Limite globale pour la journalisation des incidents d'intrusion

Les rubriques suivantes décrivent comment limiter globalement la journalisation des incidents d'intrusion :

Principes de base des seuils de règle globale

Le seuil de règle globale définit les limites de la journalisation des événements par une politique de prévention des intrusions. Vous pouvez définir un seuil de règle globale pour tout le trafic afin de limiter la fréquence à laquelle la politique consigne les événements d'une source ou d'une destination spécifique et affiche ces événements par période spécifiée. Vous pouvez également définir des seuils par règle d'objet partagé, règle de texte standard ou règle de préprocesseur dans la politique. Lorsque vous définissez un seuil global, ce seuil s'applique à chaque règle de la politique qui n'a pas de seuil spécifique de remplacement. Les seuils peuvent vous éviter d'être submergé par un grand nombre d'événements.

Chaque politique de prévention des intrusions contient un seuil de règle globale par défaut qui s'applique par défaut à toutes les règles de prévention des intrusions et de préprocesseur. Ce seuil par défaut limite le nombre d'événements sur le trafic se rendant vers une destination à un événement toutes les 60 secondes.

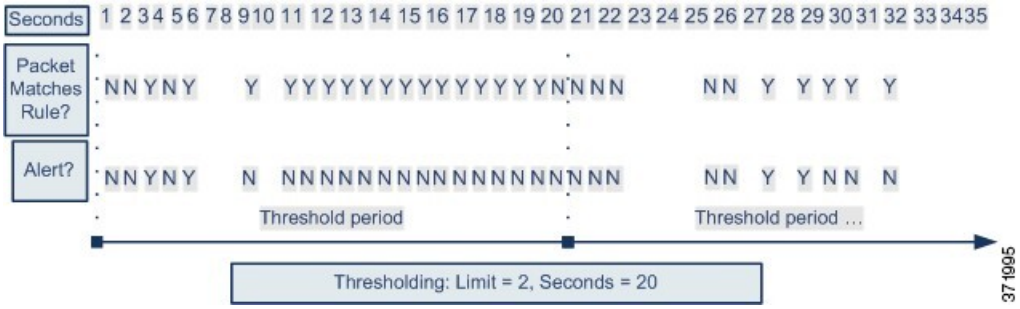
Vous pouvez réaliser les actions suivantes :

- Modifiez le seuil global.
- Désactivez le seuil global.
- Remplacer le seuil global en définissant des seuils individuels pour des règles spécifiques.

  Par exemple, vous pourriez définir un seuil global de cinq événements toutes les 60 secondes, puis définir un seuil spécifique de dix événements toutes les 60 secondes pour le SID 1315. Toutes les autres règles ne génèrent pas plus de cinq événements par période de 60 secondes, mais le système génère jusqu'à dix événements par période de 60 secondes pour la SID 1315.

Astuces Un seuil global ou individuel sur un périphérique géré avec plusieurs CPU peut entraîner un nombre d'événements plus élevé que prévu.

Le diagramme suivant montre le fonctionnement du seuillage de règle globale. Dans cet exemple, une attaque est en cours pour une règle spécifique. Le seuil de limite globale est défini pour limiter la génération d'événements pour chaque règle à deux événements toutes les 20 secondes. Notez que le point commence à une seconde et se termine à 21 secondes. À la fin de la période, le cycle recommence et les deux correspondances de règles suivantes génèrent des événements, puis le système ne génère plus d'événement pendant cette période.



Options de seuil de règle globale

Le seuil par défaut limite la génération d'événements pour chaque règle à un événement toutes les 60 secondes pour le trafic vers la même destination. Les valeurs par défaut des options de seuil des règles globales sont les suivantes :

- **Type** : limite
- **Suivi par** : destination
- **Nombre** : 1
- **Secondes** : 60

Vous pouvez modifier ces valeurs par défaut comme suit :

Tableau 1 : Types de seuils

Option	Description
Limite	Consigne et affiche les événements à propos du nombre de paquets spécifiés (spécifiés par la quantité d'arguments) qui déclenchent la règle pendant la période spécifiée. Par exemple, si vous définissez le type sur **Limite**, le **nombre** sur `10` et les **Secondes** sur `60`, et que 14 paquets déclenchent la règle, le système arrête de consigner les événements de la règle après avoir affiché les 10 premiers qui se produisent dans la même minute.

Option	Description
Seuil	Journalise et affiche un événement unique lorsque le nombre spécifié de paquets (spécifié par l'argument Nombre) déclenche la règle au cours de la période spécifiée. Notez que le compteur de l'heure redémarre une fois que vous avez atteint le nombre seuil d'événements et que le système enregistre cet événement. Par exemple, vous définissez le type sur **Seuil**, le **Nombre** sur `10` et **Secondes** à `60`, et la règle se déclenche 10 fois avant la 33ème seconde. Le système génère un événement, puis réinitialise les compteurs des secondes et du décompte à `0`. La règle se déclenche ensuite 10 autres fois dans les 25 secondes suivantes. Comme les compteurs sont réinitialisés à `0` à la 33ème seconde, le système enregistre un autre événement.
Les deux	Enregistre et affiche un événement une fois par période spécifiée, après qu'un nombre spécifié (le nombre) de paquets déclenche l'application de la règle. Par exemple, si vous définissez le type sur **Les deux**, **Nombre** sur `2`, et **Secondes** sur `10`, il en résulte le décompte des événements suivants : • Si la règle est déclenchée une fois toutes les 10 secondes, le système ne génère aucun événement (le seuil n'est pas atteint) • Si la règle est déclenchée deux fois en 10 secondes, le système génère un événement (le seuil est atteint lorsque la règle se déclenche pour la deuxième fois). • Si la règle est déclenchée quatre fois en 10 secondes, le système génère un événement (le seuil est atteint lorsque la règle se déclenche une deuxième fois et les événements suivants sont ignorés)

L'option **Track By** (suivre par) détermine si le nombre d'instances d'événement est calculé par adresse IP source ou de destination.

Vous pouvez également préciser le nombre d'instances et la période qui définit le seuil, comme suit :

Tableau 2 : Options de durée/instance de seuil

Option	Description
Quantité	Pour un seuil de **limite**, le nombre d'instances d'événement par période spécifiée et par adresse IP de suivi ou plage d'adresses requises pour atteindre le seuil. Pour un **seuil** de seuil, le nombre de correspondances de règles que vous souhaitez utiliser comme seuil.
Secondes	Pour un seuil de **limite**, il s'agit du nombre de secondes qui constituent la période pendant laquelle les attaques sont suivies. Pour un **seuil** de seuil, le nombre de secondes qui s'écoulent avant la réinitialisation du nombre. Si vous définissez le type de seuil sur **Limite**, le suivi sur **Source**, le **Nombre** sur 10 et **Secondes** sur 10, le système consigne et affiche les 10 premiers événements qui se produisent dans 10 secondes sur un port source donné. Si seulement sept événements se produisent dans les 10 premières secondes, le système se connecte et les affiche, si 40 événements se produisent dans les 10 premières secondes, le système se connecte et en affiche 10, puis recommence à compter lorsque la période de 10 secondes se produit.

Sujets connexes

Configuration des seuils globaux, à la page 4

Seuils de incidents d'intrusion

Exigences de licence pour les seuils globaux

Licence de défense contre les menaces

IPS

Licence traditionnelle

Protection

Exigences et prérequis pour les seuils globaux

Prise en charge des modèles

N'importe lequel

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin
- Administrateur d'intrusion

Configuration des seuils globaux

Dans un déploiement multidomaine, le système affiche les politiques créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les politiques créées dans les domaines ancêtres, que vous ne pouvez pas modifier. Pour afficher et modifier les politiques créées dans un domaine inférieur, basculez vers ce domaine.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 3 Cliquez sur **Advanced Settings** (paramètres avancés) dans le panneau de navigation.

Étape 4 Si le **Seuil de règles global** sous **Seuils de règles de prévention des intrusions** est désactivé, cliquez sur **Enabled** (Activé).

Étape 5 Cliquez sur **Edit** (✎) à côté de **Fixation de seuil des règles globales**.

Étape 6 À l'aide de **Type**, spécifiez le type de seuil qui s'appliquera au fil de la période que vous définissez dans le champ **Secondes**.

Étape 7 À l'aide de l'outil **Track By** (suivre par), spécifiez la méthode de suivi.

Étape 8 Saisissez une valeur dans le champ **Count** (Nombre).

Étape 9 Saisissez une valeur dans le champ **Secondes**.

Étape 10 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Déployer les changements de configuration.

Sujets connexes

Options de seuil de règle globale, à la page 2
Configuration des règles d'intrusion dans les couches
Conflits et modifications : analyse de réseau et politiques de prévention des intrusions

Désactivation du seuil global

Vous pouvez désactiver la fixation de seuil globale dans la couche de politique la plus élevée si vous souhaitez définir le seuil d'événements pour des règles spécifiques plutôt que d'appliquer le seuil à chaque règle par défaut.

Dans un déploiement multidomaine, le système affiche les politiques créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les politiques créées dans les domaines ancêtres, que vous ne pouvez pas modifier. Pour afficher et modifier les politiques créées dans un domaine inférieur, basculez vers ce domaine.

Procédure

Étape 1 Sélectionner **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 3 Cliquez sur **Advanced Settings** (paramètres avancés) dans le panneau de navigation.

Étape 4 À côté de **Seuil de règle global**, sous **Seuils de règle d'intrusion**, cliquez sur **Désactivé**.

Étape 5 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Déployer les changements de configuration.

Sujets connexes

Conflits et modifications : analyse de réseau et politiques de prévention des intrusions
Configuration des règles d'intrusion dans les couches

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.