



SGACL ハイ アベイラビリティ

- [SGACL ハイアベイラビリティの機能履歴, on page 1](#)
- [Cisco TrustSec SGACL のハイ アベイラビリティ, on page 1](#)
- [データの同期およびスイッチオーバーのプロセス, on page 2](#)
- [Cisco TrustSec SGACL 高可用性（HA）の確認, on page 3](#)

SGACL ハイアベイラビリティの機能履歴

次の表に、このモジュールで説明する機能のリリース情報とプラットフォームサポート情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能名と説明	サポートされるプラットフォーム
Cisco IOS XE 17.18.1	SGACL 高可用性（HA）： 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 技術を備えたスイッチでの高可用性（HA）をサポートしています。	Cisco C9350 シリーズ スマート スイッチ Cisco C9610 シリーズ スマート スイッチ

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 技術を備えたスイッチでの高可用性（HA）をサポートしています。StackWise はステートフルな冗長性を提供するため、フェールオーバーイベント中にもスイッチスタックがアクセス コントロール エントリ（ACE）を適用して処理できます。

スイッチスタックでの高可用性（HA）操作

スイッチスタック内で、スタックマネージャは、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に指定し、次に優先順位が高いスイッチをスタンバイスイッチに割り当てます。ステートフルスイッチオーバーの際、自動かCLIからの実行かに関係なく、スタンバイスイッチがアクティブになり、次の順位のスイッチがスタンバイロールを引き継ぎます。

運用データは、システムのブートアップ中、運用データの変更時（認可変更（CoA）など）、または運用データの更新中に、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。

ハイ アベイラビリティ セットアップでのデバイスの展開

高可用性（HA）セットアップでデバイスをデプロイする場合は、次の手順を実行します。

1. 高可用性（HA）セットアップに参加するすべてのデバイスから既存のログイン情報を削除します。
2. スタックの電源を投入し、デバイスロール（アクティブ、スタンバイ、およびメンバースイッチ）を割り当てます。
3. アクティブデバイスで、`cts credentials id id password password` コマンドを使用してログイン情報を設定します。

データの同期およびスイッチオーバーのプロセス

ステートフルスイッチオーバーが発生すると、新たにアクティブになったスイッチは、必要な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データ）とロールベースアクセス制御リスト（RBACL）は、更新時間が完了した後にのみ更新されます。

次に、アクティブスイッチにダウンロードされるさまざまなタイプの運用データを示します。

運用データ	説明
環境データ（ENVデータ）	更新または初期化中にRBACL情報を取得するための優先サーバーリストが含まれています。
Protected Access Credential（PAC）	スイッチとオーセンティケータ間の一意の共有秘密で、セキュアトンネリングを介した Extensible Authentication Protocol Flexible Authentication（EAP-FAST）を保護するために使用されます。
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を定義する可変長リスト。



Note 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 高可用性 (HA) の確認

Cisco TrustSec SGACL 高可用性構成を確認するには、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_sgac1-01
  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
```

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。