

# NS Project 1

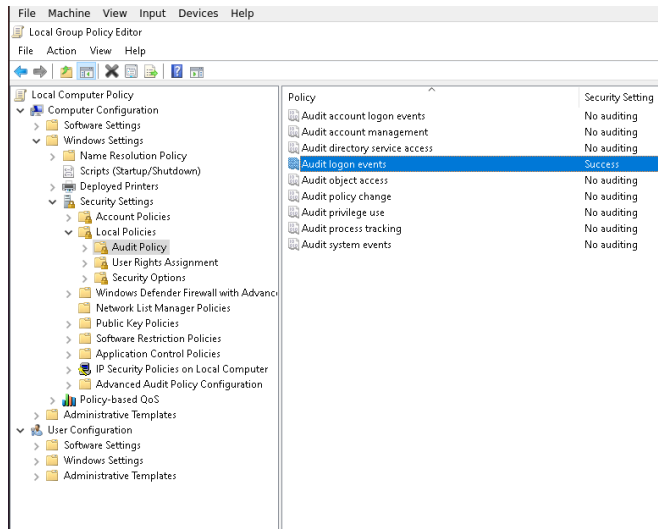
## 309551064 張凱翔

### Part A.

#### 2. Logoff:

a.

i.



@timestamp	fields.hostname	event.code	event.action	message
> Mar 27, 2021 @ 19:10:26.439	_309551064	4,634	logged-out	An account was logged off.  Subject: Security ID: S-1-5-90-0-3 Account Name: DWM-3 Account Domain: Window Manager Logon ID: 0x3A2AB4C

ii.

First, change the policy of “Audit logon events” to “Success” in “Local Group Policy Editor” to monitor the logon and logoff events as first image shown.

After logoff the account, there are log with event code “4634” in “Kibana”. As the “message” presented in second images, an account was logged off. In addition, the “event.action” of “Kibana” also shows “logged-out”.

b.

timestamp: convenience for me to find the latest log

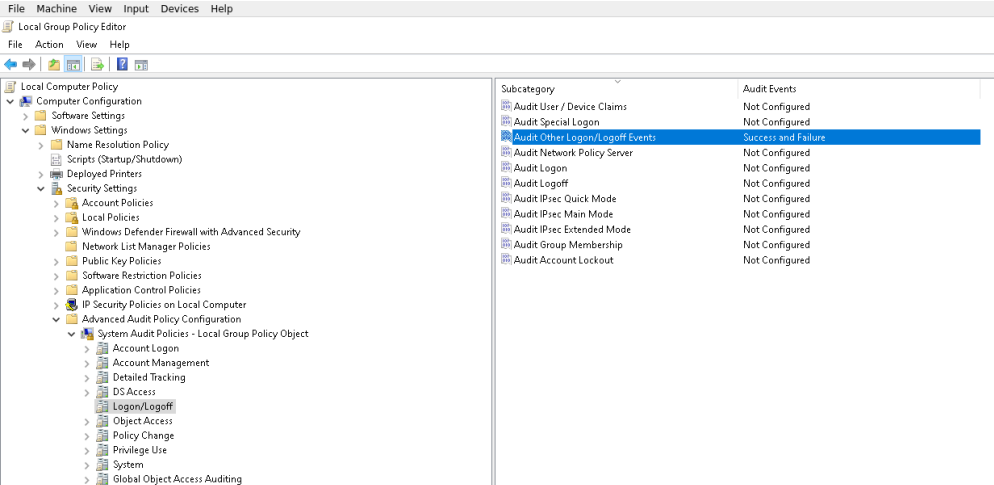
event.action: to see the category of action, and it is the same as category on “Local Group Policy Editor”

message: to see detailed information of log

### 3. Screensaver invoked:

a.

i.



The screenshot shows the 'Local Group Policy Editor' window. The left pane displays the 'Local Computer Policy' tree, expanded to 'System Audit Policies - Local Group Policy Object' > 'Logon/Logoff'. The right pane shows a list of audit events with their status. 'Audit Other Logon/Logoff Events' is highlighted and set to 'Success and Failure'.

Subcategory	Audit Events
Audit User / Device Claims	Not Configured
Audit Special Logon	Not Configured
Audit Other Logon/Logoff Events	Success and Failure
Audit Network Policy Server	Not Configured
Audit Logon	Not Configured
Audit Logoff	Not Configured
Audit IPsec Quick Mode	Not Configured
Audit IPsec Main Mode	Not Configured
Audit IPsec Extended Mode	Not Configured
Audit Group Membership	Not Configured
Audit Account Lockout	Not Configured

@timestamp	fields.hostname	event.code	event.action	message
> Mar 25, 2021 @ 01:05:17.657	_309551064	4,802	Other Logon/Logoff Events	The screen saver was invoked.  Subject: Security ID: S-1-5-21-1008724996-3079212715-1904677541-1001 Account Name: Endpoint Account Domain: DESKTOP-KKP8IJ8 Logon ID: 0xC3AC8

ii.

First, change the policy of “Audit Other Logon/Logoff Events” to “Success” in “Local Group Policy Editor” to monitor the screen saver event as first image shown.

After logoff the account, there are log with event code “4802” in “Kibana”. As the “message” presented in second images said, the screensaver was invoked.

b.

timestamp: convenience for me to find the latest log

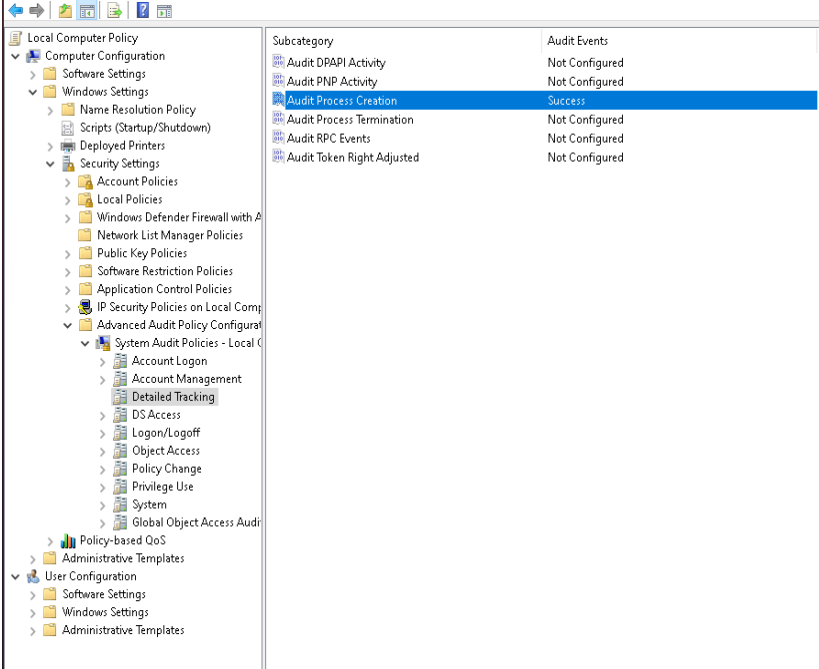
event.action: to see the category of action, and it is the same as category on “Local Group Policy Editor”

message: to see detailed information of log

## 5. Open a specific application:

a.

i.



The screenshot shows the 'Local Computer Policy' window. The left pane shows the tree structure expanded to 'System Audit Policies - Local Computer'. The right pane shows the 'Audit Process Creation' policy set to 'Success'. Below the screenshot is a table of log entries.

@timestamp	fields.hostname	event.code	event.action	process.name	message
> Mar 27, 2021 @ 19:47:44.480	_309551064	4,688	created-process	calc.exe	A new process has been created. Creator Subject: Security ID: S-1-5-21-1008724996-3079212715-1904677541-1001 Account Name: Endpoint Account Domain: DESKTOP-KXP0IJ8 Logon ID: 0x404EE6A

ii.

First, change the policy of “Audit Process Creation” to “Success” in “Local Group Policy Editor” to monitor the event of creating process as first image shown.

After open “cal.exe”, there are log with event code “4688” in “Kibana”. As the “message” presented in second images said, a new process has been created and the “process.name” is “cal.exe”.

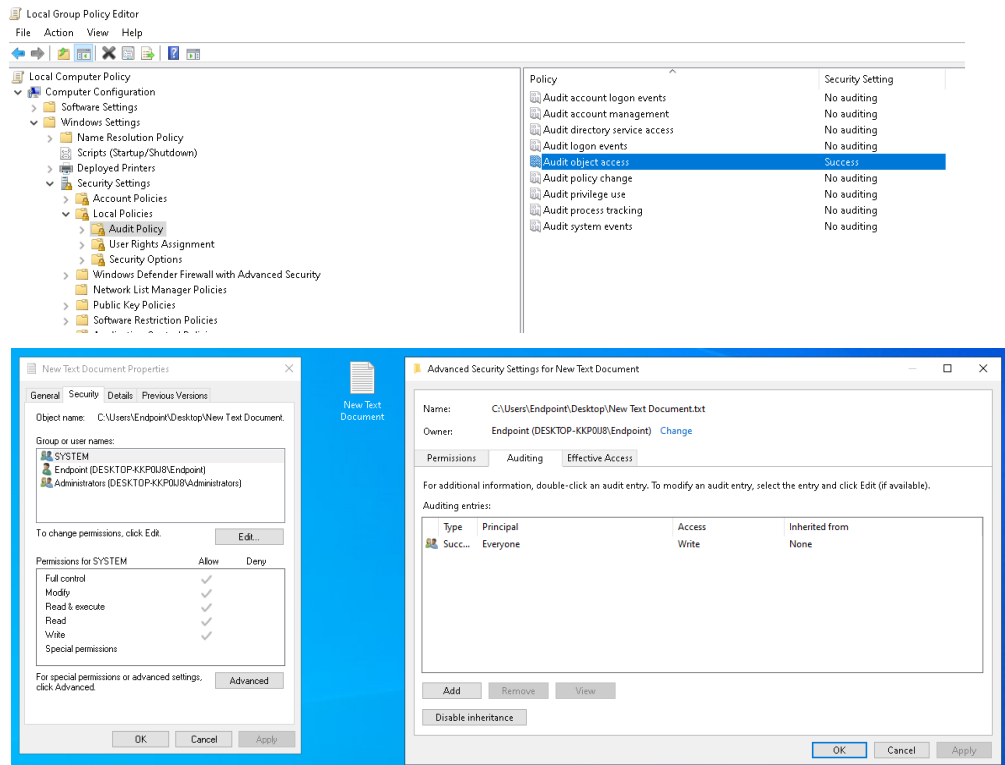
b.

timestamp: convenience for me to find the latest log  
event.action: to see the category of action, and it is the same as category on “Local Group Policy Editor”  
process.name: to see the name of the new process  
message: to see detailed information of log

## 8. Modify a file:

a.

i.



@timestamp	fields.hostname	event.code	winlog.event_data.ObjectName
Mar 27, 2021 @ 20:25:59.367	_309551064	4,656	C:\Users\Endpoint\Desktop\New Text Document.txt

ii.

First, change the policy of “Audit object access” to “Success” in “Local Group Policy Editor” to monitor the event of modifying files as first image shown. Then, audit the security policy of the file which would be modified as second image shown.

After modifying “New Text Document.txt”, there are log with event code “4656” in “Kibana”. As the information presented in third images said, the “ObjectName” is “New Text Document.txt”.

b.

timestamp: convenience for me to find the related log in event viewer and Kibana

winlog.event\_data.ObjectName: to see the file being changed

9. DNS query:

a.

i.

@timestamp ▾	fields.hostname	event.code	dns.op_code	dns.question.name
> Mar 27, 2021 @ 23:20:22.286	_309551064	-	QUERY	8.8.8.8.in-addr.arpa

ii.

After use command “nslookup 8.8.8.8”, there are new log in “Kibana”. As the information presented in first images said, the “dns.op\_code” is “Query” and the “dns.question.name” “8.8.8.8”is the same I query.

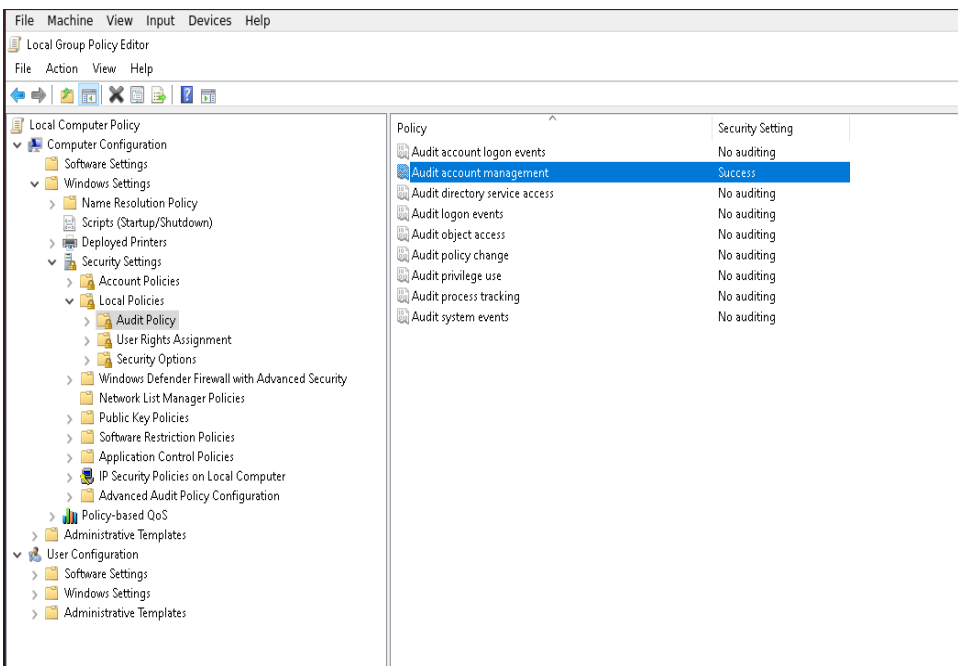
b.

- timestamp: convenience for me to get the latest log
- dns.op\_code: to see the type of dns message
- dns.question.name: to search the log which I query

## 11. Change password:

a.

i.



The screenshot shows the 'Local Group Policy Editor' window. The left pane shows the tree structure with 'Local Computer Policy' expanded, and 'Security Settings' > 'Local Policies' > 'Audit Policy' selected. The right pane shows a list of policies with 'Audit account management' highlighted, showing a 'Success' security setting.

@timestamp	fields.hostname	event.code	event.action	message x <
> Mar 27, 2021 @ 20:48:25.076	_309551064	4,738	modified-user-account	A user account was changed.

ii.

First, change the policy of “Audit account management” to “Success” in “Local Group Policy Editor” to monitor the event of account management as first image shown.

After change the account password, there are log with event code “4738” in “Kibana”. As the information presented in second images said, the “event.action” is “modified-user-account” and the detailed message shows “A user account was changed” .

b.

timestamp: convenience for me to find the related log in event viewer and Kibana

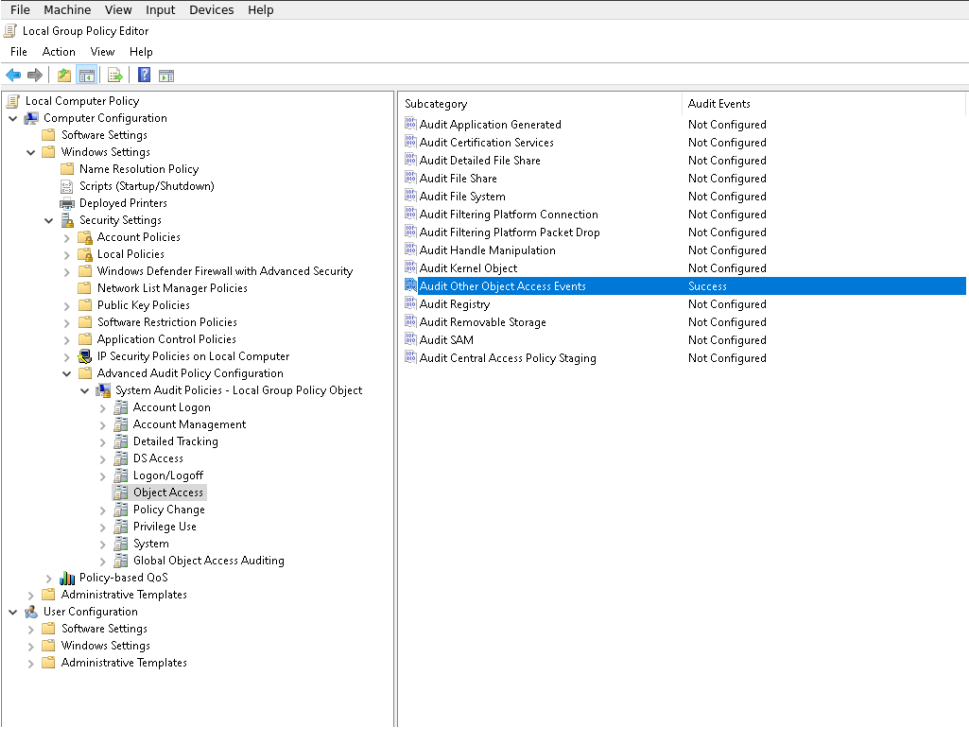
event.action: to see the category of action, and it is the same as category on “Local Group Policy Editor”

message: to see the detailed information

## 14. Scheduled task:

a.

i.



The screenshot shows the Local Group Policy Editor window. In the left-hand tree, the path is: Local Computer Policy > Computer Configuration > Windows Settings > Security Settings > Local Policies > Windows Defender Firewall with Advanced Security > Network List Manager Policies > Public Key Policies > Software Restriction Policies > Application Control Policies > IP Security Policies on Local Computer > Advanced Audit Policy Configuration > System Audit Policies - Local Group Policy Object > Object Access. The 'Object Access' policy is selected. In the right-hand pane, the 'Audit Other Object Access Events' subcategory is highlighted, and its audit event is set to 'Success'.

@timestamp	fields.hostname	event.code	event.action	winlog.event_data.TaskName	message
Mar 23, 2021 @ 06:28:12.019	_309551064	4,698	scheduled-task-created	\1	A scheduled task was created.  Subject: Security ID: S-1-5-21-1008724996-3079212715-1904677541-1001 Account Name: Endpoint Account Domain: DESKTOP-KKP8IJ8 Logon ID: 0x3E3AC

ii.

First, change the policy of “Audit Other Object Access events” to “Success” in “Local Group Policy Editor” to monitor the event of schedule task as first image shown.

After using the command in pdf with task name “1”, there are log with event code “4698” in “Kibana”. As the information presented in second images said, the “event.action” is “scheduled-task-created” and the detailed message also shows that a scheduled task was created and the “TaskName” is “1” the same I created.

b.

timestamp: convenience for me to find the related log in event viewer and Kibana

event.action: to see the category of action, and it is the same as category on “Local Group Policy Editor”

winlog.event\_data.TaskName: to see the task name

message: to see the detailed information

**Part B.**

This is my first time to use all the tool in this project and see the log information in Windows OS. I feel this is quite interesting and a sense of accomplishment to trigger the scenario and find the corresponding log in “Kibana”. However, some problems occurred when I was configuring the setup of “logwinbeat”. I could not set up the service successfully. After going through the issue in github. I figured out the problem and successfully set up both tools.