

Complemento Splunk para ServiceNow - Não está gerando incidente para usuários

Aplicabilidade

Complementos de Aplicativos Splunk

Descrição

O administrador conseguiu gerar incidentes no Service Now usando o complemento ServiceNow, mas os usuários não conseguiram.

Usando o complemento Splunk para ServiceNow versão 3.1 (não há mais suporte)
On Splunk Search Head Versão 7.2.3

Recebendo mensagem de erro em 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
```

Investigação

Verificou duas vezes a instalação e configuração da NEVE;

- Começando pelo lado da neve:

1. Faça login na sua ocorrência de Snow.
2. Você pode instalar o aplicativo na Loja do Service Now ou
3. Quando você baixar o Splunk_TA_snow e descompactá-lo, acesse o arquivo e você verá outro arquivo chamado forExport (esses são os conjuntos de atualizações do Service Now)
 - Esses são os mecanismos que o Snow usa para adicionar funcionalidade, fazer backups e restaurar.
4. Usaremos isso para configurar Snow para se comunicar com Splunk.

5. Pegue o mais recente.
6. Volte para sua instância e clique em atualizar (ou recupere Conjuntos de Atualizações).
7. Em seguida, clique no conjunto de importação de xml, escolha o arquivo e selecione o arquivo que você pegou antes.
8. Em seguida, clique no upload. Isso pode levar alguns segundos.
9. Em seguida, abra o conjunto de atualizações clicando em Splunk integration.
10. Clique em "visualizar conjunto de atualizações". Não se preocupe se você receber alguns erros neste momento.
11. Feche a janela. E verificar o que falhou. Selecionar todas as mensagens a e aceitá-las clicando em "ações nas linhas selecionadas"
12. Em seguida, clique em "Confirmar o conjunto de atualizações"
13. Precisamos adicionar o usuário que irá se comunicar com o Splunk with Service Now.
14. Se você não estiver conectado como administrador em sua conta do Service Now, terá que elevar sua função para security_admin (Basta clicar na guia do usuário e selecionar "elevar funções")
15. Na barra de pesquisa no lado esquerdo da tela, digite: Administrador de usuário Isso o levará à administração do usuário.
16. Clique em usuários/novos usuários e crie o usuário e a senha para este usuário.
 - Verifique se a senha atende às restrições de complexidade.
 - Verifique se as caixas "Ativo" (Ativo) e "Internal integration user" (Usuário de integração interna) estão marcadas.
17. Na opção Funções, clique em "editar"
18. Selecione a função x_splu2_splunk_ser.Splunk
19. Salve-o.

Essa é basicamente a configuração que precisamos no lado da NEVE.

Agora precisamos instalar o aplicativo no Splunk como qualquer outro aplicativo.

1. Reinicie o Splunk após instalar o aplicativo.
2. Ir para o aplicativo
3. Coloque a URL para sua instância Snow o usuário que você criou no Snow e sua senha e salve a configuração.
 - Se você não receber nenhuma mensagem de erro durante esse processo, isso significa que a conexão foi bem-sucedida.
4. Acesse apps e procure por SNOW
5. Clique em "exibir objetos"

Você verá que algumas pesquisas não estão habilitadas. Ative o que você precisa.

E verifique se funciona:

1. Vá para o aplicativo Snow.
2. Em "Actions" (Ações), você verá a guia "servicenow incidente integration" (integração de incidentes no momento do serviço).

O usuário deve ter permissões de leitura e gravação no aplicativo.

Podemos registrar um incidente como administrador no 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
```

Mas não foi possível gerá-lo usando outro usuário.

Recebemos esta mensagem de erro em 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
```

Resolução

Adicionamos esse recurso à função de usuário:

```
list_storage_passwords
```

Depois de fazer isso, o usuário foi capaz de criar incidentes na NEVE.

Nós o testamos com 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
```

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.