NAME

audispd−zos−remote − z/OS Remote-services Audit dispatcher plugin

SYNOPSIS

audispd−zos−remote [*config-file* **]**

DESCRIPTION

audispd−zos−remote is a remote-auditing plugin for the Audit subsystem. It should be started by the **auditd**(8) daemon and will forward all incoming audit events, as they happen, to a configured z/OS SMF (Service Management Facility) database, through an IBM Tivoli Directory Server (ITDS) set for Remote Audit service. See**SMF MAPPING** section belo w for more information about the resulting SMF record format.

auditd(8) must be configured to start the plugin. This is done by a configuration file usually located at */etc/audit/plugins.d/audispd−zos−remote.conf* , but multiple instances can be spawned by having multiple configuration files in */etc/audit/plugins.d* for the same plugin executable (see **auditd**(8)).

Each instance needs a configuration file, located by default at */etc/audit/zos−remote.conf* . Check**zos−r emote.conf**(5) for details about the plugin configuration.

OPTIONS

config-file

Use an alternate configuration file instead of */etc/audit/zos−remote.conf* .

SIGNALS

audispd−zos−remote reacts to SIGTERM and SIGHUP signals (according to the **auditd**(8) specification):

SIGHUP

Instructs the **audispd−zos−remote** plugin to re-read it's configuration and flush existing network connections.

SIGTERM

Performs a clean exit. **audispd−zos−remote** will wait up to 10 seconds if there are queued events to be delivered, dropping any remaining queued events after that time.

IBM z/OS ITDS Server and RACF configuration

In order to use this plugin, you must have an IBM z/OS v1R8 (or higher) server with IBM Tivoli Directory Server (ITDS) configured for Remote Audit service. For more detailed information about how to configure the z/OS server for Remote Auditing, refer to **z/OS V1R8.0-9.0 Integrated Security Services Enterprise Identity Mapping (EIM) Guide and Reference** (*http://publibz.boulder.ibm.com/cgi−bin/bookmgr_OS390/FRAMESET/EIMA1140/CCONTENTS?DT=20070827115119*), chapter "2.0 - Working with remote services".

Enable ITDS to process Remote Audit requests

To enable ITSD to process Remote Audit requests, the user ID associated with ITDS must be granted READ access to the IRR.AUDITX FACILITY Class profile (the profile used to protect the R_Auditx service). This user ID can usually be found in the STARTED Class profile for the ITDS started procedure. If the identity associated with ITDS is *ITDSUSER*, the administrator can configure RACF to grant Remote Auditing processing to ITDS with the following TSO commands:

TSO Commands: Grant ITDSUSER READ access to IRR.AUDITX FACILITY Class profile

rdefine FACILITY IRR.RAUDITX uacc(none)
permit IRR.RAUDITX class(FACILITY) id(ITDSUSER) access(READ)

Create/enable RACF user ID to perform Remote Audit requests

A z/OS RACF user ID is needed by the plugin - Every Audit request performed by the plugin will use a RACF user ID, as configured in the plugin configuration **zos−remote.conf**(5). This user ID needs READ access to FACILITY Class resource IRR.LDAP.REMOTE.AUDIT. If the user ID is *BINDUSER*, the administrator can configure RACF to enable this user to perform Remote Auditing requests with the following TSO commands:

TSO Commands: Enable BINDUSER to perform Remote Audit requests

```
rdefine FACILITY IRR.LDAP.REMOTE.AUDIT uacc(none)
permit IRR.LDAP.REMOTE.AUDIT class(FACILITY) id(BINDUSER) access(READ)
```

Add @LINUX Class to RACF

When performing remote auditing requests, the **audispd−zos−remote** plugin will use the special **@LINUX** *CDT Class* and the audit record type (eg.: **SYSCALL**, **AVC**, **PATH**...) as the*CDT Resour ce Class* for all events processed. To make sure events are logged, the RACF server must be configured with a Dynamic CDT Class named **@LINUX** with correct sizes and attributes. The following TSO commands can be used to add this class:

TSO Commands: Add @LINUX CDT Class

```
rdefine cdt @LINUX cdtinfo(posit(493) FIRST(alpha,national,numeric,special) OTHER(alpha,national,numeric,spec
setr classact(cdt)
setr raclist(cdt)
setr raclist(cdt) refresh
setr classact(@LINUX)
setr raclist(@LINUX)
setr generic(@LINUX)
```

Add profiles to the @LINUX Class

Once the CDT Class has been defined, you can add profiles to it, specifying resources (wildcards allowed) to log or ignore. The following are examples:

TSO Commands: Log only AVC records (One generic and one discrete profile):

```
rdefine @LINUX * uacc(none) audit(none(read))
rdefine @LINUX AVC uacc(none) audit(all(read))
setr raclist(@LINUX) refresh
```

TSO Commands: Log everything (One generic profile):

```
rdefine @LINUX * uacc(none) audit(all(read))
setr raclist(@LINUX) refresh
```

Resources always match the single profile with the *best* match.

There are many other ways to define logging in RACF. Please refer to the server documentation for more details.

SMF Mapping

The ITDS Remote Audit service will cut SMF records of type 83 subtype 4 every time it processes a request. This plugin will issue a remote audit request for every incoming Linux Audit record (meaning that one Linux record will map to one SMF record), and fill this type's records with the following:

Link Value

The Linux event serial number, encoded in network-byte order hexadecimal representation. Records within the same Event share the same Link Value.

Violation
Always zero (0) - *False*

Event Code
Always two (2) - *Authorization* event

Event Qualifier
Zero (0) - *Success*, if the event reported **success=yes** or **res=success**, Three (3) - *Fail*, if the event reported **success=no** or **res=failed**, or One (1) - *Info* otherwise.

Class
Always *@LINUX*

Resource
The Linux record type for the processed record. e.g.: *SYSCALL*,*AVC*,*PATH*,*CWD* etc.

Log String
Textual message bringing the RACF user ID used to perform the request, plus the Linux hostname and the record type for the first record in the processed event. e.g.: *Remote audit request from RACFUSER. Linux (hostname.localdomain):USER_AUTH*

Data Field List
Also known as *relocates*, this list will bring all the field names and values in a **fieldname=value** format, as a type 114 (**Application specific Data**) relocate. The plug-in will try to interpret those fields (i.e.: use human-readable username **root** instead of numeric userid **0**) whenever possible. Currently, this plugin will also add a relocate type 113 (**Date And Time Security Event Occurred**) with the Event Timestamp in the format as returned by **ctime**(3).

ERRORS

Errors and warnings are reported to syslog (under DAEMON facility). In situations where the event was submitted but the z/OS server returned an error condition, the logged message brings a name followed by a human-readable description. Below are some common errors conditions:

NOTREQ - No logging required
Resource (audit record type) is not set to be logged in the RACF server - The @LINUX Class profile governing this audit record type is set to ignore. See **IBM z/OS RACF Server configuration**

UNDETERMINED - Undetermined result
No profile found for specified resource. There is no @LINUX Class configured or no @LINUX Class profile associated with this audit record type. See **IBM z/OS RACF Server configuration**

UNAUTHORIZED - The user does not have authority the R_auditx service
The user ID associated with the ITDS doesn't have READ access to the IRR.AUDITX FACILITY Class profile. See **IBM z/OS RACF Server configuration**

UNSUF_AUTH - The user has insufficient authority for the requested function
The RACF user ID used to perform Remote Audit requests (as configured in **zos-remote.conf**(5)) don't have access to the IRR.LDAP.REMOTE.AUDIT FACILITY Class profile. See **IBM z/OS RACF Server configuration**

BUGS

The plugin currently does remote auditing in a best-effort basis, and will discard events in case the z/OS server cannot be contacted (network failures) or in any other case that event submission fails.

FILES

/etc/audit/plugins.d/audispd−zos−remote.conf /etc/audit/zos−remote.conf

SEE ALSO

auditd(8), **zos−remote.conf**(5).

AUTHOR

Klaus Heinrich Kiwi <klausk@br.ibm.com>