FMC CLIを使用したアクセスリスト要素(ACE)カウントの計算

内容

はじめに

このドキュメントでは、アクセスコントロールポリシーのどのルールがアクセスリスト要素の数まで拡張されているかを確認する方法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。

- FirePOWER の知識
- FMCでのアクセスコントロールポリシーの設定に関する知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Secure Firewall Management Center(FMC)
- Cisco Firepower Threat Defense(FTD)

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

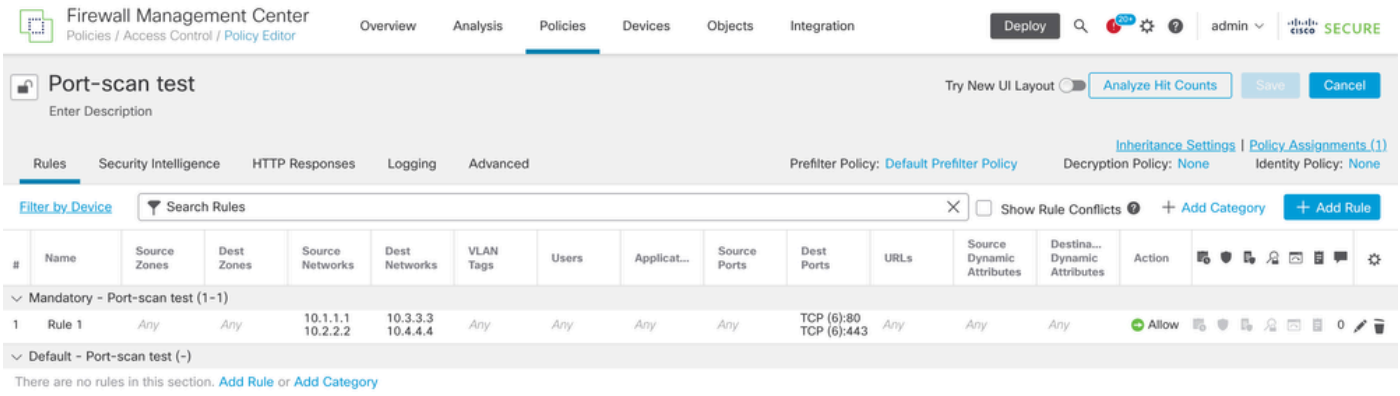
アクセスコントロールルールは、次のパラメータの1つまたは複数の組み合わせを使用して作成されます。

- IPアドレス（送信元および宛先）
- ポート（送信元および宛先）
- URL（システム提供カテゴリおよびカスタムURL）
- アプリケーションディテクタ
- VLAN
- ゾーン

アクセスルールで使用されているパラメータの組み合わせに基づいて、ルールの展開はセンサーで変更されます。このドキュメントでは、FMC上のさまざまなルールの組み合わせと、センサー上のそれぞれの関連する展開について説明します。

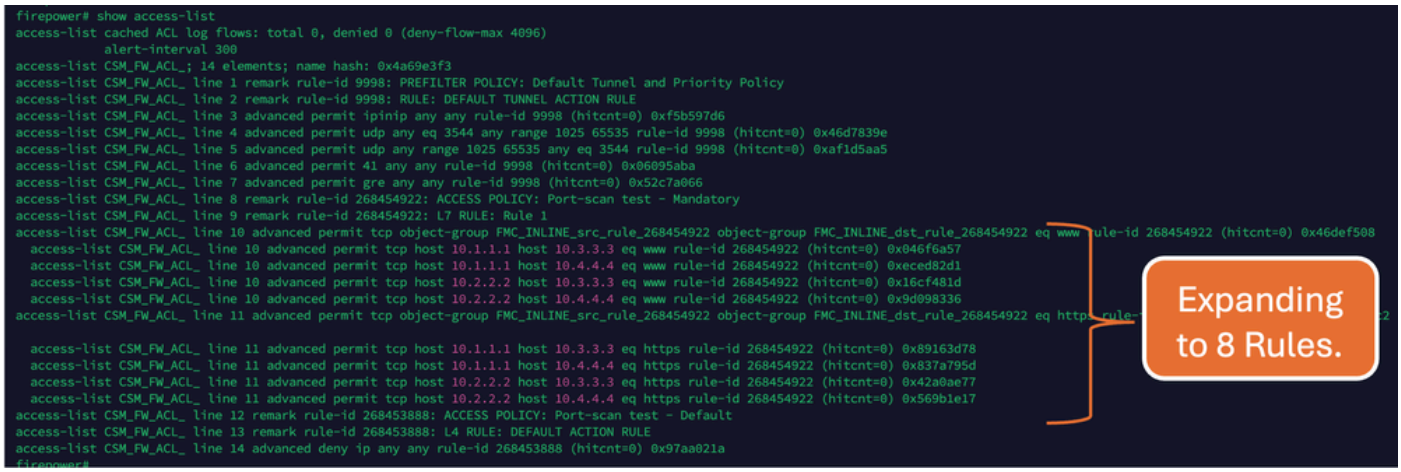
FMC CLIを使用したアクセスリスト要素カウント(ACE)の計算方法

図に示すように、FMCからのアクセスルールの設定を検討します。



アクセスコントロールポリシーでのルールの設定

このルールがFTD CLIに表示される場合、このルールが8つのルールに拡張されていることがわかります。



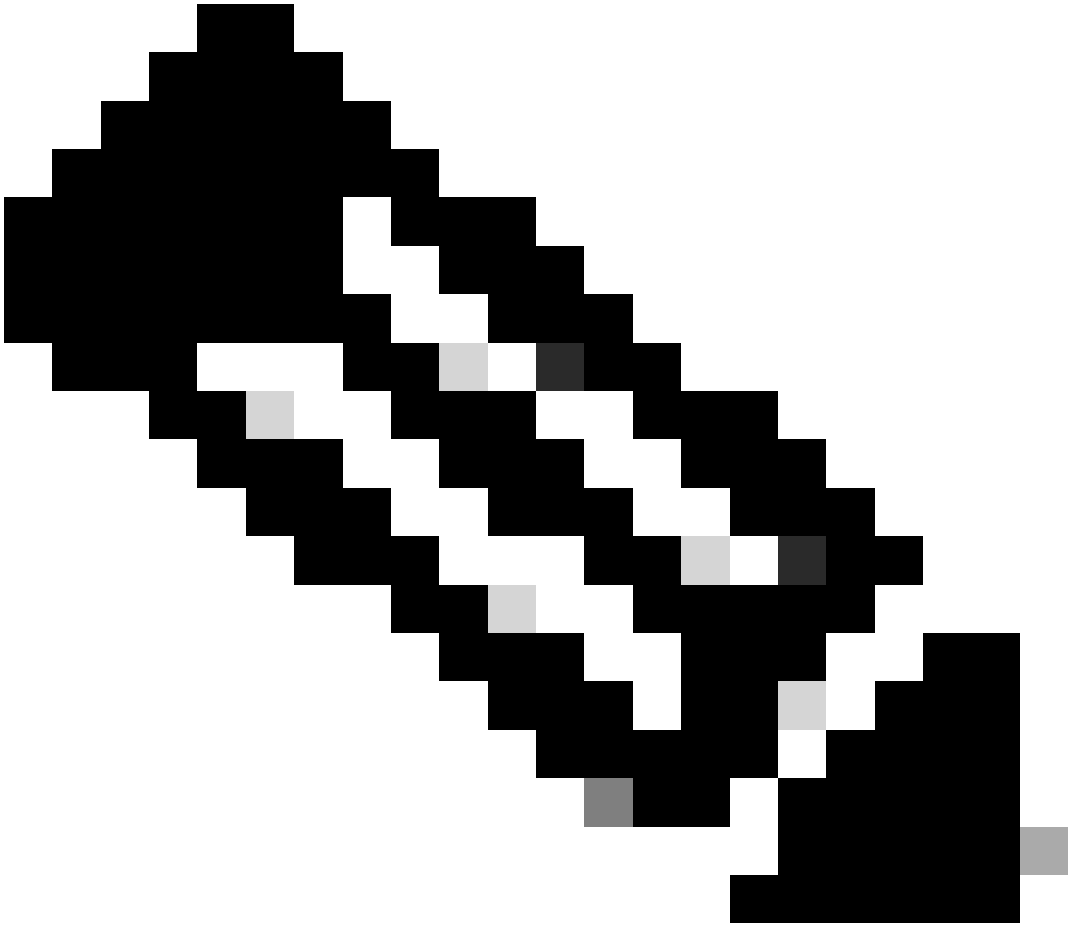
FMC CLIのperlコマンドを使用すると、どのルールがアクセスリスト要素の数をいくつ拡張しているかをチェックできます。

<#root>

perl /var/opt/CSCOpx/bin/access_rule_expansion_count.pl

```
root@firepower:/Volume/home/admin# perl /var/opt/CSCOpx/bin/access_rule_expansion_count.pl

  Secure Firewall Management Center for VMware - v7.4.1 - (build 172)

  Access Control Rule Expansion Computer



  Enter FTD UUID or Name:

  > 10.70.73.44

------------------------------------------------------------------------------------------------------------------

  Secure Firewall Management Center for VMware - v7.4.1 - (build 172)

  Access Control Rule Expansion Computer

  Device:

    UUID: 93cc359c-39be-11d4-9ae1-f2186cbddb11

    Name: 10.70.73.44

  Access Control Policy:

    UUID: 005056B9-F342-0ed3-0000-292057792375

    Name: Port-scan test

    Description:

  Intrusion Policies:
```

```
-----------------------------------------------------------------------------------------------

|  UUID                                    |  NAME                                              |

-----------------------------------------------------------------------------------------------

-----------------------------------------------------------------------------------------------

  Date: 2024-Jul-17 at 06:51:55 UTC

  NOTE: Computation is done on per rule basis. Count from shadow rules will not be applicable on device

  Run "Rule Conflict Detection" tool on AC Policy for specified device to detect and optimise such rules


-------------------------------------------------------------------------------------------------------
| UUID                                       | NAME                     |             COUNT
-------------------------------------------------------------------------------------------------------
| 005056B9-F342-0ed3-0000-000268454919       | Rule 1                   |               8
-------------------------------------------------------------------------------------------------------
|   TOTAL: 8
-------------------------------------------------------------------------------------------------------
| Access Rule Elements Count on FTD: 14
-------------------------------------------------------------------------------------------------------

>>> My JVM PID : 19417
```



注：アクセスルール要素のFTDでのカウント：14。これには、デフォルトのFTDルール（プレフィルタ）とデフォルトアクセスコントロールルールも含まれます。

デフォルトのプレフィルタルールはFTD CLIで確認できます。

```
firepower# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
           alert-interval 300
access-list CSM_FW_ACL_; 14 elements; name hash: 0x4a69e3f3
access-list CSM_FW_ACL_ line 1 remark rule-id 9998: PREFILTER POLICY: Default Tunnel and Priority Policy
access-list CSM_FW_ACL_ line 2 remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_ line 3 advanced permit ipinip any any rule-id 9998 (hitcnt=0) 0xf5b597d6
access-list CSM_FW_ACL_ line 4 advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998 (hitcnt=0) 0x46d7839e
access-list CSM_FW_ACL_ line 5 advanced permit udp any range 1025 65535 any eq 3544 rule-id 9998 (hitcnt=0) 0xaf1d5aa5
access-list CSM_FW_ACL_ line 6 advanced permit 41 any any rule-id 9998 (hitcnt=0) 0x06095aba
access-list CSM_FW_ACL_ line 7 advanced permit gre any any rule-id 9998 (hitcnt=0) 0x52c7a066
access-list CSM_FW_ACL_ line 8 remark rule-id 268454922: ACCESS POLICY: Port-scan test - Mandatory
access-list CSM_FW_ACL_ line 9 remark rule-id 268454922: L7 RULE: Rule 1
access-list CSM_FW_ACL_ line 10 advanced permit tcp object-group FMC_INLINE_src_rule_268454922 object-group FMC_INLINE_dst_rule_268454922 eq www rule-id 268454922 (hitcnt=0) 0x46def508
  access-list CSM_FW_ACL_ line 10 advanced permit tcp host 10.1.1.1 host 10.3.3.3 eq www rule-id 268454922 (hitcnt=0) 0x046f6a57
  access-list CSM_FW_ACL_ line 10 advanced permit tcp host 10.1.1.1 host 10.4.4.4 eq www rule-id 268454922 (hitcnt=0) 0xeced82d1
  access-list CSM_FW_ACL_ line 10 advanced permit tcp host 10.2.2.2 host 10.3.3.3 eq www rule-id 268454922 (hitcnt=0) 0x16cf481d
  access-list CSM_FW_ACL_ line 10 advanced permit tcp host 10.2.2.2 host 10.4.4.4 eq www rule-id 268454922 (hitcnt=0) 0x9d098336
access-list CSM_FW_ACL_ line 11 advanced permit tcp object-group FMC_INLINE_src_rule_268454922 object-group FMC_INLINE_dst_rule_268454922 eq https rule-id 268454922 (hitcnt=0) 0x548058c2

  access-list CSM_FW_ACL_ line 11 advanced permit tcp host 10.1.1.1 host 10.3.3.3 eq https rule-id 268454922 (hitcnt=0) 0x89163d78
  access-list CSM_FW_ACL_ line 11 advanced permit tcp host 10.1.1.1 host 10.4.4.4 eq https rule-id 268454922 (hitcnt=0) 0x837a795d
  access-list CSM_FW_ACL_ line 11 advanced permit tcp host 10.2.2.2 host 10.3.3.3 eq https rule-id 268454922 (hitcnt=0) 0x42a0ae77
  access-list CSM_FW_ACL_ line 11 advanced permit tcp host 10.2.2.2 host 10.4.4.4 eq https rule-id 268454922 (hitcnt=0) 0x569b1e17
access-list CSM_FW_ACL_ line 12 remark rule-id 268453888: ACCESS POLICY: Port-scan test - Default
access-list CSM_FW_ACL_ line 13 remark rule-id 268453888: L4 RULE: DEFAULT ACTION RULE
access-list CSM_FW_ACL_ line 14 advanced deny ip any any rule-id 268453888 (hitcnt=0) 0x97aa021a
```

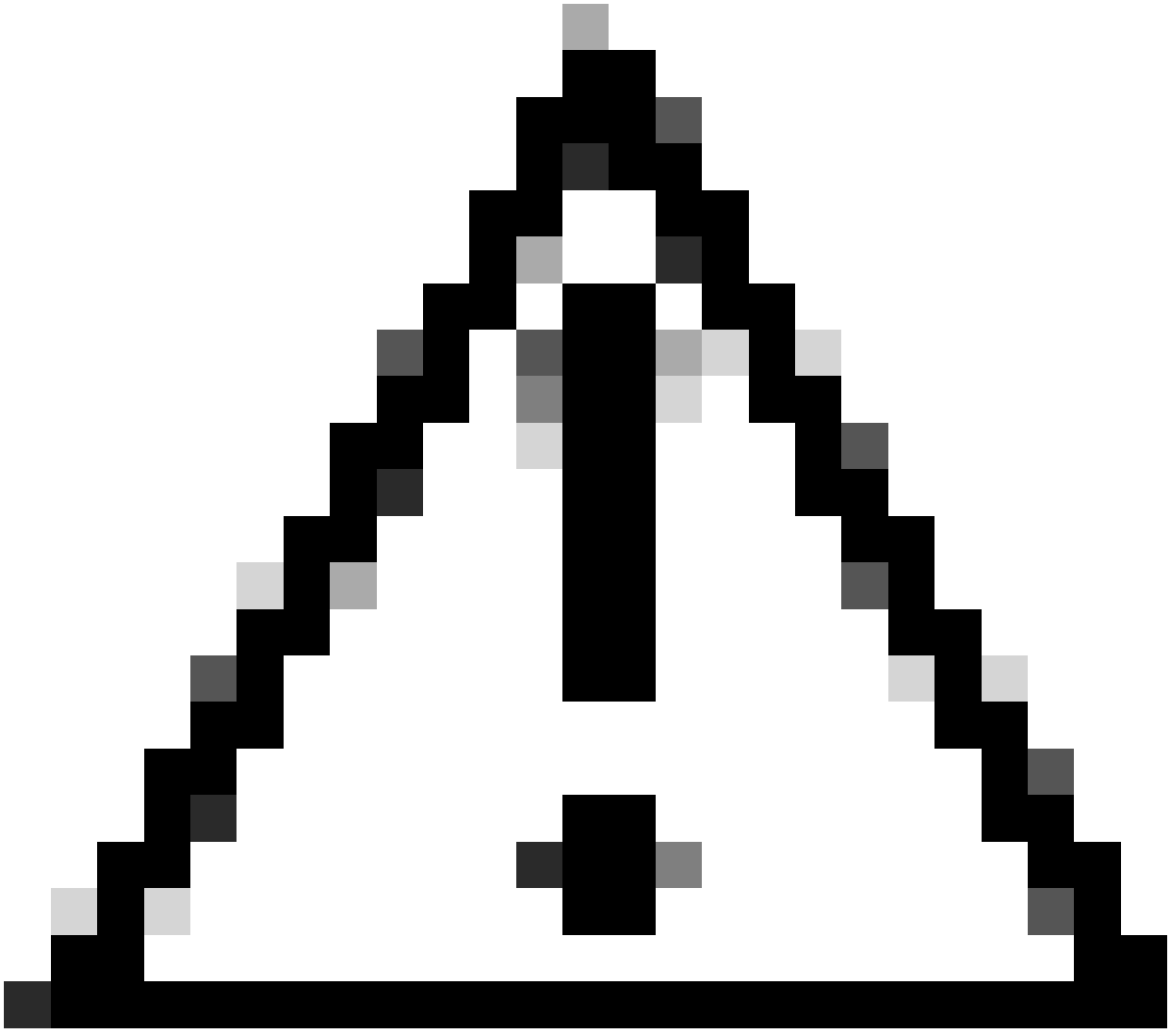
6 Default Pre-filter Rules.

高いACEの影響

- CPUの使用率が高くなっていることがわかります。
- 高いメモリが表示される。
- デバイスの速度低下が観察される可能性があります。
- 導入の失敗/導入時間の延長

オブジェクトグループ検索(OGS)を有効にするタイミングの決定

- ACEのカウントがデバイスのACE制限を超えています。
- OGSを有効にするとデバイスのCPUに負荷がかかるため、デバイスのCPUはまだ高くありません。
- 実稼働時間外に有効にします。



注意: OGSを有効にする前に、FTD CLIクラッシュモードからasp rule-engine transactional-commit access-groupを有効にしてください。これは、OGSを有効にしている間の導入プロセス中および導入直後のトラフィックドロップを回避するように設定されています。

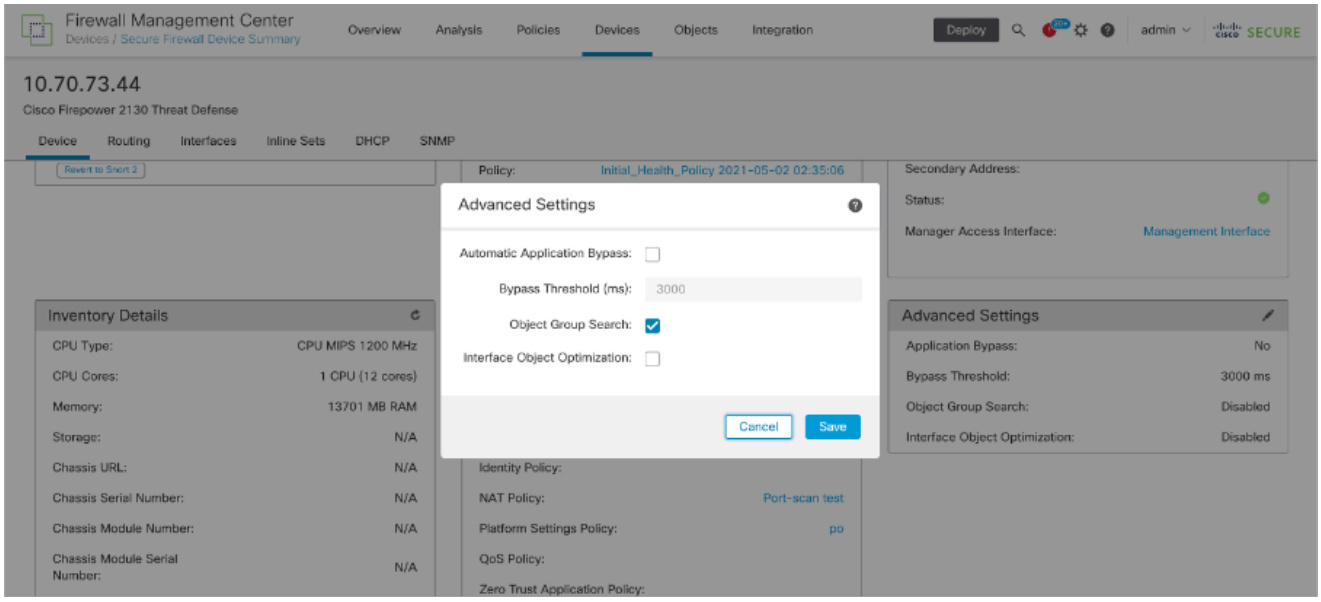
```
>
>
>
>
> asp rule-engine transactional-commit access-group
>
>
>
```

オブジェクトグループ検索の有効化

現在、OGSは有効になっていません。

```
firepower#
firepower#
firepower#
firepower# show run object-group-search
firepower#
firepower#
firepower#
```

1. FMC CLIにログインします。Devices > Device Management > Select the FTD device > Deviceの順に移動します。詳細設定からオブジェクトグループ検索を有効にします。

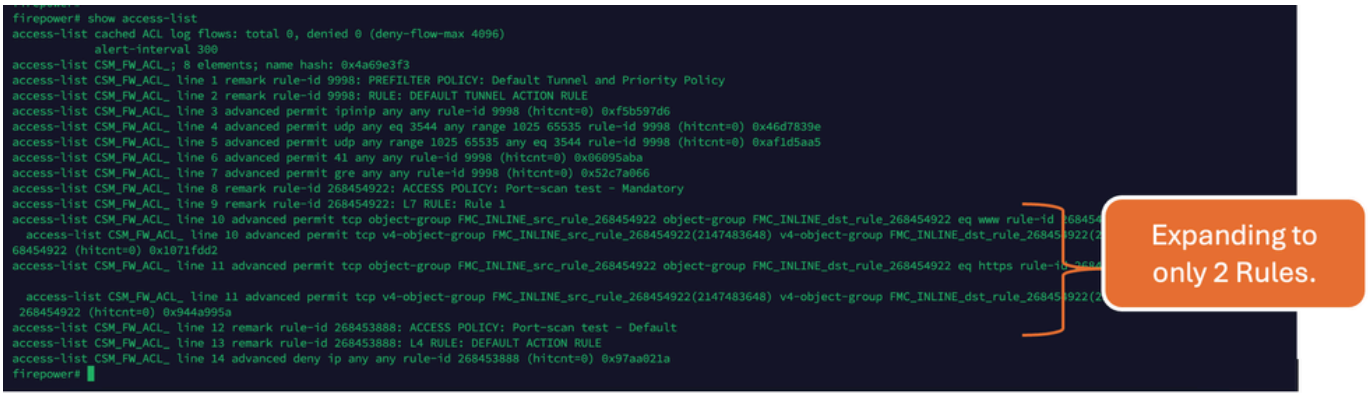


2. Save and deployをクリックします。

確認

OGSを有効にする前：

OGSを有効にした後：



関連情報

FTDでルールを展開する方法の詳細については、『FirePOWERデバイスでのルール展開について』を参照してください。

FTDのアーキテクチャとトラブルシューティングについての詳細は、『Dissecting(FTD)Firepower Threat Defense』を参照してください。

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。