Securing dCache Communications

Anupam Ashish, on behalf of dCache team

11th International dCache Workshop 2017, Umea, Sweden
Distributed Redundant Cells

Message Passing
Multi-site deployment

Primary Site

Pool Manager

Core Domain

ZK Node 1

ZK Node 3

ZK Node 3

Secondary Site 1

WebDAV

Secondary Site 2

Pool
Motivation

• Federated dCache
  • Multi-site Deployment
  • Separated Geographically

• Secure over-the-Network communications

• Requirements based on Joint-Russian-German Project
  • NRC “Kurchatov Institute”, Moscow
  • JINR, Dubna
  • DESY Hamburg
Internal dCache Communications

Inter-Cell Communication
- Message Passing
- Routing

Zookeeper
- Service discovery
- Coordination
- Configuration
Cells

- Smallest addressable unit in dCache
- Cells have names

Routing mechanism
Zookeeper

- Key/Value Store
- Strong Consistency Guarantees
- Configuration Management
- Distributed Synchronization
What we want to achieve ..

Inter-Cell Communication
- Message Passing
- Routing

Zookeeper
- Service discovery
- Coordination
- Configuration
Multi-site deployment
Multi-site deployment
Secure Cell Communications

dcache.broker.core.channel.security

- Support both TLS and Plain communication
- Disable encryption for all messages on the internal network

Core Domain

- BOTH
- TLS

Satellite Domains

- PLAIN
- OR
- TLS
Secure Communications

- dcache.broker.channel.credential.key
- dcache.broker.channel.credential.cert
- dcache.broker.channel.credential.capath

Rely on TLS authentication
Zookeeper

- Stable release 3.4.x
- No support for TLS in the stable release
- Support for TLS comes in 3.5.x and 3.6.x
Zookeeper Backwards Compatible

/dcache
    /lm
    /lmd
    /cores
    zk.desy.desy:2181
    tls://zk.desy.de:2182
tcp://zk.desy.de:2181
Zookeeper with Stunnel

- **Proxy designed to add TLS encryption functionality**
  - without any changes in the programs' code.

- **Provides**
  - Security
  - Portability
  - Scalability (including load-balancing)

### SERVER

```
[zookeeper]
accept = 2182
connect = zoocluster1.noname.de:2181
connect = zoocluster2.noname.de:2181
cert = /etc/stunnel/stunnel.pem
checkHost = zooclient1.noname.de
checkHost = zooclient2.noname.de
CAPath = /opt/noname/certs
```

### CLIENT

```
[zookeeper]
client = yes
accept = 2181
connect = stunnel.noname.de:2182
;verify = 2
cert = /etc/stunnel/stunnel.pem
CAPath = /opt/noname/certs
checkHost = stunnel.noname.de
;OCSPaia = yes
```
Zookeeper with Stunnel

Primary Site

Core Domain

Pool Manager

Stunnel Server

ZK Node 1
ZK Node 3
ZK Node 3

Secondary Site 1

Pool

Stunnel Client

Secondary Site 2

Pool

Stunnel Client
ZooKeeper with Stunnel
Zookeeper with Stunnel
Zookeeper with Stunnel

Primary Site

Core Domain

Pool Manager

Stunnel Server

ZK Node 1
ZK Node 3
ZK Node 3

Pool

Secondary Site 1

Stunnel Client

Secondary Site 2

Stunnel Client
Zookeeper with Stunnel
Overhead

Cell Ping Times

- TLS
- Plain

MILLISECONDS vs. BYTES
Recap

- dCache multi-site deployment
- Secure Cell–Communication
  - With TLS Authentication
- Secure Zookeeper
  - 3.5.x and 3.6.x
- Stunnel for Zookeeper 3.4.x
Thank You !!
<table>
<thead>
<tr>
<th>Bytes</th>
<th>TLS</th>
<th>Stddev (TLS)</th>
<th>Plain</th>
<th>Stddev (Plain)</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>6.066532</td>
<td>0.962029</td>
<td>4.923287</td>
<td>1.528073</td>
</tr>
<tr>
<td>200</td>
<td>5.852289</td>
<td>1.207879</td>
<td>4.845971</td>
<td>1.083889</td>
</tr>
<tr>
<td>500</td>
<td>5.92067</td>
<td>1.150411</td>
<td>4.965656</td>
<td>1.073847</td>
</tr>
<tr>
<td>750</td>
<td>5.991981</td>
<td>0.971823</td>
<td>4.92993</td>
<td>1.25704</td>
</tr>
<tr>
<td>1000</td>
<td>5.792476</td>
<td>0.965675</td>
<td>4.899043</td>
<td>1.085029</td>
</tr>
<tr>
<td>1500</td>
<td>5.818405</td>
<td>1.268044</td>
<td>4.947244</td>
<td>1.215096</td>
</tr>
<tr>
<td>2000</td>
<td>5.910056</td>
<td>0.985793</td>
<td>4.833325</td>
<td>1.179955</td>
</tr>
<tr>
<td>5000</td>
<td>5.744266</td>
<td>1.034607</td>
<td>4.716026</td>
<td>1.116742</td>
</tr>
<tr>
<td>10000</td>
<td>5.842495</td>
<td>1.147705</td>
<td>4.949989</td>
<td>1.120223</td>
</tr>
<tr>
<td>12000</td>
<td>5.771063</td>
<td>1.011539</td>
<td>4.836352</td>
<td>1.182209</td>
</tr>
<tr>
<td>15000</td>
<td>5.681811</td>
<td>0.996409</td>
<td>4.930635</td>
<td>1.088731</td>
</tr>
<tr>
<td>17500</td>
<td>5.687488</td>
<td>1.056684</td>
<td>4.970123</td>
<td>1.083949</td>
</tr>
<tr>
<td>20000</td>
<td>5.802021</td>
<td>1.007485</td>
<td>4.717774</td>
<td>1.14542</td>
</tr>
<tr>
<td>25000</td>
<td>5.640754</td>
<td>0.901774</td>
<td>4.913348</td>
<td>1.39213</td>
</tr>
</tbody>
</table>
Zookeeper 3.5.x and 3.6.x

**zoo.cfg**
- secureClientPort = 2281

**Server**
- zookeeper.serverCnxnFactory = org.apache.zookeeper.server.NettyServerCnxnFactory
  - zookeeper.ssl.keyStore.location
  - zookeeper.ssl.trustStore.location
  - zookeeper.ssl.keyStore.password = testpass
  - zookeeper.ssl.trustStore.password

**Client**
- zookeeper.client.secure = true
  - zookeeper.clientCnxnSocket = org.apache.zookeeper.ClientCnxnSocketNetty
    - zookeeper.ssl.keyStore.location
    - zookeeper.ssl.keyStore.password
    - zookeeper.ssl.trustStore.location
Coordination

Message Passing

Operation

Redundancy