

# ServiceNow用Splunkアドオン – ユーザのインシデントを生成しない

## 適用性

Splunkアプリケーションアドオン

## 説明

管理者はServiceNowアドオンを使用してService Nowでインシデントを生成できましたが、ユーザはこれを実行できませんでした。

ServiceNowバージョン3.1用Splunkアドオンの使用 ( サポート終了 )  
Splunk Search Headバージョン7.2.3上

snow\_ta\_ticket.logで次のエラーメッセージを受信しています。

```
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
```

## 調査

SNOWのインストールと設定を再度チェックします。

– 雪面から :

1. Snowインスタンスにログインします。
2. Service Now Storeからアプリをインストールするか、
3. Splunk\_TA\_snowをダウンロードして解凍すると、ファイルにアクセスしてforExportという別のファイルが表示されます ( これらはService Nowアップデートセットです )
  - これらは、Snowが機能を追加し、バックアップと復元を行うために使用するメカニズムです。
4. これを使用して、SnowでSplunkとの通信を設定します。

5. 最新のものを入手してください。
6. インスタンスに戻り、「更新」(または「更新セットを読み込み」)をクリックします。
7. 次に、xmlからセットをインポートをクリックし、ファイルを選択し、以前に取得したファイルを選択します。
8. 次に、uploadをクリックします。これには数秒かかることがあります。
9. 次に、Splunk統合をクリックしてアップデートセットを開きます。
10. 「プレビュー更新セット」をクリックしてください。この時点でエラーが発生しても心配する必要はありません。
11. ウィンドウを閉じます。失敗した内容を確認します。すべてのメッセージを選択し、「選択した行のアクション」をクリックして受け入れます
12. 次に、「アップデートセットを確定」をクリックします。
13. Splunk with Service Nowと通信するユーザを追加する必要があります。
14. そのため、Service Nowアカウントで管理者としてログインしていない場合は、ロールを security\_adminに昇格させる必要があります(ユーザタブをクリックして「ロールの昇格」を選択するだけです)
15. 画面の左側にある検索バーに「User admin」と入力します。これにより、ユーザ管理に移動します。
16. ユーザ/新規ユーザをクリックし、このユーザのユーザとパスワードを作成します。
  - ・ パスワードが複雑さの制約を満たしていることを確認します。
  - ・ [Active]および[Internal integration user]ボックスがオンになっていることを確認します
17. Rolesオプションの下で、「edit」をクリックします。
18. ロールx\_splu2\_splunk\_ser.Splunkを選択します。
19. 保存します。

これはSNOW側で必要な設定です。

次に、他のアプリケーションと同様にSplunkにアプリケーションをインストールする必要があります。

1. アプリケーションのインストール後にSplunkを再起動します。
2. アプリに移動
3. SnowインスタンスのURLと、Snowで作成したユーザのパスワードを入力し、設定を保存します。
  - ・ このプロセス中にエラーメッセージが表示されない場合は、接続が成功したことを意味します。
4. アプリに移動してSNOWを探す
5. 「オブジェクトの表示」をクリックします。

一部の検索が有効になっていないことがわかります。必要なオプションを有効にします。

次のように動作するかどうかを確認します。

1. Snow Appに移動します。
2. 「Actions」に「servicenow incident integration」タブが表示されます。

ユーザーは、アプリに対する読み取り権限と書き込み権限を持っている必要があります。

次のクエリを使用して、Snowの管理者としてインシデントをログに記録できます。

```
|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
```

しかし、別のユーザーを使用して生成できませんでした。

snow\_ta\_ticket.logに次のエラーメッセージが表示されました。

```
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
```

## 解決方法

この機能をユーザロールに追加しました。

```
list_storage_passwords
```

その後、ユーザはSNOWでインシデントを作成することができました。

次のクエリを使用してテストしました。

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

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。