

変更ログ、ワークフロー、およびジョブのモニタリングとレポート

Security Cloud Control は、設定変更ログ、一括デバイス操作、およびデバイスとの通信時に実行されるプロセスを効果的にモニタリングします。これは、ネットワークの既存のポリシーがセキュリティ態勢にどのように影響するかを理解するのに役立ちます。

- Security Cloud Control の変更ログ （1 ページ）
- 変更ログの差異の表示 （3 ページ）
- 変更リクエスト管理 （4 ページ）
- 変更ログのエクスポート, on page 12
- Security Cloud Control でのジョブモニタリング （13 ページ）
- Security Cloud Control でのワークフローのモニタリング （15 ページ）

Security Cloud Control の変更ログ

変更ログは、次のような設定追跡機能です。

- Security Cloud Control で行われた設定変更をキャプチャし、サポート対象のすべてのデバイスとサービスの変更を表示する単一のビューを提供します。
- デバイス構成に加えられた変更の対照比較を示します。
- デバイスのオンボーディングと削除を記録します。
- Security Cloud Control の外部で発生するポリシー変更の競合を検出します。

変更ログの管理機能

変更ログには、設定管理および障害対応に関する次の機能が用意されています。

- すべての変更ログエントリのラベルを示します。
- インシデントの調査または障害対応中に、「誰が」、「何を」、「いつ」に回答します。
- 変更ログ全体またはその一部のみを CSV ファイルとしてダウンロードできます。

（注） クラウド提供型 Firewall Management Center で行われた変更は、変更ログに反映されません。

[変更ログの容量（Change log capacity）]：Security Cloud Control は変更ログ情報を 1 年間保持し、1 年を超えるデータを削除します。

Security Cloud Control のデータベースに保存される変更ログ情報と、エクスポートした変更ログに表示される情報には違いがあります。詳細については、変更ログのエクスポート（12ページ）を参照してください。

[変更ログエントリ（Change log entries）]： 変更ログエントリには、単一のデバイス設定への変更、デバイスで実行されたアクション、または Security Cloud Control の外部でデバイスに加えられた変更が反映されます。

- 設定の変更を含む変更ログエントリの場合、対応する行の任意の場所をクリックして変更の詳細を表示できます。
- Security Cloud Control の外部で行われ、競合として検出されたアウトオブバンド変更の場合、**システムユーザー**は**最後のユーザー**として報告されます。
- Security Cloud Control 上のデバイスの設定がデバイス上の設定と同期された後、またはデバイスが Security Cloud Control から削除されたときに、Security Cloud Control は変更ログエントリを閉じます。設定は、デバイスから Security Cloud Control に設定を読み取った後に、または Security Cloud Control からデバイスに設定を展開した後に同期されたと見なされます。
- Security Cloud Control は、変更が成功したか失敗したかに関係なく、既存のエントリを完了した直後に新しい変更ログエントリを作成します。追加の設定変更は、開いている新しい変更ログエントリに追加されます。
- デバイスに対する読み取り、展開、および削除アクションのイベントが表示されます。これらのアクションで、デバイスの変更ログが閉じられます。
- Security Cloud Control が（読み取りまたは展開によって）デバイスの設定と同期されると、または Security Cloud Control がデバイスを管理しなくなると、変更ログは閉じられます。
- Security Cloud Control の外部でデバイスに変更が加えられた場合、[競合検出（Conflict Detected）] エントリが変更ログに含まれます。

[保留中および完了した変更ログエントリ（Pending and completed change log entries）]： 変更ログには、[保留中（Pending）] または [完了（Completed）] のステータスがあります。Security Cloud Control を使用してデバイスの設定を変更すると、変更は [保留中（Pending）] 変更ログエントリに記録されます。保留中の変更ログを完了するアクティビティは次のとおりです。

- デバイスから Security Cloud Control への設定の読み取り
- Security Cloud Control からデバイスへの変更の展開
- Security Cloud Control からのデバイスの削除

- 実行コンフィギュレーション ファイルを更新する CLI コマンドの実行

[変更ログエントリの検索とフィルタ処理（Search and filter change log entries）]：変更ログエントリの検索とフィルタ処理ができます。検索フィールドを使用してイベントを検索します。フィルタ（フィルタアイコン）を使用して、指定した条件を満たすエントリを検索します。また、変更ログをフィルタ処理し、検索フィールドにキーワードを追加して、2 つのタスクを組み合わせることで、フィルタ処理された結果内のエントリを検索できます。

変更ログの差異の表示

変更ログの差異を表示し、実行構成ファイルの変更前後の状態を調べることで、デバイスに加えられた設定変更を分析します。

変更ログの差異では、元の構成ファイルと変更された構成ファイルの詳細な比較が提供され、デバイス設定にどのような変更が加えられたかを把握できます。左右のビューでは、実行構成内で追加、変更、および削除された箇所が強調表示されます。

手順

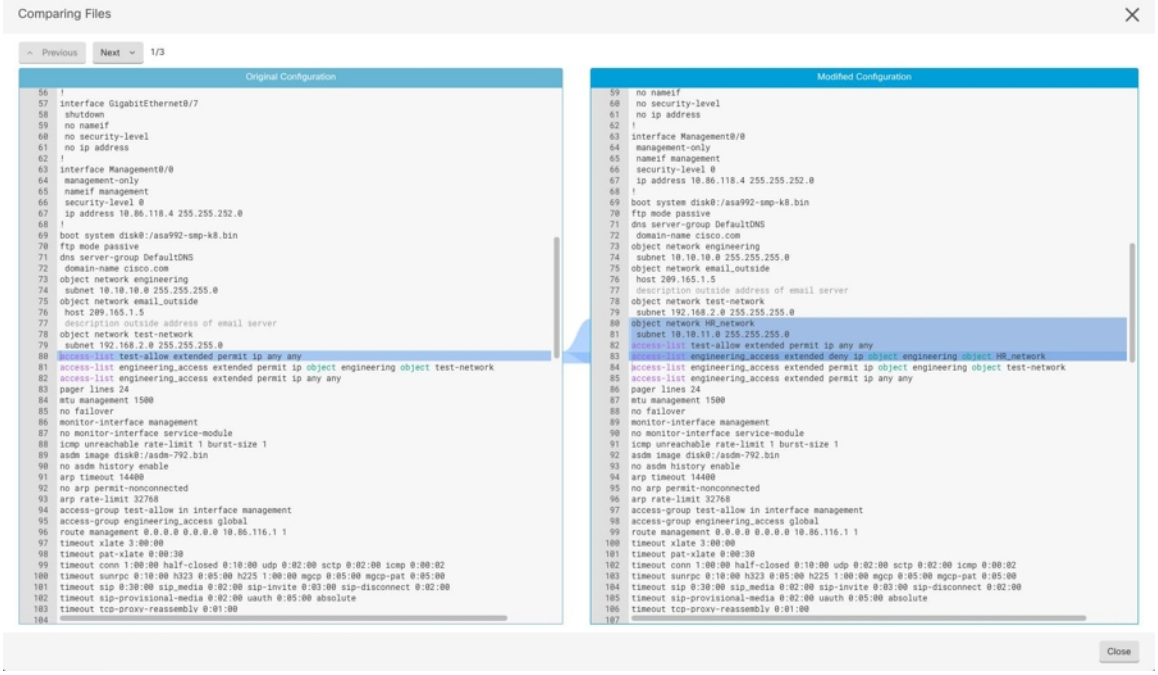
ステップ 1 変更ログで [差分（Diff）] をクリックします。

対象デバイスの実行構成ファイル内の変更が並べて表示されます。

[元の設定（Original Configuration）] 列には、変更が ASA デバイスに書き込まれる前の実行構成ファイルが表示されます。[変更済みの設定（Modified Configuration）] 列には、変更が書き込まれた後の実行コンフィギュレーション ファイルが表示されます。

ステップ 2 左の列から右の列まで線をたどって、変更を確認します。

比較ビューでは、HR_network オブジェクトや、engineering ネットワーク内のアドレスが HR_network ネットワーク内のアドレスに到達するのを防ぐアクセスルールなどの追加箇所を確認できます。[元の設定（Original Configuration）] 列では、[変更された設定（Modified Configuration）] 列の変更内容を把握するための参照ポイントとなる行が強調表示されます。



ステップ 3 [前へ（Previous）] および [次へ（Next）] ボタンをクリックして、ファイル内の変更を確認します。

元のデバイス設定と変更されたデバイス設定の差分を表示して分析し、設定の更新プロセス中にどのような変更が行われたかを正確に把握できます。

変更リクエスト管理

変更リクエスト管理には次のような機能があります。

- [変更リクエスト（Change Request）] とそのビジネス上の正当性を [変更ログ（Change Log）] イベントにリンクできます。
- サードパーティのチケットシステムで [変更リクエスト（Change Request）] を開きます。
- Security Cloud Control での [変更リクエスト（Change Request）] の作成を許可し、変更ログイベントに関連付けます。

変更リクエスト管理の使用方法

[変更リクエスト管理（Change Request Management）] を使用して、Security Cloud Control で [変更リクエスト（Change Request）] を作成し、変更ログイベントに関連付けます。この変更要求は、変更ログ内で**名前**で検索できます。

（注） Security Cloud Control では、**変更要求トラッキング**と**変更要求管理**は同じ機能を指しています。

変更リクエスト管理の有効化

変更リクエストの追跡を有効にすると、組織内のすべてのユーザーが行った設定変更を可視化し、制御できます。

変更要求トラッキングの有効化は、組織のすべてのユーザーに影響を及ぼします。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 **管理（Administration）** > **一般設定（General Settings）** の順に選択します。

ステップ 3 [変更リクエストのトラッキング（Change Request Tracking）] トグルボタンを有効にします。



有効にすると、[変更リクエスト（Change Request）] メニューが左下隅に表示され、[変更ログ（Change Log）] ページの [変更リクエスト（Change Request）] ドロップダウンリストが使用できるようになります。

組織で変更リクエストの追跡が有効になりました。[変更リクエスト（Change Request）] メニューが左下隅に表示され、[変更ログ（Change Log）] ページに [変更リクエスト（Change Request）] ドロップダウンリストが表示されます。

変更リクエストの作成

変更リクエストを作成し、ネットワーク内のデバイスに加えられる設定変更を整理して追跡することで、変更を適切に文書化して監視できるようになります。

変更リクエストでは、関連する設定変更をグループ化し、変更の監査証跡を維持するための構造化された方法が提供されます。一度作成されると、後続のすべての変更は、アクティブな変更リクエストがクリアされるか無効になるまで、その変更リクエストに関連付けられます。

Procedure

ステップ 1 Security Cloud Control で、左下隅にある [変更リクエスト（Change Request）] メニューの [変更リクエストの作成（Create Change Request）]（+）アイコンをクリックします。

ステップ 2 [名前（Name）] と [説明（Description）] に入力します。

[名前（Name）] が組織で使用する予定の [変更リクエスト（Change Request）] 名に対応していること、そして [説明（Description）] に変更の目的が記載されていることを確認します。

Note 作成後に [変更リクエスト（Change Request）] の名前を変更することはできません。

ステップ 3 [保存（Save）] をクリックします。

Note [変更リクエスト（Change Request）] が保存されると、Security Cloud Control はすべての新しい変更を対応する [変更リクエスト（Change Request）] 名に関連付けます。この関連付けは、変更リクエストを無効化するか、メニューから変更リクエストをクリアするまで続きます。

変更リクエストが作成され、アクティブな変更リクエストになります。変更リクエスト管理を無効にするか、変更リクエストの詳細をクリアするまで、後続の設定変更はすべて、この変更リクエストに関連付けられます。

変更リクエストと変更ログイベントの関連付け

変更リクエストを変更ログイベントに関連付けて、監査証跡を残し、設定変更の理由を追跡します。

設定変更の承認と理由を文書化するために、変更リクエストを特定の変更ログイベントにリンクする必要がある場合は、この手順を使用します。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 左側のペインで、[変更ログ（Change Log）]**イベントとログ（Events & Logs）** > **ログ（Logs）** > **変更ログ（Change Log）**をクリックします。

ステップ 3 変更ログを展開して、[変更リクエスト（Change Request）] に関連付けるイベントを表示します。

ステップ 4 対応する変更ログエントリの横にあるドロップダウンリストをクリックします。

Note 最新の変更リクエストが変更リクエストリストの一番上に表示されます。

ステップ 5 変更リクエストを選択して、[選択（Select）] をクリックします。

変更リクエストが変更ログイベントに関連付けられ、承認と設定変更の間にトレース可能なリンクが作成されます。

変更リクエストを使用した変更ログイベントの検索

このタスクでは、関連する変更リクエスト名を検索することによって、特定の変更ログイベントを見つけることができ、変更とそれに対応するドキュメントを追跡できるようになります。

監査、追跡、または分析の目的で、特定の変更リクエストにリンクされている変更ログイベントを検索する必要がある場合に、この手順を使用します。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 左側のペインで、[変更ログ（Change Log）]**イベントとログ（Events & Logs）** > **ログ（Logs）** > **変更ログ（Change Log）**をクリックします。

ステップ 3 [変更ログ（Change Log）] 検索フィールドに、変更リクエストの名前を入力して、関連付けられた変更ログイベントを検索します。

Security Cloud Control は、完全に一致する変更ログイベントを強調表示します。

検索条件に一致する変更ログイベントが表示されます。完全一致は強調表示され、簡単に特定できます。

変更リクエストの検索

部分一致を使用して名前や説明で検索することにより、ユーザーは既存の変更リクエストをすばやく見つけることができます。

システム内の複数のエントリ間で特定の変更リクエストを見つける必要がある場合は、この検索機能を使用します。

Procedure

ステップ 1 Security Cloud Control で、左下隅にある [変更リクエスト（Change Request）] メニューの [変更リクエストの作成（Create Change Request）]（+）アイコンをクリックします。

ステップ 2 [検索（Search）] フィールドに [変更リクエスト（Change Request）] の名前または関連するキーワードを入力します。値を入力すると、入力内容と部分的に一致する結果が [名前（Name）] フィールドと [説明（Description）] フィールドの両方に表示されます。

検索条件に一致する変更リクエストが名前フィールドと説明フィールドの両方に表示されるため、目的の変更リクエストをすばやく見つけることができます。

変更リクエストのフィルタ処理

変更リクエストをフィルタ処理して、セキュリティ環境内の特定の設定変更やイベントをすばやく見つけて確認できます。

変更ログのフィルタ機能を使用して、特定の基準に基づいて変更リクエストのリストを絞り込むことができます。この操作により、デバイス全体の設定変更を効率的に確認および管理できます。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 左側のペインで、[変更ログ（Change Log）]**イベントとログ（Events & Logs）** > **ログ（Logs）** > **変更ログ（Change Log）**をクリックします。

ステップ 3 フィルタアイコンをクリックすると、すべてのオプションが表示されます。

ステップ 4 [検索（search）] フィールドに、[変更リクエスト（Change Request）] の名前を入力します。

値を入力すると、入力した値と部分一致する結果が表示されます。

ステップ 5 対応するチェックボックスをオンにして、変更リクエストを選択します。

一致したものが [変更ログ（Change Log）] テーブルに表示されます。Security Cloud Control により、完全一致の変更ログイベントが強調表示されます。

[変更ログ（Change Log）] テーブルには、検索条件に一致するフィルタ処理された変更リクエストのみが表示されます。完全一致は強調表示され、簡単に特定できます。

変更リクエストツールバーのクリア

変更リクエストツールバーをクリアすると、変更ログイベントが既存の変更リクエストに自動的に関連付けられることを防ぐことができます。

変更ログイベントが既存の変更リクエストに自動的に関連付けられるのを防ぐ必要がある場合は、変更リクエストツールバーの情報をクリアします。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 左下隅にある [変更リクエスト（Change Request）] メニューの [変更リクエストの作成（Create Change Request）]（+）アイコンをクリックします。

ステップ 3 [クリア（Clear）] をクリックします。

[変更リクエスト（Change Request）] メニューに [なし（None）] と表示されます。

変更リクエストツールバーがクリアされ、[なし（None）] と表示され、変更ログイベントが既存の変更リクエストに自動的に関連付けられなくなります。

変更ログイベントと関連付けられた変更リクエストのクリア

このタスクでは、接続が不要になった場合や誤って作成された場合に、変更リクエストと変更ログイベント間の関連付けを削除できます。

この手順は、変更ログインターフェイスで変更ログイベントから変更リクエストの関連付けを解除する必要がある場合に使用します。不要な接続を削除することで、変更を正確に追跡し、整理できるようになります。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 左側のペインで、[変更ログ（Change Log）]**イベントとログ（Events & Logs）** > **ログ（Logs）** > **変更ログ（Change Log**）をクリックします。

ステップ 3 [変更ログ（Change Log）] を展開して、[変更リクエスト（Change Requests）] との関連付けを解除するイベントを表示します。

ステップ 4 対応する変更ログエントリの横にあるドロップダウンリストをクリックします。

ステップ 5 [クリア（Clear）] をクリックします。

変更リクエストと選択した変更ログイベントとの関連付けが正常に解除され、それらの項目間の接続が削除されました。

変更リクエストの削除

変更リクエストが不要になった場合は、変更リクエストを削除して、アクティブな変更リクエストリストから削除します。

[変更リクエスト（Change Request）] を削除するときは、[変更ログ（Change Log）] からではなく変更リクエストリストから削除します。

手順

ステップ 1 左下隅にある [変更リクエスト（Change Request）] メニューの [変更リクエストの作成（Create Change Request）]（+）アイコンをクリックします。

ステップ 2 変更リクエストを選択し、ゴミ箱アイコンをクリックして削除します。

ステップ 3 チェックマークをクリックして確定します。

変更リクエストは変更リクエストリストから削除されますが、履歴参照用に変更ログには引き続き表示されます。

変更リクエスト管理の無効化

このタスクでは、アカウントで変更リクエスト管理機能が不要になった場合、その機能を無効にします。

[変更リクエスト管理（Change Request Management）] または [変更リクエストのトラッキング（Change Request Tracking）] を無効にすると、アカウントのすべてのユーザーに影響します。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 **管理（Administration）** > **一般設定（General Settings）** の順に選択します。

ステップ 3 [変更リクエストのトラッキング（Change Request Tracking）] トグルボタンを無効化します。

変更リクエスト管理および変更リクエスト追跡の機能が、アカウント内のすべてのユーザーに対して無効になります。

変更リクエストの管理と変更ログイベントの関連付け

このタスクは、ファイアウォールデバイスに加えられた変更を追跡し、それらを変更リクエストに関連付けて、外部システムで維持されているチケットを解決するのに役立ちます。変更リクエストを作成し、変更ログイベントを関連付けて、特定の変更リクエストに関連するイベントを検索できます。

これらのユースケースは、変更リクエスト管理が有効化されていることを前提としています。さまざまなシナリオで変更リクエスト管理を使用して、監査証跡を維持し、ファイアウォールの変更を外部のチケットシステムに関連付けることができます。

手順

ステップ 1 外部システムで維持されているチケットを解決するために、ファイアウォールデバイスに加えられた変更を追跡します。

このユースケースでは、外部システムで維持されているチケットを解決するためにファイアウォールデバイスに変更を加え、これらのファイアウォールの変更から生じる変更ログイベントを変更リクエストに関連付けるシナリオについて説明します。

1. 変更リクエストの作成 （5 ページ）。
2. 外部システムのチケット名またはチケット番号を変更リクエストの名前に使用し、[説明（Description）] フィールドに変更の理由とその他の関連情報を追加します。
3. 新しい変更リクエストが変更リクエストツールバーに表示されることを確認します。
4. ファイアウォールデバイスを変更します。
5. ナビゲーションウィンドウで [変更ログ（Change Log）] をクリックし、新しい変更リクエストに関連付けられている変更ログイベントを見つけます。
6. 変更リクエストツールバーのクリア （8 ページ）、変更ログイベントが既存の変更リクエストに自動的に関連付けられないようにします。

ステップ 2 ファイアウォールデバイスの変更が行われた後、個々の変更ログイベントを手動で更新します。

このユースケースでは、ファイアウォールデバイスの変更を行って外部システムで維持されているチケットを解決したものの、変更リクエスト管理機能を使用して変更リクエストを変更ログイベントに関連付けるのを忘れたというシナリオについて説明します。チケット番号を使用して変更ログイベントを更新します。

1. 変更リクエストの作成 （5 ページ）。変更リクエストの名前として、外部システムからのチケット名または番号を使用します。[説明（Description）] フィールドを使用して、変更の理由とその他の関連情報を追加します。
2. ナビゲーションウィンドウで [変更ログ（Change Log）] をクリックし、変更に関連付けられている変更ログイベントを検索します。
3. 変更リクエストと変更ログイベントの関連付け （6 ページ）。
4. 変更リクエストツールバーのクリア （8 ページ）、変更ログイベントが既存の変更リクエストに自動的に関連付けられないようにします。

ステップ 3 変更リクエストに関連付けられた変更ログイベントを検索します。

このユースケースでは、外部システムで維持されているチケットを解決するために行われた作業の結果として、どのような変更ログイベントが変更ログに記録されたかを知りたいというシナリオについて説明します。

1. ナビゲーションウィンドウで、[変更ログ（Change Log）] をクリックします。

2. 次のいずれかの方法を使用して、変更リクエストに関連付けられた変更ログイベントを検索します。
   - [変更ログ（Change Log）]検索フィールドに、変更リクエストの正確な名前を入力して、その変更リクエストに関連付けられた変更ログイベントを検索します。Security Cloud Control により、完全一致の変更ログイベントが強調表示されます。
   - 変更リクエストのフィルタ処理 （8 ページ） を実行して変更ログイベントを検索します。
3. 各変更ログを表示して、関連する変更リクエストを示す強調表示された変更ログイベントを見つけます。

変更リクエストが正常に管理され、変更ログイベントが外部チケットに関連付けられました。変更ログには、変更リクエストにリンクされた追跡可能なイベントが含まれるようになり、ファイアウォール変更の監査証跡が提供されます。

変更ログのエクスポート

変更ログデータをカンマ区切り値（.csv）ファイルにエクスポートして、システム外での変更レコードのフィルタリング、ソート、分析を可能にします。

Security Cloud Control 変更ログのすべてまたは一部をカンマ区切り値（.csv）ファイルにエクスポートし、必要に応じて情報をフィルタリングしたり、並べ替えたりできます。

変更ログを .csv ファイルにエクスポートするには、次の手順を実行します。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 左側のペインで、[変更ログ（Change Log）]**イベントとログ（Events & Logs）** > **ログ（Logs）** > **変更ログ（Change Log）**をクリックします。

ステップ 3 次のいずれかのタスクを実行して、エクスポートする変更を見つけます。

- フィルタ（フィルタアイコン）と検索フィールドを使用して、エクスポートするものを見つけます。たとえば、デバイスでフィルタリングして、選択した 1 つまたは複数のデバイスの変更のみを表示します。
- 変更ログのすべてのフィルタリングおよび検索条件をクリアします。これにより、変更ログ全体をエクスポートできます。



Note Security Cloud Control は 1 年間の変更ログデータを保持します。1 年間分の変更ログ履歴全体をダウンロードするよりも、変更ログの内容をフィルタリングし、その結果を .csv ファイルとしてダウンロードすることをお勧めします。

ステップ 4 ページの右上隅にあるエクスポート  アイコンをクリックします。

ステップ 5 .csv ファイルにわかりやすい名前を付けてローカルファイルシステムに保存します。

変更ログデータはローカルシステム上の CSV ファイルにエクスポートされ、必要に応じて追加のフィルタリング、ソート、および分析を実行できます。

Security Cloud Control の変更ログのキャパシティとエクスポートした変更ログのサイズの差異

変更ログのキャパシティの違いとは、次のようなデータストレージの相違点です。

- Security Cloud Control のデータベースに保存されている完全な変更ログ情報と、エクスポートされたファイルに含まれる情報のサブセットを区別します。
- データベース操作とエクスポート機能ではストレージ要件が異なることに起因します。
- ユーザーが変更ログデータをエクスポートするときのファイルサイズに影響します。

変更ログのストレージ構造

すべての変更ログについて、Security Cloud Control はデバイスの設定の 2 つのコピーを保存します。1 つは「開始」設定、もう 1 つはクローズされた変更ログの場合は「終了」設定、オープンな変更ログの場合は「最新」設定です。これにより、Security Cloud Control は設定の違いを並べて表示できます。さらに、Security Cloud Control は、変更を行ったユーザー名、変更が行われた時刻、およびその他の詳細とともに、すべてのステップ（「変更イベント」）を追跡して保存します。

ただし、変更ログをエクスポートする場合、エクスポートには設定の 2 つの完全なコピーは含まれません。これには「変更イベント」のみが含まれるため、エクスポートファイルは Security Cloud Control に保存されている変更ログよりもはるかに小さくなります。

Security Cloud Control は、1 年分の変更ログ情報を保存します。これには、設定の 2 つのコピーが含まれます。

Security Cloud Control でのジョブモニタリング

Security Cloud Control でのジョブモニタリングは、次のことを行う管理インターフェイスです。

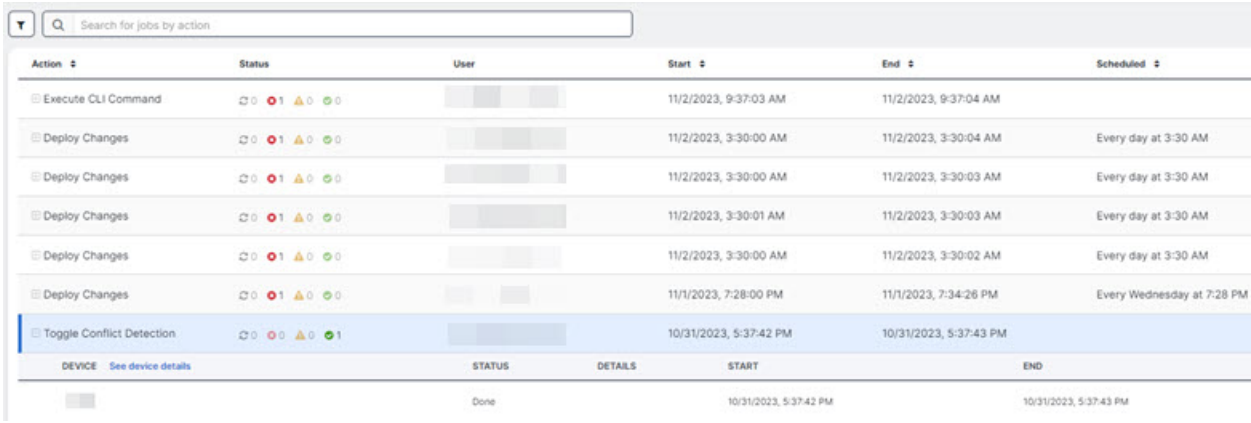
- 複数デバイスの再接続、複数デバイスからの設定の読み取り、複数デバイスの同時アップグレードなど、一括操作の進行状況の概要を示します。
- 個々のアクションのステータスとともに色分けされた行を使用し、それぞれが成功したか失敗したかを示します。
- 行を展開すると、一括操作の影響を受ける各デバイスの結果が表示されます。

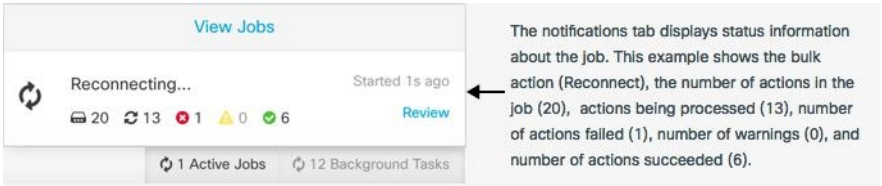
ジョブへのアクセス方法

[ジョブ（Jobs）] ページには、次の 2 つの方法でアクセスできます。

- [通知（Notification）] タブで、新しいジョブ通知があるときに、[確認（Review）] リンクをクリックします。[ジョブ（Jobs）] ページにリダイレクトされ、通知に対応する特定のジョブが表示されます。
- 左側のペインで **イベントとログ（Events & Logs）** > **イベント（Events）] 見出し** > **ジョブ（Jobs）** をクリックします。この表には、Security Cloud Control で実行される一括操作の完全なリストが示されます。

表の 1 行は、1 回の一括操作を表します。この 1 回の一括操作は、たとえば、20 台のデバイスを再接続する試みだった可能性があります。[ジョブ（Jobs）] ページの行を展開すると、一括操作の影響を受ける各デバイスの結果が表示されます。





[ジョブ（Jobs）] ページでは、異なるアクション、アクションを実行したユーザー、アクションのステータスによってフィルタ処理および検索を実行できます。

一括アクションの再開

このタスクでは、ジョブ全体を再実行せずに、一括操作内の失敗したアクションを再試行できます。

[ジョブ（Jobs）] ページを確認して、一括アクションの 1 つまたは複数のアクションの失敗が判明した場合は、必要な修正を行ってから一括アクションを再試行できます。Security Cloud Control は、失敗したアクションのみを対象にジョブを再度実行します。

Procedure

ステップ 1 [ジョブ（Jobs）] ページで、アクションの失敗を示す行を選択します。

ステップ 2 [再試行（Retry）]（↻）アイコンをクリックします。

元の一括操作で失敗したアクションのみが再試行され、ジョブのステータスはそれに応じて更新されます。

一括アクションのキャンセル

想定よりも時間がかかっている可能性がある、または不要になった複数のデバイスで進行中の操作を停止する必要がある場合、現在進行中の一括アクションをキャンセルします。

複数のデバイスで現在進行中の一括アクションをキャンセルできます。たとえば、4 台の管理対象デバイスを再接続しようとして、そのうち 3 台が正常に再接続されたが、4 台目のデバイスがまだ接続も切断もされていない場合は、一括アクションをキャンセルできます。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 左側のペインで **イベントとログ（Events & Logs）** > **イベント（Events）] 見出し** > **ジョブ（Jobs）** をクリックします。

ステップ 3 実行中の一括アクションを特定し、右側にある [キャンセル（Cancel）] リンクをクリックします。

Note 一括アクションの一部が成功している場合、それを元に戻すことはできません。進行中のアクションがキャンセルされます。

一括アクションがキャンセルされ、進行中の操作は停止しますが、正常に完了した部分は保持されます。

Security Cloud Control でのワークフローのモニタリング

ワークフローモニタリングは、次のような Security Cloud Control 機能です。

- デバイス、Secure Device Connector（SDC）、または Secure Event Connector（SEC）と通信するとき、およびルールセットの変更をデバイスに適用するときに、Security Cloud Control が実行するすべてのプロセスを追跡します。

- 各ステップのワークフローテーブルにエントリを作成し、その結果を表示します。
- Security Cloud Control によって実行されるアクションについての情報のみが含まれており、通信対象のデバイスについての情報は含まれません。

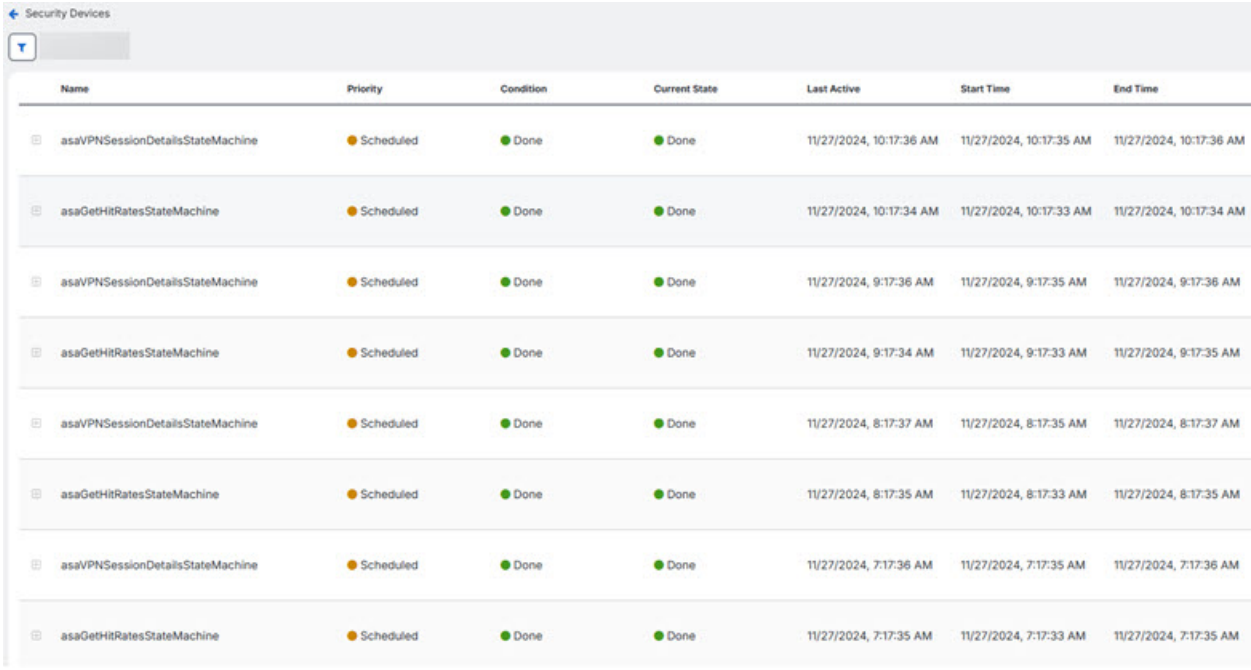
ワークフローエラーのレポートと障害対応

Security Cloud Control は、デバイスでタスクの実行に失敗した場合にエラーを報告します。詳細については、[ワークフロー（Workflows）] ページに移動して、エラーが発生したステップを確認してください。

このページでは他にも必要に応じて、エラーの特定とトラブルシュートや TAC との情報共有ができます。

[ワークフロー（Workflows）] ページに移動するには、左側のペインの [セキュリティデバイス（Security Devices）] をクリックして、[デバイス（Devices）] タブをクリックします。適切なデバイスタイプタブをクリックしてデバイスを特定し、必要なデバイスを選択します。右側のペインの [デバイスとアクション（Devices and Actions）] で、[ワークフロー（Workflows）] をクリックします。

図 *1 :* ワークフローテーブルにエントリが表示される *[*ワークフロー（*Workflows*）*]* ページ



デバイスワークフローのエクスポート：

- 完全なワークフロー情報を JSON ファイルにダウンロードして、TAC チームから詳細な分析情報を求められたときに提供できます。ワークフロー情報をエクスポートするには、該当するデバイスを選択してその [ワークフロー（Workflows）] ページに移動し、右上隅に表示されるエクスポート（ ）アイコンをクリックします。

スタックトレースのコピー：

- 解決できないエラーがあって TAC に問い合わせた場合、TAC からスタックトレースのコピーを求められる場合があります。エラーのスタックトレースを収集するには、[スタックトレース（Stack Trace）] リンクをクリックし、[スタックトレースのコピー（Copy Stacktrace）] をクリックして、画面に表示されるスタックをクリップボードにコピーします。

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。