HP Server Automation

Ultimate Edition

ソフトウェアバージョン: 10.10

管理ガイド

ドキュメントリリース日: 2014年6月30日 (英語版)
ソフトウェアリリース日: 2014年6月30日 (英語版)

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、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

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クスを参照してください。サポートマトリ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://h20230.www2.hp.com/selfsolve/manuals

ドキュメントの更新情報

このリリースのServer Automation製品の最新のドキュメントは、すべて次のSA Documentation Libraryから入手できます。

http://support.openview.hp.com/selfsolve/document/KM00417675/binary/SA_10_docLibrary.html

SA Documentation Library では、このリリースに関連するガイドライン、リリースノード、サポートマトリクス、およびホワイトペーパーにアクセスできます。また、フルドキュメントセットを一括してダウンロードすることもできます。SA Documentation Library は、リリースごとに更新されます。また、リリースノートが更新されたときや、新しいホワイトペーパーが発行されたときにも更新されます。

情報リソースを見つける方法

Server Automationの情報リソースは、次のいずれの方法でもアクセスできます。

方法1: 新しいSA Documentation Libraryから、最新のドキュメントにタイトルとバージョンを指定してアクセスします。

方法2: [All Manuals Download] からローカルディレクトリにフルドキュメントメントセットを保存します。

方法 3: サポートされるリリースの HP 製品ドキュメントを HP ソフトウェアドキュメントポータルで検索します。

各ドキュメントにアクセスするには、次の手順を実行します。

1. SA 10.x Documentation Libraryにアクセスします。

   http://support.openview.hp.com/selfsolve/document/KM00417675/binary/SA_10_docLibrary.html

2. HP Passportの資格情報を使ってログインします。
3. ドキュメントのタイトルとバージョンを指定して、[**go**] をクリックします。

ローカルディレクトリ内の完全なドキュメントセットを使用するには、次の手順を実行します。

1 フルドキュメントセットをローカルディレクトリにダウンロードするには、次の手順を実行します。

a SA Documentation Libraryにアクセスします。

http://support.openview.hp.com/selfsolve/document/KM00417675/binary/SA_10_docLibrary.html

b HP Passportの資格情報を使ってログインします。

c SA 10.1バージョンの [All Manuals Download] タイトルを探します。

d [**go**] リンクをクリックして、ローカルディレクトリにZIPファイルをダウンロードします。

e ファイルを解凍します。

2 ローカルディレクトリ内のドキュメントを探すには、ドキュメントカタログ (docCatalog.html) を使用します。ローカルディレクトリにダウンロードしたドキュメントの索引ポータルが表示されます。

3 ドキュメントセット内のすべてのドキュメントを対象としてキーワードを検索するには、次の手順を実行します。

a ローカルディレクトリ内の任意のPDFドキュメントを開きます。

b [**編集**] > [**高度な検索**] を選択します (またはShift＋Ctrl＋Fキー)。

c [以下の場所にあるすべてのPDF文書] オプションを選択し、ローカルディレクトリを指定します。

d キーワードを入力し、[検索] をクリックします。

HPソフトウェアドキュメントポータルで追加ドキュメントを探すには、次の手順を実行します。

HPソフトウェアドキュメントポータルにアクセスします。

http://h20230.www2.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

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

- Server Automation (SA) は、Server AutomationのUltimate Editionです。Server Automationについては、『SAリリースノート』および『SAユーザーガイド: Server Automation』を参照してください。
- Server Automation Virtual Appliance (SAVA) は、Server AutomationのPremium 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。

目次

第1章 ユーザーおよびユーザーグループの設定とセキュリティ

SAの役割ベースのセキュリティモデルでは、承認されたユーザーのみが特定のサーバー上で特定の操作を実行できます。この章では、セキュリティ管理者を対象に、SAで役割ベースのセキュリティ構造を設定する方法について説明します。

新規ユーザーの作成方法に関するビデオを見る (1分30秒)

SAのユーザーおよびユーザーグループについて

SAのユーザーグループは、その役割を実行するのに必要なアクセス権を定義します。各ユーザーグループに一連のアクセス権を付与した後に、ユーザーを1つ以上のユーザーグループに割り当てます。ユーザーグループごとに、そのグループに属するすべてのユーザーに一連のアクセス権が割り当てられます。

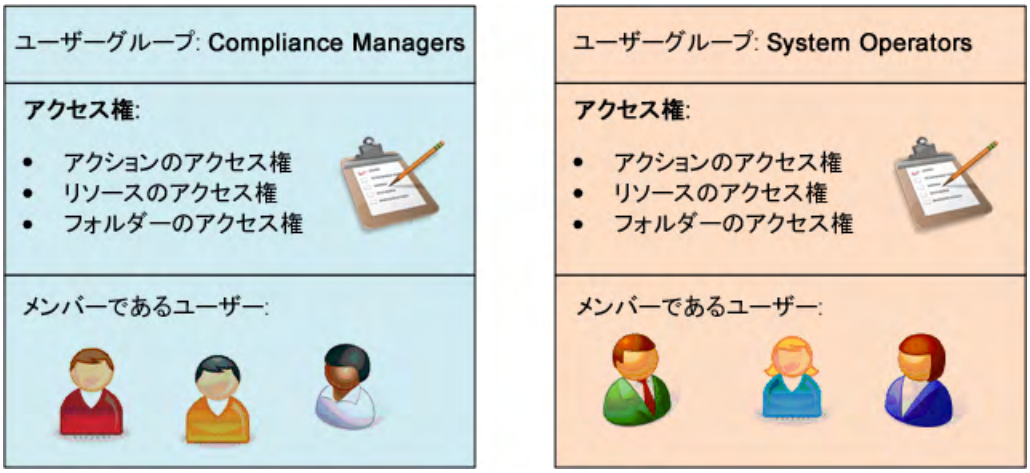
すべてのユーザーは、SAの1つ以上のユーザーグループに属することができます。ユーザーが実行できるタスクは、ユーザーが属するユーザーグループによって決まります。

SAのユーザーグループには、次の特徴があります。

- ユーザーグループは**役割を表します**。役割はタスクと職責を組み合わせたものです。
- ユーザーグループでは**アクセス権を定義します**。これにより、その役割を実行するのに必要な一連のタスクを使用できるようにします。
- ユーザーグループには、その役割を実行する**SAユーザーが含まれます**。

図1に、ユーザーグループの2つの例を示します。一方のユーザーグループは、監査レポートを実行して、企業のポリシーに対するサーバーのコンプライアンスを徹底する役割を持つコンプライアンス管理者のグループです。もう一方のユーザーグループは、サーバーの監視とソフトウェアやパッチのインストールを行う役割を持つシステムオペレーターのグループです。各ユーザーグループには、それぞれのアクセス権とユーザーが含まれます。

図1　　ユーザーグループの内容 (役割に基づく)



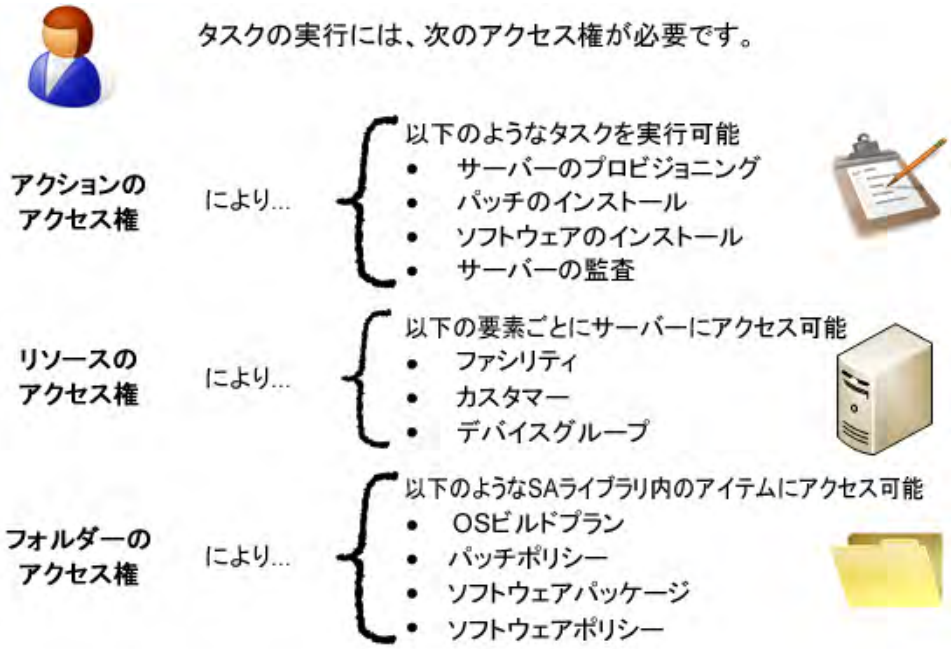
SAには事前定義のユーザーグループが用意されていますが、組織内の役割に合わせて独自のユーザーグループを作成することもできます。詳細については、事前定義のユーザーグループ (27ページ) を参照してください。

アクセス権のタイプについて - アクション、リソース、フォルダーのアクセス権

SAでは、サーバー上でアクションを実行するのに必要な、次の3つのアクセス権が利用できます。

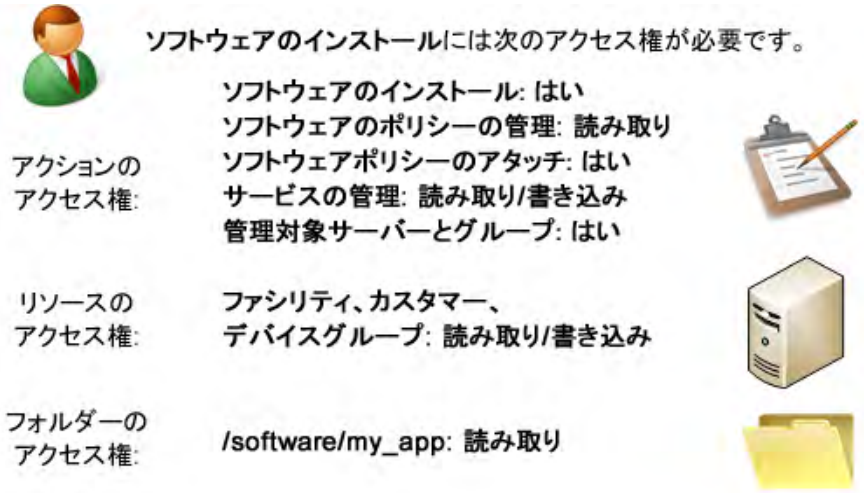
- **アクションのアクセス権**: ユーザーが実行できるアクションまたはタスクを指定します。
- **リソースのアクセス権**: ユーザーがこれらのアクションを実行できるサーバーを指定します。すべてのサーバーは、ファシリティ別、カスタマー別、デバイスグループ別にグループ化されます。リソースのアクセス権を設定するには、ファシリティ、カスタマー、デバイスグループへのアクセスを指定します。
- **フォルダーのアクセス権**: SAライブラリ内のアイテム (OSビルド計画、ソフトウェアパッケージ、ソフトウェアポリシー、パッチポリシー、監査ポリシーなど) へのアクセス権を指定します。

図2　タスクの実行に必要なSAのアクセス権のタイプ



たとえば、ソフトウェアポリシーを使用してソフトウェアをインストールする場合、ユーザーには(少なくとも)図3に示すようなアクセス権が必要です。

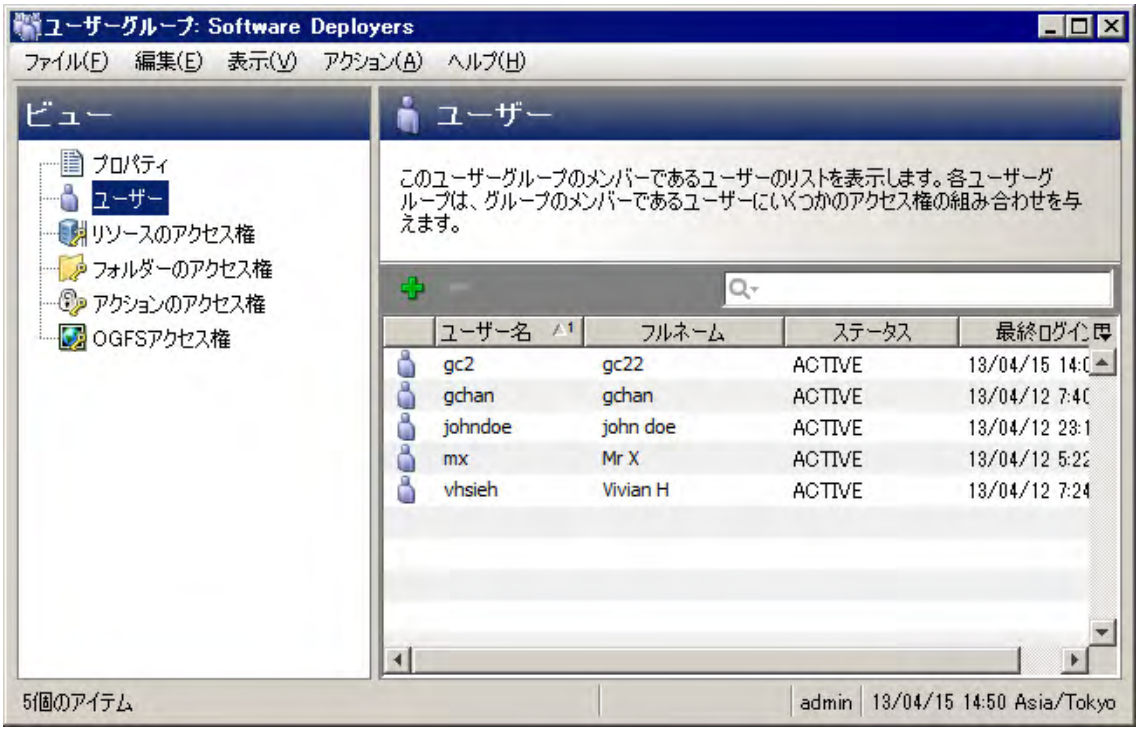
図3　ソフトウェアのインストールに必要なアクセス権



これらのアクセス権(およびその他)は、事前定義のユーザーグループであるSoftware Deployersで設定されます。詳細については、事前定義のユーザーグループ (27ページ)を参照してください。

図4は、Software Deployersという名前の事前定義のユーザーグループと、このグループに属するSAユーザーを示しています。[ビュー]ナビゲーションパネルには、このユーザーグループのリソースのアクセス権、フォルダーのアクセス権、アクションのアクセス権、OGFSアクセス権も表示されます。

図4　ユーザーグループブラウザーで所属するユーザーを表示したところ



アクションのアクセス権について

アクションのアクセス権では、ユーザーが実行できるタスクを定義します。一部のアクションのアクセス権では、次のタイプのアクセスを指定します。

- 読み取り: ユーザーはタスクを実行できます。ただし、読み取り専用モードです。
- 読み取り/書き込み: ユーザーはタスクをフルに実行できます。
- なし: タスクはSAクライアントに表示されません。ユーザーはタスクを表示または実行できません。

また、次のタイプのアクセスを指定するアクションのアクセス権もあります。

- **はい**: ユーザーはタスクを実行できます。
- **いいえ**: ユーザーはタスクを実行できません。

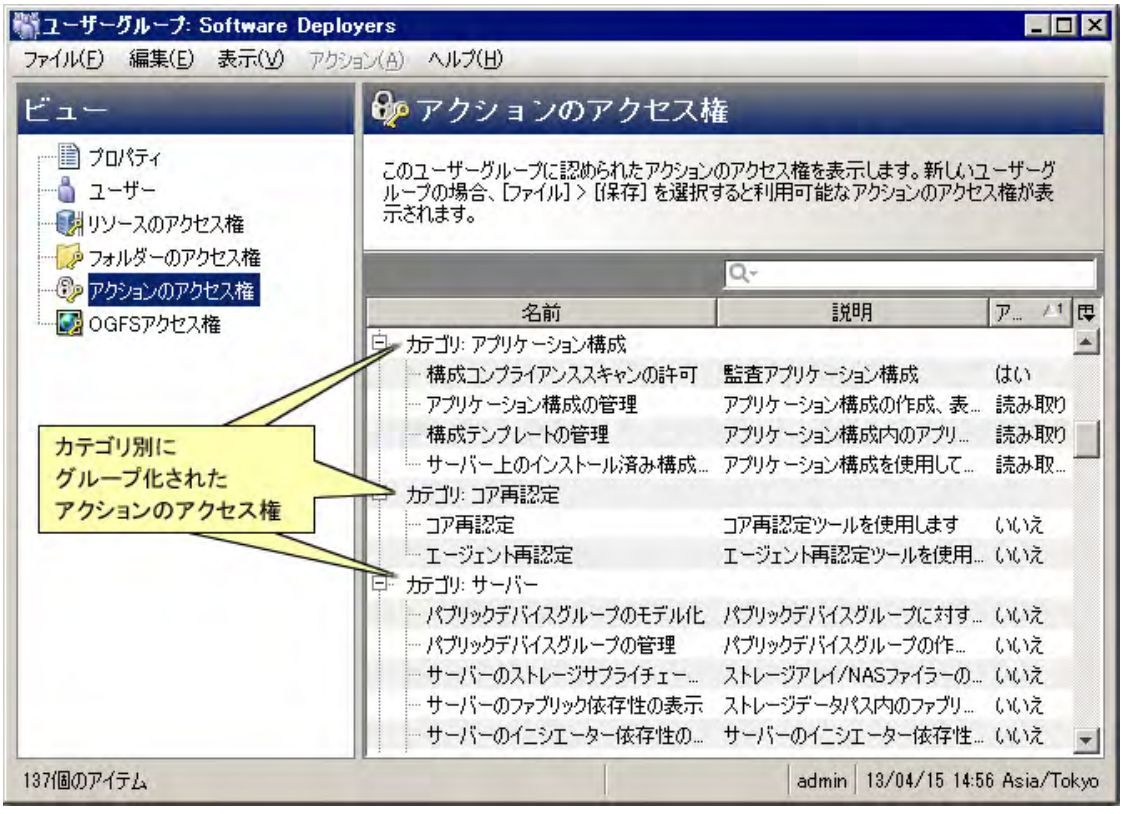
アクションのアクセス権の一覧については、アクセス権のリファレンス (249ページ) を参照してください。

詳細については、アクションのアクセス権の設定 (46ページ) も参照してください。

アクションのアクセス権のグループ化

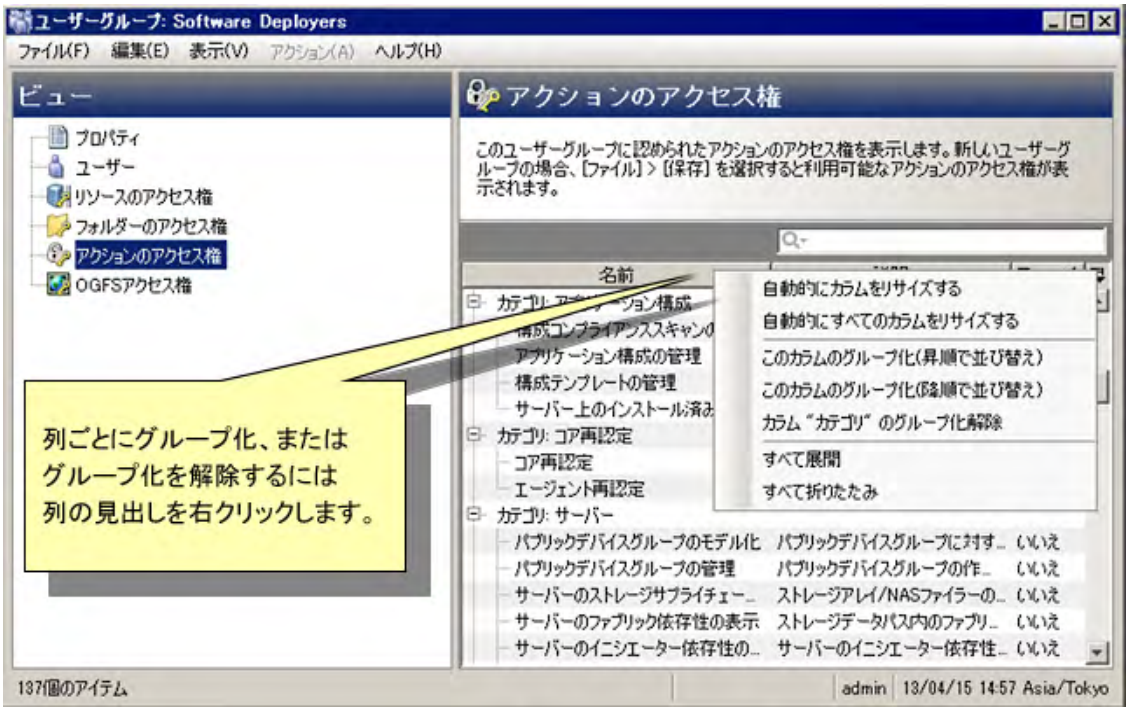
SA クライアントでユーザーグループを開くと、ユーザーグループのアクションのアクセス権が表示されます。アクションのアクセス権は、図5のように、カテゴリ別にグループ化されます。

図5　[ユーザーグループ] ウィンドウ - [アクションのアクセス権] ビュー (カテゴリ別にグループ化)



列を右クリックすると、アクションのアクセス権のグループ化の解除や、他の列でのグループ化を行うことができます (図6を参照)。

図6　[ユーザーグループ] ウィンドウ - [アクションのアクセス権] ビュー (グループ化のメニュー)



リソースのアクセス権について

リソースは1つまたは複数の管理対象サーバーです。サーバーリソースは、次のカテゴリに分けられます。

- ファシリティ: SAファシリティに関連付けられたサーバー。管理対象サーバーはすべて、いずれか1つのファシリティに属します。
- カスタマー: カスタマーに関連付けられたサーバー。カスタマーを作成して、各サーバーを1つのカスタマーに割り当てます。サーバーはすべて、いずれか1つのカスタマーに属します。これは、「未割り当て」カスタマーグループの場合もあります。
- デバイスグループ: デバイスグループに属しているサーバー。デバイスグループを作成し、それらにサーバーを割り当てます。すべてのサーバーは、1つ以上のデバイスグループに属することができます。

ユーザーグループ内のユーザーがサーバーの表示や変更を行うことができるかどうかは、ユーザーグループのリソースのアクセス権によって決まります。ユーザーグループは、リソースのアクセス権が付与されたファシリティ、カスタマー、デバイスグループのサーバーのみにアクセスできます。すべてのサーバーは1つのファシリティ、1つのカスタマー、および少なくとも1つのデバイスグループに属します。そのため、サーバーにアクセスするには、ユーザーグループに少なくとも1つのファシリティ、少なくとも1つのカスタマー、少なくとも1つのデバイスグループへのアクセス権が必要です。

カスタマー、ファシリティ、デバイスグループのアクセス権を組み合わせると、セキュリティポリシーを実装できます。たとえば、Acme Corp. カスタマーに関連付けられた、Fresno ファシリティ内にある、Windows サーバーのみを含むデバイスグループに属するサーバーに、アクセスを制限することができます。リソースのアクセス権の例 (21ページ) を参照してください。

サーバーはいずれも、1つのファシリティ内に存在し、1つのカスタマーに関連付けられ、1つまたは複数のデバイスグループに属しています。ユーザーが特定のサーバーにアクセスするには、該当するファシリティ、該当するカスタマー、およびそのサーバーを含む少なくとも1つのデバイスグループへのアクセスが必要です。

詳細については、リソースのアクセス権の設定 - ファシリティ、カスタマー、デバイスグループ (44ページ)も参照してください。

リソースへのアクセスのタイプ

リソースのアクセス権では、次のいずれかのタイプのアクセスを指定する必要があります。

- 読み取り: ユーザーはリソースの表示のみを行うことができます。
- 読み取り/書き込み: ユーザーはリソースの表示、作成、変更、または削除を行うことができます。
- なし: リソースはSAクライアントに表示されません。ユーザーはリソースを表示または変更できません。

ファシリティのアクセス権について

すべてのサーバーはいずれか1つのファシリティ内に存在します。ユーザーが特定のファシリティ内のサーバーを変更するには、そのファシリティに対する [読み取り/書き込み] アクセス権を持つユーザーグループに属している必要があります。たとえば、あるグループのユーザーがLondonファシリティ内のサーバーを表示できる (ただし、変更はできない) ようにする場合は、アクセス権を [読み取り] に設定します。

ファシリティのアクセス権では、ファシリティオブジェクト自体へのアクセスも制御されます。たとえば、ファシリティのプロパティを変更する場合、ユーザーはそのファシリティに対する [読み取り/書き込み] アクセス権とファシリティを変更するアクションのアクセス権を持つグループに属している必要があります。

カスタマーのアクセス権について

すべてのサーバーは、いずれか1つのSAカスタマーに関連付けられます。これは、「未割り当て」カスタマーグループの場合もあります。SAカスタマーとは、複数のサーバーで構成される論理的なグループです。このようにサーバーをグループ化することで、対象のカスタマーに対する読み取り / 書き込み権限を保持していて、セキュリティと認証の境界を設定できる場合に限り、SAカスタマーに所属するすべてのサーバーに対してIT管理タスクを実行できます。たとえば、あるグループのユーザーがWidget Inc.のカスタマーに関連付けられたサーバーを表示できる (ただし、変更はできない) ようにする場合は、アクセス権を [読み取り] に設定します。

カスタマーのアクセス権では、カスタマーオブジェクト自体へのアクセスも制御されます。たとえば、カスタマーにカスタム属性を追加する場合、ユーザーはそのカスタマーに対する [読み取り/書き込み] アクセス権とカスタマーを変更するアクションのアクセス権を持つグループに属している必要があります。

デバイスグループのアクセス権について

すべてのサーバーは、1つ以上のデバイスグループに属することができます。デバイスグループのアクセス権を設定すると、デバイスグループに属するサーバーに対するユーザーグループ内のユーザーのアクセスを制御できます。たとえば、あるグループのユーザーがWindows Server 2008デバイスグループ内のサーバーを表示できる (ただし、変更はできない) ようにする場合は、アクセス権を [読み取り] に設定します。

デフォルトで、各サーバーはそれぞれのオペレーティングシステムに基づいたパブリックデバイスグループに属しています。SAクライアントでこれらのデバイスグループを表示するには、[デバイス] タブを選択し、[デバイスグループ] > [Public] > [Opsware] > [Operation Systems] の順に選択します。

サーバーが複数のデバイスグループに属している場合は、ユーザーグループにその内のいずれか1つのデバイスグループに対するアクセス権があれば、そのサーバーにアクセスできます。

デバイスグループに他のデバイスグループを含めることはできますが、アクセス権が継承されることはありません。

プライベートデバイスグループへのアクセスを制御することはできません。プライベートデバイスグループは、そのグループを作成したユーザーのみが表示できます。

デバイスグループのアクセス権では、デバイスグループに属するサーバーへのアクセスを制御します。ただし、これらのアクセス権では、デバイスグループの管理を制御することはできません。デバイスグループを作成、変更、または削除するには、ユーザーが [パブリックデバイスグループの管理] と [パブリックデバイスグループのモデル化] のアクションのアクセス権、および [管理対象サーバーおよびグループ] アクションのアクセス権を持つユーザーグループに属している必要があります。アクセス制御グループとして使用されているデバイスグループにデバイスを追加するには、ユーザーがスーパー管理者である必要があります。

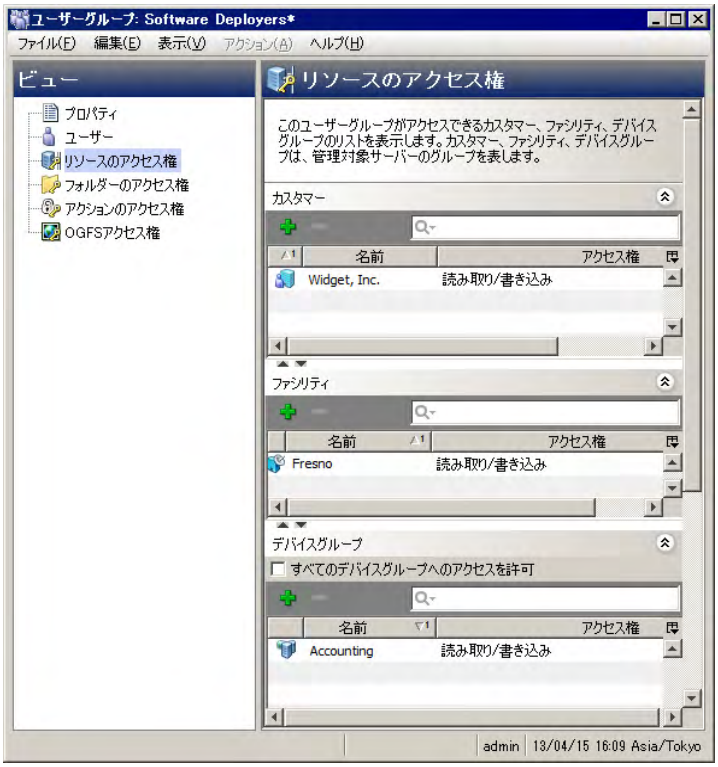
リソースのアクセス権の例

サーバーがファシリティ Fresno 内に存在し、カスタマー Widget, Inc. に関連付けられ、デバイスグループ Accountingに属しているとします。このサーバーを変更する場合、ユーザーグループには表1に示すアクセス権が必要です。図7は、これらのアクセス権を持つWin-patchersという名前のユーザーグループの例です。

表1　　リソースのアクセス権の例

リソース	アクセス権
ファシリティ : Fresno	読み取り/書き込み
カスタマー : Widget, Inc.	読み取り/書き込み
デバイスグループ: Accounting	読み取り/書き込み

図7　　[ユーザーグループ] 画面での [リソースのアクセス権] ビュー



ファシリティ、カスタマー、またはデバイスグループのアクセス権が一致しない場合は、**最も限定的な**アクセス権が適用されます。

たとえば、表2に示すように、カスタマーとデバイスグループのアクセス権が [読み取り/書き込み] で、ファシリティのアクセス権が [読み取り] である場合は、[読み取り] アクセス権が適用されるため、ユーザーはサーバーを変更できません。

カスタマーのアクセス権が [なし] である場合、ユーザーグループの他のアクセス権で [読み取り] や [読み取り/書き込み] が指定されていても、サーバーを表示することはできません。

表2　一致しないリソースのアクセス権の例

リソース	アクセス権
ファシリティ : Fresno	読み取り
カスタマー : Widget, Inc.	読み取り/書き込み
デバイスグループ: Accounting	読み取り/書き込み

リソースのアクセス権とアクションのアクセス権の組み合わせ - 例

リソースでアクションを実行するには、ユーザーがアクションとリソース (サーバー) の両方の必要なアクセス権を持つグループに属している必要があります。たとえば、サーバーがカスタマー Widget, Inc.、ファシリティ Fresno、デバイスグループRed Hat AS 4に関連付けられているとします。このサーバーにパッチをインストールする場合、ユーザーは表3に示すアクセス権を持つグループに属している必要があります。

表3　リソースのアクセス権とアクションのアクセス権の例

リソースとアクション	アクセス権
カスタマー : Widget, Inc.	読み取り/書き込み
ファシリティ : Fresno	読み取り/書き込み
デバイスグループ: Red Hat AS 4	読み取り/書き込み
アクション: パッチのインストール	はい

その他のリソースのタイプ

管理対象サーバーは最も一般的なリソースです。この他にも次のようなタイプのリソースがあります。

- ハードウェア定義
- レルム
- OSインストールプロファイル

これらのリソースはそれぞれカスタマーに関連付けることができます。

フォルダーもカスタマーに関連付けることができますが、フォルダーへのアクセスの制御は、別の方法で行います。フォルダーのアクセス権について (22ページ) を参照してください。

フォルダーのアクセス権について

フォルダーのアクセス権では、ソフトウェアポリシー、パッチポリシー、OSビルド計画、サーバースクリプト、サブフォルダーなど、SAライブラリ内のフォルダーの内容へのアクセスを制御します。フォルダーのアクセス権は、フォルダーの直下のアイテムのみに適用されます。サブフォルダーのサブフォルダーのような階層構造内のさらに下にあるアイテムには適用されません。

詳細については、フォルダーのアクセス権の設定 (46ページ) も参照してください。

フォルダーのアクセス権のタイプ

SAクライアントの[フォルダーのプロパティ]ウィンドウでは、次のアクセス権を個別のユーザーやユーザーグループに割り当てることができます。

- フォルダーの内容のリスト表示: 階層構造内のフォルダーに移動し、フォルダーをクリックして、フォルダーのプロパティを表示し、フォルダーの内容の名前とタイプ(内容の属性を除く)を参照します。
- フォルダー内のオブジェクトの読み取り: フォルダーの内容のすべての属性を表示し、フォルダーの内容に関するオブジェクトブラウザーを開き、アクションでフォルダーの内容を使用します。

  たとえば、フォルダーにソフトウェアポリシーが含まれている場合、ユーザーはポリシーを開き(表示し)、そのポリシーを使用してサーバーを修復できます。ただし、ユーザーはポリシーを変更することはできません(修復を行うには、アクションのアクセス権とリソースのアクセス権も必要です)。

  このアクセス権を選択すると、[フォルダーの内容のリスト表示]のアクセス権が自動的に追加されます。
- フォルダー内のオブジェクトの書き込み: フォルダーの内容の表示、使用、作成、変更を行います。

  このアクセス権では、新規フォルダーや新規ソフトウェアポリシーなどのアクションが利用できます。通常、アクションを実行するには、アクションのアクセス権も必要になります。

  このアクセス権を選択すると、[フォルダーの内容のリスト表示]および[フォルダー内のオブジェクトの読み取り]のアクセス権が自動的に追加されます。
- フォルダー内のオブジェクトの実行: フォルダー内のスクリプトを実行し、フォルダーの内容の名前を表示します。

  このアクセス権を持つユーザーは、スクリプトの実行は可能ですが、読み取りまたは書き込みは許可されません。スクリプトの内容を表示するには、[フォルダー内のオブジェクトの読み取り]アクセス権と関連するアクションのアクセス権が必要です。スクリプトを作成するには、[フォルダー内のオブジェクトの書き込み]アクセス権と関連するアクションのアクセス権が必要です。

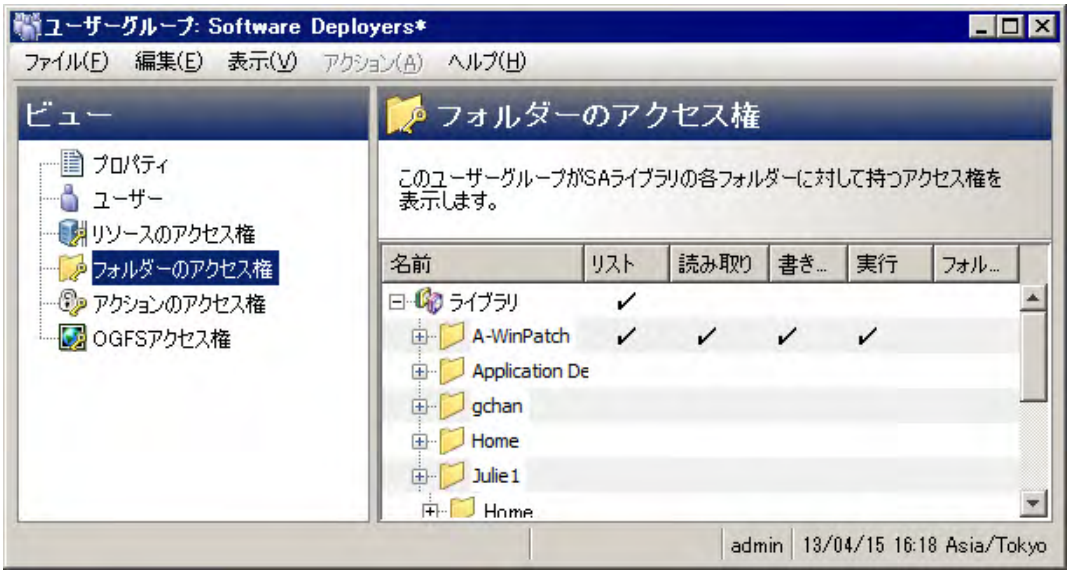
  [フォルダー内のオブジェクトの実行]アクセス権を選択すると、[フォルダーの内容のリスト表示]のアクセス権が自動的に追加されます。
- フォルダーのアクセス権の編集: アクセス権の変更やフォルダーへのカスタマーの追加を行います。

  このアクセス権を持つユーザーは、フォルダー(およびその内容)のアクセス権の管理を他のユーザーグループに委任できます。

  このアクセス権を選択すると、[フォルダーの内容のリスト表示]のアクセス権が自動的に追加されます。

図8では、Win-patchersという名前のユーザーグループで、[フォルダーのアクセス権] ビューが選択されています。このユーザーグループには、/Library/A-WinPatchという名前のフォルダーへの、リスト、読み取り、書き込み、実行のアクセス権があります。

図8 [ユーザーグループ] ウィンドウでの [フォルダーのアクセス権] ビュー



フォルダーのアクセス権とアクションのアクセス権

アクションのアクセス権では、ユーザーがSA クライアントで実行できるアクションを特定します。フォルダーのアクセス権では、ユーザーがアクセスできるSAライブラリ内のフォルダーを指定します。

フォルダーやフォルダーに含まれるアイテムでアクションを実行する場合、ユーザーはにフォルダーのアクセス権とアクションのアクセス権が必要です。たとえば、ソフトウェアポリシーをフォルダーに追加する場合、ユーザーは特定のフォルダーに対する [フォルダー内のオブジェクトの書き込み] アクセス権と [ソフトウェアポリシーの管理] のアクションのアクセス権 (読み取り/書き込み) を持つグループに属している必要があります。

フォルダー、カスタマーの制約、ソフトウェアポリシー

カスタマーをフォルダーに割り当てると、フォルダー内のソフトウェアポリシーに対する一部のアクションに、カスタマーの制約が適用されます。これらの制約はフィルター処理を通じて適用されます。ソフトウェアポリシーを関連付けることが可能なオブジェクトは、一致するカスタマーが必要です。

たとえば、`quota.rpm`パッケージをソフトウェアポリシーに追加するとします。これらのパッケージとソフトウェアポリシーは、別々のフォルダー内に存在します。ポリシーのフォルダーのカスタマーはWidget で、パッケージのフォルダーのカスタマーはAcmeです。ポリシーに対して [パッケージの追加] アクションを実行する場合、選択可能なパッケージに`quota.rpm`は含まれません。ポリシーのフォルダーのカスタマー (Widget) がフィルターとしての機能するため、ポリシーに追加できるオブジェクトが制限されます。カスタマーWidgetを`quota.rpm`のフォルダーに追加すると、`quota.rpm`をポリシーに追加できるようになります。

次に、ソフトウェアポリシーのアクションに関するカスタマーの制約を列挙します。これらの制約が適用されるのは、ソフトウェアポリシーのフォルダーに1つ以上のカスタマーが存在する場合だけです。ここに列挙されていないソフトウェアポリシーのアクション (新規フォルダーなど) には、カスタマーの制約はありません。

- ソフトウェアポリシーのアタッチ: アタッチ対象のサーバーのカスタマーは、ソフトウェアポリシーのフォルダーのカスタマーの1つである必要があります。

- ソフトウェアポリシーテンプレートのインストール: サーバーのカスタマーは、テンプレートに含まれる各ソフトウェアポリシーのフォルダーのカスタマーの1つである必要があります。

デフォルトのフォルダーのアクセス権

SAを初めてインストールすると、事前定義のユーザーグループにパッケージリポジトリなどの最上位のフォルダーに対するアクセス権が割り当てられます。新規のフォルダーを作成した場合、そのフォルダーには親のフォルダーと同じアクセス権とカスタマーが割り当てられます。

複数のユーザーグループへの所属

ユーザーが複数のユーザーグループに属している場合、ユーザーが属するすべてのグループのリソースのアクセス権とアクションのアクセス権に基づいてユーザーのアクセス権が導出されます。ユーザーのアクセス権を導出する方法は、リソースがフォルダーかどうかによって異なります。

リソースがフォルダーでない場合、導出されるアクセス権はユーザーが属するすべてのグループのリソースのアクセス権とアクションのアクセス権のクロス積になります。クロス積では、すべてのアクションのアクセス権がすべてのリソースのアクセス権に適用されます。たとえば、Jane DoeはAtlantaグループとPortlandグループの両方に属しており、それぞれのグループには表 4 に示すアクセス権が付与されています。導出されるアクセス権はクロス積であるため、JaneはWidget Inc.カスタマーに関連する管理対象サーバーでシステム診断タスクを実行できます。ただし、AtlantaグループとPortlandグループのどちらにも、この権限はありません。

表4　　クロス積アクセス権の例

リソースまたはアクション	Atlantaユーザーグループのアクセス権	Portlandユーザーグループのアクセス権
リソース: カスタマー： Widget, Inc.	読み取り/書き込み	なし
リソース: カスタマー: Acme Corp.	なし	読み取り/書き込み
アクション: システム診断	いいえ	はい

リソースが仮想化コンテナーである場合、このユーザーの導出アクセス権は累積アクセス権で、複数のユーザーグループのアクセス権のクロス積ではありません。たとえば、John Millerは表 5 に示されるSan Diegoグループと Raleighグループに属しています。Johnが仮想化インベントリフォルダー Aのサーバー Xに対する書き込みアクセス権を保持している場合、サーバー Xの電源制御操作を実行できます。Johnが仮想化インベン

トリフォルダー Bのサーバー Yに対する書き込みアクセス権を保持している場合、サーバー YのVM構成を変更できます。ただし、サーバー Yの電源制御操作を実行することも、サーバー XのVM構成を変更することもできません。

表5　　仮想化コンテナーのアクセス権の例

リソースまたはアクション	San Diegoユーザーグループのアクセス権	Raleighユーザーグループのアクセス権
リソース: ハイパーバイザーコンテナー B	なし	List
リソース: 仮想化インベントリフォルダー A	読み取り	なし
リソース: 仮想化インベントリフォルダー	なし	読み取り/書き込み
アクション: VMライフサイクル管理: 電源管理	可能	なし
アクション: VMライフサイクル管理: VMの変更	なし	可能

リソースがフォルダー (またはその内容) である場合、このユーザーの導出アクセス権は累積アクセス権で、複数のユーザーグループのアクセス権のクロス積ではありません。たとえば、Joe Smith は表 6 に示されるSunnyvaleグループとDallasグループに属しています。JoeはWebsterフォルダーでパッケージを作成できます。これは、SunnyvaleグループにWebsterフォルダーと [パッケージの管理] アクションに対する [読み取り/書き込み] アクセス権があるためです。ただし、JoeはKileyフォルダーではパッケージを作成できません。これは、そのユーザーグループにどちらのアクセス権もないためです。JoeはKileyフォルダーでOSシーケンスを作成できますが、Websterフォルダーでは作成できません。

表6　　累積アクセス権の例

リソースまたはアクション	Sunnyvaleユーザーグループのアクセス権	Dallasユーザーグループのアクセス権
リソース: フォルダー Webster	読み取り/書き込み	なし
リソース: フォルダー Kiley	なし	読み取り/書き込み
アクション: パッケージの管理	読み取り/書き込み	なし
アクション: OSシーケンスの管理	なし	読み取り/書き込み

アクセス権に基づくSAクライアントの表示の制限

SAクライアントでは、ユーザーが属するグループが [読み取り] または [読み取り/書き込み] アクセス権を持つリソースのみが表示されます。

たとえば、表7に示すアクセス権を持つBasicユーザーグループに属しているJohn Smithがログインすると、SAクライアントにはWidget Inc.のサーバーのみが表示され、Acme Corp.のサーバーは表示されません。

表7　　アクセス権と表示の制限の例

リソースまたはアクション	Basicグループのアクセス権
カスタマー : Widget, Inc.	読み取り/書き込み
カスタマー : Acme Corp.	なし
ウィザード : OSの準備	はい
ウィザード : スクリプトの実行	いいえ

サーバーを特定または表示するには、ユーザーはそのサーバーに関連するカスタマー、ファシリティ、および1つ以上のデバイスグループに対する [読み取り] (または [読み取り/書き込み]) アクセス権を持つユーザーグループに属している必要があります。この要件を満たしていない場合、ユーザーはSAクライアントでサーバーを表示できません。

事前定義のユーザーグループ

SAのインストールまたはアップグレード時には、ユーザーの役割に基づいて事前定義のユーザーグループが自動的に作成されます。その際には、読み取りまたは読み取り/書き込みのアクセス権をファシリティとカスタマーに割り当て、これらのユーザーグループに適切なアクセス権を割り当てる必要があります。事前定義のユーザーグループの使用は任意です。独自のカスタマイズしたユーザーグループを作成する場合は、デフォルトのグループを変更するのではなく、事前定義のユーザーグループのアクセス権をコピーして変更することをお勧めします。事前定義のユーザーグループの変更や削除が、SAのアップグレードによる影響を受けることはありません。表8に、事前定義のユーザーグループを示します。

表8　　事前定義のユーザーグループ

ユーザーグループ名	説明
Opsware System Administrators	SAアプリケーションの管理へのアクセス。
Superusers	SAのすべての管理対象オブジェクトや操作への完全なアクセス。
Viewers	すべてのリソースへの読み取り専用アクセス。
Reporters	レポート機能のみへのアクセス。
OS Policy Setters	OSビルド計画のインポートと定義へのアクセス。
OS Deployers	サーバーのプロビジョニングへのアクセス。
Patch Policy Setters	パッチポリシーの設定へのアクセス。
Patch Deployers	パッチのインストールへのアクセス。
Software Policy Setters	ソフトウェアポリシーの設定へのアクセス。
Software Deployers	ソフトウェアのインストールへのアクセス。

表8　事前定義のユーザーグループ

Compliance Policy Setters	コンプライアンスポリシーの定義へのアクセス。
Compliance Auditors	コンプライアンススキャンの実行へのアクセス。
Compliance Enforcers	コンプライアンスエラーの修復へのアクセス。
Virtualization Administrators	仮想化サービスの追加、変更、削除、VMおよびVMテンプレートのライフサイクルの管理、仮想化インベントリのアクセス権の管理へのアクセス。
Hypervisor Managers	(コアをSA 9.1xからアップグレードした場合) VMの作成、削除、登録へのアクセス。 アップグレードパスの詳細については、『SA 10.0 Upgrade Overview』を参照してください。
Virtual Machine Managers	VMの開始および停止へのアクセス。
VM Lifecycle Managers	VMの作成、変更、移行、複製、削除、およびVM Template Deployerのタスクへのアクセス。
VM Template Deployers	VMテンプレートからのVMの作成、VMの複製、VMゲストOSのカスタマイズ、VMの開始と停止へのアクセス。
VM Template Managers	VMテンプレートの作成、変更、削除、およびVM Lifecycle Managerのタスクへのアクセス。
Command Line Administrators	サーバーへのシェルアクセス。
Server Storage Managers	サーバーストレージの管理へのアクセス。
Storage System Managers	ストレージシステムの管理へのアクセス。
Storage Fabric Managers	ストレージファブリックの管理へのアクセス。

プライベートユーザーグループについて

プライベートユーザーグループは、SAライブラリ内のフォルダーにスクリプトを移行する目的で使用します。プライベートユーザーグループを使用してユーザーにアクセス権を割り当てないようにしてください。この場合は、通常のユーザーグループを使用します。詳細については、SAのユーザーおよびユーザーグループについて (15ページ) を参照してください。

SA管理者がユーザーを新規に作成すると、新規ユーザーのプライベートユーザーグループが自動的に作成され、新規ユーザーがプライベートユーザーグループに割り当てられます。プライベートユーザーグループの名前は、そのユーザーのユーザー名になります。

個々のプライベートユーザーグループにはSAユーザーを1つだけ含むことができます。また、各SAユーザーが属することができるプライベートユーザーグループは1つだけです。SA管理者は、続いて、アクションとリソースのアクセス権をプライベートユーザーグループに割り当てることができます。ユーザーがSAで実行できる操作は、プライベートユーザーグループに対して指定するアクセス権によって決まります。アクションのアクセス権では、ユーザーが実行できるアクションを指定します。リソースのアクセス権では、ユーザーがアクションを実行できるサーバーを指定します。Global File System (OGFS) アクセス権をプライベートユーザーグループに割り当てることはできません。

たとえば、SA管理者がユーザー名johnを使用してユーザーを新規に作成すると、プライベートユーザーグループjohnが併せて作成され、johnというデフォルトフォルダーがHomeディレクトリに作成されます。SA管理者は、続いて、アクションとリソースのアクセス権をプライベートユーザーグループjohnに割り当てることができます。

SAユーザーは複数のユーザーグループのメンバーになることが可能で、ユーザーのプライベートグループに属することができます。ただし、その場合、プライベートユーザーグループの導出されるアクセス権は、ユーザーが属するすべてのグループのリソースのアクセス権とアクションのアクセス権のクロス積にはなりません。

SAユーザーが削除されると、対応するプライベートユーザーグループは自動的に削除され、そのユーザーのデフォルトフォルダーはSAライブラリ内の/Home/deleted_usersに移動されます。

詳細については、プライベートユーザーグループのアクセス権の設定 (49ページ) を参照してください。

スーパー管理者とスーパーユーザーについて

スーパー管理者は、ユーザーとユーザーグループの作成、ユーザーグループのアクセス権の指定、およびユーザーのユーザーグループへの割り当てを行うことができるSAユーザーです。スーパー管理者は、カスタマーとファシリティの管理や、フォルダーのアクセス権の設定を行うこともできます。この章で説明するタスクでは、多くの場合、スーパー管理者としてSAクライアントにログインする必要があります。

SA をインストールすると、admin という名前のスーパー管理者がデフォルトユーザーとして作成されます。admin のパスワードはインストール時に指定します。このパスワードは、インストール後すぐに変更するようにしてください。

ベストプラクティスとして、ユーザー adminは他のユーザーグループに追加しないようにしてください。

スーパーユーザーについて

スーパーユーザーはスーパー管理者とは異なるもので、自動的にスーパー管理者になることはありません。スーパーユーザーとは、事前定義のSuperusersグループに属するユーザーです。スーパーユーザーには、ユーザーとユーザーグループの作成と変更を除く、すべてのアクションを実行するフルアクセス権があります。

ただし、スーパーユーザーは任意のサーバーに自動的にアクセスできるわけではありません。このためには、リソースのアクセス権の設定 - ファシリティ、カスタマー、デバイスグループ (44 ページ) の手順に従って、ファシリティ、カスタマー、デバイスグループへのアクセスを付与する必要があります。

スーパーユーザーを作成するには、既存のユーザーを事前定義のユーザーグループである Superusers に追加します。詳細については、事前定義のユーザーグループ (27ページ) およびユーザーグループへのユーザーの追加 (44ページ) を参照してください。

カスタマー管理者およびカスタマーグループについて

サーバーを整理してアクセス制御境界を明確にする方法として、管理対象サーバーをカスタマーごとに分離する方法があります。カスタマーは、社内の部署など、業務上の組織に関連付けられたサーバーのグループを指します。通常の場合、サーバーではカスタマー向けのアプリケーションが実行されるので、サーバーはカスタマーに関連付けられます。カスタマーの作成と管理の詳細については、『SA ユーザーガイド : Server Automation』を参照してください。

カスタマー管理者とスーパー管理者の比較

スーパー管理者は、特定のユーザーグループの管理をカスタマー管理者に委任できます。スーパー管理者と同様に、カスタマー管理者はユーザーやアクセス権をユーザーグループに割り当てることができます。ただし、カスタマー管理者は、指定されたカスタマーへのアクセスが可能なユーザーグループの変更のみを行うことができます。

カスタマー管理者は、次のような制約付きのスーパー管理者に相当します。

- スーパー管理者は、すべてのユーザーグループに対してユーザーの追加や削除を行うことができますが、カスタマー管理者は、一部のユーザーグループ (カスタマーグループに表示される特定のカスタマーへの読み取り/書き込みアクセスを持つユーザーグループ) に対してのみユーザーの追加や削除を行うことができます。
- スーパー管理者は、すべてのユーザーグループでアクセス権の変更を行うことができますが、カスタマー管理者は、一部のユーザーグループ (カスタマーグループに表示される特定のカスタマーへの [読み取り/書き込み] アクセスを持つユーザーグループ) に対してのみアクセス権の変更を行うことができます。
- スーパー管理者はSAユーザーの新規作成や削除を行うことができますが、カスタマー管理者はユーザーの作成や削除を行うことはできません。

カスタマー管理者はカスタマーグループごとに定義される

カスタマー管理者を作成するには、カスタマーグループを作成します。**カスタマーグループ**には、1つ以上のSAユーザーと1つ以上のカスタマーが含まれます。カスタマーグループ内の各ユーザーは、カスタマーグループ内のカスタマーに対するカスタマー管理者になります。カスタマー管理者が管理できるユーザーグループは、カスタマーグループに表示されるカスタマーに対する [読み取り/書き込み] アクセス権を持つユーザーグループです。

例

次の例では、Widget Co という名前のカスタマーと、Sunnyvale Admins という名前のユーザーグループについて説明します。Sunnyvale Adminsユーザーグループには、カスタマー Widget Coに対する [読み取り/書き込み] アクセス権があります。これは、Sunnyvale Admin のユーザーがカスタマー Widget Co に割り当てられたサーバーの管理を担当することを意味します。

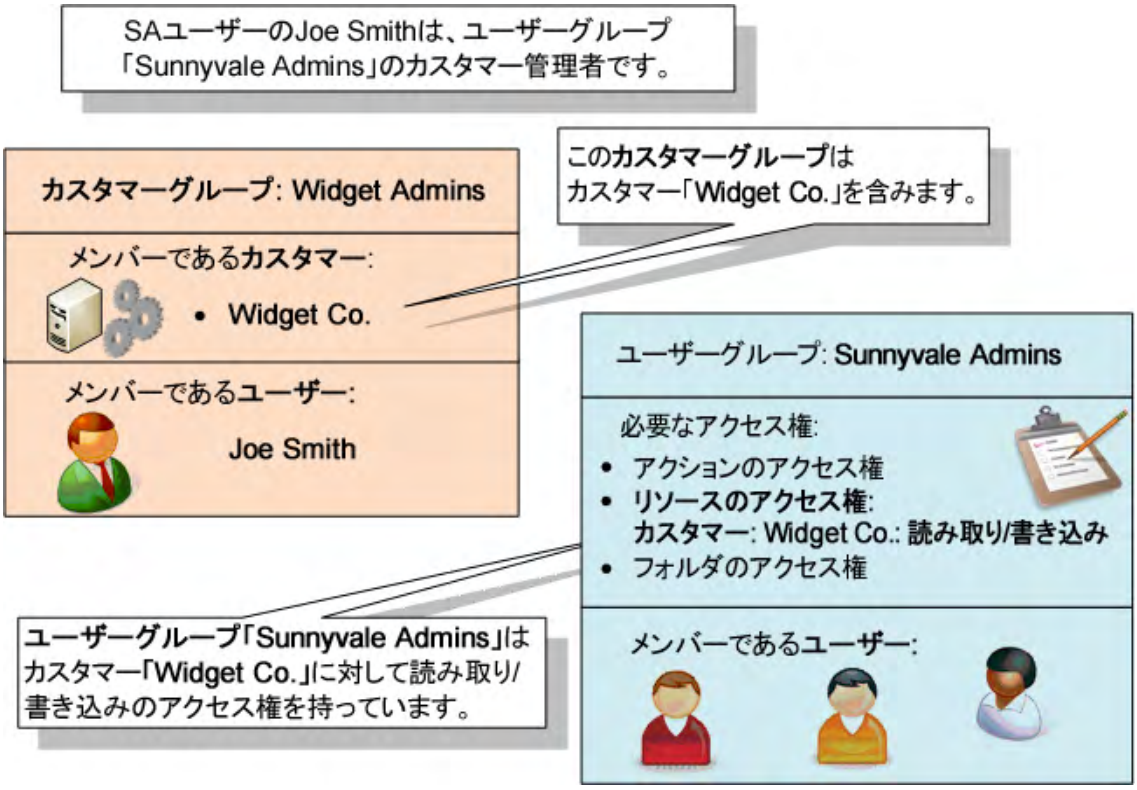
図9に、SAユーザー Joe Smithをカスタマー Widgetのカスタマー管理者にする方法を示します。カスタマーグループWidget Adminsには、ユーザーJoe Smithとカスタマー Widget Coが含まれており、Joe Smithがカスタマー Widgetのカスタマー管理者として定義されています。Joe SmithはユーザーグループSunnyvale Adminsの変更 (ユーザーの追加と削除およびアクセス権の変更) を行うことができます。

図9では、Joe SmithがユーザーグループSunnyvale Adminsを管理するのに必要な関係を示しています。

- ユーザーグループSunnyvale Adminsには、カスタマー Widget Coに対する [読み取り/書き込み] アクセス権があります。
- カスタマーグループWidget Adminsには、カスタマー Widget Coが含まれています。

- カスタマーグループWidget Adminsには、ユーザー Joe Smithが含まれています。

図9　　カスタマー管理者の定義



詳細については、カスタマー管理者とカスタマーグループの管理 - SAクライアント (55ページ) を参照してください。

セキュリティ管理者の概要

SAのセキュリティ担当者は、ユーザーとユーザーグループの作成と管理、ユーザーグループでのアクセス権の設定、およびユーザーのユーザーグループへの割り当てを行います。このセキュリティ担当者は、スーパー管理者であるユーザーとしてSAクライアントにログインする必要があります。詳細については、スーパー管理者とスーパーユーザーについて (29ページ) を参照してください。

SAのセキュリティ管理手順の概要は、次のとおりです。

1. SAのセキュリティを管理する組織内のユーザーを特定します。
2. 前の手順で特定したユーザーごとに、スーパー管理者を作成します。

   手順については、スーパー管理者の作成 (55ページ) を参照してください。
3. 管理対象サーバーが属するファシリティを確認します。

   ファシリティはデータセンターや物理的な場所を表します。それぞれの組織の事情に応じて、ファシリティにはサーバーが設置されている都市、建物、部屋の名前に基づいた名前を付けることができます。コアのファシリティの名前は、SAをインストールする際に指定します。
4. 管理対象サーバーをカスタマーに関連付けます。

SAでは、カスタマーは部門や企業などのビジネス組織に関連する一連のサーバーを表します。通常の場合、サーバーではカスタマー向けのアプリケーションが実行されるので、サーバーはカスタマーに関連付けられます。

カスタマーごとのサーバーのグループ化の詳細については、『SAユーザーガイド: Server Automation』を参照してください。

5 (オプション) デバイスグループを作成し、グループにサーバーを割り当てます。デバイスグループは管理対象サーバーをまとめるのに使用できます。

デバイスグループの詳細については、『SAユーザーガイド: Server Automation』を参照してください。

6 ユーザーグループの計画を作成します。

特定のユーザーグループが実行するSAのタスクと、対象となるサーバーを特定します。通常、ユーザーグループは役割またはジョブのカテゴリを表します。ユーザーグループの例には、UNIX System Admins、Windows Admins、DBAs、Policy Setters、Patch Admins、などがあります。詳細については、事前定義のユーザーグループ (27ページ) を参照してください。

7 事前定義のユーザーグループがニーズに合わない場合は、独自のユーザーグループを作成します。

手順については、ユーザーグループの新規作成 (41ページ) を参照してください。

8 リソースのアクセス権をユーザーグループに設定します。

これらのアクセス権では、ファシリティ、カスタマー、デバイスグループに関連するサーバーに対する読み取り/書き込みアクセスを指定します。リソースのアクセス権では、ユーザーグループのメンバーがアクセスできるサーバーを制御します。

詳細については、リソースのアクセス権の設定 - ファシリティ、カスタマー、デバイスグループ (44ページ) を参照してください。

9 アクションのアクセス権をユーザーグループに設定します。

特定のタスクの実行に必要なアクションのアクセス権を確認する場合は、アクセス権のリファレンス (249ページ) の表を参照してください。たとえば、Software Managersという名前のユーザーグループがある場合は、ユーザーのアクションに必要なソフトウェア管理のアクセス権 (265 ページ) を参照してください。

詳細については、アクションのアクセス権の設定 (46ページ) を参照してください。

10 OGFSアクセス権をユーザーグループに設定します。

OGFSアクセス権は、管理対象サーバーのファイルシステムへのアクセスが必要なアクションなどの、特定のアクションを実行するのに必要です。OGFSアクセス権は、アクセス権のリファレンス (249ページ) の表に記載されています。

手順については、OGFSアクセス権の設定 (47ページ) を参照してください。

11 SAクライアントを使用して、SAライブラリ内にフォルダーの階層構造を作成します。

SAライブラリの詳細については、『SAユーザーガイド: Server Automation』を参照してください。

12 フォルダーのアクセス権を設定します。

一般に、操作でフォルダーの内容を使用するには、フォルダーに対する読み取りアクセス権が必要、フォルダーの内容を作成または変更するには書き込みアクセス権が必要、フォルダー内に存在するスクリプトを実行するには実行アクセス権が必要です。

詳細については、フォルダーのアクセス権の設定 (46ページ) を参照してください。

13 (オプション) フォルダーのアクセス権の管理をいくつかのユーザーグループに委任します。

手順については、フォルダーのアクセス権の設定 (46ページ) を参照してください。

14 SAで新規ユーザーを作成するか、外部のLDAP (Lightweight Directory Access Protocol) ディレクトリから既存のユーザーをインポートします。

手順については、ユーザーの新規作成 (35ページ) および外部LDAPディレクトリサービスを使用した認証 (60ページ) を参照してください。

15 ユーザーを適切なグループに割り当てます。

手順については、ユーザーグループへのユーザーの追加 (44ページ) を参照してください。

Global File Systemアクセス権について

OGFS を使用するには、OGFS アクセス権を割り当てる必要があります。OGFS アクセス権は独立したアクセス権ですが、アクションのアクセス権、リソースのアクセス権、およびフォルダーのアクセス権と関係があります (アクセス権のタイプについて - アクション、リソース、フォルダーのアクセス権 (16ページ) を参照)。詳細については、OGFSアクセス権の設定 (47ページ) も参照してください。

OGFSとは、すべての管理対象サーバーと、それらのすべてのファイルシステムへのアクセスを提供する仮想ファイルシステムです。OGFSは、管理対象サーバーのファイルシステムの参照やコンプライアンスに関するサーバーのスキャンなど、SAクライアントのさまざまなアクションの基盤となります。OGFSを使用するアクションを実行するには、OGFSアクセス権を持つユーザーグループに属している必要があります。表9に、OGFSアクセス権を使用して制御する操作を示します。

表9　　OGFSアクセス権

OGFSアクセス権	このアクセス権で実行できるタスク
Global Shellの起動	Global Shellを起動できます。
サーバーへのログイン	UNIX サーバーでシェルセッションを開始できます。SA クライアントではリモート ターミナルを開くことができます。Global Shell では、roshコマンドを使用できます。
COM+データベースの読み取り	特定のログインを使用してCOM+オブジェクトを読み取ることができます。SAクライアントでは、デバイスエクスプローラーを使用して、Windowsサーバー上のこれらのオブジェクトを参照します。
サーバーファイルシステムの読み取り	特定のログインを使用して管理対象サーバーを読み取ることができます。SAクライアントでは、デバイスエクスプローラーを使用して、管理対象サーバーのファイルシステムを参照します。
IISメタベースの読み取り	特定のログインを使用して IIS メタベースのオブジェクトを読み取ることができます。SA クライアントでは、デバイスエクスプローラーを使用して、Windowsサーバー上のこれらのオブジェクトを参照します。
サーバーレジストリの読み取り	特定のログインを使用してレジストリファイルを読み取ることができます。SA クライアントでは、デバイスエクスプローラーを使用してWindowsレジストリを表示します。
RDPセッションをサーバーにリレー	WindowsサーバーでRDPセッションを開始できます。SAクライアントでは、これはWindowsサーバーのRDPクライアントウィンドウを開く [リモートターミナル] メニューです。
サーバー上でのコマンドの実行	roshユーティリティを使用して管理対象サーバーでコマンドまたはスクリプトを実行します (コマンドまたはスクリプトが既に存在する場合)。SAクライアントでは、これはデバイスエクスプローラーで アクセスするWindowsサービスで使用します。
サーバーファイルシステムの書き込み	特定のログインを使用して管理対象サーバー上のファイルを変更します。SA クライアントでは、デバイスエクスプローラーを使用して、管理対象サーバーのファイルシステムを変更できます。

OGFSアクセス権を設定する際には、[サーバーファイルシステムの書き込み] などの操作を指定し、さらに操作を適用する管理対象サーバーを指定します。管理対象サーバーを指定するには、ファシリティ、カスタマー、またはデバイスグループを選択します。また、操作を実行する管理対象サーバーのログイン名も指定します(ただし、[Global Shellの起動] の操作は例外)。

たとえば、[サーバーファイルシステムの読み取り] のアクセス権を指定する場合は、サーバーに対して Sunnyvale Servers という名前のデバイスグループを選択し、ログイン名にSAユーザー名を選択します。その後、SAクライアントで、SAユーザー jdoeがデバイスエクスプローラーで、Sunnyvale Serversデバイスグループに属するサーバーを開きます。[ビュー] ペインで、文字列jdoeが [ファイルシステム] ラベルの横に括弧で囲まれて表示されます。ユーザーがファイルシステムをドリルダウンすると、デバイスエクスプローラーにUNIXユーザー jdoeがアクセスできるファイルとディレクトリが表示されます。

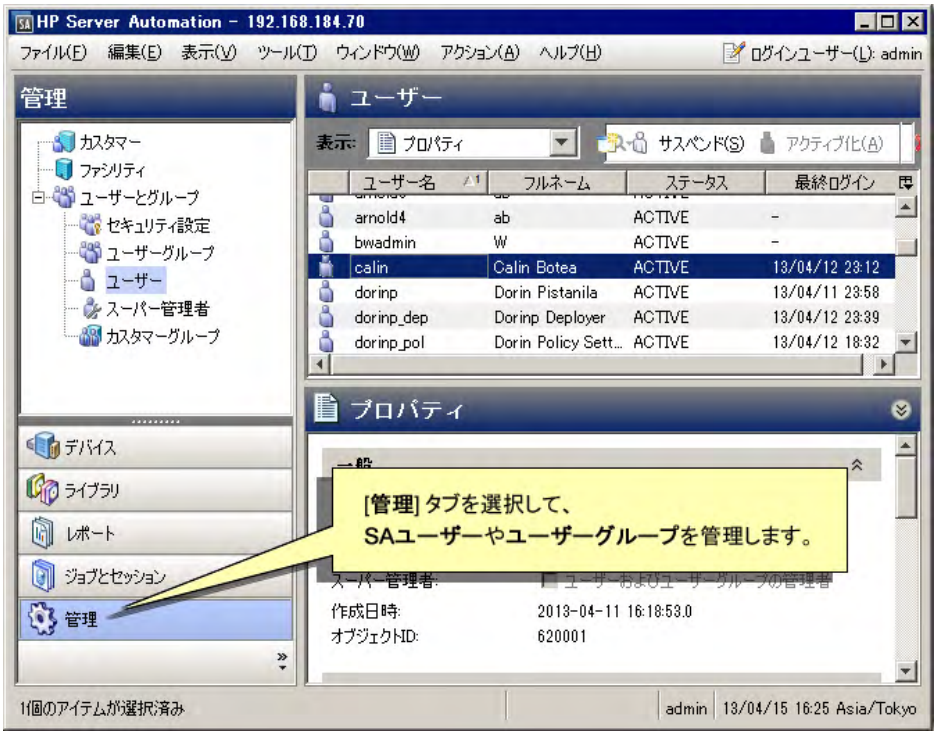
ログイン名に root などのスーパーユーザーを指定する場合は、選択するリソースで適切なサーバーに対するアクセスのみを許可するようにしてください。root の場合は、ファシリティではなく、カスタマーまたはデバイスグループごとにサーバーへのアクセスを制限してください。

[Global Shell の起動] のアクセス権では、管理対象サーバーを指定しません。これは、Global Shell セッションが特定のサーバーに関連付けられていないためです。また、このアクセス権ではログインユーザーも指定しません。SA クライアントで Global Shell セッションを開く場合は、SAの現在のログインを使用します。`ssh`コマンドでGlobal Shellセッションを開く場合は、SAのログイン (ユーザー名) が要求されます。

ユーザーの管理 - SAクライアント

この項では、SAクライアントでユーザーを管理する方法について説明します。ユーザーを管理するには、SAクライアントにスーパー管理者 (`admin`) としてログインして、[管理] タブを選択する必要があります (図10を参照)。

図10　　[管理] タブでの [ユーザー] ビュー



ユーザーの新規作成


新規ユーザーの作成方法に関するビデオを見る (1分30秒)

SAクライアントでSAユーザーを新規に作成するには、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ペインで、[管理] タブを選択します。
2. ナビゲーションペインで [ユーザーとグループ] ノードを開きます。これにより、[ユーザー] ノードが表示されます。
3. [ユーザー] ノードを選択します。これにより、すべてのSAユーザーが表示されます。
4. [**アクション**] > [**新規**] メニューを選択するか、新規の [ユーザー] アイコンを選択します。[新規ユーザー] ウィンドウが表示されます。
5. ユーザーの姓、名、フルネームを入力します。
6. 新規ユーザーがユーザーやユーザーグループを管理できるようにする場合は、[スーパー管理者] チェックボックスをオンにします。詳細については、スーパー管理者とスーパーユーザーについて (29ページ) を参照してください。
7. 新規ユーザーの連絡先情報を入力します。電子メールアドレスは必須です。
8. 新規ユーザーのログイン情報を入力します。
   - ユーザーの資格情報は、HP SAまたはSAに接続されたRSA SecurIDサーバーに保存できます。SAクライアントでユーザーパスワードを変更できるのは、資格情報ストアがHP SAの場合だけです。
   - SAユーザー名は、アルファベット、数字、ピリオド、ハイフン、アンダースコアで構成する必要があります。SAのユーザー名では、大文字と小文字を区別しません。
   - パスワードは6文字以上のASCII文字でなければなりません。また、パスワードに「\」または「^」を含めることはできません。
9. ロケール、タイムゾーン、および日付形式の設定を入力します。
10. [ユーザーグループ] ビューを選択して、ユーザーを1つまたは複数のユーザーグループに割り当てます。ユーザーをユーザーグループに割り当てると、対応するアクセス権がユーザーに付与されます。ユーザーをユーザーグループに追加する場合は、[+] ボタンを使用します。選択したユーザーグループからユーザーを削除する場合は、[-] ボタンを使用します。
11. 変更内容を破棄する場合は、[**ファイル**] > [**元に戻す**] を選択します。
12. 新しいユーザーを保存する場合は、[**ファイル**] > [**保存**] を選択します。

ユーザーのアクセス権の変更

アクセス権はすべてユーザーグループに含まれます。各ユーザーのアクセス権は、そのユーザーが属するユーザーグループによって決まります。ユーザーのアクセス権を変更するには、ユーザーが属するユーザーグループで定義されているアクセス権を変更するか、ユーザーが属するユーザーグループを変更する必要があります。詳細については、ユーザーグループへのユーザーの割り当て (40ページ) およびユーザーグループでのアクセス権の設定 - SAクライアント (44ページ) を参照してください。

ユーザーのパスワードの変更

他のSAユーザーのパスワードを変更できるのは、スーパー管理者 (admin) だけです。ユーザー名が外部のLDAPディレクトリからインポートしたものである場合、SAクライアントでパスワードを変更することはできません。詳細については、外部LDAPディレクトリサービスを使用した認証 (60ページ) を参照してください。

ユーザーのパスワードを変更するには、[ユーザー] ウィンドウでユーザーを開いて、[プロパティ] ビューを選択する必要があります。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] タブを選択します。

2 ナビゲーションペインで [ユーザーとグループ] ノードを開きます。これにより、[ユーザー] ノードが表示されます。

3 [ユーザー] ノードを選択します。これにより、すべてのSAユーザーが表示されます。

4 変更するユーザーを選択します。

5 [**アクション**] メニューを選択するか右クリックをして、[**開く**] を選択します。新しいウィンドウが開き、ユーザー情報が表示されます。

6 [プロパティ] ビューを選択します。[パスワードの変更] リンクを含むユーザーのログイン情報が表示されます。

7 [パスワードの変更] リンクを選択します。[パスワードの変更] ダイアログが表示されます。

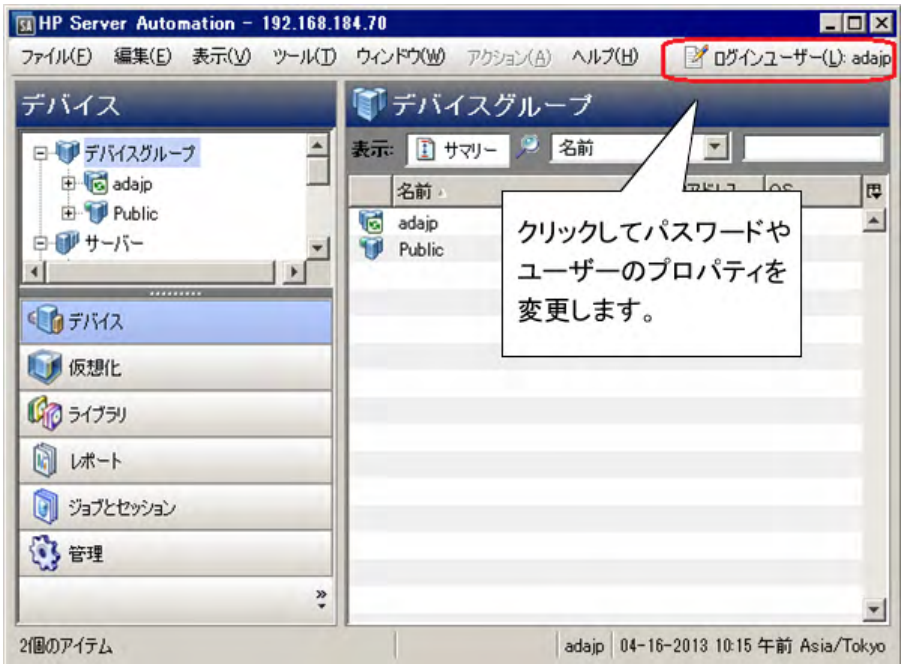
8 新しいパスワードを入力します。ユーザーのパスワードを変更した場合、変更内容は直ちに反映されます。ご注意ください。

9 [OK] を選択します。ユーザーのパスワードが変更されます。

ユーザーによる各自のパスワードやプロパティの変更

任意のユーザーは各自のパスワードやプロファイル情報を変更できます。

図11　　ユーザーによる各自のパスワードの変更



1 SAクライアント画面で、右上にある[ログインユーザー]のリンクを選択します(図11を参照)。図12のように、ユーザーのプロパティウィンドウが表示されます。

図12 ユーザーのプロパティウィンドウとパスワードの変更リンク

2 パスワードを変更するには、[パスワードの変更]リンクを選択します。パスワードを変更した場合、変更内容は直ちに反映されます。ご注意ください。

3 必要に応じて、その他のプロパティを変更します。

4 プロパティを変更した場合は、[**ファイル**] > [**保存**] を選択します。

5 [**ファイル**] > [**閉じる**] を選択します。

ユーザーの変更

SAクライアントでSAユーザーを変更するには、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] タブを選択します。

2 ナビゲーションペインで [ユーザーとグループ] ノードを開きます。これにより、[ユーザー] ノードが表示されます。

3 [ユーザー] ノードを選択します。これにより、すべてのSAユーザーが表示されます。

4 変更するユーザーを選択します。

5 [**アクション**] メニューを選択するか右クリックをして、[**開く**] を選択します。新しいウィンドウが開き、ユーザー情報が表示されます。

6 必要に応じて、ユーザーのプロパティを変更します。[**プロパティ**] ビューには、ユーザーの名前、連絡先情報、ログイン情報 (資格情報ストア、ユーザー名、パスワード変更用のリンク)、日付と時刻の設定が表示されます。ユーザーのパスワードを変更した場合、変更内容は直ちに反映されます。ご注意ください。

7 必要に応じて、ユーザーグループに対してユーザーの追加または削除を行います。**ユーザーグループ** ビューでは、ユーザーが所属するユーザーグループが表示されます。各ユーザーグループでは、そのグループに属するすべてのユーザーに一連のアクセス権が付与されます。

8 ユーザーウィンドウでは、アクセス権を表示できますが、変更することはできません。アクセス権を変更するには、ユーザーグループを変更する必要があります (ユーザーグループでのアクセス権の設定 - SA クライアント (44ページ) を参照)。

9 変更内容を破棄する場合は、[**ファイル**] > [**元に戻す**] を選択します。

10 変更内容を保存する場合は、[**ファイル**] > [**保存**] を選択します。

ユーザーの削除

SAクライアントからSAユーザーを削除するには、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] タブを選択します。

2 ナビゲーションペインで [ユーザーとグループ] ノードを開きます。これにより、[ユーザー] ノードが表示されます。

3 [ユーザー] ノードを選択します。これにより、すべてのSAユーザーが表示されます。

4 削除したいユーザーを1つまたは複数選択します。

5 [**アクション**] > [**削除**] メニューを選択するか、削除アイコンをクリックします。

特定のアクションのアクセス権を付与しているユーザーグループの確認

ユーザーが複数のユーザーグループに属している場合に、特定のアクションのアクセス権を付与しているユーザーグループを特定するには、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] タブを選択します。

2 ナビゲーションペインで [ユーザーとグループ] ノードを開きます。これにより、[ユーザー] ノードが表示されます。

3 [ユーザー] ノードを選択します。これにより、すべてのSAユーザーが表示されます。

4 表示するユーザーを選択します。

5 [**アクション**] メニューを選択するか右クリックをして、[**開く**] を選択します。新しいウィンドウが開き、ユーザー情報が表示されます。

6 [アクションのアクセス権] ビューを選択します。これにより、ユーザーが所属するユーザーグループごとに構成されたアクションのアクセス権がすべて表示されます。

7 また、任意の列の見出しを右クリックして [ユーザーグループ] 列のグループ化を解除した後に、列見出しの右端にある列セレクターを使用して [ユーザーグループ] 列を表示することもできます。これにより、各アクセス権とそのアクセス権を付与するユーザーグループが表示されます。

ユーザーのサスペンド

サスペンドされたユーザーはSAにログインできませんが、ユーザー名が削除されているわけではありません。サスペンドされたユーザーは、SAクライアントで [サスペンド済み] のステータスで示されます。ユーザーは次のようにしてサスペンドされます。

- ログイン失敗: [セキュリティ設定] タブの [ログイン失敗] チェックボックスをオンしたときに、誰かが誤ったパスワードを使用して指定された回数ログインしようとした場合、そのユーザーアカウントはサスペンドされます。[セキュリティ設定] タブにアクセスする手順については、初期パスワードのリセット (50ページ) の最初の2つの手順を参照してください。
- アカウントの非アクティブ状態: [セキュリティ設定] タブの [アカウントの非アクティブ状態] チェックボックスをオンしたときに、ユーザーが指定された日数の間ログオンしない場合、そのユーザーアカウントはサスペンドされます。
- パスワードの期限切れ: パスワードが期限切れになり、期限切れカウントが上限に達した場合に、ユーザーはサスペンドされることがあります。
- サスペンド: ユーザーのアカウントは、次の手順でサスペンドできます。ユーザーがログインしている場合は、メッセージが表示されて、ユーザーはログアウトされます。

1 SAクライアントのナビゲーションペインで、[管理] タブを選択します。

2 ナビゲーションペインで [ユーザーとグループ] ノードを開きます。これにより、[ユーザー] ノードが表示されます。

3 [ユーザー] ノードを選択します。これにより、すべてのユーザーが表示されます。

4 サスペンドするユーザーを選択します。

5 

ボタンを選択するか、[**アクション**] > [**サスペンド**] を選択します。

サスペンドされたユーザーのアクティブ化

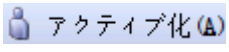
サスペンド状態のユーザーをアクティブ化するには、次の手順で実行します。

1 SAクライアントのナビゲーションペインで、[管理] タブを選択します。

2 ナビゲーションペインで [ユーザーとグループ] ノードを開きます。これにより、[ユーザー] ノードが表示されます。

3 [ユーザー] ノードを選択します。これにより、すべてのユーザーが表示されます。

4 アクティブ化するサスペンドされたユーザーを選択します。

5 

ボタンを選択するか、[**アクション**] > [**アクティブ化**] を選択します。

ユーザーグループへのユーザーの割り当て

組織内でのユーザーの役割に合わせて、SAユーザーをグループに割り当てます。SAユーザーをユーザーグループに割り当てるには、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] タブを選択します。
2. ナビゲーションペインで [ユーザーとグループ] ノードを開きます。これにより、[ユーザー] ノードが表示されます。
3. [ユーザー] ノードを選択します。これにより、すべてのSAユーザーが表示されます。
4. 割り当てるユーザーを選択します。
5. [**アクション**] メニューを選択するか右クリックをして、[**開く**] を選択します。新しいウィンドウが開き、ユーザー情報が表示されます。
6. [ユーザーグループ] ビューを選択します。ユーザーが所属するユーザーグループが表示されます。
7. [+] ボタンを選択するか、[**アクション**] > [**追加**] メニューを選択します。これにより、すべてのユーザーグループが表示されます。
8. ユーザーグループを1つまたは複数選択します。
9. [選択] ボタンをクリックします。ユーザーがユーザーグループに追加されます。
10. 変更内容を破棄する場合は、[**ファイル**] > [**元に戻す**] を選択します。
11. [**ファイル**] > [**保存**] を選択します。

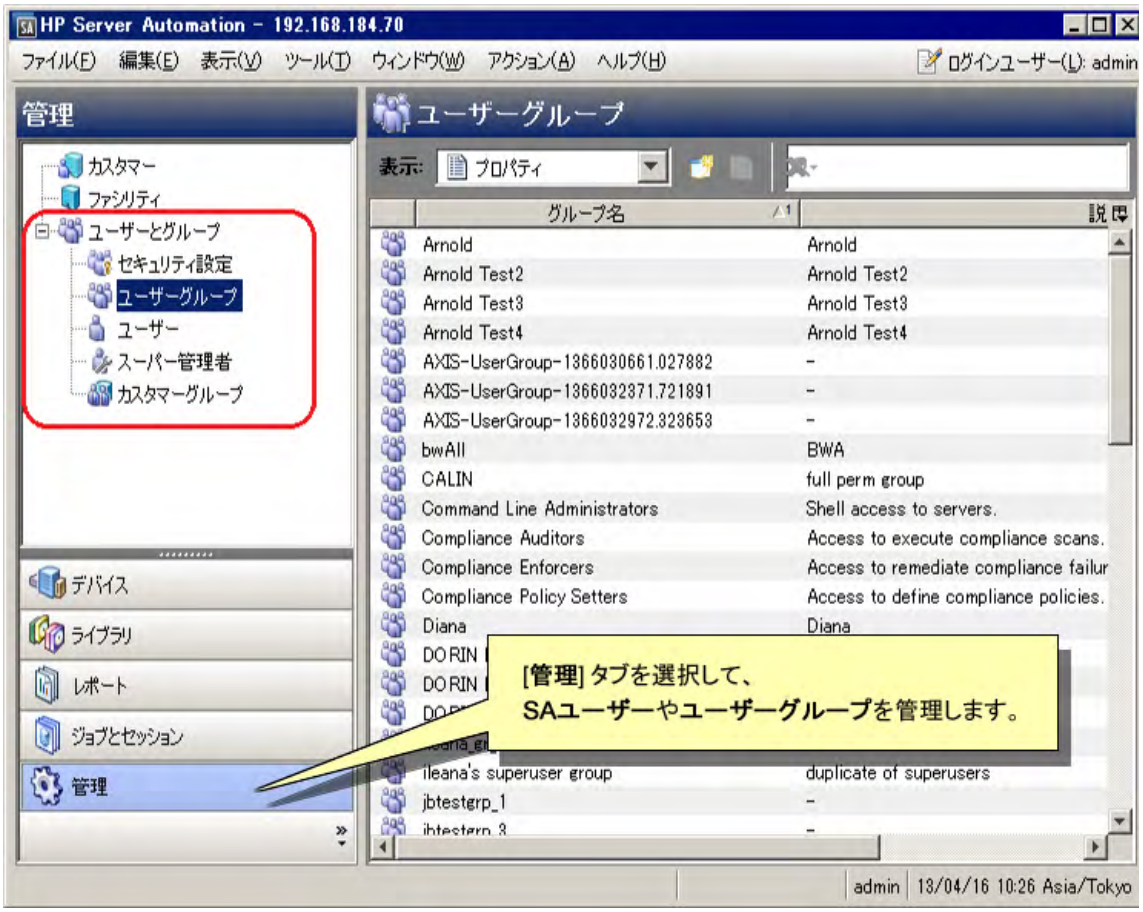
LDAPディレクトリからのユーザーのインポート

LDAPディレクトリからユーザー情報をインポートし、SAにログインする際の認証にLDAPディレクトリを使用することができます。詳細については、外部LDAPディレクトリサービスを使用した認証 (60ページ) を参照してください。

ユーザーグループの管理 - SAクライアント

この項では、ユーザーグループに関するタスクを実行する方法について説明します。ユーザーグループを管理するには、SAクライアントにスーパー管理者 (admin) としてログインして、[管理] タブを選択する必要があります (図13を参照)。

図13　[管理] タブで表示される [ユーザーグループ] ビュー



ユーザーグループの新規作成

SAクライアントでユーザーグループを新規に作成するには、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ペインで、[管理] タブを選択します。
2. ナビゲーションペインで [ユーザーとグループ] ノードを開きます。これにより、[ユーザーグループ] ノードが表示されます。
3. [ユーザーグループ] ノードを選択します。これにより、すべてのユーザーグループが表示されます。
4. [アクション] メニューを選択するか右クリックをして、[**新規**] メニューを選択します。新しいウィンドウでユーザーグループが表示されます。
5. [プロパティ] ビューを選択します。ユーザーグループの名前と説明を入力します。
6. [**ファイル**] > [**保存**] を選択し、新しいユーザーグループを保存します。
7. ユーザーグループのアクセス権を設定し、ユーザーグループにユーザーを追加します (ユーザーグループでのアクセス権の設定 - SAクライアント (44ページ) を参照)。

8 変更内容を破棄する場合は、[**ファイル**] > [**元に戻す**] を選択します。

9 変更内容を保存する場合は、[**ファイル**] > [**保存**] を選択します。

ユーザーグループの表示

SAクライアントでユーザーグループを表示するには、次の手順を実行します。

1 SAクライアントのナビゲーションペインで、[管理] タブを選択します。

2 ナビゲーションペインで [ユーザーとグループ] ノードを開きます。これにより、[ユーザーグループ] ノードが表示されます。

3 [ユーザーグループ] ノードを選択します。これにより、すべてのユーザーグループが表示されます。

4 ユーザーグループを選択して、ユーザーグループに関する情報を表示します。

5 [表示] ドロップダウンリストで、次のいずれかを選択します。

- **プロパティ** : 選択したユーザーグループの名前、説明、SAオブジェクトIDを表示します。
- **ユーザー** : 選択したユーザーグループのメンバーであるSAユーザーをすべて表示します。
- **リソースのアクセス権**: ユーザーグループのメンバーがアクセスできるカスタマー、ファシリティ、デバイスグループを表示します。また、カスタマー、ファシリティ、デバイスグループごとに、アクセスタイプ (読み取りまたは読み取り/書き込み) が表示されます。
- **フォルダーのアクセス権**: グループのメンバーに付与されたSAライブラリのフォルダーに対するアクセス権を表示します。
- **アクションのアクセス権**: ユーザーグループのメンバーがSAクライアントで実行できるアクションを表示します。
- **OGFSアクセス権**: ユーザーグループのメンバーが実行できるGlobal ShellおよびGlobal File Systemのアクション、アクセスできるリソース、Global File System、管理対象サーバーにログインしてアクションを実行するのに使用するユーザー名を表示します。

ユーザーグループのコピー

既存のユーザーグループを複製するには、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] タブを選択します。

2 ナビゲーションペインで [ユーザーとグループ] ノードを開きます。これにより、[ユーザーグループ] ノードが表示されます。

3 [ユーザーグループ] ノードを選択します。これにより、すべてのユーザーグループが表示されます。

4 コピーするユーザーグループを選択します。

5 複製アイコンを選択するか、[**アクション**] > [**複製**] メニューを選択するか、ユーザーグループを右クリックして [複製] メニューを選択します。これにより、[ユーザーグループの複製] 画面が表示されます。

6 新しいユーザーグループの名前と説明を入力します。名前は一意である必要があります。

7 [複製] ボタンを選択します。これにより、既存のユーザーグループのコピーとして新しいユーザーグループが作成されます。

ユーザーグループの変更

ユーザーグループでは、リソース、フォルダー、アクション、OGFSのアクセス権を定義します。これらのアクセス権は、そのユーザーグループに属するすべてのユーザーに付与されます。SAクライアントでユーザーグループを変更するには、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] タブを選択します。

2 ナビゲーションペインで [ユーザーとグループ] ノードを開きます。これにより、[ユーザーグループ] ノードが表示されます。

3 [ユーザーグループ] ノードを選択します。これにより、すべてのユーザーグループが表示されます。

4 ユーザーグループを選択します。これにより、画面の下部分にそのユーザーグループに関する情報が表示されます。

5 [**アクション**] メニューを選択するか右クリックをして、[**開く**] メニューを選択します。新しいウィンドウが開き、ユーザーグループが表示されます。

6 ナビゲーションペインで、次のいずれかのビューを選択します。

- **プロパティ**: 選択したユーザーグループの名前、説明、SAオブジェクト ID を表示します。ユーザーグループの名前と説明を変更できます。
- **ユーザー**: 選択したユーザーグループのメンバーであるSAユーザーをすべて表示します。ユーザーグループに対してユーザーの追加や削除を行う場合は、[+] ボタンと [-] ボタンを使用します。詳細については、ユーザーグループへのユーザーの追加 (44ページ) を参照してください。
- **リソースのアクセス権**: ユーザーグループのメンバーがアクセスできるファシリティ、カスタマー、デバイスグループを表示します。また、カスタマー、ファシリティ、デバイスグループごとに、アクセスタイプ (読み取りまたは読み取り/書き込み) が表示されます。[+] ボタンと [-] ボタンを使用して、ユーザーグループに対してファシリティ、カスタマー、デバイスグループの追加や削除を行い、アクセスタイプを設定します。詳細については、リソースのアクセス権の設定 - ファシリティ、カスタマー、デバイスグループ (44ページ) を参照してください。
- **フォルダーのアクセス権**: SA ライブラリのフォルダーとそのユーザーグループに対して各フォルダーに付与されたアクセス権を表示します。フォルダーを選択するか、[**アクション**] メニューを選択するか右クリックをして、[**フォルダーのプロパティ**] メニューを選択して、フォルダーのプロパティウィンドウを表示します。[アクセス権] タブを選択して、アクセス権の表示と変更を行います。詳細については、フォルダーのアクセス権の設定 (46ページ) を参照してください。
- **アクションのアクセス権**: ユーザーグループのメンバーが実行できるタスクを表示します。変更対象のアクセス権の横にある [アクセス権] 列を選択して、新しいアクセス権を選択します。詳細については、アクションのアクセス権の設定 (46ページ) を参照してください。
- **OGFSアクセス権**: OGFSおよびGlobal Shell (OGSH) のアクセス権を表示します。[+] アイコンまたは [-] アイコンを選択して、アクセス権の追加や削除を行います。詳細については、OGFS アクセス権の設定 (47ページ) を参照してください。

7 変更内容を破棄する場合は、[**ファイル**] > [**元に戻す**] を選択します。

8 [**ファイル**] > [**保存**] を選択します。

ユーザーグループの削除

1つまたは複数の既存のユーザーグループを削除するには、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] タブを選択します。

2 ナビゲーションペインで [ユーザーとグループ] ノードを開きます。これにより、[ユーザーグループ] ノードが表示されます。

3 [ユーザーグループ] ノードを選択します。これにより、すべてのユーザーグループが表示されます。

4 削除する1つまたは複数のユーザーグループを選択します。

5 削除アイコンを選択するか、[**アクション**] > [**削除**] メニューを選択するか、ユーザーグループを右クリックして [**削除**] メニューを選択するか、キーボードの [Delete] キーを押します。

ユーザーグループへのユーザーの追加

1つまたは複数のユーザーをユーザーグループに追加するには、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] タブを選択します。

2 ナビゲーションペインで [ユーザーとグループ] ノードを開きます。これにより、[ユーザーグループ] ノードが表示されます。

3 [ユーザーグループ] ノードを選択します。これにより、すべてのユーザーグループが表示されます。

4 ユーザーグループを選択します。これにより、画面の下部分にそのユーザーグループに関する情報が表示されます。

5 [**アクション**] メニューを選択するか右クリックをして、[**開く**] メニューを選択します。新しい画面が開き、ユーザーグループが表示されます。

6 ナビゲーションペインで [ユーザー] ビューを選択します。ユーザーグループのメンバーであるユーザーがすべて表示されます。

7 [+] アイコンを選択するか、[**アクション**] > [**追加**] メニューを選択します。これにより、すべてのSAユーザーが表示されます。

8 ユーザーを1人または複数選択します。

9 [選択] ボタンをクリックします。ユーザーがユーザーグループに追加されます。

10 変更内容を破棄する場合は、[**ファイル**] > [**元に戻す**] を選択します。

11 [**ファイル**] > [**保存**] を選択します。

ユーザーグループでのアクセス権の設定 - SAクライアント

この項では、ユーザーグループの**アクションのアクセス権**、**リソースのアクセス権**、**フォルダーのアクセス権**、**OGFSアクセス権**の設定方法について説明します。これらのアクセス権はすべて、ユーザーグループのメンバーになっているユーザーに割り当てられます。

リソースのアクセス権の設定 - ファシリティ、カスタマー、デバイスグループ

管理対象サーバーはすべて、カスタマー、ファシリティ、デバイスグループ別にグループ化されます。[**リソースのアクセス権**] ビューには、そのユーザーグループでアクセスできる**カスタマー**、**ファシリティ**、**デバイスグループ**が表示されます。詳細については、リソースのアクセス権について (19ページ) を参照してください。

ユーザーグループのリソースのアクセス権を変更するには、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] タブを選択します。

2 ナビゲーションペインで [ユーザーとグループ] ノードを開きます。これにより、[ユーザーグループ] ノードが表示されます。

3 [ユーザーグループ] ノードを選択します。これにより、すべてのユーザーグループが表示されます。

4 ユーザーグループを選択します。これにより、画面の下部分にそのユーザーグループに関する情報が表示されます。

5 [**アクション**] メニューを選択するか右クリックをして、[**開く**] メニューを選択します。新しい画面が開き、ユーザーグループが表示されます。

6 ナビゲーションペインで、[リソースのアクセス権] ビューを選択します。ユーザーグループでアクセスできるすべてのファシリティ、カスタマー、デバイスグループが表示されます。

7 カスタマーへのアクセスを追加するには、次の手順を実行します。

   a [カスタマー] の見出しの下にある [+] アイコンをクリックします。別ウィンドウが開き、すべてのカスタマーの一覧が表示されます。

b カスタマーを1つまたは複数選択します。

c [読み取り] または [読み取り/書き込み] のいずれかのアクセスを選択します。

d [追加] ボタンをクリックします。

8 カスタマーへのアクセスを削除するには、カスタマーを選択して [-] ボタンを選択します。

9 ファシリティへのアクセスを追加するには、次の手順を実行します。

a [ファシリティ] の見出しの下にある [+] アイコンをクリックします。別ウィンドウが開き、すべてのファシリティの一覧が表示されます。

b ファシリティを1つまたは複数選択します。

c [読み取り] または [読み取り/書き込み] のいずれかのアクセスを選択します。

d [追加] ボタンをクリックします。

10 ファシリティへのアクセスを削除するには、ファシリティを選択して [-] ボタンを選択します。

11 すべてのデバイスグループへのアクセスを追加するには、[すべてのデバイスグループへのアクセスを許可] チェックボックスをオンにします。

12 一部のデバイスグループへのアクセスを追加するには、次の手順を実行します。

a [すべてのデバイスグループへのアクセスを許可] チェックボックスをオフにします。これにより、[+] アイコンが表示されます。

b [デバイスグループ] の見出しの下にある [+] アイコンを選択します。別ウィンドウが開き、すべてのパブリックデバイスグループの一覧が表示されます。

c デバイスグループを1つまたは複数選択します。

d [読み取り] または [読み取り/書き込み] のいずれかのアクセスを選択します。

e [追加] ボタンをクリックします。

13 デバイスグループへのアクセスを削除するには、デバイスグループを選択して [-] ボタンを選択します。

14 変更内容を破棄する場合は、[**ファイル**] > [**元に戻す**] を選択します。

15 [**ファイル**] > [**保存**] を選択します。

アクションのアクセス権の設定

この項では、ユーザーグループに対するアクションのアクセス権を設定する方法について説明します。詳細については、アクションのアクセス権について (18ページ) を参照してください。

ユーザーグループのアクションのアクセス権を変更するには、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] タブを選択します。
2. ナビゲーションペインで [ユーザーとグループ] ノードを開きます。これにより、[ユーザーグループ] ノードが表示されます。
3. [ユーザーグループ] ノードを選択します。これにより、すべてのユーザーグループが表示されます。
4. ユーザーグループを選択します。これにより、画面の下部分にそのユーザーグループに関する情報が表示されます。
5. [**アクション**] メニューを選択するか右クリックをして、[**開く**] メニューを選択します。新しい画面が開き、ユーザーグループが表示されます。
6. ナビゲーションペインで、[アクションのアクセス権] ビューを選択します。
7. [名前] と [説明] の列を使用して変更するアクセス権を特定します。列を右クリックしてその列をグループ化またはグループ化解除すると、参照しやすくなります。
8. [アクセス権] 列でアクセス権の現在の値を選択します。これにより、選択可能な値がドロップダウンリストに表示されます。値を選択します。

複数のアクセス権を同時に選択して設定することができます。複数のアクセス権を選択するには、マウスをドラッグするか、またはキーボードの [Shift] キーや [Control] キーとマウスを使用します。右クリックして選択可能なアクセス権の値を表示し、目的の値を選択します。

> アクセス権の値が薄く表示されている場合、アクセス権が他のアクセス権によって制御されていることを示します。したがって、そのアクセス権を先に変更する必要があります。たとえば、[アプリケーションの作成] と [アプリケーションデプロイメントの管理] のアクセス権はいずれも、[アプリケーションデプロイメントへのアクセス] を [はい] に設定してから割り当てる必要があります。

9. 変更内容を破棄する場合は、[**ファイル**] > [**元に戻す**] を選択します。
10. [**ファイル**] > [**保存**] を選択します。

フォルダーのアクセス権の設定

この項では、ユーザーグループに対するフォルダーのアクセス権を設定する方法について説明します。詳細については、フォルダーのアクセス権について (22ページ) を参照してください。

ユーザーグループのフォルダーのアクセス権を変更するには、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] タブを選択します。
2. ナビゲーションペインで [ユーザーとグループ] ノードを開きます。これにより、[ユーザーグループ] ノードが表示されます。
3. [ユーザーグループ] ノードを選択します。これにより、すべてのユーザーグループが表示されます。
4. ユーザーグループを選択します。これにより、画面の下部分にそのユーザーグループに関する情報が表示されます。
5. [**アクション**] メニューを選択するか右クリックをして、[**開く**] メニューを選択します。新しい画面が開き、ユーザーグループが表示されます。
6. ナビゲーションペインで、[フォルダーのアクセス権] ビューを選択します。SAライブラリのすべてのフォルダーと現在のアクセス権が表示されます。
7. 変更するフォルダーを選択します。

8 [**アクション**] メニューを選択するか右クリックをして、[**フォルダーのプロパティ**] メニューを選択します。新しいウィンドウが開き、フォルダーのプロパティが表示されます。

9 [アクセス権] タブを選択します。そのフォルダーにアクセスできるすべてのユーザーとユーザーグループが表示されます。

10 ユーザーまたはユーザーグループを選択します。ウィンドウの下部に現在のアクセス権が表示されます。

11 画面の下部でアクセス権を設定します。

12 必要に応じて、他のユーザーまたはユーザーグループにアクセスを割り当てる場合は、[追加] ボタンを選択し、1つまたは複数のユーザーまたはユーザーグループを選択して、[追加] ボタンを選択します。

13 必要に応じて、ユーザーまたはユーザーグループのアクセスを削除する場合は、ユーザーまたはユーザーグループを選択して、[削除] ボタンを選択します。

14 [OK] ボタンを選択します。

15 変更内容を破棄する場合は、[**ファイル**] > [**元に戻す**] を選択します。

16 [**ファイル**] > [**保存**] を選択します。

OGFSアクセス権の設定

この項では、ユーザーグループに対するOGFSアクセス権を設定する方法について説明します。詳細については、Global File Systemアクセス権について (33ページ) を参照してください。

1 SAクライアントのナビゲーションペインで、[管理] タブを選択します。

2 ナビゲーションペインで [ユーザーとグループ] ノードを開きます。これにより、[ユーザーグループ] ノードが表示されます。

3 [ユーザーグループ] ノードを選択します。これにより、すべてのユーザーグループが表示されます。

4 ユーザーグループを選択します。これにより、画面の下部分にそのユーザーグループに関する情報が表示されます。

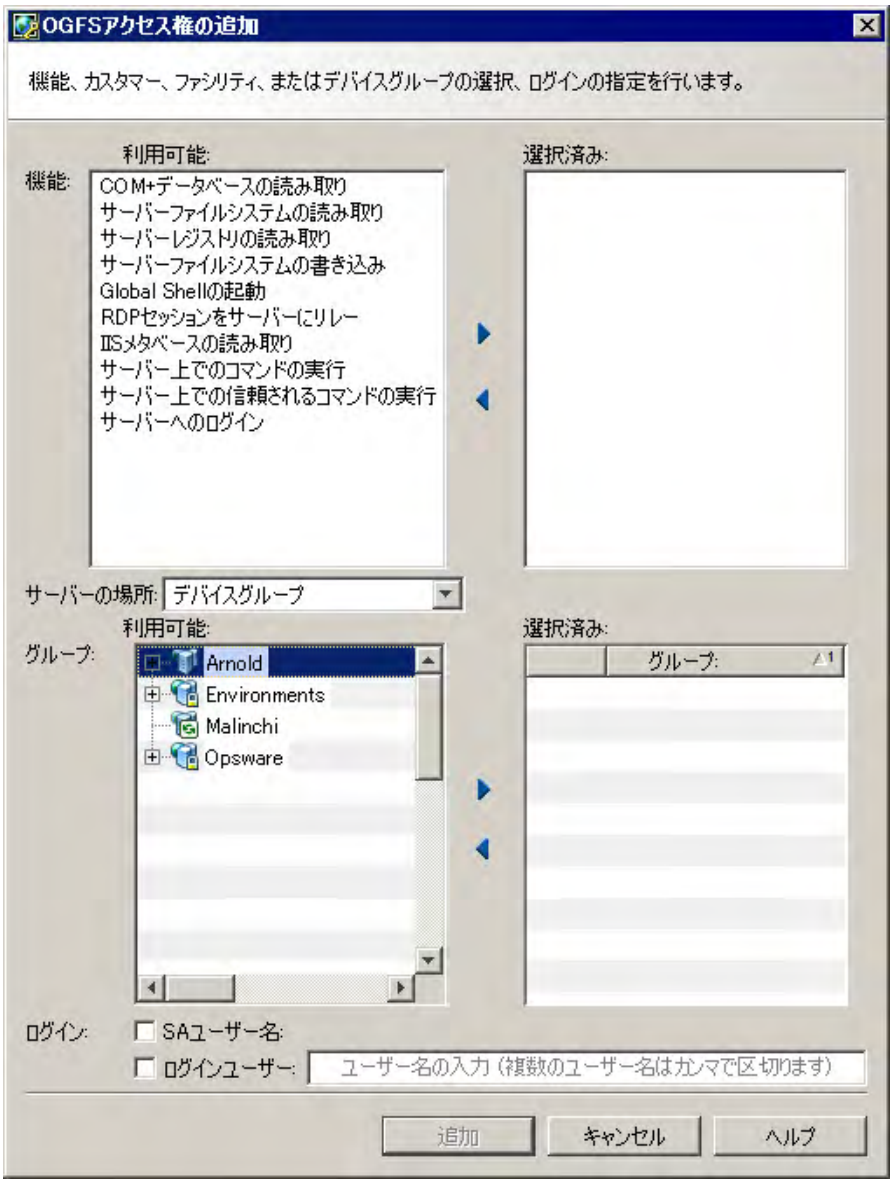
5 [**アクション**] メニューを選択するか右クリックをして、[**開く**] メニューを選択します。新しいウィンドウが開き、ユーザーグループが表示されます。

6 ナビゲーションペインで、OGFSアクセス権を選択します。現在のOGFSアクセス権が表示されます。

7 アクセス権を追加するには、[+] アイコンを選択します。次のように、[OGFSアクセス権の追加] ウィンドウが表示されます。この画面は、次の3つの部分で構成されます。

- [**機能**] には、OGFSとOGSHでのタスク実行に使用されるアクションのアクセス権が一覧表示されます。
- [**グループ**] には、アクションを実行するサーバーが一覧表示されます。サーバーは、ファシリティ、カスタマー、またはデバイスグループごとに表示されます。
- [**ログイン**] では、OGFSとOGSHによるサーバー接続で使用するログイン名を指定します。

図14 [OGFSアクセス権の追加] ウィンドウ



8 [機能] セクションで、[利用可能] リストからアクセス権を割り当てるOGFSアクションを選択します。矢印を選択して、これらのアクションを [選択済み] リストに移動します。

9 [グループ] セクションで、[サーバーの場所] ドロップダウンリストから必要なサーバーグループのタイプを選択します。カスタマー、ファシリティ、またはデバイスグループのいずれかを選択します。

10 カスタマー、ファシリティ、またはデバイスグループを1つまたは複数選択します。矢印を選択して、これらを [選択済み] リストに移動します。

11 OGFSユーザーにそれぞれのSAユーザー名を使用してログインさせる場合は、[ログイン] セクションで、[SA ユーザー名] チェックボックスをオンにします。それ以外の場合は、[ログイン ユーザー] チェックボックスをオンにして、OGFSに対応したサーバーにログインするためのユーザー名を1つまたは複数入力します。

12 [追加] ボタンをクリックします。

13 アクセス権を削除する場合は、1つまたは複数のアクセス権を選択して [-] ボタンをクリックします。

14 変更内容を破棄する場合は、[**ファイル**] > [**元に戻す**] を選択します。

15 変更内容を保存する場合は、[**ファイル**] > [**保存**] を選択します。

OGFSアクセス権の詳細については、Global File Systemアクセス権について (33ページ) を参照してください。

プライベートユーザーグループのアクセス権の設定

プライベートユーザーグループは、SA ライブラリ内のフォルダーにスクリプトを移行する目的で使用します。プライベートユーザーグループを使用してユーザーにアクセス権を割り当てないようにしてください。この場合は、通常のユーザーグループを使用します。詳細については、SAのユーザーおよびユーザーグループについて (15ページ) を参照してください。

プライベートユーザーグループについては、プライベートユーザーグループについて (28ページ) を参照してください。プライベートユーザーグループを変更するには、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] タブを選択します。

2 ナビゲーションペインで [ユーザーとグループ] ノードを開きます。これにより、[ユーザー] ノードが表示されます。

3 [ユーザー] ノードを選択します。これにより、すべてのSAユーザーが表示されます。

4 プライベートユーザーグループのアクセス権を設定するユーザーを選択します。

5 [**アクション**] メニューを選択するか右クリックをして、[**開く**] を選択します。新しいウィンドウが開き、ユーザー情報が表示されます。

6 [ユーザーグループ] ビューを選択します。ユーザーがメンバーとして所属するすべてのユーザーグループ (プライベートユーザーグループを含む) が表示されます。プライベートユーザーグループの名前はユーザー名と同じです。

7 プライベートユーザーグループを選択します。

8 [**アクション**] メニューを選択するか右クリックをして、[**開く**] を選択します。新しい画面が開き、プライベートユーザーグループが表示されます。

9 リソースのアクセス権を変更する場合は、[リソースのアクセス権] ビューを選択します。詳細については、リソースのアクセス権の設定 - ファシリティ、カスタマー、デバイスグループ (44ページ) を参照してください。

10 アクションのアクセス権を変更する場合は、[アクションのアクセス権] ビューを選択します。詳細については、アクションのアクセス権の設定 (46ページ) を参照してください。

11 変更内容を破棄する場合は、[**ファイル**] > [**元に戻す**] を選択します。

12 変更内容を保存する場合は、[**ファイル**] > [**保存**] を選択します。

パスワード、アカウント、セッションセキュリティのポリシーの設定 - SAクライアント

いくつかのポリシーを設定することにより、SAユーザーパスワードの保護、非アクティブなユーザーアカウントの自動無効化、非アクティブなユーザーセッションの自動ロックを行うことができます。次の手順を実行します。

1 SAクライアントで、[管理] タブを選択します。

2 ナビゲーションパネルで、[ユーザーとグループ] ノードを開きます。これにより、[セキュリティ設定] ノードが表示されます。

3 [セキュリティ設定] ノードを選択します。パスワードポリシー設定が表示されます。

4 次のポリシーのうちのいくつかを設定します。

- **リセット**: ユーザーがSAに最初にログインしたときにパスワードを強制的にリセットさせます。
- **有効期限**: 指定した日数を経過した時点でユーザーにパスワードを強制的に変更させます。[ログイン可能回数] を指定して、パスワードの変更を先延ばしにできる回数を指定することもできます。
- **保持**: 以前のパスワードを保存する数を指定します。これを設定すると、ユーザーはパスワードを再利用できなくなります。たとえば、10と指定した場合、ユーザーは以前に使用した10個のパスワードを再利用できなくなります。
- **ログイン失敗**: 間違ったパスワードによるログインの試行を何回まで許容するかを指定します。この回数を超えると、ユーザーアカウントはサスペンドされます。ユーザーアカウントがサスペンドされたときに、アカウントを再度アクティブ化するには、[管理] > [ユーザーとグループ] を選択し、ユーザーを選択して [アクティブ化] ボタンを選択します。詳細については、ユーザーのサスペンド (39ページ) を参照してください。
- **アカウントの非アクティブ状態**: 使用されていないユーザーアカウントを許容する期間を指定します。指定された日数を超えてユーザーアカウントが使用されない場合、ユーザーアカウントはサスペンドされます。ユーザーアカウントがサスペンドされたときに、アカウントを再度アクティブ化するには、[管理] > [ユーザーとグループ] を選択し、ユーザーを選択して [アクティブ化] ボタンを選択します。詳細については、ユーザーのサスペンド (39ページ) を参照してください。
- **SA クライアントセッションの非アクティブ状態**: 使用されていないユーザーセッションを許容する期間を指定します。この期間を過ぎると、SAクライアントはロックされます。値は分単位で指定します。

5 以前に保存した設定に戻す場合は、[**表示**] > [**更新**] メニューを選択するか、キーボードの [F5] キーを押します。

6 必要な値の設定が済んだら、[保存] ボタンを選択します。

初期パスワードのリセット

ユーザーがSAに最初にログインしたときにパスワードをリセットさせるには、次の手順を実行します。

1 SAクライアントで、[管理] タブを選択します。

2 ナビゲーションパネルで、[ユーザーとグループ] ノードを開きます。これにより、[セキュリティ設定] ノードが表示されます。

3 [セキュリティ設定] ノードを選択します。パスワードポリシー設定が表示されます。

4 [最初のログイン時にパスワードをリセット] チェックボックスをオンにします。

5 [保存] ボタンをクリックします。

パスワードの有効期限の設定

一定の日数が経過した後にSAユーザーにパスワードを変更させるには、次の手順を実行します。

1 SAクライアントで、[管理] タブを選択します。

2 ナビゲーションパネルで、[ユーザーとグループ] ノードを開きます。これにより、[セキュリティ設定] ノードが表示されます。

3 [セキュリティ設定] ノードを選択します。パスワードポリシー設定が表示されます。

4 [有効期限] チェックボックスをオンにします。

5 パスワードの有効期限が切れるまでの日数を入力します。

6 ユーザーをサスペンドせずに古いパスワードでのログインを許可する回数を入力します。

7 [保存] ボタンをクリックします。

サスペンドされたユーザーをアクティブ化する場合は、サスペンドされたユーザーのアクティブ化 (39 ページ) を参照してください。

古いパスワードの再利用の禁止

ユーザーの古いパスワードを保存して、ユーザーが古いパスワードを再利用しないようにする場合は、次の手順を実行します。

1 SAクライアントで、[管理] タブを選択します。

2 ナビゲーションパネルで、[ユーザーとグループ] ノードを開きます。これにより、[セキュリティ設定] ノードが表示されます。

3 [セキュリティ設定] ノードを選択します。パスワードポリシー設定が表示されます。

4 [保持] チェックボックスをオンにします。

5 保存して再利用を禁止する古いパスワードの数を入力します。

6 [保存] ボタンをクリックします。

ログイン失敗後のユーザーアカウントのサスペンド

何者かが一定の回数を超えて間違ったパスワードを使ってログインしようとした場合に、ユーザーアカウントをサスペンドできます。

1 SAクライアントで、[管理] タブを選択します。

2 ナビゲーションパネルで、[ユーザーとグループ] ノードを開きます。これにより、[セキュリティ設定] ノードが表示されます。

3 [セキュリティ設定] ノードを選択します。パスワードポリシー設定が表示されます。

4 [ログイン失敗] チェックボックスをオンにします。

5 ユーザーアカウントをサスペンドするログイン失敗回数を入力します。誰かがいずれかのアカウントにログインしようとして、指定した回数を超えてログインに失敗した場合、ユーザーアカウントはサスペンドされます。

6 [保存] ボタンをクリックします。

サスペンドされたユーザーをアクティブ化する場合は、サスペンドされたユーザーのアクティブ化 (39 ページ) を参照してください。

非アクティブなユーザーアカウントのサスペンド

一定期間ログインが行われない場合に、そのユーザーアカウントを自動的にサスペンドできます。

1 SAクライアントで、[管理] タブを選択します。

2 ナビゲーションパネルで、[ユーザーとグループ] ノードを開きます。これにより、[セキュリティ設定] ノードが表示されます。

3 [セキュリティ設定] ノードを選択します。パスワードポリシー設定が表示されます。

4 [アカウントの非アクティブ状態] チェックボックスをオンにします。

5 日数を入力します。ユーザーが指定した日数を超えてログインしない場合、そのユーザーアカウントはサスペンドされます。

6 [保存] ボタンをクリックします。

サスペンドされたユーザーをアクティブ化する場合は、サスペンドされたユーザーのアクティブ化 (39 ページ) を参照してください。

非アクティブなセッションのロック

ユーザーが一定期間非アクティブである場合に、SAクライアントセッションを自動的にロックすることができます。ユーザーがセッションのロックを解除するには、パスワードを入力する必要があります。

1. SAクライアントで、[管理] タブを選択します。
2. ナビゲーションパネルで、[ユーザーとグループ] ノードを開きます。これにより、[セキュリティ設定] ノードが表示されます。
3. [セキュリティ設定] ノードを選択します。パスワードポリシー設定が表示されます。
4. [SAクライアントセッションの非アクティブ状態] チェックボックスをオンにします。
5. 時間を分単位で入力します。ログインしたユーザーが指定した時間の間SAクライアントを使用しなかった場合、SAクライアントがロックされ、ユーザーはパスワードを入力しなければならなくなります。
6. [保存] ボタンをクリックします。

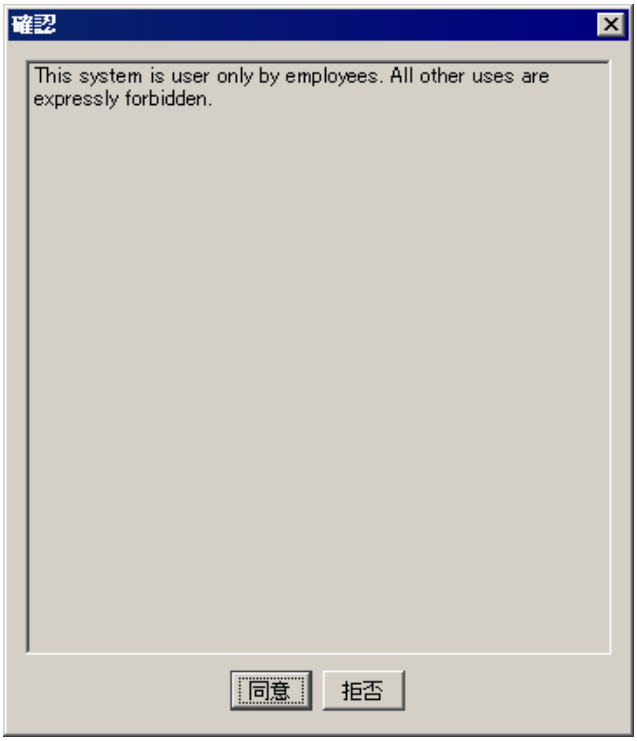
ユーザーログイン時の同意の表示

ユーザーがログインしたときにメッセージを表示して、メッセージ内容の承認を要求することができます。次の手順を実行します。

1. SAクライアントで、[管理] タブを選択します。
2. ナビゲーションパネルで、[ユーザーとグループ] ノードを開きます。これにより、[セキュリティ設定] ノードが表示されます。
3. [セキュリティ設定] ノードを選択します。これにより、ユーザー同意設定とバナー設定が表示されます。
4. [ユーザー同意設定] で、[表示の有効化] を選択します。
5. ユーザー同意に表示するテキストを入力します。
6. [保存] ボタンをクリックします。

ユーザーがSAクライアントにログインすると、次のように指定したメッセージが表示されます。ユーザーはメッセージを承認する必要があります。

図15　ユーザーログイン時の [確認] ダイアログ



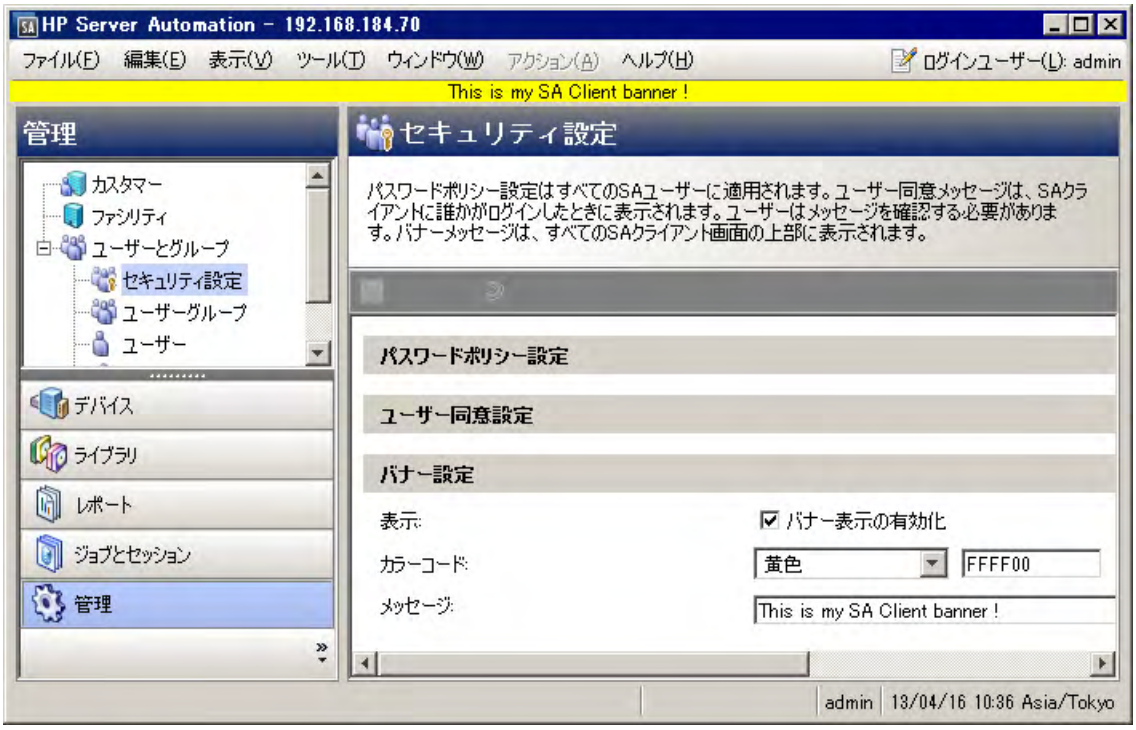
SAクライアント画面でのバナーの表示

SAクライアントの画面ごとに、任意の背景色を使用してメッセージを表示することができます。次の手順を実行します。

1. SAクライアントで、[管理] タブを選択します。
2. ナビゲーションパネルで、[ユーザーとグループ] ノードを開きます。これにより、[セキュリティ設定] ノードが表示されます。
3. [セキュリティ設定] ノードを選択します。これにより、ユーザー同意設定とバナー設定が表示されます。
4. [バナー設定] で、[バナー表示の有効化] を選択します。
5. ドロップダウンリストから色を選択するか、000000～FFFFFFの16進数のカラーコードを指定します。最初の2つの数字が赤の要素、次の2つの数字が緑の要素、最後の2つの数字が青の要素です。
6. バナーに表示するテキストを入力します。

7 [保存] ボタンをクリックします。次のように、SAクライアントのすべての画面の上部にバナーが表示されます。

図16 SAクライアントのバナー設定



スーパー管理者の管理 - SAクライアント

スーパー管理者は、ユーザーグループへのアクセス権の割り当てとユーザーグループへのユーザーの割り当てを行うことができます。スーパー管理者を管理するには、スーパー管理者としてSAクライアントにログインする必要があります。SAを最初にインストールしたときのデフォルトのスーパー管理者は、ユーザー`admin`です。

詳細については、スーパー管理者とスーパーユーザーについて (29ページ) も参照してください。

SAのすべてのスーパー管理者の表示

SAのすべてのスーパー管理者を表示するには、次の手順を実行します。

1 SAクライアントのナビゲーションペインで、[管理] タブを選択します。

2 ナビゲーションペインで [ユーザーとグループ] ノードを開きます。これにより、[スーパー管理者] ノードが表示されます。

3 [スーパー管理者] ノードを選択します。関連するすべてのスーパー管理者が表示されます。

スーパー管理者の作成

SAスーパー管理者は、SAユーザーとユーザーグループの作成と変更を行うことができるSAユーザーです。SAのスーパー管理者を作成するには、ユーザーの新規作成 (35ページ) の手順を実行し、[スーパー管理者] チェックボックスをオンにします。

既存のユーザーをSAスーパー管理者にするには、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] タブを選択します。
2. ナビゲーションペインで [ユーザーとグループ] ノードを開きます。これにより、[スーパー管理者] ノードが表示されます。
3. [スーパー管理者] ノードを選択します。関連するすべてのスーパー管理者が表示されます。
4. [**アクション**] > [**追加**] メニューを選択するか、新規ユーザーアイコンを選択します。SAのすべてのユーザーのリストが表示されます。
5. スーパー管理者にする1つまたは複数のユーザーを選択します。
6. [選択] ボタンをクリックします。これにより、選択したユーザーがスーパー管理者になります。

スーパー管理者の削除

SAユーザーからスーパー管理者の権限を削除して、ユーザーのその他のアクセス権を維持する場合は、ユーザーの変更 (38ページ) の手順を実行して、[スーパー管理者] チェックボックスをオフにします。または、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] タブを選択します。
2. ナビゲーションペインで [ユーザーとグループ] ノードを開きます。これにより、[スーパー管理者] ノードが表示されます。
3. [スーパー管理者] ノードを選択します。関連するすべてのスーパー管理者が表示されます。
4. ユーザーを1人または複数選択します。
5. [**アクション**] > [**削除**] メニューを選択するか、右クリックして [削除] を選択するか、または削除ボタンを選択します。

カスタマー管理者とカスタマーグループの管理 - SA クライアント

サーバーを整理してアクセス制御境界を明確にする方法として、管理対象サーバーをカスタマーごとに整理する方法があります。カスタマーは、社内の部署など、業務上の組織に関連付けられたサーバーのグループを指します。通常の場合、サーバーではカスタマー向けのアプリケーションが実行されるので、サーバーはカスタマーに関連付けられます。カスタマーの作成と管理の詳細については、『SA ユーザーガイド : Server Automation』を参照してください。

スーパー管理者のタスクは、カスタマー管理者に委任することができます。**カスタマー管理者**は、カスタマーに割り当てられたサーバーを管理するユーザーを管理します。カスタマー管理者は、特定のユーザーグループのみにアクセスできるスーパー管理者です。

カスタマー管理者を作成するには、カスタマーグループを作成し、そのカスタマーグループにカスタマーとユーザーを割り当てます。詳細については、カスタマー管理者およびカスタマーグループについて (29 ページ) を参照してください。

すべてのカスタマー管理者の表示

カスタマー管理者は、カスタマーグループで表示されるユーザーです。SAのすべてのカスタマー管理者を表示するには、次の手順を実行します。

1. SAクライアントのナビゲーションペインで、[管理] タブを選択します。
2. ナビゲーションペインで [ユーザーとグループ] ノードを開きます。これにより、[スーパー管理者] ノードが表示されます。
3. [スーパー管理者] ノードを選択します。関連するすべてのスーパー管理者とカスタマー管理者が表示されます。スーパー管理者とカスタマー管理者は、次のように、アイコンで区別することができます。

 カスタマー管理者のアイコン

 スーパー管理者のアイコン

カスタマーグループのすべてのカスタマー管理者の表示

カスタマー管理者は、カスタマーグループで表示されるユーザーです。特定のカスタマーグループに対するSAのすべてのカスタマー管理者を表示するには、次の手順を実行します。

1. SAクライアントのナビゲーションペインで、[管理] タブを選択します。
2. ナビゲーションペインの [ユーザーとグループ] ノードで、[カスタマーグループ] ノードを選択します。これにより、関連するすべてのカスタマーグループが表示されます。
3. カスタマーグループを選択します。
4. [ユーザー] ビューを選択します。カスタマーグループのメンバーであるユーザーがすべて表示されます。ここに表示されるユーザーは、カスタマーグループに表示されるカスタマーのカスタマー管理者です。

カスタマーグループのすべてのカスタマーの表示

カスタマー管理者は、カスタマーグループで表示されるユーザーです。カスタマーグループのすべてのカスタマーを表示するには、次の手順を実行します。

1. SAクライアントのナビゲーションペインで、[管理] タブを選択します。
2. ナビゲーションペインの [ユーザーとグループ] ノードで、[カスタマーグループ] ノードを選択します。これにより、関連するすべてのカスタマーグループが表示されます。
3. カスタマーグループを選択します。
4. [カスタマー] ビューを選択します。カスタマーグループのメンバーであるカスタマーがすべて表示されます。

カスタマーグループの作成

カスタマーグループでは、1つまたは複数のユーザーを1つまたは複数のカスタマーに関連付けます。これらのユーザーはカスタマー管理者になります。SAのカスタマー管理者は、該当するカスタマーにアクセスできるすべてのユーザーグループを変更できるSAユーザーです。SAのカスタマー管理者を作成するには、カスタマーグループを作成する必要があります。次の手順を実行します。

1. SAクライアントにスーパー管理者 (adminなど) としてログインします。
2. ナビゲーションペインで [管理] タブを選択します。

3 ナビゲーションペインの [ユーザーとグループ] ノードで、[カスタマーグループ] ノードを選択します。これにより、既存のすべてのカスタマーグループが表示されます。

4 [**アクション**] > [**追加**] メニューを選択するか、新規アイテムの作成アイコンを選択します。

5 カスタマーグループの名前と説明を入力します。

6 [カスタマー] ビューを選択します。

7 [+] アイコンを選択するか、[**アクション**] > [**追加**] メニューを選択します。これにより、すべてのカスタマーが表示されます。

8 1つまたは複数のカスタマーを選択し、[選択] を押します。

9 [ユーザー] ビューを選択します。

10 [+] アイコンを選択するか、[**アクション**] > [**追加**] メニューを選択します。これにより、すべてのSAユーザーが表示されます。

11 カスタマーグループに追加するユーザーを1つまたは複数選択して、[選択] を押します。

12 [**ファイル**] > [**保存**] を選択します。

13 [**ファイル**] > [**閉じる**] を選択します。

カスタマーグループの削除

カスタマーグループでは、1つまたは複数のユーザーを1つまたは複数のカスタマーに関連付けます。これらのユーザーはカスタマー管理者になります。SAのカスタマー管理者は、特定のユーザーグループを変更できるSAユーザーです。カスタマーグループを削除するには、次の手順を実行します。

1 SAクライアントにスーパー管理者 (adminなど) としてログインします。

2 ナビゲーションペインで [管理] タブを選択します。

3 ナビゲーションペインの [ユーザーとグループ] ノードで、[カスタマーグループ] ノードを選択します。これにより、既存のすべてのカスタマーグループが表示されます。

4 削除するカスタマーグループを選択します。

5 [X] アイコンまたは [**アクション**] > [**削除**] メニューを選択するか、右クリックして [**削除**] を選択するか、キーボードの [Delete] キーを押します。これにより、選択したカスタマーグループが削除されます

カスタマーグループビューでのカスタマー管理者の作成

SAのカスタマー管理者は、特定のユーザーグループを変更できるSAユーザーです。SAのカスタマー管理者を作成するには、SAユーザーをカスタマーグループに追加します。次の手順を実行します。

1 SAクライアントにスーパー管理者 (adminなど) としてログインします。

2 ナビゲーションペインで [管理] タブを選択します。

3 ナビゲーションペインの [ユーザーとグループ] ノードで、[カスタマーグループ] ノードを選択します。これにより、既存のすべてのカスタマーグループが表示されます。

4 カスタマーグループを選択します。詳細については、カスタマーグループの作成 (56ページ) も参照してください。

5 [**アクション**] > [**開く**] メニューを選択するか右クリックをして、[**開く**] を選択します。別ウィンドウが開いてカスタマーグループが表示されます。

6 [ユーザー] ビューを選択します。そのカスタマーグループのメンバーであるすべてのSAユーザーが表示されます。

7 [+] アイコンを選択するか、[**アクション**] > [**追加**] メニューを選択します。これにより、すべてのSAユーザーが表示されます。詳細については、ユーザーの新規作成 (35ページ) も参照してください。

8 カスタマー管理者にするユーザーを1つまたは複数選択して、[選択] を押します。

9 [**ファイル**] > [**保存**] を選択します。

10 [**ファイル**] > [**閉じる**] を選択します。

新しいカスタマー管理者が作成されます。このカスタマー管理者は、カスタマーに対するリソースのアクセス権を使用してユーザーグループを変更することができます。

ユーザービューでのカスタマー管理者の作成

SAのカスタマー管理者は、特定のユーザーグループを変更できるSAユーザーです。SAのカスタマー管理者を作成するには、SAユーザーをカスタマーグループに追加します。次の手順を実行します。

1 SAクライアントにスーパー管理者 (adminなど) としてログインします。

2 ナビゲーションペインで [管理] タブを選択します。

3 ナビゲーションペインの [ユーザーとグループ] ノードで、[ユーザー] ノードを選択します。これにより、既存のすべてのSAユーザーが表示されます。

4 ユーザーを選択します (ユーザーの新規作成 (35ページ) も参照)。

5 [**アクション**] > [**開く**] メニューを選択するか右クリックをして、[**開く**] を選択します。別ウィンドウが開いてユーザーが表示されます。

6 [カスタマーグループ] ビューを選択します。ユーザーが所属するカスタマーグループがすべて表示されます。

7 [+] アイコンを選択するか、[**アクション**] > [**追加**] メニューを選択します。これにより、関連するすべてのカスタマーグループが表示されます (カスタマーグループの作成 (56ページ) も参照)。

8 1つまたは複数のグループを選択し、[選択] を押します。

9 [**ファイル**] > [**保存**] を選択します。

10 [**ファイル**] > [**閉じる**] を選択します。

新しいカスタマー管理者が作成されます。このカスタマー管理者は、カスタマーに対するリソースのアクセス権を使用してユーザーグループを変更することができます。

カスタマーグループビューでのカスタマー管理者の削除

SAのカスタマー管理者は、特定のユーザーグループを変更できるSAユーザーです。SAカスタマー管理者を削除するには、そのSAユーザーが所属するカスタマーグループからSAユーザーを削除します。次の手順を実行します。

1 SAクライアントにスーパー管理者 (adminなど) としてログインします。

2 ナビゲーションペインで [管理] タブを選択します。

3 ナビゲーションペインの [ユーザーとグループ] ノードで、[カスタマーグループ] ノードを選択します。これにより、既存のすべてのカスタマーグループが表示されます。

4 カスタマーグループを選択します。

5 [**アクション**] > [**開く**] メニューを選択するか右クリックをして、[**開く**] を選択します。別ウィンドウが開いてカスタマーグループが表示されます。

6 [ユーザー] ビューを選択します。そのカスタマーグループのメンバーであるすべてのSAユーザーが表示されます。

7 カスタマーグループから削除するユーザーを1つまたは複数選択して、[-] アイコンまたは [**アクション**] > [**削除**] メニューを選択するか右クリックをして、[**削除**] を選択するか、キーボードの [Delete] キーを押します。選択したSAユーザーがカスタマーグループから削除されます。これにより、これらのユーザーはカスタマー管理者ではなくなります。ただし、これらのユーザーはSAユーザーとしては引き続き有効です。

8 [**ファイル**] > [**保存**] を選択します。

9 [**ファイル**] > [**閉じる**] を選択します。

ユーザービューでのカスタマー管理者の削除

SAのカスタマー管理者は、特定のユーザーグループを変更できるSAユーザーです。SAカスタマー管理者を削除するには、そのSAユーザーが所属するカスタマーグループからSAユーザーを削除します。次の手順を実行します。

1 SAクライアントにスーパー管理者 (adminなど) としてログインします。

2 ナビゲーションペインで [管理] タブを選択します。

3 ナビゲーションペインの [ユーザーとグループ] ノードで、[ユーザー] ノードを選択します。これにより、既存のすべてのSAユーザーが表示されます。

4 ユーザーを選択します。

5 [**アクション**] > [**開く**] メニューを選択するか右クリックをして、[**開く**] を選択します。別ウィンドウが開いてユーザーが表示されます。

6 [カスタマーグループ] ビューを選択します。ユーザーが所属するカスタマーグループがすべて表示されます。

7 ユーザーを削除するカスタマーグループを1つまたは複数選択している状態で、[-] アイコンまたは [**アクション**] > [**削除**] メニューを選択するか、右クリックして [**削除**] を選択するか、キーボードの [Delete] キーを押します。カスタマーグループからユーザーが削除されます。

8 [**ファイル**] > [**保存**] を選択します。

9 [**ファイル**] > [**閉じる**] を選択します。

パスワード文字の要件の指定

SAユーザーのパスワードで使用する文字の要件を指定するには、次の手順を実行します。

1 SAクライアントで [**管理**] タブを選択します。

2 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。

3 SAコンポーネントの一覧で、[Server Automation Web クライアント] 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。

4 パラメーター owm.features.MiniPasswordPolicy.allowをtrueに設定します。

このページの他のパスワードパラメーターを設定するには、このパラメーターを true にする必要があります。他のパスワードパラメーターを無効にする場合は、owm.features.MiniPasswordPolicy.allowをfalseに設定します。

5 表10に記載されているパスワードパラメーターの値を設定します。

6 [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。

7 これらのパラメーターの変更をマルチマスターメッシュ内の他のコアに適用するには、他のコアを再起動する必要があります。手順については、SAの開始/停止スクリプト (169ページ) を参照してください。

表10 構成パラメーターの変更ページのパスワードの要件

パスワードの要件	パラメーター	指定できる値	デフォルト値
同じ文字の連続する繰り返しの最大数	owm.pwpolicy.maxRepeats	0より大きな数	2
最小文字数	owm.pwpolicy.minChars	正の整数	6
アルファベット以外の文字の最小文字数	owm.pwpolicy.minNonAlphaChars	owm.pwpolicy.minCharsの値よりも小さな数	0

外部LDAPディレクトリサービスを使用した認証

ユーザー認証に外部のLDAPディレクトリサービスを使用するようにSAを構成することができます。外部の認証を使用すると、SAで使用するユーザー名とパスワードを個別に管理する必要がありません。SAクライアントにログインする際に、ユーザーはLDAPのユーザー名とパスワードを入力します。

LDAPディレクトリは、SAからは読み取り専用になります。LDAPユーザーをインポートした後で、LDAPディレクトリのユーザー属性が変更された場合は、LDAPディレクトリからユーザーを再度インポートする必要があります。

Active Directoryの資格情報を使用して`rosh/ttlg`を使用するには、すべてのドメインコントローラーにSAエージェントをインストールする必要があります。

LDAPサーバーからSAにインポートするユーザー

認証メカニズムに関係なく、SAのユーザー名はすべて一意である必要があります。

LDAPユーザーがSAにログインするには、事前にLDAPユーザーをSAにインポートしておく必要があります。

LDAPディレクトリからのユーザーのインポートは、SAユーザー管理者が行う必要があります。

インポートしたユーザーは、SAクライアントで作成したユーザーと同様に管理されます。たとえば、SAクライアントを使用してインポートしたユーザーをユーザーグループに割り当てたり、SAからインポートしたユーザーを削除したりできます。

SAクライアントでインポートしたユーザーを削除しても、ユーザーが外部のLDAPディレクトリから削除されることはありません。

SAクライアントでは、外部のLDAP内のユーザーを検索して、選択したユーザーをSAにインポートできます。フィルターを指定すると、検索結果を絞り込むことができます。

LDAPのインポートプロセスでは、次のユーザー属性をLDAPディレクトリから取得します。

```
firstName
lastName
fullName
emailAddress
phoneNumber
street
city
state
country
```

また、SAではインポート時にLDAPのユーザー識別名 (DN) も取得します。ユーザーのDNはSAのユーザー名にマッピングされます。

インポート後には、SAクライアント内でインポートしたユーザー情報を編集できます。ただし、ユーザーのログイン名やパスワードを変更することはできません。ユーザーのインポートは単発で行います。また、インポートはLDAPからSAへの片方向のプロセスです。SAクライアントを使用してユーザー属性を変更しても、その変更内容が外部のLDAPディレクトリサーバーに伝播されることはありません。

外部の認証を使用する場合でも、SAクライアントで個別のユーザーを作成することはできます。ただし、LDAPディレクトリとSAクライアントで重複するユーザーを作成してしまう可能性があるため、この方法はお勧めできません。重複するユーザーが存在する場合、SAクライアントで定義したユーザーが使用され、LDAPディレクトリのユーザーは無視されます。

SAクライアントで既にインポートされているユーザーを確認するには、[ユーザーとグループ] ビューで [ユーザー] を選択します。[資格情報ストア] 列が表示されていることを確認します。[資格情報ストア] 列のディレクトリサーバーのユーザーは、LDAPサーバーから既にインポートされています。

SSLと外部認証

外部認証ではSSLは必須ではありませんが、SSLの利用を強く推奨します。LDAP over SSLで使用する証明書ファイルには、PEM (Privacy Enhanced Mail) 形式を使用する必要があります。LDAPサーバーによっては、サーバーのCA (Certification Authority) 証明書をPEM形式に変換する必要があります。

サポート対象の外部LDAPディレクトリサーバー

SAで使用できるディレクトリサーバー製品は、次のとおりです。

- Microsoft Active Directory (Windows Server 2000/2003/2008/2012)
- Novell eDirectory 8.7
- SunDS 5.2

LDAPからSAへのサーバー証明書のインポート

SSLでは、LDAPディレクトリから必要な証明書を抽出して、SAにコピーする必要があります。サーバー証明書をLDAPディレクトリからSAにインポートするには、次の手順を実行します。

1. 外部のLDAPディレクトリからサーバー証明書を抽出します。手順については、次の項を参照してください。
2. 抽出した証明書をPEM形式に変換します。

   Windowsシステムで作成された証明書は、DER (Distinguished Encoding Rules) 形式です。次の例では、`openssl`ユーティリティを使用してDER形式からPEM形式に証明書を変換します。

   ```
   OpenSSL> x509 -inform DER -outform PEM -in mycert.der \
   -out mycert.pem
   ```

3. サーバー証明書をLDAP構成ファイル (`twist_custom.conf`) で指定された場所へコピーします。たとえば、`twist_custom.conf`ファイルには、次のような行が含まれています。

   ```
   aaa.ldap.servercert.ca.fname=/var/opt/opsware/crypto/twist/ldapcert.pem
   ```

Microsoft Active Directoryからのサーバー証明書の抽出

サーバー証明書を抽出するには、次の手順を実行します。

1. 証明書MMCスナップインコンソールまたは証明書サービスのWebインタフェースを実行します。
2. Windows CAのルートCA証明書をDER形式にエクスポートします。

Novell eDirectoryからのサーバー証明書の抽出

サーバー証明書を抽出するには、次の手順を実行します。

1. ローカルCAエントリの名前を確認します(例:CN=CORP-TREE CA.CN=Security)。
2. eDirectory Administrationユーティリティを開いて、[**Modify Object**] をクリックします。
3. エントリ名 (CN=CORP-TREE CA.CN=Security) を入力します。
4. [Certificates] タブを選択します。
5. [**Self Signed Certificate**] をクリックします。
6. [**Export**] をクリックします。
7. ダイアログで、秘密鍵のエクスポートに対して [**No**] を選択し、[**Next**] をクリックします。
8. 適切な形式を選択します (通常はDER)。
9. [**Save the exported certificate to a file**] をクリックします。

SunDSからのサーバー証明書の抽出

通常は、SunDSからサーバーのCA証明書をエクスポートする代わりに、SunDSにインポートした証明書を取得します。

外部LDAPユーザーおよびユーザーグループのインポート

この項のタスクを完了すると、ユーザーはLDAPユーザー名とパスワードを使用して、SAクライアントにログインできるようになります。

この方法では、LDAPのユーザーグループはインポートされません。ユーザーとユーザーグループをインポートする必要がある場合は、LDAP認証構成によるLDAPユーザーおよびユーザーグループのインポート (63ページ) を参照してください。

SAクライアントで外部ユーザーをインポートするには、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] タブを選択します。ナビゲーションペインに [ユーザーとグループ] ノードが表示されます。
2. ナビゲーションペインで [ユーザーとグループ] ノードを開きます。これにより、[ユーザー] ノードが表示されます。
3. [ユーザー] ノードを選択します。これにより、すべてのSAユーザーが表示されます。
4. [**アクション**] > [**ユーザーのインポート**] メニューを選択します。これにより、LDAPディレクトリの情報が表示されます。
5. [ユーザーのインポート] タブを選択します。LDAPディレクトリに含まれるすべてのユーザーが表示されます。
6. ユーザーを1人または複数選択します。
7. 必要に応じて、ユーザーを1つまたは複数のユーザーグループに割り当てることができます。[グループの割り当て] タブを選択して、1つまたは複数のユーザーグループを選択します。
8. [ユーザーのインポート] ボタンをクリックします。これにより、ユーザーがSAにインポートされます。

LDAP認証構成によるLDAPユーザーおよびユーザーグループのインポート

LDAP認証構成は、LDAPを構成する場合や、ユーザーおよびユーザーグループをSAにインポートする場合に使用するコマンドラインツールです。このツールを使用するには、何らかの準備が必要な複雑なプロセスを伴う場合があります。

LDAPを構成したら、LDAPユーザーおよびユーザーグループの同期APXを使用して、LDAPユーザーおよびユーザーグループをSAにインポートすることも可能になります。

LDAP 同期によって管理されているユーザーグループは編集しないでください。これらのユーザーグループは、__DO_NOT_EDIT__MAINTAINED_BY_LDAP_SYNC_という記述で識別できます。

前提条件

LDAP認証構成ツールはスクリプトで、SAコアのスライスコンポーネントバンドルのホストで実行する必要があります。このスクリプトを実行するには、事前に次の情報を用意する必要があります。

表11　　LDAP認証構成の必須項目

必須項目	説明
ホスト名	SAで使用するLDAPディレクトリサーバーの完全修飾ホスト名 (FQHN) またはIPアドレス。
LDAPサーバーポート	LDAPディレクトリサーバー用のポート。デフォルトのSSLポートは636で、デフォルトの非SSLポートは389。SAはStartTLSをサポートしていません。
SSL	LDAPディレクトリサーバーでSSL認証が必要かどうか。SSLを有効にした場合は、サーバーのSSL証明書の検証に使用する信頼できるCAの証明書を指定する必要があります。
サーバーのSSL証明書を検証するための信頼できるCA証明書	LDAPディレクトリサーバーのSSL証明書の検証に使用する、PEM形式の信頼できるCAの証明書を含むLDAPディレクトリサーバー上のファイルへの完全パス。
相互 (双方向) 認証に対応したSSL	次の情報を指定する必要があります。 1　サーバーのSSL証明書を検証するための信頼できるCA証明書 2　クライアントのSSL証明書を検証するための信頼できるCA証明書 3　クライアント証明書と (暗号化されていない) 秘密鍵
クライアント認証に対応したSSL	1　SSLクライアント証明書の検証に使用する、PEM形式の信頼できるCAの証明書を含むファイルへの完全パス。 2　PEM形式のクライアントSSL証明書および対応する秘密鍵を含むファイルへの完全パス。クライアントの秘密鍵は暗号化しないでください。
ディレクトリ情報ツリー (DIT) に対する匿名検索	LDAPディレクトリで、ユーザー情報が格納されているDITに対する匿名検索を許可するかどうか。これは匿名バインドの許可を意味することに注意してください。たとえば、匿名ユーザーDNとパスワードを指定しないユーザー) にDITへの読み取りアクセスを許可するかどうか。多くの企業では、匿名検索は許可されません。匿名検索が使用できない場合は、DITへの読み取りアクセスが可能なユーザーのバインドDNとパスワードを指定する必要があります。
バインドDN	匿名検索が無効な場合のみ必要。DITへの読み取りアクセスが可能なユーザーのバインドDN。

表11　LDAP認証構成の必須項目

必須項目	説明
バインドパスワード	匿名検索が無効な場合のみ必要。DITへの読み取りアクセスが可能なユーザーのバインドパスワード。
一意のユーザー名の属性	一意のユーザー名の属性。 • Active Directoryの場合、デフォルトは`SAMAccountName`です。 • Novell eDirectoryの場合、デフォルトは`cn`です。 • その他のベンダーの場合、デフォルトは`uid`です。
ユーザー表示名の属性	ユーザー表示名の属性。 • Active Directoryの場合、デフォルトは`displayName`です。 • Novell eDirectoryの場合、デフォルトは`fullName`です。 • その他のベンダーの場合、デフォルトは`cn`です。
ベースDN	DNは、ユーザーインポート操作でユーザーを検索する際に考慮対象となるDITの一部です。LDAP認証構成ツールではサブツリー検索を使用するため、検索フィルターはベースDN以下のユーザーのみに適用されます。
検索フィルターテンプレート	検索フィルターテンプレートは、オプションでフィルターを指定して、ユーザーインポート用のLDAP検索のフィルターとして使用します。 テンプレート内のドル記号 (`$`) は、SAクライアントの [ユーザーのインポート] ページで指定するフィルター文字列で置き換えられます (デフォルト値はすべてのエントリと一致するアスタリスク (`*`) です)。 • Active Directoryの場合、デフォルトは `(&(sAMAccountName=$)(objectCategory=person)(objectClass=user)(sAMAccountType=805306368))` です。 • Novell eDirectoryの場合。デフォルトは `(&(cn=$)(objectClass=person))` です。 • その他のベンダーの場合、デフォルトは`uid=$`です。

LDAP認証構成のプロセス

LDAP認証構成を実行すると、LDAPディレクトリサーバーでSSL認証が必要かどうか、および匿名検索が許可されているかどうかに応じてプロンプトが表示されます。

匿名検索: **いいえ**

SSL: **いいえ**

1. SAコアのスライスコンポーネントバンドルをホストするサーバーにログインします。
2. 次のようにユーザー `twist`としてログインします。

   ```
   su twist
   ```

3. 次のコマンドを入力します。

   ```
   cd /opt/opsware/twist
   ```

4. 次のようにLDAP認証構成を起動します。

   ```
   ./ldap_config.sh
   ```

5 必要な情報を入力します。匿名検索が可能かどうかを確認するメッセージが表示されたら、N と入力します。SSLセットアップが必要かどうかを確認するメッセージが表示されたら、Nと入力します。

6 LDAP認証構成ツールが完了したら、LDAP認証構成の検証と保存が正常に実行されていることを確認します。

7 コマンドセンターにログオンして、外部ユーザーをインポートできることを確認します。

8 LDAPユーザーとしてコマンドセンターにログオンできることを確認します。

匿名検索: **はい**

SSL: **いいえ**

1 SAコアのスライスコンポーネントバンドルをホストするサーバーにログインします。

2 次のようにユーザー twistとしてログインします。

```
su twist
```

3 次のコマンドを入力します。

```
cd /opt/opsware/twist
```

4 次のようにLDAP認証構成を起動します。

```
./ldap_config.sh
```

5 必要な情報を入力します。匿名検索が可能かどうかを確認するメッセージが表示されたら、N と入力します。SSLセットアップが必要かどうかを確認するメッセージが表示されたら、Nと入力します。

6 LDAP認証構成ツールが完了したら、LDAP認証構成の検証と保存が正常に実行されていることを確認します。

7 コマンドセンターにログオンして、外部ユーザーをインポートできることを確認します。

8 LDAPユーザーとしてコマンドセンターにログオンできることを確認します。

匿名検索: **いいえ**

SSL: **はい** (SSLサーバー認証のみ)

1 SAコアのスライスコンポーネントバンドルをホストするサーバーにログインします。

2 次のようにユーザー twistとしてログインします。

```
su twist
```

3 次のコマンドを入力します。

```
cd /opt/opsware/twist
```

4 次のようにLDAP認証構成を起動します。

```
./ldap_config.sh
```

5 匿名検索が可能かどうかを確認するメッセージが表示されたら、Nと入力します。SSLセットアップが必要かどうかを確認するメッセージが表示されたら、Yと入力します。SSLクライアント認証を使用するかどうかを確認するメッセージが表示されたら、Nと入力します。

6 LDAP認証構成ツールが完了したら、LDAP認証構成の検証と保存が正常に実行されていることを確認します。

7 コマンドセンターにログオンして、外部ユーザーをインポートできることを確認します。

8 LDAPユーザーとしてコマンドセンターにログオンできることを確認します。

匿名検索: **いいえ**

SSL: **はい** (SSL相互認証が必要)

1 SAコアのスライスコンポーネントバンドルをホストするサーバーにログインします。

2 次のようにユーザー twistとしてログインします。

```
su twist
```

3 次のコマンドを入力します。

```
cd /opt/opsware/twist
```

4 次のようにLDAP認証構成を起動します。

```
./ldap_config.sh
```

5 匿名検索が可能かどうかを確認するメッセージが表示されたら、Nと入力します。SSLセットアップが必要かどうかを確認するメッセージが表示されたら、Yと入力します。SSLクライアント認証を使用するかどうかを確認するメッセージが表示されたら、Yと入力します。

6 LDAP認証構成ツールが完了したら、LDAP認証構成の検証と保存が正常に実行されていることを確認します。

7 コマンドセンターにログオンして、外部ユーザーをインポートできることを確認します。

8 LDAPユーザーとしてコマンドセンターにログオンできることを確認します。

匿名検索: **はい**

SSL: **はい** (SSLサーバー認証のみ)

1 SAコアのスライスコンポーネントバンドルをホストするサーバーにログインします。

2 次のようにユーザー twistとしてログインします。

```
su twist
```

3 次のコマンドを入力します。

```
cd /opt/opsware/twist
```

4 次のようにLDAP認証構成を起動します。

```
./ldap_config.sh
```

5 匿名検索が可能かどうかを確認するメッセージが表示されたら、Yと入力します。SSLセットアップが必要かどうかを確認するメッセージが表示されたら、Yと入力します。SSLクライアント認証を使用するかどうかを確認するメッセージが表示されたら、Nと入力します。

匿名検索: **はい**

SSL: **はい** (SSL相互認証が必要)

1 SAコアのスライスコンポーネントバンドルをホストするサーバーにログインします。

2 次のようにユーザー twistとしてログインします。

```
su twist
```

3 次のコマンドを入力します。

```
cd /opt/opsware/twist
```

4 次のようにLDAP認証構成を起動します。

```
./ldap_config.sh
```

5 匿名検索が可能かどうかを確認するメッセージが表示されたら、Yと入力します。SSLセットアップが必要かどうかを確認するメッセージが表示されたら、Yと入力します。SSLクライアント認証を使用するかどうかを確認するメッセージが表示されたら、Yと入力します。

デフォルトで表示される値は、LDAP認証構成ツールを前回使用したときに保存された値です。

LDAP認証構成の実行例

```
>./ldap_config.sh

Retrieving LDAP configuration ...
LDAP Connectivity Configuration
Enter the fully-qualified host name or IP for the LDAP directory server
[sample-centos.example.com] :
Does the LDAP directory server require SSL?[N] :
Enter the port number for the LDAP directory server [8389] :
Does the LDAP directory server support anonymous bind and anonymous read
access to the directory information tree?[N] :
Enter the bind distinguished name (DN) of the user who has read access to the
directory information tree (DIT)
[cn=Administrator,cn=users,dc=hyrule,dc=local] :
Do you want to change the bind password for
cn=Administrator,cn=users,dc=hyrule,dc=local [N] :

You have entered the following information:
LDAP Directory Server FQHN/IP                    : sample-centos.example.com
```

```
LDAP Directory Server Port                          : 8389
SSL Enabled?                                        : false
Bind DN                                             : cn=Administrator,
cn=users,dc=hyrule,dc=local
Bind Password Provided?                             : true

Is this correct? [Y] :

Verifying LDAP directory server connectivity ...
found naming context :DC=hyrule,DC=local
found naming context :CN=Configuration,DC=hyrule,DC=local
found naming context :CN=Schema,CN=Configuration,DC=hyrule,DC=local
found naming context :DC=DomainDnsZones,DC=hyrule,DC=local
found naming context :DC=ForestDnsZones,DC=hyrule,DC=local
LDAP directory server connectivity successfully verified.

LDAP Search Configuration
Is the LDAP directory server an Active Directory (AD) directory server? [Y] :
Enter the LDAP attribute for the unique username [SamAccountName] :
Enter the LDAP attribute for the user's display name [cn] :
Enter the LDAP search filter template
[(&(sAMAccountName=$)(objectCategory=person)(objectClass=user)
(sAMAccountType=805306368))] :
Enter the LDAP search base distinguished name (DN). Usually this is the root
naming context.[cn=users,dc=hyrule,dc=local] :

You have entered the following information:
LDAP Unique Username Attribute                      : SamAccountName
LDAP User Display Name Attribute                    : cn
LDAP Search Filter Template                         :
(&(sAMAccountName=$)(objectCategory=person)(objectClass=user)
(sAMAccountType=805306368))
LDAP Search Base Distinguished Name (DN)            :
cn=users,dc=hyrule,dc=local

Is this correct? [Y] :

Verifying LDAP search configuration ...
To test LDAP search configuration, you must provide a username of a LDAP
directory user to search.
LDAP search configuration is successfully verified only if the given user is
successfully returned by the LDAP
directory server.
Enter a username to search : *

You have entered the following information:
Username To Search : *

Is this correct? [Y] :

Resulting LDAP Search Filter
:(&(sAMAccountName=*)(objectCategory=person)(objectClass=user)(sAMAcco
untType=805306368))
Searching LDAP directory server for user * ...
Found 4 users
```

```
DN : CN=Administrator,cn=users,dc=hyrule,dc=local
cn : Administrator
SamAccountName : Administrator

DN : CN=Guest,cn=users,dc=hyrule,dc=local
cn : Guest
SamAccountName : Guest

DN : CN=krbtgt,cn=users,dc=hyrule,dc=local
cn : krbtgt
SamAccountName : krbtgt

DN : CN=link,cn=users,dc=hyrule,dc=local
cn : link
SamAccountName : link

Is this correct? [Y] :
LDAP search configuration successfully verified.

LDAP Users & Groups Synchronization Configuration
Do you want to configure users & groups synchronization? [Y] :
LDAP User Group Synchronization Configuration
Enter the LDAP search base distinguished name (DN) for the user groups
[cn=users,dc=hyrule,dc=local]
 :
Enter the LDAP search filter template to search user groups
[(&(cn=$)(objectCategory=group))] :
Enter the LDAP attribute for the unique user group name [SamAccountName] :
Enter the LDAP attribute in the user group LDAP object class which contains
the DNs of its members [
member] :

You have entered the following information:
LDAP Search User Group Base DN                      :
cn=users,dc=hyrule,dc=local
LDAP Search User Group Search Filter Template       :
(&(cn=$)(objectCategory=group))
LDAP Unique User Group Name Attribute               : SamAccountName
LDAP Search User Group Membership Attribute         : member

Is this correct? [Y] :

Verifying LDAP user group synchronization configuration ...
Searching LDAP directory server for all users and user groups ...
Searching LDAP directory server for all LDAP users ...

Resulting LDAP Search Filter For All LDAP Users :
(&(sAMAccountName=*)(objectCategory=person)(object
Class=user)(sAMAccountType=805306368))
Found 4 LDAP users

Parsing search results ...
Searching LDAP directory server for all LDAP user groups ...
```

```
Resulting LDAP Search Filter For All LDAP User Groups :
(&(cn=*)(objectCategory=group))
Found 16 LDAP user groups

Parsing search results ...
Do you wish to display detail search result? [N] : y
Parsing search results ...
Denied RODC Password Replication Group: 2 members
    Administrator   : cn=administrator,cn=users,dc=hyrule,dc=local
    krbtgt   : cn=krbtgt,cn=users,dc=hyrule,dc=local
Allowed RODC Password Replication Group: 0 members
Enterprise Read-only Domain Controllers: 0 members
Group Policy Creator Owners: 1 members
    Administrator   : cn=administrator,cn=users,dc=hyrule,dc=local
Domain Controllers: 0 members
Cert Publishers: 0 members
Domain Users: 0 members
Enterprise Admins: 1 members
    Administrator   : cn=administrator,cn=users,dc=hyrule,dc=local
Schema Admins: 1 members
    Administrator   : cn=administrator,cn=users,dc=hyrule,dc=local
DnsAdmins: 0 members
Read-only Domain Controllers: 0 members
RAS and IAS Servers: 0 members
Domain Guests: 0 members
Domain Admins: 1 members
    Administrator   : cn=administrator,cn=users,dc=hyrule,dc=local
Domain Computers: 0 members
DnsUpdateProxy: 0 members
Is this correct? [Y] :
LDAP user group synchronization configuration successfully verified.

The following properties will be stored into global configuration.
aaa.ldap.hostname=gyee-centos.cup.hp.com
aaa.ldap.port=8389
aaa.ldap.ssl=false
aaa.ldap.search.binddn=cn=Administrator,cn=users,dc=hyrule,dc=local
aaa.ldap.search.pw=true
aaa.ldap.search.naming.attribute=SamAccountName
aaa.ldap.search.display.name.attribute=cn
aaa.ldap.search.filter.template=(&(sAMAccountName=$)(objectCategory=person)
  (objectClass=user)(sAMAccountType=805306368))
aaa.ldap.search.base.template=cn=users,dc=hyrule,dc=local
aaa.ldap.enable.users.groups.sync=true
aaa.ldap.search.usergroup.naming.attribute=SamAccountName
aaa.ldap.search.usergroup.membership.naming.attribute=member
aaa.ldap.search.usergroup.base.template=cn=users,dc=hyrule,dc=local
aaa.ldap.search.usergroup.filter.template=(&(cn=$)(objectCategory=group))

Are you sure? [Y] :
Saving LDAP configuration ...
LDAP configuration successfully saved.
Do you want to schedule a recurring job for LDAP users & user groups
synchronization? [Y] :
```

```
Select one of the following recurring schedule for LDAP users & user groups
synchronization job:

   1) Daily
   2) Weekly
   3) Monthly

Enter 1, 2, or 3  [3] : 1
Scheduling users & user groups synchronization job ...
LDAP users & user groups synchronization job has been successfully schedule.
Job ID=110001
```

LDAPユーザーの同期

LDAPディレクトリサーバーからユーザーをインポートした後で、LDAP認証構成コマンドラインツールまたはLDAPユーザーおよびユーザーグループ同期APXを使用してLDAPユーザーを同期することができます。

1. SAコアのスライスコンポーネントバンドルをホストするサーバーにログインします。
2. 次のようにユーザー `twist`としてログインします。

   ```
   su twist
   ```

3. 次のコマンドを入力します。

   ```
   cd /opt/opsware/twist
   ```

4. 次のようにLDAP認証構成を起動します。
5. `./ldap_config.sh`
6. 次のような出力が表示されます。

```
Retrieving LDAP configuration ...
Verifying LDAP server connectivity ...

User Synchronization Phase
Searching LDAP directory server for all LDAP users ...
Found 4 LDAP users
Parsing search results ...
4 LDAP users do not exist in SA
Creating them now ...
Creating user cn=link,cn=users,dc=hyrule,dc=local
Creating user cn=krbtgt,cn=users,dc=hyrule,dc=local
Creating user cn=guest,cn=users,dc=hyrule,dc=local
Creating user cn=administrator,cn=users,dc=hyrule,dc=local

User Group Synchronization Phase
Searching LDAP directory server for all LDAP user groups ...
Found 16 LDAP user groups
Parsing search results ...
creating user group Denied RODC Password Replication Group
creating user group Allowed RODC Password Replication Group
creating user group Enterprise Read-only Domain Controllers
creating user group Group Policy Creator Owners
creating user group Domain Controllers
creating user group Cert Publishers
creating user group Domain Users
creating user group Enterprise Admins
creating user group Schema Admins
```

```
creating user group DnsAdmins
creating user group Read-only Domain Controllers
creating user group RAS and IAS Servers
creating user group Domain Guests
creating user group Domain Admins
creating user group Domain Computers
creating user group DnsUpdateProxy
Updating user groups no longer found in LDAP ...

LDAP Users & User Groups Sync Results
================================================================
Number of LDAP Users Found                              : 4
Number of LDAP Users Does Not Exist In SA               : 4
Number of LDAP Users Successfully Created in SA         : 4
Number of LDAP Users Failed To Create In SA             : 0

Number of LDAP User Groups Found                        : 16
Number of LDAP User Groups Successfully Updated in SA : 0
Number of LDAP User Groups Successfully Created in SA : 16
Number of SA User Groups No Longer in LDAP              : 0
Number of SA User Groups Failed To Update               : 0
Number of LDAP User Groups Failed To Process            : 0

Elapsed Time                                            : 00:00:27
================================================================
```

LDAPディレクトリから削除されたLDAPユーザーがSAから削除されることはありませんが、LDAPディレクトリから対応する認証情報が削除されているため、SAにログインすることはできなくなります。

既存のSAユーザーと同じユーザーIDを持つLDAPユーザーは、資格情報ストアのタイプに関係なくスキップされます。SAでは重複するユーザーの作成や更新は行われません。

SA共通アクセスカード (CAC) と個人識別情報検証 (PIV) スマートカードの統合

共通アクセスカード (CAC カード) は、クレジットカードと同じくらいのサイズのスマートカードです。現役の軍関係者、予備役兵、米国国防総省 (DoD) 職員、および有資格の個人契約者を識別するための標準的な手段として使用されています。また、建物や管理区域に物理的にアクセスする場合にも使用される重要なカードであり、軍のコンピューターネットワークやシステムへのアクセスも可能にします。ジュネーブ条約 (第三次条約) では、身分証明書として扱われます。CACカードは、2要素認証標準 (ユーザーに属している要素とそのユーザーだけが知っている要素) と、デジタル署名やデータ暗号化テクノロジー (認証、完全性、否認防止) の標準に準拠しています。

SA/スマートカードの統合は、SAクライアントにログインしているときに限り、利用可能です。

スマートカード/SA統合認証の基本事項

SAクライアントはスマートカードを検出して、通常のSA認証画面でログインするか、新しいスマートカードベースの認証方法でログインするかを選択できるオプションをユーザーに提供します。ユーザーが必須のPINを入力したら、SA クライアントは、カードリーダー API と連携してスマートカードの証明書にアクセスします。スマートカードの証明書は失効の検証後に、一意の証明書フィールドが SA 内のユーザーアカウントとマッピングされます。これらの一意のフィールドのマッピングについては、SA管理者がオリジナルのマッピングを作成します。

ユーザーを識別する情報は、証明書と呼ばれるドキュメントの形式で、スマートカードに格納されています。この証明書には、パブリックキーと呼ばれる暗号化キーが含まれています。また、ユーザーの名前 (通常は名、姓、ミドルネームのイニシャル) や、場合によっては、組織内のユーザーの電子メールアドレスなど、ユーザーを識別するテキストフィールドも含まれています。ユーザーのスマートカード認証情報と既存のSAユーザー名を照合できるようにするため、システムはスマートカードの証明書に含まれているテキストデータからユーザー名を作成します。

スマートカードに格納されている証明書には、次のような情報が含まれています。

```
Certificate:
    Data:
        Version:3 (0x2)
        Serial Number:1501 (0x5dd)
        Signature Algorithm: ecdsa-with-SHA256
        Issuer:C=US, O=Test Certificates 2010, OU=Test CA, CN=Test ECC P-256 CA
        Validity
            Not Before:Oct  1 08:30:00 2010 GMT
            Not After :Oct  1 08:30:00 2030 GMT
        Subject:CN=Test E. Cardholder XV, C=US, O=Test Government, OU=Test Agency
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
            EC Public Key:
                pub:
                    04:03:a0:ad:22:46:01:b8:9b:1b:65:b0:94:3f:5e:
...
```

証明書からユーザー名を導出するため、SA は `/etc/opt/opsware/twist/twist.conf` ファイルで設定されたパターン指定文字列と、ユーザー名を作成する照合およびアセンブリアルゴリズムを使用します。パターン指定の例は、次のようになります。

```
sc.usernameMakeRule.1=%Subject#CN$1%Subject#CN$2%Subject#CN$3
```

ユーザー名の作成ロジックでは、上記の指定文字列を使用して、ユーザー名を作成します。

```
TestE.Cardholder
```

証明書から取得されたフィールド名は、パーセント記号 (%) で指定されます。属性 (サブフィールド) は、ポンド記号 (#) で指定されます。属性内の位置指定フィールドは、ドル記号 ($) と後に続く数字 (テキスト行のフィールド位置) で指定されます。

これは、SAインストールによって提供されるデフォルトのパターンです。SA管理者は、このパターンによって一意でないユーザー名が作成される可能性があることに注意するとともに、適切な対処法を用意しておく必要があります。

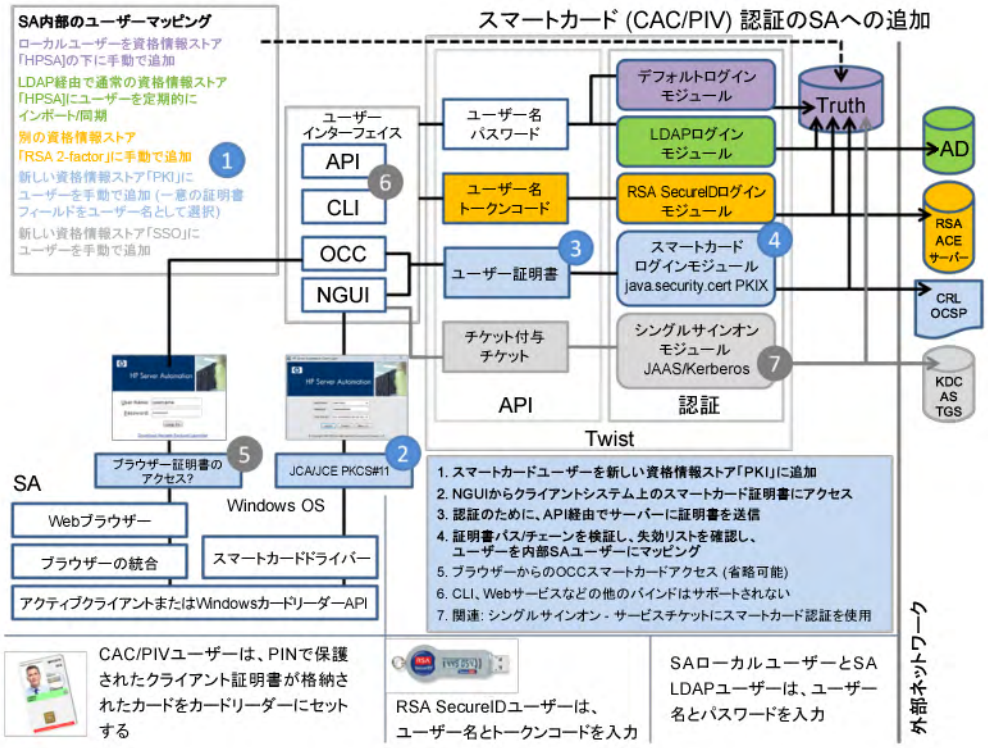
ユーザー名の作成アルゴリズムでスマートカード属性を使用しないでください。

インストール前に、スマートカードの証明書からユーザー名を作成するパターンを決定しておく必要があります。特に重要なポイントとして、メカニズムをよく理解して、ユーザー名の作成パターンを決定すること(デフォルトのパターンをそのまま使用することも、異なるパターンを指定することも可能)と、正しいパターンベースのユーザー名でSAのスマートカードユーザーアカウントを作成するように管理者を指導することが挙げられます。

SAスマートカード統合アーキテクチャー

図17に、CAC/PIVスマートカード機能をSAと統合する方法を示します。

図17　　SA/CACスマートカード統合アーキテクチャー



SA/スマートカードの設定

CACスマートカードを使用してログインする新規ユーザーを設定する方法はシンプルです。

- 新規ユーザーを作成して、資格情報ストアをスマートカードに指定します。
- ユーザーがSAクライアントにログインしたら、スマートカードをカードリーダーに通して、自分専用のPIN番号を入力します。

スマートカードの証明書の設定

次のように、`/etc/opt/opsware/twist/twist.conf`ファイルを変更する必要があります。

- 署名アルゴリズムごとに、`sc.sigAlrgName.N`というエントリが必要です。ここで、`N`は一連の番号を表します。
- アルゴリズムごとに、`sc.trustedCertPath.N`という名前の証明書ファイル(`.pem`形式)へのパスが必要です。

次に例を示します。

```
sc.sigAlgName.0=SHA256withECDSA
sc.trustedCertPath.0=/var/opt/opsware/crypto/twist/smartcard/
ECCP256IssuingCACertificate.pem
sc.sigAlgName.1=SHA384withECDSA
sc.trustedCertPath.1=/var/opt/opsware/crypto/twist/smartcard/
ECCP384IssuingCACertificate.pem
sc.sigAlgName.2=SHA256withRSA
sc.trustedCertPath.2=/var/opt/opsware/crypto/twist/smartcard/
RSA2048IssuingCACertificate.pem
```

証明書ファイルの場所は任意の場所でかまいませんが、次のディレクトリに証明書ファイルを格納しておくことをお勧めします。

```
/var/opt/opsware/crypto/twist/smartcard/
```

すべてのホストにスマートカードの証明書を設定する場合

スライスコンポーネントバンドルをホストするSAコアの各サーバーに対して、次の手順を実行する必要があります。

1. 次のフォルダーを作成します。

   ```
   mkdir /var/opt/opsware/crypto/twist/smartcard
   ```

2. スライスホストごとに、手順 1 で作成したフォルダーにユーザーのスマートカードの証明書をインポートします。

   ```
   /var/opt/opsware/crypto/twist/smartcard
   ```

3. 各証明書の所有者が`twist`に変更されていることを確認します。

   ```
   chown -R twist:users /var/opt/opsware/crypto/twist/smartcard
   ```

4. 各スライスホストでWebサービスデータアクセスエンジン (`twist`) を再開します。
5. ユーザーを設定して、そのユーザーがスマートカードで認証できることを確認します。

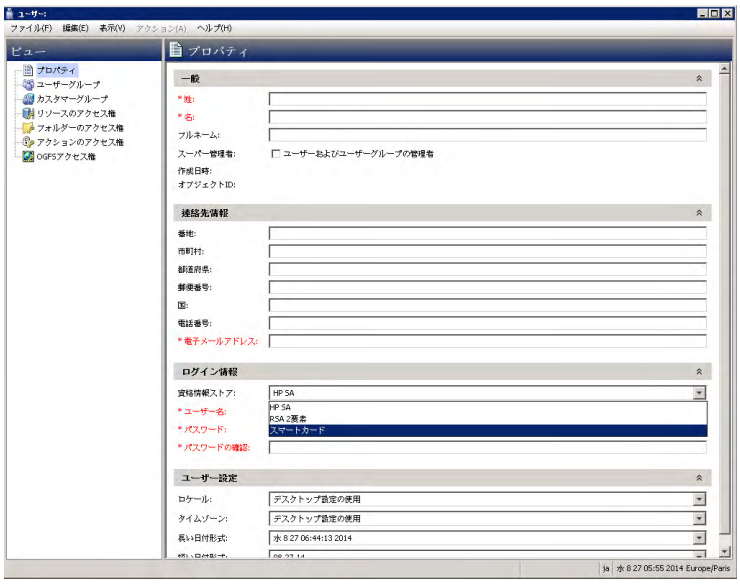
スマートカードユーザーの新規作成

SAクライアントでSAユーザーを新規に作成するには、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ペインで、[管理] タブを選択します。
2. ナビゲーションペインで [ユーザーとグループ] ノードを開きます。これにより、[ユーザー] ノードが表示されます。
3. [ユーザー] ノードを選択します。これにより、すべてのSAユーザーが表示されます。
4. [**アクション**] > [**新規**] メニューを選択するか、新規の [ユーザー] アイコンを選択します。[新規ユーザー] ウィンドウが表示されます。

ユーザーの新規作成 (35 ページ) の手順に従って、ユーザー情報フィールドに入力します。その際に、`SmartCard`を資格情報ストアとし指定します。

スマートカードアクセスは、事前設定のパスワードではなく、スマートカードの暗号化方式に基づいて実行されます。したがって、「スマートカード」を資格情報ストアとして選択すると、パスワードフィールドは画面に表示されなくなります。



上記の説明のように、[ユーザー名] フィールドには、スマートカード/SA統合認証の基本事項 (73ページ) で説明したルールに従って、ユーザーのスマートカードの証明書から導出された名前と一致する名前を指定する必要があります。管理者が新規スマートカードユーザーを作成する場合、ユーザー名の作成パターンのルールに適合するテキスト文字列を入力できるように、このルールの仕組みについて、よく理解しておく必要があります。

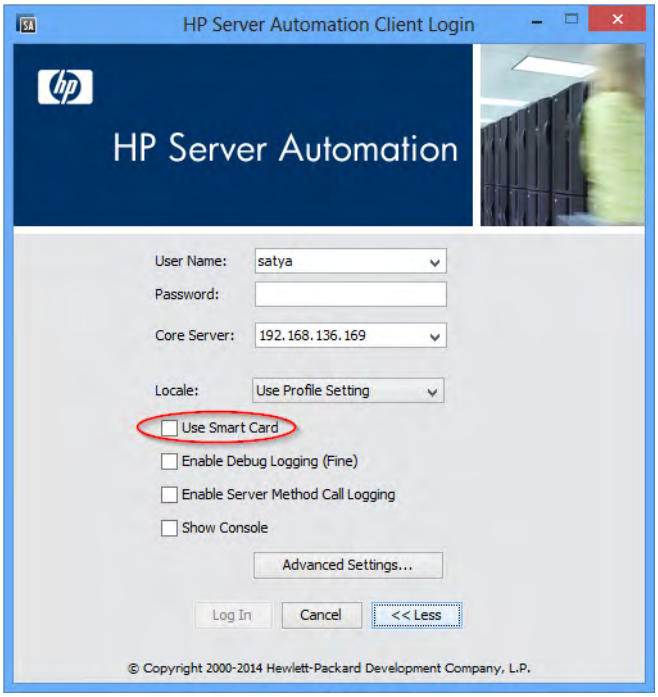
SAクライアントへのスマートカードユーザーの初期ログイン

SAクライアントを開始すると、次のような画面が表示されます。

図18 SAクライアントの標準ログインダイアログ

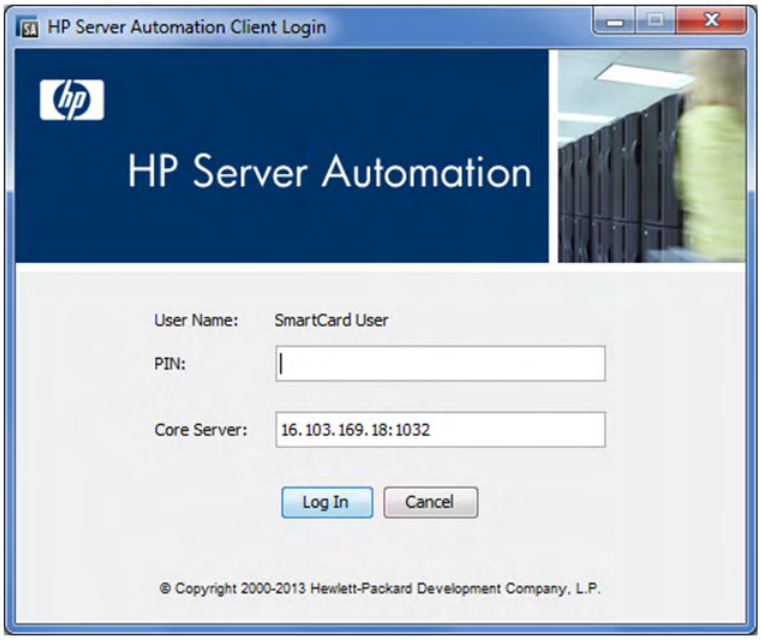
スマートカードログインを有効にするには、[More>>] ボタンをクリックして、詳細ログイン設定にアクセスします。次のような画面が表示されます。

図19　スマートカードログインを使用するSAクライアントの設定



スマートカードログインを有効にするには、[Use Smart Card] チェックボックスをオンにします。次のようなログイン画面が表示されます。

図20　SAクライアントのスマートカード対応ログイン画面



以降すべてのログインで、この画面が表示されます。元の標準的なユーザー名/パスワードログインに戻すには、[Advanced Settings] を選択して、[Use Smart Card] チェックボックスをオフにします。

スマートカードログイン画面が表示されたときに、ユーザーは、動作状態のスマートカードリーダーデバイスを接続/搭載したPCを使用している必要があります。カードリーダーをSAで使用可能にするには、[メディア]アイコンアプリケーションでWindowsデバイスとして表示されていることを確認します。スマートカードでSAにアクセスするときに使用するPCに、有効なカードリーダーが接続/搭載されていない場合は、IT管理者に相談してください。SAへのアクセスを続行するには、スマートカードのPINを入力して、[ログイン]ボタンをクリックする必要があります。

SA/RSA SecurID®の統合

RSA SecurID®は、RSA Security, Inc. (EMCの事業部門) の二要素認証システムです。二要素認証では、ユーザーが知っていること (パスワードやPIN) とユーザーが持っているもの (認証システム) とを組み合わせることで、パスワードよりも強力なユーザー認証を実現します。この項では、SAシステムでSecurID認証を利用する方法について説明します (RSA SecurIDのインストール、構成、管理に関する説明は行いません)。

RSA SecurIDの詳細については、http://www.rsa.comを参照してください。

この項では、SAの認証にRSA SecurIDを統合する方法について説明します。RSA SecurIDを既に使用しているか、導入する予定があることを前提としています。SAでSecurID認証を使用するには、事前にRSA SecurIDサーバー (RSA Authentication ManagerまたはACE Server) をインストールして、すべての構成を済ませておく必要があります。

RSA SecurID/SAの統合の概要

SAユーザーが何らかの操作を行うには、SAに対して認証を行う必要があります。SecurIDを統合すると、既存のRSA SecurIDトークンを使用して認証を行うことができます。SAの認証は既存のSecurID環境とシームレスに統合できます。RSA認証サーバーから見た場合、SA (具体的には、Webサービスデータアクセスエンジンサーバー) は、1つのSecurIDエージェントにすぎません。

SAコアのインストール環境で、SecurIDは自動的にサポートされます。次の構成手順を実行するだけで、SecurIDを有効にすることができます。

最初の2つのタスクは、マルチマスターメッシュ内または複数のWebサービスデータアクセスエンジンを持つSAインストール環境内のすべてのWebサービスデータアクセスエンジンホストで実行する必要があります。

- `sdconf.rec`という名前のRSA SecurID構成ファイルを、Webサービスデータアクセスエンジン (twist) をホストするSAコアサーバー上のディレクトリにコピーする。`sdconf.rec`はRSA Authentication Manager/ACE Serverホスト上に存在します。このファイルには、SAコアに提供する必要のあるRSA Authentication Managerに関する情報が含まれています。
- Webサービスデータアクセスエンジンをシャットダウンし、`loginModule.conf`ファイルを編集してSAでのSecurID認証を有効にした後に再起動する。
- SAクライアントでユーザーを作成または変更して、SecurID認証を使用する。

SAでのSecurID認証方式のサポート

RSA SecurIDは、SecurIDトークンとPIN (Personal Identification Number) を組み合わせて使用する二要素認証に基づいています。

ユーザーが持っているものがSecurIDトークンで、ユーザーが知っていることがPINです。これらの2つの要素を組み合わせることで、ユーザーパスワード単独の場合よりも強力な認証を実現できます。

SecurID トークンはハードウェアベース (ハードウェアトークンまたはハードトークン) でもソフトウェアベース (ソフトウェアトークンまたはソフトトークン) でも構いません。トークンはトークンコードを提供します。事前に割り当てられた (提供された) PINと組み合わせて使用する場合、トークンコードはパスコードと呼ばれます。

表12に、SA/SecurIDの統合でサポートされる代表的な認証方式を示します。

表12　　SecurIDの認証方式

認証方式	説明
標準認証	最も一般的に使用される方式です。ユーザーの PIN が割り当てられます (提供されます)。パスコードは承認されるか拒否されるかのいずれかです。
Next Tokencodeモード (サポート対象外)	この方式はユーザーが入力したパスコードが正しくない場合に使用されます。Next Tokencodeモードでは、ユーザーはトークンコードが変わるのを待って、新しいトークンコードを入力する必要があります。デフォルトでは、ユーザーが3回続けて誤ったパスコードを入力した場合に、Next Tokencodeになります。
New PINモード (サポート対象外)	このモードは、ユーザーが新しい PIN を作成するか、既存のPINを変更する必要がある場合に使用します。

制限事項

RSA SecurID認証は、非対話型のスクリプトには不向きな方式です。これは、トークンコードが60秒ごとに変更されて、非対話型のスクリプトが正常に機能しなくなるためです。スクリプトを対話型に作成し直すか、非対話型のスクリプトを実行する場合にSecurIDを使用しないようにしてください。

SecurID/SAの統合プラットフォームの要件

- Solaris
- Linux x86およびx86_64
- RSA ACE Server 6.1以上

SA/SecurIDの統合の構成

RSA SecurID認証のサポートはSAコア内に統合され、SAコアをインストールする際にインストールされます。ただし、RSA SecurID/SA認証を使用するには、いくつかの構成手順を実行する必要があります。SAコアには、SecurID認証サーバーのIPアドレスが必要で、SecurID認証サーバーと安全に通信できる必要があります。

SAコアに複数のスライスをインストールしている場合は、スライスコンポーネントバンドルホストごとに、次の手順を実行する必要があります。

フェーズ1: RSA SecurIDの認証構成ファイル

1. RSA SecurIDの管理者から、次のファイルを入手する必要があります。

   ```
   sdconf.rec
   ```

2. このファイルを、Webサービスデータアクセスエンジン (twist) をホストするコア内のすべてのサーバーの次の場所にコピーします。

   ```
   /var/opt/opsware/crypto/twist
   ```

3. 次のように、各サーバーでファイルのアクセス権を設定し、ユーザー `twist`にこのファイルの所有権と読み取り権限を付与します。

   ```
   chmod 400 /var/opt/opsware/crypto/twist/sdconf.rec
   chown twist /var/opt/opsware/crypto/twist/sdconf.rec
   ```

4. `securid`または`sdstatus.12`ファイルが `/var/opt/opsware/crypto/twist`ディレクトリ内に存在しないことを確認します。これらのファイルの一方が存在する場合は、そのファイルを削除します。

フェーズ2: SAでのRSA SecurID認証の有効化

1. デフォルトで、RSA SecurID認証は有効になっていません。これを有効にするには、Webサービスデータアクセスエンジン (twist) をホストするコア内のすべてのサーバーで、次のコマンドを使用してこのコンポーネントをシャットダウンします。

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

2. 次のファイルを確認します。

   ```
   /etc/opt/opsware/twist/loginModule.conf
   ```

   このファイルを編集して、次の例の太字で示す行を追加します。

   ```
   TruthLoginModule {
   com.opsware.login.SecurIDLoginModule sufficient debug=false
   next_tokencode_mode=false new_pin_mode=false;
   com.opsware.login.TruthLoginModule sufficient debug=false;
      };
   ```

3. 次のコマンドを使用して、すべてのサーバーでWebサービスデータアクセスエンジンを再起動します。

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

4. 複数のスライスコンポーネントバンドルがインストールされている場合は、他のすべてのスライスコンポーネントバンドルホストで、コマンドセンター (OCC) サーバーとHTTPSプロキシを停止します。

5. この時点では、RSA サーバーとして構成中のスライスコンポーネントバンドルホストのコマンドセンターのみが実行されています。このホストのOCCにログインします。これにより、ノードシークレット (`securid`ファイル) と`sdstatus.12`ファイルが `/var/opt/opsware/crypto/twist`サブディレクトリ内に生成され、スライスコンポーネントバンドルサーバーがACEに登録されます。

6. コア内の他のすべてのスライスコンポーネントバンドルホストでOCCとHTTPSプロキシを起動します。

フェーズ3: SecurID認証を使用するようにSAユーザーを作成/変更する

SecurID認証を使用する各ユーザーは、事前にRSA SecurID認証サーバー (ACEサーバー) で認証済みユーザーとして存在しているものを、SecurID認証を使用するようにSAクライアントで作成または変更する必要があります。

SAクライアントのユーザーのプロファイルページで、ユーザーの資格情報ストアとしてRSA 2-factorを指定します。

ユーザーの作成または変更の詳細については、「ユーザーの管理 - SAクライアント」(34ページ)を参照してください。

トラブルシューティング

`Authentication Failed`というエラーメッセージが何度も表示される場合は、最初にRSA SecurIDの管理者に、ユーザーとパスコードが有効かどうかを確認してください。問題が解消されない場合は、担当の技術サポートにお問い合わせください。

ユーザーおよびセキュリティレポート

SAでは、複数のサーバーのクライアントおよび機能のアクセス権のサマリーをまとめたレポートを生成できます。これらのレポートは、管理者としてSAクライアントにログインしたときにのみ使用できます。詳細については、『SAレポートガイド』を参照してください。

SAでは、次のユーザーおよびセキュリティレポートが利用できます。

- クライアントおよび機能のアクセス権
- カスタマー/ファシリティアクセス権およびデバイスグループアクセス権のオーバーライド
- ユーザーグループメンバーシップ
- ユーザーログイン
- 管理者アクション
- ユーザーと承認、ユーザーグループ別
- ユーザーと承認、個別ユーザーグループ別
- 管理者カスタマーグループ
- サーバーアクセス権、ユーザー別
- サーバーアクセス権、サーバー別
- OGFSアクセス権、ユーザー別
- OGFSアクセス権、サーバー別

第2章 SAコアおよびコンポーネントのセキュリティ

SAコアおよびコンポーネントのセキュリティアーキテクチャーの概要

SAでは、一般的なデータセンターのセキュリティを大幅に向上させることができます。具体的には、SAでは、次のことが可能です。

- データセンターのすべての場所にセキュリティを強化したサーバー用オペレーティングシステムとアプリケーションソフトウェアを確実にプロビジョニングすることができます。
- データセンター環境での制御機能とアカウンタビリティを強化できます。たとえば、サーバーで管理者レベルのパスワードを使用するユーザーの数を少なくしたり、特定のサーバー上で実行されるタスクのデジタル署名付き監査証跡を作成したりできます。
- 高度なセキュリティを維持するための面倒な構成管理を自動化します。たとえば、パッチが適用されていないサーバーの識別やパッチ適用の一貫性の確保できます。また、ロールバックしやすいように構成ファイルを変更時にバックアップします。

データセンターの自動化には大きな利点がありますが、その自動化システム自体が別のセキュリティ上の脆弱性につながらないことを保証する必要があります。組織の内外からの脅威はますます高度化しているため、セキュリティを最優先に設計された自動化ソフトウェアアーキテクチャーを使用することが必要不可欠です。SAは、セキュリティを最優先に設計されています。

この項では、SAで使用されている最新のセキュリティ対策について説明します。これらのセキュリティ対策は、厳格なセキュリティを必要する組織や、次の設計目標を持つ組織を対象としています。

- 厳格な制御とアカウンタビリティ：承認された管理者に限定して、管理アクションの実行を許可できます。SAでは、詳細な役割ベースのアクセス制御を適用して、アカウントアクティビティのデジタル署名付き監査証跡を生成できます。
- システム全体でのセキュアな通信チャネル: SAは、個々のコンポーネントがIPネットワークを介して相互にセキュアな通信を行う分散型コンピューティング環境です。SAでは、SSL/TLSおよびX.509証明書を使用してこれらのコンポーネント間の通信を保護します。
- 業界標準に基づいたコンプライアンスポリシーの自動デリバリ：SAでは、業界標準に基づいたすぐに適用可能なコンプライアンスポリシーを継続的に提供します。コンプライアンスポリシーでは、インストール済みのパッチ、インストール済みソフトウェア、パスワードの最小文字数、レジストリキーの設定、およびファイル内の個別の構成設定といった細かな属性に関して、SAのさまざまな監査と修復の機能を活用します。

厳格な制御とアカウンタビリティの適用

SAでは、強力なセキュリティとアカウンタビリティを実現できます。次の各項を参照してください。

制御とアカウンタビリティの強化

SAでは、強力な制御とアカウンタビリティを使用してデータセンター内のセキュリティを強化できます。SAを使用すると、セキュリティアーキテクトやIT管理部門は、サーバー上で特定のタスクを実行できる担当者を制御できます。タスクの制御は細かく設定できます。たとえば、管理者はパッチのインストールや特定のSA Global Shellコマンドに限定した変更権限を持つ包括的な読み取り専用アクセスを割り当てることができます。

SAでは、特定の時刻にサーバーで特定の管理タスクを実行したSAユーザーなどの詳細情報を収集する、改ざん防止機能を備えた監査証跡が自動的に作成されます。SAの細かな役割ベースのアクセス制御は、ユーザー、サーバーのグループ、管理タスク、環境を表すSAデータモデルの間の関係に沿って設計されています。この強力なアクセス制御モデルには、サーバー上で管理者アカウントを使用する人の数を少なくして、必要な管理タスクのみを実行するSAユーザーアカウントを付与できるというセキュリティ上の利点があります。

SAにログインする人にはすべて、SAの一意のユーザー名とパスワードが必要です。管理者はSA内でユーザー名を作成することも、外部の (LDAP) システムからユーザー名をインポートすることもできます。たとえば、Microsoft Active Directoryを導入済みの企業では、ディレクトリサーバーと同期することで、既存のユーザーアカウントを再利用することができます。

ユーザーアカウントの作成時に、SAユーザーはSAグループに割り当てられます。グループを使用することで、ユーザーが操作を実行できるサーバーや実行できる管理タスクを容易に指定できます。

SAにはいくつかの事前定義のグループがデフォルトで用意されています。これらのグループのアクセス権は必要に応じてカスタマイズできます。また、組織の要件に合わせてカスタマイズしたアクセス権レベルを持つ新規のグループを作成することもできます。ユーザーグループのメンバーがSAで実行できる操作は、そのユーザーグループに対して指定するアクセス権によって決まります。アクションのアクセス権では、ユーザーが実行できるアクションを指定します。リソースのアクセス権では、ユーザーがアクションを実行できるオブジェクト (通常はサーバー) を指定します。SA クライアントと呼ばれる SA のグラフィカルユーザーインタフェースには、Global Shellインタフェースと同様に、これらのタスクルールが適用されます。そのため、ユーザーはセキュリティ管理者によって承認されたタスクのみを表示および実行することができます。

セキュリティ管理者は、サーバーでのソフトウェアのインストールやアプリケーションの構成を自動化するポリシーベースのソフトウェアインストール環境を利用することもできます。指定されたユーザーは、フォルダーの階層構造に組織のアプリケーションソフトウェア構造をモデル化して、作成、表示、変更、実行に関するアクセス権を細かく設定することができます。このようなモデル化により、担当範囲を明確に区別して、それぞれの範囲を専門に担当するユーザーがポリシーの実装と調整を行い、システム管理者がソフトウェアポリシーをサーバーに適用してサーバーを管理することが可能になります。

➤ ユーザーグループとアクセス権については、第1章「ユーザーおよびユーザーグループの設定とセキュリティ」(15ページ) を参照してください。

読み取り専用のデジタル署名付き監査証跡

SAユーザーが管理対象サーバーで実行できるアクションのきめ細かな制御に加えて、SAでは、SAユーザーが実行したイベントの詳細な監査証跡を自動的に収集します。監査証跡では、ユーザー、イベント、対象サーバー、タスクが実行された時間、合計所要時間、タスクに関連するエラー状態などの詳細が記録されます。

監査証跡は、ユーザーがデータを改ざんできないように、読み取り専用のデジタル署名付きデータとしてOracleデータベースに保存されます。この監査証跡データは、それぞれの環境において、Sarbanes-Oxley法、Gramm-Leach-Bliley法 (GLB法)、Health Information Portability and Accountability Act (HIPAA) などでますます急務となる厳格なアカウンタビリティを確保するのに役立ちます。ユーザーは監査証跡を保管する期間 (デフォルトの期間は6か月) を選択できます。また、監査証跡 (および、その他のSAデータ) を長期間保管するためのデータウェアハウスを容易に作成することができます。

監査証跡はAUDIT_DATA表領域に格納されており、次の表が含まれています。

AUDIT_OBJTYPE_ATTR

AUDIT_OBJECT_TYPES

AUDIT_OBJECT_COLLECTORS

AUDIT_OBJECT_ATTR

AUDIT_FEATURES

AUDIT_EVENT_OBJECTS

AUDIT_EVENT_DETAIL_VALUES

AUDIT_EVENT_DETAILS

AUDIT_EVENTS

AUDIT_DATA_TYPES

AUDIT_DATA_OBJECTS

AUDIT_DATAOBJ_VALUES

AUDIT_CONFIG_PARAMS

AUDIT_COMPONENTS

AUDIT_ACTIONS

ソフトウェアリポジトリ内のパッケージの署名付きSHAチェックサム

SA ユーザーがソフトウェアリポジトリにソフトウェアをアップロードする場合、SA はパッケージの RSA-with-SHA1 署名を自動的に計算します。この署名を生成するため、SAはSHA1 チェックサムの計算、ソフトウェアパッケージの内容、および内部RSAプライベートキー (ソフトウェアリポジトリのみが把握) を組み合わせて使用します。このプライベートキーを変更することはできません。このため、ユーザーによるソフトウェアリポジトリ内のソフトウェアの改ざんを防ぐことができます。パッケージと対応するデジタル署名は、ソフトウェアリポジトリでローカルに保管されます。SAでは、管理対象サーバーにソフトウェアをインストールする際に、RSAキーとソフトウェアのSHA1署名を検証してからダウンロードを許可します。これにより、SAでインストールするソフトウェアをソフトウェアリポジトリにアップロードされたソフトウェアと完全に同じにすることができます。

役割ベースの承認

SAでは、きめ細かな役割ベースのアクセス制御が適用されます。セキュリティ管理者は、次のパラメーターに関する承認を設定できます。

- ファシリティ : ファシリティは、1つのSAコアで管理される一連のサーバーです。データセンター、サーバールーム、コンピュータールームの全体または一部がファシリティに該当します。ファシリティは、きめ細かな役割ベースの承認モデルにおける最上位レベルの抽象化です。
- サーバーのグループ (カスタマー別): サーバーはカスタマーごとにグループ化され、1つのデータセンター内のサーバーの任意のグループを表すことができます。グループでは、支払いを行うカスタマー、コストセンター、または Siebel や経費報告アプリケーションなどの特定のビジネスアプリケーションが稼働するサーバーを表すことができます。SAで管理されるソフトウェアパッケージはそれぞれ特定のカスタマーに属しますが、「カスタマー独立」という特殊なアカウントに属する場合もあります。この場合、ソフトウェアは任意のカスタマーのサーバーに対してプロビジョニングできます (たとえば、パッチはカスタマーアカウント「カスタマー独立」に属します)。これにより、セキュリティ管理者は特定のサーバーグループに適用できるソフトウェアパッケージ一式を正確に制御できます。

- サーバーの動的グループ (ルールベース): セキュリティ管理者は、(簡単または複雑な) 動的ルール評価に基づいたサーバーグループを作成して、そのグループに属するすべてのサーバーにアクセス権を割り当てることもできます。たとえば、セキュリティ管理者はLinuxオペレーティングシステムが稼働し、特定のIPアドレス空間に存在する管理対象サーバーをグループ化して、このサーバーグループで管理タスクを実行できるSAユーザーグループを割り当てることができます。
- ソフトウェアポリシーのモデル化と配布: ソフトウェアポリシーのモデル化は、フォルダーモデルを使用してソフトウェアをモデル化する強力なメカニズムです。フォルダーでは、セキュリティのアクセス権を定義して、ユーザーグループ間でのフォルダーの内容へのアクセスを制御できます。フォルダーのアクセス権を設定すると、フォルダー内のアイテムを表示、使用、変更できるユーザーグループを特定できます。

ユーザーアクティビティの監査ログ

SAでは、モデルリポジトリに監査証跡を一元的に保管します。監査証跡の各エントリはデジタル署名されます。SAは、監査ログに対する変更が検知されないことがないように、強力な暗号制御を用いて新たに設計されたものです。監査ログは一元的に保管されるため、管理対象サーバーから削除することはできません。実際、SAの全体的なセキュリティ設計は、個別の管理対象サーバーのセキュリティの侵害がシステム全体のセキュリティに悪影響を及ぼさないという前提に基づいて、防御を重視したものになっています。

SA内部通信のセキュリティ保護

SAには、セキュリティ保護された通信チャネル (通常はHTTPSなどの業界標準プロトコル) を介して相互に情報をやり取りする複数のコアコンポーネントが含まれます。これらのコンポーネントには、次の内容が含まれます。

- ローカルデスクトップまたはサーバー上でセキュアなブラウザーを実行するSAユーザー。SAブラウザーは、HTTPSを使用してSAコマンドセンターとセキュアに通信します。ユーザーはユーザー名とパスワードを入力してSAにログインします。これらの資格情報は、SA内または必要に応じて統合された外部LDAPサーバーで認証されます。
- 管理対象サーバー上で実行される SA サーバーエージェント。SA サーバーエージェントは、SA コアコンポーネントと通信する際にクライアントとサーバーの両方の役割を果たします。通信はすべて暗号化されて、完全性のチェックが行われます。また、SSL/TLSを使用する際にクライアント証明書を使用して認証されます。一部のコアコンポーネントは特定のTCP/IPポートを介してSAエージェントにコマンドを送信できます。SAエージェントは、それぞれ指定ポートを使用してコアコンポーネントにコールバックすることもできます。
- 少数のサーバー上で実行されるバックエンドプロセスであるSAコアコンポーネント。SAコアコンポーネントは、他のSAコアコンポーネントやSAエージェントと通信します。ここでも、SSL/TLSを用いて認証が行われます。

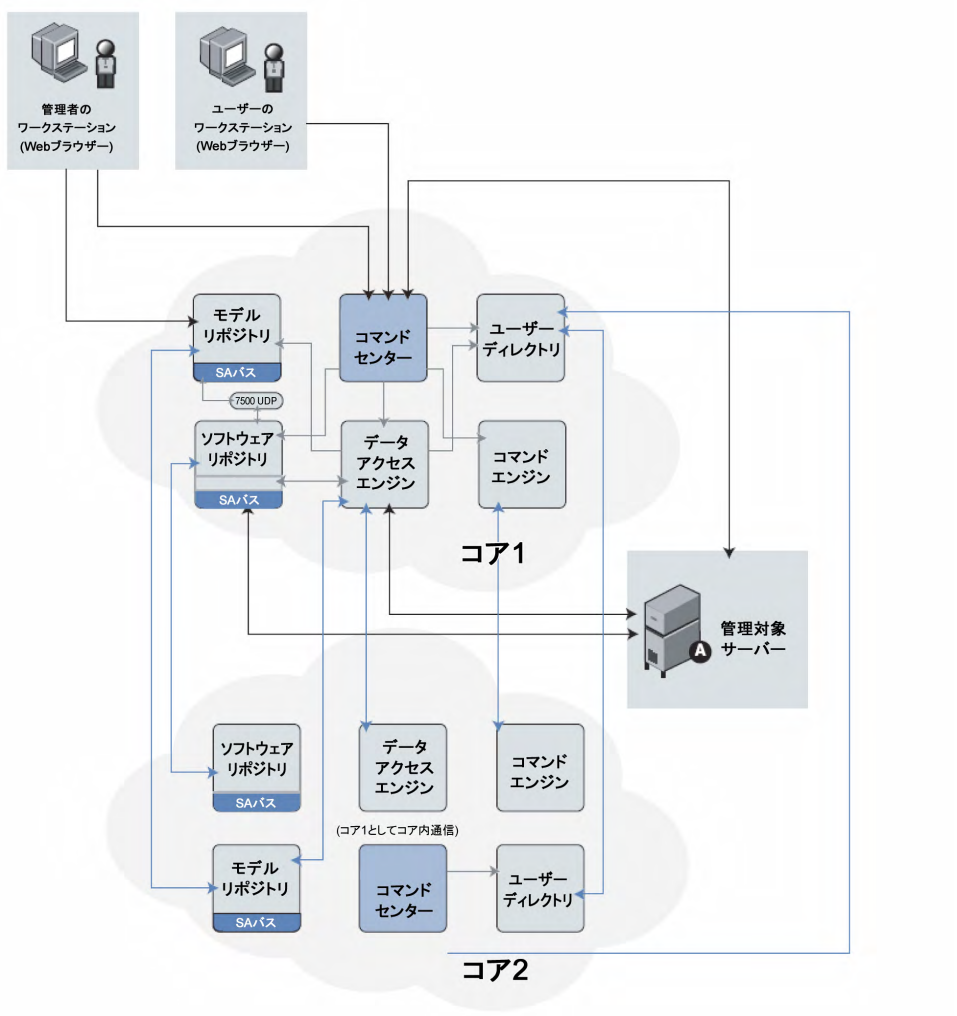
複数のデータセンターでSAを稼働させているカスタマーの場合、SA (SA Bus) に組み込まれた証明書付きメッセージングを使用して、所定のセキュアチャネルを介してSAコア間でも通信が行われます。

SAでは、分散コンポーネント間の通信チャネルを保護することにより、何者かがネットワークトラフィックを解析したり、SAを使用してSAの管理対象サーバー上で不正なタスクを実行したりするのを防いでいます。

SAコアのコンポーネント間の通信

SAコンポーネントが他のコンポーネントと通信する必要がある場合は、Well-knownポートを使用してセキュアな(通常はSSL/TLSの)通信チャネルを開きます。SAの各コンポーネントには、SAのインストール時に生成されたパブリックキー証明書があります。コンポーネントは、他のコンポーネントに対して認証を行う際に、それぞれのパブリックキー証明書を使用します。このようにして、ほとんどのプロセス間通信の確実な認証、利用可能な中で最も強力な暗号を使用した暗号化、完全性のチェックが行われます。

図21　　コンポーネントの通信



エージェントとSAコアコンポーネントとの間の通信

サーバーエージェントは上記の認証され、暗号化されたSSL/TLSトラフィックに関与します。また、エージェントがサーバー上で管理タスクを実行するように指示を受けたときに、(下記の)制御メッセージの一般的なフローによって、承認されたユーザーのみに該当のアクションを実行させることができます。このため、侵入者がエージェントに不正なタスクを実行させる有効なコマンドシーケンスを生成することは非常に困難です。

次のシーケンスは、SAの一般的な管理タスク (管理対象サーバーでのソフトウェアのプロビジョニング) を表しています。管理対象サーバー上のその他の操作は、同じ一般的なプロトコルに従います。

1. データアクセスエンジンがHTTPSを介してSAサーバーエージェントとの間の通信チャネルを開き、エージェントに管理タスクを実行するように指示します。
2. SAエージェントは、データアクセスエンジンにコールバックして、実行するタスクに関する詳細を取得します。通信チャネルを開始するには、エージェントはそれぞれのパブリックキー証明書を提示する必要があります。SA コアは証明書をマシンの IP に対応付ける内部データベースとエージェントのインストール時にSAで生成される一意のマシンIDと照らしあわせてパブリックキー証明書を確認します。このセキュリティ対策により、ユーザーがデジタル証明書と対応するキーを別のマシンにコピーしても、元の管理対象サーバーになりすますことはできません。

   通信チャネルが正常に開始されたら、SAエージェントはインストールおよび削除対象のソフトウェアのリスト (および実行するスクリプト、ソフトウェアインストールの順序、プロビジョニング時の再起動タイミング) を受け取ります。
3. SAエージェントはソフトウェアリポジトリに対する通信チャネルを (同様にHTTPSを介して) 開き、インストールに必要なソフトウェアのダウンロードを要求します。ソフトウェアリポジトリはダウンロードを開始する前に、ソフトウェアリポジトリで認識している秘密キーを使用してパッケージの SHA チェックサムを再計算します。SHA チェックサムがパッケージのアップロード時に生成されたチェックサムと一致する場合にのみ、SAエージェントは要求したソフトウェアを受け取ります。

エージェントから非同期的にSAコアに対して要求を行うことで、進行状況レポートや長時間の操作をスケーラブルにサポートできます。これは、SAコアでエージェントの数多くの同期操作を直接管理する必要がないためです。SAゲートウェイインフラストラクチャーでは、単一方向の接続上で双方向トンネリングが利用できるため、SAは、ファイアウォールによってエージェントがTCP接続を開始できないネットワーク環境でも、エージェントからコアへの非同期要求をサポートします。

エージェントとコアとの通信には、その他に次のような技術的特徴があります。

- 接続はSSL v3 で、X.509証明書により相互に認証されます (サーバーはクライアントの証明書をチェックし、クライアントはサーバーの証明書をチェックします)。
- コアおよびエージェントの証明書のプライベートキーは、root でのみ読み取り可能なファイル内に保管されます。
- 証明書はすべてインストール時に生成され、カスタマーが所有します。証明書がHPに知られることはありません。
- 証明書の有効期限はインストール後 10 年間です。SA には、証明書の有効期限が切れる前にコアおよびエージェントを再認定するための再認定ツールが用意されています。
- 証明書はSA内部の自己署名証明機関によって署名されます。WebブラウザーでHTTPS セキュリティの警告を回避するため、カスタマーはApacheのSAインスタンスに外部署名証明書をインストールすることができます。

SAコア間の通信

複数のデータセンターでSAを実行する場合、SAはSAの管理対象データセンターの関連するデータを自動的に同期します。大まかに、SAで同期されるデータは、サーバーのSAモデル (すべてのハードウェア、ソフトウェア、構成の属性情報を含む) とソフトウェアパッケージそのものの2種類です。

- **SAモデルの複製**: SAは組み込まれた証明書付きメッセージングを使用して、SAモデルデータを同期します。SA は SSL を使用してメッセージバスを流れるメッセージを保護します。実際のメッセージでは、通信の受信側のSAデータベースに対するSQLの変更について記述します。

- ソフトウェアパッケージの複製: SAはソフトウェアパッケージをオンデマンドで複製します。つまり、ソフトウェアパッケージは必要なときにのみコピーされます。ニュージャージーのデータセンターでサーバーを管理している管理者が、ニュージャージーのソフトウェアリポジトリ内に存在しないソフトウェアパッケージをインストールするようにSAに指示すると、SAは別のデータセンターからソフトウェアパッケージを要求します。実際のファイル転送には、オープンソースユーティリティ `rsync` を使用し、通信チャネルはSSHを使用して保護します。

SAサテライトのアーキテクチャーとセキュリティ

完全なSAコアではなく、SAサテライトを別の場所にインストールすると、リモートサーバーの管理を行うことが可能になります。サテライトでは、SAコアと同様にデータセンターサーバーをシームレスに管理できます。このサテライトは、SAゲートウェイとソフトウェアリポジトリキャッシュで構成されます。サテライトゲートウェイは、サテライトに対するネットワーク接続と帯域幅の管理を行います。サテライトは複数のゲートウェイを持つことができます。ソフトウェアリポジトリキャッシュには、サテライトから管理対象サーバーにインストールするソフトウェアパッケージのローカルコピーが格納されます。必要に応じて、サテライトには、OSプロビジョニングのブートサーバーやメディアサーバーコンポーネントを含めることができます。サテライトは最低1つのコア(単一コアまたはマルチマスターメッシュの一部)とリンクする必要があります。複数のサテライトは1つの単一コアにリンクすることができます。

サテライトの主要な機能は、次のとおりです。

- ネットワークの複雑さに関係なく自動化できる: サテライトは、帯域幅の小さな接続、重複のある複雑なIPアドレス空間、およびファイアウォールを含む環境で使用できるように最適化されています。
- ネットワーク障害に対応できる: SAサテライトは、高度なリンクステートルーティングアルゴリズムを実装しているため、障害の発生したネットワークリンクを迂回して動的にルーティングを行う冗長性を備えています。
- リモートサーバーのセキュリティを確保できる: サテライトによって、IT組織は、ポリシーベースのパッチ管理、デジタル署名付きの暗号化されたパッケージインストール、サーバーのすべての変更履歴を記録する包括的な監査証跡を通じて、リモートサーバーのセキュリティを積極的に確保することができます。

SAネットワーク: 効果的なリスク緩和

新たな脆弱性は絶え間なく見つかります。SAネットワークは、それぞれのSAインストール環境にすぐに使用できて、マルチベンダー対応で、優先度付けが可能なセキュリティアラートを提供する独自のサービスです。SAネットワークでは、脆弱性に関する通知を受けてすぐにその脆弱性を見つけ出して、リソースを無駄にすることなく、適切な修正をデプロイすることができます。

1つの標準ですべてのニーズに対応できるわけではないため、SAネットワークでは、各カスタマー固有のニーズに合わせたカスタマイズや拡張が容易な、幅広いコンプライアンスポリシーを用意しています。

現在、SAネットワークは、次の3つのコンプライアンス標準に重点を置いています。

1. **Center for Internet Security (CIS) 標準**: オペレーティングシステムに基づいてサーバーのセキュリティを確保する方法を詳細に定めた一連の標準。(http://www.cisecurity.org/)
2. **Microsoft (MS) セキュリティガイド**: Windowsサーバーを強化するための構成設定について詳しく説明したMicrosoftが作成した標準。(http://www.microsoft.com/)
3. **米国国家安全保証局 (NSA) のセキュリティ構成ガイド (SCG)**: 各種OSおよびアプリケーションを強化するための構成設定について詳しく説明した米国の国家安全保障局が定めた標準。(http://www.nsa.gov/)

SAの他のセキュリティツールとの互換性

SAは、侵入検知システム、脆弱性評価製品、ウイルス対策スキャナー、完全性保証製品など、既存のさまざまなセキュリティツールと組み合せて使用します。SAを使用すると、これらのツールをサーバーの効果的な保護に役立てるような変更管理を実現できます。具体的には、SAを使用することにより、これらのシステムで使用するエージェントを一貫性のある形でインストールして構成し、構成(最新のウイルス対策定義ファイルなど)を常に最新の状態に維持し、これらのシステムで通知された脆弱性(パッチの未適用や不適切な構成など)に対処することができます。

SAコアの再認定

SAのコア再認定ツールを使用すると、SAコアとエージェントを再認定することができます。コア再認定ツールでは、新規のセキュリティ証明書が自動的かつすみやかに発行されます。

➤ このツールは、既存のエージェント再認定ツールとは別ですが、互換性があります。詳細については、エージェント再認定 (108ページ) を参照してください。

コア再認定ツールの主な利点は、次のとおりです。

- SAのすべての証明書を有効期限が切れる前に再生成できます。これにより、証明書の有効期限を効果的に短縮できます。
- 証明書のセキュリティの侵害を緩和できます。

SAは、X.509 v3証明書を使用して認証、承認、セキュアなネットワーク通信を実現する独立したパブリックキーインフラストラクチャー(PKI)システムです。X.509証明書は、指定されたプリンシパルをパブリックキーと結び付ける一種の識別情報です。

証明書はそれぞれの対応するプライベートキーと組み合せてデジタルIDになります。他の多くの識別情報と同じように、証明書には有効期間があります。X.509証明書の有効期間は、`Not Before`と`Not After`の日付を使用して指定します。現在の日付がその有効期間に含まれる場合に限り、X.509証明書は有効であるとみなされます。逆に、現在の日付がその有効期間に含まれない場合、X.509証明書は無効であるとみなされます。SAでは、無効な証明書は使用できません。

SAのCAは起動時に自動的に生成され、その後はコアコンポーネントの証明書の発行に使用されます。SAエージェントの証明書は、エージェントを最初に登録する際に、エージェントCAによって発行されます。

SAのすべての証明書の有効期限はデフォルトで10年間です。構成によってSAの証明書の有効期限を変更することはできません。SAの証明書ポリシーを変更するには、カスタマイズを行う必要があります。

SAでは、クラス証明書を使用します。クラス証明書では、クラスのすべてのコアコンポーネントが1つの証明書を共有します。たとえば、コマンドエンジンはすべて、1つのコマンドエンジン証明書を共有します。1つのコマンドエンジン証明書がセキュリティの侵害を受けると、すべてのコマンドエンジン証明書がセキュリティの侵害を受けることになります。さらに、SAでは証明書の失効をサポートしていません。セキュリティの侵害を受けたコアコンポーネント証明書を無効にするには、コア全体を再認定する必要があります。

➤ このリリースのコア再認定ツールは、コアのカスタマイズインストールをサポートしていません。SAの証明書やキーを異なるホストやディレクトリに配置する、SAインストーラーの範囲外で行われたカスタマイズは、このツールではサポートされません。

エージェント再認定とコア再認定

エージェント再認定とコア再認定には、重要な違いがあります。コア再認定では、コアの証明書とすべての管理対象サーバー上のすべてのエージェント証明書を再生成します。エージェント再認定では、管理対象サーバー上のエージェント証明書のみを再生成します。

この項では、完全なコア再認定について説明します。管理対象サーバー上のエージェントのみを再認定する手順については、エージェント再認定 (108ページ) を参照してください。

コア再認定後のアップグレード

コア再認定では、すべてのコアの暗号データベース (CADB) が更新されるわけではありません。最初のコアのCADBのみが最新になります。最初のコアを確認するには、次のコマンド

```
./corerecert --status
```

を再認定を実行したコアの/opt/opsware/oi_util/OpswareCertTool/recert_utils/で実行します。

SAの最新のリリースまたはパッチにアップグレードする際には、事前に次の操作を実行する必要があります。

1. CADB (/var/opt/opsware/crypto/cadb/realm/*) を最初のコアからアップグレードするコアサーバーの同じディレクトリにコピーします。
2. アップグレードするコアサーバーで、次のコマンドを実行します。

```
rm -rf /var/opt/opsware/crypto/oi
rm -rf /var/opt/opsware/crypto/gateway
rm -rf /var/opt/opsware/crypto/dhcp
rm -rf /var/opt/opsware/crypto/word_upload
```

再認定されたSAコアマルチマスターメッシュへの新しいコアの追加

コア再認定の手順では、モデルリポジトリ (truth) データは再署名されず、署名を検証する目的で、古い/アーカイブされたCAと新しいCAの両方がロードされます。

再認定されたメッシュに新しいコアを追加するときには、古い/アーカイブされたCAをすべて手動で新しいコアにコピーする必要があります。

コア再認定のフェーズ

コア再認定には、次のフェーズがあります。必要なフェーズは、それぞれのマルチマスター構成によって異なります。

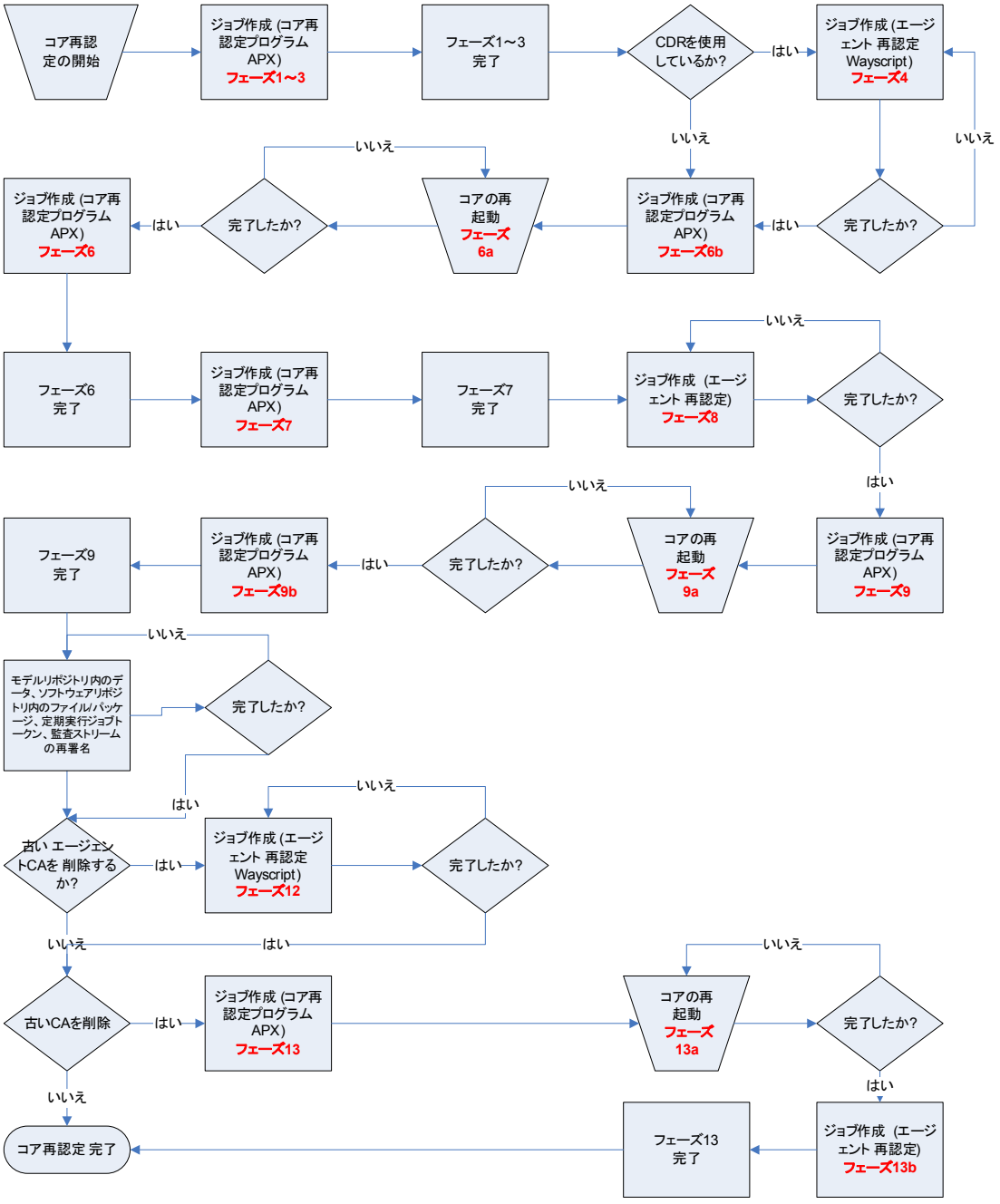
表13は、コア再認定のフェーズに関する説明です。

表13　コア再認定のフェーズ

フェーズ	説明
1〜3	既存の暗号マテリアルのバックアップ、新規の暗号マテリアルの生成、およびすべてのコアコンポーネントへの新規CAの配布を行います。これらの3つのフェーズは、コア再認定ツールを最初に実行したときに順次実行されます。既存の暗号マテリアルはすべて`crypto.<`セッション番号`>`ディレクトリにバックアップされます。コアコンポーネントごとに、専用のバックアップディレクトリが存在します。
4	エージェントが新旧両方のエージェントCAを同時に信頼するように、すべてのエージェントに新規のエージェントCAを配布します。これにより、エージェント間の通信が中断しないようにすることができます。
6a	メッシュの再開: 新旧両方のCA階層を信頼するようにメッシュを再開します。
6b	スケジュール設定されたメッシュの再開の開始: 構成ファイルパラメーターを使用して、メンテナンスウィンドウに合わせてマルチマスターメッシュのコアを再開するための遅延開始をスケジュール設定できます。
7	ゲートウェイを再認定します。
8	エージェントを再認定します。
9a	コアコンポーネントの再認定、最初のコアでのコマンド`touch /var/opt/opsware/crypto/twist/upgradeInProgress`の発行、メッシュの再開、署名の再生成を行います。
9b	メッシュの再開のステータスを確認します。メッシュが正常に再開されている場合は、すべてのコアコンポーネントが古い暗号マテリアルを信頼したまま、新規の暗号マテリアルを使用しています。
11	モデルリポジトリのデータ、ソフトウェアリポジトリのパッケージ/ファイル、および定期実行ジョブトークンと監査ストリームを再署名します。
12	[オプション] 古いエージェントCAを削除します。エージェントCAがセキュリティの侵害を受けたか、古いCAを信頼しなくなった場合のみ必須です。
13a	[オプション] 古いエージェントCA階層を削除します。エージェントCAがセキュリティの侵害を受けたか、古いCA階層を信頼しなくなった場合のみ必須です。
13b	[オプション] メッシュの再開。13aを実行する場合のみ必須です。

図22に、再認定プロセスのフローとフェーズを示します。

図22　　コア再認定のフェーズとフロー



エージェント再認定のフェーズ

図22に示す次の3つのフェーズは、エージェント再認定のフェーズです。

- フェーズ4: 新規のエージェントCAを配布します。エージェント間の通信が中断しないようにすることが、このフェーズの目的です(再認定されたエージェントがまだ再認定されていないエージェントと通信します)。
- フェーズ8: エージェントを再認定します。このフェーズは必須です。新規に暗号マテリアルをエージェントに発行することが、このフェーズの目的です。

- フェーズ 12: 古いエージェント CA をクリーンアップします。このフェーズはオプションです。新旧両方のCA階層を同時に信頼しない場合は、このフェーズで古いCAを削除する必要があります。新旧両方のCA階層を同時に信頼する場合は、このフェーズをスキップできます。

エージェント再認定のジョブ

エージェント再認定の各フェーズは、定期的なジョブで実行されます。このジョブは次のプロパティで指定します。これは、コア再認定構成ファイルで指定する必要があります。

表14　　コア再認定の構成ファイル: エージェント再認定のプロパティ

プロパティ名	必須	説明	例
agent_recert.all.facilities.start_time=<HH:mm>	はい	エージェント再認定フェーズの開始時刻。特定のファシリティに対してこの値を上書きするには、agent_recert.facility.<ファシリティ名>.start_timeプロパティを指定します。 開始時刻は次の形式にする必要があります。 HH:mm、ただし00 <= HH < 24かつ00 <= mm < 60 時間と分の要素のみ必要です。指定した時刻を過ぎている場合、エージェント再認定ジョブはその翌日の指定時刻に開始されます。	agent_recert.all.facilities.start_time=18:30
agent_recert.facility.<ファシリティ名>.start_time=<HH:mm>	いいえ	存在する場合、指定のファシリティの開始時刻がagent_recert.all.facilities.start_timeの代わりに使用されます。	agent_recert.facility.sacramento.start_time=8:00

表14　コア再認定の構成ファイル: エージェント再認定のプロパティ（続き）

プロパティ名	必須	説明	例
agent_recert.all.facilities.duration=<時間>	はい	エージェント再認定ジョブの期間 (時間)。期間では、エージェント再認定ジョブが停止せずに実行し続ける時間の長さを指定します。期間を過ぎて成功率に到達しない場合、エージェント再認定ジョブは次の開始時刻に再開されます。特定のファシリティに対してこの値を上書きするには、agent_recert.facility.<ファシリティ名>.durationプロパティを指定します。 期間は1～24の整数値でなければなりません。	agent.recert.all.facilities.duration=8
agent_recert.facility.<ファシリティ名>.duration=<hours>	いいえ	存在する場合、指定のファシリティの期間がagent_recert.all.facilities.durationの代わりに使用されます。	agent_recert.facility.sacramento.duration=10
agent_recert.all.facilities.success_rate=<全体の割合>	はい	エージェント再認定ジョブのファシリティごとの成功率 (全体の割合)。たとえば、1000の管理対象サーバーがファシリティ Xに存在し、成功率が98% である場合、980の管理対象サーバーが正常に再認定されると、エージェント再認定ジョブは停止します。 特定のファシリティに対してこの値を上書きするには、agent_recert.facility.<ファシリティ名>.success_rateプロパティを指定します。 成功率は1～100の整数値でなければなりません。	agent_recert.all.facilities.success_rate=100

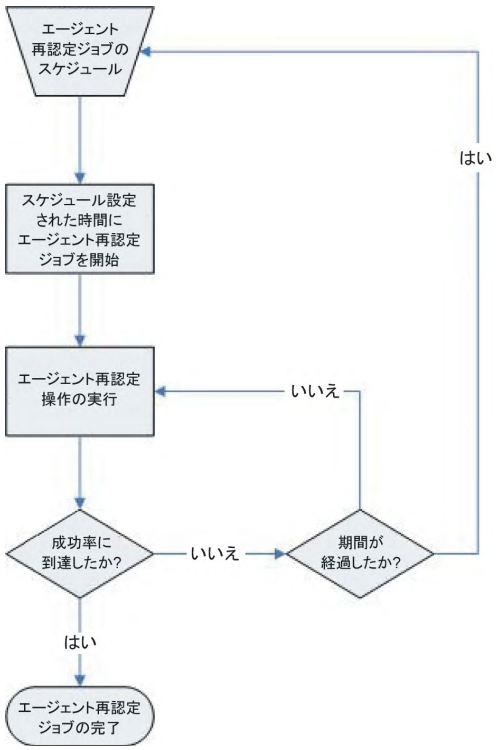
表14　コア再認定の構成ファイル: エージェント再認定のプロパティ（続き）

プロパティ名	必須	説明	例
agent_recert.facility.<ファシリティ名>.success_rate=<全体の割合>	いいえ	存在する場合、指定のファシリティの成功率がagent_recert.all.facilities.success_rateの代わりに使用されます。	agent_recert.facility.sacramento.success_rate=99
agent_recert.all.facilities.job_notification=<電子メールアドレス>	いいえ	エージェント再認定ジョブのジョブ通知。特定のファシリティに対してこの値を上書きするには、agent_recert.facility.<ファシリティ名>.job_notificatFionプロパティを指定します。	agent_recert.all.facilities.job_notification=admin@example.com
agent_recert.facility.<ファシリティ名>.job_notification=<電子メールアドレス>	いいえ	存在する場合、指定のファシリティのジョブ通知がagent_recert.all.facilities.job_notificationの代わりに使用されます。	agent_recert.facility.sacramento.job_notification=admin3@example.com

エージェント再認定のジョブフロー

図23に、エージェント再認定のジョブフローを示します。

図23　エージェント再認定のジョブフロー



スケジュール設定されたエージェント再認定ジョブまたはアクティブなエージェント再認定ジョブは、任意の時点でファシリティごとに1つだけ存在できます。エージェント再認定ジョブは、次の場合に終了します。

- 成功率に到達した場合
- ジョブを明示的にキャンセルした場合
- 致命的なエラーが発生した場合

SAコア再認定ツールの使用方法

コア再認定ツールを実行するには、次の内容を入力します。

```
/opt/opsware/oi_util/OpswareCertTool/recert_utils/corerecert [--phase
<フェーズ番号>] [--config <構成ファイルへの完全パス>] [--doit]]
[-h, --help] [-v, --version] [-s, --status] [-d, --debug] [--summary]
[--cancel_all_agent_recert_jobs] [--cancel_agent_recert_jobs_for_facility
<ファシリティ名>] [--cancel_all_jobs] [--reason <ジョブのキャンセルの理由>]
[--force_resume <ファシリティ名>]
```

コア再認定ツールの引数

表15は、コア再認定ツールで使用できる引数について説明したものです。

表15　　コア再認定ツールの引数

引数	説明
-h、--help	ヘルプを表示します。
--phase	指定したコア再認定フェーズを開始します。指定できるフェーズ番号は、1、4、6、7、8、9、12、13です。
--config <構成ファイル>	コア再認定構成ファイルへの完全修飾パス。デフォルトの構成ファイルは、次のファイルです。/opt/opsware/oi_util/OpswareCertTool/recert_utils/corerecert.conf
--doit	特定のコア再認定フェーズを再実行(強制的に再実行)します。この機能は、新しく追加したコンポーネントの再認定が完了していない場合に便利です。新規エージェントCAのプッシュや古いエージェントCAの削除など、指定したフェーズをスキップする場合にも使用します。
-v、--version	実行可能ファイルcorerecertのバージョン番号を出力します。
-s、--status	再認定プロセスの現在のステータスを表示します。
-d、--debug	コア再認定をデバッグモードに設定します。デバッグログは/tmp/recerttool.logにあります。
--summary	現在のステータスのサマリー(--statusの短縮版)を出力します。
--cancel_all_agent_recert_jobs	現在スケジュール済みのエージェント再認定ジョブをすべてキャンセルします。

表15　コア再認定ツールの引数（続き）

引数	説明
--cancel_agent_recert_jobs_for_facility <ファシリティ名>	特定のファシリティに対してスケジュール設定されているエージェント再認定ジョブをキャンセルします。
--cancel_all_jobs	コア再認定ジョブとエージェント再認定ジョブをすべてキャンセルします。
--reason <ジョブのキャンセルの理由>	ジョブのキャンセルの理由をオプションで指定します。
--force_resume <facility_name>	エージェント再認定ジョブで構成される任意のファシリティに対して、新規のジョブが自動的にスケジュールされるように指定します。実行に失敗したジョブのファシリティは、スキップされます。または、このパラメーターを指定しなかった場合、各ファシリティのジョブを個別に再開できます。

⚠ コア再認定の際に新規のコアコンポーネントを追加しないでください。コア再認定の際に新規のコアコンポーネント（スライスコンポーネントバンドルやサテライトなど）を追加することは一定の状況で可能ですが、特に必要な場合以外、コア再認定の際に新規のコアコンポーネントを追加することはお勧めできません。コア再認定の実行中に新規のコアコンポーネントを追加する場合は、前もってHPプロフェッショナルサービスにご連絡ください。

⚠ SAの証明書を（SA CAによって発行されたものではない）サードパーティの証明書に置き換えることはサポートの対象外です。サードパーティの証明書のファイル名がSAの証明書と同じである場合、コア再認定の際にサードパーティの証明書が上書きされる可能性があります。SAの証明書をサードパーティCAが発行した証明書に置き換えている場合は、コア再認定を実行する前にHP Server Automationのサポートにご連絡ください。

セキュリティに関する注意事項

次のセキュリティ上の問題点に注意してください。

暗号データベースファイル

SAコア再認定ツールでは、再認定の際にSAの暗号データベースファイルにアクセスする必要があります。

SAの暗号データベースは、次のファイルで構成されます。

/var/opt/opsware/crypto/cadb/realm/opsware-crypto.db.e

このファイルは、メッシュの最初のコアのインストール時に指定した、暗号マテリアルのパスワード（decrypt_passwd）で保護されています。その後のコアのインストール時には、追加したセカンダリコアのホストにこのファイルがコピーされます。暗号データベースファイルがセキュリティの侵害を受けると、マルチマスターメッシュ全体がセキュリティの侵害を受けることになるため、このパスワードは大切に保護する必要があります。

暗号データベースファイルは、SAのインストールまたはアップグレード時にのみ必要ですが、暗号データベースファイルは、コア再認定の際に再生成されます。そのため、HPでは暗号データベースファイルを保護する手順を作成することを強く推奨しています。また、コア再認定を行う際には、事前にこのファイルを安全な場所へバックアップする必要があります。

コア再認定の際に、SAはコア再認定ツールを呼び出したホストでのみ暗号データベースを再生成します。コア再認定によって、新しく生成された暗号データベースファイルが、再認定中にメッシュ内の他のホストへコピーされることはありません。コア再認定が完了したらすぐに、このファイルを安全な場所にバックアップしてください。

また、コアホストへのrootアクセスを厳格に制御することも重要です。コアホストの暗号マテリアル(証明書とそれぞれに対応するプライベートキー)は暗号化されません。これらは、rootユーザーアカウントで保護します。つまり、これらのファイルは、rootユーザーの読み取り専用アクセスによって保護されます。そのため、コアホストに対するrootアクセスを持つユーザーは、暗号マテリアルのパスワードと暗号データベースファイルの両方にアクセスできます。また、コア再認定は、SAのシステム管理者やコアホストへの正規のrootアクセスを持つユーザーのみが行うようにする必要があります。

コア再認定のユーザー

SAコア再認定ツールを使用するユーザーのタイプは、通常、次の3つです。

- コア再認定ユーザー: このユーザーは、コア再認定ツールを実行するのに必要なすべてのアクセス権を持っています。実際には、これはSAシステム管理者/オペレーターと同じユーザーになります。
- SA管理者: コア再認定ユーザーへのSAコア再認定の役割の割り当てと取り消しを行います。
- SAシステム管理者/オペレーター: このユーザーは、特定のコアの再開を行います。このユーザーは、コアホストに対するrootアクセスを持っています。

コア再認定ユーザーの作成

コア再認定ツールを使用するには、コア再認定グループとユーザーを作成して、必要なアクセス権を割り当てる必要があります。

1. SA管理者としてSAコマンドセンターにログオンします。
2. 次のアクセス権を使用して、コア再認定ユーザーグループを作成します。
   - すべてのファシリティに対する読み取り/書き込みアクセス
   - すべてのカスタマーに対する読み取り/書き込みアクセス
   - すべてのデバイスグループに対する読み取り/書き込みアクセス
   - カスタマーの管理
   - ファシリティの管理
   - サーバーとグループの管理
   - コア再認定([クライアント] > [コア再認定])
   - エージェント再認定([クライアント] > [エージェント再認定])
3. コア再認定ユーザーをSAのSystem Administratorsユーザーグループに追加します。

コア再認定ユーザーの削除

コア再認定ユーザーを削除するには、次のタスクを実行します。

1. SA管理者としてSAコマンドセンターにログオンします。
2. コア再認定ユーザーグループからユーザーを削除します。

コア再認定の前提条件

コア再認定を開始する前に、次のタスクを実行する必要があります。

- 暗号マテリアルを保護するための新しいパスワードを選んで、そのパスワードを提示する方法を決めます。
- 適切な値を使用してコア再認定構成ファイルを構成します。
- すべてのコアが正常に稼働していることを確認します。
- コア再認定ツールが正しくメッシュ設定を認識することを確認します。

暗号マテリアルを保護するための新規パスワードの選択

暗号データベースのパスワードは、コア再認定の際に必要です。これは、新しく生成された暗号データベース、PKCS #12ファイル、CAプライベートキーを保護するためです。コア再認定は複数のフェーズで構成され、そのほとんどで暗号データベースのパスワードが必要です。暗号データベースのパスワードの保護は、非常に重要です。

一部のコア再認定タスクは、自動化プラットフォーム拡張 (APX) ジョブによって実行されます。そのため、暗号データベースのパスワードは、困ったことにジョブパラメーターやジョブ監査ログに一時的に表示されることがあります。

ジョブパラメーターや監査ログに暗号データベースパスワードが表示されないようにするには、次の手順でファイルを使って暗号データベースパスワードをやり取りします。

1. コアホストでコア再認定ツールを起動する前に、コアホストのサーバーIDを特定します。サーバーIDは、SA Webクライアントまたは `/etc/opt/opsware/agent/mid`から取得できます。`base_core_server_ref` のサーバー IDの値を、コア再認定構成ファイルで指定する必要があります。
2. 新しい暗号データベースパスワード (例: `cadb_password=`<新しい暗号データベースパスワード>) を含むファイル `/var/opt/opsware/crypto/cadb/__recert_overwrite__`を作成します。このファイルはrootユーザーに対して読み取り専用にします。
3. コア再認定が正常に完了したら、ファイル`/var/opt/opsware/crypto/cadb/__recert_overwrite__` を削除します。

コア再認定構成ファイルで暗号データベースパスワードが要求されるため、セキュリティ対策としてコア再認定構成ファイルで無効なパスワードを指定することができます。

コア再認定では、1つのパスワードですべての暗号マテリアルを保護する必要があります。これには、暗号データベース、PKCS #12ファイル、すべてのCAプライベートキーが含まれます。暗号マテリアルを複数のパスワードで保護するカスタマイズ版の`OpswareCertTool`を使用していて、引き続き複数のパスワードで保護する必要がある場合は、コア再認定ツールを実行する前に、必ずHPプロフェッショナルサービスにご連絡ください。

コア再認定の構成

コア再認定のプロパティはすべて、構成ファイルで指定する必要があります。コア再認定ツールを起動する際に、`-config`引数を使用して構成ファイルの場所を指定することができます。`-config`引数を省略すると、コア再認定ツールは `/opt/opsware/oi_util/OpswareCertTool/recert_utils/corerecert.conf` にあるデフォルトの構成ファイルを使用します。

デフォルトの構成ファイルを直接編集するか、または新規の構成ファイルを作成します。構成ファイルには機密情報が含まれるため、適切に保護することが重要です。たとえば、rootユーザーのみが読み取り/書き込みできるようにします。

表16　コア再認定の構成ファイル: プロパティ

プロパティ名	必須	説明	例
グローバルプロパティ			
username=<ユーザー名>	はい	コア再認定操作を実行する権限を持つユーザーのユーザー名。	username=jdoe
password=<パスワード>	はい	コア再認定操作を実行する権限を持つユーザーのパスワード。	password=dontask
エージェント再認定のプロパティ			
agent_recert.cleanup_old_agent_ca=<0 | 1>	いいえ	コア再認定後に古いエージェントCAをクリーンアップするかどうかを指定します。古いエージェントCAのクリーンアップフェーズは必須ではなく、無効にすることができます。 有効な値は1 (true) または0 (false) です。その他の値を指定すると、プロパティ無効エラーになります。 このプロパティはオプションです。デフォルト: 0	agent_recert.cleanup_old_agent_ca=0
agent_recert.all.facilities.start_time=<YYYY:MM:DD:HH:mm>	はい	すべてのファシリティのエージェント再認定操作のデフォルト開始時刻。 指定したファシリティに対してこの値をオーバーライドできます (agent_recert.facility.<ファシリティ名>.startプロパティを使用してファシリティのデフォルト開始時刻を指定)。 開始時刻は次の形式である必要があります。 YYYY:MM:DD:HH:mm、ただし、2008 <= YYYY <=9999、0 < MM <= 12、0 < DD <= 31、0 <= mm < 12、0 <= MM < 60。	agent_recert.all.facilities.start_time=2009:02:15:23:00

表16　コア再認定の構成ファイル: プロパティ（続き）

プロパティ名	必須	説明	例
agent_recert.facility.<ファシリティ名>.start_time	いいえ	このプロパティを指定すると、特定のファシリティに対してデフォルト開始時刻をオーバーライドできます。 開始時刻は次の形式である必要があります。 YYYY:MM:DD:HH:mm、ただし、2008 <= YYYY <=9999、0 < MM <= 12、0 < DD <= 31、0 <= mm < 12、0 <= MM < 60。	agent_recert.facility.yellow.start_time=2008:5:01:10:00
agent_recert.all.facilities.duration=<HH>	はい	すべてのファシリティのエージェント再認定操作のデフォルトの期間(時間)。 期間は1～24の整数値でなければなりません。 特定のファシリティに対して期間をオーバーライドするには、agent_recert.facility.<ファシリティ名>.durationプロパティを指定します。	agent_recert.all.facilities.duration=2
agent_recert.facility.<ファシリティ名>.duration=<HH>	いいえ	特定のファシリティに対してデフォルト期間をオーバーライドします。	agent_recert.facility.yellow.duration=10
agent_recert.all.facilities.success_rate=<%>	はい	すべてのファシリティのエージェント再認定操作のデフォルト成功率(全体の割合)。 特定のファシリティに対してこの値をオーバーライドするには、agent_recert.facility.<ファシリティ名>.success_rate プロパティを指定します。	agent_recert.all.facilities.success_rate=50
agent_recert.facility.yellow.success_rate=<%>	いいえ	特定のファシリティに対してデフォルト成功率をオーバーライドします。	agent_recert.facility.yellow.success_rate=98

表16　コア再認定の構成ファイル: プロパティ（続き）

プロパティ名	必須	説明	例
agent_recert.all.facilities.job_notification=<電子メールアドレス>	いいえ	エージェント再認定操作のジョブに関するデフォルトの電子メール通知。 特定のファシリティに対してジョブに関するデフォルトの電子メール通知をオーバーライドするには、agent_recert.facility.<ファシリティ名>.job_notificationプロパティを指定します。	agent_recert.all.facilities.job_notification=admin@example.com
agent_recert.facility.<ファシリティ名>.job_notification=<電子メールアドレス>	いいえ	特定のファシリティのジョブに関するデフォルトの電子メール通知をオーバーライドします。	agent_recert.yellow.job_notification=saadmin@example.com
		コア再認定のプロパティ	
cadb_password=<パスワード>	はい	新しく生成される暗号データベースファイルを保護するためのパスワード。	cadb_password=crypto123
debug=<0 | 1>	いいえ	コア再認定ジョブをデバッグモードで実行するかどうかを指定します。使用できる値は1 (true) または0 (false) です。 デバッグログはGlobal Shellの/tmp/core_recert.outにあります。 デフォルト: 0	debug =1
base_core_server_ref=<n>	いいえ	コア再認定を起動するホストのサーバー参照。	base_core_server_ref=10010
job_schedule=<YYYY:MM:DD:HH:mm>	いいえ	現在のコア再認定フェーズのジョブのジョブスケジュール。次の形式を使用する必要があります。YYYY:MM:DD:HH:mm、ただし、2008 <= YYYY <=9999、0 < MM <= 12、0 < DD <= 31、0 <= HH < 12、0 <= mm < 60。 このプロパティが指定されていない場合、ジョブはすぐに開始されます。	job_schedule=2009:2:12:23:05

表16　コア再認定の構成ファイル: プロパティ（続き）

プロパティ名	必須	説明	例
job_schedule.gateway_recert.<ファシリティ名>=<YYYY:MM:DD:HH:mm>	いいえ	特定のファシリティのゲートウェイ再認定フェーズのジョブスケジュール。次の形式を使用する必要があります。YYYY:MM:DD:HH:mm、ただし、2008 <= YYYY <=9999、0 < MM <= 12、0 < DD <= 31、0 <= HH < 12、0 <= mm < 60。 このプロパティが指定されていない場合は、ゲートウェイ再認定フェーズのjob_scheduleプロパティが使用されます。	job_schedule.gateway_recert.<ファシリティ名>=2009:2:12:23:05
job_notification=<電子メールアドレス>	いいえ	すべてのコア再認定フェーズのジョブのジョブ通知。 特定のフェーズに対してこの値をオーバーライドするには、job_notification.<フェーズ番号>プロパティを指定します。	job_notification=admin@example.com>
job_notification.<フェーズ番号>=<電子メールアドレス>	いいえ	指定したコア再認定フェーズのジョブ通知。	job_notification.7= saadmin@example.com
job_notification.gateway_recert.<ファシリティ名>=<電子メールアドレス>	いいえ	特定のファシリティのゲートウェイ再認定フェーズのジョブ通知。	job_notification.gateway_recert.yellow=admin@acme.com
cleanup_old_opsware_ca=<0 | 1>	いいえ	コア再認定後に古いSA CAを消去するかどうかを指定します。 CAがセキュリティの侵害を受けた場合を除き、SA CAをクリーンアップする必要はありません。ほとんどの場合、古いSA CAのクリーンアップは必要ないため、無効にします。 有効な値は1 (true) または0 (false) です。その他の値を指定すると、プロパティ無効エラーになります。 デフォルト: 0 (false)	cleanup_old_opsware_ca=1

すべてのコアが実行中であることの確認/競合の解決

コア再認定を実行する前に、再認定対象のすべてのコアでシステム診断を実行して、すべてのコアが正常に実行されていることを確認することを強く推奨します。また、マルチマスターツールを使用して、トランザクションの競合を検出して解決しておくようにしてください。詳細については、システム診断の実行 (216ページ) およびメッシュの競合の解決 - SAクライアント (118ページ) を参照してください。

コア再認定ツールがメッシュ設定を正しく認識することの確認

次のタスクを実行して、コア再認定ツールでメッシュ設定が正しく認識されることを確認する必要があります。

1. コマンドラインから、rootユーザーとしてSAコアホストにログオンします。
2. 次のコマンドを実行します。

   ```
   /opt/opsware/oi_util/OpswareCertTool/recert_utils/discover_mesh -p
   ```

3. 出力をチェックして、現在のメッシュ設定を反映していることを確認します。現在のメッシュ設定を反映していない場合は、コア再認定を行う前に、HPプロフェッショナルサービスにご連絡ください。

SAコアの再認定

コア再認定を開始する前に、マルチマスターメッシュでバックログと競合をすべてクリアしておく必要があります。

SAコアを再認定するには、次のタスクを実行します。

1. 自分がコア再認定ユーザーであることを確認します。コア再認定ユーザーでない場合は、SAのシステム管理者に確認してください。
2. SAコアホストにログオンします。
3. ディレクトリを`/opt/opsware/oi_util/OpswareCertTool/recert_utils/`に変更します。
4. 次のファイル

   ```
   corerecert.conf
   ```

   を編集して、環境の情報が正しいことを確認します。
5. 次のコマンド

   ```
   corerecert --status
   ```

   を実行して、コア再認定が実行中でないことを確認します。
6. 次のコマンド

   ```
   discover_mesh -p
   ```

   を実行して、コア再認定ツールでメッシュ設定を正しく検出できることを確認します。
7. 次のコマンド

   ```
   corerecert --phase 1
   ```

   をコマンドラインから実行してコア再認定を開始します。
8. 次のコマンド

   ```
   corerecert --status
   ```

   を実行して進行状況を画面に表示し、フェーズ4が進行中になるのを確認します。
9. 次のコマンド

   ```
   corerecert --phase 4
   ```

をコマンドラインから実行してフェーズ4を開始します。これにより、新しいエージェントCAがすべてのエージェントに追加されます。

10 次のコマンド

```
corerecert --status
```

を実行して進行状況を画面に表示し、すべてのエージェントに新しいエージェントCAが追加されるのを確認します。

それぞれのメンテナンスウィンドウやエージェントの可用性により、この手順には数日を要する可能性があります。スケジュール設定されたエージェント再認定ジョブまたはアクティブなエージェント再認定ジョブは、任意の時点でファシリティごとに1つだけ存在できます。この段階でエラーが発生した場合は、エラーを修正して手順9 (105ページ) に戻ります。再スケジュールする必要があるのは、エラーが発生したファシリティのみです。エラーが発生しなかったファシリティのエージェント再認定ジョブを再スケジュールする必要はありません。

11 次のコマンド

```
corerecert --phase 6
```

をコマンドラインから実行して、コア再認定のフェーズ6を開始します。

12 次のコマンド

```
corerecert --status
```

を実行して進行状況を画面に表示し、mesh_restart_pendingと表示されるのを確認します。

ここで、SAシステム管理者と連携してメッシュを再開する必要があります。

それぞれのメンテナンスウィンドウにより、この手順には数日を要する可能性があります。この段階でエラーが発生した場合は、エラーを修正して手順11 (106ページ) に戻ります。

13 メッシュが正常に再開された後に、次のコマンド

```
corerecert --phase 6
```

をコマンドラインから実行してフェーズ6を続行します。

14 次のコマンド

```
corerecert --status
```

を実行して進行状況を画面に表示し、フェーズ7が開始できるようになるのを確認します。この段階でエラーが発生した場合は、エラーを修正して手順13 (106ページ) に戻ります。

15 次のコマンド

```
corerecert --phase 7
```

をコマンドラインから実行してフェーズ7を開始します。

16 次のコマンド

```
corerecert --status
```

を実行して進行状況を画面に表示し、フェーズ8が開始できるようになるのを確認します。この段階でエラーが発生した場合は、エラーを修正して手順15 (106ページ) に戻ります。

17 次のコマンド

```
corerecert --phase 8
```

をコマンドラインから実行してフェーズ8を開始します。これにより、すべてのエージェントが再認定されます。

18 次のコマンド

```
corerecert --status
```

を実行して進行状況を画面に表示し、すべてのエージェントが正常に再認定されるのを確認します。

➤ カスタマーのメンテナンスウィンドウやエージェントの可用性により、この手順には数日を要する可能性があります。スケジュール設定されたエージェント再認定ジョブまたはアクティブなエージェント再認定ジョブは、任意の時点でファシリティごとに1つだけ存在できます。この段階でエラーが発生した場合は、エラーを修正して手順17 (106ページ) に戻ります。再スケジュールする必要があるのは、エラーが発生したファシリティのみです。エラーが発生しなかったファシリティのエージェント再認定ジョブを再スケジュールする必要はありません。

19 次のコマンド

```
corerecert --phase 9
```

をコマンドラインから実行してフェーズ9を開始します。コア再認定ツールに、フェーズ9を開始するかどうかを確認するメッセージが表示されます。yを押して続行します。

20 次のコマンド

```
corerecert --status
```

を実行して進行状況を画面に表示し、mesh_restart_pendingと表示されるのを確認します。この段階でエラーが発生した場合は、エラーを修正して手順19 (107ページ) に戻ります。

ここで、SAシステム管理者と連携してメッシュを再開する必要があります。

➤ カスタマーのメンテナンスウィンドウにより、この手順には数日を要する可能性があります。この段階でエラーが発生した場合は、エラーを修正して手順19 (107ページ) に戻ります。再スケジュールする必要があるのは、エラーが発生したファシリティのみです。エラーが発生しなかったファシリティのエージェント再認定ジョブを再スケジュールする必要はありません。

21 ベーススライスコアサーバーで

a 次のコマンドを入力します。

```
touch /var/opt/opsware/crypto/twist/upgradeInProgress
/etc/init.d/opsware-sas restart
```

b 再開が正常に終了するまで待機し、続いて、

c 残りのメッシュを再開します。

22 メッシュが正常に再開した後に、再認定ユーザーは次のコマンド

```
corerecert --phase 9
```

をコマンドラインから実行してフェーズ9を続行します。

23 次のコマンド

```
corerecert --status
```

を実行して進行状況を画面に表示し、フェーズ11が開始できるようになるのを確認します。この段階でエラーが発生した場合は、エラーを修正して手順22 (107ページ) に戻ります。

24 ベーススライスコアサーバーで

a 次のコマンドを入力します。

```
touch /opt/opsware/oi_util/OpswareCertTool/recert_utils/
TruthResignStatus.txt /opt/opsware/oi_util/OpswareCertTool/
recert_utils/WordResignStatus.txt
```

b フェーズ11:

```
corerecert -phase 11
```

コマンドラインからフェーズ11を開始して、モデルリポジトリ、ソフトウェアリポジトリ、定期的ジョブ、および監査ストリームのデータに再署名します。

25 次のコマンド

```
corerecert --status
```

を実行して進行状況を画面に表示し、フェーズ12が開始できるようになるのを確認します。この段階でエラーが発生した場合は、エラーを修正して107ページの手順24bに戻ります。

26 エージェントCAの削除を行わない場合は、手順28 (108ページ) へ進みます。エージェントCAを削除する場合は、次のコマンド

```
corerecert --phase 12
```

をコマンドラインから実行してフェーズ12を開始します。これにより、古いエージェントCAがすべてのエージェントから削除されます。

27 次のコマンド

```
corerecert --status
```

を実行して進行状況を画面に表示し、古いエージェントCAがすべてのエージェントから削除されるのを確認します。

➤ カスタマーのメンテナンスウィンドウやエージェントの可用性により、この手順には数日を要する可能性があります。この段階でエラーが発生した場合は、エラーを修正して手順26 (108ページ) に戻ります。再スケジュールする必要があるのは、エラーが発生したファシリティのみです。エラーが発生しなかったファシリティのエージェント再認定ジョブを再スケジュールする必要はありません。

28 次のコマンド

```
corerecert --phase 13
```

をコマンドラインから実行してフェーズ13を開始します。古いCAを削除しない場合は、このフェーズでメッシュの再開を行う必要はありません。

29 次のコマンド

```
corerecert --status
```

を実行して進行状況を画面に表示し、`mesh_restart_pend`と表示されるのを確認します。

ここで、SAシステム管理者と連携してメッシュを再開する必要があります。

➤ カスタマーのメンテナンスウィンドウにより、この手順には数日を要する可能性があります。この段階でエラーが発生した場合は、エラーを修正して手順28 (108ページ) に戻ります。

30 メッシュが正常に再開された後に、次のコマンド

```
corerecert --phase 13
```

をコマンドラインから実行してフェーズ13を続行します。

31 次のコマンド

```
corerecert --status
```

を実行して進行状況を画面に表示し、コア再認定が完了するのを確認します。

エージェント再認定

この項では、1つまたは複数の管理対象サーバーでエージェントを再認定する方法について説明します。完全なコア再認定のプロセスとは異なり、1つまたは複数のサーバーでエージェントを再認定することができます。完全なコア再認定では、コアとすべてのエージェントが再認定されます。詳細については、エージェント再認定とコア再認定 (91ページ) およびSAコアの再認定 (90ページ) を参照してください。

1つまたは複数の管理対象サーバーでエージェントを再認定するには、次の手順を実行します。

1 SAクライアントで、[デバイス] タブを選択します。

2 [サーバー] ノードの下で、[すべての管理対象サーバー] または [仮想サーバー] を選択します。これにより、該当するサーバーがすべて表示されます。

または、[デバイスグループ] で、デバイスグループを1つまたは複数選択します。

3 [**アクション**] メニューを選択するか右クリックをして、[**拡張の実行**] > [**エージェントの再認定**] を選択します。

[**拡張の実行**] > [**エージェントの再認定**] が表示されない場合は、[**拡張の実行**] > [**拡張の選択**] を選択します。これにより、[拡張の選択] ウィンドウが開き、実行可能な拡張が表示されます。[拡張の選択] ウィンドウで**エージェント再認定の対象デバイス**を選択して、[OK] を選択します。

これにより、[プログラム拡張の実行] ウィンドウに、選択したサーバーまたはデバイスグループが表示されます。

4 [ジョブの開始] ボタンを選択すると、いつでも残りのデフォルト設定をそのまま使用してジョブを実行することができます。

5 必要に応じて、[デバイスを含める] ボタンを使用して、サーバーまたはデバイスグループを追加します。

6 必要に応じて、[削除] ボタンを使用して、サーバーまたはデバイスグループを削除します。

7 [次へ] ボタンを選択します。[プログラム] 画面が表示されます。[プログラム] 画面では、変更を行わないでください。

8 [次へ] ボタンを選択します。[オプション] 画面が表示されます。

9 [オプション] 画面では、プログラムのタイムアウト値の変更、-debugオプションを使用したジョブに関する詳細情報の要求、または保存するジョブ出力量の指定を行うことができます。

a プログラムのタイムアウト – エージェント再認定ジョブを実行する時間の最大値（分）を指定します。エージェント再認定ジョブが失敗した場合、ジョブは指定された時間が過ぎるまで継続して実行されます。指定された時間を過ぎてもジョブが成功しない場合、ジョブは中止されてエラーメッセージが表示されます。

b 使用オプション – ジョブに関する詳細を追加で表示する場合は、テキストボックスに「-debug」と入力します。

c 出力オプション – ジョブの終了後にプログラムの出力で実行する内容を指定します。[すべてのプログラム出力の破棄] を指定すると、完了したジョブを開いたときに、出力がすべて使用できなくなります。

10 [次へ] ボタンを選択します。[スケジュール設定] 画面が表示されます。ジョブを実行する時刻を指定します。

11 [次へ] ボタンを選択します。[通知] 画面が表示されます。

12 [通知] 画面では、電子メール受信者と、ジョブの失敗、成功、またはその両方のいずれの場合に電子メールメッセージを受信するかを指定します。

13 [次へ] ボタンを選択します。[ジョブステータス] 画面が表示されます。

14 [ジョブの開始] ボタンを選択します。これにより、ジョブが開始されてステータスが表示されます。

15 ジョブのステータスの詳細を表示するサーバーを指定します。

16 エージェント再認定ジョブの終了後に、必要に応じて、サーバー上で通信テストを実行してエージェントを確認することができます。詳細については、サーバー通信テストの実行 (133 ページ) を参照してください。

第3章 マルチマスターメッシュの管理

この項では、マルチマスターメッシュの管理および保守を行う方法について説明します。SAでのマルチマスターメッシュの構成方法に関する説明は行いません。マルチマスターアーキテクチャーの詳細、およびマルチマスターメッシュの計画およびインストールについては、『SA 概要とアーキテクチャーガイド』と『SA Installation Guide』を参照してください。

マルチマスターメッシュの冗長性

SAコアはそれぞれ1つのデータセンターを管理します。各データセンターは、SA内で1つのファシリティとして表されます。マルチマスターメッシュは、同じ数のファシリティを管理する2つ以上のSAコアです。マルチマスターメッシュには、オプションで1つ以上のSAサテライトを含めることができます。SAサテライトは、完全なSAコアよりも少ない数のサーバーを管理する「ミニ」SAコアです。

SAのマルチマスターメッシュ構成は、冗長性、信頼性、高可用性を備えた設計になっています。マルチマスターメッシュは、同期された複数のコアで構成されます。各コアに関するすべてのデータが他のすべてのコアと同期されるため、1つのコアがダウンした場合でも、他のコアがすべての要求とジョブを処理します。

また、マルチマスターメッシュは、パフォーマンスを向上させるための負荷分散にもなります。

マルチマスターメッシュの競合とは

マルチマスターメッシュ (定義により、2つ以上のSAコアで構成される) では、SAユーザーが任意のコアでアクションを実行すると、すべてのコアの同期を維持するために、各コアはメッシュ内の他のすべてのコアにトランザクションの詳細を転送します。2人のユーザーが異なる2つのコアで重複または競合するアクションを実行した場合に、コアから別のコアへトランザクションが転送されると、競合が発生します。

SAには、このような競合を検出して競合が発生したことを通知し、競合の解決を支援する機能があります。

SAコア自体で競合を解決することはできません。競合が発生した場合、SA管理者はSAクライアントで**マルチマスターツール**を使用してターゲットデータベースにおける競合を解決して、トランザクションが失われないようにする必要があります。

- 競合の表示については、マルチマスターメッシュの状態の表示 - SA クライアント (113ページ) を参照してください。
- 競合の解決については、メッシュの競合の解決 - SAクライアント (118ページ) を参照してください。
- また、SAクライアントでシステム診断ツールを使用して、マルチマスターコンポーネントの正常性に関する情報を表示することもできます。詳細については、SAのトラブルシューティング - 診断テスト (205ページ) を参照してください。

SAでのメッシュの競合の処理方法

SAコアはそれぞれ1つのファシリティを管理します。SAコア(ソースコア)がトランザクションを別のコア(ターゲットコア)に送信して競合が発生した場合、SAによって競合が検出され、次の処理が行われます。

1 トランザクションがキャンセルされます。

2 トランザクションの影響を受けるSAのすべてのデータベース行をロックして、データベース行への影響が拡大するのを防ぎます。

3 ソースコアはメッシュ内の他のすべてのコアにトランザクションのロックを伝播して、すべてのコアのデータベース行をロックします。

4 競合に関する情報を含むアラートメッセージを、ユーザーが構成したメールリングリストに送信します。詳細については、マルチマスターの電子メールアラート (124ページ) を参照してください。

5 ソースコアとターゲットコアが次のトランザクションへ進みます。

ソースコアまたはターゲットコアのいずれかで例外が発生して、次のトランザクションへ進むことができなくなった場合は、その問題に関する説明を記述した電子メールをユーザーが構成したメールリングリストに送信して、そのコアをシャットダウンします。

競合を手動で解決し、データベース行のロックを解除する場合は、メッシュの競合の解決 - SAクライアント (118ページ) を参照してください。

メッシュの競合を防ぐためのベストプラクティス

この項では、マルチマスターメッシュの競合を最小限に抑える方法について説明します。

マルチマスターの競合が生じる可能性は、次の要因に左右されます。

- 管理対象サーバーの数 — サーバーの数が多いほど、競合が発生する可能性が高くなります。
- マルチマスターメッシュ内のコアの数。
- SAユーザーによって使用されているSAクライアントの数 — 更新を行うユーザーの数が多いほど、競合が発生する可能性が高くなります。
- 異なる複数のSAクライアントを使用して複数のファシリティで変更を行うユーザーの傾向。

ユーザー

ユーザーは、次の点に注意する必要があります。

- 複数のファシリティのユーザーが同じデータを同時に変更することができるため、可能な場合には、競合を避けるように更新を調整します。
- SAによって変更内容が自動的に伝播されるため、ユーザーは特定のファシリティでデータを変更してすぐに、別のファシリティで同じ変更を行わないようにする必要があります。複数のファシリティで同じ変更を行なうと、多くの場合、メッシュの競合の原因になります。
- ユーザーによる変更が他のSAファシリティに伝播されるまでに、わずかな遅延が発生します。遅延の大きさは、ネットワーク接続や帯域幅などの要素に左右されます。メッシュ内の他のすべてのモデルリポジトリに伝播されていない更新がある場合は、トランザクションのやり直しや、最近の他のトランザクションに依存する更新を追加で実行する前に、トランザクションが遅延しないように十分な時間を確保してください。

管理者

次のベストプラクティスを実施して、データの競合ができるだけ発生しないようにします。

- ネットワーク接続の信頼性が高く、メッシュ内のファシリティ間のネットワーク帯域幅が十分であることを確認します。帯域幅が小さくなるほど、競合のリスクが増します。

  詳細については、マルチマスターメッシュでのネットワーク管理 (123ページ) を参照してください。

  マルチマスターメッシュでSAを実行する場合のネットワーク接続については、『SA Installation Guide』を参照してください。

- 可能であれば、異なる複数のファシリティの同一オブジェクトを変更するユーザーが 1 人だけになるように、データ空間を分割します。

- 1人のユーザー (または連携して作業する少数のユーザー) が特定のサーバー群を管理するようにします。データ空間を分割することで、サーバーの所有に関するアカウンタビリティを明確にして、ユーザーが別のユーザーのデータを変更しないようにすることができます。

  このために、SAクライアントでは、カスタマー、ファシリティ、ユーザーグループのタイプごとにアクセス権を設定することができます。

  ユーザーグループおよびSAのアクセス権の詳細については、アクセス権のリファレンス (249ページ) を参照してください。

マルチマスターメッシュの状態の表示 - SAクライアント

マルチマスターツールでは、SAデプロイメント内のファシリティの各ペア間のトランザクションステータスが表示されます。また、発生した競合を解決することもできます。マルチマスターメッシュ内のファシリティ間のすべてのトランザクションに関する詳細を表示するには、次の手順を実行します。

1 SAクライアントで、[管理] タブを選択します。

2 [マルチマスターツール] ノードで、[**状態ビュー**] を選択します。テーブルにすべてのファシリティ (各ファシリティがSAコアに対応) と、ファシリティの各ペア間のすべてのトランザクションの状態が表示されます。表17に、状態ビューの色分けの意味を示します。

表17 マルチマスタートランザクションの状態の色分け

トランザクションの色	トランザクションの状態
青	送信 - 他のファシリティに正常に送信されたトランザクションの数を示します。
緑	受信 - ファシリティで正常に受信したトランザクションの数を示します。
紫	未送信 - ファシリティの1つ以上のトランザクションが、メッシュ内の他のファシリティに送信されていません。
黄	未受信 - 他のファシリティから送信された1つ以上のトランザクションが、ファシリティで受信されていません。
赤	競合 - 1つ以上の競合が発生しています。

3 競合しているすべてのトランザクションに関する詳細を表示するには、ナビゲーションバーで[**競合ビュー**]を選択します。次の内容を含む各トランザクションの詳細が表示されます。

   — トランザクション - トランザクション ID と、競合しているトランザクションに関する詳細を確認するためのリンクです。

- アクション - トランザクションの内容に関する説明です (データベースの更新、挿入、削除など)。
- テーブル - トランザクションの影響を受けるデータベーステーブルです。
- カウント - データベース要素に対して実行されたアクションの数です。
- ユーザー - 競合の原因になったアクションを実行したSAユーザーです。競合を正確に解決するため、このユーザーに問い合わせて、ユーザーが何をしようとしていたのかを確認します。
- 作成時刻 - トランザクションが実行された日付と時刻です。
- ソースファシリティ - トランザクションの送信元のコアです。
- 競合しているファシリティ - トランザクションを受信し、競合が検出されたコアです。

4 特定のトランザクションの競合に関する詳細を表示するには、[トランザクション] リンクを選択します。選択したトランザクションに関する詳細が表示されます。

- テーブル - 競合が発生したSAデータベーステーブルが表示されます。
- DBフィールド - 競合が発生したデータベーステーブル内のすべてのSAデータベースフィールド名が表示されます。
- ファシリティ列 - 残りの列はSAデプロイメント内の各ファシリティ用です。各列には、対応するファシリティの値が示されます。競合が発生した場所に関係なく、値は赤いテキストで表示されます。

5 競合の解決については、メッシュの競合の解決 - SAクライアント (118ページ) を参照してください。

図 24 は、競合のないマルチマスターメッシュの状態ビューです。マルチマスターメッシュ内の 3 つコア (London、Paris、Vienna) がすべて最新の状態になっています。すべてのコアのすべての変更が、他のすべてのコアに正常に送信されています。

図24　　マルチマスターメッシュの競合 (状態ビュー - 競合なし)

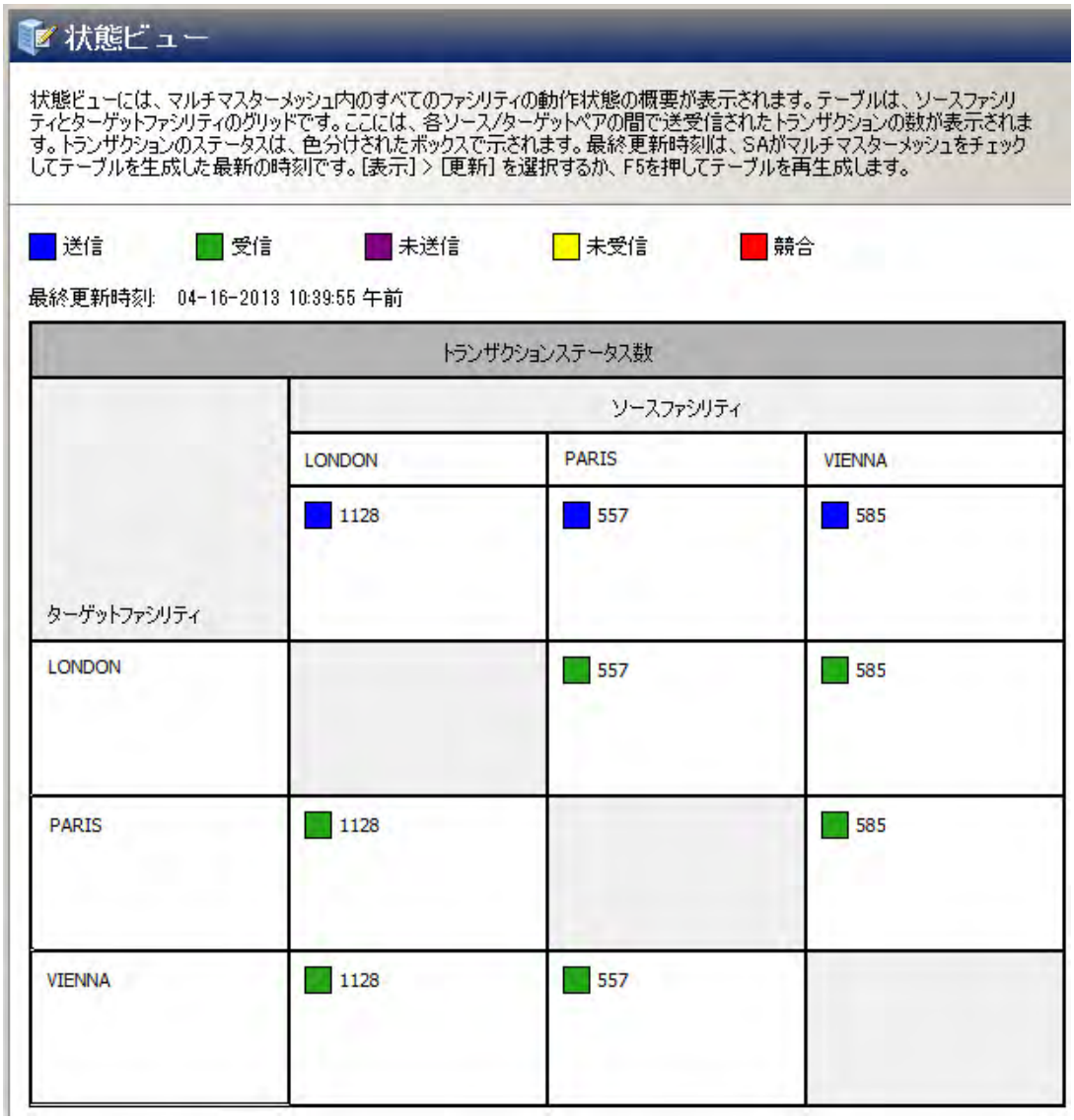


図25のメッシュの状態ビューには、競合はありませんが、2つのコアで2つの変更が行れていて、これから他のコアへ変更が伝播されるところです。Londonコアに2つの変更が加えられ、Viennaコアに2つの変更が加えられています。

図25　　マルチマスターメッシュの競合（状態ビュー - 変更の送信待ち）

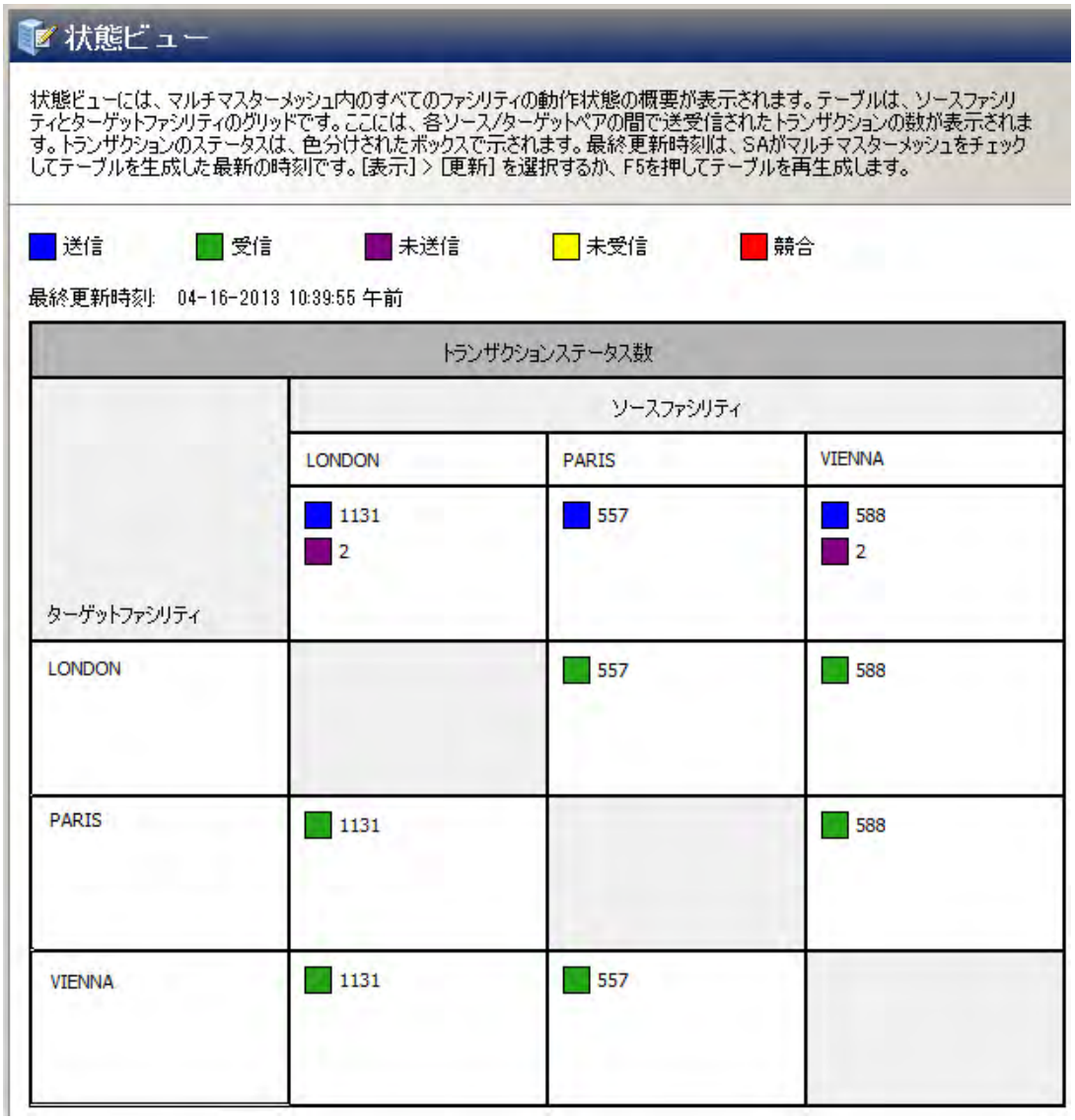
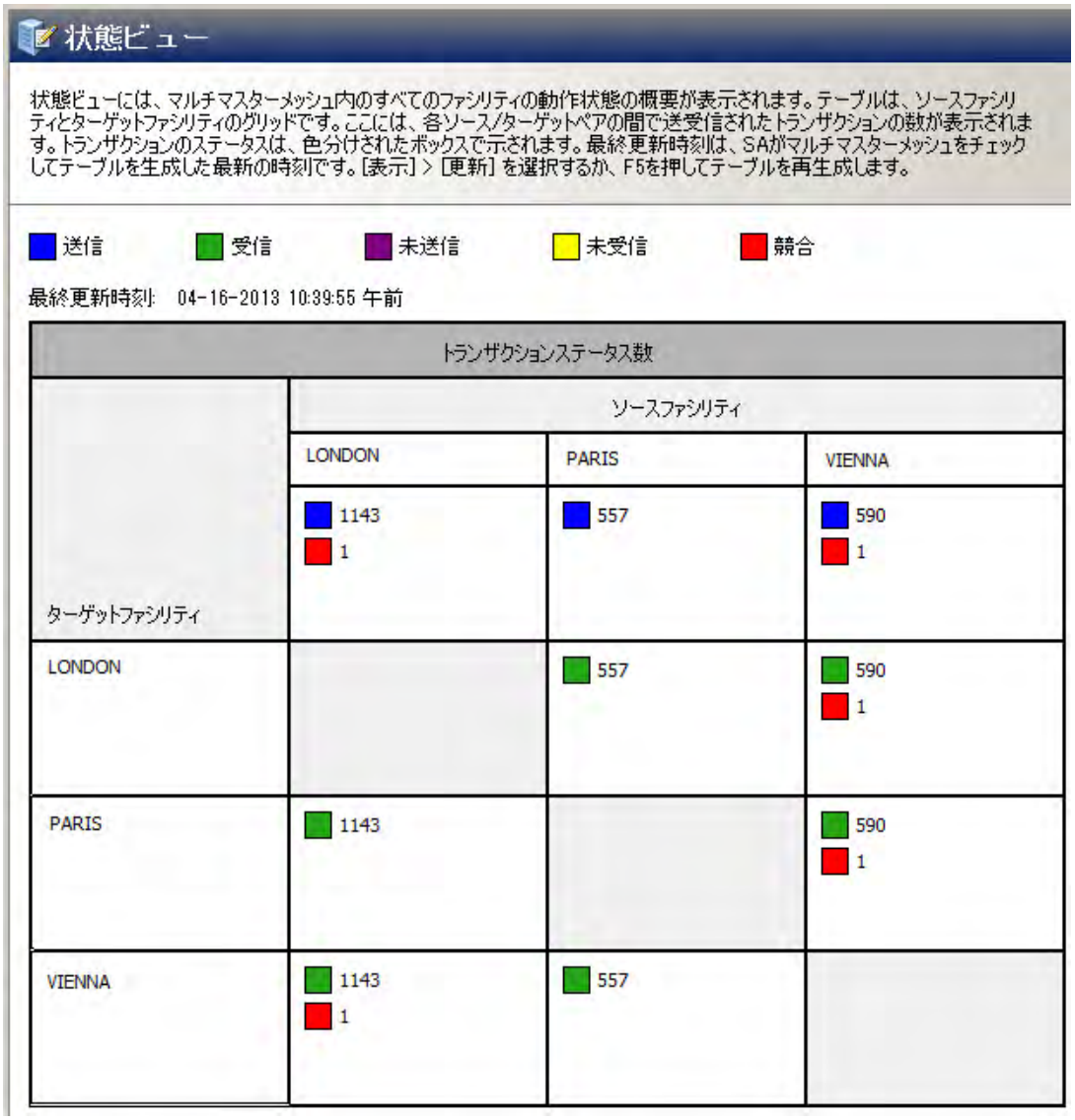


図26のメッシュの状態ビューには、LondonコアとViennaコアとの間に2つの競合があります。Londonコアにはviennaコアとの競合が1つあります。ViennaコアにはLondonとParisの両方のコアとの競合が1つあります。競合の解決については、メッシュの競合の解決 - SAクライアント (118ページ) を参照してください。

図26　　マルチマスターメッシュの競合 (状態ビュー - 2つの競合あり)



メッシュの競合の解決 - SAクライアント

SAクライアントでマルチマスターメッシュの競合を解決するには、次の手順を実行します。

競合を解決する際には、事前に電子メールアラートエイリアスのユーザーに通知してください。これらのユーザーに通知しておくことで、複数のSA管理者が個別に競合を解決しようとして、それぞれの操作が有効に機能しなくなるのを避けることができます。競合を解決する際には、1つのファシリティのSAクライアントから競合を解決するようにしてください。異なる複数のファシリティのSAクライアントから、1つの競合を重複して解決しないようにしてください。

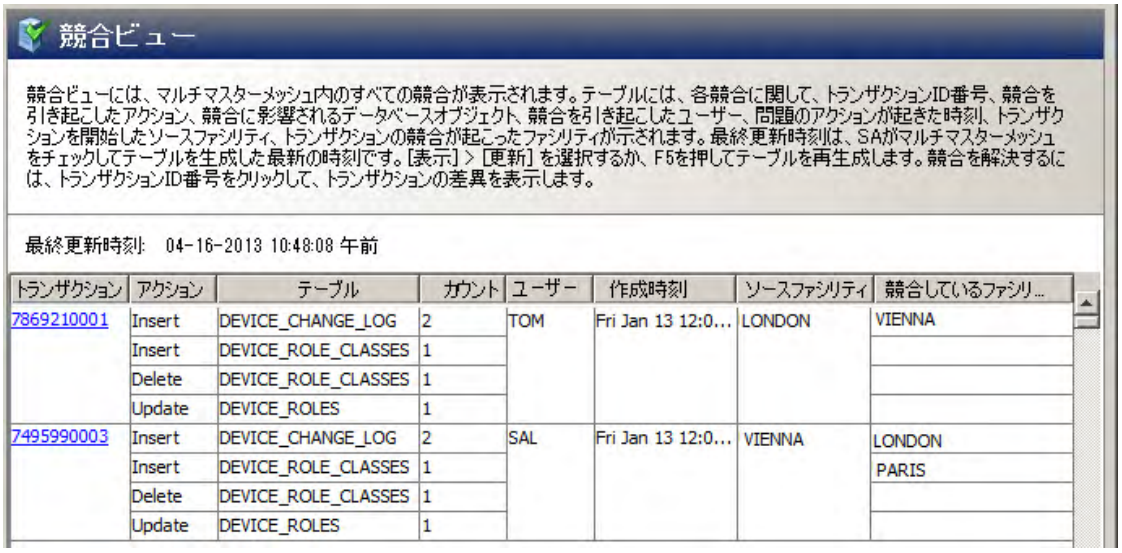
マルチマスターツールを使用して解決することができない大量の競合が発生し、データベースの同期に関する支援が必要な場合は、HP Server Automationのサポート担当までご連絡ください。

競合の表示および解決に必要なSAのアクセス権を持っていることを確認してください。アクセス権の詳細については、アクセス権のリファレンス (249ページ) を参照してください。

1 SAクライアントで、[管理] タブを選択します。

2 [マルチマスターツール] ノードで、[**競合ビュー**] を選択します。メッシュ内のすべての競合に関する詳細が表示されます。図27の競合ビューには、2つの競合が表示されています。それぞれのソースファシリティはLondonとViennaです。競合の概要については、[**状態ビュー**] を選択します。

図27　　マルチマスターメッシュの競合 — 競合ビュー



トランザクション	アクション	テーブル	カウント	ユーザー	作成時刻	ソースファシリティ	競合しているファシリ...
7869210001	Insert	DEVICE_CHANGE_LOG	2	TOM	Fri Jan 13 12:0...	LONDON	VIENNA
	Insert	DEVICE_ROLE_CLASSES	1				
	Delete	DEVICE_ROLE_CLASSES	1				
	Update	DEVICE_ROLES	1				
7495990003	Insert	DEVICE_CHANGE_LOG	2	SAL	Fri Jan 13 12:0...	VIENNA	LONDON
	Insert	DEVICE_ROLE_CLASSES	1				PARIS
	Delete	DEVICE_ROLE_CLASSES	1				
	Update	DEVICE_ROLES	1				

3 必要に応じて、キーボードで [Ctrl] + [F] キーを押します。検索ツールを使用して、特定の競合を検索することができます。[Esc] キーを押すと、検索ツールは終了します。

4 それぞれの競合を詳細に確認します。アクションを実行したユーザー、ソースファシリティ、競合しているファシリティに注意します。

5 [トランザクション] 欄のトランザクションIDのリンクを選択します。選択したトランザクションに関する詳細が表示されます。

6 必要に応じて、キーボードで [Ctrl] + [F] キーを押します。検索ツールを使用して、特定の競合の詳細を検索することができます。[Esc] キーを押すと、検索ツールは終了します。

7 それぞれの競合の詳細を確認します。それぞれの競合の詳細を確認すると、競合の内容、競合の原因となったユーザーアクション、アクションを実行したユーザー、各ユーザーの意図を特定することができます。

8 可能であれば、正しいデータが存在するファシリティを特定して、そのファシリティのデータを同期します。ファシリティからの同期を行うと、そのファシリティのデータが他のすべてのファシリティにコピーされて、競合が解決されます。

正しいデータが存在するファシリティがない場合は、特定のファシリティから同期した後に、競合の原因となった状況を回避しながら、アクションをやり直すことができます。

必要に応じて個別のデータベーステーブルを同期することもできますが、SAデータベースに関する知識がない場合、この方法は推奨できません。個別のテーブルを同期する場合は、各列の下部にある該当する [このファシリティから同期] ボタンを選択して、手順13 (119ページ) に進みます。

9 正しいデータが存在するファシリティを特定できたら、ウィンドウ上部の [すべてのオブジェクトの同期元] ドロップダウンリストからそのファシリティを選択します。

10 [同期] ボタンを選択します。これにより、選択したファシリティのデータが他のすべてのファシリティにコピーされて競合が解決され、[トランザクション同期結果:] ウィンドウが表示されます。

11 [トランザクション同期結果:] ウィンドウで [OK] を選択します。

12 [解決済みとマーク] ボタンを選択します。[競合を解決済みとマーク:] ウィンドウに、解決したメッシュの競合のステータスが表示されます。

13 [競合を解決済みとマーク:] ウィンドウで [OK] をクリックします。これにより、競合は削除されます。

14 競合ビューを開き、解決済みの競合が削除されていることを確認します。

メッシュの競合の詳細なタイプと原因

この項では、マルチマスターメッシュの競合の原因とタイプについて説明します。

ユーザーの重複による競合

ユーザーがあるファシリティでSAクライアントを使用して変更を行い、同時に別のユーザーが別のファシリティで同じオブジェクトに対して変更を行なった場合、競合が発生します。

例:

1 AliceがAtlantaファシリティ内のサーバーからノードAを削除します。

2 BobがBostonファシリティ内のサーバーからノードAを削除します。

3 SAによってAtlantaファシリティからBostonファシリティへ変更が伝播されますが、Bobがすでに Bostonファシリティ内のサーバーからノード A を削除しています。SA でモデルリポジトリマルチマスターコンポーネントの競合アラートが生成されます。これは、Aliceが存在しないノードの削除を要求しているように見えるためです。

4 SAで手順2のBobによる更新内容がBostonファシリティからAtlantaファシリティへ伝播されますが、Aliceがすでに Atlanta ファシリティ内のサーバーからノード A を削除しています。SA で別のモデルリポジトリマルチマスターコンポーネントの競合アラートが生成されます。

ユーザーの重複アクションによる競合

ユーザーが何らかの理由でモデルリポジトリに更新を加えようとして、メッシュ内の他のモデルリポジトリへ更新が伝播されるまで待たずに更新が失敗したと考えて、再度更新を実行して更新の重複が発生した場合にも競合が発生します。

たとえば、次のようなケースが考えられます。

1. Seattleファシリティ内のサーバーから、CarolがSAコマンドラインインタフェース (CLI) を使用して、パッケージ`carol.conf`をアップロードします。
2. すぐに Carol は Phoenix ファシリティで SA クライアントにログインして、このパッケージを検索します。データがSeattleからPhoenixにまだ伝播されていないため、Carolはこのパッケージを見つけることができません。Carolはファシリティ間でのデータの伝播に十分な時間を見込みました。
3. CarolはPhoenixでSAクライアントを使用してパッケージ`carol.conf`をアップロードします。
4. その後Seattleからデータが伝播されると、Phoenixにすでにデータが存在しているため、SAで競合が生成されます。

トランザクション順序の不整合による競合

2つのファシリティ間のトランザクションは、通常、送信された順序で到着します。ただし、第3のファシリティがトランザクションに関与している場合、正しい順序での到着は保証されません。次に例を示します。

1. ユーザーがファシリティ A (モデルリポジトリA) で、データを変更または追加します。
2. この変更のトランザクションは、ファシリティ B (モデルリポジトリB) およびファシリティ C (モデルリポジトリC) に伝播されます。
3. しかし、このデータはファシリティ B (モデルリポジトリB) で再度変更または参照され、その後ファシリティ AおよびCに伝播されます。
4. ファシリティ B (手順3) からのトランザクションが、ファシリティ A (手順1) からのトランザクションよりも前にファシリティ C (モデルリポジトリC) に到着した場合、競合が発生します。

この競合は、通常、ユーザーがあるファシリティでSA CLIを使用してパッケージをアップロードしてすぐに、SA クライアントを使用して別のファシリティでソフトウェアポリシーにパッケージを追加した場合に発生します。

トランザクション順序の不整合は、異なるファシリティで同時に更新を行なったり、ファシリティ間のネットワーク接続に問題がある場合に発生する可能性があります。

例:

1. HenryがDenverファシリティ内のサーバーでSA CLIを使用して、パッケージ`henry.conf`をアップロードします。
2. SAによってメッシュ内のすべてのファシリティにパッケージに関するデータが伝播されますが、ネットワーク接続がダウンしているため、Parisファシリティにはデータを伝播することができません。
3. HenryはMiamiファシリティのサーバーにログオンし、SAクライアントを使用してパッケージ`henry.conf`の説明を更新します。
4. SA によってメッシュ内のすべてのファシリティに更新されたパッケージに関するデータが伝播されますが、ネットワーク接続がまだダウンしているため、Parisファシリティにはデータを伝播することができません。
5. Parisファシリティとのネットワーク接続が回復し、手順2および4のトランザクションが遅れてParisファシリティに伝播されます。
6. 更新したパッケージの説明のトランザクションが、`henry.conf` をアップロードするトランザクションよりも前に、Parisファシリティに到着します。Parisファシリティのモデルリポジトリに`henry.conf`に関するデータが含まれないため、SAによって競合アラートが生成されます。

7 henry.confをアップロードするトランザクションがParisファシリティに到着し、問題なく処理されます。パッケージデータはParisのモデルリポジトリ内に存在しますが、パッケージの説明はメッシュ内の他のファシリティと異なっています。

データベースの競合

この項では、競合の種類に関する概要と競合を解決するための手順について説明します。データおよびトランザクションの競合の識別および解決の詳細については、Oracle データベースの管理ドキュメントを参照してください。

表18に、競合のタイプの例をいくつか示します。

表18 競合のタイプ

競合	説明
同一データの競合	マルチマスターツールにトランザクションの競合が表示されますが、各ファシリティのデータは同じです。データが同じになるのは、ユーザーが異なる複数のファシリティで同じ変更を行なったためです。
単純なトランザクションの競合	行がすべてのファシリティに存在するが、一部の列の値が異なります。または、一部のファシリティに行が存在しません (オブジェクトの欠落)。
一意キーの制約による競合	オブジェクトがファシリティ内に存在せず、オブジェクトを追加すると一意キーの制約に違反するため、オブジェクトを追加できません。
外部キーの制約による競合	行が一部のファシリティ内に存在せず、データにそのファシリティ内に存在しない別のオブジェクトへの外部キーが含まれるため、行を追加できません。
リンクされたオブジェクトの競合	まれに発生するタイプの競合です。SA には、カスタム属性の名前と値や、SA クライアントで作成されたカスタマー (リストに表示) とノード階層構造でカスタマーに関連付けられたノードなど、SA 内の関連するオブジェクトをリンクするビジネスロジックが含まれます。SA では、関連するオブジェクト間のリンクが維持されます。リンクされたオブジェクトの競合では、競合の原因となったトランザクションの意図を損なわないようにする必要があるため、競合の解決が複雑になる場合があります。リンクされたオブジェクトの競合の解決に関する支援が必要な場合は、HP Server Automation のサポート担当までご連絡ください。

それぞれの競合のタイプを解決するためのガイドライン

一般に、競合を解決する際には、元になる変更のタイムスタンプに基づいてターゲットに最新のデータが反映されるように更新を適用します。

後述のガイドラインのいずれかに従うことができない場合は、トランザクションの意図を損なわないようにします。トランザクションの生成元のユーザーに連絡して、管理対象の環境でどのような変更を実行しようとしたのかを確認します。

同一データの競合

すべてのファシリティでトランザクション内のすべてのオブジェクトに同じデータが含まれます。このタイプの競合には、すべてのファシリティにオブジェクトが存在しないケースも含まれます。

同一データの競合を解決するには、競合を解決済みとマークします。

同一データの競合 (ロック)

すべてのファシリティでトランザクションのすべてのオブジェクトに同じデータが含まれますが、トランザクションのオブジェクトがロック (競合とマーク) されたままです。

このタイプの競合を解決するには、任意のファシリティを選んで、そのファシリティを元にすべてのオブジェクトを同期します。このアクションを実行すると、オブジェクトのロックが解除されます。データを同期した後に、競合を解決済みとマークします。

単純なトランザクションの競合

データがファシリティ間で異なるか、または一部のファシリティに欠落するオブジェクトがあります。他の競合するトランザクションのアクションに依存するオブジェクトはありません。オブジェクトを同期することで、データベースの外部キーまたは一意キーの制約に違反することはありません。

単純なトランザクションの競合を解決するには、正しいデータを含むファシリティを選択して、そのファシリティを元に同期します。正しいデータを含むファシリティを特定する方法は、次のようにトランザクションのタイプによって異なります。

- 2人のユーザーがお互いの作業をオーバーライドする操作を行うことで競合が発生している場合は、2人のユーザーに確認して、いずれかのユーザーの変更を正しいものとするかを判断します。
- お互いのデータをオーバーライドする自動化されたプロセスによって競合が発生している場合は、通常、最新の変更が正しい内容です。
- トランザクション順序の不整合によって競合が発生している場合は、通常、最新の変更が正しい内容です。

データを同期した後に、競合を解決済みとマークします。

一意キーの制約による競合

これらの競合を解決すると、一意キーの制約違反が発生します。

たとえば、次のようなケースが考えられます。

1. Londonファシリティ内のSAクライアントから、JohnがノードAの下位ノードとしてノードA1を作成します。
2. San Franciscoファシリティ内のSAクライアントから、Annが同じアクションを実行します。AnnはノードAの下位ノードとしてノードA1を作成します。
3. ノード名はノード階層構造の各階層で一意である必要があります。
4. SAによって、LondonおよびSan Franciscoのファシリティから他のファシリティにノードの変更が伝播されます。他のファシリティでモデルリポジトリのデータベースに行を追加すると、一意キーの制約違反が発生して、競合が生じます。

この競合を解決するために、すべてのファシリティでLondonファシリティからの更新を追加しても、同様に一意キーの制約違反が発生します。

一意キーの制約の競合を解決するには、次の手順を実行します。

1. 関連するすべてのトランザクションを特定し、該当するオブジェクトが存在しないファシリティを元に一方のトランザクションを同期することにより、すべてのファシリティの該当するオブジェクトを削除します。
2. 該当するオブジェクトが存在するファシリティを元にもう一方のトランザクションを同期することにより、すべてのファシリティで該当するオブジェクトを追加します。競合する2つのオブジェクトが、いずれか1つに置き換えられます。

外部キーの制約による競合

これらの競合を解決すると、外部キーの制約違反が発生します。

たとえば、次のようなケースが考えられます。

1. Jerryがファシリティ 1内にノードBを作成します。

2 トランザクションが他のファシリティに伝播される前に、JerryはノードCをノードBの下位ノードとして作成します。

3 最初のトランザクションがファシリティ 2に到着したときに、関係のない理由で競合が発生します。

4 2番目のトランザクションがファシリティ 2に到着したときに、ノードCで行を追加すると、親ノード (ノードB) が存在しないため、外部キーの制約の競合が発生します。

2 番目の競合を最初に解決するために、すべてのファシリティにノード C の更新を追加しても、同様に外部キーの制約違反が発生します。

外部キーの制約の競合を解決するには、次の手順を実行します。

1 ノード B (親ノード) のトランザクションの競合を解決するには、該当するオブジェクトが存在するファシリティを元に最初のトランザクションを同期します。

2 該当するオブジェクトが存在するファシリティを元に2番目のトランザクション (ノードCの更新) を同期します。

一般には、発生した順番に競合を解決することで、外部キーの制約の競合が発生するのを避けることができます。

マルチマスターメッシュでのネットワーク管理

SAでは、マルチマスターメッシュの構成がネットワーク稼働時間に関するガイドラインに適合している必要はありません。マルチマスターメッシュの構成は、ファシリティ間ネットワークが一時的に停止する運用環境でも十分に機能します。

ただし、ネットワーク停止の時間が長くなると、競合が発生する可能性が高くなります。ファシリティ間のネットワーク停止が長くなると、次の問題が発生する可能性があります。

- マルチマスターメッセージをファシリティ間で伝播できない
- マルチマスターツールが正常に機能しなくなる
- SA Webクライアントからマルチマスターのデータアクセスエンジンにアクセスできない

マルチマスター構成の運用環境は、表19に示すパフォーマンスデータに対応しています。

表19　　マルチマスター構成のパフォーマンスデータ

ファシリティの数	ネットワーク停止の時間	マルチマスターの競合の数 *
8 (SA コアが各ファシリティにインストール済み)	12時間 (1 つのファシリティが他のファシリティとのネットワーク接続を失う)	12～24 (発生する平均値)
* 他のファシリティで SA Web クライアントを使用して接続されていないファシリティ内のサーバーを管理するユーザーの傾向によっては、競合の数が増加します。		

ネットワーク接続の問題には、SA Busの問題またはマルチキャストルーティングの問題が含まれます。

マルチマスターの電子メールアラート

マルチマスターの競合が発生するか、マルチマスターコンポーネントで問題が発生すると、SAはユーザーが構成したマルチマスター電子メールエイリアスに電子メールを送信します。この電子メールアドレスは、SAのインストール時に構成します。この電子メールアドレスを変更する必要がある場合は、HP Server Automationのサポート担当に連絡するか、詳細についてSAの通知の構成 (239ページ) を参照してください。

アラート電子メールの件名では、次の内容が特定されます。

- モデルリポジトリデータベースへのトランザクションの適用中に発生したエラーのタイプ
- マルチマスターで問題が発生する原因となったエラーのタイプ

マルチマスターに影響するSAの問題の解決について支援が必要な場合は、HP Server Automationのサポート担当にご連絡ください。

表20に、エラーメッセージを示します。

表20　　マルチマスターのエラーメッセージ

件名	エラーのタイプ	詳細
vault.ApplyTransactionError	マルチマスタートランザクションの競合	ローカルのデータベースが、その他のデータベースからの変更で正常に更新されませんでした。各更新は1つの行にのみ影響を及ぼすため、データベースエラーにはなりません。
vault.configValueMissing	SAの問題	特定の構成パラメーターで値が指定されていません。 SA Web クライアントにログインして、この構成パラメーターの値を指定します。SAの構成設定について支援が必要な場合は、HP Server Automationのサポート担当までお問い合わせください。
vault.DatabaseError	マルチマスタートランザクションの競合	他のデータベースに送信する更新についてクエリ中、またはその他のデータベースからの更新を適用中にエラーが発生しました。モデルリポジトリマルチマスターコンポーネントを再開します。
vault.InitializationError	SAの問題	モデルリポジトリマルチマスターコンポーネントのプロセスが開始されたときにエラーが発生しました。アプリケーションは指定されたメッセージを返しました。エラーが発生したスレッドは実行を停止しました。このエラーは、マルチマスターモードでSAを実行したときに発生します。 エラー状態を解決します。モデルリポジトリマルチマスターコンポーネントを再開します。

表20　マルチマスターのエラーメッセージ（続き）

件名	エラーのタイプ	詳細
vault.ParserError	マルチマスタートランザクションの競合	トランザクションのXML表現の解析時にエラーが発生しました。アプリケーションは指定されたメッセージを返しました。このエラーは、マルチマスターモードでSAを実行したときに発生します。 SA管理のマルチマスターツールを実行して、トランザクションデータにXMLパーサーが解釈できない特殊文字が含まれていないことを確認します。
vault.SOAPError	マルチマスタートランザクションの競合	SOAPライブラリを使用して、トランザクションをXML形式にマーシャル/アンマーシャルするときにエラーが発生しました。アプリケーションは指定されたメッセージを返しました。このエラーは、マルチマスターモードでSAを実行したときに発生します。 SA管理のマルチマスターツールを実行して、トランザクションデータにSOAPが解釈できない特殊文字が含まれていないことを確認します。
vault.UnknownError	SAの問題	モデルリポジトリマルチマスターコンポーネントのプロセスで、不明なエラーが発生しました。テクニカルサポートに連絡して、データベース名とSAコンポーネントのログファイルを提示してください。

ファシリティの管理

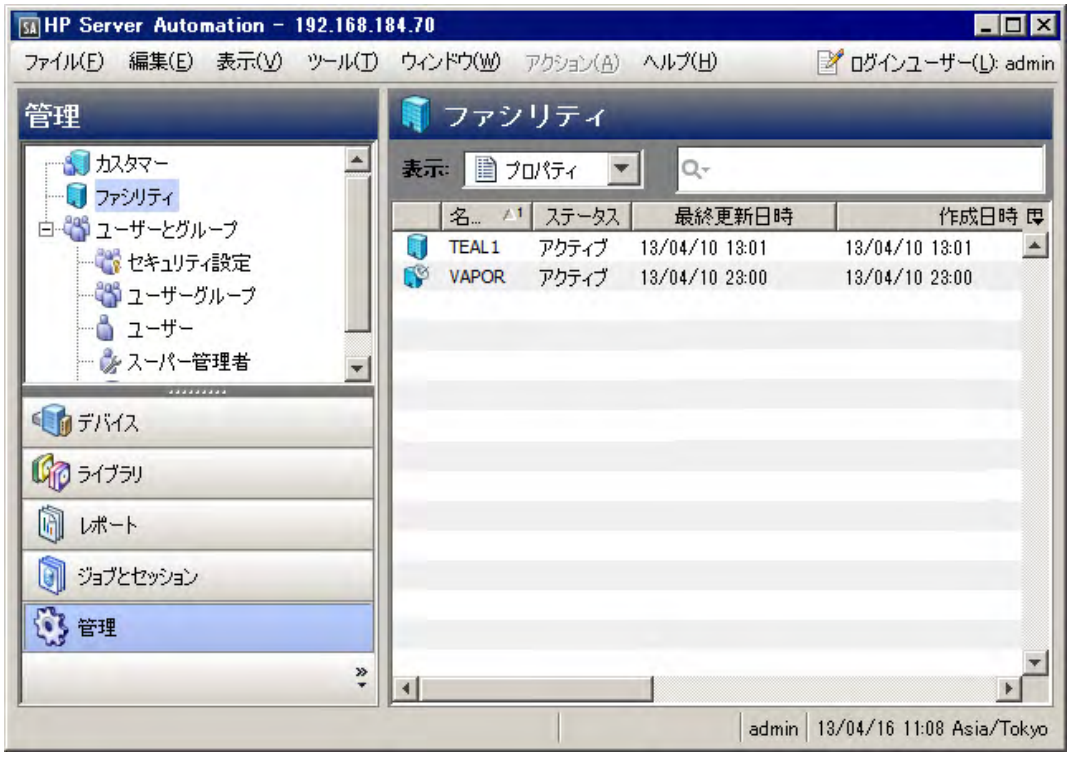
ファシリティは、単一のSAコアまたはサテライトで管理される一連のサーバーを指します。SAコアまたはSAサテライトをインストールする際には、必ず新しいファシリティを作成します。マルチマスターメッシュは、プライマリSAコアと1つ以上のセカンダリSAコアで構成されます。マルチマスターメッシュにはサテライトが含まれる場合もあります。SAコアまたはSAサテライトを追加でインストールする際には、必ず新しいファシリティが作成されます。

ファシリティ、コア、サテライトの詳細、およびマルチマスターメッシュアーキテクチャーでの構成方法については、『SA概要とアーキテクチャーガイド』および『SA Installation Guide』を参照してください。

ファシリティ情報の表示

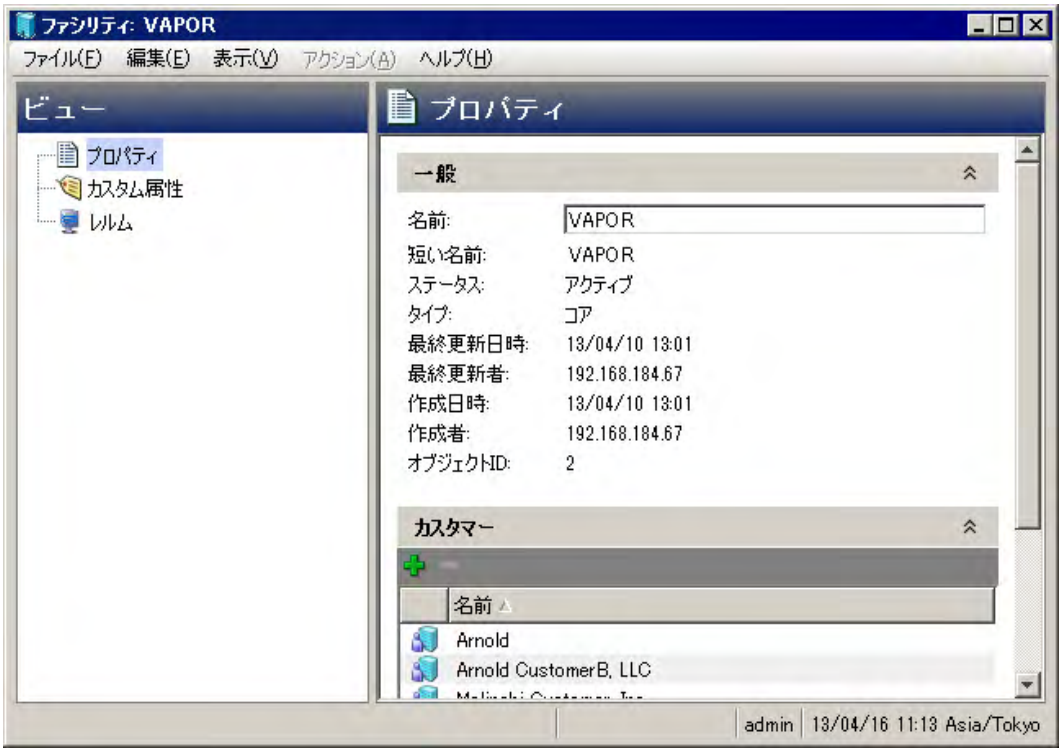
ファシリティに関する情報を表示するには、SAクライアントで[管理] タブを選択してから、[ファシリティ]を選択します。下の図28は、SAクライアントでTEAL1とVAPORという2つのファシリティを表示したところです。

図28　　SAクライアントに表示された2つのファシリティ



ファシリティに関する詳細を表示するには、ファシリティを開きます。図29は、ファシリティのプロパティ、カスタム属性、レルムなどの、VAPORファシリティの詳細を表示したところです。

図29　　ファシリティの詳細



ファシリティに関連付けられたカスタマーの変更

カスタマーを使用すると、サーバーのユーザーに基づいてサーバーを整理することができます。カスタマーはアクセス制御境界を明確にするための管理対象サーバーのグループです。カスタマーは必要な数だけ定義できます。各カスタマーグループには、任意のサーバーを割り当てることができます。ただし、最初にカスタマーを1つ以上のファシリティに割り当ててから、そのファシリティのサーバーをカスタマーグループに配置する必要があります。各サーバーはいずれか1つのファシリティに属します。また各サーバーはいずれか1つのカスタマーに属します(「未割り当て」カスタマーグループに属する場合もあります)。

カスタマーの詳細については、『SAユーザーガイド: Server Automation』を参照してください。

ファシリティに関連付けられたカスタマーを変更するには、次の手順を実行します。

1. SAクライアントで、[管理] タブを選択します。
2. ナビゲーションペインで[ファシリティ]を選択します。これにより、すべてのファシリティが表示されます。
3. 変更するファシリティを選択します。
4. [**アクション**] メニューを選択するか右クリックをして、[**開く**] メニューを選択します。別ウィンドウにファシリティが表示されます。
5. ファシリティウィンドウのナビゲーションペインで、プロパティビューを選択します。ファシリティに関連付けられたカスタマーを含むファシリティに関する情報が表示されます。
6. カスタマーを新規に追加するには、[+] アイコンを選択します。既存のカスタマーのリストが表示されます。
7. カスタマーを1つまたは複数選択します。
8. [選択] ボタンをクリックします。これにより、選択したカスタマーがファシリティに関連付けられます。

9 カスタマーを削除するには、カスタマーを選択して [-] アイコンを選択します。これにより、選択したカスタマーがファシリティから削除されます。

10 変更内容を破棄する場合は、[**ファイル**] > [**元に戻す**] を選択します。

11 変更内容を保存する場合は、[**ファイル**] > [**保存**] を選択します。

12 ファシリティウィンドウを閉じる場合は、[**ファイル**] > [**閉じる**] を選択します。

ファシリティのカスタム属性の追加または変更 - SAクライアント

ファシリティのカスタム属性の作成または変更を行うことができます。カスタム属性を使用することにより、サーバーの情報を迅速かつ簡単に保存することができます。カスタム属性は、SAのファシリティ、サーバー、およびその他のオブジェクトに対して作成できるデータ要素です。カスタム属性の詳細については、『SAユーザーガイド: Server Automation』を参照してください。

既存のカスタム属性を更新または削除する際には、十分注意してください。そのカスタム属性に依存する操作に影響が生じる可能性があります。

ファシリティのカスタム属性を追加、変更、または削除するには、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 [管理] タブを選択します。

3 ナビゲーションペインで [ファシリティ] を選択します。これにより、すべてのファシリティが表示されます。

4 変更するファシリティを選択します。

5 [**アクション**] メニューを選択するか右クリックをして、[**開く**] メニューを選択します。別ウィンドウにファシリティが表示されます。

6 ファシリティウィンドウのナビゲーションペインで、カスタム属性ビューを選択します。ファシリティで定義されているすべてのカスタム属性が表示されます。

7 カスタム属性を新規に追加するには、[+] アイコンを選択するか、[**アクション**] > [**追加**] メニューを選択します。新しいカスタム属性の名前と値を入力します。

8 カスタム属性を変更するには、値のフィールドを選択して新しい値を入力します。

9 カスタム属性を削除するには、カスタム属性を選択して、[-] アイコンを選択するか、[**アクション**] > [**削除**] メニューを選択します。

10 変更内容を破棄する場合は、[**ファイル**] > [**元に戻す**] を選択します。

11 変更内容を保存する場合は、[**ファイル**] > [**保存**] を選択します。

12 ファシリティウィンドウを閉じる場合は、[**ファイル**] > [**閉じる**] を選択します。

ファシリティ名の変更 - SAクライアント

ファシリティ名を変更するには、ファシリティの管理のアクセス権を使用してSAクライアントにログインする必要があります。ファシリティの短い名前は内部名で、変更できません。表示名は変更できます。

ファシリティの表示名を変更するには、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 [管理] タブを選択します。

3 ナビゲーションペインで [ファシリティ] を選択します。これにより、すべてのファシリティが表示されます。

4 変更するファシリティを選択します。

5 [**アクション**] メニューを選択するか右クリックをして、[**開く**] メニューを選択します。別ウィンドウにファシリティが表示されます。

6 ファシリティウィンドウのナビゲーションペインで、プロパティビューを選択します。

7 [名前] フィールドに新しいファシリティ名を入力します。

8 変更内容を破棄する場合は、[**ファイル**] > [**元に戻す**] を選択します。

9 変更内容を保存する場合は、[**ファイル**] > [**保存**] を選択します。

第4章 サテライトの管理

この項では、SAサテライトの基本的なトポロジと概念、および次の管理タスクについて説明します。

- サテライトの開始/再開
- サテライトの停止
- プライマリコアとサテライトとの通信を確認
- サテライトの管理に必要なアクセス権
- サテライト情報の表示
- サテライトの監視
- リモート接続の帯域幅管理
- サテライトのソフトウェアリポジトリキャッシュの管理
- サテライトのソフトウェアリポジトリキャッシュ内のソフトウェアの更新
- サテライトのソフトウェアリポジトリキャッシュの管理
- SAサテライトのインストールとトポロジ

サテライトの開始/再開

サテライトを開始するには、次のコマンドを実行します。

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

サテライトを再開するには、次のコマンドを実行します。

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

サテライトエージェントが再開しない場合は(通常はNFSエラーによってサテライトエージェントの通信に必要なポート1002がブロックされていることが原因)、サテライトホストを再開するか、ポート1002をブロックしているサービスを一時的に無効にして、エージェントを再開してから、ブロックしているサービスを再開してください。

サテライトの停止

サテライトを停止するには、次のコマンドを実行します。

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

プライマリコアとサテライトとの通信を確認

コア管理ゲートウェイとサテライトとの通信を確認するには、次の手順を実行します。

1. ゲートウェイの管理のアクセス権を持つユーザーグループに属するユーザーとして SA クライアントにログインします。
2. ナビゲーションパネルから、**[管理]** > **[ゲートウェイ]** をクリックします。
3. [ゲートウェイの管理] ページの左上に、新しいサテライトのリンクが表示されることを確認します。

   [ゲートウェイの管理] ページにサテライトのリンクが表示されない場合は、サテライトのプロパティの編集が必要になる可能性があります。プロパティファイルのフルパス名は次のとおりです。

   ```
   /etc/opt/opsware/opswgw/opswgw.properties
   ```

   プロパティファイルの変更が済んだら、次のコマンドでサテライトを再開する必要があります。

   ```
   /etc/init.d/opsware-sas restart opswgw
   ```
4. サテライトのファシリティに対する読み取り (または読み取り / 書き込み) のアクセス権を持つユーザーグループのユーザーとしてSA Webクライアントにログインします。
5. ナビゲーションパネルで、**[Servers]** > **[Manage Servers]** をクリックします。
6. [サーバーの管理] ページに、サテライトサーバーのホスト名が表示されるのを確認します。

『SAユーザーガイド: Server Automation』の「サーバー通信テストのトラブルシューティング」も併せて参照してください。

サテライトの管理に必要なアクセス権

SAのゲートウェイを管理するには、ゲートウェイの管理のアクセス権が必要です。デフォルトで、このアクセス権はSAのSystem Administratorsグループに含まれています。ファシリティの情報を表示するには、該当するファシリティに対する読み取り (または読み取り/書き込み) のアクセス権が必要です。ユーザーグループおよびSAのアクセス権の詳細については、アクセス権のリファレンス (249ページ) を参照してください。

サテライト情報の表示

ここでは、次の内容について説明します。

- サテライトのファシリティとレルムの表示
- サテライトの管理対象サーバーのレルムの表示
- サテライトのゲートウェイ情報の表示と管理

サテライトのファシリティとレルムの表示

コアおよびサテライトのファシリティを表示するには、SAクライアントで **[管理]** タブを選択してから、[ファシリティ] を選択します。特定のファシリティを選択した後に、レルムビューを選択すると、ファシリティに関連するレルムを参照できます。これには、ファシリティ内のレルム間の帯域幅も含まれます。ファシリティの詳細については、ファシリティの管理 (125ページ) を参照してください。

サテライトの管理対象サーバーのレルムの表示

サテライト構成でインストールしたSAでは、重複するIPアドレスを使用してサーバーを管理できます。サーバーがNATデバイスまたはファイアウォール越しに存在する場合に、このような管理を行うことができます。重複するIPアドレスを持つサーバーは、異なるレルムに存在している必要があります。

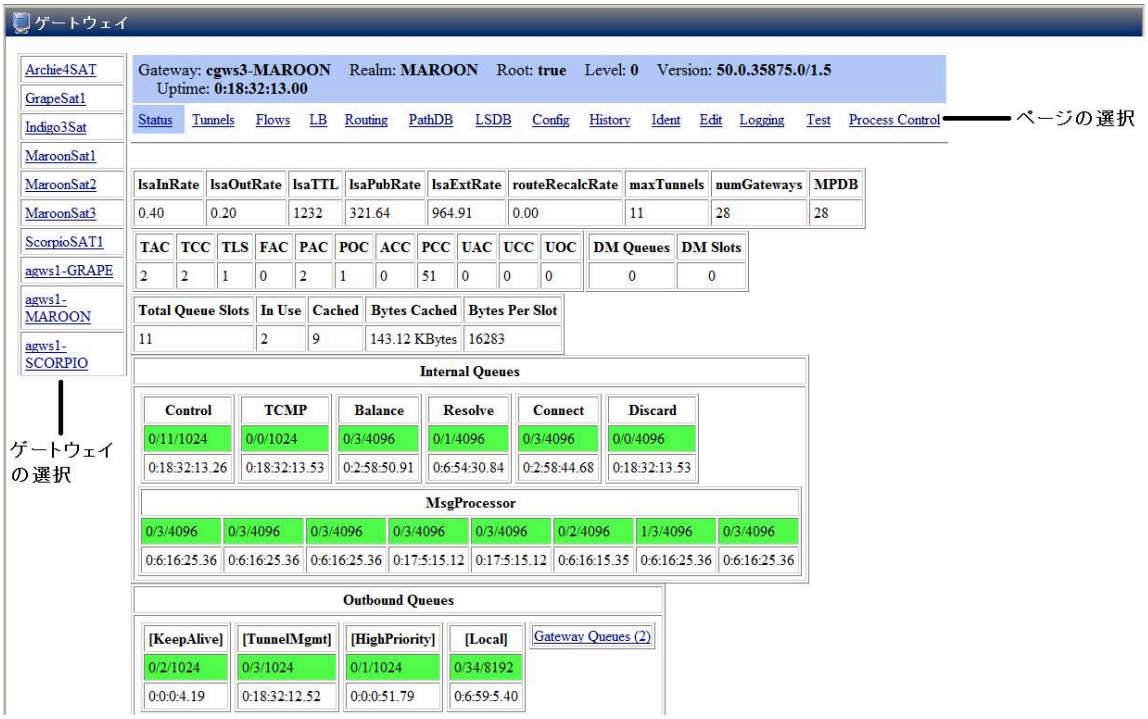
サーバーを検索すると、IPアドレスが同じで存在するレルムが異なる複数のサーバーが検索結果に表示されることがあります。また、カスタム拡張を実行しようとしたときに、カスタム拡張を実行するサーバーを選択する画面で、IPアドレスが同じサーバーが複数表示される場合もあります。

SAクライアントのサーバーのプロパティビューには、IPアドレスに対応したサーバーを識別する追加情報が表示されます。

サテライトのゲートウェイ情報の表示と管理

サテライトのゲートウェイ情報を表示するには、SAクライアントのナビゲーションパネルで、[管理] タブを選択してから、[ゲートウェイ] を選択します。これにより、図30のようにゲートウェイのステータスが表示されます。左側のゲートウェイのリストから、表示するゲートウェイを選択します。ページ上部のリンクから、表示するゲートウェイ情報を選択します。

図30　　ゲートウェイのステータス



ゲートウェイのステータスは、次のタスクで使用します。

- ゲートウェイおよびゲートウェイ間のトンネルに関するステータス情報を入手する。これはゲートウェイのデバッグに役立ちます。
- ゲートウェイインスタンス間の帯域幅制限またはトンネルコストを変更する。
- ゲートウェイプロセスを再開する。

- ゲートウェイプロセスのログレベルを変更する。

ゲートウェイの診断およびデバッグ情報の表示

1. SAクライアントで[管理]タブを選択し、続いて[ゲートウェイ]を選択します。
2. 左側のゲートウェイのリストから、情報を表示するゲートウェイを選択します。選択したゲートウェイに関する、次のステータスが表示されます。
   - 次の内容を含むアクティブなトンネルのテーブル
     - トンネルコスト
     - 帯域幅制約
     - 帯域幅予測
     - トンネルの経過時間
   - 内部メッセージキューに関する情報。キューのテーブル内の各列では、次の形式でデータが表示されます。
     - キュー内のメッセージ数
     - キューのメッセージ上限
     - キューに設定されている最大値
     - キューのメッセージ上限に到達した最終時刻。最後にメッセージ上限に到達したときのタイムスタンプを使用して、ゲートウェイの問題のトラブルシューティングを行うことができます。タイムスタンプは`DD:HH:mm:ss`の形式で表示されます。
3. ゲートウェイ間のトンネルの詳細および統計情報を表示するには、トンネルが終わるゲートウェイのリンクを選択します(図31を参照)。

図31　[ゲートウェイ]—[Status]ページ

これにより、トンネルの詳細および統計情報が表示されます。

4. 診断情報を含む次のページを表示するには、ページ上部の次のいずれかのリンクを選択します。
   - **Flows**: 選択したゲートウェイの開いているすべての接続に関する情報が表示されます。
   - **Routing**: ゲートウェイ間のルーティングテーブルが表示されます。このテーブルには、メッシュ内の別のゲートウェイにアクセスするのに使用するトンネルが表示されます。ルーティングテーブルは、パスデータベース内のデータから計算されます。ルーティングの計算は、接続のリンクコストが変わると、自動的に更新されます。

トンネルが消滅した場合、デフォルトで、ルーティング情報はルーティングテーブルに2分間保持されます。これにより、メッシュの継続性が確保されます。

- **PathDB** - パスデータベース: メッシュ内の到達可能なすべてのゲートウェイに対するコストの最も低いルートが表示されます。SAでは、リンクステートデータベースのデータから、到達可能なすべてのゲートウェイに対するコストの最も低いルートを特定します。
- **LSDB** - リンクステートデータベース: 各ゲートウェイインスタンスから見たすべてのトンネルの状態に関する情報が含まれます。LSDBには、すべてのトンネルのデータと各トンネルの帯域幅の制約が含まれます。
- **Config**: 選択したゲートウェイのプロパティファイルが表示されます。これには、ゲートウェイコンポーネントを実行しているサーバー上のプロパティファイルへのパスが含まれます。このページのプロパティ値の下には、暗号ファイル情報とメッシュプロパティデータベースがあります。[**Properties Cache**] フィールドは、プロパティ値の上にあります。ゲートウェイ間の接続の帯域幅またはリンクコストを変更して、更新が正常に完了すると、更新後の値がこのフィールドに表示されます。
- **History**: ゲートウェイメッシュを使用するホスト間の受信 (入力) 接続と送信 (出力) 接続に関する履歴情報が表示されます。たとえば、レルムAのホストAがレルムBのホストBといつ接続されていたかが表示されます。

接続のソースIPアドレスとレルムの識別

Ident: リアルタイム接続識別データベースへのインタフェースを提供します。このツールの使用方法に関する追加情報が必要な場合は、HPサポートまでご連絡ください。

1. SAクライアントで [管理] タブを選択し、続いて [ゲートウェイ] を選択します。
2. [**Ident**] リンクを選択します。リアルタイム接続識別データベースが表示されます。
3. 編集ボックスに、アクティブな接続のプロトコルとソースポートをコロンで区切って入力します（たとえば、TCP:25679)。
4. [**Lookup**] ボタンを選択します。これにより、接続元のクライアントレルムとクライアントIPアドレスが表示されます。

ゲートウェイ間の帯域幅またはリンクコストの変更

[**Edit**] リンクでは、リンク帯域幅の制約、リンクコスト、および負荷分散ルールを変更できます。

ゲートウェイ間の帯域幅の変更は、必ずコアゲートウェイで行う必要があります。その他のゲートウェイで変更を行っても、変更は反映されません。

1. SAクライアントで [管理] タブを選択し、続いて [ゲートウェイ] を選択します。

2 接続の帯域幅制限を指定するには、次の手順を実行します。

a ページ上部の [**Edit**] リンクを選択します。これにより、リンク帯域幅の制約を変更するためのコントロールが表示されます。

b トンネルで接続された2つのゲートウェイインスタンスの名前を指定します。

c 帯域幅制限をキロビット/秒 (Kbps) で指定します。接続の帯域幅制限をなくす場合は、ゼロ (0) を指定します。

d [**Apply**] をクリックします。

3 接続のリンクコストを設定するには、次の手順を実行します。

a ページ上部の [**Edit**] リンクを選択します。これにより、リンクコストを変更するためのコントロールが表示されます。

b トンネルで接続された2つのゲートウェイインスタンスの名前を指定します。

c [**Cost**] フィールドで必要なコストを指定します。

d [**Apply**] をクリックします。

4 接続の負荷分散ルールを設定するには、次の手順を実行します。

a ページ上部の [**Edit**] リンクを選択します。これにより、負荷分散ルールを変更するためのコントロールが表示されます。

b ゲートウェイのインスタンス名を指定します。

c 負荷分散ルールを指定します。

d [**Apply**] をクリックします。

ゲートウェイログの表示またはログレベルの変更

ログレベルをLOG_DEBUGまたはLOG_TRACEに変更すると、ゲートウェイのログ出力が大幅に増えて、ゲートウェイのパフォーマンスに悪影響を及ぼす可能性があります。

1 SAクライアントで [管理] タブを選択し、続いて [ゲートウェイ] を選択します。

2 ページ上部の [**Logging**] リンクを選択します。ゲートウェイのログファイルの末尾が表示されます。

3 ログレベルを変更するには、LOG_INFO、LOG_DEBUG、LOG_TRACEのいずれかを選択します。

4 [**Submit**] を選択します。

ゲートウェイプロセスの再開または停止

1 SAクライアントで [管理] タブを選択し、続いて [ゲートウェイ] を選択します。

2 ページ上部の [**Process Control**] リンクを選択します。

3 ゲートウェイプロセスを再開するには、[**restart**] を選択します。

4 ゲートウェイウォッチドッグとゲートウェイを停止するには、[**shutdown**] をクリックします。

ゲートウェイプロセスを停止すると、SAコアに問題が発生する可能性があります。たとえば、コアゲートウェイプロセスを停止した場合、そのSAコアに対するすべてのマルチマスタートラフィックを停止することになり、SAクライアントからゲートウェイを制御できなくなります。

ゲートウェイを停止した後でSAクライアントからゲートウェイを再開するには、ゲートウェイコンポーネントを実行しているサーバーにログオンして、手動でプロセスを再開する必要があります。

サテライトの監視

第7章「SAコアコンポーネントの監視」の次の項を参照してください。

- エージェントキャッシュの監視 (184ページ)
- ゲートウェイの監視 (200ページ)

リモート接続の帯域幅管理

通信ネットワークでは、ネットワークトラフィックを制御してネットワークの輻輳を抑制するために帯域幅管理を使用します。通常、SAのリモートサイト管理モデルでは、(ブランチオフィスなどの) すべての論理拠点にリモートゲートウェイを展開して、リモートサーバーへの接続の処理とネットワーク帯域幅管理を行うサテライト構成を使用します。しかし、この構成では、管理するサーバー数の少ない拠点のためにコスト効率が大きく低下します。

SAの新しい帯域幅管理では、サーバー数の少ないリモート拠点にサテライトをインストールする必要がありません。SA の帯域幅構成管理 (BCM) ツールを使用して、リモートサーバーと通信する際にエージェントまたはサテライトゲートウェイで使用する帯域幅を制御することができます。

BCM ツールを使用すると、帯域幅の構成をピアグループにプッシュすることができます。ピアにプッシュされた構成は、ファイルに保存されます。ゲートウェイの起動時に、このファイルから構成をロードして、ピア間で構成を同期します。クライアントがSAゲートウェイメッシュ経由で接続をネゴシエートしてリモートTCPサービスと接続すると、クライアントは入力ゲートウェイとTCP接続されます。また、出力ゲートウェイからリモートサービスへのTCP接続も存在します。

ゲートウェイメッシュを介したプロキシ接続が確立されると、入力/出力接続のピアアドレスが分類され、それぞれの分類ごとにランタイムキューが作成されます。この時点で、接続の帯域幅調整が有効になります。キューは接続をデータが流れるときの帯域幅使用状況に基づいて更新されます。帯域幅使用状況はピアグループ間で共有されるため、ゲートウェイクラスターごとにローカルキューを更新することができます。許容される最大帯域幅の範囲で接続にデータを流すことができます。キューの帯域幅使用状況は、1 秒間隔でリセットされます。

➤ エージェントゲートウェイの帯域幅をネゴシエートして通信を行うには、同じレルムのすべてのエージェントゲートウェイで、同じSAバージョンが実行されている必要があります。コアとサテライトのSAバージョンが異なる混在型のコア構成は、サポートされません。

SA帯域幅構成管理ツール

➤ SA BCMは、SolarisまたはRed Hat Enterprise Linux 3 x86を実行するSAコア/サテライトではサポートされません。

この項では、BCM ツールを使用した、帯域幅管理の構成の作成について説明します。これらの構成は、その後ピアゲートウェイ間で自動的に同期されます。

BCMツールを使用してゲートウェイ構成をプッシュできるのは、ゲートウェイホストへのrootアクセスが可能な管理ユーザーだけです。

➤ BCMツールは、次のデフォルトの構成ファイルを使用してインストールされます。

```
/etc/opt/opsware/gateway_name/BWT.conf
```

このファイルは直接変更しないでください。最初にファイルをコピーして、それぞれの構成に合わせてファイルを編集した後に、gwctl -fコマンドを使用してレルム内のすべてのゲートウェイに変更した構成ファイルをプッシュします。帯域幅管理構成ツールの起動を参照してください。

指定した帯域幅の構成は、構成ファイルに保存されます。次に、一般的なゲートウェイ構成ファイルの例を示します。

```
enabled

# ブランチオフィスには3Mbpsの接続しかないため、SA で
# 512Kbps以上を使用することはできない。
queue branch_office bandwidth 512KB

# ブランチオフィスAおよびB（非標準アドレス）
class 192.168.1.[1-5,10-15,20,30] for branch_office

# その他のブランチオフィス
class 192.168.2.0/24 for branch_office
```

帯域幅管理構成ツールの起動

BCMツールは、コマンドラインから起動します。

SAエージェント構成を管理するサテライトで、次のコマンドを使用します。

```
gwctl: [オプション] ...
```

表21　帯域幅構成管理ツールのオプション

オプション	説明
-?、--help	使用方法が表示されます。
-p、--port	-lとともに指定すると、エージェントゲートウェイプロキシポート (デフォルト3001) が表示されます。 他のオプション (-d、-e、-f、-v、-c、-sなど) とともに指定すると、帯域幅調整構成ポート (デフォルト8086) が表示されます。
-l、--list_gws	このレルム内のすべてのゲートウェイが表示されます。
-f、--conf	構成ファイル。
-v、--verify_conf	構成ファイルを確認して終了します。構成ファイルをゲートウェイにプッシュすることはありません。**注:** このオプションは、必ず-f <conf_path>とともに使用します。
-c、--cksum	構成ファイルのチェックサムを表示します。**注:** このオプションは、必ず-f <conf_path>とともに使用します。
-e、--enable_bwt	このレルムの帯域幅調整を有効にします。
-d、--disable_bwt	このレルムの帯域幅調整を無効にします。
-r、--request_conf	特定のゲートウェイの構成を要求します。
-s、--signature	特定のゲートウェイの構成署名を要求します。
-z、--verbose	すべてのメッセージを表示します。

次に、コマンドの例を示します。

レルム内のゲートウェイを表示する:

```
gwctl -l
```

異なるエージェントゲートウェイポートを指定する:

```
gwctl --port 2003 -l
```

構成ファイルの確認のみを行う:

```
gwctl -f myconf.conf -v
```

レルム内のすべてのエージェントゲートウェイへ構成ファイルをプッシュする (localhostを含む):

```
gwctl -f mytconf.conf
```

リモート接続の帯域幅管理の有効化/無効化

リモート接続の帯域幅管理は、次のいずれかの方法で有効または無効にする必要があります。

- ファイルの最初のエントリに`enabled`または`disabled`のキーワードを含む帯域幅構成ファイルをプッシュします。各構成ファイルの最初の行に、帯域幅調整のステータスを示す`enabled`または`disabled`が含まれている必要があります。
- コマンドラインで`gwctl -e`を使用して帯域幅管理を有効にするか、または`gwctl -d`を使用して帯域幅管理を無効にします。帯域幅管理の有効または無効の状態は、バージョンのアップグレードなしに帯域幅管理構成ファイル内に残ります。

帯域幅構成の文法

帯域幅構成の文脈自由文法 (CFG) (EBNF形式):

```
config : ((queue | class | version | config_source | config_user | disabled |
comment)?'\n')\*
```

```
queue  : 'queue' queue_name 'bandwidth' d_number bandwidth_spec
('rtt' d_number)?('parent' queue_name 'borrow')?
```

```
queue_name : "[a-zA-Z0-9_]+"
```

```
class  : 'class' pattern (',' pattern)* 'for' queue_name
```

```
pattern : ipv4 | ipv4_cidr
```

```
ipv4 : ipv4_address_pattern_element ('.' ipv4_address_pattern_element)@1:3
```

```
ipv4_cidr : d_number ('.' d_number)@1:3 '/' d_number
```

```
ipv4_address_pattern_element : single_number | range | range_class |
wildcard range_class : '[' (number ('-' number)? ',')+ ']'
```

```
wildcard : '*'
```

```
range : '[' number '-' number ']'
```

```
single_number : d_number
```

```
number : d_number
```

```
d_number : "[0-9]+"
```

```
x_number : "[a-fA-F0-9]+"
```

```
bandwidth_spec : "[GMK]?[bB]"
```

```
config_source : 'config-source' ':' "[a-zA-Z0-9.:\-]+"
```

```
config_user   : 'config-user' ':' "[a-zA-Z0-9_!@#$%^&*();.`~\-\\]+"
```

```
disabled : 'disabled'
```

```
comment  : '#' "[^\n]*"
```

サテライトのソフトウェアリポジトリキャッシュの管理

SAコア内のネットワークトラフィックは、次の場所で最も多く発生します。

- ソフトウェアリポジトリと管理対象サーバー上のサーバーエージェントとの間（アプリケーションソフトウェアまたはOSパッチのインストール時）
- OSプロビジョニング中のサーバーとプロビジョニング用のOSメディアを提供するOSプロビジョニングメディアサーバーとの間

サテライトが帯域幅の小さなネットワークリンクで接続されている場合、これらの処理の最中はパフォーマンスが低下します。コアのソフトウェアリポジトリの内容をサテライトのソフトウェアリポジトリキャッシュにコピーするか、サテライトにローカルのOSプロビジョニングメディアサーバー/ブートサーバーをインストールすると、ネットワークトラフィックを最小限に抑えることができます。

ソフトウェアリポジトリキャッシュには、SAコアのソフトウェアリポジトリ内（または別のサテライトのソフトウェアリポジトリキャッシュ）のファイルのコピーが格納されるため、SAはサテライトとSAコアとの間でネットワークを介して要求を受け渡しすることなく、ローカルにソフトウェア要求に対応することができます。同様に、OSプロビジョニングメディアサーバーは、OSイメージをローカルで提供することができます。SAサテライトは、レルムごとに複数のソフトウェアリポジトリキャッシュをサポートします。

次の各項では、ローカルのソフトウェアリポジトリキャッシュの構成と更新について説明します。また、必要に応じて、OSプロビジョニングメディア/ブートサーバーについても説明します。

ソフトウェアリポジトリキャッシュの内容の可用性

ソフトウェアリポジトリの内容はサテライトのソフトウェアリポジトリキャッシュに自動的に複製されるわけではないため、すべての内容がメッシュ内のサテライトでローカルに使用できるとは限りません。ローカルでインストールするソフトウェアをサテライトのソフトウェアリポジトリキャッシュに手動で追加する必要があります。オンデマンドの更新が利用できるのは、ソフトウェアリポジトリキャッシュのレルムのキャッシュポリシーが`on-demand`である場合に限られます。

SAでは、要求されたソフトウェアがローカルで使用できないことと、最初のコアのソフトウェアリポジトリまたは別のサテライトのソフトウェアリポジトリキャッシュから内容を更新する必要があることの警告のみを行うことができます。SAでは、パッケージがローカルで使用可能かどうかを追跡します。

代わりに、SAで管理対象サーバーでローカルに使用できない要求されたソフトウェアの修復を行おうとすると、SA Webクライアントでエラーが生成されて欠落しているパッケージのリストが表示されます。これにより、キャッシュへのコピーが必要なパッケージを識別することができます。キャッシュにコピーされたソフトウェアは、その後インストールを行う際に引き続きローカルで使用できます。

SA Webクライアントには、パッケージをサテライトにプッシュするためのユーザーインタフェースが用意されていませんが、コマンドラインツール`stage_pkg_in_realm`を使用して、サテライトにパッケージをプッシュすることができます。

このツールは、次のディレクトリにある最初のコアのモデルリポジトリホストにあります。

```
/opt/opsware/mm_wordbot/util/stage_pkg_in_realm
```

ファイルに対するURL要求で`checkonly=1`引数を使用した場合、ユーティリティはファイルを要求しますが、ソフトウェアリポジトリはファイルを送信しません。ファイルがまだキャッシュされていない場合、ソフトウェアリポジトリキャッシュは親のソフトウェアリポジトリキャッシュからファイルを取得します。ただし、キャッシュポリシーで許可されている必要があります。

サテライトのソフトウェアリポジトリキャッシュ内のソフトウェアの更新

サテライトのソフトウェアリポジトリキャッシュ内のファイルを更新するには、要求を受け取ったときにキャッシュされたファイルを更新するか（オンデマンド更新）、またはキャッシュされたファイルを手動で更新するように（手動更新）、キャッシュを構成します。

- オンデマンド更新：ローカルのソフトウェアリポジトリキャッシュが、SAコア内のソフトウェアリポジトリから必要に応じて現在のファイルを取得します。

- **手動更新:** パッケージをインストールする前に、SAでソフトウェアパッケージをサテライトのソフトウェアリポジトリキャッシュにステージングして、管理対象サーバーがコアと同じデータセンター内にある場合とパフォーマンスがほぼ同じになるようにします。

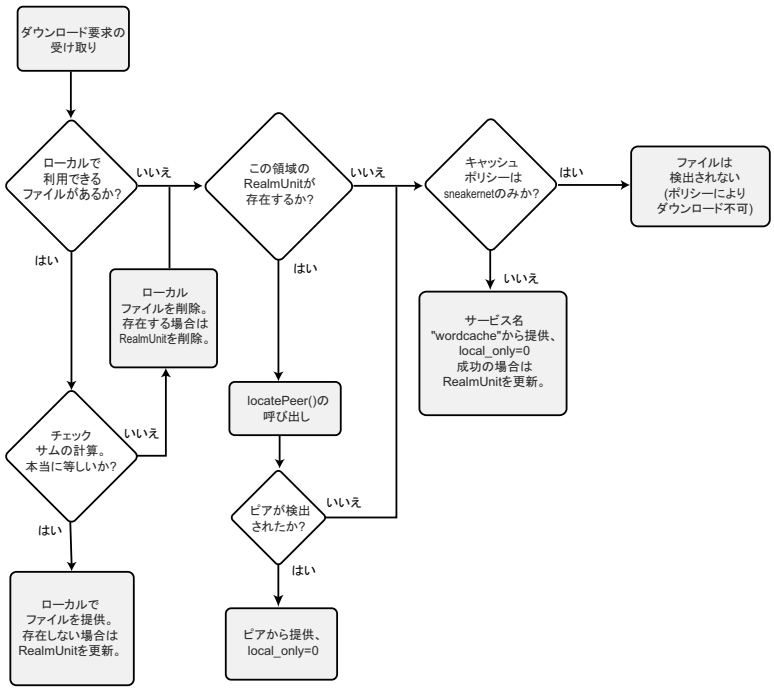
オンデマンド更新が有効でも、要求されたファイルがローカルのソフトウェアリポジトリキャッシュ内にすでに存在して、ファイルが最新である場合には、アクションは実行されません。ソフトウェアがローカルに存在しないか最新でない場合、ソフトウェアリポジトリキャッシュは、最も近い上流のソフトウェアリポジトリキャッシュまたはコアのソフトウェアリポジトリから、バックグラウンドでファイルをダウンロードしようとします。

キャッシュポリシーが手動更新の場合に、ソフトウェアのオンデマンド更新を要求すると、ソフトウェアリポジトリキャッシュは`wordbot.unableToCacheFile exception`を生成します。

ファイルをソフトウェアリポジトリキャッシュにステージングすることは、キャッシュポリシーに関係なく、いつでもできます。詳細については、この章の「ソフトウェアリポジトリキャッシュへのファイルのステージング」(146ページ)を参照してください。

図32は、ソフトウェアリポジトリキャッシュでサテライト内のパッケージの更新に使用するロジックを説明したものです。

図32　　ソフトウェアリポジトリキャッシュの更新ロジック



ソフトウェアリポジトリキャッシュの更新ポリシーの設定

各ファシリティのソフトウェアリポジトリキャッシュ更新ポリシーを指定するには、次の手順を実行します。

1. SAクライアントで **[管理]** タブを選択します。
2. 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。
3. ソフトウェアリポジトリキャッシュ更新ポリシーを設定するレルムを選択します。これにより、そのレルムのすべてのシステム構成が表示されます。
4. 構成パラメーター `word.caching_policy`を確認します。
5. このパラメーターの値を、次のいずれかに設定します。
   - **デフォルト値: JIT**を選択します。これにより、JITまたはオンデマンドの更新が指定されます。

— 新しい値ボタン  を選択して、編集フィールドに「SNEAKERNET」と入力します。これにより、手動更新が指定されます。

6 [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。

オンデマンド更新

オンデマンド更新を有効にすると、ローカルで使用できるようになっていないソフトウェアが要求されたときに、すぐにソフトウェアをサテライトのソフトウェアリポジトリキャッシュにダウンロードできます。ネットワーク接続の帯域幅が小さい場合は、要求される頻度の高いソフトウェアをソフトウェアリポジトリキャッシュにあらかじめダウンロードしておくことができる手動更新の方が適している可能性があります。詳細については、手動更新 (143ページ) を参照してください。

サテライトの管理対象サーバーのサーバーエージェントがソフトウェアを要求するたびに、ローカルのソフトウェアリポジトリキャッシュは、キャッシュされたソフトウェアが最新かどうかをチェックします。キャッシュされたファイルが最新でない場合や存在しない場合、ソフトウェアリポジトリキャッシュは、最も近い上流のソフトウェアリポジトリキャッシュまたはコアのソフトウェアリポジトリから最新のファイルのローカルコピーを取得して、要求元のサーバーエージェントに送信します。

オンデマンド更新を行うように構成したソフトウェアリポジトリキャッシュがソフトウェアの要求を受け取ると、キャッシュは最初にコアのソフトウェアリポジトリのチェックサムに対するソフトウェアのチェックサムを要求して、キャッシュのソフトウェアが最新であることを確認します。

セキュリティ上の理由から、SAはソフトウェアのチェックサムを一定期間キャッシュします。キャッシュする期間はユーザーが構成できます。

チェックサムがローカルに保存されているファイルと同じである場合、ソフトウェアリポジトリキャッシュはソフトウェアを要求元に提供します。チェックサムが一致しないか、ローカルファイルが存在しない場合、ソフトウェアリポジトリキャッシュは、最も近い上流のソフトウェアリポジトリキャッシュまたはコアのソフトウェアリポジトリから最新のソフトウェアを要求します。

ソフトウェアリポジトリキャッシュがソフトウェアをダウンロードしている最中にネットワーク接続が失われ、その後サーバーエージェントから同じソフトウェアが要求されると、ソフトウェアリポジトリキャッシュはダウンロードが中断された続きからファイルのダウンロードを再開します。

手動更新

ネットワーク接続の帯域幅が小さいサテライトの場合、ソフトウェアリポジトリキャッシュの手動更新を使用すると、インストール時にソフトウェアリポジトリキャッシュを事前に読み込んでおくことができます。また、既存のキャッシュに対する更新を構成することもできます。ソフトウェアリポジトリキャッシュの読み込みは、ネットワークを使用せずに行います。たとえば、必要なパッケージを収めたCDを作成してサテライトに送ります。手動更新を実行するには、SA DCML Exchange Tool (DET) を使用して SA コアから既存のパッケージをコピーするか、ステージングユーティリティを使用して更新を実行します。ソフトウェアリポジトリキャッシュの手動更新の作成 (144 ページ) およびソフトウェアリポジトリキャッシュへのファイルのステージング (146ページ) を参照してください。

手動更新を行うように構成したソフトウェアリポジトリキャッシュは、手動更新が実行されるまで、上流のソフトウェアリポジトリキャッシュやコアのソフトウェアリポジトリと通信しません。サテライトはそれぞれの専用のソフトウェアリポジトリキャッシュを正式なものとみなします。

キャッシュポリシーが手動更新の場合に、ソフトウェアのオンデマンド更新を要求すると、ソフトウェアリポジトリキャッシュは`wordbot.unableToCacheFile exception`を生成します。

ソフトウェアリポジトリをオンデマンド更新に構成している場合でも、更新ポリシーに関係なく、手動更新を適用できます。

複数のソフトウェアリポジトリキャッシュを含むサテライトで手動更新を適用する際には、サテライト内の各ソフトウェアリポジトリキャッシュに更新を適用する必要があります。このようにしないと、キャッシュからファイルを取得する操作を実行する際に (たとえば、サテライト内のサーバーにソフトウェアをインストールする際に)、`wordbot.unableToCache file`エラーが発生する可能性があります。

ソフトウェアリポジトリキャッシュの緊急更新

キャッシュポリシーが手動更新の場合でも、ネットワーク経由でサテライトに緊急更新をプッシュすることができます。緊急更新をソフトウェアリポジトリキャッシュにプッシュするのに、ソフトウェアリポジトリキャッシュのキャッシュポリシーを再構成する必要はありません。たとえば、CDをサテライトに送付せずに、緊急パッチをサテライトにステージングして適用することができます。

ソフトウェアリポジトリキャッシュのサイズの管理

ソフトウェアリポジトリキャッシュに手動更新を適用する場合、キャッシュサイズの上限を超えると、SAによって最近使用していないファイルが削除されます。

最近の使用頻度が最も低いパッケージが最初に削除されます。

その後、ソフトウェアリポジトリキャッシュでキャッシュをクリーンアップする際に、これらのファイルが削除されます。デフォルトで、キャッシュは12時間ごとにクリーンアップされます。使用可能なディスク容量の制限値を超えないように、パッケージが削除されます。

ソフトウェアリポジトリキャッシュがキャッシュサイズの上限を超えないようにするには、ソフトウェアリポジトリキャッシュに必要なすべてのパッケージを格納できるだけのディスク容量が必要です。

ソフトウェアリポジトリキャッシュの手動更新の作成

手動更新を作成するには、SA DCML Exchange Tool (DET)を使用して、SAコアから既存のソフトウェアをコピーして、エクスポートファイルを保存します。エクスポートファイルは、ネットワーク経由でサテライトのソフトウェアリポジトリキャッシュにコピーしたり、CD/DVDに焼いてソフトウェアリポジトリキャッシュに適用したりすることができますまた、ステージングユーティリティを使用してソフトウェアをアップロードすることもできます。詳細については、ソフトウェアリポジトリキャッシュへのファイルのステージング (146ページ) を参照してください。

ここでは、次の内容について説明します。

- DCML Exchange Tool (DET)を使用した手動更新の作成
- ソフトウェアリポジトリキャッシュへの手動更新の適用
- ソフトウェアリポジトリキャッシュへのファイルのステージング
- Microsoftユーティリティのアップロードと手動更新

DCML Exchange Tool (DET)を使用した手動更新の作成

ここでは、DETを使用します。DETを使用して、手動更新用のソフトウェアのエクスポートとソフトウェアポリシーに関連するパッケージのエクスポートを行います。

DETの詳細については、『SAコンテンツユーティリティガイド』を参照してください。

手動更新を作成するには、次の手順を実行します。

1 DET コンポーネントをインストールしたサーバーで、次のコマンドを実行して、次のディレクトリを作成します。

```
# mkdir /var/tmp/sneakernet
```

2 SAクライアントが稼働するサーバーで、
/var/opt/opsware/crypto/occディレクトリから

opsware-ca.crt

spog.pkcs.8

の2つのファイルを次のディレクトリにコピーします。

/usr/cbt/crypto

これはDETをインストールしたディレクトリです。

3 次の内容を含むファイル/usr/cbt/conf/cbt.confを作成します。

```
twist.host=<twistのホスト名>
twist.port=1032
twist.protocol=t3s
twist.username=buildmgr
twist.password=buildmgr
twist.certPaths=/usr/cbt/crypto/opsware-ca.crt
spike.username=<あなたのユーザー名>
spike.password=<あなたのパスワード>
spike.host=<wayのホスト名>
way.host=<wayのホスト名>
spin.host=<spinのホスト名>
word.host=<wordのホスト名>
ssl.keyPairs=/usr/cbt/crypto/spog.pkcs8
ssl.trustCerts=/usr/cbt/crypto/opsware-ca.crt
```

4 次の内容を含む、DCML Exchange Toolフィルターファイル/usr/cbt/filters/myfilter.rdfを作成します。

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE rdf:RDF [
<!ENTITY filter "http://www.opsware.com/ns/cbt/0.1/filter#">
]>
<rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
xmlns="http://www.opsware.com/ns/cbt/0.1/filter#">
<ApplicationFilter rdf:ID="a1">
<path>/Other Applications</path>
<directive rdf:resource="&filter;Descendants" />
</ApplicationFilter>
</rdf:RDF>
```

フィルターファイルの<path>ディレクティブでは、/Other Applicationsをエクスポートするノードへのパスに置き換えます(エクスポートするノード、その子孫、関連するすべてのパッケージに関するすべてのノード情報がエクスポートされます)。

このフィルターは、SAクライアントのアプリケーション領域からエクスポートします。SAクライアントで他のカテゴリのソフトウェアからパッケージをエクスポートする場合は、別のフィルターを作成する必要があります。詳細については、『SAコンテンツユーティリティガイド』を参照してください。

5 DETコンポーネントをインストールしたサーバーで、次のコマンドを入力して、DCML Exchange Toolを実行します。

```
# /usr/cbt/bin/cbt -e /var/tmp/myexport --config /usr/cbt/conf/cbt.conf
--filter /usr/cbt/filters/myfilter.rdf
```

DCML Exchange Toolにより、エクスポートされたノードに関連するパッケージが、次のディレクトリに配置されます。

/var/tmp/myexport/blob

パッケージには、unitid_nnnnnnn.pkgという名前が割り当てられます。

6 すべての .pkg ファイルをソフトウェアリポジトリキャッシュを実行しているサーバー上のディレクトリにコピーします。ファイルはネットワーク経由でコピーするか、CD/DVDに焼いてコピーします。

ソフトウェアリポジトリキャッシュへの手動更新の適用

ソフトウェアリポジトリキャッシュに手動更新を適用するには、ユーティリティ (import_sneakernet) を実行します。このユーティリティは、ソフトウェアリポジトリキャッシュの適切な場所に更新するソフトウェアを移動またはコピーして、SAコアのモデルリポジトリに登録します。

ソフトウェアリポジトリキャッシュに手動更新を適用するには、次の手順を実行します。

1 サテライトのソフトウェアリポジトリキャッシュを実行しているサーバーにrootとしてログインします。

2 エクスポートファイルをソフトウェアリポジトリキャッシュサーバー上のディレクトリにコピーするか、ソフトウェアエクスポートファイルを含むCDをマウントするか、CDの内容を一時ディレクトリにコピーします。

3 次のコマンドを入力して、ディレクトリを変更します。

```
# cd /opt/opsware/mm_wordbot/util
```

4 次のコマンドを入力して、エクスポートファイルの内容をソフトウェアリポジトリキャッシュにインポートします。

```
# ./import_sneakernet -d dir
```

ここで、dir はCDマウントポイントまたはエクスポートファイルを含む一時ディレクトリです。

ソフトウェアリポジトリキャッシュへのファイルのステージング

管理対象サーバー上のサーバーエージェントでは、使用中のレルムのキャッシュポリシーをオーバーライドできます。ソフトウェアリポジトリキャッシュのキャッシュポリシーをオーバーライドできるため、手動更新に構成されているキャッシュにソフトウェアをステージングすることで、次のような状況に対処することができます。

- 緊急パッチを配布する必要があるが、手動更新のエクスポートファイルを作成し、実際にファシリティまで行ってソフトウェアをアップロードする時間がない場合。
- 必要なパッチを所定のメンテナンス時間中にインストールする必要があるが、すべての管理対象サーバーでパッチをダウンロードしてインストールできるだけの時間がない場合。
- サテライトへのネットワーク接続の使用率が特定の時間帯に低くなり、アップロードに適していることがわかっている場合。

パッケージのステージングを強制的に実行するには、ステージングユーティリティの引数override_caching_policy=1をソフトウェアに対するURL要求で指定します。

ソフトウェアリポジトリキャッシュでは、クライアントがファイルの取得を要求できるようにしますが、実際にはファイルは送信されません。ファイルがまだキャッシュされていない場合、ソフトウェアリポジトリキャッシュは親のソフトウェアリポジトリキャッシュからファイルを取得します。ただし、キャッシュポリシーで許可されている必要があります。この機能を使用するには、クライアントでファイルに対するURL要求で引数checkonly=1を使用します。

ステージングユーティリティの実行

ステージングユーティリティを実行するには、次の手順を実行します。

1 ソフトウェアリポジトリコンポーネント (スライスコンポーネントバンドルに含まれる) を実行しているサーバーで、証明書token.srvがCRYPTO_PATHに存在するのを確認します。インストール時に、token.srvは次の場所にコピーされます。

```
/var/opt/opsware/crypto/gateway/token.srv
```

2 コアのソフトウェアリポジトリを実行しているサーバーにログインします。

3 次のコマンドを入力して、ディレクトリを変更します。

```
# cd /opt/opsware/mm_wordbot/util
```

4 必要なファイルをステージングするには、ユーティリティ stage_pkg_in_realm を実行します。このユーティリティの構文は、次のとおりです。

```
./stage_pkg_in_realm [-h | --help] [-d | --debug]
[--user <ユーザー>] --pkgid <ID> --realm <レルム> [--gw <IP:ポート>] [--spinurl
<URL>] [--wayurl <URL>] [--word <IP:ポート>]
```

パッケージのステージングを強制的に実行するには、ステージングユーティリティの引数 override_caching_policy=1をソフトウェアに対するURL要求で指定します。

例

```
./stage_pkg_in_realm --user admin --pkgid 80002 --realm luna
--gw 192.168.164.131:3001
Password for admin: <パスワード>
Package /packages/opsware/Linux/3ES/miniagent is now being staged in realm
luna
```

Microsoftユーティリティのアップロードと手動更新

Microsoftの新しいパッチ適用ユーティリティ(『SA Installation Guide』の「System Requirements」を参照)をアップロードする際には、ソフトウェアリポジトリキャッシュが手動更新のみに構成されているすべてのレルムに、該当するファイルを直ちにステージングしてください。

これらのファイルをリモートのレルムにステージングしないと、これらのレルム内のWindowsサーバーで実行中のサーバーエージェントで、新しいバージョンのユーティリティをダウンロードできないため、ソフトウェアパッケージを登録することができなくなります。ソフトウェアリポジトリキャッシュがオンデマンド更新に構成されている場合、レルムに対してパッケージをステージングする必要はありません。

ソフトウェアリポジトリキャッシュでは、クライアントがファイルの取得を要求できるようにしますが、実際にはファイルは送信されません。ファイルがまだキャッシュされていない場合、ソフトウェアリポジトリキャッシュは親のソフトウェアリポジトリキャッシュからファイルを取得します。ただし、キャッシュポリシーで許可されている必要があります。この機能を使用するには、クライアントでファイルに対するURL要求で引数 checkonly=1 を使用します。ファイルをステージングする方法については、この章の「ステージングユーティリティの実行」(146ページ)を参照してください。

SAサテライトのインストールとトポロジ

サテライトは、管理対象サーバーの数が少なく完全なSAコアインストールを必要としないリモートサイト向けのソリューションです。サテライトでは、ホストに最小限必要なコアコンポーネントのみをインストールでき、ホストからプライマリコア(最初のコア)のデータベースとその他サービスにSAゲートウェイ接続経由でアクセスします。

また、限られたネットワーク接続を使ってプライマリファシリティと接続する場合には、帯域幅の問題を軽減することもできます。サテライトで使用するネットワーク帯域幅の上限となるビットレートを指定することができます。これにより、サテライトのネットワークトラフィックによって、同じパイプ上にある他の重要なシステムのネットワーク帯域幅要件が影響を受けることがなくなります。

一般的に、サテライトはサテライトゲートウェイとソフトウェアリポジトリキャッシュで構成されまれますが、リモートファシリティでサーバー管理機能をフル装備することも可能です。ソフトウェアリポジトリキャッシュは、サテライトの管理対象サーバーにインストールされるソフトウェアパッケージのローカルコピーを保管するもので、サテライトゲートウェイは、プライマリコア(最初のコア)との通信を処理するものです。オプションで、OSプロビジョニングブートサーバーとメディアサーバーをサテライトホストにインストールし、サテライトOSプロビジョニングをサポートすることが可能です。

ただし、サテライトホストには、これ以外のSAコアコンポーネントはインストールできません。

サテライトのインストールおよび構成方法については、『SA Installation Guide』を参照してください。

サテライトはさまざまなトポロジを使用してインストールできます。サテライトのトポロジの詳細については、『SA概要とアーキテクチャーガイド』を参照してください。

一部の高度なトポロジでインストールやアップグレードを行う場合は、HPプロフェッショナルサービスの利用が必要です。特定のトポロジに対応したインストール手順について支援が必要な場合は、HPテクニカルサポートまたはHPプロフェッショナルサービスまでご連絡ください。

第5章 SAリモート通信の管理

この項では、SAゲートウェイの帯域幅使用を制御する方法 (帯域幅管理)、および完全なSAサテライトをインストールせずに管理対象サーバー数が 50 未満の小規模リモートサイトでソフトウェアキャッシュを構成するための方法 (管理対象サーバーのピアコンテンツキャッシュ) について説明します。

- リモート接続の帯域幅管理
- SA管理対象サーバーのピアコンテンツキャッシュ
- コンセプト: SAコア通信インフラストラクチャー

SAのサテライト、ゲートウェイ、エージェントの詳細については、『SA 概要とアーキテクチャーガイド』を参照してください。

リモート接続の帯域幅管理

通信ネットワークでは、ネットワークトラフィックを制御してネットワークの輻輳を抑制するために帯域幅管理を使用します。通常、SAのリモートサイト管理モデルでは、(ブランチオフィスなどの) すべての論理拠点にリモートゲートウェイを展開して、リモートサーバーへの接続の処理とネットワーク帯域幅管理を行うサテライト構成を使用します。しかし、この構成では、管理するサーバー数の少ない拠点のためにコスト効率が大きく低下します。

SAの新しい帯域幅管理では、サーバー数の少ないリモート拠点にサテライトをインストールする必要がありません。SAのBCMツールを使用して、リモートサーバーと通信する際にエージェントまたはサテライトゲートウェイで使用する帯域幅を制御することができます。

BCM ツールを使用すると、帯域幅の構成をピアグループにプッシュすることができます。ピアにプッシュされた構成は、ファイルに保存されます。ゲートウェイの起動時に、このファイルから構成をロードして、ピア間で構成を同期します。クライアントがSAゲートウェイメッシュ経由で接続をネゴシエートしてリモートTCPサービスと接続すると、クライアントは入力ゲートウェイとTCP接続されます。また、出力ゲートウェイからリモートサービスへのTCP接続も存在します。

ゲートウェイメッシュを介したプロキシ接続が確立されると、入力/出力接続のピアアドレスが分類され、それぞれの分類ごとにランタイムキューが作成されます。この時点で、接続の帯域幅調整が有効になります。キューは接続をデータが流れるときの帯域幅使用状況に基づいて更新されます。帯域幅使用状況はピアグループ間で共有されるため、ゲートウェイクラスターごとにローカルキューを更新することができます。許容される最大帯域幅の範囲で接続にデータを流すことができます。キューの帯域幅使用状況は、1 秒間隔でリセットされます。

エージェントゲートウェイの帯域幅をネゴシエートして通信を行うには、同じレルムのすべてのエージェントゲートウェイで、同じSAバージョンが実行されている必要があります。コアとサテライトのSAバージョンが異なる混在型のコア構成は、サポートされません。

SA帯域幅構成管理ツール

- SA BCMは、SolarisまたはRed Hat Enterprise Linux 3 x86を実行するSAコア/サテライトではサポートされません。
- BCMツールを使用する場合は、ファイアウォールでポート3001と8086のSAネットワークトラフィックを許可する必要があります。BCMツールの管理インタフェースを使用する場合は、ポート8089も開いておく必要があります。

  この項では、BCM ツールを使用した、帯域幅管理の構成の作成について説明します。これらの構成は、その後ピアゲートウェイ間で自動的に同期されます。

  BCMツールを使用してゲートウェイ構成をプッシュできるのは、ゲートウェイホストへのrootアクセスが可能な管理ユーザーだけです。
- BCMツールは、次のデフォルトの構成ファイルを使用してインストールされます。

  ```
  /etc/opt/opsware/gateway_name/BWT.conf
  ```

  このファイルは直接変更しないでください。最初にファイルをコピーして、それぞれの構成に合わせてファイルを編集した後に、`gwctl -f`コマンドを使用してレルム内のすべてのゲートウェイに変更した構成ファイルをプッシュします。帯域幅構成管理ツールの起動を参照してください。

  指定した帯域幅の構成は、構成ファイルに保存されます。次に、一般的なゲートウェイ構成ファイルの例を示します。

  ```
  enabled

  # ブランチオフィスには3Mbpsの接続しかないため、SA で
  # 512Kbps以上を使用することはできない。
  queue branch_office bandwidth 512KB

  # ブランチオフィスAおよびB （非標準アドレス）
  class 192.168.1.[1-5,10-15,20,30] for branch_office

  # その他のブランチオフィス
  class 192.168.2.0/24 for branch_office
  ```

帯域幅構成管理ツールの起動

BCMツールは、コマンドラインから起動します。

SAエージェント構成を管理するサテライトで、次のコマンドを使用します。

```
gwctl: [オプション] ...
```

表22　　帯域幅構成管理ツールのオプション

オプション	説明
`-?、--help`	使用方法が表示されます。
`-p、--port`	-lとともに指定すると、エージェントゲートウェイプロキシポート (デフォルト3001) が表示されます。 他のオプション (`-d、-e、-f、-v、-c、-s`など) とともに指定すると、帯域幅調整構成ポート (デフォルト8086) が表示されます。
`-l、--list_gws`	このレルム内のすべてのゲートウェイが表示されます。

表22　帯域幅構成管理ツールのオプション

オプション	説明
-f、--conf	構成ファイル。
-v、--verify_conf	構成ファイルを確認して終了します。構成ファイルをゲートウェイにプッシュすることはありません。**注:** このオプションは、必ず-f <conf_path>とともに使用します。
-c、--cksum	構成ファイルのチェックサムを表示します。**注:** このオプションは、必ず-f <conf_path>とともに使用します。
-e、--enable_bwt	このレルムの帯域幅調整を有効にします。
-d、--disable_bwt	このレルムの帯域幅調整を無効にします。
-r、--request_conf	特定のゲートウェイの構成を要求します。
-s、--signature	特定のゲートウェイの構成署名を要求します。
-z、--verbose	すべてのメッセージを表示します。

次に、コマンドの例を示します。

レルム内のゲートウェイを表示する:

```
gwctl -l
```

異なるエージェントゲートウェイポートを指定する:

```
gwctl --port 2003 -l
```

構成ファイルの確認のみを行う:

```
gwctl -f myconf.conf -v
```

レルム内のすべてのエージェントゲートウェイへ構成ファイルをプッシュする (localhostを含む):

```
gwctl -f mytconf.conf
```

リモート接続の帯域幅管理の有効化/無効化

リモート接続の帯域幅管理は、次のいずれかの方法で有効または無効にする必要があります。

- ファイルの最初のエントリにenabledまたはdisabledのキーワードを含む帯域幅構成ファイルをプッシュします。各構成ファイルの最初の行に、帯域幅調整のステータスを示すenabledまたはdisabledが含まれている必要があります。
- コマンドラインでgwctl -eを使用して帯域幅管理を有効にするか、またはgwctl -dを使用して帯域幅管理を無効にします。帯域幅管理の有効または無効の状態は、バージョンのアップグレードなしに帯域幅管理構成ファイル内に残ります。

帯域幅構成の文法

帯域幅構成のCFG (EBNF形式):

```
config : ((queue | class | version | config_source | config_user | disabled |
comment)? '\n')\*
```

```
queue  : 'queue' queue_name 'bandwidth' d_number bandwidth_spec
('rtt' d_number)? ('parent' queue_name 'borrow')?
```

```
queue_name : "[a-zA-Z0-9_]+"
```

```
class  : 'class' pattern (',' pattern)* 'for' queue_name
```

```
pattern : ipv4 | ipv4_cidr
```

```
ipv4 : ipv4_address_pattern_element ('.' ipv4_address_pattern_element)@1:3
```

```
ipv4_cidr : d_number ('.' d_number)@1:3 '/' d_number
```

```
ipv4_address_pattern_element : single_number | range | range_class |
wildcard range_class : '[' (number ('-' number)? ',')+ ']'
```

```
wildcard : '*'
```

```
range : '[' number '-' number ']'
```

```
single_number : d_number
```

```
number : d_number
```

```
d_number : "[0-9]+"
```

```
x_number : "[a-fA-F0-9]+"
```

```
bandwidth_spec : "[GMK]?[bB]"
```

```
config_source : 'config-source' ':' "[a-zA-Z0-9.:\-]+"
```

```
config_user   : 'config-user' ':' "[a-zA-Z0-9_!@#$%^&*();.`~\-\\]+"
```

```
disabled : 'disabled'
```

```
comment  : '#' "[^\n]*"
```

SA管理対象サーバーのピアコンテンツキャッシュ

SAの以前のリリースでは、管理対象サーバーの数が少なく完全なSAコアインストールを必要としない小規模なサイトがある場合には、SAのサテライトインストールを使用しました。サテライトでは、ホストに最小限必要なコアコンポーネントのみをインストールでき、ホストからプライマリコアのデータベースとその他サービスにSAゲートウェイ接続経由でアクセスします。

SAで管理対象サーバーのピアコンテンツキャッシュが利用できるようになりました。この機能は、管理対象サーバー数が50未満のファシリティ向けにソフトウェアリポジトリのキャッシュ機能を提供します。サテライトコンポーネントは必要ありません。

管理対象サーバーのピアコンテンツキャッシュには、次のような利点があります。

- ピアキャッシュは既存のSA管理対象サーバーを使用(ハードウェアインフラストラクチャーを追加する必要なし)
- SAサテライトのインストールが必要ない
- SAゲートウェイが必要がない
- ピアキャッシュによってソフトウェアステージング中のWANトラフィックが抑制される
- ピアキャッシュでソフトウェアパッケージを事前にステージングできる
- リモートサイトにSAサテライトまたはゲートウェイが必要ない
- ソフトウェアをキャッシュに手動でロードできる

要件

管理対象サーバーのピアコンテンツキャッシュの要件は、次のとおりです。

- SA でサポートされるオペレーティングシステムが稼働する管理対象サーバーをピアキャッシュサーバーにする必要がある
- カスタムサーバー属性を使用して管理対象サーバーをピアキャッシュを使用するように構成する必要がある

ピアキャッシュのインストール

1. ピアキャッシュとして使用する管理対象サーバーを特定します。
2. 該当する管理対象サーバーのエージェントを SA 9.14 にアップグレードします (他の管理対象サーバーのエージェントをアップグレードする必要はありません)。

エージェントのアップグレードについては、『SAユーザーガイド: Server Automation』の付録「エージェントのインストールとアップグレードのユーティリティ」を参照してください。

ピアキャッシュとSAサーバーの構成

1. ブランチ/リモートサイトにある管理対象サーバーごとにカスタム属性を作成します。
   a. たとえば、`peer_cache_dvc_id = 240001`と指定します。`240001`はピアキャッシュとして使用するサーバーのデバイスIDです。
   b. ブランチ/リモートサイトがデバイスグループとしてモデル化されている場合は、スクリプトを使用してデバイスグループレベルでカスタム属性を適用できます。あとで管理対象サーバーをデバイスグループに追加すると、このカスタム属性が自動的に継承されます。
2. ピアキャッシュを使用するすべての管理対象サーバーがピアキャッシュと同じカスタマーに属するようにします。
3. (オプション) ピアキャッシュとして使用する管理対象サーバーに、次のカスタム属性を作成します。
   a. `peer_cache_size` = <メガバイト単位の値>

      デフォルト: 1TB (上限はファイルシステムサイズ)
   b. `peer_cache_path` = <ファイルストアの場所>

パスに指定する値に`sa_cache`が追加されます。たとえば、Windowsの場合のデフォルトは、次のようになります。

```
\Program Files\Common Files\Opsware\sa_cache
```

4. デフォルトで、管理対象サーバーはキャッシュのプライマリIPアドレスを使用してピアキャッシュに接続しようとします。カスタム属性を使用すると、次の形式で別のIPアドレスを指定することができます。

   `peer_cache_ip_field = < primary_ip | management_ip | ip:<addr>>`

   引数は次のとおりです。

   `primary_ip` - (デフォルト) 管理インタフェースのIPアドレス。これは、ローカルで構成されたIPアドレスです (NAT変換後のアドレスではありません)。

   `management_ip` - SA でサーバーと通信するのに使用するIPアドレス。これには、NAT変換後のアドレスを使用できます。

   `ip:<addr>` - IPアドレスを手動で設定する場合に使用 (例: `ip:192.168.2.1`)。

   管理対象サーバーでのプライマリIPアドレスおよびNATの構成の詳細については、『SAユーザーガイド: Server Automation』を参照してください。

ピアキャッシュが有効な場合の修復

『SAユーザーガイド: ソフトウェア管理』の手順で修復を開始します。

管理対象サーバーのピアコンテンツキャッシュが有効である場合、修復では次の手順が実行されます。

1. ステージングフェーズで、管理対象サーバーにキャッシュIPアドレスが付与されます (サーバーにアタッチされた`peer_cache_dvc_id`カスタム属性から導出)。
2. 管理対象サーバーによって、ブランチ/リモートサイトのピアキャッシュからパッケージがステージングされます (ピアキャッシュからのオブジェクトの取得 (155ページ) を参照)。

ピアキャッシュからのオブジェクトの取得

ピアキャッシュからオブジェクトを取得する際に、SAは次のタスクを実行します。

1. 管理対象サーバー上のステージングコードに、構成済みのピアキャッシュのIPアドレスが渡されます。
2. ステージングコードで、エージェントのSAセキュリティ証明書を使用して、ピアキャッシュサーバーのエージェントポートとセキュアに接続します。
3. ピアキャッシュで、接続元のクライアントがキャッシュを使用するように構成されていて、ピアキャッシュと同じカスタマーに属していることを確認します。
4. ピアキャッシュに指定したユニットをステージングするように要求します。
5. ピアキャッシュサーバーがユニットを送信して要求に応えます。
6. アクションフェーズで、オブジェクトのチェックサムをソフトウェアリポジトリ内の同じオブジェクトのチェックサムに対して検証します。

発生する可能性のあるエラー

手順1: 構成済みのブランチキャッシュが存在しないか、キャッシュエージェントと通信できない。

- ステージングがWAN経由で正常に行われます。

手順3: クライアントでピアキャッシュの使用が許可されていない。

a. キャッシュに許可されていない試行がログ記録されます。
b. キャッシュからクライアントに403 Forbiddenが返されます。
c. ステージングがWAN経由で正常に行われます。

手順5: キャッシュに要求されたオブジェクトが存在しない。

a. キャッシュからクライアントに503 (Retry-Later) が返されます。
b. キャッシュがソフトウェアリポジトリからWAN経由でオブジェクトを要求します。
c. 指定の時間後にクライアントがキャッシュを再試行してファイルを取得します。

手順5: キャッシュに要求されたユニットが存在するが、チェックサムがコアのチェックサムと一致しない。

a. SAで古いファイルとして処理され、キャッシュが一杯になったときに削除されます。
b. 手順5を続行します。

手順5: ソフトウェアリポジトリに要求されたオブジェクトが存在しない。

a. この状況は分析フェーズで捕捉されます。捕捉されない場合は、
b. キャッシュから404メッセージ (ファイルが見つかりません) が返されます。

ピアキャッシュステータスページの表示

1. 次のブラウザー証明書をインストールします:`browser.p12`

   `browser.p12`はスライスコンポーネントバンドルホストの

   `/var/opt/opsware/crypto/spin/`

   にあります。このファイルをローカルマシンにコピーし、お使いのブラウザーの証明書のインポート手順に従って、`browser.p12`をブラウザーにインポートします。

2. 次のURLを使用してWebブラウザーに表示します。

   `https://<peer_cache>:1002/oplets/peer_cache.py`

コンセプト:SAコア通信インフラストラクチャー

SAは、個々のコンポーネントがIPネットワークを介して相互にセキュアな通信を行う分散型コンピューティング環境です。SAでは、SSL/TLSおよびX.509証明書を使用してこれらのコンポーネント間の通信を保護します。

SAコアコンポーネントが他のコンポーネントと通信する必要がある場合は、Well-knownポートを使用してセキュアな(通常はSSL/TLSの)通信チャネルを開きます。SAの各コアコンポーネントには、SAのインストール時に生成されたパブリックキー証明書があります。コンポーネントは、他のコンポーネントに対して認証を行う際に、このパブリックキー証明書を使用します。ほとんどのプロセス間通信は強力に認証され(強力な暗号を使用して暗号化され)、完全性のチェックが行われます。

SAコア間の通信

複数のデータセンターでSAを実行する場合、SAはSAのすべての管理対象データセンター間でデータを自動的に同期します。大まかに、SAで同期されるデータは、サーバーのSAモデル(すべてのハードウェア、ソフトウェア、構成の属性情報を含む)とソフトウェアパッケージの2種類です。

- **SAモデルの複製:** SAは組み込まれた証明書付きメッセージングを使用して、SAモデルデータを同期します。SAはSSLを使用してメッセージバスを流れるメッセージを保護します。これらのメッセージでは、SAデータベース(モデルリポジトリ)に対するSQL変更を記述します。
- **ソフトウェアパッケージの複製:** SAはソフトウェアパッケージをオンデマンドで複製します。つまり、パッケージは必要なときにのみコピーされます。たとえば、ニュージャージーのデータセンターでサーバーを管理している管理者が、ニュージャージーのソフトウェアリポジトリ内に存在しないソフトウェアパッケージをインストールするようにSAに指示すると、SAは別のデータセンターからソフトウェアパッケージを要求します。

  実際のファイル転送には、オープンソースユーティリティ`rsync`を使用し、通信チャネルはSSHを使用して保護します。このプロセスは、サテライトの場合もピアキャッシュされたソフトウェアリポジトリの場合も同じです。

図33および図34は、2つのコアと1つのサテライトで、ゲートウェイを介してコアのコンポーネント間で通信する手順を示しています。

図33　　プライマリSAコア

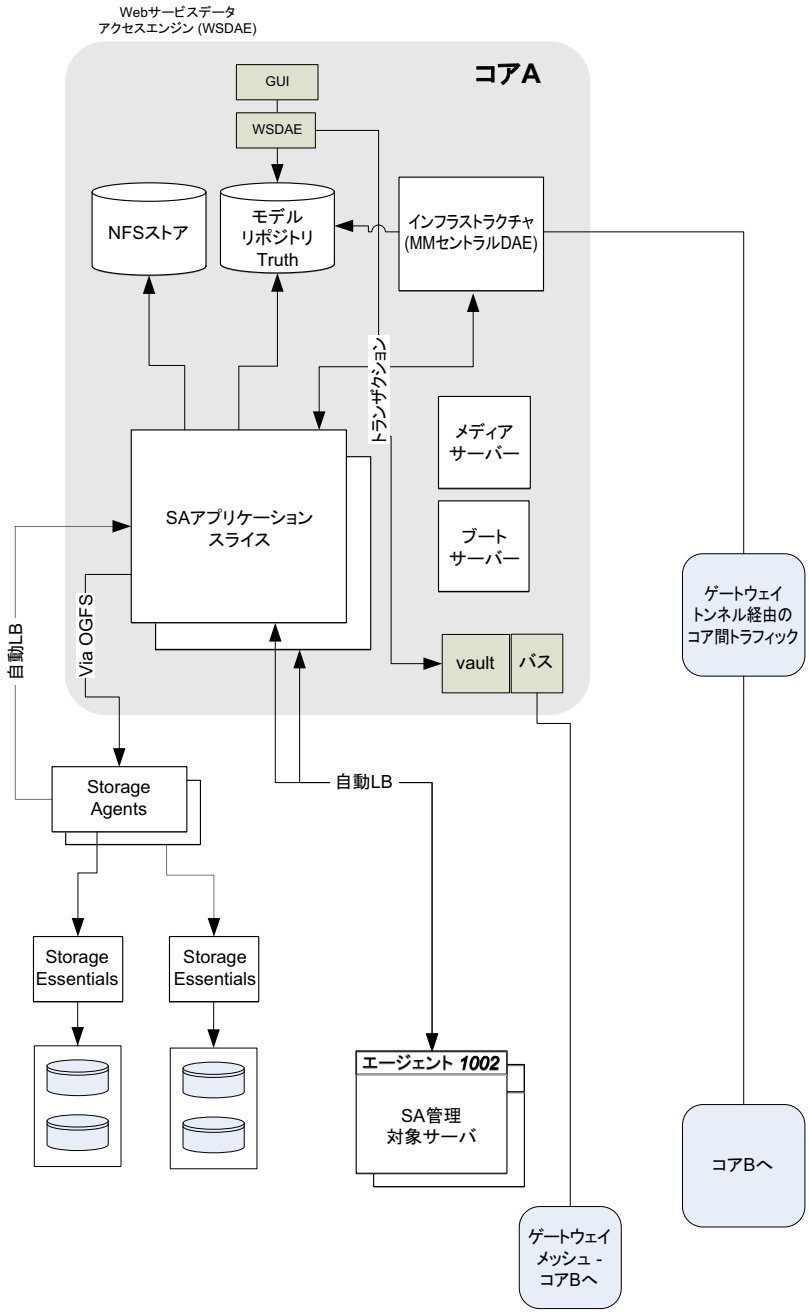
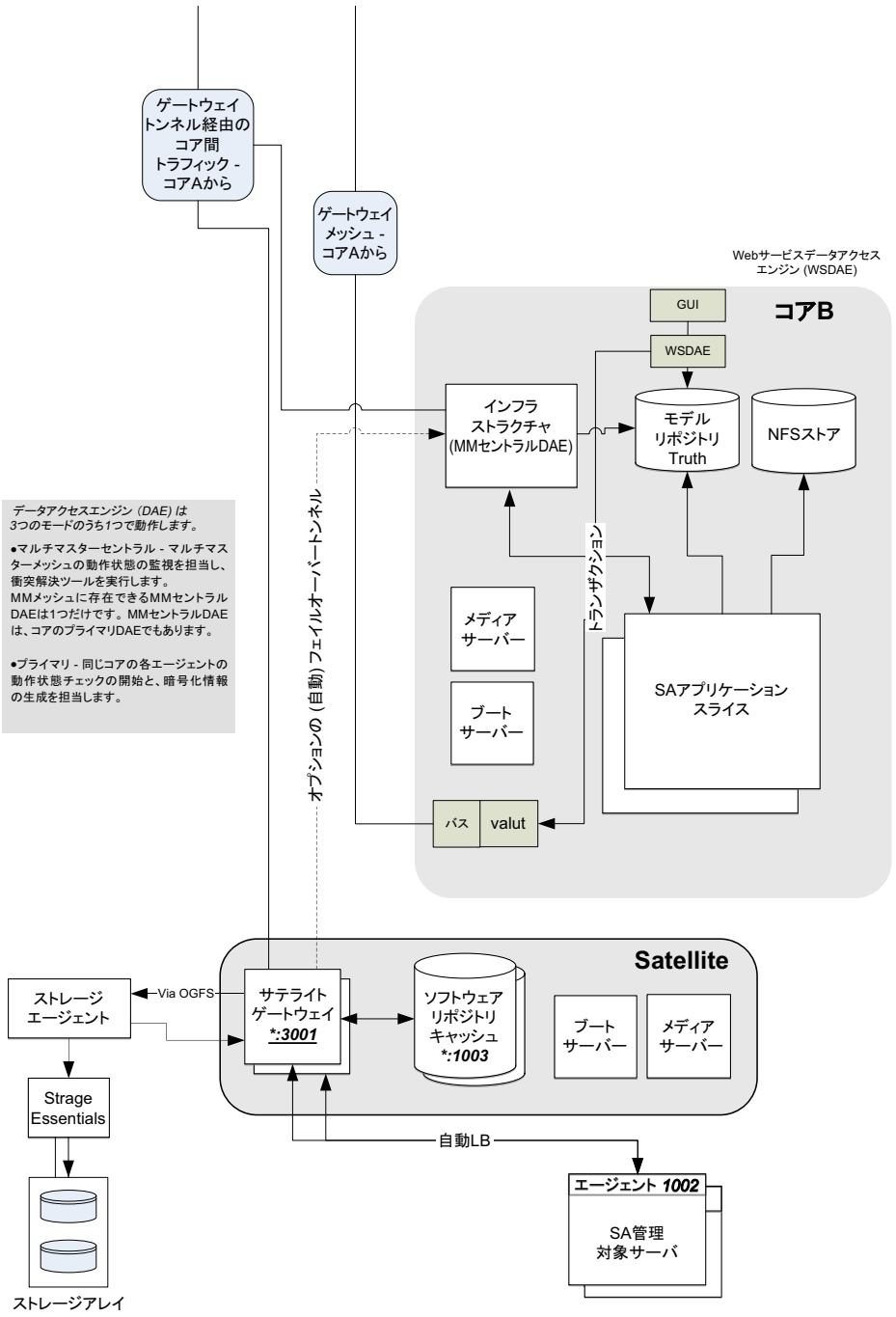


図34　　セカンダリコアとサテライト



詳細: エージェントとSAコアコンポーネントとの間の通信

管理対象サーバーのインストールされたSAエージェントは、認証済みの暗号化されたSSL/TLSトラフィックにも関与します。また、エージェントがサーバー上で管理タスクを実行するように指示を受けたときに、制御メッセージの一般的なフローによって、承認されたユーザーのみに該当のアクションを実行させることができます。このため、侵入者がエージェントに不正なタスクを実行させる有効なコマンドシーケンスを生成するのは非常に困難です。

次のシーケンスは、SAの一般的な管理タスク (SA管理対象サーバーでのソフトウェアのプロビジョニング) を表しています。管理対象サーバー上のその他の操作は、同じ一般的なプロトコルに従います。

1. データアクセスエンジンがHTTPSを介してSAエージェントと通信チャネルを開き、エージェントに管理タスクを実行するように指示します。
2. SAエージェントは、データアクセスエンジンにコールバックして、実行するタスクに関する詳細を取得します。通信チャネルを開始するには、エージェントはそれぞれのパブリックキー証明書を提示する必要があります。SA コアは証明書をマシンの IP に対応付ける内部データベースとエージェントのインストール時にSAで生成される一意のマシンIDと照らしあわせてパブリックキー証明書を確認します。このセキュリティ対策により、ユーザーがデジタル証明書と対応するキーを別のマシンにコピーしても、元の管理対象サーバーになりすますことはできません。

   通信チャネルが正常に開始されたら、SAエージェントはインストールおよび削除対象のソフトウェアのリスト (および実行するスクリプト、ソフトウェアインストールの順序、プロビジョニング時の再起動タイミング) を受け取ります。
3. SAエージェントはソフトウェアリポジトリに対する通信チャネルを (同様にHTTPSを介して) 開き、インストールに必要なソフトウェアのダウンロードを要求します。ソフトウェアリポジトリはダウンロードを開始する前に、ソフトウェアリポジトリで認識している秘密キーを使用してパッケージの SHA チェックサムを再計算します。SHA チェックサムがパッケージのアップロード時に生成されたチェックサムと一致する場合にのみ、SA エージェントは要求したソフトウェアを受け取ります。これも SA のセキュリティ対策の1つです。

   エージェントから非同期的にSAコアに対して要求を行うことで、進行状況レポートや長時間の操作をスケーラブルにサポートできます。これは、SAコアでエージェントの数多くの同期操作を直接管理する必要がないためです。SAゲートウェイインフラストラクチャーでは、単一方向の接続上で双方向トンネリングが利用できるため、SA は、ファイアウォールによってエージェントが TCP 接続を開始できないネットワーク環境でも、エージェントからコアへの非同期要求をサポートします。

エージェントとコアとの通信には、その他に次のような技術的特徴があります。

- 接続はSSL v3 で、X.509証明書により相互に認証されます (サーバーはクライアントの証明書をチェックし、クライアントはサーバーの証明書をチェックします)。
- コアおよびエージェントの証明書のプライベートキーは、root でのみ読み取り可能なファイル内に保管されます。
- 証明書はすべてインストール時に生成され、カスタマーが所有します。証明書がHPに知られることはありません。
- 証明書の有効期限はインストール後 10 年間です。SA には、証明書の有効期限が切れる前にコアおよびエージェントを再認定するための再認定ツールが用意されています。
- 証明書はSA内部の自己署名証明機関によって署名されます。Webブラウザーで HTTPS セキュリティの警告を回避するため、カスタマーはApacheのSAインスタンスに外部署名証明書をインストールすることができます。

この項では、SAゲートウェイで使用するゲートウェイプロパティファイルのパラメーターに関する参照情報について説明します。

SAゲートウェイプロパティファイルの構文

現在のホスト上のゲートウェイの動作や構成は、ゲートウェイプロパティファイル内のエントリで制御します。

SAゲートウェイプロパティファイルは、各コアホストの

`/var/opt/OPSWgw/gwname/opswgw.properties`

にあります。

SAゲートウェイプロパティファイルでは、次のエントリを指定できます。

これらのエントリを変更した場合に発生するコアへの影響がわからない場合は、これらのエントリを変更しないでください。

使用方法: `./opswgw-tc-70 [オプション]`

`--Gateway name`

(必須) SAゲートウェイの名前を設定します。この名前はゲートウェイメッシュ内で一意である必要があります。

`--Realm realm`

(必須) すべてのゲートウェイが指定したレルム内で動作します。レルムとはSAコンストラクトであり、レルム内のゲートウェイのサービス対象となる一連のサーバーを指します。レルムは他のレルムと重複する可能性のあるIPv4アドレス空間をサポートできます。また、レルムはSAの機能に対する帯域幅使用制限を定義する場合にも使用されます。

`--Root true | false`

このゲートウェイがゲートウェイメッシュのrootとして機能するように指定します。rootレルム内のすべてのゲートウェイがrootゲートウェイである必要があります。

デフォルト: false

`--Level int`

(試験段階) ゲートウェイのルーティングレベル。0～7の8つのレベルを指定できます。レルム内のすべてのゲートウェイを同じレベルにする必要があります。

デフォルト: 0

`--GWAddress lhost`

このゲートウェイで他のコンポーネントにゲートウェイへの接続方法を通知するのに使用するローカルホストアドレスを設定します (管理ゲートウェイ用に値を指定する場合は、IPアドレスのみを使用し、ホスト名は使用しません。その他の管理ゲートウェイ以外の場合は、ホスト名を使用できます)。この値はコアで新しいコア側ゲートウェイを検出するのに使用します。また、MIMEヘッダー`XOPSWGWLIST`を介して、レルムにサービスを提供しているゲートウェイのアクティブリストをプロキシクライアント (エージェントなど) に通知するのにも使用します。

`--Daemon true | false`

プロセスをデーモン化します。

デフォルト: false

--Watchdog true | false

内部ウォッチドッグプロセスを開始して、エラーまたはシグナルが発生した場合にゲートウェイを再開します。ウォッチドッグにSIGTERMが送信されると、ウォッチドッグプロセスとゲートウェイプロセスが停止します。

デフォルト: false

--User name

起動時にこのユーザーに変更します。

--RunDir path

起動時にこのディレクトリに変更します。

--ChangeRoot true | false

trueの場合、RunDirにルートディレクトリを変更します。これはヘルパースクリプトでjailを作成するのに使用できます。

デフォルト: false

--PreBind proto:ip:port, ...

セキュリティの理由から、権限のない用途でルートディレクトリを変更したゲートウェイの使用が役立つことがあります (リスナーには1024より上のポートのみを使用できます)。権限のないユーザーと権限を持つリスナーポートを使用する場合は、プロセスがrootの状態で権限が下がる前に、--PreBindを使用してポートを予約することができます。

--HardExitTimeout seconds

ハード終了を実行するまでのメインスレッドが内部スレッドとキューが静止するのを待機する再開または終了要求後の秒数。

--LogLevel INFO | DEBUG | TRACE

ログレベルを設定します。DEBUGやTRACEを指定した場合、大量の出力が生成されます。これらの出力は、通常、開発者が利用するものです。また、パフォーマンスに悪影響を与える可能性もあります。

デフォルト: INFO

--LogFile file

SAログファイルのファイル名。

--LogNum num

保持するローリングログファイルの数。

--LogSize size

各ログファイルのサイズ(バイト)。

--TunnelDst [lip1:]lport1[:crypto1],...

指定した場合、トンネルのターゲットリスナーを開始します。トンネルリスナーは複数のポート(スペースなしのカンマ区切りリスト)をリッスン対象にできます。ポートの前にIPアドレスを指定すると、リスナーはそのIPアドレスのみにバインドされます。例:2001, 10.0.0.2:2001, 2001:/var/foo.pem, 10.0.0.2:2001:/var/foo.pem

--TunnelSrc rhost1:rport1:cost1:bw1[:crypto1],...

指定した場合、このゲートウェイとrhost1:rport1でリッスンするゲートウェイとの間にトンネルを作成します。リンクcost1とリンク帯域幅bw1を設定する必要があります。コストは32ビット符号なしInt型で、帯域幅はKビット/秒(K=1024ビット)単位です(追加のトンネルはカンマで区切ります)。例:gw.foo.com:2001:1:0, gw.bar.com:2001:10:256:/var/foo.pem

--ProxyPort [lip1:]lport1,[lip2:]lport2,...

HTTP CONNECTプロキシリスナーポート。複数のプロキシリスナーポートが必要な場合は、カンマ区切りリストを使用します。IPアドレスをポートの前に付けると、インタフェースバインドを有効にすることができます。

--ForwardTCP [lip1:]lport1:realm1:rhost1:rport1,...

静的TCPポートフォワードを作成します。ローカルポートlport(x)をrealm(x)にあるリモートサービスrhost(x):rport(x)にフォワードします。realmを指定しない場合(lport::rhost:rportなど)、最も近いrootレルムにルーティングされます。

--ForwardTLS [lip1:]lport1:realm1:rhost1:rport1, ...

TLSトラフィックに特化した静的TCPポートフォワードを作成します。TLSセッションIDを解析して、負荷分散アルゴリズムで使用する出力ゲートウェイに送信します。それ以外の動作は、ForwardTCPと似ています。

--ForwardUDP [lip1:]lport1:realm1:rhost1:rport1,...

静的UDPポートフォワードを作成します。ローカルポートlport(x)をrealm(x)にあるリモートサービスrhost(x):rport(x)にフォワードします。realmを指定しない場合(lport::rhost:rportなど)、最も近いrootレルムにルーティングされます。(注:DHCPなどの一部のUDPサービスは、この方法でプロキシできません。)

--IdentPort [lip:]lport

ローカルポートlport(オプションでローカルIP lipにバインド)をリッスン対象とするIDENTサービスを開始します。

--AdminPort [lip:]lport[:crypto1]

ローカルポートlport(オプションでローカルIP lipにバインド)をリッスン対象とする管理インタフェースを開始します。cryptoを使用する場合は、crypto仕様ファイル名をインクルードします。

--ConnectionLimit int

最大接続数に対するソフトメモリチューニング制限を指定します。

--OpenTimeout seconds

リモート接続を確立するリモートCONNECT要求で、待機する最大秒数(seconds)を指定します。

--ConnectTimeout seconds

connect()の完了を待機する最大秒数(seconds)を指定します。タイムアウトが発生すると、HTTP 503メッセージが入力ゲートウェイ経由でクライアントに返されます。ConnectTimeoutとゲートウェイメッシュの中継遅延の合計がOpenTimeoutよりも短い場合、クライアントはこのメッセージを受け取ります。

--ReorderTimeout seconds

(TCPフローの)メッセージの順番に不整合が生じた場合に、再アセンブリに必要なメッセージの到着を待機する時間(seconds)を制限します。一般的に、メッセージの順番の不整合は、中継トンネルにエラーが発生した場合やフロー途中でルートが変更された場合に起こります。

--TunnelStreamPacketTimeout seconds

TCPフローの一部がエンドポイントに届かない場合に、TCP接続を破棄する秒数(seconds)を指定します。

--QueueWaitTimeout seconds

内部ルーティングキューの先頭で、トンネルの復元の待機時にトンネルメッセージが待機できる時間を指定します。

--KeepAliveRate seconds

各リンクでリンクのkeepaliveメッセージをx秒ごとに送信します。

--LsaPublishRateMultiple float

リンクステートアドバタイズ(LSA)をk*M秒に1回発行します。Mはメッシュ内のゲートウェイの数で、kは--LsaPublishRateMultipleで指定された浮動小数点定数です。たとえば、メッシュ内の100個もゲートウェイが存在し、--LsaPublishRateMultipleが2.0に設定されている場合、LSAは約200秒ごとに発行されます(実装上の要因により、時実際は190〜210の間になります)。

--LsaTTLMultiple float

LSAのTTLをfloatにLsaPublishRateを乗じた値に設定します。例: LsaPublishRateが10秒でLsaTTLMultipleが3の場合、このゲートウェイで発行されるLSAのTTLは30秒に設定されます。

--MaxRouteAge seconds

指定した秒数(seconds)内に更新されなかったルーティングテーブルのルートを破棄します。

--RouteRecalcDutyCycle percentage

ダイクストラの計算にtau秒を要する場合、
tau*(1/RouteRecalcDutyCycle-1)秒待機してから、もう一度再計算を行います。

--TunnelTimeoutMultiple float

この値にKeepAliveRateを乗じたものが、ガベージコレクションを行わずにトンネルをアイドル状態にできる最大時間になります。

--DoNotRouteService host1:port1,host2:port2,...

ローカルクライアントでhost:portとのプロキシ接続が構成された場合に、メッセージをルーティングせずに、ローカルで処理するように指定します。このプロパティは、特定のサービスをゲートウェイの現在のレルム内でローカルに処理する場合に使用します。

--ForceRouteService host1:port1:realm1,host2:port2:realm2,...

ローカルクライアントでhost:portとのプロキシ接続が構成された場合に、メッセージを指定したレルムに強制的にルーティングします。

--HijackService host1:port1,host2:port2,...

ローカルゲートウェイでトンネルを介したhost:portとの接続が確認され、ソースレルムがローカルレルムでない場合、ゲートウェイはこの接続を処理する必要があります。ローカルレルムから接続されている場合は、メッセージをそのままその宛先に送ります。この機能を使用すると、透過的なキャッシュを実装できます。

--RouteMessages *true | false

trueに指定すると、中継ルーティングがオンになります。falseの場合、中継ルーティングは無効になります。メッセージの宛先がローカルゲートウェイでない場合、デフォルトで、メッセージは現在のルーティングテーブルに基づいてルーティングされます。このようなルーティングを希望しない場合は、このプロパティをfalseに設定します。

--EgressFilter proto:dsthost1:dstport1:srchost1:srcrealm1,...

ローカルゲートウェイでsrchost1:srcrealm1からdsthost:dstportへのTCP接続が確認された場合、ゲートウェイはこの接続を許可する必要があります。何も指定しない場合、すべての接続が拒否されます。出力フィルターですべての接続を許可する場合は、*:*:*:*:* と指定します。また、出力フィルターで、rootレルムからの接続のみを許可するのも一般的です。これを指定するには、srcrealmを空欄にします。例: tcp:10.0.0.5:22:172.16.0.5: と指定すると、rootレルムの172.16.0.5から10.0.0.5 (ポート22) へのTCP接続が許可されます。

--IngressMap ip1:name,ip2:name,...

オープンメッセージの送信時に (srcipが入力マップ内にある場合に)、ip:nameのマッピングをオープンメッセージに (メタデータとして) 追加します。これにより、リモートの出力フィルターで、ipの代わりにnameをsrchostとして使用することができます。この機能はファームへのサーバーの追加をサポートします。EgressFilterの数多くのエントリにサーバーを個別に追加する必要はありません。

--LoadBalanceRule proto:thost:tport:mode:rhost1:rport1:
rhost2:rport2, ...

thost:tportの新規接続メッセージの受信時に、rhost1:rport1、rhost2:rport2などの実際のホストで接続を負荷分散します。負荷分散方式はmodeで定義します。

次の6つの負荷分散モードがあります。

STICKY: ソースIPとソースレルムのハッシュでランダム化された優先リストに基づいて、接続を有効なターゲットに送ります (ハッシュ文字列は入力MIMEヘッダーX-OPSW-LBSOURCEでオーバーライドできます)。

LC: 接続数の最も少ない有効なターゲットに接続を送ります。

RR: ラウンドロビン方式で接続を次の有効なターゲットに送ります。

TLS_STICKY: SSLv3/TLSv1.0のセッションIDを使用して、セッションIDキャッシュに基づいて前のターゲットに接続を戻します。ターゲットがエラー状態か、セッションIDがキャッシュに存在しない場合は、STICKYモードにフォールバックして選択し直します。

TLS_LC: TLS_STICKYモードと似ていますが、LCモード (最小接続数) にフォールバックします。

TLS_RR: TLS_STICKY モードと似ていますが、RR モード (ラウンドロビン) にフォールバックします。proto:thost:tportの出力フィルターは必ず追加してください。ターゲットの出力フィルターを追加する必要はありません。UDPサービスでは、TLS以外の負荷分散モードを使用できます。

--LoadBalanceRetryWindow seconds

負荷分散ターゲット (上記のrhost1:rport1) の使用時にエラーが発生した場合、ターゲットはinerrorとマークされます。このプロパティでは、再試行を行うまでゲートウェイで待機する秒数を制御します。ターゲットが見つからない場合 (接続要求時にRSTを受信した場合など)、ロードバランサーは適切なターゲットを見つけようとします。

--SessionIdTimeout seconds

負荷分散されたSSLv3/TLSクライアントをアイドル状態にすることを許容するsessionIdの関連付けを削除するまでの秒数。このプロパティはTLSフローの出力ゲートウェイに影響します。

--SessionIdCacheLimit slots

キャッシュで保持できるSSLv3/TLSのセッションIDの数に関するソフト制限。この制限を超えると、--SessionIdCacheLimitで指定されたキャッシュ制限を達成するため、ガベージコレクターによってSessionIdTimeoutの値の削減が開始されます。

--MinIdleTime seconds

過負荷状態のときに、接続を削除対象とみなす前にアイドル状態を許容する最小秒数(seconds)を指定します。

--GCOverloadTrigger float

過負荷保護を開始するSoftConnectionLimitを指定します。開いている接続数がこの過負荷トリガーポイントに到達すると、過負荷保護が開始されて、MinIdleTimeの間にアイドル状態の長かった接続が削除されます。過負荷保護は接続数が過負荷トリガーポイントを下回ったときに停止されます。

--GCCloseOverload true | false

このプロパティでは、ConnectionLimitの到達後にクライアントが接続を開始しようとしたときの、ゲートウェイで新規接続の処理方法を指定します。trueの場合、ゲートウェイは新規接続を終了します。falseの場合、ゲートウェイは新規接続をカーネルのバックログに入れて、過負荷状態が収まった後に処理します。適切な設定はアプリケーションによって異なります。

デフォルト: false.

--VerifyRate seconds

接続で指定された秒数(seconds)の間データの移動が止まったときに、接続が開いていることを確認するため、メッセージがリモートゲートウェイに送信されていることを確認します。タイムアウトの期限が切れている場合、このチェックは定期的にいつまでも繰り返し実行されます。

--OutputQueueSize slots

トンネル出力キューのサイズを指定します。これらのキューには、リモートゲートウェイ宛のメッセージが格納されます。リモートゲートウェイには1つずつ出力キューがあります。MaxQueueIdleTimeに到達すると、キューのガベージコレクションが行われます。

--MaxQueueIdleTime seconds

ガベージコレクションを行う前にアイドル状態の出力キューを維持する最大時間を指定します。

--TunnelManagementQueueSize slots

LSAなど、トンネル管理トラフィックの管理に使用するキューのサイズを指定します。

--TunnelTCPBuffer bytes

TCP SENDおよびRECVバッファーのサイズをバイト単位で指定します。指定した値に対応するようにオペレーティングシステムを構成する必要があります。オペレーティングシステムで指定内容が拒否されているかどうかを確認するには、ゲートウェイのログファイルを参照します。

--DefaultChunkSize bytes

TCPストリームをカプセル化する際のデフォルトの(最大)I/Oチャンクサイズを指定します。このプロパティ値は帯域幅制約のないリンクのみに適用できます。

--LinkSaturationTime seconds

リンクに帯域幅制約がある場合に、2つのパラメーターに基づいてチャンクサイズ(DefaultChunkSize)を計算します。1つ目のパラメーターはリンクの帯域幅制約です。2つ目のパラメーターは、帯域幅シェーパーがリンク上で実際にフル帯域幅を使用する時間です。このパラメーターは帯域幅シェーパーのデューティサイクルを制御します。値を小さくするほど帯域幅の制御はスムーズになりますが、I/Oチャンクごとにヘッダーが含まれるためオーバーヘッドは増大します。

--TunnelPreLoad slots

最初のAckメッセージを待機するまでに使用する出力キュースロットの最大数を指定します。これにより、Long Fat Pipeでのパイプライン処理が可能になります。キュースロット数が少なくなると、この値は幾何学的に小さくなって1になります。

--BandwidthAveWindow samples

帯域幅予測移動ウィンドウのI/Oレートサンプルの最大数を指定します。このウィンドウ内のサンプル数を平均して、トンネルで使用中の帯域幅のローパス予測を提供します。この予測には、フィルターウィンドウの鋭いエッジによる高周波数成分が含まれます。

--BandwidthFilterPole float

予測移動ウィンドウの高周波数成分の除去に使用する離散時間一次平滑化フィルターの極を指定します。このフィルターをオフにする場合は、0.0を設定します。

--StyleSheet URL

管理UIを表示する際にURLへのスタイルシートリンクを追加します。これは管理UIを別のWebベースUIに埋め込む場合に便利です。このプロパティを使用してデフォルトスタイルシートを制御するだけでなく、管理UIのURLに変数StyleSheet=<url>/style.cssを追加して動的スタイルシートのオーバーライドをサポートすることもできます。

--ValidatePeerCN true | false

トンネルのハンドシェーク時にピア構成に対してピアCNを検証するかどうかを指定します。信頼されていないゲートウェイのインストール時には、ピアをオフにする必要があります

デフォルト: true

--PropertiesCache file

トンネル接続でのparametermodifyメッセージを介してリンクコストと帯域幅を制御できます。これらのリアルタイムの調整は実行中のプロセスに対して実行されて、パラメーターキャッシュに書き込まれます。これにより、プロパティファイルやコマンドライン引数がオーバーライドされます。

--PropertiesInclude file

ロードして現在のプロパティとマージするインクルードファイルを指定します。インクルードファイル内のプロパティは、元のプロパティファイルのプロパティをオーバーライドできます。このプロパティはコマンドラインから指定できます。その場合は、すべてのプロパティがオーバーライドされます(コマンドラインオーバーライドを含む)。このプロパティは再帰的ではありません。また、リストをサポートしません。

--PropertiesFile file

すべてのコマンドライン引数をopswgw名前空間内でプロパティファイルに配置します。ただし、PropertiesFileコマンドライン引数自体をopswgw名前空間内でプロパティファイルに配置することはできません。

opswgwのコマンドライン引数

前の項のパラメーターはすべて、opswgwコマンドのオプションとして指定できます。たとえば、ゲートウェイプロパティファイルのopswgw.Gateway fooエントリは、次のコマンドライン引数に相当します。

```
/opt/opsware/opswgw/bin/opswgw --Gateway foo
```

コマンドライン引数は、ゲートウェイプロパティファイルの対応するエントリをオーバーライドします。前の項に列挙したエントリの他に、opswgwコマンドでは、次のようにゲートウェイプロパティファイルを引数として指定することもできます。

```
/opt/opsware/opswgw/bin/opswgw --PropertiesFile filename
```

第6章 SAのメンテナンス

SAの開始/停止スクリプト

SAには、次の多目的スクリプトが用意されています。このスクリプトでは、SAの開始、停止、ステータスの取得を行うことができます。

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

このスクリプトを使用すると、サーバーにインストールされたすべてのSAコンポーネントの表示、すべてのコアコンポーネントの開始、停止、再開、特定のSAコンポーネント (Oracleデータベース以外) の開始、停止、再開を行うことができます。

Oracleデータベースの開始および停止については、Oracleデータベース (モデルリポジトリ) の開始 (171ページ) を参照してください。

コアコンポーネントのホスト上でスクリプトを実行すると、スクリプトはローカルシステムにインストールされた各コンポーネントの前提条件チェックを実行します。

➤ SAコアのコンポーネントが複数のサーバーに分散している場合、開始/停止スクリプトでリモートのサーバーと直接やり取りして、リモートのサーバーに存在するコンポーネントを開始または停止することはできません。ただし、ローカルで依存関係のあるコンポーネントを開始する前に、リモートのサーバーに接続して前提条件に適合するかどうかを確認することはできます。

開始/停止スクリプトでは、リモートのサーバーで稼働するコンポーネントの前提条件をチェックする際に、サーバー間でのブート時間や速度の違いに対応するため、タイムアウト値を使用します。いずれかの前提条件のチェックに失敗した場合、スクリプトはエラーとなって終了します。

開始/停止スクリプトによる依存関係チェック

開始/停止スクリプトは、SAコンポーネントの依存関係を認識して、SAのコンポーネントを正しい順序で開始します。スクリプトの前提条件チェックでは、特定のコンポーネントを開始する前に、依存関係が満たされていることを確認します。このため、複数のサーバーにインストールされたSAのコンポーネントを正しい順序で開始することができます。

たとえば、開始しようとしているコンポーネントで実行中の別のコンポーネントが必要である場合、スクリプトで次の内容を確認できます。

- 必要なコンポーネントのホスト名が解決可能かどうか
- 必要なコンポーネントが実行されているホストが所定のポートをリッスン対象としているかどうか

開始/停止スクリプトのログ

開始/停止スクリプトは、次のログに書き込みます。

表23　開始/停止スクリプトのログ記録

ログ	注
/var/log/opsware/startup	サーバーの起動時に、スクリプトはローカルシステムにインストールされたすべてのSAコンポーネントの開始プロセスに関するすべてのテキスト (stdoutに送信されるすべてのテキスト) をログ記録します。
stdout	コマンドラインから呼び出したときに、スクリプトはコンポーネントの開始プロセスに関するすべてのテキストを表示します。
syslog	サーバーの起動時に、スクリプトはバックグラウンドプロセスとして実行され、システムイベントロガーにステータスメッセージを送信します。

開始/停止スクリプトの構文

SAの開始/停止スクリプトの構文は、次のとおりです。

```
/etc/init.d/opsware-sas [オプション] [コンポーネント1] [コンポーネント2]...
```

特定のコンポーネントの開始、停止、または再開を指定する場合、該当するコンポーネントがローカルシステムにインストールされている必要があります。また、listで表示される名前を正確に指定する必要があります。表24に、SAの開始/停止スクリプトのオプションを示します。同様にopsware-sasで起動する正常性チェックモニター (HCM) のオプションについては、表28を参照してください。

表24　SAの開始/停止スクリプトのオプション

オプション	説明
list	ローカルシステムにインストールされているスクリプトの管理対象のすべてのコンポーネントを表示します。コンポーネントは開始される順序で表示されます。
start	ローカルシステムにインストールされているすべてのコンポーネントを正しい順序で開始します。startオプションを使用して特定のコンポーネントを開始する場合、スクリプトは必要な前提条件をチェックしてからコンポーネントを開始します。 startオプションでOracleデータベース (モデルリポジトリ) を開始することはできません。Oracleデータベースは、SAのコンポーネントを開始する前に起動しておく必要があります。 Webサービスデータアクセスエンジン (twist) などの一部のSAコンポーネントは、開始するのに時間を要する場合があります。これらのコンポーネントでは、スクリプトがバックグラウンドプロセスとしてローカルシステム上で実行され、対応するログファイルにエラーや失敗したチェックがログ記録されるように、startオプションを使用してスクリプトを実行できます。 **注:** startオプションを使用してサーバー上にインストールされた複数のコンポーネントを開始する場合、スクリプトでは常にstartsyncオプションを使用して/etc/init.d/opsware-sasコマンドが実行されます。
startsync	startsyncオプションは、ローカルシステムにインストールされたすべてのコンポーネントを同期モードで開始します。 startsyncオプションを使用する場合、スクリプトはフォアグラウンドで実行され、進行状況に関するサマリーメッセージをstdoutに対して表示します。

表24　SAの開始/停止スクリプトのオプション（続き）

オプション	説明
restart	ローカルシステムにインストールされたすべてのコンポーネントを同期モードで停止して開始します。スクリプトはすべてのローカルコンポーネントを逆の順序で停止し、続いて、startsyncオプションを実行して正しい順序でコンポーネントを再開します。
stop	ローカルシステムにインストールされているすべてのコンポーネントを正しい順序で停止します。 このオプションでOracleデータベースを停止することはできません。

Oracleデータベース (モデルリポジトリ) の開始

SA の開始 / 停止スクリプトで Oracle データベース (モデルリポジトリに必要) を開始することはできません。Oracleデータベースは、SAのコンポーネントを開始する前に起動しておく必要があります。SAのコンポーネントを開始する前に、次のコマンドを入力してOracleリスナーとデータベースを開始する必要があります。

```
/etc/init.d/opsware-oracle start
```

スタンドアロンSAコアの開始

単一のサーバーにインストールされているコアを開始するには、次の手順を実行します。

1. rootとしてコアサーバーにログインします。
2. 次のコマンドでモデルリポジトリのOracleリスナーとデータベースを開始します。

   ```
   /etc/init.d/opsware-oracle start
   ```

3. 次のコマンドですべてのコアコンポーネントを開始します。

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

マルチサーバー SAコアの開始

SAコアの開始順序は、いくつかの要因に左右されます。この項では、マルチマスターメッシュ構成でのSAコアの開始について説明します。

コアコンポーネントホストの電源がオンになっている場合

メッシュ全体が停止していて、ホストの電源がオンになっている場合は、最初にプライマリコアを開始した後に各セカンダリコアを開始します。セカンダリコアは1つずつ開始する必要があります。

次の手順を実行します。

プライマリコア

1. 必要な場合は、コアのコンポーネントをホストしているサーバーを特定します。rootとしてモデルリポジトリホストにログインし、次のコマンドを実行します。

   ```
   /etc/init.d/opsware-sas list
   ```

2. root としてプライマリコアのモデルリポジトリホストにログインして、Oracle リスナーとデータベースを開始します。

   ```
   /etc/init.d/opsware-oracle start
   ```

3 データベースとリスナーが正常に開始されたら、次のコアコンポーネントホストで SA 開始スクリプトを、各サーバーごとに次の順序で実行します。

- インフラストラクチャーコンポーネントバンドルホスト
- スライスコンポーネントバンドル(最初のスライス) - インフラストラクチャーコンポーネントバンドルと同じホストにインストールされていない場合
- 後続のスライスコンポーネントバンドルホスト
- OSプロビジョニングコンポーネントバンドルホスト
- コアに関連するサテライトホスト

次のコマンドを使用して、各ホストでSA開始スクリプトを実行します。

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

開始スクリプトでは、各ホストですべてのコアコンポーネントを正常に開始した後に、次のサーバーでコマンドを実行する必要があります。

セカンダリコア

開始順序は上記と同様ですが、プライマリコアコンポーネントを正常に開始してから実行する必要があります。また、セカンダリコアでのコアコンポーネントの開始は、1つのコアごとに実行する必要があります。

コアコンポーネントホストの電源がオフになっている場合

コアコンポーネントホストの電源がオフになっている場合、ホストの電源をオンにすると、SAが開始されます。そのため、次の順序でホストの電源をオンにする必要があります。

- インフラストラクチャーコンポーネントバンドルホスト
- スライスコンポーネントバンドル (スライス0) - インフラストラクチャーコンポーネントバンドルと同じホストにインストールされていない場合
- 追加のスライスコンポーネントバンドルホスト (スライス1～スライスn) - 1つずつ
- OSプロビジョニングコンポーネントバンドルホスト
- コアに関連するサテライトホスト - 1つずつ

ホストの電源は1つずつオンにして、SAコアコンポーネントが正常に開始した後に、次のサーバーの電源をオンにする必要があります。`/var/opt/opsware/log/startup`にある一番新しいログファイルに対してtailコマンドを使用すると、各ホストのコンポーネントの開始ステータスを確認できます。

個別のSAコアコンポーネントの開始

1つまたは複数のコンポーネントを開始するように指定することができます。ただし、コンポーネントはローカルシステム上で実行されている必要があります。`opsware-sas`コマンドの`list`オプションで表示されるコンポーネント名を正確に指定する必要があります。

SAコアの個別のコンポーネントを開始するには、次の手順を実行します。

1 開始対象のコンポーネントが存在するサーバーに`root`としてログインします。

2 (オプション) サーバーにインストールされているSAコンポーネントを表示するには、次のコマンドを入力します。

```
/etc/init.d/opsware-sas list
```

3 次のコマンドを入力します。`component`は`list`オプションで表示される名前です。

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

たとえば、listオプションでbuildmgrが表示された場合は、次のコマンドを入力して、OS Provisioning Build Managerを開始します。

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

代わりに、サーバー上でコンポーネントを開始する際にstartsyncオプションを指定することもできます。startsyncオプションについては、この章の表24 (170ページ) を参照してください。

個別のSAコアコンポーネントの開始順序

SAの開始スクリプトでは、ホスト上にインストールされたコアコンポーネントを以下の順序で開始します。スクリプトでホスト上にインストールされたコンポーネントを停止する際には、開始したときと逆の順序で停止します。

1. opswgw-mgw: SAのプライマリコアマスターゲートウェイ
2. opswgw-cgws0-<ファシリティ>: コアが実行されているファシリティのコア側ゲートウェイ
3. opswgw-cgws: メッシュ内のその他のゲートウェイ
4. vaultdaemon: モデルリポジトリマルチマスターコンポーネント
5. dhcpd: OSプロビジョニング機能のコンポーネント
6. pxe: PXEブート環境
7. memcached: メモリ内のキャッシュレイヤーであり、ソフトウェアリポジトリアクセレーター (tsunami) コンポーネントと連携して、LinuxベースのSAコアと直接通信するエージェントでの修復と拡張性を向上します。
8. spin: データアクセスエンジン
9. mm_wordbot: ソフトウェアリポジトリのコンポーネント
10. tsunami: ソフトウェアリポジトリアクセレーターはオブジェクトストアのダウンロードアクセラレーターであり、LinuxベースのSAコアと直接通信するエージェントの修復パフォーマンスと拡張性を向上させます。
11. waybot: コマンドエンジン
12. smb: OSプロビジョニング機能のコンポーネント
13. twist: Webサービスデータアクセスエンジン
14. buildmgr: OS Provisioning Build Manager
15. opswgw-agw0-<ファシリティ>: コアが実行されているファシリティのエージェント側ゲートウェイ
16. opswgw-agws: エージェントゲートウェイ
17. hub: Global File Systemのコンポーネント
18. sshd: Global File Systemのコンポーネント
19. apxproxy: 自動化プラットフォーム拡張 (APX) プロキシ
20. spoke: Global File Systemのコンポーネント
21. agentcache: Global File Systemのコンポーネント
22. occ.server: SA Webクライアントのコンポーネント
23. httpsProxy: SA Webクライアントのコンポーネント
24. da: アプリケーションデプロイメントコンポーネント
25. opsware-agent: サーバーエージェント

ホストが複数あるSAコアの停止

メッシュをシャットダウンする際には、開始したときと逆の順序で各コアを停止し、開始したときと逆の順序でコア内の各ホストの電源をオフにする必要があります。セカンダリコアを1つずつシャットダウンした後に、最後にプライマリコアをシャットダウンします。

各コア(プライマリまたはセカンダリ)内では、/etc/init.d/opsware-sas stopを次の順序で実行する必要があります。

- コアに関連するサテライトホスト - 1つずつ
- OSプロビジョニングコンポーネントバンドルホスト
- 追加のスライスコンポーネントバンドルホスト(スライス1～スライスn) - 1つずつ
- スライスコンポーネントバンドル(スライス0) - インフラストラクチャーコンポーネントバンドルと同じホストにインストールされていない場合
- インフラストラクチャーコンポーネントバンドルホスト
- データベース/モデルリポジトリホスト

ホスト上のコアコンポーネントを停止するには、次のコマンドを実行します。

```
/etc/init.d/opsware-oracle stop
```

複数のデータアクセスエンジン

ここでは、次の内容について説明します。

複数のデータアクセスエンジンの概要

複数のデータアクセスエンジンインスタンスを含むコアでは、次のいずれかの方法で各インスタンスを指定することができます。

- プライマリデータアクセスエンジン: 各ファシリティ内のプライマリデータアクセスエンジンは1つだけです。データアクセスエンジンは管理対象サーバーを定期的にチェックして、SAがこれらの管理対象サーバーと通信できることを確認します。ファシリティ内に複数のデータアクセスエンジンがあると、到達可能性チェックが競合して相互に干渉する可能性があります。
- セカンダリデータアクセスエンジン: ファシリティに複数のデータアクセスエンジンがインストールされている場合(スケーラビリティを確保するため)、プライマリデータアクセスエンジン以外はセカンダリデータアクセスエンジンとして指定されます。最初にインストールされたデータアクセスエンジンは、プライマリまたはマルチマスターセントラルのデータアクセスエンジンに指定されます。セカンダリデータアクセスエンジンは、管理対象サーバーをチェックして到達可能かどうかを確認しません。データの読み取りまたは書き込みを行うためにモデルリポジトリと通信するだけです。
- マルチマスターセントラルデータアクセスエンジン: SAのマルチマスターメッシュには複数のコアが存在し、そのため、複数のデータアクセスエンジンが存在します。1つのコアのプライマリデータアクセスエンジンを、マルチマスターセントラルデータアクセスエンジンに指定する必要があります。これらのコアのいずれにも複数のデータアクセスエンジンが存在する可能性がありますが、メッシュでセントラルデータアクセスエンジンにできるのは1つだけです。

データアクセスエンジンのセカンダリへの再割り当て

追加のデータアクセスエンジンをインストールした場合は、次の手順を実行して、新しいデータアクセスエンジンをセカンダリに再割り当てする必要があります。

1. SAの管理者グループに属するユーザーとしてSAクライアントにログインします。SAクライアントのホームページが表示されます。
2. ナビゲーションパネルで、**[Administration]** > **[Opsware Software]** をクリックします。**[Software]** ページが表示されます。
3. **[spin]** リンクをクリックします。**[Opsware Software | spin]** ページが表示されます。
4. **[Members]** タブを選択します。データアクセスエンジンをホストしている管理対象サーバーのリストが表示されます。
5. **[additional Data Access Engine server]** のチェックボックスを選択します。
6. **[Tasks]** メニューから、**[Re-Assign Node]** を選択します。
7. **[Service Levels | Opsware | spin node]** のオプションを選択します。
8. **[Select]** をクリックします。
9. 次のノードをクリックして、ノードの階層構造を移動します。
   - Opsware
   - spin
   - Secondary
10. **[Re-Assign]** をクリックします。
11. ターミナルウィンドウで、`root`として追加のデータアクセスエンジンを実行しているサーバーにログインし、次のコマンドを入力してデータアクセスエンジンを再開します。

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

マルチマスターセントラルデータアクセスエンジン

マルチマスターセントラルデータアクセスエンジンは、HP BSAインストーラーによって自動的に割り当てられます。

⚠ ほとんどの場合、インストール後にマルチマスターセントラルデータアクセスエンジンを変更することはできません。インストール後にマルチマスターセントラルデータアクセスエンジンを変更すると、SAコアを新規バージョンにアップグレードする際に問題が発生する可能性があります。この項の手順を実行する前に、HPプロフェッショナルサービスまでご連絡ください。

マルチマスターセントラルデータアクセスエンジンを指定するには、次の手順を実行します。

1. SAのSystem Administratorsグループに属するユーザーとしてSAクライアントにログインします。
2. ナビゲーションパネルの [Administration] で、**[Opsware Software]** をクリックします。**[Opsware Software]** ページが表示されます。
3. **[spin]** リンクをクリックします。
4. **[Servers]** タブを選択します。
5. 新しいコアのデータアクセスエンジンサーバーのチェックボックスを選択します。
6. **[Server]** メニューから、**[Re-Assign Node]** を選択します。
7. **[Service Levels | Opsware | spin | node]** のオプションを選択します。
8. **[Select]** をクリックします。

9 次の各ノードをクリックして、ノードの階層構造を移動します: **Opsware | Spin | Multimaster Central**

10 **[Re-Assign]** をクリックします。

11 マルチマスターセントラルデータアクセスエンジンを再開します。

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

監査結果とスナップショットの削除のスケジュール設定

監査結果とスナップショット (スナップショット仕様の結果) は時間の経過とともに増え続ける可能性があるため (特に定期的なスケジュールで実行される場合)、指定した日数後に監査結果とスナップショットをコアから削除するようにSAコアを構成することができます。

この設定は、アーカイブされていない監査結果とスナップショットのみに適用されることに注意してください。アーカイブされた結果は、SAクライアントから手動で削除する必要があります。

また、次の 2 つの場合には、削除のスケジュール設定を行っても、監査結果やスナップショットは削除されません。

- スナップショットが監査のターゲットとして使用されている場合
- 監査結果またはスナップショットが監査またはスナップショット仕様の唯一の結果である場合　スナップショット仕様

監査結果とスナップショットの削除の構成手順:

1 SAクライアントで **[管理]** タブを選択します。

2 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。

3 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。

4 次のシステム構成パラメーターを変更します。

- `spin.cronbot.delete_audits.cleanup_days` パラメーターを見つけて、新しい値を直接入力するか、新しい値ボタン を選択して、アーカイブされていない監査結果をすべて削除するまでの経過日数を入力します。**[デフォルト値]** を選択すると、監査は削除されません。
- `spin.cronbot.delete_snapshots.cleanup_day`パラメーターを見つけて、新しい値を直接入力するか、新しい値ボタン を選択して、アーカイブされていないスナップショットをすべて削除するまでの経過日数を入力します。**[デフォルト値]** を選択すると、スナップショットは削除されません。

5 [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。

Webサービスデータアクセスエンジンの構成パラメーター

この項では、SAクライアントを使用するか、または構成ファイルを編集して、Webサービスデータアクセスエンジンのシステム構成パラメーターを変更する手順について説明します。

システム構成パラメーターの変更後に、Webサービスデータアクセスエンジンを再開する必要があります。

システム構成パラメーターの変更

この項では、SAクライアントでシステム構成パラメーターの一部を変更する手順について説明します。その他のパラメーターを変更するには、Webサービスデータアクセスエンジンの構成ファイル (177ページ) の手順に従って構成ファイルを編集する必要があります。

SAクライアントでWebサービスデータアクセスエンジンのシステム構成パラメーターを変更するには、次の手順を実行します。

1. SAクライアントで [**管理**] タブを選択します。
2. ナビゲーションパネルで [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。
3. SAコンポーネントのリストで、[Webサービス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。
4. 変更対象のシステム構成パラメーターを特定して、パラメーターを変更します。
5. [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。
6. 次のコマンドを使用して、Webサービスデータアクセスエンジンを再開します。

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

Webサービスデータアクセスエンジンの構成ファイル

Webサービスデータアクセスエンジンの構成ファイルには、SA Webサービス API 2.2のサーバー側に作用するプロパティが含まれます (これらのプロパティはSAクライアントで表示されません)。構成ファイルの完全修飾名は、次のとおりです。

```
/etc/opt/opsware/twist/twist.conf
```

SAのアップグレード時に、`twist.conf`ファイルは置き換えられますが、`twist_custom.conf`ファイルはそのまま維持されます。SAの新規バージョンにアップグレードする際に、構成設定を維持するには、`twist_custom.conf`ファイルを編集する必要があります。`twist.conf`で指定したプロパティは、`twist_custom.conf`のプロパティでオーバーライドされます。UNIXの`twist`ユーザーは、`twist_custom.conf`ファイルに対する書き込みアクセスが必要です。

構成ファイルで定義されたプロパティの変更手順:

1. テキストエディターで`twist.conf`ファイルを編集します。
2. 変更したファイルを保存します。
3. Webサービスデータアクセスエンジンを再開します。

`twist.conf`ファイルの変更は、管理者グループに属するユーザー (admin) が行う必要があります。ファイルの変更が済んだら、Webサービスデータアクセスエンジンを再開して変更内容を適用する必要があります。

次の表に、SA WebサービスAPI 2.2に作用する構成ファイルのプロパティを示します。これらのプロパティの一部は、サーバーイベントのキャッシュ (スライディングウィンドウ) に関連しています。SAには、SAオブジェクトへの変更を記述したイベントのスライディングウィンドウ (デフォルトサイズは2時間) があります。このウィンドウにより、ソフトウェア開発者はすべてのオブジェクトを取得することなく、オブジェクトのクライアント側キャッシュを更新することができます。詳細については、EventCacheServiceに関するAPIドキュメントを参照してください。

表25　　SA WebサービスAPI 2.2の構成ファイル

プロパティ	デフォルト	説明
twist.webservices.debug.level	1	サーバー側でのSA Webサービス APIのデバッグレベルを設定する整数値。次の値を指定できます。 0 - 基本情報 1 - より詳細な情報 2 - スタックトレース 3 - キャッシュに追加されたアイテムが存在する場合に、サーバーイベントキャッシュのエントリを出力する
twist.webservices.locale.country	US	ローカライザーユーティリティの各国設定パラメーター。現在はUSコードのみをサポートしています。
twist.webservices.locale.language	en	ローカライザーユーティリティの言語設定パラメーターを設定します。現在はenコードのみをサポートしています。
twist.webservices.caching.windowsize	120	サーバーイベントキャッシュを維持するスライディングウィンドウのサイズ (分単位)。
twist.webservices.caching.windowslide	15	サーバーイベントキャッシュを維持するウィンドウのスライディング範囲 (分単位)。
twist.webservices.caching.safetybuffer	5	サーバーイベントキャッシュを維持するスライディングウィンドウの安全バッファー (分単位)。
twist.webservices.caching.minwindowsize	30	サーバーイベントキャッシュを維持するスライディングウィンドウの最小サイズ (分単位)。
twist.webservices.caching.maxwindowsize	240	サーバーイベントキャッシュを維持するスライディングウィンドウの最大サイズ (分単位)。

Webサービスデータアクセスエンジンの最大ヒープメモリー割り当て量の増強

マルチマスターメッシュのデータサイズが大きくなると、Webサービスデータアクセスエンジン (twist) の最大ヒープメモリー割り当て量の増強が必要になる場合があります。デフォルト値は1280Mbです。そのためには、次のタスクを実行します。

1　テキストエディターを使用して、次のファイルを開きます。

/etc/opt/opsware/twist/twist_custom.conf

2　次のエントリを必要な割り当て量に変更します。

twist.mxMem=<メモリーサイズ>

ここで、メモリーサイズは-Xmx<メモリーサイズ>に対応します。

たとえば、

```
twist.mxMem=2048m
```

と指定すると、Webサービスデータアクセスエンジンに最大2048メガバイトのヒープメモリーが割り当てられます。アップグレードを行った後でも、この変更は維持されます。この`twist_custom.conf`のパラメーターを空欄にすると、`twist.sh`で指定されたデフォルト値(1280m)が使用されます。

ソフトウェアリポジトリミラーリングパラメーターの変更

ソフトウェアリポジトリミラーリングとは、マルチマスターメッシュ内にあるソフトウェアリポジトリを同期することにより、冗長性と災害復旧に備える機能です。この項では、ソフトウェアリポジトリミラーリングの構成パラメーターを変更する手順について説明します。詳細については、ソフトウェアリポジトリの監視(190ページ)を参照してください。

システム構成パラメーターの変更

この項では、SAクライアントでシステム構成パラメーターを変更する手順について説明します。パラメーターを変更するには、次の手順を実行します。

1. SAクライアントで[**管理**]タブを選択します。
2. ナビゲーションパネルで[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。
3. SAコンポーネントのリストで、[ソフトウェアリポジトリ]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。
4. 変更対象のシステム構成パラメーターを特定して、パラメーターを変更します。
5. [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。
6. SAコアのソフトウェアリポジトリのすべてのインスタンスを再開します。グローバルに変更を行う場合は、マルチマスターメッシュ内のすべてのコアのすべてのソフトウェアリポジトリインスタンスを再開します。

ソフトウェアリポジトリミラーリングの構成パラメーター

ソフトウェアリポジトリミラーリングを有効にして、ミラーリングジョブの実行頻度を設定するには、次の構成パラメーターを変更します。ソフトウェアリポジトリのミラーリングジョブでは、リポジトリ間でデータをコピーして、すべてのリポジトリを同期します。詳細については、ソフトウェアリポジトリの監視(190ページ)を参照してください。

表26　　ソフトウェアリポジトリミラーリングのパラメーター

パラメーター	タイプ	指定できる値	デフォルト	説明
word.enable_content_mirroring	ブール値のフラグ	0または1	0	ソフトウェアリポジトリミラーリングを有効にする場合は、この値を1に設定します。無効にする場合は、この値を0に設定します。
word.mirror_job_period	分	任意の正の整数	60	ソフトウェアリポジトリのミラーリングジョブを実行する頻度を指定します。

第7章 SAコアコンポーネントの監視

SAの監視の概要

SAでは、SAクライアントでシステム診断テストを行って、次のSAコンポーネントの機能を診断することができます。

- データアクセスエンジン
- ソフトウェアリポジトリ
- コマンドエンジン
- Webサービスデータアクセスエンジン
- マルチマスターインフラストラクチャーコンポーネント（SAのドキュメントではモデルリポジトリマルチマスターコンポーネントという）

この項では、上記のコンポーネントに関する基本的な監視について説明します。また、SAの以下の追加コンポーネントについても説明します。

- サーバーエージェント
- エージェントキャッシュ
- SAクライアント
- モデルリポジトリ
- Spoke
- ゲートウェイ
- OS Build Manager
- OSブートサーバー
- OSメディアサーバー

この情報は、SAクライアントが実行できないためにシステム診断テストが使用できない場合や、管理対象の環境で自動監視が設定されている場合に使用します。その場合には、これらのコマンドを使用して、システム診断の自動化とSAの監視を行います。

この監視には、次の内容が含まれます。

- 特定のコンポーネントプロセスが実行中であることを確認するコマンドと、期待される出力の例
- コンポーネントやオペレーティングシステムで提供されるコマンド
- コンポーネント固有のポート、ログ、管理用URL

このドキュメントで紹介するコマンドは、1行にまとめて入力する必要があります。ただし、コマンドや出力結果を読みやすくするため、コマンドが次の行に続いていることがわかるように、スペース、空白行、改行、バックスラッシュ (\) を使用してコマンドを出力結果を変更している場合があります。また、このドキュメントに示した出力は例です。実際の出力はそれぞれのサーバーによって異なります。

このドキュメントで扱うSAの各コンポーネントについては、『SA概要とアーキテクチャーガイド』を参照してください。

エージェントの監視

サーバーエージェントは、SAの管理対象の各サーバーで実行中のソフトウェアモジュールです。管理対象サーバーへの変更が必要な場合は、サーバーエージェントから要求が行われます。

サーバーエージェントの詳細については、『SAユーザーガイド: Server Automation』を参照してください。

SAクライアントを使用して、管理対象サーバー上で実行されているサーバーエージェントとSAコアの通信をテストする場合は、『SAユーザーガイド: Server Automation』の次の各項を参照してください。

- エージェントの到達可能性通信テスト
- 通信テストのトラブルシューティング

エージェントのポート

サーバーエージェントはポート1002を使用します。

エージェントのプロセスの監視

Windowsの場合、[スタート] メニューから [ファイル名を指定して実行] を選択します。[ファイル名を指定して実行] ダイアログで、`taskmgr`と入力します。Windowsタスクマネージャーで、[プロセス] タブをクリックして`watchdog.exe`と`python.exe`というプロセスを確認します。

UNIX (Solaris、Linux、AIX、HP-UX) の場合、サーバーエージェントには実行中のプロセスが2つ存在します。

Solarisの場合、次のコマンドを実行します。

```
# ps -flg `awk -F= '($1=="pgrp") {print $2}' /var/opt/opsware/agent/
daemonbot.pid`
```

このコマンドを実行すると、次のような出力が生成されます。

```
F S  UID  PID  PPID  C  PRI NI  ADDR  SZ  WCHAN  STIME  TTY  TIME  CMD
                        8 S  root 9541 9539  0  41  20  ?    1768 ?     Aug
                        08  ?    1:23 /opt
                     /opsware/agent/bin/python /opt/opsware/agent/pylibs/shadowbot/
                     daemonbot.pyc --conf /etc/opt/opsware/agent/agent.args
8 S  root  9539   1  0  99  20  ?    398  ?     Aug 08  ?    0:00 /opt
                     /opsware/agent/bin/python /opt/opsware/agent/pylibs/shadowbot/
                     daemonbot.pyc --conf /etc/opt/opsware/agent/agent.args
```

Linuxの場合、次のコマンドを実行します。

```
# ps -flg `awk -F= '($1=="pgrp") {print $2}' /var/opt/opsware/agent/
daemonbot.pid`
```

このコマンドを実行すると、次のような出力が生成されます。

```
F S  UID  PID  PPID  C  PRI NI  ADDR  SZ  WCHAN  STIME  TTY  TIME  CMD
1 S  root 2538 1     0  85  0   -    3184 wait4  Sep11  ?    0:00:00
                     /opt/opsware/agent/bin/python /opt/opsware/agent/pylibs/shadowbot/
                     daemonbot.pyc --conf /etc/opt/opsware/agent/agent.args
5 S  root 2539 2538  0  75  0   -   30890 schedu Sep11  ?    0:02:56
```

```
                    /opt/opsware/agent/bin/python /opt/opsware/agent/pylibs/shadowbot/
                    daemonbot.pyc --conf /etc/opt/opsware/agent/agent.args
```

監視デーモンはPPIDが1のプロセスです。もう一方はサーバーまたは監視スレッドです。

AIXの場合、次のコマンドを実行します。

```
# ps -flg `awk -F= '($1=="pgrp") {print $2}' /var/opt/opsware/agent/
daemonbot.pid`
```

このコマンドを実行すると、次のような出力が生成されます。

```
F    S UID  PID  PPID  C  PRI NI  ADDR  SZ  WCHAN  STIME  TTY  TIME  CMD
40001 A root 110600 168026 0 60 20 2000d018 16208 * Sep 05 -   7:15 /opt/
                    opsware/agent/bin/python /opt/opsware/agent/pylibs/shadowbot/
                    daemonbot.pyc --conf /etc/opt/opsware/agent/agent.args
40001 A root 168026 1  0  60 20 2000f25c 1352       Sep 05 -   0:02 /opt/
                    opsware/agent/bin/python /opt/opsware/agent/pylibs/shadowbot/
                    daemonbot.pyc --conf /etc/opt/opsware/agent/agent.args
```

HP-UXの場合、次のコマンドを実行します。

```
# ps -flg `awk -F= '($1=="pgrp") {print $2}' /var/opt/opsware/agent/
daemonbot.pid`
```

このコマンドを実行すると、次のような出力が生成されます。

```
F  S  UID  PID  PPID  C  PRI  NI     ADDR  SZ  WCHAN  STIME TTY TIME COMD
1  R root 10009  1    0  152 20 437eb1c0 266      - Sep 22  ? 0:00 /opt/
                    opsware/agent/bin/python /opt/opsware/agent/pylibs/shadowbot/
                    daemonbot.pyc --conf /etc/opt/opsware/agent/agent.args
1  R root 10010 10009 0  152 20 434fb440 2190    - Sep 22  ? 3:29 /opt/
                    opsware/agent/bin/python /opt/opsware/agent/pylibs/shadowbot/
                    daemonbot.pyc --conf /etc/opt/opsware/agent/agent.args
```

エージェントのURL

https://<ホスト名>:1002

エージェントのログ

サーバーエージェントでは、次のログファイルが管理対象サーバー上に作成されます。

Windowsの場合:

- %ProgramFiles%Common Files\opsware\log\agent\agent.log*
- %ProgramFiles%Common Files\opsware\log\agent\agent.err*

UNIXの場合:

- /var/log/opsware/agent/agent.log*
- /var/log/opsware/agent/agent.err*

UNIXログでの監視に使用する条件:

- 「Traceback」を含む文字列
- 「OpswareError」を含む文字列

エージェントキャッシュの監視

エージェントキャッシュは、エージェントデプロイメントプロセスでサーバーエージェントのインストールファイルを提供するコンポーネントです。エージェントキャッシュコンポーネントは、SAエージェントの最新バージョンをキャッシュします。SAでは、管理対象のサーバーにエージェントをインストールする際に、エージェントキャッシュコンポーネントからエージェントインストールバイナリファイルを取得します。

エージェントキャッシュのポート

エージェントキャッシュはポート8081を使用します。

エージェントキャッシュのプロセスの監視

いずれの構成でも、エージェントキャッシュコンポーネントには実行中のプロセスが1つ存在します。

Solarisまたは**Linux**の場合、(SAコアおよびサテライトの) ゲートウェイを実行しているサーバーで次のコマンドを実行します。

```
# ps auxwww | grep -v grep | grep agentcache
```

このコマンドを実行すると、次のような出力が生成されます。

```
root  22288  0.5  0.1  15920  4464  ? S  19:55  0:08  /opt/opsware/bin/
                    python /opt/opsware/agentcache/AgentCache.pyc -d /var/opt/opsware/
                    agent_installers -p 8081 -b
```

エージェントキャッシュのログ

エージェントキャッシュのログは、次のファイルにあります。

- /var/log/opsware/agentcache/agentcache.log
- /var/log/opsware/agentcache/agentcache.err

これらのログでの監視に使用する条件:

- 「Error downloading agent (エージェントのダウンロード中にエラーが発生しました)」を含む文字列
- 「Another process is listening on port (別のプロセスがポートをリッスンしています)」を含む文字列

コマンドセンターの監視

コマンドセンターは、SAに対するWebベースのユーザーインタフェースです。コマンドセンターには、SAクライアントを使用してアクセスします。

SAユーザーはApache HTTPSプロキシ経由でコマンドセンターコンポーネントに接続します (Apache HTTPSプロキシはHP BSAインストーラーでコマンドセンターコンポーネントとともにインストールされます)。

コマンドセンターのポート

HTTPSプロキシはポート443 (HTTPS) とポート80を使用し、接続をコマンドセンターコンポーネントへ転送します。コマンドセンターコンポーネントは、ポート1031 (Webサービスポート) を使用します。

コマンドセンターのプロセスの監視

Linuxの場合、コマンドセンターコンポーネントを実行しているサーバーで、次のコマンドを実行します。

```
# ps -eaf | grep -v grep | grep java | grep occ
```

このコマンドを実行すると、次のような出力が生成されます。

```
occ  17373  1  6  19:46  ? 00:02:35  /opt/opsware/j2sdk1.4.2_10/bin/
        java -server -Xms256m -Xmx384m -XX:NewRatio=3 -Docc.home=/opt/opsware/
        occ -Docc.cfg.dir=/etc/opt/opsware/occ -Dopsware.deploy.urls=,/opt/
        opsware/occ/deploy/ -Djboss.server.name=occ -Djboss.server.home.dir=/
        opt/opsware/occ/occ -Djboss.server.
```

コマンドセンターコンポーネントを監視する場合、URLクエリ (Wgetなどのツールを使用) をコマンドセンターのURLに送信する自動監視プロセスを設定することもできます。コマンドセンターコンポーネントのログインページが返されると、Apache HTTPSプロキシとコマンドセンターの両方のプロセスが正常に機能していると判断できます。

コマンドセンターのURL

`https://occ.<データセンター>`

コマンドセンターのログ

コマンドセンターは専用のログを生成せず、JBossサーバーを使用して次のログファイルにログを書き込みます。

- `/var/log/opsware/occ/server.log*`
- `/var/log/opsware/httpsProxy/*log*`

これらのログでの監視に使用する条件:

- `java.net.ConnectionException`
- `java.net.SocketException`
- `java.lang.NullPointerException`

負荷分散ゲートウェイの監視

負荷分散ゲートウェイは、高可用性とSAコア内での水平方向の拡張を実現します。

負荷分散ゲートウェイは、HP BSAインストーラーを実行したときに、コマンドセンターコンポーネントとともにインストールされます。

負荷分散ゲートウェイのポート

デフォルトで、負荷分散ゲートウェイはポート8080を使用します。

負荷分散ゲートウェイのプロセスの監視

いずれの構成でも、負荷分散ゲートウェイコンポーネントには実行中のプロセスが2つ存在します(ゲートウェイプロセスとウォッチドッグプロセス)。

SolarisまたはLinuxの場合、コマンドセンターコンポーネントを実行しているサーバーで、次のコマンドを実行します。

```
# ps -eaf | grep -v grep | grep opswgw | grep lb
```

このコマンドを実行すると、次のような出力が生成されます。

```
root  32149  1  0  Sep27  ? 00:00:00  [opswgw-watchdog-2.1.1: lb]
                    --PropertiesFile /etc/opt/opsware/opswgw-lb/opswgw.properties
                    --BinPath /opt/opsware/opswgw/bin/opswgw
root  32156  32149  0  Sep27  ? 00:24:31  [opswgw-gateway-2.1.1: lb]
                    --PropertiesFile /etc/opt/opsware/opswgw-lb/opswgw.properties
                    --BinPath /opt/opsware/opswgw/bin/opswgw --Child true
```

負荷分散ゲートウェイのログ

負荷分散ゲートウェイのログは、次のファイルにあります。

- `/var/log/opsware/gateway-name/opswgw.log*`

これらのログでの監視に使用する条件:

- 「ERROR」を含む文字列
- 「FATAL」を含む文字列(プロセスが終了することを示す)

データアクセスエンジンの監視

データアクセスエンジンにより、コマンドセンター、システムデータ収集、サーバー上の監視エージェントなど、各種クライアントとの連携が容易になります。

データアクセスエンジンのポート

データアクセスエンジンはポート1004(HTTPS)を外部で使用し、同じサーバーにインストールされたSAコンポーネント用にポート1007(ループバックインタフェース)を使用します。

マルチマスターセントラルデータアクセスエンジンのポートフォワード

メッシュ内のマルチマスターセントラルデータアクセスエンジンとメッシュ内の他のSAコアのモデルリポジトリとの間のSQLnetトラフィックは、SAゲートウェイメッシュを介してルーティングされます。

マルチマスターセントラルデータアクセスエンジンを実行しているサーバー上の`tnsnames.ora`ファイルでは、他のSAコア内のコア側ゲートウェイの指定されたポートをポイントします。マルチマスターセントラルデータアクセスエンジンを実行しているコア内のコア側ゲートウェイは、他の各コア内のコア側ゲートウェイに接続をフォワードします。さらに、接続がフォワードされたコア側ゲートウェイはそのコアのモデルリポジトリに接続をフォワードします。

コア側ゲートウェイのポート番号は、20000 + データセンターIDとして算出されます。たとえば、マルチマスターメッシュにファシリティA(ファシリティID 1)とファシリティB(ファシリティID 2)という2つのファシリティが存在する場合、ファシリティAにあるマルチマスターセントラルデータアクセスエンジンは、ファシリティBにあるモデルリポジトリにアクセスするために、ゲートウェイを実行しているサーバーのポート20002に接続します。

マルチマスターセントラルデータアクセスエンジンについては、複数のデータアクセスエンジン (174ページ)を参照してください。

ゲートウェイメッシュのトポロジについては、『SA概要とアーキテクチャーガイド』を参照してください。

データアクセスエンジンのプロセスの監視

Linuxの場合、データアクセスエンジンコンポーネントを実行しているサーバーで、次のコマンドを実行します。

```
# ps auxwww | grep -v grep | grep spin | grep -v java
```

このコマンドを実行すると、次のような出力が生成されます。

```
root  30202  0.0  0.0  13592  1500  ? S  Sep11 0:01  /opt/opsware/bin/
                    python /opt/opsware/pylibs/shadowbot/daemonbot.pyc --conf /etc/opt/
                    opsware/spin/spin.args
root  30204  1.3  0.6  154928  25316  ? S  Sep11  411:15  /opt/opsware/
                    bin/python /opt/opsware/pylibs/shadowbot/daemonbot.pyc
                    --conf /etc/opt/opsware/spin/spin.args
root  30256  0.1  0.3  28500  13024  ? S  Sep11  50:35  /opt/opsware/
                    bin/python /opt/opsware/spin/certgenmain.pyc --start
                    --conf /etc/opt/opsware/spin/spin.args
```

データアクセスエンジンのURL

- `https://spin.<データセンター>:1004`

  データアクセスエンジン(spin)のUIにアクセスするには、ブラウザー証明書`browser.p12`が必要です。

  `browser.p12`はスライスコンポーネントバンドルホストの

  `/var/opt/opsware/crypto/spin/`

  にあります。このファイルをローカルマシンにコピーし、お使いのブラウザーの証明書のインポート手順に従って、browser.p12をブラウザーにインポートします。

- `https://spin.<データセンター>:1004/ObjectBrowser.py?cls=Account&id=0`

  モデルリポジトリコンポーネントが実行されていない場合、このURLへのアクセスは失敗します。

- `https://spin.<データセンター>:1004/sys/dbstatus.py`

  このURLにアクセスすると、データベース接続ステータスがHTMLページに表示されます。それぞれの自動監視システムで正規表現を使用すると、アクティブなデータベース接続の数を抽出できます。

データアクセスエンジンのログ

データアクセスエンジンのログは、次のファイルにあります。

- /var/log/opsware/spin/spin.err* (データアクセスエンジンのメインのエラーファイル)
- /var/log/opsware/spin/spin.log* (データアクセスエンジンのメインのログファイル)
- /var/log/opsware/spin/spin_db.log
- /var/log/opsware/spin/daemonbot.out (アプリケーションサーバーからの出力)

1つのコアに複数のデータアクセスエンジンがある場合、データアクセスエンジンを実行している各サーバーに、これらのログファイルが一組ずつ存在します。

Webサービスデータアクセスエンジンの監視

Webサービスデータアクセスエンジンは、他のSAコンポーネントのパフォーマンスを向上させます。

Webサービスデータアクセスエンジンコンポーネントは、スライスコンポーネントバンドルの一部としてインストールされます。

Webサービスデータアクセスエンジンのポート

Webサービスデータアクセスエンジンはポート1032を使用します。

コマンドセンターコンポーネントは、ポート1026 (プライベートループバックポート) でWebサービスデータアクセスエンジンと通信します。

Webサービスデータアクセスエンジンのプロセスの監視

Linuxの場合、コマンドセンターコンポーネントを実行しているサーバーとスライスコンポーネントバンドルを実行しているサーバーで、次のコマンドを実行します。

```
# ps auxwww | grep -v grep | grep \/opt\/opsware\/twist
```

このコマンドを実行すると、次のような出力が生成されます。

```
twist  4039  0.2  11.3  2058528  458816  ? S  Sep11  80:51 /opt/opsware/
                    j2sdk1.4.2_10/bin/java -server -Xms256m -Xmx1280m -XX:MaxPermSize=192m
                    -Dorg.apache.commons.logging.Log=org.apache.commons.logging.impl.Jdk14
                    Logger ......
twist  4704  0.0  0.0  4236  1124  ? S  Sep11  1:28  /bin/sh /opt/
                    opsware/twist/watchdog.sh start 60'
twist  4743  0.0  0.6  376224  27160  ? S  Sep11  18:31 /opt/opsware/
                    j2sdk1.4.2_10/bin/java -server -Xms16m -Xmx128m -Dtwist.port=1026
                    ...... -classpath /opt/opsware/j2sdk1.4.2_10/jre/......
```

Webサービスデータアクセスエンジンのログ

Webサービスデータアクセスエンジンのログは、次のファイルにあります。

- /var/log/opsware/twist/stdout.log*
- /var/log/opsware/twist/twist.log
- /var/log/opsware/twist/access.log
- /var/log/opsware/twist/server.log* (アプリケーションレベルのログ)
- /var/log/opsware/twist/boot.log
- /var/log/opsware/twist/watchdog.log

stdout.logファイルにはstdoutとstderrが保管され、System.out.println()、System.err.println()、e.printStackTrace() のメッセージの出力がログ記録されます。ただし、これらのログには一部の例外も含まれます。ファイルの数と各ファイルのサイズは、twist.conf で構成できます。指定した最大ファイルサイズに到達すると、ログが追加で作成されます。stdout.logが最新で、stdout.log.1からstdout.log.5の順に古くなります。ファイルはスタートアップ時にもローテーションされます。

twist.logファイルには、Weblogic固有のメッセージとWeblogicレベルの例外が保管されます。これらのファイルはスタートアップ時にローテーションされます。Webサービスデータアクセスエンジン (Twist) コンポーネントが正常に開始しなかったことを示す例外については、twist.logファイルを監視します。モデルリポジトリ (Truth) 接続のセットアップ時にエラーが発生すると、エラーがtwist.logにログ記録され、次のようなエラーメッセージが生成されます。

```
####<Oct 14, 2006 1:37:43 AM UTC> <Error> <JDBC> <localhost.localdomain> <twist> <main> <<WLS
Kernel>> <> <BEA-001150> <Connection Pool "TruthPool" deployment failed with the following error:
<Specific message, such as Oracle error codes and tracebacks>
```

access.logファイルには、共通のログ形式でアクセス情報が保管されます。これらのファイルはサイズが5MBに達するとローテーションされます。

server.logファイルには、Webサービスデータアクセスエンジンから生成されたアプリケーションレベルの例外とデバッグメッセージが保管されます。server.logファイルには、モデルリポジトリ (Truth) の接続設定の問題に起因するエラーも保管されます。デバッグメッセージは、パッケージで設定したログレベルまたはtwist.confファイルのクラスレベルで制御されます。ファイルの数と各ファイルのサイズはいずれも、twist.confで構成できます。server.log.0は常に最新のファイルで、server.log.9が最も古いファイルです。

boot.logファイルには、Webサービスデータアクセスエンジンの開始時に生成されるstdoutメッセージとstderrメッセージに関する情報が保管されます。また、boot.logファイルには、Kill –QUITコマンドの出力も保管されます。

watchdog.logファイルは、Webサービスデータアクセスエンジンのステータスを1分ごとに記録します。

Webサービスデータアクセスエンジンの URL

https://occ.<データセンター>:1032

コマンドエンジンの監視

コマンドエンジンは、サーバーエージェントなどの分散型プログラムを複数のサーバーで実行するための手段です。コマンドエンジンスクリプトはPythonで記述され、コマンドエンジンサーバーで実行されます。コマンドエンジンスクリプトでは、サーバーエージェントにコマンドを発行することができます。これらの要求は安全に配信され、モデルリポジトリに保存されているデータを使用して監査できます。

コマンドエンジンのポート

コマンドエンジンはポート1018を使用します。

コマンドエンジンのプロセスの監視

Linuxの場合、コマンドエンジンコンポーネントを実行しているサーバーで、次のコマンドを実行します。

```
# ps auxwww | egrep '(COMMAND$|waybot)' | grep -v grep
```

このコマンドを実行すると、次のような出力が生成されます。

```
USER  PID  %CPU  %MEM  VSZ  RSS  TTY  STAT  START  TIME  COMMAND
root  412  0.0   0.0 13600 1472   ?   S    Sep11   0:00  /opt/opsware/
                    bin/python /opt/opsware/pylibs/shadowbot/daemonbot.pyc
                    --conf /etc/opt/opsware/waybot/waybot.args
```

カーネル2.4以降のLinuxサーバーの場合、コマンドエンジンのプロセスは1つです。

コマンドエンジンのURL

https://way.<データセンター>:1018

コマンドエンジンのログ

コマンドエンジンのログは、次のファイルにあります。

- /var/log/opsware/waybot/waybot.err*
- /var/log/opsware/waybot/waybot.log*
- /var/log/opsware/waybot/daemonbot.out*

ソフトウェアリポジトリの監視

ソフトウェアリポジトリは、SAで管理されるすべてのソフトウェアを保管するSAコアのコンポーネントです。ソフトウェアリポジトリはSAライブラリの一部です。各コアにはソフトウェアリポジトリが1つまたは複数存在します。この項では、コア内のソフトウェアリポジトリを監視する手順について説明します。

ソフトウェアリポジトリミラーリングとは、マルチマスターメッシュ内にあるソフトウェアリポジトリを同期することにより、冗長性と災害復旧に備える機能です。たとえば、メッシュ内の1つのコアにソフトウェアパッケージをアップロードすると、ソフトウェアリポジトリミラーリングジョブによってメッシュ内の他のすべてのソフトウェアリポジトリにアップロードしたパッケージが複製されます。

ソフトウェアリポジトリミラーリングを有効化/無効化する場合、またはソフトウェアリポジトリミラーリングジョブの実行頻度を変更する場合は、ソフトウェアリポジトリミラーリングパラメーターの変更 (179ページ) を参照してください。

ソフトウェアリポジトリのポート

ソフトウェアリポジトリは、次のポートを使用します。

- 1003 (暗号化)
- 1006 (クリアテキスト)
- 1005 (レプリケーター管理ユーザーインタフェース)
- 5679 (マルチマスターソフトウェアリポジトリ)

ソフトウェアリポジトリのプロセスの監視 - Linux

Linuxでソフトウェアリポジトリプロセスをチェックするには、ソフトウェアリポジトリコンポーネントを実行しているサーバーで、次のコマンドを実行します。

```
# ps auxwwww | grep -v grep | grep mm_wordbot
```

このコマンドでは、次のような出力が生成されます。

```
root  31006  0.0  0.0  13612  1492  ? S  Sep11  0:00  /opt/opsware/bin/
                     python /opt/opsware/pylibs/shadowbot/daemonbot.pyc --conf /etc/opt/
                     opsware/mm_wordbot/mm_wordbot.args
root  31007  0.0  0.1  103548  7688  ? S  Sep11  7:33 /opt/opsware/bin/
                     python /opt/opsware/pylibs/shadowbot/daemonbot.pyc --conf /etc/opt/
                     opsware/mm_wordbot/mm_wordbot.args
root  31092  0.0  0.0  13608  1480  ? S  Sep11  0:00  /opt/opsware/bin/
                     python /opt/opsware/pylibs/shadowbot/daemonbot.pyc --conf /etc/opt/
                     opsware/mm_wordbot/mm_wordbot-clear.args
root  31093  0.0  0.1  70172  6424  ? S  Sep11  2:11 /opt/opsware/bin/
                     python /opt/opsware/pylibs/shadowbot/daemonbot.pyc --conf /etc/opt/
                     opsware/mm_wordbot/mm_wordbot-clear.args
```

Linuxの場合、ソフトウェアリポジトリには実行中のプロセスが複数存在します (ほとんどはスレッドです)。暗号化されたソフトウェアリポジトリのプロセスと、クリアテキストのソフトウェアリポジトリのプロセスです。

ソフトウェアリポジトリのログ

ソフトウェアリポジトリのログは、次のファイルにあります。

- /var/log/opsware/mm_wordbot/wordbot.err*
- /var/log/opsware/mm_wordbot/wordbot.log*
- /var/log/opsware/mm_wordbot-clear/wordbot-clear.err*
- /var/log/opsware/mm_wordbot-clear/wordbot-clear.log*

ソフトウェアリポジトリミラーリング - SAクライアント

ソフトウェアリポジトリミラーリングとは、すべてのソフトウェアリポジトリを同期することにより、冗長性と災害復旧に備える機能です。1つのソフトウェアリポジトリに障害が発生しても、他のソフトウェアリポジトリでソフトウェアの要求を継続して処理することができます。ソフトウェアリポジトリミラーリングを有効にするには、ソフトウェアリポジトリミラーリングパラメーターの変更 (179 ページ) を参照してください。

ソフトウェアリポジトリミラーリングを有効にしている場合は、次のようにして、ソフトウェアリポジトリミラーリングのステータスを表示して監視することができます。

1. SAクライアントにマルチマスターツールのアクセス権を持つユーザーとしてログインします。アクセス権の詳細については、アクセス権のリファレンス (249ページ) を参照してください。
2. [**管理**] タブを選択します。
3. ナビゲーションパネルで［**ソフトウェアリポジトリミラーリング**］を選択します。マルチマスターメッシュでのソフトウェアリポジトリミラーリングのステータスが表示されます。表示される内容は、次のとおりです。
   - **メッシュ内のファイル数**：これは完全に同期された各ソフトウェアリポジトリ内のファイルの総数です。
   - **合計使用ディスク容量**：これは完全に同期されたソフトウェアリポジトリで必要な概算の合計ディスク容量です。
   - **ステータス**: 必要なファイルがすべて存在するソフトウェアリポジトリ (緑)、必要なファイルがあるソフトウェアリポジトリ (黄色)、ミラーリングが無効になっているソフトウェアリポジトリ (グレー) を表示します。
     - **緑**: 必要なファイルすべてがファシリティのソフトウェアリポジトリ内に存在します。欠落したファイルの数はゼロです。
     - **黄**: ファシリティのソフトウェアリポジトリに欠落したファイルがあるので、ソフトウェアリポジトリの更新が必要です。このファシリティは、次回のミラーリングジョブの実行時に更新されます。ミラーリングジョブは、ジョブで定義された実行間隔に基づいて、定期的に実行されます。
     - **グレー**: ファシリティでソフトウェアリポジトリミラーリングが無効になっています。

- **ファシリティ**: ソフトウェアリポジトリが実行されているSAファシリティを示します。
- **ファイル**: ホストのソフトウェアリポジトリに現在存在しているファイルの数。
- **サイズ**: ソフトウェアリポジトリのファイルで現在使用されている概算の合計ディスク容量。
- **未検出**: ファシリティのソフトウェアリポジトリによってミラーリングされるはずのファイルのうち、まだ複製されていないものの数。

ソフトウェアリポジトリミラーリングジョブの実行頻度を変更するには、ソフトウェアリポジトリミラーリングパラメーターの変更 (179ページ) を参照してください。

図35は、Bangalore、London、New Yorkという3つのSAコアでのソフトウェアリポジトリミラーリングのステータスを示しています。ソフトウェアパッケージはLondonコアにアップロードされました。黄色のステータス表示から、Bangaloreコアと New Yorkコアが同期されていない (これらのコアへのソフトウェアパッケージの複製が完了していない) ことがわかります。

図35　　ソフトウェアリポジトリミラーリングのステータス - 同期されていない

図36は、ミラーリングジョブが実行されて、ソフトウェアパッケージがすべてのコアに複製された後のソフトウェアリポジトリミラーリングの状態です。緑のステータス表示から、すべてのコアが同期されていることがわかります。

図36　　ソフトウェアリポジトリミラーリングのステータス - 同期されている

モデルリポジトリの監視

モデルリポジトリは、すべての管理対象サーバー、それぞれのハードウェア、構成、オペレーティングシステム、およびその他のすべてのアプリケーションのリストの作成、運用、管理に必要な基本情報を含むOracleデータベースです。

モデルリポジトリの詳細 (モデルリポジトリの監視に関する詳細を含む) については、『SA Installation Guide』の「付録A: モデルリポジトリでのOracleセットアップ」を参照してください。

モデルリポジトリのポート

モデルリポジトリのデフォルトポートは1521ですが、インストールを行なったデータベース管理者が変更している可能性があります。

モデルリポジトリのプロセスの監視

Oracle データベースプロセスを監視します。このプロセスが見つからない場合、データベースにエラーが発生しているか、データベースが開始されていません。

Linuxの場合、Oracleを実行しているサーバーで、次のコマンドを実行します。

```
# ps -fu oracle | grep pmon
```

このコマンドを実行すると、次のような出力が生成されます。

```
oracle    2112     1  0 21:22 ?    00:00:00 ora_pmon_truth
```

(この例のように、プロセス名にデータベースSID (truth) が含まれる場合があります。)

このプロセスが見つからない場合、リスナーにエラーが発生しているか、リスナーが開始されていません。

Linuxの場合、次のコマンドを使用してOracleリスナープロセスを監視します。

```
# ps -fu oracle | grep tnslsnr
```

このコマンドを実行すると、次のような出力が生成されます。

```
oracle    2021     1  0 21:22 ?    00:00:01 /u01/app/oracle/product/11.2.0/
db_2/bin/tnslsnr LISTENER -inherit
```

モデルリポジトリのログ

モデルリポジトリのログファイルはOracle データベースによって生成されます。ログファイルの場所はインストール環境によります。

デフォルトで、SAのモデルリポジトリのログでは、SID (この場合はtruth) ごとに1つのディレクトリを使用します。(これはOracleのインストール方法によって異なる場合があります。)

```
/u01/app/oracle/admin/truth/bdump/alter_truth.log
```

監視に使用する条件:

すべてのエラーがデータベースに関する問題を表すわけではありません。アプリケーションが原因のエラーが含まれている場合もあります。

これらの例では、問題があるのはコマンド出力がある場合です。

```
grep ORA- /u01/app/oracle/admin/truth/bdump/alter_truth.log

ORA-00600: internal error code, arguments:[729], [480], [space leak], [],
[], [], [], []

ORA-07445: exception encountered: core dump [lxmcpen()+0] [SIGSEGV]
[Address not mapped to object] ...
```

表領域の使用

表領域の使用は、重要度が段階的に大きくなるしきい値に対して監視します (たとえば、80% 以上で警告、90%以上でエラー、95%以上でクリティカルエラーなど)。

表領域の使用を監視する方法はいくつかあります。表領域に十分な空きディスク容量があるかどうかをチェックするのに使用するSQLクエリについては、『SA Installation Guide』の「付録A: モデルリポジトリでのOracleセットアップ」を参照してください。このインストールガイドのSQLクエリは、権限のあるデータベースユーザーとして実行する必要があります。

マルチマスターの競合

モデルリポジトリ内の競合するトランザクションの数を検出するには、SAの任意のデータベースユーザーとして次のSQLクエリを実行します。

```
select count(*) from transaction_conflicts where resolved = 'N';
```

マルチマスターの競合は、競合の数が増えるにつれてエスカレーションレベルが上がるように、段階的に監視します。段階に対応する値は、利用パターンによって異なります。

SA管理者は競合の数を一定期間(1週間など)記録し、記録した情報を利用して監視システムによるアラートのレベルを特定するようにしてください。

モデルリポジトリマルチマスターコンポーネントの監視

モデルリポジトリマルチマスターコンポーネントは、複数のモデルリポジトリの同期状態を維持し、元のモデルリポジトリに対する変更を他のすべてのモデルリポジトリデータベースに伝播するためのJavaプログラムです。

モデルリポジトリマルチマスターコンポーネントのポート

モデルリポジトリマルチマスターコンポーネントはポート5678を使用します。

モデルリポジトリマルチマスターコンポーネントのプロセスの監視

Linuxの場合、インフラストラクチャーコンポーネントバンドルをインストールしたサーバーで、次のコマンドを実行します。

```
# ps auxwww | grep -v grep | grep vault | grep -v twist
```

このコマンドを実行すると、次のような出力が生成されます。

```
root  28662  0.0  0.0  2284  532  ? S  Sep27  0:00  /opt/opsware//bin/
                    python /opt/opsware//pylibs/shadowbot/etc/daemonizer.pyc
                    --runpath /var/opt/opsware/vault --cmd /opt/opsware/j2sdk1.4.2_10/bin/
                    java -classpath /opt/opsware/vault/classes:/opt/opsware/vault ......
                    -ms120m -mx1024m
                    -DCONF=/etc/opt/opsware/vault/
                    -DHOSTNAME=m234.dev.opsware.com com.loudcloud.vault.Vault
root  28663  0.0  6.3  1285800  130896  ? S  Sep27  5:32  /opt/opsware/
                    j2sdk1.4.2_10/bin/java -classpath /opt/opsware/vault/classes:/opt/
                    opsware/vault ...... -ms120m -mx1024m
                    -DCONF=/etc/opt/opsware/vault/
                    -DHOSTNAME=m234.dev.opsware.com com.loudcloud.vault.Vault
```

モデルリポジトリマルチマスターコンポーネントのログ

モデルリポジトリマルチマスターコンポーネントのログは、次のファイルにあります。

- /var/log/opsware/vault/vault.n.log

ログファイル名、ログファイルサイズ、またはログレベルを構成するには、次の手順を実行します。

1. SAクライアントで[**管理**]タブを選択します。
2. ナビゲーションパネルで[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。
3. SAコンポーネントのリストで、[モデルリポジトリ、マルチマスターコンポーネント]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が表示されます。

4 必要に応じて、log、logLevel、またはlogsize構成パラメーターを変更します。

5 [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。

Global File Systemの監視

Global Shell機能は、スライスコンポーネントバンドルの一部としてインストールされます。Global File System (OGFS) 仮想ファイルシステムを動的に構成します。

Global Shellでは、サーバーエージェントと接続して、管理対象サーバーでUNIXシェルやWindowsリモートデスクトップ接続を開くことができます。

Global Shellの使用については、『SAユーザーガイド: Server Automation』のGlobal Shellの章および付録を参照してください。

Global File Systemコンポーネントは、次のプログラムで構成されます。

- ハブ: (エージェントプロキシ経由で) 管理対象サーバー上の他のコアコンポーネントやエージェントと連携してファイルシステムビューを構成するJavaプログラム。
- アダプター: Linuxの場合、FUSE (カーネル内のモジュール) とハブとの間でファイルシステム要求と応答を伝送し、FUSEユーザー空間ライブラリを使用してFUSEカーネルモジュールと通信するCプログラム。
- エージェントプロキシ: 管理対象サーバー上で実行中のエージェントとのSSL接続をハブに提供するPythonプログラム。
- FUSE (Linuxのみ): FUSE (Filesystem in Userspace) はGNU GPLライセンスで管理されるソフトウェアで、アダプターに対するファイルシステム要求のカーネル内ディスパッチを提供します。

ハブのプロセスグループIDファイルは、次のディレクトリにあります。

- /var/opt/opsware/hub/hub.pgrp

Global File Systemのプログラム (ハブ。アダプター、エージェントプロキシ、ログローテーター) はすべて、このプロセスグループで実行されます。

Global File Systemのプロセスの監視

Solarisの場合、スライスコンポーネントバンドルを実行しているサーバーで、次のコマンドを実行します。

```
# ptree $(ps -g $(cat /var/opt/opsware/hub/hub.pgrp) -o pid=)
```

このコマンドを実行すると、次のような出力が生成されます。

```
7594 /opt/opsware/bin/python /opt/opsware/hub/bin/rotator.py /opt/
                    opsware/j2sdk1.4.2......
 7598 /opt/opsware/j2sdk1.4.2_10/bin/java -server -Xms64m -Xmx1024m
                    -Dhub.kernel=SunO......
  7613 /opt/opsware/bin/python /opt/opsware/adapter/SunOS/bin/rotator.py
                    /opt/opsware/......
    7617 /opt/opsware/ogfsutils/bin/python2.4 /opt/opsware/adapter/
                    SunOS/lib/adapter.py......
     7618 /opt/opsware/adapter/SunOS/bin/mount -o hostpath=
                    /hostpath,nosuid /dev/ogdrv /v......
 7619 /opt/opsware/bin/python /opt/opsware/agentproxy/bin/rotator.pyc
                    /opt/opsware/bi......
  7625 /opt/opsware/bin/python /opt/opsware/agentproxy/lib/
                    main.pyc......
```

Solarisの場合、OGFS (特に、ハブ、アダプター、エージェントプロキシのプログラム) には実行中のプロセスが7つ存在します。

Linuxの場合、スライスコンポーネントバンドルを実行しているサーバーで、次のコマンドを実行します。

```
# ps u -g $(cat /var/opt/opsware/hub/hub.pgrp)
```

このコマンドを実行すると、次のような出力が生成されます。

```
USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND
                    root 8862 0.0 0.0 2436 1356 ? S Sep29 0:00 /opt/opsware/bin/python /
                    opt/opsware/hub/bin/rotator.py /opt/opsware/j2sdk1.4.2_10/b......
root 8868 0.1 1.8 1256536 76672 ? S Sep29 35:51 /opt/opsware/j2sdk1.4.2_
                    10/bin/java -server -Xms64m -Xmx1024m -Dhub.kernel=Linux -Dh......
root 8906 0.0 0.0 2412 1304 ? S Sep29 0:28 /opt/opsware/bin/python /opt/
                    opsware/adapter/bin/adapter......
root 8908 0.0 0.0 13088 684 ? S Sep29 0:10 /opt/opsware/adapter/Linux/
                    bin/adapter.bin /var/opt/opsware/ogfs/mnt/ogfs -f -o none......
root 8913 0.0 0.0 2308 1132 ? S Sep29 0:00 /opt/opsware/bin/python /opt/
                    opsware/agentproxy/bin/rotator.pyc /opt/opsware/bin/pyt......
root 8923 0.0 0.1 153120 6544 ? S Sep29 5:56 /opt/opsware/bin/python
                    /opt/opsware/agentproxy/lib/main.pyc......
```

Linuxの場合、OGFS (特に、ハブ、アダプター、エージェントプロキシのプログラム) には実行中のプロセスが6つ存在します。

また、Global File Systemでは、LinuxとSolarisの両方でinitスクリプトに対するstatusオプションがサポートされます。

LinuxまたはSolarisの場合、スライスコンポーネントバンドルを実行しているサーバーで次のコマンドを実行して、次のstatusオプションを実行します。

```
# /etc/opt/opsware/startup/hub status
```

このコマンドを実行すると、次のような出力が生成されます。

```
Testing for presence of Hub process group file (/var/opt/opsware/hub/hub.pgrp) ... OK
Testing that processes are running in Hub process group (8862) ... OK
Testing that OGFS is mounted ... OK
Testing that the OGFS authenticate file is present ... OK
OGFS is running
```

Global File Systemのログ

ハブのログは、次のファイルにあります。

- /var/log/opsware/hub/hub.log*
- /var/log/opsware/hub/hub.out*

  ハブのログでの監視に使用する条件:

  — 「Can't establish twist connection (twist接続を確立できません)」を含む文字列

アダプターのログは、次のファイルにあります。

- /var/log/opsware/adapter/adapter.err*

エージェントプロキシのログは、次のファイルにあります。

- /var/log/opsware/agentproxy/agentproxy.err*

FUSEのプロセスの監視 (Linuxのみ)

Linuxの場合、スライスコンポーネントバンドルを実行しているサーバーで、次のコマンドを実行します。

```
# lsmod | grep -v grep | grep fuse
```

このコマンドを実行すると、次のような出力が生成されます。

```
fuse      31196   2
```

FUSEでは、メッセージが次のファイルにログ記録されます。

- /var/log/messages

SunOSカーネルモジュールのプロセスの監視

Solarisの場合、OGFSの機能はSunOSカーネルモジュールを使用します。

スライスコンポーネントバンドルを実行しているサーバーで、次のコマンドを実行します。

```
# modinfo | grep -i opsware
```

このコマンドを実行すると、次のような出力が生成されます。

```
137 1322cd8 43a9 272 1 ogdrv (Opsware GFS driver v1.13)
138 13ac227 338df 18 1 ogfs (Opsware Global Filesystem v1.14)
```

Global File Systemでは、SunOSカーネルモジュールに関連するメッセージが次のファイルにログ記録されます。

- /var/adm/messages

Spokeの監視

SpokeはSAクライアントのバックエンドコンポーネントです。SpokeはJava RMIサーバーで、OGFS内のファイルに対するアクセスと、OGFSセッション内でコマンドを実行するためのアクセスを提供します。

Spokeのポート

Spokeはポート8020を使用します。

Spokeのプロセスの監視

Linuxの場合、スライスコンポーネントバンドルを実行しているサーバーで、次のコマンドを実行します。

```
# ps -ef | grep -v grep | grep spoke
```

このコマンドを実行すると、次のような出力が生成されます。

```
root  29191  1  0  Aug28  ? 01:12:11  /opt/opsware/j2sdk1.4.2_10/bin/
                    java -server -Xms32m -Xmx256m -Dbea.home=/opt/opsware/spoke/etc
                    -Dspoke.home=/opt/opsware/spoke
                    -Dspoke.cryptodir=/var/opt/opsware/crypto/spoke
                    -Dspoke.logdir=/var/log/opsware/spoke
                    -Djava.util.logging.config.file=/opt/opsware/spoke/etc/logg
```

Linuxの場合、Spokeコンポーネントには、実行中のJavaプロセスが1つ存在します。

Spokeのログ

Spokeのログは、次のファイルにあります。

- /var/log/opsware/spoke/spoke-*.log
- /var/log/opsware/spoke/stdout.log

ゲートウェイの監視

SAの管理ゲートウェイとコアゲートウェイを使用すると、SAコアで1つ以上のNATデバイスまたはファイアウォール越しに存在するサーバーを管理できます。ゲートウェイ間の接続は、ゲートウェイインスタンス間の永続的なTCPトンネル経由でメッセージをルーティングすることで維持されます。

ゲートウェイの構成については、『SA概要とアーキテクチャーガイド』を参照してください。

サテライトゲートウェイの管理については、サテライトの管理 (131ページ) を参照してください。

ゲートウェイのポート

デフォルトで、ゲートウェイは次のポートを使用します。

- 2001 — 管理ゲートウェイリスナーポート
- 2001 — スライスコンポーネントコアゲートウェイリスナーポート
- 3001 — エージェントゲートウェイポート
- 3001 — サテライトゲートウェイポート

ゲートウェイのプロセスの監視

いずれの構成でも、ゲートウェイコンポーネントには実行中のプロセスが2つ存在します (ゲートウェイプロセスとウォッチドッグプロセス)。

SolarisまたはLinuxの場合、ゲートウェイコンポーネントを実行しているサーバーで、次のコマンドを実行します。

```
# ps -eaf | grep -v grep | grep opswgw | grep cgw
```

このコマンドを実行すると、次のような出力が生成されます。

```
root  17092  1  0  Sep21  ? 00:00:00  [opswgw-watchdog-2.1.1: cgw0-C43]
                    --PropertiesFile /etc/opt/opsware/opswgw-cgw0-C43/opswgw.properties
                    --BinPath /opt/opsware/opswgw/bin/opswgw
root  17094  17092  0  Sep21  ? 02:23:21  [opswgw-gateway-2.1.1: cgw0-
                    C43] --PropertiesFile /etc/opt/opsware/opswgw-cgw0-C43/
                    opswgw.properties --BinPath /opt/opsware/opswgw/bin/opswgw --Child true
```

```
# ps -eaf | grep -v grep | grep opswgw | grep agw
```

このコマンドを実行すると、次のような出力が生成されます。

```
root  17207  1  0  Sep21  ? 00:00:00  [opswgw-watchdog-2.1.1: agw0-C43]
                    --PropertiesFile /etc/opt/opsware/opswgw-agw0-C43/opswgw.properties
                    --BinPath /opt/opsware/opswgw/bin/opswgw
root  17208  17207  0  Sep21  ? 01:18:54  [opswgw-gateway-2.1.1: agw0-
                    C43] --PropertiesFile /etc/opt/opsware/opswgw-agw0-C43/
                    opswgw.properties --BinPath /opt/opsware/opswgw/bin/opswgw --Child true
```

SolarisまたはLinuxの場合、サテライトファシリティで、サテライトゲートウェイコンポーネントを実行しているサーバーで、次のコマンドを実行します。

```
# ps -eaf | grep -v grep | grep opswgw | grep <ゲートウェイ名>
```

この例の<ゲートウェイ名>はSat1です。

このコマンドを実行すると、次のような出力が生成されます。

```
root  17092  1  0  Sep21  ? 00:00:00  [opswgw-watchdog-2.1.1:Sat1]
```

```
                    --PropertiesFile /etc/opt/opsware/opswgw-Sat1/opswgw.properties
                    --BinPath /opt/opsware/opswgw/bin/opswgw
root  17094  17092  0  Sep21  ? 02:23:21  [opswgw-gateway-2.1.1:Sat1]
                    --PropertiesFile /etc/opt/opsware/opswgw-Sat1/opswgw.properties
                    --BinPath /opt/opsware/opswgw/bin/opswgw --Child true
```

ゲートウェイのURL

SAクライアントのUIにログインし、ナビゲーションパネルの[管理]で[ゲートウェイ]を選択します。

`https://occ.<データセンター>/com.opsware.occ.gwadmin/index.jsp`

ゲートウェイのログ

ゲートウェイのログは、次のファイルにあります。

- `/var/log/opsware/gateway-name/opswgw.log*`

これらのログでの監視に使用する条件:

- 「ERROR」を含む文字列
- 「FATAL」を含む文字列(プロセスがまもなく終了することを示す)

OS Build Managerの監視

OS Build Managerコンポーネントは、OSビルドエージェントとコマンドエンジンの間の通信をサポートする機能を持ち、コマンドエンジンが送信したOSプロビジョニングコマンドを受信します。また、OSプロビジョニング手順を実行できるように、プラットフォーム固有のビルドスクリプトの実行時環境を提供します。

OS Build Managerのポート

OS Build Managerは、次のポートを使用します。

- 1012 (HTTPS)
- 1017 (SAビルドエージェント)

OS Build Managerのプロセスの監視

いずれの構成でも、OS Build Managerコンポーネントには実行中のプロセスが1つ存在します。

Linuxの場合、OS Build Managerコンポーネントを実行しているサーバーで、次のコマンドを実行します。

```
# ps -eaf | grep -v grep | grep buildmgr
```

このコマンドを実行すると、次のような出力が生成されます。

```
root  2174  1  0  Sep27  ? 0:13:54  /opt/opsware/j2sdk1.4.2_10/bin/
          java -Xmx256m -Dbuildmgr -Djava.security.properties=/opt/opsware/
          buildmgr/etc/java.security -DDEBUG -DDEBUG_VERBOSE=1 -DLOG_OPTIONS=tTN
          -DLOG_FILE_THRESHOLD=10485760 -DLOG_FILE_RETAIN_COUNT=7
          -DLOG_CLASSES=com.opsware.buildmgr.OutputStreamLo
```

OS Build ManagerのURL

`https://buildmgr.<データセンター>:1012`

OS Build ManagerのUIは読み取り専用です。このUIのポート1012は構成可能です。

OS Build Managerのログ

OS Build Managerのログは、次のファイルにあります。

- `/var/log/opsware/buildmgr/buildmgr.log`(ビルドエージェントのアクティビティ、OSプロビジョニングのアクティビティ)
- `/var/log/opsware/buildmgr/*.request.log`(Webサーバーログ、1日あたり1ファイル、最大90)
- `/var/log/opsware/buildmgr/console.log`
- `/var/log/opsware/buildmgr/servers/<IP_address or machine_ID or MAC_address>`(接続ごとのログ)

これらのログでの監視に使用する条件: 文字列「Traceback」

OSブートサーバーの監視

OSブートサーバーは、OSプロビジョニング機能の一部で、SunではinetBoot、x86システムではPXEを使用するネットワークブートをサポートします。このプロセスには、Internet Software ConsortiumのDHCPサーバーが使われています。

これらのアプリケーションはSAインストーラーでインストールされますが、SA固有のアプリケーションではありません。これらのプロセスの監視には、これらのアプリケーションの標準的なシステム管理の推奨方法を使用します。

OSブートサーバーのポート

OSブートサーバーは、次のポートを使用します。

- 67 (UDP) (DHCPサービス)
- 69 (UDP) (TFTPサービス)

OSブートサーバーのログ

OSブートサーバーは専用のログを生成しません。OSブートサーバーは、TFTP (INETD)、NFSサーバー、ISC DHCPDのサービスを使用します。これらのサービスはすべてsyslogでログ記録します。詳細については、ベンダードキュメントを参照してください。また、このコンポーネントのログ構成を確認するには、OSブートサーバーの構成に使用した`syslog.conf`ファイルを参照してください。

OSメディアサーバーの監視

OSメディアサーバーはOSプロビジョニング機能の一部で、OSプロビジョニングの際に使用するベンダー提供メディアへのネットワークアクセスを提供します。このサポートを提供するプロセスには、Samba SMBサーバーとSun Solaris NFSが含まれます。

これらのアプリケーションはHP BSAインストーラーでインストールされますが、SA固有のアプリケーションではありません。SAにはLinuxおよびSolaris用のSambaパッケージが用意されており、カスタマーはこれを使用してOSメディアサーバーをインストールできます。NFSサービスはオペレーティングシステムで提供されます。HP BSAインストーラーを使用してOSメディアサーバーをインストールすると、LinuxやSolaris上でNFSが構成されます。

Samba SMBサーバーとSun Solaris NFSアプリケーションの監視には、これらのアプリケーションの標準的なシステム管理の推奨方法を使用します。

OSメディアサーバーのポート

OSメディアサーバーは、次のポートを使用します。

- NFSで使用されるポートマッパーはポート111です。
- Samba SMBはポート137、138、139、445を使用します。

OSメディアサーバーのログ

OSメディアサーバーのログは、次のファイルにあります。

- `/var/log/opsware/samba/log.smbd`
- `/var/log/opsware/samba/log.nmbd`

SolarisおよびLinuxのOSプロビジョニングでは、NFSDなどのベンダーが提供するサービスを使用します。通常、これらのサービスはsyslogを使用してログ記録します。これらのログファイルの詳細については、ベンダードキュメントを参照してください。

第8章 SAのトラブルシューティング - 診断テスト

この項では、次の内容について説明します。

- **コアの正常性チェックモニター**: 個別のSAコンポーネントの正常性をチェックします。コアの正常性チェックモニター (HCM) (206ページ) を参照してください。
- **システム診断**ツール: SAコアの全体的な正常性をチェックします。システム診断の実行 (216ページ) を参照してください。

これらのツールを使用すると、SAの管理中に発生する可能性のある次のような問題を診断することができます。

- **動作上の問題**: プロセスがエラーまたは応答しなくなる (データアクセスエンジン、コマンドエンジン、ソフトウェアリポジトリなど)
- **SAコアコンポーネントのエラー**: 他のコンポーネントのエラーの原因になります。

  コアコンポーネントにエラーが起きると、次のような影響が生じます。

  - データアクセスエンジンにエラーが起きると、SAクライアント、コマンドエンジン、ソフトウェアリポジトリのコンポーネントもエラーになります。
  - ソフトウェアリポジトリからデータアクセスエンジンへアクセスできない場合、ソフトウェアリポジトリからのダウンロードができません。
  - モデルリポジトリにエラーが起きると、データアクセスエンジンもエラーになります。
  - ソフトウェアリポジトリに正常に機能しているDNSまたは適切に構成された/etc/hostsファイルがない場合、ソフトウェアリポジトリからデータアクセスエンジンにアクセスできません。
  - 管理対象の環境に到達不能なサーバーが存在する場合、通信に不具合が生じます。

システム診断は1つのファシリティごとに実行する必要があります。

SAコアコンポーネントの内部名

都合上、このドキュメントでは一部のSAコアコンポーネントを内部名を使用して表記しています。表27に、SAコンポーネントの内部名と外部名を示します。

表27 コンポーネントの内部名と外部名

内部名	外部名
agentcache	Global File Systemのコンポーネント
buildmgr	OS Provisioning Build Manager
hub	Global File Systemのコンポーネント
mm_wordbot	ソフトウェアリポジトリのコンポーネント
occ	SAコマンドセンター

表27　コンポーネントの内部名と外部名（続き）

内部名	外部名
opswgw-agw0	エージェントゲートウェイ
opswgw-mgws0	マスターゲートウェイ
spin	データアクセスエンジン
spoke	Global File Systemのコンポーネント
truth	モデルリポジトリ
twist	Webサービスデータアクセスエンジン
vault/vaultdaemon	モデルリポジトリ マルチマスターコンポーネント
way/waybot	コマンドエンジン
word	ソフトウェアリポジトリ

コアの正常性チェックモニター(HCM)

正常性チェックモニター(HCM)には、SAコアのステータスをチェックするためのテスト一式が含まれています。HCMのスクリプトは、SAインストーラーによってインストールされます。HCMとシステム診断ツールの機能には、重複する部分があります(システム診断テスト (217ページ)を参照)。

HCMでは、次の2つのタイプのテストが利用できます。

- ローカルテスト:コアの正常性をコンポーネントごとに検証します。
- グローバルテスト:コアの正常性を全体として検証します。

HCMローカルテストの概要

HCMローカルテストでは、コアコンポーネントを個別に検証します。ローカルテストは検証対象のコンポーネントと同じサーバー上に存在します。ローカルテストを実行するには、SA開始スクリプト(/etc/init.d/opsware-sas)を実行して、テストモード引数とオプションのコンポーネント名を指定します。

テストモードでは、実行するテストのセットを指定します(個別のテストを指定することはできません)。同じテストが必要な複数のコンポーネントを指定した場合でも、それぞれのテストは1回だけ実行されます。テスト結果はstdoutに表示されます。

サテライトホストから正常性チェックモニターを実行することはできません。

HCMローカルテストのスクリプトの構文

HCMローカルテストでは、次の構文を使用します。

```
/etc/init.d/opsware-sas <mode> [<component>[<component>...]]
[<name>=<value>[<name>=<value>]...]
```

HCMローカルテストの実行

ローカルテストを実行するには、次の手順を実行します。

1. テスト対象のSAコアコンポーネントを実行しているサーバーに`root`としてログオンします。
2. `status`引数を使用してSA開始スクリプトを実行するか、`mode`(テストカテゴリ)引数と1つ以上のコンポーネントを指定します(コマンドオプションについては、次の項を参照してください)。たとえば、次のスクリプトでは、Webサービスデータアクセスエンジンが利用可能であることを確認します。

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

表 28 は、HCM のコマンドライン引数について説明したものです。コアの開始および停止に関する opsware-sasのオプションについては、表24を参照してください。

表28　　HCMローカルテストスクリプトのオプション

オプション	説明
mode	実行するテストのセット。modeには次のいずれかを指定できます。 • status: 指定したコンポーネントの可用性を確認するテストを実行します。たとえば、コンポーネントが適切なポートをリッスン対象としていて、基本的なクエリに応答していることを確認するテストを実行できます。 • verify_post: statusと同じです。 • verify_pre: 指定したコンポーネントの動作に必要な条件を検証するテストを実行します。 • verify_functionality: statusモードで実行されるテストと同様のテストを実行します。ただし、こちらの方が時間がかかる可能性があります。そのため、時間を節約する場合は、これらのテストをスキップできます。 • health: status、verify_pre、verify_functionalityモードのテストを実行し、指定したコンポーネントの全体的な状態の概要を示します。
component	コアコンポーネントの内部名です。このオプションを指定しない場合は、すべてのコンポーネントが検証されます。ローカルサーバーにインストールされているコンポーネントの内部名を表示するには、次のコマンドを実行します。 /etc/init.d/opsware-sas list
name=value	テストの実行方法を制御するオプションです。次の値を指定できます。 • terse=[true|false]: trueの場合、各コンポーネントのすべての成功したテストの結果が1つのSUCCESSメッセージにまとめられます。ただし、失敗したテストの結果は個別に表示されます。デフォルトで、このオプションはfalseに設定されます(このオプションは個別のテストに渡されます)。 • parsable=[true|false]: trueの場合、各コンポーネントのすべてのテストの結果が1つのSUCCESSまたはFAILUREメッセージにまとめられます。デフォルトで、このオプションはfalseに設定されます(このオプションは個別のテストに渡されます)。 • verify_filter=<regex>: ファイル名が指定した正規表現と一致するテストのみを実行します。たとえば、verify_filter="OPSW"と指定すると、100_OPSWcheck_host_spin.shのようにファイル名に文字列OPSWを含むテストのみが実行されます。デフォルトで、このオプションは定義されません(このオプションは個別のテストに渡されません)。 特定のテストが別のファイルへのシンボリックリンクである場合、フィルターはシンボリックリンクの名前ではなく、シンボリックリンクのターゲットに対して評価されます。テストがシンボリックリンクである場合、verify_filterはポイント先のファイルのファイル名を比較に使用します。

特定のコアコンポーネントで使用される内部名とそれぞれの標準名については、SAコアコンポーネントの内部名 (205ページ) を参照してください。

HCMグローバルテストの概要

HCMグローバルテストでは、SAコア全体をチェックします。グローバルテストを実行するには、次のホストでrun_all_probes.shスクリプトを実行します。

- スライス構成 — コアの管理ゲートウェイまたはインフラストラクチャーコンポーネントをホストしているサーバー(通常のインストールでは、管理ゲートウェイはインフラストラクチャーコンポーネントをホストしているサーバーにインストールされます)。
- 非スライス構成 — 検証対象のコアのプライマリモデルリポジトリマルチマスターコンポーネントをホストしているサーバー。

テスト結果はstdoutに表示されます。グローバルテストでは、マルチマスターメッシュ内の他のコアの状態をチェックすることはできません。

マルチサーバーコアの場合、グローバルテストではSSHを使用して他のコアサーバーに接続します。接続はすべてrootで行われます。コマンドラインでrootパスワードまたはキーファイルを指定して認証を行います。両方を指定した場合は、rootパスワードが使用されます。サーバーがローカルホストでない場合は、これらの認証方法のいずれかを指定する必要があります。

HCMグローバルテストの実行

HCMグローバルテストを実行するには、次の手順を実行します。

1. モデルリポジトリマルチマスターコンポーネントまたはインフラストラクチャーコンポーネントをホストしているサーバーに、rootとしてログインします。
2. runオプションを指定してrun_all_probes.shスクリプトを実行します （オプションの詳細については、次の項を参照)。たとえば、モデルリポジトリのOracleデータベースで表領域の使用をチェックするには、次のコマンドを実行します。

   ```
   /opt/opsware/oi_util/bin/run_all_probes.sh run \
   check_database_tables
   ```

HCMグローバルテストのスクリプトの構文

HCMグローバルテストを実行するスクリプトの構文は、次のとおりです。

```
/opt/opsware/oi_util/bin/run_all_probes.sh run|list
[<test> [<test>...]
[hosts="<system>[:<password>] [<system>[:<password>]]..."
[keyfile=<keyfiletype>:<keyfile>[:<passphrase>]]
```

表29は、この構文のオプションについて説明したものです。

表29　　HCMグローバルテストスクリプトのオプション

オプション	説明
list	使用可能なテストをリスト表示します。
run	指定されたテストを実行します。
test	実行するテストの名前。テストを指定しない場合は、すべてのテストが実行されます。出荷時に、このスクリプトには次のテストが含まれています。 • check_opsware_services: 次のコマンドを各コアサーバーでリモートから実行して、指定したすべてのサーバーでローカルテストを実行します。/etc/init.d/opsware-sas health • check_MM_state: マルチマスターソースコアで、コアのマルチマスター状態をチェックします。 • check_time: マルチサーバーコアで、システムクロックがコアサーバー間で同期されていることを確認します。 • check_opsware_version: コア内のすべてのコンポーネントのバージョンが同じであることを検証します。 • check_database_tables: モデルリポジトリの表領域の使用が許容できる制限範囲内であることを検証します。表領域の詳細については、『SA Installation Guide』の「モデルリポジトリでのOracleセットアップ」を参照してください。 • check_OS_resources: SAのパーティションの仮想メモリーとディスク容量が許容できるしきい値を超えていないかどうかを検証します。 • check_fully_functional: SAのすべてのコンポーネントのすべての機能を検証します。SAクライアントでシステム診断の総合テストを実行する代わりに、この機能を使用することができます。システム診断テスト (217ページ)を参照してください。
system:password	リモートコアサーバー (ホスト名またはIPアドレス) を指定します。また、オプションでサーバーのrootパスワードを指定します。
keyfiletype	使用するキーファイルのタイプを指定します。使用可能な値は以下のとおりです。 • rsa_key_file • dsa_key_file
keyfile	現在のサーバーのSSHプライベートキーを含むファイルを指定します。
passphrase	SSHプライベートキーの暗号化に使用したpassphraseを指定します。

グローバルテストでのパスワードを使用しないSSHのセットアップ

グローバルテストでは、SSHデーモンを使用してコア内のリモートサーバーにアクセスします。これらのテストでは、rootパスワードを入力するか、SSHパブリック/プライベートキーを使用する必要があります。

ssh-keygenで生成されたパブリック/プライベートキーを使用して認証をセットアップするには、次の手順を実行します。

1　信頼されたサーバー上で次のコマンドを実行し、デフォルト設定をそのまま使用します。コマンドはLinuxとSolarisで異なります。

Linuxの場合:

```
cd /root/.ssh
ssh-keygen -t dsa
```

Solarisの場合:

```
cd /.ssh
ssh-keygen -t dsa
```

2 id_dsa.pubファイルをクライアントサーバーの.sshディレクトリにコピーした後に、名前をauthorized_keysに変更して、クライアントサーバーを更新します。次に、LinuxおよびSolarisの場合のコマンド例を示します。

Linuxの場合:

```
scp id_dsa.pub <host>:/.ssh/authorized_keys
/root/.ssh/authorized_keys
```

Solarisの場合:

```
scp id_dsa.pub <host>:/.ssh/authorized_keys
/.ssh/authorized_keys
```

3 信頼されたサーバーを確認します。次のコマンドを実行して、信頼されたサーバーがパスワードなしでクライアントサーバーに接続できることを検証します。

```
ssh -l root <host>
```

正常性チェックモニターの拡張

この項は、UNIXシェルプログラミングとSA管理の経験がある上級のシステム管理者を対象としています。

HCMは、コアサーバー上でローカルテストまたはグローバルテストを実行する一連のUNIXシェルスクリプトとして実装されます。これらのスクリプトは固有の命名規則に準拠し、あらかじめ定義されたディレクトリ内に存在します。HCMを拡張するには、独自のスクリプトを作成して/opt/opsware/oi_utilの下の適切なディレクトリにコピーする必要があります。

HCMローカルテストに対する拡張の要件

HCM ローカルテストは、/etc/init.d/opsware-sas スクリプトによって実行されるスクリプトです (HCM ローカルテストの実行 (207ページ) を参照してください)。ローカルテストスクリプトは、次の要件を満たしている必要があります。

- **UNIXシェルスクリプト:** rootとして実行するUNIXシェルスクリプトです。
- **コンポーネントサーバー:** スクリプトはスクリプトによって検証されるコンポーネントのサーバー上に存在し、このサーバー上で実行されます。たとえば、スクリプトでデータアクセスエンジン (spin) を検証する場合、スクリプトはデータアクセスエンジンを実行しているサーバー上に存在します。
- **実行可能:** スクリプトは実行可能ファイルです (chmod u+x)。
- **ファイル名:** スクリプトのファイル名の構文は、次のとおりです。

  <int><test>.sh

  この構文で、intはテスト実行順序を示す整数で、testはテストの名前です。SAで利用できるHCMスクリプトのファイル名には、たとえば100_OPSWportping.shのように、OPSWが含まれることに注意してください。
- **ディレクトリ:** スクリプトは次のディレクトリに存在します。

/opt/opsware/oi_util/local_probes/<component>/[verify_pre | verify_post | verify_functionality]/

このパスで、componentは、spinやtwistなどのコアコンポーネントの内部名です。componentディレクトリの下のディレクトリは、テストのカテゴリと同じです。たとえば、テストでコアコンポーネント上での実行時検証を行う場合、スクリプトはverify_functionalityサブディレクトリ内に存在します。詳細については、カテゴリとローカルテストのディレクトリ (213ページ) を参照してください。

componentディレクトリの下のディレクトリは、/etc/init.d/opsware-sasコマンドのmodeオプションに対応します。たとえば、verify_preサブディレクトリにスクリプトを保存した場合、verify_preオプションを指定してopsware-sasを実行したときにスクリプトが実行されます。opsware-sasのhealthオプションを指定すると、3つのすべてのディレクトリにあるスクリプトが実行されます。表30は、ディレクトリ名とモードオプションとの対応関係を示しています。

表30　opsware-sasのモードとローカルテストスクリプトのサブディレクトリ

コマンドラインのモードオプション	このオプションで実行されるスクリプトのサブディレクトリ
health	verify_pre verify_post verify_functionality
status	verify_post
verify_functionality	verify_functionality
verify_post	verify_post
verify_pre	verify_pre

- 終了コード: スクリプトが正常に終了した場合はゼロの終了コードが返されます。スクリプトが失敗した場合はゼロ以外の終了コードが返されます。/etc/init.d/opsware-sasコマンドでは、終了コードを使用してテストのステータスを特定します。
- 結果の表示: スクリプトはstdoutにテスト結果を表示します。
- ローカルプリアンブルスクリプト: テストスクリプトでは、HCMローカルテストの例 (214ページ) に示すように、local_probe_preamble.shスクリプトが実行されます。local_probe_preamble.shスクリプトには、/etc/init.d/opsware-sasコマンドで使用するライブラリとシェル変数のスーパーセットが含まれます。

  local_probe_preamble.shスクリプトは、次のタスクを実行します。

  — ローカルテストで使用するシェル変数を設定します。たとえば、$PYTHON (Pythonインタープリターを指す) と$UTILS_DIR (テストで使用できるユーティリティのディレクトリを指す) を設定します。

  — コマンドラインを解析して、name=value のすべてのペアを評価し、シェル変数を設定します。たとえば、/etc/init.d/opsware-sasの実行時にコマンドラインでtimeout=60 を指定すると、local_probe_preamble.shスクリプトは変数$timeoutを値60に設定します。

  — 成功するか指定のタイムアウトが経過するまでコマンドを複数回実行するretryなどの便利な機能へのアクセスを提供します。
- シェル変数: テストスクリプトでは、コマンドラインでname=valueオプションによって指定された変数を考慮します。事前に定義された名前については、表28のname=valueオプションを参照してください。

カテゴリとローカルテストのディレクトリ

/opt/opsware/oi_utilディレクトリには、次のサブディレクトリがあります。

local_probes/<component>/verify_pre

このディレクトリには、各コンポーネントの前提条件テストが含まれます。これらのテストでは、コンポーネントの動作に必要な条件が存在することを確認します。たとえば、ディレクトリtwist/verify_preには、テストスクリプト10check_localhost_spin.shが含まれます。これは、Webサービスデータアクセスエンジンが機能するには、データアクセスエンジンコンポーネントの利用が不可欠であるためです。

local_probes/<component>/verify_post

このディレクトリには、各コンポーネントの検証テストが含まれます。これらのテストでは、特定のコンポーネントが利用可能であることを確認します。たとえば、ディレクトリspin/verify_postにはテストスクリプト10check_primary_spin.shが含まれます。これは、データアクセスエンジンコンポーネントがポート1004をリッスン対象としていて、基本的なクエリに応答することを検証するためです。

local_probes/<component>/verify_functionality

このディレクトリには、各コンポーネントの実行時検証テストが含まれます。これらのテストでは、コンポーネントが完全に機能することを確認します。これらのテストはverify_postテストと似ていますが、こちらの方が時間がかかる可能性があります。時間を節約する場合は、これらのテストをスキップできます。

HCMローカルテストのディレクトリレイアウト:

ローカルテストが配置されているディレクトリレイアウトは、次のとおりです。

```
/opt/opsware/oi_util/
 |
 |_lib
 | |_local_probe_preamble.sh
 |
 |_local_probes
   |
   |_COMMON
   | |_<test>
   | |_ ...
   |
   |_<component>
   | |
   | |_verify_pre
   | | |_ <int><test> (../../COMMON/<test>へのシンボリックリンクも可)
   | | |_ ...
   | |
   | |_verify_post
   | | |_ <int><test> (../../COMMON/<test>へのシンボリックリンクも可)
   | | |_ ...
   | |
   | |_verify_functionality
   |   |_<int><test> (../../COMMON/<test>へのシンボリックリンクも可)
   |   |_...
   |
```

```
|_<component>
  ...
```

HCMローカルテストの例

次のスクリプトでは、cronユーティリティがローカルサーバー上で実行中であることを確認します。

```
#!/bin/sh
# cronが実行中であることを確認する
# ライブラリ/標準変数設定を読み込んで、
# コマンドラインを解析する。
/opt/opsware/oi_util/lib/local_probe_preamble.sh
printf "Verify \"cron\" is running:"
process_running=`ps -eo fname | egrep '^cron$' | head -1`
if [ -z "$process_running" ]; then
    echo "FAILURE (cron does not exist in the process table)"
    exit 1
else
    echo "SUCCESS"
    exit 0
fi
```

HCMグローバルテストに対する拡張の要件

HCMグローバルテストは、run_global_probes.shコマンドで呼び出されるスクリプトです (HCMグローバルテストの実行 (209ページ) を参照してください)。グローバルテストスクリプトは、次の要件を満たしている必要があります。

- **UNIXシェルスクリプト:** rootとして実行するUNIXシェルスクリプトです。
- **モデルリポジトリサーバー:** スクリプトはモデルリポジトリサーバー上に存在しますが、任意のコアサーバー上でリモートで実行することができます。
- **実行可能:** スクリプトは実行可能ファイルです (chmod u+x)。
- **ファイル名:** スクリプトのファイル名の構文は、次のとおりです。

  ```
  <int><test>.sh[.remote]
  ```

  この構文で、intはテスト実行順序を示す整数で、testはコマンドラインで指定されたテストの名前です。SAで利用できるHCMスクリプトのファイル名には、たとえば300_OPSWcheck_time.shのように、OPSWが含まれることに注意してください。
- **リモート実行:** HCMグローバルテストの概要 (209ページ) に記載したサーバー以外のコアサーバーでテストスクリプトを実行する場合は、ファイル名に拡張子.remoteが必要です。run_all_probes.shを実行して、このようなテストを指定した場合、スクリプトは指定されたすべてのサーバーに自動的にコピーされ、SSHプロトコルを使用してリモートで実行されます。

  モデルリポジトリマルチマスターコンポーネント (非スライスインストール) または管理ゲートウェイ/インフラストラクチャーコンポーネント (スライスインストール) と同じサーバーで実行するテストの場合、ファイル名に拡張子.remoteは必要ありません。これらのテストには、たとえば、モデルリポジトリの完全性やマルチマスターの競合のチェックなどがあります。拡張子.remoteがないスクリプトでリモートサーバーと通信する必要がある場合は、スクリプトでSSHを使用する必要があります。グローバルプリアンブルスクリプトには、SSHによるリモート通信を処理するためのヘルパー関数が含まれています。
- **ディレクトリ:** スクリプトは次のディレクトリに存在します。

```
/opt/opsware/oi_util/global_probes/[verify_pre | verify_post ]/
```

詳細については、HCMグローバルテストのディレクトリ (216ページ) を参照してください。

- 終了コード: スクリプトが正常に終了した場合はゼロの終了コードが返されます。スクリプトが失敗した場合はゼロ以外の終了コードが返されます。run_global_probes.shコマンドでは、終了コードを使用してテストのステータスを特定します。
- 結果の表示: スクリプトはstdoutにテスト結果を表示します。
- グローバルプリアンブルスクリプト: テストスクリプトでは、HCMグローバルテストの例 (215ページ)に示すように、global_probe_preamble.shスクリプトが実行されます。global_probe_preamble.shスクリプトには、HCMグローバルテストで使用するライブラリとシェル変数のスーパーセットが含まれます。

  global_probe_preamble.shスクリプトは、次のタスクを実行します。

  — テストで使用するシェル変数を設定します。

  — コマンドラインを解析して、name=value のすべてのペアを評価し、シェル変数を設定します。たとえば、run_all_probes.sh,を使ってコマンドラインでhosts="sys1:pw1 sys2:pw2"を指定した場合、global_probe_preamble.shスクリプトによって変数$hostsが値"sys1:pw1 sys2:pw2"に設定されます。

  — 次の関数へのアクセスを提供します。

    – copy_and_run_on_multiple_hosts: 複数のリモートサーバーでシェルスクリプトをコピーして実行します。

    – copy_from_remote: リモートサーバーからファイルをコピーします。

    – copy_to_remote: リモートサーバーへファイルをコピーします。

    – run_on_multiple_hosts: 複数のサーバーで既存のコマンドを実行します。

    – run_on_single_host: 1つのサーバーで既存のコマンドを実行します。
- シェル変数: テストスクリプトでは、コマンドラインでname=valueオプションによって指定されたシェル変数を考慮します。
- 認証: スクリプトにより認証またはパブリック/プライベートキーの生成を設定します。グローバルテストでのパスワードを使用しないSSHのセットアップ (210ページ)を参照してください。

HCMグローバルテストの例

次のスクリプトでは、SAで使用されるファイルシステムの空きディスク容量をチェックします。このスクリプトは、run_all_probes.shコマンドのhostsオプションで指定されたコアサーバーで実行されます。

```
# Opsware SAのファイルシステム上で空き容量の割合をチェックします
# ライブラリと標準変数設定を読み込んで、
# コマンドラインを解析する。
/opt/opsware/oi_util/lib/global_probe_preamble.sh
MAX_PERCENTAGE=80
for filesystem in /opt/opsware /var/opt/opsware \
/var/log/opsware; do
#  次のprintfの前後のスペースは
#  読みやすくするために入れたもの
    printf " Checking $filesystem: "
    percent_free=`df -k $filesystem 2> /dev/null | \
           grep -v Filesystem | \
           awk '{print $5}' | \
           sed 's/%//'`
    if [ $percent_free -ge $MAX_PERCENTAGE ] ; then
        echo "FAILURE (percent freespace > $MAX_PERCENTAGE)"
        exit_code=1
    else
        echo "SUCCESS"
```

```
        exit_code=0
    fi
done
exit $exit_code
```

HCMグローバルテストのディレクトリレイアウト

グローバルテストが配置されているディレクトリレイアウトは、次のとおりです。

```
/opt/opsware/oi_util/
 |_bin
 | |_run_all_probes.sh
 | |_remote_host.py
 | |_<support_utility>
 | |_...
 | |_lib
 | |_global_probe_preamble
 |
 |_global_probes
   |
   |_verify_pre
   | |_<int><probe>.remote
   |
   |_verify_post
     |_int<probe>[.remote]
     |_ ...
```

HCMグローバルテストのディレクトリ

/opt/opsware/oi_utilディレクトリには、次のサブディレクトリがあります。

global_probes/verify_pre

このディレクトリには、指定されたサーバーがコアサーバーかどうかを特定するテストが含まれます。このカテゴリのグローバルテストでは、サーバーでSAのコンポーネントが実行されていないことや、サーバーが到達不能であることがわかると、そのサーバーに対するテストはそれ以上実行されません。

verify_preディレクトリでは、拡張子.remoteを持つテストのみが許可されます。

global_probes/verify_post

このディレクトリには、コア全体の特定要素の状況を確認するためのテストが含まれます。たとえば、このディレクトリに含まれる600_OPSWcheck_OS_resources
.sh.remoteスクリプトは、仮想メモリーやディスク容量などのリソースをチェックします。

システム診断の実行

ここでは、一連のシステム診断の実行手順について説明します。個別の診断テストの詳細については、システム診断テスト (217ページ) を参照してください。

システム診断テストを実行するには、システム診断のアクションのアクセス権が必要です。アクセス権の詳細については、アクセス権のリファレンス (249ページ) を参照してください。

診断テストを実行する際には、事前に正常性チェックモニターを実行することをお勧めします。手順については、コアの正常性チェックモニター (HCM) (206ページ) 、HCMローカルテストの実行 (207ページ) 、およびHCMグローバルテストの実行 (209ページ) を参照してください。

システム診断テストを実行するには、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ペインで、[管理] タブを選択します。

2 ナビゲーションペインで [ファシリティ] ノードを選択します。これにより、すべてのSAファシリティが表示されます。

3 診断テストを実行するファシリティを選択します。

4 [**アクション**] メニューを選択するか、右クリックで [**システム診断の実行**] を選択します。これにより、[プログラム拡張の実行] ウィンドウに、システム診断の拡張が表示されます。

5 **プログラムのプロパティ**: [次へ] を選択します。[オプション] ウィンドウが開きます。

6 **オプション**: 次のオプションを選択して、[次へ] を選択します。デフォルト設定をそのまま使用してテストを実行する場合は、[ジョブの開始] を選択します。

   a 診断テストを実行するファシリティを確認または変更します。

   b 実行するテストを選択します。テストの詳細については、システム診断テスト (217 ページ) を参照してください。

   c ジョブのタイムアウトを確認または設定します。ジョブが指定された時間内に完了しない場合、ジョブは中止されます。

7 **スケジュール設定**: システム診断ジョブをいつ実行するかを選択して、[次へ] を選択します。

8 **通知**: ジョブが終了したときに通知を受け取る電子メールアドレスを入力します。必要な通知のタイプを選択します。オプションで、ジョブに関連付けるチケットIDを入力して、[次へ] を選択します。

9 **ジョブステータス**: [ジョブの開始] ボタンと [ジョブのスケジュール] ボタンのいずれかを選択します。これにより、ジョブが即時実行されるか、スケジュールが設定されます。ウィンドウのバナーにジョブ ID が表示されます。このジョブIDは、[ジョブとセッション] タブでジョブを検索する際に使用します。

   ジョブが実行されると、診断テストが実行されて結果が表示されます。

10 ジョブステータスの任意の行を選択して、実行された診断テストの詳細を参照します。

11 [Ctrl+F] キーを押して検索バーを表示します。

12 詳細に分析する場合は、[すべての結果のエクスポート] を選択して、検索結果を含むファイルを作成します。結果はZIPファイル、テキストファイル、カンマ区切りファイルとして保存できます。

個別の診断テストの詳細については、システム診断テスト (217ページ) を参照してください。

システム診断テスト

システム診断ツールでは、SAコアコンポーネントの機能をチェックし、管理対象サーバーがSAコアとやり取りできることを確認します。SAの診断ツールを使用すると、SAコア内で発生するエラーのほとんどを解決することができます。

システム診断ツールは、最初にSAコアコンポーネントをテストした後に、必要に応じて、指定した管理対象環境内の任意のサーバーをテストします。システム診断ツールは、次のようにコアコンポーネントの機能を集中的にテストします。

- 単独テスト: 他のSAコンポーネントを使用せずに、コンポーネントの機能を可能な限りテストします。単独テストでは、ベースレベルの機能とコンポーネントがXML-RPCに応答できるかどうかを確認します。
- 総合テスト: すべてのコアコンポーネントのすべての機能をテストします。

総合テストが終了すると、システム診断ツールには、各テストの成否、テスト結果、失敗したテストのエラー情報が表示されます。

コアコンポーネントは決まった順序でテストされるわけではありませんが、通常は次の順序でテストが実行されます。

- コンポーネントの単独テスト
- コンポーネントの総合テスト

システム診断ツールでのコアコンポーネントのテスト

コンポーネントのテストでは、コンポーネントのすべての機能をシミュレートします。エラーだけでなく、各コンポーネントが一定の状況内で機能することを確認します (たとえば、データアクセスエンジンでデータベース接続数が最大近くになるかどうかなど)。

システム診断ツールでは、次のコンポーネントをテストします。

- モデルリポジトリ
- データアクセスエンジン
- ソフトウェアリポジトリ (およびワードストア)
- コマンドエンジン
- SAコアサーバー上のサーバーエージェント
- OS Build Manager
- モデルリポジトリ マルチマスターコンポーネント
- Webサービスデータアクセスエンジン

データアクセスエンジンのテスト

この項では、データアクセスエンジンの診断テストで実行されるテストについて説明します。

単独テスト

- データアクセスエンジンの現在のバージョンをチェックします。
- モデルリポジトリデータベースの現在のバージョンをチェックします。
- すべてのOracleオブジェクトが有効であることを確認します。
- Deviceオブジェクトを取得します。
- MegaDeviceオブジェクトを取得します。
- 高度なクエリの機能を確認します。
- Deviceオブジェクトを確認します。
- ファシリティのリストを取得します。
- データアクセスエンジンのcronbotジョブの名前を取得します。
- データベース接続の使用状況が許容レベル以下かどうかをチェックします。
- 600秒以上開いた状態になっているデータベース接続の有無をチェックします。
- データアクセスエンジンとモデルリポジトリが同じファシリティ内にあるかどうかをチェックします。
- モデルリポジトリがマルチマスターモードで実行されている場合に、モデルリポジトリのすべてのガベージコレクターが稼働していることを確認します。
- データアクセスエンジンがマルチマスターセントラルデータアクセスエンジンとして構成されている場合、次の内容をチェックします。

- マルチマスタートランザクションが発行されているかどうかをチェックします。
- マルチマスタートランザクションがリモートファシリティに反映されているかどうかをチェックします。
- マルチマスタートランザクションの競合をチェックします。

総合テスト

- 構成されたポートでモデルリポジトリとの接続をテストします。
- 構成されたポートでコマンドエンジンとの接続をテストします。
- 構成されたポートでソフトウェアリポジトリとの接続をテストします。

追加のデータベース権限によるエラー

Oracleデータベース (モデルリポジトリ) に権限 (アクセス権) が手動で追加されている場合、次のエラーメッセージが表示されることがあります。

```
Test Results: The following tables differ between the Data Access Engine
and the Model Repository: facilities.
```

この問題を修正するには、データベースへの権限の追加を取り消します。手順については、『SA Installation Guide』の「システム診断エラーのトラブルシューティング」を参照してください。

ソフトウェアリポジトリのテスト

この項では、ソフトウェアリポジトリの診断テストで実行されるテストについて説明します。

単独テスト

なし。

総合テスト

- 暗号化されたファイルを提供するソフトウェアリポジトリプロセスにパッケージではないファイルをアップロードできるかどうかをテストします。このテストでは、そのファイルがソフトウェアリポジトリのファイルシステム内に存在するかどうか、およびファイルサイズがソースと一致するかどうかを確認します。
- ファイルをソフトウェアリポジトリからダウンロードできることを確認します。
- 暗号化されていないファイルを提供するソフトウェアリポジトリプロセスが実行中でファイルを提供しているかどうかを確認します。
- 暗号化を使用せずにファイルのダウンロードを試みます。
- パッケージをソフトウェアリポジトリにアップロードできること、およびパッケージがモデルリポジトリに登録されていることを確認します。
- パッケージをソフトウェアリポジトリから削除してモデルリポジトリから削除できることを確認します。

Webサービスデータアクセスのテスト

この項では、Webサービスデータアクセスの診断テストで実行されるテストについて説明します。

単独テスト

- Webサービスデータアクセスエンジンに接続してバージョン情報を取得します。

総合テスト

- Webサービスデータアクセスエンジンに接続します。
- モデルリポジトリからサーバーレコードを読み取り、それによりモデルリポジトリへの接続をチェックします。

コマンドエンジンのテスト

この項では、コマンドエンジンの診断テストで実行されるテストについて説明します。

単独テスト

- 状態マシンをチェックします。
- セッションテーブルをチェックします。
- ロックダウンステータスをチェックします。
- 署名エラーをチェックします。
- コマンドテーブルとサービステーブルをチェックします。
- ファシリティキャッシュをチェックします。

総合テスト

- データアクセスエンジンの接続をチェックします。
- セキュリティ署名をチェックします。
- ロック操作をチェックします。
- 内部スクリプトを実行します。
- 外部スクリプトを実行します。

モデルリポジトリマルチマスターコンポーネントのテスト

この項では、モデルリポジトリマルチマスターコンポーネントの診断テストで実行されるテストについて説明します。

単独テスト

- 台帳ファイルを調べて台帳の状態をチェックします。
- 送信メッセージの合計数、台帳ファイル内に残っている（たとえば、すべてのリスナーで確認済みでない) メッセージの数、各リスナーで確認された最後のメッセージのシーケンス番号をレポートします。
- 送信モデルリポジトリマルチマスターコンポーネントの状態を調べて送信コンポーネントの正常性をチェックします。
- 受信モデルリポジトリマルチマスターコンポーネントの状態を調べて受信コンポーネントの正常性をチェックします。

総合テスト

なし。

第9章 SAのトラブルシューティング - ログファイル

SAコンポーネントは、ログファイルにイベントを記録します。コンポーネントのログファイルは、SAのトラブルシューティングに非常に有効なツールの1つです。SAコンポーネントとコンポーネントのログファイルについて理解しておくと、問題をすばやく解決することができます。また、サポート要求を申請したときに、HPサポートからログファイルやセッションデータファイルの送付を求められることもあります。

この項では、ログファイル、ログファイルの保管場所、およびトラブルシューティングでの利用方法について説明します。また、セッションデータファイルの作成方法についても説明します。

SAコンポーネントの内部名については、SAコアコンポーネントの内部名 (205ページ) を参照してください。

ログファイルの表示

ターミナルウィンドウでログファイルを表示するには、コンポーネントを実行しているサーバーにログインして、`more`、`less`、`grep`、または`vi`などのコマンドラインユーティリティを使用します。SAコンポーネントのログファイルの場所については、以下の項を参照してください。

➤ コンポーネントのログファイルは、コンポーネントがインストールされているサーバー上に存在します。

ログファイルの保管場所

通常、SAのログファイルは`/var/log/opsware`に保管されます。ただし、専用のディレクトリにログ記録するものや (Oracleなど)、syslogを使用するものもあります (NFSやDHCPDなど)。表31に、SAコンポーネントとそれぞれのログディレクトリを示します。この情報を利用すると、特定の問題の解決に役立つコンポーネントやログファイルを特定することができます。

表31 SAのログファイル

製品分野	SAコンポーネント	ログファイルのディレクトリ
データベース	モデルリポジトリ (truthまたはOracleデータベース)	`/u01/app/oracle`の下の各種ディレクトリ、または構成されたディレクトリ
データアクセス、API	データアクセスエンジン (spin)	`/var/log/opsware/spin`
	Webサービスデータアクセスエンジン (twist)	`/var/log/opsware/twist`
オブジェクトストレージ	ソフトウェアリポジトリ (word/wordcache)	`/var/log/opsware/mm_wordbot`
	Tsunami	`/var/log/opsware/tsunami`
	Memcached	`/var/log/opsware/memcached`

表31　SAのログファイル（続き）

製品分野	SAコンポーネント	ログファイルのディレクトリ
ジョブおよびセッション管理	コマンドエンジン (way)	/var/log/opsware/waybot
Global Shell、APX	Global File System、OGFS (hub)	/var/log/opsware/hub
	Global File System、OGFS (spoke)	/var/log/opsware/spoke
	APXプロキシ	/var/log/opsware/apxproxy
	その他	/var/log/opsware/adapter /var/log/opsware/ogfs /var/log/opsware/agentproxy /var/log (opswsshd)
メッシュの通信	エージェントゲートウェイ	/var/log/opsware/opswgw-agwsN-FACILITY
	コアゲートウェイ	/var/log/opsware/opswgw-cgwsN-FACILITY
	管理ゲートウェイ	/var/log/opsware/opswgw-mgwsN-FACILITY
フロントエンド	SA Webクライアント (occ)	/var/log/opsware/occ
	HTTPSプロキシ	/var/log/opsware/httpsProxy
メッシュの複製	モデルリポジトリマルチマスターコンポーネント (vault/OMB)	/var/log/opsware/vault
OSプロビジョニング	Build Manager	/var/log/opsware/buildmgr
	DHCPD	/var/log、またはsyslogにより構成
	Samba	/var/log/samba
	NFS	/var/log、またはsyslogにより構成
エージェントデプロイメント	エージェントキャッシュ	/var/log/opsware/agentcache
スタートアップ	SAのInitスクリプト	/var/log/opsware/startup
SAエージェント	SAエージェント	/var/log/opsware/agent

製品分野と関連するコンポーネントのログファイル

表31に記載した各コンポーネントの機能を理解しておくと、トラブルシューティングの際に最初に調べるコンポーネントやログを判断するのに役立ちます。多くの場合、エラーメッセージやトレースバックを含む問題の背景状況から、調査対象のログを判断することができます。

たとえば、エージェントの通信に関する問題のトラブルシューティングを行う場合には、すべてのメッシュの通信に1つ以上のゲートウェイが関与していて、いずれかのゲートウェイがダウンするか正常に機能していない場合は、メッシュの通信が影響を受けるということを理解することが重要です。

表32に、トラブルシューティングの際にチェックするSAの製品分野とログファイルを示します。

表32　製品分野と関連するコンポーネントのログファイル

製品分野	データベースのログ	データアクセスのログ	オブジェクトストレージのログ	ジョブ管理のログ	Global Shellのログ	メッシュ通信のログ	エージェントのログ
エージェントデプロイメント	X	X	X		X	X	X
監査とコンプライアンス	X	X	X	X	X	X	X
ソフトウェア管理での修復	X	X	X	X		X	X
パッチ適用	X	X	X	X		X	X
スクリプトの実行	X	X		X	X	X	X
アプリケーション構成	X	X		X		X	X
OSプロビジョニング	X	X		X	X	X	X
Global Shell、APX	X	X			X	X	X
アドホックなデバイス管理	X	X			X	X	X

ログファイルのサイズについて

ログファイルの最大サイズのデフォルト値は10 MBです。指定されたファイルの最大サイズに到達すると、追加のログファイルが作成されます。

コンポーネントのログレベルを上げると、多くの場合、デフォルトのログレベルよりもかなり速いペースでログファイルが増加するようになります。そのため、トラブルシューティング中の問題に関するログ情報を収集する場合に短期間だけログレベルを上げて、ログ情報の収集が済んだらデバッグレベルをデフォルト値に戻すことが重要です。

コンポーネントのログレベルについて

デフォルトで、ほとんどのSAコンポーネントはエラーと警告のみをログ記録するように構成されます。個別のコンポーネントでログレベルを一時的に上げることで、より詳細なメッセージを収集し、特定のコンポーネントで起きている問題の把握に役立てることができます。

ログレベルを上げるとオーバーヘッドが増加してパフォーマンスを損なう可能性があります。そのため、ログレベルを長期間上げたままにしないでください。ログレベルは問題の診断を行うときに一時的に上げて、それが済んだら元に戻します。

ログレベルを上げる際には、作業が済んだ後ですぐに戻せるように、元のログレベルを保存しておきます。構成ファイルを編集する際には、元の構成ファイルをバックアップして、作業が済んだら元に戻します。

一般にログレベルの名前は共通の形式に従います。

- TRACE
- DEBUG
- INFO
- WARNまたはWARNING
- ERROR
- FATAL
- FINEST

ログレベルの名前はコンポーネントによって異なることがありますが、ほとんどの場合、標準の命名方法に準拠しています。

コンポーネントのログレベルの変更

この項では、ログをサポートしている各種SAコンポーネントでのログレベルへの変更手順について説明します。メッシュ内には複数のコンポーネントインスタンスが存在する場合があります。そのため、複数のサーバー(SAコアやSAサテライトなど)でこれらの手順の実行が必要になることがあります。

ブートサーバーのログ

ブートサーバーは専用のログを生成しません。ブートサーバーは、TFTP (INETD)、NFSサーバー、ISC DHCPDのサービスを使用します。これらのサービスはすべて`syslog`でログ記録します。詳細については、ベンダードキュメントを参照してください。また、このコンポーネントのログ構成を確認するには、ブートサーバーの構成に使用した`syslog.conf`ファイルを参照してください。

Build Managerのログ

これらのログは、次のファイルに存在します。

```
/var/log/opsware/buildmgr/buildmgr.log
```

コマンドエンジンのログ

これらのログは、次のファイルに存在します。

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

ログレベルの変更

コマンドエンジンのログレベルを変更するには、ファイル /etc/opt/opsware/waybot/waybot.args を編集し、次の行を追加して目的のログレベルを指定します。

```
loglevel: DEBUG
```

この変更を有効にするには、コマンドエンジンを再開する必要があります。手順については、個別のSAコアコンポーネントの開始 (172ページ) を参照してください。

データアクセスエンジンのログ

これらのログは、次のファイルに存在します。

```
/var/log/opsware/spin/spin.err*
/var/log/opsware/spin/spin.log*
```

1つのコアに複数のデータアクセスエンジンがある場合、データアクセスエンジンを実行している各サーバーに、これらのログファイルが一組ずつ存在します。

HP Live Network (HPLN) のログ

これらのログは、次の場所に存在します。

```
/var/log/opsware/hpln
```

メディアサーバーのログ

これらのログは、次のファイルに存在します。

```
/var/log/opsware/samba/log.smbd
/var/log/opsware/samba/log.nmbd
```

SolarisおよびLinuxのOSプロビジョニングでは、NFSDなどのベンダーが提供するサービスを使用します。通常、これらのサービスはsyslogを使用してログ記録します。これらのログファイルの詳細については、ベンダードキュメントを参照してください。

モデルリポジトリのログ

モデルリポジトリはOracleデータベースです。データベースのログを保管する場所は、それぞれのインストールによって異なります。詳細については、『SA Installation Guide』の「Oracleログファイルの監視」を参照してください。

モデルリポジトリマルチマスターコンポーネントのログ

これらのログは、次のファイルに存在します。

```
/var/log/opsware/vault/err*
/var/log/opsware/vault/vault.n.log
```

ログ記録の変更

モデルリポジトリマルチマスターコンポーネントでログファイル名、ログファイルサイズ、またはログレベルを構成するには、SAクライアントの [管理] タブを選択し、ナビゲーションパネルで [システム構成] を選択した後に、モデルリポジトリマルチマスターコンポーネントを選択します。これにより、モデルリポジトリ

マルチマスターコンポーネントで使用できる、ログファイル、ログレベル、ログサイズのシステム構成パラメーターが表示されます。目的の値の設定が済んだら、[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。

また、モデルリポジトリマルチマスターコンポーネントのログレベルを変更する場合は、ファイル/etc/opt/opsware/vault/logging.propertiesを編集して、次の行を変更することもできます。

```
.level=INFO
```

ログレベルのデフォルト値はINFOです。

この変更を有効にするには、モデルリポジトリマルチマスターコンポーネントを再開する必要があります。手順については、個別のSAコアコンポーネントの開始 (172ページ) を参照してください。

エージェントのログ

エージェントでは、次のログファイルが管理対象サーバー上に作成されます。

UNIXの場合:

```
/var/log/opsware/agent/agent.log*
/var/log/opsware/agent/agent.err*
```

Windowsの場合:

```
%ProgramFiles%Common Files\opsware\log\agent\agent.log*
%ProgramFiles%Common Files\opsware\log\agent\agent.err*
```

SA クライアントログ

SAクライアントは専用のログを生成せず、JBossサーバーを使用して次のログファイルにログを書き込みます。

```
/var/log/opsware/occ/server.log*
/var/log/opsware/httpsProxy/*log*
```

ログレベルの変更

SA クライアントのログレベルを変更するには、/opt/opsware/occ/occ/conf/log4j.xml ファイルを編集し、目的の名前空間でorg.jboss.logging.XLevelの属性値を変更します。デフォルト値はINFOです。

この変更を有効にするには、SAクライアントを再開する必要があります。

ソフトウェアリポジトリのログ

これらのログは、次のファイルに存在します。

```
/var/log/opsware/mm_wordbot/wordbot.err*
/var/log/opsware/mm_wordbot/wordbot.log*
```

ログレベルの変更

ソフトウェアリポジトリのログレベルを変更するには、ファイル/etc/opt/opsware/mm_wordbot/mm_wordbot.argsを編集し、次のプロパティを目的のログレベルに変更します。

```
logLevel: logging.Level.INFO
```

たとえば、ログをデバッグに設定する場合は、この値を次のように設定します。

```
logLevel: logging.Level.DEBUG
```

この変更を有効にするには、ソフトウェアリポジトリを再開する必要があります。手順については、個別のSAコアコンポーネントの開始 (172ページ) を参照してください。

Webサービスデータアクセスエンジンのログ

Webサービスデータアクセスエンジンには、次のログファイルがあります。

```
/var/log/opsware/twist/stdout.log*
/var/log/opsware/twist/twist.log
/var/log/opsware/twist/access.log
/var/log/opsware/twist/server.log*
/var/log/opsware/twist/boot.log
/var/log/opsware/twist/watchdog.log
```

stdout.logファイルには、デバッグ出力とサーバーで生成されるすべての例外のログが含まれます。このファイルは特定の形式に準拠しません。*はlog.1、log.2、log.3などのファイルを表します。ファイルの数と各ファイルのサイズはいずれも、twist.confで構成できます。指定した最大ファイルサイズに到達すると、ログが追加で作成されます。stdout.logが最新で、stdout.log.1からstdout.log.5の順に古くなります。ファイルはスタートアップ時にもローテーションされます。このファイルには、System.out.println()、System.err.println()、e.printStackTrace()ステートメントの出力も含まれます。

twist.logファイルには、JBoss固有のエラーまたは情報提供メッセージおよびWeblogic固有のメッセージが含まれます。これらのファイルはスタートアップ時にローテーションされます。

access.logファイルには、共通のログ形式でアクセス情報が保管されます。これらのファイルはサイズが5MBに達するとローテーションされます。

server.logファイルには、Webサービスデータアクセスエンジンから生成されたデバッグメッセージが保管されます。デバッグメッセージは、パッケージで設定したログレベルまたはtwist.confファイルのクラスレベルで制御されます。*はlog.1、log.2、log.3などのファイルを表します。ファイルの数と各ファイルのサイズはいずれも、twist.confで構成できます。server.log.0は常に最新のファイルで、server.log.9が最も古いファイルです。

boot.logファイルには、Webサービスデータアクセスエンジンの開始時に生成されるstdoutメッセージとstderrメッセージに関する情報が保管されます。また、boot.logファイルには、Kill –QUITコマンドの出力も保管されます。

watchdog.logファイルは、Webサービスデータアクセスエンジンのステータスを1分ごとに記録します。

ログレベルの変更

Webサービスデータアクセスエンジンのログレベルを変更するには、ファイル/etc/opt/opsware/twist/twist.confを編集します。デフォルトログレベルまたは別のロガー名前空間で、ログレベルをWARNINGからFINESTや別の値に変更します。このファイルには、複数の名前空間が存在します。すべての名前空間または個別の名前空間のログレベルを変更することができます。

ゲートウェイのログ

これらのログは、次のファイルに存在します。

/var/log/opsware/<ゲートウェイ名>/opswgw.log*

<ゲートウェイ名>は特定のゲートウェイコンポーネントのディレクトリです。

ログレベルの変更

ゲートウェイコンポーネントのログレベルを変更するには、ファイル/etc/opt/opsware/<ゲートウェイ名>/opswgw.customを作成または編集し、次の行でログレベルを設定します。

```
opswgw.LogLevel=INFO
```

ログレベルを変更した後でゲートウェイを再開する必要があります。手順については、ゲートウェイプロセスの再開または停止 (136ページ) を参照してください。

Global File Systemのログ

OGFSのログは、次のファイルにあります。

```
/var/log/opsware/hub/OPSWhub.log*
/var/log/opsware/ogfs/ogsh.err*
/var/log/opsware/adapter/adapter.err*
/var/log/opsware/agentcache/agentcache.log
/var/log/opsware/spoke/spoke-*.log
/var/log/opsware/spoke/stdout.log
```

ログレベルの変更 - OGFSハブコンポーネント

OGFSのハブコンポーネントのログレベルを変更するには、次の手順を実行します。

1. Global Shell (OGSH) に管理ユーザーとしてログインします。手順については、『SAユーザーガイド: Server Automation』を参照してください。
2. ファイル/opsw/sys/hub/loglevelを確認して、現在のログレベルを特定します。たとえば、次のOGSHコマンドを実行します。

   ```
   more /opsw/sys/hub/loglevel
   ```

3. 次のOGSHコマンドを実行して、ログレベルを変更します。

   ```
   echo "MESSAGE ON" > /opsw/sys/hub/loglevel
   echo "LEVEL FINE" > /opsw/sys/hub/loglevel
   ```

デフォルト値は「MESSAGE OFF」と「LEVEL INFO」です。

ログレベルの変更 - OGFS Spokeコンポーネント

OGFS Spokeコンポーネントのログレベルを変更するには、ファイル/etc/opt/opsware/spoke/spoke_custom.confを編集します。次の行を変更するかこのファイルに追加して、目的のログレベルを設定します。

```
.level=INFO
```

ログレベルを変更した後でOGFS Spokeコンポーネントを再開する必要があります。手順については、個別のSAコアコンポーネントの開始 (172ページ) を参照してください。

HTTPSサーバープロキシのログ

これらのログは、次の場所にあります。

```
/cust/apache/servers/https-Proxy/logs
```

ログファイルssl_request_logはかなり大きくなる可能性があるため、使用可能なディスク容量が気になる場合は注意してください。

APXプロキシのログ

APXプロキシのログファイルは、/var/log/opsware/apxproxy/にあります。

ログレベルの変更

APX プロキシコンポーネントのログレベルを変更するには、ファイル /etc/opt/opsware/apxproxy/apxProxyOverides.conf を作成または編集します。次の行を追加または変更して、目的のログレベルを設定します。

```
.level = INFO
com.opsware.level=INFO
com.opsware.apxproxy.level=CONFIG
```

ログレベルを変更した後でAPXプロキシを再開する必要があります。手順については、個別のSAコアコンポーネントの開始 (172ページ) を参照してください。

これらのプロパティで使用できる値は、ファイル /etc/opt/opsware/apxproxy/apxProxy.conf に記載されています。

SSHDのログ

SSHDのログファイルはsyslogで構成された場所 (通常は/var/log) にあります

ログレベルの変更

SSHD コンポーネントのログレベルを変更するには、ファイル /etc/opt/opsware/sshd/sshd_conf を編集します。次の行を変更して、目的のログレベルを設定します。

```
LogLevel INFO
```

ログレベルを変更した後でSSHDを再開する必要があります。手順については、個別のSAコアコンポーネントの開始 (172ページ) を参照してください。

Global Shellの監査ログ

ユーザーがGlobal Shell機能を使用して管理対象サーバーにアクセスするか管理対象サーバーを変更すると、監査ログにイベントが記録されます。Global Shellの監査ログには、次のイベントに関する情報が含まれます。

- Global Shellおよびリモートターミナルセッションでのログインおよびログアウト
- Global Shellおよびリモートターミナルセッションで入力したコマンド
- 管理対象サーバーでのファイルシステム操作 (作成や削除など)
- リモートシェル (rosh) を介して管理対象サーバーで実行するコマンドおよびスクリプト

Global Shellの監査ログは、OGFSがインストールされているサーバーに存在します。

ログファイルを表示するには、ターミナルウィンドウを開き、OGFSを実行しているサーバーにログインして、more、grep、またはtailなどのコマンドラインユーティリティを使用します。tailコマンドを使用する例については、Global Shellの監査ログの監視の例 (233ページ) を参照してください。

Global Shellの監査ログは、次の3つのログファイルから成ります。

- シェルイベントログ
- シェルストリームログ

- シェルスクリプトログ

シェルイベントログ

シェルイベントログには、ユーザーがGlobal Shellで管理対象サーバーに対して実行した操作に関する情報が含まれます。これらのログは、次のディレクトリにあります (ogfs-hostはOGFSを実行しているサーバーの名前です)。

```
/var/opt/opsware/ogfs/mnt/audit/event/ogfs-host
```

ログファイル名の構文は、次のとおりです (nはログのローテーション番号です)。

```
audit.log.n
```

SAではイベントごとに、イベントログファイルに1つの行が書き込まれます。ログファイルの各行には、イベントに関する次の内容が記載されます。

- イベントの一意のID
- 親イベントの一意のID
- 操作の日付
- 操作を実行したSAユーザーのID
- 操作を実行したSAユーザーの名前
- 監査イベントを生成したコンポーネントの名前
- 監査イベントを生成したSAコンポーネントのバージョン
- 監査イベントを生成したSA機能の名前
- 操作 (アクション) の名前
- 詳細レベル
- イベントの終了ステータス
- 管理対象サーバーのID
- 管理対象サーバーの名前
- イベントの詳細

次の例は、監査イベントのログファイルの1つの行を表しています。

```
jdoe@m185:051202182224813:13  jdoe@m185:051202182224790:12
2006/01/28-12:40:19.622 User.Id=2610003 User.Name=jdoe
Hub:1.1 GlobalShell     AgentRunTrustedScript     1       OK
Device.Id=10003 Device.Name=m192.dev.opsware.com
ConnectMethod=PUSH      RemotePath=     RemoteUser=root
ScriptName=__global__.sc_snapshot.sh
ScriptVersion=30b.2.1572   ChangeTime=1128971572
RemoteErrorName=
```

この例の最初のフィールドは、次に示すイベントのIDです。

```
jdoe@m185:051202182224813:13
```

このIDフィールドの構文は、次のとおりです。

```
opsware-user@ogfs-host:YYMMDDHHmmssSSS:n
```

IDフィールドの末尾のnは、各セッション内で生成された監査イベントのシーケンス番号です。IDフィールドはシェルストリームログファイルの名前と同じです。

シェルストリームログ

シェルストリームログには、Global Shellから実行されたスクリプトのstdoutが含まれます。これらのログは、次のディレクトリにあります (ogfs-hostはOGFSを実行しているサーバーの名前です)。

```
/var/opt/opsware/ogfs/mnt/audit/streams/ogfs-host
```

ログファイル名の構文は、次のとおりです。

```
opsware-user@ogfs-host:YYMMDDHHmmssSSS:n
```

ログファイル名はシェルイベントログのIDフィールドと同じです。ログファイルのヘッダー行には、ファイル名、文字セット、バージョン、SAユーザー名が表示されます。スクリプトのstdoutに制御文字が含まれる場合、シェルストリームログにも同じ制御文字が含まれます。

シェルスクリプトログ

シェルスクリプトログには、Global Shellで実行されたスクリプトの内容が含まれます。これらのログは、次のディレクトリにあります (ogfs-hostはOGFSを実行しているサーバーの名前です)。

```
/var/opt/opsware/ogfs/mnt/audit/scripts/ogfs-host
```

ログファイル名は、次のようなスクリプトの内容に基づくハッシュ文字列です。

```
23f1d546cc657137fa012f78d0adfdd56095c3b5
```

ログファイルのヘッダー行には、ファイル名、文字セット、バージョン、SAユーザー名が表示されます。

Global Shellの監査ログの監視の例

次の例では、リモートターミナルセッションで管理対象サーバーにログインしたエンドユーザーが入力したコマンドを監視します。

1. ターミナルウィンドウで、rootとしてOGFSを実行しているコアサーバーにログインします。以下の手順では、このウィンドウを「監査ウィンドウ」と呼びます。
2. 監査ウィンドウで、次のaudit/eventディレクトリに移動します。

   ```
   cd /var/opt/opsware/ogfs/mnt/audit/event/ogfs-host
   ```

3. SAクライアントで、Unixの管理対象サーバーに対してリモートターミナルを開きます。
4. 監査ウィンドウで、次のコマンドを使用してaudit.logファイルの最後の行を調べます。

   ```
   tail -1 audit.log.n
   ```

   たとえば、audit.logファイルの次のエントリは、SAユーザー jdoeがホスト (Device.Name) toro.example.comに対してリモートターミナルを開いたことを示します。イベントIDは jdoe@m235:060413184452579:59です。

   ```
   jdoe@m235:060413184452595:60 jdoe@m235:060413184452579:59 2006/04/
   13-18:44:52.728 User.Id=6220044 User.Name=jdoe Hub:1.1
   GlobalShellAgentLogin 1 OK Device.Id=840044 Device.Name=toro.example.com
   ConnectMethod=JUMP RemotePath= RemoteUser=root
   ```

5. 監査ウィンドウで、次のaudit/streamsディレクトリに移動します。

   ```
   cd /var/opt/opsware/ogfs/mnt/audit/streams/ogfs-host
   ```

6. 監査ウィンドウで、tail -fコマンドを使用して、リモートターミナルセッションに対応するファイルを監視します。ファイル名はイベントIDと同じです。たとえば、イベントIDが jdoe@m235:060413184452579:59である場合には、次のコマンドを入力します。

```
tail -f jdoe*59
```

7 リモートターミナルウィンドウで、pwdやlsなどのUNIXコマンドを入力します。

8 監査ウィンドウを注視します。リモートターミナルセッションからのコマンド（および出力）がaudit/streamsディレクトリのファイルに書き込まれます。

Global Shellの監査ログのデジタル署名

シェルストリームログファイルとシェルスクリプトログファイルには、RSA-SHA1アルゴリズムで生成されるデジタル署名とフィンガープリントが含まれます。ログファイルの署名とフィンガープリントを確認するには、ターミナルウィンドウを開き、OGFSにログインして、次のコマンドを入力します。

```
/opt/opsware/agentproxy/bin/auditverify stream_file_name  \
rsa_key_path
```

これはbashの場合の例です。

```
STREAMDIR=/var/opt/opsware/ogfs/mnt/audit/streams/acct.opsw.com
STREAMFILE=jdoe@somehost:051210003000111:61
RSAKEYPATH=/var/opt/opsware/crypto/waybot/waybot.srv

/opt/opsware/agentproxy/bin/auditverify $STREAMDIR/$STREAMFILE \ $RSAKEYPATH
```

ログファイルが改ざんされていない場合、auditverifyに次のメッセージが表示されます。

```
[AuditVerify]: Verification Result:Valid Signature
```

デフォルトで、ログは次のファイルのプライベートキーで署名されます。

```
/var/opt/opsware/crypto/agent/agent.srv
```

署名に使用するキーファイルを変更するには、Global Shellの監査ログの構成 (235ページ)の手順に従って、audit.signature.key_pathシステム構成パラメーターを変更します。

Global Shellの監査ログのストレージ管理

SAでシェルストリームログファイルやシェルスクリプトログファイルを定期的に削除すると、これらのファイルによって使用可能なディスク容量が占有されるのを防ぐことができます。SAには、ログファイルを削除する場合を特定するシステム構成パラメーターが用意されています。これらのパラメーターでは、ログファイルの経過日数 (archive_days) やファイルが使用するディスク容量 (archive_size) に基づいてファイルの削除を指定することができます。

次のパラメーターでは、削除するファイルの経過日数を指定します。

```
audit.stream.archive_days
audit.script.archive_days
```

次のパラメーターでは、ファイルを削除する上限のディスク容量を指定します。

```
audit.stream.archive_size
audit.script.archive_size
```

これらのパラメーターの詳細については、表33を参照してください。これらのシステム構成を変更する手順については、Global Shellの監査ログの構成 (235ページ) を参照してください。

表33　Global Shellの監査ログ構成のパラメーター

パラメーター	説明	デフォルト値
audit.script.archive_days	この値 (日数) よりも古い監査スクリプトファイルが削除されます。0の場合、ファイルは削除されません。	100
audit.script.archive_size	すべての監査スクリプトファイルで使用するディスク容量の最大値 (MB)。古いファイルから削除されます。0の場合は最大値なしです。	100
audit.signature.algorithm	監査ストリームを署名する際に使用する署名アルゴリズム。	RSA-SHA1
audit.signature.key_path	監査ストリームを署名する際に使用するプライベートキーの場所。	/var/opt/opsware/crypto/waybot/waybot.srv
audit.stream.archive_days	この値 (日数) よりも古い監査ストリームファイルが削除されます。0の場合、ファイルは削除されません。	10
audit.stream.archive_size	すべての監査ストリームファイルで使用するディスク容量の最大値 (MB)。古いファイルから削除されます。0の場合は最大値なしです。	1000
audit.stream.file_keep	ローテーションする監査ストリームファイルの最大数。	50
audit.stream.file_size	監査ストリームの最大ファイルサイズ。MB単位で指定します。指定できる最大値は50MBです。	10

Global Shellの監査ログの構成

ログファイルの最大サイズなど、Global Shellの監査ログの一部のシステム構成パラメーターを変更することができます。変更可能なパラメーターについては、235ページの表33を参照してください。パラメーターを構成するには、次の手順を実行します。

1. SAクライアントで [**管理**] タブを選択します。
2. 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。
3. SAコンポーネントのリストで、ハブを選択します。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。

4 変更対象のシステム構成パラメーターを変更します (235ページの表33を参照)。

5 [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。

セッションデータの抽出

SA ではジョブに関する背景状況などの情報が保存されます。ジョブは「way セッション」または単に「セッション」ともいいます。デフォルトで、このセッションデータは 7 日間保管され、その後、ディスク容量を再利用するためガベージコレクションが行われます。このデータは、ジョブやセッションの問題のトラブルシューティングに役立ちます。また、有効なセッションデータを保存して、問題のあるケースとの比較を行うこともできます。

dump_sessionツールを使用すると、この情報を抽出して保存できます。dump_sessionツールでは、Session<ジョブID>.pkl.gzという名前のファイルにセッションデータを含むTAR書庫ファイルが生成されます。

この項では、dump_session ツールとこのツールを使用してセッションデータを抽出する手順について説明します。

SAジョブのセッションデータを取得するには、次の手順を実行します。

1 問題のあるジョブまたはコマンドのジョブIDの数値を特定します。ジョブの場合は、SAクライアントで [ジョブとセッション] タブを選択して、目的のジョブを特定します。ジョブIDは [ジョブID] 列に表示されます。

2 SAコアサーバーにログインします。

3 dump_sessionツールを実行し、最初の引数としてジョブIDを指定します。例:

```
# /opt/opsware/bin/dump_session <ジョブID>
```

4 セッション出力を保存します。セッション出力は現在の作業ディレクトリに Session<ID>.pkl.gz という名前のTAR書庫として保存されます。

5 HPサポートから要求された場合は、問題のサポートインシデントにTAR書庫をアタッチします。

最近のセッションの表示

最近のジョブを表示するには、-lオプションを使用して dump_session を実行し、表示するジョブの数を指定します。たとえば、次のコマンドでは、最近の25件のジョブが表示されます。

```
# /opt/opsware/bin/dump_session -l 25
```

-lで表示されるジョブの数はデフォルトで10件です。

次の例では、5つのセッションを出力しています。

```
# /opt/opsware/bin/dump_session -l 5
Session ID | Start Date        | Session Desc
26000001   | 20100902T12:00:01 | 'Automated Communications Test for core 1'
25980001   | 20100902T15:00:00 | 'opsware.patch_compliance'
26030001   | 20100902T17:51:57 | 'Communication Test'
25990001   | 20100903T00:00:00 | 'Automated Hypervisor Scan for core:1'
26010001   | 20100903T00:00:01 | 'Automated Communications Test for core 1'
```

サンプル出力

次のサンプルは、dump_sessionコマンドとSAジョブID 1870001の出力の例です。

```
# /opt/opsware/bin/dump_session 1870001
Dumping session to 'Session1870001.pkl.gz'
Session:1870001
MegaServiceInstance:20001
WayScriptVersion:1830001
SecurityUser:60001
Realm:0
Device:10001
WayScript:1830001
```

dump_sessionコマンドリファレンス

この項では、dump_sessionコマンドの構文とオプションについて説明します。dump_sessionコマンドは、/opt/opsware/bin/dump_sessionにあります。このコマンドは、SAデータベースからSAのセッションと関連するコマンドを抽出してフォーマット化します。

構文

```
dump_session [<session_id> ...][<session_file> ...][-h] [-l <num>]
[-d<num>]
```

オプション

表34では、dump_sessionコマンドのオプションについて説明します。

表34　　dump_sessionのオプション

オプション	説明
<session_id>	1つまたは複数のSAジョブIDを指定します。これらのジョブに関する情報は、SAデータベースから現在の作業ディレクトリの「<session_id>.pkl.gz」という名前のgzip形式で圧縮された複数のpickleファイルにコピーされます。
<session_file>	以前に保存した1つまたは複数の<session_id>.pkl.gzファイルを指定します。これらのファイルは処理されて、waybotのバックエンドWeb UIに似た静的なHTMLディレクトリ構造に変換されます。
-h	ヘルプ情報を表示します。
-l <num>	メッシュ内の各コアで実行された最後の<num>件のSAジョブをstdoutに表示します。<num>を省略した場合は10件が表示されます。<num>を省略できるのは、-lがコマンドラインの最後の引数である場合に限られます。
-d<num>	デバッグレベルを指定した番号に設定します。

第10章 SAの通知の構成

この項では、SA クライアントヘルプの連絡先情報を変更して、コアのメールサーバーの構成やコアの電子メールアラートの設定などを行うための、ユーザー定義可能な構成パラメーターについて説明します。

通常、構成パラメーターは、SAコアのインストールのインタビュープロセスで指定されます。詳細については、『SA Installation Guide』を参照してください。

各種システム構成パラメーターのデフォルト値の多くは、技術サポート担当またはコンサルタントから指示された場合以外は、変更しないでください。

サーバーエージェントがシステム構成の値を読み込むのはインストール時のみです。構成の値を変更する場合は、すべてのエージェントの構成を手動で更新する必要があります。このような変更やSAのシステム構成のその他の変更に関してサポートが必要な場合は、HP Server Automationのサポート担当までご連絡ください。

SAヘルプでのSA管理者の連絡先情報の構成

Server Automationヘルプページに表示されるSA管理者の連絡先情報を構成するには、次のタスクを実行します。

1. コアのコマンドセンター (OCC) を実行しているサーバーにrootとしてログオンします。
2. 次のディレクトリに移動します。

   ```
   /etc/opt/opsware/occ
   ```
3. テキストエディターで`psrvr.properties`ファイルを開きます。
4. 次のフィールドの値を変更して、SAクライアントヘルプの連絡先情報を指定します。

   ```
   pref.occ.support.href
   ```

   ```
   pref.occ.support.text
   ```
5. ファイルを保存してエディターを終了します。
6. 次のコマンドを入力して、OCCを再起動します。

   ```
   /etc/init.d/opsware-sas restart occ.server
   ```

ファシリティのメールサーバーの構成

SAコアコンポーネントでは、システム構成パラメーターopsware.mailserverを使用して、電子メール通知に使用するメールサーバーのアドレスを指定します。デフォルトで、opsware.mailserverの値はsmtpになります。値を指定しない場合は、この値が使用されます。ほとんどのシステムでは、この値を使用できます。

opsware.mailserverに別の値を指定する必要がある場合は、次の手順を実行します。

1. SAクライアントで[**管理**]タブを選択します。
2. 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。
3. SAコンポーネントのリストで、[ファシリティ]を選択します。選択したファシリティのシステム構成パラメーターが表示されます。
4. パラメーター opsware.mailserverを探します。
5. [値]列で、新しい値を直接入力するか、または新しい値ボタン  を選択してメールサーバーのホスト名を入力します。
6. [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。

コマンドエンジンの通知電子メールの構成

1. SAクライアントで[**管理**]タブを選択します。
2. 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。
3. SAコンポーネントのリストで、[コマンドエンジン]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。
4. パラメーター way.notification.email.fromAddrを探します。
5. [値]列で、新しい値を直接入力するか、または新しい値ボタン  を選択して、スケジュール済みのジョブに関する通知をコマンドエンジンからユーザーに送信する電子メールメッセージの“from”アドレスを入力します。
6. [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。
7. 次のコマンドを入力して、コマンドエンジンコンポーネントを再開します。

   ```
   /etc/init.d/opsware-sas restart occ.server
   ```

8. SAをマルチマスターモードで実行している場合は、モデルリポジトリマルチマスターコンポーネントを再開します。

   複数のSAコンポーネントを再開する際には、正しい順序で再開する必要があります。スタンドアロンSAコアの開始 (171ページ) を参照してください。

SAコアでの電子メールアラートアドレスの構成

サーバーエージェントがシステム構成の値を読み込むのはインストール時のみです。構成の値を変更する場合は、すべてのエージェントの構成を手動で更新する必要があります。このような変更やSAのシステム構成のその他の変更に関してサポートが必要な場合は、HP SAサポート担当までご連絡ください。

電子メールアラートアドレスを構成するには、次の手順を実行します。SAコアのインストールでは、これらのパラメーターにデフォルト値 (EMAIL_ADDR) が使用されます。

1. SAクライアントで [**管理**] タブを選択します。
2. 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。
3. SAコンポーネントのリストで、[SAエージェント] 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。
4. 必要に応じて、次のパラメーターを変更します。
   - cronbot電子メールアラートを有効にするには、パラメーター CronbotMailAlertsEnabledに、値1を指定します。cronbot電子メールアラートを無効にする場合は、値0を指定します。
   - パラメーター CronbotAlertAddress に、サーバーエージェントが失敗したスケジュール済みのジョブに関するアラートを受信者に送信するのに使用する電子メールアドレスを入力します。
5. [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。

マルチマスターメッシュでの電子メールアラートアドレスの構成

マルチマスターアラート用に電子メールアラートアドレスを構成するには、次の手順を実行します。SAコアのインストールでは、これらのパラメーターにデフォルト値 (EMAIL_ADDR) が使用されます。

1. SAクライアントで [**管理**] タブを選択します。
2. 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。
3. SAコンポーネントのリストで、[モデルリポジトリ、マルチマスターコンポーネント] 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。
4. 必要に応じて、次のパラメーターを変更します。
   - フィールドsendMMErrorsToに、マルチマスターの競合の送信先の電子メールアドレスを入力します。
   - フィールド sendMMErrorsFrom に、マルチマスターの競合に関するアラート電子メールの「from」アドレスとして使用する電子メールアドレスを入力します。
5. [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。

マルチマスターメッシュ内のすべてのSAコアでモデルリポジトリマルチマスターコンポーネントを再開します。個別のSAコアコンポーネントの開始 (172ページ) を参照してください。

第11章 Global Shell:Windowsサブ認証パッケージ

Microsoft® Windowsでは、ユーザーアカウントのパスワードを提示することなく、プログラム(サービスまたはアプリケーション)でそのユーザーアカウントのログインセッションのハンドルを取得することはできません。ユーザー名とパスワードの両方がないと、実行中のプログラムは現在使用中のID以外のユーザーとして操作を行うことができません。

この制約はSAエージェントにも当てはまります。SAエージェントは、LocalSystemのセキュリティコンテキストで実行するようにインストールされます。LocalSystemのログオンセッションは、Windows Server 2003/2008/2012オペレーティングシステムを実行しているすべてのWindowsサーバーで起動時に作成される、信頼された特殊な特権付きセキュリティコンテキストです。ただし、SAエージェントが別のユーザー(<ドメイン>\<ユーザー名>など)のセキュリティコンテキストで子プロセスを実行する必要がある場合には、そのユーザーアカウントのパスワードが必要になります。ユーザー名、パスワード、子プログラム名はすべてWin32 APIの`LogonUser()`に渡されます。

SAエージェントは、SAのGlobal Shell機能により、管理対象サーバー上でアクションを実行します。SAユーザーは、Global Shell機能とSAエージェントを使用して、管理対象サーバー上でレジストリ読み取り操作、ファイル作成、参照操作を実行できます。SAユーザーがLocalSystemユーザーとして操作を実行する必要がある場合、SAエージェントはそのエージェントのセキュリティコンテキストで実行されるサブプロセスを作成するだけで済みます。SAユーザーが非LocalSystemユーザーとしてGlobal Shellの操作を実行する必用がある場合、ユーザーアカウントのパスワードが必要になるため、エージェントでWin32 APIの`LogonUser()`を使用することはできません。Global Shellの操作の詳細については、『SAユーザーガイド: Server Automation』を参照してください。

Microsoft Windowsの認証プロセス

Microsoft Windowsの認証は、ユーザーがシステムへのアクセスを許可されているかどうかを確認するプロセスです。この確認プロセスで、ユーザーはパスワードを提供します。パスワードは暗号ハッシュ化されます。その後、ハッシュ化された値を保管されている値と比較します。

Windowsでは、さまざまな形式の認証に対応したサブシステムが利用できます。このサブシステムは、Microsoft® Windows Local Security Authority Subsystem (LSASS)と呼ばれ、Windowsサーバー上でlsass.exeアプリケーションを実行するプロセスとして機能します。

LSASSは、Windowsで複数の認証パッケージをサポートできるように設計されています。これらの認証パッケージでは、パスワード、Kerberosトークン、指紋、網膜パターンなどの確認を行います。

Windows NT4の標準インストールの場合、LSASSにはMSV1_0と呼ばれる1つの認証パッケージが含まれます。MSV1_0はNT4ドメイン認証を実装する認証パッケージです。ユーザー名、パスワード、ドメイン名を入力してWindows NT4サーバーにログインするときや、Windows NT4サーバーで共有をマウントするときには、MSV1_0認証パッケージとやり取りします。Windows 2000サーバーの場合、一連の標準認証パッケージはMSV1_0とKerberosで構成されます。ドメイン構成によって異なりますが、ログインを行う際にユーザーはいずれかの認証パッケージとやり取りします。Windows Server 2003/2008/2012の場合も、MSV1_0とKerberosを認証パッケージとして使用することができます。

Microsoft Windowsのサブ認証パッケージ

Microsoft Windows のメインの認証パッケージはすべて、サブ認証パッケージと呼ばれるコードへの資格情報チェックの委任をサポートしています。サブ認証パッケージはDLLで、メインの認証パッケージで使用する認証および検証基準の一部を補完するか置き換えます。

MSV1_0認証パッケージでは、(クライアントの要求に基づいて) ユーザー名とパスワードの確認を以前に登録したサブ認証パッケージに委任することができます。デフォルトで、MSV1_0は専用の内部ユーザー名とパスワードを使用してソフトウェアをチェックします。Windowsクライアント (SAエージェントなど) で特定のサブ認証モジュールが要求される場合に限り、MSV1_0はそのモジュールに委任します。

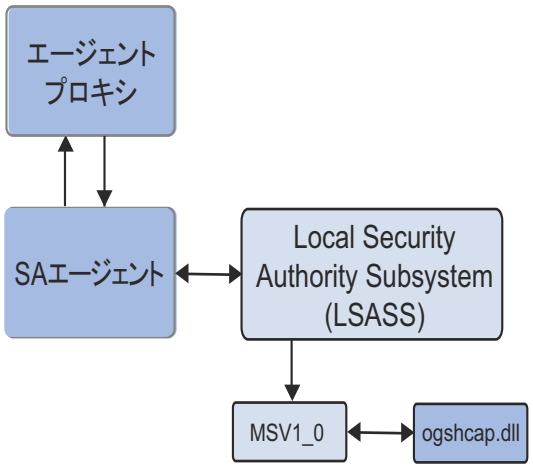
SAのサブ認証パッケージ

SAでは、SAエージェントでGlobal Shell操作 (子プロセスなど) を実行するためのユーザーを認証する際に、エージェントが要求するMSV1_0サブ認証パッケージを提供します。このサブ認証パッケージは、ogshcap.dllというDLLです (ogshcap はGlobal Shell Custom Authentication and Subauthentication Packageを表しています)。

ogshcap.dllファイルには、クライアントアプリケーションによってWindowsに提供される資格情報が渡されます。このDLLは、サポートされるすべてのWindowsオペレーティングシステム (Windows Server 2003/2008/2012) で使用され、それぞれのオペレーティングシステムで同じ方法で使用されます。

図37にSAのサブ認証プロセスを示します。

図37　　SAのサブ認証プロセスの流れ



SAエージェントの場合、特殊なWindows APIを呼び出してSAサブ認証パッケージ (ogshcap.dll) によるサブ認証を要求する際に、エージェントからNULLパスワードをユーザー名とともに渡します。その後、このWindows APIはMSV1_0認証パッケージを呼び出し、このMSV1_0認証パッケージからNULLパスワードを含む資格情報が要求されたサブ認証パッケージに渡されます。

SAのサブ認証パッケージは、ユーザーアカウントがロックされていないことやアカウントが無効ではないことを確認します。また、要求元のクライアントがSAエージェントであることを確認します。このDLLは空(NULL)のパスワードフィールドを無視します。サブ認証パッケージの確認手順が済んだら、DLLはMSV1_0に成功のステータスを返します。MSV1_0によってログインセッションが作成され、LSASSに渡されます。LSASSは、このログインセッションに対するハンドルをSAエージェントに渡します。このログインセッションに対するハンドルは、SAエージェントによってWin32 APIの`CreateProcessAsUser()`に渡され、非LocalSystemユーザーのIDで子プロセスが実行されます。

ogshcap.dllファイルを使用して1つのサブ認証操作を実行するように要求された場合、Windowsはこのファイルを開いて、サーバーが次に再起動されるまで、このファイルを開いたままにします。このため、次に再起動するまでにogshcap.dllファイルが削除されたり、再起動せずにエージェントのインストールやアップグレードを実行したときにファイルが上書きされたりすることはありません。

すべてのWindowsオペレーティングシステムで、認証対象のセキュリティプリンシパルのユーザー名はローカルサーバー上のAdministratorsグループのメンバーか、サーバーが属するプライマリドメインのDomain Adminsグループのメンバーである必要があります。

SAエージェントのインストールの変更

いずれのWindowsオペレーティングシステムの場合でも、SAエージェントをインストールすると、次のレジストリキーに新しいWindowsレジストリ値が作成されます(存在しない場合)。

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0

新しく作成されるレジストリ値の種類はREG_SZで、次の内容が含まれます。

- **Name**: Auth155
- **Value**: ogshcap

SAエージェントインストーラーにogshcap.dllファイルが含まれています。エージェントのインストール時に、ogshcap.dllファイルは次のソースディレクトリにコピーされます。

```
%SystemDrive%:\Program Files\Opsware\bin\ogshcap.dll
```

DLLファイルがこのディレクトリに作成された後に、エージェントインストーラーは次のターゲットディレクトリにファイルをコピーしようとします。

```
%SystemRoot%\system32\ogshcap.dll
```

ターゲットディレクトリに該当するファイルが存在しない場合、コピーは正常に行われます。使用中のファイルが存在してコピーできない場合、エージェントインストーラーはソースファイルとターゲットファイルの暗号ハッシュを計算します。ソースファイルとターゲットファイルのハッシュが異なる場合、エージェントインストーラーはWin32 APIの`MoveFileEx()`を呼び出し、これにより、Windows内部のレジストリキーが作成されます。このレジストリキーにより、次の再起動時にターゲットファイルをソースファイルで置き換える必要があることがWindowsに通知されます。

一方または両方のDLLファイルのハッシュを正しく計算できない場合、エージェントインストーラーはDLLを置き換える必要があるとみなします。たとえば、エージェントインストーラーでMicrosoftの暗号モジュールをロードできない場合、ハッシュを計算することはできません。この場合、エージェントインストーラーは、DLLの置き換えが必要であるとみなします。

エージェントインストーラーのコマンドラインでインストーラーオプション(`--reboot`)を指定すると、エージェントのインストール後に再起動を行うことができます。

インストール後に再起動してDLLの最新バージョンを取得する必要がある場合は、再起動によって移動操作が実行され、ソースディレクトリのDLLがターゲットディレクトリに移動されます。これにより、ソースDLLファイルによってターゲットDLLが上書きされます。

オペレーティングシステム上の既存のogshcap.dllを置き換える必要があり、このために再起動が必要な場合でも、エージェントインストーラーは(デフォルトで)再起動を行いません。再起動が行われるのは、インストールを実行する人がコマンドラインオプションとして`--reboot`を指定した場合だけです。

どのオペレーティングシステムでもエージェントインストーラーで--rebootを指定することはできますが、再起動が実行されるのはWindowsオペレーティングシステムだけです。たとえば、Linux 7.2オペレーティングシステムでエージェントをインストールする際に--rebootオプションを指定しても、エージェントインストーラーによる再起動は行われません。しかし、Windows 2000オペレーティングシステムでエージェントをインストールする際に--rebootオプションを指定すると、エージェントインストーラーによって再起動が行われます。

ハッシュが計算されて、ソースファイルとターゲットファイルが同じであると確認された場合、開いているogshcap.dllファイルに対する上書きは行われません。

エージェントは常にogshcap.dllの初回インストールを実行するか、またはエージェントインストーラーに含まれるDLLのバージョンで既存のDLLを上書きすべきかどうかの分析を行います。この場合、エージェントインストーラーによってこのDLLのインストールを止める方法はありません。

エージェントインストーラーで再起動が必要であることが示され、エージェントのインストール後に再起動が行われない場合、SAエージェントは再起動が実行されるまで古いバージョンのDLLを使用します。この場合、再起動が行われるまでは、SAエージェントで新しいDLLで提供されるバグ修正や機能修正を利用することはできません。ただし、新しいDLLへの置き換えが必要な場合でも、SAエージェントのWindows認証は古いDLLを使用して正常に実行されます。

次のエージェントインストーラーのサンプルログは、ogshcap.dllのインストールによるものです。この場合、オペレーティングシステム上の既存のDLLを置き換える必要はありません。

```
[08/Jun/2005 20:59:18] [INFO] Install CAP file if differing checksum between
new and existing file.
[08/Jun/2005 20:59:18] [TRACE] NeedToReplaceOGSHCAPDLL()
[08/Jun/2005 20:59:18] [INFO] Testing CAP file existence:
C:\WINDOWS\system32\ogshcap.dll
[08/Jun/2005 20:59:18] [INFO] C:\WINDOWS\system32\ogshcap.dll CAP file exists
[08/Jun/2005 20:59:18] [TRACE] GenerateKeyToFile()
[08/Jun/2005 20:59:18] [TRACE] Successfully called CreateFile(C:\Program
Files\Common Files\Opsware\cogbot\hmac.key)
[08/Jun/2005 20:59:18] [TRACE] Key file already exists
[08/Jun/2005 20:59:18] [TRACE] C:\Program Files\Common
Files\Opsware\cogbot\hmac.key size:36 bytes
[08/Jun/2005 20:59:18] [TRACE] Successfully called CloseHandle(C:\Program
Files\Common Files\Opsware\cogbot\hmac.key)
[08/Jun/2005 20:59:18] [TRACE] GenerateKeyToFile() = 1
[08/Jun/2005 20:59:18] [INFO] Calculate MAC for File:
C:\WINDOWS\system32\ogshcap.dll
[08/Jun/2005 20:59:18] [TRACE] C:\WINDOWS\system32\ogshcap.dll size:40960
bytes
[08/Jun/2005 20:59:18] [TRACE] C:\Program Files\Common
Files\Opsware\cogbot\hmac.key size:36 bytes
[08/Jun/2005 20:59:18] [TRACE] Successfully called CreateFileMapping() for
C:\WINDOWS\system32\ogshcap.dll
[08/Jun/2005 20:59:18] [TRACE] Successfully called CreateFileMapping() for
C:\Program Files\Common Files\Opsware\cogbot\hmac.key
[08/Jun/2005 20:59:18] [TRACE] CalculateMAC()
[08/Jun/2005 20:59:18] [TRACE] PrintHexBytes()
[08/Jun/2005 20:59:18] [TRACE] HMAC for C:\WINDOWS\system32\ogshcap.dll:0x02
0x95 0x2B 0x03 0x51 0x02 0x9F 0x6D 0x58 0xF6 0xF1 0x5E 0x1C 0xFC 0x2A 0x72
0x5D
0x7E 0x5F 0xDA
[08/Jun/2005 20:59:18] [TRACE] CalculateMACFromFile() = 1
[08/Jun/2005 20:59:18] [INFO] Calculate MAC for File:C:\Program
Files\Opsware\bin\ogshcap.dll
```

```
[08/Jun/2005 20:59:18] [TRACE] C:\Program Files\Opsware\agent\bin\ogshcap.dll
size:
40960 bytes
[08/Jun/2005 20:59:18] [TRACE] C:\Program Files\Common
Files\Opsware\cogbot\hmac.key size:36 bytes
[08/Jun/2005 20:59:18] [TRACE] Successfully called CreateFileMapping() for
C:\Program Files\Opsware\agent\bin\ogshcap.dll
[08/Jun/2005 20:59:18] [TRACE] Successfully called CreateFileMapping() for
C:\Program Files\Common Files\Opsware\cogbot\hmac.key
[08/Jun/2005 20:59:18] [TRACE] CalculateMAC()
[08/Jun/2005 20:59:18] [TRACE] PrintHexBytes()
[08/Jun/2005 20:59:18] [TRACE] HMAC for C:\Program
Files\Opsware\agent\bin\ogshcap.dll:0x02 0x95 0x2B 0x03 0x51 0x02 0x9F 0x6D
0x58
0xF6 0xF1 0x5E 0x1C 0xFC 0x2A 0x72 0x5D 0x7E 0x5F 0xDA
[08/Jun/2005 20:59:18] [TRACE] CalculateMACFromFile() = 1
[08/Jun/2005 20:59:18] [INFO] C:\WINDOWS\system32\ogshcap.dll CAP file does
not
need to be replaced
[08/Jun/2005 20:59:18] [TRACE] NeedToReplaceOGSHCAPDLL() = 0
[08/Jun/2005 20:59:18] [TRACE] UpdateCAPRegistrySetting()
[08/Jun/2005 20:59:18] [INFO] Update SubAuthentication Package Registry key
[08/Jun/2005 20:59:18] [TRACE] Successfully opened registry key
SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0.
[08/Jun/2005 20:59:18] [TRACE] Successfully found registry value:'Auth255'
at
this key, retrieved value 'ogshcap' (8) bytes.
[08/Jun/2005 20:59:18] [TRACE] Existing registry value matches expected
value:
'ogshcap'
[08/Jun/2005 20:59:18] [TRACE] UpdateCAPRegistrySetting() = 1
[08/Jun/2005 20:59:18] [INFO] UpdateCapRegistrySetting() was successful
[08/Jun/2005 20:59:18] [TRACE] Win32InstallN() = 1
[08/Jun/2005 20:59:18] [INFO] Installation completed successfully.
[08/Jun/2005 20:59:18] [INFO] An Agent install time reboot is NOT needed.
```

SAエージェントのアンインストールの変更

SAエージェントのアンインストール時に、Windowsアンインストーラーは次のファイルを削除しようとします。

```
%SystemRoot%\system32\ogshcap.dll
```

(ファイルが開いていてWindowsで使用されているために)ファイルを削除できない場合、アンインストーラーは`MoveFileEx()`を呼び出して、次回の再起動時にファイルを削除するようにWindowsに指示します。ファイルを削除できない場合は、すぐに再起動を実行する必要があるかどうかをユーザーに通知するメッセージがアンインストーラーに表示されます。

また、エージェントのインストール時に作成された特殊なサブ認証レジストリキーの値もアンインストーラーによって削除されます。詳細については、SAエージェントのアンインストールの変更 (248ページ) を参照してください。

付録A アクセス権のリファレンス

この付録では、SAでタスクを実行するのに必要なアクセス権を列挙します。アクセス権の詳細については、ユーザーおよびユーザーグループの設定とセキュリティ (15ページ) を参照してください。

サーバーオブジェクトのアクセス権

表35に、登録済みソフトウェア、Internet Information Server、ローカルセキュリティ設定、実行時状態、ユーザーとグループ、および.Net Framework構成などのサーバーオブジェクトに必要なアクセス権を示します。

表35　　サーバーオブジェクトのアクセス権

ユーザーのアクション	アクションのアクセス権	サーバーのアクセス権 (カスタマー、ファシリティ、デバイスグループ)	フォルダーのアクセス権
サーバーオブジェクトの参照	サーバーモジュールの管理: 読み取り/書き込み サーバーモジュールの実行の許可: はい	該当なし	該当なし
ライブラリに追加 (サーバーブラウザーから)	サーバーモジュールの管理: 読み取り/書き込み サーバーモジュールの実行の許可: はい パッケージの管理: 読み取り/書き込み		書き込み
ソフトウェアポリシーに追加	サーバーモジュールの管理: 読み取り/書き込み サーバーモジュールの実行の許可: はい パッケージの管理: 読み取り/書き込み ソフトウェアポリシーの管理: 読み取り/書き込み	該当なし	書き込み

サーバープロパティと再起動のアクセス権

表36に、サーバーのプロパティの変更、サーバーの再起動、SAの非アクティブ化 (エージェント) をユーザーが実行するのに必要なアクセス権を示します。セキュリティ管理者は、ユーザーが特定のアクションを実行するのに必要なアクセス権をこの表で確認することができます。

表36　　ユーザーのアクションに必要なサーバープロパティと再起動のアクセス権

ユーザーのアクション	アクションのアクセス権	サーバーのアクセス権 (カスタマー、ファシリティ、デバイスグループ)
SAの非アクティブ化 (エージェント)	非アクティブ化: はい	読み取り/書き込み
プロパティの変更: サーバー名または説明	該当なし	読み取り/書き込み
サーバーの再起動	サーバーの再起動: はい	読み取り/書き込み

デバイスグループのアクセス権

SAクライアントでデバイスグループを使用するには、表37に示すアクセス権が必要です。パブリックデバイスグループのモデル化のアクセス権が必要なタスク一覧については、表45を参照してください。

表37　デバイスグループのアクションのアクセス権

ユーザーのアクション	アクションのアクセス権
パブリック静的デバイスグループの作成	パブリックデバイスグループの管理:はい
パブリック動的デバイスグループの作成	パブリックデバイスグループの管理:はい
パブリック静的デバイスグループへのサーバーの追加	パブリックデバイスグループの管理:はい
パブリック動的デバイスグループへのサーバーの追加	パブリックデバイスグループの管理:はい
パブリック静的デバイスグループからのサーバーの削除	パブリックデバイスグループの管理:はい
パブリック動的デバイスグループからのサーバーの削除	パブリックデバイスグループの管理: はい
パブリックデバイスグループの移動	パブリックデバイスグループの管理: はい
パブリックデバイスグループの複製	パブリックデバイスグループの管理: はい
パブリックデバイスグループの削除	パブリックデバイスグループの管理: はい
アクセス制御グループとして使用されている デバイスグループへのデバイスの追加	パブリックデバイスグループの管理 およびスーパー管理者

サーバーエージェントデプロイメントのアクセス権

SAクライアントを使用してサーバーにサーバーエージェントをインストールするには、表38に示すアクセス権が必要です。

表38　エージェントのアクションのアクセス権の設定

ユーザーのアクション	アクションのアクセス権
サーバーでのSAエージェントのインストール	エージェントのインストールの許可: はい
ネットワークでエージェントレスサーバーをスキャン	ネットワークのスキャンの許可: はい
エージェントを実行しているサーバーと デバイスグループの表示	管理対象サーバーおよびグループ: はい
ファシリティの変更	ファシリティ : はい

表38のアクションのアクセス権の他に、次のサーバーリソースが必要です。

- サーバーのスキャンおよびサーバーの管理を行うファシリティへの読み取りアクセス。
- カスタマー Opswareと、サーバーを割り当てるカスタマーへの読み取りアクセス。

仮想化サービスの管理者権限

仮想化サービス (VS)、仮想マシン (VM)、VMテンプレートを管理するには、表39に示すアクセス権が必要です。

ユーザーが特定のアクションのアクセス権を持っていない (アクセス権が [いいえ] に設定されている) 場合、SAクライアントの [アクション] メニューに、対応するメニュー項目が表示されません。

表39　仮想化のアクションのアクセス権

アクションのアクセス権	説明
仮想化インベントリの表示	併せて管理対象サーバーおよびグループのアクセス権を [はい] にする必要があります。(サポート対象のテクノロジーの) 仮想化インベントリを表示できます。「データの再ロード」操作を実行すると、最新の仮想化情報を表示できます。このアクセス権が [いいえ] に設定されている場合、SAクライアントの [仮想化] タブと [Oracle Solarisゾーン] ビューは表示されません。
VMライフサイクルの管理: VMの複製	仮想マシンを複製して互換性チェックを行います。ゲストのカスタマイズを行うには「ゲストOSのカスタマイズ」も必要です。
VMライフサイクルの管理: VMの作成	VMを作成して互換性チェックを行います。VMの作成ジョブからOSビルド計画を実行する場合は、表42に記載されている「OSビルド計画の実行」に関するアクセス権も必要です。
VMライフサイクルの管理: ゲストOSのカスタマイズ	「VMの複製」または「VMテンプレートからのVMのデプロイ」でのOSゲストのカスタマイズを許可します。
VMライフサイクルの管理: VMの削除	VMの削除
VMライフサイクルの管理: VMテンプレートからのVMのデプロイ	VMテンプレートからVMをデプロイして、互換性チェックを実行します。ゲストのカスタマイズを行うには「ゲストOSのカスタマイズ」も必要です。
VMライフサイクルの管理: VMの移行	仮想マシン (ホストのみ、ストレージのみ、ホストとストレージの両方) を移行して、互換性チェックを実行します。
VMライフサイクルの管理: VMの変更	VMの構成を変更します。
VM電源状態の管理	VMの電源管理操作 (電源オン、電源オフ、一時停止、サスペンド、リセット、ゲストの再開、シャットダウンなど) を実行できます。
VMテンプレートの管理: VMからVMテンプレートへの変換	VMからVMテンプレートへの変換
VMテンプレートの管理: VMテンプレートの削除	VMテンプレートを削除します。
仮想化サービスの管理	仮想化サービスの登録、変更、削除を行います。
仮想化サービスへのホストの追加	ハイパーバイザーを仮想化サービスに追加して管理できるようにします。

仮想化コンテナーのアクセス権とサーバーリソースのアクセス権

すべての仮想化アクションを実行するには、アクションのアクセス権の他に、仮想化コンテナーのアクセス権が必要です。仮想化コンテナーのアクセス権は、仮想化コンテナー(データセンター、ハイパーバイザー、ホストグループ、クラスター、リソースプール、フォルダー、プロジェクト、およびそれらの子)へのアクセスを提供します。

アクセス制御リスト(ACL)継承ルールは、ユーザーグループが親コンテナーに対して所有するACLに基づいて、新しく追加または検出された仮想コンテナーへのアクセスをどのユーザーグループに自動的に許可するかを定義します。

[アクセス権]オプションには、[**L**(リスト)]、[**書き込み**]、[**読み取り**]、[**X**(実行)]、[**PM**(フォルダーのアクセス権の編集)]があります。XまたはPMを許可されたグループでACLを継承するように設定する場合は、"X,PM"を使用します。ルールへのパスは、次の場所です。`Administration/System Configuration/Server Automation/Web Services Data Access Engine/Twist.v12n.inventory.inheritance.acl`.

[PM]オプション(デフォルト)は、最も制限レベルの高いオプションで、マルチテナント型の制御に適しています。PMの場合、編集アクセス権を持つユーザー(通常、仮想化管理者)がアクセスをその他のグループに手動で割り当てる必要があります。アクセスできるのは、新しく追加または検出されたコンテナーの親に対するPMをすでに所有するユーザーグループのみです。

[リスト]オプションは、最も制限レベルの低いアクセス権です。ユーザーグループに親コンテナーの[リスト]アクセス権が割り当てられている場合、そのグループは、同じアクセス権設定で新しいコンテナーに自動的に追加されます。たとえばデータセンター1に対して、グループAには[リスト]アクセス権と[読み取り]アクセス権が、グループBには[リスト]、[読み取り]、[書き込み]、[実行]アクセス権が割り当てられているとします。データセンター1の下に新しいクラスタ?を追加します。グループAには新しいクラスタ?に対する[リスト]アクセス権と[読み取り]アクセス権が、グループBには新しいクラスタ?に対する[リスト]、[読み取り]、[書き込み]、[実行]アクセス権が割り当てられます。

アクションのアクセス権と仮想化コンテナーのアクセス権の他に、仮想化サービスで実行中のサーバーではサーバーリソースのアクセス権が必要です。サーバーリソースのアクセス権は、ファシリティ、カスタマー、デバイスグループを介して割り当てられます。

仮想化のアクセス権とサーバーリソースのアクセス権の詳細については、『SAユーザーガイド:仮想化管理』を参照してください。

表39はアクションのアクセス権のみですが、表40には、実行可能なユーザータスクと、アクションのアクセス権、仮想化コンテナーのアクセス権、サーバーリソースのアクセス権がすべて記載されています。また、一部のアクションでは、ユーザーアクションの実行に必要なフォルダーのアクセス権も記載されています。

仮想化タスクと必要なアクセス権

表40には、仮想化インベントリで各タスクを実行するのに必要なアクセス権を示します。この表のタスクはVMware vCenter、Microsoft SCVMMで使用されています。これらのタスクの詳細については、『SAユーザーガイド: 仮想化管理』を参照してください。

表40　　vCenterおよびSCVMMの仮想化タスクと必要なアクセス権

ユーザーのアクション	必要なアクションのアクセス権	必要な仮想化コンテナーのアクセス権	適切なサーバーリソースのアクセス権(ファシリティ、カスタマー、デバイスグループ)
SAクライアントで[仮想化]タブを表示	仮想化インベントリの表示: はい 管理対象サーバーおよびグループ: はい	VS: リスト および VSで管理する各コンテナーに個別のアクセス権。 データセンター : 読み取り (基盤となるデータストアへのアクセス用) VMとテンプレートの親コンテナー : 読み取り	VSサーバー : 読み取り
VSの追加	仮想化サービスの管理: はい 仮想化インベントリの表示: はい 管理対象サーバーおよびグループ: はい	なし	VSサーバー : 読み取り
VSの編集、VSの削除	仮想化サービスの管理: はい 仮想化インベントリの表示: はい 管理対象サーバーおよびグループ: はい	VS: 書き込み	VSサーバー : 読み取り
VSまたはVSコンテナーでのデータの再ロード	仮想化インベントリの表示: はい 管理対象サーバーおよびグループ: はい	VSまたはVSコンテナー : 読み取り	なし
仮想化サービスへのホストの追加	仮想化サービスへのホストの追加: はい 仮想化インベントリの表示: はい 管理対象サーバーおよびグループ: はい	ハイパーバイザーの追加を行うコンテナー : 書き込み または コンテナーが指定されていない場合はVSコンテナー : 書き込み	追加対象のサーバー (ハイパーバイザー): 読み取り

表40 vCenterおよびSCVMMの仮想化タスクと必要なアクセス権

ユーザーのアクション	必要なアクションのアクセス権	必要な仮想化コンテナーのアクセス権	適切なサーバーリソースのアクセス権(ファシリティ、カスタマー、デバイスグループ)
VM電源制御 - 開始、停止、リセット、ゲストの再開、ゲストのシャットダウン、サスペンド、一時停止	仮想化インベントリの表示: はい VM電源状態の管理: はい 管理対象サーバーおよびグループ: はい	VMを配置するコンテナー読み取り	VMサーバー : 書き込み
VMの作成	仮想化インベントリの表示: はい VMライフサイクルの管理: VMの作成: はい 管理対象サーバーおよびグループ: はい OSビルド計画の実行の許可はい (OSビルド計画を指定する場合) パッケージの管理: 読み取り、OSBPを指定したPXE以外のVMの作成の場合:	VMを配置するターゲットコンテナー (ハイパーバイザー、クラスター、またはリソースプール): 書き込み vCenter VMを配置するVSインベントリ内のフォルダー : 書き込み	新しく作成されたVMのServer.write 注 - 選択したOSビルド計画を含むSA ライブラリフォルダーでは実行のアクセス権も必要です。 OSBPを指定したPXE以外のVMの作成の場合: `Opsware/Tools/OS Provisioning/WinPE` フォルダーでの読み取り (Windows) `Opsware/Tools/OS Provisioning`フォルダーでの読み取り (Linux)
VMの変更	仮想化インベントリの表示: はい VMライフサイクルの管理: VMの変更: はい 管理対象サーバーおよびグループ: はい	VMを配置するコンテナー書き込み および VMが存在するハイパーバイザーコンテナー (vCenterのみ): リスト	VMサーバー : 書き込み
VMの移行	仮想化インベントリの表示: はい VMライフサイクルの管理: VMの移行: はい 管理対象サーバーおよびグループ: はい	VMを配置するコンテナー書き込み 追加: ストレージの移行 - ハイパーバイザー : リスト ホストまたはホストとストレージの移行 - VMを配置するターゲットコンテナー (ハイパーバイザー、クラスター、またはリソースプール): 書き込み	VMサーバー : 読み取り

表40 vCenterおよびSCVMMの仮想化タスクと必要なアクセス権

ユーザーのアクション	必要なアクションのアクセス権	必要な仮想化コンテナーのアクセス権	適切なサーバーリソースのアクセス権(ファシリティ、カスタマー、デバイスグループ)
VMの複製 (vCenterのみ)	仮想化インベントリの表示: はい VMライフサイクルの管理: VMの複製: はい 管理対象サーバーおよびグループ: はい	VMを配置するコンテナー読み取り 新規のVMを配置するターゲットコンテナー(ハイパーバイザー、クラスター、またはリソースプール): 書き込み 新規のVMを配置するvCenter VSインベントリ内のフォルダー : 書き込み	ソースVMサーバー : 読み取り 新規のVMサーバー : 書き込み
ゲストOSのカスタマイズ -「VMの複製」操作または「VMテンプレートからのVMのデプロイ」操作の一部として実行する場合	VMの複製の一部として実行する場合は [VMの複製] と同じ。 VMのデプロイの一部として実行する場合は [VMテンプレートからのVMのデプロイ] と同じ。 VMライフサイクルの管理: ゲストOSのカスタマイズ: はい OSビルド計画の実行の許可はい	VMの複製の一部として実行する場合は [VMの複製] と同じ。 VMのデプロイの一部として実行する場合は [VMテンプレートからのVMのデプロイ] と同じ。	VM の複製の一部として実行する場合は [VM の複製] と同じ。 VM のデプロイの一部として実行する場合は [VM テンプレートからの VM のデプロイ] と同じ。 Linuxのカスタマイズの場合は、`Opsware/Tools/Build Plans/Virtualization/Guest Customization/Linux` フォルダーで実行します。 Windowsのカスタマイズの場合は、`Opsware/Tools/Build Plans/Virtualization/Guest Customization/Windows` フォルダーで実行します。
VMの削除	仮想化インベントリの表示: はい VMライフサイクルの管理: VMの削除: はい 管理対象サーバーおよびグループ: はい	VMを配置するコンテナー : 書き込み	VMサーバー : 書き込み

表40 vCenterおよびSCVMMの仮想化タスクと必要なアクセス権

ユーザーのアクション	必要なアクションのアクセス権	必要な仮想化コンテナーのアクセス権	適切なサーバーリソースのアクセス権(ファシリティ、カスタマー、デバイスグループ)
VMテンプレートからのVMのデプロイ	仮想化インベントリの表示: はい VMライフサイクルの管理: VMテンプレートからのVMのデプロイ: はい 管理対象サーバーおよびグループ: はい	VMテンプレートを配置するコンテナー : 実行 新規のVMを配置するターゲットコンテナー（ハイパーバイザー、クラスター、またはリソースプール): 書き込み 新規のVMを配置するvCenter VSインベントリ内のフォルダー : 書き込み	VMテンプレートサーバー : 読み取り 新規のVMサーバー : 書き込み
VMからVMテンプレートへの変換	仮想化インベントリの表示: はい VMテンプレートの管理: VMからVMテンプレートへの変換: はい 管理対象サーバーおよびグループ: はい	VMを配置するコンテナー : 書き込み SCVMMライブラリ内のVMテンプレートフォルダー : 書き込み	VMサーバー : 読み取り
VMテンプレートの削除	仮想化インベントリの表示: はい VMテンプレートの管理: 削除 VMテンプレート: はい 管理対象サーバーおよびグループ: はい	VMテンプレートを配置するコンテナー : 書き込み	VMサーバー : 書き込み
サーバーのマージ	仮想化インベントリの表示: はい (仮想化サーバーと別のサーバーをマージするため) サーバーのマージはい 管理対象サーバーおよびグループ: はい	VMまたはテンプレートを配置するコンテナー : 書き込み または Hypervisor: 書き込み	マージする両サーバーのServer.write

Solaris仮想化のアクセス権

表41に、Solarisゾーンの管理に必要なアクセス権を示します。詳細については、『SAユーザーガイド: 仮想化の管理

表41　Solaris仮想化のアクセス権

ユーザーのアクション	必要なアクションのアクセス権	必要なサーバーリソースのアクセス権(ファシリティ、カスタマー、デバイスグループ)
ゾーンの作成	VMライフサイクルの管理: VMの作成 仮想化インベントリの表示: はい 管理対象サーバーおよびグループ: はい	ハイパーバイザーサーバー: 読み取り 新規のVMを割り当てるカスタマー: 書き込み
データの再ロード	仮想化インベントリの表示: はい 管理対象サーバーおよびグループ: はい	ハイパーバイザーサーバー: 読み取り VMサーバー: 読み取り
変更	VMライフサイクルの管理: VMの変更 仮想化インベントリの表示: はい 管理対象サーバーおよびグループ: はい	ハイパーバイザーサーバー: 読み取り VMサーバー: 書き込み
削除	VMライフサイクルの管理: VMの削除 仮想化インベントリの表示: はい 管理対象サーバーおよびグループ: はい	ハイパーバイザーサーバー: 読み取り VMサーバー: 読み取り
開始、停止	VM電源状態の管理: はい 仮想化インベントリの表示: はい 管理対象サーバーおよびグループ: はい	ハイパーバイザーサーバー: 読み取り VMサーバー: 書き込み

OSプロビジョニングのアクセス権

ここでは、OSプロビジョニングに必要なアクセス権について説明します。セキュリティ管理者は、表42を参照してユーザーが特定のアクションを実行するのに必要なアクセス権をこの表で確認することができます。

表42の「サーバーのアクセス権」欄は、OSシーケンスまたはインストールプロファイルで参照されるサーバーに対するアクセス権です。サーバーのアクセス権は、SA Webクライアントでカスタマー、ファシリティ、デバイスグループのアクセス権で指定します。OSシーケンスを作成してフォルダーに保存する場合は、そのフォルダーに対する書き込みアクセス権が必要です。

表42　ユーザーのアクションに必要なOSプロビジョニングのアクセス権

ユーザーのアクション	アクションのアクセス権	サーバーのアクセス権(カスタマー、ファシリティ、デバイスグループ)	フォルダーのアクセス権
OS ビルド計画			
OSビルド計画の作成	OSビルド計画の管理: 読み取り/書き込み	なし	書き込み
OSビルド計画の表示	OSビルド計画の管理: 読み取り	なし	読み取り

表42　ユーザーのアクションに必要なOSプロビジョニングのアクセス権（続き）

ユーザーのアクション	アクションのアクセス権	サーバーのアクセス権(カスタマー、ファシリティ、デバイスグループ)	フォルダーのアクセス権
OSビルド計画の編集	OSビルド計画の管理: 読み取り/書き込み	なし	書き込み
OSビルド計画の削除	OSビルド計画の管理: 読み取り/書き込み	なし	書き込み
デバイスグループのOSビルド計画への追加	下記のアクセス権の組み合わせのいずれでも可: 1) サーバーとグループの管理 + OS ビルド計画の管理: 読み取り/書き込み、 または 2) パブリックデバイスグループの管理([クライアント機能] タブ、サーバーセクション) + OS ビルド計画の管理: 読み取り/書き込み、 または 3) パブリックデバイスグループの管理(SA Webクライアント)([その他] タブ、サーバーおよびデバイスグループのアクセス権セクション) + OS ビルド計画の管理: 読み取り/書き込み	なし	OS ビルド計画を含むフォルダー: 書き込み
OGFSスクリプトのOSビルド計画への追加	OGFS スクリプトの管理: 読み取り + OSビルド計画の管理: 読み取り/書き込み	なし	OGFS スクリプトを含むフォルダー: 読み取り + OS ビルド計画を含むフォルダー: 書き込み
サーバースクリプトのOSビルド計画への追加	サーバースクリプトの管理: 読み取り + OS ビルド計画の管理: 読み取り/書き込み	なし	サーバースクリプトを含むフォルダー: 読み取り + OS ビルド計画を含むフォルダー : 書き込み

表42 ユーザーのアクションに必要なOSプロビジョニングのアクセス権（続き）

ユーザーのアクション	アクションのアクセス権	サーバーのアクセス権(カスタマー、ファシリティ、デバイスグループ)	フォルダーのアクセス権
ZIPパッケージのOSビルド計画への追加	パッケージの管理: 読み取り + OS ビルド計画の管理: 読み取り / 書き込み	なし	パッケージを含むフォルダー: 読み取り + OSビルド計画を含むフォルダー: 書き込み
ソフトウェアポリシーのOSビルド計画へのアタッチ	ソフトウェアポリシーの管理: 読み取り + OS ビルド計画の管理: 読み取り/書き込み	なし	ソフトウェアポリシーを含むフォルダー: 読み取り + OS ビルド計画を含むフォルダー: 書き込み
WindowsパッチポリシーのOSビルド計画へのアタッチ	Windows パッチの管理: ポリシー + OSビルド計画の管理: 読み取り/書き込み	なし	OS ビルド計画を含むフォルダー: 書き込み
OSビルド計画の実行 (サーバーまたはOSビルド計画ノードから)	管理対象サーバーとグループ + OS ビルド計画の管理: OS ビルド計画の実行の許可はい	読み取り/書き込み	OS ビルド計画を含むフォルダー : 実行
OSビルド計画の実行 (VMware ESXi 4.1)	サーバーとグループの管理 + OS ビルド計画の管理: 読み取り + OS ビルド計画の実行の許可: はい + サーバーの管理の許可 + 仮想サーバーの表示 + 仮想サーバーの管理	読み取り/書き込み	OSビルド計画の実行のWeb拡張を含むフォルダー (/Opsware/Tools/OS Provisioning): 実行 + OSビルド計画を含むフォルダー: 実行 + /Opsware/Tools/Virtualization Programs/Hypervisor Scanner フォルダーでのリストおよび実行のフォルダーのアクセス権

表42　ユーザーのアクションに必要なOSプロビジョニングのアクセス権（続き）

ユーザーのアクション	アクションのアクセス権	サーバーのアクセス権(カスタマー、ファシリティ、デバイスグループ)	フォルダーのアクセス権
OS シーケンス			
OSシーケンスの作成	OSシーケンスの管理: 読み取り / 書き込み + オペレーティングシステム + ウィザード : OSの準備	**注**: カスタマーに割り当てられたOSインストールプロファイルを使用してOSシーケンスを作成する場合、ユーザーにカスタマーに対する [読み取り] 以上のアクセス権が必要です。 **注**: カスタマーに依存しないOSインストールプロファイルを使用してOSシーケンスを作成する場合、カスタマーのアクセス権は必要ありません。	書き込み
OSシーケンスの表示	OSシーケンスの管理: 読み取り	なし	読み取り
OSシーケンスの編集	OSシーケンスの管理: 読み取り/書き込み	なし	書き込み
OSシーケンスの削除	OSシーケンスの管理: 読み取り/書き込み	なし	書き込み
OSシーケンスの実行 (サーバーまたはOSシーケンスから)	OSシーケンスの管理: 読み取り および OS シーケンスの実行の許可: はい	読み取り/書き込み	読み取り

表42　ユーザーのアクションに必要なOSプロビジョニングのアクセス権（続き）

ユーザーのアクション	アクションのアクセス権	サーバーのアクセス権(カスタマー、ファシリティ、デバイスグループ)	フォルダーのアクセス権
未プロビジョニングサーバーの表示	SA Webクライアントのアクセス権: サーバープール	読み取り	該当なし
ソフトウェアポリシーのアタッチ	ソフトウェアポリシーの管理: 読み取り + OSシーケンスの管理: 読み取り/書き込み	該当なし	ソフトウェアポリシーを含むフォルダー: 読み取り + OSシーケンスを含むフォルダー: 書き込み
Windowsパッチポリシーのアタッチ	Windowsパッチの管理: ポリシー + OSシーケンスの管理: 読み取り/書き込み	該当なし	OS シーケンスを含むフォルダー: 書き込み
Solarisパッチポリシーのアタッチ	ソフトウェアポリシーの管理: 読み取り + OSシーケンスの管理: 読み取り/書き込み	該当なし	Solaris パッチポリシーを含むフォルダー: 読み取り + OSシーケンスを含むフォルダー: 書き込み

表42　ユーザーのアクションに必要なOSプロビジョニングのアクセス権（続き）

ユーザーのアクション	アクションのアクセス権	サーバーのアクセス権(カスタマー、ファシリティ、デバイスグループ)	フォルダーのアクセス権
OSインストールプロファイル			
OSインストールプロファイルの作成、編集、削除	オペレーティングシステム + ウィザード : OSの準備	**注:** カスタマーに割り当てられたOSインストールプロファイルを使用してOSシーケンスを作成する場合、このカスタマーに [読み取り/書き込み] アクセス権が必要です。 **注:** カスタマーに依存しないOSインストールプロファイルを使用してOSシーケンスを作成する場合、カスタマーのアクセス権は必要ありません。	該当なし
未プロビジョニングサーバーリスト			
未プロビジョニングサーバーリストでのサーバーの表示	サーバープール	該当なし	該当なし
ブートクライアントの管理			
管理対象ブートクライアントWebアプリケーションの実行	ネットワークブートの構成の許可 + 管理対象サーバーおよびグループ + カスタマーの管理 + サーバープール	ファシリティとカスタマーに対する読み取り / 書き込み + 未割り当てのカスタマーに対する読み取り / 書き込み	`/Opsware /Tools/OS Provisioning/ Manage Boot Clients`フォルダーでのリストおよび実行

表43に、OSプロビジョニングのアクセス権ごとにユーザーが実行できるアクションを示します。表43は表42と同じデータを、アクションのアクセス権ごとに整理したものです。

セキュリティ管理者は、表43を参照して特定のアクションのアクセス権が割り当てられたユーザーが実行できるアクションを確認できます。

表43 OSプロビジョニングのアクセス権によってSAクライアントで使用できるユーザーアクション

アクションのアクセス権	ユーザーのアクション	サーバーのアクセス権 (カスタマー、ファシリティ、デバイスグループ)	フォルダー
OSシーケンスの管理: 読み取り	OSシーケンスの表示	読み取り	読み取り
OSシーケンスの管理: 読み取り/書き込み + オペレーティングシステム + ウィザード: OSの準備	OSシーケンスの作成	読み取り	書き込み
OSシーケンスの実行の許可: はい	OSシーケンスの実行	書き込み	読み取り
OSシーケンスの管理: 読み取り OSシーケンスの実行の許可: はい	OSシーケンスの実行	書き込み	読み取り
OSシーケンスの管理: 読み取り OSシーケンスの実行の許可: いいえ	OSシーケンスの表示	読み取り	読み取り
OSシーケンスの管理: 書き込み OSシーケンスの実行の許可: はい	OSシーケンスの実行 OSシーケンスの編集	書き込み	書き込み
OSシーケンスの管理: 書き込み OSシーケンスの実行の許可: いいえ	OSシーケンスの編集	読み取り	書き込み
オペレーティングシステム + ウィザード: OSの準備	OSインストールプロファイルの作成、編集、削除	読み取り/書き込み、該当なし、該当なし	該当なし
サーバープール	未プロビジョニングサーバーリストでのサーバーの表示	読み取り	該当なし

ブートクライアントの管理のアクセス権

この項では、OSプロビジョニングでのブートクライアントの管理 (MBC) ユーティリティの使用に必要なアクセス権について説明します。

表44 ブートクライアントの管理ユーティリティのアクセス権

アクションのアクセス権	ユーザーのアクション	サーバーのアクセス権 (カスタマー、ファシリティ、デバイスグループ)	フォルダー
OSビルド計画の実行の許可	OSビルド計画の実行	書き込み	読み取り
OSシーケンスの実行の許可	OSシーケンスの実行	書き込み	読み取り
サーバーおよびグループの管理	サーバーおよびグループの管理	書き込み	読み取り

アクションのアクセス権	ユーザーのアクション	サーバーのアクセス権(カスタマー、ファシリティ、デバイスグループ)	フォルダー
カスタマーの管理	カスタマーの作成、編集	書き込み	読み取り
サーバープール	サーバープールへのアクセス	書き込み	読み取り
未割り当てカスタマーに対する読み取り/書き込みアクセス権	カスタマー未割り当てに割り当てられたサーバーへのアクセス	書き込み	読み取り
ネットワークブートの構成の許可	ネットワークブートの構成	書き込み	読み取り

ソフトウェア管理のアクセス権

表45は、SAクライアントの特定のアクションをユーザーが実行するのに必要なソフトウェア管理のアクセス権を示しています。セキュリティ管理者は、ユーザーが特定のアクションを実行するのに必要なアクセス権をこの表で確認することができます。

カスタマーをフォルダーに割り当てた場合、フォルダー内のソフトウェアポリシーを関連付けることが可能なオブジェクトにカスタマーの制約が適用されることがあります。これらの制約の影響を受けるタスク一覧については、フォルダー、カスタマーの制約、ソフトウェアポリシー (24ページ) を参照してください。

ソフトウェアのインストールを行う場合は、ソフトウェアのインストールのアクセス権を持つユーザーグループに属している必要があります。このユーザーグループには、インストールするソフトウェアに関するフォルダーのアクセス権も必要です。

表45　ユーザーのアクションに必要なソフトウェア管理のアクセス権

ユーザーのアクション	アクションのアクセス権	サーバーのアクセス権(カスタマー、ファシリティ、デバイスグループ)	フォルダーのアクセス権
ソフトウェアポリシー			
ソフトウェアポリシーの作成	ソフトウェアポリシーの管理: 読み取り/書き込み	該当なし	書き込み
ソフトウェアポリシーの削除	ソフトウェアポリシーの管理: 読み取り/書き込み	該当なし	書き込み
ソフトウェアポリシーを開く (表示)	ソフトウェアポリシーの管理: 読み取り	該当なし	読み取り
ソフトウェアポリシーのプロパティの編集	ソフトウェアポリシーの管理: 読み取り/書き込み	該当なし	書き込み
パッケージの追加	ソフトウェアポリシーの管理: 読み取り/書き込み パッケージの管理: 読み取り	該当なし	ソフトウェアポリシーを含むフォルダー: 書き込み

表45　ユーザーのアクションに必要なソフトウェア管理のアクセス権（続き）

ユーザーのアクション	アクションのアクセス権	サーバーのアクセス権(カスタマー、ファシリティ、デバイスグループ)	フォルダーのアクセス権
RPMパッケージの追加	ソフトウェアポリシーの管理: 読み取り/書き込み パッケージの管理: 読み取り	該当なし	ソフトウェアポリシーを含むフォルダー: 書き込み
パッチの追加	ソフトウェアポリシーの管理: 読み取り/書き込み パッチの管理: 読み取り	該当なし	ソフトウェアポリシーを含むフォルダー: 書き込み
アプリケーション構成の追加	ソフトウェアポリシーの管理: 読み取り/書き込み アプリケーション構成の管理: 読み取り	該当なし	ソフトウェアポリシーを含むフォルダー: 書き込み
スクリプトの追加	ソフトウェアポリシーの管理: 読み取り/書き込み サーバースクリプトの管理: 読み取り	該当なし	ソフトウェアポリシーを含むフォルダー: 書き込み
サーバーオブジェクトの追加	ソフトウェアポリシーの管理: 読み取り/書き込み パッケージの管理: 読み取り	該当なし	ソフトウェアポリシーを含むフォルダー: 書き込み
ソフトウェアポリシーの管理	ソフトウェアポリシーの管理: 読み取り/書き込み	該当なし	ソフトウェアポリシーを含むフォルダー: 書き込み
パッケージの削除	ソフトウェアポリシーの管理: 読み取り/書き込み	該当なし	書き込み
RPMパッケージの削除	ソフトウェアポリシーの管理: 読み取り/書き込み	該当なし	書き込み
パッチの削除	ソフトウェアポリシーの管理: 読み取り/書き込み	該当なし	書き込み
アプリケーション構成の削除	ソフトウェアポリシーの管理: 読み取り/書き込み	該当なし	書き込み
ソフトウェアポリシーの削除	ソフトウェアポリシーの管理: 読み取り/書き込み	該当なし	書き込み
スクリプトの削除	ソフトウェアポリシーの管理: 読み取り/書き込み	該当なし	書き込み
サーバーオブジェクトの削除	ソフトウェアポリシーの管理: 読み取り/書き込み	該当なし	書き込み

表45　ユーザーのアクションに必要なソフトウェア管理のアクセス権（続き）

ユーザーのアクション	アクションのアクセス権	サーバーのアクセス権 (カスタマー、ファシリティ、デバイスグループ)	フォルダーのアクセス権
ソフトウェアのインストール/アンインストール	ソフトウェアポリシーの管理: 読み取り ソフトウェアポリシーのアタッチ/デタッチの許可: はい ソフトウェアのインストール/アンインストールの許可: はい パブリックデバイスグループのモデル化: はい (パブリックデバイスグループを修復する場合に必要)	読み取り/書き込み	読み取り
ソフトウェアポリシーのアタッチ	ソフトウェアポリシーの管理: 読み取り ソフトウェアポリシーのアタッチ/デタッチの許可: はい パブリックデバイスグループのモデル化: はい (このアクセス権は、ソフトウェアポリシーをパブリックデバイスグループにアタッチする場合に必要)	読み取り/書き込み	読み取り
ソフトウェアポリシーのデタッチ	ソフトウェアポリシーの管理: 読み取り ソフトウェアポリシーのアタッチ/デタッチの許可: はい パブリックデバイスグループのモデル化: はい (このアクセス権は、ソフトウェアポリシーをパブリックデバイスグループにアタッチする場合に必要)	読み取り/書き込み	読み取り
修復	ソフトウェアポリシーの管理: 読み取り サーバーの修復の許可: はい パブリックデバイスグループのモデル化: はい (パブリックデバイスグループを修復する場合に必要)	読み取り/書き込み	読み取り
ISMコントロールの実行	ソフトウェアポリシーの管理: 読み取り ISMコントロールの実行の許可: はい パブリックデバイスグループのモデル化: はい (パブリックデバイスグループで ISM コントロールを実行する場合に必要)	読み取り/書き込み	読み取り
ZIPパッケージの複製	ソフトウェアポリシーの管理: 読み取り/書き込み	該当なし	書き込み

表45　ユーザーのアクションに必要なソフトウェア管理のアクセス権（続き）

ユーザーのアクション	アクションのアクセス権	サーバーのアクセス権(カスタマー、ファシリティ、デバイスグループ)	フォルダーのアクセス権
ZIPインストールディレクトリの編集	ソフトウェアポリシーの管理: 読み取り/書き込み	該当なし	書き込み
ソフトウェアコンプライアンスのスキャン	該当なし	読み取り	該当なし
ソフトウェアポリシーの名前の変更	ソフトウェアポリシーの管理: 読み取り/書き込み	該当なし	書き込み
ソフトウェアポリシーの切り取り	ソフトウェアポリシーの管理: 読み取り/書き込み	該当なし	書き込み
ソフトウェアポリシーの管理:	ソフトウェアポリシーの管理: 読み取り	該当なし	読み取り
ソフトウェアポリシーの貼り付け	ソフトウェアポリシーの管理: 読み取り/書き込み	該当なし	ソースフォルダー: 読み取り (コピーして貼り付けの場合) ソースフォルダー: 読み取り (切り取り/貼り付けの場合) ターゲットフォルダー: 書き込み
ソフトウェアポリシーの移動	ソフトウェアポリシーの管理: 読み取り/書き込み	該当なし	ソースフォルダー: 書き込み ターゲットフォルダー: 書き込み
フォルダー			
フォルダーの作成	該当なし	該当なし	書き込み
フォルダーの削除	該当なし	該当なし	書き込み
フォルダーを開く	該当なし	該当なし	読み取り
フォルダーのプロパティの表示	該当なし	該当なし	読み取り
フォルダーのプロパティの編集	該当なし	該当なし	書き込み
フォルダーのアクセス権の管理	該当なし	該当なし	フォルダーのアクセス権の編集
フォルダーの切り取り	該当なし	該当なし	書き込み
フォルダーのコピー	該当なし	該当なし	読み取り
フォルダーの貼り付け	該当なし	該当なし	ソースフォルダー: 読み取り (コピーして貼り付けの場合) ソースフォルダー: 読み取り (切り取り/貼り付けの場合) ターゲットフォルダー: 書き込み

表45 ユーザーのアクションに必要なソフトウェア管理のアクセス権（続き）

ユーザーのアクション	アクションのアクセス権	サーバーのアクセス権 (カスタマー、ファシリティ、デバイスグループ)	フォルダーのアクセス権
フォルダーの移動	該当なし	該当なし	ソースフォルダー: 書き込み ターゲットフォルダー: 書き込み
フォルダーの名前の変更	該当なし	該当なし	書き込み
パッケージ			
パッケージのインポート	パッケージの管理: 読み取り/書き込み	該当なし	書き込み
パッケージのエクスポート	パッケージの管理: 読み取り	該当なし	読み取り
パッケージを開く (表示)	パッケージの管理: 読み取り	該当なし	読み取り
パッケージのプロパティの編集	パッケージの管理: 読み取り/書き込み	該当なし	読み取り
パッケージの削除	パッケージの管理: 読み取り/書き込み	該当なし	書き込み
パッケージの名前の変更	パッケージの管理: 読み取り/書き込み	該当なし	書き込み
パッケージの切り取り	パッケージの管理: 読み取り/書き込み	該当なし	書き込み
パッケージの貼り付け	パッケージの管理: 読み取り/書き込み	該当なし	ソースフォルダー: 読み取り (コピーして貼り付けの場合) ソースフォルダー: 読み取り (切り取り/貼り付けの場合) ターゲットフォルダー: 書き込み
パッケージの移動	パッケージの管理: 読み取り/書き込み	該当なし	ソースフォルダー: 書き込み ターゲットフォルダー: 書き込み

表46に、ソフトウェア管理のアクセス権ごとにユーザーが実行できるアクションを示します。表46は表45と同じデータを、アクションのアクセス権ごとに整理したものです。セキュリティ管理者は、表46を参照して特定のアクションのアクセス権が割り当てられたユーザーが実行できるアクションを確認できます。

表46　　ソフトウェア管理のアクセス権で使用できるユーザーアクション

アクションのアクセス権	ユーザーのアクション	サーバーのアクセス権(カスタマー、ファシリティ、デバイスグループ)	フォルダーのアクセス権
ソフトウェアポリシーの管理: 読み取り/書き込み	ソフトウェアポリシーの作成	該当なし	書き込み
	ソフトウェアポリシーの削除	該当なし	書き込み
	ソフトウェアポリシーの編集	該当なし	書き込み
	ソフトウェアポリシーの名前の変更	該当なし	書き込み
	ソフトウェアポリシーの切り取り	該当なし	書き込み
	ソフトウェアポリシーの貼り付け	該当なし	書き込み
	ソフトウェアポリシーの移動	該当なし	書き込み
	パッケージの削除	該当なし	書き込み
	パッチの削除	該当なし	書き込み
	アプリケーション構成の削除	該当なし	書き込み
	スクリプトの削除	該当なし	書き込み
	サーバーオブジェクトの削除	該当なし	書き込み
	ソフトウェアポリシーの削除	該当なし	書き込み
	ZIPパッケージの複製	該当なし	書き込み
ソフトウェアポリシーの管理: 読み取り	ソフトウェアポリシーを開く(表示)	該当なし	読み取り
	ソフトウェアポリシーのプロパティのコピー	該当なし	読み取り
ソフトウェアポリシーの管理: 読み取り/書き込み および パッケージの管理: 読み取り	パッケージの追加 RPMパッケージの追加	該当なし	ソフトウェアポリシーを含むフォルダー : 書き込み パッケージを含むフォルダー : 読み取り
ソフトウェアポリシーの管理: 読み取り/書き込み および パッチの管理: 読み取り	パッチの追加	該当なし	ソフトウェアポリシーを含むフォルダー : 書き込み パッチを含むフォルダー : 読み取り

表46　ソフトウェア管理のアクセス権で使用できるユーザーアクション（続き）

アクションのアクセス権	ユーザーのアクション	サーバーのアクセス権(カスタマー、ファシリティ、デバイスグループ)	フォルダーのアクセス権
ソフトウェアポリシーの管理: 読み取り/書き込み および アプリケーション構成の管理: 読み取り	アプリケーション構成の追加	該当なし	ソフトウェアポリシーを含むフォルダー : 書き込み アプリケーション構成を含むフォルダー : 読み取り
ソフトウェアポリシーの管理: 読み取り/書き込み	ソフトウェアポリシーの管理	該当なし	ソフトウェアポリシーを含むフォルダー : 書き込み 別のソフトウェアポリシーに追加するソフトウェアポリシーを含むフォルダー : 読み取り
ソフトウェアポリシーの管理: 読み取り/書き込み および サーバースクリプトの管理: 読み取り	スクリプトの追加	該当なし	ソフトウェアポリシーを含むフォルダー : 書き込み スクリプトを含むフォルダー : 読み取り
ソフトウェアポリシーの管理: 読み取り/書き込み および パッケージの管理: 読み取り	サーバーオブジェクトの追加	該当なし	ソフトウェアポリシーを含むフォルダー : 書き込み サーバーオブジェクトを含むフォルダー : 読み取り
ソフトウェアポリシーの管理: 読み取り/書き込み	パッケージの削除	該当なし	書き込み
	RPMパッケージの削除	該当なし	書き込み
	パッチの削除	該当なし	書き込み
	アプリケーション構成の削除	該当なし	書き込み
	スクリプトの削除	該当なし	書き込み
	サーバーオブジェクトの削除	該当なし	書き込み
	ソフトウェアポリシーの削除	該当なし	書き込み

表46 ソフトウェア管理のアクセス権で使用できるユーザーアクション（続き）

アクションのアクセス権	ユーザーのアクション	サーバーのアクセス権(カスタマー、ファシリティ、デバイスグループ)	フォルダーのアクセス権
ソフトウェアポリシーの管理: 読み取り および ソフトウェアポリシーのアタッチ/デタッチの許可: はい および パブリックデバイスグループのモデル化: はい (ソフトウェアポリシーをパブリックデバイスグループにアタッチする場合に必要)	ソフトウェアポリシーのアタッチ	読み取り/書き込み	読み取り
	ソフトウェアポリシーのデタッチ	読み取り/書き込み	読み取り
ソフトウェアポリシーの管理: 読み取り および サーバーの修復の許可: はい および パブリックデバイスグループのモデル化: はい (パブリックデバイスグループを修復する場合に必要)	修復	読み取り/書き込み	読み取り
ソフトウェアポリシーの管理: 読み取り および ソフトウェアポリシーのアタッチ/デタッチの許可: はい および ソフトウェアのインストール/アンインストールの許可: はい および パブリックデバイスグループのモデル化: はい (パブリックデバイスグループを修復する場合に必要)	ソフトウェアのインストール/アンインストール	読み取り/書き込み	読み取り

表46　ソフトウェア管理のアクセス権で使用できるユーザーアクション（続き）

アクションのアクセス権	ユーザーのアクション	サーバーのアクセス権(カスタマー、ファシリティ、デバイスグループ)	フォルダーのアクセス権
ソフトウェアポリシーの管理: 読み取り および ISMコントロールの実行の許可: はい および パブリックデバイスグループのモデル化: はい (パブリックデバイスグループでISMコントロールを実行する場合に必要)	ISMコントロールの実行	読み取り/書き込み	読み取り
パッケージの管理: 読み取り/書き込み	パッケージのインポート	該当なし	書き込み
	パッケージの削除	該当なし	書き込み
	パッケージの名前の変更	該当なし	書き込み
	パッケージの切り取り	該当なし	書き込み
	パッケージの貼り付け	該当なし	書き込み
	パッケージの移動	該当なし	書き込み
パッケージの管理: 読み取り/書き込み	パッケージのプロパティの編集	該当なし	読み取り
パッケージの管理: 読み取り	パッケージのエクスポート	該当なし	読み取り
	パッケージを開く (表示)	該当なし	読み取り

Chef Cookbook管理のアクセス権

ここでは、ユーザーがSAクライアントの特定のアクションを実行するのに必要なChef Cookbook管理のアクセス権を示しています。セキュリティ管理者は、ユーザーが特定のアクションを実行するのに必要なアクセス権をこの表で確認することができます。

記載されたアクションのアクセス権に加えて、すべてのユーザーのアクションで管理対象サーバーおよびグループのアクセス権が必要です。

ここでは、ユーザーがSAクライアントの特定のアクションを実行するのに必要なChef Cookbook管理のアクセス権を示しています。セキュリティ管理者は、ユーザーが特定のアクションを実行するのに必要なアクセス権をこの表で確認することができます。

記載されたアクションのアクセス権に加えて、すべてのユーザーのアクションで管理対象サーバーおよびグループのアクセス権が必要です。SAのアクセス権をセットアップする方法のその他のガイドラインについては、『SA 管理ガイド』の付録「アクセス権のリファレンス」を参照してください。

依存関係がないCookbookのChef Recipeを実行するためのアクセス権

依存関係がないCookbookのChef Recipeを実行するには、次のアクセス権が必要です。

- これらの**アクションのアクセス権**によって、実行可能なChefタスクが制御されます。

アクセス権	設定	可能になるタスク
Chef Recipeの実行	はい	特定の Chef Recipe の実行ジョブを開始またはスケジュール設定できるようになります。
パッケージの管理	読み取り (またはそれ以上)	Chef Recipe の実行ジョブで Cookbook (SA パッケージの一種) を使用できるようになります。

  Chef Recipe の実行ジョブを実行するユーザーは、Chef Recipe の実行およびパッケージの管理のアクセス権を持つユーザーグループに属している必要があります。

- **フォルダーのアクセス権**は、CookbookがあるSAライブラリフォルダーへのアクセス権を制御します。

  Chef Recipeの実行ジョブを実行するユーザーは、Cookbookがあるフォルダーに対する読み取りアクセス権を持つユーザーグループに属している必要があります。

- **リソースのアクセス権**は、SA内の管理対象サーバーに対する現在のユーザーのアクセス権を制御します。

  Chef Recipe の実行ジョブを実行するユーザーは、サーバーのファシリティ、カスタマー、および少なくともそのいずれかのデバイスグループに対する読み取りおよび書き込みアクセス権を持つユーザーグループに属している必要があります。

  リソースのアクセス権の設定の詳細については、『SA 管理ガイド』の「リソースのアクセス権について」を参照してください。

- **フォルダーに対するカスタマーの制約**は、Chef Recipeの実行ジョブのターゲットにすることができるサーバーを決定します。各サーバーはカスタマーに割り当てられるため、Cookbookフォルダーのカスタマー制約には、ターゲットサーバーのカスタマーが含まれている必要があります。

  別の方法として、カスタマー独立のカスタマーをCookbookフォルダーに割り当てて、フォルダーのカスタマーアクセス権を完全に無視することもできます。

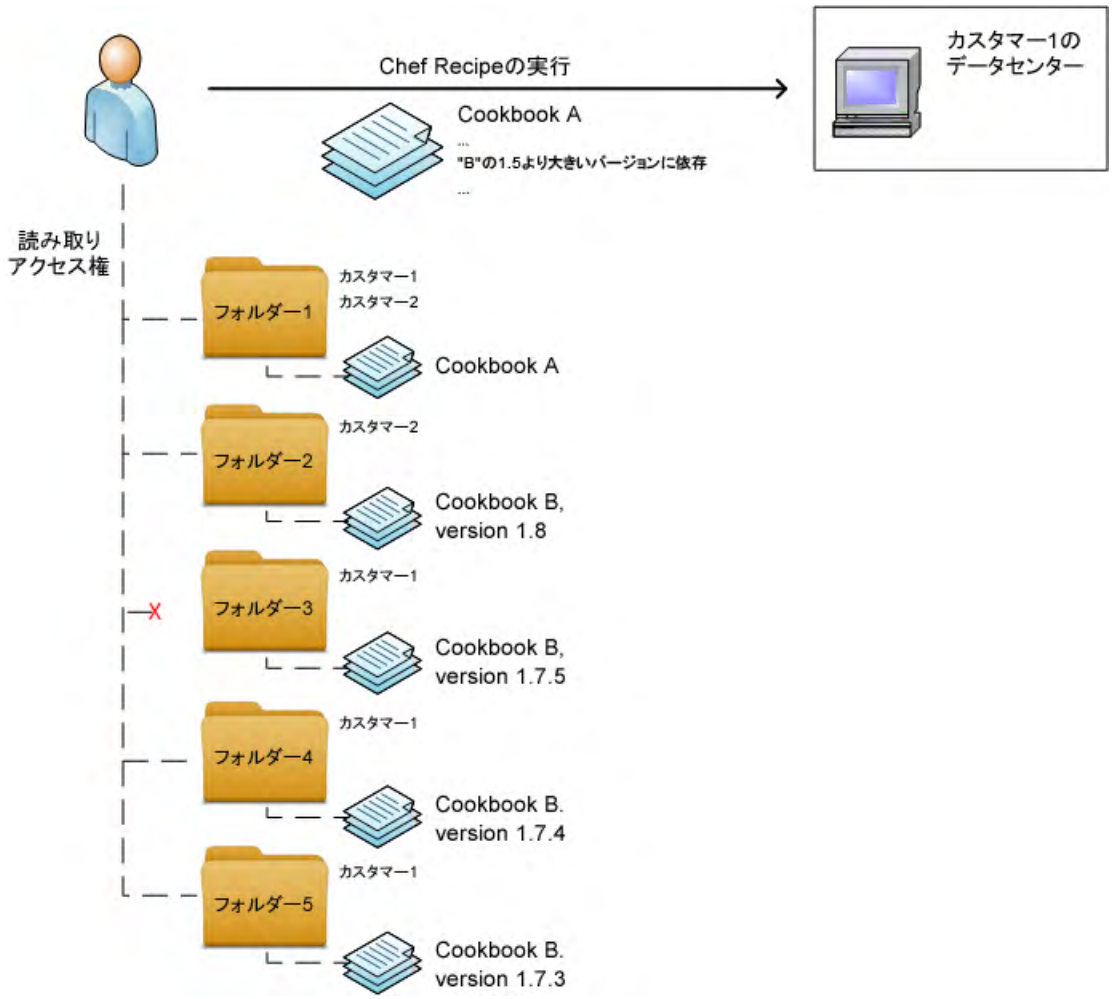
  フォルダーのアクセス権の設定の詳細については、『SA 管理ガイド』の「リソースのアクセス権について」を参照してください。

依存関係があるCookbookのアクセス権管理

Cookbookが依存するアイテムも、そのCookbookと同じアクセス権要件 (フォルダーの読み取りアクセス権および適切なフォルダーカスタマー制約) を満たしていることが必要です。依存関係のある Cookbook に複数のバージョンがある場合、SAは、依存関係グラフの全体がすべての必要なアクセス権を満足するCookbookの最新バージョンを使用します。

例: 次の設定で、ユーザーがCookbook AのRecipeを実行しようとすると、SAはCookbook Bに対する依存関係をバージョン1.7.4で解決します。

図38 Chef Recipeを実行するためのアクセス権の例



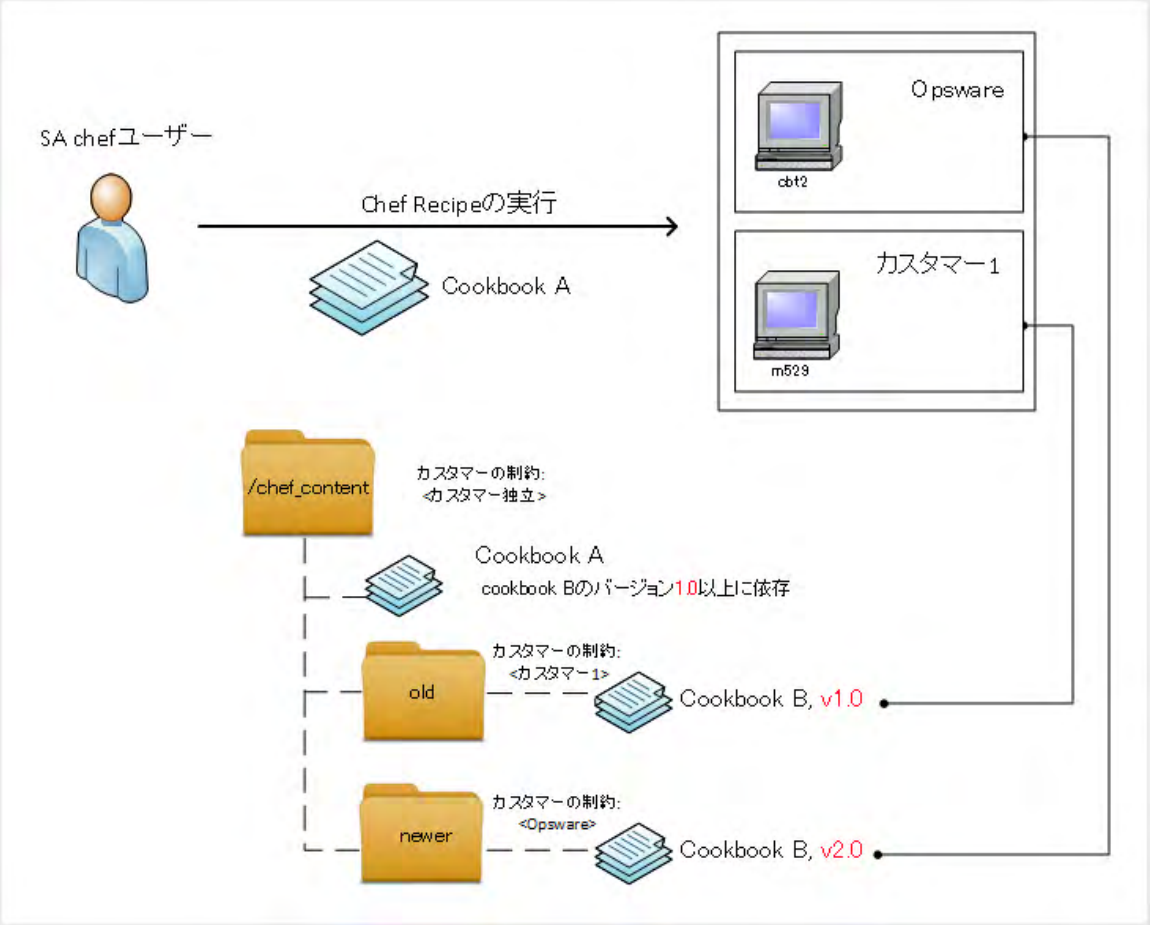
これを詳しく説明します。Cookbook Bのバージョン1.8が使用できないのは、フォルダー 2がカスタマー 1 (ターゲットのサーバーのカスタマー) に関連付けられていないためです。Cookbook Bのバージョン1.7.5が使用できないのは、ユーザーがフォルダー 3に対するアクセス権を持っていないためです。バージョン1.7.4と1.7.3は両方ともアクセス可能ですが、SAは、より高いバージョンである1.7.4を選択します。

マルチテナンシー

フォルダーに対するカスタマー制約には、マルチテナンシーをサポートするメカニズムが用意されており、異なるカスタマーに異なる内容を適用することができます。

下記の例は、2つの管理対象サーバー (cbt2およびm529) のグループにCookbook Aを適用すると、サーバーm529にはCookbook Bのバージョン1.0が適用され、サーバーcbt2にはCookbook Bのバージョン2.0が適用されることを示しています。

図39 Chef Recipeのマルチテナンシーの例



アプリケーション構成管理のアクセス権

表47は、SAクライアントのアプリケーション構成に関する特定のアクションをユーザーが実行するのに必要なアクセス権を示しています。セキュリティ管理者は、ユーザーが特定のアクションを実行するのに必要なアクセス権をこの表で確認することができます。

表47に記載したアクションのアクセス権に加えて、すべてのユーザーのアクションで管理対象サーバーおよびグループのアクセス権が必要です。

表 47 の「サーバーのアクセス権」欄は、アプリケーション構成または構成テンプレートで参照されるサーバーに対するアクセス権です。サーバーのアクセス権は、SA Webクライアントでカスタマー、ファシリティ、デバイスグループのアクセス権で指定します。表47の「フォルダーのアクセス権」欄は、アプリケーション構成および構成テンプレートを含むSAライブラリ内のフォルダーに対するアクセス権です。

ユーザーがアクションを実行するには、複数のアクセス権が必要です。たとえば、アプリケーション構成をサーバーにアタッチする場合、ユーザーには次のアクセス権が必要です。

- アプリケーション構成の管理:読み取り
- 構成テンプレートの管理: 読み取り

- サーバー上のインストール済み構成とバックアップの管理: 読み取り/書き込み
- 管理対象サーバーおよびグループ
- サーバーのファシリティ、デバイスグループ、カスタマーに対する読み取り/書き込みアクセス権
- アプリケーション構成またはテンプレートを含む SA ライブラリ内のフォルダーに対する読み取りアクセス権

表47　　ユーザーのアクションに必要なアプリケーション構成管理のアクセス権

ユーザーのアクション	アクションのアクセス権	サーバーのアクセス権 (カスタマー、ファシリティ、デバイスグループ)	フォルダーのアクセス権 (アプリケーション構成、アプリケーション構成テンプレート)
アプリケーション構成			
アプリケーション構成の作成	アプリケーション構成の管理: 読み取り/書き込み および構成テンプレートの管理: 読み取り	なし	読み取り/書き込み
アプリケーション構成の表示	アプリケーション構成の管理: 読み取り/書き込み および構成テンプレートの管理: 読み取り	なし	読み取り
アプリケーション構成の編集	アプリケーション構成の管理: 読み取り/書き込み および構成テンプレートの管理: 読み取り	なし	読み取り/書き込み
アプリケーション構成の削除	アプリケーション構成の管理: 読み取り/書き込み および構成テンプレートの管理: 読み取り	なし	読み取り/書き込み
テンプレート順序の指定	アプリケーション構成の管理: 読み取り/書き込み および構成テンプレートの管理: 読み取り	なし	読み取り/書き込み

表47　ユーザーのアクションに必要なアプリケーション構成管理のアクセス権（続き）

ユーザーのアクション	アクションのアクセス権	サーバーのアクセス権 (カスタマー、ファシリティ、デバイスグループ)	フォルダーのアクセス権 (アプリケーション構成、アプリケーション構成テンプレート)
アプリケーション構成のサーバーへのアタッチ	アプリケーション構成の管理: 読み取り および構成テンプレートの管理: 読み取り およびサーバー上のインストール済み構成とバックアップの管理: 読み取り/書き込み	読み取り/書き込み	読み取り
アプリケーション構成のデバイスグループへのアタッチ	アプリケーション構成の管理: 読み取り および構成テンプレートの管理: 読み取り およびサーバー上のインストール済み構成とバックアップの管理: 読み取り/書き込み およびパブリックデバイスグループの管理: はい およびパブリックデバイスグループのモデル化: はい	読み取り/書き込み	読み取り
サーバーでのアプリケーション構成の値の設定	アプリケーション構成の管理: 読み取り および構成テンプレートの管理: 読み取り およびサーバー上のインストール済み構成とバックアップの管理: 読み取り/書き込み	読み取り/書き込み	読み取り
アプリケーション構成のサーバーへのプッシュ	アプリケーション構成の管理: 読み取り および構成テンプレートの管理: 読み取り およびサーバー上のインストール済み構成とバックアップの管理: 読み取り/書き込み	読み取り/書き込み	読み取り

表47　ユーザーのアクションに必要なアプリケーション構成管理のアクセス権（続き）

ユーザーのアクション	アクションのアクセス権	サーバーのアクセス権 (カスタマー、ファシリティ、デバイスグループ)	フォルダーのアクセス権 (アプリケーション構成、アプリケーション構成テンプレート)
アプリケーション構成のプッシュのスケジュール	アプリケーション構成の管理: 読み取り および構成テンプレートの管理: 読み取り およびサーバー上のインストール済み構成とバックアップの管理: 読み取り/書き込み	読み取り/書き込み	読み取り
構成コンプライアンスのスキャン	構成コンプライアンススキャンの許可: はい およびアプリケーション構成の管理: 読み取り および構成テンプレートの管理: 読み取り	読み取り	読み取り
アプリケーション構成の監査のスケジュール	構成コンプライアンススキャンの許可: はい およびアプリケーション 構成の管理: 読み取り および構成テンプレートの管理: 読み取り	読み取り	読み取り
アプリケーション構成のプッシュのロールバック (元に戻す)	アプリケーション構成の管理: 読み取り および構成テンプレートの管理: 読み取り およびサーバー上のインストール済み構成とバックアップの管理: 読み取り/書き込み	読み取り/書き込み	読み取り
アプリケーション構成テンプレート			
アプリケーション構成テンプレートの作成	構成テンプレートの管理: 読み取り/書き込み	なし	読み取り/書き込み
アプリケーション構成テンプレートの表示	構成テンプレートの管理: 読み取り/書き込み	なし	読み取り

表47　ユーザーのアクションに必要なアプリケーション構成管理のアクセス権（続き）

ユーザーのアクション	アクションのアクセス権	サーバーのアクセス権(カスタマー、ファシリティ、デバイスグループ)	フォルダーのアクセス権(アプリケーション構成、アプリケーション構成テンプレート)
アプリケーション構成テンプレートの編集	構成テンプレートの管理: 読み取り/書き込み	なし	読み取り/書き込み
アプリケーション構成テンプレートの削除	構成テンプレートの管理: 読み取り/書き込み	なし	読み取り/書き込み
アプリケーション構成テンプレートのロード(インポート)	アプリケーション構成の管理: 読み取り/書き込み および構成テンプレートの管理: 読み取り/書き込み	なし	読み取り/書き込み
アプリケーション構成テンプレートをスクリプトとして実行するように設定	構成テンプレートの管理: 読み取り/書き込み	なし	読み取り/書き込み
2つのアプリケーション構成テンプレートの比較	構成テンプレートの管理: 読み取り	なし	読み取り
アプリケーション構成テンプレートを実際の構成ファイルと比較(プレビュー)	アプリケーション構成の管理: 読み取り および構成テンプレートの管理: 読み取り およびサーバー上のインストール済み構成とバックアップの管理: 読み取り	読み取り	読み取り

表48に、アクセス権ごとにユーザーがアプリケーション構成で実行できるアクションを示します。表48は表47と同じデータを、アクセス権ごとに整理したものです。表48には示されていませんが、OSプロビジョニングのすべてのアクションに対して、管理対象サーバーおよびグループのアクセス権が必要です。

セキュリティ管理者は、表48を参照して特定のアクセス権が割り当てられたユーザーが実行できるアクションを確認できます。

表48　アプリケーション構成管理のアクセス権で使用できるユーザーアクション

アクションのアクセス権	ユーザーのアクション	サーバーのアクセス権 (カスタマー、ファシリティ、デバイスグループ)	フォルダーのアクセス権 (アプリケーション構成、アプリケーション構成テンプレート)
構成コンプライアンススキャンの許可: はい およびアプリケーション構成の管理: 読み取り および構成テンプレートの管理: 読み取り	構成コンプライアンスのスキャン	読み取り	読み取り
	アプリケーション構成の監査のスケジュール	読み取り	読み取り
アプリケーション構成の管理: 読み取り/書き込み および構成テンプレートの管理: 読み取り	アプリケーション構成の作成	なし	読み取り/書き込み
	アプリケーション構成の削除	なし	読み取り/書き込み
	アプリケーション構成の編集	なし	読み取り/書き込み
	テンプレート順序の指定	なし	読み取り/書き込み
	アプリケーション構成の表示	なし	読み取り
アプリケーション構成の管理: 読み取り/書き込み および構成テンプレートの管理: 読み取り/書き込み	アプリケーション構成テンプレートのロード (インポート)	なし	読み取り/書き込み
アプリケーション構成の管理: 読み取り および構成テンプレートの管理: 読み取り およびサーバー上のインストール済み構成とバックアップの管理: 読み取り	アプリケーション構成テンプレートを実際の構成ファイルと比較 (プレビュー)	読み取り	読み取り

表48 アプリケーション構成管理のアクセス権で使用できるユーザーアクション（続き）

アクションのアクセス権	ユーザーのアクション	サーバーのアクセス権 (カスタマー、ファシリティ、デバイスグループ)	フォルダーのアクセス権 (アプリケーション構成、アプリケーション構成テンプレート)
アプリケーション構成の管理: 読み取り および構成テンプレートの管理: 読み取り およびサーバー上のインストール済み構成とバックアップの管理: 読み取り/書き込み	アプリケーション構成のサーバーへのアタッチ	読み取り/書き込み	読み取り
	アプリケーション構成のサーバーへのプッシュ	読み取り/書き込み	読み取り
	アプリケーション構成のプッシュのロールバック (元に戻す)	読み取り/書き込み	読み取り
	アプリケーション構成のプッシュのスケジュール	読み取り/書き込み	読み取り
	サーバーでのアプリケーション構成の値の設定	読み取り/書き込み	読み取り
アプリケーション構成の管理: 読み取り および構成テンプレートの管理: 読み取り およびサーバー上のインストール済み構成とバックアップの管理: 読み取り/書き込み およびパブリックデバイスグループの管理: はい およびパブリックデバイスグループのモデル化: はい	アプリケーション構成のデバイスグループへのアタッチ	読み取り/書き込み	読み取り
構成テンプレートの管理: 読み取り	2つのアプリケーション構成テンプレートの比較	なし	読み取り
構成テンプレートの管理: 読み取り/書き込み	アプリケーション構成テンプレートの作成	なし	読み取り/書き込み
	アプリケーション構成テンプレートの削除	なし	読み取り/書き込み
	アプリケーション構成テンプレートの編集	なし	読み取り/書き込み
構成テンプレートの管理: 読み取り/書き込み (続き)	アプリケーション構成テンプレートをスクリプトとして実行するように設定	なし	読み取り/書き込み
	アプリケーション構成テンプレートの表示	なし	読み取り

Windowsパッチ管理のアクセス権

表49は、SAクライアントの特定のアクションをユーザーが実行するのに必要なWindowsパッチ管理のアクセス権を示しています。セキュリティ管理者は、ユーザーが特定のアクションを実行するのに必要なアクセス権をこの表で確認することができます。

- 表49に記載したアクセス権に加えて、すべてのユーザーのアクションで管理対象サーバーおよびグループのアクセス権が必要です。

表49の「ユーザーアクション」欄のエントリは、ほとんどがSAクライアントのメニュー項目に対応しています。アクションのアクセス権のほかに、パッチの適用操作の影響を受ける管理対象サーバーではサーバーのアクセス権が必要になります。

- [パッチのインストールの許可]のアクセス権が[はい]に設定されている場合、[パッチの管理]と[Windowsパッチポリシーの管理]のアクセス権は自動的に[読み取り]に設定されます。

表49　ユーザーのアクションに必要なWindowsパッチ管理のアクセス権

ユーザーのアクション	アクションのアクセス権	サーバーのアクセス権(カスタマー、ファシリティ、デバイスグループ)
パッチ		
パッチのインストール(利用可能)	パッチのインストールの許可: はい パッチの管理: 読み取り	読み取り/書き込み
パッチのアンインストール(利用可能)	パッチのアンインストールの許可: はい およびパッチの管理: 読み取り	読み取り/書き込み
パッチのインストール(制限付き可用性)	パッチのインストールの許可: はい パッチの管理: 読み取り/書き込み	読み取り/書き込み
パッチのアンインストール(制限付き可用性)	パッチのアンインストールの許可: はい およびパッチの管理: 読み取り/書き込み	読み取り/書き込み
パッチを開く(パッチの表示)	パッチの管理: 読み取り	該当なし
パッチのプロパティの変更	パッチの管理: 読み取り/書き込み	該当なし
パッチのインポート	パッチの管理: 読み取り/書き込み およびパッケージ	該当なし
パッチデータベースのインポート	パッチの管理: 読み取り/書き込み	該当なし
パッチのエクスポート	パッチの管理: 読み取り およびパッケージ	該当なし
パッチのエクスポート	または、パッチのインストールの許可: はい およびパッケージ: はい	該当なし
パッチのエクスポート	または、パッチのアンインストールの許可: はい およびパッケージ	該当なし
パッチのエクスポート	または、ポリシーの管理: 読み取り およびパッケージ	該当なし
パッチの削除	パッチの管理: 読み取り/書き込み	該当なし

表49　ユーザーのアクションに必要なWindowsパッチ管理のアクセス権（続き）

ユーザーのアクション	アクションのアクセス権	サーバーのアクセス権(カスタマー、ファシリティ、デバイスグループ)
パッチポリシーと例外		
ポリシーの修復	パッチのインストールの許可: はい	読み取り/書き込み
パッチポリシーを開く(表示)	Windowsパッチポリシーの管理: 読み取り	該当なし
パッチをパッチポリシーに追加	パッチの管理: 読み取り およびWindowsパッチポリシーの管理: 読み取り/書き込み	該当なし
パッチをパッチポリシーから削除	Windowsパッチポリシーの管理: 読み取り/書き込み	該当なし
例外の設定	パッチのインストールの許可: はい	読み取り/書き込み
例外の設定	または、パッチのアンインストールの許可: はい	読み取り/書き込み
例外のコピー	パッチのインストールの許可: はい	読み取り/書き込み
例外のコピー	または、パッチのアンインストールの許可: はい	読み取り/書き込み
パッチポリシーのサーバー(またはデバイスグループ)へのアタッチ	Windowsパッチポリシーの管理: 読み取り	読み取り/書き込み
パッチポリシーのサーバー(またはデバイスグループ)からのデタッチ	Windowsパッチポリシーの管理: 読み取り	読み取り/書き込み
パッチポリシーの作成	Windowsパッチポリシーの管理: 読み取り/書き込み	該当なし
パッチポリシーの削除	Windowsパッチポリシーの管理: 読み取り/書き込み	該当なし
パッチポリシーのプロパティの変更	Windowsパッチポリシーの管理: 読み取り/書き込み	該当なし
パッチポリシーコンプライアンスルール		
パッチ製品の編集 ([パッチ構成]ウィンドウ)	パッチコンプライアンスルールの管理: はい	該当なし
パッチコンプライアンスのスキャン	Windowsパッチポリシーの管理: 読み取り	該当なし
パッチポリシーのスキャンのスケジュール	パッチコンプライアンスルールの管理: はい	該当なし
デフォルトのパッチの可用性の変更	パッチコンプライアンスルールの管理: はい	該当なし
パッチポリシーのコンプライアンスルールの変更	パッチコンプライアンスルールの管理: はい	該当なし
パッチポリシーのコンプライアンスルールの表示	Windowsパッチポリシーの管理: はい	該当なし

表50に、パッチ管理のアクセス権ごとにユーザーが実行できるアクションを示します。表50は表49と同じデータを、アクションのアクセス権ごとに整理したものです。表50には示されていませんが、パッチ管理のすべてのアクションに対して、管理対象サーバーおよびグループのアクセス権が必要です。

セキュリティ管理者は、表50を参照して特定のアクションのアクセス権が割り当てられたユーザーが実行できるアクションを確認できます。

表50 Windowsパッチ管理のアクセス権で使用できるユーザーアクション

アクションのアクセス権	ユーザーのアクション	サーバーのアクセス権 (カスタマー、ファシリティ、デバイスグループ)
パッチのインストールの許可: はい	例外のコピー	読み取り/書き込み
	ポリシーの修復	読み取り/書き込み
	例外の設定	読み取り/書き込み
パッチのインストールの許可: はい およびパッチの管理: 読み取り	パッチのインストール (利用可能)	読み取り/書き込み
	パッチのアンインストール (利用可能)	読み取り/書き込み
パッチのインストールの許可: はい およびパッチの管理: 読み取り/書き込み	パッチのインストール (制限付き可用性)	読み取り/書き込み
	パッチのアンインストール (制限付き可用性)	読み取り/書き込み
パッチのインストールの許可: はい およびパッケージ: はい	パッチのエクスポート	該当なし
パッチのアンインストールの許可: はい	例外のコピー	読み取り/書き込み
	例外の設定	読み取り/書き込み
パッチのアンインストールの許可: はい およびパッケージ	パッチのエクスポート	該当なし
パッチのアンインストールの許可: はい およびパッチの管理: 読み取り	パッチのアンインストール	読み取り/書き込み
パッチコンプライアンスルールの管理: はい	デフォルトのパッチの可用性の変更	該当なし
	パッチポリシーのコンプライアンスルールの変更	該当なし
	パッチ製品の編集 ([パッチ構成] ウィンドウ)	該当なし
	パッチポリシーのスキャンのスケジュール	該当なし
Windowsパッチポリシーの管理: 読み取り	パッチポリシーのサーバー (またはデバイスグループ) へのアタッチ	読み取り/書き込み
	パッチポリシーのサーバー (またはデバイスグループ) からのデタッチ	読み取り/書き込み
	パッチポリシーを開く (表示)	該当なし
Windowsパッチポリシーの管理: 読み取り/書き込み	パッチポリシーのプロパティの変更	該当なし
	パッチポリシーの作成	該当なし
	パッチポリシーの削除	該当なし
	パッチをパッチポリシーから削除	該当なし

表50 Windowsパッチ管理のアクセス権で使用できるユーザーアクション（続き）

アクションのアクセス権	ユーザーのアクション	サーバーのアクセス権 (カスタマー、ファシリティ、デバイスグループ)
Windowsパッチポリシーの管理: はい	パッチポリシーのコンプライアンスルールの表示	該当なし
パッチの管理: 読み取り	パッチを開く (パッチの表示) パッチコンプライアンスのスキャン	該当なし
パッチの管理: 読み取り/書き込み	パッチのプロパティの変更	該当なし
	パッチの削除	該当なし
	パッチデータベースのインポート	該当なし
パッチの管理: 読み取り/書き込み およびパッケージ	パッチのインポート	該当なし
パッチの管理: 読み取り およびWindowsパッチポリシーの管理: 読み取り/書き込み	パッチをパッチポリシーに追加	該当なし
パッチの管理: 読み取り およびパッケージ	パッチのエクスポート	該当なし
ポリシーの管理: 読み取り およびパッケージ	パッチのエクスポート	該当なし

Ubuntuパッチ管理のアクセス権

Ubuntuパッチ管理では、すべてのユーザーの役割が集約されています。つまり、シングルユーザーがパッチ管理のあらゆるアクションを実行できます。Ubuntu の初期設定では、次のユーザーグループの役割がユーザーに与えられます。

- Patch Policy Setter
- Patch Deployer
- Software Policy Setter
- Policy Deployer

さらに、次に示す条件を満たしている必要があります。

- Ubuntuパッチポリシーを構成する場合:
  - ユーザーは、Patch Policy SettersとSoftware Policy Settersの両方のユーザーグループに属している必要があります。
  - ユーザーは、サーバーが属しているカスタマーの読み取り/書き込みリソースのアクセス権を保持している必要があります。
  - データセンターは、上記のグループの両方に追加する必要があります。
- Ubuntuパッチポリシーをデプロイする場合:
  - ユーザーは、Patch DeployersとSoftware Deployersの両方のユーザーグループに属している必要があります。

- ユーザーは、サーバーが属しているカスタマーの読み取り/書き込みリソースのアクセス権を保持している必要があります。
- データセンターは、上記のグループの両方に追加する必要があります。

• Ubuntuパッチポリシーを Ubuntuサーバーに追加する場合:

- ユーザーは、ターゲットのパッチポリシーが格納されているフォルダーの読み取り/書き込みアクセス権を保持している必要があります。
- Debianパッケージをインポートするには、ユーザーは、Opswareカスタマーの読み取り/書き込みリソースのアクセス権を保持している必要があります。

➤ 標準のパッチアクションのアクセス権については、Windowsパッチ管理のアクセス権 (283ページ) を参照してください。

サーバーが管理対象になっているファシリティのユーザーグループの役割を与えられたユーザーが、Ubuntuパッチを使用する正しいアクセス権を保持するには、表51に示すフォルダーのアクセス権を保持している必要があります。

表51 Ubuntuユーザーグループの役割に対するフォルダーのアクセス権

フォルダー	ユーザーグループの役割	アクセス権
/Opsware	Patch Policy Setter	読み取り/書き込み
/Opsware	Software Policy Setter	読み取り/書き込み
/Opsware	Patch Policy Deployer	読み取り
/Opsware	Software Policy Deployer	読み取り
/Opsware	Superuser	読み取り/書き込み
/Opsware	Opsware System Administrator	読み取り/書き込み
/Opsware/Patching/Tools	Patch Policy Setter	読み取り、リスト、実行
/Opsware/Patching/Tools	Software Policy Setter	読み取り、リスト、実行
/Opsware/Patching/Tools	Patch Policy Deployer	読み取り、リスト、実行
/Opsware/Patching/Tools	Software Policy Deployer	読み取り、リスト、実行
/Opsware/Patching/Tools	Superuser	読み取り、リスト、実行
/Opsware/Patching/Tools	Opsware System Administrator	読み取り、リスト、実行
/Opsware/Patching/Tools	Command-Line Administrator	読み取り、リスト、実行

Solarisパッチ管理のアクセス権

この項では、Solarisシステムでパッチを管理するためのアクセス権について説明します。他のUNIXシステムのパッチについては、その他のUNIXパッチ管理のアクセス権 (291ページ) を参照してください。Solarisパッチポリシーのアクセス権については、Solarisパッチポリシー管理のアクセス権 (289ページ) を参照してください。

表52は、SAクライアントの特定のアクションをユーザーが実行するのに必要なパッチ管理のアクセス権を示しています。セキュリティ管理者は、ユーザーが特定のアクションを実行するのに必要なアクセス権をこの表で確認することができます。

➤ 表52に記載したアクセス権に加えて、すべてのユーザーのアクションで管理対象サーバーおよびグループのアクセス権が必要です。

表52の「ユーザーアクション」欄のエントリは、ほとんどがSAクライアントのメニュー項目に対応しています。アクションのアクセス権のほかに、パッチの適用操作の影響を受ける管理対象サーバーではサーバーのアクセス権が必要になります。

パッチのインストールの許可のアクセス権が [はい] に設定されている場合、パッチの管理のアクセス権は自動的に [読み取り] に設定されます。Solarisパッチポリシーを使用する予定がある場合は、ソフトウェアポリシーの管理を [読み取り] または [読み取り/書き込み] に設定してください。詳細については、Solarisパッチポリシー管理のアクセス権 (289ページ) を参照してください。

表52　ユーザーのアクションに必要なSolarisパッチ管理のアクセス権

ユーザーのアクション	アクションのアクセス権	サーバーのアクセス権 (カスタマー、ファシリティ、デバイスグループ)
パッチ		
パッチのインストール (利用可能)	パッチのインストールの許可: はい パッチの管理: 読み取り	読み取り/書き込み
パッチのアンインストール (利用可能)	パッチのアンインストールの許可: はい パッチの管理: 読み取り	読み取り/書き込み
パッチのインストール (制限付き可用性)	パッチのインストールの許可: はい パッチの管理: 読み取り/書き込み	読み取り/書き込み
パッチのアンインストール (制限付き可用性)	パッチのアンインストールの許可: はい パッチの管理: 読み取り/書き込み	読み取り/書き込み
パッチを開く (パッチの表示)	パッチの管理: 読み取り	該当なし
パッチのプロパティの変更	パッチの管理: 読み取り/書き込み	該当なし
パッチのインポート	パッチの管理: 読み取り/書き込み	該当なし
パッチのエクスポート	パッチの管理: 読み取り パッチのインストールの許可: はい (オプション) パッチのアンインストールの許可: はい (オプション) ソフトウェアポリシーの管理: 読み取り (オプション)	該当なし
パッチの削除	パッチの管理: 読み取り/書き込み	該当なし

表53に、Solarisパッチ管理のアクセス権ごとにユーザーが実行できるアクションを示します。表53は表52と同じデータを、アクションのアクセス権ごとに整理したものです。表53には示されていませんが、パッチ管理のすべてのアクションに対して、管理対象サーバーおよびグループのアクセス権が必要です。

セキュリティ管理者は、表53を参照して特定のアクションのアクセス権が割り当てられたユーザーが実行できるアクションを確認できます。

表53　Solarisパッチ管理のアクセス権で使用できるユーザーアクション

アクションのアクセス権	ユーザーのアクション	サーバーのアクセス権 (カスタマー、ファシリティ、デバイスグループ)
パッチのインストールの許可: はい	ポリシーの修復	読み取り/書き込み
パッチのインストールの許可: はい パッチの管理: 読み取り	パッチのインストール (利用可能)	読み取り/書き込み
	パッチのアンインストール (利用可能)	読み取り/書き込み
パッチのインストールの許可: はい パッチの管理: 読み取り/書き込み	パッチのインストール (制限付き可用性)	読み取り/書き込み
	パッチのアンインストール (制限付き可用性)	読み取り/書き込み
パッチのインストールの許可: はい (パッチの管理を併せて設定: 読み取り)	パッチのエクスポート	該当なし
パッチのアンインストールの許可: はい (パッチの管理を併せて設定: 読み取り)	パッチのエクスポート	該当なし
パッチのアンインストールの許可: はい (パッチの管理を併せて設定: 読み取り)	パッチのアンインストール	読み取り/書き込み
パッチの管理: 読み取り	パッチを開く (パッチの表示)	該当なし
	パッチのエクスポート	該当なし
パッチの管理: 読み取り/書き込み	パッチのプロパティの変更	該当なし
	パッチの削除	該当なし
	パッチのインポート	該当なし

Solarisパッチポリシー管理のアクセス権

表54は、SAクライアントの特定のアクションをユーザーが実行するのに必要なSolarisパッチポリシー管理のアクセス権を示しています。セキュリティ管理者は、ユーザーが特定のアクションを実行するのに必要なアクセス権をこの表で確認することができます。

カスタマーをフォルダーに割り当てた場合、フォルダー内のSolarisパッチポリシーを関連付けることが可能なオブジェクトにカスタマーの制約が適用されることがあります。これらの制約の影響を受けるタスク一覧については、フォルダー、カスタマーの制約、ソフトウェアポリシー (24ページ) を参照してください。

表54 ユーザーのアクションに必要なSolarisパッチポリシー管理のアクセス権

ユーザーのアクション	アクションのアクセス権	サーバーのアクセス権 (カスタマー、ファシリティ、デバイスグループ)	フォルダーのアクセス権
Solaris パッチポリシー			
Solarisパッチポリシーの作成	ソフトウェアポリシーの管理: 読み取り/書き込み	該当なし	書き込み
Solarisパッチポリシーの削除	ソフトウェアポリシーの管理: 読み取り/書き込み	該当なし	書き込み
Solarisパッチポリシーを開く (表示)	ソフトウェアポリシーの管理: 読み取り	該当なし	読み取り
Solarisパッチポリシーのプロパティの編集	ソフトウェアポリシーの管理: 読み取り/書き込み	該当なし	書き込み
パッチの追加	ソフトウェアポリシーの管理: 読み取り/書き込み パッチの管理: 読み取り	該当なし	ソフトウェアポリシーを含むフォルダー: 書き込み
スクリプトの追加	ソフトウェアポリシーの管理: 読み取り/書き込み サーバースクリプトの管理: 読み取り	該当なし	ソフトウェアポリシーを含むフォルダー: 書き込み
パッチの削除	ソフトウェアポリシーの管理: 読み取り/書き込み	該当なし	書き込み
スクリプトの削除	ソフトウェアポリシーの管理: 読み取り/書き込み	該当なし	書き込み
Solarisパッチポリシーのアタッチ	ソフトウェアポリシーの管理: 読み取り ソフトウェアポリシーのアタッチ/デタッチの許可: はい パブリックデバイスグループのモデル化: はい (このアクセス権は、Solarisパッチポリシーをパブリックデバイスグループにアタッチする場合に必要)	読み取り/書き込み	読み取り

表54　ユーザーのアクションに必要なSolarisパッチポリシー管理のアクセス権（続き）

ユーザーのアクション	アクションのアクセス権	サーバーのアクセス権 (カスタマー、ファシリティ、デバイスグループ)	フォルダーのアクセス権
Solarisパッチポリシーのデタッチ	ソフトウェアポリシーの管理: 読み取り ソフトウェアポリシーのアタッチ/デタッチの許可: はい パブリックデバイスグループのモデル化: はい (このアクセス権は、Solarisパッチポリシーをパブリックデバイスグループにアタッチする場合に必要)	読み取り/書き込み	読み取り
修復	ソフトウェアポリシーの管理: 読み取り サーバーの修復の許可: はい パブリックデバイスグループのモデル化: はい (パブリックデバイスグループを修復する場合に必要)	読み取り/書き込み	読み取り
Solarisパッチコンプライアンスのスキャン	該当なし	読み取り	該当なし
Solarisパッチポリシーの名前の変更	ソフトウェアポリシーの管理: 読み取り/書き込み	該当なし	書き込み
Solarisパッチポリシーの切り取り	ソフトウェアポリシーの管理: 読み取り/書き込み	該当なし	書き込み
Solarisパッチポリシーのコピー	ソフトウェアポリシーの管理: 読み取り	該当なし	読み取り
Solarisパッチポリシーの貼り付け	ソフトウェアポリシーの管理: 読み取り/書き込み	該当なし	ソースフォルダー: 読み取り (コピーして貼り付けの場合) ソースフォルダー: 読み取り (切り取り/貼り付けの場合) ターゲットフォルダー: 書き込み
Solarisパッチポリシーの移動	ソフトウェアポリシーの管理: 読み取り/書き込み	該当なし	ソースフォルダー: 書き込み ターゲットフォルダー: 書き込み

その他のUNIXパッチ管理のアクセス権

この項では、Solaris 以外の UNIX システムでパッチを管理するためのアクセス権について説明します。Solaris については、Solarisパッチ管理のアクセス権 (287ページ) を参照してください。UNIXのパッチではソフトウェアポリシーを使用できます。詳細については、ソフトウェア管理のアクセス権 (265 ページ) を参照してください。

表55は、SAクライアントの特定のアクションをユーザーが実行するのに必要なパッチ管理のアクセス権を示しています。セキュリティ管理者は、ユーザーが特定のアクションを実行するのに必要なアクセス権をこの表で確認することができます。

- 表55に記載したアクセス権に加えて、すべてのユーザーのアクションで管理対象サーバーおよびグループのアクセス権が必要です。

表55の「ユーザーアクション」欄のエントリは、ほとんどがSAクライアントのメニュー項目に対応しています。アクションのアクセス権のほかに、パッチの適用操作の影響を受ける管理対象サーバーではサーバーのアクセス権が必要になります。

- パッチのインストールの許可のアクセス権が [はい] に設定されている場合、パッチの管理のアクセス権は自動的に [読み取り] に設定されます。ポリシーを使用する予定がある場合は、ソフトウェアポリシーの管理を [読み取り] または [読み取り/書き込み] に設定してください。

表55　　ユーザーアクションに必要なUNIXパッチ管理のアクセス権

ユーザーのアクション	アクションのアクセス権	サーバーのアクセス権 (カスタマー、ファシリティ、デバイスグループ)
パッチ		
パッチのインストール (利用可能)	パッチのインストールの許可: はい パッチの管理: 読み取り	読み取り/書き込み
パッチのアンインストール (利用可能)	パッチのアンインストールの許可: はい およびパッチの管理: 読み取り	読み取り/書き込み
パッチのインストール (制限付き可用性)	パッチのインストールの許可: はい パッチの管理: 読み取り/書き込み	読み取り/書き込み
パッチのアンインストール (制限付き可用性)	パッチのアンインストールの許可: はい およびパッチの管理: 読み取り/書き込み	読み取り/書き込み
パッチを開く (パッチの表示)	パッチの管理: 読み取り	該当なし
パッチのプロパティの変更	パッチの管理: 読み取り/書き込み	該当なし
パッチのエクスポート	パッチの管理: 読み取り およびパッケージ	該当なし
パッチのエクスポート	または、パッチのインストールの許可: はい およびパッケージ: はい	該当なし
パッチのエクスポート	または、パッチのアンインストールの許可: はい およびパッケージ	該当なし
パッチのエクスポート	または、ポリシーの管理: 読み取り およびパッケージ	該当なし
パッチの削除	パッチの管理: 読み取り/書き込み	該当なし

表56に、パッチ管理のアクセス権ごとにユーザーが実行できるアクションを示します。表56は表55と同じデータを、アクションのアクセス権ごとに整理したものです。表56には示されていませんが、パッチ管理のすべてのアクションに対して、管理対象サーバーおよびグループのアクセス権が必要です。

セキュリティ管理者は、表56を参照して特定のアクションのアクセス権が割り当てられたユーザーが実行できるアクションを確認できます。

表56　UNIXパッチ管理のアクセス権で使用できるユーザーアクション

アクションのアクセス権	ユーザーのアクション	サーバーのアクセス権 (カスタマー、ファシリティ、デバイスグループ)
パッチのインストールの許可: はい	例外のコピー	読み取り/書き込み
	ポリシーの修復	読み取り/書き込み
	例外の設定	読み取り/書き込み
パッチのインストールの許可: はい およびパッチの管理: 読み取り	パッチのインストール (利用可能)	読み取り/書き込み
	パッチのアンインストール (利用可能)	読み取り/書き込み
パッチのインストールの許可: はい およびパッチの管理: 読み取り/書き込み	パッチのインストール (制限付き可用性)	読み取り/書き込み
	パッチのアンインストール (制限付き可用性)	読み取り/書き込み
パッチのインストールの許可: はい およびパッケージ: はい	パッチのエクスポート	該当なし
パッチのアンインストールの許可: はい	例外のコピー	読み取り/書き込み
	例外の設定	読み取り/書き込み
パッチのアンインストールの許可: はい およびパッケージ	パッチのエクスポート	該当なし
パッチの管理: 読み取り	パッチを開く (パッチの表示)	該当なし
パッチの管理: 読み取り/書き込み	パッチのプロパティの変更	該当なし
	パッチの削除	該当なし
	パッチデータベースのインポート	該当なし
パッチの管理: 読み取り/書き込み およびパッケージ	パッチのインポート	該当なし
パッチの管理: 読み取り およびポリシーの管理: 読み取り/書き込み	パッチをポリシーに追加	該当なし
パッチの管理: 読み取り およびパッケージ	パッチのエクスポート	該当なし
ポリシーの管理: 読み取り およびパッケージ	パッチのエクスポート	該当なし

監査と修復のアクセス権

表57は、SAクライアントの特定のアクションをユーザーが実行するのに必要な監査と修復のアクセス権を示しています。セキュリティ管理者は、ユーザーが特定のアクションを実行するのに必要なアクセス権をこの表で確認することができます。

➤ 表57に記載したアクセス権に加えて、すべてのユーザーのアクションで管理対象サーバーおよびグループのアクセス権が必要です。

監査と修復に必要なサーバーのアクセス権

監査と修復のアクションには、アクションのアクセス権とサーバーのアクセス権の両方が必要です。たとえば、監査の作成アクションでは、「監査の管理: 読み取り/書き込み」と管理対象サーバーおよびグループのアクセス権が必要です。また、このアクションでは、監査によって参照されるサーバーに対する読み取りアクセス権も必要です。表 57 の「サーバーのアクセス権」欄は、それぞれのアクションに応じて監査またはスナップショット仕様で参照されるサーバーに対するアクセス権です。サーバーのアクセス権は、SA Webクライアントでカスタマー、ファシリティ、デバイスグループのアクセス権で指定します。

監査と修復オブジェクト (スナップショット仕様など) で複数のサーバーを参照する場合は、参照されるすべてのサーバーで、少なくとも読み取りアクセス権が必要です。それ以外の場合、このオブジェクトを表示または変更できません。

監査と修復オブジェクトは、カスタマーとファシリティには直接関連付けられません。カスタマーとファシリティのアクセス権は、スナップショット仕様や監査などの監査と修復で参照されるサーバーへのアクセスを制御します。

監査と修復に関する「タスク固有ポリシーの作成の許可アクセス権」

ベストプラクティスとして、このアクセス権は有効にしない (このアクセス権を「はい」に設定しない) ようにしてください。デフォルトで、このアクセス権は無効になっています (「いいえ」に設定済みです)。監査ポリシーで監査ルールを作成した後に、監査タスクとスナップショット仕様をその監査ポリシーにリンクすることをお勧めします。

監査と修復に必要なOGFSアクセス権

管理対象サーバーのファイルシステムにアクセスするアクションでは、サーバーファイルシステムの読み取りの OGFS アクセス権が必要です。たとえば、管理対象サーバーのファイルを含むスナップショット仕様とルールを作成するには、サーバーファイルシステムの読み取りのアクセス権が必要です。これらのルールには、アプリケーション構成、カスタムスクリプト、COM+オブジェクト、ファイルシステム、IISメタベースエントリ、Windowsレジストリなどが含まれます。

その他の選択条件のタイプでは、次の対応するOGFSアクセス権が必要です。

- サーバーレジストリの読み取り
- COM+データベースの読み取り
- IISメタベースの読み取り

監査と修復のユーザーアクションのアクセス権

次の表に、監査と修復の一般的なユーザーアクションとそのアクションを実行するのに必要なアクセス権を示します。

表57　　ユーザーのアクションに必要な監査と修復のアクセス権

ユーザーのアクション	アクションのアクセス権	OGFSアクセス権	サーバーのアクセス権(カスタマー、ファシリティ、デバイスグループ)
スナップショット仕様			
スナップショット仕様の内容の表示	スナップショット仕様の管理: 読み取り	該当なし	読み取り
スナップショット仕様のスケジュールと実行	スナップショット仕様の管理: 読み取り	該当なし	読み取り
スナップショット仕様の作成	スナップショット仕様の管理: 読み取り/書き込み	該当なし	読み取り/書き込み
アプリケーション構成ルールの作成	スナップショット仕様の管理: 読み取り/書き込み	サーバーファイルシステムの書き込み	読み取り/書き込み
COM+ルールの作成	スナップショット仕様の管理: 読み取り/書き込み	COM+データベースの読み取り	読み取り/書き込み
カスタムスクリプトルールの作成	スナップショット仕様の管理: 読み取り/書き込み カスタムスクリプトポリシールールの作成の許可: はい	サーバーファイルシステムの書き込み	読み取り/書き込み
ファイルの作成	スナップショット仕様の管理: 読み取り/書き込み	サーバーファイルシステムの書き込み	読み取り/書き込み
IISメタベースルールの作成	スナップショット仕様の管理: 読み取り/書き込み	IISメタベースの読み取り	読み取り/書き込み
レジストリルールの作成	スナップショット仕様の管理: 読み取り/書き込み	サーバーレジストリの読み取り	読み取り/書き込み
スナップショット仕様への監査ポリシーのリンク	スナップショット仕様の管理: 読み取り/書き込み 監査ポリシーの管理: 読み取り ライブラリフォルダー : 読み取り	該当なし	読み取り/書き込み
スナップショット仕様への監査ポリシーのインポート	スナップショット仕様の管理: 読み取り/書き込み 監査ポリシーの管理: 読み取り ライブラリフォルダー : 読み取り	該当なし	読み取り/書き込み

表57　ユーザーのアクションに必要な監査と修復のアクセス権（続き）

ユーザーのアクション	アクションのアクセス権	OGFSアクセス権	サーバーのアクセス権(カスタマー、ファシリティ、デバイスグループ)
監査ポリシーに名前を付けて保存	スナップショット仕様の管理: 読み取り/書き込み 監査ポリシーの管理: 読み取り/書き込み ライブラリフォルダー : 読み取り/書き込み	該当なし	読み取り/書き込み
スナップショット			
スナップショットの内容の表示、リスト	スナップショットの管理: 読み取り スナップショット仕様の管理: 読み取り	該当なし	読み取り
スナップショットからの監査の作成	スナップショットの管理: 読み取り スナップショット仕様の管理: 読み取り 監査の管理: 読み取り	該当なし	読み取り
アーカイブされたスナップショットの表示	スナップショットの管理: 読み取り	該当なし	読み取り
アーカイブされたスナップショットからの監査の作成	スナップショットの管理: 読み取り 監査の管理: 読み取り	該当なし	読み取り
スナップショット結果の削除	スナップショットの管理: 読み取り/書き込み	該当なし	読み取り/書き込み
スナップショットのサーバーからのデタッチ	一般的なスナップショット管理の許可: はい スナップショットの管理: 読み取り/書き込み スナップショット仕様の管理: 読み取り	該当なし	読み取り
スナップショット結果の修復	スナップショットの管理: 読み取り スナップショット仕様の管理: 読み取り 監査/スナップショット結果の修復の許可: はい	該当なし	読み取り/書き込み
スナップショット結果の修復: アプリケーション構成	スナップショットの管理: 読み取り 監査/スナップショット結果の修復の許可: はい スナップショット仕様の管理: 読み取り	サーバーファイルシステムの書き込み	読み取り/書き込み

表57　ユーザーのアクションに必要な監査と修復のアクセス権（続き）

ユーザーのアクション	アクションのアクセス権	OGFSアクセス権	サーバーのアクセス権(カスタマー、ファシリティ、デバイスグループ)
スナップショット結果の修復: COM+	スナップショットの管理: 読み取り 監査/スナップショット結果の修復の許可: はい スナップショット仕様の管理: 読み取り	COM+データベースの読み取り	読み取り/書き込み
スナップショット結果の修復: カスタムスクリプト	スナップショットの管理: 読み取り 監査/スナップショット結果の修復の許可: はい スナップショット仕様の管理: 読み取り	サーバーファイルシステムの書き込み	読み取り/書き込み
スナップショット結果の修復: ファイルシステム	スナップショットの管理: 読み取り 監査/スナップショット結果の修復の許可: はい スナップショット仕様の管理: 読み取り	サーバーファイルシステムの書き込み	読み取り/書き込み
スナップショット結果の修復: メタベース	スナップショットの管理: 読み取り 監査/スナップショット結果の修復の許可: はい スナップショット仕様の管理: 読み取り	IISメタベースの読み取り	読み取り/書き込み
スナップショット結果の修復: レジストリ	スナップショットの管理: 読み取り 監査/スナップショット結果の修復の許可: はい スナップショット仕様の管理: 読み取り	サーバーレジストリの読み取り	読み取り/書き込み
監査			
監査の表示	監査の管理: 読み取り	該当なし	読み取り
監査の実行	監査結果の管理: 読み取り	該当なし	読み取り
監査のスケジュール	監査結果の管理: 読み取り/書き込み	該当なし	読み取り
監査の作成	監査の管理: 読み取り/書き込み	該当なし	読み取り
アプリケーション構成ルールの作成	監査の管理: 読み取り/書き込み	サーバーファイルシステムの書き込み	読み取り/書き込み
COM+ルールの作成	監査の管理: 読み取り/書き込み	COM+データベースの読み取り	読み取り/書き込み

表57 ユーザーのアクションに必要な監査と修復のアクセス権（続き）

ユーザーのアクション	アクションのアクセス権	OGFSアクセス権	サーバーのアクセス権(カスタマー、ファシリティ、デバイスグループ)
カスタムスクリプトルールの作成	監査の管理: 読み取り/書き込み カスタムスクリプトポリシールールの作成の許可: はい	サーバーファイルシステムの書き込み	読み取り/書き込み
検出されたソフトウェアルールの作成	監査の管理: 読み取り/書き込み サーバーモジュールの管理:読み取り	該当なし	読み取り/書き込み
ファイルルールの作成	監査の管理: 読み取り/書き込み	サーバーファイルシステムの書き込み	読み取り/書き込み
ハードウェアルールの作成	監査の管理: 読み取り/書き込み	該当なし	読み取り/書き込み
IISメタベースルールの作成	監査の管理: 読み取り/書き込み	IISメタベースの読み取り	読み取り/書き込み
Internet Information Serverルールの作成	監査の管理: 読み取り/書き込み	該当なし	読み取り/書き込み
登録済みソフトウェアルールの作成	監査の管理: 読み取り/書き込み サーバーモジュールの管理:読み取り	該当なし	読み取り/書き込み
ソフトウェアルールの作成	監査の管理: 読み取り/書き込み	該当なし	読み取り/書き込み
ストレージルールの作成	監査の管理: 読み取り/書き込み サーバーモジュールの管理:読み取り	該当なし	読み取り/書き込み
Weblogicルールの作成	監査の管理: 読み取り/書き込み サーバーモジュールの管理:読み取り	該当なし	読み取り/書き込み
.Net Framework構成ルールの作成	監査の管理: 読み取り/書き込み サーバーモジュールの管理:読み取り	該当なし	読み取り/書き込み
Windowsレジストリルールの作成	監査の管理: 読み取り/書き込み	サーバーレジストリの読み取り	読み取り/書き込み
Windowsサービスルールの作成	監査の管理: 読み取り/書き込み	該当なし	読み取り/書き込み
Windows/UNIXユーザーおよびグループルールの作成	監査の管理: 読み取り/書き込み サーバーモジュールの管理:読み取り	該当なし	読み取り/書き込み
監査ポリシーの監査へのリンク	監査の管理: 読み取り/書き込み 監査ポリシーの管理: 読み取り SAクライアントのライブラリフォルダー : 読み取り	該当なし	読み取り/書き込み
監査ポリシーの監査へのインポート	監査の管理: 読み取り/書き込み 監査ポリシーの管理: 読み取り ライブラリフォルダー : 読み取り	該当なし	読み取り/書き込み

表57　ユーザーのアクションに必要な監査と修復のアクセス権（続き）

ユーザーのアクション	アクションのアクセス権	OGFSアクセス権	サーバーのアクセス権(カスタマー、ファシリティ、デバイスグループ)
監査ポリシーに名前を付けて保存	監査の管理: 読み取り/書き込み 監査ポリシーの管理: 読み取り/書き込み ライブラリフォルダー : 読み取り/書き込み	該当なし	読み取り/書き込み
監査結果			
監査結果の表示	監査結果の管理: 読み取り 監査の管理: 読み取り	該当なし	読み取り
アーカイブされた監査結果の表示	監査の管理: 読み取り	該当なし	読み取り
監査結果の削除	監査結果の管理: 読み取り/書き込み	該当なし	読み取り/書き込み
監査結果の修復	監査の管理: 読み取り 監査結果の管理: 読み取り/書き込み 監査/スナップショット結果の修復の許可: はい	該当なし	読み取り/書き込み
監査結果の修復: アプリケーション構成	監査の管理: 読み取り 監査結果の管理: 読み取り/書き込み 監査/スナップショット結果の修復の許可: はい	サーバーファイルシステムの書き込み	読み取り/書き込み
監査結果の修復: COM+	監査の管理: 読み取り 監査結果の管理: 読み取り/書き込み 監査/スナップショット結果の修復の許可: はい	COM+データベースの読み取り	読み取り/書き込み
監査結果の修復: カスタムスクリプトルールの作成	監査の管理: 読み取り 監査結果の管理: 読み取り/書き込み 監査/スナップショット結果の修復の許可: はい	サーバーファイルシステムの書き込み	読み取り/書き込み

表57　ユーザーのアクションに必要な監査と修復のアクセス権（続き）

ユーザーのアクション	アクションのアクセス権	OGFSアクセス権	サーバーのアクセス権(カスタマー、ファシリティ、デバイスグループ)
監査結果の修復: 検出されたソフトウェア	監査の管理: 読み取り 監査結果の管理: 読み取り/書き込み 監査/スナップショット結果の修復の許可: はい サーバーモジュールの管理: 読み取り サーバーモジュールの実行の許可: はい	該当なし	読み取り/書き込み
監査結果の修復: ファイル	監査の管理: 読み取り 監査結果の管理: 読み取り/書き込み 監査/スナップショット結果の修復の許可: はい	サーバーファイルシステムの書き込み	読み取り/書き込み
監査結果の修復: IISメタベース	監査の管理: 読み取り 監査結果の管理: 読み取り/書き込み 監査/スナップショット結果の修復の許可: はい	IISメタベースの読み取り	読み取り/書き込み
監査結果の修復: Internet Information Serverの修復	監査の管理: 読み取り 監査結果の管理: 読み取り/書き込み 監査/スナップショット結果の修復の許可: はい	IISメタベースの読み取り	読み取り/書き込み
監査結果の修復: 検出されたソフトウェアの修復	監査の管理: 読み取り 監査結果の管理: 読み取り/書き込み 監査/スナップショット結果の修復の許可: はい サーバーモジュールの管理: 読み取り サーバーモジュールの実行の許可: はい	該当なし	読み取り/書き込み
監査結果の修復: ソフトウェアの修復	監査の管理: 読み取り 監査結果の管理: 読み取り/書き込み	該当なし	読み取り/書き込み

表57　ユーザーのアクションに必要な監査と修復のアクセス権（続き）

ユーザーのアクション	アクションのアクセス権	OGFSアクセス権	サーバーのアクセス権(カスタマー、ファシリティ、デバイスグループ)
監査結果の修復: ストレージの修復	監査の管理: 読み取り 監査結果の管理: 読み取り/書き込み 監査/スナップショット結果の修復の許可: はい サーバーモジュールの管理: 読み取り サーバーモジュールの実行の許可: はい	該当なし	読み取り/書き込み
監査結果の修復: Weblogicの修復	監査の管理: 読み取り 監査結果の管理: 読み取り/書き込み 監査/スナップショット結果の修復の許可: はい サーバーモジュールの管理: 読み取り サーバーモジュールの実行の許可: はい	該当なし	読み取り/書き込み
監査結果の修復: Windows .NET Framework構成の修復	監査の管理: 読み取り 監査結果の管理: 読み取り/書き込み 監査/スナップショット結果の修復の許可: はい サーバーモジュールの管理: 読み取り サーバーモジュールの実行の許可: はい	該当なし	読み取り/書き込み

表57　ユーザーのアクションに必要な監査と修復のアクセス権（続き）

ユーザーのアクション	アクションのアクセス権	OGFSアクセス権	サーバーのアクセス権(カスタマー、ファシリティ、デバイスグループ)
監査結果の修復: Windowsレジストリ	監査の管理: 読み取り 監査結果の管理: 読み取り/書き込み 監査/スナップショット結果の修復の許可: はい	サーバーレジストリの読み取り	読み取り/書き込み
監査結果の修復: Windowsサービス	監査の管理: 読み取り 監査結果の管理: 読み取り/書き込み 監査/スナップショット結果の修復の許可: はい	該当なし	読み取り/書き込み
監査結果の修復: Windows/UNIXユーザーおよびグループの修復	監査の管理: 読み取り 監査結果の管理: 読み取り/書き込み 監査/スナップショット結果の修復の許可: はい サーバーモジュールの管理: 読み取り サーバーモジュールの実行の許可: はい	該当なし	読み取り/書き込み

表58に、監査と修復のアクセス権ごとにユーザーが実行できるアクションを示します。表58は表57と同じデータを、アクションのアクセス権ごとに整理したものです。表58には示されていませんが、監査と修復のすべてのアクションに対して、管理対象サーバーおよびグループのアクセス権が必要です。

セキュリティ管理者は、表58を参照して特定のアクションの監査と修復のアクセス権が割り当てられたユーザーが実行できるアクションを確認できます。

表58　監査と修復のアクセス権で使用できるユーザーアクション

アクションのアクセス権	ユーザーのアクション	OGFSアクセス権	サーバーのアクセス権(カスタマー、ファシリティ、デバイスグループ)
カスタムスクリプトルールポリシーの作成の許可: いいえ および 監査の管理: 読み取り	カスタムスクリプトルールの表示: 監査	該当なし	読み取り
カスタムスクリプトルールポリシーの作成の許可: はい および 監査の管理: 読み取り/書き込み	カスタムスクリプトルールの作成: 監査	サーバーファイルシステムの書き込み	読み取り/書き込み
カスタムスクリプトルールポリシーの作成の許可: いいえ および スナップショットの管理: 読み取り/書き込み	カスタムスクリプトルールの表示: スナップショット	該当なし	読み取り
カスタムスクリプトルールポリシーの作成の許可: はい および スナップショットの管理: 読み取り/書き込み	カスタムスクリプトルールの作成: スナップショット	サーバーファイルシステムの書き込み	読み取り/書き込み
一般的なスナップショット管理の許可: はい	スナップショットのサーバーからのデタッチ	該当なし	読み取り
スナップショット仕様の管理: 読み取り および 監査/スナップショット結果の修復の許可: いいえ および 監査の管理またはスナップショットの管理: 読み取り	監査またはスナップショットの表示、修復なし	該当なし	読み取り

表58 監査と修復のアクセス権で使用できるユーザーアクション（続き）

アクションのアクセス権	ユーザーのアクション	OGFSアクセス権	サーバーのアクセス権(カスタマー、ファシリティ、デバイスグループ)
スナップショット仕様の管理: 読み取り および 監査/スナップショット結果の修復の許可: はい および 監査の管理またはスナップショットの管理: 読み取り/書き込み	監査/スナップショット結果の修復	該当なし	読み取り/書き込み
スナップショット仕様の管理: 読み取り および 監査/スナップショット結果の修復の許可: はい および 監査の管理またはスナップショット結果の管理: 読み取り/書き込み	アプリケーション構成ルールの修復	サーバーファイルシステムの書き込み	読み取り/書き込み
	COM+ルールの修復	COM+データベースの読み取り	読み取り/書き込み
	カスタムスクリプトルールの修復レジストリルール	サーバーファイルシステムの書き込み	読み取り/書き込み
	ファイルシステムルールの修復	IISメタベースの読み取り	読み取り/書き込み
	IISメタベースルールの修復	サーバーレジストリの読み取り	読み取り/書き込み
	Windowsレジストリルールの修復	サーバーファイルシステムの書き込み	読み取り/書き込み
監査の管理: 読み取り	監査の表示、スケジュール、実行	該当なし	読み取り
監査の管理: 読み取り/書き込み	監査の作成、編集、削除	該当なし	読み取り/書き込み
	監査を監査ポリシーとして保存	該当なし	読み取り/書き込み
	監査ポリシーの監査へのリンク	該当なし	読み取り/書き込み
	アプリケーション構成ルールの作成	サーバーファイルシステムの書き込み	読み取り/書き込み
	COM+ルールの作成	COM+データベースの読み取り	読み取り/書き込み
	ファイルシステムルールの作成	サーバーファイルシステムの書き込み	読み取り/書き込み
	IISメタベースルールの作成	IISメタベースの読み取り	読み取り/書き込み
	Windowsレジストリルールの作成	サーバーレジストリの読み取り	読み取り/書き込み

表58 監査と修復のアクセス権で使用できるユーザーアクション（続き）

アクションのアクセス権	ユーザーのアクション	OGFSアクセス権	サーバーのアクセス権 (カスタマー、ファシリティ、デバイスグループ)
監査の管理: 読み取り/書き込み および カスタムスクリプトポリシールールの作成の許可: はい	カスタムスクリプトルールの作成	サーバーファイルシステムの書き込み	読み取り/書き込み
監査の管理: 読み取り/書き込み および サーバーモジュールの管理: 読み取り	次の監査ルールの作成: • 検出されたソフトウェア • 登録済みソフトウェア • ストレージ • Weblogic • Windows .NET Framework 構成 • Windowsユーザーおよびグループ	該当なし	読み取り/書き込み
監査結果の管理: 読み取り	監査結果の表示	該当なし	読み取り
監査結果の管理: 読み取り/書き込み	監査結果の削除	該当なし	読み取り/書き込み
スナップショット仕様の管理: 読み取り/書き込み	スナップショット仕様の表示、スケジュール、実行	該当なし	読み取り

表58 監査と修復のアクセス権で使用できるユーザーアクション（続き）

アクションのアクセス権	ユーザーのアクション	OGFSアクセス権	サーバーのアクセス権 (カスタマー、ファシリティ、デバイスグループ)
スナップショット仕様の管理: 読み取り/書き込み	スナップショット仕様の作成、編集、削除	該当なし	
	スナップショット仕様を監査ポリシーとして保存 (このアクションでは、ポリシーが存在するライブラリフォルダーに対する読み取り/書き込みが必要。)	該当なし	
	監査ポリシーの監査へのリンク	該当なし	読み取り/書き込み
	アプリケーション構成ルールの作成	サーバーファイルシステムの書き込み	読み取り/書き込み
	COM+ルールの作成	COM+データベースの読み取り	読み取り/書き込み
	検出されたソフトウェアの作成		
	ファイルシステムルールの作成	サーバーファイルシステムの書き込み	読み取り/書き込み
	IISメタベースルールの作成	IISメタベースの読み取り	読み取り/書き込み
	Windowsレジストリルールの作成	サーバーレジストリの読み取り	読み取り/書き込み
スナップショット仕様の管理: 読み取り/書き込み および サーバーモジュールの管理: 読み取り	次のスナップショットルールの作成: • 検出されたソフトウェア • 登録済みソフトウェア • ストレージ • Weblogic • Windows .NET Framework 構成 • Windowsユーザーおよびグループ	該当なし	読み取り/書き込み
スナップショット仕様の管理: 読み取り/書き込み および カスタムスクリプトポリシールールの作成	スナップショット仕様のカスタムルールの作成	サーバーファイルシステムの書き込み	読み取り/書き込み
スナップショットの管理: 読み取り	スナップショットの内容の表示	該当なし	読み取り

表58　監査と修復のアクセス権で使用できるユーザーアクション（続き）

アクションのアクセス権	ユーザーのアクション	OGFSアクセス権	サーバーのアクセス権 (カスタマー、ファシリティ、デバイスグループ)
スナップショットの管理: 読み取り/書き込み	スナップショット結果の削除	該当なし	読み取り/書き込み
監査ポリシーの管理: 読み取り	監査およびスナップショット仕様の内容の表示	該当なし	読み取り
監査ポリシーの管理: 読み取り/書き込み	監査ポリシーの作成、編集	該当なし	読み取り/書き込み
	アプリケーション構成ルールの作成	サーバーファイルシステムの書き込み	読み取り/書き込み
	COM+ルールの作成	COM+データベースの読み取り	読み取り/書き込み
	ファイルシステムルールの作成	サーバーファイルシステムの書き込み	読み取り/書き込み
	IISメタベースルールの作成	IISメタベースの読み取り	読み取り/書き込み
	Windowsレジストリルールの作成	サーバーレジストリの読み取り	読み取り/書き込み
監査ポリシーの管理: 読み取り/書き込み サーバーモジュールの管理: 読み取り	次のスナップショットルールの作成: • 検出されたソフトウェア • 登録済みソフトウェア • ストレージ • Weblogic • Windows .NET Framework 構成 • Windowsユーザーおよびグループ	該当なし	読み取り/書き込み
監査ポリシーの管理: 読み取り/書き込み および カスタムスクリプトポリシールールの作成の許可	カスタムスクリプトルールの作成	サーバーファイルシステムの書き込み	読み取り/書き込み

コンプライアンスビューのアクセス権

この項では、SAクライアントの特定のアクションをユーザーが実行するのに必要なコンプライアンスビューのアクセス権について説明します。セキュリティ管理者は、ユーザーが特定のアクションを実行するのに必要なアクセス権をこの表で確認することができます。

表59　ユーザーのアクションに必要なコンプライアンスビューのアクセス権

ユーザーのアクション	アクションのアクセス権	サーバーのアクセス権(カスタマー、ファシリティ、デバイスグループ)
監査		
詳細の表示	監査結果の管理: 読み取り	読み取り
監査の実行	監査の管理: 読み取り 監査結果の管理: 読み取り/書き込み	読み取り/書き込み
修復	監査/スナップショット結果の修復の許可: はい 特定の監査ルールに対する修復に必要な他のアクセス権については、監査と修復のユーザーアクションのアクセス権 (295ページ) (表58) を参照してください。	読み取り/書き込み
ソフトウェア		
修復	ソフトウェアポリシーの管理: 読み取り サーバーの修復の許可: はい	読み取り/書き込み
デバイスのスキャン	ソフトウェアポリシーの管理: 読み取り または ソフトウェアポリシーのアタッチ/デタッチの許可: はい または ソフトウェアのインストール/アンインストールの許可: はい または サーバーの修復の許可: はい	読み取り/書き込み
パッチ		
修復	パッチポリシーの管理: 読み取り パッチのインストール: はい	読み取り/書き込み

表59　ユーザーのアクションに必要なコンプライアンスビューのアクセス権（続き）

ユーザーのアクション	アクションのアクセス権	サーバーのアクセス権（カスタマー、ファシリティ、デバイスグループ）
デバイスのスキャン	パッチの管理: 読み取り または パッチポリシーの管理: 読み取り または パッチのインストールの許可: はい または パッチのアンインストールの許可: はい または ソフトウェアのインストール/アンインストールの許可 または サーバーの修復の許可	読み取り/書き込み
アプリケーション構成		
詳細の表示	アプリケーション構成の管理: 読み取り	読み取り
デバイスのスキャン	構成コンプライアンススキャンの許可: はい	読み取り
特定のアプリケーション構成の修復	アプリケーション構成の修復に必要なアクセス権については、アプリケーション構成管理のアクセス権 (276ページ) を参照してください。	読み取り/書き込み

ジョブアクセス権

SA クライアントでジョブを管理するには、表 60 に示す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のアクセス権を選択すると、すべてのジョブを表示のアクセス権が自動的に選択されます。

SAクライアントで任意のジョブを表示するには、ジョブを実行するためのアクセス権が必要です。たとえば、アプリケーション構成の管理などのアクションのアクセス権を [読み取り] に設定しても、そのアクションの [書き込み] アクセス権がない場合、SAクライアントでアプリケーション構成のプッシュのジョブを表示することはできません。

表60　　ジョブ管理のアクセス権

ユーザーのアクション	アクションのアクセス権
承認の統合の有効化	承認の統合の管理
承認が必要なジョブのタイプの設定	承認の統合の管理
ブロックされた (承認待ち) ジョブを管理するための JobService APIメソッドの呼び出し (このアクションは、SAクライアントにログオンしたエンドユーザーではなく、バックエンドのカスタマイズされたソフトウェアによって実行される。)	任意のジョブの編集またはキャンセル すべてのジョブを表示
ジョブの終了 (キャンセル)	任意のジョブの編集またはキャンセル すべてのジョブを表示
スケジュールの削除	任意のジョブの編集またはキャンセル すべてのジョブを表示

スクリプト実行のアクセス権

表61は、SAクライアントの特定のアクションをユーザーが実行するのに必要なスクリプト実行のアクセス権を示しています。セキュリティ管理者は、ユーザーが特定のアクションを実行するのに必要なアクセス権をこの表で確認することができます。

カスタマーをフォルダーに割り当てた場合、フォルダー内のソフトウェアポリシーを関連付けることが可能なオブジェクトにカスタマーの制約が適用されることがあります。これらの制約の影響を受けるタスク一覧については、フォルダー、カスタマーの制約、ソフトウェアポリシー (24ページ) を参照してください。

表61　　ユーザーのアクションに必要なスクリプト実行のアクセス権

ユーザーのアクション	アクションのアクセス権	サーバーのアクセス権 (カスタマー、ファシリティ、デバイスグループ)	フォルダーのアクセス権
非スーパーユーザーサーバースクリプトの作成	サーバースクリプトの管理: 読み取り/書き込み	該当なし	書き込み
スーパーユーザーサーバースクリプトの作成	サーバースクリプトの管理: 読み取り/書き込み スーパーユーザーサーバースクリプトのコントロールの許可: はい	該当なし	書き込み
OGFSスクリプトの作成	OGFSスクリプトの管理: 読み取り/書き込み	該当なし	書き込み

表61　ユーザーのアクションに必要なスクリプト実行のアクセス権（続き）

ユーザーのアクション	アクションのアクセス権	サーバーのアクセス権 (カスタマー、ファシリティ、デバイスグループ)	フォルダーのアクセス権
非スーパーユーザーサーバースクリプトを開く (スクリプトの内容を除くすべてのスクリプトのプロパティを表示)	サーバースクリプトの管理: 読み取り	該当なし	実行
非スーパーユーザーサーバースクリプトを開く (スクリプトの内容を含むすべてのスクリプトのプロパティを表示)	サーバースクリプトの管理: 読み取り	該当なし	読み取り
スーパーユーザーサーバースクリプトを開く (スクリプトの内容を除くすべてのスクリプトのプロパティを表示)	サーバースクリプトの管理: 読み取り スーパーユーザーサーバースクリプトのコントロールの許可: はい	該当なし	実行
スーパーユーザーサーバースクリプトを開く (スクリプトの内容を含むすべてのスクリプトのプロパティを表示)	サーバースクリプトの管理: 読み取り スーパーユーザーサーバースクリプトのコントロールの許可: はい	該当なし	読み取り
OGFSスクリプトを開く (スクリプトの内容を除くすべてのスクリプトのプロパティを表示)	OGFSスクリプトの管理: 読み取り	該当なし	実行
OGFSスクリプトを開く (スクリプトの内容を含むすべてのスクリプトのプロパティを表示)	OGFSスクリプトの管理: 読み取り	該当なし	読み取り
非スーパーユーザーサーバースクリプトのプロパティの編集	サーバースクリプトの管理: 読み取り/書き込み 注:「スーパーユーザーサーバースクリプトのコントロールの許可: はい」の権限は、スクリプトのプロパティ「スーパーユーザーとして実行可能」を編集する場合に必要。	該当なし	書き込み
スーパーユーザーサーバースクリプトの編集	サーバースクリプトの管理: 読み取り/書き込み スーパーユーザーサーバースクリプトのコントロールの許可: はい	該当なし	書き込み
OGFSスクリプトのプロパティの編集	OGFSスクリプトの管理: 読み取り/書き込み	該当なし	書き込み
フォルダーでのサーバースクリプトの特定	サーバースクリプトの管理: 読み取り	該当なし	読み取り

表61　ユーザーのアクションに必要なスクリプト実行のアクセス権（続き）

ユーザーのアクション	アクションのアクセス権	サーバーのアクセス権(カスタマー、ファシリティ、デバイスグループ)	フォルダーのアクセス権
フォルダーでのOGFSスクリプトの特定	OGFSスクリプトの管理: 読み取り	該当なし	読み取り
サーバースクリプトのエクスポート	サーバースクリプトの管理: 読み取り	該当なし	読み取り
OGFSスクリプトのエクスポート	OGFSスクリプトの管理: 読み取り	該当なし	読み取り
サーバースクリプトの名前の変更	サーバースクリプトの管理: 読み取り/書き込み	該当なし	書き込み
スーパーユーザーサーバースクリプトの名前の変更	サーバースクリプトの管理: 読み取り/書き込み スーパーユーザーサーバースクリプトのコントロールの許可: はい	該当なし	書き込み
OGFSスクリプトの名前の変更	OGFSスクリプトの管理: 読み取り/書き込み	該当なし	書き込み
サーバースクリプトの削除	サーバースクリプトの管理: 読み取り/書き込み	該当なし	書き込み
スーパーユーザーサーバースクリプトの削除	サーバースクリプトの管理: 読み取り/書き込み スーパーユーザーサーバースクリプトのコントロールの許可: はい	該当なし	書き込み
OGFSスクリプトの削除	OGFSスクリプトの管理: 読み取り/書き込み	該当なし	書き込み
スーパーユーザーとしてサーバースクリプトを実行	管理対象サーバーおよびグループ: はい	読み取り/書き込み	実行
スーパーユーザーとしてサーバースクリプトを実行(別のスクリプトからスクリプトの内容をコピー)	サーバースクリプトの管理: 読み取り アドホックスクリプトの実行: はい アドホックおよびソース表示可能サーバースクリプトをスーパーユーザーとして実行: はい 管理対象サーバーおよびグループ: はい	読み取り/書き込み	読み取り
指定されたユーザーとしてサーバースクリプトを実行	管理対象サーバーおよびグループ: はい	読み取り/書き込み	実行
指定されたユーザーとしてサーバースクリプトを実行(別のスクリプトからスクリプトの内容をコピー)	サーバースクリプトの管理: 読み取り アドホックスクリプトの実行: はい 管理対象サーバーおよびグループ: はい	読み取り/書き込み	読み取り

表61　ユーザーのアクションに必要なスクリプト実行のアクセス権（続き）

ユーザーのアクション	アクションのアクセス権	サーバーのアクセス権(カスタマー、ファシリティ、デバイスグループ)	フォルダーのアクセス権
アドホックスクリプトの実行	アドホックスクリプトの実行: はい 管理対象サーバーおよびグループ: はい	読み取り/書き込み	該当なし
アドホックスクリプトのスーパーユーザーとしての実行	アドホックスクリプトの実行: はい アドホックおよびソース表示可能サーバースクリプトをスーパーユーザーとして実行: はい 管理対象サーバーおよびグループ: はい	読み取り/書き込み	該当なし
OGFSスクリプトの実行	該当なし	該当なし	実行

表62に、スクリプト実行のアクセス権ごとにユーザーが実行できるアクションを示します。表62は表61と同じデータを、アクションのアクセス権ごとに整理したものです。セキュリティ管理者は、表62を参照して特定のアクションのアクセス権が割り当てられたユーザーが実行できるアクションを確認できます。

表62　スクリプト実行のアクセス権で使用できるユーザーアクション

アクションのアクセス権	ユーザーのアクション	サーバーのアクセス権(カスタマー、ファシリティ、デバイスグループ)	フォルダーのアクセス権
サーバースクリプトの管理: 読み取り/書き込み	非スーパーユーザーサーバースクリプトの作成	該当なし	書き込み
	非スーパーユーザーサーバースクリプトのプロパティの編集	該当なし	書き込み
	非スーパーユーザーサーバースクリプトの削除	該当なし	書き込み
	非スーパーユーザーサーバースクリプトの名前の変更	該当なし	書き込み
サーバースクリプトの管理: 読み取り	非スーパーユーザーサーバースクリプトを開く(スクリプトの内容を含むすべてのスクリプトのプロパティを表示) スーパーユーザーサーバースクリプトを開く(スクリプトの内容を含むすべてのスクリプトのプロパティを表示)	該当なし	読み取り
	フォルダーでのサーバースクリプトの特定	該当なし	読み取り

表62　スクリプト実行のアクセス権で使用できるユーザーアクション（続き）

アクションのアクセス権	ユーザーのアクション	サーバーのアクセス権(カスタマー、ファシリティ、デバイスグループ)	フォルダーのアクセス権
	サーバースクリプトのエクスポート	該当なし	読み取り
サーバースクリプトの管理: 読み取り	非スーパーユーザーサーバースクリプトを開く(スクリプトの内容を除くすべてのスクリプトのプロパティを表示) スーパーユーザーサーバースクリプトを開く(スクリプトの内容を除くすべてのスクリプトのプロパティを表示)		実行
サーバースクリプトの管理: 読み取り/書き込み および スーパーユーザーサーバースクリプトのコントロールの許可: はい	スーパーユーザーサーバースクリプトの作成	該当なし	書き込み
	スーパーユーザーサーバースクリプトのプロパティの編集 非スーパーユーザーサーバースクリプトのプロパティの編集	該当なし	書き込み
	スーパーユーザーサーバースクリプトの名前の変更 非スーパーユーザーサーバースクリプトの名前の変更	該当なし	書き込み
	スーパーユーザーサーバースクリプトの削除 非スーパーユーザーサーバースクリプトの削除	該当なし	書き込み
OGFSの管理: 読み取り/書き込み	OGFSスクリプトの作成	該当なし	書き込み
	OGFSスクリプトのプロパティの編集	該当なし	書き込み
	OGFSスクリプトの削除	該当なし	書き込み
	OGFSスクリプトの名前の変更	該当なし	書き込み
OGFSスクリプトの管理: 読み取り	OGFSスクリプトを開く(スクリプトの内容を含むすべてのOGFSスクリプトのプロパティを表示)	該当なし	読み取り
	フォルダーでのOGFSの特定	該当なし	読み取り

表62　スクリプト実行のアクセス権で使用できるユーザーアクション（続き）

アクションのアクセス権	ユーザーのアクション	サーバーのアクセス権(カスタマー、ファシリティ、デバイスグループ)	フォルダーのアクセス権
	OGFSスクリプトのエクスポート	該当なし	読み取り
OGFSスクリプトの管理: 読み取り	OGFSスクリプトを開く(スクリプトの内容を除くすべてのOGFSスクリプトのプロパティを表示)	該当なし	実行
アドホックスクリプトの実行	アドホックスクリプトの実行	読み取り/書き込み	該当なし
アドホックおよびソース表示可能サーバースクリプトをスーパーユーザーとして実行	アドホックスクリプトをスーパーユーザーとして実行	読み取り/書き込み	該当なし
該当なし	非スーパーユーザーサーバースクリプトの実行	読み取り/書き込み	実行
該当なし	プライベートスクリプトの実行	読み取り/書き込み	実行(ホームフォルダー上)
該当なし	OGFSスクリプトの実行	該当なし	実行

次の表に、ソフトウェアポリシーを使用してスクリプトを実行するのに必要なスクリプト実行のアクセス権を示します。

表63　ソフトウェア管理に必要なスクリプト実行のアクセス権

ユーザーのアクション	アクションのアクセス権	サーバーのアクセス権(カスタマー、ファシリティ、デバイスグループ)	フォルダーのアクセス権
サーバースクリプトのソフトウェアポリシーへの追加	サーバースクリプトの管理: 読み取り	該当なし	読み取り
サーバースクリプトの[修復]ウィンドウの[オプション]ステップへの追加	該当なし	該当なし	実行
サーバースクリプトの[修復]ウィンドウの[オプション]ステップへの追加(スクリプトの内容のコピー)	サーバースクリプトの管理: 読み取り アドホックスクリプトの実行: はい	該当なし	読み取り

表63　ソフトウェア管理に必要なスクリプト実行のアクセス権（続き）

ユーザーのアクション	アクションのアクセス権	サーバーのアクセス権 (カスタマー、ファシリティ、デバイスグループ)	フォルダーのアクセス権
スーパーユーザーサーバースクリプトの [修復] ウィンドウの [オプション] ステップへの追加	サーバースクリプトの管理: 読み取り アドホックスクリプトの実行: はい アドホックおよびソース表示可能サーバースクリプトをスーパーユーザーとして実行: はい	該当なし	読み取り
アドホックスクリプトの [修復] ウィンドウの [オプション] ステップへの追加	アドホックスクリプトの実行: はい	該当なし	該当なし
スーパーユーザーアドホックスクリプトの [修復] ウィンドウの [オプション] ステップへの指定	アドホックスクリプトの実行: はい アドホックおよびソース表示可能サーバースクリプトをスーパーユーザーとして実行: はい	該当なし	該当なし
サーバースクリプトの [ソフトウェアのインストール] ウィンドウの [オプション] ステップへの追加	該当なし	該当なし	実行
サーバースクリプトの [ソフトウェアのインストール] ウィンドウの [オプション] ステップへの追加 (スクリプトの内容のコピー)	サーバースクリプトの管理: 読み取り アドホックスクリプトの実行: はい	該当なし	読み取り
スーパーユーザーサーバースクリプトの [ソフトウェアのインストール] ウィンドウの [オプション] ステップへの追加	サーバースクリプトの管理: 読み取り アドホックスクリプトの実行: はい アドホックおよびソース表示可能サーバースクリプトをスーパーユーザーとして実行: はい	該当なし	読み取り
アドホックスクリプトの [ソフトウェアのインストール] ウィンドウの [オプション] ステップへの追加	アドホックスクリプトの実行: はい	該当なし	該当なし
スーパーユーザーアドホックスクリプトの [ソフトウェアのインストール] ウィンドウの [オプション] ステップへの指定	アドホックスクリプトの実行: はい アドホックおよびソース表示可能サーバースクリプトをスーパーユーザーとして実行: はい	該当なし	該当なし

フローのアクセス権 - HP Operations Orchestration

SAでのフローの管理またはフローの実行には、次のアクセス権が必要です。

表64　フローに関連するアクセス権

ユーザーのアクション	アクセス権
SA-00統合の構成	フロー統合の管理
SAユーザーとしてSAクライアントでフローを実行	フローの実行

Service Automation Visualizerのアクセス権

表65は、SAクライアントの特定のアクションを実行するのに必要なService Automation Visualizer (SAV) アクセス権を示しています。セキュリティ管理者は、ユーザーが特定のアクションを実行するのに必要なアクセス権をこの表で確認することができます。

表65の「ユーザーアクション」欄のエントリは、ほとんどがSAクライアントのメニュー項目に対応しています。アクションのアクセス権の他に、分析操作の影響を受ける管理対象サーバーでサーバーの読み取りアクセス権 (リモートターミナルまたはリモートデスクトップクライアントを開くためのアクセス権、デバイスエクスプローラーを開くためのアクセス権、Service Automation VisualizerでGlobal Shellセッションを開くためのアクセス権など) が必要です。

サーバーをスキャンするのに必要なSAVのアクセス権は、物理サーバーでも仮想サーバーでも同じです。

詳細については、『SAユーザーガイド: Service Automation Visualizer』を参照してください。

表65　ユーザーのアクションに必要なSAVのアクセス権

ユーザーのアクション	アクションのアクセス権	ソースサーバーのアクセス権 (カスタマー、ファシリティ)	フォルダーのアクセス権
SAVのみの操作			
Service Automation Visualizerの起動	分析の許可: はい	読み取り	該当なし
スキャンの生成またはスナップショットの更新— 通常または仮想サーバー	分析の許可: はい	読み取り	該当なし
スナップショットの作成またはスケジュール済みスナップショットの編集	分析の許可: はい ビジネスアプリケーションの管理: 読み取り/書き込み	読み取り	該当なし
SAV内の仮想サーバーの開始、停止、一時停止、再開 (VMの一時停止はVMwareのみ—Solaris ローカルゾーンの一時停止は不可)	仮想サーバーの管理: はい	読み取り	該当なし
SAクライアントの操作			
スクリプトの実行 (非スーパーユーザーとして)	アドホックスクリプトの実行: はい	読み取り/書き込み	該当なし

表65　ユーザーのアクションに必要なSAVのアクセス権（続き）

ユーザーのアクション	アクションのアクセス権	ソースサーバーのアクセス権(カスタマー、ファシリティ)	フォルダーのアクセス権
スクリプトの実行(スーパーユーザーとして)	アドホックおよびソース表示可能サーバースクリプトをスーパーユーザーとして実行: はい	読み取り/書き込み	該当なし
OGFSスクリプトの実行	OGFSスクリプトの管理: はい	読み取り/書き込み	該当なし
ストレージ操作 (SE対応コア)			
SANアレイまたはNASファイラーデータの表示 (関係を含む)	ストレージシステムの表示: はい	読み取り	該当なし
SANスイッチデータの表示 (関係を含む)	ストレージシステムの表示: はい	読み取り	該当なし
SAクライアントのフォルダー操作			
フォルダーからビジネスアプリケーションを開く	該当なし	該当なし	フォルダー内のオブジェクトの読み取り
ビジネスアプリケーションを作成してフォルダーに保存	ビジネスアプリケーションの管理: はい	該当なし	フォルダー内のオブジェクトの書き込み
フォルダー内でのビジネスアプリケーションの名前の変更	該当なし	なし	フォルダー内のオブジェクトの書き込み
フォルダーからビジネスアプリケーションを削除	該当なし	該当なし	フォルダー内のオブジェクトの書き込み
フォルダーからのビジネスアプリケーションの切り取り、コピー、または貼り付け	該当なし	該当なし	フォルダー内のオブジェクトの書き込み

ビジネスアプリケーションをライブラリ内のユーザーの専用のホームディレクトリ (たとえば、/home/username) に保存するには、このユーザーのプライベートユーザーグループでビジネスアプリケーションの管理のアクセス権を [はい] に設定する必要があります。詳細については、『SA 管理ガイド』の「ユーザーグループの設定」を参照してください。

SAVおよびSAでのストレージの表示のアクセス権

ユーザーがストレージデバイス (SAN ファブリックやアレイなど) を表示するアクセス権を持たないグループに属している場合でも、ユーザーはSAV スナップショット内の一部のタイプのストレージ情報を表示できる可能性があります。

具体的には、ユーザーが「ビジネスアプリケーションの管理: 読み取り/書き込み」のアクセス権を持つ1つ以上のグループに属している場合、そのグループにデバイスやオブジェクトを表示するための個別のアクセス権が付与されていなくても、ユーザーは、SAVスナップショット内のファブリック (スイッチ)、ストレージアレイ、ネットワークデバイス、VM情報などのSAVスナップショット内のデバイスやオブジェクトを表示することができます。

ユーザーが「ビジネスアプリケーションの管理: 読み取り / 書き込み」のアクセス権を持たない 1 つ以上のグループに属している場合は、そのグループに個別のアクセス権が付与されている場合に限り、SAV スナップショット内のSANファブリック (スイッチ)、ストレージアレイ、ネットワークデバイス、VM情報を表示することができます。

たとえば、ユーザーが「ビジネスアプリケーションの管理: 読み取り/書き込み」のアクセス権を持つ1つまたは複数のグループに属していて、「ファブリックの管理」のアクセス権が「なし」である場合、ユーザーはSAVスナップショット内のファブリック (およびSANスイッチ) を表示することができます。

Storage Visibility and Automationのアクセス権

Storage Visibility and Automation でアクションを実行するには、特定のアクセス権が必要です。これらのアクセス権については、『Storage Visibility and Automationインストールおよび管理ガイド』を参照してください。

SA Webクライアントに必要なアクセス権

次の表に、SA Webクライアントで実行するタスクに応じて必要なアクション/機能のアクセス権を示します。

表66　SA Webクライアントのタスクに必要なアクセス権

タスク	アクション/機能のアクセス権
OSのプロビジョニング	
OSの準備	ウィザード: OSの準備
OSノードの編集	オペレーティングシステム
サーバープール内のサーバーの表示	サーバープール
サーバー管理	
サーバーのプロパティの編集	管理対象サーバーおよびグループ
サーバーのネットワークプロパティの編集	管理対象サーバーおよびグループ
サーバーのカスタム属性の編集	管理対象サーバーおよびグループ
サーバーの非アクティブ化 (エージェント)	非アクティブ化
サーバーの削除	管理対象サーバーおよびグループ
カスタマーの再割り当て	管理対象サーバーおよびグループ
サーバーの表示 (読み取り専用アクセス)	管理対象サーバーおよびグループ
サーバーの通信テストの実行	管理対象サーバーおよびグループ
サーバーのロック	管理対象サーバーおよびグループ
サーバーリストを更新するジョブのスケジュールの設定	更新ジョブの実行の許可
レポート	
レポートの作成または表示	データセンターインテリジェンスレポート
環境の管理	
カスタマーの作成または編集	カスタマー

表66　SA Webクライアントのタスクに必要なアクセス権（続き）

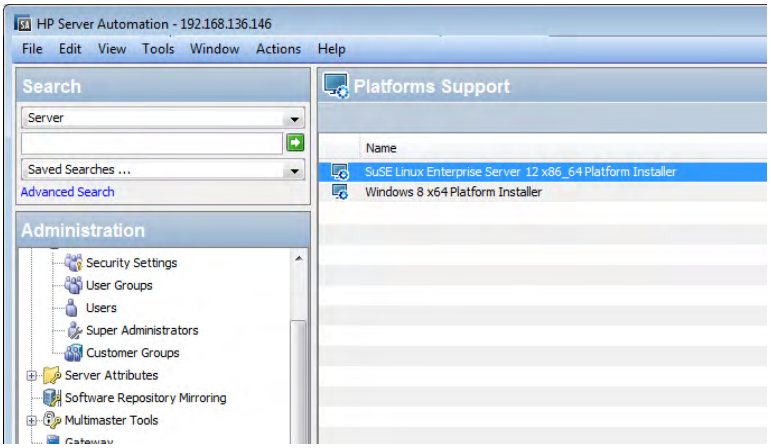
タスク	アクション/機能のアクセス権
ファシリティの作成または編集	ファシリティ
システム構成	
サーバーとグループの管理	(管理者グループのみ)
サーバー属性の定義	サーバー属性
システム診断ツールの実行	システム診断
SAシステム構成の管理	SAの構成
SAマルチマスターツールの実行	マルチマスター
ゲートウェイ管理	ゲートウェイの管理
その他のタスク	
カスタム拡張の実行	ウィザード: カスタム拡張
フローの管理	フロー統合の管理
フローの実行	フローの実行

付録B 管理対象プラットフォームのサポート

管理対象プラットフォームのサポートによって、プラットフォームをSAに簡単に追加できるようになります。また、SAコア全体を自動的に変更できるようになるので、コアコンポーネントの再起動が必要になる機会が減ります。

新しい管理対象プラットフォームごとに、プラットフォームインストーラーと呼ばれるプログラムAPXがHP Live Network (HPLN) から利用可能になります。プラットフォームインストーラーは、新しいプラットフォームのサポートを追加するため、SAコアに対して必要な操作を実行します。図40に、新しいプラットフォームパッケージの内容を示します。

図40　管理対象プラットフォームのサポート: 新しいプラットフォームパッケージ



この章では、新しいプラットフォームパッケージをインポートして、新しいプラットフォームをSAコアにデプロイする方法について説明します。

➤ 製品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。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://h20230.www2.hp.com/selfsolve/manuals

新しいプラットフォームパッケージのインポート

プラットフォームパッケージをHPLNから個別にダウンロードして、SAコアにインポートできます。

1. 次のURLを入力すると、HPLNポータルに移動します。

   https://hpln.hp.com/group/managed-platform-content-server-automation
2. インストーラーのリストが表示されます。いずれかのインストーラーをSAコアのファイルシステムにダウンロードします。
3. インストーラーはAPXであるので、次のコマンドを使用して、SAコアにインポートします。

   /opt/opsware/bin/apxtool import <プラットフォームインストーラーのファイル名>
4. プラットフォームインストーラーを実行します。

注: インストーラーを SA コアにインポートしても、新しいプラットフォームのサポートが自動的にデプロイされるわけではありません。プラットフォームインストーラーは、最新情報と変更内容を実装するため、SA ユーザーが実行する必要があります。次の項では、新しくインストールしたプラットフォームのサポートをデプロイする方法について説明します。

新しいプラットフォームのサポートのデプロイ

この項では、新しくインポートしたプラットフォームをデプロイするために、実行する必要があるアクションについて説明します。

必要な管理対象プラットフォームのアクセス権

SA クライアントプラットフォームのサポート機能とそのプラットフォームインストーラーのリストを確認するとともに、いずれかのインストーラーを実行するには、SAユーザーグループは管理対象プラットフォームのアクセス権を保持している必要があります。

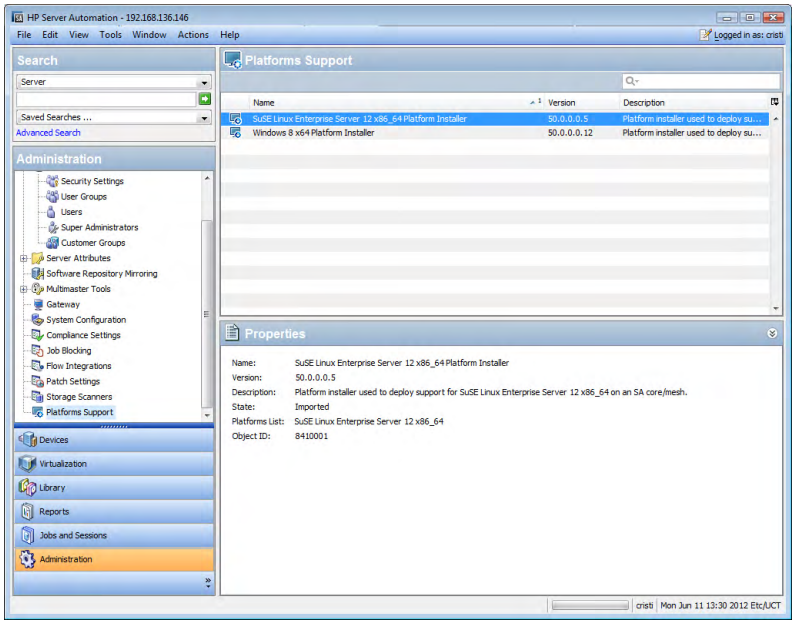
このアクセス権をSAユーザーグループに割り当てるには、次の手順を実行します。

1. SAクライアントでユーザーグループを開いて、[アクションのアクセス権] ノードを開きます。
2. 右側のパネルで、[システム管理] カテゴリの下にある [管理対象プラットフォーム] を検索します。
3. [管理対象プラットフォーム] を [**はい**] に設定して、保存します。

プラットフォームインストーラーの使用

管理対象プラットフォームのアクセス権を設定したら、SA クライアントの [管理] タブの下に [プラットフォームサポート] エントリが表示されます (図42を参照)。

図41　　[プラットフォームサポート] ウィンドウ



このウィンドウには、SAコアにインポートされたプラットフォームインストーラーが表示されます。各インストーラーは次の属性を持ちます。

- 名前
- 説明
- バージョン
- デプロイするプラットフォームのリスト

- 状態

  プラットフォームインストーラーのステータス:

  — 未実行－インストーラーがSAコアにインポートされましたが、まだ未実行であるため、OSのサポートは利用不可です。

  — 失敗－インストーラーがSAコアにインポートされて実行されましたが、実行に失敗しました。この場合、新しいOSのサポートは部分的にデプロイされた状態であり、インストーラーが正常に実行されるまで、新しいOSは使用できません。

  — インストール済み－インストーラーがSAコアにインポートされて、正常に実行されました。新しいOSのサポートも正常にデプロイされており、新しいプラットフォームがSAで使用できます。

  — 不明－インストーラーのステータスを特定できませんでした。

プラットフォームインストーラーの実行

インストーラーの実行には、次の方法があります。

- インストーラーを右クリックして、**[実行...]** をクリックする
- インストーラーを選択して、メインメニューから **[アクション]** > **[実行...]** を選択する

  [プラットフォームインストーラーの実行] ジョブウィンドウが表示されます。このウィンドウでは、特定の時刻に1回だけ実行するようにタスクをスケジュールして、電子メール通知をセットアップできます。

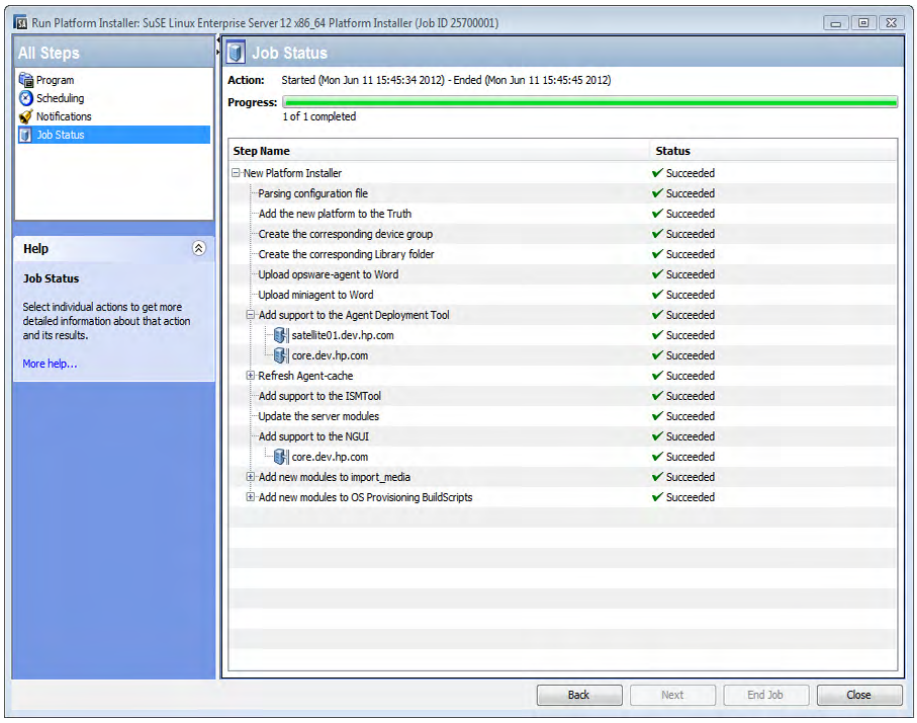
  ジョブが開始されると、メッシュで実行する必要がある変更内容がインストーラーで判別されて、一連のステップが生成されます (図42を参照)。

  いくつかのステップは、実行できる回数が1回に制限されています (新しいプラットフォームをTruthに追加するステップなど)。また、メッシュ /コア構成に含まれる複数のマシンで実行する必要があるステップもあります (エージェントデプロイメントツールへのサポートの追加など)。

  - 各ステップを選択すると、取得された **stdout** ファイルと **stderr** ファイルを確認できるようになります。ステップを複数のマシンで実行する必要がある場合、ジョブの結果ウィンドウでは、対応するノードに、マシンごとに1つの子が表示されます。

- この子ノードを選択すると、特定のマシンでステップを実行した結果の**stdout**ファイルと**stderr**ファイルを確認できるようになります。

図42　[プラットフォームインストーラーの実行] ジョブステータスウィンドウ



プラットフォームインストーラーの削除

インストーラーの削除には、次の方法があります。

- インストーラーを右クリックして、[**削除**] をクリックする
- インストーラーを選択して、メインメニューから [**アクション**] > [**削除**] を選択する

  インストーラーを削除しても、SA コアにデプロイされた OS のサポートが削除されるわけではありません。したがって、プラットフォームインストーラーをインポートして実行した後に、SAで新しいOSのサポートを無効にすることなく、プラットフォームインストーラーを安全に削除できます。

索引

さ

し

す

せ

そ

て

ろ