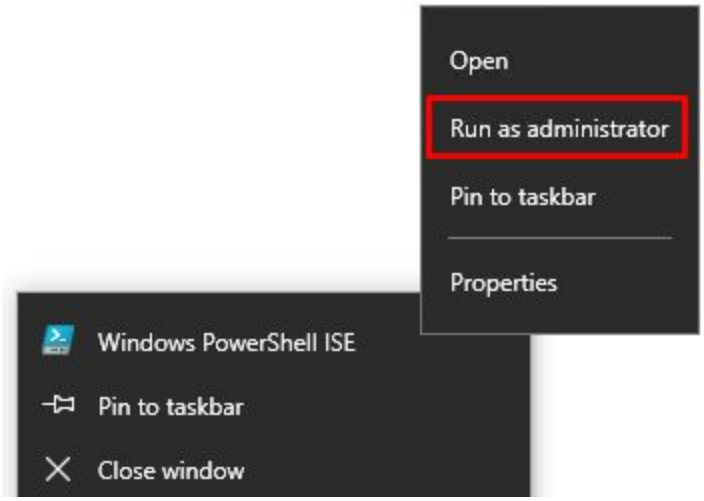
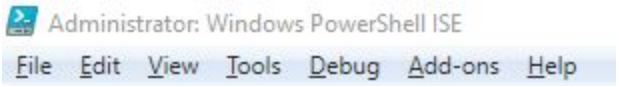
Включение

0. Убедитесь в том, что Powershell_ISE запущен в режиме администрирования





1. Включение аудита PnP устройств

```
auditpol /set /category:"Detailed Tracking"  /subcategory:"Plug and Play Events" /failure:enable /Success:enable
```

2. Импортируйте задачу в планировщик задач
Xml файл находится в конце этого документа

```
$xmlPath = "c:\Security_Microsoft-Windows-Security-Auditing_6416.xml"
Register-ScheduledTask -Xml (get-content $xmlPath | out-string) -TaskName `
"Security_Microsoft-Windows-Security-Auditing_6416" –Force
```

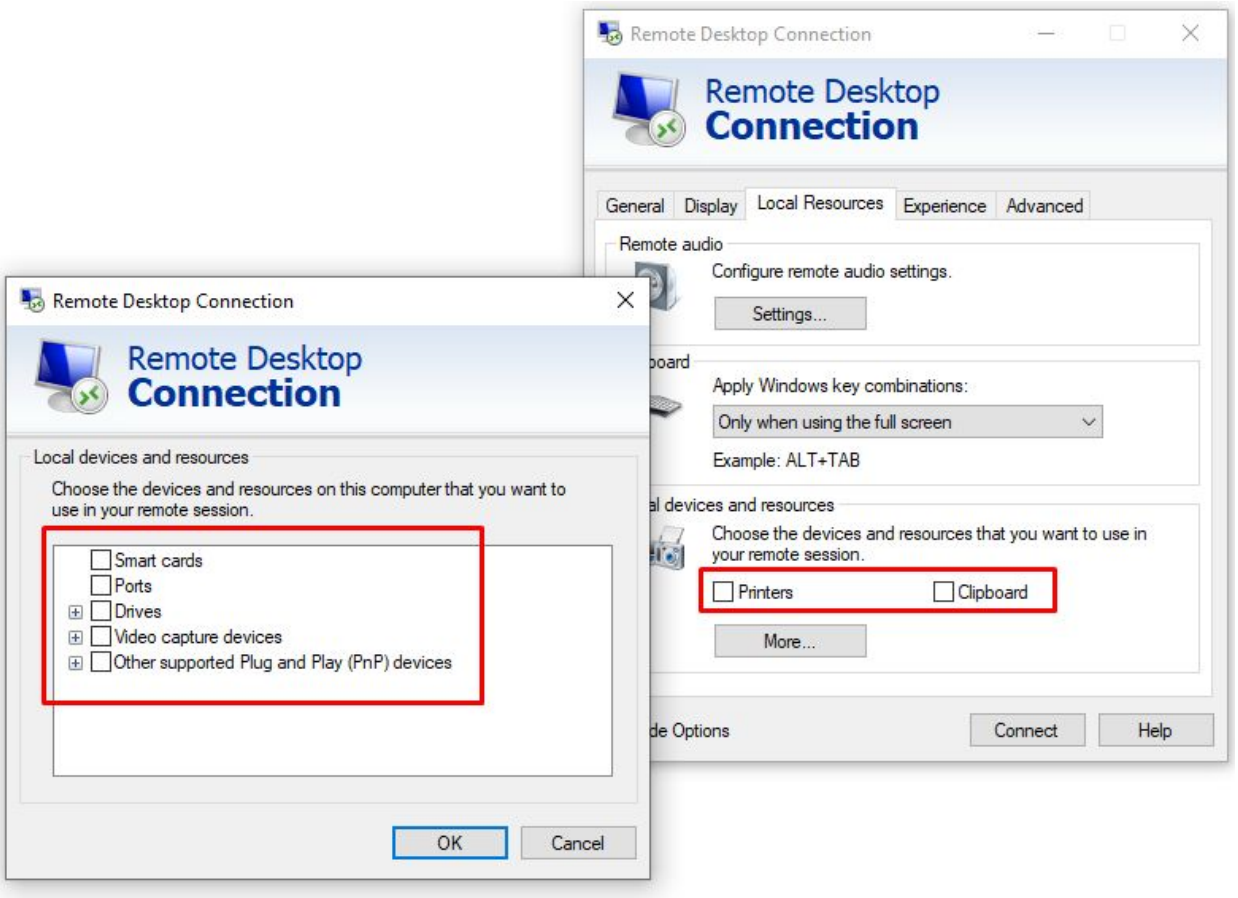
Принцип работа

После включения аудита устройств, в журнале Security создается события id 6416.
В планировщике задач, создается задача реагирующая на возникновение события.

Задача выполняет программу “shutdown.exe /r /f”

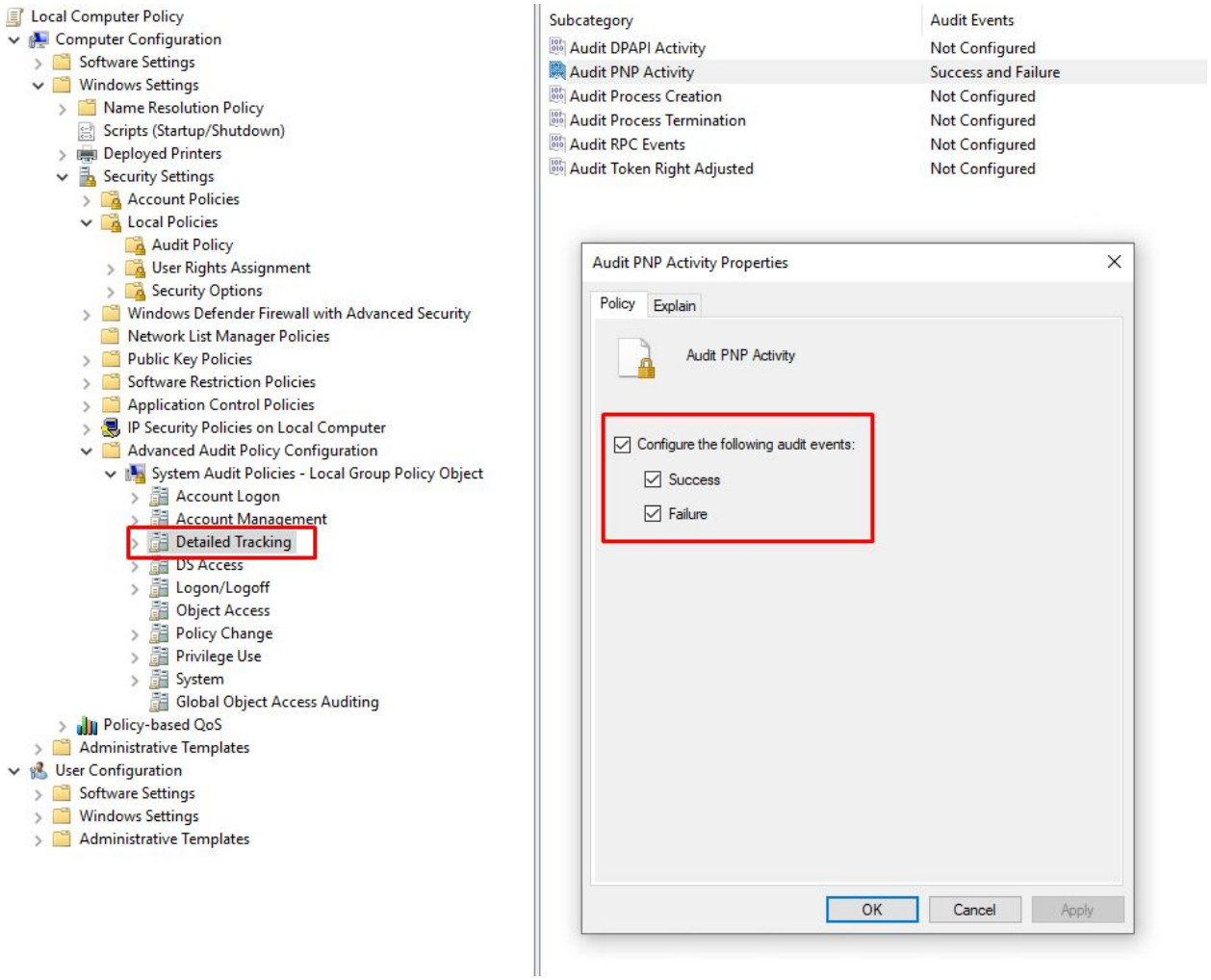
Предупреждение

В случае подключения через RDP клиент, возможно инициализация перезагрузки если предварительно не снять опции подключения устройств.

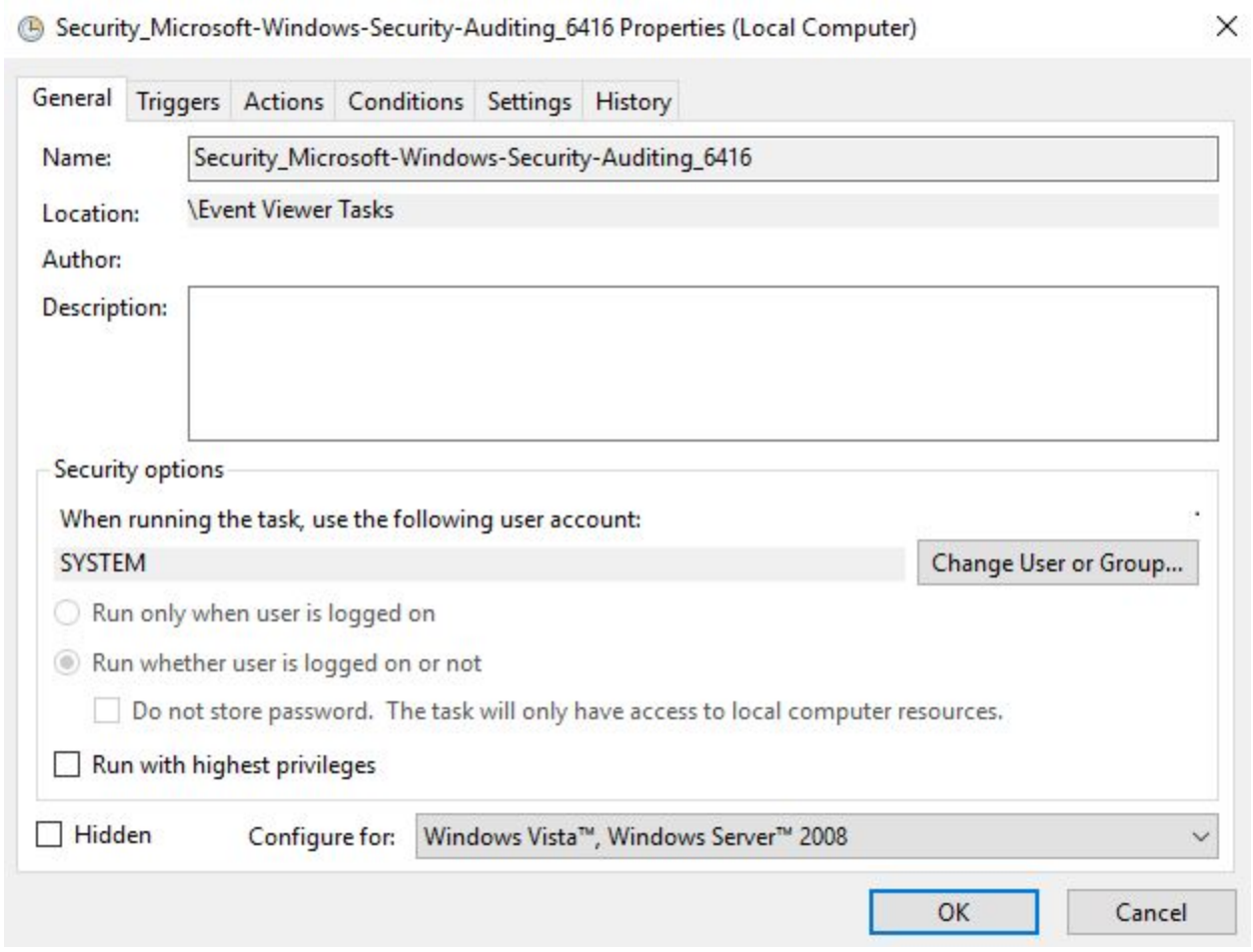


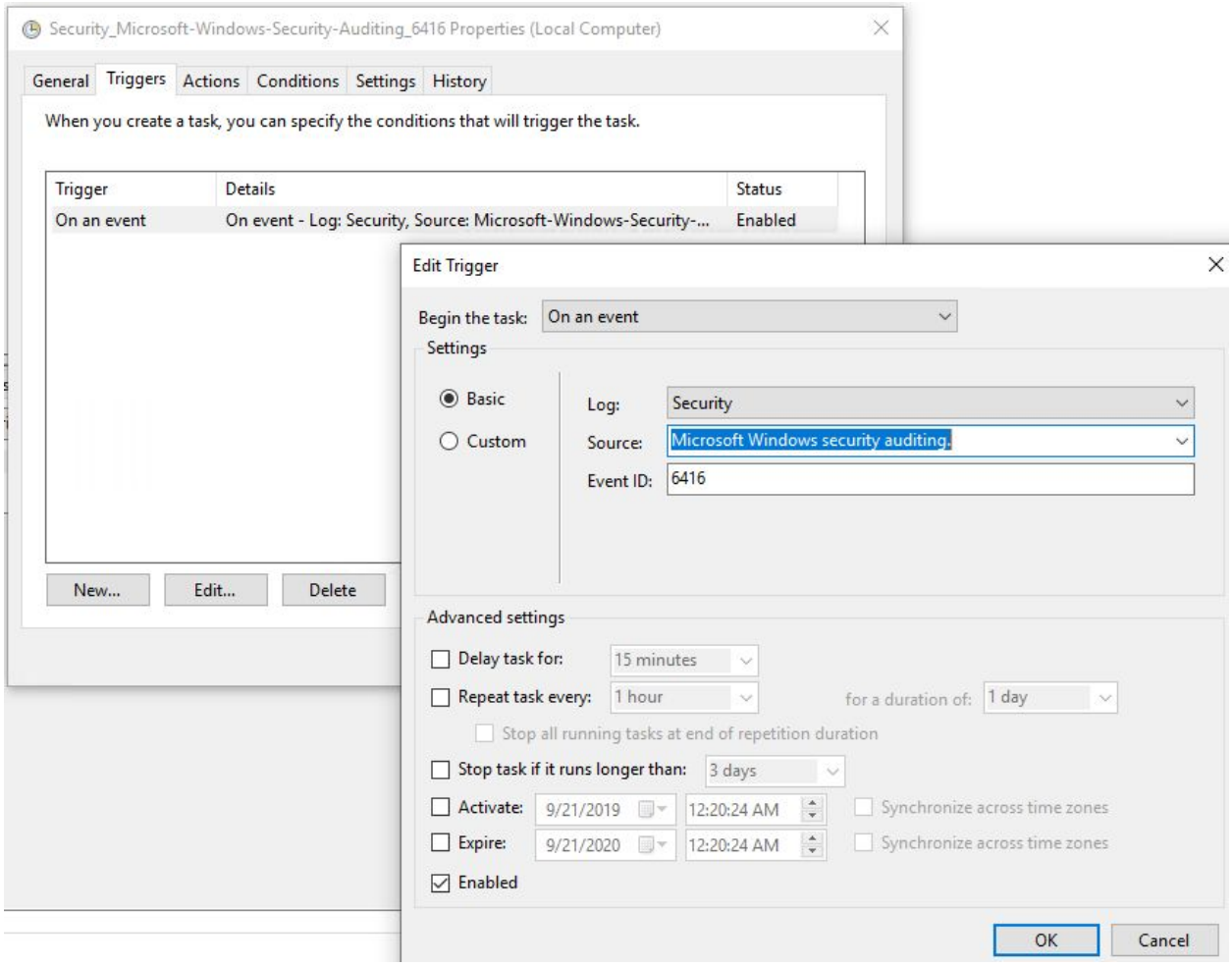
Включение вручную

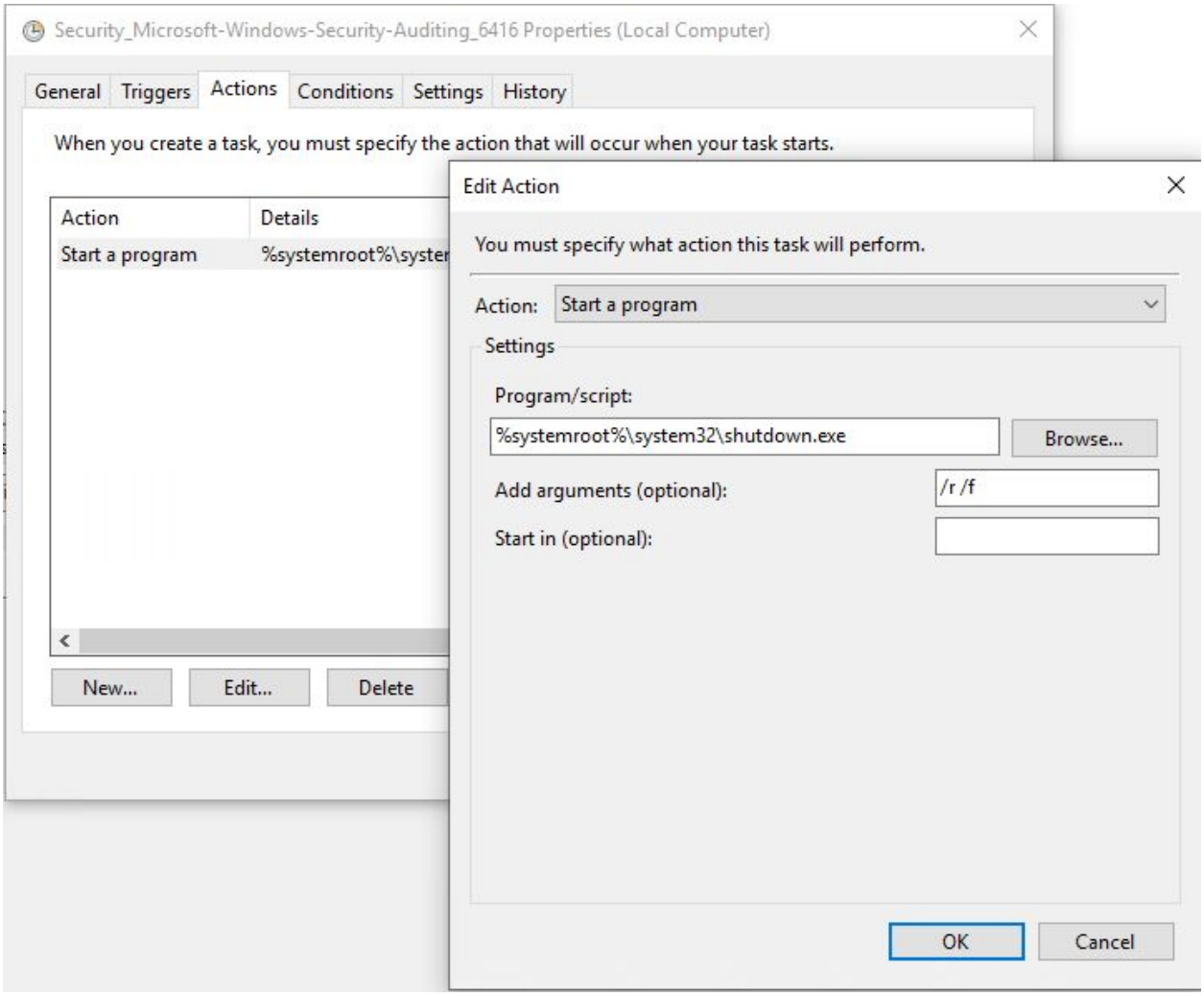
Включение аудита выполняется через локальную политику безопасности Открыть ее можно через команду “gpedit.msc”



Запланированная задача выглядит таким образом


Security_Microsoft-Windows-Security-Auditing_6416 Properties (Local Computer)
General
Triggers
Actions
Conditions
Settings
History
Name:
Security_Microsoft-Windows-Security-Auditing_6416
Location:
\Event Viewer Tasks
Author:
Description:
Security options
When running the task, use the following user account:
SYSTEM
Change User or Group...
Run only when user is logged on
Run whether user is logged on or not
Do not store password. The task will only have access to local computer resources.
Run with highest privileges
Hidden
Configure for:
Windows Vista™, Windows Server™ 2008
OK
Cancel


Security_Microsoft-Windows-Security-Auditing_6416 Properties (Local Computer)
General
Triggers
Actions
Conditions
Settings
History
When you create a task, you can specify the conditions that will trigger the task.
Trigger
Details
Status
On an event
On event - Log: Security, Source: Microsoft-Windows-Security-...
Enabled
New...
Edit...
Delete
Edit Trigger
Begin the task:
On an event
Settings
Basic
Custom
Log:
Security
Source:
Microsoft Windows security auditing.
Event ID:
6416
Advanced settings
Delay task for:
15 minutes
Repeat task every:
1 hour
for a duration of:
1 day
Stop all running tasks at end of repetition duration
Stop task if it runs longer than:
3 days
Activate:
9/21/2019
12:20:24 AM
Synchronize across time zones
Expire:
9/21/2020
12:20:24 AM
Synchronize across time zones
Enabled
OK
Cancel



XML файл задачи

```
<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.2"
xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
  <RegistrationInfo>
    <Date>2019-09-20T23:19:40.2343662</Date>
    <Author>Administrator</Author>
    <URI>\Event Viewer
Tasks\Security_Microsoft-Windows-Security-Auditing_6416</URI>
  </RegistrationInfo>
  <Triggers>
    <EventTrigger>
      <Enabled>true</Enabled>
```

```
      <Subscription>&lt;QueryList&gt;&lt;Query Id="0" Path="Security"&gt;&lt;Select
Path="Security"&gt;*[System[Provider[@Name='Microsoft-Windows-Security-Auditin
g'] and
EventID=6416]]&lt;/Select&gt;&lt;/Query&gt;&lt;/QueryList&gt;</Subscription>
    </EventTrigger>
  </Triggers>
  <Principals>
    <Principal id="Author">
      <UserId>S-1-5-18</UserId>
      <RunLevel>LeastPrivilege</RunLevel>
    </Principal>
  </Principals>
  <Settings>
    <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
    <DisallowStartIfOnBatteries>true</DisallowStartIfOnBatteries>
    <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>
    <AllowHardTerminate>true</AllowHardTerminate>
    <StartWhenAvailable>false</StartWhenAvailable>
    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>
    <IdleSettings>
      <StopOnIdleEnd>true</StopOnIdleEnd>
      <RestartOnIdle>false</RestartOnIdle>
    </IdleSettings>
    <AllowStartOnDemand>true</AllowStartOnDemand>
    <Enabled>true</Enabled>
    <Hidden>false</Hidden>
    <RunOnlyIfIdle>false</RunOnlyIfIdle>
    <WakeToRun>false</WakeToRun>
    <ExecutionTimeLimit>PT72H</ExecutionTimeLimit>
    <Priority>7</Priority>
  </Settings>
  <Actions Context="Author">
    <Exec>
      <Command>%systemroot%\system32\shutdown.exe</Command>
      <Arguments>/r /f</Arguments>
    </Exec>
  </Actions>
</Task>
```
