

用于ServiceNow的Splunk加载项 — 不为用户生成事件

适用范围

Splunk应用加载项

描述

管理员可以使用ServiceNow加载项在Service Now上生成事件，但用户无法执行此操作。

使用Splunk加载项用于ServiceNow版本3.1 (不再支持)
Splunk Search Head版本7.2.3

在snow_ta_ticket.log上收到错误消息：

```
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
```

调查

再次检查SNOW的安装和配置；

— 从雪的一侧开始：

1. 登录您的Snow实例。
2. 您可以从Service Now应用商店安装应用，或者
3. 当您下载Splunk_TA_snow并解压缩它时，访问该文件，您将看到另一个名为forExport的文件（这些是Service Now更新集）
 - 这些是Snow用于添加功能、执行备份和还原的机制。
4. 我们将利用这个设置Snow与Splunk通信。
5. 拿最新的那个。
6. 返回您的实例，然后点击update（或retrieve Update Sets）。

7. 然后点击import set from xml，选择file并选择之前捕获的文件。
8. 然后单击上传。这可能需要几秒钟。
9. 然后点击Splunk集成打开更新集。
10. 点击“预览更新集”。不必担心，如果您此时遇到一些错误。
11. 关闭窗口。检查失败之处。选择所有消息，然后单击“在选定行上操作”接受这些消息
12. 然后单击“Commit the update Set”
13. 我们需要添加要与Splunk和Service Now进行通信的用户。
14. 因此，如果您没有以管理员身份登录您的Service Now帐户，则必须将您的角色提升为 security_admin（只需单击“用户”选项卡并选择“提升角色”）
15. 在屏幕左侧的搜索栏上键入：用户管理员。这将引导您进入用户管理。
16. 点击users/new users并创建此用户的用户和密码。
 - 确保密码符合复杂性限制。
 - 确保选中“活动”和“内部集成用户”框。
17. 在“角色”选项下，单击“编辑”
18. 选择角色x_splu2_splunk_ser.Splunk
19. 保存它。

这差不多就是我们在雪地一侧需要的配置。

现在，我们需要像任何其他应用一样在Splunk上安装该应用。

1. 安装应用后重新启动Splunk。
2. 转到应用
3. 将您在Snow上创建的用户Snow实例的URL及其密码并保存配置。
 - 如果您在此过程中未收到任何错误消息，则表示连接成功。
4. 转到应用并查找SNOW
5. 点击“查看对象”

您将看到某些搜索未启用。启用您需要的设备。

并检查它是否有效：

1. 转至Snow App。
2. 在“Actions”上，您应该看到“servicenow incident integration”选项卡。

用户必须拥有对应用的读取和写入权限。

我们可以使用此查询在Snow上以管理员身份记录事件：

```
|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
```

但我们无法使用其他用户生成它。

我们在 snow_ta_ticket.log上收到以下错误消息：

```
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
```

分辨率

因此，我们将该功能添加到用户角色：

```
list_storage_passwords
```

执行此操作后，用户能够在SNOW上创建事件。

我们通过此查询测试了它：

```
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
```

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。