RSA NETWITNESS® SUITE

Guide des alertes basées sur ESA

pour la version 11.0

Informations de contact

RSA Link à l'adresse https://community.rsa.com contient une base de connaissances qui répond aux questions courantes et fournit des solutions aux problèmes connus, de la documentation produit, des discussions communautaires et la gestion de dossiers.

Marques commerciales

Pour obtenir la liste des marques commerciales de RSA, rendez-vous à l'adresse suivante : france.emc.com/legal/emc-corporation-trademarks.htm#rsa.

Contrat de licence

Ce logiciel et la documentation qui l'accompagne sont la propriété d'EMC et considérés comme confidentiels. Délivrés sous licence, ils ne peuvent être utilisés et copiés que conformément aux modalités de ladite licence et moyennant l'inclusion de la note de copyright ci-dessous. Ce logiciel et sa documentation, y compris toute copie éventuelle, ne peuvent pas être remis ou mis de quelque façon que ce soit à la disposition d'un tiers.

Aucun droit ou titre de propriété sur le logiciel ou sa documentation ni aucun droit de propriété intellectuelle ne vous est cédé par la présente. Toute utilisation ou reproduction non autorisée de ce logiciel et de sa documentation peut faire l'objet de poursuites civiles et/ou pénales.

Ce logiciel est modifiable sans préavis et ne doit nullement être interprété comme un engagement de la part d'EMC.

Licences tierces

Ce produit peut inclure des logiciels développés par d'autres entreprises que RSA. Le texte des contrats de licence applicables aux logiciels tiers présents dans ce produit peut être consulté sur la page de la documentation produit du site RSA Link. En faisant usage de ce produit, l'utilisateur convient qu'il est pleinement lié par les conditions des contrats de licence.

Remarque sur les technologies de chiffrement

Ce produit peut intégrer une technologie de chiffrement. Étant donné que de nombreux pays interdisent ou limitent l'utilisation, l'importation ou l'exportation des technologies de chiffrement, il convient de respecter les réglementations en vigueur lors de l'utilisation, de l'importation ou de l'exportation de ce produit.

Distribution

EMC estime que les informations figurant dans ce document sont exactes à la date de publication. Ces informations sont modifiables sans préavis.

février 2018

Sommaire

Mise en route avec ESA

Cette rubrique couvre les rubriques de démarrage rapide pour RSA NetWitness® Suite Event Stream Analysis (ESA) afin de vous permettre de vous mettre en route avec ESA. Les rubriques suivantes sont conçus pour vous aider à l'utilisation des règles de corrélation ESA.

- Les Bonnes pratiques vous permettent de comprendre comment bien configurer, déployer et créer des règles.
- Dépanner le service ESA vous aide à résoudre les différents aspects d'ESA, y compris le déploiement et la rédaction des règles.
- Afficher les metrics de mémoire des règles vous aide à travailler avec les metrics de mémoire pour comprendre l'utilisation de la mémoire pour les services ESA.

Il existe deux services ESA pouvant s'exécuter sur un hôte ESA :

- Event Stream Analysis (règles de corrélation ESA)
- Event Stream Analytics Server (ESA Analytics)

Le premier service est le service Event Stream Analysis qui crée des alertes à partir de règles ESA, également appelé ESA Correlation Rules, que vous créez manuellement ou téléchargez à partir de Live. Ce guide d'utilisation aborde les alertes à l'aide des règles de corrélation ESA. Pour plus d'informations sur la configuration des règles de corrélation ESA, reportez-vous à la section « Configurer les règles de corrélation ESA » du *Guide de configuration ESA*.

Le deuxième service est le service ESA Analytics, qui est utilisé pour la détection automatisée des menaces. Étant donné que le service ESA Analytics utilise des modules ESA Analytics préconfigurés pour la détection automatisée des menaces, vous n'avez pas besoin de créer ou de télécharger des règles pour l'utiliser. Pour plus d'informations sur le service ESA Analytics, reportez-vous au *Guide de détection automatisée des menaces* et à la section « Configurer ESA Analytics » dans le *Guide de configuration ESA*.

Bonnes pratiques

Les bonnes pratiques donnent des instructions pour vous aider à écrire, gérer et déployer des règles, et à conserver l'intégrité du système pour vos services ESA.

Comprendre les types de règles Event Stream Analysis

Le service Event Stream Analysis propose des fonctions avancées d'analytique des flux telles que le traitement des événements complexes et leur corrélation à hauts débits et faible latence. Il est capable de traiter de gros volumes de données d'événements disparates provenant des Concentrators. Toutefois, lorsque vous utilisez Event Stream Analysis, vous devez connaître les facteurs qui affectent l'utilisation des ressources afin de créer des règles efficaces.

Chaque événement reçu par ESA est évalué afin de déterminer s'il est susceptible de déclencher une règle. Il existe trois types de règles pouvant être déployées afin de déterminer ce que doit faire le moteur ESA avec l'événement entrant. Chacun de ces types de règles a un impact différent sur l'utilisation des ressources du système. Ces trois types de règles peuvent être créés via le Générateur de règles ou les règles EPL avancées, ou ils peuvent être téléchargés via RSA Live. Le tableau ci-dessous répertorie le type de règle et l'impact de cette règle sur les ressources du système.

Type de règle	Description
Règle de filtrage simple	Cette règle ne présente pas de corrélation avec les autres événements. Au moment de l'acquisition, cette règle est évaluée par rapport à un ensemble de conditions, et une alerte est générée si ces conditions sont remplies. Si aucune condition n'est remplie, l'événement est rapidement libéré par le moteur pour réduire l'utilisation de la mémoire. Ces règles ne consomment pas de mémoire car les événements ne sont pas retenus après l'évaluation initiale. L'utilisation des ressources mémoire n'augmentent pas avec le déploiement de nouvelles règles de filtrage simples. Toutefois, si la condition de filtrage est trop générique, il est possible que la règle déclenche de nombreuses alertes, ce qui pourrait avoir un impact sur les ressources système pour le stockage et la récupération de ces alertes. Par exemple, vous pourriez écrire une règle pour générer une alerte lorsque l'activité réseau HTTP arrive sur un port HTTP non standard.

Type de règle	Description
Règle liée à la fenêtre des événements	Cette règle évalue un ensemble d'événements par rapport à des conditions spécifiques sur une période de temps. Au moment de l'acquisition, la règle est évaluée par rapport à un ensemble de conditions. Si ces conditions sont remplies, l'événement est retenu en mémoire pendant une période spécifique. À la fin de cette période, les événements sont supprimés de la fenêtre de temps si le nombre d'événements collectés n'atteint pas le seuil à partir duquel une alerte est déclenchée. La consommation de mémoire de ces règles dépend largement du taux d'événements entrants (trafic), de la quantité de données par événement, et de la période spécifiée dans la fenêtre des événements. Chaque événement correspondant à ces critères est retenu en mémoire jusqu'à ce que la fenêtre de temps soit écoulée. Ainsi, plus la fenêtre de temps est étendue, plus le volume potentiel est élevé. Par exemple, vous pouvez écrire une règle qui génère une alerte si la connexion d'un utilisateur au système échoue cinq fois sur une période dix minutes.
Règle de séquence	Cette règle évalue une chaîne d'événements entrants afin de déterminer si la séquence des événements correspond à une condition particulière. Au moment de l'acquisition, la règle est évaluée par rapport à un ensemble de conditions. Si les conditions sont remplies, l'une des deux actions suivantes se produit : • S'il s'agit du premier événement de la séquence, une nouvelle thread d'événements est démarrée, et l'événement retenu vient en tête de séquence. • Si l'événement appartient à une thread d'événements existante, il est ajouté à cette séquence. Dans les deux cas, l'événement est retenu en mémoire. La quantité de ressources utilisées est particulièrement sensible à l'environnement client pour ce type de règle. Si la condition de filtrage génère de nombreuses threads, des ressources sont consommées pour chaque nouvelle thread (en plus de l'événement). En outre, si une thread d'événements ne se termine jamais (c'est-à-dire qu'une alerte n'est jamais générée), alors tout l'événement reste enregistré dans la mémoire de manière indéfinie. Par exemple, vous pouvez écrire une règle pour générer une alerte lorsque la connexion d'un utilisateur à un serveur échoue, qu'il effectue une connexion réussie, puis qu'il crée un nouveau compte.

En plus de l'utilisation de mémoire abordée plus haut, la génération d'alertes consomme également des ressources système. Chaque alerte générée doit être stockée pour être récupérée et traitée par NetWitness Respond. Ce processus utilise de l'espace disque pour le stockage, consomme de la mémoire de la base de données, et augmente l'utilisation du CPU pour exécuter les requêtes.

Lorsque vous écrivez et déployez des règles, vous devez savoir que chacune de ces actions a un « coût » en termes de ressources système. Les rubriques ci-dessous sont conçues pour vous aider à garder votre utilisation à un niveau sain, et à surveiller les problèmes en cas de surcharge des systèmes.

Bonnes pratiques pour l'écriture de règles

Voici les directives générales pour écrire des règles.

- **Créez des alertes pour les événements sur lesquels il est possible d'effectuer des actions.** L'objectif d'une alerte est de vous notifier d'un événement qui requiert une attention immédiate et spécifique. Pour les événements qui ne requièrent pas d'action de votre part, vous pouvez créer un rapport à titre informatif uniquement.
- **Configurez de nouvelles règles en tant que règles d'évaluation pour pouvoir observer leur réaction dans votre environnement.** Si vous déployez de nouvelles règles en tant que règles d'évaluation, elles seront désactivées si le seuil de mémoire configuré est dépassé. Vous pouvez également utiliser la fonction de snapshot mémoire pour connaître l'utilisation de la mémoire lorsqu'une règle d'évaluation est désactivée. Pour plus d'informations, consultez la rubrique Utiliser les règles d'évaluation.
- **Configurer les notifications d'alerte uniquement après votre règle de test et de réglage**. Cela peut vous éviter de recevoir un nombre trop important de notifications si le comportement d'une règle est différent de celui que vous attendez.
- **Les règles doivent être spécifiques pour que vous puissiez limiter l'utilisation des ressources.**. Utilisez les instructions suivantes pour limiter l'utilisation :
  - Assurez-vous que les filtres de la règle excluent tous les événements sauf ceux qui sont nécessaires au déclenchement précis de la règle.
  - Réduisez la taille de votre fenêtre de temps (pour la corrélation) autant que possible.
  - Limitez les événements que vous incluez dans la fenêtre : Par exemple, si vous ne souhaitez voir que les événements IDS, assurez-vous de n'inclure que les événements de votre fenêtre de temps.
- **Les règles doivent être affinées sur un niveau d'alerte gérable**. Si le nombre d'alertes est trop important, elles perdent leur objectif et leur utilité. Par exemple, vous souhaitez peut-être être informé du trafic chiffré vers d'autres pays. Mais vous pouvez limiter la liste aux pays à risque. Cela limite le volume des alertes à un niveau que vous pouvez gérer.

Bonnes pratiques pour l'utilisation de règles RSA Live

Voici les directives pour les règles RSA Live.

- **Déployez des règles RSA en petits lots**. Toutes les règles ne sont pas adaptées à tous les environnements. La meilleure façon de vérifier le succès de vos règles RSA Live est de les déployer par petits lots, de façon à les tester dans votre environnement. Si vous déployez de petits lots, il est bien plus facile de déceler les problèmes d'une règle particulière.
- **Lisez les descriptions de règle fournies par les règles RSA Live**. Les règles ESA ne sont pas « universelles ». Toutes les règles ne fonctionneront pas dans votre environnement. Les descriptions de règles vous indiquent les paramètres que vous devez modifier pour déployer correctement une règle dans votre environnement.
- **Définissez vos paramètres**. Les règles RSA Live disposent de paramètres qui doivent être modifiés. Si vous ne modifiez pas les paramètres, il est possible que la règle ne fonctionne pas ou qu'elle épuise votre mémoire.
- **Déployez de nouvelles règles en tant que règles d'évaluation afin d'observer leur réaction dans votre environnement.** Si vous déployez de nouvelles règles en tant que règles d'évaluation, elles seront désactivées si le seuil de mémoire configuré est dépassé. Pour plus de détails, reportez-vous à la rubrique Utiliser les règles d'évaluation.

Bonnes pratiques pour déployer des règles

Voici les directives générales pour déployer des règles.

- **Déployez les règles en petits lots pour pouvoir observer leur réaction dans votre environnement.** Tous les environnements ne sont pas identiques, et une règle devra être optimisée pour l'utilisation de la mémoire, le volume d'alertes et la détection efficace des événements.
- **Testez les règles avant de configurer des notifications d'alerte**. Configurez les notifications d'alerte uniquement après avoir terminé votre réglage et vos tests de règle. Cela peut vous éviter de recevoir un nombre trop important d'alertes si le comportement d'une règle est différent de celui que vous attendiez.
- **Surveiller la santé du système dans le cadre de votre processus de déploiement**. Lorsque vous déployez des règles, surveillez l'intégrité de votre système dans le cadre de votre processus de déploiement. Vous pouvez afficher l'utilisation totale de la mémoire de votre service ESA dans l'onglet Intégrité. Pour plus d'informations, consultez « Afficher les statistiques d'intégrité » dans Dépanner le service ESA.

Bonnes pratiques pour l'intégrité du système

Voici les directives générales pour l'intégrité du système.

- **Configurer de nouvelles règles en tant que règles d'évaluation**. Il arrive souvent que de nouvelles règles créent des problèmes de mémoire. Pour éviter cela, vous pouvez configurer les nouvelles règles comme règles d'évaluation. Si le seuil de mémoire configuré est atteint, toutes les règles d'évaluation sont désactivées pour éviter que le système ne manque de mémoire. Pour plus d'informations sur les règles d'évaluation, reportez-vous à la rubrique Utiliser les règles d'évaluation.
- **Configurer des seuils dans le module État de santé pour vous alerter si l'utilisation de la mémoire est trop élevée**. Certaines metrics du module Intégrité effectuent le suivi de l'utilisation mémoire. Vous pouvez configurer des alertes et notifications pour vous envoyer un email lorsque ces seuils sont dépassés. Pour plus d'informations sur les statistiques de la mémoire, consultez « Afficher les statistiques d'intégrité » dans Dépanner le service ESA.
- **Surveillez les métriques de mémoire pour chaque règle dans le module Health & Wellness**. Pour chaque règle, vous pouvez afficher l'utilisation de mémoire estimée dans le module Health & Wellness. Vous pouvez utiliser ces informations pour garantir que les règles n'utilisent pas trop de mémoire. Pour plus d'informations sur les statistiques de la mémoire, consultez « Afficher les statistiques d'intégrité » dans Dépanner le service ESA.

Dépanner le service ESA

Cette rubrique décrit les problèmes courants qui peuvent survenir lors de l'utilisation d'ESA, et propose des solutions usuelles à ces problèmes.

Résoudre les problèmes liés aux services ESA

Problème	Causes possibles	Solutions
Dans le tableau de bord NetWitness Suite, le service ESA s'affiche en rouge pour indiquer qu'il est hors ligne. Dans la vue **CONFIGURER** > **Règles ESA**, le message suivant apparaît : « Le service est hors ligne ou inaccessible. »	plusieurs pages	Lorsqu'un service ESA est hors ligne, cela peut être dû à de nombreuses causes. Cependant, bien souvent, le problème vient du fait que vous avez créé une règle qui utilise trop de mémoire, ce qui provoque l'échec du service ESA. Pour résoudre ce problème, reportez-vous à Étapes de résolution des problèmes de mémoire d'un service ESA hors ligne. Parmi les autres causes usuelles, il est possible que votre pare-feu bloque la connexion entre ESA et NetWitness Suite, ou que la machine hébergeant le service ESA soit en panne.
		Pour activer les services ESA : Dans **ADMIN** > **Services**, sélectionnez l'icône Actions  pour votre service ESA, puis choisissez **Démarrer**. Si votre service ESA s'arrête et redémarre en boucle, vous pouvez avoir à appeler le Support Clients pour faire redémarrer les services.

Problème	Causes possibles	Solutions
Après une mise à niveau effectuée récemment, le service ESA s'affiche en rouge dans le tableau de bord NetWitness Suite pour indiquer qu'il est hors ligne. Dans la vue **CONFIGURER** > **Règles ESA**, le message suivant apparaît : « Le service est hors ligne ou inaccessible. »	Problèmes liés à la configuration	Si votre système a été mis à niveau récemment, vous avez peutêtre commis une erreur de configuration. Sous **ADMIN** > **Services**, sélectionnez votre service ESA, puis cliquez sur **Modifier le service**. Dans le champ Modifier le service, cliquez sur Tester la connexion. Si la connexion n'aboutit pas, cela est dû probablement à une erreur de configuration de votre part. Tentez de corriger votre erreur de configuration, puis réessayez.
L'exécution du service ESA semble lente.	Problèmes liés à la configuration	Vous pouvez améliorer les performances en modifiant la mémoire tampon (la valeur par défaut est *1 048 576 octets*), ou en définissant le paramètre TCP sur TCPNoDelay pour empêcher le retard de réception des accusés TPC. Vous pouvez modifier ces paramètres (*readBufferSize* et *tcpNoDelay*) en accédant à */Workflow/Source/nextgenAggregation* dans la vue Explorer.

Résoudre les problèmes liés aux règles RSA Live pour ESA

Problème	Causes possibles	Solutions
J'ai importé un groupe de règles à partir de RSA Live, et maintenant mon service ESA se bloque. Pourquoi ?	Vous n'avez peut-être pas configuré les paramètres nécessaires pour rendre la règle RSA Live compatible avec votre environnement.	Chaque règle RSA Live comporte une description qui inclut les paramètres à configurer et les conditions préalables pour votre environnement. Consultez cette description pour déterminer si la règle est appropriée à votre environnement. Pour garantir le déploiement des règles en toute sécurité dans votre environnement, configurez les nouvelles règles en tant que règles d'évaluation afin de les tester dans votre environnement. Grâce aux règles d'évaluation, vous pouvez tester les nouvelles règles sans danger. Pour plus d'informations sur ce point, reportez-vous à Déployer des règles en tant que règles d'évaluation.

Problème	Causes possibles	Solutions

J'ai importé un groupe de règles à partir de RSA Live et, alors que ces règles avaient été déployées sans erreur, elles ont été désactivées ensuite.	Les règles RSA Live ne sont pas toutes destinées à chaque environnement. Vous n'avez peut-être pas les métas correctes dans votre service ESA pour exécuter la règle.	Vous pouvez vérifier qu'une règle a été désactivée en accédant à **CONFIGURER > Règles ESA > Services > Statistiques de règles déployées**. Si la règle est désactivée, l'icône verte ne s'affiche pas en regard de celle-ci.
		
		Si une règle déployée correctement a été désactivée, recherchez les exceptions liées à cette règle dans les logs. Plus précisément, vérifiez si les règles ont été désactivées à cause de métadonnées manquantes. Pour ce faire, accédez à **ADMIN** > **Services,** sélectionnez votre service ESA, puis  > **Vue** > **Logs**.
		
		Recherchez ensuite un message similaire au message suivant :
		
		`"Property named '<meta_name>' is not valid in any stream"`
		
		Par exemple, vous pouvez voir :
		
		`Failed to validate filter expression '(medium=1 and streams=2 or medium=3...(238 chars)': Property named 'tcp_flags_seen' is not valid in any stream`
		
		Si un message similaire s'affiche, vous devrez peut-être ajouter une clé méta personnalisée au Log Decoder ou Concentrator. Pour ce faire, suivez ces instructions : « Créer des clés méta personnalisées à l'aide d'un feed personnalisé » dans le *Guide de configuration de Decoder et Log Decoder*.

Résoudre les problèmes de déploiement

Problème	Causes possibles	Solutions
J'ai créé une règle, et j'ai vérifié la syntaxe. La règle semblait correcte. Lorsque j'ai déployé la règle, j'ai obtenu une erreur. Pourquoi ?	Vous n'avez peut-être pas de méta correct pour déployer la règle.	Consultez les références des clés méta. Vous n'avez peut-être pas de méta correct pour déployer la règle.

Résoudre les problèmes liés aux règles

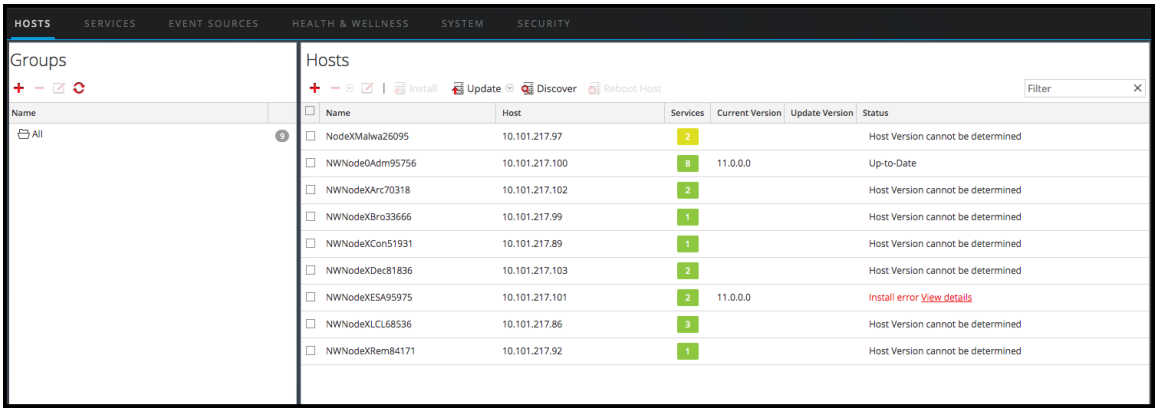
Problème	Causes possibles	Solutions
J'ai créé une règle personnalisée (via le Générateur de règles ou l'EPL avancé), et ma règle ne se déclenche pas. Pourquoi ?	Vous avez peutêtre des problèmes de connectivité.	Vérifiez la statistique « Taux fourni » sous l'onglet **CONFIGURER** > **Règles ESA** > **Services**. Si le taux fourni est égal à zéro, cela signifie que le service ESA ne reçoit pas de données de la part des composants Concentrator. Validez la connectivité du Concentrator. Accédez à **ADMIN** > **Services**, sélectionnez votre ESA, puis cliquez sur **Vue** > **Configuration**. Assurez-vous que le concentrator est activé. Sélectionnez le concentrator, puis cliquez sur **Tester la connexion**. Si le taux fourni n'est pas égal à zéro, le nom et le type de clé méta utilisés dans la règle ne correspondent probablement pas aux valeurs de la clé méta présente dans les événements. Vérifiez la validité du nom et du type de clé méta utilisés dans la règle en recherchant le nom de la clé méta sous l'onglet **CONFIGURER** > **Règles ESA** > **Paramètres** (recherche des références de clés méta).

Problème	Causes possibles	Solutions
	La règle pose peut-être un problème.	**Si une règle spécifique ne se lance pas**, accédez à **CONFIGURER** > **Règles ESA** > **Services** afin de voir si la règle a été désactivée. Dans la rubrique **Statistiques de règles déployées**, une règle désactivée affiche un bouton d'activation vide (au lieu du bouton d'activation vert). Vous pouvez également vérifier le champ Correspondances d'événements. Accédez à **CONFIGURER** > **Règles ESA** > **Services**. Ensuite, vous pouvez voir le nombre d'événements associés dans la colonne **Correspondances d'événements**. En l'absence de correspondances d'événements, assurez-vous que la logique de votre règle ne comporte pas d'erreurs. Par exemple, recherchez les erreurs de majuscules ou de minuscules dans la syntaxe, puis vérifiez la période. Si la règle ne se déclenche toujours pas, simplifiez sa logique pour voir si elle se déclenche en étant moins complexe.

Étapes de résolution des problèmes de mémoire d'un service ESA hors ligne

Étape 1 : Vérifier que votre hôte est en cours d'exécution

La première étape de résolution des problèmes consiste à vérifier si votre hôte est en cours d'exécution. Pour ce faire, accédez à **ADMIN**> **HÔTES**. Si l'hôte est en panne, les paramètres du système ne s'affichent pas (la mise à jour des informations de l'hôte peut parfois être retardée), les **Services** s'affichent en rouge, et le champ **Mises à jour** affiche un message d'erreur.



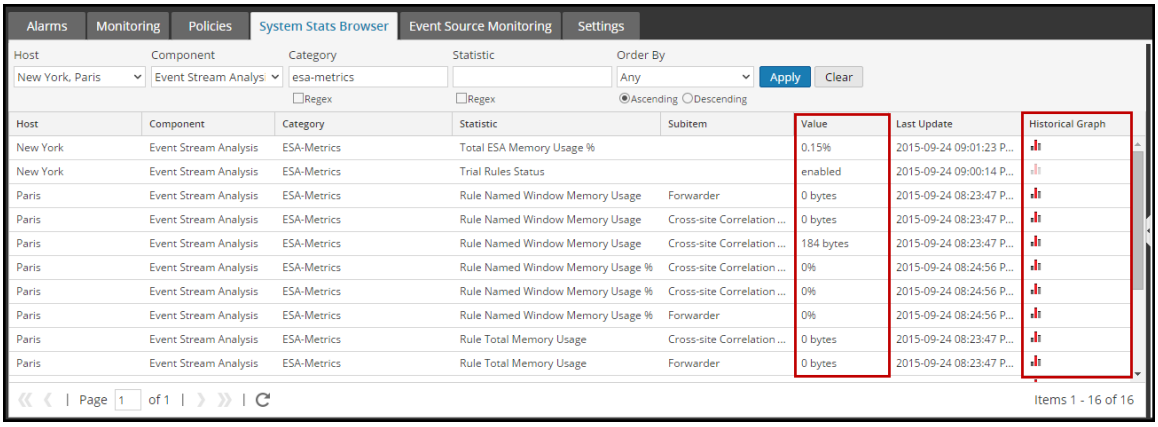
Si l'hôte est en panne, contactez votre administrateur NetWitness Suite pour le redémarrer. Sinon, passez à l'étape 2.

Étape 2 : Afficher les statistiques détaillées dans Intégrité

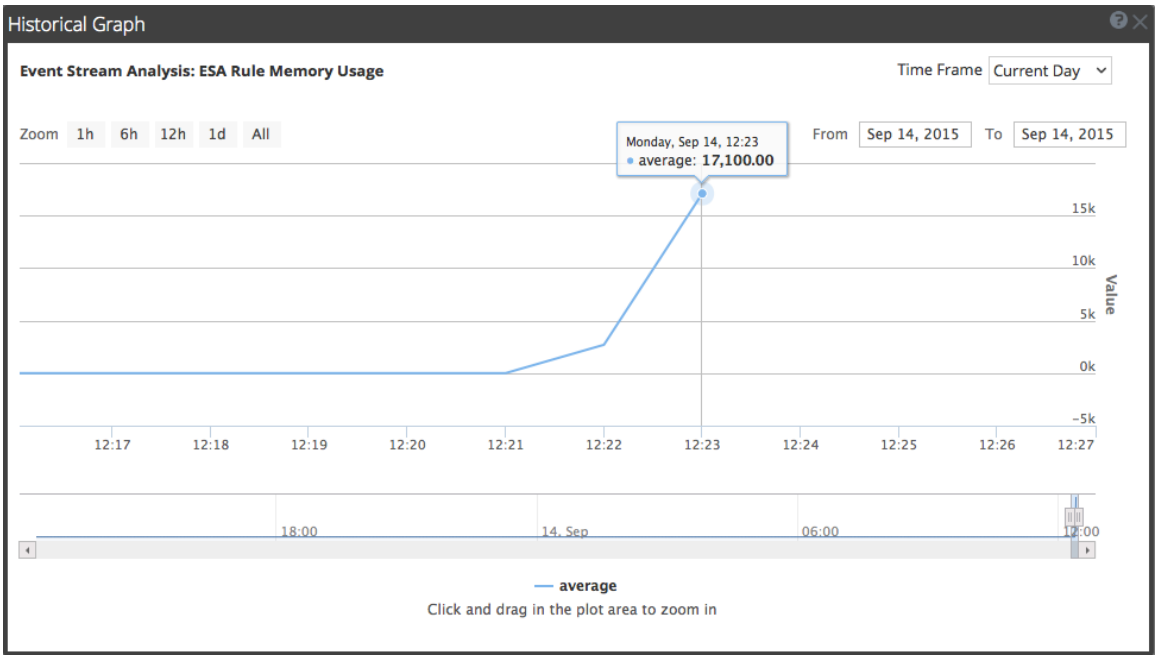
Une fois que vous êtes sûr que le service ESA est en panne, accédez à Intégrité pour voir où se produisent les problèmes potentiels. Le plus souvent, le problème vient du fait que le service ESA dépasse les seuils de mémoire, ce qui entraîne l'arrêt ou l'échec de son exécution.

1. Accédez à **ADMIN** > **Intégrité** > **Alarmes** pour voir si ESA a déclenché des alarmes. Recherchez les alarmes suivantes :
   - Utilisation de la mémoire totale par ESA > 85 %
   - Utilisation de la mémoire totale par ESA > 95 %
   - Service ESA arrêté
2. Allez à **ADMIN** > **Intégrité** > **Navigateur Stat. système** pour afficher les metrics de mémoire des performances de chaque règle. Pour afficher les métriques, renseignez les champs suivants :

Hôte	Composant	Catégorie
<votre hôte>	Event Stream Analysis	esa-metrics



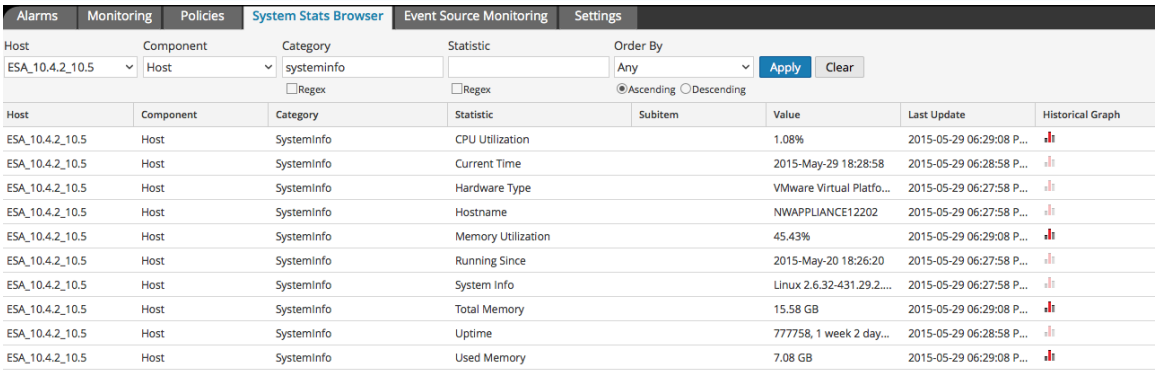
La mémoire de chaque règle est affichée dans la colonne **Valeur** et la valeur apparaît en octets. Vous pouvez afficher une vue historique de l'utilisation de la mémoire dans la colonne **Graphique historique**.



3. Accédez à **ADMIN** > **Intégrité** > **Navigateur Stat. Système** pour voir le détail des performances du service ESA. Sélectionnez votre hôte, puis utilisez les filtres suivants pour afficher les statistiques ciaprès :

Hôte	Composant	Catégorie	Statistiques	Exemple
<votre hôte>	Hôte	SystemInfo	Utilisation du CPU	1,08 %
<votre hôte>	Hôte	SystemInfo	Utilisation de mémoire	45,43 %
<votre hôte>	Hôte	SystemInfo	Mémoire utilisée	7,08 Go
<votre hôte>	Hôte	SystemInfo	Mémoire totale	15,58 Go
<votre hôte>	Hôte	SystemInfo	Uptime	77758, 1 semaine, 2 jours...
<votre hôte>	Event Stream Analysis	ProcessInfo	Utilisation de mémoire	7,07 Go

Hôte	Composant	Catégorie	Statistiques	Exemple
<votre hôte>	Event Stream Analysis	ProcessInfo	Utilisation du CPU	0,2 %
<votre hôte>	Event Stream Analysis	JVM.Memory	all	Utilisation de mémoire par segments validée 8 Go
<votre hôte>	Event Stream Analysis	Métriques ESA	% d'utilisation de la mémoire totale par ESA	4,64 %



Si vous rencontrez un problème d'utilisation de la mémoire ou du CPU, passez à l'étape 3.

Étape 3 : Activez les services ESA

1. Dans **ADMIN** > **Services**, sélectionnez l'icône Actions  du service ESA, puis choisissez **Démarrer**.
2. Revenez au service ESA pour identifier les règles qui sont à l'origine des problèmes de mémoire.

Si votre service ESA s'arrête et redémarre en boucle, vous pouvez avoir à appeler le Support Clients pour faire redémarrer les services.

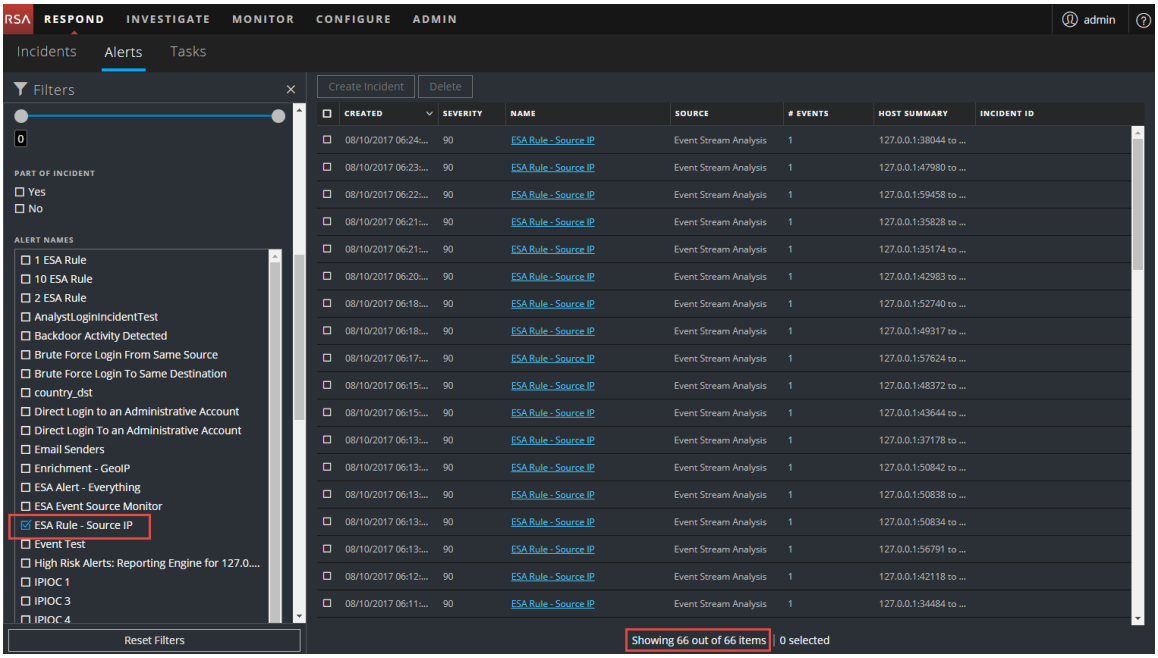
Si vous pouvez démarrer le service ESA sans qu'il s'arrête, passez à l'étape 4.

Étape 4 : Vérifier le volume d'alertes et d'événements

Une fois que vous êtes parvenu à redémarrer le service ESA sans qu'il s'arrête immédiatement, consultez les statistiques de vos règles pour voir quelles sont celles qui consomment trop de ressources. Parfois, l'exécution des services ESA échoue, car une règle génère un trop grand nombre d'alertes ou d'événements. Vérifiez ces deux aspects, si vous avez déterminé que l'utilisation de la mémoire est bien la cause de l'arrêt du service ESA.

Afficher les récapitulatifs des alertes

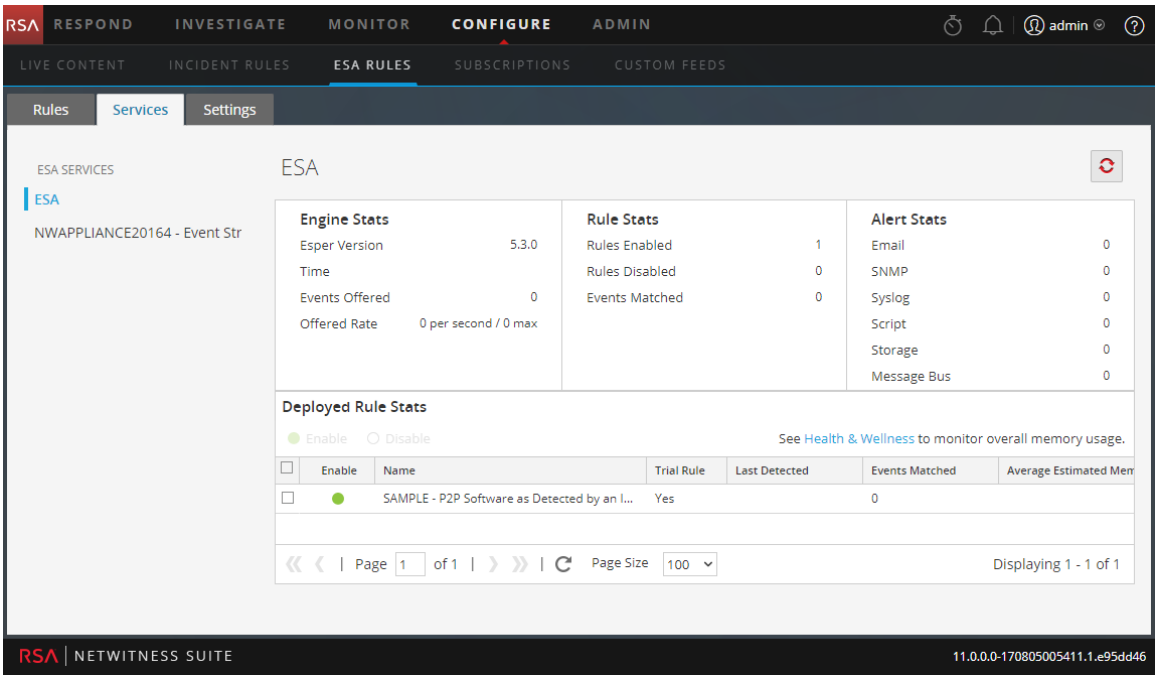
Les règles qui génèrent un volume élevé d'alertes peuvent submerger le système, et entraîner l'échec de son exécution ou provoquer son redémarrage. Pour afficher les récapitulatifs des alertes, accédez à **RÉPONDRE > Alertes**. Dans le panneau **Filtres** à gauche, dans la rubrique **NOMS D'ALERTE**, sélectionnez le nom de l'alerte pour la règle. Le nombre d'alertes portant le même nom s'affiche au bas des résultats de la liste des alertes. Si le nombre est trop élevé pour une règle spécifique, désactivezła, puis réécrivezła afin de la rendre plus efficace.



Pour effacer le filtre, cliquez sur **Réinitialiser les filtres**.

Afficher les correspondances d'événements

Parfois, une règle correspond à un trop grand nombre d'événements, ce qui entraîne une consommation excessive de la mémoire. Cela se produit habituellement si vous créez une période étendue, où un grand nombre d'événements s'accumule sans déclencher d'alerte. Il s'agit d'un problème puisque chaque événement est stocké en mémoire pendant que la règle attend que l'alerte se déclenche. Pour vérifier ce problème, accédez à **CONFIGURER > Règles ESA > Services.** À partir de là, vous pouvez voir le nombre d'événements mis en correspondance dans la colonne **Correspondances d'événements**. Si un grand nombre d'événements correspond à une règle donnée, vous pouvez analyser la règle afin de voir si vous pouvez l'optimiser.



Étape 5 : Désactiver et réparer la règle à l'origine des problèmes

Une fois que vous avez déterminé les règles à réécrire, désactivez-les et réécrivez-les afin qu'elles ne génèrent pas un volume aussi élevé d'alertes ou d'événements. Pour plus d'informations sur la façon d'écrire des règles plus efficaces, reportez-vous à la rubrique Bonnes pratiques.

Désactiver des règles

1. Pour désactiver des règles, accédez à **CONFIGURER** > **Règles ESA** > **Services**, puis sélectionnez les règles à désactiver dans le champ **Statistiques de règles déployées**.
2. Pour désactiver les règles, sélectionnez **Désactiver**.

Modifier des règles

1. Pour réparer les règles, accédez à **CONFIGURER** > **Règles ESA** > **Règles**> **Bibliothèque de règles**. Sélectionnez la règle à modifier, puis cliquez sur l'icône Actions  .
2. Sélectionnez **Modifier**.
3. Modifiez la règle pour la rendre plus efficace. Pour obtenir des instructions sur la création des règles, reportez-vous à Ajouter des règles à la Bibliothèque de règles
4. Une fois que vous êtes satisfait de votre règle, vous pouvez l'enregistrer en tant que règle d'évaluation pour vous assurer que les problèmes de mémoire n'affectent pas les

performances du service ESA. Pour ce faire, suivez les étapes répertoriées dans la rubrique Utiliser les règles d'évaluation.

Activer des règles

1. Pour activer des règles, accédez à CONFIGURER > **Règles ESA** > **Services**, puis sélectionnez les règles à activer dans le champ **Statistiques de règles déployées**.
2. Pour activer les règles, sélectionnez **Activer**.

(Facultatif) Consulter les fichiers log ESA pour plus d'informations

Une fois que vous avez constaté que des services sont à l'arrêt, et que vous avez passé en revue certaines causes possibles de dysfonctionnement du système, vérifiez si ces services ne s'arrêtent pas et ne redémarrent pas en boucle. Pour ce faire, accédez aux logs ESA. À partir de la vue **ADMIN** > **Services**, sélectionnez votre service ESA, puis > **Vue** > **Logs**.

Si vous ne pouvez pas accéder aux logs ESA à partir de l'interface NetWitness Suite, connectez-vous au système via SSH, puis accédez à `opt/rsa/esa/logs/esa.log`.

Afficher les metrics de mémoire des règles

Cette rubrique indique aux writers de la règle ESA comment afficher les metrics de mémoire des règles. Vous pouvez voir une estimation de l'utilisation de la mémoire pour chaque règle s'exécutant sur un serveur. De plus, vous pouvez utiliser ces informations pour modifier vos instructions et conditions relatives aux règles, si elles utilisent trop de mémoire.

Les règles peuvent parfois consommer plus de mémoire que prévu, ce qui entraîne le ralentissement ou l'arrêt d'ESA. Pour voir approximativement la quantité de mémoire utilisée par une règle, vous pouvez configurer des metrics de mémoire. Les metrics de mémoire vous permettent d'afficher une estimation de l'utilisation de la mémoire pour chaque règle dans le navigateur des statistiques système d'intégrité (vous aurez donc besoin d'autorisations pour accéder à ce module). Vous pouvez utiliser ces informations pour modifier vos règles de manière optimale.

À un niveau élevé, vous devrez effectuer les étapes suivantes pour utiliser les metrics de mémoire afin de résoudre les problèmes d'utilisation de la mémoire des règles :

1. Assurez-vous que la fonction des metrics de mémoire est activée (via Explorateur > CEP > Metrics > EnableStats). La fonction des metrics de mémoire est activée par défaut.
2. Vérifiez que vous disposez des autorisations nécessaires pour afficher le module Intégrité. Pour plus d'informations sur les rôles et autorisations, consultez la rubrique Autorisations du rôle.
3. Affichez les statistiques relatives à la mémoire dans Intégrité.

4. (Recommandé) Configurez les politiques d'intégrité ESA pour envoyer un e-mail si les seuils de mémoire sont dépassés. Consultez la rubrique « Gérer les règles » dans le *Guide de maintenance du système* pour obtenir des instructions sur l'envoi de notifications par e-mail.
5. Si nécessaire, utilisez les données des metrics de mémoire pour modifier les règles afin de les rendre plus efficaces.

Conditions préalables

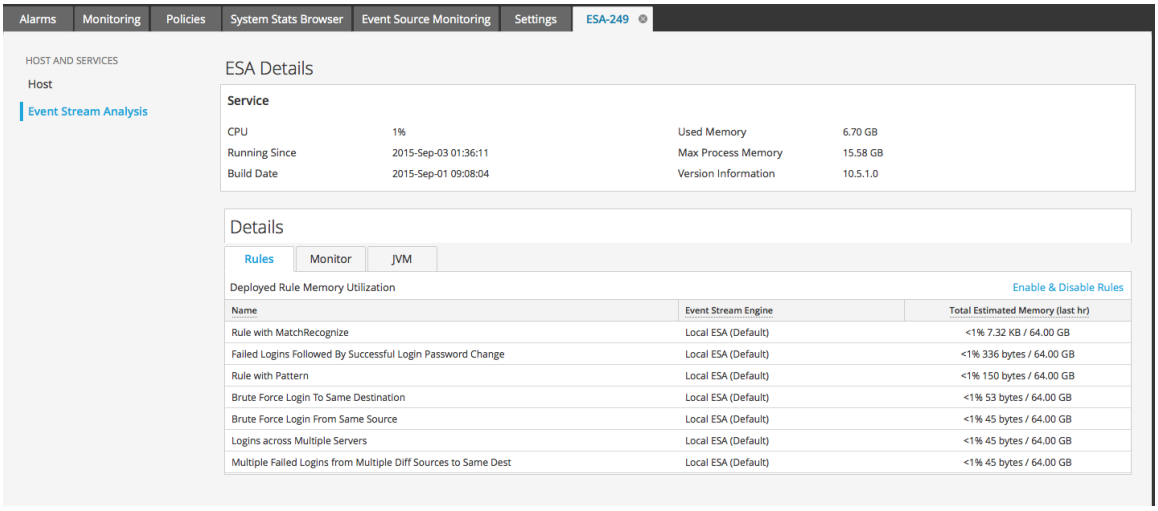
Voici les conditions requises pour l'utilisation des metrics de mémoire :

- La fonction des metrics de mémoire est activée (via **Explorateur** > **CEP** > **Metrics** > **EnableStats**).
- L'utilisateur doit disposer des autorisations appropriées pour afficher les statistiques d'intégrité.
- (Recommandé) Configurez la politique d'intégrité ESA pour envoyer un e-mail lorsque les seuils de mémoire sont dépassés.

Procédures

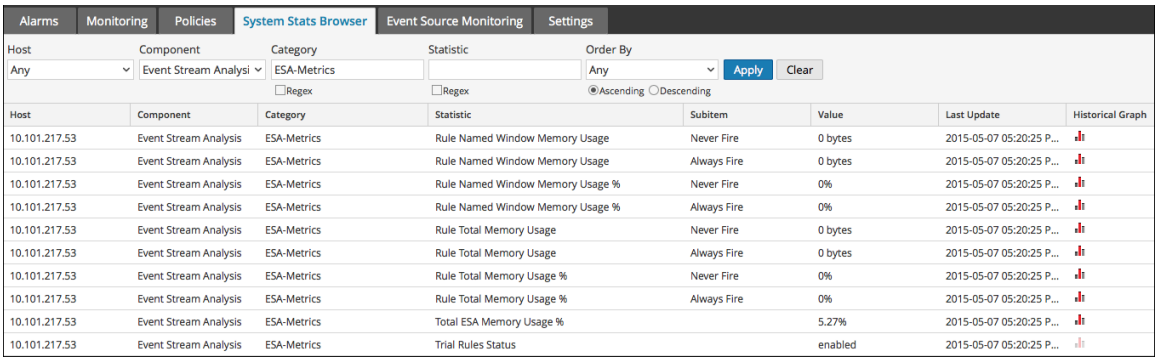
Afficher les metrics de mémoire dans le module de surveillance de l'intégrité du système

1. Accédez à **ADMIN** > **Intégrité** > **Surveillance**
2. Affichez les informations détaillées relatives à votre service ESA.
3. Cliquez sur l'onglet **Règles**.
4. Vous pouvez afficher l'utilisation moyenne de la mémoire pour chaque règle exécutée au cours de l'heure précédente.



Afficher les metrics de mémoire dans le navigateur des statistiques système d'intégrité

1. Accédez à **ADMIN** > **Intégrité** > **Navigateur Stat. système**.
2. Pour le composant, sélectionnez **Event Stream Analysis**. Pour la catégorie, saisissez **ESA-Metrics**.



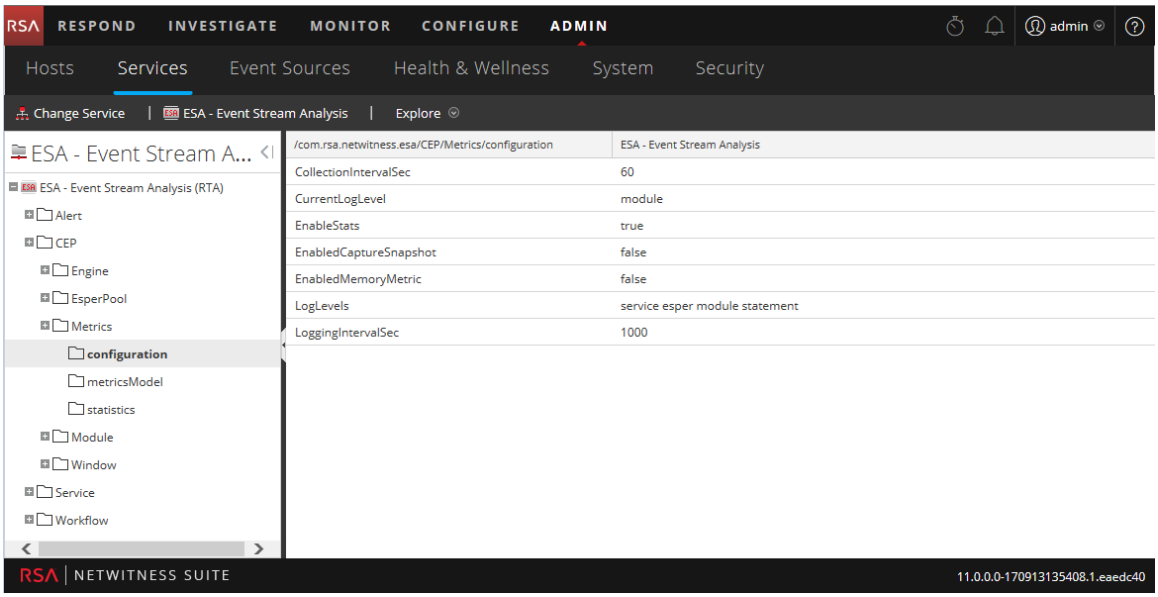
Host	Component	Category	Statistic	Subitem	Value	Last Update	Historical Graph
10.101.217.53	Event Stream Analysis	ESA-Metrics	Rule Named Window Memory Usage	Never Fire	0 bytes	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Rule Named Window Memory Usage	Always Fire	0 bytes	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Rule Named Window Memory Usage %	Never Fire	0%	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Rule Named Window Memory Usage %	Always Fire	0%	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Rule Total Memory Usage	Never Fire	0 bytes	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Rule Total Memory Usage	Always Fire	0 bytes	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Rule Total Memory Usage %	Never Fire	0%	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Rule Total Memory Usage %	Always Fire	0%	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Total ESA Memory Usage %		5.27%	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Trial Rules Status		enabled	2015-05-07 05:20:25 P...	

   Le nom de la règle s'affiche dans le champ **Sous-élément** et l'utilisation de la mémoire s'affiche dans la colonne **Valeur**.
3. Pour afficher l'historique d'utilisation de la mémoire d'une règle, cliquez sur l'icône **Graphique de l'historique**.

Remarque : Le champ **Dernière mise à jour** indique quand Intégrité interroge ESA. Toutefois, les metrics de mémoire ne sont pas synchronisés avec l'interrogation d'Intégrité. Par exemple, si le seuil de mémoire est dépassé le 10/10/15 à 12h00, et si Intégrité interroge le 10/10/15 à 12h10, le champ **Dernière mise à jour** affiche l'horodatage 10/10/15 à 12h10.

Activer ou désactiver la fonction des metrics de mémoire

1. Accédez à **ADMIN** > **Services** et sélectionnez votre ESA.
2. Une fois votre ESA sélectionné, cliquez sur **Actions** > **Afficher** > **Explorer**, puis accédez à **CEP > Metrics** > **Configuration** comme illustré ci-dessous.



3. Modifiez le champ EnabledStats en lui affectant la valeur **true** ou **false**, si vous souhaitez activer ou désactiver la fonction des metrics de mémoire.

Mode de génération d'alertes par ESA

Cette rubrique fournit une brève description du mode d'exécution des règles par un service ESA (Event Stream Analysis) pour générer des alertes. Le service ESA (Event Stream Analysis) exécute des règles qui spécifient des critères de comportement problématique ou d'événements menaçants sur votre réseau. Lorsqu'ESA détecte une menace correspondant aux critères des règles, il génère une alerte.

Pour générer des alertes, ESA effectue les actions suivantes :

1. Rassemblement des données
2. Exécution des règles ESA par rapport aux données
3. Capture d'événements qui répondent aux critères des règles
4. Génération d'alertes pour ces événements capturés

Vous pouvez utiliser le module Alertes pour bénéficier d'une meilleure visibilité du réseau et détecter les problèmes.

Données sensibles

Cette rubrique explique la façon dont ESA traite des données sensibles, comme des noms d'utilisateur ou une adresse IP, qu'il reçoit des services Core. Le rôle du responsable de la confidentialité des données peut identifier les clés méta qui contiennent des données sensibles et doivent afficher des données obfusquées. ESA n'affichera et ne stockera pas les métadonnées sensibles. Par conséquent, ESA ne transmettra pas les données sensibles de NetWitness Respond.

ESA peut également ajouter une version obfusquée des données sensibles à un événement. Par exemple, le DPO identifie user_dst comme étant sensible. ESA peut ajouter une version obfusquée, telle que user_dst_hash, à un événement. Les métadonnées obfusquées ne sont pas sensibles ; ESA les affichera et stockera donc de la même façon que toute autre métadonnée non sensible.

Pour plus d'informations sur la stratégie et les avantages de l'obfuscation des données, voir le *Guide de gestion de la confidentialité des données*.

La rubrique qui suit aborde les points suivants :

- La façon dont ESA traite les données sensibles qu'il reçoit des services Core
- La façon d'éviter les fuites de données sensibles dans une règle EPL avancée

La façon dont ESA traite les données sensibles qu'il reçoit des services Core

Lorsqu'ESA reçoit des données sensibles des services Core, ESA ne transmet que la version obfusquée des données. ESA ne stocke et n'affiche pas les données sensibles.

Les fonctionnalités suivantes sont impactées :

- Résultats – ESA ne transfère pas de données confidentielles aux résultats, comprenant les alertes, les notifications et le stockage MongoDB.
- Règles EPL avancées – Si une instruction EPL crée un alias pour une clé méta confidentielle, une fuite de données confidentielles est possible. Cette rubrique illustre la façon dont ce problème se produit afin que vous puissiez l'éviter.
- Enrichissements – Si une clé méta confidentielle est utilisée dans la condition join, une fuite de données confidentielles est possible. Cette rubrique illustre la façon dont ce problème se produit afin que vous puissiez l'éviter.

Règle EPL avancée

Si une instruction de requête EPL renomme une clé méta sensible, les données ne seront pas protégées.

ESA identifie une clé méta sensible par le nom :

ip_src est la clé méta sensible.
ip_src_hash est la version obfusquée non sensible.

Pour soutenir la confidentialité des données, la clé méta sensible ne doit pas être renommée dans une requête EPL. Si une métaclé sensible est renommée, les données ne seront plus protégées.

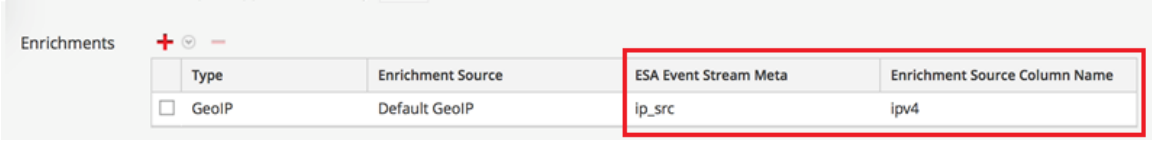
Par exemple, dans une règle telle que select ip_src as ip_alias..., ip_alias contient les données sensibles mais n'est pas protégé car ESA ne connaît qu'ip_src, et non ip_alias. Dans ce cas, les adresses IP ne seraient pas obfusquées. Les valeurs réelles seraient affichées.

Source d'enrichissement

Lorsqu'une métaclé sensible est utilisée dans une condition join, les données sensibles peuvent être affichées.

La base de données d'enrichissement, qui est l'autre partie de la condition join, possède une colonne qui correspond à la métaclé sensible. Cette référence croisée se rapporte aux valeurs réelles, et non à celles illisibles. Par conséquent, les valeurs réelles s'affichent.

Dans l'exemple suivant, les deux parties de la condition join sont mises en évidence.



- ip_src contient des données sensibles.
- ipv4 sera ajouté à l'alerte et exposé en tant que données non sensibles

La valeur ipv4 étant identique à la valeur ip_src, ipv4 contient et affiche des données sensibles.

Types de règles ESA

Cette rubrique décrit chaque type de règle ESA, le moment auquel l'utiliser et les autorisations associées à chaque rôle. Le tableau ci-dessous répertorie chaque type, fournit une description et explique quand l'utiliser.

Type de règle	Description	Utilité
Générateur de règles	Dans le générateur de règles, vous définissez les critères de règle dans une interface simple d'utilisation.	Utilisez le générateur de règles pour créer vos premières règles. Choisissez plusieurs conditions de règle dans les listes.
EPL avancé	Event Processing Language (EPL) vous permet de définir des critères de règle en écrivant une requête.	Utilisez les règles EPL avancées pour définir des critères de règle dans la syntaxe EPL.
ESA de RSA Live	RSA Live contient un catalogue de règles ESA que vous pouvez télécharger et modifier pour les exécuter sur votre réseau.	Téléchargez les règles ESA de RSA Live pour utiliser les règles déjà créées. Modifiez les paramètres configurables à personnaliser pour répondre à vos besoins.

Règles prédéfinies

Quelques exemples de règles Générateur de règles sont fournis avec NetWitness Suite et s'affichent dans la Bibliothèque de règles. Utilisez les règles prédéfinies pour vous familiariser avec les règles avant de créer les vôtres. Vous pouvez modifier et déployer ces exemples de règles en toute sécurité.

Mode Règles d'évaluation

Pour tout type de règle, vous pouvez sélectionner le paramètre Règle d'évaluation pour plus de sécurité. Les règles d'évaluation sont désactivées si elles dépassent le seuil de mémoire défini par l'administrateur. Exécutez une règle en mode d'évaluation pour contrôler l'utilisation de la mémoire et désactiver automatiquement la règle si elle dépasse le seuil de mémoire autorisé.

Autorisations du rôle

Cette rubrique répertorie toutes les autorisations ESA et indique les autorisations attribuées à chaque rôle NetWitness Suite préconfiguré. L'accès des utilisateurs est limité selon les rôles et les autorisations attribuées aux rôles.

- Administrateurs
- Opérateurs
- Analyste
- Responsables du Security Operations Center (SOC)
- Analystes du malware
- Responsable de la confidentialité des données

Il existe quatre autorisations pour ESA :

1. Accéder au module Alerting – Obligatoire pour toutes les autorisations
2. Afficher les règles – Permet d'accéder aux règles de la Bibliothèque de règles en mode affichage seulement
3. Afficher les alertes – Permet d'accéder aux alertes en mode affichage seulement pour les alertes générées par ESA
4. Gérer les règles – Vous permet d'afficher, de créer, de modifier et de supprimer des règles

Le tableau suivant répertorie les autorisations pour ESA et les rôles auxquels elles sont attribuées. Utilisez ce tableau pour voir comment chaque rôle peut utiliser les règles et les alertes.

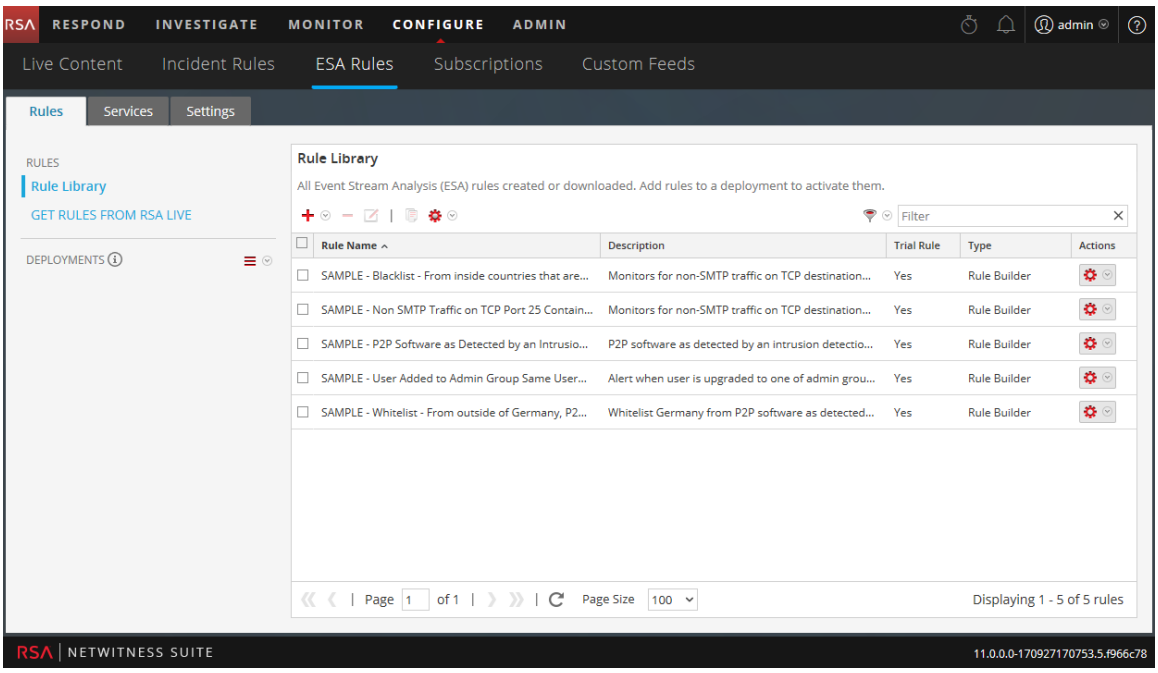
Autorisation	Administrateurs	Opérateurs	Analystes	Gest. SOC	MA	DPO
Accéder au module Alerting	Oui	Oui	Oui	Oui		Oui
Afficher les règles	Oui	Oui		Oui		Oui
Afficher les alertes	Oui		Oui	Oui		Oui
Gérer les règles	Oui	Oui		Oui		Oui

Pour plus d'informations sur les rôles et les autorisations, reportez-vous à la rubrique *Guide de la sécurité du système et de la gestion des utilisateurs*.

S'entraîner avec les règles prédéfinies

NetWitness Suite est livré avec deux règles prédéfinies qui permettent aux analystes de se familiariser avec les règles avant de commencer à en créer. Utilisez ces règles pour apprendre à utiliser le Générateur de règles, et à modifier et déployer une règle.

Les règles prédéfinies sont installées dans la Bibliothèque de règles, qui contient toutes les règles que vous téléchargez ou créez. La figure ci-dessous présente des exemples de règles de la bibliothèque de règles.



Voici les règles prédéfinies disponibles :

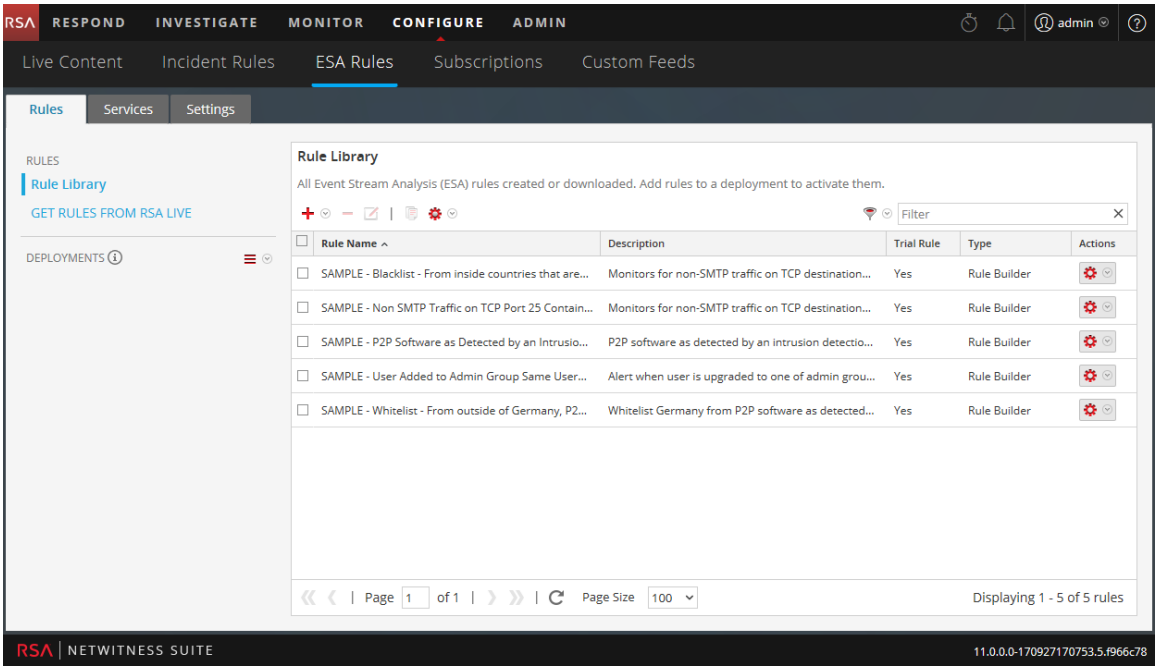
- SAMPLE : Logiciel P2P tel que détecté par un périphérique de détection d'intrusions
- SAMPLE : Trafic non SMTP sur le port TCP 25 contenant le fichier exécutable
- SAMPLE : Liste blanche -Extérieur de l'Allemagne, logiciel P2P tel qu'il est détecté par un périphérique de détection d'intrusions.
- SAMPLE : Liste noire -Pays autres que les ÉtatsUnis, trafic non SMTP sur le port TCP 25 contenant le fichier exécutable
- SAMPLE : Utilisateur ayant ajouté au groupe Admin le même utilisateur su Sudo

Chaque nom commence par SAMPLE afin de distinguer les règles installées avec NetWitness Suite de celles que vous téléchargez et créez.

Bibliothèque de règles

La Bibliothèque de règles affiche les informations suivantes sur les règles :

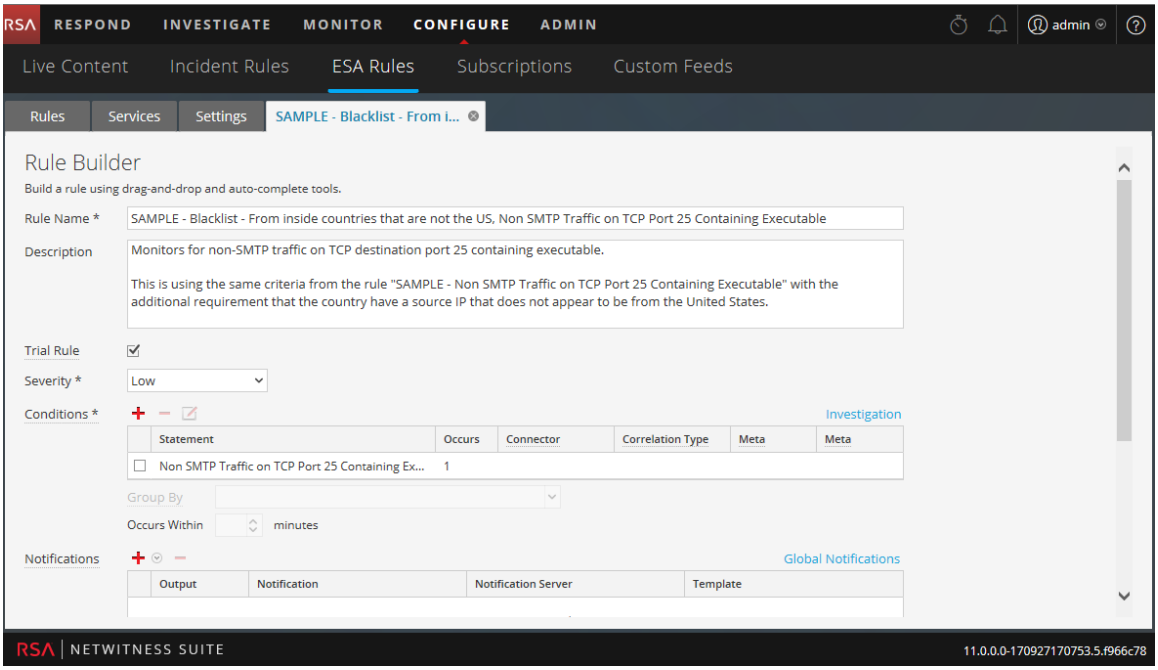
- **Nom** récapitule les données ou événements collectés par la règle.
- **Description** explique la règle de façon plus détaillée, même si seul le début s'affiche dans la Bibliothèque de règles.
- **Règle d'évaluation** indique si le mode d'essai est activé ou désactivé pour la règle.
- **Type** affiche l'origine de la règle, conçue dans le Générateur de règles ou EPL avancé ou téléchargée à partir de RSA Live.



Procédure

1. Accédez à **CONFIGURER > Règles ESA**.
   La vue Règles ESA s'affiche avec l'onglet Règles ouvert.
2. Dans la **Bibliothèque de règles**, sélectionnez un exemple de règle, puis cliquez sur , ou double-cliquez sur une règle.

La règle s'affiche dans le générateur de règles.



3. Pour utiliser une règle prédéfinie, reportez-vous aux rubriques suivantes pour obtenir des procédures et des descriptions détaillées :
   - Pour vous familiariser avec l'interface utilisateur du générateur de règles, reportez-vous à l'onglet Onglet Générateur de règles pour obtenir une description de chaque champ.
   - Pour savoir comment modifier une règle, reportez-vous à la rubrique Ajouter une règle Générateur de règles pour une procédure pas-à-pas.
   - Pour déployer une règle prédéfinie, reportez-vous à la rubrique Déployer des règles à exécuter sur ESA afin d'apprendre à associer la règle à un service ESA.

Une fois familiarisé avec les règles prédéfinies, vous pouvez télécharger, créer et déployer vos propres règles.

Utiliser les règles d'évaluation

Lorsque les règles utilisent une trop grande quantité de mémoire, votre service ESA peut ralentir ou se bloquer. Pour vous assurer que les règles n'utilisent pas une quantité excessive de mémoire, vous pouvez activer les règles d'évaluation pour tout type de règle. Par défaut, les nouvelles règles que vous créez et les règles RSA Live que vous importez sont configurées pour être des règles d'évaluation. RSA vous recommande de désactiver le paramètre de règle d'évaluation uniquement après avoir testé la nouvelle règle dans votre environnement, avec un trafic réseau normal et élevé. Lorsque vous créez une règle d'évaluation, vous définissez un seuil global du pourcentage de mémoire que les règles peuvent utiliser. Si ce seuil de mémoire configuré est dépassé, toutes les règles d'évaluation sont désactivées.

Le service Event Stream Analysis (ESA) de NetWitness Suite peut traiter de gros volumes de données d'événement disparates à partir des Concentrators. Toutefois, lors de l'utilisation d'Event Stream Analysis, il est possible de créer des règles qui utilisent une quantité excessive de mémoire. Cela peut ralentir votre service ESA ou même provoquer son arrêt inattendu. Pour éviter que cela ne se produise pas, vous pouvez configurer votre règle en tant que règle d'évaluation. Lorsque vous configurez une règle d'évaluation, vous définissez également le seuil global du pourcentage de mémoire que les règles peuvent utiliser. En cas de dépassement de ce seuil de mémoire configuré, toutes les règles d'évaluation sont désactivées automatiquement.

Pour des suggestions sur la création de règles plus efficaces, reportez-vous à la rubrique « Bonnes pratiques pour l'écriture de règles » dans Bonnes pratiques

Par défaut, les nouvelles règles et les règles RSA Live sont configurées en tant que règles d'évaluation. En guide de bonne pratique, lorsque vous modifiez une règle existante, sélectionnez l'option Règle d'évaluation qui vous permet de :

- Déployer la règle avec une plus grande sécurité.
- Afficher éventuellement un snapshot de l'utilisation de la mémoire pour comprendre si la règle crée des problèmes de mémoire.
- Déterminer si vous devez modifier les critères de la règle pour améliorer les performances.

Remarque : Exécutez une règle en tant que règle d'évaluation suffisamment longtemps pour évaluer les performances lorsque le trafic réseau est normal et élevé.

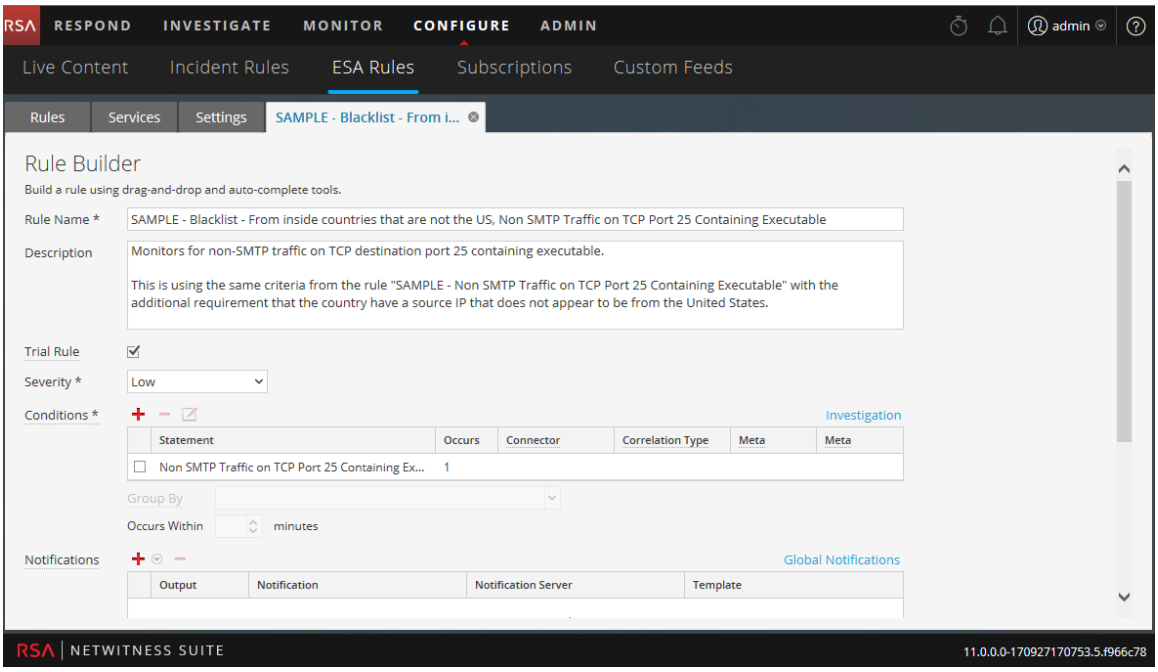
Déployer des règles en tant que règles d'évaluation

Cette rubrique explique aux administrateurs comment activer des règles d'évaluation lors de la création ou de la modification de règles. Les règles d'évaluation sont automatiquement désactivées en cas de dépassement du seuil d'utilisation de mémoire JVM spécifié.

Procédure

Pour déployer des règles comme règles d'évaluation :

1. Accédez à **CONFIGURER** > **Règles ESA**.
   La vue Configurer des règles ESA s'affiche avec l'onglet Règles ouvert.
2. Dans la Bibliothèque de règles, choisissez d'ajouter ou de modifier une règle. Le générateur de règles s'affiche dans un nouvel onglet
   .



3. Pour définir une nouvelle règle ou une règle existante comme règle d'évaluation, cochez la case **Règle d'évaluation**.
4. Ajoutez les conditions de la règle ou modifiez la règle selon les besoins. Pour des instructions sur la modification des règles, reportez-vous à la rubrique Ajouter des règles à la Bibliothèque de règles.
5. Cliquez sur **Enregistrer**.
6. Vérifiez que les règles d'évaluation sont activées pour votre service ESA et que les seuils configurés pour les règles d'évaluation vous conviennent.
   Le seuil de mémoire est défini dans le fichier de configuration. Pour le configurer, reportez-vous à « Modifier le seuil de mémoire pour les règles d'évaluation » dans le *Guide de configuration ESA*.
   Le seuil est configuré par service ESA et correspond à un pourcentage de la mémoire JVM. La valeur par défaut du paramètre de configuration, MemoryThresholdforTrialRules, est 85.

7. Vous pouvez éventuellement configurer les stratégies dans Intégrité de manière à ce qu'une notification vous soit envoyée par e-mail en cas de dépassement du seuil d'utilisation de la mémoire JVM totale.

La prochaine fois que la règle sera déployée, elle s'exécutera en mode d'évaluation.

Remarque : Si une règle d'évaluation est désactivée, vous devez cliquer sur l'onglet **CONFIGURER** > **Règles ESA** > **Services** pour réactiver les règles d'évaluation. Pour d'autres instructions sur la réactivation des règles d'évaluation au niveau d'un service, reportez-vous à la rubrique Afficher les statistiques et alertes ESA.

Afficher les metrics de mémoire pour les règles avec le mode d'essai

Cette rubrique indique aux writers de la règle ESA comment afficher des metrics de mémoire lorsque le seuil de mémoire configuré pour les règles d'évaluation est dépassé. Si le seuil de mémoire est dépassé, vous pouvez configurer un instantané de l'utilisation de la mémoire pour les règles ESA au moment où les règles d'évaluation sont désactivées. Cela vous permet d'enquêter sur l'utilisation de la mémoire et de modifier les règles afin d'être plus efficace.

Lorsque vous configurez des règles d'évaluation et que vous activez la fonction Instantané de la mémoire, si le seuil de mémoire est dépassé, toutes les règles d'évaluation sont désactivées et un instantané de l'utilisation de la mémoire de toutes les règles ESA est pris au moment de la désactivation. Cela vous permet de voir la quantité de mémoire utilisée, de telle sorte que vous pouvez modifier vos règles ESA pour davantage d'efficacité. L'instantané de la mémoire peut être affiché dans le navigateur Stat. système d'intégrité, vous aurez donc besoin d'autorisations pour accéder à ce module. Une fois que vous affichez les détails dans le navigateur Stat. système, vous pouvez modifier la syntaxe de la règle d'évaluation et réactiver les règles d'essai.

À un niveau élevé, vous devrez suivre les étapes suivantes pour utiliser l'instantané de mémoire afin de résoudre les problèmes d'utilisation de la mémoire pour les règles :

1. Activez les règles d'évaluation des nouvelles règles que vous déployez. Consultez la rubrique Déployer des règles en tant que règles d'évaluation
2. Assurez-vous que vous avez configuré les politiques d'intégrité de ESA pour envoyer un e-mail si les seuils de mémoire sont dépassés.
3. Vérifiez que vous disposez des autorisations nécessaires pour afficher le module Intégrité. Pour plus d'informations sur les rôles et autorisations, consultez la rubrique Autorisations du rôle.
4. Assurez-vous que la fonction Instantané de la mémoire est activée (via le paramètre EnabledCaptureSnapshot par l'intermédiaire de NetWitness Suite Explorer). La fonction Instantané de la mémoire est désactivée par défaut. Reportez-vous à la rubrique « Activation

et désactivation de la fonction Instantané de la mémoire » ci-dessous. RSA vous recommande de désactiver la fonction lorsque vous aurez terminé les tests de nouvelles règles.

5. Affichez les statistiques de seuil de mémoire dans Intégrité si le seuil de mémoire est déclenché pour les règles d'évaluation.
6. Modifiez la règle ou les règles qui ont déclenché l'alarme. À titre de bonnes pratiques pour la rédaction des règles, consultez la rubrique Bonnes pratiques.
7. Réactivez les règles d'évaluation qui ont été désactivées lorsque le seuil de la mémoire a été déclenché. Pour obtenir des instructions sur la réactivation des règles d'évaluation sur un service, consultez la rubrique Afficher les statistiques et alertes ESA.
8. Continuez à tester les règles d'évaluation.

Remarque : Comme tout outil de débogage, il peut y avoir des temps système exceptionnels associés à l'utilisation de la fonction Instantané de la mémoire. En prenant activement un instantané, la fonction Instantané de la mémoire peut ajouter des délais à vos services ESA. Le service ESA cesse de générer des alertes tout en prenant un instantané. RSA vous recommande de désactiver la fonction lorsque vous terminez les tests de nouvelles règles. Si vous désactivez la fonction Instantané de la mémoire, les règles d'évaluation seront toujours désactivées lorsque l'utilisation de la mémoire dépassera les seuils configurés. L'instantané ne sera pas pris et les statistiques ne figureront pas dans le navigateur Stat. système d'intégrité.

Conditions préalables

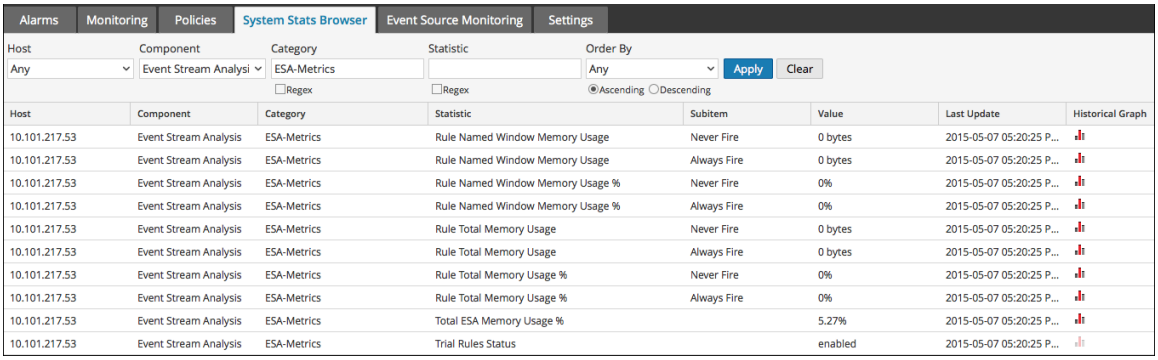
Voici les exigences pour afficher les metrics de mémoire :

- Une ou plusieurs règles ESA doivent être configurées comme règle d'évaluation.
- La fonction Instantané de la mémoire doit être activée (via le paramètre EnabledCaptureSnapshot par l'intermédiaire de NetWitness Suite Explorer).
- L'utilisateur doit disposer des autorisations appropriées pour afficher les statistiques d'intégrité.
- L'utilisateur doit avoir configuré la politique d'intégrité de ESA pour envoyer un e-mail lorsque les seuils de mémoire sont dépassés.

Procédures

Afficher les metrics de mémoire

1. Accédez à **ADMIN** > **Intégrité** > **Navigateur Stat. système**.
2. Pour le composant, sélectionnez **Event Stream Analysis**. Pour la catégorie, saisissez **ESA-Metrics**.



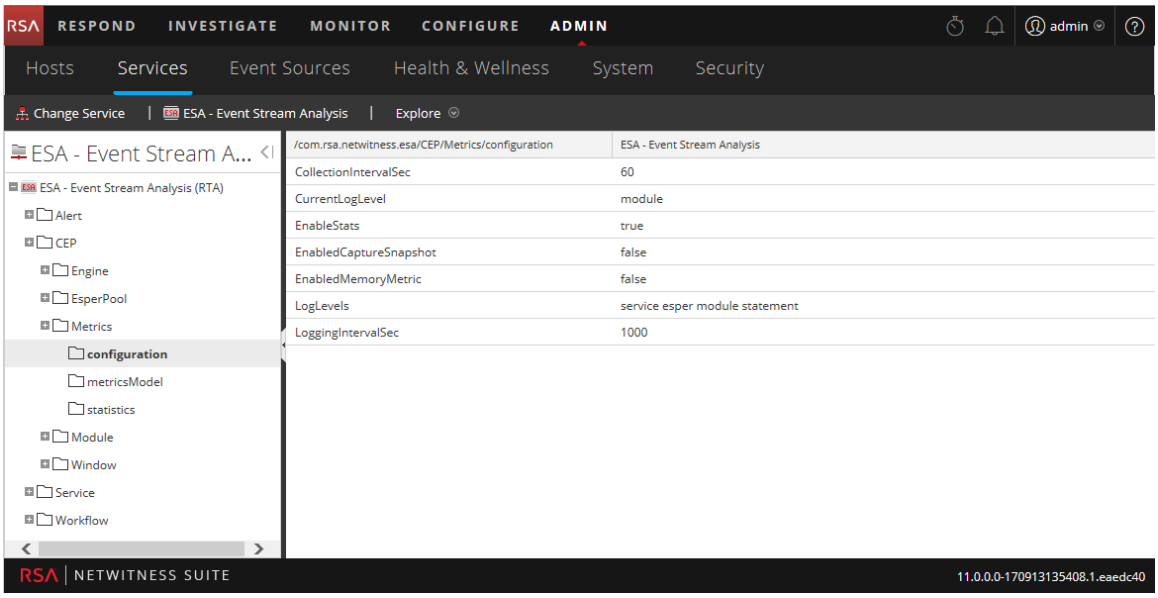
Le nom de la règle s'affiche dans le champ **Sous-élément** et l'utilisation de la mémoire s'affiche dans la colonne **Valeur**.

Remarque : Le champ **Dernière mise à jour** indique quand Intégrité interroge ESA. Toutefois, l'instantané de mémoire se produit uniquement lorsque les seuils de mémoire sont dépassés, par conséquent, ce champ ne reflète pas le moment où l'instantané a été pris ou mis à jour. L'instantané reste statique jusqu'à ce que le seuil de mémoire soit à nouveau atteint. Par exemple, si le seuil de mémoire est dépassé le 10/10/15 à 12h00, mais si Intégrité interroge le 10/10/15 à 15h00, le champ **Dernière mise à jour** affiche la date du 10/10/15 à 15h00.

Activer ou désactiver la fonction d'instantané de la mémoire

1. Accédez à **ADMIN** > **Services** et sélectionnez votre service ESA.

2. Sélectionnez > **Vue** > **Explorer**, puis accédez à CEP > Metrics > Configuration, comme indiqué ci-dessous.



3. Modifiez le champ EnabledCaptureSnapshot sur **true** ou **false** si souhaitez activer ou désactiver la fonction d'instantané de la mémoire.

Ajouter des règles à la Bibliothèque de règles

Cette rubrique explique comment ajouter chaque type de règle à la Bibliothèque de règles. Vous devez ajouter une règle à la Bibliothèque de règles pour pouvoir la déployer ensuite. L'autorisation pour gérer des règles est nécessaire pour toutes les tâches de cette section. Pour ajouter des règles, vous pouvez les télécharger à partir de ESA Live, créer une règle via le Générateur de règles ou écrire des règles EPL avancées.

Pour plus d'informations sur chacune de ces procédures, consultez :

- Télécharger des règles ESA RSA Live configurables
- Ajouter une règle Générateur de règles
- Ajouter une règle EPL avancée

Outre le déploiement d'une règle, vous pouvez modifier, dupliquer, importer, exporter et supprimer une règle de la bibliothèque. Pour plus d'informations sur ces procédures, reportez-vous à la section Utilisation des règlesUtilisation des règles

Télécharger des règles ESA RSA Live configurables

Cette rubrique explique comment télécharger des règles configurables depuis le système de gestion de contenu Live de NetWitness Suite et les adapter à vos besoins.

RSA Live contient un catalogue de règles. Chaque règle contient des paramètres configurables qui vous permettent de l'adapter à votre environnement. Si RSA Live inclut une règle qui identifie les événements à détecter dans votre réseau, téléchargez-la pour gagner du temps. Vous pouvez modifier les paramètres configurables et enregistrer la règle dans votre bibliothèque de règles.

Il s'agit d'un exemple de description de chaque règle ESA RSA Live dans RSA Live :

Nom de la règle	Description
Ouvertures de session sur plusieurs serveurs	Détecte les ouvertures de session effectuées par un même utilisateur sur au moins 3 serveurs en 5 minutes. La période et le nombre de destinations uniques sont configurables.

Comme son nom l'indique, la règle recherche les ouvertures de session effectuées sur plusieurs serveurs. La description explique les critères de la règle de façon plus détaillée et indique les paramètres modifiés.

Remarque : Quand la description d'une règle contient un paramètre configurable, le paramètre par défaut est appliqué. Dans la règle fournie en exemple, la description indique 5 minutes. Toutefois, la période est configurable. 5 est donc le nombre de minutes par défaut.

Conditions préalables

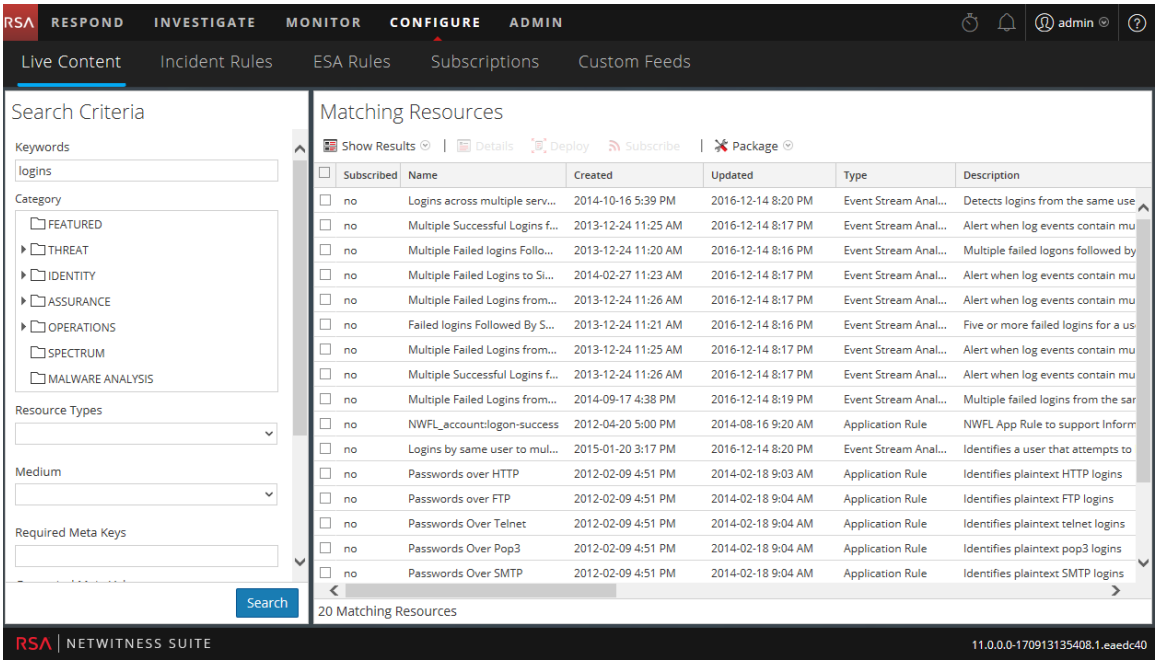
Voici les conditions préalables pour le téléchargement des règles ESA RSA Live configurables :

- Être autorisé à gérer les règles
- Créez un compte Live. Consultez le *Guide de gestion des services Live* pour plus d'informations.
- Configurez Live sur NetWitness Suite. Reportez-vous au *Guide de gestion des services Live* pour plus de détails.

Procédure

Pour télécharger des règles ESA RSA Live configurables :

1. Accédez à **CONFIGURER > Règles ESA**.
   L'onglet Règles s'affiche.
2. Dans le panneau des options, cliquez sur **Obtenir des règles de RSA Live**.
   La vue du contenu de Live Search s'affiche.



3. Dans **Critères de recherche**, pour **Type de ressource**, sélectionnez **Règle RSA Event Stream Analysis**.

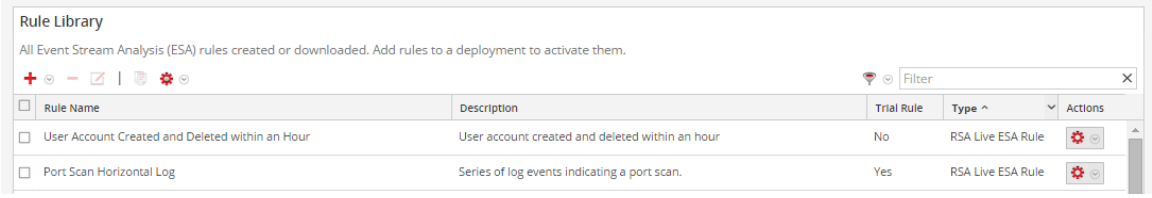
4. Indiquez l'un des critères suivants pour rechercher une règle permettant de configurer votre environnement.
   Pour obtenir une description détaillée des critères de recherche, reportez-vous à la section « La Vue Recherche Live » dans le *Guide de gestion des services Live*.
   a. Mots-clés
   b. Tags
   c. Clés méta requises
   d. Métavaleurs générées
   e. Date de création de la ressource
   f. Date de modification de la ressource
5. Cliquez sur **Search**. Les règles correspondant aux critères de recherche sont affichées dans Ressources correspondantes.
6. Sélectionnez chaque règle à télécharger et cliquez sur **Déployer**.
   L'assistant Déploiement s'affiche
7. Suivez les étapes de l'assistant. Si vous avez besoin de plus d'informations, reportez-vous à la section « Déployer des ressources dans Live » dans le *Guide de gestion des services Live*.

Une fois les étapes de l'assistant terminées, les règles sélectionnées s'affichent dans la Bibliothèque de règles.

Personnaliser une règle ESA RSA Live

Cette rubrique explique comment configurer les paramètres dans une règle ESA de RSA Live. Lorsque vous téléchargez une règle ESA de RSA Live, celle-ci apparaît dans la bibliothèque de règles, qui comprend les colonnes suivantes :

- Name
- Description
- Règle d'évaluation
- Type



Le type est Règle ESA de RSA Live.

Conditions préalables

- Les autorisations des rôles Administrateur, Opérateur, Responsable SOC ou Responsable de la confidentialité des données sont requises.
- Les règles doivent être téléchargées dans la bibliothèque de règles.

Procédure

Pour personnaliser une règle ESA de RSA Live :

1. Accédez à l'onglet **CONFIGURER > Règles ESA > Règles**.
2. Dans la **Bibliothèque de règles**, sélectionnez une règle ESA RSA Live, puis cliquez sur  .

   L'onglet Règle ESA RSA Live s'affiche.
3. (Facultatif) Modifiez les champs suivants :
   - Nom de la règle
   - Description
   - Règle d'évaluation (activée par défaut. RSA vous recommande d'exécuter une règle en tant que règle d'évaluation suffisamment longtemps pour évaluer les performances lorsque le trafic réseau est normal et élevé.)
   - Gravité
4. Pour configurer la règle pour votre environnement, dans la section **Paramètres**, remplacez la valeur par défaut dans la colonne **Valeur**.

5. Cliquez sur **Enregistrer**.

Ajouter une règle Générateur de règles

Cette rubrique présente un ensemble de procédures de bout en bout pour ajouter une règle de type Générateur de règles.

Chaque règle ESA est destinée à détecter quelque chose sur le réseau et à générer une alerte pour signaler :

- Une activité d'utilisateur non autorisée, par exemple une tentative de téléchargement de logiciel interdit
- Un comportement suspect, par exemple le nettoyage d'un audit
- Des menaces pernicieuses connues, par exemple la propagation de vers ou un outil de casse de mots de passe

Il existe deux méthodes pour concevoir une règle dans ESA :

- Le générateur de règles est une interface facile à utiliser. Il suffit de fournir une métaclé et une valeur méta, puis d'effectuer des sélections dans les listes pour renseigner les critères.
- L'EPL avancé permet d'écrire des requêtes en syntaxe EPL (Event Processing Language). Vous devez connaître la syntaxe EPL.

Si vous connaissez le langage EPL, vous pouvez utiliser les deux méthodes. Si vous ne connaissez pas EPL, vous devez utiliser le Générateur de règles. Ces rubriques expliquent le Générateur de règles.

Étape 1. Nommer et décrire la règle

Cette rubrique fournit des instructions pour identifier une règle, indiquer s'il s'agit d'une règle d'évaluation et attribuer un niveau de gravité. Lorsque vous ajoutez une nouvelle règle, les premières informations à indiquer sont un nom spécifique et la description des éléments que la règle détecte. Une fois que vous avez enregistré la règle, ces informations s'affichent dans la Bibliothèque de règles.

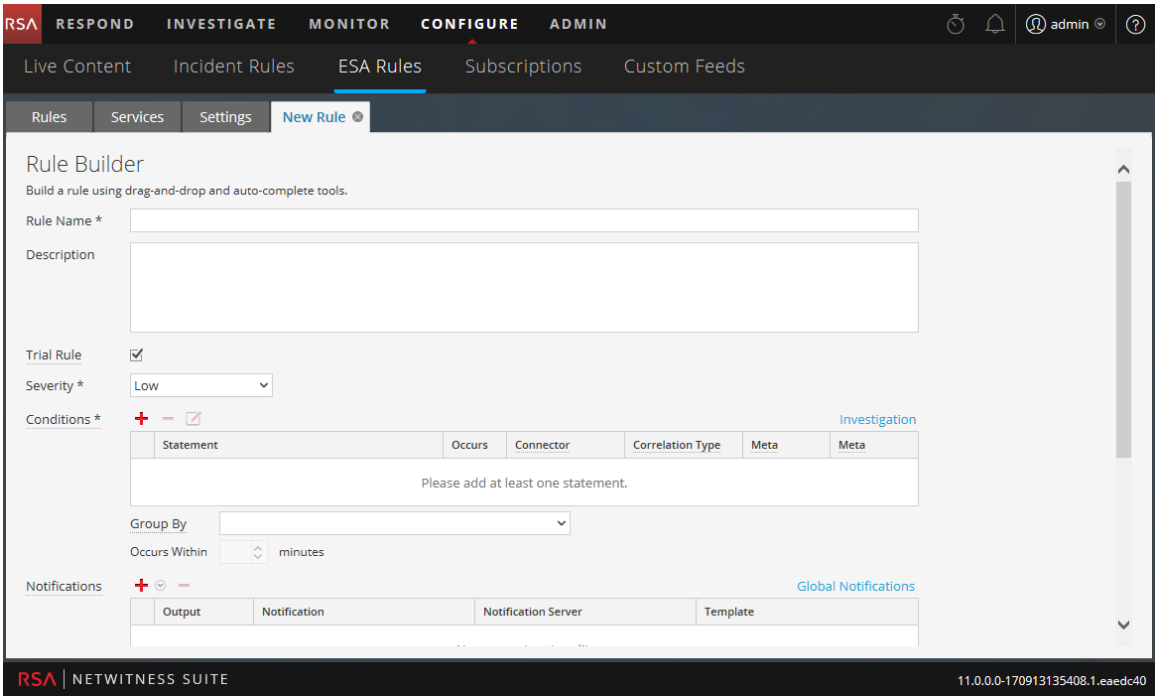
Conditions préalables

Vous devez posséder des autorisations pour gérer les règles. Reportez-vous à Autorisations du rôle.

Procédure

Pour nommer et décrire une règle :

1. Accédez à l'onglet **CONFIGURER > Règles ESA > Règles**.
2. Dans la **Bibliothèque de règles**, sélectionnez  **> Générateur de règle**.
   L'onglet Nouvelle règle s'affiche.



3. Saisissez un nom descriptif unique dans le champ **Nom de la règle**.
   Ce nom s'affichant dans la Bibliothèque de règles, soyez assez spécifique de manière à distinguer la règle des autres.
4. Dans le champ **Description**, expliquez les événements que la règle détecte.
   Le début de cette description s'affiche dans la Bibliothèque de règles.
5. Par défaut, les nouvelles règles sont configurées en tant que Règle d'évaluation. Une Règle d'évaluation désactive automatiquement la règle si toutes les règles d'évaluation dépassent collectivement le seuil de mémoire. Si vous modifiez une règle existante, vous pouvez sélectionner **Règle d'évaluation** pour tester les modifications de la règle en toute sécurité. Pour plus de sécurité, utilisez le mode de règle d'évaluation afin de déterminer si une règle s'exécute efficacement et afin d'éviter toute interruption de service liée au manque de mémoire. Pour plus d'informations, consultez Utiliser les règles d'évaluation.
6. Pour **Gravité**, utilisez Faible, Moyenne, Élevée ou Critique.

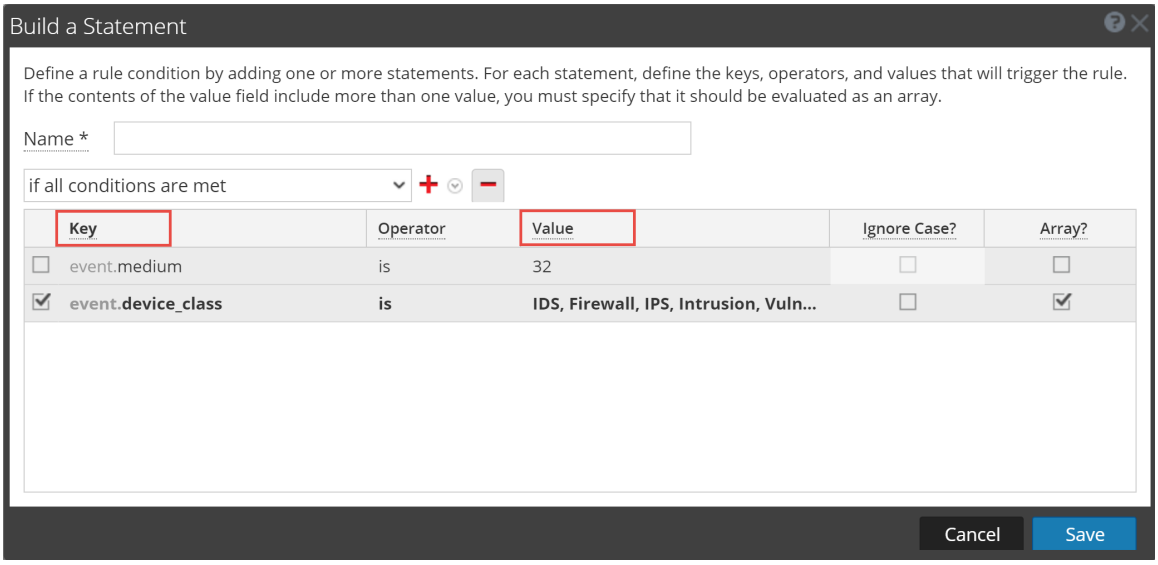
Étape 2. Créer une instruction de règle

Cette rubrique fournit des instructions pour définir des critères de règle dans le Générateur de règles en ajoutant des instructions. Une instruction est un groupe logique de critères de règle dans le Générateur de règles. Vous pouvez ajouter des instructions pour définir ce qu'une règle détecte.

Exemple

Le graphique suivant illustre un exemple d'instruction du générateur de règles.

Chaque instruction contient une clé et une valeur. Ensuite, vous élaborez une logique autour de la paire en sélectionnant une option dans chaque champ.



Conditions préalables

Pour créer une instruction de règle, vous devez connaître la clé méta et la valeur méta. Pour obtenir la liste complète des clés méta, accédez à **CONFIGURER> Règles ESA > Paramètres > Références aux clés méta**.

Procédure

Pour créer une instruction de règle :

1. Accédez à **CONFIGURER > Règles ESA**.

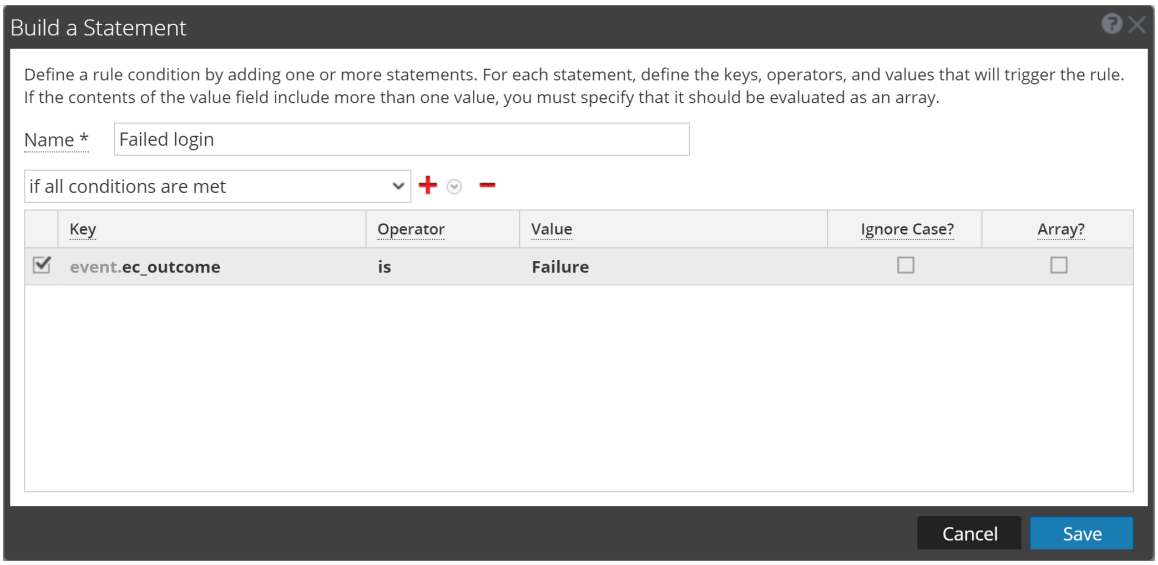
   L'onglet Règles s'affiche par défaut.

2. Dans la **Bibliothèque de règles**, cliquez sur > **Générateur de règles** ou modifiez une règle du générateur de règles.

   La vue Générateur de règles s'affiche.

3. Dans la section **Conditions**, cliquez sur .

   La boîte de dialogue Créer une instruction s'affiche.



4. **Nommez** l'instruction. Soyez clair et concis. Le nom de l'instruction apparaît dans le générateur de règles.
5. Dans la liste déroulante, sélectionnez les conditions de la règle :
   - si **toutes les conditions** sont remplies
   - si **l'une des conditions** est remplie
6. Indiquez les critères de l'instruction :
   a. Pour **Clé,** saisissez le nom de la **Clé méta**.
   b. Dans le champ **Opérateur**, indiquez la relation existant entre la clé méta et la valeur méta que vous précisez.
   Les choix sont les suivants : est, n'est pas, n'est pas nul, est supérieur à (>), est supérieur ou égal à (>=), est inférieur à (<), est inférieur ou égal à (<=), contient, ne contient pas, commence par, se termine par
   c. Saisissez la **valeur** de la clé méta.
   N'insérez pas de guillemets autour des valeurs. Séparez les différentes valeurs par une virgule.
   d. Le champ **Ignorer la casse ?** est destiné à être utilisé avec des valeurs de chaîne et de tableau de chaînes. Si vous choisissez le champ **Ignorer la casse**, la requête traitera toute chaîne de texte comme étant une valeur minuscule. Cela permet de garantir qu'une règle qui recherche un utilisateur nommé Johnson se déclenchera si un événement contient « johnson », « JOHNSON » ou « JoHnSoN ».
   e. Le champ **Tableau ?** indique si le contenu du champ Valeur représente une ou plusieurs

valeurs.

Cochez la case Tableau si vous avez saisi plusieurs valeurs séparées par une virgule dans le champ **Valeur**. Par exemple, pour « ec_activity is Logon, Logoff », vous devez cocher la case Tableau.

7. Pour utiliser une autre clé méta dans l'instruction, cliquez sur +, sélectionnez **Ajouter une condition méta** et répétez l'étape 6.
8. Pour ajouter une liste blanche, cliquez sur + et sélectionnez **Ajouter une condition de liste blanche.**
9. Pour ajouter une liste noire, cliquez sur + et sélectionnez **Ajouter une condition de liste noire**.
10. Pour enregistrer l'instruction, cliquez sur **Enregistrer**.

Ajouter une liste blanche

La liste blanche permet de s'assurer que les événements spécifiés sont exclus du déclenchement de la règle. Les listes blanches peuvent être basées sur l'emplacement géographique ou sur les sources CSV d'enrichissement définies par le client. Par exemple, pour créer une règle qui ne se déclenche que pour les adresses IP hors des États-Unis, vous pouvez créer une liste blanche d'adresses IP aux États-Unis.

1. Après avoir ajouté une métacondition, cliquez sur + et sélectionnez **Ajouter une condition de liste blanche**.
2. Dans le champ **Entrezun nom de liste blanche**, sélectionnez une source d'enrichissement. Toute source d'enrichissement chargée depuis un CSV ou une fenêtre nommée dans Esper peut être utilisée comme source pour une liste blanche.
3. Si vous avez utilisé une source GeoIP comme liste blanche, ipv4 est automatiquement saisi pour la sous-condition. Saisissez la valeur méta pour le champ de valeur correspondant. Par exemple, saisissez *IPv4 is ip_src* pour garantir que les enregistrements GeoIP sont sélectionnés en fonction de la valeur ip_src trouvée dans la base de données de consultation GeoIP. Par ailleurs, si vous avez utilisé une source GeoIP comme liste blanche, vous voudrez peut-être ajouter une sous-condition pour spécifier la région géographique à exclure des résultats de la règle. Par exemple, pour spécifier que le code de pays doit être USA, saisissez « *CountryCode is US* ».

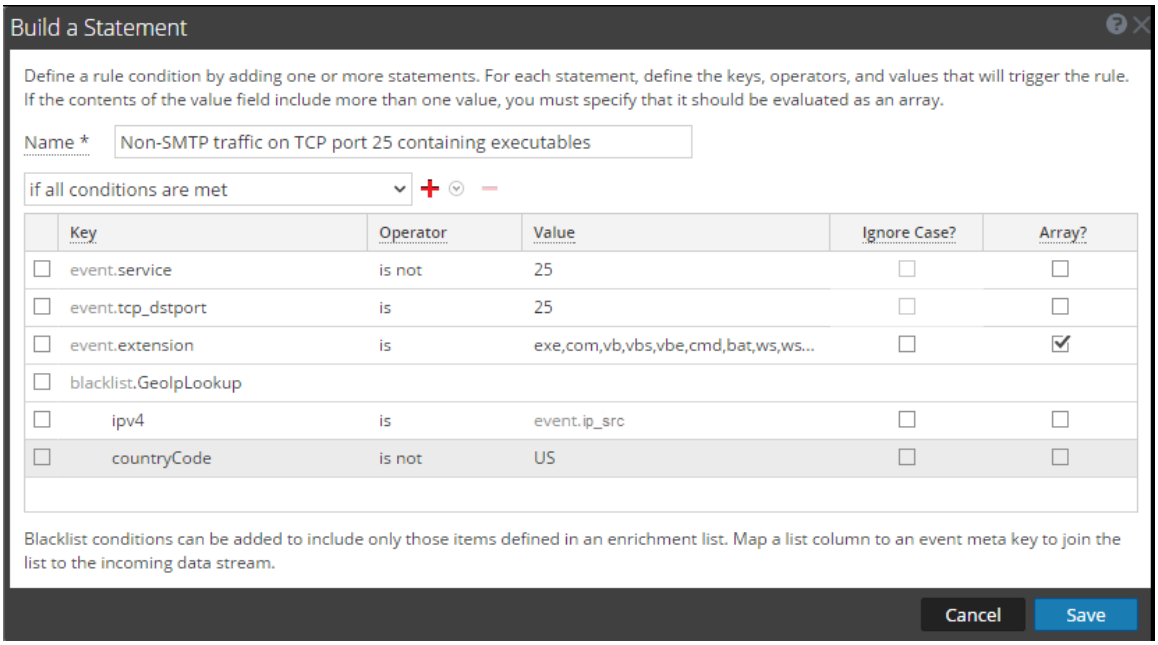
Ajouter une liste noire

La liste noire permet de s'assurer que les événements spécifiés déclenchent la règle. Les listes noires peuvent être basées sur l'emplacement géographique ou sur les sources CSV d'enrichissement définies par le client. Par exemple, vous pouvez spécifier que la règle ne comprend que les résultats provenant d'Allemagne.

1. Après avoir ajouté une métacondition, cliquez sur + et sélectionnez **Ajouter une condition de liste noire**.
2. Dans le champ **Saisir un nom de liste noire**, sélectionnez une source d'enrichissement. Toute source d'enrichissement chargée depuis un CSV ou une fenêtre nommée dans Esper peut être utilisée comme source pour une liste noire.
3. Si vous avez utilisé une source GeoIP comme liste noire, ipv4 est automatiquement saisi pour la sous-condition. Saisissez la valeur méta pour le champ de valeur correspondant. Par exemple, saisissez ipv4 is ip_src pour garantir que les enregistrements GeoIP sont sélectionnés en fonction de la valeur ip_src trouvée dans la base de données de consultation GeoIP. Par ailleurs, si vous avez utilisé une source GeoIP comme liste noire, vous voudrez peut-être ajouter une sous-condition pour spécifier la région géographique à inclure dans les résultats de la règle. Par exemple, pour spécifier que la règle n'inclut que les résultats pour l'Allemagne, saisissez « *CountryCode is DE* ».

Exemple : Liste noire

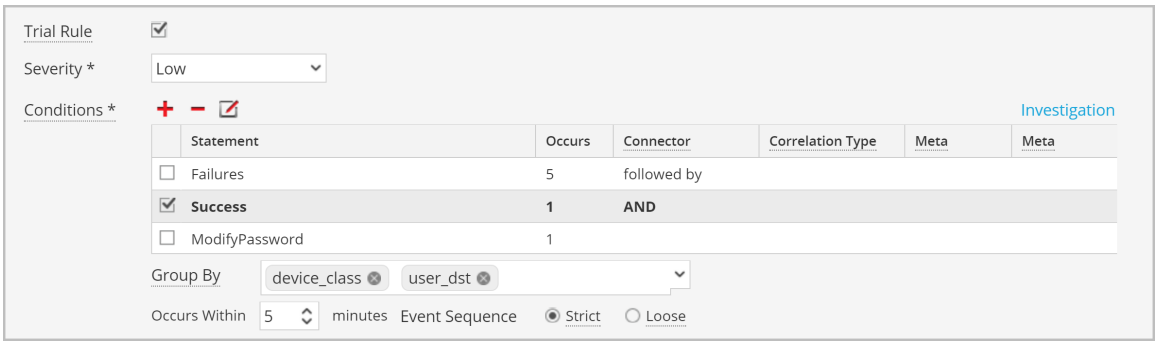
L'instruction suivante est une instruction de liste noire pour une règle qui surveille un trafic non SMTP sur une destination TCP port 25 contenant un exécutable provenant de pays autres que les États-Unis.



Instruction	Description
Le service n'est pas le service 25	Le trafic n'est pas le trafic SMTP.
tcp_dstport edt égal à 25	Le trafic est exécuté sur le port TCP 25.
L'extension est exe, com, vb, vbs, vbe, cmd, bat, ws, wsf, src, sh	L'extension de fichier correspond à un exécutable.
GeoIpLookup	La liste noire est basée sur une source GeoIPLookup.
ipv4 is ip_src	Les enregistrements GeoIP sont sélectionnés en fonction de la valeur ip_src dans la base de données de consultation GeoIP.
La valeur de countryCode n'est pas US	Lors de la recherche de l'adresse IP Event.ip_src dans la base de données GeoIP, l'enregistrement qu'il renvoie ne contient pas « US » dans le champ countryCode.

Exemple : Ignorer la casse, Correspondance stricte des schémas et utilisation de l'opérateur *N'est pas nul*

L'exemple suivant utilise la possibilité d'ignorer la casse, d'exclure les valeurs nulles et de créer une correspondance stricte des schémas afin de garantir qu'il renvoie les résultats de règle attendus. Les conditions suivantes composent la règle :

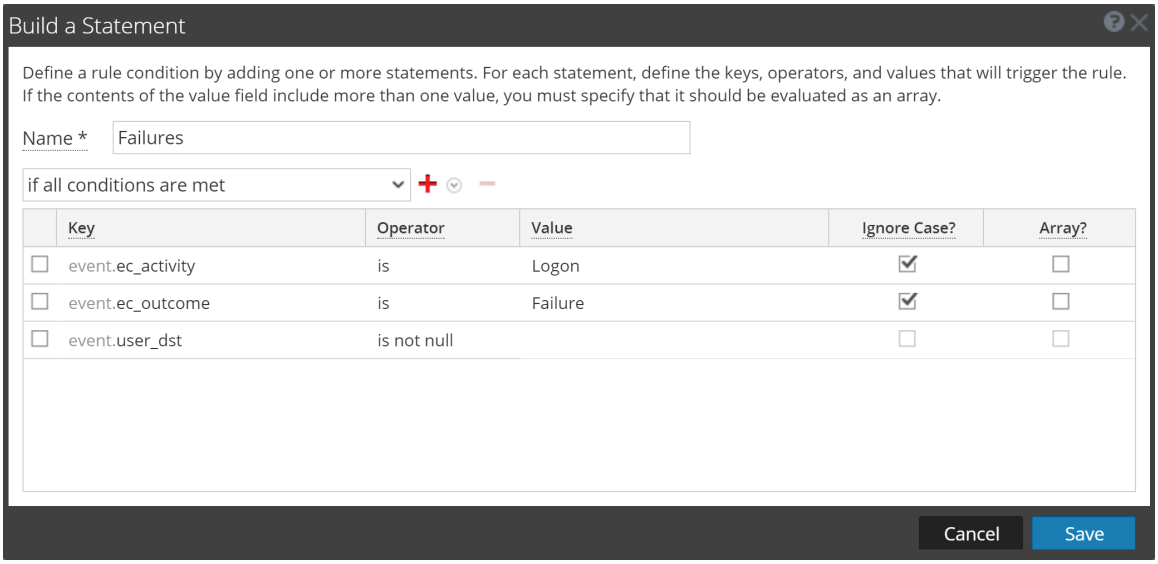


Condition de la règle	Description
Défaillances	Cette condition recherche cinq connexions qui ont échoué et qui ont un connecteur « Suivi de », qui signifie que la condition (Défaillances) doit être suivie par la condition suivante (success).
Success	Cette condition recherche une connexion réussie.
ModifyPassword	Cette condition recherche une instance où le mot de passe a été modifié.
GroupBy : user_dst, device class	Le champ GroupBy garantit que toutes les conditions précédentes sont groupées par méta user_dst (compte de destination de l'utilisateur) et classe d'appareil. C'est important pour la construction de la règle, car celle-ci tente de trouver un cas où un utilisateur a tenté de se connecter au même compte de destination plusieurs fois, a fini par se connecter, puis a changé le mot de passe. Le regroupement par classe d'appareil garantit également que l'utilisateur connecté depuis la même machine tente bien de se connecter à un compte à plusieurs reprises. La règle peut produire des résultats inattendus si vous ne regroupez pas les résultats.

Condition de la règle	Description
Se produit dans les 5 minutes	La période d'apparition des événements est égale à cinq minutes. Si les événements se produisent hors de cette période, la règle ne se déclenche pas.
Séquence d'événements Strict	La séquence d'événements est configurée pour une correspondance stricte des schémas. Cela signifie que le schéma doit correspondre exactement car il a été spécifié sans événement imprévu. La correspondance stricte des schémas vous permet de vous assurer que le moteur Esper ne génère que des alertes pour les règles qui correspondent exactement au schéma à trouver. Par exemple, une règle courante pourrait consister à rechercher cinq connexions qui ont échoué, suivies d'une connexion réussie. Si vous sélectionnez une correspondance des schémas souple, cette règle se déclenchera s'il existe un certain nombre de connexions réussies entre les connexions qui ont échoué. Étant donné que l'essentiel consiste à trouver des tentatives de connexion fréquentes *et* séquentielles, une correspondance stricte est nécessaire pour garantir que vous obtiendrez les résultats attendus.

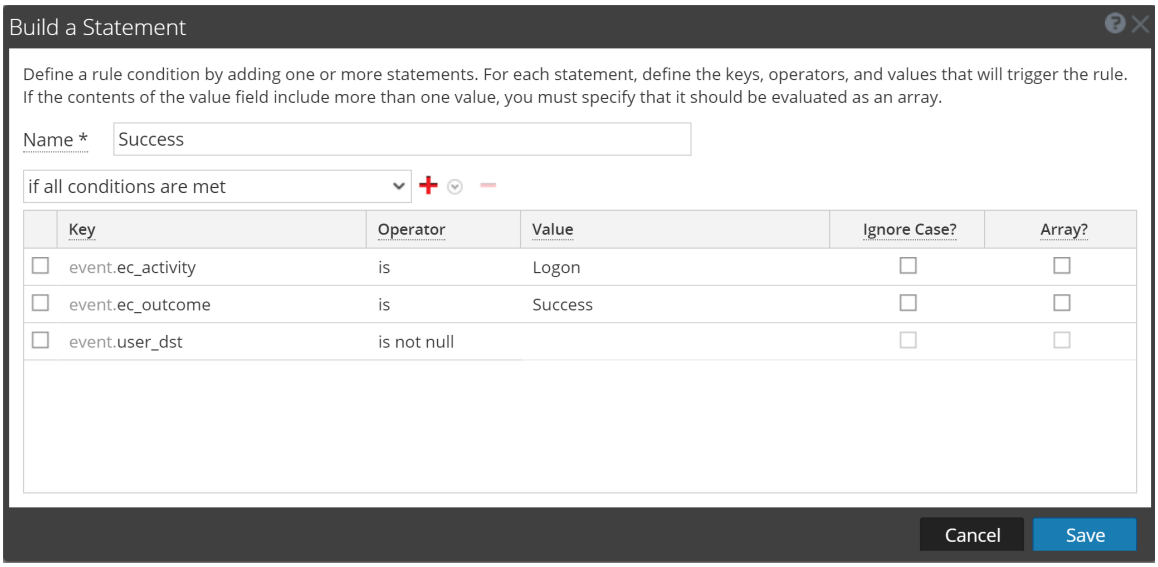
Remarque : Chacune de ces conditions est expliquée en détail dans les sections ci-dessous.

Pour chaque condition, une instruction est créée dans le générateur de règles. L'instruction suivante constitue la condition Failures :



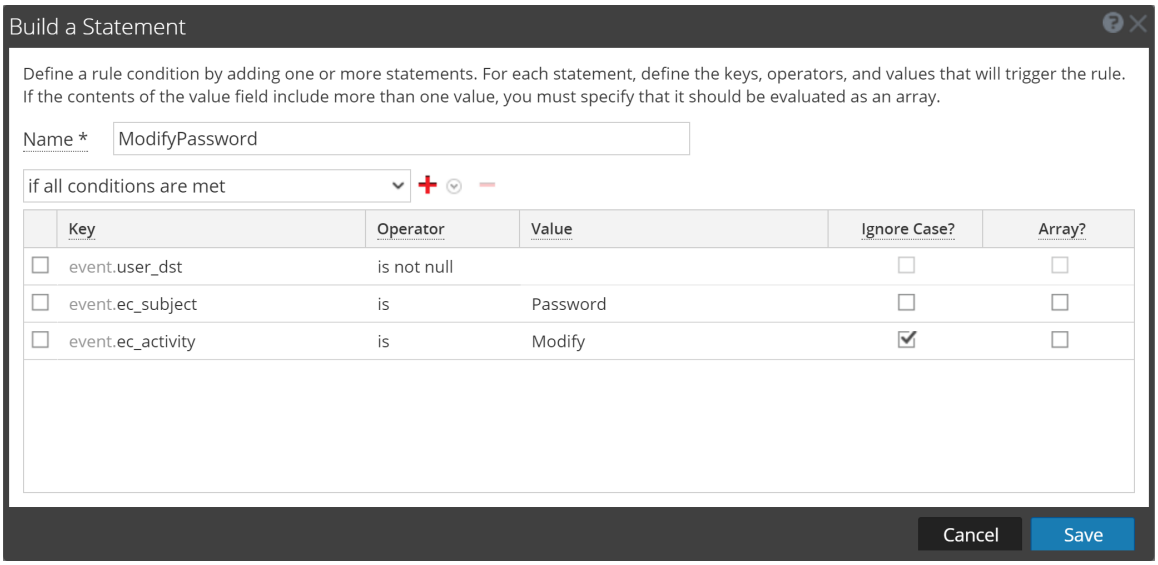
Instruction de règle	Description
ec-activity is Logon (ignore case)	Identifie l'activité qui tente de se connecter à un système. Le champ **Ignorer la casse** est destiné à être utilisé avec des valeurs de chaîne et de tableau de chaînes. Si vous choisissez le champ **Ignorer la casse**, la requête traitera toute chaîne de texte comme étant une valeur minuscule. Vous voudrez peut-être utiliser ce champ si vous n'êtes pas sûr de la casse à utiliser pour consigner un événement spécifique. Étant donné que la casse est ignorée, la règle peut se déclencher si l'activité est connectée sous la forme Logon, logon ou LoGoN.
ec_outcome is Failure (ignore case)	Identifie le résultat de l'activité consignée en tant qu'échec. Étant donné que la casse est ignorée, la règle peut se déclencher si l'activité est consignée sous la forme « failure », « Failure », ou « FaiLuRe. »
La valeur user_dst n'est pas nulle	Garantit que la condition n'a la valeur true que si user_dst est renseigné. L'opérateur **N'est pas nul** vous permet de garantir qu'un champ retourne une valeur. Si vous le souhaitez, vous pouvez utiliser ce champ lorsqu'une règle dépend d'un champ particulier renvoyant une valeur. Par exemple, vous souhaitez créer une règle qui identifie le même utilisateur qui tente de se connecter au même compte de destination plusieurs fois (éventuellement une attaque de découverte de mot de passe). Si le champ qui représente le compte de destination de l'utilisateur est vide, vous ne souhaitez pas que la règle se déclenche. Pour garantir que le champ contient une valeur, utilisez l'opérateur **N'est pas nul**.

L'instruction suivante constitue la condition Success :



Instruction de règle	Description
ec_activity is Logon	Identifie une activité de connexion.
ec_outcome is Success	Identifie une connexion réussie.
La valeur user_dst n'est pas nulle	Garantit que le champ du compte de destination de l'utilisateur doit être renseigné pour que la condition soit vraie.

L'instruction suivante constitue la condition ModifyPassword :

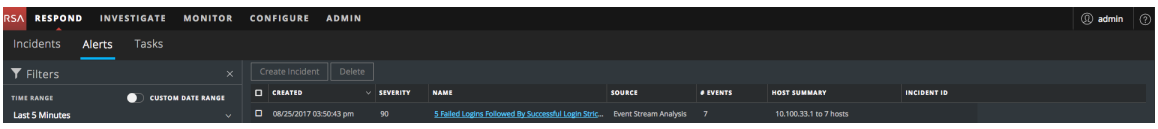


Instruction de règle	Description
La valeur user_dst n'est pas nulle	Garantit que le champ du compte de destination de l'utilisateur doit être renseigné pour que la condition soit vraie.
ec_subject is Password	Identifie un objet Mot de passe.
ec_activity is Modify	Identifie l'activité dans laquelle le mot de passe a été modifié.

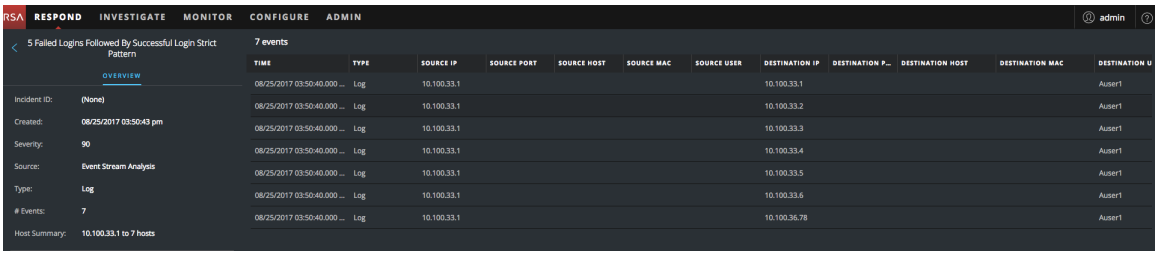
Exemple de résultats

Lorsque l'alerte se déclenche pour l'exemple de règle, vous pouvez constater que la règle s'est déclenchée pour sept événements et que chaque événement contient un utilisateur. Vous pouvez aussi constater que les événements suivent un schéma strict : cinq événements de connexion réussie, suivis par un événement de connexion qui a réussi, suivi par une modification du compte.

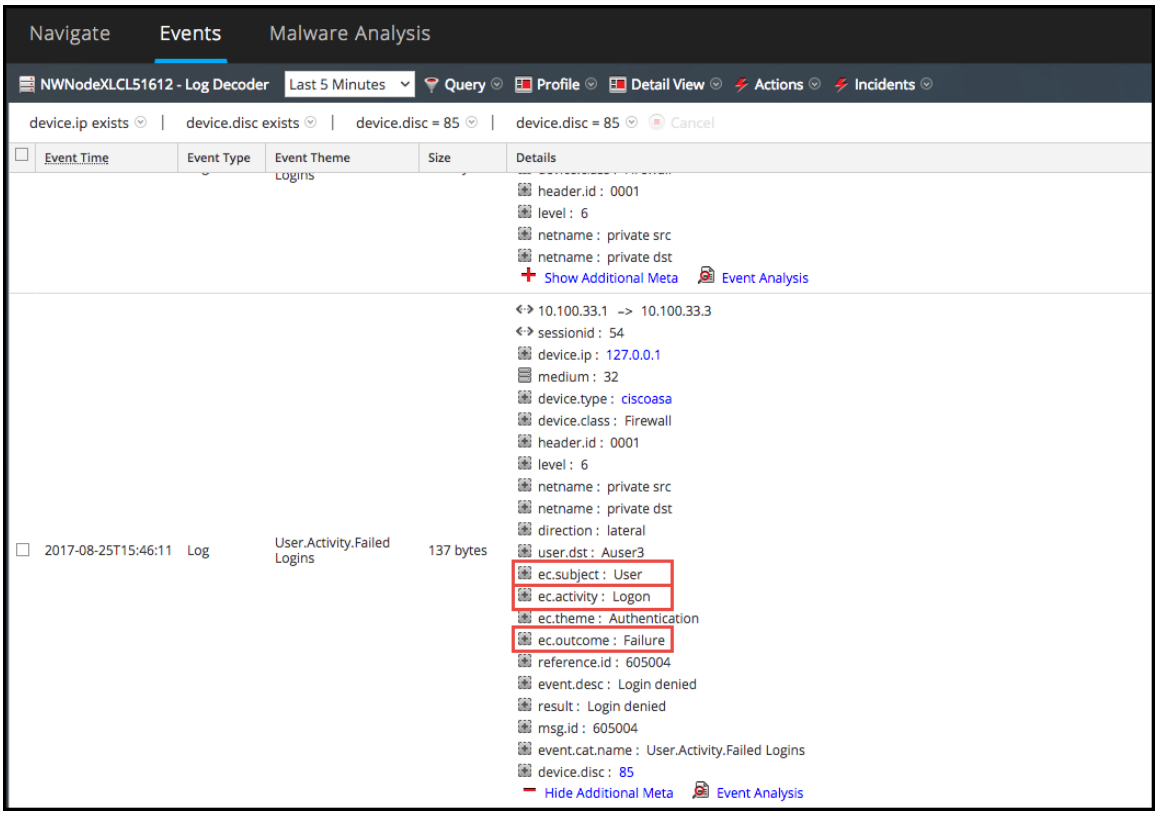
La figure suivante montre l'alerte dans la vue Liste des alertes de réponse.



La figure suivante affiche les événements dans l'alerte dans la vue Détails d'une alerte de réponse.



Si vous explorez le module Investigation en cliquant sur la source de l'un des événements, vous voyez la casse de chacune des valeurs de chaîne. Étant donné que vous avez utilisé **Ignorer la casse**, la règle se déclenchera si les chaînes de valeur contiennent des majuscules ou des minuscules.

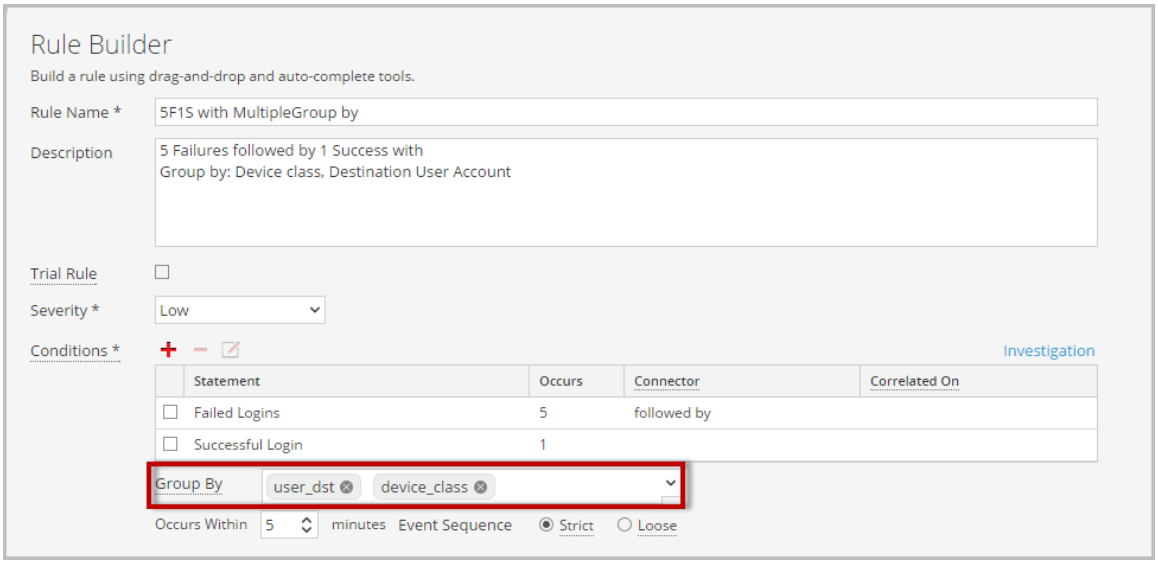


Exemple : Regroupement des résultats de règle

Le champ **Regrouper par** vous permet de grouper et filtrer les résultats de règle.Par exemple, supposons qu'il y a trois comptes d'utilisateur : Joe, Jane et John et que vous utilisez le méta **Regrouper par**, user_dst. Le résultat affichera les événements regroupés sous les comptes de Joe, Jane et John.

Vous pouvez aussi grouper par plusieurs clés, qui peuvent continuer à filtrer les résultats de règle. Par exemple, vous voudrez peut-être grouper par compte de destination d'utilisateur et machine pour voir si un utilisateur connecté au même compte de destination sur la même machine tente de se connecter à un compte plusieurs fois. Pour cela, vous pouvez grouper par device_class et user_dst.

L'exemple suivant illustre une règle groupée par device_class et user_dst.

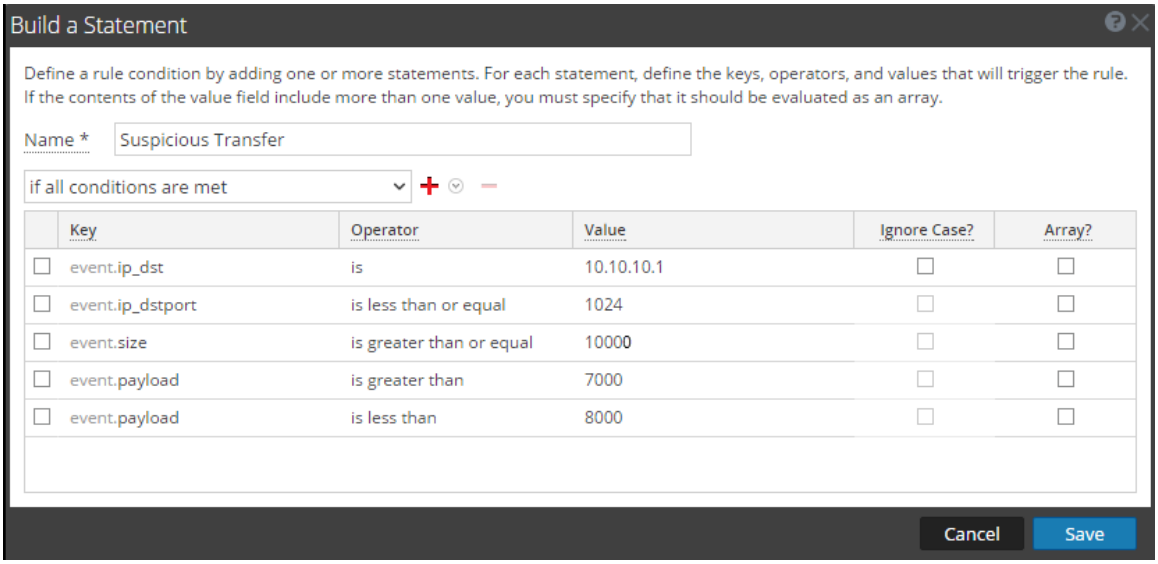


Condition de la règle	Description
Connexions ayant échoué	Identifie cinq tentatives de connexion ayant échoué (elles doivent être suivies de la condition suivante, à savoir que les cinq connexions ayant échoué doivent être suivies d'une connexion réussie).
Connexion réussie	Identifie une connexion réussie.
Group By : user_dst et device_class	Groupe les résultats de la règle par user_dst (compte de destination d'utilisateur) et device_class (type de machine sur laquelle l'utilisateur se connecte). Cela permet à la règle de rechercher un utilisateur connecté depuis la même machine au même compte de destination, ce qui génère un résultat de règle beaucoup plus ciblé.
Se produit dans les 5 minutes avec une correspondance stricte des schémas.	Les événements doivent se produire dans les cinq minutes et la correspondance des schémas est stricte, ce qui signifie que le schéma doit être suivi exactement pour que l'alerte se déclenche.

Exemple : Utilisation des opérateurs numériques

Les opérateurs numériques vous permettent d'écrire des règles pour les valeurs numériques, par exemple en spécifiant que la valeur est supérieure à, inférieure à ou égale à une valeur spécifique. Cette possibilité est utile surtout pour les cas où vous voulez spécifier un seuil numérique, par exemple, *la charge utile est supérieure à 7 000.*

Dans l'exemple suivant, il est tenté d'identifier un transfert de données vers une destination spécifique via les ports courants où la taille de transfert est élevée et la charge utile comprise dans une plage suspecte.



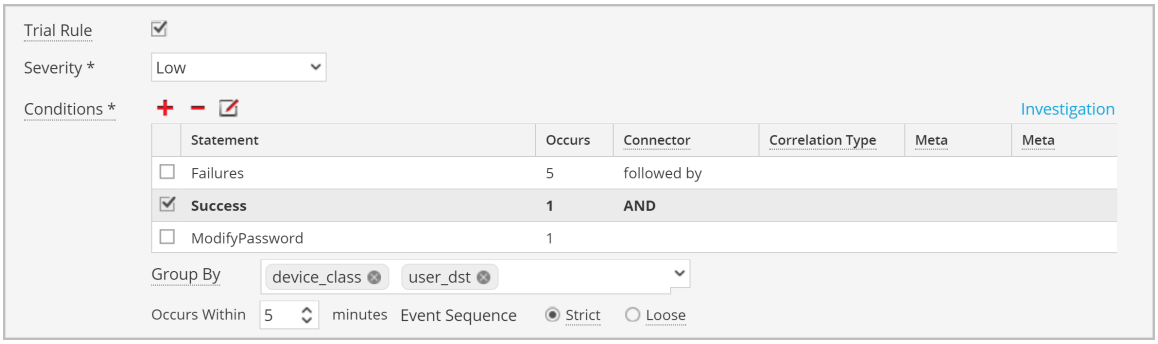
Instruction de règle	Description
ip_dst est 10.10.10.1.	Le port de destination est 10.10.10.1.
ip_dstport est supérieur ou égal à 1 024.	Le port de destination se situe dans une plage de ports couramment utilisée : 1 024 ou supérieure.
La taille est supérieure ou égale à 10 000.	La taille du transfert est 10 000 ou supérieure, ce qui correspond à un transfert trop volumineux.
La valeur payload est supérieure à 7 000	La charge utile est comprise entre 7 000 et 8 000, ce qui correspond à une charge utile trop volumineuse.
La charge utile est inférieure à 8 000.	La charge utile est comprise entre 7 000 et 8 000, ce qui correspond à une charge utile trop volumineuse.

Étape 3. Ajouter des conditions à une instruction de règle

Cette rubrique fournit des instructions pour ajouter des conditions, comme la spécification d'une certaine plage temporelle, à une instruction de règle. Lorsque vous créez une instruction, vous spécifiez les éléments détectés par une règle. Vous ajoutez des conditions pour stipuler d'autres options, comme la fréquence et la date d'application des critères.

Exemple

Le graphique ci-dessous illustre un exemple de conditions pour les instructions Générateur de règles. Combinées, les instructions et les conditions forment les critères de la règle.



Cette règle détecte 5 tentatives de connexion infructueuses, suivies d'une connexion réussie, qui peut indiquer qu'une personne a piraté le compte utilisateur. Voici les critères de la règle :

A. Cinq échecs de connexion sont requis.

B. Une connexion réussie doit suivre les échecs.

C. Un mot de passe a été modifié.

D. Tous les événements doivent se produire dans un délai de 5 minutes.

E. Les alertes sont regroupées par utilisateur (user_dst), car les étapes A et B doivent être effectuées sur le même compte utilisateur de destination. En outre, les alertes sont regroupées par machine (device_class) pour garantir que l'utilisateur connecté depuis la même machine tente bien de se connecter à un compte à plusieurs reprises.

F. La correspondance suit un modèle strict, ce qui signifie que le modèle doit correspondre parfaitement, sans intervention d'un événement extérieur.

Procédure

Pour ajouter des conditions à une instruction de règle :

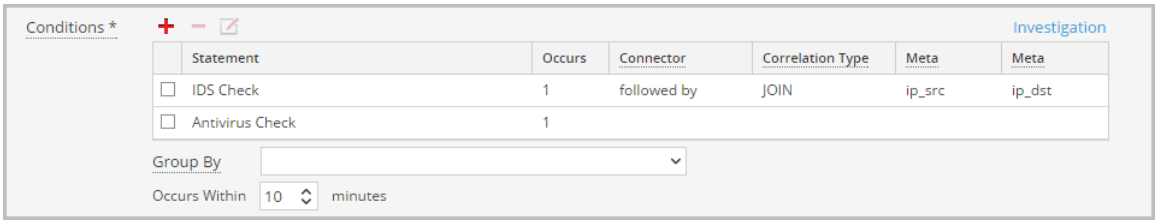
1. Dans la section **Conditions**, sélectionnez une instruction et cliquez sur  .
2. Pour **Se produit**, saisissez une valeur pour spécifier le nombre d'occurrences requises pour remplir les critères de la règle.
3. Si vous disposez de plusieurs instructions, dans le champ **Connecteur**, sélectionnez un opérateur logique pour associer une instruction à une autre :
   - suivi par
   - non suivi par
   - AND
   - OU
4. **Type de corrélation** s'applique uniquement à **suivi de** et **non suivi de**. Si vous choisissez un type de corrélation SAME, sélectionnez une méta pour la corrélation et, si vous choisissez un type de corrélation JOIN, sélectionnez deux métas pour la corrélation. Vous voudrez peut-être utiliser JOIN si vous tentez de mettre en corrélation les métas à partir de deux sources de données différentes. Par exemple, supposons que vous souhaitiez mettre en corrélation une alerte AV avec une alerte IDS. Consultez les exemples ci-dessous pour obtenir un exemple d'utilisation où deux métas provenant de différentes sources sont associées.
5. Si les événements doivent se produire dans un délai spécifique, saisissez le nombre de minutes dans le champ **Se produit dans les**.
6. Indiquez si le modèle doit suivre une correspondance de type **Strict** ou **Souple**. Si vous spécifiez une correspondance stricte, cela signifie que le modèle doit se produire exactement selon la séquence spécifiée, sans aucun événement supplémentaire dans l'intervalle. Par exemple, si la séquence spécifie cinq échecs de connexion (F) suivis d'une connexion réussie (S), la correspondance à ce modèle n'est effective que si l'utilisateur exécute la séquence suivante : F,F,F,F,F,S. Si vous spécifiez une correspondance souple, cela signifie que d'autres événements peuvent avoir lieu durant la séquence. Toutefois, la règle se déclenche quand même si tous les événements spécifiés se produisent également. Par exemple, le modèle suivant peut être créé par cinq échecs de tentatives de connexion (F), puis n'importe quel nombre intermédiaire de tentatives de connexion réussies (S), puis une tentative de connexion réussie : F,S,F,S,F,S,F,S,F,S qui déclenche la règle malgré les tentatives de connexion réussies dans l'intervalle.
7. Choisissez les champs de regroupement dans la liste déroulante. Le champ **Regrouper par** vous permet de regrouper et d'évaluer les événements entrants. Par exemple, dans la règle qui détecte 5 tentatives de connexion infructueuses, suivies d'une tentative réussie, l'utilisateur doit être identique. Par conséquent, user_dst est la clé méta du champ

Regrouper par. Vous pouvez également effectuer un regroupement en fonction de plusieurs clés. Dans l'exemple précédent, vous pouvez effectuer un regroupement par utilisateur et par machine afin de vous assurer que le même utilisateur connecté depuis la même machine tente bien de se connecter à un compte à plusieurs reprises. Pour cela, vous pouvez grouper par device_class et user_dst.

Exemple

L'illustration suivante présente un exemple des conditions pour une règle qui vous permet d'évaluer les entités mêmes sur plusieurs appareils afin que vous puissiez effectuer des exemples d'utilisation complexes. Par exemple, vous pouvez créer une règle qui se déclenche si une alerte IDS (Intrusion Detection System) est suivie d'une alerte AV (Anti-virus) pour la même station de travail. La clé de la station de travail n'est pas la même entre les deux sources (ID et AV), de sorte que vous pouvez effectuer une action JOIN afin d'évaluer les différentes entités.

Dans l'alerte IDS, la station de travail est identifiée par l'adresse IP source à partir de l'alerte IDS, et peut être comparée à l'adresse IP de destination à partir de l'alerte AV.



Voici les critères de la règle :

A. Une alerte IDS se produit.

B. L'adresse IP de destination de l'alerte AV et de l'adresse IP source pour la station de travail à partir de l'alerte IDS sont associées afin de vous permettre d'afficher les mêmes entités sur différentes sources.

C. Une alerte Antivirus suit l'alerte IDS.

Ajouter une règle EPL avancée

Cette rubrique fournit des instructions pour définir les critères de règle en écrivant une requête EPL. EPL est un langage déclaratif qui permet de gérer les données d'événement temporelles très régulières. Il sert à exprimer le filtrage, l'agrégation et les jointures sur des fenêtres potentiellement glissantes de plusieurs flux d'événement. EPL inclut également une sémantique de schéma pour exprimer une causalité temporelle complexe parmi les événements.

Élaborez une règle EPL avancée lorsque les critères de règle sont plus complexes que ce que vous pouvez spécifier dans le générateur de règles.

Notez que ce document n'a pas par pour objet de présenter la syntaxe EPL.

- Pour obtenir la documentation relative au langage EPL, consultez le site http://www.espertech.com/esper/documentation.php.
- Pour obtenir l'outil EPL en ligne, consultez le site http://esper-epl-tryout.appspot.com/epltryout/mainform.htm

Conditions préalables

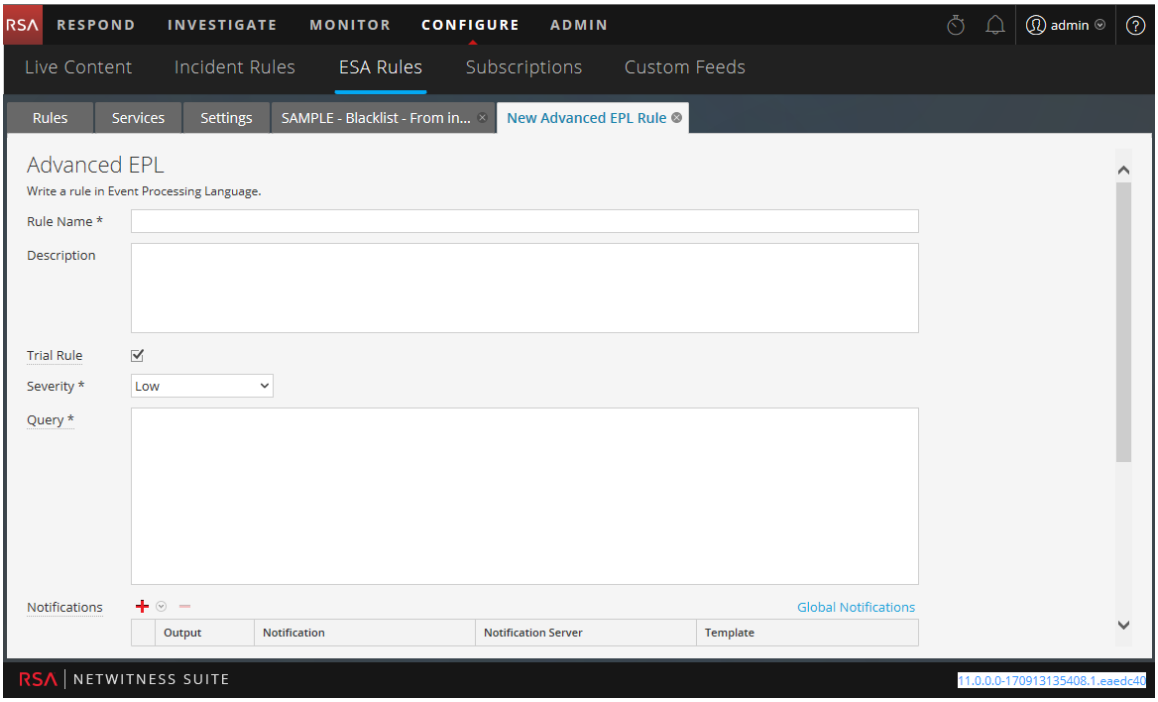
Voici les conditions préalables pour l'ajout d'une règle avancée :

- Vous devez maîtriser le langage EPL (Event Processing Language).
- Vous devez maîtriser les annotations ESA pour marquer les instructions EPL liées à la génération d'alertes.

Procédure

Pour ajouter une règle EPL avancée :

1. Accédez à **CONFIGURER > Règles ESA**.
2. Dans la **Bibliothèque de règles**, sélectionnez  **> EPL avancé**.



3. Saisissez un nom descriptif unique dans le champ **Nom de la règle**.

   Ce nom s'affichant dans la Bibliothèque de règles, soyez assez spécifique de manière à distinguer la règle des autres.

4. Dans le champ **Description**, expliquez les types d'événements que la règle détecte.

   Le début de cette description s'affiche dans la Bibliothèque de règles.

5. Sélectionnez **Règle d'évaluation** pour désactiver automatiquement la règle si toutes les règles d'évaluation dépassent collectivement le seuil de mémoire.

   Pour plus de sécurité, utilisez le mode de règle d'évaluation afin de déterminer si une règle s'exécute efficacement et afin d'éviter toute interruption de service liée au manque de mémoire. Pour plus d'informations, consultez Utiliser les règles d'évaluation.

6. Pour **Gravité**, utilisez Faible, Moyenne, Élevée ou Critique.

7. Pour définir les critères de la règle, rédigez une **requête** dans EPL.

   Remarque : Dans le nom des métaclés, utilisez un trait de soulignement au lieu d'un point. Par exemple, `ec_outcome` est correct mais pas `ec.outcome`.

8. Pour la génération de noms d'instruction dynamiques dans ESA, vous devez placer les clés méta entre accolades et inclure cette annotation dans la syntaxe :

   ```
   @Name("RIG {ip_src} {alias_host} {ec_activity}")
   ```

   où,

   - RIG est la partie statique du nom de l'instruction
   - {ip_src}, {alias_host}, {ec_activity} est la partie dynamique du nom de l'instruction

   Remarque : Si l'une des métadonnées dans la partie dynamique du nom de l'instruction possède une valeur null, elle s'affiche en tant que texte statique.

   Si une règle doit générer une alerte, incluez cette annotation ESA dans la syntaxe :

   ```
   @RSAAlert
   ```

   Pour plus d'informations sur les annotations ESA, reportez-vous à la section Annotations ESA.

Event Processing Language (EPL)

Cette rubrique décrit l'Event Processing Language (EPL), un langage déclaratif pour traiter les données d'événement basées sur le temps à fréquence élevée. ESA utilise l'Event Processing Language (EPL), un langage déclaratif pour traiter les données d'événement basées sur le temps à fréquence élevée. Il permet le filtrage, l'agrégation et l'association exprès de fenêtres potentiellement défilantes de flux d'événements multiples. L'EPL inclut également une sémantique de schéma pour exprimer une causalité temporelle complexe parmi les événements. Il peut exécuter, sans s'y limiter, les fonctions suivantes :

- Filtrage des événements
- Suppression d'alertes
- Calculer des pourcentages ou ratios
- Moyenne, nombre, valeurs minimale et maximale pour une période donnée
- Corréler des événements qui se produisent dans plusieurs flux
- Corréler des événements qui se produisent dans le désordre
- Activer/désactiver des fenêtres
- Prise en charge de Suivi de et Non suivi de
- Prise en charge du filtrage Regex

Les bases de données requièrent une interrogation explicite pour retourner des données significatives et ne sont pas adaptées pour transmettre des données lorsqu'elles sont modifiées. Le développeur doit implémenter lui-même la logique temporelle et d'agrégation. En revanche, le moteur EPL fournit une plus grande abstraction et des données et peut être considéré comme une base de données à l'envers. Au lieu de stocker les données et d'exécuter des requêtes sur les données stockées, EPL autorise les applications à stocker les requêtes et à exécuter les données en continu. Le moteur EPL répond en temps réel si les conditions répondent aux requêtes définies par l'utilisateur.

Les règles ESA avancées sont sensibles à la casse, mais dans la vue Investigation, tous les caractères sont convertis en lettres minuscules. Toutefois, les métas peuvent ne pas être en minuscules malgré les apparences dans la vue Investigation. Pour vous assurer d'utiliser la bonne casse, RSA vous recommande d'utiliser la fonction *toLowerCase()*. Par exemple,

```
@RSAAlert(oneInSeconds=0)
SELECT * FROM Event(
/* Statement: Download PDF File */
(filetype.toLowerCase() IN ( 'pdf' ) AND medium IN ( 1 ))
OR
/* Statement: Download EXE File */
(filetype.toLowerCase() IN ( 'windows_executable' , 'x86 pe' , 'windows
executable' ) AND medium IN ( 1 ))
).win:time(5 Minutes)
MATCH_RECOGNIZE (
PARTITION BY ip_src
MEASURES E1 as e1_data , E2 as e2_data
PATTERN (E1+ E2)
DEFINE
```

```
E1 as (E1.filetype.toLowerCase() IN ( 'pdf' ) AND E1.medium IN ( 1 )),
E2 as (E2.filetype.toLowerCase() IN ( 'windows_executable' , 'x86 pe' ,
'windows executable' ) AND E2.medium IN ( 1 ))
```

Pour les besoins de l'aide en ligne, des instructions simples sont utilisées pour illustrer la configuration d'ESA. Toutefois, pour plus d'informations sur l'écriture d'instructions EPL, le site http://www.espertech.com fournit des didacticiels et des exemples.

Remarque : ESA prend en charge la version 5.3.0 d'Esper.

Annotations ESA

Cette rubrique décrit les annotations proposées par NetWitness Suite pour une utilisation dans les règles EPL avancées.

Annotation @RSAAlert

L'annotation @RSAAlert permet de marquer les instructions EPL liées à la génération de notifications d'alertes. Elle est conçue pour fonctionner avec la fonction de suppression de notifications d'alerte dans l'interface utilisateur Générateur de règles.

L'annotation @RSAAlert peut être utile lorsque vous manipulez des notifications d'alerte, en particulier si vous souhaitez filtrer les notifications, telles que l'envoi d'une notification pour chaque utilisateur qui déclenche une alerte.

Par exemple, supposons que vous souhaitiez générer des notifications d'alerte pour les échecs de connexion. Vous pouvez ajouter l'instruction suivante :

*@RSAAlert select * from event(msg_id="login_fail")*

Numéro d'événement	ID de message	nom d'utilisateur	src_IP	Heure
1	login_fail	alice	1.2.3.4	10:00
2	login_fail	alice	1.2.3.4	10:01
3	login_fail	alice	6.7.8.9	10:01
4	login_fail	bob	1.2.3.4	10:01
5	login_fail	alice	1.2.3.4	10:03

Pour l'instruction ci-dessus, cinq notifications d'alerte sont générées.

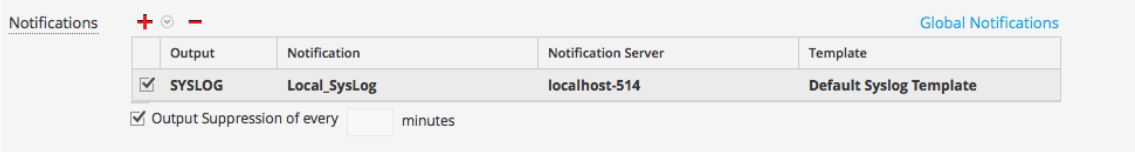
Toutefois, supposons que vous souhaitiez modifier l'instruction pour générer une alerte pour chaque nom d'utilisateur distinct. Vous pouvez utiliser l'attribut *identifiant*. Par exemple, l'instruction *@RSAAlert(identifier={"username"}) SELECT* FROM Event(msg_id="login_fail")* génère une notification pour la première alerte pour « bob » et une pour la première alerte pour « alice ». Les alertes suivantes pour « bob » et « alice » sont ignorées.

Vous pouvez distinguer davantage les utilisateurs en ajoutant des informations grâce à la variable identifiant. Par exemple, vous pouvez effectuer la distinction par l'utilisateur ou l'adresse IP à l'aide de l'instruction suivante : *@RSAAlert(identifier={"username", "src_ip"}) SELECT* FROM Event(msg_id="login_fail")*. Ensuite, vous devriez voir des notifications générées par le nom d'utilisateur et l'adresse IP (une alerte pour « alice » à 1.2.3.4, une autre alerte « Alice » à 6.7.8.9 et une alerte pour « bob » en 1.2.3.4).

Pour utiliser des identifiants avec suppression de notification d'alerte :

l'annotation @RSAAlert est conçue pour fonctionner avec la fonction de suppression de notifications d'alerte dans l'interface utilisateur Générateur de règles. Pour ce faire, procédez comme suit :

1. Créez une règle dans l'interface utilisateur du générateur de règles et sélectionnez la fonction de suppression d'alerte lors de la configuration de notifications.



2. Copiez le code de la règle Générateur de règles dans une nouvelle règle avancée.
3. Configurez la règle avancée pour inclure des identifiants (comme décrit ci-dessus) et enregistrer la règle avancée.
4. Supprimez la règle de générateur de règle d'origine.

Annotation @RSAPersist

L'annotation @RSAPersist permet de marquer une fenêtre nommée en tant que fenêtre gérée ESA à des fins de persistance. Si vous procédez ainsi, ESA enregistre régulièrement le contenu de la fenêtre sur le disque et le restaure si le déploiement de la fenêtre est annulé, puis rétabli. Les systèmes prennent un snapshot juste avant que le déploiement du module soit annulé et que la fenêtre soit supprimée. À l'inverse, il restaure le contenu de la fenêtre à partir du snapshot juste après le redéploiement du module. Cela permet d'éviter la perte du contenu de la fenêtre lorsque l'état du module est altéré ou que le service ESA s'arrête.

Par exemple, supposez que la fenêtre nommée `DHCPTracker` contienne un mappage d'adresses IP avec chacun des noms d'hôte attribués. Vous pouvez marquer une instruction avec l'annotation @RSAPersist de la façon suivante :

```
@RSAPersist
 create window DHCPTracker.std:unique(ip_src) as (ip_src string, alias_
host string);
 insert into DHCPTracker select IP as ip_src, HostName as alias_
host from DHCPAssignment(ID=32);
```

Remarque : Toutes les définitions de fenêtres ne conviennent pas pour la persistance. L'annotation `@RSAPersist` doit être utilisée avec précaution. Si la fenêtre inclut des enregistrements basés sur le temps ou si elle dépend de contraintes de temps, il est fort probable que les snapshots rétablis ne permettront pas de la restaurer dans son état approprié. De la même manière, les changements apportés à la définition de la fenêtre invalideront tous les snapshots et affecteront un état vide à la fenêtre. Le système ne génère aucune analyse sémantique pour déterminer si ces changements de la définition de la fenêtre entrent en conflit ou non. Notez que d'autres parties d'un module (autres que l'appel CREATE WINDOW spécifique qui définit la fenêtre) peuvent varier, sans invalider les snapshots.

@UsesEnrichment (10.6.1.1 et versions ultérieures)

@UsesEnrichment peut servir à référencer des enrichissements dans les règles EPL avancées. Pour synchroniser les enrichissements avec ESA, toutes les dépendances d'enrichissement dans les règles EPL doivent être référencées avec l'annotation @UsesEnrichment.

L'annotation @UsesEnrichment utilise le format suivant :

```
@UsesEnrichment(name= '<enrichment_name>')
```

Par exemple, l'EPL suivante fait référence à un enrichissement de la liste blanche :

```
@UsesEnrichment(name = 'Whitelist')

@RSAAlert

SELECT * FROM Event(ip_src NOT IN (SELECT ip_address FROM Whitelist))
```

@Name

@Name est le nom de l'instruction défini dans les règles avancées ESA. Il sert à générer de manière dynamique les noms d'instruction dans les alertes ESA. Le nom d'une seule instruction de déclenchement d'alerte s'affiche. Cette annotation contient des clés méta entourées d'accolades.

L'annotation @Name utilise le format suivant :

```
@Name("<static_part_of_statement_name> {meta_key1} {meta_
key2}…")
```

Par exemple, l'EPL suivante fait référence à des clés méta *ip_src* et *user_name* dont les valeurs sont générées dynamiquement.

@Name("Login Event to {ip_src} by {user_name}")

Remarque : Vous pouvez spécifier n'importe quel nombre de clés méta dans l'instruction pour la génération d'un nom d'instruction dynamique.
La longueur de clé méta individuelle est limitée à 64. Au-delà, la valeur est tronquée et « ... » lui est ajouté.
La longueur de la génération dynamique du nom de l'instruction est limitée à 128. Au-delà, la valeur est tronquée à 128 et « ... » lui est ajouté. Tous les autres valeurs restantes après la troncature seront traitées en tant que valeurs statiques.

Exemple de règles EPL avancées

Voici des exemples de règles ESA avancées. Pour chaque démonstration, il existe plusieurs façons d'implémenter le même exemple d'utilisation.

Exemple n° 1 :

Créez un compte utilisateur, puis supprimez-le en 300 secondes. Les informations utilisateur sont stockées dans la métavaleur user_src.

EPL n° 1 :

Nom de la règle	CreateuseraccountFollowedbyDeletionof Useraccount1
Description de la règle	Créez un compte utilisateur, puis effectuez une action permettant de supprimer le même compte utilisateur en 300 secondes.

Code de règle	`SELECT * FROM Event(ec_subject='User'`
	`  AND ec_outcome='Success'`
	`  AND user_src is NOT NULL`
	`  AND ec_activity IN ('Create',`
	`'Delete')`
	`  ).win:time(300 seconds)`
	`match_recognize (partition by user_src`
	`  measures C as c, D as d`
	`  pattern (C D)`
	`  define`
	`  C as C.ec_activity='Create' ,`
	`  D as D.ec_activity='Delete');`

Remarque	• Filtre les événements nécessaires au modèle dans la période donnée. Les conditions de filtrage doivent être définies de telle sorte que seuls les événements requis sont transmis à la fonction de détection de

	correspondance. Dans ce cas, il s'agit d'événements de création et de suppression de comptes utilisateur. Exemple : Event(ec_subject='User' AND ec_ outcome='Success' AND user_src is NOT NULL AND ec_activity IN ('Create', 'Delete') • Partition by crée des buckets. Dans le cas présent, Esper crée des buckets selon la valeur de user_src. Par conséquent, la valeur de user_src est commune aux deux événements. • Définissez le modèle souhaité. Actuellement, il correspond à Create suivi de Delete. Vous pouvez effectuer plusieurs créations suivies de suppressions (C+ D). Le modèle est très similaire à une expression régulière. • Exemple d'utilisation le plus efficace.

EPL n° 2 :

Nom de la règle	CreateuseraccountFollowedbyDeletionof Useraccount2
Description de la règle	Créez un compte utilisateur, puis effectuez une action permettant de supprimer le même compte utilisateur en 300 secondes.

Code de règle	`SELECT * from pattern[every (a= Event(ec_ subject='User' AND ec_outcome='Success' AND user_dst is NOT NULL AND ec_activity IN ('Create'))`
	`->`
	`( Event(ec_subject='User' AND ec_ outcome='Success' AND user_dst is NOT NULL AND ec_activity IN ('Create') AND user_src = a.user_src)`
	`) )where timer:within(300 Sec) ];`

Remarque	• Admettons qu'un même utilisateur soit créé deux fois, et qu'il soit supprimé une fois dans cet ordre. Dans ce cas,

	le modèle ci-dessus déclenche 2 alertes. • Un thread est créé pour chaque création d'utilisateur. • Il n'existe aucun moyen de contrôler les threads. Il est important d'avoir des limites temporelles et, si possible, de petits intervalles.

Exemple n° 2 :

Détectez un modèle comportant la création d'un utilisateur, sa connexion, puis sa suppression au final. Dans le cas de logs de fenêtres, les informations utilisateur sont stockées dans user_dst ou user_src en fonction de l'événement.

user_src(create) = user_dst(Login) = user_src(Delete)

EPL n° 3 :

Nom de la règle	CreateUserLoginandDeleteUser
Description de la règle	Détectez un schéma dans lequel un utilisateur crée un compte utilisateur suivi de la connexion par le même utilisateur, suivi de la suppression du compte utilisateur.

Code de règle	`SELECT * FROM Event(ec_subject='User'`
	`and ec_activity in`
	`('Create','Logon','Delete')`
	`and ec_theme in ('UserGroup',`
	`'Authentication')`
	`and ec_outcome='Success'`
	`).win:time(300 seconds)`
	`match_recognize (measures C as c, L as l, D as d`
	`pattern (C L D)`
	`define`
	`C as C.ec_activity = 'Create',`
	`L as L.ec_activity = 'Logon' AND L.user_dst = C.user_src,`
	`D as D.ec_activity = 'Delete' AND D.user_src = C.user_src`
	`);`

Remarque	• Dans la mesure où user_src/user_dst n'est pas commun à tous les événements, nous ne pouvons pas utiliser le partitionnement. 1 seul bucket exécute 1 modèle à la fois.

	Par exemple, pour l'utilisateur 1 et 2, si le flux d'événements est C1C2L1D1, C1L1C2D1, aucune alerte n'est émise, car le thread C1 est réinitialisé par C2. Une alerte est émise uniquement si le flux C1L1D1 est dans l'ordre, et si aucun autre événement du même utilisateur ou d'un autre utilisateur n'a lieu dans l'intervalle. • Il existe une autre solution : utiliser une fenêtre nommée, fusionner user_dst et user_src en une seule colonne, puis exécuter la détection de correspondance. (EPL n° 3). • Le modèle peut également être utilisé. Vous risquez d'obtenir plus d'alertes que prévu. (EPL n° 4).

EPL n° 4 : Utilisation de fenêtres nommées et de la détection de correspondance

Nom de la règle	CreateUserLoginandDeleteUser
Description de la règle	Détectez un schéma dans lequel un utilisateur crée un compte utilisateur suivi de la connexion par le même utilisateur, suivi de la suppression du compte utilisateur.

Code de règle	`@Name('NormalizedWindow') create window FilteredEvents.win:time(300 sec) (user String, ecactivity string, sessionid Long);`
	`@Name('UsersrcEvents') Insert into FilteredEvents select user_src as user, ec_activity as ecactivity, sessionid from Event ( ec_subject='User' and ec_activity in ('Create','Delete') and ec_theme in ('UserGroup', 'Authentication') and ec_outcome='Success' and user_src is not null );`
	`@Name('UsrdstEvents') Insert into FilteredEvents select user_dst as user, ec_activity`
	`as ecactivity, sessionid from Event( ec_subject='User' and ec_activity in (Logon') and ec_theme in ('UserGroup', 'Authentication') and ec_outcome='Success' and user_dst is not null );`
	`@Name('Pattern')`

	`@RSAAlert(oneInSeconds=0, identifiers={"user"})`
	`select * from FilteredEvents`
	`match_recognize (`
	`partition by user`
	`measures C as c, L as l, D as d`
	`pattern (C L+D)`
	`define C as C.ecactivity= 'Create',`
	`L as L.ecactivity= 'Logon',`
	`D as D.ecactivity='Delete'`
	`);`

EPL n° 5: Utilisation de chaque @RSAAlert(oneInSeconds=0, identifiers={"user_src"})

SELECT a.time as time,a.ip_src as ip_src,a.user_dst as user_dst,a.ip_dst as ip_dst,a.alias_host as alias_host from pattern[every (a=Event (ec_subject='User' and ec_activity='Create' and ec_theme='UserGroup' and ec_outcome='Success') -> (Event(ec_subject='User' and ec_activity='Logon' and ec_theme='Authentication' and user_src=a.user_dst) -> b=Event (ec_subject='User' and ec_activity='Delete' and ec_theme='UserGroup' and user_dst=a.user_dst))) where timer:within(300 sec)];

Nom de la règle	CreateUserLoginandDeleteUser
Description de la règle	Détectez un schéma dans lequel un utilisateur crée un compte utilisateur suivi de la connexion par le même utilisateur, suivi de la suppression du compte utilisateur.

Exemple n° 3 :

Nombre excessif d'échecs de connexion à partir de la même adresse IP source

EPL n° 6: @RSAAlert(oneInSeconds=0, identifiers={"ip_src"})

Nom de la règle	ExcessLoginFailure
Description de la règle	Le même utilisateur a essayé de se connecter à partir de la même IP source et a rencontré des échecs de connexion

Code de règle	`SELECT * FROM`
	`Event(`
	`ip_src IS NOT NULL AND ec_activity='Logon' AND ec_outcome = 'Failure' ).std:groupwin(ip_src).win:time_length_batch(300 sec, 10) GROUP`

<table>
<tr><td>Remarque</td><td>

```
BY ip_src HAVING COUNT(*) = 10;
```


Crée la fenêtre selon ip_src
Utilise time_length_batch : Examine les événements par lots (fenêtre bascule). Chaque événement fait partie d'une seule fenêtre. La fenêtre libère les événements lorsque le délai est écoulé ou que le nombre est atteint.
Les fenêtres bascule posent un problème : les événements qui se produisent vers la fin du lot risquent de ne pas aboutir à une alerte.

Dans la séquence d'événements ci-dessous, à t=301, bien qu'il y ait eu 10 échecs de la connexion au cours des 300 dernières secondes pour la même connexion, aucune alerte ne se déclenche, car le lot d'événements a été interrompu à t=300

Temps t	Échecs de la connexion pour des utilisateurs spécifiques	Alerte	Lot temporel
0	0	0	1
295	6	0	1
299	3	0	1
301	1	0	2
420	6	0	2
550	3	0	2
600	0	0	3
720	6	0	3
850	3	0	3
900	1	1	3 se termine et 4 commence

Vous pouvez résoudre le problème ci-dessus en utilisant des fenêtres win:time (EPL n° 7) au lieu des fenêtres win:time_length_batch.
Le regroupement externe contrôle les événements au fil du temps. Admettons que vous ayez 9 événements à la fin de 60 secondes, le moteur Esper va transmettre ces 9 événements au Listener. Les clauses de regroupement et de nombre vont limiter cette situation, car le nombre n'est pas égal à 10.
Vous pouvez modifier les valeurs de temps et de nombre comme vous

</td></tr>
</table>

	le souhaitez.

EPL n° 7: @RSAAlert(oneInSeconds=0, identifiers={"ip_src"})

Nom de la règle	ExcessLoginFailure
Description de la règle	Le même utilisateur a essayé de se connecter à partir de la même IP source et a rencontré des échecs de connexion
Code de règle	`SELECT * FROM Event( ip_src IS NOT NULL AND ec_activity='Logon' AND ec_outcome = 'Failure' ).std:groupwin(ip_src).win:time (300 sec) GROUP BY ip_src HAVING COUNT(*) = 10`
Remarque	• Il s'agit d'une fenêtre glissante. Par conséquent, une fois qu'une alerte est déclenchée pour un ensemble d'événements, ceuxei peuvent être utilisés pour une autre alerte jusqu'à ce que le délai soit dépassé. • Si 10 événements sont impliqués dans le déclenchement d'une alerte, seul le dernier événement apparaît • Si vous utilisez < ou >, il est possible que plusieurs alertes soient visibles. Vous devez utiliser la suppression d'alerte en conséquence.

Exemple n° 4 :

Plusieurs échecs de connexion de plusieurs utilisateurs différents, de la même source vers la même destination. Plusieurs échecs de connexion d'un seul utilisateur, de plusieurs sources différentes vers la même destination.

EPL n° 8 : utilisation de groupwin, time_length_batch et unique

Nom de la règle	MultiplefailedLogins
Description de la règle	Il existe plusieurs échecs de connexion pour les cas suivants : - de plusieurs utilisateurs, de la même source vers la même destination ;

Code de règle	- d'un seul utilisateur, de plusieurs sources vers la même destination. `SELECT * FROM Event( ec_activity='Logon' AND ec_outcome='Failure' AND ip_src IS NOT NULL AND ip_dst IS NOT NULL AND user_dst IS NOT NULL ).std:groupwin(ip_src,ip_dst).win:time_length_batch(300 seconds, 5}).std:unique (user_dst) group by ip_src,ip_dst having count(*) = 5;`
Remarque	• ip.dst et ip.src sont communs à tous les événements. • user_dst est unique pour tous les événements. • L'alerte se déclenche lorsqu'au moins 5 utilisateurs différents essaient de se connecter à partir de la même combinaison ip.src et ip.dst.

Exemple n° 5 :

Aucun trafic de log en provenance d'un périphérique dans une période donnée.

EPL n° 9 : utilisation de groupwin, time_length_batch et unique

Nom de la règle	NoLogTraffic
Description de la règle	Aucun trafic de log constaté en provenance d'un périphérique dans une période donnée.
Code de règle	`SELECT * FROM pattern [every a = Event (device_ip IN ('10.0.0.0','10.0.0.1') AND medium = 32) -> (timer:interval (3600 seconds) AND NOT Event(device_ip = a.device_ip AND device_type = a.device_type AND medium = 32))];`
Remarque	• La règle détecte uniquement une chute soudaine de trafic. Elle ne déclenche pas d'alerte si le trafic est inexistant. Vous avez besoin d'au moins 1 événement pour que la règle envoie l'alerte. • Liste des adresses IP ou des noms d'hôtes de périphériques en entrée. Seuls ces systèmes peuvent être

	analysés. • L'entrée du délai est obligatoire. L'alerte est déclenchée lorsque l'intervalle de temps entre les événements dépasse la durée d'entrée.

Exemple n° 6 :

Plusieurs échecs de connexion NON suivis d'un événement de verrouillage par le même utilisateur.

EPL n° 10 : utilisation de groupwin, time_length_batch et unique

Nom de la règle	FailedloginswoLockout
Description de la règle	Plusieurs échecs de connexion du même utilisateur ne sont pas suivis de l'événement de verrouillage (Lockout).

Code de règle	`SELECT * FROM pattern [every-distinct (a.user_dst, a.device_ip, 1 msec) (a= Event(ec_activity='Logon' and ec_ outcome='Failure' and user_dst IS NOT NULL) -> [2]( Event( device_ip =a.device_ip and ec_activity='Logon' and ec_outcome='Failure' and user_ dst=a.user_dst)`
	`AND NOT Event( ( ec_activity='Logon' and ec_outcome='Success' and device_ip = a.device_ip and user_dst=a.user_dst) or (ec_activity='Lockout' and device_ip = a.device_ip and user_dst=a.user_dst))))`
	
	`where timer:within(60 seconds) -> (timer:interval(30 seconds) and not Event(device_ip=a.device_ip and user_ dst=a.user_dst and ec_ activity='Lockout')) ];`

Remarque	• La requête ci-dessus détecte l'absence d'un événement de verrouillage après l'occurrence de 2 échecs de connexion pour le même utilisateur. • Les nombreux échecs de connexion sont recensés et

	supposés se produire dans un laps de temps donné. De plus, dans la pratique, on support que l'événement de verrouillage se produit dans un court délai après l'occurrence du dernier événement d'échec de connexion, car la valeur de seuil des échecs de connexion par utilisateur est définie dans un domaine donné. • Dans la requête actuelle, chaque élément distinct supprime un nouveau fil pour l'association de l'utilisateur et du périphérique pendant 1 milliseconde. • Le délai alloué pour 3 échecs de connexion est de 60 secondes, à partir du 1er échec. Le temps d'attente de l'événement de verrouillage est de 30 secondes

Exemple 7 :

Fonctions personnalisées pour effectuer des opérations LIKE et REGEX pour des éléments ARRAY.

EPL #11: @RSAAlert(oneInSeconds=0)

Nom de la règle	MatchLikeRegex
Description de la règle	Il existe pour effectuer des fonctions personnalisées pour effectuer des comparaisons LIKE et REGEX de clés méta de baie.

Code de règle	`SELECT * FROM pattern[`
	`e1=Event(matchLike(alias_host, "10.0.0.%")) AND`
	`e2=Event(matchRegex(alias_host, "10\.0\.0\.1[0-9][0-9]"))`
	`where timer:within(5 Minutes)];`

Remarque :
1. « . » dans les clés méta doit être remplacé par (”_”).
2. Tous les modèles doivent avoir une limite temporelle.
3. Les balises appropriées doivent être utilisées devant les instructions
 a) @RSAPersist:
 b) @RSAAlert:

Pour obtenir des informations supplémentaires, consultez :

- Documentation EPL : http://www.espertech.com/esper/documentation.php
- Outil EPL en ligne : http://esper-epl-tryout.appspot.com/epltryout/mainform.html

Utilisation des règles

Cette section décrit les procédures supplémentaires que vous pouvez effectuer sur des règles. Vous souhaiterez effectuer l'une des procédures suivantes :

- Modifier, dupliquer ou supprimer une règle
- Filtrer ou rechercher des règles
- Importer ou exporter des règles

Modifier, dupliquer ou supprimer une règle

Cette rubrique fournit des instructions pour modifier, dupliquer ou supprimer une règle ESA (Event Stream Analysis). Lorsque vous modifiez une règle, ESA applique les critères mis à jour. Aucune modification n'est apportée aux alertes précédemment générées.

Procédures

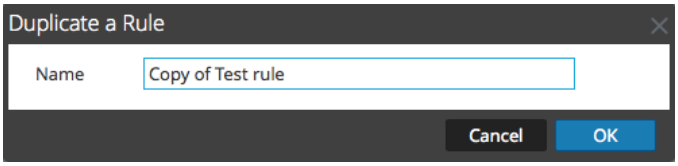
Modifier une règle

1. Accédez à l'onglet **CONFIGURER > Règles ESA > Règles**.
   L'onglet Règles s'affiche.
2. Dans la **Bibliothèque de règles**, sélectionnez la règle que vous souhaitez modifier, puis cliquez sur  .
   Selon le type de règle, l'onglet de règle correspondant s'affiche.
3. Modifiez les paramètres requis.
4. Cliquez sur **Save**.

Dupliquer une règle

1. Dans la **Bibliothèque de règles**, sélectionnez la règle à dupliquer, plus cliquez sur  .

2. La boîte de dialogue Dupliquer une règle s'affiche. Le système ajoute **Copie de** devant le nom de la règle.

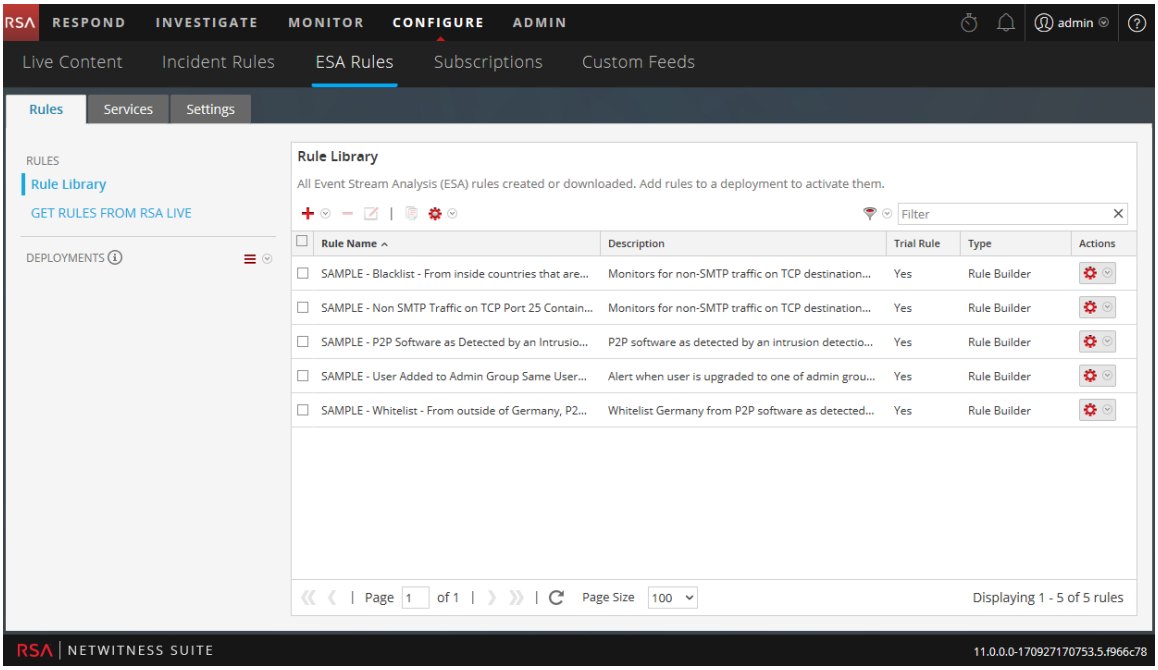


3. Dans le champ **Nom**, saisissez un nom unique pour la règle dupliquée, puis cliquez sur **OK**.

Une règle dupliquée portant le nouveau nom est ajoutée à la bibliothèque de règles.

Supprimer une règle

1. Accédez à **CONFIGURER > Règles ESA > Règles**.
   L'onglet Règles s'affiche.



2. Dans la bibliothèque de règles, sélectionnez une ou plusieurs règles, puis cliquez sur .

   Une boîte de dialogue d'avertissement s'affiche.

3. Cliquez sur **Yes**.
   Un message de confirmation de la suppression de la règle s'affiche et la règle sélectionnée est supprimée de la bibliothèque de règles.

Filtrer ou rechercher des règles

Cette rubrique montre aux analystes comment spécifier les types de règle qui s'affiche dans la bibliothèque de règles.

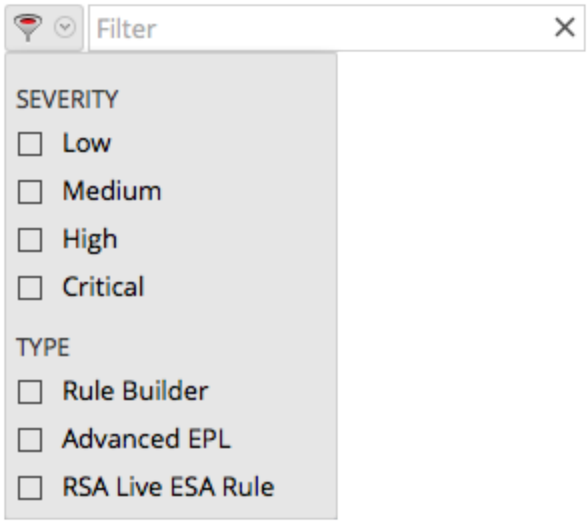
Conditions préalables

Familiarisez-vous avec les composants de la vue Bibliothèque de règles. Pour plus d'informations, reportez-vous à la rubrique Panneau Bibliothèque de règles.

Procédures

Filtrer

1. Accédez à **CONFIGURER > Règles ESA**.
   L'onglet Règles s'affiche par défaut.
2. Dans la barre d'outils du panneau **Bibliothèque de règles**, cliquez sur et sélectionnez la gravité et les types de règle à afficher dans la liste Bibliothèque de règles. La figure suivante illustre la liste déroulante Filtre.



   Les types de règle sélectionnés apparaissent dans la liste.

Recherche

1. Accédez à **CONFIGURER > Règles ESA**.
   L'onglet Règles s'affiche par défaut.
2. Dans la barre d'outils du panneau **Bibliothèque de règles**, saisissez un nom de règle dans le champ Filtre.
   Le panneau Bibliothèque de règles répertorie les règles correspondant aux noms saisis dans le champ Filtre.

Importer ou exporter des règles

La rubrique fournit des instructions pour importer des règles ESA à partir d'une instance NetWitness Suite et exporter des règles ESA sur votre disque dur pour pouvoir conserver une copie locale.

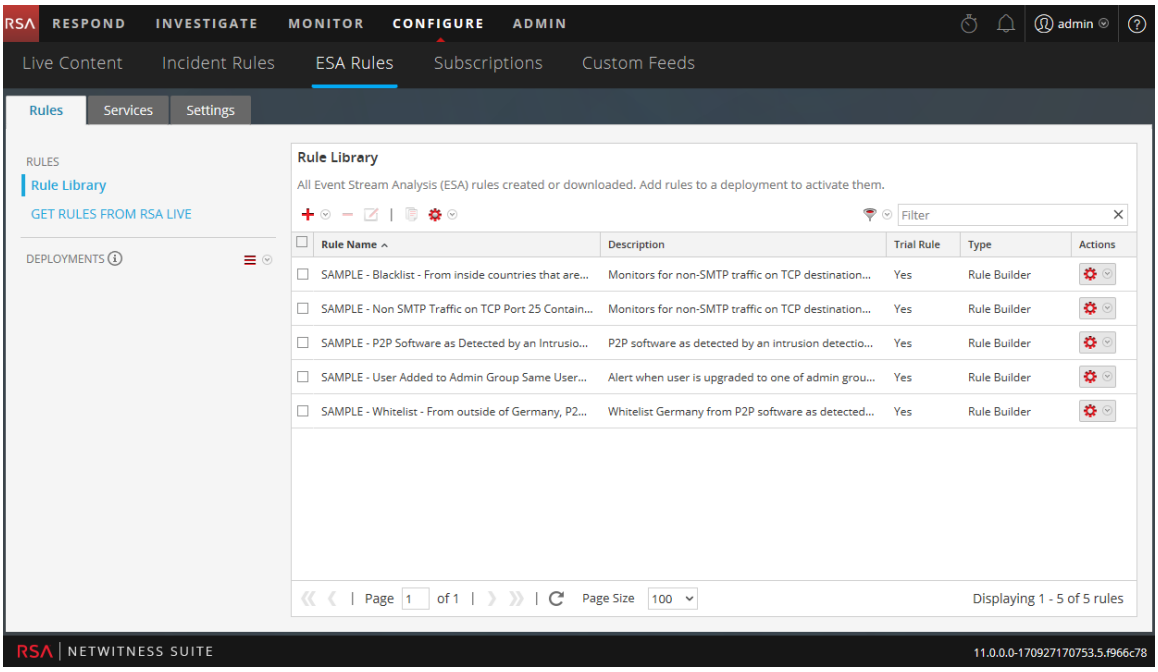
Si vous avez exporté une règle dans une version antérieure de NetWitness Suite, les conditions ci-dessous s'appliquent lorsque vous importez la règle dans la version 10.5 ou ultérieure :

- Règle exportée dans la version 10.3 – Vous ne pouvez pas importer des règles vers la version 10.5 ou ultérieure.
- Règle exportée dans la version 10.4 – Le comportement de la règle varie selon que la corrélation croisée est désactivée (valeur par défaut) ou activée :
  - Désactivée – Vous pouvez importer des règles dans la version 10.5 ou ultérieure.
  - Activée – Vous devez redémarrer NetWitness Suite ou apporter une modification mineure à la règle, enregistrer la règle, supprimer la modification mineure et enregistrer à nouveau la règle. L'une ou l'autre procédure génère la règle de transfert nécessaire à la fonction de corrélation intersites de la version 10.5 ou ultérieure.

Procédures

Importer des règles ESA

1. Accédez à l'onglet **CONFIGURER > Règles ESA > Règles**.
   L'onglet Règles s'affiche.



2. Dans la barre d'outils **Bibliothèque de règles**, sélectionnez > **Importer**.
   La boîte de dialogue Importer des règles ESA s'affiche.

3. Cliquez sur **Parcourir** pour rechercher et sélectionner le fichier contenant les règles ESA.
4. Cliquez sur **Importer**.

Exporter

1. Sélectionnez une ou plusieurs règles ESA et cliquez sur > **Exporter** dans la barre d'outils Bibliothèque de règles.
   Une boîte de dialogue d'avertissement s'affiche.
2. Cliquez sur **Yes**.
   La boîte de dialogue Exporter les règles s'affiche.
3. Dans le champ **Saisir un nom de fichier**, saisissez un nom pour le fichier contenant les règles ESA, puis cliquez sur **Exporter**.
   Le fichier est exporté en tant que fichier binaire sur votre ordinateur.

Remarque : Le fichier binaire ne peut pas être modifié.

Choisir comment être notifié des alertes

Cette rubrique explique comment ajouter différentes méthodes de notification à une règle. Les autorisations de rôle Administrateur, Responsable du SOC ou DPO sont requises pour toutes les tâches de cette section.

Lorsqu'une règle déclenche une alerte, ESA peut envoyer une notification par les moyens suivants :

- E-mail
- SNMP
- Syslog
- Script

Pour configurer une notification, vous devez configurer ces composants :

- Serveur de notification – Après avoir configuré un serveur de notification, vous pouvez l'ajouter à une règle. Lorsque la règle déclenche une alerte, la règle va utiliser ce serveur pour envoyer des notifications d'alerte.
- Notifications – Ce sont les sorties, qui peuvent être de type e-mail, script, SNMP et Syslog. Lorsque vous concevez une règle, vous pouvez spécifier la notification d'une alerte.
- Modèles – Le format d'une notification d'alerte est défini dans un modèle.

Event Stream Analysis propose deux fonctionnalités : la suppression d'alerte et la réglementation du taux d'alerte. La suppression d'alerte permet de vérifier que plusieurs e-mails ne sont pas envoyés pour la même alerte. Par exemple, utiliser une règle pour détecter les échecs de connexions des utilisateurs. Si vous définissez la suppression d'alerte sur trois minutes, vous ne verrez que les alertes générées dans ce laps de temps. Ceci est inférieur au nombre d'alertes que vous pouvez voir sans suppression d'alerte. Certaines alertes peuvent être des doublons. Avec la suppression d'alerte, les e-mails ne sont pas envoyés pour les alertes en double. Cela garantit que la boîte de réception ne soit saturée de notifications d'alerte redondantes.

La réglementation du taux d'alerte est une mesure préventive qui garantit que les alertes issues de règles mal interprétées n'inondent pas le système. Cela permet de s'assurer que ESA ne dépasse pas la limite configurée d'envoi d'e-mails en une minute.

Les serveurs de notification, les notifications et les modèles sont configurés dans la vue Système d'administration. Pour plus d'informations, consultez les sections « Configurer les serveurs de notification », « Configurer les sorties de notification » et « Configurer des modèles pour les notifications » dans le *Guide de configuration système*.

Méthodes de notification

Lorsqu'une règle déclenche une alerte, ESA peut envoyer une notification par les moyens suivants :

- E-mail
- SNMP
- Syslog
- Script

Notifications par e-mail

Event Stream Analysis peut envoyer des notifications aux utilisateurs par e-mail concernant les différents événements du système.

Pour configurer ces notifications par e-mail, vous devez :

- Configurer le serveur de messagerie SMTP en tant que fournisseur de sortie. Pour obtenir des instructions, reportez-vous à la section « Configurer les paramètres de messagerie d'un serveur de notification » dans le *Guide de configuration système*.
- Configurer un compte de messagerie pour recevoir les notifications. Pour obtenir des instructions, reportez-vous à la section « Configurer la messagerie en tant que méthode de notification » dans le *Guide de notification système*.
- Configurez un modèle pour la notification par e-mail. Pour savoir comment procéder, consultez la section « Configurer un modèle » dans le *Guide de configuration système*.

SNMP

Event Stream Analysis peut envoyer des événements comme trap SNMP à un hôte de trap SNMP configuré.

Remarque :
Le fichier MIB **NETWITNESS-MIB.txt** se trouve sur le RPM ESA à l'emplacement suivant : */usr/share/snmp/mibs*. Avec le fichier MIB, vous serez en mesure d'identifier les alertes SNMP déclenchées à partir d'ESA. La valeur Trap OID d'ESA est de 20.

Pour configurer ces notifications SNMP, vous devez :

- Configurer l'hôte de trap SNMP en tant que fournisseur de sortie. Pour obtenir des instructions, reportez-vous à la section « Configurer les paramètres SNMP d'un serveur de notification » dans le *Guide de configuration système*.
- Configurer les paramètres de trap SNMP en tant qu'action de sortie. Pour savoir comment procéder, consultez la section « Configurer le protocole SNMP en tant que méthode de notification » dans le *Guide de configuration système*.
- Configurez un modèle pour SNMP. Pour savoir comment procéder, consultez la section « Configurer un modèle» dans le *Guide de configuration système*.

Syslog

Event Stream Analysis peut envoyer des événements et consolider les logs au format Syslog vers un serveur Syslog.

Pour configurer ces notifications Syslog, vous devez :

- Configurer les paramètres du serveur Syslog en tant que fournisseur de sortie. Pour obtenir des instructions, reportez-vous à la section « Configurer les paramètres Syslog d'un serveur de notification » dans le *Guide de configuration système*.
- Configurez le format des messages Syslog en tant qu'action de sortie. Pour savoir comment procéder, consultez la section « Configurer Syslog en tant que méthode de notification » dans le *Guide de configuration système.*
- Configurez un modèle pour Syslog. Pour savoir comment procéder, consultez la section « Configurer un modèle» dans le *Guide de configuration système*.

Script Alerter

Outre les notifications d'alerte, ESA permet aux utilisateurs d'exécuter des scripts en réponse aux alertes ESA.

Les scripts vous permettent d'effectuer une intégration personnalisée avec les applications qui existent dans votre environnement. Par exemple, si vous souhaitez ouvrir un ticket d'incident à partir d'une application lorsqu'une alerte spécifique est déclenchée, Script Alerter vous permet d'écrire un script qui appelle l'API d'application et ESA l'invoque lorsque la règle ESA spécifique est déclenchée. Vous pouvez configurer un modèle FreeMarker pour définir quels détails vous souhaitez extraire de la sortie de la règle ESA et le transférer comme arguments de ligne de commande dans le script.

Pour utiliser l'alerte de script, vous devez :

- Configurer l'identité de l'utilisateur et d'autres détails qui sont nécessaires à l'exécution du script. Pour savoir comment procéder, consultez la section « Configurer un script pour un

serveur de notification » dans le *Guide de configuration système*.

- Définissez le script. Pour savoir comment procéder, consultez la section « Configurer un script en tant que méthode de notification » dans le *Guide de configuration système*.
- Configurez un modèle pour le script. Pour savoir comment procéder, consultez la section « Configurer un modèle » dans le *Guide de configuration système*.

Ajouter une méthode de notification à une règle

Cette rubrique indique aux administrateurs comment ajouter une notification, telle qu'un e-mail, à une règle. ESA utilise la méthode de notification lorsqu'elle génère une alerte pour un événement qui répond aux critères de règle.

Vous pouvez ajouter une notification à une règle pour qu'ESA vous informe quand une règle déclenche une alerte. Bien que les champs de notification ne soient pas obligatoires, il est recommandé d'ajouter une notification à une règle.

Lorsque vous ajoutez une méthode de notification à une règle, sélectionnez les informations suivantes :

- Résultat
- Notification
- Serveur de notification
- Modèle

Conditions préalables

- Votre rôle doit posséder des autorisations pour gérer les règles.
- La règle doit exister.
- La méthode de notification doit être configurée avec un serveur et un modèle pris en charge : Accédez à **ADMIN** > **Système > Notifications globales**.

  Pour les procédures détaillées, reportez-vous au *Guide de configuration système*.

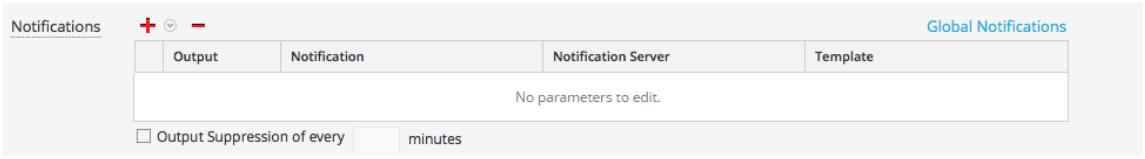
Procédure

Pour ajouter une méthode de notification à une règle :

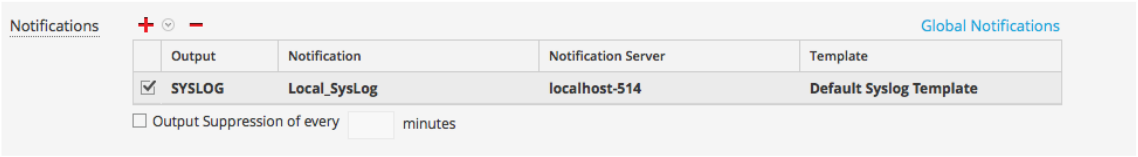
1. Accédez à l'onglet **CONFIGURER > Règles ESA > Règles**.
2. Dans la **Bibliothèque de règles**, cliquez sur  pour ajouter une nouvelle règle ou sélectionnez une règle existante, puis cliquez sur .

   Selon le type de règle, l'onglet Générateur de règles ou EPL avancé s'affiche.

La section Notifications est la même pour ces deux onglets.



3. Cliquez sur  , puis sélectionnez la **sortie** de l'alerte :
   - E-mail
   - SNMP
   - Syslog
   - Script
4. Double-cliquez sur le champ **Notification**, puis sélectionnez le nom d'une sortie précédemment configurée.
   Par exemple, Analyste niveau 1 peut être le nom d'une notification par e-mail relevant du groupe de diffusion par e-mail Analystes-L1.
5. Double-cliquez sur le champ **Serveur de notification**, puis sélectionnez le serveur qui envoie la notification.
6. Double-cliquez sur le champ **Modèle**, puis sélectionnez le format de l'alerte.
   La figure suivante montre les paramètres d'une notification syslog.

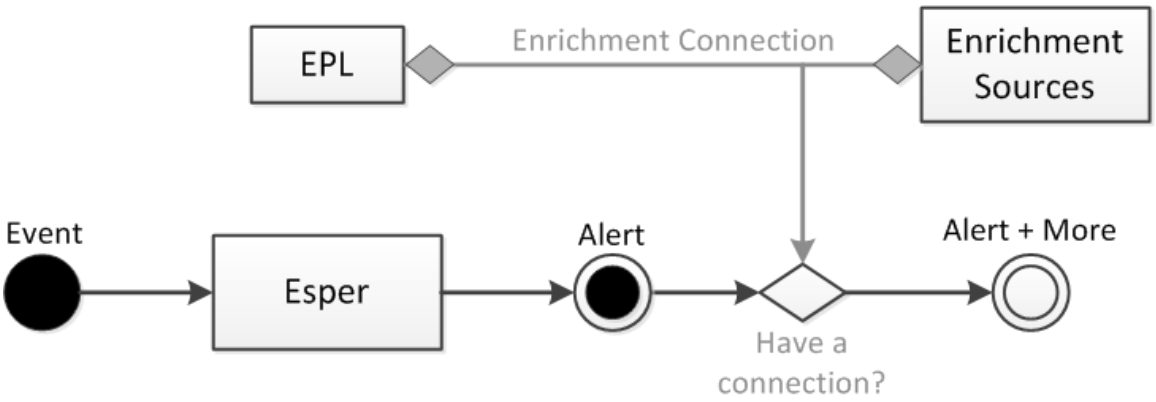


7. Pour spécifier une fréquence, sélectionnez **Limitation des sorties**, puis saisissez le nombre de **minutes**.
8. Pour ajouter une autre notification, répétez les étapes 3 à 7.
9. Cliquez sur **Enregistrer**.
   Quand ESA génère une alerte pour un événement qui répond aux critères de la règle, vous en êtes informé à l'aide de chacune des méthodes de notification ajoutées à la règle.

Ajouter une source d'enrichissement de données

Cette rubrique vous indique comment ajouter une source d'enrichissement précédemment configurée à une règle. Lorsque ESA crée une alerte, elle comprend des informations de la source.

Les enrichissements permettent d'inclure des informations contextuelles dans la logique de corrélation et la sortie d'alerte. Sans enrichissements, toutes les informations comprises dans une alerte ESA proviennent d'un service Core. Avec les enrichissements, vous pouvez demander des recherches dans différentes sources et inclure les résultats dans les alertes sortantes. La figure suivante illustre la fonction d'enrichissement.



La configuration d'enrichissement est constituée de deux unités logiques :

- Sources d'enrichissement : il s'agit des datastores d'informations contextuelles.
- Connexions d'enrichissement : elles agissent en tant que connecteurs entre les métadonnées d'alerte et les colonnes source.

ESA vous permet de réaliser des connexions entre les instructions Event Processing Language (EPL) et les sources d'enrichissement. Une fois les connexions établies, le système associe les champs sélectionnés de la sortie d'alerte aux informations dans les sources et utilise les données associées pour enrichir l'alerte envoyée. ESA peut se connecter avec les sources suivantes :

- Fenêtres nommées Esper
- Tableaux de base de données relationnelle
- Base de données MaxMindGeoIP
- Listes de surveillance RSA Warehouse Analytics

Remarque : La source d'enrichissement geoIP ne peut être ni créée, ni supprimée. Elle est fournie prête à l'emploi à l'utilisateur.

Exemple de règle avec enrichissement

L'exemple de règle suivant illustre la fonction d'enrichissement fournie par ESA :

```
@RSAAlert @Name("simple") SELECT * FROM CoreEvent(ec_theme='Login Failure')
```

La règle génère une alerte pour chaque échec de connexion et le flux d'événements suivant (simplifié) est donc reçu sur ESA :

sessionid	ec_ theme	nom d'utilisateur	ip_src	ip_dst	host_dst
1	Réussite de la connexion	dshrute	23.xx.23x.16		
2	Échec de la connexion	jhalpert	23.xx.23x.16	31.1x.x9.1x8	www.facebook.com

Une alerte possédant les composants suivants `events` peut être générée en réponse à la deuxième session :

```
{
     "events": [
         {
             "username": "jhalpert",
             "host_dst": "www.facebook.com",
             "ip_dst": "31.1x.x9.1x8",
             "sessionid": 2,
             "ec_theme": "Login Failure",
             "esa_time": 1406148964130,
             "ip_src": "23.xx.23x.16"
         }
     ]
 }
```

La sortie JSON affiche toutes les informations disponibles à inclure dans une notification ESA à l'aide d'un modèle FreeMarker
approprié. Par exemple, l'expression modèle `${events[0].username}` serait évaluée comme `jhalpert`.

Avec des enrichissements et le même flux d'événements, le même module peut générer l'alerte affichée ci-dessous. Le système
peut réaliser plusieurs connexions d'enrichissement et extraire des données contextuelles pour rendre l'alerte plus explicite.

Par exemple :
`${events[0]["RSADataScienceLookup"][0].score}`indique le score **risk** du domaine de destination calculé par le module RSA Warehouse Analytics, tandis que `${events[0]["orgchart"][0].supervisor}` indique le nom du superviseur de l'employé concerné par l'alerte (extrait d'une base de données RH) ; `${events[0]["LoginRegister"][0].username}` indique le nom de l'utilisateur dont la dernière connexion a réussi à partir du même `ip_src` (à l'aide d'une fenêtre nommée basée sur le flux).


```
{"events": [
     {
         "username": "jhalpert",
         "host_dst": "www.facebook.com",
         "GeoIpLookup": [
         {
             "city": "Cambridge",
             "longitude": -71,
             "countryCode": "US",
             "areaCode": 617,
             "metroCode": 506,
             "region": "MA",
             "dmaCode": 506,
             "ipv4Obj": "/23.62.236.16",
             "countryName": "United States",
             "postalCode": "02142",
             "ipv4": "23.62.236.16",
             "latitude": 42,
             "organization": "Verizon Business"
         }
     ],
     "RSADataScienceLookup": [
         {
             "model_id": "suspiciousDomains_1",
             "_id": "EXEC_BATCH_1_20140630153740_facebook.com",
             "score": 10,
             "key": "www.facebook.com"
         }
     ],
     "orgchart": [
         {
             "supervisor": "mscott",
             "name": "James Halpert",
             "extension": 3692,
             "location": "Scranton",
             "department": "Sales",
```

```
            "id": "jhalpert"
        }
    ],
    "ip_dst": "31.13.69.128",
    "sessionid": 2,
    "LoginRegister": [
        {
            "username": "dshrute",
            "ip_src": "23.62.236.16"
        }
    ],
    "ec_theme": "Login Failure",
    "esa_time": 1406155218912,
    "ip_src": "23.62.236.16"
    }
]}
```


Configurer une connexion à la base de données

Cette rubrique donne des éléments pour configurer une connexion à une base de données externe capable de fournir des informations supplémentaires au niveau des alertes. Configurez une connexion de base de données pour être en mesure de configurer la base de données en tant que source d'enrichissement et ajouter d'autres informations pour les alertes. Ce processus comprend trois étapes :

1. Configurer une connexion à une base de données.
2. Configurer une base de données externe en tant que source d'enrichissement.
3. Ajouter la source d'enrichissement à une règle

Cette section explique l'étape 1.

Exemple

Cet exemple montre comment l'ajout d'une base de données en tant que source d'enrichissement permet d'ajouter une valeur aux alertes.

Une règle détecte des utilisateurs qui tentent de s'inscrire à un service de messagerie furtif. Vingt-cinq utilisateurs correspondent aux critères de règle. Sans l'enrichissement, l'alerte contient 25 ID utilisateur. Avec l'enrichissement, l'alerte inclut également les informations suivantes pour chaque ID utilisateur :

- Name
- Title

- Département
- Office Location

Éléments dépendants

Lorsque vous configurez une base de données, les conditions suivantes s'appliquent :

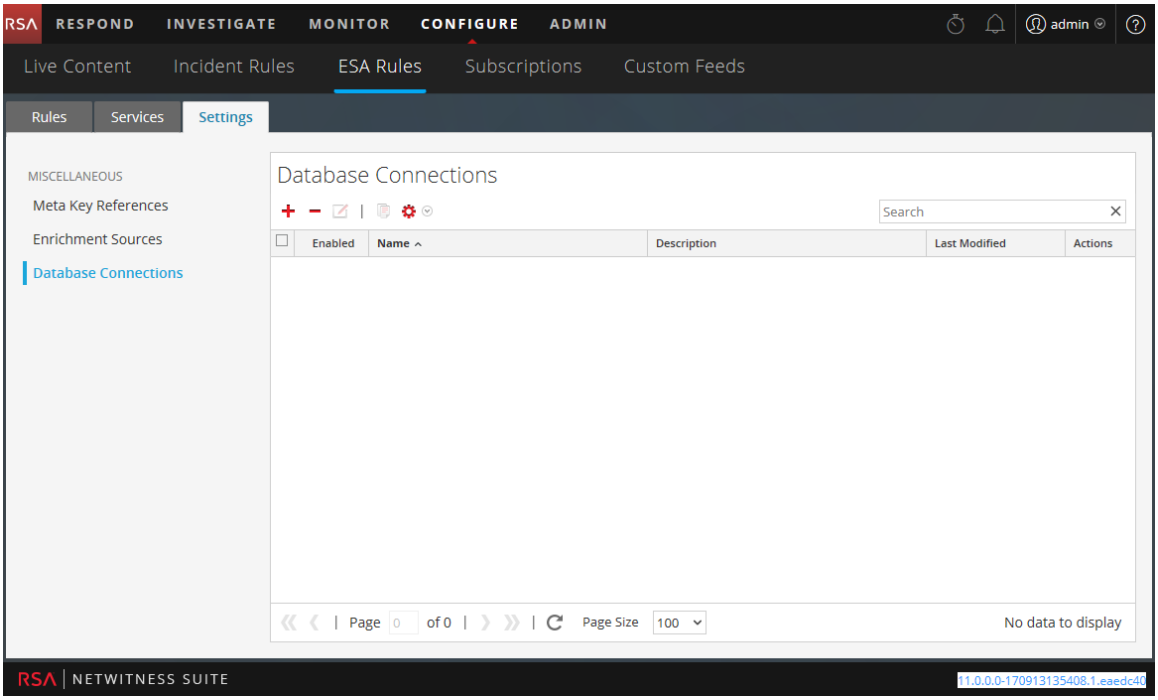
- Une référence à la base de données est déployée sur chaque ESA, même si l'ESA ne déploie aucune règle qui utilise la base de données en tant que source d'enrichissement.
- Si le serveur qui héberge la base de données est défaillant, cela impacte le déploiement.
  - Un déploiement actif continue de collecter les données et d'exécuter les règles, mais les enrichissements n'apparaîtront pas dans les alertes.
  - Le nouveau déploiement échoue tant que l'hôte n'est pas redémarré.

Procédure

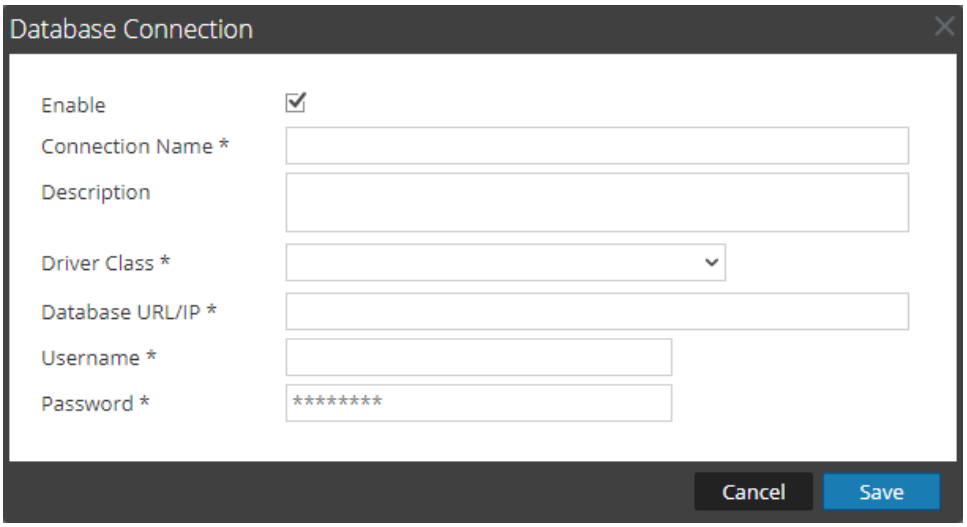
Configurer une connexion à la base de données :

1. Accédez à **CONFIGURER > Règles ESA**.
2. Cliquez sur l'onglet **Paramètres**.
3. Dans le panneau des options, sélectionnez **Connexions à la base de données**.

   Le panneau Connexions à la base de données s'affiche.



4. Cliquez sur + pour ajouter une connexion à la base de données.



5. Dans la boîte de dialogue **Connexion à la base de données**, fournissez les informations suivantes :

Champ	Description
Activer	Sélectionnez Activer pour enrichir l'alerte avec des données supplémentaires. Par défaut, l'option Activer est sélectionnée. Désélectionnez l'option Activer pour exclure les autres données de l'alerte.
Nom de la connexion	Saisissez un nom pour identifier la connexion. Lorsque vous ajoutez une base de données en tant que source d'enrichissement, ce nom s'affiche dans la liste des connexions de base de données.
Description	(Facultatif) Saisissez une brève description à propos de la connexion de base de données.
Catégorie de pilote	Sélectionnez une classe de pilote appropriée pour la base de données. Deux pilotes sont fournis avec NetWitness Suite, MongoDB et Postgres.
URL de base de données ou adresse IP	Saisissez l'URL ou l'adresse IP de la base de données à configurer.
Username	Saisissez le nom d'utilisateur permettant d'accéder à la base de données.
Mot de passe	Saisissez le mot de passe permettant d'accéder à la base de données.

6. Cliquez sur **Enregistrer.**

Pour plus d'informations, reportez-vous à la rubrique Onglet Paramètres.

Sources d'enrichissement

Cette rubrique explique les options permettant d'ajouter une source de données externe pour fournir des informations supplémentaires au niveau des alertes. Les sources d'enrichissement fournissent des informations supplémentaires au niveau des alertes. Par exemple, une base de données peut suggérer un nom, un département et un emplacement de bureau si un utilisateur répond aux critères de la règle. Il existe trois types de sources d'enrichissement :

- Référence BD externe
- Table en mémoire
- Warehouse Analytics

Configurer une base de données en tant que source d'enrichissement

Vous pouvez configurer une base de données en tant que source d'enrichissement pour pouvoir l'ajouter à une règle. Ensuite, le moteur Esper qui analyse les événements, accède aux informations de la base de données pour fournir d'autres informations dans l'alerte.

Par exemple, une règle détecte des utilisateurs qui tentent de s'inscrire à un service de messagerie furtif. Vingt-cinq utilisateurs correspondent aux critères de règle. L'alerte contient 25 ID utilisateur. Une base de données externe peut améliorer l'alerte en fournissant les informations supplémentaires suivantes pour chaque ID utilisateur :

- Name
- Title
- Département
- Site du bureau
- Destinataires des rapports

Vous pouvez modifier, dupliquer, importer ou exporter une connexion de base de données.

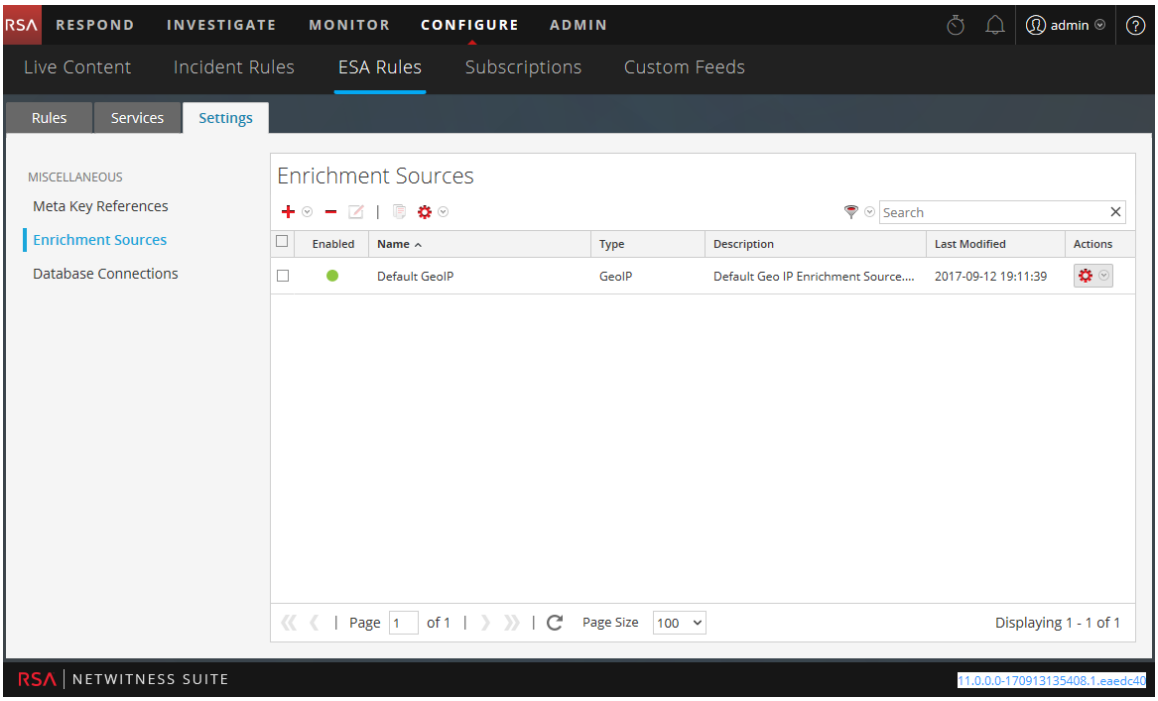
Conditions préalables

Vous devez configurer une connexion de base de données. Pour plus d'informations, reportez-vous à la rubrique Configurer une connexion à la base de données.

Procédure

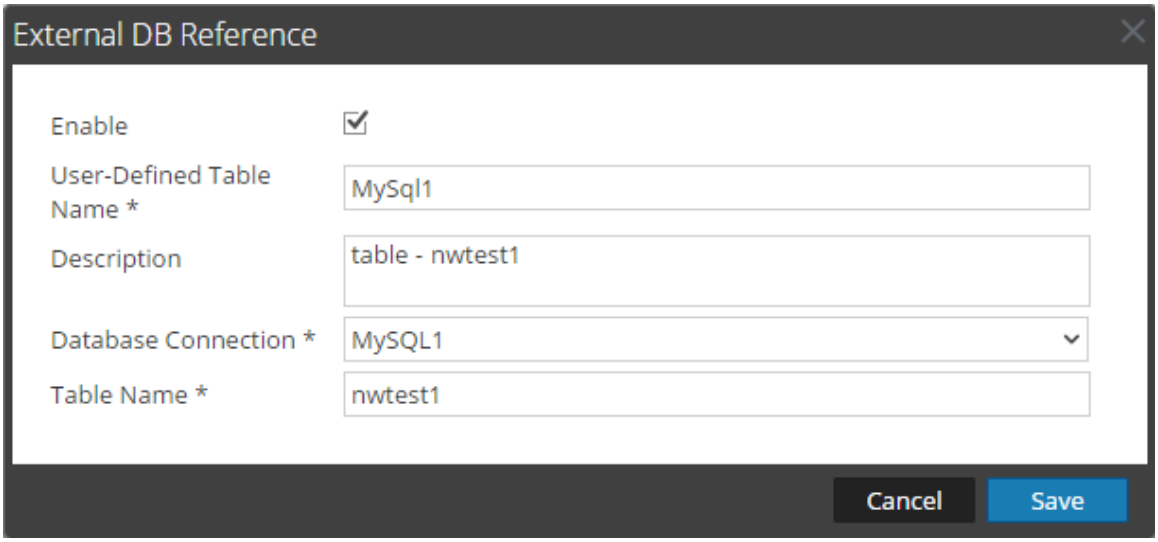
Pour configurer une base de données en tant que source d'enrichissement :

1. Accédez à **CONFIGURER > Règles ESA**.
2. Cliquez sur l'onglet **Paramètres**.
   L'onglet Paramètres s'affiche.
3. Dans le panneau d'options, sélectionnez **Sources d'enrichissement**.
   Le panneau Sources d'enrichissement s'affiche.



4. Dans le menu déroulant  , sélectionnez **Référence BD externe**. Vous devez ajouter une référence de base de données pour que cette base soit répertoriée.

La boîte de dialogue Référence BD externe s'affiche.



5. Sélectionnez **Activer** pour enrichir l'alerte avec des données supplémentaires. Cette option est sélectionnée par défaut. Si l'alerte est désactivée, elle n'est pas enrichie avec des données supplémentaires.
6. Dans le champ **Nom de la table définie par l'utilisateur**, saisissez un nom pour identifier ou intituler la configuration de base de données.
7. Dans le champ **Description**, saisissez une brève description de la configuration de base de données.
8. Dans le menu déroulant **Connexion de base de données**, sélectionnez les connexions définies.
9. Dans le champ **Nom de la table**, saisissez le nom de la table de base de données.
10. Cliquez sur **Enregistrer**.

Pour plus de détails sur les paramètres et leurs descriptions, reportez-vous à la section Onglet Paramètres.

Configurer la table en mémoire en tant que source d'enrichissement

Cette rubrique fournit des instructions sur la configuration d'une table en mémoire. Lorsque vous configurez une table en mémoire, vous téléchargez un fichier .csv en tant qu'entrée de la table. Vous pouvez associer cette table à une règle en tant que source d'enrichissement. Lorsque la règle associée génère une alerte, ESA va enrichir l'alerte avec les informations pertinentes issues de la table en mémoire.

Par exemple, une règle peut être configurée pour détecter lorsqu'un utilisateur tente de télécharger un logiciel gratuit et d'identifier la personne par un ID d'utilisateur dans l'alerte. L'alerte pourrait être enrichie avec des informations supplémentaires provenant d'une table en mémoire qui contient des détails tels que le nom complet, le titre, l'emplacement du bureau et le nombre d'employés.

Une table en mémoire est idéale pour le traitement des données simples. Elle est facile à configurer et nécessite moins de maintenance qu'une base de données. Par exemple, la Société AllTech est une petite organisation, donc l'administrateur système peut gérer les informations des employés dans un fichier .csv. Si la société AllTech se développe en une très grande entreprise, l'administrateur devra configurer une référence de base de données externe en tant qu'enrichissement et associer la base de données à une règle.

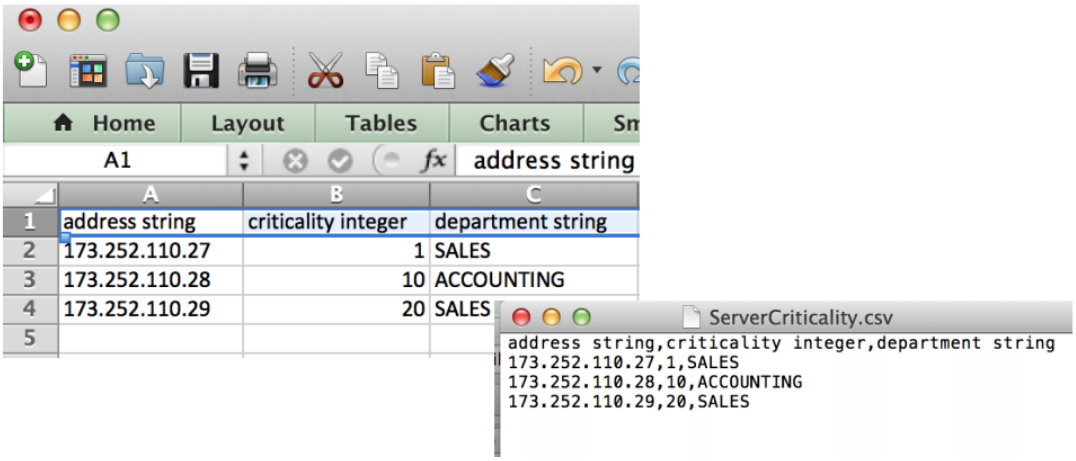
Conditions préalables

Le nom de la colonne du fichier .CSV ne peut pas contenir d'espaces.

Par exemple, *Last_Name* est correct et *Last Name* est incorrect.

Le fichier .CSV doit commencer par une ligne d'en-tête qui définit les champs et les types. Par exemple, *address string* définit le champ d'en-tête en tant qu'*address* et le type en tant que *string*.

L'exemple suivant montre un fichier .CSV valide représenté en tant que .CSV et en tant que table.

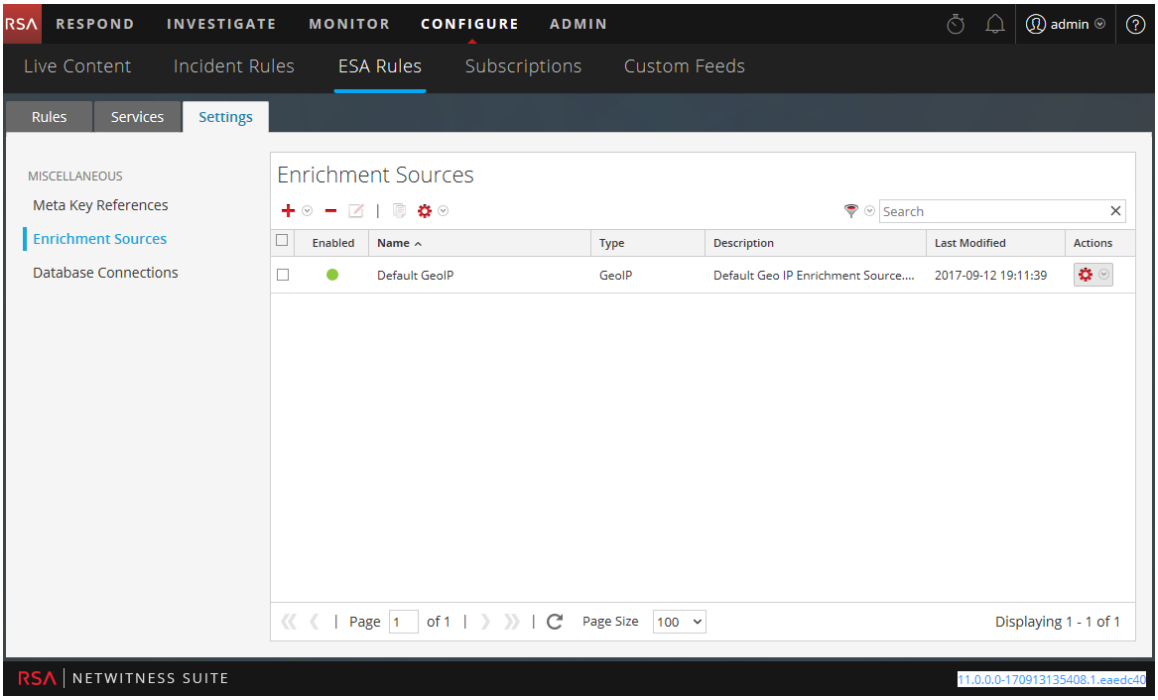


Procédures

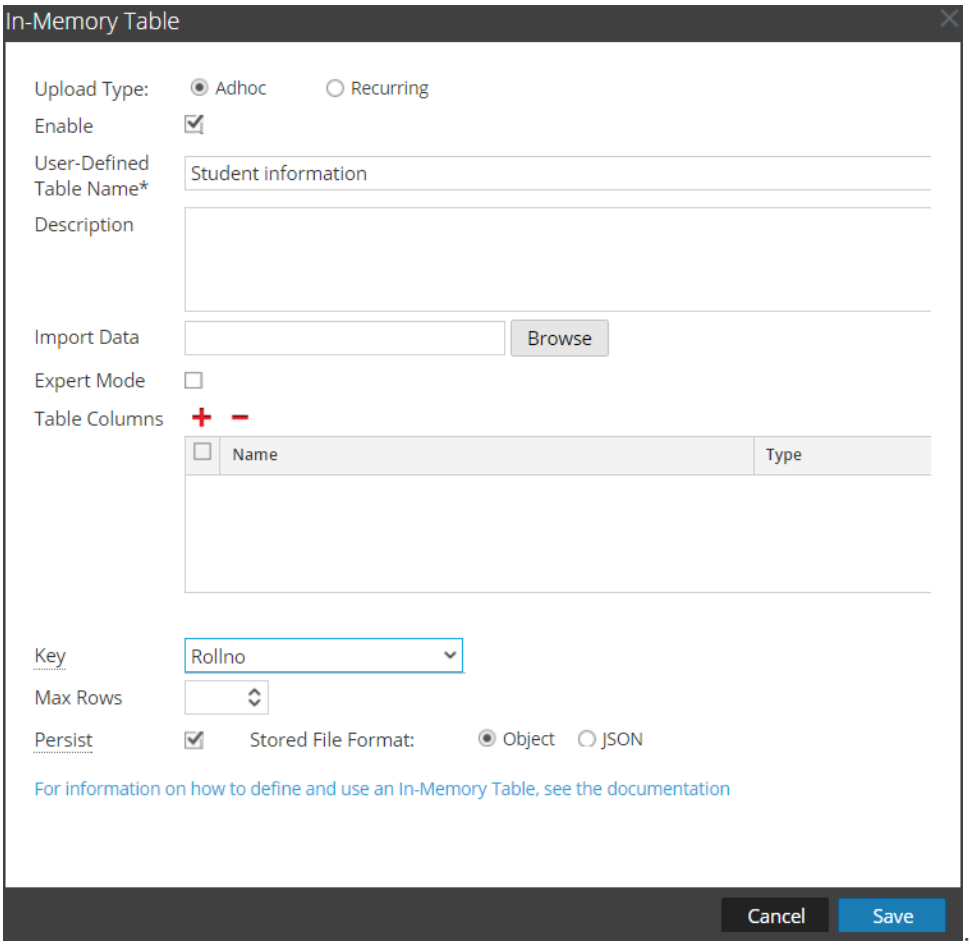
Configurer une table en mémoire Adhoc

1. Accédez à **CONFIGURER > Règles ESA**.
   La vue Configurer s'affiche avec l'onglet Règles ESA ouvert.
2. Cliquez sur l'onglet **Paramètres**.

3. Dans le panneau d'options, sélectionnez **Sources d'enrichissement**.



4. Dans la section **Sources d'enrichissement**, cliquez sur > Table en mémoire



5. Décrire la table en mémoire :

   a. Sélectionnez **Adhoc**.

   b. Par défaut, **Activer** est sélectionné. Lorsque vous ajoutez la table en mémoire à une règle, les alertes sont enrichies avec des données.
   Si vous ajoutez la table en mémoire à une règle, mais ne souhaitez pas que les alertes soient enrichies, décochez la case.

   c. Dans le champ **Nom de la table définie par l'utilisateur**, saisissez un nom, par exemple Informations sur les stagiaires, pour la configuration de la table en mémoire.

   d. Si vous souhaitez expliquer ce que l'enrichissement apporte à une alerte, saisissez une **Description** telle que :
   Lorsqu'une alerte est groupée par numéro d'inscription, cet enrichissement ajoute des informations sur les stagiaires, par exemple leur nom et leurs notes.

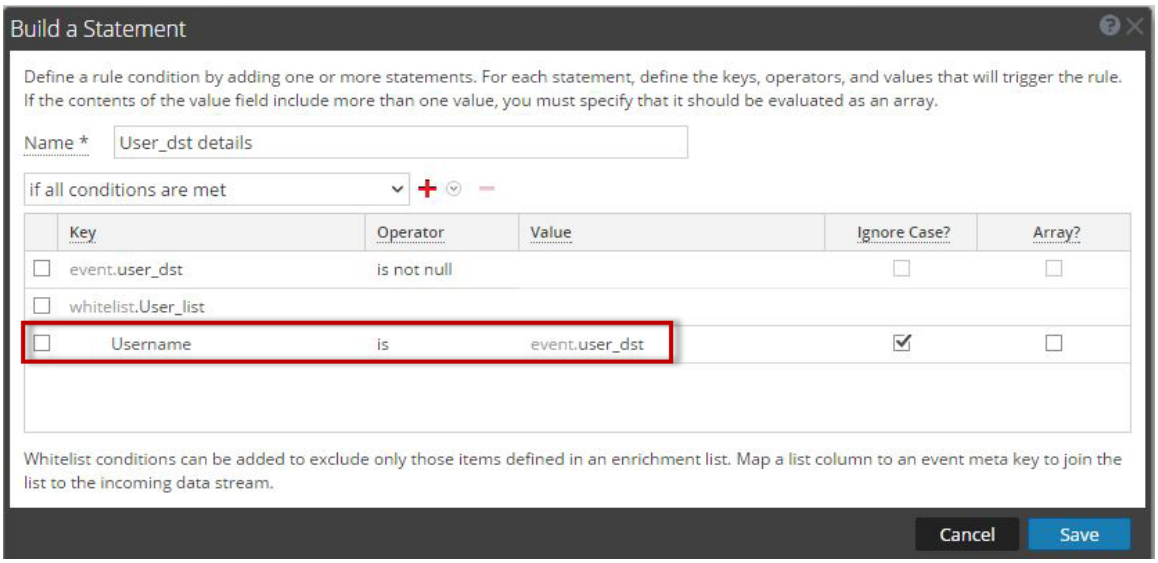
6. Dans le champ **Importer les données**, sélectionnez le fichier .CSV qui fournira les données à la table en mémoire.
7. Si vous souhaitez écrire une requête EPL pour définir une configuration de table en mémoire, sélectionnez le **Mode Expert**.
   Le champ Colonnes du tableau est remplacé par un champ **Requête**.
8. Dans la section **Colonnes du tableau**, cliquez sur + pour ajouter des colonnes à la table en mémoire.
9. Si un fichier valide est sélectionné dans le champ Importer les données, les colonnes sont renseignées automatiquement.

Remarque : Si vous avez sélectionné le mode Expert, un champ Requête s'affichera à la place de Colonnes du tableau.

10. Dans le menu déroulant **Clé**, sélectionnez le champ à utiliser comme clé par défaut pour relier les événements entrants à la table en mémoire lors de l'utilisation d'une table en mémoire de type CSV comme enrichissement. Par défaut, la première colonne est sélectionnée. Vous pouvez également modifier ultérieurement la clé lorsque vous ouvrez la table en mémoire dans les sources d'enrichissement.
11. Dans le menu déroulant **Nbre max. lignes**, sélectionnez le nombre maximum de lignes qui peut figurer dans la table en mémoire à une instance particulière.
12. Sélectionnez **Persistant** pour conserver la table en mémoire sur disque lorsque le service ESA s'arrête et pour remplir à nouveau la table lorsque le service redémarre.
13. Dans le champ **Format de fichier stocké**, effectuez l'une des actions suivantes :
    - Sélectionnez **Objet** si vous souhaitez stocker le fichier dans un format binaire.
    - Sélectionnez **JSON** si vous souhaitez stocker le fichier dans un format texte.
      Par défaut, **Objet** est sélectionné.
14. Cliquez sur **Enregistrer**
    . La table en mémoire adhoc est configurée. Vous pouvez l'ajouter à la règle comme enrichissement ou comme partie de la condition de règle. Reportez-vous à la section Ajouter un enrichissement à une règle.

Lorsque vous ajoutez une table en mémoire, vous pouvez l'ajouter à une règle comme enrichissement ou comme partie de la condition de règle. Par exemple, la règle suivante utilise une table en mémoire comme partie de la condition de règle pour créer une liste blanche. Elle utilise aussi une table de détails en mémoire dans le fichier user_dst pour enrichir l'alerte qui s'affiche.

La règle présente la table en mémoire sous la forme d'une condition de règle de liste blanche :



Ensuite, l'alerte est enrichie avec la table en mémoire User_list :

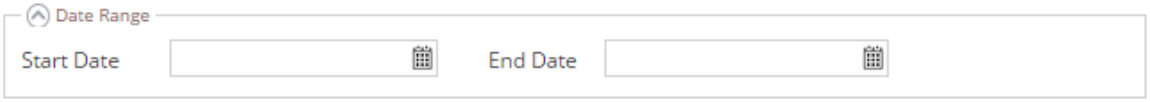
La table en mémoire user_dst sert à créer une liste blanche et est aussi utilisée pour enrichir les données dans l'alerte si l'alerte se déclenche.

Ajouter une table en mémoire récurrente

1. Accédez à **CONFIGURER > Règles ESA**.
   La vue Configurer s'affiche avec l'onglet Règles ESA ouvert.
2. Cliquez sur l'onglet **Paramètres**.
3. Dans le panneau d'options, sélectionnez **Sources d'enrichissement**.
4. Cliquez sur  > **Table en mémoire**.
5. Décrire la table en mémoire :
   a. Cliquez sur **Récurrent**.
   b. Par défaut, **Activer** est sélectionné. Lorsque vous ajoutez la table en mémoire à une règle, les alertes sont enrichies avec des données.
      Si vous ajoutez la table en mémoire à une règle, mais ne souhaitez pas que les alertes soient enrichies, décochez la case.
   c. Dans le champ **Nom de la table définie par l'utilisateur**, saisissez un nom, par exemple Informations sur les stagiaires, pour la configuration de la table en mémoire.

d. Si vous souhaitez expliquer ce que l'enrichissement apporte à une alerte, saisissez une **Description** telle que :
Lorsqu'une alerte est groupée par numéro d'inscription, cet enrichissement ajoute des informations sur les stagiaires, par exemple leur nom et leurs notes.

6. Saisissez l'URL du fichier CSV qui alimentera la table en mémoire avec des données. Cliquez sur Vérifier pour valider le lien et renseigner les colonnes du fichier .CSV. Vous pouvez ajouter ou supprimer des colonnes à l'aide du bouton plus ou moins.
7. Si le serveur est configuré derrière un autre serveur, sélectionnez **Utiliser le proxy**.
8. Si le serveur requiert des informations d'identification pour la connexion, sélectionnez **Authentifié**
9. Pour **Répéter chaque**, indiquez à quelle fréquence ESA doit rechercher la dernière version du fichier .CSV :
   a. Sélectionnez Minute(s), Heure(s), Jour(s) ou Semaine.
   b. Si vous sélectionnez Semaine, sélectionnez le jour de la semaine.
   c. Cliquez sur **Période** pour sélectionner une **date de début** et une **date de fin** pour le planning récurrent.



10. Dans le menu déroulant **Clé**, sélectionnez le champ à utiliser comme clé par défaut pour relier les événements entrants à la table en mémoire lors de l'utilisation d'une table en mémoire de type CSV comme enrichissement. Par défaut, la première colonne est sélectionnée. Vous pouvez également modifier ultérieurement la clé lorsque vous ouvrez la table en mémoire dans les sources d'enrichissement.
11. Dans le menu déroulant **Nbre max. lignes**, sélectionnez le nombre de lignes qui peut figurer dans la table en mémoire à une instance particulière.
12. Sélectionnez **Persistant** pour conserver la table en mémoire sur disque lorsque le service ESA s'arrête et pour remplir à nouveau la table lorsque le service redémarre.
13. Dans le champ **Format de fichier stocké**, effectuez l'une des actions suivantes :
    - Sélectionnez **Objet** si vous souhaitez stocker le fichier dans un format binaire.
    - Sélectionnez **JSON** si vous souhaitez stocker le fichier dans un format texte.
    Par défaut, **Objet** est sélectionné.
14. Cliquez sur **Enregistrer**.
    La table en mémoire récurrente est configurée. Vous pouvez l'ajouter à la règle comme

enrichissement ou comme partie de la condition de règle. Reportez-vous à la section Ajouter un enrichissement à une règle.

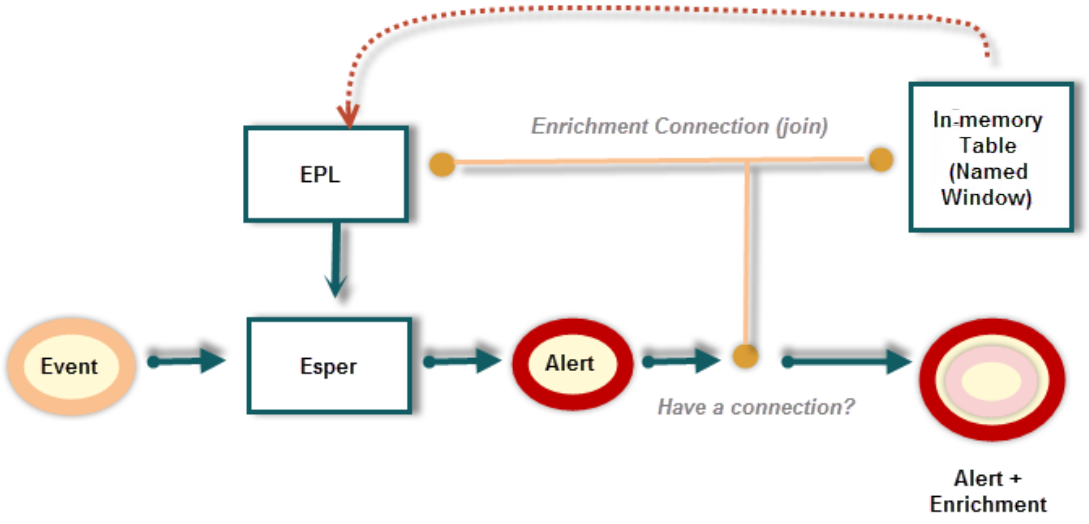
Configuration d'une requête Esper en tant que source d'enrichissement

Lorsque vous utilisez le « mode expert », vous pouvez créer une source d'enrichissement ou une fenêtre nommée d'après une requête Esper. Cela vous permet de mieux contrôler le contenu et de créer un contenu plus dynamique. Lorsque vous effectuez cette opération, une requête EPL crée la fenêtre nommée pour capturer l'état intéressant du flux d'événements.

Workflow

Le schéma suivant décrit le workflow de création d'une requête à l'aide d'une fenêtre nommée :

1. L'événement est envoyé au moteur Esper.
2. Une requête EPL est générée.
3. Une alerte est déclenchée.
4. La requête vérifie s'il existe une connexion entre l'événement et la fenêtre nommée.
5. S'il existe une connexion, la requête qui remplit la fenêtre nommée est exécutée et renseignée.
6. Le contenu issu de la fenêtre nommée est ajouté au contenu d'alerte, puis envoyé ou affiché (en fonction de vos paramètres).



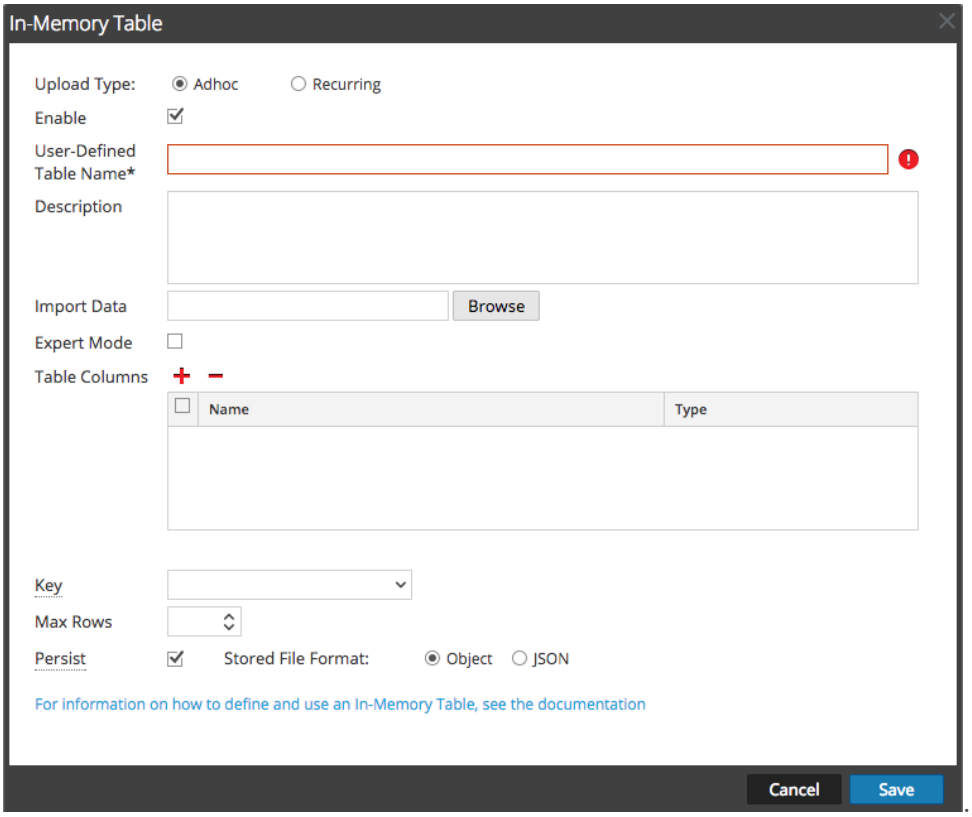
Conditions préalables

- Les métas utilisées dans l'instruction EPL doivent exister dans les données.
- Vous devez créer des instructions EPL correctes.

Procédure

Configurer une table en mémoire à l'aide d'une requête EPL

1. Accédez à **CONFIGURER > Règles ESA**.
   La vue Configurer s'affiche avec l'onglet Règles ouvert.
2. Cliquez sur l'onglet **Paramètres**.
3. Dans le panneau d'options, sélectionnez **Sources d'enrichissement**.
4. Dans la section **Sources d'enrichissement**, cliquez sur  > Table en mémoire



5. Sélectionnez **Adhoc**.
   Par défaut, Activer est sélectionné. Lorsque vous ajoutez la table en mémoire à une règle, les alertes sont enrichies avec des données.
6. Dans le champ **Nom de la table définie par l'utilisateur**, entrez un nom descriptif pour décrire la table en mémoire.
7. Si vous souhaitez expliquer ce que l'enrichissement ajoute à une alerte, saisissez ces informations dans le champ **Description**.
   Cette description s'affiche lorsque vous affichez la liste des enrichissements à partir de la

vue Sources d'enrichissement. Il est donc conseillé de saisir une description complète. Cela permet aux autres utilisateurs de comprendre le contenu de l'enrichissement sans avoir à l'ouvrir pour vérifier son contenu.

8. Sélectionnez le **Mode Expert** pour définir une configuration de table en mémoire avancée en écrivant une requête EPL.
   Le champ Colonnes du tableau est remplacé par un champ **Requête**.
9. Sélectionnez **Persistant** pour conserver la table en mémoire sur disque lorsque le service ESA s'arrête et pour remplir à nouveau la table lorsque le service redémarre.
10. Saisissez la requête EPL dans le champ **Requête**. La requête doit être correcte, et il est judicieux de la tester avant de la saisir dans le champ.
11. Cliquez sur **Enregistrer**.

Exemple

Par exemple, vous avez créé une règle consistant à rechercher cinq connexions ayant échoué, suivies d'une connexion réussie. Lorsque cette règle est déclenchée, la notification doit contenir de préférence des informations sur le dernier utilisateur connecté au système lorsque cette connexion a abouti. Pour ajouter cet enrichissement à la notification, vous pouvez choisir de créer une table de recherche en mémoire basée sur les flux de données, renseignée à partir d'événements entrants afin de maintenir un mappage d'adresses IP vers le dernier utilisateur connecté depuis cette adresse. Pour ce faire, créez un enrichissement à l'aide d'une requête en tant que source.

Étape 1 : Créer votre règle

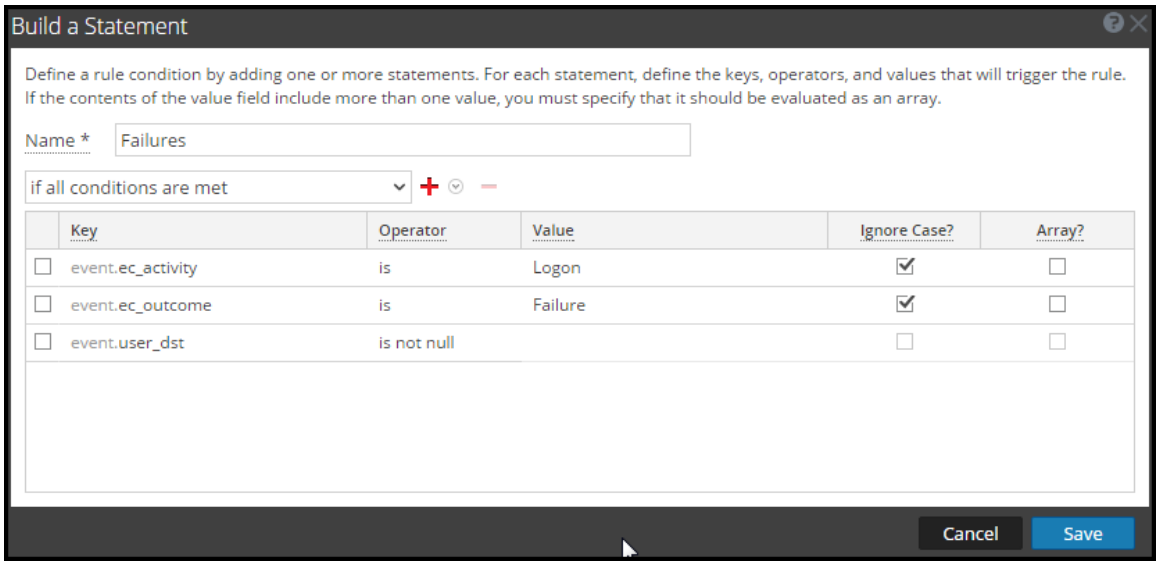
Tout d'abord, vous devez créer votre règle de corrélation. Dans ce cas, vous créez des conditions de règle d'échec et de réussite et les regroupez selon la valeur ip_src.

Condition de la règle	Description
Défaillances	Cette condition recherche cinq connexions qui ont échoué et qui ont un connecteur « Suivi de », qui signifie que la condition (Défaillances) doit être suivie par la condition suivante (success).
Success	Cette condition recherche une connexion réussie.

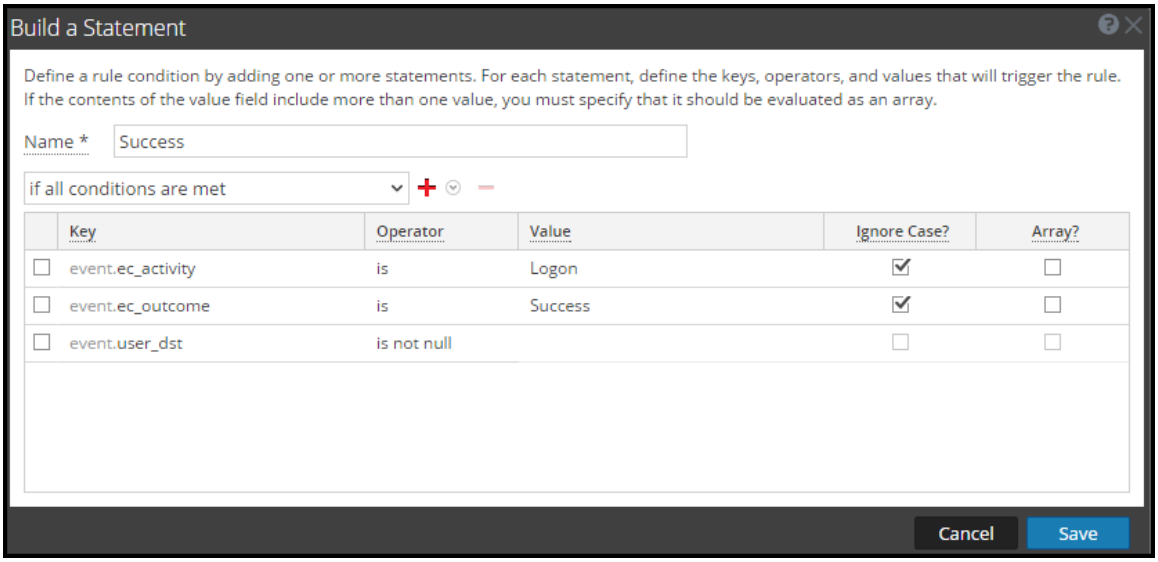
Condition de la règle	Description
GroupBy: ip_src, device class	Le champ GroupBy garantit que toutes les conditions précédentes sont groupées selon la classe d'appareil ip_srcand. C'est important pour la construction de la règle, car celle-ci tente de trouver un cas où un utilisateur a tenté de se connecter au même compte de destination à plusieurs reprises, et a fini par se connecter. Le regroupement par classe d'appareil garantit également que l'utilisateur connecté depuis la même machine tente bien de se connecter à un compte à plusieurs reprises. La règle peut produire des résultats inattendus si vous ne regroupez pas les résultats.
Se produit dans les 5 minutes	La période d'apparition des événements est égale à cinq minutes. Si les événements se produisent hors de cette période, la règle ne se déclenche pas.
Séquence d'événements Strict	La séquence d'événements est configurée pour une correspondance stricte des schémas. Cela signifie que le schéma doit correspondre exactement car il a été spécifié sans événement imprévu.

Pour les conditions de règle, vous créez les instructions suivantes :

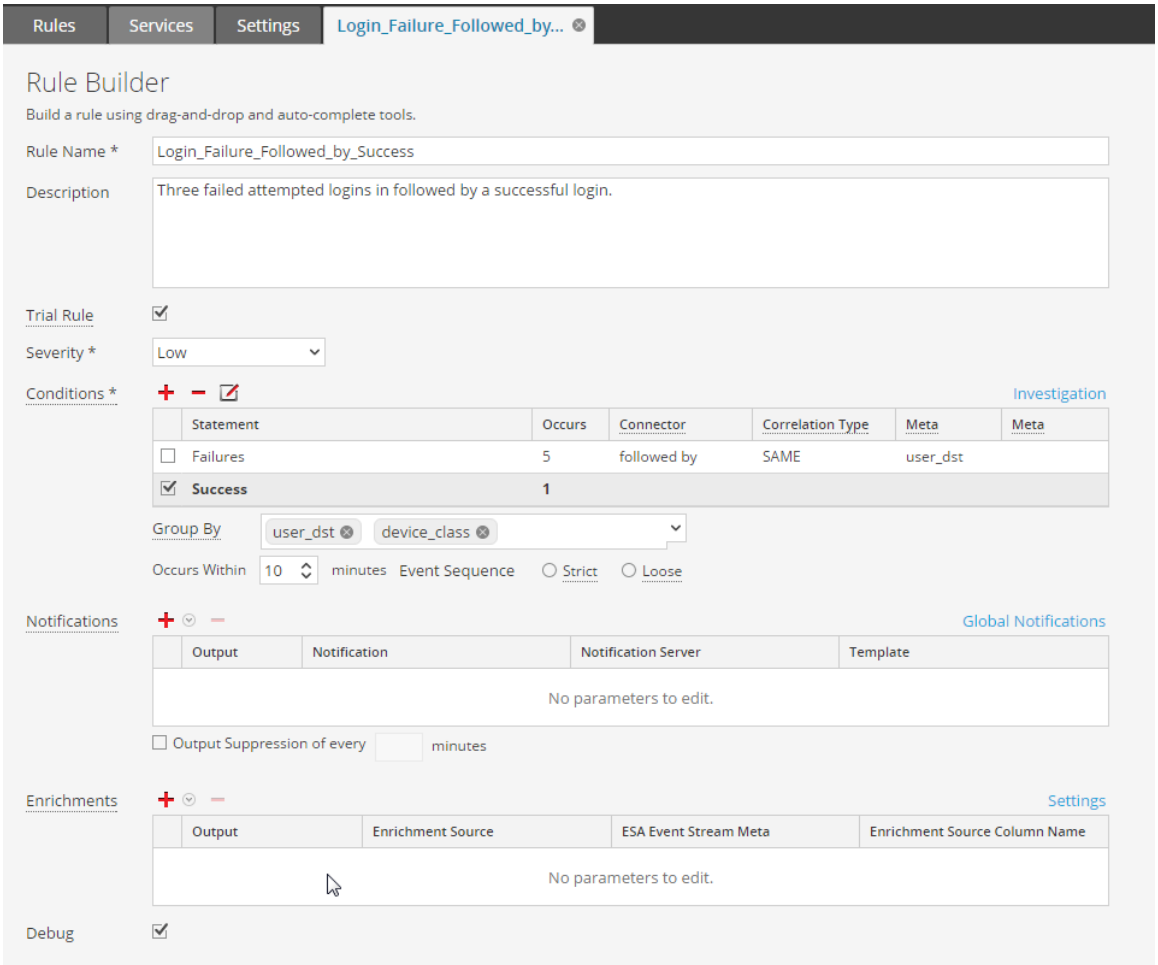
- L'instruction « Failures » recherche les tentatives de connexion ayant échoué :



- L'instruction « Success » recherche une connexion réussie :



- Lorsque ces éléments sont associés, vous disposez de la règle de corrélation suivante :



Étape 2 : Créer l'enrichissement

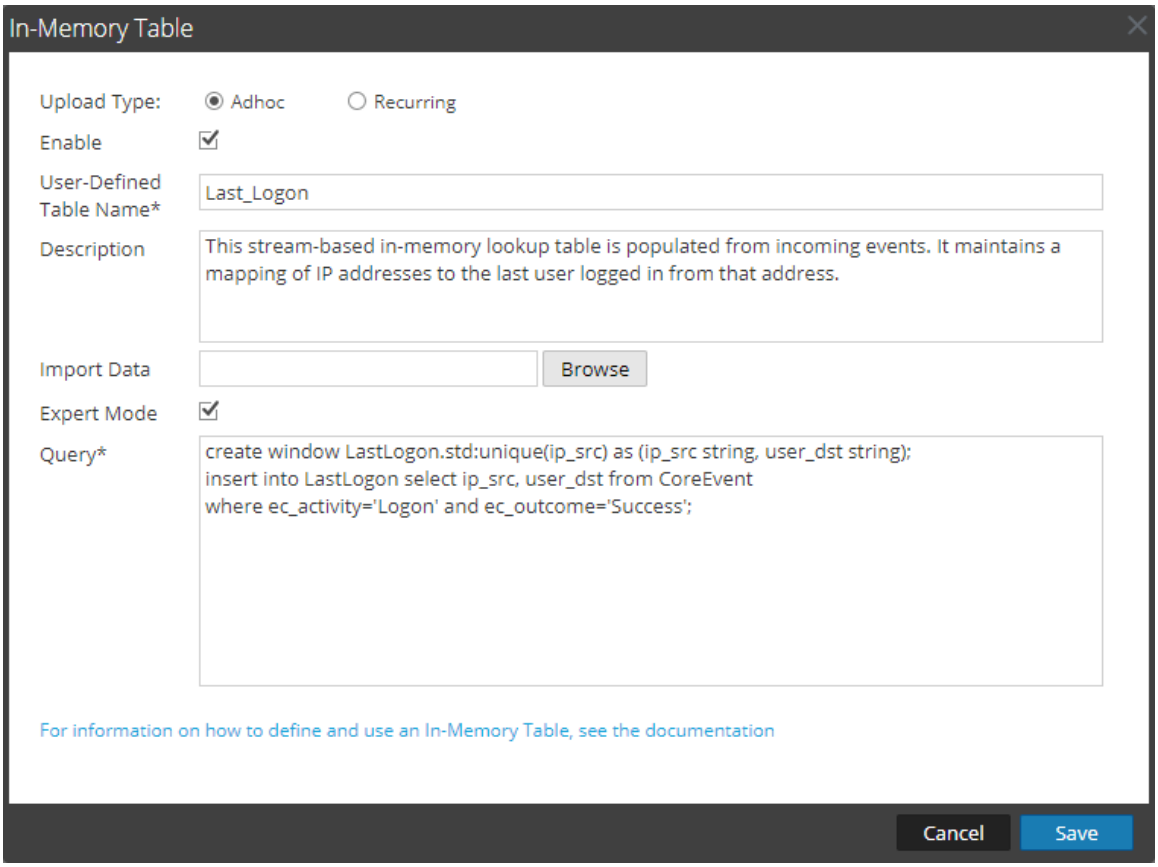
Maintenant que vous avez créé votre règle, vous devez créer l'enrichissement à ajouter à la sortie de notification. Suivez les étapes ci-dessus pour créer l'enrichissement, nommez-le *Last_Logon* et ajoutez la requête suivante :

```
create window LastLogon.std:unique(ip_src) as (ip_src string, user_dst string);

insert into LastLogon select ip_src, user_dst from CoreEvent

where ec_activity='Logon' and ec_outcome='Success';
```

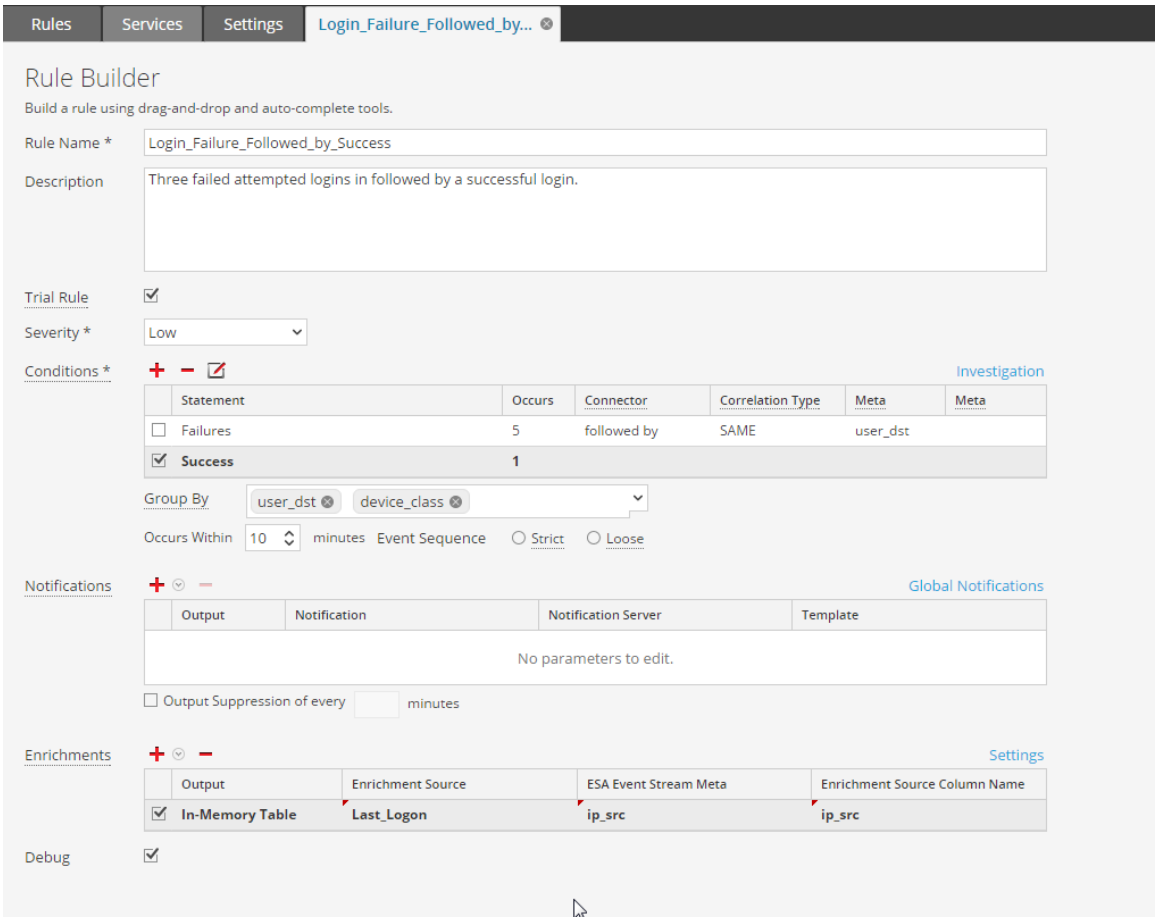
L'enrichissement doit se présenter comme suit :



Étape 3 : Ajouter l'enrichissement à la règle

Maintenant que vous avez créé votre règle de base et votre enrichissement, vous devez ajouter l'enrichissement à la règle et joindre (ou connecter) l'enrichissement à la méta dans la règle.

Ouvrez la règle Login_Failure_Followed_by_Success pour la modifier.



Champ	Saisie	Description
Sortie	Table en mémoire	L'option Table en mémoire crée une fenêtre nommée, qui peut être renseignée avec les données de requête EPL.
Source d'enrichissement	Last_Logon (enrichissement que vous avez créé ci-dessus).	Il s'agit de la table de recherche en mémoire basée sur les flux de données, renseignée à partir d'événements entrants afin de maintenir un mappage d'adresses IP vers le dernier utilisateur connecté depuis cette adresse.
Méta de flux d'événements ESA	ip_src	Il s'agit d'une méta de flux d'événements que vous pouvez joindre aux données d'enrichissement que vous renseignez. ip_src est en fait la condition join.

Champ	Saisie	Description
Nom de la colonne de la source d'enrichissement	ip_src	Il s'agit de la méta de l'enrichissement que vous pouvez joindre aux données de flux d'événements. Elle doit être identique à la condition join dans le champ Méta de flux d'événements.

Une fois que vous avez ajouté l'enrichissement, vous pouvez enregistrer la règle.

Lorsque la règle est déclenchée, le service ESA exécute la requête dans l'enrichissement et renseigne les données dans la fenêtre nommée. Si les données présentes dans la fenêtre nommée correspondent à la condition join, celles-ci sont ajoutées à la sortie que vous pouvez voir dans E-mail, SNMP, Syslog ou Script, selon la configuration de vos notifications.

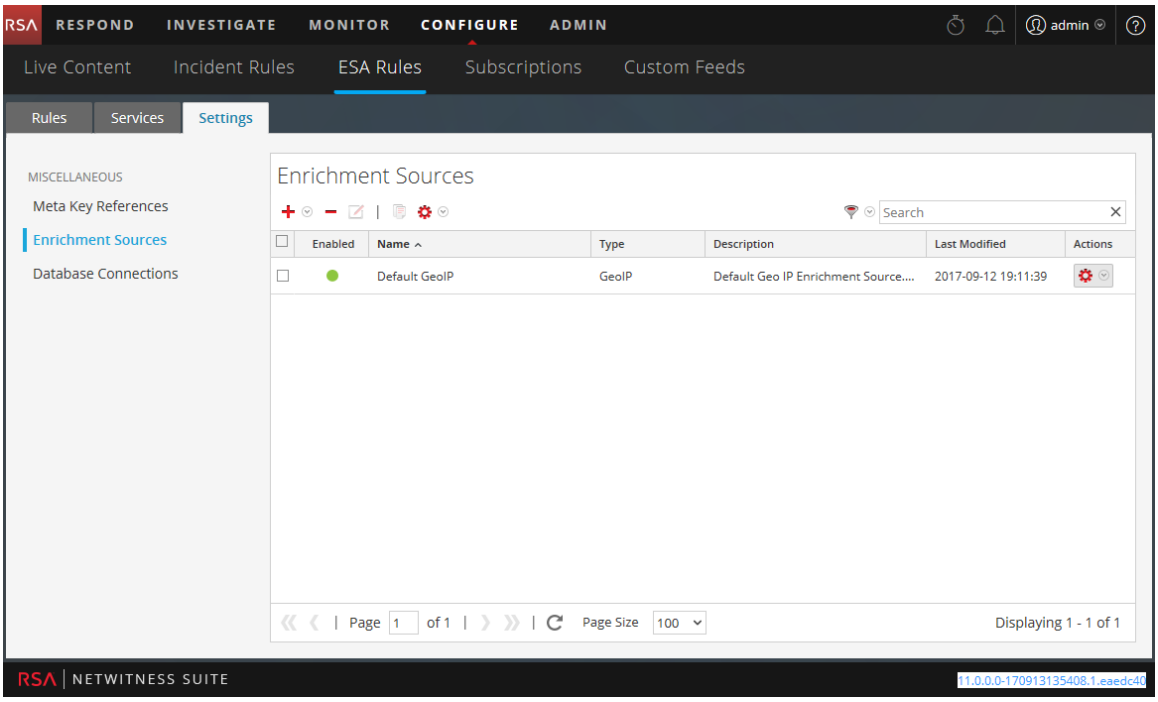
Configurer Warehouse Analytics en tant que source d'enrichissement

Cette rubrique fournit des instructions sur la manière de configurer RSA Warehouse Analytics en tant que source d'enrichissement pour ESA. Les analystes de données peuvent tirer le meilleur parti des données Warehouse Analytics pour analyser les données de session et de fichiers log.

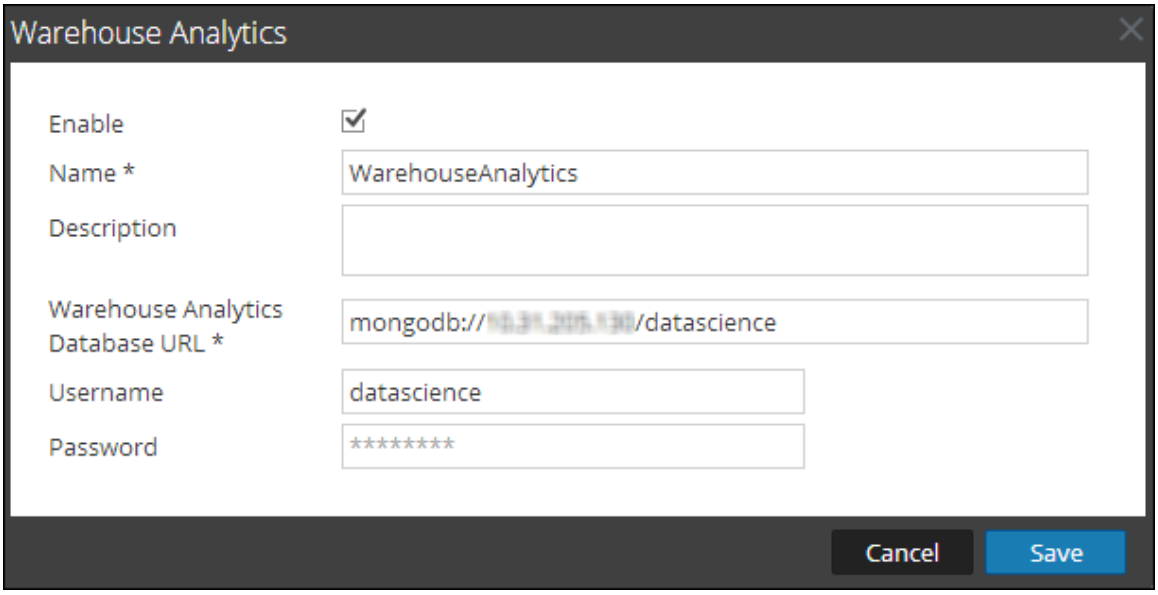
Pour configurer Warehouse Analytics comme source d'enrichissement :

1. Accédez à l'onglet **CONFIGURER > Règles ESA > Paramètres**.
2. Dans le panneau d'options, sélectionnez **Sources d'enrichissement**.

   Le panneau Sources d'enrichissement s'affiche.



3. Dans le menu déroulant  , sélectionnez **Warehouse Analytics**.



4. Sélectionnez **Activer** pour enrichir les alertes avec des données supplémentaires. Cette option est sélectionnée par défaut. Si les alertes sont désactivées, elles ne sont pas enrichies avec des données supplémentaires.
5. Dans le champ **Nom**, saisissez un nom pour identifier la configuration Warehouse Analytics ou lui attribuer un libellé.

6. Dans le champ **Description**, saisissez une brève description de la configuration Warehouse Analytics.
7. Dans le champ **URL de la base de données Warehouse Analytics**, saisissez l'URL MongoDb pour accéder à la base de données Warehouse Analytics.
8. Dans le champ **Nom d'utilisateur**, saisissez le nom d'utilisateur permettant d'accéder à la base de données MongoDB.
9. Dans le champ **Mot de passe**, saisissez le mot de passe permettant d'accéder à la base de données MongoDB.
10. Cliquez sur **Enregistrer**.

Pour plus d'informations, reportez-vous à la rubrique Onglet Paramètres.

Ajouter un enrichissement à une règle

Cette rubrique vous indique comment ajouter une source d'enrichissement précédemment configurée à une règle. Lorsque ESA crée une alerte, elle comprend des informations de la source.

L'ajout d'un enrichissement à une règle vous permet de d'effectuer des recherches dans différentes sources et d'inclure les résultats dans les alertes sortantes pour vous fournir une alerte plus détaillée. Cette procédure nécessite des autorisations de rôle pour Administrateur, DPO et Responsable du SOC.

Procédure

Pour ajouter un enrichissement à une règle :

1. Accédez à **CONFIGURER > Règles ESA**.
2. Dans la vue **Bibliothèque de règles**, exécutez l'une des opérations suivantes :
   - Double-cliquez sur une règle.
   - Sélectionnez une règle et cliquez sur  dans la barre d'outils **Bibliothèque de règles**.

   Le panneau Générateur de règles s'affiche dans un nouvel onglet NetWitness Suite.
3. Dans la section **Enrichissements**, cliquez sur  et sélectionnez l'un des types d'enrichissement suivants :
   - Table en mémoire
   - Référence BD externe

- Warehouse Analytics
- GeoIP

> **Remarque :** Si vous utilisez une source GeoIP, ipv4 est renseigné automatiquement et n'est pas modifiable.

Les types d'enrichissement sélectionnés s'affichent dans le tableau.

4. Pour le type d'enrichissement ajouté, procédez comme suit :
   - Dans la colonne **Sortie**, sélectionnez le type que vous avez configuré.
   - Dans la liste déroulante **Source d'enrichissement**, sélectionnez la source d'enrichissement définie.
   - Dans le champ **Méta de flux d'événements ESA**, saisissez la clé méta de flux d'événements dont la valeur sera utilisée comme opérande de la condition de jonction.

   - Dans le champ **Nom de la colonne de la source d'enrichissement**, saisissez le nom de la colonne de la source d'enrichissement dont la valeur sera utilisée comme autre opérande de la condition de jonction.
5. Sélectionnez **Déboguer**. Une annotation @Audit('stream') est ajoutée à la règle. Elle est utile lors du débogage des règles esper.
6. Cliquez sur **Afficher la syntaxe** pour tester si la règle ESA définie est valide.
7. Cliquez sur **Enregistrer**.

Pour plus de détails sur les paramètres et leurs descriptions, reportez-vous à la rubrique Onglet Générateur de règles.

Déployer des règles à exécuter sur ESA

Cette rubrique explique comment sélectionner un ESA et les règles à exécuter sur lui. Les autorisations de rôle Administrateur, Responsable du SOC ou DPO sont requises pour toutes les tâches de cette section.

Pour créer un déploiement, vous devez effectuer les étapes décrites dans Étapes de déploiement

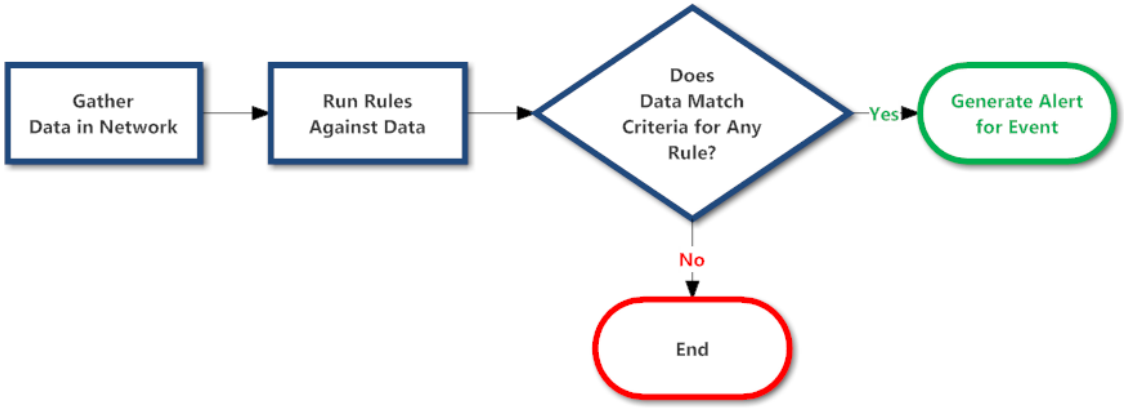
Fonctionnement du déploiement

Un déploiement se compose d'un service ESA e d'un groupe de règles ESA. Lorsque vous déployez des règles, le service ESA les exécute afin de détecter une activité suspecte ou indésirable sur votre réseau. Chaque règle ESA détecte un événement différent, tel que la création d'un compte utilisateur et sa suppression dans l'heure.

Le service ESA effectue les fonctions suivantes :

1. Rassemblement des **données** de votre réseau
2. Exécution des **règles** ESA par rapport aux données
3. Application des **critères** de règle aux données
4. Génération d'une **alerte** pour l'événement capturé

Le graphique suivant présente ce workflow :



En outre, vous avez la possibilité d'effectuer d'autres étapes de déploiement, telles que la suppression d'un service ESA dans votre déploiement, la modification ou la suppression d'une règle de votre déploiement, la modification ou la suppression d'un déploiement ou la présentation des mises à jour dans le cadre d'un déploiement. Pour obtenir une description de ces procédures, reportez-vous à la section Procédures de déploiement supplémentaires

Étapes de déploiement

Cette rubrique explique comment ajouter un déploiement, qui comprend un service ESA et un ensemble de règles ESA. Vous pouvez ajouter un déploiement pour organiser et gérer les services et règles ESA. Le déploiement est une sorte de conteneur dans lequel figurent les deux composants :

1. Un service ESA
2. Un ensemble de règles ESA

Par exemple, si vous ajoutez un déploiement d'activité Spam, il peut inclure ESA Londres et un ensemble de règles ESA pour détecter une activité d'e-mail suspecte.

Pour ajouter un déploiement, vous devez exécuter les procédures suivantes :

- Étape 1. Ajouter un déploiement
- Étape 2. Ajouter un service ESA
- Étape 3. Ajouter et déployer des règles

Étape 1. Ajouter un déploiement

Conditions préalables

Les conditions suivantes doivent être remplies pour ajouter un déploiement :

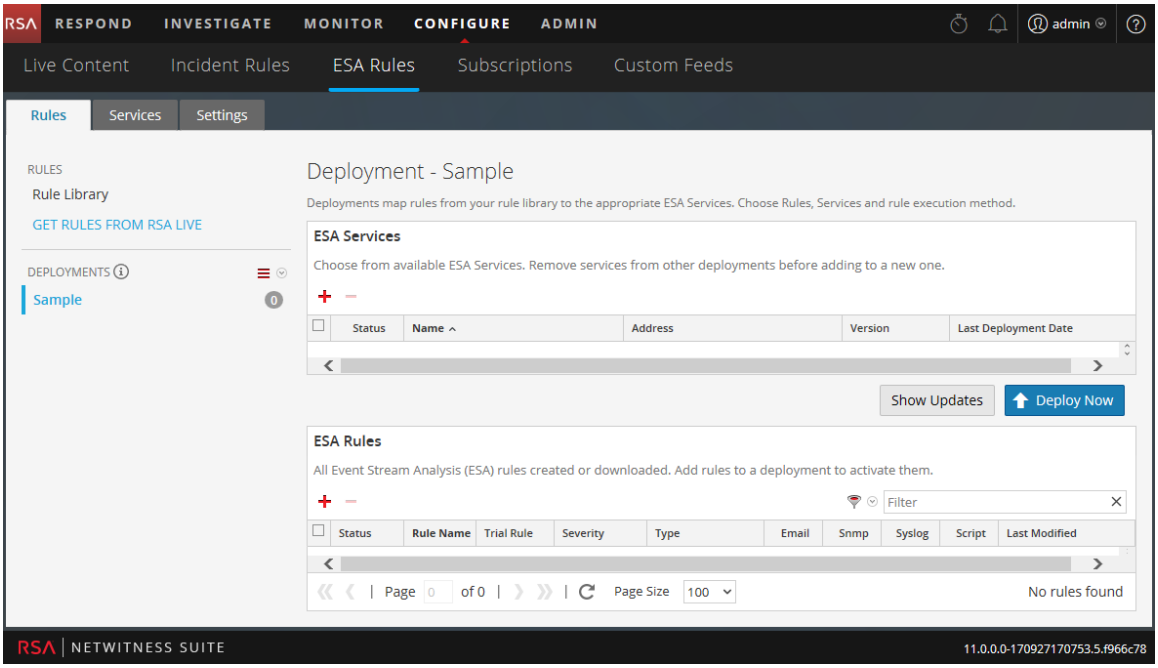
- Le service ESA doit être configuré sur l'hôte. Reportez-vous à la section « Configurer ESA », dans le *Guide de configuration d'Event Stream Analysis (ESA)*.
- Les règles doivent figurer dans la Bibliothèque de règles. Reportez-vous à la rubrique Ajouter des règles à la Bibliothèque de règles.

Procédure

Pour ajouter un déploiement :

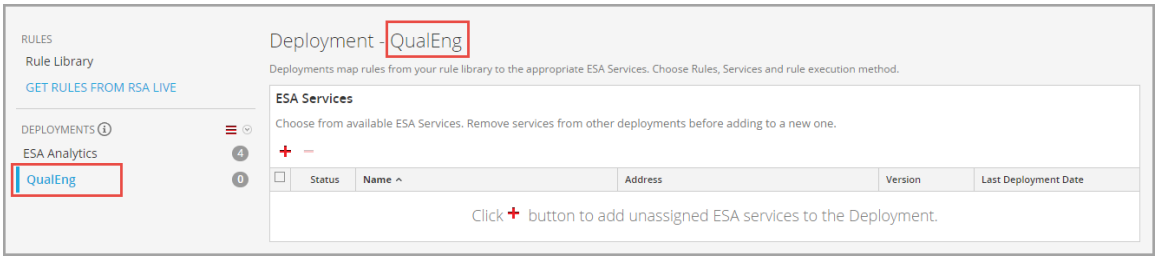
1. Accédez à **CONFIGURER > Règles ESA**.
   L'onglet Règles s’affiche.

2. Dans le panneau d'options, en regard de Déploiements, sélectionnez  > Ajouter . La vue Déploiement s'affiche à droite.



3. Dans le panneau Options, saisissez un **nom** pour le déploiement. Aucune convention de dénomination n'est applicable.
   Par exemple, ce nom peut indiquer un objectif ou identifier un propriétaire.

4. Appuyez sur **Entrée**.
   Le déploiement est ajouté.



Étape 2. Ajouter un service ESA

Le service ESA d'un déploiement collecte les données sur votre réseau et exécute les règles ESA sur les données. Le but est de capturer les événements correspondant aux critères de la règle, puis de générer une alerte pour l'événement capturé.

Vous pouvez ajouter le même service ESA à plusieurs déploiements. Par exemple, le service ESA Londres peut exister simultanément dans les déploiements suivants :

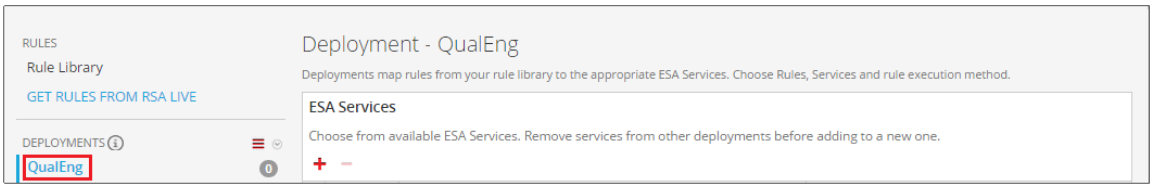
- Déploiement EUR, qui contient un ensemble de règles ESA
- Déploiement CORP, qui contient un autre ensemble de règles ESA

Lorsque vous supprimez un service ESA d'un déploiement, les règles sont également supprimées du service ESA. Par exemple, le déploiement EUR peut comprendre le service ESA Londres et un ensemble de 25 règles. Si vous supprimez le service ESA Londres du déploiement EUR, les 25 règles sont également supprimées du service ESA Londres. Par conséquent, si un service ESA ne fait pas partie d'un déploiement, il ne contient pas de règles.

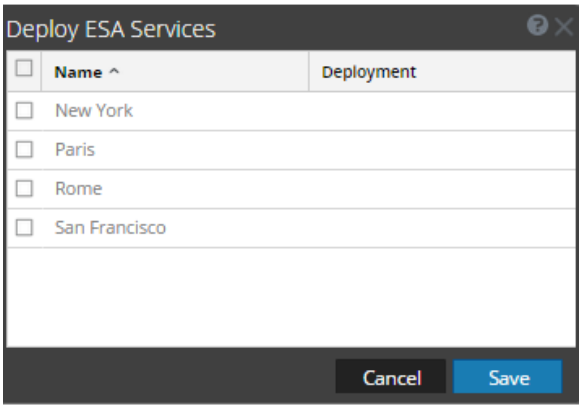
Procédure

Pour ajouter un service ESA :

1. Accédez à **CONFIGURER > Règles ESA**.
   L'onglet Règles s'affiche.
2. Dans le panneau des options, sélectionnez un **déploiement** :



3. Dans la vue **Déploiement**, cliquez sur + **dans** Services ESA
   .La boîte de dialogue Déployer les services ESA répertorie chaque service ESA configuré.



4. Sélectionnez un service ESA et cliquez sur **Enregistrer**.
   La vue Deploiement s'affiche. Le service ESA est répertorié dans la section **Services ESA** avec l'état Ajouté(e).

Étape 3. Ajouter et déployer des règles

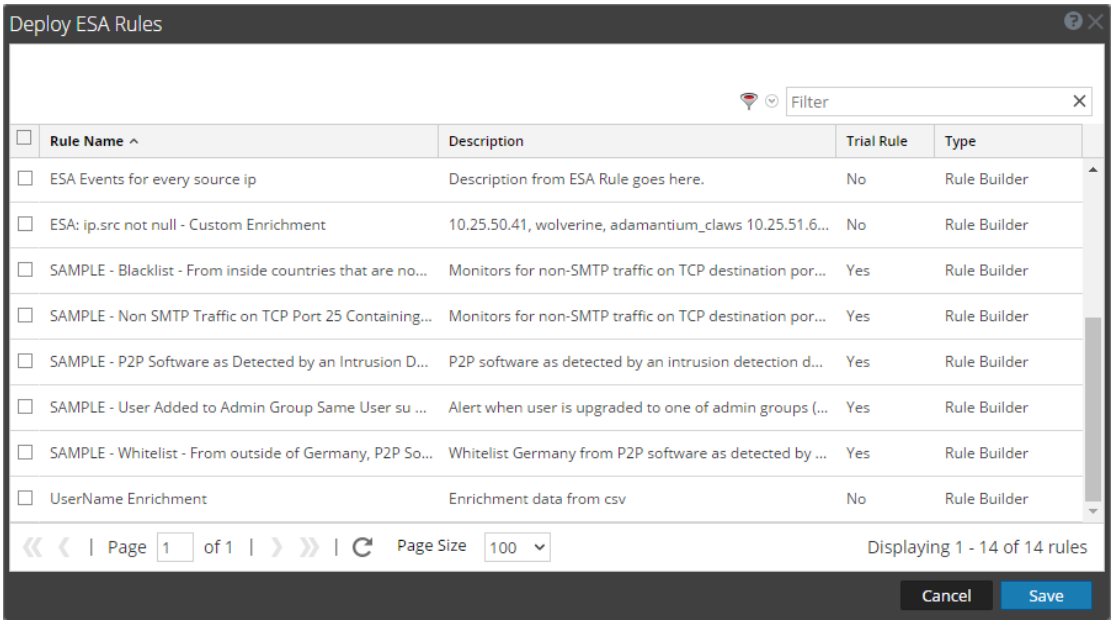
Cette rubrique explique comment ajouter des règles ESA à un déploiement, puis déployer les règles sur ESA. Chaque règle ESA a des critères uniques. Les règles ESA d'un déploiement déterminent les événements capturés par ESA, qui déterminent à leur tour les alertes que vous recevez.

Par exemple, le déploiement A comprend le service ESA Paris et, entre autres, une règle de détection d'un transfert de fichiers à l'aide d'un port non standard. Lorsque le service ESA Paris détecte un transfert de fichiers correspondant aux critères de la règle, il capture l'événement et génère une alerte. Si vous supprimez cette règle du déploiement A, ESA ne pourra plus générer une alerte pour cette occurrence.

Procédure

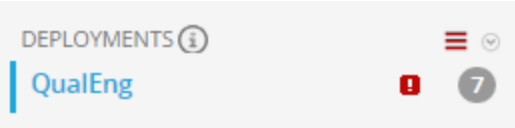
Pour ajouter et déployer des règles :

1. Accédez à **Configurer > Règles ESA**.
   L'onglet Règles s'affiche.
2. Dans le panneau des options, sélectionnez un déploiement.
3. Dans la vue **Déploiement**, cliquez sur + dans **Règles ESA**.
   La boîte de dialogue Déployer les règles ESA s'affiche et présente chaque règle contenue dans votre Bibliothèque de règles :



4. Sélectionnez des règles et cliquez sur **Enregistrer**.
   La vue Déploiement s'affiche.
5. Les règles sont répertoriées dans la section Règles ESA.

- Dans la colonne État, **Ajouté(e)** apparaît en regard de chaque nouvelle règle.
- Dans la section Déploiements, indique que des mises à jour sont disponibles pour le déploiement.
- Le nombre total de règles contenues dans le déploiement s'affiche à droite.



6. Cliquez sur **Déployer maintenant**.
   Le service ESA exécute l'ensemble de règles.

Procédures de déploiement supplémentaires

En plus du déploiement d'un service et des règles ESA, vous avez la possibilité d'effectuer d'autres étapes de déploiement, telles que la suppression d'un service ESA dans votre déploiement, la modification ou la suppression d'une règle de votre déploiement, la modification ou la suppression d'un déploiement ou la présentation des mises à jour dans le cadre d'un déploiement.

Pour effectuer ces procédures, accédez à :

- Supprimer un service ESA dans un déploiement
- Modifier ou supprimer une règle dans un déploiement
- Modifier ou supprimer un déploiement
- Affiche les mises à jour d'un déploiement

Supprimer un service ESA dans un déploiement

Cette rubrique fournit des instructions pour supprimer un service ESA dans un déploiement. Dans un déploiement avec un service, vous pouvez modifier les règles appliquées au service et supprimer le service du déploiement.

Chacune des procédures suivantes commence sous l'onglet Règles.

Procédure

Pour supprimer un service ESA :

1. Accédez à l'onglet **CONFIGURER > Règles ESA > Règles**.
   L'onglet Règles s'affiche.

2. Dans le panneau d'options, sous **Déploiements**, sélectionnez un déploiement.
3. Dans le panneau **Services ESA**, sélectionnez un service et cliquez sur dans la barre d'outils.
   Une boîte de dialogue de confirmation s'affiche.
4. Cliquez sur **Yes**.
   Le service est supprimé.

Modifier ou supprimer une règle dans un déploiement

Dans un déploiement incluant des règles, vous pouvez modifier et supprimer des règles pour personnaliser le déploiement. Chacune des procédures suivantes commence sous l'onglet Règles.

Procédures

Modifier une règle

1. Accédez à l'onglet **CONFIGURER > Règles ESA > Règles**.
   L'onglet Règles s'affiche.
2. Dans le panneau d'options, sous Déploiements, sélectionnez un déploiement.
3. Dans le panneau **Règles ESA**, double-cliquez sur une règle pour l'ouvrir dans un nouvel onglet.
4. Modifiez la règle et cliquez sur **Appliquer**.
   La règle est enregistrée.

Supprimer une règle

1. Accédez à l'onglet **CONFIGURER > Règles ESA > Règles**.
   L'onglet Règles s'affiche.
2. Dans le panneau d'options, sous **Déploiements**, sélectionnez un déploiement.
3. Dans le panneau **Règles ESA**, sélectionnez une règle et cliquez sur dans la barre d'outils.
   Une boîte de dialogue de confirmation s'affiche.
4. Cliquez sur **Yes**.
   La règle est supprimée.

Modifier ou supprimer un déploiement

Cette rubrique explique comment NetWitness Suite transmet une règle de corrélation à chaque service ESA d'un groupe de corrélation. Dans un groupe de corrélation, chaque service ESA doit exécuter le même ensemble de règles. Lorsque vous ajoutez une règle à un groupe de corrélation, NetWitness Suite transmet la règle à chaque service ESA du groupe.

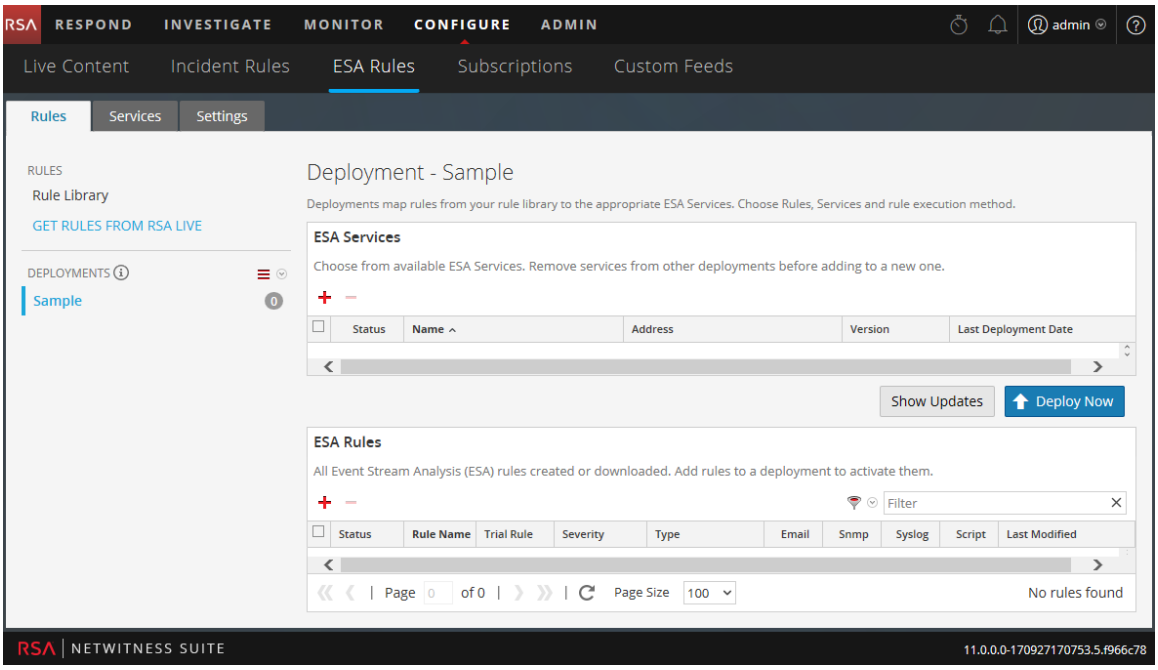
Pour accéder aux déploiements :

1. Accédez à **CONFIGURER > Règles ESA**.

   La vue Configurer s'affiche avec l'onglet Règles ouvert.

2. Dans le panneau d'options, sous **Déploiements**, sélectionnez un déploiement.

   La vue Deploiement s'affiche.



Modifier un déploiement

1. Dans le panneau d'options, sous **Déploiements**, sélectionnez un déploiement.

   La vue Deploiement s'affiche.

2. Sélectionnez  > **Modifier**.

   Le nom du déploiement peut alors être modifié.

Supprimer un déploiement

1. Dans le panneau d'options, sous **Déploiements**, sélectionnez un déploiement.

   La vue Deploiement s'affiche.

2. Sélectionnez > **Supprimer**.

   Une boîte de dialogue de confirmation s'affiche.

3. Cliquez sur **Yes**.

   Le déploiement est supprimé.

Affiche les mises à jour d'un déploiement

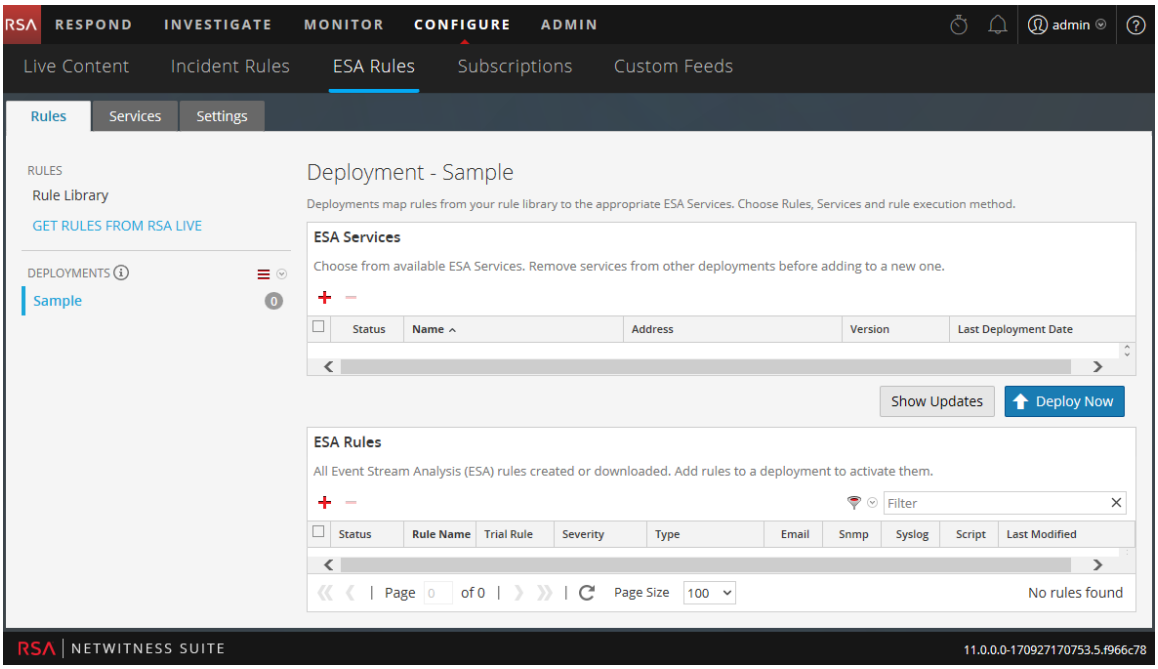
Cette rubrique explique comment afficher des mises à jour, telles que l'ajout ou la suppression de règles, dans un déploiement. Lorsque vous apportez une modification à un déploiement, l'icône de mise à jour ( ) s'affiche en regard du nom du déploiement.

Procédure

Pour afficher les mises à jour d'un déploiement :

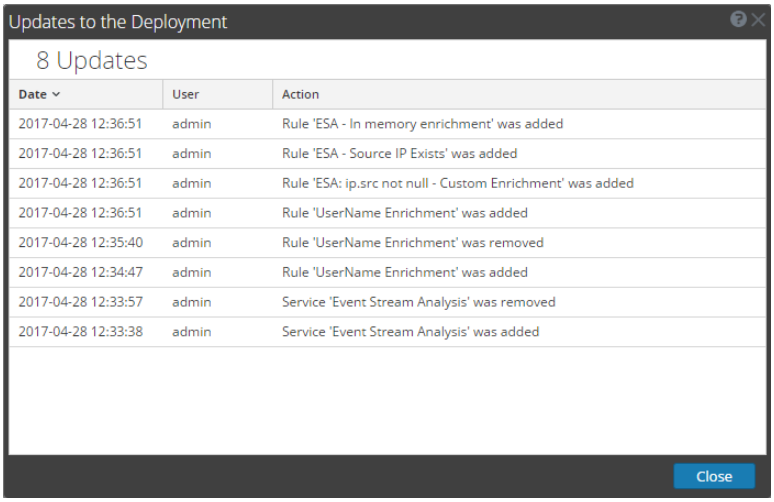
1. Accédez à **CONFIGURER > Règles ESA.**
   L'onglet Règles s'affiche.

2. Dans le panneau des options, sous **Déploiements**, cliquez sur **Afficher les mises à jour** à l'extrême droite.



   La boîte de dialogue Mises à jour appliquées au déploiement s'ouvre et affiche les

modifications apportées au déploiement.



3. Cliquez sur **Fermer**.

Afficher les statistiques et alertes ESA

Lorsque le service ESA génère des alertes, vous pouvez afficher des détails sur la façon dont les règles sont appliquées, telles que les statistiques relatives au moteur, à la règle et à l'alerte. Vous pouvez également afficher des informations sur les règles activées ou désactivées. Pour obtenir des instructions sur l'affichage des statistiques ESA, reportez-vous à la section Afficher les statistiques pour un service ESA

Lorsque votre serveur ESA génère des alertes, vous pouvez afficher les résultats dans la page Récapitulatif des alertes. Cela vous permet de voir les tendances et de comprendre le volume et la fréquence des alertes. Pour obtenir des instructions sur l'affichage des alertes, reportez-vous à la section Afficher un récapitulatif des alertes

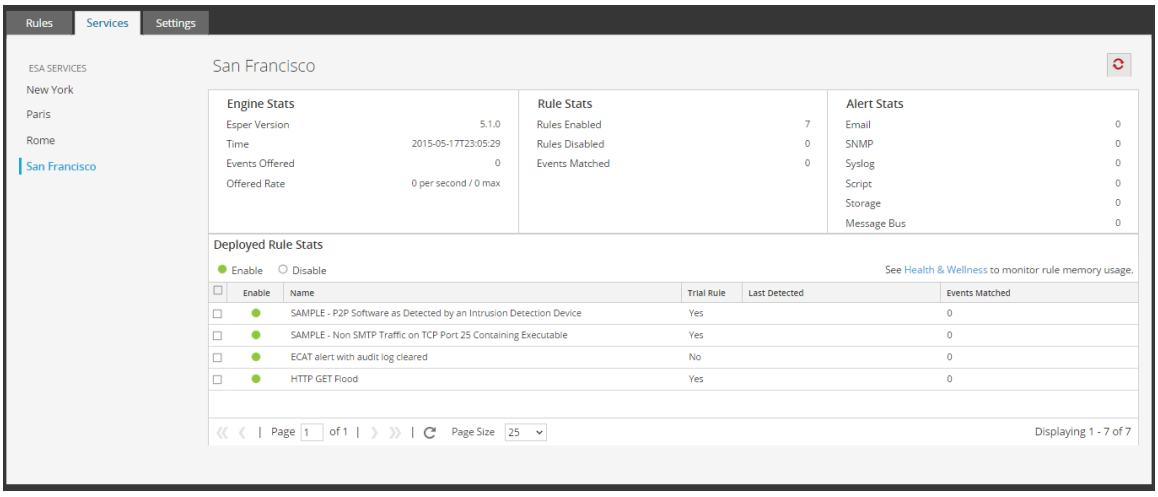
Afficher les statistiques pour un service ESA

Cette rubrique décrit comment afficher les statistiques de déploiement pour un service ESA. Cette procédure est utile lorsque vous essayez de déterminer l'efficacité d'une règle ou de résoudre les problèmes liés à un déploiement.

Procédures

Afficher les statistiques ESA

1. Accédez à l'onglet **CONFIGURER > Règles ESA > Services**.
2. Dans la liste **Services ESA** à gauche, sélectionnez un service.
   Les statistiques de déploiement pour le service sélectionné s'affichent.



3. Passez en revue les sections ci-dessous des statistiques ESA.
   Pour une description complète de chaque statistique de chaque section, reportez-vous à la

rubrique Onglet Services.

- **Stat. engine**
- **Stat. règles**
- **Statistiques liées aux alertes**

4. Dans la section Statistiques de règles déployées, consultez les détails des règles déployées sur le service ESA.
   Pour une description complète de chaque colonne de chaque section, reportez-vous à la rubrique Onglet Services.
   - Si la règle est activée ou désactivée
   - Le nom de la règle
   - Si la règle s'exécute en mode Règle d'évaluation
   - Dernière détection
   - Correspondances d'événements
5. Pour obtenir un snapshot de la mémoire de la règle, cliquez sur **Intégrité**.

Activer ou désactiver des règles

1. Dans le panneau **Statistiques de règles déployées**, sélectionnez une règle dans la grille.
2. Cliquez sur Enable pour activer la règle ou sur Disable pour la désactiver.
   L'onglet Services est actualisé pour afficher les modifications qui prennent effet immédiatement.

Actualiser les statistiques

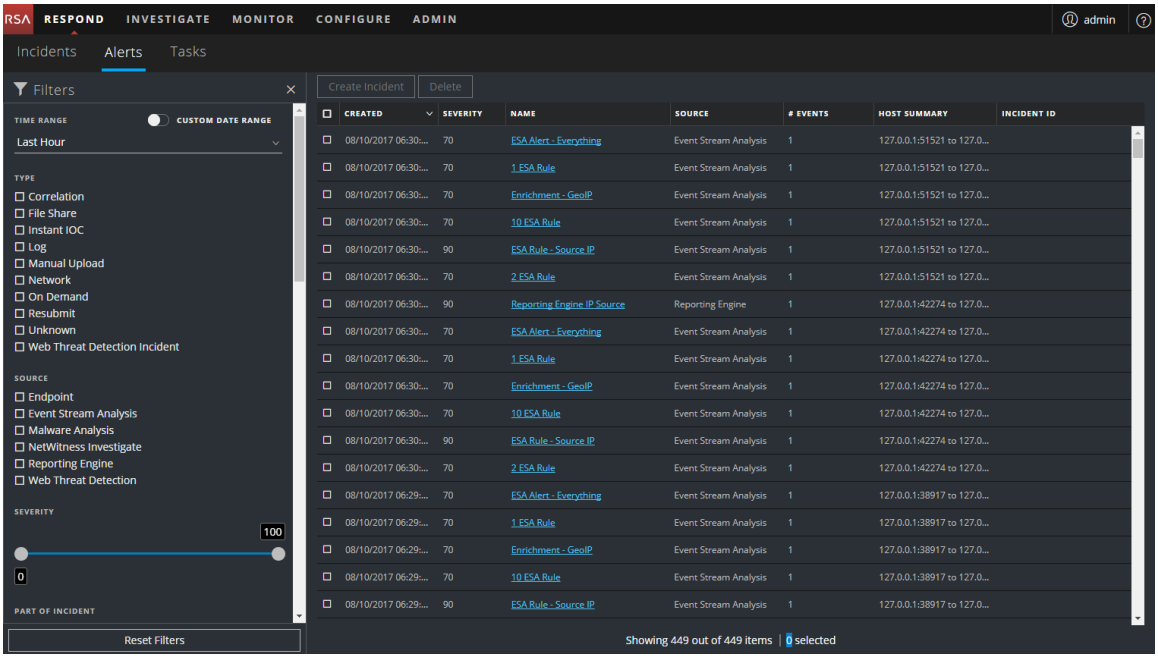
L'onglet Services ne met pas automatiquement à jour les statistiques sauf si vous activez ou désactivez une règle. Pour vous assurer d'afficher les statistiques actuelles :

1. Cliquez sur dans l'angle supérieur droit pour actualiser les informations.
2. Affichez les informations mises à jour.

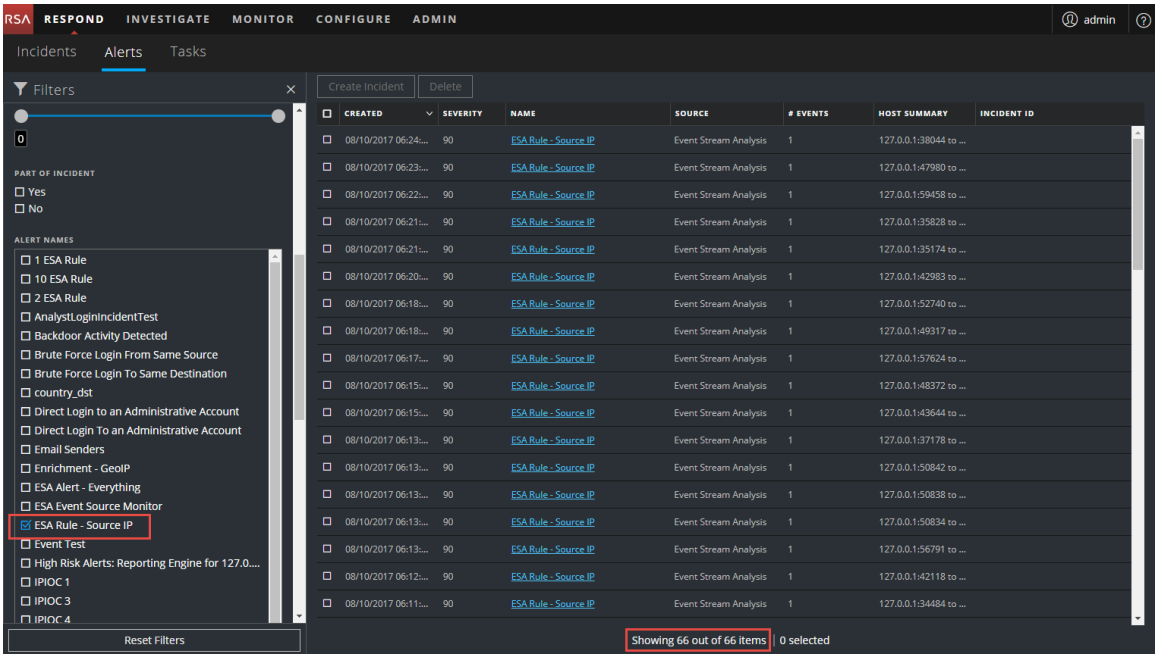
Afficher un récapitulatif des alertes

Dans la vue RÉPONDRE, vous pouvez parcourir différentes alertes provenant de plusieurs sources. Vous pouvez filtrer la liste des alertes pour afficher uniquement les alertes d'intérêt, comme par Nom de l'alerte, source d'alerte et selon une période spécifique.

1. Accédez à **RÉPONDRE > Alertes**.
   La vue Liste des alertes de réponse affiche une liste de toutes les alertes NetWitness Suite.



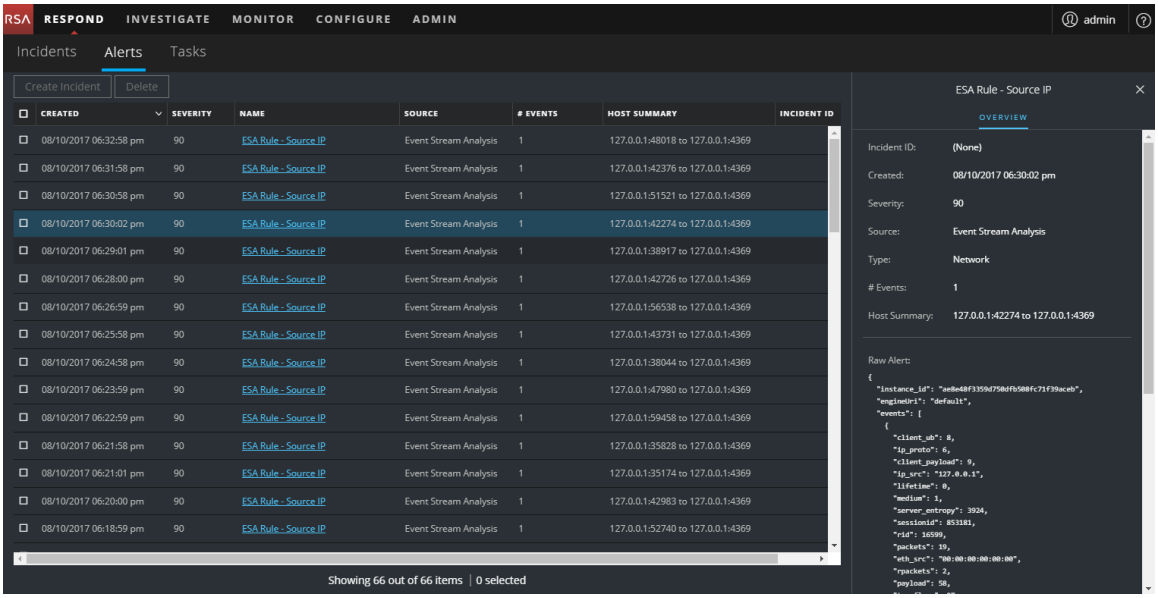
2. Dans le panneau **Filtres** sur la gauche, vous pouvez filtrer la liste des alertes pour afficher des alertes spécifiques pour une période spécifique. Par exemple, dans la section NOMS D'ALERTE, vous pouvez sélectionner une alerte pour une règle ESA, comme Règle ESA - IP source, et laisser l'INTERVALLE DE TEMPS défini sur Dernière heure.
   La liste des alertes à droite affiche la liste des alertes qui correspondent à votre sélection de filtre, ainsi qu'un nombre d'alertes au bas de la liste des alertes.



   La liste des alertes affiche des informations sur chacune des alertes.

- **Créé** : Affiche la date et l'heure auxquelles l'alerte a été créée dans le système source.
- **Gravité** : Affiche le niveau de gravité de l'alerte. Les valeurs s'étendent de 1 à 100.
- **Nom** : Affiche une description de base de l'alerte.
- **Source:** Affiche la source originale de l'alerte.
- **Décompte d'événements** : Indique le nombre d'événements contenus dans une alerte.
- **Récapitulatif de l'hôte** : Affiche les détails relatifs à l'hôte tels que le nom de l'hôte d'où l'alerte a été déclenchée.
- **ID d'incident** : Affiche l'ID d'incident de l'alerte. S'il n'existe aucun ID d'incident, l'alerte n'appartient pas à un incident.

3. Vous pouvez cliquer sur une alerte dans la liste pour ouvrir un panneau **Présentation** situé à droite, dans lequel vous pouvez afficher les métadonnées de l'alerte brute.



Pour plus d'informations sur le filtrage des alertes et l'affichage des détails de l'alerte, consultez le *NetWitness RespondGuide d'utilisation*.

Références aux alertes ESA

Dans le module Alertes, vous configurez et déployez des règles ESA pour être averti de menaces potentielles sur le réseau.

Ces rubriques explique l'interface utilisateur du module Alertes.

Onglet Nouvelle règle EPL avancée

L'onglet Règle EPL avancée vous permet de définir les critères de règle avec une requête EPL (Event Processing Language).

Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Expert du contenu	Définir une règle EPL avancée.	Ajouter une règle EPL avancée
Expert du contenu	Obtenir des exemples d'une règle EPL avancée.	Exemple de règles EPL avancées

Rubriques connexes

- Ajouter une règle Générateur de règles
- Sources d'enrichissement

Règle EPL avancée

Pour accéder à l'onglet Règle EPL avancée :

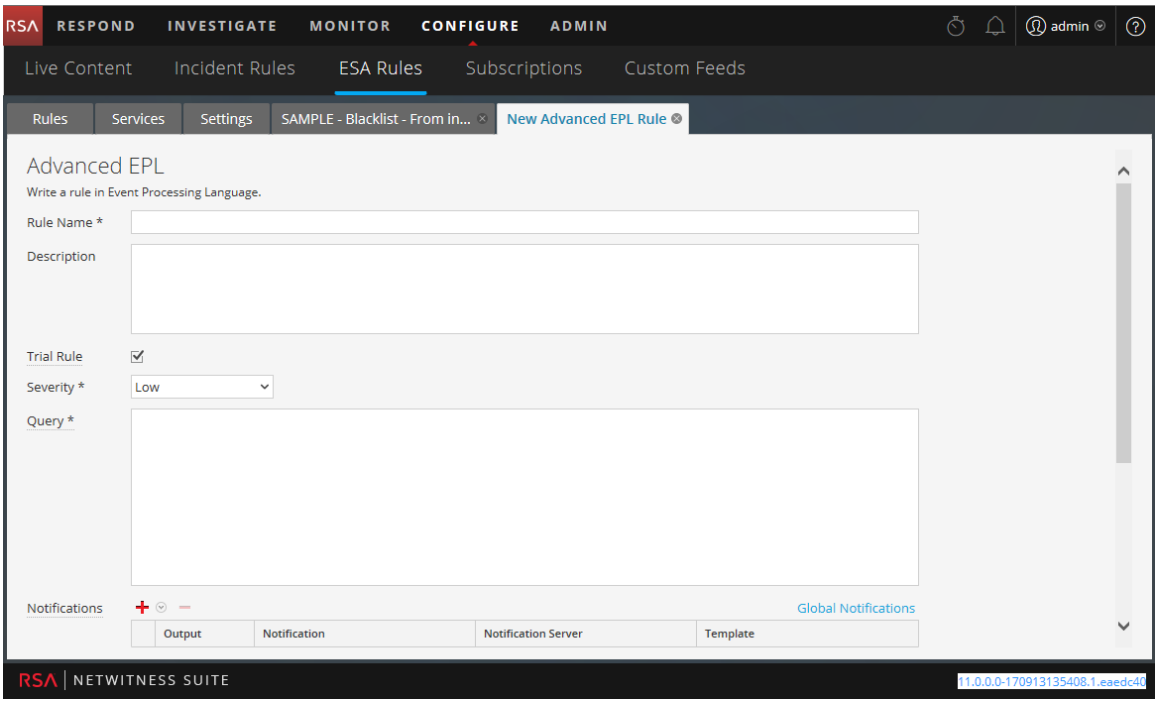
1. Accédez à **CONFIGURER > Règles ESA**.

   La vue Configurer s'affiche avec l'onglet Règles ouvert par défaut.

2. Dans la barre d'outils de la **Bibliothèque de règles**, sélectionnez  **> EPL avancé**.

   L'onglet Règle EPL avancée s'affiche.

La capture d'écran ci-dessous illustre l'onglet Règle EPL avancée.



Le tableau suivant affiche les paramètres de l'onglet Règle EPL avancée.

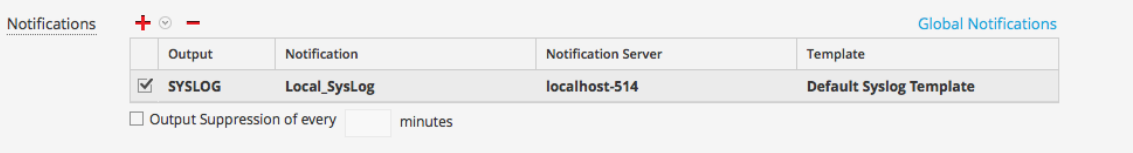
Paramètres	Description
Nom de la règle	Objectif de la règle ESA.
Description	Récapitulatif des éléments détectés par la règle ESA.
Règle d'évaluation	Mode de déploiement afin de déterminer si la règle s'exécute efficacement.
Gravité	Niveau de menace de l'alerte déclenchée par la règle.
Query	Requête EPL qui définit les critères de règle.

Notifications

Dans la section Notifications, vous pouvez choisir le mode de notification lorsqu'ESA génère une alerte pour la règle.

Pour plus d'informations sur les notifications d'alertes, reportez-vous à la rubrique Ajouter une méthode de notification à une règle.

La figure ci-dessous présente la section Notifications.



Paramètre	Description
+	Pour ajouter un type de notification d'alerte.
−	Pour supprimer le type de notification d'alerte sélectionné.
Résultat	Type de notification d'alerte. Les options possibles sont : • E-mail • SNMP • Syslog • Script
Notification	Nom de la sortie précédemment configurée, comme la liste de diffusion d'e-mails.
Serveur de notification	Nom du serveur qui envoie la sortie.
Modèle	Nom du modèle pour la notification d'alerte.
Limite des notifications aux	Option permettant de spécifier la fréquence d'alerte.
Minutes	Fréquence d'alerte en minutes.

Enrichissements

Dans la section Enrichissements, vous pouvez ajouter une source d'enrichissement de données à une règle.

Pour plus d'informations sur les enrichissements, reportez-vous à la rubrique Ajouter un enrichissement à une règle.
La figure ci-dessous présente la section Enrichissements.

Paramètre	Description
+	Pour ajouter un enrichissement.
−	Pour supprimer l'enrichissement sélectionné.
Résultat	Type de source d'enrichissement. Les options possibles sont : • Table en mémoire • Référence BD externe • Warehouse Analytics • GeoIP
Source d'enrichissement	Nom de la source d'enrichissement précédemment configurée, comme un nom de fichier .CSV pour une table en mémoire.
Méta de flux d'événements ESA	Clé méta ESA dont la valeur sera utilisée en tant qu'opérande de la condition join.
Nom de la colonne de la source d'enrichissement	Nom de la colonne de la source d'enrichissement dont la valeur sera utilisée en tant qu'autre opérande de la condition join.

Boîte de dialogue Créer une instruction

La boîte de dialogue Créer une instruction vous permet de créer une instruction de condition lors de la création d'une règle Générateur de règles.

Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Expert du contenu	Configurer une instruction de règle.	Ajouter une règle EPL avancée
Expert du contenu	Ajouter des conditions à la règle.	Étape 3. Ajouter des conditions à une instruction de règle

Rubriques connexes

- Ajouter une règle Générateur de règles

Boîte de dialogue Créer une instruction

Pour accéder à la boîte de dialogue Créer une instruction :

1. Accédez à **CONFIGURER > Règles ESA**.

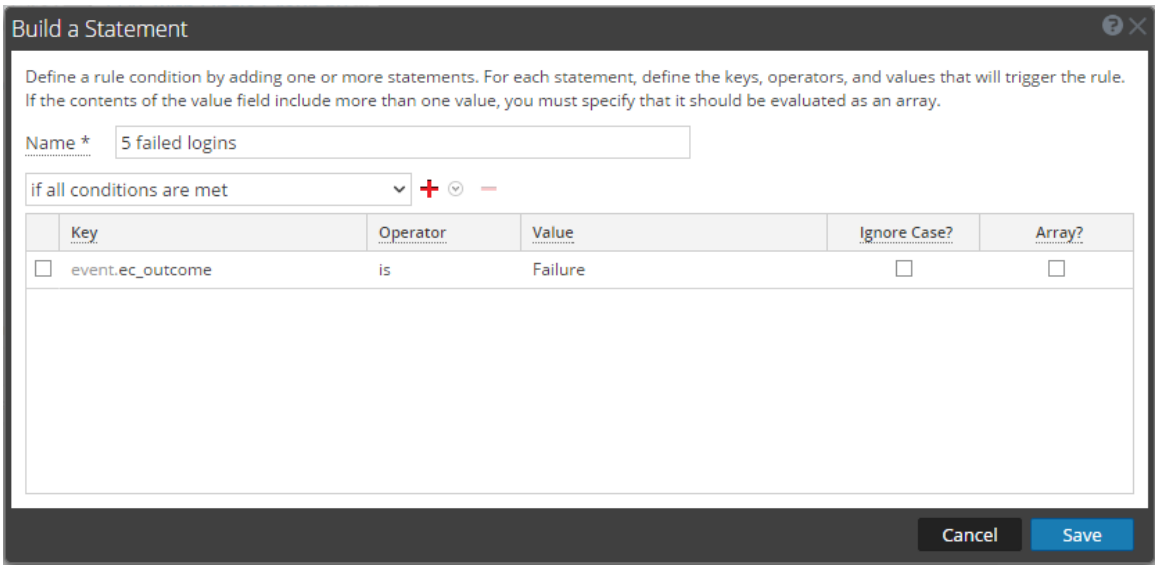
   La vue Configurer des règles ESA s'affiche avec l'onglet Règles ouvert.

2. Dans la barre d'outils **Bibliothèque de règles**, sélectionnez  **> Générateur de règles**.

   Un onglet Nouvelle règle s'affiche.

3. Dans la section **Conditions**, cliquez sur  .

   La boîte de dialogue Créer une instruction s'affiche.



Le tableau ci-dessous décrit les paramètres de la boîte de dialogue Créer une instruction.

Paramètre	Description
Nom	Objet de l'instruction.
Sélectionner	Conditions requises par la règle. Deux options sont possibles : • Si toutes les conditions sont réunies • Si l'une de ces conditions est réunie
Clé	Clé pour ESA à enregistrer dans l'instruction de la règle.

Paramètre	Description
Type d'évaluation	Relation entre la clé méta et la valeur de la clé : • est • n'est pas • n'est pas nul • est supérieur à (>) • est supérieur ou égal à (>=) • est inférieur à (<) • est inférieur ou égal à (<=) • contient • ne contient pas • commence par • se termine par
Valeur	Valeur pour ESA à rechercher dans la clé.
Ignorer la casse ?	Ce champ est conçu pour être utilisé avec les valeurs de chaînes et tableau de chaînes. Si vous choisissez le champ **Ignorer la casse**, la requête traitera toute chaîne de texte comme étant une valeur minuscule. Cela permet de garantir qu'une règle qui recherche un utilisateur nommé Johnson se déclenchera si un événement contient « johnson », « JOHNSON » ou « JoHnSoN ».
Tableau ?	Choix pour indiquer si le contenu du champ Valeur représente une ou plusieurs valeurs : • Cochez cette case pour indiquer des valeurs multiples. • Décochez cette case pour indiquer une seule valeur.
+	Permet d'ajouter une instruction. Vous pouvez ajouter une condition méta, une condition de liste blanche ou une condition de liste noire.
−	Permet de supprimer l'instruction sélectionnée.
Enregistrer	Permet d'ajouter une instruction à la section Conditions de l'onglet Générateur de règles.

Le tableau ci-dessous décrit les opérateurs que vous pouvez utiliser dans le Générateur de règles :

Opérateur	Valeur requise	Utilisation	Exemple	Signification
est	Valeur de chaîne au singulier	La clé méta équivaut au champ *valeur*.	***user_dst*** est John Doe.	***user_dst*** est égal à la chaîne *« John Doe »*.
est	Valeur de chaîne de tableau	La clé méta est égale à l'un des éléments du champ *valeur*.	*user_dst* est John, Doe, Smith.	*user_dst* est égal à la chaîne *« John »* ou à la chaîne *« Doe »* ou à la chaîne *« Smith »* (remarque : les espaces sont supprimés).
n'est pas	Valeur de chaîne au singulier	La clé méta n'est pas équivalente au champ *valeur*.	***size*** n'est pas 200.	***size*** n'est pas égale au chiffre 200 (la taille est une valeur numérique).
n'est pas	Valeur de chaîne de tableau	La clé méta n'est égale à aucun élément du champ *valeur*.	***size*** n'est pas 200, 300, 400.	***size*** n'est pas égale à *200* ou à *300* ou à *400*.
n'est pas nul	N/A (recherche toute valeur)	La valeur de la clé méta n'est pas nulle.	La valeur ***user_dst*** n'est pas nulle.	***La valeur user_dst*** est une méta contenant une valeur.
est supérieur à (>)	Nombre	La valeur numérique de la clé méta est supérieure au nombre du champ *valeur*.	La valeur ***payload*** est supérieure à 7000.	La valeur ***payload*** est une valeur numérique supérieure à 7000.
est supérieur ou égal à (>=)	Nombre	La valeur numérique de la clé méta est supérieure ou égale au nombre du champ *valeur*.	La valeur ***payload*** est supérieure ou égale à 7000.	La valeur ***payload*** est une valeur numérique supérieure ou égale à 7000.
est inférieur à (<)	Nombre	La valeur numérique de la clé méta est inférieure au nombre du champ *valeur*.	***ip_dstport*** est inférieur à 1024.	***ip_dstport*** est une valeur numérique inférieure à 1024.
est inférieur ou égal à (<=)	Nombre	La valeur numérique de la clé méta est inférieure ou égale au nombre du champ *valeur*.	***ip_dstport*** est inférieur ou égal à 1024.	***ip_dstport*** est une valeur numérique inférieure ou égale à 1024.

Opérateur	Valeur requise	Utilisation	Exemple	Signification
contient	Chaîne	Le champ *valeur* est une sous-chaîne de la clé méta (cet opérateur n'est valable que pour une clé méta de la valeur d'une chaîne).	***ec_outcome*** comprend failure.	***ec_outcome*** est une chaîne qui contient la sous-chaîne *« failure »*.
ne contient pas	Chaîne	Le champ *valeur* n'est pas une sous-chaîne de la clé méta (cet opérateur n'est valable que pour une clé méta de la valeur d'une chaîne).	***ec_outcome*** ne comprend pas failure.	***ec_outcome*** est une chaîne ne contenant pas la sous-chaîne *« failure »*.
commence par	Chaîne	Le champ *valeur* est le début de la clé méta (cet opérateur n'est valable que pour une clé méta de la valeur d'une chaîne).	***ip_dst*** commence par 127.0.	***ip_dst*** est une chaîne qui commence par *« 127.0 »*.
se termine par	Chaîne	Le champ *valeur* est la fin de la clé méta (cet opérateur n'est valable que pour une clé méta de la valeur d'une chaîne).	***user_dst*** termine par son.	***user_dst*** est une chaîne qui termine par *« son »*.

Remarque : Les termes ***en gras et italique*** sont des méta qui peuvent ne pas exister dans tous les environnements clients.

Boîte de dialogue Déployer des règles ESA

La boîte de dialogue Déployer des règles ESA vous permet de filtrer et de sélectionner des règles à déployer vers un service ESA.

Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Expert du contenu	Configurer un déploiement.	Étape 1. Ajouter un déploiement
Expert du contenu	Déployer une règle	Étape 3. Ajouter et déployer des règles

Rubriques connexes

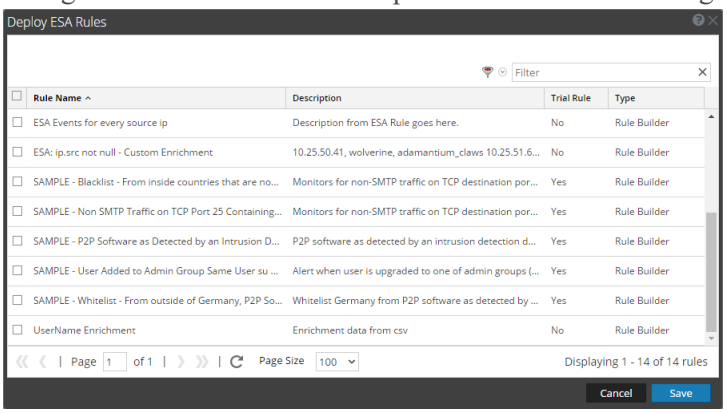
- Procédures de déploiement supplémentaires

Boîte de dialogue Déployer des règles ESA

Pour accéder à cette boîte de dialogue :

1. Accédez à **CONFIGURER > Règles ESA**.
   L'onglet Règles s'ouvre par défaut.
2. Dans le panneau des options, sous la section **Déploiement**, sélectionnez ou ajoutez un nouveau déploiement en cliquant sur  **> Ajouter**.
3. Si vous ajoutez un nouveau déploiement, saisissez le nom du déploiement dans la zone dans le panneau des options.
4. Dans le panneau **Règles ESA**, cliquez sur  .
   La boîte de dialogue Règles ESA s'affiche.

La figure suivante offre un exemple de cette boîte de dialogue.



Le tableau suivant décrit les paramètres de la boîte de dialogue Déployer des règles ESA.

Paramètres	Description
	Filtre la liste des règles par gravité et type. La zone de texte à côté de cette icône filtre par nom de règle.
Nom de la règle	Affiche le nom de la règle.
Description	Décrit la règle.
Règle d'évaluation	Indique si la règle est une règle d'évaluation.
Type	Indique le type de règle. Live ESA de RSA, EPL avancé ou Générateur de règles.

Boîte de dialogue Déployer des services ESA

La boîte de dialogue Déployer les services ESA affiche tous les services ESA pouvant être ajoutés à un déploiement.

Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Expert du contenu	Configurer un déploiement.	Étape 1. Ajouter un déploiement
Expert du contenu	Déployer un service	Étape 2. Ajouter un service ESA

Rubriques connexes

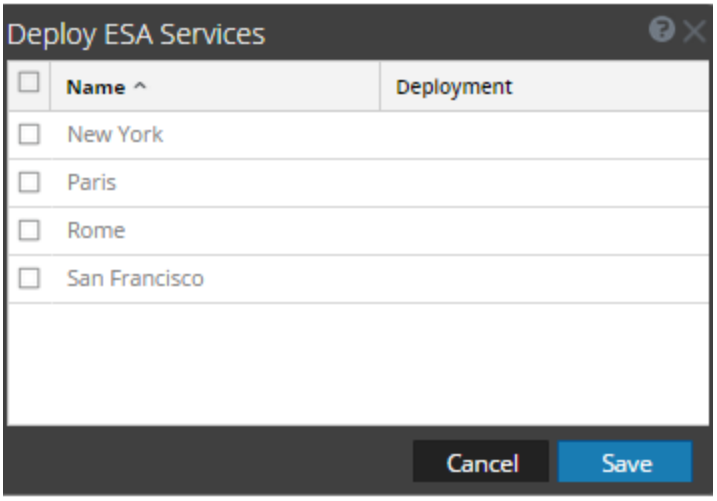
- Procédures de déploiement supplémentaires
- Afficher les statistiques pour un service ESA

Boîte de dialogue Déployer des services ESA

Pour accéder à cette boîte de dialogue :

1. Accédez à **CONFIGURER > Règles ESA**.
   L'onglet Règles s'ouvre par défaut.
2. Dans le panneau d'options, sous la section **Déploiement**, sélectionnez ou ajoutez un déploiement.
3. Dans le panneau **Services ESA**, cliquez sur  .
   La boîte de dialogue Déployer les services ESA s'affiche.

La figure suivante offre un exemple de cette boîte de dialogue.



Le tableau suivant décrit les paramètres de la boîte de dialogue Déployer les services ESA.

Paramètres	Description
Nom	Affiche le nom des services ESA configurés.
Déploiement	Affiche les déploiements auxquels le service a déjà été ajouté.

Onglet Générateur de règles

L'onglet Générateur de règles vous permet de définir une règle de type Générateur de règles.

Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Expert du contenu	Définir une règle Générateur de règles.	Ajouter une règle Générateur de règles
Expert du contenu	Définir des critères de règle.	Étape 2. Créer une instruction de règle
Expert du contenu	Ajouter des conditions à la règle.	Étape 3. Ajouter des conditions à une instruction de règle

Rubriques connexes

- Ajouter une règle EPL avancée

Générateur de règles

Pour accéder à l'onglet Générateur de règles :

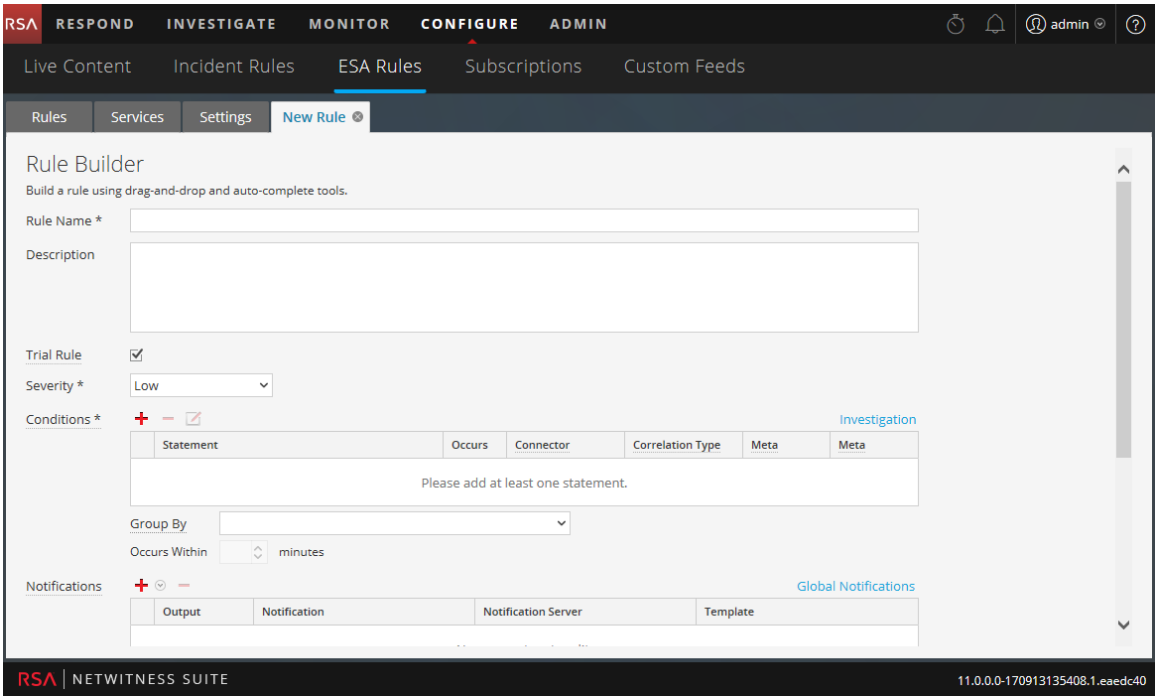
1. Accédez à **CONFIGURER** > **Règles ESA**.

   L'onglet Règles s'ouvre par défaut.

2. Dans la barre d'outils **Bibliothèque de règles**, sélectionnez  > **Générateur de règles**.

   L'onglet Générateur de règles s'affiche.

La figure ci-dessous présente l'onglet Générateur de règles.



Le tableau suivant affiche les paramètres de l'onglet Générateur de règles.

Paramètres	Description
Nom de la règle	Objectif de la règle ESA.
Description	Récapitulatif des éléments détectés par la règle ESA.
Règle d'évaluation	Mode de déploiement afin de déterminer si la règle s'exécute efficacement.
Gravité	Niveau de menace de l'alerte déclenchée par la règle.

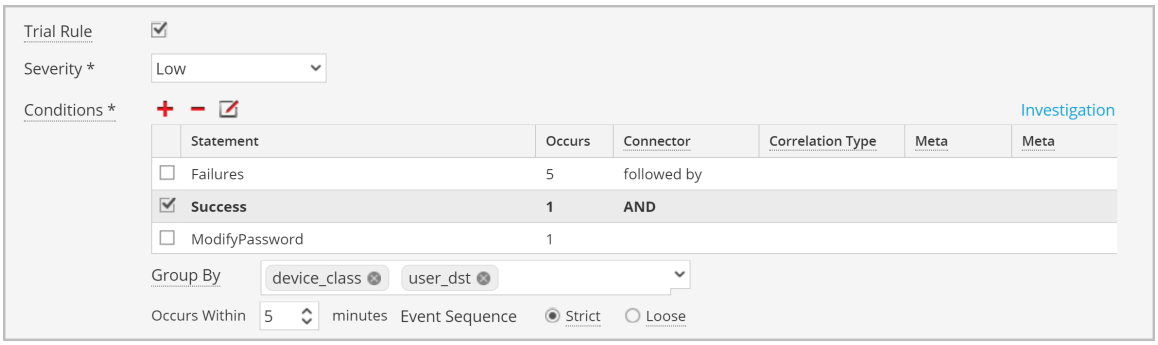
Le Générateur de règles contient les composants suivants :

- Section Conditions
- Section Notifications
- Section Enrichissements

Section Conditions

Dans la section Conditions de l'onglet Générateur de règles, définissez ce que la règle doit détecter.

La figure ci-dessous présente la section Conditions.



Le tableau suivant répertorie les paramètres de la section Conditions.

Paramètre	Description
+	Permet d'ajouter une instruction.
−	Supprime l'instruction sélectionnée.
✎	Modifie l'instruction sélectionnée.
Instruction	Groupe de conditions logiques pour une opération.
Se produit	Fréquence de l'alerte si la ou les conditions sont réunies. Cela indique que certains événements répondent aux critères pour déclencher une alerte. La période en minutes est liée au nombre défini dans le paramètre Se produit.

Paramètre	Description
Connector	Options permettant de spécifier une relation entre les instructions : • suivi par • non suivi par • AND • OR Le connecteur relie les instructions à l'aide des options ET, OU, suivi par, non suivi par. Lorsque le paramètre « suivi par » est utilisé, il désigne un séquençage d'événements. Les paramètres ET et OU permettent d'élargir les critères. Le paramètre « suivi par » crée des critères distincts qui se produisent dans une séquence.
Type de corrélation	**Type de corrélation** s'applique uniquement à **suivi de** et **non suivi de**. Si vous choisissez un type de corrélation SAME, sélectionnez une méta pour la corrélation et, si vous choisissez un type de corrélation JOIN, sélectionnez deux métas pour la corrélation. Vous voudrez peut-être utiliser JOIN si vous tentez de mettre en corrélation les métas à partir de deux sources de données différentes. Par exemple, supposons que vous souhaitiez mettre en corrélation une alerte AV avec une alerte IDS.
Meta	Saisissez la condition méta si vous avez choisi le type de corrélation SAME ou JOIN (comme décrit ci-dessus).
Meta	Saisissez la seconde condition méta si vous avez choisi le type de corrélation JOIN (comme décrit ci-dessus). Par exemple, l'adresse IP de destination de l'alerte AV et de l'adresse IP source pour la station de travail à partir de l'alerte IDS sont associées afin de vous permettre d'afficher les mêmes entités sur différentes sources.
Se produit dans les	Période de temps pendant laquelle les conditions doivent se produire.

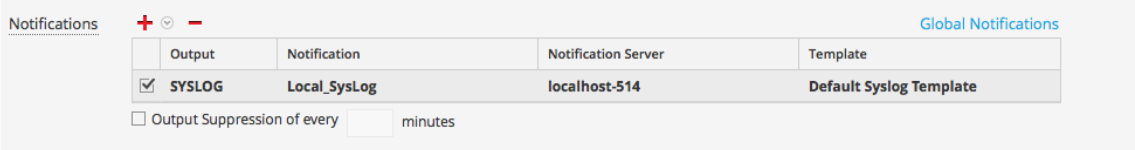
Paramètre	Description
Séquence d'événements	Indiquez si le modèle doit suivre une correspondance de type *Strict* ou *Souple*. Si vous spécifiez une correspondance stricte, cela signifie que le modèle doit se produire *exactement* selon la séquence spécifiée, sans aucun événement supplémentaire dans l'intervalle. Par exemple, si la séquence spécifie cinq échecs de connexion (F) suivis d'une connexion réussie (S), la correspondance à ce modèle n'est effective que si l'utilisateur exécute la séquence suivante : F,F,F,F,F,S. Si vous spécifiez une correspondance souple, cela signifie que d'autres événements peuvent avoir lieu durant la séquence. Toutefois, la règle se déclenche quand même si tous les événements spécifiés se produisent également. Par exemple, le modèle suivant peut être créé par cinq échecs de tentatives de connexion (F), puis n'importe quel nombre intermédiaire de tentatives de connexion réussies (S), puis une tentative de connexion réussie : F,S,F,S,F,S,F,S,F,S qui déclenche la règle malgré les tentatives de connexion réussies dans l'intervalle.
Grouper par	Sélectionnez la clé méta par laquelle grouper les résultats à partir de la liste déroulante. Par exemple, imaginez qu'il existe trois utilisateurs : Joe, Jane et John et que vous utilisez la méta Regrouper par, **user_dst** (user_dst est le champ méta pour le compte utilisateur de destination). Le résultat affiche les événements regroupés sous les comptes utilisateur Joe, Jane et John. Vous pouvez également grouper par clés multiples. Par exemple, vous pouvez grouper par utilisateur et machine pour vérifier si un utilisateur connecté à la même machine tente de se connecter plusieurs fois à un compte. Pour cela, vous pouvez grouper par device_class et user_dst.

Notifications

Dans la section Notifications, vous pouvez choisir le mode de notification lorsqu'ESA génère une alerte pour la règle.

Pour plus d'informations sur les notifications d'alertes, reportez-vous à la rubrique Ajouter une méthode de notification à une règle.

La figure ci-dessous présente la section Notifications.



Paramètre	Description
	Pour ajouter un type de notification d'alerte.

Paramètre	Description
	Pour supprimer la notification d'alerte sélectionnée.
Résultat	Type de notification d'alerte. Les options possibles sont : • E-mail • SNMP • Syslog • Script
Notification	Nom de la sortie précédemment configurée, comme la liste de diffusion d'e-mails.
Serveur de notification	Nom du serveur qui envoie la sortie.
Modèle	Nom du modèle pour la notification d'alerte.
Limite des notifications aux	Option permettant de spécifier la fréquence d'alerte.
Minutes	Fréquence d'alerte en minutes.

Enrichissements

Dans la section Enrichissements, vous pouvez ajouter une source d'enrichissement de données à une règle.

Pour plus d'informations sur les enrichissements, reportez-vous à la rubrique Ajouter un enrichissement à une règle.

La figure ci-dessous présente la section Enrichissements.

Paramètre	Description
	Pour ajouter un enrichissement.

Paramètre	Description
—	Pour supprimer l'enrichissement sélectionné.
Résultat	Type de source d'enrichissement. Les options possibles sont : • Table en mémoire • Référence BD externe • Warehouse Analytics • GeoIP
Source d'enrichissement	Nom de la source d'enrichissement précédemment configurée, comme un nom de fichier .CSV pour une table en mémoire.
Méta de flux d'événements ESA	Clé méta ESA dont la valeur sera utilisée en tant qu'opérande de la condition join.
Nom de la colonne de la source d'enrichissement	Nom de la colonne de la source d'enrichissement dont la valeur sera utilisée en tant qu'autre opérande de la condition join. Pour une table en mémoire, si vous avez configuré une clé lors de la création d'un enrichissement basé sur .CSV, cette colonne est générée automatiquement avec la clé sélectionnée. Toutefois, vous pouvez la modifier si vous le souhaitez. Pour une source d'enrichissement GeoIP, ipv4 est sélectionné automatiquement.

Onglet Règles

L'onglet Règles vous permet de gérer les règles ESA et les déploiements.

Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Expert du contenu	Afficher les types de règles.	Types de règles ESA
Expert du contenu	Déployer les règles d'évaluation.	Utiliser les règles d'évaluation
Expert du contenu	Créez une règle.	Ajouter des règles à la Bibliothèque de règles
Expert du contenu	Déployer une règle.	Déployer des règles à exécuter sur ESA

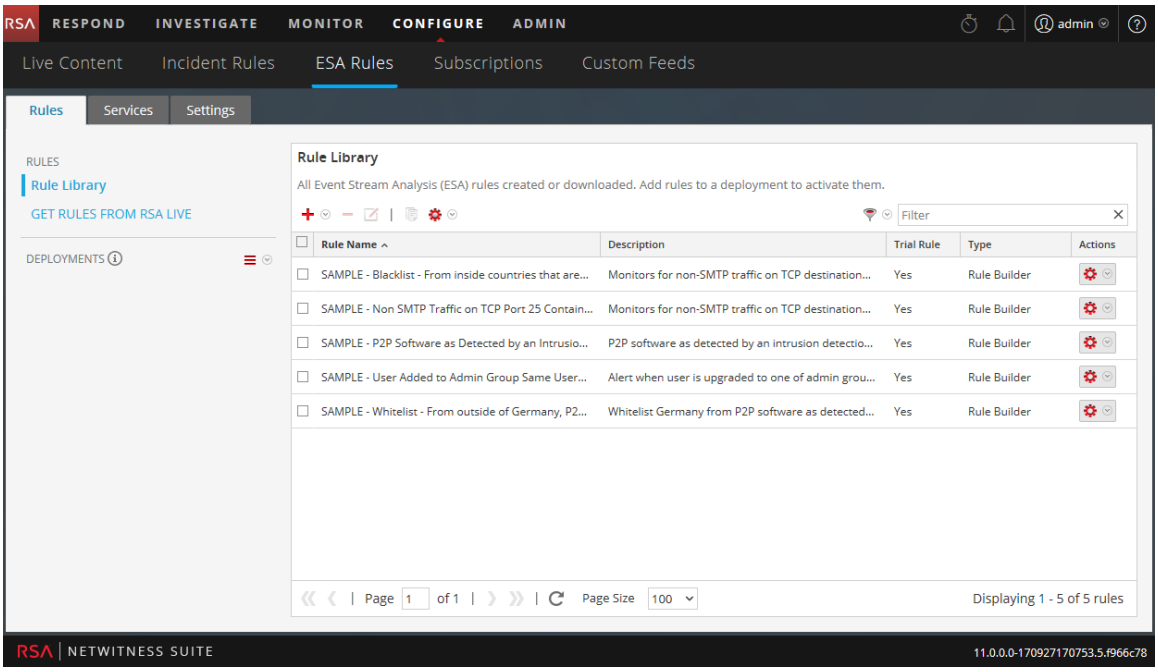
Rubriques connexes

- Mise en route avec ESA

Générateur de règles

L'onglet Règles s'affiche lorsque vous accédez à **CONFIGURER > Règles ESA**.

La figure ci-dessous présente l'onglet Règles.



L'onglet Règles est divisé en trois sections :

- Panneau Options de l'onglet Règles
- Panneau Bibliothèque de règles
- Panneau Déploiement

Panneau Options de l'onglet Règles

Dans le panneau des options de l'onglet **Règles** , à gauche, vous pouvez afficher les règles ESA dans la bibliothèque de règles et créer des déploiements.

Que voulez-vous faire ?

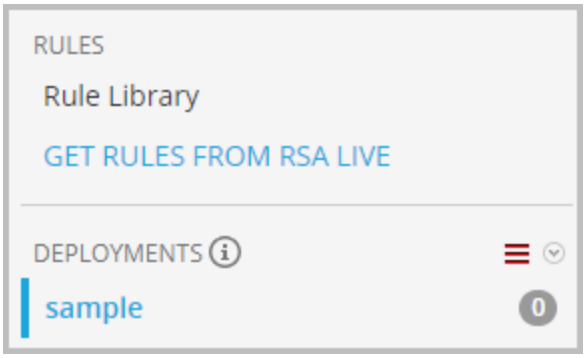
Rôle	Je souhaite...	Me montrer comment
Expert du contenu	Afficher une règle ESA.	Ajouter des règles à la Bibliothèque de règles
Expert du contenu	Créer un déploiement.	Étapes de déploiement

Rubriques connexes

- Utilisation des règles

Panneau Options

La figure suivante illustre le panneau d'options de l'onglet **Règles**.



Le panneau d'option contient deux sections : Règles et déploiements

Section Règles

La section règles contient deux options. **L'option Bibliothèque de règles** est sélectionnée par défaut, et dans ce cas, la vue Bibliothèque de règles s'affiche sous l'onglet. **Obtenir des règles de RSA Live** accède à la vue Recherche Live, où vous pouvez rechercher des règles.

Section Déploiements

La section Déploiements répertorie les déploiements et indique s'il existe des mises à jour des déploiements. Dans cette section, les déploiements peuvent être ajoutés, supprimés, modifiés et actualisés. Si vous sélectionnez un déploiement dans la liste, le panneau Déploiement s'affiche sous l'onglet. Le tableau suivant décrit les fonctions de cette section.

Fonctionnalité	Description
	Affiche un menu déroulant dans lequel vous pouvez choisir d'ajouter, de modifier ou de supprimer un déploiement. Vous pouvez aussi actualiser la liste des déploiements pour voir s'il existe de nouvelles mises à jour de cette liste.
	Indique s'il existe des mises à jour du déploiement.
	Indique le nombre de règles présentes dans le déploiement.

Panneau Bibliothèque de règles

Le panneau Bibliothèque de règles vous permet de gérer les règles.

Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Expert du contenu	Ajouter une règle ESA.	Ajouter une règle Générateur de règles
Expert du contenu	Modifier, dupliquer ou supprimer une règle ESA.	Modifier, dupliquer ou supprimer une règle
Expert du contenu	Importer ou exporter des règles ESA.	Importer ou exporter des règles
Expert du contenu	Filtrer la liste de règles ESA.	Filtrer ou rechercher des règles

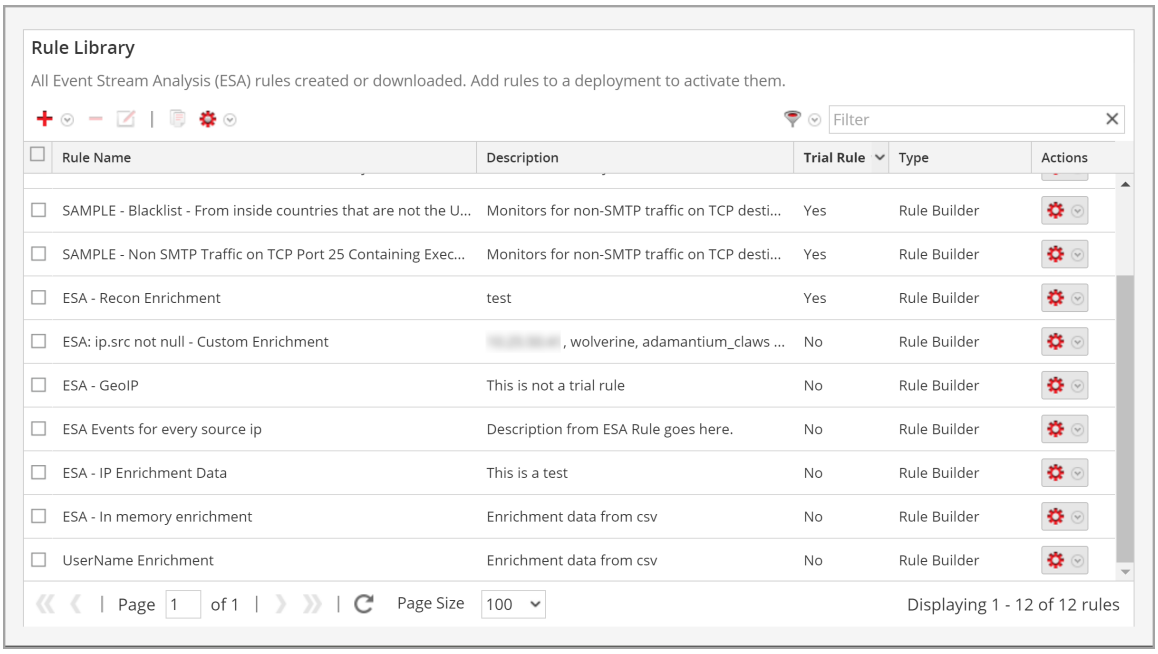
Rubriques connexes

- Ajouter une règle EPL avancée

Panneau Bibliothèque de règles

Pour accéder à cette vue, accédez à **CONFIGURER > Règles ESA**. L'onglet Règles s'affiche et le panneau Bibliothèque de règles se trouve sur la droite.

La figure ci-dessous montre le panneau Bibliothèque de règles.



Le panneau Bibliothèque de règles inclut les composants suivants :

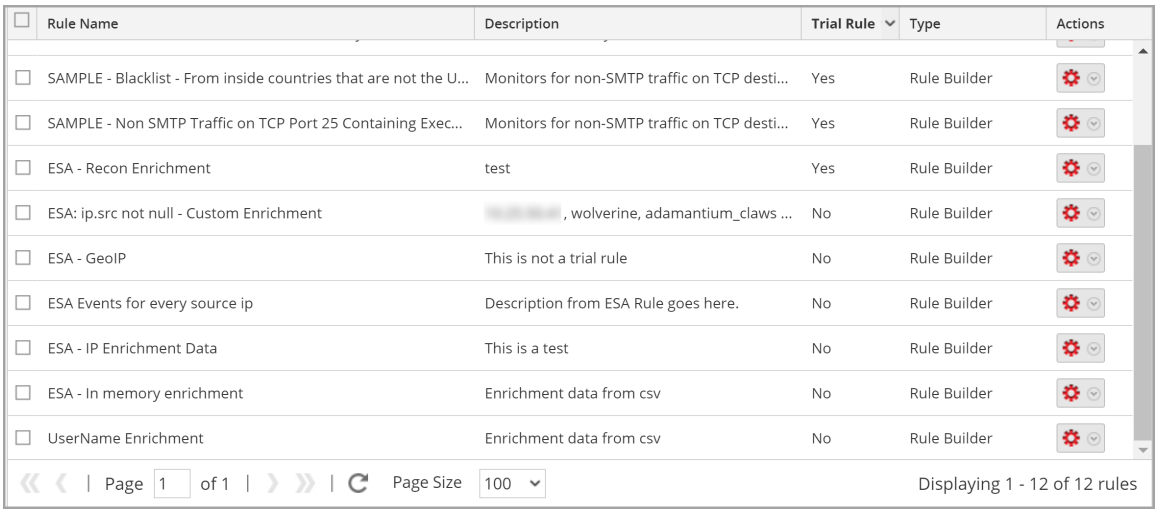
- Barre d'outils Bibliothèque de règles
- Liste Bibliothèque de règles

Barre d'outils Bibliothèque de règles

La barre d'outils Bibliothèque de règles vous permet d'ajouter, de supprimer, de modifier, de dupliquer, de filtrer, d'exporter et d'importer des règles ESA. La figure suivante montre les icônes correspondant à ces actions.

Liste Bibliothèque de règles

La figure ci-dessous présente la liste Bibliothèque de règles.

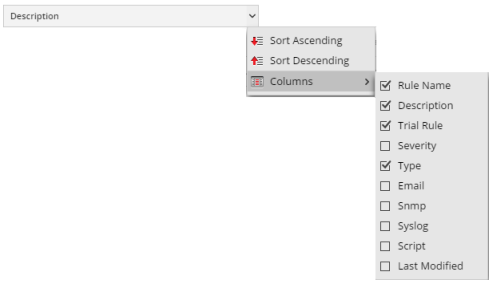


La liste Bibliothèque de règles affiche toutes les règles ESA qui ont été téléchargées à partir de RSA Live ou créées dans les onglets EPL avancé et Générateur de règles. Le tableau suivant répertorie les colonnes de la liste Bibliothèque de règles et leur description.

Colonne	Description
Nom de la règle	Objectif de la règle ESA.
Description	Récapitulatif des éléments détectés par la règle ESA.
Règle d'évaluation	Mode de déploiement afin de déterminer si la règle s'exécute efficacement.
Type	Type de règle.
Actions (⚙)	Menu pour supprimer, modifier, dupliquer ou exporter la règle sélectionnée.
Gravité	Niveau de menace de l'alerte déclenchée par la règle.
E-mail	Indique si une notification d'alerte pour la règle est envoyée par e-mail. Cette colonne n'est pas visible par défaut.
Snmp	Indique si une notification d'alerte pour la règle est envoyée avec SNMP. Cette colonne n'est pas visible par défaut.

Colonne	Description
Syslog	Indique si une notification d'alerte pour la règle est envoyée avec Syslog. Cette colonne n'est pas visible par défaut.
Script	Indique si une notification d'alerte pour la règle exécute un script. Cette colonne n'est pas visible par défaut.
Dernière modification	Date et heure auxquelles la règle ESA a été modifiée pour la dernière fois. Cette colonne n'est pas visible par défaut.

Pour afficher des colonnes qui ne sont pas visibles par défaut, passez la souris sur le titre d'une colonne et cliquez sur le **v** sur la droite. Cette action ouvre un menu déroulant dans lequel vous pouvez trier le contenu de la colonne ou choisir quelles colonnes vous souhaitez afficher dans la liste Bibliothèque de règles.



Panneau Déploiement

Cette rubrique présente le panneau Déploiement. Le panneau Déploiement permet de créer et de configurer des déploiements. Il comprend les sections suivantes :

- Services ESA
- Règles ESA

Que voulez-vous faire ?

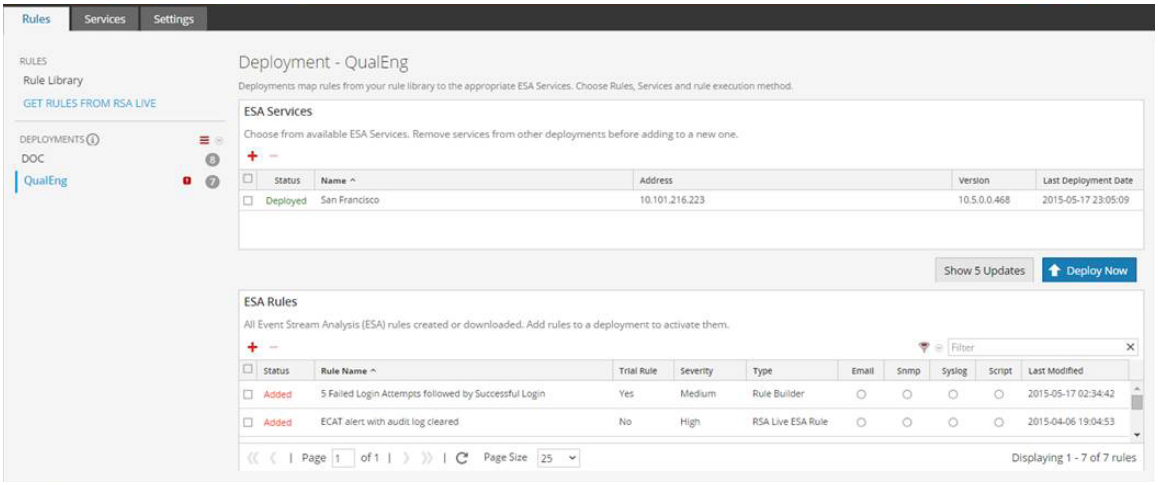
Rôle	Je souhaite...	Me montrer comment
Expert du contenu	Ajouter un déploiement.	Étapes de déploiement
Expert du contenu	Gérer des déploiements.	Procédures de déploiement supplémentaires

Rubriques connexes

- Afficher les statistiques pour un service ESA

Panneau Déploiement

La figure ci-dessous montre le panneau Déploiement.



Services ESA

Dans la section Services ESA, vous pouvez gérer chaque service ESA du déploiement.

Dans la section Services ESA, vous pouvez notamment effectuer les tâches suivantes.

Tâche	Description
+	Ajouter un service ESA au déploiement.
−	Supprimer le service ESA sélectionné du déploiement.
Afficher les mises à jour	Ouvre la boîte de dialogue Mises à jour appliquées au déploiement.
Déployer maintenant	Déploie l'ensemble de règles actuel.

Le tableau suivant répertorie les paramètres de la section Services ESA.

Paramètre	Description
État	Indique si le déploiement est **ajouté**, **déployé**, **mis à jour** ou **en échec**.
Nom	Nom du service ESA.
Adresse	Adresse IP de l'hôte sur lequel le service ESA est installé.
Version	Version du service ESA.
Date du dernier déploiement	Date et heure du dernier déploiement du service ESA.

Règles ESA

Dans la section Règles ESA, vous pouvez gérer les règles dans le déploiement. Cette section répertorie toutes les règles présentes dans le déploiement.

Dans la section **Règles ESA** , vous pouvez notamment effectuer les tâches suivantes.

Tâche	Description
+	Ouvrir la boîte de dialogue Déployer les règles ESA pour y sélectionner une règle.
−	Supprimer les règles ESA sélectionnées du déploiement.

Tâche	Description
	Filtrez la liste des règles.
	Rechercher une règle.

Le tableau suivant répertorie les paramètres de la section Règles ESA.

Paramètre	Description
État	Indique d'état de la règle : • Déployée : la règle est déployée. • Mise à jour : la règle a été mise à jour depuis son dernier déploiement. • Ajoutée : la règle a été ajoutée depuis son dernier déploiement. • En échec : le déploiement a échoué.
Nom de la règle	Objectif de la règle ESA.
Règle d'évaluation	Mode de déploiement afin de déterminer si la règle s'exécute efficacement.
Gravité	Niveau de menace de l'alerte déclenchée par la règle.
Résultat	Type de la règle ESA.
E-mail, SNMP, Syslog, Script	Indique les types de notifications qui sont utilisés pour les alertes générés par les règles.
Dernière modification	Date et heure auxquelles la règle ESA a été modifiée pour la dernière fois.

Boîte de dialogue Syntaxe de la règle

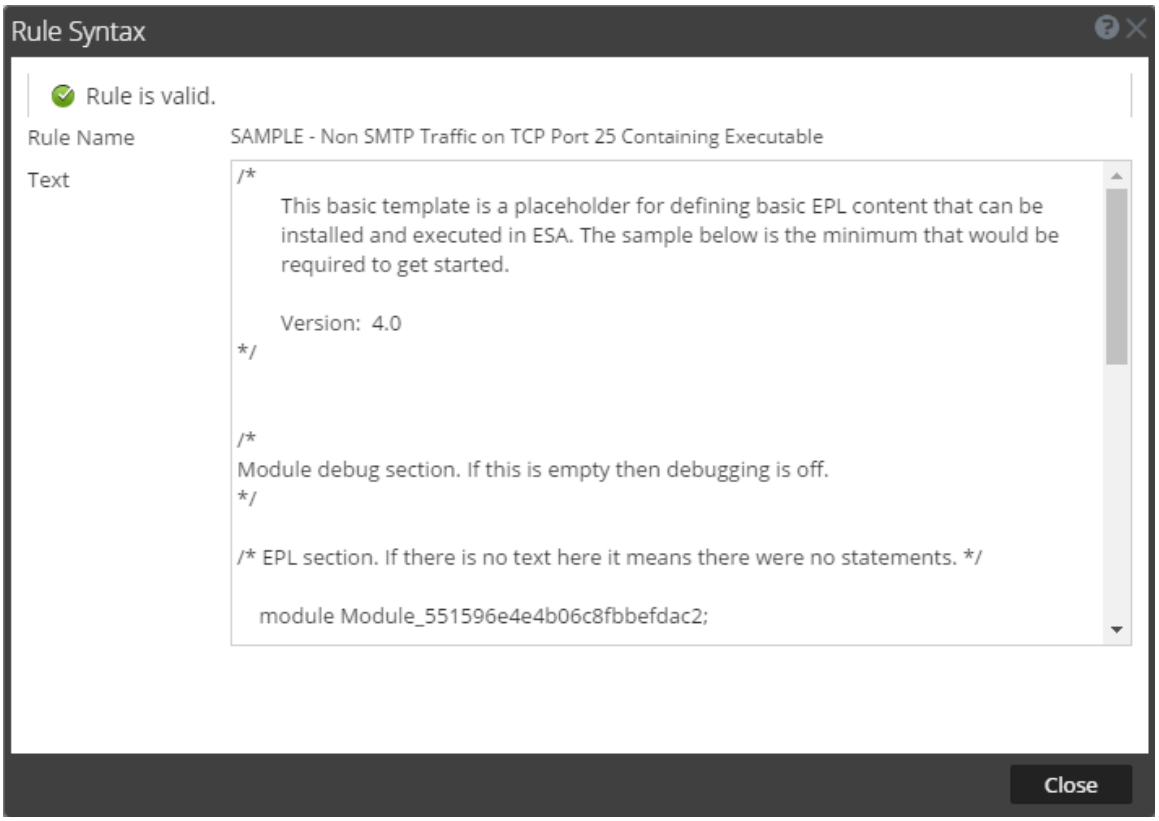
Cette rubrique décrit les fonctions de la boîte de dialogue Syntaxe de la règle. La boîte de dialogue Syntaxe de la règle affiche la syntaxe EPL des conditions, des instructions et des paramètres de débogage, et affiche un avertissement lorsque la syntaxe n'est pas valide.

Boîte de dialogue Syntaxe de la règle

Pour accéder à cette boîte de dialogue :

1. Accédez à **CONFIGURER > Règles ESA**.
2. Dans la vue **Bibliothèque de règles**, exécutez l'une des opérations suivantes :
   a. Cliquez sur , puis sélectionnez **EPL avancé** ou **Générateur de règles**.
   b. Double-cliquez sur une règle existante.
   c. Sélectionnez une règle existante et cliquez sur dans la barre d'outils **Bibliothèque de règles**.
   d. Sur la ligne d'une règle existante, sélectionnez **> Modifier**.
   La règle nouvelle ou existante s'affiche dans un nouvel onglet et peut être modifiée.
3. Cliquez sur **Afficher la syntaxe** au bas de l'onglet.

La figure suivante offre un exemple de la boîte de dialogue Syntaxe de la règle.



Le tableau suivant décrit les paramètres de la boîte de dialogue Syntaxe de la règle.

Paramètres	Description
La règle est valide ou **Erreur de validation dans la règle**	Indique si la syntaxe de règle est valide ou doit être modifiée.
Nom de la règle	Affiche le nom de la règle.
Text	Affiche la syntaxe EPL des conditions, des instructions et des paramètres de débogage si la règle est valide.

Onglet Services

Cette rubrique présente l'onglet **CONFIGURER > Règles ESA > Services**. L'onglet Services fournit des détails sur les services ESA ajoutés à NetWitness Suite.

Que voulez-vous faire ?

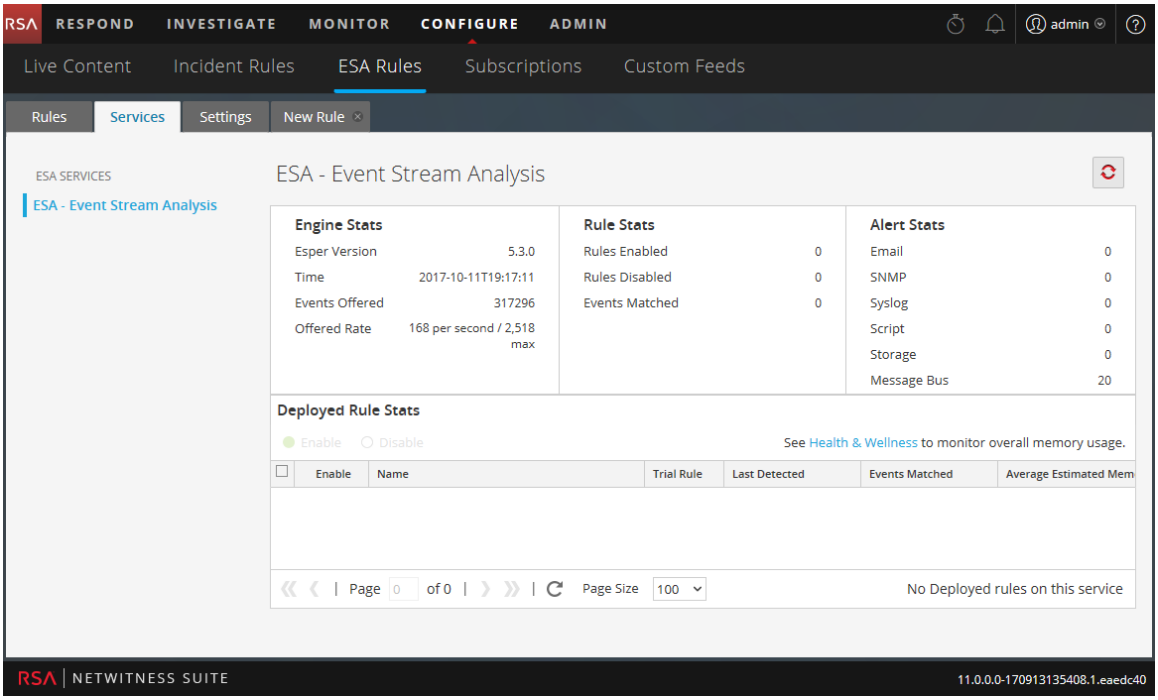
Rôle	Je souhaite...	Me montrer comment
Expert du contenu	Résoudre les problèmes liés à l'onglet Services.	Dépanner le service ESA
Expert du contenu	Afficher les statistiques de déploiement pour un service ESA.	Afficher les statistiques pour un service ESA

Rubriques connexes

- Afficher un récapitulatif des alertes

Services

La figure suivante montre l'onglet Services :



L'onglet Services contient les sections suivantes :

- Panneau Services ESA
- Panneau Statistiques générales
- Panneau Statistiques de règles déployées

Panneau Services ESA

Le panneau Services ESA affiche le nom de chaque service ESA ajouté à NetWitness Suite.

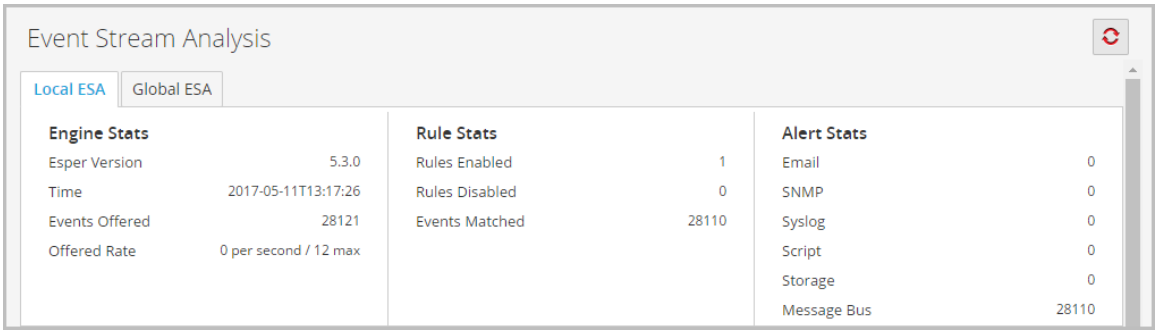
Panneau Statistiques générales

Le panneau Statistiques générales fournit des informations sur chaque moteur, règle et alerte Esper.

L'onglet Statistiques générales contient les sections suivantes :

- Stat. engine
- Stat. règles
- Statistiques d'alerte

La figure suivante affiche l'onglet Statistiques générales.



Le tableau affiche et décrit les paramètres de chaque section.

Sections	Paramètre	Description
Stat. engine	Version Esper	Version Esper exécutée sur le service ESA
	Heure	Heure d'envoi du dernier événement au moteur Esper
	Événements fournis	Nombre d'événements analysés par le service ESA depuis le dernier démarrage du service
	Taux fourni	Taux d'événements actuels sur le service ESA

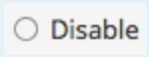
Sections	Paramètre	Description
Stat. règles	Règles activées	Nombre de règles activées
	Règles désactivées	Nombre de règles désactivées
	Correspondances d'événements	Nombre total d'événements correspondant à toutes les règles sur le service ESA.
Statistiques d'alerte	E-mail	Nombre de notifications par e-mail envoyées par le service ESA
	SNMP	Nombre de notifications SNMP envoyées par le service ESA
	Syslog	Nombre de notifications Syslog envoyées par le service ESA
	Script	Nombre de notifications par script envoyées par le service ESA
	Stockage	Nombre total d'alertes stockées dans la base de données
	Bus de messages	Nombre total d'alertes envoyées au bus de messages

Panneau Statistiques de règles déployées

Le panneau Statistiques de règles déployées fournit les détails relatifs aux règles qui sont déployées sur le service ESA.

La figure suivante affiche l'onglet Statistiques de règles déployées.

Le tableau affiche les différents paramètres dans la vue et leur description.

Paramètres	Description
	Indique que la règle est activée. Active une règle qui a été désactivée.
	Indique que la règle est désactivée. Désactive une règle qui a été activée.
Intégrité	Affiche un snapshot de l'utilisation de la mémoire lorsque les règles d'évaluation sont désactivées.
Activer	Indique si la règle est activée ou désactivée. L'icône verte indique que la règle est activée. L'icône blanche indique que la règle est désactivée.
Nom	Nom de la règle ESA.
Règle d'évaluation	Indique si la règle est exécutée en mode règle d'évaluation.
Dernière détection	Dernière fois que l'alerte a été déclenchée pour la règle.
Correspondances d'événements	Nombre total d'événements en correspondance avec la règle.

Onglet Paramètres

Cette rubrique décrit les composants de l'onglet **CONFIGURER > Règles ESA > Paramètres**. Sous l'onglet Paramètres, vous pouvez effectuer les opérations suivantes :

- Afficher une liste des clés méta
- Configurer une source d'enrichissement de données
- Ajouter une connexion à une base de données externe

Que voulez-vous faire ?

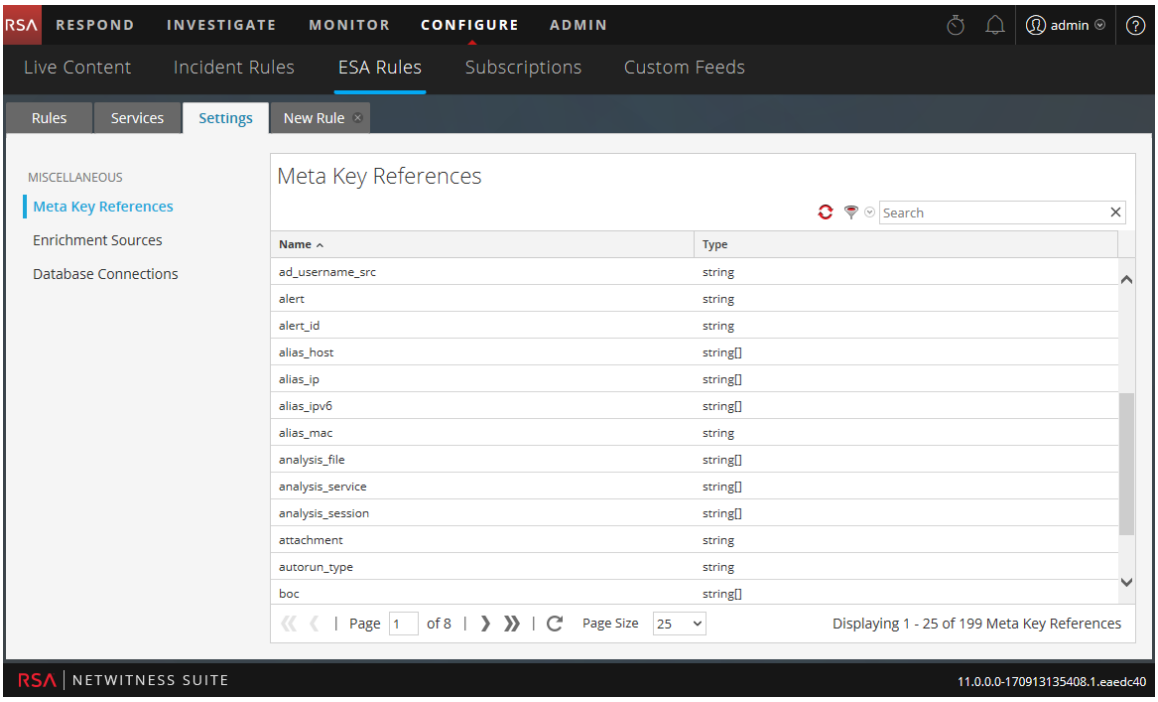
Rôle	Je souhaite...	Me montrer comment
Expert du contenu	Configurer une connexion à une base de données externe.	Configurer une connexion à la base de données
Expert du contenu	Configurer une base de données en tant que source d'enrichissement.	Sources d'enrichissement

Rubriques connexes

- Ajouter une source d'enrichissement de données

Paramètres

La figure suivante illustre la section Références aux clés méta de l'onglet Paramètres.



Références aux clés méta

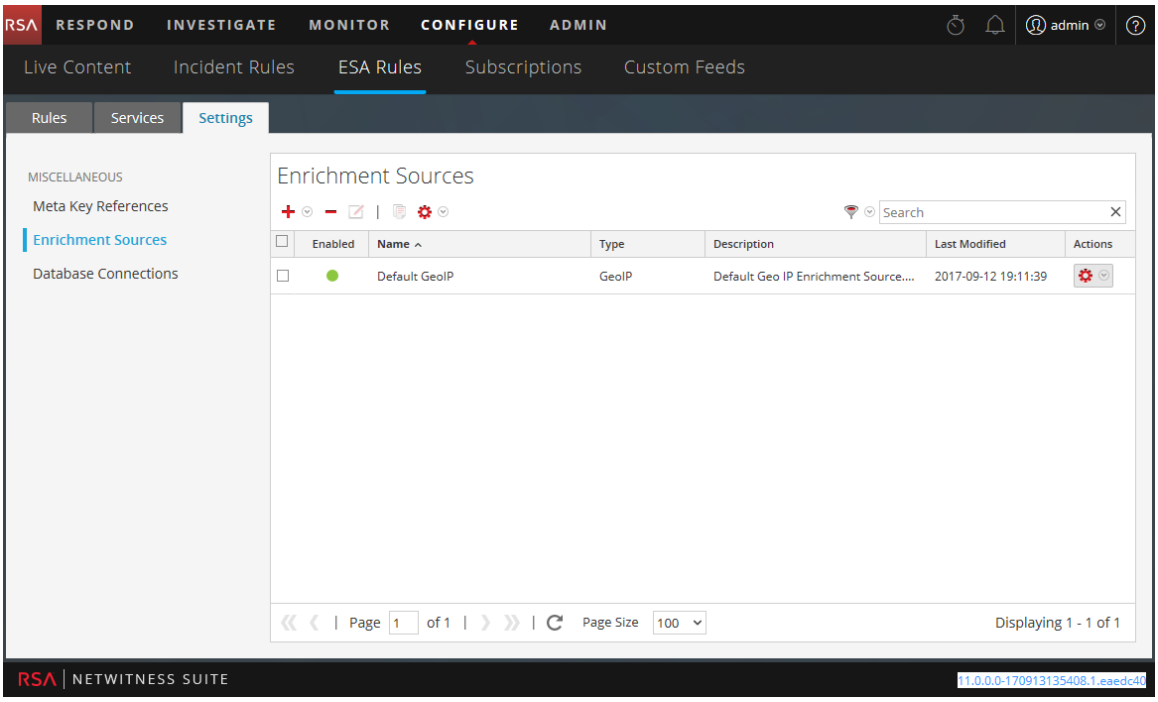
La section Références aux clés méta répertorie chaque clé méta et le type de valeur que la clé nécessite.

Sources d'enrichissement

La section Sources d'enrichissement vous permet de configurer les sources de données externes suivantes :

- GeoIP
- Référence de base de données externe
- Table en mémoire
- Warehouse Analytics

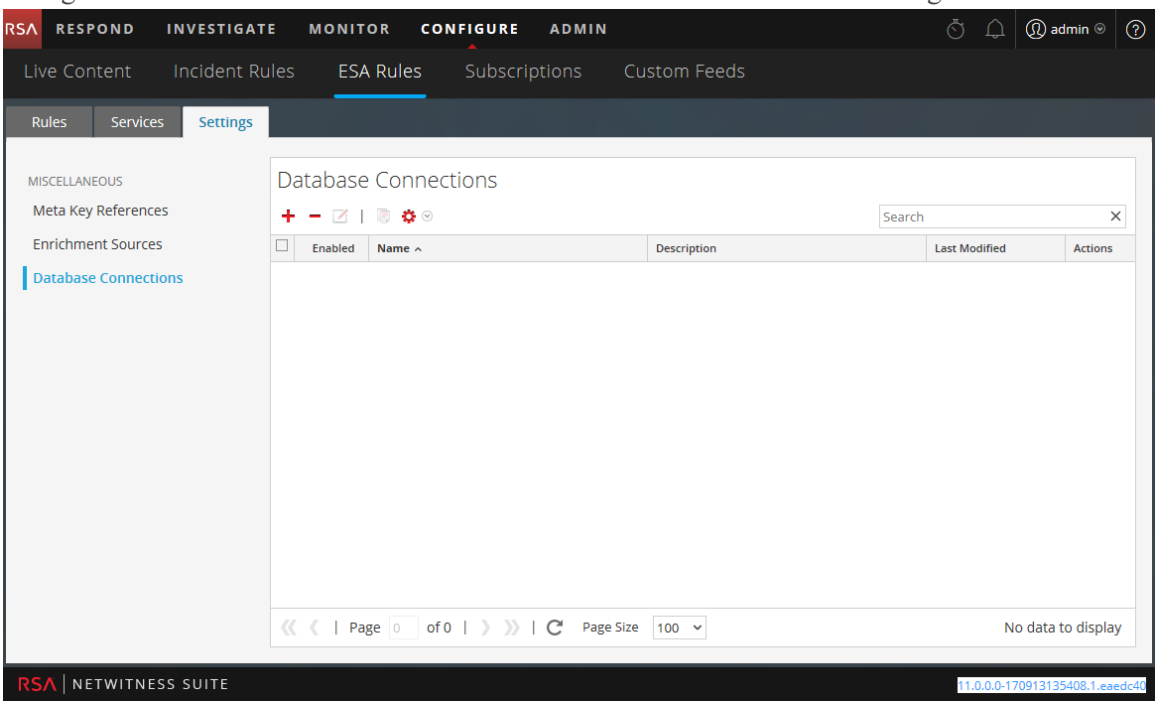
La figure suivante illustre la section Sources d'enrichissement de l'onglet Paramètres.



Connexions aux bases de données

La section Connexions aux bases de données vous permet de configurer une connexion à une base de données externe pour que ESA puisse accéder aux données.

La figure suivante illustre la section Connexions aux bases de données de l'onglet Paramètres.



Dans la section Connexions aux bases de données, vous pouvez effectuer les opérations suivantes :

- Ajouter une connexion à la base de données
- Supprimer une connexion à la base de données
- Modifier une connexion à la base de données
- Dupliquer une connexion à la base de données
- Importer une connexion à la base de données
- Exporter une connexion à la base de données

Boîte de dialogue Mises à jour appliquées au déploiement

La boîte de dialogue Mises à jour appliquées au déploiement affiche les mises à jour appliquées au déploiement, par exemple l'ajout d'une règle ou d'un service. Les mises à jour du déploiement sont indiquées par l'icône de mise à jour ( ) en regard du nom du déploiement dans le panneau d'options de l'onglet Règles.

Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Expert du contenu	Déployer des règles à exécuter sur ESA.	Étapes de déploiement
Expert du contenu	Modifier ou supprimer un déploiement	Modifier ou supprimer un déploiement
Expert du contenu	Afficher les mises à jour du déploiement.	Affiche les mises à jour d'un déploiement

Rubriques connexes

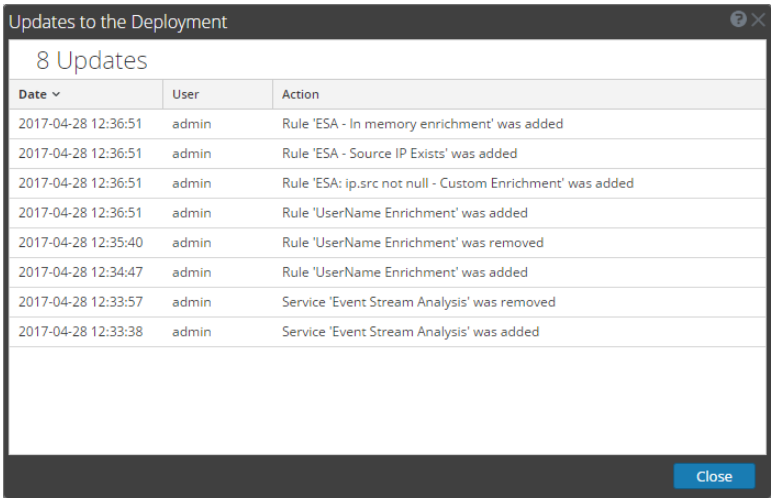
- Supprimer un service ESA dans un déploiement
- Modifier ou supprimer une règle dans un déploiement

Boîte de dialogue Déploiement

Pour accéder à cette boîte de dialogue :

1. Accédez à **CONFIGURER > Règles ESA**.
   L'onglet Règles s'ouvre par défaut.
2. Dans le panneau d'options, sous la section **Déploiements**, sélectionnez ou ajoutez un déploiement.
3. Dans le panneau **Déploiement**, cliquez sur **Afficher les mises à jour**.
   La boîte de dialogue Mises à jour appliquées au déploiement s'affiche.

La figure suivante offre un exemple de cette boîte de dialogue.



La boîte de dialogue Mises à jour appliquées au déploiement affiche le nombre de mises à jour en haut. Le tableau suivant décrit les paramètres de cette boîte de dialogue.

Paramètres	Description
Date	Affiche le jour et l'heure de la mise à jour.
Utilisateur	Affiche l'utilisateur qui a appliqué la mise à jour.
Action	Décrit la mise à jour.