

ServiceNow용 Splunk 추가 기능 - 사용자에게 대한 인시던트 생성 안 함

적용 가능성

Splunk Apps 추가 기능

설명

관리자가 ServiceNow 추가 기능을 사용하여 ServiceNow에서 인시던트를 생성할 수 있었지만 사용자가 이를 수행할 수 없었습니다.

ServiceNow 버전 3.1용 Splunk 추가 기능 사용(더 이상 지원되지 않음)
Splunk Search Head 버전 7.2.3

snow_ta_ticket.log에서 오류 메시지 수신 중:

```
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
```

조사

SNOW의 설치 및 구성을 다시 확인했습니다.

- 스노우 사이트에서 시작:

1. Snow 인스턴스에 로그인합니다.
2. Service Now Store 또는
3. Splunk_TA_snow를 다운로드하고 압축을 풀면 파일에 액세스하면 forExport라는 다른 파일이 표시됩니다(Service Now 업데이트 세트).
 - 이러한 메커니즘은 Snow가 백업 및 복원 기능을 추가하기 위해 사용하는 메커니즘입니다.
4. 우리는 이것을 스켈크와 소통할 수 있는 스노우를 세팅하기 위해 사용할 것입니다.

5. 가장 최근의 것을 잡으세요.
6. 인스턴스로 돌아가 update(업데이트) 또는 retrieve Update Sets(업데이트 세트 검색)를 클릭합니다.
7. 그런 다음 import set from xml(xml에서 가져오기 세트)을 클릭하고 file(파일)을 선택한 다음 전에 가져온 파일을 선택합니다.
8. 그런 다음 업로드를 클릭합니다. 몇 초 정도 걸릴 수 있습니다.
9. 그런 다음 Splunk integration(Splunk 통합)을 클릭하여 업데이트 세트를 엽니다.
10. "Preview Update set(업데이트 세트 미리보기)"를 클릭합니다. 이 시점에서 약간의 오류가 발생하더라도 걱정하지 마십시오.
11. 창을 닫습니다. 그리고 무엇이 실패했는지 확인하세요. 모든 메시지를 선택하고 "선택한 행의 작업"을 클릭하여 수락합니다.
12. 그런 다음 "Commit the update Set(업데이트 세트 커밋)"를 클릭합니다.
13. Splunk with Service Now와 통신할 사용자를 추가해야 합니다.
14. 따라서 Service Now 계정에 관리자로 로그인하지 않은 경우, 역할을 security_admin으로 승격해야 합니다(사용자 탭을 클릭하고 "역할 승격"을 선택하면 됨).
15. 화면 왼쪽의 검색 표시줄에 다음을 입력합니다. 사용자 관리자. 이렇게 하면 사용자 관리로 이동합니다.
16. 사용자/새 사용자를 클릭하고 이 사용자의 사용자 및 암호를 만듭니다.
 - 비밀번호가 복잡성 제약 조건을 충족하는지 확인합니다.
 - "Active(활성)" 및 "Internal integration user(내부 통합 사용자)" 상자가 선택되어 있는지 확인합니다.
17. Roles(역할) 옵션에서 "edit(수정)"를 클릭합니다.
18. x_splu2_splunk_ser.Splunk 역할 선택
19. 아껴

그것은 우리가 SNOW 측면에서 필요로 하는 거의 모든 구성입니다.

이제 다른 앱처럼 Splunk에 앱을 설치해야 합니다.

1. 앱을 설치한 후 Splunk를 다시 시작합니다.
2. 앱으로 이동
3. Snow에서 생성한 Snow 인스턴스의 URL과 비밀번호를 입력하고 컨피그레이션을 저장합니다.
 - 이 프로세스 중에 오류 메시지가 표시되지 않으면 연결이 성공했음을 의미합니다.
4. 앱으로 이동하여 SNOW 검색
5. "view objects(개체 보기)"를 클릭합니다.

일부 검색이 활성화되지 않은 것을 확인할 수 있습니다. 필요한 기능을 활성화합니다.

작동 여부를 확인합니다.

1. 스노우 앱으로 이동합니다.
2. "Actions(작업)"에 "servicenow incident integration(서비스 수준 인시던트 통합)" 탭이 표시됩니다.

사용자에게 앱에 대한 읽기 및 쓰기 권한이 있어야 합니다.

다음 쿼리를 사용하여 Snow에 대한 관리자로 인시던트를 기록할 수 있습니다.

```
|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
```

하지만 다른 사용자를 사용하여 생성할 수 없습니다.

snow_ta_ticket.log에서 이 오류 메시지를 수신했습니다.

```
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
```

해결

따라서 이 기능을 사용자 역할에 추가했습니다.

```
list_storage_passwords
```

그렇게 한 후 사용자는 SNOW에서 인시던트를 생성할 수 있었습니다.

다음 쿼리로 테스트했습니다.

```
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
```

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.