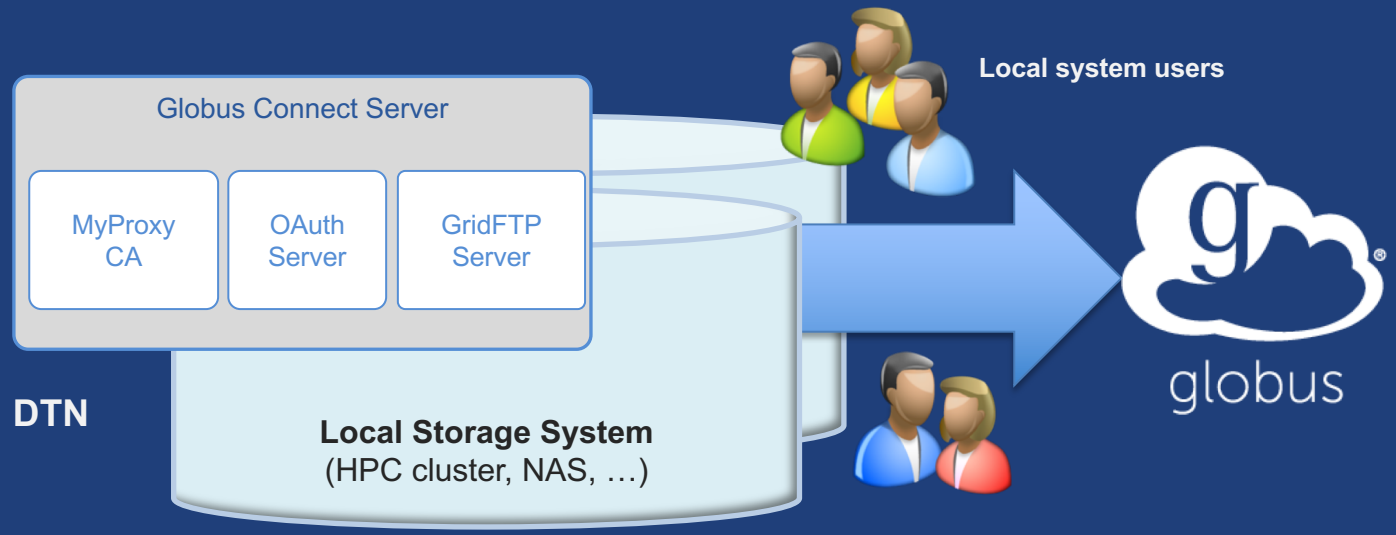
Globus Endpoints Administration

Vas Vasiliadis
vas@uchicago.edu

globus

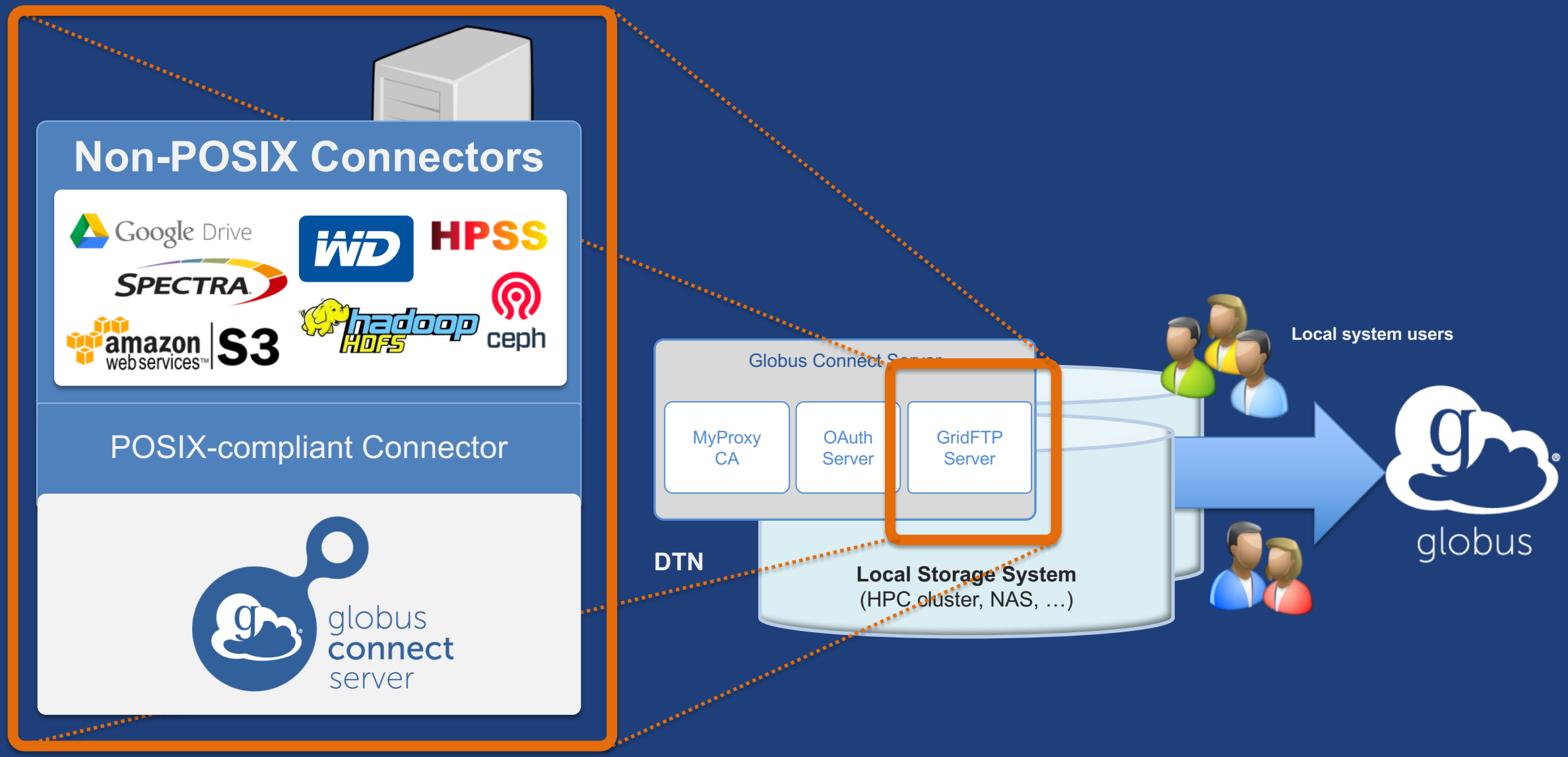
Globus Connect Server

- **Makes your storage accessible via Globus**
- **Multi-user server, installed and managed by sysadmin**
- **Default access for all local accounts**
- **Native packaging Linux: DEB, RPM**



docs.globus.org/globus-connect-server-installation-guide/

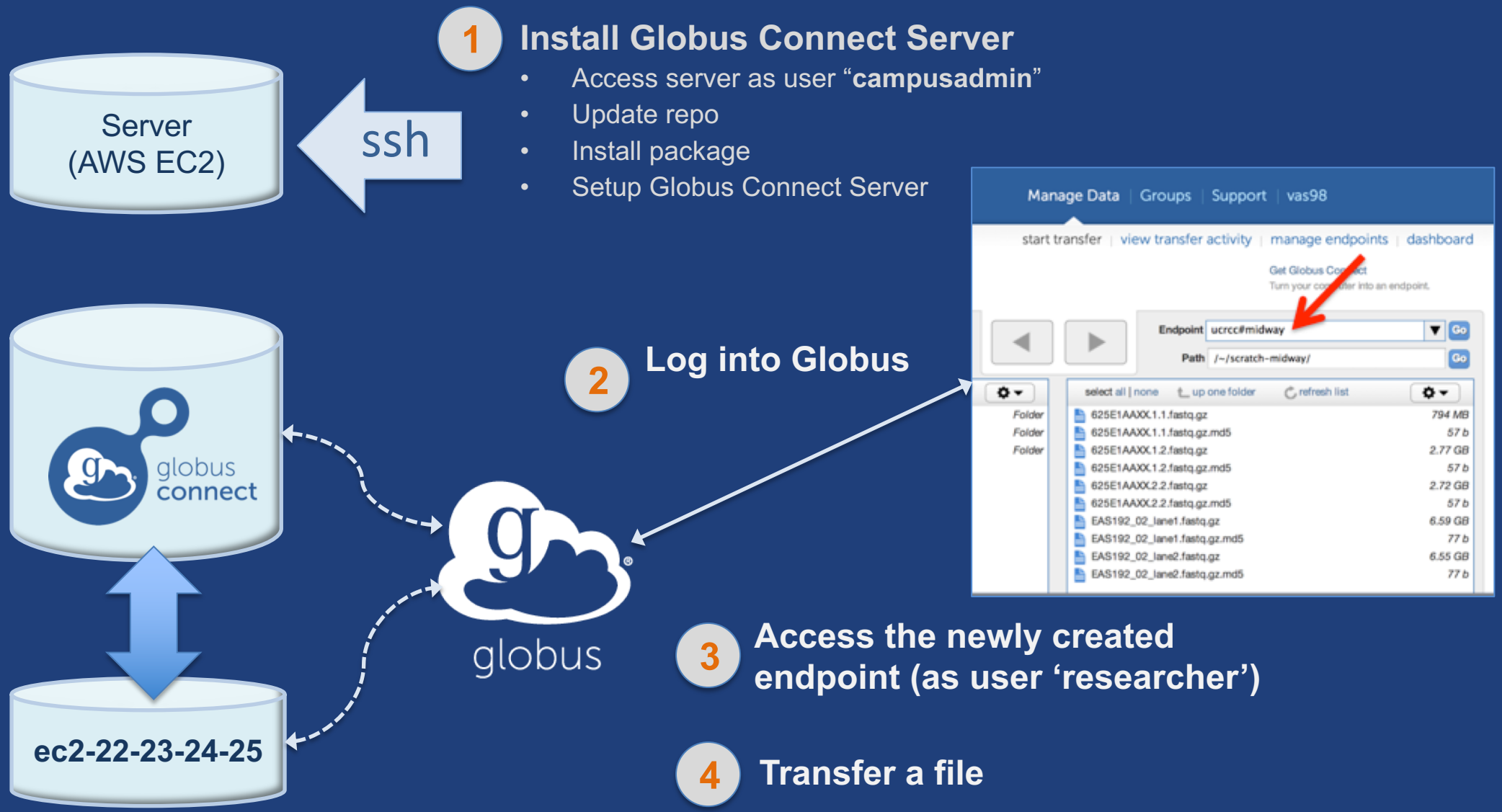
Globus Connect Server



Creating a Globus endpoint on your server

- **In this example, Server = Amazon EC2 instance**
- **Installation and configuration of Globus Connect Server requires a Globus ID**
- **Go to `globusid.org`**
- **Click “`create a Globus ID`”**
  - Optional: associate it with your Globus account

Endpoint installation walkthrough



1 Install Globus Connect Server

- Access server as user "**campusadmin**"
- Update repo
- Install package
- Setup Globus Connect Server

2 Log into Globus

3 Access the newly created endpoint (as user 'researcher')

4 Transfer a file

If you're following along…

- **Get the IP address for your EC2 server**
- **Log in as user 'campusadmin':**

```
ssh campusadmin@<EC2_instance_IP_address>
```

- **NB: Please** `sudo su` **before continuing**
  - User 'campusadmin' has sudo privileges

Globus Connect Server installation commands

```
$ sudo su
$ curl -LOs http://toolkit.globus.org/ftppub/globus-
connect-server/globus-connect-server-
repo_latest_all.deb
$ dpkg -i globus-connect-server-repo_latest_all.deb
$ apt-get update
$ apt-get -y install globus-connect-server
$ globus-connect-server-setup
```

↳ **Use your Globus ID username/password when prompted**

You have a working Globus endpoint!

Accessing our shiny, new Globus endpoint

- **Go to Manage Data → Transfer Files**
- **Access the endpoint we just created**
  - Search for your EC2 host name in the Endpoint field
  - Log in as user “researcher”; we see the user’s home directory
- **Transfer files to verify the endpoint works**
  - Use Globus Tutorial Endpoints or ESnet Read Only Test DTNs

Configuring Globus Connect Server

Endpoint configuration

- **Globus service “Manage Endpoints” page**
- **DTN (Globus Connect Server) config**
  `/etc/globus-connect-server.conf`
  - Standard .ini format: `[Section] Option = Value`
  - To enable changes you must run:
    `globus-connect-server-setup`
  - “Rinse and repeat”

Common configuration options

- **Manage Endpoints page**
  - Display Name
  - Visibility
  - Encryption
- **DTN configuration file – common options:**
  - RestrictPaths
  - IdentityMethod (CILogon, Oauth)
  - Sharing
  - SharingRestrictPaths

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~/.*

Enabling sharing on an endpoint

- **In config file, set** `Sharing=True`
- Run `globus-connect-server-setup`

* Note: Creation of shared endpoints requires a Globus subscription for the managed endpoint

- **Use Globus web app or CLI to flag as managed endpoint (associate the endpoint with a subscription)**

Limit sharing to specific local accounts

- `SharingUsersAllow =`
  - List of local user accounts that can create shared endpoints
- `SharingGroupsAllow =`
  - List of local groups that can create shared endpoints
- `SharingUsersDeny =`
  - List of local users barred from creating shared endpoints
- `SharingGroupsDeny =`
  - List of local groups barred from creating shared endpoints

Sharing Path Restriction

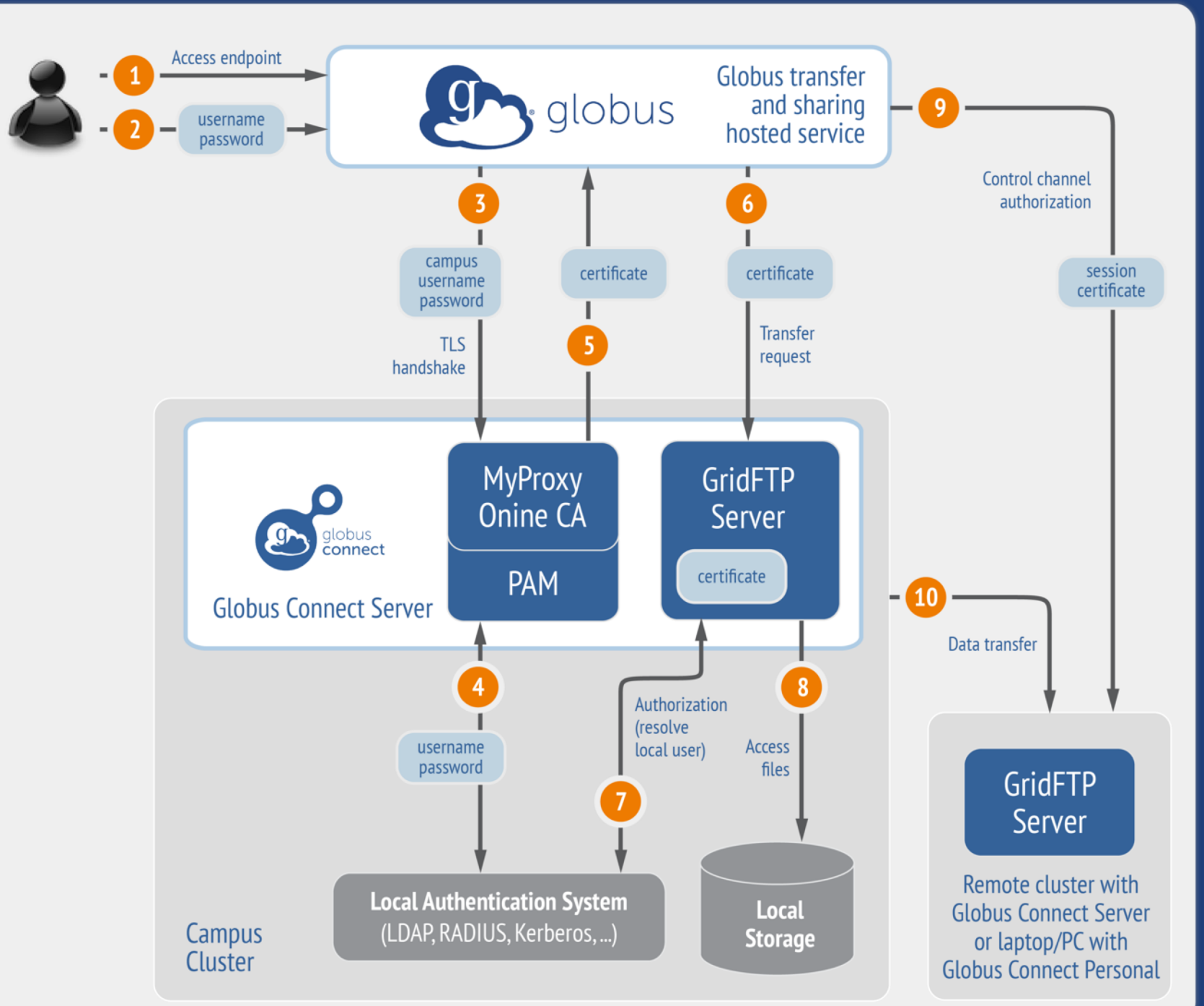
- **Restrict paths where users can create shared endpoints**
- **Use `SharingRestrictPaths` to customize**
  - Same syntax as `RestrictPaths`
- **e.g. Full access to home directory, deny hidden files:**
  - `SharingRestrictPaths = RW~,N~/.*`
- **e.g. Full access to public folder under home directory:**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

Accessing Endpoints

Ports needed for Globus

- **Inbound: 2811 (control channel)**
- **Inbound: 7512 (MyProxy), 443 (OAuth)**
- **Inbound: 50000-51000 (data channel)**
- **If restricting outbound connections, allow connections on:**
  - 80, 2223 (used during install/config)
  - 50000-51000 (GridFTP data channel)

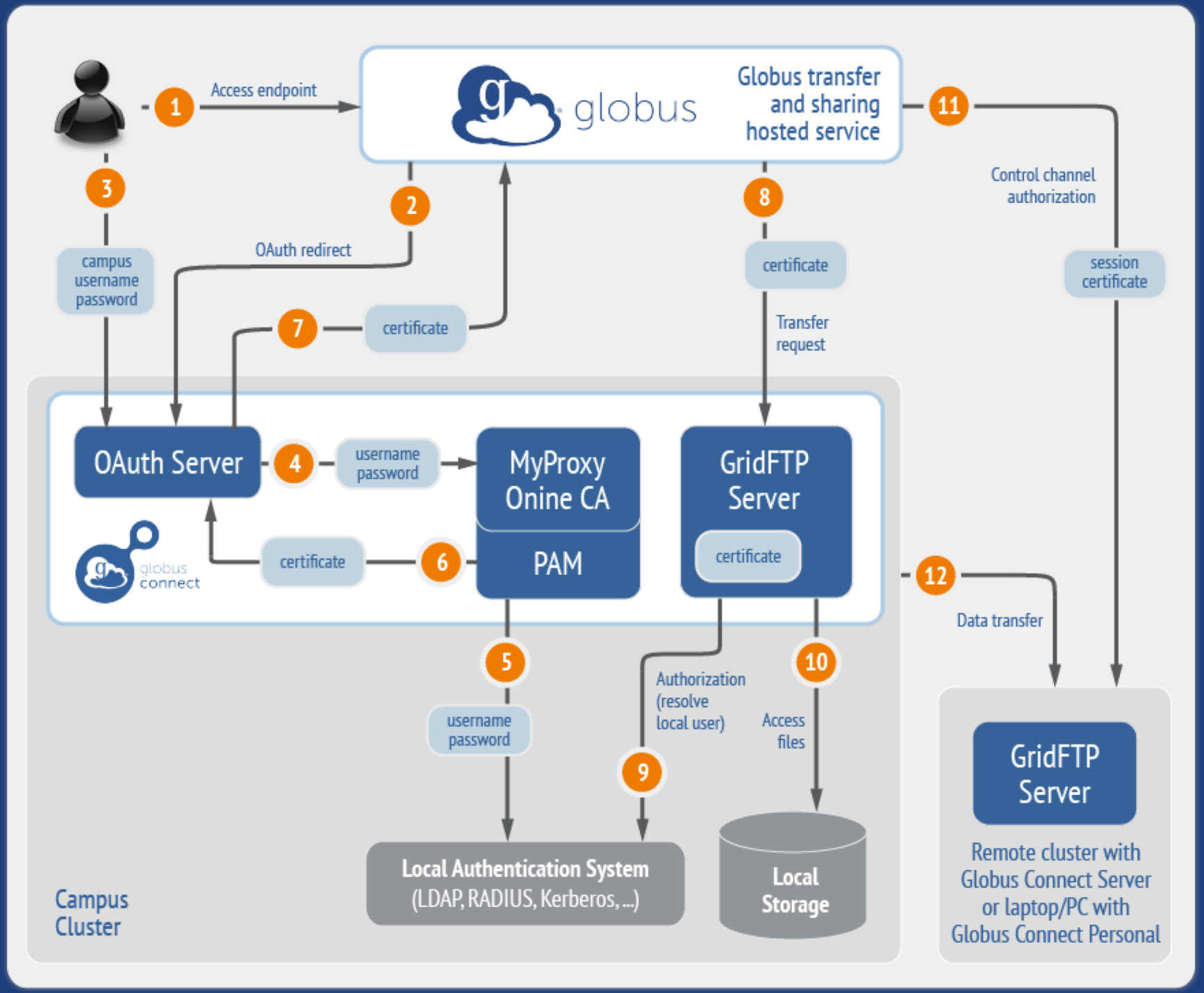
Endpoint activation using MyProxy



Default configuration

(*avoid if at all possible*)

Endpoint activation using MyProxy OAuth



Best practice configuration

Single Sign-On with InCommon/CILogon

- **Your Shibboleth server must release R&S attributes to CILogon—especially the ePPN attribute**
- **Local resource account names must match your institutional ID (InCommon ID)**
- **In** `/etc/globus-connect-server.conf` **set:**

```
AuthorizationMethod = CILogon

CILogonIdentityProvider =
<institution_listed_in_CILogon_IdP_list>
```

Managed endpoints and subscriptions

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

Creating managed endpoints

- **Required for sharing, management console, reporting, …**
- **Convert existing endpoint to managed via CLI (or web):**

```
globus endpoint update --managed <endpt_uuid>
```

- **Must be run by subscription manager**
- **Important: Re-run `endpoint update` after deleting/re-creating endpoint**

Monitoring and managing Globus endpoint activity

Management console

- **Monitor all transfers**
- **Pause/resume specific transfers**
- **Add pause conditions with various options**
- **Resume specific tasks overriding pause conditions**
- **Cancel tasks**
- **View sharing ACLs**

Endpoint Roles

- **Administrator**: define endpoint and roles
- **Activity Manager**: perform control tasks
- **Activity Monitor**: view activity
- **Access Manager**: manage permissions

Demonstration:
Management console
Endpoint Roles
Usage Reporting

…on performance

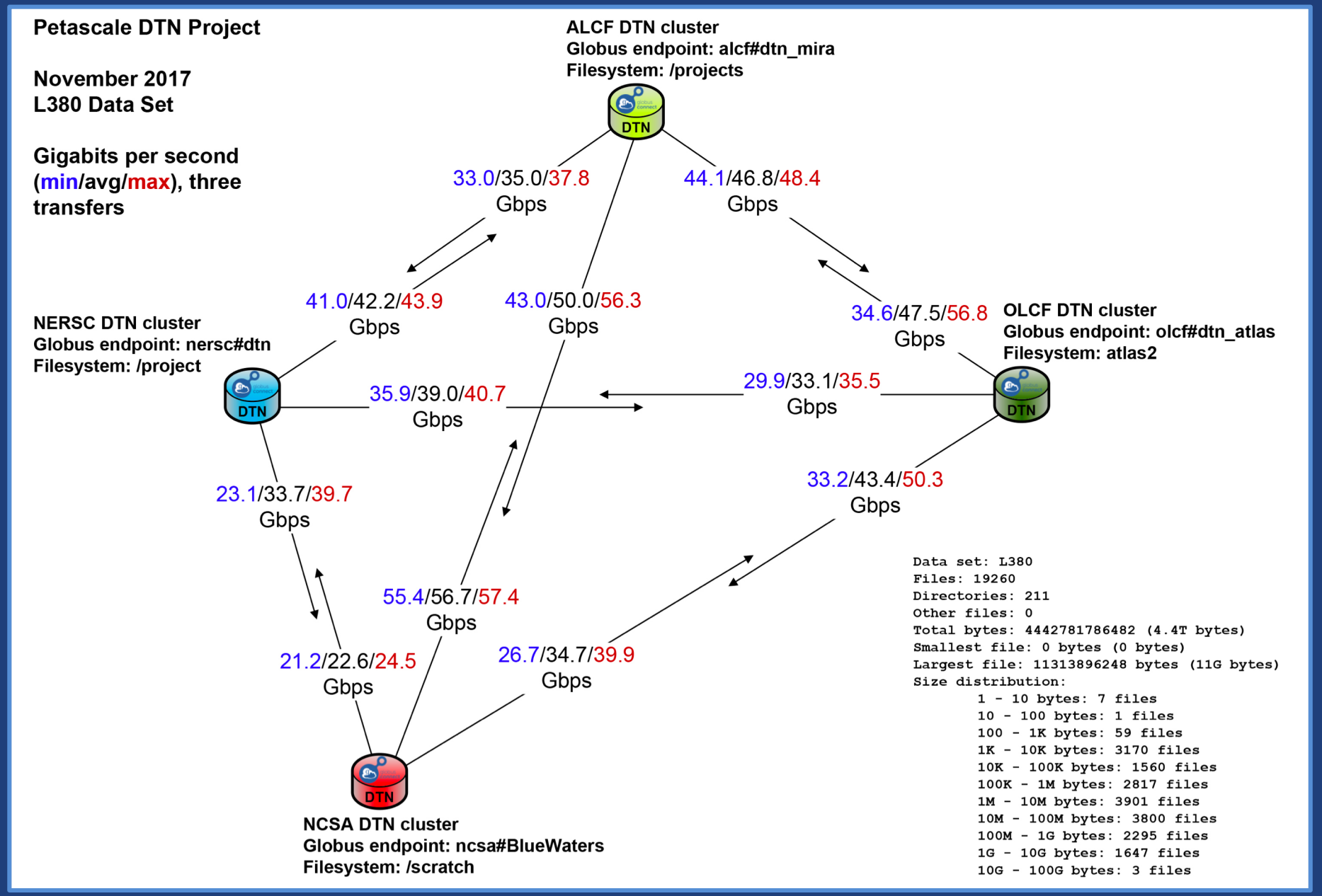
Balance: performance - reliability

- **Network use parameters: concurrency, parallelism**
- **Maximum, Preferred values for each**
- **Transfer considers source and destination endpoint settings**

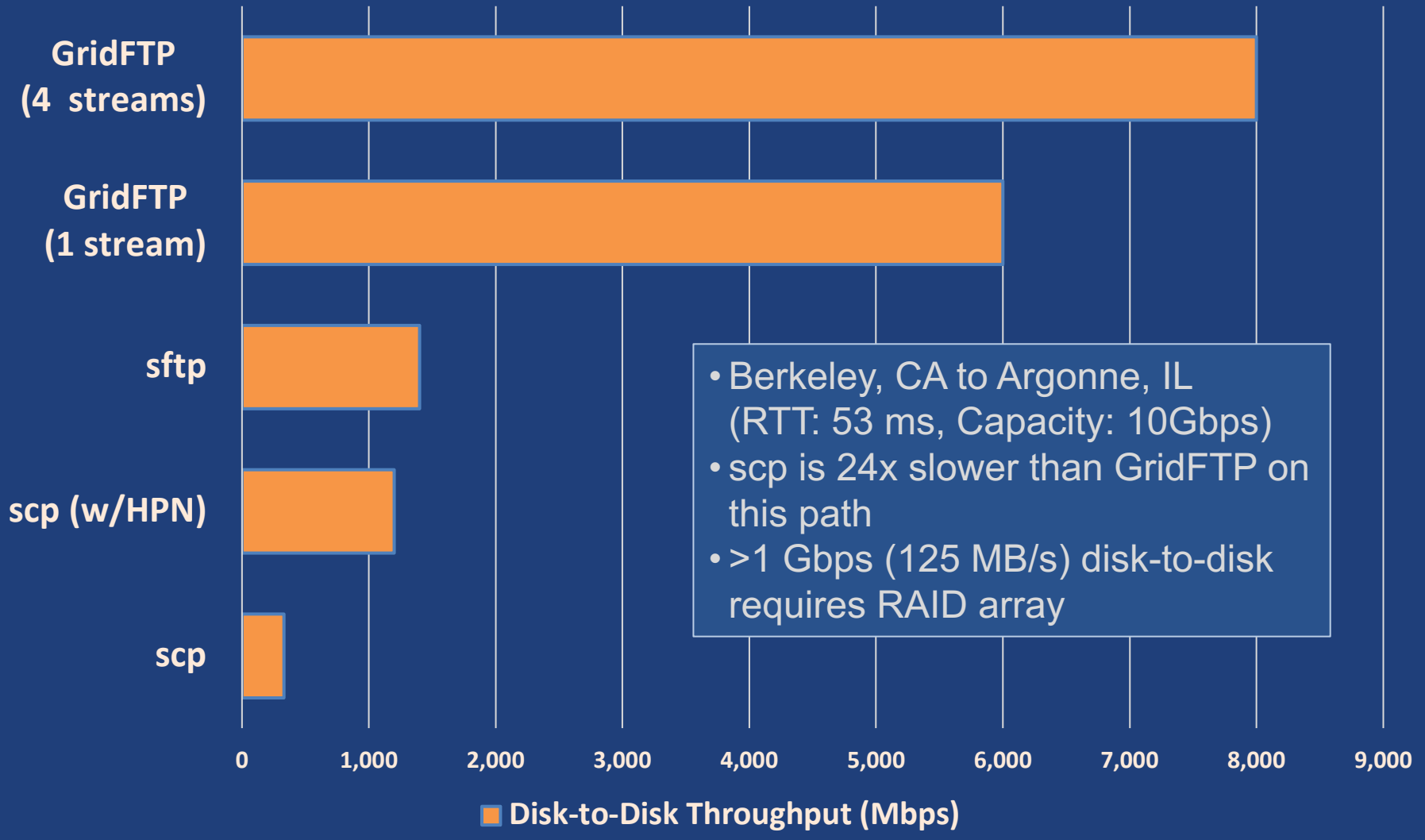
```
min(
    max(preferred src, preferred dest),
    max src,
    max dest
)
```

- **Service limits, e.g. concurrent requests**

Illustrative performance



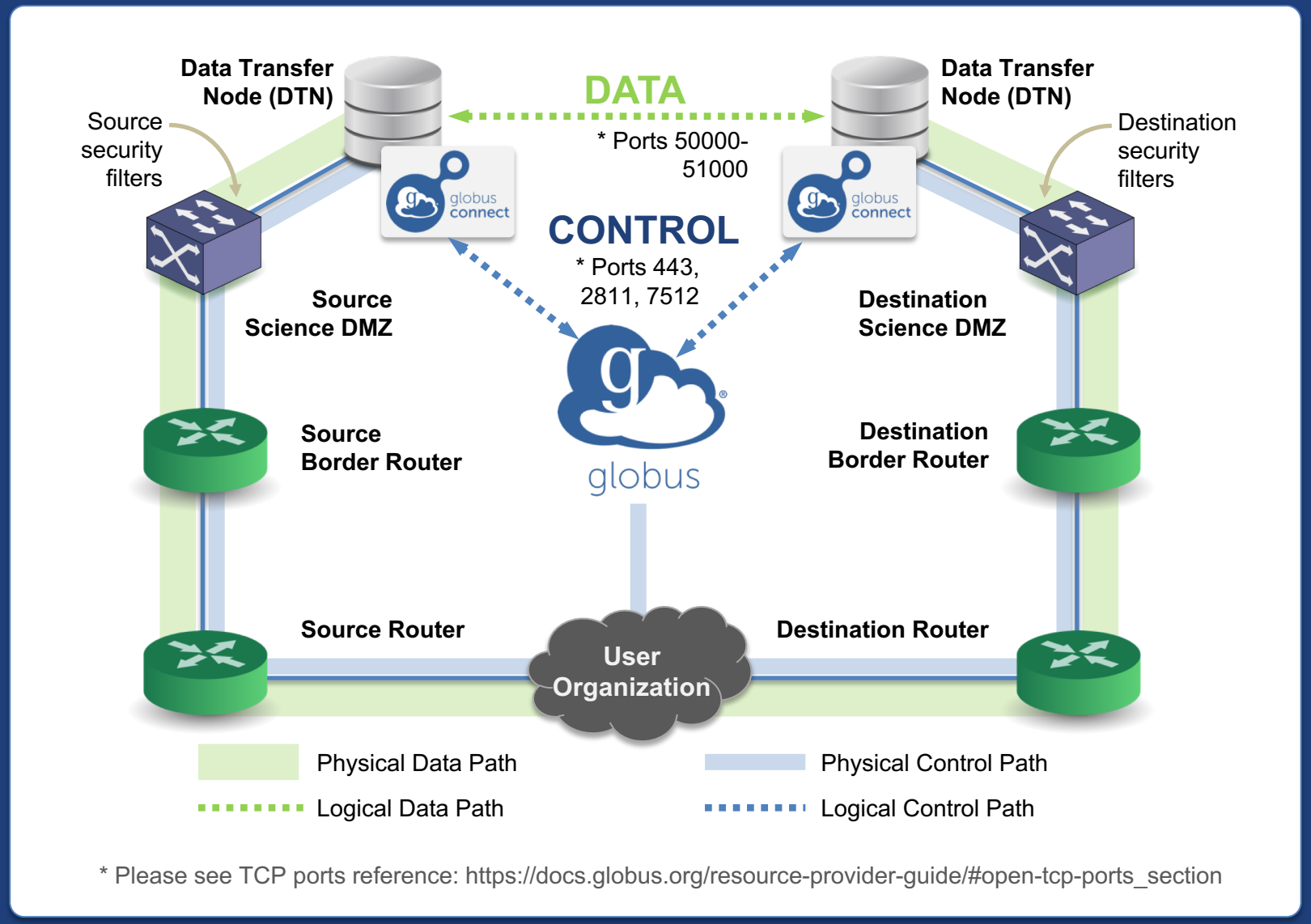
Disk-to-Disk Throughput: ESnet Testing



Source: ESnet (2016)

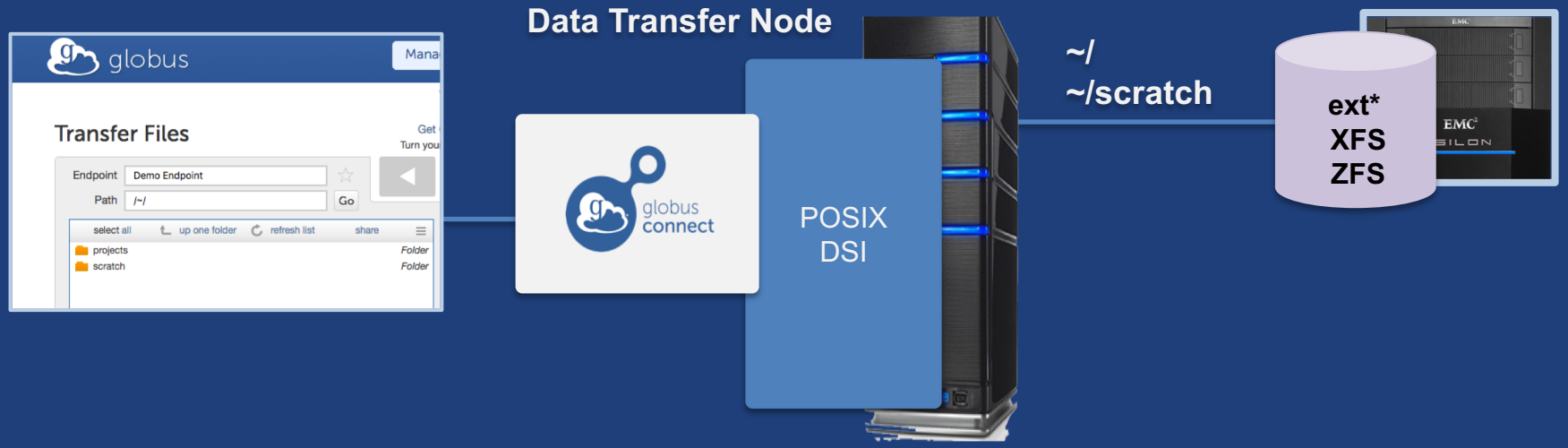
Deployment Scenarios

Best practice network configuration

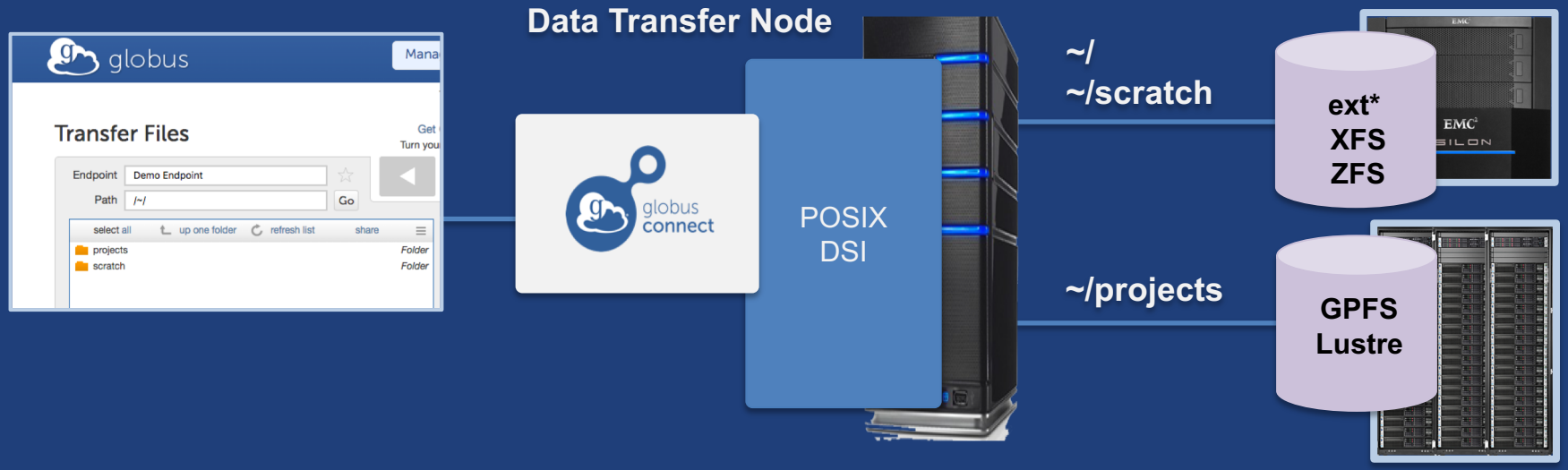


* Please see TCP ports reference: https://docs.globus.org/resource-provider-guide/#open-tcp-ports_section

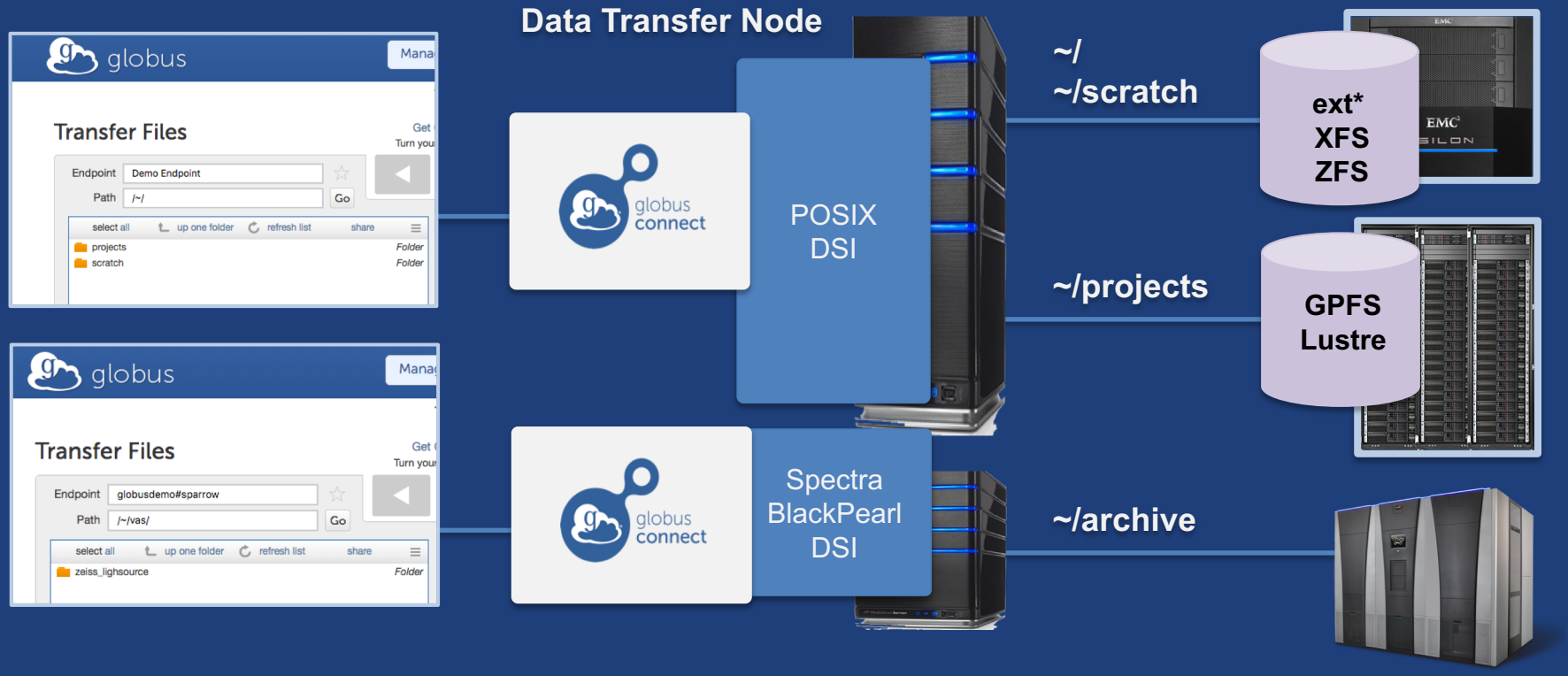
Multi-endpoint configuration



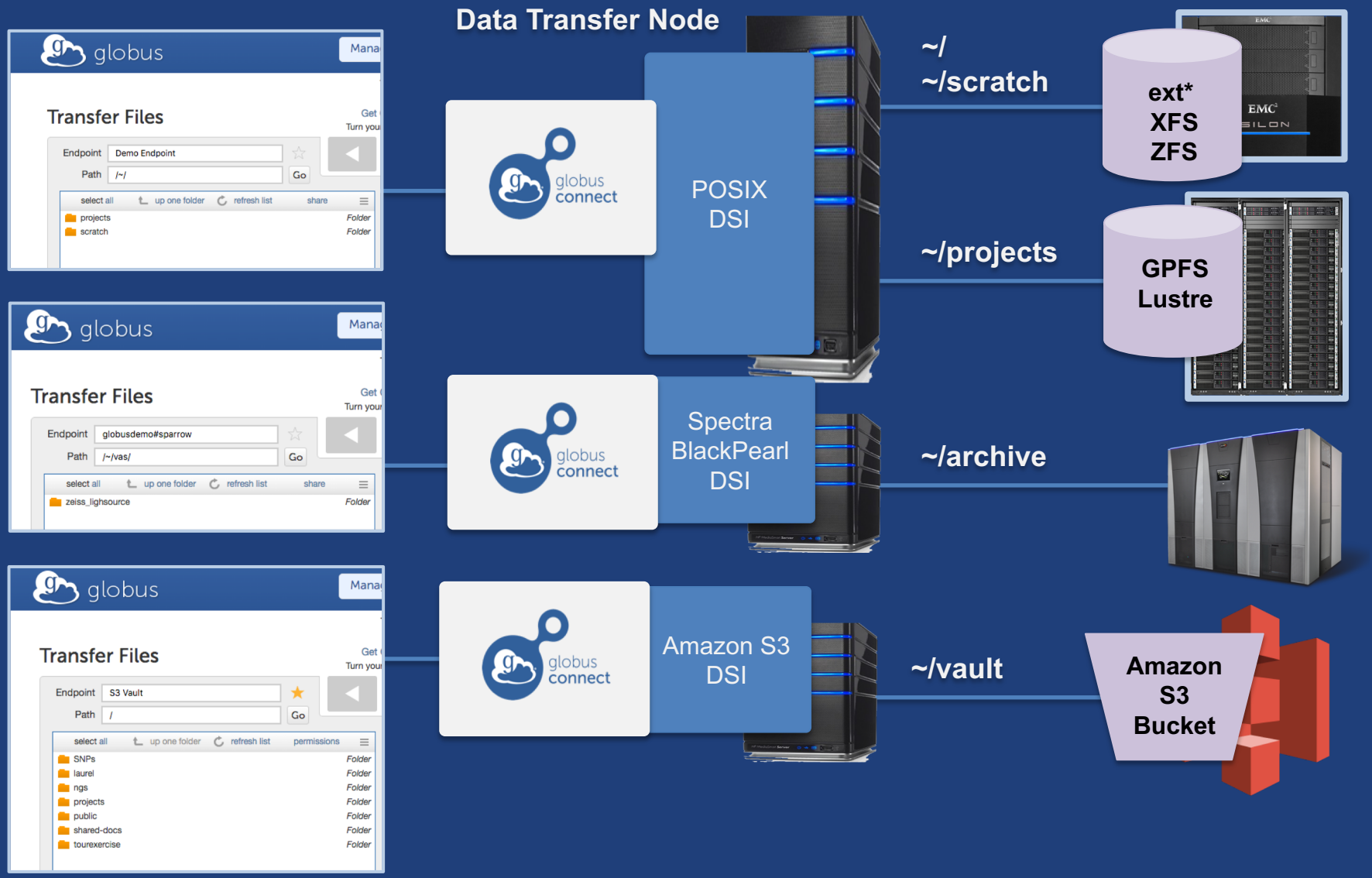
Multi-endpoint configuration



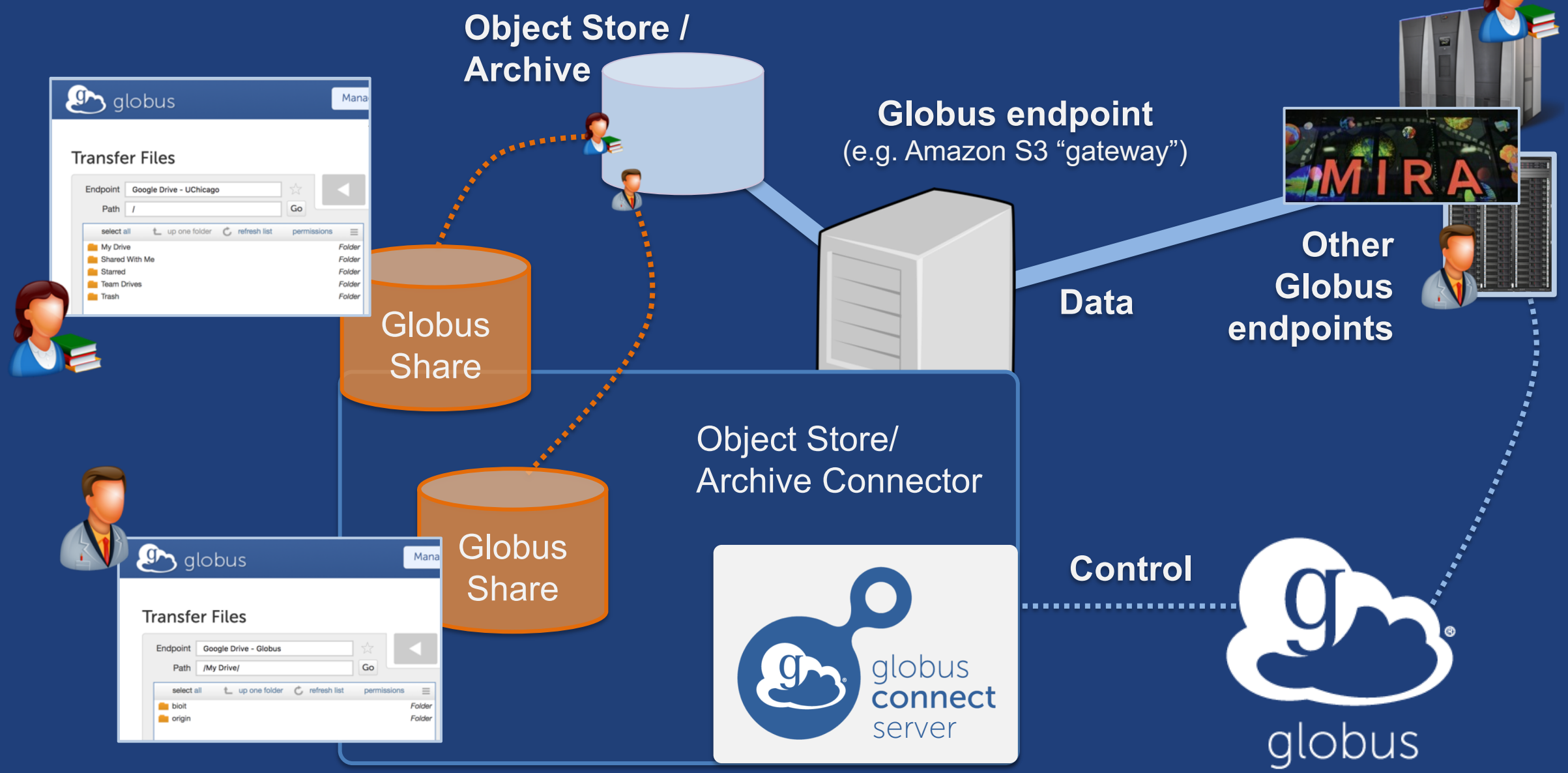
Multi-endpoint configuration



Multi-endpoint configuration

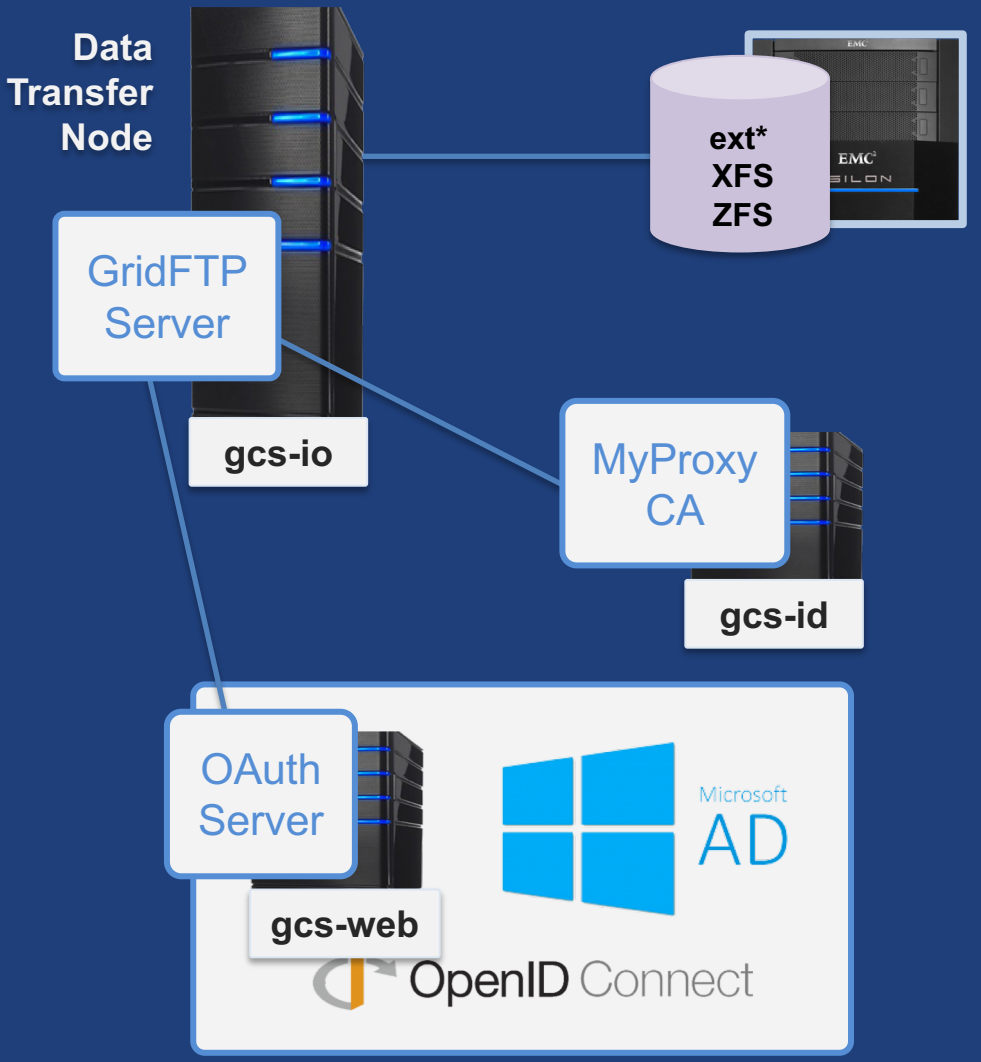


Deploying a Globus connector gateway



Other Deployment Options

Distributing Globus Connect Server components



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
- **Install Globus Connect Server on all servers**
- **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**
- **Copy the configuration file to all servers**
  - /etc/globus-connect-server.conf
- **Run globus-connect-server-setup on the server running the –id component**
- **Run globus-connect-server-setup on all other servers**
- **Repeat steps 2-5 as necessary to update configurations**

Example: Two-node DTN

-id
-io


On “primary” DTN node (34.20.29.57):

/etc/globus-connect-server.conf

```
[Endpoint] Name = globus_dtn
[MyProxy] Server = 34.20.29.57
```

-io


On other DTN nodes:

/etc/globus-connect-server.conf

```
[Endpoint] Name = globus_dtn
[MyProxy] Server = 34.20.29.57
```

Open Discussion