IBM Tivoli Access Manager
for Operating Systems

Audit Log Consolidation ReadMe

Version 4.1

IBM Tivoli Access Manager
for Operating Systems

Audit Log Consolidation ReadMe

Version 4.1

Note
Before using this information and the product it supports, read the information “Notices”, on page 37.

First Edition, (June 2003)

This edition applies to version 4, release 1, of IBM Tivoli Access Manager for Operating Systems (product number 5698-PDO).

Contents

Preface

This documentation provides information on installing, configuring, and operating the technical preview version of the audit log consolidation feature for IBM Tivoli Access Manager for Operating Systems, Version 4.1. This version of the audit log consolidation feature of IBM Tivoli Access Manager for Operating Systems is offered on an as-is basis to users who are currently using or evaluating Tivoli Access Manager for Operating Systems, Version 4.1. This feature only works with Version 4.1 of Tivoli Access Manager for Operating Systems. It is intended for evaluation purposes only and should not be used on production systems. There is no technical support available for this feature. This technical preview version of the software is not upgradeable to the next release.

Note: Install the IBM Tivoli Access Manager for Operating Systems Version 4.1, fix pack 1 (4.1–DPO-FP01) before installing the audit log consolidation code. Installation of the fix pack is not required to run the audit log consolidation code.

Who should read this guide

This book is for administrators and system programmers who have some knowledge of these topics:

- UNIX® operating system
- Internet protocols, including HTTP, TCP/IP, FTP, Telnet, SSL
- Security management
- Authentication
- Authorization
- IBM Tivoli Access Manager Base
- Lightweight Directory Access Protocol (LDAP) and directory services

Supplementary information that systems administrators may find useful includes knowledge of the following topics:

- IBM Tivoli Management Environment framework
- IBM Tivoli Enterprise Console®
- IBM SecureWay Directory
- IBM Tivoli User Administration

Publications

The Tivoli Access Manager for Operating Systems library and any other related documents are available for download from the Tivoli Information Center at:

http://publib.boulder.ibm.com/tividd/td/tdprodlist.html

Conventions used in this guide

This book uses several conventions for special terms and actions, operating system-dependent commands and paths, and margin graphics.

Typeface conventions

This guide uses the following IBM-style typeface conventions:

Bold	Lowercase and mixed-case commands, command options, and flags that appear within text are displayed like **this,** in **bold** type. Graphical user interface elements (except for titles of windows and dialogs) and names of keys are also displayed like **this,** in **bold** type.
Italics	Variables, values you must provide, new terms, and words and phrases that are emphasized are displayed like *this,* in *italic* type.
`Monospace`	Commands, command options, and flags that appear on a separate line, code examples, output, and message text are displayed like `this`, in a `monospace` font. Names of files and directories, text strings you must type, when they appear within text, names of Java methods and classes, and HTML and XML tags also are displayed like `this`, in a `monospace` font.

Chapter 1. Overview

The audit log consolidation feature of Tivoli Access Manager for Operating Systems provides the functionality to read records from the existing Tivoli Access Manager for Operating Systems audit logs and to send filtered/formatted data to the following destinations: a local text file, an e-mail address, a remote collection point (which is a Tivoli Access Manager authorization server, pdacld) or all three destinations. Additionally, audit log consolidation provides the functionality for the **pdacld** server to receive input from multiple Tivoli Access Manager for Operating Systems endpoints and consolidate the data into a single file.

The primary component of the audit log consolidation feature is **pdoslrd**, the log router daemon. The daemon reads a Tivoli Access Manager for Operating Systems audit record from an input channel, formats the record, and queues the record for the output channels to process. Each output channel dequeues a formatted audit record, applies a filter (if one has been specified for that channel), and, if the record is not filtered out, formats the record into the proper output format, and sends it to its destination (local file, e-mail, or remote host).

The audit log consolidation feature has separate control command. That is, it has a unique command for starting, stopping, and configuring the daemon. At installation, the code will be protected by native access controls. Additionally, if the other Tivoli Access Manager for Operating Systems daemons are active, default ACLs will protect the **pdoslrd** daemon and any written logs. The functions of the endpoint log router are to read records from the existing audit log, filter/format the raw data for the specified destination, and then transfer the filtered records to the specified destination. Supported destinations in this release include a text file, an e-mail notification, and a configured Tivoli Access Manager authorization server (**pdacld**). The destinations and associated filters are externally specified in a control file. The data sent to the **pdacld** destination will be encoded in UTF-8 format. The function of the **pdacld** server is to receive records sent from multiple endpoint log routers, and record them in a UTF-8 encoded file. A command-line utility (**pdoscollview**) is provided to select and output records from the UTF-8 encoded file to the screen or a text file encoded in the locale of the local machine. The **pdoscollview** utility works only on Tivoli Access Manager for Operating Systems endpoints. The endpoints do not have to be configured, however. In addition, the **pdacld** server must be running on a machine that has Tivoli Access Manager for Operating Systems installed.

Note: The audit log consolidation technical preview software is not upgradeable to the next release of the product.

Chapter 2. Installation and Configuration

This chapter contains the information necessary to install and configure the audit log consolidation technology preview code.

Installation

Prerequisites

The audit log consolidation code can be installed on any endpoint machine that is capable of running Tivoli Access Manager for Operating Systems, Version 4.1. See the *Tivoli Access Manager for Operating Systems, Version 4.1, Installation Guide* and *Tivoli Access Manager for Operating Systems, Version 4.1, Release Notes* for a list of the currently supported platforms, as well as any prerequisites, before installing the audit log consolidation files. The code will not run on any other version of Tivoli Access Manager for Operating Systems.

Note: Install the IBM Tivoli Access Manager for Operating Systems Version 4.1, fix pack 1 (4.1–PDO-FP01) before installing the audit log consolidation code. Installation of the fix pack is not required to run the audit log consolidation code.

The Tivoli Access Manager authorization server (**pdacld**) must be installed on the machine that will be used to collect inputs from the audit log consolidation endpoint machines. For testing the preview version of the software, the authorization server and the audit log consolidation endpoint can be installed on the same machine.

Installation Procedure

The technical preview software download consists of the following files:

Table 1. Packaged Files

Filename	Location	Description
	Permissions Owner Group	
pdoslrd	/opt/pdos/bin	Log router daemon
	-r-xr-s--- root ossaudit	
rc.pdoslrd	/opt/pdos/bin	Daemon startup script
	-r-xr-s-- root osseal	
pdoslradm	/opt/pdos/bin	Daemon admin command
	-r-xr-s-- root osseal	
pdoscollview	/opt/pdos/bin	Collection file viewer
	-r-xr-s--- root ossaudit	
*LRD_AuditInput	/opt/pdos/lib	Audit log input channel
	-rwxr-xr-x osseal osseal	
*LRD_FileOutput	/opt/pdos/lib	Text file output channel
	-rwxr-xr-x osseal osseal	
*LRD_NetOutput	/opt/pdos/lib	Network output channel

Table 1. Packaged Files (continued)

Filename	Location	Description
	Permissions Owner Group	
	-rwxr-xr-x osseal osseal	
*LRD_EmailOutput	/opt/pdos/mflr/channel	E-mail output channel
	-rwxr-xr-x osseal osseal	
pdoslrd.routing	/opt/pdos/etc/trac	Trace routing file
	-rw-rw---- osseal osseal	
pdoslrd.conf.template	/opt/pdos/etc	Configuration file template
	-r--r----- root osseal	
pdoslrd.xml.template	/opt/pdos/etc	Log router control file template.
	-rw-rw---- root ossaudit	
pdoslrd.dtd	/opt/pdos/etc	Control file: document type definition file
	-rw-rw---- root ossaudit	

*Shared library files will be named with the appropriate operating system extension (for example, .a, .so, .sl, etc.).

Installing on an Endpoint Machine

To install the preview software on an endpoint machine that already has Tivoli Access Manager for Operating Systems installed, complete the following procedure:

1. Log in to the system as root.
2. Stop the Tivoli Access Manager for Operating Systems daemons, using the following command:

   ```
   rc.osseal stop
   ```

3. Change directory to root, using the following command:

   ```
   cd /
   ```

4. Extract the contents of the archive file, using the following command:

   ```
   tar –xvf  $scratch/PDOS-interp.preview.tar
   ```

   where *$scratch* is the directory where the archive file is located and *interp* is one of the following: aix, solaris, hpux, linux-x86, or linux-s390.
5. Configure the log router daemon, using the following command:

   ```
   pdoscfg.preview –lrd_config on –lrd_logs num_logs –lrd_log_entries num_entries
   ```

   where *num_logs* is the number of error log files to use before recycling them and *num_entries* is the number of the entries per log. The default for num_entries is zero; if selected, the logs will never be rolled over.

   Note: Both –lrd_logs *num_logs* and –lrd_log_entries *num_entries* are optional.
6. Update the default policy, using the following command:

   ```
   pdos_defpolicy_update –f /opt/pdos/etc/osseal.per-policy.preview
   ```

   Note: This update only has to be done once per branch.

7. Restart the Tivoli Access Manager for Operating Systems daemons, using the following command:

   ```
   rc.osseal start
   ```

   Note: Ensure that auditing is enabled after restarting the Tivoli Access Manager for Operating Systems daemons.
8. Edit the log router control file, `/opt/pdos/pdoslrd.xml` and set the state of the router to on. Also, ensure to set the state of the input channel and at least one output channel to on. Otherwise, the log router daemon starts and then exits. For more information, refer to Chapter 3, “Control”, on page 9.
9. Start the log router daemon, using the following command:

   ```
   rc.pdoslrd start
   ```

Note: If you want to install the audit log consolidation code on a clean machine, you must first install Tivoli Access Manager for Operating Systems on the machine, using either the InstallShield Multiplatform procedure or the native procedure for your particular operating system. See the *IBM Tivoli Access Manager for Operating Systems, Version 4.1, Installation Guide* and the *IBM Tivoli Access Manager for Operating Systems, Version 4.1, Release Notes* for information about installing the product.

Installing the pdacld Server

If you did not install the Tivoli Access Manager authorization server (**pdacld**) when you installed the policy server, you must do so now. Review the instructions in the *IBM Tivoli Access Manager Base Installation Guide, Version 4.1*. You should also read the appropriate sections of the *IBM Tivoli Access Manager Base Administrator's Guide, Version 4.1*.

To install the **pdacld** server on a machine with Tivoli Access Manager installed, use the following procedure:

1. Ensure that you are logged onto your system as the root administrator.
2. Insert the *IBM Tivoli Access Manager Base CD* for your particular operating system.
3. Run the **ezinstall_pdacld** script, located in the root directory on the CD.

If you want to install the authorization server on a clean machine, you must first install and configure a Tivoli Access Managerpolicy server on that machine. See the *IBM Tivoli Access Manager Base Installation Guide, Version 4.1* for detailed instructions.

Configuration

Use the **pdoscfg.preview** command to configure audit log consolidation. Initial configuration occurs after the log router has been installed and before it can be executed. The **pdoscfg.preview** command has three options that pertain to the **pdoslrd** daemon:

–lrd_config (on | off)
: A value of on means that **pdoslrd** is to be configured. The default value of off means that **pdoslrd** is not to be configured. If **pdoslrd** is not configured, it will not be started when `rc.osseal start` is run.

–lrd_log_entries
: The number of **pdoslrd** error log entries to use before rolling over to a new log. The default of zero means never roll over to a new log.

–lrd_logs

The number of **pdoslrd** error log files to use before recycling log files. The default of zero indicates that log files should never be recycled. Setting lrd_logs to a nonzero value has an effect only if lrd_log_entries is nonzero.

Unconfiguring and Uninstalling

In order to unconfigure and uninstall the audit log consolidation preview software, follow these steps:

1. Log into the system as root.
2. Stop the log router daemon, using the following command:

   ```
   rc.pdoslrd stop
   ```

3. Stop the Tivoli Access Manager for Operating Systems daemons, using the following command:

   ```
   rc.osseal stop
   ```

4. Unconfigure the log router daemon, using the following command:

   ```
   pdoscfg.preview -lrd_config off
   ```

5. Remove the default policy, using the following **pdadmin** commands. /%POLICY%/ indicates the branch name. This needs to be done only once per branch.

   ```
   pdadmin> object delete   /OSSEAL/%POLICY%/TCB/Secure-Files/opt/pdos/etc/
                            pdoslrd.dtd
   pdadmin> object delete   /OSSEAL/%POLICY%/TCB/Immune-Programs/opt/pdos/
                            bin/pdoslrd
   pdadmin> object delete   /OSSEAL/%POLICY%/TCB/Immune-Programs/opt/pdos/
                            bin/pdoslradm
   pdadmin> acl detach      /OSSEAL/%POLICY%/File/opt/pdos/bin/rc.pdoslrd
   pdadmin> acl detach      /OSSEAL/%POLICY%/File/var/pdos/pdoslrd
   pdadmin> object delete   /OSSEAL/%POLICY%/File/opt/pdos/bin/rc.pdoslrd
   pdadmin> object delete   /OSSEAL/%POLICY%/File/var/pdos/pdoslrd
   ```

6. 6. Remove the following audit log consolidation preview links, files and directories.

   On all platforms:

   ```
   /usr/bin/pdoslrd
   /usr/bin/pdoslradm
   /usr/bin/pdoscollview
   /usr/bin/rc.pdoslrd
   /usr/bin/pdoscfg.preview
   /opt/pdos/bin/pdoslrd
   /opt/pdos/bin/pdoslradm
   /opt/pdos/bin/pdoscollview
   /opt/pdos/bin/rc.pdoslrd
   /opt/pdos/bin/pdoscfg.preview
   /opt/pdos/etc/osseal.per-policy.preview
   /opt/pdos/etc/pdoslrd.xml.template
   /opt/pdos/etc/pdoslrd.xml
   /opt/pdos/etc/pdoslrd.dtd
   /opt/pdos/etc/trace/pdoslrd.routing
   /var/pdos/pdoslrd
   ```

   Solaris, Linux and s390-Linux:

   ```
   /usr/lib/LRD_AuditInput.so
   /usr/lib/LRD_EmailOutput.so
   /usr/lib/LRD_FileOutput.so
   /usr/lib/LRD_NetOutput.so
   /usr/lib/libamosxerces-c.so
   /opt/pdos/lib/LRD_AuditInput.so
   ```

```
/opt/pdos/lib/LRD_EmailOutput.so
/opt/pdos/lib/LRD_FileOutput.so
/opt/pdos/lib/LRD_NetOutput.so
/opt/pdos/lib/libamosxerces-c.so
```

AIX:

```
/usr/lib/LRD_AuditInput.a
/usr/lib/LRD_EmailOutput.a
/usr/lib/LRD_FileOutput.a
/usr/lib/LRD_NetOutput.a
/usr/lib/libamosxerces-c.a
/opt/pdos/lib/LRD_AuditInput.a
/opt/pdos/lib/LRD_EmailOutput.a
/opt/pdos/lib/LRD_FileOutput.a
/opt/pdos/lib/LRD_NetOutput.a
/opt/pdos/lib/libamosxerces-c.a
```

HP-UX:

```
/usr/lib/LRD_AuditInput.sl
/usr/lib/LRD_EmailOutput.sl
/usr/lib/LRD_FileOutput.sl
/usr/lib/LRD_NetOutput.sl
/usr/lib/libamosxerces-c.sl
/opt/pdos/lib/LRD_AuditInput.sl
/opt/pdos/lib/LRD_EmailOutput.sl
/opt/pdos/lib/LRD_FileOutput.sl
/opt/pdos/lib/LRD_NetOutput.sl
/opt/pdos/lib/libamosxerces-c.sl
```

Chapter 3. Control

This chapter explains how to modify the control file in order to run the **pdoslrd** daemon.

Log Router Control File

A control file is used to specify the various parameters necessary to run the **pdoslrd** daemon. The pathname of this file is `/opt/pdos/etc/pdoslrd.xml`. Use a text editor to modify this file. You can also use the **pdoslradm** command to view and modify certain options of the Channel elements. The format of this control file must comply with the XML 1.0 specification.

Note: The log router control file, `pdoslrd.xml`, is encoded in UTF-8. This means that all the characters in the file are interpreted as UTF-8. As a result, the file should only be edited using an editor that supports UTF-8. If your locale is en_US, any editor that supports ASCII will suffice.

The following sections identify and define the various control options supported by **pdoslrd**. The first section contains a sample control file.

Log Router Control File Example

The following example shows a control file with an input channel and three output channels. All audit records are sent to the Tivoli Access Manager authorization server named gerrywaix. Only login - denies are sent to the LRD_EmailOutput channel. The file-admin channel is off.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE Server SYSTEM "opt/pdos/etc/pdoslrd.dtd">
<Server>

  <Router name="router 1" state="on"
    <Channel name="input" type="LRD_AuditInput"
             path="var/pdos/audit/audit.log" state="on"/>
    <Channel name="file-admin" type="LRD_FileOutput"
             path="var/pdos/pdoslrd/audit.out" format="keyvalue" state="off"/>
    <Channel name="mail-admin" type="LRD_EmailOutput"
             server="devmail.dev.tivoli.com" port="25"
             address="admin@myhost.tivoli.com" port="7136" filter="login-deny"
             state="on"/>
    <Channel name="netout-admin" type="LRD_NetOtput"
             server="gerrywaix.dev.tivoli.com" port="7136"
             compress="yes" state="on"
  </Router>

  <Filters>
    <Filter name="login-deny">
      <Conditional type="include">
        <Field name="resource_type" value="Login"/>
        <Field name="view" value="D"/>
      </Conditional>
    </Filter>
  </Filters>

</Server>
```

Log Router Control File Elements

The log router control file is comprised of the following elements and options:

- XML header
- Server element
- Router element
- Channel element
- Filters element
- Filter element
- Conditional element
- Field element

XML Header

The XML header is required by the XML specification and should comprise the first lines in the Log Router control file. These lines are as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE Server SYSTEM "opt/pdos/etc/pdoslrd.dtd">
```

Server Element

The Log Router control file must contain exactly one Server element. All other elements are contained within the Server element. It has no options.

Usage	
<Server>	Begin tag
</Server>	End tag
Options	
None	

Router Element

The Log Router control file must contain at least one Router element. Each Router element must contain at least one input channel and one output channel definition. In this preview release, only one router element per control file will be supported.

Usage

Usage	
<Router>	Begin tag
</Router>	End tag
Options	
name	The name of the router (a unique name). This is required.
state	The state of the router (on or off). This is required.
hi water	The maximum number of audit records that can be queued up for the output channels to process. When this point is reached for any output channel, the log router will stop reading records from the input channel until the output channel removes at least one record from its queue. The default value is 1000. If the value zero is specified, the output channel queues may grow unbounded, unless the **pdoslrd** process's virtual memory is exhausted.

Example

```
<Server>
  <Router name="router1" state="on" hi_water="5000"

    <!-- Input channel definition -->
    <Channel name="audlog" type="LRD_AuditInput"
      path="/var/pdos/audit/audit.log" state="on" />

    <!-- Output channel -->
    <Channel name="file" type="LRD_FileOutput" path="/home/sysadmin/audit.out"
      format="concise" state="on"/>

  </Router>
</Server>
```

Channel Element

The Channel element is used to specify an input channel and one or more output channels used by a particular router to process records. The input channel reads data records from a particular source and prepares the record for processing by the output channels. The output channels format the data record for output and apply any filtering or formatting that has been defined. The examples that follow the usage table provide an example of an input channel and several output channels. Channels are implemented as dynamically loaded libraries. The Channel element applies to a particular Router and can only be used between Router tags.

Usage

Usage	
<Channel.../>	Channel element
Options	
name	The name of the channel (a unique name). This is required.
type	The type of channel (such as LRD_FileOutput). This is required.
state	The state of the channel (on or off). This is required.
path	The directory and name of the input or output file.
filter	The name of the filter to be used (output channels only).
error	Error Retry Timeout. The number of seconds to wait before retrying an error. (output channels only). [default=2]
format	The name of the format for this channel (LRD_FileOutput channels only). Value may be concise or keyvalue. [default=concise]
max_*files*	Maximum number of rollover files. When this number is reached, the output file will grow without bound. A value of zero means there is no maximum number of rollover files. (LRD_FileOutput channels only). [default = 0]
rollover_size	Maximum size (in bytes) of an output file. When an output file reaches this size, a rollover is performed. A value of zero means that the file will grow indefinitely. (LRD_FileOutput channels only). [default = 0]
delimiter	Field delimiter value. This can be used to change the field delimiter value for concise or keyvalue format (for this channel only) from the default value of comma. (LRD_FileOutput channels only).

server	The host name to send the record to (only for LRD_EmailOutput and LRD_NetOutput channels).
port	The port number on the server (only for LRD_EmailOutput and LRD_NetOutput channels). [defaults: LRD_EmailOutput=25; LRD_NetOutput=7136]
rebind	Rebind Retry Timeout. The number of seconds to wait before rebinding to the server after it has become unavailable (only for LRD_EmailOutput and LRD_NetOutput channels). [defaults: LRD_EmailOutput=60; LRD_NetOutput=300]
compress	Whether to compress records (yes or no) (LRD_NetOutput channels only). Records will be uncompressed on the server machine. [default=no]
dn	Distinguished Name of remote server (LRD_NetOutput channels only).
buffer	The maximum sized message (in bytes) that will be constructed by combining audit records into a large buffer. Audit records are not split across buffers. (LRD_NetOutput channels only). [default=1024]
flush_interval	The maximum number of seconds an audit record will reside in a buffer before being forwarded (LRD_NetOutput channels only). [default=600]
queue_size	Maximum number of audit records that can be queued before blocking the requesting thread (LRD_NetOutput channels only). [default=0 (no limit)]
hi_water	Processing the input queue is scheduled regularly at the flush interval. It is also triggered by the queue size reaching the high water mark (LRD_NetOutput channels only). [default=100]
address	Email address (LRD_EmailOutput channels only).

Examples

```
<!-- This is an input channel that will read using the base file specified
  by the path -->
<Channel name="log_input" type="LRD_AuditInput" path="/var/pdos/audit/audit.log"
  state="on" />

<!-- This is an output channel that will write data records to the directory
  and file specified by the path. The format is the concise output of the
  pdosaudview command.-->
<Channel name="fileout1" type="LRD_FileOutput" path="/var/pdos/pdoslrd/audit.out"
  format="concise" state="on" />

<!-- This is an output channel that will write data records to e-mail. The format
  is fixed for this destination and cannot be changed. -->
<Channel name="mail1" type=LRD_EmailOutput" server="mailserv.tivoli.com"
  port="25" address=bjxnes@us.ibm.com state="on"/>

<!-- This is an output channel that will write data records to the server
  specified by server and port. The format is fixed for this destination
  and cannot be changed. -->
<Channel name="netout-admin" type=LRD_NetOutput" server="toasty.ibm.com"
  port="7136" state="on" />
```

Filters Element

The Log Router control file must contain exactly one Filters element. All Filter elements are contained within the Filters element. It has no options.

Usage

Usage	
<Filters>	Begin tag
</Filters>	End tag
Options	
None	

Filter Element

The Filter element is used to specify the conditions under which a particular record will be included or excluded. A Filter element must contain at least one Conditional element. All Filter elements are contained within the Filters element.

Usage

Usage	
<Filter>	Begin tag
</Filter>	End tag
Options	
name	A unique filter name.

Examples

```
<Filters>
  <!-- This is a filter with an include type Conditional element. The record will
    included if the value of the field "resource_type" is "Login" AND the value of
    the field "view"
    is "D" (for Deny) -->

  <Filter name="filter1">
    <Conditional type="include">
      <Field name="resource_type" value="Login" />
      <Field name="view" value="D" />
    </Conditional>
</Filter>

<!-- This is a filter with an exclude type Conditional element. The record will
  be excluded if the value of "view" is "Trace". -->

  <Filter name="filter2">
    <Conditional type="exclude">
      Field name="view" value="Trace" />
    </Conditional>
  </Filter>
</Filters>
```

Filter Definitions

Following are several examples of log router filter definitions. The examples show two types of conditional elements (include and exclude), as well as the Field elements options: value and name2. Some of these filters are contained in the set of standard filters that is in the file `/opt/pdos/etc/pdoslrd.xml.template`.

Note: The audit log consolidation application supports a limited wildcard capability on the *value* option of a Field element. You can use `value="*xyz"`, `value="xyz*"`, or `value="*xyz*"`, but not `value="abc*xyz"`. You can get the equivalent of `abc*xyz` by having two Field elements in the Conditional element: one with `value="abc*"` and the other with `value="*xyz"` You can

use the question mark character (?) to match any character, but you cannot use the question mark and asterisk (*) together. Thus, `value="a?b"` matches `"azb"`, `"a1b"`, `"aab"`, for example. You can have multiple question mark characters in a single value (for example, `value="a?c?e?"`). Wildcard characters are *not* supported on the name2 option of a Field element. They are only supported in the value option.

```
<--Include only login denies -->
<Filter name="login-deny">
 <Conditional type="include">
 <Field name="resource_type" value="Login"/>
 <Field name="view" value="D"/>
</Conditional>
</Filter>

<--Include only logins as root -->
 <Filter name="root-login>
  <Conditional type="include">
   <Field name="resource_type" value="Login"/>
   <Field name="acc_name" value="root"/>
</Conditional>
</Filter>

<--Include only non-root logins -->
 <Filter name="non-root-login">
  <Conditional type="exclude">
   <Field name="acc_name" value="root"/>
  </Conditional
  <Conditional type="include">
   <Field name="resource_type" value="Login"/>
  </Conditional>
</Filter>

<--Include only failures to become root. This includes failed Login or failed
Surrogate or failed Sudo. -->
 <Filter name="root-fail">
  <Conditional type="include">
   <Field name="resource_type" value="Login"/>
   <Field name="acc_name" value="root"/>
   <Field name="view" value="D"/>
  </Conditional
  <Conditional type="include">
   <Field name="resource_type" value="S*"/>
   <Field name="acc_name" value="root"/>
   <Field name="view" value="D"/>
  </Conditional>
</Filter>

<--Include only records where the accessor effective name is different from the
accessor name. This indicates a user has changed to another user at some point
in the past. This filter allows you to focus on all such activity. -->
 <Filter name="su">
  <Conditional type="exclude">
   <Field name="acc_name" name2="acc_eff_name"/>
  </Conditional>
 </Filter>

<--Include only records where an account has been locked; either following the
"three strikes and you're out" rule or using administrative action. -->
 <Filter name="account-locked">
  <Conditional type="include">
   <Field name="event_id" value="2"/>
  </Conditional>
  <Conditional type="include">
   <Field name="event_id" value="3"/>
  </Conditional>
</Filter>
```

```
<--Include only file access failures in the /etc directory. -->
 <Filter name="etc-file-failures">
  <Conditional type="include">
   <Field name="resource_type" value="File"/>
   <Field name="view" value="D"/>
   <Field name="sys_res_name" value="/etc/*" />
  </Conditional>
</Filter>

<--Include only records where a file has been marked untrusted. -->
<Filter name="file-untrust"
  <Conditional type="include">
   <Field name="event_id" value="22" />
  </Conditional>
</Filter>

<--Include only records where AMOS has entered isolation mode. -->
<Filter name="isolation"
  <Conditional type="include">
   <Field name="event_id" value="12" />
  </Conditional>
</Filter>

--Include only records where a remote access attempt has failed due to Network
Incoming Policy. -->
<Filter name="incoming"
  <Conditional type="include">
   <Field name="resource_type" value="NetIncoming" />
   <Field name="view" value="D" />
  </Conditional>
</Filter>
```

Conditional Element

A Conditional element specifies one set of conditions under which a Filter element may be evaluated. A Filter element contains one or more Conditional elements. The first Conditional element that evaluates as true determines whether a record is included in the output. If a Conditional element of type *include* evaluates as true, the record is included in the output. If a Conditional element of type *exclude* evaluates as true, the record is excluded from the output.

In order for a Conditional element to evaluate as true, all of its Field elements must match the record in question. That is, the field specified in the Field element must contain the same value in the record as appears in the Field element.

If none of the Conditional elements in a Filter element evaluate as true, then the disposition of the record is determined by the type of the last Conditional element contained within the Filter element. If the type is *include*, then the record is excluded. If the type is *exclude*, then the record is included.

Usage

Usage	
<Conditional>	Begin tag
</Conditional>	End tag
Options	
type	″include″ or ″exclude″

Examples

```
<!-- include only records with resource_type=Login AND view=D
  OR records with outcome=F -->

<Filter name="filter1>
 <Conditional type="include">
    <Field name="resource_type" value="Login" />
    <Field name= "view" value="D" />
  </Conditional>
  <Conditional type="include">
    <Field name="outcome" value="F" />
  </Conditional>
</Filter>
```

Field Element

The Field element is used to specify the fields to use when applying an output filter. The name of the field is one of the Log Router field names listed in the Field Table later in this document. The value of a Field element is case-sensitive. This element can only be used between Conditional tags.

Usage

Usage	
<Field.../>	Field element
Options	
name	The name of the field. This is required.
value	The value of field *name* which constitutes a match.
name2	The name of a second field. If the contents of field *name* equals the contents of field *name2*, it is a match.

Example

```
<!-- Field element used inside a Conditional element. -->
<!-- The value of a Field element is case-sensitive.-->

<!-- The record will be included if the value of field "view" is "D".-->

<Conditional type="include">
  <Field name="view" value="D"/>
</Conditional>

<!-- The record will be excluded if the value of the field "acc_name" is equal to
  the value of the field "acc_eff_name". -->

<Conditional type="exclude">
  <Field name="acc_name" name2="acc_eff_name" />
</Conditional>
```

Chapter 4. Commands

Three new commands are provided with the log router consolidation feature: **pdoscollview**, **pdoslrd**, and **pdoslradm** The script, **rc.pdoslrd**, which enables you to start and stop the log router, is also included in this section.

Note: The **pdoscfg** command has been modified to support **pdoslrd** for this release. This modified version is called **pdoscfg.preview**. In the next release of Tivoli Access Manager for Operating Systems, these changes will be incorporated into **pdoscfg** and **pdoscfg.preview** will no longer exist.

pdoscollview

Processes records in a collection file created by ivacld on the Tivoli Access Manager authorization server (pdacld).

Syntax

pdoscollview [**-h**] **-?**] **- V**]

pdoscollview [**-l**]

pdoscollview [**-g** *resource_type*]

pdoscollview [**-z** *azn-decision-type*]

pdoscollview [**-w** *audit–type*]

pdoscollview [**-a** *action*]

pdoscollview [**-r** *reason*]

pdoscollview [**-o** *outcome*]

pdoscollview [**-n** *accessor_name*]

pdoscollview [**-c** *accessor_effective_name*]

pdoscollview [**-s***YYYY-MM-DD{-hh:mm:ss*} | *today*{*-n*} | *now*{-n}]

pdoscollview [**-e***YYYY-MM-DD{-hh:mm:ss*} | *today*{*-n*} | *now*{-n}]

pdoscollview [**-f** *output_filename*]

pdoscollview [**-i** *input_collection_file_pathname*]

pdoscollview [**-F** *concise* | *keyvalue* | *verbose*]

pdoscollview [**-M** *keyword* | *event* | *view* | *permission* | *qualifier* | *outcome* | *all*]

pdoscollview [**-R** *YYYY-MM-DD-hh:mm:ss n*]

pdoscollview [**-F** *concise* | *keyvalue* | *verbose*]

pdoscollview [**-H** *hostname*]

pdoscollview [**-b** *base-collection-file-pathname*]

pdoscollview [**-d** *delimiter*]

pdoscollview [**-N**]

Options

-V Displays the version information.

-h Displays the usage message.

-? Displays the usage message.

-l Indicates that the command output should be sent to the screen (stdout).

-g *resource_type*
Specifies the resource type (azn, daemon, tcb, cred, policy, login, logout, trace_exec, trace_file). In addition to the preceding values, the values for the -z option can be specified here as well.

-z *azn_decision_type*
Specifies the azn_decision type: (file, netincoming, netoutgoing, login, logout, surrogate, sudo).

-w *audit_view*
Specifies the audit view (permit, deny, admin, info, trace, warning).

-a *action*
Specifies the action (check_access, add, delete, change, retrieve, apply, trust, stop, register, trace, isolated, not_isolated, unknown, login, logout, enable, disable).

-r *reason*
Specifies the reason (global_audit, resource_audit, global_warning, resource_warning).

-o *outcome*
Specifies the outcome (success, failure, trace_event, trace_permit, trace_deny).

-n *accessor_name*
Specifies the accessor name.

-c *accessor_effective_name*
Specifies the accessor effective name.

-s [*YYYY-MM-DD{hh:mm:ss}* *today***[**-*n***]** | *now***[**-*n***]]**
Sets the start time. Can be specified as a timestamp in the form of YYYY-MM-DD{-hh:mm:ss} or by using the special qualifiers of *today* and *now* to represent the current day and the current minute, respectively. Optionally, when special qualifiers are used, an integer value, *n*, can be specified to indicate the previous n days or the previous n minutes. Only records logged at or after the specified start time are formatted.

-e [*YYYY-MM-DD{hh:mm:ss}***]** *today***[**-*n***]** | *now***[**-*n***]]**
Sets the end time. Can be specified as a timestamp in the form of YYYY-MM-DD{-hh:mm:ss} or by using the special qualifiers of *today* and *now* to represent the current day and the current minute, respectively. Optionally, when special qualifiers are used, an integer value, *n*, can be specified to indicate the previous n days or the previous n minutes. Only records logged before or at the specified end time are formatted.

-f *output_filename*
Specifies the pathname of the file that is to receive the ASCII output of the command.

-i *input_collection_file_pathname*
Specifies the pathname of the input collection file that is to be processed.

-F *concise* | *keyvalue* | *verbose*
Specifies the formatting style of audit records. The default is keyvalue format unless the -l option is used. If the -l option is specified with the -F option, records are displayed in verbose format.

-M *keyword* | *event* | *view* | *permission* | *qualifier* | *outcome* | *all*
Displays the mapping of audit record fields.

-R *YYYY-MM-DD-hh:mm:ss n*
Selects a specific audit record given its timestamp (YYYY-MM-DD-hh:mm:ss) and its audit uniqifier (n).

-H *hostname*
Hostname. Specifies that only records for audit events generated on the specified host be displayed.

-b *base_collection_file_pathname*
Base pathname. Indicates the pathname of the base collection file. Specifying this option causes the command to process all the collection files in the directory that are archived versions of the base file name. For example, if the base pathname is /x/y/audit_collect, and the directory /x/y contains the collection files, audit_collect.2002-10-13-09:34:55, audit_collect.2002-10-14-10:55:03, and audit.collect, then the collection files will be processed in the order listed here. They are processed in the order of increasing time suffix, except that the base name (the file without a time suffix) is processed last, because it is the most recent.

-d *delimiter*
Delimiter. Indicates the field delimiter for concise and keyvalue formats. It consists of one or more characters and replaces the default delimiter, which is a comma. Note that some values might have to be enclosed in quotation marks in order for the shell to accept them. For example, if you want the fields to be separated by a vertical bar (|), use -d "|".

-N Indicates that the hostname should be included in the output. This option is valid for concise, keyvalue, and verbose output formats. When specified, this option causes the hostname of the machine that originally generated the audit record to be included in the output of each audit record. This is useful when the -H option is not specified because a collection file will usually contain audit records from many different hosts.

Description

The **pdoscollview** command is used to process a collection file generated by the ivacld daemon. The resulting output can be viewed, printed, or analyzed by scripts and other programs.

pdoslrd

Log router daemon.

Syntax

pdoslrd [**-h**] [**-?**] [**-V**]

pdoslrd [**-f**]

pdoslrd [**-r**]

pdoslrd [**-k**]

Options

-V Displays the version information.

-h Displays the usage message.

-? Displays the usage message.

-f Runs the daemon in the foreground.

-r Refreshes. Makes **pdoslrd** reread the control file and make adjustments accordingly (for example, turn channels on or off; start new channels).

-k Shuts down the daemon.

Description

The log router daemon routes audit records to multiple destinations as specified in its control file.

pdoslradm

Controls the log router daemon and channels in the log router control file.

Syntax

pdoslradm [*-h*] [**-?**] [**-V**]

pdoslradm [**-c** *channel_name* [*-S option=value*] [*-D options*] [-d]]

pdoslradm [**-d**]

pdoslradm [**-R**]

pdoslradm [**-k**]

Options

-V Displays the version information.

-h Displays the usage message.

-? Displays the usage message.

-c *channel_name*
Adds, modifies, or deletes the channel option.

- -S *option=value*. Sets the value of the option. If the option does not exist, it will be added.
- -D *option*. Deletes the option.
- -d *option*. Displays the channel options.

-d Displays the channels in the `pdoslrd.xml` file and their current options.

-R Makes **pdoslrd** reread the control file and make all adjustments accordingly (for example, turn channels on or off; start new channels).

-k Shuts down the **pdoslrd** daemon.

rc.pdoslrd

Startup script for the log router daemon, **pdoslrd.**

Syntax

rc.pdoslrd [**start**]

rc.pdoslrd [**stop**]

rc.pdoslrd [**refresh**]

Description

The **rc.pdoslrd** script is used to start up and shut down **pdoslrd**.

Options

start Start up **pdoslrd**.

When the **pdoslrd** daemon starts, it looks for a last- record-processed file in the directory `/var/pdos/pdoslrd` (see below). If it finds one, it starts reading audit records after that last record processed. If it does not find a last- record-processed file, it starts reading audit records with the first record in the oldest audit.log archive file. If there are no archive files, it starts with the first record in audit.log.

stop Shut down **pdoslrd**.

As part of its shutdown processing, the **pdoslrd** daemon writes a file to the directory `/var/pdos/pdoslrd` containing the timestamp and uniqifier of the last audit record processed. The name of this file is *input_channel_name*`.lrp`, where *input_channel_name* is the name of the input channel in the **pdoslrd** control file (`pdoslrd.xml`), for example, `input-admin.lrp`.

Note: The uniqifier is a Tivoli Access Manager for Operating Systems audit record field. It is used to distinguish between audit records that have an identical time stamp. An audit record will have a non-zero uniqifier only if it was generated during the same second as the previous audit record. In addition, a non-zero uniqifier will always be one greater than the uniqifier of the previous audit record. If you view an audit output file and see that this is not the case, it that means some records have been filtered out.

refresh
Reread the control file and make adjustments accordingly.

Description

The **rc.pdoslrd** script is used to start up and shut down **pdoslrd**.

Chapter 5. Operation

This chapter contains the following information:

- descriptions of the input and output channel types and how to specify them
- record fields
- field values
- output formats

Channels

The following section describes the supported channel types for this release. There is one input channel type, LRD_AuditInput, and three output channel types: LRD_FileOutput, LRD_EmailOutput, and LRD_NetOutput.

Channel Types

LRD_AuditInput
Reads the Tivoli Access Manager for Operating Systems audit log (the default is `/var/pdos/audit/audit.log*`) and formats the audit records into a form that allows filtering to be performed by the output channels.

LRD_FileOutput
Performs filtering, formats records for output, and writes records to a text file on the local host.

LRD_EmailOutput
Performs filtering, formats records for output, and sends records to the specified e-mail address.

LRD_NetOutput
Performs filtering, formats records for output, and sends records to the **pdacld** process on a remote host.

Using the channel types

The Log Router channels are specified in the Log Router control file (`/opt/pdos/etc/pdoslrd.xml`)

LRD_AuditInput

There must be one and only one input channel specified in the Log Router control file. The only input channel type currently supported is LRD_AuditInput. This channel reads audit records from the Tivoli Access Manager for Operating Systems audit log. The audit log consists of all files of the form `audit.log*` in the directory `/var/pdos/audit`. The file `audit.log` is the latest file and all other files with names that start with `audit.log` are archived versions. When the `audit.log` file reaches a certain size, it is *rolled over* or *archived* into a file of the form `audit.log.YYYY-MM-DD-hh-mm-ss`.

When the **pdoslrd** daemon is started, the input channel code looks for a file of the form *input_channel_name*`.lrp` in the directory `/var/pdos/pdoslrd`, where *input_channel_name* is the name of the input channel in the Log Router control file. An example name could be `input.lrp`. If the file exists, it contains the timestamp and uniqifier of the last record processed during a previous invocation of **pdoslrd**. The input channel code will search the `audit.log*` files in `/var/pdos/audit` until it

finds an audit record with a timestamp and uniqifier that makes it later than the values in the file `input_channel_name.lrp`. It starts reading audit records at this record. This mechanism allows the **pdoslrd** daemon to be shut down and restarted without losing its place in the audit log. If the input channel fails to find the file `input_channel_name.lrp`, it starts reading the audit log at the first record of the oldest file of the form `audit.log*`.

Note: The *uniqifier* is an Tivoli Access Manager for Operating Systems audit record field. It is used to distinguish between audit records that have an identical time stamp. An audit record will have a non-zero uniqifier only if it was generated during the same second as the previous audit record. In addition, a non-zero uniqifier will always be one greater than the uniqifier of the previous audit record. If you view an audit output file and see that this is not the case, it means that some records have been filtered out.

LRD_FileOutput

This channel type performs filtering and writes records to a local file. The main use of this channel type is to provide a real-time view of audit records. A system administrator who wants to view the audit records as they are produced in as close to real time as is possible can issue a **tail–f** command on the local file, and then view the audit records as they are generated (with a slight delay). This is likely a practice that that will only be done temporarily to gauge the current audit output. It could be done:

- to track a particular event or group of events
- prior to or just after making a change in the audit level
- to test the effect of various filters in the `pdoslrd.xml` file.

LRD_EmailOutput

This channel type performs filtering and writes records to an e-mail address. The main use of this type of channel is to allow system administrators to monitor very specific audit events that occur infrequently. It is expected that this type of channel be highly filtered, meaning that only a few audit events actually get sent through e-mail. If the channel is not highly filtered, the e-mail address might be overwhelmed with a huge number of events, which could also slow the other output channels down. The kind of filter used on this channel type is, therefore, very important. An example of a filter that might be used here is one that filters out all events except login denies, that is, audit events that were generated when a user attempted to log in to a system and was denied access.

LRD_NetOutput

This channel type performs filtering and sends records to a remote host, which is running the Tivoli Access Manager authorization server, **pdacld**. The main use of this type of channel is to provide the endpoint component of the communication. The audit log consolidation functionality refers to one or more endpoint machines sending audit events to the **pdacld** server for archival purposes. Providing this functionality is the main reason the log router was developed. The log router consists of one daemon, the log router daemon (**pdoslrd**). The functionality is performed on endpoints by having an input channel of LRD_AuditInput and an output channel of LRD_NetOutput, which sends formatted audit records to the **pdacld** server using the Tivoli Access Manager remote logging APIs. On the **pdacld** server, the collection function is performed by the Tivoli Access Manager remote logging services available through **pdacld**. This collection requires an entry under the aznapi-configuration stanza in the file `/opt/PolicyDirector/etc/ivacld.conf` similar to the following:

```
[aznapi-configuration]
logcfg = remote.channel_name:file path=/var/PolicyDirector/pdacld/amos_collection
```

where *channel_name* is the name of the LRD_NetOutput channel on the endpoint machines (for example, netout-admin).

In general, the **pdacld** server will receive audit records from several endpoint machines and store them in a single collection file. There is, however, a facility for the server to store records from each endpoint into a separate collection file. To enable this facility, you must ensure that each endpoint hostname appears in the `ivacld.conf` file as in the following example:

```
[aznapi-configuration]
logcfg = remote.channel_name.hostname1:file \
 path=/var/PolicyDirector/pdacld/hostname1/amos_collection
logcfg = remote.channel_name.hostname2:file \
 path=/var/PolicyDirector/pdacld/hostname2/amos_collection
```

In this example, records from endpoint hostname1 will be stored in one file and records from endpoint hostname2 will be stored in another.

System Externals

Log Router Audit Record Fields

The log router audit record fields include those fields that can be:

- Displayed when output is directed to a local file
- Written to a collection file
- Used in filter definitions

Supported Fields

The log router is compatible with the current Tivoli Access Manager for Operating Systems auditing code. The current Tivoli Access Manager for Operating Systems `audit.log` format is preserved. The keyvalue and concise formats of the log router are the same as the **pdosaudview** keyvalue and concise formats. The E-mail output format of the log router is the same as the **pdosaudview** verbose format.

The set of audit record fields supported by the log router includes the following:

- All the fields in the concise format of the **pdosaudview** tool. These are the same as in the keyvalue format. This means all the fields in the three audit record types: general, trace, and logout are included. These record types are described in Chapter 6, "Auditing", in the *IBM Tivoli Access Manager for Operating Systems Administration Guide, Version 4.1*.
- The host_name field. This is the name of the host that generated the audit record.

Supported Field Values

Several audit record fields have a verbose value and a concise value or keyvalue when displayed by the **pdosaudview** command. For example, the verbose values for the audit_outcome field are *Success* and *Failure*, whereas the concise value or keyvalue are *S* and *F*.

All of the values needed for the concise and keyvalue formats are supported. All of the verbose values are supported except for the event_id and qualifier fields. The numeric values for these two fields are described in Chapter 6, "Auditing", in the *IBM Tivoli Access Manager for Operating Systems Administration Guide, Version 4.1*.

Supported Formats

The supported formats are as follows:

- Concise format (of the **pdosaudview** tool).
- Keyvalue format (of the **pdosaudview** tool).
- Network output format. This consists of the fields and values of the concise format plus the host_name field.
- E-mail output format. This is the same as the **pdosaudview** verbose format.

Field Table

The following table shows all of the fields and values supported by the Log Router.

- The first column shows the field name defined in Chapter 6, "Auditing", in the *IBM Tivoli Access Manager for Operating Systems Administration Guide, Version 4.1*.
- The second column shows the name used by the log router. The log router field names are used in filter specifications.
- The third column shows the name of the field in the keyvalue format.
- The fourth column shows the formats that use the field.
  - C means the field is used by concise (and keyvalue).
  - E means the field is used by the e-mail format (Channel type = LRD_EmailOutput).
  - N means the field is used by the network output format (Channel type = LRD_NetOutput).

Audit Record Field Heading	Log Router Field Name	Keyvalue Field Name	Used By
---	host_name	---	E N
Timestamp	time_stamp	TS	C E
Audit Event Identifier	event_id	E	C E N
Audit View	view	V	C N
Audit View	view_verb	---	E
Audit Reason	reason	R	C N
Audit Reason	reason_verb	---	E
Audit Resource Type	resource_type	RT	C E N
Accessor Name	acc_name	AN	C E N
Accessor Effective Name	acc_eff_name	AEN	C E N
Audit Action	action	A	C E N
Audit Permissions	permissions	P	C N
Audit Permissions	permissions_verb	---	E
Audit Qualifier	qualifier	Q	C E N
Policy Branch Name	branch_name	PBN	C E N
Protected Object Name	prot_obj_name	PON	C E N
System Resource Name	sys_res_name	SRN	C E N
Surrogate Name	sname	SN	C E N
Network Remote Host Identifier	net_rem_host_id	NRH	C E N
Network Protocol	net_protocol	NP	C E N

Audit Record Field Heading	Log Router Field Name	Keyvalue Field Name	Used By
Network Service	net_service	NS	C E N
Login Location Identifier	login_location_id	LL	C E N
Accessor Processor ID	accessor_pid	APID	C E N
*Running Program Protected Name	run_prog_prot_name	RPPN	C E N
*Running Program System Resource Name	run_prog_sys_name	RPSN	C E N
Sudo Command and Arguments	sudo_cmdargs	SC	C E N
Sudo User Name	sudo_user	SU	C E N
Sudo Flags	sudo_flags	SF	C E N
Additional Parameters	param	AP	C E N
TCB Changed Data Attr Flags	chg_attr_flags	CDAF	C E N
Policy Epoch	policy_epoch	PE	C E N
Policy Version Number	policy_version	PVN	C E N
Audit Outcome	outcome	O	C N
Audit Outcome	outcome_verb	---	E
Audit Fail Status	fail_status	FS	C E N
Audit Uniqifier	uniqifier	UQ	C E N
*Protected Resource Specification	prot_res_spec	PRS	C E N
*Accessed Resource Specification	acc_res_spec	ARS	C E N
*The audit record fields ″Running Program Protected Name″ and ″Running Program System Resource Name″ are available when you are viewing general audit records; the fields ″Protected Resource Specification″ and ″Accessed Resource Specification″ are available when you are viewing trace audit records.			

Encoded Field Values

Field	Possible values
event_id	This is a decimal number. The meaning of each number is listed in Table 43 in Chapter 6, Auditing, in the *IBM Tivoli Access Manager for Operating Systems Administration Guide, Version 4.1*.
view	This is a single character, which will be one of the following: P— permit D—deny A—admin I—info T—trace W—warning

Field	Possible values
reason	This is a decimal number from 1 to 4: 1—global audit 2—resource audit 3—global warning 4—resource warning
outcome	This is one or two characters: S—success F—failure TE—trace event TP—trace permit TD—trace deny
resource_type	This is one of the following strings: Azn Process TCB Cred Policy File Login Logout TraceExec TraceFile Password NetIncoming NetOutgoing Surrogate Sudo
action	This is one of the following strings: Check Access Add Delete Change Retrieve Apply Trust Untrust Start Stop Register Trace Isolated Not Isolated Login Logout Enable Disable
qualifier	This is a decimal number. The meaning of each number is listed in Table 44, "Description of Audit Event Identifiers", in Section 6, "Auditing" of the *IBM Tivoli Access Manager for Operating Systems Administration Guide, Version 4.1*.

Field	Possible values
Permissions	This is a string of characters (for example, rwx). r—read w—write x—execute o—change ownership D—change directory p—change permission R—rename N—create d—delete U—utime K—kill L—login C—connect G—surrogate ?—listen l—readdir T—traverse

Log Router Output Formats

There are three log router output formats:

- Local file output: LRD__FileOutput
- E-mail Output: LRD__EmailOutput
- Network output: LRD__Output

Local File Output—LRD_FileOutput

When records are routed to a local file (Channel type= LRD_FileOutput), the user can specify the output format to be concise or keyvalue. These are the same as the concise and keyvalue formats supported by the **pdosaudview** tool.

E-mail Output—LRD_EmailOutput

When records are routed to e-mail (Channel type=LRD_EmailOutput), the format is the same as the verbose output of the **pdosaudview** command. One e-mail message is sent for each audit record. It is expected that e-mail output will be highly filtered to reduce the number of audit records sent. For example, an administrator might select on *only denies* to be sent to e-mail. The following is an example of the e-mail format:

```
Subject: audit record notification

The following audit record was sent by the log router daemon on host swing:

Timestamp                           Mon 29 Oct 2001 04:35:45 PM CST
Audit Event                         An authorization decision was made.
Audit View                          Permit
Audit Reason                        Global Audit
Audit Resource Type                 File
Accessor Name                       root
Accessor Effective Name             root
Audit Action                        Check access
Audit Permissions                    read
Audit Qualifier                     All resource policy checks permitted access.
Policy Branch Name                  bvt
Protected Object Name               File/opt/pdos
Systems Resource Name               /usr/lib/liblpm.so
```

```
Accessor Process ID                   1233
Running Program System Resource Name  /usr/sbin/in.telnetd
Audit Outcome                         Success
Audit Uniqifier                       1
```

Network Output—LRD_NetOutput

When records are written to a remote host , the output channel used is LRD_NetOutput. The Tivoli Access Manager remote logging services code on the collector machine will write the records it receives on the network to a collection file without modifying them in any way. Thus, the network output record format is identical to the collection file format. The fields of the collection file format include the host_name field and all the fields in the **pdosaudview** concise format with one exception: the timestamp field in the collection file format is in a language neutral format, while the timestamp field of the **pdosaudview** concise (and keyvalue and verbose) format is dependent on the local code page. All of the fields of the network output record are converted to UTF-8 before being sent over the network.

The number of endpoint machines that a single **pdacld** server can service depends on many variables. The level of auditing being performed is very important. If only login denies are being sent, then the server should be able to service hundreds of endpoints. If each endpoint is generating a very large number of audit records, then the server might be able to handle only a few endpoints. Of course, a great deal also depends on the relative power of the machines involved. It is assumed that **pdacld** server machines will be high-end machines when there is considerable auditing is being done or a large number of endpoints are being serviced.

File Rollover

The Channel element has a rollover_size option. When an output file reaches this size, a rollover will be performed. This applies only to LRD_FileOutput channels. A value of zero means the file will grow indefinitely. File rollovers will be performed in the same manner as the audit.log is done. That is, the file will be renamed, and the new name will have the date and time as a suffix. For example, an output file named `auditout` would be renamed to something like `auditout.2002-02-28-16-02-33`.

The Channel element also has a max_files option. This indicates the maximum number of rollover files that will be generated. If this number is reached, the last file is not rolled over, but grows without bound. If the max_files option is zero, there is no limit on the number of rollover files.

Output Compression

The Channel element has a compress option. This determines whether the output is compressed or not. This applies only to LRD_NetOutput channels. If the compress option is selected, the records will be uncompressed on the **pdacld** server before being written to the collection file. Thus, the compress option reduces the amount of data sent over the network, but it does not affect the contents of the collection file.

Chapter 6. Known Issues and Limitations

The following issues and limitations are known to exist in this preview release of the audit log consolidation software. Workarounds are provided if they are available.

1. Multiple NetOutput channels can cause shutdown problems.

   If there exists more than one NetOutput channel whose state is *on*, the log router daemon fails to shut down properly. It results in segmentation fault and also does not create the `.lrp` file. This a known limitation and there is no workaround.

2. Memory leak in the NetOutput channel.

   The NetOutput channel leaks some memory each time a record is sent to the remote server. This leak is in the remote logging services, which is part of the Tivoli Access Manager runtime. The fix is available in: Patch (4.1–TAM-FP02) for IBM Tivoli Access Manager for e-Business Base.

3. The log router daemon might fail to start on Red Hat Linux.

   If the state of the NetOutput channel is *on*, the log router might not start on Red Hat Linux. This is because the system might not have the correct level of the libstdc++ library. The required libstdc++ patch is libstdc++-2.95.2mdk.i586.rpm. It can be downloaded from http://www.linux-mandrake.com.

Chapter 7. Security

Security for commands, daemons, and files on a Tivoli Access Manager for Operating Systems endpoint will be provided by Tivoli Access Manager for Operating Systems Policy. Security for these items on a **pdacld** server machine can also be provided by Tivoli Access Manager for Operating Systems Policy. When the **pdacld** server machine does not run Tivoli Access Manager for Operating Systems, the security for these items is up to the system administrator.

Appendix. Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents.You can send license inquiries, in writing, to:

IBM Director of Licensing

IBM Corporation

North Castle Drive

Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation

Licensing

2-31 Roppongi 3-chome, Minato-ku

Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation

2Z4A/101

11400 Burnet Road

Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

IBM
IBM logo
Tivoli
Tivoli logo

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, and service names may be trademarks or service marks of others.

Printed in U.S.A.