

Intégration d'AMP for Endpoints avec Splunk

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Configuration](#)

[Dépannage](#)

Introduction

Ce document décrit le processus d'intégration entre Advanced Malware Protection (AMP) et Splunk.

Contribué par Uriel Islas and Juventino Macias, édité par Jorge Navarrete, Ingénieurs du TAC Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de connaître :

- AMP pour les points terminaux
- API (Application Programming Interface)
- Épingler
- Utilisateur Admin sur Splunk

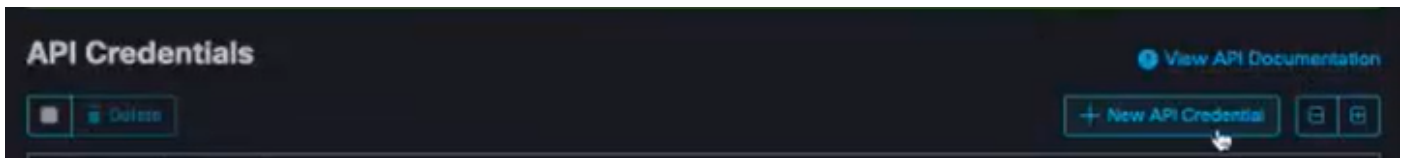
Components Used

- Cloud public AMP
- Instance Splunk

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configuration

Étape 1. Accédez à la console AMP (<https://console.amp.cisco.com>) et accédez à **Comptes>Informations d'identification de l'API**, où vous pouvez créer des flux d'événements.

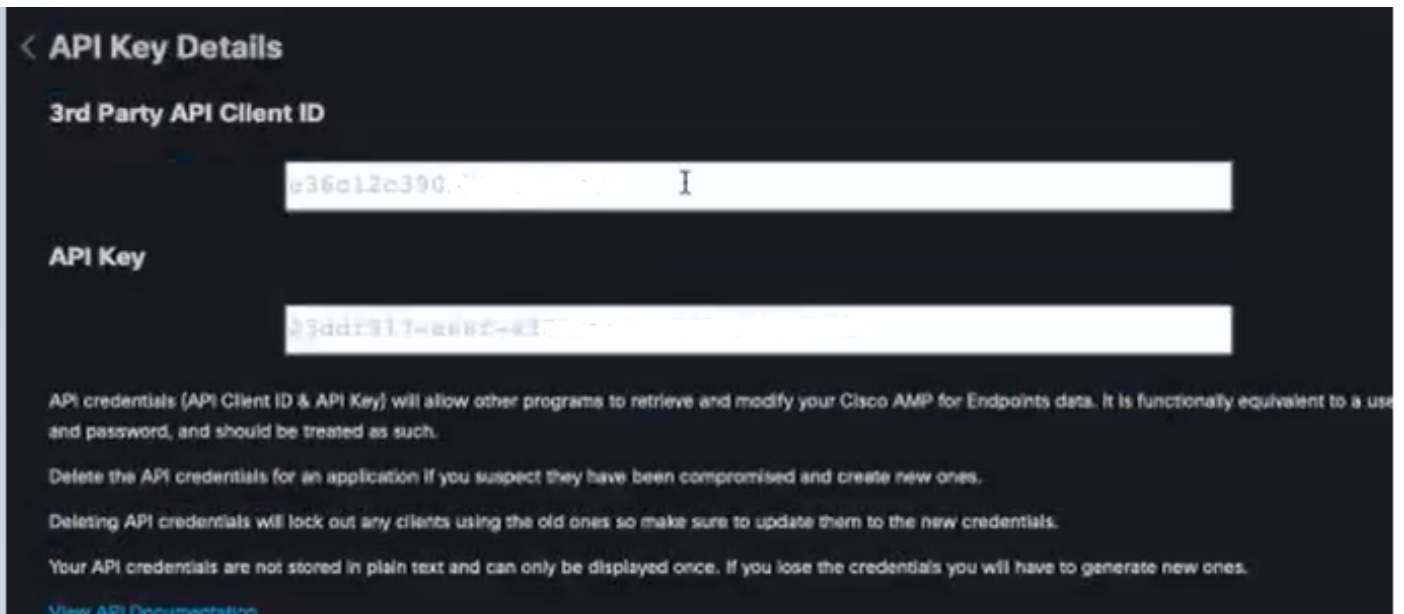


Étape 2. Pour effectuer cette intégration, cochez la case **Lecture et écriture** comme indiqué ci-dessous :



Note: Si vous souhaitez collecter plus d'informations sur les événements, cochez la case **Activer la ligne de commande**, pour obtenir les journaux d'audit générés à partir du référentiel de fichiers, cochez la case **Autoriser l'accès API au référentiel de fichiers**.

Étape 3. Une fois que vous avez créé le flux d'événements, il affiche l'ID de client et la clé d'API requis sur Splunk.

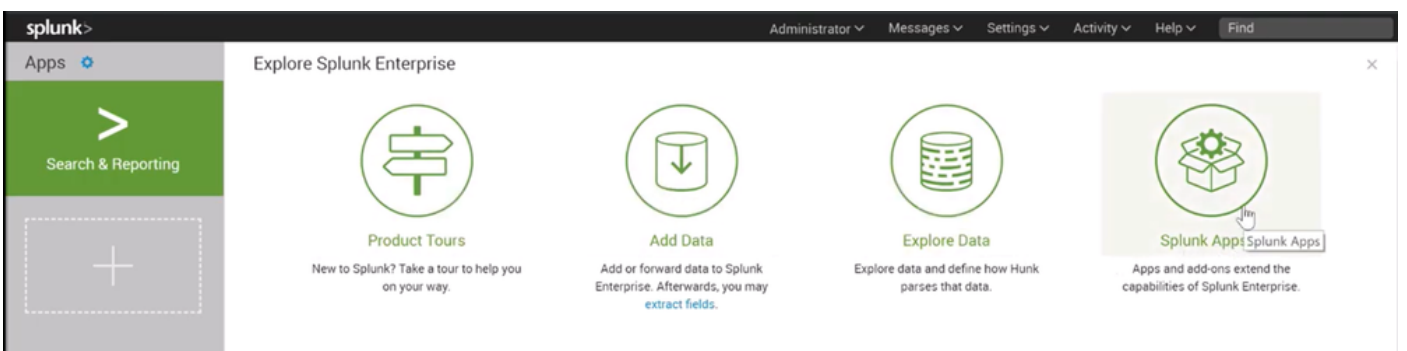


Attention : Ces informations ne peuvent être récupérées par aucun moyen, en cas de perte, une nouvelle clé d'API doit être créée.

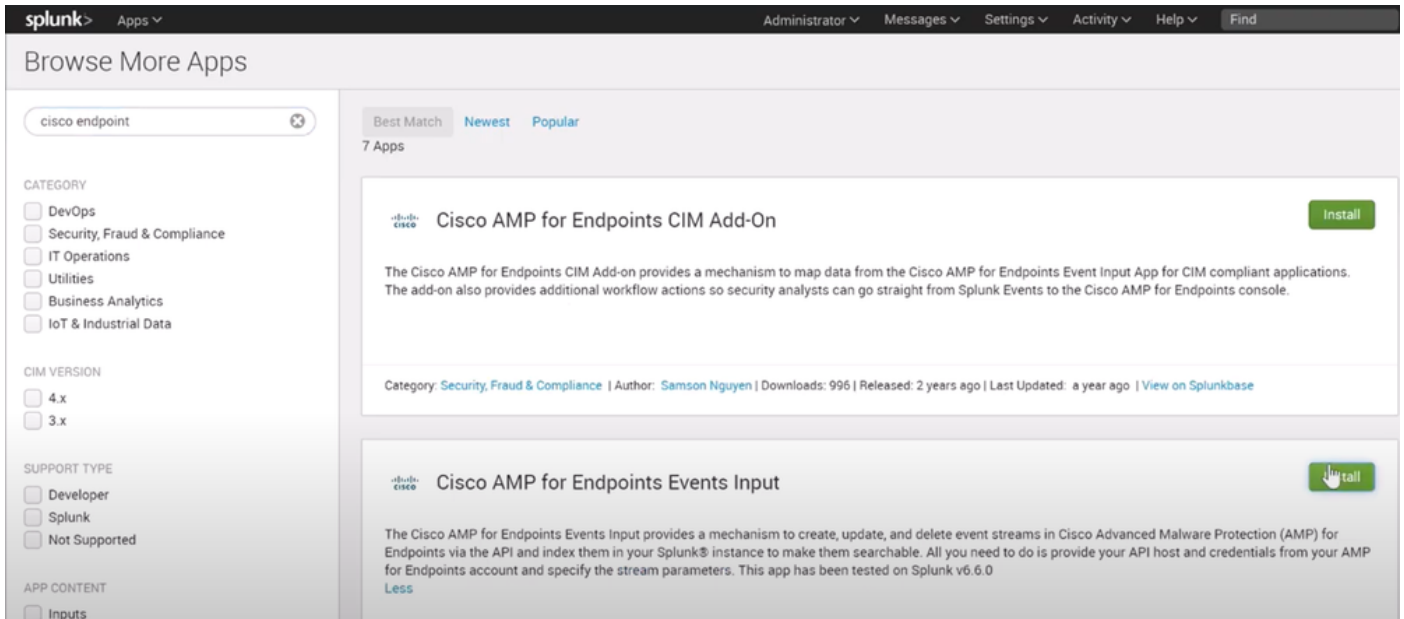
Étape 4. Afin d'intégrer Splunk à AMP pour les terminaux, assurez-vous que l'**administrateur** du compte existe sur Splunk.



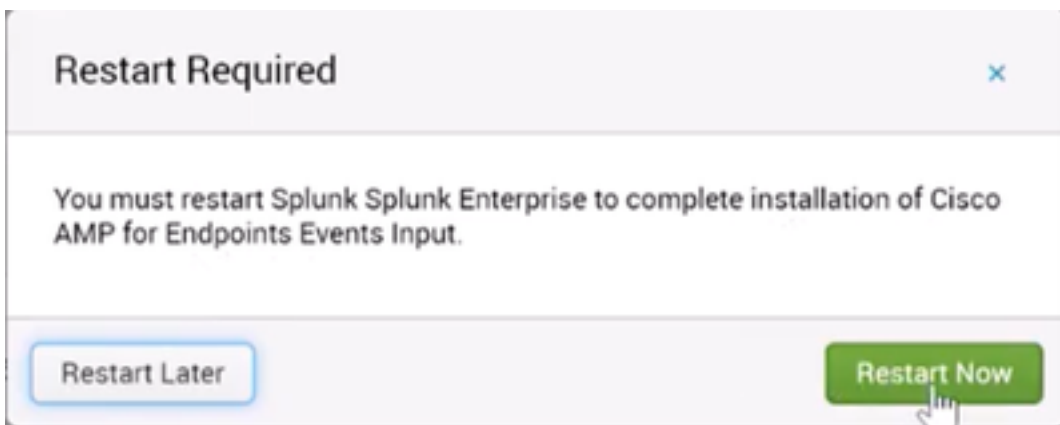
Étape 5. Une fois connecté à Splunk, téléchargez AMP à partir des applications Splunk.



Étape 6. Recherchez Cisco Endpoint sur le navigateur de l'application et installez-le (entrée d'événements Cisco AMP for Endpoints).



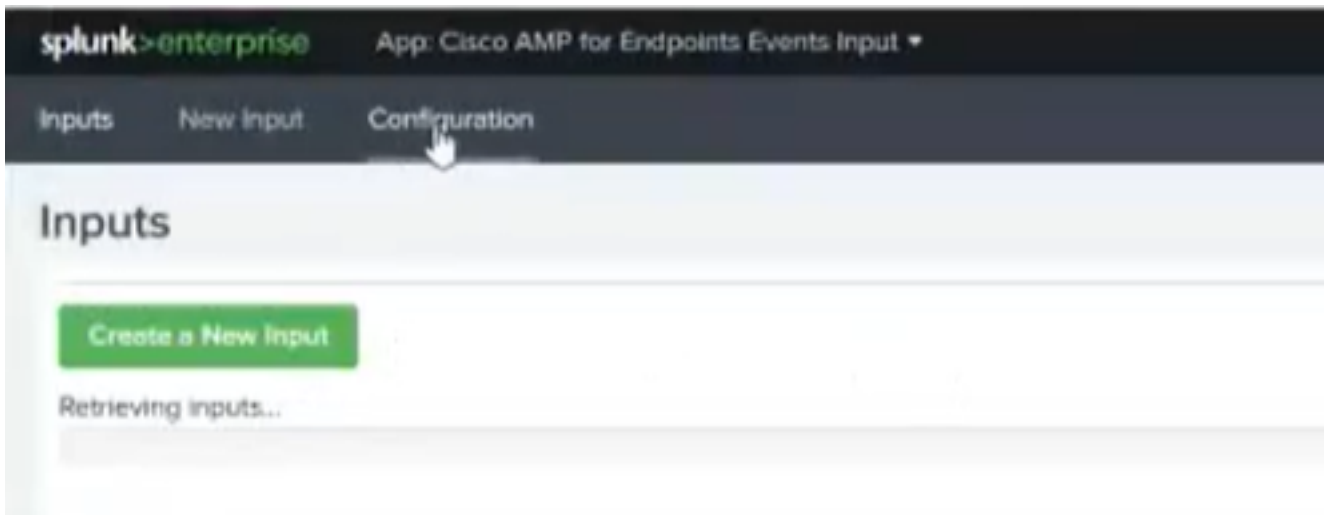
Étape 7. Un redémarrage de la session est nécessaire pour terminer l'installation sur Splunk.



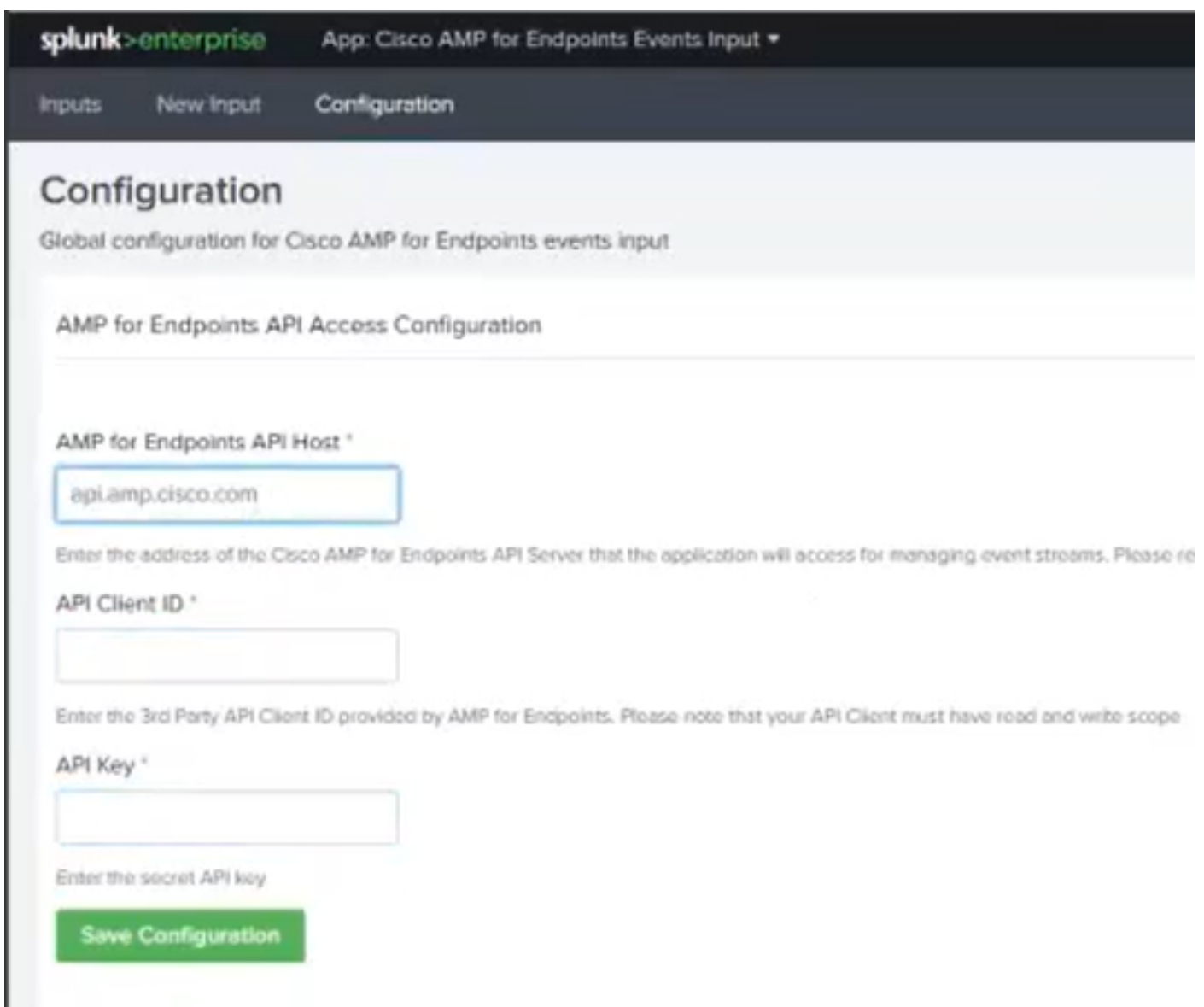
Étape 8. Une fois connecté sous Splunk, cliquez sur **Cisco AMP For Endpoints** sur le côté gauche de l'écran.



Étape 9. Cliquez sur l'étiquette **Configuration** en haut de l'écran.



Étape 10. Tapez vos informations d'identification API précédemment générées à partir de la console AMP.



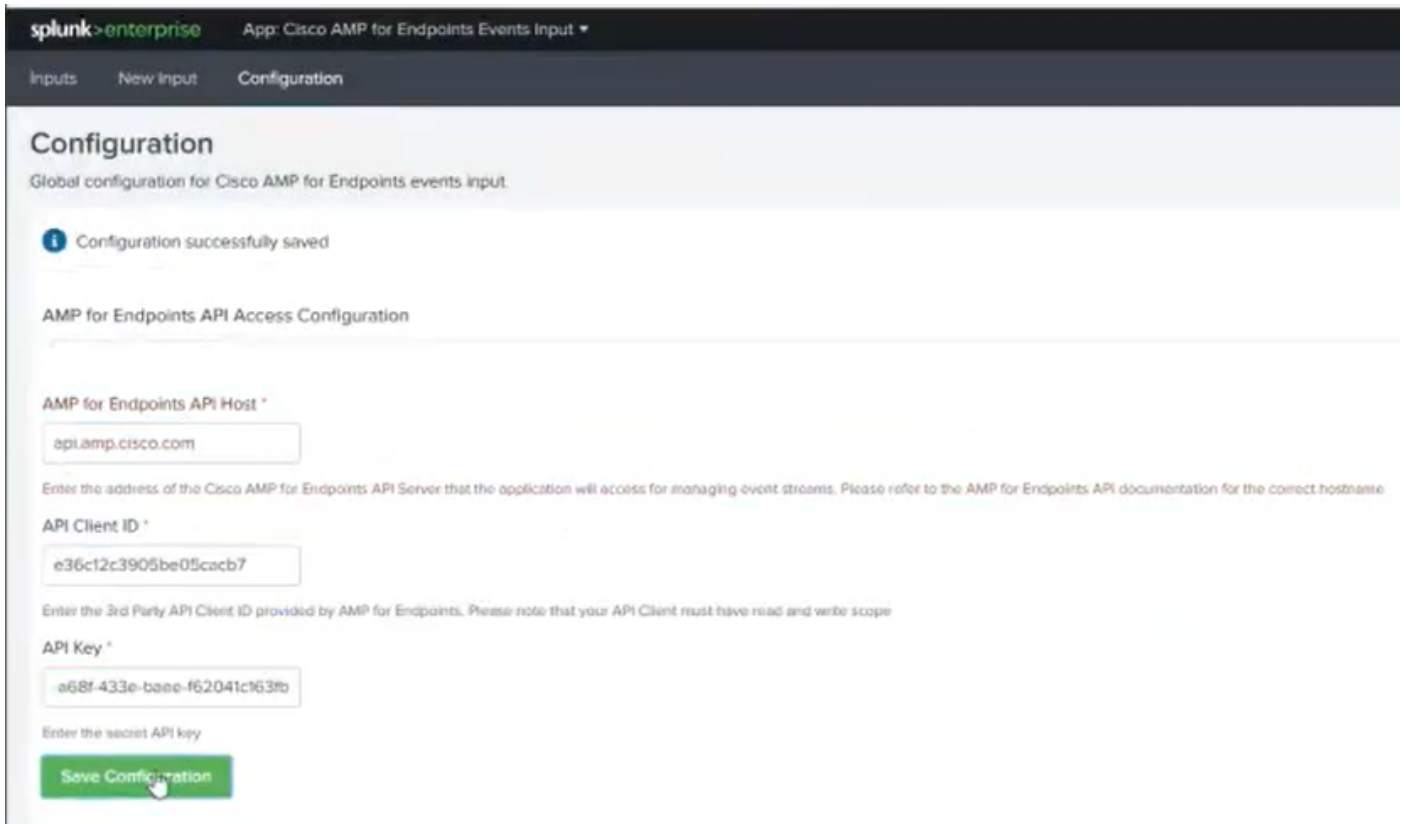
Note: L'emplacement de l'hôte API peut être différent en fonction du data center cloud sur lequel pointe votre entreprise :

Amérique du Nord: `api.amp.cisco.com`

Europe: `api.eu.amp.cisco.com`

APJC: api.apjc.amp.cisco.com

Étape 11. Incluez et enregistrez les informations d'identification API sur la console Splunk pour les lier à AMP.



The screenshot shows the Splunk configuration interface for the 'Cisco AMP for Endpoints Events Input' app. The page title is 'Configuration' and the subtitle is 'Global configuration for Cisco AMP for Endpoints events input'. A notification at the top indicates 'Configuration successfully saved'. The main section is titled 'AMP for Endpoints API Access Configuration'. It contains three input fields: 'AMP for Endpoints API Host *' with the value 'api.amp.cisco.com', 'API Client ID *' with the value 'e36c12c3905be05cabc7', and 'API Key *' with the value 'a68f433e-baee-f62041c163fb'. Below the API Key field is a note: 'Enter the secret API key'. At the bottom, there is a green 'Save Configuration' button.

Étape 12. Revenez à **Entrée** pour créer votre flux d'événements.

Inputs New Input Configuration

New Input

Name *

Index

In which index would you like the events to appear?

Stream Settings

Stream Name *

Event Types

Groups

Note: Si vous voulez obtenir tous les événements pour tous les groupes à partir d'AMP, laissez vides les champs **Types d'événements** et **Groupes**.

Étape 13. Assurez-vous que votre entrée a bien été créée.

Inputs

Name	Index
caissas	main

Note: N'oubliez pas que cette intégration n'est pas officiellement prise en charge

Dépannage

Si, pendant que vous créez un flux d'événements, tous les champs sont grisés, cela peut être dû à certaines des raisons suivantes :

The screenshot shows the 'New Input' configuration page in Splunk. The page is mostly greyed out, indicating a problem. The 'Name' field is disabled with a red prohibition icon. The 'Index' field is set to 'main'. The 'Stream Settings' section is disabled. The 'Stream Name' field is disabled. The 'Event Types' and 'Groups' dropdown menus are also disabled. A green 'Save' button is visible at the bottom left.

1. Problèmes de connectivité: Assurez-vous que l'instance Splunk est en mesure de contacter l'hôte API
2. Hôte API : Assurez-vous que l'hôte API configuré à l'étape 10 correspond à votre organisation AMP, en fonction de l'emplacement de votre entreprise.
3. Informations d'identification de l'API : Assurez-vous que la clé API et l'ID client correspondent à ceux configurés à l'étape 3.
4. Flux d'événements : Vérifiez que moins de 4 flux d'événements sont configurés.