IBM Security AppScan Source for Analysis
Version 9.0.3.7

Guide d'utilisation pour macOS

IBM Security AppScan Source for Analysis
Version 9.0.3.7

Guide d'utilisation pour macOS

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.

Chapitre 1. Présentation d'AppScan Source for Analysis

Cette section décrit comment AppScan Source for Analysis s'intègre dans la solution AppScan Source complète et fournit une base pour la compréhension du flux de travaux d'assurance logicielle.

Présentation d'IBM Security AppScan Source

IBM® Security AppScan Source offre une valeur optimale à tous les utilisateurs de votre entreprise jouant un rôle dans la sécurité logicielle. Que vous soyez analyste de la sécurité, professionnel de l'assurance qualité, développeur ou responsable en matière de sécurité, les produits AppScan Source vous apportent les fonctionnalités, la souplesse et la puissance dont vous avez besoin sur votre ordinateur.

L'ensemble de produits comprend :

- **AppScan Source for Analysis** : Plan de travail permettant de configurer les applications et les projets, d'examiner du code, d'effectuer des analyses, des tests et d'agir en cas de vulnérabilités prioritaires.
- **AppScan Source for Automation** : Permet d'automatiser les principaux aspects du flux de travaux AppScan Source et d'intégrer la sécurité aux environnements de construction pendant le cycle de vie de développement logiciel.
- **AppScan Source for Development** : Les plug-in Developer intègrent de nombreuses fonctions d'AppScan Source for Analysis à Microsoft Visual Studio, au plan de travail Eclipse et à Rational Application Developer for WebSphere Software (RAD). Cela permet aux développeurs de rechercher les vulnérabilités et de les corriger pendant le processus de développement. Le plug-in Eclipse vous permet d'examiner le code source pour détecter les vulnérabilités de sécurité ; vous pouvez aussi l'utiliser pour examiner des projets IBM MobileFirst Platform.

Pour augmenter la valeur de AppScan Source dans votre entreprise, les produits incluent ces composants :

- **Base de connaissances de sécurité AppScan Source Security** : Informations en contexte sur chaque vulnérabilité, offrant des descriptions précises sur les causes premières, la gravité du risque et des conseils de résolution concrets.
- **AppScan Enterprise Server** : La plupart des produits et composants AppScan Source doivent communiquer avec un serveur AppScan Enterprise Server. Si vous ne disposez pas d'un tel serveur, vous pouvez utiliser AppScan Source for Development en mode local, mais les fonctions telles que les règles personnalisées, les configurations d'examen partagées et les filtres partagés ne seront pas disponibles.

  Ce serveur fournit des fonctionnalités de gestion centralisée des utilisateurs et un mécanisme de partage d'évaluations via la base de données AppScan Source. Le serveur inclut un composant Enterprise Console facultatif. Si votre administrateur installe ce composant, vous pouvez publier des évaluations depuis AppScan Source for Analysis, AppScan Source for Automation et l'interface de ligne de commande (CLI) d'AppScan Source. Le composant Enterprise Console offre divers outils de gestion des évaluations, tels que des fonctions de génération de rapports, de gestion de problème et d'analyse de tendance, ainsi que des tableaux de bord.

Important : Pour certaines versions d'AppScan Source et d'AppScan Enterprise, le niveau de version et d'édition des deux produits doit correspondre pour se connecter depuis AppScan Source au serveur AppScan Enterprise Server. Voir http://www.ibm.com/support/docview.wss?uid=swg21975211 pour savoir quelles versions d'AppScan Source et d'AppScan Enterprise sont compatibles.

Remarque :

- AppScan Enterprise Server n'est pas pris en charge sur macOS.
- Si vous disposez d'une licence de serveur de base, le serveur n'est accessible que par dix (10) connexions simultanées au maximum depuis les produits AppScan. Avec une licence de serveur Premium, un nombre illimité de connexions est autorisé.

Important : Au cours de l'examen, le client AppScan Enterprise Server et le client AppScan Source (sauf AppScan Source for Development) requièrent une connexion directe à la base de données AppScan Source (solidDB ou Oracle).

Cette Offre Logiciels n'utilise pas de cookies ou d'autres techniques pour collecter des informations personnelles identifiables.

Langues nationales traduites

Les interfaces utilisateur AppScan Source sont disponibles dans les langues suivantes :

- Anglais
- Portugais brésilien
- Chinois simplifié
- Chinois traditionnel
- Allemand
- Espagnol
- Français
- Italien
- Japonais
- Coréen
- Russe

Conformité avec la législation en vigueur aux Etats-Unis

La conformité aux réglementations du gouvernement des Etats-Unis relatives aux technologies de l'information et à la sécurité permet d'éviter que les ventes ne soient entravées. Elle fournit également une preuve aux prospects du monde entier que l'objectif d'IBM est de proposer les produits les plus sûrs de l'industrie. Cette rubrique répertorie les normes et instructions prises en charge par AppScan Source.

Internet Protocol version 6 (IPv6)

AppScan Source est activé pour IPv6, avec les exceptions suivantes :

- La saisie d'adresses numériques IPv6 n'est pas prise en charge et un nom d'hôte doit être entré à la place. La saisie d'adresses numériques IPv4 est prise en charge.
- IPv6 n'est pas pris en charge lors de la connexion à Rational Team Concert.

Federal Information Processing Standard (FIPS)

Sur les plateformes Windows et Linux prises en charge par AppScan Source, AppScan Source prend en charge FIPS Publication 140-2, à l'aide d'un module cryptographique FIPS 140-2 validé et d'algorithmes approuvés. Sur les plateformes macOS prises en charge par AppScan Source, des étapes manuelles sont requises pour opérer en mode FIPS 140-2.

Pour des informations pertinentes relatives à la conformité d'AppScan Source à la norme FIPS, et pour savoir comment activer et désactiver le mode FIPS 140-2 d'AppScan Source, reportez-vous aux notes techniques suivantes :

- Operating AppScan Source version 8.7 or later in FIPS 140-2 mode on macOS
- How to enable/disable/verify FIPS 140-2 mode in AppScan Source (Linux and Windows)
- Background information about AppScan Source version 8.7 or later FIPS 140-2 support

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-131a

Les instructions NIST SP 800-131A expliquent la gestion des clés cryptographiques. Ces instructions incluent notamment :

- Les procédures de gestion des clés
- La manière d'utiliser les algorithmes de cryptographie
- Les algorithmes à utiliser et leurs puissances minimales
- Les longueurs de clé pour des communications sécurisées

Les organismes gouvernementaux et les institutions financières suivent les instructions NIST SP 800-131A pour garantir la conformité des produits aux exigences requises en matière de sécurité.

Les instructions NIST SP 800-131A sont prises en charge uniquement si AppScan Source fonctionne en mode FIPS 140-2. Pour plus de détails sur l'activation et la désactivation du mode FIPS 140-2 d'AppScan Source, voir «Federal Information Processing Standard (FIPS)».

Important : Si le serveur AppScan Enterprise Server auquel vous allez vous connecter est activé pour la conformité avec NIST 800-131a, vous devez définir AppScan Source pour qu'il force Transport Layer Security V1.2. Si la fonction Transport Layer Security V1.2 n'est pas forcée, les connexions au serveur échoueront.

- Si vous **n'installez pas** la base de données AppScan Source (par exemple, vous installez uniquement les composants client), vous pouvez forcer Transport Layer Security V1.2 en modifiant `<data_dir>\config\ounce.ozsettings` (où `<rép_données>` est l'emplacement de vos données de programme AppScan

Source, comme décrit dans «Installation et emplacements des fichiers de données utilisateur», à la page 292)). Dans ce fichier, repérez le paramètre suivant :

```
<Setting
   name="tls_protocol_version"
   read_only="false"
   default_value="0"
   value="0"
   description="Minor Version of the TLS Connection Protocol"
   type="text"
   display_name="TLS Protocol Version"
   display_name_id=""
   available_values="0:1:2"
   hidden="false"
   force_upgrade="false"
 />
```

Dans ce paramètre, modifiez `value="0"` en `value="2"`, puis enregistrez le fichier.

- Si vous installez la base de données AppScan Source, vous pouvez forcer Transport Layer Security V1.2 dans l'outil de configuration d'IBM Security AppScan Enterprise Server après avoir installé AppScan Source et Enterprise Server.

Machines Windows 7 configurées pour utiliser USGCB (United States Government Configuration Baseline)

AppScan Source prend en charge l'examen des applications sur les machines Windows 7 qui sont configurées avec la spécification USGCB.

Remarque : Sur les machines qui sont configurées avec la spécification USGCB, AppScan Source ne prend pas en charge l'intégration du système de suivi des défauts à HP Quality Center ou Rational ClearQuest.

Nouveautés dans AppScan Source

Découvrez les nouvelles fonctions qui ont été ajoutées à AppScan Source et notez les fonctions et fonctionnalités devenues obsolètes dans cette édition.

Nouveautés dans AppScan Source version 9.0.3.7

Nouveau support d'examen amélioré

- Le système d'exploitation Red Hat Enterprise Linux (RHEL) version 7.3 est désormais pris en charge.
- L'application d'AppScan Source for Development (plug-in Visual Studio) à Visual Studio 2015 est maintenant prise en charge.

Fonctions et options qui ne sont plus prises en charge dans AppScan Source version 9.0.3.7

A compter de AppScan Source version 9.0.3.7 :

- Le système d'exploitation OS X Version 10.10 n'est plus pris en charge.
- Xcode Version 6.3 n'est plus pris en charge. L'analyse des projets Objective-C avec cette version de Xcode n'est plus prise en charge.
- Les versions 5 et 6 de Tomcat ne sont plus prises en charge.

Nouveautés d'AppScan Source version 9.0.3.6

- «Nouveau support d'examen amélioré»
- «Fonctions et options qui ne sont plus prises en charge dans AppScan Source version 9.0.3.6»

Nouveau support d'examen amélioré

- Xcode 8.1 et 8.2 for Objective-C (pour applications iOS uniquement) sont désormais des compilateurs pris en charge sous macOS. La prise en charge de ces versions de Xcode est rétroactive jusqu'à AppScan Source version 9.0.3.5.

Fonctions et options qui ne sont plus prises en charge dans AppScan Source version 9.0.3.6

A compter de AppScan Source version 9.0.3.6 :

- Le système d'exploitation Red Hat Enterprise Linux version 5 n'est plus pris en charge.
- Les compilateurs Oracle WebLogic Server versions 8, 9 et 10 ne sont plus pris en charge.

Nouveautés dans AppScan Source version 9.0.3.5

- «Nouveau support d'examen amélioré»
- «La prise en charge de l'analyse incrémentielle pour la source et le bytecode Java permet de procéder à de nouvelles analyses plus rapidement et plus efficacement.»

Nouveau support d'examen amélioré

- macOS version 10.12 est désormais un système d'exploitation pris en charge. La prise en charge de macOS version 10.12 est rétroactive jusqu'à AppScan Source version 9.0.3.4.
- Xcode 8.0, 8.1 et 8.2 for Objective-C (pour applications iOS uniquement) sont désormais des compilateurs pris en charge sous macOS.

La prise en charge de l'analyse incrémentielle pour la source et le bytecode Java permet de procéder à de nouvelles analyses plus rapidement et plus efficacement.

Depuis la version 9.0.3.5, vous pouvez activer la prise en charge de l'analyse incrémentielle Java sous Windows et Linux. Lorsque l'analyse incrémentielle est activée, les données d'analyse sont mises en cache par AppScan Source. Lorsque vous procédez à une nouvelle analyse de votre projet ou de votre application, AppScan Source utilise ces données pour déterminer les changements de code et

seules les parties de code étant impactées par ces changements sont de nouveau analysées. Le résultat final est une analyse complète de votre code en un temps record.

Cette fonction est compatible avec IBM Security AppScan Source for Analysis, le Plug-in Eclipse AppScan Source for Development, IBM Security AppScan Source for Automation ou l'interface de ligne de commande (CLI) d'IBM Security AppScan Source.

Nouveautés dans AppScan Source version 9.0.3.4

Nouveau support d'examen amélioré

PHP version 7.0 peut désormais être examiné sous Windows et Linux dans IBM Security AppScan Source for Analysis, IBM Security AppScan Source for Automation, et l'interface de ligne de commande (CLI) d'interface de ligne de commande (CLI) d'IBM Security AppScan Source.

La publication d'évaluations dans AppScan Enterprise Console est désormais prise en charge lors d'une authentification CAC (Common Access Card).

Si vous utilisez l'authentification CAC pour vous connecter à AppScan Enterprise Server, vous pouvez à présent publier des évaluations dans AppScan Enterprise Console depuis l'interface utilisateur d'AppScan Source, l'interface de ligne de commande (CLI) d'AppScan Source et AppScan Source for Automation.

Prise en charge de rapport Payment Card Industry Data Security Standard (PCI DSS) version 3.2

AppScan Source prend désormais en charge le rapport de Payment Card Industry Data Security Standard (PCI DSS) version 3.2.

Documentation du produit AppScan Source for Analysis

A compter la version 9.0.3.4, lorsque vous utilisez l'option de menu **Aide** > **Contenu de l'aide** dans AppScan Source for Analysis, l'aide en ligne de AppScan Source d'IBM Knowledge Center s'affiche (pour la version 9.0.3.4, l'aide s'affiche dans la documentation de IBM Security AppScan Source version 9.0.3.4). De même,

lorsque vous cliquez sur les liens dans la vue Bienvenue dans AppScan Source for Analysis, ils s'affichent dans IBM Knowledge Center.

AppScan Source for Analysis propose aussi une aide contextuelle pour de nombreuses vues, pages de préférence et boîtes de dialogue. Le raccourci clavier pour l'aide contextuelle est F1 sous Windows, Maj+F1 sous Linux et commande+F1 sous macOS. Cette aide contextuelle s'affiche également dans AppScan Source, dans IBM Knowledge Center à compter de la version 9.0.3.4.

Si vous utilisez le produit sans connexion Internet, l'aide est disponible localement, comme suit :

- Le fichier Readme et les notes sur l'édition de IBM Security AppScan Source sont disponibles dans le fichier `readme.html` qui se trouve dans votre répertoire d'installation de AppScan Source.
- Ces guides d'utilisation au format PDF se trouvent dans le répertoire `doc/<lang>` ou `doc\<lang>` de votre répertoire d'installation de AppScan Source (où `<lang>` est la langue nationale de votre installation de AppScan Source) :
  - Windows et Linux uniquement : *IBM Security AppScan Source for Analysis - Guide d'utilisation* (`Security_AppScan_Source_Analysis.pdf`)
  - Windows et Linux uniquement : *Utilitaires IBM Security AppScan Source - Guide d'utilisation* (`Security_AppScan_Source_Utilities.pdf`)
  - macOS uniquement : *IBM Security AppScan Source for Analysis - Guide d'utilisation pour macOS* (`Security_AppScan_Source_Analysis_OSX.pdf`)
  - macOS uniquement : *Utilitaires IBM Security AppScan Source - Guide d'utilisation pour macOS* (`Security_AppScan_Source_Utilities_OSX.pdf`)
  - *IBM Security AppScan Source - Guide d'installation et d'administration* (`Security_AppScan_Source_Installation_and_Administration.pdf`)

  Adobe Acrobat Reader est requis pour lire ces fichiers. Si vous n'avez pas Acrobat Reader, vous devez le télécharger à partir du site http://www.adobe.com/.
- La documentation Javadoc de certaines fonctions de AppScan Source for Analysis se trouve dans le répertoire `doc/Javadoc` or `doc\Javadoc` de votre répertoire d'installation de AppScan Source. A compter la version 9.0.3.4, la documentation Javadoc de ces fonctions est disponible :
  - La documentation Javadoc des classes et des méthodes de l'API de l'infrastructure d'importation du serveur d'application est disponible dans `doc/Javadoc/appserverimporter` ou `doc\Javadoc\appserverimporter`.
  - La documentation Javadoc des classes et des méthodes de l'API Framework for Frameworks est disponible dans `doc/Javadoc/frameworks` ou `doc\Javadoc\frameworks`.

  Dans ces dossiers, ouvrez le fichier `index.html`.

Possibilité d'utiliser des configurations d'examen dans AppScan Source for Analysis afin de supprimer les résultats de filtres d'exclusion

Les filtres d'exclusion contiennent des règles en fonction desquelles des types de vulnérabilité, des interfaces de programme d'application (API), des fichiers, des répertoires, ou des règles de trace sont supprimés des résultats. Si vous incluez plusieurs filtres d'exclusion dans une configuration d'examen, il se peut qu'ils entrent en conflit et que ceci affecte les résultats. Par exemple, en supposant ces deux filtres :

- Le filtre 1 supprime tous les résultats sur le type de vulnérabilité `Validation.EncodingRequired`. Il n'est pas inversé. Ces constatations sont donc exclues de l'évaluation.
- Le filtre 2 supprime tous les résultats sur le type de vulnérabilité `Validation.Required`. Il n'est pas inversé et donc ces résultats sont exclus de l'évaluation.

Si ces deux filtres sont utilisés dans une configuration d'examen, ils se neutralisent mutuellement par défaut. Le filtre 1 exclura les constatations `Validation.EncodingRequired`, mais il inclura les constatations `Validation.Required`. Le filtre 2 exclura les constatations `Validation.Required`, mais il inclura les constatations `Validation.EncodingRequired`. Le résultat final sera que toutes les constatations `Validation.EncodingRequired` et `Validation.Required` seront incluses.

A compter de la version 9.0.3.4, vous pouvez supprimer les constatations de *n'importe* quel filtre d'exclusion en sélectionnant **Faire correspondre les filtres d'exclusion non inversés** lors de la création d'une configuration d'examen. Cette case à cocher figure dans la section **Informations sur les filtres** de l'onglet **Général** de la vue Configuration d'examen. D'après l'exemple ci-dessus, si cette case est cochée, toutes les constatations `Validation.EncodingRequired` et `Validation.Required` seront exclues de l'évaluation.

Gestion améliorée des bibliothèques lors de l'examen des fichiers `WAR` et `EAR` dans AppScan Source for Automation et l'interface de ligne de commande (CLI) d'AppScan Source

Lors de l'examen des fichiers `WAR`, les paramètres suivants sont désormais disponibles :

- `-include_all_lib_jars` : Utilisez ce paramètre pour prendre en compte toutes les bibliothèques du fichier `WAR` lors de l'examen.
- `-include_lib_jars` : Utilisez ce paramètre pour préciser les bibliothèques du fichier `WAR` à prendre en compte lors de l'examen.

Lors de l'importation d'un fichier `EAR`, un projet destiné au stockage des bibliothèques partagées est créé automatiquement. En l'absence de bibliothèques partagées, le fichier est quand-même créé, mais reste vide. Le nouveau paramètre facultatif `-no_ear_project` permet de ne pas créer de projet pour le fichier `EAR`.

Envoi d'évaluations AppScan Source vers le cloud à des fins d'analyse

Si vous disposez d'un abonnement au service IBM Application Security on Cloud via IBM Cloud Marketplace ou au service Application Security on Cloud for Bluemix, vous pouvez lui envoyer des évaluations AppScan Source afin qu'elles soient analysées. Les évaluations provenant d'AppScan Source version 9.0 ou d'une version ultérieure sont prises en charge et le nombre d'analyses pouvant être envoyées dépend de votre formule d'abonnement à Application Security on Cloud. Pour plus d'informations, voir http://www.ibm.com/support/knowledgecenter/SSYJJF_1.0.0/ApplicationSecurityonCloud/src_managing_assessments_cloud.html.

Fonctions et options qui ne sont plus prises en charge dans AppScan Source version 9.0.3.4

A compter de AppScan Source version 9.0.3.4 :

- Le système d'exploitation OS X Version 10.9 n'est plus pris en charge.
- Les versions 5.x, 6.0 et 6.2 de Xcode ne sont plus prises en charge. L'analyse des projets Objective-C avec ces versions de Xcode n'est plus prise en charge.
- La prise en charge de l'analyse de PHP versions 5.3 et 5.4 est obsolète.

Nouveautés dans AppScan Source version 9.0.3.3

Prise en charge de la nouvelle plateforme et de la solution d'intégration

A compter de AppScan Source version 9.0.3.3 :

- Microsoft Windows 10 est désormais pris en charge (inclut les éditions Windows 10 Education, Entreprise et Professionnel).

  Remarque :

  – Sous Windows 10, le programme d'installation d'AppScan Source (fichier `AppScanSrc_Installer.exe`) doit être exécuté en mode de compatibilité Windows 7. Sous Windows 10, le fichier `AppScan_Uninstaller.exe` doit également s'exécuter en mode de compatibilité Windows 7 avant de désinstaller AppScan Source. Ce fichier se trouve dans `<rép_install>\Uninstall_AppScan\AppScan_Uninstaller.exe` (où `<rép_install>` est l'emplacement de votre installation d'AppScan Source, comme indiqué dans la rubrique «Installation et emplacements des fichiers de données utilisateur», à la page 292). Pour plus d'informations, voir http://www.ibm.com/support/docview.wss?uid=swg21696098.

  – La prise en charge de Windows 10 est affectée par le problème décrit à la page http://www.ibm.com/support/docview.wss?uid=swg21689814.

- Si vous vous connectez à la version 9.0.3.1 d'AppScan Enterprise Server ou à une version ultérieure, la base de données IBM Security AppScan Source peut être installée sur une base de données Oracle 12c.

  Important : Si vous disposez d'une installation existante d'AppScan Source qui utilise la base de données Oracle 11g, et si vous souhaitez effectuer une mise à niveau vers Oracle 12c, vous devez mettre à niveau AppScan Source avant de procéder à la mise à niveau de la base de données Oracle.

- **Tomcat 8** est désormais inclus dans l'installation d'AppScan Source.
- Les fichiers de solution et projet Visual Studio 2015 peuvent désormais être examinés dans AppScan Source for Analysis, AppScan Source for Automation et l'interface de ligne de commande d'AppScan Source. Si vous possédez des fichiers `.sln` ou `.vcproj` créés dans Visual Studio 2015, ces fichiers peuvent être

importés et examinés lors de l'utilisation d'AppScan Source for Analysis, AppScan Source for Automation ou de l'interface de ligne de commande d'AppScan Source sous Windows.

Important :

- L'application d'AppScan Source for Development (plug-in Visual Studio) à Visual Studio 2015 n'est pas prise en charge.
- Les projets C++ gérés sont pris en charge. Les projets C++ non gérés le sont aussi s'ils ont été générés avec le composant Platform Toolset de Visual Studio 2013 ou une version antérieure (Platform Toolset version 120 ou antérieure).

- Xcode 7.3 for Objective-C (pour applications iOS uniquement) est désormais un compilateur pris en charge sous macOS (la prise en charge de Xcode 7.3 est rétroactive jusqu'à AppScan Source version 9.0.3.2).

Nouveau support d'examen amélioré

- PHP versions 5.5 et 5.6 peuvent désormais être examinés sous Windows et Linux dans IBM Security AppScan Source for Analysis, dans IBM Security AppScan Source for Automation et dans l'interface de ligne de commande (CLI) d'IBM Security AppScan Source.
- Lorsque vous utilisez la fonction d'AppScan Source pour examiner du code Java™, les annotation de méthode `@ValidatorMethod`, `@CallbackMethod` et `@SuppressSecurityTrace` sont désormais prises en charge.

Nouveau nom de fichier d'installation pour Windows

Sous Windows, le nom du fichier d'installation, `setup.exe`, a été remplacé par `AppScanSrc_Installer.exe`.

Prise en charge CAC (Common Access Card) sous Windows

La carte d'accès Common Access Card (http://www.cac.mil) est l'identification standard pour le personnel de maintenance actif, les réservistes sélectionnés, le personnel civil DoD et les sous-traitants éligibles aux Etats-Unis. Elle permet un accès physique aux bâtiments et aux espaces contrôlés ainsi qu'aux réseaux et aux systèmes informatiques du ministère de la défense. Elle peut être utilisée pour accéder à des ordinateurs et à des réseaux équipés de divers lecteurs de carte à puce. Lorsqu'elle est insérée dans le lecteur, le périphérique invite l'utilisateur à entrer un code confidentiel.

Si vous exécutez AppScan Source sous Windows si vous vous connectez à un serveur AppScan Enterprise Server version 9.0.3.1 iFix-001 ou ultérieure active pour l'authentification CAC (Common Access Card), AppScan Source prend désormais en charge l'authentification CAC.

Prise en charge du rapport DISA Application Security and Development STIG V3R10

AppScan Source prend désormais en charge le rapport Defense Information Systems Agency (DISA) Application Security and Development Security Technical Implementation Guide (STIG) V3R10.

Nouveautés dans AppScan Source version 9.0.3.2

Compatibilité des versions AppScan Source et AppScan Enterprise

Certaines versions d'AppScan Source ne nécessitent plus que les niveaux de version et d'édition d'AppScan Source et d'AppScan Enterprise correspondent lors de la connexion à AppScan Enterprise Server ou de la publication dans AppScan Enterprise Console. Voir http://www.ibm.com/support/docview.wss?uid=swg21975211 pour savoir quelles versions d'AppScan Source et d'AppScan Enterprise sont compatibles.

Ce changement est rétroactif pour certaines versions d'AppScan Source, comme décrit dans http://www.ibm.com/support/docview.wss?uid=swg21975211.

Nouveautés dans AppScan Source version 9.0.3.1

- «Prise en charge d'une nouvelle solution d'intégration»
- «Examen des fichiers WAR et EAR dans AppScan Source for Automation et l'interface de ligne de commande (CLI) d'AppScan Source»

Prise en charge d'une nouvelle solution d'intégration

A partir d'AppScan Source version 9.0.3.1 :

- Tomcat 8 est désormais pris en charge pour compiler Java et JSP.

  Remarque : La prise en charge du système d'exploitation dépend du système d'exploitation pris en charge par les compilateurs individuels.
- Xcode 7.0, 7.1 et 7.2 for Objective-C (pour applications iOS uniquement) sont désormais des compilateurs pris en charge sous macOS.

Examen des fichiers `WAR` et `EAR` dans AppScan Source for Automation et l'interface de ligne de commande (CLI) d'AppScan Source

La commande `openapplication (oa)` dans l'CLI peut désormais être utilisée pour ouvrir les fichiers `WAR` et `EAR`. Par ailleurs, ces fichiers peuvent être analysés dans AppScan Source for Automation à l'aide de la commande `ScanApplication`.

Nouveautés dans AppScan Source version 9.0.3

- «Prise en charge de la nouvelle plateforme et de la solution d'intégration», à la page 12
- «Améliorations apportées à la configuration d'examen», à la page 12
- «Les nouveaux attributs de règle vous permettent d'identifier plus précisément les constatations de sécurité catégoriques ayant une gravité élevée», à la page 12
- «La résolution de collecteur indéterminé automatique améliore les résultats d'examen», à la page 14
- «Nouveau support d'examen amélioré», à la page 14
- «Fonctions et options qui ne sont plus prises en charge dans AppScan Source version 9.0.3», à la page 15

Prise en charge de la nouvelle plateforme et de la solution d'intégration

A partir d'AppScan Source version 9.0.3, les systèmes d'exploitation suivants sont pris en charge :

- Red Hat Enterprise Linux version 6 mises à jour 6 et 7
- OS X version 10.11. La prise en charge d'OS X version 10.11 est rétroactive pour AppScan Source version 9.0.2, mais est soumise à la limitation décrite dans http://www.ibm.com/support/docview.wss?uid=swg21968948 (cette limitation affecte uniquement AppScan Source version 9.0.2).

En outre :

- Xcode 6.3 et 6.4 for Objective-C (pour applications iOS uniquement) sont désormais des compilateurs pris en charge sous OS X (le support de Xcode 6.3 et 6.4 est rétroactif pour AppScan Source version 9.0.2). Notez que le support de Xcode 6.3 et 6.4 est soumis à certaines limitations. Pour plus d'informations, voir http://www.ibm.com/support/docview.wss?uid=swg21962208. Ces limitations ne s'appliquent pas à AppScan Source version 9.0.3.1 et versions supérieures.
- Le Plug-in Eclipse AppScan Source for Development s'intègre désormais à IBM MobileFirst Platform Foundation version 7.1. Vous pouvez maintenant examiner les projets, applications, environnements et fichiers HTML de IBM MobileFirst Platform version 7.1 dans les produits AppScan Source.
- Les fichiers de projet et les espaces de travail de Rational Application Developer for WebSphere Software (RAD) version 9.1.1 peuvent être examinés, et le AppScan Source for Development (plug-in Eclipse) peut être appliqué à RAD version 9.1.1.
- Les fichiers de projet et les espaces de travail d'Eclipse version 4.5 (Java et IBM MobileFirst Platform uniquement) peuvent être examinés, et le AppScan Source for Development (plug-in Eclipse) peut être appliqué à Eclipse version 4.5.
- IBM WebSphere Application Server version 8.5.5 est désormais pris en charge pour compiler Java et JSP.

  Remarque : La prise en charge du système d'exploitation dépend du système d'exploitation pris en charge par les compilateurs individuels.

Améliorations apportées à la configuration d'examen

La vue Configuration d'examen a fait l'objet d'une nouvelle conception et elle comporte désormais les fonctions principales suivantes :

- Possibilité d'indiquer des filtres.
- Définition du type d'analyse à effectuer pendant un examen. Les types disponibles sont notamment l'analyse de flux corrompus et l'analyse basée sur des schémas.

AppScan Source inclut désormais les configurations d'examen intégrées : examen d'aperçu Web, examen rapide Web, examen réparti Web, examen profond Web

Les nouveaux attributs de règle vous permettent d'identifier plus précisément les constatations de sécurité catégoriques ayant une gravité élevée

Cette édition d'AppScan Source introduit les attributs `Attribute.Likelihood.High` et `Attribute.Likelihood.Low`. Ces attributs ont été ajoutés aux règles intégrées et peuvent également être utilisés lors de la création de règles personnalisées.

Dans AppScan Source, *likelihood* représente la probabilité ou la possibilité qu'une constatation de sécurité puisse être exploitée. AppScan Source prend la définition de la probabilité définie à l'adresse https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology#Step_2:_Factors_for_Estimating_Likelihood et l'affine en déterminant la probabilité en fonction des propriétés de trace. A partir d'un ensemble de propriétés de trace, telles que le nom de l'API source, le type de l'API source, la technologie source ou le mécanisme source, AppScan Source détermine la probabilité qu'une trace soit exploitée dans le futur en utilisant une vulnérabilité spécifique.

La probabilité est liée à l'élément source d'une trace. Une source est une entrée du programme, telle qu'un fichier, une requête de servlet, une saisie depuis la console ou un socket. Dans le cas de la plupart des sources d'entrées, les données renvoyées ne sont pas limitées en termes de contenu et de longueur. Lorsqu'une entrée n'est pas vérifiée, elle est considérée comme une source de tache.

Vous trouverez quelques exemples de probabilité ci-dessous :

- Si l'on prend une trace avec une source HTTP (par exemple, `Request.getQueryString`) et un collecteur XSS (par exemple, `Response.write`), une probabilité élevée est déterminée, augmentant ainsi le niveau de fiabilité de la constatation.
- Si l'on prend une trace avec une source de propriété système (par exemple, `getProperty`) et un collecteur XSS (par exemple, `Response.write`), une probabilité faible est déterminée, diminuant ainsi le niveau de fiabilité de la constatation.

La probabilité permet d'identifier les constatations à priorité élevée qui doivent être traitées ou corrigées immédiatement. Elle est liée aux sources de taches hautement exploitables et peut vous fournir une approche affinée pour la classification des constatations. La probabilité est stockée en tant qu'attribut lié à une source de tache dans la base de données de vulnérabilités d'AppScan Source. Cette fonction est prête à l'emploi.

Nous avons mené des recherches approfondies afin de déterminer le facteur de probabilité des sources. A l'aide de l'assistant Règles personnalisées, vous pouvez ajouter des informations de probabilité aux nouvelles sources de taches que vous ajoutez à votre base de règles. Vous améliorez ainsi la classification des constatations générées à partir d'un examen et, par conséquent, l'efficacité de votre flux de travail global de triage.

Dans l'assistant de règles personnalisées, vous pouvez définir deux valeurs (**High** et **Low**) pour la propriété **Likelihood**. La valeur **High** signifie que la source est très vulnérable aux taches. Autrement dit, la barrière aux taches entrant dans le système est très faible, ce qui permet aux agresseurs informatiques de soumettre facilement des données malveillantes de façon manuelle ou automatique. La valeur **Low** signifie que la barrière à l'entrée de données malveillantes par le biais de cette source est très élevée. Cela peut vouloir dire que pour que la tache soit introduite dans la source, un agresseur informatique doit avoir une connaissance d'initié du système et disposer d'autorisations pour opérer sur le réseau de la victime.

Remarque : Suite à l'introduction de ces attributs de règle, si vous avez généré des évaluations dans les versions précédentes d'AppScan Source, vous pourrez noter que des classifications de constatations pour la même source ont changé lors de son examen dans la version 9.0.3. Pour un complément d'informations et pour savoir comment désactiver ces attributs de règle, lisez les considérations relatives à la migration concernant ces changements.

La résolution de collecteur indéterminé automatique améliore les résultats d'examen

AppScan Source tente désormais de résoudre les collecteurs indéterminés des traces en déduisant automatiquement le marquage pour les méthodes de collecteur indéterminé, telles que getter ou setter, et pour les méthodes renvoyant des valeurs booléennes. Vous obtenez ainsi une analyse plus approfondie de votre code et une résolution améliorée des collecteurs indéterminés.

Remarque : Il résulte de cette fonction que si vous avez généré des évaluations dans des versions précédentes d'AppScan Source, vous pouvez constater un changement dans les résultats des constatations concernant les collecteurs indéterminés non résolus. Pour un complément d'informations et pour savoir comment désactiver la génération de marquage automatique, lisez les considérations relatives à la migration concernant ces changements.

Nouveau support d'examen amélioré

- PHP version 5.4 peut désormais être examiné sous Windows et Linux dans IBM Security AppScan Source for Analysis, dans IBM Security AppScan Source for Automation et dans l'interface de ligne de commande (CLI) d'IBM Security AppScan Source.
- AppScan Source inclut désormais la prise en charge intégrée de l'infrastructure Spring MVC 4.
- **Optimisations de l'examen Java :**
  - Lorsque vous examinez des pages JSP, vous avez désormais la possibilité d'examiner des fichiers de classes précompilées au lieu de les compiler au cours d'un examen. Pour examiner des fichiers de classes précompilées dans le Plug-in Eclipse AppScan Source for Development, configurez votre projet pour l'examen de sécurité (sélectionnez **Analyse de sécurité** > **Configurer l'examen** > **Configurer la sécurité des projets**), puis cochez la case **Classes précompilées**. Pour examiner des fichiers de classes précompilées dans IBM Security AppScan Source for Analysis, cochez la case **Classes précompilées** dans l'un des emplacements suivants :
    - L'onglet Dépendances de projet dans les propriétés du projet.
    - La page Dépendances de projet Java lors de la création d'un nouveau projet ou d'une nouvelle application.
  - Lors de l'examen de Java, AppScan Source examine maintenant les fichiers Java et le bytecode Java en recherchant des dépendances manquantes ou des erreurs de compilation. S'il existe des dépendances manquantes ou des erreurs de compilation, des informations associées seront consignées dans un fichier journal. Grâce à ces informations, vous pouvez ensuite ajouter les dépendances dans les propriétés de votre projet, effectuer un nouvel examen et atteindre la couverture totale des résultats d'examen.
- A partir de AppScan Source version 9.0.3, les emplacements d'en-tête et options de configuration sont déterminés de façon plus précise lors de l'importation et de l'examen de projets Xcode. Ce changement introduit l'utilisation de `xcodebuild -dry-run` pour obtenir la configuration de génération de chaque fichier, il se peut donc que l'opération soit mise en pause au début des examens, pendant que AppScan Source détermine les configurations de fichier avant de continuer.

Fonctions et options qui ne sont plus prises en charge dans AppScan Source version 9.0.3

A compter d'AppScan Source version 9.0.3 :

- Le système d'exploitation OS X version 10.8 n'est plus pris en charge.
- Xcode Version 4.6 n'est plus pris en charge. L'analyse des projets Objective-C avec cette version de Xcode n'est plus prise en charge.
- Les fichiers de projet et les espaces de travail Eclipse version 3.6 et 3.7 ne sont plus pris en charge, et le AppScan Source for Development (plug-in Eclipse) ne peut plus être appliqué à Eclipse versions 3.6 et 3.7.
- Les fichiers de projet et les espaces de travail Rational Application Developer for WebSphere Software (RAD) version 8.0.x ne sont plus pris en charge et IBM Security AppScan Source for Development pour IBM Rational Application Developer for WebSphere Software (RAD) ne peut plus être appliqué à RAD version 8.0.x.
- Les versions 3.0 et 3.0.1 de IBM Rational Team Concert ne sont plus prises en charge sur les systèmes de suivi d'incidents.
- WebSphere Application Server version 6.1 n'est plus un serveur d'application pris en charge.
- La prise en charge de l'examen des versions PHP versions 4.x à 5.2 est obsolète.

Migration vers la version actuelle d'AppScan Source

Cette rubrique contient des informations de migration pour les modifications qui ont été introduites dans cette version d'AppScan Source. Si vous mettez à niveau une version antérieure d'AppScan Source, notez bien les modifications apportées à la version d'AppScan Source que vous mettez à niveau et à toutes les versions jusqu'à cette version actuelle.

- «Migration à partir de la version 9.0.2»
- «Migration à partir de la version 9.0», à la page 17
- «Migration à partir de la version 8.7», à la page 17

Migration à partir de la version 9.0.2

- «Il est possible que les nouveaux attributs de règle génèrent des modifications de classification des constatations dans les examens existants»
- «Génération de collecteur indéterminé automatique», à la page 16

Il est possible que les nouveaux attributs de règle génèrent des modifications de classification des constatations dans les examens existants

Après la version 9.0.2, les attributs de règle `Attribute.Likelihood.High` et `Attribute.Likelihood.Low` ont été introduits. Lorsque ces attributs sont utilisés, AppScan Source est en mesure de déterminer de manière plus précise si des constatations sont catégoriques et/ou suspectes. Par conséquent, si vous examinez du code source dans AppScan Source version 9.0.2 ou précédentes, vous pouvez noter des changements dans certaines classifications de constatations lorsque ce même code source est examiné dans des versions du produit plus récentes. Ces changements sont particulièrement notables pour les constatations associées à des sources Web hautement exploitables, ou les sources de propriété ou d'environnement moins exploitables.

Ces attributs de règle sont utilisés par défaut. Vous pouvez les désactiver de la façon suivante :

1. Ouvrez <data_dir>\config\ipva.ozsettings dans un éditeur de texte (où <rép_données> est l'emplacement de vos données de programme AppScan Source, comme décrit dans «Installation et emplacements des fichiers de données utilisateur», à la page 292). Recherchez le paramètre allow_likelihood dans le fichier. Ce paramètre est similaire à ce qui suit :

   ```
   <Setting
     name="allow_likelihood"
     value="true"
     default_value="true"
     description="Allow the processing of the Likelihood
       attributes to help determine trace confidence based
       on the source API"
     display_name="Allow Likelihood"
     type="bool"
   />
   ```

   Dans ce paramètre, modifiez l'attribut value. Si l'attribut est défini sur la valeur true, ce paramètre sera activé. Si l'attribut est défini sur la valeur false, AppScan Source n'utilisera pas ces attributs de règle pendant les examens.
2. Après avoir modifié ce paramètre, sauvegardez le fichier, puis démarrez ou redémarrez AppScan Source.

Génération de collecteur indéterminé automatique

Après la version 9.0.2, la résolution de collecteur indéterminé automatique a été introduite pour les traces qui se terminent par des getters/setters et les méthodes qui retournent des valeurs booléennes. Cela est possible en déduisant automatiquement le marquage pour ces interfaces de programmation. Par conséquent, si vous examinez du code source dans AppScan Source version 9.0.2 ou précédentes, vous pouvez noter des changements dans les résultats des constatations qui contenaient des collecteurs indéterminés non résolus lorsque ce même code source est examiné dans des versions du produit plus récentes.

La fonction de génération de marquage automatique est activée par défaut. Vous pouvez la désactiver si vous voulez utiliser d'autres moyens de résolution de collecteurs indéterminés, par exemples des règles personnalisées, comme suit :

1. Ouvrez <data_dir>\config\ipva.ozsettings dans un éditeur de texte (où <rép_données> est l'emplacement de vos données de programme AppScan Source, comme décrit dans «Installation et emplacements des fichiers de données utilisateur», à la page 292). Recherchez le paramètre automatic_lost_sink_resolution dans le fichier. Ce paramètre est similaire à ce qui suit :

   ```
   <name="automatic_lost_sink_resolution"
     value="true"
     default_value="true"
     description="This setting tries to perform automatic
       lost sink resolution by assuming taint propagation
       for getters, setters and APIs which return boolean
       with no arguments."
     display_name="Auto Lost Sink Resolution"
     type="bool"
   />
   ```

Dans ce paramètre, modifiez l'attribut `value`. Si l'attribut est défini sur la valeur `true`, ce paramètre sera activé. Si l'attribut est défini sur la valeur `false`, AppScan Source ne générera pas automatiquement le marquage pour ces méthodes.

2. Après avoir modifié ce paramètre, sauvegardez le fichier, puis démarrez ou redémarrez AppScan Source.

Migration à partir de la version 9.0

Authentification d'AppScan Enterprise Server : Considérations relatives à la migration pour le remplacement du composant d'authentification des utilisateurs IBM Rational Jazz par IBM WebSphere Liberty

- **Migration à partir d'un serveur Enterprise Server qui ne possède que des utilisateurs Jazz locaux** : Dans ce scénario de mise à niveau, les précédents utilisateurs Jazz apparaîtront dans la base de données AppScan Source comme utilisateurs AppScan Enterprise Server, mais ils ne seront pas valides. Ces utilisateurs peuvent être supprimés de la base de données ou être convertis en utilisateurs AppScan Source si vous suivez les instructions de la rubrique http://www.ibm.com/support/docview.wss?uid=swg21686347 pour permettre cette conversion.
- **Migration à partir d'un serveur Enterprise Server configuré avec LDAP** : lors de la mise à niveau du serveur Enterprise Server, vous avez la possibilité de configurer de nouveau le serveur Enterprise Server avec LDAP. Les utilisateurs existants continueront alors de fonctionner dans AppScan Source.
- **Migration à partir d'un serveur Enterprise Server configuré avec l'authentification Windows** : si votre serveur Enterprise Server était configuré avec l'authentification Windows, les utilisateurs existants fonctionneront dans AppScan Source, à condition que le nouveau serveur Enterprise Server Liberty soit configuré pour utiliser l'authentification Windows.

Migration à partir de la version 8.7

- «Modifications apportées aux classifications des constatations»
- «Modifications des paramètres par défaut qui améliorent la couverture d'examen», à la page 18
- «Restauration des filtres prédéfinis d'AppScan Source à partir de versions antérieures», à la page 19

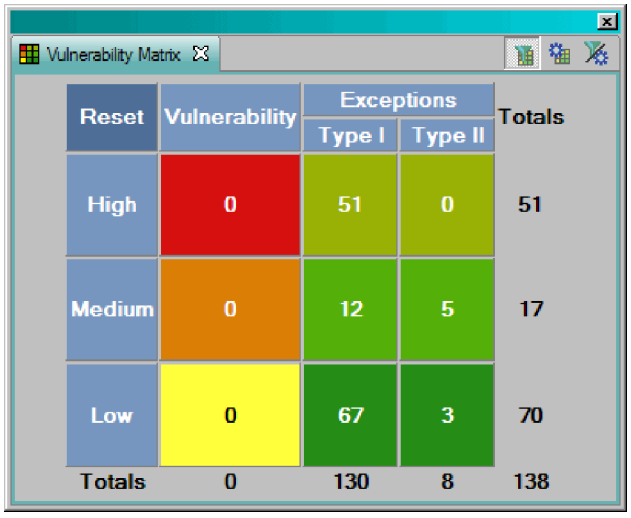
Modifications apportées aux classifications des constatations

Après la version 8.7, les classifications des constatations ont changé. Ce tableau répertorie les anciennes classifications mappées sur les nouvelles classifications :

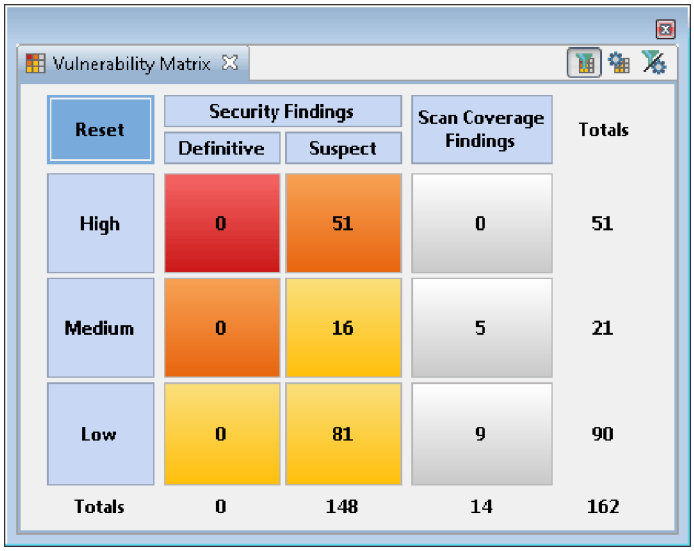
Tableau 1. Modifications apportées aux classifications des constatations

Classifications des constatations avant AppScan Source version 8.8	**Classifications à partir d'AppScan Source version 8.8**
Vulnérabilité	Constatation de sécurité définitive
Exception de type I	Constatation de sécurité suspectée
Exception de type II	Constatation de couverture d'examen

La vue Matrice de vulnérabilités offre un exemple de ces modifications.



A partir de la version 8.8, la vue s'affiche comme suit :



Modifications des paramètres par défaut qui améliorent la couverture d'examen

A partir d'AppScan Source version 8.8 :

- La valeur par défaut de `show_informational_findings` dans `scan.ozsettings` est passée de `true` à `false`.
- La valeur par défaut de `wafl_globals_tracking` dans `ipva.ozsettings` est passée de `false` à `true`. Ce paramètre permet à AppScan Source de rechercher un flux de données entre différents composants d'une application basée sur une structure (par exemple, un flux de données entre un contrôleur et une vue).

La modification apportée à `show_informational_findings` fait que les évaluations n'incluent pas les constatations d'un niveau de gravité de valeur **Info** par défaut.

Remarque : Si des configurations d'examen ont été créées avant la version 8.8 sans définir explicitement des valeurs pour ces paramètres, elles utiliseront désormais leurs nouvelles valeurs par défaut.

Restauration des filtres prédéfinis d'AppScan Source à partir de versions antérieures

Dans AppScan Source version 8.8, les filtres prédéfinis ont été améliorés pour fournir de meilleurs résultats d'examen. Si vous devez continuer à utiliser les filtres prédéfinis des versions antérieures d'AppScan Source (les filtres archivés sont répertoriés dans «Filtres prédéfinis AppScan Source (versions 8.7.x et antérieures)», à la page 129), suivez les instructions de la section «Restauration des filtres prédéfinis archivés», à la page 131.

Présentation d'AppScan Source for Analysis

AppScan Source for Analysis est un outil destiné à analyser le code et à fournir des informations spécifiques sur les vulnérabilités du code source de systèmes critiques. AppScan Source for Analysis vous permet de centraliser la gestion des risques de vos logiciels entre des applications multiples, voire votre portefeuille complet. Vous pouvez examiner le code source, effectuer un triage, et éliminer des vulnérabilités avant qu'elles ne constituent un risque avéré pour votre organisation.

AppScan Source for Analysis fournit aux équipes d'audit et d'assurance qualité des outils destinés à l'examen du code source et de triage des résultats et à la soumission des failles détectées aux systèmes de suivi des défauts.

A l'aide des enseignements en contexte de la Base de connaissances de sécurité AppScan Source Security, les analystes, auditeurs, responsables et développeurs peuvent :

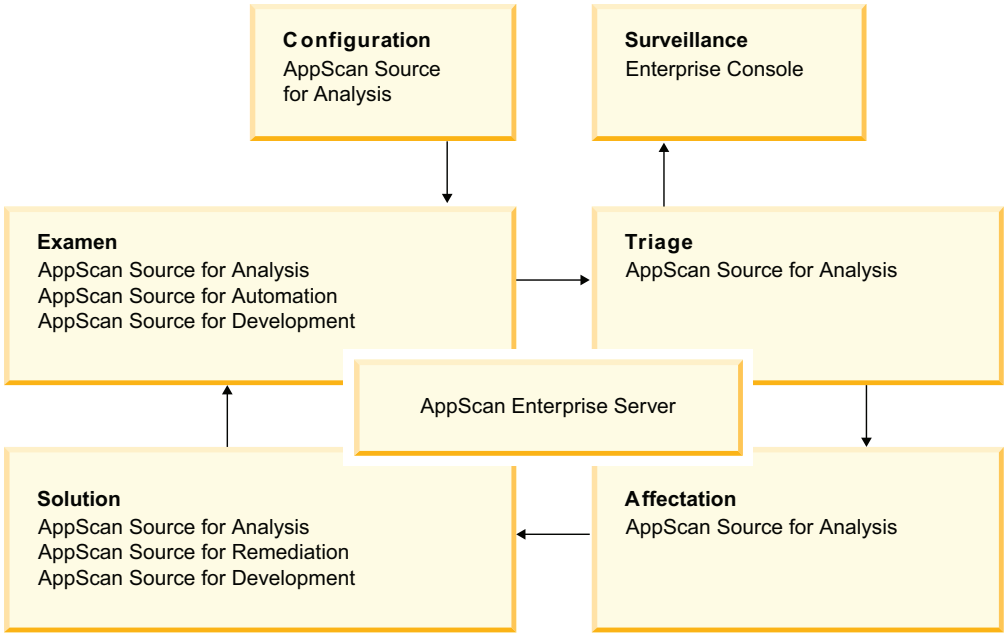
- Examiner à la demande un code source spécifique pour identifier des vulnérabilités critiques
- Recevoir des recommandations de résolution précises et appeler leur environnement de développement et leur éditeur de code de prédilection directement depuis l'analyse
- Suivre le cheminement des données entachées depuis l'entrée jusqu'à la sortie à travers un graphe d'appels précis et interactif
- Mettre en application des règles de codage et vérifier l'utilisation de routines de validation et de codage des entrées approuvées via la fonction de trace AppScan Source
- Assimiler et implémenter des pratiques de programmation optimales lors du développement de logiciels

Flux de travaux

Après l'installation, le déploiement et la gestion des utilisateurs, le flux de travaux AppScan Source se compose des étapes de base suivantes :

1. **Définir les exigences de sécurité** : un responsable ou un expert de la sécurité définit des vulnérabilités et comment déterminer leur criticité.
2. **Configurer les applications** : organiser les applications et les projets.
3. **Examiner** : exécuter l'analyse sur l'application cible pour identifier les vulnérabilités.

4. **Trier et analyser les résultats** : les résultats de l'analyse sont étudiés par les intervenants de la sécurité afin d'attribuer des priorités dans le flux de travaux de résolution et de séparer les vulnérabilités réelles des potentielles en permettant de lancer immédiatement le triage des problèmes critiques. Isoler les problèmes qu'il faut résoudre en priorité.
5. **Personnaliser la Base de connaissances** : personnaliser la Base de connaissances de sécurité AppScan Source Security en fonction des règles internes d'adresse.
6. **Publier les résultats de l'examen** : ajouter les résultats de l'examen à la base de données AppScan Source ou les publier sur AppScan Enterprise Console.
7. **Affecter les tâches de résolution** : affecter les incidents à l'équipe de développement pour résoudre les vulnérabilités.
8. **Résoudre les problèmes** : éliminer les vulnérabilités en réécrivant le code, en supprimant les failles ou en ajoutant des fonctions de sécurité.
9. **Vérifier les correctifs** : le code est analysé à nouveau pour s'assurer que les vulnérabilités ont été éliminées.



Concepts important

Avant de commencer à utiliser ou administrer AppScan Source, vous devez vous familiariser avec les concepts fondamentaux de AppScan Source. Cette section définit la terminologie et les concepts de base de AppScan Source. Les chapitres ultérieurs reviennent sur ces définitions pour vous aider à comprendre leur contexte dans AppScan Source for Analysis.

AppScan Source for Analysis *examine* le code source pour détecter des vulnérabilités et génère des *constatations*. Ces constatations sont les vulnérabilités détectées au cours d'un examen et le résultat d'un examen constitue une *évaluation*. Un *groupement* désigne une collection nommée de constatations individuelles et est stocké avec une application.

Les applications, leurs attributs et les projets sont créés et organisés dans AppScan Source for Analysis :

- **Applications** : une application contient un ou plusieurs projets et leurs attributs associés.
- **Projets** : un projet est constitué d'un ensemble de fichiers (y compris du code source) et des informations qui y sont associées (telles que les données de configuration). Un projet fait toujours partie d'une application.
- **Attributs** : un attribut est une caractéristique d'une application qui aide à organiser les résultats de l'examen en groupes significatifs, tels que par service ou par chef de projet. Vous définissez les attributs dans AppScan Source for Analysis.

L'activité principale de AppScan Source for Analysis est l'examen du code source et la détection des vulnérabilités. Les évaluations fournissent une analyse du code source pour l'identification de vulnérabilités et comprennent :

- **Gravité** : élevée, moyenne ou faible, qui identifie le niveau de risque
- **Type de vulnérabilité** : catégorie de vulnérabilité (par exemple, injection SQL ou dépassement de mémoire tampon)
- **Fichier** : fichier de code dans lequel la constatation existe
- **API/Source** : appel vulnérable, où est présenté l'API et les arguments qui lui sont transmis
- **Méthode** : fonction ou méthode depuis laquelle l'appel vulnérable est émis
- **Emplacement** : numéro de la ligne et de la colonne dans le fichier de code qui contient l'API vulnérable
- **Classification** : constatation de sécurité ou constatation de couverture d'examen. Pour plus d'informations, voir «Classifications».

Classifications

Les constatations sont classées par AppScan Source pour indiquer s'il s'agit de constatations de sécurité ou de couverture d'examen. Les constatations de sécurité représentent des vulnérabilités réelles ou probables en matière de sécurité, alors que les constatations de couverture d'examen représentent les zones dans lesquelles la configuration pourrait être améliorée afin de fournir une meilleure couverture d'examen.

Chaque constatation (ou résultat) se rattache à l'une de ces *classifications* :

- Constatation de sécurité **définitive** : Une constatation contenant une conception définitive, une implémentation ou une violation de stratégie qui présente une possibilité pour un agresseur de provoquer un fonctionnement imprévu de l'application.

  Cette attaque peut résulter en un accès non autorisé, le vol ou l'altération de données, de systèmes ou de ressources. Chaque constatation de sécurité définitive est complètement décomposée et le schéma sous-jacent spécifique de la condition vulnérable est connu et décrit.
- Constatation de sécurité **suspectée** : Une constatation qui indique une condition suspecte et potentiellement vulnérable requérant des informations ou des investigations supplémentaires. Un élément ou une structure de code qui peut créer une vulnérabilité en cas d'utilisation incorrecte.

  Une constatation suspectée diffère d'une constatation définitive car il existe une condition inconnue qui empêche la détermination définitive d'une vulnérabilité. L'utilisation d'éléments dynamiques ou de fonctions de bibliothèque pour lesquelles aucun code source n'est disponible sont des exemples de cette incertitude. En conséquence, un niveau de recherche supplémentaire s'impose pour confirmer ou rejeter une constatation suspectée comme étant définitive.

- Constatation de **couverture d'examen** : Constatations qui représentent les zones dans lesquelles la configuration pourrait être améliorée afin de fournir une meilleure couverture d'examen (par exemple, les constatations de collecteur indéterminé).

Remarque : Dans certains cas, la classification **Aucun** est utilisée pour indiquer une constatation qui n'est ni une constatation de sécurité ni une constatation de couverture d'examen.

Connexion à AppScan Enterprise Server à partir des produits AppScan Source

La plupart des produits et des composants AppScan Source requièrent une connexion à un serveur AppScan Enterprise Server. Ce serveur fournit des fonctionnalités de gestion centralisée des utilisateurs et un mécanisme de partage d'évaluations via la base de données AppScan Source.

Lorsque vous lancez AppScan Source for Analysis, vous êtes invité à vous authentifier sur un serveur AppScan Enterprise Server. Si vous exécutez AppScan Source for Development dans mode serveur, vous êtes invité à vous authentifier sur un serveur AppScan Enterprise Server lorsque vous lancez pour la première fois une action nécessitant l'accès au serveur, comme le lancement d'un examen ou l'affichage des configurations d'examen.

- «Connexion à partir d'AppScan Source for Analysis et d'AppScan Source for Development avec un ID utilisateur et un mot de passe AppScan Enterprise Server»
- «Utilisation de l'authentification CAC (Common Access Card) pour la connexion à partir des produits AppScan Source for Analysis et AppScan Source for Development», à la page 23
- «Connexion à partir d'AppScan Source for Automation et de l'interface de ligne de commande (CLI) d'AppScan Source», à la page 24
- «Certificats SSL pour AppScan Enterprise Server», à la page 24
- «Résolution des erreurs de certificat AppScan Enterprise Server», à la page 24

Connexion à partir d'AppScan Source for Analysis et d'AppScan Source for Development avec un ID utilisateur et un mot de passe AppScan Enterprise Server

Dans AppScan Source for Analysis, lorsque vous vous connectez, vous devez entrer les informations suivantes :

- **ID utilisateur** : Indiquez votre ID utilisateur (selon la configuration de votre compte, il peut s'agir d'un ID utilisateur existant à la fois sur le serveur AppScan Enterprise Server et dans la base de données AppScan Source, ou bien d'un ID utilisateur existant uniquement dans la base de données AppScan Source).
  - Si votre serveur AppScan Enterprise Server est configuré pour utiliser l'authentification Windows, entrez le nom de domaine et d'utilisateur que vous utilisez pour vous connecter au serveur Enterprise Console (en les séparant par un signe \. Par exemple, `my_domain\my_username`).
  - Si votre serveur AppScan Enterprise Server est configuré avec LDAP, entrez le nom d'utilisateur que vous utilisez pour vous connecter au serveur Enterprise Console.
- **Mot de passe** : Indiquez le mot de passe associé à votre ID utilisateur.

- **AppScan Enterprise Server** : Spécifiez l'URL de votre instance AppScan Enterprise Server. Le format de cette URL est le suivant : `http(s)://<nom_d'hôte>:<port>/ase`, où `<nom_d'hôte>` correspond au nom de la machine sur laquelle AppScan Enterprise Server est installé, et `<port>`, au port sur lequel le serveur s'exécute. Par exemple, `https://myhost.mydomain.ibm.com:9443/ase`.

Dans AppScan Source for Development, lorsque vous vous connectez, vous devez entrer les informations suivantes :

- **URL du serveur** : Spécifiez l'URL de votre instance AppScan Enterprise Server. Le format de cette URL est le suivant : `http(s)://<nom_d'hôte>:<port>/ase`, où `<nom_d'hôte>` correspond au nom de la machine sur laquelle AppScan Enterprise Server est installé, et `<port>`, au port sur lequel le serveur s'exécute. Par exemple, `https://myhost.mydomain.ibm.com:9443/ase`.
- **ID utilisateur** : Indiquez votre ID utilisateur (selon la configuration de votre compte, il peut s'agir d'un ID utilisateur existant à la fois sur le serveur AppScan Enterprise Server et dans la base de données AppScan Source, ou bien d'un ID utilisateur existant uniquement dans la base de données AppScan Source).
  - Si votre serveur AppScan Enterprise Server est configuré pour utiliser l'authentification Windows, entrez le nom de domaine et d'utilisateur que vous utilisez pour vous connecter au serveur Enterprise Console (en les séparant par un signe \. Par exemple, `my_domain\my_username`).
  - Si votre serveur AppScan Enterprise Server est configuré avec LDAP, entrez le nom d'utilisateur que vous utilisez pour vous connecter au serveur Enterprise Console.
- **Mot de passe** : Indiquez le mot de passe associé à votre ID utilisateur.

Utilisation de l'authentification CAC (Common Access Card) pour la connexion à partir des produits AppScan Source for Analysis et AppScan Source for Development

Sous Windows, vous pouvez vous connecter à AppScan Enterprise Server en utilisant l'authentification CAC (http://www.cac.mil). Avant de procéder ainsi, vous devez configurer AppScan Enterprise Server et AppScan Source pour authentification CAC (Common Access Card). Si votre serveur Enterprise Server est configuré pour authentification CAC, vous ne pouvez pas utiliser un ID utilisateur et un mot de passe Enterprise Server pour vous connecter.

Dans AppScan Source for Analysis, lorsque vous vous connectez, vous devez entrer les informations suivantes :

- **Utilisateur** : Sélectionnez votre nom commun CAC dans la liste.
- **AppScan Enterprise Server**: Spécifiez l'URL de votre instance AppScan Enterprise Server. Le format de cette URL est le suivant : `http(s)://<nom_d'hôte>:<port>/ase`, où `<nom_d'hôte>` correspond au nom de la machine sur laquelle AppScan Enterprise Server est installé, et `<port>`, au port sur lequel le serveur s'exécute. Par exemple, `https://myhost.mydomain.ibm.com:9443/ase`.

Dans AppScan Source for Development, lorsque vous vous connectez, vous devez entrer les informations suivantes :

- **URL du serveur** : Spécifiez l'URL de votre instance AppScan Enterprise Server. Le format de cette URL est le suivant : `http(s)://<nom_d'hôte>:<port>/ase`, où `<nom_d'hôte>` correspond au nom de la machine sur laquelle AppScan Enterprise Server est installé, et `<port>`, au port sur lequel le serveur s'exécute. Par exemple, `https://myhost.mydomain.ibm.com:9443/ase`.
- **Utilisateur** : Sélectionnez votre nom commun CAC dans la liste.

Une fois que vous avez cliqué sur **OK**, une boîte de dialogue Windows Security vous invite à entrer votre code confidentiel de carte CAS.

Conseil :

- Si la connexion échoue, vérifiez que votre serveur AppScan Enterprise Server est correctement configuré et que votre certificat est valide. Vérifiez si vous pouvez accéder à AppScan Enterprise Server via un navigateur. Si tel est le cas, vous devriez pouvoir sélectionner le certificat et vous connecter.
- Si la zone **Utilisateur** de la boîte de dialogue de connexion ne répertorie pas de disponibles, assurez-vous d'avoir modifié le fichier `java.security` dans votre environnement d'exécution Java, comme décrit dans «Activation de l'authentification CAC (Common Access Card)».
- Si aucune boîte de dialogue Windows Security ne s'affiche pour vous inviter à indiquer votre code confidentiel de carte CAC, vérifiez que le service Microsoft Smart Card Resource Manager est bien en opération. Notez qu'il est possible que ce service ne s'exécute pas pour certains types de connexion de bureau à distance.

Connexion à partir d'AppScan Source for Automation et de l'interface de ligne de commande (CLI) d'AppScan Source

Des actions de connexion sont également requises lors de l'exécution de AppScan Source for Automation ou de l'interface de ligne de commande (CLI) d'AppScan Source. Pour plus d'informations, voir le document *Utilitaires IBM Security AppScan Source - Guide d'utilisation*.

Certificats SSL pour AppScan Enterprise Server

Pour plus d'informations sur les certificats SSL pour AppScan Enterprise Server, voir «Certificats SSL pour AppScan Enterprise Server», à la page 27.

Résolution des erreurs de certificat AppScan Enterprise Server

Si vous vous connectez à un Enterprise Server avec une autorité de certification inconnue, vous pouvez recevoir une exception de certificat ou une erreur lors de la connexion. AppScan Source inclut un petit utilitaire, qui peut vous aider à corriger cette situation. L'outil se trouve sous `<rép_install>\bin\certificatetool.bat` (où `<rép_install>` représente l'emplacement de votre installation AppScan Source) - ou `<rép_install>/bin/certificatetool.sh` sous Linux et macOS.

Activation de l'authentification CAC (Common Access Card)

Cette rubrique décrit comment configurer AppScan Source afin d'autoriser une connexion à un serveur AppScan Enterprise Server activé pour l'authentification CAC (Common Access Card).

Avant de commencer

L'authentification CAC est uniquement prise en charge sous Windows et pour les connexions à AppScan Enterprise Server version 9.0.3.1 iFix-001 ou ultérieure.

Procédure

1. Assurez-vous que AppScan Enterprise Server n'est pas encore configuré pour l'authentification CAC,

2. Connectez-vous à AppScan Source for Analysis ou à l'interface de ligne de commande (CLI) d'AppScan Source en tant qu'administrateur AppScan Source.
3. Suivez les instructions du manuel *IBM Security AppScan Source - Guide d'installation et d'administration* pour configurer tous les utilisateurs AppScan Enterprise Server afin qu'ils disposent de tous les droits. Cette opération définit les droits par défaut initiaux pour les utilisateurs AppScan Enterprise Server sur l'accès administrateur complet ; toutefois, à l'issue de la configuration de CAC, vous pourrez changer les droits par défaut en fonction des besoins de votre organisation.
4. Quittez ou fermez toutes les applications client AppScan Source.
5. Configurez AppScan Enterprise Server pour autoriser l'authentification CAC
6. Suivez les instructions du manuel *IBM Security AppScan Source - Guide d'installation et d'administration* pour enregistrer la base de données AppScan Source avec un serveur AppScan Enterprise Server activé pour l'authentification CAC (Common Access Card).
7. Ouvrez `<data_dir>\config\ounce.ozsettings` (où `<rép_données>` est l'emplacement de vos données de programme AppScan Source, comme décrit dans «Installation et emplacements des fichiers de données utilisateur», à la page 292). Dans ce fichier, repérez le paramètre suivant :

   ```
   <Setting
      name="client_cert_auth"
      value="false"
      default_value="false"
      description="Uses client certificate authentication"
      display_name="Uses client certificate authentication"
      type="boolean"
      read_only="true"
      hidden="true"
    />
   ```
8. Remplacez `value="false"` par `value="true"` puis sauvegardez le fichier.
9. Si vous vous connectez à AppScan Enterprise Server à partir d'AppScan Source for Analysis ou du Plug-in Eclipse AppScan Source for Development :
   a. Dans votre répertoire d'installation Java, recherchez `jre/lib/security/java.security`. Pour AppScan Source for Analysis, le dossier `jre` se trouve dans votre répertoire d'installation AppScan Source. Créez une copie de sauvegarde de ce fichier.
   b. Editez le fichier `java.security`.
   c. Dans la liste des fournisseurs incluant l'ordre de préférence, ajoutez `com.ibm.security.capi.IBMCAC` comme premier fournisseur de sécurité. Par exemple, si vous éditez `java.security` pour une utilisation AppScan Source for Analysis, changez :

      ```
      security.provider.1=com.ibm.crypto.fips.provider.IBMJCEFIPS
      security.provider.2=com.ibm.jsse2.IBMJSSEProvider2
      security.provider.3=com.ibm.crypto.provider.IBMJCE
      security.provider.4=com.ibm.security.cert.IBMCertPath
      security.provider.5=sun.security.provider.Sun
      ```

      en :

      ```
      security.provider.1=com.ibm.security.capi.IBMCAC
      security.provider.2=com.ibm.crypto.fips.provider.IBMJCEFIPS
      security.provider.3=com.ibm.jsse2.IBMJSSEProvider2
      security.provider.4=com.ibm.crypto.provider.IBMJCE
      security.provider.5=com.ibm.security.cert.IBMCertPath
      security.provider.6=sun.security.provider.Sun
      ```
   d. Sauvegardez et fermez le fichier `java.security`.

10. Connectez-vous en tant qu'administrateur AppScan Source à AppScan Source for Analysis ou à l'interface de ligne de commande (CLI) d'AppScan Source via l'authentification CAC.
11. Changez les droits par défaut des utilisateurs AppScan Enterprise Server pour qu'ils correspondent aux besoins de votre organisation.

Que faire ensuite

Votre certificat ne peut pas être de type SHA-1 si vous souhaitez le mode de la norme FIPS (Federal Information Processing Standard). Vous pouvez imposer le mode FIPS en utilisant un certificat SHA-2 et en exécutant l'outil `appscanserverdbmgr_cac_fips.bat` décrit dans le manuel *IBM Security AppScan Source - Guide d'installation et d'administration*. Dans ce guide, recherchez l'aide sur l'enregistrement de la base de données AppScan Source avec un serveur AppScan Enterprise Server activé pour l'authentification CAC (Common Access Card).

Pour déterminer le type de certificat dont vous disposez, procédez comme suit :

1. Ouvrez le gestionnaire de certificat Windows : Dans le menu Démarrer de Windows, tapez `certmgr.msc` dans la zone de recherche et appuyez sur Entrée. Si vous êtes invité à entrer un mot de passe administrateur ou une confirmation, entrez le mot de passe ou confirmez.
2. Ouvrez le certificat en cliquant deux fois dessous ou utilisez l'action **Ouvrir** de l'interface utilisateur.
3. Sélectionnez l'onglet Détails du certificat.
4. Localisez la zone **Algorithme de hachage de la signature**. La valeur de cette zone indique le type du certificat.

Modification des mots de passe utilisateur de la console AppScan Source

Pour pouvoir modifier un mot de passe utilisateur AppScan Source, vous devez disposer du droit **Gérer les utilisateurs** et la modification doit être effectuée dans AppScan Source for Analysis. Si vous ne disposez pas de ce droit, demandez à votre administrateur de changer pour vous votre mot de passe en suivant les instructions de cette rubrique. Si le serveur AppScan Enterprise Server est configuré pour utiliser l'authentification LDAP ou Windows, cette rubrique ne s'applique pas.

Procédure

1. Dans AppScan Source for Analysis, sélectionnez **Admin** > **Gérer les utilisateurs** à partir du menu principal du plan de travail.
2. La boîte de dialogue Gérer les utilisateurs répertorie les utilisateurs existants de AppScan Source. Pour modifier le mot de passe pour l'un de ces utilisateurs, éditez les informations utilisateur en effectuant l'une des tâches suivantes :
   - Cliquez deux fois sur l'utilisateur.
   - Cliquez avec le bouton droit de la souris sur l'utilisateur et sélectionnez **Editer l'utilisateur**.
   - Sélectionnez l'utilisateur et cliquez sur le bouton **Editer l'utilisateur**.

   Remarque : Vous ne pouvez pas modifier le mot de passe d'un utilisateur AppScan Enterprise Server depuis AppScan Source.
3. Dans la boîte de dialogue Editer l'utilisateur, entrez un nouveau mot de passe, puis ressaisissez ce mot de passe dans la zone **Confirmation du mot de passe**.

4. Cliquez sur **OK** pour modifier le mot de passe.

Certificats SSL pour AppScan Enterprise Server

Une fois le serveur AppScan Enterprise Server installé, vous devez le configurer afin qu'il utilise un certificat SSL valide. Si vous ne le configurez pas, vous recevrez un message indiquant que la connexion n'est pas sécurisée lors de la connexion au serveur à partir d'AppScan Source for Analysis ou de l'interface de ligne de commande (CLI) d'AppScan Source, ou encore d'AppScan Source for Development sous Windows et Linux.

Emplacement de stockage du certificat SSL

Les certificats qui ont été acceptés de façon définitive sont stockés dans `<data_dir>\config\cacertspersonal` et `<data_dir>\config\cacertspersonal.pem` (où `<rép_données>` est l'emplacement de vos données de programme AppScan Source, comme décrit dans «Installation et emplacements des fichiers de données utilisateur», à la page 292). Supprimez ces deux fichiers si vous ne voulez plus que les certificats soient stockés de manière permanente.

AppScan Source for Automation et validation du certificat SSL

Par défaut, les certificats sont automatiquement acceptés lors de l'utilisation de AppScan Source for Automation. Ce comportement est déterminé par le paramètre `ounceautod_accept_ssl` dans le fichier de configuration du serveur Automation Server (`<data_dir>\config\ounceautod.ozsettings` (où `<rép_données>` est l'emplacement de vos données de programme AppScan Source, comme décrit dans «Installation et emplacements des fichiers de données utilisateur», à la page 292)). Si ce paramètre est modifié en remplaçant `value="true"` par `value="false"`, la validation SSL sera tentée et la connexion à ou la publication sur AppScan Enterprise Console échouera avec un message d'erreur en cas de détection d'un certificat non valide.

interface de ligne de commande (CLI) d'AppScan Source et validation du certificat SSL

Par défaut, lors de l'utilisation de la commande CLI `login`, la validation SSL est tentée et la connexion à AppScan Enterprise Console, ou la publication sur la console, échoue avec un message d'erreur si un certificat non valide est détecté (si vous n'avez pas déjà accepté définitivement le certificat en vous connectant via un autre produit client AppScan Source). Ce comportement peut être modifié à l'aide du paramètre `-acceptssl` en option lors de l'exécution de la commande `login`. Lorsque ce paramètre est utilisé, les certificats SSL sont automatiquement acceptés.

AppScan Source et l'accessibilité

L'accessibilité concerne les utilisateurs atteints d'un handicap physique, tel qu'une mobilité réduite ou une vision limitée. Les problèmes d'accessibilité peuvent empêcher un utilisateur d'utiliser un produit logiciel avec succès. Cette rubrique présente les problèmes d'accessibilité connus liés à AppScan Source, ainsi que les solutions pour les contourner.

Utilisation du logiciel de lecture d'écran JAWS avec le programme d'installation de AppScan Source

Pour utiliser Freedom Scientific JAWS (http://www.freedomscientific.com/products/fs/jaws-product-page.asp) lorsque vous exécutez le programme d'installation d'AppScan Source, vous devez installer Java Access Bridge sur la machine virtuelle Java d'AppScan Source. Cela permet à JAWS de prononcer correctement les libellés et les commandes dans les panneaux du programme d'installation.

- Vous trouverez des informations sur le logiciel Java Access Bridge (y compris le lien de téléchargement et les instructions d'installation) à l'adresse http://www.oracle.com/technetwork/java/javase/tech/index-jsp-136191.html.
- Vous trouverez aussi des informations sur les conditions InstallAnywhere requises pour l'installation de Java Access Bridge à l'adresse http://kb.flexerasoftware.com/selfservice/documentLink.do?externalID=Q200311.

Utilisation du logiciel de lecture d'écran JAWS dans les panneaux d'interface utilisateur avec du texte descriptif

De nombreuses parties de l'interface utilisateur AppScan Source contiennent du texte descriptif. Dans la plupart des cas, vous devez utiliser la combinaison de touches JAWS `Inser+B` pour pouvoir lire ce texte descriptif.

Remarques

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 donne 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 en contactant le Service Propriété Intellectuelle d'IBM dans votre pays ou en écrivant 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
2Z4A/101
11400 Burnet Road
Austin, TX 78758
U.S.A.

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

Le programme sous licence décrit dans le présent document et tous les éléments sous licence disponibles s'y rapportant sont fournis par IBM conformément aux dispositions du Livret Contractuel IBM, des Conditions internationales d'utilisation des Logiciels IBM ou de tout autre contrat équivalent.

Les données de performance indiquées dans ce document ont été déterminées dans un environnement contrôlé. Par conséquent, les résultats peuvent varier de manière significative selon l'environnement d'exploitation utilisé. Certaines mesures évaluées sur des systèmes en cours de développement ne sont pas garanties sur tous les systèmes disponibles. En outre, elles peuvent résulter d'extrapolations. Les résultats peuvent donc varier. Il incombe aux utilisateurs de ce document de vérifier si ces données sont applicables à leur environnement d'exploitation.

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

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.

Tous les tarifs IBM indiqués sont les prix de vente actuels suggérés par IBM et sont susceptibles d'être modifiés sans préavis. Les tarifs appliqués peuvent varier selon les revendeurs.

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

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

LICENCE DE COPYRIGHT :

Le présent logiciel contient des exemples de programmes d'application en langage source destinés à illustrer les techniques de programmation sur différentes plateformes d'exploitation. Vous avez le droit de copier, de modifier et de distribuer ces exemples de programmes sous quelque forme que ce soit et sans paiement d'aucune redevance à IBM, à des fins de développement, d'utilisation, de vente ou de distribution de programmes d'application conformes aux interfaces de programmation des plateformes pour lesquels ils ont été écrits ou aux interfaces de programmation IBM. Ces exemples de programmes n'ont pas été rigoureusement testés dans toutes les conditions. Par conséquent, IBM ne peut garantir expressément ou implicitement la fiabilité, la maintenabilité ou le fonctionnement de ces programmes. Vous avez le droit de copier, de modifier et de distribuer ces exemples de programmes sous quelque forme que ce soit et sans paiement d'aucune redevance à IBM, à des fins de développement, d'utilisation, de vente ou de distribution de programmes d'application conformes aux interfaces de programmation IBM.

Toute copie totale ou partielle de ces programmes exemples et des oeuvres qui en sont dérivées doit comprendre une notice de copyright, libellée comme suit :

© (nom de votre société) (année). Des segments de code sont dérivés des Programmes exemples d'IBM Corp. © Copyright IBM Corp. _saisissez l'année ou les années_. All rights reserved.

Si vous visualisez ces informations en ligne, il se peut que les photographies et illustrations en couleur n'apparaissent pas à l'écran.

Marques

IBM, le logo IBM et ibm.com sont des marques d'International Business Machines Corp. dans de nombreux pays. Les autres noms de produits et de services 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 à l'adresse www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript, ainsi que toutes les marques incluant Adobe, sont des marques d'Adobe Systems Incorporated aux Etats-Unis et/ou dans certains autres pays.

IT Infrastructure Library est une marque de Central Computer and Telecommunications Agency, qui fait désormais partie de Office of Government Commerce.

Intel, le logo Intel, Intel Inside, le logo Intel Inside, Intel Centrino, le logo Intel Centrino, Celeron, Intel Xeon, Intel SpeedStep, Itanium et Pentium sont des marques d'Intel Corporation ou ses filiales aux Etats-Unis et dans certains autres pays.

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

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

ITIL est une marque de The Office of Government Commerce et est enregistrée au bureau américain Patent and Trademark Office.

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

Java ainsi que tous les logos et toutes les marques incluant Java sont des marques d'Oracle et/ou de ses sociétés affiliées.

Cell Broadband Engine est une marque de Sony Computer Entertainment, Inc. aux Etats-Unis et/ou dans certains autres pays, utilisée sous licence.

Linear Tape-Open, LTO, le logo LTO, Ultrium et le logoUltrium sont des marques d'HP, IBM Corp. et Quantum aux Etats-Unis et dans d'autres pays.

Copyright

(C) Copyright IBM Corp. et ses concédants de licence 2003, 2017. All Rights Reserved.

IBM, le logo IBM, ibm.com Rational, AppScan, Rational Team Concert, WebSphere et ClearQuest sont des marques d'International Business Machines Corp. dans de nombreux pays. Les autres noms de sociétés, de produits et de services peuvent

appartenir à IBM ou à des tiers. La liste actualisée de toutes les marques d'IBM est disponible sur la page Web "Copyright and trademark information" à l'adresse http://www.ibm.com/legal/copytrade.shtml. Linux est une marque de Linus Torvalds aux Etats-Unis et/ou dans certains autres pays. Microsoft, Windows, Windows NT et le logo Windows sont des marques de Microsoft Corporation 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. Java ainsi que tous les logos et toutes les marques incluant Java sont des marques d'Oracle et/ou de ses sociétés affiliées.

Ce programme inclut : Jacorb 2.3.0, Copyright 1997-2006 Le projet JacORB et XOM1.0d22, Copyright 2003 Elliotte Rusty Harold, chacun d'eux étant disponible sous licence LGPL (Gnu Library General Public License) dont une copie figure dans le fichier des remarques accompagnant ce programme.

Chapitre 2. Configuration d'applications et de projets

Avant de pouvoir effectuer un examen, vous devez configurer les applications et les projets. Cette section décrit les assistants Application Discovery Assistant, Nouvelle application et Nouveau projet. Vous apprendrez à configurer les attributs pour AppScan Source for Analysis. Cette section vous explique également comment ajouter des applications et des projets existants pour leur examen et comment ajouter des fichiers à des projets.

Remarque : Vous ne pouvez pas créer un projet pour un projet Xcode. Les projets Xcode sont importés dans AppScan Source for Analysis en tant qu'applications ou ajoutés aux applications en tant que projets existants. Pour plus d'informations, voir «Ajout d'une application existante», à la page 42 ou «Ajout d'un projet existant», à la page 50.

La configuration de AppScan Source for Analysis inclut la création de l'application, la configuration du code source et la configuration des attributs. Après la configuration et l'examen, l'étape suivante est le triage. Vous pouvez configurer le code source depuis la vue Propriétés ou à l'aide de l'assistant Nouveau projet. Ce chapitre est destiné à vous guider le long des opérations de l'assistant. Reportez-vous à la rubrique «Vue Propriétés», à la page 255 pour une présentation des propriétés d'application et de projet.

AppScan Source for Analysis utilise un modèle d'application/de projet qui importe directement des projets Xcode, Eclipse, Rational Application Developer for WebSphere Software (RAD) ou AppScan Source créés précédemment avec les utilitaires AppScan Source (pour plus de détails, voir le document *Utilitaires IBM Security AppScan Source - Guide d'utilisation*).

Vous pouvez ajouter et configurer des projets de différents types et contenant une variété de langages, en spécifiant les paramètres recueillis depuis le codebase cible et ses procédures de construction. Lors de la configuration, vous pouvez spécifier des répertoires et des fichiers à exclure de l'examen.

Avant d'effectuer un examen, vous devez configurer les *applications* et les *projets*. Une application est un conteneur de projets ; un projet désigne l'ensemble de fichiers à examiner et les paramètres (configuration) utilisés.

Fichiers d'application et de projet AppScan Source

Les applications et les projets AppScan Source ont des fichiers correspondants qui contiennent les informations de configuration requises pour l'examen et pour la personnalisation du triage. Il est recommandé de placer ces fichiers dans le même répertoire que le code source car les informations de configuration (dépendances, options du compilateur, etc.) requises pour générer les projets sont très similaires à celles requises pour que AppScan Source puisse les examiner avec succès. Les meilleures pratiques sont de gérer ces fichiers avec votre système de contrôle des sources.

Les applications et les projets créés dans AppScan Source for Analysis ont respectivement une extension `.paf` et `.ppf`. Ces fichiers sont générés lorsque vous

créez et configurez manuellement une application ou un projet dans AppScan Source for Analysis, AppScan Source for Automation et l'interface de ligne de commande d'AppScan Source.

Sous Windows, lorsque vous importez des solutions et des projets Visual Studio dans AppScan Source for Analysis, AppScan Source for Automation ou l'interface de ligne de commande d'AppScan Source, des fichiers correspondants avec des extensions `.sln.gaf` et `.vcproj.gpf` sont créés.

Sous macOS, lorsque vous importez des répertoires et des dossiers Xcode, des fichiers dotés d'une extension `.xcodeproj.gaf` et `.xcodeproj.gpf` sont créés pour ceux-ci. De même, si vous importez un espace de travail Xcode, un fichier ayant l'extension `.xcworkspace.gaf` est créé.

Remarque : Quand un importateur Eclipse s'exécute sur un espace de travail Eclipse ou Rational Application Developer for WebSphere Software (RAD), AppScan Source crée des fichiers intermédiaires avec des extensions `.ewf` et `.epf`. Ces fichiers sont requis pour l'importation initiale dans AppScan Source for Analysis et pour les examens ultérieurs.

Important : Si vous travaillez avec un projet AppScan Source comportant des dépendances dans un environnement de développement (par exemple un projet IBM MobileFirst Platform), veillez à créer le projet dans l'environnement de développement avant de l'importer. Après avoir importé le projet, si vous modifiez des fichiers qu'il contient, pensez à le régénérer dans l'environnement de développement avant l'analyse dans AppScan Source (si vous omettez cette étape, les modifications apportées aux fichiers ne seront pas prises en compte par AppScan Source).

Tableau 2. Fichiers AppScan Source

Extension de fichier AppScan Source	Description
`ppf`	• Fichier de projet AppScan Source • Généré lorsque vous créez un projet avec AppScan Source for Analysis ou les utilitaires AppScan Source pris en charge • Nommé par l'utilisateur
`paf`	• Fichier d'application AppScan Source • Généré lorsque vous créez une application avec AppScan Source for Analysis ou les utilitaires AppScan Source pris en charge • Nommé par l'utilisateur

`sln.gaf`	• Fichier d'application AppScan Source généré quand vous importez des solutions Visual Studio
	• Utilisé pour stocker des informations d'application personnalisées telles que les exclusions et les regroupement
	• Adopte le nom de l'espace de travail ou de la solution importé Par exemple :
	`d:\mes_appls\monappl.sln`
	`d:\mes_appls\monappl.sln.gaf`

Tableau 2. Fichiers AppScan Source (suite)

Extension de fichier AppScan Source	Description

`vcproj.gpf`	• Fichier de projet AppScan Source généré quand vous importez des projets Visual Studio
	• Utilisé pour stocker des informations de projet personnalisées telles que les schémas et les exclusions
	• Adopte le nom du projet importé. Par exemple :
	`d:\mes_projets\monprojet.vcproj`
	`d:\mes_projets\monprojet.vcproj.gpf`

`xcodeproj.gaf`	• Fichier d'application AppScan Source généré lors de l'importation de répertoires Xcode
	• Utilisé pour stocker des informations d'application personnalisées telles que les exclusions et les regroupement
	• Adopte le nom de l'espace de travail ou de la solution importé Par exemple :
	`/Users/myUser/myProject.xcodeproj`
	`/Users/myUser/myProject.xcodeproj.gaf`

`xcodeproj.gpf`	• Fichier de projet AppScan Source généré lors de l'importation de projets Xcode
	• Utilisé pour stocker des informations de projet personnalisées telles que les schémas et les exclusions
	• Adopte le nom du projet importé, par exemple :
	`/Users/myUser/myProject.xcodeproj`
	`/Users/myUser/myProject.xcodeproj.gpf`

`xcworkspace.gaf`	• Fichier d'application AppScan Source qui est généré lorsque vous importez un espace de travail Xcode • Utilisé pour stocker des informations d'application personnalisées telles que les exclusions et les regroupement • Adopte le nom du projet importé, Par exemple : `/Users/myUser/myProj.xcworkspace.gaf`

Tableau 2. Fichiers AppScan Source (suite)

Extension de fichier AppScan Source	Description
ewf	• Fichier d'espace de travail Eclipse • Produit lorsque vous importez un espace de travail Eclipse dans AppScan Source • L'exportateur Eclipse crée le fichier sur la base des informations de l'espace de travail Eclipse - AppScan Source, puis importe le fichier
epf	• Fichier de projet Eclipse • Produit lorsqu'un projet Eclipse est importé dans AppScan Source • L'exportateur Eclipse crée le fichier sur la base des informations du projet Eclipse - AppScan Source, puis importe le fichier

Conseil : Lorsque vous utilisez les outils d'intégration de génération (build) pris en charge (par exemple, Ounce/Ant ou Ounce/Maven) pour générer des fichiers d'application et de projet AppScan Source, il est recommandé de mettre à jour ces fichiers dans le contrôle des sources dans le cadre de l'automatisation de la génération, afin de faciliter leur partage par l'équipe de développement. Lorsqu'un développeur met à jour la vue locale des fichiers dans le contrôle des sources, les fichiers d'application et de projet AppScan Source sont également mis à jour. Ceci garantit que toute l'équipe travaille avec un ensemble cohérent de fichiers.

Remarque : Pour savoir quelles versions des fichiers importés sont prises en charge par AppScan Source for Analysis, AppScan Source for Automation et l'interface de ligne de commande d'AppScan Source, voir http://www.ibm.com/support/docview.wss?uid=swg27027486. Dans cette page, sélectionnez l'onglet de la version d'AppScan Source que vous utilisez, puis sélectionnez le composant AppScan Source que vous utilisez. Si AppScan Source prend en charge l'ouverture et l'examen de fichiers provenant d'autres environnements de développement, cette prise en charge est indiquée à la section **Compilateurs et langues** de l'onglet **Logiciels pris en charge**.

Configuration d'applications

Vous pouvez utiliser l'assistant Nouvelle application ou l'Application Discovery Assistant pour créer des applications. L'Application Discovery Assistant automatise la configuration de l'application, tandis que l'assistant Nouvelle application vous permet d'ajouter des applications en vous guidant tout au long du processus de configuration. Cet assistant vous aide à créer manuellement un projet ou à ajouter des projets existants à une application. Cette section décrit ces deux méthodes pour l'ajout d'application et les tâches de configuration de base.

Remarque : Vous ne pouvez pas créer un projet pour un projet Xcode. Les projets Xcode sont importés dans AppScan Source for Analysis en tant qu'applications ou ajoutés aux applications en tant que projets existants. Pour plus d'informations, voir «Ajout d'une application existante», à la page 42 ou «Ajout d'un projet existant», à la page 50.

Remarque : L'Application Discovery Assistant permet de créer et de configurer rapidement des applications et des projets pour le code source Java ou les espaces

de travail Eclipse ou IBM Rational Application Developer for WebSphere Software (RAD) qui contiennent des projets Java. Pour créer une application à partir de tout autre langage pris en charge, utilisez l'assistant Nouvelle application ou importez les applications prises en charge dans AppScan Source for Analysis.

Vous devez créer une nouvelle application (voir «Création d'une application à l'aide de l'assistant Nouvelle application», à la page 38 ou «Utilisation de l'Application Discovery Assistant pour créer des applications et des projets», à la page 38) ou ajouter une application existante (voir «Ajout d'une application existante», à la page 42) avant d'ajouter des projets.

Le tableau suivant répertorie les types de fichiers d'application que vous pouvez ouvrir et examiner à l'aide de AppScan Source for Analysis.

Tableau 3. Types de fichiers d'application pris en charge

Application	**Type de fichier**
Xcode for Objective-C (pour des applications iOS uniquement) **Remarque :** Pour savoir quelles versions des fichiers importés sont prises en charge par AppScan Source for Analysis, AppScan Source for Automation et l'interface de ligne de commande d'AppScan Source, voir http://www.ibm.com/support/docview.wss?uid=swg27027486. Dans cette page, sélectionnez l'onglet de la version d'AppScan Source que vous utilisez, puis sélectionnez le composant AppScan Source que vous utilisez. Si AppScan Source prend en charge l'ouverture et l'examen de fichiers provenant d'autres environnements de développement, cette prise en charge est indiquée à la section **Compilateurs et langues** de l'onglet **Logiciels pris en charge**.	`.xcodeproj` ou `.xcworkspace`
• Espace de travail Eclipse (Java uniquement) • Espace de travail RAD (Java uniquement) Voir la configuration requise pour AppScan Source pour savoir quelles versions d'Eclipse et de RAD sont prises en charge pour l'examen de l'espace de travail).	`<répertoire de l'espace de travail>` ou `.ewf` Le répertoire de l'espace de travail contient un répertoire supplémentaire : `.metadata`.
Fichier d'application AppScan Source	`.paf`

Conseil : Une icône figure dans la vue Explorateur pour indiquer une application importée (voir «Indicateurs d'application et de projet», à la page 71).

Remarque : Lorsque des applications et des projets sont créés à l'aide de l'assistant Nouvelle application et de l'assistant Nouveau projet, leur nom de fichier est défini automatiquement en fonction du **nom** saisi dans l'assistant (par exemple, si un projet est créé et **MyProject** est saisi dans la zone **Nom**, le nom de fichier du projet est `MyProject.ppf`). Les noms d'application et de projet peuvent être modifiés à l'aide de la vue Propriétés.

Création d'une application à l'aide de l'assistant Nouvelle application

Procédure

1. Effectuez l'une des actions suivantes :
   - Sélectionnez **Fichier** > **Ajouter une application** > **Créer une nouvelle application** dans la barre de menus principale.
   - Dans la barre d'outils de la vue Explorateur, cliquez sur la flèche vers le bas du bouton **Ajouter un menu d'application** et sélectionnez **Créer une nouvelle application** dans le menu.
   - Depuis la vue Explorateur, cliquez avec le bouton droit de la souris sur **Toutes les applications**, puis sélectionnez dans le menu **Ajouter une application** > **Créer une nouvelle application**.
2. Entrez un **Nom** pour l'application.
3. Accédez au **Répertoire de travail** dans lequel sauvegarder l'application. La nouvelle application reçoit l'extension de nom de fichier `.paf`.
4. Cliquez sur **Suivant** pour configurer les projets composant l'application ou sur **Terminer** pour ajouter l'application sans configurer de projets. Vous pourrez accéder à des informations d'aide sur la configuration et l'ajout de projets plus loin dans la présente section.

Utilisation de l'Application Discovery Assistant pour créer des applications et des projets

AppScan Source inclut un assistant Application Discovery Assistant puissant qui vous permet de créer et de configurer rapidement des applications et des projets pour le code source Java. L'Application Discovery Assistant vous permet également de localiser les espaces de travail Eclipse ou Rational Application Developer for WebSphere Software (RAD) qui contiennent les projets Java. La fonction Application Discovery Assistant vous permet de pointer vers le répertoire source ou d'espace de travail. AppScan Source s'occupe ensuite du reste.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser la fonction Application Discovery Assistant pour rechercher un emplacement contenant une combinaison de source Java et/ou d'espaces de travail Eclipse. Le panneau final de l'Application Discovery Assistant vous permet de spécifier des préférences de structure d'application/de projet uniquement pour Java. Ce panneau n'a aucune influence sur l'emplacement des fichiers d'application et de projet des espaces de travail Eclipse où les fichiers d'application sont automatiquement placés à la racine de l'espace de travail et les fichiers de projet sont automatiquement placés à la racine des projets de l'espace de travail.

Procédure

1. Effectuez l'une des actions suivantes pour lancer l'Application Discovery Assistant :
   - Sélectionnez **Fichier** > **Ajouter une application** > **Reconnaître les applications** dans la barre de menus principale.
   - Dans la section **Démarrage rapide** de la vue Explorateur, sélectionnez **Reconnaître les applications**.
   - Dans la barre d'outils de la vue Explorateur, cliquez sur la flèche vers le bas du bouton **Ajouter un menu d'application** et sélectionnez **Reconnaître les applications** dans le menu.

- Dans la vue Explorateur, cliquez avec le bouton droit sur **Toutes les applications** et sélectionnez **Ajouter une application** > **Reconnaître les applications** dans le menu.

2. Dans le panneau Emplacement de recherche, indiquez l'emplacement contenant le code source ou les espaces de travail à examiner. Vous pouvez également définir un démarrage immédiat de l'examen après la fin de la reconnaissance des applications.

   Vous pouvez ensuite cliquer sur **Suivant** pour définir des options supplémentaires pour l'Application Discovery Assistant (par exemple, la spécification de dépendance externe, les règles d'exclusion et les préférences de structure d'application/de projet Java) ou cliquer sur **Démarrer** pour lancer la reconnaissance des applications. Si vous cliquez sur **Démarrer** :

   - Aucun emplacement de dépendance externe ne sera défini. Si votre application comporte des dépendances externes et qu'elles ne sont pas spécifiées, les résultats d'examen subiront un impact négatif.
   - Les règles d'exclusion prêtes à l'emploi seront utilisées (voir «Règles d'exclusion par défaut de la fonction Application Discovery Assistant», à la page 41 pour obtenir la liste des règles par défaut).
   - Si vous localisez la source Java, un projet et une application seront créés (ce projet unique contiendra toutes les racines source détectées).

   Si vous cliquez sur **Suivant**, passez à l'étape suivante.

3. Dans le panneau Dépendances externes, définissez un chemin pour chaque dépendance externe associée à votre application (par exemple, un chemin vers un kit JDK ou un serveur Web). Pour compléter ce panneau, suivez les instructions ci-après :

   a. Pour ajouter une dépendance externe, cliquez dans la table ou cliquez sur **Ajouter**, puis entrez le chemin de dépendance externe ou recherchez-le à l'aide de la fonction Parcourir.

      Conseil : La saisie de données dans la zone de chemin de dépendance pendant son édition provoque l'affichage des répertoires disponibles en sélection. Vous devez entrer au moins une lettre d'unité. Concernant le chemin spécifié, tous les dossiers qu'il contient seront affichés.

   b. Pour supprimer un chemin de dépendance externe, sélectionnez-le et cliquez sur **Supprimer**.

   c. Pour modifier un chemin de dépendance externe, cliquez dans le chemin, puis entrez le chemin de dépendance externe ou recherchez-le à l'aide de la fonction Parcourir.

   Vous pouvez ensuite cliquer sur **Suivant** pour définir des options supplémentaires pour l'Application Discovery Assistant ou cliquer sur **Démarrer** pour lancer la reconnaissance des applications. Si vous cliquez sur **Démarrer** :

   - Les règles d'exclusion prêtes à l'emploi seront utilisées (voir «Règles d'exclusion par défaut de la fonction Application Discovery Assistant», à la page 41 pour obtenir la liste des règles par défaut).
   - Si vous localisez la source Java, un projet et une application seront créés (ce projet unique contiendra toutes les racines source détectées).

   Si vous cliquez sur **Suivant**, passez à l'étape suivante.

4. Dans le panneau Règles d'exclusion, indiquez les règles de filtrage des fichiers et répertoires. Les règles sont définies par PERL, Grep, EGrep ou expression régulière de correspondance exacte. Par exemple, si vous souhaitez exclure un

répertoire nommé `temp` de la recherche via la Application Discovery, vous pouvez ajouter une règle d'exclusion PERL `.*[\\/]temp`.

Par défaut, un jeu d'expressions régulières PERL est fourni pour exclure certains répertoires courants (voir «Règles d'exclusion par défaut de la fonction Application Discovery Assistant», à la page 41 pour obtenir la liste complète). Pour modifier cette liste ou créer de nouvelles règles, suivrez les instructions ci-après :

a. Pour modifier une règle d'exclusion existante, cliquez sur la règle pour activer l'éditeur de règles. Une fois l'édition de la règle terminée, cliquez en dehors de la règle ou appuyez su la touche **Entrée**.

   Pour modifier le type d'expression régulière d'une règle existante, cliquez dans la cellule **Type RegEx** de la règle, puis sélectionnez un type d'expression régulière dans le menu.

b. Pour ajouter une règle d'exclusion, cliquez sur **Ajouter**. Vous ajoutez ainsi une nouvelle règle à la table, règle que vous pouvez modifier en suivant les instructions de modification de règle mentionnées précédemment.

c. Pour supprimer une règle d'exclusion, sélectionnez-la et cliquez sur **Supprimer** (ou cliquez sur **Supprimer tout** pour supprimer toutes les règles d'exclusion actuellement répertoriées dans la panneau).

Important : Les règles d'exclusion valides sont signalées par une coche dans la table et les règles non valides sont signalées par un `X` rouge. Vous ne pourrez pas démarrer Application Discovery ou poursuivre l'exécution de l'Application Discovery Assistant tant que toutes les règles ne seront pas valides.

A ce stade :

- Si vous recherchez uniquement une source Java, vous pouvez cliquer sur **Suivant** pour définir les préférences de structure d'application/de projet de l'Application Discovery Assistant. Vous pouvez aussi cliquer sur **Démarrer** pour exécuter l'assistant.
- Si vous recherchez uniquement des espaces de travail Eclipse, cliquez sur **Démarrer** pour exécuter l'assistant. Si vous cliquez sur **Suivant**, l'assistant passera à un panneau qui concerne uniquement la reconnaissance de source Java.

Si vous cliquez sur **Suivant**, passez à l'étape suivante.

5. Le panneau Création d'application et de projet concerne uniquement la reconnaissance de source Java. Il vous permet de spécifier la structure des applications et projets qui seront créés :

   a. Pour créer un projet unique pour toutes les racines source détectées, sélectionnez **Créer un projet unique** dans le menu **Projets**. Suite à ce choix, vous ne pourrez créer qu'une application unique.

   b. Pour créer un projet distinct pur chaque racine source détectée, sélectionnez **Créer un projet pour chaque racine source trouvée** dans le menu **Projets**. Suite à ce choix, vous pourrez choisir de créer une ou plusieurs applications. Pour créer une application unique contenant tous les projets créés, sélectionnez **Créer une application unique** dans le menu **Applications**. Pour créer une application pour chaque projet créé, sélectionnez **Créer une application par projet** dans le menu **Applications**.

   De plus, choisissez un emplacement de stockage pour les fichiers de définition de l'application et du projet.

   Si vous choisissez **Organiser les fichiers pour moi** :

   - Si vous créez un projet unique, les fichiers de projet et d'application seront créés dans l'emplacement de recherche.

- Si vous créez un projet pour chaque racine source dans une application unique, le fichier de projet de chaque racine source sera créé dans le répertoire situé au-dessus de la racine source et le fichier d'application sera créé dans l'emplacement de recherche.
- Si vous créez un projet pour chaque racine source et une application pour chaque projet, les fichiers de projet et d'application de chaque racine source seront créés dans le répertoire situé au-dessus de la racine source.

Si vous spécifiez un répertoire, tous les fichiers de projet et d'application seront créés dans ce répertoire.

6. Si vous souhaitez modifier certains des paramètres définis dans les panneaux précédents, cliquez sur **Précédent**. Une fois que vous êtes satisfait des paramètres d'Application Discovery, cliquez sur **Démarrer** pour examiner l'emplacement de recherche afin d'y détecter des racines source.

Résultats

Une fois l'exécution d'Application Discovery terminée, les nouvelles applications et les nouveaux projets créés en tant que résultats d'Application Discovery s'affichent dans la vue Explorateur et sont prêts pour l'examen (si vous avez défini l'examen afin qu'il commence immédiatement après la fin de la reconnaissance d'applications, l'examen démarre).

Si des problèmes sont survenus pendant la reconnaissance, l'Application Discovery Assistant fournit un rapport de reconnaissance après son exécution. Par exemple, si votre application possède des dépendances externes qui n'ont pas été spécifiées dans le panneau Dépendances externes, le rapport contiendra des avertissements indiquant que les dépendances externes ne peuvent pas être résolues. Dans le rapport de reconnaissance :

- Cliquez sur **Terminer** pour créer les applications et les projets. Si l'option **Ignorer les avertissements et procéder à l'examen dans tous les cas** est sélectionnée, les applications et les projets sont analysés immédiatement.
- Cliquez sur **Précédent** pour modifier les paramètres de Application Discovery Assistant ou réexécuter Application Discovery.
- Cliquez sur **Annuler** pour fermer le rapport de reconnaissance sans créer d'applications ou de projets.

Règles d'exclusion par défaut de la fonction Application Discovery Assistant

Lorsque vous utilisez la fonction Application Discovery Assistant, les règles d'exclusion par défaut sont utilisées si le panneau Règles d'exclusion n'est pas modifié ou si vous démarrez Application Discovery après avoir spécifié le répertoire de recherche. Les règles d'exclusion par défaut de Application Discovery sont répertoriées dans cette rubrique.

Tableau 4. Règles d'exclusion par défaut de la fonction Application Discovery

Règle d'exclusion	Type d'expression régulière
`.*[\\/]example`	PERL
`.*[\\/]test`	PERL
`.*[\\/]demo`	PERL
`.*[\\/]sample`	PERL

Ajout d'une application existante

Vous pouvez ajouter des applications existantes pour examen en les glissant-déposant dans la vue Explorateur ou en utilisant l'action **Ajouter une application**. Vous pouvez également ajouter des fichiers `WAR` et `EAR` en les glissant-déposant dans la vue Explorateur.

Pour déterminer comment ajouter une application existante, consultez les rubriques suivantes :

- «Ajout d'une application existante à l'aide d'actions de l'interface utilisateur»
- «Ajout d'une application existante à l'aide d'une opération de glisser-déposer»

Ajout d'une application existante à l'aide d'actions de l'interface utilisateur

Procédure

1. Effectuez l'une des actions suivantes :
   - Sélectionnez **Fichier** > **Ajouter une application** > **Ouvrir une application existante** dans le menu principal du plan de travail.
   - Dans la barre d'outils de la vue Explorateur, cliquez sur la flèche vers le bas du bouton **Ajouter un menu d'application** et sélectionnez **Ouvrir une application existante** dans le menu.
   - Depuis la vue Explorateur, cliquez avec le bouton droit de la souris sur **Toutes les applications**, puis sélectionnez dans le menu **Ajouter une application** > **Ouvrir une application existante**.
2. Sélectionnez le répertoire contenant le fichier d'application sauvegardé (`.paf` ou `.ewf`), ou le répertoire `.xcodeproj` ou `.xcworkspace`.

   Remarque : Pour savoir quelles versions des fichiers importés sont prises en charge par AppScan Source for Analysis, AppScan Source for Automation et l'interface de ligne de commande d'AppScan Source, voir http://www.ibm.com/support/docview.wss?uid=swg27027486. Dans cette page, sélectionnez l'onglet de la version d'AppScan Source que vous utilisez, puis sélectionnez le composant AppScan Source que vous utilisez. Si AppScan Source prend en charge l'ouverture et l'examen de fichiers provenant d'autres environnements de développement, cette prise en charge est indiquée à la section **Compilateurs et langues** de l'onglet **Logiciels pris en charge**.
3. Ouvrez le fichier d'application ou le répertoire.

Ajout d'une application existante à l'aide d'une opération de glisser-déposer

Procédure

1. Depuis votre poste de travail, localisez l'application (`.paf`, `.war`, `.ear` ou `.ewf`) ou le répertoire (`.xcodeproj` ou `.xcworkspace`) que vous souhaitez ajouter à l'examen. Vous pouvez également ajouter un répertoire contenant des fichiers `.war` ou `.ear` (dans certains serveurs d'applications, ceux-ci sont appelés *dossiers de dépôt*).

   Remarque : Vous ne pouvez pas effectuer de glisser-déposer sur des répertoires d'espace de travail Eclipse.

   Remarque : Si vous ajoutez un fichier `.war` ou `.ear`, ou un répertoire contenant des fichiers `.war` ou `.ear`, les fichiers doivent se trouver sur votre système de fichiers local ou dans un répertoire monté.

Remarque : Pour savoir quelles versions des fichiers importés sont prises en charge par AppScan Source for Analysis, AppScan Source for Automation et l'interface de ligne de commande d'AppScan Source, voir http://www.ibm.com/support/docview.wss?uid=swg27027486. Dans cette page, sélectionnez l'onglet de la version d'AppScan Source que vous utilisez, puis sélectionnez le composant AppScan Source que vous utilisez. Si AppScan Source prend en charge l'ouverture et l'examen de fichiers provenant d'autres environnements de développement, cette prise en charge est indiquée à la section **Compilateurs et langues** de l'onglet **Logiciels pris en charge**.

2. Sélectionnez l'application, puis faites-la glisser dans la vue Explorateur.
3. Déposez votre sélection sur ou sous le noeud **Toutes les applications**.
4. Si vous ajoutez un fichier `.war` ou `.ear`, ou un répertoire contenant des fichiers `.war` ou `.ear`, une boîte de dialogue s'ouvre pour vous permettre de spécifier le serveur d'applications dans lequel le ou les fichiers seront déployés. Cliquez sur **OK** lorsque vous avez terminé.

Ajout de plusieurs applications

Au lieu d'ajouter une seule application à la fois lorsque vous commencez à travailler avec AppScan Source for Analysis, vous pouvez importer plusieurs applications. La boîte de dialogue Sélection d'applications permet de sélectionner un répertoire racine dans lequel rechercher des applications AppScan Source (`.paf`). Plusieurs applications peuvent également être ajoutées pour examen en les faisant glisser/déposer dans la vue Explorateur.

Remarque : Vous ne pouvez pas rechercher plusieurs répertoires de projet Xcode (`.xcodeproj`) ou d'espace de travail Xcode (`.xcworkspace`) via les actions disponibles dans l'interface utilisateur. Toutefois, vous pouvez faire glisser et déposer plusieurs répertoires de projet Xcode et d'espace de travail Xcode dans la vue Explorateur.

Pour déterminer comment ajouter plusieurs applications, consultez les rubriques ci-dessous :

- «Ajout de plusieurs applications à l'aide d'actions de l'interface utilisateur»
- «Ajout de plusieurs applications à l'aide d'une opération de glisser-déposer», à la page 44

Remarque : Pour ajouter plusieurs fichiers `WAR` et `EAR`, vous pouvez effectuer un glisser-déposer d'un répertoire contenant les fichiers. Pour plus d'informations, voir «Ajout d'une application existante à l'aide d'une opération de glisser-déposer», à la page 42.

Ajout de plusieurs applications à l'aide d'actions de l'interface utilisateur

Procédure

1. Sélectionnez **Fichier** > **Ajouter une application** > **Applications multiples** dans le menu principal du plan de travail.

   Remarque : Vous ne pouvez pas rechercher plusieurs répertoires de projet Xcode (`.xcodeproj`) ou d'espace de travail Xcode (`.xcworkspace`) via les actions disponibles dans l'interface utilisateur. Toutefois, vous pouvez faire glisser et déposer plusieurs répertoires de projet Xcode et d'espace de travail Xcode dans la vue Explorateur.

2. Dans la boîte de dialogue Sélection d'applications, accédez au répertoire racine qui contient les applications à importer. Cochez la case **Opération récursive dans les sous-répertoires** pour effectuer une recherche dans les sous-répertoires.
3. Effectuez l'une des actions suivantes :
   - Cliquez sur **Terminer** pour importer les applications et les ajouter à la vue Explorateur.
   - Cliquez sur **Suivant** pour afficher les résultats de la recherche et sélectionner les applications à importer. Cliquez ensuite sur **Terminer**.

   Remarque : Pour savoir quelles versions des fichiers importés sont prises en charge par AppScan Source for Analysis, AppScan Source for Automation et l'interface de ligne de commande d'AppScan Source, voir http://www.ibm.com/support/docview.wss?uid=swg27027486. Dans cette page, sélectionnez l'onglet de la version d'AppScan Source que vous utilisez, puis sélectionnez le composant AppScan Source que vous utilisez. Si AppScan Source prend en charge l'ouverture et l'examen de fichiers provenant d'autres environnements de développement, cette prise en charge est indiquée à la section **Compilateurs et langues** de l'onglet **Logiciels pris en charge**.

Ajout de plusieurs applications à l'aide d'une opération de glisser-déposer

Procédure

1. Depuis votre poste de travail, localisez les applications (fichiers `.paf` ou `.ewf`) ou répertoires (`.xcodeproj` ou `.xcworkspace`) à ajouter à l'examen.

   Remarque : Vous ne pouvez pas effectuer de glisser-déposer sur des répertoires d'espace de travail Eclipse.

   Remarque : Pour savoir quelles versions des fichiers importés sont prises en charge par AppScan Source for Analysis, AppScan Source for Automation et l'interface de ligne de commande d'AppScan Source, voir http://www.ibm.com/support/docview.wss?uid=swg27027486. Dans cette page, sélectionnez l'onglet de la version d'AppScan Source que vous utilisez, puis sélectionnez le composant AppScan Source que vous utilisez. Si AppScan Source prend en charge l'ouverture et l'examen de fichiers provenant d'autres environnements de développement, cette prise en charge est indiquée à la section **Compilateurs et langues** de l'onglet **Logiciels pris en charge**.
2. Sélectionnez les applications ou les répertoires et faites-les glisser dans la vue Explorateur.
3. Déposez votre sélection sur ou sous le noeud **Toutes les applications**.

Importation d'applications Java à partir de serveurs d'applications Apache Tomcat et de profil Liberty WebSphere Application Server

Si des applications Java existantes ont été déployées sur un serveur d'applications pris en charge, vous ne pouvez pas les importer automatiquement dans AppScan Source.

Avant de commencer

Pour savoir quelles versions d'Apache Tomcat et du profil Liberty WebSphere Application Server sont prises en charge, reportez-vous à la configuration système

requise par AppScan Source. Dans cette page, sélectionnez l'onglet de la version d'AppScan Source que vous utilisez, puis sélectionnez le composant AppScan Source for Analysis. Les serveurs d'applications pris en charge se trouvent dans la section des **logiciels pris en charge**.

Procédure

1. Effectuez l'une des actions suivantes :
   - Sélectionnez **Fichier** > **Ajouter une application** > **Importer depuis un serveur d'applications** dans le menu de plan de travail principal.
   - Dans la barre d'outils de la vue Explorateur, cliquez sur la flèche vers le bas du bouton **Ajouter un menu d'application** et sélectionnez **Importer depuis un serveur d'applications** dans le menu.
   - Depuis la vue Explorateur, cliquez avec le bouton droit de la souris sur **Toutes les applications**, puis sélectionnez dans le menu **Ajouter une application** > **Importer depuis un serveur d'applications**.
2. Dans la boîte de dialogue Importer depuis un serveur d'applications, cliquez sur **Parcourir** pour rechercher et sélectionner l'emplacement dans lequel le serveur d'applications est installé ou entrez le chemin d'accès et le répertoire dans la zone, puis cliquez sur **Rechercher** pour rechercher des applications dans l'emplacement entré. Si l'emplacement est reconnu comme un serveur d'applications pris en charge, les applications disponibles sont répertoriées dans la section **Applications à importer** de la boîte de dialogue. Dans cette section, sélectionnez les applications à importer, puis cliquez sur **OK**.
3. Une application AppScan Source est créée pour chaque application importée du serveur d'applications.

Résultats

Si vous effectuez une importation à partir d'un serveur de profil Liberty WebSphere Application Server (WebSphere Application Server version 8.5 ou ultérieure), vous risquez de recevoir un message indiquant qu'une précompilation JSP manuelle est requise. Cela est dû au fait que le serveur de profil Liberty n'inclut pas de compilateur JSP autonome. Si vous recevez ce message, supprimez les applications créées lors de l'importation, puis suivez les instructions de la rubrique «Génération de pages JavaServer précompilées pour un profil Liberty WebSphere Application Server», à la page 46 et effectuez à nouveau une importation à partir du serveur d'applications.

Une fois l'application importée, AppScan Source examine par défaut uniquement ses fichiers JSP et le contenu de `web-inf/classes`. Le contenu de `web-inf/lib` n'est pas examiné. Si vous souhaitez que d'autres fichiers fassent l'objet d'un examen, vous pouvez utiliser les propriétés du projet pour définir des extensions de fichier supplémentaires à examiner (voir «Extensions de fichier», à la page 222). Par exemple, si vous souhaitez que les fichiers `.jar` soient examinés (y compris les fichiers figurant dans `web-inf/lib`), suivez les instructions de modification des propriétés du projet dans «Modification des propriétés d'une application et d'un projet», à la page 64. Dans la vue Propriétés du projet, sélectionnez l'onglet «Extensions de fichier», à la page 222. Dans la section Extensions supplémentaires de la vue, cliquez sur **Ajouter une extension**. Dans la boîte de dialogue Nouvelle extension, entrez `jar` dans la zone **Extension**, puis sélectionnez **Examiner les fichiers avec cette extension** et cliquez sur **OK**. Cliquez sur **Sauvegarder** en haut à droite de la vue (ou sélectionnez **Fichier** > **Sauvegarder** dans le menu principal) et

examinez à nouveau le projet. Si vous ne souhaitez pas examiner certains fichiers, vous pouvez les exclure des examens dans l'onglet «Sources», à la page 223 de la vue Projet.

Si les applications sur le serveur sont modifiées et que vous souhaitez actualiser les applications AppScan Source afin que le contenu modifié y apparaisse, vous devez effectuer à nouveau les étapes ci-dessus (vous n'avez pas besoin de supprimer les applications d'origine au préalable ; AppScan Source les supprimera automatiquement lors de la réimportation).

Remarque : Si vous importez un fichier `.war` à partir d'un serveur, puis que vous importez un autre fichier `.war` du même nom à partir d'un autre serveur, le second fichier `.war` écrase le premier fichier. Pour éviter ce comportement, renommez le second fichier `.war` avant de l'importer.

Génération de pages JavaServer précompilées pour un profil Liberty WebSphere Application Server

Si vous importez des applications depuis un profil Liberty WebSphere Application Server (WebSphere Application Server version 8.5 et suivante), une précompilation JSP manuelle est requise (le profil Liberty n'inclut pas de compilateur JSP autonome). La présente rubrique décrit les étapes nécessaires pour configurer une précompilation JSP manuelle.

Procédure

1. Suivez les instructions de création d'un serveur de profil Liberty figurant dans WebSphere Application Server Network Deployment Knowledge Center. Pour WebSphere Application Server version 8.5.5, reportez-vous à la rubrique Création d'un serveur de profil Liberty à l'aide d'outils de développement.
2. Dans le fichier `server.xml` du profil Liberty, ajoutez ce qui suit à la section `server description` :

   ```
   <jspEngine prepareJSPs="0"/>
   <webContainer deferServletLoad="false"/>
   ```

   Par exemple :

   ```
   <server description="new server">

       <!-- Enable features -->
       <featureManager>
           <feature>jsp-2.2</feature>
           <feature>localConnector-1.0</feature>
          <feature>appSecurity-2.0</feature>
           <feature>restConnector-1.0</feature>
       </featureManager>

       <!-- Pour accéder à ce serveur à partir d'un client éloigné,
            ajoutez un attribut host à l'élément suivant,
            par exemple, host="*" -->
       <httpEndpoint httpPort="9080" httpsPort="9443" id="defaultHttpEndpoint"/>

   ...
       <jspEngine prepareJSPs="0"/>
       <webContainer deferServletLoad="false"/>
   ...
   </server>
   ```

   Le fichier `server.xml` est décrit dans le WebSphere Application Server Center. Pour WebSphere Application Server version 8.5.5, reportez-vous à la rubrique Profil Liberty : Eléments de configuration dans le fichier server.xml.
3. Démarrez le serveur en mode débogage, à l'aide de l'une des méthodes suivantes :

- Ajoutez un argument JVM `-Dwas.debug.mode=true`, comme décrit dans la rubrique relative à la définition d'arguments JVM génériques dans le profil Liberty WebSphere Application Server V8.5.
- Suivez les instructions de démarrage et d'arrêt d'un serveur dans la rubrique WebSphere Application Server Network Deployment Knowledge Center. Pour WebSphere Application Server version 8.5.5, reportez-vous à la rubrique Démarrage et arrêt d'un serveur avec les outils de développement.

Résultats

Une fois que vous avez effectué ces étapes, importez vos applications Java du profil Liberty WebSphere Application Server en suivant les étapes de la rubrique «Importation d'applications Java à partir de serveurs d'applications Apache Tomcat et de profil Liberty WebSphere Application Server», à la page 44.

Ajout d'un espace de travail Eclipse ou de produit reposant sur Eclipse

Si vous disposez d'un espace de travail Eclipse ou Rational Application Developer for WebSphere Software (RAD) contenant des projets Java et/ou IBM MobileFirst Platform, vous pouvez l'importer dans AppScan Source for Analysis.

Avant de commencer

Avant d'ajouter l'espace de travail, assurez-vous d'avoir installé et mis à jour l'environnement de développement comme décrit dans la rubrique «Configuration de l'environnement de développement pour des projets Eclipse et Rational Application Developer for WebSphere Software (RAD)».

Procédure

1. Effectuez l'une des actions suivantes :
   - Sélectionnez **Fichier** > **Ajouter une application** > **Importer un espace de travail basé sur Eclipse existant** dans le menu de plan de travail principal.
   - Dans la vue Explorateur, cliquez sur la flèche vers le bas du bouton **Ajouter un menu d'application** et sélectionnez **Importer un espace de travail basé sur Eclipse existant** dans le menu.
   - Dans la vue Explorateur, cliquez avec le bouton droit de la souris sur **Toutes les applications**, puis sélectionnez **Ajouter une application** > **Importer un espace de travail basé sur Eclipse existant** dans le menu.
2. Sélectionnez le **Type d'espace de travail**.
3. Accédez à l'espace de travail, sélectionnez le répertoire et cliquez ensuite sur **OK** pour ajouter l'espace de travail.

Configuration de l'environnement de développement pour des projets Eclipse et Rational Application Developer for WebSphere Software (RAD)

Avant d'importer un projet Eclipse ou Rational Application Developer for WebSphere Software (RAD), vous devez configurer en conséquence l'environnement de développement. Bien qu'Eclipse constitue la base de chaque type de projet, AppScan Source distingue les différentes versions.

Pour en savoir plus sur les versions d'Eclipse et de Rational Application Developer for WebSphere Software (RAD) prises en charge par AppScan Source, voir http://www.ibm.com/support/docview.wss?uid=swg27027486.

Pour plus d'informations sur la configuration de votre environnement de développement, consultez les rubriques d'aide suivantes :

- «Mises à jour d'Eclipse ou d'Application Developer»
- «Importateurs d'espaces de travail Eclipse : Configuration des préférences Eclipse»

Mises à jour d'Eclipse ou d'Application Developer

Dans le cas d'environnements Eclipse ou Application Developer externes à AppScan Source, vous devez vérifier que les mises à jour logicielles appropriées ont bien été installées. Les instructions ci-après expliquent comment obtenir et installer ces mises à jour. La procédure peut varier selon les versions.

Avant de commencer

Important : AppScan Source for Development requiert un environnement JRE (Java Runtime Environment) de version 1.5 ou ultérieure. Si votre environnement pointe vers un JRE ne répondant pas à cette exigence, modifiez le fichier `eclipse.ini` dans le répertoire d'installation Eclipse afin qu'il pointe vers un JRE conforme. Pour des informations sur cette modification à apporter au fichier `eclipse.ini`, voir la section *Spécification de la machine virtuelle Java* de http://wiki.eclipse.org/Eclipse.ini.

Procédure

1. Depuis le menu **Aide** d'Eclipse, sélectionnez l'option d'installation d'un nouveau logiciel (l'intitulé du menu varie selon la version d'Eclipse que vous utilisez).
2. Sélectionnez l'option d'ajout d'un site de mise à jour local.
3. Lorsque vous êtes invité à indiquer l'emplacement du site, accédez au répertoire d'installation de AppScan Source.
4. Ajoutez ce site de mise à jour et suivez les instructions affichées jusqu'à l'invite de redémarrage d'Eclipse.
5. Le menu AppScan Source apparaît à l'issue de l'installation.

Importateurs d'espaces de travail Eclipse : Configuration des préférences Eclipse

L'installation de AppScan Source for Analysis fournit un importateur Eclipse par défaut. Cet importateur identifie l'emplacement d'Eclipse et du JRE. Si l'importateur Eclipse par défaut est incapable d'importer votre espace de travail, il peut s'avérer nécessaire de créer un nouvel importateur Eclipse.

Avant de commencer

Chaque configuration d'importateur représente une installation d'Eclipse ou de Rational Application Developer for WebSphere Software (RAD). Pour utiliser ces configurations pour importer des espaces de travail et des projets existants vers AppScan Source for Analysis, vous pouvez avoir besoin d'installer les plug-in AppScan Source for Development dans l'environnement Eclipse.

Avant d'ajouter un espace de travail RAD, vous devez créer une configuration pour le type d'espace de travail.

Procédure

1. Dans AppScan Source for Analysis, sélectionnez **Editer** > **Préférences** à partir du menu principal du plan de travail.
2. Sélectionnez **Importateurs d'espace de travail Eclipse**.
3. Cliquez sur **Créer une nouvelle configuration** et renseignez la boîte de dialogue Nouvelle configuration d'importation pour créer une nouvelle configuration :
   - **Produit** : Sélectionnez le produit approprié.

     Remarque : Si le produit utilisé pour créer l'espace de travail n'est pas disponible à la sélection, vérifiez que vous avez suivi les étapes de configuration décrites dans «Mises à jour d'Eclipse ou d'Application Developer», à la page 48 avant de tenter de créer l'importateur d'espace de travail.
   - **Nom** : Nom de l'importateur
   - **Emplacement** : Chemin du répertoire de base de l'installation Eclipse
   - **Emplacement du JRE** : Chemin du répertoire racine de l'environnement d'exécution Java (JRE). Utilisez un kit JDK fourni dans `<install_dir>\JDKS` (où `<rép_install>` représente l'emplacement de votre installation AppScan Source) ou un autre kit JDK de votre choix.
4. Cliquez sur **OK**.
5. Pour identifier l'importateur défini par défaut, sélectionnez-le et cliquez sur **Définir comme configuration par défaut celle sélectionnée**. Après cela, une icône s'affiche dans la colonne **Par défaut** de l'importateur.

Création d'un nouveau projet pour une application

Après avoir ajouté une application, vous devez lui ajouter des projets. Les types de projet pouvant être examinés sont notamment : Java/JSP, Xcode (projets iOS seulement) et JavaScript.

Pourquoi et quand exécuter cette tâche

Remarque : Vous ne pouvez pas créer un projet pour un projet Xcode. Les projets Xcode sont importés dans AppScan Source for Analysis en tant qu'applications ou ajoutés aux applications en tant que projets existants. Pour plus d'informations, voir «Ajout d'une application existante», à la page 42 ou «Ajout d'un projet existant», à la page 50.

Si vous utilisez `ant` pour compiler votre projet, utilisez Ounce/Ant pour créer un fichier de projet, puis l'ajouter. Consultez le manuel *IBM Rational AppScan Source Edition Utilities User Guide* pour plus d'informations sur Ounce/Ant.

Remarque : Le codage de fichier par défaut pour les projets AppScan Source est **ISO-8859-1**. Le codage de fichier par défaut peut être modifié sur la page de préférences générales.

Remarque : Lorsque des applications et des projets sont créés à l'aide de l'assistant Nouvelle application et de l'assistant Nouveau projet, leur nom de fichier est défini automatiquement en fonction du **nom** saisi dans l'assistant (par exemple, si un

projet est créé et **MyProject** est saisi dans la zone **Nom**, le nom de fichier du projet est `MyProject.ppf`). Les noms d'application et de projet peuvent être modifiés à l'aide de la vue Propriétés.

Procédure

1. Depuis la vue Explorateur, sélectionnez l'application à laquelle ajouter le projet (si vous n'avez pas encore ajouté d'application, reportez-vous à la rubrique «Configuration d'applications», à la page 36).
2. Effectuez l'une des actions suivantes pour ouvrir l'assistant Nouveau projet :
   a. Sélectionnez **Fichier** > **Ajouter un projet** > **Nouveau projet** dans le menu principal du plan de travail.
   b. Cliquez avec le bouton droit de la souris sur l'application concernée et sélectionnez **Ajouter un projet** > **Nouveau projet** dans le menu contextuel.
3. Exécutez l'assistant Nouveau projet.

Ajout d'un projet existant

Vous pouvez ajouter des projets AppScan Source (fichiers `.ppf`) créés précédemment avec AppScan Source for Analysis aux applications AppScan Source. Vous pouvez aussi ajouter des fichiers de projet Eclipse (`.epf`), des projets créés par les outils d'intégration de génération pris en charge (par exemple Ounce/Maven ou Ounce/Ant), ou des fichiers de projet créés avec Xcode (où vous ajoutez le répertoire `.xcodeproj`).

Ce tableau répertorie les types de fichiers de projet que vous pouvez ouvrir et examiner à l'aide de AppScan Source for Analysis :

Tableau 5. Types de fichier de projet à ouvrir

Type de fichier de projet	Extension de fichier
Répertoire Xcode	`.xcodeproj` **Remarque :** Vous pouvez aussi ouvrir ou importer des fichiers `.pbxproj` en tant que projets AppScan Source.
Fichier de projet AppScan Source	`.ppf`
Fichier de projet Eclipse	`.epf`

Pour déterminer comment ajouter un projet existant, consultez les rubriques suivantes :

- «Ajout d'un projet existant à l'aide d'actions de l'interface utilisateur», à la page 51
- «Ajout d'un projet existant à l'aide d'une opération de glisser-déposer», à la page 51

Important : Si vous travaillez avec un projet AppScan Source comportant des dépendances dans un environnement de développement (par exemple un projet IBM MobileFirst Platform), veillez à créer le projet dans l'environnement de développement avant de l'importer. Après avoir importé le projet, si vous modifiez des fichiers qu'il contient, pensez à le régénérer dans l'environnement de développement avant l'analyse dans AppScan Source (si vous omettez cette étape, les modifications apportées aux fichiers ne seront pas prises en compte par AppScan Source).

Remarque : Vous pouvez aussi ouvrir ou importer des fichiers `.pbxproj` en tant que projets AppScan Source.

Remarque : Vous pouvez également ajouter des fichiers `WAR` et `EAR` par glisser-déposer dans la vue Explorateur. Cependant, ceux-ci sont ajoutés en tant qu'applications et non en tant que projets. Pour plus d'informations, voir «Ajout d'une application existante à l'aide d'une opération de glisser-déposer», à la page 42.

Ajout d'un projet existant à l'aide d'actions de l'interface utilisateur

Procédure

1. Depuis la vue Explorateur, sélectionnez l'application à laquelle ajouter le projet (si vous n'avez pas encore ajouté d'application, reportez-vous à la rubrique «Configuration d'applications», à la page 36).
2. Effectuez l'une des actions suivantes :
   - Sélectionnez **Fichier** > **Ajouter un projet** > **Projet existant** dans le menu principal du plan de travail.
   - Cliquez avec le bouton droit de la souris sur l'application concernée et sélectionnez **Ajouter un projet** > **Projet existant** dans le menu contextuel.
3. Accédez au fichier de projet à ajouter à l'application.

   Important : Si vous travaillez avec un projet AppScan Source comportant des dépendances dans un environnement de développement (par exemple un projet IBM MobileFirst Platform), veillez à créer le projet dans l'environnement de développement avant de l'importer. Après avoir importé le projet, si vous modifiez des fichiers qu'il contient, pensez à le régénérer dans l'environnement de développement avant l'analyse dans AppScan Source (si vous omettez cette étape, les modifications apportées aux fichiers ne seront pas prises en compte par AppScan Source).

Ajout d'un projet existant à l'aide d'une opération de glisser-déposer

Procédure

1. Depuis votre poste de travail, localisez le projet (`.ppf`) ou le répertoire `.xcodeproj` que vous souhaitez ajouter à l'examen.

   Remarque : Vous ne pouvez pas effectuer un glissement-déplacement des fichiers créés avec l'un des outils d'intégration de génération pris en charge (par exemple, Ounce/Maven ou Ounce/Ant).

   Remarque : Vous pouvez aussi ouvrir ou importer des fichiers `.pbxproj` en tant que projets AppScan Source.
2. Sélectionnez le projet, puis faites-le glisser dans la vue Explorateur de AppScan Source for Analysis.
3. Effectuez l'une des étapes suivantes :
   a. Déposez votre sélection dans une application existante.
   b. Déposez votre sélection sur ou sous le noeud **Toutes les applications**. Etant donné que les projets doivent résider dans une application et que cette action n'ajoute pas le projet dans une application existante, vous serez invité par l'assistant Nouvelle application à créer une application pour ce projet. Entrez un **Nom** pour l'application, puis accédez au **Répertoire de travail**

dans lequel sauvegarder l'application. Cliquez sur **Terminer** pour créer l'application (le projet ajouté sera contenu dans cette dernière dans la vue Explorateur).

Important : Si vous travaillez avec un projet AppScan Source comportant des dépendances dans un environnement de développement (par exemple un projet IBM MobileFirst Platform), veillez à créer le projet dans l'environnement de développement avant de l'importer. Après avoir importé le projet, si vous modifiez des fichiers qu'il contient, pensez à le régénérer dans l'environnement de développement avant l'analyse dans AppScan Source (si vous omettez cette étape, les modifications apportées aux fichiers ne seront pas prises en compte par AppScan Source).

Ajout de plusieurs projets

Pour ajouter plusieurs projets à une application, vous pouvez les faire glisser et les déposer dans la vue Explorateur ou bien accéder à un répertoire de projets et en importer certains, ou tous, dans l'application en cours.

Pour déterminer comment ajouter plusieurs projets, consultez les rubriques suivantes :

- «Ajout de plusieurs projets à l'aide d'actions de l'interface utilisateur»
- «Ajout de plusieurs projets à l'aide d'une opération de glisser-déposer», à la page 53

Important : Si vous travaillez avec un projet AppScan Source comportant des dépendances dans un environnement de développement (par exemple un projet IBM MobileFirst Platform), veillez à créer le projet dans l'environnement de développement avant de l'importer. Après avoir importé le projet, si vous modifiez des fichiers qu'il contient, pensez à le régénérer dans l'environnement de développement avant l'analyse dans AppScan Source (si vous omettez cette étape, les modifications apportées aux fichiers ne seront pas prises en compte par AppScan Source).

Ajout de plusieurs projets à l'aide d'actions de l'interface utilisateur

Il est possible d'ajouter plusieurs projets à un formulaire d'application depuis un répertoire (sous-répertoires inclus) ou un espace de travail Eclipse.

Procédure

1. Depuis la vue Explorateur, sélectionnez l'application à laquelle ajouter les projets (si vous n'avez pas encore ajouté d'application, reportez-vous à la rubrique «Configuration d'applications», à la page 36).
2. Effectuez l'une des actions suivantes :
   - Sélectionnez **Fichier** > **Ajouter un projet** > **Projets multiples** à partir du menu principal du plan de travail.
   - Cliquez avec le bouton droit de la souris sur l'application concernée et sélectionnez **Ajouter un projet** > **Projets multiples** dans le menu contextuel.
3. Dans la boîte de dialogue Ajouter plusieurs projets, exécutez l'une des actions ci-dessous :
   - Sélectionnez **Importer depuis le répertoire** et accédez ensuite au répertoire racine qui contient les projets que vous voulez ajouter. Cochez la case **Opération récursive dans les sous-répertoires** pour effectuer une recherche dans les sous-répertoires.

- Sélectionnez **Importer depuis un espace de travail basé sur Eclipse**. Sélectionnez **Type d'espace de travail** et accédez ensuite à l'espace de travail. Sélectionnez le répertoire d'espace de travail et cliquez ensuite sur **OK**.

4. Effectuez l'une des actions suivantes :
   - Cliquez sur **Terminer** pour ajouter les projets à l'application.
   - Cliquez sur **Suivant** pour afficher les résultats de la recherche et sélectionner les projets à ajouter. Cliquez ensuite sur **Terminer**.

   Important : Si vous travaillez avec un projet AppScan Source comportant des dépendances dans un environnement de développement (par exemple un projet IBM MobileFirst Platform), veillez à créer le projet dans l'environnement de développement avant de l'importer. Après avoir importé le projet, si vous modifiez des fichiers qu'il contient, pensez à le régénérer dans l'environnement de développement avant l'analyse dans AppScan Source (si vous omettez cette étape, les modifications apportées aux fichiers ne seront pas prises en compte par AppScan Source).

Ajout de plusieurs projets à l'aide d'une opération de glisser-déposer

Procédure

1. Depuis votre poste de travail, localisez les projets (`.ppf`) ou les répertoires `.xcodeproj` que vous souhaitez ajouter à l'examen.

   Remarque : Vous ne pouvez pas effectuer un glissement-déplacement des fichiers créés avec l'un des outils d'intégration de génération pris en charge (par exemple, Ounce/Maven ou Ounce/Ant).

   Remarque : Vous pouvez aussi ouvrir ou importer des fichiers `.pbxproj` en tant que projets AppScan Source.
2. Sélectionnez les projets à ajouter et faites-les glisser dans la vue Explorateur.
3. Déposez votre sélection dans une application existante.

   Remarque : Vous pouvez également déposer votre sélection sur ou au dessous du noeud **Toutes les applications**, bien que ceci ne soit pas recommandé. Il est conseillé, par contre, que plusieurs projets soient déposés dans une application existante, ou individuellement, si de nouvelles applications sont requises.

   Etant donné que les projets doivent résider dans une application et que le placement de projets sur ou au dessous du noeud **Toutes les applications** ne les ajoute pas à une application existante, vous serez invité par l'assistant Nouvelle application à créer une nouvelle application pour chaque projet que vous ajoutez à la vue.

   Pour ajouter plusieurs projets à une nouvelle application n'existant pas encore, créez d'abord l'application avant de faire glisser-déposer les projets sélectionnés sur celle-ci.

   Important : Si vous travaillez avec un projet AppScan Source comportant des dépendances dans un environnement de développement (par exemple un projet IBM MobileFirst Platform), veillez à créer le projet dans l'environnement de développement avant de l'importer. Après avoir importé le projet, si vous modifiez des fichiers qu'il contient, pensez à le régénérer dans l'environnement de développement avant l'analyse dans AppScan Source (si vous omettez cette étape, les modifications apportées aux fichiers ne seront pas prises en compte par AppScan Source).

Ajout d'un nouveau projet Arxan

L'assistant Configuration de projet vous aide à créer manuellement un projet Arxan et à l'ajouter à une application.

Pourquoi et quand exécuter cette tâche

Les étapes décrites dans cette rubrique vous indiquent comment renseigner toutes les pages de l'assistant Nouveau projet (ou de l'assistant Nouvelle application, si vous créez le projet dans celui-ci). Les paramètres définis dans l'assistant peuvent être modifiés après la création du projet dans la vue Propriétés d'un projet sélectionné.

Procédure

1. Depuis la vue Explorateur, sélectionnez l'application à laquelle ajouter le projet (si vous n'avez pas encore ajouté d'application, reportez-vous à la rubrique «Configuration d'applications», à la page 36).
2. Effectuez l'une des actions suivantes pour ouvrir l'assistant Nouveau projet :
   a. Sélectionnez **Fichier** > **Ajouter un projet** > **Nouveau projet** dans le menu principal du plan de travail.
   b. Cliquez avec le bouton droit de la souris sur l'application concernée et sélectionnez **Ajouter un projet** > **Nouveau projet** dans le menu contextuel.
3. Depuis la page Sélectionner un type de projet de l'assistant, sélectionnez comme type de projet **Arxan Android** ou **Arxan iOS**, puis cliquez sur **Suivant** pour accéder à la page suivante de l'assistant.
4. Depuis la page de l'assistant Sources de projet :
   a. Identifiez les sources de projet. Ces dernières sont constituées par les répertoires dans lesquels sont situés les fichiers de projet et des fichiers individuels supplémentaires à inclure au projet.

      Attribuez un nom au projet et spécifiez le répertoire de travail. Le **répertoire de travail** désigne l'emplacement du fichier de projet AppScan Source (`.ppf`). Il constitue également la base de tous les chemins relatifs.
   b. Cliquez sur **Ajouter une racine source** afin de spécifier une racine de code source et les répertoires ou fichiers à inclure ou à exclure de l'examen. Après l'ajout de la racine source, vous pouvez en exclure certains répertoires ou fichiers. Pour ce faire, sélectionnez le répertoire ou le fichier (ou plusieurs de ces éléments) dans la racine source, cliquez avec le bouton droit de la souris sur votre sélection, puis sélectionnez **Exclure** dans le menu. Si vous incluez ou excluez des fichiers, l'icône à gauche du nom de fichier est modifiée en conséquence.
5. Cliquez sur **Terminer**.

Ajout d'un nouveau projet Java ou JavaServer Page (JSP)

Lorsque vous ajoutez un nouveau projet Java à l'application, vous spécifiez le nom du projet, accédez au répertoire de travail, puis spécifiez les racines source et les dépendances du projet.

Pourquoi et quand exécuter cette tâche

Les étapes décrites dans cette rubrique vous indiquent comment renseigner toutes les pages de l'assistant Nouveau projet (ou de l'assistant Nouvelle application, si vous créez le projet dans celui-ci). Toutefois, certaines pages de l'assistant sont facultatives (les paramètres requis sont définis une fois le bouton **Terminé** activé).

Les paramètres définis dans l'assistant peuvent être modifiés après la création du projet dans la vue Propriétés d'un projet sélectionné. Si vous terminez l'exécution de l'assistant Nouveau projet sans remplir les pages facultatives, vous pourrez modifier ultérieurement les paramètres contenus dans ces pages dans la vue Propriétés.

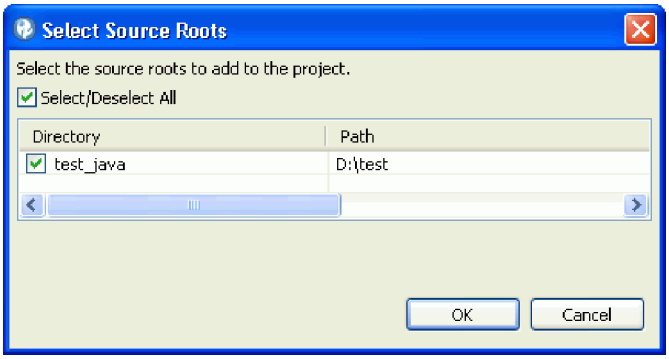
Procédure

1. Depuis la vue Explorateur, sélectionnez l'application à laquelle ajouter le projet (si vous n'avez pas encore ajouté d'application, reportez-vous à la rubrique «Configuration d'applications», à la page 36).
2. Effectuez l'une des actions suivantes pour ouvrir l'assistant Nouveau projet :
   a. Sélectionnez **Fichier** > **Ajouter un projet** > **Nouveau projet** dans le menu principal du plan de travail.
   b. Cliquez avec le bouton droit de la souris sur l'application concernée et sélectionnez **Ajouter un projet** > **Nouveau projet** dans le menu contextuel.
3. Depuis la page Sélectionner un type de projet de l'assistant, sélectionnez comme type de projet **Java/JSP**, puis cliquez sur **Suivant** pour accéder à la page suivante de l'assistant.
4. Depuis la page de l'assistant Sources de projet :
   a. Identifiez les sources de projet qui sont constituées par les répertoires dans lesquels sont situés les fichiers de projet et les fichiers individuels supplémentaires à inclure dans le projet.

      Attribuez un nom au projet et spécifiez le répertoire de travail. Le **répertoire de travail** désigne l'emplacement du fichier de projet AppScan Source (`.ppf`) et constitue la base de tous les chemins relatifs à celui-ci.
   b. Ajoutez manuellement les racines source ou autorisez AppScan Source for Analysis à identifier automatiquement les racines source valides.

      Important :

      - Pour analyser les fichiers de classe Java, ceux-ci doivent avoir été compilés avec `javac` en utilisant l'option `-g`. L'analyse AppScan Source repose sur les informations de débogage générées par cette option.
      - Si votre projet contient des fichiers source Java incluant des caractères de langue nationale et que vous exécutez un environnement local différent de l'environnement local natif (par exemple, UTF-8), l'examen échouera avec des erreurs et/ou des avertissements sur la console.
      - Pour détecter automatiquement les racines source, procédez comme suit :
        1) Cliquez sur **Rechercher des racines source** et accédez au répertoire racine du code source.
        2) Dans la liste de toutes les racines source détectées, sélectionnez celles à ajouter au projet.

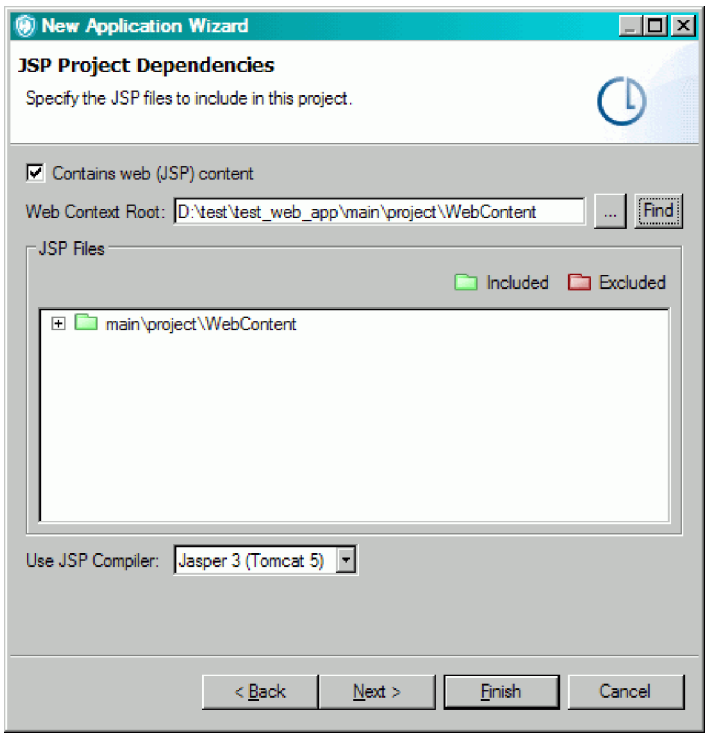


3) Cliquez sur **OK**. Les sources à inclure dans l'analyse sont affichées dans la boîte de dialogue **Sources de projet**.

- Pour détecter manuellement les racines source, procédez comme suit :
  1) Cliquez sur **Ajouter une racine source**.
  2) Sélectionnez le répertoire racine du code source ou le fichier.
  3) Cliquez sur **OK**. Après l'ajout de la racine source, vous pouvez en exclure certains répertoires ou fichiers. Pour ce faire, sélectionnez le répertoire ou le fichier (pu plusieurs de ces éléments), effectuez un clic avec le bouton droit de la souris sur votre sélection, puis sélectionnez **Exclure** dans le menu. Si vous incluez ou excluez des fichiers, l'icône à gauche du nom de fichier est modifiée en conséquence.

Cliquez sur **Terminer** pour ajouter le projet sans définir de dépendances de projet ou sur **Suivant** pour identifier celles-ci.

5. Depuis la page Dépendances de projet JSP :
   a. Identifiez les dépendances de projet JSP (JavaServer Page) : Pour les projets Java contenant des pages JavaServer Pages, identifiez les dépendances de projet JSP. Cochez la case **Contient un contenu Web (JSP)** si le projet est une application Web comportant des pages JavaServer Pages.



b. Sélectionnez manuellement la **Racine de contexte Web** ou cliquez sur **Rechercher** pour la localiser. La **Racine de contexte Web** est un fichier `WAR` ou un répertoire hébergeant le répertoire `WEB-INF`. La racine de contexte Web doit être la racine d'une application Web valide.

c. Sélectionnez le **Compilateur JSP** pour le projet. Prêt à l'emploi, Tomcat 7 est le compilateur JSP sélectionné par défaut (il est possible d'en changer sur la page de préférences Java et JSP). Pour en savoir plus sur les compilateurs pris en charge par AppScan Source, voir http://www.ibm.com/support/docview.wss?uid=swg27027486.

   Les versions d'Apache Tomcat versions 7 et 8 sont incluses dans l'installation d'AppScan Source. Si les pages de préférences **Tomcat 7** et **Tomcat 8** ne sont pas configurées, AppScan Source compile les fichiers JSP à l'aide du compilateur JSP Tomcat fourni et indiqué comme valeur par défaut. Si vous souhaitez employer un compilateur Tomcat externe pris en charge, utilisez les pages de préférences Tomcat pour pointer sur votre installation Tomcat locale.

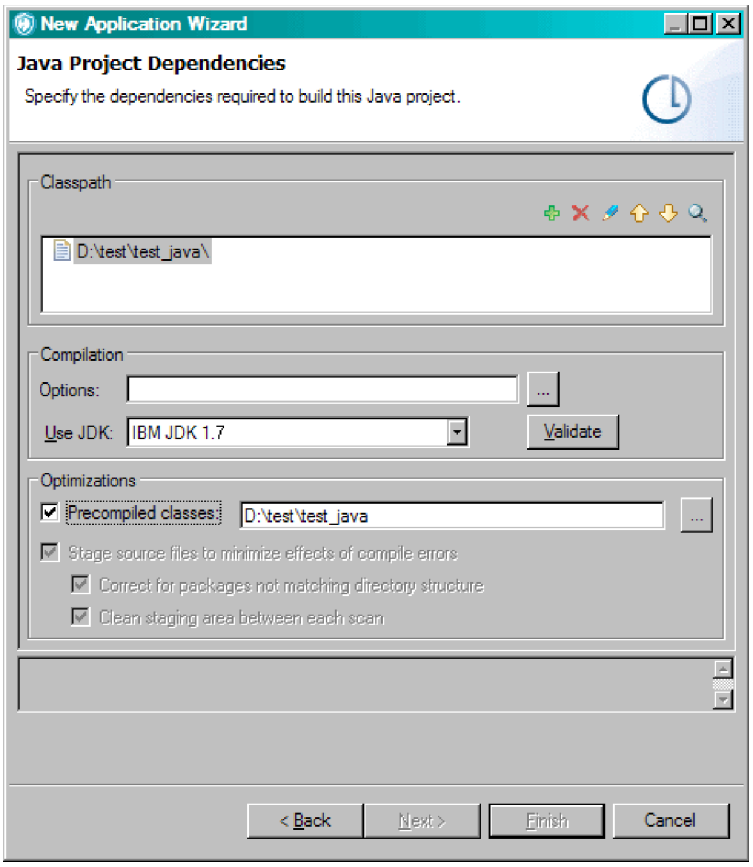
   Si vous utilisez Oracle WebLogic Server ou WebSphere Application Server, vous devez configurer la page de préférences correspondante, le but étant de désigner votre installation locale du serveur d'applications afin qu'elle puisse être utilisée pour la compilation du code JSP durant l'analyse. Si vous n'avez pas encore terminé cette configuration, un message vous demandera de la faire lorsque vous sélectionnerez le compilateur JSP. Si vous répondez **Oui** au message, la page de préférences appropriée s'affiche. Si vous répondez **Non**, un lien d'avertissement s'affiche à côté de la sélection du compilateur JSP (ce lien permet d'ouvrir la page de préférences).

Cliquez sur **Terminer** pour ajouter le projet avec les dépendances de projet JSP ou sur **Suivant** pour identifier les dépendances de projet Java.

6. Dans la page Dépendances de projet Java, identifiez les dépendances requises pour la construction de ce projet Java :

a. Ajoutez manuellement le fichiers JAR ou cliquez sur **Rechercher** afin que AppScan Source for Analysis recherche lui-même les répertoires contenant les fichiers JAR et les fichiers de classe dépendants.

La liste **Chemin de classes** affiche le chemin d'accès relatif au projet. Le chemin de classes doit spécifier les fichiers JAR requis et les répertoires contenant les fichiers de classe requis par le projet.



- **Ajouter**, **Supprimer**, **Déplacer vers le haut** et **Déplacer vers le bas** : Ajoutez ou supprimez des fichiers au chemin de classes, ou modifiez leur ordre en les déplaçant vers le haut ou vers leur bas.
- **Rechercher** : Recherchez des fichiers JAR et des entrées de chemin de classe basés sur les fichiers source du projet.

Important : Si le projet Java comporte des pages JavaServer Pages, vous devez ajouter des dépendances de projet JSP.

- Pour identifier manuellement les dépendances de projet, procédez comme suit :
  1) Cliquez sur **Ajouter** dans la barre d'outils de la section Chemin d'accès aux classes et sélectionnez ensuite les fichiers JAR et les répertoires de fichiers de classe requis pour compiler le projet Java.
  2) Cliquez sur **OK**. Les fichiers JAR et les répertoires apparaissent dans le chemin de classes. Modifiez leur ordre en cas de besoin.
- Pour identifier automatiquement les dépendances, procédez comme suit :
  1) Cliquez sur **Rechercher** dans la barre d'outils de la section Chemin d'accès aux classes.
  2) Spécifiez les répertoires dans lesquels rechercher les fichiers JAR et les fichiers de classe nécessaires pour compiler le projet Java.

3) Cochez la case **Rechercher à l'intérieur des fichiers source et JAR** si vous souhaitez que AppScan Source for Analysis recherche les dépendances de projet requises en fonction des sources et du chemin de recherche indiqué.
4) Cliquez sur **Suivant** pour rechercher les dépendances de projet et identifier les conflits.

- Pour résoudre les conflits, procédez comme suit :
  1) Si des conflits existent, sélectionnez dans la boîte de dialogue Résolution de conflits l'entrée à résoudre et cliquez sur **Résoudre** (ou cliquez sur **Suivant** pour résoudre automatiquement les conflits). Un conflit est présent lorsque AppScan Source for Analysis détecte plusieurs fichiers `JAR` ou classes faisant l'objet de la dépendance dans un répertoire.

     Une icône rouge apparaît à la gauche des conflits non résolus. Une fois les conflits résolus, l'icône rouge passe au vert indiquant que l'élément concerné est **résolu**. Vous pouvez également **supprimer** un conflit.
  2) Après avoir résolu ou supprimé un conflit, vous pouvez le cas échéant vérifier, modifie l'ordre ou supprimer les entrées concernées du chemin de classes. Prenez note de la liste des importations introuvables. Toutes les importations non résolues génèrent des erreurs de compilation lors de l'examen par AppScan Source for Analysis.

b. **Options** : Spécifiez les paramètres de compilation supplémentaires du projet.

   Les options de compilation sont celles qui sont transmises au compilateur pour permettre la compilation des fichiers. Par exemple, `-source 1.5` indique le niveau de la source du projet.

c. **Utiliser le kit JDK** : Indiquez le kit JDK (Java Development Kit) à utiliser lors de l'examen de ce code. **IBM JDK 1.8** est utilisé par défaut, mais AppScan Source propose également **IBM JDK 1.7** en sélection. Pour définir d'autres kits JDK ou définir un autre kit JDK par défaut, utilisez les **Préférences Java/JSP**.

   Remarque : Prêt à l'emploi, le compilateur par défaut des projets JSP est Tomcat 7, qui requiert Java version 1.6 ou version ultérieure. Si **Tomcat 7** est conservé par défaut et que vous sélectionnez un JDK plus ancien, des erreurs de compilation seront générées pendant les examens.

d. L'action **Valider** garantit que les dépendances du projet soient correctement configurées. Elle vérifie l'absence dans les projets Java de conflits de configuration entre les sources et le chemin de classes et vérifie également l'absence d'erreurs de compilation. Un conflit existe si une classe du chemin de classes est dupliquée dans la racine source.

   Si un conflit existe, la zone du texte de validation indique le fichier `JAR` ou l'emplacement où la classe est définie sur le chemin de classes et si le doublon existe dans les sources. Supprimez le conflit du chemin de classes et exécutez à nouveau la vérification.

   Après la vérification de l'absence de conflits, l'option **Valider** détermine si le projet peut être compilé et rend compte des erreurs de compilation éventuelles.

e. **Classes précompilées** : Cette zone vous permet d'utiliser des fichiers de classe Java ou JSP précompilés au lieu de la compilation pendant un examen.

f. **Déployer pour pré-traitement les fichiers source pour minimiser les effets d'erreur de compilation** : Décochez cette case si la compilation de votre code source s'effectue correctement et si celui-ci est organisé comme il se doit dans les répertoires correspondant aux packages.

g. **Corriger pour les packages non conformes à la structure de répertoire** : Sélectionnez cette option si les packages ne correspondent pas à la structure des répertoires.

h. **Nettoyer la zone de préparation entre chaque examen** : Option d'optimisation.

7. Cliquez sur **Terminer**.

Résultats

Conseil : Si vous examinez Java et qu'il manque des dépendances dans votre projet Java, AppScan Source crée des traces en synthétisant les éléments que les dépendances auraient fournis. Cette synthèse ne reflète peut-être pas exactement les informations qui figurent dans les fichiers `.jar`. Pour limiter cette synthèse et par conséquent améliorer l'exactitude des constatations, vous pouvez spécifier les dépendances manquantes de la façon suivante :

1. Après l'examen, ouvrez `<data_dir>\logs\scanner_exceptions.log` (où `<rép_données>` est l'emplacement de vos données de programme AppScan Source, comme décrit dans «Installation et emplacements des fichiers de données utilisateur», à la page 292) pour vérifier si AppScan Source a signalé des dépendances manquantes.
2. Modifiez les propriétés du projet afin d'inclure les dépendances. Pour ce faire, suivez les instructions figurant dans la rubrique «Modification des propriétés d'une application et d'un projet», à la page 64, puis spécifiez et sauvegardez les dépendances dans l'onglet **Dépendances de projet JSP** ou **Dépendances de projet**.
3. Examinez à nouveau le projet.

Remarque : Par défaut, AppScan Source examine les fichiers Java et le bytecode Java en recherchant les dépendances manquantes ou les erreurs de compilation. Vous pouvez modifier ces paramètres de la façon suivante :

1. Ouvrez `<data_dir>\config\scan.ozsettings` dans un éditeur de texte.
2. Pour modifier le paramètre d'erreur de compilation, recherchez `compile_java_sources_with_errors` dans le fichier. Ce paramètre est similaire à ce qui suit :

```
<Setting
  name="compile_java_sources_with_errors"
  value="true"
  default_value="true"
  type="bool"
  hidden="true"
  display_name="compile_java_sources_with_errors"
  description="Attempt to scan java code with compilation errors."
/>
```

3. Pour modifier le paramètre de dépendance manquante, recherchez `scan_java_bytecode_without_dependencies` dans le fichier. Ce paramètre est similaire à ce qui suit :

```
<Setting
  name="scan_java_bytecode_without_dependencies"
  value="true"
  default_value="true"
  type="bool"
  hidden="true"
```

```
  display_name="scan_java_bytecode_without_dependencies"
  description="Scans Java bytecode even when some of
    the dependencies are missing by artificially
    synthesizing the unresolved symbols."
/>
```

4. Dans le paramètre, modifiez l'attribut `value`. Si l'attribut est défini sur la valeur `true`, ce paramètre sera activé. Si le paramètre d'erreur de compilation est défini sur la valeur `false`, AppScan Source ignorera le code Java présentant des erreurs de compilation au cours des examens. Si le paramètre de dépendance manquante est défini sur la valeur `false`, AppScan Source n'examinera pas le bytecode Java si des dépendances sont manquantes.
5. Après avoir modifié ce paramètre, sauvegardez le fichier, puis démarrez ou redémarrez AppScan Source.

Ajout de contenu à un projet JSP

Les projets JSP (JavaServer Page) incluent des applications Web construites à partir de pages JavaServer.

Pourquoi et quand exécuter cette tâche

Pour que l'examen de projets JSP aboutisse, les pages JSP (JavaServer Pages) doivent résider dans une structure d'application Web valide. Cette section décrit la structure de fichiers requise sous la racine de contexte Web pour la réussite de l'examen. Vous devez avoir une bonne connaissance de la structure d'application Web avant de configurer vos projets JSP.

Une application Web déployée sur un serveur d'application Web, tel que Tomcat, requiert une structure de répertoires standard. L'application déployée peut être composée d'un ensemble de fichiers organisés dans une structure de répertoire ou d'un fichier `WAR`. Dans le cas d'un fichier `WAR`, la structure du répertoire est contenue dans la fichier ZIP, la `racine de contexte Web` constituant la racine de la structure des répertoires.

Au-dessous d'une racine de contexte Web figurent les répertoires standard suivants :

Tableau 6. Répertoires de la racine de contexte Web

`<web-context-root>\`	
`WEB-INF\`	
`classes\`	Fichiers de classe Java organisés en répertoires (packages)
`lib\`	Fichiers Jar ajoutés au chemin de classes
`web.xml`	`web.xml` décrit les ressources disponible à l'application

D'autres répertoires contiennent des fichiers requis pouvant également exister. Par exemple, vous rencontrez souvent un répertoire pour le contenu (fichiers JSP et HTML) et pour les bibliothèques de balises (tag) :

Tableau 7. Autres répertoires

`<racine-contexte-Web>\`	
`jsp\`	Contient les pages JSP (JavaServer Pages) de l'application

Tableau 7. Autres répertoires (suite)

`WEB-INF\`	
`tld\`	Contient les bibliothèques de balises utilisées dans l'application

Outre ces répertoires d'application Web standard, un serveur d'application Web peut comporter des répertoires spéciaux dans lesquels il s'attend à trouver les fichiers de classe et les fichiers `JAR` partagés par toutes les applications Web déployées. Par exemple, Tomcat 7 place ces fichiers `JAR` dans les répertoires `common\lib` ou `common\endorsed`. L'emplacement de ces répertoires non standard est spécifique à chaque serveur d'application.

Important : Avant d'examiner des pages JSP (JavaServer Pages), vérifiez que tous les fichiers requis existent sous la racine de contenu Web. AppScan Source for Analysis examine uniquement les pages JavaServer Pages situées sous la racine de contexte Web.

Procédure

1. En cas de besoin, copiez les fichiers vers l'emplacement approprié sous la racine de contexte Web.
2. Spécifiez comme racine de contexte Web le répertoire ou un fichier `WAR` contenant toutes les pages JSP (JavaServer Pages).
3. Assurez-vous que le chemin de classes inclut le fichier `JAR` ou les répertoires de fichiers de classe.
4. Configurez les propriétés du projet.

Résultats

AppScan Source for Analysis ajoute le répertoire `WEB-INF\classes` et tous les fichiers `JAR` sous `WEB-INF\lib` au chemin de classes, et ce uniquement pour JSP. Vous pouvez ajouter des éléments non inclus dans le chemin `Web-INF` mais nécessaires pour la compilation des pages JSP. Ces fichiers `JAR` sont similaires au fichier `weblogic.jar`, ou au fichier `JAR` d'un autre éditeur, placé sous le répertoire commun d'un serveur d'application.

Les sources JSP sont les pages JavaServer Pages sous la racine de contexte Web que vous désirez examiner. Les fichiers source sont relatifs à la racine de contexte Web. Vous êtes limité à l'ensemble de fichiers sous la racine de contexte Web lorsque vous spécifiez les sources JSP.

Les sources de projet JSP consistent des répertoires dans lesquels sont situés les fichiers de projet et des fichiers individuels supplémentaires à inclure au projet.

- Spécifiez le sous-ensemble de pages JSP (JavaServer Pages) sous la racine de contexte Web. Si vous ne le faites pas, tous les fichiers seront analysés.
- Si les pages JSP dépendent de code Java, vous devez spécifier ces sources.
- Les fichiers JSP incluent des fichiers `jsp` et `jspx`.

Ajout d'un nouveau projet JavaScript

L'assistant Configuration de projet vous aide à créer manuellement un projet JavaScript et à l'ajouter à une application.

Pourquoi et quand exécuter cette tâche

Les étapes décrites dans cette rubrique vous indiquent comment renseigner toutes les pages de l'assistant Nouveau projet (ou de l'assistant Nouvelle application, si vous créez le projet dans celui-ci). Les paramètres définis dans l'assistant peuvent être modifiés après la création du projet dans la vue Propriétés d'un projet sélectionné.

Procédure

1. Depuis la vue Explorateur, sélectionnez l'application à laquelle ajouter le projet (si vous n'avez pas encore ajouté d'application, reportez-vous à la rubrique «Configuration d'applications», à la page 36).
2. Effectuez l'une des actions suivantes pour ouvrir l'assistant Nouveau projet :
   a. Sélectionnez **Fichier** > **Ajouter un projet** > **Nouveau projet** dans le menu principal du plan de travail.
   b. Cliquez avec le bouton droit de la souris sur l'application concernée et sélectionnez **Ajouter un projet** > **Nouveau projet** dans le menu contextuel.
3. Dans la page Sélectionner un type de projet de l'assistant, sélectionnez **JavaScript** comme type de projet, puis cliquez sur **Suivant** pour accéder à la page suivante de l'assistant.
4. Depuis la page de l'assistant Sources de projet :
   a. Identifiez les sources de projet. Ces dernières sont constituées par les répertoires dans lesquels sont situés les fichiers de projet et des fichiers individuels supplémentaires à inclure au projet.

      Attribuez un nom au projet et spécifiez le répertoire de travail. Le **répertoire de travail** désigne l'emplacement du fichier de projet AppScan Source (`.ppf`). Il constitue également la base de tous les chemins relatifs.
   b. Cliquez sur **Ajouter une racine source** afin de spécifier une racine de code source et les répertoires ou fichiers à inclure ou à exclure de l'examen. Après l'ajout de la racine source, vous pouvez en exclure certains répertoires ou fichiers. Pour ce faire, sélectionnez le répertoire ou le fichier (ou plusieurs de ces éléments) dans la racine source, cliquez avec le bouton droit de la souris sur votre sélection, puis sélectionnez **Exclure** dans le menu. Si vous incluez ou excluez des fichiers, l'icône à gauche du nom de fichier est modifiée en conséquence.
5. Cliquez sur **Terminer**.

Copie de projets

AppScan Source for Analysis vous permet de copier tous les types de projet excepté les projets .NET. Les modifications apportées au projet n'affectent pas sa copie ; après la copie du projet, aucune connexion n'existe entre l'original et sa copie. Lorsque vous copiez un projet importé, vous créez un fichier de projet AppScan Source (`.ppf`) avec toutes les informations de configuration.

Procédure

1. Depuis la vue Explorateur, cliquez avec le bouton droit de la souris sur le projet que vous désirez copier, puis sélectionnez **Copier le projet** dans le menu.
2. Dans la boîte de dialogue Copie de projet :
   a. Nommez le nouveau projet.

b. Identifiez l'application de destination du projet dupliqué (il doit s'agir d'une application AppScan Source créée manuellement ou par le biais d'Application Discovery Assistant).
c. Identifiez un répertoire de destination (répertoire de travail du nouveau projet).

Modification des propriétés d'une application et d'un projet

Lorsque vous sélectionnez une application ou un projet dans la vue Explorateur, ses propriétés actuelles figurent dans la vue Propriétés depuis laquelle vous pouvez leur apporter des modifications.

Pourquoi et quand exécuter cette tâche

La «Vue Propriétés : application sélectionnée», à la page 219 et la «Vue Propriétés : projet sélectionné», à la page 220 fournissent des informations détaillées sur les paramètres pouvant être modifiés dans la vue Propriétés lorsqu'une application ou un projet est sélectionné.

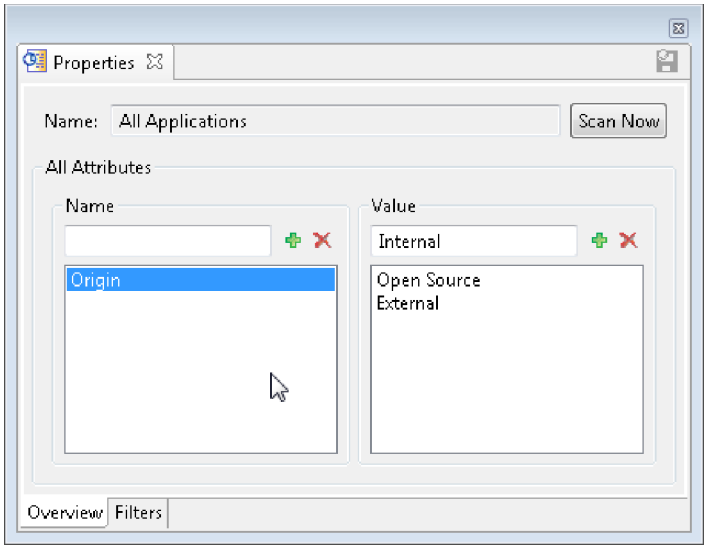
Procédure

1. Ouvrez la vue Propriétés de l'application ou du projet en procédant de l'une des manières suivantes :
   a. Sélectionnez l'application ou le projet dans la vue Explorateur, puis ouvrez la vue Propriétés afin d'y afficher ses propriétés.
   b. Cliquez avec le bouton droit de la souris sur l'application ou le projet dans la vue Explorateur et sélectionnez **Propriétés**.
2. Examinez ses propriétés dans la vue Propriétés.
3. Apportez les modifications voulues sur les pages d'onglet appropriés. Les pages de propriétés disponibles sont fonction du langage.
4. Cliquez sur **Sauvegarder**.

Attributs globaux

Les attributs globaux doivent être définis pour pouvoir être associés à des applications individuelles. Ils sont définis dans la vue Propriétés en sélectionnant **Toutes les applications** dans la vue Explorateur.

Pourquoi et quand exécuter cette tâche



Pour supprimer un attribut ou sa valeur, sélectionnez son nom et cliquez sur **Supprimer un attribut** ( ). La suppression d'un attribut n'affecte pas les résultats de l'historique.

Pour créer un attribut et le rendre disponible dans une application :

Procédure

1. Sélectionnez **Toutes les applications** depuis la vue Explorateur.
2. Ouvrez l'onglet **Présentation** dans la vue Propriétés.
3. Entrez un nom pour l'attribut et cliquez sur **Ajouter un attribut** ( ) ou cliquez sur **Ajouter un attribut** sans spécifier un nom au préalable (vous serez invité ultérieurement à le spécifier dans une boîte de dialogue).
4. Entrez une **Valeur** pour l'attribut et cliquez sur **Ajouter une valeur d'attribut**, ou cliquez sur **Ajouter une valeur d'attribut** sans spécifier de valeur au préalable (vous serez invité ultérieurement à l'ajouter dans une boîte de dialogue).
5. Répétez cette étape pour ajouter d'autres valeurs d'attribut.

Attributs de l'application

Les attributs d'application s'appliquent à l'application actuellement sélectionnée et dépendent des attributs globaux créés auparavant.

Procédure

1. Sélectionnez l'application dans la vue Explorateur.
2. Ouvrez l'onglet **Présentation** dans la vue Propriétés.
3. Cliquez sur **Ajouter des attributs**. La boîte de dialogue **Attributs globaux** s'affiche avec la liste des attributs créés auparavant (les instructions à suivre pour créer des attributs globaux sont disponibles dans «Attributs globaux», à la page 64).
4. Cliquez deux fois sur l'attribut à ajouter ou sélectionnez-le et cliquez sur **OK**. L'attribut est ajouté à la section Attributs d'application de la vue Propriétés.

5. Cliquez sur la colonne **Valeur** et sélectionnez dans la liste une valeur pour cette application (plusieurs valeurs sont disponibles si l'attribut global a été créé avec plusieurs valeurs). Vous pouvez associer plusieurs attributs à une application.

Suppression d'applications et de projets

Vous pouvez supprimer des applications et des projets dans AppScan Source for Analysis si ces éléments ne sont pas enregistrés.

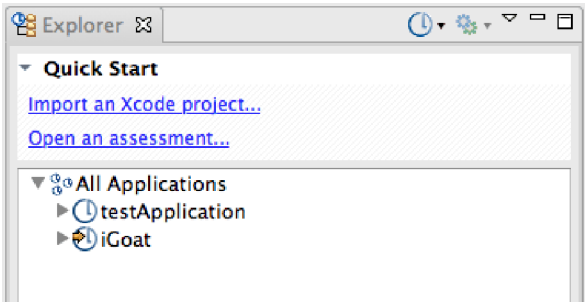
Procédure

1. Sélectionnez l'application ou le projet que vous souhaitez supprimer. Plusieurs applications et plusieurs projets peuvent être sélectionnés pour suppression, mais pas une combinaison d'applications et de projets.
2. Effectuez l'une des actions suivantes :
   - Cliquez avec le bouton droit de la souris sur votre sélection, puis sélectionnez **Supprimer une application** ou **Supprimer un projet** dans le menu.
   - Appuyez sur la touche Suppr de votre clavier.
   - Sélectionnez **Editer** > **Supprimer** dans le menu de plan de travail principal.

Vue Explorateur

La vue Explorateur contient une section **Démarrage rapide** dans sa partie supérieure et une section explorateur dans sa partie inférieure, qui contient un noeud, **Toutes les applications**. La section **Démarrage rapide** contient plusieurs liens utiles qui permettent de lancer les actions courantes. La section explorateur se compose d'une sous-fenêtre de navigation qui fournit une vue hiérarchique de vos ressources : applications, projets, répertoires et fichiers de projet, avec **Toutes les applications** comme racine. Vous pouvez naviguer entre ces ressources comme dans un explorateur de fichiers. Lorsque vous naviguez dans l'arborescence, le statut de votre sélection détermine les onglets disponibles dans la vue Propriétés.

Généralités



Depuis la vue Explorateur, vous pouvez ajouter des applications et des projets et examiner leur code à l'aide des boutons de la barre d'outils. Vous trouvez également des liens dans la section **Démarrage rapide**. Une fois les applications

ajoutées, la section explorateur fournit des indicateurs visuels relatifs à vos applications et projets, ainsi que le statut de chacun(e).

Conseil : Dans la vue Explorateur, une infobulle est disponible pour indiquer le nom de fichier et le chemin des applications, des projets et des fichiers. L'infobulle indique également si une application ou un projet est enregistré.

Section Démarrage rapide

La section **Démarrage rapide** contient les liens suivants pour le lancement des tâches courantes :

- **Importer un projet ou un espace de travail Xcode** : Lance une boîte de dialogue d'ouverture qui permet de rechercher et d'ajouter un répertoire `.xcodeproj` ou `.xcworkspace` existant en tant qu'application AppScan Source.
- **Importer un espace de travail basé sur Eclipse** : Lance la boîte de dialogue Ajout d'espace de travail qui vous permet d'ajouter un espace de travail Eclipse ou IBM Rational Application Developer for WebSphere Software (RAD) existant qui contient des projets Java. Une fois l'espace de travail importé, vous pouvez examiner n'importe quel projet Java inclus dans cet espace.

  Remarque : Avant d'importer l'espace de travail, assurez-vous d'avoir installé et mis à jour l'environnement de développement comme décrit dans la rubrique «Configuration de l'environnement de développement pour des projets Eclipse et Rational Application Developer for WebSphere Software (RAD)», à la page 47.
- **Importer depuis un serveur d'applications** : Importe une application Java existante d'un serveur d'applications Apache Tomcat ou WebSphere Application Server Liberty.
- **Ouvrir une évaluation** : Lance une boîte de dialogue d'ouverture qui vous permet de rechercher un fichier d'évaluation AppScan Source. Les types de fichier pouvant être inclus sont notamment `.ozasmt` et `.xml`.

Boutons de la barre d'outils

Tableau 8. Boutons de la barre d'outils

Action	Icône	Description
Ajouter un menu d'application		Lorsque vous cliquez sur la flèche vers le bas du bouton **Ajouter un menu d'application**, vous pouvez sélectionner des actions de création d'application, d'ouverture d'une application existante, d'importation d'un espace de travail ou de lancement de l'Application Discovery Assistant.

Tableau 8. Boutons de la barre d'outils (suite)

Action	Icône	Description
Examiner la sélection		Le bouton **Examiner la sélection** vous permet d'examiner l'objet sélectionné dans la section explorateur. La configuration d'examen par défaut est utilisée pour l'examen. Pour choisir une autre configuration d'examen à utiliser pour l'examen, cliquez sur la flèche vers le bas du bouton **Examiner la sélection**. Sélectionnez la configuration d'examen que vous souhaitez utiliser ou choisissez l'action **Editer des configurations** pour définir une autre configuration d'examen par défaut (dans la vue Configuration d'examen, sélectionnez la configuration que vous souhaitez définir par défaut et cliquez sur **Sélectionner comme valeur par défaut**).
Menu Vue		Le bouton **Menu Vue** affiche un menu qui vous permet d'actualiser la section explorateur et de masquer les éléments enregistrés.

Options du menu contextuel

La disponibilité des options de menu contextuel varie en fonction de l'élément qui est sélectionné dans la section explorateur.

- Lorsque l'élément **Toutes les applications** est sélectionné dans la section explorateur, les options de menu contextuel suivantes sont disponibles :
  - **Examiner toutes les applications** : Examine toutes les applications. L'examen s'exécute avec la configuration d'examen par défaut.
  - **Examiner toutes les applications avec** : Sélectionnez la configuration d'examen que vous souhaitez utiliser ou choisissez l'action **Editer des configurations** pour définir une autre configuration d'examen par défaut (dans la vue Configuration d'examen, sélectionnez la configuration que vous souhaitez définir par défaut et cliquez sur **Sélectionner comme valeur par défaut**).
  - **Ajouter une application**
    - **Créer une application** : Ajoute une nouvelle application à l'ensemble des applications. Cette action lance l'assistant Nouvelle application.
    - **Ouvrir une application existante** : Lance une boîte de dialogue d'ouverture qui vous permet de rechercher et d'ajouter une application existante à l'ensemble des applications. Les types de fichier ou de répertoire pouvant être ajoutés sont notamment `.paf`,`.xcodeproj`, `.xcworkspace` et `.ewf`.

- **Importer un espace de travail basé sur Eclipse existant** : Lance la boîte de dialogue Ajout d'espace de travail qui vous permet d'ajouter un espace de travail Eclipse ou IBM Rational Application Developer for WebSphere Software (RAD) existant qui contient des projets Java. Une fois l'espace de travail importé, vous pouvez examiner n'importe quel projet Java inclus dans cet espace.

  Remarque : Avant d'importer l'espace de travail, assurez-vous d'avoir installé et mis à jour l'environnement de développement comme décrit dans la rubrique «Configuration de l'environnement de développement pour des projets Eclipse et Rational Application Developer for WebSphere Software (RAD)», à la page 47.
- **Reconnaître les applications** : Lance l'Application Discovery Assistant qui permet de créer et de configurer rapidement des applications et des projets pour le code source Java.

– **Développer tout**
– **Réduire tout**
– **Propriétés** : Cette option permet d'ouvrir la vue Propriétés pour l'élément sélectionné.

• Lorsqu'une application est sélectionnée dans la section explorateur, les options de menu contextuel suivantes sont disponibles :
  – **Examiner l'application** : Examine l'application, le projet ou le fichier sélectionné. L'examen s'exécute avec la configuration d'examen par défaut.
  – **Examiner l'application avec** : Sélectionnez la configuration d'examen que vous souhaitez utiliser ou choisissez l'action **Editer des configurations** pour définir une autre configuration d'examen par défaut (dans la vue Configuration d'examen, sélectionnez la configuration que vous souhaitez définir par défaut et cliquez sur **Sélectionner comme valeur par défaut**).
  – **Ajouter un projet**
    - **Nouveau projet** : Si une application est sélectionnée dans la vue Explorateur, cette action est disponible et le fait de la choisir permet d'ajouter un nouveau projet à l'application. Cette action lance l'assistant Nouveau projet.
    - **Projet existant** : Si une application est sélectionnée dans la vue Explorateur, cette action est disponible et le fait de la choisir permet d'ajouter un projet existant à l'application. Cette action ouvre une boîte de dialogue dans laquelle vous pouvez accéder à un fichier `.ppfou .epf` , ou bien à un répertoire `.xcodeproj`, à ouvrir.
    - **Projets multiples** : Ajoute plusieurs projets à l'application qui est sélectionnée dans la vue Explorateur. Cette action lance une boîte de dialogue qui vous permet d'exécuter l'une des tâches suivantes :
      • Spécifier un répertoire dans lequel rechercher les projets.
      • Spécifier un espace de travail dans lequel rechercher les projets.

      Parmi les résultats de la recherche, vous pouvez sélectionner un ou plusieurs projets à ajouter.
  – **Supprimer une application** : Si une application est sélectionnée dans la vue Explorateur, cette action est disponible et le fait de la choisir permet de supprimer l'application sélectionnée.
  – **Ajouter une constatation personnalisée** : Cette action ouvre la boîte de dialogue Créer une constatation personnalisée afin de vous permettre de créer une constatation personnalisée pour l'application sélectionnée.

  - **Actualiser** : Actualise le contenu d'une application, d'un projet ou d'une vue sélectionné.
  - Enregistrer/Annuler l'enregistrement :
    - **Enregistrer l'application** : Enregistre l'application ou le projet sélectionné auprès de AppScan Source. Vous devez enregistrer des applications et des projets avant de pouvoir les publier dans la base de données AppScan Source.
    - **Enregistrer l'application comme...** : Cette option permet d'enregistrer à nouveau l'application sous un nouveau nom.
    - **Annuler l'enregistrement de l'application** : Annule l'enregistrement de l'application ou du projet sélectionné.
    - **Localiser** : Cette option permet d'associer une application ou un projet local à une application ou un projet qui a été enregistré par un autre utilisateur AppScan Source.
  - **Développer tout**
  - **Réduire tout**
  - **Propriétés** : Cette option permet d'ouvrir la vue Propriétés pour l'élément sélectionné.
- Lorsqu'un projet est sélectionné dans la section explorateur, les options de menu contextuel suivantes sont disponibles :
  - **Examiner le projet** : Examine l'application, le projet ou le fichier sélectionné. L'examen s'exécute avec la configuration d'examen par défaut.
  - **Examiner le projet avec** : Sélectionnez la configuration d'examen que vous souhaitez utiliser ou choisissez l'action **Editer des configurations** pour définir une autre configuration d'examen par défaut (dans la vue Configuration d'examen, sélectionnez la configuration que vous souhaitez définir par défaut et cliquez sur **Sélectionner comme valeur par défaut**).
  - **Copier le projet** : Si un projet est sélectionné dans la vue Explorateur, cette action est disponible et le fait de la choisir ouvre une boîte de dialogue qui permet de copier le projet dans une autre application ou de créer une copie du projet dans l'application où il est actuellement inclus.
  - **Supprimer le projet** : Supprime l'objet sélectionné.
  - Enregistrer/Annuler l'enregistrement :
    - **Enregistrer le projet** : Enregistre l'application ou le projet sélectionné auprès de AppScan Source. Vous devez enregistrer des applications et des projets avant de pouvoir les publier dans la base de données AppScan Source.
    - **Annuler l'enregistrement du projet** : Annule l'enregistrement de l'application ou du projet sélectionné.
    - **Localiser** : Cette option permet d'associer une application ou un projet local à une application ou un projet qui a été enregistré par un autre utilisateur AppScan Source.
  - **Développer tout**
  - **Réduire tout**
  - **Propriétés** : Cette option permet d'ouvrir la vue Propriétés pour l'élément sélectionné.
- Lorsqu'un fichier est sélectionné dans la section explorateur, les options de menu contextuel suivantes sont disponibles :
  - **Examiner le fichier** : Examine l'application, le projet ou le fichier sélectionné. L'examen s'exécute avec la configuration d'examen par défaut.

- **Examiner le fichier avec** : Sélectionnez la configuration d'examen que vous souhaitez utiliser ou choisissez l'action **Editer des configurations** pour définir une autre configuration d'examen par défaut (dans la vue Configuration d'examen, sélectionnez la configuration que vous souhaitez définir par défaut et cliquez sur **Sélectionner comme valeur par défaut**).
- **Exclure des examens** : Permet de supprimer le fichier sélectionné des examens.
- **Ouvrir dans l'éditeur interne** : Permet d'ouvrir le fichier sélectionné dans l'éditeur AppScan Source (dans la perspective Analyse).
- **Ouvrir dans l'éditeur externe** : Permet de choisir un éditeur externe dans lequel ouvrir le fichier sélectionné.
- **Propriétés** : Cette option permet d'ouvrir la vue Propriétés pour l'élément sélectionné.

Indicateurs d'application et de projet

Le tableau ci-après répertorie les icônes d'application et de projet dans la vue Explorateur.

Tableau 9. Icônes d'application et de projet

Type d'application ou de projet	Non enregistré	Enregistré	Manquant/ Introuvable
Application importée			
Application qui est créée manuellement ou à l'aide de l'Application Discovery Assistant			
Projet importé			
Projet qui est créé manuellement ou à l'aide de l'Application Discovery Assistant			

La vue Explorateur affiche les applications et projets locaux, ainsi que ceux enregistrés sur le serveur (ceux qui sont enregistrés sur le serveur mais qui ne sont pas enregistrés localement - par exemple, les applications et les projets enregistrés par d'autres utilisateurs - apparaissent grisés). Si vous cliquez sur le bouton **Menu d'affichage** dans la barre d'outils et que vous basculez vers l'option de menu **Masquer les éléments enregistrés sur le serveur** afin qu'il n'y ait pas de sélection, vous pouvez afficher les applications et projets existants sur le serveur. Si un projet est grisé, vous pouvez cliquer dessus avec le bouton droit de la souris et sélectionner dans le menu l'option **Localiser**.

Chapitre 3. Préférences

Les préférences sont les choix personnels de l'utilisateur concernant l'apparence et le fonctionnement de AppScan Source for Analysis.

Pour ouvrir la page des préférences, sélectionnez **Editer** > **Préférences** à partir du menu principal du plan de travail. Vous pouvez parcourir les préférences en naviguant dans tous les titres du panneau de gauche ou seulement dans un sous-ensemble de ces titres en utilisant la zone de filtre au sommet de ce panneau. Les résultats renvoyés par le filtre correspondent aussi bien aux titres de la page des préférences qu'à des mots clés tels que JSP ou courrier électronique.

La flèche à l'angle supérieur droit du panneau de droite vous permet d'accéder à des pages déjà visualisées. Pour revenir à une page antérieure, cliquez sur la flèche pointant vers le bas afin d'afficher la liste des pages de préférences récemment affichées.

Préférences générales

Les préférences générales vous permettent d'adapter certains paramètres par défaut de AppScan Source for Analysis en fonction de vos préférences personnelles.

Sélection de langue

L'interface utilisateur de AppScan Source for Analysis peut être affichée en différentes langues. Pour modifier la langue nationale qui s'affiche, sélectionnez-la dans la liste de **sélection de langue**, puis cliquez sur **OK** dans la boîte de dialogue des préférences. Vous devez redémarrer manuellement le plan de travail pour que les modifications soient prises en compte.

Remarque : Pour utiliser cette fonction, un module linguistique au minimum doit être installé lors de la procédure d'installation. Si l'anglais est la seule langue installée, le produit s'affichera en anglais une fois cette préférence utilisée et le plan de travail redémarré. Dans ce cas, si vous souhaitez afficher une autre langue que l'anglais, lancez à nouveau l'assistant d'installation et choisissez de réparer l'installation en ajoutant un ou plusieurs modules linguistiques.

Codage du fichier

Le codage de caractères des fichiers dans votre projet doit être défini afin que AppScan Source puisse lire ces fichiers correctement (et, par exemple, afin qu'il puisse les afficher correctement dans la vue Source). Sélectionnez le codage de caractères par défaut dans cette section.

Niveau de journalisation

Modifiez le niveau de journalisation afin de fournir le niveau d'information à inclure dans les journaux des erreurs. Choisissez **Trace**, **Déboguer**, **Informations**, **Avertissements**, **Erreurs** ou **Fatal**. **Trace** offre le niveau de consignation le plus bruyant, **Fatal** consigne uniquement les événements critiques et les autres paramètres offrent respectivement des niveaux de consignation plus élevés par incréments.

Sauvegarder tous les filtres à la sortie

Lorsque vous sélectionnez cette option, l'invite est désactivée et tous les filtres nouveaux ou modifiés sont automatiquement sauvegardés lorsque vous quittez AppScan Source.

Annuler l'examen en cas d'erreur

Cette option évite les examens incomplets en annulant ceux-ci en cas d'erreur.

Créer un marqueur pour chaque constatation

Lorsque cette option est sélectionnée lorsqu'une évaluation est ouverte, la source provenant de l'examen ouvert dans l'éditeur inclura des marqueurs aux emplacements auxquels se trouvent des constatations.

Par défaut, la création de marqueurs est activée.

La création de marqueurs peut ralentir un examen. Si votre projet inclut de nombreux fichiers source (ou des fichiers source volumineux), vous pouvez désactiver la création de marqueurs pour optimiser les performances.

A l'achèvement d'un examen

Par défaut, une invite s'affiche pour vous demander si vous désirez que l'évaluation s'ouvre automatiquement à la fin d'un examen. Pour que cette invite ne s'affiche pas, sélectionnez **Toujours ouvrir la nouvelle évaluation** ou **Ne jamais l'ouvrir**.

A l'achèvement d'un examen, s'il existe des examens non sauvegardés des mêmes cibles

Par défaut, vous êtes invité à sauvegarder ou annuler les examens non sauvegardés existants. Vous pouvez modifier cette préférence afin que des examens en doublon soient toujours supprimés automatiquement, ou jamais supprimés automatiquement. Lors de la définition de cette préférence, sachez que l'utilisation de la mémoire est réduite lorsque des examens en doublon sont supprimés.

Lors de la publication ou de l'exportation d'une évaluation avec des chemins absolus

Par défaut, vous êtes invité à définir des variables de chemin absolu lors de la publication. Les paramètres dans cette section permettent de désactiver cette invite par défaut ou d'ouvrir automatiquement la boîte de dialogue qui permet de définir des variables lorsque des chemins absolus existent.

Enregistrer automatiquement les applications lors de leur publication initiale

Par défaut, lorsque vous publiez des évaluations pour des applications ou des projets non enregistrés, vous êtes invité à les enregistrer. Vous pouvez choisir de toujours enregistrer des applications et des projets lorsqu'ils sont publiés ou de ne jamais les enregistrer.

Important : Vous devez disposer du droit **Enregistrer** afin de pouvoir enregistrer des applications et des projets.

En cas de conflit entre les noms d'applications

Plusieurs applications du même nom peuvent exister dans AppScan Source for Analysis, mais leur utilisation peut être ingérable. Par défaut, si vous tentez d'attribuer à une application un nom déjà utilisé (ou d'importer une application ayant le même nom qu'une application existante), un avertissement est émis. Le message d'avertissement vous permet de générer un nom unique pour l'application, de conserver le nom conflictuel ou d'annuler.

Pour que AppScan Source for Analysis génère automatiquement un nom d'application unique lorsque des conflits se produisent, sélectionnez **Générer un nom unique** dans la page de préférences. Si vous souhaitez accepter automatiquement les noms d'application conflictuels, sélectionnez **Conserver le nom existant**.

Remarque : Les applications sont stockées sous le nom de fichier `<nom_application>.paf`. Si vous sélectionnez **Conserver le nom existant**, vous ne pouvez pas définir le répertoire de travail comme étant le même que celui de l'application existante du même nom. Dans ce cas, vous êtes invité à remplacer le nom de fichier existant, mais cette opération échoue car l'application existante est déjà ouverte dans AppScan Source for Analysis.

En cas de conflit entre les noms de projet

Ce paramètre s'applique uniquement lorsque vous tentez de créer ou d'importer un projet du même nom que celui qui existe dans la même application. Dans ce cas, les noms de projets ne sont pas conflictuels. Vous êtes alors invité par défaut à générer un nom unique ou à annuler l'action. Pour que AppScan Source for Analysis génère automatiquement un nom de projet unique lorsque des conflits se produisent, sélectionnez **Générer un nom unique** dans la page de préférences.

Nombre d'évaluations affichées au démarrage dans Evaluations publiées et Mes évaluations

Définissez le nombre maximal d'évaluations à afficher dans la vue Evaluations publiées ou Mes évaluations.

Flux RSS affiché dans la vue de bienvenue

Par défaut, la vue de bienvenue affiche le contenu du flux RSS X-Force. Pour afficher un autre contenu, entrez l'adresse URL souhaitée dans la zone **Flux RSS affiché dans la vue de bienvenue**.

Optimiser pour temps de latence réseau élevé

Cochez cette case pour mettre en cache plus d'informations sur le client afin de minimiser les appels au serveur.

Recharger la configuration système

Charge les paramètres système les plus récents. Si vous avez modifié les paramètres en dehors du produit pendant son exécution, par exemple, si vous avez modifié les fichiers `.ozsettings` dans le répertoire `<data_dir>\config` (où `<rép_données>` est l'emplacement de vos données de programme AppScan Source, comme décrit dans «Installation et emplacements des fichiers de données

utilisateur», à la page 292), sélectionnez ce bouton pour actualiser les paramètres dans le produit.

Préférences AppScan Enterprise Console

Si votre serveur AppScan Enterprise Server a été installé avec l'option AppScan Enterprise Console, vous pouvez publier des évaluations sur cette console. Le composant Enterprise Console offre divers outils de gestion des évaluations, tels que des fonctions de génération de rapports, de gestion de problème et d'analyse de tendance, ainsi que des tableaux de bord.

Pour activer cette fonction, renseignez la page des préférences AppScan Enterprise Console. Toutes les zones de cette page doivent être renseignées avec des entrées valides avant l'activation de la publication d'Enterprise Console :

- Zone **ID utilisateur** : Entrez votre ID utilisateur AppScan Enterprise Server (l'ID utilisateur créé pour publication au nom de votre utilisateur AppScan Source).
  - Si votre serveur AppScan Enterprise Server est configuré pour utiliser l'authentification Windows, entrez le nom de domaine et d'utilisateur que vous utilisez pour vous connecter au serveur Enterprise Console (en les séparant par un signe \. Par exemple, `my_domain\my_username`).
  - Si votre serveur AppScan Enterprise Server est configuré avec LDAP, entrez le nom d'utilisateur que vous utilisez pour vous connecter au serveur Enterprise Console.

  Au minimum, vous devez être un utilisateur QuickScan. Si vous êtes connecté à un serveur AppScan Enterprise Server antérieur à la version 9.0.3, vous devez disposer de votre propre dossier utilisateur sur le serveur Enterprise Server.
- Zone **Mot de passe** : Entrez le mot de passe utilisé pour connexion au serveur Enterprise Console (le mot de passe correspondant à l'ID utilisateur saisi).
- Zone **URL de la console Enterprise** : indiquez l'URL utilisée pour accéder à l'application Web Enterprise Console.

  Le format de cette URL est le suivant :

  `http(s)://<nmhôte>:<port>/ase`

  Où `<nom_d'hôte>` est le nom de la machine sur laquelle Enterprise Console a été installé, et `<port>`, le port sur lequel la console s'exécute (par défaut, `<port>` correspond au port `9443`). Exemple: `https://myhost.mydomain.ibm.com:9443/ase`.

  Remarque :
  - Cette zone n'a pas besoin d'être modifiée si l'**URL de la console Enterprise** a déjà été définie.
  - Pour pouvoir définir la zone **URL de la console Enterprise**, vous devez être connecté à AppScan Source avec l'autorisation **Gérer les paramètres AppScan Enterprise**. Pour plus d'informations sur les comptes utilisateur et les autorisations, voir la section *Administration* du centre de documentation du produit - ou la section *Administration de AppScan Source* du document *IBM Security AppScan Source - Guide d'installation et d'administration*.
  - L'**ID utilisateur** et le **mot de passe** sont stockés sur le poste sur lequel le client AppScan Source s'exécute (par exemple, AppScan Source for Analysis), tandis que l'**URL de la console Enterprise** est stockée dans Enterprise Server (qui peut se trouver sur un poste distant). Vous ne pouvez pas accéder aux informations de nom d'utilisateur et de mot de passe à partir du poste distant (par exemple, en émettant la commande `getaseinfo`).

– AppScan Source ne prend pas en charge la publication sur une instance d'AppScan Enterprise Console ayant été configurée pour utiliser des paramètres de proxy. Toute tentative de publication vers une telle instance se soldera par une erreur.

Après avoir renseigné ces paramètres, il est fortement recommandé de vérifier que la connexion au serveur Enterprise Console est valide en cliquant sur **Tester la connexion**.

Conseil : Si le test de connexion échoue, vérifiez que le serveur Enterprise Console est en cours d'exécution et que vous pouvez accéder à l'URL de son centre de contrôle dans un navigateur (en utilisant la même **URL de console Entreprise** que celle spécifié ci-dessus).

Préférences de serveur d'applications pour la compilation des JSP

Si vous examinez une application contenant des pages JSP (JavaServer Pages), le moteur d'analyse de AppScan Source doit pouvoir compiler le code JSP afin de l'analyser. Lorsque vous créez votre projet JSP, vous devez spécifier le compilateur JSP devant être utilisé par AppScan Source (ou accepter le compilateur par défaut, qui peut être défini sur la page de préférences Java et JSP). Si AppScan Source ne peut pas compiler vos fichiers JSP, utilisez les pages de préférences du serveur d'applications pour configurer le compilateur de JSP employé par votre application.

Les versions d'Apache Tomcat versions 7 et 8 sont incluses dans l'installation d'AppScan Source. Si les pages de préférences **Tomcat 7** et **Tomcat 8** ne sont pas configurées, AppScan Source compile les fichiers JSP à l'aide du compilateur JSP Tomcat fourni et indiqué comme valeur par défaut. Si vous souhaitez employer un compilateur Tomcat externe pris en charge, utilisez les pages de préférences Tomcat pour pointer sur votre installation Tomcat locale.

Si vous utilisez Oracle WebLogic Server ou WebSphere Application Server, vous devez configurer la page de préférences correspondante, le but étant de désigner votre installation locale du serveur d'applications afin qu'elle puisse être utilisée pour la compilation du code JSP durant l'analyse (si vous créez votre projet JSP sans d'abord configurer le serveur d'applications, vous serez invité à configurer ce dernier à ce moment-là).

Tomcat

Cette rubrique décrit les préférences que vous devez définir pour configurer AppScan Source afin qu'il pointe sur un serveur d'applications Apache Tomcat autre que celui fourni avec AppScan Source.

Les versions d'Apache Tomcat versions 7 et 8 sont incluses dans l'installation d'AppScan Source. Si les pages de préférences **Tomcat 7** et **Tomcat 8** ne sont pas configurées, AppScan Source compile les fichiers JSP à l'aide du compilateur JSP Tomcat fourni et indiqué comme valeur par défaut. Si vous souhaitez employer un compilateur Tomcat externe pris en charge, utilisez les pages de préférences Tomcat pour pointer sur votre installation Tomcat locale.

Si vous utilisez un compilateur Tomcat externe pris en charge, allez à la page de préférences appropriée et spécifiez le répertoire d'installation du serveur d'applications. La spécification du répertoire d'installation permet à AppScan Source de détecter automatiquement les dépendances de serveur d'application lors de la configuration de projets.

WebLogic 11 et 12

Cette rubrique décrit les préférences que vous devez définir pour configurer AppScan Source afin qu'il pointe sur un serveur Oracle WebLogic Server.

Dans les pages de préférences de WebLogic, vous pouvez spécifier le répertoire d'installation du serveur et vous pouvez définir les options de configuration avancées. La spécification du répertoire d'installation permet à AppScan Source de détecter automatiquement les dépendances de serveur d'application lors de la configuration de projets.

Configurez AppScan Source afin qu'il fasse référence au répertoire d'installation de WebLogic, au fichier JAR WebLogic et aux options de compilateur JSP (JavaServer Page).

Cochez la case **Activer les options de configuration avancées** uniquement si vous devez modifier les options de compilateur JSP WebLogic par défaut ou localiser le fichier `weblogic.jar`. Les options de compilateur JSP WebLogic par défaut sont les suivantes :

```
%JSP_JVM_OPTIONS%
 -Dcom.sun.xml.namespace.QName.useCompatibleSerialVersionUID=1.0
 -classpath
%JSP_COMPILER_CLASSPATH% weblogic.jspc
%JSP_OPTIONS% -verboseJspc -package
%PACKAGE_NAME% -linenumbers -g -debug -keepgenerated -compiler
%JAVAC_PATH% -webapp
%WEB_CONTEXT_ROOT_PATH% -d
%OUTPUT_PATH%
```

WebSphere Application Server

Cette rubrique décrit les préférences que vous devez définir pour configurer AppScan Source afin qu'il fasse référence à WebSphere Application Server pour la compilation JSP.

Pour en savoir plus sur les versions de WebSphere Application Server prises en charge par AppScan Source, voir http://www.ibm.com/support/docview.wss?uid=swg27027486.

Dans les pages des préférences WebSphere Application Server, vous devez spécifier le répertoire d'installation du serveur et pouvez définir des options de configuration avancées. La spécification du répertoire d'installation permet à AppScan Source de trouver et d'utiliser le compilateur JSP WebSphere Application Server.

Configurez AppScan Source pour pointer vers le répertoire d'installation de WebSphere Application Server. Des options de configuration avancée vous permettent également de définir la ligne de commande du compilateur JSP de WebSphere Application Server et le chemin de classes du serveur.

Cochez la case **Activer les options de configuration avancées** si vous devez personnaliser la ligne de commande JSP WebSphere Application Server ou spécifier un chemin d'accès aux classes autre que le chemin d'accès aux classes WebSphere Application Server par défaut (modifiez ce paramètre si vous souhaitez inclure des fichiers JAR supplémentaires dans le chemin d'accès aux classes utilisé par vos applications WebSphere Application Server).

Par défaut, l'option de ligne de commande du compilateur JSP de WebSphere Application Server est la suivante :

```
%CMD_EXE% %CMD_ARGS%
'%FILE(%%JSP_COMPILER_INSTALL_DIR%/bin/JspBatchCompiler%BAT%%)%'
-response.file
'%TMP_FILE(%-keepgenerated=true -recurse=true -useFullPackageNames=true
-verbose=false -createDebugClassfiles=true -jsp.file.extensions=%WEB_EXTS%
-javaEncoding=%ENCODING%
%JSP_OPTIONS% %QUOTE%-war.path=%WEB_CONTEXT_ROOT_PATH%%QUOTE%
%QUOTE%-filename=%RELATIVE_FILENAME_NO_QUOTE% %QUOTE%  %)%'
```

Définition de variables

Lors de la sauvegarde d'évaluations ou de groupements, ou de la publication d'évaluations, AppScan Source for Analysis peut vous suggérer de créer une variable pour remplacer des chemins absolus (sans variables, AppScan Source for Analysis consigne des chemins absolus vers le fichier d'évaluation pour référencer des éléments tels que des fichiers source). La configuration de variables pour des chemins absolus facilite le partage des évaluations entre plusieurs ordinateurs. L'utilisation de variables est conseillée en cas de partage des évaluations.

Pourquoi et quand exécuter cette tâche

Les variables peuvent être créées avant le lancement d'une action de sauvegarde ou de publication en suivant les instructions fournies dans cette rubrique, ou après son lancement en suivant les étapes décrites dans «Définition de variables lors de la publication et de la sauvegarde», à la page 114.

Pour savoir par exemple comment les variables peuvent apporter leur contribution lors du partage des évaluations, voir «Exemple : définition de variables», à la page 115.

Procédure

1. Sélectionnez **Editer** > **Préférences** dans le menu principal. Dans la boîte de dialogue Préférences, choisissez **Modifier les variables**.
2. Cliquez sur le bouton **Ajouter une variable** dans la page de préférences Modifier les variables.
3. Entrez le nom de la variable et recherchez un emplacement de fichier qui sera remplacé par la variable (AppScan Source for Analysis insère les symboles pourcentage encadrant la variable (%) une fois cette dernière créée).
4. Répétez l'étape ci-dessus pour d'autres éléments de référence dans l'évaluation (par exemple, si l'évaluation référence la source à plusieurs emplacements, ajoutez une variable pour chaque emplacement).
5. La page de préférences vous permet d'éditer et de supprimer des variables, respectivement à l'aide des boutons **Modifier** et **Supprimer**.
6. Cliquez sur **OK** une fois la définition des variables terminée.

Activation du suivi des défauts depuis les préférences

Les préférences du système de suivi des défauts permettent d'activer la soumission des constatations à un système de suivi des défauts et de déterminer la manière dont celle-ci s'effectue.

L'onglet Options générales de la page des préférences Système de suivi des défauts permet d'activer ou de désactiver la fonction d'intégration de ce système avec

AppScan Source. Si la case **Activer l'intégration du système de suivi des défauts** est cochée, l'action **Soumettre un défaut** sera disponible dans le menu contextuel pour son application aux constatations de l'évaluation.

Pour en savoir plus sur les préférences pouvant être définies pour les systèmes de suivi des défauts pris en charge, consultez les rubriques d'aide ci-dessous.

- «Préférences Rational Team Concert»

Préférences Rational Team Concert

L'onglet des préférences Rational Team Concert vous permet de configurer une connexion avec un serveur Rational Team Concert, ainsi que les valeurs des attributs des éléments de travail.

Après avoir saisi vos informations de connexion et avoir établi une connexion, vous pouvez opter de vous connecter à une ou plusieurs zones de projet. Chaque zone projet peut disposer de sa propre configuration de valeurs d'attributs prédéfinies.

Remarque : Lorsque vous vous connectez à Rational Team Concert (en configurant des préférences ou en soumettant des défauts), il se peut que le système vous invite à accepter un certificat SSL. Pour plus d'informations, voir «Certificats SSL pour Rational Team Concert».

Pour configurer les valeurs d'attributs d'une zone de projet donnée, sélectionnez celle-ci, puis l'option **Configurer**. Dans la boîte de dialogue de configuration, vous pouvez affecter à ces zones des valeurs d'attributs codées en dur ou, dans certains cas, des variables se référant à une constatation spécifique. Par exemple, l'utilisation de `{Finding.fileName}` comme valeur d'attribut sera remplacée lors de sa soumission par le nom de fichier effectif du code source d'une constatation. Une assistance sur le contenu (`<Ctrl>+<Espace>`) est fournie pour les valeurs d'attributs prenant en charge ces variables. Nous encourageons les équipes à partager ces configurations à l'aide des boutons **Importer** et **Exporter** disponibles sur la page des préférences Rational Team Concert.

Certificats SSL pour Rational Team Concert

Une fois qu'un serveur Rational Team Concert est installé, vous devez le configurer afin qu'il utilise un certificat SSL valide. Faute de quoi, vous recevez un message indiquant que la connexion est non sécurisée lors de la connexion au serveur (lors de configuration de préférences ou de la soumission de défauts). Cette rubrique contient des remarques sur le certificat SSL Rational Team Concert.

Emplacement de stockage du certificat SSL

Les certificats qui ont été acceptés de manière définitive sont stockés dans `<user_home>/.jazzcerts` (où `<user_home>` est le répertoire d'accueil de votre système d'exploitation (par exemple, sous Windows, le répertoire peut être `C:\Documents and Settings\Administrator\`)). Si vous supprimez `<user_home>/.jazzcerts`, tous les certificats stockés pour les clients AppScan Source et Rational Team Concert sont supprimés.

Partage de certificat SSL avec des clients Rational Team Concert

AppScan Source partage son magasin de certificats avec des clients Rational Team Concert. Si vous acceptez un certificat de façon définitive à l'aide d'un client Rational Team Concert, il sera réutilisé par AppScan Source (AppScan Source vous

invitera à accepter un certificat). De la même façon, si vous acceptez un certificat de façon définitive dans AppScan Source, il sera réutilisé par des clients Rational Team Concert.

Considérations relatives au renommage du serveur Rational Team Concert lorsque le suivi des défauts est activé pour AppScan Source for Analysis

Si vous avez activé le suivi des défauts Rational Team Concert dans AppScan Source for Analysis et que le serveur Rational Team Concert est renommé, toute configuration existante pour les zones de projet sur ce serveur n'est plus disponible dans AppScan Source for Analysis. Vous devez alors vous connecter au serveur via son nouvel URI de référentiel et recréer la configuration dans les préférences du système de suivi des défauts.

Importateurs d'espaces de travail Eclipse : Configuration des préférences Eclipse

L'installation de AppScan Source for Analysis fournit un importateur Eclipse par défaut. Cet importateur identifie l'emplacement d'Eclipse et du JRE. Si l'importateur Eclipse par défaut est incapable d'importer votre espace de travail, il peut s'avérer nécessaire de créer un nouvel importateur Eclipse.

Avant de commencer

Chaque configuration d'importateur représente une installation d'Eclipse ou de Rational Application Developer for WebSphere Software (RAD). Pour utiliser ces configurations pour importer des espaces de travail et des projets existants vers AppScan Source for Analysis, vous pouvez avoir besoin d'installer les plug-in AppScan Source for Development dans l'environnement Eclipse.

Avant d'ajouter un espace de travail RAD, vous devez créer une configuration pour le type d'espace de travail.

Procédure

1. Dans AppScan Source for Analysis, sélectionnez **Editer** > **Préférences** à partir du menu principal du plan de travail.
2. Sélectionnez **Importateurs d'espace de travail Eclipse**.
3. Cliquez sur **Créer une nouvelle configuration** et renseignez la boîte de dialogue Nouvelle configuration d'importation pour créer une nouvelle configuration :
   - **Produit** : Sélectionnez le produit approprié.

     Remarque : Si le produit utilisé pour créer l'espace de travail n'est pas disponible à la sélection, vérifiez que vous avez suivi les étapes de configuration décrites dans «Mises à jour d'Eclipse ou d'Application Developer», à la page 48 avant de tenter de créer l'importateur d'espace de travail.
   - **Nom** : Nom de l'importateur
   - **Emplacement** : Chemin du répertoire de base de l'installation Eclipse
   - **Emplacement du JRE** : Chemin du répertoire racine de l'environnement d'exécution Java (JRE). Utilisez un kit JDK fourni dans `<install_dir>\JDKS` (où `<rép_install>` représente l'emplacement de votre installation AppScan Source) ou un autre kit JDK de votre choix.
4. Cliquez sur **OK**.

5. Pour identifier l'importateur défini par défaut, sélectionnez-le et cliquez sur **Définir comme configuration par défaut celle sélectionnée**. Après cela, une icône s'affiche dans la colonne **Par défaut** de l'importateur.

Courrier électronique

Configurez les paramètres de courrier électronique utilisés pour l'envoi des constatations à l'étude en tant que défauts.

- **Adresse de destination** : adresse électronique du destinataire. Par défaut, la zone **Envoyer à** de la boîte de dialogue d'envoi de constatations par courrier électronique contient cette adresse électronique, toutefois, elle peut facilement être modifiée lors de la préparation du courrier électronique.
- **Adresse de l'expéditeur** : adresse électronique de l'expéditeur.

  Remarque : Une adresse électronique valide est recommandée afin d'éviter que le client de messagerie destinataire considère les messages comme étant du spam.
- **Serveur de messagerie** : serveur de messagerie SMTP configuré, comme `mail.myexample.com`.

  Important : Consultez votre administrateur système pour vérifier que vous disposez des informations de serveur de messagerie correctes.

Java et JavaServer Pages

Cette page de préférences permet d'ajouter, modifier ou supprimer le JDK (Java Development Kit) qui est utilisé pour les examens (et de définir un kit JDK par défaut). Elle permet, de plus, de définir le compilateur JSP (JavaServer Page) par défaut.

Par défaut

Identifie l'emplacement du kit JDK utilisé pour les examens. L'examen utilise le chemin JDK par défaut lorsque le projet ne spécifie pas explicitement un kit JDK. Pour définir le kit JDK par défaut, cliquez avec le bouton droit de la souris sur le nom du kit voulu et sélectionnez **Définir le kit JDK par défaut**. L'icône de valeur par défaut apparaît dans la table, identifiant le kit par défaut JDK actuel.

Remarque : Prêt à l'emploi, le compilateur par défaut des projets JSP est Tomcat 7, qui requiert Java version 1.6 ou version ultérieure. Si **Tomcat 7** est conservé par défaut et que vous sélectionnez un JDK plus ancien, des erreurs de compilation seront générées pendant les examens.

Nom et chemin d'accès JDK

Identifie le nom et l'emplacement du kit JDK.

Compilateur par défaut pour les projets JSP

Prêt à l'emploi, Tomcat 7 est le compilateur JSP par défaut. Pour en savoir plus sur les compilateurs pris en charge par AppScan Source for Analysis, voir http://www.ibm.com/support/docview.wss?uid=swg27027486.

Articles de la Base de connaissances

Utilisez la page de préférences Articles de la Base de connaissances pour définir les emplacements qui contiennent les articles de la Base de connaissances de sécurité AppScan Source Security.

La page dresse la liste des répertoires qui contiennent des articles. Pour ajouter un répertoire, cliquez sur **Ajout d'un répertoire de contenu** et naviguez jusqu'à l'endroit où se trouvent les articles. Pour retirer un répertoire de la liste, sélectionnez-le et cliquez sur **Supprimer**.

Extensions de fichier de projet

Configurez ou ajoutez des extensions de fichier globales valides pour chaque type de projet, modifiez les extensions à inclure dans les analyses ou à exclure de ces dernières, et spécifiez des extensions en tant que fichiers Web.

Une page d'onglet apparaît pour chaque langage ou type de projet disponible :Java, JavaScript et Objective-C. Lors de l'ajout d'une nouvelle extension, indiquez si les fichiers concernés peuvent être analysés, considérés comme étant des fichiers Web ou exclus.

Les paramètres dans cette page sont globaux. Pour définir les extensions de fichier pour des projets individuels, utilisez l'onglet «Extensions de fichier», à la page 222 de la vue Propriétés pour le projet sélectionné.

Paramètres d'extension de fichier

Tableau 10. Paramètres d'extension de fichier

Paramètre	Description	Exemples d'utilisation
Examen ou **Evaluation**	Inclure les fichiers ayant l'extension indiquée dans l'analyse complète.	• Si une extension `.xxx` est créée pour les projets Java et marquée comme **Examen** ou **Evaluation**, les fichiers dotés de cette extension seront compilés et examinés. • Un fichier peut faire partie d'un projet mais ne pas être marqué comme **Examen** ou **Evaluation** s'il ne doit pas être compilé et examiné.
Fichier Web	Marquer les fichiers ayant l'extension indiquée pour la compilation JSP. Ce paramètre autorise AppScan Source à séparer les sources Web des sources non Web.	Si une extension `.yyy` est créée pour les projets Java et marquée comme **Fichier Web**, les fichiers ayant cette extension sont organisés en sources Web dans les projets. Lorsqu'AppScan Source se prépare pour l'analyse, ces fichiers seront précompilés en classes à analyser.

Tableau 10. Paramètres d'extension de fichier (suite)

Paramètre	Description	Exemples d'utilisation
Exclure	Ne pas créer de fichiers source dans le projet pour des fichiers ayant l'extension indiquée. Les fichiers ayant cette extension ne seront pas examinés.	Créez une extension `.zzz` pour les fichiers qui sont nécessaires à vos projets pour la compilation, mais qui ne doivent pas être inclus dans l'analyse.

Chapitre 4. Examen du code source et gestion des évaluations

Cette section explique comment examiner votre code source et gérer les évaluations.

Une fois que vous avez configuré des applications et des projets ou que vous avez utilisé la fonction Application Discovery Assistant pour créer des applications et des projets, vous êtes prêt à examiner leur code source. Le résultat d'un examen, nommé *évaluation*, peut être sauvegardé ou publié. Une *évaluation sauvegardée* désigne un fichier de résultats de l'examen sauvegardé localement et qui peut être publié, ouvert plus tard pour un triage supplémentaire ou ouvert dans AppScan Source for Development. Une *évaluation publiée* indique que les résultats de l'examen ont été sauvegardés sur le serveur AppScan Enterprise Server.

Vous pouvez gérer les évaluations depuis deux vues :

- Mes évaluations
- Evaluations publiées

Remarque : Lors de la sauvegarde, de la publication ou de l'ouverture d'une évaluation, la progression de l'opération est indiquée dans la barre d'état.

Analyse du code source

Cette tâche décrit les diverses méthodes de lancement des examens.

Pourquoi et quand exécuter cette tâche

Vous pouvez effectuer des examens à divers niveaux (toutes les applications, une ou plusieurs applications, un ou plusieurs projets, un ou plusieurs fichiers). Si vous avez terminé un examen, vous pouvez la relancer à condition que son évaluation soit ouverte.

- «Examen de toutes les applications», à la page 86
- «Examen d'une ou de plusieurs applications», à la page 86
- «Examen d'un ou de plusieurs projets», à la page 86
- «Examen d'un ou de plusieurs fichiers», à la page 87
- «Nouvel examen du code», à la page 87

Voir «Considérations relatives aux examens», à la page 87 pour plus de détails sur les considérations spécifiques à un système d'exploitation, les considérations spécifiques à une langue ou d'autres restrictions qui peuvent affecter vos examens.

On utilise toujours une configuration d'examen lors d'un examen. Si vous définissez une configuration d'examen par défaut et que vous la supprimez, la configuration d'examen intégrée **Examen normal** sera utilisée en mode silencieux lors de l'examen. Pour en savoir plus sur les configurations d'examen, voir «Gestion des configurations d'examen», à la page 90 et les descriptions d'option d'examen ci-dessous.

Examen de toutes les applications

Procédure

Effectuez l'une des actions suivantes :

1. Sélectionnez **Examiner** > **Examiner tout** dans le menu principal du plan de travail. L'analyse s'exécute alors avec la configuration d'analyse par défaut.
2. Dans la vue Explorateur :
   - Dans la vue Explorateur, cliquez avec le bouton droit de la souris sur **Toutes les applications**, puis sélectionnez **Examiner toutes les applications** dans le menu. L'analyse s'exécute alors avec la configuration d'analyse par défaut.
   - Pour utiliser une autre configuration d'examen, cliquez avec le bouton droit de la souris sur **Toutes les applications**, puis sélectionnez **Examiner toutes les applications avec** dans le menu. Sélectionnez la configuration d'examen que vous souhaitez utiliser ou, si vous souhaitez définir une autre configuration d'examen par défaut, choisissez l'action **Editer des configurations** (dans la vue Configuration d'examen, sélectionnez la configuration que vous souhaitez définir par défaut et cliquez sur **Sélectionner comme valeur par défaut**).

Examen d'une ou de plusieurs applications

Procédure

1. Dans la vue Explorateur, sélectionnez une ou plusieurs applications.
2. Effectuez l'une des actions suivantes :
   a. Sélectionnez **Examiner** > **Examiner la sélection** dans le menu principal du plan de travail. L'analyse s'exécute alors avec la configuration d'analyse par défaut.
   b. Dans la vue Explorateur :
      - Cliquez avec le bouton droit de la souris sur votre sélection et sélectionnez **Examiner l'application** dans le menu. L'analyse s'exécute alors avec la configuration d'analyse par défaut.
      - Pour utiliser une autre configuration d'examen, cliquez avec le bouton droit de la souris sur la sélection, puis sélectionnez **Examiner l'application avec** dans le menu. Sélectionnez la configuration d'examen que vous souhaitez utiliser ou, si vous souhaitez définir une autre configuration d'examen par défaut, choisissez l'action **Editer des configurations** (dans la vue Configuration d'examen, sélectionnez la configuration que vous souhaitez définir par défaut et cliquez sur **Sélectionner comme valeur par défaut**).

Examen d'un ou de plusieurs projets

Procédure

1. Depuis la vue Explorateur, sélectionnez un ou plusieurs projets.
2. Effectuez l'une des actions suivantes :
   a. Sélectionnez **Examiner** > **Examiner la sélection** dans le menu principal du plan de travail. L'analyse s'exécute alors avec la configuration d'analyse par défaut.
   b. Dans la vue Explorateur :
      - Cliquez avec le bouton droit de la souris sur votre sélection et sélectionnez **Examiner le projet** dans le menu. L'analyse s'exécute alors avec la configuration d'analyse par défaut.

- Pour utiliser une autre configuration d'examen, cliquez avec le bouton droit de la souris sur la sélection, puis sélectionnez **Examiner le projet avec** dans le menu. Sélectionnez la configuration d'examen que vous souhaitez utiliser ou, si vous souhaitez définir une autre configuration d'examen par défaut, choisissez l'action **Editer des configurations** (dans la vue Configuration d'examen, sélectionnez la configuration que vous souhaitez définir par défaut et cliquez sur **Sélectionner comme valeur par défaut**).

Examen d'un ou de plusieurs fichiers

Procédure

1. Depuis la vue Explorateur, sélectionnez un ou plusieurs fichiers.
2. Effectuez l'une des actions suivantes :
   a. Sélectionnez **Examiner** > **Examiner la sélection** dans le menu principal du plan de travail. L'analyse s'exécute alors avec la configuration d'analyse par défaut.
   b. Dans la vue Explorateur :
      - Cliquez avec le bouton droit de la souris sur votre sélection et sélectionnez **Examiner le fichier** dans le menu. L'analyse s'exécute alors avec la configuration d'analyse par défaut.
      - Pour utiliser une autre configuration d'examen, cliquez avec le bouton droit de la souris sur la sélection, puis sélectionnez **Examiner le fichier avec** dans le menu. Sélectionnez la configuration d'examen que vous souhaitez utiliser ou, si vous souhaitez définir une autre configuration d'examen par défaut, choisissez l'action **Editer des configurations** (dans la vue Configuration d'examen, sélectionnez la configuration que vous souhaitez définir par défaut et cliquez sur **Sélectionner comme valeur par défaut**).

Nouvel examen du code

Procédure

Pour examiner à nouveau la cible en cours, sélectionnez **Examiner** > **Examiner à nouveau** dans le menu principal. La dernière configuration d'examen utilisée pour examiner l'élément (ou les éléments sélectionnés) sera réutilisée pour cet examen :

- Si la configuration d'examen par défaut a été utilisée pour l'examen précédent et qu'un nouvel examen par défaut a été défini, la nouvelle configuration d'examen par défaut sera utilisée pour l'examen.
- Si une configuration d'examen autre que celle par défaut a été utilisée pour l'examen précédent, elle sera utilisée pour cet examen. Si cette configuration d'examen a été modifiée et sauvegardée depuis l'examen précédent, la configuration d'examen modifiée sera utilisée.

Considérations relatives aux examens

Cette rubrique décrit les restrictions et les considérations qui peuvent avoir une incidence sur vos examens.

- «Général», à la page 88
- «macOS», à la page 88
- «Java», à la page 89

Général

Restriction : Lorsque vous examinez plusieurs applications ou projets, un noeud parent contenant des évaluations pour chaque élément analysé est créé dans la vue Mes évaluations. Les évaluations enfant individuelles ne peuvent pas être gérées dans ce cas (par exemple, les évaluations enfant ne peuvent pas être supprimées ni publiées individuellement). Lorsque plusieurs applications ou projets sont analysés en même temps, vous pouvez gérer les évaluations uniquement en tant que groupe (le noeud parent).

Important : Si vous travaillez avec un projet AppScan Source comportant des dépendances dans un environnement de développement (par exemple un projet IBM MobileFirst Platform), veillez à créer le projet dans l'environnement de développement avant de l'importer. Après avoir importé le projet, si vous modifiez des fichiers qu'il contient, pensez à le régénérer dans l'environnement de développement avant l'analyse dans AppScan Source (si vous omettez cette étape, les modifications apportées aux fichiers ne seront pas prises en compte par AppScan Source).

macOS

Vous pouvez examiner des projets Xcode iOS dans AppScan Source.

Pour analyser des projets Xcode comportant des dépendances, vous devez créer le projet en une seule fois dans Xcode pour créer les dépendances requises par le scanner AppScan Source. Par exemple, si vous travaillez sur un projet Xcode généré par IBM MobileFirst Platform, pour analyser l'environnement **iPhone** ou **iPad** ou un projet Xcode dans l'un de ces environnements, vous devrez construire le projet pour l'appareil iOS en Xcode. Vous pouvez effectuer cette opération depuis la ligne de commande :

```
xcodebuild -project <nom_rép_projet>.xcodeproj -configuration Release
```

Où `<nom_rép_projet>` correspond au chemin et au nom du fichier du projet Xcode.

Si le projet Xcode n'a pas été généré en premier, les types suivants d'erreur peuvent apparaître au cours de l'examen :

```
01/11/14 07:33:03 - Scanning /Users/smith/MobileFirst_Apps/
  wl_newapps/BasicHybridApp/apps/HybridApp/iphone/native/
  Classes/CDVMainViewController.m (1 of 3)
01/11/14 07:33:05 - In file included from /Users/smith/MobileFirst_Apps/
  wl_newapps/BasicHybridApp/apps/HybridApp/iphone/native/Classes/
  CDVMainViewController.m:14:
In file included from /Users/smith/MobileFirst_Apps/wl_newapps/
  BasicHybridApp/apps/HybridApp/iphone/native/Classes/
  CDVMainViewController.h:15:
 /Users/smith/MobileFirst_Apps/wl_newapps/BasicHybridApp/apps/HybridApp/
  iphone/native/MobileFirstSDK/include/MainViewController.h:35:9:
  fatal error: 'Cordova/CDVViewController.h' file not found
#import <Cordova/CDVViewController.h>
```

ou

```
2/06/14 15:19:43 - Scanning /Users/smith/MobileFirst_Apps/
  xcodeapps/WLMarkupTest-1.0-iphone/Classes/
  CDVMainViewController.m (1 of 3)
02/06/14 15:19:45 - In file included from /Users/smith/MobileFirst_Apps/
  xcodeapps/WLMarkupTest-1.0-iphone/Classes/CDVMainViewController.m:14:
In file included from /Users/smith/MobileFirst_Apps/xcodeapps/
  WLMarkupTest-1.0-iphone/Classes/CDVMainViewController.h:15:
/Users/smith/MobileFirst_Apps/xcodeapps/WLMarkupTest-1.0-iphone/
```

```
  MobileFirstSDK/include/MainViewController.h:41:63: error: expected ':'
- (BOOL) execute:(CDVInvokedUrlCommand*)command CDV_DEPRECATED
  (2.2, "Use direct method calls instead, this is now a no-op");
```

Java

Conseil : Si vous examinez Java et qu'il manque des dépendances dans votre projet Java, AppScan Source crée des traces en synthétisant les éléments que les dépendances auraient fournis. Cette synthèse ne reflète peut-être pas exactement les informations qui figurent dans les fichiers `.jar`. Pour limiter cette synthèse et par conséquent améliorer l'exactitude des constatations, vous pouvez spécifier les dépendances manquantes de la façon suivante :

1. Après l'examen, ouvrez `<data_dir>\logs\scanner_exceptions.log` (où `<rép_données>` est l'emplacement de vos données de programme AppScan Source, comme décrit dans «Installation et emplacements des fichiers de données utilisateur», à la page 292) pour vérifier si AppScan Source a signalé des dépendances manquantes.
2. Modifiez les propriétés du projet afin d'inclure les dépendances. Pour ce faire, suivez les instructions figurant dans la rubrique «Modification des propriétés d'une application et d'un projet», à la page 64, puis spécifiez et sauvegardez les dépendances dans l'onglet **Dépendances de projet JSP** ou **Dépendances de projet**.
3. Examinez à nouveau le projet.

Remarque : Par défaut, AppScan Source examine les fichiers Java et le bytecode Java en recherchant les dépendances manquantes ou les erreurs de compilation. Vous pouvez modifier ces paramètres de la façon suivante :

1. Ouvrez `<data_dir>\config\scan.ozsettings` dans un éditeur de texte.
2. Pour modifier le paramètre d'erreur de compilation, recherchez `compile_java_sources_with_errors` dans le fichier. Ce paramètre est similaire à ce qui suit :

   ```
   <Setting
     name="compile_java_sources_with_errors"
     value="true"
     default_value="true"
     type="bool"
     hidden="true"
     display_name="compile_java_sources_with_errors"
     description="Attempt to scan java code with compilation errors."
   />
   ```

3. Pour modifier le paramètre de dépendance manquante, recherchez `scan_java_bytecode_without_dependencies` dans le fichier. Ce paramètre est similaire à ce qui suit :

   ```
   <Setting
     name="scan_java_bytecode_without_dependencies"
     value="true"
     default_value="true"
     type="bool"
     hidden="true"
     display_name="scan_java_bytecode_without_dependencies"
     description="Scans Java bytecode even when some of
       the dependencies are missing by artificially
       synthesizing the unresolved symbols."
   />
   ```

4. Dans le paramètre, modifiez l'attribut `value`. Si l'attribut est défini sur la valeur `true`, ce paramètre sera activé. Si le paramètre d'erreur de compilation est défini sur la valeur `false`, AppScan Source ignorera le code Java présentant des

erreurs de compilation au cours des examens. Si le paramètre de dépendance manquante est défini sur la valeur `false`, AppScan Source n'examinera pas le bytecode Java si des dépendances sont manquantes.

5. Après avoir modifié ce paramètre, sauvegardez le fichier, puis démarrez ou redémarrez AppScan Source.

Gestion des configurations d'examen

Les configurations d'examen sont utilisées lors du lancement des examens. Dans une configuration d'examen, vous pouvez spécifier les règles source à utiliser lors de l'examen. Les paramètres définis dans une configuration d'examen permettent souvent d'obtenir de meilleurs résultats d'examen et la sauvegarde de ces paramètres peut faciliter l'examen et la rendre plus efficace et plus performante.

Pourquoi et quand exécuter cette tâche

Cette tâche décrit les étapes impliquées dans la gestion des configurations d'examen.

- «Création d'une configuration d'examen»
- «Modification d'une configuration d'examen», à la page 94
- «Suppression d'une configuration d'examen», à la page 94
- «Partage de configurations d'examen et utilisation des configurations d'examen», à la page 94
- «Définition de configurations d'examen en tant que configurations par défaut», à la page 95
- «Configurations d'examen intégrées», à la page 95

Les configurations d'examen sont gérées à partir de la vue «Vue Configuration d'examen», à la page 95. Pour ouvrir cette vue, sélectionnez **Vue** > **Configuration d'examen** dans la barre de menus principale ou sélectionnez l'action **Editer des configurations** dans la vue Explorateur.

Une fois que les configurations d'examen sont en place, vous pouvez les utiliser lors du lancement des examens dans AppScan Source for Analysis (pour plus d'informations, voir «Analyse du code source», à la page 85). Vous pouvez également utiliser les configurations d'examen lors du lancement des examens dans AppScan Source for Automation, dans AppScan Source for Development et dans l'interface de ligne de commande (CLI) d'AppScan Source.

Création d'une configuration d'examen

Procédure

1. Effectuez l'une des actions suivantes :
   a. Cliquez sur le bouton **Nouveau** de la vue Configuration.
   b. Sélectionnez une configuration existante dans la liste, puis cliquez sur **Dupliquer**. Une configuration d'examen est alors créée en fonction des paramètres de la configuration d'examen d'origine. Cette configuration peut alors être modifiée et sauvegardée en tant que nouvelle configuration.
2. Dans la section **Informations de base** de l'onglet **Général** :
   a. Entrez un nom unique pour la configuration dans la zone **Nom**. Notez que, dans une configuration d'examen, l'indication d'un nom unique est le seul paramètre obligatoire et tous les autres paramètres sont facultatifs.
   b. Facultatif : Entrez une description de la configuration d'examen.

3. Facultatif : Utilisez la section **Informations sur les filtres** de l'onglet **Général** pour définir les filtres de l'examen. Pour plus d'informations sur les filtres, voir «Triage avec filtres», à la page 121. Dans cette section, vous pouvez choisir un ou plusieurs filtres à appliquer à l'examen à chaque utilisation de la configuration d'examen. Lors de la sélection d'un filtre, vous pouvez choisir un filtre prédéfini par AppScan Source ou un filtre partagé ou un que vous avez créé. Dans cette section :
   a. Cliquez sur **Ajouter** et, dans la boîte de dialogue Sélection de filtre, choisissez le ou les filtres que vous voulez ajouter. Lorsqu'un filtre est sélectionné, ses caractéristiques apparaissent en lecture seule dans la partie droite de la boîte de dialogue. Cliquez sur **OK** pour ajourer le ou les filtres à la configuration d'examen.

      Remarque :

      - Pour appliquer l'inverse du filtre à la configuration d'examen, cochez la case **Inverser le filtre** avant de cliquer sur **OK**.
      - Lorsque vous vous trouvez dans la boîte de dialogue Sélection de filtre, vous pouvez sélectionner plusieurs filtres à ajouter. Si la case à cocher **Inverser le filtre** est sélectionnée lorsque vous faites cela, l'inverse de tous les filtres sélectionnés sera ajouté à la configuration d'examen.

      Après que vous avez quitté la boîte de dialogue Sélection de filtre, le ou les filtres apparaissent dans la liste et la colonne **Inversé** indique si le filtre est inversé.
   b. Pour supprimer des filtres que vous avez ajoutés, sélectionnez-les et cliquez sur **Supprimer**.
   c. Les filtres d'exclusion contiennent des règles en fonction desquelles des types de vulnérabilité, des interfaces de programme d'application (API), des fichiers, des répertoires, ou des règles de trace sont supprimés des résultats. Si vous incluez plusieurs filtres d'exclusion dans une configuration d'examen, il se peut qu'ils entrent en conflit et que ceci affecte les résultats. Par exemple, en supposant ces deux filtres :
      - Le filtre 1 supprime tous les résultats sur le type de vulnérabilité `Validation.EncodingRequired`. Il n'est pas inversé et donc ces résultats sont exclus de l'évaluation.
      - Le filtre 2 supprime tous les résultats sur le type de vulnérabilité `Validation.Required`. Il n'est pas inversé et donc ces résultats sont exclus de l'évaluation.

      Si ces deux filtres sont utilisés dans une configuration d'examen, ils se neutralisent mutuellement par défaut. Le filtre 1 exclura les constatations `Validation.EncodingRequired`, mais il inclura les constatations `Validation.Required`. Le filtre 2 exclura les constatations `Validation.Required`, mais il inclura les constatations `Validation.EncodingRequired`. Le résultat final sera que toutes les constatations `Validation.EncodingRequired` et `Validation.Required` seront incluses.

      Pour exclure les constatations de *n'importe* quel filtre d'exclusion spécifié, sélectionnez **Faire correspondre les filtres d'exclusion non inversés**. D'après l'exemple ci-dessus, si cette case est cochée, toutes les constatations `Validation.EncodingRequired` et `Validation.Required` seront exclues de l'évaluation.
4. Facultatif : Utilisez la section **Analyse de flux corrompus** de l'onglet **Analyse de flux corrompus** pour activer l'analyse de flux corrompus. **Analyse de flux**

corrompus est sélectionné par défaut et il s'agit du principal type d'analyse effectuée par AppScan Source. Lorsque vous lancez un examen, l'analyse de flux corrompus produit des traces de flux de données qui vous permettent de mieux déterminer les vulnérabilités. Vous pouvez définir la **Portée** de l'analyse comme suit :

- Portée **Application** : l'analyse de flux corrompus sera effectuée entre les projets au sein d'une application et les fichiers au sein d'un projet.
- Portée du **Projet** : l'analyse de flux corrompus sera effectuée entre les fichiers au sein d'un projet.
- Portée **Fichier** : l'analyse de flux corrompus sera effectuée sur chaque fichier séparément.

Remarque : Les paramètres de l'onglet **Analyse de flux corrompus** ne s'appliquent pas lors de l'examen du langage JavaScript.

5. Facultatif : La section **Règles d'examen** de l'onglet **Analyse de flux corrompus** vous permet de spécifier les règles d'examen qui seront utilisées pour l'examen (pour plus d'informations, voir «Onglet Analyse de flux corrompus», à la page 97). Dans cette section, vous pouvez choisir d'effectuer l'examen avec des ensembles de règles source sélectionnés ou sélectionner des propriétés de règles individuelles à utiliser lors de l'examen :
   a. Par défaut, cette section vous permet de choisir les ensembles de règles à appliquer. Sélectionnez une ou plusieurs des cases à cocher associées aux ensembles de règles disponibles.
   b. Pour choisir des propriétés de règles individuelles au lieu d'ensembles de règles, cliquez sur **Annuler les ensembles de règles sélectionnés et me laisser sélectionner des propriétés de règles individuelles**. Ceci a pour effet d'ouvrir la boîte de dialogue Sélection des propriétés de règle qui permet de sélectionner des propriétés de règles individuelles. Si cette boîte de dialogue est renseignée, les ensembles de règles sélectionnés sont annulés. Les règles d'examen qui possèdent les propriétés de règle sélectionnées seront utilisées pour l'examen.

   Si vous avez choisi des propriétés de règles individuelles pour l'examen et que vous souhaitez ensuite sélectionner des ensembles de règles, cliquez sur **Annuler les propriétés de règle sélectionnées et permettre la sélection par ensemble de règles**. Cette option permet d'annuler les propriétés de règle sélectionnées dans la boîte de dialogue Sélection des propriétés de règle et de sélectionner à la place des ensembles de règles.

   Remarque :
   - Lorsque vous sélectionnez des propriétés de règles individuelles, les éléments sélectionnés s'appliquent aux propriétés des sources et non des collecteurs. Cela signifie que vous limitez la surface d'attaque aux sources possédant les propriétés sélectionnées seulement. Vos résultats peuvent présenter des vulnérabilités qui ne correspondent pas aux propriétés sélectionnées, car les types de vulnérabilité reposent sur le collecteur et non sur la source.
   - Les paramètres de l'onglet **Analyse de flux corrompus** ne s'appliquent pas lors de l'examen du langage JavaScript.
6. Facultatif : La section **Paramètres avancés** de l'onglet **Analyse de flux corrompus** est uniquement destinée aux utilisateurs avancés. Elle contient un certain nombre de paramètres qui peuvent améliorer les résultats d'examen. Une infobulle décrit chaque paramètre de cette section.

Remarque : Les paramètres de l'onglet **Analyse de flux corrompus** ne s'appliquent pas lors de l'examen du langage JavaScript.

7. Facultatif : Les paramètres de l'onglet **Analyse de schémas** vous permettent d'activer et de définir des règles pour l'examen basé sur des schémas. L'examen basé sur des schémas est un examen de votre code source basée sur des critères de recherche personnalisés. Pour plus d'informations, voir «Personnalisation à l'aide de règles basées sur des schémas», à la page 209. Pour activer l'examen basé sur des schémas, cochez la case **Analyse de schéma**. Lorsque vous faites cela, les sections **Ensembles de règles de schémas** et **Règles de schémas** deviennent actives :
   a. Pour ajouter un ensemble de règles, cliquez sur **Ajouter** dans la section **Ensembles de règles de schémas**. Ceci a pour effet d'ouvrir la boîte de dialogue Ajouter des ensembles de règles de schémas qui vous permet de sélectionner un ou plusieurs ensembles de règles. Lorsque vous sélectionnez un ensemble de règles, les règles qu'il contient sont affichés dans la partie droite de la boîte de dialogue, et les types de projet auxquels s'applique l'ensemble de règles sont répertoriés dans la zone **Types de projets**. Cliquez sur **OK** pour ajouter les ensembles de règles sélectionnés.
   b. Pour ajouter une règle, cliquez sur **Ajouter** dans la section **Règles de schéma**. Ceci a pour effet d'ouvrir la boîte de dialogue Ajouter des règles de schéma, ce qui vous permet de sélectionner une ou plusieurs règles. Vous pouvez également cliquer sur **Créer une règle** afin de créer une nouvelle règle (voir «Création d'une règle de schémas», à la page 213). Si vous créez une nouvelle règle, elle sera ajoutée à la liste et sélectionnée. Après avoir sélectionné ou créé des règles, cliquez sur **OK** pour les ajouter à la configuration d'examen.

      Conseil : Dans la boîte de dialogue Ajouter des règles de schéma, l'infobulle d'aide indique les expressions qui sont utilisées pour chaque règle.

      Remarque :

      - Lorsque vous ajoutez une ensemble de règles, les règles de ce dernier sont filtrées en dehors de boîte de dialogue Ajouter des règles de schéma.
      - Si vous ajoutez une règle puis un ensemble de règles qui inclut également cette règle, la section Règles de schéma répertorie la règle en indiquant qu'elle est incluse dans un ensemble de règles. Cette règle étant déjà incluse dans un ensemble de règles, si vous essayez de supprimer la règle individuelle, elle ne sera supprimée que de la section Règles de schéma et non de la configuration d'examen. Pour supprimer la règle de la configuration d'examen, supprimez l'ensemble de règles ou modifiez-le de sorte qu'il n'inclue pas la règle.
   c. Les ensembles de règles ou les règles que vous ajoutez peuvent être supprimés à l'aide du bouton **Supprimer** ou en cliquant sur le bouton droit de la souris et en sélectionnant **Supprimer**. Vous pouvez aussi sélectionner plusieurs règles et ensembles de règles lors de l'utilisation de cette action.

      Remarque : Si une configuration d'examen inclut des règles ou des ensembles de règles par la suite retirés de la base de données de vulnérabilités, ces règles ou ensembles de règles apparaîtront avec un message indiquant qu'ils n'existent pas lors de la prochaine ouverture de la configuration d'examen. Les actions **Supprimer** ne seront pas disponibles

pour ces règles ou ensembles de règles. En revanche, ceux-ci seront automatiquement supprimés la prochaine fois que vous sauvegarderez la configuration d'examen.

8. Une fois que tous les paramètres ont été définis dans la configuration d'examen, cliquez sur **Sauvegarder**.

Modification d'une configuration d'examen

Procédure

1. Dans la vue Configuration d'examen, sélectionnez la configuration d'examen à modifier.

   Remarque : Pour partager des configurations d'examen ou modifier ou supprimer une configuration d'examen partagée, vous devez disposer de l'autorisation **Gérer les configurations partagées**. Pour plus d'informations sur la définition des autorisations, voir le manuel *IBM Security AppScan Source - Guide d'installation et d'administration*.

   Remarque : Vous ne pouvez pas modifier «Configurations d'examen intégrées», à la page 95.

2. Une fois la configuration d'examen modifiée, cliquez sur **Sauvegarder**.

Suppression d'une configuration d'examen

Procédure

1. Dans la vue Configuration d'examen, sélectionnez la configuration d'examen à supprimer.

   Remarque : Vous ne pouvez pas supprimer «Configurations d'examen intégrées», à la page 95.

2. Cliquez sur **Supprimer**.

Partage de configurations d'examen et utilisation des configurations d'examen

Pourquoi et quand exécuter cette tâche

Les configurations d'examen peuvent être sauvegardées sur base de données AppScan Source afin d'être partagées avec d'autres. Pour partager une configuration d'examen avec d'autres, cliquez sur **Partager**.

Remarque : Pour partager des configurations d'examen ou modifier ou supprimer une configuration d'examen partagée, vous devez disposer de l'autorisation **Gérer les configurations partagées**. Pour plus d'informations sur la définition des autorisations, voir le manuel *IBM Security AppScan Source - Guide d'installation et d'administration*.

Les configurations d'examen qui ont été partagées par d'autres s'affichent dans la liste des configurations d'examen.

Remarque :

- Une fois qu'une configuration d'examen a été partagée, vous ne pouvez pas supprimer le partage. Vous pouvez par contre effectuer l'une des tâches suivantes :
  - Supprimer la configuration d'examen partagée. Elle est alors supprimée sur le serveur.

– Dupliquer la configuration d'examen partagée, puis la supprimer. La duplication de la configuration d'examen crée une copie locale identique de cette dernière.

- Si vous partagez une configuration d'examen contenant des filtres déjà partagés, l'action de partage s'effectuera sans invite. Si toutefois vous partagez une configuration d'examen contenant des filtres que vous avez créés localement, une invite vous indiquera que les filtres seront également partagés. Vous aurez la possibilité d'annuler l'action de partage de la configuration d'examen si vous ne souhaitez pas partager les filtres locaux.
- Vous ne pouvez pas modifier et sauvegarder des configurations d'examen partagées en ajoutant des filtres locaux. Pour ajouter ces filtres à une configuration d'examen partagée, partagez les filtres puis ajoutez-les à la configuration d'examen partagée.
- Si vous disposez de l'autorisation **Gérer les configurations partagées** mais pas de l'autorisation **Gérer les filtres partagés**, vous ne pouvez pas partager une configuration d'examen contenant des filtres locaux.

Définition de configurations d'examen en tant que configurations par défaut

Pourquoi et quand exécuter cette tâche

Vous pouvez définir n'importe quelle configuration d'examen comme configuration d'examen par défaut, qu'elle soit locale, intégrée ou partagée. Si vous définissez une configuration d'examen partagée comme configuration par défaut, le paramétrage est uniquement local et n'affecte pas les autres utilisateurs. On utilise toujours une configuration d'examen lors d'un examen. Si vous définissez une configuration d'examen par défaut et que vous la supprimez, la configuration d'examen intégrée **Examen normal** sera utilisée en mode silencieux lors de l'examen.

Pour connaître la façon dont est utilisée la configuration par défaut, voir «Analyse du code source», à la page 85.

Procédure

1. Dans la vue Configuration d'examen, sélectionnez la configuration d'examen à définir comme configuration par défaut.
2. Cliquez sur **Sélectionner comme valeur par défaut**.

Configurations d'examen intégrées

Pourquoi et quand exécuter cette tâche

AppScan Source fournit des configurations d'examen intégrées. Elles ne peuvent être ni modifiées ni supprimées. Lorsque vous les sélectionnez dans la liste, vous pouvez les dupliquer ou afficher leurs paramètres.

Vue Configuration d'examen

La vue Configuration d'examen vous permet de créer des configurations que vous pouvez ensuite utiliser lors du lancement des examens. Vous pouvez aussi utiliser cette vue pour définir une configuration d'examen par défaut. Dans une configuration d'examen, vous pouvez spécifier les règles source à utiliser lors de l'examen et inclure de nombreux paramètres d'examen. Les paramètres définis dans une configuration d'examen permettent souvent d'obtenir de meilleurs résultats d'examen et la sauvegarde de ces paramètres peut faciliter l'examen et le rendre plus efficace et plus performant.

La vue Configuration d'examen comporte les sections principales suivantes :

- «Gestion de la configuration d'examen»
- «Onglet Général»
- «Onglet Analyse de flux corrompus», à la page 97
- «Onglet Analyse de schéma», à la page 98

Gestion de la configuration d'examen

Cette section permet de sélectionner, d'ajouter, de supprimer, de sauvegarder et de partager des configurations d'examen, ainsi que de définir des configurations d'examen par défaut.

- Pour créer une configuration d'examen, cliquez sur **Nouveau**. Une fois les paramètres de configuration d'examen définis, cliquez sur **Sauvegarde** pour enregistrer les modifications. Pour définir la configuration d'examen comme configuration par défaut, cliquez sur **Sélectionner comme valeur par défaut** après l'avoir sauvegardée. Pour connaître la façon dont est utilisée la configuration par défaut, voir «Analyse du code source», à la page 85.
- Pour utiliser une configuration d'examen existante, sélectionnez-la dans la liste :
  - Si vous modifiez les paramètres de configuration d'examen, cliquez sur **Sauvegarde** pour enregistrer les modifications (les modifications non souhaitées peuvent être supprimées en basculant vers une autre configuration d'examen et en cliquant sur **Supprimer**).
  - Pour supprimer la configuration d'examen sélectionnée, cliquez sur **Supprimer**.
  - Pour dupliquer la configuration d'examen, cliquez sur **Dupliquer**. Une configuration d'examen est alors créée en fonction des paramètres de la configuration d'examen d'origine.
  - Pour définir la configuration d'examen comme configuration par défaut, cliquez sur **Sélectionner comme valeur par défaut**. Pour connaître la façon dont est utilisée la configuration par défaut, voir «Analyse du code source», à la page 85.
  - Pour partager une configuration d'examen avec d'autres, cliquez sur **Partager**. Cette opération sauvegarde la configuration d'examen sur le serveur base de données AppScan Source.

    Remarque : Pour partager des configurations d'examen ou modifier ou supprimer une configuration d'examen partagée, vous devez disposer de l'autorisation **Gérer les configurations partagées**. Pour plus d'informations sur la définition des autorisations, voir le manuel *IBM Security AppScan Source - Guide d'installation et d'administration*.

Remarque : AppScan Source fournit des configurations d'examen intégrées. Elles ne peuvent être ni modifiées ni supprimées. Lorsque vous les sélectionnez dans la liste, vous pouvez les dupliquer ou afficher leurs paramètres.

Onglet Général

Informations de base

Cette section vous permet de nommer des configurations d'examen et de fournir une description pour chacune.

Filtres

Dans cette section, vous pouvez choisir un ou plusieurs filtres à appliquer à l'examen à chaque utilisation de la configuration d'examen. Lors de la sélection d'un filtre, vous pouvez choisir un filtre prédéfini par AppScan Source ou un filtre partagé ou un que vous avez créé. Voir «Gestion des configurations d'examen», à la page 90 pour plus de détails.

Onglet Analyse de flux corrompus

Analyse de flux corrompus

Activez et définissez la portée de l'analyse de flux corrompus.

Règles d'examen

Cette section permet de déterminer les règles source utilisées pour l'examen.

Une source est une entrée du programme, telle qu'un fichier, une requête de servlet, une saisie depuis la console ou un socket. En excluant certaines règles source, vous pouvez accélérer l'examen et éviter la détection des vulnérabilités provenant des entrées sans intérêt.

Les règles sont balisées à l'aide de propriétés de règle qui indiquent qu'elles sont liées à une vulnérabilité, un mécanisme, un attribut ou une technologie spécifique. Ces propriétés sont regroupées en ensembles de règles qui correspondent à un ensemble commun de règles connexes. Vous pouvez limiter les règles source incluses dans l'examen en spécifiant des ensembles de règles ou des propriétés de règles individuelles.

- Sélectionnez un ou plusieurs types de vulnérabilité (les vulnérabilités sont organisées par type dans les ensembles de règles) à inclure dans l'examen :
  - **Tout** : si cette option est sélectionnée, les vulnérabilités provenant de toutes les sources d'entrée prises en charge seront détectées.
  - **Entrée utilisateur** : si cette option est sélectionnée, les vulnérabilités provenant des entrées de l'utilisateur final seront détectées.
  - **Applications Web** : si cette option est sélectionnée, les vulnérabilités provenant des risques des applications Web seront détectées.
  - **Consignation et traitement des erreurs** : si cette option est sélectionnée, les vulnérabilités provenant de la consignation et du traitement des erreurs seront détectées.
  - **Environnement** : si cette option est sélectionnée, les vulnérabilités provenant des fichiers de configuration, des fichiers d'environnement système et des fichiers de propriété seront détectées.
  - **Systèmes externes** : si cette option est sélectionnée, les vulnérabilités provenant des entités externes seront détectées.
  - **Magasin de données** : si cette option est sélectionnée, les vulnérabilités provenant des magasins de données (tels que les bases de données et les caches) seront détectées.
  - **Données inhabituelles** : si cette option est sélectionnée, les vulnérabilités provenant des routines qui ne font normalement pas partie d'une application de production seront détectées.
  - **Système de fichiers** : si cette option est sélectionnée, les vulnérabilités provenant des systèmes de fichiers seront détectées.
  - **Données sensibles** : si cette option est sélectionnée, les vulnérabilités provenant des données sensibles seront détectées.

Une infobulle décrit chaque ensemble de règles de cette section.

- Sélectionnez les propriétés de règles d'examen individuelles à inclure dans l'examen : cliquez sur **Annuler les ensembles de règles sélectionnés et me laisser sélectionner des propriétés de règles individuelles**. Ceci a pour effet d'ouvrir la boîte de dialogue Sélection des propriétés de règle qui permet de sélectionner des propriétés de règles individuelles. Si cette boîte de dialogue est renseignée, les ensembles de règles sélectionnés sont annulés. Les règles d'examen qui possèdent les propriétés de règle sélectionnées seront utilisées pour l'examen.

Paramètres avancés

Cette section est uniquement destinée aux utilisateurs avancés. Elle contient un certain nombre de paramètres qui peuvent améliorer les résultats d'examen. Une infobulle décrit chaque paramètre de cette section.

Onglet Analyse de schéma

analyse de schéma

Utilisez cette section pour activer l'examen basé sur des schémas lors de l'utilisation de la configuration d'examen. L'examen basé sur des schémas est un examen de votre code source basée sur des critères de recherche personnalisés.

Ensembles de règles de schémas et **Règles de schéma**

Utilisez ces sections pour ajouter des règles et des ensembles de règles à utiliser lors de l'analyse de schéma. Pour plus d'informations, voir «Personnalisation à l'aide de règles basées sur des schémas», à la page 209 et «Gestion des configurations d'examen», à la page 90.

Exclusion d'un fichier dans l'examen

Avant de commencer

Remarque : Si l'application est un espace de travail Eclipse, vous ne pouvez pas exclure des fichiers des examens.

Procédure

1. Depuis la vue Explorateur, sélectionnez le(s) fichier(s) à éliminer de l'examen.
2. Cliquez avec le bouton droit de la souris sur la sélection et cliquez sur **Exclure des examens** dans le menu.

Résultats

Lorsque la vue Propriétés est ouverte pour le projet contenant le fichier, l'onglet **Sources** de la vue répertorie les fichiers du projet, y compris les fichiers exclus.

Les fichiers de projet sont affichés sous l'icône **Racine source**. Les fichiers qui sont exclus de l'examen sont accompagnés d'une icône de fichier rouge (si vous faites un clic droit sur un fichier exclus, l'option **Exclure** de son menu est désactivée et l'option **Inclure** est activée). Pour exclure un fichier inclus, faites un clic droit dessus et sélectionnez **Exclure** dans le menu. Pour inclure un fichier exclus, faites un clic droit dessus et sélectionnez **Inclure** dans le menu.

Annulation ou arrêt d'un examen

Bien qu'il soit possible d'annuler un examen en cours, cette opération provoque la perte de toutes les données de l'examen. Vous pouvez plutôt arrêter un examen pour l'interrompre et générer une évaluation avec les résultats obtenus à ce stade.

Annulation ou arrêt d'un examen dans AppScan Source for Analysis

Pour annuler un examen en cours, sélectionnez **Examen** > **Annuler l'examen** ou **Examen** > **Arrêter l'examen** dans le menu principal.

Annuler l'examen met fin à l'examen et ne génère aucun résultat. **Arrêter l'examen** interrompt l'examen et renvoie une évaluation avec les résultats produits jusqu'à ce stade.

Annulation ou arrêt d'un examen dans AppScan Source for Development (plug-in Eclipse)

Lorsque l'examen est en cours :

- Pour annuler l'examen, choisissez **Analyse de sécurité** > **Examen** > **Annuler l'examen** dans le menu principal. L'examen prend fin et ne génère aucun résultat, et les messages de diagnostic d'annulation apparaissent dans la console Eclipse.
- Pour arrêter l'examen, choisissez **Analyse de sécurité** > **Examen** > **Arrêter l'examen** dans le menu principal. L'examen prend fin et produit une évaluation des résultats qui ont été collectés jusqu'au moment où l'action d'arrêt a été lancée.

Remarque : AppScan Source for Development (plug-in Eclipse) est pris en charge sous Windows et Linux seulement.

Annulation d'un examen dans AppScan Source for Development (plug-in Microsoft Visual Studio)

Pendant l'exécution de l'examen, sélectionnez **IBM Security AppScan Source** > **Examen** > **Annuler l'examen** dans le menu principal. L'examen prend fin et ne génère aucun résultat.

Remarque : Le plug-in Microsoft Visual Studio d'AppScan Source for Development est pris en charge sous Windows seulement.

Gestion de Mes évaluations

La vue Mes évaluations contient une liste d'évaluations (évaluation actuellement ouverte, ainsi que les évaluations que vous avez enregistrées). Depuis cette vue, vous pouvez ouvrir, supprimer, sauvegarder, renommer ou comparer des évaluations. Lorsqu'un examen se termine ou que vous ouvrez une évaluation, celle-ci apparaît dans la vue Mes évaluations. Cette vue contient un tableau des évaluations ouvertes ou sauvegardées et identifie les évaluations publiées ou modifiées. La suppression d'une évaluation de cette vue (sans qu'elle soit sauvegardée ni publiée) est définitive.

Pour plus d'informations sur la vue Mes évaluations, voir «Vue Mes évaluations», à la page 271.

Restriction : Lorsque vous examinez plusieurs applications ou projets, un noeud parent contenant des évaluations pour chaque élément analysé est créé dans la vue Mes évaluations. Les évaluations enfant individuelles ne peuvent pas être gérées dans ce cas (par exemple, les évaluations enfant ne peuvent pas être supprimées ni publiées individuellement). Lorsque plusieurs applications ou projets sont analysés en même temps, vous pouvez gérer les évaluations uniquement en tant que groupe (le noeud parent).

Conseil : Vous ne pouvez ouvrir en même temps que les résultats d'examen relevant de la même application. Pour afficher les résultats d'un examen multi-applications ou multi-projets, vous devez développer l'arborescence de la vue Mes évaluations et cliquez deux fois sur l'évaluation que vous désirez ouvrir.

Soumission d'évaluations AppScan Source au cloud pour analyse

Si vous êtes abonné à IBM Application Security on Cloud sur IBM Cloud Marketplace ou à Application Security on Cloud for Bluemix, vous pouvez soumettre des évaluations AppScan Source pour analyse, via ce canal. Les évaluations d'AppScan Source version 9.0 ou des versions ultérieures sont prises en charge et le nombre d'analyses que vous pouvez soumettre dépend de votre abonnement à Application Security on Cloud.

Pourquoi et quand exécuter cette tâche

Lorsque vous utilisez la fonction d'analyse statique du service Application Security on Cloud, vous pouvez générer des rapports d'analyse de sécurité utilisant la technologie IFA (Intelligent Finding Analytics). La technologie IFA est une technologie d'apprentissage automatique puissante, qui effectue une bonne partie du travail d'analyse des besoins à votre place, entre autres, en filtrant et en éliminant les faux positifs et en regroupant les résultats qui peuvent être corrigés par un correctif dans un point de code. Pour en savoir plus sur la technologie IFA, voir cet article.

Si vous utilisez AppScan Source version 9.0 ou une version ultérieure et disposez d'un abonnement à Application Security on Cloud, vous pouvez bénéficier de cette technologie en téléchargeant votre évaluation AppScan Source vers Application Security on Cloud. En retour, vous recevrez une nouvelle évaluation qui a été triée par cette technologie. Cette évaluation peut se présenter sous la forme d'un rapport HTML ou d'une évaluation qui peut être ouverte dans votre produit AppScan Source.

Si vous possédez un abonnement à Application Security on Cloud, il est possible que ayez un nombre limité d'examens par mois. Voir http://www.ibm.com/support/knowledgecenter/SSYJJF_1.0.0/ApplicationSecurityonCloud/src_managing_assessments_cloud.html pour obtenir des informations supplémentaires sur les autorisations relatives aux examens et aux examens simultanés.

Remarque : Si vous examinez une évaluation AppScan Source avec une version d'essai gratuite d'Application Security on Cloud, vous pouvez télécharger un rapport HTML complet, en plus du fichier d'évaluation AppScan Source trié par l'IFA. Pour tous les autres types d'examen, vous pouvez uniquement télécharger un rapport récapitulatif si vous disposez d'une version d'essai gratuite.

Procédure

1. **Ignorez cette étape si vous utilisez déjà Application Security on Cloud pour l'analyse statique :**
   a. Si vous ne possédez pas d'abonnement à Application Security on Cloud, vous pouvez vous en procurer un de la manière suivante :
      - **IBM Cloud Marketplace :** Accédez à https://appscan.ibmcloud.com/serviceui/home et connectez-vous avec votre ID IBM. Si vous ne possédez pas d'ID IBM, utilisez le lien qui vous permet d'en créer un. Inscrivez-vous ensuite pour obtenir une version d'essai gratuite ou un abonnement payant à l'aide des liens du service.
      - **IBM Bluemix :** Accédez à https://console.ng.bluemix.net/ puis sélectionnez le bouton **INSCRIPTION** et complétez le formulaire d'inscription de Bluemix. Créez ensuite une instance de service Application Security on Cloud for Bluemix.

   b. **IBM Cloud Marketplace uniquement :** Dans le service Application Security on Cloud, créez une application (voir http://www.ibm.com/support/knowledgecenter/SSYJJF_1.0.0/ApplicationSecurityonCloud/ent_create_application.html) puis cliquez sur **Créer un examen**.
   c. Dans l'écran **Quel type d'application analysez-vous aujourd'hui ?**, sélectionnez **Bureau** ou **Web** > **Statique**.
   d. Si vous n'avez pas déjà téléchargé et configuré l'utilitaire client Static Analyzer, faites-le maintenant. Voir http://www.ibm.com/support/knowledgecenter/SSYJJF_1.0.0/ApplicationSecurityonCloud/src_utility_install.html pour de plus amples informations.
2. Générez une évaluation (fichier `.ozasmt`) dans le produit AppScan Source ou avec l'outil de votre choix. Les versions 9.0 et ultérieures sont prises en charge.
3. Utilisez l'interface de ligne de commande (interface CLI) de l'utilitaire client pour générer un fichier de représentation intermédiaire (IRX ou `.irx`) pour l'évaluation (fichier `.ozasmt`) :
   a. Après avoir extrait l'utilitaire client vers une unité locale, ajoutez l'emplacement de son répertoire `\bin` dans votre variable d'environnement `PATH`. Si vous n'effectuez pas cette opération, toutes les commandes CLI de l'utilitaire client auront besoin d'être qualifiées à l'aide du répertoire `\bin` à chaque fois que la commande sera émise. Voir http://www.ibm.com/support/knowledgecenter/SSYJJF_1.0.0/ApplicationSecurityonCloud/src_irx_gen_cli.html pour de plus amples informations.
   b. Emettez la commande suivante sur Windows :

      ```
      appscan package -d <save_path> -f <assessment_file> -n <file_name>
      ```

      ou la commande suivante sur Linux :

      ```
      appscan.sh package -d <save_path> -f <assessment_file> -n <file_name>
      ```

      Les arguments de commande sont facultatifs :
      - `-d` : spécifiez `-d <save_path>`, où `<save_path>` est le répertoire dans lequel vous souhaitez sauvegarder le fichier IRX.
      - `-f` : spécifiez `-f <assessment_file>`, où `<assessment_file>` est le fichier `.ozasmt` à conditionner pour l'examen. Si le fichier `<assessment_file>` ne se trouve pas dans le répertoire de travail, utilisez cette option pour spécifier le chemin d'accès et le nom du fichier d'évaluation.

        Remarque : Cette option est uniquement requise si l'une des deux affirmations suivantes est vraie :

- Vous entrez la commande depuis un répertoire qui contient plusieurs fichiers d'évaluation. Si le répertoire contient un seul fichier d'évaluation, ce fichier est conditionné si l'option `-f` n'est pas utilisée.
- Vous émettez la commande depuis un répertoire qui ne contient pas de fichier d'évaluation. Dans ce cas, vous devez utiliser l'option `-f` pour spécifier le chemin d'accès et le nom du fichier d'évaluation à conditionner.

• `-n` : spécifiez `-n <file_name>`, où `<file_name>` est le nom du fichier IRX. Vous pouvez spécifier le nom de fichier avec ou sans l'extension de fichier `.irx`. Si vous le spécifiez sans l'extension, celle-ci est ajoutée automatiquement lorsque le fichier est généré.

Vous trouverez des informations supplémentaires sur la commande `package`, notamment des exemples d'utilisation sous Commandes de configuration (Windows) ou Commandes de configuration (Linux).

4. Utilisez la commande CLI `queue_analysis` pour télécharger le fichier IRX
   a. Connectez-vous au service à partir de l'interface de ligne de commande. La méthode utilisée est différente dans IBM Cloud Marketplace et IBM Bluemix. Vous trouverez des informations détaillées sur l'authentification auprès du service dans l'interface CLI sous Commandes d'authentification (Windows) ou Commandes d'authentification (Linux).

   • **IBM Cloud Marketplace:**

   Emettez la commande suivante sur Windows :

   ```
   appscan scx_login -P <password> -u <user_name> -persist
   ```

   ou la commande suivante sur Linux :

   ```
   appscan.sh scx_login -P <password> -u <user_name> -persist
   ```

   Les arguments suivants sont obligatoires :

   – `-P` : spécifiez `-P <password>`, où `<password>` est le mot de passe spécifié lors de l'enregistrement au service Application Security on Cloud.

   – `-u` : spécifiez `-u <user_name>`, où `<user_name>` est l'adresse électronique spécifiée lors de l'enregistrement au service Application Security on Cloud.

   L'argument suivant est facultatif :

   – `-persist` : tenter une nouvelle authentification automatique auprès du service lorsque le fichier jeton de connexion arrive à expiration.

   • **IBM Bluemix:**

   Emettez la commande suivante sur Windows :

   ```
   appscan login -P <password> -u <user_name> -persist
   ```

   ou la commande suivante sur Linux :

   ```
   appscan.sh login -P <password> -u <user_name> -persist
   ```

   Les arguments suivants sont obligatoires :

   – `-P` : entrez `-P <password>`, où `<password>` est le mot de passe indiqué dans les données d'identification du service.

   – `-u` : entrez `-u <user_name>`, où `<user_name>` est l'ID de liaison indiqué dans les données d'identification du service.

   Pour déterminer les données d'identification du service Bluemix, sélectionnez **Données d'identification pour le service** dans le panneau de navigation gauche du tableau de bord du service. Voir Utilisation des services Bluemix avec des applications externes.

   L'argument suivant est facultatif :

– `-persist` : tenter une nouvelle authentification automatique auprès du service lorsque le fichier jeton de connexion arrive à expiration.

b. Téléchargez le fichier IRX à l'aide de la commande `queue_analysis` :

- Emettez la commande suivante sur Windows :

  ```
  appscan queue_analysis -a <app_id> -f <irx_file> -n <scan_name>
  ```

  ou la commande suivante sur Linux :

  ```
  appscan.sh queue_analysis -a <app_id> -f <irx_file> -n <scan_name>
  ```

  Les arguments suivants sont obligatoires :

  – `-f` : spécifiez `-f <irx_file>`, où `<irx_file>` est le fichier IRX file à soumettre à l'examen. Si le fichier IRX ne se trouve pas dans le répertoire de travail, utilisez cette option pour spécifier le chemin et le nom du fichier IRX.

    Remarque : Cette option est uniquement requise si l'une des deux affirmations suivantes est vraie :

    - Vous émettez la commande depuis un répertoire qui contient plusieurs fichiers IRX. Si le répertoire ne contient qu'un fichier IRX, ce fichier est soumis si l'option `-f` n'est pas utilisée.
    - Vous émettez la commande depuis un répertoire qui ne contient pas de fichier IRX. Dans ce cas, l'option `-f` doit être utilisée pour spécifier le chemin et le nom du fichier IRX à soumettre.

  – `-n` : spécifiez `-n <scan_name>`, où `<scan_name>` est le nom de l'examen qui est réalisé dans le cloud.

  – `-a` **(IBM Cloud Marketplace uniquement)** : si vous êtes connecté au service Application Security on Cloud sur IBM Cloud Marketplace, les fichiers IRX que vous envoyez vers le cloud doivent être associés à une application Application Security on Cloud existante. Avec cette option, spécifiez `-a <app_id>`, où `<app_id>` est l'ID de l'application à associer. Pour déterminer l'ID, utilisez la commande `list_apps`.

- Lorsque la commande `queue_analysis` termine, un ID s'affiche pour le travail d'analyse. Si vous souhaitez recevoir le rapport d'analyse d'Application Security on Cloud via l'interface CLI, vous devrez inclure cet ID de travail dans la commande `get_result` et noter l'ID. Si vous utilisez l'interface CLI pour recevoir le rapport d'analyse, vous aurez l'option de recevoir un fichier archive (`.zip`) comprenant un fichier `.ozasmt` pour pouvoir ouvrir le rapport d'analyse dans AppScan Source. Si vous souhaitez uniquement obtenir un rapport HTML, vous pouvez utiliser l'interface CLI ou le client Web d'Application Security on Cloud pour télécharger le rapport.

Vous trouverez des détails concernant l'utilisation de la commande `queue_analysis` sous Commandes d'analyse (Windows) ou Commandes d'analyse (Linux).

5. Une fois l'analyse terminée, vous recevrez un courrier électronique si vous avez téléchargé le fichier IRX à l'aide de l'interface CLI ou si vous avez coché la case **Email me when the scan is complete** dans le client Web d'Application Security on Cloud.
6. Sélectionnez une méthode d'extraction du rapport d'analyse. Vous pouvez utiliser la commande `get_result` de l'interface CLI ou vous pouvez utiliser le client Web d'Application Security on Cloud. Si vous utilisez l'interface CLI pour recevoir le rapport d'analyse, vous aurez l'option de recevoir un fichier archive (`.zip`) comprenant un fichier `.ozasmt` pour pouvoir ouvrir le rapport d'analyse dans AppScan Source. Si vous souhaitez uniquement obtenir un rapport

HTML, vous pouvez utiliser l'interface CLI ou le client Web d'Application Security on Cloud pour télécharger le rapport.

7. **Effectuez cette étape si vous souhaitez utiliser la commande `get_result` de l'interface CLI pour extraire le rapport d'analyse :**
   a. Vérifiez que vous êtes connecté au service à partir de l'interface CLI.
   b. Emettez la commande suivante sur Windows :

      ```
      appscan get_result -d <file_path> -i <job_id> -t <type>
      ```

      ou la commande suivante sur Linux :

      ```
      appscan.sh get_result -d <file_path> -i <job_id> -t <type>
      ```

      L'argument suivant est obligatoire :

      - `-i` : spécifiez `-i <job_id>`, où `<job_id>` est l'ID du travail d'analyse.

      Remarque : Si vous n'avez pas noté l'ID lors de l'émission de la commande `queue_analysis`, vous pouvez utiliser la commande `appscan list` ou `appscan.sh list` pour afficher une liste de tous les travaux d'analyse. Voir Commandes d'analyse (Windows) ou Commandes d'analyse (Linux) pour de plus amples informations.

      Les arguments suivants sont facultatifs :

      - `-d` : spécifiez `-d <file_path>`, où `<file_path>` est le chemin d'accès complet au fichier de destination et/ou son nom. Si aucun nom de fichier n'est spécifié, le nom de fichier est basé sur le nom du travail d'examen. Si aucun chemin n'est spécifié, le fichier est sauvegardé dans le répertoire de travail. Si cette option n'est pas incluse, le fichier est sauvegardé dans le répertoire de travail avec un nom de fichier basé sur le nom du travail d'examen.
      - `-t` : spécifiez `-t <type>`, où `<type>` est `html` ou `zip`. Les résultats sont sauvegardés dans un fichier HTML ou dans un fichier `.zip` contenant les résultats au format HTML. Si cette option n'est pas incluse, les résultats sont sauvegardés dans un fichier HTML.

        Si les résultats de l'examen concernent un fichier IRX généré par la commande `package`, l'option `-t zip` sauvegarde les résultats avec un nouveau fichier `.ozasmt` qui peut être chargé dans votre produit AppScan Source version 9.0 ou dans une version ultérieure.

      Vous trouverez des détails concernant la commande `get_result` sous Commandes de résultats (Windows) ou Commandes de résultats (Linux).

8. **Effectuez cette étape si vous souhaitez utiliser le client Web pour extraire le rapport d'analyse :** si vous souhaitez uniquement obtenir un rapport HTML, vous pouvez utiliser le client Web d'Application Security on Cloud pour télécharger le rapport.

   Lorsque vous vous connectez au service, vous devriez voir automatiquement une liste de vos examens (si vous avez navigué vers une autre section du service, cliquez sur l'icône **X** situé en haut à droite de l'écran pour retourner à la liste des examens). Dans la liste des examens, localisez l'examen et sélectionnez l'icône **Télécharger**, puis sélectionnez le format XML ou HTML.

   Pour en savoir plus sur les résultats d'examens d'Application Security on Cloud dans IBM Cloud Marketplace, voir http://www.ibm.com/support/knowledgecenter/en/SSYJJF_1.0.0/ApplicationSecurityonCloud/appseccloud_results_dashboard_cm.html. Dans IBM Bluemix, voir https://console.ng.bluemix.net/docs/services/ApplicationSecurityonCloud/appseccloud_results.html#results.

Publication d'évaluations

AppScan Source offre deux options de publication. Vous pouvez publier des évaluations sur base de données AppScan Source pour les stocker et pour les partager. Si votre serveur AppScan Enterprise Server a été installé avec l'option Enterprise Console, vous pouvez publier dessus des évaluations. Le composant AppScan Enterprise Console offre divers outils de gestion des évaluations, tels que des fonctions de génération de rapports, de gestion de problème et d'analyse de tendance, ainsi que des tableaux de bord.

Pour en savoir plus sur les fonctions de publication de AppScan Source, voir «Publication des évaluations sur AppScan Source», à la page 106 et «Publication des évaluations sur AppScan Enterprise Console», à la page 107.

Remarque : Pour certaines versions de AppScan Source et de AppScan Enterprise, la version et le niveau d'édition des deux produits doivent correspondre pour pouvoir effectuer la publication depuis AppScan Source vers AppScan Enterprise Console. Voir http://www.ibm.com/support/docview.wss?uid=swg21975211 pour savoir quelles versions d'AppScan Source et AppScan Enterprise sont compatibles lors de la publication d'évaluations.

Enregistrement des applications et des projets pour la publication sur AppScan Source

Pour qu'une évaluation puisse être publiée dans la base de données AppScan Source, les applications ou les projets qui ont été analysés pour créer cette évaluation doivent être enregistrés. Par défaut, si vous tentez de publier une évaluation d'une application ou d'un projet qui n'a pas encore été enregistré, vous serez invité à le faire à ce moment-là. AppScan Source for Analysis les *enregistre automatiquement* pour vous si, pour la préférence **Général**, **Enregistrer automatiquement les applications lors de leur publication initiale**, vous avez spécifié **Toujours les enregistrer**.

Important : Vous devez disposer du droit **Enregistrer** afin de pouvoir enregistrer des applications et des projets.

Pour enregistrer des applications et des projets avant l'examen, sélectionnez-les dans la vue Explorateur, puis sélectionnez **Fichier** > **Enregistrer** dans le menu principal du plan de travail. Les actions **Enregistrer l'application** et **Enregistrer le projet** sont également disponibles lorsque vous effectuez un clic droit sur les éléments sélectionnés dans la vue Explorateur.

Si une application est déjà enregistrée, vous pouvez l'enregistrer à nouveau sous un autre nom. Pour ce faire, sélectionnez et cliquez avec le bouton droit sur cet élément, puis sélectionnez **Enregistrer l'application sous** dans le menu. Dans la boîte de dialogue Attribution d'un nouveau nom, entrez un nouveau nom pour l'application ou le projet enregistré.

Pour annuler l'enregistrement d'applications et de projets, sélectionnez-les dans la vue Explorateur, puis sélectionnez **Fichier** > **Annuler l'enregistrement** dans la barre de menus principale du plan de travail. Les actions **Annuler l'enregistrement de l'application** et **Annuler l'enregistrement du projet** sont également disponibles lorsque vous effectuez un clic droit sur les éléments sélectionnés dans la vue Explorateur.

Remarque : L'annulation de l'enregistrement d'un élément ne supprime aucune donnée publiée de la base de données AppScan Source.

Publication des évaluations sur AppScan Source

Vous pouvez publier des évaluations sur la base de données AppScan Source pour les stocker et pour les partager.

Pourquoi et quand exécuter cette tâche

Les applications et les projets doivent être enregistrés auprès de AppScan Source pour que leurs évaluations puissent être publiées. Pour plus d'informations, voir «Enregistrement des applications et des projets pour la publication sur AppScan Source», à la page 105. Par défaut, si vous tentez de publier une évaluation d'une application ou d'un projet qui n'a pas encore été enregistré, vous serez invité à le faire à ce moment-là (le droit **Enregistrer** est requis).

Remarque : Les évaluations créées après l'examen de fichiers individuels ne peuvent pas être publiées.

Restriction : Lorsque vous examinez plusieurs applications ou projets, un noeud parent contenant des évaluations pour chaque élément analysé est créé dans la vue Mes évaluations. Les évaluations enfant individuelles ne peuvent pas être gérées dans ce cas (par exemple, les évaluations enfant ne peuvent pas être supprimées ni publiées individuellement). Lorsque plusieurs applications ou projets sont analysés en même temps, vous pouvez gérer les évaluations uniquement en tant que groupe (le noeud parent).

Procédure

1. Pour publier l'évaluation actuellement ouverte dans la perspective Triage, sélectionnez **Fichier** > **Publier l'évaluation dans AppScan Source** dans le menu principal de l'espace de travail.
2. Pour publier une évaluation dans la vue Mes évaluations, sélectionnez-la et cliquez sur le bouton **Publier l'évaluation dans AppScan Source** de la vue ou cliquez avec le bouton droit de la souris sur l'évaluation et sélectionnez **Publier l'évaluation dans AppScan Source**.

Résultats

Lors de la sauvegarde d'évaluations, AppScan Source for Analysis consigne des chemins d'accès absolus dans le fichier d'évaluation pour référencer des éléments tels que des fichiers source. Ces chemins d'accès absolus peuvent gêner le partage du fichier sur un autre ordinateur doté d'une structure de répertoires différente. Pour créer des fichiers d'évaluation portables, vous devez créer une variable (voir «Définition de variables», à la page 79 ou «Définition de variables lors de la publication et de la sauvegarde», à la page 114).

Une fois publiée, l'évaluation comporte une icône dans la colonne **Publiée** de la vue Mes évaluations. L'évaluation apparaît également dans la vue Evaluations publiées, laquelle est une vue filtrée des évaluations publiées dans la base de données AppScan Source. Cette vue peut être configurée pour n'afficher que les évaluations répondant aux critères de filtrage. Par exemple, si 1 000 évaluations ont été publiées et que vous souhaitez visualiser uniquement celles que vous avez publiées, vous pouvez créer un filtre avec **Par publicateur** comme critère et **Utilisateur actuel** ou votre nom d'utilisateur comme valeur.

Définition d'un filtre dans la vue Evaluations publiées

Les filtres peuvent être utilisés pour limiter le nombre d'évaluations qui s'affichent dans la vue Evaluations publiées.

Procédure

1. Dans la vue Evaluations publiées, cliquez sur le bouton **Définir un filtre** de la barre d'outils.
2. Cochez la ou les cases des critères de filtrage voulus :
   - **Par application** : sélectionnez l'application dont vous souhaitez afficher les évaluations. Si une évaluation a été générée pour plusieurs applications, elle est affichée dès lors que l'application spécifiée est l'une d'entre elles.
   - **Par publicateur** : configurez la vue de manière à afficher les évaluations qui ont été publiées par l'utilisateur actuel ou par un utilisateur désigné.
   - **Par proximité de date** : indiquez une plage de dates relative à la date actuelle en heures, jours, semaines, mois ou années. Vous pouvez sélectionnez **Par proximité de date** ou **Par plage de dates**, mais pas les deux.
   - **Par plage de dates** : spécifiez une plage de dates correspondant à la période dont vous souhaitez afficher les évaluations. Vous pouvez sélectionnez **Par proximité de date** ou **Par plage de dates**, mais pas les deux.
3. Cliquez sur **OK** pour définir le filtre.

Résultats

Clique sur **Régénérer le filtre** après l'application des critères de filtrage afin d'actualiser la vue avec les évaluations ajoutées ou retirées entre-temps. Cliquez sur **Effacer le filtre** pour ôter le filtre existant et afficher toute les évaluations.

Suppression des évaluations publiées dans AppScan Source

Si vous avez publié une évaluation sur AppScan Source, vous pouvez utiliser des actions de la vue Evaluations publiées pour les supprimer.

Procédure

1. Dans la vue Evaluations publiées, sélectionnez l'évaluation que vous souhaitez supprimer. Vous pouvez également sélectionner plusieurs évaluations avec les touches du clavier commande ou maj.
2. Sélectionnez le bouton **Supprimer des évaluations** dans la barre d'outils de la vue ou cliquez avec le bouton droit de la souris sur votre sélection et choisissez **Supprimer des évaluations** dans le menu.

Publication des évaluations sur AppScan Enterprise Console

Si votre serveur AppScan Enterprise Server a été installé avec l'option de Enterprise Console, vous pouvez publier des évaluations sur cette console. La Enterprise Console offre divers outils de gestion des évaluations, tels que des fonctions de génération de rapports, de gestion de problème et d'analyse de tendance, ainsi que des tableaux de bord.

Pourquoi et quand exécuter cette tâche

Pour pouvoir publier des évaluations dans la Enterprise Console, vous devez configurer les paramètres du serveur dans la page des préférences de la AppScan Enterprise Console. Pour plus d'informations sur la définition de ces préférences, reportez-vous à la rubrique «Préférences AppScan Enterprise Console», à la page 76.

Remarque : Pour certaines versions de AppScan Source et de AppScan Enterprise, la version et le niveau d'édition des deux produits doivent correspondre pour pouvoir effectuer la publication depuis AppScan Source vers AppScan Enterprise Console. Voir http://www.ibm.com/support/docview.wss?uid=swg21975211 pour savoir quelles versions d'AppScan Source et AppScan Enterprise sont compatibles lors de la publication d'évaluations.

Restriction : Lorsque vous examinez plusieurs applications ou projets, un noeud parent contenant des évaluations pour chaque élément analysé est créé dans la vue Mes évaluations. Les évaluations enfant individuelles ne peuvent pas être gérées dans ce cas (par exemple, les évaluations enfant ne peuvent pas être supprimées ni publiées individuellement). Lorsque plusieurs applications ou projets sont analysés en même temps, vous pouvez gérer les évaluations uniquement en tant que groupe (le noeud parent).

Procédure

1. Utilisez l'une des méthodes suivantes pour publier une ou plusieurs évaluations dans Enterprise Console :
   a. Sélectionnez une ou plusieurs évaluations dans la vue Mes évaluations, puis cliquez sur **Publier l'évaluation dans AppScan Enterprise Console**.
   b. Cliquez avec le bouton droit de la souris sur l'évaluation (ou une sélection d'évaluations) dans la vue Mes évaluations et sélectionnez l'option de menu **Publier l'évaluation dans AppScan Enterprise Console**.
   c. Lorsqu'une évaluation est ouverte, choisissez **Fichier** > **Publier l'évaluation dans AppScan Enterprise Console** dans le menu principal.
2. Dans la boîte de dialogue Publier dans AppScan Enterprise Console :
   a. Spécifiez une application AppScan Enterprise Console à laquelle associer l'évaluation. Ceci est nécessaire en cas de connexion à AppScan Enterprise Server versions 9.0.3 et supérieures (sauf si vous désactivez l'exigence, comme indiqué ici). L'association à une application est facultative en cas de connexion aux versions antérieures de AppScan Enterprise Server. Si vous êtes connecté à une version antérieure d'AppScan Enterprise Server, l'application est application est définie par défaut selon la dernière application spécifiée pour sa publication. Si aucune application n'a été spécifiée précédemment lors de la publication, aucune application n'est utilisée par défaut. Pour spécifier une application :
      1) Cliquez sur le bouton **Sélectionner** de la zone **Application**.
      2) La boîte de dialogue Sélectionner une application s'ouvre et affiche toutes les applications qui existent déjà dans AppScan Enterprise Console. Pour afficher les attributs d'une application dans AppScan Enterprise Console, cliquez sur **Afficher le profil** à côté de l'application.
      3) Sélectionnez l'application à laquelle associer l'examen ou créez une application dans ce but en cliquant sur **Créer une nouvelle application**. Si vous cliquez sur ce lien, AppScan Enterprise Console s'ouvre et vous permet de créer une application. Une fois les attributs de la nouvelle application sauvegardés, la boîte de dialogue Sélectionner une application est actualisée automatiquement pour que l'application soit incluse dans la sélection (si la nouvelle application n'est pas incluse automatiquement, cliquez sur **Actualiser**).

         Conseil : Dans la boîte de dialogue Sélectionner l'application, vous pouvez utiliser la zone de filtre afin de restreindre la liste des applications. Au fur et à mesure que vous entrez du texte, le filtre est appliqué automatiquement à la liste des applications. L'astérisque (*) et

le point d'interrogation (?) peuvent être utilisés comme caractères génériques. Un astérisque correspond à un groupe de zéro ou plusieurs caractères et le point d'interrogation correspond à un caractère.

4) Cliquez sur **OK** une fois l'application sélectionnée.

b. Obligatoire : Dans la zone **Nom**, spécifiez un nom sous lequel sauvegarder l'évaluation dans AppScan Enterprise Console.

c. Facultatif : **Lors d'une connexion à une version AppScan Enterprise Server antérieure à la version 9.0.3 :** Utilisez la zone **Dossier** pour définir l'emplacement de publication. Par défaut, l'emplacement est le dernier emplacement utilisé pour la publication. Si aucune évaluation n'a été préalablement publiée, le dossier de AppScan Enterprise Console par défaut est sélectionné (notez qu'il s'agit du dossier par défaut associé à l'ID utilisateur spécifié dans la page des préférences de AppScan Enterprise Console). Pour choisir un autre dossier de publication, cliquez sur le bouton **Sélectionner** de la zone **Dossier**, puis choisissez un dossier (seuls les dossiers dans lesquels vous disposez du droit de publication sont disponibles). Si le dossier dans lequel vous souhaitez effectuer la publication n'est pas disponible, cliquez sur **Actualiser** pour mettre à jour l'arborescence de dossiers en fonction des modifications que vous avez effectuées sur le serveur.

3. Cliquez sur **Publier**.

Résultats

Lors de la sauvegarde d'évaluations, AppScan Source for Analysis consigne des chemins d'accès absolus dans le fichier d'évaluation pour référencer des éléments tels que des fichiers source. Ces chemins d'accès absolus peuvent gêner le partage du fichier sur un autre ordinateur doté d'une structure de répertoires différente. Pour créer des fichiers d'évaluation portables, vous devez créer une variable (voir «Définition de variables», à la page 79 ou «Définition de variables lors de la publication et de la sauvegarde», à la page 114).

Une fois l'évaluation publiée, un lien vers AppScan Enterprise (Enterprise Console) vous sera fourni dans un message d'information. Un clic sur ce lien ouvrira la page du portail dans votre navigateur Web externe par défaut.

Conseil : En cas d'échec de la publication, vérifiez que le serveur de la console Enterprise Console est en cours d'exécution et que vous pouvez accéder à l'URL de son centre de contrôle dans un navigateur (utilisez la même **URL de la console Enterprise** que celle spécifiée dans la page des préférences de AppScan Enterprise Console).

Remarque :

- Les évaluations volumineuses peuvent prendre un certain temps avant leur affichage dans le portail. Si vous ne recevez pas de messages d'erreur après la publication, mais que le rapport n'apparaît pas dans le portail, contactez votre administrateur.
- Toute tentative de publication d'une évaluation portant le même nom que celle actuellement en cours de traitement par Enterprise Console échouera. De plus, si vous publiez l'évaluation sous ce même nom après le traitement de la première, la seconde évaluation écrasera la précédente (Enterprise Console peut fournir une analyse de tendances pour des rapports portant le même nom s'il a été configuré d'avance pour le faire). Pour déterminer si le traitement d'une

évaluation est terminé, accédez au centre de contrôle de Enterprise Console dans un navigateur Web, puis au répertoire utilisateur approprié et vérifiez le statut du rapport.

- AppScan Source ne prend pas en charge la publication sur une instance de Enterprise Console ayant été configurée pour utiliser des paramètres de proxy. Toute tentative de publication vers une telle instance se soldera par une erreur.

Important :

Lors de la mise à niveau vers AppScan Source version 9.0.3.4, vous remarquerez les modifications suivantes :

- Lors de la publication d'une évaluation sur AppScan Enterprise Console, vous devez désormais associer celle-ci à une application dans AppScan Enterprise (si vous utilisez AppScan Enterprise Server version 9.0.3 ou supérieure). En conséquence, les scripts d'automatisation peuvent échouer s'ils ne contiennent pas l'association d'applications. AppScan Enterprise Server, l'association d'applications est requise pour bénéficier de ses fonctions de gestion des risques de sécurité pour les applications. Voir http://www.ibm.com/support/knowledgecenter/SSW2NF_9.0.3/com.ibm.ase.help.doc/topics/c_overview.html.
- En outre, vous devez retirer le port de l'URL d'AppScan Enterprise.
  1. Dans AppScan Source for Analysis, cliquez sur **Editer** > **Préférences**.
  2. Dans les paramètres d'AppScan Enterprise Console, retirez le port de la zone **URL de la console Enterprise**.
- Après sa publication, l'évaluation n'est disponible que dans la vue Surveillance de AppScan Enterprise (dans les versions précédentes, elle était disponible dans les vues Examens). La migration vers cette vue est décrite à la rubrique http://www.ibm.com/support/knowledgecenter/SSW2NF_9.0.3/com.ibm.ase.help.doc/topics/t_workflow_for_applications.html.

Il s'agit du résultat du changement de protocole de communication entre AppScan Source et AppScan Enterprise Server, requis pour la publication sur AppScan Enterprise Server lors de l'utilisation de l'authentification CAC (Common Access Card).

Si vous ne souhaitez pas publier des évaluations sur AppScan Enterprise Server lorsque l'authentification CAC est activée, ni tirer parti des fonctions de gestion des risques de sécurité pour les applications offertes par Enterprise Server, vous pouvez rétablir l'ancien protocole de communication de la manière suivante :

1. Ouvrez `<datrép_données;\config\ounce.ozsettings` (où `<rép_données>` est l'emplacement de vos données de programme AppScan Source, comme décrit dans «Installation et emplacements des fichiers de données utilisateur», à la page 292).
2. Dans ce fichier, repérez le paramètre suivant :

```
<Setting
  name="force_ase902_assessment_publish"
  value="false"
  default_value="false"
  description="Use ASE 9.0.2-style assessment publish"
  display_name="Use ASE 9.0.2-style assessment publish"
  type="boolean"
  read_only="true"
  hidden="true"
/>
```

3. Remplacez `value="false"` par `value="true"` puis sauvegardez le fichier.

4. Redémarrez le produit AppScan Source à partir duquel vous publiez les évaluations.

Lorsque ce paramètre est défini sur `value="true"` :

- Si vous associez une évaluation à une application dans AppScan Enterprise lors de la publication, l'évaluation sera disponible dans les vues Surveillance et Examens.
- Si vous n'associez pas l'évaluation à une application lors de la publication, celle-ci sera disponible dans la vue Examens.
- Vous ne pourrez pas publier des évaluations dans AppScan Enterprise Server lorsque l'authentification CAC est activée.

Pour plus d'informations, voir http://www.ibm.com/support/docview.wss?uid=swg21993010.

Préférences AppScan Enterprise Console

Si votre serveur AppScan Enterprise Server a été installé avec l'option AppScan Enterprise Console, vous pouvez publier des évaluations sur cette console. Le composant Enterprise Console offre divers outils de gestion des évaluations, tels que des fonctions de génération de rapports, de gestion de problème et d'analyse de tendance, ainsi que des tableaux de bord.

Pour activer cette fonction, renseignez la page des préférences AppScan Enterprise Console. Toutes les zones de cette page doivent être renseignées avec des entrées valides avant l'activation de la publication d'Enterprise Console :

- Zone **ID utilisateur** : Entrez votre ID utilisateur AppScan Enterprise Server (l'ID utilisateur créé pour publication au nom de votre utilisateur AppScan Source).
  - Si votre serveur AppScan Enterprise Server est configuré pour utiliser l'authentification Windows, entrez le nom de domaine et d'utilisateur que vous utilisez pour vous connecter au serveur Enterprise Console (en les séparant par un signe \. Par exemple, `my_domain\my_username`).
  - Si votre serveur AppScan Enterprise Server est configuré avec LDAP, entrez le nom d'utilisateur que vous utilisez pour vous connecter au serveur Enterprise Console.

  Au minimum, vous devez être un utilisateur QuickScan. Si vous êtes connecté à un serveur AppScan Enterprise Server antérieur à la version 9.0.3, vous devez disposer de votre propre dossier utilisateur sur le serveur Enterprise Server.
- Zone **Mot de passe** : Entrez le mot de passe utilisé pour connexion au serveur Enterprise Console (le mot de passe correspondant à l'ID utilisateur saisi).
- Zone **URL de la console Enterprise** : indiquez l'URL utilisée pour accéder à l'application Web Enterprise Console.

  Le format de cette URL est le suivant :

  `http(s)://<nmhôte>:<port>/ase`

  Où `<nom_d'hôte>` est le nom de la machine sur laquelle Enterprise Console a été installé, et `<port>`, le port sur lequel la console s'exécute (par défaut, `<port>` correspond au port `9443`). Exemple: `https://myhost.mydomain.ibm.com:9443/ase`.

  Remarque :
  - Cette zone n'a pas besoin d'être modifiée si l'**URL de la console Enterprise** a déjà été définie.
  - Pour pouvoir définir la zone **URL de la console Enterprise**, vous devez être connecté à AppScan Source avec l'autorisation **Gérer les paramètres AppScan Enterprise**. Pour plus d'informations sur les comptes utilisateur et les

autorisations, voir la section *Administration* du centre de documentation du produit - ou la section *Administration de AppScan Source* du document *IBM Security AppScan Source - Guide d'installation et d'administration*.

- L'**ID utilisateur** et le **mot de passe** sont stockés sur le poste sur lequel le client AppScan Source s'exécute (par exemple, AppScan Source for Analysis), tandis que l'**URL de la console Enterprise** est stockée dans Enterprise Server (qui peut se trouver sur un poste distant). Vous ne pouvez pas accéder aux informations de nom d'utilisateur et de mot de passe à partir du poste distant (par exemple, en émettant la commande `getaseinfo`).
- AppScan Source ne prend pas en charge la publication sur une instance d'AppScan Enterprise Console ayant été configurée pour utiliser des paramètres de proxy. Toute tentative de publication vers une telle instance se soldera par une erreur.

Après avoir renseigné ces paramètres, il est fortement recommandé de vérifier que la connexion au serveur Enterprise Console est valide en cliquant sur **Tester la connexion**.

Conseil : Si le test de connexion échoue, vérifiez que le serveur Enterprise Console est en cours d'exécution et que vous pouvez accéder à l'URL de son centre de contrôle dans un navigateur (en utilisant la même **URL de console Entreprise** que celle spécifié ci-dessus).

Sauvegarde des évaluations

Avant de commencer

Important : Pour sauvegarder les évaluations, vous devez disposer du droit **Sauvegarder les évaluations**. Pour plus d'informations sur la définition des autorisations, voir le manuel *IBM Security AppScan Source - Guide d'installation et d'administration*.

Pourquoi et quand exécuter cette tâche

Les évaluations peuvent être sauvegardées en local et ouvertes à nouveau à tout moment. Par défaut, les évaluations sont sauvegardées avec une extension de fichier `.ozasmt` dans le répertoire de base de votre système d'exploitation (par exemple, sous Windows, le répertoire peut être `C:\Documents and Settings\Administrator\`).

Procédure

1. Pour sauvegarder l'évaluation actuellement ouverte dans la perspective Triage, sélectionnez **Fichier** > **Sauvegarde de l'évaluation** ou **Fichier** > **Sauvegarder l'évaluation sous** dans le menu principal du plan de travail. Le choix de l'action **Sauvegarder l'évaluation sous** vous permet d'indiquer l'emplacement et le nom de fichier de l'évaluation sauvegardée.
2. Pour sauvegarder une évaluation dans la vue Mes évaluations, sélectionnez-la et cliquez sur le bouton **Sauvegarde de l'évaluation** or **Sauvegarder l'évaluation sous** de la vue, ou cliquez avec le bouton droit de la souris sur l'évaluation et sélectionnez **Sauvegarde de l'évaluation** ou **Sauvegarder l'évaluation sous**.

Résultats

Lors de la sauvegarde d'évaluations, AppScan Source for Analysis consigne des chemins d'accès absolus dans le fichier d'évaluation pour référencer des éléments tels que des fichiers source. Ces chemins d'accès absolus peuvent gêner le partage du fichier sur un autre ordinateur doté d'une structure de répertoires différente. Pour créer des fichiers d'évaluation portables, vous devez créer une variable (voir «Définition de variables», à la page 79 ou «Définition de variables lors de la publication et de la sauvegarde», à la page 114).

Sauvegarde automatique des évaluations

Par défaut, les examens sont sauvegardés automatiquement dans `<data_dir>\scans` (où `<rép_données>` est l'emplacement de vos données de programme AppScan Source, comme décrit dans «Installation et emplacements des fichiers de données utilisateur», à la page 292) pendant trois jours. Ce comportement est déterminé par les paramètres `assessment_auto_save`, `assessment_auto_save_location` et `assessment_auto_save_stale_period` du fichier `<data_dir>\config\scanner.ozsettings`.

- Lorsque le paramètre `assessment_auto_save` est associé à la valeur `true`, les évaluations sont sauvegardées automatiquement lorsqu'elles sont terminées (vous devez disposer du droit **Sauvegarder les évaluations**).
- Le paramètre `assessment_auto_save_location` détermine l'emplacement de stockage des évaluations. Par défaut, les évaluations sont sauvegardées dans `<data_dir>\scans`. Pour modifier cet emplacement, affectez un nom de répertoire de votre choix à l'attribut `value`. Par exemple, pour définir l'emplacement `C:\myFolder`, affectez `value="C:\myFolder"` à l'attribut.
- Le paramètre `assessment_auto_save_stale_period` détermine le nombre de jours pendant lesquels les évaluations doivent être conservées dans `assessment_auto_save_location`. Vous pouvez modifier ce paramètre à l'aide de l'attribut `value`. Par exemple, les évaluations sauvegardées seront supprimées de `assessment_auto_save_location` au bout de 10 jours si vous indiquez `value="10"` pour l'attribut.

Suppression d'évaluations dans la vue Mes évaluations

Lorsque des évaluations sont supprimées de la vue Mes évaluations, elles ne sont pas supprimées de votre système de fichiers local. Si une évaluation est supprimée de la vue, elle peut être ajoutée à nouveau à l'aide de l'action **Ouvrir une évaluation**.

Pourquoi et quand exécuter cette tâche

Restriction : Lorsque vous examinez plusieurs applications ou projets, un noeud parent contenant des évaluations pour chaque élément analysé est créé dans la vue Mes évaluations. Les évaluations enfant individuelles ne peuvent pas être gérées dans ce cas (par exemple, les évaluations enfant ne peuvent pas être supprimées ni publiées individuellement). Lorsque plusieurs applications ou projets sont analysés en même temps, vous pouvez gérer les évaluations uniquement en tant que groupe (le noeud parent).

Procédure

1. Dans la vue Mes évaluations, sélectionnez l'évaluation que vous souhaitez supprimer. Vous pouvez également sélectionner plusieurs évaluations avec les touches du clavier commande ou maj.

2. Sélectionnez le bouton **Retirer de Mes évaluations** dans la barre d'outils de la vue ou cliquez avec le bouton droit de la souris sur votre sélection et choisissez **Retirer de Mes évaluations** dans le menu.

Définition de variables

Lors de la sauvegarde d'évaluations ou de groupements, ou de la publication d'évaluations, AppScan Source for Analysis peut vous suggérer de créer une variable pour remplacer des chemins absolus (sans variables, AppScan Source for Analysis consigne des chemins absolus vers le fichier d'évaluation pour référencer des éléments tels que des fichiers source). La configuration de variables pour des chemins absolus facilite le partage des évaluations entre plusieurs ordinateurs. L'utilisation de variables est conseillée en cas de partage des évaluations.

Pourquoi et quand exécuter cette tâche

Les variables peuvent être créées avant le lancement d'une action de sauvegarde ou de publication en suivant les instructions fournies dans cette rubrique, ou après son lancement en suivant les étapes décrites dans «Définition de variables lors de la publication et de la sauvegarde».

Pour savoir par exemple comment les variables peuvent apporter leur contribution lors du partage des évaluations, voir «Exemple : définition de variables», à la page 115.

Procédure

1. Sélectionnez **Editer** > **Préférences** dans le menu principal. Dans la boîte de dialogue Préférences, choisissez **Modifier les variables**.
2. Cliquez sur le bouton **Ajouter une variable** dans la page de préférences Modifier les variables.
3. Entrez le nom de la variable et recherchez un emplacement de fichier qui sera remplacé par la variable (AppScan Source for Analysis insère les symboles pourcentage encadrant la variable (%) une fois cette dernière créée).
4. Répétez l'étape ci-dessus pour d'autres éléments de référence dans l'évaluation (par exemple, si l'évaluation référence la source à plusieurs emplacements, ajoutez une variable pour chaque emplacement).
5. La page de préférences vous permet d'éditer et de supprimer des variables, respectivement à l'aide des boutons **Modifier** et **Supprimer**.
6. Cliquez sur **OK** une fois la définition des variables terminée.

Définition de variables lors de la publication et de la sauvegarde

Lorsque vous tentez de sauvegarder ou de publier une évaluation, AppScan Source for Analysis détecte les chemins absolus dans l'évaluation. Si les variables correspondantes n'ont pas été créées pour les chemins absolus, vous êtes invité à les créer.

Pourquoi et quand exécuter cette tâche

Les variables peuvent être créées avant le lancement d'une action de sauvegarde ou de publication en suivant les instructions fournies dans «Définition de variables», à la page 79 - ou après leur lancement en suivant les étapes décrites dans la présente rubrique.

Pour savoir par exemple comment les variables peuvent apporter leur contribution lors du partage des évaluations, voir «Exemple : définition de variables».

Procédure

1. Après avoir lancé l'action de sauvegarde ou de publication, cliquez sur **Oui** dans le message Détection de chemins absolus.
2. Dans la boîte de dialogue Définition de variables, AppScan Source for Analysis suggère un ensemble de chemins qui couvrent les donnée.
3. Sélectionnez un répertoire et cliquez sur **Ajouter une variable**.
4. Répétez l'étape ci-dessus pour d'autres éléments de référence dans l'évaluation (par exemple, si l'évaluation référence la source à plusieurs emplacements, ajoutez une variable pour chaque emplacement).
5. La boîte de dialogue Définition de variables permet de modifier et de supprimer des variables à l'aide des boutons **Modifier** et **Supprimer**.
6. Cliquez sur **OK** pour exécuter la sauvegarde ou la publication.

Exemple : définition de variables

Pour partager les données des évaluations, vous devez définir les variables appropriées. L'exemple de cette rubrique illustre la nécessité d'une variable.

L'utilisateur Joe effectue un examen sur l'ordinateur A sur lequel tout le code source réside sous le répertoire `C:\dev\my_code`. Joe souhaite sauvegarder dans un fichier les résultats de son examen et les partager avec Bill. Bill utilise l'ordinateur B et a examiné le même code que Joe sous le répertoire `C:\code\bills_code`. En l'absence de variables, le fichier d'évaluation référencera tous les fichiers source avec des chemins absolus à partir de `C:\dev\my_code`. Si Bill ouvre ce fichier d'évaluation sur l'ordinateur B, AppScan Source for Analysis ne parviendra pas à localiser les fichiers source puisqu'ils résident sous `C:\code\bills_code` sur l'ordinateur B.

Solution

Joe et Bill doivent tous deux créer une variable qui pointe vers la racine du code source. Joe crée une variable dans AppScan Source for Analysis nommée `SRC_ROOT` et lui attribue la valeur `C:\dev\my_code`. Cette variable est locale à l'installation AppScan Source for Analysis de Joe. Joe communique ensuite à Bill le nom de la variable (`SRC_ROOT`) et l'emplacement vers lequel elle pointe. Bill crée alors une variable nommée `SRC_ROOT` en lui attribuant la valeur `C:\code\bills_code` sur son installation AppScan Source for Analysis. Lorsque Joe sauvegarde son examen, la variable `SRC_ROOT` remplace le chemin d'accès `C:\dev\my_code`. Lorsque Bill ouvre le fichier d'évaluation reçu de Joe, `C:\code\bills_code` est substitué à la variable `SRC_ROOT`.

Chapitre 5. Triage et analyse

Le regroupement de constatations similaires permet aux analystes de la sécurité ou aux auditeurs du service informatique d'effectuer une segmentation et un triage des problèmes affectant le code source. Cette section explique comment procéder au triage des évaluations AppScan Source et à l'analyse des résultats.

Lorsque vous examinez le code, les résultats de l'examen, dénommés *constatations*, apparaissent. Le *triage* désigne le processus d'évaluation des constatations et de détermination de la manière de les résoudre. Cependant, les procédures requises pour atteindre cet objectif dépendent de facteurs multiples, notamment du nombre total de constatations, de questions de sécurité spécifiques, de l'évaluation des risques de l'application, etc. Outre le fait de déterminer si une constatation dénote un problème de sécurité valide, le triage implique également la modification des attributs des constatations (gravité, type, classification), le cas échéant.

L'utilisation d'une stratégie de triage est importante pour garantir la réalisation de vos objectifs dans l'ordre voulu et les délais impartis. Le triage optimal est réalisé par le biais d'une itération dans laquelle vous évaluez un sous-ensemble de constatations et déterminez la position de chaque sous-ensemble dans chaque itération. Plusieurs approches valides sont possibles pour décider comment définir les itérations du triage. Une approche consiste à créer des sous-ensembles de constatations à haut risque basés sur leur gravité globale. Vous pouvez alors commencer à résoudre les constatations présentant le risque potentiel le plus élevé, avant de passer aux constatations mineures. Une autre approche consiste à définir des sous-ensembles en fonction de la menace posée à la sécurité (par exemple, injection SQL ou validation requise).

Le triage est généralement effectué par un analyste de la sécurité ou un auditeur du service informatique. Celui-ci peut soumettre les constatations imposant des modifications du code à un système de suivi des défauts, puis aux développeurs pour leur résolution. Dans certains cas, les développeurs peuvent procéder eux-mêmes au triage et à la résolution des problèmes.

Lors de la phase de triage, vous pouvez :

- Examiner les constatations associées à des types de vulnérabilité particulièrement pertinents
- Afficher les API d'une catégorie spécifique
- Comparer les constatations d'évaluations différentes
- Filtrer ou exclure des constatations spécifiques
- Modifier la gravité ou le type de vulnérabilité d'une constatation
- Promouvoir les constatations suspectées et les constatations de couverture d'examen en constatations définitives
- Annoter des constatations
- Soumettre des défauts à des systèmes de suivi de défaut ou transmettre des constatations à d'autres intervenants par courrier électronique.

AppScan Source fournit tous les outils nécessaires pour analyser les résultats par le biais de différentes stratégies de triage. Le filtrage permet de visualiser exclusivement les constatations à traiter au cours d'une itération de triage spécifique. Si votre stratégie d'itération repose sur leur gravité et classification,

vous pouvez filtrer les constatations depuis la vue Matrice de vulnérabilités. AppScan Source for Analysis fournit également un éditeur de filtre prenant en charge des approches d'itération complexes.

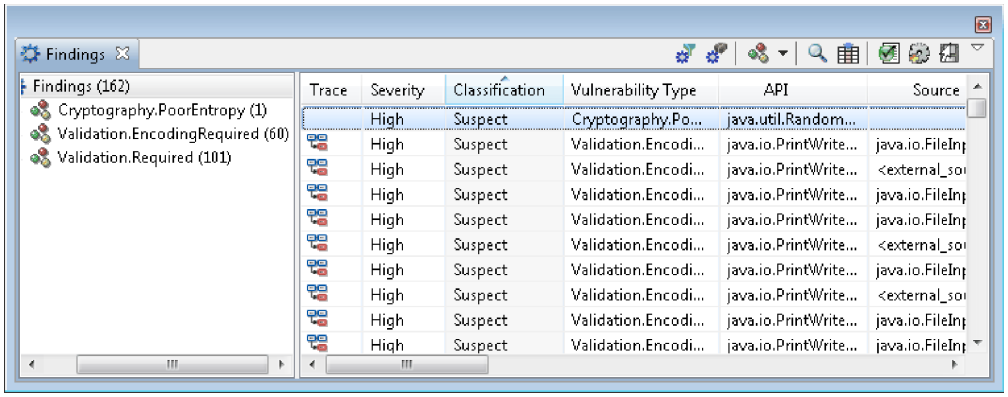
Une fois votre approche de triage sélectionnée, AppScan Source for Analysis prend en charge le traitement des constatations.

- Exclusion de collections ou de constatations individuelles
- Modification des caractéristiques des constatations (type, gravité, classification)
- Création de groupements (mécanisme d'agrégation de constatations)
- Comparaison d'évaluations par le biais de la vue Différences entre les évaluations

Affichage de constatations

La vue Constatations, ou toute autre vue contenant des constatations, affiche leur arborescence (regroupement hiérarchique des critères d'évaluation) et un Tableau des constatations pour chaque examen. L'élément sélectionné dans l'arborescence des constatations déterminent celles qui apparaissent dans le tableau.

Lorsque vous sélectionnez la racine de l'arborescence, toutes les constatations s'affichent dans le tableau. Lorsque vous sélectionnez un type de groupement, seules les constatations de ce type apparaissent.



AppScan Source for Analysis affiche les constatations dans des regroupements différents incluant :

- **Type de vulnérabilité**
- **Classification**
- **Fichier**
- **Source**
- **Collecteur**
- **API**
- **Groupement**
- **CWE**
- **Tableau**

Remarque : Les classifications et gravités sont triés par défaut par ordre descendant. Toutes les autres colonnes sont triées par ordre descendant.

Les colonnes suivantes apparaissent dans un tableau des constatations.

Tableau 11. Tableau de constatations

En-tête de la colonne	Description
Trace	Une icône dans cette colonne indique qu'il existe une trace pour les collecteurs perdus ou connus.
Gravité	• **Elevée** : Pose un risque pour la confidentialité, l'intégrité et la disponibilité des données et/ou des ressources de traitement. Vous devriez affecter cette priorité aux conditions nécessitant une résolution immédiate. • **Moyenne** : Pose un risque pour la sécurité des données et l'intégrité des ressources mais la condition est moins susceptible de subir des attaques. Les conditions de gravité moyenne devraient être examinées et résolues dans la mesure du possible. • **Faible** : Pose un risque minime à la sécurité des données et à l'intégrité des ressources. • **Info** : La constatation elle-même ne présente pas de risque. Elle décrit plutôt les technologies, les caractéristiques de l'architecture ou les mécanismes de sécurité utilisés dans le code.
Classification	Type de constatation : constatation de sécurité **Définitive** ou **Suspectée** - ou constatation de **Couverture d'examen**. **Remarque :** Dans certains cas, la classification **Aucun** est utilisée pour indiquer une constatation qui n'est ni une constatation de sécurité ni une constatation de couverture d'examen.
Type de vulnérabilité	Catégorie de la vulnérabilité, telle que `Validation.Required` ou `Injection.SQL`.
API	Indique l'appel vulnérable, en présentant à la fois l'API et les arguments qui lui sont transmis.
Source	Une source est une entrée du programme, telle qu'un fichier, une requête de servlet, une saisie depuis la console ou un socket. Dans le cas de la plupart des sources d'entrées, les données renvoyées ne sont pas limitées en termes de contenu et de longueur. Lorsqu'une entrée n'est pas vérifiée, elle est considérée comme entachée.
Collecteur	Un collecteur peut être un format externe quelconque dans lequel des données peuvent être consignées. Comme exemples de collecteurs, on peut citer des bases de données, des fichiers, des sorties console et des sockets. La consignation de données dans un collecteur sans leur vérification peut donner lieu à une vulnérabilité sérieuse de la sécurité.

Tableau 11. Tableau de constatations (suite)

En-tête de la colonne	Description
Répertoire	Chemin d'accès complet des fichiers analysés.
Fichier	Nom du fichier de code dans lequel la constatation de sécurité ou la constatation de couverture d'examen survient. Les chemins de fichier dans les constatations sont relatifs au répertoire de travail du projet analysé.
Méthode d'appel	Fonction (ou méthode) depuis laquelle l'appel vulnérable est effectué.
Ligne	Numéro de la ligne dans le fichier de code contenant l'API vulnérable.
Groupement	Groupement contenant cette constatation.
CWE	ID et sujet du dictionnaire de faiblesses logicielles courantes développé par la communauté (rubriques CWE - Common Weakness Enumeration).

Remarque : Si vous sélectionnez une constatation et que AppScan Source ne peut pas trouver de source liée à celle-ci, vous verrez apparaître une boîte de dialogue qui vous permet de choisir si vous souhaitez être consulté lorsque cette situation se produit. Si vous sélectionnez **Oui**, vous serez consulté à chaque fois qu'une constatation est sélectionnée et qu'aucun fichier source ne peut être trouvé pour celle-ci. Si vous sélectionnez **Non**, vous ne serez pas consulté. Ce paramètre demeure disponible tant que l'évaluation en cours est ouverte. Ce paramètre est réinitialisé à chaque fois que l'évaluation est ouverte ou si vous quittez AppScan Source.

Processus de triage AppScan Source

Le processus de triage désigne la manipulation des constatations via des groupements, des filtres et des exclusions et la comparaison des résultats des évaluations.

Filtres

Un *filtre* désigne un ensemble de règles définissant des constatations dotées de certaines caractéristiques. Il permet de présenter une vue dynamique de ces constatations et d'effectuer un triage de constatations similaires.

Les filtres sont soit *partagés*, soit *locaux* :

- Les filtres partagés résident sur le serveur AppScan. Tout utilisateur connecté au serveur peut utiliser le filtre.
- Les filtres locaux résident sur l'ordinateur local.

Groupements

Un *groupement* est une collection nommée de constatations individuelles qui est stockée avec une application. Un groupement est créé en sélectionnant des constatations et en les ajoutant à un nouveau groupement ou à un groupement existant.

L'organisation de constatations similaires en groupements permet aux analystes de la sécurité d'effectuer une segmentation et un triage des problèmes du code source. Vous pouvez soumettre des groupements à un système de suivi des défauts ou les envoyer par courrier électronique à des développeurs pour leur examen dans le cadre du processus de triage et d'analyse.

Exclusions

Une *exclusion* omet les constatations correspondantes des examens. AppScan Source comporte un **Groupement exclu** intégré qui contient les constatations que vous excluez (car elles n'ont pas besoin d'être résolues par exemple).

Remarque : Les constatations exclues des résultats de l'évaluation ne participent pas au calcul des métriques de l'application ou du projet.

Constatations modifiées

Une constatation *modifiée* désigne une constatation dont le type de vulnérabilité, la gravité ou la classification ont été changés. Si vous ajoutez des notes à une constatation, celle-ci est également considérée avoir été modifiée.

Comparaison des évaluations

Les évaluations sont comparées dans AppScan Source for Analysis à l'aide de l'action **Différences entre les évaluations**. Lorsque deux évaluations sont comparées, leurs différences s'affichent dans la vue Différences entre les évaluations (sorte de combinaison entre la vue Mes évaluations et la vue Constatations).

Remarque : Lorsque les évaluations sont comparées, les filtres et les groupements sont ignorés.

Triage avec filtres

AppScan Source for Analysis rend compte de toutes les vulnérabilités de sécurité potentielles et peut donc générer des milliers de constatations pour une base de code de moyenne/grande envergure. Lors de l'analyse, vous pouvez conclure que la liste des constatations contient des éléments sans importance dans votre cas. Pour éliminer certains éléments de la vue Constatations, vous pouvez choisir un filtre prédéfini ou créer votre propre *filtre*. Un filtre spécifie les critères déterminant quelles constatations éliminer de la vue.

- «Présentation des filtres»
- «Règles de filtrage», à la page 122
- «Exemples de filtre», à la page 125

Présentation des filtres

Les filtres permettent de supprimer ou de restreindre l'affichage d'éléments qui répondent à des critères déterminés par des règles de filtre. Ils peuvent aussi vous aider à gérer les résultats d'examen pendant le triage ou la génération de rapports. Un filtre aide à piloter le flux de travaux et à focaliser les analystes de la sécurité sur les zones les plus critiques d'un sous-ensemble de constatations. Par exemple, lors de l'examen du code, un analyste peut créer un filtre afin d'éviter l'affichage de constatations à faible gravité. Il pourrait également vouloir exclure des

vulnérabilités des fichiers d'`inclusion` de la bibliothèque système. Un filtre peut éliminer l'affichage de ces éléments et exclure des fichiers individuels ou déjà examinés.

Des filtres peuvent être appliqués avant ou après un examen.

- Pour appliquer des filtres avant l'examen, vous définissez des filtres globaux dans les propriété du projet ou de l'application, ou bien vous effectuez un examen à l'aide d'une configuration d'examen comportant des filtres. Lorsque vous appliquez des filtres avant l'examen, vous ne pouvez pas afficher des constatations non filtrés ou supprimer le filtre sans effectuer un nouvel examen.
- Différentes vues (en particulier la vue Editeur de filtre) vous permettent d'appliquer des filtres après l'examen. Lorsque ces vues sont utilisées pour le filtrage, tous les éléments filtrés demeurent dans les résultats de l'examen et n'apparaissent dans la vue Constatations que si l'option à bascule **Afficher les constatations filtrées** ( ) est sélectionnée.

AppScan Source inclut plusieurs filtres prédéfinis qui peuvent être sélectionnés pour le filtrage des résultats d'examen.

Dès lors que vous avez un filtre, vous pouvez définir une propriété pour caractériser le filtre comme une *exclusion*. Une exclusion affecte les analyses et élimine toutes les constatations qui correspondent au filtre ou, à l'inverse, toutes celles qui ne s'y conforment pas.

Règles de filtrage

Chaque filtre est composé de règles qui définissent à quelles constatations les restreindre (inclure) ou lesquelles supprimer (exclure) dans les résultats du tableau des constatations (pour les règles de trace, vous pouvez restreindre et supprimer des éléments en fonction des propriétés de trace).

- Une règle de **restriction** (règle inclusive) exclut les constatations ne correspondant pas aux critères spécifiés et les retire des résultats visibles dans le tableau des constatations.
- Une règle de **suppression** (règle exclusive) retire les constatations correspondant aux critères spécifiés des résultats d'examen. Une règle de suppression retire les constatations correspondant aux critères spécifiés des résultats visibles de l'examen.

Une règle de filtrage peut inclure ces caractéristiques :

- **Gravité** : Identifie l'impact ou le risque potentiel des constatations individuelles. Les règles de gravité sont de type restriction uniquement.
  - **Elevée** : Pose un risque pour la confidentialité, l'intégrité et la disponibilité des données et/ou des ressources de traitement. Vous devriez affecter cette priorité aux conditions nécessitant une résolution immédiate.
  - **Moyenne** : Pose un risque pour la sécurité des données et l'intégrité des ressources mais la condition est moins susceptible de subir des attaques. Les conditions de gravité moyenne devraient être examinées et résolues dans la mesure du possible.
  - **Faible** : Pose un risque minime à la sécurité des données et à l'intégrité des ressources.
  - **Info** : La constatation elle-même ne présente pas de risque. Elle décrit plutôt les technologies, les caractéristiques de l'architecture ou les mécanismes de sécurité utilisés dans le code.

- **Classification :** Filtre les constatations d'après les classifications décrites dans cette rubrique. Les règles de classification sont de type restriction uniquement.
- **Type de vulnérabilité** : Filtrage d'après une catégorie de vulnérabilité spécifique, par exemple `dépassement de mémoire tampon`. Lorsque vous ajoutez un type de vulnérabilité, vous pouvez effectuer une sélection dans la liste de tous les types de vulnérabilité possibles ou vous pouvez choisir uniquement les types qui ont été détectés dans l'évaluation en cours. Pour choisir un type de vulnérabilité parmi ceux qui ont été détectés dans l'évaluation en cours, sélectionnez l'option **Afficher uniquement les valeurs de l'évaluation ouverte** dans la boîte de dialogue Sélection de valeurs.

  Une sélection parmi tous les types de vulnérabilité possibles est utile lorsque vous créez une filtre pour des examens ultérieurs. Pour afficher tous les types de vulnérabilité, désélectionnez la case **Afficher uniquement les valeurs de l'évaluation ouverte** (en l'absence d'évaluations ouvertes, tous les types de vulnérabilité sont affichés par défaut et la case à cocher **Afficher uniquement les valeurs de l'évaluation ouverte** n'est pas disponible).
- **API** : Filtre toutes les vulnérabilités d'une API spécifique.
- **Fichier** : Filtre toutes les vulnérabilités d'un fichier spécifique.
- **Répertoire** : Filtre toutes les vulnérabilités d'un répertoire spécifique.
- **Projet** : Filtre toutes les vulnérabilités d'un projet spécifique.
- **Trace** : Permet de filtrer les constatations d'après les propriétés de trace (voir «Sources et collecteurs», à la page 161 pour plus d'informations sur ces propriétés). Les filtres peuvent inclure des règles de trace qui effectuent des restrictions ou des suppressions en fonction de propriétés de trace. Lorsque vous cliquez sur **Ajouter** dans l'une ou l'autre des sections (restriction ou suppression), la boîte de dialogue Entrée de règle de trace s'ouvre. Vous pouvez spécifier dans celle-ci :
  - **Source** : Dans la zone **RegEx d'API** de la section Source, spécifiez la source de la trace ou une expression régulière couvrant plusieurs sources (l'entrée par défaut est `.*`, correspondant à l'expression régulière ou le caractère générique les renvoyant toutes). Si vous utilisez une expression régulière, sélectionnez son type dans le menu de la zone **Type RegEx** (le type par défaut étant **PERL**). Si vous n'utilisez pas d'expression régulière, sélectionnez l'option **Correspondance exacte** dans le menu de la zone **Type RegEx**.

    Si l'entrée **RegEx d'API** correspond à une expression valide, une coche verte apparaît en regard de la zone. Si elle n'est pas valide, un symbole X en rouge apparaît en regard de la zone et le bouton **OK** de la boîte de dialogue est alors désactivé. Le survol des ces indications fournit des résultats supplémentaires sur les résultats de la validation. Si votre entrée ne correspond pas à une expression valide mais que vous désirez néanmoins l'utiliser, cochez la case **Ignorer les erreurs de validation ci-dessus** au bas de la boîte de dialogue. Ceci réactive le bouton **OK** (pour autant que l'expression n'est pas vide) et l'icône en regard de l'expression non valide change pour afficher une coche verte avec une infobulle **Validation désactivée**.

    Vous pouvez aussi affiner le filtre par mécanisme ou technologie en utilisant le bouton **Ajouter une propriété VMAT** dans la section Propriétés de source (plus d'informations sur les propriétés VMAT disponibles ci-dessous) ; toutefois, l'utilisation de cette fonction pour appliquer une limitation par vulnérabilité n'aura pas l'effet souhaité car le type de vulnérabilité est déterminé par le collecteur et non par la source.
  - **Collecteur** : Dans la section Collecteur, vous pouvez ajouter des collecteurs en tant que filtre de la même manière que vous spécifiez les sources.

Vous pouvez affiner le filtre en le limitant à des types de vulnérabilité spécifiques (pour limiter l'effet de l'entrée de règle de trace à des types spécifique de vulnérabilité, de mécanisme ou de technologie). Pour ce faire, cliquez sur le bouton **Ajouter une propriété VMAT** dans la section Propriétés de collecteur, puis sélectionnez la propriété dans la boîte de dialogue Sélection des propriétés. La liste des propriétés peut être filtrée à l'aide de la zone **Filtre**.

VMAT est une catégorisation des quatre principaux types de propriétés appliquées par AppScan Source. Les catégories de propriété VMAT incluent :

- **Vulnérabilité** : type d'exploit ou de vecteur d'attaque débouchant sur une violation de la sécurité
- **Mécanisme** : mécanisme de sécurité utilisé pour empêcher une vulnérabilité
- **Attribut** : ces propriétés ne sont actuellement pas disponibles dans la boîte de dialogue Sélection des propriétés
- **Technologie** : description générale du type de fonctionnalité assuré par une API

Exemple de filtre : Pour filtrer toutes les injections SQL et les scripts intersites (XSS) provenant d'HTTP (la source essentielle de risques), créez une règle de trace **Restreindre à** qui contient un filtre `Technology.Communications.HTTP` dans la section Propriétés de source et des règles `Vulnerability.Injection.SQL` et `Vulnerability.CrossSiteScripting` dans la section Propriétés de collecteur.

– **Appels requis** : Dans la section Appels requis, ajoutez des appels d'API spécifiques devant figurer sur le chemin d'accès de la source vers le collecteur. Les appels requis limitent les constatations à celles dont les traces passent à travers les appels requis spécifiés. Lorsque vous cliquez sur **Ajouter un appel intermédiaire**, la boîte de dialogue Configuration d'API s'ouvre. Dans cette boîte de dialogue, spécifiez l'appel approprié de la même manière que vous avez spécifié des sources et des collecteurs.

– **Appels interdits** : Dans la section Appels interdits, ajoutez des appels d'API spécifiques ne devant pas figurer sur le chemin d'accès de la source au collecteur. Les appels interdits limitent les constatations à celles dont les traces ne passent pas à travers les appels interdits spécifiés. Ajoutez des appels interdits de la même manière que ceux requis.

Conseil :

– Lorsque le filtrage par **Type de vulnérabilité**, **API**, **Fichier**, **Répertoire** ou **Projet** est utilisé, la liste qui apparaît dans la boîte de dialogue Sélection de valeurs peut être filtrée en tapant un schéma dans la zone de filtre située en haut de la boîte de dialogue.

– Depuis un tableau de constatations quelconque, examinez les colonnes **Source** et **Collecteur** pour vous faire une idée des sources et collecteurs que vous voudrez filtrer.

– Pour vous faire une idée des propriétés de source, collecteur et appel que vous voudrez filtrer, examinez la colonne **Type de vulnérabilité** d'un tableau de constatations quelconque.

– Pour afficher les appels que vous pourriez vouloir filtrer, examinez les entrées de la colonne **API** d'un tableau de constatations quelconque.

Exemples de filtre

Tableau 12. Exemples de filtre

Comportement du filtre dans un tableau de constatations	**Paramètres de filtrage dans la vue Editeur de filtre**
Le tableau des constatations contient uniquement des constatations de sécurité suspectées à gravité élevée.	• Dans la section Gravité, cochez la case **Elevée** et décochez toutes les autres. • Dans la section Classification, cochez la case **Suspectée** et désélectionnez toutes les autres cases.
Le tableau des constatations inclut toute celles d'un projet nommé `ProjectA`, à l'exception des types information sur les vulnérabilités.	• Dans la section Type de vulnérabilité, sélectionnez le bouton d'option **Supprimer** et cliquez sur **Ajouter**. Dans la boîte de dialogue Sélection de valeurs, sélectionnez **Vulnerability.Info**. • Dans la section Projet, sélectionnez le bouton d'option **Restreindre à** et cliquez sur **Ajouter**. Dans la boîte de dialogue Sélection de valeurs, sélectionnez `ProjectA`.
Seules les constatations comportant une trace sont affichées.	Dans la section Trace, cliquez sur **Ajouter** dans la section **Restreindre à**. Acceptez les entrées par défaut de la boîte de dialogue Entrée de règle de trace et cliquez sur **OK**. Les valeurs par défaut de cette boîte de dialogue sont les suivantes : • Zone **RegEx d'API** de la section Source : `.*` ; Type d'expression régulière : **PERL**. Ceci indique à AppScan Source de rechercher uniquement les constatations avec une source (à l'aide de la syntaxe d'expression régulière Perl). • Zone **RegExe d'API** de la zone Collecteur : `.*` ; Type d'expression régulière : **PERL**. Ceci indique à AppScan Source de rechercher uniquement les constatations avec un collecteur (à l'aide de la syntaxe d'expression régulière Perl).

Tableau 12. Exemples de filtre (suite)

Comportement du filtre dans un tableau de constatations	Paramètres de filtrage dans la vue Editeur de filtre
Le tableau des constatations affiche les sources associées à HTTP vers des collecteurs associés à une injection SQL et ne passant pas par `java.lang.Integer.parseInt`.	Dans la section Trace, cliquez sur **Ajouter** dans la section **Restreindre à**. Dans la boîte de dialogue Entrée de règle de trace, procédez comme suit : • Dans la section Source, cliquez sur **Ajouter une propriété VMAT**. Dans la boîte de dialogue Sélection de valeurs, sélectionnez `Technology.Communications.HTTP`. Cliquez sur **OK** pour ajouter la propriété VMAT et revenir à la boîte de dialogue Entrée de règle de trace. • Dans la section Collecteur, cliquez sur **Ajouter une propriété VMAT**. Dans la boîte de dialogue Sélection de valeurs, sélectionnez `Vulnerability.Injection.SQL`. Cliquez sur **OK** pour ajouter la propriété VMAT et revenir à la boîte de dialogue Entrée de règle de trace. • Dans la section Appels interdits, cliquez sur **Ajouter un appel intermédiaire**. Dans la boîte de dialogue Configuration d'API, entrez `java.lang.Integer.parseInt.*` dans la zone **RegEx d'API**. Cliquez sur **OK** pour ajouter l'appel intermédiaire et revenir à la boîte de dialogue Entrée de règle de trace, puis sur **OK** pour ajouter cette entrée.

Utilisation des filtres prédéfinis AppScan Source

AppScan Source inclut un ensemble de filtres prédéfinis que vous pouvez sélectionner pour le filtrage des résultats d'examen. La présente rubrique d'aide décrit ces filtres prêts à l'emploi.

Remarque : Dans AppScan Source version 8.8, les filtres prédéfinis ont été améliorés pour fournir de meilleurs résultats d'examen. Si vous devez continuer à utiliser les filtres prédéfinis des versions antérieures d'AppScan Source (les filtres archivés sont répertoriés dans «Filtres prédéfinis AppScan Source (versions 8.7.x et antérieures)», à la page 129), suivez les instructions de la section «Restauration des filtres prédéfinis archivés», à la page 131.

Remarque : Dans AppScan Source for Development (plug-in Visual Studio), cette vue fait partie de la fenêtre Edition de filtres.

! - Le minimum vital AppScan

Ce filtre correspond aux constatations entrant dans les catégories de vulnérabilités les plus dangereuses. Les résultats sont limités aux vulnérabilités de gravité Elevée et Moyenne. Les résultats issus de sources spécifiques sont supprimés des constatations. Ce filtre inclut les catégories de vulnérabilités spécifiques suivantes :

```
Vulnerability.CrossSiteScripting
Vulnerability.CrossSiteScripting.Reflected
Vulnerability.CrossSiteScripting.Stored
Vulnerability.Injection.OS
Vulnerability.Injection.LDAP
Vulnerability.Injection.SQL
Vulnerability.Injection.Mail
```

! - Sources à risque élevé

Ce filtre limite les constatations à des sources et des types de vulnérabilité spécifiques à l'aide de l'une des propriétés suivantes :

```
Technology.Communications.HTTP
Technology.Communications.IP
Technology.Communications.RCP
Technology.Communications.TCP
Technology.Communications.UDP
Technology.Communications.WebService
```

! - Types importants

Ce filtre contient les constatations issues d'une plus large plage de catégories de vulnérabilités importantes. Les constatations sont limitées aux gravités Elevée et Moyenne avec les classifications Définitive ou Suspectée. Il inclut les catégories spécifiques suivantes :

```
Vulnerability.AppDOS
Vulnerability.Authentication.Credentials.Unprotected
Vulnerability.BufferOverflow
Vulnerability.BufferOverflow.FormatString
Vulnerability.BufferOverflow.ArrayIndexOutOfBounds
Vulnerability.BufferOverflow.BufferSizeOutOfBounds
Vulnerability.BufferOverflow.IntegerOverflow
Vulnerability.BufferOverflow.Internal
Vulnerability.CrossSiteRequestForgery
Vulnerability.CrossSiteScripting
Vulnerability.CrossSiteScripting.Reflected
Vulnerability.CrossSiteScripting.Stored
Vulnerability.FileUpload
Vulnerability.Injection
Vulnerability.Injection.LDAP
Vulnerability.Injection.OS
Vulnerability.Injection.SQL
```

```
Vulnerability.Injection.XML
Vulnerability.Injection.XPath
Vulnerability.Malicious.EasterEgg
Vulnerability.Malicious.Trigger
Vulnerability.Malicious.Trojan
Vulnerability.PathTraversal
Vulnerability.Validation.EncodingRequired
Vulnerability.Validation.EncodingRequired.Struts
```

Vulnérabilités CWE SANS Top 25 2010

Ce filtre porte principalement sur les types de vulnérabilité liés à la liste des 25 erreurs logicielles les plus dangereuses, *CWE/SANS TOP 25 Most Dangerous Software Errors* pour 2010.

Pour en savoir plus sur la liste *2011 CWE/SANS Top 25 Most Dangerous Software Errors*, voir http://cwe.mitre.org/top25/.

Communications externes

Ce filtre correspond aux constatations de menaces externes à l'application et traversant le réseau. Il trouve tout ce qui provient d'une source `Technology.Communications`.

Faible gravité et message d'information

Ce filtre contient les constatations dont la gravité est faible et le message informationnel. Toutes les classifications (Définitive, Suspectée et Couverture d'examen) sont incluses.

Bruit - Qualité

Avec ce filtre, les résultats incluent uniquement les types de vulnérabilité qui sont liés aux pratiques de codage de qualité.

OWASP Mobile Top 10 Vulnerabilities

Ce filtre porte principalement sur les types de vulnérabilité liés à la liste des 10 premières éditions candidates mobiles OWASP (Open Web Application Security Project) v1.0.

Pour plus d'informations sur OWASP, voir https://www.owasp.org/index.php/Main_Page. Des liens vers divers documents et risques de sécurité OWASP sont disponibles sur le site https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project.

OWASP Top 10 2010 Vulnerabilities

Ce filtre porte principalement sur les types de vulnérabilité liés à la liste des 10 projets OWASP (Open Web Application Security Project) 2010.

Pour plus d'informations sur OWASP, voir https://www.owasp.org/index.php/Main_Page. Des liens vers divers documents et risques de sécurité OWASP sont disponibles sur le site https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project.

OWASP Top 10 2013 Vulnerabilities

Ce filtre porte principalement sur les types de vulnérabilité liés à la liste des 10 projets OWASP (Open Web Application Security Project) 2013.

Pour plus d'informations sur OWASP, voir https://www.owasp.org/index.php/Main_Page. Des liens vers divers documents et risques de sécurité OWASP sont disponibles sur le site https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project.

Vulnérabilités PCI Data Security Standard

Ce filtre porte principalement sur les types de vulnérabilité liés à PCI DSS (Payment Card Industry Data Security Standard) version 3.2 standard.

Pour plus d'informations, voir https://www.pcisecuritystandards.org/security_standards/index.php.

Constatations de couverture d'examen

Avec ce filtre, les résultats incluent uniquement les constatations de couverture d'examen (voir «Classifications», à la page 21 pour plus d'informations).

Vulnérabilités ciblées - `EncodingRequired` pour sources HTTP

Ce filtre porte principalement sur les constatations issues des catégories de vulnérabilités `Validation.EncodingRequired` et `Validation.EncodingRequired.Struts`. Seules les constatations provenant de la source `Technology.Communications.HTTP` sont incluses. Les constatations sont limitées aux gravités Elevée et Moyenne avec les classifications Définitive ou Suspectée.

Vulnérabilités ciblées - Validation requise pour collecteurs C/C++

Ce filtre concerne les vulnérabilités `Validation.Required` pour un ensemble de collecteurs C et C++ connus. Les constatations sont limitées aux gravités Elevée et Moyenne avec les classifications Définitive ou Suspectée.

Sources sécurisées

Ce filtre considère que les données provenant de certaines sources, par exemple des objets de session ou des attributs de demande, sont sûres.

Vulnérabilités sans trace

Ce filtre permet d'afficher les vulnérabilités qui ne contiennent pas de traces.

Filtres prédéfinis AppScan Source (versions 8.7.x et antérieures)

Cette rubrique répertorie les filtres prédéfinis inclus dans AppScan Source versions 8.7.x et antérieures.

Pour accéder à ces filtres, suivez les instructions contenues dans «Restauration des filtres prédéfinis archivés», à la page 131.

! - Le minimum vital

Ce filtre correspond aux constatations entrant dans les catégories de vulnérabilités les plus dangereuses. Seules sont incluses les constatations des menaces qui proviennent d'un réseau de communication externe. Ce filtre pointe du doigt les constatations à haut risque. Il inclut les catégories spécifiques suivantes :

```
Vulnerability.BufferOverflow
Vulnerability.BufferOverflow.FormatString
Vulnerability.PathTraversal
Vulnerability.CrossSiteScripting
Vulnerability.CrossSiteScripting.Reflected
Vulnerability.CrossSiteScripting.Stored
Vulnerability.Injection
Vulnerability.Injection.LDAP
Vulnerability.Injection.SQL
Vulnerability.Injection.OS
Vulnerability.Injection.XML
Vulnerability.Injection.XPath
```

Haute priorité - Communications externes

Ce filtre correspond aux constatations de menaces externes à l'application et traversant le réseau. Il trouve tout ce qui provient d'une source `Technology.Communications`.

Haute priorité - Types importants

Ce filtre correspond aux constatations entrant dans les catégories de vulnérabilités les plus dangereuses, telles que `CrossSiteScripting` et `Injection.SQL`. Il inclut les catégories spécifiques suivantes :

```
Vulnerability.AppDOS
Vulnerability.Authentication.Credentials.Unprotected
Vulnerability.Authentication.Entity
Vulnerability.BufferOverflow
Vulnerability.BufferOverflow.FormatString
Vulnerability.CrossSiteScripting
Vulnerability.CrossSiteScripting.Reflected
Vulnerability.CrossSiteScripting.Stored
Vulnerability.Injection
Vulnerability.Injection.LDAP
Vulnerability.Injection.OS
Vulnerability.Injection.SQL
Vulnerability.Injection.XML
Vulnerability.Injection.XPath
Vulnerability.PathTraversal
```

Basse priorité - Code de test

Ce filtre contient les constatations issues d'un code de test. Il inclut les types spécifiques suivants :

```
Vulnerability.Quality.TestCode
```

Bruit - Opérations de copie conforme

Ce filtre contient les constatations relatives aux opérations de copie conforme. Une opération de copie conforme se produit lorsque des données proviennent d'une source sécurisée ou non, mais que les actions effectuées sur les données sont sécurisées.

Les schémas suivants sont recherchés :

```
Technology.Database --> Vulnerability.Injection.SQL
Mechanism.SessionManagement --> Mechanism.SessionManagement
Technology.XML, Technology.XML.DOM, Technology.XML.Schema,
Technology.XML.XPath --> Vulnerability.AppDOS.XML,
Vulnerability.Injection.XML
```

Bruit - Problèmes de consignation

Ce filtre contient les constatations en rapport avec le traitement des erreurs. Ces constatations émanent d'une routine de traitement d'erreurs et vont vers un mécanisme de consignation. Le schéma suivant est recherché :

```
Mechanism.ErrorHandling -->
Vulnerability.Logging, Vulnerability.Logging.Forge, Vulnerability.Logging.Required
```

Bruit - Faible gravité

Ce filtre contient les constatations dont la gravité est faible. Toutes les classifications sont incluses.

Bruit - Source fiable

Ce filtre contient les constatations issues d'une source de confiance. Seules les constatations dont la source est `java.lang.System.getProperty.*` sont incluses dans ce filtre.

Restauration des filtres prédéfinis archivés

Il est possible de rajouter au produit des filtres prédéfinis fournis dans AppScan Source avant la version 8.8 en suivant la procédure de cette tâche. Une fois restaurés sur une seule machine, ils peuvent être gérés de la même manière que les filtres que vous créez (par exemple, vous pouvez les partager entre plusieurs clients).

Pourquoi et quand exécuter cette tâche

Les filtres prédéfinis archivés se trouvent dans `<data_dir>\archive\filters` (où `<rép_données>` est l'emplacement de vos données de programme AppScan Source, comme décrit dans «Installation et emplacements des fichiers de données utilisateur», à la page 292).

Procédure

1. Dans `<data_dir>\archive\filters`, recherchez le ou les filtres que vous souhaitez restaurer (les filtres AppScan Source portent l'extension de fichier `.off`).
2. Copiez le ou les filtres dans `<data_dir>\scanner_filters`.
3. Redémarrez AppScan Source.

Que faire ensuite

Pour savoir comment gérer les filtres (notamment les filtres archivés que vous avez restaurés), voir «Création et gestion de filtres depuis la vue Editeur de filtre», à la page 133.

Création et gestion de filtres

AppScan Source propose plusieurs méthodes pour la création et l'utilisation des filtres. L'éditeur de filtre, la vue principale pour la création de filtres, propose un ensemble de règles robustes pouvant être définies manuellement, puis enregistrées

dans un filtre. Il fournit également un mécanisme afin de gérer les filtres que vous avez créés, en vous permettant de les modifier ou de les supprimer aisément. Vous pouvez également filtrer le tableau des constatations depuis les vues présentant des représentations graphiques de celles-ci, puis enregistrer ces filtres depuis la vue Editeur de filtre. Lorsque vous créez un filtre, les autres vues sont actualisées en reflétant les propriétés du filtre.

- «Création, gestion et application de filtres * depuis la vue Editeur de filtre»
- «Filtrage depuis les vues Récapitulatif de l'évaluation et Matrice de vulnérabilités»
- «Création de filtres depuis la vue Sources et collecteurs»

Création, gestion et application de filtres * depuis la vue Editeur de filtre

Cette vue vous permet de créer des filtres en spécifiant des règles de filtrage. Les filtres créés dans cette vue peuvent être sauvegardés, modifiés ou supprimés. Une fois qu'un filtre est créé dans cette vue, il peut être appliqué via le menu déroulant de la vue. Voir «Création et gestion de filtres depuis la vue Editeur de filtre», à la page 133.

Dans AppScan Source for Analysis, vous pouvez partager des filtres que vous avez créés dans AppScan Enterprise Server, et accéder à des filtres partagés par d'autres. Dans AppScan Source for Development, vous pouvez accéder aux filtres partagés si vous êtes en mode serveur.

Remarque : Dans AppScan Source for Development (plug-in Visual Studio), cette vue fait partie de la fenêtre Edition de filtres.

Filtrage depuis les vues Récapitulatif de l'évaluation et Matrice de vulnérabilités

Remarque :

- La vue Récapitulatif de l'évaluation n'est pas disponible sous macOS.
- Dans AppScan Source for Development (plug-in Visual Studio), ces vues font partie de la fenêtre Edition de filtres.

Ces vues offrent une représentation graphique des constatations. Dans ces vues, les constatations sont regroupées de diverses manières. Ces groupes peuvent être sélectionnés de sorte à filtrer le tableau des constatations afin de n'afficher que celles appartenant au(x) groupe(s) sélectionné(s). Le filtrage opéré à l'aide de cette méthode se reflète automatiquement dans la vue Editeur de filtre, depuis laquelle vous pouvez sauvegarder les paramètres du filtre.

Création de filtres depuis la vue Sources et collecteurs

Remarque : La vue Sources et collecteurs n'est pas disponible dans AppScan Source for Development (plug-in Visual Studio).

La vue Sources et collecteurs permet d'afficher et de filtrer des constatations en fonction d'une trace des entrées et sorties. Le filtrage effectué ici peut être sauvegardé directement depuis cette vue. Pendant la création du filtre, vous pouvez l'appliquer immédiatement aux résultats de l'examen.

Voir «Création de filtres depuis la vue Sources et collecteurs», à la page 134.

Création et gestion de filtres depuis la vue Editeur de filtre

Dans cette vue, vous pouvez créer, éditer, sauvegarder, supprimer et gérer des filtres. Si vous utilisez AppScan Source for Analysis, vous pouvez partager des filtres et accéder à des filtres qui ont été partagés par d'autres. Dans AppScan Source for Development, vous pouvez accéder aux filtres partagés si vous utilisez le mode serveur et que vous êtes connecté à AppScan Enterprise Server.

Procédure

1. Dans la barre d'outils de l'«Vue Editeur de filtre», à la page 289, cliquez sur **Nouveau**. Le nouveau filtre porte le libellé `Untitled<-nombre>` (le premier filtre sans nom est libellé `Untitled`, le suivant `Untitled-1`, etc.).

   Remarque : Dans AppScan Source for Development (plug-in Visual Studio), cette vue fait partie de la fenêtre Edition de filtres.
2. Développez les catégories et sélectionnez les critères de votre choix pour le filtre.
3. Cliquez sur **Sauvegarder** ou sur **Sauvegarder sous**.
4. Attribuez un nom au filtre et cliquez sur **OK**. Le nouveau nom du filtre remplace son libellé `Untitled<-nombre>` antérieur dans la liste des filtres.

Que faire ensuite

Pour appliquer le filtre, sélectionnez-le dans le menu déroulant de la vue Editeur de filtre.

Remarque : Les filtres qui sont appliqués hors de la vue Matrice de vulnérabilités peuvent ne pas affecter la vue Matrice de vulnérabilités. Le bouton de la barre d'outils **Afficher le nombre de constatations filtrées** de la vue Matrice de vulnérabilités doit être sélectionné pour que le filtre soit reflété dans la vue Matrice de vulnérabilités.

Les filtres peuvent être gérés directement depuis la vue Editeur de filtre en sélectionnant le filtre dans la liste, puis en opérant sur celui-ci, ou en cliquant sur **Gérer les filtres** pour ouvrir la boîte de dialogue correspondante, laquelle affiche la liste des filtres sauvegardés.

- **Modification de filtres** : Sélectionnez le filtre depuis la vue Editeur de filtre ou depuis la boîte de dialogue Gestion de filtres, puis modifiez les règles de filtrage et sauvegardez vos modifications.

  Remarque : Les filtres intégrés ne peut être ni modifiés ni supprimés.
- **Suppression de filtres** : Sélectionnez le filtre depuis la vue Editeur de filtre ou depuis la boîte de dialogue Gestion de filtres, puis cliquez sur **Supprimer**. Depuis la boîte de dialogue Gestion de filtres, vous pouvez sélectionner plusieurs filtres, puis cliquer sur **Supprimer** pour les supprimer en une seule opération.
- **Création d'un filtre à partir d'un autre** : Vous pouvez modifier un filtre, puis cliquer sur **Sauvegarder sous** pour enregistrer le filtre modifié sous un autre nom. Ceci vous permet de créer un nouveau filtre en vous basant sur les paramètres d'un filtre existant. Vous pouvez effectuer cette opération depuis la vue Editeur de filtre ou la boîte de dialogue Gestion de filtres.

  Conseil : Il est également possible d'ouvrir un filtre et d'utiliser l'action **Sauvegarder sous** pour le sauvegarder sous un nouveau nom. Vous pouvez

ensuite ouvrir le nouveau filtre et le modifier. En choisissant cette méthode, vous pouvez créer un filtre à partir de l'un des filtres intégrés.

- **Rétablissement des paramètres de filtrage** : Si vous avez modifié les propriétés d'un filtre et désirez annuler ces modifications, cliquez sur **Restaurer** pour rétablir les paramètres tels que lors de leur dernier enregistrement. Vous pouvez effectuer cette opération depuis la vue Editeur de filtre ou la boîte de dialogue Gestion de filtres. Dans la boîte de dialogue, si les modifications de plusieurs filtres n'ont pas été sauvegardées, le fait de cliquer sur **Restaurer** rétablira les paramètres enregistrés de tous les filtres sélectionnés dont les modifications n'ont pas encore été sauvegardées.
- **Partage de filtres** (AppScan Source for Analysis seulement) : Pour créer un filtre partagé, ouvrez un filtre dans l'éditeur de filtre et cliquez sur **Partager le filtre** dans la barre d'outils de la vue Editeur de filtre.

  Remarque : Pour modifier, supprimer ou créer des filtres partagés, vous devez disposer de l'autorisation **Gérer les filtres partagés**. Pour plus d'informations sur la définition des autorisations, voir le manuel *IBM Security AppScan Source - Guide d'installation et d'administration*.

Filtrage depuis la matrice des vulnérabilités

Cette vue affiche le nombre total de constatations pour toutes les applications couvertes par l'examen. Ces constatations sont regroupées dans la matrice par niveau de gravité. Vous pouvez créer des filtres en sélectionnant ces groupes de constatations.

Pourquoi et quand exécuter cette tâche

Lorsque vous sélectionnez des constatations groupées dans la «Vue Matrice de vulnérabilités», à la page 289, le tableau des constatations est modifié en conséquence afin d'afficher uniquement celles sélectionnées dans cette matrice.

Remarque : Dans AppScan Source for Development (plug-in Visual Studio), cette vue fait partie de la fenêtre Edition de filtres.

Remarque : Les constatations sur la **Qualité** et celles classées avec le niveau de gravité **Info** ne sont pas incluses dans la vue Matrice de vulnérabilités.

Procédure

1. Depuis la vue Matrice de vulnérabilités, sélectionnez la section que vous désirez voir figurer dans le tableau des constatations. Par exemple, pour n'afficher dans le tableau que les constatations de sécurité **suspectées** de gravité **élevée**, sélectionnez la section correspondante dans la matrice. Les résultats filtrés apparaissent alors dans le tableau des constatations.
2. Les opérations de filtrage entraînent la transposition dans la vue Editeur de filtre des paramètres de règles de filtrage de la sélection effectuée dans la Matrice de vulnérabilités. Ce filtre peut être sauvegardé depuis la vue Editeur de filtre (pour plus d'informations sur les paramètres et la sauvegarde des règles de filtrage, voir «Création et gestion de filtres depuis la vue Editeur de filtre», à la page 133).

Création de filtres depuis la vue Sources et collecteurs

Procédure

1. Ouvrez la vue Sources et collecteurs, ou accédez-y.

2. Cette vue comporte trois sections. La section Tableau des constatations présente les constatations pour les sources, les collecteurs et les noeuds intermédiaires que vous avez choisi d'afficher dans les deux autres sections. Ceci est décrit dans la rubrique «Vue Sources et collecteurs», à la page 283.
3. Après avoir configuré le tableau des constatations afin d'afficher celles qui vous intéressent, cliquez sur **Créer un nouveau filtre basé sur la source sélectionnée, le collecteur et les noeuds intermédiaires**.
4. Dans la boîte de dialogue Création de filtre, procédez comme suit :
   - Spécifiez un nom pour le filtre dans la zone **Nom**.
   - Sélectionnez **Appliquer ce filtre immédiatement** de sorte que ce filtre soit appliqué à tous les tableaux de constatations de votre évaluation. La sélection de cette case revient à sélectionner un filtre dans la vue Editeur de filtre. Elle définit le filtre principal actif, ce qui affecte toutes les vues (par exemple, les vues Matrice de vulnérabilités et Constatations).

     Remarque : Les filtres qui sont appliqués hors de la vue Matrice de vulnérabilités peuvent ne pas affecter la vue Matrice de vulnérabilités. Le bouton de la barre d'outils **Afficher le nombre de constatations filtrées** de la vue Matrice de vulnérabilités doit être sélectionné pour que le filtre soit reflété dans la vue Matrice de vulnérabilités.
   - Si les constatations écartées par le filtrage ne sont pas pertinentes à votre travail actuel, vous pouvez les éliminer de l'évaluation en cochant la case **Créer un filtre d'application qui exclut ces constatations**. La sélection de cette case à cocher ajoute le nouveau filtre en tant que filtre d'exclusion dans les propriétés de l'application (pour afficher la liste des filtres d'exclusion, cliquez sur l'onglet Exclusions dans la vue Propriétés de l'application). Lors des examens ultérieurs de l'application, les constatations correspondant à ce filtre seront mentionnées dans la vue Constatations exclues et non plus dans la vue Constatations.
5. Cliquez sur **OK** pour filtrer ou exclure les constatations.

Application de filtres

Des filtres peuvent être appliqués avant ou après l'examen. Pour appliquer des filtres après l'examen, utilisez l'Editeur de filtre ou une autre vue qui vous permet d'appliquer des filtres. Pour appliquer des filtres avant l'examen, définissez un filtre global à l'aide d'une configuration d'examen. Lorsque vous appliquez des filtres avant l'examen, vous ne pouvez pas afficher des constatations non filtrés ou supprimer le filtre sans effectuer un nouvel examen.

Application des filtres avant l'examen

Voir «Application globale des filtres», à la page 136 pour en savoir plus sur la définition d'un filtre global - ou «Gestion des configurations d'examen», à la page 90 pour en savoir plus sur la définition de filtres dans les configurations d'examen.

Application des filtres après l'examen

Lorsque vous sélectionnez un filtre dans la vue Editeur de filtre, il est automatiquement appliqué à la liste de constatations. D'autres vues fournissent des actions de filtrage, comme décrit dans «Création et gestion de filtres», à la page 131.

Application globale des filtres

Il est possible d'appliquer les filtres déjà créés à toutes les applications, à des applications individuelles et à des projets individuels. Les filtres globaux sont appliqués dans la vue Propriétés, dans laquelle vous pouvez spécifier leur type d'application (directement ou inversé). Par exemple, si vous souhaitez définir un filtre global pour une application, sélectionnez-le dans la vue Explorateur, puis ouvrez sa vue Propriétés (via le menu **Vue** ou en cliquant avec le bouton droit de la souris sur l'application, puis en cliquant sur **Propriétés**).

Avant de commencer

Si vous définissez un filtre pour toutes les applications ou pour un projet individuel, utilisez l'onglet Filtres de la vue Propriétés. Si vous définissez un filtre pour une application individuelle, utilisez l'onglet Exclusions et filtres de la vue Propriétés.

Procédure

1. Dans la section Filtres de l'onglet, cliquez sur **Ajouter**.
2. Dans la boîte de dialogue Sélection de filtre, sélectionnez le filtre que vous souhaitez appliquer globalement.
3. Facultatif : Si vous souhaitez appliquer l'inverse du filtre (au lieu d'appliquer le filtre directement), sélectionnez **Inverser le filtre**.
4. Cliquez sur **OK** pour fermer la boîte de dialogue Sélection de filtre.
5. Après avoir ajouté les filtres, enregistrez les modifications dans la vue Propriétés.

Détermination des filtres appliqués

Il est possible d'appliquer des filtres globalement aux applications et aux projets avant leur examen, ou de les appliquer aux évaluations après l'examen. Pour vous permettre de déterminer rapidement la façon dont les filtres ont été appliqués aux constatations dans une évaluation, AppScan Source fournit un indicateur de filtre en bas du plan de travail principal.

Si aucun filtre n'a été appliqué, l'indicateur de filtre situé en bas du plan de travail indique que les **constatations ne sont pas filtrées**.

Si des filtres ont été appliqués, l'indicateur se transforme en un lien indiquant que les **constatations sont filtrées**. Si vous sélectionnez ce lien, un message s'affiche et vous permet de déterminer la façon dont les filtres ont été appliqués :

- **Les filtres de durée d'examen** sont des filtres globaux appliqués aux applications et aux projets :
  - Si l'évaluation est le résultat de l'examen d'une application ou d'un projet qui ne comporte pas de filtres configurés, le message indique qu'aucun filtre de durée d'examen n'a été appliqué.
  - Si l'application ou le projet examiné comporte des filtres configurés, ces filtres sont répertoriés par nom.
  - Dans certains cas, AppScan Source détecte que des filtres de durée d'examen ont été appliqués, mais l'évaluation ne contient pas d'information les concernant. Par exemple, cela peut être le cas lorsqu'une ancienne évaluation est ouverte.
- **Les filtres actuels** sont des filtres qui ont été appliqués aux constatations après l'examen. Le message indique si des filtres actuels ont été appliqués ou non. Si

des filtres ont été appliqués, un lien de **réinitialisation** est disponible. Lorsque ce lien est sélectionné, les filtres actuels sont supprimés des constatations.

Triage avec exclusions

Après un examen, vous pouvez décider que certaines constatations ne sont pas pertinentes pour votre travail actuel et que vous ne désirez pas qu'elles soient visibles dans le tableau des constatations lors du triage de ces résultats. Ces *exclusions* (ou constatations exclues) n'apparaissent plus dans la vue Constatations et les métriques des évaluations sont immédiatement actualisées avec les résultats modifiés. Le filtrage et les exclusions de groupements ajoutés à une configuration ne prennent effet que lors des examens ultérieurs.

Portée des exclusions

Les exclusions peuvent s'appliquer à toutes les applications (globales), à des applications individuelles ou à des projets.

- Les **exclusions globales** s'appliquent à tous les examens.
- Les **exclusions d'application** s'appliquent uniquement à un examen effectué vis à vis d'une application spécifique et des projets correspondants.
- Les **exclusions de projet** s'appliquent aux constatations présentes dans un projet spécifique.

Remarque : Les exclusions affectent les métriques des évaluations, notamment au nombre total de constatations (les constatations exclues ne sont pas incluses dans les mesures d'évaluation).

Exclusions globales

Vous pouvez stocker ou accéder à une exclusion globale depuis n'importe quelle application AppScan Source for Analysis et ces exclusions s'appliquent à tous les examens. Seuls les filtres partagés peuvent devenir des filtres globaux.

Exclusions d'application et de projet

Les exclusions de groupement s'appliquent uniquement à une application. Une exclusion de filtre peut s'appliquer à un application ou à un projet. Les exclusions appliquées aux applications et aux projets peuvent être partagées ou locales.

Spécification d'exclusions

Des constatations peuvent être marquées en tant qu'exclusions depuis un Tableau des constatations ou la vue Propriétés. Les exclusions peuvent être composées de constatations individuelles, de filtres ou de groupements. Généralement, les exclusions créées depuis un Tableau des exclusions prennent effet immédiatement. Celles créées dans la vue Propriétés prennent effet à l'examen suivant.

Une exclusion s'applique immédiatement à l'application à l'issue d'une des procédures suivantes :

- Sélection d'une ou de plusieurs constatations, clic avec le bouton droit de la souris sur votre sélection, puis sélection de **Exclure des constatations** dans le menu.
- Ajout d'une ou de plusieurs constatations à un groupement actuellement exclu, y compris le *groupement exclu*.

- Suppression d'une ou de plusieurs constatations d'un groupement exclu auparavant, y compris le *groupement exclu*.
- Suppression d'un groupement exclu.

Une exclusion ne s'applique pas immédiatement à l'application dans les circonstances suivantes :

- Ajout d'un groupement en tant qu'exclusion.
- Ajout d'un filtre en tant qu'exclusion.
- Modification d'une constatation de sorte à ce qu'elle corresponde aux critères d'un filtre exclu.
- Modification d'une constatation de sorte à ce qu'elle ne corresponde plus aux critères d'un filtre exclu.

Marquage de constatations en tant qu'exclusions dans un tableau de constatations

Procédure

1. Dans le tableau des constatations, sélectionnez la constatation (ou le groupe de constatations) qui n'ont pas d'importance ou que vous ne désirez pas voir affichée.
2. Cliquez avec le bouton droit de la souris sur votre sélection et sélectionnez **Exclure des constatations** dans le menu. Les exclusions prennent immédiatement effet. Les constatations exclues n'apparaissent plus dans le tableau et les métriques sont immédiatement mises à jour.

Résultats

Pour afficher des constatations exclues, ouvrez la vue Constatations exclues. Ces dernières apparaissent également dans un groupement intitulé **Groupement exclu**.

Pour ajouter des constatations qui ont été exclues, suivez les instructions décrites dans «Nouvelle inclusion de constatations qui ont été marquées comme des exclusions».

Nouvelle inclusion de constatations qui ont été marquées comme des exclusions

Les constatations relevant d'exclusions figurent dans la vue Constatations exclues. Depuis cette vue, vous pouvez réintégrer les constatations exclues.

Procédure

1. Dans la vue Constatations exclues, sélectionnez celle(s) que vous désirez réintégrer.
2. Cliquez avec le bouton droit de la souris sur votre sélection et sélectionnez **Inclure des constatations** dans le menu.

Résultats

Les constatations incluses sont de nouveau ajoutées dans l'évaluation et les tableaux et métriques de constatations sont immédiatement mis à jour pour répercuter les constatations qui ont été de nouveau incluses. Ces constatations n'apparaissent plus dans la vue Constatations exclues.

Remarque : Dans AppScan Source for Analysis, vous pouvez également ré-inclure des constatations exclues depuis la vue groupée **Exclusions** en retirant de ce groupement des exclusions ou en les transférant vers un nouveau groupement ne faisant pas l'objet d'une exclusion.

Exemple : Spécification d'exclusions dans un filtre

Les critères de filtre déterminent si celui-ci doit exclure les constatations correspondant ou ne correspondant pas au filtre.

Cet exemple indique comment créer des filtres qui excluent des constatations :

- «Exemple : Filtrage et exclusion d'API»

Exemple : Filtrage et exclusion d'API

Un scénario de triage usuel peut intervenir de bonne heure dans le processus de triage lorsque vous désirez attribuer des priorités à vos constatations et en exclure certaines. Vous pourriez, par exemple, convenir que trois API ne constituent pas une menace et vouloir par conséquent les exclure des examens ultérieurs.

Procédure

1. Dans la section API de l'éditeur de filtre, cliquez sur **Ajouter** et sélectionnez trois API.
2. Sélectionnez **Restreindre à**.
3. Sauvegardez le filtre en lui attribuant un nom.
4. Revenez à la perspective Configuration et, dans la vue Explorateur, sélectionnez le projet (ou l'application).
5. Dans la vue Propriétés, affectez au comportement du filtre la valeur **Inversé** (dans la boîte de dialogue Sélection de filtre, sélectionnez **Inverser le filtre**).
6. Effectuez un nouvel examen. Les API du filtre ne figurent plus dans les constatations.

Résultats

Toujours avec ce même exemple, vous pourriez vouloir afficher uniquement les constatations incluses dans le filtre. Dans ce cas, lors de l'ajout du filtre à la liste, ne sélectionnez pas l'option **Inverser le filtre**. A l'issue de la nouvel examen, seuls les constatations figurant dans le filtre seront affichées.

Spécification d'exclusions de groupement depuis la vue Propriétés

Une exclusion de groupement élimine les constatations figurant dans le groupement. Vous pouvez exclure des groupements des applications.

Procédure

1. Créez un groupement comme décrit dans la rubrique «Création de groupements», à la page 140.
2. Depuis la vue Explorateur, sélectionnez l'application à associer au groupement.
3. Depuis la vue Propriétés, sélectionnez l'onglet **Exclusions**.
4. Cliquez sur **Ajouter un groupement** et, dans la boîte de dialogue Sélection de groupement, sélectionnez le groupement contenant les constatations à exclure pour l'application.
5. Cliquez sur **OK**.

6. Effectuez un nouvel examen. Les constatations groupées n'apparaissent plus dans la table de constatations.

Triage avec des groupements

Les groupements, lesquels comportent des caractéristiques uniques, peuvent être importants pour votre processus de triage.

Pourquoi et quand exécuter cette tâche

- Les groupements peuvent être exportés vers des systèmes de suivi des défauts en tant que défaut unique ou en tant que défaut distinct pour chaque constatation présente dans le groupement.
- Les groupements peuvent être la base de la génération de rapports.
- Les groupements sont rattachés à des applications.

Important : Une constatation ne peut exister que dans un seul groupement à la fois. Lorsque vous déplacez une constatation d'un groupement vers un autre, elle est supprimée du premier groupement.

Cet exemple illustre un triage simple avec des groupements :

Procédure

1. Examinez le code source.
2. Créez un groupement nommé `A résoudre en priorité`.
3. Ajoutez des constatations critiques au groupement.
4. Ajoutez des annotations aux constatations du groupement.
5. Soumettez le groupement ou les constatations au système de suivi des défauts ou soumettez-les par courrier électronique à d'autres développeurs.
6. Résolvez les problèmes.

Création de groupements

La création de groupements s'effectue depuis la vue Groupements ou depuis une vue contenant un tableau Constatations. Vous pouvez ajouter des constatations à un groupement existant ou à un nouveau groupement.

Ces rubriques décrivent la création de groupements dans les vues Groupements et Constatations :

- «Création d'un nouveau groupement dans la vue Groupements», à la page 141
- «Création d'un nouveau groupement dans la vue Constatations», à la page 141

Remarque : Pour pouvoir créer des groupements pour une évaluation, l'application qui a été analysée pour créer l'évaluation doit être chargée dans AppScan Source for Analysis. Si vous ouvrez une évaluation pour une application qui n'a pas été chargée, les actions de création de groupement ne sont pas disponibles.

Une fois que vous avez créé un ou plusieurs groupements, l'action **Masquer les constatations groupées** de la vue Constatations ( ) vous permet de basculer l'affichage des constatations groupées dans la vue. Cette action masque les constatations dans tous les groupements inclus que vous avez créés. Ce paramètre n'affecte pas l'affichage des constatations présentes dans les groupements exclus. Ces constatations ne sont jamais affichées dans la vue Constatations.

Création d'un nouveau groupement dans la vue Groupements

Procédure

1. Depuis la vue Groupements, cliquez sur **Nouveau groupement** dans la barre d'outils.
2. Attribuez un nom au groupement et cliquez sur **OK**. Le nom du groupement apparaît dans la vue Groupements.
3. Pour ajouter des constatations au groupement, suivez les instructions fournies dans «Ajout de constatations à des groupements existants».

Création d'un nouveau groupement dans la vue Constatations

Procédure

1. Sélectionnez dans la vue Constatations des éléments à ajouter à un groupement.
2. Cliquez avec le bouton droit de la souris sur votre sélection et sélectionnez dans le menu **Ajouter au groupement** > **Nouveau**.
3. Attribuez un nom au groupement et cliquez sur **OK**.

Ajout de constatations à des groupements existants

Pourquoi et quand exécuter cette tâche

Vous pouvez ajouter des constatations à un groupement depuis plusieurs vues :

- Vue Constatations
- Vue Constatations exclues
- Vue Constatations corrigées/modifiées
- Vue Constatations manquantes
- Vue Rapport
- Constatation détaillée

Conseil : Vous pouvez déplacer une constatation depuis la vue Constatations vers la vue Groupements à l'aide d'une opération déplacer/déposer.

Pour ajouter des constatations à un groupement, procédez comme suit :

Procédure

1. Sélectionnez les constatations que vous souhaitez ajouter au groupement.
2. Cliquez avec le bouton droit de la souris sur votre sélection et sélectionnez **Ajouter au groupement** > **<nom du groupement>** (cette liste contient les cinq groupements créés le plus récemment) ou depuis le menu **Ajouter au groupement** > **Sélectionner**.
3. Si vous sélectionnez l'option **Ajouter au groupement** > **Sélectionner**, sélectionnez le groupement auquel ajouter les constatations dans la boîte de dialogue Sélection de groupement, puis cliquez sur **OK**.

Déplacement de constatations entre groupements

Procédure

1. Dans la vue Groupements, ouvrez le groupement qui contient les constatations à déplacer.

2. Sélectionnez la ou les constatations que vous souhaitez déplacer, puis exécutez l'une des actions suivantes :
   - Cliquez sur **Déplacer vers un groupement** ou **Déplacer vers un nouveau groupement** dans la barre d'outils de la vue. Sélectionnez ensuite le groupement vers lequel vous voulez déplacer la constatation ou créez un nouveau groupement pour la constatation.
   - Cliquez avec le bouton droit de la souris sur votre sélection, puis cliquez sur **Déplacer vers un groupement**. Cette opération entraîne l'affichage d'un menu permettant de sélectionner un groupement dans une liste ou une boîte de dialogue ou de créer un groupement dans lequel déplacer la sélection.

Résultats

Remarque : Les constatations déplacées ou ajoutées dans un groupement exclu ne seront pas exclues de l'évaluation en cours. Pour marquer des constatations comme étant exclues dans l'évaluation en cours, utilisez l'action **Exclure des constatations**.

Affichage des constatations d'un groupement

Lorsque vous ajoutez des constatations à un groupement, celles-ci figurent sous forme de ligne dans le groupement. Si vous ouvrez le groupement, vous pouvez voir toutes les constatations qu'il contient.

Pourquoi et quand exécuter cette tâche

Les constatations de plusieurs projets dans les groupements peuvent figurer différemment. Une constatation dans un groupement figure en vert et en italiques si elle n'était pas présente lors du dernier examen.

Examinez l'exemple suivant d'une application X.

Procédure

1. L'application X contient les projets A et B.
2. Examinez l'application X.
3. Créez un groupement contenant les constatations provenant du projet A et du projet B.
4. Examinez le projet B. Dans la vue Groupements, les constatations du projet B apparaissent et celles du projet A figurent en vert et en italiques.

Résultats

Une constatation figurant avec une couleur verte et en italiques correspond à une *constatation corrigée/manquante*. Une constatation corrigée manquante correspond à une constatation présente dans un groupement mais absente de l'évaluation actuelle. Une constatation est identifiée en tant que corrigée/manquante étant donné qu'elle été résolue, retirée ou bien que son fichier source n'a pas été examiné. Dans la vue Groupements, la colonne **Exclu** identifie si le groupement a été exclu.

Sauvegarde de groupements dans un fichier

Vous pouvez sauvegarder un groupement dans un fichier pour l'ouvrir dans AppScan Source for Development. Un groupement vous permet également d'importer un instantané de constatations depuis AppScan Source for Analysis vers AppScan Source for Remediation.

Procédure

1. Effectuez l'une des actions suivantes :
   a. Dans la vue Groupements, sélectionnez le groupement et cliquez sur **Sauvegarder le groupement dans un fichier** dans la barre d'outils.
   b. Ouvrez le groupement et cliquez sur **Sauvegarder le groupement dans un fichier** dans la barre d'outils.
2. Sélectionnez le répertoire dans lequel sauvegarder le fichier du groupement.
3. Attribuez un nom au fichier de groupement (`<nom_fichier>.ozbdl`).

Résultats

Pour ouvrir un groupement sauvegardé :

- Dans AppScan Source for Development (plug-in Eclipse), sélectionnez **Analyse de sécurité** > **Ouvrir** > **Ouvrir un groupement**.
- Dans AppScan Source for Development (plug-in Microsoft Visual Studio), sélectionnez **IBM Security AppScan Source** > **Ouvrir un groupement**.
- Dans AppScan Source for Analysis, cliquez sur **Ouvrir un groupement** dans la barre d'outils de la vue Groupements.

Conseil : Sur les systèmes Windows, cliquez deux fois sur le fichier de groupement dans la vue Groupements pour l'ouvrir dans AppScan Source for Analysis ou AppScan Source for Development.

Soumission de groupements au système de suivi des défauts et par courrier électronique

Les constatations figurant dans des groupements peuvent être soumises au système de suivi des défauts de votre entreprise ou envoyées par e-mail. Une fois ces constatations placées dans un groupement, vous pouvez les soumettre en tant que bogues pour leur résolution par un développeur.

Procédure

1. Ouvrez le groupement.
2. Cliquez sur la flèche vers le bas du bouton de barre d'outils **Soumettre un groupement pour suivi des défauts** et sélectionnez ensuite le système de suivi des défauts.

   Remarque : En fonction de votre système de suivi des défauts, il peut s'avérer nécessaire de modifier les préférences Système de suivi des défauts avant de soumettre le groupement.

   Dans la barre d'outils Groupement, vous pouvez également cliquer sur **Envoi du groupement par courrier électronique** pour envoyer le groupement à d'autres (les préférences de courrier électronique doivent avoir été configurées précédemment).
3. Renseignez les boîtes de dialogue de configuration qui s'affichent. Celles-ci varient en fonction du système de suivi des défauts que vous avez choisi. Elles sont décrites dans la section de l'aide relative à *AppScan Source for Analysis et au système de suivi des défauts*.

Ajout de notes à des groupements

Procédure

1. Dans la vue Groupements, sélectionnez le groupement à annoter.

2. Cliquez sur **Ajouter des notes** dans la barre d'outils Groupement ou cliquez avec le bouton droit de la souris sur votre sélection et sélectionnez **Ajouter des notes** dans le menu.
3. Entrez le texte de votre annotation et cliquez sur **OK**.

Modification de constatations

Les constatations modifiées correspondent à des constatations dont les types de vulnérabilité, les classifications ou les niveaux de gravité ont été modifiés ou auxquelles des annotations ont été ajoutées. La vue Constatations modifiées affiche ces constatations pour l'application en cours (application qui est active suite à l'ouverture d'une évaluation qui lui est associée). Dans la vue Mes évaluations (disponible uniquement dans AppScan Source for Analysis), la colonne **Modifié** indique si une constatation a été modifiée dans l'évaluation en cours.

Les modifications des constations prennent effet immédiatement et entraînent la mise à jour des métriques. Les modifications sont stockées avec des applications et sont appliquées à leur examen ultérieur.

Les constatations peuvent être modifiées depuis la vue Constatation détaillée ou depuis n'importe quelle vue comportant un tableau des constatations. La vue Constatation détaillée permet la modification de constatations individuelles. Vous pouvez aussi modifier plusieurs constatations dans un tableau de constatations.

Remarque : Vous devez disposer du droit **Sauvegarder les évaluations** pour pouvoir sauvegarder les modifications après avoir modifié une évaluation.

Apport de modifications depuis un tableau de constatations

Il peut s'avérer nécessaire de modifier les constatations par le biais d'un tableau de constatations si vous prévoyez d'apporter des modifications à plusieurs fichiers. Si vous devez modifier une seule constatation, utilisez un tableau de constatations ou la vue Constatation détaillée.

- «Modification du type de vulnérabilité»
- «Promotion de classifications de constatations»
- «Modification de la gravité», à la page 145
- «Annotations et attributs pris en charge», à la page 155

Modification du type de vulnérabilité

Les types de vulnérabilité peuvent être modifiés pour des constatations individuelles ou un groupe de constatations.

Procédure

1. Dans le tableau des constatations, sélectionnez une constatation ou un groupement de constatations à modifier.
2. Cliquez avec le bouton droit de la souris sur la sélection et cliquez dans le menu sur **Définir le type de vulnérabilité**.
3. Dans la boîte de dialogue Sélectionnez le type de vulnérabilité, choisissez le type de vulnérabilité voulu et cliquez sur **OK**.

Promotion de classifications de constatations

Une constatation avec une classification de constatation de sécurité suspectée ou de constatation de couverture d'examen peut devenir une constatation définitive.

Procédure

1. Dans le tableau des constatations, sélectionnez une constatation ou un groupement de constatations à modifier.
2. Cliquez avec le bouton droit de la souris sur la sélection et sélectionnez **Promouvoir vers définitive** dans le menu.

Modification de la gravité

La sélection d'un nouveau niveau de gravité modifie la gravité de chaque constatation sélectionnée. Il se peut, par exemple, que AppScan Source signale une API comme présentant un niveau de gravité moyen, tandis que votre stratégie interne l'identifie comme étant plus sérieuse. Vous pouvez modifier la gravité pour l'adapter à vos besoins, mais notez cependant que l'aide à la résolution AppScan Source n'intègre pas cette modification.

Procédure

1. Dans le tableau des constatations, sélectionnez une constatation ou un groupement de constatations à modifier.
2. Cliquez avec le bouton droit de la souris sur votre sélection et sélectionnez dans le menu **Définir la gravité**.
3. Sélectionnez comme nouveau niveau de gravité **Elevée**, **Moyenne**, **Faible** ou **Information**.

Annotation de constatations

Les notes peuvent servir de rappels vous avisant d'effectuer des actions complémentaires pour une constatation ou pour acheminer des informations à quelqu'un d'autre. Vous pouvez ajouter une note à une constatation isolée ou à un groupe de constatations.

Procédure

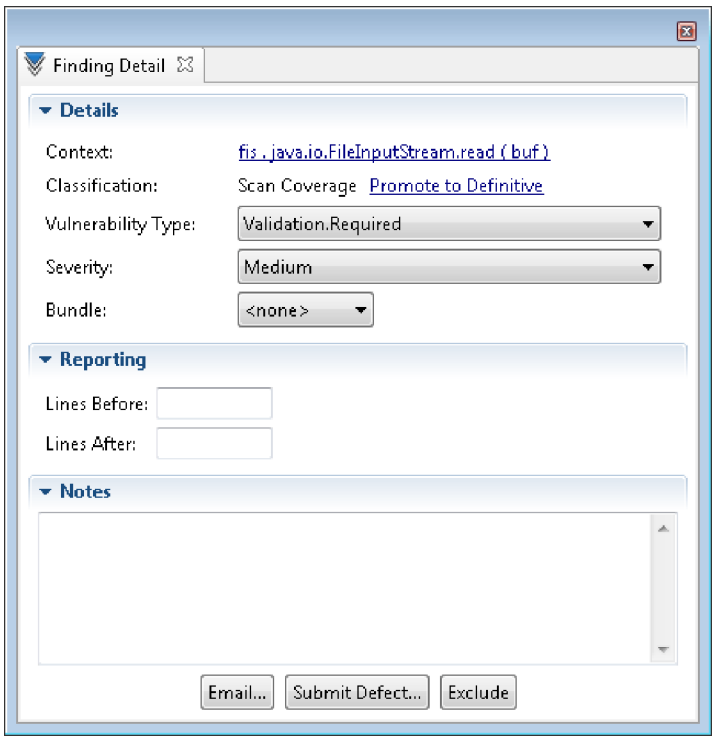
1. Dans le tableau des constatations, sélectionnez une constatation ou un groupement de constatations à modifier.
2. Cliquez avec le bouton droit de la souris sur votre sélection et choisissez **Ajouter des notes** dans le menu.
3. Entrez la note, puis cliquez sur **OK**.

Modification de constatations depuis la vue Constatation détaillée

Vous pouvez modifier des constatations individuelles depuis la vue Constatation détaillée. Si vous sélectionnez une constatation dans un tableau et ouvrez la vue Constatation détaillée, la constatation sélectionnée et ses caractéristiques s'affichent.

Vue Constatation détaillée

Lorsque vous sélectionnez une constatation, la vue Constatation détaillée, dans laquelle vous pouvez modifier ses propriétés, s'affiche. Avec cette vue, vous pouvez modifier une constatation individuelle.



- «Section Détails»
- «Section Rapport (disponible dans AppScan Source for Analysis et AppScan Source for Development (plug-in Eclipse) seulement)»
- «Section Notes»
- «Actions de la vue Constatation détaillée», à la page 147
- «Vue Constatation détaillée pour les constatations personnalisées (disponible uniquement dans AppScan Source for Analysis)», à la page 147

Section Détails

- **Contexte** : Fragment de code encadrant la vulnérabilité
- **Classification** : Constatations de sécurité définitive ou suspectée - ou Constatations de couverture d'examen - avec lien pour promouvoir la constatation en **Définitive** ou pour revenir à la valeur initiale si la vulnérabilité a été modifiée.
- **Type de vulnérabilité**
- **Gravité** : Elevée, moyenne, faible ou information
- **Groupement** : Nom du groupement contenant les constatations (non disponible dans AppScan Source for Development (plug-in Visual Studio))

Section Rapport (disponible dans AppScan Source for Analysis et AppScan Source for Development (plug-in Eclipse) seulement)

Spécifiez le nombre de lignes de code à inclure avant et/ou après la constatation dans les rapports.

Section Notes

Annotez la constatation.

Actions de la vue Constatation détaillée

- **Exclure** : Cliquez sur **Exclure** pour exclure (supprimer) la constatation du tableau des constatations. Pour visualiser des constatations exclues, ouvrez la vue Constatations exclues.
- Disponible dans AppScan Source for Analysis seulement :
  - **Courrier électronique** : Si vous avez configuré des préférences de courrier électronique, vous pouvez envoyer directement un groupement de constatations à des développeurs pour les aviser des défauts potentiels détectés après un examen. Le courrier électronique inclut en pièce jointe un groupement contenant les constatations et le courrier décrit ces constatations.
    1. Pour envoyer par courrier électronique la constatation actuelle depuis la vue Constatation détaillée, cliquez sur **Courrier électronique**.
    2. Dans la boîte de dialogue Nom de fichier de pièce jointe, spécifiez un nom pour le fichier de groupement qui sera joint à l'e-mail. Par exemple, si vous spécifiez `ma_constatation` dans la zone **Nom du fichier de pièce jointe**, un groupement avec le nom de fichier `ma_constatation.ozbdl` sera joint au courrier.
    3. Cliquez sur **OK** pour ouvrir la boîte de dialogue Envoi de constatations par courrier électronique. Par défaut, la zone **Envoyer à** de la boîte de dialogue d'envoi de constatations par courrier électronique contient les données de la zone **Adresse de destination** qui est spécifiée dans les préférences de courrier électronique. Toutefois, elle peut facilement être modifiée lors de la préparation du courrier électronique. Dans cette boîte de dialogue, cliquez sur **OK** pour envoyer le courrier électronique après avoir vérifié son contenu.
  - **Soumettre un défaut** : Pour soumettre la constatation en tant que défaut, cliquez sur **Soumettre un défaut**. Ceci ouvre la boîte de dialogue Sélection du système de suivi des défauts.
    - Si vous sélectionnez **ClearQuest** et cliquez sur **OK**, la boîte de dialogue Nom de fichier de pièce jointe s'affiche. Spécifiez dans celle-ci un nom pour le fichier de groupement qui sera joint au défaut, puis cliquez sur **OK**. Connectez-vous à Rational ClearQuest et soumettez les constatations.
    - Si vous sélectionnez **Quality Center** et cliquez sur **OK**, la boîte de dialogue Connexion s'ouvre pour vous permettre d'ouvrir une session Quality Center et de soumettre les constatations.
    - Si vous sélectionnez l'option **Team Foundation Server**, une boîte de dialogue s'affiche pour vous inviter à vous connecter au système de suivi des défauts et fournir d'autres détails de configuration.

    Remarque : Rational Team Concert est le seul système de suivi d'incidents pris en charge sous macOS.

Vue Constatation détaillée pour les constatations personnalisées (disponible uniquement dans AppScan Source for Analysis)

La vue Constatation détaillée fournit des informations supplémentaires que vous pouvez modifier :

- Fichier
- Ligne
- Colonne
- API

De plus, la méthode suivant laquelle vous modifiez la «Section Détails», à la page 146 est différente des constatations standard pour certaines zones (par exemple, les classifications pour les constatations personnalisées apparaissent dans une liste).

Suppression de modifications apportées à des constatations

Si vous avez modifié des constatations, vous pouvez supprimer les modifications (rétablir les valeurs d'origine des constatations) à l'aide des méthodes décrites dans cette rubrique.

Pourquoi et quand exécuter cette tâche

Il existe un grand nombre de méthodes vous permettant de supprimer des modifications apportées à des constatations :

- «Suppression de modifications dans la vue Constatations modifiées» : cette méthode nécessite que votre évaluation soit ouverte pour l'application qui contient les modifications à supprimer. Elle est utile lorsque vous souhaitez rétablir les valeurs d'origine de plusieurs constatations modifiées.
- «Suppression de modifications dans d'autres vues comportant des constatations», à la page 149 : cette méthode qui nécessite une évaluation ouverte est très utile si vous avez apporté plusieurs modifications à une constatation et que vous souhaitez rétablir une partie des valeurs d'origine que vous avez modifiées. Par exemple, si vous avez modifié le niveau de gravité et la classification d'une constatation et que vous souhaitez rétablir le niveau de gravité d'origine tout en conservant la classification modifiée, cette méthode est la plus adaptée.
- «Suppression de modifications dans l'onglet Constatations modifiées de la vue Propriétés (AppScan Source for Analysis uniquement)», à la page 149 : cette méthode est utile si vous souhaitez supprimer les modifications d'une application pour laquelle aucune évaluation n'est ouverte. Vous pouvez l'utiliser pour rétablir les valeurs d'origine de plusieurs constatations modifiées.

Suppression de modifications dans la vue Constatations modifiées

Procédure

1. Dans la vue Constatations modifiées, sélectionnez la constatation modifiée dont vous souhaitez rétablir les valeurs d'origine. Vous pouvez sélectionner plusieurs constatations à l'aide des touches clavier Ctrl et Maj sous Windows, ou les touches Cmd et Maj sous macOS.
2. Cliquez sur **Supprimer les modifications** ou cliquez avec le bouton droit de la souris sur votre sélection et choisissez **Supprimer les modifications** dans le menu.

Résultats

Cette action supprime toutes les modifications qui ont été apportées à une constatation. Si vous avez apporté plusieurs modifications à une constatation et que vous souhaitez rétablir une partie des valeurs d'origine que vous avez modifiées, utilisez la méthode décrite dans la section «Suppression de modifications dans d'autres vues comportant des constatations», à la page 149.

Suppression de modifications dans d'autres vues comportant des constatations

Pourquoi et quand exécuter cette tâche

Dans n'importe quelle vue comportant un tableau de constatations, vous pouvez choisir les colonnes à afficher à l'aide de l'action **Sélectionnez et ordonnez les colonnes**. Vous pouvez ainsi afficher les colonnes **Gravité (originale)**, **Gravité (personnalisée)**, **Classification (originale)** et **Classification (personnalisée)**. Ces colonnes vous aident à rétablir les valeurs d'origine des modifications apportées (à l'aide des actions du tableau de constatations ou de la vue Constatation détaillée). Par exemple, dans le cas d'une constatation dont la colonne **Gravité** ou **Gravité (personnalisée)** contient la valeur **Elevée** et la colonne **Gravité (originale)** contient la valeur **Moyenne**, la valeur **Moyenne** peut être rétablie pour le niveau de gravité à l'aide de diverses méthodes, telles que celles décrites ci-dessous :

- Dans un tableau de constatations, cliquez avec le bouton droit de la souris sur la constatation concernée, puis choisissez **Définir la gravité** > **Moyenne** dans le menu.
- Sélectionnez la constatation, puis, dans la vue Constatation détaillée, affectez la valeur **Elevée** à la zone **Gravité**.

Suppression de modifications dans l'onglet Constatations modifiées de la vue Propriétés (AppScan Source for Analysis uniquement)

Procédure

1. Dans la vue Explorateur, sélectionnez l'application qui contient les modifications que vous souhaitez supprimer.
2. Dans la vue Constatations modifiées, sélectionnez la constatation modifiée dont vous souhaitez rétablir les valeurs d'origine. Plusieurs constatations peuvent être sélectionnées à l'aide des touches Ctrl et Maj du clavier.
3. Cliquez sur **Supprimer les modifications** ou cliquez avec le bouton droit de la souris sur votre sélection et choisissez **Supprimer les modifications** dans le menu.

Résultats

Cette action supprime toutes les modifications qui ont été apportées à une constatation. Si vous avez apporté plusieurs modifications à une constatation et que vous souhaitez rétablir une partie des valeurs d'origine que vous avez modifiées, utilisez la méthode décrite dans la section «Suppression de modifications dans d'autres vues comportant des constatations».

Comparaison de constatations

Les évaluations sont comparées à l'aide de l'action **Evaluations de différences**. Lorsque deux évaluations sont comparées, leurs différences s'affichent dans la vue Différences entre les évaluations. Cette vue affiche les constatations nouvelles, corrigées/manquantes et communes.

Ces contrôles sont disponibles dans la vue Différences entre les évaluations :

- **Evaluations de différences** : Affiche les différences entre les deux évaluations sélectionnées.

- **Nouvelles constatations** (bleu) : Utilisez ce bouton de barre d'outils pour basculer l'affichage des nouvelles constatations (constatations qui figurent dans l'évaluation portant un libellé bleu, mais pas dans l'évaluation portant un libellé vert).
- **Constatations corrigées/manquantes** (vert) : Utilisez ce bouton de barre d'outils pour basculer l'affichage des constatations corrigées/manquantes (constatations qui figurent dans l'évaluation portant un libellé vert, mais pas dans l'évaluation portant un libellé bleu).
- **Commune** (blanc) : Utilisez ce bouton de barre d'outils pour basculer l'affichage des constatations communes entre les deux évaluations.
- **Suivante** : Passe au bloc suivant de constatations nouvelles ou corrigées/manquantes.
- **Précédente** : Passe au bloc précédent de constatations nouvelles ou corrigées/manquantes.

Comparaison de deux évaluations dans la vue Différences entre les évaluations

Procédure

1. Dans le panneau de gauche, sélectionnez deux évaluations à comparer.
2. Cliquez sur le bouton **Différences entre les évaluations** ou cliquez avec le bouton droit de la souris sur votre sélection, puis sélectionnez **Différences entre les évaluations** dans le menu.

Comparaison de deux évaluations dans la barre de menus principale

Procédure

1. Sélectionnez **Outils** > **Evaluations des différences** dans la barre de menus principale.
2. Dans la boîte de dialogue Différences entre les évaluations, sélectionnez deux évaluations.
3. Cliquez sur **OK** pour ouvrir une comparaison des deux évaluations dans la vue Différences entre les évaluations.

Recherche de différences entre les évaluations dans les vues Mes évaluations et Evaluations publiées

Procédure

1. Sélectionnez deux évaluations dans l'une des vues.
2. Cliquez sur le bouton **Différences entre les évaluations** ou cliquez avec le bouton droit de la souris sur votre sélection, puis sélectionnez **Différences entre les évaluations** dans le menu. Une comparaison des deux évaluations apparaît dans la vue Différences entre les évaluations.

Constatations personnalisées

Pour étoffer vos résultats d'analyse, vous pouvez créer des *constatations personnalisées*. Il s'agit de constatations créées par l'utilisateur que AppScan Source for Analysis ajoute à l'évaluation ouverte actuellement ou à l'application sélectionnée. Les constatations personnalisées affectent les métriques d'évaluations

et peuvent être incluses dans des rapports. Une fois créée, une constatation personnalisée est incluse automatiquement dans les examens ultérieurs de l'application.

Le comportement d'une constatation personnalisée dépend de la vue depuis laquelle elle est créée.

Lorsqu'elle est créée depuis la vue Constatations, la constatation personnalisée :

- Est appliquée à l'évaluation ouverte actuellement.
- Est sauvegardée en même temps que l'application et figure dans les propriétés de celle-ci.
- Affecte l'examen actuel et les examens ultérieurs de la même application.
- Affecte immédiatement les métriques de l'évaluation.

Lorsqu'elle est créée à partir de la vue Propriétés ou via l'action **Ajouter une constatation personnalisée** pour une application sélectionnée, la constatation personnalisée :

- Est appliquée à l'application sélectionnée.
- Est ajoutée à l'évaluation en cours si l'application est celle ayant été analysée.
- Est contenue dans les examens ultérieurs de cette application.

Lorsqu'elle est créée depuis l'éditeur de code :

- Si une évaluation est ouverte, la constatation personnalisée opère comme lorsqu'elle a été créée dans la vue Constatations.
- Si aucune évaluation n'est ouverte, la constatation personnalisée opère comme lorsqu'elle a été créée dans la vue Propriétés.

AppScan Source for Analysis sauvegarde automatiquement l'application après la création de constatations personnalisées. Vous ne pouvez pas modifier l'évaluation sans modifier l'application. Cependant, si une évaluation n'est pas associée à une application, aucune application n'est modifiée.

Si vous ajoutez des constatations personnalisées à une application, celles-ci sont intégrées dans les examens ultérieurs de cette application et ne peuvent en être exclues. Pour retirer une constatation personnalisée, vous devez l'exclure d'une évaluation ou la supprimer de l'application.

Remarque : Les constatations personnalisées ne peuvent pas être *corrigées/manquantes*.

Une constatation personnalisée est composée des attributs suivants :

- **Type de vulnérabilité** (requis)
- **Gravité** (requise)
- **Classification** (requise)
- **Fichier** (requis)
- **Contexte**
- Numéro de **ligne**
- Numéro de **colonne**
- **API**
- **Notes**
- **Groupement**

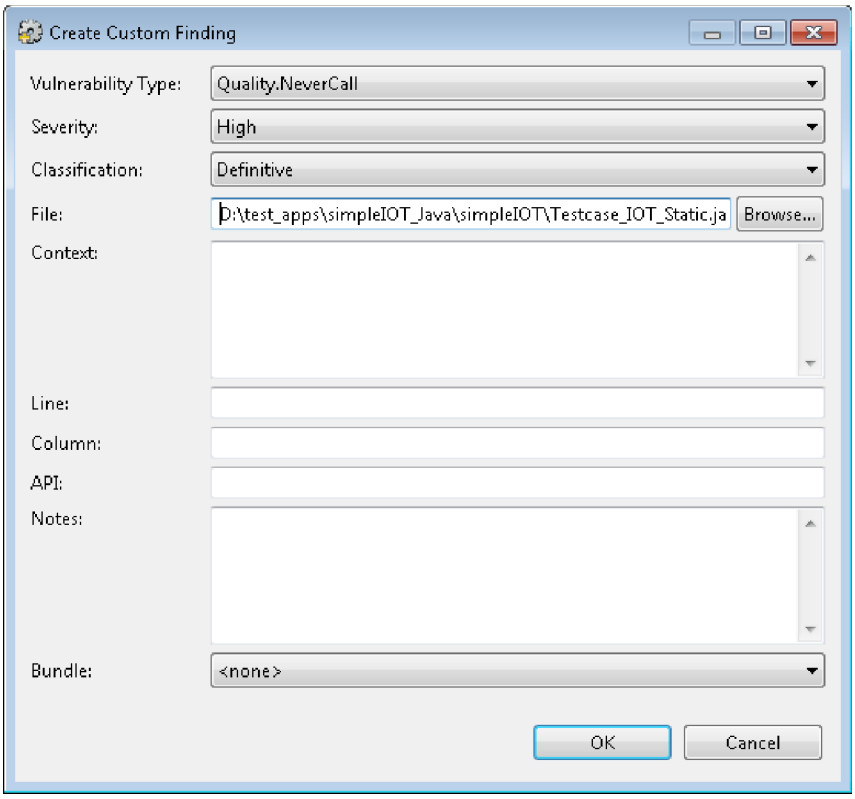
Création d'une constatation personnalisée dans la vue Propriétés

La création ou la modification d'une constatation personnalisée depuis la vue Propriétés de l'application affecte les résultats de l'évaluation en cours et des examens ultérieurs.

Procédure

1. Sélectionnez l'application dans la vue Explorateur.
2. Depuis la vue Propriétés, sélectionnez l'onglet **Constatations personnalisées**.
3. Cliquez dans la barre d'outils sur **Créer une constatation personnalisée**.
4. Dans la boîte de dialogue Création d'une constatation personnalisée, ajoutez les renseignements requis :
   - **Type de vulnérabilité**
   - **Gravité**
   - **Classification**
   - **Fichier**

   Ajoutez éventuellement le contexte, le numéro de ligne, la colonne, une API, des notes et une désignation de groupement.



5. Cliquez sur **OK** pour sauvegarder les constatations personnalisées dans l'application.

Modification ou suppression d'une constatation personnalisée dans la vue Propriétés

La création ou la modification d'une constatation personnalisée depuis la vue Propriétés de l'application affecte les résultats de l'évaluation en cours et des examens ultérieurs.

Procédure

1. Sélectionnez la constatation. Si vous supprimez des constatations personnalisées, vous pouvez sélectionner un groupe de constatations à supprimer.
2. Pour modifier la constatation personnalisée, cliquez sur **Editer la constatation sélectionnée** dans la barre d'outils et modifiez ensuite les informations sur les constatations définies précédemment.
3. Pour supprimer la ou les constatations personnalisées, cliquez sur **Supprimer les constatations sélectionnées** dans la barre d'outils.

Création de constatations personnalisées depuis une vue de constatations

Vous pouvez créer et gérer des constatations personnalisées depuis plusieurs vues de constatations (vue Constatations et Constatations personnalisées, par exemple).

La création d'une constatation personnalisée ajoute la nouvelle constatation à l'évaluation en cours et actualise les métriques de l'évaluation.

Lors de l'ajout d'une constatation personnalisée dans une vue de constatations, cliquez sur le bouton de barre d'outils **Créer une constatation personnalisée** de la vue. La vue Créer une constatation personnalisée s'affiche ; renseignez-la comme indiqué dans «Création d'une constatation personnalisée dans la vue Propriétés», à la page 152.

Pour supprimer une constatation personnalisée, vous devez l'exclure d'une évaluation ou la supprimer de l'application, ou suivre les instructions de la rubrique «Modification ou suppression d'une constatation personnalisée dans la vue Propriétés», à la page 152. Ces actions ne sont pas disponibles dans les autres vues de constatations.

Création de constatations personnalisées dans l'éditeur de code source

Pourquoi et quand exécuter cette tâche

Lors de l'ajout de constatations personnalisées par le biais de l'éditeur de code source, les conditions suivantes s'appliquent :

- Si le fichier source visible dans l'éditeur de code source est rattaché à l'évaluation ouverte actuellement, la constatation personnalisée est ajoutée à cette évaluation et à l'application associée.
- Si elle n'est pas rattachée à l'évaluation ouverte actuellement, la constatation personnalisée est ajoutée uniquement à l'application contenant le fichier source.
- Si le fichier source est rattaché à plusieurs applications ou que AppScan Source for Analysis ne parvient pas déterminer à quelle application il appartient, vous devez sélectionner l'application appropriée.

Si vous créez une constatation personnalisée depuis l'éditeur de code source, la boîte de dialogue Création d'une constatation personnalisée est pré-renseignée avec les informations provenant de l'éditeur.

- **Fichier** : Nom du fichier ouvert

- **Contexte** : N'importe quel texte sélectionné dans l'éditeur. Si aucun texte n'est sélectionné, le contexte correspond à la ligne actuelle à l'emplacement du curseur. Si plusieurs lignes sont sélectionnées, toutes ces lignes deviennent le contexte.
- Numéro de **ligne** et numéro de **colonne** : Numéro de la ligne et de la colonne actuelles

Pour créer une constatation personnalisée depuis l'éditeur, procédez comme suit :

Procédure

1. Sélectionnez les lignes de code à ajouter comme constatation personnalisée.
2. Cliquez avec le bouton droit de la souris sur votre sélection et sélectionnez dans le menu **Créer une constatation personnalisée**. La boîte de dialogue Création d'une constatation personnalisée est alimentée avec les informations de fichier, contexte, numéro de ligne et de colonne.
3. Sélectionnez le **Type de vulnérabilité**, la **Gravité** et la **Classification**. Ajoutez le cas échéant une API, des notes ou une désignation de groupement.
4. Cliquez sur **OK**.

Résolution des problèmes de sécurité et affichage de l'aide à la résolution

AppScan Source vous alerte en cas d'erreurs ou de failles de conception courantes de la sécurité et vous assiste dans leur processus de résolution. La Base de connaissances de sécurité AppScan Source Security et les éditeurs de code internes ou externes vous aident au cours de ce processus.

Pourquoi et quand exécuter cette tâche

La Base de connaissances de sécurité AppScan Source Security propose des suggestions pour la correction des constatations. Ces informations contextuelles pour chaque vulnérabilité comprennent des descriptions précises de leur cause principale, de la gravité du risque encouru, ainsi que des conseils de résolution concrets. Elle décrit, par exemple `strcpy()` (vulnérabilité de type Dépassement de mémoire tampon) comme ayant un niveau de gravité élevé et fournit ces conseils de résolution :

> `strcpy` est vulnérable à un dépassement de la mémoire tampon de destination car elle ne connaît pas sa longueur et ne peut pas s'assurer de ne pas l'écraser. Vous devriez envisager d'utiliser `strncpy` lequel reçoit un paramètre de longueur (length). `strncpy` représente également un risque pour la sécurité, quoique à un moindre degré.

Pour afficher la Base de connaissances de sécurité AppScan Source Security :

Procédure

- Dans AppScan Source for Analysis, ouvrez la vue Aide à la résolution et sélectionnez ensuite une constatation dans le tableau des constatations. L'aide à la résolution pour cette constatation spécifique s'affiche. Vous pouvez à la place sélectionner **Aide** > **Base de connaissances de sécurité** dans le menu principal pour ouvrir l'ensemble de Base de connaissances de sécurité AppScan Source Security dans un navigateur.

- Dans AppScan Source for Development (plug-in Eclipse), ouvrez la vue Aide à la résolution et sélectionnez ensuite une constatation dans le tableau des constatations. L'assistance à la résolution pour cette constatation spécifique s'affiche.
- Dans AppScan Source for Development (plug-in Visual Studio), sélectionnez une constatation dans un tableau de constatations. Sélectionnez **IBM Security AppScan Source** > **Aide de la base de connaissances** dans la barre de menus principale ou cliquez avec le bouton droit de la souris sur la constatation et sélectionnez **Aide de la base de connaissances** dans le menu. L'aide à la résolution s'affiche pour la constatation sélectionnée.

Analyse de code source dans un éditeur

Avec AppScan Source, vous pouvez analyser ou modifier le code source dans un éditeur interne ou choisir parmi une variété d'éditeurs externes.

Les éditeurs externes vous permettent d'examiner les résultats AppScan Source for Analysis et d'apporter des modifications au code dans l'environnement de développement de votre choix. Les éditeurs externes comprennent :

- vi
- Eclipse (voir la configuration requise pour AppScan Source pour savoir quelles versions d'Eclipse sont prises en charge)
- Valeur par défaut du système

Remarque : Vous ne pouvez pas éditer les fichiers source dans un fichier `WAR`.

Pour afficher/modifier le code source de l'éditeur, choisissez l'une des options ci-dessous :

- Effectuez un double-clic sur une constatation dans leur table. L'éditeur interne s'ouvre sur la ligne de code.
- Cliquez avec le bouton droit de la souris sur une constatation dans le tableau et sélectionnez **Ouvrir dans l'éditeur interne** ou **Ouvrir dans l'éditeur externe** > **<éditeur>** (où **<éditeur>** correspond à l'un des éditeurs externes pris en charge répertoriés dans le tableau ci-dessus).
- Sélectionnez un noeud de trace, puis cliquez sur le bouton **Ouvrir dans l'éditeur interne** ou **Ouvrir dans l'éditeur externe** > **<éditeur>** dans la barre d'outils, ou cliquez avec le bouton droit de la souris sur la sélection et sélectionnez **Ouvrir dans l'éditeur interne** ou **Ouvrir dans l'éditeur externe** > **<éditeur>** dans le menu.

Si vous avez ouvert un fichier dans l'éditeur, des marqueurs indiquent les emplacements dans le fichier qui représentent les constatations. Pour remonter à eux dans le tableau des constatations, cliquez avec le bouton droit de la souris sur la ligne de code dans l'éditeur et sélectionnez **Afficher dans la vue Constatations** dans le menu.

Annotations et attributs pris en charge

Certaines annotations ou attributs utilisés pour *enrichir* le code sont traités lors des examens. Lorsqu'une annotation ou un attribut pris en charge est détecté lors d'un examen, ces informations sont utilisées pour marquer la méthode enrichie en tant que rappel entaché. Une méthode marquée comme rappel entaché est traitée si tous ses arguments comportent des données entachées. Ceci débouche sur un plus grand nombre de constatations accompagnées de traces. Les annotations et attributs pris en charge sont répertoriés dans cette rubrique d'aide.

- «Annotations Java prises en charge»
- «Annotations AppScan Source Java prises en charge»
- «Attributs Microsoft .NET pris en charge», à la page 157

Annotations Java prises en charge

Tableau 13. Annotations Java prises en charge

Annotation	Abréviation
javax.xml.ws.WebServiceProvider	@WebServiceProvider
javax.jws.WebService	@WebService
javax.jws.WebMethod	@WebMethod

Annotations AppScan Source Java prises en charge

- «Utilisation des annotations AppScan Source»
- «@ValidatorMethod», à la page 157
- «@SuppressSecurityTrace», à la page 157
- «@CallbackMethod», à la page 157

Lorsque vous utilisez la fonction d'AppScan Source pour examiner du code Java, les annotation de méthode `@ValidatorMethod`, `@CallbackMethod` et `@SuppressSecurityTrace` sont prises en charge.

Utilisation des annotations AppScan Source

L'utilisation des annotations est décrite ci-dessous :

1. Les annotations sont prises en charge par défaut. Le fichier d'annotation `.jar` se trouve dans `<install_dir>\lib\SecurityAnnotations.jar` (où `<rép_install>` représente l'emplacement de votre installation AppScan Source).
2. Si vous analysez des classes pré-compilées, des fichiers `.war` ou des fichiers `.jar`, localisez le projet Java contenant les sources annotées. -
3. Ajoutez `SecurityAnnotations.jar` au chemin de classe du projet.
4. Régénérez le projet.

Les annotations peuvent être ajoutées au code source avant l'examen, ou après l'examen et pendant le triage pour identifier et éliminer les faux positifs.

Les annotations permettent d'insérer directement des connaissances dans le code source sous la forme d'annotations de sécurité. Les annotations pouvant être utilisées pour déclarer fiables des portions de code, elles doivent être utilisées avec beaucoup de précautions. Elles ne doivent pas être utilisées pour du code dans lequel des vulnérabilités de sécurité doivent être recherchées. Si vous utilisez des annotations, un analyste de sécurité peut choisir de les ignorer en désactivant la fonction dans `<data_dir>\config\scanner.ozsettings` (où `<rép_données>` est l'emplacement de vos données de programme AppScan Source, comme décrit dans «Installation et emplacements des fichiers de données utilisateur», à la page 292). Dans ce fichier, repérez le paramètre suivant :

```
<Setting
name="process_security_annotations"
value="true"
default_value="true"
description="When turned on, security annotations in the
```

```
     source code will be processed by AppScan Source."
display_name="Process Security Annotations"
type="bool"
/>
```

Pour désactiver la fonction, remplacez `value="true"` par `value="false"`.

@ValidatorMethod

Les valideurs sont des méthodes qui vérifient les données en entrée et renvoient généralement une valeur booléenne qui indique si l'entrée est valide. Plutôt que d'accepter ou de rejeter les entrées utilisateur à l'aide de valideurs, vous pouvez les modifier pour leur donner un format acceptable. Ces méthodes s'appellent des nettoyeurs.

L'annotation `@ValidatorMethod` permet d'identifier toutes les méthodes de validation et de nettoyage dans le code source de l'application. Au cours des examens d'AppScan Source, ces informations sont utilisées pour supprimer les flux de données qui transitent par ces méthodes, puisque ces données sont alors considérées comme fiables.

Remarque : Il n'est actuellement pas possible de spécifier quels paramètres de la méthode annotée doivent être considérés comme validés. Pendant les examens d'AppScan Source, tous les paramètres d'entrée sont considérés comme validés.

@SuppressSecurityTrace

Toutes les traces qui passent par une méthode marquée avec cette annotation sont supprimées. Cette annotation est utile lorsqu'un groupe de traces est identifié comme des faux positifs, ou est moins important ou intéressant que d'autres. Vous pouvez l'utiliser pour éliminer ces traces, ou pour les masquer afin de réduire l'encombrement.

@CallbackMethod

Cette annotation est utilisée pour identifier des rappels ou les points d'entrée d'une application. Tous les arguments sont considérés comme tachés.

Attributs Microsoft .NET pris en charge

Tableau 14. Attributs Microsoft .NET pris en charge

Attribut	Abréviation
`System.Web.Services.WebServiceAttribute`	`WebService`
`System.Web.Services.WebMethodAttribute`	`WebMethod`

Chapitre 6. Trace AppScan Source

La trace AppScan Source permet de vérifier que la validation et le codage des entrées répondent à vos règles de sécurité logicielle. Elle permet d'examiner les constatations qui génèrent des traces d'entrée/sortie et de marquer des méthodes en tant que routines de validation et codage, sources ou collecteurs, rétro-appels ou propagateurs de taches.

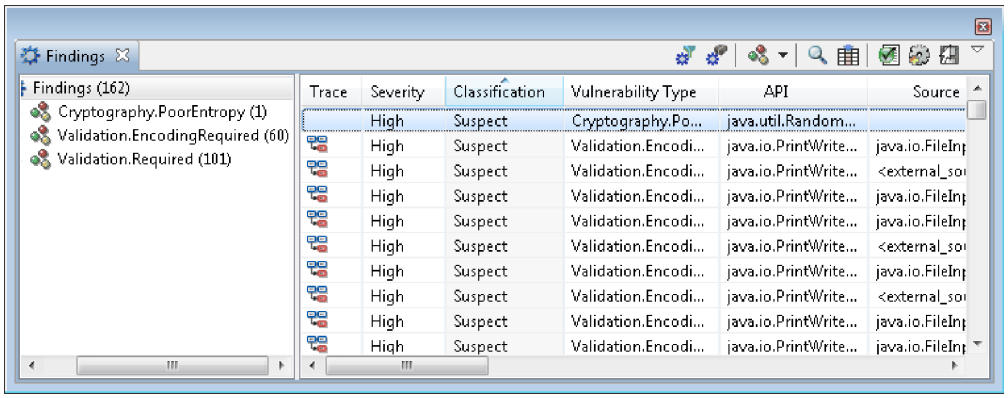
AppScan Source trace le flux des données à travers une application, entre modules et langages. Il affiche les chemins de données potentiellement dangereuses dans un graphe d'appel, ce qui indique les zones où une application peut subir des vulnérabilités.

La fonction de trace vous aide à neutraliser les attaques par injection SQL, script intersite, et autres attaques liées à la validation des entrées en identifiant l'absence de routines de validation et de codage des entrées approuvées dans les applications. Vous pouvez appliquer une trace interactive à la totalité du graphe d'appel en cliquant directement depuis la vue Trace pour visualiser la source dans l'environnement de développement ou l'éditeur de code de votre choix. La fonction de trace active également l'application de règles, en vous permettant d'identifier les routines approuvées requises pour une validation et un codage approprié, la propagation de taches, ou les collecteurs et sources, et les inclure dans des examens ultérieurs.

Lorsqu'un examen débouche sur une trace, vous pouvez créer des routines de validation ou de codage, des vulnérabilités, des collecteurs, des sources ou des propagateurs de taches pour des constatations spécifiques depuis la vue Trace. Par exemple, si vous marquez une routine comme étant une routine de validation dans AppScan Source for Analysis et que vous l'ajoutez à Base de connaissances de sécurité AppScan Source Security, les examens ultérieurs ne renvoient plus de constatations de type `Validation.Required` ou `Validation.Encoding.Required` pour les chemins de données sur lesquels ces routines sont appelées. Dans la vue Trace, vous pouvez également définir des vulnérabilités en tant que source, collecteur, ou les deux, et identifier une méthode en tant que propagateur de taches, retro-appel entaché, ou non vulnérable aux taches.

Résultats d'examen de la trace AppScan Source

Les résultats de l'examen peuvent inclure des traces identifiées par une trace AppScan Source. L'icône dans la colonne **Trace** indique l'existence d'une trace du graphe d'appels.



Les examens peuvent générer des constatations du type `Validation.Required` et `Validation.EncodingRequired`. Ces constatations indiquent un emplacement dans le code source où des données sont lues depuis une source externe ou sauvegardées dans un collecteur externe. L'examen signale ces cas car ces données doivent être validées ou codées afin d'empêcher des données malveillantes ou erronées de causer des dommages.

Validation et codage

La *validation* désigne le processus de vérification des données en entrée pour s'assurer qu'elles sont construites correctement. Une constatation `Validation.Required` indique qu'aucune validation n'est intervenue sur un chemin de données spécifié depuis la source jusqu'au collecteur. La validation peut être aussi simple qu'une limitation des données à une longueur maximale et aussi complexe que la vérification de noms et d'adresses correctement formés. La validation peut également dépister des attaques (par injection SQL, par exemple) en détectant des séquences de caractères proscrits qui induisent ces attaques.

Le *codage* désigne le processus de transformation des données pour qu'elles soient construites correctement. Une constatation `Validation.EncodingRequired` indique qu'aucun codage n'est intervenu sur un chemin de données spécifié depuis la source jusqu'au collecteur. Le codage peut être aussi simple que l'adjonction de caractères d'échappement ou aussi complexe que le chiffrement des données. Le codage peut également empêcher des attaques (par script intersite, par exemple) en échappant les caractères qui invitent ces attaques.

Lors du premier examen, AppScan Source peut identifier une constatation en tant que constatation de sécurité suspectée. Lorsque vous créez une routine de validation ou de codage s'appliquant à une source spécifique, AppScan Source for Analysis signale la constatation en tant que constatation définitive (au lieu de suspectée) si cette routine n'est pas appelée après la réception de données de cette source.

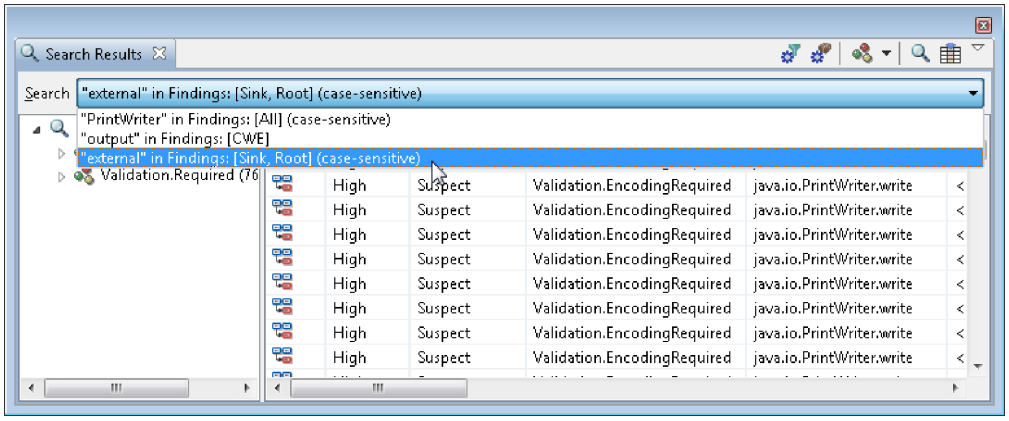
Les évaluations suivent les données provenant de sources connues à travers un projet. Si des données peuvent être suivies depuis une source connue jusqu'à un

collecteur connu, des routines de validation et de codage spécifiées peuvent garantir qu'une attaque malveillante ne puisse pas exploiter des données d'entrée non bornées.

Recherche de traces AppScan Source

Si vous désirez regrouper les constatations de traces, vous pouvez effectuer une recherche sur des sources ou des collecteurs. Les constatations de trace apparaissent dans la vue Résultats de la recherche.

Dans la vue Trace, cliquez sur **Rechercher des traces avec la même routine de type**. Puis, dans la boîte de dialogue Rechercher des constatations, sélectionnez des appels de source, de collecteur, de collecteur indéterminé (inclut les collecteurs indéterminés virtuels), de collecteur indéterminé virtuel ou de trace pour restreindre les résultats aux traces contenant la chaîne. Les résultats sont cumulatifs et apparaissent dans la vue Résultats de la recherche. Vous pouvez effectuer une nouvelle recherche dans cette vue pour affiner les résultats.



Traçage des entrées/sorties

Une *trace des entrées/sorties* est générée lorsque AppScan Source for Analysis peut suivre le cheminement des données depuis une source connue vers un *collecteur* ou un *collecteur indéterminé*.

Trace des entrées/sorties

Si l'analyse du code peut suivre une source entachée jusqu'à un collecteur ou un collecteur indéterminé, elle génère alors une trace des entrées/sorties. La racine de la trace est la méthode qui obtient des données depuis des sources entachées et les transmet à une série d'appels qui les consignent finalement dans un collecteur non protégé.

Sources et collecteurs

- **Source** : une source est une entrée du programme, telle qu'un fichier, une requête de servlet, une saisie depuis la console ou un socket. Dans le cas de la plupart des sources d'entrées, les données renvoyées ne sont pas limitées en termes de contenu et de longueur. Lorsqu'une entrée n'est pas vérifiée, elle est considérée comme entachée. Les sources sont répertoriées dans les tables de constatations sous la colonne **Source**.
- **Collecteur** : un collecteur peut être un format externe quelconque dans lequel des données peuvent être consignées. Comme exemples de collecteurs, on peut citer des bases de données, des fichiers, des sorties console et des sockets. La

consignation de données dans un collecteur sans leur vérification peut donner lieu à une vulnérabilité sérieuse de la sécurité.

- **Collecteur indéterminé** : un collecteur indéterminé est une méthode API qui ne peut plus faire l'objet d'une trace.

  Remarque : Les collecteurs indéterminés ne s'appliquent pas aux constatations JavaScript.

Utilisation de la vue Trace

Pourquoi et quand exécuter cette tâche

La vue Trace affiche une trace d'entrée/sortie unique correspondant à une constatation. Le panneau est divisé en trois volets :

- Piles d'entrées et de sorties
- Flux de données
- Diagramme d'appels graphique

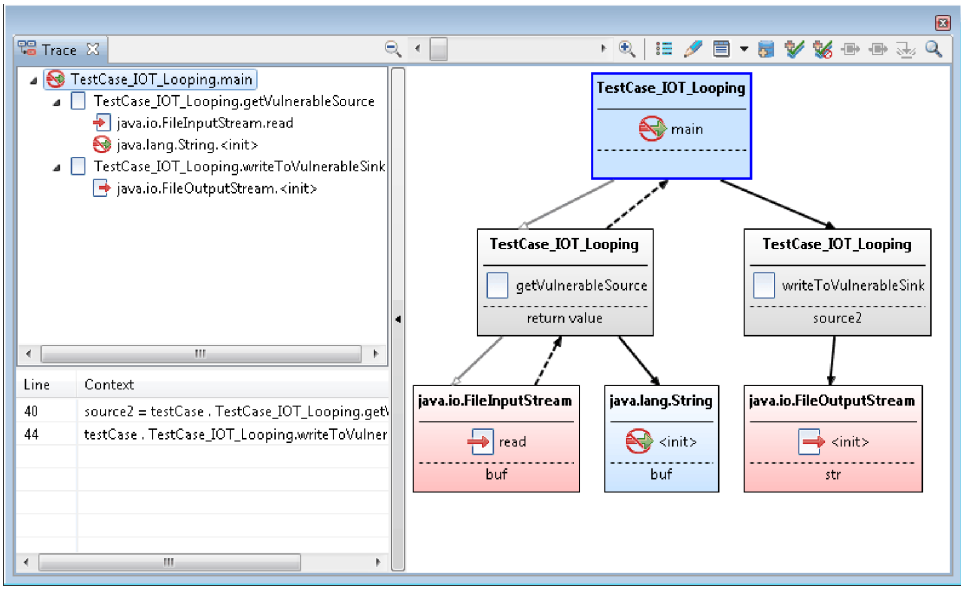
Ces panneaux sont décrits plus en détail dans «Piles d'entrée/sortie dans la vue Trace», à la page 163.

Remarque : Dans une trace JavaScript, un «Diagramme d'instructions JavaScript», à la page 164 s'affiche, plutôt qu'un diagramme d'appels graphique.

Pour afficher une trace AppScan Source :

Procédure

1. Examiner et recherchez les résultats de trace dans la vue Constatations.
2. Depuis le menu Vue, ouvrez la vue Trace.
3. Sélectionnez les lignes de la table des constatations affichant l'icône **Trace**. La vue Trace affiche les détails de trace.



Piles d'entrée/sortie dans la vue Trace

Le panneau supérieur gauche affiche les piles d'**entrée** et de **sortie**. La pile est une séquence d'appels qui se terminent soit sur une source (pile d'entrée), soit sur un collecteur (pile de sortie).

Flux de données

Le panneau inférieur gauche héberge le flux de données pour la méthode sélectionnée. Les données peuvent circuler via un appel de méthode ou une affectation. La section flux de données affiche le numéro de ligne dans le code source où figurent l'élément et le contexte.

Graphe d'appels

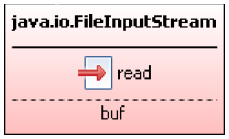
Remarque : Dans une trace JavaScript, un «Diagramme d'instructions JavaScript», à la page 164 s'affiche, plutôt qu'un diagramme d'appels graphique.

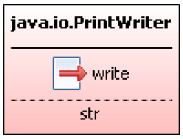
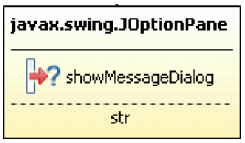
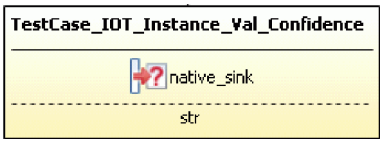
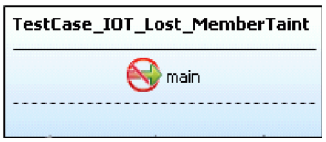
Ce diagramme est une représentation graphique du graphe d'appels. Chaque appel de méthode est représenté par un rectangle dans le graphique affichant le nom de classe et le nom de méthode :

- Une couleur rouge indique que l'appel de méthode concerne une source, un collecteur, ou les deux.
- Un *collecteur indéterminé* est une méthode API qui ne peut plus faire l'objet d'une trace. Un *collecteur indéterminé virtuel* est un collecteur indéterminé qui est également une fonction virtuelle (une fonction qui peut avoir plusieurs mises en oeuvre). La couleur jaune identifie l'appel de méthode comme concernant un collecteur indéterminé ou un collecteur indéterminé virtuel.
- La couleur bleue indique que l'appel de méthode n'est pas une routine de validation/codage.
- La couleur grise représente tous les autres types de noeud de trace.

Chaque appel de méthode est divisé en trois sections : le nom de classe, le nom de méthode et le nom d'argument entaché. L'infobulle associée à l'appel de méthode présente plus de détails.

Les lignes avec des flèches représentent des appels d'une méthode à une autre. Une tête de flèche creuse indique l'absence de données entachées connues dans l'appel, tandis qu'une flèche pleine indique un flux de données entachées. Une flèche discontinue indique une instruction de retour.

Symbole	Description
	Appel de méthode sans données entachées connues
	Appel de méthode avec données entachées
	Retour avec données entachées
	Source (rouge) : méthode, fonction ou paramètre à l'origine de données potentiellement non sécurisées.

Symbole	Description
	Collecteur (rouge) : méthode ou fonction potentiellement vulnérable aux données entachées ou dont l'utilisation est potentiellement dangereuse.
	Collecteur indéterminé (jaune) : méthode ou fonction qui est potentiellement vulnérable aux données entachées ou dont l'utilisation est potentiellement dangereuse.
	Collecteur indéterminé virtuel (jaune) : type de collecteur indéterminé qui est résolu par plusieurs implémentation concrètes.
	N'est pas une routine de validation (bleu). Le marquage d'une API comme n'étant *pas une routine de validation/codage* indique que cette API ne valide aucune donnée.
	Propagateur de tâche : fonction ou méthode qui propage une tâche à un ou plusieurs de ses paramètres, à sa valeur de retour ou à ce pointeur.

Conseil :

- Dans la vue Trace, survolez les noeuds de trace du graphique pour afficher des informations sur le noeud.
- Les deux panneaux de gauche de la vue (le panneau des piles d'entrée/sortie et le panneau des flux de données) peuvent être réduits pour améliorer l'affichage du diagramme d'appels graphique. Pour réduire ces panneaux, sélectionnez la flèche de **masquage de l'arborescence**. Pour afficher ces panneaux lorsqu'ils sont masqués, sélectionnez la flèche d'**affichage de l'arborescence**.
- Déplacez la barre de défilement pour effectuer un zoom avant détaillé ou effectuer un zoom arrière pour une vue plus générale. Si vous survolez la barre de défilement du zoom, le niveau de zoom actuel s'affiche. Pour effectuer un zoom avant maximum, sélectionnez le **zoom à 200 %**. Pour effectuer un zoom arrière maximal, sélectionnez le **zoom pour ajuster**.

Diagramme d'instructions JavaScript

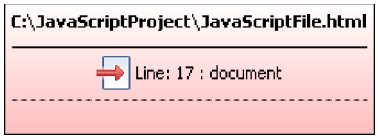
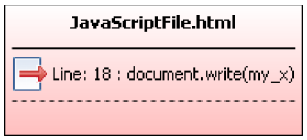
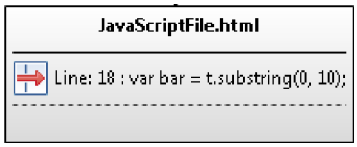
La section du diagramme des instructions d'une trace JavaScript affiche le flux de données entre les instructions.

Dans le diagramme, chaque instruction est un rectangle qui fournit les informations suivantes :

- Le chemin et le nom du fichier affecté. Si l'instruction qui suit se trouve dans le même fichier, seul le nom du fichier est répertorié.
- Le numéro de la ligne qui contient l'instruction.
- Le cas échéant, la section de code qui présente de l'intérêt.
- Si le rectangle est rouge, l'instruction est une source, un collecteur ou les deux.
- Si le rectangle est gris, l'instruction est un propagateur de tache.

- L'infobulle associée à l'instruction contient plus de détails.

Les flèches représentent les données transmises d'une instruction à l'autre.

Symbole	Description
	Flux de données tachées
	Source (rouge) : instruction à l'origine de données potentiellement non sécurisées.
	Collecteur (rouge) : instruction potentiellement vulnérable aux données entachées ou dont l'utilisation est potentiellement dangereuse.
	Propagateur de tache : instruction qui propage une tache à un ou plusieurs de ses paramètres, à sa valeur de retour ou à ce pointeur.

Conseil :

- Dans la vue Trace, survolez les noeuds de trace du graphique pour afficher des informations sur le noeud.
- Les deux panneaux de gauche de la vue (le panneau des piles d'entrée/sortie et le panneau des flux de données) peuvent être réduits pour améliorer l'affichage du diagramme d'appels graphique. Pour réduire ces panneaux, sélectionnez la flèche de **masquage de l'arborescence**. Pour afficher ces panneaux lorsqu'ils sont masqués, sélectionnez la flèche d'**affichage de l'arborescence**.
- Déplacez la barre de défilement pour effectuer un zoom avant détaillé ou effectuer un zoom arrière pour une vue plus générale. Si vous survolez la barre de défilement du zoom, le niveau de zoom actuel s'affiche. Pour effectuer un zoom avant maximum, sélectionnez le **zoom à 200 %**. Pour effectuer un zoom arrière maximal, sélectionnez le **zoom pour ajuster**.

Analyse de code source dans un éditeur

Avec AppScan Source, vous pouvez analyser ou modifier le code source dans un éditeur interne ou choisir parmi une variété d'éditeurs externes.

Les éditeurs externes vous permettent d'examiner les résultats AppScan Source for Analysis et d'apporter des modifications au code dans l'environnement de développement de votre choix. Les éditeurs externes comprennent :

- vi
- Eclipse (voir la configuration requise pour AppScan Source pour savoir quelles versions d'Eclipse sont prises en charge)
- Valeur par défaut du système

Remarque : Vous ne pouvez pas éditer les fichiers source dans un fichier `WAR`.

Pour afficher/modifier le code source de l'éditeur, choisissez l'une des options ci-dessous :

- Effectuez un double-clic sur une constatation dans leur table. L'éditeur interne s'ouvre sur la ligne de code.
- Cliquez avec le bouton droit de la souris sur une constatation dans le tableau et sélectionnez **Ouvrir dans l'éditeur interne** ou **Ouvrir dans l'éditeur externe** > **<éditeur>** (où **<éditeur>** correspond à l'un des éditeurs externes pris en charge répertoriés dans le tableau ci-dessus).
- Sélectionnez un noeud de trace, puis cliquez sur le bouton **Ouvrir dans l'éditeur interne** ou **Ouvrir dans l'éditeur externe** > **<éditeur>** dans la barre d'outils, ou cliquez avec le bouton droit de la souris sur la sélection et sélectionnez **Ouvrir dans l'éditeur interne** ou **Ouvrir dans l'éditeur externe** > **<éditeur>** dans le menu.

Si vous avez ouvert un fichier dans l'éditeur, des marqueurs indiquent les emplacements dans le fichier qui représentent les constatations. Pour remonter à eux dans le tableau des constatations, cliquez avec le bouton droit de la souris sur la ligne de code dans l'éditeur et sélectionnez **Afficher dans la vue Constatations** dans le menu.

Portée de la validation et du codage

Depuis la vue Trace, vous pouvez spécifier des routines de validation et de codage personnalisées qui, une fois stockées dans la Base de connaissances de sécurité AppScan Source Security, marquent les données comme étant vérifiées plutôt qu'entachées. A l'aide de l'assistant Règles personnalisées, vous devez définir ces routines en fonction de leur portée.

Reportez-vous à la rubrique «Exemple 4 : Validation approfondie», à la page 177 pour la procédure de création de routines de validation et de codage.

Les routines de validation ou de codage sont basées sur leur portée et sont définies comme :

- «Spécifique à une API»
- «Spécifique à un site d'appel»

Spécifique à une API

Les routines de validation et de codage spécifiques à des API peuvent être associées à un projet unique ou à plusieurs projets.

Les routines spécifiques à une API désentachent les données provenant de toutes les instances d'une API source spécifique. Vous pourriez, par exemple, spécifier une routine de validation pour toutes les entrées de l'API :

```
javax.servlet.ServletRequest.getParameter
(java.lang.string):java.lang.string
```

Les routines spécifiques à une API sont stockées sur le serveur. Les routines spécifiques aux API d'un projet sont stockées dans le projet.

Spécifique à un site d'appel

Les routines spécifiques à un site d'appel sont toujours associées à un seul projet.

Les routines spécifiques à un site d'appel désentachent les données provenant d'un emplacement spécifique dans le code. Lorsque vous créez une routine de

validation ou de codage spécifique à un site d'appel, vous spécifiez qu'elle s'applique à un site d'appel donné. Les routines spécifiques à un site d'appel sont toujours stockées dans le projet.

Remarque : Elles s'appliquent à tous les appels de la routine de validation dans la même méthode.

Création de règles personnalisées depuis une trace AppScan Source

Vous pouvez créer depuis la vue Trace des règles personnalisées qui vous permettent de filtrer les constatations comportant des traces qui sont des propagateurs de tâche, non vulnérables aux tâches ou des collecteurs. Vous pouvez également marquer les méthodes dans la trace comme des routines de validation/codage (ou indiquer qu'il ne s'agit pas de routines de validation/codage).

Pourquoi et quand exécuter cette tâche

Reportez-vous à la rubrique «Exemple 2 : Création d'une routine de validation/codage depuis la vue Trace», à la page 172 pour consulter un exemple du code source, de la sortie et de la procédure de création des routines de validation et de codage.

Tableau 15. Marquages valides pour les noeuds de la vue Trace

Méthode sélectionnée	Marquage valide
Noeuds intermédiaires	• Routines de validation/codage • Non vulnérable aux tâches • N'est pas une routine de validation/codage
Collecteur indéterminé	• Propagateur de tâche • Non vulnérable aux tâches • Collecteur

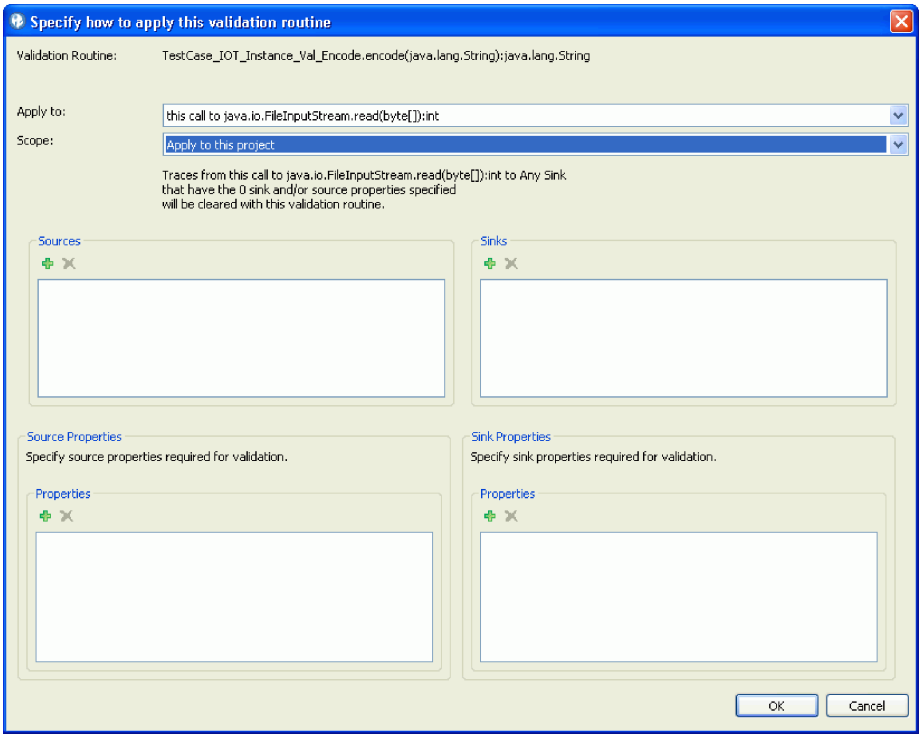
Procédure

1. Dans la vue Trace, cliquez avec le bouton droit de la souris sur la méthode ou le noeud pour lequel vous voulez créer une règle personnalisée, puis sélectionnez la règle personnalisée à créer, ou bien sélectionnez la méthode ou le noeud et cliquez sur le bouton de règle personnalisée approprié dans la barre d'outils. Les options de marquage des routines et des méthodes sont les suivantes :

Option	Description
Marquer comme étant une routine de validation/codage	
Marquer comme n'étant pas une routine de validation/codage	
Marquer comme étant un propagateur de tâche	
Marquer comme non vulnérable aux tâches	
Marquer comme étant un collecteur	

Remarque : Si la vue Trace ne contient aucune entrée pour la méthode pour laquelle vous voulez créer une règle personnalisée, cliquez sur **Lancez l'assistant de règles personnalisées pour ajouter une routine de validation ne figurant pas sur le diagramme de trace**. Dans l'assistant Règles personnalisées, passez à la page Sélectionner une routine de validation/codage. Sélectionnez la routine de validation, puis indiquez l'emplacement, la portée, les sources ou collecteurs, ou les propriétés conformément aux instructions de l'étape suivante. Pour plus de détails sur la création d'une routine de validation à l'aide de cet assistant, voir «Exemple 2 : Création d'une routine de validation/codage depuis l'assistant Règles personnalisées», à la page 175.

2. Si vous créez une règle personnalisée qui marque une méthode comme un collecteur ou une routine de validation/codage, vous devrez peut-être définir d'autres paramètres :
   a. Si vous marquez la méthode comme étant un collecteur, spécifiez les attributs du collecteur :
      - **Type de vulnérabilité**
      - **Gravité**
   b. Pour les routines de validation, indiquez l'emplacement et la portée, ainsi que toutes les sources ou les collecteurs, ou leurs propriétés, pour lesquels la routine de validation doit s'appliquer.



      - **Appliquer à** :
        - **cet appel de <nom méthode>** (spécifique à un site d'appel) : s'applique aux entrées uniquement pour cet appel.
        - **tout appel de <nom méthode>** (spécifique à une API) : s'applique à la routine de validation/codage pour n'importe quel appel de la méthode.

– **<nom de la méthode> non pris en compte, toutes les contraintes spécifiées ci-dessous** : autorise toutes les sources à être affectées par la règle.

- **Portée** :
  – **Appliquer à ce projet** : lorsque ce paramètre est sélectionné, la règle est stockée dans le fichier de projet (`.ppf`).
  – **Appliquer à tous les projets** : les règles de validation créées avec ce paramètre sont stockées dans la base de données.
- **Sources** : sélectionnez les sources d'entrée auxquelles la routine de validation doit s'appliquer. Pour ajouter une source, cliquez sur **Ajouter**, puis sélectionnez la source dans la boîte de dialogue Sélectionner des signatures. Pour ajouter plusieurs sources, vous pouvez les sélectionner simultanément dans la boîte de dialogue Sélectionner des signatures.
- **Collecteurs** : sélectionnez les collecteurs auxquels la routine de validation doit s'appliquer. Pour ajouter un collecteur, cliquez sur **Ajouter**, puis sélectionnez le collecteur dans la boîte de dialogue Sélectionner des signatures. Pour ajouter plusieurs collecteurs, vous pouvez les sélectionner simultanément dans la boîte de dialogue Sélectionner des signatures.
- **Propriétés de source** : si vous voulez que la règle supprime les traces qui commencent dans une source ayant une propriété spécifique, cliquez sur **Ajouter une propriété VMAT** puis sélectionnez la propriété dans la boîte de dialogue Sélection des propriétés. Pour ajouter plusieurs propriétés, vous pouvez les sélectionner simultanément dans la boîte de dialogue Sélection des propriétés.
- **Propriétés de collecteur** : si vous voulez que la règle écarte les traces qui se terminent dans un collecteur ayant une propriété spécifique, cliquez sur **Ajouter une propriété VMAT** puis sélectionnez la propriété dans la boîte de dialogue Sélection des propriétés. Pour ajouter plusieurs propriétés, vous pouvez les sélectionner simultanément dans la boîte de dialogue Sélection des propriétés.

3. Après avoir créé des règles personnalisées dans la vue Trace, vous devez examiner à nouveau votre code pour voir ces règles reflétées dans les traces et les listes de constatations. Les règles personnalisées que vous créez dans la vue Trace peuvent être affichées et supprimées dans la vue Règles personnalisées. Pour afficher les détails d'une règle dans la vue Règles personnalisées, sélectionnez la règle et cliquez sur **Informations de règle personnalisée**.

Exemples de code pour le traçage

Cette section fournit des exemples de code qui illustrent le suivi de trace de données entachées depuis une source vers un collecteur et décrivent comment créer une routine de validation et de codage.

Exemple 1 : D'une source au collecteur

Dans l'exemple de code suivant, la méthode principale appelle une méthode, `getVulnerableSource`, qui renvoie une chaîne. Notez que bien que la méthode lise des données depuis un fichier complètement inconnu, elle ne vérifie jamais la validité des données renvoyées. La méthode principale transmet alors ces données entachées dans `writeToVulnerableSink`. La méthode `writeToVulnerableSink` écrit les données dans le fichier, sans jamais vérifier leur validité.

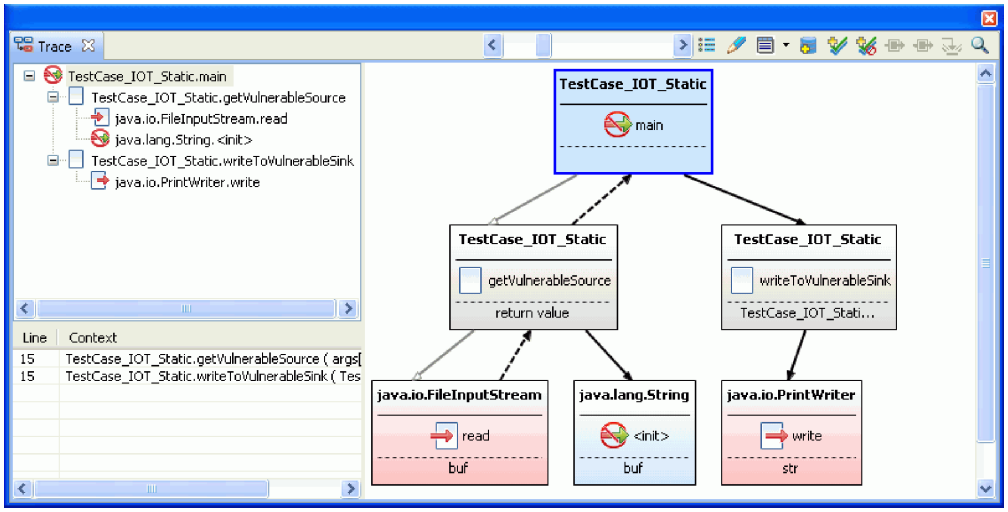
```
import java.io.*;

public class TestCase_IOT_Static {
  public static void main(String[] args) {
    try {
      writeToVulnerableSink(getVulnerableSource(args[0]));
    } catch (Exception e) {
    }
  }

  public static String getVulnerableSource(String file)
    throws java.io.IOException, java.io.FileNotFoundException {
    FileInputStream fis = new FileInputStream(file);
    byte[] buf = new byte[100];
    fis.read(buf);
    String ret = new String(buf);
    fis.close();
    return ret;
  }

  public static void writeToVulnerableSink(String str)
    throws java.io.FileNotFoundException {
    FileOutputStream fos = new FileOutputStream(str);
    PrintWriter writer = new PrintWriter(fos);
    writer.write(str);
  }
}
```

L'exemple de code génère la trace suivante :



Le panneau présente la pile d'entrée dans laquelle `main` appelle `getVulnerableSource` qui appelle `FileInputStream.read` - et la pile de sortie dans laquelle `main` appelle `writeToVulnerableSink` qui appelle `PrintWriter.write`. Le graphique décrit le flux de données depuis la méthode de lecture vers la méthode d'écriture avec la méthode `main` joignant les deux piles d'appel. La section Flux de données indique les numéros de ligne des opérations de la méthode `main` qui

transmettent la tache. Dans cet exemple, les deux appels de méthode existent sur la même ligne (ligne 15) dans la méthode (dans l'exemple de code ci-dessus, cela est transmis au numéro de ligne 7 - dans la capture d'écran, le fichier inclut 8 lignes de commentaires).

Exemple 2 : D'une source au collecteur, avec modification

L'exemple 2 est une modification du code de l'exemple 1. Il étend l'exemple 1 en ajoutant une routine de validation, appelée `getVulnerableSource`, et une routine de codage, appelée dans `writeToVulnerableSink`.

```
import java.io.*;

public class TestCase_IOT_Instance_Val_Encode {
  public static void main(String[] args) {
    try {
      TestCase_IOT_Instance_Val_Encode testCase = new
        TestCase_IOT_Instance_Val_Encode();
      String file = args[0];
      String source = testCase.getVulnerableSource(file);
      source = testCase.validate(source);
      String encodedStr = testCase.encode(source);
      testCase.writeToVulnerableSink(file, encodedStr);
    } catch (Exception e) {
    }
  }

  public String getVulnerableSource(String file) throws Exception {
    FileInputStream fis = new FileInputStream(file);
    byte[] buf = new byte[100];
    fis.read(buf);
    fis.close();

    String ret = new String(buf);
    return ret;
  }

  public void writeToVulnerableSink(String file, String str)
      throws FileNotFoundException {
    FileOutputStream fos = new FileOutputStream(file);
    PrintWriter writer = new PrintWriter(fos);
    writer.write(str);
  }

  private String validate(String source) throws Exception {
    if (source.length() > 100) {
      throw new Exception("Length too long: " + source.length());
    }
  return source;
  }

  private String encode(String source) {
    return source.trim();
  }
}
```

Le premier examen produit une trace de pile similaire à celle de l'exemple 1.

L'extension de la Base de connaissances afin d'inclure des routines de validation et de codage réduit les données parasites dans les constatations et vérifie que ces routines sont appelées pour tous les graphes d'appels. Par exemple, si vous aviez spécifié les données d'un appel quelconque à `java.io.FileInputStream.read(byte[]):int` dans l'exemple précédent, l'examen éliminerait tous les appels de `read` qui appelaient également cette routine de

validation. De même, les appels de `read` n'appelant pas la méthode de validation personnalisée passeraient à l'état de constatation de sécurité définitive, puisque l'abstention de l'appel d'une méthode de validation connue dans le code peut induire des attaques malveillantes.

La routine de validation peut également valider les autres variations des méthodes `read` de `FileInputStream`. Elles peuvent être spécifiées comme des sources supplémentaires. En outre, vous savez peut-être également que seuls certains collecteurs (ou des collecteurs ayant certaines propriétés) sont validés par cette méthode. Par exemple, cette routine pourrait être limitée aux collecteurs ayant la propriété `Technology.IO`, tels que le collecteur `PrintWriter.write` qui est utilisé pour consommer les données de cet exemple.

Exemple 2 : Création d'une routine de validation/codage depuis la vue Trace

Pourquoi et quand exécuter cette tâche

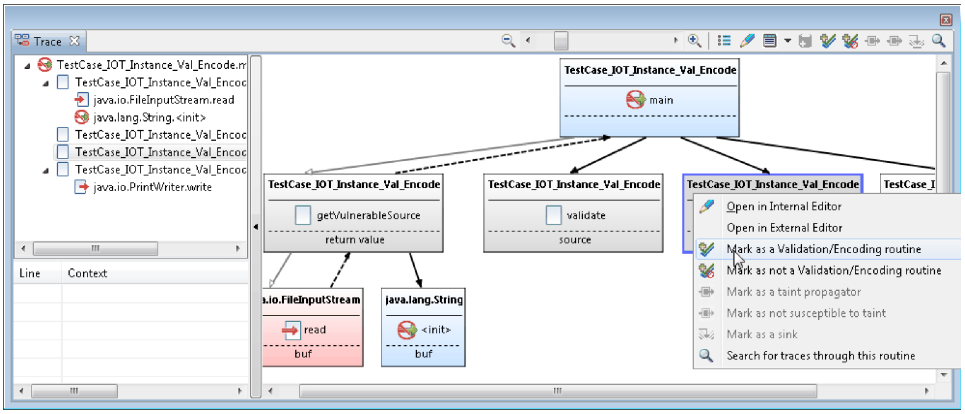
Etant donné que trace AppScan Source identifie la méthode `FileInputStream.read` en tant que source générant des données entachées, vous devriez créer une routine de validation ou de codage de sorte à éliminer cette constatation lors des examens ultérieurs.

Pour créer une routine de validation des entrées pour `FileInputStream.read`, procédez comme suit :

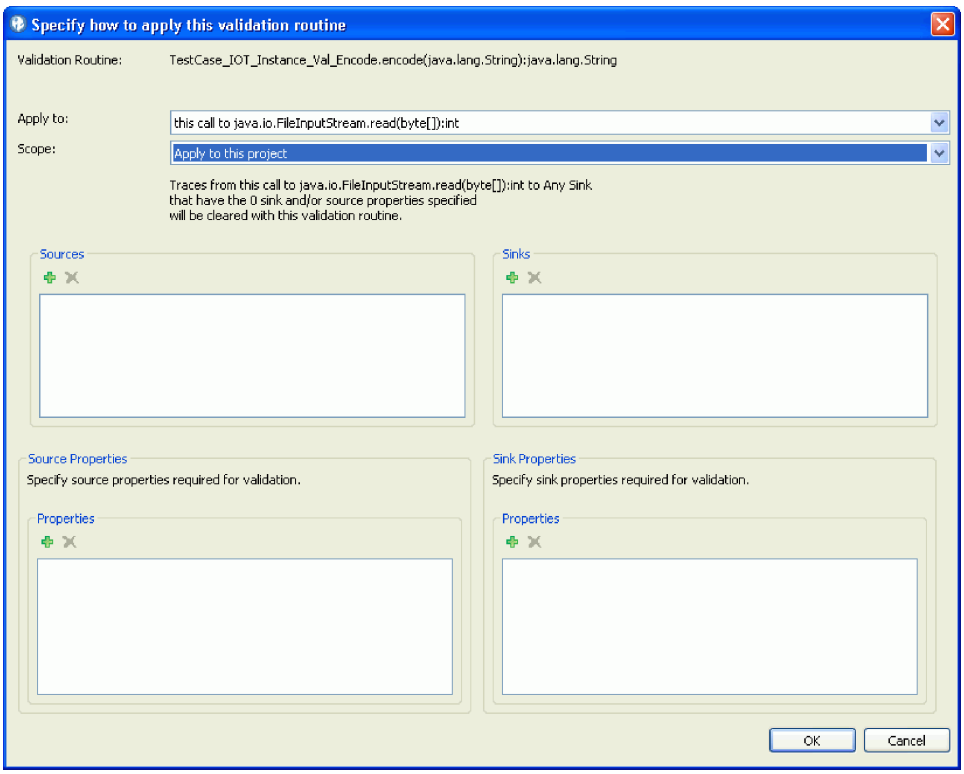
Procédure

1. Dans le graphe d'appels de la vue Trace, sélectionnez et cliquez avec le bouton droit de la souris sur la méthode `TestCase_IOT_Instance_Val_Encode.encode`.

   Conseil : Si la routine de validation/codage que vous voulez créer ne s'affiche pas dans le diagramme de trace, vous pouvez créer la routine en lançant l'assistant Règles personnalisées depuis la vue Trace. L'«Exemple 2 : Création d'une routine de validation/codage depuis l'assistant Règles personnalisées», à la page 175 explique les étapes à suivre dans ce cas.
2. Sélectionnez **Marquer comme étant une routine de validation/codage** dans le menu.



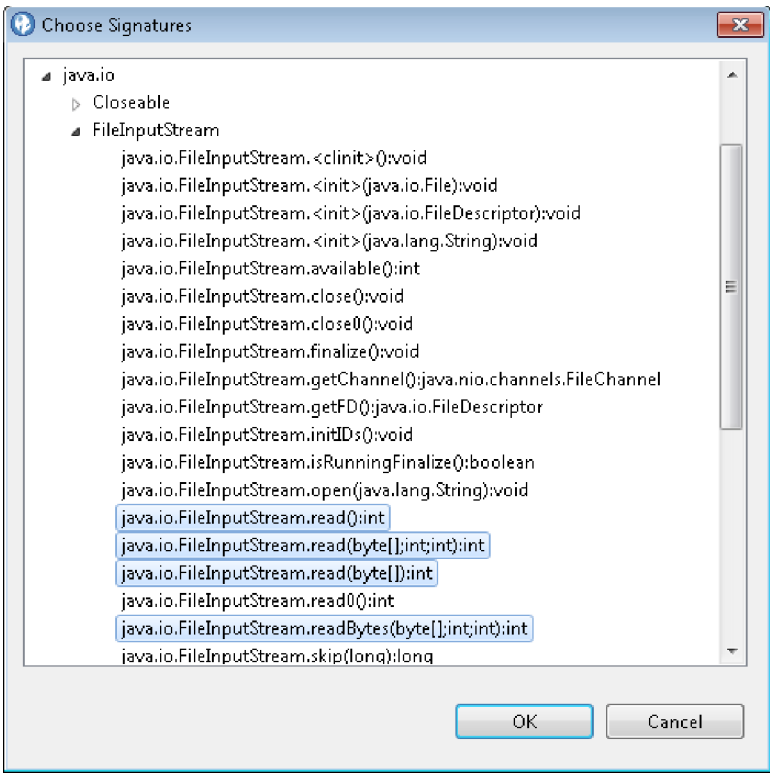
3. Si la routine `encode` s'applique uniquement à cette instance d'appel spécifique `FileInputStream.read`, sélectionnez **cet appel de java.io.FileInputStream.read** dans la boîte de dialogue Spécifiez comment appliquer cette routine de validation.



Généralement, vous devez sélectionner **cet appel de java.io.FileInputStream.read** étant donné que la méthode `validate` est privée pour la classe et étroitement associée à son code.

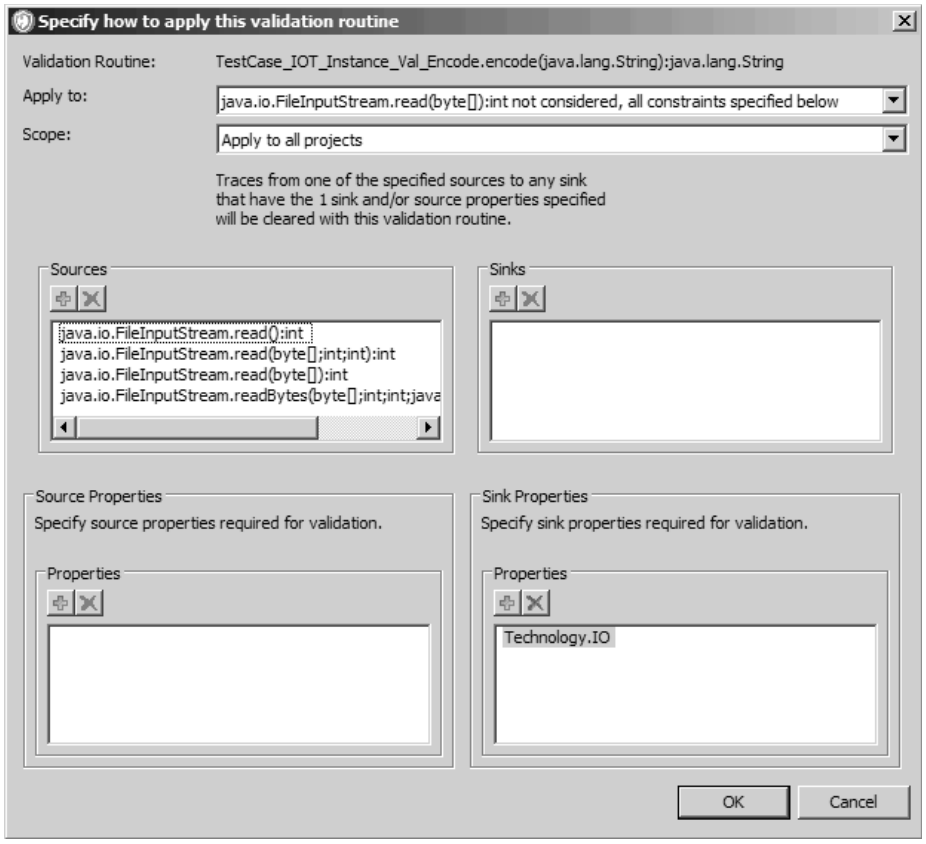
Sélectionnez **tout appel de java.io.FileInputStream.read** pour appliquer la routine de validation à tous les appels de la méthode `read`. Si vous sélectionnez cette option, sélectionnez également **Appliquer à ce projet** si ceci n'est valide que pour le projet en cours ou bien **Appliquer à tous les projets**.

4. Configurez la routine à appliquer à toutes les méthodes `read` de la classe `FileInputStream` et à tout collecteur ayant la propriété `Technology.IO` (par exemple, les méthodes `java.io.PrintWrite.write`) :
   a. **Ajout des méthodes read comme sources** : bien que vous puissiez indiquer **tout appel de java.io.FileInputStream.read(byte[]):int** pour ajouter `java.io.FileInputStream.read(byte[]):int` comme source, nous allons plutôt ajouter les sources individuellement. Dans la boîte de dialogue Spécifiez comment appliquer cette routine de validation, sélectionnez **java.io.FileInputStream.read(byte[]):int non pris en compte, toutes les contraintes spécifiées ci-dessous** dans le menu **Appliquer à**. Cliquez ensuite sur le bouton **Ajouter** de la section **Sources**. Dans la boîte de dialogue Sélectionner des signatures, développez les sections `java.io` puis `FileInputStream`. Sélectionnez les divers noeuds `java.io.FileInputStream.read*`, puis cliquez sur **OK**.



b. **Ajout de la propriété du collecteur** : cliquez sur le bouton **Ajouter une propriété VMAT** de la section **Propriétés de collecteur**. Dans la boîte de dialogue Sélection des propriétés, sélectionnez la propriété `Technology.IO` et cliquez ensuite sur **OK**.

c. Lorsque tous les paramètres sont définis, la boîte de dialogue doit se présenter comme suit :



5. Cliquez sur **OK** pour ajouter la routine de validation à la base de données.

Exemple 2 : Création d'une routine de validation/codage depuis l'assistant Règles personnalisées

Si la routine de validation/codage que vous voulez créer ne s'affiche pas dans le diagramme de trace, vous pouvez créer la routine en lançant l'assistant Règles personnalisées depuis la vue Trace.

Pourquoi et quand exécuter cette tâche

Cet exemple va créer la même routine de validation que celle créée dans l'«Exemple 2 : Création d'une routine de validation/codage depuis la vue Trace», à la page 172, cependant, dans cet exemple, la routine sera créée à l'aide de l'assistant Règles personnalisées.

Procédure

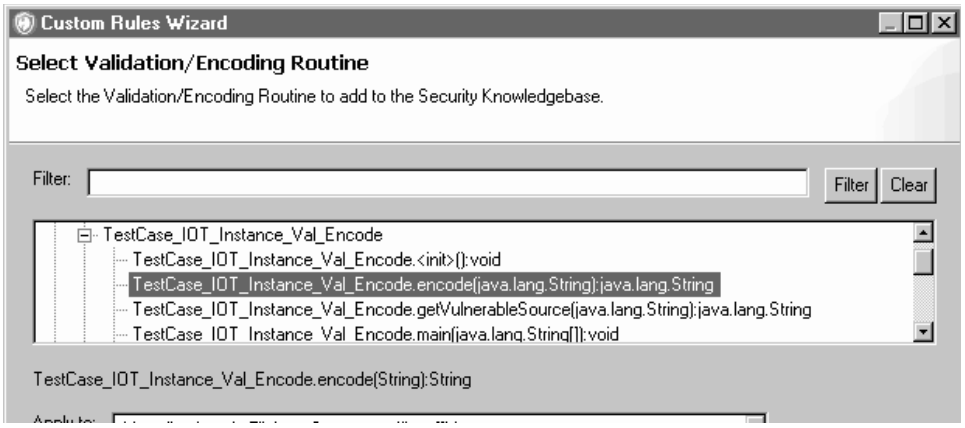
1. Dans la vue Trace, cliquez sur **Lancez l'assistant de règles personnalisées pour ajouter une routine de validation ne figurant pas sur le diagramme de trace** dans la barre d'outils.

   Remarque : Vous ne pouvez pas créer une routine de validation à partir de l'assistant Règles personnalisées lorsque ce dernier est lancé à partir de la vue Règles personnalisées.

2. Dans la page Sélectionner une routine de validation/codage de l'assistant, indiquez l'emplacement de la routine de validation.

   Pour cet exemple, sélectionnez la routine suivante :

   ```
   TestCase_IOT_Instance_Val_Encode.encode(java.lang.String):
   java.lang.String
   ```



3. Complétez les autres sections de la page de l'assistant avec les mêmes paramètres que ceux définis dans la boîte de dialogue **Spécifiez comment appliquer cette routine de validation** dans l'«Exemple 2 : Création d'une routine de validation/codage depuis la vue Trace», à la page 172.
4. Cliquez sur **Terminer** pour ajouter la routine de validation à la base de données.

Exemple 3 : Fichiers source et collecteur modifiés

L'exemple suivant illustre la source dans un fichier différent du collecteur.

TestCase_IOT_Xfile_Part1.java:

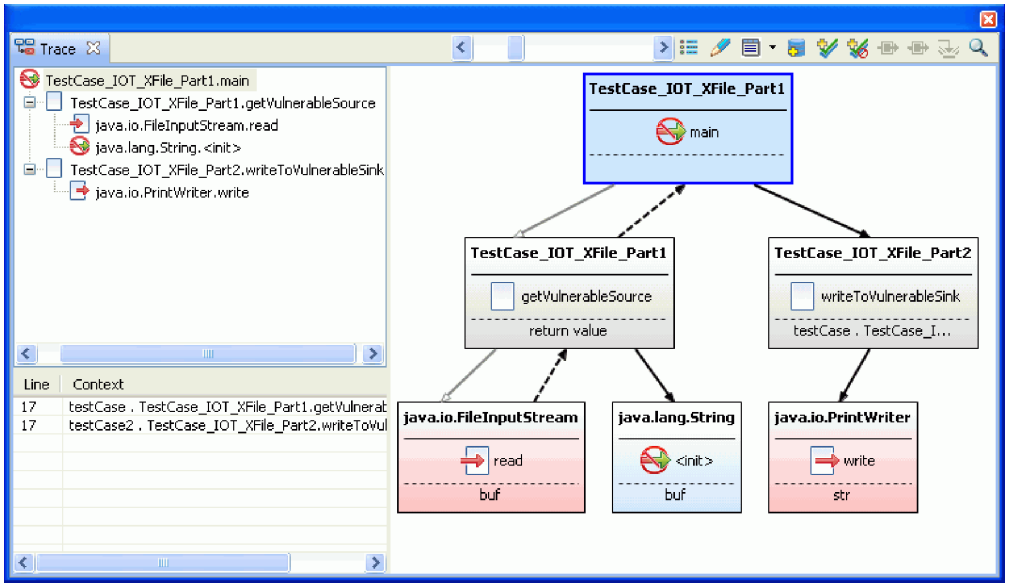
```
public class TestCase_IOT_XFile_Part1 {
 public static void main(String[] args) {
  try {
   TestCase_IOT_XFile_Part1 testCase =
    new TestCase_IOT_XFile_Part1();
   TestCase_IOT_XFile_Part2 testCase2 =
    new TestCase_IOT_XFile_Part2();
   testCase2.writeToVulnerableSink(
    testCase.getVulnerableSource(args[0]));
  } catch (Exception e) {
  }
 }

 public String getVulnerableSource(String file)
  throws IOException, FileNotFoundException {
  FileInputStream fis = new FileInputStream(file);
  byte[] buf = new byte[100];
  fis.read(buf);
  String ret = new String(buf);
  fis.close();
  return ret;
 }
}
```

TestCase_IOT_Xfile_Part2.java:

```
public class TestCase_IOT_XFile_Part2 {
 public void writeToVulnerableSink(String str)
  throws FileNotFoundException {
  FileOutputStream fos = new FileOutputStream(str);
  PrintWriter writer = new PrintWriter(fos);
  writer.write(str);
 }
}
```

Le traçage des données depuis `TestCase_IOT_Xfile_Part1.java` vers `TestCase_IOT_Xfile_Part2.java` permet de tracer le flux de données à travers tout le programme. La trace de pile affiche :



Cet exemple illustre le flux des données depuis `TestCase_IOT_XFile_Part1` vers `TestCase_IOT_XFile_Part2` via la méthode 'main'.

Exemple 4 : Validation approfondie

Lorsque vous examinez le code de l'exemple 4, le premier examen inclut trois traces AppScan Source avec une racine aux routines de trace correspondantes. Cet exemple suppose la sélection de la méthode `FileInputStream.read` dans `trace1` et l'ajout de la routine `validate`. Les sections à la suite de l'exemple de code source décrivent les effets de chaque portée pour la routine de validation.

```
public class TestCase_IOT_UserValidation {
    ResultSet resultSet;
    FileInputStream fileInputStream;
    PrintWriter printWriter;
    byte[] buffer;

    public static void main(String[] args) throws Exception {
        TestCase_IOT_UserValidation testCase = new TestCase_IOT_UserValidation();
        testCase.trace1();

        TestCase_IOT_UserValidation testCase2 = new TestCase_IOT_UserValidation();
        testCase2.trace2();

        TestCase_IOT_UserValidation testCase3 = new TestCase_IOT_UserValidation();
        testCase3.trace3();
    }

    private void trace1() throws Exception {
        String source = getVulnerableSource1();
        source = validate(source);
        writeToVulnerableSink(source);
    }

    private void trace2() throws Exception {
        String source = getVulnerableSource2();
        source = validate(source);
        writeToVulnerableSink(source);
    }
```

```
    private void trace3() throws Exception {
        String source = getVulnerableSource3();
        source = validate(source);
        writeToVulnerableSink(source);
    }

    public String getVulnerableSource1() throws Exception {
        fileInputStream.read(buffer);
        return new String(buffer);
    }

    public String getVulnerableSource2() throws Exception {
        fileInputStream.read(buffer);
        return new String(buffer);
    }

    public String getVulnerableSource3() throws Exception {
        return resultSet.getString("x");
    }

    public void writeToVulnerableSink(String str) throws Exception {
        printWriter.write(str);
    }

    private String validate(String source) throws Exception {
        // validate
        return source;
    }
}
```

Routine de validation spécifique à un site d'appel - Entrées pour cet appel de `FileInputStream.read`

Créez une routine de validation spécifique à un site d'appel lorsque cette validation n'est adaptée qu'à un concept très étroit ou que la méthode d'entrée est trop générique pour ne prévoir qu'une seule routine de validation. Lorsque vous sélectionnez **Appliquer à cet appel de FileInputStream.read** dans la méthode `trace1`, `trace1` n'apparaît pas comme une constatation après l'examen suivant étant donné que sa pile d'appels inclut un appel de la méthode `validate`. Cependant, `trace2` est toujours signalé bien qu'il appelle `validate`, étant donné que la portée de la routine de validation est liée au site d'appel `trace1`. La méthode `trace3` appelle également `validate`, mais continue à être signalée car elle utilise `ResultSet.getString` comme source.

Routine de validation spécifique à un site d'appel - Entrées pour cet appel de `FileInputStream.read`

Créez une routine de validation spécifique à une API lorsque la validation est applicable uniquement pour une source déterminée. Lorsque vous sélectionnez la méthode **Appliquer à tout appel de FileInputStream.read**, les méthodes `trace1` et `trace2` ne génèrent pas de constatation à l'examen suivant car elles incluent un appel de la méthode `validate`. Cependant, la méthode `trace3` continue à être signalée bien qu'elle appelle `validate` vu qu'elle utilise `ResultSet.getString` comme source.

Chapitre 7. AppScan Source for Analysis et suivi des défauts

AppScan Source for Analysis s'intègre à IBM Rational Team Concert pour signaler directement les vulnérabilités logicielles avérées au bureau du développeur. La soumission de défaut à un système de suivi des défauts comprend une description du bogue, ainsi qu'un fichier contenant uniquement les constatations soumises avec le défaut.

Avant de soumettre un défaut au système de suivi des défauts ou de le soumettre à un développeur par courrier électronique, il se peut que vous ayez à configurer les préférences du système de suivi des défauts (voir «Activation du suivi des défauts depuis les préférences», à la page 79).

Activation du suivi des défauts depuis les préférences

Les préférences du système de suivi des défauts permettent d'activer la soumission des constatations à un système de suivi des défauts et de déterminer la manière dont celle-ci s'effectue.

L'onglet Options générales de la page des préférences Système de suivi des défauts permet d'activer ou de désactiver la fonction d'intégration de ce système avec AppScan Source. Si la case **Activer l'intégration du système de suivi des défauts** est cochée, l'action **Soumettre un défaut** sera disponible dans le menu contextuel pour son application aux constatations de l'évaluation.

Pour en savoir plus sur les préférences pouvant être définies pour les systèmes de suivi des défauts pris en charge, consultez les rubriques d'aide ci-dessous.

- «Préférences Rational Team Concert», à la page 80

Préférences Rational Team Concert

L'onglet des préférences Rational Team Concert vous permet de configurer une connexion avec un serveur Rational Team Concert, ainsi que les valeurs des attributs des éléments de travail.

Après avoir saisi vos informations de connexion et avoir établi une connexion, vous pouvez opter de vous connecter à une ou plusieurs zones de projet. Chaque zone projet peut disposer de sa propre configuration de valeurs d'attributs prédéfinies.

Remarque : Lorsque vous vous connectez à Rational Team Concert (en configurant des préférences ou en soumettant des défauts), il se peut que le système vous invite à accepter un certificat SSL. Pour plus d'informations, voir «Certificats SSL pour Rational Team Concert», à la page 80.

Pour configurer les valeurs d'attributs d'une zone de projet donnée, sélectionnez celle-ci, puis l'option **Configurer**. Dans la boîte de dialogue de configuration, vous pouvez affecter à ces zones des valeurs d'attributs codées en dur ou, dans certains cas, des variables se référant à une constatation spécifique. Par exemple, l'utilisation de `{Finding.fileName}` comme valeur d'attribut sera remplacée lors de sa soumission par le nom de fichier effectif du code source d'une constatation. Une assistance sur le contenu (`<Ctrl>+<Espace>`) est fournie pour les valeurs d'attributs

prenant en charge ces variables. Nous encourageons les équipes à partager ces configurations à l'aide des boutons **Importer** et **Exporter** disponibles sur la page des préférences Rational Team Concert.

Intégration de Rational Team Concert et de AppScan Source for Analysis

L'intégration de Rational Team Concert avec AppScan Source for Analysis ne nécessite pas l'installation d'un client Rational Team Concert supplémentaire sur votre ordinateur.

Pour configurer une connexion avec Rational Team Concert, accédez à l'onglet Rational Team Concert dans les préférences Système de suivi des défauts (vous pouvez également soumettre un défaut, auquel cas vous serez invité à ce point à vous connecter et à configurer votre connexion).

Les préférences Rational Team Concert vous permettent également de configurer les valeurs de zones prédéfinies qui seront utilisées lors de la soumission de défauts. Ceci vous permet de définir les valeurs que vous désirez utiliser pour chaque défaut et de modifier celles fournies par défaut avec AppScan Source.

Remarque : Lorsque vous vous connectez à Rational Team Concert (en configurant des préférences ou en soumettant des défauts), il se peut que le système vous invite à accepter un certificat SSL. Pour plus d'informations, voir «Certificats SSL pour Rational Team Concert», à la page 80.

Soumission de défauts à Rational Team Concert

Vous pouvez soumettre à Rational Team Concert des groupements contenant une ou plusieurs constations ou bien lui soumettre des constatations individuelles. Lors de la première soumission d'une constatation depuis AppScan Source for Analysis à Rational Team Concert, vous devez vous connecter en fournissant votre nom d'utilisateur et votre mot de passe. Si vous désirez configurer les valeurs de zones prédéfinies à utiliser lors de la soumission de défauts, accédez à la page des préférences Rational Team Concert.

Pourquoi et quand exécuter cette tâche

Lors de la soumission d'un groupement à Rational Team Concert, le numéro de l'élément de travail est associé aux constatations spécifiques du groupement et non pas au groupement lui-même. De la sorte, vous pouvez continuer à manipuler le groupement tout en préservant l'association de constatations spécifiques avec des numéros d'élément de travail.

Procédure

1. Sélectionnez les constatations dans le tableau ou ouvrez le groupement (dans ce cas, sélectionnez dans le groupement les constatations à soumettre).
2. Cliquez avec le bouton droit de la souris sur votre sélection et sélectionnez **Soumettre un défaut** > **Envoyer à Rational Team Concert** dans le menu.
3. La boîte de dialogue de soumission vous guidera alors le long de la procédure, y-compris la connexion, en cas de besoin, et le renseignement des attributs requis.

   Remarque : Lorsque vous vous connectez à Rational Team Concert (en configurant des préférences ou en soumettant des défauts), il se peut que le

système vous invite à accepter un certificat SSL. Pour plus d'informations, voir «Certificats SSL pour Rational Team Concert», à la page 80.

Résultats

Un groupement sera automatiquement ajouté à l'élément de travail soumis et ce groupement pourra être ouvert par la suite par un utilisateur de AppScan Source for Analysis ou de AppScan Source for Development.

Certificats SSL pour Rational Team Concert

Une fois qu'un serveur Rational Team Concert est installé, vous devez le configurer afin qu'il utilise un certificat SSL valide. Faute de quoi, vous recevez un message indiquant que la connexion est non sécurisée lors de la connexion au serveur (lors de configuration de préférences ou de la soumission de défauts). Cette rubrique contient des remarques sur le certificat SSL Rational Team Concert.

Emplacement de stockage du certificat SSL

Les certificats qui ont été acceptés de manière définitive sont stockés dans `<user_home>/.jazzcerts` (où `<user_home>` est le répertoire d'accueil de votre système d'exploitation (par exemple, sous Windows, le répertoire peut être `C:\Documents and Settings\Administrator\`)). Si vous supprimez `<user_home>/.jazzcerts`, tous les certificats stockés pour les clients AppScan Source et Rational Team Concert sont supprimés.

Partage de certificat SSL avec des clients Rational Team Concert

AppScan Source partage son magasin de certificats avec des clients Rational Team Concert. Si vous acceptez un certificat de façon définitive à l'aide d'un client Rational Team Concert, il sera réutilisé par AppScan Source (AppScan Source vous invitera à accepter un certificat). De la même façon, si vous acceptez un certificat de façon définitive dans AppScan Source, il sera réutilisé par des clients Rational Team Concert.

Exploitation des défauts soumis

Lorsque vous soumettez plusieurs constatations en tant que défauts distincts, le processus s'exécute en arrière-plan tandis que vous poursuivez la procédure de triage. Après la soumission du défaut, un ID de défaut reçu du système de suivi des défauts est rattaché aux constatations pertinentes et leur reste associé. Pour travailler avec un défaut soumis à votre système de suivi des défauts, suivez les procédures décrites dans cette rubrique.

Procédure

1. Ouvrez votre système de suivi des défauts et localisez le défaut concerné.
2. Enregistrez la pièce jointe en tant que fichier de groupement AppScan Source (`.ozbdl`). Vous pouvez ouvrir ce fichier dans AppScan Source for Analysis.

Soumission de groupements au système de suivi des défauts et par courrier électronique

Les constatations figurant dans des groupements peuvent être soumises au système de suivi des défauts de votre entreprise ou envoyées par e-mail. Une fois ces constatations placées dans un groupement, vous pouvez les soumettre en tant que bogues pour leur résolution par un développeur.

Procédure

1. Ouvrez le groupement.
2. Cliquez sur la flèche vers le bas du bouton de barre d'outils **Soumettre un groupement pour suivi des défauts** et sélectionnez ensuite le système de suivi des défauts.

   Remarque : En fonction de votre système de suivi des défauts, il peut s'avérer nécessaire de modifier les préférences Système de suivi des défauts avant de soumettre le groupement.

   Dans la barre d'outils Groupement, vous pouvez également cliquer sur **Envoi du groupement par courrier électronique** pour envoyer le groupement à d'autres (les préférences de courrier électronique doivent avoir été configurées précédemment).
3. Renseignez les boîtes de dialogue de configuration qui s'affichent. Celles-ci varient en fonction du système de suivi des défauts que vous avez choisi. Elles sont décrites dans la section de l'aide relative à *AppScan Source for Analysis et au système de suivi des défauts*.

Suivi des défauts par courrier électronique (envoi de constatations par courrier électronique)

Pourquoi et quand exécuter cette tâche

Si vous avez configuré des préférences de courrier électronique, vous pouvez envoyer directement des constatations ou des groupements par courrier électronique à des développeurs pour les informer des défauts potentiellement détectés après un examen. Le courrier électronique comportera une pièce jointe contenant les constatations et le texte décrivant ces constatations.

Remarque : Certains relais SMTP ne distribuent les courriers qu'à des domaines spécifiques. Dans ce cas, si vous envoyez un courrier électronique depuis `mydomain.com`, seuls les destinataires sur de ce domaine peuvent recevoir le courrier électronique via AppScan Source for Analysis.

Pour envoyer par courrier électronique les constatations à partir d'un tableau des constatations :

Procédure

1. Sélectionnez les constatations dans le tableau ou ouvrez un regroupement. Si vous ouvrez un regroupement, sélectionnez les constatations à envoyer par courrier électronique.
2. Cliquez avec le bouton droit de la souris sur votre sélection et sélectionnez **Envoi de constatations par courrier électronique** dans le menu.
3. Le courrier électronique inclut en pièce jointe un groupement contenant les constatations. Dans la boîte de dialogue Nom de fichier de pièce jointe,

spécifiez un nom pour le groupement de constatations. Par exemple, si vous spécifiez `ma_constatation` dans la zone **Nom du fichier de pièce jointe**, un groupement avec le nom de fichier `ma_constatation.ozbdl` sera joint au courrier. Cliquez sur **OK** pour ouvrir la boîte de dialogue Envoi de constatations par courrier électronique.

4. Par défaut, la zone **Envoyer à** de la boîte de dialogue d'envoi de constatations par courrier électronique contient les données de la zone **Adresse de destination** qui est spécifiée dans les préférences de courrier électronique. Toutefois, elle peut facilement être modifiée lors de la préparation du courrier électronique. Dans cette boîte de dialogue, cliquez sur **OK** pour envoyer le courrier électronique après avoir vérifié son contenu.

Résultats

Exemple de contenu de courrier électronique :

```
1 constatations :
Nom : JavaAny.test_DataInput
Type : Vulnerability.Validation.Required
Gravité : Faible
Classification : Suspectée
Nom de fichier : C:\TestApps\java\JavaAny\src\JavaAny.java
Ligne / Col : 275 / 0
Contexte : di . java.io.DataInput.readFully ( ba )
Remarques : Examinez cette vulnérabilité et rendez compte dès que possible.
```

Conseil : Vous pouvez envoyer par courrier électronique des constatations individuelles ou des groupements depuis la vue Constatation détaillée. Vous pouvez également envoyer les groupements par e-mail en cliquant sur **Envoi du groupement par courrier électronique** dans la barre d'outils Groupement.

Chapitre 8. Recherche des rapports et des rapports d'audit

Les analystes de la sécurité et les gestionnaires des risques peuvent accéder à des rapports sur des constatations spécifiques ou à une série de rapports d'audit évaluant la conformité avec les pratiques optimales en matière de sécurité et les exigences réglementaires. Cette section décrit comment créer des rapports sur les données de constatations agrégées.

AppScan Source for Analysis génère deux types de rapport - les rapports sur les constatations et les rapports AppScan Source. Un *rapport sur les constatations* est un rapport sur des constatations sélectionnées. Un *rapport AppScan Source* est un rapport basé sur les regroupements en catégories de toutes les constatations adapté à une politique de sécurité spécifique. Les rapports AppScan Source sont répertoriés dans «Rapports AppScan Source», à la page 187.

Les rapports fournissent des informations détaillées sur les constatations recueillies lors d'un examen spécifique et tous les rapports AppScan Source peuvent contenir des notes et des données de trace quelconques ajoutées aux constatations. La longueur du rapport est fonction du nombre de constatations incluses dans le rapport. Vous pouvez générer des rapports sous forme de fichiers PDF ou HTML (Hypertext Markup Language). Les rapports HTML fonctionnent comme des pages Web dans lesquelles vous pouvez accéder à une section en cliquant sur un bouton ou sur un lien. Vous pouvez ensuite naviguer dans les informations à l'aide des fonctions présentes dans les navigateurs Web.

Les rapports répertorient également les filtres de durée d'examen qui ont été appliqués aux constatations. Ces filtres sont décrits dans «Détermination des filtres appliqués», à la page 136.

Création de rapports sur les constatations

Pourquoi et quand exécuter cette tâche

Après un examen, vous pouvez vouloir générer des rapports sur les vulnérabilités identifiées. Vous pouvez générer de nombreux rapports sur les constatations :

- Constatations
- Constatations par type
- Constatations par classification
- Constatations par fichier
- Constatations par API
- Constatations par groupement
- Constatations par énumération des faiblesses courantes (CWE)
- Activité DTS

Remarque : Les rapports Constatations présentent les constatations détaillées par catégorie, de manière similaire aux résultats de la table des constatations. La génération de rapports sur les constatations peut utiliser beaucoup de mémoire (voir la rubrique associée à l'adresse https://xmlgraphics.apache.org/fop/1.1/running.html#memory) et nécessiter jusqu'à 1024 Mo de mémoire système supplémentaire. Si vous générez un rapport d'examen d'une application

volumineuse et que vous observez des problèmes de mémoire, vous pouvez examiner des parties de votre application séparément ou modifier votre configuration d'examen, puis essayer de générer à nouveau le ou les rapports.

Les hyperliens des ID CWE dans le rapport des constatations renvoient au site CWE à l'adresse http://cwe.mitre.org/.

Pour générer un rapport sur les constatations, procédez comme suit :

Procédure

1. Dans une vue contenant des constatations, sélectionnez celles à inclure dans le rapport. Si vous n'en sélectionnez aucune, le rapport couvre toutes les constatations présentes dans la vue active.

   Dans le menu **Outils**, cliquez sur **Générer un rapport sur les constatations**. Vous pouvez également sélectionner et cliquer avec le bouton droit de la souris sur un ensemble de constatations dans une vue, puis cliquer sur **Générer un rapport sur les constatations** dans le menu.
2. Dans la boîte de dialogue **Sélection du rapport sur les constatations**, sélectionnez un type de rapport.

   Cliquez sur **Terminer** pour générer le rapport ou cliquez sur **Suivant** pour spécifier les paramètres facultatifs dans la page Spécifiez la destination et la feuille de style :

   - Vous pouvez spécifier la destination et le format du rapport. Vous pouvez générer le rapport au format HTML, en tant que fichier ZIP contenant tous les éléments du rapport HTML ou en tant que fichier PDF (vous devez disposer d'Adobe Acrobat Reader pour afficher les rapports au format PDF). Si vous ne spécifiez pas la destination ni le format du rapport (ou si vous cliquez sur **Terminer** dans la page Sélection du rapport sur les constatations), le format HTML est choisi par défaut et le rapport est sauvegardé dans `<data_dir>\reports` (où `<rép_données>` est l'emplacement de vos données de programme AppScan Source, comme décrit dans «Installation et emplacements des fichiers de données utilisateur», à la page 292).

     Remarque : Si vous créez un rapport personnalisé (plutôt qu'un rapport de constatations) au format PDF, vous pouvez indiquer le niveau de détail à inclure dans le rapport :

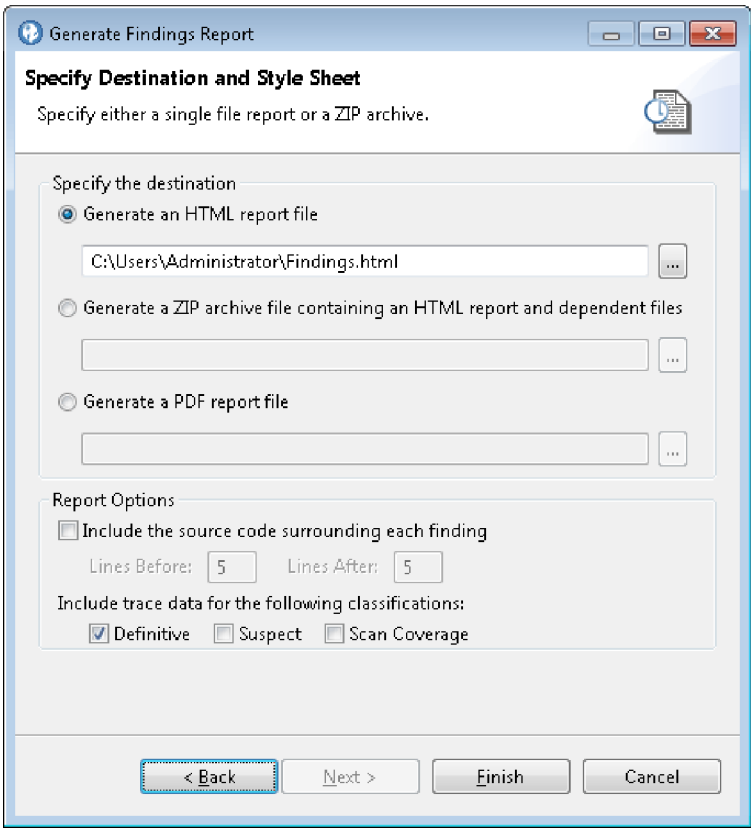
     – **Récapitulatif** : contient un comptage pour chaque groupe du rapport
     – **Détaillé** : contient un comptage pour chaque API de chaque propriété d'une vulnérabilité
     – **Complet** : contient des tableaux pour chaque constatation de chaque API
     – **Annoté** : contient toutes les constatations et les notes, données de trace ou fragments de code éventuels inclus avec les constatations
   - Pour inclure un fragment de code dans le rapport, sélectionnez **Inclure le code source autour de chaque constatation** et indiquez le nombre de ligne avant et après la ligne de code vulnérable à inclure dans le rapport.

     Conseil : Dans la section Génération de rapport de la vue Constatation détaillée, vous pouvez également définir le nombre de lignes de code à inclure avant et après la constatation dans les rapports.

     Une fois le rapport généré, lorsque vous développez une constatation contenant des notes ou des fragments de code, le code source apparaît en dessous de la constatation dans un cadre bleu ou en-dessous de la note en jaune. Le texte rouge en gras met en évidence la ligne de code vulnérable.

- Pour inclure les données de trace AppScan Source dans le rapport, sélectionnez une ou plusieurs classifications (**Définitive**, **Suspectée** ou **Couverture d'examen**) sous **Inclure les données de trace pour les classifications suivantes**.

Cliquez sur **Terminer** pour générer le rapport.



Rapports AppScan Source

Les rapports AppScan Source aident les analystes de la sécurité des logiciels, les responsables du développement et les auditeurs de la gestion du risque à mesurer la conformité avec les pratiques optimales en matière de sécurité et les exigences réglementaires. Les rapports AppScan Source aident à vérifier que vos applications critiques respectent les normes de sécurité que vous avez établies.

AppScan Source utilise les résultats des analyses de vulnérabilité du code source alimentent une série de rapports fournissant aux professionnels de la sécurité, du développement ou de l'audit une image détaillée de la conformité.

Les rapports AppScan Source se distinguent par :

- Une carte de rapport : carte de rapport affichant succinctement l'état de la sécurité de chaque catégorie principale
- Une revue d'audit détaillée : audit détaillé des constatations sans conformité
- Une fonction d'exploration en aval : permet un accès direct au code non conforme pour analyse complémentaire et établissement des priorités de résolution et d'affectation

AppScan Source for Analysis génère différents rapports AppScan Source :

- «Rapport CWE/SANS Top 25 2011», à la page 189
- «Rapport DISA Application Security and Development STIG V3R10», à la page 190
- «Rapport Open Web Application Security Project (OWASP) Mobile Top 10», à la page 190
- «Rapport Open Web Application Security Project (OWASP) Top 10 2013», à la page 190
- «Rapport PCI DSS (Payment Card Industry Data Security Standard) version 3.2», à la page 190
- «Rapport Profil de sécurité logicielle», à la page 190 : fournit une vue d'ensemble de l'état de la sécurité d'une application en couvrant les catégories de vulnérabilité essentielles.

Création d'un rapport AppScan Source personnalisé

Procédure

1. Dans le menu **Outils**, cliquez sur **Générer un rapport**.
2. Dans la boîte de dialogue Générer le rapport, sélectionnez un rapport AppScan Source :
   - **CWE SANS Top 25 2011**
   - **DISA Application Security and Development STIG V3R10**
   - **OWASP Mobile Top 10**
   - **OWASP Top 10 2013**
   - **PCI Data Security Standard version 3.2**
   - **Profil de sécurité logicielle**

   Cliquez sur **Terminer** pour générer le rapport ou cliquez sur **Suivant** pour spécifier les paramètres facultatifs dans la page Spécifiez la destination et la feuille de style :
   - Vous pouvez spécifier la destination et le format du rapport. Vous pouvez générer le rapport au format HTML, en tant que fichier ZIP contenant tous les éléments du rapport HTML ou en tant que fichier PDF (vous devez disposer d'Adobe Acrobat Reader pour afficher les rapports au format PDF). Si vous ne spécifiez pas la destination ni le format du rapport (ou si vous cliquez sur **Terminer** dans la page Sélection du rapport sur les constatations), le format HTML est choisi par défaut et le rapport est sauvegardé dans `<data_dir>\reports` (où `<rép_données>` est l'emplacement de vos données de programme AppScan Source, comme décrit dans «Installation et emplacements des fichiers de données utilisateur», à la page 292).

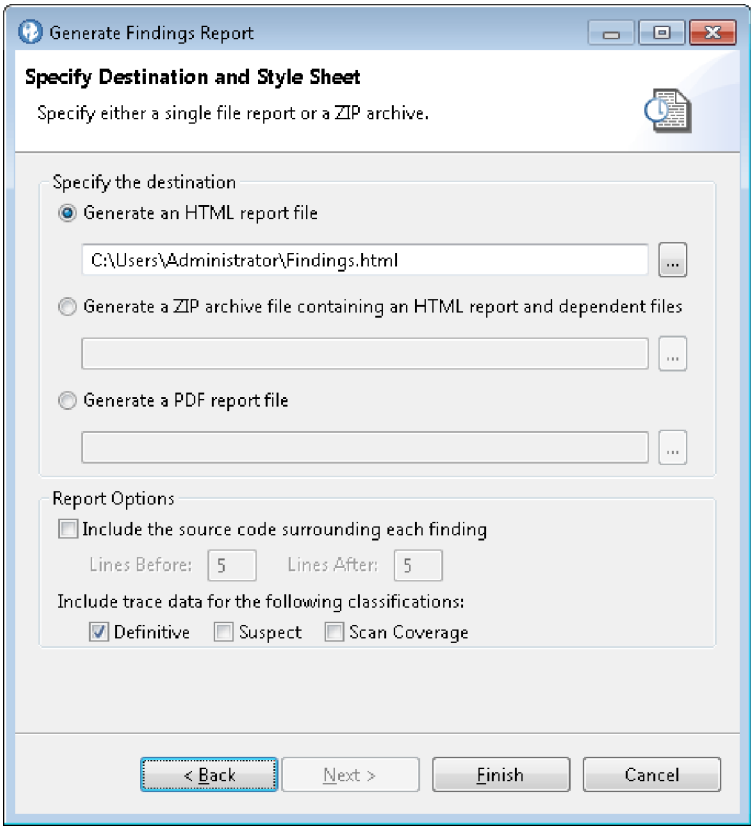
     Remarque : Si vous créez un rapport personnalisé (plutôt qu'un rapport de constatations) au format PDF, vous pouvez indiquer le niveau de détail à inclure dans le rapport :
     - **Récapitulatif** : contient un comptage pour chaque groupe du rapport
     - **Détaillé** : contient un comptage pour chaque API de chaque propriété d'une vulnérabilité
     - **Complet** : contient des tableaux pour chaque constatation de chaque API
     - **Annoté** : contient toutes les constatations et les notes, données de trace ou fragments de code éventuels inclus avec les constatations
   - Pour inclure un fragment de code dans le rapport, sélectionnez **Inclure le code source autour de chaque constatation** et indiquez le nombre de ligne avant et après la ligne de code vulnérable à inclure dans le rapport.

Conseil : Dans la section Génération de rapport de la vue Constatation détaillée, vous pouvez également définir le nombre de lignes de code à inclure avant et après la constatation dans les rapports.

Une fois le rapport généré, lorsque vous développez une constatation contenant des notes ou des fragments de code, le code source apparaît en dessous de la constatation dans un cadre bleu ou en-dessous de la note en jaune. Le texte rouge en gras met en évidence la ligne de code vulnérable.

- Pour inclure les données de trace AppScan Source dans le rapport, sélectionnez une ou plusieurs classifications (**Définitive**, **Suspectée** ou **Couverture d'examen**) sous **Inclure les données de trace pour les classifications suivantes**.

Cliquez sur **Terminer** pour générer le rapport.



Rapport CWE/SANS Top 25 2011

Le rapport CWE/SANS Top 25 2011 est basé sur la liste des 25 erreurs logicielles CWE/SANS les plus dangereuses, *2011 CWE/SANS Top 25 Most Dangerous Software Errors*, pour 2011.

Pour en savoir plus sur la liste *2011 CWE/SANS Top 25 Most Dangerous Software Errors*, voir http://cwe.mitre.org/top25/.

Pour en savoir plus sur toutes les faiblesses Common Weakness Enumeration (CWE) prises en charge par AppScan Source, voir Chapitre 15, «Prise en charge de CWE», à la page 297.

Rapport DISA Application Security and Development STIG V3R10

Cette rubrique propose des liens vers le site Web du guide d'implémentation technique de sécurité de développement et de sécurité d'application (STIG) du DISA (Defense Information Systems Agency) ainsi que vers des documents d'aide.

Pour plus d'informations sur le guide d'implémentation technique de sécurité (STIG) de développement et de sécurité d'application du DISA (Defense Information Systems Agency), voir http://iase.disa.mil/.

Rapport Open Web Application Security Project (OWASP) Top 10 2013

Cette rubrique fournit des liens vers le site Web Open Web Application Security Project (OWASP) et des documents d'aide.

Pour plus d'informations sur OWASP, voir https://www.owasp.org/index.php/Main_Page. Des liens vers divers documents et risques de sécurité OWASP sont disponibles sur le site https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project.

Rapport Open Web Application Security Project (OWASP) Mobile Top 10

Cette rubrique fournit des liens vers le site Web Open Web Application Security Project (OWASP) et des documents d'aide.

Pour en savoir plus sur le projet de sécurité mobile OWASP, voir https://www.owasp.org/index.php/OWASP_Mobile_Security_Project.

Rapport PCI DSS (Payment Card Industry Data Security Standard) version 3.2

Ce rapport fournit les données pertinentes nécessaires pour garantir la conformité à la norme PCI DSS (Payment Card Industry Data Security Standard).

Pour plus d'informations, voir https://www.pcisecuritystandards.org/security_standards/index.php.

Rapport Profil de sécurité logicielle

Le rapport Profil de sécurité logicielle présente une analyse exhaustive des caractéristiques de votre application ayant un impact direct sur sa sécurité. Il fournit un audit détaillé des fonctions de sécurité cruciales du logiciel pour un projet spécifique. Ce rapport vous aide à vérifier l'implémentation d'exigences telles que le chiffrement, le contrôle d'accès, la journalisation et le traitement des erreurs avant la certification du logiciel pour son déploiement.

Ce rapport composite identifie les zones de risque potentiel et présente des recommandations en vue de les minimiser. Il facilite l'évaluation de la sécurité globale de l'application, laquelle est utile pour l'examen de la conformité, des règles et de l'architecture. Les constatations se basent sur une analyse statique approfondie du code source à l'aide d'une base de données de failles, de vulnérabilités, de normes sectorielles spécifiques et de pratiques générales optimales.

Le rapport Profil de sécurité logicielle présente les informations suivantes :

- Carte de rapport : Contient des liens vers les détails du rapport et des indicateurs de gravité récapitulant la section.
- Présentation : Récapitule l'objectif du rapport et décrit la configuration de l'application.
- Métriques : Identifient le nombre total de packages, de classes, de méthodes et de lignes de code dans tous les packages du projet.
- Constatations détaillées par catégorie : Rend compte de chaque catégorie de vulnérabilités détectée avec le nom de la catégorie et une icône indiquant le niveau de gravité de la vulnérabilité.

Chapitre 9. Création de rapports personnalisés

Vous pouvez créer depuis l'éditeur de rapport des modèles qui vous serviront à générer des rapports personnalisés.

Un rapport de constatations AppScan Source ou un rapport AppScan Source peut ne pas fournir les données exactes dont vous avez besoin. Il se peut que votre rapport doive comporter plus ou moins d'informations. L'éditeur de rapport AppScan Source for Analysis vous permet de créer des rapports personnalisés.

Généralement, vous créez un rapport personnalisé lorsque vous devez :

- Générer un rapport mappé à et concernant une règle de sécurité unique. Vous créez alors un rapport personnalisé, puis l'appliquez à une évaluation spécifique.
- Définir et générer un rapport mettant en évidence des constatations et caractéristiques uniques.
- Modifier un rapport existant ou lui ajouter des éléments.

Lorsque vous enregistrez le canevas de rapport dans `<data_dirr>\reports` (où `<rép_données>` est l'emplacement de vos données de programme AppScan Source, comme décrit dans «Installation et emplacements des fichiers de données utilisateur», à la page 292), le rapport est disponible pour les évaluations de n'importe quelle application. Si vous le sauvegardez sous le répertoire d'une application spécifique, ce rapport est disponible pour les examens de l'application concernée et de tous ses projets.

Avant de commencer à créer ou à éditer un rapport AppScan Source, familiarisez-vous avec les types de rapport et les éléments qui composent chaque rapport. Lorsque vous créez un rapport personnalisé, vous pouvez mapper les éléments du rapport dans l'ordre de votre choix. Les éléments du rapport incluent des informations sur les constatations, des fragments de code, des traces, des contenus concernant la résolution, ainsi que du texte et des éléments graphiques.

Editeur de rapport

L'éditeur de rapport permet de modifier des rapports ou des modèles personnalisés ou de créer un nouveau rapport. Les rapports personnalisés incluent des éléments disponibles dans un rapport sur les constatations, comme les informations sur les constatations, les fragments de code, la trace AppScan Source et le contenu de la résolution, ainsi qu'une matrice de vulnérabilités. Avant de commencer à concevoir de nouveaux rapports, il est recommandé de vous familiariser avec le processus de création de rapports en modifiant un modèle de rapport existant dans l'éditeur de rapport.

L'éditeur de rapport se compose des onglets Agencement du rapport, Catégories et Aperçu.

- **Agencement du rapport** : permet de concevoir l'apparence du rapport. Dans cet agencement, vous pouvez ajouter, retirer et réorganiser les éléments du rapport AppScan Source.
- **Catégories** : permet de créer et de modifier des catégories. Une *catégorie* est un groupe de constatations. La catégorie indique les constatations à inclure dans le rapport, comment les grouper et l'ordre de ce groupement.

- **Aperçu** : permet de visualiser en cours d'édition le rapport pour l'évaluation actuelle.

Les trois onglets comportent des zones communes :

- **Fichier** : chemin du fichier de groupement sauvegardé (en lecture seule). Rien n'apparaît dans cette zone tant que le fichier n'est pas sauvegardé. Une fois sauvegardé, le fichier de groupement est un fichier XML qui définit le rapport.
- **Nom** : Nom du rapport défini par l'utilisateur.

Les boutons de la barre d'outils destinées à la sauvegarde, l'ouverture, le création, la copie et la génération de rapports personnalisés incluent :

- **Créer un nouveau rapport** : crée un rapport personnalisé
- **Nouveau rapport à partir d'un rapport existant** : crée un rapport personnalisé à partir d'un modèle de rapport existant
- **Ouvrir un rapport sauvegardé** : ouvre un fichier de groupement pour son édition
- **Sauvegarder** : sauvegarde le rapport en cours dans le fichier spécifié
- **Sauvegarder sous** : sauvegarde le rapport en cours dans un nouveau fichier
- **Générer une instance de ce rapport** : crée une copie du rapport pour l'évaluation actuellement ouverte

Conseil : Pour afficher des exemples de rapports existants, cliquez sur **Nouveau rapport à partir d'un rapport existant** et choisissez l'un des modèles de rapport AppScan Source. Vous aurez un aperçu de la manière dont les rapports sont conçus en explorant les onglets Agencement du rapport et Catégories.

Onglet Agencement du rapport

L'onglet Agencement du rapport comporte les sections Palette et Présentation et des sections qui permettent de spécifier un en-tête ou un pied de page qui apparaît sur chaque page.

En-tête et pied de page

La zone **En-tête de la page** permet de spécifier le texte qui apparaît en haut de la chaque page de rapport, tandis que la zone **Pied de page** permet de spécifier le texte qui apparaît au bas de chaque page.

Palette

La palette affiche une liste des éléments constitutifs des rapports AppScan Source standard. Certains éléments affichent uniquement des informations pour des catégories qui ont été définies dans l'onglet Catégories (voir tableau 17, à la page 195).

Tableau 16. Palette d'agencement du rapport - éléments qui ne dépendent pas des catégories

Elément de rapport	Description
En-tête	Ajoute un bloc de texte en gras à l'agencement du rapport.
Image d'en-tête	Affiche une image aux dimensions spécifiées en pixels.

Tableau 16. Palette d'agencement du rapport - éléments qui ne dépendent pas des catégories (suite)

Elément de rapport	Description
En-tête AppScan Source	En-tête de rapport contenant la marque AppScan Source.
Titre et date	Titre du rapport qui inclut le nom de l'élément ayant été examiné, ainsi que la date de l'examen et la date de génération du rapport.
Bloc de texte	Texte quelconque défini par l'utilisateur. Un en-tête peut également être ajouté pour le bloc de texte dans la zone **Libellé**.
Matrice de vulnérabilités	Matrice de vulnérabilités de l'évaluation (affiche le même graphique que celui qui apparaît dans la vue Matrice de vulnérabilité).
Métriques	Identifie le nombre total de packages, de classes, de méthodes et de lignes de code dans tous les packages du projet.
Historique des examens	Métriques pour l'examen en cours et métriques historiques des examens de la même cible.

Tableau 17. Palette d'agencement du rapport - éléments qui dépendent des catégories

Elément de rapport	Description
Carte de rapport	Décomposition succincte des niveaux de vulnérabilité de chaque catégorie définie dans l'onglet Catégories. Contient des liens vers les détails du rapport et des indicateurs de gravité récapitulant la section.
Décomposition des vulnérabilités	Tableau décomposant les vulnérabilités dans toutes les catégories définies dans l'onglet Catégories, par gravité et classification.
Carte de rapport partielle	Décomposition des niveaux de vulnérabilité des catégories spécifiées par l'utilisateur comme indiqué dans l'onglet Catégories.
catégories	Répertorie toutes les données de constatations des catégories spécifiées dans l'onglet Catégories.
Catégorie	Répertorie toutes les constatations dans une ou plusieurs catégories qui ont été définies dans l'onglet Catégories.

Présentation

Lorsque vous ajoutez des éléments à partir de la palette, ceux-ci apparaissent dans l'agencement. Utilisez la barre d'outils de section pour supprimer, modifier ou déplacer des éléments dans l'agencement.

Onglet Catégories

Dans l'onglet Catégories, vous pouvez ajouter des catégories qui contiennent les constatations basées sur les groupements, les propriétés ou les constatations

sélectionnées choisis. Les catégories peuvent ensuite être utilisées lors de l'ajout de certains éléments à l'agencement. Par exemple, lorsque vous ajoutez une décomposition de vulnérabilité, un tableau décomposant les vulnérabilités dans toutes les catégories (par gravité et classification) est ajouté à l'agencement. Cet onglet est constitué d'un volet contenant une arborescence des catégories et d'un volet permettant l'édition des attributs de la catégorie sélectionnée. Chaque catégorie contient les constatations de l'évaluation qui répondent aux diverses exigences que vous avez définies.

Les catégories disponibles sont les suivantes :

- Groupement : cette catégorie contient une liste de noms de groupements. Toutes les constatations d'un groupement dont le nom figure dans la liste apparaissent dans cette catégorie. Bien que vous sélectionniez des groupements depuis l'évaluation en cours, vous pouvez appliquer la catégorie du groupement à n'importe quelle évaluation puisque les groupements sont appariés par nom.
- Constatations individuelles : sélectionnez des constatations spécifiques à ajouter à la catégorie. Seul un instantané de la constatation est ajouté au rapport. Si vous modifiez la constatation après son ajout au rapport, celui-ci ne reflète pas les modifications.
- Propriétés de types de vulnérabilité, de mécanismes et de technologies : sélectionnez des propriétés et des ensembles de propriétés requis à partir des API dans la Base de connaissances de sécurité AppScan Source Security. Si une constatation contient au moins une des **Propriétés** et toutes les **Propriétés requises**, elle est incluse dans le rapport.

Ce tableau identifie les volets de catégorie et les éléments composant le volet.

Tableau 18. Attributs de l'onglet Catégories

Attribut	Description	Procédure d'édition
Libellé	Nom court de la catégorie, comme Dépassement de mémoire tampon. Le libellé identifie la catégorie dans la liste arborescente des catégories et il est utilisé comme en-tête dans le rapport personnalisé.	Entrez un libellé sur une seule ligne de la zone de texte.
Récapitulatif	Ossature d'une phrase indiquant combien de constatations figurent dans cette catégorie. Leur compte effectif remplace `%FindingCount%` lors de la génération du rapport.	Entrez une brève description de la catégorie et cliquez sur **Ajouter un comptage** afin de placer la variable `%FindingCount%` à l'emplacement du curseur dans la phrase.
Texte	Brève description de la catégorie.	Entrez un texte décrivant la catégorie.
Propriétés (catégories Propriété uniquement)	Les constatations comportant au moins l'une de ces propriétés seront incluses dans cette catégorie. Si une constatation ne comporte pas toutes les propriétés requises listées, cette constatation n'est pas incluse dans cette catégorie.	Dans la barre d'outils, cliquez sur **Ajouter** et sélectionnez une propriété dans la boîte de dialogue Ajout de propriétés. Cliquez sur **Supprimer** pour supprimer les éléments sélectionnés de la liste.

Tableau 18. Attributs de l'onglet Catégories (suite)

Attribut	Description	Procédure d'édition
Propriétés requises (catégories Propriété uniquement)	Les constatations contenant toutes les propriétés requises et au moins l'une des propriétés apparaissent dans le rapport sous cette catégorie.	Dans la barre d'outils, cliquez sur **Ajouter** et sélectionnez une propriété dans la boîte de dialogue Ajout de propriétés. Cliquez sur **Supprimer** pour supprimer les éléments sélectionnés de la liste.
Groupements (catégories Groupement uniquement)	Spécifie le nom des groupements à inclure dans cette catégorie.	Cliquez sur **Ajouter un groupement** dans la section Groupements et sélectionnez les groupements dans la liste.
Constatations (catégories Constatations uniquement)	Spécifie les constatations à inclure dans cette catégorie.	Sélectionnez les constatations dans un tableau de constatations et cliquez ensuite sur **Ajouter des constatations** dans la barre d'outils du tableau pour ajouter les constatations sélectionnées. Si plusieurs vues contiennent les constatations sélectionnées, vous êtes invité à sélectionner celle qui contient celles que vous voulez ajouter. Vous pouvez également faire glisser les constatations d'un tableau des constatations vers le tableau dans la vue Editeur de rapport ou directement vers une catégorie de constatations existantes dans l'arborescence de catégories.

Onglet Aperçu

Vous pouvez afficher un aperçu des rapports AppScan Source for Analysis lorsque vous éditez vos modèles. Depuis le panneau Aperçu, cliquez sur **Aperçu** pour afficher le rapport sur l'évaluation ouverte.

Génération de rapports personnalisés

Les procédures décrites dans cette section indiquent comment concevoir et générer un rapport à partir d'un rapport personnalisé existant. Vous pouvez également créer un nouveau rapport. Pour modifier un rapport existant, ouvrez ce rapport et suivez les procédures de conception, de modification et d'aperçu.

Conception d'un rapport depuis un rapport personnalisé existant

Procédure

1. Depuis la vue Editeur de rapport, cliquez sur **Nouveau rapport à partir d'un rapport existant** sur la barre d'outils.
2. Sélectionnez un modèle de rapport dans la liste des rapports existants. Consultez l'aperçu du modèle de rapport dans le volet Présentation.
3. Modifiez le nom du rapport, ses en-têtes et ses pieds de page, ou les éléments du modèle :
   a. Ajouter un **En-tête de page** ou un **Pied de page**. L'en-tête et le pied de page apparaissent sur chaque page.
   b. Ajoutez des éléments supplémentaires au rapport. Sélectionnez les éléments voulus dans la **Palette** et cliquez sur **Insérer** (chaque élément doit être inséré séparément).
   c. Supprimez des éléments du rapport. Sélectionnez les éléments à supprimer du modèle et cliquez sur le bouton de barre d'outils **Supprimer l'élément de rapport sélectionné**.
4. Réorganisez les éléments du rapport. Sélectionnez un élément dans l'aperçu et cliquez sur **Déplacer l'élément de rapport sélectionné vers le haut** ou sur **Déplace l'élément de rapport sélectionné vers le bas** dans la barre d'outils pour faire monter ou descendre l'élément du rapport.
5. Cliquez deux fois sur un élément dans le volet Présentation pour l'éditer ou sélectionnez cet élément et cliquez sur **Editer l'élément de rapport sélectionné** sur la barre d'outils.

   Dans la boîte de dialogue qui s'affiche, apportez les modifications voulues. Pour éditer, par exemple, un bloc de texte, modifiez-le dans la boîte de dialogue Edition de bloc de texte en changeant son libellé et sa description.

   Remarque : Certains éléments ne peuvent pas être modifiés.

Inclusion de catégories dans le rapport

Après avoir défini son agencement, déterminez les catégories à inclure dans le rapport.

Procédure

1. Dans le volet Catégories, cliquez sur **Créer une nouvelle catégorie de propriété**, **Créer une nouvelle catégorie de groupement** ou **Créer une nouvelle catégorie de constatations**.
2. Nommez la catégorie en entrant un libellé pour celle-ci, un bref récapitulatif de la catégorie pouvant contenir un comptage, et un texte.

   Vous pouvez promouvoir ou rétrograder une catégorie, ou une sous-catégorie, à l'aide des boutons fléchés de la barre d'outils.
3. Ajoutez les groupements, les constatations ou les propriétés à la catégorie.

Ajout de groupements à une catégorie

Procédure

1. Ouvrez une évaluation contenant des groupements. Si l'évaluation ne contient pas déjà un groupement, vous ne pouvez pas ajouter de groupement au rapport.
2. Dans le volet Groupements, cliquez sur **Ajouter un groupement** et indiquez le(s) groupement(s) à inclure dans la catégorie.

Ajout de constatations à une catégorie

Procédure

1. Ouvrez la vue Constatations qui contient les constatations que vous souhaitez ajouter. Sélectionnez les constatations appropriées et faites-les glisser dans la table des constatations ou sur le noeud de l'arborescence des catégories dans l'éditeur de rapport.
2. Vous pouvez également cliquer sur **Ajouter des constatations** dans la barre d'outils au-dessus de la table des constatations afin d'ajouter des constatations sélectionnées dans d'autres vues. Si vous avez sélectionné des constatations dans plusieurs vues, vous devez sélectionner la vue contenant les constatations ajoutées à la catégorie.
3. Sélectionnez les constatations depuis une vue quelconque comportant une table des constatations.

Ajout de propriétés à une catégorie

Procédure

1. Cliquez sur **Ajouter une propriété** (les propriétés incluent Vulnérabilités, Mécanismes et Technologies). Lorsque vous sélectionnez une propriété, sa description dans la Base de connaissances apparaît (si elle est disponible).
2. Sélectionnez au minimum une propriété, ainsi que les propriétés requises. Une constatation doit comporter toutes les propriétés figurant dans la liste **Propriétés requises** afin d'être incluse dans la catégorie.

   Pour créer une sous-catégorie, sélectionnez une catégorie et cliquez sur la flèche gauche ou droite de la barre d'outils.

Aperçu du rapport

Lorsque vous concevez un rapport, vous pouvez le prévisualiser avant de générer le rapport définitif. Depuis le panneau Aperçu, cliquez sur **Aperçu** pour afficher le rapport sur l'évaluation actuellement ouverte.

Sauvegarde du modèle de rapport

Depuis la barre d'outils de l'éditeur de rapport, vous pouvez cliquer sur **Sauvegarder** afin de conserver le modèle de rapport actuel ou sur **Sauvegarder sous** afin de l'enregistrer dans un nouveau fichier.

Si vous sauvegardez le modèle de rapport dans le même répertoire qu'un fichier d'application (`.paf` ou `.gaf`), il devient disponible dans la liste des options dans l'assistant Rapport personnalisé et dans la vue Editeur de rapport pour son utilisation dans des examens ultérieurs de cette application. Si vous l'enregistrez dans le répertoire `<data_dir>\reports` (où `<rép_données>` est l'emplacement de vos données de programme AppScan Source, comme décrit dans «Installation et

emplacements des fichiers de données utilisateur», à la page 292), il est disponible pour les examens de toutes les applications.

Chapitre 10. Personnalisation de la base de données des vulnérabilités et des règles de schémas

Cette section explique comment personnaliser la base de données et intégrer des vulnérabilités personnalisées et d'autres routines dans des examens.

Le processus d'examen comporte plusieurs phases :

- Un examen spécifique au langage est exécuté à l'aide de la base de données des vulnérabilités (ou de Base de connaissances de sécurité AppScan Source Security).
- Une trace est lancée à l'aide de la base de données des vulnérabilités.
- Un examen basé sur des schémas est lancé à l'aide des règles de schémas de la bibliothèque de règles de schémas globales.

Vous pouvez utiliser des règles personnalisées afin d'adapter la Base de connaissances de sécurité AppScan Source Security à vos normes de sécurité spécifiques et de les appliquer systématiquement dans votre entreprise. Vous pouvez également personnaliser ces règles.

Extension de la Base de connaissances de sécurité AppScan Source Security

Cette section explique comment personnaliser la base de données et intégrer des vulnérabilités personnalisées et d'autres routines dans des examens. Les règles personnalisées adaptent la Base de connaissances de sécurité AppScan Source Security (ou la base de données des vulnérabilités) à vos normes de sécurité spécifiques et appliquent des normes de manière systématique dans votre entreprise.

Il devient fréquemment important de spécifier vos propres routines de validation et de codage ou de définir certaines API en tant que vulnérabilités, collecteurs et sources, propagateurs de tâches ou éléments informatifs. La création de ces règles permet de personnaliser et d'étendre la base de données de vulnérabilités de AppScan Source, laquelle est partie intégrante de la Base de connaissances de sécurité AppScan Source Security. Une fois que vous avez ajouté une règle personnalisée à la base de données, celle-ci est identifiée par AppScan Source for Analysis lors d'un examen. Les appels à l'interface API personnalisée sont indiqués comme des constatations de sécurité ou des constatations de couverture d'examen, puis les constatations sont signalées.

Un analyste pourrait, par exemple, ajouter une API nommée `readBuffer( )`, laquelle est du type `BufferOverflow`. Les examens ultérieurs se réfèrent alors à cette nouvelle API lorsque AppScan Source for Analysis détecte une vulnérabilité correspondant à sa spécification. Pour plus d'informations sur les types de vulnérabilité, voir la Base de connaissances de sécurité AppScan Source Security (sélectionnez **Aide** > **Base de connaissances de sécurité** dans le menu du plan de travail principal).

Lorsque vous ajoutez des routines de validation et de codage personnalisées, AppScan Source for Analysis ne traite plus les données transitant dans ces routines comme des vulnérabilités. En ajoutant une routine personnalisée à la Base de

connaissances, AppScan Source for Analysis détermine si les données émanent d'une source entachée sans validation ou codage avant leur sortie.

Remarque : La Base de connaissances de sécurité AppScan Source Security ne propose pas d'aide en ligne pour les enregistrements personnalisés mais affiche une aide pour le type de vulnérabilité.

Important : Vous devez disposer des droits de `gestion de la Base de connaissances` pour apporter des modifications à la Base de connaissances de sécurité AppScan Source Security.

Création de règles personnalisées

Vous pouvez ouvrir depuis la vue Règles personnalisées l'assistant Règles personnalisées pour vous guider dans la création d'enregistrements de base de données personnalisés. Après avoir créé des règles personnalisées, celles-ci sont affichées dans la vue Règles personnalisées. Le tableau affiche leur signature, leur langage et leur objet.

Les routines de validation et de codage spécifiques au projet ne sont affichées dans la vue Règles personnalisées que si le projet auquel s'appliquent les règles existe dans une application figurant sous **Toutes les applications** dans la vue Explorateur.

- **Signature** : la signature est le nom qualifié complet de la fonction. Par exemple, la signature Java inclut des arguments et des types de retour, tels que `com.test.vulnerable.VulnClass.vulnerable(java.lang.string;int):int.`
- **Langage** : C/C++, Java, Visual Basic, Classic ASP, ou .NET
- **Objet** : Type(s) d'enregistrement personnalisé de la méthode concernée, tel que routine `Validation.EncodingRequired`, collecteur ou source.

Conseil : En affinant votre évaluation d'un codebase en l'examinant par itérations et en ajoutant des règles personnalisées, puis en l'examinant à nouveau sans modifier le code source, vous pouvez réduire considérablement la durée de l'examen en définissant les propriétés du projet de sorte à utiliser un cache d'analyse des vulnérabilités. Pour ce faire, cochez la case **Activer le cache d'analyse de vulnérabilités** dans les propriétés du projet. Pour déterminer comment définir les propriétés de projet, reportez-vous aux instructions d'utilisation de l'«Onglet Présentation du projet sélectionné», à la page 221.

Utilisation de l'assistant Règles personnalisées

L'assistant Règles personnalisées vous aide à ajouter des méthodes à la Base de connaissances de sécurité AppScan Source Security. La portée de la plupart des règles de méthode est globale (s'applique à tous les projets). Les constatations sans trace, les sources, les collecteurs et les propagateurs de tache personnalisés sont toujours globaux. Les routines de validation/codage personnalisées ne sont pas globales.

Remarque : L'assistant Règles personnalisées ne valide pas vos sélections. Vous pouvez définir, par exemple, une règle personnalisée qui identifie une méthode en tant que propagateur de tâche et un collecteur, ce qui ne constitue pas un scénario valide.

L'assistant Règles personnalisées vous guide tout au long du processus de définition et d'ajout des éléments suivants à la Base de connaissances :

- Collecteurs et sources

- Propagateurs de tâche
- Interfaces de programme d'application (API) non vulnérables aux taches
- Vulnérabilités
- API générant des constatations sans trace
- API n'étant pas des routines de codage/validation
- Rappels entachés
- Constatations à titre informatif

Source (de tache)

Méthode qui fournit des entrées à un programme pouvant être incorrectement formé ou malveillant.

Collecteur (vulnérable aux taches)

API qui extrait les données du programme (ou de la partie visible du programme) pour les envoyer vers un fichier, le réseau, une base de données, une autre bibliothèque ou une unité pouvant être vulnérable à une entrée malveillante.

Propagateur de tâche

La marquage d'une méthode en tant que propagateur de tâche implique que si des arguments de l'API sont dérivés de données d'entrée utilisateur non validées (données entachées), après l'appel, les données non constantes référencées par les autres arguments, tout comme la valeur renvoyée, seront elles-mêmes potentiellement entachées. Ces données doivent être validées ou codées avant leur envoi à un collecteur. Cette situation se produit généralement lorsque les données de l'argument entaché sont copiées ou annexées aux autres arguments, ou renvoyées.

Non vulnérable aux tâches

Le marquage d'une API comme non vulnérable aux tâches (comme n'étant pas un propagateur de tâche) implique que l'appel de l'API avec un argument dérivé de données d'entrée utilisateur non validées (données entachées) n'entraîne pas un comportement non sécurisé ou malveillant de l'API.

Si des données entachées parviennent à un appel et que celui-ci est marqué comme non vulnérable aux tâches, AppScan Source ignore cet appel en ce qui concerne les traces. trace AppScan Source ne signale pas que la trace est perdue et ne traite pas les données propagées comme des données entachées.

Remarque : Si des données entachées parviennent à une méthode qui n'est pas une routine de validation ou de codage, un collecteur, un propagateur de tâche ou qui n'est pas vulnérable aux tâches, cette méthode est signalée comme une trace perdue. Les arguments autres que des constantes et les valeurs renvoyées peuvent être ou ne pas être entachés. Le diagramme d'appel de trace AppScan Source affiche une trace perdue.

Constatation sans trace

Méthode ou API qui apparaît toujours comme une constatation mais qui ne génère pas une trace.

N'est pas une routine de validation/codage

Le marquage d'une API comme n'étant **pas une routine de validation/codage** indique que cette API ne valide aucune donnée.

Rappel entaché

Un rappel est une routine de votre code généralement appelée par un *autre* code (par exemple, depuis une infrastructure de plus bas niveau). Le rappel est transmis à l'autre code sous forme d'argument et peut être appelé ultérieurement avec des arguments éventuellement entachés. Si vous soupçonnez qu'un rappel peut contenir des données entachées transmises à ses arguments, vous pouvez le marquer en tant que rappel entaché. Ceci rend visible le flux de données entachées dans la routine.

Une routine marquée en tant que rappel entaché sera analysée comme si elle était placée à la racine du diagramme d'appel (en d'autres termes, comme si elle était appelée par un appelant externe) et tous ses arguments d'entrée seront considérés être entachés. Par conséquent, AppScan Source renverra des constatations avec des traces commençant aux arguments du rappel entaché.

Si la même routine est appelée dans d'autres contextes par votre code applicatif, elle sera traitée sans prise en compte spéciale des tâches éventuelles. Dans ces contextes, l'analyse ordinaire sera appliquée.

Message d'information

Les lignes de code identifiées comme constatations relatives à des informations peuvent ne pas être vulnérables mais doivent être incluses dans un audit de sécurité.

Ajout d'une règle

Cette rubrique de tâche décrit la procédure d'ajout d'une règle personnalisée à l'aide de l'Assistant Règles personnalisées.

Pourquoi et quand exécuter cette tâche

Remarque : L'ajout ou la suppression de constatations de sécurité ou de couverture d'examen et la modification de leur gravité affecte la densité V du projet.

Procédure

1. Ouvrez l'assistant depuis la vue Règles personnalisées en cliquant sur le bouton **Lancer l'assistant Règles personnalisées**.
2. Sur la page **Sélectionnez l'application, le projet et les fichiers**, sélectionnez l'**application** et le **projet** auxquels la règle s'appliquera. Assurez-vous que l'application et le projet concerné se rapportent au code source de l'élément que vous souhaitez ajouter à la Base de connaissances. Sélectionnez la **configuration** si celle-ci est disponible.
3. Dans la section **Portée**, définissez la portée de l'examen. Les options d'examen sont les suivantes et varient en fonction du langage que vous examinez :

Tableau 19. Options de fichiers de projet par langage

Langage	Options de fichiers de projet
Java	• **Examiner le projet complet pour signatures de méthodes** • **Sélectionner un ou plusieurs fichiers dans le projet** • **Sélectionner un ou plusieurs fichiers externes au projet** Un projet Java inclut des fichiers `.jar` ou `.class` ou une hiérarchie de répertoires de fichiers de classe.

- Le mode d'examen par défaut est : **Examiner le projet complet pour signatures de méthodes**. Ce mode examine la totalité du projet et renvoie toutes les signatures disponibles. Ce mode d'examen peut prendre du temps.
- L'option **Sélectionnez un ou plusieurs fichiers dans le projet** permet d'isoler certains fichiers de projet contenant des méthodes qui peuvent nécessiter des règles personnalisées.
- L'option **Sélectionnez un ou plusieurs fichiers externes au projet** identifie des fichiers externes à ce projet qui doivent être inclus dans l'examen.

4. Dans la section **Mise en cache**, cochez la case permettant de relire un projet ou un code modifié. Le cache d'analyse de vulnérabilité sera lui aussi vidé (si le projet en cours est configuré pour mise en cache de l'analyse de vulnérabilité, ce cache sera recréé à l'analyse suivante).
5. **Analyse de chaîne** : L'analyse de chaîne surveille les manipulations de chaînes dans les projets Java. Elle assure la détection automatique des routines d'assainissement et de validation. Grâce à cette détection, il est possible de réduire les résultats faussement positifs ou faussement négatifs. Pour activer l'analyse de chaîne, cochez la case **Activer l'analyse de chaîne pour trouver les fonctions permettant de valider et rendre inoffensif**. La case **Appliquer les règles importées à la portée globale** détermine si les routines d'assainissement ou de validation découvertes doivent être appliquées à l'échelle du projet ou au niveau global (à tous les projets).

   Remarque : L'analyse de chaîne peut ralentir l'examen du code. Il est donc recommandé de ne l'appliquer qu'après un changement de code, puis de la désactiver pour les examens suivants. En outre, les routines découvertes doivent être considérées comme des *suggestions* et examinées par les auditeurs. Ces routines peuvent être visualisées dans la vue Règles personnalisées.
6. Cliquez sur **Suivant** pour passer à la page suivante de l'assistant.
7. Sur la page **Sélectionner des méthodes** :
   a. Sélectionnez la ou les méthode(s) à ajouter à la Base de connaissances. La méthode est le nom de l'API vulnérable.

      La liste de méthodes peut être filtrée des deux façons suivantes :

      - Filtrage automatique : tapez le texte du filtre dans la zone **Filtrer**. A mesure que vous tapez le texte, le filtre correspondant est automatiquement appliqué à la liste de méthodes. Il s'agit du mode de filtrage par défaut.
      - Filtrage manuel : tapez le texte du filtre dans la zone **Filtrer**, puis cliquez sur le bouton **Filtrer** (ou appuyez sur Entrée) pour appliquer le

filtre à la liste. Vous souhaiterez peut-être utiliser le filtrage manuel car un nombre élevé de méthodes provoque des délais dans le cas du filtrage automatique.

Dans le deux cas, l'astérisque et le point d'interrogation peuvent être utilisés comme caractères génériques. Un astérisque correspond à un groupe de zéro ou plusieurs caractères et le point d'interrogation correspond à un caractère.

Pour modifier le mode de filtrage, utilisez le bouton **Filtrer** comme option à bascule en cliquant deux fois dessus ou en utilisant le clavier pour y accéder et en appuyant sur la barre d'espacement. Lorsque le filtrage manuel est activé, le bouton **Filtrer** apparaît comme non utilisé et l'infobulle correspondante indique **Apply filter (double-click or press space to filter automatically)**. Lorsque le filtrage automatique est utilisé, le bouton apparaît comme utilisé et l'infobulle correspondante indique **Filter manually**.

Pour optimiser l'affichage de la liste de méthodes, des actions de développement et de réduction sont disponibles. Pour développer ou réduire l'ensemble de l'arborescence, cliquez avec le bouton droit de la souris et sélectionnez **Développer tout** ou **Réduire tout**. Pour développer un package ou une classe et toutes les sous-entrées correspondantes, cliquez avec le bouton droit de la souris sur le package ou la classe, puis sélectionnez **Expand Children**.

Pour sélectionner plusieurs méthodes, utilisez les touches du clavier de commande ou maj.

Cochez la case **Afficher les signatures complètes** pour afficher la signature entièrement qualifiée des méthodes dans l'arborescence. Par exemple, la signature Java entièrement qualifiée inclut le package, la classe, la méthode, les types d'argument et les types de retour, comme `com.test.vulnerable.VulnClass.vulnerable(java.lang.string;int):int`.

b. Déterminez si l'examen doit marquer la méthode comme étant l'une de celles-ci :
   - «Source (de tache)», à la page 203
   - «Collecteur (vulnérable aux taches)», à la page 203
   - «Propagateur de tâche», à la page 203
   - «Non vulnérable aux tâches», à la page 203
   - «Constatation sans trace», à la page 203
   - «N'est pas une routine de validation/codage», à la page 204
   - «Rappel entaché», à la page 204
   - «Message d'information», à la page 204

8. Si vous ajoutez des méthodes en tant que «Non vulnérable aux tâches», à la page 203, «N'est pas une routine de validation/codage», à la page 204, «Propagateur de tâche», à la page 203 ou «Rappel entaché», à la page 204, cliquez sur **Terminer** pour ajouter les enregistrements à la Base de connaissances de sécurité AppScan Source Security.
9. Si vous ajoutez des méthodes en tant que «Source (de tache)», à la page 203 ou «Message d'information», à la page 204, procédez comme suit :
   a. Cliquez sur **Suivant** pour passer à la page **Affecter des attributs de règle**.
   b. Pour chaque méthode que vous avez ajoutée, sélectionnez une ou plusieurs propriétés à affecter à la méthode. La colonne **Type** de la méthode sera mise à jour pour indiquer le type de vulnérabilité des constatations qui seront générées par la règle personnalisée.

Conseil : Pour ajouter les mêmes propriétés à plusieurs méthodes, sélectionnez les méthodes en utilisant les touches du clavier de commande ou maj, puis sélectionnez les propriétés que vous souhaitez affecter aux méthodes.

c. Cliquez sur **Terminer** pour ajouter les enregistrements à la Base de connaissances de sécurité AppScan Source Security.

10. Si vous ajoutez des méthodes en tant que «Collecteur (vulnérable aux taches)» , à la page 203 :
    a. Cliquez sur **Suivant** pour passer à la page **Affecter des attributs de règle**.
    b. Pour chaque méthode que vous avez ajoutée :
       - Sélectionnez le niveau de **Gravité** de l'impact de la vulnérabilité : **Elevée**, **Moyenne** ou **Faible**.
       - Sélectionnez le **Type de vulnérabilité** à appliquer à la méthode.

       Conseil : Pour ajouter les mêmes propriétés à plusieurs méthodes, sélectionnez les méthodes en utilisant les touches du clavier de commande ou maj, puis sélectionnez les propriétés que vous souhaitez affecter aux méthodes.
    c. Cliquez sur **Terminer** pour ajouter les enregistrements à la Base de connaissances de sécurité AppScan Source Security.
11. Si vous ajoutez des méthodes en tant que «Constatation sans trace», à la page 203 :
    a. Cliquez sur **Suivant** pour passer à la page **Affecter des attributs de règle**.
    b. Pour chaque méthode que vous avez ajoutée :
       - Sélectionnez le niveau de **Gravité** de l'impact de la vulnérabilité : **Elevée**, **Moyenne** ou **Faible**.
       - Sélectionnez la **Classification** à affecter à la méthode : **Catégorique**, **Suspecte** ou **Configuration**.
       - Sélectionnez le **Type de vulnérabilité** à appliquer à la méthode.

       Conseil : Pour ajouter les mêmes propriétés à plusieurs méthodes, sélectionnez les méthodes en utilisant les touches du clavier de commande ou maj, puis sélectionnez les propriétés que vous souhaitez affecter aux méthodes.
    c. Cliquez sur **Terminer** pour ajouter les enregistrements à la Base de connaissances de sécurité AppScan Source Security.

Attributs de règle `Likelihood`

Les attributs `Attribute.Likelihood.High` et `Attribute.Likelihood.Low` font partie des règles intégrées et ils peuvent être utilisés lors de la création de règles personnalisées.

Dans AppScan Source, *likelihood* représente la probabilité ou la possibilité qu'une constatation de sécurité puisse être exploitée. AppScan Source prend la définition de la probabilité définie à l'adresse https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology#Step_2:_Factors_for_Estimating_Likelihood et l'affine en déterminant la probabilité en fonction des propriétés de trace. A partir d'un ensemble de propriétés de trace, telles que le nom de l'API source, le type de l'API source, la technologie source ou le mécanisme source, AppScan Source détermine la probabilité qu'une trace soit exploitée dans le futur en utilisant une vulnérabilité spécifique.

La probabilité est liée à l'élément source d'une trace. Une source est une entrée du programme, telle qu'un fichier, une requête de servlet, une saisie depuis la console ou un socket. Dans le cas de la plupart des sources d'entrées, les données renvoyées ne sont pas limitées en termes de contenu et de longueur. Lorsqu'une entrée n'est pas vérifiée, elle est considérée comme une source de tache.

Vous trouverez quelques exemples de probabilité ci-dessous :

- Si l'on prend une trace avec une source HTTP (par exemple, `Request.getQueryString`) et un collecteur XSS (par exemple, `Response.write`), une probabilité élevée est déterminée, augmentant ainsi le niveau de fiabilité de la constatation.
- Si l'on prend une trace avec une source de propriété système (par exemple, `getProperty`) et un collecteur XSS (par exemple, `Response.write`), une probabilité faible est déterminée, diminuant ainsi le niveau de fiabilité de la constatation.

La probabilité permet d'identifier les constatations à priorité élevée qui doivent être traitées ou corrigées immédiatement. Elle est liée aux sources de taches hautement exploitables et peut vous fournir une approche affinée pour la classification des constatations. La probabilité est stockée en tant qu'attribut lié à une source de tache dans la base de données de vulnérabilités d'AppScan Source. Cette fonction est prête à l'emploi.

Nous avons mené des recherches approfondies afin de déterminer le facteur de probabilité des sources. A l'aide de l'assistant Règles personnalisées, vous pouvez ajouter des informations de probabilité aux nouvelles sources de taches que vous ajoutez à votre base de règles. Vous améliorez ainsi la classification des constatations générées à partir d'un examen et, par conséquent, l'efficacité de votre flux de travail global de triage.

Dans l'assistant de règles personnalisées, vous pouvez définir deux valeurs (**High** et **Low**) pour la propriété **Likelihood**. La valeur **High** signifie que la source est très vulnérable aux taches. Autrement dit, la barrière aux taches introduites dans le système est très faible, ce qui permet aux agresseurs informatiques de soumettre facilement des données malveillantes de façon manuelle ou automatique. La valeur **Low** signifie que la barrière à l'entrée de données malveillantes par le biais de cette source est très élevée. Cela peut vouloir dire que pour que la tache soit introduite dans la source, un agresseur informatique doit avoir une connaissance d'initié du système et disposer d'autorisations pour opérer sur le réseau de la victime.

Personnalisation de la trace des entrées/sorties via la fonction de trace AppScan Source

Certaines applications (notamment les applications Web) requièrent une trace des entrées/sorties en vue d'identifier les vulnérabilités de la sécurité associées à une injection SQL, une injection de commande ou à un script intersite. A l'aide de la fonction de trace de AppScan Source, vous pouvez spécifier d'utiliser une routine de validation qui élimine alors le compte rendu de ces vulnérabilités. Toutes les autres sorties sont marquées en tant que vulnérabilités si leurs entrées n'ont pas été validées.

Les routines de validation définies par l'utilisateur sont des routines qui traitent les données en entrée de sorte à pouvoir les transmettre sans danger aux routines de sortie. Si une routine de validation traite les données en entrée avant de les transmettre à une routine de sortie, aucune vulnérabilité liée à l'absence de

validation des entrées ne subsiste. Les développeurs peuvent spécifier leurs propres routines de validation et de codage à utiliser avec la fonction de trace.

Personnalisation à l'aide de règles basées sur des schémas

L'examen AppScan Source basé sur des schémas est une analyse de votre code source basée sur des critères de recherche personnalisés. Cet examen est similaire à celui de la fonction grep (grep recherche une chaîne de caractères donnés ou un schéma dans un ou plusieurs fichiers). Les auditeurs ou les analystes de la sécurité effectuant un triage peuvent utiliser un examen basé sur des schémas afin de rechercher des schémas spécifiques dans les applications indiquées ou dans un projet. Après avoir défini un schéma comme constituant un type de vulnérabilité, un examen de votre code source identifie la présence de ce schéma comme une vulnérabilité. Lorsque AppScan Source détecte une correspondance, l'élément concerné figure dans le tableau des constatations. La bibliothèque de règles AppScan Source prête à l'emploi inclut des règles et des ensembles de règles (collections de règles) prédéfinis.

L'examen basé sur des schémas recherche une *expression régulière*. Une expression régulière, fréquemment appelée schéma, désigne une chaîne qui décrit ou correspond à un ensemble de chaînes, compte tenu de certaines règles de syntaxe. Vous pouvez indiquer une recherche en créant une règle. Une règle est similaire à une règle personnalisée que vous ajoutez à la Base de connaissances de sécurité AppScan Source Security dans la vue Règles personnalisées. Lorsque vous créez une règle, vous devez définir sa gravité, sa classification, le type de vulnérabilité, ainsi que d'autres critères.

La section «Vue Bibliothèque de règles de schémas», à la page 255 vous permet de créer de nouvelles règles de schémas et ensembles de règles, mais aussi de modifier ou de supprimer des règles ou ensembles existants. Vous utilisez ensuite la vue Propriétés pour une application sélectionnée, la vue Propriétés pour un projet sélectionné ou des configurations d'examen pour appliquer les règles de schémas et les ensembles de règles (vous pouvez aussi lancer la boîte de dialogue qui vous permet de créer un nouvelle règle depuis ces vues). Pour plus d'informations sur l'application des règles et des ensembles de règles, voir «Application de règles et d'ensembles de règles de schémas», à la page 215.

Exemples de règles de schéma pouvant être créées :

- Correspondances de schéma de nom de fichier
- Règle unique avec multiples schémas
- Règles d'absence

Remarque : Vous devez disposer des droits **Gérer les schémas** pour pouvoir créer des règles de schéma ou des ensembles de règles - ou encore pour modifier et supprimer des règles et des ensembles de règles personnalisés.

Ensembles de règles de schémas

Un ensemble de règles de schémas représente une collection de règles de schémas. Vous pouvez en créer de nouveaux, ou modifier ou supprimer des ensembles de règles de schémas existants. AppScan Source fournit une série d'ensembles de règles de schémas spécifiques au langage que vous choisissez d'appliquer à vos projets ou applications (par exemple, vous pouvez appliquer l'ensemble de règles de schémas **Java** aux projets **Java/JSP**).

La section «Vue Bibliothèque de règles de schémas», à la page 255 vous permet de créer de nouvelles règles de schémas et ensembles de règles, mais aussi de modifier ou de supprimer des règles ou ensembles existants. Vous utilisez ensuite la vue Propriétés pour une application sélectionnée, la vue Propriétés pour un projet sélectionné ou des configurations d'examen pour appliquer les règles de schémas et les ensembles de règles (vous pouvez aussi lancer la boîte de dialogue qui vous permet de créer un nouvelle règle depuis ces vues). Pour plus d'informations sur l'application des règles et des ensembles de règles, voir «Application de règles et d'ensembles de règles de schémas», à la page 215.

Certains ensembles de règles de schémas livrés avec AppScan Source ne contiennent pas de règles. Vous pouvez ajouter à ces ensembles de règles les règles adaptées à votre organisation. Ces ensembles de règles sont les suivants :

- ColdFusion
- JQuery
- JavaScript côté client
- Visual Basic 6
- MooTools

Conseil : Dans la vue Bibliothèque de règles de schémas, cliquez avec le bouton droit de la souris sur un ensemble de règles et sélectionnez **Propriétés** pour ouvrir une boîte de dialogue affichant des informations sur cet ensemble de règles. La boîte de dialogue Propriétés de l'ensemble de règles fournit des informations comme le nombre de règles dans l'ensemble de règles de schémas et les relations parent/enfant avec d'autre ensembles de règles. Vous pouvez aussi modifier le **Nom d'affichage** et les **Types de projets** de l'ensemble de règles.

Remarque : Vous devez disposer des droits **Gérer les schémas** pour pouvoir créer des règles de schéma ou des ensembles de règles - ou encore pour modifier et supprimer des règles et des ensembles de règles personnalisés.

Création d'une ensemble de règles dans la vue Bibliothèque de règles de schémas

Un ensemble de règles de schémas représente une collection de règles de schémas. Pour savoir comment créer un ensemble de règles, suivez les instructions de cette rubrique.

Avant de commencer

Remarque : Vous devez disposer des droits **Gérer les schémas** pour pouvoir créer des règles de schéma ou des ensembles de règles - ou encore pour modifier et supprimer des règles et des ensembles de règles personnalisés.

Procédure

1. Depuis la vue Bibliothèque de règles de schémas, cliquez sur **Nouvel ensemble de règles**.
2. Dans la boîte de dialogue Nouvel ensemble de règles, entrez un nom pour l'ensemble de règles dans la zone **Nom**.
3. Sélectionnez un ou plusieurs types de projet auxquels s'appliquera l'ensemble de règles.
4. Cliquez sur **OK**.
5. Le nouvel ensemble de règles apparaît dans la liste des ensembles de règles. Vous pouvez alimenter l'ensemble de règles de deux manières :

a. Sélectionnez une ou plusieurs règles dans la section des règles de schémas et faites-les glisser dans l'ensemble de règles.
b. Sélectionnez une ou plusieurs règles dans la section des règles de schémas, puis cliquez avec le bouton droit de la souris sur votre sélection et choisissez l'option de menu **Ajouter à l'ensemble de règles**. Dans la boîte de dialogue Sélection d'un ensemble de règles, sélectionnez l'ensemble de règles d'examen auquel ajouter ces règles.

Modification et suppression d'ensembles de règles

Les ensembles de règles de schémas prêtes à l'emploi que vous avez créées peuvent être modifiées et supprimées depuis la vue Bibliothèque de règles de schémas.

Remarque : Vous devez disposer des droits **Gérer les schémas** pour pouvoir créer des règles de schéma ou des ensembles de règles - ou encore pour modifier et supprimer des règles et des ensembles de règles personnalisés.

Modification d'un ensemble de règles

Vous pouvez apporter les modifications suivantes à un ensemble de règles :

- Vous pouvez ajouter une règle à un ensemble de règles existant en suivant les instructions de la rubrique «Création d'une ensemble de règles dans la vue Bibliothèque de règles de schémas», à la page 210.
- Pour supprimer un ou plusieurs règles d'un ensemble de règles, sélectionnez la ou les règles à supprimer, puis effectuez l'une des actions suivantes :
  - Cliquez sur **Retirer des règles de leur ensemble**.
  - Cliquez avec le bouton droit de la souris et sélectionnez **Retirer des règles de leur ensemble**.
- Vous pouvez ajouter un ensemble de règles à un autre ensemble de règles de deux manières :
  - Sélectionnez un ensemble de règles et faites-le glisser dans un autre.
  - Cliquez avec le bouton droit de la souris sur un ensemble de règles et sélectionnez **Ajouter un ensemble de règles en tant qu'élément enfant**, puis, dans la boîte de dialogue Sélection d'un ensemble de règles, sélectionnez celui à ajouter en tant qu'ensemble de règles parent.
- Vous pouvez modifier le **Nom d'affichage** et les **Types de projet** d'un ensemble de règles comme suit : cliquez avec le bouton droit sur l'ensemble de règles et sélectionnez **Propriétés** pour ouvrir la boîte de dialogue Propriétés du jeu de règles. Dans cette boîte de dialogue, vous pouvez éditer la zone **Nom d'affichage**, ou bien cliquer sur la zone **Types de projet** et sur le bouton **Editer** pour sélectionner un ou plusieurs types de projet.

Suppression d'un ensemble de règles

Pour supprimer un ensemble de règles, sélectionnez celui-ci et exécutez l'une des actions suivantes :

- Cliquez sur **Retirer l'ensemble de règles**.
- Cliquez avec le bouton droit de la souris et sélectionnez **Supprimer**.

Règles de schéma

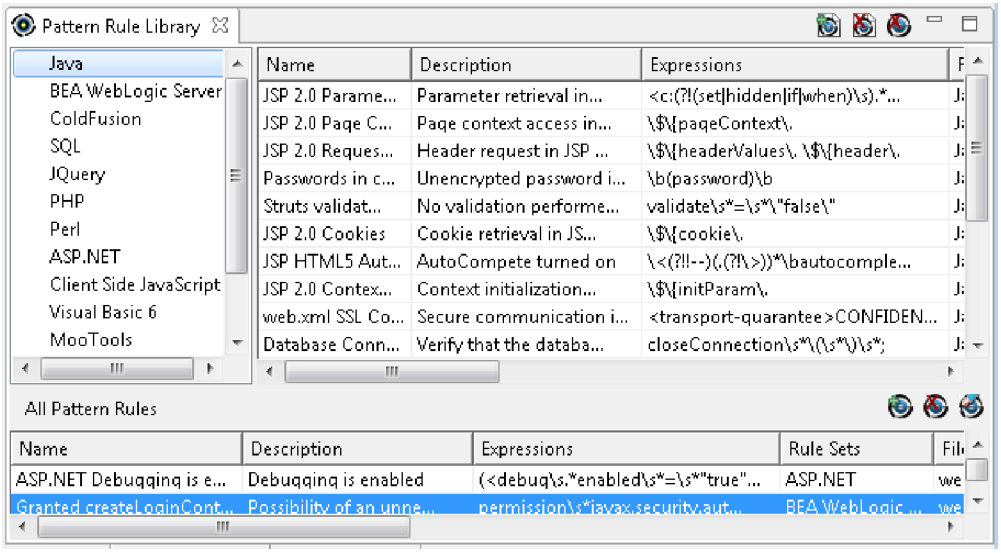
Les règles de texte AppScan Source peuvent être des expressions régulières Extended Global Regular Expressions Print (egrep), Global Regular Expressions

(grep), ou Perl. Ces expressions régulières (expressions comportant des valeurs de chaîne qui utilisent le jeu complet de caractères alphanumériques et de caractères spéciaux) respectent les règles.

Caractère	Description
^	Commence par
$	Finit par
\n, \t ou \r	Littéral retour à la ligne, tabulation, renvoi
[xyz]	N'importe lequel des caractères indiqués
[^abx]	N'importe quel caractère excepté ceux indiqués
[a-fA-F0-9]	N'importe quel caractère hexadécimal
.	N'importe quel caractère
|	L'un ou l'autre
\	Annule la signification d'un caractère spécial \$ \^ \\ \?

Les règles de schéma sont stockées dans une bibliothèque de règles de schémas globales (dans la base de données AppScan Source) et elles peuvent être partagées entre les projets et les applications. Les règles et les ensembles de règles peuvent également être partagés par tous les utilisateurs. Les règles sont ajoutées par voie de référence, celle-ci pouvant être désactivée en supprimant la référence dans l'objet associé sans pour autant supprimer la règle d'examen sous-jacente.

Les règles sont créées depuis la vue Bibliothèque de règles de schémas, l'onglet Propriétés de la vue Explorateur ou une configuration d'examen. Lorsque vous installez AppScan Source, la vue Bibliothèque de règles affiche les règles provenant de AppScan Source. Depuis cette vue, vous pouvez éditer, supprimer ou créer une règle.



Important : Vous pouvez ajouter ou supprimer des critères de recherche, mais chaque règle basée schéma doit comporter au moins un critère de recherche.

Recherche de schémas de texte

Dans un fichier source donné, l'examen basé sur des schémas recherche des schémas de texte dans des fichiers d'après leur extension, permettant à la recherche d'opérer sur des fichiers source, des fichiers de configuration XML et d'autres fichiers texte.

Vous pourriez, par exemple, créer une recherche de schéma pour vous assurer que des adresses électroniques inappropriées ne soient pas codées en dur dans votre application. Dans ce cas, pour vérifier que l'application n'utilise pas d'adresses électroniques de l'entreprise, vous pourriez rechercher un schéma tel que `.*@mycompany.com`.

Exemples

Ce schéma découvre	Schéma
Une adresse électronique	`[A-Za-z]\.[A-Za-z]@[A-Za-z][A-Za-]\.com`
Toutes les instances du schéma, telles que `passWord =`	`[Pp][Aa][Ss][Ss][Ww][Oo][Rr][Dd]\W*=`
Une instance quelconque de l'algorithme de hachage MD5	`getInstance[[:space:]]*\ ([[:space:]]*"MD5`

Création d'une règle de schémas

Il est possible de créer des règles dans la vue Bibliothèque de règles de schémas, la vue Propriétés d'un projet ou d'une application, ou dans une configuration d'examen.

Avant de commencer

Remarque : Vous devez disposer des droits **Gérer les schémas** pour pouvoir créer des règles de schéma ou des ensembles de règles - ou encore pour modifier et supprimer des règles et des ensembles de règles personnalisés.

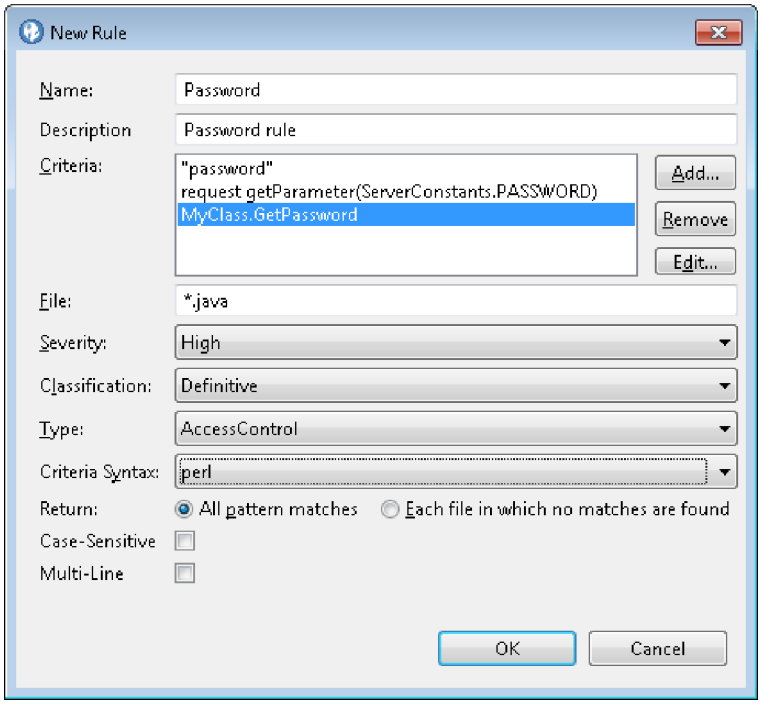
Les règles sont créées dans la boîte de dialogue Nouvelle règle :

- Pour ouvrir cette boîte de dialogue dans la vue Bibliothèque de règles de schémas, cliquez sur **Nouvelle règle**.
- Dans une configuration d'examen, sélectionnez l'onglet Analyse de schéma puis la case à cocher **Analyse de schéma**. Dans la section Règles de schémas de l'onglet, cliquez sur **Ajouter** afin d'ouvrir la boîte de dialogue Ajouter des règles de schéma. Dans cette boîte de dialogue, cliquez sur **Créer une règle** pour ouvrir la boîte de dialogue Nouvelle règle.
- Pour ouvrir cette boîte de dialogue depuis la vue Propriétés d'une application ou d'un projet sélectionné, cliquez sur l'onglet **Règles et ensembles de règles** de la vue Propriétés, cliquez sur **Ajouter** ou cliquez avec le bouton droit de la souris dans la section Règles et sélectionnez **Ajouter**. Cliquez sur **Nouvelle règle** dans la boîte de dialogue Choisir une règle.

Procédure

1. Dans la boîte de dialogue Nouvelle règle, attribuez un **Nom** à la règle.
2. Facultatif : Ajoutez une **Description** pour la règle.
3. Ajoutez les **critères**. Cliquez sur **Ajouter** et entrez une expression régulière pour chaque règle.
4. Identifiez le type de fichier, par exemple, `*.java` ou `*.xml`. Vous pouvez entrer le type de fichier avec ou sans caractères génériques.

5. Facultatif : Sélectionnez la **gravité** :
   - **Elevée**
   - **Moyenne**
   - **Faible**
   - **Info**
6. Facultatif : Sélectionnez la **Classification** :
   - **Définitive**
   - **Suspectée**
   - **Couverture d'examen**
7. Facultatif : Sélectionnez le type de vulnérabilité à rechercher dans l'examen. (Pour plus d'informations sur les types de vulnérabilités, consultez la Base de connaissances de sécurité AppScan Source Security)



8. Facultatif : Sélectionnez la syntaxe des critères :
   - **egrep**
   - **grep**
   - **perl**
9. Facultatif : Indiquez si les résultats renvoyés doivent inclure **Toutes les correspondances de schéma** ou **Chaque fichier sans correspondance**. Lorsqu'aucune correspondance n'est trouvée, le schéma est une règle d'absence.
10. Facultatif : Cochez la case **Sensible à la casse** si la correspondance de schéma doit respecter la casse.
11. Facultatif : Cochez la case **Multiligne** si la règle doit correspondre à un schéma qui s'étend sur plusieurs lignes.
12. Cliquez sur **OK** pour vérifier que les expressions régulières de la règle sont valides. La règle est alors ajoutée à la bibliothèque de règles.

Modification et suppression de règles de schéma

Les règles de schémas que vous avez créées peuvent être modifiées et supprimées depuis la vue Bibliothèque de règles de schémas.

Remarque : Vous devez disposer des droits **Gérer les schémas** pour pouvoir créer des règles de schéma ou des ensembles de règles - ou encore pour modifier et supprimer des règles et des ensembles de règles personnalisés.

Modification d'une règle

Pour modifier une règle, sélectionnez-la et exécutez l'une des actions suivantes :

- Cliquez sur **Editer une règle**.
- Cliquez avec le bouton droit de la souris et sélectionnez **Editer**.

Ceci a pour effet d'ouvrir la boîte de dialogue Editer une règle, laquelle vous permet de modifier tous les paramètres de la règle, excepté son nom.

Suppression d'une règle

Sélectionnez une ou plusieurs règles et exécutez l'une des actions suivantes :

- Cliquez sur **Retirer la règle**.
- Cliquez avec le bouton droit de la souris et sélectionnez **Supprimer**.

Application de règles et d'ensembles de règles de schémas

Les règles et les ensembles de règles sont appliqués au niveau de l'application ou du projet dans la vue Propriétés, ou dans une configuration d'examen. Après l'examen d'applications ou de projets avec les règles pertinentes - ou l'utilisation d'une configuration d'examen incluant des règles - les résultats de la recherche de règle figurent dans les vues contenant des constatations.

Application de règles et d'ensembles de règles dans une configuration d'examen

Pour activer l'examen basé sur des schémas, cochez la case **Analyse de schéma**. Lorsque vous faites cela, les sections **Ensembles de règles de schémas** et **Règles de schémas** deviennent actives :

- Pour ajouter un ensemble de règles, cliquez sur **Ajouter** dans la section **Ensembles de règles de schémas**. Ceci a pour effet d'ouvrir la boîte de dialogue Ajouter des ensembles de règles de schémas qui vous permet de sélectionner un ou plusieurs ensembles de règles. Lorsque vous sélectionnez un ensemble de règles, les règles qu'il contient sont affichés dans la partie droite de la boîte de dialogue, et les types de projet auxquels s'applique l'ensemble de règles sont répertoriés dans la zone **Types de projets**. Cliquez sur **OK** pour ajouter les ensembles de règles sélectionnés.
- Pour ajouter une règle, cliquez sur **Ajouter** dans la section **Règles de schéma**. Ceci a pour effet d'ouvrir la boîte de dialogue Ajouter des règles de schéma, ce qui vous permet de sélectionner une ou plusieurs règles. Vous pouvez également cliquer sur **Créer une règle** afin de créer une nouvelle règle (voir «Création d'une règle de schémas», à la page 213). Si vous créez une nouvelle règle, elle sera ajoutée à la liste et sélectionnée. Après avoir sélectionné ou créé des règles, cliquez sur **OK** pour les ajouter à la configuration d'examen.

  Conseil : Dans la boîte de dialogue Ajouter des règles de schéma, l'infobulle d'aide indique les expressions qui sont utilisées pour chaque règle.

Application de règles et d'ensembles de règles à l'aide de la vue Propriétés

Sélectionnez le projet ou l'application dans la vue Explorateur, puis apportez les modifications mentionnées ci-dessous à l'onglet Règles de schéma et Ensembles de règles de sa vue Propriétés. Après avoir spécifié les règles et les ensembles de règles à appliquer au projet ou à l'application, sauvegardez les propriétés de l'application ou du projet. Les examens ultérieurs de l'application ou du projet intégreront ces règles.

- Pour ajouter un ensemble de règles, cliquez sur **Ajouter** dans la section **Ensembles de règles**, ou cliquez avec le bouton droit de la souris dans la section et sélectionnez **Ajouter**. Ceci a pour effet d'ouvrir la boîte de dialogue Sélection des propriétés de règle qui vous permet de sélectionner un ensemble de règles à ajouter.
- Pour supprimer un ensemble de règles afin qu'il ne soit pas utilisé lors d'examens de l'application ou du projet, sélectionnez cet ensemble et cliquez sur **Supprimer**, ou cliquez avec le bouton droit de la souris sur l'ensemble de règles et sélectionnez **Supprimer**.
- Pour ajouter une règle, cliquez sur **Ajouter** dans la section **Règles**, ou cliquez avec le bouton droit de la souris dans la section et sélectionnez **Ajouter**. Ceci a pour effet d'ouvrir la boîte de dialogue Choisir une règle qui vous permet de sélectionner une règle à ajouter. Dans cette boîte de dialogue, vous pouvez également cliquer sur **Nouvelle règle** afin de créer une nouvelle règle (voir «Création d'une règle de schémas», à la page 213). Si vous créez une nouvelle règle, elle sera ajoutée à la liste et sélectionnée. Après avoir sélectionné ou créé une règle, cliquez sur **OK** pour l'ajouter.
- Pour supprimer une règle afin qu'elle ne soit pas utilisée lors d'examens de l'application ou du projet, sélectionnez cette règle et cliquez sur **Supprimer**, ou cliquez avec le bouton droit de la souris sur la règle et sélectionnez **Supprimer**. Vous pouvez également sélectionner plusieurs règles et les supprimer à l'aide de ces mêmes actions.

Vue Configuration d'examen

La vue Configuration d'examen vous permet de créer des configurations que vous pouvez ensuite utiliser lors du lancement des examens. Vous pouvez aussi utiliser cette vue pour définir une configuration d'examen par défaut. Dans une configuration d'examen, vous pouvez spécifier les règles source à utiliser lors de l'examen et inclure de nombreux paramètres d'examen. Les paramètres définis dans une configuration d'examen permettent souvent d'obtenir de meilleurs résultats d'examen et la sauvegarde de ces paramètres peut faciliter l'examen et le rendre plus efficace et plus performant.

La vue Configuration d'examen comporte les sections principales suivantes :

- «Gestion de la configuration d'examen», à la page 96
- «Onglet Général», à la page 96
- «Onglet Analyse de flux corrompus», à la page 97
- «Onglet Analyse de schéma», à la page 98

Gestion de la configuration d'examen

Cette section permet de sélectionner, d'ajouter, de supprimer, de sauvegarder et de partager des configurations d'examen, ainsi que de définir des configurations d'examen par défaut.

- Pour créer une configuration d'examen, cliquez sur **Nouveau**. Une fois les paramètres de configuration d'examen définis, cliquez sur **Sauvegarde** pour enregistrer les modifications. Pour définir la configuration d'examen comme configuration par défaut, cliquez sur **Sélectionner comme valeur par défaut** après l'avoir sauvegardée. Pour connaître la façon dont est utilisée la configuration par défaut, voir «Analyse du code source», à la page 85.
- Pour utiliser une configuration d'examen existante, sélectionnez-la dans la liste :
  - Si vous modifiez les paramètres de configuration d'examen, cliquez sur **Sauvegarde** pour enregistrer les modifications (les modifications non souhaitées peuvent être supprimées en basculant vers une autre configuration d'examen et en cliquant sur **Supprimer**).
  - Pour supprimer la configuration d'examen sélectionnée, cliquez sur **Supprimer**.
  - Pour dupliquer la configuration d'examen, cliquez sur **Dupliquer**. Une configuration d'examen est alors créée en fonction des paramètres de la configuration d'examen d'origine.
  - Pour définir la configuration d'examen comme configuration par défaut, cliquez sur **Sélectionner comme valeur par défaut**. Pour connaître la façon dont est utilisée la configuration par défaut, voir «Analyse du code source», à la page 85.
  - Pour partager une configuration d'examen avec d'autres, cliquez sur **Partager**. Cette opération sauvegarde la configuration d'examen sur le serveur base de données AppScan Source.

    Remarque : Pour partager des configurations d'examen ou modifier ou supprimer une configuration d'examen partagée, vous devez disposer de l'autorisation **Gérer les configurations partagées**. Pour plus d'informations sur la définition des autorisations, voir le manuel *IBM Security AppScan Source - Guide d'installation et d'administration*.

Remarque : AppScan Source fournit des configurations d'examen intégrées. Elles ne peuvent être ni modifiées ni supprimées. Lorsque vous les sélectionnez dans la liste, vous pouvez les dupliquer ou afficher leurs paramètres.

Onglet Général

Informations de base

Cette section vous permet de nommer des configurations d'examen et de fournir une description pour chacune.

Filtres

Dans cette section, vous pouvez choisir un ou plusieurs filtres à appliquer à l'examen à chaque utilisation de la configuration d'examen. Lors de la sélection d'un filtre, vous pouvez choisir un filtre prédéfini par AppScan Source ou un filtre partagé ou un que vous avez créé. Voir «Gestion des configurations d'examen», à la page 90 pour plus de détails.

Onglet Analyse de flux corrompus

Analyse de flux corrompus

Activez et définissez la portée de l'analyse de flux corrompus.

Règles d'examen

Cette section permet de déterminer les règles source utilisées pour l'examen.

Une source est une entrée du programme, telle qu'un fichier, une requête de servlet, une saisie depuis la console ou un socket. En excluant certaines règles source, vous pouvez accélérer l'examen et éviter la détection des vulnérabilités provenant des entrées sans intérêt.

Les règles sont balisées à l'aide de propriétés de règle qui indiquent qu'elles sont liées à une vulnérabilité, un mécanisme, un attribut ou une technologie spécifique. Ces propriétés sont regroupées en ensembles de règles qui correspondent à un ensemble commun de règles connexes. Vous pouvez limiter les règles source incluses dans l'examen en spécifiant des ensembles de règles ou des propriétés de règles individuelles.

- Sélectionnez un ou plusieurs types de vulnérabilité (les vulnérabilités sont organisées par type dans les ensembles de règles) à inclure dans l'examen :
  - **Tout** : si cette option est sélectionnée, les vulnérabilités provenant de toutes les sources d'entrée prises en charge seront détectées.
  - **Entrée utilisateur** : si cette option est sélectionnée, les vulnérabilités provenant des entrées de l'utilisateur final seront détectées.
  - **Applications Web** : si cette option est sélectionnée, les vulnérabilités provenant des risques des applications Web seront détectées.
  - **Consignation et traitement des erreurs** : si cette option est sélectionnée, les vulnérabilités provenant de la consignation et du traitement des erreurs seront détectées.
  - **Environnement** : si cette option est sélectionnée, les vulnérabilités provenant des fichiers de configuration, des fichiers d'environnement système et des fichiers de propriété seront détectées.
  - **Systèmes externes** : si cette option est sélectionnée, les vulnérabilités provenant des entités externes seront détectées.
  - **Magasin de données** : si cette option est sélectionnée, les vulnérabilités provenant des magasins de données (tels que les bases de données et les caches) seront détectées.
  - **Données inhabituelles** : si cette option est sélectionnée, les vulnérabilités provenant des routines qui ne font normalement pas partie d'une application de production seront détectées.
  - **Système de fichiers** : si cette option est sélectionnée, les vulnérabilités provenant des systèmes de fichiers seront détectées.
  - **Données sensibles** : si cette option est sélectionnée, les vulnérabilités provenant des données sensibles seront détectées.

  Une infobulle décrit chaque ensemble de règles de cette section.
- Sélectionnez les propriétés de règles d'examen individuelles à inclure dans l'examen : cliquez sur **Annuler les ensembles de règles sélectionnés et me laisser sélectionner des propriétés de règles individuelles**. Ceci a pour effet d'ouvrir la boîte de dialogue Sélection des propriétés de règle qui permet de sélectionner des propriétés de règles individuelles. Si cette boîte de dialogue est renseignée, les ensembles de règles sélectionnés sont annulés. Les règles d'examen qui possèdent les propriétés de règle sélectionnées seront utilisées pour l'examen.

Paramètres avancés

Cette section est uniquement destinée aux utilisateurs avancés. Elle contient un certain nombre de paramètres qui peuvent améliorer les résultats d'examen. Une infobulle décrit chaque paramètre de cette section.

Onglet Analyse de schéma

analyse de schéma

Utilisez cette section pour activer l'examen basé sur des schémas lors de l'utilisation de la configuration d'examen. L'examen basé sur des schémas est un examen de votre code source basée sur des critères de recherche personnalisés.

Ensembles de règles de schémas et **Règles de schéma**

Utilisez ces sections pour ajouter des règles et des ensembles de règles à utiliser lors de l'analyse de schéma. Pour plus d'informations, voir «Personnalisation à l'aide de règles basées sur des schémas», à la page 209 et «Gestion des configurations d'examen», à la page 90.

Vue Propriétés : application sélectionnée

Cette vue permet de configurer des attributs pour l'application sélectionnée. Les attributs d'application dépendent des attributs globaux créés auparavant.

- «Présentation»
- «Exclusions et filtres»
- «Règles et ensembles de règles», à la page 220
- «Constatations modifiées», à la page 220
- «Constatations personnalisées», à la page 220

Présentation

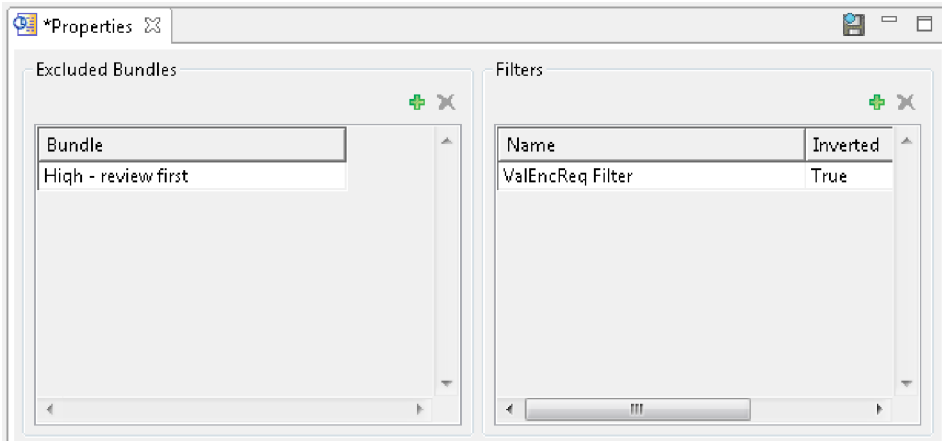
L'onglet Présentation contient les éléments suivants :

- Nom de l'application. L'application peut être renommée en entrant un nouveau nom dans la zone.
- Attributs de l'application

Exclusions et filtres

Cet onglet vous permet de spécifier les filtres existants pour l'application sélectionnés, et la façon dont vous souhaitez que les filtres soient appliqués (un filtre peut être appliqué directement ou de manière inversée). Dans l'onglet, vous pouvez également gérer des groupements qui excluent des résultats de l'examen. Voir Chapitre 5, «Triage et analyse», à la page 117 pour plus d'informations sur les filtres, et «Application globale des filtres», à la page 136 pour plus de détails sur leur application globale.

Les constatations exclues et filtrées n'apparaissent pas dans les résultats de l'examen et ne sont pas prises en compte dans les métriques de l'application ou du projet.



Règles et ensembles de règles

Lorsque vous sélectionnez une application dans la vue Explorateur, l'onglet Règles de schéma et Ensembles de règles de la vue Propriétés vous permet d'ajouter des règles de schéma et des ensembles de règles qui seront appliqués lors de l'examen de l'application. L'examen basé sur des schémas permet de rechercher des schémas de texte que vous désirez voir figurer en tant que constatations. Des règles et des ensembles de règles individuels peuvent être appliqués à la fois aux applications et aux projets. Voir «Personnalisation à l'aide de règles basées sur des schémas», à la page 209 pour plus de détails sur l'analyse basée sur des schémas et «Application de règles et d'ensembles de règles de schémas», à la page 215 pour plus de détails sur l'application de règles et d'ensembles de règles dans la vue Propriétés.

Constatations modifiées

Depuis cet onglet, vous pouvez visualiser, éditer ou supprimer des constatations modifiées auparavant ou modifier une constatation existante. Les *constatations modifiées* désignent des constatations dont le type de vulnérabilité, la gravité, la classification ou les notes ont été changés.

Constatations personnalisées

Depuis cet onglet, vous pouvez visualiser, ajouter, modifier ou supprimer des constatations personnalisées. Pour plus de détails, voir «Constatations personnalisées», à la page 150.

Vue Propriétés : projet sélectionné

Ce mode de la vue Propriétés permet de configurer des paramètres pour le projet sélectionné. Les attributs de projet dépendent des attributs globaux créés auparavant. Les propriétés varient selon le projet sélectionné.

- «Onglet Présentation du projet sélectionné», à la page 221
- «Filtres», à la page 222
- «Règles de schéma et ensembles de règles», à la page 222
- «Extensions de fichier», à la page 222
- «Sources», à la page 223
- «Dépendances de projet JSP (JavaServer Page)», à la page 224
- «Dépendances de projet», à la page 224
- «Compilation», à la page 224

- «Optimisations», à la page 225

Onglet Présentation du projet sélectionné

L'onglet Présentation contient les éléments suivants :

- **Nom** du projet. Le projet peut être renommé en entrant un nouveau nom dans la zone.
- Nom et chemin du **fichier** de projet
- **Type du projet**
- Configuration : cette section affiche la configuration cible. Pour les projets Objective-C, elle affiche la configuration cible qui a été sauvegardée dans l'onglet Dépendances de projet. Pour tous les autres types de projet, elle affiche **Par défaut**.
- Option de filtrage : Sélectionnez **Filtrer les constatations contenues dans des sources externes** pour écarter les constatations provenant de fichiers qui ne sont pas des fichiers source du projet analysé. Cette option réduit le bruit pour les projets où les constatations sont signalées dans des fichiers générés par le compilateur ou temporaires.
- Options de mise en cache de l'analyse de vulnérabilités : Si vous affinez votre évaluation d'un codebase en l'examinant par itérations et en ajoutant des règles personnalisées, puis en l'examinant à nouveau sans modifier le code source, vous pouvez réduire considérablement la durée de l'examen en définissant les propriétés du projet de sorte à utiliser un cache d'analyse des vulnérabilités. Pour ce faire, cochez la case **Activer le cache d'analyse de vulnérabilités** dans les propriétés du projet. Un cache d'analyse de vulnérabilités est créé la première fois que vous examinez le projet après avoir coché cette case. Ce cache sera utilisé à chaque examen ultérieur du projet, réduisant ainsi la durée de l'examen.

  Pour vider le cache d'analyse de vulnérabilité, cliquez sur **Vider le cache**. Lors du prochain examen du projet, un examen complet aura lieu et un nouveau cache d'analyse de vulnérabilité sera créé. Vous pouvez envisager de vider le cache si :

  – Le code source du projet a été modifié depuis le dernier examen.
  – Vous avez apporté des modifications à la configuration du projet (par exemple, l'ajout ou la suppression de fichiers source).
  – Vous avez modifié des options de configuration du code. Par exemple, vous pouvez vouloir vider le cache si vous examinez un projet Java et que le chemin de classes a changé ou si vous examinez un projet C ou C++ et que vous avez modifié le chemin `include` ou les définitions de préprocesseur.

  Remarque : Vous pouvez également vider le cache d'analyse de vulnérabilités en cochant la case **Vider le cache** lors de la création de règles personnalisées dans l'assistant Règles personnalisées.
- **Analyse de chaîne** : L'analyse de chaîne surveille les manipulations de chaînes dans les projets Java. Elle assure la détection automatique des routines d'assainissement et de validation. Grâce à cette détection, il est possible de réduire les résultats faussement positifs ou faussement négatifs. Pour activer l'analyse de chaîne, cochez la case **Activer l'analyse de chaîne pour trouver les fonctions permettant de valider et rendre inoffensif**. La case **Appliquer les règles importées à la portée globale** détermine si les routines d'assainissement ou de validation découvertes doivent être appliquées à l'échelle du projet ou au niveau global (à tous les projets).

Remarque : L'analyse de chaîne peut ralentir l'analyse du code. Il est donc recommandé de ne l'appliquer qu'après un changement de code, puis de la désactiver pour les analyses suivantes. En outre, les routines découvertes doivent être considérées comme des *suggestions* et examinées par les auditeurs. Ces routines peuvent être visualisées dans la vue Règles personnalisées.

- **Codage du fichier** : Le codage de caractères des fichiers dans votre projet doit être défini afin que AppScan Source puisse lire ces fichiers correctement (et, par exemple, afin qu'il puisse les afficher correctement dans la vue Source).

  Remarque : Le codage de fichier par défaut pour les projets AppScan Source est **ISO-8859-1**. Le codage de fichier par défaut peut être modifié sur la page de préférences générales.

Filtres

Cet onglet vous permet de spécifier les filtres existants pour le projet sélectionné, et la façon dont vous souhaitez que les filtres soient appliqués (un filtre peut être appliqué directement ou de manière inversée). Voir Chapitre 5, «Triage et analyse», à la page 117 pour plus d'informations sur les filtres, et «Application globale des filtres», à la page 136 pour plus de détails sur leur application globale.

Règles de schéma et ensembles de règles

Lorsque vous sélectionnez un projet dans la vue Explorateur, l'onglet Règles de schéma et Ensembles de règles de la vue Propriétés vous permet d'ajouter des règles de schéma et des ensembles de règles qui seront appliqués lors de l'examen du projet. L'analyse basée schéma permet de rechercher des schémas de texte que vous désirez voir figurer en tant que constatations. Des règles et des ensembles de règles individuels peuvent être appliqués à la fois aux applications et aux projets. Voir «Personnalisation à l'aide de règles basées sur des schémas», à la page 209 pour plus de détails sur l'analyse basée sur des schémas et «Application de règles et d'ensembles de règles de schémas», à la page 215 pour plus de détails sur l'application de règles et d'ensembles de règles dans la vue Propriétés.

Extensions de fichier

Utilisez cet onglet pour configurer ou ajouter des extensions de fichier valides pour le projet - et pour exclure des fichiers des examens et spécifier des extensions comme fichiers Web.

La section **Extensions de fichier** répertorie les extensions qui ont été définies de manière globale dans la page de préférences «Extensions de fichier de projet», à la page 83 du type de projet en cours (vous pouvez choisir des extensions de fichier pour un type de projet différent en utilisant le menu **Ensemble d'extensions de fichier**). Pour exclure une extension des examens du projet en cours, sélectionnez-la dans la liste et cliquez sur **Exclure une extension**. L'extension apparaît alors dans la section **Extensions exclues** de l'onglet.

Pour ajouter une extension supplémentaire pour le projet, sélectionnez **Ajouter une extension** dans la section **Extensions supplémentaires** et entrez ensuite l'extension du fichier et indiquez si les fichiers ayant cette extension doivent être examinés, considérés comme des fichiers Web ou exclus.

Tableau 20. Paramètres d'extension de fichier

Paramètre	Description	Exemples d'utilisation
Examen ou **Evaluation**	Inclure les fichiers ayant l'extension indiquée dans l'analyse complète.	• Si une extension `.xxx` est créée pour les projets Java et marquée comme **Examen** ou **Evaluation**, les fichiers dotés de cette extension seront compilés et examinés. • Un fichier peut faire partie d'un projet mais ne pas être marqué comme **Examen** ou **Evaluation** s'il ne doit pas être compilé et examiné.
Fichier Web	Marquer les fichiers ayant l'extension indiquée pour la compilation JSP. Ce paramètre autorise AppScan Source à séparer les sources Web des sources non Web.	Si une extension `.yyy` est créée pour les projets Java et marquée comme **Fichier Web**, les fichiers ayant cette extension sont organisés en sources Web dans les projets. Lorsqu'AppScan Source se prépare pour l'analyse, ces fichiers seront précompilés en classes à analyser.
Exclure	Ne pas créer de fichiers source dans le projet pour des fichiers ayant l'extension indiquée. Les fichiers ayant cette extension ne seront pas examinés.	Créez une extension `.zzz` pour les fichiers qui sont nécessaires à vos projets pour la compilation, mais qui ne doivent pas être inclus dans l'analyse.

Sources

Spécifiez les sources à inclure dans l'examen.

- Répertoire de travail : Emplacement du fichier de projet AppScan Source (`ppf`) qui constitue la base de tous les chemins relatifs.
- **Ajouter une racine source** et **Supprimer une racine source** : L'onglet Sources affiche les propriétés définies pour le projet à partir de l'assistant Configuration de projet ou dans le `ppf` importé.

  L'option **Supprimer la racine source** est uniquement disponible si l'icône **Racine source** est sélectionnée. Elle permet de supprimer le répertoire racine de code source.
- Rechercher des racines source (projets Java uniquement) : Permet à AppScan Source for Analysis d'identifier automatiquement les racines source valides.
- Les fichiers de projet sont affichés sous l'icône **Racine source**. Les fichiers qui sont exclus de l'examen sont accompagnés d'une icône de fichier rouge (si vous faites un clic droit sur un fichier exclus, l'option **Exclure** de son menu est désactivée et l'option **Inclure** est activée). Pour exclure un fichier inclus, faites un clic droit dessus et sélectionnez **Exclure** dans le menu. Pour inclure un fichier exclus, faites un clic droit dessus et sélectionnez **Inclure** dans le menu.

Dépendances de projet JSP (JavaServer Page)

Cet onglet affiche les propriétés définies pour le projet JSP sélectionné.

- Contient un contenu Web (JSP) : Indique si le projet est une application Web contenant des pages JavaServer Pages.
- Racine de contexte Web : Fichier `WAR` ou répertoire hébergeant le répertoire `WEB-INF`. La racine de contexte Web doit être la racine d'une application Web valide.
- Compilateur JSP : Prêt à l'emploi, Tomcat 7 est le compilateur JSP sélectionné par défaut (il est possible d'en changer sur la page de préférences Java et JSP). Pour en savoir plus sur les compilateurs pris en charge par AppScan Source, voir http://www.ibm.com/support/docview.wss?uid=swg27027486.

  Les versions d'Apache Tomcat versions 7 et 8 sont incluses dans l'installation d'AppScan Source. Si les pages de préférences **Tomcat 7** et **Tomcat 8** ne sont pas configurées, AppScan Source compile les fichiers JSP à l'aide du compilateur JSP Tomcat fourni et indiqué comme valeur par défaut. Si vous souhaitez employer un compilateur Tomcat externe pris en charge, utilisez les pages de préférences Tomcat pour pointer sur votre installation Tomcat locale.

  Si vous utilisez Oracle WebLogic Server ou WebSphere Application Server, vous devez configurer la page de préférences correspondante, le but étant de désigner votre installation locale du serveur d'applications afin qu'elle puisse être utilisée pour la compilation du code JSP durant l'analyse. Si vous n'avez pas encore terminé cette configuration, un message vous demandera de la faire lorsque vous sélectionnerez le compilateur JSP. Si vous répondez **Oui** au message, la page de préférences appropriée s'affiche. Si vous répondez **Non**, un lien d'avertissement s'affiche à côté de la sélection du compilateur JSP (ce lien permet d'ouvrir la page de préférences).

Dépendances de projet

Cet onglet présente les propriétés du projet. Les paramètres de configuration qui figurent dans cet onglet varient selon le langage. Exemple :

- Les paramètres du JDK sont propres à Java.
- La configuration cible est disponible pour les projets Objective-C seulement.

Remarque : Dans l'onglet Dépendances de projet d'un projet Objective-C, la section **Configuration cible** seulement peut être éditée. Toutes les autres sections de l'onglet sont accessibles en lecture seule.

Compilation

- Options : Paramètres de compilation requis supplémentaires pour la configuration du projet.
- Utiliser le kit JDK : Identifiez le kit JDK utilisé pour la compilation du projet et configuré dans les préférences. Voir Chapitre 3, «Préférences», à la page 73.

  Les projets Java peuvent se référer à un emplacement de kit JDK (Java Development Kit) local. Lorsque les projets sont transférés au serveur, le chemin du kit JDK peut ne plus être valide. Pour transférer des projets locaux au serveur, vous devez identifier le chemin JDK par défaut pour chaque projet spécifiant nominativement un kit JDK.

  Remarque : Prêt à l'emploi, le compilateur par défaut des projets JSP est Tomcat 7, qui requiert Java version 1.6 ou version ultérieure. Si **Tomcat 7** est conservé

par défaut et que vous sélectionnez un JDK plus ancien, des erreurs de compilation seront générées pendant les examens.

- Valider : L'option **Valider** garantit que les dépendances du projet soient correctement configurées. Elle vérifie l'absence dans les projets Java de conflits de configuration entre les sources et le chemin de classes et vérifie également l'absence d'erreurs de compilation. **Un conflit existe** si une classe du chemin de classes est dupliquée dans une racine source. (En cas de conflit, modifiez le chemin de classes en supprimant celle en conflit).

  Après la vérification de l'absence de conflits, l'option **Valider** détermine si le projet peut être compilé et rend compte des erreurs de compilation éventuelles.

Optimisations

- **Classes précompilées** : Utilise des fichiers de classes Java ou JSP précompilées au lieu de la compilation pendant l'examen. Lorsque cette option est sélectionnée, celles de zone de préparation de la source sont désactivées.
- Déployer pour pré-traitement les fichiers source pour minimiser les effets d'erreur de compilation : Détermine si AppScan Source doit copier les sources vers le répertoire de préparation.

  Corriger pour les packages non conformes à la structure de répertoire requiert Java Compile pour ouvrir chaque fichier source.

  Nettoyer la zone de préparation entre chaque examen améliore les performances entre les examens.

Chapitre 11. Extension de l'infrastructure d'importation de serveur d'applications

AppScan Source vous permet d'importer des applications Java depuis Apache Tomcat et le profil Liberty WebSphere Application Server. Vous pouvez importer des applications Java à partir d'autres serveurs d'applications en étendant l'infrastructure d'importation de serveur d'applications, comme expliqué dans cette rubrique.

Pourquoi et quand exécuter cette tâche

L'infrastructure d'importation de serveur d'applications est accompagnée par une documentation d'API qui n'est pas disponible au format PDF. Si avez accès à cette rubrique d'aide via Adobe PDF, vous ne pouvez accéder à la documentation d'API qu'en lançant l'aide en ligne d'AppScan Source for Analysis et en navigant jusqu'à **Extension des fonctions du produit** > **Extension de l'infrastructure d'importation de serveur d'applications** > **Classes et méthodes d'API d'extension d'infrastructure d'importation de serveur d'applications**, ou en recherchant cette section de l'aide dans http://www.ibm.com/support/knowledgecenter/SSS9LM/welcome.

Pour étendre l'infrastructure d'importation de serveur d'applications, exécutez la procédure ci-dessous. Ces étapes vous feront exécuter les opérations suivantes :

- Configurer un environnement de développement intégré Eclipse
- Créer un nouveau plug-in dans Eclipse
- Définir les dépendances requises dans le plug-in nouvellement créé
- Dans le plug-in, définir une extension pour votre serveur d'applications
- Tester le plug-in
- Activer le plug-in pour AppScan Source for Analysis

Procédure

1. Configurez un environnement de développement intégré Eclipse pour les dépendances requises par l'infrastructure d'importation de serveur d'applications AppScan Source :
   a. Dans Eclipse, sélectionnez **Fenêtre** > **Préférences** dans le menu principal.
   b. Dans la boîte de dialogue Préférences, développez **Développement de plug-in**, puis sélectionnez **Plateforme cible**.
   c. Dans la page des préférences de plateforme cible, cliquez sur **Ajouter** pour créer une définition de cible.
   d. Dans la page d'assistant de définition de cible, sélectionnez **Rien : cette option créer une définition de cible vide** et cliquez sur **Suivant**.
   e. Dans la page de l'assistant de contenu cible, entrez un nom pour la cible dans la zone **Nom** et cliquez sur **Ajouter** pour ajouter votre répertoire d'installation AppScan Source (voir «Installation et emplacements des fichiers de données utilisateur», à la page 292).
   f. Facultatif : Sélectionnez **Afficher le contenu de l'emplacement** pour vérifier que des plug-ins sont disponibles.
   g. Cliquez sur **Terminer**.

h. Dans la page des préférences de plateforme cible, sélectionnez la plateforme cible que vous venez de créer et cliquez sur **Appliquer**. Puis, cliquez sur **OK**.

2. Créez un nouveau plug-in dans Eclipse :
   a. Sélectionnez **Fichier** > **Nouveau projet** dans le menu principal pour ouvrir l'assistant Nouveau projet.
   b. Dans la page de sélection d'un assistant, sélectionnez **Projet de plug-in** et cliquez sur **Suivant**.
   c. Dans la page Projet de plug-in, entrez un nom pour le plug-in dans la zone **Nom du projet** (cette rubrique d'aide utilisera `com.example.appserverimporter` comme exemple) et cliquez sur **Suivant**.
   d. Dans la page de contenu, désélectionnez **Générer un activateur, une classe Java qui contrôle le cycle de vie du plug-in** et cliquez sur **Terminer**.
3. Dans le plug-in que vous venez de créer, définissez les dépendances nécessaires :
   a. Ouvrez `META-INF\MANIFEST.MF` et sélectionnez l'onglet **Dépendances**.
   b. Dans la section **Plug-ins requis** de l'éditeur :
      - Cliquez sur **Ajouter**, puis ajoutez `com.ouncelabs.core.appserverimporter` et `org.eclipse.core.runtime`.
      - Sélectionnez le plug-in `com.ouncelabs.core.appserverimporter` que vous venez d'ajouter et cliquez sur **Propriétés**. Dans les propriétés du plug-in, supprimez les entrées des zones **Version minimale** et **Version maximale**, puis cliquez sur **OK**.
      - Répétez l'étape ci-dessus pour le plug-in `org.eclipse.core.runtime`.
   c. Sélectionnez **Fichier** > **Sauvegarder** dans le menu principal pour sauvegarder les modifications apportées à l'éditeur.
   d. L'étape suivante vous permettra de définir une extension pour votre serveur d'applications. Pour cette étape, vous continuez à travailler dans l'éditeur `META-INF\MANIFEST.MF`.
4. Définissez une extension d'importateur pour votre serveur d'applications en procédant comme suit :
   a. Sélectionnez l'onglet **Extensions**, cliquez sur **Ajouter** pour ajouter `com.ouncelabs.appserver`, puis sélectionnez **Fichier** > **Sauvegarder** dans le menu principal.
   b. Sélectionnez l'onglet **plugin.xml**. Son contenu doit ressembler à ceci :

```
<?xml version="1.0" encoding="UTF-8"?>
<?eclipse version="3.4"?>
<plugin>
  <extension
    point="com.ouncelabs.appserver">
  </extension>
</plugin>
```

   Effectuez la définition d'extension en éditant le contenu. Par exemple :

```
<?xml version="1.0" encoding="UTF-8"?>
<?eclipse version="3.4"?>
<plugin>
  <extension
    point="com.ouncelabs.appserver">
    <importer
     class="com.example.appserverimporter.MyAppServerImporter"
     id="com.example.appserverimporter.myappserver"
     name="Mon Serveur App">
   </importer> </extension>
</plugin>
```

c. Sélectionnez **Fichier** > **Sauvegarder** dans le menu principal pour sauvegarder les modifications apportées à **plugin.xml**.

5. Créer la classe d'importateur (dans cet exemple, `com.example.appserverimporter.MyAppServerImporter`) pour définir le comportement du nouvel importateur de serveur d'applications. Cette classe doit étendre `BaseAppServerImporter`, l'implémentation de base de l'infrastructure pour l'interface `AppServerImporter`. Dans cette classe :
   a. Implémentez `AppServerImporter.importAppServer(String)`. Cette méthode est utilisée par l'infrastructure pour déterminer les projets Java EE à importer et leur emplacement. En règle générale, seuls le nom et le chemin du projet Java EE sont nécessaires pour chaque projet. Si des projets d'application d'entreprise (EAR) sont créés, les projets Java EE qu'ils contiennent sont masqués lorsque vous sélectionnez des projets dans l'interface utilisateur AppScan Source. Dans notre cas, la totalité du fichier d'archive d'entreprise sera importé. Sinon, tous les projets sont répertoriés pour être sélectionnés individuellement.

      L'utilisation de ces méthodes est fortement recommandée, le cas échéant :

      - `BaseAppServerImporter.processDropInsFolder(AppServerProfile, File)`
      - `BaseAppServerImporter.processEARFile(AppServerProfile, File)`

   b. Implémentez `AppServerImporter.isValidLocation(String)`. Cette méthode permet de détecter le type de serveur, en fonction du répertoire d'installation.
   c. Facultatif : Redéfinissez `BaseAppServerImporter.getJSPCompilerType()`. Cette méthode renvoie le compilateur JSP à utiliser pour le projet AppScan Source. Si vous n'effectuez pas cette opération, l'implémentation de base renvoie la valeur NULL, et le compilateur JSP par défaut du produit sera utilisé.
6. Facultatif : En tant qu'option avancée, vous pouvez personnaliser la compilation JSP pour utiliser un compilateur de JSP précompilé (la compilation JSP a lieu avant ou pendant l'importation) :
   a. Redéfinissez `BaseAppServerImporter.getJSPCompilerType()` pour renvoyer `JSPCompilerType.PRECOMPILED`.
   b. Redéfinissez `BaseAppServerImporter.getJSPCompilerType()` pour appeler JMX, l'API Java et des scripts externes pour compiler les fichiers JSP, ou copiez simplement des fichiers de classe dans le répertoire de transfert du projet AppScan Source. Utilisez `Application.getStagingDirectory(Project)` pour obtenir le répertoire de transfert.
   c. Redéfinissez `BaseAppServerImporter.createJSPCompilerSupport()` pour renvoyer une extension personnalisée de `JSPCompilerSupport`. Cette méthode est utilisée pour conserver le mappage entre les fichiers JSP et les fichiers de classe générés, ainsi que pour la validation après la compilation JSP.
   d. Redéfinissez `BaseAppServerImporter.createClasspathProvider()` pour renvoyer une implémentation personnalisée de `AppServerClasspathProvider`. Cette classe est requise pour compiler tout fichier Java ou JSP comportant des dépendances sur des bibliothèques de serveur. La classe doit étendre `BaseAppServerClasspathProvider`. Notez que `BaseAppServerClasspathProvider.installDirectory` sera déjà défini sur le répertoire d'installation pour le serveur d'applications lorsque `getClasspathEntries()` est appelé.
7. Testez le plug-in en procédant comme suit :

a. Sélectionnez **Exécuter** > **Exécuter les configurations** dans le menu principal (ou **Exécuter** > **Déboguer** si vous souhaitez effectuer le test en mode débogage).
b. Créez une nouvelle configuration **Application Eclipse**.
   - Accédez à **Onglet Principal** de la nouvelle configuration. Dans la section **Programme à exécuter**, sélectionnez **Exécuter un produit** et définissez la zone pour exécuter **com.ouncelabs.osa.rcp.product**.
   - Accédez à l'onglet **Arguments**. Dans la section **Répertoire de travail**, sélectionnez **Autre** et entrez votre répertoire de données AppScan Source dans la zone (voir «Installation et emplacements des fichiers de données utilisateur», à la page 292).
   - Dans l'onglet **Plug-ins**, définissez la sélection **Lancer avec** sur **plug-ins sélectionnés au-dessous uniquement**. Développez **Espace de travail** et vérifiez que le plug-in que vous avez créé est sélectionné, puis désélectionnez les plug-ins suivants sous **Plateforme cible**:
     - `com.ouncelabs.plugin.base`
     - `com.ouncelabs.plugin.base`
     - `com.ouncelabs.plugin.base.nl`
     - `com.ouncelabs.plugin.base.nl`
     - `com.ouncelabs.plugin.enhanced`
     - `com.ouncelabs.plugin.enhanced`
     - `com.ouncelabs.plugin.enhanced.nl`
     - `com.ouncelabs.plugin.enhanced.nl`
c. Avant de cliquer sur **Exécuter** dans la boîte de dialogue Exécuter les configurations, accédez à votre répertoire d'installation AppScan Source et exécutez `bin\OunceScanner.exe`.
d. Revenez à la boîte de dialogue Exécuter les configurations, puis cliquez sur **Exécuter** pour lancer AppScan Source for Analysis et tester le plug-in.

8. Activez le plug-in pour AppScan Source for Analysis en procédant comme suit :
   a. Cliquez avec le bouton droit de la souris sur le projet et sélectionnez **Exporter**.
   b. Dans la page de sélection de l'assistant d'exportation, développez **Développement de plug-in**, sélectionnez **Plug-ins et fragments déployables**, puis cliquez sur **Suivant**.
   c. Dans la page Plug-ins et fragments déployables :
      - Accédez à l'onglet **Destination** et définissez le **Répertoire** en navigant jusqu'à un répertoire temporaire de votre machine.
      - Accédez à l'onglet **Options**, puis sélectionnez **Mettre en forme les plug-ins sous forme d'archives JAR distinctes** et **Remplacement de qualifiant**.
      - Cliquez sur **Terminer**.
   d. Recherchez le répertoire temporaire utilisé comme destination pour exporter le plug-in et ouvrez son dossier `plugins\`. Dans ce dossier, recherchez le fichier `.jar` qui a été créé et copiez-le dans `<install_dir>\dropins` (où `<rép_install>` représente l'emplacement de votre installation AppScan Source).

      Remarque :
      - Si le répertoire `\dropins` n'existe pas, vous devez le créer manuellement.

- Vous pouvez avoir besoin des privilèges d'administration pour modifier le répertoire d'installation AppScan Source.

e. Recherchez `<install_dir>\configuration\org.eclipse.equinox.simpleconfigurator\bundles.info`. Effectuez une copie de sauvegarde du fichier, puis éditez le fichier et ajoutez ceci à la fin de celui-ci :

```
<mon_plugin>,<ma_version_plugin>,
dropins/<mon_plugin>_<ma_version_plugin>.jar,4,false
```

Où :

- `<mon_plugin>` est le nom du plug-in que vous avez créé.
- `<ma_version_plugin>` est le numéro de version du plug-in que vous avez créé.

Remarque : Au début de cette entrée, `<mon_plugin>`, `<ma_version_plugin>`, et l'emplacement `dropins/` sont séparés par des virgules (`,`).

f. Démarrez AppScan Source for Analysis.

g. Sélectionnez **Aide** > **A propos de AppScan Source for Analysis** dans le menu principal et cliquez sur **Détails de l'installation**. Sélectionnez l'onglet **Plug-ins** et vérifiez que votre plug-in y figure.

h. Fermez la boîte de dialogue Détails de l'installation et commencez à utiliser votre infrastructure d'importation de serveur d'applications.

Chapitre 12. Exemples AppScan Source for Analysis

AppScan Source for Analysis comporte un exemple d'application que vous pouvez utiliser pour vous familiariser avec le produit.

Une fois AppScan Source for Analysis installé, les exemples d'application se trouvent dans `<data_dir>\samples` (où `<rép_données>` est l'emplacement de vos données de programme AppScan Source, comme décrit dans «Installation et emplacements des fichiers de données utilisateur», à la page 292).

Exemple d'application Java : `simpleIOT`

L'exemple `simpleIOT` est une petite application Java qui contient plusieurs vulnérabilités de sécurité. Vous pouvez l'importer manuellement dans le plan de travail AppScan Source for Analysis, ou importer le fichier d'application (`SimpleIOT.paf`) ou le fichier de projet (`SimpleIOT.ppf`) qui sont inclus dans l'exemple. Pour savoir comment ajouter des applications et des projets, voir Chapitre 2, «Configuration d'applications et de projets», à la page 33.

Après avoir ajouté l'exemple dans AppScan Source, vous pouvez l'examiner et explorer ses constatations.

Chapitre 13. Environnement de travail AppScan Source for Analysis

Afin d'exploiter pleinement les capacités de AppScan Source, vous devez avoir une bonne connaissance des concepts fondamentaux de l'environnement de travail AppScan Source for Analysis et savoir comment utiliser les options correspondant le mieux à votre flux de travaux.

Plan de travail AppScan Source for Analysis

Le flux de travaux AppScan Source for Analysis se déroule dans un *plan de travail*, lequel est composé de perspectives, de vues et d'éditeurs qui sont visibles ou masqués en fonction du contexte.

Perspectives

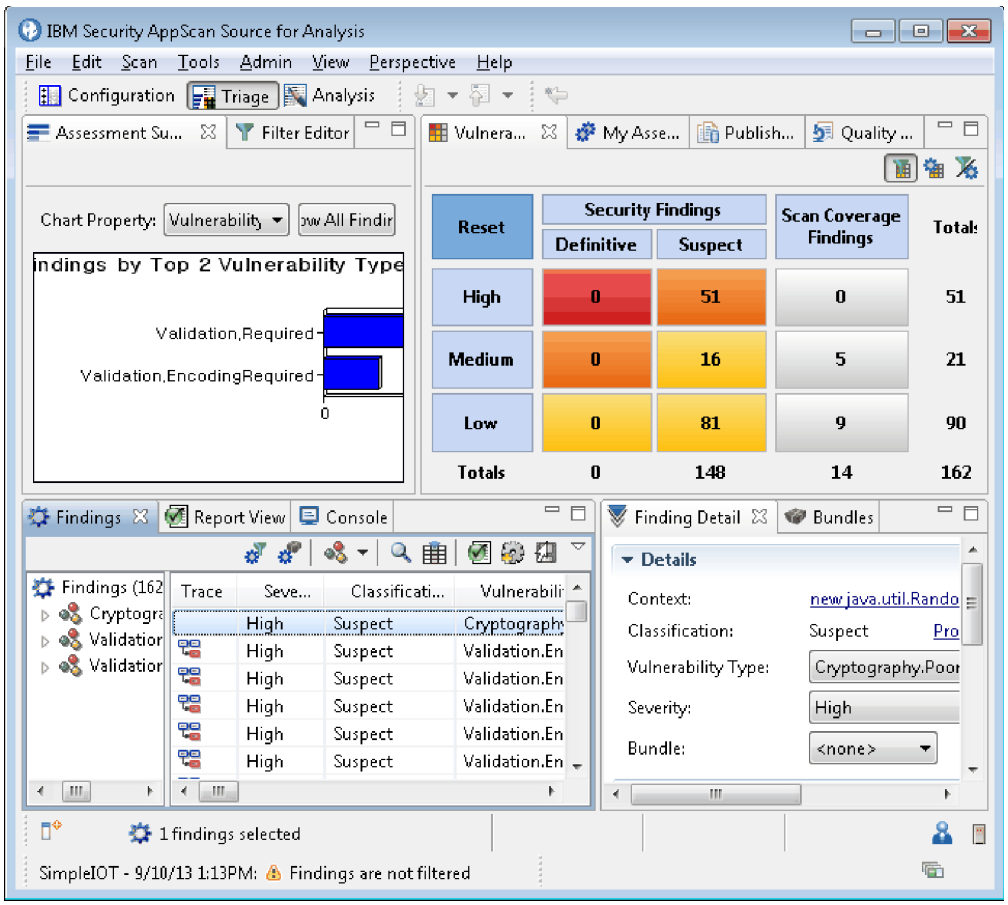
Les trois perspectives du produit, Configuration, Triage et Analyse, sont composées de plusieurs vues. Bien que chaque perspective s'ouvre avec des vues par défaut, vous pouvez réorganiser ces dernières afin de personnaliser chaque perspective. Les vues sont décrites en détail dans la section d'aide Chapitre 14, «Vues», à la page 249.

- Perspective Configuration : permet de créer et gérer des applications, des projets et des attributs.
- Perspective Triage : permet d'afficher les résultats de l'examen afin d'attribuer des priorités dans le flux de travaux de résolution des vulnérabilités et séparer les vulnérabilités réelles des potentielles. Cette perspective peut être utilisée pour isoler les problèmes que vous devez résoudre en premier lieu.
- Perspective Analyse : permet d'explorer les constatations individuelles et de vérifier le code source, les recommandations de résolution et la trace AppScan Source.

Fenêtre du plan de travail

La fenêtre du plan de travail AppScan Source for Analysis se compose des éléments suivants :

- Menu principal : menus permettant d'accéder aux fonctions AppScan Source for Analysis.
- Barre d'outils : icônes et boutons correspondant aux fonctions fréquemment utilisées.
- Perspectives : collections de vues.
- Vues : présentations et moyens de navigation entre les informations du plan de travail.



Barres d'outils et informations affichées en bas du plan de travail

- Barre d'outils de la **vue rapide** : Les vues rapides sont des vues masquées qui peuvent être rapidement ouvertes et refermées. Elles fonctionnent comme les autres vues sans prendre de place dans la fenêtre du plan de travail. Les vues rapides sont représentées par des boutons de barre d'outils situés dans la barre de vue rapide, qui est la barre d'outils située en bas à gauche de la fenêtre du plan de travail. Lorsque vous cliquez sur le bouton de barre d'outils d'une vue rapide, cette vue s'ouvre temporairement dans la perspective en cours (en superposition). Dès que vous cliquez en dehors de cette vue ou que la vue n'est plus mise en évidence, elle est de nouveau masquée. Pour configurer une vue en vue rapide, cliquez sur l'option d'**affichage de la vue comme vue rapide**, puis sélectionnez la vue dans le menu.
- Constatations sélectionnées : Lorsque des constatations sont sélectionnées, un indicateur situé en bas du plan de travail affiche le nombre de constatations sélectionnées.
- Informations sur les fichiers source : Lorsqu'un fichier source est ouvert, les informations suivantes relatives au fichier s'affichent en bas du plan de travail :
  - Fichier accessible en écriture ou en lecture seule. Si vous tentez d'éditer un fichier en lecture seule, une invite dans AppScan Source for Analysis vous permet de rendre ce fichier accessible en écriture.
  - Système d'exploitation en mode d'entrée insertion ou écrasement.
  - Emplacement actuel du curseur dans le fichier (numéros de ligne et de colonne).

- Informations de connexion au serveur : Le fait de survoler l'icône de l'utilisateur indique l'utilisateur actuellement connecté à AppScan Enterprise Server, et le fait de survoler l'icône du serveur vous permet de voir le serveur AppScan Enterprise Server auquel est connecté AppScan Source for Analysis.
- Une fois l'évaluation ouverte, le bas du plan de travail affiche les informations suivantes :
  - Le nom de l'évaluation et la date et l'heure de sa création.
  - Un indicateur qui vous permet de déterminer rapidement la façon dont les filtres ont été appliqués aux constatations dans l'évaluation. Pour plus d'informations, voir «Détermination des filtres appliqués», à la page 136.
- Un indicateur de progression s'affiche en bas du plan de travail qui indique les actions en cours. Par exemple, cet indicateur apparaît lors des examens et de la publication des évaluations. En outre, cette section indique lorsqu'une évaluation est ouverte.

Menu principal

La barre du menu principal contient des menus vous permettant d'exécuter une grande diversité d'actions. Vos droits utilisateur peuvent contrôler les commandes qui sont mises à votre disposition dans ces menus.

AppScan Source

Le menu **Source AppScan** fournit des liens rapides vers des actions AppScan Source clés, de même que vers des actions courantes du menu produit macOS.

Tableau 21. Menu Fichier

Option de menu	Description	Raccourci clavier
A propos d'IBM Security AppScan Source for Analysis	Cette action ouvre une boîte de dialogue qui fournit des informations sur le produit AppScan Source for Analysis.	
Préférences	Cette option permet d'ouvrir la boîte de dialogue Préférences. Les préférences sont les choix personnels de l'utilisateur concernant l'apparence et le fonctionnement de AppScan Source for Analysis.	command+,
QuitIBM Security AppScan Source for Analysis	Quitte AppScan Source for Analysis.	command+Q

Menu Fichier

Le menu **Fichier** propose des options pour les applications, les projets et les évaluations, et vous permet de quitter le produit. Certaines options du menu **Fichier** varient selon le contexte, en fonction de la vue active et de l'option actuellement sélectionnée dans cette vue.

Tableau 22. Menu Fichier

Option de menu	Description	Raccourci clavier
Ajouter une application > **Créer une nouvelle application**	Ajoute une nouvelle application à l'ensemble des applications. Cette action lance l'assistant Nouvelle application.	commande+N
Ajouter une application > **Ouvrir une application existante**	Lance une boîte de dialogue d'ouverture qui vous permet de rechercher et d'ajouter une application existante à l'ensemble des applications. Les types de fichier ou de répertoire pouvant être ajoutés sont notamment `.paf`,`.xcodeproj`, `.xcworkspace` et `.ewf`.	commande+O
Ajouter une application > **Importer un espace de travail basé sur Eclipse existant**	Lance la boîte de dialogue Ajout d'espace de travail qui vous permet d'ajouter un espace de travail Eclipse ou IBM Rational Application Developer for WebSphere Software (RAD) existant qui contient des projets Java. Une fois l'espace de travail importé, vous pouvez examiner n'importe quel projet Java inclus dans cet espace. **Remarque :** Avant d'importer l'espace de travail, assurez-vous d'avoir installé et mis à jour l'environnement de développement comme décrit dans la rubrique «Configuration de l'environnement de développement pour des projets Eclipse et Rational Application Developer for WebSphere Software (RAD)», à la page 47.	
Ajouter une application > **Importer depuis un serveur d'applications**	Importe une application Java existante d'un serveur d'applications Apache Tomcat ou WebSphere Application Server Liberty.	

Tableau 22. Menu Fichier (suite)

Option de menu	Description	Raccourci clavier
Ajouter une application > **Applications multiples**	Ajoute plusieurs applications à l'ensemble des applications. Cette action ouvre une boîte de dialogue qui vous permet de spécifier un répertoire dans lequel rechercher des applications. Parmi les résultats de la recherche, vous pouvez sélectionner une ou plusieurs applications à ajouter.	
Ajouter une application > **Reconnaître les applications**	Lance l'Application Discovery Assistant qui permet de créer et de configurer rapidement des applications et des projets pour le code source Java.	
Supprimer une application	Si une application est sélectionnée dans la vue Explorateur, cette action est disponible et le fait de la choisir permet de supprimer l'application sélectionnée.	
Ajouter un projet > **Nouveau projet**	Si une application est sélectionnée dans la vue Explorateur, cette action est disponible et le fait de la choisir permet d'ajouter un nouveau projet à l'application. Cette action lance l'assistant Nouveau projet.	
Ajouter un projet > **Projet existant**	Si une application est sélectionnée dans la vue Explorateur, cette action est disponible et le fait de la choisir permet d'ajouter un projet existant à l'application. Cette action ouvre une boîte de dialogue dans laquelle vous pouvez accéder à un fichier `.ppf`ou `.epf` , ou bien à un répertoire `.xcodeproj`, à ouvrir. **Remarque :** Vous pouvez aussi ouvrir ou importer des fichiers `.pbxproj` en tant que projets AppScan Source.	

Tableau 22. Menu Fichier (suite)

Option de menu	Description	Raccourci clavier
Ajouter un projet > **Copier le projet**	Si un projet est sélectionné dans la vue Explorateur, cette action est disponible et le fait de la choisir ouvre une boîte de dialogue qui permet de copier le projet dans une autre application ou de créer une copie du projet dans l'application où il est actuellement inclus.	
Ajouter un projet > **Projets multiples**	Ajoute plusieurs projets à l'application qui est sélectionnée dans la vue Explorateur. Cette action lance une boîte de dialogue qui vous permet d'exécuter l'une des tâches suivantes : • Spécifier un répertoire dans lequel rechercher les projets. • Spécifier un espace de travail dans lequel rechercher les projets. Parmi les résultats de la recherche, vous pouvez sélectionner un ou plusieurs projets à ajouter.	
Enregistrer	Enregistre l'application ou le projet sélectionné auprès de AppScan Source. Vous devez enregistrer des applications et des projets avant de pouvoir les publier dans la base de données AppScan Source.	
Annuler l'enregistrement	Annule l'enregistrement de l'application ou du projet sélectionné.	
Ouvrir une évaluation	Lance une boîte de dialogue d'ouverture qui vous permet de rechercher un fichier d'évaluation AppScan Source. Les types de fichier pouvant être inclus sont notamment `.ozasmt` et `.xml`.	F7
Fermer l'évaluation	Ferme l'évaluation qui est actuellement ouverte dans la perspective Triage.	
Sauvegarder une évaluation	Sauvegarde dans un fichier l'évaluation ouverte.	Maj+commande+S
Sauvegarder l'évaluation sous	Sauvegarde l'évaluation sous un autre nom, un répertoire différent, ou les deux.	

Tableau 22. Menu Fichier (suite)

Option de menu	Description	Raccourci clavier
Publier l'évaluation dans AppScan Source	Stocke l'évaluation actuelle dans la base de données AppScan Source. L'application qui a été analysée (ou le projet ou fichier que l'application contient) doit être enregistrée avant que l'action de publication puisse être exécutée. Si l'application n'a pas été enregistrée, vous serez invité à le faire lorsque vous choisirez l'action de publication.	
Publier l'évaluation dans AppScan Enterprise Console	Si votre serveur AppScan Enterprise Server a été installé avec l'option Enterprise Console, vous pouvez publier des évaluations sur cette console. Pour pouvoir publier des évaluations sur Enterprise Console, vous devez renseigner la page de préférences AppScan Enterprise Console.	
Sauvegarder	Cette action est disponible dans les conditions suivantes : • Les propriétés d'une application ont été modifiées dans la vue Propriétés. • Les propriétés d'un projet ont été modifiées dans la vue Propriétés. • Un fichier qui est ouvert dans l'éditeur interne a été modifié. Cette action permet de sauvegarder les modifications.	commande+S
Quitter	Quitte AppScan Source for Analysis.	command+Q

Remarque : Pour savoir quelles versions des fichiers importés sont prises en charge par AppScan Source for Analysis, AppScan Source for Automation et l'interface de ligne de commande d'AppScan Source, voir http://www.ibm.com/support/docview.wss?uid=swg27027486. Dans cette page, sélectionnez l'onglet de la version d'AppScan Source que vous utilisez, puis sélectionnez le composant AppScan Source que vous utilisez. Si AppScan Source prend en charge l'ouverture

et l'examen de fichiers provenant d'autres environnements de développement, cette prise en charge est indiquée à la section **Compilateurs et langues** de l'onglet **Logiciels pris en charge**.

Menu Edition

Ce menu propose des contrôles de modification et de recherche/remplacement standard. Il est également utilisé pour les préférences de lancement de produit. Certaines options du menu **Editer** varient selon le contexte, en fonction de la vue active et de l'option actuellement sélectionnée dans cette vue.

Tableau 23. Menu Edition

Option de menu	Description	Raccourci clavier
Couper	Copie et supprime du texte sélectionné. Cette action est utilisée pour du texte qui est sélectionné dans la console, l'éditeur ou différentes zones de texte.	contrôle+X
Copier	Copie le texte sélectionné dans le presse-papiers. Cette action est utilisée pour du texte qui est sélectionné dans la console, l'éditeur ou différentes zones de texte.	contrôle+C
Coller	Colle le texte qui a été copié ou découpé. Cette action est généralement utilisée pour dupliquer des informations et les reproduire dans une autre partie du produit.	contrôle+V
Renommer	Renomme l'élément sélectionné. Les objets qui peuvent être renommés sont des applications, des projets, des évaluations et des groupements.	F2
Supprimer	Supprime l'objet sélectionné.	Supprimer
Sélectionner tout	Sélectionne la totalité du corps de texte. Cette action est utilisée pour du texte contenu dans la console, l'éditeur ou différentes zones de texte.	commande+A
Régénérer	Actualise le contenu d'une application, d'un projet ou d'une vue sélectionné.	F5
Rechercher	Recherche un texte dans la console ou l'éditeur ou recherche des constatations dans un tableau de constatations.	commande+F

Tableau 23. Menu Edition (suite)

Option de menu	Description	Raccourci clavier
Rechercher suivant	Si l'action de recherche a été utilisée pour rechercher du texte dans la console ou l'éditeur, cette action est utilisée pour rechercher l'instance suivante du texte.	F3
Préférences	Cette option permet d'ouvrir la boîte de dialogue Préférences. Les préférences sont les choix personnels de l'utilisateur concernant l'apparence et le fonctionnement de AppScan Source for Analysis.	command+,

Menu Examen

A partir du menu **Examen**, vous gérez les examens d'une application, d'un projet ou d'un fichier sélectionné.

Tableau 24. Menu Examen

Option de menu	Description	Raccourci clavier
Tout examiner	Examine toutes les applications. L'examen s'exécute avec la configuration d'examen par défaut.	
Examiner la sélection	Examine l'application, le projet ou le fichier sélectionné. L'examen s'exécute avec la configuration d'examen par défaut.	F4
Examiner à nouveau	Examine à nouveau les cibles de l'évaluation. C'est la dernière configuration d'examen utilisée pour examiner l'élément (ou les éléments sélectionnés) qui est réutilisée pour cet examen.	
Annuler l'examen	Met fin à l'examen sans générer de résultats.	
Arrêter l'examen	Arrête l'examen en générant des résultats partiels.	

Tableau 24. Menu Examen (suite)

Option de menu	Description	Raccourci clavier
Générer la configuration	Définit les paramètres de génération du projet, tels que les définitions de préprocesseur ou les chemins d'inclusion. Généralement, une configuration intitulée **Release** ou **Debug** accompagne un projet importé. Cette option de menu est désactivée lorsqu'elle n'est pas applicable.	

Menu Outils

Ce menu inclut des options permettant de comparer des évaluations et de générer des rapports et de vérifier les fichiers ou les constatations dans un éditeur. Certaines options du menu **Outils** varient selon le contexte, en fonction de la vue active et de l'option actuellement sélectionnée dans cette vue.

Tableau 25. Menu Outils

Option de menu	Description
Différences entre évaluations	Cette action ouvre une boîte de dialogue qui vous permet de sélectionner deux évaluations à comparer.
Générer un rapport sur les constatations	Génère un rapport sur le contenu des constatations ou du groupement sélectionné. Une vue de constatations ou de groupements doit être sélectionnée avec cette action. Si des constatations ne sont pas sélectionnées dans la vue, le rapport contient toutes les constatations de la vue.
Générer un rapport	Génère un rapport identifiant toutes les constatations basées sur des exigences de conformité ou des consignes spécifiques.
Ouvrir dans l'éditeur interne	Ouvre un fichier à l'aide de l'éditeur AppScan Source for Analysis interne. Utilisée pour une constatation sélectionnée, cette action provoque l'ouverture du fichier qui lui est associé dans l'éditeur.
Ouvrir dans l'éditeur externe	Ouvre un fichier à l'aide d'un éditeur externe. Utilisée pour une constatation sélectionnée, cette action provoque l'ouverture du fichier qui lui est associé dans l'éditeur.

Menu Admin

Le menu **Admin** fournit des actions qui vous permettent de gérer des utilisateurs et de lancer des informations d'audit.

Tableau 26. Menu Admin

Option de menu	Description
Gérer les utilisateurs	Cette action ouvre une boîte de dialogue qui vous permet de créer et d'éditer des utilisateurs et des droits. Vous devez disposer des droits d'administration AppScan Source pour gérer des utilisateurs.
Audit	Cette action lance une vue qui vous permet de visualiser des informations d'audit, telles que des événements d'authentification.

Pour plus de détails sur les tâches d'administration, reportez-vous au document *IBM Security AppScan Source - Guide d'installation et d'administration*.

Menu Vue

Le menu **Vue** contrôle l'affichage de chaque vue ou sélectionne une vue ouverte.

Pour en savoir plus sur les vues disponibles dans AppScan Source for Analysis, voir Vues AppScan Source for Analysis.

Menu Perspective

Le menu **Perspective** contrôle l'affichage des *perspectives* AppScan Source for Analysis qui sont des collectes préconfigurées de vues et d'options.

Tableau 27. Menu Perspective

Option de menu	Description	Raccourci clavier
Configuration	Cette perspective permet de créer et de gérer des applications, des projets et des attributs.	option+1
Triage	Cette perspective permet d'afficher les résultats de l'examen afin d'attribuer des priorités dans le flux de travaux de résolution des vulnérabilités et de séparer les vulnérabilités réelles des potentielles. Cette perspective peut être utilisée pour isoler les problèmes que vous devez résoudre en premier lieu.	option+2
Analyse	Cette perspective permet d'explorer les constatations individuelles et d'afficher le code source, les recommandations de résolution et la trace AppScan Source.	option+3

Tableau 27. Menu Perspective (suite)

Option de menu	Description	Raccourci clavier
Réinitialiser la perspective	Lorsque cette option est sélectionnée, la perspective actuellement affichée est réinitialisée avec ses vues et ses présentations par défaut.	

Menu Aide

Le menu **Aide** comporte des actions qui vous permettent d'ouvrir divers outils destinés à vous aider à utiliser le produit. Il s'agit notamment du message de bienvenue, de l'aide aux utilisateurs en ligne et de la Base de connaissances de sécurité AppScan Source Security.

Tableau 28. Menu Aide

Option de menu	Description
Bienvenue	Cette action ouvre la vue Bienvenue d'AppScan Source for Analysis. Cette vue offre des liens rapides vers diverses ressources d'aide, y compris un flux RSS X-Force.
Contenu de l'aide	Cette action ouvre l'aide aux utilisateurs du produit AppScan Source for Analysis.
Base de connaissances de sécurité	Cette action ouvre la Base de connaissances de sécurité AppScan Source Security. La Base de connaissances fournit des informations instantanées sur chaque vulnérabilité et offre des descriptions précises des causes premières, du niveau de gravité du risque et des recommandations de résolution concrètes.
Journaux	Cette action ouvre la vue Journaux. Dans la vue, des onglets vous permettent de sélectionner le fichier journal à afficher.
A propos deIBM Security AppScan Source for Analysis	Cette action ouvre une boîte de dialogue qui fournit des informations sur le produit AppScan Source for Analysis.

Barres d'outils

Les barres d'outils présentes dans le plan de travail AppScan Source for Analysis fournissent des raccourcis graphiques vers des commandes. Pour identifier une icône de barre d'outils spécifique, arrêtez brièvement la souris au-dessus de cette icône jusqu'à ce qu'une infobulle apparaisse. Les boutons de la barre d'outils représentent des opérations fréquemment utilisées (figurant également dans le menu **principal**). Les opérations disponibles dans la barre d'outils sont dépendantes du contexte.

La barre d'outils principale fournit des liens rapides vers les perspectives AppScan Source for Analysis. En outre, la plupart des vues comportent des barres d'outils qui permettent de lancer rapidement des actions communes relatives à ces vues.

Infobulles

Une infobulle est un type d'aide contextuelle qui s'affiche dans une petite fenêtre en incrustation lorsque vous placez le pointeur de la souris sur un élément de l'interface. Le texte en incrustation contient une brève description de la zone désignée par le pointeur.

Outre les infobulles fournies pour les boutons et les icônes, AppScan Source for Analysis offre également des infobulles dans de nombreux autres endroits, tels que les suivants :

- Dans la vue Explorateur, une infobulle est disponible pour indiquer le nom de fichier et le chemin des applications, des projets et des fichiers. L'infobulle indique également si une application ou un projet est enregistré.
- Dans la vue Trace, le fait de survoler des noeuds de trace dans le graphique permet d'afficher des informations sur ces noeuds.
- Dans la section **Trace** de la vue Editeur de filtre, le fait de survoler une entrée de trace permet d'afficher des informations détaillées sur cette trace.
- Dans la section **Paramètres avancés** de la vue Configuration d'examen, une infobulle est disponible pour chaque paramètre.
- Dans la barre d'état du plan de travail (située au bas du plan de travail), le fait de survoler l'icône de l'utilisateur permet d'afficher l'infobulle identifiant l'utilisateur connecté. Le fait de survoler l'icône du serveur permet d'ouvrir l'infobulle indiquant le serveur Enterprise Server auquel AppScan Source for Analysis est connecté.

Barre d'état

La barre d'état, située au bas du plan de travail, affiche des messages d'information identifiant l'action en cours (par exemple, un examen).

Par exemple, lors d'un examen, la barre d'état peut afficher `Examen en cours de <Nom du projet>`, avec un indicateur de progression. En outre, l'étape en cours de l'examen est affichée, par exemple, `Préparation en cours de l'analyse de vulnérabilité : 99 %`. Une fois l'examen terminé, le temps écoulé est affiché dans la barre d'état.

La barre d'état contient également des informations sur l'utilisateur et la connexion serveur en cours. Le fait de survoler l'icône de l'utilisateur permet d'afficher l'infobulle identifiant l'utilisateur connecté. Le fait de survoler l'icône du serveur permet d'ouvrir l'infobulle indiquant le serveur Enterprise Server auquel AppScan Source for Analysis est connecté.

Chapitre 14. Vues

L'environnement de travail AppScan Source for Analysis est composé de plusieurs perspectives et vues qui contiennent différentes données d'évaluation ou d'examen.

Les vues AppScan Source for Analysis fournissent des présentations alternatives de constatations (certaines d'entre elles prennent en charge l'édition de code) et vous permettent de naviguer parmi les informations de votre plan de travail. La vue Explorateur, par exemple, présente des applications, des projets et d'autres ressources. Une vue peut figurer seule ou être juxtaposée à d'autres dans un bloc-notes à onglets. Vous pouvez modifier la présentation d'une perspective en ouvrant et en fermant les vues et en les verrouillant dans différentes positions au sein de la fenêtre du plan de travail.

Les sections suivantes présentent les vues de manière plus détaillée :

- «Vues de configuration»
- «Vues qui vous aident à traiter les sorties d'examen», à la page 270
- «Vues qui vous aident à effectuer le triage», à la page 273
- «Vues qui permettent d'effectuer des investigations sur une constatation unique», à la page 284
- «Vues qui vous permettent d'utiliser des évaluations», à la page 289
- «Vue Groupements», à la page 291

Vues de configuration

Les vues présentées dans cette section permettent de configurer AppScan Source.

- «Vue Règles personnalisées»
- «Vue Explorateur», à la page 66
- «Vue Bibliothèque de règles de schémas», à la page 255
- «Vue Propriétés», à la page 255
- «Vue Configuration d'examen», à la page 95
- «Editeur de rapport», à la page 193

Vue Règles personnalisées

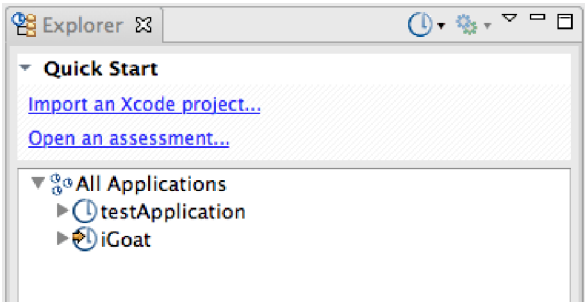
Cette vue permet de créer des règles personnalisée à l'aide de l'assistant Règles personnalisées. Vous pouvez ajouter, afficher ou supprimer des règles existantes.

Pour plus de détails, voir «Création de règles personnalisées», à la page 202.

Vue Explorateur

La vue Explorateur contient une section **Démarrage rapide** dans sa partie supérieure et une section explorateur dans sa partie inférieure, qui contient un noeud, **Toutes les applications**. La section **Démarrage rapide** contient plusieurs liens utiles qui permettent de lancer les actions courantes. La section explorateur se compose d'une sous-fenêtre de navigation qui fournit une vue hiérarchique de vos ressources : applications, projets, répertoires et fichiers de projet, avec **Toutes les applications** comme racine. Vous pouvez naviguer entre ces ressources comme dans un explorateur de fichiers. Lorsque vous naviguez dans l'arborescence, le statut de votre sélection détermine les onglets disponibles dans la vue Propriétés.

Généralités



Depuis la vue Explorateur, vous pouvez ajouter des applications et des projets et examiner leur code à l'aide des boutons de la barre d'outils. Vous trouvez également des liens dans la section **Démarrage rapide**. Une fois les applications ajoutées, la section explorateur fournit des indicateurs visuels relatifs à vos applications et projets, ainsi que le statut de chacun(e).

Conseil : Dans la vue Explorateur, une infobulle est disponible pour indiquer le nom de fichier et le chemin des applications, des projets et des fichiers. L'infobulle indique également si une application ou un projet est enregistré.

Section Démarrage rapide

La section **Démarrage rapide** contient les liens suivants pour le lancement des tâches courantes :

- **Importer un projet ou un espace de travail Xcode** : Lance une boîte de dialogue d'ouverture qui permet de rechercher et d'ajouter un répertoire `.xcodeproj` ou `.xcworkspace` existant en tant qu'application AppScan Source.
- **Importer un espace de travail basé sur Eclipse** : Lance la boîte de dialogue Ajout d'espace de travail qui vous permet d'ajouter un espace de travail Eclipse ou IBM Rational Application Developer for WebSphere Software (RAD) existant qui contient des projets Java. Une fois l'espace de travail importé, vous pouvez examiner n'importe quel projet Java inclus dans cet espace.

  Remarque : Avant d'importer l'espace de travail, assurez-vous d'avoir installé et mis à jour l'environnement de développement comme décrit dans la rubrique «Configuration de l'environnement de développement pour des projets Eclipse et Rational Application Developer for WebSphere Software (RAD)», à la page 47.
- **Importer depuis un serveur d'applications** : Importe une application Java existante d'un serveur d'applications Apache Tomcat ou WebSphere Application Server Liberty.
- **Ouvrir une évaluation** : Lance une boîte de dialogue d'ouverture qui vous permet de rechercher un fichier d'évaluation AppScan Source. Les types de fichier pouvant être inclus sont notamment `.ozasmt` et `.xml`.

Boutons de la barre d'outils

Tableau 29. Boutons de la barre d'outils

Action	Icône	Description
Ajouter un menu d'application		Lorsque vous cliquez sur la flèche vers le bas du bouton **Ajouter un menu d'application**, vous pouvez sélectionner des actions de création d'application, d'ouverture d'une application existante, d'importation d'un espace de travail ou de lancement de l'Application Discovery Assistant.
Examiner la sélection		Le bouton **Examiner la sélection** vous permet d'examiner l'objet sélectionné dans la section explorateur. La configuration d'examen par défaut est utilisée pour l'examen. Pour choisir une autre configuration d'examen à utiliser pour l'examen, cliquez sur la flèche vers le bas du bouton **Examiner la sélection**. Sélectionnez la configuration d'examen que vous souhaitez utiliser ou choisissez l'action **Editer des configurations** pour définir une autre configuration d'examen par défaut (dans la vue Configuration d'examen, sélectionnez la configuration que vous souhaitez définir par défaut et cliquez sur **Sélectionner comme valeur par défaut**).
Menu Vue		Le bouton **Menu Vue** affiche un menu qui vous permet d'actualiser la section explorateur et de masquer les éléments enregistrés.

Options du menu contextuel

La disponibilité des options de menu contextuel varie en fonction de l'élément qui est sélectionné dans la section explorateur.

- Lorsque l'élément **Toutes les applications** est sélectionné dans la section explorateur, les options de menu contextuel suivantes sont disponibles :
  - **Examiner toutes les applications** : Examine toutes les applications. L'examen s'exécute avec la configuration d'examen par défaut.
  - **Examiner toutes les applications avec** : Sélectionnez la configuration d'examen que vous souhaitez utiliser ou choisissez l'action **Editer des configurations** pour définir une autre configuration d'examen par défaut

(dans la vue Configuration d'examen, sélectionnez la configuration que vous souhaitez définir par défaut et cliquez sur **Sélectionner comme valeur par défaut**).

– **Ajouter une application**
  - **Créer une application** : Ajoute une nouvelle application à l'ensemble des applications. Cette action lance l'assistant Nouvelle application.
  - **Ouvrir une application existante** : Lance une boîte de dialogue d'ouverture qui vous permet de rechercher et d'ajouter une application existante à l'ensemble des applications. Les types de fichier ou de répertoire pouvant être ajoutés sont notamment `.paf`,`.xcodeproj`, `.xcworkspace` et `.ewf`.
  - **Importer un espace de travail basé sur Eclipse existant** : Lance la boîte de dialogue Ajout d'espace de travail qui vous permet d'ajouter un espace de travail Eclipse ou IBM Rational Application Developer for WebSphere Software (RAD) existant qui contient des projets Java. Une fois l'espace de travail importé, vous pouvez examiner n'importe quel projet Java inclus dans cet espace.

    Remarque : Avant d'importer l'espace de travail, assurez-vous d'avoir installé et mis à jour l'environnement de développement comme décrit dans la rubrique «Configuration de l'environnement de développement pour des projets Eclipse et Rational Application Developer for WebSphere Software (RAD)», à la page 47.
  - **Reconnaître les applications** : Lance l'Application Discovery Assistant qui permet de créer et de configurer rapidement des applications et des projets pour le code source Java.
– **Développer tout**
– **Réduire tout**
– **Propriétés** : Cette option permet d'ouvrir la vue Propriétés pour l'élément sélectionné.

• Lorsqu'une application est sélectionnée dans la section explorateur, les options de menu contextuel suivantes sont disponibles :
– **Examiner l'application** : Examine l'application, le projet ou le fichier sélectionné. L'examen s'exécute avec la configuration d'examen par défaut.
– **Examiner l'application avec** : Sélectionnez la configuration d'examen que vous souhaitez utiliser ou choisissez l'action **Editer des configurations** pour définir une autre configuration d'examen par défaut (dans la vue Configuration d'examen, sélectionnez la configuration que vous souhaitez définir par défaut et cliquez sur **Sélectionner comme valeur par défaut**).
– **Ajouter un projet**
  - **Nouveau projet** : Si une application est sélectionnée dans la vue Explorateur, cette action est disponible et le fait de la choisir permet d'ajouter un nouveau projet à l'application. Cette action lance l'assistant Nouveau projet.
  - **Projet existant** : Si une application est sélectionnée dans la vue Explorateur, cette action est disponible et le fait de la choisir permet d'ajouter un projet existant à l'application. Cette action ouvre une boîte de dialogue dans laquelle vous pouvez accéder à un fichier `.ppfou .epf` , ou bien à un répertoire `.xcodeproj`, à ouvrir.
  - **Projets multiples** : Ajoute plusieurs projets à l'application qui est sélectionnée dans la vue Explorateur. Cette action lance une boîte de dialogue qui vous permet d'exécuter l'une des tâches suivantes :
    • Spécifier un répertoire dans lequel rechercher les projets.

- Spécifier un espace de travail dans lequel rechercher les projets.

  Parmi les résultats de la recherche, vous pouvez sélectionner un ou plusieurs projets à ajouter.

  - **Supprimer une application** : Si une application est sélectionnée dans la vue Explorateur, cette action est disponible et le fait de la choisir permet de supprimer l'application sélectionnée.
  - **Ajouter une constatation personnalisée** : Cette action ouvre la boîte de dialogue Créer une constatation personnalisée afin de vous permettre de créer une constatation personnalisée pour l'application sélectionnée.
  - **Actualiser** : Actualise le contenu d'une application, d'un projet ou d'une vue sélectionné.
  - Enregistrer/Annuler l'enregistrement :
    - **Enregistrer l'application** : Enregistre l'application ou le projet sélectionné auprès de AppScan Source. Vous devez enregistrer des applications et des projets avant de pouvoir les publier dans la base de données AppScan Source.
    - **Enregistrer l'application comme...** : Cette option permet d'enregistrer à nouveau l'application sous un nouveau nom.
    - **Annuler l'enregistrement de l'application** : Annule l'enregistrement de l'application ou du projet sélectionné.
    - **Localiser** : Cette option permet d'associer une application ou un projet local à une application ou un projet qui a été enregistré par un autre utilisateur AppScan Source.
  - **Développer tout**
  - **Réduire tout**
  - **Propriétés** : Cette option permet d'ouvrir la vue Propriétés pour l'élément sélectionné.
- Lorsqu'un projet est sélectionné dans la section explorateur, les options de menu contextuel suivantes sont disponibles :
  - **Examiner le projet** : Examine l'application, le projet ou le fichier sélectionné. L'examen s'exécute avec la configuration d'examen par défaut.
  - **Examiner le projet avec** : Sélectionnez la configuration d'examen que vous souhaitez utiliser ou choisissez l'action **Editer des configurations** pour définir une autre configuration d'examen par défaut (dans la vue Configuration d'examen, sélectionnez la configuration que vous souhaitez définir par défaut et cliquez sur **Sélectionner comme valeur par défaut**).
  - **Copier le projet** : Si un projet est sélectionné dans la vue Explorateur, cette action est disponible et le fait de la choisir ouvre une boîte de dialogue qui permet de copier le projet dans une autre application ou de créer une copie du projet dans l'application où il est actuellement inclus.
  - **Supprimer le projet** : Supprime l'objet sélectionné.
  - Enregistrer/Annuler l'enregistrement :
    - **Enregistrer le projet** : Enregistre l'application ou le projet sélectionné auprès de AppScan Source. Vous devez enregistrer des applications et des projets avant de pouvoir les publier dans la base de données AppScan Source.
    - **Annuler l'enregistrement du projet** : Annule l'enregistrement de l'application ou du projet sélectionné.
    - **Localiser** : Cette option permet d'associer une application ou un projet local à une application ou un projet qui a été enregistré par un autre utilisateur AppScan Source.

- **Développer tout**
- **Réduire tout**
- **Propriétés** : Cette option permet d'ouvrir la vue Propriétés pour l'élément sélectionné.

- Lorsqu'un fichier est sélectionné dans la section explorateur, les options de menu contextuel suivantes sont disponibles :
  - **Examiner le fichier** : Examine l'application, le projet ou le fichier sélectionné. L'examen s'exécute avec la configuration d'examen par défaut.
  - **Examiner le fichier avec** : Sélectionnez la configuration d'examen que vous souhaitez utiliser ou choisissez l'action **Editer des configurations** pour définir une autre configuration d'examen par défaut (dans la vue Configuration d'examen, sélectionnez la configuration que vous souhaitez définir par défaut et cliquez sur **Sélectionner comme valeur par défaut**).
  - **Exclure des examens** : Permet de supprimer le fichier sélectionné des examens.
  - **Ouvrir dans l'éditeur interne** : Permet d'ouvrir le fichier sélectionné dans l'éditeur AppScan Source (dans la perspective Analyse).
  - **Ouvrir dans l'éditeur externe** : Permet de choisir un éditeur externe dans lequel ouvrir le fichier sélectionné.
  - **Propriétés** : Cette option permet d'ouvrir la vue Propriétés pour l'élément sélectionné.

Indicateurs d'application et de projet

Le tableau ci-après répertorie les icônes d'application et de projet dans la vue Explorateur.

Tableau 30. Icônes d'application et de projet

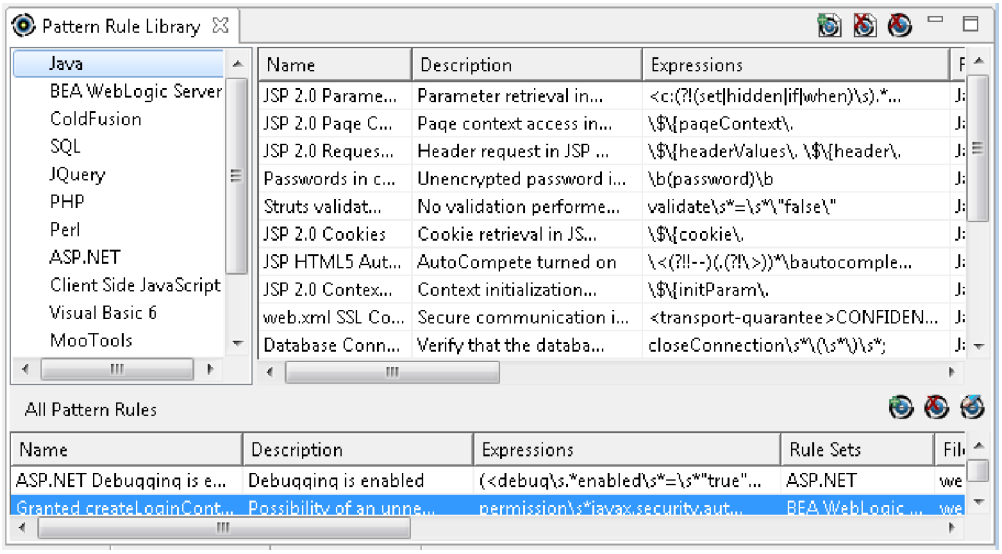
Type d'application ou de projet	Non enregistré	Enregistré	Manquant/ Introuvable
Application importée			
Application qui est créée manuellement ou à l'aide de l'Application Discovery Assistant			
Projet importé			
Projet qui est créé manuellement ou à l'aide de l'Application Discovery Assistant			

La vue Explorateur affiche les applications et projets locaux, ainsi que ceux enregistrés sur le serveur (ceux qui sont enregistrés sur le serveur mais qui ne sont pas enregistrés localement - par exemple, les applications et les projets enregistrés par d'autres utilisateurs - apparaissent grisés). Si vous cliquez sur le bouton **Menu d'affichage** dans la barre d'outils et que vous basculez vers l'option de menu **Masquer les éléments enregistrés sur le serveur** afin qu'il n'y ait pas de sélection, vous pouvez afficher les applications et projets existants sur le serveur. Si un projet est grisé, vous pouvez cliquer dessus avec le bouton droit de la souris et sélectionner dans le menu l'option **Localiser**.

Vue Bibliothèque de règles de schémas

L'examen basé sur des schémas est une analyse de votre code source basée sur des critères de recherche personnalisés. La vue Bibliothèque de règles de schémas permet de visualiser des règles basées sur des schémas existantes, par langage (y compris la bibliothèque de règles de schémas AppScan Source prête à l'emploi). En outre, la vue vous permet d'ajouter des règles et des schémas pour les examens basés sur des schémas.

Après avoir créé une bibliothèque de règles, vous pouvez appliquer l'analyse de schéma à des applications ou projets spécifiques. Voir «Personnalisation à l'aide de règles basées sur des schémas», à la page 209 pour plus d'informations sur la recherche de schémas.



Vue Propriétés

Le contenu de la vue Propriétés varie en fonction de l'élément qui est sélectionné dans la vue Explorateur. Les propriétés s'appliquent selon le cas à toutes les applications, à des applications individuelles, à des projets ou à des fichiers. Les propriétés visibles varient en fonction du langage ou du type de projet sélectionné.

- «Vue Propriétés : Toutes les applications»
- «Vue Propriétés : application sélectionnée», à la page 219
- «Vue Propriétés : projet sélectionné», à la page 220
- «Propriétés de fichier», à la page 263

Vue Propriétés : Toutes les applications

Si vous sélectionnez **Toutes les applications** dans la vue Explorateur, la vue Propriétés affiche les onglets Présentation et Filtres.

Présentation

L'onglet Présentation affiche les attributs globaux. Les *attributs* sont des groupements nommés d'éléments définis par l'utilisateur et dotés de caractéristiques similaires. Vous pouvez ajouter et supprimer des attributs, ainsi que leurs valeurs.

Filtres

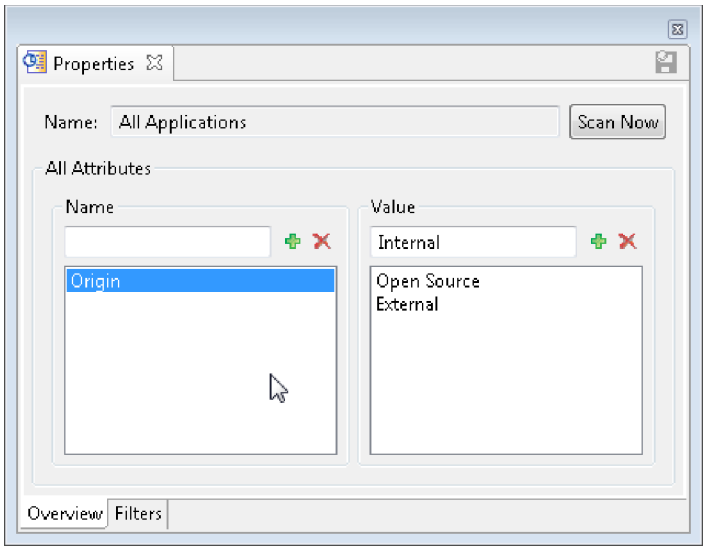
Cet onglet vous permet de spécifier les filtres existants pour toutes les applications, et la façon dont vous souhaitez que les filtres soient appliqués (un filtre peut être appliqué directement ou de manière inversée). Voir Chapitre 5, «Triage et analyse», à la page 117 pour plus d'informations sur les filtres, et «Application globale des filtres», à la page 136 pour plus de détails sur leur application globale.

Les constatations filtrées n'apparaissent pas dans les résultats de l'examen et ne sont pas prises en compte dans les métriques de l'application ou du projet.

Ajout et suppression d'attributs globaux :

Vous devez définir des attributs pour **Toutes les applications** avant de regrouper des attributs pour des applications.

Pourquoi et quand exécuter cette tâche



Pour supprimer un attribut global ou sa valeur, sélectionnez son nom et cliquez sur **Suppression d'attribut**. Le nom ou la valeur n'apparaît plus dans la liste.

Remarque : La suppression d'un attribut n'affecte pas les résultats de l'historique.

Pour ajouter un attribut global et sa valeur, procédez comme suit :

Procédure

1. Sélectionnez **Toutes les applications**.
2. Dans l'onglet Présentation de la vue Propriétés, entrez un nom pour l'attribut.
3. Cliquez sur **Ajouter un attribut**. Le nom de l'attribut apparaît dans leur liste.
4. Sélectionnez le nom de l'attribut.
5. Entrez une **Valeur** pour l'attribut.
6. Cliquez sur **Ajouter une valeur**. La valeur de l'attribut apparaît dans leur liste.

Vue Propriétés : application sélectionnée

Cette vue permet de configurer des attributs pour l'application sélectionnée. Les attributs d'application dépendent des attributs globaux créés auparavant.

Présentation

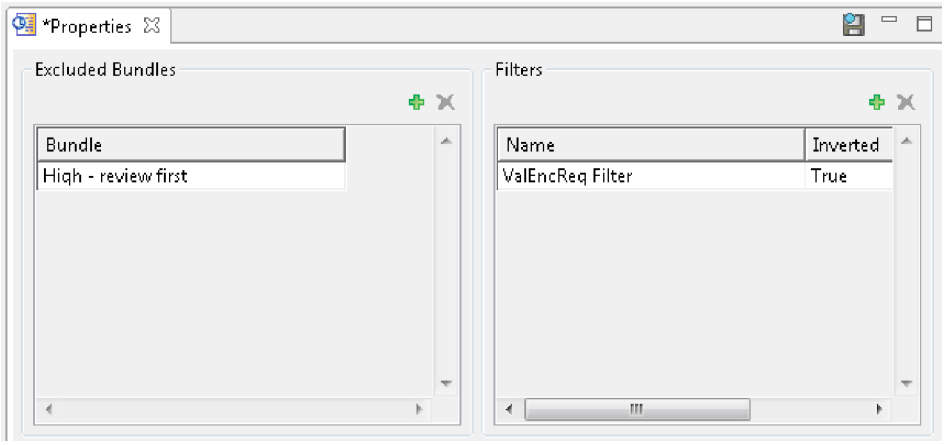
L'onglet Présentation contient les éléments suivants :

- Nom de l'application. L'application peut être renommée en entrant un nouveau nom dans la zone.
- Attributs de l'application

Exclusions et filtres

Cet onglet vous permet de spécifier les filtres existants pour l'application sélectionnés, et la façon dont vous souhaitez que les filtres soient appliqués (un filtre peut être appliqué directement ou de manière inversée). Dans l'onglet, vous pouvez également gérer des groupements qui excluent des résultats de l'examen. Voir Chapitre 5, «Triage et analyse», à la page 117 pour plus d'informations sur les filtres, et «Application globale des filtres», à la page 136 pour plus de détails sur leur application globale.

Les constatations exclues et filtrées n'apparaissent pas dans les résultats de l'examen et ne sont pas prises en compte dans les métriques de l'application ou du projet.



Règles et ensembles de règles

Lorsque vous sélectionnez une application dans la vue Explorateur, l'onglet Règles de schéma et Ensembles de règles de la vue Propriétés vous permet d'ajouter des règles de schéma et des ensembles de règles qui seront appliqués lors de l'examen de l'application. L'examen basé sur des schémas permet de rechercher des schémas de texte que vous désirez voir figurer en tant que constatations. Des règles et des ensembles de règles individuels peuvent être appliqués à la fois aux applications et aux projets. Voir «Personnalisation à l'aide de règles basées sur des schémas», à la page 209 pour plus de détails sur l'analyse basée sur des schémas et «Application de règles et d'ensembles de règles de schémas», à la page 215 pour plus de détails sur l'application de règles et d'ensembles de règles dans la vue Propriétés.

Constatations modifiées

Depuis cet onglet, vous pouvez visualiser, éditer ou supprimer des constatations modifiées auparavant ou modifier une constatation existante. Les *constatations modifiées* désignent des constatations dont le type de vulnérabilité, la gravité, la classification ou les notes ont été changés.

Constatations personnalisées

Depuis cet onglet, vous pouvez visualiser, ajouter, modifier ou supprimer des constatations personnalisées. Pour plus de détails, voir «Constatations personnalisées», à la page 150.

Création d'un attribut d'application :

Procédure

1. Dans l'onglet Présentation, cliquez sur **Ajouter des attributs**.
2. Dans la boîte de dialogue **Attributs globaux**, sélectionnez le nom de l'attribut à appliquer à l'application.
3. Cliquez sur la colonne **Valeur** et sélectionnez la valeur de l'attribut dans la liste.

Vue Propriétés : projet sélectionné

Ce mode de la vue Propriétés permet de configurer des paramètres pour le projet sélectionné. Les attributs de projet dépendent des attributs globaux créés auparavant. Les propriétés varient selon le projet sélectionné.

Onglet Présentation du projet sélectionné

L'onglet Présentation contient les éléments suivants :

- **Nom** du projet. Le projet peut être renommé en entrant un nouveau nom dans la zone.
- Nom et chemin du **fichier** de projet
- **Type du projet**
- Configuration : cette section affiche la configuration cible. Pour les projets Objective-C, elle affiche la configuration cible qui a été sauvegardée dans l'onglet Dépendances de projet. Pour tous les autres types de projet, elle affiche **Par défaut**.
- Option de filtrage : Sélectionnez **Filtrer les constatations contenues dans des sources externes** pour écarter les constatations provenant de fichiers qui ne sont pas des fichiers source du projet analysé. Cette option réduit le bruit pour les projets où les constatations sont signalées dans des fichiers générés par le compilateur ou temporaires.

- Options de mise en cache de l'analyse de vulnérabilités : Si vous affinez votre évaluation d'un codebase en l'examinant par itérations et en ajoutant des règles personnalisées, puis en l'examinant à nouveau sans modifier le code source, vous pouvez réduire considérablement la durée de l'examen en définissant les propriétés du projet de sorte à utiliser un cache d'analyse des vulnérabilités. Pour ce faire, cochez la case **Activer le cache d'analyse de vulnérabilités** dans les propriétés du projet. Un cache d'analyse de vulnérabilités est créé la première fois que vous examinez le projet après avoir coché cette case. Ce cache sera utilisé à chaque examen ultérieur du projet, réduisant ainsi la durée de l'examen.

  Pour vider le cache d'analyse de vulnérabilité, cliquez sur **Vider le cache**. Lors du prochain examen du projet, un examen complet aura lieu et un nouveau cache d'analyse de vulnérabilité sera créé. Vous pouvez envisager de vider le cache si :

  – Le code source du projet a été modifié depuis le dernier examen.
  – Vous avez apporté des modifications à la configuration du projet (par exemple, l'ajout ou la suppression de fichiers source).
  – Vous avez modifié des options de configuration du code. Par exemple, vous pouvez vouloir vider le cache si vous examinez un projet Java et que le chemin de classes a changé ou si vous examinez un projet C ou C++ et que vous avez modifié le chemin `include` ou les définitions de préprocesseur.

  Remarque : Vous pouvez également vider le cache d'analyse de vulnérabilités en cochant la case **Vider le cache** lors de la création de règles personnalisées dans l'assistant Règles personnalisées.
- **Analyse de chaîne** : L'analyse de chaîne surveille les manipulations de chaînes dans les projets Java. Elle assure la détection automatique des routines d'assainissement et de validation. Grâce à cette détection, il est possible de réduire les résultats faussement positifs ou faussement négatifs. Pour activer l'analyse de chaîne, cochez la case **Activer l'analyse de chaîne pour trouver les fonctions permettant de valider et rendre inoffensif**. La case **Appliquer les règles importées à la portée globale** détermine si les routines d'assainissement ou de validation découvertes doivent être appliquées à l'échelle du projet ou au niveau global (à tous les projets).

  Remarque : L'analyse de chaîne peut ralentir l'analyse du code. Il est donc recommandé de ne l'appliquer qu'après un changement de code, puis de la désactiver pour les analyses suivantes. En outre, les routines découvertes doivent être considérées comme des *suggestions* et examinées par les auditeurs. Ces routines peuvent être visualisées dans la vue Règles personnalisées.
- **Codage du fichier** : Le codage de caractères des fichiers dans votre projet doit être défini afin que AppScan Source puisse lire ces fichiers correctement (et, par exemple, afin qu'il puisse les afficher correctement dans la vue Source).

  Remarque : Le codage de fichier par défaut pour les projets AppScan Source est **ISO-8859-1**. Le codage de fichier par défaut peut être modifié sur la page de préférences générales.

Filtres

Cet onglet vous permet de spécifier les filtres existants pour le projet sélectionné, et la façon dont vous souhaitez que les filtres soient appliqués (un filtre peut être appliqué directement ou de manière inversée). Voir Chapitre 5, «Triage et analyse», à la page 117 pour plus d'informations sur les filtres, et «Application globale des filtres», à la page 136 pour plus de détails sur leur application globale.

Règles de schéma et ensembles de règles

Lorsque vous sélectionnez un projet dans la vue Explorateur, l'onglet Règles de schéma et Ensembles de règles de la vue Propriétés vous permet d'ajouter des règles de schéma et des ensembles de règles qui seront appliqués lors de l'examen du projet. L'analyse basée schéma permet de rechercher des schémas de texte que vous désirez voir figurer en tant que constatations. Des règles et des ensembles de règles individuels peuvent être appliqués à la fois aux applications et aux projets. Voir «Personnalisation à l'aide de règles basées sur des schémas», à la page 209 pour plus de détails sur l'analyse basée sur des schémas et «Application de règles et d'ensembles de règles de schémas», à la page 215 pour plus de détails sur l'application de règles et d'ensembles de règles dans la vue Propriétés.

Extensions de fichier

Utilisez cet onglet pour configurer ou ajouter des extensions de fichier valides pour le projet - et pour exclure des fichiers des examens et spécifier des extensions comme fichiers Web.

La section **Extensions de fichier** répertorie les extensions qui ont été définies de manière globale dans la page de préférences «Extensions de fichier de projet», à la page 83 du type de projet en cours (vous pouvez choisir des extensions de fichier pour un type de projet différent en utilisant le menu **Ensemble d'extensions de fichier**). Pour exclure une extension des examens du projet en cours, sélectionnez-la dans la liste et cliquez sur **Exclure une extension**. L'extension apparaît alors dans la section **Extensions exclues** de l'onglet.

Pour ajouter une extension supplémentaire pour le projet, sélectionnez **Ajouter une extension** dans la section **Extensions supplémentaires** et entrez ensuite l'extension du fichier et indiquez si les fichiers ayant cette extension doivent être examinés, considérés comme des fichiers Web ou exclus.

Tableau 31. Paramètres d'extension de fichier

Paramètre	Description	Exemples d'utilisation
Examen ou **Evaluation**	Inclure les fichiers ayant l'extension indiquée dans l'analyse complète.	• Si une extension `.xxx` est créée pour les projets Java et marquée comme **Examen** ou **Evaluation**, les fichiers dotés de cette extension seront compilés et examinés. • Un fichier peut faire partie d'un projet mais ne pas être marqué comme **Examen** ou **Evaluation** s'il ne doit pas être compilé et examiné.

Tableau 31. Paramètres d'extension de fichier (suite)

Paramètre	Description	Exemples d'utilisation
Fichier Web	Marquer les fichiers ayant l'extension indiquée pour la compilation JSP. Ce paramètre autorise AppScan Source à séparer les sources Web des sources non Web.	Si une extension `.yyy` est créée pour les projets Java et marquée comme **Fichier Web**, les fichiers ayant cette extension sont organisés en sources Web dans les projets. Lorsqu'AppScan Source se prépare pour l'analyse, ces fichiers seront précompilés en classes à analyser.
Exclure	Ne pas créer de fichiers source dans le projet pour des fichiers ayant l'extension indiquée. Les fichiers ayant cette extension ne seront pas examinés.	Créez une extension `.zzz` pour les fichiers qui sont nécessaires à vos projets pour la compilation, mais qui ne doivent pas être inclus dans l'analyse.

Sources

Spécifiez les sources à inclure dans l'examen.

- Répertoire de travail : Emplacement du fichier de projet AppScan Source (`ppf`) qui constitue la base de tous les chemins relatifs.
- **Ajouter une racine source** et **Supprimer une racine source** : L'onglet Sources affiche les propriétés définies pour le projet à partir de l'assistant Configuration de projet ou dans le `ppf` importé.

  L'option **Supprimer la racine source** est uniquement disponible si l'icône **Racine source** est sélectionnée. Elle permet de supprimer le répertoire racine de code source.
- Rechercher des racines source (projets Java uniquement) : Permet à AppScan Source for Analysis d'identifier automatiquement les racines source valides.
- Les fichiers de projet sont affichés sous l'icône **Racine source**. Les fichiers qui sont exclus de l'examen sont accompagnés d'une icône de fichier rouge (si vous faites un clic droit sur un fichier exclus, l'option **Exclure** de son menu est désactivée et l'option **Inclure** est activée). Pour exclure un fichier inclus, faites un clic droit dessus et sélectionnez **Exclure** dans le menu. Pour inclure un fichier exclus, faites un clic droit dessus et sélectionnez **Inclure** dans le menu.

Dépendances de projet JSP (JavaServer Page)

Cet onglet affiche les propriétés définies pour le projet JSP sélectionné.

- Contient un contenu Web (JSP) : Indique si le projet est une application Web contenant des pages JavaServer Pages.
- Racine de contexte Web : Fichier `WAR` ou répertoire hébergeant le répertoire `WEB-INF`. La racine de contexte Web doit être la racine d'une application Web valide.
- Compilateur JSP : Prêt à l'emploi, Tomcat 7 est le compilateur JSP sélectionné par défaut (il est possible d'en changer sur la page de préférences Java et JSP). Pour en savoir plus sur les compilateurs pris en charge par AppScan Source, voir http://www.ibm.com/support/docview.wss?uid=swg27027486.

  Les versions d'Apache Tomcat versions 7 et 8 sont incluses dans l'installation d'AppScan Source. Si les pages de préférences **Tomcat 7** et **Tomcat 8** ne sont pas

configurées, AppScan Source compile les fichiers JSP à l'aide du compilateur JSP Tomcat fourni et indiqué comme valeur par défaut. Si vous souhaitez employer un compilateur Tomcat externe pris en charge, utilisez les pages de préférences Tomcat pour pointer sur votre installation Tomcat locale.

Si vous utilisez Oracle WebLogic Server ou WebSphere Application Server, vous devez configurer la page de préférences correspondante, le but étant de désigner votre installation locale du serveur d'applications afin qu'elle puisse être utilisée pour la compilation du code JSP durant l'analyse. Si vous n'avez pas encore terminé cette configuration, un message vous demandera de la faire lorsque vous sélectionnerez le compilateur JSP. Si vous répondez **Oui** au message, la page de préférences appropriée s'affiche. Si vous répondez **Non**, un lien d'avertissement s'affiche à côté de la sélection du compilateur JSP (ce lien permet d'ouvrir la page de préférences).

Dépendances de projet

Cet onglet présente les propriétés du projet. Les paramètres de configuration qui figurent dans cet onglet varient selon le langage. Exemple :

- Les paramètres du JDK sont propres à Java.
- La configuration cible est disponible pour les projets Objective-C seulement.

Remarque : Dans l'onglet Dépendances de projet d'un projet Objective-C, la section **Configuration cible** seulement peut être éditée. Toutes les autres sections de l'onglet sont accessibles en lecture seule.

Compilation

- Options : Paramètres de compilation requis supplémentaires pour la configuration du projet.
- Utiliser le kit JDK : Identifiez le kit JDK utilisé pour la compilation du projet et configuré dans les préférences. Voir Chapitre 3, «Préférences», à la page 73.

  Les projets Java peuvent se référer à un emplacement de kit JDK (Java Development Kit) local. Lorsque les projets sont transférés au serveur, le chemin du kit JDK peut ne plus être valide. Pour transférer des projets locaux au serveur, vous devez identifier le chemin JDK par défaut pour chaque projet spécifiant nominativement un kit JDK.

  Remarque : Prêt à l'emploi, le compilateur par défaut des projets JSP est Tomcat 7, qui requiert Java version 1.6 ou version ultérieure. Si **Tomcat 7** est conservé par défaut et que vous sélectionnez un JDK plus ancien, des erreurs de compilation seront générées pendant les examens.
- Valider : L'option **Valider** garantit que les dépendances du projet soient correctement configurées. Elle vérifie l'absence dans les projets Java de conflits de configuration entre les sources et le chemin de classes et vérifie également l'absence d'erreurs de compilation. **Un conflit existe** si une classe du chemin de classes est dupliquée dans une racine source. (En cas de conflit, modifiez le chemin de classes en supprimant celle en conflit).

  Après la vérification de l'absence de conflits, l'option **Valider** détermine si le projet peut être compilé et rend compte des erreurs de compilation éventuelles.

Optimisations

- **Classes précompilées** : Utilise des fichiers de classes Java ou JSP précompilées au lieu de la compilation pendant l'examen. Lorsque cette option est sélectionnée, celles de zone de préparation de la source sont désactivées.

- Déployer pour pré-traitement les fichiers source pour minimiser les effets d'erreur de compilation : Détermine si AppScan Source doit copier les sources vers le répertoire de préparation.

  Corriger pour les packages non conformes à la structure de répertoire requiert Java Compile pour ouvrir chaque fichier source.

  Nettoyer la zone de préparation entre chaque examen améliore les performances entre les examens.

Propriétés de fichier

Les propriétés de fichier sont similaires aux dépendances de projet couramment configurées pour les applications C/C++.

Inclure les données de configuration du projet : Inclut les données de configuration du projet dans la configuration du fichier. La configuration du fichier consiste alors de la configuration cumulée du projet et du fichier. La configuration du fichier supplante la configuration du projet.

Vue Configuration d'examen

La vue Configuration d'examen vous permet de créer des configurations que vous pouvez ensuite utiliser lors du lancement des examens. Vous pouvez aussi utiliser cette vue pour définir une configuration d'examen par défaut. Dans une configuration d'examen, vous pouvez spécifier les règles source à utiliser lors de l'examen et inclure de nombreux paramètres d'examen. Les paramètres définis dans une configuration d'examen permettent souvent d'obtenir de meilleurs résultats d'examen et la sauvegarde de ces paramètres peut faciliter l'examen et le rendre plus efficace et plus performant.

La vue Configuration d'examen comporte les sections principales suivantes :

- «Gestion de la configuration d'examen», à la page 96
- «Onglet Général», à la page 96
- «Onglet Analyse de flux corrompus», à la page 97
- «Onglet Analyse de schéma», à la page 98

Gestion de la configuration d'examen

Cette section permet de sélectionner, d'ajouter, de supprimer, de sauvegarder et de partager des configurations d'examen, ainsi que de définir des configurations d'examen par défaut.

- Pour créer une configuration d'examen, cliquez sur **Nouveau**. Une fois les paramètres de configuration d'examen définis, cliquez sur **Sauvegarde** pour enregistrer les modifications. Pour définir la configuration d'examen comme configuration par défaut, cliquez sur **Sélectionner comme valeur par défaut** après l'avoir sauvegardée. Pour connaître la façon dont est utilisée la configuration par défaut, voir «Analyse du code source», à la page 85.
- Pour utiliser une configuration d'examen existante, sélectionnez-la dans la liste :
  - Si vous modifiez les paramètres de configuration d'examen, cliquez sur **Sauvegarde** pour enregistrer les modifications (les modifications non souhaitées peuvent être supprimées en basculant vers une autre configuration d'examen et en cliquant sur **Supprimer**).
  - Pour supprimer la configuration d'examen sélectionnée, cliquez sur **Supprimer**.

- Pour dupliquer la configuration d'examen, cliquez sur **Dupliquer**. Une configuration d'examen est alors créée en fonction des paramètres de la configuration d'examen d'origine.
- Pour définir la configuration d'examen comme configuration par défaut, cliquez sur **Sélectionner comme valeur par défaut**. Pour connaître la façon dont est utilisée la configuration par défaut, voir «Analyse du code source», à la page 85.
- Pour partager une configuration d'examen avec d'autres, cliquez sur **Partager**. Cette opération sauvegarde la configuration d'examen sur le serveur base de données AppScan Source.

  Remarque : Pour partager des configurations d'examen ou modifier ou supprimer une configuration d'examen partagée, vous devez disposer de l'autorisation **Gérer les configurations partagées**. Pour plus d'informations sur la définition des autorisations, voir le manuel *IBM Security AppScan Source - Guide d'installation et d'administration*.

Remarque : AppScan Source fournit des configurations d'examen intégrées. Elles ne peuvent être ni modifiées ni supprimées. Lorsque vous les sélectionnez dans la liste, vous pouvez les dupliquer ou afficher leurs paramètres.

Onglet Général

Informations de base

Cette section vous permet de nommer des configurations d'examen et de fournir une description pour chacune.

Filtres

Dans cette section, vous pouvez choisir un ou plusieurs filtres à appliquer à l'examen à chaque utilisation de la configuration d'examen. Lors de la sélection d'un filtre, vous pouvez choisir un filtre prédéfini par AppScan Source ou un filtre partagé ou un que vous avez créé. Voir «Gestion des configurations d'examen», à la page 90 pour plus de détails.

Onglet Analyse de flux corrompus

Analyse de flux corrompus

Activez et définissez la portée de l'analyse de flux corrompus.

Règles d'examen

Cette section permet de déterminer les règles source utilisées pour l'examen.

Une source est une entrée du programme, telle qu'un fichier, une requête de servlet, une saisie depuis la console ou un socket. En excluant certaines règles source, vous pouvez accélérer l'examen et éviter la détection des vulnérabilités provenant des entrées sans intérêt.

Les règles sont balisées à l'aide de propriétés de règle qui indiquent qu'elles sont liées à une vulnérabilité, un mécanisme, un attribut ou une technologie spécifique. Ces propriétés sont regroupées en ensembles de règles qui correspondent à un

ensemble commun de règles connexes. Vous pouvez limiter les règles source incluses dans l'examen en spécifiant des ensembles de règles ou des propriétés de règles individuelles.

- Sélectionnez un ou plusieurs types de vulnérabilité (les vulnérabilités sont organisées par type dans les ensembles de règles) à inclure dans l'examen :
  - **Tout** : si cette option est sélectionnée, les vulnérabilités provenant de toutes les sources d'entrée prises en charge seront détectées.
  - **Entrée utilisateur** : si cette option est sélectionnée, les vulnérabilités provenant des entrées de l'utilisateur final seront détectées.
  - **Applications Web** : si cette option est sélectionnée, les vulnérabilités provenant des risques des applications Web seront détectées.
  - **Consignation et traitement des erreurs** : si cette option est sélectionnée, les vulnérabilités provenant de la consignation et du traitement des erreurs seront détectées.
  - **Environnement** : si cette option est sélectionnée, les vulnérabilités provenant des fichiers de configuration, des fichiers d'environnement système et des fichiers de propriété seront détectées.
  - **Systèmes externes** : si cette option est sélectionnée, les vulnérabilités provenant des entités externes seront détectées.
  - **Magasin de données** : si cette option est sélectionnée, les vulnérabilités provenant des magasins de données (tels que les bases de données et les caches) seront détectées.
  - **Données inhabituelles** : si cette option est sélectionnée, les vulnérabilités provenant des routines qui ne font normalement pas partie d'une application de production seront détectées.
  - **Système de fichiers** : si cette option est sélectionnée, les vulnérabilités provenant des systèmes de fichiers seront détectées.
  - **Données sensibles** : si cette option est sélectionnée, les vulnérabilités provenant des données sensibles seront détectées.

  Une infobulle décrit chaque ensemble de règles de cette section.
- Sélectionnez les propriétés de règles d'examen individuelles à inclure dans l'examen : cliquez sur **Annuler les ensembles de règles sélectionnés et me laisser sélectionner des propriétés de règles individuelles**. Ceci a pour effet d'ouvrir la boîte de dialogue Sélection des propriétés de règle qui permet de sélectionner des propriétés de règles individuelles. Si cette boîte de dialogue est renseignée, les ensembles de règles sélectionnés sont annulés. Les règles d'examen qui possèdent les propriétés de règle sélectionnées seront utilisées pour l'examen.

Paramètres avancés

Cette section est uniquement destinée aux utilisateurs avancés. Elle contient un certain nombre de paramètres qui peuvent améliorer les résultats d'examen. Une infobulle décrit chaque paramètre de cette section.

Onglet Analyse de schéma

analyse de schéma

Utilisez cette section pour activer l'examen basé sur des schémas lors de l'utilisation de la configuration d'examen. L'examen basé sur des schémas est un examen de votre code source basée sur des critères de recherche personnalisés.

Ensembles de règles de schémas et **Règles de schéma**

Utilisez ces sections pour ajouter des règles et des ensembles de règles à utiliser lors de l'analyse de schéma. Pour plus d'informations, voir «Personnalisation à l'aide de règles basées sur des schémas», à la page 209 et «Gestion des configurations d'examen», à la page 90.

Editeur de rapport

L'éditeur de rapport permet de modifier des rapports ou des modèles personnalisés ou de créer un nouveau rapport. Les rapports personnalisés incluent des éléments disponibles dans un rapport sur les constatations, comme les informations sur les constatations, les fragments de code, la trace AppScan Source et le contenu de la résolution, ainsi qu'une matrice de vulnérabilités. Avant de commencer à concevoir de nouveaux rapports, il est recommandé de vous familiariser avec le processus de création de rapports en modifiant un modèle de rapport existant dans l'éditeur de rapport.

L'éditeur de rapport se compose des onglets Agencement du rapport, Catégories et Aperçu.

- **Agencement du rapport** : permet de concevoir l'apparence du rapport. Dans cet agencement, vous pouvez ajouter, retirer et réorganiser les éléments du rapport AppScan Source.
- **Catégories** : permet de créer et de modifier des catégories. Une *catégorie* est un groupe de constatations. La catégorie indique les constatations à inclure dans le rapport, comment les grouper et l'ordre de ce groupement.
- **Aperçu** : permet de visualiser en cours d'édition le rapport pour l'évaluation actuelle.

Les trois onglets comportent des zones communes :

- **Fichier** : chemin du fichier de groupement sauvegardé (en lecture seule). Rien n'apparaît dans cette zone tant que le fichier n'est pas sauvegardé. Une fois sauvegardé, le fichier de groupement est un fichier XML qui définit le rapport.
- **Nom** : Nom du rapport défini par l'utilisateur.

Les boutons de la barre d'outils destinées à la sauvegarde, l'ouverture, le création, la copie et la génération de rapports personnalisés incluent :

- **Créer un nouveau rapport** : crée un rapport personnalisé
- **Nouveau rapport à partir d'un rapport existant** : crée un rapport personnalisé à partir d'un modèle de rapport existant
- **Ouvrir un rapport sauvegardé** : ouvre un fichier de groupement pour son édition
- **Sauvegarder** : sauvegarde le rapport en cours dans le fichier spécifié
- **Sauvegarder sous** : sauvegarde le rapport en cours dans un nouveau fichier
- **Générer une instance de ce rapport** : crée une copie du rapport pour l'évaluation actuellement ouverte

Conseil : Pour afficher des exemples de rapports existants, cliquez sur **Nouveau rapport à partir d'un rapport existant** et choisissez l'un des modèles de rapport AppScan Source. Vous aurez un aperçu de la manière dont les rapports sont conçus en explorant les onglets Agencement du rapport et Catégories.

Onglet Agencement du rapport

L'onglet Agencement du rapport comporte les sections Palette et Présentation et des sections qui permettent de spécifier un en-tête ou un pied de page qui apparaît sur chaque page.

En-tête et pied de page

La zone **En-tête de la page** permet de spécifier le texte qui apparaît en haut de la chaque page de rapport, tandis que la zone **Pied de page** permet de spécifier le texte qui apparaît au bas de chaque page.

Palette

La palette affiche une liste des éléments constitutifs des rapports AppScan Source standard. Certains éléments affichent uniquement des informations pour des catégories qui ont été définies dans l'onglet Catégories (voir tableau 17, à la page 195).

Tableau 32. Palette d'agencement du rapport - éléments qui ne dépendent pas des catégories

Elément de rapport	Description
En-tête	Ajoute un bloc de texte en gras à l'agencement du rapport.
Image d'en-tête	Affiche une image aux dimensions spécifiées en pixels.
En-tête AppScan Source	En-tête de rapport contenant la marque AppScan Source.
Titre et date	Titre du rapport qui inclut le nom de l'élément ayant été examiné, ainsi que la date de l'examen et la date de génération du rapport.
Bloc de texte	Texte quelconque défini par l'utilisateur. Un en-tête peut également être ajouté pour le bloc de texte dans la zone **Libellé**.
Matrice de vulnérabilités	Matrice de vulnérabilités de l'évaluation (affiche le même graphique que celui qui apparaît dans la vue Matrice de vulnérabilité).
Métriques	Identifie le nombre total de packages, de classes, de méthodes et de lignes de code dans tous les packages du projet.
Historique des examens	Métriques pour l'examen en cours et métriques historiques des examens de la même cible.

Tableau 33. Palette d'agencement du rapport - éléments qui dépendent des catégories

Elément de rapport	Description
Carte de rapport	Décomposition succincte des niveaux de vulnérabilité de chaque catégorie définie dans l'onglet Catégories. Contient des liens vers les détails du rapport et des indicateurs de gravité récapitulant la section.

Tableau 33. Palette d'agencement du rapport - éléments qui dépendent des catégories (suite)

Elément de rapport	Description
Décomposition des vulnérabilités	Tableau décomposant les vulnérabilités dans toutes les catégories définies dans l'onglet Catégories, par gravité et classification.
Carte de rapport partielle	Décomposition des niveaux de vulnérabilité des catégories spécifiées par l'utilisateur comme indiqué dans l'onglet Catégories.
catégories	Répertorie toutes les données de constatations des catégories spécifiées dans l'onglet Catégories.
Catégorie	Répertorie toutes les constatations dans une ou plusieurs catégories qui ont été définies dans l'onglet Catégories.

Présentation

Lorsque vous ajoutez des éléments à partir de la palette, ceux-ci apparaissent dans l'agencement. Utilisez la barre d'outils de section pour supprimer, modifier ou déplacer des éléments dans l'agencement.

Onglet Catégories

Dans l'onglet Catégories, vous pouvez ajouter des catégories qui contiennent les constatations basées sur les groupements, les propriétés ou les constatations sélectionnées choisis. Les catégories peuvent ensuite être utilisées lors de l'ajout de certains éléments à l'agencement. Par exemple, lorsque vous ajoutez une décomposition de vulnérabilité, un tableau décomposant les vulnérabilités dans toutes les catégories (par gravité et classification) est ajouté à l'agencement. Cet onglet est constitué d'un volet contenant une arborescence des catégories et d'un volet permettant l'édition des attributs de la catégorie sélectionnée. Chaque catégorie contient les constatations de l'évaluation qui répondent aux diverses exigences que vous avez définies.

Les catégories disponibles sont les suivantes :

- Groupement : cette catégorie contient une liste de noms de groupements. Toutes les constatations d'un groupement dont le nom figure dans la liste apparaissent dans cette catégorie. Bien que vous sélectionniez des groupements depuis l'évaluation en cours, vous pouvez appliquer la catégorie du groupement à n'importe quelle évaluation puisque les groupements sont appariés par nom.
- Constatations individuelles : sélectionnez des constatations spécifiques à ajouter à la catégorie. Seul un instantané de la constatation est ajouté au rapport. Si vous modifiez la constatation après son ajout au rapport, celui-ci ne reflète pas les modifications.
- Propriétés de types de vulnérabilité, de mécanismes et de technologies : sélectionnez des propriétés et des ensembles de propriétés requis à partir des API dans la Base de connaissances de sécurité AppScan Source Security. Si une constatation contient au moins une des **Propriétés** et toutes les **Propriétés requises**, elle est incluse dans le rapport.

Ce tableau identifie les volets de catégorie et les éléments composant le volet.

Tableau 34. Attributs de l'onglet Catégories

Attribut	Description	Procédure d'édition
Libellé	Nom court de la catégorie, comme Dépassement de mémoire tampon. Le libellé identifie la catégorie dans la liste arborescente des catégories et il est utilisé comme en-tête dans le rapport personnalisé.	Entrez un libellé sur une seule ligne de la zone de texte.
Récapitulatif	Ossature d'une phrase indiquant combien de constatations figurent dans cette catégorie. Leur compte effectif remplace `%FindingCount%` lors de la génération du rapport.	Entrez une brève description de la catégorie et cliquez sur **Ajouter un comptage** afin de placer la variable `%FindingCount%` à l'emplacement du curseur dans la phrase.
Texte	Brève description de la catégorie.	Entrez un texte décrivant la catégorie.
Propriétés (catégories Propriété uniquement)	Les constatations comportant au moins l'une de ces propriétés seront incluses dans cette catégorie. Si une constatation ne comporte pas toutes les propriétés requises listées, cette constatation n'est pas incluse dans cette catégorie.	Dans la barre d'outils, cliquez sur **Ajouter** et sélectionnez une propriété dans la boîte de dialogue Ajout de propriétés. Cliquez sur **Supprimer** pour supprimer les éléments sélectionnés de la liste.
Propriétés requises (catégories Propriété uniquement)	Les constatations contenant toutes les propriétés requises et au moins l'une des propriétés apparaissent dans le rapport sous cette catégorie.	Dans la barre d'outils, cliquez sur **Ajouter** et sélectionnez une propriété dans la boîte de dialogue Ajout de propriétés. Cliquez sur **Supprimer** pour supprimer les éléments sélectionnés de la liste.
Groupements (catégories Groupement uniquement)	Spécifie le nom des groupements à inclure dans cette catégorie.	Cliquez sur **Ajouter un groupement** dans la section Groupements et sélectionnez les groupements dans la liste.

Tableau 34. Attributs de l'onglet Catégories (suite)

Attribut	Description	Procédure d'édition
Constatations (catégories Constatations uniquement)	Spécifie les constatations à inclure dans cette catégorie.	Sélectionnez les constatations dans un tableau de constatations et cliquez ensuite sur **Ajouter des constatations** dans la barre d'outils du tableau pour ajouter les constatations sélectionnées. Si plusieurs vues contiennent les constatations sélectionnées, vous êtes invité à sélectionner celle qui contient celles que vous voulez ajouter. Vous pouvez également faire glisser les constatations d'un tableau des constatations vers le tableau dans la vue Editeur de rapport ou directement vers une catégorie de constatations existantes dans l'arborescence de catégories.

Onglet Aperçu

Vous pouvez afficher un aperçu des rapports AppScan Source for Analysis lorsque vous éditez vos modèles. Depuis le panneau Aperçu, cliquez sur **Aperçu** pour afficher le rapport sur l'évaluation ouverte.

Vues qui vous aident à traiter les sorties d'examen

Les vues présentées dans cette section permettent d'afficher et de gérer les sorties d'examen.

- «Vue Console»
- «Vue Métriques», à la page 271
- «Vue Mes évaluations», à la page 271
- «Vue Evaluations publiées», à la page 272

Vue Console

La vue Console affiche la sortie de l'examen actuel, notamment les informations de statut, le texte de la sortie et les messages d'erreur. Cette vue peut être composée de deux consoles, une pour l'examen en cours et une autre pour l'examen terminé.

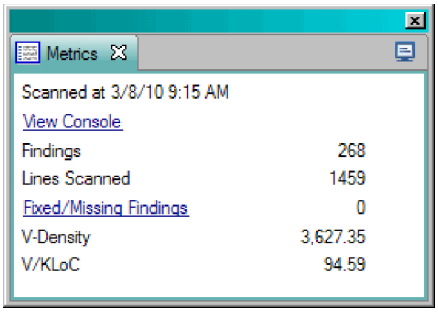
Une console de sortie affiche la sortie complète de l'examen, y-compris les fichiers examinés, le nombre total de fichiers examinés, de vulnérabilités détectées, l'heure de l'examen et la densité des vulnérabilités.

Les boutons de la barre d'outils permettent de manipuler la sortie de la console.

Une console d'erreurs affiche les messages d'erreur de la sortie et le nombre d'erreurs survenues lors de l'examen. Le nombre des erreurs est mis à jour au fur et à mesure de l'examen.

Vue Métriques

Cette vue présente des statistiques basées sur une évaluation et inclut le nombre de lignes de code analysées, la nombre total de constatations, la densité des vulnérabilités et V/KLoC.



Vue Console

Hyperlien ouvrant la vue Console pour consulter la sortie de l'examen actuel.

Constatations

Nombre de constatations identifiées par l'examen.

Lignes examinées

Nombre de lignes de code examinées.

Constatations corrigées/manquantes

Nombre d'éléments contenus dans les groupements de l'application mais non détectés dans cet examen.

Densité V

Expression numérique permettant une évaluation cohérente de la vulnérabilité de vos applications. Cette densité est calculée en rapportant le nombre et la criticité des constatations à la taille de l'application ou du projet qui sont analysés.

V/KLoC

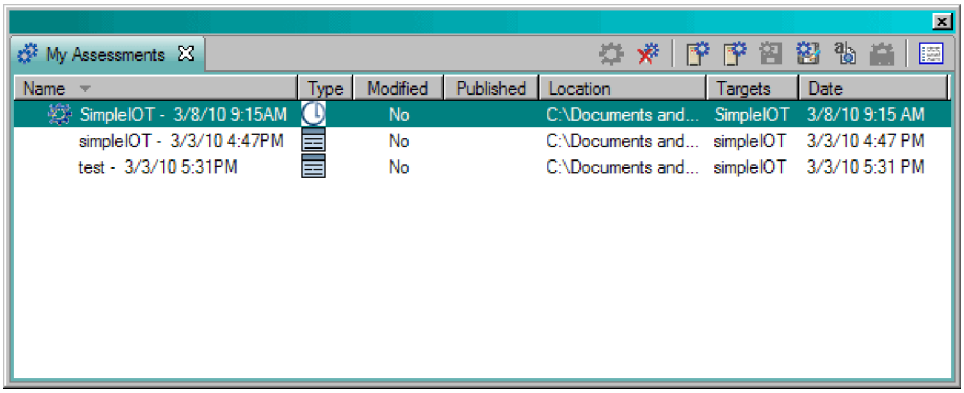
Vulnérabilités détectées par millier de lignes de code.

Vue Mes évaluations

La vue Mes évaluations contient une liste d'évaluations (évaluation actuellement ouverte, ainsi que les évaluations que vous avez enregistrées). Si le jeu d'évaluations en cours est modifié (par exemple, si vous ajoutez ou modifiez une évaluation), un astérisque est placé à côté du titre de la vue pour indiquer que le jeu en cours contient des modifications qui n'ont pas été enregistrées.

- **Nom** : nom de l'évaluation.
- **Type** : icône indiquant si l'examen a porté sur des applications ( ), des projets ( ) ou des fichiers ( ). Une étoile placée à côté du nom de l'évaluation indique qu'elle est ouverte.
- **Configuration d'examen** : configuration d'examen utilisée pour l'examen.

- **Modifiée** : La mention **Oui** ou **Non** indique l'état de modification de l'évaluation.
- **Publiée** : Indique que les évaluations sont publiées dans la base de données AppScan Source.
- **Emplacement** : Chemin du fichier d'évaluation (`<nom_fichier>.ozasmt`).
- **Cibles** : Applications, projets ou fichiers analysés.
- **Date** : Date d'achèvement de l'examen.



A l'issue de l'examen, celles-ci apparaissent automatiquement dans la vue Mes évaluations. Les évaluations visibles dans cette vue comprennent les examens effectués depuis cet ordinateur et ceux que vous avez ajoutés.

Depuis cette vue, vous pouvez ouvrir, ajouter, supprimer, publier, sauvegarder, renommer ou comparer des évaluations. Le retrait d'une évaluation de cette vue sans la sauvegarder ou la publier la supprime définitivement. Notez que chaque évaluation sauvegardée inclut tous les résultats, sa sortie et les journaux d'erreurs. Voir «Sauvegarde des évaluations», à la page 112 pour plus d'informations sur la sauvegarde et la publication d'évaluations.

Voir «Comparaison de deux évaluations dans la vue Différences entre les évaluations», à la page 150 pour plus d'informations sur la comparaison d'évaluations.

Conseil : Une préférence au niveau **Général** détermine le nombre maximal d'évaluations à afficher dans les vues Evaluations publiées et Mes évaluations.

Vue Evaluations publiées

La vue Evaluations publiées répertorie les évaluations qui ont été publiées dans la base de données AppScan Source.

- **Nom** : nom de l'évaluation.
- **Type** : icône indiquant si l'examen a porté sur des applications ( ), des projets ( ) ou des fichiers ( ). Une étoile placée à côté du nom de l'évaluation indique qu'elle est ouverte.
- **Configuration d'examen** : configuration d'examen utilisée pour l'examen.
- **Publiée par** : Nom de l'utilisateur ayant publié l'évaluation
- **Cibles** : Applications, projets ou fichiers analysés.
- **Date** : Date d'achèvement de l'examen.

Depuis la vue Evaluations publiées, vous pouvez :

- Ajouter des évaluations à la vue Mes évaluations

- Filtrer des évaluations
- Ouvrir et supprimer des évaluations
- Fermer des évaluations
- Comparer des évaluations
- Sauvegarder des évaluations
- Renommer des évaluations
- Visualiser des métriques

Conseil : Une préférence au niveau **Général** détermine le nombre maximal d'évaluations à afficher dans les vues Evaluations publiées et Mes évaluations.

Vues qui vous aident à effectuer le triage

Les vues présentées dans cette section permettent d'afficher et de gérer les sorties d'examen avec une granularité fine.

- «Vue Différences entre les évaluations»
- «Vue Constatations personnalisées», à la page 274
- «Vue Constatations exclues», à la page 279
- «Vue Constatations», à la page 277
- «Vue Constatations corrigées/manquantes», à la page 280
- «Vue Constatations modifiées», à la page 279
- «Vue Résultats de la recherche», à la page 280
- «Vue Rapport», à la page 280
- «Vue Sources et collecteurs», à la page 283

Vue Différences entre les évaluations

La vue Différences entre les évaluations représente une combinaison des vues Mes évaluations et Constatations. Lorsque vous sélectionnez deux évaluations pour les comparer, les différences entre les deux évaluations sont affichées.

Cette vue présente le nombre total de constatations nouvelles, corrigées/manquantes, et communes.

- Les constatations communes sont celles figurant dans les deux évaluations
- Les constatations nouvelles sont celles figurant uniquement dans l'évaluation la plus récente (signalées en bleu)
- Les constatations corrigées/manquantes sont celles figurant uniquement dans l'évaluation la plus ancienne (signalées en vert et en italiques)

Le panneau de droite présente les constatations. Cliquez avec le bouton droit de la souris sur une constatation pour :

- Générer un rapport sur les constatations
- Soumettre les constatations en tant que défauts
- L'ouvrir dans un éditeur externe
- L'ouvrir dans l'éditeur interne

Le panneau de gauche liste les évaluations à comparer.

Remarque : La vue Différences entre les évaluations ne tient pas compte des filtres.

Vue Constatations personnalisées

Cette vue affiche les constatations définies par l'utilisateur, ou encore *constatations personnalisées*, existant dans l'évaluation ouverte actuellement. Depuis cette vue, vous pouvez créer, supprimer ou modifier des constatations personnalisées pour l'évaluation en cours. Lorsqu'une constatation personnalisée est créée dans cette vue, la nouvelle constatation est ajoutée à l'évaluation en cours et ses métriques actualisées en conséquence.

Les filtres et les groupements n'affectent pas les constatations dans la vue Constatations personnalisées. Cette vue ne vous permet pas de consulter les résultats de rapports personnalisés ou de sauvegarder des constatations spécifiques.

Vues comportant des constatations

De nombreuses vues AppScan Source for Analysis contiennent des constatations :

- Vue Constatations
- Vue Constatations modifiées
- Vue Constatations personnalisées
- Vue Constatations exclues
- Vues Groupement
- Vue Constatations corrigées/manquantes
- Vue Rapport
- Vue Résultats de la recherche
- Vue Différences entre les évaluations

Tableau Constatations

Ce tableau décrit les colonnes disponibles dans les tableaux de constatations. Si une colonne n'est pas disponible, elle est probablement cachée dans le tableau. Pour sélectionner une colonne pour affichage (ou exécuter toute autre tâche de personnalisation dans un tableau), suivez les instructions de la section «Personnalisation du tableau de constatations», à la page 276.

Tableau 35. Tableau de constatations

En-tête de la colonne	Description
Trace	Une icône dans cette colonne indique qu'il existe une trace pour les collecteurs perdus ou connus.

Tableau 35. Tableau de constatations (suite)

En-tête de la colonne	Description
Gravité	• **Elevée** : Pose un risque pour la confidentialité, l'intégrité et la disponibilité des données et/ou des ressources de traitement. Vous devriez affecter cette priorité aux conditions nécessitant une résolution immédiate. • **Moyenne** : Pose un risque pour la sécurité des données et l'intégrité des ressources mais la condition est moins susceptible de subir des attaques. Les conditions de gravité moyenne devraient être examinées et résolues dans la mesure du possible. • **Faible** : Pose un risque minime à la sécurité des données et à l'intégrité des ressources. • **Info** : La constatation elle-même ne présente pas de risque. Elle décrit plutôt les technologies, les caractéristiques de l'architecture ou les mécanismes de sécurité utilisés dans le code.
Classification	Type de constatation : constatation de sécurité **Définitive** ou **Suspectée** - ou constatation de **Couverture d'examen**. **Remarque :** Dans certains cas, la classification **Aucun** est utilisée pour indiquer une constatation qui n'est ni une constatation de sécurité ni une constatation de couverture d'examen.
Type de vulnérabilité	Catégorie de la vulnérabilité, telle que `Validation.Required` ou `Injection.SQL`.
API	Indique l'appel vulnérable, en présentant à la fois l'API et les arguments qui lui sont transmis.
Source	Une source est une entrée du programme, telle qu'un fichier, une requête de servlet, une saisie depuis la console ou un socket. Dans le cas de la plupart des sources d'entrées, les données renvoyées ne sont pas limitées en termes de contenu et de longueur. Lorsqu'une entrée n'est pas vérifiée, elle est considérée comme entachée.
Collecteur	Un collecteur peut être un format externe quelconque dans lequel des données peuvent être consignées. Comme exemples de collecteurs, on peut citer des bases de données, des fichiers, des sorties console et des sockets. La consignation de données dans un collecteur sans leur vérification peut donner lieu à une vulnérabilité sérieuse de la sécurité.
Répertoire	Chemin d'accès complet des fichiers analysés.

Tableau 35. Tableau de constatations (suite)

En-tête de la colonne	Description
Fichier	Nom du fichier de code dans lequel la constatation de sécurité ou la constatation de couverture d'examen survient. Les chemins de fichier dans les constatations sont relatifs au répertoire de travail du projet analysé.
Méthode d'appel	Fonction (ou méthode) depuis laquelle l'appel vulnérable est effectué.
Ligne	Numéro de la ligne dans le fichier de code contenant l'API vulnérable.
Groupement	Groupement contenant cette constatation.
CWE	ID et sujet du dictionnaire de faiblesses logicielles courantes développé par la communauté (rubriques CWE - Common Weakness Enumeration).

Personnalisation du tableau de constatations :

Vous pouvez personnaliser les tables de constatations dans toutes les vues comportant des constatations (hormis la vue Différences entre les évaluations dans AppScan Source for Analysis) en identifiant les seules colonnes et l'ordre dans lequel vous désirez les afficher. Chaque vue peut avoir des paramètres distincts ou vous pouvez appliquer vos options à toutes les vues. Pour personnaliser l'ordre des colonnes, suivez les procédures de cette rubrique de tâche.

Pourquoi et quand exécuter cette tâche

Pour plus d'informations sur les colonnes d'un tableau de constatations, reportez-vous à la rubrique «Tableau Constatations», à la page 274.

Procédure

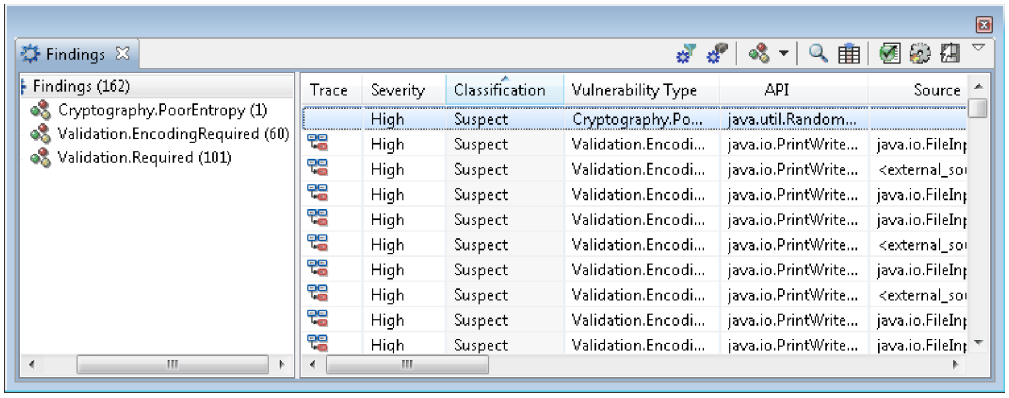
1. Cliquez sur le bouton **Sélection et classement des colonnes** dans la barre d'outils.

   Remarque : Dans AppScan Source for Development (plug-in Visual Studio), cliquez sur le bouton de barre d'outils **Sélectionner et ordonner les colonnes de table**.
2. Dans la boîte de dialogue **Sélectionnez et ordonnez les colonnes**, sélectionnez le nom de la colonne, puis cliquez sur la flèche **Haut** ou **Bas** pour modifier la position de la colonne.
3. Cliquez sur le bouton **Ajouter une colonne** pour ajouter une colonne à la vue. Vous pouvez également cliquer sur le bouton **Supprimer une colonne** pour supprimer une colonne de la vue.

   Remarque : Dans AppScan Source for Development (plug-in Visual Studio), ces boutons s'appellent **Insérer** et **Supprimer** respectivement.
4. Cliquez sur **Restaurer les valeurs par défaut** pour réinitialiser les colonnes et l'ordre des colonnes par défaut.
5. Cliquez sur **OK** pour sauvegarder ces paramètres.

Vue Constatations

La vue Constatations contient des données liées aux constatations d'une évaluation. Les constatations peuvent être regroupées en fonction des paramètres répertoriés dans cette rubrique.



A faire : Dans AppScan Source for Development (plug-in Eclipse) et AppScan Source for Analysis, il s'agit des *vues* dans l'interface utilisateur. Dans AppScan Source for Development (plug-in Visual Studio), il s'agit des *fenêtres* dans l'interface utilisateur. Dans la présente documentation, le terme *vue* est généralement utilisé pour parler aussi bien de *vues* que de *fenêtres*.

Regroupement des paramètres de la table des constatations

Dans la vue Constatations, sélectionnez la flèche vers le bas du bouton de la barre d'outils **Sélectionnez une arborescence hiérarchique**, puis choisissez le paramètre selon lequel les constatations doivent être regroupées.

Tableau 36. Regroupement des paramètres du tableau des constatations

Mode	Regroupement
Type de vulnérabilité	Type, Gravité, Classification
Classification	Classification, Gravité, Type
Fichier	Projet, Répertoire, Fichier, Méthode
API	API, Type
Groupement	Groupement, Type, API
CWE	Enumération de faiblesses courantes
Tableau	Pas de regroupement

Boutons de la barre d'outils

Tableau 37. Boutons de la barre d'outils

Action	Icône	Description
Afficher les constatations ne correspondant pas au filtre		Ce bouton vous permet de basculer l'affichage des constatations filtrées dans la vue Constatations.

Tableau 37. Boutons de la barre d'outils (suite)

Action	Icône	Description
Afficher les constatations groupées		Ce bouton vous permet de basculer l'affichage des constatations groupées dans la vue Constatations. Cette action masque les constatations dans tous les groupements inclus que vous avez créés. Ce paramètre n'affecte pas l'affichage des constatations dans les groupements exclus (ces constatations ne sont jamais affichées dans la vue Constatations.
Sélectionnez une arborescence hiérarchique	Varie en fonction du regroupement qui est sélectionné.	Voir «Regroupement des paramètres de la table des constatations», à la page 277.
Rechercher		Ce bouton ouvre une boîte de dialogue qui vous permet de rechercher des constatations. Diverses options de recherche sont disponibles dans la boîte de dialogue. Après une recherche, des résultats apparaissent dans la vue Résultats de la recherche.
sélection et classement des colonnes		Ce bouton ouvre la boîte de dialogue Sélectionnez et ordonnez les colonnes qui vous permet d'ajouter, de supprimer ou de modifier des colonnes.
Vue Rapport		Ce bouton ouvre la vue Rapport qui affiche les constatations en fonction de rapports d'audit complets qui mesurent la conformité avec les meilleures pratiques en matière de sécurité logicielle et les exigences en matière de réglementation.
Créer une constatation personnalisée		Ce bouton est disponible uniquement dans AppScan Source for Analysis. Lorsque vous le sélectionnez, la boîte de dialogue Créer une constatation personnalisée s'ouvre afin de vous permettre d'ajouter une constatation personnalisée à l'évaluation en cours.

Tableau 37. Boutons de la barre d'outils (suite)

Action	Icône	Description
Sauvegarder les constatations sélectionnées		Si une ou plusieurs constatations sont sélectionnées, ce bouton ouvre la boîte de dialogue Sauvegarde des constatations sélectionnées qui vous permet de sauvegarder les constatations sélectionnées dans un nouveau fichier d'évaluation.
Menu Vue		Ce menu permet d'accéder rapidement à toutes les actions de barre d'outils.

Depuis la vue Constatations, vous pouvez :

- Ouvrir la constatation dans l'éditeur de code
- Créer des exclusions
- Modifier des constatations
- Afficher les constatations des différents groupements
- Rechercher des constatations concernant des éléments spécifiques

Lors de l'utilisation de la vue dans AppScan Source for Analysis, vous pouvez également :

- Déplacer des constatations vers un groupement
- Soumettre des défauts aux systèmes de suivi des défauts
- Créer des constatations personnalisées
- Générer des rapports sur les constatations
- Envoyer des constatations ou des groupements par courrier électronique

Vue Constatations exclues

Cette vue contient uniquement les constatations exclues. Une constatation exclue est omise des examens. Depuis cette vue, vous pouvez rechercher des constatations spécifiques. Les colonnes de cette vue sont identiques à celles de la vue Constatations.

Pour ajouter des constatations qui ont été exclues, suivez les instructions décrites dans «Nouvelle inclusion de constatations qui ont été marquées comme des exclusions», à la page 138.

Vue Constatations modifiées

Cette vue contient toutes les constatations modifiées de l'application actuelle. Les *constatations modifiées* désignent des constatations dont le type de vulnérabilité, la gravité, la classification ou les notes ont été changés. Les *modifications perdues*(c'est-à-dire ne figurant pas dans l'évaluation actuellement ouverte) figurent en vert et en italiques et ne peuvent pas être modifiées.

Depuis cette vue, vous pouvez :

- Rechercher des constatations spécifiques.
- Apporter des modifications supplémentaires

Dans AppScan Source for Analysis, vous pouvez également exécuter ces actions dans cette vue :

- Ajouter des constatations à des groupements
- Soumettre des défauts aux systèmes de suivi des défauts
- Envoyer des constatations (défauts) par courrier électronique
- Générer des rapports sur les constatations

Vue Constatations corrigées/manquantes

Cette vue identifie les constatations figurant dans des groupements mais absentes de l'évaluation en cours. Une constatation est identifiée comme corrigée/manquante si elle a été résolue, supprimée ou que son fichier source n'a pas été analysé.

Vue Résultats de la recherche

Lorsque vous recherchez des constatations, les résultats apparaissent dans la vue Résultats de la recherche.

Depuis cette vue, vous pouvez :

- Trier les constatations
- Editer le code dans un éditeur interne ou externe
- Définir le type de vulnérabilité
- Promouvoir les constatations suspectées et les constatations de couverture d'examen en constatations définitives
- Définir le niveau de gravité
- Annoter des constatations
- Exclure des constatations spécifiques
- Effectuer des recherches supplémentaires

Lors de l'utilisation de la vue dans AppScan Source for Analysis, vous pouvez également :

- Ajouter des constatations à des groupements
- Soumettre des défauts à des systèmes de suivi de défaut ou transmettre des constatations par courrier électronique.
- Générer des rapports sur les constatations

Cette vue ne contient que les éléments correspondant aux critères de la recherche et comprend tout au plus cinq résultats. Par exemple, si vous recherchez dans cette vue le type de vulnérabilité Dépassement de mémoire tampon, puis la classification Définitive, le résultat sera l'intersection des deux recherches.

Les résultats de la recherche figurent dans la zone Recherche sous la forme `"<mot clé>" dans <vue_d'origine> : <zones recherchées>` (par exemple, `"arrêt" dans Constatations [Contexte, API, Méthode]`. Si vous fermez l'évaluation actuelle, tous les résultats de la recherche sont éliminés et la zone Recherche affiche le texte `Pas de recherche en cours`.

Vue Rapport

La vue Rapport vous permet d'organiser les résultats d'un examen en fonction de divers rapports d'audit qui mesurent la conformité avec les meilleures pratiques en matière de sécurité logicielle et les exigences en matière de réglementation.

La vue affiche des constatations en fonction des rapports suivants :

- «Rapport CWE/SANS Top 25 2011», à la page 189
- «Rapport DISA Application Security and Development STIG V3R10», à la page 190
- «Rapport Open Web Application Security Project (OWASP) Mobile Top 10», à la page 190
- «Rapport Open Web Application Security Project (OWASP) Top 10 2013», à la page 190
- «Rapport PCI DSS (Payment Card Industry Data Security Standard) version 3.2», à la page 190
- «Rapport Profil de sécurité logicielle», à la page 190

Si vous utilisez AppScan Source for Analysis pour créer un rapport personnalisé qui a été sauvegardé dans `<data_dir>\reports\profile` (où `<rép_données>` est l'emplacement de vos données de programme AppScan Source, comme décrit dans «Installation et emplacements des fichiers de données utilisateur», à la page 292), vous pouvez également utiliser le rapport Vue pour afficher des constatations via le rapport personnalisé.

Les colonnes du rapport sont identiques à celles de la «Vue Constatations», à la page 277.

Recherche de constatations

Vous pouvez rechercher des constatations spécifiques dans plusieurs vues contenant des constatations. Les critères de recherche incluent les groupements, le code, les fichiers, les projets et les types de vulnérabilité. Les résultats figurent dans la vue Résultats de la recherche.

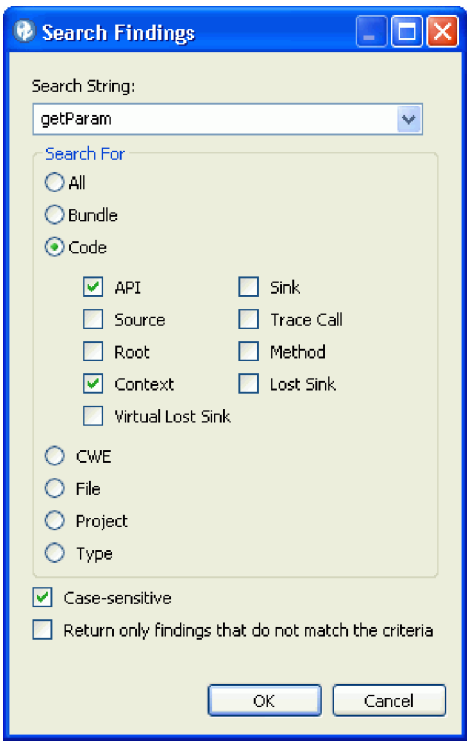
Lors d'une recherche dans le code, la recherche peut couvrir plusieurs éléments ou tous les éléments, notamment :

- API
- Contexte
- Méthode
- Source
- Collecteur
- Collecteur indéterminé
- Racine
- Appel de trace

Recherche de chaque occurrence d'un élément dans toutes les constatations :

Procédure

1. Sélectionnez la vue dans laquelle effectuer la recherche.
2. Sélectionnez **Editer** > **Rechercher** dans le menu principal (dans AppScan Source for Development (plug-in Eclipse), sélectionnez **Editer** > **Rechercher/Remplacer** ou dans AppScan Source for Development (plug-in Visual Studio), cliquez sur le bouton **Rechercher** dans une vue comportant des constatations).



3. Entrez une chaîne de recherche dans la boîte de dialogue **Recherche de constatations**.
4. Recherchez la chaîne dans un **Groupement**, **Code**, **CWE**, **Fichier**, **Projet**, **Type**, ou **Tout**. Les constatations correspondantes apparaissent dans la vue Résultats de la recherche.

   Sélectionnez **Sensible à la casse** pour respecter la casse dans la recherche du texte.

   Si vous utilisez AppScan Source for Analysis ou AppScan Source for Development (plug-in Eclipse), sélectionnez **Renvoyer uniquement les constatations ne correspondant pas aux critères** pour renvoyer uniquement les constatations qui ne correspondent pas aux critères de recherche.

Recherche de constatations dans un tableau de constatations :

Procédure

1. Cliquez dans la barre d'outils sur **Rechercher**.
2. Indiquez les caractéristiques de la recherche et cliquez sur **OK**.

Recherche dans une arborescence de constatations :

Procédure

1. Cliquez dans la barre d'outils sur **Rechercher**.
2. Indiquez les caractéristiques de la recherche et cliquez sur **OK**.

Résultats

Dans une vue des constatations, vous pouvez également effectuer une recherche dans un sous-ensemble des constatations visibles. Vous pouvez, par exemple, rechercher des constatations dans un sous-ensemble spécifique, tel que le Type de vulnérabilité.

Vue Sources et collecteurs

Cette vue permet de visualiser des constatations en fonction d'une trace des entrées et des sorties.

Cette vue est divisée en trois sections :

- **Sources et collecteurs** : Le panneau de gauche comporte trois noeuds de premier niveau :
  - **Source** : une source est une entrée du programme, telle qu'un fichier, une requête de servlet, une saisie depuis la console ou un socket. Dans le cas de la plupart des sources d'entrées, les données renvoyées ne sont pas limitées en termes de contenu et de longueur. Lorsqu'une entrée n'est pas vérifiée, elle est considérée comme entachée. Les sources sont répertoriées dans les tables de constatations sous la colonne **Source**.
  - **Collecteur** : un collecteur peut être un format externe quelconque dans lequel des données peuvent être consignées. Comme exemples de collecteurs, on peut citer des bases de données, des fichiers, des sorties console et des sockets. La consignation de données dans un collecteur sans leur vérification peut donner lieu à une vulnérabilité sérieuse de la sécurité.
  - **Collecteur indéterminé** : un collecteur indéterminé est une méthode API qui ne peut plus faire l'objet d'une trace.

  Chaque noeud peut être développé pour afficher les packages affectés. Ceux-ci peuvent eux-mêmes être développés pour afficher les classes affectées, puis les méthodes. Ces méthodes peuvent à leur tour être développées afin d'afficher le package, la classe et la méthode à l'extrémité opposée de la trace. Par exemple, si vous êtes préoccupé par un collecteur spécifique, vous pouvez descendre jusqu'à la méthode sous la racine **Collecteurs**. A partir de là, l'arborescence sous la méthode afficherait les chemins remontant à toutes les sources ayant conduit à ce collecteur :

```
- Sources
 - package A
  - classe A
   - méthode A
    - package B
     - classe B
      - méthode B (à l'extrémité opposée de la trace)
- Collecteurs
 - package B
  - classe B
   - méthode B
    - package A
     - classe A
      - méthode A
- Collecteurs indéterminés
```

  La sélection opérée dans cette vue de l'arborescence détermine ce qui sera affiché dans les deux autres sections de la vue.

- **Noeuds intermédiaires** : Cette section de la vue affiche l'agrégation de tous les noeuds intermédiaires des traces qui s'appliquent à la sélection dans la section Sources et collecteurs. Elle vous permet d'affiner l'affichage du tableau des constatations.

  Cette section est masquée par défaut. Vous pouvez l'afficher (ou la masquer à nouveau) en cliquant sur **Afficher/Masquer la table des appels intermédiaires**.

  Pour afficher uniquement les constatations concernant un package, une classe ou une méthode, cochez la case dans sa colonne **Requis**. Pour expurger les constatations concernant un package, une classe ou une méthode, cochez la case

dans sa colonne **Supprimer**. Les paramètres de filtrage de cette section peuvent être utilisés pour créer un nouveau filtre.

Exemple d'utilisation : Supposons le noeud d'arborescence suivant dans la section Sources et collecteurs :

```
- Sources
 - java.util
  - Properties
   - getProperty
```

Lorsque `getProperty` est sélectionnée, le tableau des constatations affiche uniquement celles contenant des traces avec pour source `getProperty`. A ce point, la section des noeuds intermédiaires les affiche tous (tous les noeuds dans la trace autres que la source et le collecteur) pour toutes les traces avec pour source `getProperty`. Cependant, le fait que la trace transite par une API spécifique peut vous être indifférent. Vous pouvez, par exemple, disposer d'une routine de validation qui garantit que les données provenant de `getProperty` sont valides et ne désirez donc pas voir affichées les traces empruntant cette routine de validation. La section des noeuds intermédiaires inclura cette routine de validation puisqu'il s'agit d'un noeud intermédiaire dans la trace. Vous pouvez accédez à cette routine de validation dans la section des noeuds intermédiaires et cocher sa case **Supprimer**. Ceci éliminera du tableau des constatations toutes celles dont la trace transite par ce noeud intermédiaire.

- **Constatations** : Cette section contient la même «Tableau Constatations», à la page 274 (et les actions associées) que celle de la «Vue Constatations», à la page 277 et des autres vues contenant des constatations. Elle affiche les constatations concernant les sources, collecteurs et noeuds intermédiaires que vous avez choisi d'afficher dans les deux autres sections de la vue.

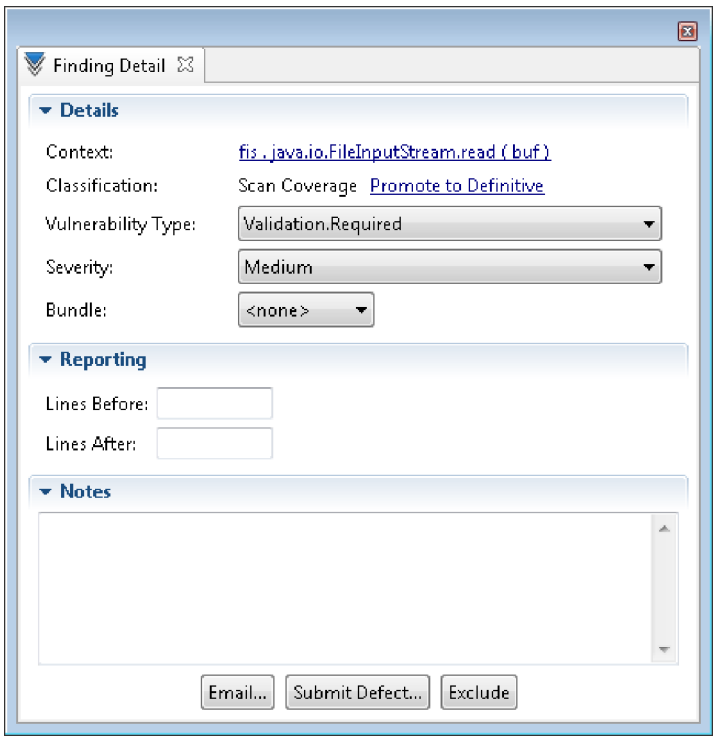
Vues qui permettent d'effectuer des investigations sur une constatation unique

Les vues présentées dans cette section permettent d'effectuer des investigations sur des constatations uniques.

- «Vue Constatation détaillée», à la page 145
- «Vue Assistance à la résolution», à la page 287
- «Vue Trace», à la page 287

Vue Constatation détaillée

Lorsque vous sélectionnez une constatation, la vue Constatation détaillée, dans laquelle vous pouvez modifier ses propriétés, s'affiche. Avec cette vue, vous pouvez modifier une constatation individuelle.



- «Section Détails», à la page 146
- «Section Rapport (disponible dans AppScan Source for Analysis et AppScan Source for Development (plug-in Eclipse) seulement)», à la page 146
- «Section Notes», à la page 146
- «Actions de la vue Constatation détaillée», à la page 147
- «Vue Constatation détaillée pour les constatations personnalisées (disponible uniquement dans AppScan Source for Analysis)», à la page 147

Section Détails

- **Contexte** : Fragment de code encadrant la vulnérabilité
- **Classification** : Constatations de sécurité définitive ou suspectée - ou Constatations de couverture d'examen - avec lien pour promouvoir la constatation en **Définitive** ou pour revenir à la valeur initiale si la vulnérabilité a été modifiée.
- **Type de vulnérabilité**
- **Gravité** : Elevée, moyenne, faible ou information
- **Groupement** : Nom du groupement contenant les constatations (non disponible dans AppScan Source for Development (plug-in Visual Studio))

Section Rapport (disponible dans AppScan Source for Analysis et AppScan Source for Development (plug-in Eclipse) seulement)

Spécifiez le nombre de lignes de code à inclure avant et/ou après la constatation dans les rapports.

Section Notes

Annotez la constatation.

Actions de la vue Constatation détaillée

- **Exclure** : Cliquez sur **Exclure** pour exclure (supprimer) la constatation du tableau des constatations. Pour visualiser des constatations exclues, ouvrez la vue Constatations exclues.
- Disponible dans AppScan Source for Analysis seulement :
  - **Courrier électronique** : Si vous avez configuré des préférences de courrier électronique, vous pouvez envoyer directement un groupement de constatations à des développeurs pour les aviser des défauts potentiels détectés après un examen. Le courrier électronique inclut en pièce jointe un groupement contenant les constatations et le courrier décrit ces constatations.
    1. Pour envoyer par courrier électronique la constatation actuelle depuis la vue Constatation détaillée, cliquez sur **Courrier électronique**.
    2. Dans la boîte de dialogue Nom de fichier de pièce jointe, spécifiez un nom pour le fichier de groupement qui sera joint à l'e-mail. Par exemple, si vous spécifiez `ma_constatation` dans la zone **Nom du fichier de pièce jointe**, un groupement avec le nom de fichier `ma_constatation.ozbdl` sera joint au courrier.
    3. Cliquez sur **OK** pour ouvrir la boîte de dialogue Envoi de constatations par courrier électronique. Par défaut, la zone **Envoyer à** de la boîte de dialogue d'envoi de constatations par courrier électronique contient les données de la zone **Adresse de destination** qui est spécifiée dans les préférences de courrier électronique. Toutefois, elle peut facilement être modifiée lors de la préparation du courrier électronique. Dans cette boîte de dialogue, cliquez sur **OK** pour envoyer le courrier électronique après avoir vérifié son contenu.
  - **Soumettre un défaut** : Pour soumettre la constatation en tant que défaut, cliquez sur **Soumettre un défaut**. Ceci ouvre la boîte de dialogue Sélection du système de suivi des défauts.
    - Si vous sélectionnez **ClearQuest** et cliquez sur **OK**, la boîte de dialogue Nom de fichier de pièce jointe s'affiche. Spécifiez dans celle-ci un nom pour le fichier de groupement qui sera joint au défaut, puis cliquez sur **OK**. Connectez-vous à Rational ClearQuest et soumettez les constatations.
    - Si vous sélectionnez **Quality Center** et cliquez sur **OK**, la boîte de dialogue Connexion s'ouvre pour vous permettre d'ouvrir une session Quality Center et de soumettre les constatations.
    - Si vous sélectionnez l'option **Team Foundation Server**, une boîte de dialogue s'affiche pour vous inviter à vous connecter au système de suivi des défauts et fournir d'autres détails de configuration.

    Remarque : Rational Team Concert est le seul système de suivi d'incidents pris en charge sous macOS.

Vue Constatation détaillée pour les constatations personnalisées (disponible uniquement dans AppScan Source for Analysis)

La vue Constatation détaillée fournit des informations supplémentaires que vous pouvez modifier :

- Fichier
- Ligne
- Colonne
- API

De plus, la méthode suivant laquelle vous modifiez la «Section Détails», à la page 146 est différente des constatations standard pour certaines zones (par exemple, les classifications pour les constatations personnalisées apparaissent dans une liste).

Vue Assistance à la résolution

La Base de connaissances de sécurité AppScan Source Security fournit des renseignements sur chaque vulnérabilité dans son contexte spécifique. Elle vous explique la nature de la vulnérabilité, pourquoi son utilisation n'est pas sûre, comment la corriger et comment l'éviter à l'avenir. Une fois que vous avez analysé le code source, la Base de connaissances fournit les informations spécifiques nécessaires pour éliminer les risques dans les applications critiques pour votre activité. Le conseil pour la résolution provenant de la Base de connaissances apparaît dans la vue Aide à la résolution. Une fois l'examen réalisé, la Base de connaissances fournit les informations spécifiques nécessaires pour éliminer les risques dans les applications critiques pour votre activité.

Pour consulter la Base de connaissances et obtenir des conseils pour la résolution

- Sélectionnez une constatation dans un tableau de constatations, puis ouvrez l'aide de la Base de connaissances ou la vue Aide à la résolution.
- Dans AppScan Source for Analysis, vous pouvez également sélectionner **Aide** > **Base de connaissances de sécurité** dans le menu pour afficher la totalité de la Base de connaissances.

Le niveau et le type de gravité des API est indiqué dans la base de données. Par exemple l'API `strcpy()` (vulnérabilité de type Dépassement de mémoire tampon) est associée à un niveau de gravité élevé. La description indique que `strcpy()` est vulnérable à un dépassement de la mémoire tampon de destination car elle ne connaît pas sa longueur et ne peut pas s'assurer de ne pas l'écraser. Corrigez ce problème en utilisant `strncpy ()`, laquelle reçoit un paramètre de longueur.

Si la constatation est associée à un ID CWE (énumération des faiblesses courantes), un hyperlien figure dans la vue Assistance à la résolution vers la rubrique CWE correspondante (`CWE: <id>`) à l'adresse `http://cwe.mitre.org/data/definitions/<ID_CWE>.html`.

Vue Trace

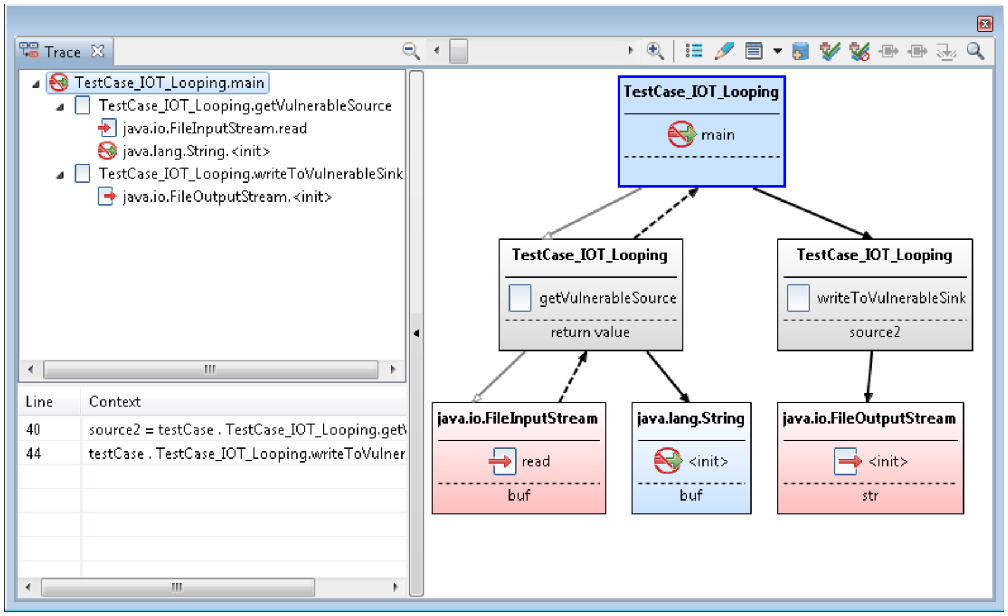
AppScan Source effectue une analyse des entrées/sorties, puis identifie et affiche les vulnérabilités détectées. Une icône identifie dans la liste des constatations les lignes contenant un diagramme de trace AppScan Source.

Dans la vue Trace, le noeud racine où se rejoignent les piles d'entrée/sortie est affiché. La pile des entrées correspond à une série d'appels conduisant à une *source* connue pour contenir des données entachées. La pile des sorties correspond à une série d'appels menant à un *collecteur*. Une trace AppScan Source est générée lorsque le code analysé peut retracer l'utilisation d'une source non protégée dans un collecteur non protégé.

- **Source** : une source est une entrée du programme, telle qu'un fichier, une requête de servlet, une saisie depuis la console ou un socket. Dans le cas de la plupart des sources d'entrées, les données renvoyées ne sont pas limitées en termes de contenu et de longueur. Lorsqu'une entrée n'est pas vérifiée, elle est considérée comme entachée. Les sources sont répertoriées dans les tables de constatations sous la colonne **Source**.

- **Collecteur** : un collecteur peut être un format externe quelconque dans lequel des données peuvent être consignées. Comme exemples de collecteurs, on peut citer des bases de données, des fichiers, des sorties console et des sockets. La consignation de données dans un collecteur sans leur vérification peut donner lieu à une vulnérabilité sérieuse de la sécurité.
- **Collecteur indéterminé** : un collecteur indéterminé est une méthode API qui ne peut plus faire l'objet d'une trace.

Ce diagramme illustre la séquence d'appels depuis la racine de la pile d'entrée et de la pile de sortie.



Dans ce diagramme :

- Les flèches creuses identifient les appels dont le flux de données n'est pas connu pour être entaché.
- Les flèches pleines contiennent des données potentiellement entachées. Les lignes discontinues indiquent un chemin de retour des données.
- Les lignes pleines correspondent à un appel de méthode.

Conseil :

- Dans la vue Trace, survolez les noeuds de trace du graphique pour afficher des informations sur le noeud.
- Les deux panneaux de gauche de la vue (le panneau des piles d'entrée/sortie et le panneau des flux de données) peuvent être réduits pour améliorer l'affichage du diagramme d'appels graphique. Pour réduire ces panneaux, sélectionnez la flèche de **masquage de l'arborescence**. Pour afficher ces panneaux lorsqu'ils sont masqués, sélectionnez la flèche d'**affichage de l'arborescence**.
- Déplacez la barre de défilement pour effectuer un zoom avant détaillé ou effectuer un zoom arrière pour une vue plus générale. Si vous survolez la barre de défilement du zoom, le niveau de zoom actuel s'affiche. Pour effectuer un zoom avant maximum, sélectionnez le **zoom à 200 %**. Pour effectuer un zoom arrière maximal, sélectionnez le **zoom pour ajuster**.

Vues qui vous permettent d'utiliser des évaluations

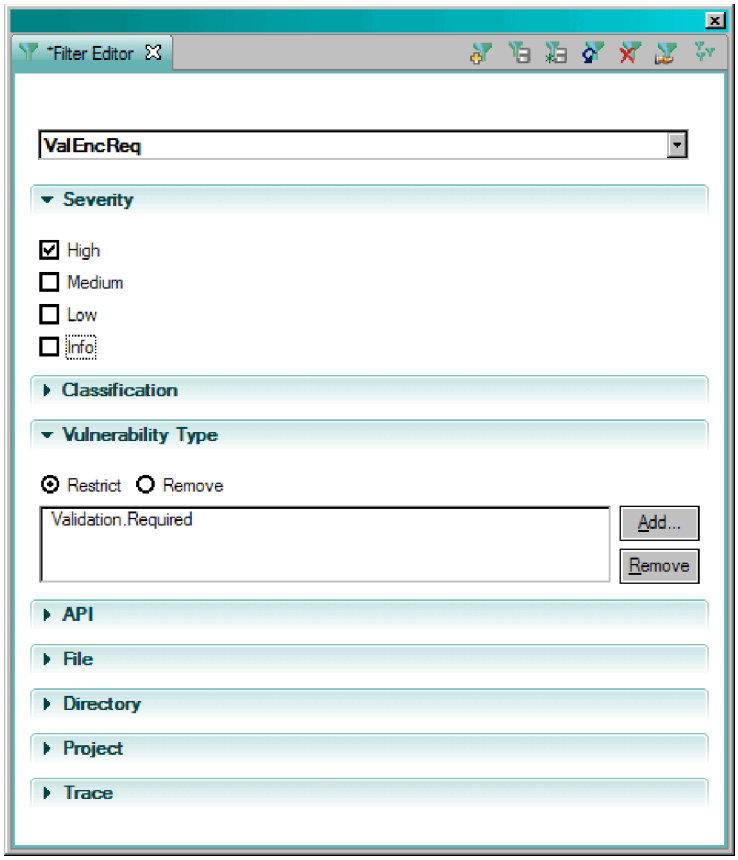
Les vues présentées dans cette section permettent un haut niveau d'utilisation des évaluations.

- «Vue Editeur de filtre»
- «Vue Matrice de vulnérabilités»

Vue Editeur de filtre

La vue Editeur de filtre permet une manipulation plus granulaire du filtre sélectionné que d'autres vues AppScan Source. Elle consiste de tous les éléments d'après lesquels vous pouvez effectuer un filtrage.

Remarque : Dans AppScan Source for Development (plug-in Visual Studio), cette vue fait partie de la fenêtre Edition de filtres.

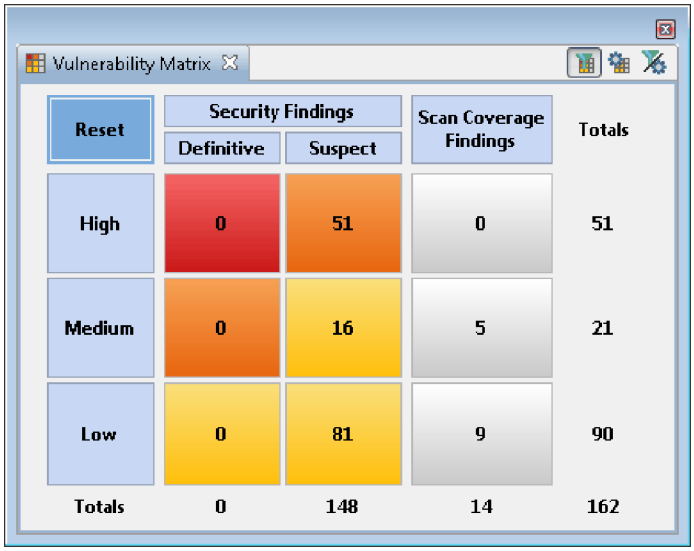


Conseil : Dans la section **Trace** de la vue Editeur de filtre, survolez une entrée de trace pour obtenir des informations sur cette entrée.

Vue Matrice de vulnérabilités

Cette vue affiche le nombre total de constatations pour toutes les applications couvertes par l'examen. Les modifications apportées aux constatations actualisent cette matrice.

Remarque : Dans AppScan Source for Development (plug-in Visual Studio), cette vue fait partie de la fenêtre Edition de filtres.



Les constatations de sécurité et de couverture d'examen figurent dans des rectangles dont la couleur indique l'ordre de priorité à suivre pour examiner ou gérer les constations :

1. Les constatations de sécurité définitives dont la gravité est élevée s'affichent en rouge, couleur indiquant la priorité la plus élevée.
2. Les constatations de sécurité suspectées dont la gravité est moyenne s'affichent en orange et doivent être traitées ensuite.
3. Les entrées de matrice suivantes s'affichent en jaune et doivent être examinées ensuite :
   - Constatations de sécurité définitives dont la gravité est faible
   - Constatations de sécurité suspectées dont la gravité est moyenne et faible
4. Les constatations de couverture d'examen s'affichent dans des carrés gris et peuvent se voir attribuer la priorité la plus faible.

Lorsque vous cliquez sur une cellule, un en-tête de ligne ou de colonne dans la **Matrice de vulnérabilités**, ceci actualise le filtre en cours de sorte à n'afficher que les résultats de cette cellule, ligne ou colonne. Cliquez ensuite sur **Réinitialiser** pour revenir à la vue contenant toutes les constatations.

Dans la vue Matrice de vulnérabilités, les boutons de la barre d'outils déterminent les chiffres affichés dans les rectangles colorés. Vous pouvez afficher :

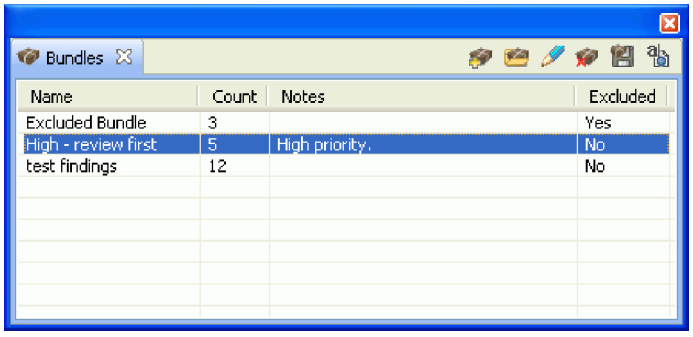
- Uniquement le nombre et le total de constatations filtrées
- Le nombre et le total des constatations

  Remarque : Les constatations sur la **Qualité** et celles classées avec le niveau de gravité **Info** ne sont pas incluses dans la vue Matrice de vulnérabilités.
- Le nombre et le total des constatations filtrées et de toutes les constatations

Remarque : Les filtres qui sont appliqués hors de la vue Matrice de vulnérabilités peuvent ne pas affecter la vue Matrice de vulnérabilités. Le bouton de la barre d'outils **Afficher le nombre de constatations filtrées** de la vue Matrice de vulnérabilités doit être sélectionné pour que le filtre soit reflété dans la vue Matrice de vulnérabilités.

Vue Groupements

La vue Groupements permet de créer de nouveaux groupements, d'ajouter des constatations à un groupement, d'afficher des groupements et des annotations, de renommer ou de supprimer un groupement. Cette vue liste le nom du groupement, les notes qui lui sont éventuellement rattachées, le nombre de constatations dans le groupement et indique si celui-ci est exclu. Si vous ouvrez le groupement pour afficher son contenu, vous pouvez déplacer des constatations vers d'autres groupements, modifier les constatations, éditer le code ou soumettre le groupement à un système de suivi des défauts.



Pour plus d'informations, voir «Triage avec des groupements», à la page 140.

Vue Groupement

La vue Groupement affiche les constatations d'un groupement. Les groupements sont des ensembles de constatations créés dans AppScan Source for Analysis.

Pour visualiser les constatations d'un groupement, cliquez deux fois sur le nom d'un groupement dans la vue Groupement. Le nom du groupement s'affiche comme titre de la vue Groupement. Vous pouvez également importer un groupement et afficher son contenu dans la Vue Groupement. Vous ne pouvez pas modifier ou supprimer de constatations dans un groupement.

La vue Groupement, comme une table de constatations, contient les informations détaillées suivantes :

Tableau 38. Colonnes de la vue Groupement

Colonne	Description
Trace	Une icône dans cette colonne indique qu'il existe une trace pour les collecteurs perdus ou connus.
Fichier	Nom du fichier de code dans lequel la constatation de sécurité ou la constatation de couverture d'examen survient. Les chemins de fichier dans les constatations sont relatifs au répertoire de travail du projet analysé.
Classification	Type de constatation : constatation de sécurité **Définitive** ou **Suspectée** - ou constatation de **Couverture d'examen**. **Remarque :** Dans certains cas, la classification **Aucun** est utilisée pour indiquer une constatation qui n'est ni une constatation de sécurité ni une constatation de couverture d'examen.

Tableau 38. Colonnes de la vue Groupement (suite)

Colonne	Description
Gravité	• **Elevée** : Pose un risque pour la confidentialité, l'intégrité et la disponibilité des données et/ou des ressources de traitement. Vous devriez affecter cette priorité aux conditions nécessitant une résolution immédiate. • **Moyenne** : Pose un risque pour la sécurité des données et l'intégrité des ressources mais la condition est moins susceptible de subir des attaques. Les conditions de gravité moyenne devraient être examinées et résolues dans la mesure du possible. • **Faible** : Pose un risque minime à la sécurité des données et à l'intégrité des ressources. • **Info** : La constatation elle-même ne présente pas de risque. Elle décrit plutôt les technologies, les caractéristiques de l'architecture ou les mécanismes de sécurité utilisés dans le code.
Type de vulnérabilité	Catégorie de la vulnérabilité, telle que `Validation.Required` ou `Injection.SQL`.
Contexte	Fragment de code encadrant la vulnérabilité.
Méthode d'appel	Fonction (ou méthode) depuis laquelle l'appel vulnérable est effectué.
CWE	ID et sujet du dictionnaire de faiblesses logicielles courantes développé par la communauté (rubriques CWE - Common Weakness Enumeration).
Ligne	Numéro de la ligne dans le fichier de code contenant l'API vulnérable.
Notes	Toute note ajoutée à cette constatation.
ID du défaut	ID du défaut provenant d'un système de suivi des défauts.

Installation et emplacements des fichiers de données utilisateur

Lorsque vous installez AppScan Source, les fichiers de configuration et de données utilisateur sont stockés en dehors du répertoire d'installation.

- «Répertoire d'installation par défaut»
- «Répertoire AppScan Source par défaut», à la page 293
- «Emplacement de fichier temporaire AppScan Source», à la page 293

Répertoire d'installation par défaut

Lorsque AppScan Source est installé, le logiciel est placé dans l'un des répertoires par défaut suivants :

- Versions 32 bits de Microsoft Windows :
  `<UNITESYSTEME>:\Program Files\IBM\AppScanSource`

- Versions 64 bits de Microsoft Windows :
  `<UNITESYSTEME>:\Program Files (x86)\IBM\AppScanSource`
- Linux : si vous êtes l'utilisateur root, l'assistant d'installation installe votre logiciel dans `/opt/ibm/appscansource`. Si vous n'êtes pas l'utilisateur root, vous pouvez installer le plug-in Eclipse AppScan Source for Development qui s'installe par défaut dans `<rép_base>/AppScan_Source`.
- macOS : `/Applications/AppScanSource.app`

Important :

- Le nom du répertoire d'installation peut uniquement contenir des caractères anglais. Les noms de dossiers contenant des caractères autres qu'anglais ne sont pas autorisés.
- Si vous effectuez l'installation sous Windows, vous devez disposer de droits d'administrateur pour installer les composants AppScan Source.
- Si vous effectuez l'installation sous Linux, vous devez disposer de droits root pour installer les composants serveur AppScan Source.

Répertoire AppScan Source par défaut

Les données AppScan Source sont des éléments tels que des fichiers de configuration, des exemples de fichiers et des fichiers journaux. Lorsque AppScan Source est installé, les fichiers de données sont placés aux emplacements suivants par défaut :

- Microsoft Windows : `<UNITESYSTEME>:\ProgramData\IBM\AppScanSource`

  Remarque : `ProgramData\` est un dossier masqué et, pour l'afficher, vous devez modifier les préférences d'affichage dans l'**explorateur** afin d'afficher les fichiers et les dossiers masqués.
- Linux : `/var/opt/ibm/appscansource`
- macOS : `/Users/Shared/AppScanSource`

Pour savoir comment modifier l'emplacement du répertoire de données AppScan Source, voir «Modification du répertoire de données AppScan Source», à la page 294.

Emplacement de fichier temporaire AppScan Source

Certaines opérations AppScan Source génèrent des fichiers temporaires qui sont stockés dans les emplacements par défaut suivants :

- Microsoft Windows: `<UNITESYSTEME>:\ProgramData\IBM\AppScanSource\temp`

  Remarque : `ProgramData\` est un dossier masqué et, pour l'afficher, vous devez modifier les préférences d'affichage dans l'**explorateur** afin d'afficher les fichiers et les dossiers masqués.
- Linux : `/var/opt/ibm/appscansource/temp`
- macOS : `/Users/Shared/AppScanSource/temp`

Le fichier temporaire réside toujours dans un répertoire `temp` dans le répertoire de données AppScan Source. Vous pouvez modifier l'emplacement du fichier temporaire en changeant le répertoire de données, comme indiqué dans la rubrique «Modification du répertoire de données AppScan Source», à la page 294. Dans ce cas, le répertoire `temp` se trouvera dans le répertoire de données que vous avez choisi.

Modification du répertoire de données AppScan Source

Vous pouvez modifier l'emplacement du répertoire de données AppScan Source afin de gérer l'espace sur le disque dur. Vous pouvez modifier l'emplacement après l'installation d'AppScan Source en exécutant les étapes décrites dans cette rubrique.

Avant de commencer

Avant d'exécuter cette tâche, assurez-vous que toutes les applications client AppScan Source ont été fermées. Les applications client AppScan Source sont notamment les suivantes :

- AppScan Source for Analysis
- AppScan Source for Development (plug-in Eclipse ou Visual Studio) (pris en charge sous Windows et Linux seulement)
- interface de ligne de commande (CLI) d'AppScan Source
- AppScan Source for Automation

En outre, si vous avez installé AppScan Source for Automation, assurez-vous que le Automation Server a été arrêté :

- Sous Windows, arrêtez le service **IBM Security AppScan Source Automation**.
- Sous Linux, exécutez la commande suivante : `/etc/init.d/ounceautod stop`
- Sous macOS, lancez la commande suivante : `launchctl stop com.ibm.appscan.autod`

Procédure

1. Définissez une variable d'environnement `APPSCAN_SOURCE_SHARED_DATA=<data_dir>`, où `<data_dir>` correspond à l'emplacement où vous souhaitez stocker les données AppScan Source.

   Remarque :

   - L'emplacement `<data_dir>` doit être un chemin d'accès absolu et complet qui existe déjà sur la même machine que votre installation AppScan Source.
   - Le nom du répertoire `<data_dir>` ne peut contenir que des caractères anglais. Les dossiers portant des noms contenant des caractères non anglais ne sont pas autorisés.
2. Localisez le répertoire de données par défaut qui a été créé lorsque AppScan Source a été installé (voir «Répertoire AppScan Source par défaut», à la page 293 pour en savoir plus sur les emplacements de répertoire de données par défaut).
3. Copiez ou déplacez le contenu du répertoire de données par défaut à l'emplacement `<data_dir>` qui est spécifié dans la variable d'environnement.
4. **S'applique uniquement à AppScan Source for Automation installé sous Linux** :
   a. Editez le fichier `/etc/init.d/ounceautod`.
   b. Localisez la ligne suivante :

   ```
   su - ounce -c
   'export LD_LIBRARY_PATH="/opt/IBM/AppScan_Source/bin":$LD_LIBRARY_PATH &&
   cd "/opt/IBM/AppScan_Source/bin" &&
   "/opt/IBM/AppScan_Source/bin/ounceautod" -s' >>
   "/var/opt/ibm/appscansource/logs/ounceautod_output.log" 2>&1 &
   ```

   et remplacez-la par la ligne suivante :

```
su - ounce -c
'export APPSCAN_SOURCE_SHARED_DATA=<nouveau chemin répertoire de données> &&
export LD_LIBRARY_PATH="/opt/IBM/AppScan_Source/bin":$LD_LIBRARY_PATH &&
cd "/opt/IBM/AppScan_Source/bin" &&
"/opt/IBM/AppScan_Source/bin/ounceautod" -s' >>
"<nouveau chemin répertoire de données>/logs/ounceautod_output.log" 2>&1 &
```

Remarque : La commande ci-dessus est sur une ligne.

c. Enregistrez le fichier `/etc/init.d/ounceautod`.

Que faire ensuite

Si vous avez installé AppScan Source for Automation, démarrez le Automation Server :

- Sous Windows, démarrez le service **IBM Security AppScan Source Automation**.
- Sous Linux, lancez la commande suivante : `/etc/init.d/ounceautod start`
- Sous macOS, lancez la commande suivante : `launchctl start com.ibm.appscan.autod`

Chapitre 15. Prise en charge de CWE

La liste Common Weakness Enumeration (CWE) est une liste de normes sectorielles qui fournit des noms communs pour les faiblesses logicielles connues publiquement. Cette rubrique répertorie les ID CWE pris en charge dans la version actuelle de AppScan Source.

Lors des analyses, AppScan Source cherche ces identificateurs de la liste CWE et les identificateurs parents ou enfants associés :

Tableau 39. Prise en charge de CWE

15, 16, 20, 73, 74, 77, 79, 88, 89, 90, 91, 95, 98
105, 109, 112, 113, 116, 117, 120, 129, 130, 131, 134, 185, 190
201, 209, 242, 250, 257, 264, 266, 267, 285, 287, 288, 295
310, 311, 312, 319, 327, 331, 335, 345, 352, 359, 367, 382, 388, 390, 398
400, 404, 407, 425, 434, 447, 470, 472, 477, 489, 497
506, 507, 511, 517, 520, 521, 522, 523, 524, 525, 532, 538, 543, 544, 546, 547, 565, 569, 586
601, 613, 615, 624, 643, 645

Glossaire

Ce glossaire inclut les termes et définitions relatifs à AppScan Source.

Les références croisées suivantes sont utilisées dans ce glossaire :

- Voir renvoie d'un terme vers son synonyme préféré ou d'un acronyme ou d'une abréviation vers sa forme complète définie.
- Voir aussi vous renvoie vers un terme associé ou un contraire.

Pour visualiser les glossaires d'autres produits IBM, accédez à www.ibm.com/software/globalization/terminology.

A

application
Un ou plusieurs programmes informatiques ou composants logiciels fournissant une fonction de support direct pour un ou plusieurs processus métier spécifiques.

assemblage
Collection de types et de ressources formant une unité de déploiement, un contrôle des versions, une configuration de réutilisation, de configuration et des droits de sécurité dans des applications .NET Framework.

attaque
Toute tentative, par une personne non autorisée, de compromettre l'exécution d'un programme informatique ou d'un système en réseau.

attribut
Caractéristique d'une application qui aide à organiser les résultats de l'examen en groupes significatifs, tels que par service ou par chef de projet.

C

cache d'analyse de vulnérabilité
Cache des vulnérabilités trouvées lors d'un examen de code source et pouvant être utilisée pour les examens suivants en vue de réduire le temps d'examen.

collecteur
Format externe quelconque dans lequel des données peuvent être consignées. Comme exemples de collecteurs, on peut citer des bases de données, des fichiers, des sorties console et des sockets.

collecteur indéterminé
Méthode API qui ne peut plus faire l'objet d'une trace.

constatation
Reconnaissance d'une instance d'un risque de sécurité dans un code. AppScan classe les constatations en deux catégories : vulnérabilité et exception.

D

densité V
Expression numérique permettant une évaluation cohérente de la vulnérabilité de vos applications. Cette densité est calculée en rapportant le nombre et la criticité des vulnérabilités et des exceptions à la taille de l'application ou du projet qui sont analysés.

E

encoder
Dans le domaine de la sécurité informatique, convertir du texte en clair en un format inintelligible au moyen d'un système de codes.

évaluation
Collection de constatations provenant d'un code analysé avec laquelle un utilisateur peut travailler et qu'il peut enregistrer et partager avec d'autres utilisateurs.

examiner
Processus AppScan d'exploration et de test d'une application et de présentation des résultats.

exception
Indication d'une condition suspecte et potentiellement vulnérable requérant des informations ou des investigations supplémentaires.

exclusion
Constatation pouvant être marquée et ignorée par un utilisateur.

F

filtre Ensemble de règles définissant des constatations dotées de certaines caractéristiques.

G

graphe d'appels
Un graphe utilisant des lignes représente le flux de données entre des sous-routines d'un programme.

groupement
Ensemble de constatations créé par l'utilisateur. Les groupements peuvent être exportés et partagés entre des personnes et des applications.

I

incident
Type de demande de changement identifiant une anomalie ou une faille dans un produit de travail.

P

perspective
Groupe de vues présentant divers aspects des ressources du plan de travail.

pile Zone de la mémoire stockant généralement des informations telles que des

informations d'enregistrement temporaires, des valeurs de paramètres et des adresses expéditeur de sous-routines et basée sur le principe LIFO (premier entré, dernier sorti).

plan de travail
Interface utilisateur et environnement de développement intégré (IDE) dans Eclipse et les outils basés sur Eclipse, comme IBM Rational Application Developer.

R

rappel Moyen permettant à une unité d'exécution de notifier une autre unité d'exécution d'application qu'un événement s'est produit.

règle de schéma
Schéma ou expression régulière recherché lors d'un examen.

résolution
Suggestion de correction d'un incident.

S

script intersite
Technique d'attaque forçant un site Web à répercuter des données fournies par le client qui s'exécutent dans un navigateur Web d'un utilisateur.

socket Gestionnaire de communications utilisé par TCP/IP.

T

tache Données non sécurisées autorisées à circuler via le code.

triage Processus d'évaluation des constatations et de détermination de leur résolution.

X

XSS Voir script intersite.

Remarques

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 donne 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 également, à tout moment et sans préavis, apporter des améliorations et/ou des modifications aux produits et/ou programmes décrits sur le site.

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
2Z4A/101
11400 Burnet Road
Austin, TX 78758
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, des Conditions internationales d'utilisation des logiciels IBM ou de tout autre accord équivalent.

Les données de performance indiquées dans ce document ont été déterminées dans un environnement contrôlé. Par conséquent, les résultats peuvent varier de manière significative selon l'environnement d'exploitation utilisé. Certaines mesures évaluées sur des systèmes en cours de développement ne sont pas garanties sur tous les systèmes disponibles. En outre, elles peuvent résulter d'extrapolations. Les résultats peuvent donc varier. Il incombe aux utilisateurs de ce document de vérifier si ces données sont applicables à leur environnement d'exploitation.

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

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.

Tous les tarifs indiqués sont les prix de vente actuels suggérés par IBM et sont susceptibles d'être modifiés sans préavis. Les tarifs appliqués peuvent varier selon les revendeurs.

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

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

LICENCE DE COPYRIGHT :

Le présent logiciel contient des exemples de programmes d'application en langage source destinés à illustrer les techniques de programmation sur différentes plateformes d'exploitation. Vous avez le droit de copier, de modifier et de distribuer ces exemples de programmes sous quelque forme que ce soit et sans paiement d'aucune redevance à IBM, à des fins de développement, d'utilisation, de vente ou de distribution de programmes d'application conformes aux interfaces de programmation des plateformes pour lesquels ils ont été écrits ou aux interfaces de programmation IBM. Ces exemples de programmes n'ont pas été rigoureusement testés dans toutes les conditions. Par conséquent, IBM ne peut garantir expressément ou implicitement la fiabilité, la maintenabilité ou le fonctionnement de ces programmes. Vous avez le droit de copier, de modifier et de distribuer ces exemples de programmes sous quelque forme que ce soit et sans paiement d'aucune redevance à IBM, à des fins de développement, d'utilisation, de vente ou de distribution de programmes d'application conformes aux interfaces de programmation IBM.

Toute copie totale ou partielle de ces programmes exemples et des oeuvres qui en sont dérivées doit comprendre une notice de copyright, libellée comme suit :

© (nom de votre société) (année). Des segments de code sont dérivés des Programmes exemples d'IBM Corp. © Copyright IBM Corp. _indiquez l'année ou les années_. All rights reserved.

Si vous visualisez ces informations en ligne, il se peut que les photographies et illustrations en couleur n'apparaissent pas à l'écran.

Marques

IBM, le logo IBM et ibm.com sont des marques d'International Business Machines Corp. dans de nombreux pays. Les autres noms de produits et de services 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 à l'adresse www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript et toutes les marques incluant Adobe sont des marques d'Adobe Systems Incorporated aux Etats-Unis et/ou dans certains autres pays.

IT Infrastructure Library est une marque de The Central Computer and Telecommunications Agency qui fait désormais partie de The Office of Government Commerce.

Intel, le logo Intel, Intel Inside, le logo Intel Inside, Intel Centrino, le logo Intel Centrino, Celeron, Intel Xeon, Intel SpeedStep, Itanium, et Pentium sont des marques d'Intel Corporation ou de ses filiales aux Etats-Unis et dans certains autres pays.

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

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

ITIL est une marque de The Office of Government Commerce et est enregistrée au bureau américain Patent and Trademark Office.

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

Java ainsi que tous les logos et toutes les marques incluant Java sont des marques d'Oracle et/ou de ses filiales.

Cell Broadband Engine est une marque de Sony Computer Entertainment, Inc., aux Etats-Unis et/ou dans certains autres pays, et y est utilisé sous licence.

Linear Tape-Open, LTO, le logo LTO, Ultrium et le logo Ultrium sont des marques de HP, IBM Corp. et Quantum aux Etats-Unis et/ou dans certains autres pays.

Index

Caractères spéciaux

A

B

C

D

E

F

G

H

S

T

V

W