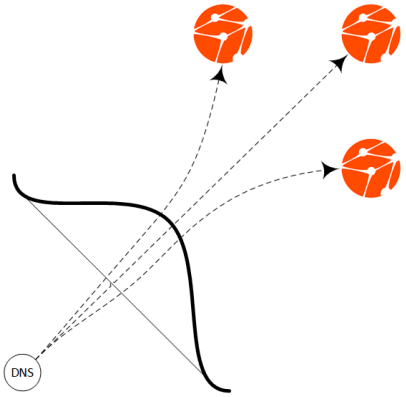

ARCHERY

ARC Hierarchical Endpoints Registry

ARCHITECTURE OVERVIEW

Overview

ARC Hierarchical Endpoints Registry (ARCHERY) is a method of publishing information about available grid resource providers endpoints directly in the DNS using the domain name as an entry point for resource discovery.

An information in the ARCHERY organized in hierarchies at community, country or infrastructure levels. Several registries identified by different domain names can be created on static or dynamic basis. The main entry point for the Nordugrid-wide resource discovery is nordugrid.org.

DNS Features that Empowers ARCHERY

1. Existing DNS infrastructure services of the Internet already established and does not requires dedicated services setup compared to EGIIS or EMIR.
2. DNS provides out-of-the box **reliability** for endpoints discovery (information is replicated).
3. DNS out-of-the box OS-level and network-level **caching** of endpoints provides:
    a. access-time ARCHERY reachability protection
    b. transparent endpoint list updates without any extra tools
    c. minimal load on the endpoint origins (authoritative DNS servers)
    d. registry-defined record cache TTL per each registry entry
4. DNS out-of-the box **delegation** mechanisms allows to distribute registry administration tasks to different people (e.g. country-level registries)
5. Dynamic DNS Update requests [RFC2136] secured with TSIG [RFC 2845] opens the controlled modification of registry content in many automated ways.

From the EGIIS and Static Lists to ARCHERY

ARCHERY can be technically used the same way as EGIISes - it is possible to find and implement the methods and tools to allow clusters to register in appropriate ARCHERY endpoint but **we should not**.

"*Bottom-to-top*" registration approach is not much useful in the production. It involves EGIIS admins to the registration process anyway (to add particular CE to the whitelist). This whitelist is not much different from static list of LDAP endpoints in most production cases but without whitelisting you will be DOSed by public unprotected LDAP write queries.

Moreover successful registration, as turned out from operational side of the EGIIS epoch, does not guarantee CE availability and responsiveness. It is also does not scale well when particular CE needs to register to the different registries when it supports multiple VOs.

"Top-to-bottom" approach with a static list of endpoints is a current approach used by VOs. ARCHERY in DNS is a static list on steroids:

- ARCHERY guaranties **integrity** out-of-the box, compared to the static list distribution (regular download)
- ARCHERY eliminates the need of organizing and updating more files on the client side (you should be already tired with all CA stuff) - an **entry point is a just domain name** of the VO/country/etc.
- As already mentioned ARCHERY allows you **delegate** part of the list management. Imagine how you will be syncing the list from multiple sources in case of static files.
- It provides the way to **make changes rapidly** by means of defining desired TTL for the DNS resource record
- Any dynamic updates to the ARCHERY secured with HMAC signature and there is possible to use native DNSSEC technologies to guarantee information authenticity in ARCHERY.

ARCHERY Components

ARCHERY as a registry itself established on the top of existing DNS infrastructure using the common DNS configuration and records publishing techniques.

To automate ARCHERY records maintaining in DNS zones the `archery-manage` tool is introduced. Taking the static list of endpoints defined in file, archery-manage can query ARIS GLUE2 LDAP, filter records and generate the service endpoint records that will be incrementally updated in ARCHERY by means of dynamic DNS updates secured with TSIG key.

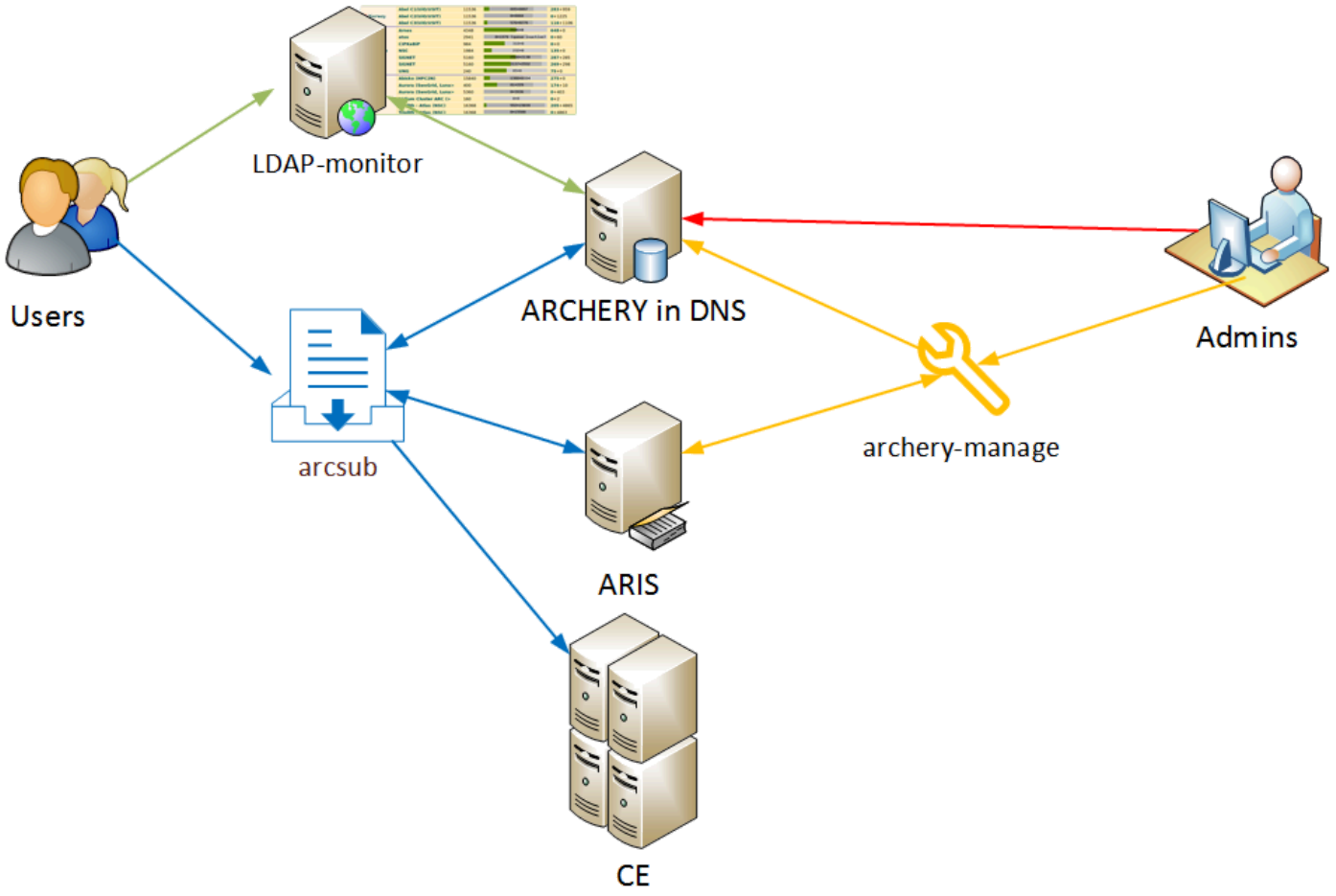

Fig. 1. Components involved in organizing and managing ARCHERY

From the client side, service endpoints retrieval from ARCHERY is included in ARC Client Library and available for transparent usage with corresponding tools, like arcsub or arctest.

Nordugrid Monitor also includes the code for querying ARCHERY.

DNS Records Specifications for ARCHERY

ARCHERY rely on DNS TXT resource record (RR) that holds an endpoint information. The approach is similar to defining SFP [RFC 7208], DKIM [RFC 6376], DMARK [RFC 7489] or simply Kerberos realm.

Distinguishing ARCHERY from the other RRs in DNS

For the each domain used as an entry point to the registry an `_archery` TXT RR SHOULD BE defined.

Defining dedicated RR is inspired by similar implementations mentioned above and open the possibility to delegate this record by means of NS RR to the different DNS authoritative server.

Example: User use `nordugrid.org` domain as an entry point. ARCHERY client SHOULD query `_archery.nordugrid.org`.

General TXT RR format

General record syntax defined in the RFC 1464 and can be summarized as follows:

```
<owner> <class> <ttl> TXT "<attribute name>=<attribute value>"
```

In particular it holds TTL field used by DNS caching routines and key-value defined TXT-DATA.

ARCHERY TXT-DATA format

The general suggested syntax of ARCHERY data stored in TXT RR is:

```
u=<endpoint uri> t=<endpoint type> [s=<endpoint status>]
```

Endpoint URI

Endpoint URI can hold any particular endpoints supported by the ARC client library.

Example: `https://arc.univ.kiev.ua:443/arex`

Endpoint type

Type is a multivalued attribute that declare the protocols used to access this endpoint. All service endpoint types supported by ARC client library can be used. The most relevant information system endpoint types are:

- `org.nordugrid.ldapng`
- `org.nordugrid.ldapglue2`
- `org.ogf.glue.emies.resourceinfo`
- `org.nordugrid.archery` (type used to point to another ARCHERY endpoints)

Endpoint status

Optional argument that MUST BE treated as endpoint availability indicator. Status values are:

- s=1 - active and can be used (default)
- s=0 - inactive and should be skipped by client

Optional status argument allows an ARCHERY admin to temporarily disable the service without removal of the entire TXT RR.

Organizing Endpoints to Hierarchies

DNS Response Limit

Depend on the transport layer protocol DNS response size is limited to 512 or 4096 bytes UDP and 65535 bytes TCP in the ISC Bind and most service implementations.

This is enough space to hold near 500 endpoints in one DNS record, but it will be much better from the caching and manageability point of view to split info between several records, and the most natural and structural way - to organize hierarchy.

Manageability

Nordugrid-wide ARCHERY instance follows the former EGIIS logic and structure endpoints in the following hierarchy: **Entry point -> Country/Project -> Computing Element -> Endpoints**

When setting up dedicated ARCHERY instance for the project/VO out of the common Nordugrid structure it is advised to use archery-manage, that creates **Computing Element -> Endpoints** structure automatically.

TXT Records Format for Making Hierarchies

To split information among several DNS RR owners (in the same or different zones) `org.nordugrid.archery` endpoint type SHOULD BE used as a glue.

Endpoint URIs specified for ARCHERY endpoint type can be specified as:

- `u=grid.org.ua`
  - SHOULD BE treated as an entry point. ARCHERY client will add `_archery` and query `_archery.grid.org.ua` RRSet to obtain further endpoints information.
- `u=dns://arc.univ.kiev.ua._archery.grid.org.ua`
  - SHOULD BE treated as an exact DNS RRSet pointer. Client will query `arc.univ.kiev.ua`._archery.grid.org.ua RRset directly

The archery-manage tool

The archery-manage is designed to simplify common ARCHERY administrator operations, including the registry initial bootstrap, migration from EGIIS and keeping information up to date in the registry in the most transparent way.

Managing ARCHERY with archery-manage

Typical workflow for managing ARCHERY with the archery-manage is the following:

- ARCHERY admin maintaining static list of CE hostnames
  - It is simple (compared to writing records in DNS zone)
  - It does not require deep DNS knowledge
- ARCHERY admin run `archery-manage` than uses hostnames from the list and:
  - query CE ARIS
  - collect all available CE endpoints
  - optionally filter endpoints (for example by type or supported VO)
  - send incremental updates to ARCHERY by means of DDNS protocol with TSIG authorization
- CE querying with archery-manage can be established on regular basis (by means of e.g. cron job) to keep information up to date

Archery-manage operations flow

The operations flow of archery-manage shown on Fig. 2.

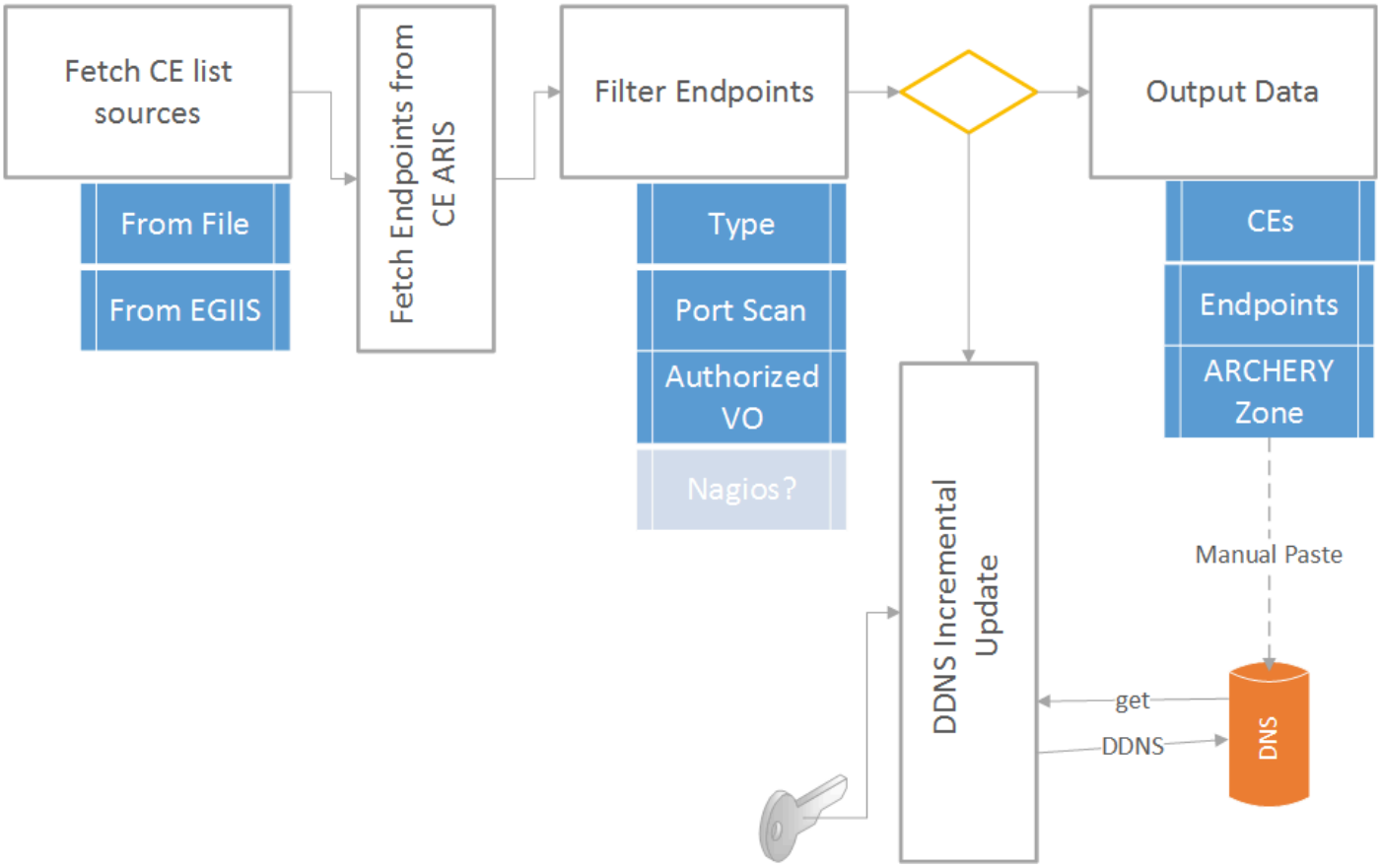

Fig. 2. The archery-manage operation flow

It starts with CE list parsing, than query CE ARIS for available endpoints and their statuses, optionally apply filters and output data to stdout or send incremental update to DNS directly.

The supported CE list sources are **file** and **egiis.** The second can be used for migration purposes and the implied usage is to dump CE list from EGIIS to file:

```
archery-manage -s egiis:ldap://index1.nordugrid.org:2135/Mds-Vo-Name=Nordugrid,o=grid \
               -s egiis:ldap://index2.nordugrid.org:2135/Mds-Vo-Name=Nordugrid,o=grid \
               -s egiis:ldap://index3.nordugrid.org:2135/Mds-Vo-Name=Nordugrid,o=grid \
               -s egiis:ldap://index4.nordugrid.org:2135/Mds-Vo-Name=Nordugrid,o=grid \
               -o CEs > all.celist
```

Filters are extensible by design, the current archery-manage implementation supports filtering by endpoint types, port availability and CE authorized VOs. For example, following command will output all LDAP GLUE2 resource information endpoints that supports MolDynGrid VO:

```
archery-manage -s file:all.celist  -f type:org.nordugrid.ldapglue2  -f vo:moldyngrid -o
endpoints
```

There are different options to format output, including already shown list of CEs, list of endpoints. It is possible to output endpoints in the DNS zonefile format or use JSON output modifier.

The most powerful part of `archery-manage` is DDNS updates that makes whole ARCHERY operations transparent and eliminates the DNS configuration manual changes. Admin need to supply necessary

ARCHERY master DNS server parameters along with TSIG key and archery-manage will do the rest. The following command publishes all EMI ES Resource Info endpoints to the moldyngrid.org registry:

```
archery-manage -s file:moldyngrid.celist -f type:org.ogf.glue.emies.resourceinfo \
              --ddns-update --ddns-tsig-keyfile archery.key \
              --domain index.moldyngrid.org --ddns-master-ip 194.44.249.94
```

FAQ

1. 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
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. The client is pretty simple and can be bug-fix supported by anyone. The archery-manage tool is a bit more complex, but still share the simplicity of LDAP and DNS queries.