Cisco Defense Orchestrator での SSH デバイスの管理

Cisco Defense Orchestrator での SSH デバイスの管理

Cisco Defense Orchestrator（CDO）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 CDO 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、CDO 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。[競合検出（Conflict Detection）] を有効にすると、CDO 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。CDO 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」に変換できます。CDO 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を検出および管理します。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、CDO 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。

Cisco Defense Orchestrator での SSH デバイスの管理

- 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。