

Features – Alarms

Albert L. Rossi

Fermi National Accelerator
Laboratory

dCache Alarms

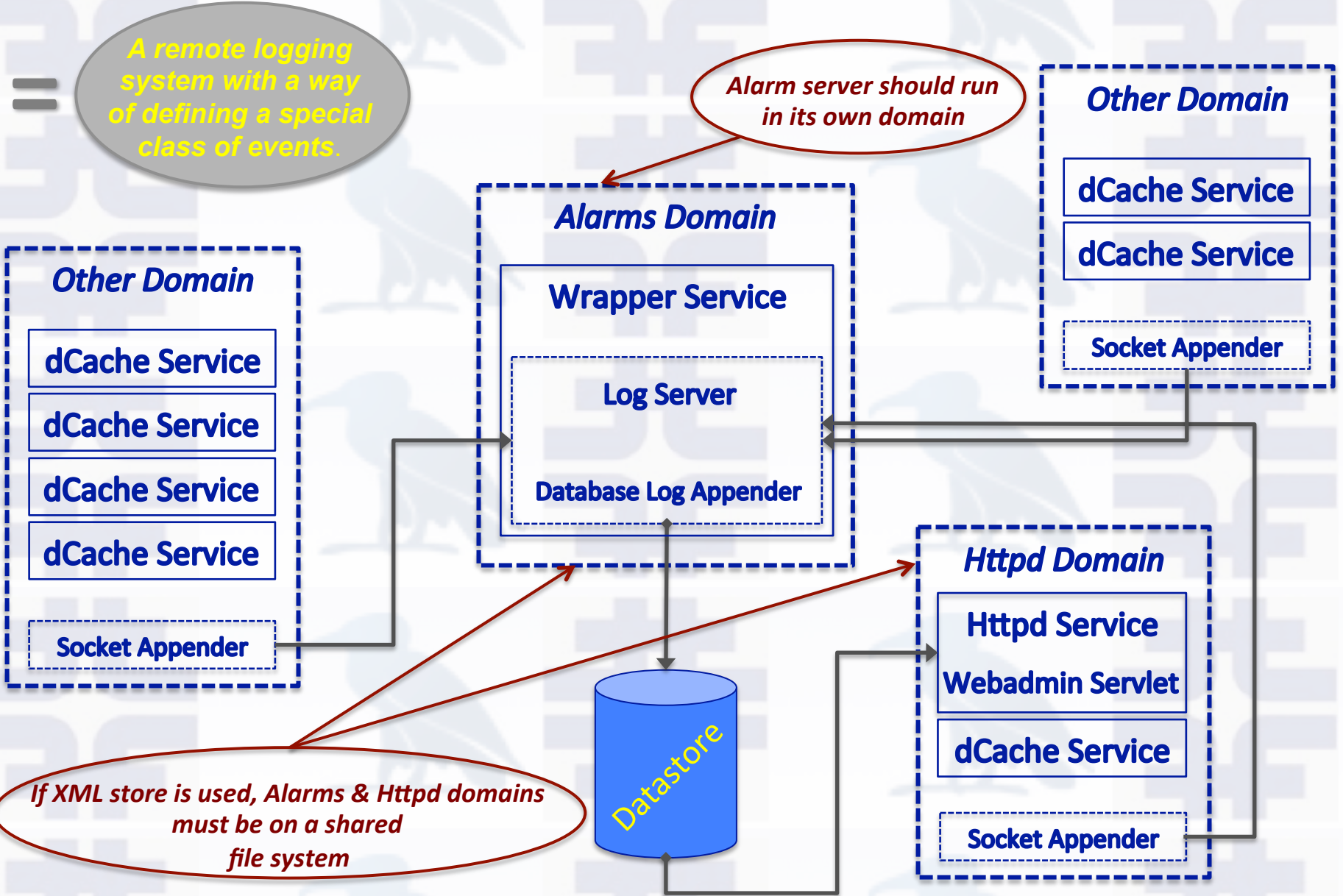
- New with version 2.6 (prototyped in 2.5)
- *What?* A simple and flexible extension to logging
- *Why?* Provide a single location:
 - to discover and resolve critical system-wide issues
 - to maintain a record of critical events and a brief description of their resolution, if so desired

Note: with this additional feature, dCache now provides three ways of accessing logged events:

1. in the domain logs (e.g., /var/log/dcache/dCacheDomain.log);
2. on the admin pinboard;
3. on the alarms web page (but there is a caveat which I will mention momentarily).

→ ***dCache Book, Chapter 16.***

Alarms – A Structural Overview



A remote logging system with a way of defining a special class of events.

Alarm server should run in its own domain

If XML store is used, Alarms & Httpd domains must be on a shared file system

The Two Kinds of Alarm Events

1. Marked directly by the dCache client services (hardcoded; there are as yet none implemented, but coming soon!).
 - These appear as type “ALARM[optional subtype]”.
2. Filtered from the usual logging events.
 - These are pattern-matched against a set of definitions, and will appear with the type name given by the match, e.g., “POOL_OFFLINE”.
 - dCache comes with a set of predefined types.
 - These can be extended by adding new definitions.

Predefined Alarms

- XML file corresponding to the property `alarms.definitions.path`
- default is `/var/lib/dcache/alarm-definitions.xml`
- used by both the alarm service and httpd service
- we provide for 4 possible “severity” levels:
 - CRITICAL, HIGH, MODERATE and LOW
 - for the hard-coded alarms, the ERROR logging level translates automatically to CRITICAL or HIGH, WARN to MODERATE, and anything below that to LOW.

CRITICAL

- SERVICE_CREATION_FAILURE
- DB_OUT_OF_CONNECTIONS
- DB_UNAVAILABLE
- JVM_OUT_OF_MEMORY
- OUT_OF_FILE_DESCRIPTOR

The affected dCache domain can't work (is down).

HIGH

- IO_ERROR
- HSM_READ_FAILURE
- HSM_WRITE_FAILURE
- LOCATION_MANAGER_UNAVAILABLE
- POOL_MANAGER_UNAVAILABLE

These functions are not working or not working properly, even though the dCache domain may be running.

MODERATE

- POOL_DISABLED
- CHECKSUM

There is an issue which should be taken care of in the interest of performance or usability, but which is not impeding the functioning of the system as a whole.

LOW

This issue might be worth investigating if it occurs, but is not urgent (no predefined types).

Configuring the Alarm Server

- Run the alarms service in a separate domain
 - not a question of efficiency but configuration (it uses a logback.xml different from the usual dCache domains and which would interfere with logging from any other service running in that domain).
- It is preferable to list the alarm domain first in the layout file
 - the alarms service will get booted first and has a better chance of catching startup errors reported by the other domains.
- The server can be configured for RDBMS (default) or for XML using `alarms.store.db.type=rdbms|xml`
 - XML is recommended only for small-scale installations which intend to send only ERROR-level log events to the server.
 - A file is generated at (`/var/lib/dcache/alarms/store.xml`); since both the httpd and alarms services must access the store, they need in this case to be running on the same host (or at least a shared file system); the default location can be modified by setting
 - `alarms.store.path`
 - It is advisable to run the automatic cleaner agent because XML query efficiency degrades significantly when the file becomes saturated. Use the following properties to configure it:
 - `webadmin.alarm.cleaner.enabled=true|false`
 - `webadmin.alarm.cleaner.timeout=168 (24 X 7 hours)`
 - `webadmin.alarm.cleaner.delete-threshold=336 (24 X 14 hours)`
 - RDBMS is PostgreSQL, and as usual can be set up for remote connections (hence the above constraint for XML does not apply)
 - Create the database before the first time you start the alarm service domain: `createdb -U srmdcache alarms`
 - The usual db properties (`alarms.store.db.host`, `alarms.store.db.user`, `alarms.store.db.password`) can also be used
 - While not strictly necessary, the cleaner may be useful if you plan to run the alarm system at a level lower than ERROR
- The logback xml used to configure the server is defined by the property:
 - `alarms.server.config` (by default at `/var/lib/dcache/alarms/logback-server.xml`)
 - it can be modified directly (for instance, to stop appending to history.xml), but usually will not need to be
 - the level at which events are handled by the server is set by `alarms.server.log.level`

Running the Alarm Server Outside of dCache

- The dCache wrapper cell/service for alarms only does the minimal location manager communication. Once the server is started no work outside this is done by the wrapper.
 - *Note:* server-specific and wrapper cell errors will appear in `/var/lib/dcache/alarms/server.log` and are not communicated to the main store
- It is possible, if deemed preferable, to run the server entirely outside of dCache. Chapter 16 of the *dCache Book* provides a *bash* snippet for doing this.
- Of course, with this one loses the nice feature of having the lifetime of the service managed by the dCache script.

Configuring the dCache Instances For Remote Logging

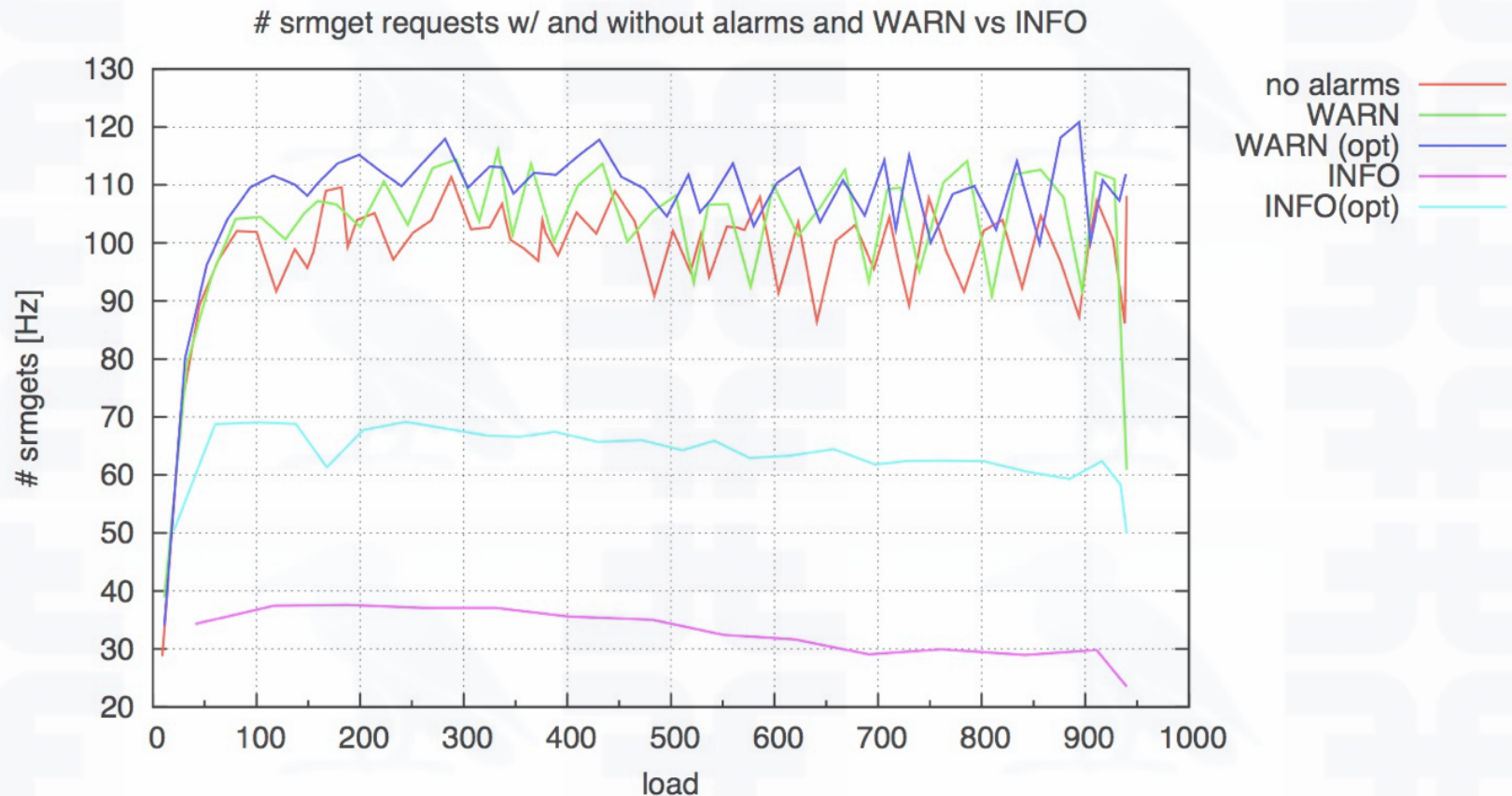
- Each instance needs to have its remote logging endpoint correspond to the location of the alarm server. This is controlled by the two properties `alarms.server.host` (default is localhost) and `alarms.server.port` (default is 60001).
- The log levels for the various loggers (see the turbo-filter definition in the logback.xml for the instance) can now be set using dCache properties. The property controlling remote logging is `dcache.log.level.remote`, which defaults to WARN. This means that *all logging events at WARN or higher will be sent over the wire to the server.*

Design Choice and Performance Impact

1. Alarms matched against definitions on server side (regex expansion costly, would slow client domains down).
2. This means all events at a given level (ERROR, WARN) are sent to the remote server.
3. Traffic increases significantly from ERROR to WARN, and dramatically from WARN to INFO.
4. This alarm system was not intended to scale to info/debug levels; not intended as a full-blown remote debugging service. In the interest of flexibility, we have allowed for alarms possibly defined at these levels, but we do not recommend this. Possible exceptions:
 - short-lived diagnostic runs
 - selected domains (hosts) set to lower logging levels
 - running a cleaner with a very short period (a few hours)obviously, this does not solve the network issue, only a database-related one; one would have to monitor the alarms closely in this case, as history would not be maintained (note, however, that the logback-server.xml also includes a rolling file appender for a “history” log which is attached by default)

Performance Impact

900+ clients doing SRM get



dCache Alarm Commands (man page)

```
Terminal — tcsh

Generates schema documentation for the database of a service. The documentation is written as HTML to
the output directory specified.

ALARM COMMANDS

alarm send [-s=<source info uri>] [-l=<log level>] [-t=<alarm type>] message
Command for sending an arbitrary alarm message to the alarm server.

source info uri the host, domain and service issuing the alarm, in the form:
"src://[host]/[domain]/[service]"; if host is not given, it defaults to the hostname of the node where
the command is issued; if domain is not given, it defaults to "NA"; if service is not given, it
defaults to "command-line".

log level can be ERROR (default), WARN, INFO, DEBUG; these translate into HIGH, MODERATE, LOW and LOW
severity levels.

alarm type additional subtype marker; all alarms are marked ALARM; with type defined, the marker
becomes: ALARM [type].

alarm add
Activates interpreter for adding an alarm definition to the alarm definition xml file. The path for
the latter is determined from alarms.definitions.path.

alarm modify
Activates interpreter for modifying an alarm definition in the alarm definition xml file. The path for
the latter is determined from alarms.definitions.path.

alarm remove
Activates interpreter for removing an alarm definition from the alarm definition xml file. The path
for the latter is determined from alarms.definitions.path.

MISCELLANEOUS COMMANDS

kpwd COMMAND [-debug] [ARGUMENT]...
Management commands for the kpwd authentication file. Allows users and mappings to be created, read,
updated, and deleted.

DEBUGGING COMMANDS

check-config
Checks the dCache main configuration file, dcache.conf, and the node's layout file for any problems
```

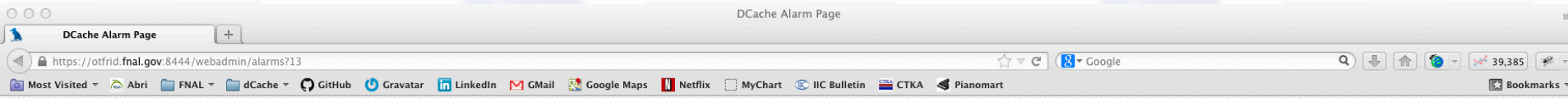
Alarms Web Page

- The Alarms Web Page is an admin page and thus requires authentication. You must enable HTTPS and provide a gid (by default the gid is 0):

```
[httpdDomain]  
    authenticated=true  
    webadminAdminGid=1234  
[httpdDomain/httpd]
```

- Note: for the authenticated mode you need to have a host certificate for your server host and place the hostcert.p12 in the directory /etc/dcache.
- The cleaner daemon runs here. Since RDBMS is the default store, the cleaner is disabled by default.
- The page consists of two panels: a query filter, and a table. The table is paged to contain a maximum of 100 rows per page.
- The web form is set to auto-refresh every minute.

Webadmin Alarms Page



Logged in as arossi | logout

- HOME
- CELL SERVICES
- POOL USAGE
- POOL QUEUES
- POOL QUEUE PLOTS
- POOLGROUPS
- TAPE TRANSFER QUEUE
- ACTIVE TRANSFERS
- BILLING PLOTS
- POOL SELECTION SETUP
- POOL ADMIN
- CELL ADMIN

SPACE TOKENS INFO XML **ALARMS**

QUERY FILTER

Include: All Only Alarms No Alarms Show Closed

Last Update Range: Beginning [17] Ending [17]

Severity: MODERATE Refresh

Type (Alarm) or Level (Warning):

Match Expression: Regular Expression

Limit: From [] Up To []

Refresh forces updates and deletes and then repopulates the table using the current query filter.

Alarms appear in red when "All" is selected

The default behavior is ALL (unspecified properties).

Closed is a way of marking the alarm as having been dealt with while maintaining a record of it.

check or uncheck the respective columns for all displayed items

titles in white can be clicked to sort by that column

database

in memory database

The Match Expression filters in a single string and doing a search. If the Regular Expression box is checked, the match expression is treated as a regex (Java-style).

editable column

ALARMS / WARNINGS

Delete	Close	First	Last	Severity	Type	Count	Host	Domain	Service	Info	Notes
<input type="checkbox"/>	<input type="checkbox"/>	Wed May 22 15:54:01 CDT 2013	Thu May 23 16:28:41 CDT 2013	MODERATE	POOL_SIZE_REDUCTION	186	otftrid.fnal.gov	otftridDomain	pool3	The file system containing the data files appears to have less free space (379,360,948,224 bytes) than expected (379,361,030,144 bytes); reducing the pool size to 379,823,370,240 bytes to compensate. Notice that this does not leave any space for the meta data. If such data is stored on the same file system, then it is paramount that the pool size is reconfigured to leave enough space for the meta data.	...
<input type="checkbox"/>	<input type="checkbox"/>	Wed May 22 15:54:00 CDT 2013	Thu May 23 16:28:40 CDT 2013	MODERATE	POOL_SIZE_REDUCTION	186	otftrid.fnal.gov	otftridDomain	pool1	The file system containing the data files appears to have less free space (379,360,989,184 bytes) than expected (379,361,030,144 bytes); reducing the pool size to 379,851,726,192 bytes to compensate. Notice that this does not leave any space for the meta data. If such data is stored on the same file system, then it is paramount that the pool size is reconfigured to leave enough space for the meta data.	...
<input type="checkbox"/>	<input type="checkbox"/>	Thu May 23 16:28:38 CDT 2013	Thu May 23 16:28:38 CDT 2013	MODERATE	WARN	1	otftrid.fnal.gov	weakftp-otftridDomain	FTP-otftrid-<unknown>-107	Login denied for Subject: Private Credential: PasswordCredential[user=anonymous]	...
<input type="checkbox"/>	<input type="checkbox"/>	Thu May 23 16:28:38 CDT 2013	Thu May 23 16:28:38 CDT 2013	MODERATE	WARN	1	otftrid.fnal.gov	weakftp-otftridDomain	FTP-otftrid-<unknown>-106	Login denied for Subject: Private Credential: PasswordCredential[user=anonymous]	...
<input type="checkbox"/>	<input type="checkbox"/>	Thu May 23 16:28:38 CDT 2013	Thu May 23 16:28:38 CDT 2013	MODERATE	WARN	1	otftrid.fnal.gov	gPlazmaDomain	gPlazma	Login attempt failed; detailed explanation follows: LOGIN FAIL in: PasswordCredential[user=anonymous] +-AUTH OK +-xacml SUFFICIENT:FAIL (no subjects found to map) => OK +-x509 SUFFICIENT:FAIL (no X509 certificate chain) => OK +-kpwd SUFFICIENT:FAIL (anonymous is unknown) => OK +-MAP OK +-kpwd OPTIONAL:FAIL (no mappable principals) => OK +-authzdb OPTIONAL:FAIL (no mappable principal) => OK +-ACCOUNT OK +-SESSION OK +-kpwd OPTIONAL:FAIL (no record found) => OK +-authzdb REQUISITE:OK => OK +-VALIDATION FAIL (no username, no UID, no primary gid)	...
<input type="checkbox"/>	<input type="checkbox"/>	Thu May 23 16:28:38 CDT 2013	Thu May 23 16:28:38 CDT 2013	HIGH	ERROR	1	otftrid.fnal.gov	adminDoorDomain	alm-<unknown>-103	Failed to close socket: java.io.IOException: Broken pipe	...
<input type="checkbox"/>	<input type="checkbox"/>	Thu May 23 16:28:38 CDT 2013	Thu May 23 16:28:38 CDT 2013	MODERATE	WARN	1	otftrid.fnal.gov	adminDoorDomain	alm-<unknown>-103	I/O Failure: java.io.IOException: Broken pipe	...
<input type="checkbox"/>	<input type="checkbox"/>	Thu May 23 16:28:37 CDT 2013	Thu May 23 16:28:37 CDT 2013	MODERATE	WARN	1	otftrid.fnal.gov	adminDoorDomain	ssh2Admin	Exception caught	...
<input type="checkbox"/>	<input type="checkbox"/>	Thu May 23 16:28:37 CDT 2013	Thu May 23 16:28:37 CDT 2013	MODERATE	WARN	1	otftrid.fnal.gov	kerberosdcap-otftridDomain	DCap-Kerberos-otftrid	Exception in secure protocol : java.lang.reflect.InvocationTargetException	...

Webadmin Alarms Page

QUERY FILTER

Include	All <input checked="" type="radio"/> Only Alarms <input type="radio"/> No Alarms <input type="radio"/>	Show Closed <input type="checkbox"/>
Last Update Range	Beginning <input type="text"/> 17	Ending <input type="text"/> 17
Severity	MODERATE ▾	Refresh
Type (Alarm) or Level (Warning)	S	
Match Expression	ALARM	Regular Expression <input type="checkbox"/>
Limit		

Delete	Close	First	Type	Count	Host	Domain
<input type="checkbox"/>	<input type="checkbox"/>	Wed May 22 15:54:01 CDT 2013	SIZE_REDUCTION	187	otfrid.fnal.gov	otfridDomain
<input type="checkbox"/>	<input type="checkbox"/>	Wed May 22 15:54:00 CDT 2013	SIZE_REDUCTION	187	otfrid.fnal.gov	otfridDomain
		Thu May 23				

The filter makes use of the **alarms-definition.xml** file for auto-completion on the type field. If the httpd service is running on a different host from the alarm server, you currently will need to copy changes from the latter manually to keep the options up to date.

The Alarm Definition Schema

- *type*: defines the alarm
- *logger*: require event to be issued from this logger
- *regex*: capture message pattern as basis for definition
- *regexFlags*: Java options; see the Java Tutorials on Regular Expressions [<http://docs.oracle.com/javase/tutorial/essential/regex/>])
- *matchException*: match the embedded exception(s) along with the message
- *depth*: level to which to continue to search for a match in embedded exceptions
- *level*: require event to be issued at this level
- *severity*: classifies the alarm
- *thread*: restrict alarm to this thread
- *includeInKey*: this combination of attribute values serves uniquely to identify the alarm
 - fields are: *groupN*, *timestamp*, *message*, *logger*, *type*, *domain*, *service*, *host* and *thread*

See Chapter 16 of the dCache Book for fuller explanation of possible values and defaults for each.

The dcache alarm add & modify commands are a useful way of creating or editing alarms without having to remember all the options or required values.

Suggestion: backup the *alarms-definition.xml* file before running these commands or modifying it by hand.

```

58 <matchException>true</matchException>
59 <level>ERROR</level>
60 <severity>CRITICAL</severity>
61 <includeInKey>type host domain</includeInKey>
62 </alarmType>
63 <alarmType>
64 <type>IO_ERROR</type>
65 <regex>I/O.*failed(.+)|I/O error occur.*ed(.+)</regex>
66 <matchException>true</matchException>
67 <level>WARN</level>
68 <severity>HIGH</severity>
69 <includeInKey>group1 type host service domain</includeInKey>
70 </alarmType>
71 <alarmType>
72 <type>HSM_READ_FAILURE</type>
73 <regex>Fetch failed: HSM script failed</regex>
74 <level>WARN</level>
75 <severity>HIGH</severity>
76 <includeInKey>type host service domain</includeInKey>
77 </alarmType>
78 <alarmType>
79 <type>HSM_WRITE_FAILURE</type>
80 <regex>Store failed: HSM script failed</regex>
81 <level>WARN</level>
82 <severity>HIGH</severity>

```

Demo 1 – Sending an Ad Hoc Alarm

The terminal window shows the following commands and output:

```
[arossi@otfrid ~]$ dcache alarm send ALARM 1
sending alarm to localhost:60001
24 May 2013 08:35:57 [host=otfrid.fnal.gov, service=command-line, domain=NA] ALARM 1
[arossi@otfrid ~]$ dcache alarm send -l="WARN" ALARM 2
sending alarm to localhost:60001
24 May 2013 08:36:02 [host=otfrid.fnal.gov, service=command-line, domain=NA] ALARM 2
[arossi@otfrid ~]$ dcache alarm send -l="INFO" ALARM 3
sending alarm to localhost:60001
24 May 2013 08:36:08 [host=otfrid.fnal.gov, service=command-line, domain=NA] ALARM 3
[arossi@otfrid ~]$ dcache alarm send -t="TEST" ALARM 4
sending alarm to localhost:60001
24 May 2013 08:36:38 [host=otfrid.fnal.gov, service=command-line, domain=NA] ALARM 4
[arossi@otfrid ~]$ dcache alarm send -t="TEST" -s="src://otfrid.fnal.gov/arossi/home" ALARM 5
sending alarm to localhost:60001
24 May 2013 08:37:47 [host=otfrid.fnal.gov, service=home, domain=arossi] ALARM 5
[arossi@otfrid ~]$
```

The browser window shows the dCache ALARMS page. A red arrow points from the terminal output for ALARM 3 to the 'ALARMS' tab in the browser. A text box next to the browser says: "System Level = WARN, INFO does not get sent".

The 'ALARMS' table in the browser shows the following data:

Delete	Close	First	Last	Severity	Type	Count	Host	Domain	Service	Info	Notes
<input type="checkbox"/>	<input type="checkbox"/>	Fri May 24 08:37:47 CDT 2013	Fri May 24 08:37:47 CDT 2013	HIGH	ALARM [TEST]	1	otfrid.fnal.gov	arossi	home	ALARM 5	...
<input type="checkbox"/>	<input type="checkbox"/>	Fri May 24 08:36:38 CDT 2013	Fri May 24 08:36:38 CDT 2013	HIGH	ALARM [TEST]	1	otfrid.fnal.gov	NA	command-line	ALARM 4	...
<input type="checkbox"/>	<input type="checkbox"/>	Fri May 24 08:36:02 CDT 2013	Fri May 24 08:36:02 CDT 2013	MODERATE	ALARM	1	otfrid.fnal.gov	NA	command-line	ALARM 2	...
<input type="checkbox"/>	<input type="checkbox"/>	Fri May 24 08:35:57 CDT 2013	Fri May 24 08:35:57 CDT 2013	HIGH	ALARM	1	otfrid.fnal.gov	NA	command-line	ALARM 1	...

At the bottom of the browser window, there is a search bar with the text "Find: SMTP" and navigation buttons: "< Previous", "> Next", "Highlight all", and "Match case".

Demo 2 – Alarm Discovery and Definition

Example: missing CRL Certs

1. *check that srmIs works:*

```
[arossi@otfrid dcache]$ srmIs srm://otfrid/  
512 //
```

2. *remove DOE certs:*

```
[root@otfrid dcache]# cd /etc/grid-security/certificates/  
[root@otfrid certificates]# mkdir ../DOEGrids  
[root@otfrid certificates]# for i in `grep "DC=DOEGrids" *.namespaces | grep PERMIT | cut -d '.' -f 1`; do mv ${i}.* ../DOEGrids ; done;  
[root@otfrid certificates]# ls -l ../DOEGrids/  
total 116  
-rw-r--r--. 1 root root 1448 May 13 14:38 0119347c.0  
-rw-r--r--. 1 root root 621 May 13 14:38 0119347c.namespaces  
-rw-r--r--. 1 root root 2238 May 13 14:38 0119347c.signing_policy  
-rw-r--r--. 1 root root 1610 May 13 14:38 12d0da68.0  
-rw-r--r--. 1 root root 833 May 13 14:38 12d0da68.namespaces  
-rw-r--r--. 1 root root 2316 May 13 14:38 12d0da68.signing_policy  
-rw-r--r--. 1 root root 1610 May 13 14:38 1c3f2ca8.0  
-rw-r--r--. 1 root root 833 May 13 14:38 1c3f2ca8.namespaces  
-rw-r--r--. 1 root root 21702 May 13 14:38 1c3f2ca8.r0  
-rw-r--r--. 1 root root 2316 May 13 14:38 1c3f2ca8.signing_policy  
-rw-r--r--. 1 root root 1448 May 13 14:38 d1b603c3.0  
-rw-r--r--. 1 root root 621 May 13 14:38 d1b603c3.namespaces  
-rw-r--r--. 1 root root 1028 May 13 14:38 d1b603c3.r0  
-rw-r--r--. 1 root root 2238 May 13 14:38 d1b603c3.signing_policy  
-rw-r--r--. 1 root root 107 May 13 14:38 DOEGrids.crl_url  
-rw-r--r--. 1 root root 457 May 13 14:38 DOEGrids.info  
-rw-r--r--. 1 root root 833 May 13 14:38 DOEGrids.namespaces  
-rw-r--r--. 1 root root 1610 May 13 14:38 DOEGrids.pem  
-rw-r--r--. 1 root root 2316 May 13 14:38 DOEGrids.signing_policy  
-rw-r--r--. 1 root root 102 May 13 14:38 ESnet.crl_url  
-rw-r--r--. 1 root root 438 May 13 14:38 ESnet.info  
-rw-r--r--. 1 root root 621 May 13 14:38 ESnet.namespaces  
-rw-r--r--. 1 root root 1448 May 13 14:38 ESnet.pem  
-rw-r--r--. 1 root root 2238 May 13 14:38 ESnet.signing_policy
```

Demo 2 – Alarm Discovery and Definition

Example: missing CRL Certs

3. restart dCache:

```
dcache restart
```

4. srmIs now reports this error:

```
[arossi@otfrid ~]$ srmIs srm://otfrid/  
SRMClientV2 : srmIs: try # 0 failed with error  
SRMClientV2 : ; nested exception is:  
    java.net.SocketException: Connection reset  
SRMClientV2 : srmIs: try again
```

5. We go to the srm log and find:

```
24 May 2013 12:52:31 (SRM-otfrid) [131.225.80.252:48693] Problem while establishing secure connection:  
org.globus.common.ChainedIOException: Authentication failed [Caused by: Path validation failed: No trusted path can be  
constructed]
```

6. Let's say we have finally diagnosed this as a missing CRL certificate problem. Now we want to define an alarm as:

type:	MISSING_CRL_CERT
logger:	(don't know this)
level:	ERROR?
severity:	HIGH
regex:	No trusted path can be constructed
matchException:	true
depth:	2?
includeInKey:	host type

7. Let's add it using the interpreter:

```
[root@otfrid certificates]# cd /var/lib/dcache/alarms/  
[root@otfrid alarms]# cp alarm-definitions.xml alarm-definitions.xml-20130528  
[root@otfrid alarms]# ls  
alarm-definitions.xml alarm-definitions.xml-20130524 datanucleus.properties history.log logback-server.xml logback-  
server.xml-2.6 logback-server.xml-2.7 server.log  
[root@otfrid alarms]# dcache alarm add
```

Demo 2 – Alarm Discovery and Definition

Example: missing CRL Certs

Choose attribute to define, 'h[elp]' to describe attributes, 'q[uit]' to abort, return to process the definition.

Attributes: [depth, includeInKey, level, logger, matchException, regex, regexFlags, severity, thread, type]

>> **depth**

(match nested exception messages using regex only to this level (integer, optional; default: undefined))

hit return to skip, - to remove value

>> **2**

Choose attribute to define, 'h[elp]' to describe attributes, 'q[uit]' to abort, return to process the definition.

Attributes: [depth, includeInKey, level, logger, matchException, regex, regexFlags, severity, thread, type]

>> **includeInKey**

(create the unique identifier for this alarm event based on the selected fields (whitespace delimited) [timestamp, message, groupN, logger, type, domain, service, host, thread] (required))

hit return to skip, - to remove value

>> **host type**

Choose attribute to define, 'h[elp]' to describe attributes, 'q[uit]' to abort, return to process the definition.

Attributes: [depth, includeInKey, level, logger, matchException, regex, regexFlags, severity, thread, type]

>> **level**

(match events at this logging level or greater [ERROR, WARN, INFO, DEBUG, TRACE] (required))

hit return to skip, - to remove value

>> **ERROR**

Choose attribute to define, 'h[elp]' to describe attributes, 'q[uit]' to abort, return to process the definition.

Attributes: [depth, includeInKey, level, logger, matchException, regex, regexFlags, severity, thread, type]

>> **matchException**

(apply the regex to nested exception messages (boolean, optional; default: false))

hit return to skip, - to remove value

>> **true**

Choose attribute to define, 'h[elp]' to describe attributes, 'q[uit]' to abort, return to process the definition.

Attributes: [depth, includeInKey, level, logger, matchException, regex, regexFlags, severity, thread, type]

>> **regex**

(Java-style regular expression used to match messages (required if logger is not specified))

hit return to skip, - to remove value

>> **No trusted path can be constructed**

Demo 2 – Alarm Discovery and Definition

Example: missing CRL Certs

Choose attribute to define, 'h[elp]' to describe attributes, 'q[uit]' to abort, return to process the definition.

Attributes: [depth, includeInKey, level, logger, matchException, regex, regexFlags, severity, thread, type]

>> **(ARE WE DONE? LET'S HIT RETURN AND SEE ...)**

type is a required attribute

incomplete or invalid definition

Choose attribute to define, 'h[elp]' to describe attributes, 'q[uit]' to abort, return to process the definition.

Attributes: [depth, includeInKey, level, logger, matchException, regex, regexFlags, severity, thread, type]

>> **type**

(choose a name to call this type of alarm (required))

hit return to skip, - to remove value

>> **MISSING_CRL_CERT**

Choose attribute to define, 'h[elp]' to describe attributes, 'q[uit]' to abort, return to process the definition.

Attributes: [depth, includeInKey, level, logger, matchException, regex, regexFlags, severity, thread, type]

>> **(ARE WE DONE?)**

Alarm Definition:

```
-----  
<alarmType>  
<depth>2</depth>  
<includeInKey>host type</includeInKey>  
<level>ERROR</level>  
<regex>No trusted path can be constructed</regex>  
<severity>MODERATE</severity>  
<type>MISSING_CRL_CERT</type>  
</alarmType>  
-----
```

Add/Update definition? <y/n> [n]: **(OOPS, FORGOT TO MAKE SEVERITY "HIGH" ...)**

n

Quit? <q>: **(JUST HIT RETURN TO KEEP GOING ...)**

Choose attribute to define, 'h[elp]' to describe attributes, 'q[uit]' to abort, return to process the definition.

Attributes: [depth, includeInKey, level, logger, matchException, regex, regexFlags, severity, thread, type]

>> **severity**

(alarm-specific level [LOW, MODERATE, HIGH, CRITICAL] (optional; default: MODERATE))

hit return to skip, - to remove value

>> **HIGH**

Demo 2 – Alarm Discovery and Definition

Example: missing CRL Certs

Choose attribute to define, 'h[elp]' to describe attributes, 'q[uit]' to abort, return to process the definition.

Attributes: [depth, includeInKey, level, logger, matchException, regex, regexFlags, severity, thread, type]

>> **(ARE WE DONE?)**

Alarm Definition:

```
-----  
<alarmType>  
  <depth>2</depth>  
  <includeInKey>host type</includeInKey>  
  <level>ERROR</level>  
  <regex>No trusted path can be constructed</regex>  
  <severity>HIGH</severity>  
  <type>MISSING_CRL_CERT</type>  
</alarmType>  
-----
```

Add/Update definition? <y/n> [n]: **(YES, LET'S COMMIT ...)**

y

[root@otfrid alarms]# less alarm-definitions.xml

...

```
<alarmType>  
  <depth>2</depth>  
  <includeInKey>host type</includeInKey>  
  <level>ERROR</level>  
  <regex>No trusted path can be constructed</regex>  
  <severity>HIGH</severity>  
  <type>MISSING_CRL_CERT</type>  
</alarmType>  
</definitions>
```

8. restart alarmserver:

[root@otfrid alarms]# dcache restart alarmserverDomain

Stopping alarmserverDomain 0 done

Starting alarmserverDomain done

Demo 2 – Alarm Discovery and Definition

Example: missing CRL Certs

9. *do srmls to see if we can produce an alarm:*

```
[arossi@otfrid ~]$ srmls srm://otfrid/
SRMClientV2 : srmls: try # 0 failed with error
SRMClientV2 : ; nested exception is:
    java.net.SocketException: Connection reset
SRMClientV2 : srmls: try again
```

10. *Let's check Alarms Web Page:*

ALARMS / WARNINGS

Delete	Close	First	Last	Severity	Type	Count	Host	Domain	Service	Info	Notes
<input type="checkbox"/>	<input type="checkbox"/>	Fri May 24 17:54:48 CDT 2013	Fri May 24 17:54:48 CDT 2013	MODERATE	WARN	1	otfrid.fnal.gov	srm-otfridDomain	SRM-otfrid	Problem while establishing secure connection: org.globus.common.ChainedIOException: Authentication failed [Caused by: Path validation failed: No trusted path can be constructed]	...
<input type="checkbox"/>	<input type="checkbox"/>	Fri May 24 17:53:26 CDT 2013	Fri May 24 17:53:26 CDT 2013	MODERATE	WARN	1	<unknown host>	<unknown domain>	<unknown service>	... for while reading from tunnel: null	...
<input type="checkbox"/>	<input type="checkbox"/>	Fri May 24 17:53:26 CDT 2013	Fri May 24 17:53:26 CDT 2013	MODERATE	WARN	1	<unknown host>	<unknown domain>	<unknown service>	Sleeping 17 seconds	...

HEY, WHERE'S MY ALARM?

no alarm, but I see a WARN level message. Should have checked there first! We misdefined it, so let's modify:

```
[root@otfrid alarms]# dcache alarm modify
```

Demo 2 – Alarm Discovery and Definition

Example: missing CRL Certs

Alarm type to modify:

>> **MISSING_CRL_CERT**

Alarm Definition:

```
-----  
<alarmType>  
  <depth>2</depth>  
  <includeInKey>type</includeInKey>  
  <level>ERROR</level>  
  <regex>No trusted path can be constructed</regex>  
  <severity>HIGH</severity>  
  <type>MISSING_CRL_CERT</type>  
</alarmType>
```

Choose attribute to define, 'h[elp]' to describe attributes, 'q[uit]' to abort, return to process the definition.

Attributes: [depth, includeInKey, level, logger, matchException, regex, regexFlags, severity, thread, type]

>> **level**

(match events at this logging level or greater [ERROR, WARN, INFO, DEBUG, TRACE] (required))

hit return to skip, - to remove value

>> **WARN**

Choose attribute to define, 'h[elp]' to describe attributes, 'q[uit]' to abort, return to process the definition.

Attributes: [depth, includeInKey, level, logger, matchException, regex, regexFlags, severity, thread, type]

>> **(DONE ...)**

Alarm Definition:

```
-----  
<alarmType>  
  <depth>2</depth>  
  <includeInKey>host type</includeInKey>  
  <level>WARN</level>  
  <matchException>>false</matchException>  
  <regex>No trusted path can be constructed</regex>  
  <severity>HIGH</severity>  
  <type>MISSING_CRL_CERT</type>  
</alarmType>
```

Add/Update definition? <y/n> [n]:

y

Demo 2 – Alarm Discovery and Definition

Example: missing CRL Certs

11. restart alarmserver:

```
[root@otfrid alarms]# dcache restart alarmserverDomain
Stopping alarmserverDomain 0 done
Starting alarmserverDomain done
```

12. do srmls again to see if we can produce an alarm:

```
[arossi@otfrid ~]$ srmls srm://otfrid/
SRMClientV2 : srmLs: try # 0 failed with error
SRMClientV2 : ; nested exception is:
    java.net.SocketException: Connection reset
SRMClientV2 : srmLs: try again
```

13. Let's check Alarms Web Page:

ALARMS / WARNINGS

Delete	Close	First	Last	Severity	Type	Count	Host	Domain	Service	Info	Notes
<input type="checkbox"/>	<input type="checkbox"/>	Fri May 24 17:58:26 CDT 2013	Fri May 24 17:58:26 CDT 2013	HIGH	MISSING_CRL_CERT	1	otfrid.fnal.gov	srm-otfridDomain	SRM-otfrid	Problem while establishing secure connection: org.globus.common.ChainedIOException: Authentication failed [Caused by: Path validation failed: No trusted path can be constructed]	...
<input type="checkbox"/>	<input type="checkbox"/>	Fri May 24 17:56:33 CDT 2013	Fri May 24 17:56:33 CDT 2013	MODERATE	WARN	1	<unknown host>	<unknown domain>	<unknown service>	Error while reading from tunnel: null	...
<input type="checkbox"/>	<input type="checkbox"/>	Fri May 24 17:56:33 CDT 2013	Fri May 24 17:56:33 CDT 2013	MODERATE	WARN	1	<unknown host>	<unknown domain>	<unknown service>	Sleeping 25 seconds	...
<input type="checkbox"/>	<input type="checkbox"/>	Fri May 24 17:54:48 CDT 2013	Fri May 24 17:54:48 CDT 2013	MODERATE	WARN	1	otfrid.fnal.gov	srm-otfridDomain	SRM-otfrid	Problem while establishing secure connection: org.globus.common.ChainedIOException: Authentication failed [Caused by: Path validation failed: No trusted path can be constructed]	...

SUCCESS!

Questions or Comments Welcome