SNAでのテレメトリ取り込み用のNetFlow/IPFIXの設定

内容

はじめに

このドキュメントでは、Secure Network Analytics(SNA)がテレメトリ取り込みに必要とするNetflow/IPFIXのベストプラクティスと基本設定について説明します。

前提条件

- Cisco SNAの知識
- NetFlow/IPFIXの知識

要件

- 7.2.1以降のSecure Network Analytics
- 7.2.1以降のフローコレクタ
- フローコレクタへのルートとしてのCLIアクセス

使用するコンポーネント

- これは、ネットワーク設計と、NetFlow/IPFIXをSecure Network Analyticsに送信するために選択したデバイスに完全に依存します。NetFlow/IPFIXの設定は各エクスポータで異なります。詳細な設定については、各エクスポータのサポートチームに問い合わせてください。

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

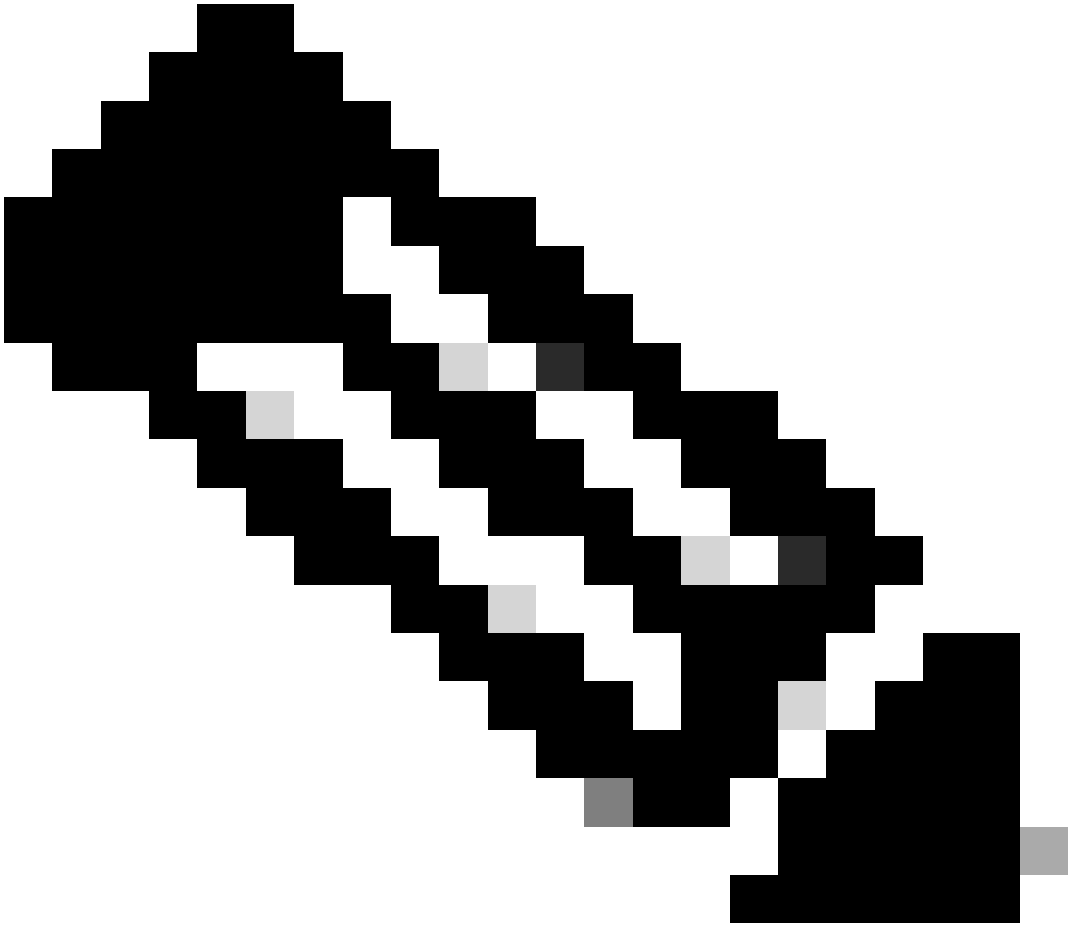
フローコレクタは、Secure Network Analyticsに送信されるフローの収集、処理、および保存を担当するSNAアプライアンスです。NetFlowバージョン9またはIPFIXの場合、ネットワークトラフィックに関連する情報を追加するためにNetFlow/IPFIXテンプレートにいくつかのフィールドを含めることができますが、Flow Collectorがこれらのフローを処理するためにNetFlow/IPFIXテンプレートに含める必要がある特定のフィールドが9つあります。フローコレクタは、無効なテンプレートを含む着信フローを処理しません。そのため、SNAはWeb UIまたはデスクトップクライアントでこれらのエクスポータのフロー情報を表示しません。

設定

必須フィールド

次のフィールドは、テレメトリ取り込み用のNetFlow/IPFIXテンプレートに含める必要があります。Secure Network Analyticsで着信フローを処理するために、これら9つのフィールドがNetFlow/IPFIXテンプレートに含まれていることを確認します。

- 送信元 IP アドレス
- 宛先 IP アドレス
- 送信元ポート
- 宛先ポート
- レイヤ3プロトコル
- バイト数
- パケット数
- フロー開始時間
- フロー終了時間



注:NetFlow/IPFIX設定には他のフィールドを含めることもできますが、前述のフィールドはSecure Network Analytics for Telemetry Ingestの最小要件です。

推奨フィールド

インターフェイス情報に関する情報を収集するために、NetFlow/IPFIXテンプレートに次のフィールドを含めることをお勧めします。この設定は、名前や速度などのインターフェイス情報を表示するために必要です。

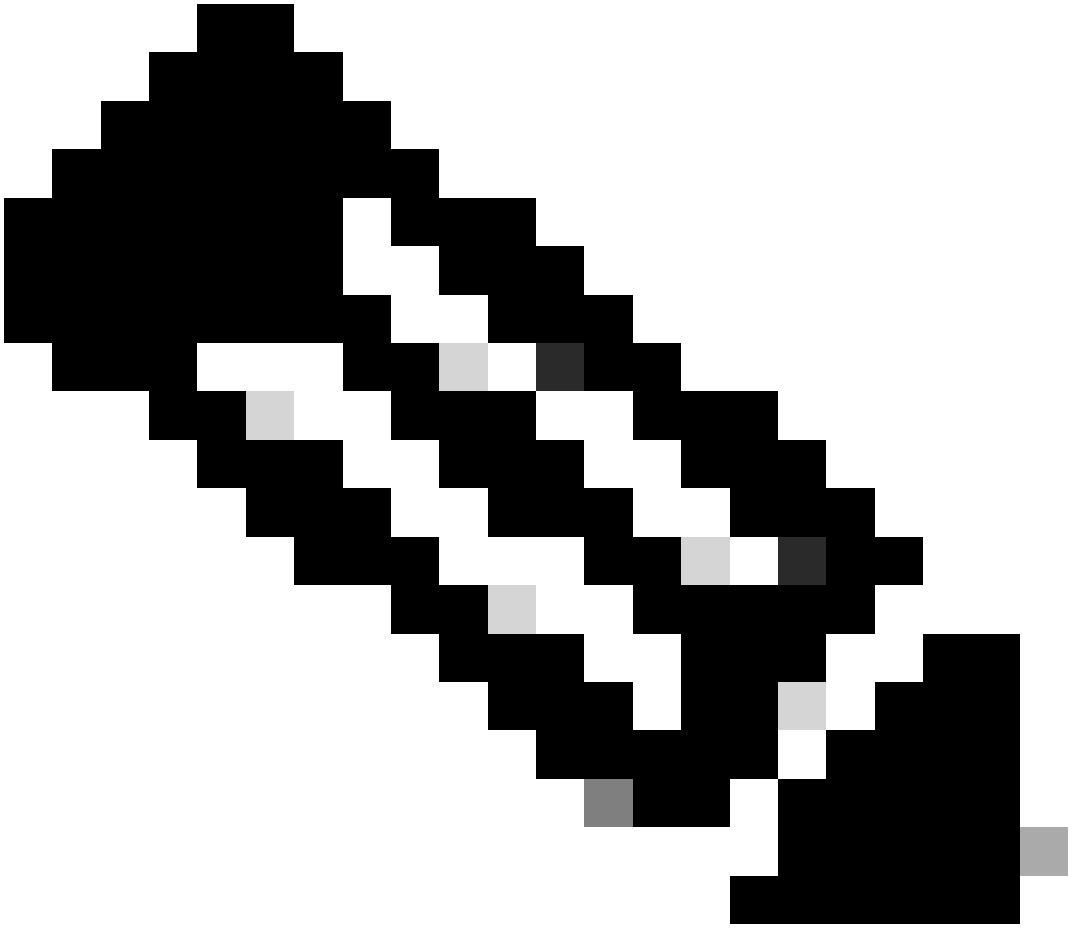
- インターフェイス入力
- インターフェイス出力

ベスト プラクティス

また、Secure Network Analyticsを適切に実行するためのベストプラクティスとして、次の設定を推奨します。

- アクティブタイムアウトを60秒に設定

- 非アクティブタイムアウトを15秒に設定
- テンプレートのタイムアウトを30秒に設定する



注:NetFlowのデフォルトポートは2055ですが、別のポートを選択することもできます。フローコレクタでのlc-astプロセスでは、必ず同じポートを使用してください。

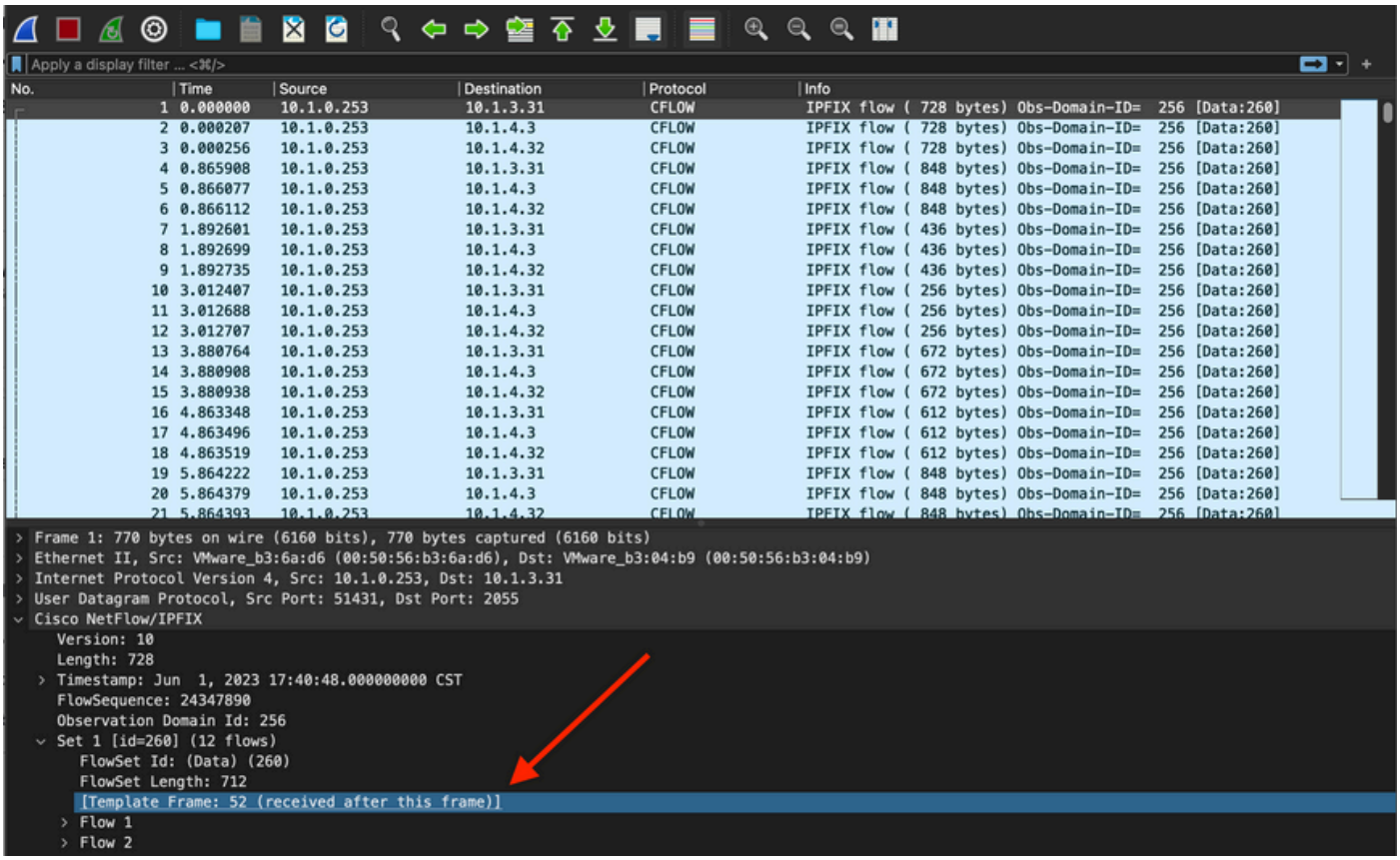
確認

NetFlow/IPFIXテンプレートの設定を検証するために、エクスポータとフローコレクタ間でパケットキャプチャを実行できます。SSH経由でrootユーザを使用してフローコレクタにログインし、次のコマンドを実行します。

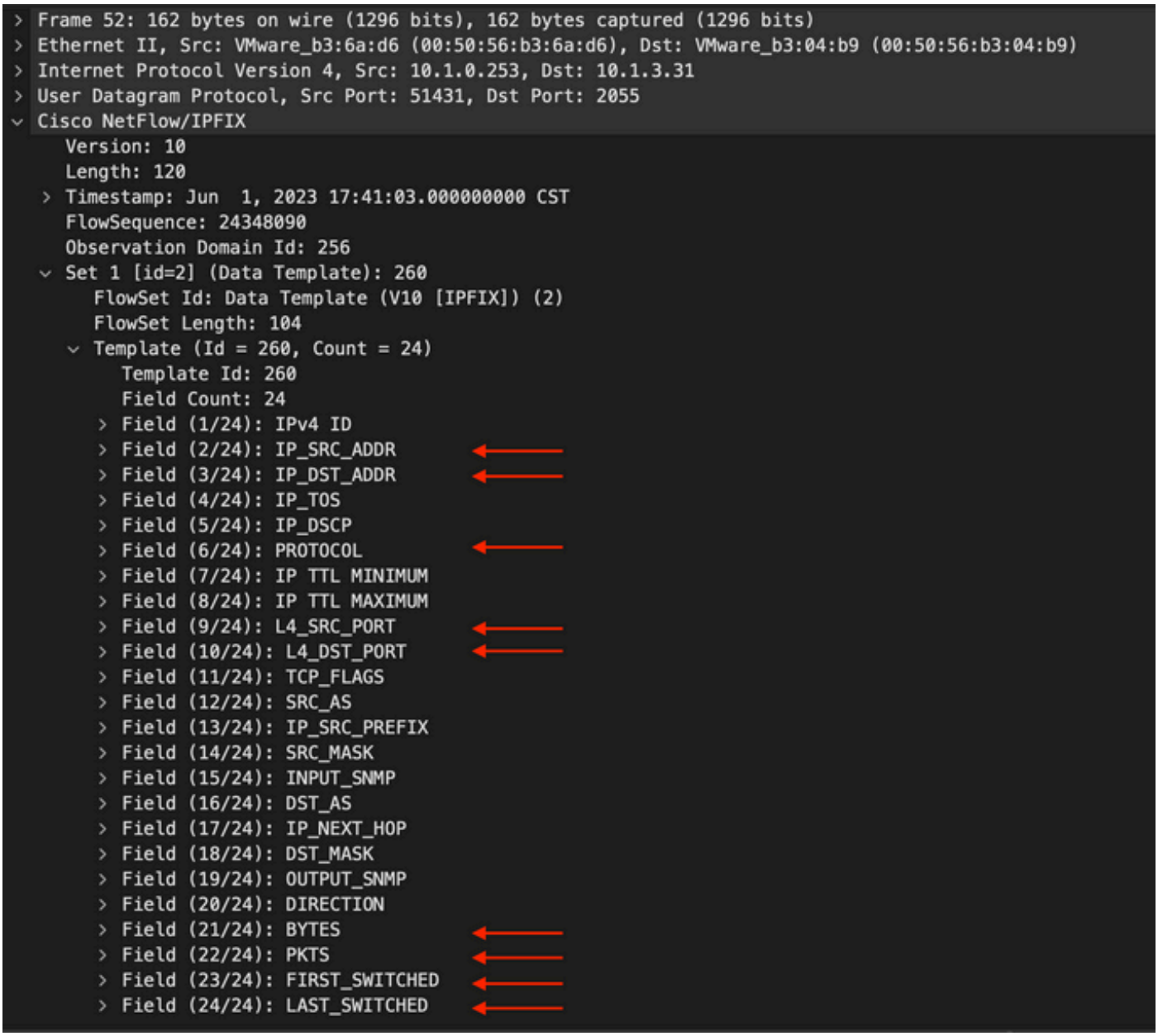
```
tcpdump -nli [Collecting_Interface] host [Exporter_IP_Address] and port [NetFlow_Port] -w /lancope/var/
```

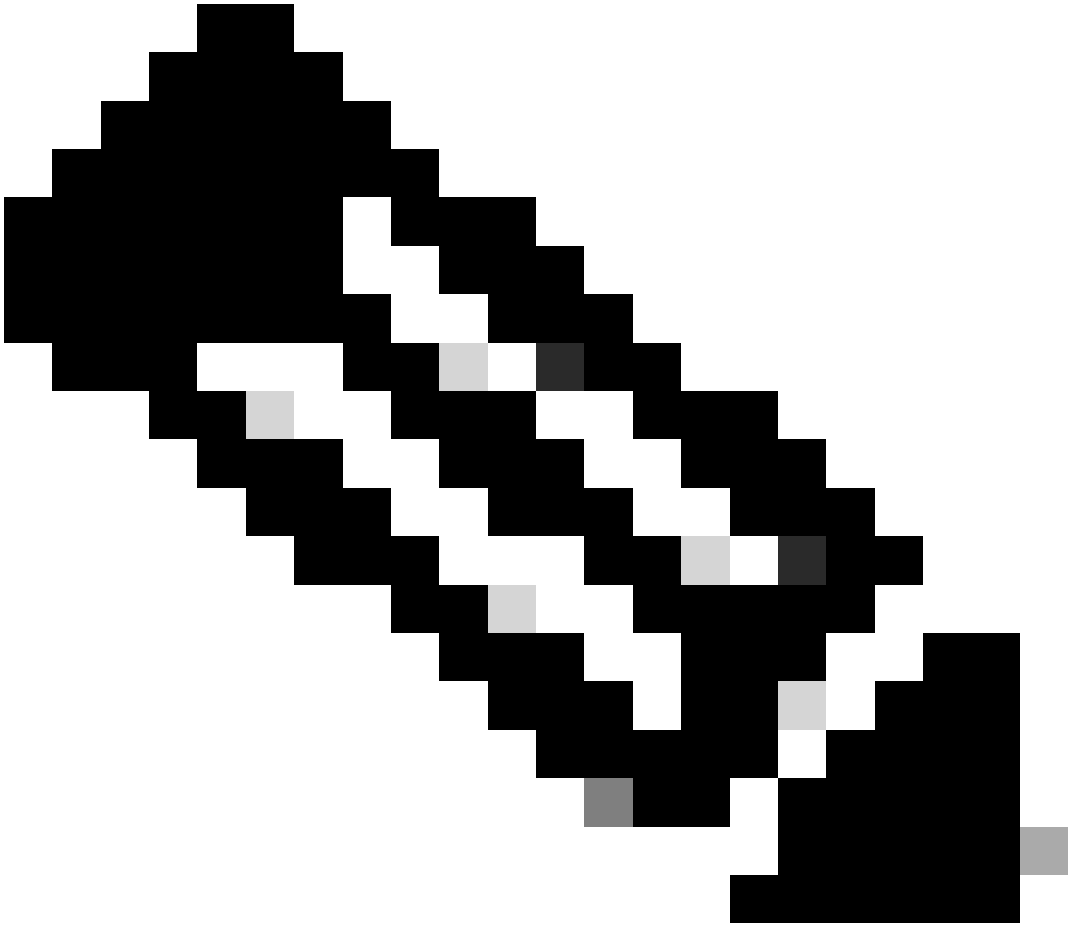
- SCPツールを使用して、フローコレクタ(/lancope/var/tcpdump内にあります)からローカル

マシンにパケットキャプチャをエクスポートし、Wiresharkで開きます



- NetFlow/IPFIXテンプレートが受信されたフレームを特定し、それを開いてテンプレートに含まれるフィールドを検証します


Frame 52: 162 bytes on wire (1296 bits), 162 bytes captured (1296 bits)
Ethernet II, Src: VMware_b3:6a:d6 (00:50:56:b3:6a:d6), Dst: VMware_b3:04:b9 (00:50:56:b3:04:b9)
Internet Protocol Version 4, Src: 10.1.0.253, Dst: 10.1.3.31
User Datagram Protocol, Src Port: 51431, Dst Port: 2055
Cisco NetFlow/IPFIX
Version: 10
Length: 120
Timestamp: Jun 1, 2023 17:41:03.000000000 CST
FlowSequence: 24348090
Observation Domain Id: 256
Set 1 [id=2] (Data Template): 260
FlowSet Id: Data Template (V10 [IPFIX]) (2)
FlowSet Length: 104
Template (Id = 260, Count = 24)
Template Id: 260
Field Count: 24
Field (1/24): IPv4 ID
Field (2/24): IP_SRC_ADDR
Field (3/24): IP_DST_ADDR
Field (4/24): IP_TOS
Field (5/24): IP_DSCP
Field (6/24): PROTOCOL
Field (7/24): IP TTL MINIMUM
Field (8/24): IP TTL MAXIMUM
Field (9/24): L4_SRC_PORT
Field (10/24): L4_DST_PORT
Field (11/24): TCP_FLAGS
Field (12/24): SRC_AS
Field (13/24): IP_SRC_PREFIX
Field (14/24): SRC_MASK
Field (15/24): INPUT_SNMP
Field (16/24): DST_AS
Field (17/24): IP_NEXT_HOP
Field (18/24): DST_MASK
Field (19/24): OUTPUT_SNMP
Field (20/24): DIRECTION
Field (21/24): BYTES
Field (22/24): PKTS
Field (23/24): FIRST_SWITCHED
Field (24/24): LAST_SWITCHED



注：表示されるフィールド名はエクスポータごとに異なる場合があります。これは、これらのフィールドを検証する方法を示すだけです。

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。