1.1 Logging and Alerting

Logging is only created in the event logs. A custom task must be created to trigger the event log information and log it in a log file.

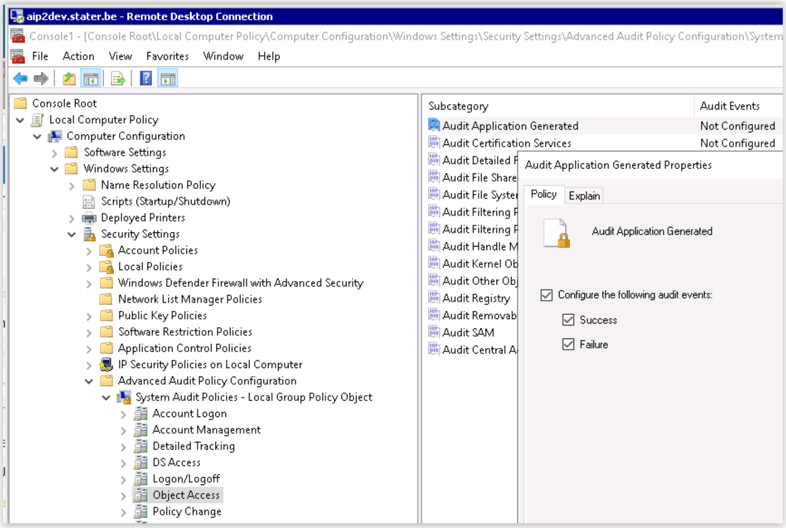
The script can be found in D:\logging\ReadEventlogs.vbs on every ADFS server.

1.1.1 Prerequisites

The 2019 server is by default allowing to save credentials. Otherwise a scheduled task will not work.

A service account must be created with limited rights: _sp_p(q)_AdfsLogging@xxx.xx
The service account on the ADFS server must have rights to:

- Read Event logs: Add user to Local group “Event log readers”.
- Start a Scheduled Task: Add the user to the local group “Performance logs users”.
- Modify rights on the folder D:\logging



aip2dev.stater.be - Remote Desktop Connection

Console1 - [Console Root\Local Computer Policy\Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System

- Console Root
  - Local Computer Policy
    - Computer Configuration
      - Software Settings
      - Windows Settings
        - Name Resolution Policy
        - Scripts (Startup/Shutdown)
        - Deployed Printers
        - Security Settings
          - Account Policies
          - 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
              - Account Logon
              - Account Management
              - Detailed Tracking
              - DS Access
              - Logon/Logoff
              - Object Access
              - Policy Change

Subcategory	Audit Events
Audit Application Generated	Not Configured
Audit Certification Services	Not Configured
Audit Detailed F	
Audit File Share	
Audit File Syster	
Audit Filtering F	
Audit Filtering F	
Audit Handle M	
Audit Kernel Ob	
Audit Other Obj	
Audit Registry	
Audit Removab	
Audit SAM	
Audit Central A	

Audit Application Generated Properties

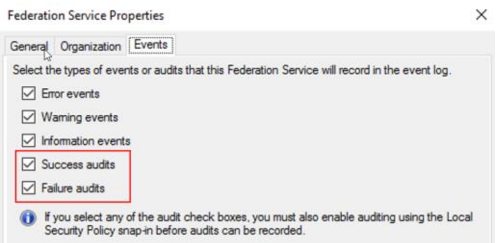
Audit Application Generated

☑ Configure the following audit events:

☑ Success

☑ Failure

Enable Object Access “Success” and “Failure” in the local group policy (restart server)



Federation Service Properties

Select the types of events or audits that this Federation Service will record in the event log.

☑ Error events

☑ Warning events

☑ Information events

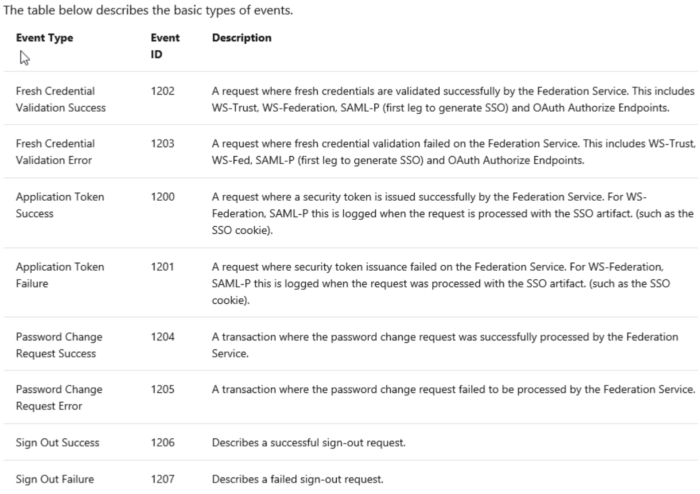
☑ Success audits

☑ Failure audits

If you select any of the audit check boxes, you must also enable auditing using the Local Security Policy snap-in before audits can be recorded.

Enable “Success audits” and “Failure audits” in the properties of the ADFS service.

https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/troubleshooting/ad-fs-tshoot-logging

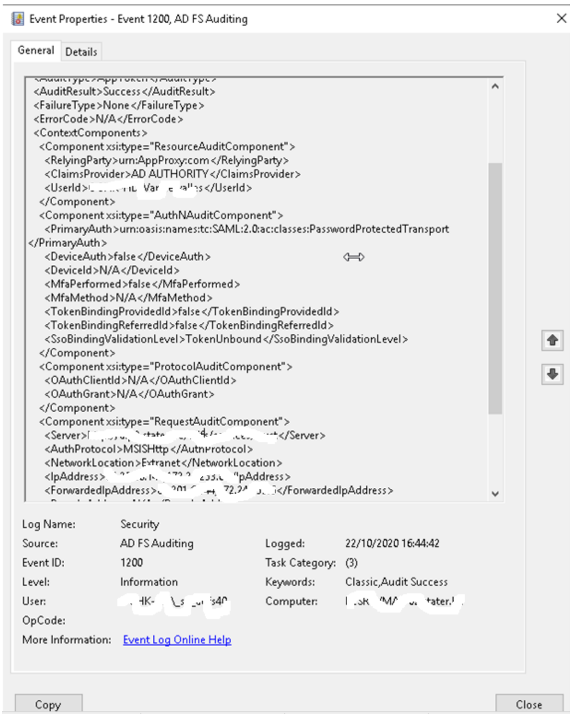


The table below describes the basic types of events.

Event Type	Event ID	Description
Fresh Credential Validation Success	1202	A request where fresh credentials are validated successfully by the Federation Service. This includes WS-Trust, WS-Federation, SAML-P (first leg to generate SSO) and OAuth Authorize Endpoints.
Fresh Credential Validation Error	1203	A request where fresh credential validation failed on the Federation Service. This includes WS-Trust, WS-Fed, SAML-P (first leg to generate SSO) and OAuth Authorize Endpoints.
Application Token Success	1200	A request where a security token is issued successfully by the Federation Service. For WS-Federation, SAML-P this is logged when the request is processed with the SSO artifact. (such as the SSO cookie).
Application Token Failure	1201	A request where security token issuance failed on the Federation Service. For WS-Federation, SAML-P this is logged when the request was processed with the SSO artifact. (such as the SSO cookie).
Password Change Request Success	1204	A transaction where the password change request was successfully processed by the Federation Service.
Password Change Request Error	1205	A transaction where the password change request failed to be processed by the Federation Service.
Sign Out Success	1206	Describes a successful sign-out request.
Sign Out Failure	1207	Describes a failed sign-out request.

1.1.2 Eventlog Trigger

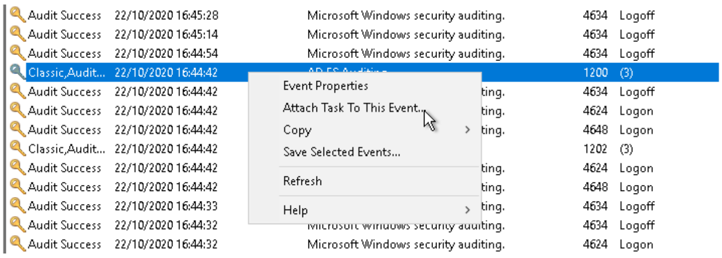
EventID 1200 shows which user is logged on for a specific application, from which WAP server, and which IP address, internal or external.



```
 <AuditResult>Success</AuditResult>
 <FailureType>None</FailureType>
 <ErrorCode>N/A</ErrorCode>
 <ContextComponents>
  <Component xsi:type="ResourceAuditComponent">
   <RelyingParty>urn:AppProxy:com</RelyingParty>
   <ClaimsProvider>AD AUTHORITY</ClaimsProvider>
   <UserId>[redacted]</UserId>
  </Component>
  <Component xsi:type="AuthNAuditComponent">
   <PrimaryAuth>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
</PrimaryAuth>
   <DeviceAuth>false</DeviceAuth>
   <DeviceId>N/A</DeviceId>
   <MfaPerformed>false</MfaPerformed>
   <MfaMethod>N/A</MfaMethod>
   <TokenBindingProvidedId>false</TokenBindingProvidedId>
   <TokenBindingReferredId>false</TokenBindingReferredId>
   <SsoBindingValidationLevel>TokenUnbound</SsoBindingValidationLevel>
  </Component>
  <Component xsi:type="ProtocolAuditComponent">
   <OAuthClientId>N/A</OAuthClientId>
   <OAuthGrant>N/A</OAuthGrant>
  </Component>
  <Component xsi:type="RequestAuditComponent">
   <Server>[redacted]</Server>
   <AuthProtocol>MSISHttp</AutnProtocol>
   <NetworkLocation>Extranet</NetworkLocation>
   <IpAddress>[redacted]pAddress>
   <ForwardedIpAddress>[redacted]</ForwardedIpAddress>
```

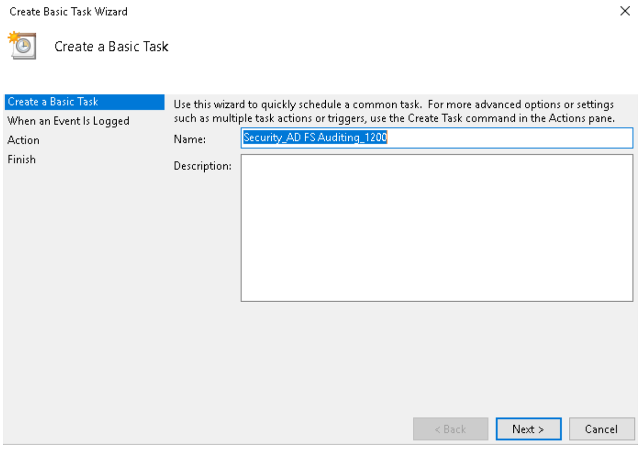
Log Name:	Security		
Source:	AD FS Auditing	Logged:	22/10/2020 16:44:42
Event ID:	1200	Task Category:	(3)
Level:	Information	Keywords:	Classic,Audit Success
User:	[redacted]	Computer:	[redacted]
OpCode:			
More Information:	Event Log Online Help		

This information must be stored in a log file.



```
Audit Success    22/10/2020 16:45:28    Microsoft Windows security auditing.    4634  Logoff
Audit Success    22/10/2020 16:45:14    Microsoft Windows security auditing.    4634  Logoff
Audit Success    22/10/2020 16:44:54    Microsoft Windows security auditing.    4634  Logoff
Classic,Audit... 22/10/2020 16:44:42                                            1200  (3)
Audit Success    22/10/2020 16:44:42                                    ting.   4634  Logoff
Audit Success    22/10/2020 16:44:42                                    ting.   4624  Logon
Audit Success    22/10/2020 16:44:42                                    ting.   4648  Logon
Classic,Audit... 22/10/2020 16:44:42                                            1202  (3)
Audit Success    22/10/2020 16:44:42                                    ting.   4624  Logon
Audit Success    22/10/2020 16:44:42                                    ting.   4648  Logon
Audit Success    22/10/2020 16:44:33                                    ting.   4634  Logoff
Audit Success    22/10/2020 16:44:32                                            4634  Logoff
Audit Success    22/10/2020 16:44:32    Microsoft Windows security auditing.    4624  Logon
```

Right click on EventID 1200 / Attach Task to This Event…



Create Basic Task Wizard

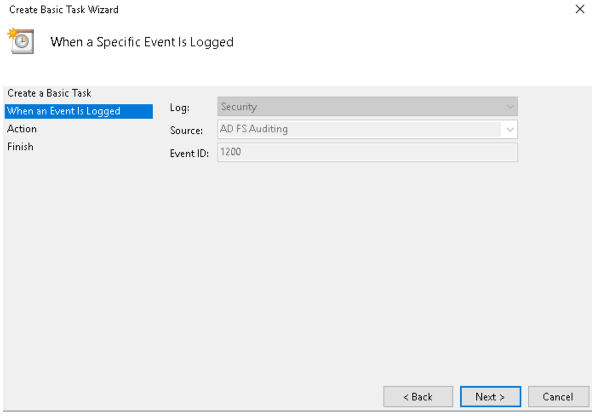
Create a Basic Task

Use this wizard to quickly schedule a common task. For more advanced options or settings such as multiple task actions or triggers, use the Create Task command in the Actions pane.

Name: Security_AD FS Auditing_1200

Description:

Leave the default, click on Next



Create Basic Task Wizard

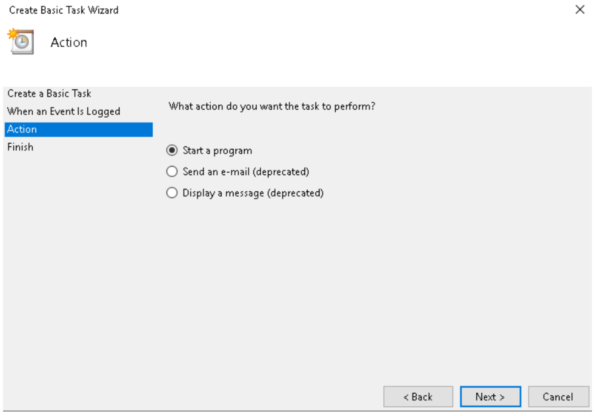
When a Specific Event Is Logged

Log: Security

Source: AD FS Auditing

Event ID: 1200

/Next



Create Basic Task Wizard

Action

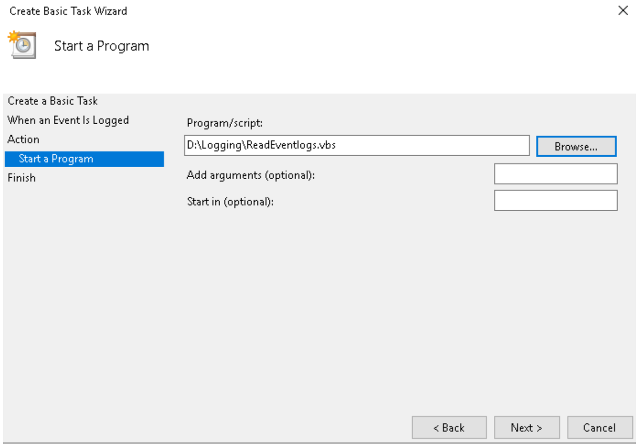
What action do you want the task to perform?

● Start a program

○ Send an e-mail (deprecated)

○ Display a message (deprecated)

/Next



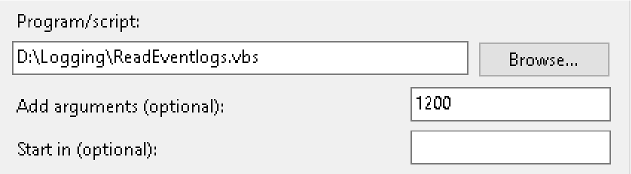
Create Basic Task Wizard

Start a Program

Program/script: D:\Logging\ReadEventlogs.vbs

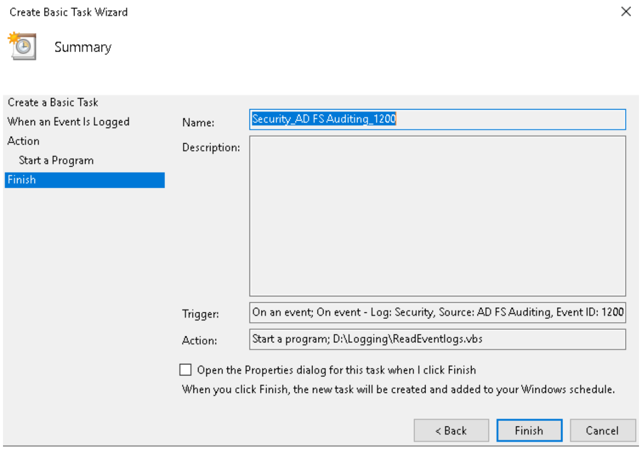
Add arguments (optional):

Start in (optional):


Program/script:
D:\Logging\ReadEventlogs.vbs

Add arguments (optional): 1200
Start in (optional):

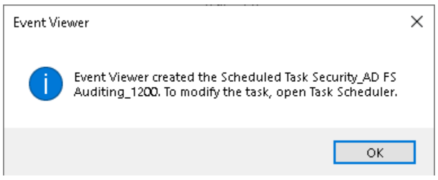
Browse to D:\logging\ReadEventlogs.vbs. Add arguments (optional) = 1200 (number of EventID) /Next


Create Basic Task Wizard

Summary

Name: Security_AD FS Auditing_1200
Description:
Trigger: On an event; On event - Log: Security, Source: AD FS Auditing, Event ID: 1200
Action: Start a program; D:\Logging\ReadEventlogs.vbs
□ Open the Properties dialog for this task when I click Finish
When you click Finish, the new task will be created and added to your Windows schedule.

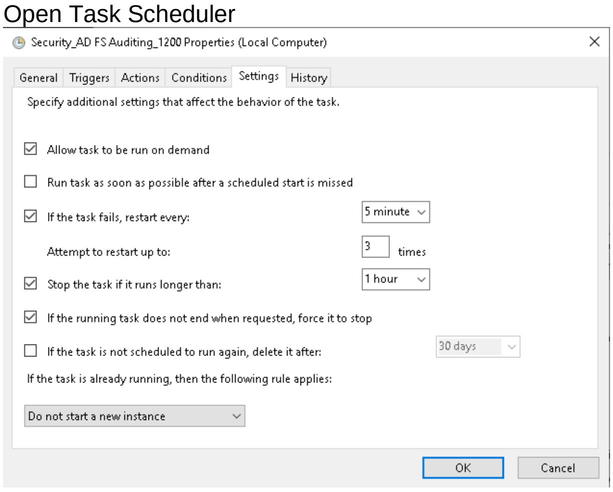
Click on ‘Finish’


Event Viewer

Event Viewer created the Scheduled Task Security_AD FS Auditing_1200. To modify the task, open Task Scheduler.

Click on ‘OK’

Open Task Scheduler


Security_AD FS Auditing_1200 Properties (Local Computer)

Specify additional settings that affect the behavior of the task.

☑ Allow task to be run on demand

□ Run task as soon as possible after a scheduled start is missed

☑ If the task fails, restart every: 5 minute

Attempt to restart up to: 3 times

☑ Stop the task if it runs longer than: 1 hour

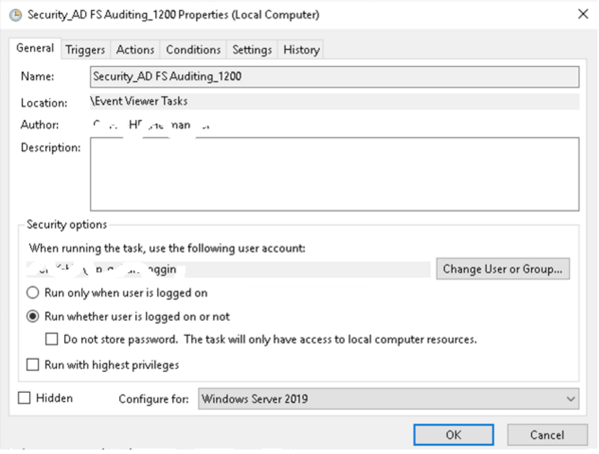
☑ If the running task does not end when requested, force it to stop

□ If the task is not scheduled to run again, delete it after: 30 days

If the task is already running, then the following rule applies:

Do not start a new instance

Fill in the above values



Security_AD FS Auditing_1200 Properties (Local Computer)

Name: Security_AD FS Auditing_1200

Location: \Event Viewer Tasks

Author: [redacted]

Description:

Security options

When running the task, use the following user account:

[redacted]

○ 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 Server 2019

Run whether user is logged on or not
Configure for: Windows Server 2019
Service account _sp_AdfsLog@xxx.xx

Now to this for EventID 1201, 1203, 1206 and 1210 (PS.: 1210 is a locked user)
For EventID 364 you need to select a specific VBS file: ReadEventlog364.vbs
EventID can contain a lot of information. Currently 2 specific 364 events are implemented in the script.