HP Server Automation

Ultimate Edition

ソフトウェアバージョン: 10.10

ユーザーガイド: 監査とコンプライアンス

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 監査と修復の概要

HP Server Automation (SA) では、監査と修復により、IT環境内でチェック対象のオブジェクトと、チェックを行う場所とタイミングを指定できます。

- 監査ポリシーでは、チェック対象 (ファイル、ディレクトリ、構成値など) を定義します。
- 監査では、チェック対象となる場所 (サーバー、複数のサーバーなど) を定義します。
- 監査スケジュールでは、チェックを行うタイミング (特定の日時、反復実行など) を定義します。

これらの機能を使用することによって、管理対象サーバー環境でコンプライアンスを確保し、サーバーのコンプライアンス状態を維持する方法を理解できます。SAでは、ファシリティ内のサーバーを標準ポリシーに準拠した状態にする方法として、サーバー構成ポリシーを使用します。非コンプライアンス状態 (想定通りに構成されていない状態) として検出されたサーバーは、修復によって、組織で規定されている標準に準拠した状態にすることが可能です。

SAクライアントでは、動作中のサーバーまたはサーバースナップショット、ユーザー指定の値、事前定義された監査ポリシーをベースに、サーバー構成値の監査を実行します。また、サーバー構成スナップショットを使ってシステムの現在の状態を取得し、他のサーバーと比較することも可能です。

監査ポリシーでは、会社全体または業界共通のコンプライアンス標準を定義し、監査やスナップショット仕様などの監査ポリシーで使用できます。監査やスナップショット仕様で定義した監査ポリシーを参照すれば、組織内の最新のコンプライアンス定義に適応できているかどうかを確認できます。

ベストプラクティス: BSA Essentials サブスクリプションサービスへのコンテンツサブスクリプションがある場合は、データセンターのニーズに応じて業界コンプライアンス標準を最新の状態に更新することができます。たとえば、サブスクリプションサービスは、Center for Internet Security (CIS) やPayment Card Industry (PCI) などの定期的に更新されるセキュリティのベストプラクティスへのアクセスを提供します。また、Microsoft Patch Supplement for Server Automationなどの、その他の無償の非サブスクリプションコンテンツにもアクセスできるようになります。BSA Essentialsサブスクリプションサービスを使用して、Federal Information Security Management Act (FISMA) や Sarbanes-Oxley (SoX) 法などの最新の法規制コンプライアンスポリシーや、日次の脆弱性アラートにアクセスできます。さらに、HP Live Network (HPLN) ポータル上のコンテンツ開発者コミュニティに参加でき、カスタム作成された監査ポリシーとルールの共有とアクセスが可能になります。BSA Essentialsサブスクリプションサービスのサブスクリプションの詳細については、HPの販売担当者にお問い合わせください。

監査と修復でサポートされているオペレーティングシステムの詳細については、『SA Support and Compatibility Matrix』を参照してください。

用語

以下のリストは、HP Server Automation 監査と修復で使用される主な用語と概念を定義します。

- **アーカイブ済み監査結果/スナップショット**: 監査結果とスナップショットをアーカイブすると、これらを監査結果またはスナップショットのリストから移動して、履歴情報として利用可能にすることができます。
- **監査**: 個別のチェックを含む一連のルールで、管理対象サーバーの構成オブジェクト (サーバーのファイルシステムのディレクトリ構造、サーバーのWindowsレジストリ、アプリケーション構成など) の必要な状態を表します。監査には、ソース (サーバー、スナップショット、またはスナップショット仕様)、ターゲット (サーバーまたはスナップショット)、ルールの例外、およびスケジュールが含まれます。

  監査のルールは、監査ポリシーにリンクすることも可能です。つまり、監査ポリシーのルールが監査のルールの代わりに使用されます。監査を実行し、サーバー構成オブジェクトの値をゴールデンサーバー、サーバースナップショット、またはユーザー定義値とベースライン比較して、各値の差異を判定できます。監査により、サーバーまたはユーザー入力値の間に差異が報告された場合、ソフトウェアとサーバーオブジェクトをインストールして差異を修復し、サーバーが監査ルールに準拠するようにできます。
- **監査ジョブ**: 監査を実行すると発生するプロセス。監査ジョブは、即時に1回だけ実行するか、ジョブをスケジュールして定期的に実行することができます。監査ジョブが完了すると、監査結果が生成され、差異が報告されます。
- **監査ルールタイプ**: 監査には以下のルールタイプを含めることができます。
  - **比較**: サーバーの構成またはサーバーのスナップショットの構成を他の管理対象サーバーまたはスナップショットと比較するルール。
  - **値ベース (ユーザー定義)**: 1つまたは複数のユーザー定義値のセットを比較するルール。このタイプの監査には監査ポリシーにリンクされた監査も含まれます。
  - **非存在:** オブジェクトの非存在のチェック、すなわちターゲットサーバー上にオブジェクトが存在しないことを確認します。ターゲットサーバー上にオブジェクトが存在する場合、ルールはコンプライアンス違反になります。実行時に、ソースサーバーが存在しても、このサーバーに対する照会は行われません。また、ワイルドカードルールオブジェクトを選択すると、ターゲットサーバーにのみ適用されます。
- **監査ポリシー**: サーバーに対する目的の構成を定義するルールの集合。監査では、以下の方法でポリシーを使用できます。
  - **リンク**: リンクされたポリシーにより、監査とポリシーの間の接続が常に保持されます。つまり、監査のルールと監査ポリシーのルールは正確に一致しており、ポリシーが更新された場合は、最新の変更内容がそのポリシーがリンクされている監査にも反映されます。監査ポリシーが監査またはスナップショット仕様にリンクされている場合、ルールは監査またはスナップショット仕様内で読み取り専用として表示されます。監査ポリシー内のルールは引き続き編集可能です。
  - **インポート (置換、非リンク)**: ポリシーを監査にインポートすると、監査と監査ポリシー間の接続は保持されなくなります。ポリシーに影響を与えることなく監査を変更することができます。これに対して、ポリシーに対して行われた変更や更新は監査には反映されません。
  - **インポート (マージ)**: 監査ポリシーをインポートし、監査にマージすると、監査ポリシーのルールが既存の監査のルールに追加されます。監査と監査ポリシー間の接続は保持されません。マージ処理中にルールの競合が検出された場合、監査ポリシーのルールは監査ポリシーから新しくインポートされたルールで置き換えられます。
- **監査結果**: 監査の実行結果。この情報は、ターゲットサーバーまたは複数サーバーの構成オブジェクトの値が監査で定義された値とどの程度一致または不一致であるかを示します。

- **例外**: 監査の実行時にルール例外が選択されたサーバーに対してチェックされないようにするために、例外または無効として設定されたサーバーおよび特定のルール。このサーバーは監査コンプライアンスの判定から除外されます。
- **コンプライアンス**: 監査、スナップショット仕様、または監査ポリシーで定義された一連のルールによって作成されたチェックまたはテストにサーバーの構成がどの程度適合しているかを表します。監査と修復のコンプライアンスは、ターゲットサーバーで想定される値を指定する監査またはスナップショットのルールによって定義されます。ターゲットサーバー上の値が監査のルールで指定された値と異なる場合、サーバーは非コンプライアンス状態と見なされます。
- **ポリシー設定担当者**: サーバー構成のコンプライアンス標準 (サーバーの構成方法) および組織内の監査ポリシーの定義を担当するユーザー。
- **ルール**: 目的の値およびオプションの修復値を含む、特定のサーバー構成オブジェクトに対するチェック。

  ルールには、次の2つのタイプがあります。

  — サーバーベースのルール: ソースサーバーから直接派生

  — ユーザー定義ルール: ユーザーが作成

  BSA Essentialsサブスクリプションサービスへのサブスクリプションがある場合、さまざまな業界のコンプライアンス標準を定義する、事前定義されたルールにアクセス可能です。たとえば、Microsoft Windowsの最新のPatch Supplementや、現行の法規制コンプライアンスポリシー (FISMA、Sarbanes-Oxley (SoX) 法)、EP開発者コミュニティでユーザーが作成したルール、脆弱性コンテンツの日次更新などにアクセスできます。
- **サーバーオブジェクト**: 監査またはスナップショット仕様のルールの適用対象となるサーバーからのオブジェクト。パスワードの最小文字数などの値や、ファイルやディレクトリなどのオブジェクト、レジストリエントリ、Windowsサービスのハードウェア構成などを使用できます。
- **スナップショット**: 特定の日付と特定の時間に情報が取得された管理対象サーバーの構成状態の表現。スナップショットはこれまでに実行されたスナップショット仕様ジョブの結果です。
- **スナップショット仕様**: 監査のソース。これは一般的に「再帰的監査」と呼ばれます。スナップショット仕様から監査を実行すると、監査では仕様で定義されたすべての情報が使用され、定義したフィルターがすべて適用されます。
- **スナップショット仕様ジョブ**: スナップショット仕様を実行すると発生するプロセス。スナップショットジョブは、1 回だけ実行するか、ジョブをスケジュールして定期的に実行することができます。スナップショット仕様ジョブが完了すると、スナップショットが生成されます。
- **ターゲット**: 監査の実行またはスナップショットの取得の対象となるサーバー。監査のターゲットには、サーバー、複数のサーバー、サーバーグループ、スナップショットを使用できます。スナップショットのターゲットには他のサーバーも使用できます。

サーバー構成

以下のベストプラクティスと例は、SAでファシリティ内のサーバー構成を管理する方法を示します。

- セキュリティ標準の強制
- ゴールデンサーバーの取得と複製

セキュリティ標準の強制

一般的に、IT組織には強制的に適用すべきセキュリティポリシーがあります。これらのポリシーは、サーバーが正しく構成されているか、セキュリティ攻撃から保護されているかを検証します。ポリシー設定担当者は監査ポリシーを作成して、これらのセキュリティ標準を強制することができます。事前定義された監査ポリシーは複数の監査やスナップショット仕様にリンクすることができます。動作中のサーバーを管理する管理者は、適正な監査ポリシーを参照してサーバーが正しく監査されているかどうか確認できます。

例: 会社でSolaris 10サーバーを使用しており、このサーバーをCommon Vulnerabilities and Exposures (CVE) で指定される一般的に知られている最新のセキュリティ脆弱性に関して、最新の状態に保たなければならないとします。会社からは、サーバーがSolaris 10に対する既知の脅威に対して脆弱性を持たないようにすることを要求されています。たとえば、Sun Solaris 10およびOpenSolaris snv_61からsnv_106でPPD File Manager (ppdmgr) 内の不特定の脆弱性をチェックするCVE-2009-0168 (CVSS 4.9) などです。BSA Essentialsサブスクリプションサービスをサブスクライブすると、オンライン上の一連のコンプライアンスチェックにアクセス可能になります。これらのチェックを使用して、Solaris 10サーバーを監査し、セキュリティ脆弱性に対するリスクがないかどうか確認できます。組織内でのコンプライアンス標準の定義を担当するシステム管理者は、CVE-2009-0168コンプライアンスチェックを含む監査ポリシーを作成できます。

ベストプラクティス: Solarisサーバーの管理を担当するシステム管理者は、サーバーの監査を作成し、その監査ルールを監査ポリシーにリンクすることができます。監査が監査ポリシーにリンクされている場合、ポリシーへの変更はすべて監査に即時に反映されます。そのため、サーバー上で監査を実行する担当者は、監査ルールが常に最新のものであることを認識しています。たとえば、Solaris 10サーバーに対してCVEが新しく更新された場合、ポリシー設定担当者がポリシーを更新すると、そのポリシーにリンクされているすべての監査に最新のコンプライアンスチェックが適用されます。監査には常に最新の脆弱性チェックが含まれているとわかっているため、ポリシー設定担当者は、監査を定期的に実行するようスケジュールして、管理対象のSolaris 10サーバーをすべてチェックすることができます。監査結果により、新しいCVEセキュリティチェックが含まれていないターゲットサーバーが見つかった場合は、これらのサーバーを修復して問題を解決できます。

ゴールデンサーバーの取得と複製

ファシリティ内の特定の目的に対するサーバー構成の理想的な状態を表すように、サーバーが構成されている場合があります。たとえば、Webトラフィックを処理するサーバーの集まりを設定する場合、Webサーバーのグループに対して、理想的な構成を表す1つのサーバー (ゴールデンサーバー構成) を設定することができます。このゴールデンサーバーを構成した後、その構成をSAで管理されたサーバーのグループ全体に複製することができます。

例: 固有に構成されたApache Webサーバーを持つRed Hat Linuxサーバーがあり、この構成を他の複数の管理対象サーバーに正確に複製するとします。監査と修復を使用して、ゴールデンサーバーをソース構成として使用する監査を作成することができます。監査では、これらの構成を選択して、アプリケーションポリシーや特定のアプリケーション構成ルールなどの、他のサーバーの監査に使用できます。監査のターゲットとしてこれらのサーバーを選択し、ゴールデンサーバーと同様に構成します。監査の実行後、ゴールデンサーバーと一致しないターゲットサーバーの構成を修復します。監査をスケジュールして、定期的に実行できます。サーバーが非コンプライアンス状態になった場合は、ゴールデンサーバーとの偏差を修復します。

第2章 監査、監査ポリシー、監査結果

監査

監査は、管理対象サーバーまたは管理対象サーバーのグループが組織のコンプライアンス標準に一致するかどうかを判定するためのルールまたは構成値のセットを定義します。監査ルールはアドホックに構成することもできますが、あらかじめ定義された監査ポリシーを参照するのがより効果的な方法です。監査ポリシーは、HP Server Automationでの管理対象サーバーの必要な構成を具体的に定義するものです。

監査では、次のことができます。

- サーバーの構成を、監査ポリシーに定義されたルールと比較します。
- 構成値が監査ルールに指定された基準を満たすことを確認します。
- 特定の値が存在するかまたは存在しないことを確認します。

監査ルールによっては、スクリプトを実行することで、より詳細な構成情報を取得できる場合もあります。

ベストプラクティス: 監査ポリシーを定義することで、次のことが可能です。

- IISメタベース値が存在するかどうかを確認します。特に、存在してはならない場合に使用します。
- 特定のLinuxサービスが常に実行されるように設定されていることを確認します。特に、セキュリティ上の理由で常に動作している必要がある重要なサービスに対して使用します。
- 特定のファイルシステムディレクトリが特定のサイズ制限を超えていないかどうかを判定します。
- ユーザーパスワードの最大長さの設定を超過していないことを確認します。

監査で調査する対象、サーバー上に存在すべき値、差異が見つかったときに修正のために置き換える値を定義できます。

構成が完了したら、監査を1回だけ実行するか、将来実行するためにスケジュールするか、定期的に実行するためにスケジュールすることができます。監査を実行した後、結果を見れば、対象のサーバーが監査ルールに設定された定義をどの程度満たすかを知ることができます。不一致が見つかった場合、サーバーを修復して、コンプライアンス状態に戻すことができます。

監査ポリシー

監査ポリシーは、業界標準と組織のコンプライアンス目標に基づいて、サーバー構成の必要な状態を定義する、再使用可能なルールの集合です。監査ポリシーは、監査、スナップショット仕様、および他の監査ポリシーにリンクすることができます。監査ポリシーを変更した場合、その監査ポリシーへの参照もすべて更新されます。

監査ポリシーの作成は、一般的にポリシー設定の担当者が行います。担当者は、特定の構成ドメインとオペレーティングシステムに関して会社のサーバーが満たすべきコンプライアンス標準を理解しています。サーバーの管理者は、あらかじめ定義された監査ポリシーを、自分が作成した監査仕様またはスナップショット仕様にリンクすることで、監査ポリシーを利用できます。監査ポリシーが変更された場合、それにリンクされた監査にも更新されたルールが含まれます。SAの管理対象サーバーを監査する管理者は、組織の最新のポリシー標準が自分の監査に反映されることを確信できます。

スナップショット

スナップショットは、管理対象サーバーの構成状態の表現であり、特定の日付と時刻に取得された情報に基づいています。スナップショットは、ファシリティ内の他のサーバーとの比較の基準となるゴールデンサーバーの構成を記録するのに便利です。スナップショットは監査のソースとして使用できます。スナップショットに記録された構成と一致しないサーバーがある場合、監査の実行後にそのサーバーを修復できます。

コンプライアンスと修復

SAクライアントのコンプライアンスビューでは、ファシリティ内のSA管理対象サーバー全体のコンプライアンスレベルを表示できます。コンプライアンスビューは、コンプライアンスダッシュボードとも呼ばれます。コンプライアンスダッシュボードでは、コンプライアンスの問題を発見して修復できます。

監査管理

監査は、サーバーの構成に何があるべきで、何があるべきでないかを定義するルールの集合です。監査には、ルール、ソース、ターゲットサーバー、および監査の実行のタイミングと頻度を定義するスケジュールが含まれます。

監査ルールでは、管理対象サーバー上のさまざまな構成またはオブジェクトやファイルの状態を定義し、チェックできます。たとえば、サーバーのファイルシステムの状態、レジストリ設定、インストールおよび登録されているソフトウェア (パッチやパッケージ)、イベント、ソフトウェア、アプリケーション構成、オペレーティングシステムの設定などが対象となります。

注: ターゲットサーバーの構成またはオブジェクトが監査ルールに定義された状態と異なっている場合、またはソースサーバーに存在するオブジェクトまたはルールがターゲットサーバーに存在しない場合、ルールは非コンプライアンス状態と見なされます。

たとえば、グループまたはユーザーをソースサーバーに追加し、ターゲットサーバーに追加しなかった場合は、監査または修復は成功しません。また、ソースサーバーのレジストリ設定を変更し、ターゲットサーバーでは変更しなかった場合も、エラーが発生します。

監査結果を表示する際に、ターゲットサーバーの構成が必要な構成と一致するように、オブジェクト構成を修復することができます。

サーバー構成値の監査は、1 台のサーバー、複数のサーバー、または別のサーバースナップショットに対して実行できます。監査は、ただちに実行するか、繰り返し実行するようにスケジュールでき、監査が完了したときに電子メール通知を送信することができます。また、実行中の監査ジョブはキャンセルできます。

監査の比較タイプ

一般的に、監査では、監査のソースに基づいて、次の比較タイプが使用できます。

- **比較**: 監査の作成時に指定されたソースサーバーまたはソーススナップショットの構成値に基づく監査が作成されます。ソースサーバーまたはサーバースナップショットは、ゴールデンサーバーとも呼ばれます。たとえば、ファイルディレクトリまたはファイル内容、レジストリ構造、IISメタベースエントリ、またはユーザーグループ設定を、管理対象サーバーの間で比較できます。スナップショットを監査のソースとして使用すると、スナップショットをファシリティ内の他のサーバーと比較できます。

比較監査では、次のタイプの比較を実行できます。

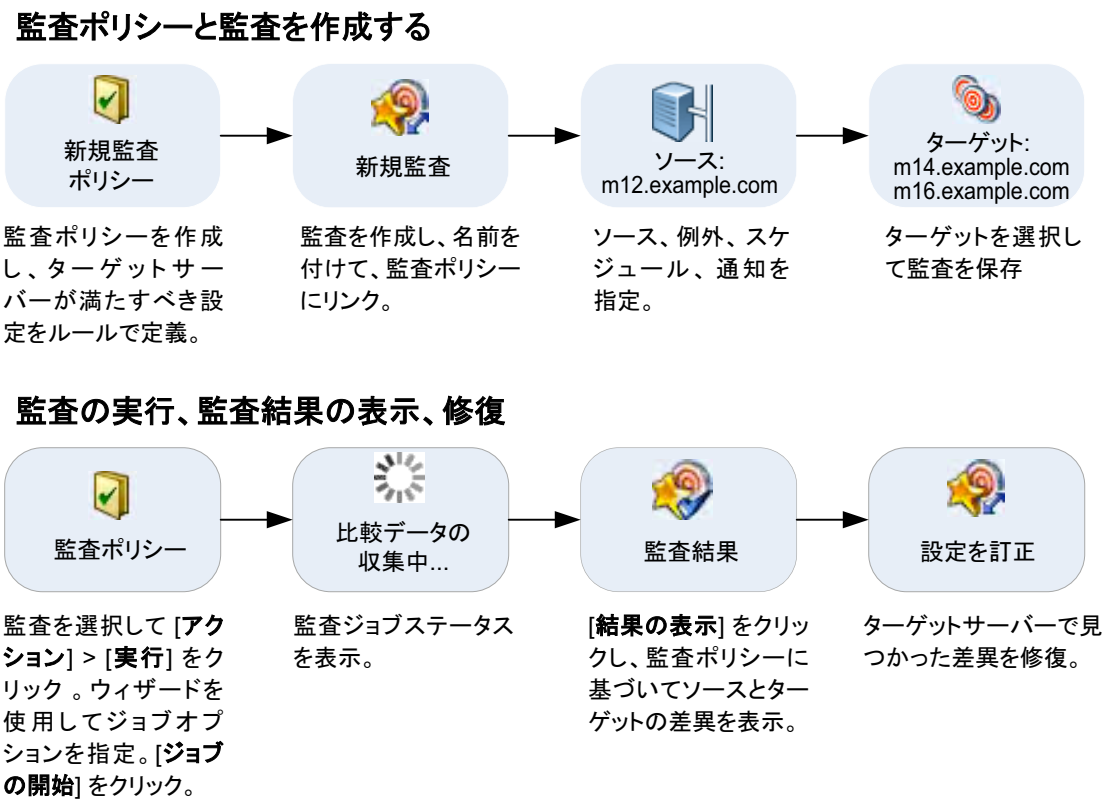
- **プロパティ**：選択したオブジェクトまたはオブジェクト構成のプロパティをチェックします。たとえば、ターゲットサーバーまたは複数のサーバー上のパッチのリリースバージョンをチェックして、ターゲットにインストールされている必要があるものと一致するかどうかを確認できます。このバージョン番号は、ソースサーバーまたはスナップショットに基づいて選択することも、独自の値を追加することもできます。
- **等価**: ターゲットサーバー構成が、監査のソースサーバーまたはスナップショットと一致することを確認します。たとえば、監査のターゲットが、ソースサーバーから選択したグループと同じユーザーグループを持つかどうかをチェックできます。
- **非存在**: オブジェクトの非存在のチェック、すなわちターゲットサーバー上にオブジェクトが存在しないことを確認します。ターゲットサーバー上にオブジェクトが存在する場合、ルールはコンプライアンス違反になります。たとえば、サーバーに特定のCOM+オブジェクトが含まれないことを確認できます。実行時に、ソースサーバーが存在しても、このサーバーに対する照会は行われません。また、ワイルドカードルールオブジェクトを選択すると、ターゲットサーバーにのみ適用されます。

- **値ベース (ユーザー定義)**: 各サーバーオブジェクト (ファイルシステム、Windowsサービス、IIS メタベース、ユーザーとグループなど) に対するユーザー定義のカスタム値に基づく監査。これらの値は、ソースサーバー、SA属性、またはカスタム属性から取得できます。このタイプの監査には、監査ポリシーに基づくものが含まれます。監査ポリシーでは、ポリシー設定担当者が、会社または業界のコンプライアンス標準に基づいて、各構成オブジェクトの値をあらかじめ定義します。

監査プロセス

図1に、監査プロセスの各ステップの説明を示します。

図1　　監査プロセス



監査の要素

監査は次の要素から構成されます。

- **プロパティ**：監査の名前と説明。
- **ソース**：監査のソースとしてはサーバーまたはスナップショットが使用でき、ソースを使用しないこともできます。ただし、ルールによってはソースが必須のものもあります。
  - 監査のソースとしてサーバーを選択すると、そのサーバーのサーバーオブジェクトを監査の基礎として選択できます。
  - スナップショットを監査のソースとして選択すると、スナップショットの構成値を使用できます。
  - スナップショット仕様をソースとして使用すると、サーバーを過去の同じサーバーと比較して監査できます。

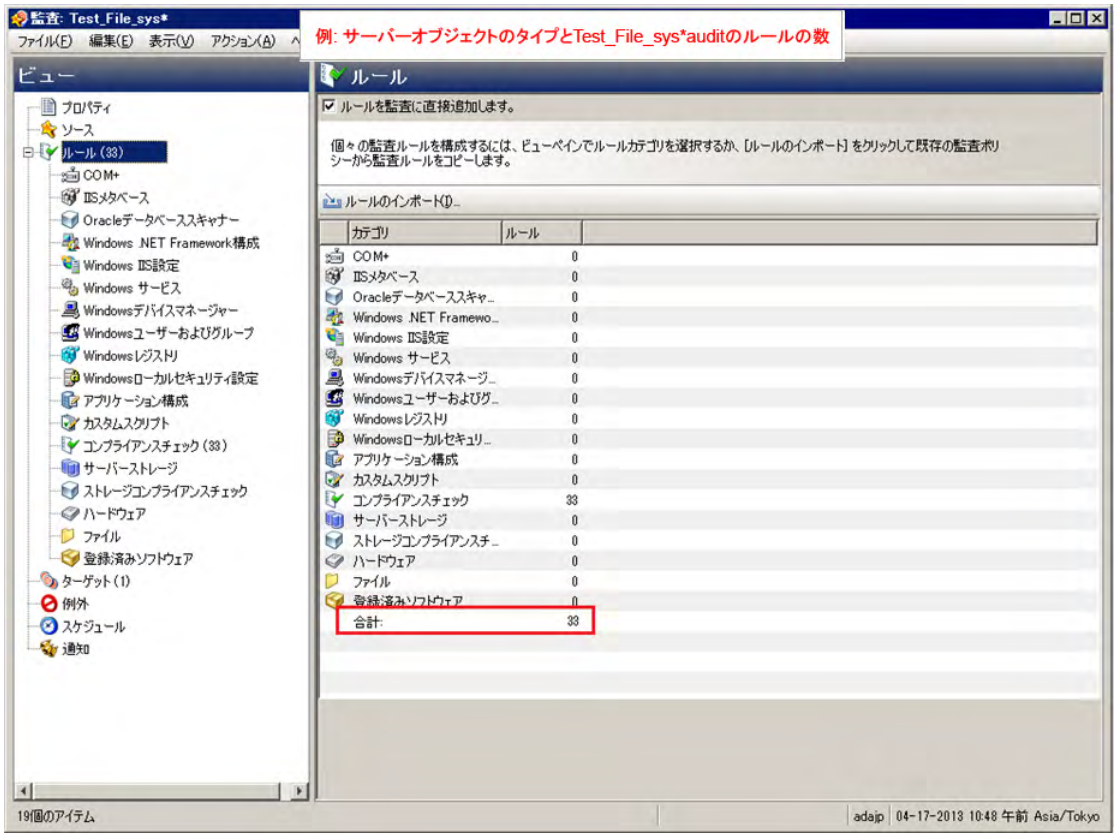
  たとえば、サーバーのスナップショットを取得して、そのスナップショット仕様を監査のソースに使用し、定期的スケジュールで監査を実行すれば、監査のたびにサーバーの元の状態と実際の構成とを比較できます。ソースなしを選択した場合、監査またはスナップショットに対して独自のカスタム値を定義する必要があります。
- **ルール**：特定のサーバーオブジェクトに対するチェックで、必要な値とオプションの修復値を備えています。たとえば、このサーバーに特定のWindowsサービスが含まれるかどうかを調べ、見つかった場合は、サービスがオフになっているかどうかを判定できます。サーバーオブジェクト (33ページ) を参照してください。
- **ターゲット**：監査でコンプライアンスをチェックするサーバー。監査またはスナップショットの対象として選択可能なサーバーとサーバーグループの数には制限はありません。

監査またはスナップショットのターゲットにVMware ESXiサーバーは指定できません。

- **例外**：監査の実行時にコンプライアンスをチェックされないサーバーと特定のルール。
- **スケジュール**：監査は1回だけ実行することも、定期的スケジュールで実行することもできます。定期的スケジュールで実行される監査は、コンプライアンスダッシュボードでは1つのコンプライアンス列に表示されます。
- **通知**：監査の実行が終了したときに電子メールを送信できます。通知は、監査ジョブの成功、失敗、または完了に基づいて行うことができます。

監査を構成するには、サーバー構成オブジェクトを選択し、これらのオブジェクトにルールを適用して、必要な構成状態を定義します。図 2 に、33 個のルールが定義された監査の例を示します。これらのルールは、ターゲットサーバーの構成が監査のルールに一致するかどうかの判定に使用されます。

図2　　監査のオブジェクトを示す監査ブラウザー



監査の作成

SAクライアントでは、いくつかの方法で監査を作成できます。

次の操作を実行できます。

- 管理対象サーバーを監査のソースとして選択し、1台のサーバーに対して監査を実行します。

  サーバーからの監査の作成 (20ページ) を参照してください。

- 管理対象サーバーのグループを監査のソースとして選択し、そのグループのすべてのサーバーに対して監査を実行します。

  サーバーのグループからの監査の作成 (20ページ) を参照してください。

- SAライブラリから新しい監査を作成します。

  SAライブラリからの監査の作成 (20ページ) を参照してください。

- スナップショットに取得したサーバー構成に基づいて監査を作成します。

  スナップショットからの監査の作成 (21ページ) を参照してください。

- 監査ポリシーに基づく監査を作成します。

  詳細については、監査ポリシーからの監査の作成 (21ページ) を参照してください。

サーバーからの監査の作成

管理対象サーバーから新しい監査を作成すると、選択したサーバーが監査のソースとして使用されます。別のサーバーまたはスナップショットを監査ソースとして選択することも、ソースを選択せずに独自のカスタムルールを定義することもできます。

管理対象サーバーを監査するには、サーバーが到達可能であり、サーバーへのアクセス権を持っている必要があります。

サーバーから監査を作成するには、次の手順を実行します。

1. ナビゲーションペインで、[**デバイス**] > [**サーバー**] > [**すべての管理対象サーバー**] を選択します。
2. サーバーを選択します。
3. [**アクション**] メニューで、[**作成**] > [**監査**] を選択して、[監査] ウィンドウを開きます。

   監査の構成 (29ページ) を参照してください。

サーバーのグループからの監査の作成

サーバーのグループから監査を作成すると、そのグループ内のすべてのアクセス可能なサーバーが評価されます。ただし、グループ内で評価の対象となるのは、ユーザーがアクセス権を持つサーバーだけです。

サーバーのグループを監査するには、次の手順を実行します。

1. ナビゲーションペインで、[**デバイス**] > [**デバイスグループ**] を選択します。
2. 内容ペインで、[パブリック] または [プライベート] を選択します。
3. 監査するサーバーグループを選択します。
4. 内容ペインで、サーバーグループを選択します。
5. [**アクション**] メニューで、[**作成**] > [**監査**] を選択して、[監査] ウィンドウを開きます。

   サーバーのグループを選択して監査を実行すると、サーバーのクループがターゲットとなります。監査ルールにソースが必要な場合は、ソースを指定する必要があります。監査の構成 (29ページ) を参照してください。

SAライブラリからの監査の作成

SAライブラリから監査を作成するには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**監査と修復**] を選択します。
2. ナビゲーションペインで [**監査**] を展開します。
3. オペレーティングシステムを選択します(WindowsまたはUnix)。
4. [**アクション**] メニューで、[**新規**] を選択して、[監査] ウィンドウを開きます。

   監査の構成 (29ページ) を参照してください。

スナップショットからの監査の作成

SAライブラリから任意のスナップショットを選択して、スナップショットに取得されたサーバー構成に基づく監査を作成できます。スナップショットは監査のソースとなります。ただし、スナップショットから新しい監査を作成した後で、別のスナップショットまたはサーバーをソースとして選択することもできます。

スナップショットから監査を作成するには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**監査と修復**] を選択します。
2. ナビゲーションペインで [**スナップショット仕様**] を展開します。
3. オペレーティングシステムを選択します(WindowsまたはUnix)。
4. [**アクション**] メニューで、[**新規**] を選択して、[スナップショット仕様] ウィンドウを開きます。

   監査の構成 (29ページ) を参照してください。

監査ポリシーからの監査の作成

監査ポリシーは、監査から使用するために設計されています。監査ポリシーから監査を作成すると、監査ポリシーが監査にリンクされます。その監査ポリシーが更新されると、すべての変更が監査に反映されます。

監査ポリシーから監査を作成するには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**監査と修復**] を選択します。
2. ナビゲーションペインで [**監査ポリシー**] を展開します。
3. オペレーティングシステムを選択します(WindowsまたはUnix)。
4. [**アクション**] メニューで、[**新規**] を選択して、[監査ポリシー] ウィンドウを開きます。

   監査の構成 (29ページ) を参照してください。

監査の実行

監査を実行すると、監査のターゲットサーバーまたはスナップショットに対して、選択した監査が実行されます。監査に定義されたルールに基づいて、ターゲットが評価されます。監査はSAクライアントの次の場所から実行できます。

- SAライブラリから (21ページ)
- すべての管理対象サーバーから (22ページ)
- 監査結果から (23ページ)

SAライブラリから

SAライブラリには、実行可能なすべての監査が、オペレーティングシステム別に分類されて含まれています(WindowsまたはUnix)。ライブラリ内の監査のリストは、名前、最終更新日など、任意の列によってソートできます。また、検索ツールを使用して、名前、ID、監査の作成者などを入力して監査リストを検索することもできます。

SAライブラリから監査を実行するには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**監査と修復**] を選択します。
2. [監査] を選択し、WindowsまたはUnixを選択します。
3. 実行する監査を選択し、右クリックして、[**監査の実行**] を選択します。

4 [監査の実行] ウィンドウの [サマリー] ページでは、ステップ1で監査の名前、監査のソースとなるサーバーまたはスナップショット、監査で定義されているルールの総数、監査のすべてのターゲット (サーバーおよびスナップショット) が表示されます。[**ルールの詳細の表示**] をクリックすると、ルールの定義が表示されます。

(オプション) 監査をただちに実行する場合は、プロセスの任意の時点で [**ジョブの開始**] をクリックします。

5 [**次へ**] をクリックします。

6 [スケジュール設定] ページで、監査をただちに実行するか、別の日時に実行するかを選択します。後で実行する場合は、[**次の時刻にタスクを実行**] を選択し、日付と時刻を指定します。

7 [**次へ**] をクリックします。

8 [通知] ウィンドウのデフォルト設定では、監査ジョブの成否に関係なく、監査の完了時にユーザーへ通知電子メールが送信されます。電子メールでの通知を追加するには、[**通知の追加**] をクリックして電子メールアドレスを入力します。

9 (オプション) 電子メールを、監査ジョブが成功した場合または失敗した場合のどちらの場合に送信するかを指定できます。

10 (オプション) [チケットID] フィールドでチケットトラッキングIDを指定します。[チケットID] フィールドが使用されるのは、SAプロフェッショナルサービスのSAが変更管理システムに統合されている場合のみです。それ以外の場合は空白にしてください。

11 [**次へ**] をクリックします。

12 [ジョブステータス] ページで [**ジョブの開始**] をクリックして、監査を実行します。実行完了後、[**結果の表示**] をクリックすると監査の結果が表示されます。

すべての管理対象サーバーから

サーバーが監査のターゲットとして使用されている場合、この場所から監査を実行できます。

すべての管理対象サーバーリストから監査を実行するには、次の手順を実行します。

1 ナビゲーションペインで、[**デバイス**] > [**サーバー**] > [**すべての管理対象サーバー**] を選択します。

2 サーバーを選択します。

3 [表示] ドロップダウンリストから、[監査と修復] を選択します。内容ペインの下に詳細ペインが表示されます。

4 詳細ペインの [表示] ドロップダウンリストで、[監査 - サーバーがターゲット] を選択します。

5 リストから監査を選択し、右クリックして、[**実行**] > [**監査**] を選択します。

6 [監査の実行] ウィンドウの [サマリー] ページでは、ステップ1で監査の名前、監査のソースとなるサーバーまたはスナップショット、監査で定義されているルールの総数、監査のすべてのターゲット (サーバーおよびスナップショット) が表示されます。[**ルールの詳細の表示**] をクリックすると、ルールの定義が表示されます。

(オプション) 監査をただちに実行する場合は、プロセスの任意の時点で [**ジョブの開始**] をクリックします。

7 [**次へ**] をクリックします。

8 [スケジュール設定] ページで、監査をただちに実行するか、別の日時に実行するかを選択します。後で実行する場合は、[**次の時刻にタスクを実行**] を選択し、日付と時刻を指定します。

9 [**次へ**] をクリックします。

10 [通知] ウィンドウのデフォルト設定では、監査ジョブの成否に関係なく、監査の完了時にユーザーへ通知電子メールが送信されます。電子メールでの通知を追加するには、[**通知の追加**] をクリックして電子メールアドレスを入力します。

11 (オプション) 電子メールを、監査ジョブが成功した場合または失敗した場合のどちらの場合に送信するかを指定できます。

12 (オプション) [チケットID] フィールドでチケットトラッキングIDを指定します。[チケットID] フィールドが使用されるのは、SAプロフェッショナルサービスのSAが変更管理システムに統合されている場合のみです。それ以外の場合は空白にしてください。

13 [**次へ**] をクリックします。

14 [ジョブステータス] ページで [**ジョブの開始**] をクリックして、監査を実行します。実行完了後、[**結果の表示**] をクリックすると監査の結果が表示されます。

監査結果から

同じ監査を後でもう一度実行したい場合には、監査結果から監査を再実行できます。

監査またはスナップショットの結果をレビューしているときに、その結果から監査を再実行する場合、結果が取得された後で元の監査のルールが変更されている可能性があります。このような場合、実行されるのは更新された監査であり、結果を生成した元の監査ではありません。

監査を再実行するには、次の手順を実行します。

1 ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**監査と修復**] を選択します。

2 [監査] を選択し、WindowsまたはUnixを選択します。

3 監査を選択し、詳細ペインで監査結果を選択します。監査を実行するたびに、結果が詳細ペインに追加されます。

4 監査結果をダブルクリックして開きます。

5 [**アクション**] メニューで [**監査の再実行**] を選択します。

6 [監査の実行] ウィンドウの [サマリー] ページでは、ステップ1で監査の名前、監査のソースとなるサーバーまたはスナップショット、監査で定義されているルールの総数、監査のすべてのターゲット (サーバーおよびスナップショット) が表示されます。[**ルールの詳細の表示**] をクリックすると、ルールの定義が表示されます。

(オプション) 監査をただちに実行する場合は、プロセスの任意の時点で [**ジョブの開始**] をクリックします。

7 [**次へ**] をクリックします。

8 [スケジュール設定] ページで、監査をただちに実行するか、別の日時に実行するかを選択します。後で実行する場合は、[**次の時刻にタスクを実行**] を選択し、日付と時刻を指定します。

9 [**次へ**] をクリックします。

10 [通知] ウィンドウのデフォルト設定では、監査ジョブの成否に関係なく、監査の完了時にユーザーへ通知電子メールが送信されます。電子メールでの通知を追加するには、[**通知の追加**] をクリックして電子メールアドレスを入力します。

11 (オプション) 電子メールを、監査ジョブが成功した場合または失敗した場合のどちらの場合に送信するかを指定できます。

12 (オプション) [チケットID] フィールドでチケットトラッキングIDを指定します。[チケットID] フィールドが使用されるのは、SAプロフェッショナルサービスのSAが変更管理システムに統合されている場合のみです。それ以外の場合は空白にしてください。

13 [**次へ**] をクリックします。

14 [ジョブステータス] ページで [**ジョブの開始**] をクリックして、監査を実行します。実行完了後、[**結果の表示**] をクリックすると監査の結果が表示されます。

監査またはスナップショットの結果をレビューしているときに、その結果から監査を再実行する場合、結果の取得およびレビュー後に元の監査のルールが変更されている可能性があることを考慮してください。監査を再実行する場合、実行されるのは更新された監査であり、結果を生成した元の監査ではありません。

監査の削除またはスナップショット結果

サーバー上で監査またはスナップショットを実行して結果を表示したら、別のサーバー上で監査またはスナップショットを実行する前に、監査ウィンドウまたはスナップショットウィンドウを閉じて、結果を削除する必要があります。ウィンドウを閉じない場合、表示される結果とルールはすべて、元のサーバーに所属します。

監査のスケジュール設定

監査のスケジュールを設定するには、監査をいつ実行するか (1 回または定期的ジョブとして) と、ジョブのステータスに関する電子メール通知の受信者を指定する必要があります。また、すでにスケジュールが設定されている監査の表示、編集、削除またはキャンセルも実行できます。スケジュール設定された監査を削除すると、その監査に関連して作成したすべてのスケジュールが削除されます。また、実行中の監査ジョブをキャンセルすることもできます。アクティブな監査ジョブのキャンセル (26ページ) を参照してください。

監査スケジュールの作成、表示、編集、削除のためのアクセス権が必要です。アクセス権の取得については、SAの管理者にお問い合わせください。アクセス権の詳細については、『SA 管理ガイド』を参照してください。

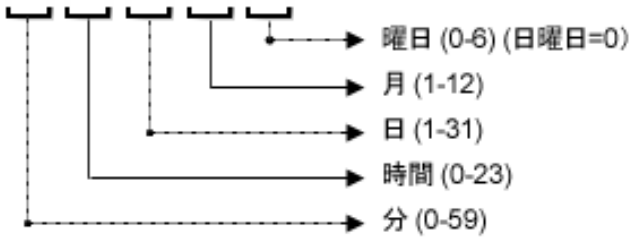
定期的監査のスケジュール設定

監査を作成して構成し、保存したら、監査を定期的に実行するためのスケジュールを指定できます。定期的スケジュールを指定する場合、終了日は監査ジョブが少なくとも 1 回実行されるように設定する必要があります。スケジュールを設定した後で、必要に応じてスケジュールを編集できます。

定期的な監査をスケジュール設定するには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**監査と修復**] を選択し、[監査] を選択します。
2. OS (WindowsまたはUNIX) を選択し、監査をダブルクリックして開きます。
3. [監査] ウィンドウのビューペインで [スケジュール] を選択します。
4. [スケジュール] セクションで、1回、毎日、毎週、毎月、またはカスタムのスケジュールを選択します。次のパラメーターを指定します。
   - **なし**: スケジュールは設定されません。監査を実行するには、監査を選択して右クリックし、[**監査の実行**] を選択します。
   - **毎日**: 指定した時刻に毎日実行します。
   - **毎週**: 監査を実行する曜日を選択します。
   - **毎月**: 監査を実行する月と日を選択します。
   - **カスタム**: [カスタムcrontab文字列] フィールドに、スケジュールを示す文字列を入力します。

     crontab ファイルには5つのフィールドがあり、曜日、月、日、そして時間と分を指定します。次の図は、crontabファイル内の各位置とそれぞれに対応するもの、設定できる値を示しています。



crontab 文字列は、シリアル値 (1、2、3、4) と範囲 (1-5) で指定できます。一部のオペレーティングシステムでは、監査を2分ごと、または10分ごとに実行する場合に、/2または/10のような形式で分を指定します。アスタリスク (*) は、年間のすべての月のように、そのフィールドのすべての値を意味します。日は、日にちと曜日の2つのフィールドで指定できます。両方の日を指定すると、両方の値が実行されます。各フィールド内のカンマ区切り値は、すべてのオペレーティングシステムでサポートされています。

次に例を示します。

5,10 0 10 * 1は、毎月10日および毎週月曜日の午前0時5分および午前0時10分に、監査を実行することを意味します。

crontabの入力形式の詳細については、Unixのmanページを参照してください。

5 [時刻と期間] セクションで、スケジュールのタイプごとに、毎日のスケジュールを開始する時刻 (時と分) を指定します。終了時刻を指定しないと、監査は無期限に実行されます。

監査スケジュールを終了する日付を選択するには、[終了] を選択して日付を選択します。監査スケジュールを無期限に実行するには、タイムゾーンの設定で [終了] オプションの選択を解除します。

6 監査スケジュールを保存するには、[**ファイル**] メニューから [**保存**] を選択します。これで、指定したスケジュールに従って監査が実行されます。

監査スケジュールの編集

監査を作成 (または編集) して保存した後で、監査スケジュールを編集できます。

スケジュール済み監査を編集するには、次の手順を実行します。

1 ナビゲーションペインで、[ジョブとセッション] を選択します。

2 [定期的スケジュール] を選択します。

3 内容ペインの上部にあるドロップダウンリストで、[サーバーの監査] を選択します。

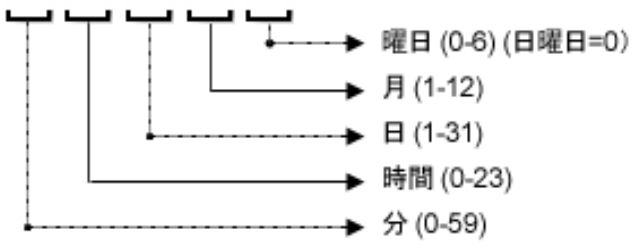
4 スケジュール済みの監査ジョブを選択し、右クリックして [**開く**] を選択します。

5 [監査] ウィンドウで、ビューペインで [スケジュール] を選択して、監査スケジュールを表示します。

6 監査スケジュールを編集するには、次のパラメーターを変更します。

- **なし**: スケジュールは設定されません。監査を実行するには、監査を選択して右クリックし、[**監査の実行**] を選択します。
- **毎日**: 指定した時刻に毎日実行します。
- **毎週**: 監査を実行する曜日を選択します。
- **毎月**: 監査を実行する月と日を選択します。
- **カスタム**: [カスタムcrontab文字列] フィールドに、スケジュールを示す文字列を入力します。

  crontab ファイルには5つのフィールドがあり、曜日、月、日、そして時間と分を指定します。次の図は、crontabファイル内の各位置とそれぞれに対応するもの、設定できる値を示しています。



crontab 文字列は、シリアル値 (1、2、3、4) と範囲 (1-5) で指定できます。一部のオペレーティングシステムでは、監査を2分ごと、または10分ごとに実行する場合に、/2または/10のような形式で分を指定します。アスタリスク (*) は、年間のすべての月のように、そのフィールドのすべての値を意味します。日は、日にちと曜日の2つのフィールドで指定できます。両方の日を指定すると、両方の値が実行されます。各フィールド内のカンマ区切り値は、すべてのオペレーティングシステムでサポートされています。

次に例を示します。

5,10 0 10 * 1は、毎月10日および毎週月曜日の午前0時5分および午前0時10分に、監査を実行することを意味します。

crontabの入力形式の詳細については、Unixのmanページを参照してください。

7 [時刻と期間] セクションで、スケジュールのタイプごとに、毎日のスケジュールを開始する時刻 (時と分) を指定します。終了時刻を指定しないと、監査は無期限に実行されます。監査スケジュールを終了する日付を選択するには、[終了] を選択して日付を選択します。[タイムゾーン] には、ユーザープロファイルで設定されているタイムゾーンが適用されます。

8 (オプション) 監査スケジュールを無期限に実行するには、[終了] オプションの選択を解除します。

9 監査スケジュールを保存するには、[**ファイル**] メニューから [**保存**] を選択します。これで、指定したスケジュールに従って監査が実行されます。

以前のリリース (SA 10.0 以前) で監査スケジュールの設定があり、システムタイムゾーン (SystemV/PST8 またはSystem V/PST8PDT) を使用していた場合は、監査スケジュールをリセットして、サポートされているタイムゾーンを使用します。リセットしない場合、実行時にエラーが発生します。

完了した監査ジョブの表示

完了した監査ジョブに関する情報を表示するには、次の手順を実行します。

1 ナビゲーションペインで、[ジョブとセッション] を選択します。

2 [ジョブログ] を選択します。

3 内容ペインには、この SA コアのすべてのジョブ実行が表示されます。監査ジョブだけを表示するには、内容ペインの上部にあるドロップダウンリストから、[監査タスクの実行] を選択します。スケジュール済みの監査だけを表示するには、内容ペインの上部にある [ユーザー ID] フィールドにユーザー IDを入力します。

4 監査結果を表示する監査ジョブを開き、[**結果の表示**] をクリックします。

監査のエクスポート/インポート

監査フィルターを使用すると、SAコア/メッシュからどの監査をエクスポートするかをDETに指示できます。エクスポートした監査は、別の SA コア/メッシュにインポートできます。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。

アクティブな監査ジョブのキャンセル

SAクライアントでは、アクティブな監査ジョブを終了できます。アクティブな監査ジョブとは、すでに開始されて実行中のものです。

アクティブな監査ジョブに対する終了アクションは、ソフトキャンセルと呼ばれます。ソフトキャンセルとは、ジョブが途中まで実行された状態で、[サーバーの監査] ウィザードの [ジョブステータス] ステップで [**ジョブの終了**] をクリックすることによりジョブを停止する操作です。ソフトキャンセルは、停止しようとしているアクティブな監査ジョブだけに適用されます。

進行中の監査をキャンセルするアクセス権が必要です。一般的に、監査ジョブを開始するアクセス権があれば、実行中の監査ジョブを停止することもできます。この他、「任意のジョブの編集またはキャンセル」アクセス権があれば、実行中の監査ジョブをソフトキャンセルできます。詳細については、『SA 管理ガイド』のアクティブなジョブの終了の項目とアクセス権リファレンスの章を参照してください。アクセス権の取得については、SAの管理者にお問い合わせください。

アクティブな監査ジョブを停止するには、次の手順を実行します。

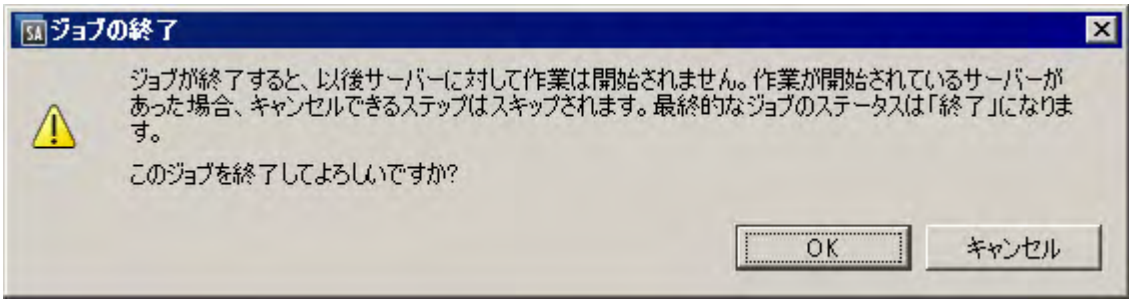
1 [ジョブステータス] ペインで [**ジョブの終了**] をクリックします

このボタンは、ジョブが実行中のときだけ使用できます。

2 [ジョブの終了] ダイアログが表示されます。このダイアログには、ジョブの終了がどのように動作するかが簡単に示されます。

- その後のサーバーに対してはジョブの作業は開始されません。
- すでに作業が開始されているサーバーに対しては、ジョブのステップのうちスキップ可能なものがキャンセルされます。
- [ジョブステータス] に、完了したステップとスキップされたステップが示されます。

3 ジョブが正常に終了した場合、最終的なジョブステータスは「終了済み」になります。



4 [**OK**] をクリックして、ジョブの終了を確認します。[ジョブステータス] ウィンドウに、終了アクションの進行状況が表示されます。

ジョブステータスは終了済みになります。サーバーステータスはキャンセルになります。タスクステータスは成功またはスキップ済みになります。

5 終了が完了したら、SAクライアントジョブログでもジョブを確認できます。

SAクライアントのナビゲーションペインで、[**ジョブとセッション**] を選択します。[ジョブログ] ビューにジョブが終了済みステータスで表示されます。

監査とスナップショットの使用状況の表示

監査を作成して実行したら、すべての管理対象サーバーリストまたはデバイスエクスプローラーから監査を表示したり、特定のサーバーに関連付けられているすべての監査を表示したりできます。

すべての管理対象サーバーから

すべての管理対象サーバーリストからサーバーの監査の使用状況を表示するには、次の手順を実行します。

1 ナビゲーションペインで、[**デバイス**] > [**サーバー**] > [**すべての管理対象サーバー**] を選択します。

2 内容ペインで、サーバーを選択します。

3 [表示] ドロップダウンリストから、[監査] または [スナップショット仕様] を選択します。詳細ペインに、監査とスナップショットの使用状況に関する情報が表示されます。

4 [監査] を選択した場合、詳細ペインで次のオプションのうち1つを選択できます。

- **監査 - サーバーはターゲット**: 選択したサーバーが監査のターゲットであるすべての監査。
- **監査 - サーバーはソース**: 選択したサーバーが監査のソースとして使用されるすべての監査。

または

5 [スナップショット仕様] を選択した場合、選択したサーバーをターゲットとするすべてのスナップショット仕様が詳細ペインに表示されます。

6 (オプション) どのビューでも、監査またはaudit resultsを選択して、[アクション] メニューからアクションを実行できます。たとえば、監査を開いたり、監査を作成したり、監査を再実行したり、監査を削除したりできます。

デバイスエクスプローラーから

デバイスエクスプローラーからサーバーの監査の使用状況を表示するには、次の手順を実行します。

1 ナビゲーションペインで、[**デバイス**] > [**すべての管理対象サーバー**] を選択します。

2 内容ペインで、サーバーを選択し、右クリックして [**開く**] を選択します。

3 デバイスエクスプローラーのビューペインで、[**管理ポリシー**] > [**監査**] を選択します。

4 内容ペインで、[表示] ドロップダウンリストから次のオプションのうち1つを選択します。

- **監査 - サーバーはターゲット**: 選択したサーバーが監査のターゲットであるすべての監査。
- **監査 - サーバーはソース**: 選択したサーバーが監査のソースとして使用されるすべての監査。

5 (オプション) このビューでは、監査を選択して、[アクション] メニューからアクションを実行できます。たとえば、監査を開いたり、監査を作成したり、監査を再実行したり、監査を削除したりできます。

6 次に、ビューペインで [アーカイブされた監査結果] を選択して、このサーバーに関連付けられたアーカイブ済みのすべての監査結果を表示できます。

監査の構成

監査または監査ポリシーを構成するには、次の作業が必要です。

- 監査または監査ポリシーの名前と説明の指定
- 監査または監査ポリシーのソース (サーバー、スナップショット、スナップショット仕様、またはなし) の選択
- 監査ルールの構成—オプションで監査ポリシーをリンクできます。これにより、監査ポリシーのルールを監査で使用するように指定できます。また、これにより、個々のルールを構成することはできなくなります。監査ポリシーのすべてのルールを監査にインポートすることもできます。
- 監査の対象となるターゲットサーバー、サーバーのグループ、またはスナップショットの選択
- 監査ルールの例外の追加 (オプション)
- 監査のスケジュール設定
- 電子メール通知の設定 (オプション)
- 監査の保存

VMware ESXiサーバーは、監査またはスナップショットのソースまたはターゲットに指定できません。

監査を構成するには、次の手順を実行します。

1 監査の作成 (19ページ) に示されているいずれかの方法で、新しい監査を作成します。[監査] ウィンドウが開きます。

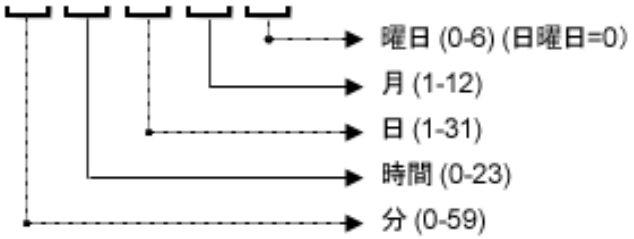
2 監査に関する次の情報を入力します。

- **プロパティ**: 監査の名前と説明を入力します。
- **ソース**: 監査のソースとしては、サーバー、スナップショット、またはスナップショット仕様が使用できます (または、ソースを選択せずにルールを独自に定義することもできます)。サーバーをソースとして使用した場合、監査のルールを定義する値をサーバーから参照することができます。スナップショットを選択した場合、監査ルールを定義する際に、スナップショットおよびスナップショット結果にあるルールに制限されます。スナップショット仕様を選択した場合、スナップショット仕様のターゲットから取得されたスナップショットと、監査のターゲットとが比較されます。スナップショット仕様をソースとして選択した場合、スナップショット内のルールは編集できません。ソースなしを選択した場合、独自のルールを定義するか、監査ポリシーをルールセクションにリンクする必要があります。ただし、一部のルールは定義の際にソースを指定する必要があります。
- **ルール**: リストからルールカテゴリを選択して、監査のルールの構成を開始します。各監査ルールは固有のもので、個別の指示が必要です。個々の監査ルールの構成方法については、監査と修復のルール (35ページ) を参照してください。

  監査ポリシーを使用して監査のルールを定義するには、[ポリシーのリンク] または [ポリシーのインポート] をクリックします。監査ポリシーをリンクすると、監査と監査ポリシーが直接に結び付けられ、ルールを作成することはできなくなります。ポリシーをリンクした場合、監査ポリシーに構成されたルールだけが監査で使用されます。したがって、ポリシーが変更されると、監査にも変更が反映されます。監査ポリシーをインポートした場合、監査はポリシーに定義されているすべてのルールを使用しますが、監査ポリシーとのリンクは維持されません。監査ポリシーの詳細については、監査ポリシーの管理 (79ページ) を参照してください。
- **ターゲット**: 監査のターゲットを選択します。これは、評価と比較の対象として監査ルールで設定するサーバー、サーバーグループ、スナップショットです。サーバーまたはサーバーグループを追加するには、**[追加]** をクリックします。スナップショットターゲットを追加するには、[スナップショットターゲット] セクションで **[追加]** をクリックします。

- **例外**: [**追加**] をクリックして、監査のルールに対する例外を追加します。[例外の追加] ウィンドウで、1つまたは複数のサーバー (またはデバイスグループ) を選択し、選択したサーバーから除外するルールを選択します。監査の任意のルールを、任意のターゲットサーバーまたはスナップショットから除外できます。オプションで、例外の説明、チケットID、有効期限を追加できます。
- **スケジュール** (オプション): 1回、毎日、毎週、毎月、指定のスケジュールを選択します。次のパラメーターを指定します。
  - **なし**: スケジュールは設定されません。監査を即時実行したい場合や1回のみ実行したい場合は、監査を選択して右クリックし、[**監査の実行**] をクリックします。
  - **毎日**: 指定した時刻に毎日実行します。
  - **毎週**: 監査を実行する曜日を選択します。
  - **毎月**: 監査を実行する月を選択します。
  - **カスタム**: [カスタムcrontab文字列] フィールドに、スケジュールを示す文字列を入力します。

    crontabファイルには5つのフィールドがあり、曜日、月、日、そして時間と分を指定します。次の図は、crontabファイル内の各位置とそれぞれに対応するもの、設定できる値を示しています。

    crontab 文字列は、シリアル値 (1、2、3、4) と範囲 (1-5) で指定できます。一部のオペレーティングシステムでは、監査を2分ごと、または10分ごとに実行する場合に、/2または/10のような形式で分を指定します。アスタリスク (*) は、年間のすべての月のように、そのフィールドのすべての値を意味します。日は、日にちと曜日の 2 つのフィールドで指定できます。両方の日を指定すると、両方の値が実行されます。各フィールド内のカンマ区切り値は、すべてのオペレーティングシステムでサポートされています。次に例を示します。

    5,10 0 10 * 1は、毎月10日および毎週月曜日の午前0時5分および午前0時10分に、監査を実行することを意味します。

    crontabの入力形式の詳細については、Unixのmanページを参照してください。
  - **時刻と期間**: スケジュールタイプごとに、監査を開始する時間、分、曜日、月を指定します。終了時刻を指定しないと、監査は無期限に実行されます。終了日を選択するには、[終了] を選択します。カレンダーセレクターで、終了日を選択します。[タイムゾーン] には、ユーザープロファイルで設定されているタイムゾーンが適用されます。
  - **通知**: 監査ジョブの実行が終了したときに通知を送信する電子メールアドレスを入力します。電子メール送信の条件として、監査ジョブが成功した場合と失敗した場合 (監査ルールの成功と失敗ではありません) を選択できます。電子メールアドレスを追加するには、[通知の追加] ルールをクリックします (これが有効なのは、定期的に監査を実行する場合のみです)。

3 監査の構成が終了したら、[**ファイル**] メニューから [**保存**] を選択します。

監査とスナップショットのソース

監査またはスナップショット仕様のソースを選択するには、いくつかのオプションがあります。

- ソース: サーバー (31ページ)
- ソース: スナップショット (32ページ)
- ソース: スナップショット仕様 (32ページ)
- ソース: ルール (33ページ)

監査のソースによって、監査またはスナップショット仕様で選択および構成可能なルールが決まります。ソースの選択は、監査またはスナップショット仕様の目的によって変わります。

ソース: サーバー

管理対象サーバーを監査またはスナップショット仕様のソースにすることができます。

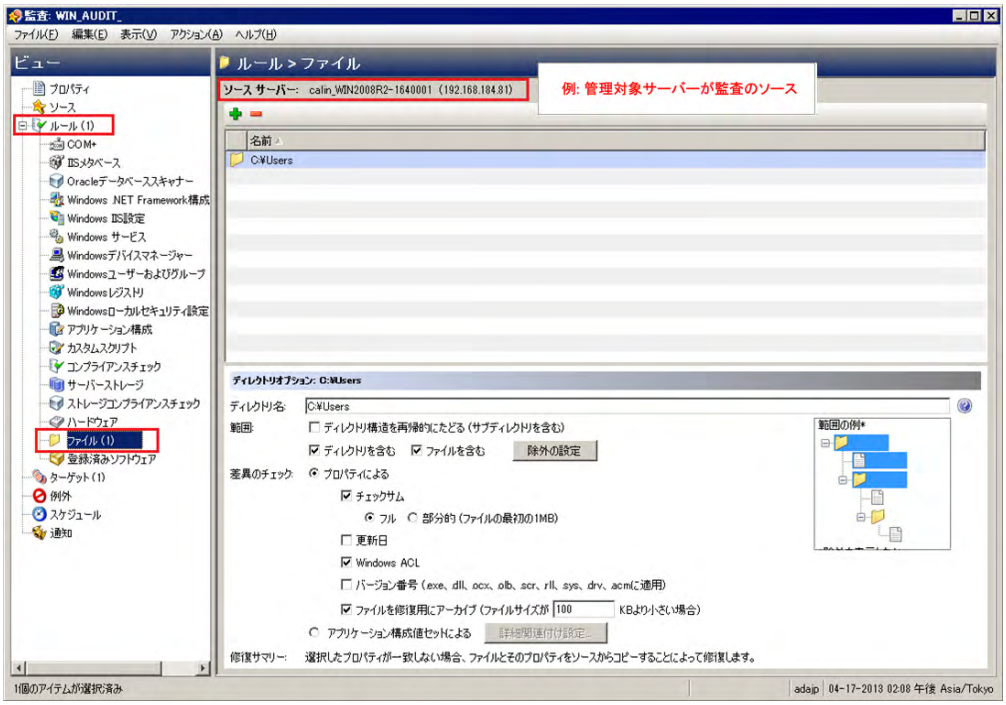
監査またはスナップショット仕様に追加する必要があるサーバーオブジェクトが特定のサーバーに含まれていることがわかっている場合、そのサーバーを監査のソースとして選択します。たとえば、特定のターゲットサーバー上のApache Webサーバーのアプリケーション構成ファイル (httpd.confなど) に対して、監査またはスナップショットの取得を行う場合、Apacheがインストールされて正しく構成されているサーバーを、監査のソースとして選択します。

監査またはスナップショット仕様ルールを作成する際に、いくつかの異なるソースサーバーを選択できます。また、各サーバーオブジェクトルールに対して異なるソースを選択することもできます。

監査またはスナップショットのソースにVMware ESXiサーバーは指定できません。

図3に、サーバーを監査のソースとして選択したときに、[監査] ウィンドウまたは [スナップショット仕様] ウィンドウに表示される内容ペインを示します。

図3　　監査のソースとしてのサーバー : 監査ルールの作成



ディレクトリオプションの詳細については、範囲の一般的な使用法と図 (47ページ) を参照してください。

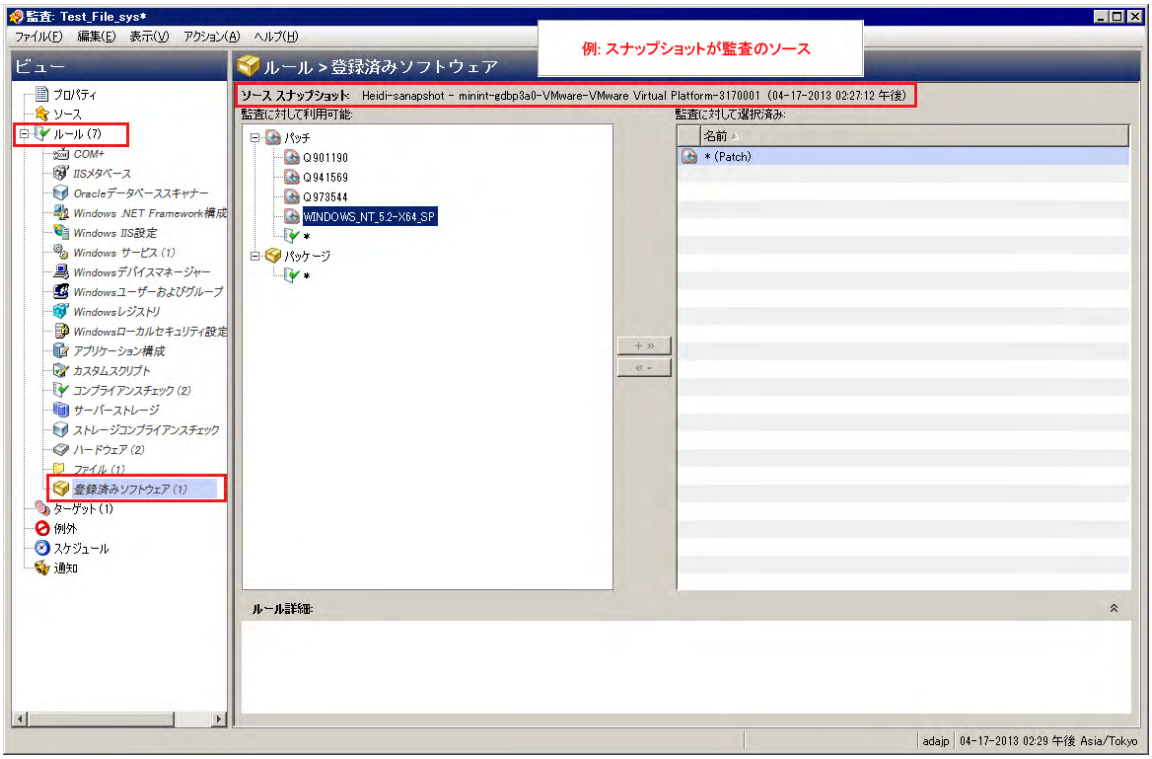
ソース: スナップショット

スナップショットを監査またはスナップショット仕様のソースにすることができます。

既知の望ましい状態にある管理対象サーバーのスナップショット (ゴールデンサーバー構成) が存在し、監査でそのスナップショットを他のサーバーと比較する場合、そのスナップショットを監査またはスナップショット仕様のソースとして選択します。また、取得したサーバー値を使用して、別のサーバーのスナップショットを取得することもできます。スナップショットを監査またはスナップショット仕様のソースとして使用した場合、スナップショットの元になったスナップショット仕様の結果とルールの両方を選択できます。

図 4 に、スナップショットをソースとして使用する場合の監査またはスナップショット仕様ルール作成のためのオプションを示します。スナップショットの結果およびスナップショットのルールからの選択が可能です。

図4　監査のソースとしてのスナップショット: 監査ルールの作成に利用可能なサーバーオブジェクト



ソース: スナップショット仕様

スナップショット仕様を監査のソースにすることができます。これは一般的に「再帰的監査」と呼ばれます。スナップショット仕様から監査を実行すると、監査では仕様で定義されたすべての情報が使用され、定義したフィルターがすべて適用されます。

このオプションは、サーバーの構成を時間に沿って追跡し、変更を監視する場合に使用します。たとえば、アプリケーションを追跡することで、ある期間にわたって構成が常に正しいことを確認できます。このアプリケーションが複数のサーバーで動作している場合、サーバー構成の必要な状態を定義するスナップショット仕様を作成して、スナップショットを実行することができます。

次に、監査を作成し、スナップショット仕様を監査のソースとして使用します。スナップショットのターゲットとなったすべてのサーバーが、監査のターゲットとなります。監査をその場で、またはスケジュールによって実行すると、各サーバーの現在の構成が、スナップショットから最初に取得された状態と比較されます。監査のソースとなるスナップショット仕様が定期的に実行されるように設定されている場合、監査は最も新しく実行されたスナップショットとの比較を行います。変更がある場合は、監査結果ウィンドウに表示されます。

ソース: ルール

ソースサーバーからのソース値を使用するルールは、監査のソースとして使用できます。

ほとんどのルールの定義にはソースが必要ですが、次のルールは例外です。

- ソース (サーバーまたはスナップショットまたはスナップショット仕様) に由来する値を設定していない事前構成済みのルール
- ソース (サーバーまたはスナップショットまたはスナップショット仕様) に由来する比較値を設定していないカスタムスクリプトルール

監査にソースを必要とするルールがあり、ソースが指定されていない場合、監査を保存することはできません。すべての比較チェックと、ソース値との比較を行うルールに対して、ソースを選択する必要があります。

サーバーオブジェクト

表 1 に、監査またはスナップショット仕様でルールを作成できるすべてのサーバーオブジェクトの一覧を示します。一部のサーバーオブジェクト値の取得と監査はライブで行われ、一部のオブジェクトはモデルリポジトリから取得されます。

表1　　監査とスナップショットで使用されるサーバーオブジェクト

サーバーオブジェクト	説明	取得方法 (ライブまたはモデルリポジトリから)
アプリケーション構成	アプリケーション構成ファイルの内容とその値	ライブ
Windows COM+ (表の下の注を参照)	COM+オブジェクトとコンポーネントカテゴリ。	ライブ
カスタムスクリプト	サーバーから情報を取得し、内容を比較する独自のカスタムスクリプトを作成します。たとえば、カスタムアプリケーションからの出力を収集し、返された出力を監査に設定された値と比較するスクリプトを作成できます (Python スクリプトの場合はPythonのみ)。	ライブ
検出されたソフトウェア	検出されたソフトウェアは、Windows および UNIX 管理対象サーバーに適用する署名ベースのソフトウェア検出メカニズムであり、SAの管理対象ではないアプリケーションとソフトウェアの管理を行います。	ライブ
ファイル	ファイルとディレクトリ (およびサブディレクトリ) の内容、ユーザーおよびグループのアクセス、ファイルのチェックサム、ファイル更新日、Windows ACL (Windowsのみ)。	ライブ
ハードウェア	CPU、ストレージデバイス、メモリ。	モデルリポジトリ
IISメタベース	スナップショットまたは監査の対象とするMicrosoft IISメタベースオブジェクトおよび構成値。	ライブ
IIS 7.0	Microsoft IIS 7.0	ライブ

表1　監査とスナップショットで使用されるサーバーオブジェクト（続き）

サーバーオブジェクト	説明	取得方法(ライブまたはモデルリポジトリから)
Internet Information Server	Windows サーバーの IIS に関するリアルタイム情報。サーバー名、サーバータイプ、サーバー状態、ログファイルのパス、ドキュメントファイルのパスなど。	ライブ
ローカルセキュリティ設定	セキュリティ設定に関するリアルタイム情報。パスワードポリシー、監査ポリシー、ユーザー権限、セキュリティオプションなど。	ライブ
登録済みソフトウェア	ソースサーバーに実際にインストールされているすべてのパッケージまたはパッチ。モデルリポジトリに登録されているかどうかには関係しません。	ライブ
ストレージ	データセンターのストレージデバイスおよび SAN デバイスおよび接続に関連する情報 (コアでストレージが有効になっている場合)。 SAN オブジェクトの監査とスナップショットを実行するには、Storage Essentials (SE) バージョン6.1.1以後が必要で、Server AutomationのSE Connectorコンポーネントを SA コアにインストールして構成しておく必要があります。	ライブ
BSA Essentials Subscription Servicesのコンプライアンスチェック	BSA Essentials Subscription Servicesに登録している場合、さまざまな種類の監査ルールやその構成要素 (コンプライアンスチェックとも呼ばれる) にアクセスできます。アクセスできるチェックの種類はサブスクリプションによって異なりますが、Microsoft Windows 用の最新のパッチ、現行の規制コンプライアンスポリシー (FISMA、Sarbanes-Oxley など)、BSA Essentials Subscription Services開発者コミュニティによるユーザー作成のルール、毎日更新される脆弱性情報などが含まれる可能性があります。	ライブ
ユーザーとグループ	サーバー上のユーザーとグループに関する情報を比較します。最後にログインしたユーザー名、CTRL＋ALT＋DELETEが有効かどうかなどです。	ライブ
Windows .NET Framework 構成	アセンブリキャッシュおよび構成アセンブリリストに関するリアルタイム情報。アセンブリ名、バージョン、ロケール、パブリックキートークン、キャッシュファイル (GACまたはZAP)、プロセッサーアーキテクチャー、カスタム、ファイル名など。 各構成アセンブリリストに対して、アセンブリ名、パブリックキートークン、コードベース、バインドポリシー、ファイル名、ファイルデータなどの情報を使用できます。	ライブ

表1　監査とスナップショットで使用されるサーバーオブジェクト（続き）

サーバーオブジェクト	説明	取得方法(ライブまたはモデルリポジトリから)
Windowsレジストリ (表の下の警告を参照)	取得して比較するWindowsレジストリディレクトリまたはレジストリキー値を選択します。	ライブ
Windowsサービス	Windowsサービスを選択します。	ライブ
Windowsユーザーおよびグループ	Windows Unixサーバーのユーザーおよびグループ情報。	ライブ

Windows COM+カテゴリ(フォルダー)にオブジェクトがない場合、デバイスエクスプローラーには空のCOM+フォルダーが表示されますが、そのカテゴリはスナップショットまたは監査には含められません。

SAクライアントでは、Windowsレジストリ全体のスナップショットやシステムキー全体のスナップショットは作成できません。これは、現在の設計で対応可能なデータサイズを超えてしまうからです。

SA監査と修復は、デバイスファイルまたはソケットをサポートしません。

監査と修復のルール

監査またはスナップショット仕様を作成する際には、監査と修復ルールを構成する必要があります。ルールは次の内容を定義します。

- スナップショットまたは監査と比較を行うサーバーオブジェクトのタイプ。これらは、サーバーのファイルシステム、ハードウェア情報、アプリケーション構成、インストール済みのパッチまたはソフトウェア、ユーザーとユーザーグループ: などのオブジェクトです。
- 監査またはスナップショットを行うオブジェクトに関する情報。たとえば、サーバーのファイルシステムの場合、Windows NTファイルのアクセス制御レベルを取得できます。アプリケーションの場合、スナップショットまたは監査を行うアプリケーション構成値と、ルールとターゲットサーバー上の実際の値との間に差異が見つかったかどうかを指定する修復値を取得できます。

ルールにカスタムスクリプトを追加することにより、ファイルに記録されているすべてのパスワードが特定の長さに一致するかどうかを判定できます。ルールには、特定のWindowsサービスがサーバー上で実行中または無効になっているかどうかを判定するチェックも含めることができます。ルールによっては、監査またはスナップショットに定義された値が監査の実行後にサーバーの値と異なっていた場合に使用する、サーバーオブジェクトの修復値を指定できます。たとえば、Windowsサービスが無効になっている場合、修復値によってサービスを再開するように指定できます。修復値は、監査の実行後に、[監査結果]ウィンドウから手動で適用されます。

構成ルール

最も単純なルールの場合は、スナップショットまたは監査を行うサーバーオブジェクトを選択するだけで構成と定義が終わります。サーバー上の構成ファイルに値またはプロパティが存在することをチェックするだけで、詳細パラメーターをいっさい設定する必要がないルールもあります。

例: 検出されたソフトウェアルールは、ターゲットサーバー上にインストールまたはデプロイされている登録済みと未登録のすべてのソフトウェアをチェックします。

例: ハードウェアルールでは、ターゲットサーバー上に存在するCPU、メモリ、またはストレージの値をチェックできます。この場合、その他のルールパラメーターはいっさい不要です。

ルールの中には、もっと複雑で、詳細な構成を必要とするものもあります。たとえば、値の範囲をチェックする式を指定するものや、間違った値を置き換える修復を指定するものなどです。

監査および監査ポリシーでは、必要な場合、オブジェクトに設定する修復値を定義することもできます。修復値は、サーバーオブジェクトが必要な状態と異なっていることが検出された場合のみ使用されます。すなわち、ターゲットサーバーの構成が監査のルールに対してコンプライアンス違反になっている場合です。修復値は、監査の実行後に、[監査結果] ウィンドウから手動で適用されます。

監査ルールは次の要素から構成されます。

- **サーバーオブジェクト**: これは監査で評価できる特定のサーバー構成、すなわち、サーバーのファイルシステム、アプリケーション構成ち、ハードウェア情報、インストール済みソフトウェア (パッチやパッケージ)、Windowsレジストリエントリなどです。サーバーオブジェクトは通常いくつかの他のオブジェクトから構成されており、それらもチェックできます。

  例: Windowsサーバーで、ターゲットサーバーに特性のWindowsサービスが存在するかどうかと、それが有効になっているかどうかを知りたいとします。

- **ターゲット値**: これは、ターゲットサーバー上でチェックする値または設定です。

  例: たとえば、特定のディレクトリがサーバー上に存在するかどうか、アプリケーションが正しく構成されているかどうか、特定のサービスがオンになっているかどうかなどを判定できます。

- **修復値**: これは、ターゲットサーバー上にターゲット値が見つからなかった場合に、サーバーオブジェクトに対して変更する値です。修復値は自動的には適用されません。監査の実行後に修復変更を実行する必要があります。

図5に、File Replicationという名前のWindowsサービスに対して定義された監査ルールを示します。

図5　　修復値が構成されたカスタム監査ルール

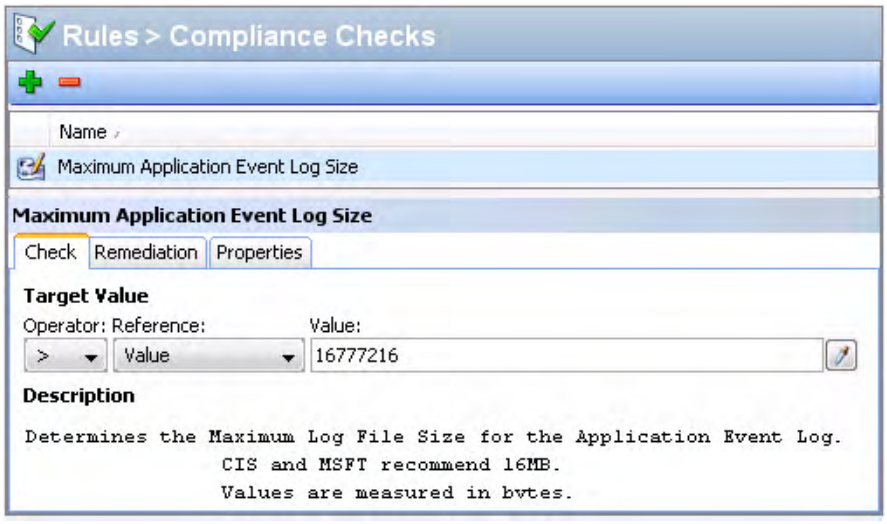


図5の監査ルールは、次の方法で構成されています。

- **[ルール] > [コンプライアンスチェック]**: BSA Essentials Subscription Servicesから選択したルール (最大アプリケーションイベントログサイズ) をリストします。
- **ルール詳細チェック**
  - **ターゲット値**: これは、監査のターゲットとなるサーバー上の値と比較する正しい値です。この例の場合、ルールは、ターゲットサーバーのアプリケーションイベントログファイルのサイズが16777216バイトを超えていないかどうかを確認するように構成されています。たとえば、ターゲット値パラメーターは次のように設定されています: `> Value 16777216`。

— **説明**: ターゲットサーバー上でチェックする値の説明です。この例の場合、監査は、アプリケーションイベントログファイルのサイズが、CISおよびMSFTの推奨サイズ制限である16MB (16777216バイト) を超えていないかどうかをチェックします。

この情報は、ターゲットサーバーのアプリケーションイベントログファイルのサイズを評価して、16MBを超えるかどうかを判定するように監査に指示します。

- **修復**: 修復値は、ターゲットサーバー上の値が、監査に定義した値 (ターゲット値) と一致しない場合に取るアクションを決定します。この例では、修復値はCIS およびMSFT の推奨サイズ制限である16MB (16777216バイト) に設定されています。この値は、監査の実行後に、ターゲットサーバーの値がルール基準に違反した場合のみ、[監査結果] ウィンドウから修復できます。

監査とスナップショットのルール

監査と修復ルールの作成と構成のためのアクセス権を持つ必要があります。アクセス権の取得については、SAの管理者にお問い合わせください。アクセス権の詳細については、『SA 管理ガイド』を参照してください。

各タイプのサーバーオブジェクトに対して設定できるルールの情報については、対象のサーバーオブジェクトに関する次の項目を参照してください。

- アプリケーション構成ルールの構成
- COM+ルールの構成
- カスタムスクリプトルールの構成
- 検出されたソフトウェアルールの構成
- ファイルルールの構成
- ハードウェアルールの構成
- IISメタベースルールの構成
- IISルールの構成
- IIS 7.0ルールの構成
- ローカルセキュリティ設定ルールの構成
- 登録済みソフトウェアルールの構成
- ストレージルールの構成
- Windows .NET Framework構成ルールの構成
- Windowsレジストリルールの構成
- Windowsサービスルールの構成
- Windows/UNIXユーザーおよびグループルールの構成
- コンプライアンスチェックの構成

SAコアの一部には、コンプライアンスチェックの付いたイベントロギング、オペレーティングシステム、ユーザーとユーザーグループルールといった古い内容が含まれるものがあります。これらのチェックは、EPから利用できるCISポリシーに統合されました。

アプリケーション構成ルールの構成

アプリケーション構成監査ルールを使用すると、管理対象サーバー上の構成ファイルの値を監査して、これらのファイルが適切に構成されているかどうかをチェックできます。

監査するターゲット構成ファイルとの比較の基礎として、あらかじめ定義されたアプリケーション構成テンプレートをリストから選択できます。また、組織のユーザーが監査、スナップショット仕様、または監査ポリシーで使用できるように作成したカスタムアプリケーション構成を選択することもできます。

監査で使用するアプリケーション構成は、アプリケーションの構成ファイルの値と構造をモデル化します。これにより、管理対象サーバー上の既存の構成ファイルの値をチェックするルールを設定できます。

監査、スナップショット仕様、または監査ポリシーでアプリケーション構成を選択して [**表示**] をクリックすると、監査のソースからの構成ファイルの内容が表示されます。監査ルールに追加できるすべてのキーと値のペアが表示されます。

[監査] ウィンドウに表示される値は、監査のソースまたは監査ポリシー (またはスナップショット仕様のターゲット) によって次のように異なります。

- 監査または監査ポリシーのソースとしてサーバーを選択した場合、監査ルールに表示されるアプリケーション構成値は、アプリケーション構成テンプレートによってフィルターされた後の、ソースサーバー上の構成ファイルの値です。
- 監査または監査ポリシーのソースとしてスナップショットを選択した場合、スナップショットが実行された時点で取得された値だけを変更できます。
- ソースを選択しない場合、アプリケーション構成ファイルに対してルールを構成することはできません。
- スナップショット仕様でアプリケーション構成を構成した場合、構成の値はターゲットサーバーから得られます。

監査のアプリケーション構成ルールには、ソース構成ファイルの値のうち、アプリケーション構成でモデル化されたものだけが表示されます。アプリケーション構成がカスタマイズされ、カスタム属性が定義されていない (ただしソース構成ファイルに値が存在する) 場合、アプリケーション構成は監査または監査ポリシーには表示されません。

ソースアプリケーション構成ファイルの内容を表示した後で、ソースファイルから値を選択し、ターゲット構成に対するチェックに使用するルールを作成することにより、ルールを定義できます。また、監査でルールとターゲット構成ファイルの値に差異が見つかった場合に使用する修復値も定義できます。

アプリケーション構成ルールの作成

アプリケーション構成ルールの構成方法を理解するために、例を見てみましょう。

例: 目的は、UNIXのhostsファイル (`/etc/hosts`) に対する監査ルールを作成し、サーバーのグループの `/etc/hosts` ファイルを監査して、正しい値が含まれていることを確認することです。特定のゴールデンサーバー上の UNIX hosts ファイルが、他のサーバーが適合すべき理想的な hosts ファイル構成の状態を表すことがわかっています。このゴールデンサーバーを監査のソースに選択し、そのファイルの内容を借りて、監査のルールを作成できます。ルールを作成して監査を保存したら、サーバーのグループに対して監査を実行して、`/etc/hosts`ファイルが (監査ルールに基づいて) 正しく構成されているかどうかを判定できます。

この例では、「等しい」(=) 演算子が使用されています。アプリケーション構成ルールで使用できる演算子は次のとおりです。
= (等しい)、<> (等しくない), < (小さい)、<= (以下)、> (大きい)、>= (以上)、含む、含まない、正規表現に一致、正規表現に一致しない

アプリケーション構成ルールを作成するには、次の手順を実行します。

1 監査の作成（19 ページ）に示されている方法のいずれかで、監査を作成します。このルールをスナップショット仕様に対して作成する場合は、スナップショット仕様の作成 (115ページ) を参照してください。

2 監査ソースを選択します。サーバー、スナップショット、スナップショット仕様、またはソースなしが選択できます。監査で選択したソースは、アプリケーション構成に対して作成できるルールの種類を決定します。ソースを選択しないと、アプリケーション構成ルールを構成することはできません。

3 [監査] ウィンドウのビューペインで、[ルール] > [アプリケーション構成] を選択します。

4 内容ペインで をクリックして、利用可能なすべての構成テンプレートにアクセスします。

5 [構成テンプレートの選択] ウィンドウで、監査ルールに追加するテンプレートを 1 つまたは複数選択して、**[OK]** をクリックします。

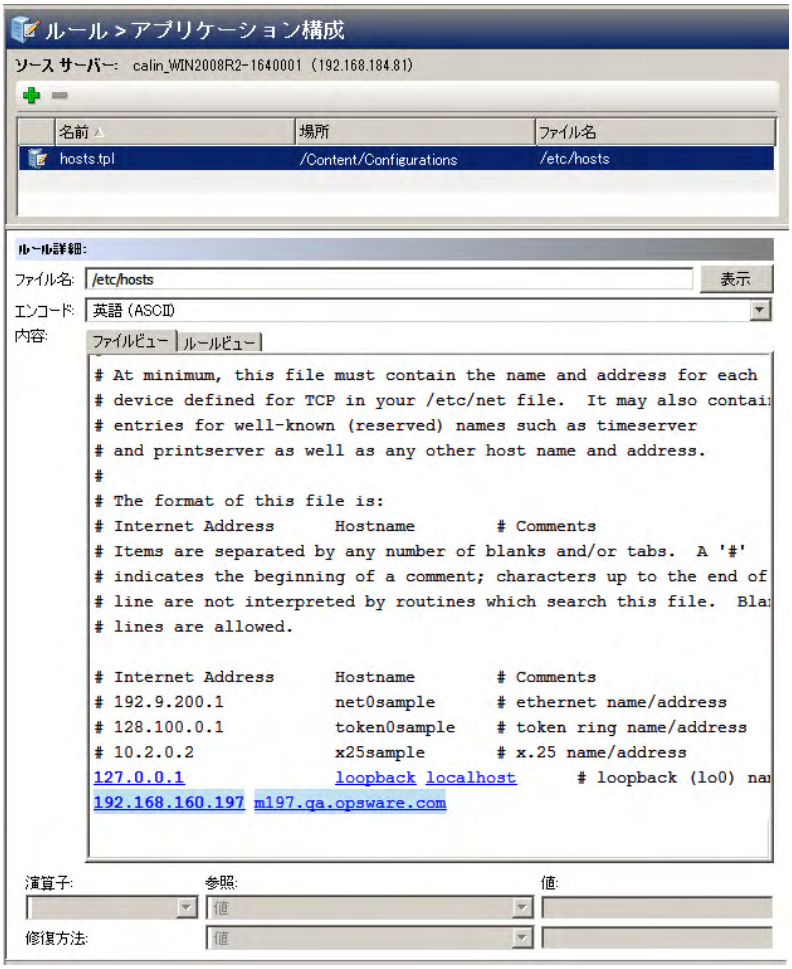
6 構成するテンプレートを選択します。その内容がテンプレートエディターに表示されます。

7 **[表示]** をクリックして、構成ファイルの内容を [ファイルビュー] タブに表示します。

構成ファイルの内容が表示されない場合、[ファイル名] セクションに正しいパスを入力します。

例: UNIX hostsファイルを表示すると、図6に示すような情報が表示されます。ソースhostsファイルの内容とIPアドレス/ホスト名ペア (青で強調表示) が表示されます。

図6 hostsファイル用のアプリケーション構成監査ルール



8 この構成ファイルに対する監査ルールを作成するには、ソースサーバー (監査のソースとして選択したサーバー) 上のhostsファイルからキーと値のペアを選択します。

9 このルールを作成するには、[ファイルビュー] タブ領域でIPアドレスを選択します。ソースサーバーから取得したファイルの内容が表示されます。図6の例では、127.0.0.1などのIPアドレスを選択できます。IPアドレスを選択すると、要素が青で強調表示されます。青のテキストは、要素からルールを作成できることを示します。

アプリケーション構成監査ルールの構成時の色分けの詳細については、表2を参照してください。

内容領域でIPアドレスを選択した後、[演算子] フィールドの値は空です。これは、ルールに演算子がまだ追加されていないからです。この値をルールに追加するには、値をダブルクリックするか、内容の下のルール式領域に次のパラメーターを入力します。

- **演算子**: [=] (等しい) を選択します。演算子を [=] に変更すると、「等しい」演算子がただちにルールに追加されます。演算子を選択なしに変更すると、演算子はただちにルールから削除されます。
- **参照**: [値] を選択します。
- **値**: 127.0.0.1と入力します。
- **修復方法**: 127.0.0.1と入力します。

これは、値が127.0.0.1のIPアドレスを探すことを表します。このアドレスが見つからなくても、修復値は127.0.0.1となるので、このIPアドレスが含まれないターゲットサーバー上のホストファイルにこの値を追加できます。

10 [ファイルビュー] タブ領域でホスト名を選択します。前のステップで最初に選択したIPアドレスが緑になっています。緑のテキストは、次に設定するルールパラメーターが、前に選択したIPアドレスとペアになることを示します。

11 [ルール] セクションで、次のパラメーターを設定します。

- **演算子**: [=] (等しい) を選択します。
- **参照**: [値] を選択します。ルール定義に対してカスタム属性を選択した場合、このカスタム属性がターゲットサーバー上に存在しないと、このルールの監査は失敗します。
- **値**: hostを選択します。
- **修復方法**: hostを選択します。これにより、ルールの最後の部分が追加されます。この部分は、IPアドレス127.0.0.1がhostと一致するキーと値のペアをターゲットサーバー上でチェックする役割を果たします。

12 [ルールビュー] タブを選択します。このルールは次のように表現されます。

「IPアドレスが値127.0.0.1に等しく、ホスト名に値hostに等しいエントリが含まれるエントリをチェック」

このルールが、ターゲットサーバーまたはスナップショット仕様のhostsファイルを監査する際に使用されます。

注: IPアドレスとホスト名はキーと値のペアなので、IPアドレスとホスト名は必ず組み合わせて指定する必要があります。

13 追加のアプリケーション構成ルールを構成するには、[監査に対して利用可能] セクションでその他のアプリケーション構成を選択します。

14 監査の構成を終了するには、他のルールを定義して、監査のターゲットサーバー、スケジュール、通知を設定します。

15 監査を保存します。

16 監査を実行するには、[**アクション**] メニューから [**監査の実行**] を選択します。詳細については、監査の実行 (21ページ) を参照してください。

アプリケーション構成監査ルールの色分け

初めてアプリケーション構成を表示したときには、監査ルールの作成に使用可能なすべての要素が、青の下線付きテキストで表示されます。ルールの選択と作成を開始すると、色が変化していきます。表 2 に、アプリケーション構成監査ルールの構成で使用される色分けを示します。

表2　　アプリケーション構成監査ルールの色分け

テキストの色	説明
青の下線付き	ルールに使用可能なソース構成ファイル内のすべての要素。
強調表示の濃い青	選択された要素のうち、関連付けられたルールがない要素。
強調表示の薄い青	ルールに追加された要素。
強調表示の中間の濃さの青	選択された要素のうち、関連付けられたルールがある要素。
緑	要素はプライマリキーであり、現在選択されている要素に関連しています。また、この要素は、現在選択されている要素と同じルールで使用されます。 現在選択されている要素に比較値 (=、含む、一致など) を設定した場合、緑のテキストのその他の要素には、自動的に比較値=が設定されます。例: `127.0.0.1  localhost` localhostを選択すると、`127.0.0.1`は緑になります。localhostに比較値を指定した場合、`127.0.0.1`にも自動的に比較値が設定され、次のようなルールができます。 IPが`127.0.0.1`に等しく、かつ`hostname`が`localhost`に等しいエントリが存在する。
太字	プライマリキー。
イタリック	カスタム属性またはSA属性。

COM+ルールの構成

Windows COM+ ルールを構成するには、ターゲットサーバー上で監査またはスナップショットを行うソース COM+ オブジェクトを選択します。COM+ ルールは、選択したオブジェクトのアクセス制御レベル (ACL) もチェックします。これには、継承されたACLも含まれます。

COM+オブジェクトは、オブジェクトの属性に基づいてカテゴリに分類されます。COM+オブジェクトは0個以上のカテゴリを指定します。監査またはスナップショットウィンドウでは、COM+オブジェクトツリーの [ルール] セクションの1つのノードに、すべてのCOM+オブジェクトが表示されます。監査またはスナップショットにCOM+ルールを追加するには、ルールを選択してから右矢印ボタンをクリックします。

監査またはスナップショット結果で COM+ ルールを修復できるようにするには、COM+ オブジェクトまたはカテゴリを選択する際に [関連するすべてのファイルのアーカイブ] オプションを選択します。このオプションを選択すると、COM+オブジェクトに関連付けられたすべてのアクセス許可と起動アクセス許可も監査またはスナップショットルールに含められます。これには、親COM+オブジェクトから継承したものも含まれます。

➤ COM+ ルートフォルダーを監査することはできません。ただし、COM+ の個々のオブジェクトまたはサブカテゴリを監査することはできます。

COM+ルールを構成するには、次の手順を実行します。

1 監査の作成 (19 ページ) に示されている方法のいずれかで、新しい監査を作成します。このルールをスナップショット仕様に対して作成する場合は、スナップショット仕様の作成 (115 ページ) を参照してください。

2 監査ソースを選択します。サーバー、スナップショット、スナップショット仕様、またはソースなしが選択できます。一部の監査ルール (アプリケーション構成、Windowsユーザーおよびグループなど) には、ソースが必要です。

3 [監査] ウィンドウのビューペインで、[**ルール**] > [**COM+**] を選択します。

4 [監査] ウィンドウの内容ペインで、[監査に対して利用可能] セクションのトップレベルノードを展開して、COM+オブジェクトまたはオブジェクトカテゴリを選択します。

5 右矢印ボタンをクリックして、COM+オブジェクトまたはオブジェクトカテゴリを [監査に対して選択済み] セクションに移動します。選択したすべてのCOM+オブジェクトまたはオブジェクトカテゴリが、ターゲットサーバーまたはスナップショット仕様で監査されます。ルールに対して個々のオブジェクトとCOM+カテゴリを選択できます。ルートフォルダーを選択して監査ルールに追加することはできません。

6 ルールウィンドウの下部でオプションを選択します。

   - [関連するすべてのファイルのアーカイブ] オプションを選択すると、監査またはスナップショット結果でCOM+ルールを修復できるようになります。
   - [フルパス名でなくファイル名だけを比較] を選択すると、COM+ルールは選択したファイル名だけをチェックし、フルパスはチェックしません。

7 監査の構成を終了するには、必要な他のCOM+オブジェクトまたはオブジェクトカテゴリルールを定義して、監査のターゲットサーバー、スケジュール、通知を設定します。

8 監査を保存するには、[**ファイル**] メニューから [**保存**] を選択します。監査をポリシーとして保存することもできます。詳細については、監査またはスナップショット仕様の監査ポリシーとしての保存 (85ページ) を参照してください。

9 監査を実行するには、[**アクション**] メニューから [**監査の実行**] を選択します。監査の実行の詳細については、監査ポリシーの作成 (81ページ) を参照してください。

カスタムスクリプトルールの構成

カスタムスクリプトルールを使用すると、独自のスクリプト (バッチ、Python、Visual Basic) を定義して、監査、監査ポリシー、またはスナップショット仕様で使用する値を取得して比較することができます。また、独自の修復スクリプトを作成することもできます。

カスタムスクリプトルールを構成する際には、ターゲット値、すなわちスクリプトが返すことを期待される値を指定します。監査はこの情報を、次の方法に基づいて収集できます。

- **比較ベースの監査**: ソースサーバーに対してスクリプトを実行します。スクリプトの戻り値 (終了コードまたは標準出力) が、ターゲットサーバーに対する実行後のスクリプトの出力と比較されます。このオプションは、「ソース」と呼ばれます。
- **値ベースの監査**: 独自の値を指定します。この値は、ターゲットサーバーに対する実行後のスクリプトの出力と比較されます。スクリプトの期待される結果がわかっている場合には、この値を手動で入力します。または、ソースサーバーに対してスクリプトを実行して、その戻り値を使用することもできます。監査の実行時には、ターゲットサーバーに対する実行後にスクリプトが返した結果とこの値が比較されます。このオプションは、「値」と呼ばれます。

監査に対しては、修復スクリプトを構成することもできます。これは、ルールと、ターゲットサーバーに対する実行後にスクリプトが返した値との間に差異が見つかった場合に使用されます。

スナップショットの場合、スクリプトの結果は、ターゲットサーバーに対して(ルール詳細での定義に従って)スクリプトを実行することによって生成され、スナップショットに取得されます。スナップショット仕様をセットアップする場合も、修復スクリプトを追加することができます。このタイプのスクリプトは、ターゲットサーバーに対する修復を行うために使用できます。スナップショットのターゲットサーバーに対する修復スクリプトは、[スナップショット]ウィンドウから個々のサーバーに対して実行できます。

カスタムスクリプトルールを構成するには、次の手順を実行します。

1 監査の作成 (19ページ) の方法のいずれかで、新しい監査を作成します(このルールをスナップショット仕様に対して作成する場合は、スナップショット仕様の作成 (115ページ) を参照してください)。

2 監査ソースを選択します。サーバー、スナップショット、スナップショット仕様、またはソースなしが選択できます(アプリケーション構成、Windowsユーザーおよびグループなど、一部の監査ルールにはソースが必要です)。

3 スクリプトを作成して監査ルールを定義するには、次のオプションが選択できます。

ソース

- **ルール**: **[ルールの追加]** をクリックして、新しいカスタムスクリプトルールを追加します。
- **上に移動**: **[上に移動]** をクリックして、選択した監査ルールを上に移動し、カスタムスクリプト監査ルールの実行順序を指定します。監査ルールは、指定した順序で保存されます。この順序は、監査または監査ポリシーを開いたときに表示されます。
- **下に移動**: **[下に移動]** をクリックして、選択した監査ルールを下に移動し、カスタムスクリプト監査ルールの実行順序を指定します。監査ルールは、指定した順序で保存されます。この順序は、監査または監査ポリシーを開いたときに表示されます。

ルール詳細

- **名前**: スクリプトの名前を入力します。
- **スクリプトのタイプ**: バッチ、Python、PowerShell、Visual Basic (VBS) の中から選択します。
- **スクリプト**: スクリプトの内容をここに入力するか、コピーして貼り付けます。または、**[スクリプトのインポート]** をクリックして、ローカルドライブからスクリプトをインポートします。

成功条件

- **出力**: 終了コードまたは標準出力。
- **演算子**: 演算子を選択します。等しい (=)、等しくない (<>)、小さい (<)、大きい (>) などが使用できます。
- **参照**: スクリプト出力のソースを選択します。
- **ソース**: このオプションを選択すると、監査の実行時にソースに対してスクリプトが実行され、スクリプトが要求する値が取得されます。得られた値は、ターゲットサーバーに対して実行されたスクリプトから取得された値と比較されます。

  スナップショット仕様に対してこのオプションを選択した場合、スクリプトはターゲットに対して実行され、スクリプト実行の結果がスナップショット (結果) に取得されます。

  監査のソースがスナップショットの場合、カスタムスクリプトルールはスナップショット仕様に構成されているカスタムスクリプト定義を使用します。
- **値**: 独自の値を入力します。このオプションは、入力した値を使用して、ターゲットサーバーに対する実行後にスクリプトから返された値と比較します。このオプションを使用した場合、監査の実行時にスクリプトはソースサーバーに対して実行されません。ソースサーバーからのスクリプト出力をただちに取得するには、  アイコンをクリックします。返された値はテキストボックスに表示され、そのまま使用することも、必要に応じて編集することもできます。

監査のソースがスナップショットの場合、カスタムスクリプトルールはスナップショット仕様に構成されているカスタムスクリプト定義を使用します。

- **サーバー属性**: このオプションを選択すると、ソースサーバーのサーバー属性が、ターゲットサーバーに対して実行されたスクリプトの出力と比較されます。
- **カスタム属性**: このオプションを選択すると、ターゲットサーバーのカスタム属性が、ターゲットサーバーに対して実行されたスクリプトの出力と比較されます。このオプションに使用するカスタム属性は、監査で選択されたソースサーバーから得られます。

  ルール定義に対してここでカスタム属性を選択した場合、このカスタム属性がターゲットサーバー上に存在しないと、このルールの監査は失敗します。

  監査のソースを選択しない場合、このリストは空になります。

修復

- **スクリプトのタイプ**: バッチ、Python、PowerShell、Visual Basic (VBS) の中から選択します。
- **スクリプト**: スクリプトの内容をここに入力するか、コピーして貼り付けます。または、[**スクリプトのインポート**] をクリックして、ローカルドライブからスクリプトをインポートします。

4 (オプション) 監査の比較が失敗したときに実行する修復スクリプトを追加することができます。修復は自動的には適用されません。修復スクリプトは、監査の実行後に監査結果から実行する必要があります。

スナップショットの場合、ここで定義した修復スクリプトは、個々のターゲットサーバーに対して実行できます。修復の実行順序は独立には指定されません。選択された非コンプライアンスルールの修復は、監査または監査ポリシーに定義されているのと同じ順序で実行されます。たとえば、監査ポリシーに10個のルールがあり、ルール2、4、6、8が非コンプライアンスで、ルール4と8が修復対象として選択されている場合、ルール4の修復スクリプトが先に実行され、次にルール8の修復スクリプトが実行されます。

5 監査の構成を終了するには、監査のターゲットサーバー、スケジュール、通知を設定します。

6 監査を保存するには、[**ファイル**] メニューから [**保存**] を選択します。監査をポリシーとして保存することもできます。詳細については、監査またはスナップショット仕様の監査ポリシーとしての保存 (85ページ) を参照してください。

7 監査を実行するには、[**アクション**] メニューから [**監査の実行**] を選択します。監査の実行の詳細については、監査ポリシーの作成 (81ページ) を参照してください。

カスタムスクリプトの例

次の例は、Windowsユーザーアカウントを有効にし、ユーザーのパスワードを設定するように設計された、カスタムVBスクリプトルールです。このスクリプトは、Windows NT 4.0より後のWindows OSバージョンのみで動作します。Windows NT 4.0 でユーザーアカウントを有効にし、パスワードを設定するには、必要な操作を手動で実行する必要があります。

```
strComputer = "."
strAccountName = "red2"
Set objUser = GetObject("WinNT://"& strComputer & "/" & strAccountName )
objUser.AccountDisabled = False
objUser.SetPassword "AiH345^hjq"
objUser.SetInfo
```

検出されたソフトウェアルールの構成

検出されたソフトウェアルールは、Windows および UNIX 管理対象サーバーに適用する署名ベースのソフトウェア検出メカニズムであり、SA の管理対象ではないアプリケーションとソフトウェアの監査とスナップショット取得を行います。検出されたソフトウェアルールでは、次のことができます。

- 現在SAで管理されていない未登録のソフトウェアを検出します。
- OS に登録されたアプリケーションの一部としてインストールされていないソフトウェアまたはカスタム作成されたソフトウェアのインベントリを作成します。
- サーバーで検出されたソフトウェアのスナップショットを作成し、スナップショットを基準とする監査を定期的に実行できます。
- 内製またはカスタム作成のソフトウェアを追跡できます。

検出されたソフトウェアルールを構成するには、次の手順を実行します。

1 監査の作成 (19ページ) のいずれかの方法で、新しい監査を作成します (このルールをスナップショット仕様に対して作成する場合は、スナップショット仕様の作成 (115ページ) を参照してください)。

2 監査ソースを選択します。サーバー、スナップショット、スナップショット仕様、またはソースなしが選択できます。

3 [監査] ウィンドウのビューペインで、[ルール] > [検出されたソフトウェア] を選択します。

4 [監査] ウィンドウの内容ペインで、[監査に対して利用可能] セクションの [ソフトウェア] アイコンを展開します。監査またはスナップショットのソースを選択してある場合、初めてルールをロードするときには多少時間がかかることがあります。

5 リストから要素を選択し、右矢印ボタンをクリックして、ルールオブジェクトを [監査に対して選択済み] セクションに移動します。これにより、その要素に対するルールを作成できます。

6 ルールに構成するチェックのそれぞれに対して、[監査] ウィンドウの下部で、次のルール条件タイプのうち1つを選択できます。

   - **プロパティ値**: ターゲットオブジェクトの個々のプロパティをチェックする値ベースのチェック。このタイプのチェックの場合、各オブジェクトに対して、オブジェクトに関連するプロパティを定義する式を、ルールウィンドウ下部のドロップダウンリストを使用して作成する必要があります。オブジェクトのタイプに応じて固有の演算子を指定できます。使用できるのは、文字列、数値 (整数または浮動小数点数)、ブール値 (真と偽の値の比較)、日付 (時刻でなく日付の比較)、配列です。
   - **ソースと同等**: ソース上のオブジェクトとターゲットサーバーとの1対1の比較を行う比較チェック。このタイプのチェックでは、ソースサーバーとターゲットサーバーの両方から選択された各プロパティが正確に一致する場合のみ、オブジェクトはコンプライアンス状態と見なされます。
   - **非存在**: オブジェクトの非存在チェックを行い、ターゲットサーバーにオブジェクトが存在するかどうかを判定するルール。オブジェクトがターゲットサーバーに存在する場合、ユーザーまたはグループルールが非コンプライアンス状態にあります。実行時に、ソースサーバーが存在しても、このサーバーに対する照会は行われません。また、ワイルドカードルールオブジェクトを選択すると、ターゲットサーバーにのみ適用されます。

7 ワイルドカードルールオブジェクト  を選択することにより、ワイルドカード検索に基づいてルールを構成することもできます。このオブジェクトを選択した場合、ウィンドウ下部のルール構成セクションに [名前] フィールドが表示され、ターゲットサーバーで検索される名前 (プライマリキー) を入力できます。

   たとえば、単に*と入力すると、ターゲット上のすべてのものに一致します。P*は大文字のPで始まるすべてのオブジェクトに一致し、*Pは大文字のPで終わるすべての要素に一致します。

   名前またはワイルドカード文字列を入力した後、ステップ 6 と同じ手順でルールパラメーターを構成できます。

   ワイルドカードを使用する場合、一致するオブジェクトはすべてルール構成に制約されることに注意してください。このタイプの監査ルールは、見つかったすべてのオブジェクトがルールパラメーターに一致する場合にコンプライアンス状態と見なされます。

8 監査の構成を終了するには、監査のターゲットサーバー、ルールの例外、スケジュール、通知を設定します。

9 監査を保存するには、[**ファイル**] メニューから [**保存**] を選択します。監査をポリシーとして保存することもできます。これにより、監査で作成したルールセットが他のユーザーからアクセスできるようになります。詳細については、監査またはスナップショット仕様の監査ポリシーとしての保存 (85ページ) を参照してください。

10 監査を実行するには、[**アクション**] メニューから [**監査の実行**] を選択します。監査の実行の詳細については、監査の実行 (21ページ) を参照してください。

ファイルルールの構成

ファイルルールでは、次のオプションを指定することにより、ターゲットサーバー上のファイルとディレクトリを監査して比較できます。

- **ディレクトリ名**: 選択したファイルまたはディレクトリの絶対パス。

   (オプション) 環境変数 (`${varName}`) またはカスタム属性 (`@varName@`) への参照を追加することもできます。SA/カスタム属性でのファイル名のパラメーター化 (75ページ) およびパス名の環境変数 (77ページ) を参照してください。

- **範囲**: デフォルトの範囲はディレクトリ＋ファイルです。[ディレクトリオプション] ペインの [範囲の例] の図に、選択したオプションに基づく範囲の使用法の階層が表示されます。この図には除外は表示されません。[**除外の設定**] をクリックすると、[含める対象/除外する対象の選択] ウィンドウに除外が表示されます。

  ディレクトリ構造を再帰的にたどる: 監査対象として選択したファイルシステムフォルダーのすべてのサブディレクトリの内容を含めます。たとえば、ディレクトリ＋ファイル (再帰的)、ファイルのみ (再帰的)、ディレクトリのみ (再帰的) のようになります。

  ディレクトリを含む: 監査に含めるか除外するファイルシステム内のディレクトリを指定します。ファイルの含める/除外ルール (71ページ) を参照してください。

  ファイルを含む: 監査に含めるか除外するファイルシステム内のファイルを指定します。ファイルの含める/除外ルール (71ページ) を参照してください。

  次のリストは、8つの一般的な使用法を、優先度の順番に示します。この後の範囲の一般的な使用法と図を参照してください。

  範囲の使用法1: ディレクトリ＋ファイル (再帰的) (48ページ)

  範囲の使用法2: ディレクトリ＋ファイル (デフォルト) (48ページ)

  範囲の使用法3: ファイルのみ (48ページ)

  範囲の使用法4: ファイル (再帰的) (49ページ)

  範囲の使用法5: ディレクトリ (再帰的) (49ページ)

  範囲の使用法6: ディレクトリのみ (49ページ)

  範囲の使用法7: 複数のディレクトリのみ (50ページ)

  範囲の使用法8: 再帰的のみ (50ページ)

- **差異のチェック**:

  プロパティによる

  チェックサム: ディレクトリ内の選択したファイルの内容に対してチェックサムを実行します。ファイルの内容全体を監査するか (フル)、またはファイルの最初の1MBだけを監査するか (部分的) を選択できます。

  更新日: ファイルまたはフォルダーの比較にファイルの更新日を使用して監査します。

  ユーザーとグループのアクセス権 (UNIX のみ): ファイルとディレクトリに関連するユーザーとグループのアクセス権を監査します。

Windows ACL (Windowsのみ)**:** ファイルとディレクトリのWindowsアクセス制御リスト (ACL) を監査します。

注: ファイルルールでACLをチェックしていて、ユーザーとグループのACLがターゲットに存在しない場合、監査と修復のプロセスが完了した後に、一時的なユーザーとグループが作成され、不明な名前が割り当てられます。次に監査を実行すると、このユーザーとグループが不明な名前で表示されます。修復の詳細については、監査結果 (86ページ) を参照してください。

バージョン番号: 一部の Windows ファイルタイプ (.exe、.dll、.ocx、.olb、.scr、.rll、.sys、.drv、.acm) に対しては、ファイルの作成者がファイルバージョンと製品バージョンを設定できます。このオプションは、これらのバージョン番号を比較します。差異がある場合、ルールは非コンプライアンス状態と見なされ、ターゲットファイルの実際の値を監査結果に表示することができます。

注: 上記の拡張子のファイルがすべて製品バージョンまたはファイルバージョン属性を持つわけではありません。

ファイルを修復用にアーカイブ: ファイル全体をアーカイブします。このオプションを使用すると、ルールに指定した差違に基づいて、指定したファイルの差異を監査でチェックできます。このオプションは、ルールとターゲットファイルとの間のファイルの差異を表示して修復したい場合に使用します。差異が見つかった場合、修復を行うと、ソースファイルがターゲットサーバーにコピーされ、ターゲットファイルがソースに置き換えられます。

注: このオプションを使用すると、比較するファイルのサイズと数によっては、SAコアのデータベースの必要ディスク容量が増加する可能性があります。

アプリケーション構成値セットによる: アプリケーション構成を使用して、ターゲットサーバー上の構成ファイルを評価します。このオプション ([**詳細関連付け設定**] を含む) では、構成テンプレートを使用して、ソース構成ファイルとターゲットサーバー上の構成ファイルの間の値の差異を比較できます。構成テンプレートによる監査でのファイルの比較 **(52ページ)** を参照してください。

- **修復サマリー**: 選択したプロパティが一致しない場合に、ソースからファイルとそのプロパティをコピーすることによって修復を行います。

範囲の一般的な使用法と図

次の例は、スコープの使用法のタイプごとのWindowsディレクトリオプションと、関連するファイルシステムの図を示します。Windowsでは、[**Windows ACL**] オプションが使用できます。Unixでは、[**ユーザーとグループのアクセス権**] オプションが使用できます。

- 範囲の使用法1: ディレクトリ＋ファイル (再帰的) (48ページ)
- 範囲の使用法2: ディレクトリ＋ファイル (デフォルト) (48ページ)
- 範囲の使用法3: ファイルのみ (48ページ)
- 範囲の使用法4: ファイル (再帰的) (49ページ)
- 範囲の使用法5: ディレクトリ (再帰的) (49ページ)
- 範囲の使用法6: ディレクトリのみ (49ページ)
- 範囲の使用法7: 複数のディレクトリのみ (50ページ)
- 範囲の使用法8: 再帰的のみ (50ページ)

図7は、ディレクトリ＋ファイル(再帰的)に必要なオプションの例です。

図7　　範囲の使用法1: ディレクトリ＋ファイル(再帰的)

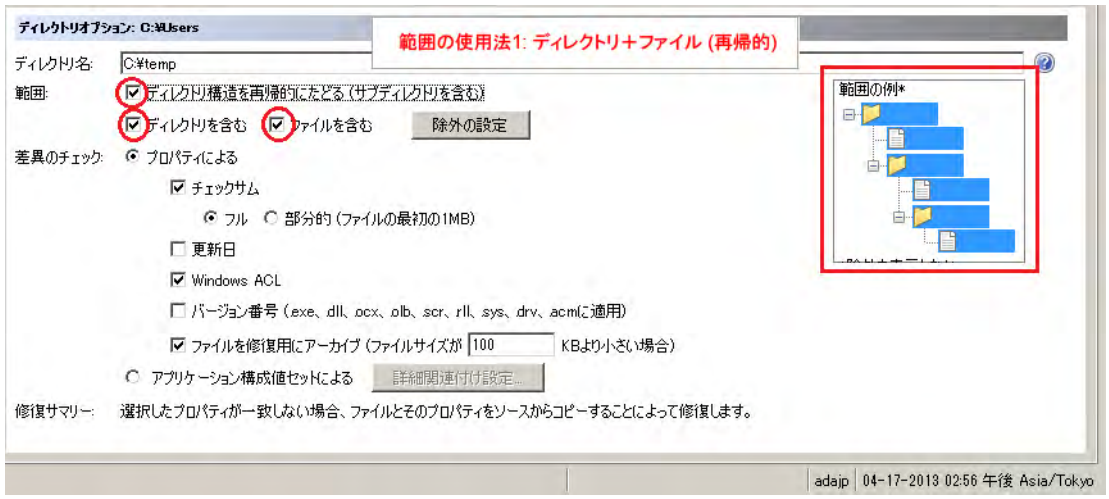


図8は、ディレクトリ＋ファイルに必要なオプションの例です。これらはデフォルトのオプションです。

図8　　範囲の使用法2: ディレクトリ＋ファイル(デフォルト)

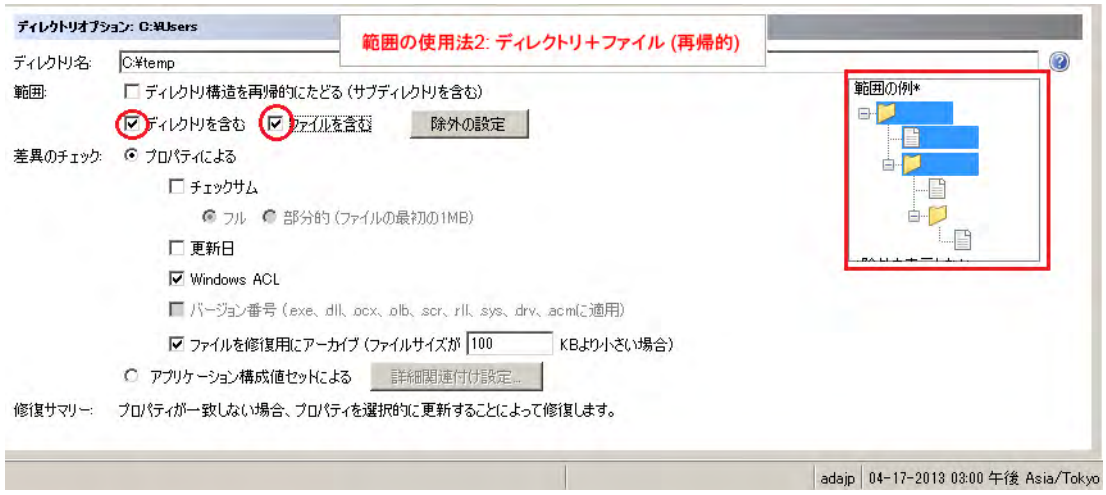


図9は、ファイルのみに必要なオプションの例です。

図9　　範囲の使用法3: ファイルのみ

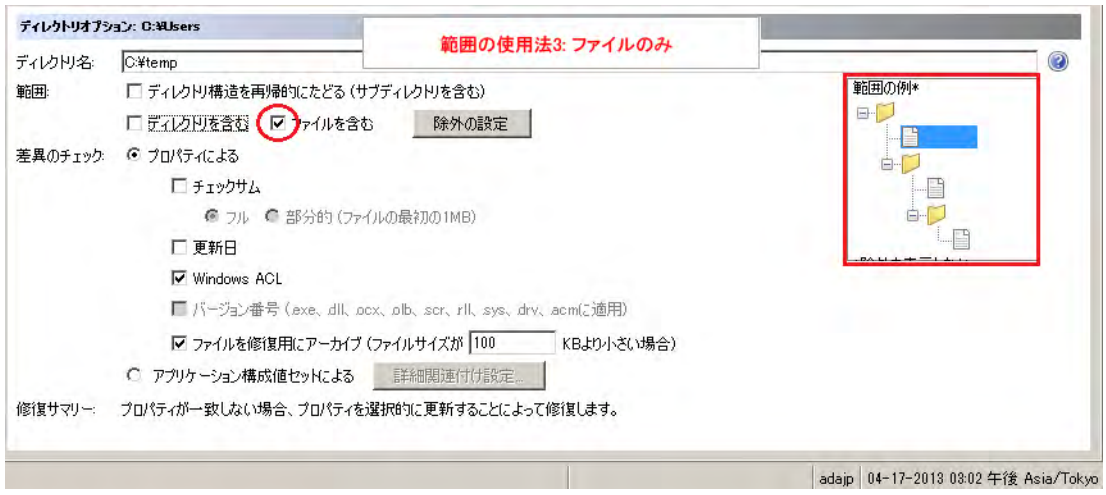


図10は、ファイル (再帰的) に必要なオプションの例です。

図10　　範囲の使用法4: ファイル (再帰的)

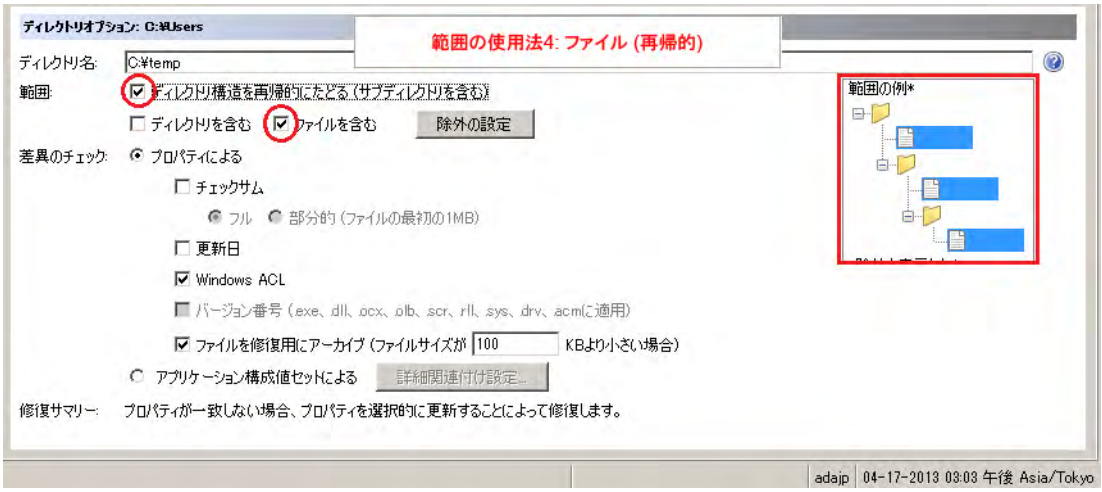


図11は、ディレクトリ (再帰的) に必要なオプションの例です。

図11　　範囲の使用法5: ディレクトリ (再帰的)

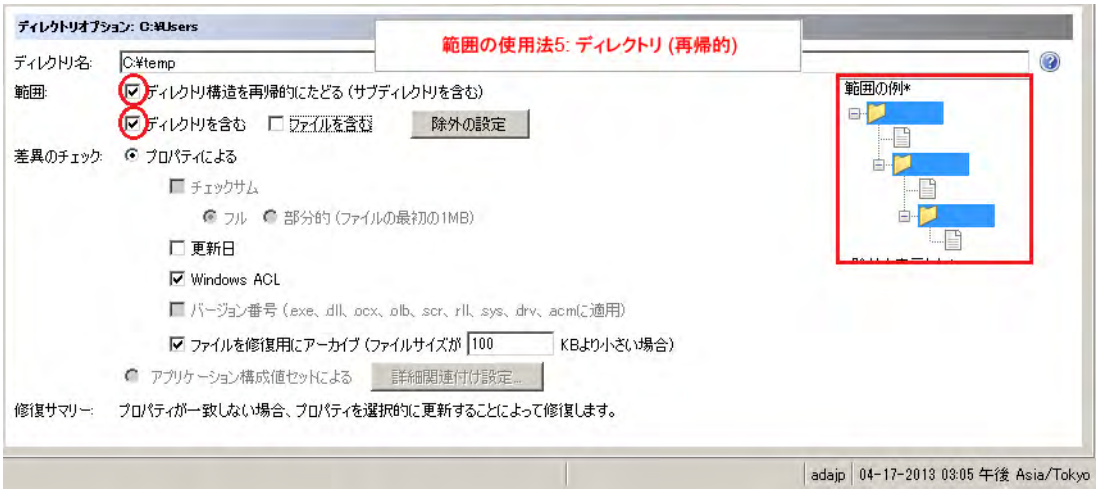


図12は、ディレクトリのみに必要なオプションの例です。

図12　　範囲の使用法6: ディレクトリのみ

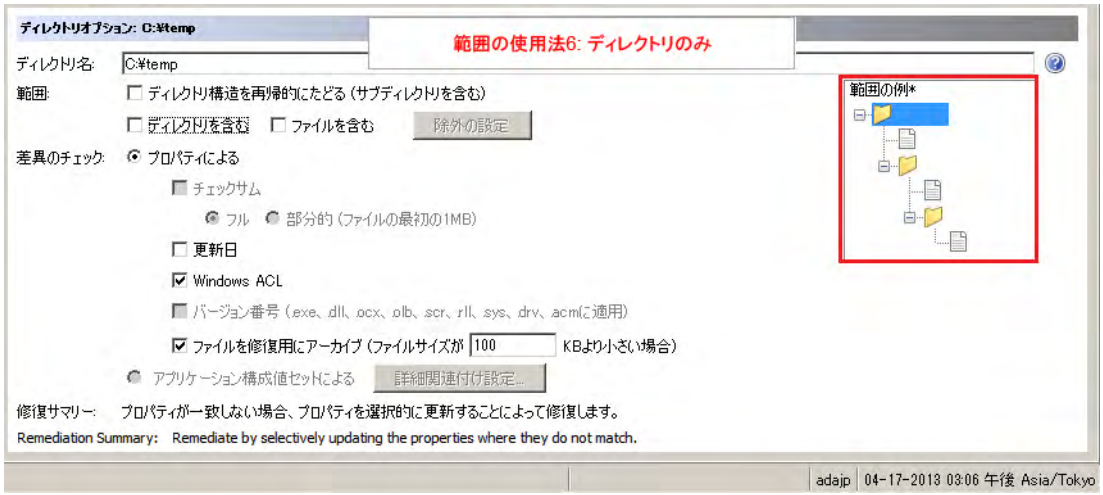


図13は、複数のディレクトリのみに必要なオプションの例です。

図13　　範囲の使用法7: 複数のディレクトリのみ

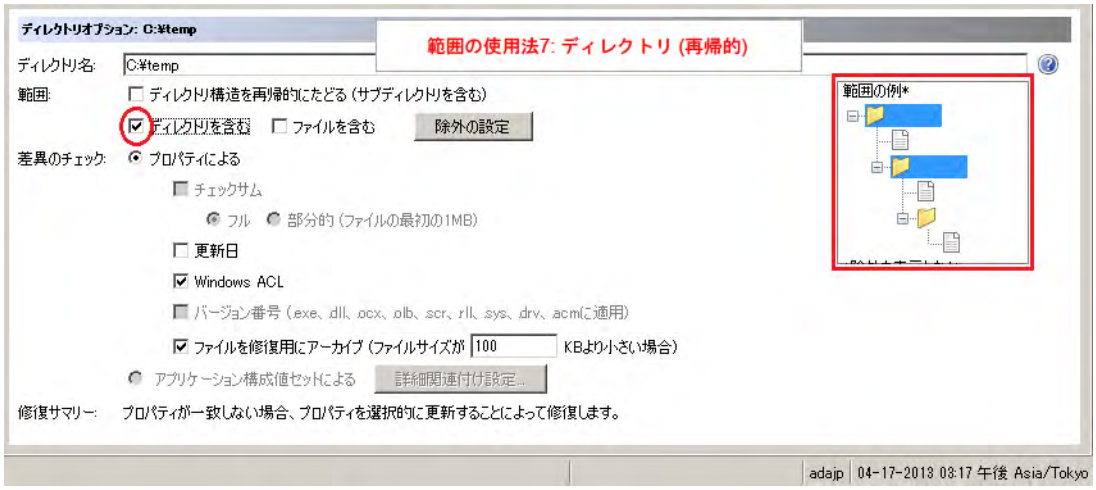
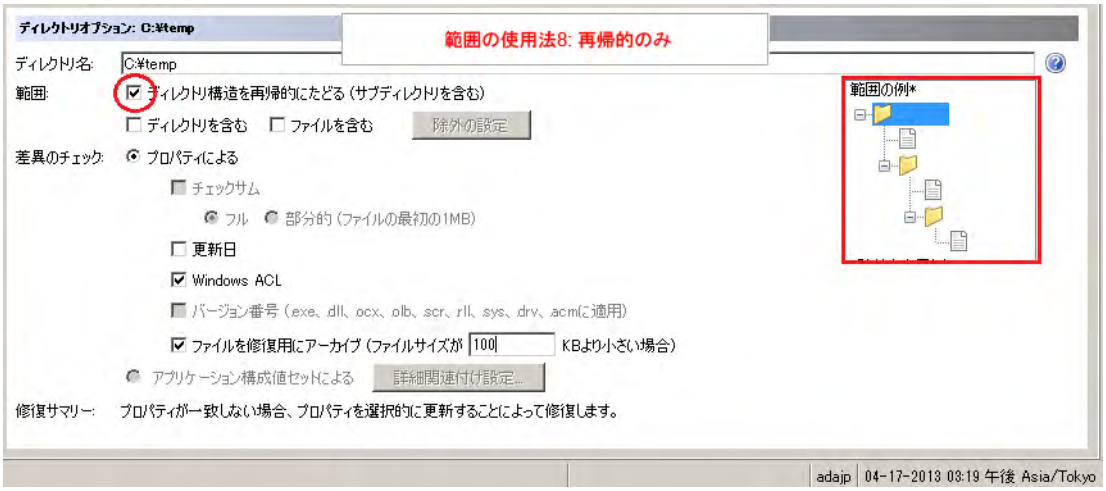


図14は、再帰的のみに必要なオプションの例です。

図14　　範囲の使用法8: 再帰的のみ



監査にルールを追加する方法

監査にルールを追加するには、いくつかの方法があります。

次の操作を実行できます。

- (推奨) 既存の監査ポリシーへのリンク。監査ポリシーの監査またはスナップショット仕様へのリンク (82ページ) および監査ポリシーのマスター監査ポリシーへのリンク (83ページ) を参照してください。
- 監査ポリシーのインポート。監査ポリシールールのインポート (84ページ) を参照してください。
- 監査内部でのルールの選択。

ファイルルールを構成するには、次の手順を実行します。

1. 監査の作成 (19ページ) のいずれかの方法で、新しい監査を作成します。このルールをスナップショット仕様に対して作成する場合は、スナップショット仕様の作成 (115ページ) を参照してください。
2. ターゲット値と比較する参照データのソースを指定します。

ベストプラクティス: ソースは、サーバーまたはそのアプリケーションの理想的な構成を表現するものにします。

a [監査] ウィンドウのビューペインで、[**ソース**] を選択します。

b [ソース] ペインで、ターゲット値と比較する参照データのソースを指定します。[**ソースなし**]、[**サーバー**]、[**スナップショット - すべてのターゲットに1つ**]、[**スナップショット仕様 - ターゲットごとの最新**] が選択できます。スナップショットを選択した場合、スナップショットで取得されたファイルを比較できます。一部の監査ルール (アプリケーション構成、Windowsユーザーおよびグループなど) には、ソースが必要です。

選択したソースに応じて、次のいずれかのウィンドウが表示されます。

[**サーバー**] を選択した場合、[サーバーの選択] ウィンドウが表示されます。

[**スナップショット - すべてのターゲットに1つ**] を選択した場合、[スナップショットの選択] ウィンドウが表示されます。

[**スナップショット仕様 - ターゲットごとの最新**] を選択した場合、[スナップショット仕様の選択] ウィンドウが表示されます。

c 選択して [**OK**] をクリックし、設定を保存して選択ウィンドウを閉じます。

3 ファイルルールを選択します。

a [監査] ウィンドウのビューペインで、[**ルール**] > [**ファイル**] を選択します。

(推奨) [ルール] 内容ペインで、 をクリックして [監査ポリシーの選択] ウィンドウを開きます。ポリシーを選択して [**OK**] をクリックします。

ベストプラクティス: この選択により、リンクされたルールを作成できます。これは既存の監査ポリシーへのリンクです。すなわち、ポリシーが変更されると、この監査ルールにも変更が反映されます。

または

b (オプション) リンクされないルールを作成するには、[**リンクされないルールを有効にする (定義済みの監査ポリシーにリンクしない)**] をチェックします。

[ルール] 内容ペインで、[**ルールのインポート**] をクリックして [監査ポリシーの選択] ウィンドウを開きます。ポリシーを選択して [**OK**] をクリックします。

または

c (オプション) 監査または監査ポリシーで、[**リンクされないルールを有効にする (定義済みの監査ポリシーにリンクしない)**] をチェックします。

をクリックして、[ファイルの選択] ウィンドウを開きます。ファイルシステムを展開して、ファイルまたはディレクトリを選択します。[**OK**] をクリックして、選択したルールを監査に追加します。

4 監査するファイルとディレクトリを選択します。

a [監査] ウィンドウのビューペインで、[**ルール**] > [**ファイル**] を選択します。

[ソースサーバー] 内容ペインで、 をクリックして [ファイルの選択] ウィンドウを開きます。

b [監査に対して利用可能] セクションで、トップレベルノードを展開し、ルールを適用するフォルダーまたはファイルを選択します。

c 選択して [**選択**] をクリックし、設定を保存して [ファイルの選択] ウィンドウを閉じます。

または

a [監査] ウィンドウのビューペインで、[**ルール**] > [**ファイル**] を選択します。

[ソースサーバー] 内容ペインでファイルまたはディレクトリを選択して、詳細ペインで [ファイルオプション] または [ディレクトリオプション] を変更します。

b (オプション) フォルダーの場合、ファイル/ディレクトリのワイルドカードオプションを選択して、監査に含めるか除外するファイルやディレクトリを指定できます。

c  をクリックして新しいルールを追加するか、 をクリックしてルールを削除します。ファイルとディレクトリの入力方法およびそれによる監査への影響の詳細については、ファイルの含める/除外ルール (71ページ) を参照してください。

5 (オプション) アプリケーション構成を使用して構成ファイルを比較する場合、[**アプリケーション構成値セットによる**] を選択し、[**詳細関連付け設定**] をクリックします。

[AppConfigファイル比較関連付け] ウィンドウの [AppConfigテンプレート] リストで、ソースとターゲットの構成ファイルの比較に使用するテンプレートを選択します。[関連付けられたファイル] セクションで、ソース構成ファイルのデフォルトのパスを使用するか、パスを編集します。  をクリックして、ターゲット上の構成ファイルと比較する別のソース構成ファイルのパスを追加します。

終わったら、[**OK**] をクリックします。

6 監査の構成を終了するには、監査のターゲットサーバー、スケジュール、通知を設定します。

7 監査を保存するには、[**ファイル**] メニューから [**保存**] を選択します。監査をポリシーとして保存することもできます。詳細については、監査またはスナップショット仕様の監査ポリシーとしての保存 (85ページ) を参照してください。

8 監査を実行するには、[**アクション**] メニューから [**監査の実行**] を選択します。監査の実行の詳細については、監査ポリシーの作成 (81ページ) を参照してください。

注: [更新] ボタンを使用して、[ファイルの選択] 画面を更新します。

構成テンプレートによる監査でのファイルの比較

ターゲットサーバー上のファイルを監査するもう1つの方法は、アプリケーション構成 (AppConfig) テンプレートに基づいてソースサーバーのファイルと比較することです。

構成テンプレートは、構成ファイルの構造をモデル化し、その内容と構成を決定します。監査のファイルルールで構成テンプレートを使用してファイルを比較した場合、監査では、ソースとターゲットの両方のファイルの内容が、構成テンプレートによってフィルターされた後で比較されます。このため、監査を実行してファイルを比較する際に、テンプレートに定義された値セットだけが比較の対象となります。

たとえば、複数のターゲットサーバー上の`/etc/passwd`ファイルを比較して、適切な値を持つことがわかっているゴールデンサーバー上の `/etc/passwd` ファイルに定義された値だけが含まれることを確認したいとします。構成ファイル比較機能を使用すれば、`/etc/passwd` ファイルをモデル化した構成テンプレート (`passwd.tpl`) を選択して、ゴールデンソースサーバーと監査のターゲットサーバーの両方にある実際の`passwd`ファイルに関連付けることができます。

関連付けを作成するには、テンプレートを選択し、ターゲットサーバー上のファイルのパス名を入力します。この機能で複数のファイルを比較することもできます。たとえば、比較対象の複数の構成ファイルが存在するディレクトリを選択して、構成テンプレートをそのディレクトリに関連付けることができます。

監査での構成ファイルの比較機能を使用するには、次の手順を実行します。

1 監査の作成 (19ページ) のいずれかの方法で、新しい監査を作成します。

2 ターゲット値と比較する参照データのソースを指定します。

ベストプラクティス: ソースは、サーバーまたはそのアプリケーションの理想的な構成を表現するものにします。

a [監査] ウィンドウのビューペインで、[**ソース**] を選択します。

b [ソース] ペインで、ターゲット値と比較する参照データのソースを指定します。[**ソースなし**]、[**サーバー**]、[**スナップショット - すべてのターゲットに1つ**]、[**スナップショット仕様 - ターゲットごとの最新**] が選択できます。スナップショットを選択した場合、スナップショットで取得されたファイルを比較できます。一部の監査ルール (アプリケーション構成、Windowsユーザーおよびグループなど) には、ソースが必要です。

選択したソースに応じて、次のいずれかのウィンドウが表示されます。

[**サーバー**] を選択した場合、[サーバーの選択] ウィンドウが表示されます。

[**スナップショット - すべてのターゲットに1つ**] を選択した場合、[スナップショットの選択] ウィンドウが表示されます。

[**スナップショット仕様 - ターゲットごとの最新**] を選択した場合、[スナップショット仕様の選択] ウィンドウが表示されます。

c 選択して [**OK**] をクリックし、設定を保存して選択ウィンドウを閉じます。

3 [監査] ウィンドウのビューペインで、[**ルール**] > [**ファイル**] を選択します。

4 [監査] ウィンドウの詳細ペインで、[**アプリケーション構成値セットによる**] を選択し、[**詳細関連付け設定**] をクリックします。

5 [AppConfigファイル比較関連付け] ウィンドウの [AppConfigテンプレート] リストで、ソースとターゲットの構成ファイルの比較に使用するテンプレートを選択します。[関連付けられたファイル] セクションで、ソース構成ファイルのデフォルトのパスを使用するか、パスを編集します。 をクリックして、ターゲット上の構成ファイルと比較する別のソース構成ファイルのパスを追加します。

6 [関連付けられたファイル] セクションで、ソースサーバーとターゲットサーバー上の実際のソースおよびターゲット構成ファイルが存在する場所のパス名を入力します。

注: 構成テンプレートと比較するファイルは、すべて同じディレクトリに存在する必要があります。

7 (オプション) テンプレートに対して複数の関連付けを行う場合は、 をクリックして別のディレクトリを追加します。追加したすべてのディレクトリが、[AppConfigテンプレート] セクションで選択したテンプレートに適用されます。このウィンドウでは必要な数だけの関連付けを行うことができます。

8 終わったら、[**OK**] をクリックします。

9 監査の構成を終了するには、監査のターゲットサーバー、スケジュール、通知を設定します。

10 監査を保存するには、[**ファイル**] メニューから [**保存**] を選択します。監査をポリシーとして保存することもできます。詳細については、監査の監査ポリシーとしての保存 (82ページ) を参照してください。

11 監査を実行するには、[**アクション**] メニューから [**監査の実行**] を選択します。監査の実行の詳細については、監査ポリシーの作成 (81ページ) を参照してください。

ハードウェアルールの構成

ハードウェアルールを構成すると、サーバーのハードウェアに関する次の情報を監査できます。

- **インタフェース**: サーバーのデュプレックスの不一致とすべてのネットワークインタフェースを比較します。
- **CPU**: ターゲットサーバーのCPUのタイプと仕様を比較します。
- **メモリ**: ターゲットサーバーのメモリを比較します。
- **ストレージ**: ターゲットサーバーのストレージ容量を比較します。

- **インタフェース**: デバイスにアタッチされたすべてのネットワークインタフェースを比較します。

最近SAエージェントがインストールされたサーバー上でハードウェアルールの監査またはスナップショット取得を実行する場合、モデルリポジトリにハードウェアが完全に登録されていないために、正確なハードウェア情報の監査やスナップショット取得ができない可能性があります(SAエージェントによるハードウェアの登録は、通常エージェントのインストールから24時間以内に行われます)。不明な場合は、SA管理者または、SAエージェントをサーバーにインストールした担当者にお問い合わせください。サーバーのハードウェアを手動で登録する手順については、『SAユーザーガイド: Server Automation』を参照してください。

ハードウェアルールを構成するには、次の手順を実行します。

1. 監査の作成 (19ページ) に示す方法のいずれかで、新しい監査を作成します(このルールをスナップショット仕様に対して作成する場合は、スナップショット仕様の作成 (115ページ) を参照してください)。
2. 監査ソースを選択します。サーバー、スナップショット、スナップショット仕様、またはソースなしが選択できます。(アプリケーション構成、Windowsユーザーおよびグループなど、一部の監査ルールにはソースが必要です)。
3. [監査] ウィンドウのビューペインで、[ルール] > [ハードウェア] を選択します。
4. [監査] ウィンドウの内容ペインで、[監査に対して利用可能] セクションのトップレベルノードを展開して、ルールを作成するハードウェアカテゴリを選択します。
5. 右矢印ボタンをクリックして、ハードウェアアイテムを [監査に対して選択済み] セクションに移動します。選択したすべてのアイテムが、ターゲットサーバーの監査またはスナップショット取得に用いられます。
6. 監査の構成を終了するには、監査のターゲットサーバー、スケジュール、通知を設定します。
7. 監査を保存するには、[**ファイル**] メニューから [**保存**] を選択します。監査をポリシーとして保存することもできます。詳細については、監査またはスナップショット仕様の監査ポリシーとしての保存 (85ページ) を参照してください。
8. 監査を実行するには、[**アクション**] メニューから [**監査の実行**] を選択します。監査の実行の詳細については、監査ポリシーの作成 (81ページ) を参照してください。

IISメタベースルールの構成

IISメタベース監査ルールを使用すると、IISメタベースオブジェクトおよびオブジェクトフォルダーを監査で比較できます。監査では、IISメタベースオブジェクトのID、名前、パス、属性などのプロパティ情報が取得されます。

メタベースルールでACLをチェックしていて、ユーザーとグループのACLが存在しない場合、監査が実行されて修復が行われた後に、ターゲット上にユーザーとグループが存在しなければ、一時的なユーザーとグループが不明な名前で作成されます。次に監査を実行すると、ソースユーザー以外の不明な名前が表示されます。

また、ソースサーバーからIISメタベースルールを作成していて、ルールで選択したメタベースオブジェクトが親メタベースオブジェクトから値を継承している場合、監査の実行後に差異が表示されます。たとえば、修復を1回実行してその後に監査を再実行した場合、ソースキーが継承されておらず、属性がターゲットサーバー上での作成時にIEDを持っていると、オブジェクトは親キーの継承に基づいて作成されます。監査を再実行すると、結果ではIEDがオブジェクトの属性の差異として表示されます。

修復の詳細については、監査結果 (86ページ) を参照してください。

Windows Server 2008サーバー上でMicrosoft IIS 7.0を監査する場合は、監査でIIS 7.0ルールを作成して構成します。IIS 7.0ルールの構成 (56ページ) を参照してください。

IISメタベースルールを構成するには、次の手順を実行します。

1. 監査の作成 (19ページ) に示す方法のいずれかで、新しい監査を作成します(このルールをスナップショット仕様に対して作成する場合は、スナップショット仕様の作成 (115ページ) を参照してください)。
2. 監査ソースを選択します。サーバー、スナップショット、スナップショット仕様、またはソースなしが選択できます。(アプリケーション構成、Windowsユーザーおよびグループなど、一部の監査ルールにはソースが必要です)。
3. [監査] ウィンドウのビューペインで、[**ルール**] > [**IISメタベース**] を選択します。
4. [監査] ウィンドウの内容ペインで、[監査に対して利用可能] セクションのトップレベルノードを展開して、ルールを作成するIISメタベースフォルダーまたはオブジェクトを選択します (ルールに対して任意のメタベースフォルダーまたはオブジェクトを選択できますが、ルートフォルダーをルールとして使用するように選択することはできません)。
5. 右矢印ボタンをクリックして、フォルダーまたはオブジェクトを [監査に対して選択済み] セクションに移動します。選択したすべてのアイテムが、ターゲットサーバーの監査またはスナップショット取得に用いられます。
6. 監査の構成を終了するには、監査のターゲットサーバー、スケジュール、通知を設定します。
7. 監査を保存するには、[**ファイル**] メニューから [**保存**] を選択します。監査をポリシーとして保存することもできます。詳細については、監査またはスナップショット仕様の監査ポリシーとしての保存 (85ページ) を参照してください。
8. 監査を実行するには、[**アクション**] メニューから [**監査の実行**] を選択します。監査の実行の詳細については、監査ポリシーの作成 (81ページ) を参照してください。

IISルールの構成

Microsoft Internet Information Serverルールを使用すると、WindowsサーバーのIISに関するリアルタイム情報を監査に使用できます。たとえば、サーバー名、サーバータイプ、サーバー状態、ログファイルのパス、ドキュメントファイルのパスなどです。

Internet Information Serverルールを構成するには、次の手順を実行します。

1. 監査の作成 (19ページ) のいずれかの方法で、新しい監査を作成します。(このルールをスナップショット仕様に対して作成する場合は、スナップショット仕様の作成 (115ページ) を参照してください)。
2. 監査ソースを選択します。サーバー、スナップショット、スナップショット仕様、またはソースなしが選択できます。(アプリケーション構成、Windowsユーザーおよびグループなど、一部の監査ルールにはソースが必要です)。
3. [監査] ウィンドウのビューペインで、[ルール] > [Internet Information Server] を選択します。
4. [監査] ウィンドウの内容ペインで、[監査に対して利用可能] セクションのトップレベルノードを展開して、ルールを作成する元になるInternet Information Serverルールを選択します。
5. 右矢印ボタンをクリックして、ルールオブジェクトを［監査に対して選択済み］セクションに移動します。構成したすべてのInternet Information Serverルールが、ターゲットサーバーまたはスナップショット仕様で監査されます。
6. 各ルールに対して、次のいずれかのチェックタイプを選択します。
   - **プロパティ値**: ターゲットオブジェクトの個々のプロパティをチェックする値ベースのチェック。このタイプのチェックの場合、各オブジェクトに対して、オブジェクトに関連するプロパティを定義する式を、ルールウィンドウ下部のドロップダウンリストを使用して作成する必要があります。オブジェクトのタイプに応じて固有の演算子を指定できます。使用できるのは、文字列、数値 (整数または浮動小数点数)、ブール値 (真と偽の値の比較)、日付 (時刻でなく日付の比較)、配列です。

- **ソースと同等**: ソース上のオブジェクトとターゲットサーバーとの1対1の比較を行う比較チェック。このタイプのチェックでは、ソースサーバーとターゲットサーバーの両方から選択された各プロパティが正確に一致する場合のみ、オブジェクトはコンプライアンス状態と見なされます。
- **非存在:** オブジェクトの非存在チェックを行い、ターゲットサーバーにオブジェクトが存在するかどうかを判定するルール。オブジェクトがターゲットサーバーに存在する場合、ユーザーまたはグループルールが非コンプライアンス状態にあります。実行時に、ソースサーバーが存在しても、このサーバーに対する照会は行われません。また、ワイルドカードルールオブジェクトを選択すると、ターゲットサーバーにのみ適用されます。

7 ワイルドカードルールオブジェクト  を選択することにより、ワイルドカード検索に基づいてルールを構成することもできます。このオブジェクトを選択した場合、ウィンドウ下部のルール構成セクションに[名前]フィールドが表示され、ターゲットサーバーで検索される名前(プライマリキー)を入力できます。

たとえば、単に*と入力すると、ターゲット上のすべてのものに一致します。P*は大文字のPで始まるすべてのオブジェクトに一致し、*Pは大文字のPで終わるすべての要素に一致します。

名前またはワイルドカード文字列を入力した後、ステップ6と同じ手順でルールパラメーターを構成できます。

ワイルドカードを使用する場合、一致するオブジェクトはすべてルール構成に制約されることに注意してください。このタイプの監査ルールは、見つかったすべてのオブジェクトがルールパラメーターに一致する場合にコンプライアンス状態と見なされます。

8 監査の構成を終了するには、監査のターゲットサーバー、ルールの例外、スケジュール、通知を設定します。

9 監査を保存するには、[**ファイル**]メニューから[**保存**]を選択します。監査をポリシーとして保存することもできます。監査またはスナップショット仕様の監査ポリシーとしての保存 (85ページ) を参照してください。

10 監査を実行するには、[**アクション**]メニューから[**監査の実行**]を選択します。監査ポリシーの作成 (81ページ) を参照してください。

IIS 7.0ルールの構成

SA 9.10では、Windows Server 2008上で動作しているMicrosoft IIS 7.0に対する監査およびスナップショット仕様ルールを作成できます。IIS 7.0のアプリケーションプール、Webサイト、機能を展開して参照し、監査またはスナップショット仕様に追加して、組織のコンプライアンス標準に適合するかどうかを判定できます。監査またはスナップショットの実行後に結果を表示し、違反があれば修復できます(いくつか例外があります)。

たとえば、IIS 7.0を実行しているいくつかのWindows Server 2008サーバーを監査して、すべてのサーバーで匿名認証が有効になっていることを確認できます。

このコンプライアンスチェックを実行するには、匿名認証が有効になっているWindows Server 2008サーバーを監査のソースサーバーとして選択します。その後、監査ルールを構成して、監査のターゲットとなるすべてのサーバーで匿名認証が有効であることをチェックします。

監査を実行すると(定期的に実行するようにスケジュールすることも可能)、ルールはターゲットサーバーをチェックし、匿名認証が有効になっていないサーバーがあるかどうかを検出します。違反が見つかった場合、該当するサーバーを修復して、IIS 7.0の匿名認証を有効にすることができます。

このリリースでは、IIS 7.0監査ルールでISAPIフィルターを修復することはできません。

IIS 7.0ルールを構成するには、次の手順を実行します。

1 監査の作成 (19ページ) のいずれかの方法で、新しい監査を作成します(このルールをスナップショット仕様に対して作成する場合は、スナップショット仕様の作成 (115ページ) を参照してください)。

2 監査ソースを選択します。サーバー、スナップショット、スナップショット仕様、またはソースなしが選択できます。

一部の監査ルール (アプリケーション構成、Windowsユーザーおよびグループなど) には、ルールの基礎となるソースサーバーが必要です。また、具体的なルールと基準の中にも、IIS 7.0 の匿名認証のチェックのように、ソースサーバーの選択が必要なものがあります。ソースサーバーを選択しない場合、ルールの具体性が制限されます。

3 [監査] ウィンドウのビューペインで、[**ルール**] > [**IIS 7.0**] を選択します。

4 [監査] ウィンドウの内容ペインの [監査に対して利用可能] セクションで、ルールを作成するIIS 7.0要素 (アプリケーションプール、サイト、機能など) の1つを展開します。該当する要素を初めてロードする場合は、多少時間がかかることがあります。

5 リストから要素を選択し、右矢印ボタンをクリックして、ルールオブジェクトを [監査に対して選択済み] セクションに移動します。これにより、その要素に対するルールを作成できます。たとえば、[認証] フォルダーを展開して [匿名認証] を選択し、右矢印ボタンをクリックして選択したアイテムを監査に追加します。

6 ルールのそれぞれに対して、[監査] ウィンドウの下部で、次のルール条件タイプのうち1つを選択します。

- **プロパティ値**: ターゲットオブジェクトの個々のプロパティをチェックする値ベースのチェック。このタイプのチェックの場合、各オブジェクトに対して、オブジェクトに関連するプロパティを定義する式を、ルールウィンドウ下部のドロップダウンリストを使用して作成する必要があります。オブジェクトのタイプに応じて固有の演算子を指定できます。使用できるのは、文字列、数値 (整数または浮動小数点数)、ブール値 (真と偽の値の比較)、日付 (時刻でなく日付の比較)、配列です。
- **ソースと同等**: ソース上のオブジェクトとターゲットサーバーとの1対1の比較を行う比較チェック。このタイプのチェックでは、ソースサーバーとターゲットサーバーの両方から選択された各プロパティが正確に一致する場合のみ、オブジェクトはコンプライアンス状態と見なされます。

  IIS 7.0 ルールの修復が可能なのは、監査に [ソースと同等] チェックがセットアップされている場合に限ります。
- **非存在**: オブジェクトの非存在チェックを行い、ターゲットサーバーにオブジェクトが存在するかどうかを判定するルール。オブジェクトがターゲットサーバーに存在する場合、ユーザーまたはグループルールが非コンプライアンス状態にあります。実行時に、ソースサーバーが存在しても、このサーバーに対する照会は行われません。また、ワイルドカードルールオブジェクトを選択すると、ターゲットサーバーにのみ適用されます。

たとえば、IIS 7.0 を実行しているターゲットサーバー (または複数のサーバー) で匿名認証が有効になっていることをチェックするには、[監査] ウィンドウの下部で次の値を選択します。

- プロパティ値
- ステータス
- =
- 有効

これは、各ターゲットサーバーの IIS 7.0 匿名認証が有効になっているかどうかを調べるように監査に指示します。

7 ワイルドカードルールオブジェクト  を選択することにより、ワイルドカード検索に基づいてルールを構成することもできます。このオブジェクトを選択した場合、ウィンドウ下部のルール構成セクションに [名前] フィールドが表示され、ターゲットサーバーで検索される名前 (プライマリキー) を入力できます。

たとえば、アスタリスク (*) を入力すると、ターゲット上のすべてのものに一致します。P*は大文字のPで始まるすべてのオブジェクトに一致し、*Pは大文字のPで終わるすべての要素に一致します。

名前またはワイルドカード文字列を入力した後、ステップ 6 と同じ手順でルールパラメーターを構成できます。

ワイルドカードを使用する場合、一致するオブジェクトはすべてルール構成に制約されることに注意してください。このタイプの監査ルールは、見つかったすべてのオブジェクトがルールパラメーターに一致する場合にコンプライアンス状態と見なされます。

8 監査の構成を終了するには、監査のターゲットサーバー、ルールの例外、スケジュール、通知を設定します。

9 監査を保存するには、[**ファイル**] メニューから [**保存**] を選択します。監査をポリシーとして保存することもできます。これにより、監査で作成したルールセットが他のユーザーからアクセスできるようになります。監査またはスナップショット仕様の監査ポリシーとしての保存 (85ページ) を参照してください。

10 監査を実行するには、[**アクション**] メニューから [**監査の実行**] を選択します。監査の実行 (21ページ) を参照してください。

ローカルセキュリティ設定ルールの構成

ローカルセキュリティ設定ルールでは、セキュリティ設定に関するリアルタイム情報を使用できます。たとえば、パスワードポリシー、監査ポリシー、ユーザー権限、セキュリティオプションなどです。

ローカルセキュリティ設定ルールを構成するには、次の手順を実行します。

1 監査の作成 (19ページ) のいずれかの方法で、新しい監査を作成します。(このルールをスナップショット仕様に対して作成する場合は、スナップショット仕様の作成 (115ページ) を参照してください)。

2 監査ソースを選択します。サーバー、スナップショット、スナップショット仕様、またはソースなしが選択できます。(アプリケーション構成、Windowsユーザーおよびグループなど、一部の監査ルールにはソースが必要です)。

3 [監査] ウィンドウのビューペインで、[**ルール**] > [**ローカルセキュリティ設定**] を選択します。

4 [監査] ウィンドウの内容ペインで、[監査に対して利用可能] セクションのトップレベルノードを展開して、ルールを作成する元になるInternet Information Serverルールを選択します。

5 右矢印ボタンをクリックして、ルールオブジェクトを［監査に対して選択済み］セクションに移動します。構成したすべてのInternet Information Serverルールが、ターゲットサーバーまたはスナップショット仕様で監査されます。

6 各ルールに対して、次のいずれかのチェックタイプを選択します。

- **プロパティ値**: ターゲットオブジェクトの個々のプロパティをチェックする値ベースのチェック。このタイプのチェックの場合、各オブジェクトに対して、オブジェクトに関連するプロパティを定義する式を、ルールウィンドウ下部のドロップダウンリストを使用して作成する必要があります。オブジェクトのタイプに応じて固有の演算子を指定できます。使用できるのは、文字列、数値 (整数または浮動小数点数)、ブール値 (真と偽の値の比較)、日付 (時刻でなく日付の比較)、配列です。
- **ソースと同等**: ソース上のオブジェクトとターゲットサーバーとの1対1の比較を行う比較チェック。このタイプのチェックでは、ソースサーバーとターゲットサーバーの両方から選択された各プロパティが正確に一致する場合のみ、オブジェクトはコンプライアンス状態と見なされます。
- **非存在:** オブジェクトの非存在のチェック、すなわちターゲットサーバー上にオブジェクトが存在しないことを確認します。ターゲットサーバー上にオブジェクトが存在する場合、ルールはコンプライアンス違反になります。たとえば、サーバーに特定のCOM+オブジェクトが含まれないことを確認できます。実行時に、ソースサーバーが存在しても、このサーバーに対する照会は行われません。また、ワイルドカードルールオブジェクトを選択すると、ターゲットサーバーにのみ適用されます。

7 ワイルドカードルールオブジェクト  を選択することにより、ワイルドカード検索に基づいてルールを構成することもできます。このオブジェクトを選択すると、ウィンドウ下部のルール構成セクションに、[名前] フィールドが表示されます。ターゲットサーバー上で検索される名前 (プライマリキー) を入力します。

たとえば、単に*と入力すると、ターゲット上のすべてのものに一致します。P*は大文字のPで始まるすべてのオブジェクトに一致し、*Pは大文字のPで終わるすべての要素に一致します。

名前またはワイルドカード文字列を入力した後、ステップ 6 と同じ手順でルールパラメーターを構成できます。

ワイルドカードを使用する場合、一致するオブジェクトはすべてルール構成に制約されることに注意してください。このタイプの監査ルールは、見つかったすべてのオブジェクトがルールパラメーターに一致する場合にコンプライアンス状態と見なされます。

8 監査の構成を終了するには、監査のターゲットサーバー、ルールの例外、スケジュール、通知を設定します。

9 監査を保存するには、[**ファイル**] メニューから [**保存**] を選択します。監査をポリシーとして保存することもできます。監査またはスナップショット仕様の監査ポリシーとしての保存 (85ページ) を参照してください。

10 監査を実行するには、[**アクション**] メニューから [**監査の実行**] を選択します。監査の実行 (21ページ) を参照してください。

登録済みソフトウェアルールの構成

登録済みソフトウェアルールを使用すると、ソースサーバー上に実際にインストールされているすべてのパッケージまたはパッチをルールの作成に使用できます。パッチとパッケージは、SAモデルリポジトリによる登録の有無に関係なく検出されます。

登録済みソフトウェアルールを構成するには、次の手順を実行します。

1 監査の作成 (19ページ) のいずれかの方法で、新しい監査を作成します。(このルールをスナップショット仕様に対して作成する場合は、スナップショット仕様の作成 (115ページ) を参照してください)。

2 監査ソースを選択します。サーバー、スナップショット、スナップショット仕様、またはソースなしが選択できます。(アプリケーション構成、Windowsユーザーおよびグループなど、一部の監査ルールにはソースが必要です)。

3 [監査] ウィンドウのビューペインで、[ルール] > [登録済みソフトウェア] を選択します。

4 [監査] ウィンドウの内容ペインで、[監査に対して利用可能] セクションのトップレベルノードを展開して、ルールを作成する元になるパッチまたはパッケージを選択します。

5 右矢印ボタンをクリックして、ルールオブジェクトを［監査に対して選択済み］セクションに移動します。構成したすべてのルールが、ターゲットサーバーまたはスナップショット仕様で監査されます。

6 各ルールに対して、次のいずれかのチェックタイプを選択します。

- **プロパティ値**: ターゲットオブジェクトの個々のプロパティをチェックする値ベースのチェック。このタイプのチェックの場合、各オブジェクトに対して、オブジェクトに関連するプロパティを定義する式を、ルールウィンドウ下部のドロップダウンリストを使用して作成する必要があります。オブジェクトのタイプに応じて固有の演算子を指定できます。使用できるのは、文字列、数値 (整数または浮動小数点数)、ブール値 (真と偽の値の比較)、日付 (時刻でなく日付の比較)、配列です。
- **ソースと同等**: ソース上のオブジェクトとターゲットサーバーとの 1 対 1 の比較を行う比較チェック。このタイプのチェックでは、ソースサーバーとターゲットサーバーの両方から選択された各プロパティが正確に一致する場合のみ、オブジェクトはコンプライアンス状態と見なされます。

- **非存在**: オブジェクトの非存在チェックを行い、ターゲットサーバーにオブジェクトが存在するかどうかを判定するルール。オブジェクトがターゲットサーバーに存在する場合、ユーザーまたはグループルールが非コンプライアンス状態にあります。実行時に、ソースサーバーが存在しても、このサーバーに対する照会は行われません。また、ワイルドカードルールオブジェクトを選択すると、ターゲットサーバーにのみ適用されます。

7 ワイルドカードルールオブジェクト  を選択することにより、ワイルドカード検索に基づいてルールを構成することもできます。このオブジェクトを選択すると、ウィンドウ下部のルール構成セクションに、[名前] フィールドが表示されます。ターゲットサーバー上で検索される名前 (プライマリキー) を入力します。

たとえば、アスタリスク (*) を入力すると、ターゲット上のすべてのものに一致します。P*は大文字のPで始まるすべてのオブジェクトに一致し、*Pは大文字のPで終わるすべての要素に一致します。

名前またはワイルドカード文字列を入力した後、ステップ 6 と同じ手順でルールパラメーターを構成できます。

ワイルドカードを使用する場合、一致するオブジェクトはすべてルール構成に制約されることに注意してください。このタイプの監査ルールは、見つかったすべてのオブジェクトがルールパラメーターに一致する場合にコンプライアンス状態と見なされます。

8 監査の構成を終了するには、監査のターゲットサーバー、ルールの例外、スケジュール、通知を設定します。

9 監査を保存するには、[**ファイル**] メニューから [**保存**] を選択します。監査をポリシーとして保存することもできます。監査またはスナップショット仕様の監査ポリシーとしての保存 (85ページ) を参照してください。

10 監査を実行するには、[**アクション**] メニューから [**監査の実行**] を選択します。監査の実行 (21ページ) を参照してください。

ストレージルールの構成

ストレージルールを使用すると、コアがSEに接続するように構成されていれば、データセンター内のストレージデバイス、SANデバイス、接続に関してサーバーを監査できます。

SANオブジェクトの監査とスナップショットを実行するには、Storage Essentials (SE) バージョン6.1.1以後が必要で、Server AutomationのSE Connectorコンポーネントを SAコアにインストールして構成しておく必要があります。詳細については、SA管理者に問い合わせるか、Storage Visibility and Automationドキュメントを参照してください。

ストレージルールを構成するには、次の手順を実行します。

1 監査の作成 (19ページ) のいずれかの方法で、新しい監査を作成します。(このルールをスナップショット仕様に対して作成する場合は、スナップショット仕様の作成 (115ページ) を参照してください)。

2 監査ソースを選択します。サーバー、スナップショット、スナップショット仕様、またはソースなしが選択できます。(アプリケーション構成、Windowsユーザーおよびグループなど、一部の監査ルールにはソースが必要です)。

3 [監査] ウィンドウのビューペインで、[ルール] > [ストレージ] を選択します。

4 [監査] ウィンドウの内容ペインで、[監査に対して利用可能] セクションのトップレベルノードを展開して、ルールを作成する元になるストレージルールを選択します。各ストレージ監査ルールは、各カテゴリの許容される値をチェックします。ルールは、最小値、最大値、または正確な数値をチェックするように構成できます。

- **アンマウントされたボリューム容量**: 許容されるマウント解除されたボリュームの合計容量 (バイト)。
- **アンマウントされたボリューム数**: 許容されるマウント解除されたボリューム数。
- **ファブリック**: 許容されるファブリック数。
- **FCA**: 許容されるファイバーチャネルアダプター (FCA) 数。
- **イニシエーターポート**: 許容されるイニシエーターポート数。
- **スイッチ**: 許容されるSANスイッチ数。

- **ターゲットポート**: 許容されるターゲットポート数。
- **RAID タイプ**: ターゲットストレージアレイ上で使用可能な RAID タイプ (**注**: このルールが選択され、RAIDタイプが指定されていない場合、監査は失敗します)。

ポート、スイッチ、ファブリックに関連するコンプライアンスルールは、アクティブなポートだけをチェックします。これらのコンプライアンスルールは、物理ポートの接続はチェックしません。

5 右矢印ボタンをクリックして、ルールオブジェクトを［監査に対して選択済み］セクションに移動します。構成したすべてのストレージルールが、ターゲットサーバーまたはスナップショット仕様で監査されます。

6 各ルールに対して、次のいずれかのチェックプロパティを選択します。

- 演算子。等しい (=)、小さい (<)、以下 (<=) などが使用できます。
- 値。数値など、ルールのタイプによって異なります。

7 監査の構成を終了するには、監査のターゲットサーバー、ルールの例外、スケジュール、通知を設定します。

8 監査を保存するには、[**ファイル**] メニューから [**保存**] を選択します。監査をポリシーとして保存することもできます。監査またはスナップショット仕様の監査ポリシーとしての保存 (85ページ) を参照してください。

9 監査を実行するには、[**アクション**] メニューから [**監査の実行**] を選択します。監査の実行 (21ページ) を参照してください。

Windows .NET Framework構成ルールの構成

Windows .NET Framework 構成ルールを使用すると、アセンブリキャッシュおよび構成アセンブリリストに関する情報を監査に使用できます。たとえば、アセンブリ名、バージョン、ロケール、パブリックキートークン、キャッシュファイル (GACまたはZAP)、プロセッサーアーキテクチャー、カスタム、ファイル名などです。

Windows .NET Framework構成ルールを構成するには、次の手順を実行します。

1 監査の作成 (19ページ) のいずれかの方法で、新しい監査を作成します。(このルールをスナップショット仕様に対して作成する場合は、スナップショット仕様の作成 (115ページ) を参照してください)。

2 監査ソースを選択します。サーバー、スナップショット、スナップショット仕様、またはソースなしが選択できます。(アプリケーション構成、Windowsユーザーおよびグループなど、一部の監査ルールにはソースが必要です)。

3 [監査] ウィンドウのビューペインで、[ルール] > [Windows .NET Framework構成] を選択します。

4 [監査] ウィンドウの内容ペインで、[監査に対して利用可能] セクションのトップレベルノードを展開して、ルールを作成する元になるWindows .NET Framework構成ルールを選択します。

5 右矢印ボタンをクリックして、ルールオブジェクトを［監査に対して選択済み］セクションに移動します。構成したすべてのWindows .NET Framework構成ルールが、ターゲットサーバーまたはスナップショット仕様で監査されます。

6 各ルールに対して、次のいずれかのチェックタイプを選択します。

- **プロパティ値**: ターゲットオブジェクトの個々のプロパティをチェックする値ベースのチェック。このタイプのチェックの場合、各オブジェクトに対して、オブジェクトに関連するプロパティを定義する式を、ルールウィンドウ下部のドロップダウンリストを使用して作成する必要があります。オブジェクトのタイプに応じて固有の演算子を指定できます。使用できるのは、文字列、数値 (整数または浮動小数点数)、ブール値 (真と偽の値の比較)、日付 (時刻でなく日付の比較)、配列です。
- **ソースと同等**: ソース上のオブジェクトとターゲットサーバーとの1対1の比較を行う比較チェック。このタイプのチェックでは、ソースサーバーとターゲットサーバーの両方から選択された各プロパティが正確に一致する場合のみ、オブジェクトはコンプライアンス状態と見なされます。

- **非存在**: オブジェクトの非存在チェックを行い、ターゲットサーバーにオブジェクトが存在するかどうかを判定するルール。オブジェクトがターゲットサーバーに存在する場合、ユーザーまたはグループルールが非コンプライアンス状態にあります。実行時に、ソースサーバーが存在しても、このサーバーに対する照会は行われません。また、ワイルドカードルールオブジェクトを選択すると、ターゲットサーバーにのみ適用されます。

7 ワイルドカードルールオブジェクト  を選択することにより、ワイルドカード検索に基づいてルールを構成することもできます。このオブジェクトを選択した場合、ウィンドウ下部のルール構成セクションに[名前]フィールドが表示され、ターゲットサーバーで検索される名前(プライマリキー)を入力できます。

たとえば、アスタリスク(*)を入力すると、ターゲット上のすべてのものに一致します。P*は大文字のPで始まるすべてのオブジェクトに一致し、*Pは大文字のPで終わるすべての要素に一致します。

名前またはワイルドカード文字列を入力した後、ステップ6と同じ手順でルールパラメーターを構成できます。

ワイルドカードを使用する場合、一致するオブジェクトはすべてルール構成に制約されることに注意してください。このタイプの監査ルールは、見つかったすべてのオブジェクトがルールパラメーターに一致する場合にコンプライアンス状態と見なされます。

8 監査の構成を終了するには、監査のターゲットサーバー、ルールの例外、スケジュール、通知を設定します。

9 監査を保存するには、[**ファイル**]メニューから[**保存**]を選択します。監査をポリシーとして保存することもできます。監査またはスナップショット仕様の監査ポリシーとしての保存(85ページ)を参照してください。

10 監査を実行するには、[**アクション**]メニューから[**監査の実行**]を選択します。監査の実行(21ページ)を参照してください。

Windowsレジストリルールの構成

Windowsレジストリルールは、比較ベースのルールであり、監査またはスナップショット仕様のソースからWindowsレジストリキーまたはフォルダーを選択して、ターゲットサーバーと比較できます。監査では、選択したレジストリフォルダーとキーが比較され、ターゲットサーバー上に存在するかどうかが判定されます。ルールにターゲット値または修復値を設定することはできません。

Windowsレジストリオブジェクト

Windowsレジストリオブジェクトを使用すると、レジストリキー、レジストリ値、サブキーを取得できます。レジストリキーはレジストリ値を含むディレクトリであり、レジストリ値はディレクトリ内のファイルに似ています。サブキーはサブディレクトリのようなものです。SAクライアントでサポートされるWindowsレジストリキーは、HKEY_CLASSES_ROOT、HKEY_CURRENT_CONFIG、HKEY_LOCAL_MACHINE、HKEY_USERSです。

監査と取得の際にキーエントリ(データ)の内容で有効な制御文字は、#x9、#xA、[#xD、#x20-#xD7FF]、[#xE000-#xFFFD]、[#x10000-#x10FFFF]です。無効な制御文字はSAクライアントに記録できないため、XMLエンティティに変換されて&#;で表示されます。たとえば、データ値が00 00(バイト)の場合、監査またはスナップショット仕様の結果には&#x00;が表示されます。

アクセス制御レベル(ACL)

Windowsレジストリルールでは、アクセス制御レベル(ACL)を比較するように選択することも可能です。WindowsレジストリルールでACLをチェックしていて、ユーザーとグループのACLが存在しない場合、監査が実行されて修復が行われた後に、ターゲット上にユーザーとグループが存在しなければ、一時的なユーザーとグループが不明な名前を使用して作成されます。次に監査を実行すると、ソースユーザーと異なる不明な名前が表示されます。詳細については、監査結果(86ページ)を参照してください。

Windowsレジストリ監査ルールを構成するには、次の手順を実行します。

1 新しい監査を作成します。監査の作成方法については、監査の作成 (19ページ) を参照してください。

(オプション) このルールをスナップショット仕様に対して作成する場合は、スナップショット仕様の作成 (115ページ) を参照してください。

2 監査ソースを選択します。サーバー、スナップショット、スナップショット仕様、またはソースなしが選択できます。

一部の監査ルール (アプリケーション構成、Windowsユーザーおよびグループなど) には、ソースが必要です。

3 [監査] ウィンドウのビューペインで、[ルール] > [Windowsレジストリ] を選択します。

4 [監査] ウィンドウの内容ペインで、[監査に対して利用可能] セクションのトップレベルノードを展開して、ルールを作成するWindowsレジストリフォルダーまたはキーを選択します。

5 右矢印ボタンをクリックして、Windowsレジストリフォルダーまたはキーを [監査に対して選択済み] セクションに移動します。選択したすべてのアイテムが、ターゲットサーバーの監査またはスナップショット取得に用いられます。

6 作成したレジストリエントリキールールのそれぞれに対して、監査でターゲットをチェックする際に次のオプションを使用するように設定できます。

- **サブキーの内容も比較**—選択したレジストリキーに属するすべてのサブキーを評価します。
- **ACLも比較**—選択したレジストリキーのACLを比較します。
- **キー値に対して大文字と小文字を区別しない比較を使用** — 名前の大文字と小文字が異なっている場合に、キー値の差異を監査結果に表示しません。

7 監査の構成を終了するには、監査のターゲットサーバー、スケジュール、通知を設定します。

8 [**ファイル**] メニューの [**保存**] を選択して、監査を保存します。

(オプション) 監査をポリシーとして保存することもできます。監査またはスナップショット仕様の監査ポリシーとしての保存 (85ページ) を参照してください。

9 監査を実行するには、[**アクション**] メニューから [**監査の実行**] を選択します。監査の実行 (21ページ) を参照してください。

注: [監査ポリシー] ウィンドウで特定のサーバーを選択して登録情報を表示した後に、別のサーバーの登録情報を確認する場合、[監査ポリシー] ウィンドウを閉じてから再度開き、登録内容のフィールドを更新します。

Windowsサービスルールの構成

Windows サービスルールは、比較ベースのルールであり、監査またはスナップショット仕様のソースからWindowsサービスを選択して、ターゲットサーバーと比較できます。監査またはスナップショット仕様では、選択したサービスがターゲットサーバー上のサービスと比較され、サービスが存在するかどうかと、サービスが開始済み、停止済み、または無効であるかどうかが判定されます。このタイプのルールにターゲット値または修復値を設定することはできません。

Windowsサービス監査ルールを構成するには、次の手順を実行します。

1 新しい監査を作成します。監査の作成方法については、監査の作成 (19ページ) を参照してください。

(オプション) このルールをスナップショット仕様に対して作成する場合は、スナップショット仕様の作成 (115ページ) を参照してください。

2 監査ソースを選択します。サーバー、スナップショット、スナップショット仕様、またはソースなしが選択できます。

一部の監査ルール (アプリケーション構成、Windowsユーザーおよびグループなど) には、ソースが必要です。

3 [監査] ウィンドウのビューペインで、[ルール] > [Windowsサービス] を選択します。

4 [監査] ウィンドウの内容ペインで、[監査に対して利用可能] セクションのトップレベルノードを展開して、ルールを作成するWindowsサービスを選択します。利用可能な任意のサービスを選択できますが、すべてのWindowsサービスのルートフォルダーを選択することはできません。

5 右矢印ボタンをクリックして、選択したWindowsサービスを [監査に対して選択済み] セクションに移動します。選択したすべてのアイテムが、ターゲットサーバーの監査またはスナップショット取得に用いられます。

6 監査の構成を終了するには、監査のターゲットサーバー、スケジュール、通知を設定します。

7 監査を保存します。

8 監査を実行するには、[**アクション**] メニューから [**監査の実行**] を選択します。監査の実行 (21ページ) を参照してください。

Windows/UNIXユーザーおよびグループルールの構成

WindowsまたはUnixユーザーおよびグループルールを使用すると、WindowsおよびUnixサーバーのローカルユーザーおよびグループ情報にアクセスできます。

ユーザーおよびグループルールを構成するには、次の手順を実行します。

1 監査の作成 (19ページ) のいずれかの方法で、新しい監査を作成します。(このルールをスナップショット仕様に対して作成する場合は、スナップショット仕様の作成 (115ページ) を参照してください)。

2 監査ソースを選択します。サーバー、スナップショット、スナップショット仕様、またはソースなしが選択できます。(アプリケーション構成、Windowsユーザーおよびグループなど、一部の監査ルールにはソースが必要です)。

3 [監査] ウィンドウのビューペインで、[ルール] > [**Windows/UNIXユーザーおよびグループ**] を選択します。

4 [監査] ウィンドウの内容ペインで、[監査に対して利用可能] セクションのトップレベルノードを展開して、ルールを作成する元になるユーザーおよびグループルールを選択します。

5 右矢印ボタンをクリックして、ルールオブジェクトを［監査に対して選択済み］セクションに移動します。構成したすべてのユーザーおよびグループルールが、ターゲットサーバーまたはスナップショット仕様で監査されます。

6 各ルールに対して、次のいずれかのチェックタイプを選択します。

- **プロパティ値**: ターゲットオブジェクトの個々のプロパティをチェックする値ベースのチェック。このタイプのチェックの場合、各オブジェクトに対して、オブジェクトに関連するプロパティを定義する式を、ルールウィンドウ下部のドロップダウンリストを使用して作成する必要があります。オブジェクトのタイプに応じて固有の演算子を指定できます。使用できるのは、文字列、数値 (整数または浮動小数点数)、ブール値 (真と偽の値の比較)、日付 (時刻でなく日付の比較)、配列です。一部のプロパティタイプでは、値セレクターボックスから値を選択できます。
- **ソースと同等**: ソース上のオブジェクトとターゲットサーバーとの1対1の比較を行う比較チェック。このタイプのチェックでは、ソースサーバーとターゲットサーバーの両方から選択された各プロパティが正確に一致する場合のみ、オブジェクトはコンプライアンス状態と見なされます。
- **非存在:** オブジェクトの非存在のチェック、すなわちターゲットサーバー上にオブジェクトが存在しないことを確認します。ターゲットサーバー上にオブジェクトが存在する場合、ルールはコンプライアンス違反になります。実行時に、ソースサーバーが存在しても、このサーバーに対する照会は行われません。また、ワイルドカードルールオブジェクトを選択すると、ターゲットサーバーにのみ適用されます。

7 ワイルドカードルールオブジェクト  を選択することにより、ワイルドカード検索に基づいてルールを構成することもできます。このオブジェクトを選択すると、ウィンドウ下部のルール構成セクションに、[名前] フィールドが表示されます。ターゲットサーバー上で検索される名前 (プライマリキー) を入力します。

たとえば、アスタリスク (*) を入力すると、ターゲット上のすべてのものに一致します。P*は大文字のPで始まるすべてのオブジェクトに一致し、*Pは名前が大文字のPで終わるすべてのユーザーに一致します。

名前またはワイルドカード文字列を入力した後、ステップ 6 と同じ手順でルールパラメーターを構成できます。

ワイルドカードを使用する場合、一致するオブジェクトはすべてルール構成に制約されることに注意してください。このタイプの監査ルールは、見つかったすべてのオブジェクトがルールパラメーターに一致する場合にコンプライアンス状態と見なされます。

8 監査の構成を終了するには、監査のターゲットサーバー、ルールの例外、スケジュール、通知を設定します。

9 監査を保存するには、[**ファイル**] メニューから [**保存**] を選択します。監査をポリシーとして保存することもできます。監査またはスナップショット仕様の監査ポリシーとしての保存 (85ページ) を参照してください。

10 監査を実行するには、[**アクション**] メニューから [**監査の実行**] を選択します。監査の実行 (21ページ) を参照してください。

コンプライアンスチェックの構成

BSA Essentials Subscription Servicesに登録している場合、多数のコンプライアンスルールやその構成要素 (コンテンツ開発者の間ではコンプライアンスチェックと呼ばれる) にアクセスできます。

アクセスできるチェックの種類はコンテンツサブスクリプションによって異なりますが、Microsoft Windows用の最新のパッチ、現行の規制コンプライアンスポリシー (FISMA、Sarbanes-Oxleyなど)、コンテンツ開発者コミュニティが配布しているユーザー作成のチェック、毎日更新される脆弱性情報などが含まれる可能性があります。

BSA Essentials Subscription Servicesに登録していない場合、監査、監査ポリシー、スナップショット、コンプライアンスチェックエディターに、コンプライアンスチェックは表示されません。コンテンツサブスクリプションと、コンプライアンスチェックの入手方法の詳細については、BSA Essentials Subscription Services営業担当者までお問い合わせください。

各コンプライアンスチェックは少しずつ異なっており、独自の構成値が必要ですが、各チェックの基本パラメーターとして、ターゲット値 (サーバー上に見つかることが期待される値) とオプションの修復値を定義する必要があります。

チェックのプロパティデータの編集や、コンプライアンスチェックのグループの作成など、コアのコンプライアンスチェックの管理の詳細については、コンプライアンスチェック (68ページ) を参照してください。

監査またはスナップショット仕様でコンプライアンスチェックを構成するには、次の手順を実行します。

1 監査の作成 (19ページ) に示されているいずれかの方法で、監査またはスナップショットを作成します(このルールをスナップショット仕様に対して作成する場合は、スナップショット仕様の作成 (115 ページ) を参照してください)。

2 監査ソースを選択します。サーバー、スナップショット、スナップショット仕様、またはソースなしが選択できます。

3 [監査] ウィンドウのビューペインで、[ルール] オブジェクトを展開します。

4 コンプライアンスチェック ルールを選択します。

5 [監査] ウィンドウの内容ペインで、[追加] ボタンをクリックします。

6 [チェックの選択] ウィンドウの [参照] タブで、コンプライアンスチェックのカテゴリを参照して、監査またはスナップショットに使用するチェックを選択できます。

別の方法として、[検索] タブを選択し、チェックを名前で検索することもできます。チェック検索ツールは、チェックの名前と、チェックの説明の中にある語句を検索します。たとえば、最大パスワード長をチェックするルールを検索するには、[キーワード] フィールドに`max password`と入力します。

[詳細検索] オプションを使用すると、より詳細なチェック検索パラメーターを設定できます。

7 チェックを選択し (複数のチェックを選択するには [CTRL] キーまたは [SHIFT] キーを押しながらクリック)、[**OK**] をクリックして、チェックを監査に追加します。

8 チェックを選択し、次のパラメーターを定義または設定します。

入力値

一部のカスタムチェックでは、ターゲット値の構成の一部として入力値が必要です。このようなチェックに対しては、真または偽に設定することで成功または失敗を指定する必要があります。監査ルールの [説明] セクションに、推奨される値の説明があります。

ターゲット値

監査のターゲットサーバー上に存在することが期待される値、またはスナップショットで取得する値を指定します。次のパラメーターを変更できます。

- **演算子**: スクリプトの出力から式を作成するには、演算子を選択します。等しい (=)、等しくない (<>)、小さい (<)、大きい (>) などが使用できます。
- **参照**: スクリプト出力のソースを選択します。
- **ソース**: ソースサーバーからの値を使用して、ターゲットサーバー上に見つかった値と比較します。
- **値**: 独自の値を入力します。このオプションは、入力した値を使用して、ターゲットサーバーで返された値と比較します。  アイコンをクリックして、ソースサーバーから値を取得します。返された値はテキストボックスに表示され、そのまま使用することも、必要に応じて編集することもできます。
- **サーバー属性**: ソースサーバー上にあるサーバー属性を比較します。
- **カスタム属性**: ターゲットサーバー上にあるカスタム属性を比較します。

修復値

修復値設定はルールのタイプに応じて異なるので、適切なものを選択します。

9 監査の構成を終了するには、監査のターゲットサーバー、スケジュール、通知を設定します。

10 監査を保存するには、[**ファイル**] メニューから [**保存**] を選択します。監査をポリシーとして保存することもできます。監査またはスナップショット仕様の監査ポリシーとしての保存 (85ページ) を参照してください。

11 監査を実行するには、[**アクション**] メニューから [**監査の実行**] を選択します。監査の実行 (21ページ) を参照してください。

コンプライアンスチェックの名前の変更

監査、監査ポリシー、スナップショット仕様のコンプライアンスチェックのインスタンス名は、右クリックメニューから簡単に変更できます。

コンプライアンスチェックの名前の変更とプロパティの編集の詳細については、コンプライアンスチェック (68ページ) を参照してください。

コンプライアンスチェックの名前を変更するには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] >[**監査と修復**] を選択し、監査、監査ポリシー、またはスナップショット仕様を開きます。
2. [監査] (または [監査ポリシー] または [スナップショット仕様]) ウィンドウのビューペインで、カスタムチェックを含む特定のルール (ユーザーとグループなど) を選択します。
3. 内容ペインの [監査に対して利用可能] セクションで、カスタムルールチェックを選択し、右クリックして [**ルールの名前変更**] を選択して、ルールの名前を変更します。

➤ 監査またはスナップショット仕様が監査ポリシーにリンクされている場合、ルールチェックの名前は変更できません。

[監査/スナップショット仕様] ウィンドウからのコンプライアンスチェックの検索

SAには多数のコンプライアンスチェックが存在する可能性があるので、[監査] または [スナップショット仕様] ウィンドウ内部の検索ツールを使用して、必要なチェックを見つけることができます。

監査またはスナップショット仕様の内部からコンプライアンスチェックを検索するには、次の手順を実行します。

1. [監査] または [スナップショット仕様] ウィンドウのビューペインで、[ルール] オブジェクトを展開します。
2. コンプライアンスチェック  ルールを選択します。
3. 内容ペインで [**追加**]  をクリックします。
4. [チェックの選択] ウィンドウの [参照] タブで、コンプライアンスチェックのカテゴリを参照して、監査またはスナップショットに使用するチェックを選択できます。
5. [検索] タブを選択し、チェックを名前で検索します。チェック検索ツールは、チェックの名前と、チェックの説明の中にある語句を検索します。たとえば、最大パスワード長をチェックするルールを検索するには、[キーワード] フィールドに`max password`と入力します。
6. [詳細検索] リンクをクリックして、詳細な検索基準を作成します。詳細検索では、テキスト文字列による検索だけでなく、チェックのプロパティ (セキュリティレベル、外部ID、プラットフォーム、テストIDなど) の値によってクエリを制限できます。  をクリックして、詳細検索パラメーターを追加します。

   テストID、セキュリティレベル、外部IDをコンプライアンスチェックのプロパティに追加する方法については、コンプライアンスチェックのプロパティの編集 (68ページ) を参照してください。
7. 検索を実行するには、[**検索**] をクリックします。
8. 検索結果で、監査またはスナップショット仕様に追加するチェックを選択して、[**OK**] をクリックします。

コンプライアンスチェック

コンプライアンスチェックエディターへのアクセス権が必要です。アクセス権を取得するには、SA管理者にお問い合わせください。詳細については、『SA 管理ガイド』を参照してください。

コンプライアンスチェックエディターでは、コアの BSA Essentials Subscription Services のコンプライアンスチェックに関するプロパティ情報 (メタデータ) の参照、再グループ化、編集を行います。

たとえば、組織のデータセンター内のサーバーに対して実行されるすべてのコンプライアンスチェックに、外部の番号付け方式を対応付ける必要があるとします。コンプライアンスチェックエディターを使用すれば、外部IDをチェックに追加できます。また、外部IDを追加したチェックのカスタムグループを作成して、これらのチェックにアクセスする場合に、カスタムフォルダー内に容易に見つかるようにすることもできます。この外部IDを検索条件に使用すれば、ID番号または文字列でチェックを見つけることもできます。

また、カスタムチェックに関する情報を編集することで、チェックの名前の変更、カスタムセキュリティレベルの追加、チェックの説明の変更なども行えます。たとえば、チェックの修復の説明を追加して、修復の際に何が起きるかを示すことができます。これは、他の人がチェックを使用する場合に非常に有用な情報です。

コンプライアンスチェックのプロパティの編集

コンプライアンスチェックエディターでは、コンプライアンスチェックのプロパティを変更できます。名前の変更、説明の追加、プロパティ情報の変更、外部IDの追加などを実行できます。

コンプライアンスチェックのプロパティ情報を編集するには、次の手順を実行します。

1. SAクライアントの [**ツール**] メニューから [**コンプライアンスチェックエディター**] を選択します。このメニュー項目が見つからない場合は、SAに連絡してアクセス権を取得してください。
2. [コンプライアンスチェックエディター] ウィンドウの [参照] タブで、カスタムチェックのカテゴリを展開して、編集するチェックを見つけます。[プラットフォーム] フィルタードロップダウンリストでオペレーティングシステムを選択して、リストを絞り込むことができます。
3. [検索] タブを選択すると、名前または、名前と説明のフィールドのキーワードでチェックを検索できます。

   たとえば、セキュリティログをチェックするルールを検索するには、[キーワード] フィールドに `security log`と入力します。検索をさらに絞り込むには、キーワード `size`を追加して、セキュリティログファイルのサイズを監査するすべてのチェックを見つけます。

   [詳細検索] オプションを使用すると、より詳細なチェック検索パラメーターを設定できます。詳細検索では、セキュリティレベル、外部ID、プラットフォーム、テストIDなどの他のプロパティによるフィルタリングが可能です。

   追加の検索パラメーターを指定するには、  をクリックします。
4. チェックのプロパティ情報を編集するには、[参照] タブまたは [検索] タブの結果からチェックを選択します。
5. コンプライアンスチェックエディターの右側にある [プロパティ] タブで、次のチェック情報を編集します。
   - **名前**: [名前] の値フィールドの内部をダブルクリックして、チェックの名前を変更します。
   - **カテゴリ**: [クリックして編集] リンクをクリックして、チェックをカスタムフォルダーに追加します。たとえば、リンクをクリックして、[カテゴリ] ウィンドウで、キーボードの [ENTER] キーを押してから名前を入力して、新しいコンプライアンスチェックカテゴリを作成します。[**適用**] をクリッ

クします。カスタムグループフォルダーを作成するには、コンプライアンスチェックエディターウィンドウの下部にある [**変更の適用**] をクリックします。チェックのカスタムグループの作成の詳細については、カスタムコンプライアンスチェックカテゴリの作成 (69ページ) を参照してください。

- **外部ID**: 値フィールドの内部をダブルクリックして、外部IDを追加または変更します。
- **セキュリティレベル**: 値フィールドの内部をダブルクリックして、チェックのセキュリティレベルを入力または変更します。

6 コンプライアンスチェックエディターウィンドウの下部にある [**変更の適用**] をクリックして、変更をチェックに適用します。

7 チェックの説明を編集するには、[説明]、[修復の説明]、または [技術的説明] タブを選択して、それぞれの説明テキストを編集します。

8 説明用のHTMLエディターを使用するには、編集アイコン  をクリックします。

9 HTMLエディターで、説明ウィンドウの左下にあるHTML編集アイコンをクリックします。

10 HTMLの説明を編集します。

11 [**適用**] をクリックします。変更を元に戻すには、[**ファイル**] メニューで [**元に戻す**] を選択します。

12 [コンプライアンスチェックエディター] ウィンドウの下部にある [**変更の適用**] をクリックして、説明の変更をチェックに適用します。

カスタムコンプライアンスチェックカテゴリの作成

コンプライアンスチェックエディターでは、コアにインストールされているコンプライアンスチェックを含む独自のカスタムカテゴリを作成できます。たとえば、カスタムカテゴリを作成し、Windows サーバー上にあるユーザーとグループ設定を監査するすべてのチェックを追加します。または、特定のLinuxサービスに関連するチェックだけにアクセスしたい場合は、そのための専用のカテゴリを作成できます。

カスタムコンプライアンスチェックカテゴリを作成するには、次の手順を実行します。

1 SAクライアントの [**ツール**] メニューから [**コンプライアンスチェックエディター**] を選択します。このメニュー項目が見つからない場合は、SAに連絡してアクセス権を取得してください。

2 [コンプライアンスチェックエディター] ウィンドウの [参照] タブで、カスタムチェックのカテゴリを展開して、編集するチェックを見つけます。[プラットフォーム] フィルタードロップダウンリストでオペレーティングシステムを選択して、リストを絞り込むことができます。

3 コンプライアンスチェックを選択します。

4 [コンプライアンスチェックエディター] ウィンドウの右上にある [プロパティ] タブの [カテゴリ] 行で、[クリックして編集] リンクをクリックします。

5 [カテゴリ] ウィンドウで、マウスポインターをメインチェックカテゴリ名の末尾に置いて、キーボードの [ENTER] を押します。

6 名前を入力して、新しいコンプライアンスチェックカテゴリを作成します。これにより、新しいコンプライアンスチェックカテゴリがコンプライアンスチェックエディターで作成されます。その他のカテゴリを追加するには、もう一度 ENTER を入力して新しい行を開始し、カテゴリの名前を入力します。選択したチェックは新しいカテゴリすべてに追加されます。

7 [**適用**] をクリックします。

8 カスタムグループフォルダーを作成するには、コンプライアンスチェックエディターウィンドウの下部にある [**変更の適用**] をクリックします。

9 カスタムカテゴリを削除するには、上記の手順をもう一度実行して、[カテゴリ] ウィンドウからカテゴリの名前を削除します。

コンプライアンスチェックのデフォルトへの復元

コンプライアンスチェックをすべてデフォルトの状態、すなわちBSA Essentials Subscription Servicesポータルから最初にダウンロードしたときの状態に戻すには、[デフォルトに戻す] 操作を使用します。[デフォルトに戻す] を実行すると、コンプライアンスチェックに対するカスタマイズは削除され、コンプライアンスチェックはリリースされた元の状態に戻ります。

コンプライアンスチェックをデフォルトの状態に戻すには、次の手順を実行します。

1. SAクライアントの [**ツール**] メニューから [**コンプライアンスチェックエディター**] を選択します。このメニュー項目が見つからない場合は、SAに連絡してアクセス権を取得してください。
2. [コンプライアンスチェックエディター] ウィンドウで、[編集] メニューから [**デフォルトに戻す**] を選択します。

   [デフォルトに戻す] 操作は、選択したコンプライアンスチェックだけに適用されます。

非推奨のチェックの表示

非推奨となったコンプライアンスチェックをコンプライアンスチェックエディターに表示することができます。

非推奨のチェックをコンプライアンスチェックエディターに表示するには、次の手順を実行します。

1. SAクライアントの [**ツール**] メニューから [**コンプライアンスチェックエディター**] を選択します。このメニュー項目が見つからない場合は、SAに連絡してアクセス権を取得してください。
2. [**表示**] メニューから [**非推奨のチェックの表示**] を選択します
3. チェックされたカテゴリを展開すると、非推奨のチェックが表示されます。

   非推奨のチェックは、薄いグレーのイタリックフォントで表示されます。

チェックに含める対象/除外する対象の設定

コンプライアンスチェックに含める、またはコンプライアンスチェックから除外するファイルまたはディレクトリを指定できます。

含めるまたは除外するファイルまたはディレクトリを指定するには、次の手順を実行します。

1. [監査] ブラウザーのビューペインで、[ルール] を展開し、[ファイル] を選択します。
2. [**ルール**] > [**ファイル**] の内容ペインで、[ディレクトリオプション] の [**除外の設定**] をクリックします。
3. [含める対象/除外する対象の選択] ウィンドウで、各ドロップダウンリストから [含める] または [除外] を指定します。
4. [**参照**] をクリックしてソースサーバーのファイルまたはディレクトリを選択するか、ファイルパスを入力します。

   有効なワイルドカード文字は、アスタリスク (*) とパーセント記号 (%) です。たとえば、コンプライアンスチェックから.exeファイルをすべて除外するには、[除外] フィールドに "*.exe" と入力します (引用符なし)。

   ディレクトリの選択では、そのディレクトリの下にあるファイルとサブディレクトリも参照できます。操作は、C: ディレクトリやルートディレクトリ以外からも開始できます。

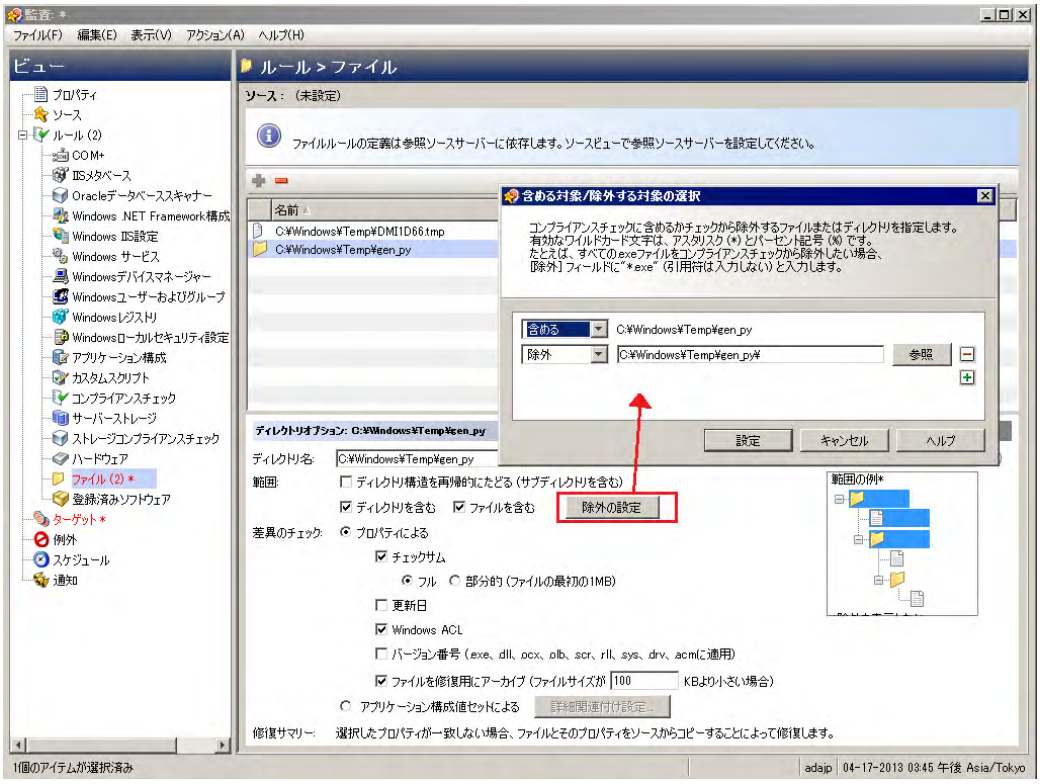
5.  をクリックして別の行を追加するか、 をクリックして行を削除します。
6. [参照] ウィンドウで、[**選択**] をクリックして選択を保存します。
7. [含める対象/除外する対象の選択] ウィンドウで、[**設定**] をクリックして設定を保存します。

ファイルの含める/除外ルール

監査、監査ポリシー、またはスナップショット仕様内部でファイルルールを構成する場合、監査またはスナップショットに含める対象または除外する対象として、ディレクトリまたはファイルを指定できます。この項では、含める/除外ルールについて説明し、これらのルールがファイルの絶対パスの相対サブセットにどのように適用されるかを示します。

監査のファイルルール内の含める/除外ルールは、図15に示すように、監査またはスナップショット仕様ウィンドウの下部にあります。

図15　　ファイルシステムのファイル/ディレクトリのワイルドカードの含める/除外ルール



監査またはスナップショット仕様でファイルルールを構成する際に、[ファイル/ディレクトリのワイルドカード]フィールドに含める/除外ルールを入力できます。ルールを入力した後、[含める]または[除外]をドロップダウンリストから選択します。新しい含める/除外ルールを追加するには、 をクリックします。

監査またはスナップショット仕様に対するファイルシステムルールの作成と構成の方法については、ファイルルールの構成 (46ページ) を参照してください。

含める/除外ルールのタイプ

監査と修復では、次のタイプの含める/除外ルールを、ファイルルールの構成に使用できます。

- ファイルタイプルールは、ファイル名パスに適用され、“/”と“\”のどちらも含みません。
- 相対タイプのルールは、相対パスに適用され、Unixの場合は“/”、Windowsの場合は“\”を含み、完全修飾でないものです。

- 絶対タイプのルールは、絶対パスに適用されます。Unixの場合、絶対パスの先頭は“/”です。Windowsの場合、絶対パスの先頭はボリューム文字で、その後に“:\”が付き、完全修飾になります。例としては、“C:\”、“d:\”、“f:\”などがあります。Windowsのパスに“/”(スラッシュ)を使用した場合、監査と修復は有効なパスにするためにこれを“\”(バックスラッシュ)に変換します。
- ファイル名とパスに対する環境変数とカスタム属性のパラメーター化。詳細については、SA/ カスタム属性でのファイル名のパラメーター化 (75ページ)を参照してください。

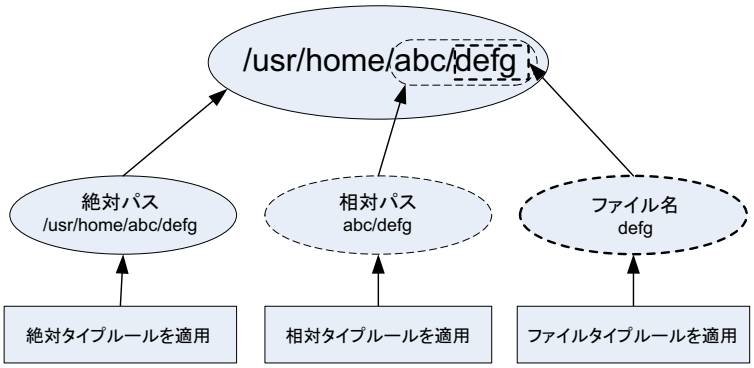
監査と修復は、すべての除外ルールを先に処理します。除外ルールがすべて適用された後で、含めるルールが適用されます。含めるルールのデフォルトは、ファイルシステムのすべてのオブジェクトを含めることです。多くの場合、含めるルールは処理自体行われないことがあります。除外ルール(先に処理される)と組み合わせたときに、これらのルールが意味をなさない場合があるからです。

含める/除外ルールには、アスタリスク(*)と疑問符(?)をワイルドカードとして使用することもできます。ワイルドカード文字は、パスまたは1文字以上の文字列に一致するプレースホルダーです。

含める/除外ルールのタイプに応じて、ルールはファイルの絶対パスの特定のサブセットだけに適用されます。監査と修復では、各スナップショットまたは監査に対して、1つのトップレベルが存在します。含める/除外ルールに対して比較するファイルには、1つの絶対パスがあります。図16では、絶対パスは`/usr/home/abc/defg`です。スナップショットまたは監査は、`/usr/home/abc/defg`絶対パスを下にたどって、相対パス`abc/defg`と、ファイル名`defg`を見つけます。この例では、含める/除外ルールは次のように適用されます。

- ファイルタイプのルールは、ファイル名パス`defg`に適用されます。
- 相対タイプのルールは、相対パス`abc/defg`に適用されます。
- 絶対タイプのルールは、絶対パス`/usr/home/abc/defg`に適用されます。監査と修復が含める/除外ルールをファイルのパスの相対サブセットにどのように適用するかについては、図16を参照してください。

図16　　含める/除外ルールの適用方法



これらのルールの適用方法の説明のために、次の例を使用します。

例: すべての.txtファイルをスナップショットまたは監査に含める (73ページ) と例: 最後のtemp.txtファイルを含め、他のすべてを除外 (74ページ) で使用されているファイルシステム構造の例は次のとおりです。

```
/dir1/dir2/a
/dir1/dir2/b
/dir1/dir2/names.txt
/dir1/dir2/temp.txt
/dir1/dir2/version1.exe
/dir1/dir2/subdir/version2.exe
```

例: すべての.txtファイルをスナップショットまたは監査に含める

拡張子が.txtのファイルをすべてスナップショットまたは監査に含める場合、含める/除外ルールは次のようになります。

- /dir1/dir2
- *.txtを含める (ファイルタイプのルール)
- *を除外 (ファイルタイプのルール)

次に示すのは、監査と修復がファイル構造を反復処理して、対応する含める/除外ルールを適用する手順です。

a. *によって/dir1/dir2/aが除外されます。次に*.txtが/dir1/dir2/aのファイル部分 (a) に適用され、一致が見つかりません。このファイルは含められません。

b. *によって/dir1/dir2/bが除外されます。次に*.txtが/dir1/dir2/bのファイル部分 (b) に適用され、一致が見つかりません。このファイルは含められません。

c. *はnames.txtに一致しますが、*.txtもnames.txtに一致するため、このファイルは除外されます。

d. ステップ3と同じ。

e. aを*と比較します。これは一致します。aをaと比較します。これは一致します。このファイルは含められます。

f. bを*と比較します。これは一致します。bをaと比較します。これは一致しません。このファイルは除外されます。

これらのステップ番号は、ファイル構造の例のパスに対応し、番号はトップレベルパスから始まります。

例: ファイルaだけをスナップショットまたは監査に含める

このファイルだけをスナップショットまたは監査に含める場合、含める/除外ルールは次のようになります。

- /dir1/dir2
- *を除外 (ファイルタイプのルール)
- aを含める (ファイルタイプのルール)

次に示すのは、監査と修復がファイル構造を反復処理して、対応する含める/除外ルールを適用する手順です。

a. *によって/dir1/dir2/aが除外されます。次に*.txtが/dir1/dir2/aのファイル部分 (a) に適用され、一致が見つかりません。このファイルは含められません。

b. *によって/dir1/dir2/bが除外されます。次に*.txtが/dir1/dir2/bのファイル部分 (b) に適用され、一致が見つかりません。このファイルは含められません。

c. *はnames.txtに一致しますが、*.txtもnames.txtに一致するため、このファイルは含められます。

d. ステップ3と同じ。

e. aを*と比較します。これは一致します。aをaと比較します。これは一致します。このファイルは含められます。

f. bを*と比較します。これは一致します。bをaと比較します。これは一致しません。このファイルは除外されます。

これらのステップ番号は、ファイル構造の例のパスに対応し、番号はトップレベルパスから始まります。

例: 最後のtemp.txtファイルを含め、他のすべてを除外

最後のtemp.txtファイルをスナップショットまたは監査に含め、他のすべてを除外する場合、含める/除外ルールは次のようになります。

- /dir1/dir2
- *を除外 (ファイルタイプのルール)
- dir3/temp.txtを含める (相対タイプのルール)

次に示すのは、監査と修復がファイル構造を反復処理して、対応する含める/除外ルールを適用する手順です。

a. *によって/dir1/dir2/aが除外されます。次に*.txtが/dir1/dir2/aのファイル部分 (a) に適用され、一致が見つかりません。このファイルは含められません。

b. *によって/dir1/dir2/bが除外されます。次に*.txtが/dir1/dir2/bのファイル部分 (b) に適用され、一致が見つかりません。このファイルは含められません。

c. *はnames.txtに一致しますが、*.txtもnames.txtに一致するため、このファイルは含められます。

d. ステップ3と同じ。

e. dir3/temp.txtが/dir1/dir2/dir3/temp.txtの相対部分と比較されます。これは一致します。

f. aを*と比較します。これは一致します。aをsubdir/version2.exeと比較します。これは一致しません。このファイルは除外されます。

これらのステップ番号は、ファイル構造の例のパスに対応し、番号はトップレベルパスから始まります。

ファイルルールのオーバーラップ

ルールに親ディレクトリを (オプション付きで) 含め、子ディレクトリを (別のオプション付きで) 追加パラメーターとして使用した場合、親ディレクトリのスナップショットと子ディレクトリのスナップショットは、1つのスナップショットとしてオーバーラップします。このロジックは、Windows NTのACLコレクションおよびコンテンツコレクションオプションと、Windows レジストリのコンテンツコレクションオプションにも適用されます。次の例は、親ディレクトリと子ディレクトリの監査ルールのオーバーラップを示します。

次のファイルシステムを例に取ります。ここで、末尾がスラッシュ (/) のものはディレクトリを表します。

```
/cust/app/bin/
/cust/app/bin/file1
/cust/app/bin/conf/
/cust/app/bin/conf/conf1
/cust/app/bin/conf/conf2
/cust/app/bin/conf/dev/
/cust/app/bin/conf/dev/conf3
```

例A

次の2つのルールでスナップショットを作成したとします。

ディレクトリ `/cust/app/bin` (再帰的、チェックサムなし)

ディレクトリ `/cust/app/bin/conf` (非再帰的、チェックサム)

スナップショットは次のファイルシステム情報を記録します。

/cust/app/bin/ （ディレクトリ）
/cust/app/bin/file1 （チェックサムなし）
/cust/app/bin/conf/ （ディレクトリ）
/cust/app/bin/conf/conf1 （*チェックサム*）
/cust/app/bin/conf/conf2 （*チェックサム*）
/cust/app/bin/conf/dev/ （ディレクトリ）
/cust/app/bin/conf/dev/conf3 （チェックサムなし）

このように、/cust/app/binが再帰的でチェックサムがないにも関わらず、/cust/app/bin/confディレクトリがそれをオーバーライドして、このディレクトリ内のすべてのファイルはチェックサムが記録されます。

例B

次の2つの監査ルールを使用してスナップショットを作成したとします（例Aで使用したオプションが入れ替わっています）。

ディレクトリ/cust/app/bin （再帰的、チェックサム）
ディレクトリ/cust/app/bin/conf （非再帰的、チェックサムなし）

スナップショットは次のファイルシステム情報を記録します。

/cust/app/bin/ （ディレクトリ）
/cust/app/bin/file1 （チェックサム）
/cust/app/bin/conf/ （ディレクトリ）
/cust/app/bin/conf/conf1 （*チェックサムなし*）
/cust/app/bin/conf/conf2 （*チェックサムなし*）
/cust/app/bin/conf/dev/ （ディレクトリ）
/cust/app/bin/conf/dev/conf3 （チェックサム）

例C

次の3つの監査ルールを使用してスナップショットを作成したとします（ファイルオプションが追加されています）。

ディレクトリ/cust/app/bin（再帰的、チェックサム）

ディレクトリ/cust/app/bin/conf（非再帰的、チェックサムなし）

ファイル/cust/app/bin/conf/conf1（チェックサム）

スナップショットは次のファイルシステム情報を記録します。

/cust/app/bin/ （ディレクトリ）
/cust/app/bin/file1 （チェックサム）
/cust/app/bin/conf/ （ディレクトリ）
/cust/app/bin/conf/conf1 （*チェックサム*）
/cust/app/bin/conf/conf2 （チェックサムなし）
/cust/app/bin/conf/dev/ （ディレクトリ）
/cust/app/bin/conf/dev/conf3 （チェックサム）

この例では、conf1に対する詳細な監査ルールによって、
/cust/app/bin/confの監査ルールがオーバーライドされています。

SA/カスタム属性でのファイル名のパラメーター化

監査またはスナップショット仕様でファイルルールを作成する際に、ファイル名で環境変数およびカスタム属性を参照できます。ルールウィンドウの[ファイル/ディレクトリのワイルドカード]領域で、ファイル名を編集してこれらの参照を追加できます。

Windows環境変数を参照する構文は%envVarName%で、Unixの構文は${varName}です。

カスタム属性を指定する構文は@varName@です。例:

```
@/customattribute/custAttrbuteNAME@\rest\of\the\path
@/customattribute/FacilityCustomAttrbuteNAME@\rest\of\the\path
@/customattribute/CustomerCustomAttributeNAME@\rest\of\the\path
@/customattribute/ServerAttrbuteNAME@\rest\of\the\path
@/customattribute/GrpAttrbuteNAME@\rest\of\the\path
```

これにより、パラメーター化された環境変数またはカスタム属性をファイル名に使用して、ソースサーバーとターゲットサーバーの相対パスを監査できます。

パラメーター化されたファイル名の例

たとえば、監査対象のサーバーで、アプリケーションへの相対パスはわかっていても、すべてのサーバーで絶対パスがわからない場合があります。監査のファイルルールでパスをパラメーター化することにより、相対パス名が除去され、監査はターゲットサーバー上に存在する相対パスをチェックします。

たとえば、監査に使用するゴールデンソースサーバーの'%ProgramFiles%'が:\Program Files"で、ターゲットサーバーの%ProgramFiles%がD:\Program Filesだとします。

ファイルルールの[ファイル/ディレクトリのワイルドカード]セクションで、監査のディレクトリルールのルートを%ProgramFiles%\Company\MyAppと指定できます。監査を実行すると、ターゲットとなるサーバーのパスから%ProgramFiles%が除去されます。すなわち、ソースサーバーのC:\Program Files\Company\MyApp\file1.txtがターゲットサーバーのD:\Program Files\Company\MyApp\file1.txtと比較されます。

もう1つの例として、2つの異なるサーバー上のまったく異なるサブディレクトリにインストールされたアプリケーションを監査するとします。

たとえば、監査でゴールデンソースサーバーの構成から次のインストールパスを選択します。

```
/usr/local/app-version-1232/prog
```

そして、ターゲットサーバーでは次のパスの下にアプリケーションがインストールされています。

```
/usr/local/app
```

ターゲットサーバーを監査するには、カスタム属性APP_INSTALL_LOCを定義し、その値をゴールデンサーバーに対しては/usr/local/app-version-1232/progに、プロダクションサーバーに対しては/usr/local/appに設定します。監査のファイルルールは次のようになります。

```
@/customattribute/APP_INSTALL_LOC@/prog
```

この場合、監査は@/opsware/customattribute/APP_INSTALL_LOC@をターゲットサーバー上の環境変数のように扱い、パスの置き換えを実行します。

サーバー属性を参照する場合は、パスは次のように入力します。

```
@/server/APP_INSTALL_LOC@/prog
```

パス名の環境変数

ベストプラクティス: Unixでファイル名のパスに環境変数を使用する場合 (一般にパラメーター化チェックと呼ばれる)、環境変数は次のファイルとディレクトリで定義するのが最善です。`etc/opt/opsware/snapshot/env`.Unixで環境変数を定義するのに`/etc/profile`は使用しないでください。

ファイルルール構成に使用する環境変数を定義するには、監査またはスナップショットのターゲットとなる管理対象サーバー上に変数定義のファイルを作成できます。

例:

1. 監査またはスナップショットのターゲットとする管理対象サーバーにsshで接続します。
2. 次の場所に新しいディレクトリを作成します。

   ```
   mkdir /etc/opt/opsware/snapshot
   ```

3. 新しい空のファイルを次のように作成します。

   ```
   touch /etc/opt/opsware/snapshot/env
   ```

4. 新しいファイルに、ファイルルールで使用する環境変数の定義を入力します。**例:**

   ```
   TEST1='/tmp/test1'
   TEST2='/home/test2'
   export TEST1 TEST2
   ```

5. 編集が終了したら、ファイルを保存します。

監査ルールの例外

ほとんどの監査ルールでは、選択した監査のターゲットサーバー (またはサーバーのグループ) に対する一時的または永久的なルールの例外を作成できます。すなわち、監査の実行時に選択した監査のターゲットに対して特定のルールを除外できます。

たとえば、複数のサーバーを監査している場合、ターゲットサーバーの一部に対していくつかのルールを使用しないことが必要な場合があります。たとえば、会社のセキュリティ標準を満たすため、Windowsサーバーの集合に対して定期的に監査を実行して、IISサービスが無効になっていることを確認しているとします。監査は、すべてのサーバーをチェックして、IISが無効であることを確認するように構成されます。いずれかのサーバーでIISが有効になっていると、監査は失敗します。

ところが、監査のターゲットとなるサーバーのいくつかで、IIS サービスを必要とするビジネスアプリケーションを短期間だけ実行する必要が生じたとします。この場合、IISサービスをチェックするルールに例外を作成して、そのアプリケーションを実行するサーバーに関連付けることができます。これにより、IISサービスが有効になっているサーバーがあっても、監査は成功します。

ルールの例外には有効期限を設定できます。これにより、ルールの例外が不要になるか許可されなくなったときには、監査のすべてのサーバーにルールが適用されます。また、例外の理由を記述したり、チケット ID を関連付けたりすることができます。ある監査で作成した例外は、他の監査には影響しません。

例外を作成できないルール

ほとんどの監査ルールには、例外を作成できます。ただし、ルールのセットのすべてを含むルールカテゴリには、例外を作成できません。

デバイスグループに例外を適用する際の考慮事項

デバイスグループに対して監査ルールの例外を設定した場合、例外はグループ内のすべてのサーバーに適用されます。場合によっては、例外が設定されたグループに属するサーバーの1つが別のデバイスグループに属しており、そのグループがやはり監査のターゲットで、例外が適用されていないという可能性があります。

このような場合、例外がないデバイスグループに属しているにも関わらず、そのサーバーには常に例外が適用されます。経験則として、ルールの例外が適用されたデバイスグループに属するすべてのサーバーは、常に監査ルールの例外となると覚えておいてください。これは、そのサーバーが、監査のターゲットでかつ同じルールが例外なしに適用されるデバイスグループに属しているかどうかには無関係です。

監査へのルールの例外の追加

監査ルールの例外を作成するには、監査で構成されているいずれかのルールを選択し、[ルールの例外の追加]ウィンドウで、監査のターゲットサーバーに関連付けます。監査を実行すると、選択したルールと、そのルールに関連付けられたターゲットサーバーまたはスナップショットは適用されません。

ルールの例外はデバイスグループに適用することもできます。ルールの例外は、無期限に適用することも、将来のある時点で期限切れになるように設定することもできます。例外を作成する理由を示すコメントを追加し、例外にチケットIDを関連付けることができます。

一部の監査ルールおよび監査ルールのコレクションには、例外を作成できません。詳細については、例外を作成できないルール (78ページ) を参照してください。

監査にルールの例外を追加するには、次の手順を実行します。

1. 最初に、監査を作成します。詳細については、監査の作成 (19ページ) を参照してください。
2. 監査に対して監査ルールを構成します。監査ルールの構成方法については、監査と修復のルール (35ページ) を参照してください。
3. 左側の監査ビューペインで、[例外]  アイコンを選択します。
4. 次に、内容ペインで、[**追加**] をクリックします。

[監査] ウィンドウでルールを選択することもできます。右クリックして [**例外の追加**] を選択します。ただし、監査がリンクされた監査ポリシーを参照している場合、ルールを右クリックして例外を追加することはできません。

5. [例外の追加] ウィンドウの [ターゲットサーバーの選択] セクションで、ルールの例外を適用する1つまたは複数のサーバーまたはデバイスグループを選択します。
6. 次に、[ルールの選択] セクションで、前のステップで選択したサーバーに関連付ける1つ以上のルールを選択します。
7. (オプション) [例外の理由] セクションで、説明を追加します。
8. (オプション) [チケットID] セクションで、この例外に関連付けるチケットIDを追加します。
9. [期限切れ] セクションで、例外が期限切れになる日付を入力するか、ドロップダウンリストから日付を選択します。

10 例外の構成が終わったら、[**追加**] をクリックします。

11 監査を実行したときに適用されるルールの例外のリストが表示されます。

ルールの例外の編集または削除

例外を編集するには、次の2つの方法があります。

- 例外をダブルクリックして、例外の理由、チケットID、有効期限の日付を変更します。
- [**追加**] をクリックして、ルールを編集します (既存のルールは上書きされます)。

例外を編集するには、次の手順を実行します。

1 [監査] ウィンドウを開きます。

2 ビューペインで [例外] アイコンを選択します。

3 内容ペインで例外をダブルクリックします。

4 [例外の編集] ウィンドウで、任意の例外と、それが割り当てられているサーバーまたはデバイスグループを編集できます。例外の編集が終わったら、[**追加**] をクリックします。

5 ルールを完全に変更する場合は、[**追加**] をクリックした後、[例外の追加] ウィンドウで、ターゲットサーバーと1つ以上のルールを選択してルールを変更します。終わったら、[**追加**] をクリックして例外を変更します。

例外を削除するには、次の手順を実行します。

1 [監査] ウィンドウを開きます。

2 左側の監査ビューペインで、[例外] アイコンを選択します。

3 内容ペインで、例外を選択して [**削除**] をクリックします。

監査ポリシーの管理

監査ポリシーを使用すると、サーバー構成コンプライアンスルールの集中化された再使用可能なコレクションを定義して保存できます。監査ポリシーは、監査、スナップショット仕様、および他の監査ポリシーにリンクすることができます。

監査ポリシーの作成は、一般的にポリシー設定の担当者が行います。担当者は、会社のサーバーが満たすべきコンプライアンス標準を理解しています。実際のサーバーの管理と監査を担当する別のユーザーは、自分が作成した監査またはスナップショット仕様に監査ポリシーをリンクすることで、あらかじめ定義された監査ポリシーを利用できます。監査ポリシーが変更された場合、それにリンクされた監査またはスナップショット仕様は、監査ポリシーの更新されたルールを参照します。サーバーの監査担当者は、組織の最新のコンプライアンス標準が自分の監査に反映されることを確信できます。

監査ポリシーは、別の監査ポリシーにリンクすることもできます。たとえば、複数の異なる別個の監査ポリシーを1つのマスターポリシーにまとめて、Windowsサービスの正しい構成を定義することができます。監査の実行後に、違反が見つかった場合は、監査結果から修復できます。

監査ポリシーは1から作成することも、監査、スナップショット仕様（または別の監査ポリシー）のルールを監査ポリシーとして保存することもできます。すべての監査ポリシーは、SAクライアントライブラリに保存されます。

特定の監査ポリシーにアタッチされている管理対象サーバー（ターゲット）のステータスを表示することもできます。

監査ポリシーのリンクとインポート

監査ポリシーは、監査およびスナップショット仕様、または他の監査ポリシー内部から、リンクによって使用できます。監査とスナップショット仕様では、インポートによって監査ポリシーを使用することもできます。

監査ポリシーのリンク

ベストプラクティス: 監査ポリシーを監査またはスナップショット仕様にリンクすることにより、監査またはスナップショット仕様で監査ポリシーと正確に同じルールセットを使用できるようになります。監査およびスナップショット仕様のルールは監査ポリシーに定義されたルールセットにリンクされているため、監査ポリシー内のいずれかのルールが変更された場合、次の監査およびスナップショット仕様の実行時には、同じ変更がそのルールに反映されます。

このリンクを解除するには、[**リンクされないルールを有効にする（定義済みの監査ポリシーにリンクしない）**]オプションを選択します。ファイルルールの構成（46ページ）を参照してください。

監査ポリシーは、他の監査ポリシーにリンクすることも可能です。任意の数の監査ポリシーを１つの監査ポリシーにリンクできます。監査ポリシー間のリンクでは、リンクする監査ポリシーが子となり、親の監査ポリシーには１つまたは複数の子をリンクします。監査を作成して親の監査ポリシーにリンクした場合、その監査をターゲットサーバーに対して実行すると、リンク先のポリシーのすべてのルールがターゲットサーバーに対して実行されます。

監査ポリシーのインポート

監査ポリシーを監査またはスナップショット仕様にインポートすると、監査ポリシーのすべてのルールがインポートされます。インポートされたルールは編集可能になります。監査ポリシーを監査にインポートする場合、監査の現在の値を置き換えるか、監査ポリシーのルールを監査またはスナップショット仕様のルールとマージするかを選択できます。監査ポリシーに別の監査ポリシーのルールをインポートすることはできませんが、別の監査ポリシーにリンクすることはできます。

複数のリンクされた監査ポリシーとのルールのオーバーラップ

監査またはスナップショット仕様からリンクしている監査ポリシーが、さらに別の監査ポリシーにリンクしている場合、リンクされたポリシーに、構成オプションが異なる同一のルールが含まれる可能性があります。

ルールに対して同じオブジェクトが見つかり、ルールをカスタマイズする方法がオプションの設定以外にない場合、ルールはマージされます。オプションは異なる場合もそうでない場合もありますが、いずれにせよ実行前にルールは1つにマージされ、結果は1つだけになります。オプションが異なる場合、オプションは1つのルールの中でORで結合されます。例としては、ファイルルール、レジストリルール、メタベースルール（古い比較タイプ）、Windowsサービスルールなどが挙げられます。

パラメーターを取るルールまたはユーザーがコンプライアンス基準を指定するルールは、パラメーターと基準が正確に一致する場合のみマージされます。それ以外の場合は、別々のルールとして実行されます。例としては、コンプライアンス（プラグ可能）ルール、カスタムスクリプトルール、サーバーモジュールベースのルールが挙げられます。

監査ポリシーの作成

監査ポリシーの作成の際には、ルールの作成方法として、ライブサーバーをソースとしてルールを選択する方法、独自のカスタムルールを作成する方法、または別の監査ポリシーのルールにリンクする方法があります。

ソースサーバーを使用して監査ポリシールールを作成する場合、監査ポリシーのルールを管理対象サーバーの実際の構成に基づいて作成できます。ポリシーが監査またはスナップショット仕様にリンクされている場合、監査ポリシーのソースサーバーは使用されません。

監査ポリシーは、SAクライアントライブラリのフォルダーに保存する必要があります。監査ポリシーの名前はフォルダー内で一意である必要があります。監査ポリシーをフォルダーに保存するには、そのフォルダーへの書き込みアクセス権が必要です。フォルダーのアクセス権の詳細については、『SA 管理ガイド』参照してください。

監査ポリシーを作成するには、次の手順を実行します。

1 ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**監査と修復**] > [**監査ポリシー**] を選択します。

2 オペレーティングシステムを選択します(WindowsまたはUnix)。

3 [**アクション**] メニューから [**新規**] を選択します。

4 (オプション) [プロパティ] 内容ペインで、名前と説明を入力します。名前には下線を使用できます。

5 [**選択**] をクリックして、監査ポリシーを保存するSAライブラリ内の場所を指定します。

6 [フォルダーの選択] ウィンドウで、場所のフォルダーを選択します。ポリシーを保存するフォルダーに書き込むためのアクセス権が必要です。

7 場所を選択したら、[**選択**] をクリックします。

8 監査ポリシーのルールを管理対象サーバーに基づいて作成する場合、[監査ポリシー] ウィンドウのビューペインで [**ソース**] を選択します。

9 [ソース] 内容ペインで、[**選択**] をクリックして監査ポリシーのソースサーバーを選択します。

10 [サーバーの選択] ウィンドウで、サーバーを選択して [**OK**] をクリックします。

11 [監査ポリシー] ウィンドウのビューペインで、[**ルール**] を選択します。

他の監査ポリシーをこの監査にリンクするには、  をクリックして監査ポリシーを選択します。

リンクされた監査ポリシーを編集するには、[ルール] リストで監査ポリシーを選択し、  をクリックして [監査ポリシー] ウィンドウを開きます。

12 [監査ポリシーの選択] ウィンドウで、監査ポリシーにリンクする1つ以上の監査ポリシーを選択し、[**OK**] をクリックして選択を保存します。

監査ポリシーに別の監査ポリシーをリンクした場合でも、監査ポリシーの個々のルールは構成可能です。外部参照される監査ポリシーのすべてのルールは、ここで作成したルールと結合されて、1つのルールセットを構成します。

13 ビューペインの [ルール] リストで、監査ポリシーに含める他のルールを作成します。特定の監査と修復ルールの構成方法については、第2章「監査とスナップショットのルール」(37ページ) を参照してください。

14 監査の構成が終了したら、[**ファイル**] メニューから [**保存**] を選択します。保存が終了すると、監査ポリシーは、監査、スナップショット仕様、または他の監査ポリシーにリンクできるようになります。

注: [監査ポリシー] ウィンドウで特定のサーバーを選択して登録情報を表示した後に、別のサーバーの登録情報を確認する場合、[監査ポリシー] ウィンドウを閉じてから再度開き、登録内容のフィールドを更新します。

監査の監査ポリシーとしての保存

監査を監査ポリシーとして保存できます。この操作では、監査のルールだけが保存されて、新しい監査ポリシーが作成されます。監査ルールがターゲットサーバー上に最新のエージェントを必要とする場合、SAクライアントは、ランタイムエラーを避けるため、エージェントを更新するか、監査に例外を作成するように促すメッセージを表示します。

作成したすべての監査ポリシーは、SAライブラリ内のフォルダーに保存する必要があります。監査ポリシーの名前はフォルダー内で一意である必要があります。監査ポリシーを保存するフォルダーに書き込むためのアクセス権が必要です。フォルダーのアクセス権の詳細については、『SAユーザーガイド: Server Automation』を参照するか、SA管理者にお問い合わせください。

監査を保存して監査ポリシーを作成するには、次の手順を実行します。

1. [監査] または [スナップショット仕様] ウィンドウで、[ファイル] メニューから **[名前を付けて保存]** を選択します。
2. [名前を付けて保存] ウィンドウで、名前を入力します。監査またはスナップショット仕様の名前を変更する場合は、一意の名前を使用する必要があります。
3. (オプション) 説明を入力します。
4. [タイプ] ドロップダウンリストから、[監査] または [監査ポリシー] を選択します。
5. [監査ポリシー] を選択した場合、[場所] セクションで **[選択]** をクリックします。
6. 監査ポリシーを保存するSAライブラリ内のフォルダーを選択します。監査ポリシーを保存するには、このフォルダーへの書き込みアクセス権が必要です。
7. **[OK]** をクリックします。

監査ポリシーのリンクとインポートの方法

監査ポリシーは、監査、スナップショット仕様、または別の監査ポリシーにインポートするか保存できます。

- 監査またはスナップショット仕様の監査ポリシーとしての保存 (85ページ)
- 監査ポリシーのマスター監査ポリシーへのリンク
- 監査ポリシールールのインポート (置換またはマージ)
- 監査またはスナップショット仕様の監査ポリシーとしての保存 (85ページ)

監査ポリシーの監査またはスナップショット仕様へのリンク

監査ポリシーを監査またはスナップショット仕様にリンクすると、監査ポリシーのルールが監査またはスナップショット仕様で使用されるリンクが作成されます。

ベストプラクティス: 監査ポリシーへのリンクを使用すると、ポリシー設定担当者がサーバーに対するサーバー構成ポリシーを定義し、他のユーザーは自分の監査やスナップショット仕様を同じ監査ポリシーにリンクできます。ポリシー設定担当者が監査ポリシーを変更した場合、ポリシーにリンクされている監査またはスナップショット仕様にも変更が反映されます。

監査ポリシーを監査またはスナップショット仕様にリンクした場合、監査またはスナップショット仕様のコンテキストでルールを変更することはできません。ただし、必要なユーザーアクセス権があれば、監査ポリシーにアクセスしてそのルールを編集することはできます。

監査ポリシーにリンクする監査またはスナップショット仕様にすでにルールが定義されている場合、外部の監査ポリシーにリンクした時点で、監査またはスナップショット仕様の既存のルールはすべて上書きされます。

監査ポリシーを監査またはスナップショット仕様にリンクするには、次の手順を実行します。

1 既存の監査またはスナップショット仕様をSAライブラリから開きます。

   a ナビゲーションペインで、[**ライブラリ**] > [**監査と修復**] > [**監査**] を選択します。オペレーティングシステムを選択します(WindowsまたはUnix)。内容ペインから監査を開きます。

   b ナビゲーションペインで、[**ライブラリ**] > [**監査と修復**] > [**スナップショット仕様**] を選択して、既存のスナップショット仕様を開きます。内容ペインからスナップショット仕様を開きます。

2 [**アクション**] メニューで [**ポリシーにリンク**] を選択します。

3 [監査ポリシーの選択] ウィンドウで、監査またはスナップショット仕様にリンクする監査ポリシーを選択します。1つの監査またはスナップショット仕様からは、1つの監査ポリシーだけにリンクできます。ただし、複数の監査ポリシーを1つの監査ポリシーにリンクすることは可能です。監査ポリシーの作成 (81ページ) または監査ポリシーのマスター監査ポリシーへのリンク (83ページ) を参照してください。

4 監査ポリシーを選択したら、[**OK**] をクリックします。

   すでにルールが定義されている監査またはスナップショット仕様に監査ポリシーをリンクしようとした場合、既存のルール定義を上書きするかどうかを確認するメッセージが表示されます。[**はい**] をクリックして、監査ポリシーをインポートし、既存のルールを上書きします。

5 [**ファイル**] メニューの [**保存**] を選択して、監査またはスナップショット仕様を保存します。

監査ポリシーのマスター監査ポリシーへのリンク

監査ポリシーを別の監査ポリシーにリンクすることにより、複数の監査ポリシーを1つのマスター監査ポリシーに統合できます。1つの監査ポリシーにリンクできる監査ポリシーの数には制限がないので、作成済みの既存の監査ポリシーを再使用して、特定の監査ニーズを満たす1つの監査ポリシーを作成できます。

監査ポリシーを別の監査ポリシーにリンクした場合、リンクした監査ポリシーは、親 (マスター) 監査ポリシーの子となります。監査を作成して親の監査ポリシーにリンクした場合、その監査をターゲットサーバーに対して実行すると、リンク先のポリシーのすべてのルールがターゲットサーバーに対して実行されます。

例: SAライブラリに、HP-UXサーバーのグループに対するコンプライアンス標準を定義するいくつかの個別の監査ポリシーが含まれているとします。1つのポリシーには、FTPサービスが有効になっていることをチェックするルールが含まれます。別のポリシーには、cron ロギングが常に有効になっていることをチェックするルールが含まれます。この例では、これら2つのポリシーにリンクする1つのマスター監査ポリシーを作成できます。その後、このマスター監査ポリシーを他の監査から参照できます。

監査ポリシーをマスター監査ポリシーにリンクするには、次の手順を実行します。

1 ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**監査と修復**] > [**監査ポリシー**] を選択します。

2 オペレーティングシステムを選択します (WindowsまたはUnix)。

3 既存の監査ポリシーを選択するか、新しい監査ポリシーを作成します。監査ポリシーの作成 (81ページ) を参照してください。

4 監査ポリシーのルールを管理対象サーバーに基づいて作成する場合、[監査ポリシー]　ウィンドウのビューペインで [**ソース**] を選択します。

   a [**選択**] をクリックして監査ポリシーのソースサーバーを選択します。

   b [サーバーの選択] ウィンドウで、サーバーを選択して [**OK**] をクリックします。

5 [監査ポリシー]ウィンドウのビューペインで、[**ルール**]を選択します。

a 他の監査ポリシーをこの監査にリンクするには、  をクリックして監査ポリシーを選択します。

b リンクされた監査ポリシーを編集するには、[ルール]リストで監査ポリシーを選択し、  をクリックして[監査ポリシー]ウィンドウを開きます。

6 [監査ポリシーの選択]ウィンドウで、監査ポリシーにリンクする1つ以上の監査ポリシーを選択し、[**OK**]をクリックして選択を保存します。

監査ポリシーに別の監査ポリシーをリンクした場合でも、監査ポリシーの個々のルールは構成可能です。外部参照される監査ポリシーのすべてのルールは、監査ポリシーに作成したルールと結合されます。

7 ビューペインの［ルール］リストで、監査ポリシーに含める他のルールを作成します。監査とスナップショットのルール (37ページ) を参照してください。

リンクされた監査ポリシーを編集するには、[ルール]リストで監査ポリシーを選択し、  をクリックします。

8 監査ポリシーの構成が終了したら、[**ファイル**]メニューから[**保存**]を選択します。保存が終了すると、監査ポリシーは他の監査ポリシーにリンクできるようになります。

監査ポリシールールのインポート

監査ポリシーを監査またはスナップショット仕様にインポートすると、監査ポリシーのルールが監査またはスナップショット仕様にインポート (オプションでマージ) されます。この場合、監査ポリシーへのリンクは維持されません。

監査ポリシーをインポートした後では、その監査ポリシーとの関連はなくなります。ソース監査ポリシーに変更があっても、インポート先には反映されません。

監査ポリシーを監査にインポートするには、次の手順を実行します。

1 既存の監査またはスナップショット仕様をSAライブラリから開きます。

a ナビゲーションペインで、[**ライブラリ**] > [**監査と修復**] > [**監査**]を選択します。オペレーティングシステムを選択します(WindowsまたはUnix)。内容ペインから監査を開きます。

b ナビゲーションペインで、[**ライブラリ**] > [**監査と修復**] > [**スナップショット仕様**]を選択して、既存のスナップショット仕様を開きます。内容ペインからスナップショット仕様を開きます。

2 [**アクション**]メニューで[**ポリシーにリンク**]を選択します。

3 監査またはスナップショット仕様にすでにルールが定義されている場合、既存のルールを上書きするか、監査ポリシーのルールを既存のルールにマージするかを選択できます。

ベストプラクティス: ルールをマージした結果は、ルールのタイプに応じて異なります。ベストプラクティスとしては、すべてのルールをレビューし、マージした監査ポリシールールが要件を満たしていることを確認してから、必要に応じて変更してください。

[**はい**]をクリックすると、監査ポリシーは監査またはスナップショット仕様の既存のルールを上書きします。

[**いいえ**]をクリックすると、監査ポリシーは監査ポリシールールを既存のルールとマージします。衝突が見つかった場合、監査ポリシーは既存のルールを上書きします。

4 [**ファイル**]メニューの[**保存**]を選択して、監査またはスナップショット仕様を保存します。

監査またはスナップショット仕様の監査ポリシーとしての保存

監査またはスナップショット仕様のルールを監査ポリシーとして保存できます。監査ポリシーは、別の監査またはスナップショット仕様で使用できます。監査ルールがターゲットサーバー上に最新のエージェントを必要とする場合、SAクライアントは、ランタイムエラーを避けるため、エージェントを更新するか、監査に例外を作成するように促すメッセージを表示します。

作成したすべての監査ポリシーは、SAライブラリ内のフォルダーに保存する必要があります。監査ポリシーの名前はフォルダー内で一意である必要があります。監査ポリシーをフォルダーに保存するには、そのフォルダーへの書き込みアクセス権が必要です。フォルダーのアクセス権の詳細については、『SA ユーザーガイド: Server Automation』を参照するか、SA管理者にお問い合わせください。

監査またはスナップショット仕様を監査ポリシーとして保存するには、次の手順を実行します。

1. 既存の監査またはスナップショット仕様をSAライブラリから開きます。
   a. ナビゲーションペインで、[**ライブラリ**] > [**監査と修復**] > [**監査**] を選択します。オペレーティングシステムを選択します(WindowsまたはUnix)。内容ペインから監査を開きます。
   b. ナビゲーションペインで、[**ライブラリ**] > [**監査と修復**] > [**スナップショット仕様**] を選択して、既存のスナップショット仕様を開きます。内容ペインからスナップショット仕様を開きます。
2. 監査またはスナップショット仕様のルールを構成した後で、[**ファイル**] メニューから [**名前を付けて保存**] を選択します。
3. [名前を付けて保存] ウィンドウで、名前と説明を入力します。
4. [タイプ] リストで、[監査ポリシー] を選択します。
5. [**選択**] をクリックします。
6. [フォルダーの選択] ウィンドウで、監査ポリシーを保存するフォルダーを選択し、[**OK**] をクリックします。監査ポリシーが保存され、[**ライブラリ**] > [**監査と修復**] > [**監査ポリシー**] でアクセスできるようになります。

フォルダーライブラリでの監査ポリシーの検索

監査ポリシーを作成してフォルダーライブラリに保存したら、[フォルダー内で検索] 機能を使用して、SAライブラリから監査ポリシーを容易に検索できます。

フォルダー内の監査ポリシーを検索するには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**監査と修復**] > [**監査ポリシー**] を選択し、WindowsまたはUnixを選択します。
2. 監査を選択し、右クリックして、[**フォルダー内で検索**] を選択します。監査ポリシーが保存されている場所が表示されます。

監査ポリシーのエクスポート

監査ポリシーに含まれ、構成されているすべてのルールのリストを見る場合、ポリシーをCSVやHTMLにエクスポートできます。

監査ポリシーをエクスポートするには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**監査と修復**] > [**監査ポリシー**] を選択します。
2. WindowsまたはUnixを選択します。

3 監査ポリシーを開きます。

a 監査を選択してダブルクリックします。

または

b 監査を選択し、右クリックして、[**開く**] を選択します。

4 [アクション] メニューから [**エクスポート**] を選択し、**CSV**または**HTML**のいずれかの形式を選択します。

5 ファイルのパスとファイル名を選択し、[**エクスポート**] をクリックします。

6 ファイルを開いて、エクスポートされた情報を表示します。

注: エクスポートされた情報を正しく表示するには、.csvファイルをテキストエディターで開き、ワードラップをオフにし、テキストウィンドウを水平方向に拡大します。

監査ポリシーのコンプライアンスの表示

監査ポリシーブラウザーで、特定の監査ポリシーにアタッチされている管理対象サーバー (ターゲット) のステータスを表示できます。

監査ポリシーを作成し、これにターゲットをアタッチした場合、コンプライアンス情報を表示するには監査を実行する必要があります。ターゲットサーバーのコンプライアンスステータスを表示するには、監査を1回以上実行するか、監査ポリシーをターゲットにリンクしている既存の監査結果が1つ以上必要です。

ベストプラクティス: データセンターのコンプライアンス維持で重要な役割を果たす監査ポリシーを選択します。また、コンプライアンスに準拠していない管理対象サーバーの表示が可能です。コンプライアンスステータスは、前回の監査結果または監査ポリシーの変更に基づいて表示されます。

監査ポリシーのコンプライアンスを表示するには、次の手順を実行します。

1 ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**監査と修復**] > [**監査ポリシー**] を選択します。

2 オペレーティングシステムを選択します (WindowsまたはUnix)。

3 既存の監査ポリシーを選択します。

4 [監査ポリシー] ウィンドウのビューペインで、[**コンプライアンス**] を選択します。

内容ペインに、監査ポリシーで参照されるすべての管理対象サーバーと、そのコンプライアンスステータスのリストが表示されます。

5 (オプション) リスト内のサーバーの詳細な情報を表示するには、サーバーを選択して [**表示**] をクリックし、サーバーブラウザーを表示します。

監査結果

監査は、サーバー上でチェックするサーバー構成を、監査のルールに基づいて定義します。監査結果は、監査を実行することによって生成されます。結果には、各ターゲットサーバーまたはターゲットスナップショットに関して、監査ルールと実際のサーバー構成値との間の差異が示されます。

ルールを修復できるかどうかは、ルールのタイプに依存します。ルールが修復をサポートするとともに、そのサーバーに対する監査ルールのソースに、修復をサポートするデータが含まれる必要があります。

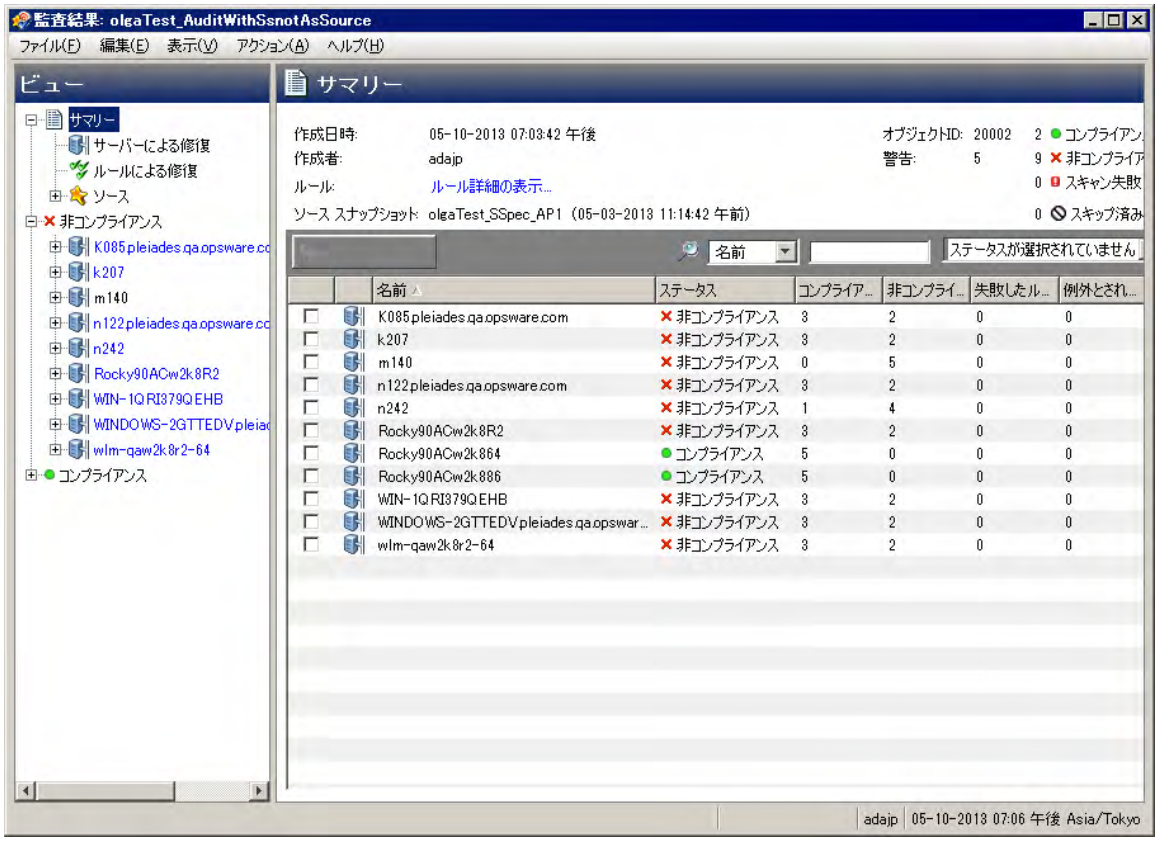
例: ハードウェアルールなど、一部のルールは修復をサポートしません。サーバーの物理メモリやハードウェアを修復することはできません。また、監査がスナップショットをソースとして使用しており、スナップショットがルールから十分な情報を収集できなかった場合は、そのルールは修復されません。

監査ポリシーにリンクしている監査を実行した場合、すべてのルールの結果が表示されます。ただし、ルールがもともとどの監査ポリシーで定義されたかは結果には示されません。

監査結果の表示

SAクライアントでは、任意の監査の監査結果のリストを図17のように表示できます。ライブラリで監査を選択すると、その監査に関連付けられたすべての結果のリストが、下の詳細ペインに表示されます。

図17　　監査結果



監査結果ウィンドウ

[監査結果]ウィンドウには、監査ジョブに関する詳細な情報が表示されます。たとえば、図18に示すように、監査のターゲットサーバーの間の差異や、監査で定義されたルールなどです。この情報は、監査されたサーバーが、データセンターに対して設定された標準を満たしているかどうかの判定に役立ちます。

図18　　監査結果ウィンドウ

既知の制限として、SAは名前だけがパッケージを一意に識別するとは見なしません(登録済みソフトウェアルール)。

例: 特定のバージョン番号を持つ特定のパッケージがサーバーにインストールされているかどうかをチェックするルール(登録済みソフトウェアルール)がある場合、パッケージ名が同じでもバージョン番号が異なると、目的のパッケージだとは認識されず、ルールに合致するパッケージは検出されなかったとみなされます。

ビュー

ビューペインには、監査結果の概要が表示されます。たとえば、修復オプションや、コンプライアンスステータスごとにグループ化されたサーバー(ターゲット)などです。

- **サマリー**: サーバーごと、ルールごと、またはすべてのサーバーのすべてのルールに対する修復が可能な修復オプション。修復が実行できるのは、ターゲットサーバー構成が監査のルールの定義に一致しないインスタンスのみです。この[サマリー]ビューには、結果の基になった監査のソースサーバーも表示されます。監査のソースとしてはサーバーまたはスナップショットが使用でき、ソースを使用しないこともできます。ただし、ルールによってはソースが必須のものもあります。監査の要素(18ページ)を参照してください。
- **コンプライアンス**: 監査のすべてのルールに一致するサーバー。
- **非コンプライアンス**: 監査の一部のルールに一致しなかったサーバー。
- **スキャン失敗**: 監査でターゲット構成を判定できなかったサーバー。たとえば、SAコアと通信できなかったサーバーなど。
- **スキップ済み**: スキップされたサーバー。

サマリー

[サマリー] ペインには、監査ジョブに関する次の情報が表示されます。

- **作成日時、作成者**: 監査の作成日時と、作成したユーザーの名前。
- **ソース**: 結果の基になった監査のソースサーバー。監査のソースとしてはサーバーまたはスナップショットが使用でき、ソースを使用しないこともできます。ただし、ルールによってはソースが必須のものもあります。監査の要素 (18ページ) を参照してください。
- **ルール: ルール詳細の表示...**このリンクは、[ルール] ウィンドウを開いて、監査のルールを表示します。
- **警告**: 監査中に発見された警告の数。
- **オブジェクトID**: SAクライアントによって使用される内部識別番号。
- **コンプライアンス**: 監査のすべてのルールに一致したサーバーの数。
- **非コンプライアンス**: 監査の一部のルールに一致しなかったサーバーの数。
- **スキャン失敗**: 監査でターゲット構成を判定できなかったサーバーの数。たとえば、SAコアと通信できなかったサーバーなど。
- **スキップ済み**: スキップされたサーバー。
- **部分監査の実行**: このリンクでは、サーバーを選択して、コンプライアンスステータスが [非コンプライアンス] または [スキャン失敗] のルールだけを対象に監査を再実行できます。

詳細

詳細ペインには、監査が実行されたすべてのサーバーのリストと、各サーバーのコンプライアンスステータス、および監査のルールのうちコンプライアンス、非コンプライアンス、スキャン失敗のステータスを持つものの数が表示されます。例外とされたルールおよび失敗したルールの数も表示されます。

列セレクターツールを使用して、表示の設定を変更できます。列の順序を変更するには、列見出しをクリックして左右にドラッグし、表示設定を変更します。

- **コンプライアンス**: ターゲットサーバー構成が監査のルールに一致したルールの数。
- **非コンプライアンス**: 監査のルールに一致しなかったターゲットサーバー構成の数。
- **スキャン失敗**: 監査でターゲット構成を判定できなかったルールの数。たとえば、SAコアと通信できなかったサーバーなど。
- **スキップ済み**: スキップされたサーバー。

修復方法: すべて、サーバーによる、ルールによる

[監査結果] ウィンドウでは、いくつかの方法で監査結果の非コンプライアンスルールを修復できます。

- すべて修復: [監査結果] ウィンドウの [アクション] メニューで、[すべて修復] を選択して、監査結果に見つかった差異を修復します。
- サーバーによる修復: 監査結果のターゲットサーバーごとに修復します。
- ルールによる修復: 個々の監査ルールを修復します。

- SAは、Windows Server 2000サーバーに対して、Windowsローカルセキュリティ設定ルールのセキュリティオプションの下の、Administratorアカウント名の変更とGuestアカウント名の変更の2つの値の修復をサポートしません。
- このリリースでは、IIS 7.0監査ルールでISAPIフィルターを修復することはできません。

すべて修復

修復可能なすべてのルールに関して、監査結果で見つかったすべての差異を修復するように選択できます。このオプションは、監査のすべてのターゲットサーバーに対して、すべての修復可能なルールを修復します。ステータスがコンプライアンス のルールは、監査の実行時に修復されません。

監査結果で見つかったすべての差異を修復するには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**監査と修復**] > [**監査**] を選択します。
2. 監査を選択します。監査リストの下の詳細ペインに、監査に関連付けられたすべての監査結果が表示されます。
3. 監査結果を選択し、右クリックして、[**開く**] を選択します。
4. [監査結果] ウィンドウで、[アクション] メニューから [**すべて修復**] を選択します。
5. 監査結果ウィンドウのステップ 1 では、監査の名前、監査対象、監査で定義されているルールの総数が表示されます。[**ジョブの開始**] をクリックすると、監査タスクのステップがすべて省略され、監査ジョブがすぐに開始します。
6. [**次へ**] をクリックします。
7. [スケジュール設定] ページで、監査をただちに実行するか、別の日時に実行するかを指定します。後で実行する場合は、[次の時刻にタスクを実行] を選択し、日付と時刻を指定します。
8. [**次へ**] をクリックします。
9. [通知] ページのデフォルト設定では、監査ジョブの成否に関係なく、監査の完了時にユーザーへ通知電子メールが送信されます。電子メールでの通知を追加するには、[**通知の追加**] をクリックして電子メールアドレスを入力します。
10. (オプション) 電子メールを、監査ジョブが成功した場合または失敗した場合のどちらに送信するかを指定できます。
11. (オプション) [チケットID] フィールドでチケットトラッキングIDを指定できます。[チケットID] フィールドが使用されるのは、HPプロフェッショナルサービスのSAが変更管理システムに統合されている場合のみです。それ以外の場合、このフィールドは空のままとします。
12. [**次へ**] をクリックします。
13. [ジョブステータス] ページで [**ジョブの開始**] をクリックして、監査を実行します。実行完了後、[**結果の表示**] をクリックすると監査の結果が表示されます。

ルールによる修復

監査結果のルールで見つかった特定の差異を修復できます。このためには、コンプライアンス違反の個々のルールを選択し、監査を再実行して、選択したルールだけを修復します。監査のすべてのターゲットサーバーに対して個々のルールを修復するか、または選択したサーバーだけでルールを修復するかを選択できます。

監査結果で見つかった特定の差異を修復するには、次の手順を実行します。

1 ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**監査と修復**] > [**監査**] を選択します。

2 監査を選択します。

3 監査リストの下の詳細ペインに、監査に関連付けられたすべての監査結果が表示されます。

4 監査結果を選択し、右クリックして、[**開く**] を選択します。

5 [監査結果] ウィンドウで、[サマリー] リストを展開し、[ルールによる修復] を選択します。監査結果内の、ルールによって検出されたすべての差異が表示されます。

6 修復する各ルールに対して、[修復の有効化] 列のリストのチェックマークを選択します。これにより、監査結果を修復すると、そのルールが適用される監査のターゲットサーバーすべてに対してルールが修復されます。

すべてのルールをグローバルに選択するには、右クリックして [**すべて選択**] を選択します。すべてのルールを選択解除するには、右クリックして [**すべて選択解除**] を選択します。

7 修復するルールを選択したら、[**アクション**] メニューから [**修復**] を選択します。

8 監査結果ウィンドウのステップ 1 では、監査の名前、監査対象、監査で定義されているルールの総数が表示されます。[**ジョブの開始**] をクリックすると、監査タスクのステップがすべて省略され、監査ジョブがすぐに開始します。

9 [**次へ**] をクリックします。

10 [スケジュール設定] ページで、監査をただちに実行するか、別の日時に実行するかを指定します。後で実行する場合は、[次の時刻にタスクを実行] を選択し、日付と時刻を指定します。

11 [**次へ**] をクリックします。

12 [通知] ページのデフォルト設定では、監査ジョブの成否に関係なく、監査の完了時にユーザーへ通知電子メールが送信されます。電子メールでの通知を追加するには、[**通知の追加**] をクリックして電子メールアドレスを入力します。

13 (オプション) 電子メールを、監査ジョブが成功した場合または失敗した場合のどちらに送信するかを指定できます。

14 (オプション) [チケットID] フィールドでチケットトラッキングIDを指定できます。[チケットID] フィールドが使用されるのは、HPプロフェッショナルサービスのSAが変更管理システムに統合されている場合のみです。それ以外の場合、このフィールドは空のままとします。

15 [**次へ**] をクリックします。

16 [ジョブステータス] ページで [**ジョブの開始**] をクリックして、監査を実行します。実行完了後、[**結果の表示**] をクリックすると監査の結果が表示されます。

サーバーによる修復

監査のターゲットサーバーごとに、監査結果でルールによって検出された特定の差異を修復できます。すべてのサーバーに対してすべてのルールを修復するか、選択したサーバーに対してすべてルールを修復するかを選択できます。

監査結果で見つかった特定の差異をサーバーごとに修復するには、次の手順を実行します。

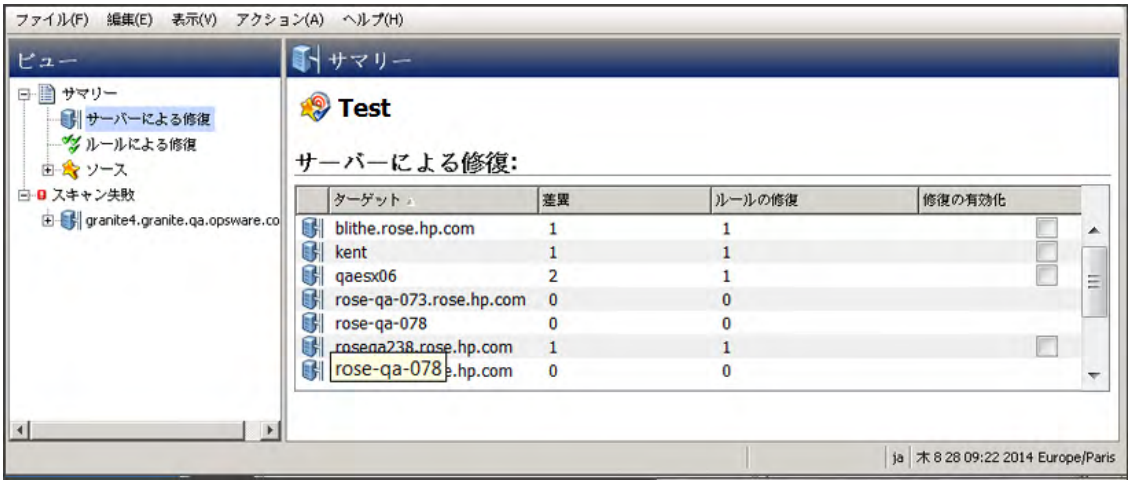
1 ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**監査と修復**] > [**監査**] を選択します。

2 監査を選択します。

3 監査リストの下の詳細ペインに、監査に関連付けられたすべての監査結果が表示されます。

4 監査結果を選択し、右クリックして、[**開く**] を選択します。

5 [監査結果] ウィンドウで、[サマリー] リストを展開します。



6 内容ペインに、監査のターゲットサーバーのリストが表示されます。監査する各サーバーに対して、[修復の有効化] 列のリストのサーバー隣のチェックボックスを選択し、[**部分監査の実行**] をクリックします。

または

ビューペインでサーバーのリストを展開すると、各サーバーに対して、監査のすべてのターゲットサーバーで検出されたすべての差異が表示されます。

修復する各サーバーに対して、[修復の有効化] 列のリストのチェックマークを選択します。これにより、監査結果を修復すると、選択したサーバーに対してすべてのルールが修復されます。

または

監査結果内のすべてのサーバーをグローバルに選択するには、右クリックして [**すべて選択**] を選択します。すべてのサーバーを選択解除するには、右クリックして [**すべて選択解除**] を選択します。

7 修復するサーバーを選択したら、[**アクション**] メニューから [**修復**] を選択します。

8 監査結果ウィンドウのステップ 1 では、監査の名前、監査対象、監査で定義されているルールの総数が表示されます。[**ジョブの開始**] をクリックすると、監査タスクのステップがすべて省略され、監査ジョブがすぐに開始します。

9 [**次へ**] をクリックします。

10 [スケジュール設定] ページで、監査をただちに実行するか、別の日時に実行するかを指定します。後で実行する場合は、[次の時刻にタスクを実行] を選択し、日付と時刻を指定します。

11 [**次へ**] をクリックします。

12 [通知] ページのデフォルト設定では、監査ジョブの成否に関係なく、監査の完了時にユーザーへ通知電子メールが送信されます。電子メールでの通知を追加するには、[**通知の追加**] をクリックして電子メールアドレスを入力します。

13 (オプション) 電子メールを、監査ジョブが成功した場合または失敗した場合のどちらに送信するかを指定できます。

14 (オプション) [チケットID] フィールドでチケットトラッキングIDを指定できます。[チケットID] フィールドが使用されるのは、HPプロフェッショナルサービスのSAが変更管理システムに統合されている場合のみです。それ以外の場合、このフィールドは空のままとします。

15 [**次へ**] をクリックします。

16 [ジョブステータス] ページで [**ジョブの開始**] をクリックして、監査を実行します。実行完了後、[**結果の表示**] をクリックすると監査の結果が表示されます。

比較ベースの監査結果の修復

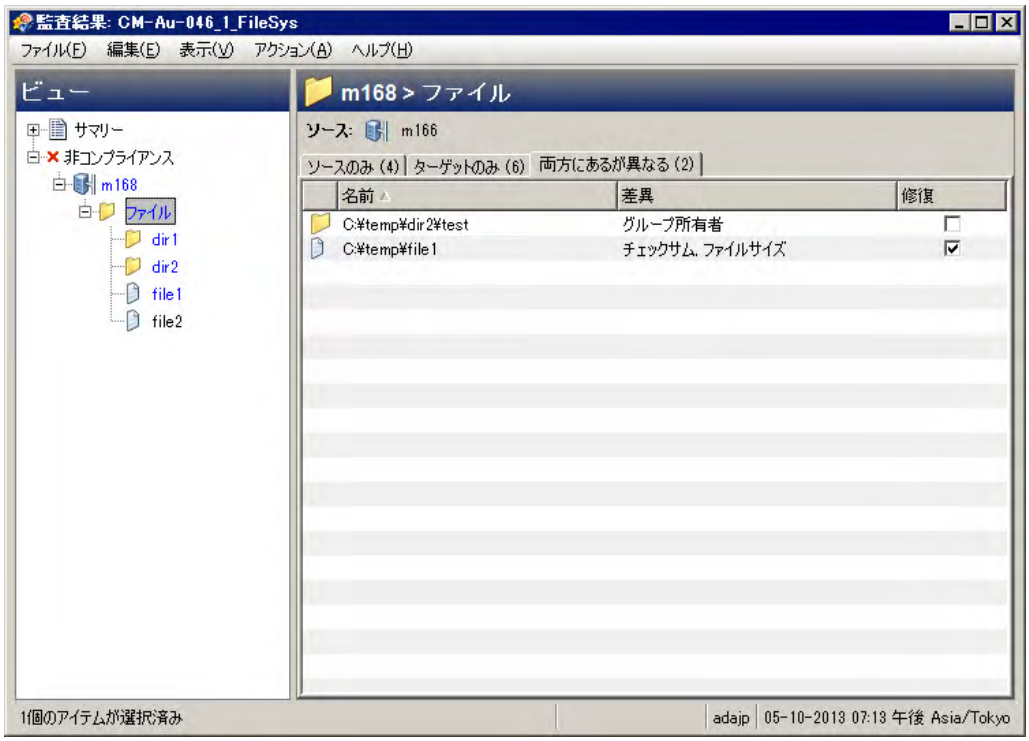
比較ベースの監査に基づく監査結果では、ソースサーバーまたはスナップショットとターゲットサーバーまたはスナップショットの間の差異を表示できます。監査結果が失敗の場合、すなわちソースとターゲットの間に差異が検出された場合、差異を修復できます (ほとんどのルールタイプの場合)。監査のソースオブジェクトのルール値を修復して、ターゲットの値を上書きできます (または、ソースに存在してターゲットに存在しない値を追加できます)。

[監査結果] ウィンドウでは、監査に定義されているすべてのオブジェクトがビューペインに表示されます。また、失敗した監査結果、監査とターゲットサーバーとの間に検出された差異が、薄い青のフォントで強調表示されます。

たとえば、図19に示すWindowsファイルシステムルールの監査結果では、選択したファイルとパスがソース (監査ルールのソースサーバー) とターゲットの両方に存在するが異なっているため、[監査結果] ウィンドウの [両方にあるが異なる] タブに表示されます。

[監査結果]ウィンドウで、ファイルルールを選択し、[**アクション**]メニューから[**修復**]を選択できます。

図19　　比較ベースの監査ルールの監査結果



この例では、ソースとターゲットの間にファイルの差異が見つかっており、ルールをダブルクリックすることで差異を別ウィンドウに表示できます。差異情報を確認して、修復を実行するかどうかを判断します。その後、[**アクション**]メニューから[**修復**]を選択してコンプライアンス違反のルールを修復するか、後で監査を実行するようにスケジュール設定できます。修復を行う場合、監査の値(ソースから得られたもの)によってターゲットサーバー上の値が置き換えられます。

スナップショットまたは監査結果からCOM+オブジェクトを修復する場合、SAクライアントはCOM+オブジェクトのバージョンをチェックしません。差異が存在するかどうかに関わらず、オブジェクトは常に修復されます。

継承された値によるルールの修復

親オブジェクトからプロパティを継承しているオブジェクトに基づく監査ルールを作成した場合、ルールを修復すると、ターゲットサーバーのオブジェクトは親オブジェクトのプロパティを継承しないことに注意してください。

例: レジストリエントリに対するルールを作成し、そのレジストリエントリが親から値を継承している場合、ターゲットサーバーに対してルールを修復すると、親から継承された値は修復されず、ルールは監査結果に差異として表示されます。

また、監査がファイル、レジストリ、またはIISメタベースルールでACLをチェックしていて、ユーザーとグループのACLが存在しない場合、監査が実行されて修復が行われた後に、ターゲット上にユーザーとグループが存在しなければ、一時的なユーザーとグループが不明な名前で作成されます。次に監査を実行すると、ソースユーザーを示さない不明な名前が表示されます。

また、ソースサーバーからIISメタベースルールを作成していて、ルールで選択したメタベースオブジェクトが親メタベースオブジェクトから値を継承している場合、監査の実行後に差異が表示されます。

例: 修復を1回実行してその後に監査を再実行した場合、ソースキーが継承されておらず、属性がターゲットサーバー上での作成時にIEDを持っていると、オブジェクトは親キーの継承に基づいて作成されます。監査を再実行すると、結果ではIEDがオブジェクトの属性の差異として表示されます。

SA 5.1で作成された監査による差異が監査結果に存在する場合、SA 6.x以上にアップグレードした後で、その監査結果をアップグレードしたバージョンのSAクライアントで表示すると、監査結果リストの[差異]列に、-1個の差異という正しくない値が表示されます。実際の結果の数を表示するには、[監査結果]ウィンドウを開いて、結果のすべての差異を表示します。

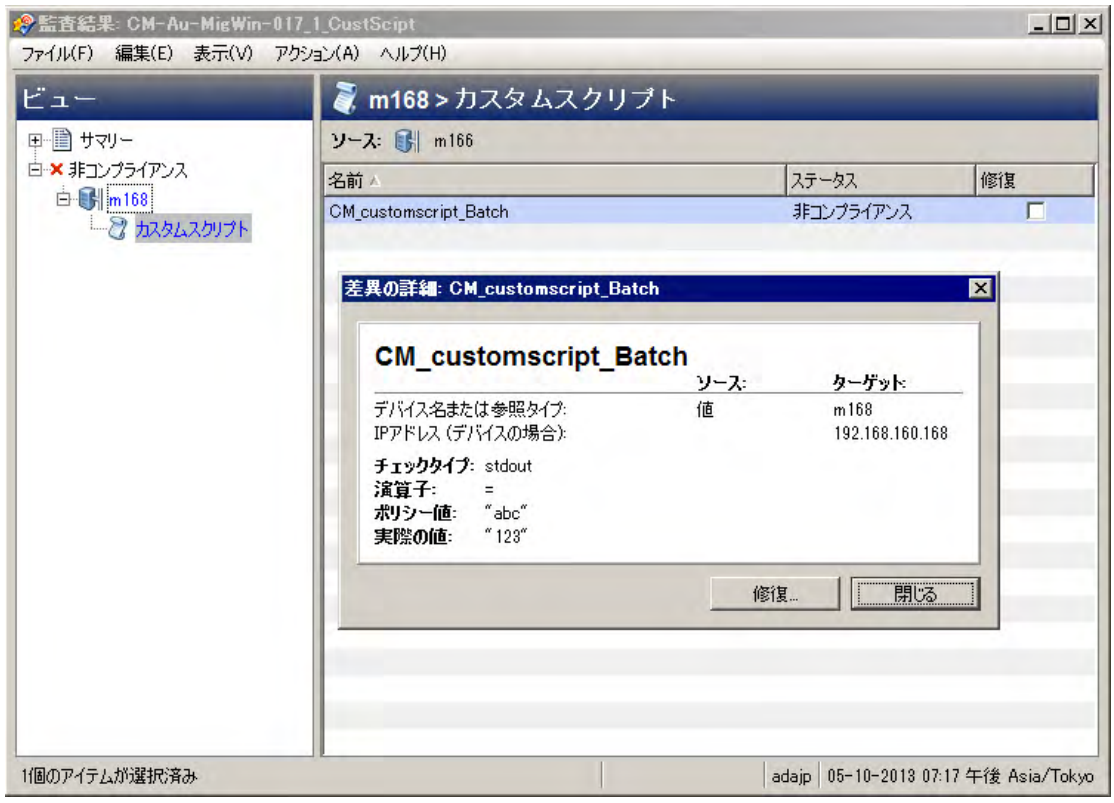
値ベースの監査結果の表示-監査ルールの修復

値ベースの監査結果は、サーバー構成が監査ルールに定義された値に一致するかどうかを示します。ルールに予期される値として定義されたものと、ターゲットサーバー上に実際に見つかった値との差異を表示できます。ルールによっては、ターゲットサーバー上に見つかった差異を、ルールに指定された値に置き換えることによって修復できます。

値ベースのルールの一部は修復不可能です。たとえば、Windows/Unixユーザーおよびグループや、プロパティ値チェックは修復できません。

図20は、カスタムスクリプト形式の値ベースの監査ルールを示します。ここでは、スクリプトの出力が、ソースサーバーに対して実行された同じスクリプトの結果と異なっています。ルールの[ステータス]列には[非コンプライアンス]と表示されています。これは、スクリプトルールの出力がソースとターゲットで異なっていることを示します。この違反を修正するには、[修復]オプションを選択し、[**アクション**]メニューから[**修復**]を選択します。または、ルールをダブルクリックして[**修復**]をクリックします。

図20　　値ベースの監査ルールの監査結果



継承された値によるルールの修復

親オブジェクトからプロパティを継承しているオブジェクトに基づく監査ルールを作成した場合、ルールを修復すると、ターゲットサーバーのオブジェクトは親オブジェクトのプロパティを継承しないことに注意してください。

例: レジストリエントリに対するルールを作成し、そのレジストリエントリが親から値を継承している場合、ターゲットサーバーに対してルールを修復すると、親から継承された値は修復されず、ルールは監査結果に差異として表示されます。

また、監査がファイル、レジストリ、またはIISメタベースルールでACLをチェックしていて、ユーザーとグループのACLが存在しない場合、監査が実行されて修復が行われた後に、ターゲット上にユーザーとグループが存在しなければ、一時的なユーザーとグループが不明な名前で作成されます。次に監査を実行すると、ソースユーザーを示さない不明な名前が表示されます。

また、ソースサーバーからIISメタベースルールを作成していて、ルールで選択したメタベースオブジェクトが親メタベースオブジェクトから値を継承している場合、監査の実行後に差異が表示されます。

例: 修復を1回実行してその後に監査を再実行した場合、ソースキーが継承されておらず、属性がターゲットサーバー上での作成時にIEDを持っていると、オブジェクトは親キーの継承に基づいて作成されます。監査を再実行すると、結果ではIEDがオブジェクトの属性の差異として表示されます。

SA 5.1で作成された監査による差異が監査結果に存在する場合、SA 6.x以上にアップグレードした後で、その監査結果をアップグレードしたバージョンのSAクライアントで表示すると、監査結果リストの[差異]列に、-1個の差異という正しくない値が表示されます。実際の結果の数を表示するには、[監査結果]ウィンドウを開いて、結果のすべての差異を表示します。

監査結果の差異の表示と修復

監査結果の一部のオブジェクトに対しては、ターゲットとソースの両方に存在し、その間に違いがあるオブジェクトの差異を表示できます。また、差異の内容を確認し、必要なら修復することもできます。

一部の監査ルールに対しては、サービスのステータス、パッチのリリース番号、レジストリキーの値など、一般的な差異を表示できます。ファイルなどのサーバーオブジェクトの場合は、ファイルの内容の差異を表示できます。

ファイルの差異の表示と修復

ファイルシステムなど、一部のルールでは、ファイルの間の差異を並べて行単位で表示できます。追加、削除、または変更された行を確認できます。

監査で差異が見つかった2つのファイルの内容を表示して修復するには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**監査と修復**] > [**監査**] を選択します。
2. 監査を選択します。
3. 監査リストの下の詳細ペインに、選択した監査に関連付けられたすべての監査結果が表示されます。
4. 監査結果を選択し、右クリックして、[**開く**] を選択します。
5. [監査結果] ウィンドウのビューペインで、ターゲットサーバーの1つを展開し、結果を選択します。
6. 内容ペインで、ターゲットサーバーを展開し、結果の1つを選択します。
7. 次に、内容ペインで、[両方にあるが異なる] タブを選択します。
8. ファイルを選択して右クリックし、[差異の表示] を選択します。

9 [比較] ウィンドウで、[エンコード] ドロップダウンリストからアイテムを選択して、表示データの文字エンコードを指定します。

問題のファイルのサイズが2MBを超える場合、監査と修復ではファイルの差異を表示できません。

10 矢印をクリックすると、追加、削除、または変更された最初の行、次の行、前の行、最後の行を表示できます。差異は次の色で表示されます。

- **緑**: 追加されたコンテンツ。
- **青**: 変更されたコンテンツ。
- **赤**: 削除されたコンテンツ。
- **黒**: 変更されていないコンテンツ。

11 このウィンドウを閉じるには、[**閉じる**] をクリックします。

12 ファイルの差異を修復するには、[監査結果] ウィンドウ内部で、[ソースのみ] タブまたは [両方にあるが異なる] タブを選択し、ファイルを選択して右クリックし、[**修復**] を選択します。

13 [サーバーの選択] ウィンドウで、ソースからファイルをコピーするサーバーを選択し、[**OK**] を選択します。

アクティブな監査結果の修復ジョブのキャンセル

SA クライアントでは、アクティブな監査結果の修復ジョブを終了できます。アクティブな監査結果の修復ジョブとは、すでに開始されて実行中のものです。

アクティブな監査結果の修復ジョブに対する終了アクションは、ソフトキャンセルと呼ばれます。ソフトキャンセルとは、ジョブが途中まで実行された状態で、[監査結果の修復] ウィザードの [ジョブステータス] ステップで [**ジョブの終了**] をクリックすることによりジョブを停止する操作です。ソフトキャンセルは、停止しようとしているアクティブな監査結果の修復ジョブだけに適用されます。

進行中の監査結果の修復ジョブをキャンセルするアクセス権が必要です。一般的に、監査結果の修復ジョブを開始するアクセス権があれば、実行中の監査結果の修復ジョブを停止することもできます。この他、「任意のジョブの編集またはキャンセル」アクセス権があれば、実行中の監査結果の修復ジョブをソフトキャンセルできます。監査関連のアクセス権の詳細については、『SA 管理ガイド』を参照してください。アクセス権の取得については、SAの管理者にお問い合わせください。

アクティブな監査結果の修復ジョブを停止するには、次の手順を実行します。

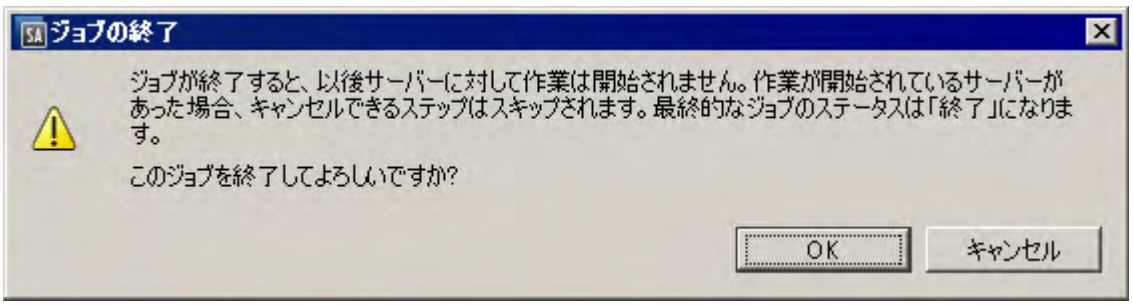
1 [ジョブステータス] ペインで [**ジョブの終了**] をクリックします

このボタンは、ジョブが実行中のときだけ使用できます。

2 [ジョブの終了] ダイアログが表示されます。このダイアログには、ジョブの終了がどのように動作するかが簡単に示されます。

- その後のサーバーに対してはジョブの作業は開始されません。
- すでに作業が開始されているサーバーに対しては、ジョブのステップのうちスキップ可能なものがキャンセルされます。
- [ジョブステータス] に、完了したステップとスキップされたステップが示されます。

3 ジョブが正常に終了した場合、最終的なジョブステータスは「終了済み」になります。



4 [**OK**] をクリックして、ジョブの終了を確認します。[ジョブステータス] ウィンドウに、終了アクションの進行状況が表示されます。

ジョブステータスは終了済みになります。サーバーステータスはキャンセルになります。タスクステータスは成功またはスキップ済みになります。

5 終了が完了したら、SAクライアントジョブログでもジョブを確認できます。

SAクライアントのナビゲーションペインで、[**ジョブとセッション**] を選択します。[ジョブログ] ビューにジョブが終了済みステータスで表示されます。

オブジェクトの差異の表示と修復

ユーザーとグループ、IIS メタベース、Windows レジストリなど、多くのサーバーオブジェクトでは、ソースオブジェクトとターゲットオブジェクトの間に差異がある場合、オブジェクトプロパティの差異を並べて表示できます。各サーバーオブジェクトは、オブジェクトの種類と、設定された監査ルールが比較ベース (ソースとターゲットの比較) か値ベース (ユーザー定義の監査ルールとターゲットの比較) かに応じて、異なるウィンドウを表示します。

一部の値ベースの監査ルールでは、ターゲットサーバー上の値を修復できます。

異なる2つのオブジェクトの内容を表示するには、次の手順を実行します。

1 ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**監査と修復**] > [**監査**] を選択します。

2 監査を選択します。

3 監査リストの下の詳細ペインに、選択した監査に関連付けられたすべての監査結果が表示されます。

4 監査結果を選択し、右クリックして、[**開く**] を選択します。

5 ビューペインで、ターゲットサーバーの1つを展開し、結果を選択します。

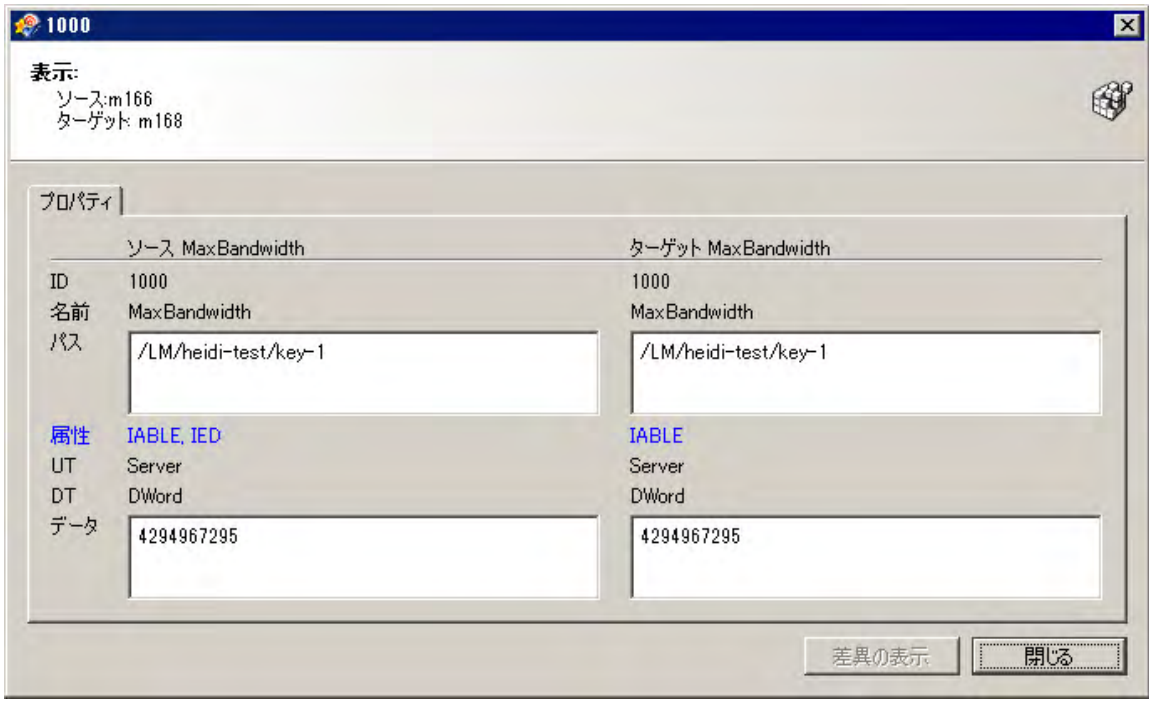
6 ビューペインでオブジェクトを選択します。

7 内容ペインで、[両方にあるが異なる] タブを選択します。

8 内容ペインで、オブジェクトを選択し、右クリックして [**開く**] を選択します。監査で定義されたオブジェクトとターゲットサーバー上のオブジェクトとの間の差異を示すウィンドウが開きます。

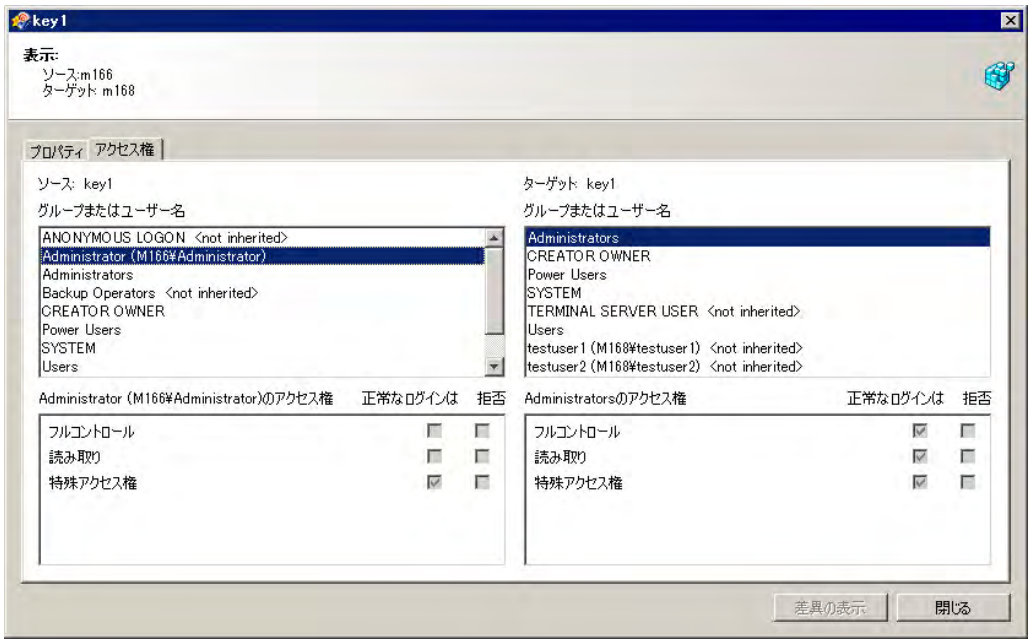
図21の例には、2つのIISメタベースオブジェクトの監査結果の差異が示されています。ここには、サーバーに存在するがソースサーバーに存在しないオブジェクトの属性が青のフォントで表示されています。

図21　　比較ベースの監査結果の差異: IISメタベースオブジェクト



値ベースのルールの場合、差異ウィンドウは多少異なり、修復が可能な場合はやはり [修復] オプションが表示されます。この差異ウィンドウには、ポリシー値を含む監査ルールと、ターゲットサーバー上に実際に見つかった値が表示されます。図22の例は、値ベースのWindowsレジストリルールでのアクセス権の差異を示します。

図22 ルールベースの監査結果の差異: Windowsレジストリのアクセス権の差異



9 差異を修復するには、各ルールの隣にある [修復] チェックマークを選択します。

10 [**アクション**] メニューから [**修復**] を選択します。

11 [修復] ウィンドウで、修復の実行またはスケジュール設定の手順を実行します。監査結果の修復の詳細については、監査結果の差異の表示と修復 (96ページ) を参照してください。

例外のある監査結果の表示

監査でルールの例外が設定されている場合、例外とされたルールは監査の実行時にターゲットサーバーでチェックされません。ただし、監査結果では、例外として処理されたルールの詳細が報告されます。

ルールの例外が監査結果にどのように表示されるかは、例外とされたルールのタイプによって異なります。

- カスタムスクリプトとカスタムまたはプラグ可能チェックのルールの例外 (開発者が作成したものやEPコンテンツサブスクリプションで提供されたものなど) は、[監査結果] ウィンドウの内容ペインに表示されます。ルールの例外をダブルクリックすると、例外の詳細情報が表示されます。
- ファイルシステム、レジストリ設定、サービス、IISメタベース、COM+ルールなど、その他すべてのルールの例外に関しては、[監査結果] ウィンドウのビューペインに例外アイコン が表示され、これを選択することで例外の詳細が内容ペインに表示されます。

監査の検索

SA クライアントの検索ツールを使用して、ファシリティ内の監査を検索できます。監査の検索には、名前、オペレーティングシステム、その他さまざまな条件が使用できます。

監査を検索するには、次の手順を実行します。

1. SAクライアントで、[**表示**] > [**検索**] ペインを選択して、検索ペインをアクティブにします。
2. ドロップダウンリストで [監査] を選択します。
3. 緑の矢印ボタンをクリックするか、[ENTER] キーを押して検索を実行します。
4. 検索結果が内容ペインに表示されます。

検索条件を拡張するには、内容ペイン上部の検索パラメーターセクションに新しい条件を追加します。[**保存**] をクリックして検索を保存したり、検索結果をエクスポートしたりできます。監査結果のエクスポート (102ページ) を参照してください。

注: 検索結果を正しく表示するには、.csv ファイルをテキストエディターで開き、ワードラップをオフにし、テキストウィンドウを水平方向に拡大します。

監査の削除

ディスクスペースを節約するため、不要になった監査を削除できます。検査の記録を保持したい場合は、監査から生成されたすべての監査結果をアーカイブするように選択できます。

監査を削除すると、それに関連付けられているすべてのスケジュールも削除されます。

監査を削除するには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**監査と修復**] > [**監査**] を選択します。
2. WindowsまたはUnixを選択します。
3. 1つ以上の監査を選択して、[**アクション**] > [**削除**] を選択します。
4. 確認ダイアログで、[**はい**] をクリックしてこの監査を削除するか、[**いいえ**] をクリックして削除を中止します。[監査のアーカイブ] オプションを選択すると、監査から生成されたすべての監査結果がアーカイブされます。アーカイブオプションを選択しないと、選択した監査からの監査結果もすべて削除されます。

監査結果の削除

ベストプラクティス: 不要になった監査結果は削除します。

スナップショットを削除するには、読み取りアクセス権が必要です。アクセス権の取得については、SAの管理者にお問い合わせください。詳細については、『SA 管理ガイド』を参照してください。

監査結果を削除するには、次の手順を実行します。

1. 1つまたは複数のスナップショットを選択して、[**アクション**] > [**削除**] を選択します。
2. 確認ダイアログで、[**はい**] をクリックしてこのスナップショットを削除するか、[**いいえ**] をクリックして削除を中止します。
3. スナップショットを削除するのでなくアーカイブするには、スナップショットを選択して右クリックし、[**アーカイブ**] を選択します。

スナップショットを削除しても、その作成に使用されたスナップショット仕様は削除されません。スナップショット仕様の削除 (115ページ) を参照してください。

監査結果のアーカイブ

ベストプラクティス: 一部の監査は大量の結果を生成します。特に、定期的に実行するようにスケジュール設定されているものはそうです。ある監査からのすべての監査結果の記録を保持するには、すべての監査結果をアーカイブします。監査結果をアーカイブすると、SAは監査結果と元の監査との関係を削除します。ただし、結果と監査のターゲットは影響されません。

監査結果をアーカイブするには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**監査と修復**] > [**監査**] を選択します。
2. オペレーティングシステムを選択します(WindowsまたはUnix)。
3. 監査を選択します。
4. 監査リストの下の詳細ペインに、選択した監査に関連付けられたすべての監査結果が表示されます。
5. 監査結果をアーカイブするには、監査結果を選択して右クリックし、[**アーカイブ**] を選択します。
6. [監査結果のアーカイブを続行しますか?] ウィンドウで、監査結果をアーカイブして監査への参照を削除するかどうかを確認します。[**はい**] をクリックすると、監査結果がアーカイブされ、結果と監査との間のリンクが削除されます。
7. アーカイブされた監査結果をすべて表示するには、ナビゲーションペインで [**ライブラリ**] > [**タイプ別**] > [**監査と修復**] > [**アーカイブされた監査結果**] を選択します。

監査結果のエクスポート

監査結果は、CSVまたはHTML形式でエクスポートできます。

監査結果をエクスポートするには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**監査**] を選択します。
2. WindowsまたはUnixを選択します。
3. 監査を選択します。監査リストの下のパネルに、監査結果が表示されます。
4. 監査結果を右クリックします。
5. [開く] を選択します。
6. [監査結果] ウィンドウで、[**アクション**] > [**エクスポート**] を選択します。
7. **CSV**、**HTML**のいずれかの形式を選択します。
8. [エクスポート] ウィンドウで、フォルダーにエクスポートされる内容、ファイル名、エンコードタイプ、ファイルタイプを選択します。
9. [**エクスポート**] をクリックします。

   エクスポート進行状況バーが表示されます。このとき、ステータスバーは不確定モードであり、ステータスバーには以下のメッセージが表示されます。「データを取得しています...」。その後、SAはサーバーに接続されます。接続が確立された時点で、完了したエクスポートタスクの数に基づいて、エクスポート進行状況ステータスがバーに表示されます。
10. エクスポートの進行を停止するには、[停止] をクリックします。
11. 進行状況ウィンドウを閉じて、バックグラウンドでエクスポート処理の実行を継続するには、[バックグラウンドで実行] をクリックします。

    [バックグラウンドで実行] をクリックすると、右下隅に一時ウィンドウが数秒間表示されます。この一時ウィンドウのリンクをクリックすると、進行状況バーが再表示されます。

12 エクスポートのタイプがHTML以外の場合、エクスポート処理の完了時に進行状況バーの表示を閉じるには、[閉じる]をクリックします。

監査のエクスポートタイプがHTMLの場合は、エクスポートプロセスが完了した時点で進行状況ウィンドウが自動的に閉じて、監査結果がブラウザーに表示されます。

13 ファイルを開いて、エクスポートされた情報を表示します。

注: エクスポートされたCVS情報を正しく表示するには、.csvファイルをテキストエディターで開き、ワードラップをオフにし、テキストウィンドウを水平方向に拡大します。

第3章 スナップショット、スナップショット仕様、スナップショットジョブ

スナップショット

スナップショットには、特定の時点での管理対象サーバーの構成がキャプチャーされます。また、既知の稼働 (または既知の停止) サーバーの現在の状態を取得する手段を提供します。スナップショットは、適切な構成状態を表すサーバー構成を取得するのに役立ちます。

ベストプラクティス: 監査のスナップショットを使用して、スナップショットをファシリティ内の他のサーバーと比較することも可能です。

また、スナップショットは管理対象サーバーのバックアップにも役立つ機能です。特に、サーバーに変更を加える予定があり、変更前に記録を残しておきたい場合に有効です。

管理対象サーバー上のオブジェクトに関する情報を記録するほか、スナップショットには一部のオブジェクトの内容を保持することもできます。サーバースナップショットは、Windows レジストリや Windows サービス、アプリケーション構成、COM+オブジェクト、ハードウェア情報、インストール済みのパッチなど、特定の種類のオペレーティングシステム上にあるその他のオブジェクトの属性も識別します。ターゲット管理対象サーバーからデータを収集するカスタムスクリプトを作成することもできます。

SA クライアントでは、Windows レジストリ全体のスナップショットやシステムキー全体のスナップショットは作成できません。これは、現在の設計で対応可能なデータサイズを超えてしまうからです。

スナップショットのソースまたはターゲットに、VMware ESXiサーバーは指定できません。

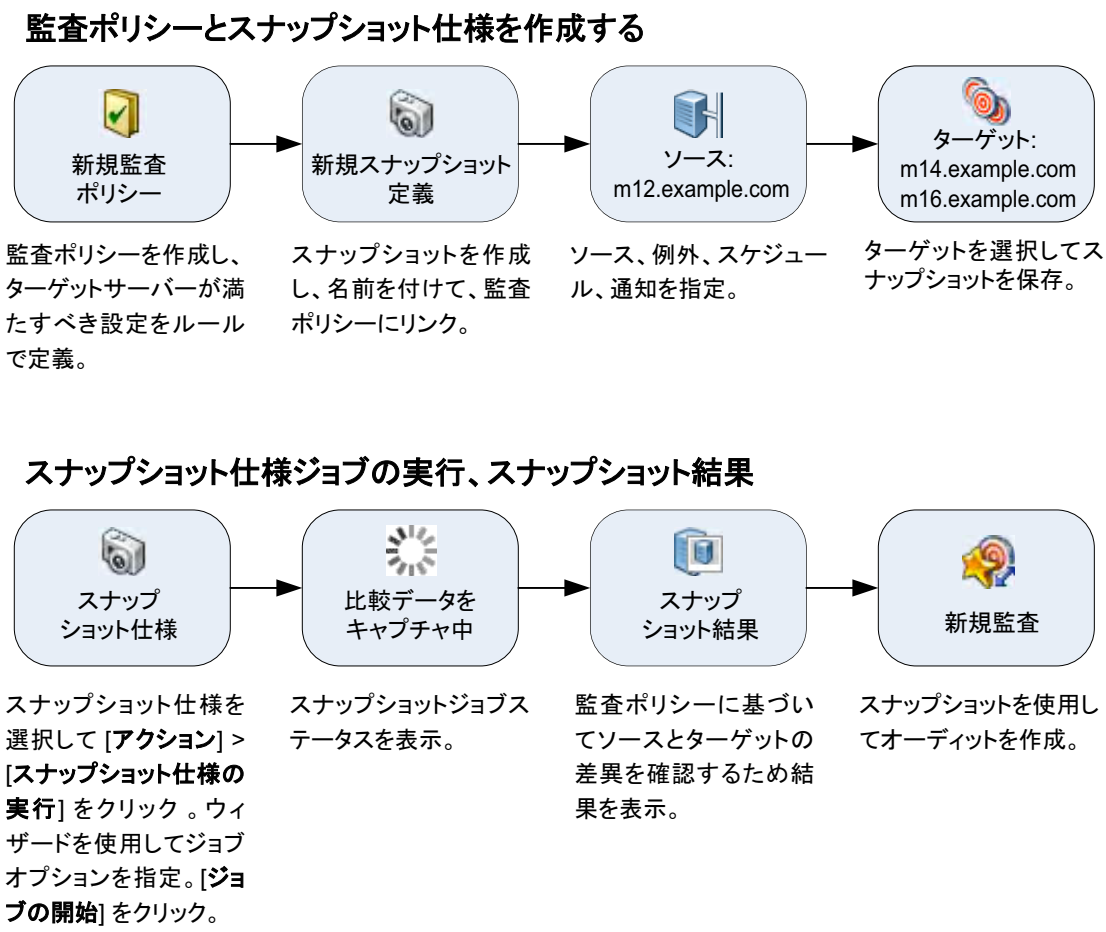
スナップショットのプロセス

サーバー構成のスナップショット作成は、次の手順で行います。

- スナップショット仕様を作成します。これは、ターゲットサーバー上で取得する構成パラメーターを定義するテンプレートです。
- スナップショット仕様のジョブを実行して、スナップショットを取得します。

図23で、スナップショットのプロセスを詳しく説明します。

図23　　スナップショットのプロセス



スナップショットとスナップショット仕様

スナップショットは、監査の構成と同じ方法で構成されます。初めに、スナップショット仕様を作成します。これは、サーバーの構成について、取得したい内容を具体的に定義するテンプレートのようなものです。次に、スナップショット仕様のルールを構成したら、実行します。その結果、得られるものが、サーバーの構成を表すスナップショットです。スナップショットと監査の主な違いは、スナップショットがサーバーの構成を写し取るのに対し、監査はサーバー構成を定義したルールの値と比較することです。

スナップショットを作成するタイミングは、特定の日時または定期的ジョブとして指定できます。また、ジョブのステータスに関する電子メール通知の送信先も指定できます。

監査で使用するスナップショット

スナップショットを監査で使用して、管理対象サーバーやサーバーグループ、スナップショットの比較ができます。スナップショットを監査で使用すれば、問題のあるサーバー (監査のターゲット) を既知の稼働サーバー (監査のソースとしてスナップショットを取得) と比較できます。監査の定義をさらに広げて、サーバーオブジェクトに対するルールも定義できます。

スナップショットを監査のソースとして使用する場合は、スナップショット結果で取得されるすべてのサーバー構成値を監査のルールとして使用できます。監査でのスナップショット使用に関する詳細については、監査の構成 (29ページ) を参照してください。

監査で使用するスナップショット仕様

サーバーの構成履歴を維持し、すべての変更を監視したい場合は、スナップショット仕様を監査のソースとして使用できます。たとえば、特定のアプリケーションについて履歴を維持し、一定の期間、構成が正常な状態を保っているかを確認したいとします。このアプリケーションを数台のサーバーで実行している場合、適切なサーバー構成状態を定義するスナップショット仕様を作成して、スナップショットを実行できます。

次に、監査を作成し、元のスナップショット仕様を監査のソースとして使用できます。スナップショットでターゲットとした各サーバーは、これで監査のターゲットにも含まれます。次に、必要に応じて、またはスケジュールに基づき監査を実行する際に、各サーバーの現在の構成が、最初のスナップショットを取得したときの状態と比較されます。変更がある場合は、監査結果ウィンドウに表示されます。監査の構成 (29 ページ) を参照してください。

スナップショット仕様の要素

スナップショット仕様は、次の要素で構成されます。

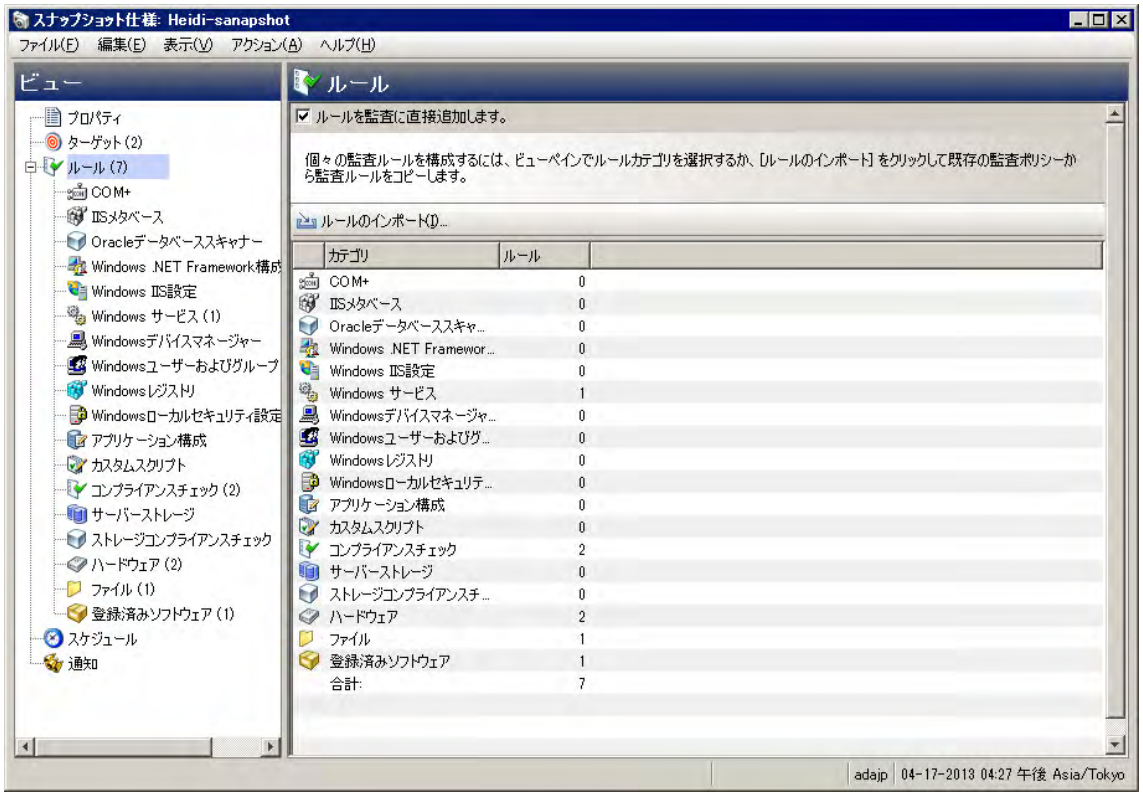
- **プロパティ**: スナップショット仕様の名前および説明。スナップショット仕様のインベントリを作成するには、[インベントリの実行] を選択します。これにより、スナップショット結果として、ターゲットサーバーから指定したルールの情報がすべて収集されます。このオプションを使用できるのは、検出されたソフトウェア、Internet Information Server、ローカルセキュリティ設定、登録済みソフトウェア、Windowsユーザーおよびグループ、Unixユーザーおよびグループの各ルールです。
- **ターゲット**: スナップショットの取得対象となるサーバー。スナップショット仕様のルールの定義に従って、特定のサーバー構成を取得します。選択可能なサーバーとサーバーグループの数には制限はありません。
- **ソース**: スナップショット仕様のソース。サーバーを指定して、そのサーバーからスナップショットのベースとなるサーバーオブジェクトを選択できます。サーバーをスナップショット仕様のソースに指定するか、ソースを何も指定しないこともできます。(一部のルールでは、ソースサーバーが必要です。ソースの指定が不要で、独自のカスタム値で定義が可能なルールもあります。)
- スナップショット取得の際に、ソースのパラメーター値は使用しないことに注意してください。ソースのパラメーター値は、スナップショット仕様を定義する際に使用します。
- **ルール**: 特定のサーバーオブジェクトに対するチェックで、必要な値とオプションの修復値を備えています。たとえば、サーバーに特定の Windows サービスが含まれるかチェックします。見つかった場合は、サービスがオフになっているか確認します。スナップショット仕様でルールを定義できるサーバーオブジェクトの説明については、監査と修復のルール (35ページ) を参照してください。

- **スケジュール**: スナップショットを実行する時刻。スナップショット仕様をジョブとして、1回のみ、または定期的スケジュールで実行できます。
- **通知**: スナップショットの実行後に送られる電子メール通知。通知の送信は、成功時、失敗時、または単にスナップショット仕様ジョブの完了時ベースのように指定できます。

スナップショット仕様を設定する際は、ターゲットサーバー上でチェックするオブジェクトを選択します。また、適切な構成状態を定義するルールを、これらのオブジェクトに適用することもできます。一部のルールについては、結果のスナップショットを監査のソースとして使用する場合に、修復値を定義できます。

図24は、イベントロギングやオペレーティングシステム、Windowsサービスなど、ターゲットサーバーの構成情報を取得する3つのルールをもつスナップショット仕様を示しています。

図24　　スナップショット仕様のサーバーオブジェクト



スナップショットの表示

作成したスナップショットは、SAクライアントのいくつかの場所で表示できます。

SAライブラリに表示

特定のサーバーに関するスナップショットを表示するには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**監査と修復**] > [**スナップショット仕様**] を選択します。
2. オペレーティングシステムを選択します (WindowsまたはUnix)。
3. リストからスナップショット仕様を選択します。詳細ペインに、選択したスナップショット仕様で実行されたすべてのスナップショットが表示されます。

デバイスエクスプローラーに表示

特定のサーバーに関するスナップショットを表示するには、次の手順を実行します。

1. ナビゲーションペインで、[**デバイス**] > [**サーバー**] > [**すべての管理対象サーバー**] を選択します。
2. リストからサーバーを選択して右クリックし、[**開く**] を選択します。
3. [デバイスエクスプローラー] ウィンドウで、[**インベントリ**] > [**スナップショット仕様**] を選択します。
4. 内容ペインで、スナップショット仕様を選択します。詳細ペインには、関連するすべてのスナップショットが表示されます。
5. スナップショットを表示するには、ペインから選択してダブルクリックし、開きます。

スナップショットの検索

SA クライアントの検索ツールを使用して、ファシリティ内のスナップショットを検索できます。スナップショットの検索には、名前、オペレーティングシステム、その他さまざまな条件が使用できます。

スナップショットを検索するには、次の手順を実行します。

1. SAクライアントで、[**表示**] > [**検索ペイン**] を選択します。
2. ドロップダウンリストからスナップショットを選択します。
3. 緑の矢印をクリック、または [ENTER] キーを押して、検索を開始します。検索結果が内容ペインに表示されます。

   検索条件を広げるには、内容ペインの上部にある検索パラメーターセクションで条件を追加します。また、検索を保存したり、検索結果を.htmlファイルまたは.csvファイルにエクスポートしたりすることもできます。

注: 結果を正しく表示するには、.csvファイルをテキストエディターで開き、テキストの折り返しをオフにして、テキストウィンドウを水平に広げてください。

スナップショット結果の表示

スナップショットの内容を表示したり、記録されたサーバー構成の詳細情報を表示したりすることができます。

スナップショット結果の修復については、オブジェクトのコピー (113ページ) を参照してください。

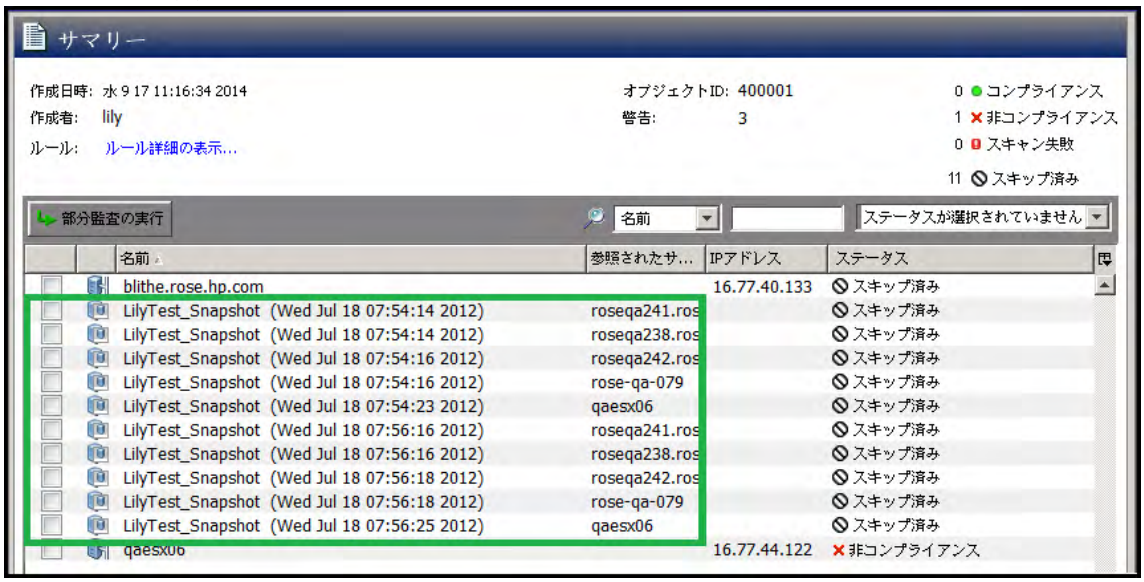
スナップショットの内容を表示するには、次の手順を実行します。

1 スナップショットの表示 (109ページ) で説明したいずれかの開始点から、スナップショットを開きます。

図25 Windowsサーバーのスナップショット

2 [スナップショット] ウィンドウでは、ビューペインで次のサーバーオブジェクトを選択または展開できます。

- **サマリー**: スナップショットの一般的な情報として、スナップショットの作成日時と作成者、スナップショットのソース (管理対象サーバーの名前)、スナップショットファイルのサイズ、スナップショットID番号、スナップショット結果が参照するサーバー、そのサーバーのIPアドレスなどを表示します。



[**ルール詳細の表示**] をクリックして、このスナップショットの元となったスナップショット仕様を見ることもできます。

- **コンプライアンスライブラリ**： スナップショット仕様で構成される特定のコンプライアンスチェックに関する情報。利用可能なBSA Essentialsサブスクリプションサービスのコンプライアンスチェックの種類と、それらの構成方法の詳細については、コンプライアンスチェックの構成 (65ページ) を参照してください。
- **インストール済みハードウェア**: CPUプロセッサーのタイプと速度、キャッシュサイズ、SWAPメモリとRAMメモリの容量、ストレージデバイスなど、スナップショットに記録されている情報。
- **インストール済みのパッチ**: パッチタイプなど、スナップショットに記録されているインストール済みのパッチに関する情報を表示します。
- **インストール済みのパッケージ**: パッケージタイプ、パッケージバージョン、リリース番号など、スナップショットに記録されているインストール済みのパッケージに関する情報を表示します。
- .zip パッケージについては、スナップショットはバージョン番号を表示しません。代わりに、サーバー上のパッケージのインストールパスを表示します。
- **イベントロギング**: スナップショットに記録されているセキュリティ、アプリケーション、システムの各ログファイルを表示します。
- **ファイルシステム**: スナップショットに記録されているディレクトリ、ファイルプロパティ、属性、ファイルの内容を表示します。

スナップショットのファイルサイズが2MBを超える場合、監査と修復ではファイルの内容を表示できません。

- **Windowsサービス**: スナップショットに記録されている実行サービスについて、サービスの名前、説明、スタートアップ状態、スタートアップタイプ、ログインアカウントなどの情報を表示します。
- **Windowsレジストリ**: スナップショット内にあるWindowsレジストリエントリについて、レジストリキー、レジストリの値、サブキーなどの情報を表示します。レジストリキーは、レジストリ値を含むディレクトリです。ここでは、レジストリ値がディレクトリ内のファイルと同様になります。サブキーはサブディレクトリのようなものです。このウィンドウのコンテンツ領域には、サブキーは含まれません。監査と修復でサポートされるWindowsレジストリキーは、HKEY_CLASSES_ROOT、HKEY_CURRENT_CONFIG、HKEY_LOCAL_MACHINE、HKEY_USERSです。
- **COM+**: スナップショット内のWindows COM (コンポーネントオブジェクトモデル) オブジェクトについて、オブジェクトの名前とGUID (Globally Unique Identifier)、処理中のサーバー DLLへのパスなどの情報を表示します。
- SAは、Windows COMフォルダーの処理方法を説明する警告メッセージを出します。これは、次のようなシナリオに適用されます。
- スナップショットを作成して、オブジェクトが1つも存在しないWindows COMフォルダーを選択すると、スナップショットウィンドウにサマリーが表示されます。SAは、そのフォルダーのGUID (Globally Unique Identifier) が無効であることを示す警告を表示します。これは、Windows COMフォルダーにオブジェクトが1つも存在しないことを意味します。
- スナップショット仕様を作成して、ターゲット上に存在しないWindows COM+オブジェクトを選択すると、SAはそのフォルダーが無効であることを示す警告を表示します。
- スナップショットを作成して、オブジェクトが1つも存在しないWindows COMフォルダーを選択すると、SAはそのフォルダーが空であることを示す警告を表示します。
- **メタベース**: スナップショット内のIISメタベースオブジェクトについて、オブジェクトのID、名前、パス、属性、データを表示します。
- **カスタムスクリプト**： スナップショットに記録されているカスタムスクリプトのルールに関する情報を表示します。
- **ユーザーとグループ**： サーバー上のユーザーとグループについて、最終ログインしたユーザー名、[CTRL]+[ALT]+[DELETE] の有効または無効などの情報を表示します。

3 [**閉じる**] をクリックして、オブジェクトブラウザーを閉じます。

スナップショットのアーカイブ

一部のスナップショット仕様、特に定期的に実行するようスケジュール済みの仕様は、数多くのスナップショットを生み出します。すべてのスナップショットはアーカイブが可能で、サーバーやサーバーグループに対して実行したすべてのスナップショットの履歴を保存することができます。

スナップショットをアーカイブする際は、そのスナップショットをサーバーからデタッチし、元のスナップショット仕様への接続を削除します。

スナップショットをアーカイブするには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**監査と修復**] > [**スナップショット仕様**] を選択します。
2. オペレーティングシステムを選択します (WindowsまたはUnix)。
3. スナップショット仕様を選択します。
   詳細ペインに、選択したスナップショット仕様に関するすべてのスナップショットが表示されます。
4. スナップショットをアーカイブするには、スナップショットを選択して右クリックし、[**アーカイブ**] を選択します。
5. [**はい**] をクリックして、スナップショットをアーカイブするかどうかを確認します。これは、アーカイブによってスナップショットとスナップショット仕様の関連が削除されるためです。
6. アーカイブされたスナップショット結果をすべて表示するには、ナビゲーションペインで [**ライブラリ**] > [**タイプ別**] > [**監査と修復**] > [**アーカイブされたスナップショット**] を選択します。

スナップショットの削除

ベストプラクティス: スナップショットは不要になった場合のみ、ソフトウェアリポジトリから削除します。これにより、ディスク容量を節約できます。

スナップショットを削除するには、読み取りアクセス権が必要です。アクセス権の取得については、SAの管理者にお問い合わせください。詳細については、『SA 管理ガイド』を参照してください。

スナップショットを削除するには、次の手順を実行します。

1. 1つまたは複数のスナップショットを選択して、[**アクション**] > [**削除**] を選択します。
2. 確認ダイアログで、[**はい**] をクリックしてこのスナップショットを削除するか、[**いいえ**] をクリックして削除を中止します。
3. スナップショットを削除するのでなくアーカイブするには、スナップショットを選択して右クリックし、[**アーカイブ**] を選択します。

スナップショットを削除しても、その作成に使用されたスナップショット仕様は削除されません。スナップショット仕様の削除 (115ページ) を参照してください。

スナップショットのエクスポートとインポート

スナップショットフィルターを使用して、SAコア/メッシュからエクスポートするスナップショットをDETで指定します。これにより、エクスポートした内容を別のSAコア / メッシュにインポートできます。スナップショットフィルターの詳細については、『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。

オブジェクトのコピー

スナップショットからサーバーへ

スナップショットの内容を表示したら、特定のオブジェクトをターゲットサーバーにコピーできます。SAでは、ディレクトリ、ファイル、Windowsサービス(状態のみ)、IISメタベースオブジェクト、COM+オブジェクトとカテゴリ、Windowsレジストリキーを、管理対象サーバーにコピーできます。

オブジェクトをコピーするには、コピー先サーバーへの書き込みアクセス権が必要です。アクセス権の取得については、SAの管理者にお問い合わせください。アクセス権の詳細については、『SA 管理ガイド』を参照してください。

COM+ルールのスナップショット結果をスナップショットからサーバーにコピーするには、COM+ルールの構成時に「関連するすべてのファイルのアーカイブ」オプションを選択しておく必要があります。また、コピー対象のCOM+オブジェクトは、コピー先の修復を正常に実行するため、どのアプリケーションでも使用中ではない必要があります。COM+ルールの構成 (41ページ) を参照してください。

これらのオブジェクトを管理対象サーバーにコピーする前に、コピー先サーバーに実際にどのようなオブジェクトがコピーまたは作成されるかを確認してください。

- ディレクトリを選択すると、ディレクトリのみがサーバーにコピーされ、ディレクトリ内のファイルはコピーされません。たとえば、dir1にfile1とfile2が格納されていて、dir1を選択した場合、監査と修復はdir1のみサーバーにコピーします(file1とfile2はコピーされません)。
- ファイルを選択して、親ディレクトリがコピー先サーバーに存在しない場合、監査と修復はサーバー上にディレクトリを作成してファイルをコピーします。たとえば、file1を選択して、dir1がコピー先サーバーに存在しない場合、監査と修復はサーバー上にdir1を作成してfile1をコピーします。
- Windowsサービスオブジェクトをコピーする場合、開始済み、停止済み、一時停止済みなど、サービスの状態がコピーされます。1回のコピープロセスで、1つ以上のWindowsサービスオブジェクトを選択できます。
- Windowsレジストリオブジェクトをコピーする場合、1回のコピープロセスで、1つ以上のレジストリキーおよびサブキーを選択できます。
- ACLは、COM+オブジェクトまたはMicrosoft IISオブジェクトとともに、ターゲットサーバーにコピーされません。
- [コピー先]を使用してスナップショット結果からCOM+オブジェクトを修復する場合、SAクライアントはCOM+オブジェクトのバージョンをチェックしません。そのため、オブジェクトに差異があるかどうかに関わらず、常にそのオブジェクトがコピーされます。

オブジェクトをスナップショットから管理対象サーバーへコピーするには、次の手順を実行します。

1 スナップショットを開きます。スナップショットの表示 (109ページ) を参照してください。

2 [ビュー] ペインで、ファイルシステム、Windows サービス、Windows レジストリオブジェクトを選択します。

3 内容ペインで、コピーするオブジェクトを1つ以上選択します。

4 [**アクション**] > [**コピー先**] を選択します。

5 [サーバーの選択] ウィンドウで、コピー先サーバーを選択します。

 検索ツールを使用して、サーバー名、IPアドレス、またはオペレーティングシステムを入力することで、このリストを動的にフィルター処理します。

6 [**選択**] をクリックしてオブジェクトを管理対象サーバーにコピーするか、[**キャンセル**] をクリックして変更を保存せずにウィンドウを閉じます。

注: 監査、監査結果の修復、スナップショットジョブの作成では、ソフトキャンセルがサポートされています。しかし、スナップショットからサーバーへの [コピー先] などのスナップショット修復ジョブでは、ソフトキャンセルがサポートされていません。

スナップショット仕様

SAクライアントでは、次のタスクを実行してスナップショット仕様を管理できます。

- スナップショット仕様と監査ポリシー (114ページ)
- スナップショット仕様の作成 (115ページ)
- スナップショット仕様の削除 (115ページ)
- スナップショット仕様の構成 (116ページ)
- スナップショット仕様ルールの構成 (118ページ)
- 監査ポリシーとしてのスナップショット仕様の保存 (118ページ)
- スナップショット仕様の実行 (118ページ)
- 定期的なスナップショットジョブのスケジュール設定 (119ページ)

スナップショット仕様と監査ポリシー

監査ポリシーは、サーバーの適切な構成状態を定義するルールの集まりです。監査ポリシーは、リンクまたはインポートを通じてスナップショット仕様内で使用できます。監査ポリシーにより、ポリシー設定担当者はサーバー構成コンプライアンスの値を定義できます。また、定義した値は、他のユーザーがスナップショット仕様で使用できるので便利です。

監査ポリシーは監査またはスナップショット仕様とリンクできるため、ポリシーを変更すると、そのポリシーを使用している監査またはスナップショット仕様にも、最新の変更が反映されます。または、ソースの監査ポリシーへのリンクを持たずに、監査ポリシーをスナップショット仕様にインポートすることもできます。監査ポリシーをスナップショット仕様にインポートする際は、監査内の現在の値を置換したり、監査ポリシーの値をスナップショット仕様の値とマージしたりすることも選択できます。

スナップショット仕様の作成

スナップショット仕様は、SAクライアントの次の場所から作成できます。

- サーバーから (115ページ)
- SAライブラリから (115ページ)

スナップショット仕様を作成または変更するには、適切なアクセス権が必要です。これらのアクセス権の取得については、SA管理者にお問い合わせください。アクセス権の詳細については、『SA 管理ガイド』を参照してください。

サーバーから

新しいスナップショット仕様を管理対象サーバーから作成する場合、スナップショット仕様では選択したサーバーをソースとして使用します。ルールを定義する際、スナップショット仕様に異なる数台のサーバーをソースとして選択できます。または、ソースを1台も選択せず、独自のカスタムルールを定義することも可能です。ただし、ルールによってはソースが必須のものもあります。

管理対象サーバーのスナップショットを取るには、サーバーに到達可能で、サーバーへのアクセス権をもつ必要があります。

サーバーからスナップショット仕様を作成するには、次の手順を実行します。

1. ナビゲーションペインで、[**デバイス**] > [**サーバー**] > [**すべての管理対象サーバー**] を選択します。
2. サーバーを選択して、[**アクション**] > [**スナップショット仕様の作成**] を選択します。

SAライブラリから

新しいスナップショット仕様を作成し、すべてに独自のルールを設定する場合は、次の手順を実行してSAクライアントライブラリから監査を作成します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**監査と修復**] を選択します。
2. ナビゲーションペインで、スナップショット仕様を選択して、WindowsまたはUnixを選択します。

スナップショット仕様の削除

ディスク容量を節約するため、不要になったスナップショット仕様を削除できます。スナップショット結果の履歴を保存したい場合は、スナップショット仕様から作成されたすべてのスナップショットのアーカイブを選択できます。または、スナップショット仕様とそれに関連するすべてのスナップショットの削除も選択できます。

スナップショット仕様を削除するには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**監査と修復**] > [**スナップショット仕様**] を選択します。
2. WindowsまたはUnixを選択します。
3. 1つまたは複数のスナップショット仕様を選択して、[**アクション**] > [**削除**] を選択します。
4. 確認ダイアログで、[**はい**] をクリックしてこのスナップショット仕様を削除するか、[**いいえ**] をクリックして削除を中止します。また、[スナップショットのアーカイブ] オプションを選択して、スナップショットで作成されたすべてのスナップショットをアーカイブすることもできます。アーカイブオプションを選択しない場合、選択したスナップショット仕様から作成されたすべてのスナップショットが削除されます。

スナップショット仕様を削除すると、それに関連するすべてのスケジュールも削除されます。スナップショットジョブ (119ページ) を参照してください。

スナップショット仕様の構成

スナップショット仕様の構成は、次の手順で行います。

- スナップショット仕様に名前と説明を付け、インベントリを実行するかどうかを決定します。
- スナップショットを取りたいターゲットサーバーを選択します。複数のサーバー、またはサーバーグループのスナップショットを取ることも選択できます。
- 独自のカスタムルールを構成するか、スナップショット仕様ルールのベースとなるソースサーバーの設定を選択します。
- スナップショット仕様ジョブをスケジュールし、特定の日時または定期的スケジュールで実行します。
- 電子メール通知の設定をし、スナップショット仕様ジョブが正常に完了したとき、ジョブが失敗したとき、または両方の条件でユーザーに通知します。
- スナップショット仕様を保存します。

COM+オブジェクトのスナップショットを32ビットWindowsサーバーから取得し、Windows 64ビットサーバー上で [コピー先] を使用して結果を修復する場合、このアクションは失敗する場合があります。

監査またはスナップショットのターゲットにVMware ESXiサーバーは指定できません。

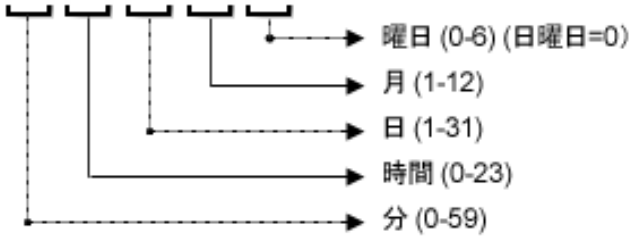
スナップショット仕様を構成するには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**監査と修復**] を選択します。
2. ナビゲーションペインで、[スナップショット仕様] を選択して、WindowsまたはUnixを選択します。
3. [**アクション**] メニューから [**新規**] を選択します。
4. [スナップショット仕様] ウィンドウに次の情報を入力します。
   - **プロパティ**: スナップショット仕様の名前と説明を入力します。また、特定のスナップショット仕様のルール (検出されたソフトウェア、Internet Information Server、ローカルセキュリティ設定、パッケージとパッチ、Windowsユーザーおよびグループ、Unixユーザーおよびグループ) については、[インベントリの実行] オプションを選択できます。これにより、そのルールと関連するすべてのリソースを取得できます。
   - **ソース**: スナップショット仕様のソースを選択します。デフォルトでは、スナップショット仕様のソースサーバーは、スナップショット仕様のソースとして選択した管理対象サーバーになります。ソースサーバーの値を参照して、スナップショット仕様のルールを読み込みます。また、各ルールカテゴリのスナップショット仕様のベースに、異なるソースサーバーを選択することもできます。ソースを指定しないことも可能です。ソースを指定しない場合は独自のルールを定義するか、ルールセクション内の監査ポリシーへのリンクを選択する必要があります。
   - **ルール**: リストからルールカテゴリを選択して、スナップショット仕様のルールの構成を開始します。各ルールは固有で独自の手順が必要となるため、特定のルールの構成については、監査と修復のルール (35ページ) を参照してください。

     監査ポリシーを使用して、スナップショット仕様のルールを定義する場合は、[**ポリシーのリンク**] または [**ポリシーのインポート**] をクリックします。監査ポリシーにリンクする場合、スナップショット仕様はその監査ポリシーと直接接続を維持します。そのためポリシーが変更されると、新規の変更でスナップショット仕様を更新します。監査ポリシーをインポートする場合、スナップショット仕様ではポリシー内で定義されているすべてのルールを使用し、監査ポリシーへのリンクは維持しません。スナップショット仕様のインポートまたはリンク方法については、監査ポリシーのリンクとインポートの方法 (82ページ) を参照してください。

- **ターゲット**: スナップショット仕様のターゲットを選択します。ターゲットは、構成済みスナップショット仕様のルールで取得するサーバーまたはサーバーグループです。サーバーまたはサーバーグループを追加するには、[**追加**] をクリックします。使用するソースサーバーを選択して、スナップショット仕様のルールを作成するには、[**選択**] をクリックします。
- **スケジュール**: スナップショット仕様をただちに実行するか、定期的スケジュールで実行するかを選択します。1 回、毎日、毎週、毎月、指定のスケジュールから希望するものを選択します。次のパラメーターを指定します。
- **なし**: スケジュールは設定されません。スナップショット仕様を実行するには、スナップショット仕様を選択して右クリックし、[**スナップショット仕様の実行**] を選択します。
- **毎日**: スナップショット仕様を指定した時刻に毎日実行します。
- **毎週**: スナップショット仕様を実行する曜日を選択します。
- **毎月**: スナップショット仕様を実行する月を選択します。
- **カスタム**: [カスタムcrontab文字列] フィールドに、スケジュールを示す文字列を入力します。

  crontab ファイルには5つのフィールドがあり、曜日、月、日、そして時間と分を指定します。次の図は、crontabファイル内の各位置とそれぞれに対応するもの、設定できる値を示しています。



  crontab 文字列は、シリアル値 (1、2、3、4) と範囲 (1-5) で指定できます。一部のオペレーティングシステムでは、監査を2分ごと、または10分ごとに実行する場合に、/2または/10のような形式で分を指定します。アスタリスク (*) は、年間のすべての月のように、そのフィールドのすべての値を意味します。日は、日にちと曜日の 2 つのフィールドで指定できます。両方の日を指定すると、両方の値が実行されます。各フィールド内のカンマ区切り値は、すべてのオペレーティングシステムでサポートされています。次に例を示します。

  5,10 0 10 * 1は、毎月10日および毎週月曜日の午前0時5分および午前0時10分に、監査を実行することを意味します。

  crontabの入力形式の詳細については、Unixのmanページを参照してください。

- **時刻と期間:** スケジュールの各タイプについて、日次スケジュールを開始する時間と分を指定します。終了時刻を指定しないと、スナップショット仕様は無期限に実行されます。終了日を選択してスナップショット仕様スケジュールを終了するには、[終了] を選択して、カレンダーから日付を選択します。[タイムゾーン] には、ユーザープロファイルで設定されているタイムゾーンが適用されます。
- **通知**: スナップショット仕様ジョブの実行が完了したときに、電子メールを送信するユーザーの電子メールアドレスを入力します (カンマまたはスペース区切り)。電子メール送信の条件として、スナップショット仕様ジョブが成功した場合と失敗した場合 (監査ルールの成功と失敗ではありません) を選択できます。電子メールアドレスを追加するには、[**通知の追加**] ルールをクリックします。

5 スナップショット仕様の構成が完了したら、[**ファイル**] メニューから [**保存**] を選択します。

増大プロセスを防ぐため、スナップショットプロセスが60分以上続くか、管理対象サーバーから回収されるデータが 1 ギガバイト (GB) を超えるとタイムアウトします。選択条件に合致するファイルのすべての内容を回収するよう指定した場合、回収データはスナップショットに正常に記録できる最大サイズを超える可能性があります。

スナップショット仕様ルールの構成

特定のスナップショット仕様ルールの構成方法については、監査と修復のルール (35ページ) を参照してください。

監査ポリシーとしてのスナップショット仕様の保存

スナップショットで使用した選択条件を、監査ポリシーとして保存できます。これは、スナップショット仕様で構成されたルールを他のスナップショット仕様または監査で使用する場合に便利です。監査ルールがターゲットサーバー上に最新のエージェントを必要とする場合、SAクライアントでは実行時のエラーを回避するために、エージェントの更新を促すメッセージを表示します。

作成したすべての監査ポリシーは、SAライブラリ内のフォルダーに保存する必要があります。監査ポリシーを保存するフォルダーに書き込むためのアクセス権が必要です。フォルダーのアクセス権の詳細については、『SAユーザーガイド: Server Automation』を参照するか、SA管理者にお問い合わせください。

監査ポリシーとしてスナップショット仕様を保存するには、次の手順を実行します。

1. SAクライアントを起動します。
2. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**監査と修復**] を選択します。
3. スナップショット仕様を選択し、監査ポリシーとして保存するスナップショット仕様をダブルクリックします。
4. [スナップショット仕様] ウィンドウで、[**ファイル**] > [**名前を付けて保存**] を選択します。
5. [名前を付けて保存] ウィンドウで、名前と短い説明を入力します。
6. [タイプ] ドロップダウンリストから、[監査ポリシー] を選択します。
7. [**保存**] をクリックします。選択したスナップショット仕様が、監査ポリシーとして保存されます。
8. 監査ポリシーを表示するには、ナビゲーションペインから [**ライブラリ**] > [**タイプ別**] >[**監査と修復**] >[**監査ポリシー**] を選択します。監査ポリシーの使用に関する詳細については、監査ポリシーの管理 (79ページ) を参照してください。

スナップショット仕様の実行

スナップショット仕様の実行時に、SAは (ターゲットサーバーから) ルール内で構成されているすべての構成パラメーターを取得します。スナップショット仕様を実行すると、スナップショットジョブの結果がスナップショットとなり、スナップショット内に表示できるようになります。

スナップショット仕様を実行するには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**監査と修復**] を選択します。
2. ナビゲーションペインで [スナップショット仕様] を選択します。
3. WindowsまたはUnixを選択します。
4. スナップショット仕様を選択して右クリックし、[**実行**] を選択します。[スナップショット仕様の実行] ウィンドウで、ステップ1にスナップショットの名前、定義済みルールの総数、そしてすべてのターゲットが表示されます。
5. [**ルール詳細の表示**] をクリックすると、ルールの定義が表示されます。
6. [**次へ**] をクリックします。

7 [スケジュール設定] ウィンドウで、監査をただちに実行するか、別の日時に実行するかを選択します。監査を後で実行するには、2番目のオプションを選択して日付と時刻を指定します。

8 [**次へ**] をクリックします。

9 [通知] ビューのデフォルト設定では、監査ジョブの成否に関係なく、監査の完了時にユーザーへ通知電子メールが送信されます。電子メールでの通知を追加するには、[**通知の追加**] をクリックして電子メールアドレスを入力します。

10 (オプション) 電子メールを、監査ジョブが成功した場合 () または失敗した場合 () のどちらに送信するかを指定できます。

11 (オプション) [チケットID] フィールドでチケットトラッキングIDを指定できます。[チケットID] フィールドが使用されるのは、HPプロフェッショナルサービスのSAが変更管理システムに統合されている場合のみです。それ以外の場合、このフィールドは空のままとします。

12 [**次へ**] をクリックします。

13 [ジョブステータス] ビューで [**ジョブの開始**] をクリックして、監査を実行します。実行完了後、[**結果の表示**] をクリックすると監査の結果が表示されます。

スナップショットジョブ

スナップショット仕様ジョブにより、SAクライアントでスナップショットを作成するタイミングを、特定の日時または定期的に実行するよう指定できます。また、ジョブのステータスに関する電子メール通知の送信先も指定できます。また、既存のスナップショット仕様のスケジュールを、表示、編集、または削除することもできます。スナップショット仕様を削除すると、そのスナップショット仕様に関連するすべてのスケジュールが削除されます。

SAクライアントでは、次のタスクを実行してスナップショットジョブを管理できます。

- 定期的なスナップショットジョブのスケジュール設定 (119ページ)
- スナップショットジョブスケジュールの表示と編集 (120ページ)
- スナップショットジョブスケジュールの削除 (122ページ)

定期的なスナップショットジョブのスケジュール設定

スナップショット仕様を作成、構成、保存したら、スナップショット仕様を定期的なスナップショットジョブとしてスケジュール設定できます。スケジュールを設定した後で、必要に応じてスケジュールを編集できます。

定期的なスナップショット仕様をスケジュール設定するには、次の手順を実行します。

1 ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**監査と修復**] > [**スナップショット仕様**] を選択します。

2 WindowsまたはUnixのいずれかを選択します。

3 スナップショットを選択してダブルクリックし、開きます。

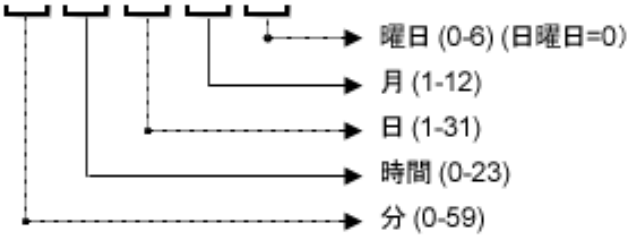
4 [スナップショット仕様] ウィンドウの [ビュー] ペインで、[スケジュール] を選択します。

5 [スケジュール] セクションで、スナップショットジョブをただちに実行するか、定期的スケジュールで実行するかを選択します。1回、毎日、毎週、毎月、指定のスケジュールから選択します。

- **なし**: スケジュールは設定されません。スナップショットジョブを実行するには、スナップショット仕様を選択して右クリックし、[**監査の実行**] を選択します。

- **毎日**: スナップショットジョブを指定した時刻に毎日実行します。
- **毎週**: スナップショット仕様ジョブを実行する曜日を選択します。
- **毎月**: スナップショット仕様ジョブを実行する月を選択します。
- **カスタム**: [カスタムcrontab文字列] フィールドに、スケジュールを示す文字列を入力します。

  crontabファイルには5つのフィールドがあり、曜日、月、日、そして時間と分を指定します。次の図は、crontabファイル内の各位置とそれぞれに対応するもの、設定できる値を示しています。



  crontab 文字列は、シリアル値 (1、2、3、4) と範囲 (1-5) で指定できます。一部のオペレーティングシステムでは、監査を2分ごと、または10分ごとに実行する場合に、/2または/10のような形式で分を指定します。アスタリスク (*) は、年間のすべての月のように、そのフィールドのすべての値を意味します。日は、日にちと曜日の2つのフィールドで指定できます。両方の日を指定すると、両方の値が実行されます。各フィールド内のカンマ区切り値は、すべてのオペレーティングシステムでサポートされています。次に例を示します。

  5,10 0 10 * 1は、毎月10日および毎週月曜日の午前0時5分および午前0時10分に、監査を実行することを意味します。

  crontabの入力形式の詳細については、Unixのmanページを参照してください。

- [時刻と期間] セクションで、スケジュールのタイプごとに、毎日のスケジュールを開始する時刻 (時と分) を指定します。終了時刻を指定しないと、スナップショット仕様ジョブは無期限に実行されます。終了日を選択して監査スケジュールを終了するには、[終了] を選択して終了日を指定します。[タイムゾーン] には、ユーザープロファイルで設定されているタイムゾーンが適用されます。
- (オプション) スナップショット仕様ジョブを無期限に実行する場合は、[終了] オプションを解除してください。

6 スナップショット仕様ジョブのスケジュールを保存するには、[**ファイル**] メニューから [**保存**] を選択します。これでスナップショット仕様は、定義済みのスケジュールに従い実行されます。

スナップショットジョブスケジュールの表示と編集

スナップショット仕様のスケジュールは、作成 (または編集) して保存した後に編集できます。

スケジュール済みスナップショット仕様を編集するには、次の手順を実行します。

1 ナビゲーションペインで、[ジョブとセッション] を選択します。

2 [定期的スケジュール] を選択します。

3 ドロップダウンリストから、[スナップショットの作成] を選択します。リストにすべてのスケジュール済みスナップショット仕様ジョブが表示されます。

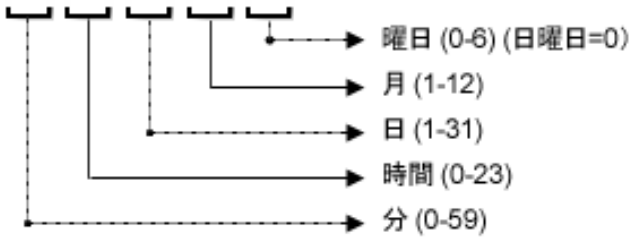
4 スケジュール済みのスナップショット仕様を表示するには、1つを選択してダブルクリックします。

5 [ビュー] ペインで、[スケジュール] オブジェクトを選択します。

6 スナップショット仕様ジョブのスケジュール設定を編集するには、次のパラメーターを変更します。

- **スケジュール**: スナップショット仕様をただちに実行するか、定期的スケジュールで実行するかを選択します。1回、毎日、毎週、毎月、指定のスケジュールから選択します。次のパラメーターを指定します。
- **なし**: スケジュールは設定されません。スナップショット仕様を実行するには、スナップショット仕様を選択して右クリックし、[**スナップショット仕様の実行**] を選択します。
- **毎日**: スナップショットジョブを指定した時刻に毎日実行します。
- **毎週**: スナップショットジョブの実行を希望する曜日を選択します。
- **毎月**: スナップショット仕様ジョブを実行する月を選択します。
- **カスタム**: [カスタムcrontab文字列] フィールドに、スケジュールを示す文字列を入力します。

  crontabファイルには5つのフィールドがあり、曜日、月、日、そして時間と分を指定します。次の図は、crontabファイル内の各位置とそれぞれに対応するもの、設定できる値を示しています。



  crontab 文字列は、シリアル値 (1、2、3、4) と範囲 (1-5) で指定できます。一部のオペレーティングシステムでは、監査を2分ごと、または10分ごとに実行する場合に、/2または/10のような形式で分を指定します。アスタリスク (*) は、年間のすべての月のように、そのフィールドのすべての値を意味します。日は、日にちと曜日の2つのフィールドで指定できます。両方の日を指定すると、両方の値が実行されます。各フィールド内のカンマ区切り値は、すべてのオペレーティングシステムでサポートされています。次に例を示します。

  5,10 0 10 * 1は、毎月10日および毎週月曜日の午前0時5分および午前0時10分に、監査を実行することを意味します。

  crontabの入力形式の詳細については、Unixのmanページを参照してください。

- **時刻と期間**: スケジュールの各タイプについて、日次スケジュールを開始する時間と分、曜日 (および月) を指定します。終了時刻を指定しないと、スナップショット仕様ジョブは無期限に実行されます。日付を指定してスナップショット仕様ジョブのスケジュールを終了するには、[終了] を選択して日付を指定します。[タイムゾーン] には、ユーザープロファイルで設定されているタイムゾーンが適用されます。
- (オプション) スナップショット仕様のスケジュールを無期限に実行する場合は、[終了] オプションを解除してください。

7 スナップショット仕様のスケジュールを保存するには、[**ファイル**] メニューから [**保存**] を選択します。これでスナップショットジョブは、定義済みのスケジュールに従い実行されます。

スナップショットジョブスケジュールの削除

スナップショットジョブスケジュールを削除するには、次の手順を実行します。

1. ナビゲーションペインで、[ジョブとセッション] を選択します。
2. [定期的スケジュール] を選択します。
3. ドロップダウンリストから、[スナップショットの作成] を選択します。
4. 内容ペインに、このSAコアで実行されたすべてのスナップショット仕様ジョブが表示されます。スナップショット仕様ジョブのみを表示するには、内容ペイン上部のドロップダウンリストから、[スナップショットタスクの実行] を選択します。スケジュール設定または実行したスナップショット仕様のみ確認したい場合は、内容ペイン上部の [ユーザー ID] フィールドにユーザー IDを入力します。
5. スケジュールを削除するには、スケジュールを選択して右クリックし、[**スケジュールの削除**] を選択します。

アクティブなスナップショットジョブのキャンセル

SAクライアントでは、アクティブなスナップショットジョブを終了させることができます。アクティブなスナップショットジョブとは、すでに開始しており実行中のジョブのことを指します。

アクティブなスナップショットジョブの終了アクションは、「ソフトキャンセル」と呼ばれます。ソフトキャンセルは、部分的に実行しているジョブを、[サーバーのスナップショット] ウィザードの [ジョブステータス] ステップで [**ジョブの終了**] をクリックして停止させるアクティビティです。ソフトキャンセルは、停止させたいアクティブなスナップショットジョブにのみ適用できます。

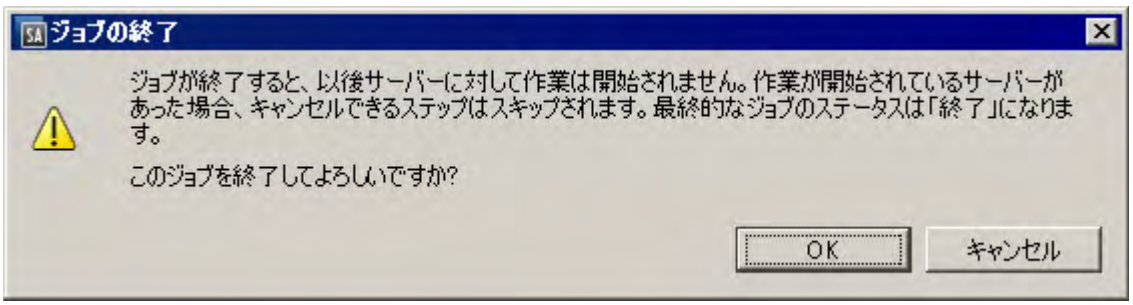
注: 監査、監査結果の修復、スナップショットジョブの作成では、ソフトキャンセルがサポートされています。しかし、スナップショットからサーバーへの [コピー先] などのスナップショット修復ジョブでは、ソフトキャンセルがサポートされていません。

進行中のスナップショットをキャンセルするには、アクセス権が必要です。通常、スナップショットジョブを開始する権限がある場合、実行中のスナップショットジョブを終了させることも可能です。また、[任意のジョブの編集またはキャンセル] 権限がある場合、実行中のスナップショットジョブをソフトキャンセルすることもできます。監査関連のアクセス権の詳細については、『SA 管理ガイド』を参照してください。これらのアクセス権はSA管理者から取得することもできます。

アクティブなスナップショットジョブを終了するには、次の手順を実行します。

1. [ジョブステータス] ペインで [**ジョブの終了**] をクリックします

   このボタンは、ジョブが実行中のときだけ使用できます。
2. [ジョブの終了] ダイアログが表示されます。このダイアログには、ジョブの終了がどのように動作するかが簡単に示されます。
   - その後のサーバーに対してはジョブの作業は開始されません。
   - すでに作業が開始されているサーバーに対しては、ジョブのステップのうちスキップ可能なものがキャンセルされます。
   - [ジョブステータス] に、完了したステップとスキップされたステップが示されます。
3. ジョブが正常に終了した場合、最終的なジョブステータスは「終了済み」になります。



4 **[OK]** をクリックして、ジョブの終了を確認します。[ジョブステータス] ペインに、終了アクションの進行状況が表示されます。

ジョブステータスは終了済みになります。サーバーステータスはキャンセルになります。タスクステータスは成功またはスキップ済みになります。

5 終了が完了したら、SAクライアントジョブログでもジョブを確認できます。

SAクライアントのナビゲーションペインで、**[ジョブとセッション]** を選択します。[ジョブログ] ビューに、ジョブが終了済みステータスで表示されます。

第4章 SAクライアントでのコンプライアンス

概要

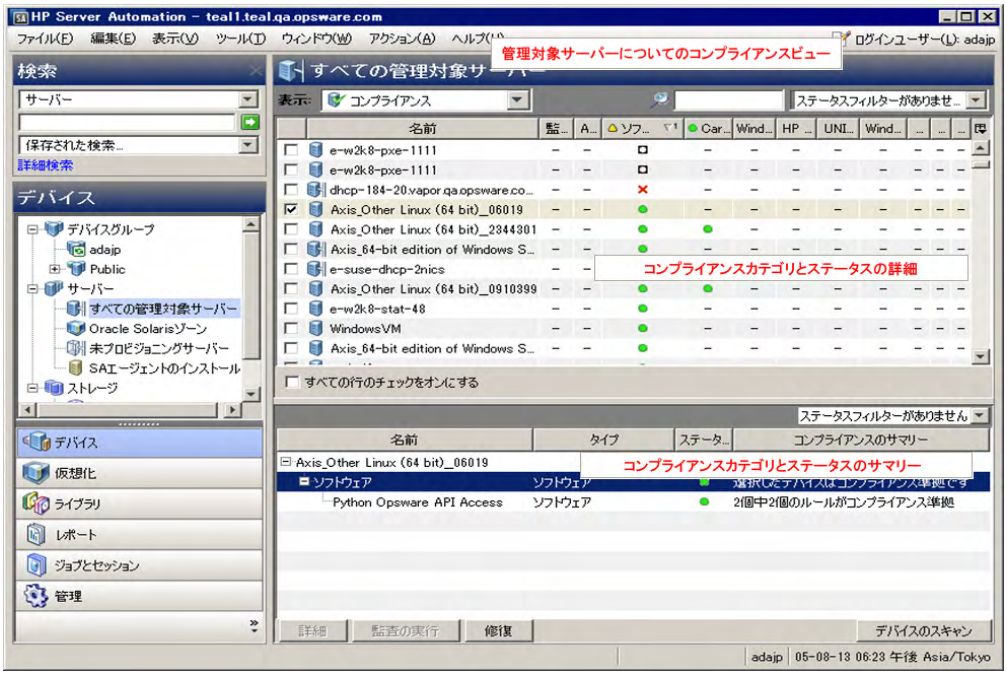
SAクライアントのコンプライアンスビューでは、ファシリティ内にあるすべてのサーバーとサーバーグループの全体的なコンプライアンスレベルを確認できます。一般的にはコンプライアンスダッシュボードと呼ばれるこのビューから、非コンプライアンス状態のサーバーを修復することができます。コンプライアンスを表示する対象として、個々のサーバー、複数のサーバー、サーバーグループ、すべてのSA管理対象サーバーを選択できます。

コンプライアンスダッシュボードには、サーバーまたはサーバーグループの監査、監査ポリシー、ソフトウェアポリシー、パッチポリシー、アプリケーション構成に対するすべてのコンプライアンスステータスの結果が表示されます。サーバーのコンプライアンスステータスは、コンプライアンスポリシーを基準に判定されます。コンプライアンスポリシーではサーバー構成の設定や値が一意に定義されており、これに基づいてIT環境が想定通りに構成されているかどうかが確認されます。

コンプライアンスポリシーの作成と定義は、一般的にポリシー設定の担当者が行います。環境によっては、システム管理者がアドホックポリシーを作成する場合もあります。ポリシー設定担当者は、作成したコンプライアンスポリシーをサーバーにアタッチします。これによって、サーバーが組織の標準とポリシーに準拠しているかどうかを確認できます。たとえば、ポリシー設定の担当者は、ソフトウェアポリシーを作成し、サーバー上にインストールしなくてはならないパッチとパッケージの標準セットを定義します。また、サーバーでの特定のアプリケーションファイルの構成方法も定義できます。サーバーまたはサーバーグループの構成が、ポリシー設定担当者がコンプライアンスポリシーで定義したルールと一致した場合、コンプライアンス状態であるとみなされます。

コンプライアンスダッシュボードでは、サーバーにインストールされているソフトウェア、パッケージ、パッチ、構成ファイルの実際の設定が、ソフトウェアポリシーで定義した構成と一致しているかどうかを確認できます。コンプライアンスビューでは、サーバーグループのコンプライアンスステータスを、グループのすべてのメンバーとサブグループのメンバーごとに表示できます。また、非コンプライアンス状態のサーバーとサーバーグループを検出し、問題を修復できます。図26および図30を参照してください。

図26　コンプライアンスビュー —管理対象サーバー



コンプライアンスダッシュボードに表示される情報は、SAクライアントが最後にコアからコンプライアンス情報を要求した時点での最新情報です。デフォルトで、SA クライアントは新しいコンプライアンス情報を 5 分ごとにチェックします。

この間隔を変更する手順については、自動コンプライアンスチェック頻度の設定 (141 ページ) を参照してください。

デフォルトの間隔 (5分) を待たずにコンプライアンス情報をすぐに取得する場合は、**[F5]** キーを押します。

ベストプラクティス: コンプライアンスダッシュボードを定期的に確認して、サーバーのコンプライアンスレベルを評価し、必要に応じて問題を修復するためのアクションを実行します。たとえば、コンプライアンスビューを使用して、個別にスケジュール設定された監査のステータスを確認し、Apache の http.conf ファイルなどの Web アプリケーションの構成がそれぞれのグループで設定された標準に適合していることを確認します。アプリケーションの構成が何者かによって変更されていないことを確認することができます。必要のない変更が加えられていないことを確認するには、サーバーのデバイスエクスプローラーでコンプライアンスビューを定期的にチェックして、スケジュール設定した監査のコンプライアンスステータスが非コンプライアンスに変わっているかどうかを確認します。このステータスが非コンプライアンスになっている場合は、監査結果を参照して問題を修復します。

ベストプラクティス: コンプライアンスダッシュボードを使用して、特定の疑問に答えたり問題を診断したりすることができます。たとえば、ファシリティ内のサーバーのグループに対するセキュリティ標準を定めた監査をスケジュール設定することができます。この監査の例では、Windows Server 2003のすべてのサーバーに特定のセキュリティパッチが含まれている必要があります。Microsoft が最新のセキュリティパッチを公開したときに、最新のパッチを含むWindows Server 2003サーバーと最新のパッチを含まないサーバーを識別する必要があります。監査を更新して最新のセキュリティパッチを追加し、デバイスグループのコンプライアンスビューでWindows Server 2003サーバーを参照します。監査を再度実行してパッチが必要なサーバーを検出し、必要な最新のセキュリティパッチをインストールしてサーバーを修復します。

用語

以下に、HP Server Automationサーバーコンプライアンスで使用される主な用語と概念の定義を列挙します。

- **コンプライアンス**: 監査、スナップショット仕様、または監査ポリシーで定義された一連のルールによって作成されたチェックまたはテストにサーバーの構成がどの程度適合しているかを表します。監査と修復のコンプライアンスは、ターゲットサーバーで想定される値を指定する監査またはスナップショットのルールによって定義されます。ターゲットサーバー上の値が監査のルールで指定された値と異なる場合、サーバーは非コンプライアンス状態と見なされます。
- **コンプライアンスカテゴリ**: コンプライアンスビューには、監査、監査ポリシー、ソフトウェア、パッチ、パッチポリシー、構成 (アプリケーション構成) のコンプライアンスカテゴリのコンプライアンスステータスが表示されます。
- **コンプライアンスポリシー**: サーバーやデバイスの適切な構成または設定状態を表すユーザー定義の構成です。

  例:

  パッチポリシーでは、コンピューター上にインストールされている必要があるパッチを定義します。

  監査ポリシーでは、たとえば、特定のWindowsサービスを常に無効にしておく必要があることを定義できます。

  アプリケーション構成ポリシーでは、構成ファイルの構成方法を定義します。
- **コンプライアンスルール**: サーバーの理想的な構成を定義するポリシー内の内容または設定 (パッチまたはパッケージ、ファイル構成、ソフトウェアインストール順序、ユーザーとグループのメンバーと権限など)。
- **コンプライアンスステータス**: コンプライアンスカテゴリのコンプライアンスステータスを示します。望ましい状態 (コンプライアンスポリシー) と実際の状態 (サーバー構成) との差異を通知します。たとえば、ポリシーで定義されたすべての構成がサーバー構成と一致している場合、コンプライアンスビューのソフトウェアコンプライアンスカテゴリに表示されるステータスはコンプライアンスになります。グループのコンプライアンスの計算は、個別のサーバーとはやや異なります。
- **コンプライアンススキャン結果**: コンプライアンススキャンの結果です。コンプライアンスステータスと詳細情報が表示されます。また、修復オプションが表示される場合もあります。
- **コンプライアンススキャン**: コンプライアンスポリシー (監査、ソフトウェア、パッチ、アプリケーション構成) の対象となるサーバーをチェックして、SA クライアントに結果を返すメカニズムです。コンプライアンススキャンでは、パッチポリシーまたはソフトウェアポリシーの対象となるコンピューターにインストールされているパッチを確認して結果を返すか、または構成ファイルの内容をチェックしてアプリケーション構成で定義されたルールと一致しているかどうかを確認することができます。コンプライアンスビューでは、ソフトウェア、パッチ、構成のカテゴリのコンプライアンススキャンを実行できます。監査にはスキャン機能はありませんが、監査を実行した場合も同様の結果が得られます。監査の実行では、監査対象のサーバーをチェックして、監査のルールの定義に適合しているかどうかを確認します。
- **コンプライアンスビュー**: ファシリティ内のすべての管理対象サーバーまたはサーバーグループの全体および個別のコンプライアンスレベルを表示します。コンプライアンスビューは、コンプライアンスダッシュボードとも呼ばれます。

コンプライアンスカテゴリ

サーバーおよびサーバーグループのコンプライアンスビューには、次のカテゴリのコンプライアンスが表示されます。

- **監査**: 監査のコンプライアンスは定期的なスケジュールで実行されるすべての監査を集計したもので、スケジュール設定された監査で定義されたルールと監査対象のサーバーにインストールされている内容や構成内容とが一致しているかどうかを示します。
- **監査ポリシー**: 監査ポリシーは監査を通じて管理対象サーバーと関連付けられます。監査は複数のコンプライアンスルールに対応する監査ポリシーにリンクされます。また、監査では、ルールの確認を行う複数のサーバーが定義されます。必要に応じて、監査では定期的なスケジュールを定義できます。監査ポリシーには、他の監査ポリシーを含めることもできます。
- **ソフトウェア**: ソフトウェアのコンプライアンスは、ソフトウェアポリシーの定義がサーバーのインストール内容と一致しているかどうかによって判断します。ソフトウェアポリシーでは、パッチ、パッケージ、アプリケーション構成、スクリプト、その他の各種サーバーオブジェクト (サービス、Windowsレジストリ、COM+、IISメタベースなど) を定義します。ソフトウェアポリシーには、他のソフトウェアポリシーを含めることもできます。詳細については、『SAユーザーガイド: ソフトウェア管理』を参照してください。
- **パッチ**: パッチのコンプライアンスは、パッチポリシーの定義がサーバーまたはサーバーグループにインストールされているパッチと一致するかどうかによって判断します。コンプライアンスビューには、Windowsパッチのみの情報が表示されます。詳細については、『SAユーザーガイド: サーバーのパッチ適用』を参照してください。
- **パッチポリシー**: パッチポリシーでは、コンピューター上にインストールされている必要があるパッチを定義します。
- **構成**: 構成のコンプライアンスは、アプリケーション構成の定義がサーバーまたはサーバーグループの構成と一致するかどうかによって判断します。アプリケーション構成では、アプリケーション構成ファイルの構成設定と値を定義します。構成コンプライアンスのステータスは、サーバーにアタッチされているすべてのアプリケーション構成全体のステータスです。個別のステータスはサポートされません。詳細については、『SAユーザーガイド: アプリケーション構成』を参照してください。次の各項も併せて参照してください。

コンプライアンスステータス

一般に、サーバーまたはサーバーグループのステータスは、コンプライアンスまたは非コンプライアンスになります。この情報はコンプライアンスビューに表示されます。

コンプライアンス: サーバーがサーバーにアタッチされたポリシーに適合している場合、コンプライアンスビューにはこのアイコンが表示されます。ポリシーで定義したルールがポリシーがアタッチされたサーバーの実際の構成と一致している場合、サーバーはコンプライアンスと見なされます。

非コンプライアンス: サーバーの実際の構成がポリシーで構成されたルールと一致しない場合、コンプライアンスビューにはこのアイコンが表示されます。たとえば、Windows Server 2003サーバーでWindows CIS推奨の8文字以上のパスワードを順守するための監査を構成することができます。この監査を実行してサーバーのユーザーパスワードをチェックして4文字のユーザーパスワードが見つかった場合、コンプライアンスビューにはサーバーの監査ポリシーが非コンプライアンスと表示されます。

ベストプラクティス: 非コンプライアンスルールの数と相違するオブジェクトの数は同一ではないので注意が必要です。1つの非コンプライアンスルールに複数の相違するオブジェクトが表示されることがあります。SAでは、非コンプライアンスルールの数は考慮されますが、相違するオブジェクトの数は考慮されません。たとえば、ディレクトリ内に多数のファイル (オブジェクト) があり、これをディレクトリルールで定義しているとします。監査の結果、相違するオブジェクトがいくつか検出された場合、SAは相違の数を1つとみなし、複数の相違があるとはみなしません。SAクライアントでは、監査結果ブラウザーのコンプライアンスビューとサマリービューに、非コンプライアンスのルールの数が表示されます。これらのビューには、相違するオブジェクトの数は表示されません。

複数のポリシーがサーバーにアタッチされている場合は、集計列にすべてのポリシーのステータスがまとめられます (ロールアップされます)。このサーバーが複数のサーバーから成るデバイスグループに属している場合は、そのグループのコンプライアンスビューにアクセスして、サブグループ内のサーバーを含めて、グループ内のすべてのサーバーで実行されるすべての監査のコンプライアンスステータスレベルを確認することができます。グループのコンプライアンスステータスの判断は、デフォルトの計算方法に基づいて行われ

ます。そのグループに属するサーバーの少なくとも95%のステータスがコンプライアンスである場合、そのサーバーグループはコンプライアンスであると見なされます。ステータスがコンプライアンスであるサーバーが95%未満の場合、グループのステータスは部分コンプライアンスと表示されます。

サーバーグループのコンプライアンスステータスのデフォルトのしきい値はカスタマイズできます。デバイスグループのコンプライアンス設定の変更 (128ページ) を参照してください。

実際のサーバー構成やポリシー情報は、コンプライアンスビューでサーバーやサーバーグループのコンプライアンスを最後に確認したときから変更されている可能性があります。SAコアから最新のコンプライアンスデータを取得するには、[**表示**] メニューから [**更新**] を選択するか、[**F5**] キーを押します。また、サーバーやサーバーグループでコンプライアンススキャンを実行して、最新のコンプライアンスステータスを確認することもできます。

コンプライアンスステータスの定義

表3に、ポリシー、サーバー、デバイスグループのデフォルトのコンプライアンスステータスを示します。

表3　　コンプライアンスステータスのアイコン

アイコン	コンプライアンスステータスの説明
	**コンプライアンス** • **ポリシー**: ポリシーで定義されているすべてのルールまたは項目が実際のサーバー構成と一致しています。 • **サーバー**: コンプライアンススキャンが正常に実行され、サーバー構成がサーバーにアタッチされたすべてのポリシーで定義されているすべてのルールと一致しています。 • **デバイスグループ**: コンプライアンススキャンが正常に実行され、コンプライアンス状態のサーバーの割合が [管理] ペインの [コンプライアンス設定] オプションで設定した最小しきい値を上回っています。デフォルトで、コンプライアンス状態のしきい値は、グループ内のサーバーの 95% です。コンプライアンス状態のしきい値の定義は変更できます。
	**部分コンプライアンス** • **ポリシー**: ポリシーで定義されている1つ以上のルールまたは項目が、いずれかのルールに例外が適用されたことにより、実際のサーバー構成と一致しません。これは Windows パッチポリシーのみに適用されます。 • **サーバー**: コンプライアンススキャンが正常に実行され、いずれかのルールに例外が適用されたことにより、サーバー構成がサーバーにアタッチされたポリシーで定義されたルールの少なくとも 1 つと一致しませんでした。これは Windows パッチポリシーのみに適用されます。 • **デバイスグループ**: コンプライアンススキャンが正常に実行され、グループ内の十分な数のサーバーが [管理] ペインの [コンプライアンス設定] で設定された非コンプライアンスのしきい値条件を満たしています。グループ内の残りのサーバーはコンプライアンス状態です。部分コンプライアンスのしきい値の定義は変更できます。
	**非コンプライアンス** • **ポリシー**: ポリシーで定義されている1つ以上のルールまたは項目が実際のサーバー構成と一致していません。 • **サーバー**: コンプライアンススキャンが実行され、実際のサーバー構成がポリシー内で定義されている1つ以上のルールと一致しません。 • **デバイスグループ**: コンプライアンススキャンが実行され、グループ内の十分な数のサーバーが [管理] ペインの [コンプライアンス設定] オプションで設定された非コンプライアンスのしきい値条件を満たしていて、グループが非コンプライアンスであることを示しています。非コンプライアンスのしきい値の定義は変更できます。
	**スキャン失敗** コンプライアンススキャンを実行できませんでした。
	**スキップ済み** サーバーがスキップされました。

表3　　コンプライアンスステータスのアイコン（続き）

アイコン	コンプライアンスステータスの説明
	**スキャンが必要** 未定義の結果です。コンプライアンススキャンが実行されていないか (新規インストールの場合など)、最後にSAクライアントに情報が報告された後にサーバー (またはデバイスグループ内のサーバー) の構成が変更されている場合に、このステータスになることがあります。
	**スキャン中**: コンプライアンススキャンは現在実行中です。
—	**テスト定義なし** このタイプのコンプライアンスポリシーが、サブグループのサーバーを含めて、サーバーまたはデバイスグループ内のすべてのサーバーにアタッチされていません。

コンプライアンスステータスのしきい値—ポリシー、サーバー、複数のサーバー

ポリシー: ポリシーのコンプライアンスステータスは、ポリシー内のすべてのルールに基づきます。ポリシー内のルールのいずれかが非コンプライアンスである場合 (管理対象サーバーの実際の構成と一致しない場合)、サーバーのポリシー全体が非コンプライアンスと見なされます。

サーバーおよび複数のサーバー : サーバーのコンプライアンスステータスは、サーバーにアタッチされているすべてのポリシーまたはサーバーをターゲットとして定義しているすべてのポリシーに基づきます。コンプライアンスカテゴリのいずれかに非コンプライアンス状態のコンプライアンスステータスが存在する場合、サーバーのコンプライアンスステータス全体が非コンプライアンスと見なされます。サーバーのコンプライアンスステータス全体がコンプライアンス状態になるには、すべてのコンプライアンスカテゴリのすべてのポリシーがコンプライアンス状態である必要があります。

コンプライアンスステータスのしきい値—デバイスグループ

コンプライアンスビューでデバイスグループのコンプライアンスを表示する際には、サーバーがコンプライアンスまたは非コンプライアンスと見なされるかどうかが重要になります。このステータスは、構成およびカスタマイズ可能なデフォルトのしきい値の計算に基づきます。

非コンプライアンス: デバイスグループのコンプライアンスビューで、コンプライアンスカテゴリ (監査、監査ポリシー、ソフトウェア、パッチ、または構成) に対して非コンプライアンスのステータスが表示されるには、そのカテゴリに対して非コンプライアンス状態のサーバーがグループ内のすべてのサーバーの5%を超えている必要があります。デバイスグループの非コンプライアンス状態は、コンプライアンス状態のサーバーが95%未満である場合に非コンプライアンスのステータスが表示されると覚えることもできます。

部分コンプライアンス: デバイスグループのコンプライアンスビューで、コンプライアンスカテゴリ (監査、監査ポリシー、ソフトウェア、パッチ、または構成) に対して部分コンプライアンスのステータスが表示されるには、そのカテゴリに対して非コンプライアンス状態のサーバーがグループ内のすべてのサーバーの2%より多く5%以下である必要があります。デバイスグループの部分コンプライアンス状態は、コンプライアンス状態のサーバーが95%以上98%未満である場合に部分コンプライアンスのステータスが表示されると覚えることもできます。

コンプライアンス: デバイスグループのコンプライアンスビューで、コンプライアンスカテゴリ (監査、ソフトウェア、パッチ、または構成) に対してコンプライアンスのステータスが表示されるには、そのカテゴリに対して非コンプライアンス状態のサーバーがグループ内のすべてのサーバーの2% 未満である必要があります。デバイスグループのコンプライアンス状態は、サーバーの98%以上がコンプライアンス状態であると覚えることもできます。

デバイスグループのステータスは、グループに属するすべてのサーバーにアタッチされた (すべてのコンプライアンスカテゴリの) すべてのポリシーに基いて計算されます。これには、選択したグループの下位のすべてのサブグループのサーバーも含まれます。

コンプライアンスステータスの計算に使用するデフォルトのしきい値は変更できます。たとえば、グループのコンプライアンスステータスを非再帰的に計算するように構成して、サブグループのサーバーをコンプライアンスの計算に含めないようにすることができます。

デバイスグループのコンプライアンス設定の変更

デフォルトで、SAクライアントでは、デバイスグループのコンプライアンスを判断する方法を構成できます。

デバイスグループのコンプライアンス設定を変更するには、SA機能モデルOpswareへのアクセス権が割り当てられているグループのメンバーでなければなりません。割り当てられているアクセス権の詳細については、SAの管理者にお問い合わせください。

デバイスグループのコンプライアンス設定を変更する手順:

1. ナビゲーションペインで、**[管理]** > **[コンプライアンス設定]** を選択します。
2. [コンプライアンス設定] ペインの [デバイスグループのコンプライアンス] セクションで、**[設定の編集]** をクリックします。
3. [デバイスグループのコンプライアンス設定] ウィンドウで、次の設定を構成します。
   - **デバイスグループのロールアップコンプライアンスの表示**: 各コンプライアンスカテゴリ列の最上部に表示される親グループのコンプライアンスステータスを示すアイコンを表示したり、非表示にしたりすることができます。このアイコンは、選択したグループのすべてのメンバーについてのコンプライアンスステータスのロールアップを示します。

     たとえば、このオプションを選択した場合、グループを選択して [表示] ドロップダウンリストから [コンプライアンス] を選択したときに、各コンプライアンスカテゴリ列 (監査、ソフトウェア、パッチ、構成) の先頭の列見出しに、選択したグループのすべてのサーバーのコンプライアンスステータスを示すアイコンが表示されます。この列見出しにカーソルを置くと、このカテゴリのすべてのデバイスのコンプライアンスステータスを表示できます。
   - **メンバー計算**: コンプライアンスカテゴリのグループ全体のコンプライアンスレベルを計算する際に、サブグループに所属するサーバーを考慮するかどうかを選択できます。次に例を示します。
     - **サーバーメンバーとグループメンバーが考慮されます。**: デバイスグループのコンプライアンスステータスで、グループ内のすべてのサーバーと選択したデバイスグループに所属するすべてのサブグループ内のすべてのサーバーに対してコンプライアンスが再帰的にチェックされます。
     - **サーバーメンバーだけが考慮されます。**: 選択したデバイスグループのコンプライアンスステータスで、グループのトップレベルにあるサーバーのみに対してコンプライアンスがチェックされ、サブグループのメンバーに所属するサーバーはすべて除外されます。
   - **しきい値**: すべてのコンプライアンスカテゴリのデバイスグループのコンプライアンスステータスの決定に使用するコンプライアンスのしきい値計算の割合 (%) を変更できます。

     デフォルトでは、デバイスグループに次のステータスが表示されます。

     非コンプライアンス — 非コンプライアンスであるメンバーが5%を超える場合。

     部分コンプライアンス — 非コンプライアンスであるメンバーが2%を超えて5%未満の場合。

     コンプライアンス — 非コンプライアンスであるメンバーが2%以下の場合。
   - **列タイプ**: 検出して表示できるコンプライアンスカテゴリ (監査、監査ポリシー、ソフトウェア、パッチ、構成) を変更できます。
4. **[OK]** をクリックして設定を保存します。

コンプライアンスダッシュボード

SAクライアントでは、個別のサーバー、複数のサーバー、およびその両方のコンプライアンスを表示することができます。

- 個別サーバーのコンプライアンスの表示
- 複数サーバーのコンプライアンスの表示
- グループのコンプライアンスの表示

複数サーバーのコンプライアンスステータスを表示する場合、表示用のアクセス権がユーザーに割り当てられていないサーバーがグループ内に存在する可能性があります。また、ユーザーアカウントに、サーバーグループのコンプライアンスステータスの計算に使用するポリシー(監査、ソフトウェア、パッチ)のいずれかを表示するアクセス権が割り当てられていない可能性もあります。

このような場合は、一部のサーバーや一部のポリシーが表示されなくても、ユーザーが表示可能な複数サーバーの全体的なコンプライアンスステータスを表示することはできます。また、一部のポリシーがビューに表示されない場合でも、コンプライアンスカテゴリのロールアップを表示することはできます。

個別サーバーのコンプライアンスの表示

個別サーバーのコンプライアンス情報を表示する手順:

1. ナビゲーションペインで、[**デバイス**] > [**すべての管理対象サーバー**] または [**仮想サーバー**] を選択します。
2. 内容ペインで、サーバーを選択します。
3. 右クリックして [開く] を選択し、サーバーブラウザーを表示します。
4. [情報] ペインで [**管理ポリシー**] を選択します。
5. [**管理ポリシー**] ペインで [**コンプライアンス**] を選択します。

   内容ペインに、コンプライアンスカテゴリごとのコンプライアンスステータスのサマリーが円グラフで表示されます。また、個別のポリシーの詳細なステータス情報も表示されます。図27を参照してください。
6. いずれかのコンプライアンスカテゴリまたはカテゴリ内の個別のポリシーに関するアクションを実行するには、詳細リストで選択してから、[**監査の実行**] (監査のみ)、[**修復**]、または [**デバイスのスキャン**] をクリックします。

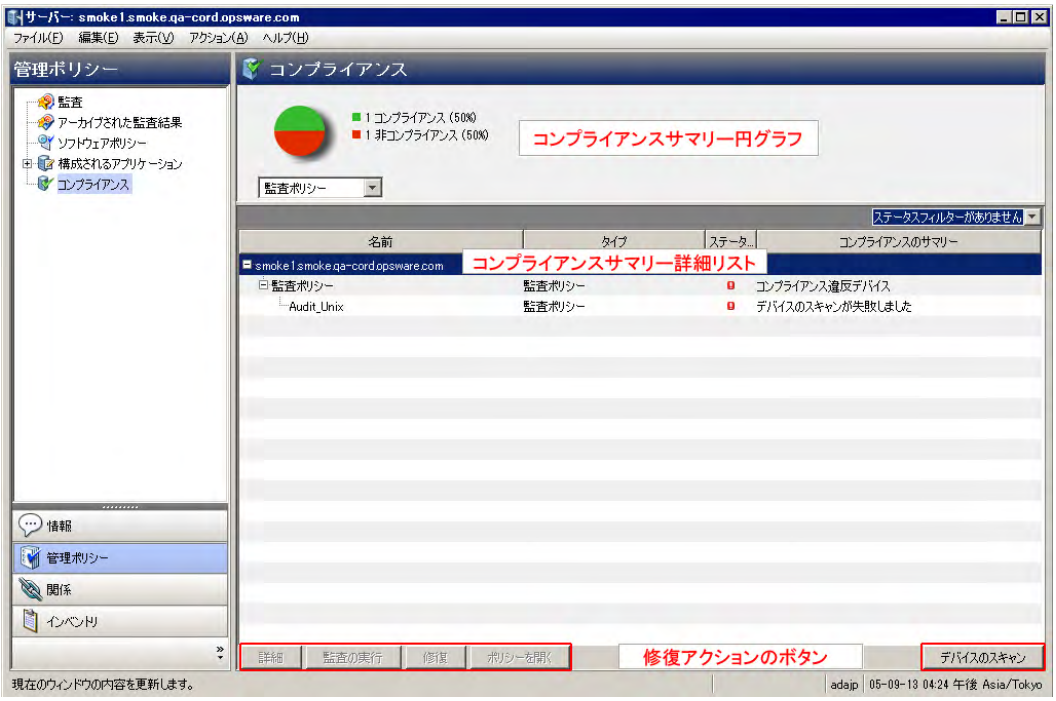
ポリシーの表示とポリシーに対する修復操作の両方を実行できるかどうかは、ユーザーのアクセス権によって決まります。ポリシーの表示またはポリシーに対するアクションの実行を行うことができない場合は、それぞれのSA管理者に相談してください。

コンプライアンスサマリーの円グラフと詳細情報

コンプライアンスビューは、次のセクションにわかれています。

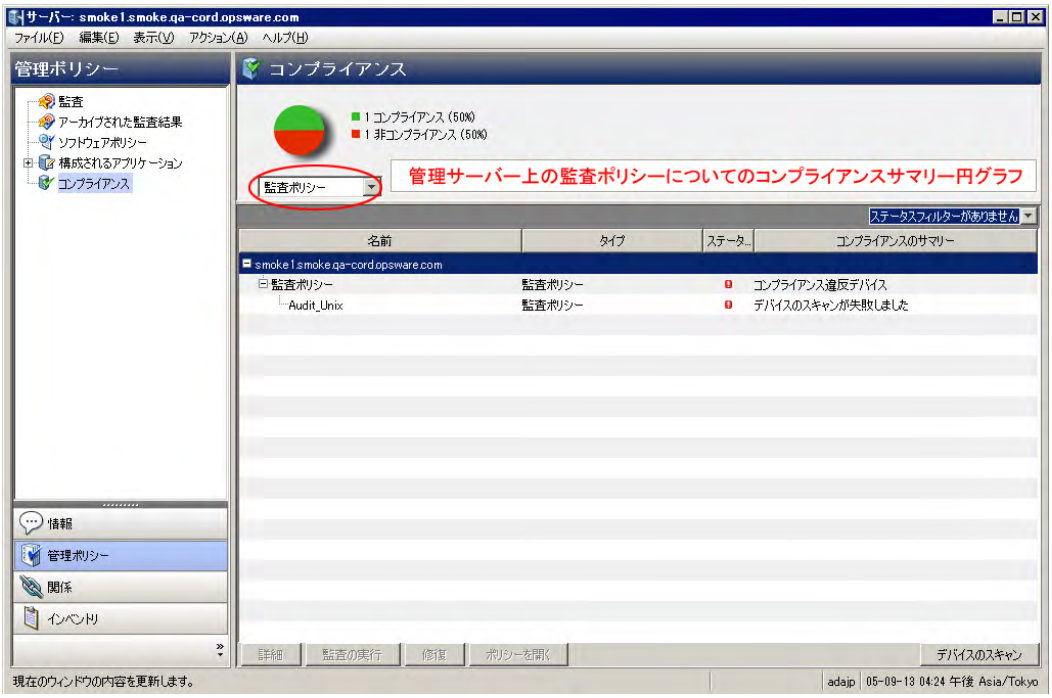
- コンプライアンスサマリーの円グラフでは、選択したサーバーにアタッチされているすべてのポリシーに対する全体のコンプライアンスステータスがグラフィカルに表示されます。特定のコンプライアンスカテゴリのみのステータスを表示するように、この円グラフをフィルター処理することもできます。図27を参照してください。
- コンプライアンスサマリー詳細リストでは、各コンプライアンスカテゴリごとにドリルダウンして、全体のコンプライアンスステータス、各カテゴリに含まれるポリシー、各ポリシーのコンプライアンスステータス、それぞれのサマリー説明を参照することができます。それぞれの選択内容に応じて、非コンプライアンス状態のポリシーを修復するためのアクション(ポリシーの詳細の表示、監査の実行、またはデバイスのコンプライアンススキャンなど)を実行することができます。図27を参照してください。

図27　　管理対象サーバーのコンプライアンスサマリー —すべてのポリシー



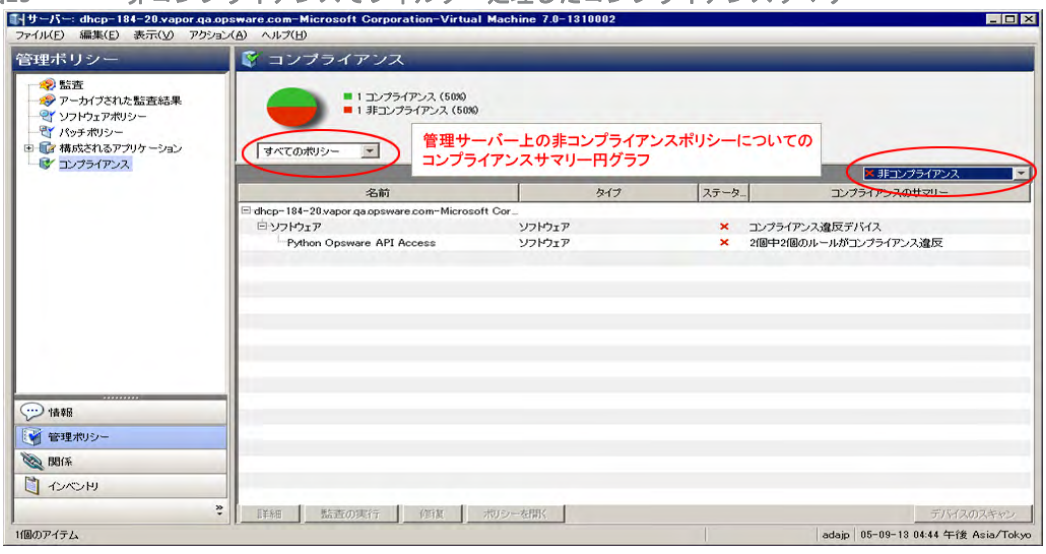
円グラフの下のドロップダウンリストを選択すると、コンプライアンステストカテゴリ(監査ポリシーなど)でフィルター処理された円グラフが表示されます。図28を参照してください。

図28　　管理対象サーバーのコンプライアンスサマリー —監査ポリシー



また、円グラフの下にある詳細ペインでコンプライアンスポリシーの内訳をフィルター処理して、特定のコンプライアンスステータスを含むすべてのコンプライアンスポリシーを表示することもできます。たとえば、図29では、非コンプライアンス状態のすべてのコンプライアンスポリシーのみを表示するようにコンプライアンスビューをフィルター処理しています。

図29　　非コンプライアンスでフィルター処理したコンプライアンスサマリー



前の例で、コンプライアンスビューの詳細ペインには、サーバーにアタッチされている非コンプライアンス状態のすべてのポリシーが表示されます。ポリシーで構成されたルールの少なくとも1つがサーバー上の構成と一致しない場合、ポリシーは非コンプライアンスであると見なされます。

複数サーバーのコンプライアンスの表示

複数のサーバーのコンプライアンス情報を表示するには、次の手順を実行します。

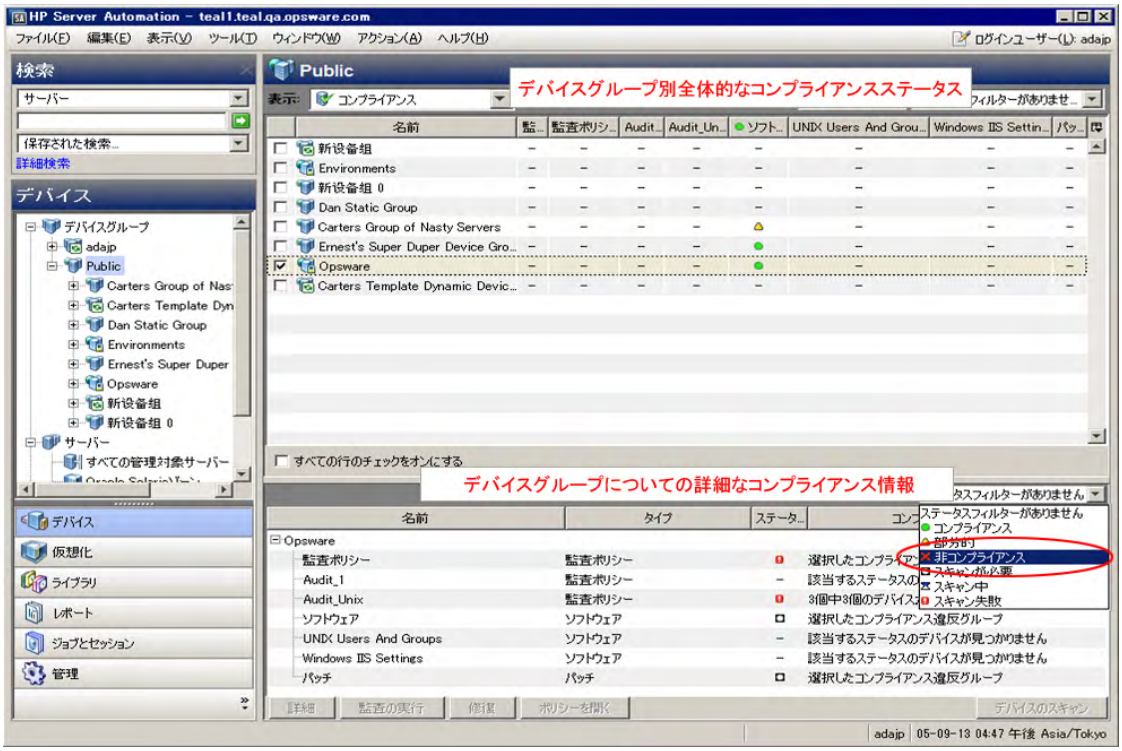
1 ナビゲーションペインで、[**デバイス**] > [**デバイスグループ**] を選択します。

2 [デバイスグループ] ツリーで、[Public] を選択するか、独自のユーザーグループリストを選択します。内容ペインに、すべてのデバイスグループ (すべてのパブリックグループまたはユーザーが作成したすべてのグループ) の内容がリスト表示されます。

3 [表示] ドロップダウンリストから、[コンプライアンス] を選択します。

4 コンプライアンスビューの詳細ペインに含める場合は、リストの 1 つまたは複数のデバイスグループまたは任意のサーバーの横にあるチェックボックスをオンにします。図 30 の詳細ペインに、選択したグループ内のすべてのサーバーのコンプライアンス情報が表示されます。

図30 コンプライアンスビュー—デバイスグループ



5 (オプション) ステータスフィルターのドロップダウンリストを使用して、コンプライアンスステータスでビューをフィルター処理します。たとえば、非コンプライアンス ✖ ステータスのデバイスグループのみを表示することができます。

6 (オプション) 詳細ペインで、いずれかのカテゴリを選択します。選択したカテゴリとユーザーのアクセス権に応じ、ペインの下部にあるいずれかのアクションボタンをクリックして、詳細の表示、監査の実行、ソフトウェアポリシーやパッチポリシーの修復、またはグループのすべてのメンバーに対するコンプライアンススキャンの実行を行います。

デバイスグループのコンプライアンス: ステータスのロールアップ

デバイスグループの内容ペインには、すべてのグループメンバーのコンプライアンスステータスのロールアップサマリーと、ナビゲーションペインで選択したグループ ([**デバイス**] > [**デバイスグループ**]) の内容が表示されます。

リスト上部にある列見出しのコンプライアンスステータス (コンプライアンス、非コンプライアンス、部分コンプライアンスなど) のアイコンは、リストのすべてのグループのロールアップステータスを示します。表示されるすべてのグループに対するコンプライアンスカテゴリの全体的なステータスを表示するには、カテゴリの列見出しの上にカーソルを移動します。

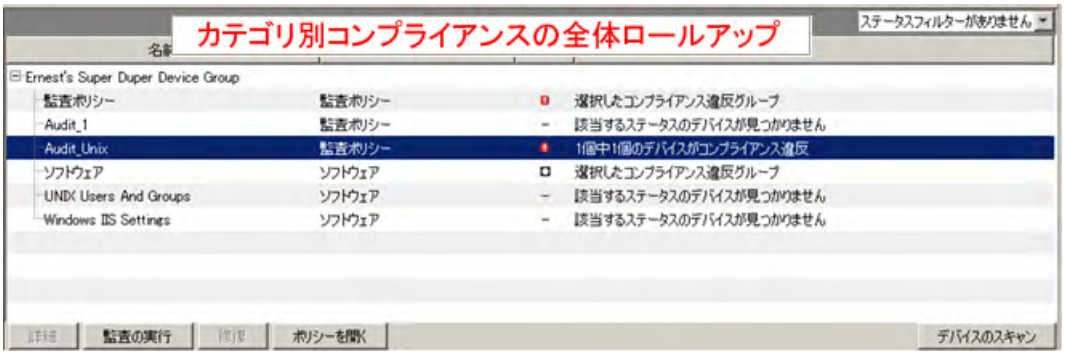
このビューのリストの各行では、すべてのコンプライアンスカテゴリにグループごとのコンプライアンスステータスが表示されます。これらのカテゴリには監査、監査ポリシー、ソフトウェア、パッチ、構成などが含まれます。また、このビューに表示するように設定した個別にスケジュール設定した監査も含まれます。図31では、コンプライアンスカテゴリごとに、グループ内のサーバーにアタッチされているすべてのポリシーのコンプライアンスステータスが表示されています。

図31　　デバイスグループのコンプライアンスのロールアップ

デバイスグループのコンプライアンス: 全体ロールアップ

内容ペインで1つまたは複数のグループ (またはすべてのグループ) を選択すると、詳細ペインには、グループのすべてのメンバーに対する内容ペインの各列のデバイスコンプライアンスの全体ロールアップが表示されます。図32を参照してください。

図32　　デバイスグループのコンプライアンスの全体ロールアップ



ステータスフィルターのドロップダウンリストを使用して、コンプライアンスステータスでビューをフィルター処理します。たとえば、非コンプライアンス ✕ ステータスのデバイスグループのみを表示することができます。

選択したカテゴリとユーザーのアクセス権に応じ、いずれかのアクションボタンをクリックして、詳細の表示、監査の実行、ソフトウェアポリシーやパッチポリシーの修復、またはグループのすべてのメンバーに対するコンプライアンススキャンの実行を行います。

グループのコンプライアンスの表示

グループエクスプローラーでは、コンプライアンスビューにグループのすべてのメンバーに対するコンプライアンスポリシーのロールアップがポリシータイプごとに表示されます。個々のサーバーのコンプライアンスステータスは表示されません。これにより、ポリシータイプごとにグループ内のすべてのサーバーに対してグループがコンプライアンス状態かどうかがわかります。

ステータスフィルターのドロップダウンリストを使用して、コンプライアンスステータスでビューをフィルター処理します。たとえば、非コンプライアンス ステータスのデバイスグループのみを表示することができます。

選択したカテゴリとユーザーのアクセス権に応じ、いずれかのアクションボタンをクリックして、詳細の表示、監査の実行、ソフトウェアポリシーやパッチポリシーの修復、またはグループのすべてのメンバーに対するコンプライアンススキャンの実行を行います。

デバイスグループエクスプローラーでのサーバーグループの表示:

1. ナビゲーションペインで、[**デバイス**] > [**デバイスグループ**] を選択します。
2. [デバイスグループ] ツリーで、[Public] を選択するか、独自のユーザーグループリストを選択します。内容ペインに、すべてのデバイスグループ (すべてのパブリックグループまたはユーザーが作成したすべてのグループ) の内容がリスト表示されます。
3. サーバーグループを選択します。
4. 右クリックして [**開く**] を選択します。
5. グループエクスプローラーのビューペインで ［コンプライアンス］ を選択します。コンプライアンスビューに、グループ内のすべてのサーバーに関するサマリーのロールアップコンプライアンスステータス情報が表示されます。図33を参照してください。

図33　　グループのコンプライアンスビュー

コンプライアンスサマリーの円グラフでは、グループ内の関連するすべてのサーバーに対するすべてのポリシーの全体的なコンプライアンスステータスがグラフィカルに表示されます。円グラフの区分は、カテゴリごとのコンプライアンスステータスと各ステータスレベルの割合を示しています (コンプライアンス、非コンプライアンス、スキャンが必要、スキャン失敗など)。この円グラフは、特定のコンプライアンスカテゴリのみのステータスを表示するようにフィルター処理することもできます。

詳細ペインには、コンプライアンスカテゴリごとのデバイスのコンプライアンスの全体ロールアップが表示されます。

選択したカテゴリとユーザーのアクセス権に応じ、いずれかのアクションボタンをクリックして、詳細の表示、監査の実行、ソフトウェアポリシーやパッチポリシーの修復、またはグループのすべてのメンバーに対するコンプライアンススキャンの実行を行います。

コンプライアンスビューでの列の追加と削除

コンプライアンスビューでデバイスグループを表示する場合、デフォルトでは、内容ペインの列に、監査、監査ポリシー、ソフトウェア、パッチ、構成のコンプライアンスカテゴリが表示されます。これらのカテゴリはいずれも表示または非表示にすることができます。また、各カテゴリでポリシーを個別に追加または削除することもできます。

コンプライアンスビューでデバイスグループのコンプライアンスカテゴリを追加または削除する手順:

1. ナビゲーションペインで、[**デバイス**] > [**デバイスグループ**] を選択します。
2. デバイスグループで、デバイスグループの独自のリストまたはPublicリストを展開します。
3. 内容ペインで、デバイスグループを選択します。
4. [表示] ドロップダウンリストで [コンプライアンス] を選択します。

   内容ペインに、監査、監査ポリシー、ソフトウェア、パッチ、構成のコンプライアンスカテゴリが表示されます。内容ペインには、デバイスグループの各メンバーのステータスも表示されます。

5. 列セレクター  を使用して、カテゴリを追加または削除します。
6. [コンプライアンスビュー列の選択] ウィンドウの左側に、各コンプライアンスカテゴリのタブと参照するアクセス権のあるカテゴリのすべてのコンプライアンスポリシーが表示されます。このウィンドウの右側には、コンプライアンスビューの各カテゴリの現在表示可能なポリシーが表示されます。デフォルトで、コンプライアンスビューには、カテゴリのすべてのポリシーの全体 (ロールアップ) が表示されます。
7. コンプライアンスビューの列に個別のポリシーを追加する場合は、左側でコンプライアンスカテゴリのタブとポリシーを選択して、プラス (+) 矢印ボタンをクリックします。
8. コンプライアンスビューから個別のポリシーや集計列を削除する場合は、ウィンドウの右側でいずれかを選択して、マイナス (-) 矢印ボタンをクリックします。
9. [**OK**] をクリックして変更内容を保存します。

コンプライアンスカテゴリ表示のソート

ベストプラクティス: コンプライアンスビューの表示をカスタマイズするには、コンプライアンスカテゴリを昇順または降順に配置するのが便利です。

コンプライアンスビューで列をソートする手順:

1. コンプライアンスビューで、列見出しをクリックします。

   コンプライアンスカテゴリ名の横に上付き文字で番号「1」が表示されます。これは、このテーブルのプライマリソートキーです。

2. 列見出し内の上矢印または下矢印をクリックして、データを昇順にソートするか降順にソートするかを指定します。
3. [**Ctrl**] キーを押して、別の列見出しをクリックします。

   コンプライアンスカテゴリ名の横に上付き文字で番号「2」が表示されます。これは、このテーブルのセカンダリソートキーです。

4. (オプション) 必要に応じて手順3を繰り返します。
5. (オプション)　列見出しの上にカーソルを移動して、特定のカテゴリのコンプライアンスステータスのロールアップを表示します。
6. ソートキーをリセットするには、注釈の付いていない列見出しをクリックします。

コンプライアンスステータスによるフィルター処理

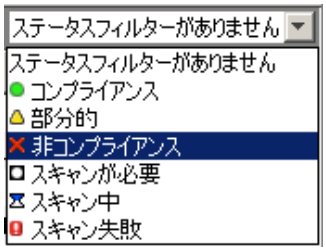
コンプライアンスビューで個別の管理対象サーバーとサーバーグループのコンプライアンスを表示する際には、表示するコンプライアンスカテゴリに対して、特定のコンプライアンスステータスと一致するサーバーが少なくとも1つ存在するグループとサーバーのみを表示するようにビューをフィルター処理することができます。たとえば、グループを選択してからコンプライアンスビューを選択する場合にステータスフィルターを使用すると、選択したグループの非コンプライアンス状態のメンバーのみをコンプライアンスカテゴリ(監査、監査ポリシー、パッチ、ソフトウェアなど)ごとに表示することができます。

コンプライアンスステータスでコンプライアンスビューをフィルター処理する手順:

1. ナビゲーションペインで、[**デバイス**] > [**デバイスグループ**] を選択します。
2. [デバイスグループ] ツリーで、[Public] を選択するか、独自のユーザーグループリストを選択します。
3. [Public] ペインで、デバイスグループを選択します。

   内容ペインには、選択したグループのすべてのメンバーのコンプライアンスビューステータスが表示されます。
4. このビューをコンプライアンスステータスでフィルター処理するには、ステータスフィルターのドロップダウンリストからいずれか1つを選択します。図34を参照してください。

図34　　コンプライアンスステータスフィルター



5. コンプライアンスビューには、ステータスが非コンプライアンス ✕ のメンバー(個別のサーバーおよびサブグループのサーバー)のみが表示されます。
6. リストに表示されたグループ内のサーバーまたはサブグループのいずれかを選択します。

   詳細ペインには、選択したサーバーのコンプライアンスステータス情報が表示されます。このペインでステータスフィルターを使用すると、詳細ペインの情報をフィルター処理することができます。

コンプライアンス情報の更新

ベストプラクティス: コア内の最新のコンプライアンス情報を確認するには、コンプライアンスビューを更新するのが便利です。コアの最新のコンプライアンス情報を取得するには、[ビュー] メニューから [更新] を選択するか、[**F5**] キーを押します。

コンプライアンスビューを最初に選択したときには、各コンプライアンスカテゴリごとにSAコアから通知された最新情報が表示されます。コンプライアンスビューで表示した後にサーバーの構成が変更されているかもしれません。また、コンプライアンスビューでサーバーやグループを表示した後にポリシーが変更されているかもしれません。このような場合には、コンプライアンススキャンや監査を再度実行して、コンプライアンスビューに表示する最新のデータを生成することができます。

自動コンプライアンスチェック頻度の設定

デフォルトで、SAクライアントはコアのコンプライアンス情報を5分ごとにチェックします。この間隔は [オプションの設定] ウィンドウで変更できます。

SAクライアントでコアのコンプライアンス情報をすぐにチェックする場合は、[**F5**] キーを押します。

自動コンプライアンスチェック頻度の設定を変更する手順:

1. SAクライアントの [ツール] メニューで [オプション] を選択します。
2. [オプションの設定] ウィンドウのビューペインで、[一般] を選択します。
3. [キャッシュ] セクションの「更新を確認する間隔 <xx> 分」フィールドに、SA クライアントでコアのコンプライアンス情報をチェックする頻度に対応した間隔を入力します。

   チェック対象には、コンプライアンス情報だけでなく、SAクライアントがコアからアクセス可能なすべての情報が含まれます。間隔を長くするほど、参照情報が古くなっている可能性も高くなります。間隔を短くするほど、新しい情報を参照できるようになりますが、コアとの送受信に伴うネットワークトラフィックも増えます。
4. (オプション) [**キャッシュの更新**] をクリックして、コアの最新情報をすぐにチェックします。
5. (オプション) [**キャッシュの再ロード**] をクリックして、キャッシュをすぐに再ロード (更新) します。
6. [**保存**] をクリックします。

コンプライアンスビューの情報のエクスポート

コンプライアンスビューに表示されるすべての情報をファイルに保存する場合は、ビューを.htmlまたは.csv形式でエクスポートすることができます。

コンプライアンスビュー情報をファイルにエクスポートする手順:

1. ナビゲーションペインで、[**デバイス**] > [**デバイスグループ**] を選択します。
2. コンプライアンスを表示するグループを選択し、[**ビュー**] メニューの [**コンプライアンス**] を選択します。
3. 内容ペインで、グループ内のサーバーを選択します。

4 右クリックで[**エクスポート先**]を選択してから、CSVまたはHTMLを選択します。

5 [コンプライアンスビューのエクスポート]ウィンドウで、次の手順を実行します。

a ファイルの名前を入力します。

b (オプション)保存したファイルで特定のエンコード方式を使用する場合は、エンコードを変更します。

c [**保存**]をクリックします。

注: コンプライアンス結果を正しく表示するには、.csvファイルをテキストエディターで開き、ワードラップをオフにし、テキストウィンドウを水平方向に拡大します。

コンプライアンスダッシュボードでの修復

コンプライアンスビューでは、サーバーおよびグループのコンプライアンスステータス情報を表示するだけでなく、監査、ソフトウェア、パッチ、アプリケーション構成のコンプライアンスポリシーで定義された組織の標準に準拠していないサーバー構成を修復することができます。

サーバーまたはサーバーグループを修復するということは、サーバーまたはサーバーグループのコンプライアンス違反状態(非コンプライアンス状態)を検出して、サーバーの実際の構成をコンプライアンスポリシーに適合させることを意味します。

サーバーまたはサーバーグループのコンプライアンスビューでは、次のアクションを実行できます。

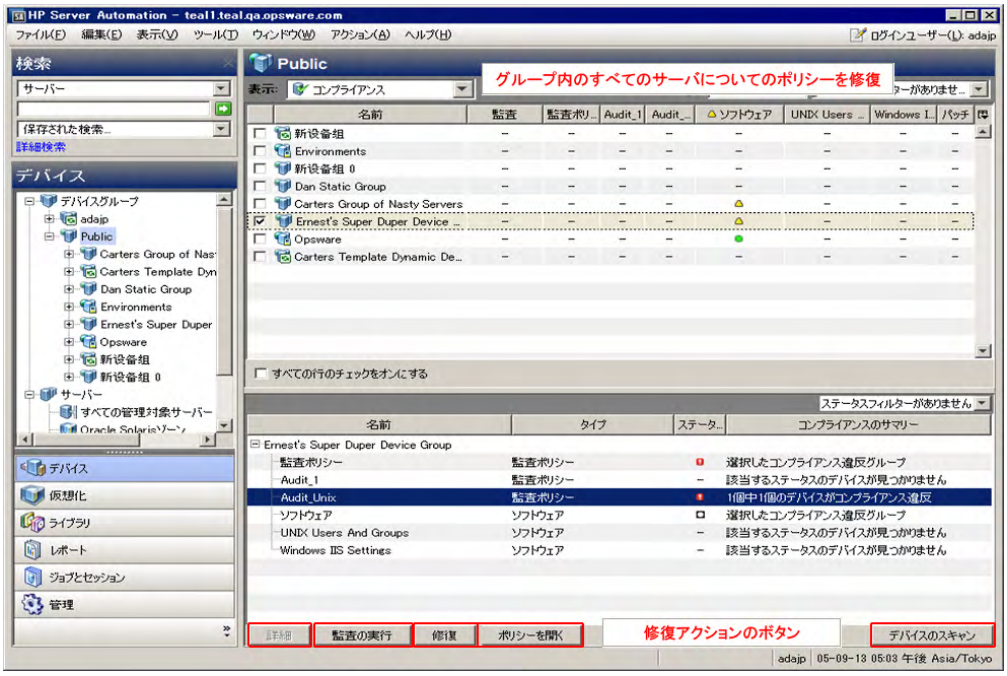
- パッチポリシーまたはソフトウェアポリシーを修復できます。
- 監査を実行して結果を表示して修復できます。
- アプリケーション構成をサーバーへプッシュできます。
- パッチ、ソフトウェア、またはアプリケーション構成のコンプライアンススキャンを実行して、サーバーの最新のコンプライアンス情報を取得できます。

サーバーまたはサーバーグループをコンプライアンスビューで選択するか、デバイスエクスプローラーまたはデバイスグループエクスプローラーで表示したときに、詳細ペインのアクションボタンを使用して、コンプライアンスに適合しないポリシーを検出して修復することができます。実行できるアクションのタイプは、ポリシーのタイプ、単一の管理対象サーバーまたはサーバーグループのいずれを選択するか、および詳細ペインで個別のポリシー、複数のポリシー、またはコンプライアンスカテゴリのロールアップを選択するかどうかによって異なります。

コンプライアンスビューでの修復 — サーバーグループ

図35は、サーバーグループで修復アクションを行うコンプライアンスビューの機能を示しています。

図35　　サーバーグループの修復



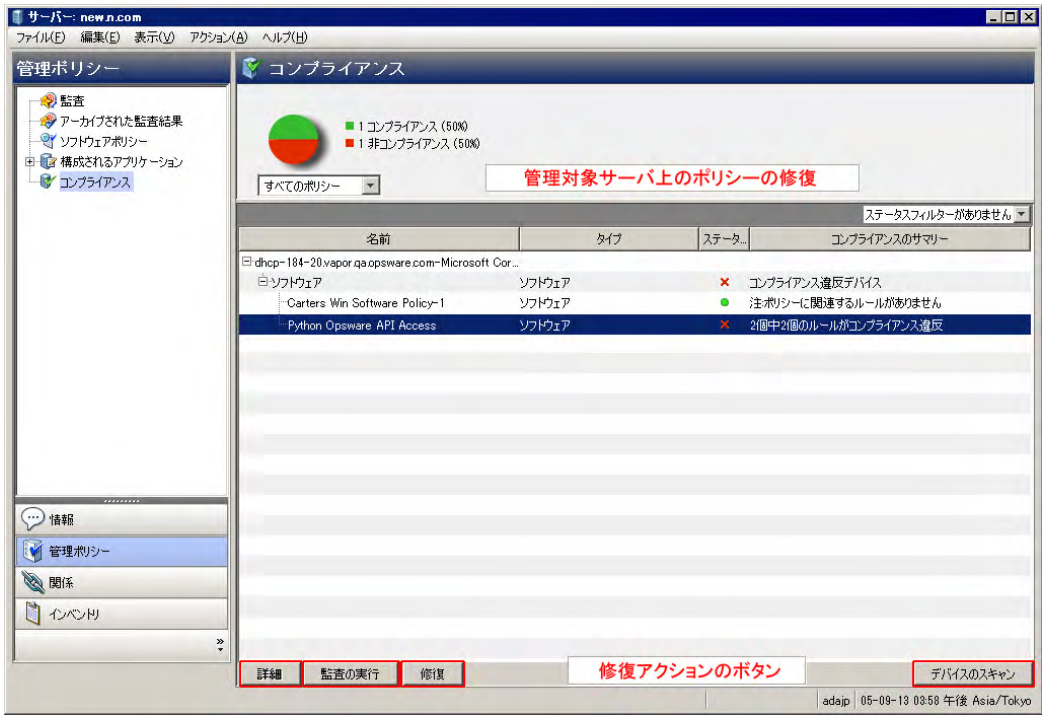
選択したグループの詳細ペインには、グループ内のすべてのサーバー (およびサブグループ内のすべてのサーバー) にアタッチされているすべてのポリシーのサマリーが、コンプライアンスカテゴリ (監査、監査ポリシー、ソフトウェア、パッチ、構成) ごとにまとめて表示されます。グループを選択する場合は、ポリシーのカテゴリ全体 (グループ内のすべてのサーバーにアタッチされているすべてのソフトウェアポリシーやすべてのパッチポリシーなど) での修復のみを行うことができます。詳細ペインでソフトウェアカテゴリを選択すると、**[修復]** ボタンが有効になります。**[修復]** ボタンをクリックすると、SAクライアントから [修復] ウィザードが起動します。このウィザードの手順を実行して、グループ内のすべてのサーバーのコンプライアンス違反状態のポリシー構成を修復します。

グループを選択して、[アクション] メニューから **[開く]** を選択した場合も、同じ内容が表示され、これらのオプションを利用することができます。この操作を行うと、グループエクスプローラーが起動して、同じグループの詳細ペインが表示され、詳細ペインにアクションボタンが表示されます。

コンプライアンスビューでの修復—サーバー

図36は、個別のサーバーで修復アクションを行うコンプライアンスビューの機能を示しています。

図36　　個別のサーバーでの修復



サーバーグループの場合、修復アクションはグループのすべてのメンバーに適用されます。個別の管理対象サーバーの場合は、サーバーにアタッチされているすべてのポリシーまたは選択したポリシーのいずれかを修復できます。たとえば、サーバーを起動し、サーバーのデバイスエクスプローラーで[**管理ポリシー**]>[コンプライアンス]を選択して、サーバーにアタッチされているすべてのコンプライアンスポリシーを表示することができます。

詳細ペインでは、監査またはソフトウェアポリシーを選択して監査を表示します。アクションボタンを使用して、監査の実行、ソフトウェアポリシーの修復、またはデバイスのコンプライアンススキャンを実行します。

コンプライアンススキャン

コンプライアンスビューでは、監査、監査ポリシー、ソフトウェア、パッチ、構成のカテゴリのコンプライアンススキャンを実行できます。コンプライアンススキャンでは、コンプライアンスポリシーの対象となるサーバーをスキャンして、サーバー構成がポリシーのルールの定義と一致しているかどうかを判断します。たとえば、コンピューター上にインストールされているパッチを確認し、パッチポリシーやソフトウェアポリシーと比較して、結果をコンプライアンスビューに返すことができます。または、サーバー上の構成ファイルの内容をチェックして、アプリケーション構成で定義されているルールと一致するかどうかを判断することができます。

監査にはスキャン機能はありませんが、監査を実行した場合も同様の結果が生成されます。監査の場合は、SAで監査を実行したときに、対象のサーバー構成がチェックされ、監査のルールの定義との適合状況が判断されます。

各カテゴリのコンプライアンススキャンでは、次のアクションが実行されます。

- **ソフトウェアコンプライアンススキャン**: サーバー上のファイルを比較して、サーバーにアタッチされているソフトウェアポリシーの内容と一致するかどうかを判断します。

- **パッチコンプライアンススキャン**: サーバーにインストールされているパッチを、サーバーにアタッチされているパッチポリシーやパッチポリシー例外と比較します。このスキャンの結果には、コンプライアンス状態の (必須のパッチがすべてインストールされている) サーバーとコンプライアンス違反の (必須のパッチが一部インストールされていない) サーバーが示されます。パッチコンプライアンスのスキャンは、Windowsパッチ管理のみに適用されます。
- **構成コンプライアンススキャン**: サーバー上の構成ファイルをサーバーにアタッチされているテンプレートで定義したアプリケーション構成と比較します。このスキャンの結果には、コンプライアンス状態の (構成ファイルの定義が構成テンプレートと一致している) サーバーとコンプライアンス違反の (構成ファイルの定義が構成テンプレートと一致していない) サーバーが示されます。構成コンプライアンスの詳細については、ドキュメントを参照してください。

パッチコンプライアンス

HP Server Automation のパッチ管理では、管理対象のサーバーやサーバーグループでパッチの識別、インストール、削除を行うことができます。Windowsパッチ管理を使用すると、Windows Server 2000 SP4、Windows Server 2003、Windows Server 2008オペレーティングシステムで、サービスパック、更新プログラムのロールアップ、ホットフィックスなどのパッチの識別とインストールを行うことができます。

コンプライアンスビューでは、パッチポリシーのコンプライアンスステータスを確認して、サーバーに適切なパッチがインストールされているかどうかを確認できます。HP Server Automationのパッチコンプライアンススキャンでは、管理対象サーバーとパブリックデバイスグループをチェックして、ポリシーおよびポリシー例外のパッチがすべて正常にインストールされているかどうかを判断します。サーバーにインストール済みのパッチ (またはインストールされていないパッチ) がパッチポリシーの定義と一致しない場合、コンプライアンスビューでサーバーのパッチポリシーが非コンプライアンス ✖ 状態として表示されます。

コンプライアンスポリシーは1回のみ実行することも、定期的スケジュールで実行することもできます。パッチポリシーをサーバーに合わせて修復すると、サーバーまたはサーバーグループのパッチコンプライアンスを確保することができます。

詳細については、『SAユーザーガイド: サーバーのパッチ適用』を参照してください。

パッチコンプライアンスのステータスの基準

パッチコンプライアンスのステータスは、次の基準で決まります。

- **パッチコンプライアンス—1つのサーバー**: パッチポリシーの少なくとも1つの項目が、ポリシーがアタッチされているサーバーで検出された内容と一致しない (またはポリシーがアタッチされているサーバーに存在しない) 場合、サーバーのパッチコンプライアンスのステータスは非コンプライアンス ✖ になります。サーバーのデバイスエクスプローラーの詳細ペインには、パッチカテゴリが非コンプライアンスとして表示され、サマリー列にルールの総数と非コンプライアンス状態のルール (パッチポリシーの項目) の数が表示されます。

  たとえば、パッチポリシーに10の項目が含まれていて、このうちの6つが非コンプライアンス状態の場合、パッチポリシーのステータスは非コンプライアンスとなり、サマリーには「10個中6個のルールがコンプライアンス違反」と表示されます。

  1つのサーバーを対象とするパッチポリシーが複数存在して、そのうちの少なくとも1つが非コンプライアンスである場合、パッチの全体のコンプライアンスステータスも非コンプライアンスと表示されます。詳細ペインのパッチカテゴリを展開すると、コンプライアンス状態でないポリシーを参照することができます。これには、各ポリシー内のコンプライアンス状態またはコンプライアンス違反のルールの数の内訳も含まれます。
- **パッチポリシー—ルールの例外**: パッチポリシーのいずれかの項目にルールの例外が適用される場合、サーバーのパッチコンプライアンスには、部分コンプライアンス ⚠ のコンプライアンスステータスが表示されます。ポリシーレベルでルールの例外が許容されるコンプライアンスカテゴリはパッチのみです。

パッチコンプライアンス－デバイスグループ: ポリシーにアタッチされているグループ内のサーバーの5% 超のステータスが非コンプライアンス ✖ である場合、サーバーグループにアタッチされたパッチポリシーはコンプライアンス状態と見なされます。この場合、パッチポリシーの全体のコンプライアンスは非コンプライアンスと表示されます。デバイスグループの非コンプライアンス状態は、コンプライアンス状態のサーバーが95%未満である場合に非コンプライアンスのステータスが表示されると覚えることもできます。

ただし、そのカテゴリで非コンプライアンス状態のサーバーがグループ内のすべてのサーバーの2%より多く 5% 以下である場合、ステータスは部分コンプライアンス ⚠ になります。デバイスグループの部分コンプライアンス状態は、コンプライアンス状態のサーバーが95%以上98%未満である場合に部分コンプライアンスのステータスが表示されると覚えることもできます。

そのカテゴリで非コンプライアンス状態のサーバーがグループ内のすべてのサーバーの 2% 未満である場合、全体のステータスはコンプライアンスになります。デバイスグループのコンプライアンス状態は、サーバーの98%以上がコンプライアンス状態であると覚えることもできます。

コンプライアンスビューのサーバーグループの詳細ペインには、パッチポリシーがコンプライアンス状態かどうかが表示されます。この情報を展開して個別のサーバーやポリシーの内訳を表示することはできません。

サーバーグループのコンプライアンスの判断に使用するしきい値は変更できます。

サーバーでのパッチコンプライアンスの修復

1 つのサーバーまたは複数のサーバーのパッチコンプライアンスを修復する際には、サーバーにアタッチされているすべてのポリシーを修復するか、個別のポリシーを修復するかを選択できます。サーバーのデバイスエクスプローラーを表示して 1 つのサーバーのパッチポリシーを修復するか、またはデバイスグループリストでポリシーを選択して複数のサーバーのパッチポリシーを修復することができます。

1つのサーバーでパッチポリシーを修復するには、次の手順を実行します。

1. デバイスエクスプローラーで 1 つのサーバーのパッチポリシーを修復するには、ナビゲーションペインで、[**デバイス**] > [**サーバー**] > [**すべての管理対象サーバー**] を選択します。
2. 内容ペインでサーバーを選択します。
3. 右クリックして [**開く**] を選択し、サーバーブラウザーを表示します。
4. ナビゲーションペインで [**管理ポリシー**] > [**コンプライアンス**] を選択します。
5. コンプライアンスビューの詳細ペインで、パッチカテゴリを展開して、個別のポリシーを選択するか、最上位のパッチカテゴリを選択します。最上位のパッチカテゴリを選択すると、サーバーにアタッチされているすべてのパッチポリシーを修復することができます。
6. [**修復**] をクリックして、[修復] ウィザードの手順を実行します。

複数のサーバーでパッチポリシーを修復するには、次の手順を実行します。

1. 複数のサーバーのパッチポリシーを修復するには、ナビゲーションペインで [**デバイス**] > [**デバイスグループ**] を選択した後に、グループを選択します。
2. [表示] ドロップダウンリストから、[コンプライアンス] を選択します。
3. コンプライアンスビューの詳細ペインで、パッチカテゴリを展開して、選択したサーバーにアタッチされているパッチポリシーを選択します。または、選択したサーバーにアタッチされているすべてのパッチポリシーを修復する場合は、最上位のパッチカテゴリを選択します。
4. 次のいずれかのボタンをクリックして、パッチポリシーを修復します。
   - **修復**: [修復] ウィザードが起動されます。このウィザードでは、選択した1つまたは複数のサーバーに対して、選択した1つまたは複数のパッチポリシーを修復できます。

- **デバイスのスキャン**:[コンプライアンスのスキャン]ウィンドウが表示されます。このウィンドウでは、最初にポリシーのタイプを選択してから、[**スキャン**]をクリックしてジョブを起動します。このプロセスでは、選択したサーバーにアタッチされている監査、監査ポリシー、ソフトウェア、パッチ、構成のすべてのポリシーに対してサーバーがスキャンされます。このプロセスによって、このサーバーを対象とする監査が影響を受けることはありません。

  スキャンの進行状況を監視するには、[コンプライアンス]ウィンドウを更新してください([F5]キーを押します)。

注:[アクション]>[スキャン]を選択して、スキャンの進行状況を表示することもできます。

グループでのパッチコンプライアンスの修復

1つのサーバーグループまたは複数のサーバーグループに対するパッチポリシーを修復する際には、1つのグループまたは複数のグループのすべてのサーバーにアタッチされているすべてのポリシーを修復できます。ただし、1つまたは複数のグループを選択する場合は、グループやサブグループ内のすべてのサーバーにアタッチされているすべてのパッチポリシーの修復のみを行うことができます。

1つのサーバーグループでパッチポリシーを修復するには、次の手順を実行します。

1. デバイスエクスプローラーで1つのサーバーのパッチポリシーを修復するには、ナビゲーションペインから[**デバイス**]>[**サーバー**]>[**すべての管理対象サーバー**]を選択します。
2. 内容ペインでサーバーを選択します。
3. 右クリックして[**開く**]を選択し、サーバーブラウザーを表示します。
4. ナビゲーションペインで[**管理ポリシー**]>[**コンプライアンス**]を選択します。
5. コンプライアンスビューの詳細ペインで、パッチカテゴリを展開して、個別のパッチポリシーを選択するか、最上位のパッチカテゴリを選択します。最上位のパッチカテゴリを選択すると、サーバーにアタッチされているすべてのパッチポリシーを修復することができます。
6. [**修復**]をクリックして、[修復]ウィザードの手順を実行します。

複数のサーバーグループでパッチポリシーを修復するには、次の手順を実行します。

1. 複数のサーバーのパッチポリシーを修復するには、ナビゲーションペインから[**デバイス**]>[**デバイスグループ**]を選択した後に、グループを選択します。
2. [表示]ドロップダウンリストから、[コンプライアンス]を選択します。
3. コンプライアンスビューの詳細ペインで、パッチカテゴリを展開して、選択したサーバーにアタッチされているポリシーを選択します。または、選択したサーバーにアタッチされているすべてのポリシーを修復する場合は、最上位のパッチカテゴリを選択します。
4. [**修復**]をクリックして、[修復]ウィザードの手順を実行します。

監査コンプライアンス

HP Server Automationの監査と修復では、監査でサーバー構成ポリシーを定義することができます。監査を使用すると、ファシリティ内のサーバーが監査ポリシーの標準に適合していることを確認することができます。監査は一連のルールで構成されます。これらのルールを定義することで、監査ポリシーの標準をモデル化することができます。たとえば、Windows COM+の構成、レジストリ設定、サービス、ファイルシステムの設定、ハードウェア構成、ユーザーとグループのパスワード設定、ソフトウェアインストール、パッケージ、ストレージ設定などで監査を構成して、理想的なサーバー構成を定義することができます。または、監査で否定的なサーバー構成を作成して、望ましくないサーバー構成を判断するのに使用することもできます。

監査コンプライアンスでは、監査の対象となるすべてのサーバーで定期的監査で定義されたルールが実際のサーバー構成と一致するかどうかを判断します。コンプライアンスビューでは、サーバーまたはサーバーグループで定期的スケジュールで実行されるすべての監査の全体および個別のコンプライアンスステータスを参照できます。非コンプライアンス ✖ 状態の監査がある場合は、監査と監査対象のサーバーとの間で検出された差異を修復できます。

コンプライアンスビューでは、定期的なスケジュールで実行される監査から監査コンプライアンスのサーバーとサーバーグループを取得します。

監査コンプライアンスのステータスの基準

監査コンプライアンスのステータスは、次の基準で決まります。

- **監査コンプライアンス—1つのサーバー**: 監査の1つのルールが監査対象のサーバーの構成と一致しない場合、サーバーの監査コンプライアンスのステータスは非コンプライアンス ✖ になります。サーバーのデバイスエクスプローラーの詳細ペインには、監査カテゴリが非コンプライアンスとして表示され、サマリー列にルールの総数と非コンプライアンス状態のルールの数が表示されます。

  たとえば、監査に10のルールが含まれていて、このうちの4つが非コンプライアンス状態の場合、監査のステータスは非コンプライアンスとなり、サマリーには「10個中4個のルールがコンプライアンス違反」と表示されます。

  サーバーを対象とする監査が複数存在して、そのうちの少なくとも1つが非コンプライアンスである場合、監査の全体のコンプライアンスステータスも非コンプライアンスと表示されます。詳細ペインの監査カテゴリを展開すると、コンプライアンス状態でない監査を参照できます。これには、各監査内のコンプライアンス状態またはコンプライアンス違反のルールの数の内訳も含まれます。

- **監査コンプライアンス—デバイスグループ**: グループに含まれるサーバーの少なくとも95%のステータスがコンプライアンス ● である場合、そのサーバーグループ (およびすべてのサブグループのすべてのサーバー) を対象とする監査はコンプライアンスであると見なされます。

  監査の対象となるグループ内のサーバーの5%超のステータスが非コンプライアンスである場合、監査の全体のコンプライアンスには非コンプライアンスと表示されます。デバイスグループの非コンプライアンス状態は、コンプライアンス状態のサーバーが95%未満である場合に非コンプライアンスのステータスが表示されると覚えることもできます。

  ただし、そのカテゴリで非コンプライアンス状態のサーバーがグループ内のすべてのサーバーの2%より多く5%以下である場合、ステータスは部分コンプライアンス ⚠ になります。デバイスグループの部分コンプライアンス状態は、コンプライアンス状態のサーバーが95%以上98%未満である場合に部分コンプライアンスのステータスが表示されると覚えることもできます。

  そのカテゴリで監査ステータスが非コンプライアンスのサーバーがグループ内のすべてのサーバーの2%未満である場合、全体のステータスはコンプライアンスになります。デバイスグループのコンプライアンス状態は、サーバーの98%以上がコンプライアンス状態であると覚えることもできます。

  コンプライアンスビューのサーバーグループの詳細ペインには、すべての監査がコンプライアンス状態かどうかが表示されます。この情報を展開して個別のサーバーや監査の内訳を表示することはできません。

監査コンプライアンスでの修復

コンプライアンスビューでは、サーバーまたはサーバーグループを対象とするすべての監査を表示し、コンプライアンス違反状態の結果を修復することができます。これにより、サーバーの構成を監査で定義したルールに適合させることができます。

修復を行うと、コンプライアンス違反状態の (サーバーの構成がルールの定義と一致しないか、サーバーの構成が存在しない) 監査ルールごとに、ルールに適合するようにルールオブジェクトがターゲットサーバーにコピーされます。また、値ベースの監査ルールの場合は、修復を行うことで、ターゲットサーバーの構成がルールに適合するように変更されます。

例: Windowsサーバーのグループをチェックして特定のレジストリキーとACLが含まれることを確認する監査で、あるWindowsサーバーに対して監査を実行した結果、いくつかのルールがコンプライアンス違反状態になることがあります。これは、監査ルールで指定したレジストリキーがターゲットサーバー上で検出されなかったことを意味します。修復を行うと、監査機能によって監査ルールで指定したレジストリキーがターゲットサーバーにコピーされます。このようにして、特定のレジストリキーと関連するACLがサーバー内に含まれるようにすることができます。サーバーのグループの場合も、修復の結果は同じです。ただし、修復操作はグループ内のすべてのサーバーに適用されます。これには、サブグループ内すべてのサーバーも含まれます。

サーバーにアタッチされている監査の修復

1つのサーバーにアタッチされている監査または複数のサーバーにアタッチされている監査を修復することができます。修復できるのは個別の監査のみです。最上位で監査を集約することはできません。選択されている任意のグループの直下に存在するすべてのサーバーが修復の対象となります。

詳細ペインで1つのポリシーが選択され、サマリーペインで1つまたは複数のサーバーが選択されている場合でも、コンプライアンスビューで[**修復**]ボタンが有効にならない場合は、通常、そのポリシーで修復対象となる監査結果が存在しないことを意味します。

コンプライアンスビューからサーバーグループに対して監査を実行することはできません。ただし、サーバーのグループに対して実行する監査を作成して、[監査結果]ウィンドウでサーバーグループに対する監査結果を修復することはできます。

1つのサーバーで個別の監査を修復する手順:

1. ナビゲーションペインで、[**デバイス**] > [**サーバー**] > [**すべての管理対象サーバー**] を選択します。
2. 内容ペインで、サーバーを選択します。
3. 右クリックして[**開く**]を選択し、サーバーエクスプローラーを表示します。
4. ナビゲーションペインで[**管理ポリシー**] > [**コンプライアンス**]を選択します。
5. コンプライアンスビューの詳細ペインで、監査カテゴリを展開して、個別のポリシーを選択します。
6. [**修復**]をクリックして、[修復]ウィザードの手順を実行します。

複数のサーバーで個別の監査を修復する手順:

1. ナビゲーションペインで[**デバイス**] > [**デバイスグループ**]を選択した後に、グループを選択します。
2. [表示]ドロップダウンリストから、[コンプライアンス]を選択します。
3. 各サーバーの横のチェックボックスをオンにして複数のサーバーを選択します。
4. コンプライアンスビューの詳細ペインで、監査カテゴリを展開し、選択したすべてのサーバーを対象とする個別の監査を選択します。
5. 次のいずれかのボタンをクリックして、1 つのサーバーまたは複数のサーバーで監査に対する修復を行います。
   - **詳細**: [監査結果] ウィンドウに、検出された監査とターゲットとの間のすべての差異が表示され、ルールまたはサーバーごとに差異を修復することができます。[**ルール詳細の表示**]リンクをクリックし、[ルール]ウィンドウを開いて監査ルールを表示します。サーバーを選択し、[**部分監査の実行**]をクリックして[サーバーの監査]ウィザードを起動します。
   - **監査の実行**: [サーバーの監査]ウィザードが起動され、監査をただちに実行するか、別の日時に監査を実行するようにスケジュール設定することができます。監査は監査対象のすべてのサーバーに対して実行されます。

- **修復**:[修復]ウィザードが起動され、監査ルールと一致しないターゲットサーバーの構成を修復することができます。ルールによる差異の修復またはサーバーによる差異の修復を行うことができます。選択したいずれのサーバーにも選択したポリシーに関して修復すべき結果がない場合は、「**修復する結果が見つかりません**」というメッセージが表示されます。
- **デバイスのスキャン**:[コンプライアンスのスキャン]ダイアログが表示されます。このダイアログでは、最初にポリシーのタイプを選択してから、[**スキャン**]をクリックしてジョブを起動します。このプロセスでは、選択したサーバーにアタッチされている監査、監査ポリシー、ソフトウェア、パッチ、構成のすべてのポリシーに対してサーバーがスキャンされます。このプロセスによって、このサーバーを対象とする監査が影響を受けることはありません。

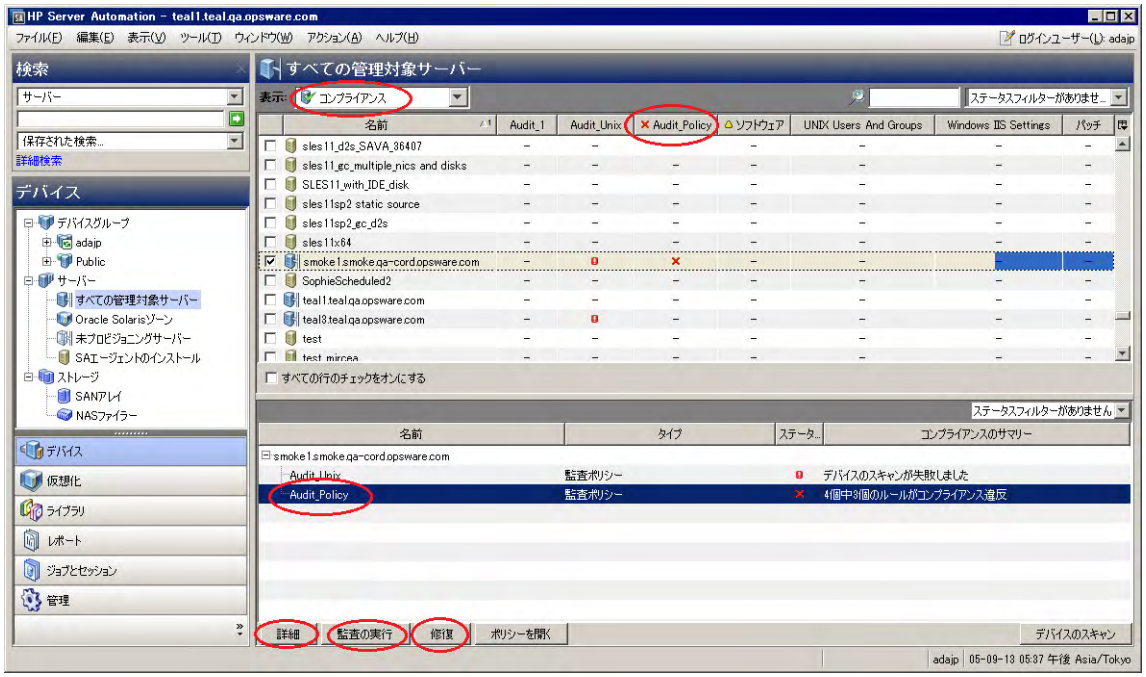
  スキャンの進行状況を監視するには、[コンプライアンス]ウィンドウを更新してください([F5]キーを押します)。

注:[アクション]>[スキャン]を選択して、スキャンの進行状況を表示することもできます。

監査ポリシーコンプライアンス

定期的に実行する監査をコンプライアンスビューに追加することができます。コンプライアンスビューには、その監査を最後に実行した結果が表示されます。監査には直接監査ルールを含めることができます。また、ソーススナップショットまたはソーススナップショット仕様から監査ルールを継承することもできます。コンプライアンスビューでは、関連する監査ルールを確認するための[監査]列を表示する必要があります。図37を参照してください。

図37　　コンプライアンスビューの監査と監査ポリシー



ベストプラクティス: 監査は監査ルールに対応した監査ポリシーにリンクします。これは一般的な推奨される使用方法です。この構造では、複数の監査を同じ監査ポリシーにリンクすることができます。監査ごとに異なるサーバーのセットや異なる定期的スケジュールを持つ複数のサーバーを含めることができます。コンプライアンスビューの[監査ポリシー]列には、監査ポリシーにリンクされた監査のすべてのコンプライアンス結果が表示されます。

サーバーのセットが重複する複数の監査が存在する場合、[監査ポリシー]列には、最後にどの監査が実行されたかに関係なく、各サーバーの最新の結果のステータスが表示されます。特定の操作に関する最新の監査結果を表示するには、コンプライアンスビューで監査を選択して、[**詳細**]、[**監査の実行**]、または[**修復**]をクリックします。図37を参照してください。

監査ポリシーは階層化できます。つまり、監査ポリシーは別の監査ポリシーにリンクすることができます。

例:

ポリシー Aはポリシー Bとリンクしています。また、ポリシー Bはポリシー Cとリンクしています。

- 監査を作成してポリシー Aにリンクした場合、その監査はポリシー A、ポリシー B、およびポリシー Cに属するコンプライアンスルールのリストを使用して実行されます。
- ポリシー A に対してコンプライアンスビューで［監査ポリシー］列を追加すると、コンプライアンスステータスにはポリシー A、ポリシー B、およびポリシー Cのすべてのルールを含む監査の結果が表示されます。
- ポリシー B またはポリシー C と直接リンクされた監査が存在しない場合、これらのポリシーに対応する個別の結果は存在しません。これらのポリシーに対してコンプライアンスビューで［監査ポリシー］列を追加すると、表示する結果が存在しないことを示すダッシュ (-) が表示されます。

➤ コンプライアンスビューの［監査］列と［監査ポリシー］列には、定期的スケジュールに対応した監査のみを表示に使用できるという違いもあります。ただし、ソフトウェアポリシーやパッチポリシーの場合と同様に、どの監査ポリシーを列にすることもできます。

コンプライアンスビューで選択可能なコンプライアンスカテゴリ (列) は構成可能です。

- デフォルト設定には、監査ポリシー、ソフトウェア、パッチ、構成が含まれます。
- 新規インストールの場合、監査カテゴリは表示されません。

ソフトウェアコンプライアンス

HP Server Automationでは、ソフトウェア管理でソフトウェアポリシーを作成し、ソフトウェアのインストールとアプリケーションの構成を同時に行うことができます。ソフトウェアポリシーには、パッケージ、RPM パッケージ、パッチ、アプリケーション構成などの異なる複数の項目を含めることができます。作成したソフトウェアポリシーは、サーバーまたはサーバーグループへアタッチすることができます。

ソフトウェアコンプライアンスは、ソフトウェアポリシーの項目が実際のサーバー構成に準拠しているかどうかを示します。実際のサーバー構成とソフトウェアポリシーの定義が一致しない場合、サーバーのソフトウェアポリシーは非コンプライアンス ✖ になります。

コンプライアンスビューでは、サーバーまたはグループのソフトウェアコンプライアンスをスキャンしたときに、ソフトウェアポリシーに対するソフトウェアコンプライアンス情報を取得します。

詳細については、『SAユーザーガイド: ソフトウェア管理』を参照してください。

ソフトウェアコンプライアンスのステータスの基準

ソフトウェアコンプライアンスのステータスは、次の基準で決まります。

- **ソフトウェアコンプライアンス—1つのサーバー**: ソフトウェアポリシーの少なくとも1つの項目が、ポリシーがアタッチされているサーバーで検出された内容と一致しない (またはポリシーがアタッチされているサーバーに存在しない) 場合、サーバーのソフトウェアコンプライアンスのステータスは非コンプライアンス ✖ になります。サーバーのデバイスエクスプローラーの詳細ペインには、ソフトウェアカテゴリが非コンプライアンスとして表示され、サマリー列にルールの総数と非コンプライアンス状態のルール (ソフトウェアポリシーの項目) の数が表示されます。

  たとえば、ソフトウェアポリシーに10の項目が含まれていて、このうちの6つが非コンプライアンス状態の場合、ソフトウェアポリシーのステータスは非コンプライアンスと表示され、サマリーには「10個中6個のルールがコンプライアンス違反」と表示されます。

1つのサーバーを対象とするソフトウェアポリシーが複数存在して、そのうちの少なくとも1つが非コンプライアンスである場合、ソフトウェアの全体のコンプライアンスステータスも非コンプライアンスと表示されます。詳細ペインのソフトウェアカテゴリを展開すると、コンプライアンス状態でないポリシーを参照できます。これには、各ポリシー内のコンプライアンス状態またはコンプライアンス違反のルールの数の内訳も含まれます。

- **ソフトウェアコンプライアンス—デバイスグループ**: ポリシーにアタッチされているグループ内のサーバーの 5% 超のステータスが非コンプライアンス ✖ である場合、サーバーグループにアタッチされたソフトウェアポリシーはコンプライアンス状態と見なされます。この場合、ソフトウェアポリシーの全体のコンプライアンスは非コンプライアンスと表示されます。デバイスグループの非コンプライアンス状態は、コンプライアンス状態のサーバーが95%未満である場合に非コンプライアンスのステータスが表示されると覚えることもできます。

  ただし、そのカテゴリで非コンプライアンス状態のサーバーがグループ内のすべてのサーバーの2%より多く 5% 以下である場合、ステータスは部分コンプライアンス ⚠ になります。デバイスグループの部分コンプライアンス状態は、コンプライアンス状態のサーバーが95%以上98%未満である場合に部分コンプライアンスのステータスが表示されると覚えることもできます。

  そのカテゴリでソフトウェアポリシーが非コンプライアンス状態のサーバーがグループ内のすべてのサーバーの2%未満である場合、全体のステータスはコンプライアンスになります。コンプライアンス状態は、サーバーの98%以上がコンプライアンス状態であると覚えることもできます。

  コンプライアンスビューのサーバーグループの詳細ペインには、ソフトウェアポリシーがコンプライアンス状態かどうかが表示されます。この情報を展開して個別のサーバーやポリシーの内訳を表示することはできません。

  サーバーグループのコンプライアンスの判断に使用するしきい値は変更できます。

ソフトウェアコンプライアンスでの修復

コンプライアンスビューでは、サーバーまたはサーバーグループにアタッチされているすべてのソフトウェアポリシーを表示し、コンプライアンス違反状態のサーバーを修復することができます。これにより、サーバーのソフトウェア構成をソフトウェアポリシーの定義に適合させることができます。

ソフトウェアの修復では、ソフトウェアポリシーの項目 (ソフトウェア、パッケージ、パッチ、スクリプト、アプリケーション構成など) ごとに、ターゲットサーバーに該当する項目がインストール (スクリプトの場合は実行) されます。項目がサーバー上に存在しない場合は、それらの項目がインストールされます。項目が存在するがポリシーと一致しない場合は、それらの項目が正しいバージョンに更新されます。

たとえば、複数のパッケージ、パッチ、スクリプトと1つのアプリケーション構成から成るソフトウェアポリシーがあり、すべてが適切なインストールおよび実行順序で構成されています。最初に、サーバーが企業のソフトウェアインストール標準に適合するように、サーバー上のソフトウェアポリシーを修復します。やがて、ソフトウェアポリシーの一部の項目が更新されます (新規パッケージ一式の追加など)。また、何らかの理由で、サーバー上のソフトウェア項目がアンインストールされます。

ソフトウェアコンプライアンススキャンを実行すると、ソフトウェアポリシーの内容とサーバー上にインストールされた実際のソフトウェアが比較され、サーバーのコンプライアンスステータスが判断されます。いずれか1つのサーバーにアタッチされている1つのソフトウェア項目だけがポリシーに適合しない場合でも、

サーバーのソフトウェアコンプライアンスステータスは非コンプライアンス ✖ になります。

サーバーまたはサーバーグループの修復を行うと、ポリシーで指定されたパッチ、パッケージ、アプリケーション構成が、ポリシーで指定された順序でインストールまたは適用されます。サーバーのグループの場合も、修復の結果は同じです。ただし、修復操作はグループ内のすべてのサーバーに適用されます。これには、サブグループ内すべてのサーバーも含まれます。

サーバーでのソフトウェアコンプライアンスの修復

1つのサーバーまたは複数のサーバーのソフトウェアコンプライアンスを修復する際には、サーバーにアタッチされているすべてのポリシーを修復するか、個別のポリシーを修復するかを選択できます。

選択したすべてのサーバーのすべてのソフトウェアポリシーを修復するソフトウェア全体ポリシーを選択することができます。グループが選択されている場合、そのグループの直下に存在するすべてのサーバーに対して修復が行われます。詳細ペインで1つのソフトウェアポリシーが選択されている場合、サマリーペインで選択されたエンティティで該当するポリシーが修復されます。

1つのサーバーでソフトウェアポリシーを修復する手順:

1. ナビゲーションペインで、[**デバイス**] > [**サーバー**] > [**すべての管理対象サーバー**] を選択します。
2. 内容ペインでサーバーを選択します。
3. 右クリックして [**開く**] を選択し、サーバーブラウザーを表示します。
4. ナビゲーションペインで [**管理ポリシー**] > [**コンプライアンス**] を選択します。
5. コンプライアンスビューの詳細ペインで、ソフトウェアカテゴリを展開して、個別のソフトウェアポリシーを選択するか、最上位のソフトウェアカテゴリを選択します。最上位のソフトウェアカテゴリを選択すると、サーバーにアタッチされているポリシーを修復することができます。
6. [**修復**] をクリックして、[修復] ウィザードの手順を実行します。SAで修復するデバイスが見つからない場合は、警告ダイアログが表示されます。

複数のサーバーでソフトウェアポリシーを修復する手順:

1. ナビゲーションペインで [**デバイス**] > [**デバイスグループ**] を選択した後に、グループを選択します。
2. [表示] ドロップダウンリストから、[コンプライアンス] を選択します。
3. 内容ペインで、サーバーを選択します。
4. コンプライアンスビューの詳細ペインで、ソフトウェアカテゴリを展開して、選択したサーバーにアタッチされているソフトウェアポリシーを選択します。または、選択したサーバーにアタッチされているすべてのソフトウェアポリシーを修復する場合は、最上位のソフトウェアカテゴリを選択します。
5. 次のいずれかのボタンをクリックして、ソフトウェアポリシーを修復します。
   - **修復**: [修復] ウィザードが起動されます。このウィザードでは、選択した1つまたは複数のサーバーに対して、選択した1つまたは複数のソフトウェアポリシーを修復できます。
   - **デバイスのスキャン**: [コンプライアンスのスキャン] ウィンドウが表示されます。このウィンドウでは、最初にポリシーのタイプを選択してから、[**スキャン**] をクリックしてジョブを起動します。このプロセスでは、選択したサーバーにアタッチされている監査、監査ポリシー、ソフトウェア、パッチ、構成のすべてのポリシーに対してサーバーがスキャンされます。このプロセスによって、このサーバーを対象とする監査が影響を受けることはありません。

     スキャンの進行状況を監視するには、[コンプライアンス] ウィンドウを更新してください ([F5] キーを押します)。

注: [アクション] > [スキャン] を選択して、スキャンの進行状況を表示することもできます。

グループでのソフトウェアコンプライアンスの修復

1つのサーバーグループまたは複数のサーバーグループに対するソフトウェアポリシーを修復する際には、1つのグループまたは複数のグループのすべてのサーバーにアタッチされているすべてのポリシーを修復できます。ただし、1つまたは複数のグループを選択する場合は、グループやサブグループ内のすべてのサーバーにアタッチされているすべてのソフトウェアポリシーの修復のみを行うことができます。

1つのサーバーグループまたは複数のサーバーグループに対するソフトウェアポリシーを修復する手順:

1 デバイスエクスプローラーで 1 つのサーバーのソフトウェアポリシーを修復するには、ナビゲーションペインで、[**デバイス**] > [**サーバー**] > [**すべての管理対象サーバー**] を選択します。

2 内容ペインで、サーバーを選択します。

3 右クリックして [**開く**] を選択し、デバイスブラウザーを表示します。

4 ナビゲーションペインで [**管理ポリシー**] > [**コンプライアンス**] を選択します。

5 コンプライアンスビューの詳細ペインで、ソフトウェアカテゴリを展開して、個別のソフトウェアポリシーを選択するか、最上位のソフトウェアカテゴリを選択します。最上位のソフトウェアカテゴリを選択すると、サーバーにアタッチされているすべてのポリシーを修復することができます。

6 [**修復**] をクリックして、[修復] ウィザードの手順を実行します。

または

7 グループに属するサーバーのリストを表示する内容ペインで、サーバーの横にあるチェックボックスをオンにして複数のサーバーを選択します。(オプション) すべてのサーバーを選択する場合は、[**すべての行のチェックをオンにする**] を選択します。

8 複数のサーバーのソフトウェアポリシーを修復するには、ナビゲーションペインで [**デバイス**] > [**デバイスグループ**] を選択した後に、グループを選択します。

9 [表示] ドロップダウンリストから、[コンプライアンス] を選択します。

10 コンプライアンスビューの詳細ペインで、ソフトウェアカテゴリを展開して、選択したサーバーにアタッチされているソフトウェアポリシーを選択します。または、選択したサーバーにアタッチされているすべてのソフトウェアポリシーを修復する場合は、最上位のソフトウェアカテゴリを選択します。

11 次のいずれかのボタンをクリックして、ソフトウェアポリシーを修復します。

- **修復**: [修復] ウィザードが起動されます。このウィザードでは、選択した1つまたは複数のサーバーに対して、選択した1つまたは複数のソフトウェアポリシーを修復できます。
- **デバイスのスキャン**: [コンプライアンスのスキャン] ウィンドウが表示されます。このウィンドウでは、最初にポリシーのタイプを選択してから、[**スキャン**] をクリックしてジョブを起動します。このプロセスでは、選択したサーバーにアタッチされている監査、監査ポリシー、ソフトウェア、パッチ、構成のすべてのポリシーに対してサーバーがスキャンされます。このプロセスによって、このサーバーを対象とする監査が影響を受けることはありません。

  スキャンの進行状況を監視するには、[コンプライアンス] ウィンドウを更新してください ([F5] キーを押します)。

注: [アクション] > [スキャン] を選択して、スキャンの進行状況を表示することもできます。

構成コンプライアンス

HP Server Automationでは、アプリケーション構成を使用して、管理対象サーバー上の構成ファイルを管理します。アプリケーション構成では、個別のサーバーまたはサーバーグループの 1 つまたは複数の構成ファイルを管理できます。個々のアプリケーション構成には、フィールドの理想的な構成状態をモデル化する 1 つまたは複数のテンプレートが含まれます。これらのテンプレートを使用すると、サーバー上の特定のファイルの構成値 (キーと値のペア) を管理できます。

たとえば、データセンター内のサーバーのhostsファイルを管理するアプリケーション構成を作成することができます。標準的な Unix hosts ファイルの IP アドレスとホスト名のキーと値のペアを定義して、そのアプリケーション構成を hosts ファイルを含む複数のサーバーやサーバーグループにアタッチすることができます。このアプリケーション構成は、ターゲットサーバー上のhostsファイルに含まれるIPアドレスとホスト名の定義が正しいことを確認するためのポリシーとして機能します。

アプリケーション構成コンプライアンスは、サーバーにアタッチされているすべてのアプリケーション構成(ポリシー)が、管理対象サーバー上の実際のアプリケーション構成ファイルと適合しているかどうかを示します。hostsファイルの例では、サーバー構成のhostsファイルの内容がアプリケーション構成で定義した値と一致しない場合に、サーバーの[構成]が非コンプライアンス ✖ になります。複数のアプリケーション構成がサーバーにアタッチされており、アプリケーション構成のターゲットとなる実際の構成ファイルのいずれか1つでも異なる場合は、コンプライアンスビューでサーバー全体が非コンプライアンスと表示されます。

逆に、アプリケーション構成とサーバー上のファイルの間に違いがない場合、[構成]のコンプライアンスステータスはコンプライアンス ● 状態になります。コンプライアンスビューでサーバーの[構成]のコンプライアンスステータスがコンプライアンスと表示されるには、すべてのアプリケーション構成が完全にコンプライアンス状態である必要があります。

アプリケーション構成のターゲットとなる構成ファイルの最新の状態をチェックするには、アプリケーション構成のコンプライアンススキャンを実行して、アプリケーション構成とサーバー上の実際の構成ファイルとの間に違いがあるかどうかを確認します。

詳細については、『SAユーザーガイド: アプリケーション構成』を参照してください。

構成コンプライアンスのステータスの基準

構成コンプライアンスのステータスは、次の基準で決まります。

- **構成コンプライアンス—1つのサーバー**: アプリケーション構成と、ターゲットサーバー上の実際の構成ファイルとの間に違いが見つかった場合、サーバーの構成コンプライアンスのステータスは非コンプライアンス ✖ になります。サーバーのデバイスエクスプローラーの詳細ペインでは、構成カテゴリが非コンプライアンスと表示されます。複数のアプリケーション構成がサーバーにアタッチされており、アプリケーション構成のターゲットとなる実際の構成ファイルのいずれか1つでもアプリケーション構成と異なる場合は、コンプライアンスビューでサーバー全体が非コンプライアンスとみなされます。
- **構成コンプライアンス—デバイスグループ**: アプリケーション構成にアタッチされているグループ内のサーバーの5%超のステータスが非コンプライアンス ✖ である場合、サーバーグループにアタッチされたアプリケーション構成はコンプライアンス状態と見なされます。この場合、構成の全体のコンプライアンスは非コンプライアンスと表示されます。デバイスグループの非コンプライアンス状態は、コンプライアンス状態のサーバーが95%未満である場合に非コンプライアンスのステータスが表示されると覚えることもできます。

  ただし、そのカテゴリに対して非コンプライアンス状態のサーバーがグループ内のすべてのサーバーの2%より多く5%以下である場合、ステータスは部分コンプライアンス ⚠ になります。デバイスグループの部分コンプライアンス状態は、コンプライアンス状態のサーバーが95%以上98%未満である場合に部分コンプライアンスのステータスが表示されると覚えることもできます。

  そのカテゴリで構成が非コンプライアンス状態のサーバーがグループ内のすべてのサーバーの2%未満である場合、全体のステータスはコンプライアンスになります。コンプライアンス状態は、サーバーの98%以上がコンプライアンス状態であると覚えることもできます。

  コンプライアンスビューのサーバーグループの詳細ペインには、アプリケーション構成がコンプライアンス状態かどうかが表示されます。この情報を展開して個別のサーバーやポリシーの内訳を表示することはできません。

  サーバーグループのコンプライアンスの判断に使用するしきい値は変更できます。

構成コンプライアンスの修復—サーバーおよびグループ

アプリケーション構成での修復は、他のコンプライアンスカテゴリタイプとやや異なります。(監査ポリシー、ソフトウェア、またはパッチの場合のように) サーバー上でポリシーを修復するのではなく、アプリケーション構成を修復する場合は、デバイスエクスプローラーまたはグループエクスプローラーでアプリケーション構成を選択します。その後、プッシュ機能を使用して、アプリケーションで定義された値をサーバーまたはサーバーグループの実際の構成ファイルにプッシュします。アプリケーション構成をプッシュすると、アプリケーション構成テンプレートで定義されたすべての値が、ターゲットの構成ファイルに追加されるか、構成ファイルの既存の値と置き換えられます。

アプリケーション構成の値がどのようにプッシュされるか (リストやスカラーのシーケンスなど) は、アプリケーション構成の継承階層での値の設定方法と、構成テンプレートで構成されているシーケンスマージモードによって異なります。

サーバーまたはサーバーグループでアプリケーション構成を修復する手順:

1. デバイスエクスプローラーで 1 つのサーバーのアプリケーション構成を修復するには、ナビゲーションペインで、[**デバイス**] > [**サーバー**] > [**すべての管理対象サーバー**] を選択した後に、サーバーを選択します。

   または

2. サーバーのグループのアプリケーション構成を修復するには、ナビゲーションペインで [**デバイス**] > [**デバイスグループ**] を選択した後に、グループを選択します。
3. 右クリックして [**開く**] を選択し、デバイスブラウザーを表示します。
4. 情報ペインで、[**管理ポリシー**] > [**構成されるアプリケーション**] を選択します。『SAユーザーガイド: アプリケーション構成』を参照して操作を続行します。次の項も併せて参照してください。

索引

き

け

こ

さ

し