HP Server Automation

Enterprise Edition

ソフトウェアバージョン: 10.0

統合ガイド

ドキュメントリリース日: 2013年6月13日 (英語版)

ソフトウェアリリース日: 2013年6月

invent

ご注意

保証

HP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。ここでの記載で追加保証を意図するものは一切ありません。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、HP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、HP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、FAR12.211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

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。

Intel®およびItanium®は、Intel Coporationの米国およびその他の国における登録商標です。

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

OracleとJavaは、Oracle Corporationおよびその関連会社の登録商標です。

UNIX®は、The Open Groupの登録商標です。

サポート

次のHPソフトウェアサポートオンラインのWebサイトを参照してください。

http://support.openview.hp.com

このサイトでは、HP のお客様窓口のほか、HP 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。

HP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。HP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
- ソフトウェアパッチのダウンロード
- サポート契約の管理
- HP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、HP 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。HP Passport IDを登録するには、次のWebサイトにアクセスしてください。

http://h20229.www2.hp.com/passport-registration.html (英語サイト)

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。

http://support.openview.hp.com/access_level.jsp

サポートマトリックス

サポートおよび互換性情報については、関連する製品リリースのサポートマトリックスを参照してください。サポートマトリックスと製品マニュアルは、次のHPソフトウェアサポートオンラインのWebサイトで参照できます。

http://h20230.www2.hp.com/sc/support_matrices.jsp

また、本リリースの『HP Server Automation Support and Compatibility Matrix』は、次のHPソフトウェアサポートオンラインの製品マニュアルWebサイトからダウンロードできます。

http://support.openview.hp.com/selfsolve/manuals

ドキュメントの更新情報

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。

http://support.openview.hp.com/selfsolve/manuals

このサイトを利用するには、HP Passportへの登録とサインインが必要です。HP Passport IDの登録は、HP Passportのサインインページの [**New users - please register**] リンク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、更新版または最新版をご入手いただけます。詳細は、HPの営業担当にお問い合わせください。改訂状況については、「ドキュメントの更新情報」を参照してください。

製品エディション

HP Server Automationには、次の2つの製品エディションがあります。

- HP Server Automation (SA) は、Server AutomationのEnterprise Editionです。Server Automationについては、『SA Release Notes』および『SAユーザーガイド: Server Automation』を参照してください。
- HP Server Automation Virtual Appliance (SAVA) は、Server AutomationのStandard Editionです。SAVAの機能については、『SAVA Release Notes』および『SAVAクイックガイド』を参照してください。

ドキュメント変更に関する注

次の表は、前回のリリース後にこのドキュメントに加えられた変更を示します。

日付	変更内容
2012年8月	SA 10.0におけるこのドキュメントの最初のリリース

目次

第 1 章　SA-DMA統合

この章では、HP Database and Middleware Automation (DMA) のフローをHP Server Automationのアプリケーションデプロイメントマネージャーとともに使用する方法について説明します。

この章の手順を実行するには、DMA のフロー、DMA のインタフェース、およびアプリケーションデプロイメントマネージャーのインタフェースに関する知識が必要です。

この章のトピックは、次のとおりです。

DMAフローまたはアプリケーションデプロイメントマネージャーの詳細については、『Database and Middleware Automation User Guide』および『Application Deployment Manager User Guide』を参照してください。

DMAフローを実行するための前提条件

この項では、DMAフローの実行に必要な主要手順について説明します。

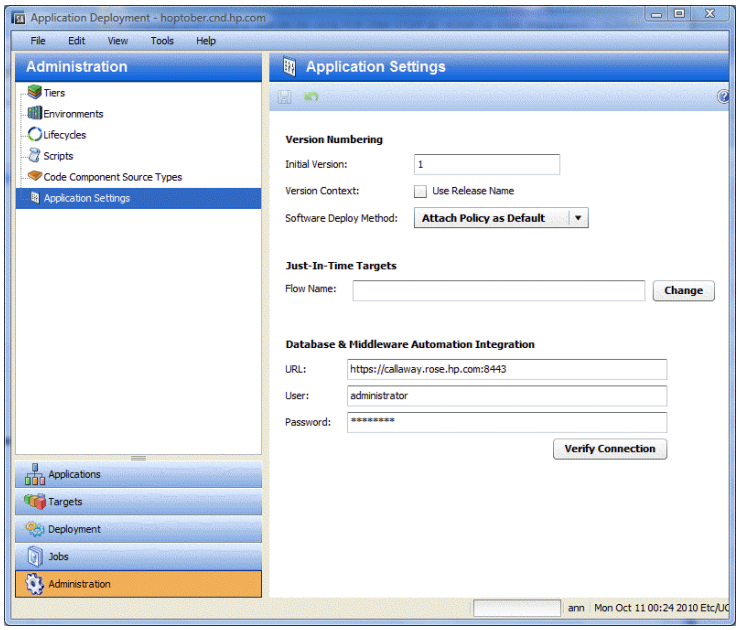
- DMA サーバーをインストールし構成する。このプロセスの手順は、『DMA Installation Guide』に記載されています。
- DMA と通信できるようにアプリケーションデプロイメントマネージャーを構成する。DMA への接続 (9 ページ) および『Application Deployment Manager User Guide』の「Application Settings」の項を参照してください。
- DMAフローが実行される管理対象サーバーにDMAエージェントをインストールする。『DMA Installation Guide』を参照してください。
- DMAワークフローまたはデプロイメントを含むアプリケーションを作成する。9.02の『Application Deployment Manager User Guide』の「Creating DMA Flow Components」を参照してください。
- アプリケーションデプロイメントマネージャーを使用して、アプリケーションをデプロイする。『Application Deployment Manager User Guide』を参照してください。

DMAへの接続

DMAとアプリケーションデプロイメントマネージャーとの間の接続を作成するには、次の手順を実行します。

1. アプリケーションデプロイメントマネージャー管理者として、SA内からアプリケーションデプロイメントマネージャーを開きます ([ツール] > [アプリケーションデプロイメント] を選択します)。
2. アプリケーションデプロイメントマネージャーで、[Administration] タブを選択します。
3. [Application Settings] を選択します。

図 1　　[Application Settings] セクション



4　[Application Settings] セクションに次の情報を入力します。

- URL: DMAがインストールされているサーバーのURL。
- User name: DMAの管理権限を持つユーザー名。
- Password: ユーザー名に対応するパスワード。

5　[**Verify Connection**] をクリックして、アプリケーションデプロイメントマネージャー /DMA の接続をテストします。

接続ステータスメッセージが表示されます。

DMAエージェントのインストール

DMAエージェントのインストールには、3つの主要な手順が関係します。

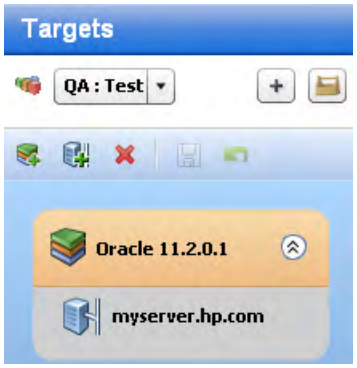
- エージェントのインストールが必要な管理対象サーバー候補を特定する (管理対象サーバー候補の特定 (11ページ) を参照)。
- DMAエージェントがシステムにインストールできることを確認し、エージェントのインストール手順を正しく実行する (システムへのDMAエージェントのインストール (11ページ) を参照)。
- DMAエージェントをアクティブ化する (DMAエージェントのアクティブ化 (13ページ) を参照)。

管理対象サーバー候補の特定

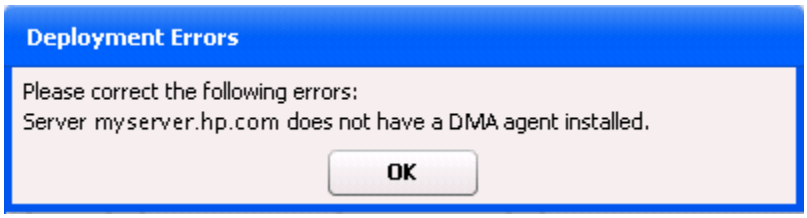
アプリケーションデプロイメントマネージャーのターゲットを使用して、どの管理対象サーバーにDMAエージェントをインストールすればよいかを決定できます。

DMAフローを実行するアプリケーションをターゲットにデプロイするには、ターゲットが参照するすべての管理対象サーバーにDMAエージェントがインストールされている必要があります。たとえば、次の図に示すように、アプリケーションをターゲットQA: Testにデプロイする場合に、そのターゲットが管理対象サーバーmyserver.hp.comを参照するのであれば、myserver.hp.comサーバーにDMAエージェントをインストールする必要があります。

図 2　　ターゲットサーバー



注: デプロイメント時に、参照される管理対象サーバーにDMAエージェントがインストールされていなければ、アプリケーションデプロイメントマネージャーは次の警告を発行します。



システムへのDMAエージェントのインストール

DMAエージェントは、次のプラットフォームでサポートされています。

表 1　　DMAエージェントをサポートするプラットフォーム

プラットフォーム	バージョン
AIX	5.1 pSeries 5.3 pSeries 6.1 pSeries
HP-UX	11.23 pa-risc 11.23 Itanium2 11.31 pa-risc 11.31 Itanium2
Linux - RedHat EL 4	i386、x86_64

表 1　　DMAエージェントをサポートするプラットフォーム (続き)

プラットフォーム	バージョン
Linux - RedHat EL 5	i386 x86_64
Solaris 9	Sparc
Solaris 10	Sparc x86
Windows 2003 Server	x86 x86_64
Windows 2008 Server	x86 x86_64

エージェントを各プラットフォームにインストールする方法の詳細については、『DMA Installation Guide』を参照してください。

DMAエージェントのアクティブ化

この項では、DMAエージェントをアクティブ化する方法について説明します。

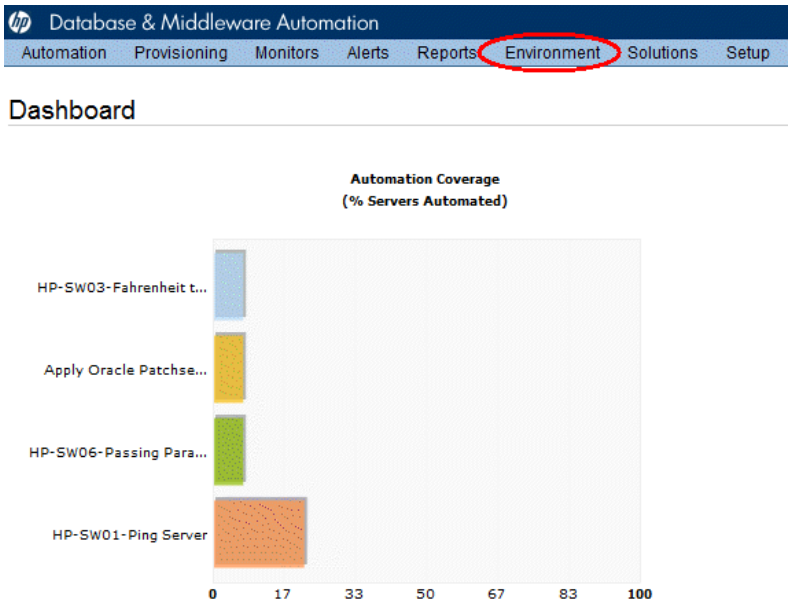
注: bulk エージェントを一括でアクティブ化する操作については、HPサポート担当者にお問い合わせください。

管理対象サーバー候補の特定 (11ページ) で選択した管理対象サーバーにDMAエージェントをインストールしたら、DMAインタフェースを使用してエージェントをアクティブ化する必要があります。

エージェントをアクティブ化するには、次の手順を実行します。

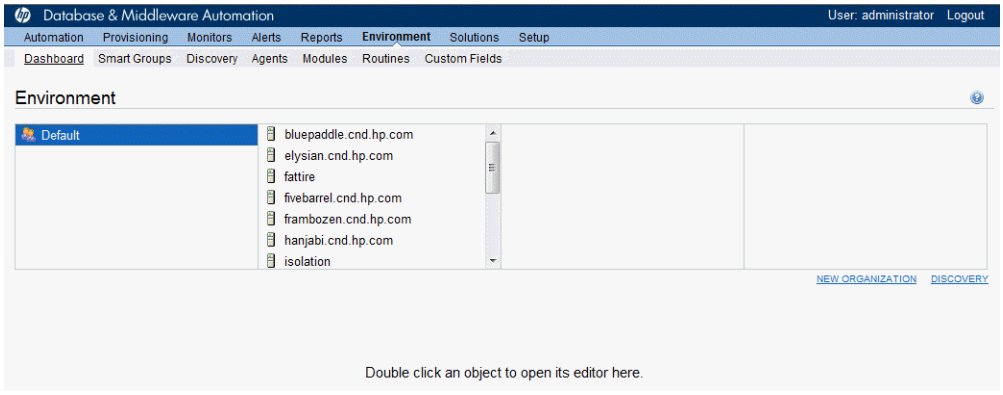
1 DMA Nerve Centerにログインします。

図 3 DMA Dashboard



2 ナビゲーションバーで [**Environment**] を選択します。

図 4 [Environment] タブ



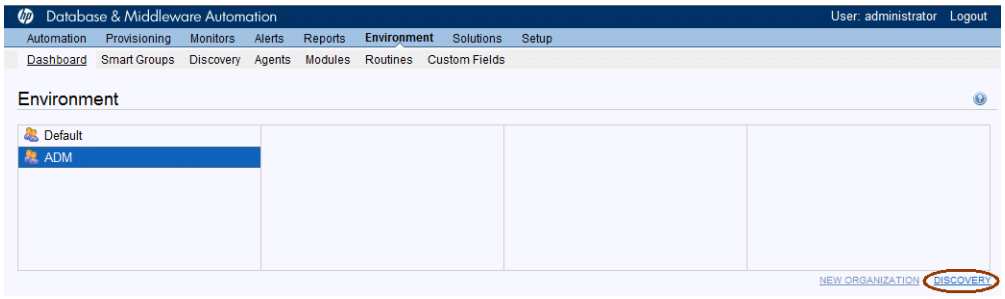
3 [Environment] ウィンドウの右側の [New Organization] をクリックして、新しいADM組織を作成します。

図 5　　新しい組織の作成

4　[New Organization] ウィンドウの [Name] フィールドに「ADM」と入力し、[**Save**] をクリックします。

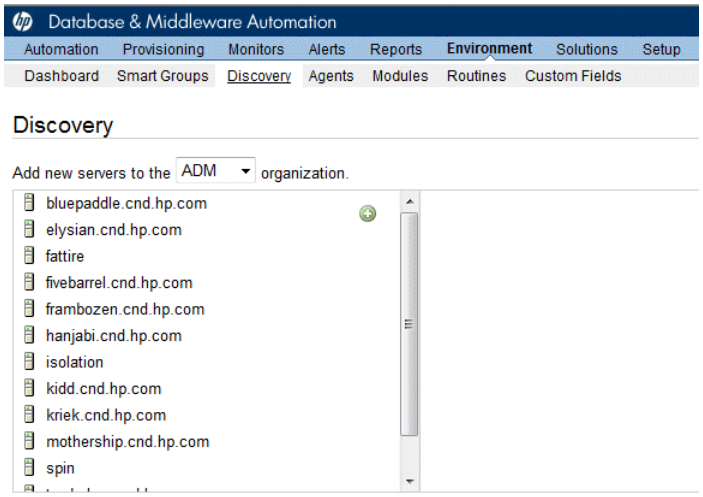
情報が正しく保存されると、「an Organization Saved Correctly」メッセージとADM環境アイコンが表示されます。

図 6　　ADM環境アイコン



5　[Environment] ウィンドウの左側の [**Discovery**] をクリックします。

図 7　　[Discovery] ウィンドウ



6　[Discovery] ウィンドウで、次の手順を実行します。

a　組織メニューから [ADM] を選択します。

b　新規サーバーリストからサーバーを選択します。

c　緑のプラスアイコン をクリックして、サーバーをADM組織に追加します。

7　[**Save**] をクリックします。

エージェントが必要な各管理対象サーバーに対して、この操作手順を繰り返します。

DMAエージェントのインストールのトラブルシューティング

Linuxインストール

RPMの依存コンポーネントを追加でインストールすることが必要な場合があります。

注: 以前のリリースのStratavia Data PaletteからDMA 1.0にアップグレードする場合は、既存のソリューションパックを削除し、同等なHP DMAソリューションパックをインストールし直すことが必要になります。

DMA構成のテスト

この章で説明した構成処理が完了したら、DMAフローをアプリケーションデプロイメントマネージャーで使用できるようになります。DMA 統合が正しく動作することを確認するには、DMA フローを使用するアプリケーションを作成し、アプリケーションデプロイメントマネージャーを使用してデプロイします。詳細については、『Application Deployment Manager User Guide』を参照してください。

第 2 章　SA/NA統合

SA/NA統合の概要

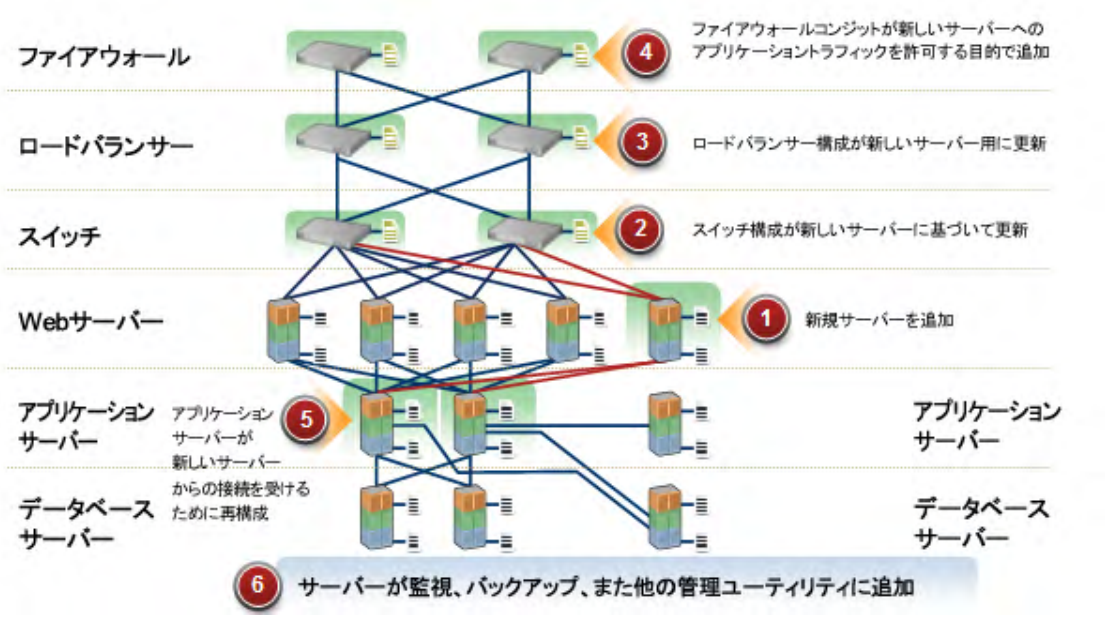
IT環境を変更するときは、往々にして、ネットワーク管理者、システム管理者、アプリケーション技術者が調整して作業することが必要になります。これは、管理しなければならないアプリケーション環境が、さまざまなオペレーティングシステムのサーバーやネットワークデバイスで構成されており、ファイアウォール、ロードバランサー、スイッチ、サーバー、Webアプリケーションなどが含まれることがあるためです。

たとえば、環境によっては、アプリケーションの直前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。

SA/NA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。

図8に、SA/NA統合で行うことができる調整タスクの一部を示します。

図 8　　SA/NA統合を使用した調整タスクの概要



この項では、NAとSAの統合を構成する方法を示しています。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、SA/NA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。

- HP Server Automation (SA)
- Network Automation (NA)
- SA Global Shell
- HP Service Automation Visualizer (SA内)
- HPReports (SA内)

SA/NA統合の機能

SA/NA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概略と詳細を表示する。
- 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。
- NAスクリプトを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 (および推定されるレイヤー 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。

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データの収集方法

SA/NA統合機能では、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。

NAトポロジデータの収集診断

NA ト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アドレスが必要なのは、物理接続を検出してSAデータモデルに追加するためです。

たとえば、サーバーをスイッチに追加すると、次回NAト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。NAト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、『NA ユーザガイド』を参照してください。

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 (31ページ) と『NAユーザガイド』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、SAによって認証が処理されます。詳細については、NA認証の構成 (23ページ) 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。

前提条件

次の前提条件を満たす必要があります。

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ことが必要です。

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にアクセスできることが必要です。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でリッスンします。

- **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) にアクセスできることが必要です。

- **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/NA統合の構成タスク

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、SA/NA統合を有効にする必要があります。

構成作業では、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、ユーザーアクセス件をいくつか構成します。

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 (26ページ) を参照してください。

jboss_wrapper.confファイルの編集

NA のバージョンが 7.6 より前の場合にのみ必要です。バージョン 7.6 以降の場合、次のエントリは jboss_wrapper.conf内にありません。

wrapper.java.additional.x (x>8は通し番号) の値を調整してください。

次に例を示します。

変更前:

```
wrapper.java.additional.1=-DTCMgmtEngine=1
wrapper.java.additional.2=-Duser.dir=/opt/NA750/server/ext/jboss/bin
wrapper.java.additional.3=-Xmn170m
wrapper.java.additional.4=-Djava.awt.headless=true
wrapper.java.additional.5=-Dfile.encoding=UTF8

#Following are added for bug 150387
wrapper.java.additional.6=-Dorg.omg.CORBA.ORBClass=com.sun.corba.se.internal.
Interceptors.PIORB
wrapper.java.additional.7=-Dorg.omg.CORBA.ORBSingletonClass=com.sun.corba.se.
internal.corba.ORBSingleton
wrapper.java.additional.8=-Xbootclasspath/p:/opt/NA750/server/ext/wrapper/
lib/CORBA_1.4.2_13.jar

#Add location of keystore.This is used to make SSL request.
wrapper.java.additional.9=-Djavax.net.ssl.trustStore=/opt/NA750/server/ext/
jboss/server/default/conf/truecontrol.keystore

# Bug 171948 - Need more PermGen
wrapper.java.additional.10=-XX:MaxPermSize=80m
```

変更後:

```
wrapper.java.additional.1=-DTCMgmtEngine=1
wrapper.java.additional.2=-Duser.dir=/opt/NA750/server/ext/jboss/bin
wrapper.java.additional.3=-Xmn170m
wrapper.java.additional.4=-Djava.awt.headless=true
wrapper.java.additional.5=-Dfile.encoding=UTF8

#Following are added for bug 150387
#wrapper.java.additional.6=-Dorg.omg.CORBA.ORBClass=com.sun.corba.se.internal.
Interceptors.PIORB
#wrapper.java.additional.7=-Dorg.omg.CORBA.ORBSingletonClass=com.sun.corba.se.
internal.corba.ORBSingleton
#wrapper.java.additional.8=-Xbootclasspath/p:/opt/NA750/server/ext/wrapper/
lib/CORBA_1.4.2_13.jar

#Add location of keystore.This is used to make SSL request.
wrapper.java.additional.6=-Djavax.net.ssl.trustStore=/opt/NA750/server/ext/
jboss/server/default/conf/truecontrol.keystore

# Bug 171948 - Need more PermGen
wrapper.java.additional.7=-XX:MaxPermSize=80m
```

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**

  SAコアインストーラーインタビューでNAサーバー名を指定しなかった場合は、`twist.nasdata.host=`**ホスト名**パラメーターの値を `/etc/opt/opsware/twist/twist.conf` ファイルで指定する必要があります。

  次のエントリを探します。

  ```
  twist.nasdata.host=
  ```

  NAサーバーのホスト名またはIPアドレスを追加してください。

  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がある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、こ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 管理ガイド』を参照してください。

統合用のNAの構成

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、『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、『NA Satellite Guide』を参照してください。

ユーザーのアクセス権

SA/NA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 管理ガイド』を参照してください。

NA認証の構成

SA/NA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 (図10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。

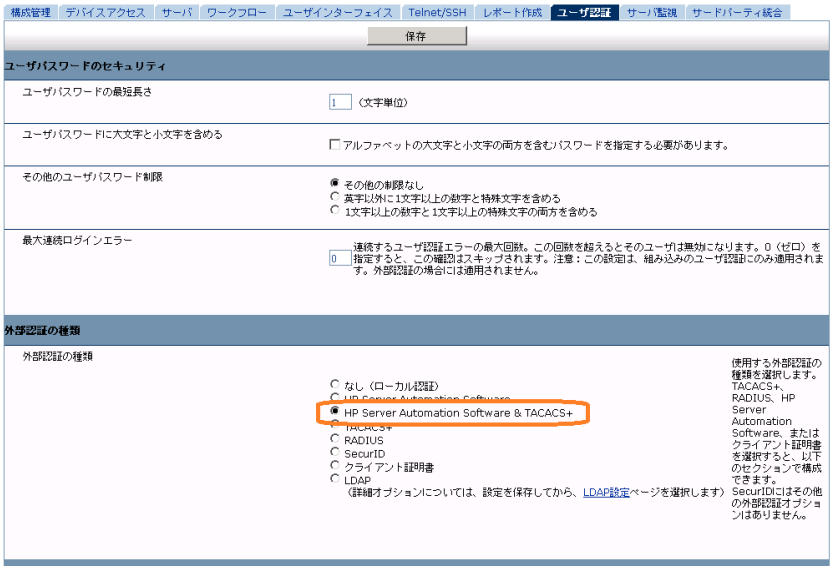
認証の設定をNAで変更するには、次のタスクを実行します。

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 図9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、HP Server Automationソフトウェアおよびを(使用されている場合) を選択します。

図 9 NAの外部認証タイプ



4 スクロールダウンして、図10に示すように、[HP Server Automationソフトウェア認証] 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。

図 10 HP Server Automationソフトウェア認証

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ユーザガイド』を参照してください。

CiscoWorks NCMがあるSA/NA統合の構成

SAをCiscoWorks NCM 1.2とともにデプロイする場合は、構成変更がいくつか必要です。CiscoWorks NCMの一部のデプロイメント(CiscoWorks LMSがNCMとともに存在する場合)では、SAとの統合に影響する非標準のポートが使用されます。

どのような変更が必要になるかを特定するには、次のタスクを実行します。

フェーズ1: tomcat4-service.xmlの編集:

1 NCMサーバーにログインします。

2 XMLファイルを開きます。

`NCM`**インストールディレクトリ**`/server/ext/jboss/server/default/deploy/tomcat4-service.xml`

3 文字列`'scheme=https'`を検索します。

4 直前のエントリを確認します。これは、次のようになっているはずです。

`port =` **"ポート番号"**

ポート番号の値が443であれば、フェーズ4に進みます。そうでない場合は、指定されているポートをメモしてフェーズ2に進みます。

フェーズ2: ポート番号の割り当て:

1 SAクライアントにログインします。

2 SAクライアントの [**ツール**] メニューから [**オプション**] を選択します。

3 [オプションの設定] ウィンドウで [**Network Automation**] を選択します。

4 [ホスト] フィールドで、ホスト名の後ろに**:ポート**を追加します。ここで、<**ポート**>はフェーズ1の**手順4**で確認したポート番号です。次に例を示します。

`mycore.opsware.com:443`

[保存] をクリックします。

< General.Host > は有効なホスト文字列である必要があります。という警告が表示されます。この警告は無視してください。[オプションの設定] ウィンドウを閉じます。

(フェーズ2は、SAクライアントのすべてのユーザーに対して実行する必要があります。)

フェーズ3: プライマリデータアクセスエンジンファイルの編集:

1 プライマリデータアクセスエンジン (インフラストラクチャーコンポーネントバンドルの一部) がインストールされているSAコアサーバーにログインします。

2 `/opt/opsware/twist/twist.sh`ファイルを開いて、次の行を変更します。

`https://$NASHOST/tcdocs/truecontrol-client.jar`

この行を次のように変更します(フェーズ1の**手順4**でメモしたポートは443だとします)。

`https://${NASHOST}:443/tcdocs/truecontrol-client.jar`

3 Webサービスデータアクセスエンジン(スライスコンポーネントバンドルの一部)をホストしているサーバーを再起動します。

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

(フェーズ3は、Webサービスデータアクセスエンジンサーバーのインストールごとに実行する必要があります。)

フェーズ4: SSHポートの割り当て:

1. NCMにログインします。
2. [**Admin**] > [**Administrative Settings**] > [**Telnet/SSH**] を選択して、[Administrative Settings - Telnet/SSH] ページを表示します。
3. [SSH Server] セクションで、SSHサーバーポートを探します。
4. ポートが8022であれば終了です。そうでない場合は、使用されているポートをメモして、フェーズ4の**手順5**に進みます。
5. Global File System (OGFS) (スライスコンポーネントバンドルの一部) がインストールされているSAコアサーバーにログインします。
6. `/etc/opt/opsware/hub/hub.conf`ファイルを開いて、`nas.port`の値をフェーズ4の**手順4**で見つけたポートに変更します。次に例を示します。

   ```
   nas.port=9022
   ```

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ユーザガイド』を参照してください。

トラブルシューティングのヒント

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。

SAクライアントでのNAホストのリセット

使用するSA/NA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 Standard/Advanced Installation Guide』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、ファイルウォールが原因で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、[HP 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。

SA/NA統合の使用

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/NA統合の機能は、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。OSIモデルのレイヤーの定義については、図11を参照してください。

図 11　OSI7階層モデル

データリンク接続

SA/NA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 (35ページ) 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

SA/NA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

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 (30ページ) 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。

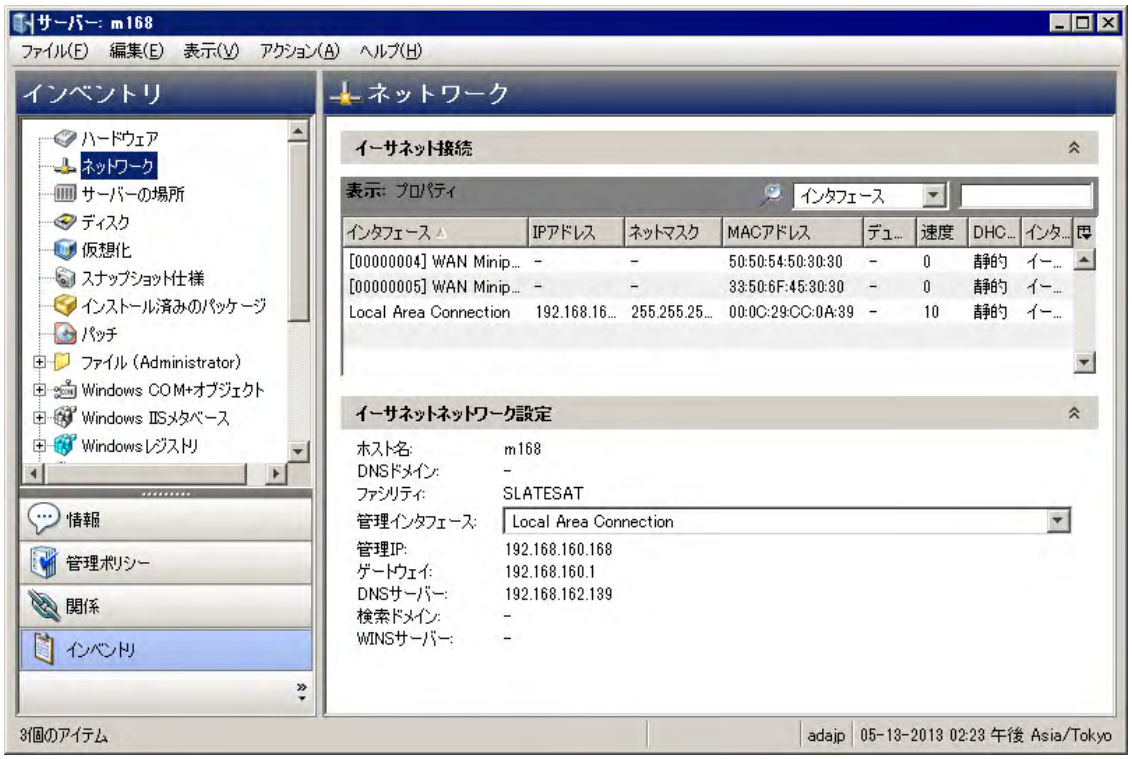
1 SAクライアントにログインします。

2 ナビゲーションペインから [**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で [ハードウェア] 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。図12を参照してください。

図 12　サーバーエクスプローラーのネットワークビュー



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。

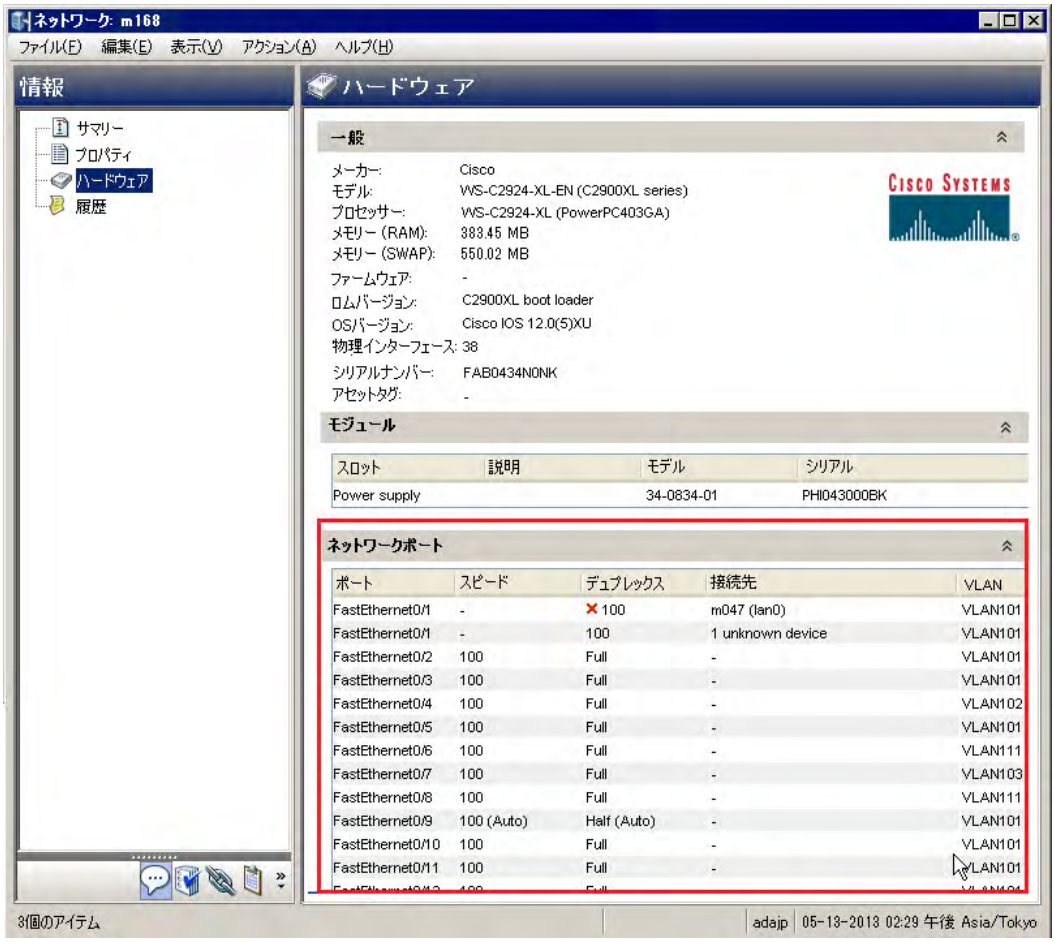
1 SAクライアントにログインします。

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。図13を参照してください。

図 13　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



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。SA/NA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

ネットワークデバイスの詳細情報を表示するには、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。

図 14　NAでのネットワークデバイスの詳細

イベント履歴の表示

[イベント詳細] 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。

図 15　NAでのネットワークデバイスのイベント詳細

デュプレックスの不一致

SA/NA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 (19ページ) 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。詳細については、『NAユーザガイド』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にあるとみなされます。

SA/NA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ユーザーガイド: 監査とコンプライアンス』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から [**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。図12を参照してください。

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 Reports 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。

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 レポートガイド』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 `.gif`、`.jpg`、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。

SAVおよびダイアグラムツールの詳細については、『SAユーザーガイド: Service Automation Visualizer (SAV)』および『NAユーザガイド』を参照してください。

HP Service Automation Visualizerの起動

SAV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から [**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 [**HP Service 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ユーザーガイド: Service Automation Visualizer (SAV)』でHP Service 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、『NAユーザガイド』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ユーザーガイド: Server Automation』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ユーザーガイド: Server Automation』の「Global Shellセッションを開く」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、『SAユーザーガイド: Server Automation』の「SA Global Shell」および「OGFSディレクトリ」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ユーザーガイド: Server Automation』の「リモートターミナル」および「roshによる管理対象サーバーへのログオン」を参照してください。

推定される物理接続

SA/NA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間に、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間にハブがある。

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、『NAユーザガイド』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

第 3 章　SA-OO統合 – フローの実行

この章では、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。

この章で説明する手順を実行するには、SA、OO、およびOOフローに関する知識が必要です。

この章のトピックは、次のとおりです。

- SA-OO統合の新機能 (37ページ)
- 管理者: フローのセットアップ (39ページ)
- ユーザー : フローの実行 (44ページ)

ドキュメントの更新状況、ご使用のドキュメントが最新版かどうか、および最新情報のリリースノートは、次のサイトで確認できます。

http://support.openview.hp.com/selfsolve/manuals

SA-OO統合の新機能

この項では、このバージョンのSA-OO統合の新機能について説明します。

SAからフローを実行する機能

ユーザーがSAからフローを実行できるようになりました。フローをユーザーとして実行する処理の詳細については、ユーザー : フローの実行 (44ページ) を参照してください。

[フロー統合設定の編集] ウィンドウ

このウィンドウ、このウィンドウの下位ウィンドウ、およびこのウィンドウのパネルには、リアルタイムフロー情報の表示、OOコネクター構成ファイル機能の置き換えという2つの新機能があります。

リアルタイム情報の表示

[フロー統合] パネルには、SAからフローを実行し、SAとOOが相互に通信できることを確認し、有効なOOユーザーであることを検証する際に資格情報が使用されるユーザーについて、そのOOユーザーのリアルタイム情報が表示されます。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。

このパネルの詳細については、フロー統合設定の編集 (40ページ) を参照してください。

OOコネクターファイル機能の置き換え

OOコネクター構成ファイル機能が、[フロー統合設定の編集] SAウィンドウで置き換えられました。管理者は、構成入力をSAインタフェースで入力できます。

フロー入力を使用する場合は、アップグレードするときに、これまでのOOコネクター構成ファイルの入力を、対応する [フロー統合設定の編集] ウィンドウフィールドで置き換える必要があります。コネクター設定のマッピングについては、表2を参照してください。インタフェースの詳細については、フロー統合設定の編集 (40ページ) を参照してください。

表 2　　構成ファイル入力と統合ウィンドウフィールドの対応

OOコネクター構成入力	説明	[フロー統合設定の編集] のフィールド
iconclude.enabled	整数、次のいずれか: 1 – **コネクターの有効化** 0 – **コネクターの無効化** デフォルト: 0	[ジョブのブロック] の [接続ステータス] ([フローの実行] フィールド内)
iconclude.host	OOサーバーのホスト名またはIPアドレス デフォルト: なし (必須)	OO URL 次の構文を使用します。 <**プロトコル**>://<**ホスト名またはIPアドレス**>:<**ポート番号**>/
iconclude.port	OOリスナーのポート デフォルト: 8443	OO URL 次の構文を使用します。 <**プロトコル**>://<**ホスト名またはIPアドレス**>:<**ポート番号**>/
iconclude.protocol	OOサーバーに接続するためのプロトコル (httpまたはhttps) デフォルト: https	OO URL 次の構文を使用します。 <**プロトコル**>://<**ホスト名またはIPアドレス**>:<**ポート番号**>/
iconclude.flow.approve	実行されるフローへのパス (フローはOOライブラリ内にあります) デフォルト: なし (必須)	承認フロー
iconclude.user	OOユーザー名 デフォルト: なし (必須)	OOユーザー名
inconclude.password	OOユーザーの平文パスワード このプロパティは、運用環境に含めないでください デフォルト: なし (必須)	パスワード

必要な新しい権限

フローを処理するには、次の新しい権限 (1 つは管理者用、もう1つはユーザー用) が必要です。

- フロー統合の管理

この権限は、管理者がOO統合設定を構成することを許可します。

- フローの実行

  この権限は、ユーザーがSAでフローを実行することを許可します。

管理者: フローのセットアップ

この項では、システム管理者とフロー管理者がSAでOOフローをセットアップする方法について説明します。

前提条件

この項では、SAクライアントでフローをセットアップし実行する際に満たす必要がある前提条件について説明します。

OOを使用するための前提条件

この項では、OOを使用するために必要な環境と権限について説明します。

注: SA統合は、OOの1つのバージョンでのみ実行できます。

環境

OOをSAとともに使用してフローをセットアップし実行するには、次の要件が使用環境で満たされている必要があります。

- SAバージョン9.0
- HP Operations Orchestration (OO) バージョン7.60.Xまたは9.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サーバー上の予約ポート8443
- OOと通信するための有効なOO SDKクライアント証明書

注: SAバージョン9.0には、OO 7.51用のOO SDKクライアント証明書が同梱されています。

OO SDKクライアント証明書のインポート

この項では、必要なOO SDKクライアント証明書インポートする方法について説明します。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。

SDK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。

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。

c コマンドを実行したときにエラーが発生していないことを確認します。

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/jdk1.6/jre/bin/keytool –list –alias pas –keystore /opt/opsware/
jdk1.6/jre/lib/security/cacerts
```

出力例:

```
pas, 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) を起動します。

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

アクセス権

新しい管理者権限である「フロー統合の管理」が必要です。この権限は、管理者がOO統合設定を構成することを許可します。

この権限を設定するには、SA Web クライアントの [Administration] セクションにアクセスします。アクセス権の詳細については、『Server Automation管理ガイド』のアクセス権の項を参照してください。

次の表を参考にして、アクセス権が適切に付与されているかどうかを確認してください。

表 3 ユーザーのアクセス権の確認

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。

フロー統合設定の編集

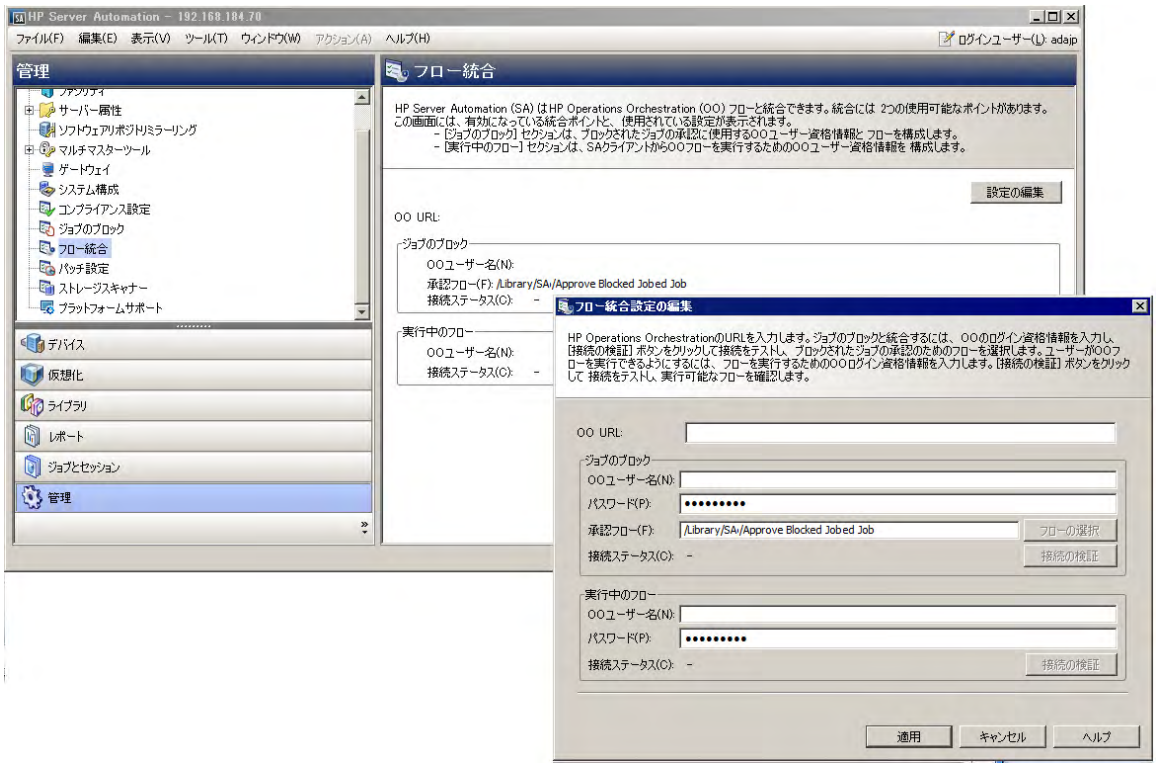
SAのフロー統合設定では、Server AutomationとHP Operations Orchestrationの統合を設定できます。

フロー統合設定を指定または編集するには、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。

図 16 [フロー統合設定の編集] ウィンドウ



[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

詳細については、表2を参照してください。

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」の章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。

[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。

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、表4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。

表 4 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 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

表 4　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
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。 • 未割り当て (値が1つの場合) • 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。
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つの場合にのみ設定されます。 2つの値を (OOで) 設定できます。 • 未割り当て (値が1つの場合) • 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。
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。

変更と設定の検証

この項では、変更または設定が適用済みであることを検証する方法について説明します。

フロー編集とフローステータス

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。

図 17 [フロー統合] パネル

[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。

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す。

ユーザー：フローの実行

この項では、フローの実行、サーバーの選択、およびフロー入力の選択をユーザーが行う方法について説明します。

SAでフローを実行するユーザーは、フローの実行権限を持っている必要があります。

実行するフローの選択

この項では、実行するフローの選択方法について説明します。

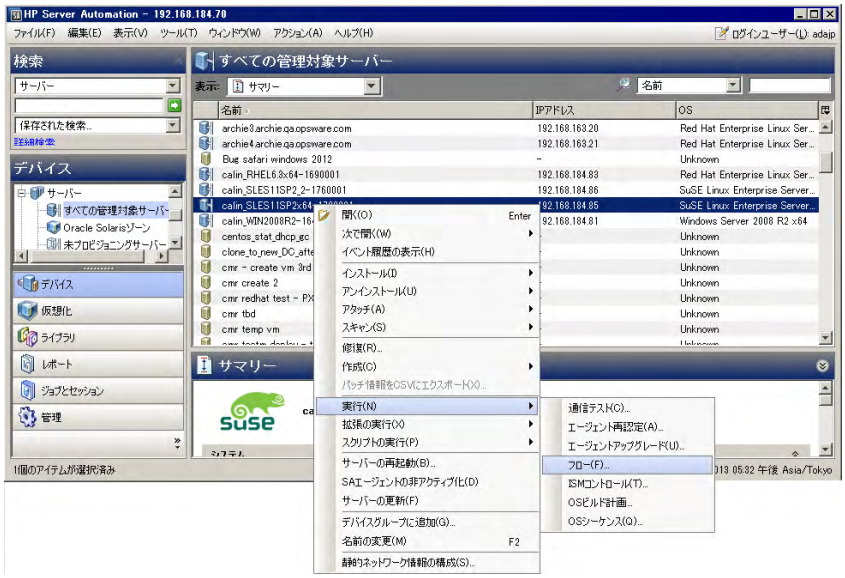
1 SAクライアントのナビゲーションパネルで、[デバイス] を選択します。

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。

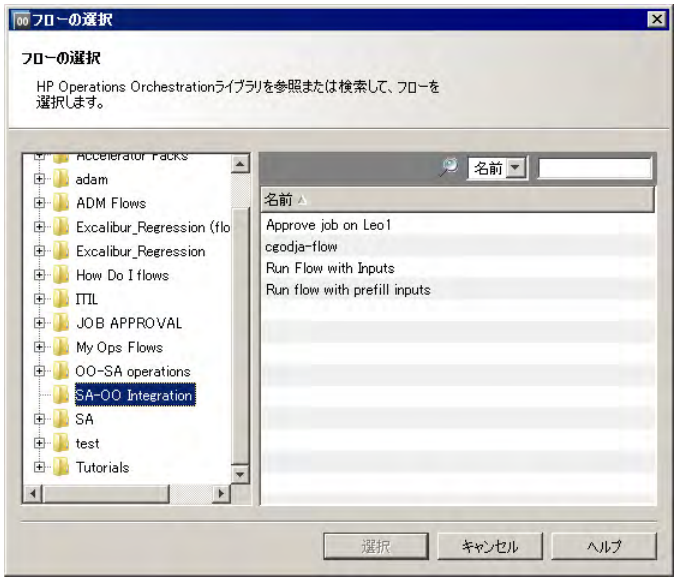
3 サーバー名を右クリックします。

図 18　[フローの実行] オプション



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

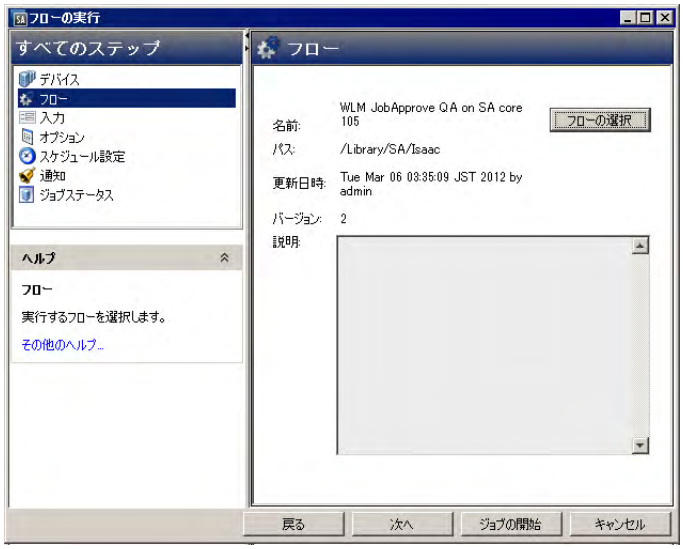
図 19　[フローの選択] ウィンドウ



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。

図 20　[フローの実行] ウィンドウ



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、および通知パラメーターを選択できます。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、および通知パラメーターの選択 (46ページ)を参照してください。

サーバーの追加または削除

サーバーを追加または削除するには、まず実行するフローの選択 (44ページ)の手順を実行してから、次の手順を実行します。

1　[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。

2　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。

3　[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。

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、および通知パラメーターの選択

フロー入力、実行時オプション、スケジュール設定、および通知の値を入力できます。一部のパラメーターは、あらかじめ自動的に入力されます。

1　実行するフローの選択 (44ページ)の手順を実行してから、以下の手順を実行します。

2　[フローの実行] ウィンドウの [すべてのステップ] 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。

3　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。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、表4を参照してください。

4 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。

5 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

6 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

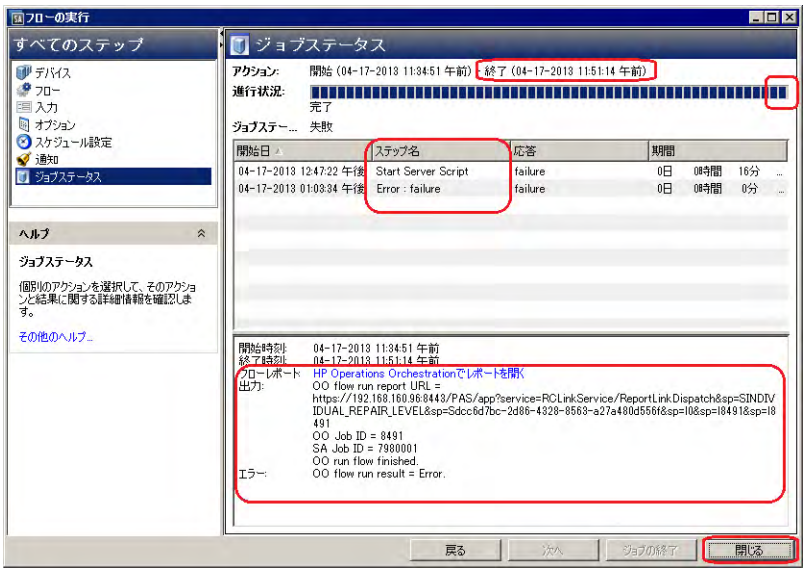
   b 通知 ([通知の追加] をクリック)

   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。)

7 [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。

8 [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)

図 21 SAジョブのステータス



[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。

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。(フロー統合設定の編集 (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、フロー統合設定の編集 (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、フロー統合設定の編集 (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。

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。

第 4 章　SA-OO統合 – ジョブのブロックと承認

Software Automation (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。

この章では、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 Application Deployment User Guide』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。

この章のトピックは、次のとおりです。

ジョブの詳細については、『SA Application Deployment User Guide』を参照してください。SAOOでの作業の詳細については、OOのドキュメントを参照してください。

ドキュメントの更新状況、ご使用のドキュメントが最新版かどうか、および最新情報のリリースノートは、次のサイトで確認できます。

http://support.openview.hp.com/selfsolve/manuals

ジョブのブロック

この項では、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

SAジョブの中には、実行する前に確認と承認が必要なものがあります。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になります。

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になります。

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。

ブロック可能なSAジョブのタイプ

次の表に、SAジョブのタイプを示します。

表 5　　ブロック可能なSAジョブのタイプ

ジョブタイプ	機能
仮想マシンの複製	VMwareサーバー上に仮想マシンを複製します
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します
仮想マシンの作成 (Hyper-V)	仮想マシンをプロビジョニングし、Hyper-V仮想マシンにオペレーティングシステムをインストールします
仮想マシンの作成 (VMWare)	仮想マシンをプロビジョニングし、VMware ESX サーバーにオペレーティングシステムをインストールします
仮想ゾーンの作成	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
パッチのインストール	管理対象サーバーに任意のパッチ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任意のソフトウェアをインストールします
仮想マシンの変更	VMware仮想マシンのプロパティを変更します
仮想マシンの変更 (Hyper-V)	Hyper-V仮想マシンのプロパティを変更します
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
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
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されます
仮想マシンの削除	VMware ESXサーバー (Hypervisor) から仮想マシンを削除します
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

表 5　　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、1つ前の構成が保存され、後で復元できます。
監査の実行	監査を実行します
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スクリプトを使用すると、SAクライアントからGlobal Shellでスクリプトを実行できます。
OSビルド計画の実行	OSビルド計画を実行します
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

必要なアクセス権

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 (フローを起動するユーザーがジョブを編集またはキャンセルできます)
- すべてのジョブを表示 (フローを起動するユーザーがジョブを表示できます)
- ジョブのブロックの管理 (ジョブのブロックとブロック解除を実行できます)
- フロー統合の管理 (OOへのSA-OO統合の接続設定を構成し、承認フローを指定できます)

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。

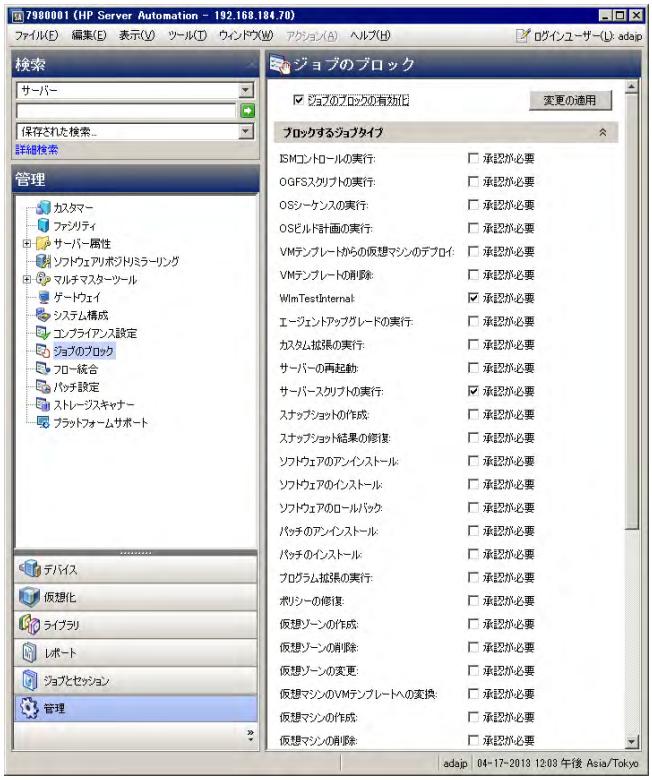
ブロックするジョブタイプの指定方法

ブロックするジョブのタイプを指定するには、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] 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。

図 22　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、表5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

ジョブのブロックを無効にするには、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] 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。(図22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。.

[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。

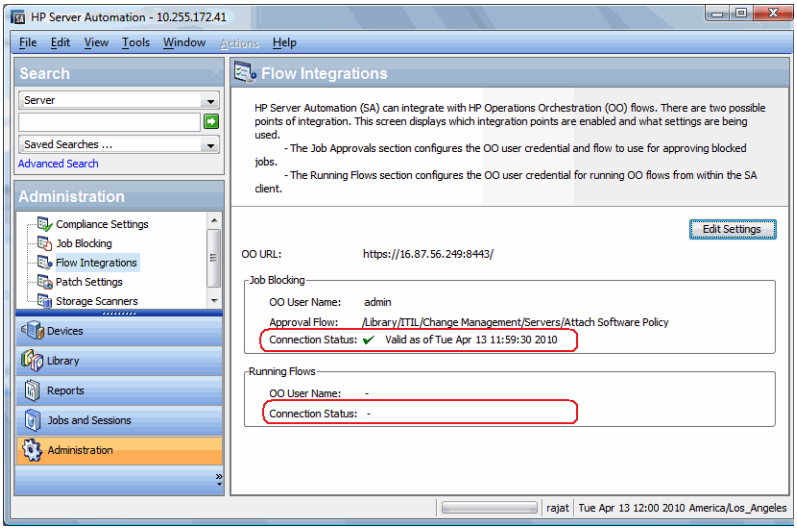
ブロックされたジョブの情報の表示方法

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。

図 23 [フロー統合] パネル



[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。

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、表7を参照してください。

フロー設定の構成または編集

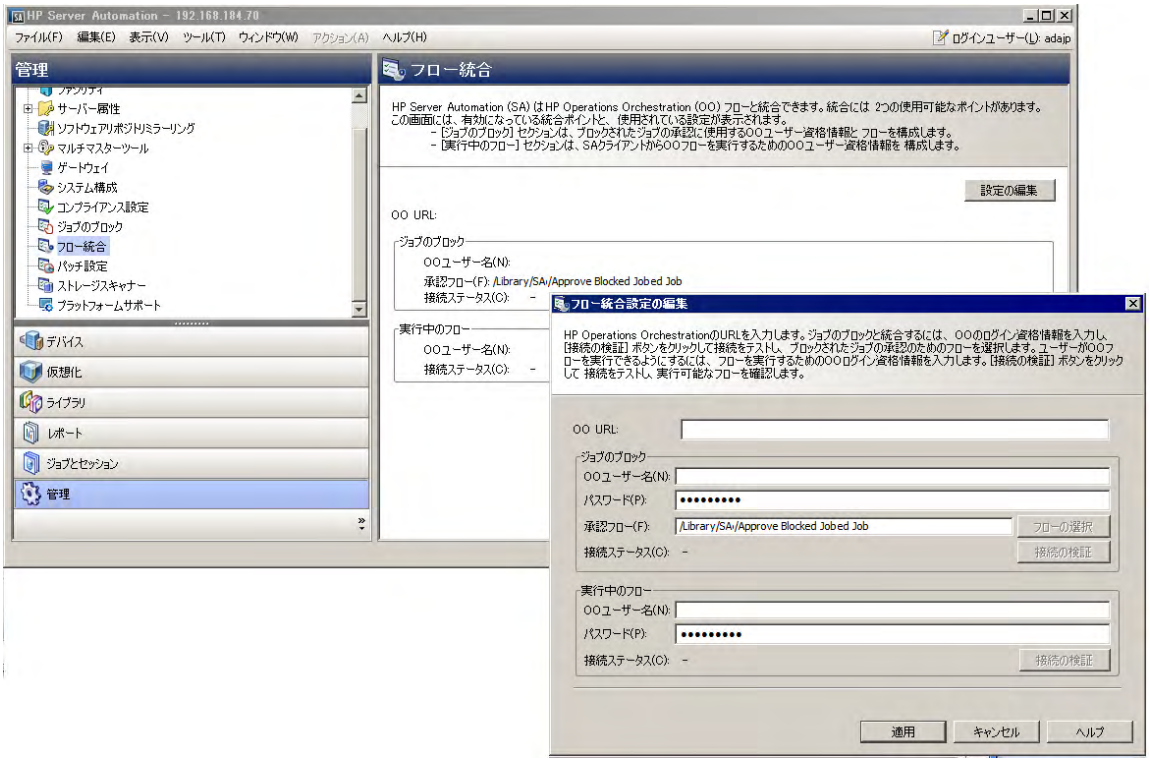
フロー設定を編集または構成するには、OOとSAにログインしている必要があります。

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] をクリックして、[フロー統合設定の編集] ウィンドウを表示します。

図 24 [フロー統合設定の編集] ウィンドウ



[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/
  ```

- 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

詳細については、表2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。

[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 プラットフォーム開発者ガイド』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、OOのドキュメントを参照してください。

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]

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。

表 6　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=$job_id
JobService. updateBlockedJob	SA クライアントの [ジョブステータス] ウィンドウでブロックされたジョブの Ticket ID フィールド (userTag パラメーターに対応) および Reason フィールド (blockReason パラメーターに対応) の値を変更します。 **注:** SAインタフェースを使用して、これらのフィールドを変更することはできません。	cd /opsw/api/com/opsware/job/JobService/method./updateBlockedJob self:i=$job_id userTag=$ticket_id \blockReason= "This type of job requires approval of CMB."
JobService. cancelScheduledJob	ブロックされたジョブをキャンセルして、実行できないようにします。 ブロックされたジョブのステータスを [承認待ち] から [キャンセル] に変更します。	(IDパラメーターはjobRefであり、selfではないことに注意) cd /opsw/api/com/opsware/job/JobService/method./cancelScheduledJob jobRef:i=$job_id \reason="Job was scheduled to run outside of change window." 現在実行中のジョブ (job_status = "ACTIVE") はキャンセルできません。
JobService. findJobRefs	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。 他のユーザーが起動したジョブを表示できます。	(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。) cd /opsw/api/com/opsware/job/JobService/method./.findJobRefs:i filter=job:{job_status = "BLOCKED" }

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)。

表7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のではありません)。

表 7　　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	コマンドエンジンスクリプトのエラー	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有効でなくなりました。
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	
SUCCESS	6	完了	ジョブの実行が正常に終了しました。
TAMPERED	9	改竄	
UNKNOWN	7	不明	
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	

第 5 章　SA-UCMDB統合

ここでは、**SA-UCMDB Connector** を使用して、HP Server Automation (SA) と HP Universal Configuration Management Database (UCMDB) を統合する方法について説明します。SA-UCMDB Connector は、資産のコンプライアンスレポートの構成データ用の単一ソースを提供します。

HP 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HP 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に自動的に送信します。

HP Universal CMDB は、ビジネスサービスの定義および関連するインフラストラクチャーの関係をエンタープライズのIT組織で文書化し、保管し、管理するための構成管理データベース (CMDB) です。UCMDBは、ビジネスサービス管理、ITサービス管理、変更管理、および資産管理の取り組みをサポートするために共有される単一バージョンのTruthを提供します。このような取り組みにより、IT作業がビジネス要件に合うように調整され、IT操作をより効果的、効率的に実行できるようになります。

HP Server Automation は、エンタープライズのサーバーとアプリケーションのライフサイクル管理を提供し、検出からプロビジョニング、パッチ処理から構成管理、スクリプトの実行からコンプライアンスの保証までを処理します。HP Server Automationは、異なるITチームやシステムにまたがる操作と処理を自動化します。

SA-UCMDB Connectorのインストールと構成

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。

SA-UCMDB Connectorを構成して実行するには、次の手順を実行します。

1. HP Live Network (HPLN) から最新の UCMDB コンテンツパックを入手します。これには、UCMDB が SA-UCMDB Connectorをサポートするための構成が含まれています。SA-UCMDB Connectorを使用するには、HP UCMDB 9.04以降とコンテンツパック10以降が必要です。
   - HPLNについては、『Live Network connector Users Guide』(『LNc Users Guide』) を参照してください。このガイドは、HP Live Network (http://www.hp.com/go/livenetwork) にあります。
   - HPLNにログインするには、HP BSA Essentialsアカウントが必要です。BSA Essentialsアカウントは、HP Live Network (HPLN) (http://www.hp.com/go/livenetwork) で要求できます。
   - SAコアサーバーにLive Network connector (LNc) がインストールされ、構成されている必要もあります。LNcは、HP Live Networkのクライアントです。LNcはServer Automationとともにインストールされます。手順については、HP Live Networkにある『Live Network connector Users Guide』(『LNcユーザーガイド』) を参照してください。
2. `enable`コマンドを探して実行します。このコマンドの説明は、enableコマンド (62ページ) を参照してください。次に、このコマンドの例を示します。

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

3 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
```

これにより、SA-UCMDB Connectorが起動されます。詳細については、SA-UCMDB Connectorの起動 (60ページ) を参照してください。

4 (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 (61ページ) を参照してください。

SA-UCMDB Connectorの起動

SA-UCMDB Connectorを起動すると、SAデータベースのデータがUCMDBに転送されるようになります。起動する前に、SA-UCMDB Connectorを構成し、enableコマンドで有効にしてください (enableコマンド (62ページ) を参照)。

SA-UCMDB Connectorを起動するには、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 start telldaemon
```

これにより、SA-UCMDB Connectorが起動されます。

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の停止

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が不要になった場合は、disableコマンドで無効にすることができます。disableコマンド (63ページ) を参照してください。

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 Connectorの再構成

いったん実行されたSA-UCMDB Connectorの構成 (UCMDBサーバーのIPアドレスやポート番号など) を変更するには、次の手順を実行します。

1. 次のコマンドを入力して、SA-UCMDB Connectorを停止します。

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

   詳細については、SA-UCMDB Connectorの停止 (60ページ) を参照してください。

2. 次のコマンドを入力して、SA-UCMDB Connectorをdisableにします。

   disable

   詳細については、disableコマンド (63ページ) を参照してください。

3. enableコマンドを実行して、SA-UCMDB Connectorの構成を変更します。次に、このコマンドの例を示します。

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

   詳細については、enableコマンド (62ページ) を参照してください。

4. 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
   ```

   詳細については、SA-UCMDB Connectorの起動 (60ページ) を参照してください。

5. (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 (61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せきません。

SA-UCMDB Connectorを有効にしたら、SA-UCMDB Connectorの起動 (60ページ) の説明に従って起動してください。

enableコマンドは、次の処理を行います。

- SA-UCMDB　Connector構成ファイル /etc/opt/opsware/tell/tell.confを変更して、UCMDBサーバーのホスト名またはIPアドレス、ポート番号、およびログインをファイルに入力する。
- 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コアサーバーの次のディレクトリにあります。
/opt/opsware/tell/bin

enableコマンドの構文

enable [--host <IP**アドレス**>] [--port <**ポート番号**>] [--user <**ユーザー名**>] [--password <**パスワード**>]

- --host <IPアドレス> – このオプションは、HP 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 <ポート番号> – このオプションは、HP 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。
- --user <ユーザー名> – このオプションは、HP 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 <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。

enableコマンドの例

次に、enableコマンドの例を示します。

enable --host 192.168.8.93 --port 9999 --user john-ucmdb --password mypass1234

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コアサーバーの次のディレクトリにあります。
/opt/opsware/tell/bin

disableコマンドの構文

```
disable
```

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。このコネクターは、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 (63ページ) を参照してください。

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。

表 8　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

表 8　　SAによって設定されるUCMDBのCIと属性

UCMDBのCI	UCMDBの属性
Node	NetBiosName
Node	MemorySize
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

維持されるCIの関係

次の表に、SA-UCMDB Connectorで維持されるCIの関係を示します。

表 9　　維持されるCIの関係

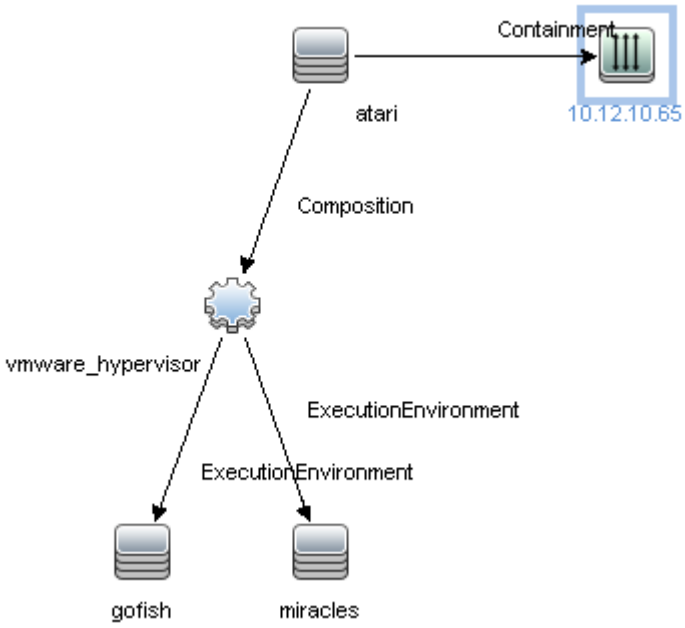
UCMDBのCIから	方法	UCMDBのCIへ
Node	containment	IpAddress
Node	composition	InstalledSoftware
Node	composition	Hypervisor
Node	aggregation	PolicyResult
Hypervisor	ExecutionEnvironment	Node
Policy	composition	PolicyResult
SASystem	aggregation	Node
SASystem	aggregation	Policy

SA管理対象サーバーを示すUCMDBの例

図25は、HP 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。

図 25　UCMDBに表示されたSA管理対象サーバー



トラブルシューティング - 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。

トラブルシューティング - 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、SA-UCMDB Connectorの起動 (60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 (61ページ)の説明に従ってステータスを確認してください。