

Splunk Add-on for ServiceNow — 不為使用者生成事件

適用性

Splunk應用載入項

說明

管理員可以使用ServiceNow載入項在Service Now上生成事件，但使用者無法執行此操作。

使用用於ServiceNow 3.1版的Splunk載入項（不再支援）
Splunk搜尋頭版本7.2.3

在snow_ta_ticket.log上收到錯誤消息：

```
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
```

調查

再次檢查SNOW的安裝和配置；

— 從雪的一面開始：

1. 登入您的Snow例項。
2. 您可以從Service Now應用商店安裝應用，或者
3. 當您下載Splunk_TA_snow並解壓縮它時，訪問該檔案，您將看到另一個名為forExport的檔案（這些是Service Now更新集）
 - 這些是Snow用於新增功能、執行備份和還原的機制。
4. 我們將利用這個來建立Snow與Splunk的通訊。
5. 拿上最新的一個。
6. 返回您的例項，然後按一下更新（或檢索更新集）。

7. 然後按一下「從xml匯入集」，選擇「檔案」並選擇之前捕獲的檔案。
8. 然後按一下上傳。這可能需要幾秒鐘。
9. 然後，通過按一下Splunk整合開啟更新集。
10. 按一下「預覽更新集」。如果此時遇到一些錯誤，不必擔心。
11. 關閉視窗。檢查哪些失敗。選擇所有消息，然後按一下「對選定行執行的操作」接受這些消息
12. 然後按一下「提交更新集」
13. 我們需要新增要與Service Now通訊Splunk的使用者。
14. 因此，如果您沒有以管理員身份登入您的Service Now帳戶，則必須將您的角色提升為 security_admin (只需按一下「使用者」頁籤並選擇「提升角色」)
15. 在螢幕左側的搜尋欄上鍵入：User admin。這將帶您進入使用者管理。
16. 按一下使用者/新使用者，然後為此使用者建立使用者和密碼。
 - 確保密碼符合複雜性限制。
 - 確保選中「活動」和「內部整合使用者」框。
17. 在「角色」選項下，按一下「編輯」
18. 選擇角色x_splu2_splunk_ser.Splunk
19. 省省吧。

這差不多就是雪地方面需要的配置了。

現在，我們需要像任何其他應用一樣在Splunk上安裝該應用。

1. 安裝應用後重新啟動Splunk。
2. 轉到應用
3. 將您在Snow上建立的使用者Snow例項的URL及其密碼並儲存配置。
 - 如果您在此過程中未收到任何錯誤消息，則表示連線成功。
4. 轉到應用並查詢SNOW
5. 按一下「檢視對象」

您將看到某些搜尋未啟用。啟用您需要的裝置。

並檢查其是否有效：

1. 轉到Snow App。
2. 在「操作」上，您應該會看到「servicenow事件整合」頁籤。

使用者必須擁有對應用的讀取和寫入許可權。

我們可以使用此查詢在Snow上以管理員身份記錄事件：

```
|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
```

但我們無法使用其他使用者生成它。

我們在 snow_ta_ticket.log 上收到以下錯誤消息：

```
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
```

解析

因此，我們將該功能新增到使用者角色中：

```
list_storage_passwords
```

執行此操作後，使用者能夠在 SNOW 上建立事件。

我們使用以下查詢對其進行測試：

```
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
```

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。