

Splunk Add-on für ServiceNow - Keine Incident-Generierung für Benutzer

Geltungsbereich

Splunk-Apps-Add-ons

Beschreibung

Der Administrator konnte mithilfe des ServiceNow-Add-Ons Vorfälle für Service Now generieren, die Benutzer konnten dies jedoch nicht tun.

Verwenden des Splunk-Add-Ons für ServiceNow Version 3.1 (nicht mehr unterstützt)
Auf Splunk-Suchkopf Version 7.2.3

Empfang der Fehlermeldung auf 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
```

Untersuchung

Doppelte Überprüfung der Installation und Konfiguration von SNOW;

- Start auf der Schneeseite:

1. Melden Sie sich bei Ihrer Snow-Instanz an.
2. Sie können die App im Service Now Store installieren oder
3. Wenn Sie Splunk_TA_snow herunterladen und entpacken, greifen Sie auf die Datei zu und sehen eine weitere Datei namens forExport (dies sind Service Now Updates Sets)
 - Dies sind die Mechanismen, die Snow verwendet, um Funktionen hinzuzufügen, Backups zu erstellen und wiederherzustellen.
4. Wir werden dies verwenden, um Snow für die Kommunikation mit Splunk einzurichten.

5. Schnapp dir die neueste.
6. Kehren Sie zu Ihrer Instanz zurück und klicken Sie auf Update (oder rufen Sie Update Sets ab).
7. Klicken Sie dann auf Import Set aus XML, wählen Sie eine Datei und wählen Sie die Datei, die Sie zuvor erfasst haben.
8. Klicken Sie dann auf "Hochladen". Dies kann einige Sekunden dauern.
9. Öffnen Sie dann das Update-Set, indem Sie auf Splunk-Integration klicken.
10. Klicken Sie auf "Vorschau Update Set". Mach dir keine Sorgen, wenn du an diesem Punkt Fehler bekommst.
11. Schließen Sie das Fenster. Überprüfen Sie, was fehlschlägt. Wählen Sie alle Nachrichten aus und akzeptieren Sie sie, indem Sie auf "Aktionen für ausgewählte Zeilen" klicken.
12. Dann klicke auf "Commit the update Set"
13. Wir müssen den Benutzer hinzufügen, der Splunk mit Service Now kommunizieren wird.
14. Wenn Sie also nicht als Administrator in Ihrem Service Now-Konto angemeldet sind, müssen Sie Ihre Rolle auf security_admin erweitern (klicken Sie einfach auf die Registerkarte "Benutzer" und wählen Sie "Rollen erweitern").
15. Geben Sie in der Suchleiste auf der linken Seite Ihres Bildschirms Folgendes ein: Benutzer-Administrator Dadurch gelangen Sie zur Benutzerverwaltung.
16. Klicken Sie auf Benutzer/neue Benutzer, und erstellen Sie den Benutzer und das Kennwort für diesen Benutzer.
 - Stellen Sie sicher, dass das Kennwort die Komplexitätseinschränkungen erfüllt.
 - Stellen Sie sicher, dass die Kontrollkästchen "Active" (Aktiv) und "Internal integration user" (Interne Integration) aktiviert sind.
17. Klicken Sie unter der Option Rollen auf "Bearbeiten".
18. Wählen Sie die Rolle x_splu2_splunk_ser.Splunk aus
19. Speichern.

Das ist so ziemlich die Konfiguration, die wir auf der SNOW-Seite brauchen.

Jetzt müssen wir die App auf Splunk wie jede andere App zu installieren.

1. Starten Sie Splunk nach der Installation der App neu.
2. Zur App wechseln
3. Legen Sie die URL für Ihre Snow-Instanz, den Benutzer, den Sie auf Snow erstellt haben, und sein Passwort und speichern Sie die Konfiguration.
 - Wenn Sie während dieses Vorgangs keine Fehlermeldung erhalten, bedeutet dies, dass die Verbindung erfolgreich hergestellt wurde.
4. Gehen Sie zu apps und suchen SNOW
5. Klicken Sie auf "Objekte anzeigen".

Sie werden sehen, dass einige Suchvorgänge nicht aktiviert sind. Aktivieren Sie das Gerät, das Sie benötigen.

Und überprüfen Sie, ob es funktioniert:

1. Rufen Sie die Schnee-App auf.
2. Unter "Aktionen" sollte die Registerkarte "servicenow Incident Integration" angezeigt

werden.

Der Benutzer muss über Lese- und Schreibberechtigungen für die App verfügen.

Mit dieser Abfrage könnten wir einen Vorfall als Administrator bei Snow protokollieren:

```
|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
```

Sie konnten jedoch nicht mit einem anderen Benutzer generiert werden.

Wir erhielten diese Fehlermeldung auf 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
```

Auflösung

Daher fügten wir diese Funktion der Benutzerrolle hinzu:

```
list_storage_passwords
```

Danach konnte der Benutzer Vorfälle im SNOW erstellen.

Wir haben es mit dieser Abfrage getestet:

```
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
```


Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.