Ivanti Patch for Windows® Servers

アップグレード ガイド

著作権および商標

文書情報および印刷履歴

文書番号:該当なし

日付	バージョン	説明
2010 年 9 月	NetChk Protect 7.6	製品のブランディングを更新し、新しい7.6の機能と改善点に関する情報を追加します。
2011 年 3 月	NetChk Protect 7.8	新しい7.8 の機能と改良に関する情報を追加。
2011 年 10 月	VMware vCenter Protect 8.0	製品のブランディングを更新し、8.0アップグレードタスクに関する情報を追加します。7.5 より前のバージョンの情報をすべて削除する
2011 年 12 月	Vmware vCenter Protect 8.0, 文書改訂 A	アップグレードプロセスを開始する前に、データベースを圧縮する方法を説明するステップを追加。
2012 年 9月	VMware vCenter Protect 8.0.1	製品名とバージョンを更新し、カバー グラフィックスを更新します。
2013年 5 月	Shavlik Protect 9.0	システム要件を更新。新しい9.0 の機能と改良に関する情報を追加。
2014 年 4 月	Shavlik Protect 9.1	システム要件の更新新しい9.1 の機能と改良に関する情報を追加。
2015年 9月	Shavlik Protect 9.2	システム要件の更新新しい9.2 の機能と改良に関する情報を追加。
2017年4月	Ivanti Patch for Windows® Servers 9.3	ブランド名を Ivanti に変更し、ウイルス対策への参照を削除し、システム要件を更新し、新しい v9.3の機能と改良の情報を追加しました。

はじめに

このガイドの目的

Ivanti Patch for Windows® Servers 9.3 のご利用について。本書では、Shavlik Protect 9.1または Shavlik Protect 9.2 から Ivanti Patch for Windows® Servers 9.3にアップグレードする方法について説明します。

アップグレード手順の説明に加えて、このドキュメントでは、Ivanti Patch for Windows® Servers 9.3にアップグレードする際に気をつけなければならないいくつかの機能上の相違点を挙げています。また、大幅に変更されたユーザーインターフェイスの領域を強調表示します。

新しいシステム要件と前提条件

Ivanti Patch for Windows® Servers 9.3の新しい要件と前提条件を確認してください。

- Windows Server 2016および Windows 10はコンソール コンピュータとしてサポートされます
- Microsoft .NET Framework 4.6.2以降
- Microsoft Visual C++ Redistributable for Visual Studio 2015
- SQL Server 2005のサポートが削除されました。新しい最低要件は SQL Server 2008です。
- Windows XP および Windows Server 2003 はエージェント コンピュータでサポートされません n
- ウイルス対策はこのリリースではサポートされていません

不足している前提条件ソフトウェアはすべて、アップグレード処理中に自動的にインストールされます。システム要件の一覧については、*Ivanti Patch for Windows® Servers インストール ガイド*をご参照ください。

アップグレードを実行するためのユーザ アカウント要件

アップグレードを実行するには、ユーザ アカウントが次の要件を満たしている必要があります。

- データベース アップグレードを実行するユーザは、db_owner ロールのメンバーでなければなりません。
- 複数のコンソールがデータベースを共有し、別のコンソールがアップグレード済みのデータベースにリンクしている場合、使用するユーザ アカウントは、db_datareader、db_datawriter、STExec、および STCatalogupdate データベース ロールのメンバーでなければなりません。また、バックグラウンド処理で使用されるサービス アカウントは、db_owner ロールのメンバーでなければなりません。アカウントが db_securityadmin および db_accessAdmin のメンバーである場合、データベース アップグレード ツールは必要なロールを自動的にマッピングして構成しようとします。

アップグレード手順

概要

このセクションでは、Shavlik Protect 9.1または Shavlik Protect 9.2 から Ivanti Patch for Windows® Servers 9.3にアップグレードする方法について説明します。アップグレード時に、Migration Tool を使用してコンソールを新しいコンピュータに移行する場合は、アップグレードを実行する前に、『移行ツール ユーザ ガイド』をご参照ください。

アップグレードを実行する前に、必ず、ページの*「重要な変更と機能強化」*セクションに目を通し、17 アップグレードによるシステムへの影響を理解してください。また、アップグレード中に保持されないものもあるため、現在のすべてのカスタム ユーザ設定のメモを作成することをお勧めします (14ページを参照)。

メモ: コンソールのアップグレードが完了した後には、ターゲット コンピュータにインストールされるすべてのエージェントは、次回のコンソールへのチェックインのときに自動的にアップグレードされます。

アップグレードの実行

1. スキャン結果とパッチ配布結果を格納するために使用されるデータベースの未使用の領域を解放します。

   SQL Server Management Studio で、ShavlikScans データベースを右クリックし、**[タスク] > [圧縮] > [データベース]** の順に選択します。

2. SQL Server Management Studio を使用して現在のデータベースのバックアップを作成します。

   データベースにはプログラム処理の結果が含まれ、構成情報も含まれます。データベースのバックアップは重要なステップです。

3. Shavlik Protect などのコンソール コンピュータを実行するすべてのプログラムを終了します。

4. 次のリンクを使用して、Ivanti Patch for Windows® Servers 9.3実行ファイルをコンソール コンピュータにダウンロードします。

   https://www.ivanti.com/ja-JP/resources/downloads

5. 次の方法のいずれかでインストール処理を開始します。

   - ファイル **IvantiPatchForServers.exe** をダブルクリックします。
   - コマンド プロンプトにファイル名を入力します。これで、1つ以上のコマンドライン オプションを使用できます。きわめて大規模なデータベースをアップグレードする場合には、この方法を検討してください。DBCOMMANDTIMEOUT オプションは、インストール中に SQL コマンド タイムアウト値を指定するために使用されます。既定値は1 GB につき15分です。最低タ

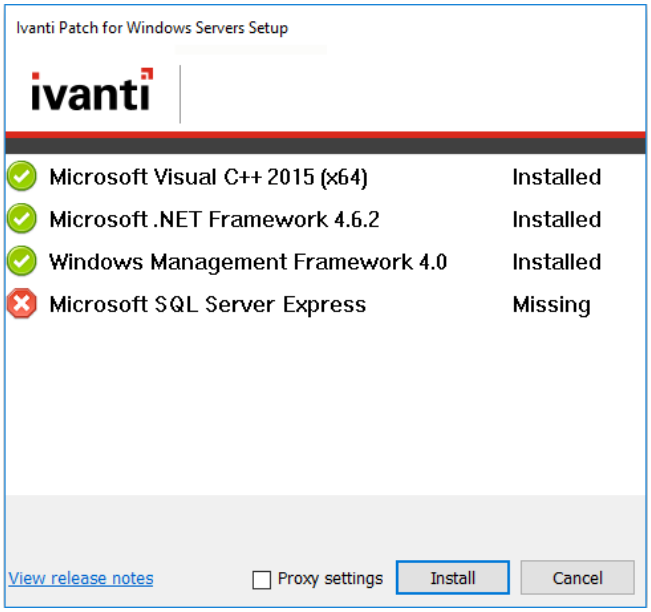
イムアウト値は、1 GB につき15分または1800秒 (30分) の大きい方の値です。制約されたリソースのためアップグレードに例外的に長い時間がかあることが想定される場合にのみ、既定値を上書きしてください。たとえば、4 GB のデータベースがある場合、既定のタイムアウト値を3600秒 (60分) から7200秒 (120分) に2倍にするには、次のコマンドを入力します。

```
IvantiPatchForServers /wi:"DBCOMMANDTIMEOUT =7200"
```

メモ:再起動が必要であることを示すメッセージが表示された場合は、[OK] をクリックすると、再起動した後に、自動的にインストール処理が再開されます。

6. アップグレードを続行するかどうかを確認するダイアログに応答します。

   [はい] をクリックして、コンソール コンピュータに1つ以上の前提条件がない場合は、次のようなダイアログが表示されます。すべての前提条件がある場合は、次の手順をスキップして、**[ようこそ]** ダイアログに進みます。



7. **[インストール]** をクリックし、インストールされていない前提条件をインストールします。

   インストール処理のこの段階で、セットアップ ウィザードが再起動を実行しなければならない場合があります。再起動が必要な場合は、コンピュータが再起動すると、[セットアップ] ダイアログが再表示されます。もう一度 **[インストール]** をクリックして、アップグレードを続行します。

   [ようこそ] ダイアログが表示されます。

8. **[ようこそ]** ダイアログの情報を確認し、**[次へ]** をクリックします。

   使用許諾契約が表示されます。プログラムをインストールするには、使用許諾契約の条項に同意する必要があります。

9. **[使用許諾契約に同意する]** チェックボックスを有効にし、**[次へ]** をクリックします。

   [インストール先フォルダ] ダイアログが表示されます。

10. プログラムの既定の場所を変更する場合は、[参照] ボタンをクリックし、新しい場所を選択します。また、デスクトップにショートカット アイコンをインストールすることもできます。完了したら、**[次へ]** をクリックします。

    [製品改善プログラム] ダイアログが表示されます。説明を読み、プログラムに参加するかどうかを決定します。このプログラムでは、Ivanti が、今後の製品バージョンを改善する目的で、製品の使用状況情報を収集できます。

11. **[次へ]** をクリックします。

    [インストール準備完了] ダイアログが表示されます。

12. インストールを開始するには、**[インストール]** をクリックします。

    インストール処理が終わりに近づくと、**[データベース セットアップ ツール]** ダイアログが表示されます。

    重要!次のステップでは、**[新しいデータベースを作成する]** を選択しないでください。選択した場合は、新しいデータベースが作成され、既存のデータが使用されません。

13. 必ず **[既存のデータベースを使用する]** を選択し、**[次へ]** をクリックします。

14. 指定されたボックスを使用し、ユーザおよびサービスが SQL Server データベースにアクセスする方法を定義します。

    データベース サーバとインスタンスの選択

    - **サーバ名:**コンピュータを指定するか、コンピュータおよびコンピュータで実行中の SQL Server インスタンスを指定できます。
    - **データベース名:**使用するデータベース名を指定します。既定のデータベース名は **Protect** です。

    ユーザによる対話方式でのデータベース接続方法の選択

    ユーザがデータベースへのアクセスを必要とする処理を実行するときに、プログラムで使用する認証資格情報を指定します。

    - **統合 Windows 認証:**これは推奨される既定のオプションです。Ivanti Patch for Windows® Servers は現在ログインしているユーザの認証資格情報を使用して、SQL Server データベースに接続します。**[ユーザ名]** および **[パスワード]** ボックスは使用できません。

- **特定の Windows ユーザ:**SQL Server データベースがリモート コンピュータにある場合にのみ、このオプションを選択します。データベースがローカル (コンソール) コンピュータにある場合は、このオプションの効果はありません。(ローカル コンピュータ認証資格情報の詳細については、『*Ivanti Patch for Windows® Servers 管理ガイド*』の「認証資格情報の指定TAG」をご参照ください。すべての Ivanti Patch for Windows® Servers ユーザは、リモートSQL Server データベースとのインタラクションが必要な操作を実行する場合、提供された資格情報を使用します。
  SQL 認証:このオプションを選択すると、指定された SQL Server にログインするための特定のユーザ名およびパスワードの組み合わせを入力できます。

  注意!SQL 認証資格情報を指定し、SQL 接続の SSL 暗号化が実装されていない場合、認証資格情報はクリア テキスト形式でネットワーク上に渡されます。

- **データベース接続のテスト:**指定したインタラクティブ ユーザ認証資格情報を使用してデータベースに接続できることを検証するには、このボタンをクリックします。

サービスによるデータベース接続方法の選択

データベースに接続するときに、バックグラウンド サービスで使用する認証資格情報を指定します。SQL Server にログインし、ステータス情報を提供するために、結果のインポート ユーザ、エージェント処理、および他のサービスが使用する認証資格情報があります。

- **コンソール サービスでの別の認証資格情報の使用:**
  - SQL Server データベースがローカル コンピュータにインストールされている場合、一般的に、このオプションを無視するには、チェック ボックスをオフにします。この場合、インタラクティブ ユーザに対して指定した認証資格情報および認証モードが使用されます
  - 通常、SQL Server データベースがリモート コンピュータにある場合にのみ、このチェック ボックスをオンにします。データベースがリモート コンピュータ上にある場合、リモート データベース サーバのデータベースで認証できるアカウントが必要です。
- **認証方法:[コンソール サービスでの別の認証資格情報の使用]** が有効な場合にのみ使用できます。
  - **統合 Windows 認証:**このオプションを選択すると、リモート SQL Server に接続するためにコンピュータ アカウントが使用されます。認証資格情報を安全に送信するためには、Kerberos ネットワーク認証プロトコルが使用できなければなりません。[ユーザ名] および [パスワード] ボックスは使用できません。

メモ:[統合 Windows 認証]を選択した場合、コンピュータ アカウントで SQL Server ログイン情報を作成しようとします。アカウント作成処理が失敗した場合、リモート *SQL Server を手動*

*で構成し、コンピュータ*アカウント認証資格情報を許可する手順について、*Ivanti Patch for Windows® Servers インストール ガイドの* ページの「SQL Server のインストール後の注記」をご参照ください。この手順は、Ivanti Patch for Windows® Servers のアップグレード処理が完了した後、プログラムを起動する前に実行します。

- **特定の Windows ユーザ:**これにより、特定のユーザ名およびパスワードの組み合わせを指定できます。Ivanti Patch for Windows® Servers のバックグラウンド サービスでは、これらの認証資格情報を使用して、SQL Server データベースに接続します。これは、何らかの理由により、統合 Windows 認証を実装できない場合、優れたフォールバック オプションになります。
- **SQL 認証:**このオプションを選択すると、SQL Server にログインするときに使用するサービスで、特定のユーザ名およびパスワードの組み合わせを指定します。

15. すべての必須情報を入力した後、**[次へ]** をクリックします。

メモ:インストール プログラムで、指定した認証資格情報に関する問題が検出された場合、エラー メッセージが表示されます。通常、これは指定したユーザ アカウントが存在しないことを示します。修正してから、再試行してください。

コンソールは既存のデータベースにリンクされます。

16. **[次へ]** をクリックします。
17. **[インストール完了]** ダイアログで **[完了]** をクリックします。
18. **[Ivanti Patch for Windows® Servers セットアップ ウィザードの完了]** ダイアログで **[Ivanti Patch for Windows® Servers を起動する]** チェックボックスをオンにし、**[完了]** をクリックします。

コンソールで実行されるアップグレード タスク

アップグレードを完了するには、Ivanti Patch for Windows® Servers コンソールで次のタスクを実行する必要があります。

スケジューラ認証資格情報の割り当て

メモ: これは、v9.1からv9.3にアップグレードする場合にのみ適用されます。

スケジュールされたコンソールタスクを実行するには、現在のユーザアカウントと一致するスケジューラ認証資格情報が必要です。コンソールでスケジュールされたタスクがあり、スケジューラ認証資格情報が設定されていない場合は、プロンプトが表示され、起動時に認証資格情報を設定する必要があります。Ivanti Patch for Windows® Servers が起動するたびにこのチェックが実行され、スケジュールされたタスクが継続的に実行されることを保証します。

スケジュールされたタスクの確認

スケジュールされたタスクは、2つの別の領域で監視および管理されます。両方のスケジュール タスク マネージャを確認し、既存のタスクが正しく移行されたことを検証してください。

- **スケジュール コンソール タスク マネージャ**を使用すると、1つの場所から、パッチ スキャン、資産スキャン、コンソール コンピュータへのパッチ配布、スクリプト実行、スケジュールされたレポートなどの現在コンソールでスケジュールされているタスクを表示できます。
- **スケジュール リモート タスク マネージャ**を使用すると、1つの場所から、リモート ターゲット コンピュータで現在スケジュールされている電源タスクおよびパッチ配布タスクを表示できます。

ライセンスの更新 (オフライン コンソールのみ)

コンソールがオフライン (インターネット接続がない) の場合、Ivanti Patch for Windows® Servers 9.3の新機能を表示して使用するには、手動でライセンスを更新する必要があります。

オフライン コンソールの認証については、オンライン ヘルプ システムの **[クイック スタート] > [設定] > [プログラムの初期表示] > [プログラムの認証]** をご参照ください。

コンソールがオンラインの場合、アップグレード処理中にライセンスが自動的に更新されます。

パッチ スキャン テンプレートとパッチ グループの確認

特に、v9.1からv9.3にアップグレードする場合には、これらの領域で3つの問題を考慮する必要があります。

- **パッチ スキャン テンプレート:[パッチ スキャン テンプレート]**ダイアログの **[フィルタリング]**タブが更新され、スキャンの精度が改善されました。アップグレード処理では、既存のパッチ スキャン テンプレートが自動的に新しいスタイルに更新されますが、テンプレートを再確認し、変更を検証してください。
- **パッチ グループ:**パッチ グループは別のダイアログで定義されません。パッチ ビューで作成および管理されるようになりました。Ivanti は多数の古いパッチのサポートを廃止したため、アップグレード後にはパッチ グループが小さくなる場合があります。
- **変更および自動生成されたパッチ グループ:**パッチ スキャン テンプレートの動作を保持するには、アップグレード処理中に 1 つ以上の既存のパッチ グループが変更され、1 つ以上の新しいパッチ グループが自動的に生成されるる場合があります。
    - **変更されたパッチグループ：**9.0または9.1のパッチスキャンテンプレートの**パッチフィルタ設定**セクション内のパッチグループを参照し、**[選択したスキャン]**を有効にすると、スキャンテンプレートフィルタで定義された条件を満たさないパッチはグループから削除されます 。理由: Protect 9.1では、スキャンテンプレートフィルタは、実際にスキャンまたはデプロイすることを意図しないパッチタイプをパッチグループに含めることを隠すことができます。Ivanti Patch for Windows® Servers 9.3では、パッチグループをベースラインとして使用すると、スキャンテンプレートフィルタが適用されず、パッチグループの不正確さが明らかになります。アップグレードプロセスでこの状況が検出されると、スキャンテンプレートとパッチグループ間の意図したやりとりを維持するために、パッチグループが自動的に変更されます。

      例:

      1パッチ グループには、セキュリティ、セキュリティ以外、ソフトウェア配布パッチが混在すると仮定します。このパッチ グループを参照するスキャン テンプレートでは、**[パッチ フィルタ設定]** セクションが **[選択した項目のスキャン]** に設定され、**[パッチ プロパティ]** セクションがセキュリティ パッチのみを検出するように設定されています。この構成では、**パッチ プロパティ** フィルタが優先され、セキュリティ パッチのみが検出されます (パッチ グループには、セキュリティ以外のパッチおよびソフトウェア配布パッチのみが含まれるという事実は無視されます)。

      9.3にアップグレードすると、スキャン テンプレートはベースライン フィルタとしてパッチ グループを定義し、他のすべてのスキャン テンプレート フィルタは無視されます。パッチ グループが修正されない場合は、セキュリティ以外のパッチとソフトウェア パッチが検出されます (スキャンを実行するときに **[スキャン後にパッチを自動配布する]** チェックボックスを有効にした

場合は配布もされます)。アップグレード処理はこの不一致を認識し、セキュリティ以外のパッチとソフトウェア配布パッチをパッチ グループから削除します。

メモ:今後は、不要なパッチまたはパッチ タイプを追加せずに、注意して、パッチ グループを正しく管理してください。

- **自動生成されたパッチ グループ:**既存のパッチ グループのコピーは、次の条件のいずれかが満たされた場合に、アップグレード処理によって自動的に生成されます。
  - パッチ グループはパッチ スキャン テンプレートの **[パッチ フィルタ設定]** セクションで参照され、**[選択した項目のスキャン]** が有効な場合
  - パッチ グループがエージェント ポリシーまたは別のフィルタ定義を含む2つ目のスキャン テンプレートによって参照される場合
  - パッチ グループが互換性を維持するためにアップグレード処理によって修正される必要がある場合 (上記を参照)

  上記のとおり、この状況では、パッチ グループのコピーが生成され、その後に修正されます。新しいパッチ グループの名前は ***<パッチ グループ名> -generated for <スキャン テンプレート名>** です。パッチ グループを参照するスキャン テンプレートは、新しいパッチ グループ名を使用するように更新されます。元のパッチ グループは保持され、エージェント ポリシーまたは他のスキャン テンプレートからの参照が保持されます。

  変更を確認し、必要に応じて、自動生成されたパッチ グループをよりわかりやすい意味のある名前に変更してください。

コンソールへのエイリアスの割り当て

次の条件の1つ以上が該当する場合には、このタスクが必要です。

- コンソール コンピュータを新しいドメインに割り当てた場合
- コンソールの新しい共通名または IP アドレスを指定した場合
- エージェントを手動でインストールし、エージェントが IP アドレスを使用してコンソールと通信する場合

このような条件に該当する場合、**コンソール エイリアス エディタ** ツールを使用して、古いコンソール名とアドレスを信頼できるエイリアスに指定する必要があります。そうでない場合は、エージェントが Ivanti Patch for Windows® Servers コンソールにチェックインする際、またはエージェントレス コンピュータがパッチ配布ステータス メッセージをコンソールに送信しようとする際に、接続しているコンピュータが信頼できることを検証できません。

1. **[ツール] > [コンソール エイリアス エディタ]** を選択します。

[コンソール エイリアス エディタ] ダイアログが表示されます。現在コンソール名を識別するために使用される名前と IP アドレスが表示されます。

2. コンソール コンピュータのエイリアスとして使用する名前または IP アドレスを入力します。

   IPv4 または IPv6 形式を使用して、IP アドレスを指定できます。

3. **[更新]** をクリックします。

4. **[続行]** または **[キャンセル]** をクリックします。

   [続行] をクリックすると、コンソール サービスと Ivanti Patch for Windows® Servers プログラムが自動的に再起動します。これは、コンソール エイリアス リストを更新するために必要です。**[キャンセル]** をクリックすると、コンソール エイリアス リストが更新されません。

重要！ エージェントは、再起動されたコンソールにチェックインするまで、新しいエイリアスを認識しません。コンソールからエージェントに発行されたチェックイン コマンドでは、コンソール認証資格情報は更新されません。

配布サーバの同期

最新のパッチ、スキャン エンジン、およびコンソールに含まれる XML 定義ファイルを使用して、配布サーバを更新する必要があります。エージェントが配布サーバを使用してこれらのファイルをダウンロードする場合、この作業が特に重要です。エージェントがチェックインを実行する**前**に、配布サーバが更新されたコンソール ファイルと同期する必要があります。

配布サーバを同期するには:

1. **[ヘルプ] > [ファイルの更新]** を選択し、コンソールに最新のファイルがすべて含まれていることを確認します。
2. **[ツール] > [オプション] > [配布サーバ]** の順に選択します。
3. 上部ウィンドウの **[スケジュールされた同期の追加]** ボックスで、同期するコンポーネントを選択します。
4. 上部ウィンドウで、コンソールと同期する配布サーバを選択します。
5. **[スケジュールされた同期の追加]** をクリックします。
6. 同期を実行するタイミングを指定し、**[保存]** をクリックします。
7. **[自動同期のスケジュール]** ウィンドウで、スケジュールされた同期エントリを選択します。
8. **[今すぐ実行]** をクリックします。

配布サーバとの同期を完了する前にエージェントがチェックインしない場合でも、問題はありません。次回、スケジュールされたタスクが実行されるとき、またはエージェントがバイナリを更新するときに、エージェントが更新されます。

予測パッチ機能の有効化を検討

この機能は v9.2で使用できるため、v9.1からアップグレードしている場合の新機能です。Ivanti Patch for Windows® Serversは、近い将来に配布される可能性が高いパッチを自動的にダウンロードできます。配布サーバを使用する場合は、配布サーバと予測パッチを同期し、ダウンロードされたパッチのコピーを配布することができます。予測パッチ オプションは、**[ツール] > [オプション] > [ダウンロード]** タブで有効にします。配布サーバと同期するには、**[配布サーバ]** ダイアログで **[予測パッチを同期する]**オプションをオンにします。 詳細については、ヘルプ システムをご参照ください。

データ ロールアップ コンソール間のセキュリティの再確立

メモ: これは、v9.1からv9.3にアップグレードする場合にのみ適用されます。v9.2で確立されたセキュリティ関連付けは v9.3でも動作します。

複数のコンソールを使用し、データ ロールアップ構成が実装されている場合、セントラル コンソールと各リモート コンソール間のセキュリティ関連付けを再確立する必要があります。

重要!アップグレードプロセスを開始すると、セントラルコンソールとリモートコンソールの両方がアップグレードされ、2つのコンソール間のセキュリティアソシエーションが再確立されるまで、データのロールアップアクティビティは実行されません。このため、ごく僅かなデータ ロールアップ アクティビティが予想される際にコンソールを並行してアップグレードすることを強くお勧めします。

セントラル コンソール

1. セントラル コンソールをアップグレードします。
2. **[ツール オプション] > [データ ロールアップ]** を選択し、**[結果を承認してロールアップ送信者から結果をインポートする]** チェックボックスが有効になっていることを確認します。

リモート コンソール

1. 各リモート コンソールをアップグレードします。
2. **[ツール オプション] > [データ ロールアップ]** を選択します。
3. ロールアップ コンソールの IP アドレス/ホスト名およびポート番号を確認します。
4. **[登録]** をクリックします。

データ ロールアップの詳細については、オンライン ヘルプ システムの **[管理] > [複数コンソールの管理] > [データ ロールアップ構成]** をご参照ください。

仮想マシンのスキャン

メモ: これは、v9.1からv9.3にアップグレードする場合にのみ適用されます。

[ホストされた仮想マシン] タブまたは **[ワークステーション仮想マシン]** タブで、コンピュータ グループで仮想マシンが定義されている場合は、アップグレードを実行した後に、ホームページまたはコンピュータ グループからこれらのコンピュータのスキャンを開始する必要があります。Ivanti Patch for Windows® Servers でコンピュータ ID を再確立するには、この手順を実行する必要があります。スキャンを実行しない場合は、**[仮想サーバ]** および **[パス]** フィールドがコンピュータ ビューに表示されず、これらのコンピュータへの配布が失敗する可能性があります。

カスタム ユーザ設定の確認

次のカスタム ユーザ設定はアップグレード中に保持されません。

- [ツール] > [オプション] > [表示] タブ:
  - 最近の項目 (日数)
  - アーカイブ項目
  - 自分が作成した項目のみを表示する
  - メイン ニュースフィードに表示する
  - パッチ スキャン結果に情報項目を表示する
  - [表示] > [パッチ] にサービス パックを表示する
- [ツール] > [オプション] > [通知と警告] タブ:
  - 配布をスケジュールする前に警告する
  - 完了時に更新ファイルを閉じる
  - Protect Cloud 同期がこのコンソールで有効ではない場合に警告する
  - 7個以上のセキュリティ情報を開く前に警告する
- [ツール] > [オプション] > [パッチ] タブ:
  - グローバル スレッド プール

    これは v9.3の新機能であり、製品のすべての機能に適用されます。v9.2では、資産スキャン テンプレートでスレッド プールが定義されていましたが、アップグレード中に削除されます。新しい既定値は、古いスレッド プール オプションで指定した値とは異なる場合があります。
- [ツール] > [オプション] > [ロギング] タブ:
  - 診断パッチ スキャン
- 配布追跡:
  - エラーを表示する

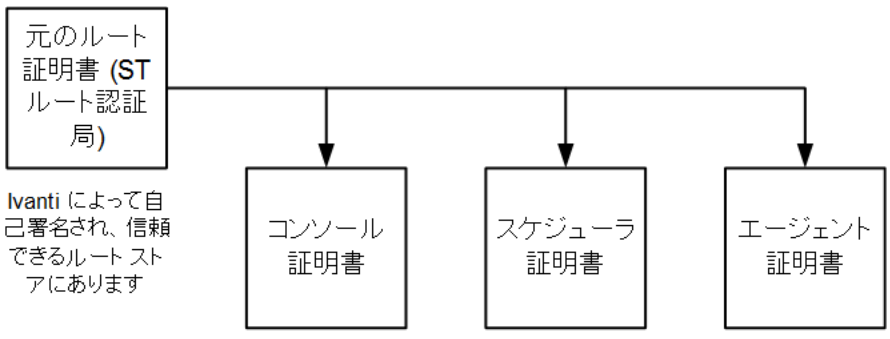
- 表示する日数
- エラーを表示する
- レポート ダイアログ
- 正常に終了したものを表示する

- レポート ダイアログ
  - IAVA ID で並べ替える
- [ESXi Hypervisor Bulletins]タブ：
  - 最新のみを表示
- イベント履歴
  - 結果を前の日数に制限する
- ITScripts 結果表示
  - 結果

v9.3が異なる証明書構造を使用することについての把握

証明書の場所と関係は、Shavlik Protect 9.1または9.2 を Ivanti Patch for Windows® Servers 9.3にアップグレードするときに変更されます。v9.1および v9.2では、スケジューラとエージェント証明書がコンソール証明書によって発行されていました。v9.3では、コンソール証明書、スケジューラ証明書、およびエージェント証明書はすべて自己署名ルート証明書によって発行されます。

Ivanti Patch for Windows® Servers 9.3にアップグレードした後



- コンソール証明書は、コンピュータ アカウントのパーソナル ストアの Windows ®サーバ コンソールのパッチにあります.
- スケジューラ証明書は /ProPatches/ スケジューラ ディレクトリにあります.
- エージェント コンピュータでは、コンソール証明書とエージェント証明書はコンピュータ アカウントの Shavlik Protect Agent ストアにあります。

アップグレード処理が完了した後、Ivanti Patch for Windows® Servers 9.3は証明書管理画面の背後で独自のプロセスを開始します。

- 既存のコンソール証明書は中間認証局ストアから削除されます。これは、メンテナンス作業に応じて、運用の最初の1、2日以内に発生します。
- 新しいスケジューラ証明書は、Ivanti Scheduler がインストールされるか、Ivanti Scheduler を使用したエージェントレス配布が実行されるたびに、ルート証明書から発行されます。古いスケジューラ証明書 (9.2コンソール証明書で最初に発行された証明書) は削除されます。
- 新しいエージェントがインストールされるか、既存のエージェントの証明書を再発行する必要があるときには、新しいエージェント証明書がルート証明書から発行されます。エージェントはローカルストアにエージェント証明書を保存し、エージェント コンピュータの信頼できるルートストアから個人ストアにコンソール証明書を移動します。古いエージェント証明書 (9.2コンソールで最初に発行された証明書) は削除されます。

  エージェント アップグレード処理には、エージェントのチェックインを待機し、新しい保留中のルート証明書を受信する処理があります。要素数によっては、この処理に数日または数週間かかる場合がありますが、すべてバックグラウンドで実行されます。ユーザ側で必要な作業は、イベント履歴ログを監視し、注意が必要な問題が発生しているかどうかの確認をすることです。

コンソールでエージェントを使用する場合

Ivanti Patch for Windows® Server コンソールにエージェントがインストールされている場合は、エージェントを手動で再インストールしてください。コンソール エージェントが新しいエージェント証明書で正常にアップグレードされることを確認するためにこれを実施してください。ターゲット コンピュータにインストールされているエージェントでは処理が不要です。

IVANTI PATCH FOR WINDOWS® SERVERS 9.3 の重要な変更と機能強化

次の各トピックの詳細については、オンライン ヘルプシステムをご参照ください。

https://help.ivanti.com/sh/help/ja_JP/PWS/93/PWS.htm

API 機能

API 機能は PowerShell の実践的な知識を有し、Ivanti Patch for Windows® Servers ユーザインターフェイスで提供されている以外のタスクを実行する上級者ユーザ向けです。API 機能を使用すると、次のことができます。

- 環境内の異なるシステムとの連携
- 依存関係を含む一連の複雑なイベントのスクリプト化
- 一括処理を実行するか、他のシステムのリスト入力を処理します
- 体系的にパッチ配布を段階的に実行するか、パッチのダウンロードを開始します

API 機能の使用方法の詳細については、*API クイック スタート ガイド*をご参照ください。

ナビゲーション ペインのフォルダ パス

別の新機能は、コンピュータ グループ、パッチ スキャン テンプレート、およびパッチ配布テンプレートの階層構造を作成する機能です。多数のグループまたはテンプレートを作成する場合は、論理フォルダに整理することを検討してください。このようにすると、グループとテンプレートをすばやく検索して管理できます。Y

ナビゲーション ペインでは必要な数のフォルダとサブフォルダを作成できます。たとえば、ロケーション別などの含まれるコンピュータのタイプに基づいてグループを整理できます。

作成すると、フォルダ間で項目をドラッグしてドロップできます。階層の任意のレベルを右クリックし、すべての項目または下位レベルで処理を実行できます。

段階的な配布

パッチ スキャンと配布処理には、4つの個別のスケジュール可能な点があります。これにより、プロセス全体をより効果的に制御できます。次のことができます。

- スキャンのみを実行する
- スキャンを実行し、パッチをインストールせずに特定の時間にターゲット コンピュータで不足しているパッチを段階的に計画します

- スキャンを実行し、ターゲット コンピュータで不足しているパッチを段階的に計画し、選択した時間にインストールします

スケジュールされたスナップショット メンテナンス

この新機能により、1回限りのタスクまたは繰り返しタスクをスケジュールし、サーバから古い仮想コンピュータ スナップショットを削除できます。以前は、古いスナップショットを削除する唯一の方法は、配布タスク中にリアルタイムで削除することでした。この機能を使用するには、**[ツール] > [オプション] > [スナップショット メンテナンス]** を選択し、タスクを追加します。

第三者 CA を使用する機能

独自の PKI インフラストラクチャから信頼できる認証局 (CA) を使用し、Ivanti Patch for Windows® Servers の置換ルート証明書を発行できます。これは必要ではありませんが、既定の自己署名ルート証明書を中レベルのセキュリティ リスクと見なすセキュリティ ツールを使用する場合は、置換証明書を生成するためにプロセスを使用できます。詳細については、オンライン ヘルプ システムで、**[管理] > [ユーティリティ] > [第三者 CA からの証明書の生成]** をご参照ください。

スケジュールされたリモート タスク マネージャ

スケジュールされたリモート タスク マネージャには複数の変更が行われました。

- コンピュータ ビューまたはスキャン ビューでコンピュータを右クリックするか、**[スケジュールされたタスクの表示]** を選択してアクセスできます。
- 電源タスクとパッチ配布タスクに関する情報は、スケジュールされたコンソール タスク マネージャに似た形式で表示されます。
- Ivanti Scheduler または Microsoft Task Scheduler を使用してリモート コンピュータでスケジュールされるタスクが表示されます。

新しいスキン

新しいオプションが **[表示オプション]** ダイアログで提供され、Ivanti Patch for Windows® Servers インターフェイスで使用するカラー テーマを指定できます。目に合った色を選択するだけではなく、特に低帯域幅 RDP 環境で十分なコントラストを提供するスキンを考慮することもできます。

新しい列フィルタ機能

グリッドの1つ以上の列ヘッダーにフィルタを適用できます。このためには、列ヘッダーにカーソルを置き、右上端のフィルタ アイコンをクリックします。例:

フィルタ メニューを使用して、表示される現在の列の値を選択します。

手動ダウンロード方法

新しい**ダウンロード方法**列は、パッチを自動的にダウンロードできるかどうか、または手動でダウンロードする必要があるかどうかを示します。この列の値が**自動**の場合、Ivanti Patch for Windows® Servers はパッチを自動的にダウンロードできます。値が **[ベンダから取得]** または他の値の場合は、パッチを手動でダウンロードし、パッチ ダウンロード ディレクトリに移動する必要があります。パッチがある場合は、標準の配布処理を使用して配布できます。自動配布が使用され、パッチで手動ダウンロードが必要な場合は、自動配布処理は動作しません。

パッチを自動的にダウンロードできない理由は多数ある場合があります。たとえば、プロプライエタリ ソフトウェア プログラムで作成されたパッチを使用したり、ベンダによって正式にサポートされなくなったプログラムのパッチを受信できます。

配布構成情報

[配布構成] ダイアログには、パッチを配布するときのディスク領域要件に関する情報が表示されます。

統合プログラム オプション

すべてのプログラム オプションは1つの場所に統合されています。オプションを表示するには、**[ツール] > [オプション]** を選択します。**[ツール] > [処理]** メニューが削除されました。

パッチ グループ フィルタ

パッチ ビューには新しいパッチ グループ フィルタがあります。**[選択したパッチ グループに現在含まれているパッチ (上) を表示する]** チェックボックスを使用すると、選択したパッチ グループに含まれるパッチがパッチ ビュー リストに表示されるかどうかを選択できます。

配布追跡の UI 変更

配布追跡は、現在実行中のパッチ配布タスクに関する詳細を提供するために再設計されました。配布追跡を使用して配布をキャンセルすることもできます。配布準備処理を完了する必要がありますが、実際の配布を開始できません。

ダウンロード パッケージのエクスポート

カンマ区切り値 (CSV) ファイルに選択したパッチのダウンロード リンクをエクスポートできます。これは特に、オフライン環境のコンソールで有用です。オンラインのコンピュータは CSV ファイルを使用し、パッチをダウンロードできます。その後に、パッチはオフラインのコンソールのパッチ ディレクトリにコピーできます。

メモ: ファイル ダウンローダ PowerShell スクリプトはファイル ダウンロード処理を支援するために提供されています。

新しい IAVA レポート

2つの新しい IAVA が使用できます。コンピュータ準拠 (IAVA) とコンピュータ非準拠 (IAVA) です。これらの2つのレポートには、報告書データを送信するときに米国政府によって求められる追加情報が含まれます。

グローバル スレッド プール

スレッド管理はテンプレート レベルからシステム プールに移動し、**[ツール] > [オプション] > [パッチ]** ダイアログで定義されます。既定では、CPU コアごとに8スレッドを使用しますが、適合するように値を調整できます。この1つの値は、パッチ スキャンまたは配布、資産スキャンまたは電源ステータス スキャン中に使用できるスレッドの合計数を指定します。

拡張検索機能

製品の検索機能は複数の領域に拡張されました。検索を実行できます。

- コンピュータ グループの **[ホストされた仮想マシン]** タブ。
- ナビゲーション ペインのコンピュータ グループを右クリックし、**[コンピュータ グループの検索]** を選択する。これにより、すべてのコンピュータ グループで特定のコンピュータとグループを検索できます。
- スキャン ビューとコンピュータ ビューの中央のペインにある新しい検索ボックスを使用する。