IBM Security Network Protection Manager

Guide d'installation et de configuration

Version 1 Edition 0

Cette édition s'applique à la version 1.0.0 d'IBM Network Protection Manager et à toutes les éditions et modifications ultérieures jusqu'à indication contraire dans les nouvelles éditions.

Réf. FR : GC**-****-**

Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. Les informations qui y sont fournies sont susceptibles d'être modifiées avant que les produits décrits ne deviennent eux-mêmes disponibles. En outre, il peut contenir des informations ou des références concernant certains produits, logiciels ou services non annoncés dans ce pays. Cela ne signifie cependant pas qu'ils y seront annoncés.

Pour plus de détails, pour toute demande d'ordre technique, ou pour obtenir des exemplaires de documents IBM, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial.

Vous pouvez également consulter les serveurs Internet suivants :

- http://www.fr.ibm.com (serveur IBM en France)
- http://www.ibm.com/ca/fr (serveur IBM au Canada)
- http://www.ibm.com (serveur IBM aux Etats-Unis)

Compagnie IBM France
Direction Qualité
17, avenue de l'Europe
92275 Bois-Colombes Cedex

Informations juridiques

Cette section contient les informations juridiques concernant IBM Security Network Protection Manager.

Remarque : Ce produit n'est pas destiné à être connecté, directement ou indirectement, par quelque moyen que ce soit, à des interfaces de réseaux de télécommunications publiques.

Utilisation des cookies

Cette offre logicielle n'utilise pas de cookies ou d'autres technologies pour collecter des informations personnellement identifiables.

Déclaration de pratiques de sécurité recommandées

La sécurité des systèmes informatiques implique la protection des systèmes et des informations par la prévention, la détection et la réponse aux accès non autorisés depuis l'intérieur ou l'extérieur de votre entreprise. Un accès non autorisé peut se traduire par la modification, la destruction ou une utilisation inadéquate ou malveillante de vos systèmes, y compris l'utilisation de ces derniers pour attaquer d'autres systèmes. Aucun système ou produit informatique ne doit être considéré comme étant complètement sécurisé et aucun produit, service ou mesure de sécurité ne peut être entièrement efficace contre une utilisation ou un accès non autorisé. Les systèmes, les produits et les services IBM sont conçus pour s'intégrer à une approche de sécurité complète, qui implique nécessairement des procédures opérationnelles supplémentaires, et peuvent avoir besoin d'autres systèmes, produits ou services pour optimiser leur efficacité. IBM NE GARANTIT PAS QUE TOUS LES SYSTEMES, PRODUITS OU SERVICES SONT A L'ABRI DES CONDUITES MALVEILLANTES OU ILLICITES DE TIERS OU QU'ILS PROTEGERONT VOTRE ENTREPRISE CONTRE CELLES-CI.

Table des matières

Chapitre 1. Présentation du produit

Introduction

IBM® Security Network Protection Manager est un système de gestion centralisée qui unifie la gestion d'IBM Security Network Protection (XGS). Dans cette version, il complète IBM Security SiteProtector System comme module complémentaire permettant de servir les nouvelles fonctionnalités de gestion avec la console Web d'IBM Security Network Protection (XGS).

Fonctions principales

IBM Security Network Protection Manager version 1.0 contient les fonctions principales ci-après.

Recherche avancée et filtrage à facettes

L'interface utilisateur Web d'IBM Security Network Protection Manager dispose de fonctionnalités de recherche avancées, qui permettent aux utilisateurs de rechercher des mots clés à l'aide de la barre de recherche à accès rapide qui se trouve dans la partie supérieure de l'interface. Les résultats de la recherche sont mis à jour simultanément pendant la saisie des mots clés. Vous pouvez affiner les résultats de la recherche en ajoutant ou en supprimant des filtres.

Edition de règle en un clic

Le bouton **Editer en un clic** est disponible dans les détails récapitulatifs d'un résultat de recherche d'une signature. Vous pouvez utiliser cette fonction pour déterminer l'état de protection contre une menace, effectuer des modifications nécessaires et déployer rapidement les règles IPS mises à jour sur les agents IBM Security Network Protection (XGS).

Statut de l'agent

Le récapitulatif du statut de l'agent est fourni dans le tableau de bord de l'interface utilisateur Web d'IBM Security Network Protection Manager après connexion. Vous pouvez cliquer sur le nombre du statut de l'agent pour afficher les détails de la santé de l'agent et du déploiement des règles.

Notifications

Vous pouvez afficher les notifications en cliquant sur l'icône d'enveloppe dans le coin supérieur droit de la page. Le nombre inscrit dans l'icône indique le nombre de notifications non lues. Les notifications sont répertoriées dans l'ordre chronologique inverse, en commençant par la plus récente.

Chapitre 2. Installation d'IBM Security Network Protection Manager

Configuration requise par le produit

Vérifiez la configuration ci-après avant d'installer et d'utiliser IBM Security Network Protection Manager 1.0.

- IBM Security SiteProtector System 3.1.1 avec Database Service Pack (DBSP) 3.1.1.41 ou version ultérieure
- VMWare ESXi 5.5 et versions ultérieures
- Google Chrome 51 et versions ultérieures

Installation d'IBM Security SiteProtector System

Vous devez installer IBM Security SiteProtector System 3.1.1 avant d'installer des instances d'IBM Security Network Protection Manager.

Pourquoi et quand exécuter cette tâche

Consultez les étapes d'installation détaillées d'IBM Security SiteProtector System sur le site https://www.ibm.com/support/knowledgecenter/SSETBF_3.1.1/com.ibm.siteprotector.doc/tasks/sp_t_installing.htm.

Que faire ensuite

Passez à la rubrique «Mise à jour d'IBM Security SiteProtector System avec DBSP 3.1.1.41 ou une version ultérieure».

Mise à jour d'IBM Security SiteProtector System avec DBSP 3.1.1.41 ou une version ultérieure

Avant d'installer IBM Security Network Protection Manager, vous devez configurer IBM Security SiteProtector System.

Pourquoi et quand exécuter cette tâche

Mettez à jour IBM Security SiteProtector System Database Service Pack (DBSP) à la version 3.1.1.41.

Procédure

1. Connectez-vous et accédez au système SiteProtector.
2. Dans la sous-fenêtre de gauche, sélectionnez le **noeud du site**.
3. Dans la liste **Go to**, sélectionnez **Agent**. La vue Agent apparaît dans le panneau de droite.
4. Dans le panneau de droite, cliquez à l'aide du bouton droit de la souris sur le composant SiteProtector à mettre à jour, puis sélectionnez **Updates** > **Apply XPU**. La fenêtre Schedule Update s'affiche.
5. "Voulez-vous mettre à jour l'agent immédiatement ?"
   - Si la réponse est oui, sélectionnez **Run Once** à la section Recurrence Pattern, cliquez sur **OK**, puis passez à l'étape 6.
   - Si la réponse est non, planifiez un travail de commande pour mettre à jour les agents de façon périodique, puis cliquez sur **OK**.

Remarque : Si vous avez sélectionné **Run Once** pour installer la mise à jour immédiatement, le processus d'installation commence. Si vous avez planifié l'installation ultérieure de la mise à jour, le processus d'installation commence à l'heure dite.
Dans le cas des installations immédiates, IBM Security SiteProtector System affiche la progression comme suit :

Indicateur	Description
Overall progress	Indique la progression du processus d'installation complet
Current step progress	Indique la progression de chaque étape du processus de mise à jour ; la zone de texte affiche un récapitulatif de l'étape en cours

La fenêtre End User License Agreement s'affiche.

6. Lisez le contrat, puis sélectionnez **I Accept**. La fenêtre Select XPU s'affiche.
7. Cliquez sur **Product feature**.
8. Lorsque vous êtes prêt à installer les mises à jour, cliquez sur **Finish**.
9. Cliquez sur **Finish** lorsque le processus d'installation est terminé.

Que faire ensuite

Passez à la rubrique «Configuration de Microsoft SQL Server».

Configuration de Microsoft SQL Server

Vous avez besoin d'un compte utilisateur SQL pour accéder à la base RealSecureDB de SiteProtector pour IBM Security Network Protection Manager. Vous pouvez utiliser un compte utilisateur SQL existant ou en créer un. Pour la prise en charge de SQL Server, veuillez contacter Microsoft.

Avant de commencer

- Effectuez les étapes décrites dans la rubrique relative à la mise à jour du système SiteProtector avec le dernier Service Pack de base de données.

Important : Vous devez être connecté avec les droits d'administrateur de RealSecureDB pour effectuer les tâches ci-après.

Pourquoi et quand exécuter cette tâche

Ajouter un utilisateur au rôle ISNPM_Application.

Important : N'utilisez pas de compte d'administrateur système (SA) pour vous connecter à la base de données d'IBM Security Network Protection Manager.

Procédure

1. Dans SQL Server Management Studio, connectez-vous à la base de données SiteProtector
2. Dans **Explorateur d'objets**, cliquez pour développer le dossier **Bases de données**.
3. Cliquez sur **RealSecureDB** > **Sécurité** > **Rôles** > **Rôles de base de données**, cliquez sur **ISNPM_Application** à l'aide du bouton droit de la souris, puis sélectionnez **Propriétés**.
4. Cliquez sur **Général** dans le coin supérieur gauche de la fenêtre, puis cliquez sur **Ajouter** sous la section Membres de ce rôle dans la partie inférieure gauche de la fenêtre.
5. Entrez votre nom d'utilisateur RealSecureDB, cliquez sur **Vérifier les noms**, puis cliquez sur **OK**.
6. Cliquez sur **OK** pour terminer cette tâche.

Que faire ensuite

Passez à la rubrique «Installation d'IBM Security Network Protection Manager».

Installation d'IBM Security Network Protection Manager

IBM Security Network Protection Manager 1.0 est un module complémentaire d'IBM Security SiteProtector System. Vous devez posséder une licence IBM Security SiteProtector System active pour installer et utiliser IBM Security Network Protection Manager selon les dispositions du contrat d'abonnement et d'assistance logiciels d'IBM Security SiteProtector System.

Avant de commencer

- Effectuez les étapes décrites dans la rubrique «Configuration de Microsoft SQL Server», à la page 4.
- Installez VMWare ESXi 5.5 ou une version ultérieure.
- Vérifiez que le port de la base de données (1433 par défaut) est actif et non bloqué par le pare-feu.

Procédure

1. Déployez le fichier OVA d'IBM Security Network Protection Manager 1.0 sur un serveur ESX VMware.

   Remarque : Pour les étapes de déploiement du modèle OVA, voir Déployer un modèle OVF sur VMware.com.
2. Démarrez la machine virtuelle d'IBM Security Network Protection Manager et effectuez les étapes de la configuration initiale à l'aide de l'interface de ligne de commande.
3. Connectez-vous à l'Assistant de paramètres de dispositif initiaux de ligne de commande avec les donnée d'identification par défaut :
   - **Nom d'utilisateur :** admin
   - **Mot de passe :** admin
4. L'étape Bienvenue est affichée au lancement de l'**Assistant de paramètres de dispositif initiaux de ligne de commande**.

   Remarque : A partir de cette étape, vous pouvez vous déplacer entre les étapes de l'assistant à l'aide des options suivantes :
   - `p` : étape précédente
   - `n` : étape suivante
5. Modifiez votre mot de passe dans l'étape Mot de passe système.

   Remarque : Il est fortement recommandé de modifier le mot de passe par défaut lors de cette étape.
6. Modifiez le nom d'hôte dans l'étape Configuration de l'hôte.
7. Affichez les paramètres des unités et configurez les interfaces réseau de gestion dans l'étape Paramètres de l'interface de gestion.
8. Configurez les serveurs DNS dans l'étape Configuration DNS.
9. Configurez l'heure, la date et le fuseau horaire dans l'étape Configuration de l'heure.
10. Affichez les paramètres de connexion, configurez la connexion à la base de données et testez la connexion à la base de données configurée, dans l'étape Configuration de la base de données :
    - Vous devez créer un utilisateur SQL sur la base de données et octroyez à l'utilisateur le rôle de base de données "ISNPM_Application".
    - Effectuez les tâches suivantes :
      a. Sélectionnez **Configurer la base de données** pour vous connecter au système SiteProtector.
      b. Entrez le nom de la base de données (RealSecureDB), puis appuyez sur **Entrée** pour utiliser la valeur par défaut.

c. Entrez le nom du serveur de base de données (), puis entrez l'adresse IP de la base de données SiteProtector.
d. Entrez le numéro de port de la base de données (1433), puis appuyez sur **Entrée** pour utiliser la valeur par défaut.
e. Entrez le nom d'utilisateur de la base de données () : `User_member_of_the_ISNPM_Application_role`
f. Entrez le mot de passe de la base de données : entrez le mot de passe de l'utilisateur de base de données.
g. Entrez l'option de chiffrement de la base de données (requis) : appuyez sur **Entrée** pour utiliser la valeur par défaut.

11. Vérifiez le récapitulatif des détails de configuration et effectuez l'une des tâches suivantes :
    - Sélectionnez **Accepter la configuration** pour enregistrer les paramètres et fermer l'**Assistant de paramètres de dispositif initiaux de ligne de commande**.
    - Sélectionnez **Annuler la configuration** pour annuler les paramètres précédemment configurés.
    - Sélectionnez **Modifier la configuration** pour modifier les paramètres précédemment configurés.

Chapitre 3. Configuration d'IBM Security Network Protection Manager

Informations sur la configuration de la sécurité, du réseau et des paramètres système d'IBM Security Network Protection Manager.

Utilisation de l'interface utilisateur Web

IBM Security Network Protection Manager offre une interface graphique accessible par l'intermédiaire d'un navigateur.

Pour vous connecter à l'interface utilisateur Web, effectuez les tâches suivantes :

1. Entrez l'adresse IP ou le nom d'hôte d'IBM Security Network Protection Manager dans votre navigateur Web.
2. Facultatif : cliquez sur la liste déroulante dans le coin supérieur droit de la fenêtre pour modifier la langue de l'interface utilisateur Web.
3. Entrez le nom d'utilisateur et le nouveau mot de passe modifié dans l'étape 5 décrite dans la rubrique **Installation d'IBM Security Network Protection Manager**.
4. Cliquez sur **Ouverture de session**.

   Remarque : La première fois que vous vous connectez, IBM Security Network Protection Manager affiche le contrat de licence logiciel IBM.

   - Cliquez sur **J'accepte** pour accepter les dispositions du contrat de licence logiciel et accéder à l'interface utilisateur Web.
   - Si vous les refusez, cliquez sur **Je n'accepte pas**. Vous serez redirigé vers la page de connexion.

Pour vous déconnecter de l'interface utilisateur Web, cliquez sur **Utilisateur en cours** > **Déconnexion** dans le coin supérieur droit de la fenêtre.

Conseil :

- Une fois que vous vous êtes connecté, vous devez vous déconnecter pour retourner à la page de connexion afin de modifier la langue d'affichage.
- Une fois que vous vous êtes connecté, si vous appuyez sur la touche du point d'interrogation **?**, la liste **Raccourcis clavier** s'affiche dans l'interface utilisateur Web.
- Lorsque vous vous connectez à IBM Security Network Protection Manager, le 6e échec de connexion consécutif déclenche un verrouillage. Une connexion réussie par tout utilisateur réinitialise le décompte des échecs de connexion et met fin au verrouillage.

IBM Security Network Protection Manager a été développé à l'aide de recherches sur Equipe de recherche et développement IBM X-Force. Cliquez sur le lien de la page de connexion pour en savoir plus sur IBM Security.

Utilisation du tableau de bord

Tableau de bord est la première page après la connexion. Vous pouvez afficher Statut de l'agent ou Modifications récentes dans la page Tableau de bord.

Cliquez sur **Accéder au tableau de bord** dans le coin supérieur droit de la fenêtre pour accéder au tableau de bord.

Affichage du statut de l'agent

Le récapitulatif du statut de l'agent est fourni dans le tableau de bord d'IBM Security Network Protection Manager après connexion.

Pourquoi et quand exécuter cette tâche

Vous pouvez accéder au statut actuel de l'agent à partir du tableau de bord pour afficher les détails de la santé de l'agent et le déploiement des règles.

Procédure

1. Une fois que vous vous êtes connecté à IBM Security Network Protection Manager, cliquez sur un nombre répertorié dans le tableau de bord pour afficher la catégorie spécifiée.
2. Cliquez sur l'un des résultats pour afficher les détails de son récapitulatif.

Affichage des modifications récentes

La sous-fenêtre Modifications récentes à gauche de la page Tableau de bord répertorie les modifications récentes dans l'ordre chronologique inverse, en commençant par la plus récente.

Légendes des icônes

Icône	Description
	Référentiel de règles.
	Indicateurs déployés.
	Indicateurs non déployés.
	Version des règles.
	Nom de l'utilisateur.
	Heure de l'opération.

Configuration de l'interface réseau

Utilisez la page Interface réseau pour afficher et gérer la configuration de l'interface réseau.

Pourquoi et quand exécuter cette tâche

Si vous modifiez l'adresse IP de l'interface réseau, connectez votre navigateur Web à la nouvelle adresse IP pour les sessions ultérieures.

Procédure

1. Cliquez sur **Paramètres du système** dans le coin supérieur droit de la fenêtre.
2. Cliquez sur **Interface réseau** dans la sous-fenêtre Paramètres système sur le côté gauche de la fenêtre.
3. Entrez un nom d'hôte dans la page Interface réseau .
4. Sélectionnez l'une des options suivantes dans la section DNS :

Option	Description
Auto	Acquiert les adresses du serveur DNS à partir d'un serveur DHCP.
Manuel	Indiquez les serveurs DNS. • **DNS principal** indique l'adresse IP du serveur DNS principal. • **DNS secondaire** indique l'adresse IP d'un serveur DNS secondaire facultatif. • **DNS tertiaire** indique l'adresse IP d'un serveur DNS tertiaire facultatif. • **Chemin de recherche DNS** indique un ou plusieurs chemins de recherche DNS. Entrez les chemins séparés par des virgules.

5. Dans la section **IPV4**, configurez les options suivantes :
   - Auto
   - Manuel
     - Adresse
     - Masque de réseau
     - Passerelle
6. Dans la section **IPV6**, configurez les options suivantes :
   - Auto
   - Manuel
     - Adresse
     - Préfixe
     - Passerelle
7. Cliquez sur l'icône **Enregistrer les modifications** dans le coin inférieur droit de la fenêtre.

Configuration des paramètres de date et d'heure

Utilisez la page Date et heure pour configurer la date, l'heure et les informations sur le serveur NTP.

Procédure

1. Cliquez sur **Paramètres du système** dans le coin supérieur droit de la fenêtre.
2. Cliquez sur **Date et heure** dans la sous-fenêtre Paramètres système sur le côté gauche de la fenêtre.
3. Si nécessaire, modifiez la date et l'heure sur la page Date et heure.
4. Vérifiez le paramètre Fuseau horaire configuré.

   Remarque : Vous ne pouvez modifier le paramètre de fuseau horaire qu'à l'aide de commandes de l'interface de ligne de commande.
5. Pour entrer les adresses de serveur NTP (Network Time Protocol) utilisées par le système, cochez la case **Activer NTP**.

   Remarque : Vous pouvez entrer plusieurs serveurs NTP, séparés par des virgules.

6. Cliquez sur l'icône **Enregistrer les modifications** dans le coin inférieur droit de la fenêtre.

Installation d'un groupe de correctifs

Installez un groupe de correctifs lorsque le service clients IBM vous demande de le faire. Vous ne pouvez pas désinstaller de groupe de correctifs à partir de l'interface utilisateur Web. Un groupe de correctifs ne peut être désinstallé qu'à partir de l'interface de ligne de commande.

Avant de commencer

Les groupes de correctifs sont appliqués à votre partition active. Vous pouvez créer manuellement une sauvegarde de votre partition active avant d'appliquer un groupe de correctifs, de sorte que vous puissiez annuler vos modifications.

Procédure

1. Cliquez sur **Paramètres du système** dans le coin supérieur droit de la fenêtre.
2. Cliquez sur **Groupes de correctifs** dans la sous-fenêtre Paramètres système sur le côté gauche de la fenêtre.
3. Cliquez sur **Nouveau** dans la page Groupes de correctifs.
4. Recherchez le fichier du groupe de correctifs, puis cliquez sur **Ouvrir**.
5. Cliquez sur l'icône **Enregistrer les modifications** dans le coin inférieur droit de la fenêtre pour installer le groupe de correctifs.

Gestion des paramètres du microprogramme

Le système IBM Security Network Protection Manager comporte deux partitions ; chacune avec un microprogramme distinct. Les partitions sont permutées lors des mises à jour du microprogramme, de sorte que vous puissiez annuler ces dernières.

Pourquoi et quand exécuter cette tâche

Chacune des deux partitions peut être active. Si elle a été installée d'origine, la partition 1 est active et contient la version de microprogramme correspondant à la version actuelle du produit. Lorsque vous appliquez une mise à jour de microprogramme, cette dernière est installée sur la partition 2 et vos règles et paramètres sont copiés de la partition 1 vers la partition 2. IBM Security Network Protection Manager redémarre le système à l'aide de la partition 2, qui est maintenant la partition active.

Remarque : IBM Security Network Protection Manager est livré avec des versions de microprogramme identiques installées sur les deux partitions.

Procédure

1. Cliquez sur **Paramètres du système** dans le coin supérieur droit de la fenêtre.
2. Cliquez sur **Paramètres de microprogramme** dans la sous-fenêtre Paramètres système sur le côté gauche de la fenêtre.
3. Effectuez une ou plusieurs des actions suivantes, dans la page Paramètres de microprogramme :

Option	Description
Editer	1. Cliquez sur **Editer** pour éditer les commentaires. 2. Cliquez sur **ENREGISTRER** pour enregistrer les modifications.

Option	Description
Sauvegarder	Cliquez sur **OUI** pour confirmer les modifications. **Important :** Créez une sauvegarde de votre microprogramme uniquement lorsque vous installez un groupe de correctifs fourni par IBM Customer Support.Les groupes de correctifs sont installés sur la partition active et vous ne pourrez peut-être pas les désinstaller. **Remarque :** Le processus de sauvegarde peut durer plusieurs minutes.
Activer	1. Définissez une partition active lorsque vous souhaitez utiliser le microprogramme installé sur cette partition. Par exemple, vous pouvez définir une partition active pour utiliser le microprogramme ne contenant pas de mise à jour récemment appliquée ou de groupe de correctifs. 2. Cliquez sur **OUI** pour confirmer les modifications. **Remarque :** Si vous définissez une partition active, IBM Security Network Protection Manager redémarre le système à l'aide de la partition nouvellement activée.

Modification des mots de passe

La page Mot de passe administrateur permet de modifier le mot de passe que vous utilisez pour accéder à IBM Security Network Protection Manager.

Procédure

1. Cliquez sur **Paramètres du système** dans le coin supérieur droit de la fenêtre.
2. Cliquez sur **Mot de passe administrateur** dans la sous-fenêtre Paramètres système sur le côté gauche de la fenêtre.
3. Entrez le mot de passe à modifier dans la zone **Mot de passe actuel** de la page Mot de passe administrateur.
4. Entrez votre nouveau mot de passe deux fois pour le confirmer, puis cliquez sur l'icône **Enregistrer les modifications** dans le coin inférieur droit de la fenêtre.

   Remarque : La longueur du mot de passe doit être comprise entre 6 et 15 caractères alphanumériques.

Configuration des paramètres de base de données

Utilisez la page Paramètres de base de données pour configurer les paramètres de base de données d'IBM Security Network Protection Manager .

Pourquoi et quand exécuter cette tâche

Les paramètres de base de données contiennent des informations relatives à la base de données, comme le nom de la base de données, le serveur de la base de données, le port de la base de données, l'ID utilisateur, le mot de passe et le chiffrement de la base de données.

Procédure

1. Cliquez sur **Paramètres du système** dans le coin supérieur droit de la fenêtre.
2. Cliquez sur **Paramètres de base de données** dans la sous-fenêtre Paramètres système sur le côté gauche de la fenêtre.

3. Configurez les zones suivantes dans la page Paramètres de base de données.

Option	Description
Nom de la base de données	Nom de la base de données.
Serveur de la base de données	Adresse IP du serveur de base de données.
Port de la base de données	Numéro de port du serveur de la base de données.
ID utilisateur	Nom d'utilisateur requis pour l'authentification sur le serveur de base de données.
Mot de passe	Mot de passe requis pour l'authentification sur le serveur de base de données.
Chiffrement de la base de données	Le chiffrement est requis par défaut. **Important :** Pour utiliser **Chiffrement de la base de données**, votre base de données doit prendre en charge Transport Layer Security version 1.2 (TLSv1.2).

4. Cliquez sur l'icône **Enregistrer les modifications** dans le coin inférieur droit de la fenêtre.

Mise à jour d'IBM Security Network Protection Manager

La page Mises à jour permet d'afficher et d'effectuer la procédure de mise à jour d'IBM Security Network Protection Manager.

Installation des mises à jour disponibles

Les mises à jour applicables à votre instance IBM Security Network Protection Manager sont affichées dans la sous-fenêtre Mises à jour disponibles.

Effectuez l'une des tâches suivantes pour gérer vos mises à jour disponibles :

- Cliquez sur **Actualiser** pour recharger les données afin de vérifier si de nouvelles mises à jour sont disponibles.
- Cliquez sur **Télécharger** pour appliquer les mises à jour avec le fichier de mise à jour déjà téléchargé.
- Pour installer des mises à jour de la liste Mises à jour disponibles, sélectionnez le fichier de mise à jour à installer, puis cliquez sur **Installer**.

Affichage de l'historique des mises à jour

Vous pouvez afficher l'historique de vos mises à jour dans la sous-fenêtre Historique des mises à jour.

Cliquez sur **ACTUALISER** pour recharger les données et renouveler l'historique.

Configuration des paramètres du serveur de mises à jour d'IBM Security Network Protection Manager

Configurez IBM Security Network Protection Manager pour télécharger les fichiers de mise à jour à partir d'un serveur de mises à jour. Vous ne pouvez utiliser qu'un serveur de mises à jour à la fois.

Pourquoi et quand exécuter cette tâche

- Si vous souhaitez mettre à jour un certificat existant car il est arrivé à expiration ou n'est plus valide, cliquez sur **Effacer les certificats** pour supprimer le certificat actuel. Un nouveau certificat sera importé lors de la prochaine connexion au serveur de mises à jour.
- Cliquez sur **Annuler les modifications** pour restaurer les paramètres sauvegardés précédemment.

Remarque : Par défaut, IBM Security Network Protection Manager communique directement avec le serveur de mises à jour d'IBM Security X-Press, avec les paramètres suivants :

- **Adresse du serveur** : ibmxpu.flexnetoperations.com

- **Port** : 443 (ce paramètre ne peut pas être modifié pour `ibmxpu.flexnetoperations.com`)
- **Niveau de confiance** : Approuver la première fois (ce paramètre ne peut pas être modifié pour `ibmxpu.flexnetoperations.com`)

Procédure

1. Cliquez sur **Paramètres du système** dans le coin supérieur droit de la fenêtre.
2. Cliquez sur **Mises à jour** dans la sous-fenêtre Paramètres système sur le côté gauche de la fenêtre.
3. Configurez les options suivantes dans la sous-fenêtre Serveur de mises à jour.

Option	Description
Adresse du serveur	Adresse IPv4/IPv6 ou nom de domaine complet du serveur de mises à jour.
Port	Numéro de port utilisé par IBM Security Network Protection Manager pour communiquer avec le serveur de mises à jour.
Niveau de confiance	Définit la manière dont IBM Security Network Protection Manager est authentifié avec le serveur de mises à jour. **Approuver la première fois** Si aucun certificat n'est disponible, IBM Security Network Protection Manager en télécharge un à partir du serveur lorsqu'il se connecte à celui-ci pour la première fois. Le niveau de confiance Première accréditation est plus sécurisé que le niveau Faire confiance à tous et moins sécurisé que le niveau Explicite. **Explicite (IBM XPU)** IBM Security Network Protection Manager utilise le certificat local du serveur de mises à jour IBM Security pour authentifier la connexion au serveur de mises à jour. Le certificat du serveur de mises à jour IBM ISS est installé sur IBM Security Network Protection Manager par défaut. Le niveau de confiance explicite correspond au niveau de confiance le plus sécurisé. **Approuver tout** IBM Security Network Protection Manager fait confiance au serveur de mises à jour, et n'utilise pas de certificats SSL pour l'authentification. Le niveau de confiance Faire confiance à tous est le niveau le moins sécurisé. **Avertissement :** Le niveau de confiance Faire confiance à tous présente un risque de sécurité car le serveur de mises à jour interne peut être usurpé et redirigé vers un serveur factice.

4. Facultatif : Si vous utilisez un serveur proxy, configurez les paramètres suivants dans la section **Paramètres du proxy**. Les zones Adresse proxy, Port du proxy, Nom de l'utilisateur du proxy et Mot de passe du proxy sont affichées lorsque vouc cochez la case Utiliser le proxy.

Option	Description
Utiliser le proxy	Permet à IBM Security Network Protection Manager d'utiliser un serveur proxy pour les serveurs de mises à jour.
Adresse du serveur	Adresse IP ou nom DNS du serveur proxy.
Port	Numéro de port que le serveur proxy utilise pour communiquer avec le serveur de mises à jour.
Utiliser l'authentification	Permet à IBM Security Network Protection Manager de s'authentifier sur un serveur proxy.
Nom d'utilisateur	Nom d'utilisateur requis pour l'authentification sur le serveur proxy.
Mot de passe	Mot de passe requis pour l'authentification sur le serveur proxy.

5. Cliquez sur l'icône **Enregistrer les modifications** dans le coin inférieur droit de la fenêtre.

Redémarrage ou arrêt d'IBM Security Network Protection Manager

Utilisez la page Redémarrage ou arrêt pour redémarrer ou arrêter IBM Security Network Protection Manager.

Procédure

1. Cliquez sur **Paramètres du système** dans le coin supérieur droit de la fenêtre.
2. Cliquez sur **Redémarrage ou arrêt** dans la sous-fenêtre Paramètres système sur le côté gauche de la fenêtre.
3. Exécutez l'une des tâches suivantes :

Option	Description
Redémarrer	Le redémarrage place IBM Security Network Protection Manager hors ligne pendant plusieurs minutes.
Arrêter	L'arrêt d'IBM Security Network Protection Manager le met hors ligne et le rend inaccessible sur le réseau jusqu'à ce que vous le redémarriez.

4. Cliquez sur **OUI** pour redémarrer le système ou sur **NON** pour annuler l'opération.

Gestion des fichiers d'assistance

IBM Customer Support utilise des fichiers d'assistance pour vous aider à identifier et résoudre les problèmes d'IBM Security Network Protection Manager. Ces fichiers d'assistance contiennent tous les fichiers journaux, fichiers temporaires et intermédiaires ainsi que les résultats de commandes nécessaires au diagnostic des problèmes.

Pourquoi et quand exécuter cette tâche

Les fichiers d'assistance peuvent contenir des informations identifiables du client, telles que des adresses IP, des noms d'hôte, des noms d'utilisateur et des fichiers de règles. Ils ne contiennent pas d'informations confidentielles, telles que des mots de passe, des certificats et des clés. Tous les fichiers d'un fichier d'assistance contiennent du texte pouvant être contrôlé et censuré par le client.

Le contenu du fichier d'assistance est stocké au format de fichier compressé `.zip`.

Conseil :

- Vous pouvez créer plusieurs fichiers d'assistance pour effectuer un suivi d'un incident au fil du temps.

- Pour activer/désactiver la consignation du débogage :
  1. Cliquez sur **Journalisation de débogage** dans la page Fichiers d'assistance pour basculer entre **Activé** et **Désactivé**.
  2. Cliquez sur l'icône **Enregistrer les modifications** dans le coin inférieur droit de la fenêtre.

Procédure

1. Cliquez sur **Paramètres du système** dans le coin supérieur droit de la fenêtre.
2. s
3. Cliquez sur **Fichiers d'assistance** dans la sous-fenêtre Paramètres système sur le côté gauche de la fenêtre.
4. Effectuez l'une des tâches suivantes dans la page Fichiers d'assistance :

Option	Description
Nouveau	Pour créer un fichier d'assistance, cliquez sur **Nouveau**, entrez un commentaire décrivant le fichier d'assistance, puis cliquez sur **ENREGISTRER LA CONFIGURATION**. Un nouveau fichier d'assistance est créé sur le système.
Editer	Pour modifier le commentaire d'un fichier d'assistance, sélectionnez le fichier d'assistance, cliquez sur **Editer**, entrez un nouveau commentaire, puis cliquez sur **ENREGISTRER**.
Supprimer	Pour supprimer un fichier d'assistance, sélectionnez-le, puis cliquez sur **OUI**.
Télécharger	Pour télécharger des fichiers d'assistance, sélectionnez-les, puis cliquez sur l'icône **Télécharger**. Les fichiers d'assistance possèdent le suffixe `.support`. **Remarque :** Si vous téléchargez plusieurs fichiers d'assistance, ces derniers sont téléchargés au format de fichier compressé `.zip`.

Gestion des licences

La page Licence permet d'afficher et de gérer les licences d'IBM Security Network Protection Manager.

Pourquoi et quand exécuter cette tâche

Contactez votre représentant IBM pour obtenir un numéro d'enregistrement de licence. Vous pouvez télécharger et enregistrer votre licence à partir du centre d'enregistrement des licences IBM à l'adresse https://ibmss.flexnetoperations.com.

Procédure

1. Cliquez sur **Paramètres du système** dans le coin supérieur droit de la fenêtre.
2. Cliquez sur **Licence** dans la sous-fenêtre Paramètres système sur le côté gauche de la fenêtre.
3. Cliquez sur **Sélectionner** dans le coin supérieur droit de la page de gestion des licences, puis recherchez le fichier de licence à installer.
4. Sélectionnez le fichier de licence et cliquez sur **Ouvrir**.

Utilisation de l'interface de ligne de commande

L'interface de ligne de commande (CLI) permet aux administrateurs de gérer IBM Security Network Protection Manager.

Connexion à l'interface de ligne de commande

Vous pouvez vous connecter à l'interface de ligne de commande par l'intermédiaire de la console VMware ou d'une session SSH (Secure Shell). Vous devez utiliser des connexions sécurisées pour accéder à IBM Security Network Protection Manager.

Important : Lorsque vous vous connectez à IBM Security Network Protection Manager, le 6e échec de connexion consécutif déclenche un verrouillage. Une connexion réussie par tout utilisateur réinitialise le décompte des échecs de connexion et met fin au verrouillage.

Déconnexion de l'interface de ligne de commande

A l'invite de commande, entrez la commande exit pour vous déconnecter de l'interface de ligne de commande.

Affichage de l'aide de l'interface de ligne de commande

Pour afficher l'aide sur la syntaxe des commandes d'une catégorie spécifique, entrez Catégorie help.

La touche Tab permet également de compléter la syntaxe dans l'interface de ligne de commande. Depuis l'interface de ligne de ligne de commande, vous pouvez entrer une commande partielle et appuyer sur la touche Tab. En appuyant sur la touche Tab, vous complétez la commande ou affichez une liste des options permettant de compléter la syntaxe de la commande.

Commandes de l'interface de ligne de commande

L'interface de ligne de commande (CLI) fournit un ensemble limité de commandes pour contrôler et recevoir des réponses à partir du système IBM Security Network Protection Manager.

Commandes globales

Tableau 1. Commandes globales

Commande globale	Description
back	Revient au mode commande précédent.
exit	Se déconnecte du système.
help <*command*>	Affiche les informations sur l'utilisation de la commande spécifiée.
reboot	Réamorce le système.
shutdown	Arrête l'opération du système et met hors tension l'alimentation.
top	Revient au niveau supérieur.

Commandes de mode

Tableau 2. Commande de mode supérieur

Commandes de mode	Description
fips	Affiche l'état et les événements de FIPS 140-2.
firmware	Utilise des images de microprogramme.
fixpacks	Utilise des groupes de correctifs.
license	Utilise des licences.
management	Utilise des paramètres de gestion.
support	Utilise des fichiers d'installation des options.

Tableau 2. Commande de mode supérieur (suite)

Commandes de mode	Description
tools	Utilise des outils de diagnostic réseau.
updates	Utilise des mises à jour de sécurité.

Tableau 3. Commandes en mode microprogramme

Commande en mode microprogramme	Description
backup	Sauvegarde du microprogramme sur la partition principale vers la partition inactive.
get_comment [<*index*>]	Affiche le commentaire associé à une image du microprogramme.
get_info [<*index*>]	Affiche des informations de version associées à une image de microprogramme.
list	Liste les informations sur les images de microprogramme installées. Les informations de microprogramme comprennent l'image du microprogramme actif, une description du microprogramme, la date à laquelle le microprogramme a été installé, et des informations de sauvegarde facultatives.
set_comment [<*index*> [<*commentaire*> **...**]]	Remplace le commentaire associé à une image du microprogramme.
swap_active	Remplace l'image du microprogramme actif. Le système redémarre le système à l'aide de l'image du microprogramme inactif.

Tableau 4. Commandes en mode groupes de correctifs

Commande en mode groupes de correctifs	Description
install	Installe les groupes de correctifs disponibles à partir de la clé USB insérée.
list	Liste des groupes de correctifs disponibles sur la clé USB insérée.
rollback	Désinstalle le groupe de correctifs installé le plus récemment.
view_history	Affiche l'historique d'installation pour tous les groupes de correctifs.

Tableau 5. Commande en mode licence

Commande en mode licence	Description
install	Installe un fichier de licence à partir d'une clé USB insérée.
list	Liste les fichiers de licence disponibles sur la clé USB insérée.
show	Affiche les informations sur la licence active actuellement.

Tableau 6. Commandes en mode gestion

Commande en mode gestion	Description
database	Utilise les paramètres de la base de données. Les commandes suivantes sont disponibles pour **database** : • **set** *nom_base_données* : configure la base de données. • **set_password** : définit le mot de passe de base de données. • **show** : affiche les paramètres de base de données. • **test** : teste la connexion à la base de données.
dns	Utilise les paramètres du système DNS. Les commandes suivantes sont disponibles pour **dns** : • **set** [*dns*] : définit le DNS du système. • **show** : affiche le DNS du système.
hostname	Utilise le nom d'hôte du système. Les commandes suivantes sont disponibles pour **hostname**: • **set** [*nom_hôte*] : définit le nom d'hôte du système. • **show** : affiche le nom d'hôte du système.
interfaces	Utilise les paramètres de l'interface de gestion. Les commandes suivantes sont disponibles pour les interfaces : • **list** : répertorie les interfaces de gestion sur le système. • **set** [*nom-interface*] : définit la configuration de réseau pour une interface de gestion. • **show** [*nom-interface*] : affiche la configuration d'une interface réseau de gestion.
set_password	Définit le mot de passe du système.
time	Utilise les paramètres de l'heure, de la date et du fuseau horaire. Les commandes suivantes sont disponibles pour les interfaces : • **date** : change la date. • **show** : affiche la configuration de l'heure. • **time** : change l'heure. • **timezone** : modifie le fuseau horaire.

Tableau 7. Commandes en mode prise en charge

Commande en mode prise en charge	Description
create [<*commentaire*> ...]	Crée un fichier d'installation des options.
delete [<*index*>]	Supprime un fichier d'installation des options.
download [<*index*>]	Télécharge un fichier d'installation des options sur une clé USB.
get_comment [<*index*>]	Affiche le commentaire associé à un fichier d'installation des options.

Tableau 7. Commandes en mode prise en charge (suite)

Commande en mode prise en charge	Description
list	Liste les fichiers d'installation des options.
set_comment [<*index*> [<*commentaire*> ...]]	Remplace le commentaire associé au un fichier d'installation des options.

Tableau 8. Commande en mode outils

Commande en mode outils	Description
connections	Affiche les connexions réseau du système.
nslookup [<*hôte*>] [<*serveur*>]	Interroge les serveurs de noms de domaine Internet.
ping [-c <*nombre*>] [-s <*taille*>] <*hôte*>	Envoie une demande ICMP ECHO_REQUEST aux hôtes du réseau. **Remarque :** Le nombre doit être compris entre 0 et 5535. Si le nombre est 0, le système envoie des commandes PING ICMP ECHO_REQUEST jusqu'à ce qu'il soit interrompu par l'utilisateur à l'aide de la commande de clavier Ctrl+C. Le nombre par défaut est 0. La taille doit être comprise entre 0 et 65535. La taille par défaut est de 56 octets.
traceroute [-6] <*hôte*> [<*taille*>]	Trace un paquet depuis un ordinateur vers une destination distante, indiquant le nombre de tronçons nécessaire pour que le paquet atteigne la destination et la durée de chaque tronçon. **Remarque :** La taille doit être comprise entre 38 et 32768. La taille par défaut est de 38 octets.

Tableau 9. Commande en mode mises à jour

Commande en mode mises à jour	Description
install[<index>[usb|server]]	Installation d'une mise à jour à partir de la clé USB insérée ou d'un serveur de mises à jour. **Remarque :** La commande clavier Ctrl + C n'interrompt pas la commande **install** en mode mise à jour.
list[<index>[usb|server]]	Répertorie les mises à jour disponibles sur le lecteur flash USB inséré ou sur le serveur de mise à jour.
rollback	Annule une mise à jour de sécurité. **Remarque :** La commande clavier Ctrl + C n'interrompt pas la commande **rollback** en mode de mise à jour.
show	Affiche les informations de version pour la mise à jour de sécurité actuellement installée.
view_history	Affichage de l'historique d'installation et d'annulation pour toutes les mises à jour.

Chapitre 4. Administration

Informations et tâches à effectuer pour utiliser et gérer IBM Security Network Protection Manager.

Recherche dans IBM Security Network Protection Manager

IBM Security Network Protection Manager intègre une barre de recherche dans la partie supérieure centrale de la fenêtre d'application.

Pourquoi et quand exécuter cette tâche

La barre de recherche peut être utilisée pour rechercher des agents, des règles, des signatures ou toutes combinaisons de ces mots clés. Vous pouvez affiner une recherche avec plusieurs facettes des entités stockées dans IBM Security Network Protection Manager.

Procédure

1. Entrez la chaîne de recherche dans la barre de recherche. Vous pouvez entrer des chaînes partielles ou complètes.
2. Les résultats correspondants sont immédiatement affichés à mesure que vous saisissez les chaînes de recherche.
3. Utilisez les filtres à facettes du panneau de gauche pour affiner vos résultats.
   - Agents : Modèle, Statut de mise à jour, Version XPU, Dernier redémarrage, Microprogramme, Statut, Performances, Santé.
   - Règles : Type de référentiel, Type de règle, Référentiel, Date de modification, Microprogramme applicable.
   - Signatures (règle d'événement de prévention contre les intrusions) : Type, Niveau de protection, Niveau de menace, Version XPU.
4. Affinez votre recherche en effectuant les étapes suivantes :
   - Modifiez vos chaînes de recherche.
   - Cliquez sur la croix (X) en regard d'un filtre pour le supprimer de la zone **Filtrage par**.
5. Cliquez sur le résultat pour afficher les détails récapitulatifs.

Editer en un clic

Le bouton Editer en un clic permet de configurer rapidement l'état de protection contre une menace et de déployer les objets IPS (système de prévention contre les intrusions) mis à jour sur les agents IBM Security Network Protection (XGS).

Pourquoi et quand exécuter cette tâche

Le bouton **EDITER EN UN CLIC** est disponible dans la sous-fenêtre des détails récapitulatifs des résultats de recherche liés aux signatures IPS.

Remarque : Les agents IBM Security Network Protection (XGS) n'appliqueront pas l'objet IPS mis à jour tant que le prochain signal de présence ne s'est pas connecté à IBM Security SiteProtector System.

Procédure

1. Entrez des chaînes de recherche (nom ou CVE) pour rechercher une signature dans la barre de recherche.
2. Cliquez sur le résultat pour afficher les détails récapitulatifs.

3. Cliquez sur **EDITER EN UN CLIC** dans la partie inférieure de la page pour éditer les règles de prévention contre les intrusions de la signature sélectionnée.
4. Cliquez sur l'icône en forme d'oeil pour basculer entre les états "Activé" et "Désactivé".
5. Cliquez sur l'icône de bouclier ou de flèche pour basculer entre les états "Bloqué" et "Autoriser".
6. Un libellé "Modifications non enregistrées" indique que les modifications apportées ne sont ni enregistrées, ni appliquées.
7. Cliquez sur l'icône **Enregistrer les modifications** dans le coin inférieur droit de la page, puis entrez des commentaires dans la fenêtre Editer le commentaire.
8. Dans la fenêtre Editer le commentaire, cliquez sur **Enregistrer**.

Objets IPS

Les règles IBM Security Network Protection Intrusion Prevention contiennent des objets IPS. Chaque objet IPS contient la configuration de chaque signature y compris l'état de la signature et sa mise en application.

Les résultats des objets IPS identifient les états activé et blocage actuels pour le contrôle de sécurité au sein de l'objet IPS spécifique. L'objet IPS par défaut contient tous les événements de sécurité configurés par Equipe de recherche et développement IBM X-Force avec des paramètres et des réponses spécifiques permettant d'assurer une protection contre un grand nombre de menaces. Vous pouvez remplacer l'état de signature (activé ou désactivé) et les états de mise en application (bloqué ou autorisé) pour des objets IPS individuels.

Paramètres X-Force par défaut

Les paramètres X-Force par défaut permettent d'analyser le niveau de protection du réseau.

Les événements de sécurité d'une mise à jour X-Press (XPU) incluent un grand nombre de paramètres X-Force par défaut : **Activer**, **Niveau des menaces** et **Bloc**. Le paramètre **Activer** permet d'indiquer si l'événement de sécurité analyse le trafic. Le niveau des menaces est indiqué comme étant élevé, moyen, faible ou par défaut (reportez-vous à la rubrique «Descriptions du niveau des menaces»). X-Force configure les événements de sécurité avec la réponse de blocage pour assurer la protection contre une attaque ou un audit. Pour bloquer, le système supprime les paquets suspects et envoie des réinitialisations aux connexions TCP.

Savoir de quelle façon X-Force assure la protection contre les attaques et les audits permet d'analyser le niveau de sécurité réseau.

- Recherchez les attaques et les audits configurés par X-Force pour être **bloqués**.
- Evaluez le niveau de protection actif et étendez ce niveau de protection aux événements de sécurité connus pour résulter en des faux positifs.
- Comparez les informations X-Force relatives aux événements de sécurité avec les informations système relatives aux vulnérabilités et expositions communes (CVE). Pour plus d'informations, reportez-vous à la rubrique «Numéros CVE», à la page 23.
- Comparez les recommandations X-Force par défaut avec les autres solutions de sécurité en termes de précision.

Descriptions du niveau des menaces

Il est utile de savoir ce que signifient les niveaux de menace élevé, moyen et bas lorsque la gestion des événements de sécurité.

Le niveau de menace **Par défaut** est le niveau affecté par Equipe de recherche et développement IBM X-Force à l'événement de sécurité. Vous pouvez modifier ce paramètre sur élevé, moyen ou bas pour répondre aux besoins de votre réseau.

Niveau	Description
Elevé	Problèmes de sécurité permettant un accès immédiat à distance ou local, ou l'exécution immédiate de code ou de commandes, avec des droits non autorisés. **Exemples :** La plupart des dépassements de mémoire tampon, portes dérobées, mots de passe par défaut ou inexistants, et le contournement de la sécurité sur les pare-feux ou autres composants réseau
Moyen	Problèmes de sécurité ayant le potentiel d'accorder l'accès ou d'autoriser l'exécution de code avec des procédures d'utilisation complexes ou longues. Ces problèmes peuvent être à faible risque pour les principaux composants Internet. **Exemples :** Script intersite, attaques de l'homme du milieu, injection SQL, refus de service des principales applications, et saturation résultant de la divulgation d'informations système (telles que des fichiers core)
Faible	Problèmes de sécurité qui refusent un service ou fournissent des informations non liées au système, pouvant être utilisées pour formuler des attaques structurées sur une cible, mais ne gagnant pas directement un accès non autorisé. **Exemples :** Attaques par force brute, révélation d'informations non liées au système (telles que configurations et chemins) et attaque par saturation

Numéros CVE

Certains événements de sécurité X-Force correspondent à un numéro CVE (vulnérabilités et expositions communes).

Les numéros CVE permettent d'identifier les vulnérabilités et les expositions communes. La MITRE Corporation affecte les numéros CVE et conserve des enregistrements des événements dans le système CVE. Vous pouvez interroger ce système à l'aide des numéros CVE afin de rechercher des informations sur ces événements. Pour plus d'informations sur le système, consultez le site Web CVE à l'adresse http://cve.mitre.org/.

Les relations entre les événements de sécurité et les numéros CVE sont les suivantes :

- Plusieurs événements de sécurité peuvent avoir le même numéro CVE. La vulnérabilité associée au numéro CVE peut correspondre à des modèles de plusieurs événements de sécurité.
- Certains événements de sécurité peuvent ne pas avoir de numéro CVE pour les raisons suivantes :
  - La vulnérabilité associée à l'événement de sécurité est nouvelle et le système CVE de la MITRE Corporation ne comporte pas d'événement pour cette vulnérabilité ou cette exposition.
  - La vulnérabilité associée à l'événement de sécurité n'est liée à aucune vulnérabilité ou exposition répertoriée dans le système CVE.
  - La menace identifiée par l'événement de sécurité n'est liée à aucune vulnérabilité ou exposition.

Exemples d'utilisation des fonction de recherche et d'édition en un clic

Exemples d'utilisation des recherches avancées et du filtrage à facettes dans IBM Security Network Protection Manager.

Recherche des signatures d'audit X-Force

Dans une organisation où sont installés plusieurs dispositifs IBM Security Network Protection (XGS) qui protègent différents sites et segments de réseau, l'administrateur de la sécurité souhaite exploiter les signatures d'audit X-Force pour désactiver toutes les connexions SSLv3 entrantes et sortantes des serveurs critiques. Les étapes suivantes sont effectuées par l'administrateur pour accomplir cette tâche :

1. Entrez SSLv3 dans la barre de recherche pour rechercher rapidement la signature "SSLv3_In_Use".
2. Cliquez sur la signature **SSLv3_In_Use** pour afficher ses détails récapitulatifs.
3. Cliquez sur **EDITER EN UN CLIC** pour afficher le statut actuel des règles d'objet IPS.
4. Cliquez sur les filtres de référentiel dans la sous-fenêtre de gauche et recherchez les règles déployées sur les dispositifs XGS.
5. Activez la signature, changez son comportement en "bloquer", puis déployez la règle.
6. Le dispositif XGS applique la nouvelle règle et bloque le trafic des connexions SSLv3 entrantes et sortantes des serveurs critiques.

Recherche d'une règle récemment déployée

Un administrateur de la sécurité souhaite rechercher une règle d'accès réseau récemment déployée et effectue pour cela la tâche suivante :

1. Cliquez sur le filtre **Règles** > **Type de règle** dans la sous-fenêtre de gauche pour filtrer et rechercher les règles déployées sur les dispositifs XGS.
2. Cliquez sur **Accès au réseau** dans la sous-fenêtre de gauche pour affiner les résultats de la recherche.
3. Entrez une chaîne de recherche (par exemple, le commentaire "révision 15") afin d'affiner davantage les résultats de la recherche.

Affichage des notifications

Les notifications d'IBM Security Network Protection Manager sont accessibles en cliquant sur l'icône d'enveloppe, dans le coin supérieur droit de la page. Le nombre inscrit dans l'icône indique le nombre de notifications non lues. Les notifications sont répertoriées dans l'ordre chronologique inverse, en commençant par la plus récente.

Pourquoi et quand exécuter cette tâche

Vous pouvez afficher les notifications avec des filtres à facettes.

Procédure

1. Cliquez sur l'icône **Accéder aux notifications**  dans le coin supérieur droit de la page.
2. Vous pouvez filtrer la vue des notifications en cliquant sur l'une des options suivantes :
   - Type
   - Gravité
   - Etat
   - Agent
3. Les notifications non lues sont indiquées par le libellé **Nouveau**. Cliquez sur une notification non lue pour désactiver le libellé **Nouveau** et changer la pondération textuelle de la description de caractère gras à normal.

Remarques

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Ce document peut être disponible dans d'autres langues auprès d'IBM. Toutefois, une copie du produit ou de la version du produit dans cette langue peut être nécessaire pour y accéder.

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial IBM. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM. Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM.

IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous accorde aucun droit de licence sur ces brevets ou demandes de brevet. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Les informations sur les licences concernant les produits utilisant un jeu de caractères double octet peuvent être obtenues par écrit auprès d'IBM à l'adresse suivante :

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

LE PRESENT DOCUMENT EST LIVRE "EN L'ETAT" SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut, à tout moment et sans préavis, modifier les produits et logiciels décrits dans ce document.

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit IBM et l'utilisation de ces sites Web relève de votre seule responsabilité.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Ces informations peuvent être soumises à des conditions particulières, prévoyant notamment le paiement d'une redevance.

Le logiciel sous licence décrit dans ce document et tous les éléments sous licence disponibles s'y rapportant sont fournis par IBM conformément aux dispositions de l'ICA (Contrat sur les produits et services IBM), des Conditions internationales d'utilisation des logiciels IBM ou de tout autre accord équivalent.

Les données de performance et les exemples client ne sont présentés qu'à des fins d'illustration. Les performances réelles peuvent varier en fonction des configurations et des conditions d'exploitation.

Les informations concernant des produits non IBM ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via d'autres sources disponibles. IBM n'a pas testé ces produits et ne peut confirmer l'exactitude de leurs performances ni leur compatibilité. Elle ne peut recevoir aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits non IBM doit être adressée aux fournisseurs de ces produits.

Les instructions relatives aux intentions d'IBM pour ses opérations à venir sont susceptibles d'être modifiées ou annulées sans préavis, et doivent être considérées uniquement comme des objectifs.

Ces informations sont fournies uniquement à titre de planification. Elles sont susceptibles d'être modifiées avant la mise à disposition des produits décrits.

Le présent document peut contenir des exemples de données et de rapports utilisés couramment dans l'environnement professionnel. Ces exemples mentionnent des noms fictifs de personnes, de sociétés, de marques ou de produits à des fins illustratives ou explicatives uniquement. Toute ressemblance avec des noms de personnes, de sociétés ou des données réelles serait purement fortuite.

LICENCE DE COPYRIGHT :

Le présent document contient des exemples de programmes d'application en langue source destinés à illustrer les techniques de programmation sous différentes plateformes d'exploitation. Vous avez le droit de copier, de modifier et de distribuer ces exemples de programme sous quelque forme que ce soit et sans paiement d'aucune redevance à IBM, à des fins de développement, d'utilisation, de vente ou de distribution de programmes d'application conformes aux interfaces de programmation des plateformes pour lesquels ils ont été écrits ou aux interfaces de programmation IBM. Ces exemples de programmes n'ont pas été rigoureusement testés dans toutes les conditions. Par conséquent, IBM ne peut garantir expressément ou implicitement la fiabilité, la maintenabilité ou le fonctionnement de ces programmes. Les exemples de programme sont fournis "EN L'ETAT", sans garantie d'aucune sorte. IBM ne sera en aucun cas responsable de tout dommage résultant de votre utilisation de ces programmes.

Marques

IBM, le logo IBM et ibm.com sont des marques d'International Business Machines dans de nombreux pays. D'autres noms de services et de produits peuvent être des marques d'IBM ou d'autres sociétés. La liste actualisée de toutes les marques d'IBM est disponible dans la page Web "Copyright and trademark information" à l'adresse www.ibm.com/legal/copytrade.shtml.

Dispositions relatives à la documentation du produit

Les droits d'utilisation relatifs à ces publications sont soumis aux dispositions suivantes :

Conditions d'utilisation

Ces dispositions s'ajoutent à celles applicables au site Web d'IBM.

Usage personnel

Vous pouvez reproduire ces publications pour votre usage personnel, non commercial, sous réserve que toutes les mentions de propriété soient conservées. Vous ne pouvez distribuer ou publier tout ou partie de ces publications ou en faire des oeuvres dérivées sans le consentement exprès d'IBM.

Usage commercial

Vous pouvez reproduire, distribuer et afficher ces publications uniquement au sein de votre entreprise, sous réserve que toutes les mentions de propriété soient conservées. Vous ne pouvez reproduire, distribuer, afficher ou publier tout ou partie de ces publications en dehors de votre entreprise, ou en faire des oeuvres dérivées, sans le consentement exprès d'IBM.

Autorisations

Sauf autorisation expresse, aucun autre droit, autorisation ou licence n'est accordé de façon explicite ou implicite aux publications ou à toute information, donnée ou tout logiciel ou autre propriété intellectuelle contenu dans ces publications.

IBM se réserve le droit de retirer les autorisations accordées ici si, à sa discrétion, l'utilisation des publications s'avère préjudiciable à ses intérêts ou si, selon son appréciation, les instructions susmentionnées n'ont pas été respectées.

Vous ne pouvez télécharger, exporter ou réexporter ces informations qu'en total accord avec toutes les lois et règlements applicables dans votre pays, y compris les lois et règlements américains relatifs à l'exportation.

IBM N'ACCORDE AUCUNE GARANTIE SUR LE CONTENU DE CES PUBLICATIONS. LES PUBLICATIONS SONT LIVREES "EN L'ETAT" SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE.

Index