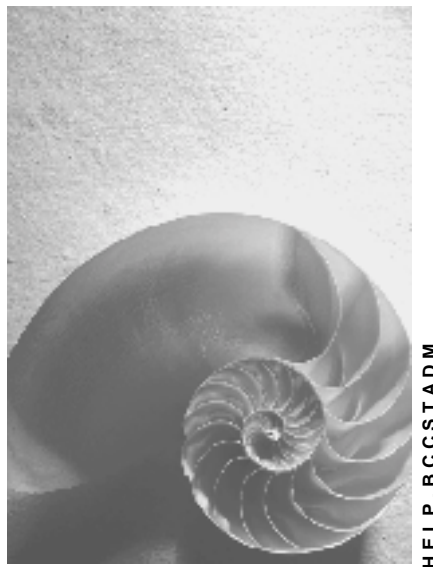


Security-Audit-Log



Release 4.6C



Copyright

© Copyright 2001 SAP AG. Alle Rechte vorbehalten.

Weitergabe und Vervielfältigung dieser Publikation oder von Teilen daraus sind, zu welchem Zweck und in welcher Form auch immer, ohne die ausdrückliche schriftliche Genehmigung durch SAP AG nicht gestattet. In dieser Publikation enthaltene Informationen können ohne vorherige Ankündigung geändert werden.

Die von SAP AG oder deren Vertriebsfirmen angebotenen Software-Produkte können Software-Komponenten auch anderer Software-Hersteller enthalten.

Microsoft[®], WINDOWS[®], NT[®], EXCEL[®], Word[®], PowerPoint[®] und SQL Server[®] sind eingetragene Marken der Microsoft Corporation.

IBM[®], DB2[®], OS/2[®], DB2/6000[®], Parallel Sysplex[®], MVS/ESA[®], RS/6000[®], AIX[®], S/390[®], AS/400[®], OS/390[®] und OS/400[®] sind eingetragene Marken der IBM Corporation.

ORACLE[®] ist eine eingetragene Marke der ORACLE Corporation.

INFORMIX[®]-OnLine for SAP und Informix[®] Dynamic Server[™] sind eingetragene Marken der Informix Software Incorporated.

UNIX[®], X/Open[®], OSF/1[®] und Motif[®] sind eingetragene Marken der Open Group.

HTML, DHTML, XML, XHTML sind Marken oder eingetragene Marken des W3C[®], World Wide Web Consortium, Massachusetts Institute of Technology.

JAVA[®] ist eine eingetragene Marke der Sun Microsystems, Inc.

JAVASCRIPT[®] ist eine eingetragene Marke der Sun Microsystems, Inc., verwendet unter der Lizenz der von Netscape entwickelten und implementierten Technologie.

SAP, SAP Logo, R/2, RIVA, R/3, ABAP, SAP ArchiveLink, SAP Business Workflow, WebFlow, SAP EarlyWatch, BAPI, SAPPHIRE, Management Cockpit, mySAP.com Logo und mySAP.com sind Marken oder eingetragene Marken der SAP AG in Deutschland und vielen anderen Ländern weltweit. Alle anderen Produkte sind Marken oder eingetragene Marken der jeweiligen Firmen.

Symbole

Symbol	Bedeutung
	Achtung
	Beispiel
	Empfehlung
	Hinweis
	Syntax
	Tip

Inhalt

Security-Audit-Log	5
Aufbau des Security-Audit-Log.....	7
Vergleich von Security-Audit-Log und Systemprotokoll.....	10
Statische Profile pflegen.....	12
Filter dynamisch ändern	14
Filter definieren.....	16
Audit-Analysereport anzeigen.....	18
Lesen des Audit-Analysereports	20
Alte Audit-Dateien löschen.....	22
Security-Alerts im CCMS-Alert-Monitor	24
Security-Alerts anzeigen.....	25
Security-Alerts mittels BAPIs lesen.....	26
Anzeigeoptionen des Audit-Log	27
Beispielfilter	28

Security-Audit-Log

Einsatzmöglichkeiten

Das Security-Audit-Log ist ein Werkzeug für Auditoren, die sich die Ereignisse im SAP-System detailliert ansehen müssen. Durch Aktivierung des Audit-Log werden die Aktionen aufgezeichnet, die Sie als wichtig für die Verfolgung einstufen. Sie können dann auf diese Informationen in Form eines Audit-Analysereports zugreifen und sie auswerten.

Oberstes Ziel des Audit-Log ist die Aufzeichnung von:

- sicherheitsbezogenen Änderungen an der SAP-Systemumgebung (z. B. Änderungen an Benutzerstammsätzen)
- Informationen, die mehr Transparenz bieten (z. B. erfolgreiche und erfolglose Anmeldeversuche)
- Informationen, die der Nachvollziehbarkeit einer Reihe von Ereignissen dienen (z. B. erfolgreiche oder erfolglose Transaktionsstarts)

Im einzelnen können Sie mit dem Security-Audit-Log folgende Informationen aufzeichnen:

- erfolgreiche und erfolglose Dialoganmeldeversuche
- erfolgreiche und erfolglose RFC-Anmeldeversuche
- RFC-Aufrufe von Funktionsbausteinen
- erfolgreiche und erfolglose Transaktionsstarts
- erfolgreiche und erfolglose Reportstarts
- Änderungen an Benutzerstammsätzen
- Änderungen an der Audit-Konfiguration

Einführungshinweise



Das Security-Audit-Log enthält personenbezogene Daten, die eventuell Datenschutzgesetzen unterliegen. Vergewissern Sie sich, daß Sie die für Ihren Anwendungsbereich geltenden Datenschutzgesetze einhalten, bevor Sie das Security-Audit-Log einsetzen!

Integration

Mit dem Security-Audit-Log zeichnen SAP-Systeme alle Aktivitäten auf, die den angegebenen Filtern entsprechen.

Informationen über die technischen Aspekte des Audit-Log finden Sie unter [Aufbau des Security-Audit-Log \[Seite 7\]](#).

Das Security-Audit-Log ergänzt das Systemprotokoll, dient jedoch einem etwas anderen Zweck und richtet sich an eine andere Zielgruppe (siehe [Vergleich von Security-Audit-Log und Systemprotokoll \[Seite 10\]](#)).

Security-Audit-Log**Aktivitäten**

Weitere Informationen zu den verschiedenen Aktionen, die Sie bei Verwendung des Security-Audit-Log ausführen müssen, finden Sie unter:

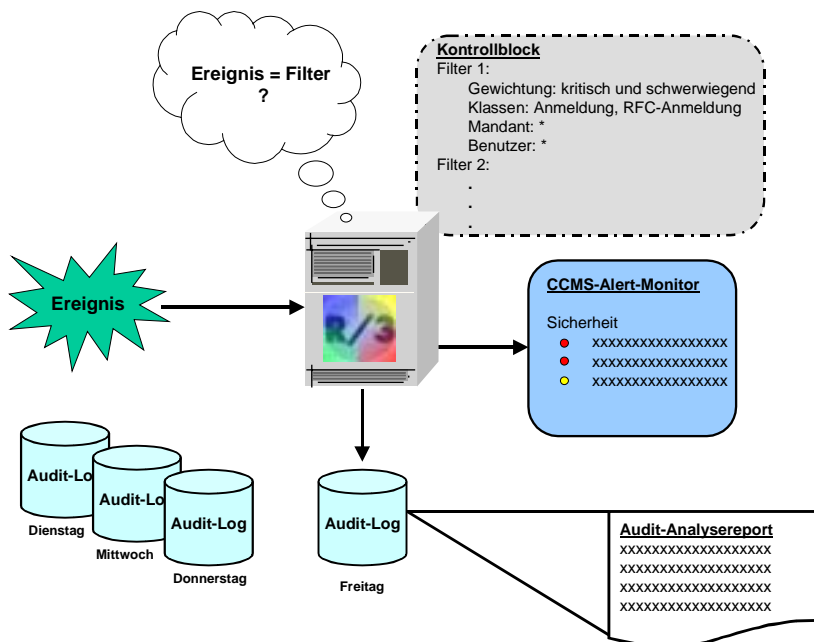
- [Filter definieren \[Seite 16\]](#), um die Verfolgung zu ermöglichen und die zu verfolgenden Informationen zu konfigurieren
- [Audit-Analysereport anzeigen \[Seite 18\]](#); dort wird genau beschrieben, wie Sie Ihren Audit-Analyse-Report angeben. [\[Seite 18\]](#) Sie können die aufgezeichneten Informationen je nach Bedarf anzeigen und entweder alle protokollierten Informationen anzeigen oder eine Untergruppe auswählen (z. B. bestimmte Transaktionen oder Benutzer).
- [Alte Audit-Dateien löschen \[Seite 22\]](#); dort erhalten Sie Informationen zum Archivieren und Löschen Ihrer Audit-Dateien.

Aufbau des Security-Audit-Log

Überblick

Das Security-Audit-Log zeichnet sicherheitsrelevante Aktivitäten in SAP-Systemen auf. Die Informationen werden auf jedem Anwendungsserver täglich in einer Audit-Datei aufgezeichnet. Das Audit-Log ermittelt anhand von Filtern, die in einem Kontrollblock im Speicher liegen, welche Informationen in die Datei zu schreiben sind. Tritt ein Ereignis ein, das einem aktiven Filter entspricht (z. B. der Start einer Transaktion), erstellt das Audit-Log eine entsprechende Audit-Meldung und schreibt sie in die Audit-Datei. Außerdem wird ein entsprechender Alert an den CCMS-Alert-Monitor geschickt. Details zu den Ereignissen finden Sie im Audit-Analysereport des Security-Audit-Log.

Aufbau des Security-Audit-Log



SAP-Systeme pflegen ihre Audit-Logs täglich. Die Audit-Dateien der vorangegangenen Tage werden weder gelöscht noch überschrieben, sondern vom System solange aufbewahrt, bis Sie sie manuell löschen. Da sich große Datenmengen ansammeln können, sollten Sie die Dateien regelmäßig archivieren und die Originale auf dem Anwendungsserver löschen (siehe [Alte Audit-Dateien löschen \[Seite 22\]](#)).

Audit-Datei / Audit-Datensatz

Die Audit-Dateien befinden sich auf den einzelnen Anwendungsservern. Den Namen und das Verzeichnis der Dateien definieren Sie in Profilparameter `rsau/local/file`. Tritt ein zu

Aufbau des Security-Audit-Log

protokollierendes Ereignis ein, erzeugt das System einen entsprechenden Audit-Datensatz, auch Audit-Meldung, und schreibt ihn in die Datei. Der Audit-Datensatz enthält folgende Informationen (sofern bekannt):

- Ereignisbezeichner (3 Zeichen langer Schlüssel)
- SAP-Benutzerkennung und Mandant
- Terminalnamen
- Transaktionscode
- Reportnamen
- Uhrzeit und Datum des Ereignisses
- Prozeß-ID
- Modusnummer
- Zusatzinformationen

Die maximale Größe der Audit-Datei definieren Sie in Profilparameter `rsau/max_diskspace/local`. Der Vorschlagswert ist 1.000.000 Byte (ca. 1 MB). Bei Erreichen der maximalen Größe wird die Verfolgung sicherheitsrelevanter Ereignisse gestoppt.

Filter

Die zu verfolgenden Ereignisse definieren Sie in Filtern. Die Informationen werden im Kontrollblock im Shared Memory des Anwendungsservers abgelegt. Anhand dieser Informationen bestimmt das SAP-System, welche Audit-Meldungen in die Audit-Datei geschrieben werden.

Filter bestehen aus folgenden Informationen:

- Mandant
- Benutzer
- Audit-Klasse
 - Dialoganmeldung
 - RFC-/CPIC-Anmeldung
 - RFC-Funktionsaufruf
 - Transaktionsstart
 - Reportstart
 - Benutzerstammsatzänderung
 - sonstiges
- Gewichtung der zu verfolgenden Ereignisse
 - nur kritische
 - schwerwiegende und kritische
 - alle

Weitere Informationen finden Sie unter [Filter definieren \[Seite 16\]](#).

Der Audit-Analysereport

Den Inhalt der Audit-Dateien können Sie im Audit-Analysereport anzeigen. Information über den Audit-Analysereport finden Sie unter [Audit-Analysereport anzeigen \[Seite 18\]](#) und [Audit-Analysereport lesen \[Seite 20\]](#).

Alerts im Alert-Monitor des Computing Center Management System

Das Security-Audit-Log generiert auch Security-Alerts für die im Alert-Monitor des Computing Center Management System (CCMS) aufgezeichneten Ereignisse. Weitere Informationen finden Sie unter [Security-Alerts im CCMS-Alert-Monitor \[Seite 24\]](#).

Vergleich von Security-Audit-Log und Systemprotokoll

Vergleich von Security-Audit-Log und Systemprotokoll

Das Security-Audit-Log ergänzt das Systemprotokoll. Mit beiden Werkzeugen werden auf SAP-Systemen durchgeführte Aktionen aufgezeichnet. Allerdings verwenden sie geringfügig unterschiedliche Strategien und verfolgen andere Ziele wie der Vergleich unten zeigt.

Security-Audit-Log	Systemprotokoll
Ziel	
zeichnet sicherheitsrelevante Informationen auf, mit denen eine Reihe von Ereignissen nachvollzogen werden kann (z. B. erfolglose Anmeldeversuche oder Transaktionsstarts)	zeichnet Informationen auf, die Systemprobleme anzeigen (z. B. Datenbanklesefehler, Rollbacks)
Zielgruppe	
Auditoren	Systemverwalter
Flexibler Einsatz	
Sie können das Security-Audit-Log nach Bedarf aktivieren und deaktivieren. Ihnen steht frei, ob Sie die Verfolgung sicherheitsrelevanter Ereignisse in Ihrem System täglich durchführen. Sie können beispielsweise das Security-Audit-Log während eines Zeitraums vor einer geplanten Verfolgung sicherheitsrelevanter Ereignisse aktivieren und in der Zeit zwischen den Verfolgungen sicherheitsrelevanter Ereignisse deaktivieren.	Das Systemprotokoll wird ständig benötigt und sollte nicht deaktiviert werden.

Vergleich von Security-Audit-Log und Systemprotokoll

Verfügbarkeit der Protokolle

Die Audit-Logs werden lokal auf jedem Anwendungsserver gepflegt. Im Gegensatz zum Systemprotokoll werden die Audit-Logs täglich vom System gepflegt, und Sie müssen die Protokolldateien manuell archivieren oder löschen. Somit können Sie auf Audit-Logs der letzten Tage zugreifen, und die Audit-Logs sind länger verfügbar.

Es gibt zwei Arten Systemprotokolle: lokale und zentrale. Lokale Protokolle werden auf jedem einzelnen Anwendungsserver gepflegt. Diese Dateien sind zyklisch, werden also der Reihe nach wieder überschrieben, wenn sie voll sind. Die Größe der Protokolle sowie die Zeit, in der sie zur Verfügung stehen, sind begrenzt.

Sie haben auch die Möglichkeit, ein zentrales Protokoll zu pflegen. Allerdings ist das zentrale Protokoll derzeit nicht vollständig plattformunabhängig. Zur Zeit kann es nur auf einer UNIX-Plattform gepflegt werden. Das zentrale Protokoll wird ebenfalls nicht unbefristet aufbewahrt.

Umgang mit personenbezogenen Daten

Das Security-Audit-Log enthält personenbezogene Daten, die eventuell Datenschutzgesetzen unterliegen.

Sie müssen die Datenschutzgesetze sehr sorgfältig lesen, bevor Sie das Security-Audit-Log aktivieren.

Das Systemprotokoll enthält keine personenbezogenen Daten.

Statische Profile pflegen

Statische Profile pflegen

Verwendung

Sie geben die zu verfolgenden Informationen in Filtern an, die Sie

1. permanent in den statischen Profilen in der Datenbank erstellen und sichern

Wenn Sie diese Möglichkeit wählen, verwenden alle Anwendungsserver identische Filter, um die im Audit-Log aufzuzeichnenden Ereignisse zu bestimmen. Sie müssen die Filter nur einmal für alle Anwendungsserver definieren.

Sie können auch mehrere verschiedene Profile definieren, die Sie alternativ aktivieren können.

2. dynamisch auf einem oder mehreren Anwendungsservern ändern

Mit dieser Option können Sie Filter, mit denen Ereignisse für die Verfolgung ausgewählt werden, dynamisch ändern. Das System verteilt diese Änderungen an alle aktiven Anwendungsserver.

Dieser Abschnitt beschreibt wie Sie die Filter in statischen Profilen permanent in der Datenbank sichern. Informationen über das dynamische Ändern von Filtern finden Sie unter [Filter dynamisch ändern \[Seite 14\]](#).



In statischen Profilen gesicherte Filter werden nach dem nächsten Start des Anwendungsservers wirksam.

Voraussetzungen

Folgende Profilparameter müssen eingestellt sein:

Audit-Log-Profilparameter

Profilparameter	Beschreibung
rsau/enable	Security-Audit-Log aktivieren
rsau/local/file	Namen und Verzeichnisse der Audit-Dateien
rsau/max_diskspace/local	maximaler Platz, der Audit-Dateien zugewiesen werden kann
rsau/selection_slots	Anzahl der Filter, die für das Security-Audit-Log zulässig sind

Vorgehensweise

1. Um auf das Konfigurationsbild des Security-Audit-Log zu gelangen, wählen Sie im *SAP-Menü Werkzeuge* → *Administration* → *Monitor* → *Security-Audit-Log* → *Konfiguration*.

Sie gelangen auf das Bild *Security-Audit: Audit-Profil verwalten*, auf dem die Karteikarte *Stat. Konfiguration* aktiviert ist. Ist bereits ein aktives Profil vorhanden, wird es im Feld *Aktives Profil* angezeigt.

2. Geben Sie im Feld *Angezeigtes Profil* den Namen des zu pflegenden Profils ein.
3. Um ein neues Audit-Profil anzulegen, wählen Sie *Profil* → *Anlegen*. Um ein vorhandenes Profil zu ändern, wählen Sie *Profil* → *Anzeigen* <-> *Ändern*.



Um ein vorhandenes Profil anzuzeigen, bevor Sie es ändern, wählen Sie *Profil* → *Anzeigen*.

Der untere Bildbereich enthält Karteikarten, mit denen die Filter definiert werden. Die Anzahl der Registerkarten entspricht dem Wert des Profilparameters `rsau/selection_slots`. Auf jeder Registerkarte definieren Sie einen einzigen Filter.

4. [Definieren Sie Filter \[Seite 16\]](#) für Ihr Profil.
5. Vergewissern Sie sich, daß das Kennzeichen *Filter aktiv* für jeden der Filter gesetzt ist, die Sie für Ihr Audit verwenden wollen.
6. Sichern Sie die Daten.
7. Um das Profil zu aktivieren, wählen Sie *Profil* → *Aktivieren*.
8. Damit die Änderungen wirksam werden, fahren Sie den Anwendungsserver herunter und starten ihn erneut.

Ergebnis

Die von Ihnen definierten Filter werden im Audit-Profil gesichert. Wenn Sie das Profil aktivieren und den Anwendungsserver neu starten, werden Aktionen, die einem der aktiven Filterereignisse entsprechen, im Security-Audit-Log aufgezeichnet.



Auf einigen UNIX-Plattformen müssen Sie auch ausdrücklich das Programm `cleanipc` ausführen, um gemeinsamen Speicher frei zu machen. Sonst steht weiterhin die alte Konfiguration im gemeinsamen Speicher und die Änderungen am statischen Profil werden nicht wirksam.

Filter dynamisch ändern

Filter dynamisch ändern

Verwendung

Sie geben die zu verfolgenden Informationen in Filtern an, die Sie

1. permanent in den statischen Profilen in der Datenbank erstellen und sichern

Wenn Sie diese Möglichkeit wählen, verwenden alle Anwendungsserver identische Filter, um die im Audit-Log aufzuzeichnenden Ereignisse zu bestimmen. Sie müssen Filter nur einmal für alle Anwendungsserver definieren.

Sie können auch mehrere verschiedene Profile definieren, die Sie alternativ aktivieren können.

2. dynamisch auf einem oder mehreren Anwendungsservern ändern

Mit dieser Option können Sie Filter, mit denen Ereignisse für die Verfolgung ausgewählt werden, dynamisch ändern. Das System verteilt diese Änderungen an alle aktiven Anwendungsserver.

Dieser Abschnitt behandelt die dynamisch geänderten Filter. Informationen über das Definieren der Filter in statischen Profilen finden Sie unter [Statische Profile pflegen \[Seite 12\]](#).



Diese Änderungen sind solange aktiv, bis sie geändert werden oder der Anwendungsserver heruntergefahren wird.

Voraussetzungen

Folgende Profilparameter müssen eingestellt sein:

Audit-Log-Profilparameter

Profilparameter	Beschreibung
rsau/enable	Security-Audit-Log aktivieren
rsau/local/file	Namen und Verzeichnisse der Audit-Dateien
rsau/max_diskspace/local	maximaler Platz, der Audit-Dateien zugewiesen werden kann
rsau/selection_slots	Anzahl der Filter, die für das Security-Audit-Log zulässig sind

Vorgehensweise



1. Um auf das Konfigurationsbild des Security-Audit-Log zu gelangen, wählen Sie im *SAP-Menü Werkzeuge* → *Administration* → *Monitor* → *Security-Audit-Log* → *Konfiguration*.

Sie gelangen auf das Bild *Security-Audit: Audit-Profil verwalten*, auf dem die Karteikarte *Stat. Konfiguration* aktiviert ist.

2. Wählen Sie die Karteikarte *Dyn. Konfiguration* oder in der Menüleiste *Springen* → *Dyn. Konfiguration*.

Filter dynamisch ändern

Im oberen Bereich des Bildes erhalten Sie eine Liste der aktiven Instanzen mit deren Audit-Status. Der untere Bildbereich enthält Karteikarten zur Pflege der Filter.

3. Wählen Sie *Konfiguration* → *Anzeigen* <-> *Ändern*.
4. Definieren Sie für den Anwendungsserver [Filter \[Seite 16\]](#).
5. Vergewissern Sie sich, daß das Kennzeichen *Filter aktiv* für jeden der Filter gesetzt ist, die Sie im Audit auf dem Anwendungsserver anwenden wollen.
6. Falls Sie die Filterdefinition an alle Anwendungsserver verteilen wollen, wählen Sie *Konfiguration* → *Konfig. verteilen*.
7. Um den Audit-Status eines bestimmten Anwendungsservers zu ändern, markieren Sie das Statuskennzeichen in der Tabelle *Liste der aktiven Instanzen*.
 -  zeigt an, daß das Audit aktiviert ist.
 -  zeigt an, daß das Audit deaktiviert ist.
9. Um den (oder die) Filter auf allen Anwendungsservern zu aktivieren, wählen Sie *Konfiguration* → *Audit aktivieren*. (Um die Filter auf allen Anwendungsservern zu deaktivieren, wählen Sie *Konfiguration* → *Audit deaktivieren*.)



Wenn das Programm abbricht, prüfen Sie, ob Ihr Berechtigungsprofil die Berechtigung S_RFC mit dem Wert SECU enthält. (Das System verwendet Remote Function Calls, um eine Liste der Server zu erhalten; deshalb benötigen Sie die entsprechenden Berechtigungen.)

Ergebnis

Die Audit-Filter werden auf allen aktiven Anwendungsservern dynamisch erzeugt. Wenn Sie das (die) Profil(e) aktivieren, werden alle Aktionen, die diesen Filtern entsprechen, im Audit-Log aufgezeichnet. Änderungen an den Filterdefinitionen sind sofort wirksam und werden beibehalten bis der Anwendungsserver heruntergefahren wird.

Filter definieren

Filter definieren

Verwendung

Ereignisse, die das Security-Audit-Log aufzeichnen soll, definieren Sie in Filtern.

In den Filtern können Sie folgende Informationen angeben:

- Benutzer
- SAP-System-Mandant
- Audit-Klasse (z. B. Dialoganmeldeversuche oder Änderungen an den Benutzerstammsätzen)
- Gewichtung des Ereignisses (z. B. kritisch oder schwerwiegend)

Beispiele zu den Filtern finden Sie unter [Beispielfilter \[Seite 28\]](#).

Entweder definieren Sie Filter, die Sie in den statischen Profilen der Datenbank sichern (siehe [Statische Profile pflegen \[Seite 12\]](#)), oder Sie definieren dynamische Filter für einen oder mehrere Anwendungsserver (siehe [Filter dynamisch ändern \[Seite 14\]](#)).

Voraussetzungen

- Die Anzahl der Filter, die Sie angeben können, ist in Profilparameter `rsau/selection_slots` definiert.
- Entweder definieren Sie [statische Profile \[Seite 12\]](#) oder ändern [Filter dynamisch \[Seite 14\]](#) mit dem Konfigurationswerkzeug des Security-Audit-Log. Für jeden zugewiesenen Filter erscheint im unteren Bereich des Bildes eine Karteikarte.

Vorgehensweise

1. Wählen Sie die Karteikarte des Filters, den Sie definieren wollen.
2. Geben Sie in den entsprechenden Feldern die *Mandanten-* und *Benutzernamen* an.



Mit dem Platzhalter (*) können Sie den Filter für alle Mandanten und Benutzer definieren. Allerdings ist eine teilweise generische Eingabe wie z. B. 0* oder ABC* **nicht** möglich.

3. Wählen Sie die entsprechenden *Audit-Klassen* für die Ereignisse, die Sie verfolgen wollen.
4. Audit-Ereignisse werden in drei Kategorien unterteilt: kritische, schwerwiegende und unkritische. Wählen Sie die entsprechenden Kategorien für zu verfolgende Ereignisse:
 - *nur kritische*
 - *schwerwiegende und kritische*
 - *alle*
5. Sie können die zu verfolgenden Ereignisse genauer definieren:
 - a. Wählen Sie *Detailanzeige*.

Sie gelangen auf eine Tabelle, die eine detaillierte Liste der Audit-Klassen mit deren entsprechenden Ereignisklassen (kritisch, schwerwiegend, unkritisch) und

Filter definieren

Meldungstexten enthält. (Die Meldungstexte entsprechen den Systemprotokollmeldungen AU<X>.)

- b. Markieren Sie die Ereignisse, die verfolgt werden sollen. Sie können
- ein einzelnes Ereignis auswählen, indem Sie das Kennzeichen *Aufzeichnung* für ein besonderes Ereignis aktivieren
 - alle Ereignisse einer Audit-Klasse auswählen, indem Sie die Audit-Klasse (z. B. *Dialoganmeldung*) auswählen

- c. Wählen Sie *Änderungen übernehmen*. ✓

Sie gelangen wieder auf die Filterkarteikarten.



Falls Sie detaillierte Einstellungen vorgenommen haben, erscheinen die Kennzeichen der Audit- und Ereignisklassen nicht mehr auf den entsprechenden Filterkarteikarten. Um die detaillierten Einstellungen zurückzunehmen und wieder die Standardkonfiguration zu laden, wählen Sie *Reset*.

6. Um den Filter zu aktivieren, markieren Sie das Kennzeichen *Filter aktiv*.
7. Fahren Sie mit [statische Profile definieren \[Seite 12\]](#) oder [Filter dynamisch ändern \[Seite 14\]](#) fort.

Audit-Analysereport anzeigen

Audit-Analysereport anzeigen

Verwendung

Das Security-Audit-Log erzeugt einen Audit-Analysereport, der die verfolgten Aktivitäten enthält. Mit einem Audit-Analysereport können Sie Ereignisse analysieren, die auf einem lokalen, entfernten oder auf allen Servern des SAP-Systems eintraten und aufgezeichnet wurden.

Der vom Security-Audit-Log erstellte Audit-Analysereport ist genauso aufgebaut wie das [Systemprotokoll \[Extern\]](#).

Vorgehensweise

1. Wählen Sie im *SAP-Menü Werkzeuge* → *Administration* → *Monitor* → *Security-Audit-Log* → *Auswertung*.

Sie gelangen auf das Dialogfenster *AuditLog: lokale Auswertung auf <Rechnername>*; die lokale Auswertung ist standardmäßig eingestellt.

2. Wenn Sie einen entfernten Server analysieren wollen, wählen Sie *AuditLog* → *Auswählen* → *Entfernter AuditLog*. Wenn Sie alle Server analysieren wollen, wählen Sie *AuditLog* → *Auswählen* → *Alle AuditLogs*.

Ihre Wahl wird neben dem Feld *Eingelesene AuditLog-Einträge* angezeigt.

3. Wenn Sie einen entfernten Server analysieren wollen, geben Sie den Namen des Anwendungsservers im Feld *Instanzname* ein.
4. Geben Sie in den entsprechenden Feldern (z. B. *von Datum / Uhrzeit, bis Datum / Uhrzeit, Benutzer, Transaktionscode, Audit-Klassen* oder *Auszuwählende Ereignisse*) oder durch Auswählen der gewünschten Kennzeichen Eingrenzungen an, die Sie für den Audit-Analysereport verwenden wollen.



Ereignisse werden in drei Kategorien (kritische, schwerwiegende und unkritische Ereignisse) unterteilt, wobei kritische Ereignisse am wichtigsten sind. Sie können *nur kritische, schwerwiegende und kritische* oder *alle* Ereignisse anzeigen.

5. Um bestimmte Meldungen des Reports auszulassen oder aufzunehmen,
 - a. wählen Sie *Bearbeiten* → *Expertenmodus*
 - b. wählen Sie *Meldungsfilter*
 - c. wählen Sie *nur diese Meldungen* oder *alle außer diesen Meldungen*
 - d. geben Sie die Nummern der Meldungen an, die Sie aufnehmen oder auslassen wollen (Die Meldungsnummern entsprechen den Systemprotokollmeldungen AU<X>.)
 - e. wählen Sie *Benutzen*
6. Das Ausgabeformat können Sie mit der Auswahl in der Gruppe *Aufbereitung* ändern. Weitere Informationen finden Sie unter [Anzeigeoptionen für das Audit-Log \[Seite 27\]](#).
7. Wählen Sie eine der folgenden Möglichkeiten, um das Security-Audit-Log zu lesen:
 - Wählen Sie *AuditLog* → *AuditLog erneut lesen*, um ein Audit-Log zum ersten Mal zu lesen oder ein bereits gelesenes Audit-Log zu ersetzen.

Audit-Analysereport anzeigen

- Wählen Sie *AuditLog* → *Neu aufbereiten*, um das zuletzt angezeigte Audit-Log anzuzeigen. Sie können beispielsweise die Auswahlmöglichkeiten ändern, um den Audit-Analysereport zu modifizieren, ohne das Protokoll erneut zu lesen.
- Wählen Sie *Security-Audit-Log* → *AuditLog hinzulesen*, um den im Audit-Analysereport vorhandenen Informationen neue Informationen mit anderen Selektionskriterien hinzuzufügen.



Das Feld *Eingelesene AuditLog-Einträge* gibt an, wie viele Protokolleinträge das System aus der Protokolldatei gelesen hat. Wenn Sie das Einstiegsbild *AuditLog: lokale Auswertung auf <Rechnername>* zum ersten Mal aufrufen, enthält das Feld den Wert "0".

Audit-Log-Anzeige sortieren

Um den Audit-Analysereport zu sortieren, wählen Sie *AuditLog* → *Sortieren* → *<Sortieroption>*.

Folgende Sortieroptionen stehen zur Verfügung:

- Schreibfolge
- Uhrzeit
- Instanz

Ergebnis

Als Ergebnis erhalten Sie den Audit-Analysereport mit den Meldungen, die Ihre Selektionskriterien erfüllen. Durch Auswahl einer einzelnen Meldung erhalten Sie detailliertere Informationen (siehe [Audit-Analysereport lesen \[Seite 20\]](#)).

Lesen des Audit-Analysereports

Lesen des Audit-Analysereports

Dieser Abschnitt beschreibt, wie der in der Vorgehensweise [Audit-Analysereport anzeigen \[Seite 18\]](#) erstellte Audit-Analysereport ausgewertet wird.

Der zentrale Audit-Analysereport

Der Audit-Analysereport ist in vier Hauptbereiche unterteilt:

- Allgemeine Angaben
- Audit-Report
- Statistische Auswertung
- Inhaltsverzeichnis

Allgemeine Angaben

Ganz oben auf dem Report sehen Sie die Selektionsoptionen, die Sie für die Audit-Datei zur Erstellung dieses Reports verwendet haben (z. B. *von Datum / Uhrzeit, bis Datum / Uhrzeit, Benutzer* und *Audit-Klassen*).

Audit-Report

Der Audit-Report steht unter den Allgemeinen Angaben und enthält folgende Informationen zu jedem in der Audit-Datei gefundenen, den Selektionskriterien entsprechenden Audit-Ereignis (abhängig von Ihrer Anzeigekonfiguration):

- Datum
- Uhrzeit
- Instanz
- Kategorie (Dialog oder Hintergrund)
- Meldungsnummer
- Audit-Klassencode (z. B. gehört ein Dialoganmeldeversuch zu Klasse Nummer 002.)
- Benutzer
- Transaktionscode
- Terminalnummer

Am Ende der Liste befinden sich zusammenfassende Informationen (z. B. Anzahl der gelesenen Sätze, Anzahl der übersprungenen Sätze und die Audit-Dateinamen).

Statistische Auswertung

Wenn Sie die Anzeigeeption *mit statistischer Auswertung* gewählt haben, werden nach den Audit-Daten folgende Informationsblöcke aufgeführt:

- Instanzstatistik (wenn Sie alle Instanzen analysieren)
- Mandantenstatistik
- Reportstatistik
- Transaktionsstatistik

Lesen des Audit-Analysereports

- Benutzerstatistik
- Meldungsstatistik

Inhaltsverzeichnis

Am Ende des Reports befindet sich ein Inhaltsverzeichnis.

Der detaillierte Audit-Analysereport

Um Details zu einer bestimmten Meldung anzuzeigen, setzen Sie den Cursor auf den Eintrag und wählen *Bearbeiten* → *Details*. Eine detaillierte Beschreibung der Meldung, die Informationen wie den Aufgabennamen, die Klasse, die Meldungsdocumentation und die technischen Details des Audit-Datensatzes enthält, wird angezeigt.

Alte Audit-Dateien löschen

Alte Audit-Dateien löschen

Verwendung

Das Security-Audit-Log sichert seine Audits täglich in eine entsprechende Audit-Datei. Je nach Größe Ihres SAP-Systems und der angegebenen Filter, kann sich in kurzer Zeit eine enorme Datenmenge ansammeln.



Wir empfehlen Ihnen, Ihre Audit-Dateien regelmäßig zu archivieren und die Originaldateien nach Bedarf zu löschen.

Löschen Sie alte Audit-Dateien mit diesem Verfahren. Sie können die Dateien auf allen Anwendungsservern oder nur auf dem lokalen Server, auf dem Sie arbeiten, löschen. Ist ein Anwendungsserver während des Löschens nicht verfügbar, wird er bei der nächsten Reorganisation eingebunden.



Mit dieser Vorgehensweise löschen Sie nur die Audit-Log-Datei(en)! Andere Verwaltungsaufgaben wie Archivierungen werden **nicht** durchgeführt. Wenn Sie Archivierungen zu einem späteren Zeitpunkt noch einmal benötigen, müssen Sie die Audit-Log-Dateien vor dem Löschen manuell archivieren.



Sie können Dateien, die weniger als drei Tage alt sind, nicht löschen!

Vorgehensweise

1. Um das Reorganisationswerkzeug des Security-Audit-Log aufzurufen, wählen Sie im *SAP-Menü Werkzeuge* → *Administration* → *Monitor* → *Security-Audit-Log* → *Reorganisation*.
Sie gelangen auf das Bild *Security-Audit: Löschen alter Audit-Dateien*.
2. Geben Sie das *Mindestalter* der zu löschenden Dateien an (Standardwert = 30 Tage).
Dieser Wert muß > 3 sein.
3. Markieren Sie *Auf allen aktiven Instanzen*, um die Audit-Dateien auf allen Anwendungsservern zu löschen. Setzen Sie kein Kennzeichen, wenn Sie die Dateien nur auf dem lokalen Anwendungsserver löschen wollen.
4. Markieren Sie *Nur Simulation*, wenn Sie die Dateien eigentlich nicht löschen wollen. Dann wird das Löschen nur simuliert.
5. Wählen Sie *AuditLog* → *Weiter*.

Ergebnis

Das System löscht die entsprechenden Audit-Dateien (sofern Sie nicht *Nur Simulation* gewählt haben). Sie erhalten eine Liste, in der steht, wie viele Dateien auf jedem der Anwendungsserver gelöscht oder aufbewahrt wurden.

Security-Alerts im CCMS-Alert-Monitor

Security-Alerts im CCMS-Alert-Monitor

Wenn das Security-Audit-Log Ereignisse aufzeichnet, löst es auch einen entsprechenden Security-Alert im Alert-Monitor des Computing Center Management System (CCMS) aus.

Die erzeugten Security-Alerts entsprechen den Audit-Klassen der Ereignisse, die im Security-Audit-Log definiert sind. Dazu zählen:

- Dialoganmeldeversuche
- RFC-/CPIC-Anmeldeversuche
- Transaktionsstarts
- Reportstarts
- RFC-Funktionsaufrufe
- Änderungen an Benutzerstammsätzen
- Änderungen an der Konfiguration des Security-Audit-Log

Durch die Überwachung der Security-Alerts im CCMS-Alert-Monitor, können Sie schnell sicherheitsrelevante Probleme in Ihrem System identifizieren. Nachdem Sie die Sofortmaßnahmen zur Behebung des Alert ergriffen haben, können Sie die Security-Audit-Log-Dateien nach weiteren Informationen zu dem bestimmten Ereignis durchsuchen, das den Alert ausgelöst hat.

Sie können die Security-Alerts direkt am CCMS-Alert-Monitor anzeigen (siehe [Security-Alerts anzeigen \[Seite 25\]](#)) oder BAPIs (Business Application Program Interfaces) einsetzen, um über externe Programme auf Alerts zuzugreifen (siehe [Security-Alerts mittels BAPIs lesen \[Seite 26\]](#)).

Security-Alerts anzeigen

Voraussetzungen

Das Security-Audit-Log muß auf dem Anwendungsserver aktiviert sein, damit das Ereignis auch im CCMS-Alert-Monitor ausgelöst wird.

Vorgehensweise

1. Um den CCMS-Alert-Monitor aufzurufen, wählen Sie im *SAP-Menü Werkzeuge* → *CCMS* → *Steuerung/Monitoring* → *Alert-Monitor*.
Sie gelangen auf das Bild *CCMS-Monitorsammlungen*.
2. Um die Security-Alerts zu finden, expandieren Sie den Knoten *SAP CCMS Monitor Templates*.
3. Setzen Sie den Cursor auf den Knoten *Security*, und wählen Sie *Monitor* → *Monitor starten*.
Sie gelangen auf den Monitor *Security*.
Die vom Security-Audit-Log ausgelösten Alerts stehen unter dem Knoten des jeweiligen Anwendungsservers.
4. Expandieren Sie den Knoten des (oder der) betreffenden Anwendungsserver(s), den (die) Sie untersuchen wollen.
Die angezeigten Kategorien entsprechen den im Security-Audit-Log aufgezeichneten Audit-Klassen. Einträge mit aktiven Alerts werden rot oder gelb dargestellt, je nach dem höchsten Alert-Grad (kritisch oder schwerwiegend) in dieser Kategorie.
5. Markieren Sie die Kategorien, die Sie auf dem jeweiligen Anwendungsserver untersuchen wollen, oder den gesamten Knoten des Anwendungsservers.
6. Wählen Sie *Bearbeiten* → *Alerts* → *Alerts anzeigen*.
Sie gelangen auf eine Liste der ausgewählten Kategorien.
7. Bearbeiten Sie die Alerts, falls erforderlich.



Weitere Informationen zum CCMS-Alert-Monitor und wie Sie Alerts verarbeiten, finden Sie unter [Der Alert-Monitor \[Extern\]](#).

Security-Alerts mittels BAPIs lesen

Security-Alerts mittels BAPIs lesen

Die Security-Alerts stehen über BAPIs (Business Application Programming Interfaces) auch externen Programmen zur Verfügung. Der Report RSAU_READ_AUDITLOG_EXTERNAL ist ein Muster-SAP-Programm, das Sie als Vorlage für den Zugriff auf die Security-Alerts mittels BAPIs verwenden können.

Anzeigeoptionen des Audit-Log

Option	Bedeutung
<i>Anz. Seiten für Einzeleinträge</i>	Gibt die maximale Seitenanzahl an, die Sie anzeigen wollen. Dies gilt nur für den Hauptteil des Reports, nicht für die allgemeinen Angaben oder die zusammenfassenden Informationen.
<i>mit statistischer Auswertung</i>	Wenn Sie diese Option aktivieren, werden folgende Statistiken in Ihren Report aufgenommen: <ul style="list-style-type: none"> • Instanzstatistik (wenn Sie alle Instanzen analysieren) • Mandantenstatistik • Reportstatistik • Transaktionsstatistik • Benutzerstatistik • Meldungsstatistik
<i>Einstellungen</i>	Gibt das Layout und die Ausgabegeräte an.

Beispielfilter

Beispielfilter

Im folgenden Beispiel wird das Security-Audit-Log auf Server `pawdf021` aktiviert. Profil `PROFILE1` ist aktiv.

Bei *Filter 1* zeichnet das System alle Dialoganmeldeversuche, RFC- oder CPIC-Anmeldeversuche oder Transaktionsstarts auf, die als schwerwiegende oder kritische Ereignisse eingestuft sind. Die Ereignisse werden für alle Benutzer und für Ereignisse in allen Mandanten des SAP-Systems aufgezeichnet.

Für *Filter 2* zeichnet das System nur Ereignisse auf, die in Mandant 000 für `TESTBENUTZER` als kritisch eingestuft sind.

Beide Filter sind im System aktiv.

Filter 1



Filter 2

Beispielfilter

The screenshot shows the SAP Security Audit configuration interface. At the top, there is a menu bar with 'Profil', 'Bearbeiten', 'Springen', 'Umfeld', 'System', and 'Hilfe'. Below the menu is a toolbar with various icons. The main title is 'Security Audit: Audit-Profil ändern'. Underneath, there is a 'Stat. Konfiguration' tab. The configuration area shows 'Aktives Profil' and 'Angezeigtes Profil' both set to 'PROFILE1'. Below this, there are two filter tabs: 'Filter 1' and 'Filter 2'. The 'Filter 1' tab is active, showing a 'Filter Aktiv' checkbox checked, a 'Reset' button, and a 'Detaileinstellung' button. The filter settings are organized into three columns: 'Auswahl', 'Audit-Klassen', and 'Ereignisse'. The 'Auswahl' column has 'Mandant' set to '000' and 'Benutzer' set to 'TESTBENUTZER'. The 'Audit-Klassen' column has several checked items: 'Dialog-Anmeldung', 'RFC-/CPIC-Anmeldung', 'RFC Funktionsaufruf', 'Transaktionsstart', 'Reportstart', 'Benutzerstammänderung', and 'sonstiges'. The 'Ereignisse' column has three radio button options: 'nur kritische' (selected), 'schwerwiegende und kritische', and 'alle'. At the bottom of the window, there is a status bar showing 'A9B (1) (003)', 'pawdf021', and 'OVR'.