Yêu cầu

1. hoàn thiện phần cảnh báo + hệ thống mail + các mức cảnh báo (ở đô án I). - Vinh

2. Thiết lập phần IPS - Qui

- Xác định nhóm người dùng có quyền sử dụng tài nguyên
- Xác định cách thức chặn sử dụng tài nguyên trái phép

3. Xác định thêm các log trên các workstation liên quan đến - Duẩn - Luân

- thực hiện các APP không có trong danh mục cho phép.
- đọc, cập nhật các file trong các thư mục hệ thống
- cài đặt các APP mới
- Mở/ chạy service mới

Kết quả dự kiến

STT	Phân rã	Thời gian (ngày)	Tổng thời gian (ngày)	Kết quả dự kiến
1	1. Phân tích log trên windows có sẵn.	1	3	Nhận dạng log
	2. Cấu hình gửi mail cảnh báo và active response	2		Gửi thành công mail cảnh báo đến mail quản trị. Chặn thành công các tác vụ nguy hiểm.
2				
	1. Lấy log trên Windows và phân tích	6		Nhận dạng log

3	2. Viết Decoder	4	16 (12-28/9/2016)	Decoder cho từng log
	3. Viết Rule	4		Rule và mức cảnh báo cho Decoder
	4. Test	2		Sinh ra cảnh báo và gửi mail

3. Xác định thêm các log trên các workstation liên quan

3.1. Thực hiện các APP không có trong danh mục cho phép.

3.2. Đọc, cập nhật các file trong các thư mục hệ thống

- **Even log ID**

  Event ID 4663: An attempt was made to access an object (used to decoder)

  Sự kiện này ghi lại các hoạt động xảy ra với tập tin hoặc các đối tượng khác. Được ghi log lại giữa 2 sự kiện mở (4656) và đóng (4658).

  Event ID 4656: A handle to an object was requested

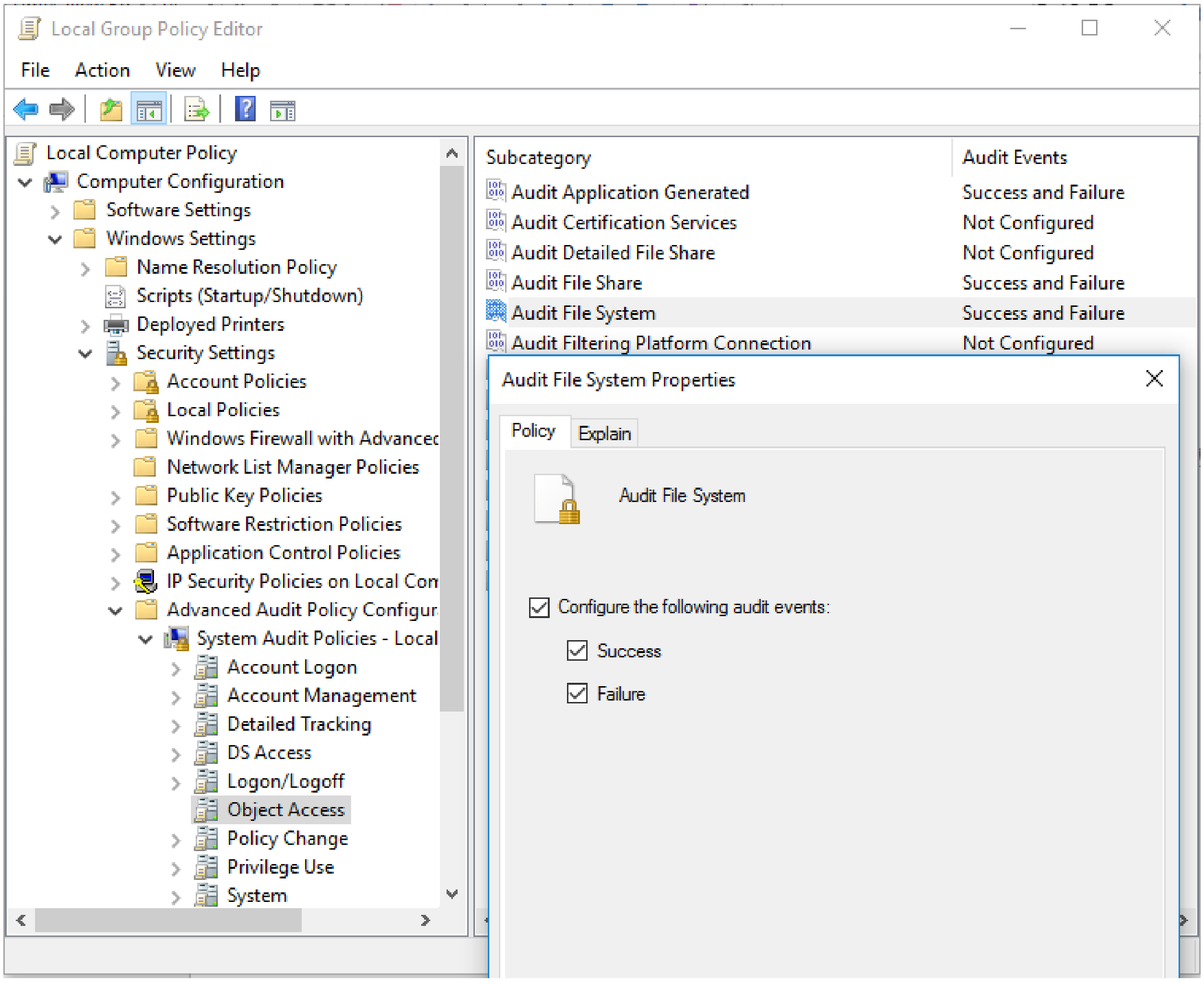
  Sự kiện này ghi lại khi một ứng dụng cố gắng truy cập vào một file (đối tượng). Sự kiện trả về thành công hoặc thất bại.

  Event ID 4658: The handle to an object was closed

  Sau khi mở thành công một đối tượng, một chương trình đóng nó lại sẽ được ghi lại bởi sự kiện này.

- **Bật ghi log**

  Open **Run** (Windows+R), type **gpedit.msc** and fllowing picture



- Local Computer Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Deployed Printers
      - Security Settings
        - Account Policies
        - Local Policies
        - Windows Firewall with Advancec
        - Network List Manager Policies
        - Public Key Policies
        - Software Restriction Policies
        - Application Control Policies
        - IP Security Policies on Local Con
        - Advanced Audit Policy Configur
          - System Audit Policies - Local
            - Account Logon
            - Account Management
            - Detailed Tracking
            - DS Access
            - Logon/Logoff
            - Object Access
            - Policy Change
            - Privilege Use
            - System

Subcategory	Audit Events
Audit Application Generated	Success and Failure
Audit Certification Services	Not Configured
Audit Detailed File Share	Not Configured
Audit File Share	Success and Failure
Audit File System	Success and Failure
Audit Filtering Platform Connection	Not Configured

Audit File System Properties

Audit File System

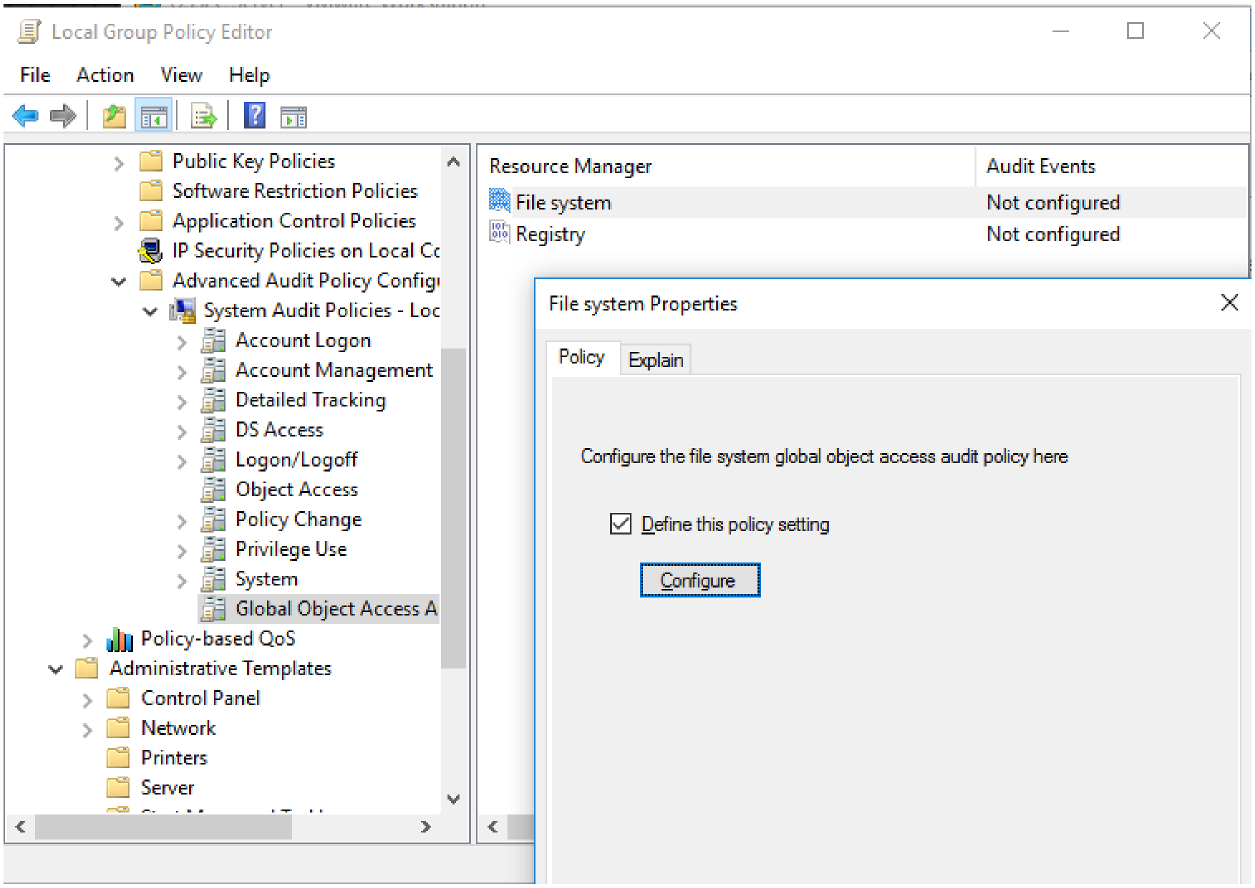
☑ Configure the following audit events:

☑ Success

☑ Failure

(By the way, make sure you also enable *Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Audit: Force audit policy subcategory settings to override audit policy category settings* to make sure your audit policy takes effect.)

❖ **Thực hiện giám sát trên toàn bộ thư mục hệ thống**



Resource Manager	Audit Events
File system	Not configured
Registry	Not configured

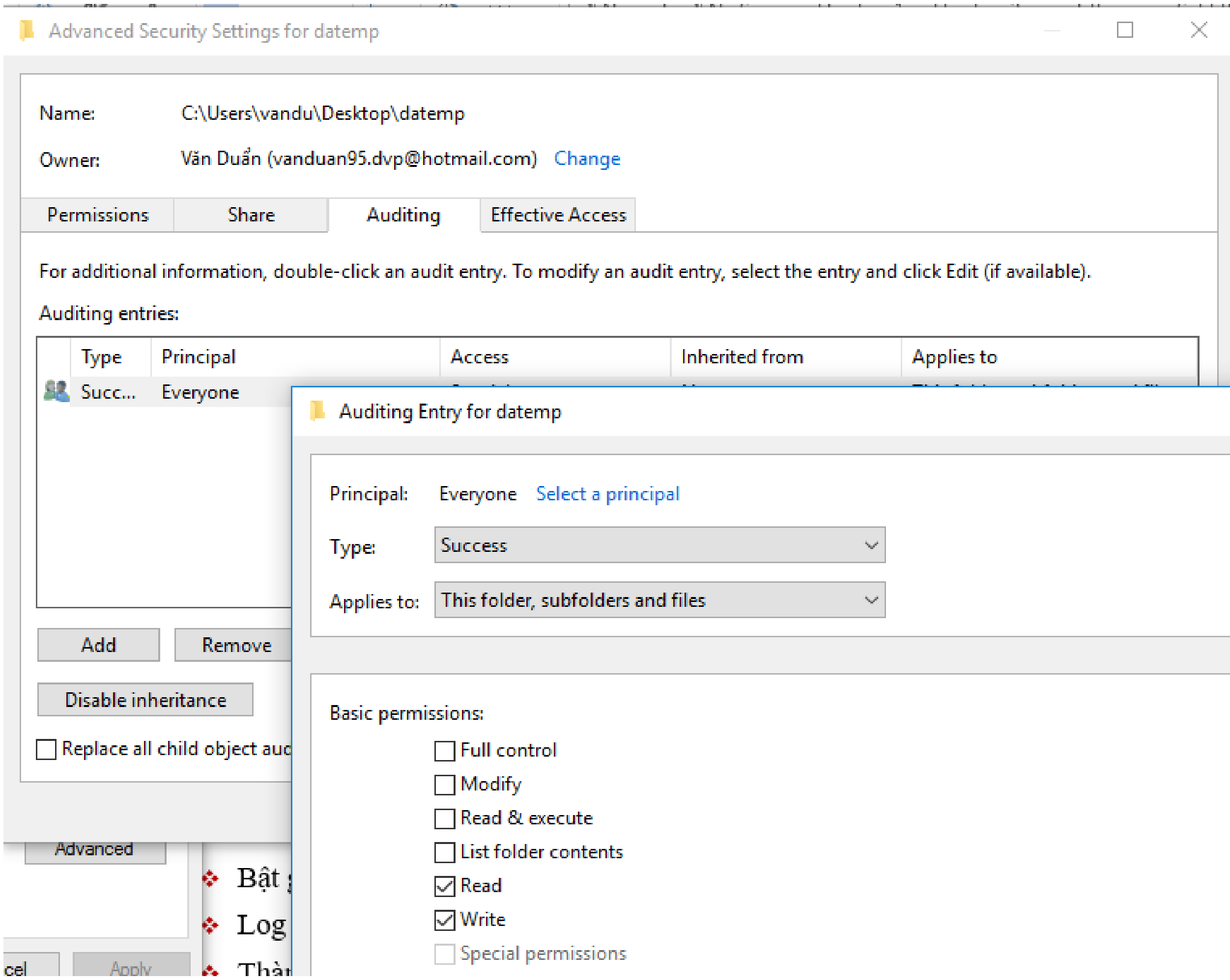
File system Properties

Configure the file system global object access audit policy here

☑ Define this policy setting

❖ **Thực hiện giám sát trên thư mục ngoài hệ thống**(*hướng dẫn thực hiện trên windows 10*)

- Chuột phải trên thư mục, chọn **Properties**
- Trong tab **Security**, chọn **Advanced**
- Trong tab **Auditing,** chọn **Continue**
- Tiếp theo thêm **User** và hành động cần giám sát, tương tự như hình



Advanced Security Settings for datemp

Name: C:\Users\vandu\Desktop\datemp

Owner: Văn Duẩn (vanduan95.dvp@hotmail.com) Change

For additional information, double-click an audit entry. To modify an audit entry, select the entry and click Edit (if available).

Auditing entries:

Type	Principal	Access	Inherited from	Applies to
Succ...	Everyone			

□ Replace all child object auc

Auditing Entry for datemp

Principal: Everyone Select a principal

Type: Success

Applies to: This folder, subfolders and files

Basic permissions:

□ Full control
□ Modify
□ Read & execute
□ List folder contents
☑ Read
☑ Write
□ Special permissions

❖ Access Mask

Access Mask	Detail	Other
0x1	Read Data (or List Directory)	
0x2	Write Data (or Add File)	0x6
0x4	Append Data (or Add Subdirectory)	
0x6	Write Data (or AddFile) Append Data (or Add Subdirectory or Create PipeInstance)	
0x80	Read Attributes	
0x100	Write Attributes	

0x10000	Delete	
0x20000	READ_CONTROL (read the information in the security descriptor for the object)	

Log mẫu (Failed, Successfull) trên Windows

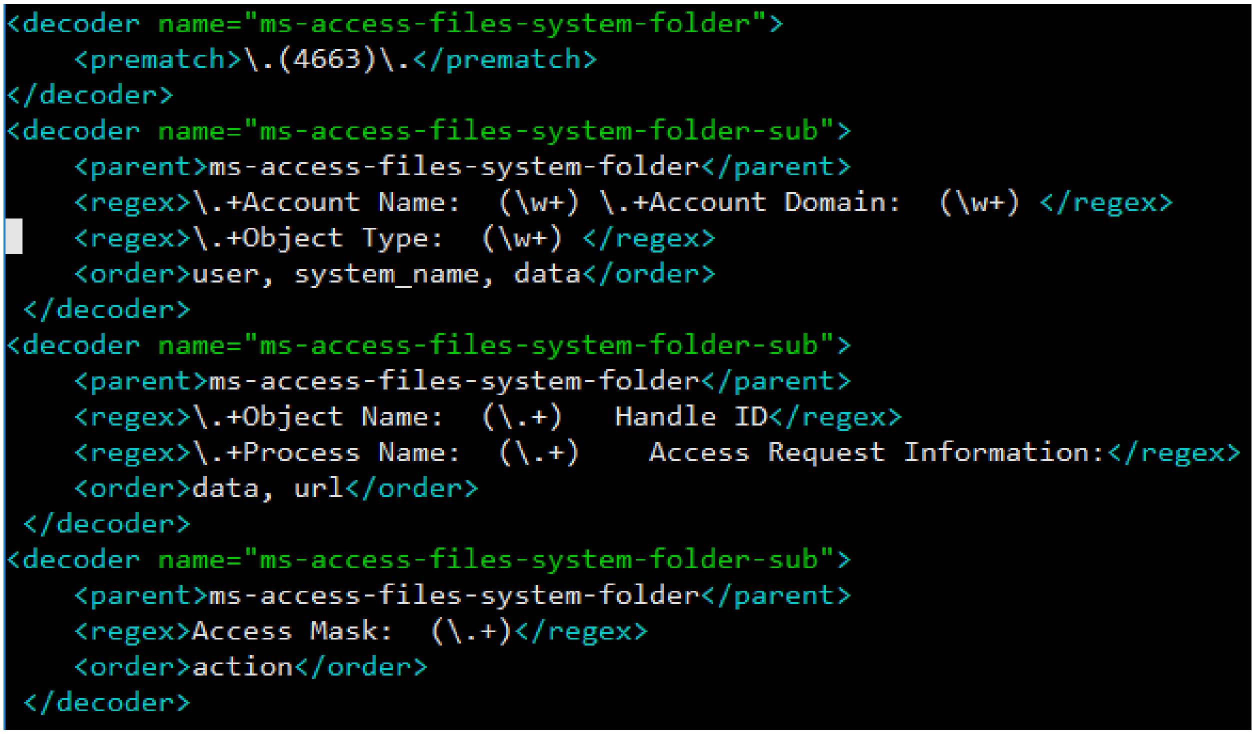
```
WinEvtLog 2016 Sep 19 12:55:49 WinEvtLog: Security:
AUDIT_SUCCESS(4663): Microsoft-Windows-Security-Auditing:  (no user): no
domain: VanDuan-PC: An attempt was made to access an object.   Subject:
Security ID:  S-1-5-21-2011668779-2805874254-784660433-1001  Account
Name:  vandu   Account Domain:  VANDUAN-PC   Logon ID:  0x76E4F93
Object:   Object Server:  Security   Object Type:  File   Object Name:  C:\Test
Folder   Handle ID:  0x230   Resource Attributes: S:AI    Process Information:
Process ID:  0xd08   Process Name:  C:\Windows\System32\notepad.exe
Access Request Information:    Accesses:  ReadData (or ListDirectory)
Access Mask:  0x1
```

```
WinEvtLog 2016 Sep 19 12:55:39 WinEvtLog: Security:
AUDIT_SUCCESS(4663): Microsoft-Windows-Security-Auditing:  (no user): no
domain: VanDuan-PC: An attempt was made to access an object.   Subject:
Security ID:  S-1-5-21-2011668779-2805874254-784660433-1001  Account
Name:  vandu   Account Domain:  VANDUAN-PC   Logon ID:  0x76E4F93
Object:   Object Server:  Security   Object Type:  File   Object Name:  C:\Test
Folder   Handle ID:  0xd30   Resource Attributes: S:AI    Process Information:
Process ID:  0x1304   Process Name:  C:\Windows\explorer.exe     Access
Request Information:    Accesses:  READ_CONTROL        Access Mask:
0x20000
```

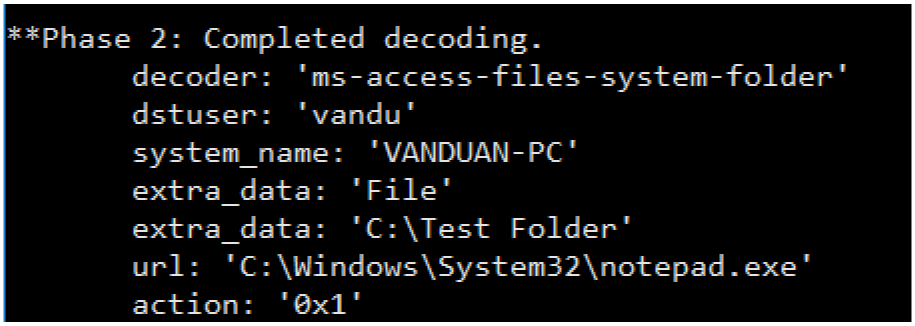
Thành phần quan trọng (cần lấy)

- Log ID:
- Account Name:
- Account Domain:
- Object Type:
- Object Name:
- Process Name:
- Accesses Mask:

Viết Decoder

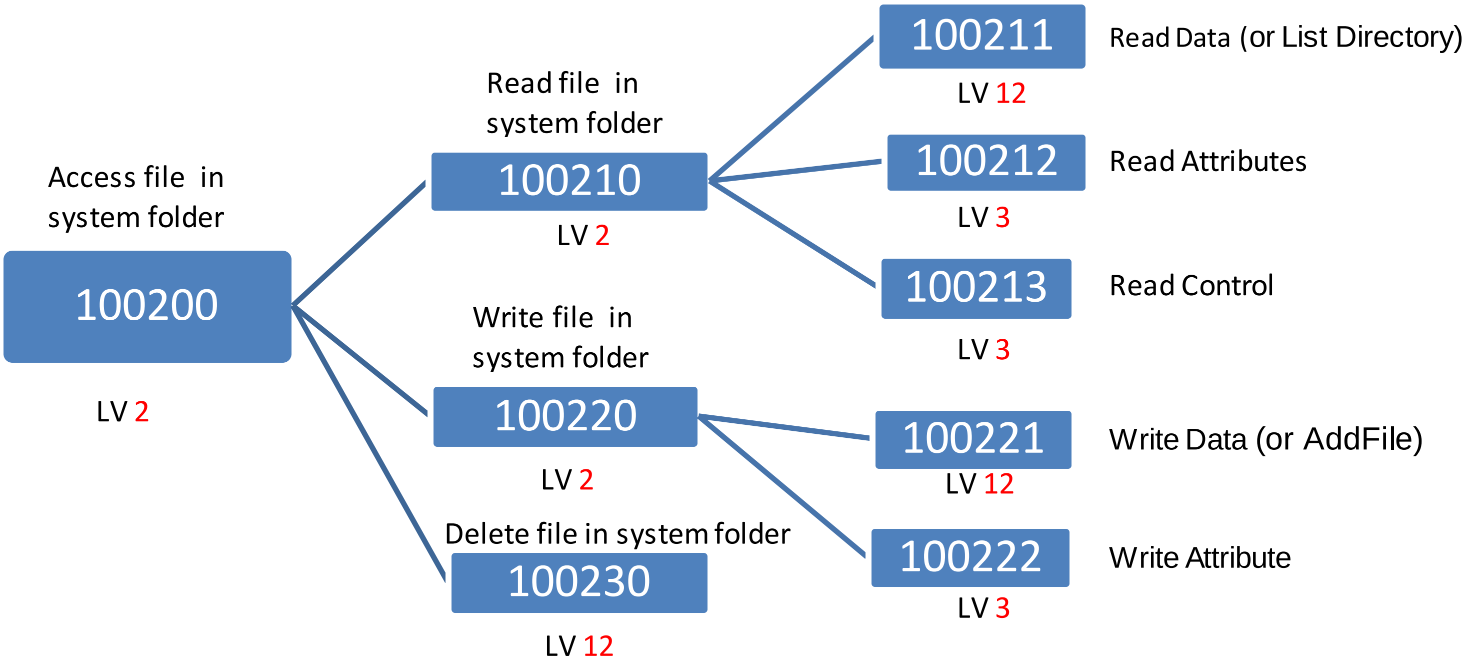


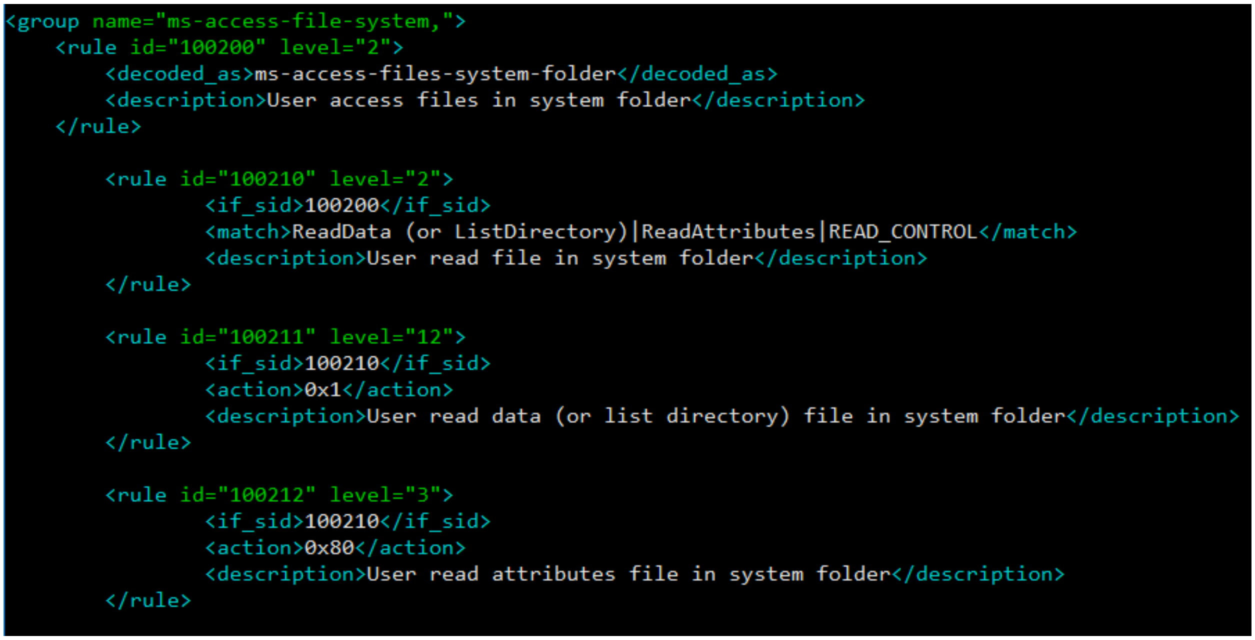
```
<decoder name="ms-access-files-system-folder">
    <prematch>\.(4663)\.</prematch>
</decoder>
<decoder name="ms-access-files-system-folder-sub">
    <parent>ms-access-files-system-folder</parent>
    <regex>\.+Account Name:  (\w+) \.+Account Domain:  (\w+) </regex>
    <regex>\.+Object Type:  (\w+) </regex>
    <order>user, system_name, data</order>
 </decoder>
<decoder name="ms-access-files-system-folder-sub">
    <parent>ms-access-files-system-folder</parent>
    <regex>\.+Object Name:  (\.+)   Handle ID</regex>
    <regex>\.+Process Name:  (\.+)    Access Request Information:</regex>
    <order>data, url</order>
 </decoder>
<decoder name="ms-access-files-system-folder-sub">
    <parent>ms-access-files-system-folder</parent>
    <regex>Access Mask:  (\.+)</regex>
    <order>action</order>
 </decoder>
```



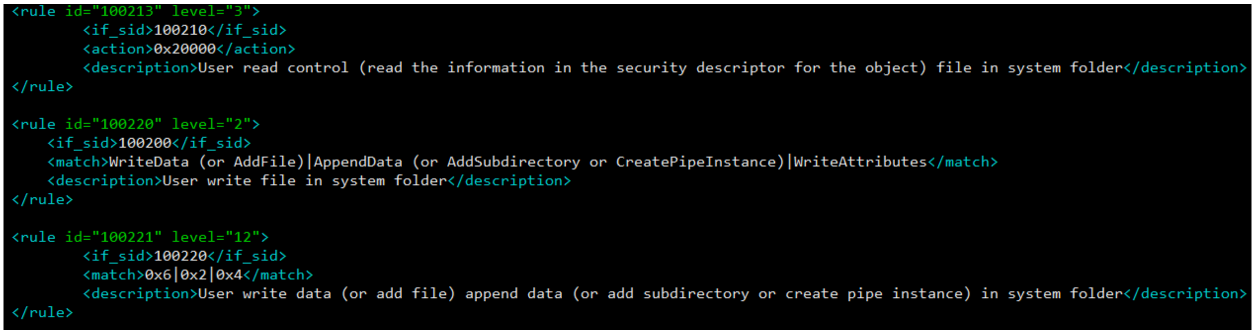
```
**Phase 2: Completed decoding.
       decoder: 'ms-access-files-system-folder'
       dstuser: 'vandu'
       system_name: 'VANDUAN-PC'
       extra_data: 'File'
       extra_data: 'C:\Test Folder'
       url: 'C:\Windows\System32\notepad.exe'
       action: '0x1'
```

- **Viết Rule**

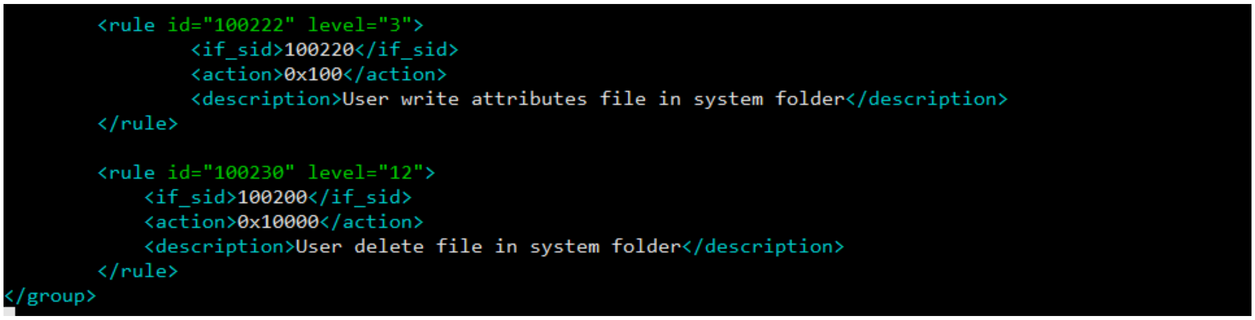




```
<group name="ms-access-file-system,">
    <rule id="100200" level="2">
        <decoded_as>ms-access-files-system-folder</decoded_as>
        <description>User access files in system folder</description>
    </rule>

        <rule id="100210" level="2">
                <if_sid>100200</if_sid>
                <match>ReadData (or ListDirectory)|ReadAttributes|READ_CONTROL</match>
                <description>User read file in system folder</description>
        </rule>

        <rule id="100211" level="12">
                <if_sid>100210</if_sid>
                <action>0x1</action>
                <description>User read data (or list directory) file in system folder</description>
        </rule>

        <rule id="100212" level="3">
                <if_sid>100210</if_sid>
                <action>0x80</action>
                <description>User read attributes file in system folder</description>
        </rule>
```



```
<rule id="100213" level="3">
        <if_sid>100210</if_sid>
        <action>0x20000</action>
        <description>User read control (read the information in the security descriptor for the object) file in system folder</description>
</rule>

<rule id="100220" level="2">
    <if_sid>100200</if_sid>
    <match>WriteData (or AddFile)|AppendData (or AddSubdirectory or CreatePipeInstance)|WriteAttributes</match>
    <description>User write file in system folder</description>
</rule>

<rule id="100221" level="12">
        <if_sid>100220</if_sid>
        <match>0x6|0x2|0x4</match>
        <description>User write data (or add file) append data (or add subdirectory or create pipe instance) in system folder</description>
</rule>
```



```
        <rule id="100222" level="3">
                <if_sid>100220</if_sid>
                <action>0x100</action>
                <description>User write attributes file in system folder</description>
        </rule>

        <rule id="100230" level="12">
            <if_sid>100200</if_sid>
            <action>0x10000</action>
            <description>User delete file in system folder</description>
        </rule>
</group>
```

3.3. Cài đặt các APP mới

❖ Even log ID

Event ID 1033 — Windows Installer Application Installation (used to decoder)

Event Details

Product:	Windows Installer - Unicode
ID:	1033
Source:	MsiInstaller
Version:	4.0
Symbolic Name:	EVENTLOG_TEMPLATE_INSTALLATION_STATUS
Message:	Windows Installer installed the product. Product Name: %1. Product Version: %2. Product Language: %3. Installation success or error status: %4. - Status: 0(S) or 1603 (E)

Event ID 11708 — Installation operation failed

Event ID 11728 — Installation operation successfully

❖ Bật ghi log

Click **Start**, click **Run**, type Notepad, and then click **OK**.
Type the following commands in Notepad.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer]
"Logging"="voicewarmupx"
"Debug"=dword:00000007
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate
\Trace]
"Flags"=dword:00000016
"Level"=dword:00000004
```

On the **File** menu, click **Save As**.
In the **Save in** list, click **Desktop**.
In the **File name** box, type LoggingOn.reg, click **All Files** in the **Save as type** list, and then click **Save**.
On the desktop, double-click the LoggingOn.reg file to add the registry keys to the Windows registry.
Click **OK** in the message box.
Try to install the update again to capture the additional error information in the Windows Installer .log file.

❖ Log mẫu (Failed, Successfull) trên Windows

- Eventlog format

```
WinEvtLog 2016 Sep 14 23:01:08 WinEvtLog: Application:
INFORMATION(1033): MsiInstaller: vandu: VANDUAN-PC: VanDuan-PC:
Skype� 6.20 6.20.104 1033 0 Skype Technologies S.A. (NULL)
```

```
WinEvtLog 2016 Sep 14 23:33:30 WinEvtLog: Application:
INFORMATION(1033): MsiInstaller: vandu: VANDUAN-PC: VanDuan-PC:
Skype� 6.20 6.20.104 1033 1603 Skype Technologies S.A. (NULL)
```

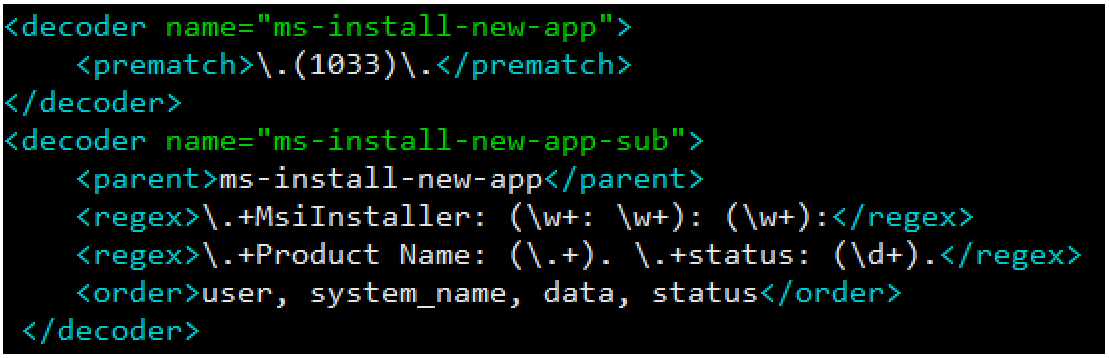
- Eventchannel format

```
WinEvtLog 2016 Sep 14 23:37:37 WinEvtLog: Application:
INFORMATION(1033): MsiInstaller: vandu: VANDUAN-PC: VanDuan-PC:
Windows Installer installed the product. Product Name: Skype™ 6.20.
Product Version: 6.20.104. Product Language: 1033. Manufacturer: Skype
Technologies S.A.. Installation success or error status: 1603.
```

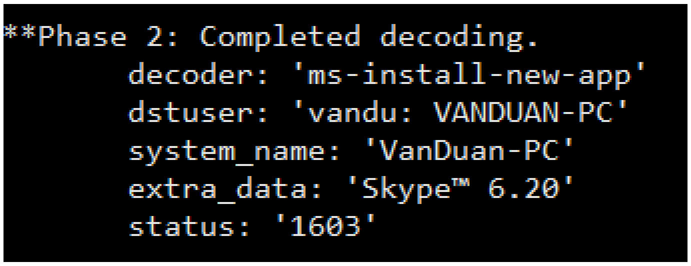
❖ Thành phần quan trọng (cần lấy)

- App name:
- User:
- Computer:
- Status:

Viết Decoder

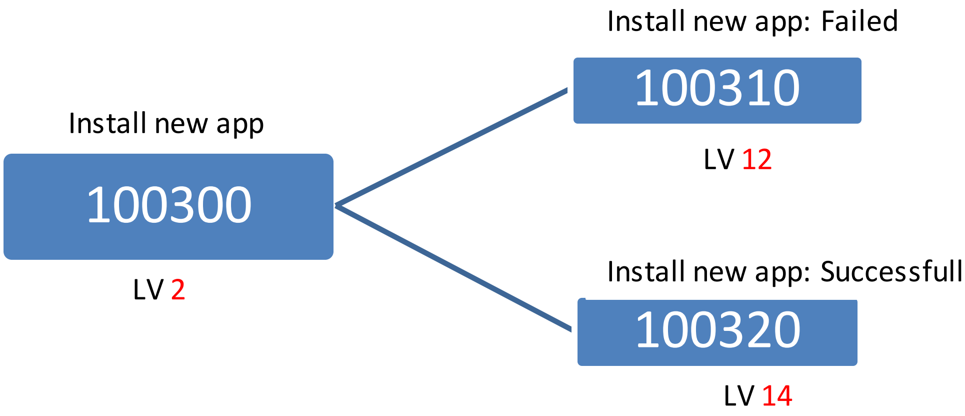


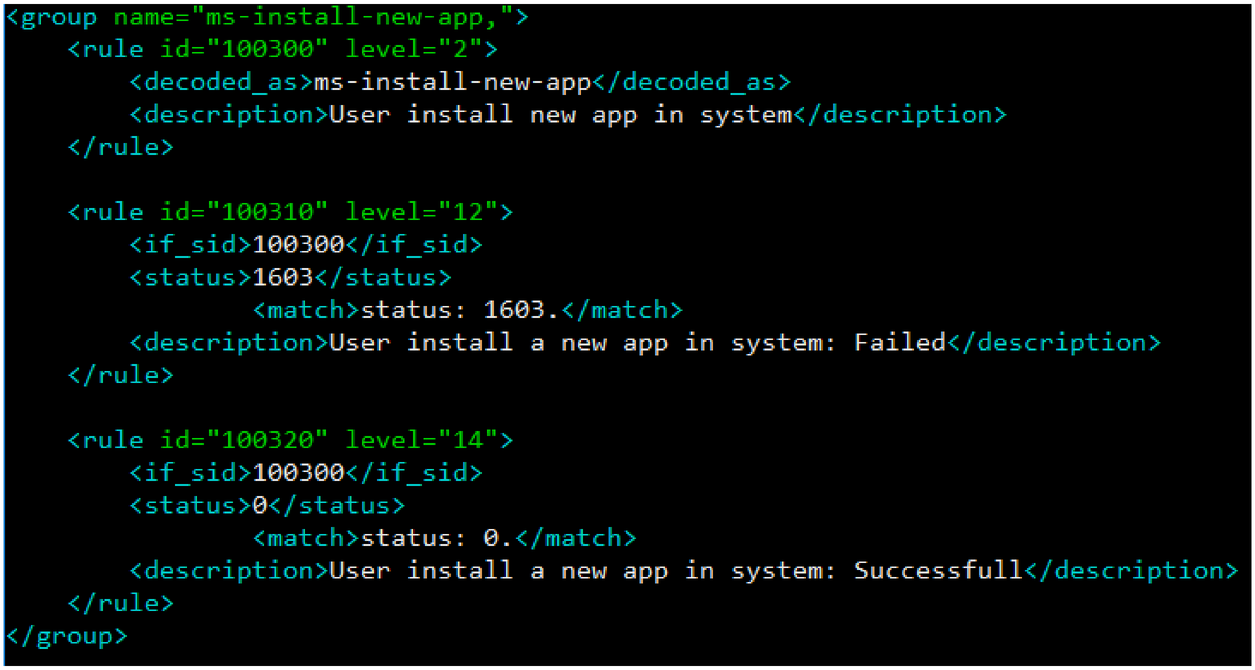
```
<decoder name="ms-install-new-app">
    <prematch>\.(1033)\.</prematch>
</decoder>
<decoder name="ms-install-new-app-sub">
    <parent>ms-install-new-app</parent>
    <regex>\.+MsiInstaller: (\w+: \w+): (\w+):</regex>
    <regex>\.+Product Name: (\.+). \.+status: (\d+).</regex>
    <order>user, system_name, data, status</order>
 </decoder>
```



```
**Phase 2: Completed decoding.
       decoder: 'ms-install-new-app'
       dstuser: 'vandu: VANDUAN-PC'
       system_name: 'VanDuan-PC'
       extra_data: 'Skype™ 6.20'
       status: '1603'
```

Viết Rule





```
<group name="ms-install-new-app,">
    <rule id="100300" level="2">
        <decoded_as>ms-install-new-app</decoded_as>
        <description>User install new app in system</description>
    </rule>

    <rule id="100310" level="12">
        <if_sid>100300</if_sid>
        <status>1603</status>
                <match>status: 1603.</match>
        <description>User install a new app in system: Failed</description>
    </rule>

    <rule id="100320" level="14">
        <if_sid>100300</if_sid>
        <status>0</status>
                <match>status: 0.</match>
        <description>User install a new app in system: Successfull</description>
    </rule>
</group>
```

3.4. Mở/ chạy service mới

❖ **Event Log ID**

Windows 10 chưa/không có logID 7035

Event ID 7035 — Servies was successfully sent a start/stop control. (Khi yêu cầu một dịch vụ chạy/dừng)

Event ID 7040 — Change status a services (Khi thay đổi trạng thái khởi động của dịch vụ: tự khởi động, bằng tay, tắt)

Event ID 7045 — Install a new services (Khi cài một dịch vụ mới)

❖ **Log mẫu**

<7035>

```
WinEvtLog 2016 Sep 30 15:02:12 WinEvtLog: System:
INFORMATION(7035): Service Control Manager: vanduan: VANDUAN-
5A94E18: VANDUAN-5A94E18: The Windows Installer service was
successfully sent a start control.
```

```
WinEvtLog 2016 Sep 30 15:15:18 WinEvtLog: System:
INFORMATION(7035): Service Control Manager: vanduan: VANDUAN-
5A94E18: VANDUAN-5A94E18: The Windows Installer service was
successfully sent a stop control.
```

<7040>

```
WinEvtLog 2016 Sep 15 10:20:47 WinEvtLog: System:
INFORMATION(7040): Service Control Manager: Vo: Asus: Asus:
```

```
The start type of the Superfetch service was changed from disabled to
auto start.

WinEvtLog 2016 Sep 15 10:23:48  WinEvtLog: System:
INFORMATION(7040): Service Control Manager: Vo: Asus: Asus:
The start type of the Superfetch service was changed from auto start to
demand start.

WinEvtLog 2016 Sep 15 10:23:48  WinEvtLog: System:
INFORMATION(7040): Service Control Manager: Vo: Asus: Asus:
The start type of the Superfetch service was changed from auto start to
demand start.

WinEvtLog 2016 Sep 15 10:24:06  WinEvtLog: System:
INFORMATION(7040): Service Control Manager: Vo: Asus: Asus:
The start type of the Superfetch service was changed from demand
start to auto start.
```

Startup type : **Automatic <=> auto start**

Manual <=> demand start

Disable <=> disabled

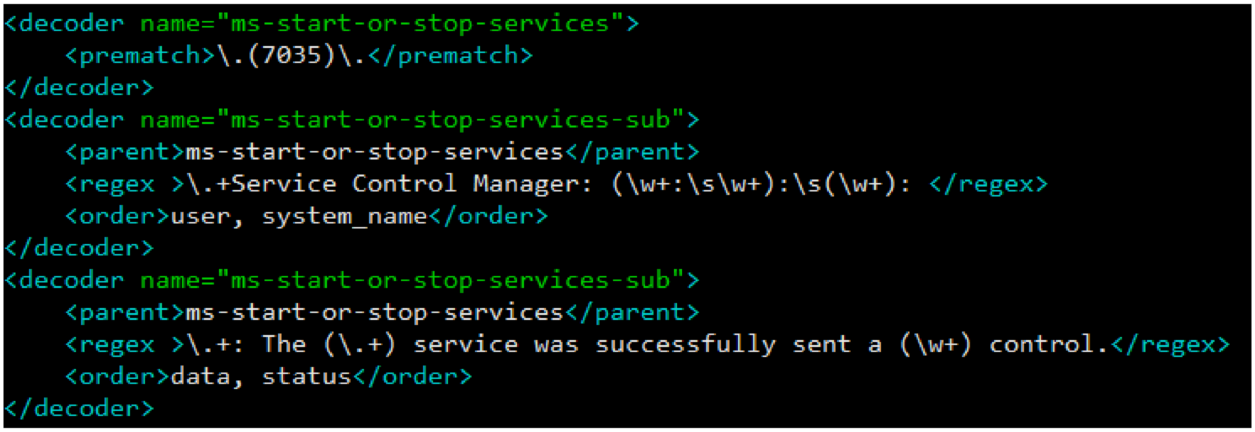
<7045>

```
WinEvtLog 2016 Sep 15 10:08:49  WinEvtLog: System:
INFORMATION(7045): Service Control Manager: Vo: Asus: Asus: A
service was installed  in the system.   Service Name:  TeamViewer  11
Service File Name:  "C:\Program Files
(x86)\TeamViewer\TeamViewer_Service.exe"   Service Type:  user mode
service  Service Start Type:  auto start  Service Account:  LocalSystem
```

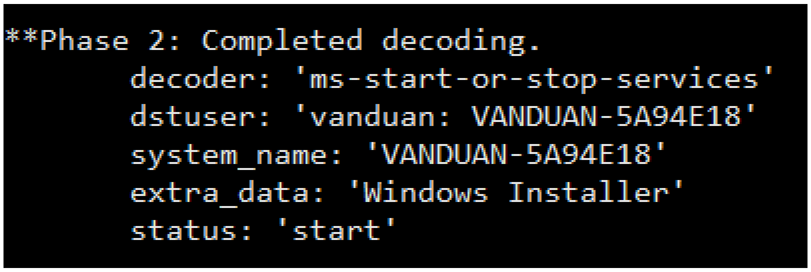
```
WinEvtLog 2016 Sep 15 11:11:21  WinEvtLog: System:
INFORMATION(7045): Service Control Manager: SYSTEM: NT
AUTHORITY: Asus: A service was installed  in the system.   Service Name:
Skype Updater  Service File Name:  "C:\Program Files
(x86)\Skype\Updater\Updater.exe"  Service Type:  user mode service
Service Start Type:  auto start  Service Account:  LocalSystem
```

- **Decoder**

<7035>

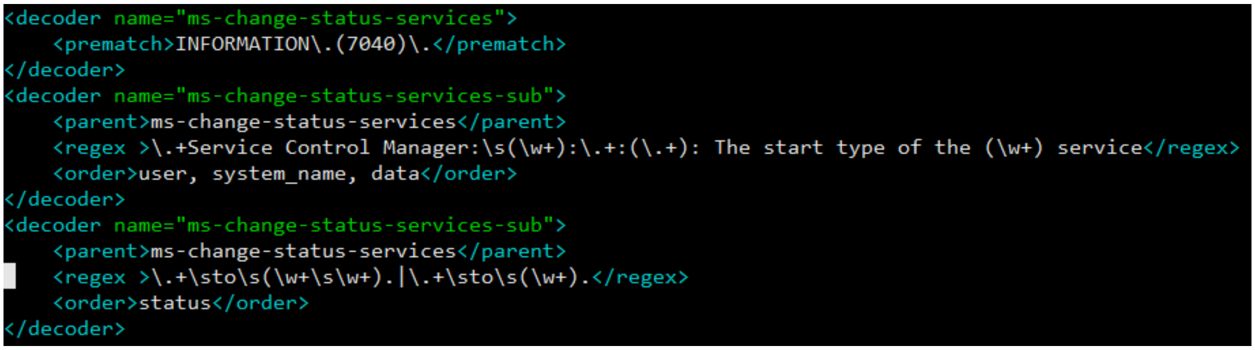


```
<decoder name="ms-start-or-stop-services">
    <prematch>\.(7035)\.</prematch>
</decoder>
<decoder name="ms-start-or-stop-services-sub">
    <parent>ms-start-or-stop-services</parent>
    <regex >\.+Service Control Manager: (\w+:\s\w+):\s(\w+): </regex>
    <order>user, system_name</order>
</decoder>
<decoder name="ms-start-or-stop-services-sub">
    <parent>ms-start-or-stop-services</parent>
    <regex >\.+: The (\.+) service was successfully sent a (\w+) control.</regex>
    <order>data, status</order>
</decoder>
```

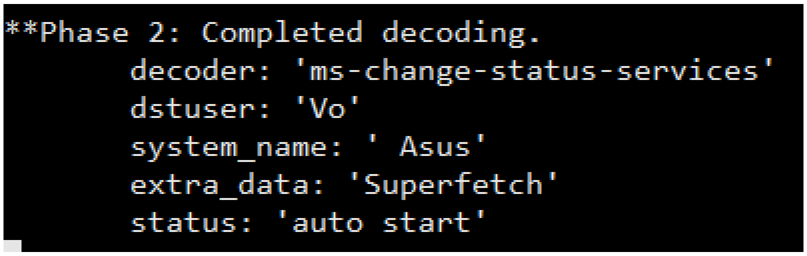


```
**Phase 2: Completed decoding.
       decoder: 'ms-start-or-stop-services'
       dstuser: 'vanduan: VANDUAN-5A94E18'
       system_name: 'VANDUAN-5A94E18'
       extra_data: 'Windows Installer'
       status: 'start'
```

<7040>

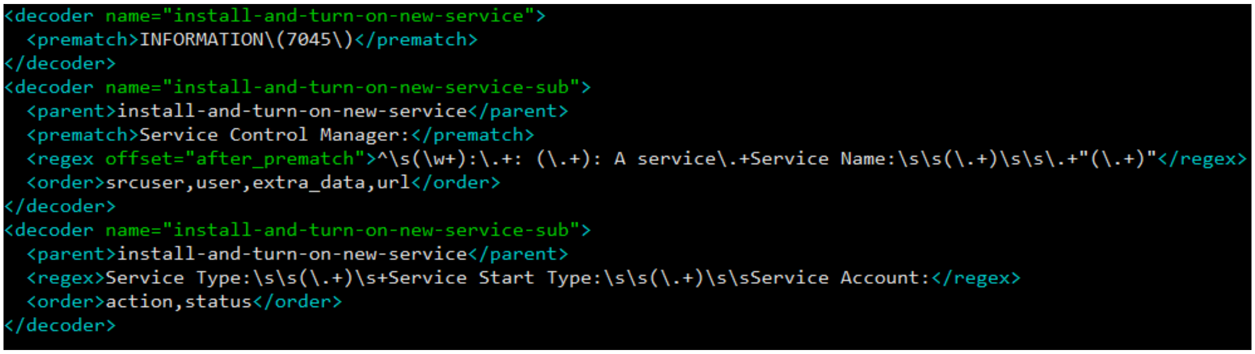


```
<decoder name="ms-change-status-services">
    <prematch>INFORMATION\.(7040)\.</prematch>
</decoder>
<decoder name="ms-change-status-services-sub">
    <parent>ms-change-status-services</parent>
    <regex >\.+Service Control Manager:\s(\w+):\.+:(\.+): The start type of the (\w+) service</regex>
    <order>user, system_name, data</order>
</decoder>
<decoder name="ms-change-status-services-sub">
    <parent>ms-change-status-services</parent>
    <regex >\.+\sto\s(\w+\s\w+).|\.+\sto\s(\w+).</regex>
    <order>status</order>
</decoder>
```

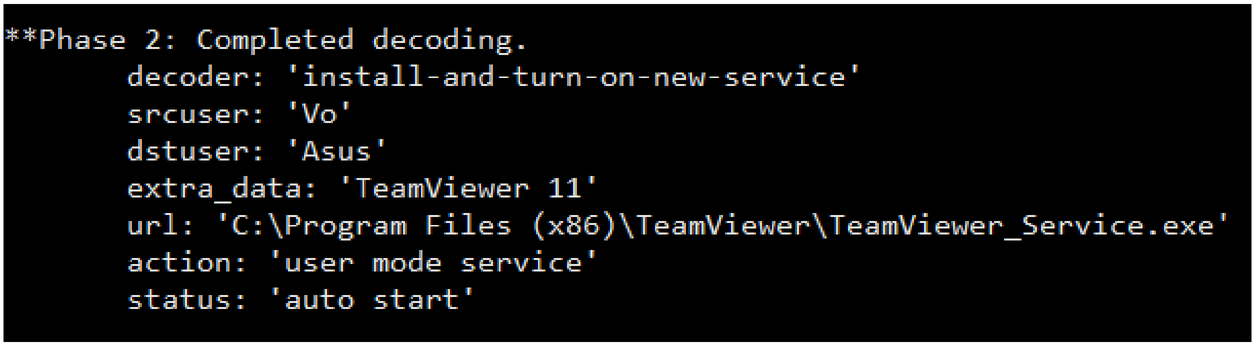


```
**Phase 2: Completed decoding.
       decoder: 'ms-change-status-services'
       dstuser: 'Vo'
       system_name: ' Asus'
       extra_data: 'Superfetch'
       status: 'auto start'
```

<7045>

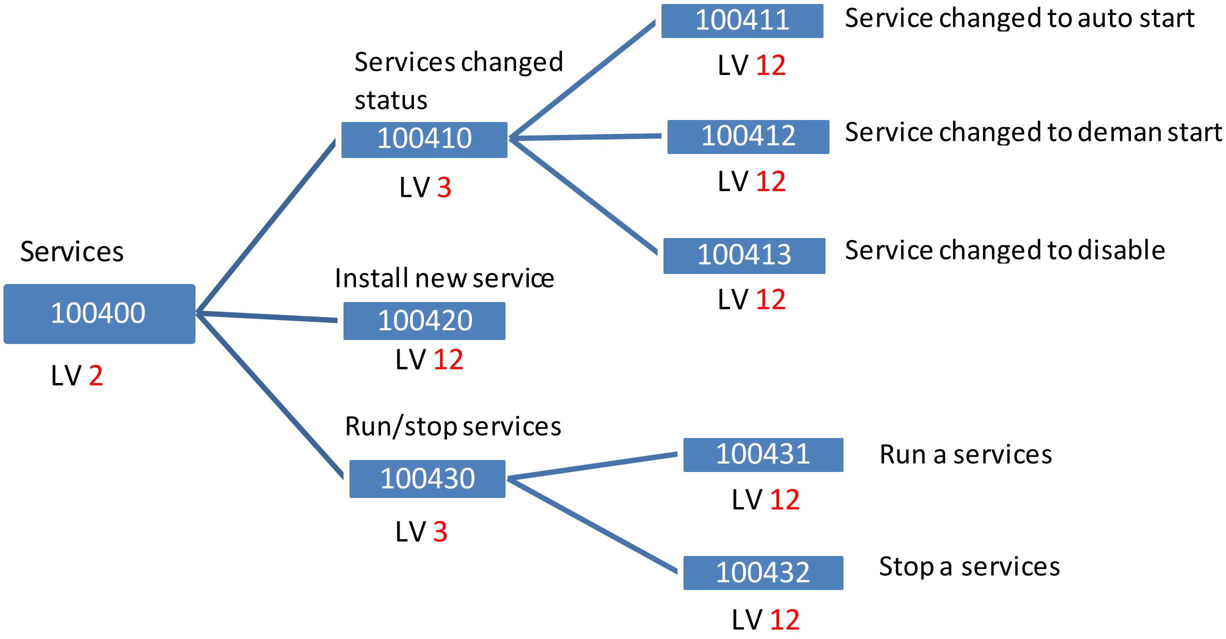


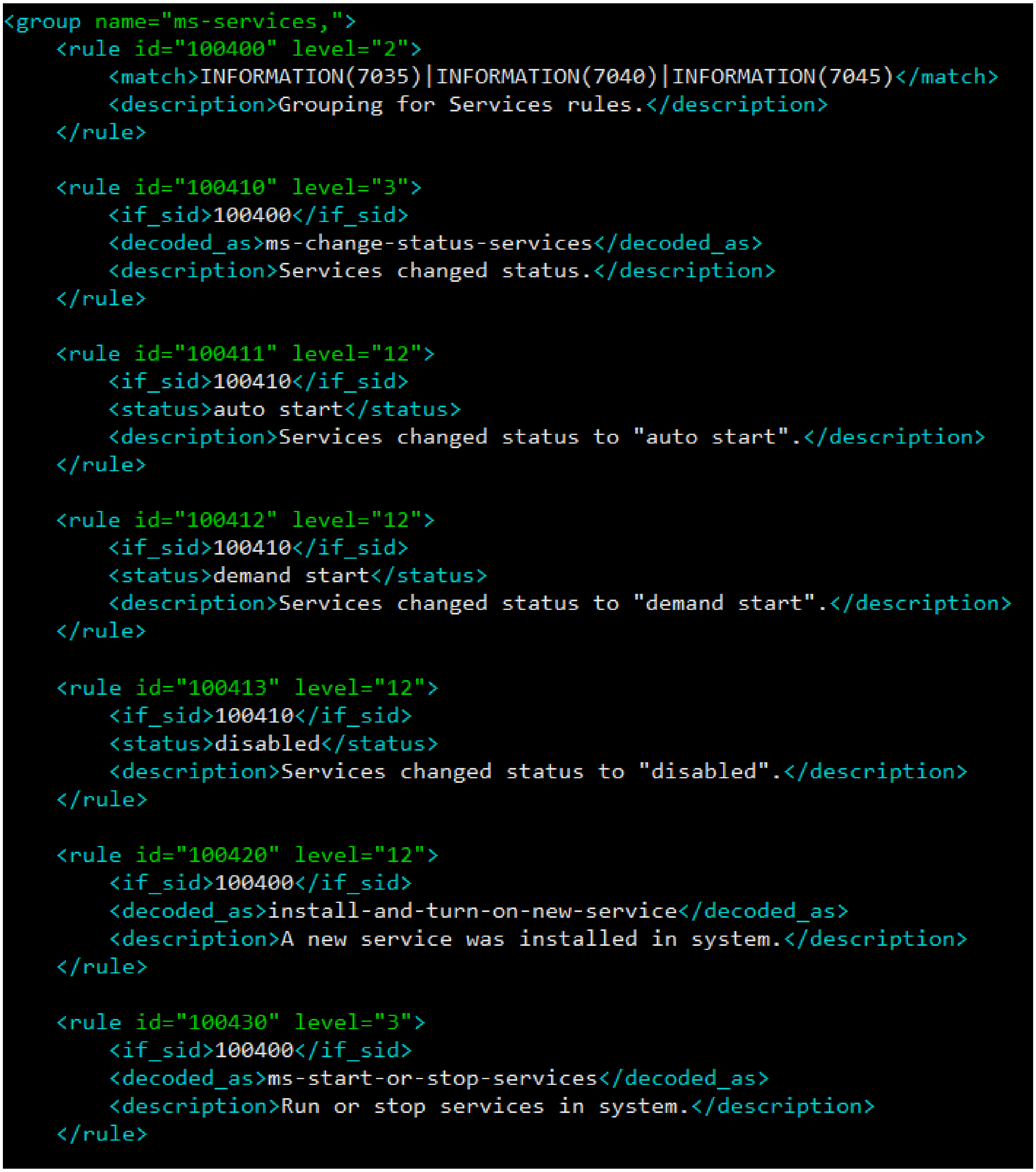
```
<decoder name="install-and-turn-on-new-service">
  <prematch>INFORMATION\(7045\)</prematch>
</decoder>
<decoder name="install-and-turn-on-new-service-sub">
  <parent>install-and-turn-on-new-service</parent>
  <prematch>Service Control Manager:</prematch>
  <regex offset="after_prematch">^\s(\w+):\.+: (\.+): A service\.+Service Name:\s\s(\.+)\s\s\.+"(\.+)"</regex>
  <order>srcuser,user,extra_data,url</order>
</decoder>
<decoder name="install-and-turn-on-new-service-sub">
  <parent>install-and-turn-on-new-service</parent>
  <regex>Service Type:\s\s(\.+)\s+Service Start Type:\s\s(\.+)\s\sService Account:</regex>
  <order>action,status</order>
</decoder>
```



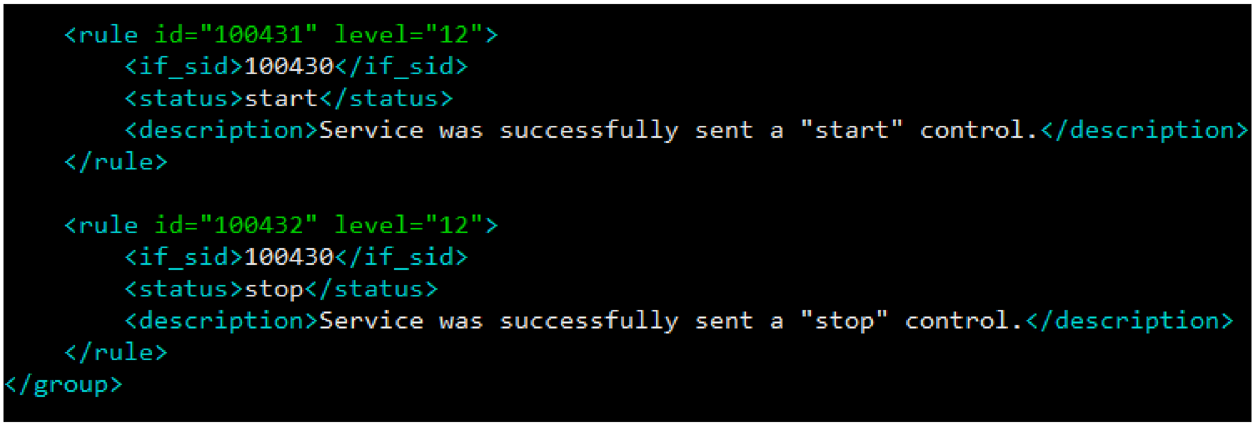
```
**Phase 2: Completed decoding.
       decoder: 'install-and-turn-on-new-service'
       srcuser: 'Vo'
       dstuser: 'Asus'
       extra_data: 'TeamViewer 11'
       url: 'C:\Program Files (x86)\TeamViewer\TeamViewer_Service.exe'
       action: 'user mode service'
       status: 'auto start'
```

❖ Rule





```
<group name="ms-services,">
    <rule id="100400" level="2">
        <match>INFORMATION(7035)|INFORMATION(7040)|INFORMATION(7045)</match>
        <description>Grouping for Services rules.</description>
    </rule>

    <rule id="100410" level="3">
        <if_sid>100400</if_sid>
        <decoded_as>ms-change-status-services</decoded_as>
        <description>Services changed status.</description>
    </rule>

    <rule id="100411" level="12">
        <if_sid>100410</if_sid>
        <status>auto start</status>
        <description>Services changed status to "auto start".</description>
    </rule>

    <rule id="100412" level="12">
        <if_sid>100410</if_sid>
        <status>demand start</status>
        <description>Services changed status to "demand start".</description>
    </rule>

    <rule id="100413" level="12">
        <if_sid>100410</if_sid>
        <status>disabled</status>
        <description>Services changed status to "disabled".</description>
    </rule>

    <rule id="100420" level="12">
        <if_sid>100400</if_sid>
        <decoded_as>install-and-turn-on-new-service</decoded_as>
        <description>A new service was installed in system.</description>
    </rule>

    <rule id="100430" level="3">
        <if_sid>100400</if_sid>
        <decoded_as>ms-start-or-stop-services</decoded_as>
        <description>Run or stop services in system.</description>
    </rule>
```



```
    <rule id="100431" level="12">
        <if_sid>100430</if_sid>
        <status>start</status>
        <description>Service was successfully sent a "start" control.</description>
    </rule>

    <rule id="100432" level="12">
        <if_sid>100430</if_sid>
        <status>stop</status>
        <description>Service was successfully sent a "stop" control.</description>
    </rule>
</group>
```