverride.json

الخطوة 2. أدخل هذا النص داخل الملف

```
{"logLevel": "1"}
```

الخطوة 3. ضع الملف في الدليل الصحيح استنادا إلى نظام التشغيل

- Windows: C:\ProgramData\Cisco\Cisco Secure Client\Umbrella\SWG\
- نظام التشغيل MacOS: /opt/cisco/secureclient/umbrella/swg

الخطوة 4. قم بإعادة تشغيل وحدة SWG النمطية أو Cisco Secure Client لتأثير السجلات.

## تمكين سجلات تصحيح الأخطاء ل DUO

إتاحة سجلات KDF الثنائية ( أستكشاف أخطاء الوضع وإصلاحها، مشاكل التسجيل)

```
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Duo\Duo Device Health” /v verbose_logging_enabled /d 1 /f
```

قم بتعطيل سجلات KDF الثنائية

```
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Duo\Duo Device Health” /v verbose_logging_enabled /d 0 /f
```

# تجميع سجلات KDF ل ZTNA و SWG، وحدات DNS (في Windows)

في بعض السيناريوهات يتطلب فريق دعم مجموعة مثل تلك السيناريوهات جمع سجلات kdf من أجل التعرف على المشاكل الأكثر تعقيدا.

أتمت ال steps يزوي في اذه قسم أن يشكل وجمع ال kdf سجل.

## المتطلبات الأساسية

يلزم تثبيت DebugView لتجميع السجلات بشكل صحيح. الذي يمكن تثبيته باستخدام المصدر اذه: https://learn.microsoft.com/en-us/sysinternals/downloads/debugview

تمكين مفتاح تسجيل DNS

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\acsock" /v DebugFlags /d 0x20801FF /t reg
```

تمكين مفتاح تسجيل SWG

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\acsock" /v DebugFlags /d 0x70C01FF /t reg
```

تمكين مفتاح تسجيل ZTNA

```
"%ProgramFiles(x86)%\Cisco\Cisco Secure Client\acsocktool.exe" -sdf 0x40018EF52
```

تعطيل كافة العلامات

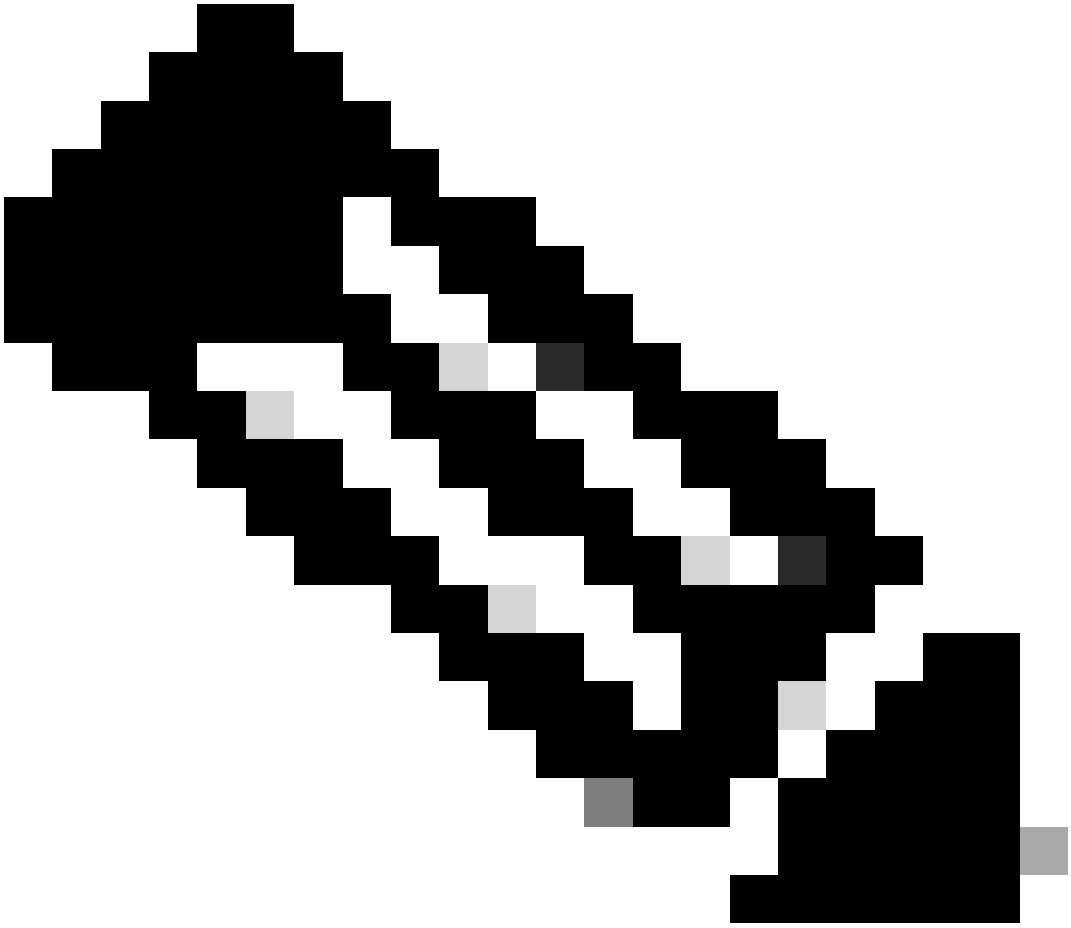
```
"%ProgramFiles(x86)%\Cisco\Cisco Secure Client\acsocktool.exe" -cdf
```

# التقاط أرشيف HTTP (HAR)

يمكن جمع HAR من مستعرضات مختلفة. وهو ويوفر معلومات متعددة تتضمن:

1. إصدار طلبات HTTPS التي تم فك تشفيرها.
2. معلومات داخلية حول رسائل الخطأ وتفاصيل الطلب والرؤوس.
3 - معلومات التوقيت والتأخير
4 - معلومات متنوعة أخرى عن الطلبات القائمة على المستعرض.

لتجميع التقاط HAR، يرجى إستخدام الخطوات الموضحة في اذه المصدر:
https://toolbox.googleapps.com/apps/har_analyzer/



ملاحظة: تحتاج إلى تحديث جلسة عمل المستعرض لتجميع البيانات الصحيحة

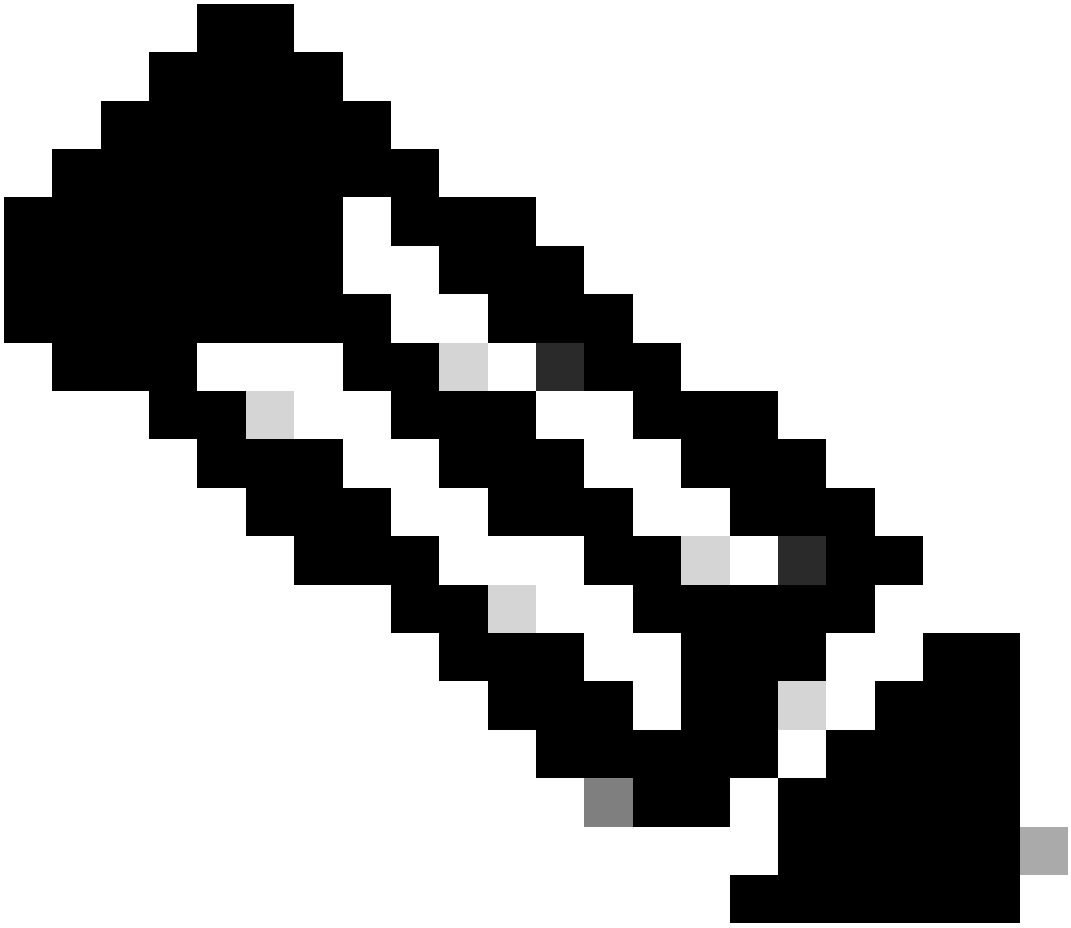
---

# عمليات التقاط الحزم

تكون حزم الالتقاط مفيدة في سيناريو حيث يتم اكتشاف مشكلة في الأداء أو فقدان حزمة، أو انقطاع إجمالي للشبكة. أكثر الأدوات شيوعا لجمع الالتقاط هي**tcpdump** وwireshark. أو إمكانية مضمنة لتجميع تنسيق ملفات PCAP ضمن الجهاز نفسه، مثل جدار حماية Cisco أو الموجه.

لتجميع التقاط حزم مفيد على نقطة نهاية، الرجاء التأكد من تضمين:

1. واجهة الاسترجاع الالتقاط حركة مرور البيانات المرسلة من خلال الوظائف الإضافية الخاصة بالعميل الآمن.
2. جميع الواجهات الأخرى المعنية في مسار الحزمة.
3. تطبيق الحد الأدنى من عوامل التصفية، أو عدم وجود عوامل تصفية على الإطلاق للتأكد من تجميع جميع البيانات.



ملاحظة: عند تجميع عمليات الالتقاط على جهاز شبكة، تأكد من التصفية على مصدر حركة المرور ووجهتها، وحدد عمليات الالتقاط بالمنافذ والخدمات ذات الصلة فقط، لتجنب أي أداء يتسبب فيه هذا النشاط.

## إخراج تصحيح أخطاء النهج

إخراج تصحيح أخطاء النهج هو إخراج تشخيصي يتم إرساله من خلال مستعرض المستخدم عند حمايته بواسطة Secure Access. والتي تتضمن معلومات حساسة حول عملية النشر.

1. معرف المؤسسة
2. نوع النشر
3. الوكيل المتصل
4. عنوان بروتوكول الإنترنت العام والخاص
5. معلومات أخرى متعلقة بمصدر حركة المرور.

لتشغيل نتائج إختبار النهج، الرجاء تسجيل الدخول إلى هذا الارتباط من نقطة نهاية محمية: https://policy.test.sse.cisco.com/

يرجى التأكد من أنك تثق بشهادة جذر الوصول الآمن في حالة تقديم رسالة خطأ شهادة في المستعرض الخاص بك.

لتنزيل شهادة جذر الوصول الآمن:

انتقل إلى الوصول الآمن Dashboard > Secure > Settings > Certificate > (Internet Destinations tab)

# الأوامر الشائعة لاستكشاف أخطاء النفق من موقع إلى موقع وإصلاحها

<#root>

**# Tunnel Establishment**

asa>show crypto ikev1 sa
asa>show crypto ikev2 sa
asa>show crypto ipsec sa
asa>show crypto session

**#BGP Troubleshooting**

asa>show running-config router bgp
asa>show bgp summary
asa>show ip bgp neighbors

**#Routes Advertisements**

asa>show bgp ipv4 unicast neighbors <sse-dc-ip> advertised-routes
asa>show bgp ipv4 unicast neighbors <sse-dc-ip> received-routes
asa>show bgp ipv4 unicast neighbors <sse-dc-ip> routes

**#Debug BGP events**

asa>debug ip bgp
asa>debug ip bgp events
asa>debug ip bgp updates
asa>debug ip routing

**#Disable Debugs**

asa>undebug all

# أوامر شائعة لاستكشاف أخطاء موصل الموارد وإصلاحها

توفر القائمة المقدمة طريقة عرض شاملة حول موصل الموارد وتفاصيل استكشاف

الأخطاء وإصلاحها الهامة لفريق دعم الوصول الآمن

<#root>

**#DNS and connectivity tests on the local IP address, gateway, Secure Access APIs**

rc-cli> diagnostic

**#Software version, VPN tunnel state, system health, sysctl settings, routes and iptables**

rc-cli> techsupport

**#Packet captures**

rc-cli> tcpdump <host>

## تحميل النتائج إلى طلب خدمة الدعم من Cisco

يمكنك تحميل الملفات إلى حالة الدعم من خلال الخطوات التالية:

الخطوة 1. سجل الدخول إلى SCM.

الخطوة 2. لعرض الحالة وتحريرها، انقر فوق رقم الحالة أو عنوان الحالة في القائمة. يتم فتح صفحة ملخص الحالة.

الخطوة 3. انقر فوق إضافة الملفات لاختيار ملف وتحميله كمرفق بالحالة. يعرض النظام أداة تحميل ملف SCM.

الخطوة 4. في مربع الحوار أختر ملفات لتحميلها، اسحب الملفات التي تريد تحميلها أو انقر داخلها لاستعراض الجهاز المحلي الخاص بك بحثا عن الملفات التي تريد تحميلها.

الخطوة 5. أضف وصفا وحدد فئة لكل الملفات، أو بشكل فردي.

## معلومات ذات صلة

- الدعم الفني والتنزيلات من Cisco
- وثائق الوصول الآمن ودليل المستخدم
- تنزيل برنامج Cisco Secure Client

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).