NORDUGRID

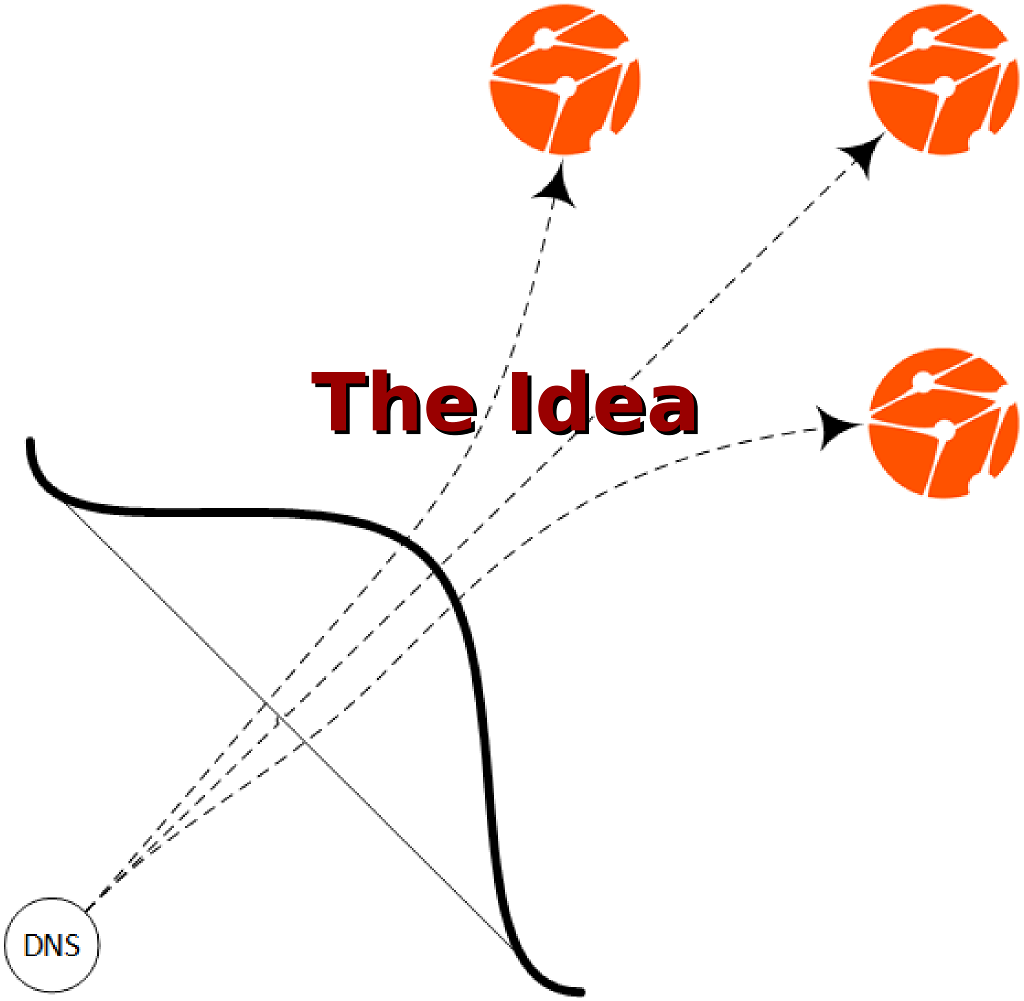
Grid Solution for Wide Area
Computing and Data Handling

ARCHERY, the ARC Hierarchical Endpoints Registry

The next generation Information Index Service for ARC

Andrii Salnikov

The Idea



EGIIS issues

- Bottom-to-top registration anyway requires whitelisting on the “top”
  - otherwise anyone can modify/DOS public EGIIS
- Registration of resource does not guarantee its availability
  - registration process is completely separated from AREX/ARIS operation
- Communities relies on static lists of CEs
  - EGIIS is still useful for ldap-monitor only

BUT static list needs to be distributed

ARCHERY Origins

- ARCHERY is a static list on steroids
  - DNS powerful services infrastructure
    - **integrity**
      - your static list delivery included in price
    - **resiliency**
      - no single point of failure
    - **caching**
      - on OS and network level controlled by TTL
  - Static and single for clients, but
    - **dynamically update-able** with DDNS/TSIG
    - **delegated** to several (country-based?) NS
    - and yes, **H** is for “**Hierarchical**” by design

ARCHERY specification

- **_archery** TXT RR as an entry point
- RR format for each endpoint is:
  - **u=**<uri> **t=**<type> [**t=**<type>...] [**s=**<status>]

```
_archery    300 IN TXT "u=https://arc.univ.kiev.ua:443/arex
t=org.ogf.glue.emies.resourceinfo"

_archery    300 IN TXT "u=ldap://arc.univ.kiev.ua:2135/Mds-Vo-
Name=local,o=grid t=org.nordugrid.ldapng"

_archery    300 IN TXT "u=ldap://arc.univ.kiev.ua:2135/o=glue
t=org.nordugrid.ldapglue2"
```

Endpoint Types

- Resource information system endpoint types:
  - org.nordugrid.ldapng
  - org.nordugrid.ldapglue2
  - org.ogf.glue.emies.resourceinfo
- Endpoint registries types:
  - **org.nordugrid.archery**
  - org.nordugrid.ldapegiis
  - org.nordugrid.emir
  - org.nordugrid.bdii

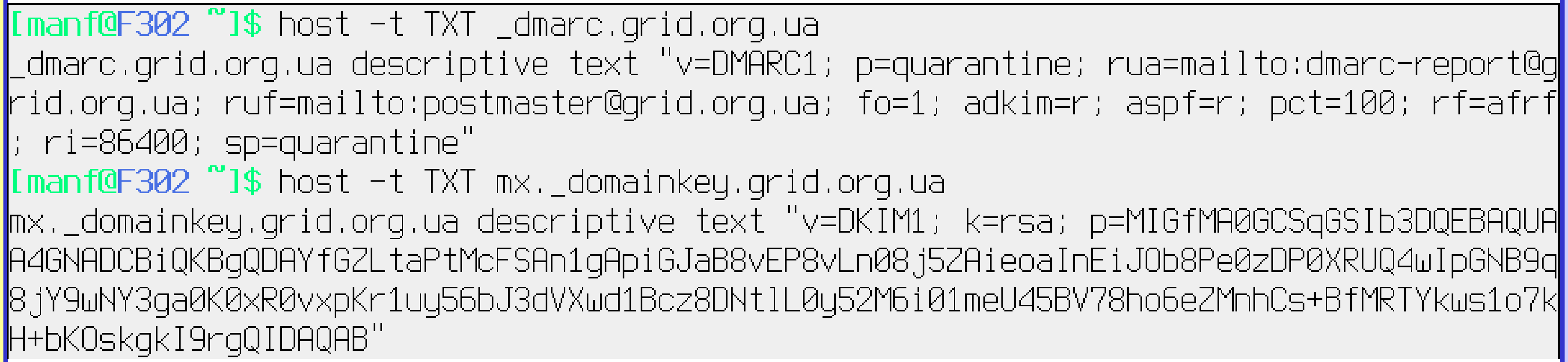
H for Hierarchical

- Index→[Index→...]→CE Endponts
- ARCHERY pointer VS direct DNS pointer

```
$ORIGIN nordugrid.org.
_archery       TXT   "u=grid.org.ua t=org.nordugrid.archery"

$ORIGIN grid.org.ua.
_archery       TXT   "u=dns://knu._archery.grid.org.ua
                       t=org.nordugrid.archery"
_archery       TXT   "u=dns://imbg._archery.grid.org.ua
                       t=org.nordugrid.archery"

knu._archery   TXT   "u=ldap://arc.univ.kiev.ua:2135/Mds-Vo-
                       Name=local,o=grid t=org.nordugrid.ldapng"
knu._archery   TXT   "u=ldap://arc.univ.kiev.ua:2135/o=glue
                       t=org.nordugrid.ldapglue2"

imbg._archery  TXT   "u=https://arc.imbg.org.ua:60000/arex
                        t=org.ogf.glue.emies.resourceinfo"
```

Is DNS ever used this way?

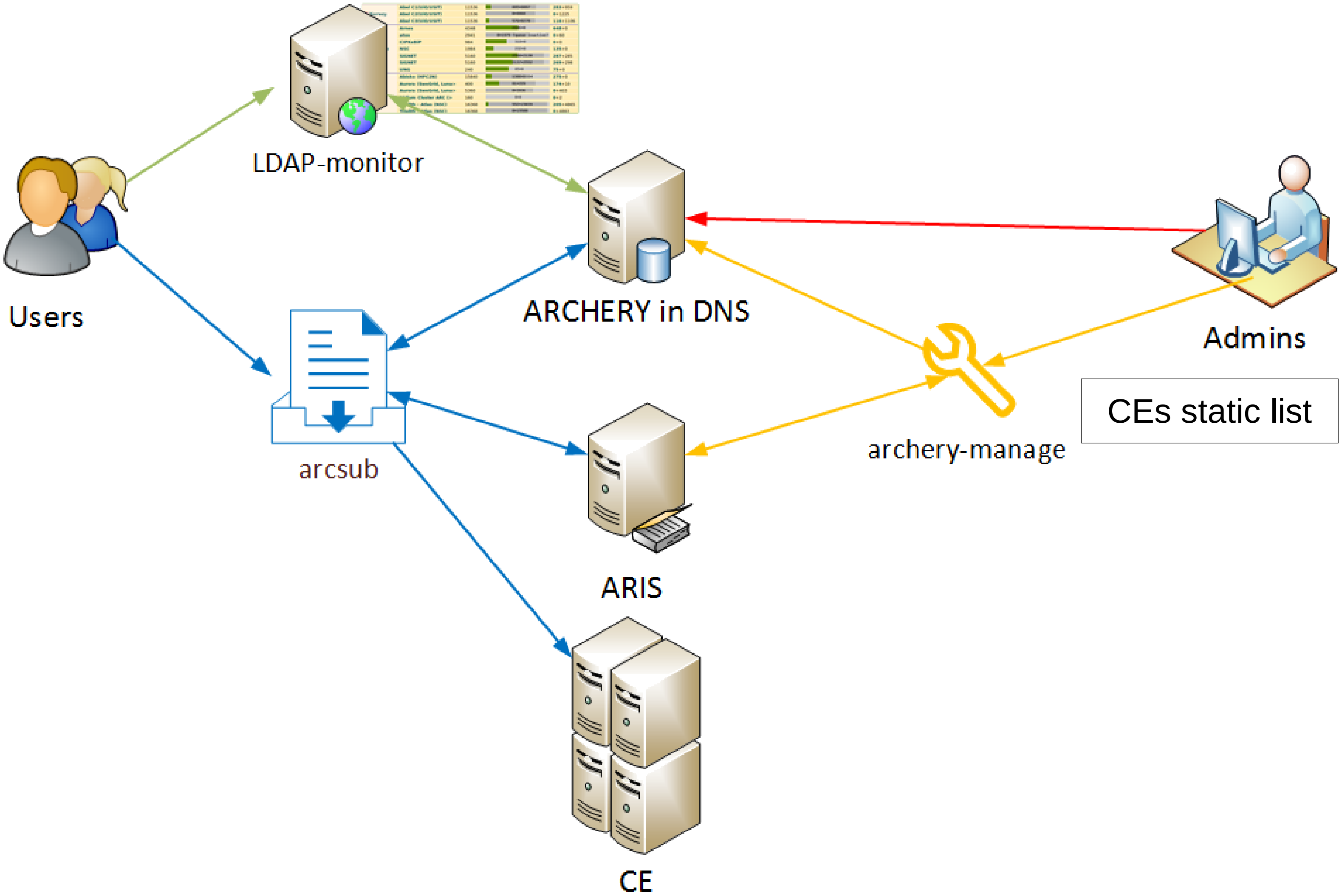
- Yes, the major example is
  - e-mail security is heavily rely on DNS RR
    - SFP [RFC 7208], DKIM [RFC 6376], DMARK [RFC 7489]



```
[manf@F302 ~]$ host -t TXT _dmarc.grid.org.ua
_dmarc.grid.org.ua descriptive text "v=DMARC1; p=quarantine; rua=mailto:dmarc-report@g
rid.org.ua; ruf=mailto:postmaster@grid.org.ua; fo=1; adkim=r; aspf=r; pct=100; rf=afrf
; ri=86400; sp=quarantine"
[manf@F302 ~]$ host -t TXT mx._domainkey.grid.org.ua
mx._domainkey.grid.org.ua descriptive text "v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQDAYfGZLtaPtMcFSAn1gApiGJaB8vEP8vLn08j5ZAieoaInEiJOb8Pe0zDP0XRUQ4wIpGNB9q
8jY9wNY3ga0K0xR0vxpKr1uy56bJ3dVXwd1Bcz8DNtlL0y52M6i01meU45BV78ho6eZMnhCs+BfMRTYkws1o7k
H+bKOskgkI9rgQIDAQAB"
```

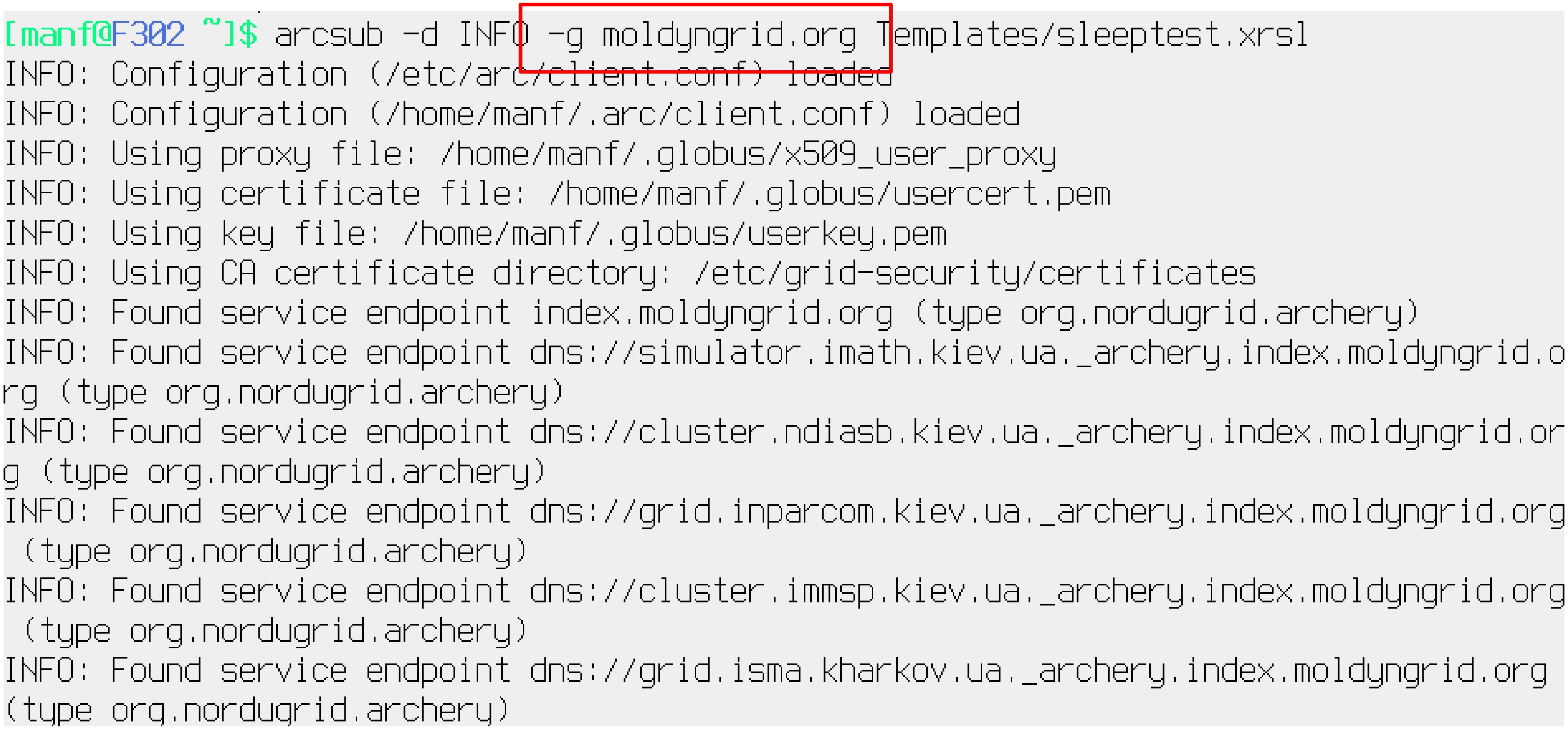
ARCHERY Ecosystem

Choose your side



User side (arcsub)

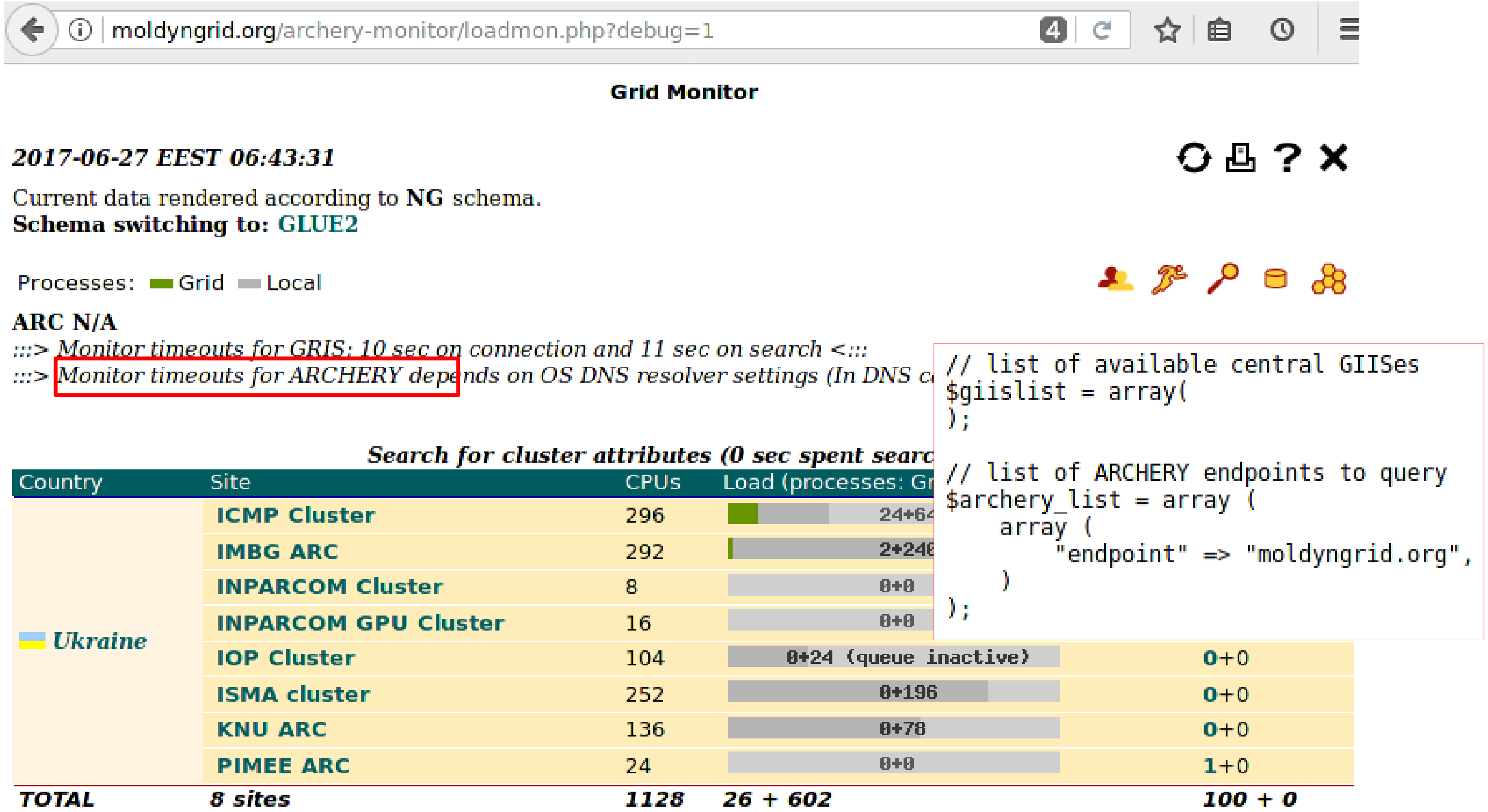
- SER plugin has been implemented and available in Nightlies



```
[manf@F302 ~]$ arcsub -d INFO -g moldyngrid.org Templates/sleeptest.xrsl
INFO: Configuration (/etc/arc/client.conf) loaded
INFO: Configuration (/home/manf/.arc/client.conf) loaded
INFO: Using proxy file: /home/manf/.globus/x509_user_proxy
INFO: Using certificate file: /home/manf/.globus/usercert.pem
INFO: Using key file: /home/manf/.globus/userkey.pem
INFO: Using CA certificate directory: /etc/grid-security/certificates
INFO: Found service endpoint index.moldyngrid.org (type org.nordugrid.archery)
INFO: Found service endpoint dns://simulator.imath.kiev.ua._archery.index.moldyngrid.o
rg (type org.nordugrid.archery)
INFO: Found service endpoint dns://cluster.ndiasb.kiev.ua._archery.index.moldyngrid.or
g (type org.nordugrid.archery)
INFO: Found service endpoint dns://grid.inparcom.kiev.ua._archery.index.moldyngrid.org
 (type org.nordugrid.archery)
INFO: Found service endpoint dns://cluster.immsp.kiev.ua._archery.index.moldyngrid.org
 (type org.nordugrid.archery)
INFO: Found service endpoint dns://grid.isma.kharkov.ua._archery.index.moldyngrid.org
(type org.nordugrid.archery)
```

User side (ldap-monitor)

- Trunk ldap-monitor can be configured to fetch ARCHERY andpoints



Grid Monitor

2017-06-27 EEST 06:43:31

Current data rendered according to **NG** schema.
Schema switching to: GLUE2

Processes: 🟩 Grid ▨ Local

ARC N/A
:::> *Monitor timeouts for GRIS: 10 sec on connection and 11 sec on search* <:::
:::> *Monitor timeouts for ARCHERY depends on OS DNS resolver settings (In DNS c*

Search for cluster attributes (0 sec spent searc

Country	Site	CPUs	Load (processes: Gr	
Ukraine	ICMP Cluster	296	24+64	
	IMBG ARC	292	2+240	
	INPARCOM Cluster	8	0+0	
	INPARCOM GPU Cluster	16	0+0	
	IOP Cluster	104	0+24 (queue inactive)	0+0
	ISMA cluster	252	0+196	0+0
	KNU ARC	136	0+78	0+0
	PIMEE ARC	24	0+0	1+0
TOTAL	***8 sites***	***1128***	***26 + 602***	***100 + 0***

```
// list of available central GIISes
$giislist = array(
);

// list of ARCHERY endpoints to query
$archery_list = array (
    array (
        "endpoint" => "moldyngrid.org",
    )
);
```

Admin side (direct way)

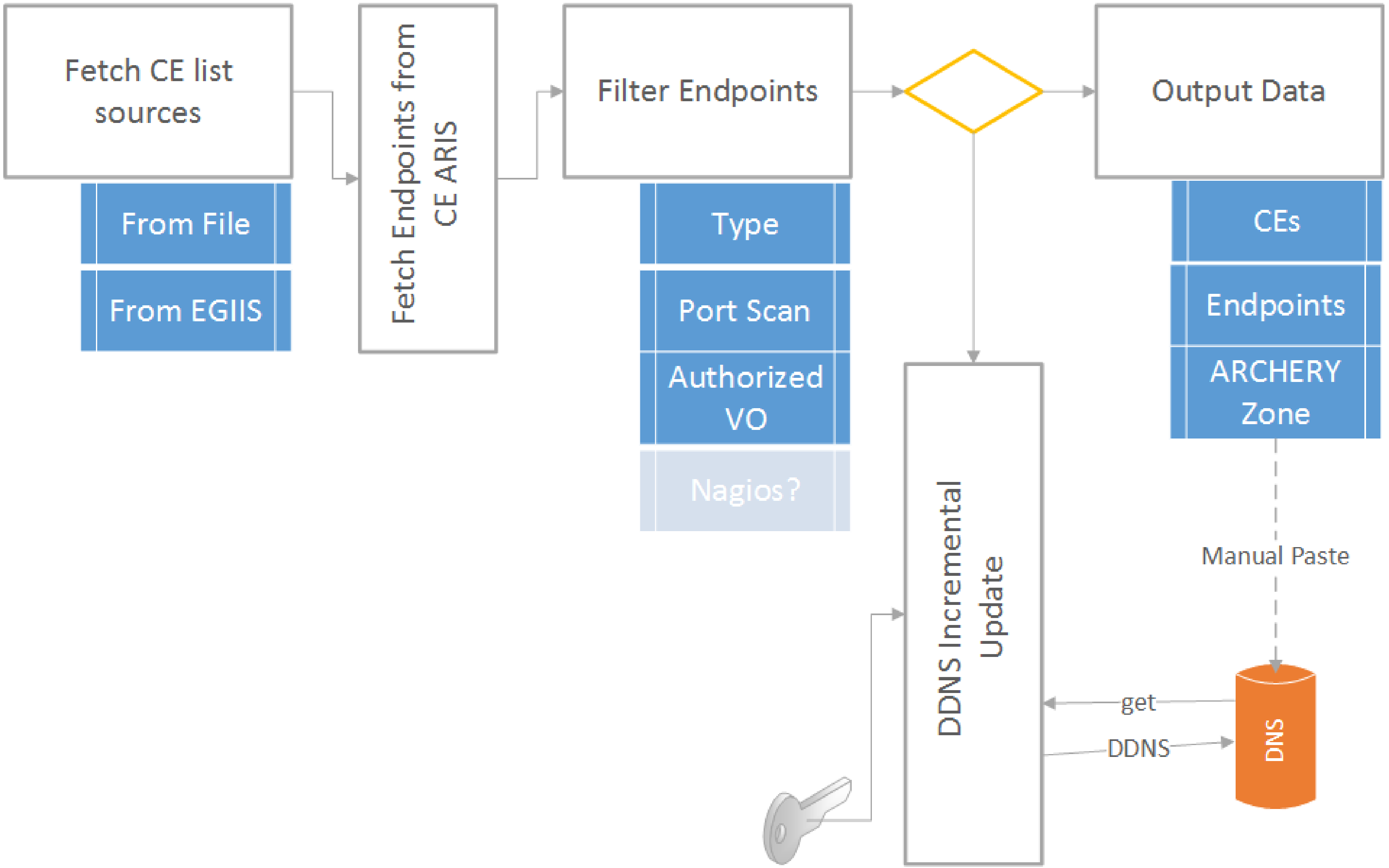
- Have a DNS server and be aware of bind (or whatever you prefer) configuration
- Manually discover endpoints
- Manually create TXT records in zone file
- No much handy but can be used for small setup, especially for index-only

```
_archery         TXT    "u=dns://egiis._archery.nordugrid.org t=org.nordugrid.archery"

_archery         TXT    "u=grid.org.ua t=org.nordugrid.archery"

egiis._archery   TXT    "u=ldap://index1.nordugrid.org:2135/Mds-Vo-
name=NorduGrid,o=grid t=org.nordugrid.ldapegiis"

egiis._archery   TXT    "u=ldap://index2.nordugrid.org:2135/Mds-Vo-
name=NorduGrid,o=grid t=org.nordugrid.ldapegiis"
```

Admin side (archery-manage)

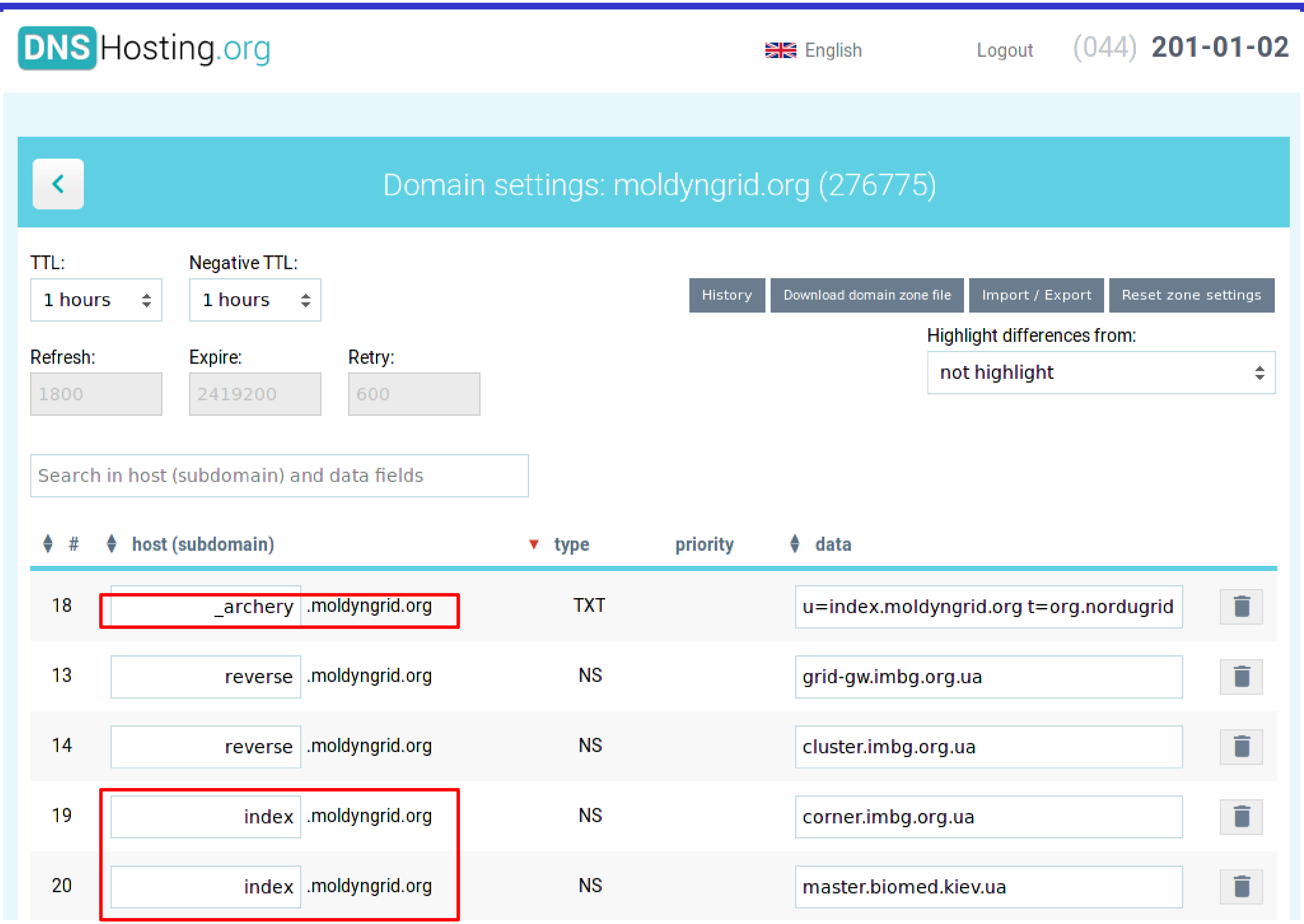
- NOW available in trunk
  - not packaged yet
- Designed to automate ARCHERY records management:
  - Automatically **discover CE endpoints** and their statuses
  - Automatically **create content** of zonefile
  - Capable of **dynamically update zone** via DDNS protocol with TSIG auth
  - Provides **EGIIS migration** capabilities

archery-manage operation



Example: MolDynGrid VO ARCHERY Demo

moldyngrid.org DNS zone



DNSHosting.org

English   Logout   (044) 201-01-02

Domain settings: moldyngrid.org (276775)

TTL: 1 hours

Negative TTL: 1 hours

History | Download domain zone file | Import / Export | Reset zone settings

Highlight differences from: not highlight

Refresh: 1800

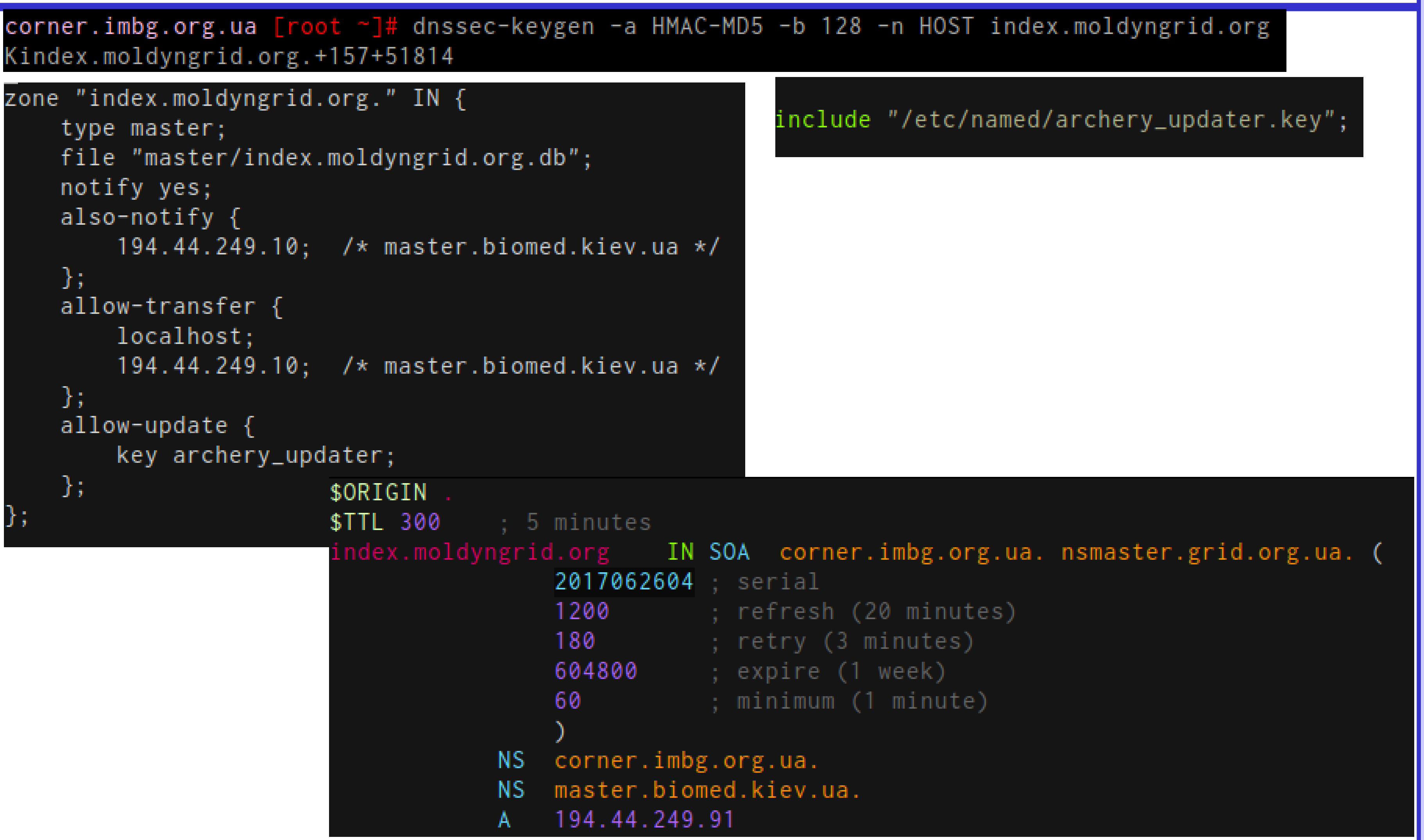
Expire: 2419200

Retry: 600

Search in host (subdomain) and data fields

#	host (subdomain)		type	priority	data
18	_archery	.moldyngrid.org	TXT		u=index.moldyngrid.org t=org.nordugrid
13	reverse	.moldyngrid.org	NS		grid-gw.imbg.org.ua
14	reverse	.moldyngrid.org	NS		cluster.imbg.org.ua
19	index	.moldyngrid.org	NS		corner.imbg.org.ua
20	index	.moldyngrid.org	NS		master.biomed.kiev.ua

index.moldyngrid.org BIND



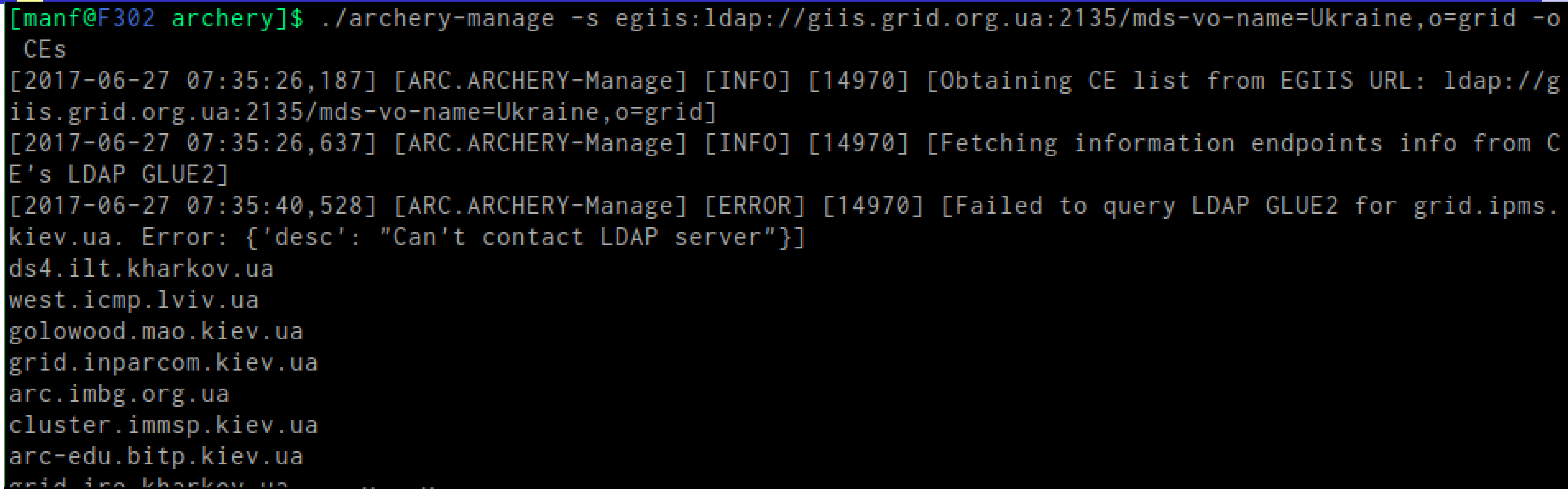
```
corner.imbg.org.ua [root ~]# dnssec-keygen -a HMAC-MD5 -b 128 -n HOST index.moldyngrid.org
Kindex.moldyngrid.org.+157+51814
```

```
zone "index.moldyngrid.org." IN {
    type master;
    file "master/index.moldyngrid.org.db";
    notify yes;
    also-notify {
        194.44.249.10;  /* master.biomed.kiev.ua */
    };
    allow-transfer {
        localhost;
        194.44.249.10;  /* master.biomed.kiev.ua */
    };
    allow-update {
        key archery_updater;
    };
};
```

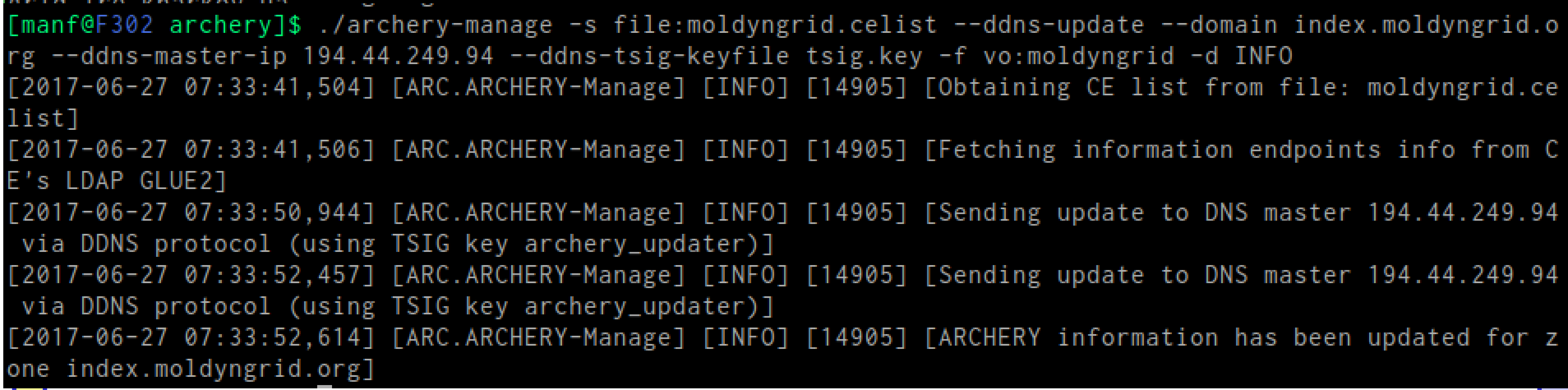
```
include "/etc/named/archery_updater.key";
```

```
$ORIGIN .
$TTL 300      ; 5 minutes
index.moldyngrid.org    IN SOA  corner.imbg.org.ua. nsmaster.grid.org.ua. (
                                2017062604 ; serial
                                1200       ; refresh (20 minutes)
                                180        ; retry (3 minutes)
                                604800     ; expire (1 week)
                                60         ; minimum (1 minute)
                                )
                            NS  corner.imbg.org.ua.
                            NS  master.biomed.kiev.ua.
                            A   194.44.249.91
```

archery-manage



```
[manf@F302 archery]$ ./archery-manage -s egiis:ldap://giis.grid.org.ua:2135/mds-vo-name=Ukraine,o=grid -o
 CEs
[2017-06-27 07:35:26,187] [ARC.ARCHERY-Manage] [INFO] [14970] [Obtaining CE list from EGIIS URL: ldap://g
iis.grid.org.ua:2135/mds-vo-name=Ukraine,o=grid]
[2017-06-27 07:35:26,637] [ARC.ARCHERY-Manage] [INFO] [14970] [Fetching information endpoints info from C
E's LDAP GLUE2]
[2017-06-27 07:35:40,528] [ARC.ARCHERY-Manage] [ERROR] [14970] [Failed to query LDAP GLUE2 for grid.ipms.
kiev.ua. Error: {'desc': "Can't contact LDAP server"}]
ds4.ilt.kharkov.ua
west.icmp.lviv.ua
golowood.mao.kiev.ua
grid.inparcom.kiev.ua
arc.imbg.org.ua
cluster.immsp.kiev.ua
arc-edu.bitp.kiev.ua
grid.ira.kharkov.ua
```



```
[manf@F302 archery]$ ./archery-manage -s file:moldyngrid.celist --ddns-update --domain index.moldyngrid.o
rg --ddns-master-ip 194.44.249.94 --ddns-tsig-keyfile tsig.key -f vo:moldyngrid -d INFO
[2017-06-27 07:33:41,504] [ARC.ARCHERY-Manage] [INFO] [14905] [Obtaining CE list from file: moldyngrid.ce
list]
[2017-06-27 07:33:41,506] [ARC.ARCHERY-Manage] [INFO] [14905] [Fetching information endpoints info from C
E's LDAP GLUE2]
[2017-06-27 07:33:50,944] [ARC.ARCHERY-Manage] [INFO] [14905] [Sending update to DNS master 194.44.249.94
 via DDNS protocol (using TSIG key archery_updater)]
[2017-06-27 07:33:52,457] [ARC.ARCHERY-Manage] [INFO] [14905] [Sending update to DNS master 194.44.249.94
 via DDNS protocol (using TSIG key archery_updater)]
[2017-06-27 07:33:52,614] [ARC.ARCHERY-Manage] [INFO] [14905] [ARCHERY information has been updated for z
one index.moldyngrid.org]
```

FAQ and Discussion

FAQ

- Why ARCHERY is better than static list of endpoints distribution?
  - Users does not need to download and keep in sync endpoints list all will be fetched automatically and cached on many levels
  - ARCHERY transparently provides integrity/resiliency/caching/delegation features
  - VO/Country domain name is all you need to start your work - it is simple and elegant

FAQ (2)

- Isn’t ARCHERY will die like EMIR when development support suddenly stopped for whatever reason?
  - No, ARCHERY is not a service itself! It is an approach for seamless DNS usage so it cannot die for “no more developments” reason.
  - The only code we need to support is a client and archery-manage. Both are simple enough to be bug-fix supported by anyone

Discussion

- **archery-manage** now has a lot of options and some hardcoded values
- **arc.conf for archery-manage?**

```
[archery]
[archery/filter/portscan]
[archery/filter/vo]
[archery/ddns]
[archery/ce:arc.univ.kiev.ua]
```

or

```
[archery-manage/...]
```

Discussion

- Migration plans
- Entry point(s)
- Per-country or some central “static list by phone/e-mail” services

Crazy Followups with DNS

- /etc/vomses to DNS support in client library
  - no need to configure vomses, use domain name instead
- DNSBL for blacklisting
  - one common blacklist based on EGI Nagios testing
  - minimize ARIS LDAP connection delays