

# Audit Audit

## Verbeter de beveiliging van uw OpenVMS omgeving

Audit verbetert de aanwezige OpenVMS security door het bieden van volledige terminal-logging, het analyseren en rapporteren van beveiligingsaspecten.

### Logging van gebruikerssessies

De mogelijkheden van de standaard OpenVMS audit trails zijn zeer beperkt omdat OpenVMS geen activiteiten logt die gebeuren binnen de applicatie zelf. De logging van Audit geeft veel uitgebreidere informatie over het gebruik van de applicatie zelf. Hierdoor kan men precies zien hoe bepaalde bedrijfskritische of gevoelige applicaties gebruikt worden.

Het monitoring proces van Audit omvat alle terminal activiteiten vanaf het moment dat de gebruiker inlogt tot het moment van uitloggen. Men kan Audit dusdanig configureren dat alleen bepaalde activiteiten van gespecificeerde werkstations of specifieke gebruikers wordt opgeslagen. Bijvoorbeeld het gebruik van het systeem buiten normale kantooruren of in het weekend.

Twee typen logfiles kunnen worden gemaakt: Output-only of Input-only logfiles. Output logfiles bevatten alle informatie die verstuurd is naar de specifieke terminal gedurende de sessie. Input logfiles bevatten alle informatie die de gebruiker tijdens het werken met de terminal heeft ingetypt. Iedere regel wordt voorafgegaan door een tijdcodering. Audit files kunnen vastgelegd worden door alle soorten terminals, inclusief netwerkterminals. De logfiles kunnen op het scherm bekeken worden of je kunt ze printen met de speciale FRAMER utility.

### AUDIT Analyse en verslaglegging

Teneinde behulpzaam te zijn met de organisatie van alle vastgelegde logfiles zal het Audit programma automatisch de

## Belangrijkste kenmerken

- **Verbeter de beveiliging van OpenVMS**
- **Legt terminalsessies vast**
- **Voorziet in analyse en verslaglegging**
- **Detecteert indringers met de standaard module Intruder Alert**

bestanden analyseren op potentiële problemen en creëert vervolgens een drietal rapporten:

- Een samenvatting
- Een chronologische lijst met gebeurtenissen
- Geeft aan welke logfiles beveiligingsaspecten bevatten.

Tijdens de analyse van Audit zullen tevens de session logfiles en de OpenVMS audit trails geanalyseerd worden. Audit kan zo ingesteld worden dat het alle logfiles doorneemt of alleen die van specifieke gebruikers.

Het totale verslag zorgt ervoor dat men snel een totaal beeld te krijgt van potentiële problemen op het systeem, het totale netwerk of in een cluster.

### Belangrijke eigenschappen

Er is geen enkel product vergelijkbaar met Audit. Er bestaat geen utility met de zelfde functionaliteit als Audit. Audit verbetert de veiligheid van uw OpenVMS omgeving.

Belangrijke eigenschappen zijn:

- **Complete audit trails voor alle of geselecteerde gebruikers, met minimale systeemoverhead.** Audit legt alle input van de gebruiker vast compleet met de corresponderende output naar de terminal. OpenVMS audit trail legt uitsluitend vast dat

# Audit

een applicatie opgestart is en dat er een bestand is geopend. Alle activiteiten die dieper gaan worden niet vastgelegd. Audit kan alle gebruikers monitoren, geselecteerde gebruikers of specifieke terminals en toch slechts 3% van de systeemcapaciteit gebruiken.

- **Audit voorziet in vastlegging, rapportage en analyse van de logging voor alle systemen.** De standaard security informatie die OpenVMS met de standaard aanwezige tools genereert maakt het zeer complex voor een beveiligingsbeambte te zoeken naar specifieke gebeurtenissen. Audit maakt gebruik van de standaard VMS audit logs, zijn eigen audit logging en genereert geconsolideerde rapporten teneinde de problemen duidelijk vast te leggen. Samengestelde rapportage is mogelijk voor geclusterde en genetwerkte systemen.
- **Flexibele detectie van indringers.** Het onderdeel Intruder Alert van Audit kan eenvoudig geconfigureerd worden voor site-specifieke beveiligingsaspecten en om tijdig actie te ondernemen teneinde het risico te minimaliseren.

## Belangrijke voordelen van Audit

1. **Het helpt voorkomen, detecteren en oplossen van beveiligingsproblemen.** De wetenschap dat er een complete Audit trail wordt vastgelegd zal in vele gevallen voorkomen dat er gebeurtenissen zullen plaatsvinden die niet conform de voorschriften van het bedrijf zijn. De vastlegging van mogelijk systeem misbruik zorgt ervoor dat er tijdig maatregelen genomen kunnen worden om dit in de toekomst te voorkomen.
2. **Reduceert de tijd die nodig is om handmatig beveiligingsproblemen te detecteren.** Geen enkele systeembeheerder heeft tijd om eindeloze loggings te doorzoeken teneinde potentiële beveiligingsproblemen te detecteren. Door gebruik te maken van Audit kan men automatisch de gegevens analyseren en vastleggen in een rapport
3. **Voorziet in een pro-actieve benadering van de**

**beveiliging.** Audit en Intruder Alert maken het mogelijk voor een systeembeheerder om pro-actief en continue te reageren op mogelijke beveiligingsproblemen. Door het aangeven van beveiligingsproblemen en het nemen van acties om er voor te zorgen dat er opgetreden wordt, zorgt Intruder Alert ervoor dat de problemen niet meer zullen voorkomen.

4. **Beveiligt het systeem zonder de gebruikers te belasten.** Aangezien Audit in de achtergrond aanwezig is zullen de gebruikers er niets van merken.
5. **Vult de eis in van een vastlegging van een volledige audit trail.** Audit voorziet in de behoefte van het vastleggen van de complete sessie indien de bedrijfsvoorschriften die eisen, enige voorbeelden zijn:
  - Financiële instituten kunnen gedetailleerd vastleggen wat een gebruiker deed of juist niet heeft gedaan tijdens het gebruik van de applicatie
  - Verzekeringsmaatschappijen en ziekenhuizen kunnen bewijzen wie er toegang heeft gehad tot gevoelige informatie.
  - Farmaceutische bedrijven kunnen volledige Audit trails gebruiken teneinde aan te tonen dat ze volledig voldoen aan de door de FDA geëiste procedures voor het testen van een nieuw geneesmiddel

## Audit versie 5.4 ondersteunt de volgende eigenschappen en functionaliteit:

- OpenVMS 7.1 VAX en AXP
- Compatibiliteit met CONTRL 4.2 en hoger

## Informatie...

Raxco Software is marktleider in de distributie en marketing van high-performance system administration software en resource management oplossingen voor de werkplek.

Gedurende meer dan 20 jaar heeft Raxco bedrijven geholpen hun client/server omgevingen te optimaliseren.

Thans levert Raxco krachtige oplossingen voor het beheer van Windows NT/2000, OpenVMS en UNIX omgevingen.

De oplossingen die Raxco aanbiedt verminderen de beheerskosten van al uw systemen over uw complete netwerk.

## WWW.RAXCO.NL

Raxco Software, Postbus 52  
5175 ZH Loon op Zand, Nederland  
Tel: (0416) 365141, Fax: (0416) 365342  
Email: info@raxco.nl



Copyright 2000. All rights reserved  
All trademarks or trade names are property of their respective companies