

Module complémentaire Splunk pour ServiceNow - Ne génère aucun incident pour les utilisateurs

Applicabilité

Modules complémentaires des applications Splunk

Description

L'administrateur a pu générer des incidents sur Service Now à l'aide du module complémentaire ServiceNow, mais les utilisateurs n'ont pas pu le faire.

Utilisation du module complémentaire Splunk pour ServiceNow version 3.1 (non pris en charge)
Sur Splunk Search Head Version 7.2.3

Réception du message d'erreur sur snow_ta_ticket.log :

```
2019-07-30 20:00:01,597 ERROR pid=24194 tid=MainThread file=snow_ticket.py:_get_service_account:158 | username=<encrypted>, password=<encrypted>, url=https://something.com
2019-07-30 20:00:01,618 ERROR pid=24194 tid=MainThread file=snow_ticket.py:_get_service_account:162 | url=https://something.com, app=Splunk_TA_snow
2019-07-30 20:00:01,618 ERROR pid=24194 tid=MainThread file=snow_ticket.py:_get_service_account:165 | Failed to get clear credentials for https://something.com
```

Enquête

Double vérifié l'installation et la configuration de SNOW ;

- En commençant par le côté neige :

1. Connectez-vous à votre instance Snow.
2. Vous pouvez installer l'application à partir du Service Now Store ou
3. Lorsque vous téléchargez le Splunk_TA_snow et que vous le décompressez, accédez au fichier et vous verrez un autre fichier appelé forExport (ce sont des ensembles de mises à jour de Service Now)

- Ce sont les mécanismes que Snow utilise pour ajouter des fonctionnalités, effectuer des sauvegardes et des restaurations.
4. Nous allons l'utiliser pour configurer Snow pour communiquer avec Splunk.
 5. Prends le dernier.
 6. Retournez à votre instance et cliquez sur Mettre à jour (ou récupérer des jeux de mises à jour).
 7. Puis cliquez sur le jeu d'importation à partir du xml, choisissez fichier et sélectionnez le fichier que vous avez saisi avant.
 8. Cliquez ensuite sur Télécharger. Cette opération peut prendre quelques secondes.
 9. Ensuite, ouvrez le jeu de mises à jour en cliquant sur Intégration de Splunk.
 10. Cliquez sur « Aperçu du jeu de mises à jour ». Ne vous inquiétez pas si vous avez des erreurs à ce stade.
 11. Fermez la fenêtre. Et vérifiez ce qui échoue. Sélectionnez tous les messages a et acceptez-les en cliquant sur "actions sur les lignes sélectionnées"
 12. Cliquez ensuite sur « Valider le jeu de mises à jour »
 13. Nous devons ajouter l'utilisateur qui va communiquer le Splunk avec le service maintenant.
 14. Ainsi, si vous n'êtes pas connecté en tant qu'administrateur sur votre compte Service Now, vous devez élever votre rôle à security_admin (il vous suffit de cliquer sur l'onglet Utilisateur et de sélectionner « élever les rôles »)
 15. Dans la barre de recherche à gauche de l'écran, tapez : Administrateur utilisateur. Vous allez maintenant accéder à l'administration des utilisateurs.
 16. Cliquez sur Utilisateurs/nouveaux utilisateurs et créez l'utilisateur et le mot de passe pour cet utilisateur.
 - Assurez-vous que le mot de passe respecte les contraintes de complexité.
 - Assurez-vous que les cases « Active » et « Internal integration user » sont cochées.
 17. Sous l'option Rôles, cliquez sur « Modifier »
 18. Sélectionnez le rôle x_splu2_splunk_ser.Splunk
 19. Garde-le.

C'est à peu près la configuration dont nous avons besoin du côté de la NEIGE.

Maintenant, nous devons installer l'application sur Splunk comme toute autre application.

1. Redémarrez Splunk après avoir installé l'application.
2. Accéder à l'application
3. Saisissez l'URL de votre instance Snow pour l'utilisateur que vous avez créé sur Snow et son mot de passe, puis enregistrez la configuration.
 - Si vous n'obtenez aucun message d'erreur pendant ce processus, cela signifie que la connexion a réussi.
4. Accédez aux applications et recherchez SNOW
5. Cliquez sur "Afficher les objets"

Vous constaterez que certaines recherches ne sont pas activées. Activez celui dont vous avez besoin.

Et vérifiez si cela fonctionne :

1. Accédez à l'application Snow.
2. L'onglet « intégration des incidents de service maintenant » doit s'afficher dans la zone « Actions ».

L'utilisateur doit disposer d'autorisations de lecture et d'écriture sur l'application.

Nous pourrions enregistrer un incident en tant qu'administrateur sur Snow en utilisant cette requête :

```
|snowincident --category "Network" --short_description "testing search" --contact_type "email" --urgency "3" --subcategory "intranet" --state "1" --location "Hawaii" --impact --priority "5" --assignment_group "network" --opened_by "ME" --ci_identifier "1234567" --comments "these are Don's comments" --splunk_url "www.splunk.com" --correlation_id "12
```

Mais nous n'avons pas pu le générer en utilisant un autre utilisateur.

Nous recevions ce message d'erreur sur snow_ta_ticket.log :

```
2019-07-30 20:00:01,597 ERROR pid=24194 tid=MainThread file=snow_ticket.py:_get_service_account:158 | username=<encrypted>, password=<encrypted>, url=https://something.com
2019-07-30 20:00:01,618 ERROR pid=24194 tid=MainThread file=snow_ticket.py:_get_service_account:162 | url=https://something.com, app=Splunk_TA_snow
2019-07-30 20:00:01,618 ERROR pid=24194 tid=MainThread file=snow_ticket.py:_get_service_account:165 | Failed to get clear credentials for https://something.com
```

Résolution

Nous avons donc ajouté cette fonctionnalité au rôle d'utilisateur :

```
list_storage_passwords
```

Après cela, l'utilisateur a pu créer des incidents sur SNOW.

Nous l'avons testé avec cette requête :

```
index=servicenow_eo sourcetype="snow:incident" "Splunk provided the following enrichment information" | table number, short_description, dv_state, dv_cmdb_ci, dv_assignment_grou
```

dv_opened_at | sort dv_state

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.