IBM Security

IBM Security SiteProtector System Guide d'installation

Version 3.0

Important
Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à la section «Mentions légales», à la page 71.

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.

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.can.ibm.com (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

Cette édition s'applique à la version 3.0 de IBM Security SiteProtector System et à toutes les versions et modifications suivantes, sauf indication contraire dans les nouvelles éditions.

Table des matières

Avis aux lecteurs canadiens

Le présent document a été traduit en France. Voici les principales différences et particularités dont vous devez tenir compte.

Illustrations

Les illustrations sont fournies à titre d'exemple. Certaines peuvent contenir des données propres à la France.

Terminologie

La terminologie des titres IBM peut différer d'un pays à l'autre. Reportez-vous au tableau ci-dessous, au besoin.

IBM France	IBM Canada
ingénieur commercial	représentant
agence commerciale	succursale
ingénieur technico-commercial	informaticien
inspecteur	technicien du matériel

Claviers

Les lettres sont disposées différemment : le clavier français est de type AZERTY, et le clavier français-canadien de type QWERTY.

OS/2 et Windows - Paramètres canadiens

Au Canada, on utilise :

- les pages de codes 850 (multilingue) et 863 (français-canadien),
- le code pays 002,
- le code clavier CF.

Nomenclature

Les touches présentées dans le tableau d'équivalence suivant sont libellées différemment selon qu'il s'agit du clavier de la France, du clavier du Canada ou du clavier des États-Unis. Reportez-vous à ce tableau pour faire correspondre les touches françaises figurant dans le présent document aux touches de votre clavier.

France	Canada	Etats-Unis
(Pos1)		Home
Fin	Fin	End
(PgAr)		PgUp
(PgAv)		PgDn
Inser	Inser	Ins
Suppr	Suppr	Del
Echap	Echap	Esc
Attn	Intrp	Break
Impr écran	ImpEc	PrtSc
Verr num	Num	Num Lock
Arrêt défil	Défil	Scroll Lock
(Verr maj)	FixMaj	Caps Lock
AltGr	AltCar	Alt (à droite)

Brevets

Il est possible qu'IBM détienne des brevets ou qu'elle ait déposé des demandes de brevets portant sur certains sujets abordés dans ce document. Le fait qu'IBM vous fournisse le présent document ne signifie pas qu'elle vous accorde un permis d'utilisation de ces brevets. Vous pouvez envoyer, par écrit, vos demandes de renseignements relatives aux permis d'utilisation au directeur général des relations commerciales d'IBM, 3600 Steeles Avenue East, Markham, Ontario, L3R 9Z7.

Assistance téléphonique

Si vous avez besoin d'assistance ou si vous voulez commander du matériel, des logiciels et des publications IBM, contactez IBM direct au 1 800 465-1234.

A propos de ce document

Ce document fournit les informations dont vous avez besoin pour installer IBM® Security SiteProtector System.

Public visé

Ce guide s'adresse aux administrateurs réseau et aux administrateurs de sécurité ou à toute autre personne chargée de l'installation de SiteProtector System et de la gestion de la sécurité du réseau. Pour utiliser ce guide, vous devez être familiarisé avec les périphériques réseau, y compris la configuration des pare-feux et des proxy, ainsi que la configuration des bases de données Microsoft SQL.

Prérequis et informations associées

Avertissement : Ce produit n'est pas conçu pour être connecté directement ou indirectement d'aucune façon à des interfaces de réseaux de télécommunications publics.

本製品は、電気通信事業者の通信回線への直接、またはそれに準ずる方法での接続を目的とするものではありません。

Le tableau suivant présente les documents SiteProtector à utiliser pour configurer SiteProtector System après son installation :

Document	Contenu
IBM Security SiteProtector System - Guide de configuration	Contient des informations sur la configuration, la mise à jour et la maintenance de SiteProtector
IBM Security SiteProtector System Policies and Responses Configuration Guide	Contient des informations sur la configuration des politiques et des réponses, y compris les réponses Central Responses
IBM Security SiteProtector System - Configuration de pare-feu pour le trafic SiteProtector	Contient des informations pour qu'un gestionnaire Security Manager puisse configurer des pare-feux de sorte que les périphériques réseau et les composants de SiteProtector System puisssent communiquer entre eux.
IBM Security SiteProtector System User Guide for Security Analysts	Contient des informations permettant à un analyste de la sécurité de gérer les politiques et les réponses de SiteProtector System
IBM Security SiteProtector Information Center (Aide)	Contient toutes les procédures nécessaires pour utiliser SiteProtector, y compris les procédures avancées qui ne figurent pas forcément dans un document utilisateur imprimé

Localisez tous les documents SiteProtector au format PDF (Portable Document Format) à l'emplacement suivant :

- Centre de documentation des produits d'IBM Security.

Chapitre 1. Introduction à SiteProtector

Le système IBM Security SiteProtector est un système de gestion centralisée qui unifie la gestion et l'analyse du réseau, du serveur et des agents Desktop Endpoint Security, ainsi que des dispositifs ou des réseaux de petite taille. Vous pouvez facilement adapter SiteProtector pour assurer la sécurité dans des environnements de grande taille à l'échelle d'une entreprise.

SiteProtector fournit les commandes, le contrôle et les fonctions de surveillance pour tous vos produits IBM Security.

Terminologie associée à SiteProtector

La documentation de SiteProtector utilise une terminologie spécifique.

Termes utilisés pour les produits de sécurité dans ce document.

Terme	Description
agent	Terme générique pour tous les dispositifs, les scanners et les détecteurs réseau, serveur et de bureau.
dispositif	Périphérique de sécurité en ligne sur un réseau ou une passerelle. Selon son type, le dispositif peut fournir toute combinaison de fonctions de détection et de prévention d'intrusion, d'antivirus, d'antispam, de réseau privé virtuel, de filtrage sur le Web et de pare-feu.
scanneur	Agent qui analyse les actifs à la recherche de vulnérabilités et autres risques de sécurité
détecteur	Agent qui surveille le trafic rsur le réseau et sur les serveurs pour identifier les attaques et les stopper si besoin est.

Architecture de SiteProtector

L'architecture de SiteProtector se prête à une installation sur plusieurs ordinateurs.

Présentation des composants d'un site SiteProtector.

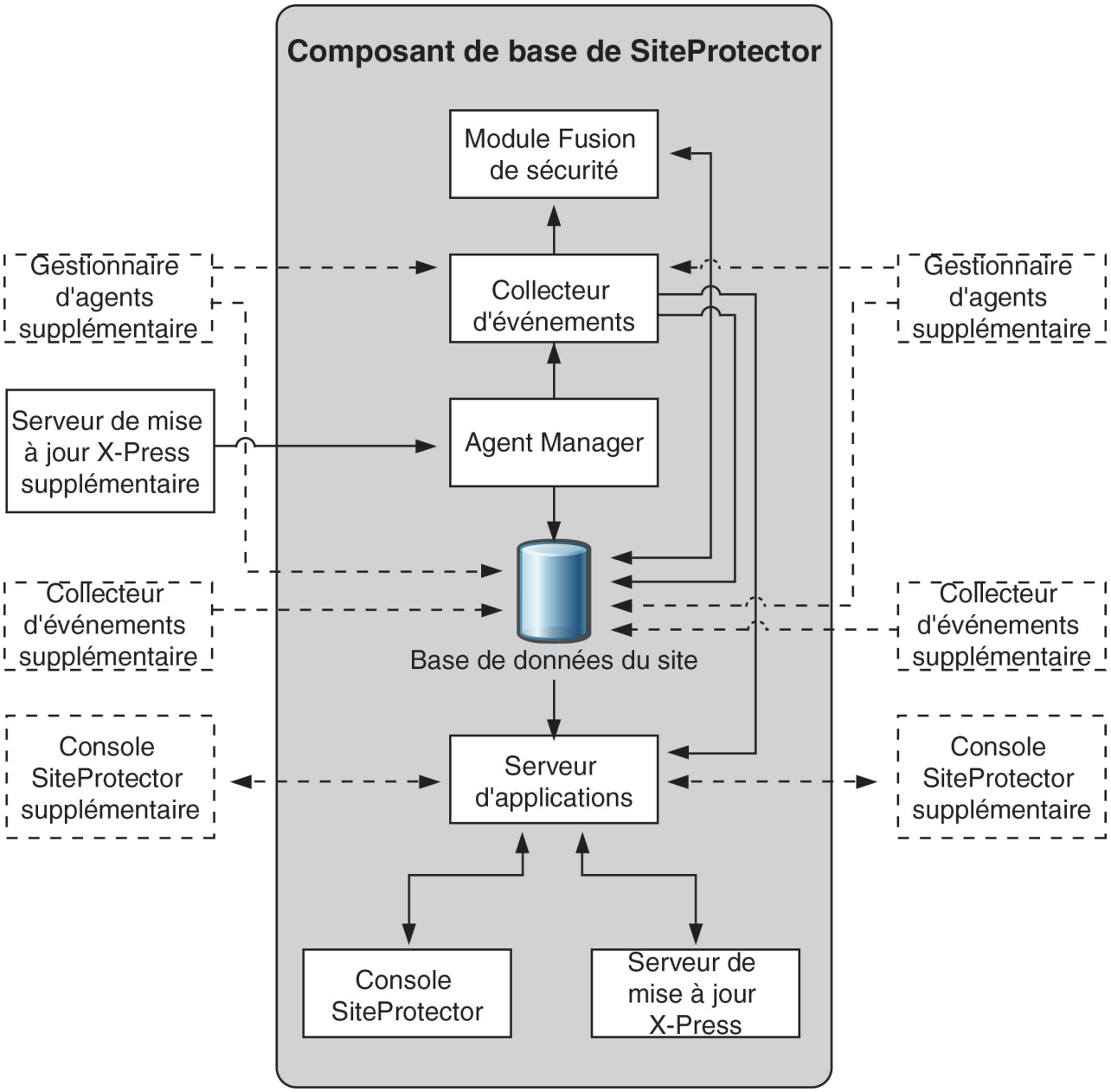

Figure 1. Composants d'un site standard

Canaux de communication

Les composants du système SiteProtector ont recours à des canaux spécifiques pour communiquer entre eux et avec d'autres produits IBM Security. Pour obtenir une liste complète des ports utilisés pour la communication, voir le document *Configuring Firewalls for SiteProtector System Traffic* disponible à l'adresse http://pic.dhe.ibm.com/infocenter/sprotect/v2r8m0/index.jsp?topic=%2Fcom.ibm.siteprotector.doc%2Fpdfs%2Fsp_printable_pdfs.htm.

Composants de SiteProtector

Le système SiteProtector comprend de nombreux composants.

Composant de SiteProtector	Description
Agent Manager	Agent Manager gère les activités de commande et de contrôle des agents Desktop Endpoint Security et des dispositifs d'IBM Security. Agent Manager facilite également le transfert des données des agents vers le composant Event Collector. Agent Manager permet à SiteProtector de collecter et gérer les données des agents et des composants. Agent Manager est installé avec les options Express et Recommended.
Console	La console SiteProtector est l'interface utilisateur principale de SiteProtector. Vous effectuez la plupart des fonctions de SiteProtector, telles que la surveillance des événements, la planification des analyses, la génération de rapport et la configuration des agents sur la console.
Event Archiver	Event Archiver stocke les données d'événements et permet d'améliorer les performances en réduisant le nombre d'événements que la base de données Site Database doit stocker.
Event Collector	Event Collector gère les événements en temps réel à partir des détecteurs et des données de vulnérabilité des programmes d'analyse.
Event Viewer (facultatif)	SiteProtector Event Viewer reçoit les événements non traités du composant Event Collector pour fournir l'accès quasiment en temps réel aux données de sécurité afin d'identifier et résoudre les incidents.
Module SecurityFusion	Le module SecurityFusion augmente votre capacité à identifier et répondre rapidement aux menaces critiques sur votre site. A l'aide de techniques d'analyse avancées, le module SecurityFusion fait remonter les attaques à fort impact afin que vous puissiez vous concentrer sur les menaces les plus importantes.
Site Database	La base de données de SiteProtector (Site Database) stocke les données d'agent brutes, les indicateurs d'occurrences (statistiques pour les événements de sécurité déclenchés par les agents), les informations de groupe, les données de contrôle et de commande, ainsi que le statut des mises à jour X-Press (XPU).
Rapports SiteProtector	les rapports de conformité et les rapports récapitulatifs graphiques fournissent les informations nécessaires aux responsables pour évaluer l'état de leur sécurité. Les rapports couvrent l'évaluation des vulnérabilités, les attaques, l'audit, le filtrage de contenu, l'activité de Desktop Endpoint Security, du module SecurityFusion et des virus.
Noyau SP	Le noyau SP inclut les composants suivants : • Le serveur d'applications (Application Server) qui permet la communication entre la console SiteProtector et la base de données Site Database. • Le contrôleur d'agent (Agent Controller) qui gère les activités de commande et de contrôle des agents, telles que la commande pour lancer ou arrêter la collecte des événements. • X-Press Update Server qui est un serveur Web qui stocke les mises à jour X-Press (XPU) après leur téléchargement à partir d'IBM Download Center et les met à disposition des agents et des composants du réseau. Ce serveur de mises à jour évite d'avoir à télécharger les mises à jour de produits similaires plusieurs fois et permet aux utilisateurs de gérer le processus de mise à jour de manière plus efficace. • SiteProtector Web Access est une interface en lecture seule qui permet d'accéder facilement à SiteProtector pour surveiller les actifs d'événement SiteProtector et les événements de sécurité.

Composant de SiteProtector	Description
X-Press Update Server	X-Press Update Server est un serveur Web qui stocke les mises à jour X-Press (XPU) après leur téléchargement à partir d'IBM Download Center et les met à la disposition des agents et des composants du réseau. Ce serveur de mises à jour évite d'avoir à télécharger les mises à jour de produits similaires plusieurs fois et permet aux utilisateurs de gérer le processus de mise à jour de manière plus efficace.

Composant complémentaire

Un composant complémentaire de SiteProtector fournit des fonctions et une protection supplémentaires.

Remarque : Le composant complémentaire décrit ici est une fonction sous licence séparée disponible dans SiteProtector.

SiteProtector SecureSync Failover

La fonction SiteProtector SecureSync Failover fournit à l'utilisateur des informations sur la configuration de SiteProtector pour effectuer une reprise en ligne et récupérer SiteProtector après une panne totale.

Chapitre 2. Configuration matérielle et logicielle requise

Chaque composant d'IBM Security SiteProtector System comporte une configuration matérielle et logicielle requise spécifique.

Les tableaux des rubriques relatives à la configuration requise de cette section incluent des entrées pour les configurations suivantes :

- **Base de référence SiteProtector** fait référence aux conditions requises pour le système SiteProtector principal.
- **Support XGS** fait référence aux conditions requises pour la modification de règles pour les dispositifs IBM Security Network Protection. Cette modification des règles nécessite Internet Explorer v9 et au-delà, qui est pris en charge uniquement par des systèmes d'exploitation Microsoft spécifiques.
- **Support SP800-131A** fait référence aux conditions requises pour le chiffrement strict (SP800-131A) tel qu'il est défini par National Institute of Standards and Technology (NIST). Le chiffrement strict nécessite le protocole TLS (Transport Layer Security) v1.2 qui est pris en charge uniquement par Internet Explorer v8 et au-delà. Seuls des systèmes d'exploitation Microsoft spécifiques prennent en charge Internet Explorer v8 et au-delà.

Important : L'installation de certains composants de SiteProtector nécessite une dénomination courte de type 8dot3 dans les paramètres de registre du système de fichiers Windows. Si vous avez désactivé les noms courts dans les paramètres de registre sur les serveurs sur lesquels vous envisagez d'installer les composants SiteProtector, vous devez les réactiver avant d'installer SiteProtector.

Remarque : Le système SiteProtector ne prend pas en charge le système ReFS (Resilient File System) disponible avec Windows Server 2012 Standard.

Configuration système requise pour le support de virtualisation (VMware)

Le tableau suivant décrit la configuration système requise pour la virtualisation :

Composant	Configuration minimale requise
Virtualisation	• VMware ESX 4.x ou ESXi 4.x ou 5.x • Microsoft Windows Server 2008 Hyper-V • Microsoft Virtual Server 2005

Remarque : Tous les composants de SiteProtector peuvent être installés dans un environnement virtuel, à condition que les machines virtuelles respectent la configuration requise décrite dans «Configuration requise pour l'installation Express de SiteProtector», à la page 6.

Configuration requise pour le chiffrement Strict (SP800-131A)

Le chiffrement strict (SP800-131A) nécessite le protocole TLS (Transport Layer Security) v1.2 qui est pris en charge uniquement par Internet Explorer 8 et les versions ultérieures. Seuls certains systèmes d'exploitation prennent en charge Internet Explorer 8 et les versions ultérieures.

Pour utiliser le chiffrement strict, Internet Explorer doit être configuré pour prendre en charge TLS 1.2.

Pour utiliser le chiffrement strict, vous devez configurer IPsec pour la base de données SiteProtector. Reportez-vous à la tâche associée répertoriée ci-dessous pour plus de détails.

Pour obtenir les exigences spécifiques, reportez-vous à la colonne **SP800-131A Support** des tableaux des rubriques relatives à la configuration requise dans cette section.

Configuration requise pour l'installation Express de SiteProtector

L'installation Express de SiteProtector constitue la configuration de déploiement minimale prise en charge par le système SiteProtector. Elle installe tous les composants de SiteProtector sur un seul ordinateur. Il s'agit de l'installation la plus adaptée aux réseaux de petite taille et aux environnements de test.

Le tableau suivant décrit la configuration requise pour l'installation Express et inclut des entrées pour les configurations suivantes :

- **Base de référence SiteProtector** fait référence aux conditions requises pour le système SiteProtector principal.
- **Support XGS** fait référence aux conditions requises pour la modification de règles pour les dispositifs IBM Security Network Protection. Cette modification des règles nécessite Internet Explorer v9 et au-delà, qui est pris en charge uniquement par des systèmes d'exploitation Microsoft spécifiques.
- **Support SP800-131A** fait référence aux conditions requises pour le chiffrement strict (SP800-131A) tel qu'il est défini par National Institute of Standards and Technology (NIST). Le chiffrement strict nécessite le protocole TLS (Transport Layer Security) v1.2 qui est pris en charge uniquement par Internet Explorer v8 et au-delà. Seuls des systèmes d'exploitation Microsoft spécifiques prennent en charge Internet Explorer v8 et au-delà.

Composant	Configuration minimale requise	Base de référence SP	Support XGS	Support SP800-131A*
Processeur	Xeon 3000 Series ou Core 2 Duo (minimum) Intel Xeon E5540 2,53 GHz (recommandé)	✓	✓	✓
Système d'exploitation SiteProtector prend en charge les versions 32 et 64 bits des systèmes d'exploitation Windows. Les systèmes 64 bits uniquement sont indiqués. **Remarque :** Vous devez exécuter SiteProtector et ses composants sur une partition NTFS. Les partitions FAT et FAT32 ne permettent pas de renforcer la sécurité de votre système correctement.	Windows Server 2012 Standard[1] (64 bits uniquement)	✓	✓	✓

Composant	Configuration minimale requise	Base de référence SP	Support XGS	Support SP800-131A*
	Windows Server 2008 R2 Standard (64 bits uniquement)	✓	✓	✓
	Windows Server 2008 R2 Enterprise (64 bits uniquement)	✓	✓	✓
	Windows Server 2008 Standard	✓	✓	
	Windows Server 2008 Enterprise	✓	✓	
	Windows Server 2003 R2 Standard	✓		
	Windows Server 2003 R2 Enterprise	✓		
	Windows Server 2003 SP2 Standard	✓		
	Windows Server 2003 SP2 Enterprise	✓		
Mémoire RAM	2 Go (minimum) 8 Go (recommandé)	✓	✓	✓
espace disponible sur le disque dur pour le système d'exploitation et le SGBD	18 Go (minimum) 36 Go (recommandé)	✓	✓	✓
espace disponible sur le disque dur pour 30 jours supplémentaires de données	20 Go (minimum) 38 Go (recommandé)	✓	✓	✓
espace disponible sur le disque dur pour 90 jours supplémentaires de données	23 Go (minimum) 41 Go (recommandé)	✓	✓	✓
Résolution d'écran	1024 x 768 pixels	✓	✓	✓
Logiciels tiers (inclus)	IBM Java Runtime Environment (JRE), version 1.7.0 SR2	✓	✓	✓
Logiciels tiers (non inclus)	• SQL Server 2012 Express Edition (recommandé uniquement pous les systèmes de test) **Remarque :** SQL Server 2012 Express limite la taille de la base de données à 10 Go. • SQL Server 2012 Standard Edition • SQL Server 2012 Enterprise Edition • SQL Server 2008 Standard Edition • SQL Server 2008 R2 Standard Edition • SQL Server 2008 Enterprise Edition • SQL Server 2008 R2 Enterprise Edition • SQL Server 2008 64 bits • SQL Server 2005 Enterprise Edition • SQL Server 2005 Standard Edition • SQL Server 2005 64 bits	✓	✓	✓
	Internet Explorer 8.0 ou version ultérieure http://www.microsoft.com/windows/internet-explorer/default.aspx	✓		✓ avec TLS 1.2
	Internet Explorer 9.0 ou version ultérieure http://www.microsoft.com/windows/internet-explorer/default.aspx	✓	✓	✓ avec TLS 1.2

Composant	Configuration minimale requise	Base de référence SP	Support XGS	Support SP800-131A*
	• Adobe Reader 8.0 ou version ultérieure http://get.adobe.com/reader/ • Pour obtenir les mises à jour des logiciels du système d'exploitation Windows et du matériel fonctionnant sur Windows, accédez au site Web Microsoft Updates à l'adresse : http://www.windowsupdate.com	✓	✓	✓
Adresse IP statique ?	Oui	✓	✓	✓
Configurations requises supplémentaires	Mémoire et espace disque supplémentaires, en fonction de divers facteurs, par exemple : • Nombre de vues • Nombre d'actifs • Nombre d'agents • Nombre d'utilisateurs simultanés • Type de politiques mises en oeuvre sur les agents • Quantité de données à stocker sur le serveur	✓	✓	✓

[1]Windows Server 2012 doit être installé en mode normal ; SiteProtector ne prend pas en charge Windows Server 2012 installé en mode "noyau seul".

*Voir «Configuration requise pour le chiffrement Strict (SP800-131A)», à la page 6 pour plus de détails.

Configuration requise pour la base de données SiteProtector

Le tableau suivant décrit la configuration requise pour la base de données SiteProtector et inclut des entrées pour les configurations suivantes :

- **Base de référence SiteProtector** fait référence aux conditions requises pour le système SiteProtector principal.
- **Support XGS** fait référence aux conditions requises pour la modification de règles pour les dispositifs IBM Security Network Protection. Cette modification des règles nécessite Internet Explorer v9 et au-delà, qui est pris en charge uniquement par des systèmes d'exploitation Microsoft spécifiques.
- **Support SP800-131A** fait référence aux conditions requises pour le chiffrement strict (SP800-131A) tel qu'il est défini par National Institute of Standards and Technology (NIST). Le chiffrement strict nécessite le protocole TLS (Transport Layer Security) v1.2 qui est pris en charge uniquement par Internet Explorer v8 et au-delà. Seuls des systèmes d'exploitation Microsoft spécifiques prennent en charge Internet Explorer v8 et au-delà.

Si vous souhaitez utiliser le chiffrement strict (SP800-131A) avec votre base de données SiteProtector, reportez-vous à la rubrique «Configuration du protocole IPsec pour sécuriser les communications de la base de données SiteProtector», à la page 35.

Composant	Configuration minimale requise	Base de référence SP	Support XGS	Support SP800-131A*
Processeur	Xeon 3000 Series ou Core 2 Duo (minimum) Intel Xeon E5450 3,00 GHz (recommandé)	✓	✓	✓
Système d'exploitation SiteProtector prend en charge les versions 32 et 64 bits des systèmes d'exploitation Windows. Les systèmes 64 bits uniquement sont indiqués. **Remarque :** Vous devez exécuter SiteProtector et ses composants sur une partition NTFS. Les partitions FAT et FAT32 ne permettent pas de renforcer la sécurité de votre système correctement.	Windows Server 2012 Standard[1] (64 bits uniquement)	✓	✓	✓
	Windows Server 2008 R2 Standard (64 bits uniquement)	✓	✓	✓
	Windows Server 2008 R2 Entreprise (64 bits uniquement)	✓	✓	✓
	Windows Server 2008 Standard	✓	✓	
	Windows Server 2008 Entreprise	✓	✓	
	Windows Server 2003 R2 Standard	✓		
	Windows Server 2003 R2 Enterprise	✓		
	Windows Server 2003 SP2 Standard	✓		
	Windows Server 2003 SP2 Enterprise	✓		
Mémoire RAM	2 Go (minimum) 4 Go (recommandé)	✓	✓	✓
Espace disponible sur le disque dur	18 Go (minimum) 36 Go (recommandé)	✓	✓	✓
Logiciels tiers (inclus)	IBM Java Runtime Environment (JRE), version 1.7.0 SR2	✓	✓	✓

Composant	Configuration minimale requise	Base de référence SP	Support XGS	Support SP800-131A*
Logiciels tiers (non inclus)	• SQL Server 2012 Express Edition (recommandé uniquement pous les systèmes de test) **Remarque :** SQL Server 2012 Express limite la taille de la base de données à 10 Go. • SQL Server 2012 Standard Edition • SQL Server 2012 Enterprise Edition • SQL Server 2008 Standard Edition • SQL Server 2008 R2 Standard Edition • SQL Server 2008 Enterprise Edition • SQL Server 2008 R2 Enterprise Edition • SQL Server 2008 64 bits • SQL Server 2005 Enterprise Edition • SQL Server 2005 Standard Edition • SQL Server 2005 64 bits	✓	✓	✓
	Internet Explorer 8.0 ou version ultérieure http://www.microsoft.com/windows/internet-explorer/default.aspx	✓		✓ avec TLS 1.2
	Internet Explorer 9.0 ou version ultérieure http://www.microsoft.com/windows/internet-explorer/default.aspx	✓	✓	✓ avec TLS 1.2
	• Pour obtenir les mises à jour des logiciels du système d'exploitation Windows et du matériel fonctionnant sur Windows, accédez au site Web Microsoft Updates à l'adresse : http://www.windowsupdate.com	✓	✓	✓
Adresse IP statique ?	Oui	✓	✓	✓
Configurations requises supplémentaires	Mémoire et espace disque supplémentaires, en fonction de divers facteurs, par exemple : • Nombre de vues • Nombre d'actifs • Nombre d'agents • Nombre d'utilisateurs simultanés • Type de politiques mises en oeuvre sur les agents • Quantité de données à stocker sur le serveur	✓	✓	✓

[1]Windows Server 2012 doit être installé en mode normal ; SiteProtector ne prend pas en charge Windows Server 2012 installé en mode "noyau seul".

*Voir «Configuration requise pour le chiffrement Strict (SP800-131A)», à la page 6 pour plus de détails.

Configuration requise pour Application Server

Le package d'installation d'Application Server inclut X-Press Update Server et la console Web.

Le tableau suivant décrit la configuration requise pour Application Server et inclut des entrées pour les configurations suivantes :

- **Base de référence SiteProtector** fait référence aux conditions requises pour le système SiteProtector principal.

- **Support XGS** fait référence aux conditions requises pour la modification de règles pour les dispositifs IBM Security Network Protection. Cette modification des règles nécessite Internet Explorer v9 et au-delà, qui est pris en charge uniquement par des systèmes d'exploitation Microsoft spécifiques.
- **Support SP800-131A** fait référence aux conditions requises pour le chiffrement strict (SP800-131A) tel qu'il est défini par National Institute of Standards and Technology (NIST). Le chiffrement strict nécessite le protocole TLS (Transport Layer Security) v1.2 qui est pris en charge uniquement par Internet Explorer v8 et au-delà. Seuls des systèmes d'exploitation Microsoft spécifiques prennent en charge Internet Explorer v8 et au-delà.

Composant	Configuration minimale requise	Base de référence SP	Support XGS	Support SP800-131A*
Processeur	Xeon 3000 Series ou Core 2 Duo (minimum) Intel Xeon E5450 3,00 GHz (recommandé)	✓	✓	✓
Système d'exploitation SiteProtector prend en charge les versions 32 et 64 bits des systèmes d'exploitation Windows. Les systèmes 64 bits uniquement sont indiqués. **Remarque :** Vous devez exécuter SiteProtector et ses composants sur une partition NTFS. Les partitions FAT et FAT32 ne permettent pas de renforcer la sécurité de votre système correctement.	Windows Server 2012 Standard[1] (64 bits uniquement)	✓	✓	✓
	Windows Server 2008 R2 Standard (64 bits uniquement)	✓	✓	✓
	Windows Server 2008 R2 Entreprise (64 bits uniquement)	✓	✓	✓
	Windows Server 2008 Standard	✓	✓	
	Windows Server 2008 Entreprise	✓	✓	
	Windows Server 2003 R2 Standard	✓		
	Windows Server 2003 R2 Enterprise	✓		
	Windows Server 2003 SP2 Standard	✓		
	Windows Server 2003 SP2 Enterprise	✓		
Mémoire RAM	2 Go (minimum) 4 Go (recommandé)	✓	✓	✓
Espace disponible sur le disque dur	18 Go (minimum) 40 Go (recommandé)	✓	✓	✓
Résolution d'écran	1024 x 768 pixels	✓	✓	✓
Logiciels tiers (inclus)	IBM Java Runtime Environment (JRE), version 1.7.0 SR2	✓	✓	✓
Logiciels tiers (non inclus)	Internet Explorer 8.0 ou version ultérieure http://www.microsoft.com/windows/internet-explorer/default.aspx	✓		✓ avec TLS 1.2

Composant	Configuration minimale requise	Base de référence SP	Support XGS	Support SP800-131A*
	Internet Explorer 9.0 ou version ultérieure http://www.microsoft.com/windows/internet-explorer/default.aspx	✓	✓	✓ avec TLS 1.2
	• Java J2SE Runtime Environment 5.0 (1.5.0) ou version ultérieure • Adobe Reader 8.0 ou version ultérieure http://get.adobe.com/reader/ • Pour obtenir les mises à jour des logiciels du système d'exploitation Windows et du matériel fonctionnant sur Windows, accédez au site Web Microsoft Updates à l'adresse : http://www.windowsupdate.com	✓	✓	✓
Adresse IP statique ?	Oui	✓	✓	✓
Virtualisation	• VMware ESX 4.x ou ESXi 4.x ou 5.x • Microsoft Windows Server 2008 Hyper-V • Microsoft Virtual Server 2005	✓	✓	✓
Configurations requises supplémentaires	Mémoire et espace disque supplémentaires, en fonction de divers facteurs, par exemple : • Nombre de vues • Nombre d'actifs • Nombre d'agents ou de dispositifs • Nombre d'utilisateurs simultanés • Type de politiques mises en oeuvre sur les agents ou les dispositifs	✓	✓	✓

[1]Windows Server 2012 doit être installé dans mode normal ; SiteProtector ne prend pas en charge Windows Server 2012 installé en mode "noyau seul".

*Voir «Configuration requise pour le chiffrement Strict (SP800-131A)», à la page 6 pour plus de détails.

Remarque : Des tests ont détecté que l'allocation de ressources avec l'utilisation de Microsoft Virtual Server 2005 affectait les performances globales de SiteProtector. Par exemple, lorsque le système d'exploitation de base et une instance virtuelle s'exécutaient sur une unité à processeur unique, SiteProtector fonctionnait plus lentement que lorsqu'il s'exécutait sur une instance de matériel répondant aux spécifications de l'instance virtuelle seule. C'est pourquoi il vous faut envisager la fourniture de ressources supplémentaires avec Virtual Server 2005.

Configuration requise pour la console

Remarque : La première fois que vous cliquez sur **Help** dans SiteProtector Console, vous risquez de recevoir une "Erreur de certificat" dans Internet Explorer. Pour éviter cette erreur à l'avenir, installez le certificat de sécurité généré par le composant Application Server. Pour plus d'informations, consultez le site Web Microsoft Support : http://support.microsoft.com/kb/931850

Le tableau suivant décrit la configuration requise pour une console unique et inclut des entrées pour les configurations suivantes :

- **Base de référence SiteProtector** fait référence aux conditions requises pour le système SiteProtector principal.

- **Support XGS** fait référence aux conditions requises pour la modification de règles pour les dispositifs IBM Security Network Protection. Cette modification des règles nécessite Internet Explorer v9 et au-delà, qui est pris en charge uniquement par des systèmes d'exploitation Microsoft spécifiques.
- **Support SP800-131A** fait référence aux conditions requises pour le chiffrement strict (SP800-131A) tel qu'il est défini par National Institute of Standards and Technology (NIST). Le chiffrement strict nécessite le protocole TLS (Transport Layer Security) v1.2 qui est pris en charge uniquement par Internet Explorer v8 et au-delà. Seuls des systèmes d'exploitation Microsoft spécifiques prennent en charge Internet Explorer v8 et au-delà.

Composant	Configuration minimale requise	Base de référence de SP	Support XGS	Support SP800-131A*
Processeur	Xeon 3000 Series ou Core 2 Duo (minimum) Intel Xeon E5450 3,00 GHz (recommandé)	✓	✓	✓
Système d'exploitation SiteProtector prend en charge les versions 32 et 64 bits des systèmes d'exploitation Windows. Les systèmes 64 bits uniquement sont indiqués. **Remarque :** Vous devez exécuter SiteProtector et ses composants sur une partition NTFS. Les partitions FAT et FAT32 ne permettent pas de renforcer la sécurité de votre système correctement.	Windows 8	✓	✓	✓
	Windows 7	✓	✓	✓
	Windows 7 Enterprise	✓	✓	✓
	Windows 7 Edition Intégrale	✓	✓	✓
	Windows Server 2012 Standard[1] (64 bits uniquement)	✓	✓	✓
	Windows Server 2008 R2 Standard (64 bits uniquement)	✓	✓	✓
	Windows Server 2008 R2 Enterprise (64 bits uniquement)	✓	✓	✓
	Windows Vista Professionnel	✓	✓	
	Windows Vista Enterprise	✓	✓	
	Windows Server 2008 Standard	✓	✓	
	Windows Server 2008 Enterprise	✓	✓	
	SQL Server 2008 R2 Standard Edition	✓		
	SQL Server 2008 R2 Enterprise Edition	✓		
	Windows Server 2003 R2 Standard	✓		
	Windows Server 2003 R2 Enterprise	✓		
	Windows Server 2003 SP2 Standard	✓		
	Windows Server 2003 SP2 Enterprise	✓		

Composant	Configuration minimale requise	Base de référence de SP	Support XGS	Support SP800-131A*
Mémoire RAM	512 Mo (minimum) 1 Go (recommandé)	✓	✓	✓
Espace disponible sur le disque dur	4 Go (minimum) 20 Go (recommandé)	✓	✓	✓
Résolution d'écran	1024 x 768 pixels	✓	✓	✓
Paramètres de couleurs	65536 Couleurs (16 bits)			
Adresse IP statique ?	Non			
Logiciels tiers (inclus)	IBM Java Runtime Environment (JRE), version 1.7.0 SR2	✓	✓	✓
Logiciels tiers (non inclus)	Internet Explorer 8.0 ou version ultérieure http://www.microsoft.com/windows/internet-explorer/default.aspx	✓		✓ avec TLS 1.2
	Internet Explorer 9.0 ou version ultérieure http://www.microsoft.com/windows/internet-explorer/default.aspx	✓	✓	✓ avec TLS 1.2
	• Adobe Reader 8.0 ou version ultérieure http://get.adobe.com/reader/ • Pour obtenir les mises à jour des logiciels du système d'exploitation Windows et du matériel fonctionnant sur Windows, accédez au site Web Microsoft Updates à l'adresse : http://www.windowsupdate.com	✓	✓	✓

[1]Windows Server 2012 doit être installé en mode normal ; SiteProtector ne prend pas en charge Windows Server 2012 installé en mode "noyau seul".

* Voir «Configuration requise pour le chiffrement Strict (SP800-131A)», à la page 6 pour plus de détails.

Configuration requise pour le composant Event Viewer

Le tableau suivant décrit la configuration requise pour un composant Event Viewer unique et inclut des entrées pour les configurations suivantes :

- **Base de référence SiteProtector** fait référence aux conditions requises pour le système SiteProtector principal.
- **Support XGS** fait référence aux conditions requises pour la modification de règles pour les dispositifs IBM Security Network Protection. Cette modification des règles nécessite Internet Explorer v9 et au-delà, qui est pris en charge uniquement par des systèmes d'exploitation Microsoft spécifiques.
- **Support SP800-131A** fait référence aux conditions requises pour le chiffrement strict (SP800-131A) tel qu'il est défini par National Institute of Standards and Technology (NIST). Le chiffrement strict nécessite le protocole TLS (Transport Layer Security) v1.2 qui est pris en charge uniquement par Internet Explorer v8 et au-delà. Seuls des systèmes d'exploitation Microsoft spécifiques prennent en charge Internet Explorer v8 et au-delà.

Composant	Configuration minimale requise	Base de référence de SP	Support XGS	Support SP800-131A
Processeur	Xeon 3000 Series ou Core 2 Duo (minimum) Intel Xeon E5450 3,00 GHz (recommandé)	✓	✓	✓
Système d'exploitation SiteProtector prend en charge les versions 32 et 64 bits des systèmes d'exploitation Windows. Les systèmes 64 bits uniquement sont indiqués. **Remarque :** Vous devez exécuter SiteProtector et ses composants sur une partition NTFS. Les partitions FAT et FAT32 ne permettent pas de renforcer la sécurité de votre système correctement.	Windows 8	✓	✓	✓
	Windows 7	✓	✓	✓
	Windows 7 Enterprise	✓	✓	✓
	Windows 7 Edition Intégrale	✓	✓	✓
	Windows Server 2012 Standard[1] (64 bits uniquement)	✓	✓	✓
	Windows Server 2008 R2 Standard (64 bits uniquement)	✓	✓	✓
	Windows Server 2008 R2 Enterprise (64 bits uniquement)	✓	✓	✓
	Windows Vista Professionnel	✓	✓	
	Windows Vista Enterprise	✓	✓	
	Windows Server 2008 Standard	✓	✓	
	Windows Server 2008 Enterprise	✓	✓	
	SQL Server 2008 R2 Standard Edition	✓		
	SQL Server 2008 R2 Enterprise Edition	✓		
	Windows Server 2003 R2 Standard	✓		
	Windows Server 2003 R2 Enterprise	✓		
	Windows Server 2003 SP2 Standard	✓		
	Windows Server 2003 SP2 Enterprise	✓		
Mémoire RAM	512 Mo (minimum) 1 Go (recommandé)	✓	✓	✓
Espace disponible sur le disque dur	4 Go (minimum) 20 Go (recommandé)	✓	✓	✓
Résolution d'écran	1024 x 768 pixels	✓	✓	✓
Paramètres de couleurs	65536 Couleurs (16 bits)	✓	✓	✓
Adresse IP statique ?	Non	✓	✓	✓

Composant	Configuration minimale requise	Base de référence de SP	Support XGS	Support SP800-131A
Logiciels tiers (inclus)	IBM Java Runtime Environment (JRE), version 1.7.0 SR2	✓	✓	✓

[1]Windows Server 2012 doit être installé en mode normal ; SiteProtector ne prend pas en charge Windows Server 2012 installé en mode "noyau seul".

Configuration système requise pour le composant Event Archiver

Le tableau suivant décrit la configuration requise pour Event Archiver et inclut des entrées pour les configurations suivantes :

- **Base de référence SiteProtector** fait référence aux conditions requises pour le système SiteProtector principal.
- **Support XGS** fait référence aux conditions requises pour la modification de règles pour les dispositifs IBM Security Network Protection. Cette modification des règles nécessite Internet Explorer v9 et au-delà, qui est pris en charge uniquement par des systèmes d'exploitation Microsoft spécifiques.
- **Support SP800-131A** fait référence aux conditions requises pour le chiffrement strict (SP800-131A) tel qu'il est défini par National Institute of Standards and Technology (NIST). Le chiffrement strict nécessite le protocole TLS (Transport Layer Security) v1.2 qui est pris en charge uniquement par Internet Explorer v8 et au-delà. Seuls des systèmes d'exploitation Microsoft spécifiques prennent en charge Internet Explorer v8 et au-delà.

Composant	Configuration minimale requise	Base de référence SP	Support XGS	Support SP800-131A
Processeur	Xeon 3000 Series ou Core 2 Duo (minimum) Intel Xeon E5450 3,00 GHz (recommandé)	✓	✓	✓
Système d'exploitation SiteProtector prend en charge les versions 32 et 64 bits des systèmes d'exploitation Windows. Les systèmes 64 bits uniquement sont indiqués. **Remarque :** Vous devez exécuter SiteProtector et ses composants sur une partition NTFS. Les partitions FAT et FAT32 ne permettent pas de renforcer la sécurité de votre système correctement.	Windows Server 2012 Standard[1] (64 bits uniquement)	✓	✓	✓
	Windows Server 2008 R2 Standard (64 bits uniquement)	✓	✓	✓
	Windows Server 2008 R2 Enterprise (64 bits uniquement)	✓	✓	✓
	Windows Server 2008 Standard	✓	✓	
	Windows Server 2008 Enterprise	✓	✓	
	Windows Server 2003 R2 Standard	✓		
	Windows Server 2003 R2 Enterprise	✓		

Composant	Configuration minimale requise	Base de référence SP	Support XGS	Support SP800-131A
	Windows Server 2003 SP2 Standard	✓		
	Windows Server 2003 SP2 Enterprise	✓		
Mémoire RAM	512 Mo (minimum) 1 Go (recommandé)	✓	✓	✓
Espace disponible sur le disque dur	9 Go (minimum) 20 Go (recommandé)	✓	✓	✓
Logiciels tiers (non inclus)	• Pour obtenir les mises à jour des logiciels du système d'exploitation Windows et du matériel fonctionnant sur Windows, accédez au site Web Microsoft Updates à l'adresse : http://www.windowsupdate.com	✓	✓	✓
Adresse IP statique ?	Oui	✓	✓	✓
Configurations requises supplémentaires	Mémoire et espace disque supplémentaires, en fonction de divers facteurs, par exemple : • Nombre d'agents ou de dispositifs • Nombre d'utilisateurs simultanés • Type de politiques mises en oeuvre sur les agents ou les dispositifs • Consignation des événements	✓	✓	✓

[1]Windows Server 2012 doit être installé en mode normal ; SiteProtector ne prend pas en charge Windows Server 2012 installé en mode "noyau seul".

Configuration requise pour les composants Event Collector et Agent Manager

Le tableau suivant décrit la configuration requise pour un composant Event Collector ou Agent Manager unique et inclut des entrées pour les configurations suivantes :

- **Base de référence SiteProtector** fait référence aux conditions requises pour le système SiteProtector principal.
- **Support XGS** fait référence aux conditions requises pour la modification de règles pour les dispositifs IBM Security Network Protection. Cette modification des règles nécessite Internet Explorer v9 et au-delà, qui est pris en charge uniquement par des systèmes d'exploitation Microsoft spécifiques.
- **Support SP800-131A** fait référence aux conditions requises pour le chiffrement strict (SP800-131A) tel qu'il est défini par National Institute of Standards and Technology (NIST). Le chiffrement strict nécessite le protocole TLS (Transport Layer Security) v1.2 qui est pris en charge uniquement par Internet Explorer v8 et au-delà. Seuls des systèmes d'exploitation Microsoft spécifiques prennent en charge Internet Explorer v8 et au-delà.

Composant	Configuration minimale requise	Base de référence SP	Support XGS	Support SP800-131A*
Processeur	Xeon 3000 Series ou Core 2 Duo (minimum) Intel Xeon E5450 3,00 GHz (recommandé)	✓	✓	✓
Système d'exploitation SiteProtector prend en charge les versions 32 et 64 bits des systèmes d'exploitation Windows. Les systèmes 64 bits uniquement sont indiqués. **Remarque :** Vous devez exécuter SiteProtector et ses composants sur une partition NTFS. Les partitions FAT et FAT32 ne permettent pas de renforcer la sécurité de votre système correctement.	Windows Server 2012 Standard[1] (64 bits uniquement)	✓	✓	✓
	Windows Server 2008 Standard	✓	✓	✓
	Windows Server 2008 R2 Standard (64 bits uniquement)	✓	✓	✓
	Windows Server 2008 Enterprise	✓	✓	✓
	Windows Server 2008 R2 Enterprise (64 bits uniquement)	✓	✓	✓
	Windows Server 2003 R2 Standard	✓	✓	
	Windows Server 2003 R2 Enterprise	✓	✓	
	Windows Server 2003 SP2 Standard	✓	✓	
	Windows Server 2003 SP2 Enterprise	✓	✓	
Mémoire RAM	2 Go (minimum) 4 Go (recommandé)	✓	✓	✓
Espace disponible sur le disque dur	4 Go (minimum) 20 Go (recommandé)	✓	✓	✓
Adresse IP statique ?	Oui	✓	✓	✓
Logiciels tiers (inclus)	IBM Java Runtime Environment (JRE), version 1.7.0 SR2	✓	✓	✓
Logiciels tiers (non inclus)	• Pour obtenir les mises à jour des logiciels du système d'exploitation Windows et du matériel fonctionnant sur Windows, accédez au site Web Microsoft Updates à l'adresse : http://www.windowsupdate.com	✓	✓	✓
Système dédié ?	Oui	✓	✓	✓

Composant	Configuration minimale requise	Base de référence SP	Support XGS	Support SP800-131A*
Configurations requises supplémentaires	Mémoire et espace disque supplémentaires, en fonction de divers facteurs, par exemple : • Nombre d'agents ou de dispositifs • Nombre d'utilisateurs simultanés • Type de politiques mises en oeuvre sur les agents ou les dispositifs • Consignation des événements	✓	✓	✓

[1]Windows Server 2012 doit être installé en mode normal ; SiteProtector ne prend pas en charge Windows Server 2012 installé en mode "noyau seul".

* Voir «Configuration requise pour le chiffrement Strict (SP800-131A)», à la page 6 pour plus de détails.

Configuration système requise pour le composant X-Press Update Server

Le tableau suivant décrit la configuration requise pour le composant X-Press Update Server et inclut des entrées pour les configurations suivantes :

- **Base de référence SiteProtector** fait référence aux conditions requises pour le système SiteProtector principal.
- **Support XGS** fait référence aux conditions requises pour la modification de règles pour les dispositifs IBM Security Network Protection. Cette modification des règles nécessite Internet Explorer v9 et au-delà, qui est pris en charge uniquement par des systèmes d'exploitation Microsoft spécifiques.
- **Support SP800-131A** fait référence aux conditions requises pour le chiffrement strict (SP800-131A) tel qu'il est défini par National Institute of Standards and Technology (NIST). Le chiffrement strict nécessite le protocole TLS (Transport Layer Security) v1.2 qui est pris en charge uniquement par Internet Explorer v8 et au-delà. Seuls des systèmes d'exploitation Microsoft spécifiques prennent en charge Internet Explorer v8 et au-delà.

Composant	Configuration minimale requise	Base de référence SP	Support XGS	Support SP800-131A
Processeur	Xeon 3000 Series ou Core 2 Duo (minimum) Intel Xeon E5450 3,00 GHz (recommandé)	✓	✓	✓
Système d'exploitation SiteProtector prend en charge les versions 32 et 64 bits des systèmes d'exploitation Windows. Les systèmes 64 bits uniquement sont indiqués. **Remarque :** Vous devez exécuter SiteProtector et ses composants sur une partition NTFS. Les partitions FAT et FAT32 ne permettent pas de renforcer la sécurité de votre système correctement.	Windows Server 2012 Standard[1] (64 bits uniquement)	✓	✓	✓

Composant	Configuration minimale requise	Base de référence SP	Support XGS	Support SP800-131A
	Windows Server 2008 R2 Standard (64 bits uniquement)	✓	✓	✓
	Windows Server 2008 R2 Entreprise (64 bits uniquement)	✓	✓	✓
	Windows Server 2008 Standard	✓	✓	
	Windows Server 2008 Entreprise	✓	✓	
	Windows Server 2003 R2 Standard	✓		
	Windows Server 2003 R2 Enterprise	✓		
	Windows Server 2003 SP2 Standard	✓		
	Windows Server 2003 SP2 Enterprise	✓		
Mémoire RAM	512 Mo (minimum) 1 Go (recommandé)	✓	✓	✓
Espace disponible sur le disque dur	9 Go (minimum) 20 Go (recommandé)	✓	✓	✓
Adresse IP statique ?	Oui	✓	✓	✓
Logiciels tiers (non inclus)	• Pour obtenir les mises à jour des logiciels du système d'exploitation Windows et du matériel fonctionnant sur Windows, accédez au site Web Microsoft Updates à l'adresse : http://www.windowsupdate.com	✓	✓	✓

[1]Windows Server 2012 doit être installé en mode normal ; SiteProtector ne prend pas en charge Windows Server 2012 installé en mode "noyau uniquement".

Chapitre 3. Planification de l'installation de SiteProtector

Directives relatives à l'évolutivité

Utilisez ces informations pour planifier un déploiement de SiteProtector ou lorsque vous prévoyez d'étendre une configuration existante pour répondre à des besoins croissants en performance.

Scénarios de déploiement

Vous pouvez déployer le système SiteProtector dans une configuration minimale avec un seul ordinateur ou utiliser des déploiements plus grands avec plusieurs ordinateurs pour les moyens et grands réseaux. Chaque scénario de déploiement nécessite une configuration différente du matériel et des logiciels. Tenez compte de ces scénarios lorsque vous déterminez le mode d'installation et de configuration de SiteProtector.

Déploiement minimum

Ce scénario nécessite un ordinateur et constitue le plus petit déploiement de SiteProtector que vous puissiez avoir. Ce déploiement est particulièrement adapté aux petits réseaux et aux environnements de test.

Approche
Procédez à une installation Express de SiteProtector de sorte qu'Application Server et la base de données SiteProtector se trouvent sur un seul ordinateur.

Déploiement de petite taille

Ce scénario ne nécessite qu'un seul ordinateur, mais dont les capacités sont supérieures à celui du déploiement minimum.

Approche
Procédez à une installation Express de SiteProtector de sorte qu'Application Server et la base de données SiteProtector se trouvent sur un seul ordinateur.

Déploiement de taille moyenne

Ce scénario nécessite trois à quatre ordinateurs.

Ordinateur 1
Installez la base de données SiteProtector sur le premier ordinateur.

Ordinateur 2
Installez le composant Application Server sur le deuxième ordinateur. L'installation du composant Application Server inclut le composant X-Press Update Server et la console Web.

Installez également la console SiteProtector sur le deuxième ordinateur. L'installation de la console SiteProtector inclut le composant Event Viewer.

Ordinateur 3 et 4
Installez les composants Agent Manager et Event Collector sur le troisième ordinateur et toute paire Agent Manager/Event Collector supplémentaire sur le quatrième ordinateur.

Réseau de grande taille

Ce scénario nécessite quatre à cinq ordinateurs.

Ordinateur 1
Installez la base de données SiteProtector sur le premier ordinateur.

Ordinateur 2
Installez le composant Application Server sur le deuxième ordinateur. L'installation du composant Application Server inclut le composant X-Press Update Server et la console Web.

Installez également la console SiteProtector sur le deuxième ordinateur. L'installation de la console SiteProtector inclut le composant Event Viewer.

Ordinateur 3, 4 et 5
Installez les composants Agent Manager et Event Collector sur le troisième ordinateur et toute paire Agent Manager/Event Collector supplémentaire sur les quatrième et cinquième ordinateurs.

Considérations relatives aux performances

Les performances de SiteProtector System sont influencées par de nombreux facteurs tels que le chargement d'événement, les opérations multiples de la console, les longues demandes d'analyse et la génération de rapports.

Si le nombre moyen d'événements par jour et le nombre maximal de signaux de présence par jour de votre site sont régulièrement plus élevés que les recommandations présentées ici, votre site pourra être confronté à des problèmes de performances, quel que soit le nombre d'agents que vous utilisez. Les problèmes potentiels comprennent :

- La console peut devenir lente ou ne plus répondre.
- La base de données peut temporairement ne plus pouvoir accepter de nouveaux événements tant que l'activité ne revient pas dans les limites propres à votre configuration.
- La base de données peut traiter les événements à un rythme très lent tant que l'activité ne revient pas dans les limites propres à votre configuration.

Si l'activité de votre environnement dépasse les limites de la taille de votre déploiement, tenez compte des recommandations suivantes pour ajuster votre déploiement.

Facteurs ayant un impact sur les performances

Plusieurs facteurs peuvent avoir une incidence sur les performances globales et la réactivité de SiteProtector :

- opérations multiples sur la console
- requêtes d'analyse à exécution longue
- génération de rapports
- analyse de fusion
- opérations de maintenance

Configuration pour Event Collector et Agent Manager

Pour les déploiements de grande taille et de taille moyenne, IBM Security recommande l'installation des composants Event Collector et Agent Manager sur le même ordinateur. La configuration système requise pour l'installation d'Agent Manager sur un système dédié s'applique également aux autres composants Event Collector et Agent Manager partageant le même ordinateur. Pour plus d'informations sur la configuration requise d'Agent Manager, voir Chapitre 2, «Configuration matérielle et logicielle requise», à la page 5.

Utilisation de plusieurs composants Agent Manager et Event Collector

Les paires multiples Event Collector - Agent Manager sont nécessaires pour s'adapter à l'augmentation de la bande passante nécessaire lors de la mise à jour des agents, notamment pour fournir la redondance.

Toutefois, augmenter le nombre de composants Agent Manager et Event Collector n'augmente pas pour autant le nombre limite d'événements et de signaux de présence référencé.

Pour les déploiements de grande taille et de taille moyenne

Pour optimiser les performances, le composant Event Collector installé sur le serveur de base de données ne doit être utilisé qu'à de fins de redondance. Ainsi, les ressources du serveur sont dédiées au service de base de données, ce qui peut améliorer les performances.

Pour optimiser les performances, le composant Agent Manager résidant sur le serveur d'applications ne doit être utilisé qu'à des fins de redondance. Ainsi, les ressources du serveur sont dédiées au serveur d'applications, ce qui peut améliorer les performances.

Serveurs de mise à jour pour Proventia Desktop Endpoint Security

A partir de la version 9.0, Proventia Desktop Endpoint Security est équipé d'un antivirus basé sur les signatures et d'un filtrage anti-logiciel espion, ce qui nécessite la mise à jour fréquente des définitions de virus. Pour vous assurer d'être en mesure de traiter ces mises à jour, voir la note technique *Number of Update Servers to Support AntiVirus Capability for Proventia Desktop 9.0 Agents* (Technote 1435588) sur le site https://www-304.ibm.com/support/docview.wss?uid=swg21435588.

Recommandations

Des recommandations sont fournies pour le matériel, les logiciels et l'espace disque disponible. Ces recommandations s'appuient sur les environnements client standard et peuvent ne pas s'appliquer à l'environnement que vous utilisez.

Important : Le présent document fournit des critères d'évaluation pour les agents actifs, les événements, les signaux de présence, ainsi que d'autres facteurs. Ne dépassez pas le nombre moyen d'événements par jour ou le nombre maximal de signaux par jour quel que soit le nombre de détecteurs figurant dans votre configuration.

Matériel et logiciels

Les recommandations concernant le matériel et les logiciels s'appuient sur les éléments suivants :

Elément	Description
Nombre maximal d'agents actifs du site	Ce nombre représente le nombre maximal d'agents actifs sur l'ensemble du site. Les recommandations fournies ici supposent que le nombre total d'agents actifs sur l'ensemble de votre site ne dépasse pas régulièrement le nombre inscrit dans cette colonne.
Nombre maximal d'événements par jour du site	Ce nombre représente le nombre maximal d'événements traités par jour sur l'ensemble du site. Les recommandations fournies ici supposent que le nombre total d'événements par jour sur l'ensemble de votre site ne dépassera pas régulièrement le nombre inscrit dans cette colonne.
Nombre maximal de signaux de présence par jour	Ce nombre représente le nombre maximal de signaux de présence traités par jour par la base de données sur l'ensemble de votre site. Les recommandations fournies ici supposent que le nombre total de signaux de présence par jour sur l'ensemble de votre site ne dépassera pas régulièrement le nombre inscrit dans cette colonne.
Nombre maximal de signaux de présence recommandé par jour et par agent	Ce nombre représente le nombre maximal de signaux de présence recommandés par jour et par agent sur l'ensemble de votre site. Les recommandations fournies ici supposent que le nombre maximal de signaux de présence recommandés par jour et par agent sur l'ensemble de votre site ne dépassera pas régulièrement le nombre inscrit dans cette colonne.

Elément	Description
Intervalle minimal des signaux de présences (heures)	Ce nombre représente l'intervalle des signaux de présence le plus court par agent affiché à la fois en secondes et en heures. Les recommandations fournies ici supposent que l'intervalle des signaux de présence minimal par agent sur l'ensemble de votre site ne sera pas régulièrement inférieur au nombre inscrit dans cette colonne.
Seuil de groupe d'agents qui ne répond pas en minutes (heures)	Ce nombre indique le seuil en minutes et en heures après lequel un agent est considéré comme ne répondant pas si aucun signal de présence n'est reçu.
Nombre supplémentaire suggéré de paires Event Collector - Agent Manager	Ce nombre indique le nombre supplémentaire recommandé de paires de composants Event Collector-Agent Manager pour un scénario de déploiement particulier.

Espace disponible sur le disque dur

Les recommandations d'espace disponible sur le disque dur s'appuient sur les éléments suivants :

- volume d'événements attendu
- espace requis pour stocker les données d'événement pendant 30 jours
- espace requis pour stocker les données d'événement pendant 90 jours
- espace requis pour exécuter la maintenance régulière de la base de données

Structure de la base de données

Pour plus d'informations sur la structure de vos fichiers de base de données, accédez au site Web de Microsoft SQL à l'adresse : http://www.microsoft.com/sql/

Déploiement minimum

Un déploiement minimum de SiteProtector System peut être installé sur un seul ordinateur. Il convient le mieux aux environnements de test. Vous pouvez utiliser l'installation Express pour accomplir cette tâche.

Environnement

Un **déploiement minimum avec un ordinateur** est approprié dans l'environnement suivant :

Nombre maximal d'agents actifs du site	Nombre maximal d'événements par jour du site	Nombre maximal de signaux de présence par jour	Nombre maximal de signaux de présence recommandé par jour et par agent	Intervalle minimal des signaux de présence en secondes (heures)	Seuil de groupe d'agents qui ne répond pas en minutes (heures)	Nombre supplémentaire suggéré de paires Event Collector - Agent Manager
500	50 000	1 000	2	43 200 (12)	720 (12)	0[a]

[a] Voir «Utilisation de plusieurs composants Agent Manager et Event Collector» dans la rubrique «Considérations relatives aux performances», à la page 22.

Matériel et logiciels

Le tableau suivant présente les recommandations matérielles et logicielles pour le déploiement minimum :

Elément	Minimum	Recommandation
processeur	Xeon 3000 Series ou Core 2 Duo	(1) 2.53 GHz Intel Xeon E5540
système d'exploitation	Windows Server 2003	Windows Server 2012[1]
SQL Server	Serveur SQL 2005	SQL Server 2012
mémoire RAM	1 Go	2 Go
espace disponible sur le disque dur pour le système d'exploitation et le SGBD	18 Go	36 Go
espace disponible sur le disque dur pour 30 jours supplémentaires de données	20 Go	38 Go
espace disponible sur le disque dur pour 90 jours supplémentaires de données	23 Go	41 Go

[1]Windows Server 2012 doit être installé en mode normal ; SiteProtector ne prend pas en charge Windows Server 2012 installé en mode "noyau seul".

Remarque : Voir Chapitre 2, «Configuration matérielle et logicielle requise», à la page 5 pour connaître la configuration minimale requise et obtenir la liste de tous les systèmes d'exploitation et des serveurs de base de données pris en charge.

Déploiement de petite taille

Un déploiement de petite taille de SiteProtector System peut être installé sur un seul ordinateur. Vous pouvez utiliser l'installation Express pour effectuer cette tâche.

Notez que la configuration matérielle et logicielle requise du déploiement de petite taille présenté ici correspond au dispositif IBM Security SiteProtector System SP3001.

Pour obtenir les spécifications du dispositif SiteProtector System SP3001, reportez-vous à la fiche technique IBM Security SiteProtector System à l'adresse : http://www.ibm.com/common/ssi/cgi-bin/ssialias?subtype=SP&infotype=PM&appname=SWGE_WG_WG_USEN&htmlfid=WGD03013USEN&attachment=WGD03013USEN.PDF.

Environnement

Un **déploiement de petite taille** est approprié dans l'environnement suivant :

Nombre maximal d'agents actifs du site	Nombre maximal d'événements par jour du site	Nombre maximal de signaux de présence par jour	Nombre maximal de signaux de présence recommandé par jour et par agent	Intervalle minimal des signaux de présence en secondes (heures)	Seuil de groupe d'agents qui ne répond pas en minutes (heures)	Nombre supplémentaire suggéré de paires Event Collector - Agent Manager
25 000	1 250 000	150 000	6	14 400 (4)	240 (4)	0[a]

[a] Voir «Utilisation de plusieurs composants Agent Manager et Event Collector» dans la rubrique «Considérations relatives aux performances», à la page 22.

Matériel et logiciels

Le tableau suivant fournit les recommandations concernant le matériel et les logiciels pour un déploiement de petite taille :

Elément	Recommandation
processeur	(1) Intel Xeon E5540 2,53 GHz avec 8 Mo de cache
système d'exploitation	Windows Server 2012[1]
SQL Server	SQL Server 2012
mémoire RAM	12 Go
vitesse de l'unité de disque dur	SAS 10 500 tr/min
configuration de l'unité de disque dur	RAID 1+0
espace disponible sur le disque dur pour le système d'exploitation et le SGBD	36 Go
espace disponible sur le disque dur pour 30 jours supplémentaires de données	52 Go
espace disponible sur le disque dur pour 90 jours supplémentaires de données	157 Go

[1]Windows Server 2012 doit être installé en mode normal ; SiteProtector ne prend pas en charge Windows Server 2012 installé en mode "noyau seul".

Remarque : Voir Chapitre 2, «Configuration matérielle et logicielle requise», à la page 5 pour connaître la configuration minimale requise et obtenir la liste de tous les systèmes d'exploitation et des serveurs de base de données pris en charge.

Déploiement de taille moyenne

Un déploiement de taille moyenne de SiteProtector System nécessite au moins trois ordinateurs.

Dans un déploiement de grande taille, la fonctionnalité de SiteProtector System peut être répartie sur trois ou quatre ordinateurs :

Ordinateur	Composants
1	Database
2	Application Server (l'installation d'Application Server inclut X-Press Update Server et la console Web.)
3 et 4	Event Collector Agent Manager

Environnement

Un **déploiement de taille moyenne** est approprié dans l'environnement suivant :

Nombre maximal d'agents actifs du site	Nombre maximal d'événements par jour du site	Nombre maximal de signaux de présence par jour	Nombre maximal de signaux de présence recommandé par jour et par agent	Intervalle minimal des signaux de présence en secondes (heures)	Seuil de groupe d'agents qui ne répond pas en minutes (heures)	Nombre supplémentaire suggéré de paires Event Collector - Agent Manager
50 000	5 000 000	300 000	6	14 400 (4)	240 (4)	2[a]

[a] Voir «Utilisation de plusieurs composants Agent Manager et Event Collector» dans la rubrique «Considérations relatives aux performances», à la page 22.

Matériel et logiciels

Le tableau suivant fournit les recommandations concernant le matériel et les logiciels pour un déploiement de taille moyenne :

Ordinateur	Elément	Recommandation
1 (base de données)	processeur	(1) Intel Xeon E5450 3,00 GHz avec 8 Mo de cache
	système d'exploitation	Windows Server 2012[1]
	SQL Server	SQL Server 2012
	mémoire RAM	8 Go
	Configuration du disque dur (base de données)	
	utilisation de la base de données pendant 30 jours en Go	176 Go
	utilisation de la base de données pendant 90 jours en Go	528 Go
	vitesse de l'unité de disque dur de la base de données	Disques SCSI 15 000 tr/min
	configuration de l'unité de disque dur (base de données)	RAID 5 / RAID 1+0
	accès à l'unité de disque dur de la base de données	réseau SAN Fiber Channel 2G+
2 (Application Server)	processeur	(1) Intel Xeon E5450 3,00 GHz avec 8 Mo de cache
	système d'exploitation	Windows Server 2012[1]
	mémoire RAM	4 Go
	espace disponible sur le disque dur	36 Go
	vitesse de l'unité de disque dur (système d'exploitation)	Disques 10 000 tr/min
	configuration de l'unité de disque dur (système d'exploitation)	RAID 1+0
3 et 4 (Event Collector/Agent Manager)	processeur	(1) Intel Xeon E5450 3,00 GHz avec 8 Mo de cache
	système d'exploitation	Windows Server 2012[1]
	mémoire RAM	2 Go
	espace disponible sur le disque dur	36 Go

[1]Windows Server 2012 doit être installé en mode normal ; SiteProtector ne prend pas en charge Windows Server 2012 installé en mode "noyau seul".

Remarque : Voir Chapitre 2, «Configuration matérielle et logicielle requise», à la page 5 pour connaître la configuration minimale requise et obtenir la liste de tous les systèmes d'exploitation et des serveurs de base de données pris en charge.

Déploiement de grande taille

Un déploiement de grande taille de SiteProtector System nécessite quatre ordinateurs au minimum.

Dans un déploiement de grande taille, la fonctionnalité de SiteProtector System peut être répartie sur cinq ordinateurs ou plus.

Ordinateur	Composants
1	Database
2	Application Server (l'installation d'Application Server inclut X-Press Update Server et la console Web.)
3, 4 et 5	Event Collector Agent Manager

Environnement

Un **déploiement de grande taille** est approprié dans l'environnement suivant :

Nombre maximal d'agents actifs du site	Nombre maximal d'événements par jour du site	Nombre maximal de signaux de présence par jour	Nombre maximal de signaux de présence recommandé par jour et par agent	Intervalle minimal des signaux de présence en secondes (heures)	Seuil de groupe d'agents qui ne répond pas en minutes (heures)	Nombre supplémentaire suggéré de paires Event Collector - Agent Manager
100 000	5 000 000	600 000	6	14 400 (4)	240 (4)	3[a]

[a] Voir «Utilisation de plusieurs composants Agent Manager et Event Collector» dans la rubrique «Considérations relatives aux performances», à la page 22.

Matériel et logiciels

Le tableau suivant fournit les recommandations concernant le matériel et les logiciels pour un déploiement de grande taille :

Ordinateur	Elément	Recommandation
1 (base de données)	processeur	(2) Intel Xeon E5450 3,00 GHz avec 12 Mo de cache
	système d'exploitation	Windows Server 2012[1]
	SQL Server	SQL Server 2012
	mémoire RAM	8 Go
	Configuration du disque dur (base de données)	
	utilisation de la base de données pendant 30 jours en Go	176 Go
	utilisation de la base de données pendant 90 jours en Go	528 Go
	vitesse de l'unité de disque dur de la base de données	Disques SCSI 15 000 tr/min
	configuration de l'unité de disque dur (base de données)	RAID 5 / RAID 1+0
	accès à l'unité de disque dur de la base de données	Réseau SAN Fiber Channel 2G+

Ordinateur	Elément	Recommandation
2 (Application Server)	processeur	(2) Intel Xeon E5450 3,00 GHz avec 12 Mo de cache
	système d'exploitation	Windows Server 2012[1]
	mémoire RAM	8 Go
	espace disponible sur le disque dur	36 Go
	vitesse de l'unité de disque dur (système d'exploitation)	Disques 10 000 tr/min
	configuration de l'unité de disque dur (système d'exploitation)	RAID 1+0
3, 4 et 5 (Event Collector/Agent Manager)	processeur	(1) Intel Xeon E5450 3,00 GHz avec 12 Mo de cache
	système d'exploitation	Windows Server 2012[1]
	mémoire RAM	2 Go
	espace disponible sur le disque dur	36 Go

[1]Windows Server 2012 doit être installé en mode normal ; SiteProtector ne prend pas en charge Windows Server 2012 installé en mode "noyau seul".

Remarque : Voir Chapitre 2, «Configuration matérielle et logicielle requise», à la page 5 pour connaître la configuration minimale requise et obtenir la liste de tous les systèmes d'exploitation et des serveurs de base de données pris en charge.

Déploiement multisite

Vous pouvez répartir votre déploiement sur plusieurs sites s'il devient trop volumineux.

Envisagez la répartition de votre configuration sur plusieurs sites plus petits si votre configuration en cours est trop volumineuse. Utilisez les directives et les configurations requises pour les déploiements de petite, de moyenne et de grande taille afin de choisir le déploiement le mieux adapté à chaque site.

Le déploiement multisite est constitué de plusieurs déploiements de grande taille qui se réfèrent à une instance récapitulative des sites. Utilisez le déploiement multisite dans les cas suivants :

- les critères d'évaluation de votre configuration excède les valeurs indiquées dans le déploiement de grande taille
- votre configuration est répartie sur une zone géographique très étendue

Considérations relatives à l'installation

Vous devez prendre plusieurs facteurs en compte avant d'installer le système SiteProtector.

Options d'installation

Les options d'installation de SiteProtector sont adaptées à de nombreux environnements. Des détails sont fournis dans la section Planification.

Le tableau suivant décrit les options d'installation de SiteProtector.

Option d'installation	Description
Express	Installe une version rationalisée de SiteProtector sur un ordinateur. L'option Express est prévue à des fins de test ou d'évaluation ou pour les environnements de petite taille.
Installation manuelle	Permet d'installer SiteProtector sur trois ordinateurs ou plus et offre ainsi de meilleures performances dans les environnements les plus grands. Vous pouvez ajouter des composants supplémentaires, si nécessaire.
Clustered SQL	Permet d'installer SiteProtector sur deux ordinateurs ou plus et de le configurer pour fonctionner dans un environnement de clusters SQL.

Conseil : Vous pouvez utiliser l'authentification Windows ou l'authentification SQL pour toutes ces installations de SiteProtector.

Event Collector, Agent Manager et la console SiteProtector sont inclus avec l'installation. Event Collector et Agent Manager communiquent avec la base de données du site et Application Server, et la console SiteProtector communiquent avec Application Server.

Localisation des programmes d'installation

SiteProtector fournit des programmes autonomes pour les packages d'installation de base, les composants complémentaires et les modules.

Programmes autonomes

Vous pouvez utiliser des programmes autonomes (également appelés packages) pour installer les composants de SiteProtector séparément. Ces fichiers n'étant pas installés à partir d'un emplacement central, vous devez entrer des informations supplémentaires si vous les utilisez.

Emplacement du programme d'installation

Vous pouvez accéder au programme d'installation Express depuis l'un des emplacements suivants :

- IBM Security Download Center à l'adresse https://ibmss.flexnetoperations.com.
- IBM Passport Advantage - Certains produits IBM Security vendus sur IBM Passport Advantage incluent les téléchargements logiciels de SiteProtector.

IBM Security Download Center fournit les versions les plus récentes du programme d'installation Express et de tous les packages (programmes) d'installation autonomes.

Autres éléments à prendre en compte dans une installation

D'autres éléments sont à prendre en compte avant d'installer SiteProtector. Notez qu'à partir de la version 3.0, SiteProtector n'utilise plus et ne prend plus en charge Deployment Manager.

Configuration requise supplémentaire

En plus de la configuration système requise, vous devez également respecter les conditions requises suivantes :

- Installez SiteProtector sur un ordinateur dédié.
- N'utilisez pas l'ordinateur SiteProtector comme serveur DNS ou serveur proxy.
- N'installez pas SiteProtector sur des systèmes qui ont été configurés comme contrôleurs de domaine principaux ou secondaires.

Noms de domaine dans l'installation Express

Vous devez utiliser un nom de domaine qualifié complet comportant jusqu'à 64 caractères lors de l'installation Express.

Conseil : N'utilisez pas le caractère de trait de soulignement (_) lors de la définition du nom de domaine de SiteProtector.

Archives de clé de chiffrement

Vous pouvez archiver des clés de chiffrement pour les composants suivants :

- Agent Manager
- X-Press Update Server (version autonome)

Lorsque vous installez ou désinstallez ces composants, vous êtes invité à indiquer un répertoire d'archivage. Indiquez un emplacement qui n'est pas en local, de préférence un support amovible. Les archives de clés de chiffrements peuvent simplifier la reprise après incident en cas de panne de votre serveur. Si vous n'archivez pas les clés de chiffrement, ces certificats sont détruits si vous désinstallez les composants qui utilisent ces clés. Vous devez alors redistribuer les certificats sur les clients qui communiquent avec ce serveur. Cette redistribution des certificats de serveur peut nécessiter pas mal de temps et un surcroît de travail si, par exemple, le serveur est un gestionnaire d'agents qui doit communiquer avec des milliers d'agents Desktop Endpoint Security. Cela s'applique uniquement s'il faut que vos clients valident des certificats à partir de ce serveur (options «Niveau de confiance explicite» ou «Première accréditation»).

Instructions pour sélectionner des fournisseurs de services de chiffrement

RSA est le fournisseur cryptographique par défaut de toutes les communications de SiteProtector. RSA est le fournisseur par défaut des systèmes d'exploitation Microsoft et est pris en charge par tous les produits IBM Security.

Important : Vous pouvez utiliser d'autres fournisseurs cryptographiques que ceux par défaut s'ils sont installés sur votre ordinateur mais ils ne sont pas pris en charge. Vous êtes responsable de la configuration de ces fournisseurs et de vous assurer qu'ils sont compatibles avec les agents et les composants qui communiquent avec SiteProtector.

Adresses IP et disques durs multiples

Si vous disposez de plusieurs adresses IP et de plusieurs disques durs :

- Adresses IP multiples : vous devez sélectionner l'adresse IP que les clients (composants situés sur d'autres ordinateurs) utiliseront pour communiquer avec l'ordinateur.
- Disques durs multiples : vous devez spécifier un disque dur.

Ajout manuel d'utilisateurs dans la base de données

Pour ajouter des utilisateurs manuellement à SQL Server et à la base de données du site, utilisez le format Domaine\Nom d'utilisateur. A défaut, des conflits d'utilisateur pourront se produire lors de l'installation des composants. Pour utiliser l'authentification Windows, vous devez ajouter les utilisateurs manuellement avant d'installer les composants de SiteProtector.

Microsoft Windows Server 2008

Si vous exécutez Microsoft Windows Server 2008 :

- Désactivez l'option de téléchargement renforcée. Par défaut, Microsoft Windows Server vous empêche d'ouvrir des fichiers de programme à partir d'un navigateur. Le programme d'installation vous invite à

enregistrer les fichiers et à les exécuter sur votre unité locale. Pour exécuter le programme d'installation à distance, vous devez désactiver ce paramètre de sécurité.

- Ajoutez les sites suivants à votre liste des sites de confiance avant de télécharger des fichiers depuis IBM Security Download Center :
  - https://www.iss.net
  - http://www.iss.net

Bureau à distance Windows

Lorsque vous utilisez le Bureau à distance Windows, assurez-vous que le lissage des polices est désactivé dans les paramètres du client du protocole RDP.

Cluster SQL Server

La base de données SiteProtector est le seul composant de SiteProtector que vous pouvez installer sur un cluster SQL Server.

Informations générées par les programmes d'installation

Les programmes d'installation génèrent des fichiers journaux qui contiennent des informations sur le processus d'installation. Utilisez ces informations pour l'identification et la résolution des problèmes d'installation ou lorsque vous communiquez avec le support IBM.

Fichiers journaux

Les programmes d'installation génèrent un fichier journal pour chaque composant de SiteProtector que vous installez. Les programmes d'installation créent également un fichier journal détaillé pour chaque copie en bloc des données chargées dans une table particulière de la base de données du site. Les programmes d'installation vous invitent à afficher ces journaux à la fin du programme d'installation s'il y a eu des erreurs ou des avertissements.

Préparation à l'installation de SiteProtector

Avant d'installer SiteProtector, vous devez renforcer la sécurité et mettre en place des mesures pour garantir que les systèmes sur lesquels vous installez SiteProtector sont sécurisés.

Considérations relatives à la sécurité

Avant d'installer un composant de SiteProtector sur un système, envisagez les moyens que vous pouvez mettre en oeuvre pour renforcer la sécurité du système, comme l'activation des écrans de veille ou la limitation du nombre d'applications installées.

Vous pouvez accroître la sécurité des systèmes en mettant en oeuvre les mesures suivantes :

- Activer les écrans de veille avec une autorisation par mot de passe. Cela vous permettra d'éviter l'utilisation non autorisée de SiteProtector.
- Limiter le nombre d'applications installées sur un système SiteProtector.

Ecrans de veille

Suivez ces guides de bonne pratique lorsque vous activez les écrans de veille :

- Utilisez un écran de veille avec un écran noir. Ces types d'écran de veille consomment moins d'UC ou de mémoire que d'autres écrans de veille.
- Définissez un délai d'inactivité court.
- Protégez les écrans de veille par mot de passe.

Conseil : Verrouillez le système lorsqu'il n'est pas utilisé pour empêcher tout accès non autorisé.

Limiter le nombre d'applications

Si possible, n'installez pas d'application supplémentaire sur les systèmes sur lesquels vous allez installer les composants de SiteProtector. Les applications supplémentaires peuvent introduire des risques de sécurité.

Considérations relatives à la sécurité du chiffrement Strict (SP800-131A)

La norme de Publication spéciale 800-131A (SP800-131A) du NIST (National Institute of Standards and Technology) renforce les algorithmes et augmente les longueurs de clés pour améliorer la sécurité. Avant d'installer un composant SiteProtector sur un système, vous devez décider si vous souhaitez vous conformer à la norme SP800-131A de chiffrement strict.

La norme SP800-131A offre également une période de transition pour passer à la nouvelle norme. La période de transition permet à un utilisateur de travailler dans un environnement mixte de paramètres non pris en charge par la norme et de paramètres pris en charge. Le norme SP800-131A nécessite que les utilisateurs soient configurés pour la mise en application stricte de la norme. Pour plus de détails, reportez-vous au site Web du National Institute of Standards and Technology à l'adresse http://www.nist.gov/index.html.

Pour être conforme à la norme SP800-131A, les composants doivent respecter les critères suivants.

- Utiliser le protocole TLS (Transport Layer Security) v1.2 pour sécuriser les communications entre les composants de SiteProtector. Le protocole SSL (Secure Sockets Layer) doit utiliser le protocole TLS v1.2.
- Utiliser SHA-256 ou des fonctions de hachage plus fortes.
- Utiliser la puissance 2048 bits ou des clés RSA plus fortes.

Remarque : Voir la note techique 1636383 (http://www.ibm.com/support/docview.wss?uid=swg21636383) pour plus d'informations sur les types d'agents IBM Security qui prennent en charge le chiffrement strict.

Remarque : Le mode strict conforme à la norme SP800-131A n'est pas pris en charge sur le dispositif SiteProtector.

Choisir entre le chiffrement Strict et Compatible

Lorsque vous effectuez une installation Express de SiteProtector v3.0 ou une installation d'un composant de SiteProtector v3.0, vous devez choisir entre le chiffrement Strict et le chiffrement Compatible.

- *Strict* implique l'utilisation du protocole TLS v1.2, des fonctions de hachage SHA-256 ou plus fortes et des clés RSA de puissance 2048 bits ou plus fortes uniquement.
- *Compatible* implique l'utilisation du protocole TLS v1.0, TLS v1.1 ou TLS v1.2, des fonctions de hachage SHA-1 et de la puissance de clé RSA 2048 bits.

Selon le cas, vous pouvez rencontrer deux scénarios de chiffrement :

- Strict : tous les périphériques sont configurés pour utiliser la norme SP800-131A.
- Compatible : tous les périphériques ne sont pas configurés pour utiliser la norme SP800-131A.

Remarque : Un mélange des modes Strict et Compatible n'est pas pris en charge.

Variantes d'installation

Trois différents scénarios d'installation sont possibles en ce qui concerne la norme SP800-131A.

Scénario d'installation	Processus
Mise à niveau d'une version antérieure de SiteProtector (par exemple, v2.9) vers SiteProtector v3.0	La norme SP800-131A n'est pas prise en charge dans ce cas. Vous devez effectuer une réinstallation de la version 3.0 pour bénéficier des capacités de la norme SP800-131A.
Installation Express de SiteProtector v3.0	Vous devez choisir entre les chiffrements Strict et Compatible durant le processus d'installation
Installation d'un composant de SiteProtector v3.0	Vous devez choisir entre les chiffrements Strict et Compatible pour chaque composant durant le processus d'installation. **Important :** Le choix effectué pour le premier composant s'applique automatiquement à tous les composants installés sur le même ordinateur.

Configuration de TLS v1.2 pour Internet Explorer

Vous devez configurer Internet Explorer pour utiliser le protocole TLS (Transport Layer Security) v1.2 si vous souhaitez utiliser le chiffrement strict (SP800-131A) avec SiteProtector. Seuls Internet Explorer 8 et les versions supérieures prennent en charge TLS v1.2.

Pourquoi et quand exécuter cette tâche

Internet Explorer est le navigateur pris en charge pour le système SiteProtector. Les versions suivantes d'Internet Explorer prennent en charge TLS v1.2 :

- IE 8 ou supérieur sous Microsoft Windows 7
- IE 10 sous Microsoft Windows 8
- IE 8 ou supérieur sous Windows Server 2008 R2 Standard (64 bits uniquement)
- IE 8 ou supérieur sous Windows Server 2008 R2 Enterprise (64 bits uniquement)
- IE 10 sous Windows Server 2012 Standard

Procédure

1. Ouvrez Internet Explorer.
2. Sélectionnez **Outils** > **Options Internet**.
3. Sélectionnez l'onglet **Avancé**.
4. Faites défiler jusqu'à la section **Sécurité**.
5. Cochez la case **Utiliser TLS 1.2** pour utiliser le chiffrement strict.

   Remarque : Si vous prévoyez d'utiliser Internet Explorer **uniquement** pour vous connecter à SiteProtector à l'aide du chiffrement strict et **non** pour vous connecter à d'autres sites, désélectionnez les cases suivantes :

   - **Utiliser SSL 2.0**
   - **Utiliser SSL 3.0**
   - **Utiliser TLS 1.0**
   - **Utiliser TLS 1.1**

   Si vous effectuez cette action, les autres sites qui ne prennent pas en charge TLS v1.2 ne se connecteront plus.
6. Cliquez sur **OK**.

Configuration du protocole IPsec pour sécuriser les communications de la base de données SiteProtector

Vous devez configurer IPsec entre la base de données SiteProtector et les autres composants de SiteProtector pour sécuriser les communications si vous souhaitez utiliser le chiffrement strict (SP800-131A) avec SiteProtector. Cette fonctionnalité nécessite l'utilisation du pare-feu Windows.

Pourquoi et quand exécuter cette tâche

Remarque : La configuration du protocole IPsec pour sécuriser les communications de la base de données SiteProtector n'est pas prise en charge sur les dispositifs SiteProtector.

Important : La configuration du protocole IPsec pour la base de données SiteProtector nécessite que le pare-feu Windows soit activé. Si vous utilisez IBM Security Server Protection for Windows, qui empêche par défaut le démarrage du pare-feu Windows, vous devez désinstaller IBM Security Server Protection for Windows ou désactiver manuellement le service d'agent et activer le pare-feu Windows.

Reportez-vous à la note technique 1638945 (http://www.ibm.com/support/docview.wss?uid=swg21638945) pour obtenir des instructions détaillées sur la configuration du protocole IPsec entre la base de données SiteProtector et les autres composants de SiteProtector afin de sécuriser les communications.

Préparation du système de la base de données du site

Le logiciel Microsoft SQL Server est une application de requête de base de données qui vous aide à organiser et à maintenir à jour les informations des événements SiteProtector. Toutefois, SQL Server peut rendre votre système vulnérable à certains types d'attaques. Avant d'installer SiteProtector sur le système de la base de données du site (ou un autre système sur lequel SQL Server est installé), assurez-vous que le système a été correctement préparé.

Procédure

1. Appliquez les mises à jour les plus récentes de Microsoft Windows. Vous pouvez télécharger les mises à jour depuis le site Web de Microsoft à l'adresse http://www.microsoft.com.
2. Renforcez la sécurité de SQL Server.

Préparation des systèmes sur lesquels vous allez installer un composant de SiteProtector

Avant d'installer des composants de SiteProtector, vérifiez que le système a été préparé de manière adéquate.

Procédure

1. Installez les Service Packs et les correctifs logiciels de Microsoft.
2. Vérifiez que la version la plus récente de Microsoft Internet Explorer ainsi que tous les correctifs associés sont installés.
3. Assurez-vous qu'un écran de veille est activé avec autorisation par mot de passe.

Installation des mises à jour Microsoft

Pour corriger les éventuelles failles de sécurité, mettez à jour les systèmes d'exploitation Microsoft Windows avec les derniers service packs, correctifs logiciels et correctifs de sécurité. Lorsque vous appliquez les mises à jour, suivez les pratiques recommandées, telles que les tests d'assurance qualité et les procédures de contrôle des modifications.

Mises à jour Microsoft

Microsoft fournit différents types de mise à jour : service packs, correctifs logiciels et correctifs de sécurité.

Service packs
Mises à jour cumulatives qui corrigent les problèmes connus et offrent les outils, les pilotes et les mises à jour qui étendent la fonctionnalité des produits.

Correctifs logiciels
Correctifs de produits à base de code, fournis à des clients individuels lorsqu'ils rencontrent des problèmes. Des groupes de correctifs logiciels qui subissent des tests plus rigoureux sont régulièrement incorporés aux service packs.

Correctifs de sécurité
Correctifs à base de code semblables aux correctifs logiciels, mais qui éliminent réellement les vulnérabilités en matière de sécurité. Installez les correctifs de sécurité dès que possible car ils protègent votre configuration contre les virus et les agressions.

Téléchargement des mises à jour Microsoft

Pourquoi et quand exécuter cette tâche

Téléchargez les derniers correctifs Microsoft à partir du site Web de Microsoft (http://www.microsoft.com). Vous pouvez également télécharger le service de notification des mises à jour critiques à partir de ce site Web. Après avoir installé ce service, vous serez automatiquement averti des mises à jour critiques.

Gestion des mises à jour Microsoft

Pourquoi et quand exécuter cette tâche

Microsoft fournit plusieurs utilitaires pour gérer les mises à jour si vous n'avez pas accès à Internet. Servez-vous des utilitaires décrits dans le tableau suivant pour déterminer les mises à jour à télécharger et le mode de gestion de ces mises à jour après leur installation sur votre ordinateur :

Utilitaire	Description
HFNetChk	Identifie tout correctif logiciel qui n'a pas été appliqué à votre ordinateur spécifique. **Conseil :** Exécutez cet utilitaire en mode détaillé (suffixe -v).
QChain	Vérifie que les correctifs logiciels ont été installés dans l'ordre. **Conseil :** Exécutez QChain avec le suffixe -z.
Qfecheck	Vérifie que les correctifs logiciels ont été installés correctement **Conseil :** Exécutez cet utilitaire en mode détaillé (suffixe -v).

Listes de contrôle d'installation

Ce chapitre fournit une présentation du processus et des listes de contrôle pour vous assurer que vous avez réalisé les tâches obligatoires requises sur votre site et que vous pouvez les exécuter efficacement.

Suggestion

IBM Security vous recommande d'effectuer des copies des listes de contrôle de cette section et de les utiliser pour garder une trace de votre progression. Servez-vous des cases à cocher pour marquer les tâches terminées ou éliminer les tâches qui ne s'appliquent pas à votre situation.

Liste de contrôle de pré-installation

Vous devez respecter certaines conditions et exécuter plusieurs tâches de configuration avant d'installer SiteProtector. Cette rubrique fournit une liste de contrôle pour vous aider à exécuter ces tâches.

Liste de contrôle

Le tableau suivant fournit une liste de contrôle pour vous assurer d'exécuter toutes les tâches requises avant l'installation de SiteProtector :

✓	**Tâche**
☐	Acheter les licences pour les agents que vous envisagez d'ajouter à SiteProtector et disposer des fichiers de licence pour l'installation. **Remarque :** Si vous n'avez pas reçu ces fichiers, envoyez un courrier électronique à mailto:// licenses@iss.net.
☐	Vérifier que les ordinateurs que vous utiliserez sont conformes à la configuration système requise.
☐	Obtenir les privilèges d'administrateur sur chaque ordinateur sur lequel seront installés les composants de SiteProtector, y compris les privilèges d'administrateur pour SQL Server.
☐	Déterminer l'option d'installation à utiliser.
☐	Lire le document readme qui s'applique à l'édition de SiteProtector que vous installez.
☐	Installer les logiciels tiers requis et les correctifs les plus récents. Voir *Configuration système requise de SiteProtector* pour obtenir la liste des logiciels tiers requis.
☐	Logiciels Windows renforcés et SQL Server.
☐	Ajouter les sites suivants à votre liste de sites de confiance : • https://www.iss.net • http://www.iss.net
☐	Configurer votre connexion Internet sur Application Server avec Internet Explorer.
☐	Développer une stratégie d'archivage des clés de chiffrement, par exemple les stocker à un emplacement distant ou sur un support amovible.

Liste de contrôle des informations requises

Cette rubrique fournit une liste de contrôle des informations dont vous pourrez avoir besoin pour exécuter les procédures d'installation décrites dans ce guide. Consultez cette liste de contrôle pour vous assurer de disposer de ces informations avant de commencer le processus d'installation.

Important : D'autres informations peuvent être requises pour le programme spécifique que vous installez. Ces informations sont répertoriées dans chaque rubrique.

Liste de contrôle

Le tableau suivant fournit une liste de contrôle avec les informations dont vous avez besoin avant d'installer SiteProtector :

✓	**Informations pour les programmes d'installation**
☐	Nom unique de votre site ou de vos composants permettant de les distinguer dans un environnement à plusieurs sites ou à plusieurs composants.
☐	Adresse IP ou nom de domaine complet de chaque ordinateur sur lequel est installé SiteProtector.

✓	Informations pour les programmes d'installation
☐	Nom complet de SQL Server pour l'ordinateur de la base de données du site dans l'un des formats suivants : • *NomOrdinateur* • *NomOrdinateur\InstanceNommée* • *NomOrdinateur.NomDomaine.com* • *NomOrdinateur.NomDomaine.com\InstanceNommée*
☐	Unités de l'ordinateur sur lesquelles vous voulez installer les composants de SiteProtector si plusieurs unités sont disponibles.
☐	Si vous disposez de plusieurs cartes d'interface réseau sur l'ordinateur, vous devez connaître l'adresse IP utilisée par les autres composants de SiteProtector pour communiquer avec le composant que vous installez.

Liste des tâches d'installation de l'option Express

L'option Express installe SiteProtector System sur un seul ordinateur.

Présentation des tâches

Le tableau suivant fournit un aperçu des tâches que vous devez effectuer pour installer l'option Express :

Tâche	Description
1	Télécharger le fichier du programme d'installation de SiteProtector Express (`SiteProtectorExpress-Setup.exe`) depuis IBM Security Download Center à l'adresse https://ibmss.flexnetoperations.com.
2	Installer l'option Express.
3	Vérifier que le protocole TCP/IP est activé sur l'ordinateur sur lequel vous installez SiteProtector.
4	Installer les modules facultatifs en les téléchargeant à partir du site IBM Security Download Center. Pour plus d'informations sur la configuration du composant Event Archiver, voir *IBM Security SiteProtector System - Guide de configuration*.

Liste des tâches d'installation des packages SiteProtector

Cette rubrique fournit une présentation des tâches des procédures d'installation que vous devez effectuer pour installer les packages individuels de SiteProtector.

Utilisez cette méthode si vous envisagez d'effectuer les tâches suivantes :

- Authentification Windows NT sur la base de données SQL Server
- Installation dans un environnement de cluster SQL Server
- Installez les composants SiteProtector dans une configuration autre que les options Express

Présentation des tâches

Le tableau suivant fournit une liste de contrôle des tâches d'installation avec l'authentification Windows NT :

Tâche	Description
1	Accéder aux fichiers d'installation du package à partir du site IBM Security Download Center.
2	Installer la base de données du site.

Tâche	Description
3	Installer les packages dans l'ordre suivant : 1. Java Runtime Environment 2. Application Server (qui inclut le composant X-Press Update Server et la console Web) 3. Console (qui inclut le composant Event Viewer) 4. Event Collector 5. Agent Manager
4	Installer les modules facultatifs tels qu'un composant X-Press Update Server ou Event Archiver supplémentaire. Pour plus d'informations sur la configuration du composant Event Archiver, voir *IBM Security SiteProtector System - Guide de configuration*.

Tâches de post-installation

Ces tâches permettent de s'assurer que les composants SiteProtector peuvent communiquer de manière sécurisée. Vous pouvez effectuer ces tâches après l'installation de SiteProtector et des modules facultatifs, mais avant de configurer SiteProtector

Présentation des tâches

Le tableau suivant fournit la liste des tâches de post-installation :

Tâche	Description
1	Sécuriser les communications de base de données.
2	Activer la communication par le biais de pare-feux. Voir le document *IBM Security SiteProtector System Configuring Firewalls for SiteProtector Traffic* disponible sur le site http://publib.boulder.ibm.com/infocenter/sprotect/v2r8m0/topic/com.ibm.siteprotector.doc/pdfs/sp_printable_pdfs.htm.

Etapes suivantes

Après avoir installé SiteProtector, vous devez passer au processus de configuration de SiteProtector. Lors de ce processus, vous allez effectuer toutes les tâches requises pour utiliser SiteProtector pour la première fois, par exemple :

- Ajouter des licences ou des jetons
- Configurer les agents de SiteProtector
- Mettre à jour les agents de SiteProtector
- Configurer les utilisateurs et les droits de SiteProtector
- Configurer les groupes pour les actifs de réseau
- Configurer d'autres produits IBM Security pour les utiliser avec SiteProtector
- Configurer les politiques et les réponses de sécurité
- Ajouter des actifs de réseau à SiteProtector

Pour obtenir des informations et des instructions sur ce processus, voir les manuels *IBM Security SiteProtector System - Guide de configuration* et *IBM Security SiteProtector System Policies and Responses Configuration Guide*.

Chapitre 4. Installation de SiteProtector

Ce chapitre décrit les options et les procédures utilisées pour installer SiteProtector.

Installation d'un déploiement de petite taille ou de taille moyenne à l'aide de l'installation Express

Vous pouvez utiliser l'installation Express pour installer un déploiement de petite taille ou de taille moyenne. La version de SiteProtector qui est installée est particulièrement adaptée aux évaluations, aux tests et aux environnements de petite taille. Elle inclut tous les composants par défaut de SiteProtector. Vous pouvez télécharger l'installation Express depuis IBM Security Download Center.

Préparation à l'exécution de l'installation Express

L'installation Express vous permet d'utiliser une base de données SQL Server existante sur votre ordinateur.

Pourquoi et quand exécuter cette tâche

Si une base de données SQL Server présente sur votre ordinateur n'est pas à jour, vous devez effectuer les actions suivantes, puis exécuter à nouveau l'installation Express :

- Mettez à niveau la base de données selon la configuration minimale requise.
- Désinstallez l'instance de base de données qui n'est pas en conformité avec la configuration minimale requise.

Avant d'installer l'option Express, procédez comme suit :

- Téléchargez le fichier du programme d'installation de SiteProtector Express (`SiteProtectorExpress-Setup.exe`) depuis IBM Security Download Center à l'adresse https://ibmss.flexnetoperations.com.
- Si vous disposez de plusieurs instances SQL Server sur cet ordinateur, vous devez sélectionner l'instance sur laquelle vous souhaitez installer la base de données du site.
- Pour installer une version de SQL Server dans une autre langue que l'anglais, vous devez d'abord l'installer avant d'exécuter l'installation Express.

Activation de la communication SQL Server Express via TCP/IP

Par défaut, la base de données SQL Server 2012 Express n'est pas configurée pour communiquer par le biais du protocole TCP/IP. Si vous installez une base de données de site qui utilise SQL Server Express, vous devez activer le protocole TCP/IP avant que la base de données de site ne puisse fonctionner correctement.

Procédure

1. Dans le menu Démarrer, cliquez sur **Tous les programmes** > **Microsoft SQL Server 2012** > **Outils de configuration** > **Gestionnaire de configuration SQL Server**.
2. Cliquez sur **Services SQL Server 2012**.
3. Développez le noeud **Configuration du réseau SQL Server 2012**, puis sélectionnez **Protocoles pour MSSQLServer** ***(nom de l'instance SQL)***.
4. Cliquez avec le bouton droit de la souris sur **TCP/IP**, puis cliquez sur **Activer**.
5. Sélectionnez **Services SQL Server 2012** dans l'arborescence.
6. Cliquez avec le bouton droit de la souris sur **SQL Server** ***(nom de l'instance SQL)***, puis cliquez sur **Redémarrer**.

Exécution de l'installation Express

Vous pouvez télécharger le programme d'installation Express depuis IBM Security Download Center à l'adresse https://ibmss.flexnetoperations.com.

Avant de commencer

Si vous n'avez aucune instance de SQL Server installée, vous devez installer une version prise en charge de SQL Server avant de poursuivre. Voir «Configuration requise pour l'installation Express de SiteProtector», à la page 6 pour une liste des versions de SQL Server prises en charge.

Procédure

1. Exécutez le fichier `SiteProtectorExpress-Setup.exe`. La fenêtre de bienvenue s'affiche.
2. Cliquez sur **Next**. La fenêtre de sélection de la langue apparaît.
3. Sélectionnez la langue que vous souhaitez utiliser pour SiteProtector.
4. Cliquez sur **Next**. La fenêtre du contrat de licence s'affiche.
5. Passez en revue les termes du contrat de licence, cliquez sur **I accept**, puis sur **Next**. La fenêtre de sélection d'un emplacement de destination s'affiche.
6. Sélectionnez le dossier par défaut ou sélectionnez un dossier dans la fenêtre Open, puis cliquez sur **Next**. La fenêtre Cryptographic Security Standard apparaît.
7. Sélectionnez si vous souhaitez exécuter SiteProtector en mode de chiffrage Compatible ou Strict. La fenêtre Site Name apparaît.
8. Entrez le nom du site que vous créez, puis cliquez sur **Suivant**.

   Conseil : Entrez un nom significatif pour distinguer ce site des autres sites dans un environnement multisite.
9. Si la fenêtre de SQL Server s'affiche, sélectionnez l'instance de SQL Server sur laquelle vous installez la base de données du site, puis cliquez sur **Suivant**.
10. Dans la fenêtre Encryption Key Archival, entrez l'emplacement du **dossier**, puis cliquez sur **Next**. Indiquez un dossier et un support non local, par exemple une unité réseau ou Zip.
11. Dans la fenêtre InstallShield Wizard Complete, cliquez sur **Finish**.

    Remarque : Par défaut, le programme d'installation crée automatiquement une icône Console SiteProtector dans le dossier du Bureau. Si vous ne souhaitez pas que l'icône Console SiteProtector soit créée, désélectionnez la case.

Que faire ensuite

Remarque : Si vous prévoyez d'utiliser des Comptes de domaine Windows pour accéder à la base de donnés du site, vous devez configurer les services SQL Server et SQL Agent pour s'exécuter en tant que Compte de domaine avec les droits adéquats pour exécuter SQL Server. Pour obtenir les conditions requises précises, voir la documentation relative à SQL Server.

Installation d'un déploiement de SiteProtector de taille moyenne

Les étapes répertoriées ici permettent d'installer un déploiement de SiteProtector de taille moyenne sur trois à quatre ordinateurs. Un déploiement de SiteProtector de taille moyenne inclut la base de données du site, Application Server, X-Press Update Server, la console Web, Event Viewer, Event Collector et Agent Manager.

Avant de commencer

Assurez-vous que vos ordinateurs sont conformes à la configuration requise détaillée dans la rubrique «Déploiement de taille moyenne», à la page 26 et dans les rubriques relatives aux exigences matérielles et logicielles de la section Planification.

Obtenez les privilèges d'administrateur sur chaque ordinateur sur lesquels vous avez prévu d'installer les composants de SiteProtector, y compris les privilèges d'administrateur pour Microsoft SQL Server.

Déterminez et notez les informations suivantes avant de démarrer le processus d'installation :

- Nom que vous souhaitez utiliser pour le site SiteProtector.
- Adresse IP ou nom de domaine complet de chaque ordinateur sur lesquels vous souhaitez installer les composants de SiteProtector.
- Nom complet du serveur SQL pour l'ordinateur de la base de données du site dans l'un des formats suivants :
  - *NomOrdinateur*
  - *NomOrdinateur\InstanceNommée*
  - *NomOrdinateur.NomDomaine.com*
  - *NomOrdinateur.NomDomaine.com\InstanceNommée*
- Lorsque vous installez les composants Application Server, Event Collector et Agent Manager, vous devez fournir les informations d'authentification d'un utilisateur du domaine Windows. Incluez le nom de domaine avec le nom d'utilisateur. Par exemple : *Domaine_SP\Nom_utilisateur_SP*.
- Informations d'authentification d'un utilisateur du domaine Windows avec les droits d'exécution des services.
- Tout autre nom d'utilisateur d'administrateur de clé publique du serveur.
- Si plusieurs unités sont disponibles, vous devez savoir sur quelle unité d'ordinateur vous souhaitez installer les composants de SiteProtector.
- Si vous disposez de plusieurs cartes d'interface réseau (NIC) sur l'ordinateur, vous devez connaître l'adresse IP qui sera utilisée par les autres composants de SiteProtector pour communiquer avec le composant que vous installez.
- Si vous utilisez un proxy, vous avez besoin des informations de proxy pour Internet et des informations de proxy pour Agent Manager.

Procédure

1. Accès à IBM Security Download Center à l'adresse https://ibmss.flexnetoperations.com.
2. Connectez-vous à IBM Security Download Center et cliquez sur **Download** sous l'en-tête My software.
3. Sous My Products, cliquez sur **IBM Security SiteProtector System**.
4. Sous Product Lines, cliquez sur **SiteProtector 3.0**.
5. Cliquez sur le lien **Installation Packages**.

6. Téléchargez les fichiers suivants depuis IBM Security Download Center vers un emplacement connu :

Option	Description
SiteProtectorJRE-Setup.exe	Java Runtime Environment (JRE)
SiteDatabase-Setup.exe	Base de données SiteProtector
ApplicationServer-Setup.exe	Application Server (inclut X-Press Update Server et la console Web)
Console-Setup.exe	Console (inclut Event Viewer)
EventCollector-Setup.exe	Event Collector
AgentManager-Setup.exe	Agent Manager

7. Sur le premier ordinateur, exécutez `SiteDatabase-Setup.exe` et entrez les informations requises.

   Remarque : Si vous prévoyez d'utiliser les Comptes de domaine Windows pour accéder à la base de données du site, vous devez configurer les services SQL Server et SQL Agent pour s'exécuter comme Compte de domaine avec les droits adéquats pour exécuter SQL Server. Pour obtenir les conditions requises précises, voir la documentation relative à SQL Server.
   La base de données SiteProtector est installée.
8. Sur le deuxième ordinateur, exécutez `SiteProtectorJRE-Setup.exe` pour installer Java Runtime Environment.
9. Sur le deuxième ordinateur, exécutez `ApplicationServer-Setup.exe` et entrez les informations requises. Application Server, X-Press Update Server et la console Web sont installés sur le deuxième ordinateur.
10. Sur le deuxième ordinateur, exécutez `Console-Setup.exe` et entrez les informations requises. La console et Event Viewer sont installés sur le deuxième ordinateur.
11. Sur le troisième ordinateur, exécutez `SiteProtectorJRE-Setup.exe` pour installer Java Runtime Environment.
12. Sur le troisième ordinateur, exécutez `EventCollector-Setup.exe` et entrez les informations requises. Le composant Event Collector est installé sur le troisième ordinateur.
13. Sur le troisième ordinateur, exécutez `AgentManager-Setup.exe` et entrez les informations requises. Le composant Agent Manager est installé sur le troisième ordinateur.
14. Si vous souhaitez installer les composants Event Collector et Agent Manager sur un quatrième ordinateur, exécutez `SiteProtectorJRE-Setup.exe` pour installer Java Runtime Environment.
15. Exécutez éventuellement `EventCollector-Setup.exe` sur le quatrième ordinateur et entrez les informations requises.
16. Exécutez éventuellement `AgentManager-Setup.exe` sur le quatrième ordinateur et entrez les informations requises.

Que faire ensuite

Vous pouvez télécharger et installer des composants facultatifs depuis IBM Security Download Center, par exemple un composant X-Press Update Server (`UpdateServer-Setup.exe`) supplémentaire ou le composant Event Archiver (`EventArchiver-Setup.exe`). Pour plus d'informations sur la configuration du composant Event Archiver, voir *IBM Security SiteProtector System - Guide de configuration*.

Installation d'un déploiement de SiteProtector de grande taille

Suivez les étapes répertoriées ici pour installer un déploiement de SiteProtector de grande taille sur quatre ou cinq ordinateurs. Un déploiement de SiteProtector de grande taille inclut la base de données du site, Application Server, X-Press Update Server, la console Web, Event Viewer, Event Collector et Agent Manager.

Avant de commencer

Assurez-vous que votre ordinateur respecte la configuration requise détaillée dans la rubrique «Déploiement de grande taille», à la page 27 et dans les rubriques relatives aux exigences matérielles et logicielles de la section Planification.

Obtenez les privilèges d'administrateur sur chaque ordinateur sur lesquels vous avez prévu d'installer les composants de SiteProtector, y compris les privilèges d'administrateur pour Microsoft SQL Server.

Déterminez et notez les informations suivantes avant de démarrer le processus d'installation :

- Nom que vous souhaitez utiliser pour le site SiteProtector.
- Adresse IP ou nom de domaine complet de chaque ordinateur sur lesquels vous souhaitez installer les composants de SiteProtector.
- Nom complet du serveur SQL pour l'ordinateur de la base de données du site dans l'un des formats suivants :
  - *NomOrdinateur*
  - *NomOrdinateur\InstanceNommée*
  - *NomOrdinateur.NomDomaine.com*
  - *NomOrdinateur.NomDomaine.com\InstanceNommée*
- Lorsque vous installez les composants Application Server, Event Collector et Agent Manager, vous devez fournir les informations d'authentification d'un utilisateur du domaine Windows. Incluez le nom de domaine avec le nom d'utilisateur. Par exemple : *Domaine_SP\Nom_utilisateur_SP*.
- Informations d'authentification d'un utilisateur du domaine Windows avec les droits d'exécution des services.
- Tout autre nom d'utilisateur d'administrateur de clé publique du serveur.
- Si plusieurs unités sont disponibles, vous devez savoir sur quelle unité d'ordinateur vous souhaitez installer les composants de SiteProtector.
- Si vous disposez de plusieurs cartes d'interface réseau (NIC) sur l'ordinateur, vous devez connaître l'adresse IP qui sera utilisée par les autres composants de SiteProtector pour communiquer avec le composant que vous installez.
- Si vous utilisez un proxy, vous avez besoin des informations de proxy pour Internet et des informations de proxy pour Agent Manager.

Procédure

1. Accès à IBM Security Download Center à l'adresse https://ibmss.flexnetoperations.com.
2. Connectez-vous à IBM Security Download Center et cliquez sur **Download** sous l'en-tête My software.
3. Sous My Products, cliquez sur **IBM Security SiteProtector System**.
4. Sous Product Lines, cliquez sur **SiteProtector 3.0**.
5. Cliquez sur le lien **Installation Packages**.
6. Téléchargez les fichiers suivants depuis IBM Security Download Center vers un emplacement connu :

Option	Description
SiteProtectorJRE-Setup.exe	Java Runtime Environment (JRE)
SiteDatabase-Setup.exe	Base de données SiteProtector
ApplicationServer-Setup.exe	Application Server (inclut X-Press Update Server et la console Web)
Console-Setup.exe	Console (inclut Event Viewer)
EventCollector-Setup.exe	Event Collector

Option	Description
AgentManager-Setup.exe	Agent Manager

7. Sur le premier ordinateur, exécutez SiteDatabase-Setup.exe et entrez les informations requises.

   Remarque : Si vous prévoyez d'utiliser les Comptes de domaine Windows pour accéder à la base de données du site, vous devez configurer les services SQL Server et SQL Agent pour s'exécuter comme Compte de domaine avec les droits adéquats pour exécuter SQL Server. Pour obtenir les conditions requises précises, voir la documentation relative à SQL Server.
   La base de données SiteProtector est installée.
8. Sur le deuxième ordinateur, exécutez SiteProtectorJRE-Setup.exe pour installer Java Runtime Environment.
9. Sur le deuxième ordinateur, exécutez ApplicationServer-Setup.exe et entrez les informations requises. Application Server, X-Press Update Server et la console Web sont installés sur le deuxième ordinateur.
10. Sur le deuxième ordinateur, exécutez Console-Setup.exe et entrez les informations requises. La console et Event Viewer sont installés sur le deuxième ordinateur.
11. Sur le troisième ordinateur, exécutez SiteProtectorJRE-Setup.exe pour installer Java Runtime Environment.
12. Sur le troisième ordinateur, exécutez EventCollector-Setup.exe et entrez les informations requises. Le composant Event Collector est installé sur le troisième ordinateur.
13. Sur le troisième ordinateur, exécutez AgentManager-Setup.exe et entrez les informations requises. Le composant Agent Manager est installé sur le troisième ordinateur.
14. Sur le quatrième ordinateur, exécutez SiteProtectorJRE-Setup.exe pour installer Java Runtime Environment.
15. Sur le quatrième ordinateur, exécutez EventCollector-Setup.exe et entrez les informations requises. Le composant Event Collector est installé sur le quatrième ordinateur.
16. Sur le quatrième ordinateur, exécutez AgentManager-Setup.exe et entrez les informations requises. Le composant Agent Manager est installé sur le quatrième ordinateur.
17. Si vous souhaitez installer les composants Event Collector et Agent Manager sur un cinquième ordinateur, exécutez SiteProtectorJRE-Setup.exe pour installer Java Runtime Environment.
18. Sur le cinquième ordinateur, exécutez éventuellement EventCollector-Setup.exe et entrez les informations requises.
19. Sur le cinquième ordinateur, exécutez éventuellement AgentManager-Setup.exe et entrez les informations requises.

Que faire ensuite

Vous pouvez télécharger et installer des composants facultatifs depuis IBM Security Download Center, par exemple un composant X-Press Update Server (UpdateServer-Setup.exe) supplémentaire ou le composant Event Archiver (EventArchiver-Setup.exe). Pour plus d'informations sur la configuration du composant Event Archiver, voir *IBM Security SiteProtector System - Guide de configuration*.

Installation de SiteProtector sur un cluster SQL Server

Le cluster SQL Server peut utiliser l'authentification SQL ou l'authentification Windows, mais pas la confiance implicite. Les instructions ci-dessous s'appliquent à l'authentification SQL et à l'authentification Windows.

Avant de commencer

Assurez-vous que vos ordinateurs sont conformes aux exigences détaillées dans la rubrique qui décrit votre type de déploiement et dans les rubriques relatives aux exigences matérielles et logicielles de la section Planification.

Obtenez les privilèges d'administrateur sur chaque ordinateur sur lesquels vous avez prévu d'installer les composants de SiteProtector, y compris les privilèges d'administrateur pour Microsoft SQL Server.

Déterminez et notez les informations suivantes avant de démarrer le processus d'installation :

- Nom que vous souhaitez utiliser pour le site SiteProtector.
- Adresse IP ou nom de domaine complet de chaque ordinateur sur lesquels vous souhaitez installer les composants de SiteProtector.
- Nom complet du serveur SQL pour l'ordinateur de la base de données du site dans l'un des formats suivants :
  - *NomOrdinateur*
  - *NomOrdinateur\InstanceNommée*
  - *NomOrdinateur.NomDomaine.com*
  - *NomOrdinateur.NomDomaine.com\InstanceNommée*
- Lorsque vous installez les composants Application Server, Event Collector et Agent Manager, vous devez fournir les informations d'authentification d'un utilisateur du domaine Windows. Incluez le nom de domaine avec le nom d'utilisateur. Par exemple : *Domaine_SP\Nom_utilisateur_SP*.
- Informations d'authentification d'un utilisateur du domaine Windows avec les droits d'exécution des services.
- Tout autre nom d'utilisateur d'administrateur de clé publique du serveur.
- Si plusieurs unités sont disponibles, vous devez savoir sur quelle unité d'ordinateur vous souhaitez installer les composants de SiteProtector.
- Si vous disposez de plusieurs cartes d'interface réseau (NIC) sur l'ordinateur, vous devez connaître l'adresse IP qui sera utilisée par les autres composants de SiteProtector pour communiquer avec le composant que vous installez.
- Si vous utilisez un proxy, vous avez besoin des informations de proxy pour Internet et des informations de proxy pour Agent Manager.

Procédure

1. Accès à IBM Security Download Center à l'adresse https://ibmss.flexnetoperations.com.
2. Connectez-vous à IBM Security Download Center et cliquez sur **Download** sous l'en-tête My software.
3. Sous My Products, cliquez sur **IBM Security SiteProtector System**.
4. Sous Product Lines, cliquez sur **SiteProtector 3.0**.
5. Cliquez sur le lien **Installation Packages**.
6. Téléchargez les fichiers suivants depuis IBM Security Download Center vers un emplacement connu :

Option	Description
SiteProtectorJRE-Setup.exe	Java Runtime Environment (JRE)
SiteDatabase-Setup.exe	Base de données SiteProtector
ApplicationServer-Setup.exe	Application Server (inclut X-Press Update Server et la console Web)
Console-Setup.exe	Console (inclut Event Viewer)
EventCollector-Setup.exe	Event Collector

Option	Description
AgentManager-Setup.exe	Agent Manager

7. Installez le certificat SSL sur tous les noeuds du cluster.

   Remarque : Pour plus d'informations sur l'installation d'un certificat SSL, consultez l'une des pages Web Microsoft suivantes :
   - Comment activer le chiffrement SSL pour SQL Server 2005 (http://support.microsoft.com/kb/318605/en-us) avec le serveur de certificats
   - Comment activer le chiffrement SSL pour SQL Server 2005 avec la console de gestion Microsoft (http://support.microsoft.com/kb/316898/en-us)
   - Comment activer le chiffrement SSL pour SQL Server 2008 et 2008 R2 (http://technet.microsoft.com/en-us/library/ms189067%28v=sql.105%29.aspx)
   - Comment activer le chiffrement SSL pour SQL Server 2012 (http://technet.microsoft.com/en-us/library/ms191192%28v=sql.110%29.aspx)
8. Installez la base de données SiteProtector à partir du package `SiteDatabase-Setup.exe` en suivant les invites et en entrant les informations requises.

   Important : N'installez rien d'autre que la base de données SiteProtector sur l'ordinateur sur lequel le cluster SQL est installé.

   Remarque : Si vous prévoyez d'utiliser les Comptes de domaine Windows pour accéder à la base de données du site, vous devez configurer les services SQL Server et SQL Agent pour s'exécuter en tant que Compte de domaine avec les droits adéquats pour exécuter SQL Server. Pour obtenir les conditions requises précises, voir la documentation relative à SQL Server.
9. Sur le deuxième ordinateur, exécutez `SiteProtectorJRE-Setup.exe` pour installer Java Runtime Environment.
10. Sur le deuxième ordinateur, exécutez `ApplicationServer-Setup.exe` et entrez les informations requises.

    Remarque : Le composant Application Server nécessite le certificat SSL pour pouvoir communiquer avec la base de données Site Database. Le programme d'installation d'Application Server vérifie que vous l'installez sur une plateforme de cluster et recherche le certificat SSL requis. Si le certificat n'est pas disponible, SSL est alors désactivé.
    Application Server, X-Press Update Server et la console Web sont installés sur le deuxième ordinateur.
11. Sur le deuxième ordinateur, exécutez `Console-Setup.exe` et entrez les informations requises. La console et Event Viewer sont installés sur le deuxième ordinateur.
12. Sur le troisième ordinateur, exécutez `SiteProtectorJRE-Setup.exe` pour installer Java Runtime Environment.
13. Sur le troisième ordinateur, exécutez `EventCollector-Setup.exe` et entrez les informations requises. Le composant Event Collector est installé sur le troisième ordinateur.
14. Sur le troisième ordinateur, exécutez `AgentManager-Setup.exe` et entrez les informations requises. Le composant Agent Manager est installé sur le troisième ordinateur.
15. Si vous souhaitez installer les composants Event Collector et Agent Manager sur un quatrième ordinateur, exécutez `SiteProtectorJRE-Setup.exe` pour installer Java Runtime Environment.
16. Exécutez éventuellement `EventCollector-Setup.exe` sur le quatrième ordinateur et entrez les informations requises.
17. Exécutez éventuellement `AgentManager-Setup.exe` sur le quatrième ordinateur et entrez les informations requises.

Que faire ensuite

Vous pouvez télécharger et installer des composants facultatifs depuis IBM Security Download Center, par exemple un composant X-Press Update Server (`UpdateServer-Setup.exe`) supplémentaire ou le composant Event Archiver (`EventArchiver-Setup.exe`). Pour plus d'informations sur la configuration du composant Event Archiver, voir *IBM Security SiteProtector System - Guide de configuration*.

Installation de SiteProtector sur une plateforme 64 bits

Vous pouvez installer SiteProtector sur une plateforme Windows 64 bits ou SQL Server 64 bits Enterprise. Les instructions référencées ici s'appliquent à l'authentification SQL et à l'authentification Windows.

Pourquoi et quand exécuter cette tâche

Remarque : Tous les systèmes doivent être dans le même domaine et les comptes de domaine Windows doivent être utilisés.

Suivez l'une des procédures ci-dessous pour installer SiteProtector sur une plateforme 64 bits :

- «Installation d'un déploiement de petite taille ou de taille moyenne à l'aide de l'installation Express», à la page 41
- «Installation d'un déploiement de SiteProtector de taille moyenne», à la page 43
- «Installation d'un déploiement de SiteProtector de grande taille», à la page 44
- «Installation de SiteProtector sur un cluster SQL Server», à la page 46

Installation de SiteProtector lorsque vous utilisez l'authentification Windows NT

Lorsque vous installez SiteProtector sur un réseau qui utilise l'authentification Windows NT, vous devez installer chaque composant séparément. Vous pouvez obtenir les packages d'installation des composants depuisIBM Security Download Center à l'adresse https://ibmss.flexnetoperations.com.

Avant de commencer

Vous devez disposer des informations suivantes :

- Nom du serveur SQL Server
- Données d'authentification d'un utilisateur Windows NT avec le droit d'exécuter les services
- Nom du serveur Application Server
- Autres noms d'utilisateur éventuels d'administrateurs de clé publique du serveur
- Nom du site
- Emplacement d'Agent Manager
- Nom et mot de passe de compte d'authentification pour Agent Manager

  Remarque : Ceci crée un compte sur le serveur X-Press Update Server permettant d'interagir avec Agent Manager.
- (Facultatif) Nom de groupe SiteProtector
- Informations de proxy pour Internet
- Informations de proxy d'Agent Manager

L'environnement JRE SiteProtector doit être installé avant d'installer le composant Event Collector.

Remarque : Si vous envisagez d'utiliser des Comptes de domaine Windows pour accéder à la base de données du site, vous devez configurer les services SQL Server et SQL Agent pour s'exécuter en tant que compte de domaine avec les droits appropriés pour exécuter SQL Server. Pour obtenir les conditions requises précises, voir la documentation relative à SQL Server.

Pourquoi et quand exécuter cette tâche

Vous devez installer les packages individuels dans l'ordre suivant :

1. Site Database
2. Java Runtime Environment
3. Application Server (qui inclut X-Press Update Server et la console Web)
4. Console (qui inclut Event Viewer)
5. Event Collector
6. Agent Manager
7. Autres packages, comme un serveur X-Press Update Server supplémentaire et Event Archiver

Procédure

1. Téléchargez les packs de composants depuis IBM Security Download Center à l'adresse https://ibmss.flexnetoperations.com.
2. Suivez les instructions d'installation d'un déploiement de petite, moyenne ou grande taille. Choisissez le déploiement qui convient le mieux à la taille de votre réseau.

Chapitre 5. Installation de composants supplémentaires

Vous pouvez installer des composants supplémentaires, notamment une autre console, Event Collector, Agent Manager, X-Press Update Server et Event Viewer. Vous pouvez également installer un composant Event Archiver.

Présentation de composants supplémentaires

Comprendre comment les composants de SiteProtector fonctionnent ensemble est essentiel.

La figure suivante présente les dépendances entre les composants. Les composants supplémentaires installés après l'installation initiale sont représentés avec des lignes en pointillé dans la figure suivante :

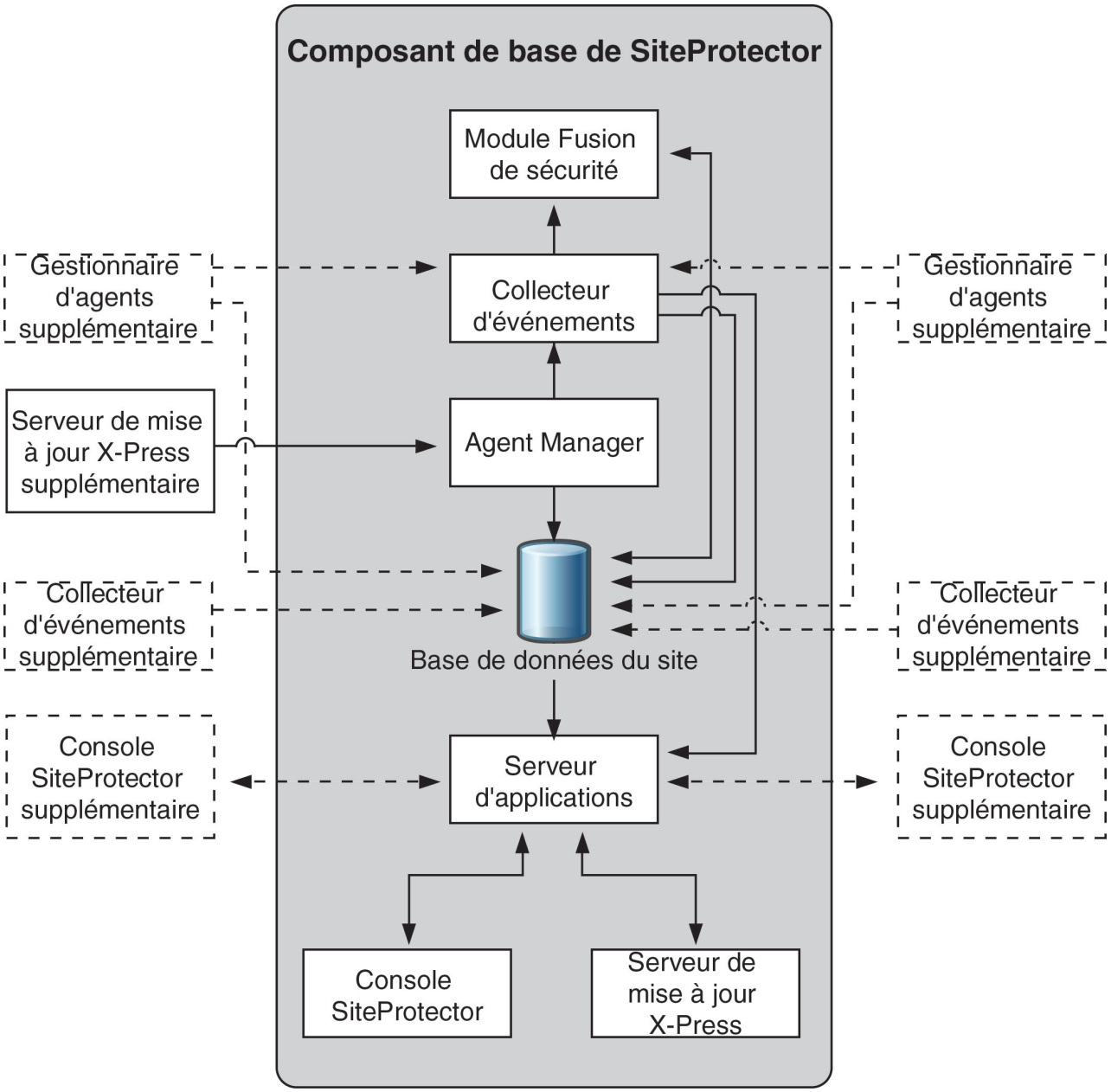

Figure 2. Composants de SiteProtector et flux d'événements

Le tableau suivant fournit une liste de composants supplémentaires que vous pouvez envisager d'installer et décrit brièvement les motifs qui vous pousseront à les installer.

Composant	Motif d'installation
Agent Manager	• Assurer l'évolutivité pour travailler avec un grand nombre d'agents • Le réseau est partitionné en différentes zones géographiques
Console	Fournir à plusieurs utilisateurs leur propre console pour contrôler SiteProtector.
Event Collector	Prendre en charge plus d'agents que vous ne le pouvez avec vos collecteurs d'événements actuels. Un composant Event Collector est installé avec l'installation Express.
Event Viewer	Contrôler les événements sur un ordinateur qui n'a aucun autre composant de SiteProtector installé.
Event Archiver	Stocker les données d'événement et améliorer les performances en réduisant le nombre d'événements que la base de données du site doit stocker.
X-Press Update Server	Regrouper en cluster les serveurs X-Press Update Server pour améliorer les performances et permettre la reprise en ligne si nécessaire.

Installation d'un autre composant Console

Après avoir installé SiteProtector, vous pouvez souhaiter installer des consoles SiteProtector supplémentaires. Cela permet à plusieurs utilisateurs de surveiller SiteProtector à distance. Lorsque vous installez une console SiteProtector supplémentaire, un composant Event Viewer supplémentaire est automatiquement installé.

Procédure

1. Accès à IBM Security Download Center à l'adresse https://ibmss.flexnetoperations.com.
2. Connectez-vous à IBM Security Download Center et cliquez sur **Download** sous l'en-tête My software.
3. Sous My Products, cliquez sur **IBM Security SiteProtector System**.
4. Sous Product Lines, cliquez sur **SiteProtector 3.0**.
5. Cliquez sur le lien **Installation Packages**.
6. Téléchargez le package `Console-Setup.exe` vers un emplacement connu.
7. Exécutez `Console-Setup.exe`.
8. Suivez les invites d'installation et entrez les informations requises. La console et le composant Event Viewer sont installés sur l'ordinateur.

Installation d'un autre composant Event Collector

Envisagez l'installation d'un autre composant Event Collector pour la prise en charge d'agents supplémentaires dans votre environnement. Après l'installation de ce composant supplémentaire, vous devez rediriger les agents vers lui.

Avant de commencer

Vous devez installer Java Runtime Environment (JRE) avant d'installer le composant Event Collector.

Procédure

1. Accès à IBM Security Download Center à l'adresse https://ibmss.flexnetoperations.com.
2. Connectez-vous à IBM Security Download Center et cliquez sur **Download** sous l'en-tête My software.
3. Sous My Products, cliquez sur **IBM Security SiteProtector System**.
4. Sous Product Lines, cliquez sur **SiteProtector 3.0**.
5. Cliquez sur le lien **Installation Packages**.

6. Téléchargez les packages `SiteProtectorJRE-Setup.exe` et `EventCollector-Setup.exe` vers un emplacement connu.
7. Exécutez `SiteProtectorJRE-Setup.exe` pour installer Java Runtime Environment.
8. Exécutez `EventCollector-Setup.exe`.
9. Suivez les invites d'installation et entrez les informations requises. Le composant Event Collector est installé sur l'ordinateur.
10. Redirigez les agents vers le composant Event Collector :
    a. Sélectionnez l'agent.
    b. Sélectionnez **Action** > **Configure Agents** > **Assign Event Collector**. La page Assign Event Collector s'affiche.
    c. Sélectionnez le nouveau composant Event Collector et cliquez sur **OK**.

Installation d'un autre composant Agent Manager

Envisagez l'installation d'un autre composant Agent Manager si votre environnement contient un grand nombre d'agents ou s'il est dispersé géographiquement. Chaque instance d'Agent Manager doit être installée sur un système séparé.

Avant de commencer

Vous devez installer Java Runtime Environment (JRE) avant d'installer le composant Agent Manager.

Pourquoi et quand exécuter cette tâche

Si votre environnement utilise Network Address Translation (NAT), envisagez d'affecter une adresse IP personnalisée à Agent Manager lorsque le programme d'installation vous invite à entrer une adresse IP. Vous devez sélectionner l'option qui désactive la liste des adresses IP actuellement affectées à la carte d'interface réseau (NIC), puis entrer l'adresse IP personnalisée dans la zone **Custom IP address**.

Procédure

1. Accès à IBM Security Download Center à l'adresse https://ibmss.flexnetoperations.com.
2. Connectez-vous à IBM Security Download Center et cliquez sur **Download** sous l'en-tête My software.
3. Sous My Products, cliquez sur **IBM Security SiteProtector System**.
4. Sous Product Lines, cliquez sur **SiteProtector 3.0**.
5. Cliquez sur le lien **Installation Packages**.
6. Téléchargez les packages `SiteProtectorJRE-Setup.exe` et `AgentManager-Setup.exe` vers un emplacement connu.
7. Exécutez `SiteProtectorJRE-Setup.exe` pour installer Java Runtime Environment.
8. Exécutez `AgentManager-Setup.exe`.
9. Suivez les invites d'installation et entrez les informations requises. Le composant Agent Manager est installé sur l'ordinateur.

Installation d'un autre composant Event Viewer

Vous pouvez installer un composant Event Viewer sur un système sans autre composant de SiteProtector installé, si vous pouvez vous connecter à un autre Event Collector et un autre Application Server. Cela permet d'obtenir un accès quasiment en temps réel aux informations d'événements de sécurité. (L'installation Express installe automatiquement un composant Event Viewer sur le même système que la console.)

Procédure

1. Accès à IBM Security Download Center à l'adresse https://ibmss.flexnetoperations.com.
2. Connectez-vous à IBM Security Download Center et cliquez sur **Download** sous l'en-tête My software.
3. Sous My Products, cliquez sur **IBM Security SiteProtector System**.
4. Sous Product Lines, cliquez sur **SiteProtector 3.0**.
5. Cliquez sur le lien **Installation Packages**.
6. Téléchargez les packages `SiteProtectorJRE-Setup.exe` et `EventViewer-Setup.exe` vers un emplacement connu.
7. Exécutez `SiteProtectorJRE-Setup.exe` pour installer Java Runtime Environment.
8. Exécutez `EventViewer-Setup.exe`.
9. Suivez les invites d'installation et entrez les informations requises. Le composant Event Viewer est installé sur l'ordinateur.

Installation d'un autre composant XPU Server

Suivez ces instructions pour installer un composant X-Press Update (XPU) Server supplémentaire.

Avant de commencer

Important : N'installez pas XPU Server sur le même ordinateur que le composant Agent Manager. Autrement, les performances d'Agent Manager pourraient en être affectées.

Procédure

1. Accédez à IBM Security Download Center à l'adresse https://ibmss.flexnetoperations.com.
2. Connectez-vous à IBM Security Download Center et cliquez sur **Download** sous l'en-tête My software.
3. Sous My Products, cliquez sur **IBM Security SiteProtector System**.
4. Sous Product Lines, cliquez sur **SiteProtector 3.0**.
5. Cliquez sur le lien **Installation Packages**.
6. Téléchargez le package `UpdateServer-Setup.exe` vers un emplacement connu.
7. Exécutez `UpdateServer-Setup.exe`. La fenêtre de bienvenue de l'assistant InstallShield s'affiche.
8. Cliquez sur **Next**. La fenêtre du contrat de licence s'affiche.
9. Passez en revue les termes du contrat de licence, cliquez sur **I Accept**, puis sur **Next**. La fenêtre de sélection d'un emplacement de destination s'affiche.
10. Sélectionnez un dossier de destination, puis cliquez sur **Next**. La fenêtre X-Press Update Server Configuration (Specify Manager location) s'affiche.
11. Renseignez les zones suivantes, puis cliquez sur **Next** :

zone	Description
Name	Nom du composant Agent Manager auquel XPU Server se connectera. **Exemple :** AgentManager_100
Address (IP or DNS)	Adresse IP ou DNS d'hébergement du composant Agent Manager.
Port	Port que doit utiliser XPU Server pour communiquer avec Agent Manager. (3995 est le port par défaut.)
Account Name	Nom d'utilisateur que doit utiliser XPU Server pour établir la communication avec Agent Manager.
Password	Mot de passe que XPU Server doit utiliser pour établir la communication avec Agent Manager.

La fenêtre X-Press Update Server Configuration (Specify SiteProtector Group Name) s'affiche.

12. Renseignez les zones suivantes, puis cliquez sur **Next** :

zone	Description
SiteProtector Group Name	Nom du groupe sur lequel placer XPU Server. Si vous laissez cette zone vide, SiteProtector System met le composant XPU Server dans la zone des actifs non regroupés.
X-Press Update Server security mode	Un des modes suivants : • Trust all, qui permet à d'autres serveurs de se connecter à XPU Server à chaque tentative de connexion. Aucun certificat n'est utilisé pour l'authentification. • First time trust, qui permet à d'autres serveurs de se connecter à ce composant XPU Server une seule fois. Après la première connexion, XPU Server utilise le certificat du serveur de connexion pour authentifier toutes les futures connexions. • Explicit trust, qui nécessite que le composant XPU Server utilise un certificat local pour authentifier le serveur auquel il se connecte.
Primary IP	Si l'ordinateur local comporte plusieurs interfaces réseau, sélectionnez l'adresse IP qui sera utilisée pour les communications de XPU Server.
Address (IP or DNS)	Si XPU Server nécessite un accès via un pare-feu ou un serveur proxy, entrez l'adresse IP ou le DNS du pare-feu ou du serveur proxy.
Port	Port via lequel XPU Server accèdera au pare-feu ou au serveur proxy.

La fenêtre Archival: Private Key Archival s'affiche.

13. Dans la case **Folder**, entrez un emplacement sur lequel vous voulez archiver les clés privées, puis cliquez sur **Next**.

    Conseil : IBM Security recommande d'archiver les clés sur un support amovible.
    La fenêtre Ready to Install the Program s'affiche.
14. Cliquez sur **Install**. La fenêtre InstallShield Wizard Complete s'affiche.
15. Cliquez sur **Finish**.

Résultats

Le composant X-Press Update Server supplémentaire est installé sur l'ordinateur.

Installation du composant Event Archiver

Vous pouvez installer le composant Event Archiver pour archiver les données d'événement et améliorer les performances de la base de données. Le composant Event Archiver réduit le nombre d'événements que la base de données du site doit stocker. (Le composant Event Archiver n'est pas inclus dans toutes les offres tarifaires de SiteProtector.)

Avant de commencer

Vous devez disposer des informations suivantes :

- Nom d'hôte ou adresse IP du système sur lequel est installé Agent Manager
- Nom du serveur Application Server
- (Facultatif) Nom et mot de passe du compte pour Agent Manager
- (Facultatif) Nom de groupe de SiteProtector

Procédure

1. Accès à IBM Security Download Center à l'adresse https://ibmss.flexnetoperations.com.
2. Connectez-vous à IBM Security Download Center et cliquez sur **Download** sous l'en-tête My software.
3. Sous My Products, cliquez sur **IBM Security SiteProtector System**.
4. Sous Product Lines, cliquez sur **SiteProtector 3.0**.
5. Cliquez sur le lien **Installation Packages**.
6. Téléchargez le package `EventArchiver-Setup.exe` vers un emplacement connu.
7. Cliquez sur le lien **Installation Packages**.
8. Exécutez `EventArchiver-Setup.exe`.
9. Suivez les invites d'installation et entrez les informations requises. Le composant Event Archiver est installé sur l'ordinateur.

Chapitre 6. Traitement des incidents liés à l'installation

Identification et résolution des problèmes d'une installation ratée

Pourquoi et quand exécuter cette tâche

Le processus de réparation d'une installation ratée est plus simple à comprendre si vous comprenez le fonctionnement d'une installation standard de SiteProtector :

- Si l'installation de la base de données du site échoue, le programme d'installation n'installe aucun autre composant.
- Si l'installation d'un composant autre que la base de données du site échoue, le programme d'installation continue d'installer les autres composants sélectionnés.

Pour réparer une installation ratée, vous devez réinstaller les composants :

- Pour la base de données du site, désinstallez chaque composant de SiteProtector et réinstallez-les.

  ATTENTION :
  Si vous réinstallez uniquement la base de données du site, SiteProtector ne reprend pas sont état de préinstallation.
- Pour chaque composant à l'exception de la base de données du site, exécutez à nouveau le programme d'installation de ce composant.
- Si l'installation de plusieurs composants échoue, veillez à respecter leur ordre d'installation.

Problèmes d'installation

Cette section contient des informations sur les problèmes d'installation courants et leur résolution.

La connexion issApp existe déjà

Lors de l'installation du composant Application Server, une erreur indique que la connexion au serveur d'applications issApp existe déjà, puis le processus d'installation s'interrompt.

Erreur

En général, cette erreur se produit lorsque vous tentez d'installer le composant Application Server après une désinstallation ayant échoué. Si le service Application Server ou le service Sensor Controller ne peut pas être arrêté durant le processus de désinstallation, la connexion issApp est toujours en cours d'utilisation et ne peut pas être supprimée de la base de données du site.

Solution

1. Assurez-vous que les deux services (ou applications, selon le cas) sont arrêtés.
2. Utilisez SQL Server 2005/2008/2012 Management Studio pour supprimer manuellement la connexion issApp existante, qui se trouve dans le dossier `/Security/Logins` de la base de données du site.

Impossible de supprimer la connexion au composant Event Collector

Lorsque vous désinstallez le composant Event Collector, une erreur indique que la connexion à `<machine>_EventCollector` ne peut pas être supprimée car le service est en cours d'exécution, puis le processus de désinstallation s'interrompt.

Exécutez l'une des tâches suivantes :

- Si vous désinstallez la base de données du site, désinstallez la base de données, puis répétez le processus de désinstallation pour le composant Event Collector.
- Si vous ne désinstallez pas la base de données du site, arrêtez le service issDaemon, puis répétez le processus de désinstallation du composant Event Collector. Si le processus de désinstallation continue, mais qu'un avertissement vous indique que la connexion existe toujours, utilisez SQL Server 2005/2008/2012 Management Studio pour supprimer manuellement la connexion **EventCollector_<ordinateur>** existante, située dans le dossier `/Security/Logins` de la base de données du site.

Tâches associées:

«Désinstallation d'un composant de SiteProtector», à la page 61
Suivez cette procédure pour désinstaller un composant de SiteProtector.

Impossible d'arrêter le composant Event Collector

Vous avez supprimé les composants Application Server et Console, mais vous ne parvenez pas à arrêter Event Collector.

Effectuez l'une des tâches suivantes :

- Supprimez la base de données du site.
- Si vous ne supprimez pas la base de données du site, contactez le support IBM pour obtenir de l'aide afin d'arrêter manuellement le composant Event Collector.

Tâches associées:

«Désinstallation d'un composant de SiteProtector», à la page 61
Suivez cette procédure pour désinstaller un composant de SiteProtector.

La base de données est en cours d'utilisation

Lors de la désinstallation de la base de données du site, une erreur indique que la base de données est en cours d'utilisation.

Utilisez SQL Server 2005/2008/2012 Management Studio pour arrêter manuellement tous les processus associés à la base de données du site, puis désinstallez la base de données.

Tâches associées:

«Désinstallation d'un composant de SiteProtector», à la page 61
Suivez cette procédure pour désinstaller un composant de SiteProtector.

Chapitre 7. Désinstallation

Désinstallation d'un composant de SiteProtector

Suivez cette procédure pour désinstaller un composant de SiteProtector.

Procédure

1. Cliquez sur **Démarrer** sur la barre des tâches, puis sélectionnez **Programmes** > **ISS** > **SiteProtector** > **Uninstall SiteProtector**. La page de sélection des composants s'affiche.
2. Sélectionnez un ou plusieurs composants à supprimer, puis cliquez sur **Uninstall**. Un message s'affiche avec la liste des composants sélectionnés.
3. Cliquez sur **Yes**.
4. Si la fenêtre SQL Login Password s'affiche, effectuez l'une des actions suivantes :
   - Si vous n'avez pas supprimé la base de données, entrez l'ID utilisateur et le mot de passe de connexion SQL.
   - Si vous n'avez pas supprimé la base de données, ou si le composant ne parvient pas à se connecter à la base de données pour une raison autre qu'un mot de passe incorrect, sélectionnez la case à cocher **Do not connect to the database**.
5. Si le programme n'arrive pas à supprimer un composant correctement, effectuez l'une des actions suivantes :
   - Si c'est la première fois que vous essayez de supprimer le composant, passez à l'étape 1 et relancez la désinstallation du composant.
   - Si vous avez essayé de supprimer le composant plus d'une fois, cliquez sur Yes pour consulter le fichier journal, puis contactez le support IBM si vous avez besoin d'assistance.
6. Cliquez sur **OK**, puis redémarrez votre ordinateur.

Référence associée:

«Impossible de supprimer la connexion au composant Event Collector», à la page 59
Lorsque vous désinstallez le composant Event Collector, une erreur indique que la connexion à `<machine>_EventCollector` ne peut pas être supprimée car le service est en cours d'exécution, puis le processus de désinstallation s'interrompt.

«Impossible d'arrêter le composant Event Collector», à la page 60
Vous avez supprimé les composants Application Server et Console, mais vous ne parvenez pas à arrêter Event Collector.

«La base de données est en cours d'utilisation», à la page 60
Lors de la désinstallation de la base de données du site, une erreur indique que la base de données est en cours d'utilisation.

Désinstallation de SiteProtector

Cette rubrique explique comment désinstaller complètement SiteProtector. Dans la plupart des cas, vous devez supprimer tous les composants de SiteProtector en même temps.

Pourquoi et quand exécuter cette tâche

L'ordre de suppression des composants est important.

Important : Si vous supprimez les composants en sélectionnant **Uninstall SiteProtector** par le biais du menu Démarrer comme décrit ci-dessous, le programme de désinstallation supprime automatiquement les composants dans l'ordre adéquat.

Si vous supprimez les composants via le Panneau de configuration de Windows, vous devez les supprimer dans l'ordre suivant :

1. SiteProtector Console
2. X-Press Update Server
3. Agent Manager
4. Application Server
5. Event Collector
6. SecurityFusion Module
7. Site Database

Si vous avez installé SiteProtector sur plusieurs ordinateurs, supprimez les composants dans l'ordre, ordinateur par ordinateur.

Procédure

1. Cliquez sur **Démarrer** sur la barre des tâches, puis sélectionnez **Programmes** > **ISS** > **SiteProtector** > **Uninstall SiteProtector**.
2. Sélectionnez tous les composants installés, puis cliquez sur **Uninstall**. Le message SiteProtector Installation répertorie les composants que vous avez choisis de supprimer.
3. Cliquez sur **Yes**. Un message s'affiche pour indiquer que la suppression des composants a abouti.
4. Si le programme n'arrive pas à supprimer un composant correctement, effectuez l'une des actions suivantes :
   - Si c'est la première fois que vous essayez de supprimer le composant, répétez les étapes 1 à 3 et essayez à nouveau de supprimer le composant.
   - Si vous avez essayé de supprimer le composant plus d'une fois, cliquez sur Yes pour afficher le fichier journal. Contactez le support IBM pour obtenir de l'aide.
5. Cliquez sur **OK**, puis redémarrez votre ordinateur.

Chapitre 8. Sécurisation des communications de la base de données

Les communications entre la base de données du site et les composants de SiteProtector ne sont pas automatiquement activées. La base de données du site contient des informations sensibles sur la sécurité de votre réseau, envisagez donc de chiffrer et d'authentifier les communications de la base de données à l'aide de SSL (Secure Socket Layers).

Protocoles de chiffrement

Vous pouvez utiliser SSL (Secure Socket Layers) pour sécuriser les communications entre la base de données du site et les composants de SiteProtector.

Utilisez le protocole de chiffrement SSL (Secure Sockets Layer) pour sécuriser les communications de la base de données. Le chiffrement SSL nécessite l'achat de certificats. Pour en savoir plus, voir l'article de Microsoft *Encrypting Connections to SQL Server* : http://msdn.microsoft.com/en-us/library/ms189067.aspx

Activation du chiffrement SSL

Vous devez activer SSL manuellement sur les composants Event Collector, Application Server et Agent Manager et le module SecurityFusion, si les composants ne sont pas installés sur le même système que la base de données du site.

Considérations relatives au chiffrement SSL

Remarque : Si vous choisissez d'utiliser SSL, vous devez installer le certificat de SQL Server sur tous les ordinateurs qui utiliseront SSL pour accéder à la base de données du site.

Activation de SSL sur le composant Event Collector

Vous pouvez activer SSL (Secure Socket Layers) sur le composant Event Collector pour sécuriser les communications de la base de données.

Avant de commencer

Vous devez disposer des privilèges suivants :

- Privilèges d'administrateur de SiteProtector
- Privilèges d'administrateur système sur la base de données du site

Procédure

1. Sur l'ordinateur sur lequel le composant Event Collector est installé, localisez la source de données ODBC du module en exécutant l'un des programmes suivants à partir de la boîte de dialogue de recherche ou d'exécution du menu Démarrer :
   - Pour les systèmes 32 bits, exécutez `%systemroot%\System32\odbcad32.exe`
   - Pour les systèmes 64 bits, exécutez `%systemroot%\SysWoW64\odbcad32.exe`
2. Dans la fenêtre ODBC Data Source Administrator, sélectionnez l'onglet **System DSN** (Système DNS).
3. Sélectionnez **RSNTEventCollector**.
4. Cliquez sur **Configurer**, puis sur **Suivant**.
5. Entrez les informations de connexion, cliquez sur **Suivant**, puis à nouveau sur **Suivant**.

6. Sélectionnez **Utiliser le chiffrement renforcé pour les données**, puis cliquez sur **Terminer**.
7. Dans la fenêtre du récapitulatif, cliquez sur **Tester la source de données** pour vous assurer que tout fonctionne correctement.
8. Si le test ne fonctionne pas, voir l'article de Microsoft référencé à la rubrique «Protocoles de chiffrement», à la page 63 pour déterminer le problème.
9. Depuis la console SiteProtector, arrêtez et redémarrez le composant Event Collector.

Activation de SSL sur le composant Application Server

Vous pouvez activer SSL (Secure Socket Layers) sur le serveur d'applications pour sécuriser les communications de la base de données.

Avant de commencer

Vous devez disposer des privilèges suivants :

- Privilèges d'administrateur de SiteProtector
- Privilèges d'administrateur système sur la base de données du site

Procédure

1. Sur l'ordinateur sur lequel le composant Application Server est installé, localisez le fichier `geronimo-ra.xml`. Vous devez modifier le paramètre jdbc dans ce fichier.

   Conseil : Dans une installation standard, il se trouve dans le dossier suivant :

   ```
   C:\Program Files\ISS\SiteProtector\JavaEE\Geronimo2.1.8\repository\iss\
   SPDataSource\1.0\SPDataSource-1.0.rar\rar\META-INF\geronimo-ra.xml
   ```

2. Modifiez la ligne suivante :

   `jdbc:jtds:sqlserver://`*`computer name`*`:1433/RealSecureDB;ssl=off`

   de sorte qu'elle se présente comme suit :

   `jdbc:jtds:sqlserver://`*`computer name`*`:1433/RealSecureDB;ssl=require`

3. Sur le même ordinateur (sur lequel Application Server est installé), localisez la source de données ODBC du module.

   Conseil : Elle est nommée IssADReconciler et il s'agit d'un DSN système.

4. Sélectionnez la source de données, cliquez sur **Configurer**, puis sur **Suivant**.
5. Entrez les informations de connexion, cliquez sur **Suivant**, puis à nouveau sur **Suivant**.
6. Sélectionnez **Utiliser le chiffrement renforcé pour les données**, puis cliquez sur **Terminer**.
7. Dans la fenêtre du récapitulatif, cliquez sur **Tester la source de données** pour vous assurer que tout fonctionne correctement.
8. Si le test ne fonctionne pas, voir l'article de Microsoft référencé à la rubrique «Protocoles de chiffrement», à la page 63 pour déterminer le problème.
9. A partir d'une console SiteProtector, arrêtez et redémarrez le service ISS Application Server.

Activation de SSL sur le composant Agent Manager

Vous pouvez activer Secure Socket Layers (SSL) sur le composant Agent Manager pour sécuriser les communications de la base de données.

Avant de commencer

Vous devez disposer des privilèges suivants :

- Privilèges d'administrateur de SiteProtector
- Privilèges d'administrateur système sur la base de données du site

Procédure

1. Localisez le répertoire d'installation d'Agent Manager, puis ouvrez le fichier RSSPDC.INI dans un éditeur de texte.
2. Recherchez la propriété nommée **dbEncrypt**, puis affectez-lui la valeur «1».
3. Enregistrez, puis fermez le fichier.
4. A partir d'une console SiteProtector, arrêtez et redémarrez le composant Agent Manager.

   Remarque : Si le composant Agent Manager ne démarre pas car il n'arrive pas à communiquer avec la base de données du site, le système consigne les erreurs dans un journal. Voir l'article de Microsoft référencé à la rubrique «Protocoles de chiffrement», à la page 63 pour déterminer le problème.

Activation de SSL sur le module SecurityFusion

Vous pouvez activer SSL (Secure Socket Layers) sur le module SecurityFusion pour sécuriser les communications de la base de données.

Avant de commencer

Vous devez disposer des privilèges suivants :

- Privilèges d'administrateur de SiteProtector
- Privilèges d'administrateur système de la base de données du site

Procédure

1. Dans la console SiteProtector, localisez le module SecurityFusion que vous souhaitez mettre à jour.
2. Cliquez avec le bouton droit de la souris sur le module SecurityFusion et sélectionnez **Manage Policy**. FusionPolicy s'affiche.
3. Cliquez avec le bouton droit de la souris sur FusionPolicy et sélectionnez **Open**. FusionPolicy s'affiche dans Policy Editor.
4. Dans l'arborescence de gauche, sélectionnez **Advanced Settings**.
5. Dans l'arborescence, sélectionnez **Encrypt communications with the Site database using SSL**.

   ATTENTION :
   Voir l'aide avant d'activer cette option.
6. Enregistrez les paramètres et fermez Policy Editor.
7. Depuis une console SiteProtector, sélectionnez le module SecurityFusion à mettre à jour et appliquez les règles modifiées au détecteur.

   Remarque : Si le module SecurityFusion ne démarre pas car il ne peut pas communiquer avec la base de données du site, le système génère des erreurs dans un journal. Voir l'article de Microsoft référencé à la rubrique «Protocoles de chiffrement», à la page 63 pour déterminer le problème.

Annexe A. Agents et dispositifs pris en charge

SiteProtector prend en charge les agents et les dispositifs produits par IBM Security. Cette rubrique contient la liste des produits pris en charge, avec les informations de modèle et de version.

Produit (par ordre alphabétique)	Modèle	Version
IBM Proventia Network Multi-Function Security (MFS)	MX0804	4.6 (pris en charge) 4.1 à 4.5 (effort optimal)
	MX1004	4.6 (pris en charge) 4.1 à 4.5 (effort optimal)
	MX3006	4.6 (pris en charge) 4.1 à 4.5 (effort optimal)
	MX4006	4.6 (pris en charge) 4.1 à 4.5 (effort optimal)
	MX5008	4.6 (pris en charge) 4.1 à 4.5 (effort optimal)
	MX5010	4.6 (pris en charge) 4.1 à 4.5 (effort optimal)
	MX5010A	4.6 (pris en charge) 4.1 à 4.5 (effort optimal)
	MX5110	4.6 (pris en charge) 4.1 à 4.5 (effort optimal)
	MX5110A	4.6 (pris en charge) 4.1 à 4.5 (effort optimal)
IBM RealSecure Server Sensor	pour AIX	7.0 SR 4.3
	pour Solaris	7.0 SR 4.4
	pour HP-UX	7.0 SR 4.1
	pour Windows	7.0 SR 4.4
IBM Security Network Intrusion Prevention System (IPS)	G400	Tous les modèles
	G2000	Tous les modèles

Produit (par ordre alphabétique)	Modèle	Version
IBM Security Network Intrusion Prevention System (IPS) Modèles GX	GC1200	
	GX3002	
	GX4002	GX4002-C
	GX4004	GX4004-C
	GX5008	GX5008-C GX5008-CF
	GX5108	GX5108-C GX5108-CF
	GX5208	
	GX6116	
	GX7800	GX7800SFP
	GX7412	
	GX7412-10	
	GX7412-05	
IBM Security Network Protection	XGS 5100	5.1
IBM Security QRadar Vulnerability Manager		7,2
IBM Security Server Protection	pour Windows	2.2
IBM Security Virtual Server Protection	pour VMware	1.1
Proventia Desktop Endpoint Security		8.0, 9.0, 10.0, 10.1
Proventia Network Anomaly Detection System	AD5003	4.0
	AD5100	4.0
	AD5200	4.0
	AD5300	4.0
Proventia Network Enterprise Scanner	ES750	
	ES1500	
Proventia Network Internet Scanner		7.0 Service Pack 2
Proventia Server	pour Linux	1.0, 1.5, 1.5.2
	pour Windows	1.0, 2.0, 2.1

Annexe B. Contacter le support IBM

Le support IBM fournit une assistance pour les défauts de produit, répond aux questions courantes et aide les utilisateurs à résoudre les incidents liés au produit.

Avant de commencer

Avant de contacter le support IBM, commencez par rechercher une réponse ou une solution à l'aide d'autres options :

- Reportez-vous à la rubrique Support portfolio dans le document *Software Support Handbook* pour plus d'informations sur les types de support disponibles.
- Consultez les notes techniques IBM, disponibles via le portail de support IBM.

Si vous ne parvenez pas à trouver une réponse ou une solution dans le portefeuille de support ou dans les notes techniques IBM, vérifiez que votre entreprise ou organisation dispose d'un contrat de maintenance IBM actif et que vous êtes autorisé à soumettre un problème à IBM, avant de contacter le support IBM.

Procédure

Pour contacter le support IBM :

1. Définissez l'incident, collectez les informations d'arrière-plan et identifiez la gravité de l'incident. Pour plus d'informations, voir la rubrique Getting IBM support du manuel *Software Support Handbook*.
2. Rassemblez les informations de diagnostic.
3. Soumettez l'incident au support IBM de l'une des manières suivantes :
   - En utilisant IBM Support Assistant (ISA), si l'outil Demande de service est activé sur votre produit.
     - Toute donnée collectée peut être jointe à la demande de service. En utilisant ISA de cette manière, vous pouvez accélérer l'analyse et réduire le délai de résolution.
   - En ligne via le portail du support IBM : vous pouvez ouvrir, mettre à jour et afficher l'ensemble des demandes de service depuis le portlet de demande de service dans la page correspondante.
   - Par téléphone pour les problèmes critiques, de panne de système ou de gravité 1. Pour obtenir le numéro de téléphone à composer dans votre région, consultez la page Web Directory of worldwide contacts.

Résultats

Si le problème que vous voulez soumettre concerne un défaut logiciel ou une documentation manquante ou imprécise, le support IBM crée un rapport officiel d'analyse de programme (APAR). Ce rapport décrit le problème de manière détaillée. Dès que possible, le support IBM propose une solution de contournement que vous pouvez implémenter jusqu'à ce que l'APAR soit résolu et qu'une solution vous soit proposée. IBM publie les APAR résolus sur le site Web du support IBM quotidiennement afin que les personnes qui rencontrent le même problème puissent profiter de cette solution.

Mentions légales

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
Armonk, NY 10504-1785
U.S.A.

Pour le Canada, veuillez adresser votre courrier à :

IBM Director of Commercial Relations
IBM Canada Ltd.
3600 Steeles Avenue East
Markham, Ontario
L3R 9Z7
Canada

Les informations sur les licences concernant les produits utilisant un jeu de caractères double octet peuvent être obtenues par écrit 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 paragraphe suivant ne s'applique ni au Royaume-Uni, ni dans aucun pays dans lequel il serait contraire aux lois locales. 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 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 Corporation
Project Management
C55A/74KB
6303 Barfield Rd.,
Atlanta, GA 30328
U.S.A

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.

Toute instruction relative aux intentions d'IBM pour ses opérations à venir est susceptible d'être modifiée ou annulée sans préavis, et doit être considérée uniquement comme un objectif.

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 sur la page Web Copyright and trademark information, accessible à l'adresse www.ibm.com/legal/copytrade.shtml.

Linux est une marque de Linus Torvalds aux Etats-Unis et/ou dans certains autres pays.

UNIX est une marque enregistrée de The Open Group aux Etats-Unis et/ou dans certains autres pays.

Microsoft et Windows sont des marques de Microsoft Corporation aux Etats-Unis et/ou dans certains autres pays.

Remarques relatives aux règles de confidentialité

Les produits logiciels IBM, notamment les solutions SaaS (Software-as-a-Service, solutions de logiciel sous forme de services), ("Offres logicielles") peuvent utiliser des cookies ou d'autres technologies pour collecter des informations sur l'utilisation des produits, afin de contribuer à améliorer l'acquis de l'utilisateur final et de personnaliser les interactions avec celui-ci, ou à d'autres fins. Dans la plupart des cas, aucune information identifiant la personne n'est collectée par les Offres logicielles. Certaines de nos offres logicielles peuvent vous permettre de collecter des informations identifiant la personne. Si cette offre logicielle utilise des cookies pour collecter des informations identifiant la personne, des informations spécifiques sur l'utilisation de cookies par cette offre sont présentées ci-après.

Cette offre logicielle n'utilise pas de cookies ni aucune autre technologie afin de collecter des informations personnellement identifiables.

Si les configurations déployées pour cette Offre logicielle vous fournissent à vous en tant que client la possibilité de collecter des informations identifiant d'autres personnes via des cookies et d'autres technologies, vous devez vous renseigner sur l'avis juridique et les lois applicables à ce type de collecte de données, notamment les exigences d'information et de consentement.

Pour plus d'informations sur l'utilisation des différentes technologies, notamment les cookies, à ces fins, reportez-vous aux règles de confidentialité d'IBM à l'adresse http://www.ibm.com/privacy et à la Déclaration IBM de confidentialité sur Internet à l'adresse http://www.ibm.com/privacy/details/us/en, sections "Cookies, pixels espions et autres technologies" et "Produits logiciels et SaaS".

Déclaration de bonnes pratiques de sécurité

La sécurité des systèmes informatiques implique la protection des systèmes et des informations via la prévention, la détection et la réponse aux accès incorrects depuis l'intérieur et l'extérieur de votre entreprise. Un accès incorrect peut se traduire par l'altération, la destruction, l'inadaptation ou la mauvaise utilisation des informations ou être à l'origine de dommages ou d'usage abusif de vos systèmes, notamment dans le cadre d'attaques envers d'autres systèmes. Aucun système ou produit informatique ne doit être considéré comme complètement sécurisé et aucun produit, service ou mesure de sécurité unique ne peut être complètement efficace en matière de prévention d'un usage ou d'un accès abusif. 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.

Index