

Shavlik

—
アップグレード ガイド



shavlik

著作権

Copyright © 2009 - 2015 LANDESK Software, Inc. All rights reserved. この製品は、米国およびその他の国における著作権法および知的財産法ならびに国際条約によって保護されています。

LANDESK Software, Inc. の書面による許可なく、購入者の個人的な使用以外の目的のために、本書のいかなる部分も、あらゆる形式において、あるいはコピーおよび記録を含む電子的、機械的、またはその他の手段において、複製または再送信することが禁止されています。

商標

LANDESK および Shavlik は米国およびその他の管轄地域における LANDESK Software, Inc. の登録商標または商標です。本書に記載されているその他のすべてのマークおよび名称は、各会社の商標である場合があります。

本書に記載されているその他のすべての商標、取引名、または画像は各所有者に帰属します。

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
2009 年 11 月	NetChk Protect 7.2 文書改訂 B	システム要件セクションに Windows 7 情報を追加。
2010 年 4 月	NetChk Protect 7.5	スキャン ビュー、新しい電源管理機能、ソフトウェア資産スキャンの改良、および仮想マシン機能に関する情報を追加。
2010 年 5 月	NetChk Protect 7.5、文書改訂 A	ライセンス情報、一部の追加機能に関する説明を明確化。
2010 年 9 月	NetChk Protect 7.6	製品ブランドを更新、新しい 7.6 機能と改良に関する情報を追加。
2011 年 3 月	NetChk Protect 7.8	新しい 7.8 機能と改良に関する情報を追加。
2011 年 10 月	VMware vCenter Protect 8.0	製品ブランドを更新、8.0 アップグレード タスクに関する情報を追加。7.5 よりも前のバージョンに関する情報をすべて削除。
2011 年 12 月	VMware vCenter Protect 8.0、文書改訂 A	アップグレード処理を開始する前に、データベースの圧縮方法を説明する手順を追加。
2012 年 9 月	VMware vCenter Protect 8.0.1	製品名、バージョン、および表紙のグラフィックスを更新。
2013 年 5 月	Shavlik Protect 9.0	システム要件を更新。新しい v9.0 機能と改良に関する情報を追加。
2014 年 4 月	Shavlik Protect 9.1	システム要件を更新。新しい v9.1 機能と改良に関する情報を追加。
2015年9月	Shavlik Protect 9.2	システム要件を更新。新しい v9.2の機能と改良に関する情報を追加。

はじめに

このガイドの目的

Shavlik Protect 9.2を使用する前にここでは、VMware vCenter Protect 9.0または Shavlik Protect 9.1から Shavlik Protect 9.2にアップグレードする方法について説明します。

この文書では、アップグレード手順の説明の他に、Shavlik Protect 9.2にアップグレードする際に理解しておくべき様々な機能の違いを一覧で示します。また、大幅に変更されたユーザ インターフェイスの領域についても強調表示しています。

新しいシステム要件と前提条件

Shavlik Protect 9.2では、次の新しい要件と前提条件に注意してください。

- Windows 2000は、クライアント コンピュータでサポートされないオペレーティング システムになりました。
- Windows 10 (Pro および Enterprise エディション) はクライアント コンピュータでサポートされるようになりました。

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。システム要件の詳細な一覧については、『Shavlik Protect 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、VMware vCenter Protect 9.0または Shavlik Protect 9.1から Shavlik Protect 9.2にアップグレードする方法について説明します。アップグレードの際に、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、『Shavlik Protect Migration Tool 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、18 ページの「重要な変更と機能強化」セクションに目を通し、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（17ページを参照）。

アップグレードの実行

1. スキャン結果、パッチ配布結果、および脅威修正結果を保存するためのデータベースを圧縮します。

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。
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、Shavlik Protect 9.2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。

<http://www.shavlik.com/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。

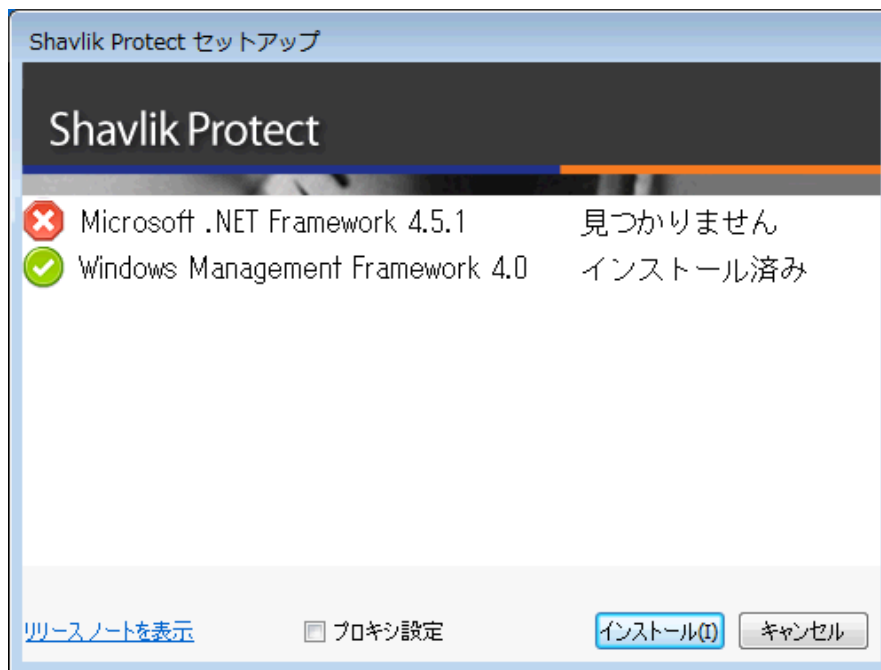
- **ShavlikProtect.exe** ファイルをダブルクリックします。
- コマンド プロンプトにファイル名を入力します。これで、1つ以上のコマンドライン オプションを使用できます。きわめて大規模なデータベースをアップグレードする場合には、この方法を検討してください。DBCCommandTimeout オプションは、インストール中に SQL コマンド タイムアウト値を指定するために使用されます。既定値は1 GB につき15分です。最低タイムアウト値は、1 GB につき15分または1800秒（30分）の大きい方の値です。4 GB のデータベースの場合、タイムアウト値を3600秒（60分）に上げる必要があります。例:

```
ShavlikProtect /wi:"DBCCommandTimeout =3600"
```

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。

- 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。



- [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。

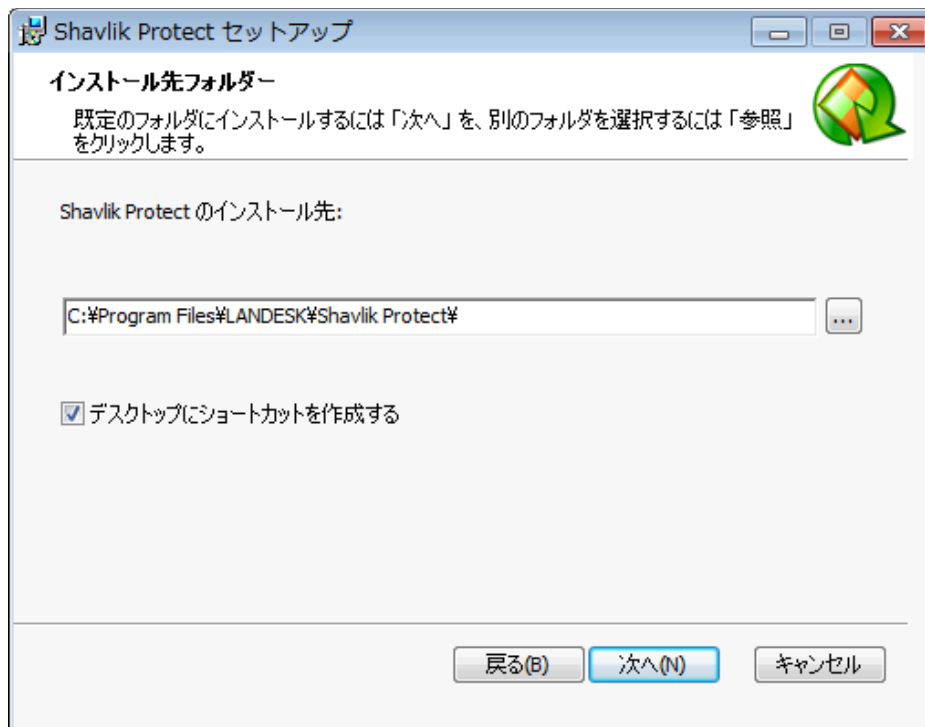
[ようこそ] ダイアログが表示されます。

- [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。

- [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。



- 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。

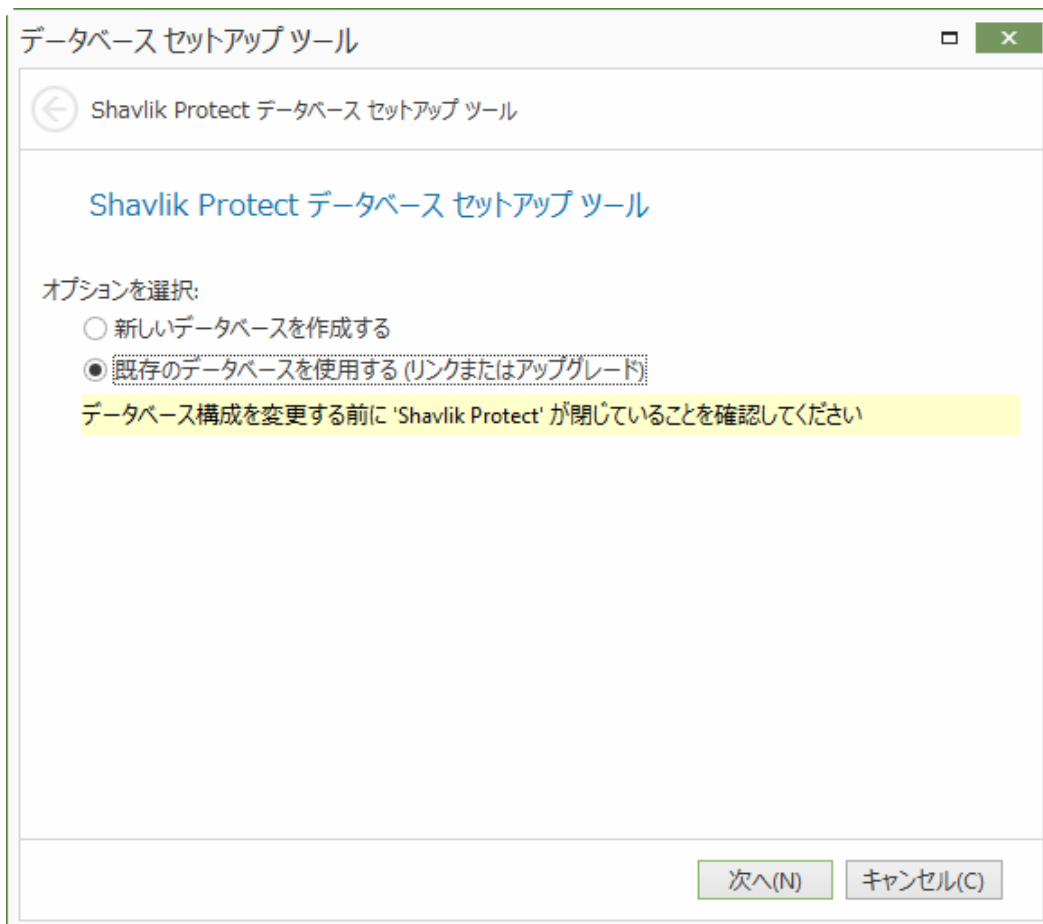
[製品改善プログラム] ダイアログが表示されます。説明をお読みにになり、プログラムに参加することに同意するかどうかを決定します。このプログラムでは、Shavlik が、今後の製品バージョンを改善する目的で、製品の使用状況情報を収集できます。

- [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。

- 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。

- 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。
次のようなダイアログが表示されます。

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。Shavlik Protect 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、『Shavlik Protect 管理ガイド』の「認証資格情報の指定」をご参照ください。)すべての Shavlik Protect ユーザは、リモート SQL Server データベースを操作する必要がある処理を実行するときに、指定された認証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 サービスで別の認証資格情報を使用する:**
 - 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 サービスで別の認証資格情報を使用する] 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、『Shavlik Protect 9.2 インストール ガイド』の「SQL Server のインストール後の注記」

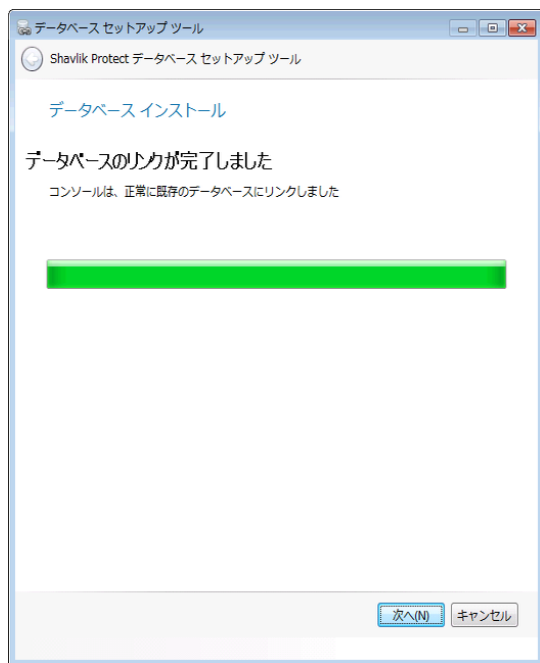
をご参照ください。この手順は、Shavlik Protect のアップグレード処理が完了した後、プログラムを起動する前に実行します。

- **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。Shavlik Protect 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。リンク処理が完了すると、次のダイアログが表示されます。



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. **[Shavlik Protect セットアップ ウィザードの完了]** ダイアログで、**[Shavlik Protect 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、Shavlik Protect 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

スケジューラ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ラ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。Shavlik Protect が起動するたびにこのチェックが実行され、スケジューラされたタスクが継続的に実行されることを保証します。

スケジューラ されたタスク の確認

スケジューラされたタスクは、2つの別の領域で監視および管理されます。両方のスケジューラ 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。

- **スケジューラ 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、スケジューラされたレポートなどの現在コンソールでスケジューラされているタスクを表示できます。
- **スケジューラ 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ラ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、Shavlik Protect 9.2 の新機能を表示および使用するには、ライセンスを手動で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、ヘルプ システムの **[インストールと設定] > [製品の使用開始] > [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

ここでは考慮する問題が 3 つあります。

- **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。アップグレード処理では、既存のパッチ グループが自動的に新しい規則に更新されますが、グループを再確認し、変更を検証してください。Shavlik は多数の古いパッチのサポートを終了したため、アップグレード後はパッチ グループが小さくなる可能性があります。

- **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 パッチ スキャン テンプレートの **パッチ フィルタ設定** セクションでパッチ グループを参照し、**[選択した項目のスキャン]** が有効な場合、スキャン テンプレート フィルタによって定義された条件を満たさないパッチはすべてグループから削除されます。理由:Protect 9.0 および 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配布することを意図していないパッチ タイプがパッチ グループに含まれる可能性があるという事実を考慮していません。Protect 9.2 では、パッチ グループがベースラインとして使用されるときに、スキャン テンプレート フィルタが適用されず、パッチ グループの不正確性が生じる可能性があります。アップグレード処理でこの状況が検出される場合は、パッチ グループが自動的に修正され、スキャン テンプレートとパッチ グループ間の想定された動作が保持されます。

例:

9.1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)。

9.2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

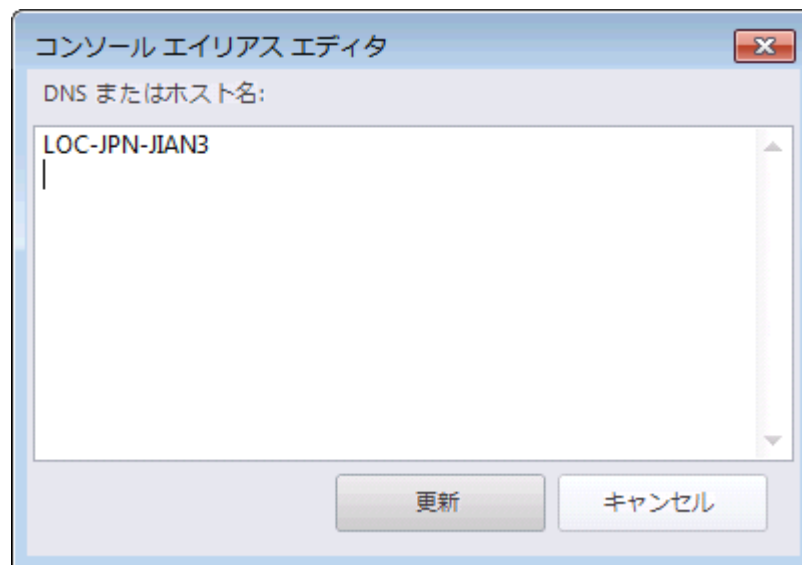
次の条件の1つ以上が該当する場合には、このタスクが必要です。

- コンソール コンピュータの新しいドメインへの割り当て
- コンソールの新しい共通名または IP アドレスへの指定
- エージェントの手動でインストール。 エージェントによる IP アドレスを使用したコンソールとの通信

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 Shavlik Protect 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。例：

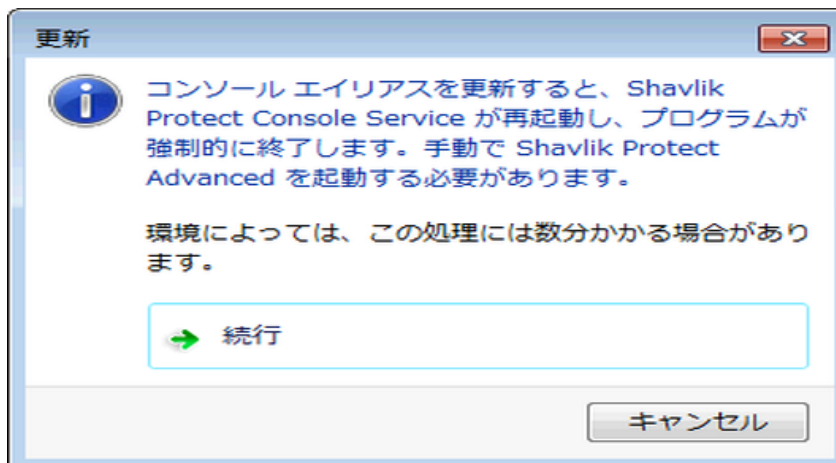


2. コンソール コンピュータのエイリアスとして使用する名前または IP アドレスを入力します。

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。

次のダイアログが表示されます。



コンソール エイリアスを更新するには、コンソール サービスを再起動する必要があります。Shavlik Protect を閉じてから手動で再起動する必要があります。

重要! エージェントは、再起動し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。チェックインは、エージェントによって手動で開始するか、エージェント クライアント プログラムまたはスケジュールされたチェックイン経由で手動で開始する必要があります。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] > [処理] > [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時、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

この新しい機能により、Shavlik Protect では、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] > [処理] > [ダウンロード] タブで有効にします。[配布サーバ] ダイアログで [予測パッチを同期する] オプションを有効にすると、配布サーバと同期されます。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を再確立する

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!アップグレード処理を開始すると、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関連付けが再確立されるまで、データ ロールアップ アクティビティが実行されません。このため、データ ロールアップ アクティビティがほとんど発生しないと想定されるタイミングで、コンソールを順次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. [ツール処理] > [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] > [処理] > [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、ヘルプ システムの [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

[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。Protect 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] > [ロギング] タブ:
 - 診断パッチ スキャン
- 配布追跡:
 - 更新速度
 - 表示する日数
 - エラーを表示する
 - 実行中を表示する
 - 正常終了した配布を表示する
- レポート ダイアログ
 - IAVA ID 順に表示
- ESXi Hypervisor セキュリティ情報タブ:
 - 最新のみ表示する
- イベント履歴
 - 過去の結果を表示(日数)
- ITScript 結果ビュー
 - 次の日付以降の結果

Protect 9.2 が SHA-2 ルート証明書を使用していることを確認

Shavlik は Protect 9.2 で SHA-2 ルート証明書およびコンソール証明書を使用しています。これには2つの主な理由があります。2048ビットの SHA-2 証明書は1024ビットの SHA-1 よりも安全です。また、SHA-1 ルート証明書は廃止予定であり、2017年1月1日以降の Windows では認められなくなります。

アップグレード処理を完了した後は、Shavlik Protect 9.2 で独自の処理がバックグラウンドで開始し、新しい SHA-2 ルート証明書と新しい SHA-2 コンソール証明書を発行します。エージェントを使用していない場合は、この処理は表示されず、無視することができます。エージェントを使用している場合は、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。

SHAVLIK PROTECT 9.2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、ヘルプシステムをご参照ください。

<http://help.shavlik.com/Protect/onlinehelp/92/ENU/PRT.htm>

パッチ配布

パッチをパッケージ化し、コンピュータに配布するためのエンジンが完全に再作成されました。パフォーマンスと信頼性が改善されました。

パッチ コンテンツ

Shavlik Protect が使用するパッチ評価と配布データが再パッケージ化され、さまざまな点において改善されました。

パッチ スキャン テンプレート フィルタリング

より多くのメタデータがパッチ コンテンツに追加されました。また、[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。

パッチ ビュー/パッチ グループ

パッチ ビューが完全に再設計され、更新されました。新しいコンテンツ形式を活用し、より簡潔な方法でパッチ情報を表示できます。また、パッチ ビューでパッチ グループを作成し、管理できます。これにより、パッチを調査し、より統合された方法でパッチ グループを作成できます。

スケジュールされたタスク

コンソールのスケジュールされたタスクは Microsoft タスク スケジューラを使用します。[管理] > [スケジュールされたコンソール タスク] メニューから開く新しいダイアログでは、これらのタスクを表示および管理できます。

レポート

新しい製品別サポート終了日レポートを使用できます。また、[ツール] > [レポートのスケジュール] メニューから開く新しい [レポートのスケジュール] ダイアログでは、将来の特定の日にレポートを自動的に生成できます。レポートは 1 回のみ、または繰り返して生成することができます。

予測パッチ

この新しいオプションにより、Shavlik Protect では、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。予想される配布のパッチを事前にダウンロードすることで、配布処理が高速化します。

Patch Tuesday + X (日) スケジュール

コンソール スキャンをスケジュールするときには、定期的なイベントに合わせて、反復スキャンを遅延する日数を指定できます。たとえば、新しい [遅れ (日) を追加] オプションを使用して、Patch Tuesday の翌日に月次パッチ スキャンを実行するスケジュールを設定できます。

サービス終了通知

使用しているバージョンの Shavlik Protect がサービス終了日に近づいている場合、Shavlik Protect を起動したときに通知が表示されます。

Protect Cloud 統合

パッチ スキャンと配布結果が定期的に Protect Cloud に送信されます。Shavlik Empower ユーザの場合は、パッチ データが定期的に Empower によって Protect Cloud から取得されます。データを表示するには、ブラウザベースの Shavlik Empower ユーザ インターフェイスを使用します。

ユーザ インターフェイスの変更

次のユーザ インターフェイス項目が変更されました。

- パッチ ビューが完全に再設計されました。
- パッチ ビューでパッチ グループを作成し、管理できます。
- コンピュータ ビュー：
 - 上部ウィンドウには次の3つの新しい列があります。仮想サーバ、VM 名、パッチ
 - 中央ウィンドウから **【仮想資産】** タブが削除されました。
 - 下部ウィンドウの **【見つからないコンピュータ】** および **【インストールされているコンピュータ】** タブが1つの新しいタブ **【影響を受けるコンピュータ】** に統合されました。
- パッチ配布テンプレート：
 - Office インストール ポイントと元のメディア サポートが削除されました。
 - **【アンインストールのファイルをバックアップする】** および **【サイレント モード】** オプションが削除されました。これらは常に有効です。
 - **【配布サーバ】** タブが再設計され、ダウンロード ソースが使用される順序を識別しやすくなりました。
- パッチ スキャン テンプレート：
 - **【フィルタリング】** タブが完全に再設計されました。
 - ユーザの重大度が削除されました。
 - **【ソフトウェア配布】** タブには、置き換えられていない製品のみが表示されます。
- エージェント ポリシーでは、すべてのタスクを繰り返しスケジュールなしで作成できるようになりました。これにより、エージェント ユーザ インターフェイスまたはコンソールのリモート タスク開始によってのみ実行されるタスクを定義できます。
- コンピュータ グループでは、**【存在のテスト】** および **【認証資格情報のテスト】** オプションが統合され、電源ステータス スキャンを実行したときに起動します。

- 仮想資産概要はコンピュータ ビューに表示されなくなりました。すべての仮想資産情報を表示するには、仮想インベントリ機能を使用します。
- 仮想マシン ハードウェア詳細、仮想マシン メモリ利用率、仮想マシン ディスク利用率レポートが削除されました。
- スキャン ビューでは、スキャン概要サブウィンドウを折りたたむことができなくなりました。
- スケジュールされたタスクが次の2つの個別のダイアログに分離されました。
[管理] > [スケジュールされたリモート タスク] と [管理] > [スケジュールされたコンソール タスク]
- [ツール] > [オプション]:
 - **表示:**新しいチェックボックス [ビューでサービスパックを表示] > [パッチ] が追加されました。
 - **通知と警告:**新しいチェックボックス [7個以上のセキュリティ情報を開く前に警告する] が追加され、[既定の認証資格情報が現在のユーザと一致しないときに、処理をスケジュールする前に警告する] チェックボックスが削除されました。
 - **パッチの言語:**このタブは削除されました。管理されたコンピュータで使用されるオペレーティング システム言語が自動的に検出され、パッチ ファイルに必要な言語バージョンだけがダウンロードされます。
 - **スキャン:**新しいチェックボックス [コンピュータ グループの除外を常に適用する] が追加されました。
 - **配布:**[配布追跡アドレス] オプションが削除されました。このアドレスは、[コンソール エイリアス エディタ] で定義されます。
 - **ロギング:**新しいチェックボックス [診断パッチ スキャン] が追加されました。