

Splunk-invoegtoepassing voor ServiceNow - Geen incident genereren voor gebruikers

toepasbaarheid

Splunk Apps-add-ons

Beschrijving

De beheerder kon incidenten genereren op Service Now met behulp van de ServiceNow-invoegtoepassing, maar gebruikers konden dit niet doen.

Splunk-invoegtoepassing gebruiken voor ServiceNow versie 3.1 (niet langer ondersteund)
Op Splunk Search Head versie 7.2.3

Foutbericht ontvangen op 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
```

onderzoek

Dubbel gecontroleerd op de installatie en configuratie van SNOW;

- Beginnend aan de sneeuwkant:

1. Log in op uw Snow-exemplaar.
2. U kunt de app installeren vanuit de Service Now Store of
3. Wanneer u de Splunk_TA_snow downloadt en Unzip, opent u het bestand en ziet u een ander bestand met de naam Export (dit zijn Service Now-updates sets)
 - Dit zijn de mechanismen die Snow gebruikt om functionaliteit toe te voegen, om back-ups te maken en te herstellen.
4. We zullen dit gebruiken om Snow in te stellen om met Splunk te communiceren.

5. Pak de nieuwste.
6. Ga terug naar uw exemplaar en klik op Bijwerken (of Update Sets ophalen).
7. Klik vervolgens op de importset van xml, kies het bestand en selecteer het bestand dat u eerder hebt gepakt.
8. Klik vervolgens op uploaden. Dit kan enkele seconden duren.
9. Open vervolgens de updateset door op Splunk-integratie te klikken.
10. Klik op "Preview Update set". Maak je geen zorgen als je op dit moment fouten maakt.
11. Sluit het raam. Check wat mislukt. Selecteer alle berichten en accepteer ze door te klikken op "Acties op geselecteerde rijen"
12. Klik vervolgens op "Commit the update set"
13. We moeten de gebruiker toevoegen die gaat communiceren met Splunk Service Now.
14. Dus als u niet bent ingelogd als beheerder op uw Service Now-account, moet u uw rol naar security_admin verhogen (klik op het tabblad Gebruiker en selecteer "rollen verhogen")
15. In de zoekbalk aan de linkerkant van het scherm typt u: User admin. Dit brengt u naar de gebruikersadministratie.
16. Klik op gebruikers/nieuwe gebruikers en maak de gebruiker en het wachtwoord voor deze gebruiker.
 - Zorg ervoor dat het wachtwoord voldoet aan de complexiteitsvereisten.
 - Zorg ervoor dat de vakjes "Actieve" en "Interne integratie gebruiker" zijn aangevinkt.
17. Klik onder de optie Rollen op "bewerken"
18. Selecteer de rol x_splu2_splunk_ser.Splunk
19. Bewaar het.

Dat is zo'n beetje de configuratie die we nodig hebben aan de SNEEUWKANT.

Nu moeten we de app op Splunk installeren zoals elke andere app.

1. Start Splunk opnieuw na het installeren van de app.
2. Ga naar de app
3. Plaats de URL voor uw Snow-instantie, de gebruiker die u op Snow hebt gemaakt en zijn wachtwoord en sla de configuratie op.
 - Als u tijdens dit proces geen foutmelding krijgt, betekent dit dat de verbinding succesvol was.
4. Ga naar apps en zoek naar SNEEUW
5. Klik op "Objecten bekijken"

U zult zien dat sommige zoekopdrachten niet zijn ingeschakeld. Schakel degene in die je nodig hebt.

Controleer of het werkt:

1. Ga naar de Snow App.
2. Op "Acties" moet u het tabblad "service now incident integration" zien.

De gebruiker moet lees- en schrijfrechten hebben op de app.

We kunnen een incident registreren als beheerder op Snow met behulp van deze query:

```
|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
```

Maar we konden het niet genereren met een andere gebruiker.

We kregen dit foutbericht op 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
```

resolutie

Daarom hebben we deze mogelijkheid toegevoegd aan de gebruikersrol:

```
list_storage_passwords
```

Daarna kon de gebruiker incidenten op SNEEUW maken.

We hebben het getest met deze vraag:

```
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
```

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.