

Splunk Add-on per ServiceNow - Nessuna generazione di eventi imprevisti per gli utenti

Applicabilità

Componenti aggiuntivi applicazioni Splunk

Descrizione

L'amministratore è stato in grado di generare richieste di supporto in Service Now utilizzando il componente aggiuntivo ServiceNow, ma gli utenti non sono stati in grado di farlo.

Utilizzo del componente aggiuntivo Splunk per ServiceNow versione 3.1 (non più supportato)
Su Splunk Search Head versione 7.2.3

Ricezione del messaggio di errore in 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
```

Indagine

ha controllato due volte l'installazione e la configurazione di SNOW;

- Partendo dalla neve:

1. Accedere all'istanza di Snow.
2. È possibile installare l'app da Service Now Store o
3. Quando si scarica Splunk_TA_snow e lo si decompone, accedere al file e viene visualizzato un altro file denominato forExport (questi sono set di aggiornamenti di Service Now)
 - Questi sono i meccanismi che Snow utilizza per aggiungere funzionalità, eseguire backup e ripristinare.
4. Useremo questo per impostare Snow per comunicare con Splunk.

5. Prendete l'ultima.
6. Tornate alla vostra variante e fate clic su aggiorna (update) o recupera insiemi di aggiornamenti (retrieve Update Sets).
7. Quindi fare clic su set di importazione da xml, scegliere file e selezionare il file che si è afferrato prima.
8. Quindi fai clic su Carica. L'operazione potrebbe richiedere alcuni secondi.
9. Aprire quindi il set di aggiornamenti facendo clic su Integrazione con splunk.
10. Fare clic su "preview Update set". Non preoccuparti se ci sono degli errori a questo punto.
11. Chiudete la finestra. E controlla cosa non va. Selezionare tutti i messaggi a e accettarli facendo clic su "azioni sulle righe selezionate"
12. Quindi fare clic su "Commit the update Set"
13. È necessario aggiungere l'utente che comunicherà Splunk con Service Now.
14. Pertanto, se non si è connessi come amministratore con l'account Service Now, è necessario elevare il proprio ruolo a security_admin. È sufficiente fare clic sulla scheda utente e selezionare "elevare i ruoli".
15. Sulla barra di ricerca a sinistra dello schermo digitare: Amministratore utenti. Verrà visualizzata la pagina Amministrazione utenti.
16. Fare clic su utenti/nuovi utenti e creare l'utente e la relativa password.
 - Assicurarsi che la password soddisfi i vincoli di complessità.
 - Assicurarsi che le caselle "Attivo" e "Utente integrazione interna" siano selezionate.
17. Sotto l'opzione Ruoli fare clic su "modifica"
18. Selezionare il ruolo x_splu2_splunk_ser.Splunk
19. Salvatela.

Questa è più o meno la configurazione di cui abbiamo bisogno sul lato NEVE.

Ora dobbiamo installare l'app su Splunk come qualsiasi altra app.

1. Riavviare Splunk dopo aver installato l'app.
2. Vai all'app
3. Inserire l'URL per la tua istanza di Snow l'utente che hai creato su Snow e la sua password e salvare la configurazione.
 - Se non viene visualizzato alcun messaggio di errore durante il processo, significa che la connessione è riuscita.
4. Vai alle app e cerca SNOW
5. Fare clic su "visualizza oggetti".

Alcune ricerche non sono attivate. Abilitare quello necessario.

E verificare se funziona:

1. Vai alla Snow App.
2. In "Azioni" dovrebbe essere visualizzata la scheda "integrazione richiesta di assistenza servicenow".

L'utente deve disporre delle autorizzazioni di lettura e scrittura per l'app.

Possiamo registrare un incidente come amministratore su Snow utilizzando questa 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
```

Ma non è stato possibile generarlo usando un altro utente.

È stato ricevuto questo messaggio di errore in 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
```

Risoluzione

È stata quindi aggiunta questa funzionalità al ruolo utente:

```
list_storage_passwords
```

Dopo aver fatto questo l'utente è stato in grado di creare incidenti su SNOW.

L'abbiamo testata con questa domanda:

```
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
```

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).