



Cisco TrustSec SGACL のハイアベイラビリティ

Cisco TrustSec セキュリティ グループ アクセス コントロール リスト (SGACL) は、Cisco StackWise 技術をサポートしているスイッチでのハイアベイラビリティ機能をサポートしています。この技術によってステータフルな冗長性が提供され、スイッチスタックはアクセス制御 エントリを強制し、処理できます。

- [Cisco TrustSec SGACL のハイアベイラビリティの前提条件 \(1 ページ\)](#)
- [Cisco TrustSec SGACL のハイアベイラビリティの制約事項 \(1 ページ\)](#)
- [Cisco TrustSec SGACL のハイアベイラビリティに関する情報 \(2 ページ\)](#)
- [Cisco TrustSec SGACL のハイアベイラビリティの確認 \(3 ページ\)](#)
- [Cisco TrustSec SGACL のハイアベイラビリティの設定に関するその他の関連資料 \(5 ページ\)](#)
- [SGACL のハイアベイラビリティの機能情報 \(5 ページ\)](#)

Cisco TrustSec SGACL のハイアベイラビリティの前提条件

このマニュアルでは、次のことを前提としています。

- Cisco TrustSec およびセキュリティ グループ アクセス コントロール リスト (SGACL) 構成を理解している。
- デバイスは、スタックとして機能するように設定されている。
- スタック内のすべてのデバイスが同一バージョンの Cisco IOS XE ソフトウェアを実行している。

Cisco TrustSec SGACL のハイアベイラビリティの制約事項

- アクティブスイッチとスタンバイスイッチの両方で同時に障害が発生した場合、SGACL のステータフル スイッチオーバーは行われません。

Cisco TrustSec SGACL のハイアベイラビリティに関する情報

Cisco TrustSec セキュリティ グループ アクセス コントロール リスト (SGACL) は、Cisco StackWise 技術をサポートしているスイッチでのハイアベイラビリティ機能をサポートしています。この技術によってステータフルな冗長性が提供され、スイッチスタックはアクセス制御 エントリを強制し、処理できます。

この機能を有効にする Cisco TrustSec 固有の設定はありません。これは、Cisco IOS XE Denali 16.2.1 以降のリリースでサポートされます。

高可用性の概要

スイッチスタックでは、スタックマネージャが最も高い優先順位を持つスイッチをアクティブ スイッチとして割り当て、次に高い優先順位を持つスイッチをスタンバイスイッチとして割り当てます。自動または CLI ベースのステータフルスイッチオーバー中は、スタンバイスイッチがアクティブスイッチになり、次に優先順位の高いスイッチがスタンバイスイッチになります。

運用データは、初期のシステムブートアップ、運用データの変更（認可変更 (CoA) と呼ばれる）、または運用データのリフレッシュ時に、アクティブスイッチからスタンバイスイッチに同期されます。

ステータフルスイッチオーバー中に、新たにアクティブになったスイッチは、運用データを要求してダウンロードします。環境データ (ENV-data) とロールベース アクセス コントロール リスト (RBACL) は、リフレッシュ時間が完了するまで更新されません。

次の運用データがアクティブスイッチにダウンロードされます。

- 環境データ (ENV-data) : リフレッシュ時または初期化時に RBACL 情報を取得するための優先サーバリストで構成される可変長フィールド。
- Protected Access Credential (PAC) : Authentication Protocol Flexible Authentication via the Secure Tunneling (EAP-FAST) のトンネルを保護するために、スイッチとオーセンティケータ間で相互に一意に共有される共有秘密。
- ロールベースのポリシー (RBACL または SGACL) : スイッチ上のすべてのセキュリティ グループタグ (SGT) マッピングのポリシー定義で構成される可変長ロールベースのポリシーリスト。



(注) デバイス ID とパスワードの詳細で構成される Cisco TrustSec クレデンシャルは、アクティブ スイッチでコマンドとして実行されます。

Cisco TrustSec SGACL のハイアベイラビリティの確認

Cisco TrustSec SGACL ハイアベイラビリティ設定を確認するには、アクティブスイッチとスタンバイスイッチの両方で **show cts role-based permissions** コマンドを実行します。コマンドの出力は、両方のスイッチで同じである必要があります。

次に、アクティブスイッチでの **show cts role-based permissions** コマンドの出力例を示します。

```
Device# show cts role-based permissions

IPv4 Role-based permissions default (monitored):
    default_sgacl-01
    Deny IP-00
IPv4 Role-based permissions from group 10:SGT_10 to group 15:SGT_15:
    SGACL_3-01
IPv4 Role-based permissions from group 14:SGT_14 to group 15:SGT_15:
    multiple_ace-14
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

次に、スタンバイスイッチでの **show cts role-based permissions** コマンドの出力例を示します。

```
Device-stby# show cts role-based permissions

IPv4 Role-based permissions default (monitored):
    default_sgacl-01
    Deny IP-00
IPv4 Role-based permissions from group 10:SGT_10 to group 15:SGT_15:
    SGACL_3-01
IPv4 Role-based permissions from group 14:SGT_14 to group 15:SGT_15:
    multiple_ace-14
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

ステートフルスイッチオーバー後、アクティブスイッチで次のコマンドを実行して機能を確認します。

次に、**show cts pacs** コマンドの出力例を示します。

```
Device# show cts pacs

AID: A3B6D4D8353F102346786CF220FF151C
PAC-Info:
    PAC-type = Cisco Trustsec
    AID: A3B6D4D8353F102346786CF220FF151C
    I-ID: CTS_ED_21
    A-ID-Info: Identity Services Engine
    Credential Lifetime: 17:22:32 IST Mon Mar 14 2016
PAC-Opaque:
000200B80003000100040010A3B6D4D8353F102346786CF220FF151C0006009C00030100E044B2650D8351FD06
F23623C470511E0000001356DEA96C00093A80538898D40F633C368B053200D4C9D2422A7FEB4837EA9DBB89D1
E51DA4E7B184E66D3D5F2839C11E5FB386936BB85250C61CA0116FDD9A184C6E96593EEAF5C39BE08140AFBB19
4EE701A0056600CFF5B12C02DD7ECEAA3CCC8170263669C483BD208052A46C31E39199830F794676842ADEECBB
A30FC4A5A0DEDA93
Refresh timer is set for 01:00:05
```

次に、**show cts environment-data** コマンドの出力例を示します。

```

Device# show cts environment-data

CTS Environment Data
=====
Current state = COMPLETE
Last status = Successful
Local Device SGT:
  SGT tag = 0:Unknown
Server List Info:
Installed list: CTSServerList1-000D, 1 server(s):
  *Server: 10.78.105.47, port 1812, A-ID A3B6D4D8353F102346786CF220FF151C
  Status = ALIVE
  auto-test = FALSE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs
Multicast Group SGT Table:
Security Group Name Table:
0001-45 :
  0-00:Unknown
  2-ba:SGT_2
  3-00:SGT_3
  4-00:SGT_4
  5-00:SGT_5
  6-00:SGT_6
  7-00:SGT_7
  8-00:SGT_8
  9-00:SGT_9
  10-16:SGT_10
!
!
!
Environment Data Lifetime = 3600 secs
Last update time = 14:32:53 IST Mon Mar 14 2016
Env-data expires in 0:00:10:04 (dd:hr:mm:sec)
Env-data refreshes in 0:00:10:04 (dd:hr:mm:sec)
Cache data applied = NONE
State Machine is running

```

次に、ステートフル スイッチオーバー後の **show cts role-based permissions** コマンドの出力例を示します。

```

Device# show cts role-based permissions

IPv4 Role-based permissions default:
  default_sgacl-01
  Deny IP-00
IPv4 Role-based permissions from group 10:SGT_10 to group 15:SGT_15:
  SGACL_3-01
IPv4 Role-based permissions from group 14:SGT_14 to group 15:SGT_15:
  multiple_ace-14
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE

```

Cisco TrustSec SGACL のハイアベイラビリティの設定に関するその他の関連資料

関連資料

シスコのテクニカル サポート

説明	リンク
<p>シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。</p> <p>お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service (Field Notice からアクセス)、Cisco Technical Services Newsletter、Really Simple Syndication (RSS) フィードなどの各種サービスに加入できます。</p> <p>シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。</p>	<p>http://www.cisco.com/support</p>

SGACL のハイアベイラビリティの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレーンで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 1: Cisco TrustSec SGACL のハイアベイラビリティの機能情報

機能名	リリース	機能情報
Cisco TrustSec SGACL のハイアベイラビリティ	Cisco IOS XE Denali 16.2.1	<p>Cisco TrustSec セキュリティグループアクセスコントロールリスト (SGACL) は、スイッチスタックマネージャで利用可能なハイアベイラビリティ機能をサポートしています。</p> <p>この機能を有効にする Cisco TrustSec 固有の設定はありません。この機能は、スタックマネージャアーキテクチャを備えた、Cisco IOS XE Denali 16.2.1 以降のリリースを使用するスイッチでのみ使用できます。</p>