



# Server Automation

ソフトウェアバージョン: 10.50

## 統合ガイド

ドキュメントリリース日: 2016年7月 (英語版)

ソフトウェアリリース日: 2016年7月



**Hewlett Packard**  
Enterprise

## ご注意

### 保証

Hewlett Packard Enterprise製品、またはサービスの保証は、当該製品、およびサービスに付随する明示的な保証文によってのみ規定されるものとします。ここでの記載は、追加保証を提供するものではありません。ここに含まれる技術的、編集上の誤り、または欠如について、Hewlett Packard Enterpriseはいかなる責任も負いません。

ここに記載する情報は、予告なしに変更されることがあります。

### 権利の制限

機密性のあるコンピューターソフトウェアです。これらを所有、使用、または複製するには、Hewlett Packard Enterpriseからの有効な使用許諾が必要です。商用コンピューターソフトウェア、コンピューターソフトウェアに関する文書類、および商用アイテムの技術データは、FAR 12.211および12.212の規定に従い、ベンダーの標準商用ライセンスに基づいて米国政府に使用許諾が付与されます。

### 著作権について

© Copyright 2000-2016 Hewlett Packard Enterprise Development LP

### 商標について

Adobe®は、Adobe Systems Incorporated (アドビシステムズ社) の登録商標です。

Microsoft®およびWindows®は、Microsoft Corporationの米国における登録商標です。

UNIX®は、The Open Groupの登録商標です。

## ドキュメントの更新情報

このマニュアルの表紙には、以下の識別情報が記載されています。

- ソフトウェアバージョン番号: ソフトウェアバージョンを示します。
- ドキュメントリリース日: ドキュメントが更新されるたびに変更されます。
- ソフトウェアリリース日: このソフトウェアバージョンのリリース日を示します。

更新状況、およびご使用のドキュメントが最新版かどうかは、次のサイトで確認できます。<https://softwaresupport.hpe.com/>

このサイトを利用するには、HPE Passportへの登録とサインインが必要です。HPE Passport IDの登録は、HPEソフトウェアサポートサイトで **[Register]** をクリックするか、HPE Passportのログインページで **[Create an Account]** をクリックしてください。

適切な製品サポートサービスをお申し込みいただいたお客様は、最新版または最新版をご入手いただけます。詳細は、HPEの営業担当にお問い合わせください。

## サポート

HPEソフトウェアサポートサイトを参照してください。<https://softwaresupport.hpe.com>

このサイトでは、HPEのお客様窓口のほか、HPEソフトウェアが提供する製品、サービス、およびサポートに関する詳細情報をご覧いただけます。

HPEソフトウェアオンラインではセルフソルブ機能を提供しています。お客様のビジネスを管理するのに必要な対話型の技術サポートツールに、素早く効率的にアクセスできます。HPEソフトウェアサポートのWebサイトでは、次のようなことができます。

- 関心のあるナレッジドキュメントの検索
- サポートケースの登録とエンハンスメント要求のトラッキング
- ソフトウェアバッチのダウンロード
- サポート契約の管理
- HPEサポート窓口の検索
- 利用可能なサービスに関する情報の閲覧
- 他のソフトウェアカスタマーとの意見交換
- ソフトウェアトレーニングの検索と登録

一部のサポートを除き、サポートのご利用には、HPE Passportユーザーとしてご登録の上、サインインしていただく必要があります。また、多くのサポートのご利用には、サポート契約が必要です。HPE Passport IDを登録するには、HPEサポートサイトで **[Register]** をクリックするか、HPE Passportのログインページで **[Create an Account]** をクリックします。

アクセスレベルの詳細については、次のWebサイトをご覧ください。<https://softwaresupport.hpe.com/web/softwaresupport/access-levels>

**HPE Software Solutions Now**では、HPESWソリューションおよび統合ポータルWebサイトにアクセスできます。このサイトでは、お客様のビジネスニーズに合ったHPE製品ソリューションをご覧いただけます。また、HPE製品間の統合リストとITILプロセスのリストも用意しています。このWebサイトのURLは<https://softwaresupport.hpe.com/>です。

# 目次

概要 .....	7
NAとの統合 .....	8
概要 .....	8
NA/SA統合の機能 .....	9
NAデータ収集 .....	10
統合のセットアップ .....	11
SAクライアントとNAの通信 .....	11
SA構成の変更 .....	11
統合用のNAの構成 .....	12
トポロジデータの収集 .....	15
トラブルシューティング .....	15
前提条件 .....	16
時間の要件 .....	16
NA統合ポートの要件 .....	16
SAクライアントでのNAホストのリセット .....	17
ユースケース .....	17
ネットワークデバイスとサーバー間の接続 .....	18
SAのネットワークデバイス情報 .....	19
ネットワークインタフェースの表示 .....	20
ネットワークポートの表示 .....	21
NAのネットワークデバイス情報 .....	22
イベント履歴の表示 .....	22
デュプレックスの不一致 .....	23
ネットワークレポート .....	24
ネットワーク図 .....	25
HPE Server Automation Visualizerの起動 .....	25
NAとSA Global Shell .....	26
推定される物理接続 .....	27
デバイスグループとNA .....	27
SA-NA統合のトラブルシューティング .....	28

OOとの統合 .....	29
概要 .....	29
補足情報 .....	29
SA-OOジョブ .....	31
ジョブステータスの値 .....	36
統合のセットアップ .....	37
OOフローのセットアップ .....	37
OOジョブのセットアップ .....	40
ユースケース: SA-OOフロー .....	40
管理者: OOフローの構成 .....	40
フローを構成するには、次の手順を実行します。 .....	41
フローの変更と設定を確認するには、次の手順を実行します。 .....	42
ユーザー: OOフローの実行 .....	43
フローを実行するには、次の手順を実行します。 .....	44
サーバーを追加または削除するには、次の手順を実行します。 .....	48
SA-OO統合のトラブルシューティング .....	48
SA-OO接続エラー .....	48
フローの実行エラー .....	49
ユースケース: SA-OOジョブ .....	49
管理者: OOジョブの構成 .....	49
ジョブのブロック .....	50
ブロックされるジョブとは .....	50
ジョブをブロックする理由 .....	51
ジョブのブロックとブロック解除の実行方法 .....	51
ジョブのブロックを無効にする方法 .....	53
ブロックされたジョブの情報の表示方法 .....	53
ブロックされたジョブのステータスをジョブログでチェック .....	54
フロー設定の構成または編集 .....	55
ブロックされたジョブの承認と削除 .....	57
uCMDB Connectorとの統合 .....	58
概要 .....	58
SA-uCMDB統合のセットアップ .....	58
SA-uCMDB Connectorのダウンロード .....	59
SA-uCMDB Connectorの有効化と起動 .....	60

enableコマンド .....	60
uCMDBサーバーに送られるSAデータのカスタマイズ .....	62
マッピングファイル .....	62
マッピングファイルのカスタマイズ .....	63
マッピングファイルの編集 .....	64
SAカスタム属性の使用方法 .....	67
追加の標準マッピング .....	69
データ変換関数のカスタマイズ .....	69
ユースケース .....	73
SA-uCMDB統合のトラブルシューティング .....	82
別のコアでのSA-uCMDB Connectorの実行 .....	82
オンデマンド同期 .....	83
ログファイルの表示 .....	83
SA-uCMDB Connectorデーモン .....	84
HPELNとの統合 .....	89
概要 .....	89
統合のセットアップ .....	89
前提条件 .....	90
Live Networkコネクタの構成 .....	90
サービスとストリーム .....	92
サービスとストリームの表示 .....	93
コンテンツストリームとセキュリティストリームの構成 .....	94
Microsoft Patch Supplementストリームの構成 .....	94
ソフトウェア検出ストリームの構成 .....	95
SA DMAストリームの構成 .....	96
コンテンツのオペレーティングシステムプラットフォームファミリのストリームの構成 .....	96
Solarisパッチ供給ストリームの構成 .....	97
セキュリティスキャナーストリームの構成 .....	97
SA脆弱性コンテンツストリームの構成 .....	98
SAコンプライアンスコンテンツストリームの構成 .....	98
ユースケース .....	99
一般的なトラブルシューティングのヒント .....	99
接続の問題 .....	101
コマンドオプション、コマンドラインオプション、コンテンツのインポート、ログファイル	101
コマンドオプション .....	101

コマンドラインオプション .....	104
コンテンツのプレビュー (--preview) .....	106
コンテンツのインポート .....	108
Live Networkコネクターのログファイル .....	108
標準コンテンツストリーム .....	108
SA脆弱性コンテンツストリーム .....	109
コンプライアンスコンテンツストリーム .....	111
DMAとの統合 .....	113
DMAの概要 .....	113
統合タスク .....	113
OBRとの統合 .....	114
HPE OBRの概要 .....	114
OBRとの統合 .....	114
ドキュメントのフィードバックを送信 .....	117

## 概要

本書では、SAと他のHPE製品との統合について説明します。

- 「DMAとの統合」(113ページ)
- 「OBRとの統合」(114ページ)
- 「HPELNとの統合」(89ページ)
- 「uCMDB Connectorとの統合」(58ページ)
- 「OOとの統合」(29ページ)
- 「NAとの統合」(8ページ)

# NAとの統合

ここでは、SAとNAの統合について説明します。

## 概要

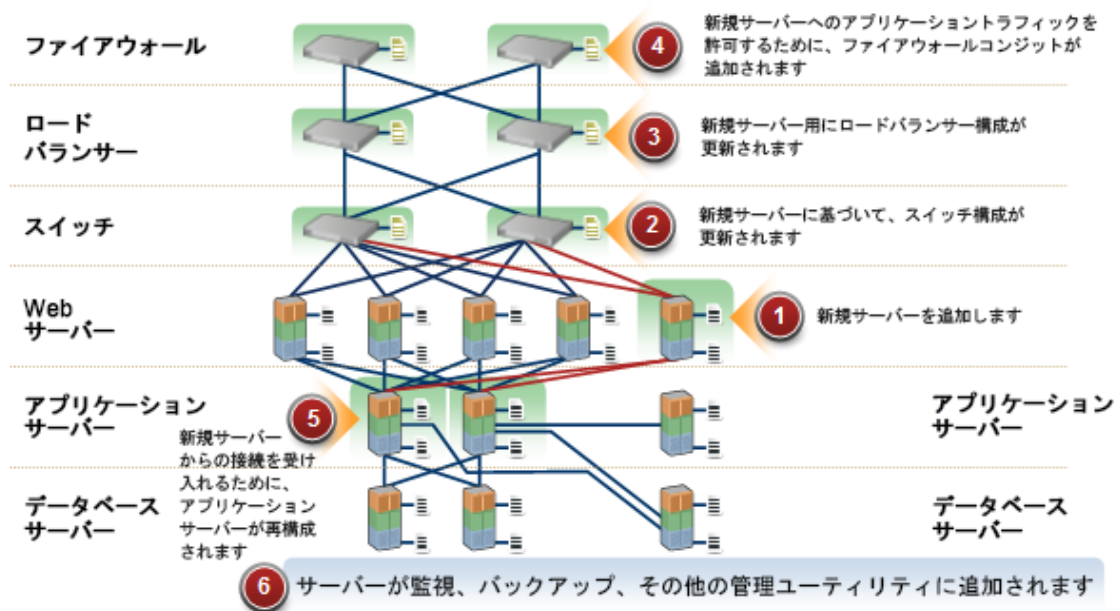
IT環境を変更するときは、往々にして、ネットワーク管理者、システム管理者、アプリケーション技術者が調整して作業することが必要になります。これは、管理するアプリケーション環境が、さまざまなオペレーティングシステムのサーバーやネットワークデバイスで構成されており、ファイアウォール、ロードバランサー、スイッチ、サーバー、Webアプリケーションなどが含まれるためです。

たとえば、環境によっては、アプリケーション環境のネットワークデバイス(ロードバランサー、ファイアウォール、スイッチなど)への変更が必要になります。

NA/SA統合では、ユーザーがサーバーとネットワークデバイスの接続状態を把握し、管理対象サーバーをきめ細かくチェックできるようにすることで、これらのプロセスを容易にしています。この情報に基づいて、デバイスの相互関係を確認し、必要な変更を調整および実施します。

NA/SA統合で実行できる調整タスクの一部を次の図に示します。

### SA-NA統合を使用した調整タスクの概要





統合を確立したら、デバイスの詳細を表示し、ネットワークデバイスとサーバー間の接続を検査し、デュプレックスの不一致を識別し、デバイスの複合履歴情報を表示できます。また、この項には、環境全体への変更の実装と、ネットワークレポートの生成に関する情報も記述しています。

統合化された方法で、環境の変更 (サーバーの再配置など) を行い、サーバーおよびネットワークデバイス全体の整合性を保証し、デュプレックスの不一致を検出して解決するため、NA/SA統合には次のインタフェースポイントが用意されています。

- HPE Server Automation (SA)
- Network Automation (NA)
- SA Global Shell
- HPE Server Automation Visualizer (SA内)
- HPEレポート (SA内)

## NA/SA統合の機能

NA/SA統合を構成したら、次のタスクを実行できます。

- SAの管理対象サーバーとそれにアタッチされるネットワークデバイス、およびそれらのネットワーク接続 (インタフェースとポート) についてのハードウェア情報の詳細を表示する。
- SA Global File System (OGFS) を使用して、次の操作を実行する。
  - 管理対象サーバーと接続ネットワークデバイス間を、関連付けられた物理接続をたどってナビゲートする
  - ネットワークデバイスの構成を検出する
  - サーバーとネットワークデバイスにまたがってスクリプトを実行する。
- NASクリプトをSAスクリプトから呼び出して、サーバーおよびネットワークデバイスにまたがる操作を自動化する。
- SAとNAの機能を使用して、環境内の管理対象サーバー、ネットワークデバイス、レイヤー2 (および推奨されるレイヤー1) 接続を示す図を作成する。
- SAを使用して、管理対象サーバーとネットワークデバイス間の構成上のデュプレックスの不一致を識別し、トラブルシューティングし、修復する。
- SAを使用して、サーバーとネットワークデバイスの両方を含むことができるSAデバイスグループに対してアクションを実行する。

- SAを使用して、環境内のアプリケーションに加えられた変更を記録する、サーバーとネットワークデバイスの複合イベント履歴ログを確認する。
- SAを使用して、複合イベント履歴ログをCSVファイルやHTMLファイルにエクスポートする。
- NAを使用して、ネットワークデバイスの追加詳細情報とイベント履歴に直接アクセスする。
- SAでネットワークレポートを実行して、レイヤー2接続と推定されるレイヤー1接続および構成上の不一致 (デュプレックスのコンプライアンス) を識別する。

**注:** このドキュメントに記述された接続という語は、注記がある場合を除き、物理的な接続を意味します。

## NAデータ収集

NA/SA統合機能では、NATポロジデータの収集およびNA通信モードデータの収集診断ツールを使用して、ネットワークデバイスに関する情報が収集されます。

### NATポロジデータの収集診断

NATポロジデータの収集診断は、すべてのスイッチのMACアドレスを収集するようNAに指示します。MACアドレスを使用すると、物理接続を検出してSAデータモデルに追加することができます。

たとえば、サーバーをスイッチに追加すると、次回NATポロジデータの収集診断が実行されたときにその情報が収集されます。NATポロジデータの収集診断やNA通信モードデータの収集診断は、特定のネットワークデバイスに対して手動で実行することもできます。これらの診断の詳細については、『SA 10.50 ユーザーガイド』を参照してください。

**注:** NAのパフォーマンス上の理由から、これらの診断を複数のデバイスに対して実行するのは、1週間あたり1度までにしてください。NAデータを高い頻度で更新する必要がある場合は、サポート担当者に相談してください。1つのデバイスに対してこれらの診断を実行する場合は、頻度を高くすることができます。

### NA通信モードデータの収集診断

ネットワークデバイスについては、NA通信モードデータの収集診断によって速度とデュプレックスが収集されます。この診断は、デバイスがNAに初めて追加されたときに実行され、その後は定義するスケジュールに従って実行されます。

ネットワークデバイスの速度とデュプレックスの情報が最新であることを保証するには、診断を実行する定期的なスケジュールを設定することを推奨します。この診断とスケジュール設定の詳細については、「[デュプレックスの不一致](#)」および『SA 10.50 ユーザーガイド』を参照してください。

### NAデータベース/SAデータベース

NAデータベースとSAデータベースは統合されません (NAとSAでそれぞれ独自のデータを管理します)。

## 認証

SA/NAの統合機能については、SAIによって認証が処理されます。詳細については、「[前提条件](#)」を参照してください。NAのみの機能については、引き続きNAの資格情報を使用して認証が行われます。

# 統合のセットアップ

SA管理者は、SAコアサーバーでいくつかのタスクを実行して、NA/SA統合を有効にする必要があります。

設定作業では、NAとSAの両方について構成設定をいくつか変更し、NAトポロジデータの診断を実行し、ユーザーのアクセス権をいくつか構成します。

統合はNAコアのフェイルオーバーをサポートしていません。統合されたNAコアが別のNAコアにフェイルオーバーする場合、新しいNAコアに接続するために、HPE SAのtwist.confのtwist.nasdata.hostを新しいNAコアに変更する必要があります。詳細については、「[SA構成の変更](#)」の「[NAサーバー名の指定](#)」を参照してください。

## SAクライアントとNAの通信

SAクライアントがNAと通信できることを確認してください。SAクライアントとNAサーバーが通信できない場合は、「[SAクライアントでのNAホストのリセット](#)」を参照してください。

## SA構成の変更

次のタスクを実行して、SAをNA統合用に準備します。

- **NAサーバー名の指定**

NA/SA統合が機能するのは、SA twist.conf (/etc/opt/opsware/twist/twist.conf) 内にNAのFQDNがtwist.nasdata.host=<NAサーバーのFQDN> の形式で構成されている場合に限りです。

このファイルの変更の詳細については、『SA管理ガイド』を参照してください。

複数のスライスコンポーネントバンドルをインストール済みの場合は、すべてのスライスについて

twist.confファイルを編集する必要があります。次に、すべてのNAサービスとWebサービスデータアクセスエンジンをスライスコンポーネントバンドルごとに再起動する必要があります。

- **SAでのNAポート (Windowsのみ) の指定**

NAがWindowsサーバーで実行されている場合は、/etc/opt/opsware/hub/hub.confファイルのポート設定パラメーターをnas.port=8022からnas.port=22に変更する必要があります。


デフォルトのWindowsサーバーインストールでは、ポート22/23でプロキシSSH/Telnetサーバーが実行されます。Unixデフォルトの8022/8023ポートではありません。

この構成変更を実行したら、スライスコンポーネントバンドルをホストしているサーバーを再起動する必要があります。

- spin.cronbot.check\_duplex.enabledパラメーターの有効化

spin.cronbot.check\_duplex.enabledシステム構成パラメーターをNA統合用に有効にする必要があります。

このシステム構成パラメーターを有効にするには、次の手順を実行します。

- a. SAクライアントで[管理]タブを選択します。
- b. ナビゲーションペインで[システム構成]を選択します。これにより、システム構成パラメーターを含むSAコンポーネント、ファシリティ、およびレルムが表示されます。
- c. SAコンポーネントのリストで、[データアクセスエンジン]を選択します。これにより、そのコンポーネントのシステム構成パラメーターが表示されます。
- d. パラメーターspin.cronbot.check\_duplex.enabledを探します。
- e. [値]列で、新しい値ボタンを選択し、値を「1」に設定します。
- f. [元に戻す]ボタンを選択して変更を破棄するか、[保存]ボタンを選択して変更を保存します。

システム構成の詳細については、『SA 10.50管理ガイド』を参照してください。

## 統合用のNAの構成

**注：**NA統合を現在のSAバージョンで構成するには、互換性のあるNetwork Automation (NA) がインストールされている必要があります。詳細については、SSO (<https://softwaresupport.hpe.com/>)にある『NA Support Matrix』を参照してください。

NA管理者は、NAサーバーで次のタスクを実行する必要があります。

### SAゲートウェイの要件

NAは、統合しようとするSAコアのマスターゲートウェイを使用するように構成されている必要があります。NAでSAコアのマスターゲートウェイを指定する方法の詳細については、SSO (<https://softwaresupport.hpe.com/>)にある『NA Satellite Guide』を参照してください。

### ユーザーのアクセス権

NA/SA統合のアクセス権限は、2つの別々のデータベース (NAデータベースとSAデータベース) に基づきます。NAは、認証用に自分自身のデータベースを使用します。SAは、認証用に別のセキュリティメカニズムを使用します。ただし、NA統合については、すべての認証 (NAとSAの両方) がSAで処理されます。

NAが、SA認証を使用するように構成されていると、NAは、まずSAに対して認証を試みます。NAがSAに対する認証に失敗すると、NAデータベースにフォールバックします。NAデータベース内にアカウントがあるときは、フォールバック認証が許可されるようにそのユーザーが構成されている場合にのみ、フォールバックが許可されます。NA認証の詳細については、『NAユーザーガイド』を参照してください。

新しいユーザーがSAで認証されると、NA内にアカウントが作成されます。このアカウントは、NAの管理設定でSA認証が有効化されたときに指定されたデフォルトユーザーグループ内に配置されます。構成可能なこのユーザーグループにより、システム管理者がSAユーザーに割り当てたデフォルトのアクセス権が制御されます。

必要なアクセス権セットを持っていないければ、サーバーとネットワークデバイスは表示できません。アクセス権を取得するには、SA管理者にお問い合わせください。詳細については、『SA 10.50管理ガイド』を参照してください。

### NA認証の構成

NA/SA統合を設定するには、SA認証を使用するようにNAを構成する必要があります。この構成を開始する前に、次の情報を把握しておく必要があります ([Server Automation Software Authentication](#)を参照)。

**Twistサーバー:** Webサービスデータアクセスエンジン (twist) をホストしているサーバーのIPアドレスまたはホスト名。twistは、スライスコンポーネントバンドルの一部で、一般にSAコアホストにインストールされますが、別のホストにインストールされることもあります。

- **Twistポート番号:** Webサービスデータアクセスエンジンがリッスンするポート番号。
- **Twistユーザー名:** Webサービスデータアクセスエンジンのユーザー名。
- **Twistパスワード:** Webサービスデータアクセスエンジンのユーザーのパスワード。
- **OCCサーバー:** コマンドセンター (OCC) をホストしているサーバーのIPアドレスまたはホスト名。
- **デフォルトユーザーグループ:** 新しいSAユーザー用のデフォルトのユーザーグループ。

認証の設定をNAで変更するには、次のタスクを実行します。

1. NAにログインします。
2. **[管理] > [管理設定] > [ユーザー認証]** を選択して、**[管理設定 - ユーザー認証]** ページを表示します。
3. 次の図に示すように、**[外部認証タイプ]** セクションでラジオボタンを使用して、**HPE Server AutomationソフトウェアおよびTACACS+ (使用されている場合)** を選択します。

### NAの外部認証タイプ

The screenshot shows the 'User Authentication' configuration page. The 'External Authentication Type' section is expanded, showing the following options:

- None (Local Auth)
- HPE Server Automation Software
- HPE Server Automation Software & TACACS+
- TACACS+
- RADIUS
- SecurID
- SAML2.0

Additional information and warnings are provided for the selected options:

- WARNING:** The SAML configuration includes additional steps that must be performed before you select this option. After you perform these steps, restart NA. (To restart NA, go to [Start/Stop services](#).) For more information, see the NA Administration Guide. Incomplete SAML configuration can lead to all users being locked out from the HPE Network Automation console. (To export the Service Provider Metadata, go to [SAML Configuration and Metadata Export](#).)
- WARNING:** PKI configuration includes additional steps that must be done before selecting this option. Follow the steps outlined [here](#), before saving the settings on this page. Incomplete PKI configuration can lead to all users being locked out from the HPE Network Automation console.
- Choose the type of external authentication you would like to use.** If you choose TACACS+, RADIUS, HPE Server Automation Software, SAML, or PKI, configure that type in the related section on this page. SecurID has no additional external authentication options.

The 'Save' button is located at the top right of the configuration area.

4. スクロールダウンして、次の図に示すように、**[HPE Server Automation Software Authentication]** セクションのすべてのフィールドに入力します。

NAは、Webサービスデータアクセスエンジン (twist) のユーザー名とパスワードを使用して、レイヤー2データを収集します。NAは、Twistユーザーのアクセス権を使用して、MACアドレス別にサーバーインタフェース情報を収集します。Twistユーザーは、サーバー情報に対する読み取りアクセス権を持っている必要があります。

### HPE Server Automation Software Authentication

HPE Server Automation Software Authentication		
Twist Server	<input type="text" value="twist.c43.example.com"/>	Web Services Data Access Engine host name or IP address
Twist Port Number	<input type="text" value="1032"/>	Web Services Data Access Engine listening port (typically 1032)
Twist Username	<input type="text" value="defuser"/>	Web Services Data Access Engine Username for finding connected servers.
Twist Password	<input type="password" value="*****"/>	Web Services Data Access Engine Password for finding connected servers.
OCC Server	<input type="text" value="occ.c43.exmpale.com"/>	HPE Command Center host name for linking to connected servers.
Default User Group	<input type="text" value="Limited Access User"/>	User Group for new HPE Server Automation Software users.

5. [保存] をクリックして、構成の変更内容を保存します。

NA構成の詳細については、『NAユーザーガイド』を参照してください。

## トポロジデータの収集

SA-NA統合のタスクが完了したら、NAトポロジデータの収集およびNA通信モードデータの収集診断を実行する必要があります。これらのユーティリティを実行する手順については、『NAユーザーガイド』を参照してください。

## トラブルシューティング

SAがNAと通信しているかどうかをテストするには、次の状態を確認します。

- 自分のSA資格情報でNAにログインできること。これにより、NAがSAと通信できることが確認されます。
- [外部認証タイプ] の下のNAの[管理設定] で指定されたSA資格情報がSAに設定されていること。これにより、NAがサーバーのMACアドレスを調査できることが確認されます。
- NAトポロジデータの収集診断が正常に実行されていること。この状態を確認するには、タスクを探して、その結果をチェックします。これにより、NAがMACアドレスを収集し、SAで調査を試みたことが確認されます。

## 前提条件

統合を行うには、次の前提条件が満たされている必要があります。

- 時間の要件
- ポートの要件

## 時間の要件

SAとNAのコアサーバーは、同期していて、時刻とタイムゾーンの設定が同じである必要があります。

## NA統合ポートの要件

NA統合を構成する前に、SAとNAが、次のポートを使用して相互に通信できることを確認してください。

- **ポート1032 (NAからSAへ)**

NAは、SA Webサービスデータアクセスエンジンのコンポーネント (スライスコンポーネントバンドルの一部) を実行しているサーバー上のポート1032にアクセスできる必要があります。デフォルトでは、Webサービスデータアクセスエンジンはポート1032でリスンします。

- **ポート8022 (Unix)/ポート22 (Windows) (SAからNAへ)**

Global File System (OGFS) 機能を使用してネットワークデバイスに関するデータを表示できるようにするには、SAがポート8022 (UnixベースのNAサーバー) または22 (WindowsベースのNAサーバー) にアクセスできる必要があります。

- **NA API用のRMIポート**

NA APIは、Java RMIを使用してNAサーバーに接続します。SAは、NA統合でNA APIを使用します。RMIを使用するには、次のポートが開いている必要があります。

- **ポート1099**

- JNDI

- **ポート4444 (NAバージョン9.10以前の場合)**

- RMIオブジェクト



- **ポート4446 (NAバージョン9.20以降の場合)**  
RMIオブジェクト
- **ポート1098**  
RMIメソッド

## SAクライアントでのNAホストのリセット

使用するNA/SA統合機能によっては、ユーザーが特定のNAイベントに関する追加詳細情報にアクセスできるように、SAクライアント (Java) がNA Webインタフェースを (SAから直接) 開くことが要求される場合があります。管理者が『SAインストールガイド』のセットアップタスクを完了していても、NAホスト (サーバー) Webインタフェースを実行しているサーバーとSAクライアントが直接通信できなければ、SAクライアントでNAオプションを変更することが必要になる場合があります。たとえば、ファイアウォールが原因でSAクライアントがNAホストに到達できないのであれば、NAホストのプロキシとして動作しているサーバーの名前を指定する必要があります。これは、デフォルトの設定より優先されます。この作業は、NAホストと通信できないSAクライアントを実行しているすべてのデスクトップで実行する必要があります。

SAクライアントでNAホストをリセットするには、次の手順を実行します。

1. SAクライアントウィンドウの [ツール] メニューから [オプション] を選択します。
2. [ビュー] ペインで、[HPE Network Automation] を選択します。
3. [ホスト] フィールドにNAホストのプロキシとして動作するサーバーの名前を入力します。たとえば、「m208」(m208.example.com NAホストのプロキシ) のように入力します。
4. (オプション) [デフォルトに戻す] をクリックすると、以前に保存されているNAホスト名が復元されます。
5. (オプション) [テスト] をクリックすると、NAログインウィンドウが開きます。
6. [保存] をクリックします。

## ユースケース

SA-NA統合を正しく構成できたら、次の機能を使用できます。

- [ネットワークデバイスとサーバー間の接続](#)
- [SAのネットワークデバイス情報](#)
- [「ネットワークインタフェースの表示」\(20ページ\)](#)

- ネットワークポートの表示
- NAのネットワークデバイス情報
- デュプレックスの不一致
- ネットワークレポート
- NAとSA Global Shell
- 推定される物理接続
- デバイスグループとNA

## ネットワークデバイスとサーバー間の接続

NA/SA統合の機能は、OSI7階層モデルのレイヤー2接続および推定されるレイヤー1接続に基づいています。

### OSI7階層モデル



### データリンク接続

NA/SA統合機能には、データリンク(レイヤー2)接続を検出し、物理(レイヤー1)接続とデータリンク接続についてレポートする機能も含まれています。このようなデータリンク接続には、管理対象サーバー直

結のスイッチや他のスイッチを介して間接的に接続しているスイッチが含まれます。これらの接続は、デバイスによって報告されたMACアドレスと、サーバーとスイッチの既知のMACアドレスを関連付けることで検出されます。

### 物理接続

物理接続は、データリンク接続から推定されます(「[推定される物理接続](#)」を参照してください)。物理接続は、サーバーとスイッチ間の直接的な接続(ケーブル)を表します。

物理接続は、SAクライアントでは、サーバーエクスプローラー、ネットワークデバイスエクスプローラー、およびService Automation Visualizer (SAV)の詳細レイアウト図に表示できます。NAのダイアグラム機能では、物理接続、データリンク接続、またはネットワーク(レイヤー3)接続を表示できます。

## SAのネットワークデバイス情報

NA/SA統合機能では、管理対象サーバーとネットワークデバイスに関する基本的なハードウェア詳細に加えて、ネットワークインタフェースとネットワークポートに関する次の情報もレポートされます。

- サーバー側のネットワークインタフェースには、次のプロパティがあります。
  - MACアドレス
  - サブネットマスク
  - インタフェースタイプ
  - IPアドレス
  - DHCP設定
  - 接続されているスイッチポート
  - 速度
  - デュプレックス (Windowsを除く)
- ネットワークデバイス側のネットワークポートには、次のプロパティがあります。
  - ポート名
  - 速度
  - デュプレックス設定
  - 接続されているデバイス
  - インタフェースタイプ

**注:** ほとんどのデバイスでは、接続の両側(サーバーとネットワークデバイス)が自動ネゴシエートモードに設定されていれば、自動ネゴシエーションが最も有効に機能します。たとえば、デュプレックスポリ

シーで、ポートがフル、ハーフ、または自動に設定されるように指定し、フル(自動)にならないように指定できます。フル(自動)のデュプレックス設定は、ポートが自動ネゴシエートに設定され、ネゴシエートの結果フルデュプレックスになったことを示します。

ここからのタスクでは、サーバーおよびネットワークデバイスの詳細なハードウェア情報にSAで直接アクセスする方法について説明します。ネットワークデバイスに関するハードウェア情報にNAで直接アクセスする手順については、「[NAのネットワークデバイス情報](#)」を参照してください。

## ネットワークインタフェースの表示

サーバーに関するハードウェア情報 (ネットワークインタフェースも含む) を表示するには、次の手順を実行します。

1. SAクライアントにログインします。
2. ナビゲーションペインで [デバイス] > [すべての管理対象サーバー] を選択します。
3. [表示] ドロップダウンリストから、[ネットワーク] を選択します。
4. 内容ペインのサーバーをダブルクリックして、ハードウェアの詳細をサーバーエクスプローラーに表示します (次の図を参照)。

### サーバーエクスプローラーのハードウェアビュー

The screenshot displays the HPE Server Automation interface. On the left is the 'インベントリ' (Inventory) pane with a tree view where 'ネットワーク' (Network) is selected. The main area is titled 'ネットワーク' (Network) and shows 'イーサネットネットワーク設定' (Ethernet Network Configuration) for host 'teal14.teal.qa.opsware.com'. Below this is the 'イーサネット接続' (Ethernet Connections) section, which includes a table of network interfaces.

インタフェース /	IPアドレス	ネットマスク	MACアドレス	デュプレックス	速度	DHCP設定	インタフ...
Network adapter 1	-	-	00:50:56:81:4F:93	-	-	無効	イーサネ...

## ネットワークポートの表示

ネットワークデバイスに関するハードウェア情報 (ネットワークポートも含む) を表示するには、次の手順を実行します。

1. SAクライアントにログインします。
2. ナビゲーションペインから [デバイス] > [デバイスグループ] > [パブリック] を選択してから、デバイスグループを選択します。
3. 内容ペインのネットワークデバイスをダブルクリックして、ネットワークデバイスエクスプローラーを表示します。
4. ビューペインで [ハードウェア] を選択し、選択したネットワークデバイスに関する情報を表示します。次の図を参照してください。

### ネットワークデバイスエクスプローラーのハードウェアビュー

The screenshot shows the 'Hardware' view of a network device. The left pane shows a tree view with 'ハードウェア' selected. The main pane displays the following information:

**ハードウェア**

▼ 一般

メーカー: HP  
モデル: 2910a1-48G  
プロセッサ: -  
メモリー: -  
ファームウェア: -  
ROMバージョン: -  
OSバージョン: HP ProCurve W.15.14.0012  
物理インタフェース: 48  
シリアル番号: SG1191R1K1  
資産タグ: -

▼ モジュール

スロット	説明	モデル	シリアル	母
Chassis		2910a1-48G J9147A	SG1191R1K1	-

▼ ネットワークポート

ポート	速度	デュプレックス	接続先	VLAN	母
1	1000	フル	-	-	-
2	1000	フル	-	-	-
3	100	フル	-	-	-
4	-	-	-	-	-
5	-	-	-	-	-
6	100	フル	-	-	-
7	100	フル	-	-	-
8	100	フル	-	-	-
9	100	フル	-	-	-
10	100	フル	-	-	-
11	100	フル	-	-	-
12	100	フル	-	-	-
13	-	-	-	-	-
14	-	-	-	-	-
15	-	-	-	-	-
16	-	-	-	-	-

49個のアイテム | peter | 金 9 09 16:35 2016 Asia/Calcutta

## NAのネットワークデバイス情報

環境内のネットワークデバイスが関係するタスクをトラブルシューティングするときは、NAに直接ログインして、ネットワークデバイスの追加詳細情報とイベント履歴を確認できます。NA/SA統合機能に用意されているログインオプションを使用すると、ネットワークデバイスについて、NAに記録された詳細情報とイベント履歴にアクセスできます。

### ネットワークデバイスの表示

1. ナビゲーションペインで、[デバイス] > [デバイスグループ] > [/パブリック] を選択します。
2. 内容ペインでネットワークデバイスを選択します。

### NAでのネットワークデバイスの詳細

The screenshot displays the Network Automation interface for a device named CiscoASA2. The interface includes a navigation sidebar on the left with options like 'Current Device', 'My Settings', and 'My Profile'. The main content area shows device details such as Hostname (CiscoASA2), Device IP (10.78.58.144), and Last Snapshot Attempt (Jun-16-16 03:13:45). A warning message indicates that 'Startup and Running Configurations differ'. Below the details, there is a section for 'Device Details' with fields for Vendor (Cisco), Model (ASA5505), Device Family (Cisco PIX), Software Version (8.2(1)), Driver Name (Cisco firewalls, FW5M series, OS version 3.x & 4.x, PIX, ASA, & LocalDirector series, OS version 4.x, 5.x, 6.x, 7.x, 8.x, 9.x), Device Type (Firewall), Serial Number (JMX1120Z0NL), Asset Tag, System Memory (256.0 MB), Location (Global), and Device Origin (Imported on Jun-16-16 02:51:00). There is also a 'Comments' section with the text 'Live Network Device' and an 'Update Comments' button.

## イベント履歴の表示

[イベントの詳細] ウィンドウで [デバイス] リンクをクリックすると、デバイスの追加時のタイムスタンプ、前回のスナップショット、前回の構成変更などの追加情報が表示されます。

### NAでのネットワークデバイスのイベントの詳細



## デュプレックスの不一致

NA/SA統合機能には、デュプレックスの不一致の自動検出機能が用意されています。デュプレックスの不一致とは、管理対象サーバーと接続されているネットワークデバイス間の速度とデュプレックスに関する構成の不一致です。

サーバーのネットワークインタフェースについては、24時間ごとに発生するハードウェアの登録時に、速度とデュプレックスの情報が収集されます。

Windowsオペレーティングシステムを実行しているサーバーでは、デバイスに依存せずにデュプレックスを決定する方法がないため、Windowsのサーバーエージェントは、初期設定ではデュプレックスの設定を報告しません。カスタムスクリプトをサーバーエージェントに追加すると、特定のネットワークインタフェースの速度とデュプレックスの設定を収集し報告することができます。スクリプトを作成してエージェントと統合する手順については、サポート担当者にお問い合わせください。

サーバーの速度とデュプレックスの情報は、SAクライアントで**[表示]** > **[更新]**を選択したりF5キーを押しても、更新されません。このデータは、NA通信モードデータの収集診断が実行されたときに更新されます。「[NA通信モードデータの収集診断](#)」を参照してください。

ネットワークデバイスについては、NA通信モードデータの収集診断によって速度とデュプレックスが収集されます(この診断は、定義するスケジュールに従って実行されます)。ネットワークデバイスの速度とデュプレックスの情報が最新であることを保証するには、診断を実行する定期的なスケジュールを設定することを推奨します。『SA 10.50ユーザーガイド』を参照してください。

サーバーのネットワークインタフェース情報(速度とデュプレックス)と、接続されたネットワークデバイスのネットワークポート情報(速度とデュプレックス)が一致しない場合、そのデバイスは非コンプライアンス状態であるとみなされます。


NA/SA統合機能では、ダッシュボードを使用して、トップレベルで識別されたデュプレックスの不一致を確認できます。また、サーバーとネットワークデバイスによって識別されたデュプレックスの不一致を、それぞれサーバーエクスプローラーとネットワークデバイスエクスプローラーで確認することもできます。

### ダッシュボードでのデュプレックスの不一致の表示

デュプレックスのコンプライアンスレベルと、それがダッシュボードにどのように表示されるかについては、『SA 10.50管理ガイド』を参照してください。


### デュプレックスの不一致の表示 (サーバー別)

サーバーエクスプローラーを使用してデュプレックスの不一致を表示するには、次の手順を実行します。

1. ナビゲーションペインで [デバイス] > [すべての管理対象サーバー] を選択します。
2. 内容ペインで、サーバーを選択します。
3. サーバーをダブルクリックして、サーバーエクスプローラーを表示します。
4. [ビュー] ペインで、[ハードウェア] を選択します。
5. [ネットワークインタフェース] セクションの [デュプレックス] 列で、検出された不一致を確認します。不一致は、 アイコンで示されます。このアイコンは [デュプレックス] 列のデュプレックス設定 (フル、ハーフ、自動) の前に表示されます。

### デュプレックスの不一致の表示 (ネットワークデバイス別)

ネットワークデバイスエクスプローラーを使用してデュプレックスの不一致を表示するには、次の手順を実行します。

1. ナビゲーションペインで、[デバイス] > [デバイスグループ] > [パブリック] を選択します。
2. 内容ペインでネットワークデバイスを選択します。
3. ネットワークデバイスをダブルクリックして、ネットワークデバイスエクスプローラーを表示します。
4. [ビュー] ペインで、[ハードウェア] を選択します。
5. [ネットワークポート] セクションの [デュプレックス] 列で、検出された不一致を確認します。不一致は、 アイコンで示されます。このアイコンは [デュプレックス] 列のデュプレックス設定 (フル、ハーフ、自動) の前に表示されます。

## ネットワークレポート

物理接続とデュプレックスのコンプライアンスが関係する問題をトラブルシューティングするために、ネットワークレポートを実行して調査することができます。SAクライアントのレポート機能を使用すると、次のネット



ワークレポートを生成して、環境内の管理対象サーバーとネットワークデバイス間のレイヤー1接続を識別できます。

### ネットワークデバイスごとの接続

このレポートには、選択したネットワークデバイスへのすべての物理接続が表示されます。

### サーバーごとの接続

このレポートには、選択した管理対象サーバーへのすべての物理接続が表示されます。

注：これらのレポートを実行、エクスポート、および印刷する方法については、『SA 10.50管理ガイド』を参照してください。

## ネットワーク図

SAのService Automation Visualizer (SAV) 機能およびNAのダイアグラム機能を使用すると、環境内の管理対象サーバー、ネットワークデバイス、レイヤー2およびレイヤー1接続を表す詳細な図を作成できます。また、このようなネットワーク図を.png、.png、および.svgファイルにエクスポートし、図に注釈を付けて、他のアプリケーションで使用することもできます。

## HPE Server Automation Visualizerの起動

SAVIにアクセスするには、次の手順を実行します。

1. ナビゲーションペインで **[デバイス]** > **[すべての管理対象サーバー]** を選択します。
2. 内容ペインで、1つまたは複数のサーバーを選択します。
3. **[ツール]** メニューから **[HPE Server Automation Visualizer]** を選択し、次のいずれかのオプションを選択します。
  - SAVウィンドウを開くには、**[新規]** を選択します。
  - 以前に保存されたトポロジを開くには、**[開く]** を選択します。
4. トポロジ図を作成してエクスポートするには、『SA 10.50ユーザーガイド』でHPE Server Automation Visualizerの使用手順を参照してください。

### NAダイアグラムの起動

NAのダイアグラム機能を起動し使用する手順については、『SA 10.50ユーザーガイド』を参照してください。

## NAとSA Global Shell

SA Global File System (OGFS) を使用して、サーバーと接続ネットワークデバイス間をナビゲートできます。それには、OGFSの`/opsw/Servers/@および/opsw/Network/@`ディレクトリで、その物理接続をたどります。

また、次の3種類のNAスクリプトをOGFSで実行することもできます。

- コマンド
- 詳細
- 診断

これらのスクリプトは、

`/opsw/Scripts/Network`の下にあるOGFSの3つのディレクトリに対応します。『SA 10.50ユーザーガイド』の「ネットワークディレクトリ」を参照してください。

また、BourneシェルおよびPythonのスクリプトを作成し、OGFSでの実行時に次のタスクを実行することもできます。

- サーバーとネットワークデバイスを検出する。
- 特定のスイッチに接続されているすべてのサーバーを検出する。
- デュプレックスの不一致があるサーバーを検出する。
- 特定のサーバーのネットワークインタフェースを表示する。
- すべてのデバイスのIPアドレスを取得する。
- 2つのファイルを比較して、ネットワークデバイス構成の変更点を特定する。
- デバイスの詳細 (snmp-locationなど) を変更する。

### OGFSの起動

Global Shell機能でOGFSにアクセスするには、次の手順を実行します。

1. [ツール]メニューの[Global Shell]を選択して、ターミナルウィンドウを起動します。OGFSの使用の詳細については、『SA 10.50ユーザーガイド』を参照してください。
2. サーバーと接続ネットワークデバイス間をナビゲートするには、使用の「SA Global Shell」および「OGFSディレクトリ」の項に示すガイドラインに従ってください。

### リモートターミナル (rosh)

roshユーティリティを使用すると、デバイス(サーバーおよびネットワークデバイス)にログインして、ネイティブコマンドを実行できます。roshは、Global Shellセッション内から呼び出します。ネイティブコマンドは、roshを実行して対話形式で入力することも、roshのオプションとして指定することもできます。たとえば、roshでスイッチにログインして、show vlanコマンドを実行すると、すべてのVLANの詳細を表示できます。

roshユーティリティの使用の詳細については、『SA 10.50ユーザーガイド』を参照してください。

## 推定される物理接続

NA/SA統合機能には、推定される物理(レイヤー1)接続を検出して報告する機能も含まれています。これらの接続は、データ(スイッチによって認識されたMACアドレスなど)から推定され、キャプチャーされ、SAデータモデルに追加されます。

これらの物理接続(推定されるレイヤー1データ)は、ヒューリスティックに基づいています。OSIモデルで、それぞれのレイヤーは下位のレイヤーを隠すための抽象概念です。したがって、デバイスから収集されたレイヤー2データで、100%正確なレイヤー1データを生成することはできません。特に、次のような状態が1つでも存在すると、レイヤー1データは正しくない場合があります。

- デバイスが、MACアドレスが認識されるポート番号を返さない。
- NAが(MACアドレスが認識される)トポロジデータを収集してから数分以内に、デバイス間のトラフィックがなかった。
- 2つの管理対象デバイスの中に、管理されていないデバイスがある。
- 2つの管理対象デバイスの中にハブがある。

SAクライアントでは、Global Shellでネットワークデバイスディレクトリをナビゲートすることで、推定されるレイヤー1接続を表示できます。

## デバイスグループとNA

デバイスグループは、組織に合わせてデバイス(サーバーおよびネットワークデバイス)を分類するのに役立ちます。たとえば、顧客、ファシリティ、使用方法、アプリケーションなどを基準にデバイスをグループ化し、そのグループ内のすべてのデバイスに対してアクションを実行できます。

SAのデバイスグループには、管理対象サーバーとネットワークデバイス、または管理対象サーバーのみを入れることができます。NAのデバイスグループには、ネットワークデバイスしか入れることができません。ネットワークデバイスグループの作成と編集は、NAのみで実行できます。roshユーティリティの使用の詳細については、『SA 10.50ユーザーガイド』を参照してください。

複数のサーバー上で実行され、環境内の複数のネットワークデバイスに依存するアプリケーションを監視するには、そのアプリケーションが実行されるすべてのサーバーとネットワークデバイスを含むデバイスグループとして、アプリケーションをモデル化することを推奨します。これにより、SAを使用してアプリケーションに関するトラブルシューティングを行うことができます。

### NAデバイスグループの関連付け

SAのパブリックなデバイスグループをNAのデバイスグループに関連付けると、関心があるすべてのサーバーとネットワークデバイスの情報を監視できるようになります。デバイスグループは、同じグループ名を使用することで関連付けます。

関連付けるデバイスグループには、次の要件があります。

- SAデバイスグループはパブリックであること。
- SAデバイスグループは静的であること。
- 関連付けられるNAとSAのデバイスグループの名前が同じであること。

SAとNAのデバイスグループを関連付けるには、次の手順を実行します。

1. ナビゲーションペインで、**[デバイス]** > **[デバイスグループ]** > **[パブリック]** を選択します。
2. 内容ペインで、デバイスグループを選択します。
3. デバイスグループを右クリックし、**[開く]** を選択して、デバイスグループエクスプローラーを表示します。
4. **[表示]** ドロップダウンリストで **[プロパティ]** を選択します。
5. **[同じ名前のNAデバイスグループとの関連付け]** チェックボックスをオンにして、この機能を有効にします。
6. **[ファイル]** メニューから **[保存]** を選択します。

## SA-NA統合のトラブルシューティング

SAがNAと通信しているかどうかをテストするには、次の状態を確認します。

- 自分のSA資格情報でNAにログインできること。これにより、NAがSAと通信できることが確認されます。
- **[外部認証タイプ]** の下のNAの**[管理設定]** で指定されたSA資格情報がSAに設定されていること。これにより、NAがサーバーのMACアドレスを調査できることが確認されます。
- NATポロジデータの収集診断が正常に実行されていること。この状態を確認するには、タスクを探して、その結果をチェックします。これにより、NAがMACアドレスを収集し、SAで調査を試みたことが確認されます。

# OOとの統合

## 概要

本項では、システム統合担当者とフロー管理者がServer Automation (SA) を使用してフローを設定し、SAを使用して実行する方法について説明します。また、ユーザーがフローを実行する方法についても説明します。フローは、最も一般的な自動化タスクの一部を実行する操作です。SA-Operations Orchestration (OO) 統合を使用すると、フローの作成者はSAと統合されるOOフローを構築し、ユーザーはSAからフローを実行できます。フローの詳細については、OOのドキュメントを参照してください。

SAとOOを統合する前に、次の項で説明する手順を実施するために、SA、OO、OOフロー、OOジョブについて十分に理解する必要があります。

この項では、次の内容について説明します。

- 「統合のセットアップ」
- 「ユースケース: SA-OOフロー」
- 「ユースケース: SA-OOジョブ」

フローの詳細については、SSO (<https://softwaresupport.hpe.com/>)にあるOOのドキュメントを参照してください。

## 補足情報

この項では、SA-OOフローおよびジョブに関する補足情報 (表 やリストなど) を示します。

SA-OOフロー

SA-OO統合フロー

この項では、フロー入力を示します。フローの作成者は、入力名、入力タイプ、およびテンプレートをOOで定義できます。これらの入力が定義され、フローが実行されると、その値がOO-SAライブラリのSACoreInputsテーブルに自動的に入力されます (これらの値を手動で入力する必要はありません)。

これらの入力について:

- 入力にテキスト、暗号化フィールド、またはフリーフォームリストフィールドがあり、OOにデフォルト値が用意されている場合は、フィールドにデフォルト値が入力されます。デフォルト値がない場合は、次の表のガイドラインに従っていれば、既知のいずれかの入力 (変更可能) がテキストフィールドに入力されます。
- 入力に単一選択リストフィールドまたは複数選択リストフィールドがある場合、OOによって値が指定されます (この値は変更できません)。

フロー入力の定義の詳細については、OOのドキュメントを参照してください。

### フロー入力

フロー入力	関連	(SAによって)自動的に割り当てられる値
coreHostおよび coreIPAddress	SAコア	SAクライアントにログインしているSAユーザーに関連付けられているSAコアのホストおよびIPアドレス
coreUsernameまたは coreUser	SAコア	SAクライアントにログインしているSAユーザーに関連付けられているユーザー名
corePassword	SAコア	SAクライアントにログインしているSAユーザーに関連付けられているパスワードSAは、パスワードがOOで難読化されている場合のみ、パスワードの値を提供します。  フィールドの内容は暗号化されます。
coreVersion	SAコア	現在のSAコアのバージョン  この値はSAから提示されます
saServerIdentifier	SA管理対象 サーバー	選択されているサーバーのID:  2つの値を (OOで) 設定できます。 <ul style="list-style-type: none"> <li>• 未割り当て (値が1つの場合)</li> <li>• 値のリスト (値が複数の場合) - 入力を freeFormListタイプとしてOOで定義します。</li> </ul>
saServerScriptName	SA管理対象 サーバー	SAコアで使用可能なサーバースクリプトの名前 (その特定のサーバーのオペレーティングシステム用)  自動的に割り当てられる値: なし  代わりに、ユーザーが (OGFSスクリプト以外の) サーバースクリプトを選択できるウィジェットがSAクライアントで提供されます。
saServerName/hostName	SA管理対象 サーバー	選択されているサーバーのDNS名  この値は、選択されているサーバーが1つの場合のみ設定されます。

## フロー入力 (続き)

フロー入力	関連	(SAによって)自動的に割り当てられる値
		2つの値を(OOで)設定できます。 <ul style="list-style-type: none"><li>未割り当て(値が1つの場合)</li><li>値のリスト(値が複数の場合)</li></ul> 入力をfreeFormListタイプとしてOOで定義します。
platformName	SA管理対象 サーバー	選択されているサーバーのオペレーティングシステム名 この値は、選択されているサーバーが1つの場合にのみ設定されます。
customerName	SA管理対象 サーバー	選択されているサーバーのカスタマー名 この値は、選択されているサーバーが1つの場合にのみ設定されます。
facilityName	SA管理対象 サーバー	選択されているサーバーがあるファシリティの名前 この値は、選択されているサーバーが1つの場合にのみ設定されます。
saJobId	OO	OOフローの実行に使用されたSAジョブのジョブID(レポート機能を使用してOOで追跡) この入力 は表示されません。

# SA-OOジョブ

## ブロックされたジョブを扱うためのJavaメソッド

SA APIのJobService Javaインターフェースは、ブロックされたジョブを扱うためのJavaメソッドを提供します。これらのメソッドは、ジョブ承認の統合を可能にするSAへのコールバックです。

これらのメソッドを起動するユーザーは、次のアクセス権が必要です。[任意のジョブの編集またはキャンセル] および [すべてのジョブを表示]

## ブロック可能なSAジョブのタイプ

次の表に、ブロック可能なSAジョブのタイプを示します。

### ブロック可能なSAジョブのタイプ

ジョブタイプ	機能
仮想化サービスへのホストの追加	仮想化サービスにホストを追加します。
仮想化サービスの追加	仮想化サービスを追加します (その追加先は?)。
仮想マシンの複製	VMwareサーバー上に仮想マシンを複製します。
仮想マシンのVMテンプレートへの変換	仮想マシンをVMテンプレートに変換します。
スナップショットの作成	スナップショットを作成して、特定の時点での管理対象サーバーの構成をキャプチャーします。
仮想マシンの作成	仮想マシンを作成します。
仮想ゾーンの実行	Solaris仮想マシン (非グローバルゾーン) をグローバルゾーン (Hypervisor) 上にプロビジョニングします。
仮想マシンの削除	仮想マシンを削除します。
VMテンプレートの削除	VMテンプレートを削除します。
VMテンプレートからの仮想マシンのデプロイ	VMテンプレートから仮想マシンをデプロイします。
仮想化サービスの編集	仮想化サービスを編集します。
パッチのインストール	管理対象サーバーにパッチをインストールします。
SAエージェントのインストール	SAエージェントをインストールします。
ソフトウェアのインストール	管理対象サーバーにソフトウェアをインストールします。
仮想マシンの移行	仮想マシンを移行します。
仮想マシンの変更	仮想マシンを変更します。
仮想ゾーンの変更	Solaris仮想マシンのプロパティを変更します。
仮想マシンの電源制御	仮想マシンの電源制御を行います。



ブロック可能なSAジョブのタイプ (続き)

ジョブタイプ	機能
構成のプッシュ	管理対象サーバー上の構成ファイルを変更します。
サーバーの再起動	サーバーを再起動します。
仮想化データの再ロード	仮想化データを再ロードします。
監査結果の修復	監査操作で検出された内容に基づいてサーバーを修復します。
ポリシーの修復	ソフトウェアポリシーまたはパッチポリシーに基づいてサーバーを修復します。
スナップショット結果の修復	スナップショットに基づいてサーバーを修復します。スナップショットには、特定の時点での管理対象サーバーの構成がキャプチャーされます。
仮想ゾーンの削除	グローバルゾーン (Hypervisor) からSolaris仮想マシン (非グローバルゾーン) を削除します。
仮想化サービスの削除	仮想化サービスを削除します。
構成の復元	以前のバージョンの構成ファイルをサーバー上に復元します。 構成をサーバーにプッシュするたびに、以前の構成が保存され、後で復元できます。
ソフトウェアのロールバック	ソフトウェアをロールバックします。
エージェントアップグレードの実行	SAエージェントのアップグレードプロセスを起動します。
監査の実行	監査を実行します。
Chef Recipeの実行	サーバー上でChef Recipeを実行します。
カスタム拡張の実行	カスタム拡張を実行します。
ISMコントロールの実行	ISM (インテリジェントソフトウェアモジュール) コントロールを実行します。 ISMは、ISM開発キット (IDK) で作成されたインストール可能なソフトウェアパッケージです。ISMには、日々処理するアプリケーション固有のタスク (ソフトウェアサーバーの起動など) を実行するコントロールスクリプトを含めることができます。
OGFSスクリプトの実行	サーバー上でOGFS (Global File System) スクリプトを実行します。 OGFSスクリプトは、SAクライアントからGlobal Shellで実行できるスクリプトです。
OSビルド計画の実行	OSビルド計画を実行します。

ブロック可能なSAジョブのタイプ (続き)

ジョブタイプ	機能
OSシーケンスの実行	OSシーケンスを使用して、サーバーをプロビジョニングし、オペレーティングシステムをインストールします。  OSシーケンスでは、未プロビジョニングサーバーにインストールする内容 (OSインストールプロファイルのOSビルド情報、ソフトウェアポリシーとパッチポリシー、修復設定など)を設定します。
プログラム拡張の実行	SAに追加されたカスタム機能を実行します。  SAの機能は、特定の顧客ニーズに対応するカスタム拡張を作成して拡張できます。
サーバースクリプトの実行	サーバー上でスクリプトを実行します。
パッチのアンインストール	サーバー上のパッチをアンインストールします。
ソフトウェアのアンインストール	サーバー上のソフトウェアをアンインストールします。

次の表で、ブロックされたジョブの処理に使用可能なSA JobService Javaメソッドについて説明します。

SA JobService Javaメソッド

Javaメソッド	メソッドの説明	SA CLIメソッドの例
JobService. approveBlockedJob	ジョブを承認してブロックを解除し、実行できるようにします。	Global Shellセッション内で: cd /opsw/api/com/opsware/job/JobService/method./approveBlockedJob self:i=\$job_id
JobService. updateBlockedJob	SAクライアントの[ジョブステータス]ウィンドウでブロックされたジョブのTicket IDフィールド (userTagパラメーターに対応) およびReasonフィールド (blockReasonパラメーターに対応)の値を変更します。	cd /opsw/api/com/opsware/job/JobService/method./updateBlockedJob self:i=\$job_id userTag=\$ticket_id \blockReason="This type of job requires approval of CMB."

SA JobService Javaメソッド (続き)

Javaメソッド	メソッドの説明	SA CLIメソッドの例
	<p><b>注:</b> SAインターフェースを使用して、これらのフィールドを変更することはできません。</p>	
JobService. cancelScheduled Job	<p>ブロックされたジョブをキャンセルして、実行できないようにします。</p> <p>ブロックされたジョブのステータスを [承認待ち] から [キャンセル] に変更します。</p>	<p>(ID/パラメーターはjobRefであり、selfではないことに注意)</p> <pre>cd /opsw/api/com/opsware/job/JobService/method./cancelScheduledJob jobRef:i=\$job_id \reason="Job was scheduled to run outside of change window."</pre> <p>現在実行中のジョブ (job_status = "ACTIVE") はキャンセルできません。</p>
JobService. findJobRefs	<p>既存のすべてのジョブを検索し、ブロックされているすべてのジョブまたはその他の状態にあるジョブ (進行中のジョブ、期限切れのジョブ、スケジュール設定されたジョブなど) のIDを返します。</p> <p>他のユーザーが起動したジョブを表示できます。</p>	<p>フィルターにはJobInfoVO.status整数ではなく、job_status文字列を指定してください。</p> <pre>cd /opsw/api/com/opsware/job/JobService/method./findJobRefs:i filter=job:{job_status = "BLOCKED" }</pre>

フローをSAに戻し、フローとジョブがやり取りを行う必要がある場合は、job\_id属性が必要です。ジョブのブロックでは、この属性をSAからOOに送信する必要があります。

## ジョブステータスの値

この項では、`job_status`検索可能属性で使用可能なジョブステータスの値について説明します。また、それに対応する`JobInfoVO.status`の整数値についても説明します (この値は、クライアントコードが値オブジェクト (VO) をすでに取得している場合に確認できます)。

「[ジョブステータスの値](#)」(36ページ)に、ジョブステータスの有効な値を示します。

Javaクライアントでは、`JobInfoVO.status`を`STATUS_ACTIVE`などのフィールド定数と比較できます (この表に示されている整数を使用するものではありません)。

### ジョブステータスの値

job_status検索可能属性の値	JobInfoVO.statusの値	SAクライアントに表示されるジョブステータス	ジョブステータスの説明
ABORTED	0	コマンドエンジンクリプトのエラー	ジョブの実行が終了しました。 コマンドエンジンのエラーが検出されています。
ACTIVE	1	進行中	ジョブは現在実行中です。
BLOCKED	11	承認待ち	ジョブは起動されていますが、実行する前に承認が必要です。
CANCELLED	2	該当しない	スケジュールが削除されました。
DELETED	3	キャンセル	ジョブのスケジュールが設定されましたが、後でキャンセルされました。
EXPIRED	13	期限切れ	現在の日付がジョブスケジュールの終了日を過ぎているため、ジョブスケジュールは無効になりました。
FAILURE	4	エラーを起こして完了	ジョブの実行が終了し、エラーが検出されています。
PENDING	5	スケジュール済み	ジョブは、将来に一度実行するようにスケジュールされています。
RECURRING	12	定期的	ジョブは、将来に繰り返し実行するようにスケジュールされています。
STALE	10	古い	承認が得られなかったため、ブロックされたジョブを実行する機会が期限切れになりました。

### ジョブステータスの値 (続き)

job_status検索可能属性の値	JobInfoVO.statusの値	SAクライアントに表示されるジョブステータス	ジョブステータスの説明
STATUS	15	終了中	ジョブは、ユーザーからの終了要求に応じて、シャットダウン中です。
STATUS	16	終了済み	ジョブは、ユーザー要求に応じて早期に終了しました。
SUCCESS	6	完了	ジョブの実行が正常に終了しました。
TAMPERED	9	改竄	ジョブは改竄されています。
UNKNOWN	7	不明	不明なエラーが発生しました。
WARNING	8	警告ありで完了	ジョブの実行が終了し、警告が検出されています。
ZOMBIE	14	孤立	ジョブは孤立しました。

### 入力が定義されていないか、サーバーが1つのデバイスのみを受け入れる

フローを実行しようとしたときに、次のエラーを受け取ることがあります。

SAは選択したデバイスをこのフローに渡しません。フローに必要なサーバーID入力が定義されていないか、入力が1つのデバイスだけを受け入れます。

このエラーを受け取った場合は、管理者にServerIdentifier入力をチェックするよう依頼してください。

## 統合のセットアップ

この項では、SAと統合するOOフローおよびジョブの構築方法について説明します。

- [OOフローのセットアップ](#)
- [OOジョブのセットアップ](#)

## OOフローのセットアップ

SA-OO統合の管理者は、ユーザーのアクセス権の設定、システム環境が要件を満たすかどうかのチェック、必要なOO SDKクライアント証明書のインポートを行う必要があります。

ユーザーのアクセス権の設定

OOフローのユーザーには、次のOOアクセス権が必要です。

#### OOフローのユーザーに必要なアクセス権

アクセス権	SAクライアントでのアクセス権設定の確認方法
AdministerFlowIntegrations (OO統合設定の構成権限)	ナビゲーションパネルで[管理]を選択します。ナビゲーションツリーの選択枝のリストに[フロー統合]オプションが表示された場合は、アクセス権が付与されています。
RunFlowOption (OOフローの実行権限)	ナビゲーションパネルで[デバイス]を選択します。[サーバー]>[すべての管理対象サーバー]を選択します。サーバー名を右クリックし、[実行]を選択します。[フロー...]オプションが表示された場合は、アクセス権が付与されています。

#### 環境のチェック

システム要件は次のとおりです。

- SAバージョン10.0
- HPE Operations Orchestration (OO) バージョン10.x
- SAコアサーバーにネットワーク接続されたOOインストールサーバー
- OOと通信を行うための有効なOO SDKクライアント証明書 (「OO SDKクライアント証明書のインポート」を参照)

#### OO SDKクライアント証明書のインポート

OOフローをSAから実行する前に、証明書をインポートしておく必要があります。

**注:** 使用するアーキテクチャーに1つのマスターコアと1つ以上のセカンダリコアが含まれる場合は、この項の手順をマスターコアと各セカンダリコアに対して実行してください。同様に、使用するSAコンピューターに、1つ以上のスライスがあるスライスコアインストールがある場合は、スライスごとに手順を繰り返してください。

証明書をインポートするには、次の手順を実行します。

1. Webサービスデータアクセスエンジン (Twist) を停止します。  
`/etc/init.d/opsware-sas stop twist`
2. OO Central証明書をSAに転送します。

(次の手順でパスワードの入力を求められた場合は、「changeit」を使用してください)

- a. OO Central証明書をエクスポートします。

OOサーバー上のOSバージョンに応じて、証明書のエクスポート手順が異なる場合があります。詳細については、OOのドキュメントを参照してください。

**注:** 証明書のエクスポートのコマンドはOOサーバーで実行する必要があります (クライアント証明書はSAにバンドルされていません)。

WindowsサーバーにインストールされているOO 10.xインスタンスから証明書をエクスポートするコマンドの例:

```
<OOインストールディレクトリ>\java\bin\keytool.exe -exportcert -alias tomcat -file  
C:\oocentral.crt -keystore <OOインストールディレクトリ  
>\central\var\security\key.store
```

次に、C:\oocentral.crtファイルをSAコアの/tmp/oocentral.crtにコピーします。

- b. OO Central証明書をSA Java Runtime Environment (JRE) キーストアにインポートします。

```
/opt/opsware/jdk1.8/jre/bin/keytool -importcert -alias oocert -file  
/tmp/oocentral.crt -keystore /opt/opsware/jdk1.8/jre/lib/security/cacerts
```

**注:** 上記の例では、エイリアス: oocertを使用しています。ただし、キーストアでまだ使用されていないければ、任意のエイリアスを証明書のインポートで使用できます。

3. OO Central証明書が正しくインポートされたことを確認します。

```
/opt/opsware/jdk1.8/jre/bin/keytool -list -alias oocert -keystore  
/opt/opsware/jdk1.8/jre/lib/security/cacerts
```

**出力例:**

```
oocert, Feb 3, 2010, trustedCertEntry,  
Certificate fingerprint (MD5): DF:DD:22:1B:A2:1E:A9:9C:1C:AF:8F:E0:14:1F:B5:E0
```

4. Webサービスデータアクセスエンジン (Twist) を再開します。

```
/etc/init.d/opsware-sas restart twist
```

**注:** jssecacertsファイルがcacerts (/opt/opsware/jdk1.8/jre/lib/security/)と同じ場所にある場合、jssecacertsファイルを削除するか、cacertsの代わりにjssecacertsに証明書を確実にインポートしてください。

## OOジョブのセットアップ

SA-OOジョブの管理者は、ユーザーがSAでジョブを操作できるように、次のアクセス権を作成する必要があります。

### ユーザーのアクセス権

アクセス権	説明	SAクライアントでのチェック
AdministerFlowIntegrations	OO統合設定の構成	ナビゲーションパネルで[管理]を選択します。ナビゲーションツリーの選択肢のリストに[フロー統合]オプションが表示された場合は、アクセス権が付与されています。
RunFlowOption (フローを実行するユーザー用)	OOフローの実行	ナビゲーションパネルで[デバイス]を選択します。[サーバー]>[すべての管理対象サーバー]を選択します。サーバー名を右クリックし、[実行]を選択します。[フロー...]オプションが表示された場合は、アクセス権が付与されています。

## ユースケース: SA-OOフロー

この項では、SA-OOフローに関連するユースケースについて説明します。この項は、管理者のユースケースとエンドユーザーのユースケースの2つに分かれています。

## 管理者: OOフローの構成

管理者は、ユーザーがSAでフローを実行できるようにするために、OOフローを構成し、変更内容と設定を確認する必要があります。



## フローを構成するには、次の手順を実行します。

1. SAクライアントのナビゲーションパネルで、[管理] > [フロー統合] を選択します。
2. [フロー統合] パネルで [設定の編集] をクリックすると、[フロー統合設定の編集] ウィンドウが開きます。

フロー統合

HPE Server Automation (SA)はHPE Operations Orchestration (OO) フローと統合できます。統合には2つの使用可能なポイントがあります。この画面には、有効になっている統合ポイントと、使用されている設定が表示されます。

- [ジョブのブロック]セクションは、ブロックされたジョブの承認に使用するOOユーザー資格情報と フローを構成します。
- [実行中のフロー]セクションは、SAクライアントからOOフローを実行するためのOOユーザー資格情報を 構成します。

設定の編集

OO URL:

**ジョブのブロック**

OOユーザー名(N):

パスワード(P):

承認フロー(E):

接続ステータス(C): -

**フローの実行**

OOユーザー名(N):

パスワード(P):

接続ステータス(C): -

[フロー統合] パネルには、次のユーザーのリアルタイム情報が表示されます。

- a. [ジョブのブロック] に対して: 承認フローを実行する権限を持つOOユーザー。
- b. [フローの実行] に対して: SAからフローを実行する際に使用される資格情報を持つOOユーザー。

このパネルが開いているときに、ユーザーアカウントの変更 (アカウントの無効化、OO資格情報 (ユーザー名、パスワード、URLなど) の変更) があれば、その変更内容が即座に表示されます。

3. フローの実行に対して、次の情報を入力または変更します。

- OO URL - OOサーバーの場所 (次の書式を使用)  
<プロトコル>://<ホスト名またはIPアドレス>:<ポート番号>/

例:

https://10.255.166.110:8443/

https://10.255.166.110:8443/PAS/

- OOユーザー名とパスワード

ジョブのブロックおよびこのウィンドウの [ジョブのブロック] セクションについては、「SA-OO - ジョブのブロック」の項を参照してください。

ハイフンは未構成のステータス、赤のチェックマークは無効のステータス、緑のチェックマークは有効のステータスを示します。有効と無効の両方のステータスについては、最新の検証のタイムスタンプも表示されます。

4. [接続の検証] をクリックして、入力した資格情報が有効であることを確認します。

接続ステータスが有効の場合は、チェックマークが表示されます。

5. [適用] をクリックして、フロー統合設定の変更内容を保存します。

**注:** [フロー統合設定の編集] パネルにデータが存在しない場合、フィールドのデータが正しくない場合、または接続ステータスの横にチェックマークが表示されていない場合は、[適用] ボタンは使用できません。

## フローの変更と設定を確認するには、次の手順を実行します。

1. SAクライアントにログオンします。
2. ナビゲーションパネルで、[管理] を選択します。
3. ナビゲーションツリーで、[フロー統合] を選択します。



[フロー統合] パネルには、次のユーザーのリアルタイム情報が表示されます。

- [ジョブのブロック] に対して: 承認フローを実行する権限を持つOOユーザー。
- [フローの実行] に対して: SAからフローを実行する際に使用される資格情報を持つOOユーザー。

このパネルが開いているときに、ユーザーアカウントの変更 (アカウントの無効化、OO資格情報 (ユーザー名、パスワード、URLなど) の変更) があれば、その変更内容が即座に表示されます。

フローアクションまたはジョブのブロックアクションが終了すると、チェックマークがステータスの横に表示されません。

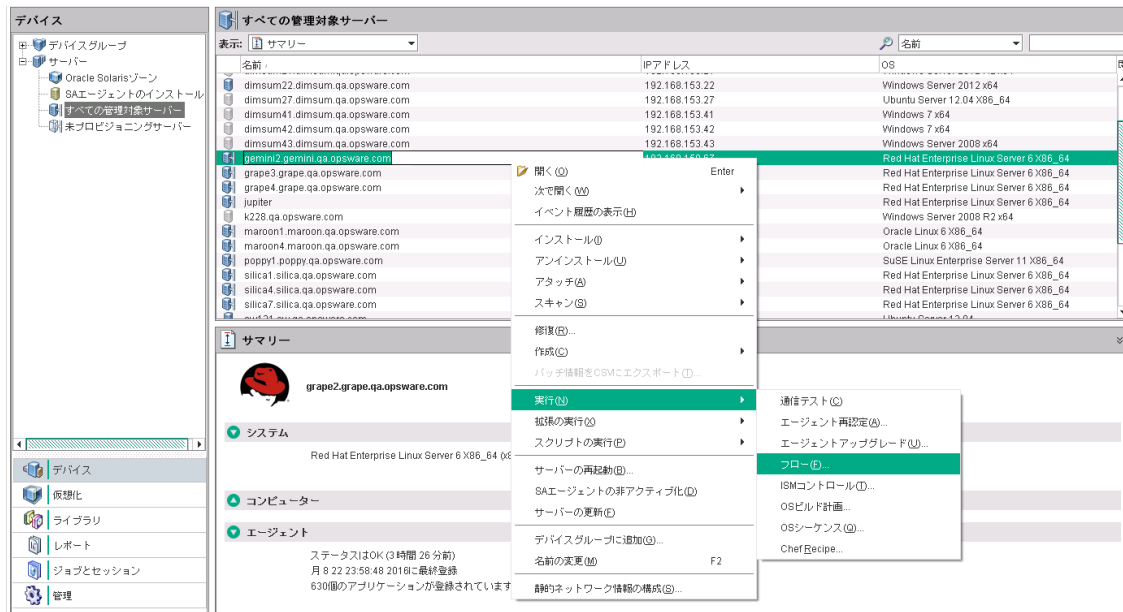
## ユーザー: OOフローの実行

フローは、最も一般的な自動化タスクの一部を実行する操作です。SA-OO統合によって、ユーザーはSAからフローを実行できるようになります。

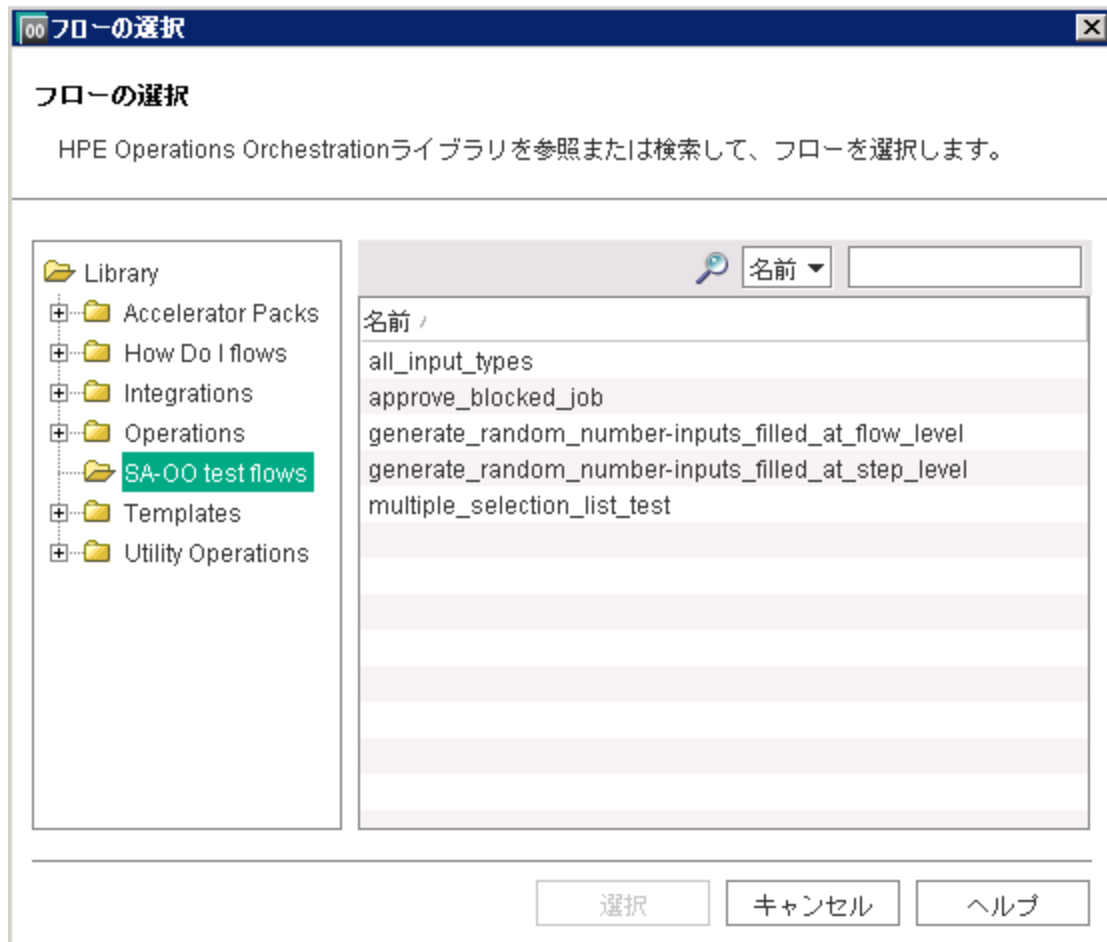
ユーザーは、サーバーとフローの選択、フロー入力、実行時オプション、スケジュール設定オプション、通知パラメーターの入力または選択、サーバーの追加または削除を行うことができます。

## フローを実行するには、次の手順を実行します。

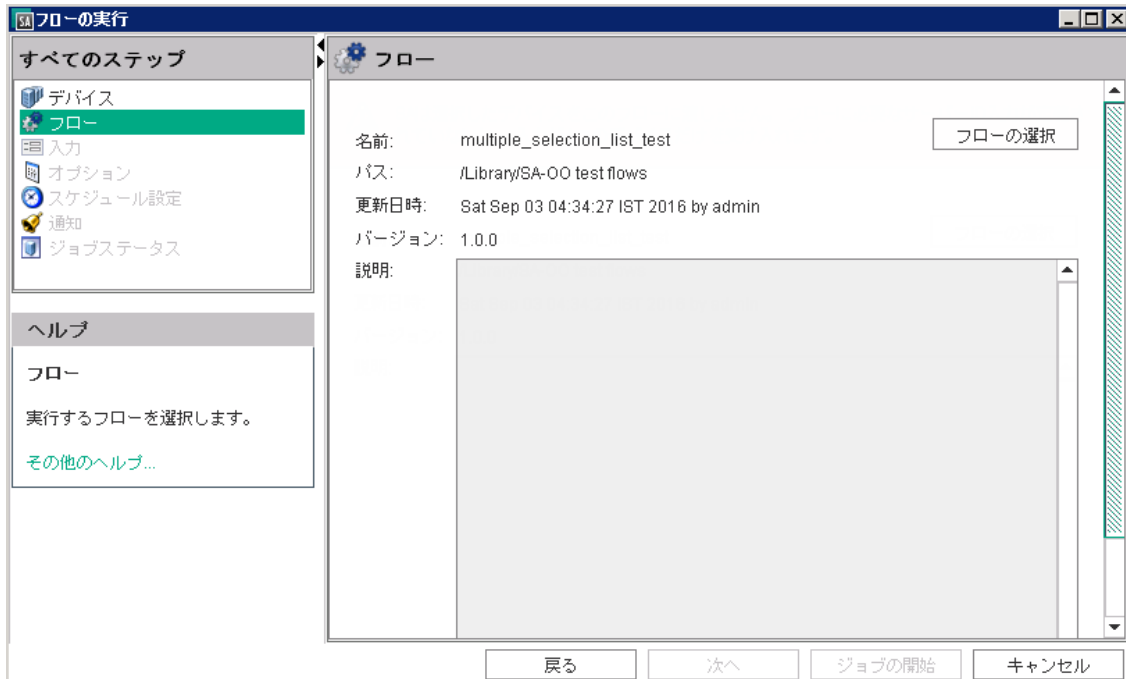
1. SAクライアントのナビゲーションパネルで、[デバイス] を選択します。
2. 上部パネルで、[サーバー] > [すべての管理対象サーバー] を選択します。  
フローは、サーバーを選択してからでなければ選択できません。
3. サーバー名を右クリックします。



4. [実行]>[フロー...]を選択して、OOの[フローの選択]ウィンドウを表示します。



5. [フローの選択]ウィンドウのライブラリツリーからフローのカテゴリを選択して、そのコンポーネントフローを表示します。
6. 名前リストでフローを選択し、[選択]をクリックして、[フローの実行]ウィンドウにフローの詳細を表示します。



[フローの実行] ウィンドウの [すべてのステップ] パネルで、順番に各カテゴリ ([入力]、[オプション]、[スケジュール設定]、[通知]) を選択し、これ以降の手順説明に従って、それぞれのパラメーターの値を入力します。また、各パネルで [次へ] を選択して、カテゴリを表示することもできます。

7. フロー入力の値を入力するには、[すべてのステップ] パネルで [入力] を選択し、パネルに表示された入力の値を入力します (一部の値は自動的に入力されています)。

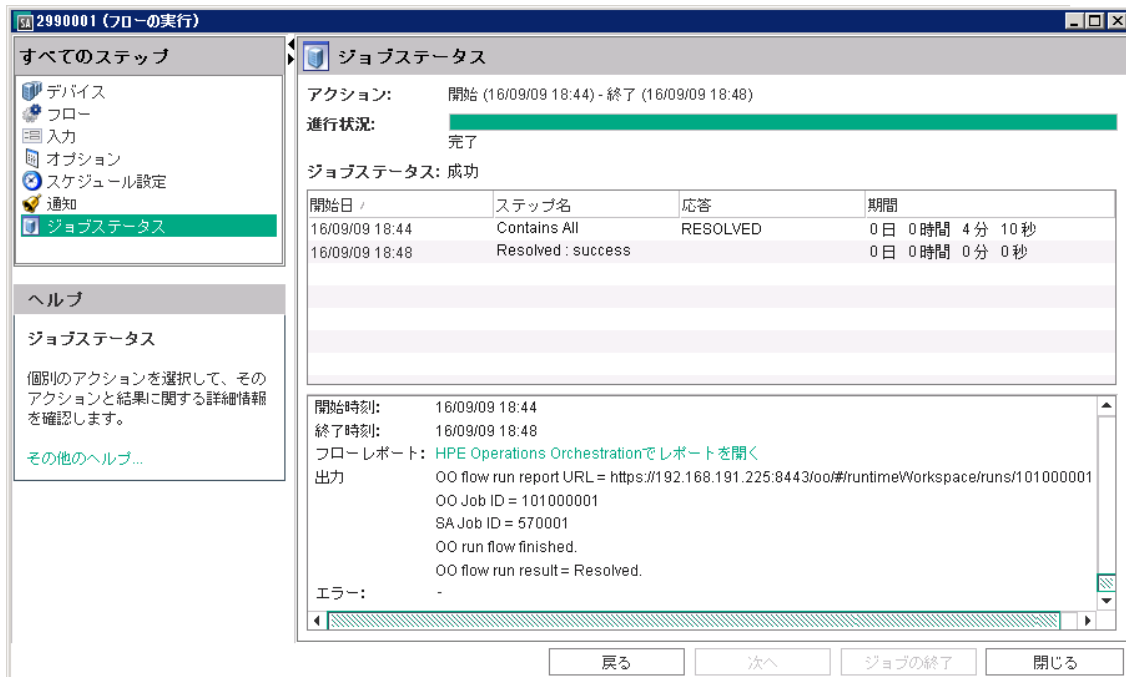
例:

- a. saServerScriptName。または [スクリプトの選択] をクリックして、スクリプトのリストを表示します。
- b. saServerName
- c. saServerIdentifier

入力の詳細については、[補足情報のフロー入力](#)を参照してください。

8. 実行時オプションの値を入力するには、[すべてのステップ] パネルで [オプション] を選択し、ジョブのタイムアウトの値を入力します。サーバーがこの時間 (分) だけジョブを実行すると、ジョブはタイムアウトします。デフォルト値は180分です。タイムアウト値は1分から1440分の間です。
9. スケジュール設定オプションを選択するには、[すべてのステップ] パネルで [スケジュール設定] を選択して、次の値を入力します。
  - a. スケジュール頻度
  - b. 時刻と期間

10. 通知情報を入力するには、[すべてのステップ] パネルで [通知] を選択して、次の値を追加します。
  - a. 受信者の電子メールアドレス
  - b. 通知 ([通知の追加] をクリック)
  - c. チケットID番号 (ID番号の規則はありません。任意の番号を選択できます。)
11. [ジョブの開始] をクリックして、ジョブを開始します。または、[キャンセル] をクリックして、このセッションで選択した内容を消去します。
12. [ジョブステータス] をクリックして、SAジョブのステータスを表示します。(オプション)



[ジョブステータス] ウィンドウに表示されるのは、フローの実行ステータスではなく、OOでフローを開始し監視するSAジョブのステータスです。

SAジョブが完了すると、このウィンドウには、フローの各ステップのステータスが ([応答] フィールドに) 表示され、OO上の詳細なフロー関連情報を指すURLが表示されます。

ステップが1つ以上失敗しても、SAジョブの監視は成功している可能性があります。OO APIには、OOフロー全体の成功または失敗を正確に判断する呼び出しが用意されていません。そのため、OOフローの成功または失敗をSAジョブのステータス画面から確認することはできません。また、URLで提供される情報からも確認できません。

## サーバーを追加または削除するには、次の手順を実行します。

1. フローを実行します。
2. [フローの実行] ウィンドウの[すべてのステップ] ナビゲーションパネルで、[デバイス] を選択します。
3. サーバーアイコンを右クリックし、[追加] または [削除] を選択するか、プラス記号またはマイナス記号をクリックします。

[サーバーおよびデバイスグループの選択] ウィンドウが表示されます。

4. [選択] をクリックして、サーバーをサーバーのリストに追加します。

[フローの実行] ウィンドウの[デバイス] パネルに新しいサーバーが表示されるか削除されたサーバーがないことが示されます。

## SA-OO統合のトラブルシューティング

### SA-OO接続エラー

SAからOOに接続できない場合、管理者が実行できる処理は次のとおりです。

- [フロー統合設定の編集] ウィンドウのフィールドの設定が正しいことを確認する。詳細については、[「ユースケース: SA-OOフロー」\(40ページ\)](#)を参照してください。
- 次のログファイルを調査して、コマンドエンジンサーバーに関するエラーメッセージがないかどうかを確認する。

```
/var/log/opsware/waybot/waybot.err
```

エラーメッセージはSAクライアントに表示されません。

- OO URL、ユーザー名、パスワードが正しいことを確認する。
- 指定されたOOユーザーに、フローを実行する正しい権限があることを確認する。



フローステータスを確認するには、[フロー統合] パネルを参照してください。このパネルの詳細については、[「ユースケース: SA-OOフロー」\(40ページ\)](#)を参照してください。

ユーザーに対してこのエラーが表示されたときは、管理者に問い合わせてください。

## フローの実行エラー

この項では、フローをユーザーとして実行しているときに発生する可能性があるエラーについて説明します。

### 正しくない入力

フローを実行しようとしたときに、次のいずれかのエラーを受け取ることがあります。

- SAは選択したデバイスをこのフローに渡しません。
- SA-OO統合の構成エラー: フロー統合設定が正しくありません。フロー統合のURL、ユーザー名、およびパスワードが正しいことを確認してください。

このようなエラーが表示されるのは、一般に次のような状況が発生したときです。

- 実行するフローをユーザーが間違って選択した。
- OOサーバーが応答していない。管理者に相談してください。
- 管理者が[フロー統合設定の編集] ウィンドウに入力した値が正しくない。[フロー統合設定の編集] ウィンドウの情報を確認するよう管理者に依頼してください。詳細については、[「ユースケース: SA-OOフロー」\(40ページ\)](#)を参照してください。
- フローの作成者が、命名規則を使用するようにフロー定義を変更する必要がある。

## ユースケース: SA-OOジョブ

SAジョブは、パッチのインストール、コンプライアンスのチェックなどを行う主要プロセスで、SAクライアントで実行されます。

## 管理者: OOジョブの構成

管理者は、構成に従ってジョブをブロックします。

この項では、システム統合担当者とソフトウェア開発者がSAでSAジョブをブロックする方法と、SA APIを呼び出すフローを使用してSAでジョブを承認またはキャンセルする方法について説明します。

SAジョブの詳細については、『SA 10.50開発者ガイド』を参照してください。

ジョブのブロックおよびブロック解除を実行するには、SA、Operations Orchestration (OO)、SAジョブ、およびOOフローに関する知識が必要です。

この項では、次の内容について説明します。

- 「[ジョブのブロック](#)」
- 「[ブロックされたジョブの承認と削除](#)」

ジョブの詳細については、『SA 10.50開発者ガイド』を参照してください。OOでの作業の詳細については、SSO (<https://softwaresupport.hpe.com/>)にあるOOのドキュメントを参照してください。

## ジョブのブロック

実行する前に確認と承認が必要な可能性があるジョブは、実行できないようにブロックすることができます。この項では、ブロックするジョブを定義し、ジョブをブロックするためのいくつかのシナリオ、ブロックすることが可能なジョブのタイプ、ジョブのブロックに必要なアクセス権、ジョブをブロックする方法、ジョブのブロックを無効にする方法、ブロックされたジョブの関連情報を表示する方法について説明します。

## ブロックされるジョブとは

ブロックされるジョブには、次のようなジョブがあります。

- ブロック可能なジョブタイプに属しているジョブ。
- システム管理者によってブロック処理が有効にされたジョブタイプに属しているジョブ。
- ブロックが配置されているジョブ。
- 実行する前に確認が必要なジョブ。
- 実行する前に承認が必要なジョブ。

## ジョブをブロックする理由

この項では、ジョブのブロック処理の候補となるジョブについて、その3つのサンプルシナリオを示し、ジョブのブロックが必要となる状況について説明します。

### シナリオ1

ジョブの実行にシステムの再起動が必要な場合は、ジョブが早朝の時間帯に実行できるようになるまで、ジョブの承認を遅らせる必要があります。通常の業務時間内にジョブを実行すると、通常の作業プロセスが乱されることとなります。

### シナリオ2

さらに詳しく確認してからでなければ、実行できないジョブもあります。たとえば、サーバー上の特定のソフトウェアアプリケーションを更新するジョブがある場合、変更諮問委員会 (CAB) は、提案されたアップグレードをレビューして、そのアップグレードが環境内で実行されている他のアプリケーションと衝突しないことを確認しなければならないかもしれません。この委員会は、ジョブを実行すべきかどうか、またいつ実行すべきかを決定することとなります。

### シナリオ3

多くのIT環境では、特定の操作を実行またはキャンセルする前に、その操作にチケットを割り当て、評価し、承認することが必要です。このようなジョブは、チケット発行システムでチケットを作成し、評価し、解決できるように、ブロックする必要があります。

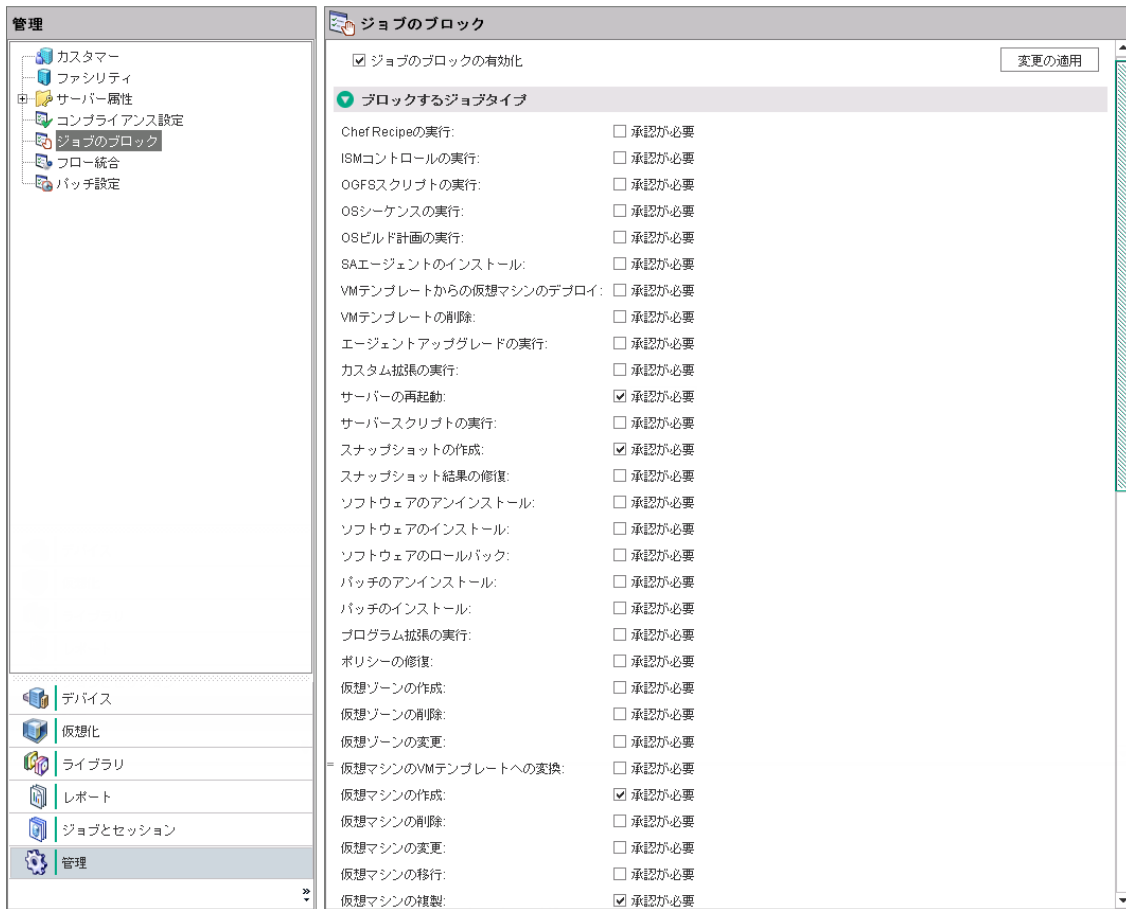
## ジョブのブロックとブロック解除の実行方法

この項では、ブロックするジョブタイプを指定する方法と、ジョブのブロックを無効にする方法について説明します。

### ブロックするジョブタイプの指定方法

1. SAクライアントの[ナビゲーション] ペインで、[管理] を選択します。
2. ナビゲーションツリーで [ジョブのブロック] を選択します。右側のペインにジョブタイプのリストが表示され、各タイプの横にチェックボックスが表示されます。

### SAジョブのタイプのブロック



指定可能なジョブのタイプについては、**ブロック可能なSAジョブのタイプ**を参照してください。

3. [ジョブのブロックの有効化] チェックボックスを選択します。

この操作により、パネル内に表示されるあらゆるジョブタイプをブロックできるようになります。

4. [ジョブのブロックの有効化] チェックボックスの下のパネルで、ブロックする各ジョブタイプの横にあるチェックボックスを選択します。ブロックされたジョブタイプに対応するジョブは、所定の承認が得られるまで実行できなくなります。

この操作により、ブロックする個々のジョブタイプが指定されます。


5. [変更の適用] をクリックすると、選択したジョブタイプに属しているジョブがブロックされます。

**注:** あるタイプのジョブをブロックすると、そのタイプに属しているすべての将来のジョブが、そのジョブの [承認が必要] ボックスの選択を解除するまでブロックされます。

## ジョブのブロックを無効にする方法

1. SAクライアントの[ナビゲーション] ペインで、[管理] を選択します。
2. ナビゲーションペインで [ジョブのブロック] を選択します。
3. ブロックの必要がなくなったジョブについて、それに対応するチェックボックスを選択解除します。

この操作を実行すると、それぞれのジョブタイプについてジョブのブロックが無効になります。

4. ジョブタイプのリストの上にある [ジョブのブロックの有効化] チェックボックスを選択解除します。上の  を参照してください。

この操作を実行すると、すべてのジョブタイプについてジョブのブロックが無効になります。

5. [変更の適用] をクリックします。

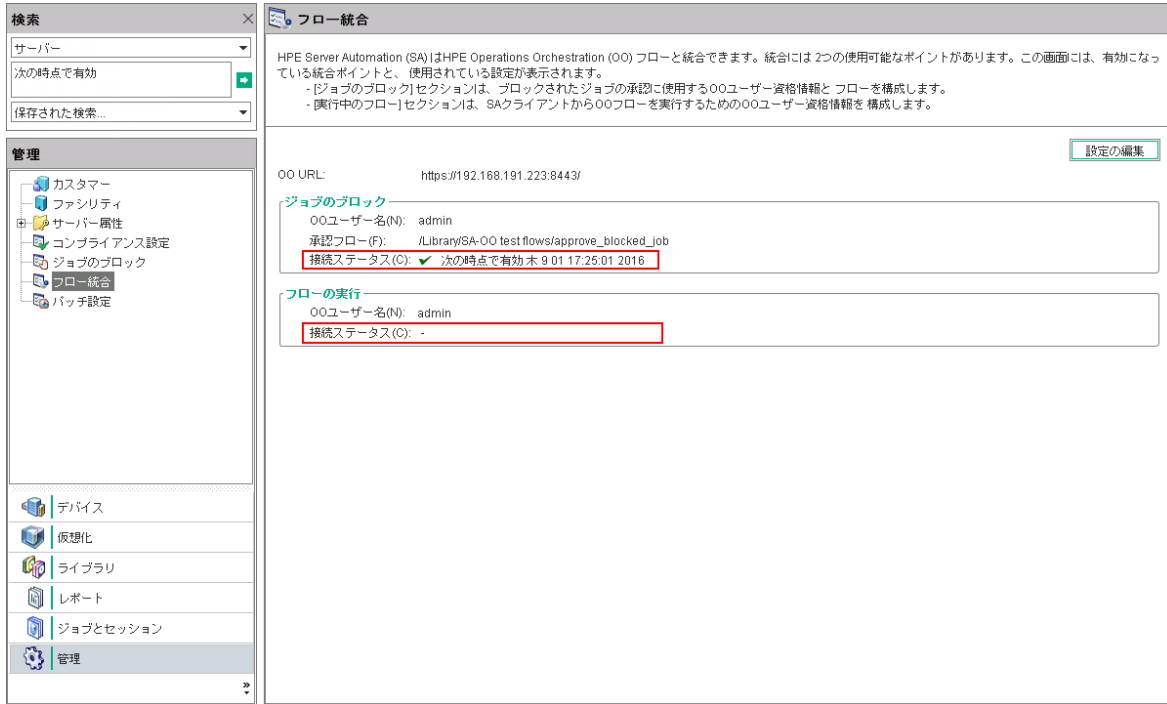
**注:** [ジョブのブロックの有効化] チェックボックスを選択解除しても、ブロック処理を指定したジョブタイプの横のチェックは、ユーザーの便宜を考えてチェックされたままに保持されます。

## ブロックされたジョブの情報の表示方法

OO接続情報は [フロー統合] パネルで確認できます。また、ジョブのステータス情報はジョブログでチェックできます。

SAの [フロー統合] パネルでのOO接続情報の確認

[管理] > [フロー統合] を選択して、[フロー統合] パネルにアクセスします。



[フロー統合] パネルには、次のユーザーのリアルタイム情報が表示されます。

- [ジョブのブロック] に対して: 承認フローを実行する権限を持つOOユーザー
- [フローの実行] に対して: SAからフローを実行する際に使用される資格情報を持つOOユーザー

このパネルが開いているときに、ユーザーアカウントの変更 (アカウントの無効化、OO資格情報 (ユーザー名、パスワード、URLなど) の変更) があれば、その変更内容が即座に表示されます。

OOへの接続がアクティブな場合は、ステータスの横にチェックマークが表示されます。

## ブロックされたジョブのステータスをジョブログで チェック

ブロックされたことがわかっているジョブについて、そのジョブのブロックが解除されたかどうかを確認するには、ジョブログをチェックします ([ジョブとセッション] > [ジョブログ] > [任意のステータス] を選択します)。

ジョブステータスの有効な値のリストと、その値の意味については、[ジョブステータスの値](#)を参照してください。

## フロー設定の構成または編集

フロー設定を編集または構成するには、OOとSAIにログインしている必要があります。

SAクライアントのナビゲーションパネルで、次の手順を実行します。

1. [管理] > [フロー統合] を選択します。
2. [フロー統合] パネルで [設定の編集] をクリックすると、[フロー統合設定の編集] ウィンドウが開きます。

The screenshot shows a dialog box titled "フロー統合設定の編集" (Edit Flow Integration Settings). It contains the following elements:

- Header:** タブ "フロー統合" (Flow Integration).
- Text:** HPE Server Automation (SA)はHPE Operations Orchestration (OO) フローと統合できます。統合には2つの使用可能なポイントがあります。この画面には、有効になっている統合ポイントと、使用されている設定が表示されます。
  - [ジョブのブロック]セクションは、ブロックされたジョブの承認に使用するOOユーザー資格情報と フローを構成します。
  - [実行中のフロー]セクションは、SAクライアントからOOフローを実行するためのOOユーザー資格情報を 構成します。
- Buttons:** "設定の編集" (Edit Settings) button in the top right.
- Input Fields:** "OO URL:" field with the value "https://192.168.191.223:8443/".
- Job Blocking Section (ジョブのブロック):**
  - OOユーザー名(N): admin
  - パスワード(P): [masked]
  - 承認フロー(E): /Library/SA-OO test flows/approve\_blocked\_job (with "フローの選択" button)
  - 接続ステータス(C): - (with "接続の検証" button)
- Flow Execution Section (フローの実行):**
  - OOユーザー名(N): admin
  - パスワード(P): [masked]
  - 接続ステータス(C): - (with "接続の検証" button)
- Footer:** "適用" (Apply), "キャンセル" (Cancel), and "ヘルプ" (Help) buttons.

[フロー統合] パネルには、次のユーザーのリアルタイム情報が表示されます。

- [ジョブのブロック] に対して: 承認フローを実行する権限を持つOOユーザー。

**注:** この値を空白にしても、統合に影響はありません。

- [フローの実行] に対して: SAからフローを実行する際に使用される資格情報を持つOOユーザー。

このパネルが開いているときに、ユーザーアカウントの変更 (アカウントの無効化、OO資格情報 (ユーザー名、パスワード、URLなど) の変更) があれば、その変更内容が即座に表示されます。

**注:** [フローの実行] と [ジョブのブロック] は互いに無関係に設定することができます。ただし、これら ([フローの実行] と [ジョブのブロック]) の少なくともどちらかに、OO URLをはじめとするすべての入力を指定する必要があります。[接続の検証] が検証された後で、[適用] ボタンが有効になります。

3. フローの実行に対して、次の情報を入力または変更します。

- OO URL - OOサーバーの場所 (次の書式を使用)

<プロトコル>://<ホスト名またはIPアドレス>:<ポート番号>/

例:

https://10.255.166.110:8443/

https://10.255.166.110:8443/PAS/

- 承認フロー - 承認フローの場所
- OOとの通信が承認されているユーザーのOOユーザー名 およびパスワード

ハイフンは未構成のステータス、赤のチェックマークは無効のステータス、緑のチェックマークは有効のステータスを示します。有効と無効の両方のステータスについては、最新の検証のタイムスタンプも表示されます。

4. [接続の検証] をクリックして、入力した資格情報が有効であることを確認します。

接続ステータスが有効の場合は、チェックマークが表示されます。

5. [適用] をクリックして、フロー統合設定の変更内容を保存します。

**注:** [フロー統合設定の編集] パネルにデータが存在しない場合、フィールドのデータが正しくない場合、または接続ステータスの横にチェックマークが表示されていない場合は、[適用] ボタンは使用できません。



## ブロックされたジョブの承認と削除

SAアプリケーションプログラミングインタフェース (SA API) を使用して、ジョブを承認または削除できます。このAPIは、ブロックされたジョブを管理する唯一の手段です。ブロックされたジョブの承認をSAクライアントで行うことはできません。SA APIの使用の詳細については、『SA 10.50開発者ガイド』を参照してください。

OOでのジョブのブロックについては、SSO (<https://softwaresupport.hpe.com/>)にあるOOのドキュメントを参照してください。

# uCMDB Connectorとの統合

## 概要

この項では、SA-uCMDB Connectorを使用したUniversal Configuration Management Database (uCMDB) - Server Automation (SA) 統合について説明します。SAは、使用するサーバーとソフトウェアに関する大量の情報をSAデータベースに格納します。SA-uCMDB Connectorは、このデータの一部をHPE uCMDBにコピーします。SAのデータに変更があると、そのたびにSA-uCMDB Connectorは更新されたデータをuCMDBサーバーに自動的に送信します。

この項で説明する手順を実行するには、SAおよびuCMDBに関する知識が必要です。

サポートと互換性の最新情報については、関連する製品リリースの『SA 10.5 Support and Compatibility Matrix』を参照してください。

この項では、次の内容について説明します。

- 「SA-uCMDB統合のセットアップ」
- 「ユースケース」
- 「SA-uCMDB統合のトラブルシューティング」

## SA-uCMDB統合のセットアップ

管理者としてこの統合をセットアップするには、次の手順を実行します。

- SA-uCMDB Connectorのダウンロード
- SA-uCMDB Connectorの有効化と起動

SA-uCMDB Connectorをセットアップし、SA-uCMDB Connectorに送信されるSAデータをカスタマイズし、SAカスタム属性をuCMDBに転送し、データ変換関数をカスタマイズします。

## SA-uCMDB Connectorのダウンロード

SAクライアントは、SA-uCMDB Connectorを使用して、SA管理対象サーバーに対してuCMDBブラウザ-インパクト ウィジェットを起動する機能を提供します。

SA-uCMDB Connectorは、SAをインストールするときにインストールされます。インストールを別途行う必要はありません。

Server Automation 10.5にアップグレードする場合は、uCMDBサーバーがリリース10.01以降にアップグレード済みであることが必要です。

累積更新パッケージをダウンロードするには、次の手順を実行します。

このSAバージョンには、uCMDB 10.01以降が必要です。uCMDB 10.01には、コンテンツパック12が含まれています。

最新のCUP HPEソフトウェアパッチは、次の場所のSSOポータルにあります。

Linuxの場合: [https://softwaresupport.hpe.com/group/softwaresupport/search-result/-/facetsearch/document/LID/UCMDB\\_00150](https://softwaresupport.hpe.com/group/softwaresupport/search-result/-/facetsearch/document/LID/UCMDB_00150)

Windowsの場合: [https://softwaresupport.hpe.com/group/softwaresupport/search-result/-/facetsearch/document/LID/UCMDB\\_00150](https://softwaresupport.hpe.com/group/softwaresupport/search-result/-/facetsearch/document/LID/UCMDB_00150)

このサイトを使用するには、HPE Passportへの登録とサインインが必要です。

バージョンサポート情報については、HPEソフトウェアサポートサイトの『SA 10.5 Support and Compatibility Matrix』を参照してください。

**enable**コマンドを実行して、SA-uCMDB Connectorを新しいuCMDBサーバーで構成します。

**enable**コマンドの構文は、使用環境によって異なります。**enable**コマンドの構文とオプションについては、このドキュメントの「[enableコマンド](#)」(60ページ)を参照してください。

次のコマンドを入力して、SA-uCMDB Connectorを起動します。

```
/etc/init.d/opsware-sas start telldaemon
```

(オプション) 次のコマンドでSA-uCMDB Connectorのステータスをチェックします。

```
/etc/init.d/opsware-sas status telldaemon
```

## SA-uCMDB Connectorの有効化と起動

SA-uCMDB Connectorを起動するには、その前にSA-uCMDB Connectorを有効化して、uCMDBサーバーの名前またはIPアドレス、ポート番号、ログイン、およびパスワードを指定する必要があります。

**enable**コマンドは、SAコアサーバーの/opt/opsware/tell/binディレクトリにあります。

SA-uCMDB Connectorを有効化して起動するには、**enable**コマンドを実行してSA-uCMDB Connectorの構成を変更します。**enable**コマンドには、構成に応じて複数のオプションがあります。

次に、このコマンドの単純な例を示します。

```
enable --host myserver01.hpe.com --port 8888 --user ucmdb-admin  
--password leM93A3dme
```

パラメーター、構文、およびオプションの詳細については、「[enableコマンド](#)」(60ページ)を参照してください。

**start**コマンドを実行して、SA-uCMDB Connectorを再起動します。

```
/etc/init.d/opsware-sas start telldaemon
```

(オプション) 次のコマンドでSA-uCMDB Connectorのステータスをチェックします。

```
/etc/init.d/opsware-sas status telldaemon
```

詳細については、「[SA-uCMDB Connectorのステータスの表示](#)」(74ページ)を参照してください。

## enableコマンド

SA-uCMDB Connectorは、起動する前に**enable**コマンドで有効にしておく必要があります。有効にするときは、uCMDBサーバーの名前またはIPアドレス、ポート番号、ログイン、およびパスワードを指定する必要があります。

**enable**コマンドを使用して、SA-uCMDB Connectorを構成し有効にします。この項では、**enable**コマンドについて説明します。SA-uCMDB Connectorは、有効にしてからでなければ起動できません。

**enable**コマンドは、次の処理を行います。

SA-uCMDB Connectorのカスタム構成ファイル/etc/opt/opsware/tell/tell\_custom.confがまだ存在していなければ、作成する(デフォルトでは、手動で作成されていない限り、デプロイメント時にカスタム構成ファイルは存在しません)。

カスタム構成ファイル/etc/opt/opsware/tell/tell\_custom.confを変更し、uCMDBサーバーのホスト名またはIPアドレス、ポート番号、およびログインを入力する。

ユーザーのパスワードを保存する。

ファイル/opt/opsware/oi\_util/startup/components.configを変更し、telldaemon (SA-uCMDB Connectorのプロセス)の行のコメントを解除する。

SA-uCMDB Connectorの実行中にuCMDB構成パラメーターを変更する場合は、SA-uCMDB Connectorを停止し再起動しなければ、変更が有効になりません。

### enableコマンドの場所

enableコマンドは、SAコアサーバーの/opt/opsware/tell/binディレクトリにあります。

### enableコマンドの新しい構文

SA 9.14で、新しいuCMDBブラウザーをサポートするためのパラメーターが、SA-uCMDB Connectorのenableコマンドに追加されました。その新しいパラメーターについて、この項と「[enableコマンドの新しいパラメーター](#)」(61ページ)で説明します。

```
enable [--protocol <uCMDBプロトコル>] [--host <uCMDBホストIP>] [--port <uCMDBホストポート番号>] [--browser_protocol <uCMDBブラウザープロトコル>] [--browser_host <uCMDBブラウザーホストIP>] [--browser_port <uCMDBブラウザーホストポート>] [--user <uCMDB管理ユーザー>] [--password <uCMDB管理パスワード>] [--help]
```

### enableコマンドの新しいパラメーター

パラメーター	説明	新規
--protocol <uCMDBプロトコル>	uCMDBサーバーのプロトコル、httpまたはhttps。デフォルトはhttpです。	新規
--host <uCMDBホストIP>	このオプションは、HPE uCMDBサーバーのIPアドレスまたはホスト名を指定します。デフォルト値はlocalhostです。	—
--port <uCMDBホストポート番号>	このオプションは、HPE uCMDBサーバーのポート番号を指定します。デフォルト値は8080です。	—
--browser_protocol <uCMDBブラウザープロトコル>	uCMDBブラウザーサーバーのプロトコル、httpまたはhttps。デフォルトはhttpです。	新規
--browser_host <uCMDBブラウザーホストIP>	このオプションは、HPE uCMDBブラウザーホストの名前またはIPアドレスを指定します。デフォルト値	新規

**enableコマンドの新しいパラメーター (続き)**

パラメーター	説明	新規
	はlocalhostです。	
--browser_port <uCMDBブラウザーストポート>	このオプションは、uCMDBブラウザーストのポートを指定します。デフォルト値は8080です。	新規
--user <uCMDB管理ユーザー>	このオプションは、HPE uCMDBサーバーの管理ユーザーのユーザー名を指定します。デフォルト値はadminです。	—
--password <uCMDB管理パスワード>	このオプションは、--userオプションで指定したユーザーのパスワードを指定します。デフォルト値はadminです。	—

SSLを有効にしない場合のenableコマンドの例:

```
enable --protocol http --host 192.168.8.93 --port 9999 --browser_protocol http --browser_host 192.168.8.100 --browser_port 8888 --user john-ucmdb --password mypass1234
```

uCMDBサーバーとuCMDBブラウザーストに対してSSLを有効にする場合のenableコマンドの例:

```
enable --protocol https --host 192.168.8.93 --port 9999 --browser_protocol https --browser_host 192.168.8.100 --browser_port 8888 --user john-ucmdb --password mypass1234
```

## uCMDBサーバーに送られるSAデータのカスタマイズ

### マッピングファイル

SA-uCMDB ConnectorのXMLマッピングファイルには、SA-uCMDB Connectorによって転送されるデータが記述され、データマッピングをカスタマイズすることができます。

このmapping.xmlは、コネクタが初めて実行されたときに生成されます。新しく生成されたマッピングファイルは、次の場所にあります。

/etc/opt/opsware/tell/metadata/mapping.xml

マッピングファイルを使って、次の内容を制御できます。

- uCMDBに入力するデータの型と属性
- オプションのSAカスタム属性と、uCMDBデータモデル構成アイテム(CI)属性との対応付け

マッピングファイルの初期の内容の詳細については、「[例 – SA-uCMDB Connectorのマッピングファイル](#)」(84ページ)を参照してください。

## マッピングファイルのカスタマイズ

データのマッピング方法をカスタマイズするには、mapping\_custom.xmlファイルを作成し変更してから、Connectorを再起動する必要があります。

**mapping\_custom.xml**ファイルは、デフォルトでは使用されません。そのため、カスタマイズしたマッピングファイルを使用するには、Connectorを再起動する必要があります。

uCMDB Connectorのマッピングをカスタマイズするには、次の手順を実行します。

1. uCMDB Connectorが実行中の場合は、マッピングファイルを編集する前に、Connectorを停止し無効にする必要があります。

手順については、「[SA-uCMDB Connectorの停止と無効化](#)」(73ページ)を参照してください。

**重要:** コネクタが停止され、無効になっていることを確認してください。コネクタが停止されず、無効化されていないときにマッピングファイルを編集すると、Connectorを再起動しようとしたときに問題が発生することがあります。

2. カスタムのマッピングファイルを作成します。
  - a. 次の場所に移動します: /etc/opt/opsware/tell/metadata
  - b. mapping.xmlファイルをそのフォルダーにコピーし、名前をmapping\_custom.xmlにします。

mapping\_custom.xmlファイルは、mapping.xmlファイルと同じ指定フォルダー内になければ、正しく機能しません。

3. /etc/opt/opsware/tell/metadata/mapping\_custom.xmlを必要に応じて編集します。

さまざまな目的でマッピングファイルを変更する方法の詳細については、「[マッピングファイルの編集](#)」(64ページ)を参照してください。

4. **enable**コマンドを実行して、SA-uCMDB Connectorの構成を変更します。

**enable**コマンドの構文は、使用環境によって異なります。**enable**コマンドの構文とオプションについては、このドキュメントの「[enableコマンド](#)」(60ページ)を参照してください。

5. **start**コマンドを実行して、SA-uCMDB Connectorを再起動します。

```
/etc/init.d/opsware-sas start telldaemon
```

6. (オプション) 次のコマンドでSA-uCMDB Connectorのステータスをチェックします。

```
/etc/init.d/opsware-sas status telldaemon
```

## マッピングファイルの編集

カスタマイズするマッピングは、管理者が簡単に確認し編集できるように、すべて**mapping\_custom.xml**構成ファイルで定義します。SA-uCMDBコネクタによって転送されるデータは、このXMLマッピングファイルを修正して変更できます。マッピングファイルには、特定のCIと属性を除外する機能もあります。**mapping\_custom.xml**が存在しない場合、コネクタは標準の**mapping.xml**をデフォルトで使用します。

**アクセス権:** **mapping\_custom.xml**ファイルを表示または編集するには、読み取り/書き込み権限を得るために、まずSAコアにrootとしてログインする必要があります。

**注:** この項では、カスタマイズするマッピングファイル内での編集オプションについて説明します。マッピングファイルをカスタマイズするプロセス(変更内容を有効にするためにコネクタの停止/起動を行うタイミングなど)の手順については、「[マッピングファイルのカスタマイズ](#)」(63ページ)を参照してください。

### マッピングファイルの説明

ここに示しているのは、標準のマッピングファイルの一部です。

```
<Model-Definition model-name='hosts'>
  <CI ucmdb-ci-type-name='node' enable='true' base-class='node'
    <Attribute source='Node/Name' target-attr='name' enable='true' />
    <Attribute source='Node/Description' target-attr='description'
  enable='true' />
  </CI>
</Model-Definition>
```

強調表示したテキストは、編集可能なフィールドを示しています。

**注:** 完全な標準マッピングファイルについては、「[例 – SA-uCMDB Connectorのマッピングファイル](#)」(84ページ)を参照してください。



マッピングファイルのモデル定義タグは、それぞれが特定のモデル名を定義します。この例のModel-Definitionは、'hosts' モデルを定義しています。

それぞれモデルには、複数の構成アイテム (CI) を含めることができます。CIタグは、それぞれがCIの合成を定義します。この例で定義されるCIは 'node' です。

各属性では、**source**によって、ソースデータベースでのデフォルトの属性名が示されます。

- **target-attr**フィールドは、ソースをマップする先のuCMDB属性名を指定します。
- **enable**フィールドは、属性をマップするかどうかを定義します。**enable**のデフォルト値は 'true' です。これは属性がuCMDB内にロードされることを意味します。**enable**を 'false' に設定すると、属性はマップされません。つまり、その属性はuCMDBにロードされません。

### XML属性の値

本項では、XML属性の値と、その値が編集可能かどうかを示します。

**注意:** 編集不可の属性の値は変更しないでください。source='Node/Name' などの編集不可の値は、変更せずに維持することが極めて重要です。これらの値を変更すると、同期が適切に行われなくなり、エラーの発生する可能性があります。

### XML属性

XML属性タグ	属性	属性値の例と注	編集可能?
Model-Definition	model-name	'hosts'、'sa'、'software'、'compliance'、'hypervisor'、'vmrelations'、'compliance_status'	編集不可
	enable	この属性を有効にするには 'true'、無効にするには 'false'	編集可能
CI	ucmdb-ci-type-name	uCMDBのCIタイプを指定します。例: 'node'、'ip_address'	編集可能
	enable	この属性を有効にするには 'true'、無効にするには 'false'	編集可能
属性	source	SAのカスタム属性の名前を指定します。例: 'Node/Name'、'Node/Description'、 'Node/BiosAssetTag'、'Node/BiosSerialNumber'、 'Node/Facility'、'Node/VirtualizationTypeId'  <b>注意:</b> source値は編集しないでください。source値を編集すると、マッピングが破損し、エラーの発生する可能性があります。	編集不可
	target-attr	sourceをマップする先のuCMDBの属性名を指定します。例: 'name'、'description'	編集可能

XML属性タグ	属性	属性値の例と注	編集可能?
		注: target-attr値は、一意の名前である必要があります。	
	enable	この属性を有効にするには 'true'、無効にするには 'false'。	編集可能
	conversion-name	変換関数のみで使用します。詳細については、「 <a href="#">データ変換関数のカスタマイズ</a> 」(69ページ)を参照してください。 例: 'com.hpe.tell.ConversionMethod\$com.hpe.tell.MyConvertVirtualizationType'	編集可能
Attribute-Custom	sa-custom-attribute-key-value	SAのカスタム属性の名前を指定します。例: 'HW_RACK'、'DEVICE_RACK' 注:「 <a href="#">SAカスタム属性の使用方法</a> 」(67ページ)を参照してください。	編集可能
	target-attr	sourceをマップする先のuCMDBの属性名を指定します。 例: 'serial_number'、'facility' 注: target-attr値は、一意の名前である必要があります。	編集可能
	enable	この属性を有効にするには 'true'、無効にするには 'false'。	編集可能
CI-Filter	enable	この属性を有効にするには 'true'、無効にするには 'false'。 注: CDATAブロックの変更については、「 <a href="#">クエリでのフィルターのサポート</a> 」(68ページ)を参照してください。	編集可能
Relation	ucmdb-relation-type-name	uCMDBでのCI間の関係を指定します。 例: 'containment'、'aggregation'	編集可能
	ucmdb-relation-from-ci-type-name	uCMDBでの 'from' CIのCI間の関係を指定します。 たとえば、nodeからip_addressへの含有関係を指定するのであれば、'node' がこの関係の 'from' CIになります。	編集可能
	ucmdb-relation-to-ci-type-name	uCMDBでの 'to' CIのCI間の関係を指定します。 たとえば、nodeからip_addressへの含有関係を指定するのであれば、'ip-address' がこの関係の 'to' CIになります。	編集可能
	enable	この属性を有効にするには 'true'、無効にするには 'false'。	編集可能
	ucmdb-	関係にIDリンクが含まれる場合は 'true'。'true' 値を指定	編集可能

XML属性タグ	属性	属性値の例と注	編集可能？
	relation-id-link	する場合は、'from' CIが存在する必要があります。関係にIDリンクが含まれない場合は、'false' にします。	

### モデル定義

「[モデル定義](#)」(67ページ)に、モデル定義を示します。マッピングファイル内に定義され、データオブジェクトをuCMDB内でどのように表現するかを決定するモデルは7種類あります。たとえば、SAモデルであれば、uCMDB内でSAを表現します。

### モデル定義

モデル定義のmodel-name	説明
'sa'	installed_software.xmlを生成します
'hosts'	node.xmlを生成します
'software'	installed_software.xmlを生成します
'compliance'	policy.xmlを生成します
'hypervisor'	hypervisor.xmlを生成します
'vmrelations'	hypervisor.Relationxmlを生成します
'compliance_status'	policyResult.xmlを生成します

**注：**これらのXMLファイルは、マッピングファイルに基づいて内部的に生成されます。直接編集しないでください。生成されたXMLファイルを直接編集することはサポートされていません。生成されたファイルに変更を加えても、上書きされます。

## SAカスタム属性の使用法

**注：**マッピングファイルの編集は、必ずmapping\_custom.xmlファイルで行う必要があります。標準のmapping.xmlファイルは編集しないでください。mapping.xmlファイルを直接編集すると、同期が適切に行われなくなり、エラーの発生する可能性があります。

### SAカスタム属性のuCMDBへの転送

カスタム属性もuCMDBにロードできます。

**mapping\_custom.xml**ファイルのマッピングを使用すると、uCMDBと同期されるSAの属性に加えて、SAデバイスで定義されたSAカスタム属性や、SAファンリテリから継承されたSAカスタム属性も指定できます。

カスタム属性は、次のようにして**mapping\_custom.xml**ファイルで指定できます。

次の例は、マッピングファイルを構成して、カスタム属性のDEVICE\_RACKを抽出し、uCMDB内のmy\_location\_rackにロードする方法を示しています。**enable**属性は 'true' に設定されていますが、これは、この属性をuCMDBにロードするよう選択したことを示します。

```
<CI ucmdb-ci-type-name='node' enable='true' base-class='node'>
  <Attribute-Custom sa-custom-attribute-key-value='DEVICE_RACK' targetattr='
    my_location_rack' enable='true' />
</CI>
```

強調表示したテキストは、編集可能なフィールドを示しています。

#### クエリでのフィルターのサポート

**mapping\_custom.xml**ファイルには、特定の条件でフィルター処理する機能もあります。

**特定の条件でフィルター処理するには、次の手順を実行します。**

- CI-FilterタグのCDATAセクションにフィルタリング句を記述します。
- **enable**属性の値 (有効にする場合は 'true'、無効にする場合は 'false') を記述して、フィルターを有効にするかどうか指定します。

**注:** CI-FilterはSAデータベースに基づいて指定するため、SAスキーマについて理解していることが必要です。CI-Filterは、CIタイプごとに1つのみ指定できます。フィルターが複数必要な場合は、AND句とOR句を使用した単純なフィルター式を指定できます。

単一フィルターの例 (mapping.xmlファイル内の標準マッピング):

```
<CI ucmdb-ci-type-name='node' enable='true' base-class='node'>
  <Attribute source='Node/Name' target-attr='name' enable='true' />
  <CI-Filter enable='true'>(DEVICES.OPSW_LIFECYCLE =
'MANAGED')</CI-Filter>
</CI>
```

上記の例のフィルターは、State: 'managed' のSAデバイスを選択しています。デフォルトでは、SA-uCMDB ConnectorはManagedのデバイスオブジェクトのみを同期します。

AND句を含むフィルターの例 (mapping\_custom.xml内の修正済みマッピング):

```
<CI-Filter enable='true'>(DEVICES.DVC_MODEL = 'POWEREDGE 2950') and (DEVICES.DVC_ID
> 300000000)</CI-Filter>
```

上記の例のフィルターは、Modelが 'POWEREDGE 2950' で、かつIDが '300000000' より大きいSAデバイスを選択しています。

## 拡張された標準マッピング

マッピングファイルが提供される目的は、次の処理を実行できるようにすることです。

- uCMDBに入力する属性の名前を変更
- データをuCMDBに入力する方法を変更
- 入力するuCMDBのCIタイプを指定

## 追加の標準マッピング

**Facility**および**VirtualizationType**属性は、標準のマッピングファイルではデフォルトで無効になっています。ただし、次のようにすると、有効にすることができます。

### ServerVO.getFacility()

```
<Attribute source='Node/Facility' target-attr='facility' enable='true'/>
```

### ServerVO.getVirtualizationType()

```
<Attribute source='Node/VirtualizationTypeId' target-attr='virtualization_type_id' enable='true'/>
```

## データ変換関数のカスタマイズ

uCMDBに入力するデータを同期中にカスタマイズする必要がある場合は、カスタム変換メソッドを作成して、SA-uCMDB Connectorに提示することができます。SA-uCMDB Connectorは、その関数を適用して、SA構文のデータを、希望するuCMDB構文に変換できます。カスタム変換メソッドを作成すると、たとえば、小文字を大文字に変換したり、バイトをメガバイトに変換したりすることができます。

カスタマイズした変換関数は、tell\_conversions.jarというjarファイルを使ってSA-uCMDB Connectorに提示します(このファイルは、コネクタを起動する前に、/etc/opt/opsware/tell/libに配置しておきます)。コネクタを再起動したら、カスタム変換javaクラスによって**ConversionMethod**クラスが拡張され、**com.hp.e.tell.ConversionMethod**パッケージがインポートされます。

データ変換をカスタマイズするには、次の手順を実行します。

1. SA-uCMDB Connectorが実行中の場合は、マッピングファイルを編集する前に、Connectorを停止し無効にする必要があります。
  - **stop**コマンドを実行して、SA-uCMDB Connectorを停止します。  
/etc/init.d/opsware-sas stop telldaemon

- disableコマンドを実行して、SA-uCMDB Connectorを無効にします。

```
disable
```

**注:** コネクタが停止され、無効になっていることを確認してください。コネクタが停止されず、無効化されていないときにマッピングファイルを編集すると、Connectorを再起動しようとしたときに問題が発生することがあります。

2. カスタマイズした変換関数のコードをjavaで作成します。

例については、「[変換ファイルのサンプル- MyConvertVirtualizationType.Java](#)」(71ページ)を参照してください。この例の変換ファイルの名前はMyConvertVirtualizationType.javaです。

3. 今作成した変換ファイルを利用するように、mapping\_custom.xmlファイルを変更します。

たとえば、javaファイル**MyConvertVirtualizationType.java**を指すように、mapping\_custom.xmlファイルに次の行を配置します。

マッピングファイル内の元のテキスト

```
<Attribute source='Node/VirtualizationTypeId' target-attr='virtualization_type_id' enable='false' />
```

マッピングファイル内のカスタマイズ済みテキスト

```
<Attribute source='Node/VirtualizationTypeId' target-attr='device_isVirtual' enable='true' conversion-name='com.hpe.tell.ConversionMethod$com.hpe.tell.MyConvertVirtualizationType' />
```

XMLのこの修正行には、次の値があります。

- **'device\_isVirtual'**は、target-attrの新しい値です。この変換はデータ型を変更するため、別のuCMDB属性にマップする必要があります。ただし、データ型を変更しない場合は、同じtarget-attr値にマップします。\*
- **conversion-name**は、変換属性のXML名です。これは、そのままのラベルであり、置き換えることはできません。
- **'com.hpe.tell.ConversionMethod\$com.hpe.tell.MyConvertVirtualizationType'**は、conversion-nameの属性値で、MyConvertVirtualizationType.javaが、java変換コードのファイル名です。

変換操作を正しく行うには、target-attr値が極めて重要:

データ型の変更

変換によって属性のデータ型が変更される場合は、**target-attr**で指定される変換後の属性の要件(長さ、フォーマットなど)が同じまたは互換であることを確認してください。前の例で**target-attr**の値を変更し

たのは、変換によって実際のデータ型が変更されるためです。たとえば、測定単位 (UOM) のみを変換したのであれば、実際のデータ型は変化しないため、同じ**target-attr**値を指定できます。

target-attrごとに一意のファイル名

**target-attr**の変換では、それぞれに一意のjava変換コードファイル名が必要です。java変換ファイルは、1つのtarget-attr(出力)を表現します。たとえば、1つのソース属性に対して複数の**target-attr**変換シナリオを設定できますが、それぞれの**target-attr**は、次の例に示すように、マッピングファイル内の別々の属性タグで指定する必要があります。

```
<Attribute source='Node/VirtualizationTypeId' target-attr='virtualization_type_id1'  
enable='true' conversion-  
name='com.hpe.tell.ConversionMethod$com.hpe.tell.MyConvertVirtualizationType1' />  
<Attribute source='Node/VirtualizationTypeId' target-attr='virtualization_type_id2'  
enable='true' conversion-  
name='com.hpe.tell.ConversionMethod$com.hpe.tell.MyConvertVirtualizationType2' />
```

4. カスタマイズした変換ファイル(この例ではMyConvertVirtualizationType.java)をコンパイルします。これで、実行可能なバイナリが生成されます。
5. すべての変換バイナリをjarファイルに圧縮します。ファイル名は、tell\_conversions.jarにします。

**注:** SA-uCMDB Connectorに認識させるには、このjarファイル名を使用する必要があります。

6. jarファイルをSAコアのディレクトリ/etc/opt/opsware/tell/libに配置します。これは、uCMDB Connectorを起動する前に行います。

**注:** SA-uCMDB Connectorに認識させるには、このディレクトリパスを使用する必要があります。

7. SA-uCMDB Connectorを起動します。

SA-uCMDB Connectorの再起動時に、変換関数によってデータが動的に変換されます。

変換ファイルのサンプル - MyConvertVirtualizationType.Java

この変換ファイルサンプルには、ガイドラインとして使用するjavaコードサンプルが含まれています。このjavaサンプルは、SAの**VirtualizationType**をType: NumericからuCMDB用のType: Stringに変換します。

**注:** 属性変換は、javaファイルごとに1つのみ設定できます。複数の属性を変換するには、複数のjavaファイルが必要です。ターゲットの属性には、変換を1つのみ設定できます。

**ヒント:** 変換ファイルの名前は、変更する属性に基づいたものにしてください。この例のjavaファイルはVirtualizationType属性を変換するため、その名前はMyConvertVirtualizationTypeとなっています。

```
package com.hpe.tell;
import java.math.BigDecimal;
import com.hpe.tell.ConversionMethod;
public class MyConvertVirtualizationType extends ConversionMethod {
    public Object convert(Object value) throws Exception{
        Integer vType = putInteger(value);
        String vValue;
        /*
         * SAのVirtualizationType (数値) を、uCMDB用の文字列タイプに変換する関数。
         */
        if (vType > 0) {
            vValue = "True";
        } else {
            vValue = "False";
        }
        return vValue;
    }
    private Integer putInteger(Object o) throws Exception {
        if (o instanceof String) {
            return Integer.valueOf((String) o);
        }
        if (o instanceof BigDecimal) {
            return ((BigDecimal)o).intValue();
        }
        if (o instanceof Integer) {
            return (Integer)o;
        }
        throw new Exception("Invalid conversion in putInteger "+o.getClass
        ().toString());
    }
}
```



## ユースケース

この項では、セットアップ後のSA-uCMDB Connectorを使用するための必要事項について説明します。

- 「SA-uCMDB Connectorの停止と無効化」(73ページ)
- 「SA-uCMDB Connectorのステータスの表示」(74ページ)
- 「SA-uCMDBデータの関係と転送」(75ページ)
- 「uCMDBへのデータ転送頻度」(78ページ)
- 「SAクライアントからuCMDBブラウザーにアクセス」(78ページ)
- 「uCMDBブラウザーの構成」(79ページ)
- 「グローバルuCMDB ID」(80ページ)
- 「uCMDBサーバーとuCMDBブラウザーへのSSL接続」(80ページ)
- 「アップグレード時にアーカイブされる構成可能ファイル」(81ページ)

## SA-uCMDB Connectorの停止と無効化

SA-uCMDB Connectorが実行中の場合は、Connectorを停止し、無効にしてからでなければ、どのような種類の構成変更も行うことができません。

stopコマンド

SA-uCMDB Connectorを停止すると、SAデータベースからuCMDBへのデータ転送も停止されます。SA-uCMDB Connectorを停止するには、SAコアサーバーで次のコマンドを入力します。

```
/etc/init.d/opsware-sas stop telldaemon
```

これにより、SA-uCMDB Connectorが停止されます。

SA-uCMDB Connectorが無効化されている場合、出力は次のようになります。

```
opsware-sas: 指定された1つまたは複数のコンポーネントが次のファイル内に存在しません:
```

```
/opt/opsware/oi_util/startup/components.config
```

SA-uCMDB Connectorが必要でなくなった場合は、disableコマンドを使用して無効にすることができます。詳細については、「[disableコマンド](#)」(73ページ)を参照してください。

**disableコマンド**

SA-uCMDB Connectorを無効にするには、**disable**コマンドを使用します。SA-uCMDB Connectorが実行されている場合、**disable**コマンドはそれを無効にする前に停止します。SA-uCMDB Connectorが無効になっているときは、起動できません。

**disable**コマンドは、ファイル/opt/opsware/oi\_util/startup/components.configを変更し、**telldaemon** (SA-uCMDB Connectorのプロセス)の行をコメントアウトします。

#### **disable**コマンドの場所

**disable**コマンドは、SAコアサーバーの/opt/opsware/tell/binディレクトリにあります。

#### **disable**コマンドの構文

```
/opt/opsware/tell/bin/disable
```

SA-uCMDB Connectorを停止し、無効にするには、次の手順を実行します。

**stop**コマンドを実行して、SA-uCMDB Connectorを停止します。

```
/etc/init.d/opsware-sas stop telldaemon
```

**disable**コマンドを実行して、SA-uCMDB Connectorを無効にします。

```
disable
```

**注:** コネクタが停止され、無効になっていることを確認してから、構成の変更を行ってください。コネクタが停止されず、無効になっていない場合は、Connectorを再起動しようとしたときに問題が発生することがあります。

## SA-uCMDB Connectorのステータスの表示

SA-uCMDB Connectorのステータスを表示するには、SAコアサーバーで次のコマンドを入力します。

```
/etc/init.d/opsware-sas status telldaemon
```

SA-uCMDB Connectorが有効だが実行されていない場合、出力は次のようになります。

```
"telldaemon" が実行されていることを確認してください: エラー (pidfileが存在しない)  
Opsware SASコンポーネントに対して "status" 操作を実行できませんでした。
```

SA-uCMDB Connectorが無効化されている場合、出力は次のようになります。

```
opsware-sas: 指定された1つまたは複数のコンポーネントが次のファイル内に存在しません:  
/opt/opsware/oi_util/startup/components.config
```

## SA-uCMDBデータの関係と転送

### 維持されるCIの関係

「維持されるCIの関係」(75ページ)の表に、SA-uCMDB Connectorで維持される構成アイテム (CI) の関係を示します。

### 維持されるCIの関係

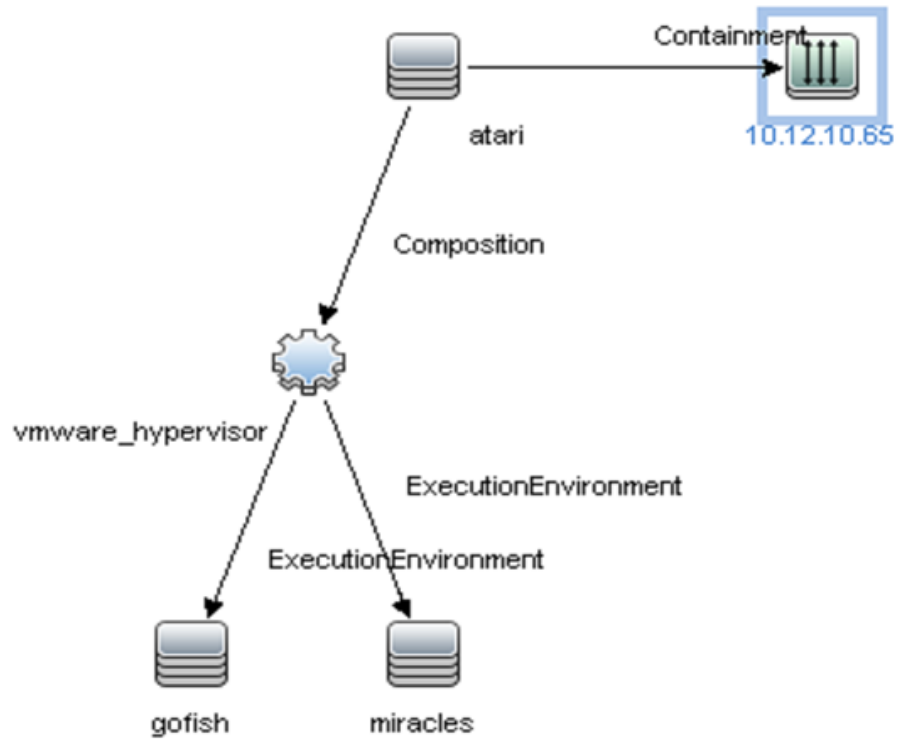
uCMDBのCIから	方法	uCMDBのCIから
Node	containment	IpAddress
Node	composition	InstalledSoftware
Node	composition	Hypervisor
Node	aggregation	PolicyResult
Hypervisor	ExecutionEnvironment	Node
Policy	composition	PolicyResult
SaSystem	aggregation	Node
SaSystem	aggregation	Policy

### SA管理対象サーバーを示すuCMDBの例

「uCMDBに表示されたSA管理対象サーバー」(75ページ)の図は、HPE uCMDB画面から取ったもので、下記を表しています。

- 1つのSA管理対象サーバー(名前はatari)。
- 管理対象サーバーのIPアドレス10.12.10.65。
- 管理対象サーバーatariはVMwareハイパーバイザーを実行している。
- 2つの仮想マシンが、gofishおよびmiraclesというハイパーバイザーで実行されている。

### uCMDBに表示されたSA管理対象サーバー



**uCMDBに転送されるSAデータ**

SAデータベースの次のデータが、uCMDBの構成アイテム (CI) と属性に転送されます (次の表を参照)。

**SAによって設定されるuCMDBのCIと属性**

uCMDBのCI	uCMDBの属性
Node	Name
Node	Description
Node	BiosAssetTag
Node	DefaultGatewayIpAddress
Node	NodeModel
Node	SerialNumber
Node	BiosUuid
Node	NetBiosName
Node	MemorySize

**SAによって設定されるuCMDBのCIと属性 (続き)**

uCMDBのCI	uCMDBの属性
Node	OsDescription
Node	OsFamily
Node	TenantOwner
IpAddress	Name
IpAddress	RoutingDomain
InstalledSoftware	Name
InstalledSoftware	Vendor
InstalledSoftware	BuildNumber
InstalledSoftware	DmlProductName
Hypervisor	Name
Hypervisor	Description
Hypervisor	ProductName
Policy	Name
Policy	Description
Policy	PolicyCategory
Policy	PolicyDefinedBy
PolicyResult	Name
PolicyResult	PolicyResultDateTime
PolicyResult	ComplianceStatus
PolicyResult	RulesCompliant
PolicyResult	RulesNonCompliant
PolicyResult	ComplianceLevel
SASystem	Name
SASystem	Description
SASystem	Version

## uCMDBへのデータ転送頻度

SA-uCMDB Connectorが初めて実行を開始すると、SAデータベースにクエリを行い、uCMDB内にCIを作成し、SAからuCMDBにデータを転送します。その後は、SAデータベースのデータに変更があるたびに、SA-uCMDB Connectorが変更を自動的に検知し、変更データをuCMDBに転送します。このコネクタは、ログファイル/var/log/opsware/tell/LOAD\_STATS.0.logに情報を記録します。

SAからuCMDBに転送されるデータの詳細なリストは、「[uCMDBに転送されるSAデータ](#)」(76ページ)を参照してください。

## SAクライアントからuCMDBブラウザにアクセス

### uCMDBブラウザウィンドウ

サーバーの詳細情報は、uCMDBブラウザウィンドウに表示できます。サーバーの詳細情報を表示するには、次の手順を実行します。

1. SAクライアントにログインします。
2. [デバイス] > [すべての管理対象サーバー] を選択します。
3. 任意のサーバーを選択し、[アクション] > [uCMDBブラウザで開く] をクリックします。

オプション: この画面または [検索] パネルでコンテキストメニューを使用することもできます。サーバーを選択して右クリックし、[次で開く] > [uCMDBブラウザ] を選択してください。

SAが特定の管理対象サーバーに対してuCMDBブラウザを開くときに使用するURLのサンプル:

```
http://my-ucmdb.mycomp.com:8080/ucmdb-api/ucmdb-browser/?locale=en&theme=LIGHT#refocus-selection=<グローバルなuCMDB ID>
```

4. uCMDBブラウザにまだログインしていない場合は、これでuCMDBブラウザのログイン画面が開きます。自分のuCMDBのログイン認証情報を画面に入力してください。サインインは、セッションごとに一度のみ必要です。

**ヒント:** uCMDBブラウザを開いたときに空白のページや「ページが見つかりません」エラーが表示された場合は、uCMDBがセットアップされていない、またはuCMDBサーバーが実行されていないか正しく構成されていない可能性があります。uCMDBサーバーが構成され、Tellconnectorが実行されていることを確認してください。

SA-uCMDB Connectorが未構成で、[uCMDBブラウザーで開く]メニューを無効にする必要がある場合は [システム構成] > [Opware] > [Tell] を選択し、[uCMDBブラウザーのURL] および [uCMDBのURL] の値を値なしに設定します。

## uCMDBブラウザーの構成

uCMDBブラウザーをSAクライアントから起動する必要がある場合は、SA-uCMDB Connectorを有効にした後で、`/opt/opsware/tell/bin/enable`のパラメーターを使用して、uCMDBブラウザーの関連パラメーターを指定する必要があります。

`-browser_protocol` - uCMDBブラウザーサーバーのプロトコル、httpまたはhttps

`-browser_host` - uCMDBブラウザーのホスト名またはIP

`-browser_port` - uCMDBブラウザーのホストポート

uCMDB 10.01ベースのブラウザーを使用するには、次の手順を実行します。

1. **stop**コマンドを実行して、SA-uCMDB Connectorを停止します。

```
/etc/init.d/opsware-sas stop telldaemon
```

2. **disable**コマンドを実行して、SA-uCMDB Connectorを無効にします。

```
disable
```

**注:** コネクターが停止され、無効になっていることを確認してください。コネクターが停止されず、無効化されていないときに構成ファイルを改訂すると、Connectorを再起動しようとしたときに問題が発生することがあります。

3. SA-uCMDB Connectorのカスタム構成ファイル`/etc/opt/opsware/tell/tell_custom.conf`で、ご使用のuCMDBブラウザーのバージョンに合わせてuCMDBブラウザーのサフィックスを更新します。

例:

変更の対象となるデフォルトURLは次のとおりです。

```
com.hp.e.sa.tell.ucmdb.browser.path.suffix=/ucmdb-browser/?locale=en&theme=LIGHT
```

uCMDBブラウザー3.21以降を使用する場合は、URLを次のように変更します。

```
com.hp.e.sa.tell.ucmdb.browser.path.suffix=/ucmdb-browser/?locale=en
```

uCMDBの設定に合わせてhttp GETパラメーターを適宜、追加、削除、または変更することができます。

4. 構成ファイルを更新したら、**enable**コマンドを実行して、SA-uCMDB Connectorを有効にします。

**enable**コマンドの構文は、使用環境によって異なります。**enable**コマンドの構文とオプションについては、このドキュメントの「[enableコマンド](#)」(60ページ)を参照してください。

5. uCMDB Connectorを再起動します。次のコマンドを入力して、SA-uCMDB Connectorを起動します。

```
/etc/init.d/opsware-sas start telldaemon
```

6. (オプション) 次のコマンドでSA-uCMDB Connectorのステータスをチェックします。

```
/etc/init.d/opsware-sas status telldaemon
```

## グローバルuCMDB ID

uCMDB 9.04以前では、そのuCMDBサーバーが認識しているローカルのuCMDB IDのみがSAで同期されていました。

uCMDBグローバルIDジェネレーターとしてuCMDBサーバーを構成できます。そこで生成されるuCMDB IDは、複数uCMDBサーバー環境に対してグローバルかつ一意です。このような環境でuCMDBブラウザーを適切に起動するには、これらのグローバルIDが必要です。

uCMDBサーバーがグローバルIDジェネレーターとして構成されている場合、SA 9.14のSA-uCMDB Connectorは、CIのグローバルuCMDB IDを自動的に使用するように機能強化されました。SA-uCMDB Connectorについて、特別な構成は不要です。

## uCMDBサーバーとuCMDBブラウザーへのSSL 接続

SA-uCMDB Connectorは、uCMDBサーバーとuCMDBブラウザーに対してSSLプロトコルをサポートしています。

セキュアソケットレイヤー通信 (SSL) を有効にする場合は、SA-uCMDB Connector用に適切な証明書とキーストアが揃っていることが必要です。

**SSLを有効にするには、次の手順を実行します。**

『uCMDBデプロイメントガイド』の「[セキュアソケットレイヤー通信の有効化](#)」の指示に従って、uCMDBキーストアを作成し、証明書をファイルにエクスポートします。



ステップ1でエクスポートした証明書をSA-uCMDB Connectorがインストールされている場所にインポートします。たとえば、キーストアを/var/opt/opsware/crypto/tellに配置する必要があります。その際、キーストアファイル名はtell.keystoreとし、キーストアパスワードはhppassとします。

インポートコマンドの例:

```
/opt/opsware/jdk1.8/bin/keytool -import -noprompt -alias hpsaucmdb -file <path_to_the_exported_hpcert> -keypass hppass -keystore  
/var/opt/opsware/crypto/tell/tell.keystore -storepass hppass
```

## アップグレード時にアーカイブされる構成可能 ファイル

アップグレード時には、カスタマイズ可能で構成可能な特定ファイルが、保全のためにアーカイブされます。

SA-uCMDB Connector 9.14から10.0にアップグレードする場合は、次のファイルが

/var/opt/opsware/install\_opsware/config\_file\_archive/<ファイルのそれぞれのパス>にアーカイブされます。

- tell.conf
- mapping.xml
- logging.properties
- tell\_conversions.jar
- tell.pwd
- tell.keystore

たとえば、/etc/opt/opsware/tell/tell\_custom.comにあるtell\_custom.confは

/var/opt/opsware/install\_opsware/config\_file\_archive/etc/opt/opsware/tell/tell\_custom.com<アップグレードのタイムスタンプ>にアーカイブされます。

SA-uCMDB Connector 10.0および将来のアップグレードでは、**tell\_custom.conf**と**mapping\_custom.xml**も保全のためにアーカイブされます。

# SA-uCMDB統合のトラブルシューティング

## 別のコアでのSA-uCMDB Connectorの実行

ときには、マルチマスターSAメッシュ内の特定のコアを非アクティブにし、そのメッシュ内の別のコアからSA-uCMDB Connectorを実行することが必要になる場合があります。この処理は、別のコアからuCMDBサーバーにネットワークした方が望ましい性能が得られる場合にも必要になります。このような場合は、次の手順が必要になります。

コネクタを別のコアで実行するには、次の手順を実行します。

1. 最初のコアでSA-uCMDB Connectorを停止し、そのコアに対するアフィニティを削除します。  

```
/etc/init.d/opsware-sas stop telldaemon  
/opt/opsware/tell/bin/tell --release
```
2. 2番目のコアで**enable**コマンドを実行して、SA-uCMDB Connectorを有効にします。**enable**コマンドの構文は、使用環境によって異なります。enableコマンドの構文とオプションについては、このドキュメントの「[enableコマンド](#)」(60ページ)を参照してください。
3. SA-uCMDB統合の責任を引き受けてから、SA-uCMDB Connectorを起動します。  

```
/opt/opsware/tell/bin/tell --take  
/etc/init.d/opsware-sas start telldaemon
```

追加のログ処理を有効にするには、次の手順を実行します。

1. SA-uCMDB Connectorを起動します。通常のログファイルは、`/var/log/opsware/tell`ディレクトリに保存されます。デフォルトのファイル名は次のとおりです。  
tell.0.log (通常のスタートアップログ)  
ucmdb\_failure.\*.log (同期中に認識されたuCMDBエラー)  
LOAD\_STATS.\*.log (処理したデータの数)
2. 追加のログ詳細を要求するために、次の表を参考にして、要求する情報を  
`/etc/opt/opsware/tell/logging.properties`ファイルで指定します。

### `/etc/opt/opsware/tell/logging.properties`のフィールド

フィールド	説明
<code>java.util.logging.FileHandler.limit</code>	任意の1ファイルに書き込む最大バイト数を指定します。デフォルト値は10000000です。

**/etc/opt/opsware/tell/logging.propertiesのフィールド (続き)**

フィールド	説明
java.util.logging.FileHandler.count	使用するファイルの数を指定します。デフォルト値は10です。
java.util.logging.FileHandler.append	アペンドモードを指定します。デフォルトはtrueです。
java.util.logging.FileHandler.pattern	出力ファイルの命名パターン (ログファイルの場所) を指定します。デフォルトは <code>/var/log/opsware/tell/tell.%g.log</code> です。

**注意:** ファイルの制限を変更するときは、注意してください。値が大きいと、パフォーマンスに影響することがあります。

## オンデマンド同期

SAを再起動すると、SA-uCMDB Connectorは、通常は再起動の前に終了していたところから、uCMDB に対するSAデータの同期を続行します。このコネクタは、定期的に完全同期も実行します。ただし、ネットワークやサーバーに問題があって、更新データがuCMDBサーバーに届かないような場合は、完全同期をオンデマンドで開始しなければならないこともあります。

同期をオンデマンドで開始するには、次の手順を実行します。

1. SA-uCMDB Connectorを停止します。
2. 次のオプションを指定して、SA-uCMDB Connectorを再起動します。

```
/opt/opsware/tell/bin/tell --startfresh
```

## ログファイルの表示

SA-uCMDB Connectorは、次のテキストログファイルを生成します。これらのログファイルは、テキストエディターで表示して、詳細情報を得ることができます。

- `/var/log/opsware/tell/tell.0.log`は、SA-uCMDB Connectorで発生する情報、警告、およびエラー用のメインのログファイルです。
- `/var/log/opsware/tell/LOAD_STATS.0.log`には、初期データロードのステータスと統計、および初期データロードの完了にかかった概略時間が含まれます。
- `/var/log/opsware/tell/ucmdb_failure.0.log`には、uCMDBエラーが含まれます。SAデータが不完全な場合 (たとえば、必要なuCMDBキーがない場合)、これは主として調整エラーです。これは、たとえ

ば、サーバーにシリアル番号やIPアドレスがない場合などに発生します。このログには、uCMDB例外、エラーが発生した原因、例外の原因となったCIのトレースが含まれます。

## SA-uCMDB Connectorデーモン

SA-uCMDB Connectorは、SAコアサーバー上でデーモン/etc/opt/opsware/startup/telldaemonを実行します。このプロセスがSAコアサーバーで実行されていることを確認してください。

実行されていない場合は、「[Enableコマンドの新しい構文](#)」(61ページ)の説明に従って起動してください。

実行されている場合は、「[SA-uCMDB Connectorのステータスの表示](#)」(74ページ)の説明に従ってステータスを確認してください。

### 例 – SA-uCMDB Connectorのマッピングファイル

```
<DB-UCMDB-HIGHLEVEL-MAPPING>
```

```
    <!-- generates installed_software.xml -->
    <Model-Definition model-name='sa' enable='true'>
        <CI ucmdb-ci-type-name='server_automation_system' enable='true' base-class='server_automation_system'>
            <Attribute source='SA/Description' target-attr='description'
enable='true' />
            <Attribute source='SA/Name' target-attr='name' enable='true' />
            <Attribute-Default target-attr='version' target-attr-value='9.14'
enable='true' />
        </CI>
    </Model-Definition>
    <!-- generates node.xml -->
    <Model-Definition model-name='hosts' enable='true'>
        <CI ucmdb-ci-type-name='server_automation_system' reference-ci='true'
enable='true' />
        <CI ucmdb-ci-type-name='ip_address' enable='true' base-class='node'>
            <Attribute source='IpAddress/PrimaryIpName' target-attr='name'
enable='true' />
            <Attribute source='IpAddress/RoutingDomain' target-attr='routing_
domain' enable='true' />
        </CI>
```

```
<CI ucmdb-ci-type-name='node' enable='true' base-class='node'>
  <Attribute source='Node/Name' target-attr='name' enable='true' />
  <Attribute source='Node/Description' target-attr='description'
enable='true' />
  <Attribute source='Node/BiosAssetTag' target-attr='bios_asset_tag'
enable='true' />
  <Attribute source='Node/BiosSerialNumber' target-attr='serial_number'
enable='true' />
  <Attribute source='Node/BiosUuid' target-attr='bios_uuid'
enable='true' />
  <Attribute source='Node/DefaultGatewayIpAddress' target-attr='default_
gateway_ip_address' enable='true' />
  <Attribute source='Node/NetBiosName' target-attr='net_bios_name'
enable='true' />
  <Attribute source='Node/NodeModel' target-attr='node_model'
enable='true' />
  <Attribute source='Node/MemorySize' target-attr='memory_size'
enable='true' />
  <Attribute source='Node/OsDescription' target-attr='os_description'
enable='true' />
  <Attribute source='Node/OsFamily' target-attr='os_family'
enable='true' />
  <Attribute source='Node/TenantOwner' target-attr='TenantOwner'
enable='true' />
  <Attribute source='Node/Facility' target-attr='facility'
enable='false' />
  <Attribute source='Node/VirtualizationTypeId' target-
attr='virtualization_type_id' enable='false' />
  <Attribute source='IpAddress/ManagementIpName' target-attr='ip_address'
enable='false' />
  <CI-Filter enable='true'>(DEVICES.OPSW_LIFECYCLE = 'MANAGED')</CI-
Filter>
</CI>
  <Relation ucmdb-relation-type-name='containment' ucmdb-relation-from-ci-
type-name='node' ucmdb-relation-to-ci-type-name='ip_address' enable='true' ucmdb-
relation-id-link='true' />
```

```
<Relation ucmdb-relation-type-name='aggregation' ucmdb-relation-from-ci-
type-name='server_automation_system' ucmdb-relation-to-ci-type-name='node'
enable='true' ucmdb-relation-id-link='false'/>

</Model-Definition>

<!-- generates installed_software.xml -->

<Model-Definition model-name='software' enable='true'>

  <CI ucmdb-ci-type-name='node' base-class='node' reference-ci='true'
enable='true'/>

  <CI ucmdb-ci-type-name='installed_software' enable='true' base-
class='installed_software'>

    <Attribute source='InstalledSoftware/DmlProductName' target-attr='dml_
product_name' enable='true'/>

    <Attribute source='InstalledSoftware/Name' target-attr='name'
enable='true'/>

    <Attribute source='InstalledSoftware/Version' target-attr='version'
enable='true'/>

    <Attribute source='InstalledSoftware/Vendor' target-attr='vendor'
enable='true'/>

  </CI>

  <Relation ucmdb-relation-type-name='composition' ucmdb-relation-from-ci-
type-name='node' ucmdb-relation-to-ci-type-name='installed_software' ucmdb-
relation-id-link='true' enable='true'/>

</Model-Definition>

<!-- generates policy.xml -->

<Model-Definition model-name='compliance' enable='true'>

  <CI ucmdb-ci-type-name='server_automation_system' reference-ci='true'
enable='true'/>

  <CI ucmdb-ci-type-name='policy' base-class='policy' enable='true'>

    <Attribute source='Policy/Name' target-attr='name' enable='true'/>

    <Attribute source='Policy/Description' target-attr='description'
enable='true'/>

    <Attribute-Default target-attr='policy_defined_by' target-attr-
value='SA' enable='true'/>

    <Attribute-Default target-attr='policy_category' target-attr-
value='audit' enable='true'/>

  </CI>
```

```
<Relation ucmdb-relation-type-name='aggregation' ucmdb-relation-from-ci-
type-name='server_automation_system' ucmdb-relation-to-ci-type-name='policy'
enable='true' ucmdb-relation-id-link='false'/>

</Model-Definition>

<!-- generates hypervisor.xml -->

<Model-Definition model-name='hypervisor' enable='true'>

  <CI ucmdb-ci-type-name='node' base-class='node' reference-ci='true'
enable='true'/>

  <CI ucmdb-ci-type-name='hypervisor' base-class='hypervisor' enable='true'>

    <Attribute source='Hypervisor/Name' target-attr='name' enable='true'/>

    <Attribute source='Hypervisor/Description' target-attr='description'
enable='true'/>

    <Attribute source='Hypervisor/ProductName' target-attr='product_name'
enable='true'/>

  </CI>

  <Relation ucmdb-relation-type-name='composition' ucmdb-relation-from-ci-
type-name='node' ucmdb-relation-to-ci-type-name='hypervisor' ucmdb-relation-id-
link='true' enable='true'/>

</Model-Definition>

<!-- generates hypervisorRelation.xml -->

<Model-Definition model-name='vmrelations' enable='true'>

  <CI ucmdb-ci-type-name='hypervisor' base-class='hypervisor' reference-
ci='true' enable='true'/>

  <CI ucmdb-ci-type-name='node' base-class='node' reference-ci='true'
enable='true'/>

  <Relation ucmdb-relation-type-name='execution_environment' ucmdb-relation-
from-ci-type-name='hypervisor' ucmdb-relation-to-ci-type-name='node' ucmdb-
relation-id-link='false' enable='true'/>

</Model-Definition>

<!-- generates policyResult.xml -->

<Model-Definition model-name='compliance_status' enable='true'>

  <CI ucmdb-ci-type-name='policy' base-class='policy' reference-ci='true'
enable='true'/>

  <CI ucmdb-ci-type-name='node' base-class='node' reference-ci='true'
enable='true'/>
```

```
<CI ucmdb-ci-type-name='policy_result' base-class='policy_result'
enable='true'>
  <Attribute source='PolicyResult/Name' target-attr='name'
enable='true' />
  <Attribute source='PolicyResult/ComplianceStatus' target-
attr='compliance_status' enable='true' />
  <Attribute source='PolicyResult/PolicyResultDateTime' target-
attr='policy_result_date_time' enable='true' />
  <Attribute source='PolicyResult/RulesCompliant' target-attr='rules_
compliant' enable='true' />
  <Attribute source='PolicyResult/RulesNonCompliant' target-attr='rules_
non_compliant' enable='true' />
  <Attribute source='PolicyResult/ComplianceLevel' target-
attr='compliance_level' enable='true' />
</CI>
  <Relation ucmdb-relation-type-name='composition' ucmdb-relation-from-ci-
type-name='policy' ucmdb-relation-to-ci-type-name='policy_result' ucmdb-relation-
id-link='false' enable='true' />
  <Relation ucmdb-relation-type-name='aggregation' ucmdb-relation-from-ci-
type-name='node' ucmdb-relation-to-ci-type-name='policy_result' ucmdb-relation-id-
link='true' enable='true' />
</Model-Definition>
</DB-UCMDB-HIGHLEVEL-MAPPING>
```



# HPELNとの統合

## 概要

HPE Live Networkコネクター (HPE LNC) は、HPE Server Automation (HPE SA) をはじめとするいくつかのHPEソフトウェア製品と統合された動的なコンテンツ更新ツールです。

セキュリティポリシーとコンプライアンスポリシーの提供を通じて、HPEソフトウェア製品への投資効果を最大限に引き出し、拡張可能な自動化プラットフォームで新しい自動化機能を継続的に提供します。

HPE LNCは、Business Service Automation製品とHPELNを直接リンクします。LNCによって、HPE SAのコンテンツとコンテンツ更新をリアルタイムにダウンロードすることができます。

HPEの顧客企業は、LNCを使用することで、全世界のデータセンターにサブスクリプションサービスのコンテンツを毎日提供することができます。

LNCは、プロファイルと呼ばれるプラグインでカスタマイズすることができます。LNCと統合するどの製品にも、LNCをカスタマイズするプロファイルが必要です。

『HPE Live Network Connector User Guide』、『LNC Release Notes』、HPE LNCインストーラーは、<https://hpln.hpe.com/contentoffering/hpe-live-network-connector>で入手可能です (HPE Passportの資格情報で接続する必要があります)。

Live Networkコネクターは、通常、HPE SAコアとともに次のディレクトリにインストールされます。

`/opt/opsware/hpln/..`

Live Networkコネクターのバイナリは、`/opt/opsware/hpln/lnc/bin/`にあります。

注: LNCガイドの最新版は、次の場所にあります。

[https://lnast01pcache.saas.hpe.com/asset/resources/co/1284/10f1459953792/HPELN\\_LNC\\_Users\\_Guide.pdf](https://lnast01pcache.saas.hpe.com/asset/resources/co/1284/10f1459953792/HPELN_LNC_Users_Guide.pdf)

## 統合のセットアップ

この項では、LNCの構成と、そのサービスおよびストリームの構成方法について説明します。さらに、コンテンツがダウンロード済みかどうかを確認する方法と、LNCログファイルの場所の確認方法についても説明します。

## 前提条件

LNcは、SAコアコンポーネントサーバーにインストールされている必要があります。LNcを起動するには、SAコアコンポーネントサーバーで(LNcスクリプトは\$PATHにあると仮定)live-network-connectorコマンドを入力します。

LNcは、デフォルトで次の処理を行います。

- SSL接続
- 失敗したダウンロードの再試行 (1回)
- 指定された製品のコア更新 (ある場合) のダウンロードとインポート
- 有効化したストリームからのコンテンツのインポート

**注:** 最初の更新にはかなりの時間を要する可能性があります。

## Live Networkコネクターの構成

この項では、HPE Live Networkに接続するためにLNcを構成する方法について説明します。

1. PATH変数に次の項目を追加します。

- <インストールディレクトリ>/lnc/bin

例:

```
export PATH=$PATH:<インストールディレクトリ>/lnc/bin
```

2. LNcがインストールされたコンピューターでコマンドプロンプトを開きます。
3. ユーザー名とパスワードを設定するために、次のコマンドを入力します。

```
live-network-connector write-config --username=<ユーザー名> --password=<パスワード>
```

--usernameコマンドと--passwordコマンドは別々に実行することもできます。

**注:** LNc構成ファイルの手動編集はサポートされていません。手動編集を行うと、ファイルが破損したり、設定が失われたりするおそれがあります。代わりにwrite-configコマンドを使用してください。

4. コンテンツのダウンロードに使用するLNcの接続先URLをチェックするために、次のコマンドを実行しま

す。live-network-connector read-config --url

次のURLが出力されます。

<https://hpln.glob.itcs.hp.com>

5. (オプション) HPE Live Networkにアクセスするためにプロキシサーバーを使用する必要がある場合は、次のコマンドを実行します。

```
live-network-connector write-config --http-proxy=<HTTPプロキシ> --http-proxy-user=<HTTPプロキシのユーザー名> --http-proxy-pass=<HTTPプロキシのパスワード>
```

**--http-proxy**、**--http-proxy-user**、**--http-proxy-pass**の各コマンドは、別々に実行することもできます。

6. LNCログファイルのデフォルトパスは次のとおりです。

- <インストールディレクトリ>/lnc/log/live-network-connector.log

7. LNCキャッシュディレクトリのデフォルトパスは次のとおりです。

- <インストールディレクトリ>/lnc/cache

- (オプション) この値の変更は可能ですが、取得したコンテンツの再ダウンロードと再インポートが行われる可能性があるため、注意が必要です。このデフォルト値を変更するには、LNCがインストールされたシステムで次のコマンドを実行します。

```
live-network-connector write-config --cache=<パス>
```

8. LNCロックファイルのデフォルトパスは次のとおりです。

- <インストールディレクトリ>/lnc/live-network-connector.lock

9. 特定の製品用にLNCを構成するために、--productでその製品を指定します。

長い製品名をはじめ、サポート対象製品の値を列挙するには、コマンドlive-network-connector list-productsを実行します。

現在サポートされている製品のリストが表示されます。このリストは次の構成手順で使用します。

たとえば、Server Automation (sas) をサポートするためにLNCインストールを構成するには、LNCがインストールされたシステムで次のコマンドを実行します。

```
live-network-connector write-config --product=sas
```

**重要:** 複数の製品を有効にするには、**--product**を指定した**write-config**コマンドを各製品につき1回実行します。なお、**write-config**コマンドを続けて実行すると、前の値は上書きされません。

- LNC構成ファイルの手動編集はサポートされていません。手動編集を行うと、ファイルが破損したり、設定が失われたりするおそれがあります。代わりにwrite-configコマンドを使用してください。
- 有効にする製品によっては、追加の設定が必要になります。詳細については、製品のドキュメントを参照するか、製品の管理者にお問い合わせください。

10. 製品を構成した後、選択した製品で利用可能なコンテンツ(ストリーム)のリストをlist-streamsコマンドで表示することができます。

例: live-network-connector list-streams

**注:** ストリームが表示されない場合は、特定の製品用にシステムを設定済みであることを確認してください。

11. 必要に応じて、それらのストリームに対して追加のクエリを実行します (describeコマンドの実行など)。

例:

```
live-network-connector write-config --stream=content.ms_patch_supp
```

12. SAへのアクセスに使用するSAユーザーアカウントのユーザー名 (sas\_user) とパスワード (SAS\_pass) の値を設定するために、次のコマンドを実行します。

```
live-network-connector write-config  
--setting=sas.sas_user=<SAユーザー名>  
--setting=sas.sas_pass=<SAユーザーパスワード> --add
```

13. **cbt\_path**の値をCBT実行可能ファイルのパスに、**cbt\_config\_path**の値をCBT構成ファイルのパスに設定するために、次のコマンドを実行します。

```
live-network-connector write-config  
--setting=sas.cbt_path=<CBT実行可能ファイルのパス>  
--setting=sas.cbt_config_path=<CBT構成ファイルのパス> --add
```

## サービスとストリーム

HPE Live Networkは、コンテンツをストリームとサービスという形で提供します。

- **ストリーム:** 関連するコンテンツのグループ。形式、機能、または用途の面で互いに関連し合う複数のコンテンツオブジェクトをまとめたものです。

- **サービス:** ストリームのグループ。顧客がその資格に基づいて使用できるすべてのストリームを集めたものです。資格は、特定のHPE Live Networkアカウントの資産および有効なライセンス契約または保守契約に基づいて決定されます。

LNC構成ファイルでは、ストリームはサービスまたは製品のブロックでグループ化されます。

## サービスとストリームの表示

利用可能なサービスとストリームのリストを表示するには、**list-streams**コマンドまたは**describe**コマンドを使用します。

**注:** コマンドを正常に実行するには、製品の設定 (write-config --productを使用するか、コマンドラインで--productを指定する) が不可欠です。利用可能な製品を表示するには、list-productsコマンドを使用します。

- コマンドプロンプトで、次のコマンドを入力します。

```
live-network-connector list-streams
```

list-streamsコマンドが返す値の形式は次のとおりです。

<製品> <サービス> <ストリーム> (<ストリーム>.<名前>)

このコマンドが返すストリームの例は次のとおりです。

```
sas security vc_cisco (security.vc_cisco)
```

- コマンドプロンプトで、次のコマンドを入力します。

```
live-network-connector describe
```

describeコマンドが返す値の形式は次のとおりです。

<製品> <サービス> <ストリーム> (<ストリーム>.<名前>) <有効/無効のステータス>

<そのストリームの説明やURL> <利用可能なタグ>

このコマンドが返す出力の例は次のとおりです。

```
Product      Stream                                     Enabled
=====
hpca         security.hpca_config                       0
                                                    Description
```

Configuration definition to allow for the HPCA product to add new or adapt to changes in subscriptions services.

Tags

---

hpca\_config

## コンテンツストリームとセキュリティストリームの構成

サービスの各ストリームは、LNC構成で有効にする必要があります。有効にするには、**live-network-connector**コマンドの後に**write-config**と記述し、その後に各ストリームの具体的なパラメーターを指定します。ストリームをアクティブにするには、値を1に設定します。

たとえば、ストリームをアクティブにするには、LNCがインストールされたサーバーで、シェルから次のコマンドを入力します。

```
live-network-connector write-config --stream=security.cc_library --enable
```

LNCは、SAソフトウェアリポジトリコンポーネントのインストール先と同じサーバーにインストールする必要があります。さらに、「[Live Networkコネクターの構成](#)」の説明に従ってLNCを構成する必要があります。

**注:** **live-network-connector write-config**コマンドの結果、構成パラメーターがないことを示すメッセージが表示された場合、コマンドの後に**--add**オプションを追加してください。LNC構成ファイルの手動編集はサポートされていません。手動編集を行うと、ファイルが破損したり、設定が失われたりするおそれがあります。代わりに**write-config**コマンドを使用してください。

## Microsoft Patch Supplementストリームの構成

LNCを構成してMicrosoft Patch Supplementストリームをアクティブにするには、次の手順を実行します。

1. LNCがインストールされたシステムで次のコマンドを実行して、Microsoft Patch Supplementストリームを有効にします。

```
live-network-connector write-config --stream=content.ms_patch_supp --enable
```

2. (オプション) Microsoft Patch Supplementストリームを無効にするには、`--disable`コマンドを使用してコマンドを実行します。

```
live-network-connector write-config --stream=content.ms_patch_supp --disable
```

3. (オプション) Microsoft Patch Supplementストリームを有効にして、SAにコンテンツをインポートしたときのメタデータに上書きするには、`sas.force_win_patch_import`パラメーターを設定します。

たとえば、このオプションを有効にするには、次のコマンドを実行します。

```
live-network-connector write-config --setting=  
sas.force_win_patch_import=1 --add
```

4. (オプション) このオプションを無効にするには、次のコマンドを実行します。

```
live-network-connector write-config --setting=  
sas.force_win_patch_import=0 --add
```

5. 次のコマンドを入力して、LNCを起動します。

```
live-network-connector
```

## ソフトウェア検出ストリームの構成

SAソフトウェア検出ストリームをアクティブにするためにLNCを構成するには、次の手順を実行します。

1. LNCがインストールされたシステムで次のコマンドを実行して、ソフトウェア検出ストリームを有効にします。

```
live-network-connector write-config  
--stream=content.software_discovery --enable
```

2. (オプション) ソフトウェア検出ストリームを無効にするには、`--disable`オプションを使用してコマンドを実行します。

```
live-network-connector write-config  
--stream=content.software_discovery --disable
```

3. 次のコマンドを入力して、LNCを起動します。

```
live-network-connector
```

## SA DMAストリームの構成

sa\_dmaストリームをアクティブにするためにLNcを構成するには、次の手順を実行します。

1. LNcがインストールされたシステムで次のコマンドを実行して、sa\_dmaストリームを有効にします。

```
live-network-connector write-config --stream=content.sa_dma --enable
```

2. (オプション) sa\_dmaストリームを無効にするには、--disableオプションを使用してコマンドを実行します。

```
live-network-connector write-config --stream=content.sa_dma --disable
```

3. 次のコマンドを入力して、LNcを起動します。

```
live-network-connector
```

## コンテンツのオペレーティングシステムプラットフォームファミリのストリームの構成

LNcを構成してプラットフォームストリーム (Linux、Unix、Windows、VMware) をアクティブにするには、次の手順を実行します。

1. LNcがインストールされたシステムで次のコマンドを実行して、platform\_<プラットフォームファミリタイプ> ストリームを有効にします。

```
live-network-connector write-config --stream=content.platform_<プラットフォームファミリタイプ> --enable
```

2. (オプション) platform\_<プラットフォームファミリタイプ> ストリームを無効にするには、--disableオプションを使用してコマンドを実行します。

```
live-network-connector write-config --stream=content.platform_<プラットフォームファミリタイプ> --disable
```

3. 次のコマンドを入力して、LNcを起動します。

```
live-network-connector
```



## Solaris/パッチ供給ストリームの構成

このコンテンツをダウンロードする前提条件として、`/etc/opt/opsware/solpatch_import/`の`solpatch_import.conf`ファイルを編集する必要があります。具体的には、`sa`のユーザー名/パスワード、ダウンロードのユーザー名/パスワード、プロキシホスト、`fujitsu_download_user/pass`の値を追加します。

`solpatch_import.conf`を使用してdbを作成する必要があります。

LNcを構成して`solaris_patching`ストリームをアクティブにするには、次の手順を実行します。

1. LNcがインストールされたシステムで次のコマンドを実行して、`solaris_patching`ストリームを有効にします。

```
live-network-connector write-config --stream=content.solaris_patching --enable
```

2. (オプション) `solaris_patching`ストリームを無効にするには、`--disable`オプションを使用してコマンドを実行します。

```
live-network-connector write-config --stream=content.solaris_patching --disable
```

3. 次のコマンドを入力して、LNcを起動します。

```
live-network-connector
```

## セキュリティスキャナーストリームの構成

`security_scanner`ストリームをアクティブにするためにLNcを構成するには、次の手順を実行します。

1. LNcがインストールされたシステムで次のコマンドを実行して、`security_scanner`ストリームを有効にします。

```
live-network-connector write-config  
--stream=security.security_scanner --enable
```

2. (オプション) `security_scanner`ストリームを無効にするには、`--disable`オプションを使用してコマンドを実行します。

```
live-network-connector write-config  
--stream=security.security_scanner --disable
```

3. 次のコマンドを入力して、LNcを起動します。

```
live-network-connector
```

## SA脆弱性コンテンツストリームの構成

LNcを構成してSA脆弱性コンテンツストリームをアクティブにするには、次の手順を実行します。

1. LNcがインストールされたシステムにログインします。
2. 更新情報の送信元の各SA脆弱性コンテンツストリームをアクティブにするために、コマンドラインで特定のLNc構成パラメーターを1に設定します。

たとえば、SAの脆弱性コンテンツへのサブスクリプションがある場合、次のコマンドを実行します。

```
live-network-connector write-config --stream=security.vc_winxp  
--stream=security.vc_win2k3 --stream=security.vc_rhel3  
--stream=security.vc_hpux11 --enable
```

3. (オプション) ストリームを無効にするには、`--disable`オプションを使用してコマンドを実行します。

```
live-network-connector write-config --stream=security.vc_winxp  
--stream=security.vc_win2k3 --stream=security.vc_rhel3  
--stream=security.vc_hpux11 --disable
```

## SAコンプライアンスコンテンツストリームの構成

`security.cc_library`ストリームは、すべてのSAコンプライアンスストリームを有効にするための前提となるストリームであり、コンテンツのダウンロード先となる各SAシステムで少なくとも1回実行する必要があります。HPELNから新しいコンテンツをインポートする場合、そのたびにこのストリームを有効にする必要があります。

LNcを構成してSAコンプライアンスコンテンツストリームをアクティブにするには、次の手順を実行します。

1. LNcがインストールされたシステムにログインします。
2. 更新情報の送信元の各SAコンプライアンスコンテンツストリームをアクティブにするために、コマンドラインで特定のLNc構成パラメーターを1に設定します。

たとえば、SA監査と修復のコンプライアンスコンテンツを有効にするには、次のコマンドを実行します。

```
live-network-connector write-config --stream=security.cc_library  
--stream=security.ec_disa_stig --enable
```

3. (オプション) ストリームを無効にするには、`--disable`オプションを使用してコマンドを実行します。

```
live-network-connector write-config --stream=security.cc_library  
--stream=security.ec_disa_stig --disable
```

## ユースケース

### 一般的なトラブルシューティングのヒント

LNcに関する問題が発生した場合は、次の手順を実行します。

1. このドキュメントを熟読し、発生した問題の解決策を見つけます。また、必須設定をすべて目的どおりに構成するために、製品とコンテンツのドキュメントを参照し、追加の必須パラメーターがあればそれらも正しく構成されていることを確認します。
2. 次のコマンドを実行します。

```
live-network-connector read-config
```

ユーザー名と製品の値をすべて確認し、スペルミスがなく、必要なストリームが有効であることを確認します。なお、アルファベット以外の文字を含むパスワードは、特別な処理が必要になる場合があります。

入力されたパスワードは、オペレーティングシステムのコマンドインタプリターによって解釈されます。一部の文字は特別な意味を持つため、LNcに正しく渡すにはエスケープが必要です。特殊文字と、コマンドラインでの特殊文字のエスケープ処理や引用符処理の詳細については、Linuxの場合はbashの"man" ページ (例: man bash) を、それ以外のUnixの場合は使用中の各shellの"man" ページを参照してください。

Unixシステムでの簡単な例を示します。

LNcにパスワードmy\$?9FYI^を渡すには、特殊文字を次のようにエスケープします。

```
live-network-connector write-config --password='my$?9FYI^'
```

3. 次のコマンドが正しく実行されることを確認します。これにより、資格情報と製品設定が正しいかどうかを検証できます。エラーが表示される場合は、ユーザー名、パスワード、製品設定を確認し、必要に応じて再構成を行います。

```
live-network-connector list-streams
```

4. アカウントにフルアクセス権があることを確認するために、ユーザー資格情報を使用して <https://hpln.hpe.com> にログインし、関連する製品またはコンテンツの領域を表示して、自分自身がコンテンツ閲覧者として表示されることを確認します。

表示されない場合、次のサイトでアカウントにサービスアグリーメントIDが関連付けられていることを確認します。

<https://softwaresupport.hpe.com/>

5. コンテンツを無事にダウンロードできるものの、インポート時に問題が発生する場合、一般に、製品またはコンテンツ固有の問題が構成に存在します。必須設定を確認し、それに従って環境を更新してください。
6. 以上の手順を実行しても問題が解決されない場合、次の手順を実行します。

- a. 次のコマンドの出力を保存します。

```
live-network-connector read-config
```

```
live-network-connector list-status --product=all --stream=all
```

- b. <インストールパス>/lnc/log の下の既存のLNCログファイルを切り詰めるか、移動または削除し、問題が発生するコマンドの末尾に `--debug` を付けてコマンドを再実行します。

たとえば、ユーザー資格情報と必要に応じてプロキシ情報を指定してLNCを正しく構成し、製品を有効にし、コンテンツのサブスクリプションのためにストリームを1つ以上選択し、そのコンテンツを更新してインポートする場合、次のコマンドを実行します。

```
live-network-connector download-import --debug
```

実行後、`live-network-connector.log` ファイルを圧縮またはアーカイブ (zip、gzipなど) します。

- c. 必要に応じてサポートケースを開きます。構成に製品またはコンテンツ固有の問題が存在する場合、またはコンテンツがダウンロードされるもののインポートできない場合、関連製品のサポートケースを開きます。

接続、コンテンツのダウンロード、またはコンテンツのインポートがまったくできないといったLNC固有の問題が発生した場合、HPE Live Networkコネクターのサポートケースを開きます。問題の内容と手順6の情報を添付してください。

## 接続の問題

LNCで接続エラーが発生する場合、ネットワーク管理者に相談し、ファイアウォール/プロキシのアクセス権や必須設定を確認します。また、各HPELNホストに対してping/digを実行します。さらに、traceroute、wget、curlなどのさまざまなコマンドライントラブルシューティングツールを使用して、IPが正しく解決されるかどうかや、LNC外部の環境からホストにアクセスできるかどうかを確認します。

## コマンドオプション、コマンドラインオプション、コンテンツのインポート、ログファイル

この項では、LNCのコマンドとコマンドラインオプション、コンテンツのインポート、LNCログファイルについて説明します。

## コマンドオプション

利用可能なコマンド、オプション、オンラインヘルプのリストをすべて表示するには、次の手順を実行します。

1. コマンドプロンプトを開きます。
2. 次のコマンドを実行します。

```
live-network-connector --help
```

LNCを起動するときにコマンドラインで呼び出すことができる利用可能なモードの一部を示します。

- **download**: ローカルにインストールされたLNCで構成されたサービスとストリームのコンテンツをダウンロードします。

注: 指定された製品のコア更新 (ある場合) もダウンロードされ、インポートされます。

- **download-import**: デフォルトのコマンドモード。コマンドを指定せずにLNCを実行すると、この操作モードで実行されます。ローカルにインストールされたLNCで構成されたサービスとストリームのコンテンツをダウンロードし、そのコンテンツをインポートします。

**注:** 指定された製品のコア更新 (ある場合) もダウンロードされ、インポートされます。

- **import:** downloadコマンドを使用して事前にダウンロードしたコンテンツをインポートします。

**注:** 指定された製品のコア更新 (ある場合) もインポートされます。

- **encrypt-passwords:** 構成ファイルでプレーンテキストで入力されたパスワードを暗号化します。
- **list-streams:** 利用可能なサービスとストリームを表示します。--format=xmlオプションを使用して、XML形式で出力することもできます。

**注:** 指定された製品のコア更新 (ある場合) もダウンロードされ、インポートされます。

- **list-products:** 利用可能な製品を表示します。デフォルト出力はテキスト形式ですが、--format=xmlオプションを付加することで、XML出力に切り替えることができます。
- **list-locales:** 指定された製品とストリームで利用可能なコンテンツロケールを表示します。製品バージョンが検出不能な場合は、利用可能なすべてのコンテンツロケールが表示されます。

オプション:

--product-version=<値>: 指定された製品バージョンに基づいてロケールをフィルター処理します。

--all-versions: バージョンによるフィルター処理は行われません。

デフォルト出力はテキスト形式ですが、--format=xmlオプションを付加すると、XML出力に切り替えることができます。

例:

```
live-network-connector list-locales --product=hpca --stream=security.hpca_nvd
Product Stream Locales
=====
hpca security.hpca_nvd en_US
```

- **list-status:** コンテンツの最新ステータスを表示します。インポート履歴を表示するには、--historyパラメーターを追加します。例:

```
live-network-connector list-status --product=sas --stream=content.software_
discovery
```

次のような情報が表示されます。

```
Name Product Stream Version Date Status
```

```
=====
=====
dssm sas content.software_discovery 37.0.0.0.29.0 2011-09-06 16:36:37 success
```

- **export:** HPE Live Networkからダウンロードしたコンテンツをエクスポートします。

注: 指定された製品のコア更新 (ある場合) もインポートされます。

- **download-export:** HPE Live Networkからコンテンツをダウンロードし、エクスポートします。

注: 指定された製品のコア更新 (ある場合) もダウンロードされ、インポートされます。

- **read-config:** LNC構成ファイルの構成属性の値を表示します。たとえば、LNC構成ファイルのusernameの値を表示するには、次のコマンドを実行します。

```
live-network-connector read-config --username
```

- **write-config:** LNC構成ファイルの構成属性の値を設定します。たとえば、LNC構成ファイルのusernameの値を特定のユーザーに設定し、パスワードを暗号化するには、次のコマンドを実行します。

```
live-network-connector write-config --username=<ユーザー>
--password=<パスワード>
```

この方法でユーザー名とパスワードを設定するときには、encrypt-passwordsコマンドの使用は不要です。

注: LNC構成ファイルの手動編集はサポートされていません。手動編集を行うと、ファイルが破損したり、設定が失われたりするおそれがあります。代わりに、ここに記した**write-config**コマンドを使用してください。

- **describe:** 利用可能なストリーム、それらの状態 (有効/無効)、関連する説明やURL、利用可能なタグのうち、入手可能な情報を表示します。

その他のオプション:

--content-object=<コンテンツオブジェクト名>を指定すると、構成された製品やストリームの<コンテンツオブジェクト名>の詳細も表示されます。

--content-object=allを指定すると、構成された製品やストリームのすべてのコンテンツオブジェクトの詳細も表示されます。

--stream=allを指定すると、write-configでどのストリームが構成されたかに関係なく、構成された製品で利用可能なすべてのストリームが表示されます。

--extendedを指定すると、ストリームの拡張データも表示されます。--content-object=<コンテンツオブジェクト名>または--content-object=allを追加すると、構成されたコンテンツオブジェクトの拡張データも表示されます。

--announcementオプションを使用するとお知らせが、--release-notesオプションを使用するとリリースノートが表示されます。これらのオプションは、--contentobjectオプションを指定した場合にのみ機能します。

**注:** 指定された製品のコア更新 (ある場合) もダウンロードされ、インポートされます。

- **search:** 指定されたテキストをストリームのタグ名、説明、URL、さらにサービス名、製品名の中から検索し、結果を表示します。ストリームタグのみを検索するには、--tagオプションを使用します。

## コマンドラインオプション

次のコマンドを実行すると、特定のコマンドで利用可能なコマンドラインオプションが表示されます。

```
live-network-connector command --help
```

オプション	機能	該当するコマンド
--http-proxy、--http-proxy-user、--http-proxy-pass	httpのプロキシ設定を構成します。	download、download-import、download-export
--export-to-directory	特定のディレクトリにコンテンツをエクスポートします。	download-export、export
--import-from-directory	特定のディレクトリからコンテンツをインポートします。	import
--product	操作対象のコンテンツを特定の製品に限定します。たとえば、--product=sasは、対象をSA関連のコンテンツに限定します。	download、download-export、export、download-import、import、list-streams、list-status、list-locales、describe、search
--stream	操作対象のコンテンツを特定のストリーム(複数可)に限定します。このオプションの値が“all”の場合、構成された製品に存在する全サービスの全ストリームが対象になります。 <b>注:</b> write-configでこのオプションを使用すると、構成さ	download、download-export、export、download-import、import、list-products、list-



オプション	機能	該当するコマンド
	<p>れた製品のストリームのうち、前回の接続コマンド (download、download-importなど) の実行以降認識されたストリームがすべて有効になります。</p>	status、list-locales、describe、search、write-config
--platform	<p>コンテンツを使用する、エアギャップ環境内の隔離システムのプラットフォームを指定します。例: linux2、sunos5、win32</p>	download-export、export
--status-file	<p>エアギャップ環境内の隔離システムのステータスファイルを示します。通常はInc/etc/imports.jsです。このファイルを接続先ノードに転送し、このファイルを使用して必要なファイルのみをdownload-export (またはexport) します。</p>	download-export、export
--product-version	<p>製品コアのバージョンを指定します。たとえば、エアギャップ環境では、LNcはコアの製品バージョンを検出することはできません。コアの製品バージョンは、--product-flagsを指定した場合の製品順序と同じ順序で処理されます。</p>	download-export、export
--locale	<p>コンテンツのロケールを指定します。値を指定しない場合、デフォルト値はen_USです。"all" に設定すると、ロケールによるコンテンツのフィルター処理は行われません。</p> <p>ロケールが変更された場合は、インポート済みのコンテンツに--reloadを実行してください。</p> <p>ローカライズされたコンテンツが利用可能かどうかは、製品とコンテンツのドキュメントを参照してください。</p>	download、download-import、import、download-export、export
--secondary-product --secondary-version	<ul style="list-style-type: none"> <li>製品または製品のリスト (カンマ区切り) を指定します。</li> <li>バージョンまたはバージョンのリスト (カンマ区切り) を指定します。</li> </ul> <p>この2つのオプションは、同時に設定する必要があり、しかも同じ項目数であることが必要です。コンテンツにセカンダリの製品とバージョンを設定すると、プライマリの製品バージョンの検証に合格し、セカンダリの製品バージョンの検証にも合格した場合に、このコンテンツの使用 (ダウンロード、インポート、エクスポート) が許可されます。コンテンツそのものは、プライマリ製品でのみ使用されます。</p>	write-config、download、download-import、import、download-export、export
--release-notes	<p>構成された製品とストリームに含まれる構成済みコンテンツオブジェクトのリリースノートを表示します。</p>	describe
--announcement	<p>構成された製品とストリームに含まれる構成済みコンテンツオブジェクトに関するお知らせを表示します。</p>	describe

## コンテンツのプレビュー (--preview)

--previewオプションを指定すると、コンテンツのダウンロード、ダウンロードとインポート、インポート、ダウンロードとエクスポート、またはエクスポートを開始する前に、要求したストリームの新しいコンテンツをすべて示すプレビューを生成することができます。download、download-import、import、download-export、exportの各コマンドとともに--previewオプションを使用すると、ダウンロードとインポート、インポート、ダウンロードとエクスポート、またはエクスポートが開始される前に、利用可能なすべての新しいコンテンツに関するレポートが出力されます。

たとえば、1つ以上のコンテンツストリームへのサブスクリプションがあり、新しいコンテンツのダウンロードかつインポートの前に新しい更新をプレビューする場合、次のように引数を入力します。

```
live-network-connector download-import --preview
```

このコマンドは、現在サブスクリプションのある全ストリームのコンテンツのうち、LNcキャッシュと配布サーバーのどちらかに存在し、まだダウンロードまたはインポートされていない新しいコンテンツ更新のレポートを出力します。

サブスクリプションに新しいコンテンツがない場合、プレビューレポートにコンテンツオブジェクトは列挙されません。

デフォルトでは、レポートはSTDOUTにプレーンテキスト形式で出力されますが、プレビューレポートをXML形式で出力する場合は、--format=xmlオプションを使用してXML出力を要求します。

例:

```
live-network-connector download-import --preview --format=xml
```

### --previewで利用可能なオプション

- **download --preview:** このレポートは、現在サブスクリプションのある全ストリームのコンテンツオブジェクトのうち、まだダウンロードされていないコンテンツオブジェクトをすべて列挙します。対象となるコンテンツオブジェクトは、現在配布サーバーに公開されているセットに限られます。
- **download --preview --allow-update:** このレポートは、download --previewレポートと似ていますが、LNcと構成済み製品プロファイルの更新も行います。実際のコンテンツの捕捉は行いません。捕捉されるプロファイルデータは、LNcで構成されている製品に基づきます。
- **import --preview:** このレポートは、現在サブスクリプションのある全ストリームのコンテンツオブジェクトのうち、LNcキャッシュ内にあり、まだインポートされていないコンテンツオブジェクトをすべて列挙します。対象となるコンテンツオブジェクトは、現在LNcキャッシュ内にあるセットに限られます。具体的に言えば、配布サーバーは考慮されません。

- **import --preview --allow-update:** このレポートは、import --previewレポートと似ていますが、LNcと構成済み製品プロファイルの更新も行います。実際のコンテンツの捕捉は行われません。捕捉されるプロファイルデータは、LNcで構成されている製品に基づきます。
- **download-import --preview:** このレポートは、現在サブスクリプションのある全ストリームのコンテンツオブジェクトのうち、配布サーバーからまだダウンロードされていないコンテンツオブジェクトと、LNcキャッシュからまだインポートされていないコンテンツオブジェクトの最新バージョンをすべて列挙します。対象となるコンテンツオブジェクトは、現在配布サーバーに公開されているセットと、現在LNcキャッシュ内にあるコンテンツオブジェクトのセットの両方です。
- **download-import --preview --allow-update:** このレポートは、download-import --previewレポートと似ていますが、LNcと構成済み製品プロファイルの更新も行います。実際のコンテンツの捕捉は行われません。捕捉されるプロファイルデータは、LNcで構成されている製品に基づきます。
- **download-export --preview:** このレポートは、現在サブスクリプションのある全ストリームのコンテンツのうち、配布サーバーまたはLNcキャッシュ内にあり、現在の構成に適しているエクスポート可能な最新コンテンツを列挙します。対象となるコンテンツオブジェクトは、現在配布サーバーに公開されているセットと、現在LNcキャッシュ内にあるコンテンツオブジェクトのセットの両方です。
- **download-export --preview --allow-update:** このレポートは、download-export --previewレポートと似ていますが、LNcと構成済み製品プロファイルの更新も行います。実際のコンテンツのエクスポートは行われません。捕捉されるプロファイルデータは、LNcで構成されている製品に基づきます。
- **export --preview:** このレポートは、現在サブスクリプションのある全ストリームのコンテンツオブジェクトのうち、LNcキャッシュ内にあり、エクスポート可能なコンテンツオブジェクトをすべて列挙します。対象となるコンテンツオブジェクトは、現在LNcキャッシュ内にあるセットに限られます。具体的に言えば、配布サーバーは考慮されません。通常、このオプションは、エアギャップ環境にコンテンツをエクスポートするために使用します。
- **export --preview --allow-update:** このレポートは、export --previewレポートと似ていますが、ダウンロード済みのデータを使用してLNcと構成済み製品プロファイルの更新も行います。実際のコンテンツのエクスポートは行われません。捕捉されるプロファイルデータは、LNcで構成されている製品に基づきます。
- **--tags:** このレポートは、コンテンツオブジェクトレベルで定義されている検索タグを列挙します。
- **--release-notes:** このレポートは、構成された製品およびストリームの各コンテンツオブジェクトで利用可能なリリースノートを列挙します。
- **--announcement:** このレポートは、構成された製品およびストリームの各コンテンツオブジェクトに関連するお知らせを列挙します。

## コンテンツのインポート

コンテンツがダウンロードされたかどうかを検証できるように、LNcはダウンロードされたファイルのSHA256チェックサムを計算し、ストリーム内にある同ファイルのSHA256チェックサムと結果を比較します。LNcはキャッシュ内にファイルを保持します。

LNcは、インポートコマンドから返されたステータスをチェックして、インポートが成功したかどうかを確認します。インポートが成功した場合、LNcはそのファイルにインポート済みのマークを付け、情報をキャッシュに書き込みます。コンテンツが無事にインポートされたかどうかは、ログファイルでチェックしてください。

## Live Networkコネクターのログファイル

LNcは、インポートコマンドから返されたステータスをチェックして、インポートが成功したかどうかを確認します。インポートが成功した場合、LNcはそのファイルにインポート済みのマークを付け、情報をキャッシュに書き込みます。コンテンツが無事にインポートされたかどうかは、ログファイルでチェックしてください。

<インストールディレクトリ>/lnc/log/live-network-connector.log

このデフォルトパスを変更するには、write-configコマンドを使用して、logfile\_pathの値を必要なパスとファイル名に設定します。

## 標準コンテンツストリーム

HPE Live Networkで現在利用可能なストリームの名前と説明を次の表に示します。

**注:** この項の各表は、現在利用可能なストリームの一部にすぎません。

この表のストリームをアクティブにするには、指定されたサーバーでLNcの構成ファイルを変更します。

名前	説明
ms_patch_supp	Microsoft Patch Supplement
platform_linux	管理対象プラットフォームコンテンツ - Linux用プラットフォームインストーラー
platform_unix	管理対象プラットフォームコンテンツ - Unix用プラットフォームインストーラー
platform_vmware	管理対象プラットフォームコンテンツ - VMware用プラットフォームインストーラー

名前	説明
platform_windows	管理対象プラットフォームコンテンツ - Windows用プラットフォームインストーラー
software_discovery	ソフトウェア検出サーバーモジュールコンテンツ
solaris_patching	Solarisパッチコンテンツ
security_scanner	運用上のセキュリティ評価を行うサーバーモジュール。システムをスキャンして既知の脆弱性を検出します。
sa_dma	DMAワークフローを実行するときに管理対象サーバーでDMAクライアントを呼び出すプログラムAPXコンテンツ
sa_se_connector	Storage Essentialsコネクタ
os_provisioning	OSプロビジョニングコンテンツ

## SA脆弱性コンテンツストリーム

SA脆弱性ストリームには、CVE (Common Vulnerabilities and Exposures) データとOVAL (Open Vulnerability and Assessment Language) データに基づいてプラットフォームの脆弱性を検査する、監査と修復 (A&R) ポリシーが含まれています。

名前	説明
vc_aix43	SA用脆弱性コンテンツ、AIX 4.3版
vc_aix51	SA用脆弱性コンテンツ、AIX 5.1版
vc_aix52	SA用脆弱性コンテンツ、AIX 5.2版
vc_aix53	SA用脆弱性コンテンツ、AIX 5.3版
vc_aix61	SA用脆弱性コンテンツ、AIX 6.1版
vc_aix71	SA用脆弱性コンテンツ、AIX 7.1版
vc_centos5	SA用脆弱性コンテンツ、Centos 5版
vc_centos6	SA用脆弱性コンテンツ、Centos 6版
vc_centos7	SA用脆弱性コンテンツ、Centos 7版
vc_oel5	SA用脆弱性コンテンツ、OEL 5版
vc_oel6	SA用脆弱性コンテンツ、OEL 6版
vc_oel7	SA用脆弱性コンテンツ、OEL 7版

名前	説明
vc_esx3	SA用脆弱性コンテンツ、VMware ESX 3.0版
vc_esx35	SA用脆弱性コンテンツ、VMware ESX 3.5版
vc_esx4	SA用脆弱性コンテンツ、VMware ESX 4.0版
vc_esx41	SA用脆弱性コンテンツ、VMware ESX 4.1版
vc_winxp	SA用脆弱性コンテンツ、Windows XP版
vc_win2k	SA用脆弱性コンテンツ、Windows 2000版
vc_win2k3	SA用脆弱性コンテンツ、Windows 2003版
vc_win2k8	SA用脆弱性コンテンツ、Windows 2008版
vc_win2k8r2	SA用脆弱性コンテンツ、Windows 2008 R2版
vc_win2k12	SA用脆弱性コンテンツ、Windows 2012版
vc_win2k12r2	SA用脆弱性コンテンツ、Windows 2012 R2版
vc_sol7	SA用脆弱性コンテンツ、Solaris 7版
vc_sol8	SA用脆弱性コンテンツ、Solaris 8版
vc_sol9	SA用脆弱性コンテンツ、Solaris 9版
vc_sol10	SA用脆弱性コンテンツ、Solaris 10版
vc_hpux10	SA用脆弱性コンテンツ、HP-UX 10版
vc_hpux11	SA用脆弱性コンテンツ、HP-UX 11版
vc_rhel3	SA用脆弱性コンテンツ、RHEL3版
vc_rhel4	SA用脆弱性コンテンツ、RHEL4版
vc_rhel5	SA用脆弱性コンテンツ、RHEL5版
vc_rhel6	SA用脆弱性コンテンツ、RHEL6版
vc_rhel7	SA用脆弱性コンテンツ、RHEL7版
vc_suse10	SA用脆弱性コンテンツ、SuSE Linux 10版
vc_suse11	SA用脆弱性コンテンツ、SuSE Linux 11版
vc_suse12	SA用脆弱性コンテンツ、SuSE Linux 12版
vc_ubuntu	SA用脆弱性コンテンツ、Ubuntu版

## コンプライアンスコンテンツストリーム

次の表に、利用可能なコンプライアンスコンテンツストリームを示します。

名前	説明
<b>必須項目</b>	<b>追加ポリシーをインストールするための前提となるコンテンツ</b>
cc_library	監査と修復 (A&R) の構成可能なコンプライアンスポリシー、Windows およびUnix用
<b>監査と修復の動的ポリシー</b>	<b>カスタマイズ可能でアクティブにサポートされる動的ポリシー</b>
cc_pci_windows	SA用動的A&R PCIポリシー、Windows版
cc_pci_unix	SA用動的A&R PCIポリシー、UNIX版
ec_cis_aix	SA用動的A&R CISポリシー、AIX版
ec_cis_esx	SA用動的A&R CISポリシー、ESX版
ec_cis_hpux	SA用動的A&R CISポリシー、HP-UX版
ec_cis_rhel	SA用動的A&R CISポリシー、RHEL版
ec_cis_solaris	SA用動的A&R CISポリシー、Solaris版
ec_cis_suse	SA用動的A&R CISポリシー、SUSE版
ec_cis_windows	SA用動的A&R CISおよびMSポリシー、Windows版
ec_disa_stig	SA用動的A&R DISAポリシー、UNIXおよびWindows版
<b>基本的な監査と修復のポリシー</b>	<b>カスタマイズ不可能なポリシー</b>
cc_fisma_windows	SA用A&R FISMAポリシー、Windows版
cc_fisma_unix	SA用A&R FISMAポリシー、UNIX版
cc_hipaa_windows	SA用A&R HIPAAポリシー、Windows版
cc_hipaa_unix	SA用A&R HIPAAポリシー、UNIX版
cc_sox_windows	SA用A&R SOXポリシー、Windows版
cc_sox_unix	SA用A&R SOXポリシー、UNIX版
cc_cis_ubuntu	SA用A&R CISポリシー、Ubuntu版
cc_cis_centos	SA用A&R CISポリシー、Centos版

名前	説明
cc_cis_oel	SA用 A&R CISポリシー、OEL版
cc_iso_windows	SA用 A&R ISOポリシー、Windows版
cc_iso_unix	SA用 A&R ISOポリシー、UNIX版



## DMAとの統合

本項では、HPE Database and Middleware Automation (DMA) のフローをHPE Server Automation (SA) とともに使用する方法について説明します。DMAは、そのサーバー管理ツールとしてSAを使用します。

### DMAの概要

DMAは、カスタムスクリプトや個々のアドホックツールでは対応しきれない状況に対処します。これは、コンプライアンス、ミドルウェアとデータベースのパッチ処理、ミドルウェアとデータベースのプロビジョニング、およびコードのリリースにかかわる課題に対処するための、業界標準のベストプラクティスと各分野の専門技術を提供します。ITチームは、DMAを使用することで、組織標準を社内全体に徹底できます。DMAは、複数のベンダーのデータベースおよびミドルウェアのテクノロジーをサポートしています。

### 統合タスク

DMAとSAの統合は、SSO (<https://softwaresupport.hpe.com/>) で入手可能な『HPE DMAインストールガイド』で説明されています。

『HPE DMAインストールガイド』の該当する項を参照して、次の作業を行ってください。

タスク	項
DMAのインストール - SAとの必要な統合をすべて含む	「How to Install HPE DMA」
DMAのアンインストール - SA管理対象サーバーからのDMAのアンインストールを含む	「How to Uninstall HPE DMA」
DMAの新バージョンへのアップグレード - SAコアへのDMA APXの再インストールを含む	「How to Upgrade HPE DMA」
現在のDMAバージョンをSAにリンク	「How to Link HPE DMA into HPE Server Automation」

## OBRとの統合

HPE Server Automation (SA) には、レポート作成のためにHPE Operations Bridge Reporter (OBR) が統合されています。レポートには、次の内容が含まれます。

1. SA監査コンプライアンス
2. SAパッチコンプライアンス
3. SAサーバーインベントリ

## HPE OBRの概要

Operations Bridge Reporter (OBR) は、HPE Server Automationのレポート作成ソリューションです。

データセンターの自動化アクティビティに関する詳細な分析が行われるため、SAを活用して日々 (最新) の履歴データに基づいた判断を行うことができます。分析対象データは、データセンターで自動化サービスと監視サービスを行うSAから収集されます。

HPE OBRを使用すると、次の機能を実行できます。

- 独自のコンテンツパックの作成。HPE OBRには、
- コンテンツパックの新規作成と既存のコンテンツパックのカスタマイズを行えるコンテンツ開発環境 (CDE) が用意されています。
- 製品提供の標準コンテンツパックのカスタマイズと拡張
- レポート用の独自のグループの作成。たとえば、ビジネス管理チェーンやビジネス機能に基づいてグループを作成することができます。

OBRには、次のソフトウェアコンポーネントがあります。

- SAP BusinessObjects。レポート作成に使用します。
- HP Verticaデータベース。パフォーマンスデータの格納、処理、管理に使用します。

## OBRとの統合

次のワークフローでは、レポート生成のためにOBRを構成し、SAに統合するまでの流れを示します。

タスク	詳細	リソース
<p style="text-align: center;">計画</p>	<ul style="list-style-type: none"> <li>• 計画については、HPE OBRのドキュメントを参照してください。</li> <li>• 次のHPE OBRコアコンポーネントをダウンロードします。 <ul style="list-style-type: none"> <li>◦ HPE OBR</li> <li>◦ Vertica</li> <li>◦ Verticaのライセンス</li> <li>◦ SAP BusinessObjects Enterprise (BOE)</li> <li>◦ HPELNからHPE Server Automation監査コンプライアンスコンテンツパックをダウンロードします。</li> </ul> </li> </ul>	<p>HPELNでHPE OBRのドキュメントを見つけ、<b>[Document Type]</b> から <b>[manuals]</b> に移動します。</p>
<p style="text-align: center;">OBRコアのインストール</p>	<ol style="list-style-type: none"> <li>1. HPE OBRコアをインストールします。</li> <li>2. Verticaをインストールし、Verticaのライセンスを適用します。</li> <li>3. データウェアハウスをセットアップします。</li> <li>4. SAP BOEをインストールします。</li> </ol>	<p>HPELNでHPE OBRのドキュメントを見つけ、<b>[Document Type]</b> から <b>[manuals]</b> に移動します。</p>
<p style="text-align: center;">コンテンツパックのインストール</p>	<p>HPE OBR-SAレポートコンテンツパックをインストールします。</p>	<p>HPELNからコンテンツパックを取得します。</p>
<p style="text-align: center;">OBRのデータソースとしてSAを構成</p>	<p>OBRのデータソースとしてHPE SAを構成します。</p>	<p>詳細については、HPELNの『HPE OBR-SA Reports Content Pack Configuration Guide』を参照してください。HPELNで、<b>[Resource]</b> &gt; <b>[File Repository]</b> &gt; <b>[Documentation]</b> に移動します。</p>

タスク	詳細	リソース
		詳細については、 <a href="#">HPELN</a> の『HPE OBR-SA Reports Content Pack Configuration Guide』を参照してください。HPELNで、 <a href="#">[Resource]</a> > <a href="#">[File Repository]</a> > <a href="#">[Documentation]</a> に移動します。
		詳細については、 <a href="#">HPELN</a> の『レポートガイド』を参照してください。HPELNで、 <a href="#">[Resource]</a> > <a href="#">[File Repository]</a> > <a href="#">[Documentation]</a> に移動します。

# ドキュメントのフィードバックを送信

本ドキュメントについてのご意見、ご感想については、電子メールでドキュメント制作チームまでご連絡ください。このシステムに電子メールクライアントが設定されている場合は、上記のリンクをクリックすると、次の情報が件名行に記載された電子メールウィンドウが開きます。

**フィードバック: 統合ガイド (Server Automation 10.50)**

フィードバックを追加して [送信] をクリックしてください。

電子メールクライアントが使用できない場合は、Webメールクライアントのメッセージに上記の情報をコピーし、hpe\_sa\_docs@hpe.com までフィードバックをお送りください。

ご協力をお願いいたします。