Secure Accessサポートチームの基本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)で作業しているとき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 Client
- WiresharkおよびtcpdumpによるパケットキャプチャA

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の操作中に、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特定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を収集する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

シスコエンジニアがアカウントを検索できるように、セキュアアクセスダッシュボードにログインした後のURLに表示される組織IDを入力します。

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、正しい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を収集するのに役立ちます。

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：

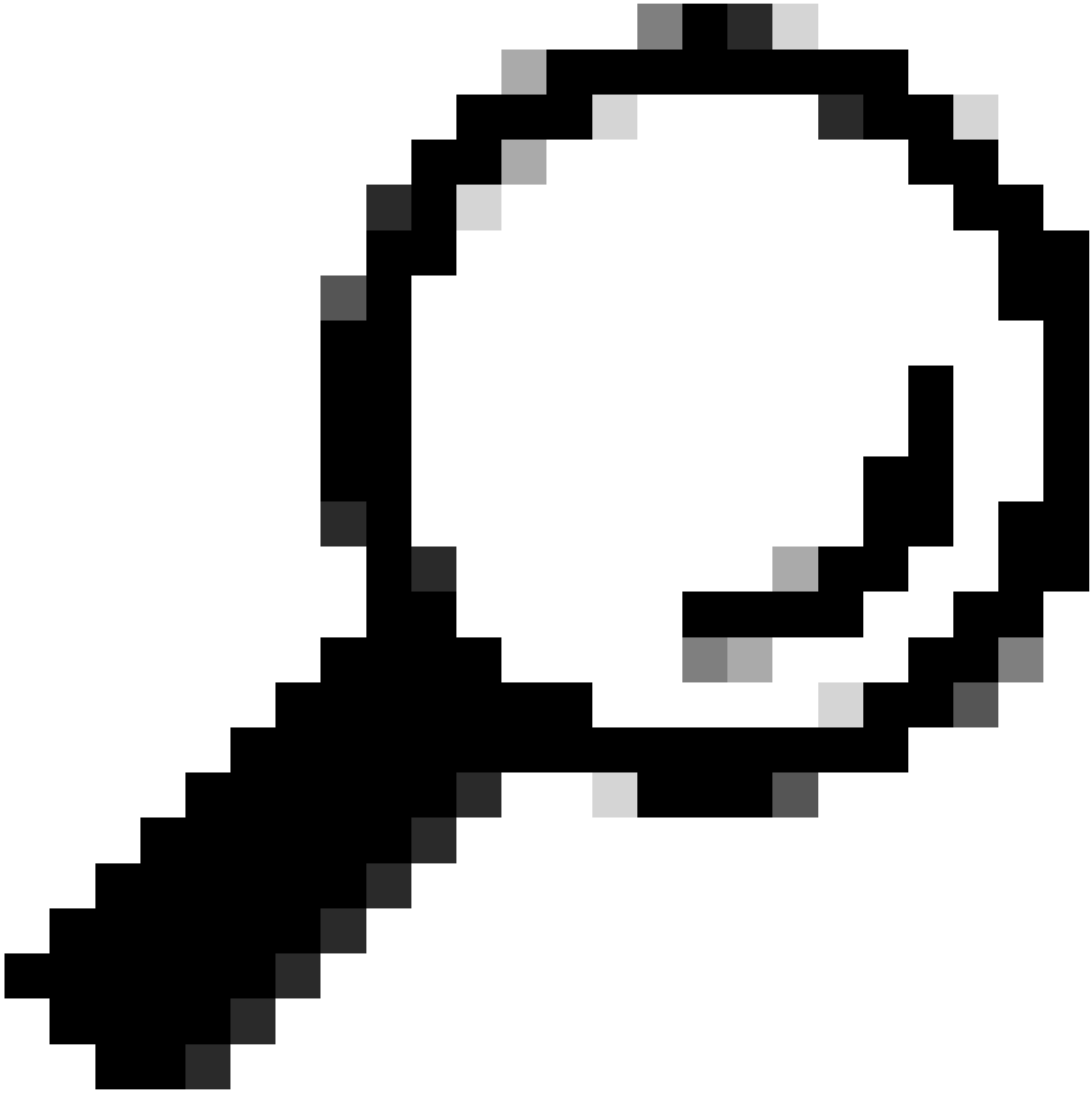
ステップ 1：DARTを起動します。

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

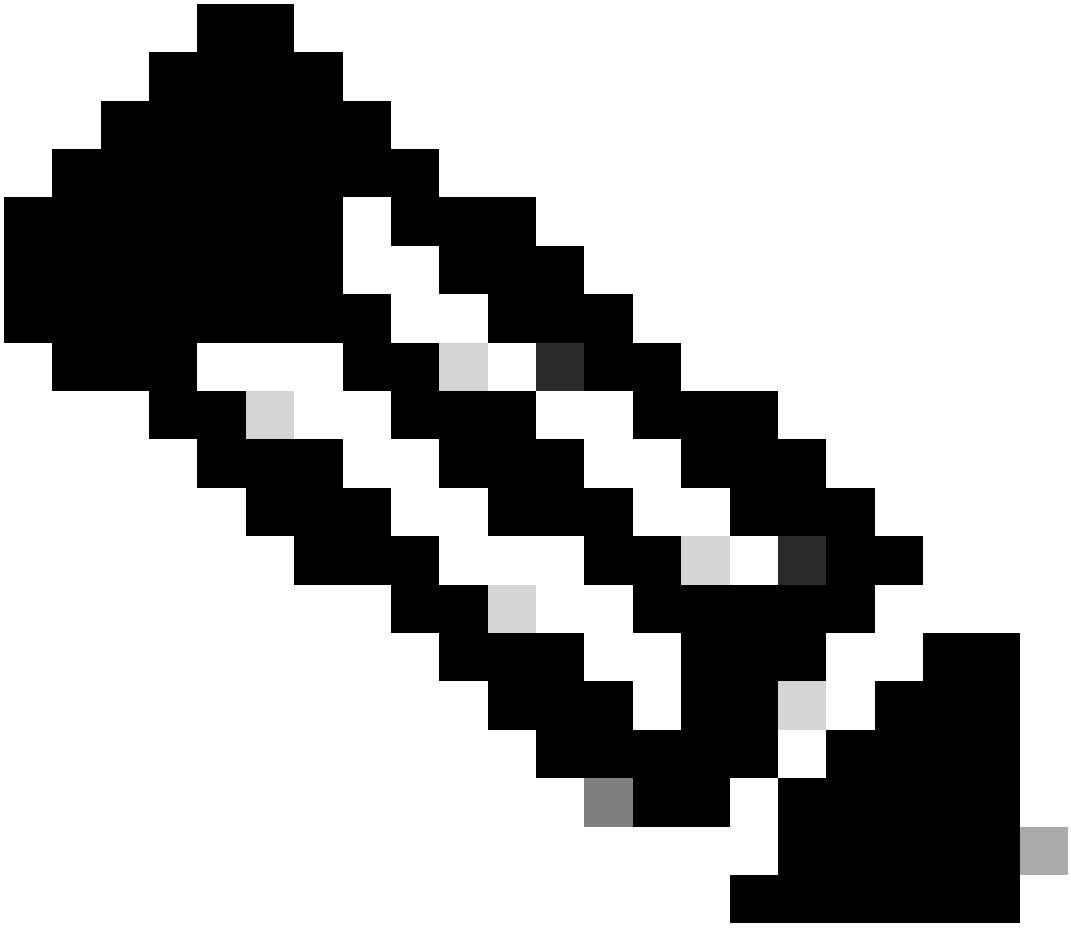
/opt/cisco/anyconnect/dart/dartuiを選択します。
3. Macコンピュータの場合は、 Applications > Cisco > Cisco DARTを選択します。

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：DefaultまたはCustom bundle creation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

ZTNAおよびSWGモジュールのデバッグログの有効化

一部のシナリオでは、サポートチームがより複雑な問題を特定するために、トレースレベルまたはデバッグレベルのログを有効にする必要があります。

各モジュールのデバッグを有効にするには、このセクションで説明する手順を実行します。

ZTNAのデバッグログの有効化

ステップ 1：logconfig.jsonという名前でjsonファイルを作成します。

ステップ 2：このテキストをファイル内に入力します

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

ステップ 3：オペレーティングシステムに基づいて適切なディレクトリにファイルを配置する

- Windowsの場合：C:\ProgramData\Cisco\Cisco Secure Client\ZTA
- MacOS:/opt/cisco/secureclient/zta

ステップ 4：ZTNAモジュールまたはCisco Secure Clientを再起動して、ログを有効にします。

SWGのデバッグログの有効化

ステップ 1： SWGConfigOverride.jsonという名前のjsonファイルを作成します。

ステップ 2：このテキストをファイル内に入力します

```
{"logLevel": "1"}□
```

ステップ 3：オペレーティングシステムに基づいて適切なディレクトリにファイルを配置する

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

ステップ 4：ログを有効にするには、SWGモジュールまたはCisco Secure Clientを再起動します。

DUOのデバッグログの有効化

DUO KDFログを有効にする（ポスチャのトラブルシューティング、登録の問題）

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

DUO KDFログを無効にする

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

ZTNAおよびSWGのKDFログ、DNSモジュールの収集(Windows)

一部のシナリオでは、サポートチームがより複雑な問題を特定するためにkdfログを収集する必要があります。

kdfログを設定および収集するには、このセクションで説明する手順を実行します。

前提条件

ログを適切に収集するには、DebugViewのインストールが必要です。このログは、次のソースを使用してインストールできます。https://learn.microsoft.com/en-us/sysinternals/downloads/debugview

DNSレジストリキーの有効化

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

SWGレジストリキーの有効化

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

ZTNAレジストリキーの有効化

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

すべてのフラグを無効にする

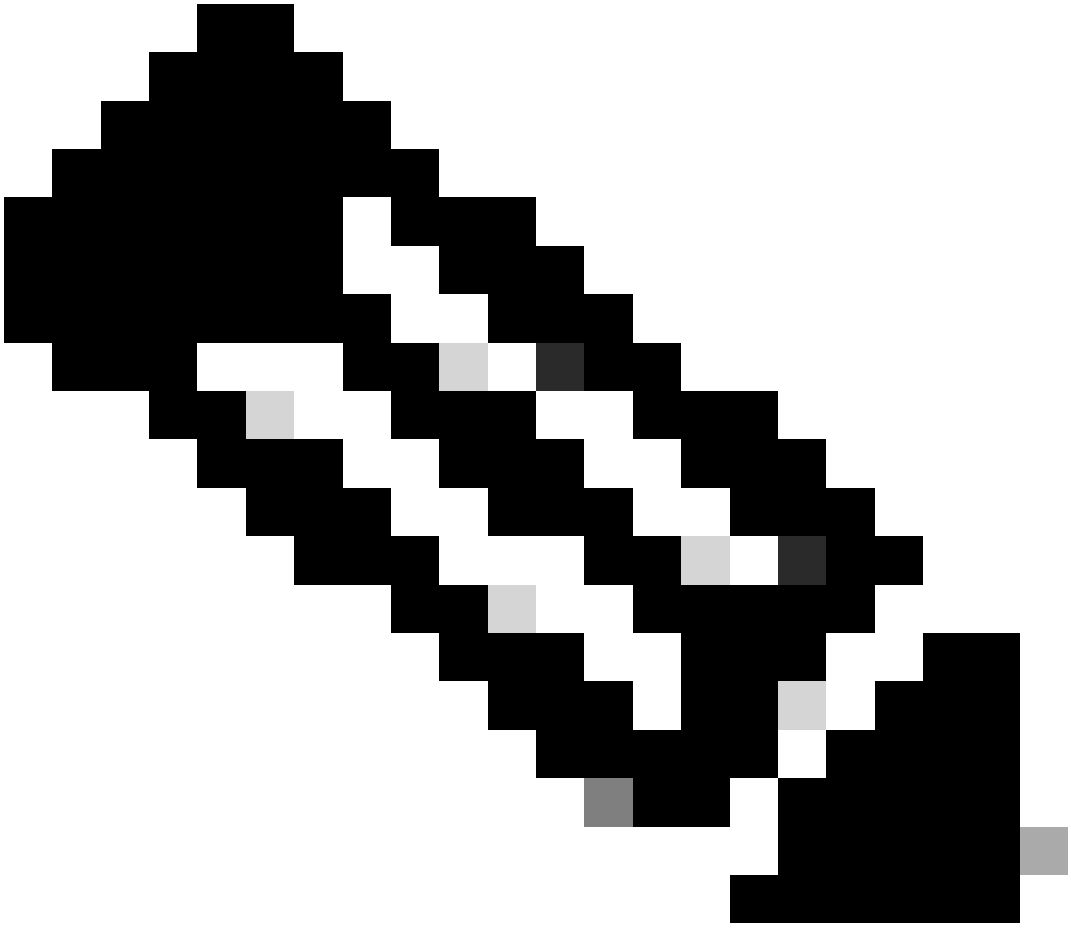
```
"%ProgramFiles(x86)%\Cisco\Cisco Secure Client\acsocktool.exe" -cdf
```

HTTPアーカイブ(HAR)キャプチャ

HARはさまざまなブラウザから収集でき、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、ヘッダーに関する内部情報。
3. タイミング及び遅延に関する情報
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、次のソースに記載されている手順を使用してください。
https://toolbox.googleapps.com/apps/har_analyzer/



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

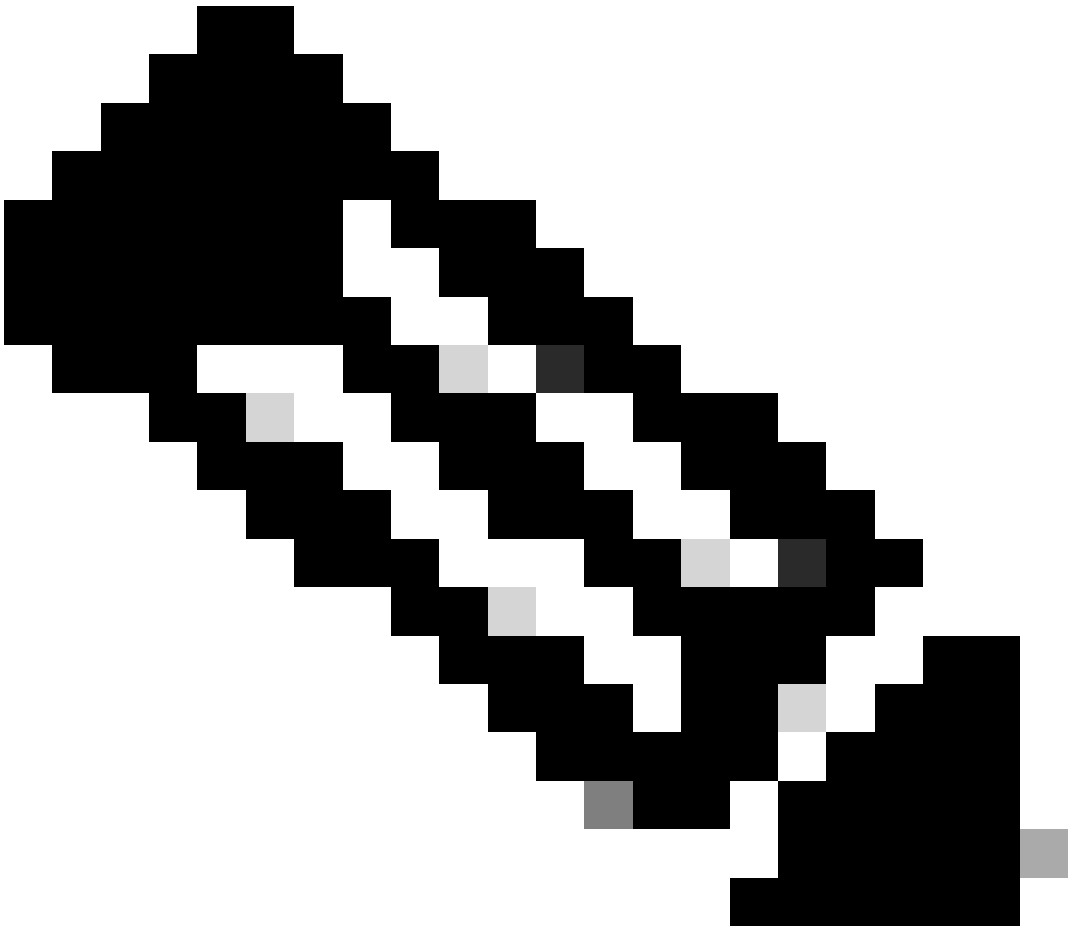
パケット キャプチャ

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、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と**tcpdump**です。または、Ciscoファイアウォールやルータなど、デバイス自体の内部で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た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. すべてのデータが確実に収集されるように、最小限のフィルタを適用するか、全くフィルタを

適用しない。



注：ネットワークデバイスでキャプチャが収集される際、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、このアクティビティによるパフォーマンスの発生を防いでください。

ポリシーのデバッグ出力

ポリシーデバッグ出力は、Secure Accessによって保護されている場合にユーザーブラウザーから送信される診断出力です。これには、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。

ブラウザに証明書のエラーメッセージが表示される場合は、セキュアアクセスのルート証明書を信頼してください。

セキュアアクセス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)

一般的なコマンドサイト間トンネルのトラブルシューティング

<#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
```

一般的なコマンドリソースコネクタのトラブルシューティング

提供されるリストには、リソースコネクタに関する包括的なビューと、Secure Access Support Teamの重要なトラブルシューティングの詳細が記載されています

<#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>

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の選択]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
- Secure Access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。