Ticket-based Access

DICE-UCSD

Wayne Schroeder

http://irods.org















Tickets Overview

Requested by iPlant for specific use cases

Less secure but flexible and various features improve safety

- Plain-text, shared in email, etc.
- Restrictions on client host, uses, users/groups, etc.

Pseudo-random, like 6tvQlqNXIbTCTX, or owner-selected

All Attributes Maintained in ICAT

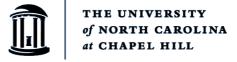
Owner can mod, add/remove restrictions, remove at any time.

Changes to internal ICAT SQL Access control

- irods users, anonymous, strict mode
- Collections, data-object queries















Ticket Interfaces

iticket

– create, modify, remove, list iget/iput -t Ticket

Java Jargon-interface

- create, modify, remove, list
- And utilize















iticket sub-commands

create read/write Object-Name [string] (create a new ticket) mod Ticket_string-or-id uses/expire string-or-none (modify restrictions) mod Ticket_string-or-id write-bytes-or-file number-or-0 (modify restrictions) mod Ticket_string-or-id add/remove host/user/group string (modify restrictions) Is [Ticket_string-or-id] (non-admins will see just your own) Is-all (list all your tickets, even with missing targets) delete ticket_string-or-id quit















iticket examples

schroeder@zuri:~\$ iticket Is d3w

id: 27070 string: d3w

ticket type: write obj type: collection owner name: rods

owner zone: newZone

uses count: 0 uses limit: 0

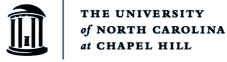
write file count: 3 write file limit: 10 write byte count: 0 write byte limit: 0 expire time: none

collection name: /newZone/home/rods/d3

No host restrictions No user restrictions No group restrictions schroeder@zuri:~\$















iticket examples

schroeder@zuri:~\$ iput file1

schroeder@zuri:~\$ iticket create read file1 file1t

schroeder@zuri:~\$ iticket Is file1t

id: 28071 string: file1t

ticket type: read

obj type: data

owner name: rods

owner zone: newZone

uses count: 0 uses limit: 0

write file count: 0
write file limit: 10
write byte count: 0
write byte limit: 0
expire time: none

data-object name: file1

data collection: /newZone/home/rods

No host restrictions No user restrictions No group restrictions

schroeder@zuri:~\$















iticket examples

schroeder@zuri:~\$ iticket

iticket>mod file1t add host pivo.ucsd.edu

iticket>ls file1t

id: 28071

string: file1t

ticket type: read

obj type: data

owner name: rods

owner zone: newZone

uses count: 0 uses limit: 0

write file count: 0 write file limit: 10 write byte count: 0 write byte limit: 0

expire time: none

data-object name: file1

data collection: /newZone/home/rods restricted-to host: 137.110.243.161

No user restrictions No group restrictions

iticket>

















iticket testing

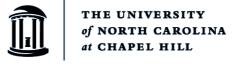
Jargon Java Test Suite

server/test/bin/icatTicketTest.pl:

```
# Basic means access fails without ticket, succeeds with it.
# 'use' checks that it updates and limit is enforced.
# 'write-bytes' and 'write-files' also check for updates and limits enforced.
              basic expire use host user group
#read file user
#read file anon
#read file strict
#read coll user
                         Χ
                              Χ
#read coll anon
                          Χ
                                    Χ
                                        Χ
#read coll strict
                        Χ
                             X X
                                     х х
                                     write-bytes write-files
#write file user
                                                       Χ
#write file anon
                                                        Χ
#write file strict
                                                      Х
#write coll user
                         Χ
                                  Χ
                                                        Χ
#write coll anon
                          Χ
                               Х
                                                        Χ
#write coll strict
                                 X \quad X \quad X
                        Χ
                                                       Χ
```















More Information

irods.org

- Ticket-based Access page
- Release Notes 3.1

iticket h iticket h mod















Wayne Schroeder schroeder@diceresearch.org http://irods.org







