Advanced Globus Deployment for System Administrators

Vas Vasiliadis
Rachana Ananthakrishnan

GlobusWorld
April 21, 2016
Presentation material available at

globusworld.org/tutorial2016
Agenda

• Managed endpoints and subscriptions
• Controlling access
• Authentication and endpoint activation
• Optimizing transfer performance
• Advanced endpoint configuration
• Deployment scenarios
Managed endpoints and subscriptions
Creating managed endpoints

- **Required** for sharing, management console, reporting, etc.

- **Convert existing endpoint to managed:**
  
  ```
  endpoint-modify --managed-endpoint <endpoint_name>
  ```

- **Must be run by subscription manager, using the Globus CLI**

- **Important:** Re-run endpoint-modify after deleting/re-creating endpoint
Subscription configuration

- **Subscription manager**
  - Create/upgrade managed endpoints
  - Requires Globus ID linked to Globus account

- **Management console permissions**
  - Independent of subscription manager
  - Map managed endpoint to Globus ID

- **Globus Plus group**
  - Subscription Manager is admin
  - Can grant admin rights to other members
Using the Management Console

- Monitor all transfers
- Pause/resume specific transfers
- Add pause conditions with various options
- Resume specific tasks overriding pause conditions
- Cancel tasks
Authentication and Endpoint Activation
Integrating your Campus IdP

• **InCommon members**
  – Must release R&S attributes to CILogon
  – Mapping uses ePPN; can use GridMap
    AuthorizationMethod = CILogon
    CILogonIdentityProvider = 
      <institution_name_in_CILogon_IdP_list>

• **Non-members**
  – IdP must support OpenID Connect
  – Requires Alternate IdP subscription

• **Using an existing MyProxy server**
Optimizing transfer performance
Network Use Parameters

• Concurrency and parallelism configuration to tune transfers
• Maximum and Preferred
• Use values set for source and destination to determine parameters for a given transfer
• min (max (preferred src, preferred dest), max src, max dest)
Network paths

- Separate control and data interfaces
- "DataInterface=" option in globus-connect-server-conf
- Common scenario: route data flows over Science DMZ link
Globus Network Manager

- Information from GridFTP to facilitate dynamic network changes
- Callbacks during GridFTP execution on local DTN
- Supplements information available via Globus transfer API
Globus Network Manager Callbacks

- Pre-listen (binding of socket)
- Post-listen
- Pre-accept/Pre-connect (no Data yet)
- Post-accept/Post-connect (data in flight)
- Pre-close
- Post-close
Network manager use cases

- **Science DMZ Traffic Engineering**
  - Use SDN to dynamically route data path
  - Control path uses traditional route

- **Automated WAN bandwidth reservation**
  - OSCARS, AL2S

- **Note: All this requires custom code**
Advanced Endpoint Configuration
Path Restriction

• Default configuration:
  – All paths allowed, access control handled by the OS

• Use `RestrictPaths` to customize
  – Specifies a comma separated list of full paths that clients may access
  – Each path may be prefixed by `R` (read) and/or `W` (write), or `N` (none) to explicitly deny access to a path
  – `~` for authenticated user’s home directory, and `*` may be used for simple wildcard matching.

• e.g. Full access to home directory, read access to `/data`:
  – `RestrictPaths = RW~,R/data`

• e.g. Full access to home directory, deny hidden files:
  – `RestrictPaths = RW~,N~/.*`
Limit sharing to specific accounts

• `SharingUsersAllow` =
• `SharingGroupsAllow` =
• `SharingUsersDeny` =
• `SharingGroupsDeny` =
Sharing Path Restriction

• Restrict paths where users can create shared endpoints
• Use `SharingRestrictPaths` to customize
  – Same syntax as `RestrictPaths`
• e.g. Full access to home directory, deny hidden files:
  – `SharingRestrictPaths = RW~,N~/.*`
• e.g. Full access to public folder under home directory:
  – `SharingRestrictPaths = RW~/public`
• e.g. Full access to `/proj`, read access to `/scratch`:
  – `SharingRestrictPaths = RW/proj,R/scratch`
Access Manager

• Allow others to manage access to a shared endpoint
• Owner of shared endpoint can set role
• Assignable to user or group
• Common Use Case: Data distribution
Encryption

• Requiring encryption on an endpoint
• FIPS-140-2 compliance
  – Limit number of ciphers used by OpenSSL
  – https://access.redhat.com/solutions/137833
Deployment Scenarios
Distributing Globus Connect Server components

- **Globus Connect Server components**
  - `globus-connect-server-io`, `-id`, `-web`
- **Default**: `-io` and `-id` (no `-web`) on single server
- **Common options**
  - Multiple `-io` servers for load balancing, failover, and performance
  - No `-id` server, e.g. third-party IdP such as CILogon
  - `-id` on separate server, e.g. non-DTN nodes
  - `-web` on either `-id` server or separate server for OAuth interface
Setting up multiple –io servers

- **Guidelines**
  - Use the same .conf file on all servers
  - First install on the server running the –id component, then all others

1. **Install Globus Connect Server on all servers**
2. **Edit .conf file on one of the servers and set [MyProxy] Server to the hostname of the server you want the –id component installed on**
3. **Copy the configuration file to all servers**
   - `/etc/globus-connect-server.conf`
4. **Run `globus-connect-server-setup` on the server running the –id component**
5. **Run `globus-connect-server-setup` on all other servers**
6. **Repeat steps 2-5 as necessary to update configurations**
Enable your storage system

- **Signup:** [globus.org/signup](https://globus.org/signup)
- **Create endpoint:** [globus.org/globus-connect-server](https://globus.org/globus-connect-server)
- **Need help?** [support.globus.org](https://support.globus.org)
- **Subscribe to help us make Globus self-sustaining:** [globus.org/provider-plans](https://globus.org/provider-plans)
- **Follow us:** [@globusonline](https://twitter.com/globusonline)