Cisco Security Cloud Control を使用した SSH デバイスの管理

Cisco Security Cloud Control を使用した SSH デバイスの管理

Cisco Security Cloud Control（旧称 Cisco Defense Orchestrator）を使用すると、SSH を介してデバイスを管理できます。これらのデバイスでサポートされている機能は次のとおりです。

- SSH デバイスのオンボーディング。SSH デバイスに保存されている、高レベルの権限を持つユーザーのユーザー名とパスワードを使用して、デバイスをオンボーディングできます。
- デバイス設定の表示。デバイス コンフィギュレーション ファイルを表示できます。
- デバイスからのポリシーと設定の変更を確認します。Cisco IOS または SSH から Security Cloud Control への変更の読み取り SSH デバイスからコンフィギュレーション ファイルが読み取られると、Security Cloud Control のデータベースに保存されます。
- アウトオブバンド変更検出。デバイスで [競合検出（Conflict Detection）] を有効にすると、Security Cloud Control は 10 分ごとにデバイスの設定の変更をチェックします。変更がある場合、デバイスのステータスは [競合検出（Conflict Detected）] に変わり、競合を解決可能になります。
- コマンド ライン インターフェイスのサポート。Security Cloud Control のコマンド ライン インターフェイスを介して、すべての SSH デバイス コマンドをデバイスに発行できます。
- 個々の CLI コマンドおよびコマンドのグループを、編集および再利用可能な「マクロ」に変換可能。Security Cloud Control が提供するシステム定義マクロを使用して、頻繁に実行するタスク用に独自のマクロを作成できます。
- SSH フィンガープリントの変更の検出と管理。デバイスのログイン情報またはプロパティが変更され、それによって SSH フィンガープリントが変更された場合、Security Cloud

Cisco Security Cloud Control を使用した SSH デバイスの管理

Control はその変更を検出し、新しいフィンガープリントを確認して許可する機会を提供します。

- 変更ログ。変更ログには、SSHデバイスに発行するすべてのコマンドがキャプチャされます。

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。