

# **ITDS Audit Log Parser**

Version 0.2b

File Parsed: 6.0audit.log

May 4, 2006 7:53:56 PM EDT

# Summary

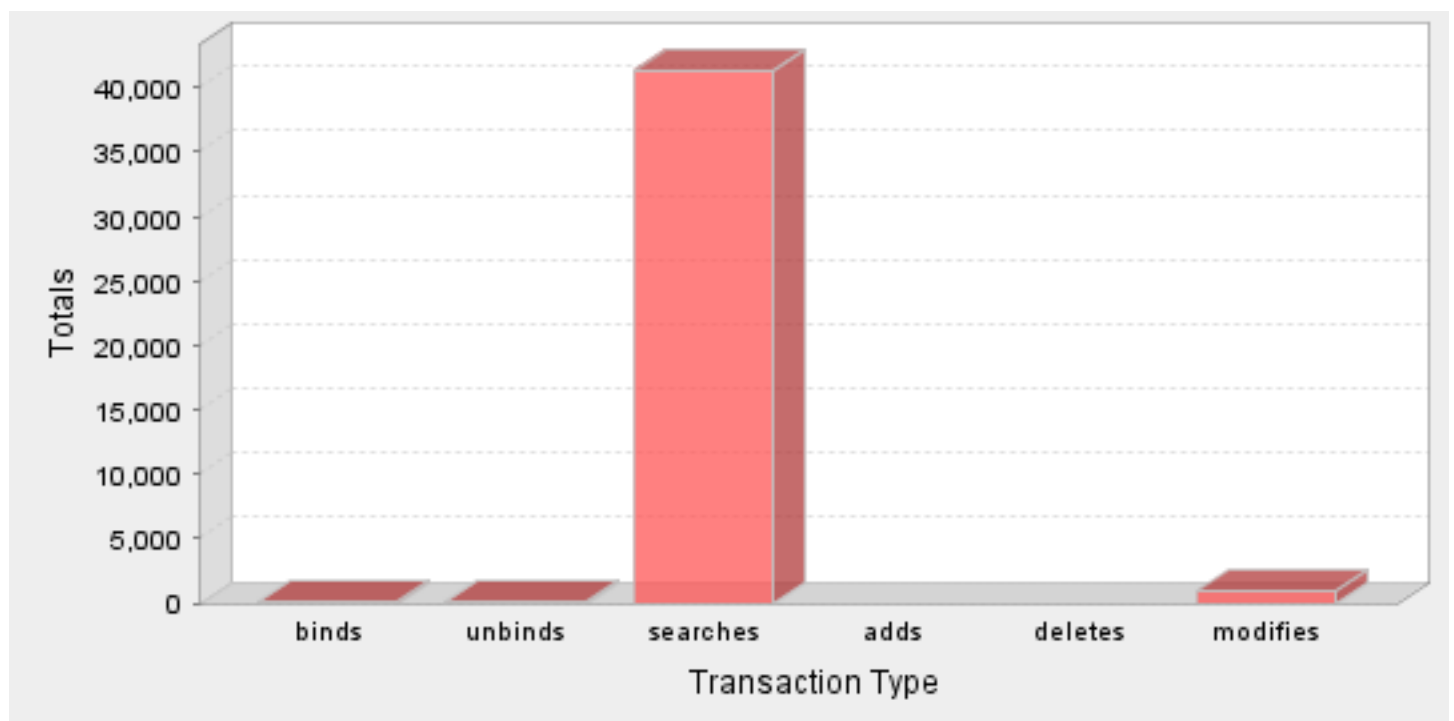
The summary information below provides an overview of the transaction types and performance of the directory operations contained within the audit log. This information can/should be used as a starting point and before/after picture of any tuning operations taken against the directory.

## Totals and Averages

This section describes the total transactions and their average transaction time. Note: The transaction time includes the time necessary to transmit any results to the client and for large transactions (e.g. searches that return thousands of results) it can make the numbers appear excessively large.

Transaction Types and Totals		
Operation	Count	Average (ms)
Binds	6	1
Unbinds	6	0
Searches	41406	183
Adds	0	0
Deletes	0	0
Modifies	914	35
Totals	42332	180

**Table 1: Totals by type**

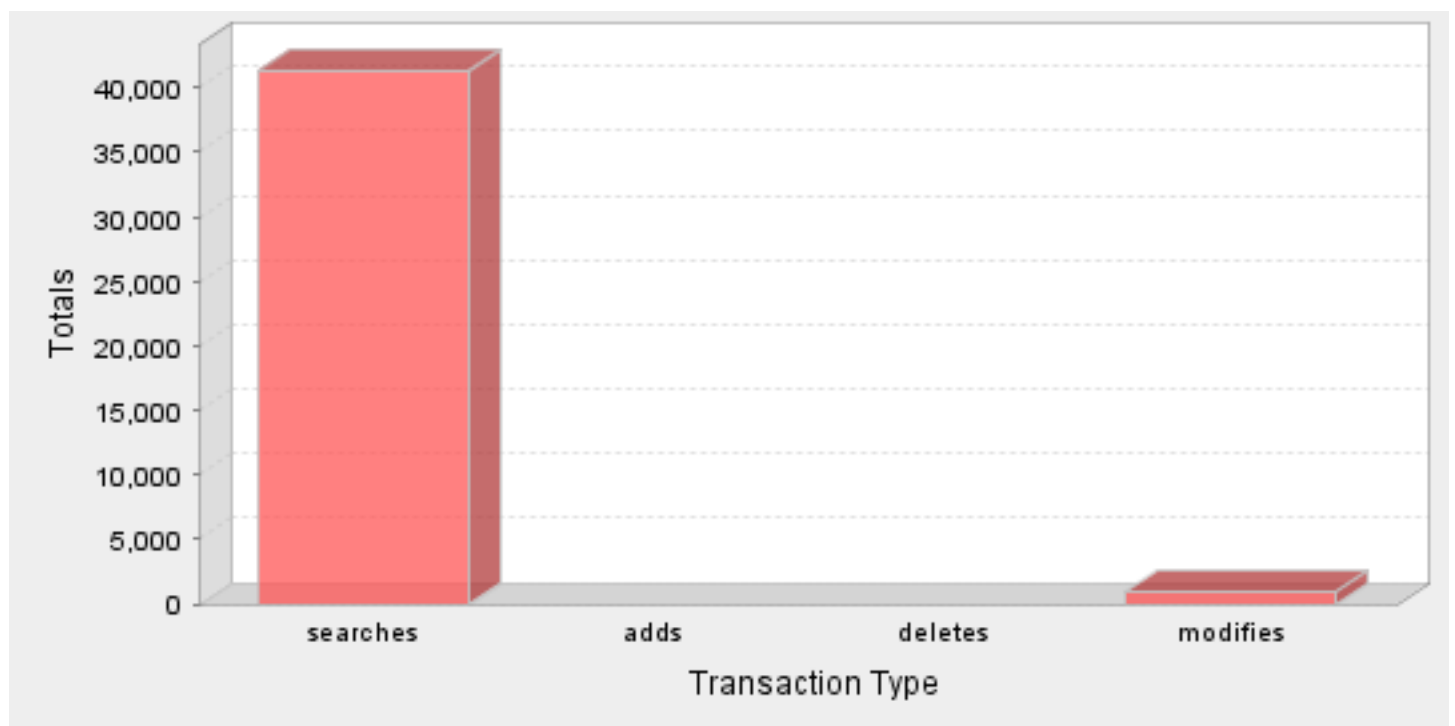


**Figure 1 Totals by type**

Binds and Unbinds are normally low overhead operations. If the directory is being used as an authentication source, including these operations can skew the results. The following table/chart excludes Binds and Unbinds.

Transaction Types and Totals (w/o Un/Binds)		
Operation	Count	Average (ms)
Searches	41406	183
Adds	0	0
Deletes	0	0
Modifies	914	35
Totals	42320	180

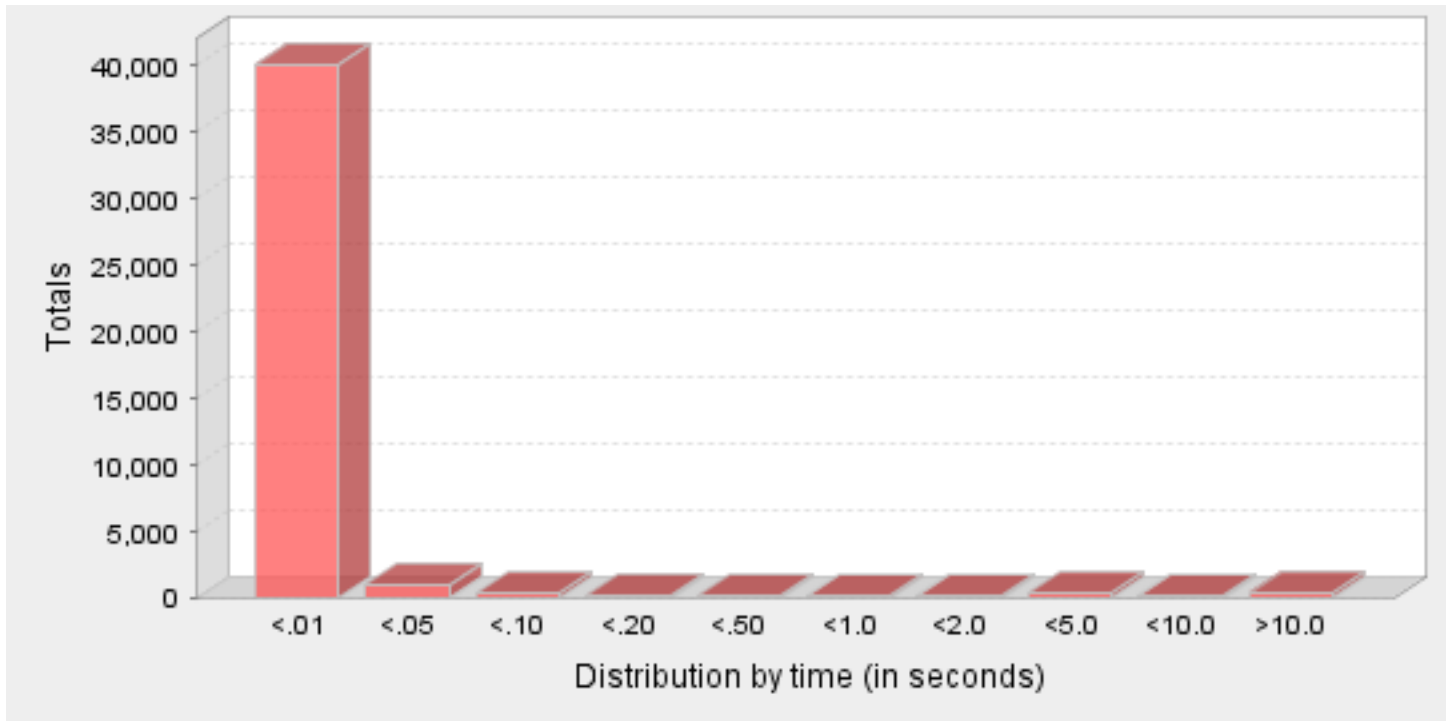
**Table 2: Totals by type (w/o Un/Binds)**



**Figure 2 Totals by type (w/o Un/Binds)**

## Transaction Distributions

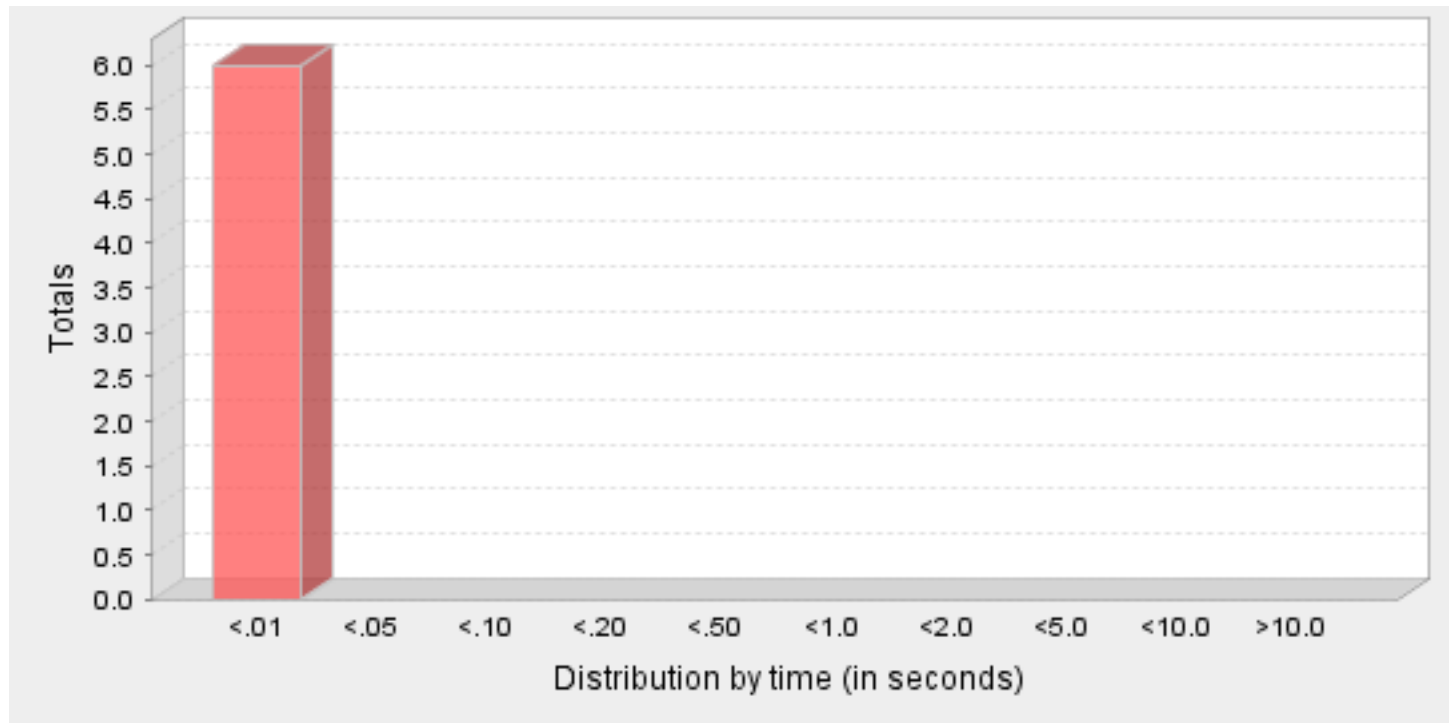
This section shows the distribution (count) of transactions based upon their total duration against time thresholds. Note: Abnormally long transactions can skew the performance perception of the directory and also point to needed tuning or possibly changes in the client application(s) queries (e.g. wildcard requests).



**Figure 3 Distribution by time**

### Bind Summaries

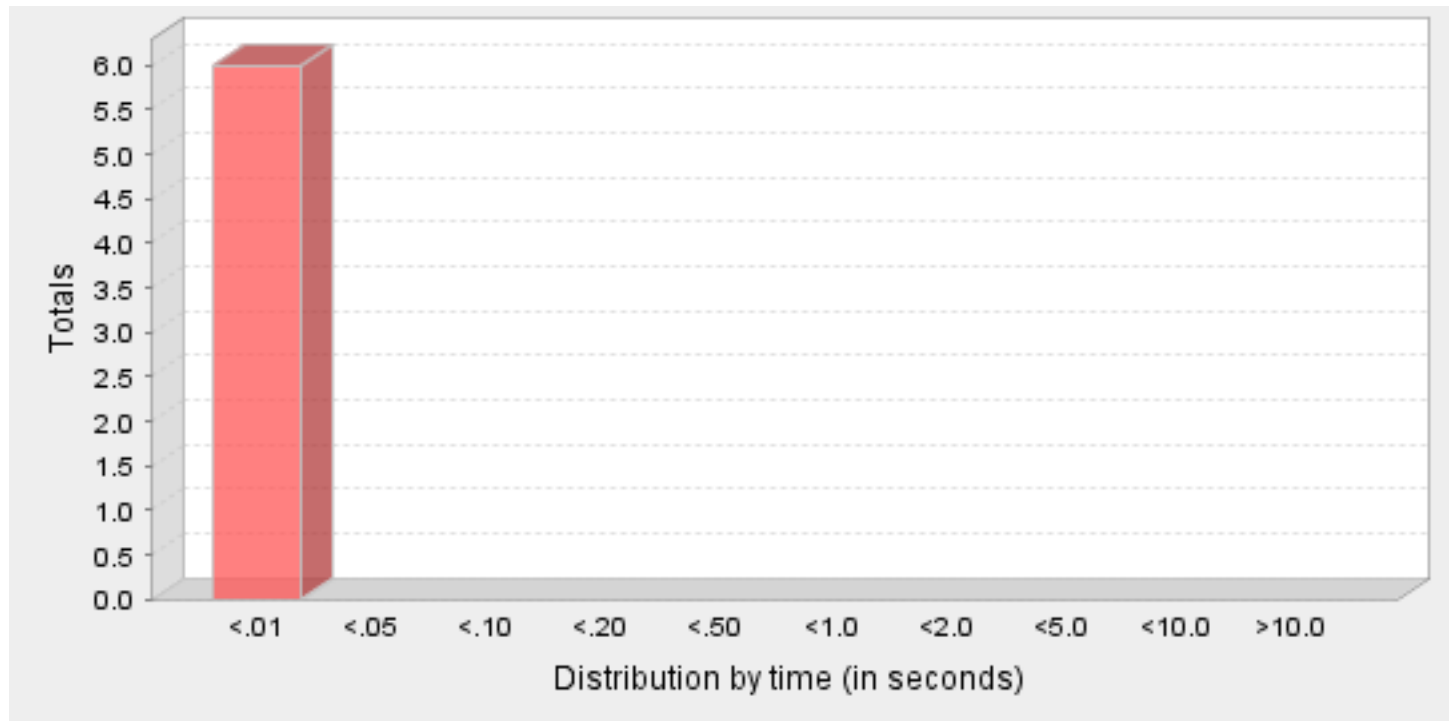
The following charts/tables show information on binds performed against the directory. Depending upon when the audit log was run (e.g. the client app was already connected) or what role the directory is providing (e.g. authentication engine) there may be no, minimal or large quantities of binds



Bind distribution by time

## Unbind Summaries

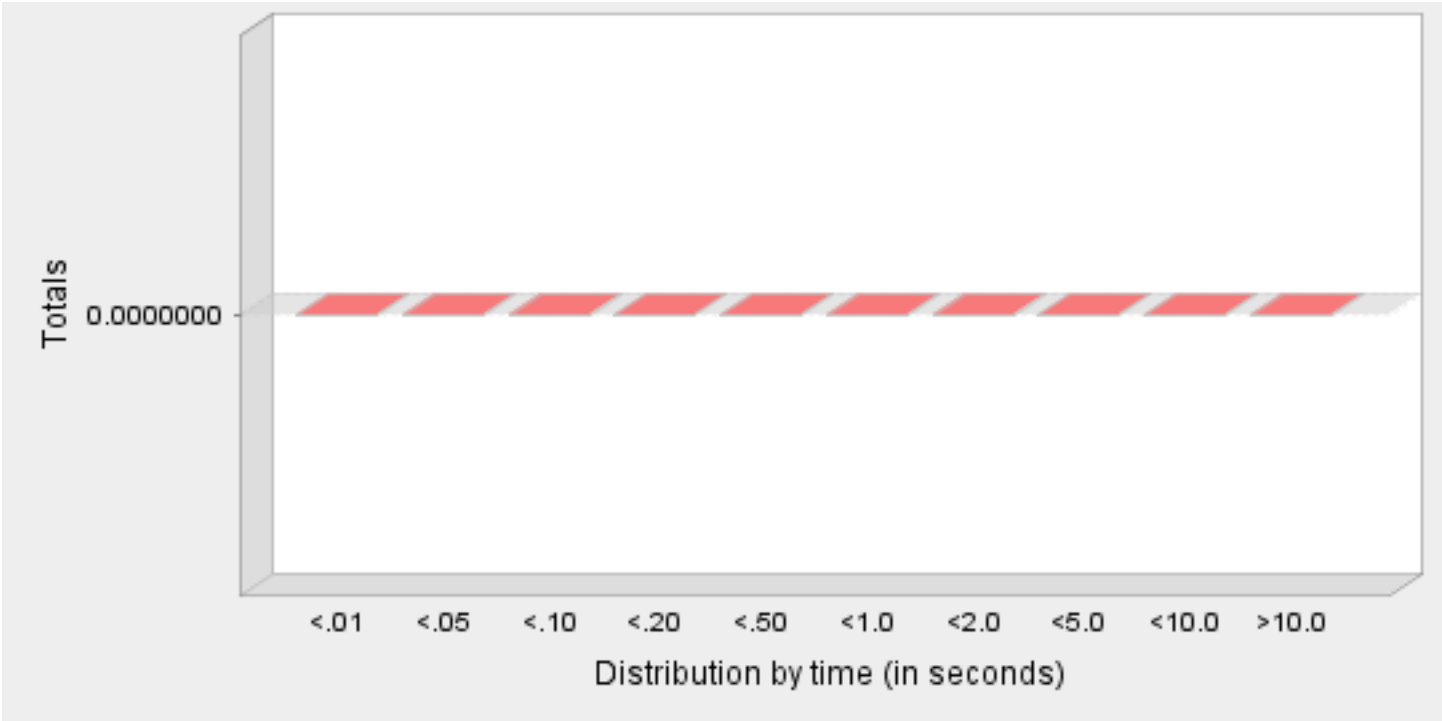
The following charts/tables show information on unbinds performed against the directory. Depending upon when the audit log was run (e.g. the client app was already connected) or what role the directory is providing (e.g. authentication engine) there may be no, minimal or large quantities of unbinds



Unbind distribution by time

**Add Summaries**

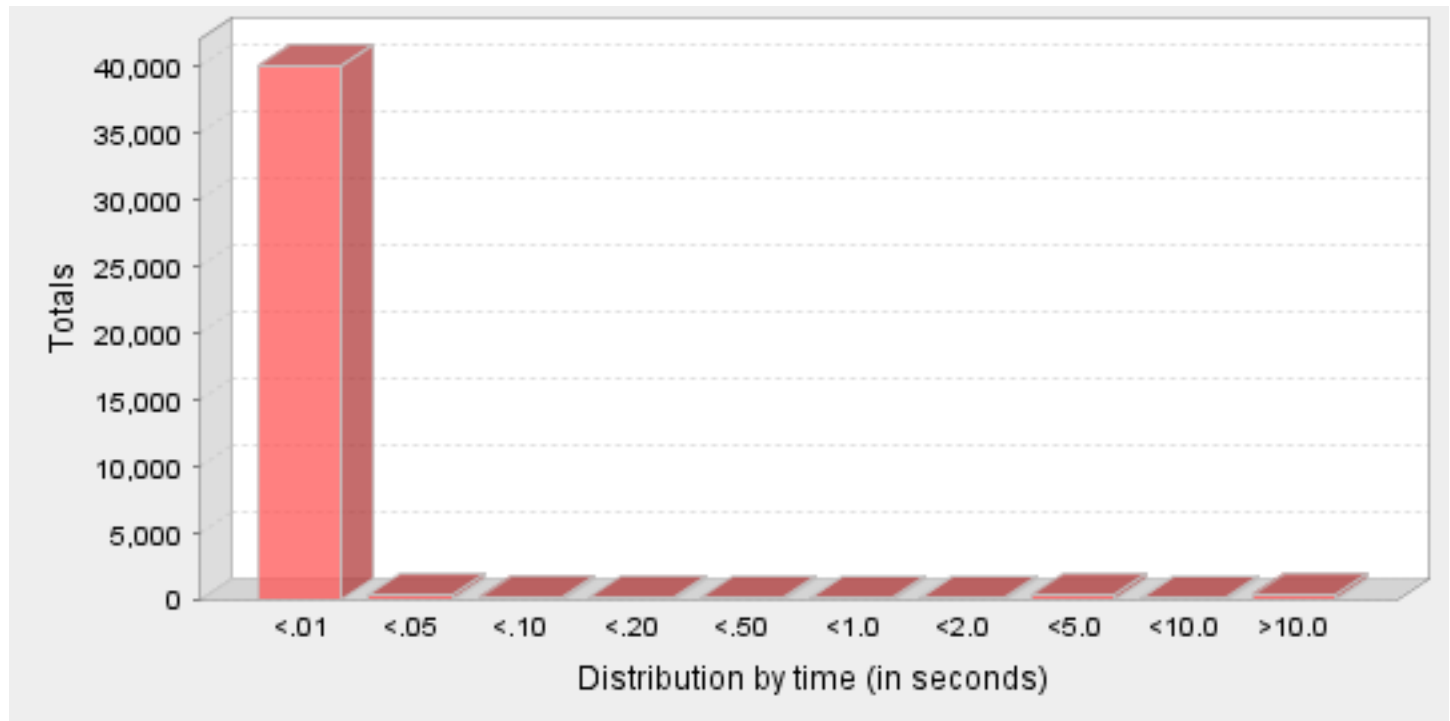
The following charts/tables show information on adds performed against the directory. Adds can have a significant impact on the performance of the directory since they can cause a cache reload



**Add distribution by time**

## Search Summaries

The following charts/tables show information on the searches performed against the directory. Immediately following the chart, we display the search query of the longest transaction and the attribute totals used in all searches. Note: Look for wildcard or complex queries in order to determine the optimizations required



### Search distribution by time

#### Longest Search Text

Longest Search (time in Milliseconds) = 18947

AuditV3--2006-03-09-15:14:46.990-05:00--V3 Search--bindDN: cn=Directory Manager--client:

166.86.124.79:62309--connectionID: 98--received: 2006-03-09-15:14:28.043-05:00--Success

base: ou=orgChart,erglobalid=00000000000000000000,ou=abccompany,dc=itim

scope: singleLevel

derefAliases: derefAlways

typesOnly: false

filter:

(&(erparent=ERGLOCALID=6776123625579741330,OU=ORGCHART,ERGLOCALID=00000000000000000000,OU=abccompany,DC=ITIM)(|(objectclass=ERBPORGITEM)(objectclass=ERLOCATIONITEM)(objectclass=ERORGUNITITEM)(objectclass=ERSECURITYDOMAINITEM)))

attributes: erparent, objectclass,

#### Filter Attributes Used

Total # of Attributes used in search filters = 16

Attribute = erpolicytarget Attribute count = 9772

Attribute = erprerequisite Attribute count = 21

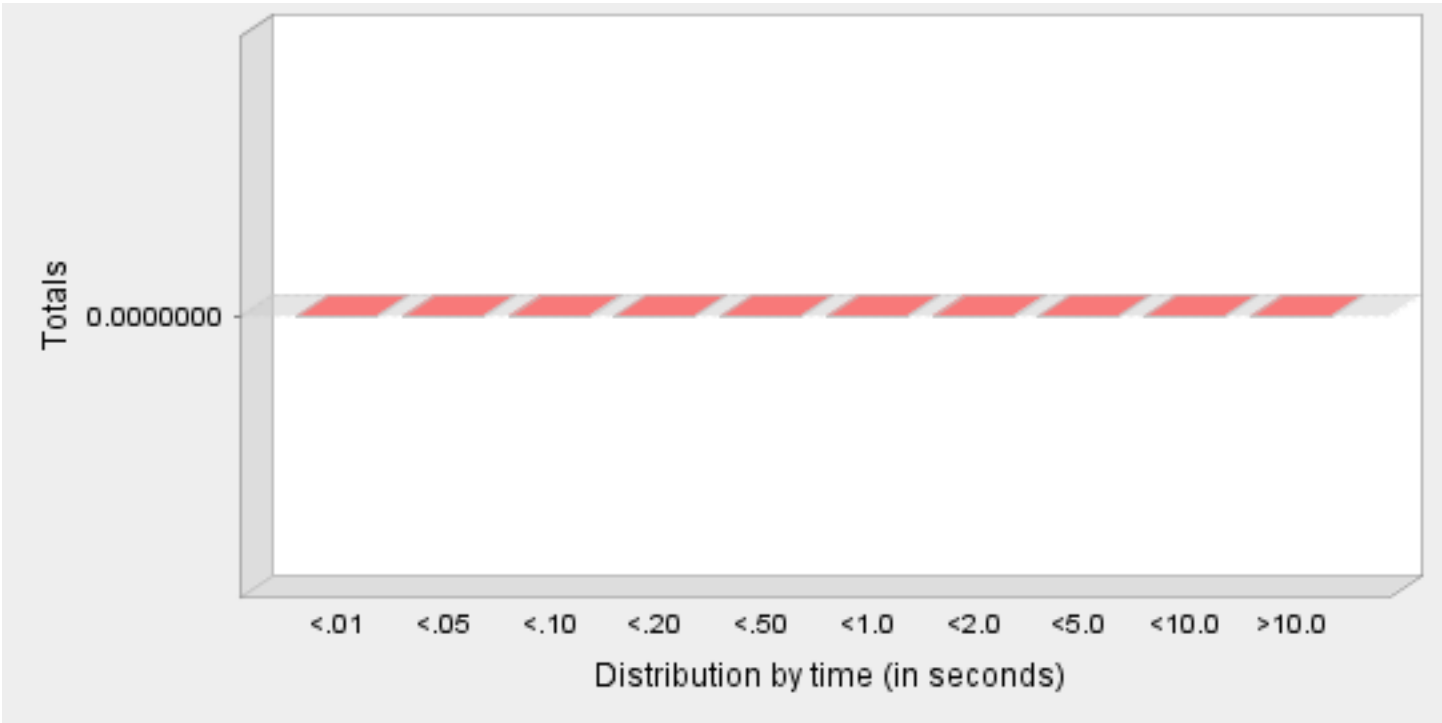
Attribute = erpolycymembership Attribute count = 11386



Attribute = ou Attribute count = 4  
Attribute = objectclass Attribute count = 47838  
Attribute = owner Attribute count = 1264  
Attribute = businesscategory Attribute count = 3660  
Attribute = uid Attribute count = 613  
Attribute = erobjectprofilename Attribute count = 3662  
Attribute = erreqpolicytarget Attribute count = 10077  
Attribute = erword Attribute count = 921  
Attribute = erenabled Attribute count = 10686  
Attribute = cemploymentstatus Attribute count = 610  
Attribute = erisdeleted Attribute count = 24  
Attribute = erparent Attribute count = 14958  
Attribute = erservicename Attribute count = 1831

**Delete Summaries**

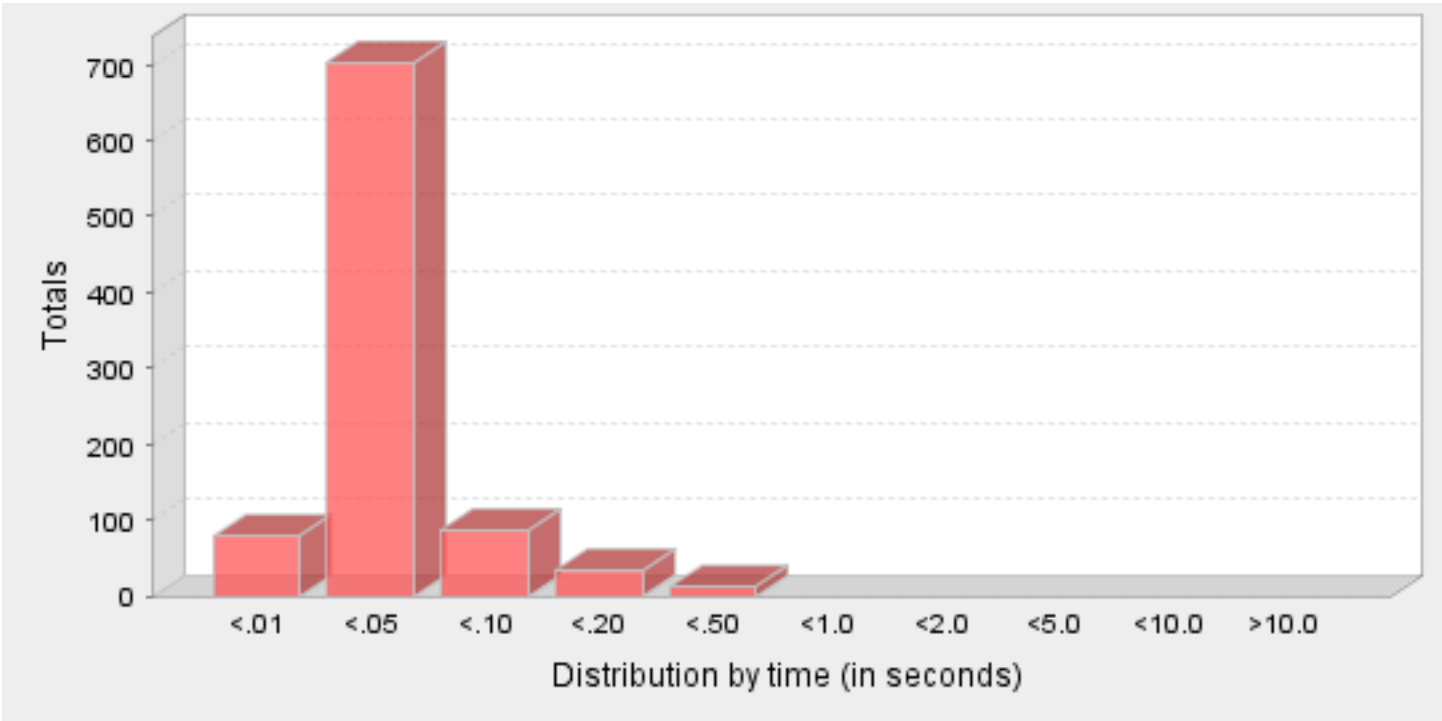
The following charts/tables show information on deletes performed against the directory.



**Delete distribution by time**

**Modify Summaries**

The following charts/tables show information on modifies performed against the directory.



**Modify distribution by time**