TLP:GREEN

OR-10 CONFIGURATIEHANDLEIDING

Monitoring & Detectie – SOC Operational Readiness – **Log audit policies**

Best Practice versie 1.2

Complexiteit document
Eenvoudig

Samenwerken maakt

DIGITAAL VEILIGER

VSSR

Inhoudsopgave

Voorwoord

De Rijksoverheid verwerkt grote hoeveelheden gevoelige informatie en is daarmee een interessant en gewild doelwit. Cybercriminelen en statelijke actoren zoeken naar kwetsbaarheden om zich zo toegang te verschaffen tot de supplychain, netwerken, systemen en (gevoelige) informatie.

De wereld van cyberdreigingen verandert snel en vraagt om gezamenlijke inspanning om weerbaar te zijn. Dit vraagt om samen te werken aan breder toegepaste én verbeterde SOC-dienstverlening. Het programma Versterken SOC Stelsel Rijk (VSSR) is opgezet om hieraan bij te dragen.

Een belangrijk onderdeel van SOC-diensten zijn de monitoring- en detectiediensten. Deze zijn erop gericht om een veelheid aan loggegevens en andere (meta-)datastromen afkomstig van de IT-infrastructuur, randapparatuur, bedrijfsapplicaties en andere dataverwerkingen in een organisatie te analyseren, aggregeren en correleren. Monitoring en detectiesystemen kunnen op basis hiervan verdachte gedragingen detecteren en alarm slaan.

Om een SOC effectief en doelmatig in te zetten is het noodzakelijk dat er een aantal onderwerpen binnen een organisatie zijn ingericht. VSSR levert diverse producten die rijksorganisaties ondersteunen bij het inrichten van een SOC en de daarvoor benodigde randvoorwaarden.

Achtergrond

VSSR levert verschillende kennisproducten. Dit document maakt onderdeel uit van een set van miniproducten die rijksorganisaties helpt om een aantal SOC operationele randvoorwaarden in te richten.

Doelgroep

Versterken SOC Stelsel Rijk (VSSR) biedt met dit document handvatten voor Windows IT-beheerders, Systeemeigenaren, IT-Assetmanagers, Uitbestedingsmanagers, Security vertegenwoordigers en functionarissen betrokken bij informatiebeveiliging.

1. Documentgegevens

1.1 Documenthistorie

Versie	Datum	Omschrijving
V1.0	21-03-2025	Initiële versie
V1.1	03-11-2025	Toevoeging "Bijlage I – Configuratiestatus checklist"
V1.2	08-07-2026	Referenties geactualiseerd

1.2 Referenties

Document	Link
Checklist basisbeveiliging (OR-5)	Zie "Checklist basisbeveiliging ..(OR-5)" onder SOC Operational Readiness (Configuratie & Logging)
Log audit policies – Implementatiehandleiding (OR-10)	Zie "Log audit policies – Implementatiehandleiding (OR-10)" onder SOC Operational Readiness (Configuratie & Logging)
VSSR-kennisdocumenten	VSSR (ncsc.nl)

1.3 Definities

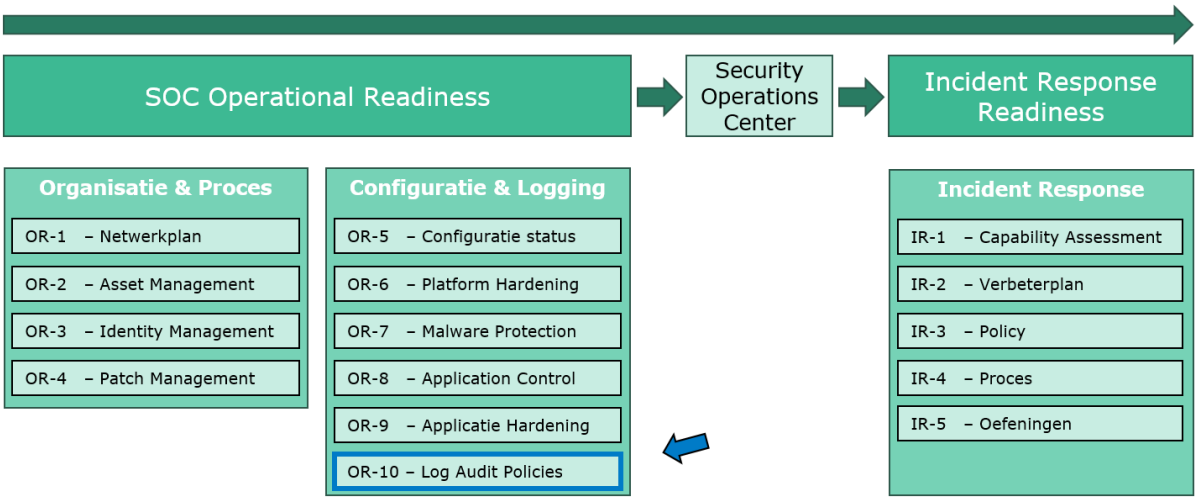
Ter verduidelijking van de terminologie en begrippen die in dit document worden gebruikt is er een verzameling van definities te vinden op Woordenboek - Cyberveilig Nederland.

2. Context miniproducten

Dit document maakt onderdeel uit van de SOC Readiness Assistance **miniproducten**. De SOC Readiness Assistance miniproducten ondersteunen uw organisatie bij de voorbereidingen die nodig zijn voor het optimaal benutten van een SOC(-dienst). Deze producten hebben een samenhangende opbouw maar kunnen ook los van elkaar worden gebruikt. De producten zijn in drie groepen te verdelen:

1) **Organisatie & Proces:** Helpt bij het inrichten van processen met als doel het SOC van de juiste informatie te voorzien om goed te kunnen monitoren.
2) **Configuratie & Logging:** Helpt bij het inrichten van basisbeveiliging met als doel om beter beschermd te zijn en de juiste logdata bij een SOC aan te kunnen leveren.
3) **Incident Response:** Met behulp van monitoring & Detectie zal een SOC security melding genereren. De Incident Response producten helpen bij het inrichten van de opvolging van deze meldingen binnen uw organisatie.

Onderstaande weergave toont dit document als onderdeel van **Configuratie & Logging** in het VSSR-Minipoducten raamwerk.



Figuur 1 - Dit document als onderdeel van het VSSR-Miniproducten raamwerk

De twee productgroepen behorende bij *SOC Operational Readiness* bestaan telkens uit een vergelijkbare set document die in figuur 1 per groep zijn weergegeven. Niet elk product bestaat uit exact de zelfde componenten maar veelal wordt de zelfde structuur gebruikt waarbij dit document de configuratiehandleiding is voor Log audit policies (OR-10), binnen **Configuratie & Logging**, behandelt.

3. Inleiding

In de hedendaagse digitale wereld, waar systemen voortdurend worden blootgesteld aan bedreigingen, speelt het implementeren van audit policies een cruciale rol in het beschermen van IT-infrastructuur. Deze policies helpen organisaties bij het vastleggen en analyseren van verdachte gedragingen en ongeautoriseerde toegangspogingen, wat essentieel is voor SOC-readiness.

3.1 Doel en Reikwijdte

Het doel van deze handleiding is het definiëren en configureren van geavanceerde audit policies op systemen zoals Windows-werkplekken, Windows Servers, Active Directory en Linux. Dit helpt organisaties zich voor te bereiden op SOC-readiness door monitoring en logbeheer te verbeteren.

3.2 Uitgangspunt en Resultaat

Het instellen van gedetailleerde audit policies stelt organisaties in staat om verdachte activiteiten te detecteren, vast te leggen en te analyseren. Door een goed auditbeleid te implementeren, inclusief passende retentieperioden voor loggegevens, kunnen organisaties voldoen aan wettelijke eisen en beter reageren op beveiligingsincidenten. Dit vormt een solide basis voor een sterker beveiligde IT-omgeving en betere SOC-readiness

4. Configureren van audit policies

Aanvullende audit policies zijn essentiële configuraties die verder gaan dan de standaard logginginstellingen en helpen om meer gedetailleerde en specifieke systeemgebeurtenissen vast te leggen. Waar standaard logbestanden een basisregistratie bieden van systeemgebeurtenissen, zijn aanvullende audit policies noodzakelijk om te voldoen aan strenge compliance-eisen en om diepgaand inzicht te verkrijgen vanuit een incident response of forensisch onderzoeksperspectief.

Met behulp van geavanceerde auditinstellingen kunnen kritieke activiteiten effectief worden gemonitord, zoals:

- Succesvolle en mislukte inlogpogingen
- Wijzigingen in gebruikersrechten en machtigingen
- Services en procesactiviteiten
- Toegang tot gevoelige bestanden en configuraties
- Wijzigingen in het systeemregister
- Specifieke netwerkactiviteiten

Deze extra log-events zorgen voor een gedetailleerder beeld van een systeemactiviteit, waardoor aanvallen sneller kunnen worden gedetecteerd en er adequaat op kan worden gereageerd.

4.1 Audit Policies voor Windows

Dit hoofdstuk richt zich op Windows-systemen zonder Endpoint Detection and Response (EDR)-oplossingen, zoals Microsoft Defender for Endpoint. Voor dergelijke systemen is het essentieel om geavanceerde audit policies te configureren om inzicht te krijgen in systeemactiviteiten, compliance te waarborgen, en incidentrespons te ondersteunen.

Let op: Als er wel een EDR-oplossing actief is, controleer dan welke inzichten al via de EDR beschikbaar zijn. Veel EDR-oplossingen loggen en monitoren uitgebreide activiteiten, zoals inlogpogingen, privilegegebruik, en wijzigingen aan beveiligingsinstellingen. Hierdoor kan het zijn dat bepaalde configuraties uit de onderstaande categorieën overbodig worden of dat ze dubbel worden gelogd, wat extra opslagruimte en verwerkingskracht vraagt. Stem in dat geval de audit policies af op de aanvullende waarde die de EDR niet biedt.

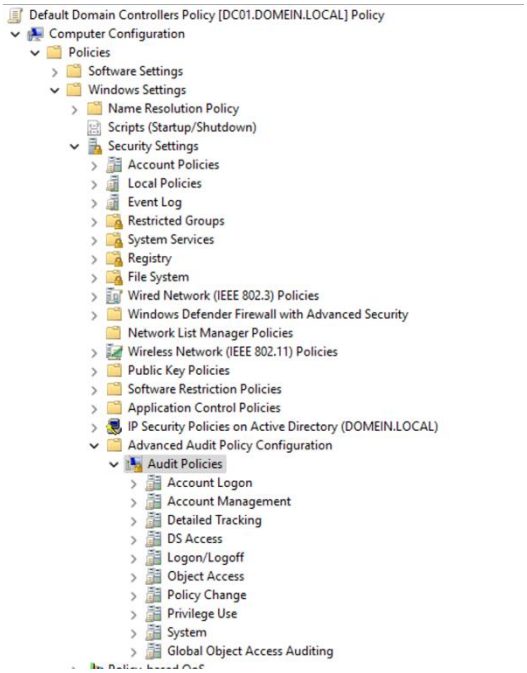
In de volgende secties bespreken we de meest relevante audit policies en hoe deze kunnen worden toegepast.

4.1.1 Het configureren van audit policies voor Windows

Het configureren van logretentie voor Windows kan eenvoudig worden uitgevoerd via Group Policy Objects (GPO). Hiermee stel je uniforme instellingen in voor logbeheer binnen een Active Directory (AD)-omgeving. Hieronder beschrijven we de stappen en de specifieke GPO-instellingen die nodig zijn.

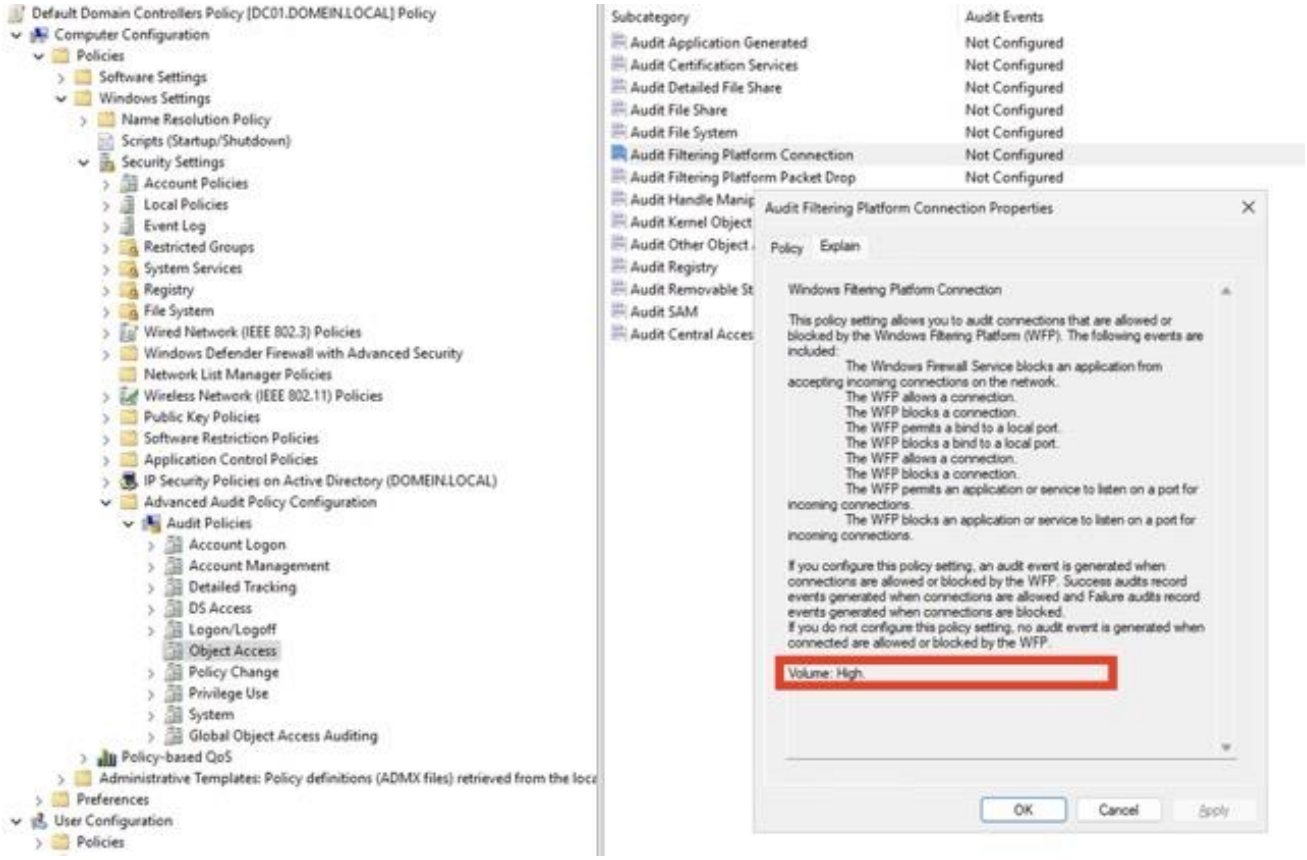
Stappenplan voor het configureren van logretentie via GPO.

1. Open de Group Policy Management Console (GPMC):
    a. Log in op een domeincontroller.
    b. Start de Group Policy Management Console (gpmc.msc).
2. Maak of bewerk een GPO:
    a. Klik met de rechtermuisknop op de gewenste Organizational Unit (OU) of het domein waarvoor je de instellingen wilt toepassen.
    b. Selecteer Create a GPO in this domain and link it here... of kies een bestaande GPO.
3. Navigeer naar de loginstellingen: Ga naar het volgende pad in de GPO Editor: Computer Configuration → Policies → Windows Settings → Security → Settings Advanced Audit Policy Configuration → Audit Policies



Figuur 2 - Audit policies overzicht in GPO

Sommige Event IDs genereren meer logging dan andere en kunnen de systeemperformance beïnvloeden. Controleer in de properties van een audit event policy onder het tabblad Explain wat elk event precies doet. Dit helpt je in te schatten hoeveel logvolume je kunt verwachten en zorgt ervoor dat je bewuste keuzes maakt om overbodige logging en impact op de performance te minimaliseren.



Figuur 3 - Log volume van een specifieke audit policy

4.1.2 Relevante Windows audit policies

Dit document bevat tabellen met belangrijke audit policies die van toegevoegde waarde zijn voor compliance, incident response en forensisch onderzoek. Het is belangrijk te realiseren dat niet alle audit policies voor elk systeem noodzakelijk zijn. De tabel is onderverdeeld in vier kolommen:

1. Audit Policy Category or Subcategory
2. Windows 7 en later
3. Windows server 2008 en later
4. Domain controller

Elke kolom geeft aan welke audit policies relevant zijn voor de verschillende Windows-versies. Deze lijst is gebaseerd op de aanbevolen baselines van Windows, waarbij we onze eigen aanvullingen hebben toegevoegd, die volgens ons cruciaal zijn voor SOC-readiness.

Voor meer informatie zie: Audit Policy Recommendations

De onderstaande legenda beschrijft wat de aanduidingen IF, Success & Failure betekenen in de context van de aanbevelingen

Success & Failure: Beide succes- en foutgebeurtenissen moeten worden gemonitord. Dit betekent dat zowel geslaagde als mislukte pogingen worden geregistreerd om een volledig overzicht te krijgen van de beveiligingsgebeurtenissen.

Waarde	Beschrijving
IF	Schakel in indien nodig voor een specifiek scenario, of als een rol of functie waarvoor auditing gewenst is, op de machine is geïnstalleerd. Kan een hoge impact op het volume hebben of vereist aanvullende beleidsinstellingen zoals System Access Control List (SACL).
Success & Failure	Beide succes- en foutgebeurtenissen moeten worden gemonitord. Dit betekent dat zowel geslaagde als mislukte pogingen worden geregistreerd om een volledig overzicht te krijgen van de beveiligingsgebeurtenissen.
Lege cel	Geen aanbeveling

4.1.2.1 Account Logon

Audit Policy Subcategory	Windows 7 en later	Windows Server 2008 en later	Domain controller	Niveau
Audit Credential Validation	Success & Failure	Success & Failure	Success & Failure	L1
Audit Kerberos Authentication Service			Success & Failure	L2
Audit Kerberos Service Ticket Operations	Success & Failure	Success & Failure	Success & Failure	L3
Audit Other Account Logon Events	Success & Failure	Success & Failure	Success & Failure	L4

4.1.2.2 Accountmanagement

Audit Policy Category	Windows 7 en later	Windows server 2008 en later	Domain controller	Niveau
Audit Application Group Management				-
Audit Computer Account Management	Success & Failure	Success & Failure	Success & Failure	L2
Audit Distribution Group Management			Success & Failure	L4
Audit Other Account Management Events	Success & Failure	Success & Failure	Success & Failure	L3
Audit Security Group Management	Success & Failure	Success & Failure	Success & Failure	L2
Audit User Account Management	Success & Failure	Success & Failure	Success & Failure	L1

4.1.2.3 Detailed Tracking

Audit Policy Subcategory	Windows 7 en later	Windows server 2008 en later	Domain controller	Niveau
Audit DPAPI Activity	Success & Failure	Success & Failure	Success & Failure	L3
Audit Process Creation	Success & Failure	Success & Failure	Success & Failure	L2
Audit Process Termination	IF	IF	IF	L3
Audit RPC Events				-
Audit Token Right Adjusted				-
Audit PNP Activity				-

4.1.2.4 DS Access

Audit Policy Subcategory	Windows 7 en later	Windows server 2008 en later	Domain controller	Niveau
Audit Detailed Directory Service Replication			Success & Failure	L4
Audit Directory Service Access			Success & Failure	L1
Audit Directory Service Changes			Success & Failure	L2
Audit Directory Service Replication			Success & Failure	L3

4.1.2.5 Object access

Audit Policy Subcategory	Windows 7 en later	Windows server 2008 en later	Domain controller	Niveau
Audit Application Generated				-
Audit Certification Services				-
Audit Detailed File Share				-
Audit File System				-
Audit Filtering Platform Connection				-
Audit Filtering Platform Packet Drop				-
Audit Handle Manipulation				-
Audit Kernel Object				-
Audit Other Object Access Events				-
Audit Registry				-
Audit Removable Storage				-
Audit SAM				-
Audit Central Access Policy Staging				-

4.1.2.6 Logon and Logoff

Audit Policy Subcategory	Windows 7 en later	Windows server 2008 en later	Domain controller	Niveau
Audit Account Lockout	Success	Success	Success	L2
Audit User/Device Claims				-
Audit IPsec Extended Mode				-
Audit IPsec Main Mode	IF & IF	IF & IF	IF & IF	L4
Audit IPsec Quick Mode				-
Audit Logoff	Success	Success	Succes	L1
Audit Logon	Success & Failure	Success & Failure	Success & Failure	L1
Audit Network Policy Server				-
Audit Other Logon/Logoff Events		Success & Failure	Success & Failure	L3
Audit Special Logon	Success & Failure	Success & Failure	Success & Failure	L2

4.1.2.7 Policy Change

Audit Policy Subcategory	Windows 7 en later	Windows server 2008 en later	Domain controller	Niveau
Audit Audit Policy Change	Success & Failure	Success & Failure	Success & Failure	L1
Audit Authentication Policy Change	Success & Failure	Success & Failure	Success & Failure	L2
Audit Authorization Policy Change	Success	Success	Success	L4
Audit Filtering Platform Policy Change				-
Audit MPSSVC Rule-Level Policy Change	Success	Success	Success	L3
Audit Other Policy Change Events				-

4.1.2.8 Privilege Use

Audit Policy Subcategory	Windows 7 en later	Windows server 2008 en later	Domain controller	Niveau
Audit Non-Sensitive Privilege Use				-
Audit Other Privilege Use Events				-
Audit Sensitive Privilege Use	Success	Success	Success	L2

4.1.2.9 System

Audit Policy Subcategory	Windows 7 en later	Windows server 2008 en later	Domain controller	Niveau
Audit IPsec Driver	IF & IF	IF & IF	IF & IF	L4
Audit Other System Events				-
Audit Security State Change	Success & Failure	Success & Failure	Success & Failure	L1
Audit Security System Extension	Success & Failure	Success & Failure	Success & Failure	L3
Audit System Integrity	Success & Failure	Success & Failure	Success & Failure	L2

4.1.2.10 Global Object Access Auditing

Audit Policy Subcategory	Windows 7 en later	Windows server 2008 en later	Domain controller	Niveau
File system				-
Registry				-

4.1.2.11 Configureren van command-line process auditing

Command-line process auditing registreert alle processen die via de opdrachtregel op een systeem worden uitgevoerd, inclusief de invoer van commando's en bijbehorende details. Dit helpt beheerders en security-specialisten om verdachte of ongewenste activiteiten te detecteren door een gedetailleerd overzicht van alle uitgevoerde commando's te verkrijgen.

Policy configuratie	Details
Benodidge configuratie	Audit Process Creation van tabel 3.1.1.3 moet minimaal op succes staan
Pad in GPO voor command line process auditing	Computer Configuration\Administrative Templates\System\Audit Process Creation
Instelling	Include command line in process creation events
Omschrijving	Deze beleidsinstelling bepaalt welke informatie wordt vastgelegd in beveiligingslogboekgebeurtenissen wanneer een nieuw proces wordt aangemaakt. Deze instelling is alleen van toepassing wanneer het beleid Audit Process Creation is ingeschakeld. Als je deze beleidsinstelling inschakelt, wordt de opdrachtregelinformatie van elk proces in platte tekst gelogd in het beveiligingsgebeurtenislogboek. Dit gebeurt als onderdeel van de Audit Process Creation-gebeurtenis 4688: "Een nieuw proces is aangemaakt" op de werkstations en servers waarop deze beleidsinstelling wordt toegepast. Als je deze beleidsinstelling uitschakelt of niet configureert, wordt de opdrachtregelinformatie van processen niet opgenomen in de Audit Process Creation-gebeurtenissen. Standaardinstelling: Niet geconfigureerd Opmerking: Wanneer deze beleidsinstelling is ingeschakeld, kan elke gebruiker met leesrechten op de beveiligingsgebeurtenissen de opdrachtregelargumenten zien van elk succesvol aangemaakt proces. Opdrachtregelargumenten kunnen gevoelige of privé-informatie bevatten, zoals wachtwoorden of gebruikersgegevens.

4.1.3 Configureren van NTLM-auditing

NTLM is een verouderd authenticatieprotocol dat nog steeds in veel netwerken wordt gebruikt, ondanks bekende beveiligingsrisico's zoals pass-the-hash-aanvallen. Door NTLM-auditing in te schakelen, kan een SOC-inzicht krijgen in waar NTLM nog actief is en welke systemen of accounts hierop vertrouwen. Dit helpt bij het identificeren van kwetsbaarheden en het detecteren van mogelijke bedreigingen.

Voor een SOC biedt NTLM-auditing waardevolle inzichten door NTLM-gerelateerde events te correleren met andere securitylogboeken. Dit maakt het mogelijk om aanvallen zoals pass-the-hash en laterale bewegingen vroegtijdig te signaleren en te mitigeren. Deze configuratie is enkel toepasbaar voor domain controllers.

Om NTLM-auditing te configureren:

Nadat de initiële instellingen voor het Advanced Audit Policy geconfigureerd zijn. Open de Group Policy Management. Ga vervolgens naar **Default Domain Controllers Policy > Lokale beleidsregels > Beveiligingsopties.**

Configureer de opgegeven beveiligingsbeleidinstellingen als volgt:

Beveiligingsbeleidinstelling	Waarde
Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers	Audit all
Network security: Restrict NTLM: Audit NTLM authentication in this domain	Enable all
Network security: Restrict NTLM: Audit Incoming NTLM Traffic	Enable auditing for all accounts

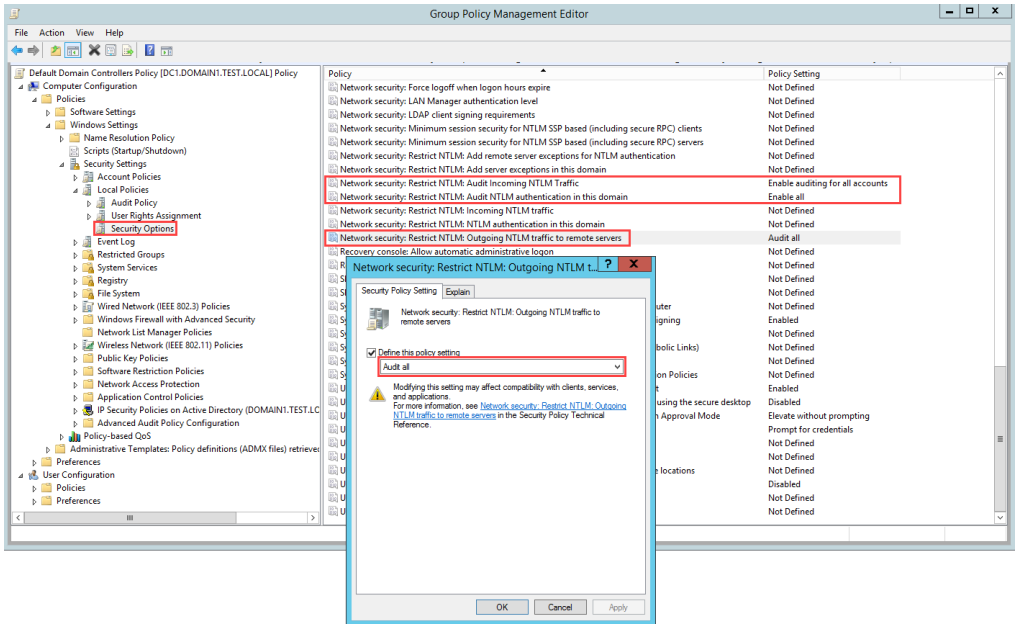


Figure 3 - Group Policy Management NTLM auditing

4.1.4 Logretentie en opslag implementatie voor Windows

Een goed ingestelde logretentie is essentieel voor effectieve monitoring, forensisch onderzoek en naleving van compliance-eisen. Voor Windows audit policies kan dit op de volgende manier worden toegepast:

De Event Viewer verzamelt alle logs die gegenereerd worden door Windows-auditpolicies, met name in de **Security-log**. Hier kun je eenvoudig de retentie-instellingen aanpassen:

1. Open de Event Viewer door eventvwr.msc uit te voeren.
2. Navigeer naar Windows Logs > Security.
3. Klik met de rechtermuisknop op **Security** en selecteer **Properties**.
4. In het **Log Properties**-venster kun je de maximale grootte van het logbestand instellen. Zodra deze limiet is bereikt, kun je kiezen uit drie opties:
    a. **Overwrite events as needed (oldest events first):** Oude logs worden overschreven zodra de limiet bereikt is.
    b. **Archive the log when full, do not overwrite events:** Logs worden gearchiveerd voordat ze worden overschreven.
    c. **Do not overwrite events (clear log manually):** Logs blijven staan en moeten handmatig worden gewist wanneer het log vol is.

Deze methode is snel en eenvoudig, maar minder geschikt voor grootschalige implementaties in een domeinomgeving.

Configureren via Group Policy (GPO)

Voor een consistente configuratie en een schaalbare aanpak is het gebruik van Group Policy Objects (GPO's) de aanbevolen methode.

1. Open de **Group Policy Management Console (GPMC)** op een domeincontroller (gpmc.msc).
2. Maak een nieuwe GPO of bewerk een bestaande.
3. Ga naar het volgende pad:
   Computer Configuration > Policies > Administrative Templates > Windows Components > Event Log Service > Security
4. Configureer de volgende instellingen:
    - **Maximum log size (KB):** Stel de maximale grootte van het log in, bijvoorbeeld 32,768 KB.
    - **Retention method:** Kies de gewenste retentiemethode:
        - **Overwrite as needed:** Voor continue logging zonder tussenkomst.
        - **Archive the log:** Voor het bewaren van volledige logs.
        - **Do not overwrite events:** Om logs permanent te bewaren (handmatige clearing vereist).

Herhaal de bovenstaande stappen indien dit ook vereist is voor de andere logtabellen.

Best Practices voor Retentie en Opslag

- **Log Grootte:** Stel een loggrootte in die in verhouding staat tot de hoeveelheid gegenereerde gebeurtenissen. Voor domeincontrollers is een grotere log aanbevolen
- **Archivering:** Overweeg een logrotatie- of archiveringssysteem om te voorkomen dat logs verloren gaan.
- **Bewaartermijn:** Stem de retentieperiode af op compliance-eisen zoals beschreven in in de BIO bijvoorbeeld een bewaarperiode van 90 of 180 dagen.
- **Centralisatie:** Implementeer een SIEM-oplossing om logs centraal op te slaan en te analyseren, terwijl lokale retentie wordt ingesteld als back-up.
- **Controleer regelmatig:** Gebruik scripts of monitoringtools om te controleren of de ingestelde limieten en retentie correct functioneren.

4.2 Audit Policies voor Linux

Het configureren van audit policies voor Linux kan op verschillende manieren, waarbij Auditd een van de meest gebruikte tools is. Hoewel er online veel informatie beschikbaar is over Auditd, kan het een uitdaging zijn om een configuratie samen te stellen die zowel voldoet aan compliance-eisen als waardevol is voor forensisch onderzoek.

In dit hoofdstuk bespreken we de belangrijkste aspecten van het configureren van audit policies op Linux-systemen. We gaan in op waar log-events worden opgeslagen, hoe je Auditd installeert, en hoe je een basisconfiguratie opstelt die geschikt is voor zowel compliance als beveiligingsanalyse. Daarnaast behandelen we hoe specifieke gebeurtenissen, zoals gebruikersauthenticatie en wijzigingen in bestanden, kunnen worden gemonitord.

Let op: Als er wel een EDR actief is, zoals bijvoorbeeld Defender for Endpoint, controleer dan welke inzichten de EDR al biedt. Veel EDR-oplossingen loggen activiteiten zoals bestandstoegang, procesmonitoring en rootgebruik. In dat geval kunnen bepaalde auditregels overbodig zijn of leiden tot dubbele logging.

4.2.1 Installatie van Auditd

Het installeren van **Auditd** is eenvoudig en kan worden uitgevoerd via de pakketbeheerder van je Linux-distributie. Gebruik bijvoorbeeld het volgende commando:

Voor Debian/Ubuntu:

> *sudo apt update && sudo apt install auditd –y*

Voor Red Hat/CentOS:

> *sudo yum install audit –y*

Na installatie start je de dienst en stel je deze in om automatisch te starten:

> *sudo systemctl start auditd*
> *sudo systemctl enable auditd*

Met Auditd geïnstalleerd, kun je beginnen met het configureren van auditregels voor jouw specifieke behoeften. De volgende paragrafen bieden hiervoor verdere handreikingen.

4.2.2 Logbestanden

Bij het gebruik van Auditd zijn er een aantal belangrijke bestanden en locaties die je moet kennen voor het beheer en de analyse van audit logs. Hieronder vind je een overzicht:

Audit Logbestand: /var/log/audit/audit.log
Dit is het primaire logbestand waarin alle gebeurtenissen worden vastgelegd die door Auditd zijn geregistreerd.

Het bestand bevat informatie zoals gebruikersactiviteiten, wijzigingen aan bestanden, netwerkactiviteiten, en meer. Gebruik tools zoals ausearch of auditctl om specifieke gegevens uit deze logs te filteren en te analyseren.

System Log: /var/log/messages of /var/log/syslog
Afhankelijk van de distributie kunnen audit-gerelateerde meldingen ook in de algemene systeemlogs worden opgenomen.

Auditd Configuration Log: /etc/audit/auditd.conf
Hier configureer je hoe Auditd werkt, zoals de grootte van logbestanden, rotatie-instellingen, en wat er gebeurt als de schijfruimte vol is.

4.2.3 Belangrijke bestanden om rekening mee te houden

Audit Rules: /etc/audit/rules.d/
In deze map kun je specifieke auditregels definiëren die bepalen wat er wordt gelogd.

Regels in bestanden zoals audit.rules worden bij het opstarten van Auditd geladen.

Onderstaande regel bewaakt het bestand /etc/passwd voor lezen, schrijven en wijzigingen, met de sleutel passwd_changes.

-w /etc/passwd -p rwa -k passwd_changes

Audit Daemon Configuratie: /etc/audit/auditd.conf

Hier stel je parameters in zoals:

- l**og_file**: Locatie van het auditlogbestand (standaard /var/log/audit/audit.log).
- **max_log_file:** Maximale grootte van het logbestand in MB.
- **num_logs**: Aantal logbestanden dat moet worden bewaard bij rotatie.

4.2.4 Auditd Configureren

Na installatie gebruikt auditd een standaard configuratiebestand dat zich bevindt in ***/etc/audit/auditd.conf.*** Dit bestand bevat belangrijke parameters die bepalen hoe het auditing systeem functioneert.

Onderstaand is een tabel samengesteld met de meest belangrijke parameters

Parameter	Standaardwaarde	Beschrijving	Mogelijke waarden
log_file	/var/log/audit/audit.log	Locatie van het audit logbestand.	Elk pad naar een bestand, bijv. /var/log/custom_audit.log
log_group	adm	Groep met leesrechten op audit logs.	Elke geldige Linux-groep, bijv. root, wheel, audit
flush	INCREMENTAL_ASYNC	Wanneer logs naar de schijf worden geschreven.	NONE, DATA, SYNC, INCREMENTAL_ASYNC, INCREMENTAL
freq	50	Hoe vaak logs naar disk worden geschreven.	Elk positief geheel getal, bijv. 10, 100, 500
max_log_file	8	Maximale grootte van een logbestand (MB).	Elk positief getal, bijv. 5, 50, 100
num_logs	5	Aantal bewaarde oude logbestanden.	Elk positief geheel getal, bijv. 1, 10, 20
priority_boost	4	Prioriteit van auditd verhogen.	0 (geen boost) tot 10 (hoogste boost)
space_left	75	Waarschuwing bij minder vrije schijfruimte (MB).	Elk positief getal, bijv. 50, 100, 500
max_log_file_action	ROTATE	Actie bij het bereiken van max loggrootte.	IGNORE, SUSPEND, ROTATE, KEEP_LOGS
space_left_action	SYSLOG	Actie bij weinig vrije schijfruimte.	IGNORE, SYSLOG, EMAIL, SUSPEND, HALT, EXEC
verify_email	yes	Controleert of e-mails kunnen worden verzonden.	yes, no

Parameter	Standaardwaarde	Beschrijving	Mogelijke waarden
action_mail_acct	root	Ontvanger van waarschuwingen per e-mail.	Elke geldige e-mail of systeemgebruiker, bijv. admin@example.com
admin_space_left	50	Kritische drempel voor vrije schijfruimte (MB).	Elk positief getal, bijv. 25, 75, 100
admin_space_left_action	SUSPEND	Actie bij kritiek lage vrije schijfruimte.	IGNORE, SYSLOG, EMAIL, SUSPEND, HALT, EXEC
disk_full_action	SUSPEND	Actie als de schijf vol is.	IGNORE, SYSLOG, EMAIL, SUSPEND, HALT, EXEC
disk_error_action	SUSPEND	Actie bij een schrijffout op de schijf.	IGNORE, SYSLOG, EMAIL, SUSPEND, HALT, EXEC

4.2.5 Logrotatie en Retentie

Bij het configureren van logrotatie en retentie voor auditd zijn er twee belangrijke benaderingen: rotatie op bestandsgrootte of rotatie op datum.

Rotatie op Basis van Bestandsgrootte

Voor het behouden van logs op basis van het aantal bestanden zijn de volgende instellingen in auditd.conf noodzakelijk:

```
max_log_file = 50
max_log_file_action = ROTATE
num_logs = 30
```

Deze configuratie:

- Limiteert elk logbestand tot 50 MB
- Bewaart 30 logbestanden (1 actief + 29 gearchiveerde)
- Roteert automatisch wanneer een bestand de maximale grootte bereikt

Belangrijk: Monitor hoeveel data er dagelijks wordt gelogd om te verzekeren dat de gekozen bestandsgrootte voldoende is voor de retentie-eisen.

Rotatie op Basis van Datum

Als logs op datum geroteerd moeten worden, is logrotate een betere optie. Creëer hiervoor een configuratie in /etc/logrotate.d/auditd:

```
{
compress                    # Comprimeer oude logbestanden
dateext.                    # Voeg een datumextensie toe aan de logbestanden
rotate 30                   # Bewaar de laatste 30 rotaties
Daily                       # Voer de rotatie dagelijks uit
missingok                   # Negeer als het logbestand ontbreekt
notifempty                  # Voer geen rotatie uit als het logbestand leeg is
create 600 root root        # Maak nieuwe logbestanden aan met de juiste permissies (600) en eigenaar (root)
sharedscripts               # Voer postrotate scripts slechts één keer uit voor alle logs in deze configuratie
postrotate
/sbin/service auditd restart 2> /dev/null > /dev/null || true  # Herstart de auditd service na rotatie
endscript
}
```

Figuur 4 - logrotate configuratie voorbeeld

Bij gebruik van logrotate is het noodzakelijk om auditd.conf aan te passen:

```
max_log_file = 50
max_log_file_action = IGNORE
```

Deze methode:

- Zorgt voor dagelijkse logrotatie
- Bewaart exact 30 dagen aan logs
- Voegt datumextensies toe aan geroteerde bestanden
- Biedt betere controle over retentieperiodes

Kies de methode die het beste past bij je bedrijfsbeleid en compliance-eisen, en zorg voor voldoende schijfruimte voor de gekozen retentieperiode.

Schijfruimtebeheer

- Configureer **space_left** ruim boven **admin_space_left** om tijdig te kunnen reageren
- Stel passende acties in voor space_left_action en admin_space_left_action
- Overweeg **EMAIL** als actie voor vroege waarschuwingen

Voor een volledig overzicht van alle configuratieopties en hun gedetailleerde beschrijvingen kunt u de officiële auditd.conf manual page raadplegen via het commando man auditd.conf of online op de Linux manual pages website.

4.2.6 Auditd regelset implementeren

Een goede auditconfiguratie voor Linux begint met een zorgvuldig samengestelde Auditd-regelset. Dit is essentieel om beveiligingsgebeurtenissen effectief te monitoren en mogelijke dreigingen tijdig te detecteren. Het gebruik van een bestaande, bewezen regelset biedt tal van voordelen, zowel op het gebied van veiligheid als efficiëntie.

Een hoogwaardige Auditd-regelset dekt een breed scala aan belangrijke gebeurtenissen, waaronder pogingen om gevoelige systeembestanden te openen of te wijzigen, veranderingen in gebruikers- en groepsbeheer zoals het aanmaken of verwijderen van accounts, activiteiten die wijzen op privilege-escalatie zoals het gebruik van sudo of aanpassingen in /etc/sudoers, en netwerk- en procesactiviteiten die kunnen wijzen op malware of reverse shells. Met deze dekking wordt het risico geminimaliseerd dat kritieke gebeurtenissen onopgemerkt blijven, wat cruciaal is voor effectieve beveiligingsmonitoring.

Het ontwikkelen van een eigen regelset vergt diepgaande kennis van Linux-systemen, beveiligingsrisico's en Auditd zelf. Dit proces is niet alleen complex maar ook tijdsintensief. Door te kiezen voor een bestaande regelset kun je direct beginnen met monitoring, zonder dat je tijd hoeft te investeren in onderzoek en testen.

Er zijn veel Auditd-regelsets online beschikbaar, maar lang niet allemaal worden ze regelmatig bijgewerkt of bieden ze een goede balans tussen signalering en het voorkomen van overbodige ruis. Sommige regelsets zijn niet betrouwbaar omdat ze verouderd zijn, onvoldoende getest of niet aansluiten bij hedendaagse dreigingsmodellen, waardoor belangrijke incidenten mogelijk onopgemerkt blijven.

Een van de betere en meest bekende regelsets is die van Neo23x0. Deze regelset is ontworpen met een sterke focus op security, gebaseerd op praktijkervaring en voortdurend geoptimaliseerd om relevant te blijven in een steeds veranderend dreigingslandschap.

https://github.com/Neo23x0/auditd/blob/master/audit.rules

Volg de onderstaande stappen om de regelset te configureren.

Download de regelset

> *wget https://raw.githubusercontent.com/Neo23x0/auditd/master/audit.rules -O /etc/audit/rules.d/audit.rules*

Controleer de configuratie
Zorg dat de Auditd-service goed is ingesteld en verwijst naar de juiste regels. Start Auditd opnieuw om de nieuwe regels te laden:

> *systemctl restart auditd*

Test de configuratie
Voer een paar acties uit die door de regels worden gecontroleerd (bijvoorbeeld bestandstoegang of sudo-commando's) en controleer of de logs correct worden vastgelegd:

> *ausearch -m USER_AUTH*

Het implementeren van een Auditd-regelset vereist een strategische aanpak om ervoor te zorgen dat de configuratie betrouwbaar, consistent en toekomstbestendig is. Hier zijn enkele best practices:

Gebruik een versiebeheersysteem

Maak een werkkopie van een originele regelset (een zogenaamde 'fork') vanuit een betrouwbare bron, zoals de Neo23x0-regelset, naar een eigen versiebeheeroplossing. Dit zorgt ervoor dat je wijzigingen kunt bijhouden, gemakkelijk kunt samenwerken met andere teamleden, en altijd een terugvaloptie hebt als updates niet naar wens werken.

Pas de regelset aan op je omgeving

Elke Linux-omgeving is uniek, met specifieke processen en beveiligingsvereisten. Controleer de standaardregelset en pas deze aan om irrelevante meldingen te minimaliseren en de focus te leggen op kritieke gebeurtenissen. Zorg er bijvoorbeeld voor dat extra monitoring wordt ingesteld voor bedrijfskritische bestanden of services.

Implementeer de configuratie centraal

Maak gebruik van tools zoals Ansible, Puppet of Chef om de aangepaste regelset centraal uit te rollen naar alle systemen binnen je netwerk. Dit voorkomt inconsistenties en zorgt voor een uniforme configuratie.

Beveilig toegang tot de configuratie

De Auditd-configuratie is een kritieke component van je beveiligingsstrategie. Zorg ervoor dat alleen bevoegde gebruikers wijzigingen kunnen aanbrengen. Implementeer toegangsbewaking en gebruik bijvoorbeeld versiebeheer met beperkte schrijfrechten.

Bijlage I – Configuratiestatus checklist

Level	Configuration Control	Status
L1	Account Logon: Audit Credential Validation (H 4.1.2.1)	
	Account Management: Audit User Account Management (H 4.1.2.2)	
	Detailed Tracking: Audit Directory Service Access (H 4.1.2.3)	
	DS Access: None at this level (H 4.1.2.4)	
	Logon and Logoff: Audit Logon, Audit Logoff (H 4.1.2.6)	
	Policy Change: Audit Audit Policy Change (H 4.1.2.7)	
	Privilege Use: None at this level (H 4.1.2.8)	
	System: Audit Security State Change (H 4.1.2.9)	
L2	Account Logon: Audit Kerberos Authentication Service (H 4.1.2.1)	
	Account Management: Audit Security Group Management, Audit Computer Account Management (H 4.1.2.2)	
	Detailed Tracking: Audit Process Creation (H 4.1.2.3)	
	DS Access: Audit Directory Service Changes (H 4.1.2.4)	
	Logon and Logoff: Audit Account Lockout, Audit Special Logon (H 4.1.2.6)	
	Policy Change: Audit Authentication Policy Change (H 4.1.2.7)	
	Privilege Use: Audit Sensitive Privilege Use (H 4.1.2.8)	
	System: Audit System Integrity (H 4.1.2.9)	
L3	Account Logon: Audit Kerberos Service Ticket Operations (H 4.1.2.1)	
	Account Management: Audit Other Account Management Events (H 4.1.2.2)	
	Detailed Tracking: Audit Process Termination, Audit DPAPI Activity (H 4.1.2.3)	
	DS Access: Audit Directory Service Replication (H 4.1.2.4)	
	Logon and Logoff: Audit Other Logon/Logoff Events (H 4.1.2.6)	
	Policy Change: Audit MPSSVC Rule-Level Policy Change (H 4.1.2.7)	
	Privilege Use: None at this level (H 4.1.2.8)	
	System: Audit Security System Extension (H 4.1.2.9)	
L4	Account Logon: Audit Other Account Logon Events (H 4.1.2.1)	
	Account Management: Audit Distribution Group Management (H 4.1.2.2)	
	Detailed Tracking: None at this level (H 4.1.2.3)	
	DS Access: Audit Detailed Directory Service Replication (H 4.1.2.4)	
	Logon and Logoff: Audit IPsec Main Mode (H 4.1.2.6)	
	Policy Change: Audit Authorization Policy Change (H 4.1.2.7)	
	Privilege Use: None at this level (H 4.1.2.8)	
	System: Audit IPsec Driver for network-level security (H 4.1.2.9)	
L5	Configureren van command line process auditing (H 4.1.2.11)	
	Configureren van NTLM auditing (H 4.1.3)	
	Configure logretentie voor Windows (H 4.1.4)	

Uitgave

Versterken SOC Stelsel Rijk (VSSR)

Postbus 117, 2501 CC Den Haag

Turfmarkt 147, 2511 DP Den Haag

070 751 5555

Meer informatie

https://www.ncsc.nl/vssr

info@ncsc.nl

vssr.info@minjenv.nl (Rijksoverheid)

Maart 2025