

Shavlik Protect

Guide de mise à niveau



shavlik

Copyright

Copyright © 2009 – 2015 LANDESK Software, Inc. Tous droits réservés. Ce produit est protégé par copyright et par les lois sur la propriété intellectuelle des États-Unis et d'autres pays, ainsi que par des clauses de traités internationaux.

Il est interdit de reproduire ou de retransmettre un élément quelconque de ce document, sous quelque forme et par quelque moyen que ce soit, électronique, mécanique ou autre, y compris par photocopie ou enregistrement, dans un but autre que l'utilisation personnelle du produit par la personne qui l'a acheté, sans l'autorisation écrite de LANDESK Software, Inc.

Marques

LANDESK et Shavlik sont des marques déposées de LANDESK Software, Inc. aux États-Unis et dans d'autres juridictions. Tous les autres noms et marques de produit mentionnés ici sont des marques commerciales de leurs propriétaires respectifs.

Tous les autres noms commerciaux, marques ou images utilisés dans ce document appartiennent à leur propriétaire respectif.

Informations sur le document et historique d'impression

Numéro de document : N/A

Date	Version	Description
Mars 2011	NetChk Protect 7.8	Ajout d'informations sur les nouveautés et améliorations de la version 7.8.
Octobre 2011	VMware vCenter Protect 8.0	Mise à jour des marques de produit, ajout d'infos sur les tâches de mise à niveau vers la version 8.0. Suppression de toutes les infos sur les versions antérieures à 7.5.
Décembre 2011	VMware vCenter Protect 8.0, Rév. A du document	Ajout d'une étape expliquant comment compresser la base de données avant de lancer le processus de mise à niveau.
Septembre 2012	VMware vCenter Protect 8.0.1	Mise à jour du nom de produit et de la version, mise à jour des images de couverture.
Mai 2013	Shavlik Protect 9.0	Mise à jour de la configuration système requise. Ajout d'informations sur les nouveautés et améliorations de la version 9.0.
Avril 2014	Shavlik Protect 9.1	Mise à jour de la configuration système requise. Ajout d'informations sur les nouveautés et améliorations de la version 9.1.
Septembre 2015	Shavlik Protect 9.2	Mise à jour de la configuration système requise. Ajout d'informations sur les nouveautés et améliorations de la version 9.2.

BIENVENUE

Objectif de ce guide

Bienvenue dans Shavlik Protect 9.2. Ce document explique comment mettre à niveau Shavlik Protect 9.0 ou Shavlik Protect 9.1 vers Shavlik Protect 9.2.

Outre la description de la procédure de mise à niveau, ce document répertorie un certain nombre de différences de fonctionnement que vous devez connaître lorsque vous mettez votre installation à niveau vers Shavlik Protect 9.2. Il met également en évidence les éléments de l'interface utilisateur qui ont beaucoup changé.

Nouvelle configuration système requise et nouveaux prérequis

Merci de noter les nouveaux prérequis et la configuration système requise pour Shavlik Protect 9.2, ci-dessous.

- Le système d'exploitation Windows 2000 n'est plus pris en charge sur les machines client.
- Windows 10 (versions Pro ou Enterprise Edition) est désormais pris en charge sur les machines client.

Tous les logiciels prérequis manquants sont automatiquement installés lors du processus de mise à niveau. Pour consulter la liste complète de la configuration système requise, reportez-vous au *Guide d'installation de Shavlik Protect*.

Configuration de compte d'utilisateur requise pour la mise à niveau

Pour que vous puissiez réaliser la mise à niveau, votre compte d'utilisateur doit respecter les exigences suivantes :

- L'utilisateur qui réalise la mise à niveau de la base de données doit être membre du rôle db_owner.
- Si vous utilisez plusieurs consoles partageant la même base de données et que vous liez une console supplémentaire à une base de données déjà mise à niveau, le compte d'utilisateur que vous employez doit être membre des rôles de base de données suivants : db_datareader, db_datawriter, STExec et STCatalogupdate. De plus, le compte de service utilisé pour les opérations en arrière-plan doit être membre du rôle db_owner. Si votre compte est membre des rôles db_securityadmin et db_accessAdmin, l'outil de mise à niveau des bases de données tente automatiquement de mapper et de configurer à votre place les rôles requis.

PROCEDURE DE MISE A NIVEAU

Introduction

Cette section explique comment mettre à niveau Shavlik Protect 9.0 ou Shavlik Protect 9.1 vers Shavlik Protect 9.2. Si vous profitez de l'opération pour déplacer la console vers une autre machine et que vous souhaitez effectuer la migration avec l'outil de migration, consultez le manuel *Guide de l'utilisateur de l'outil de migration Shavlik Protect* avant d'effectuer la mise à niveau.

Avant toute mise à niveau, lisez attentivement la section « *Changements et améliorations importants* », page 19, afin de prendre connaissance de l'impact de cette mise à niveau sur votre système. Vous pouvez également prendre note de tous vos paramètres utilisateur personnalisés, car la mise à niveau ne les conserve pas (voir page 17).

Réalisation de la mise à niveau

1. Comprimez la base de données servant à stocker les résultats d'analyse, les résultats de déploiement de correctifs et les résultats de correction des menaces.

Vous pouvez réaliser l'opération dans SQL Server Management Studio : cliquez avec le bouton droit sur la base de données ShavlikScans et sélectionnez **Tâches > Compacter > Base de données**.

2. Créez une sauvegarde de votre base de données actuelle avec SQL Server Management Studio.
3. Fermez tous les programmes en cours d'exécution sur la machine de console, y compris Shavlik Protect.
4. Téléchargez le fichier exécutable Shavlik Protect 9.2 sur votre machine de console à l'aide du lien suivant :

<http://www.shavlik.com/downloads/>

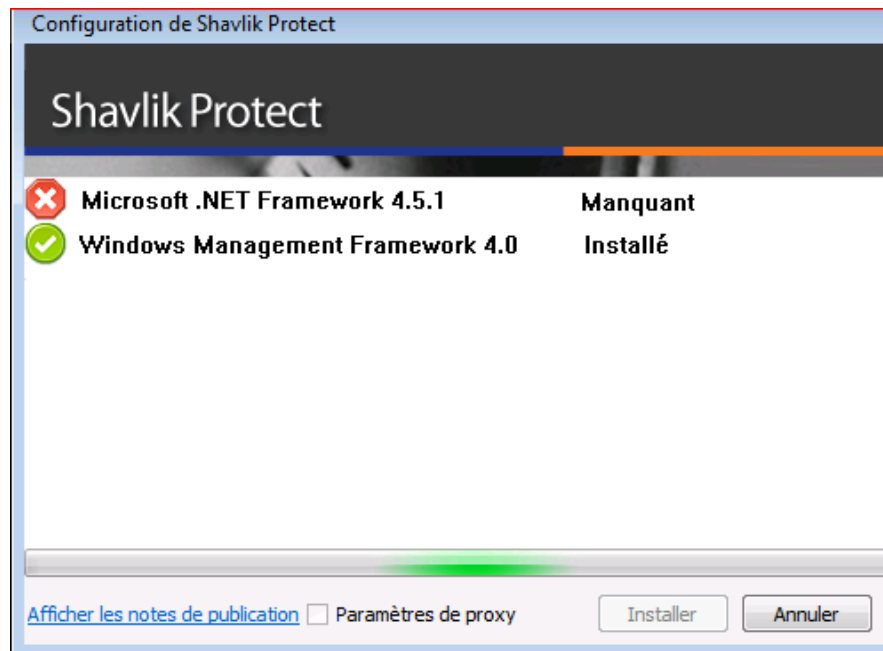
5. Lancez le processus d'installation à l'aide de l'une des méthodes suivantes :
 - Double-cliquez sur le fichier **ShavlikProtect.exe**.
 - Entrez le nom du fichier dans une invite de commandes. Cela vous permet d'utiliser une ou plusieurs options de ligne de commande. Choisissez de préférence cette méthode si vous mettez à niveau une base de données très volumineuse. L'option `DBCOMMANDTIMEOUT` permet de spécifier la valeur de temporisation des commandes SQL pendant l'installation. La valeur par défaut est de 15 minutes par Go. La valeur de temporisation minimale est soit 15 minutes par Go, soit 1 800 secondes (30 minutes). La valeur la plus élevée s'applique. Pour une base de données de 4 Go, fixez la valeur de temporisation à 3 600 secondes (60 minutes). Par exemple :

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

Remarque : Si une invite s'affiche, signalant qu'un redémarrage est nécessaire, cliquez sur **OK**. Le processus d'installation reprend automatiquement après le redémarrage.

- Répondez à la boîte de dialogue qui vous demande si vous souhaitez continuer la mise à niveau.

Si vous cliquez sur Oui alors que votre machine de console ne respecte pas certains prérequis, une boîte de dialogue semblable à la suivante s'affiche. Si tous les prérequis sont respectés, sautez l'étape suivante et passez directement à la boîte de dialogue **Bienvenue**.

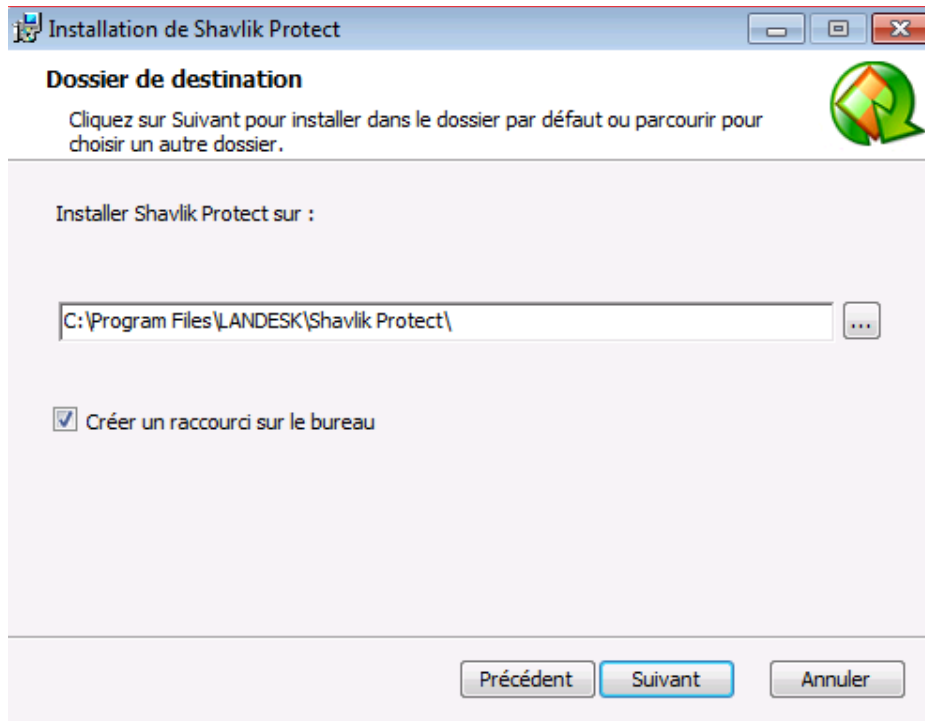


- Cliquez sur **Installer** pour installer tous les prérequis manquants.

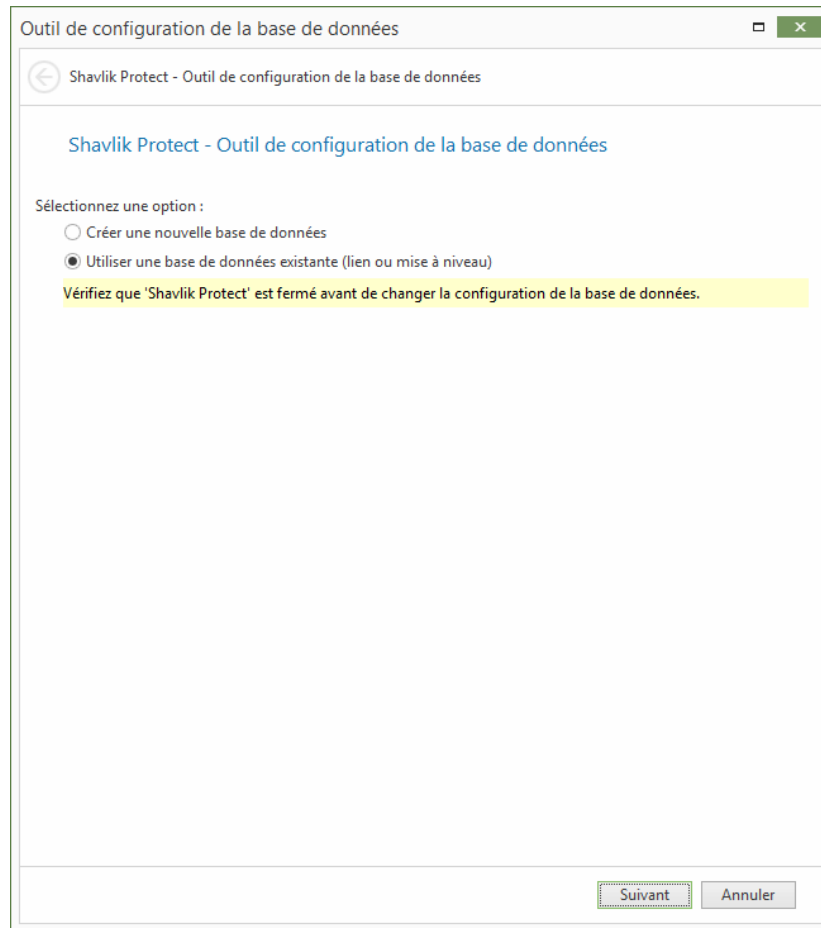
L'assistant de configuration peut être contraint de redémarrer l'ordinateur à ce stade du processus d'installation. Si un redémarrage est requis, la boîte de dialogue Configuration réapparaît au redémarrage de la machine. Cliquez simplement une nouvelle fois sur **Installer** pour poursuivre la mise à niveau.

La boîte de dialogue **Bienvenue** s'affiche.

- Lisez attentivement le contenu de la boîte de dialogue **Bienvenue** et cliquez sur **Suivant**.
Le contrat de licence est affiché. Vous devez accepter les termes du contrat de licence pour installer le programme.
- Cochez la case **J'accepte les termes de ce contrat de licence**, puis cliquez sur **Suivant**.
La boîte de dialogue **Dossier de destination** s'affiche.



10. Pour changer l'emplacement par défaut du programme, cliquez sur le bouton Parcourir et choisissez un nouveau dossier. Vous pouvez aussi, à cette étape, choisir d'installer une icône de raccourci sur le bureau. Lorsque vous avez terminé, cliquez sur **Suivant**.
La boîte de dialogue **Programme d'amélioration des produits** s'affiche. Consultez la description et décidez si vous acceptez de participer au programme. Ce programme permet à Shavlik de collecter des informations d'utilisation des produits, qui aident à améliorer les futures versions du produit.
11. Cliquez sur **Suivant**.
La boîte de dialogue **Prêt à installer** s'affiche.
12. Pour commencer l'installation, cliquez sur **Installer**.
Vers la fin du processus d'installation, la boîte de dialogue **Outil de configuration de la base de données** s'affiche.



Important ! À l'étape suivante, ne sélectionnez PAS **Créer une nouvelle base de données**. Si vous le faites, le programme crée une nouvelle base au lieu d'utiliser vos données existantes.

13. Vérifiez que l'option **Utiliser une base de données existante** est bien sélectionnée, puis cliquez sur **Suivant**.

Une boîte de dialogue semblable à la suivante s'affiche :

Outil de configuration de la base de données

Shavlik Protect - Outil de configuration de la base de données

Configuration de la base de données SQL

Choisir un serveur de base de données et une instance

Nom du serveur : (local)\SQLEXPRESS

Nom de base de données : Protect

Choisir comment les utilisateurs interactifs se connectent à la base de données

Mode d'authentification : Authentification Windows intégrée

Nom d'utilisateur :

Mot de passe :

Tester la connexion de base de données

Choisir comment les services se connectent à la base de données

L'utilisation de l'authentification Windows intégrée avec des bases de données distantes nécessite Kerberos.

Utiliser des références d'authentification alternatives pour les services de console

Mode d'authentification : Authentification Windows intégrée

Nom d'utilisateur :

Mot de passe :

Suivant Annuler

14. Utilisez les champs disponibles pour définir la façon dont les utilisateurs et les services doivent accéder à la base de données SQL Server.

Choisir un serveur de base de données et une instance

- **Nom du serveur** : Vous pouvez spécifier une machine, ou bien spécifier à la fois la machine et l'instance SQL Server exécutée sur cette machine.
- **Nom de base de données** : Spécifiez le nom de la base de données que vous souhaitez utiliser. Le nom de base de données par défaut est **Protect**.

Choisir comment les utilisateurs interactifs se connectent à la base de données

Spécifiez les références d'authentification que le programme doit utiliser lorsqu'un utilisateur exécute une action qui nécessite un accès à la base de données.

- **Authentification Windows intégrée** : Option recommandée, activée par défaut. Shavlik Protect utilise les références d'authentification de l'utilisateur actuellement connecté pour la connexion à la base de données SQL Server. Les champs **Nom d'utilisateur** et **Mot de passe** sont grisés.
- **Utilisateur Windows spécifique** : Sélectionnez cette option uniquement si la base de données SQL Server se trouve sur une machine distante. Cette option n'a aucun effet si la base de données se trouve sur la machine locale (de console). (Pour en savoir plus sur les références d'authentification de la machine locale, reportez-vous à « *Entrée de références d'authentification* » dans le **Guide d'administration de Shavlik Protect**.) Tous les utilisateurs de Shavlik Protect emploient les références d'authentification fournies pour réaliser des actions qui nécessitent une interaction avec la base de données SQL Server distante.
- **Authentification SQL** : Sélectionnez cette option pour entrer une combinaison nom d'utilisateur plus mot de passe spécifique pour SQL Server pour la connexion au serveur SQL Server spécifié.

Attention ! Si vous entrez des références d'authentification SQL alors que le cryptage SSL des connexions SQL n'est pas activé, ces références d'authentification sont transmises au réseau sous forme de texte en clair.

- **Tester la connexion de base de données** : Pour vérifier que le programme peut utiliser les références d'authentification d'utilisateur interactif spécifiées pour la connexion à la base de données, cliquez sur ce bouton.

Choisir comment les services se connectent à la base de données

Spécifiez les références d'authentification que les services d'arrière-plan doivent utiliser pour établir la connexion à la base de données. Il s'agit des références d'authentification utilisées par l'outil d'importation des résultats, diverses opérations d'agent et autres services pour la connexion au serveur SQL Server, ainsi que pour fournir des informations d'état.

- **Utiliser des références d'authentification alternatives pour les services de console** :
 - Si la base de données SQL Server est installée sur la machine locale, vous ignorez généralement cette option : vous ne cochez pas cette case. Dans ce cas, le programme utilise les mêmes références d'authentification et le même mode d'authentification que ceux spécifiés ci-dessus pour les utilisateurs interactifs.
 - En général, vous cochez cette case uniquement si la base de données SQL Server se trouve sur une machine distante. Lorsque la base de données réside sur une machine distante, vous avez besoin d'un compte capable de s'authentifier auprès de la base de données sur le serveur de base de données distant.
- **Méthode d'authentification** : Disponible uniquement si vous activez l'option **Utiliser des références d'authentification alternatives pour les services de console**.
 - **Authentification Windows intégrée** : Sélectionnez cette option pour utiliser le compte de la machine pour la connexion au serveur SQL Server distant. Le protocole d'authentification réseau Kerberos doit être disponible pour que le

programme puisse transmettre les références d'authentification en toute sécurité. Les champs Nom d'utilisateur et Mot de passe sont grisés.

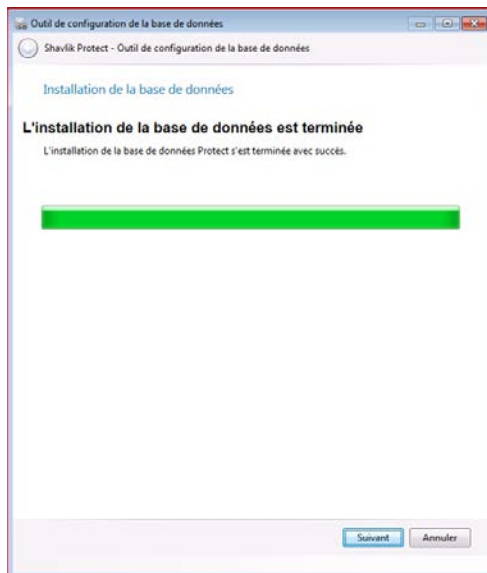
Remarque : Si vous choisissez **Authentification Windows intégrée**, le programme d'installation tente de créer un nom de connexion SQL Server pour le compte de machine. Si le processus de création du compte échoue, reportez-vous à « *Remarques sur SQL Server : après l'installation* » dans le manuel *Guide d'installation de Shavlik Protect* pour obtenir des instructions concernant la configuration manuelle d'un serveur SQL Server distant afin qu'il accepte les références d'authentification du compte de machine. Effectuez cette opération après avoir réalisé le processus de mise à niveau de Shavlik Protect mais avant de démarrer le programme.

- **Utilisateur Windows spécifique :** Sélectionnez cette option pour fournir une combinaison nom d'utilisateur plus mot de passe unique. Shavlik Protect comporte des services d'arrière-plan qui utilisent ces références d'authentification pour se connecter à la base de données SQL Server. C'est une bonne solution de rechange si, pour une raison quelconque, vous avez du mal à mettre en place l'authentification Windows intégrée.
- **Authentification SQL :** Sélectionnez cette option pour entrer une combinaison spécifique nom d'utilisateur plus mot de passe, que les services utiliseront pour la connexion au serveur SQL Server.

15. Après avoir fourni toutes les informations requises, cliquez sur **Suivant**.

Remarque : Si le programme d'installation détecte un problème concernant l'une des références d'authentification spécifiées, un message d'erreur s'affiche. Cela signifie généralement que le compte d'utilisateur spécifié n'existe pas. Corrigez votre saisie et réessayez.

La console est liée à votre base de données existante. Une fois le processus de liaison terminé, la boîte de dialogue suivante s'affiche :



16. Cliquez sur **Suivant**.

17. Dans la boîte de dialogue **Installation terminée**, cliquez sur **Terminer**.

18. Dans la boîte de dialogue **Assistant de configuration de Shavlik Protect terminé**, cochez la case **Lancer Shavlik Protect** et cliquez sur **Terminer**.

TACHES DE MISE A NIVEAU REALISEES SUR LA CONSOLE

Pour achever la mise à niveau, vous devez réaliser les opérations suivantes sur la console Shavlik Protect.

Affectation de références d'authentification du Planificateur

Il est désormais obligatoire d'indiquer la référence d'authentification du Planificateur, qui doit correspondre à votre compte d'utilisateur actuel, pour exécuter les tâches planifiées de la console. S'il n'existe aucune tâche planifiée sur la console et que la référence d'authentification de Planificateur n'a pas été définie, une invite s'affiche au démarrage, vous demandant de créer cette référence d'authentification. Cela se produit à chaque démarrage de Shavlik Protect pour garantir que les tâches planifiées continuent à s'exécuter.

Passage en revue des tâches planifiées

Vous surveillez et gérez désormais les tâches planifiées depuis deux zones distinctes. Il est conseillé de passer en revue les deux gestionnaires de tâches planifiées pour vous assurer que vos tâches existantes ont été correctement récupérées de la version précédente.

- Le **gestionnaire de tâches de console planifiées** offre un point central où sont affichées toutes les tâches actuellement planifiées sur la console. Il peut s'agir d'analyses des correctifs, d'analyses des biens, de déploiements de correctifs sur la machine de console, d'exécutions de scripts ou de rapports planifiés.
- Le **gestionnaire de tâches planifiées distant** fournit un emplacement unique où sont affichées toutes les tâches d'alimentation et tâches de déploiement de correctifs actuellement planifiées sur vos machines distantes cible.

Actualisation de votre licence (Consoles hors ligne uniquement)

Si votre console est hors ligne (sans connexion Internet), vous devez actualiser manuellement votre licence pour voir et utiliser les nouveautés de Shavlik Protect 9.2. Pour en savoir plus sur l'activation d'une console déconnectée, reportez-vous à la rubrique d'aide **Installation et configuration > Mise en route > Activation du programme**.

Si la console est en ligne, la licence est automatiquement actualisée au cours du processus de mise à niveau.

Passage en revue des modèles d'analyse des correctifs et groupes de correctifs

Vous devez tenir compte de trois facteurs pour ces opérations.

- **Modèles d'analyse des correctifs** : L'onglet **Filtrage** de la boîte de dialogue **Modèle d'analyse des correctifs** a été mis à jour pour permettre une plus grande précision d'analyse. Bien que le processus de mise à niveau convertisse automatiquement vos modèles d'analyse des correctifs vers le nouveau style, pensez à passer vos modèles en revue pour voir les changements apportés.
- **Groupes de correctifs** : Les groupes de correctifs ne sont plus définis dans une boîte de dialogue distincte ; ils sont désormais créés et gérés dans la vue Correctif. Bien que le processus de mise à niveau convertisse automatiquement vos groupes de correctifs vers la nouvelle convention, pensez à passer vos groupes en revue

pour voir les changements apportés. Vos groupes de correctifs risquent d'être plus petits après la mise à niveau car Shavlik a cessé de prendre en charge un grand nombre d'anciens correctifs.

- **Groupes de correctifs modifiés et générés automatiquement** : Pour préserver le comportement de vos modèles d'analyse des correctifs, un ou plusieurs groupes de correctifs existants peuvent être modifiés lors du processus de mise à niveau, et un ou plusieurs nouveaux groupes de correctifs peuvent être générés automatiquement.
 - **Groupes de correctifs modifiés** : Si vous faites référence à un groupe de correctifs dans la section **Paramètres de filtre des correctifs** de votre modèle d'analyse des correctifs version 9.0 ou 9.1, et que vous activez l'option **Analyser la sélection**, tous les correctifs qui ne répondent pas aux critères définis par les filtres de modèle d'analyse sont supprimés du groupe. Voici pourquoi : Dans Protect 9.0 et 9.1, les filtres de modèle d'analyse peuvent masquer le fait que votre groupe de correctifs peut contenir des types de correctif que vous ne souhaitez pas réellement rechercher ou déployer. Dans Protect 9.2, si vous utilisez le groupe de correctifs comme ligne de base, les filtres de modèle d'analyse ne sont pas appliqués et les inexactitudes de vos groupes de correctifs sont parfois révélées. Si le processus de mise à niveau détecte cette situation, il modifie automatiquement le groupe de correctifs pour préserver l'interaction prévue entre le modèle d'analyse et le groupe de correctifs.

Exemple :

Supposons que votre groupe de correctifs version 9.1 contient un mélange de correctifs Sécurité, Correctifs autres que sécurité et Distribution de logiciels. Dans le modèle d'analyse qui fait référence à ce groupe de correctifs, la section **Paramètres de filtre des correctifs** est configurée sur **Analyser la sélection** et la section **Propriétés du correctif** est configurée pour détecter uniquement les correctifs de sécurité. Dans cette configuration, le filtre **Propriétés du correctif** est appliqué et seuls les correctifs de sécurité sont détectés (même si le groupe de correctifs contient des correctifs autres que sécurité et des correctifs Distribution de logiciels).

Après la mise à niveau vers la version 9.2, le modèle d'analyse définit le groupe de correctifs en tant que filtre de ligne de base et tous les autres filtres de modèle d'analyse sont ignorés. Si le groupe de correctifs n'est pas modifié, les correctifs de type Correctifs autres que sécurité et Distribution de logiciels sont désormais détectés (et déployés, si vous avez coché la case **Déploiement auto. des correctifs après l'analyse** lors de l'analyse). Le processus de mise à niveau reconnaît cette différence, et supprime du groupe de correctifs les correctifs autres que sécurité et les correctifs Distribution de logiciels.

Remarque : Pour aller plus loin, veillez à gérer correctement vos groupes de correctifs : n'ajoutez pas de correctifs ou types de correctif inutiles ou indésirables.

- **Groupes de correctifs générés automatiquement** : Une copie d'un groupe de correctifs existant est automatiquement générée par le processus de mise à niveau si toutes les conditions suivantes sont réunies :
 - Vous faites référence au groupe de correctifs dans la section **Paramètres de filtre des correctifs** d'un modèle d'analyse des correctifs et vous activez l'option **Analyser la sélection**, ET
 - Vous faites référence au groupe de correctifs dans une stratégie d'agent ou un autre modèle d'analyse qui contient d'autres définitions de filtre, ET
 - Le groupe de correctifs doit être modifié par le processus de mise à niveau pour garantir la compatibilité (voir ci-dessus)

Dans cette situation, une copie du groupe de correctifs est générée et modifiée comme décrit ci-dessus. Le nom du nouveau groupe de correctifs est ***<nom-groupe-correctifs>-generated for <nom-modèle-analyse>**. Le ou les modèles qui font référence au groupe de correctifs sont mis à jour pour utiliser le nouveau nom. Le groupe de correctifs d'origine est conservé, si bien que les stratégies d'agent et autres modèles d'analyse qui y font référence sont préservés.

Vous devez passer les changements en revue et, si nécessaire, renommer le groupe de correctifs généré automatiquement pour lui donner un nom plus convivial ou plus explicite.

Affectation d'alias à la console

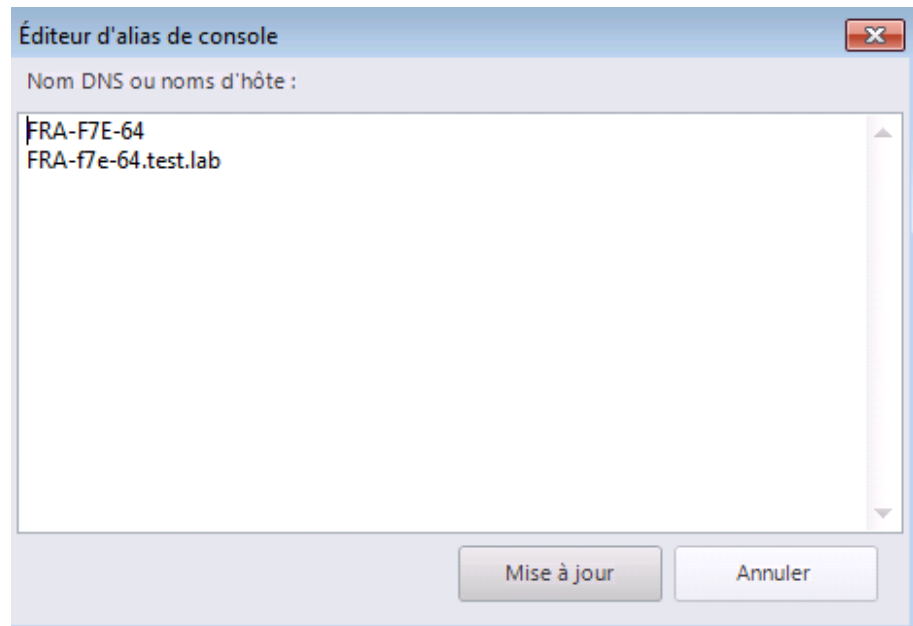
Cette opération est nécessaire si une ou plusieurs des conditions suivantes sont remplies :

- Vous avez affecté la machine de console à un nouveau domaine.
- Vous avez attribué un nouveau nom commun ou une nouvelle adresse IP à la console.
- Vous avez installé manuellement des agents et ils utilisent une adresse IP pour communiquer avec la console.

Dans ces conditions, vous devez utiliser l'outil **Éditeur d'alias de console** pour identifier les anciens noms ou adresses de console en tant qu'alias de confiance. Si vous ne le faites pas, lorsque l'agent prend contact avec la console Shavlik Protect (ou lorsqu'une machine sans agent tente d'envoyer des messages d'état du déploiement des correctifs à la console), il ne peut pas vérifier que la machine qu'il vient de contacter est une machine de confiance.

1. Sélectionnez **Outils > Éditeur d'alias de console**.

La boîte de dialogue **Éditeur d'alias de console** s'affiche. Elle contient les noms et adresses IP actuellement utilisés pour identifier la machine de console. Par exemple :

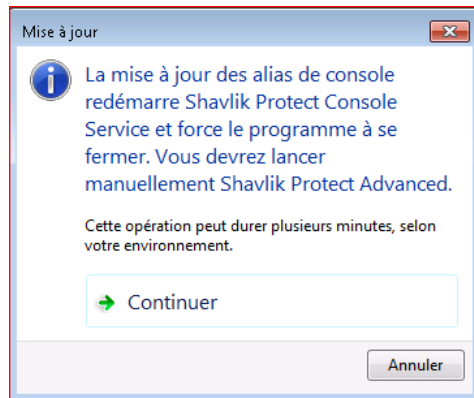


2. Entrez les noms et/ou les adresses IP à utiliser comme alias pour la machine de console.

Vous pouvez spécifier les adresses IP au format IPv4 ou IPv6.

3. Cliquez sur **Mettre à jour**.

La boîte de dialogue suivante s'affiche :



Pour mettre à jour les alias de console, vous devez redémarrer le service de console et fermer Shavlik Protect, puis le rouvrir manuellement.

IMPORTANT ! Les agents ne reconnaissent les nouveaux alias que lorsqu'ils prennent contact avec la console redémarrée. Le contact doit être lancé depuis l'agent, soit manuellement avec le programme de client d'agent, soit via un contact planifié. L'émission d'une commande de contact (check-in) depuis la console à l'attention de l'agent ne met pas à jour le certificat de la console.

Synchronisation de vos serveurs de distribution

Vous devez mettre à jour vos serveurs de distribution à l'aide des derniers correctifs, et/ou des derniers moteurs d'analyse et fichiers XML de définitions disponibles sur la console. C'est particulièrement important si vos agents utilisent des serveurs de distribution pour télécharger ces fichiers. Les serveurs de distribution doivent être synchronisés avec les fichiers de console mis à jour **avant** que les agents prennent contact.

Pour synchroniser vos serveurs de distribution :

1. Sélectionnez **Aide > Actualiser les fichiers** pour vous assurer que la console contient tous les fichiers les plus récents.
2. Sélectionnez **Outils > Opérations > Serveurs de distribution**.
3. Dans la zone **Ajouter une synchro. planifiée** du volet supérieur, sélectionnez le composant à synchroniser.
4. Dans le volet supérieur, sélectionnez le serveur de distribution à synchroniser avec la console.
5. Cliquez sur **Ajouter une synchro. planifiée**.
6. Spécifiez le moment où la synchronisation doit se produire, puis cliquez sur **Enregistrer**.
7. Dans le volet **Planifier la synchronisation automatique**, sélectionnez l'entrée de synchronisation planifiée.
8. Cliquez sur **Exécuter maintenant**.

Ne vous inquiétez pas si les agents prennent contact avant que vous ayez fini de synchroniser les serveurs de distribution. Les agents seront mis à jour lors de la prochaine exécution d'une tâche planifiée ou de la prochaine mise à jour des fichiers binaires par l'agent.

Suggestion : Activation de Predictive Patch (Correctif prédictif)

Cette nouvelle fonction permet à Shavlik Protect de télécharger automatiquement les correctifs susceptibles d'être déployés dans un futur proche. Si vous utilisez des serveurs de distribution, vous pouvez synchroniser Predictive Patch (Correctif prédictif) avec vos serveurs de distribution pour que ces derniers reçoivent une copie des correctifs téléchargés. Vous activez l'option Predictive Patch dans l'onglet **Outils > Opérations > Téléchargements**. Pour la synchronisation avec vos serveurs de distribution, activez l'option **Synchroniser avec Predictive Patch** dans la boîte de dialogue **Serveur de distribution**. Pour en savoir plus, reportez-vous à l'aide.

Rétablissement de la sécurité entre vos consoles de consolidation des données

Si vous utilisez plusieurs consoles avec une configuration de consolidation des données, vous devez rétablir l'association de sécurité entre la console centrale et chacune des consoles distantes.

IMPORTANT ! Une fois le processus de mise à niveau lancé, aucune activité de consolidation des données n'est réalisée tant que vous n'avez pas mis à niveau à la fois la console centrale et la console distante, puis rétabli l'association de sécurité entre les deux consoles. C'est pourquoi il est fortement recommandé de mettre à niveau vos consoles en tandem, à un moment où vous prévoyez très peu d'activités de consolidation des données.

Dans la console centrale

1. Mettez à niveau la console centrale.
2. Sélectionnez **Outils > Opérations > Consolidation des données** et vérifiez que vous avez bien coché la case **Accepter et importer les résultats depuis un expéditeur de consolidation**.

Dans chaque console distante

1. Mettez à niveau chaque console distante.
2. Sélectionnez **Outils > Opérations > Consolidation des données**.
3. Vérifiez les valeurs Adresse IP/Nom d'hôte et Port de votre console de consolidation.
4. Cliquez sur **Inscription**.

Pour en savoir plus sur la consolidation des données, consultez dans l'aide la rubrique **Gestion de plusieurs consoles > Configuration de la consolidation des données**.

Analyse de vos machines virtuelles

Si vous avez défini des machines virtuelles dans un groupe de machines dans l'onglet **Machines virtuelles hébergées** ou dans l'onglet **Machines virtuelles de poste de travail**, vous devez, après la mise à niveau, lancer une analyse de ces machines depuis la page d'accueil ou depuis le groupe de machines. L'opération est obligatoire pour rétablir les identités de ces machines dans Protect. Si vous ne réalisez pas cette analyse, les champs **Serveur virtuel** et **Chemin** risquent de ne pas s'afficher dans la vue Machine, et les déploiements vers ces machines risquent d'échouer.

Vérification de vos paramètres utilisateur personnalisés

Les paramètres utilisateur personnalisés suivants ne sont pas conservés lors de la mise à niveau.

- Outils > Options > onglet Affichage :
 - Éléments récents (jours)
 - Éléments d'archive
 - Afficher uniquement les éléments créés par moi
 - Afficher le flux d'actualités principal
 - Afficher les éléments Informations dans les résultats d'analyse des correctifs
 - Afficher les Service Packs dans Afficher >Correctifs
- Outils > Options > onglet Notifications et avertissements :
 - Avertissement avant la planification de déploiements
 - Fermer Actualiser les fichiers lorsque terminé
 - Avertissement si la synchronisation Protect Cloud n'est pas activée sur cette console
 - Avertissement avant ouverture de 7 bulletins ou plus
- Outils > Options > onglet Consignation :
 - Analyse des correctifs de diagnostic
- Utilitaire de suivi du déploiement :
 - Vitesse de la mise à jour
 - Jours à afficher
 - Afficher les échecs
 - Afficher les éléments en cours
 - Afficher les éléments terminés avec succès
- Boîte de dialogue Rapports
 - Trier par ID IAVA
- Hyperviseur ESXi, onglet Bulletins :
 - Afficher uniquement les derniers
- Historique des événements
 - Limiter les résultats aux x derniers (jours)
- Vue Résultats ITScript
 - Résultats depuis

Attention :
Protect 9.2
utilise un
certificat
racine SHA-2

Shavlik utilise pour la première fois des certificats racine et de console de type SHA-2 dans Protect 9.2. Ce choix a été fait pour deux raisons principales : les certificats SHA-2 2 048 bits sont plus sécurisés que la version précédente (SHA-1 1 024 bits), et la prise en charge des certificats racine SHA-1 s'arrête. Windows n'acceptera plus ces certificats à compter du 1er janvier 2017.

Une fois le processus de mise à niveau terminé, Shavlik Protect 9.2 lance ses propres opérations en coulisse en vue d'émettre un nouveau certificat racine SHA-2 et un nouveau certificat de console SHA-2. Si vous n'utilisez pas d'agents, ce processus est invisible et vous pouvez l'ignorer. Si vous utilisez des agents, une partie du processus consiste à attendre que vos agents prennent contact afin qu'ils reçoivent le nouveau certificat racine en attente. Ce processus peut prendre quelques jours ou quelques semaines, car plusieurs facteurs entrent en jeu, mais tout se fait à l'arrière-plan. Vous intervenez uniquement pour surveiller l'historique des événements afin de vérifier s'il s'est produit des incidents qui nécessitent votre attention.

CHANGEMENTS ET AMELIORATIONS IMPORTANTS DANS SHAVLIK PROTECT 9.2

Pour en savoir plus sur chacun de ces sujets, consultez le système d'aide :

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

Déploiements de correctifs

Le moteur de création de paquets et de déploiement des correctifs sur les machines a été entièrement réécrit. Les performances et la fiabilité ont été fortement améliorées.

Contenu de correctifs

Les données d'évaluation et de déploiement des correctifs que Shavlik Protect exploite ont été remaniées et améliorées de différentes manières.

Filtrage des modèles d'analyse des correctifs

Davantage de métadonnées ont été ajoutées au contenu de correctifs. De plus, l'onglet **Filtrage** de la boîte de dialogue **Modèle d'analyse des correctifs** a été mis à jour pour permettre une plus grande précision d'analyse.

Vue Correctif/Groupes de correctifs

La vue Correctif a été entièrement remaniée et mise à jour. Elle utilise le nouveau format de contenu, qui vous permet d'afficher les informations de correctifs de façon plus concise. De plus, les groupes de correctifs sont désormais créés et gérés dans la vue Correctif. Cela vous permet de faire des recherches dans les correctifs et de créer des groupes de correctifs de manière plus unifiée.

Tâches planifiées

Les tâches planifiées sur la console utilisent désormais le Planificateur de tâches Microsoft. Une nouvelle boîte de dialogue, accessible via le menu **Gérer > Tâches de console planifiées**, vous permet d'afficher et de gérer ces tâches.

Rapports

Un nouveau rapport nommé **Fin de vie par produit** est désormais disponible. De plus, vous disposez d'une nouvelle boîte de dialogue **Planifier le rapport**, accessible via le menu **Outils > Planifier le rapport**. Elle vous permet de générer automatiquement un rapport à une date future. Ce rapport peut être créé automatiquement une seule fois ou de façon récurrente.

Predictive Patch (Correctif prédictif)

Cette nouvelle option permet à Shavlik Protect de télécharger automatiquement les correctifs susceptibles d'être déployés dans un futur proche. Le téléchargement des correctifs par anticipation avant leur déploiement accélère le processus de déploiement.

Planification « Foire aux correctifs + X (jours) »

Lorsque vous planifiez des analyses de console, vous pouvez désormais retarder une analyse récurrente d'un certain nombre de jours pour qu'elle coïncide avec un événement périodique. Par exemple, vous pouvez planifier une analyse de correctifs mensuelle afin qu'elle s'exécute le jour qui suit la Foire aux correctifs, en utilisant la nouvelle option **Ajouter un délai (jours)**.

Notification de fin de vie

Au fil du temps, si la version de Shavlik Protect que vous utilisez approche de sa date de fin de vie (EOL), une notification s'affiche lorsque vous démarrez Shavlik Protect.

Intégration de Protect Cloud

Les résultats d'analyse des correctifs et de déploiement peuvent être périodiquement envoyés à Protect Cloud. Si vous utilisez Shavlik Empower, les données de correctif sont périodiquement extraites depuis Protect Cloud par Empower et peuvent être affichées dans l'interface utilisateur de type navigateur de Shavlik Empower.

Changements apportés à l'interface utilisateur

Les éléments suivants de l'interface utilisateur ont été changés :

- La vue Correctif a été entièrement remaniée.
- Les groupes de correctifs sont désormais créés et gérés dans la vue Correctif.
- Dans la vue Machine :
 - Le volet supérieur contient trois nouvelles colonnes : Serveur virtuel, Nom de VM et Chemin
 - L'onglet **Biens virtuels** a été supprimé du volet central.
 - Dans le volet inférieur, les onglets **Machines manquantes** et **Machines installées** ont été combinés en un seul, nommé **Machines affectées**.
- Dans le modèle de déploiement de correctifs :
 - La prise en charge des points d'installation Office et des supports d'origine a été supprimée.
 - Les options **Sauvegarder les fichiers pour la désinstallation** et **Mode silencieux** ne sont plus disponibles. Ces fonctions sont désormais toujours activées.
 - L'onglet **Serveurs de distribution** a été remanié afin de mieux identifier l'ordre d'utilisation des sources de téléchargement.
- Dans le modèle d'analyse des correctifs :
 - L'onglet Filtrage a été entièrement remanié.
 - L'option Criticité de l'utilisateur n'est plus disponible.
 - L'onglet Distribution de logiciels inclut désormais uniquement les produits qui n'ont pas été remplacés.
- Dans une stratégie d'agent, il est désormais possible de créer toutes les tâches sans planification récurrente. Vous pouvez donc définir des tâches qui s'exécuteront uniquement via l'interface utilisateur de l'agent ou par lancement à distance depuis la console.

- Dans un groupe de machines, les options **Tester l'existence** et **Tester les références d'authentification** ont été combinées. Vous les activez désormais en exécutant une analyse d'état de l'alimentation.
- Les récapitulatifs des biens virtuels ne sont plus disponibles dans la vue Machine. Toutes les informations sur les biens virtuels sont désormais disponibles via la fonction Inventaire virtuel.
- Les rapports suivants ont été supprimés : Détails du matériel des machines virtuelles, Utilisation de la mémoire et Rapport d'utilisation des disques des machines virtuelles.
- Dans la vue Analyse, le sous-volet Récapitulatif de l'analyse ne peut plus être réduit.
- Les tâches planifiées sont désormais séparées en deux boîtes de dialogue distinctes : **Gérer > Tâches distantes planifiées** et **Gérer > Tâches de console planifiées**.
- Sous **Outils > Options** :
 - **Affichage** : Contient la case à cocher **Afficher les Service Packs dans Afficher->Correctifs**.
 - **Notifications et avertissements** : Contient une nouvelle case à cocher nommée **Avertissement avant ouverture de 7 bulletins ou plus**. Par contre, la case à cocher **Avertissement avant la planification d'opérations si les références d'authentification par défaut diffèrent de celles de l'utilisateur actuel** n'est plus disponible.
 - **Langues de correctif** : Cet onglet a été supprimé. Le programme détecte désormais automatiquement les langues de systèmes d'exploitation utilisées sur vos machines gérées, et télécharge uniquement les versions des correctifs correspondant aux langues nécessaires.
 - **Analyses** : Contient une nouvelle case à cocher, nommée **Toujours appliquer les exclusions de groupe de machines**.
 - **Déploiement** : L'option **Adresse de l'utilitaire de suivi du déploiement** a été supprimée. L'adresse est désormais définie dans l'outil **Éditeur d'alias de console**.
 - **Consignation** : Contient une nouvelle case à cocher, nommée **Analyse des correctifs de diagnostic**.