

Splunk Add-on for ServiceNow - No genera incidentes para los usuarios

Aplicabilidad

Complementos de aplicaciones Splunk

Descripción

El administrador ha podido generar incidentes en Service Now con el complemento ServiceNow, pero los usuarios no han podido hacerlo.

Uso del complemento Splunk para la versión 3.1 de ServiceNow (ya no se admite)

Encabezado de búsqueda en Splunk versión 7.2.3

Recibiendo mensaje de error en 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
```

Investigación

Se comprobó dos veces la instalación y configuración de SNOW;

- Empezando por el lado de la nieve:

1. Inicie sesión en su instancia de Snow.
2. Puede instalar la aplicación desde la Tienda Service Now o
3. Al descargar Splunk_TA_snow y descomprimirlo, acceda al archivo y verá otro archivo llamado forExport (estos son conjuntos de actualizaciones de Servicio Ahora)
 - Estos son los mecanismos que utiliza Snow para agregar funcionalidad, hacer copias de seguridad y restaurar.
4. Usaremos esto para configurar a Snow para que se comuniquen con Splunk.

5. Coge la última.
6. Vuelva a la instancia y haga clic en actualizar (o recupere conjuntos de actualizaciones).
7. A continuación, haga clic en el conjunto de importación de xml, elija archivo y seleccione el archivo que capturó antes.
8. A continuación, haga clic en Cargar. Esta operación puede tardar unos segundos.
9. A continuación, abra el conjunto de actualizaciones haciendo clic en Integración de Splunk.
10. Haga clic en "previsualizar conjunto de actualizaciones". No se preocupe si recibe algunos errores en este punto.
11. Cerrar ventana Y comprobar lo que fallan. Seleccione todos los mensajes a y acéptelos haciendo clic en "acciones en las filas seleccionadas"
12. A continuación, haga clic en "Confirmar el conjunto de actualizaciones".
13. Tenemos que agregar el usuario que va a comunicar Splunk con Service Now.
14. Por lo tanto, si no ha iniciado sesión como administrador en su cuenta de Service Now, debe elevar su función a security_admin (simplemente haga clic en la ficha de usuario y seleccione "Elevar funciones")
15. En la barra de búsqueda de la parte izquierda de la pantalla, escriba: Administrador de usuarios. Esto le llevará a la administración de usuarios.
16. Haga clic en Users/new users (Usuarios/Nuevos usuarios) y cree el usuario y la contraseña para este usuario.
 - Asegúrese de que la contraseña cumple las restricciones de complejidad.
 - Asegúrese de que las casillas "Active" (Activo) y "Internal integration user" (Usuario de integración interna) estén marcadas.
17. En la opción Roles, haga clic en "editar".
18. Seleccione el rol x_splu2_splunk_ser.Splunk
19. Guárdalo...

Esa es prácticamente la configuración que necesitamos en el lado de la NIEVE.

Ahora tenemos que instalar la aplicación en Splunk como cualquier otra aplicación.

1. Reinicie Splunk después de instalar la aplicación.
2. Ir a la aplicación
3. Coloque la URL de su instancia de Snow en el usuario que creó en Snow y su contraseña y guarde la configuración.
 - Si no aparece ningún mensaje de error durante este proceso, significa que la conexión se ha realizado correctamente.
4. Ir a aplicaciones y buscar NIEVE
5. Haga clic en "ver objetos"

Verá que algunas de las búsquedas no están habilitadas. Habilite el que necesite.

Y compruebe si funciona:

1. Vaya a la aplicación Snow.
2. En "Acciones" debería ver la pestaña "integración de incidentes de servicenow".

El usuario debe tener permisos de lectura y escritura en la aplicación.

Podríamos registrar un incidente como administrador en Snow usando esta consulta:

```
|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
```

Pero no pudimos generarlo usando otro usuario.

Recibimos este mensaje de error en 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
```

Resolución

Así que añadimos esta capacidad a la función de usuario:

```
list_storage_passwords
```

Después de hacer eso, el usuario fue capaz de crear incidentes en SNOW.

Lo probamos con esta consulta:

```
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
```

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).