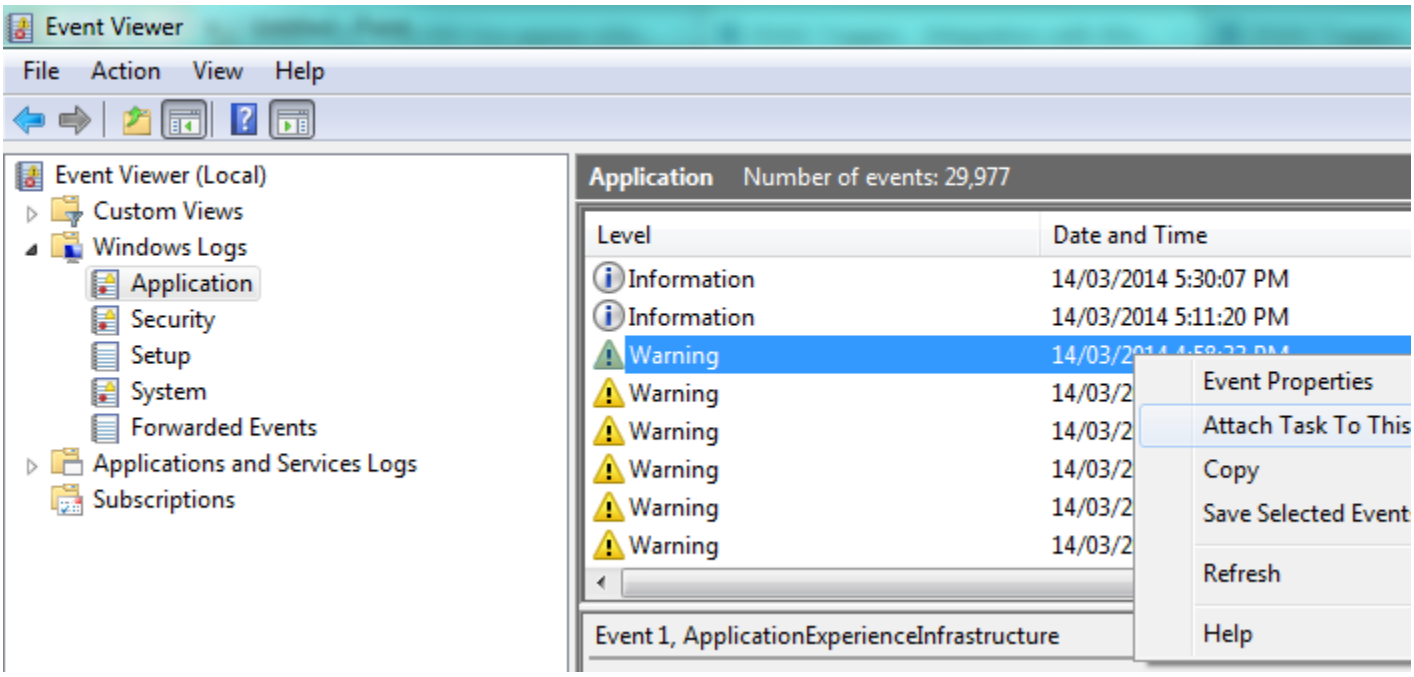
Description

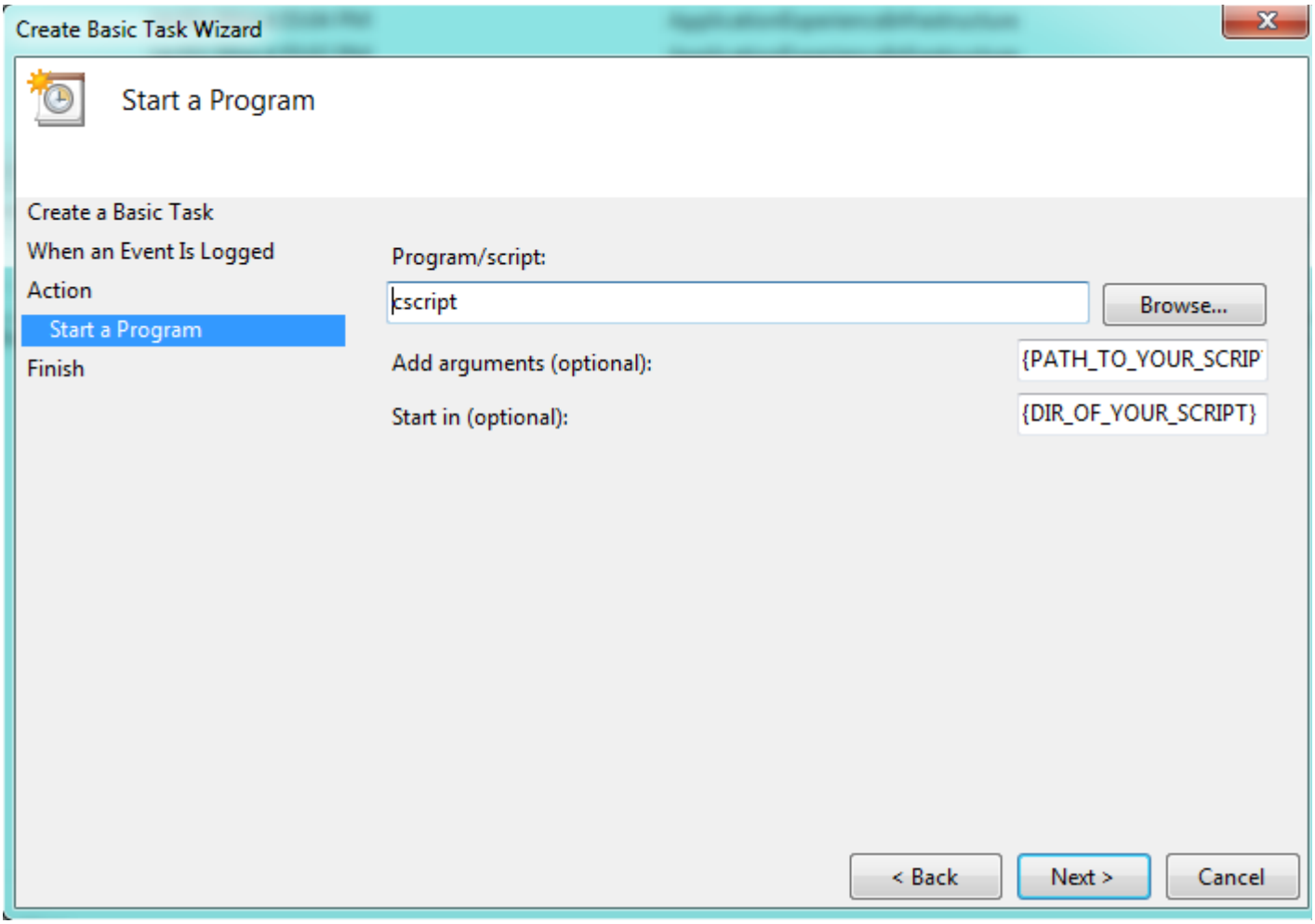
Follow this **How to** tutorial to trigger Dollar Universe task based on a Windows System Event

Define the Windows Event to monitor

- Open the "**Control Panel**".
- Open "**Administrative Tools**".
- Open "**Event Viewe**r".
- Search for the Windows event you want to attach a $U trigger to.
- Select this event and right click on it.
- Click on the "***Attach Task To This Event...***" menu.



- Define a name and click on "***Next***" twice.
- Choose "***Start a program***" and click on "***Next***".
- Enter "cscript" as the program to start, the path to the given script as arguments and the directory where the script is as the working directory.



Providing event properties to the $U trigger

- From the "**Administrative Tools**" window, open "**Task Scheduler**".
- Under "***Event Viewer Tasks***" part, select the task you have just created.
- Right click on it and on the "***Export***..." menu.
- Edit the corresponding .xml file.
- The "<*EventTrigger*>" section gives the filter on the Windows events. Just add a following lines in it, after <Subscription> keyword:

```
<ValueQueries>
<Value name="LOG">Event/System/Channel</Value>
<Value name="COMPUTER">Event/System/Computer</Value>
<Value
name="PROVIDER">Event/System/Provider/@Name</Value>
<Value name="EVENTID">Event/System/EventID</Value>
<Value name="LEVEL">Event/System/Level</Value>
<Value name="TASK">Event/System/Task</Value>
<Value
name="DATE">Event/System/TimeCreated/@SystemTime</Value>

</ValueQueries>
```

- At the end of the .xml file, you will find an <*Arguments*> keyword with "*{PATH_TO_YOUR_SCRIPT}*" as value.
- Just add the exported event properties as follow:

```
{PATH_TO_YOUR_SCRIPT} LOG="$(LOG)" COMPUTER="$(COMPUTER)"
PROVIDER="$(PROVIDER)" EVENTID="$(EVENTID)" LEVEL="$(LEVEL)" TASK="$(TASK)"
DATE="$(DATE)"
```

- Come back to "**Task Scheduler**" window and remove the original task.
- Click on "***Import Task***..." menu on the right panel and select the .xml file you have just edited.

Define which Dollar Universe node to target

- Download and edit the script attached to this page
- Inform the attributes giving the definition of the target Dollar Universe node:
  - ***host:*** The hostname of the Dollar Universe node.
  - ***port****:* The port number of the Dollar Universe API
  - ***area***: The target area.
- Inform the attributes giving the way you are going to authenticate yourself to Dollar Universe node:**NB:** You must inform either the authentication key or your credentials.

NB: If you inform both the authentication key and your credentials, only the authentication will be taken into account.

- ***authentication_key***: The authentication key you got via UVC OR
- ***user*** / ***password***: Your credentials.
- [optional] You can modify the event type that will be raised on Dollar Universe. By default this event type is: "**WINDOWS_EVENT**".
- Save and close the script.

Event properties

The given script transmit, by default, the following event properties:

- ***LOG***: The log where the event appear.
- ***COMPUTER***: The source computer
- ***PROVIDER***: The source of the event (program).
- ***EVENTID***: The event ID.
- ***LEVEL***: The numeric value of the level.
- ***TASK***: The numeric value of the task category
- ***DATE***: The date/time of the event

Customize the transmitted event properties

- Edit the .xml file corresponding to your schedule task.
- On the "<*EventTrigger*><*ValueQueries*>" , you should add lines giving the definition of the event property you want to transmit.
- Your "<*EventTrigger*>" should look like:

```
<EventTrigger>
        <Enabled>true</Enabled>
        <Subscription>...</Subscription>
        <ValueQueries>
                ...
```

```
                <Value
name="ACCOUNT">Event/EventData/Data[@Name='AccountName']</Value>

        </ValueQueries>
</EventTrigger>
```

- At the end of the .xml file, you will find an <*Arguments*> keyword with "*{PATH_TO_YOUR_SCRIPT}*" as value.
- Just add the event property you want to transmit:

```
{PATH_TO_YOUR_SCRIPT} LOG="$(LOG)" COMPUTER="$(COMPUTER)"
PROVIDER="$(PROVIDER)" EVENTID="$(EVENTID)" LEVEL="$(LEVEL)" TASK="$(TASK)"
DATE="$(DATE)" ACCOUNT="$(ACCOUNT)"
```

- You can also remove some event properties as follow (to remove ***PROVIDER*** and ***TASK*** properties):

```
{PATH_TO_YOUR_SCRIPT} LOG="$(LOG)" COMPUTER="$(COMPUTER)"
EVENTID="$(EVENTID)" LEVEL="$(LEVEL)" DATE="$(DATE)" ACCOUNT="$(ACCOUNT)"
```

- Come back to "**Task Scheduler**" window and remove the original task.
- Click on "***Import Task***..." menu on the right panel and select the .xml file you have just edited.