



# Globus for High Assurance Data Management

Rachana Ananthakrishnan - [rachana@globus.org](mailto:rachana@globus.org)

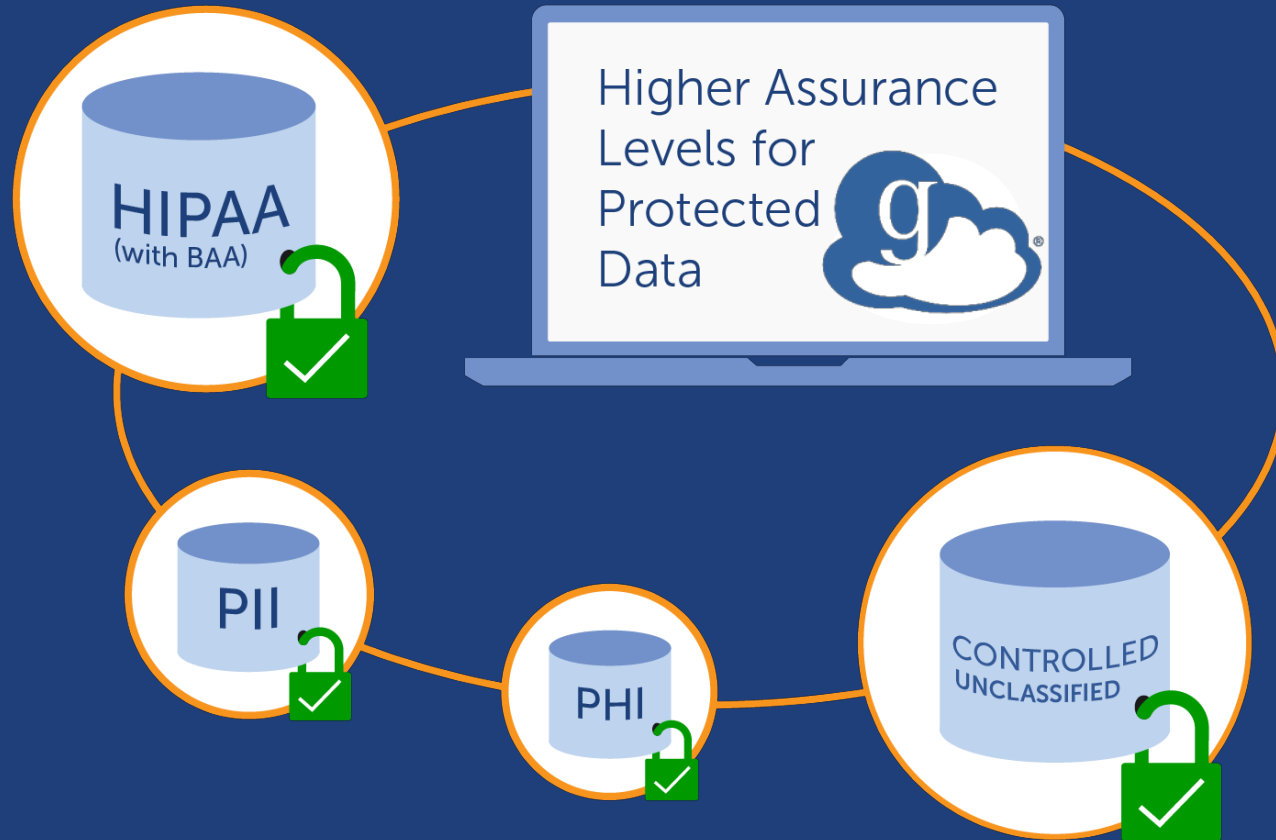
Greg Nawrocki - [greg@globus.org](mailto:greg@globus.org)

Johns Hopkins University  
February 21, 2019



# Manage Protected Data

## Higher assurance levels for HIPAA and other regulated data



- Support for protected data such as health related information
- Share data with collaborators while meeting compliance requirements
- Includes BAA option



# Globus for high assurance data management

- **Restricted data handling**
  - PHI (Protected Health Information)
  - PII (Personally identifiable information)
  - Controlled Unclassified Information
- **University of Chicago security controls**
  - NIST 800-53 Low
  - Superset of 800-171 Low
- **Business Associate Agreements (BAA) will be between University of Chicago and our subscribers**
  - University of Chicago has a BAA with Amazon



# Compliance focus areas

Although there was a good deal of “product work” much of the effort was focused on the way we do things

- **Access Control:** Least privilege model
- **Configuration Management:** Change control, impact/risk
- **Maintenance:** Automation, vulnerability mitigation
- **Accountability:** Detailed audit trail (protection, forensics)
- **Information integrity:** Protection, monitoring



# Restricted data disclosure to Globus

- **With High Assurance and BAA tier, PHI data can be moved and shared**
- **Globus never sees file contents**
  - File contents can have restricted data
- **File paths/name can have restricted data (e.g. PHI)**
- **None of the other elements (endpoint definitions, labels, collection definitions) can contain restricted data**

# Globus services in scope for first release

- **Globus Service: Auth, Transfer, Groups, DNS, Sharing**
- **Globus Connect Server v5.2**
- **Globus Connect Personal v3.x**
- **New web app ([app.globus.org](https://app.globus.org)) – try it now!**
- **Globus Command Line Interface (CLI)**



## Other features/services/products

- **Connectors: AWS S3 as priority (future release)**
- **Platform: Globus Search (future release)**
- **Out of scope: Globus ID, data publication SaaS, current web app, GCS v4.x, GCSv5.0, 5.1, GCP2.x**
- **Discontinued: Hosted CLI (as of August 1, 2018)**



# Globus Connect Server 5.2

- **Support high assurance data access**
- **Multiple storage connectors per endpoint**
  - POSIX
  - Google Drive
- **New terminologies and ways of doing things**

See <https://docs.globus.org/globus-connect-server-v5-installation-guide/> for 4.x – 5.x terminology and architecture changes

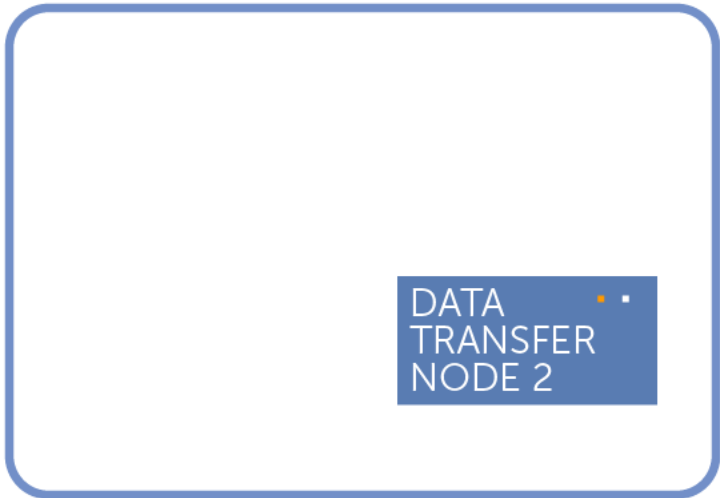
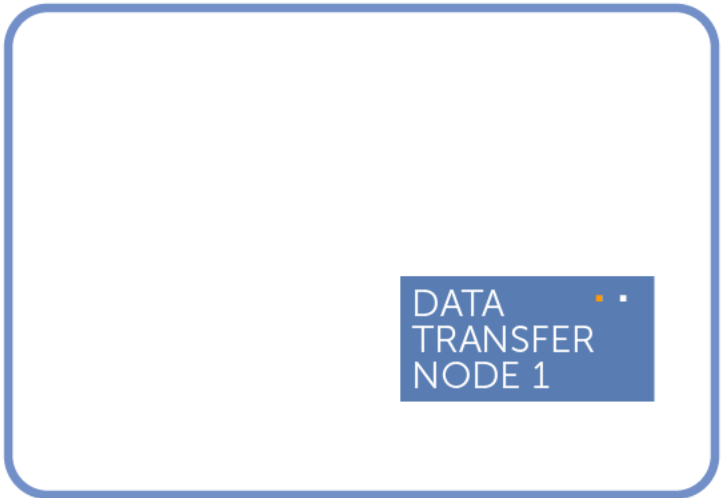
See <https://docs.globus.org/high-assurance/> for instructions on how to create a high assurance collection





# Out with the old, in with the new

- **Host endpoints → Mapped collections**
  - Need local account to access data
- **Shared endpoints → Guest collections**
  - No local account needed for data access, permissions set in Globus
- **Use host endpoint to create shared endpoint →  
Use storage gateway to create (guest) collections**
- **Access via GridFTP → Access via GridFTP or HTTPS**
- **Initially available via Globus Connect Server v5.2**



---

DATA  
TRANSFER  
NODES

Network & storage  
connected servers  
in ScienceDMZ



# ENDPOINT



globus  
connect  
server  
NODE 1

DATA  
TRANSFER  
NODE 1



globus  
connect  
server  
NODE 2

DATA  
TRANSFER  
NODE 2

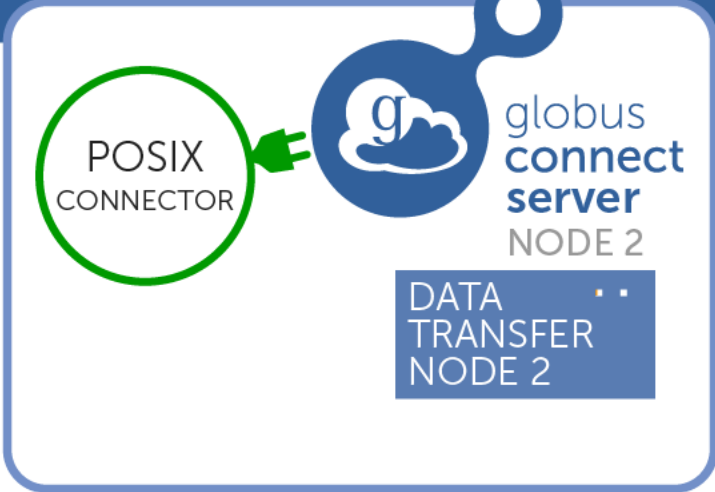
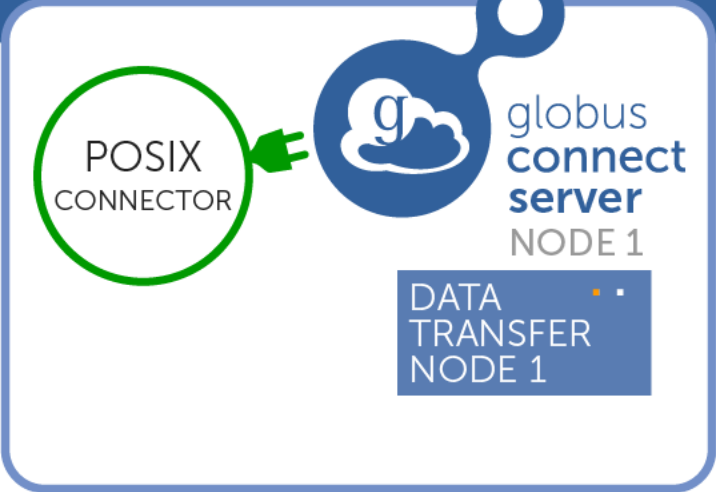
---

ENDPOINT  
Management &  
config interface

---

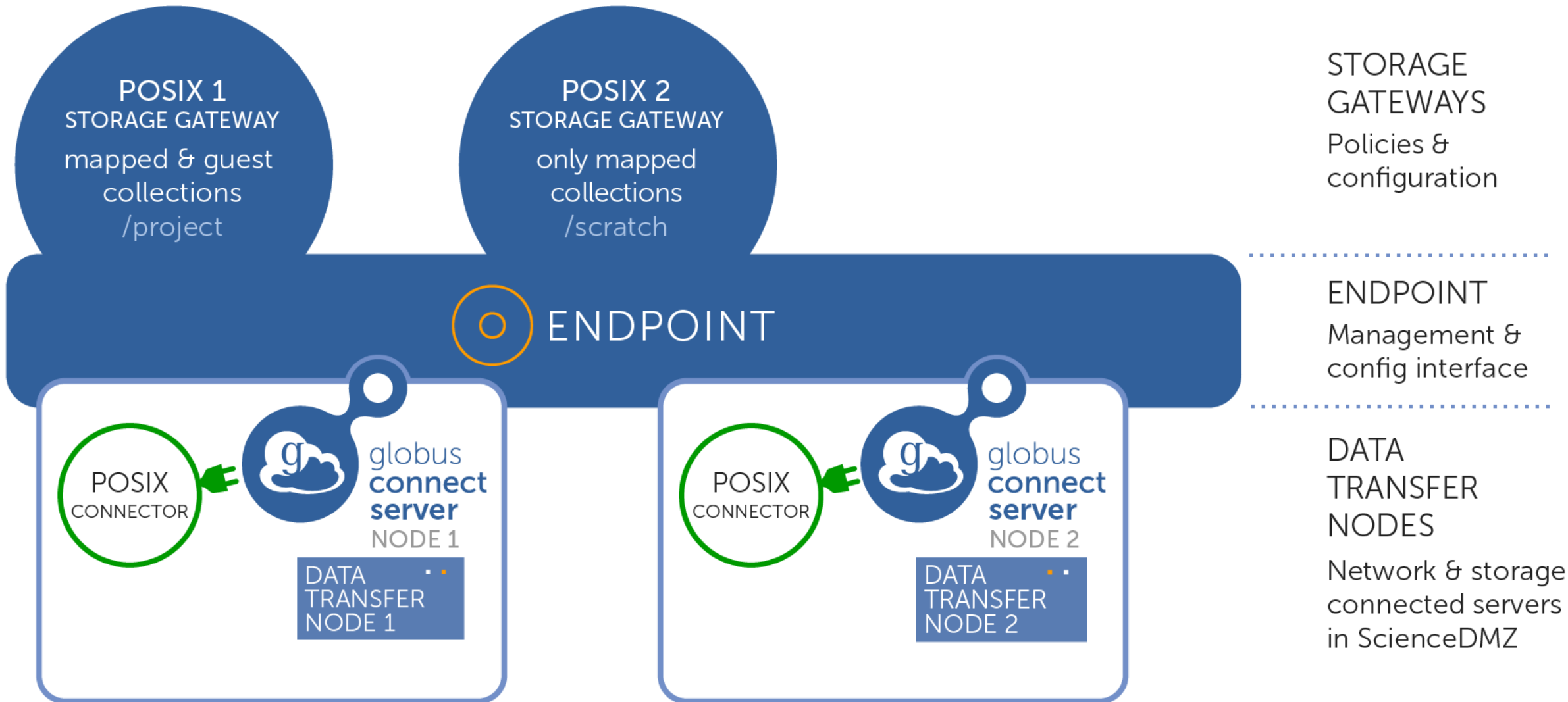
DATA  
TRANSFER  
NODES  
Network & storage  
connected servers  
in ScienceDMZ

# ENDPOINT



ENDPOINT  
Management &  
config interface

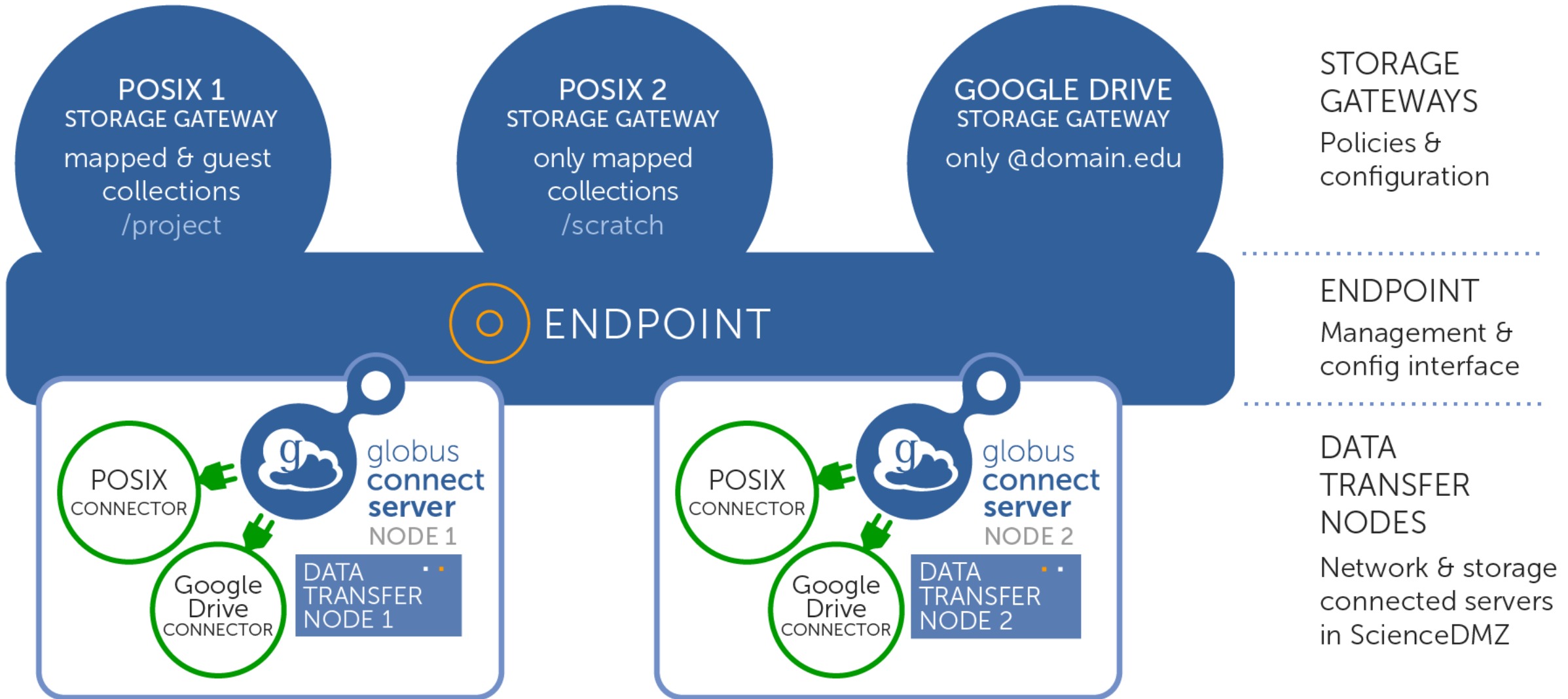
DATA  
TRANSFER  
NODES  
Network & storage  
connected servers  
in ScienceDMZ



STORAGE GATEWAYS  
Policies & configuration

ENDPOINT  
Management & config interface

DATA TRANSFER NODES  
Network & storage connected servers in ScienceDMZ



**POSIX 1  
STORAGE GATEWAY**  
mapped & guest  
collections  
/project

**POSIX 2  
STORAGE GATEWAY**  
only mapped  
collections  
/scratch

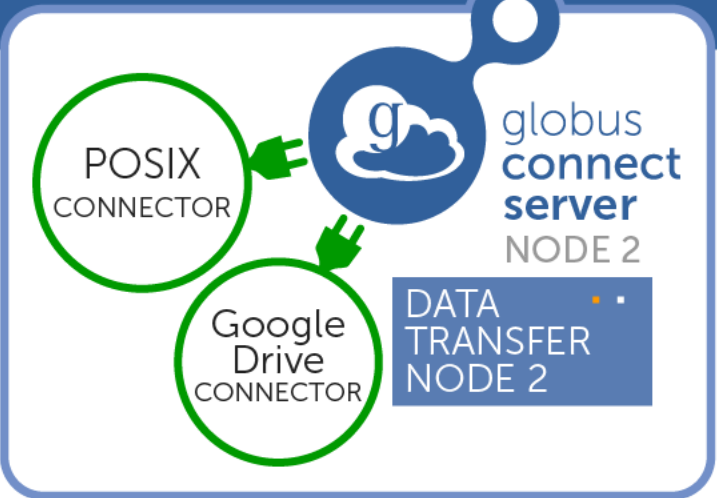
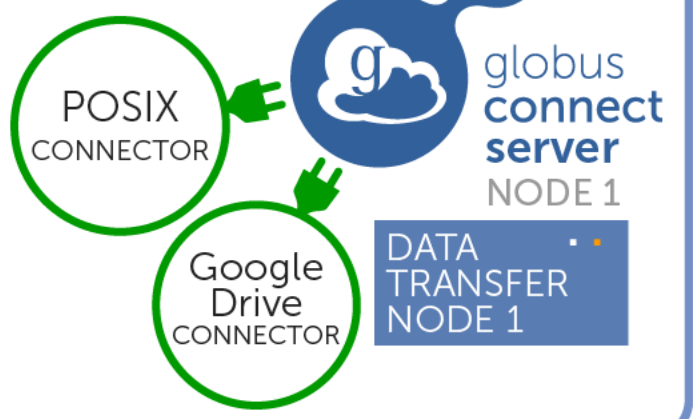
**GOOGLE DRIVE  
STORAGE GATEWAY**  
only @domain.edu

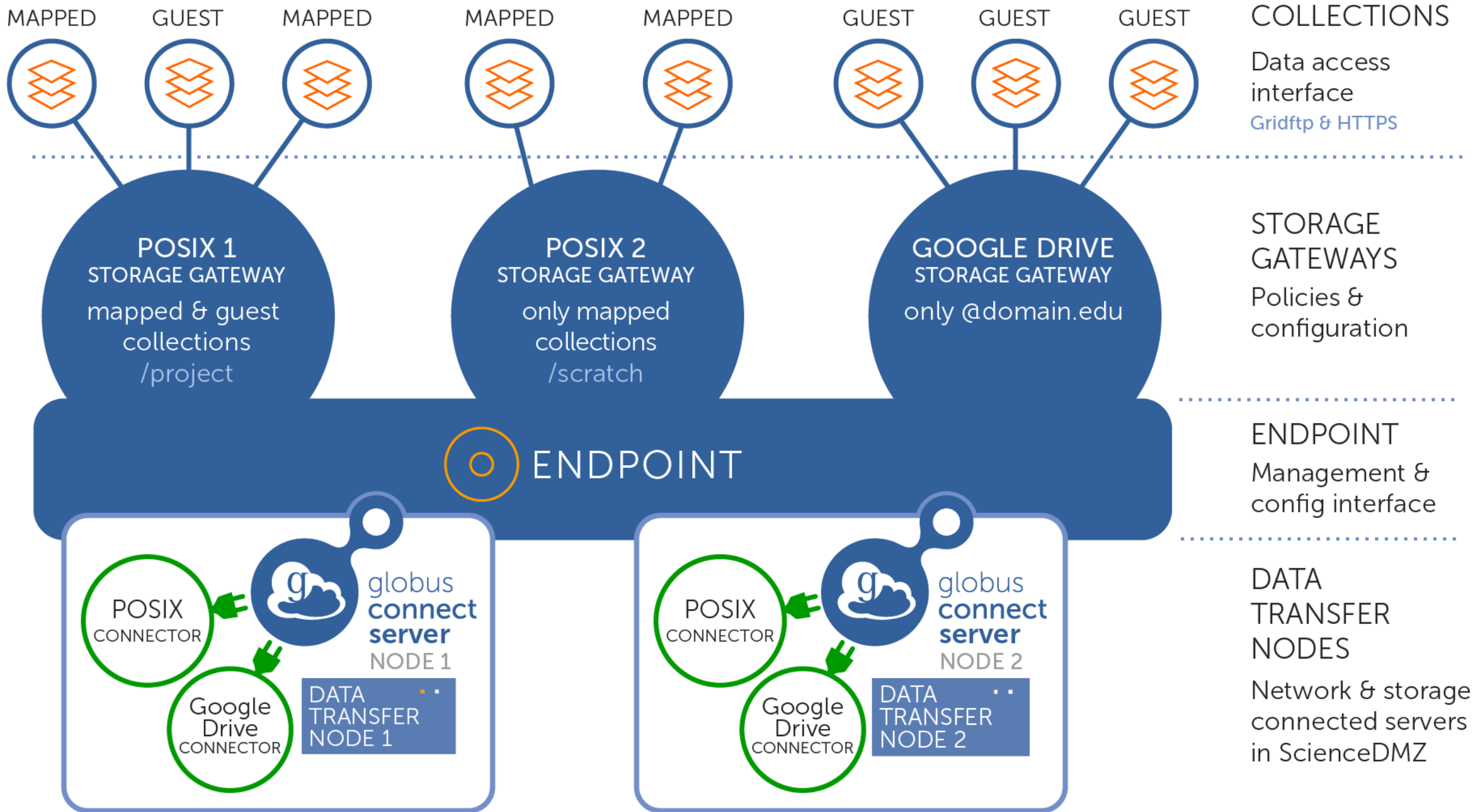
**ENDPOINT**

**STORAGE  
GATEWAYS**  
Policies &  
configuration

**ENDPOINT**  
Management &  
config interface

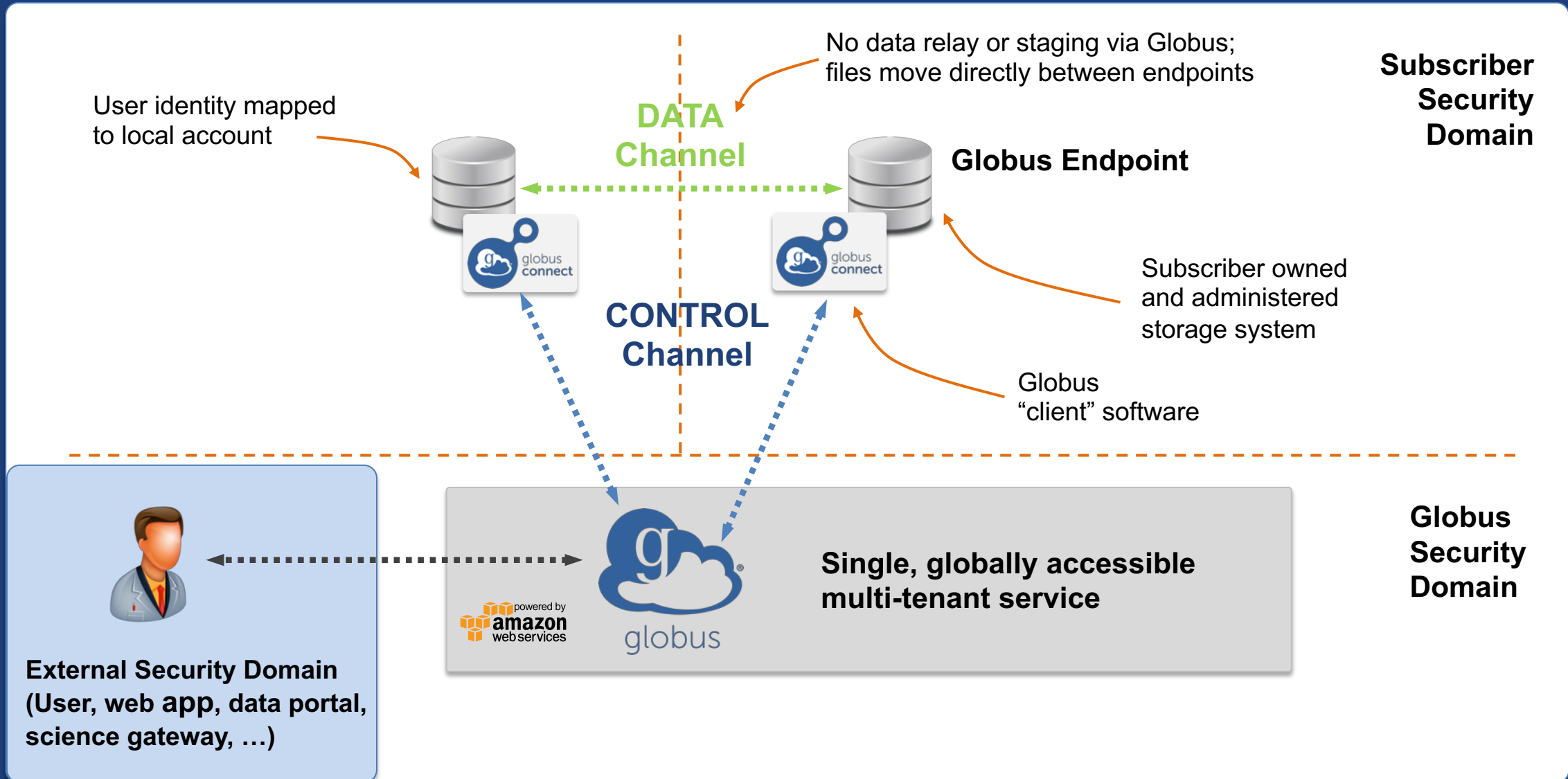
**DATA  
TRANSFER  
NODES**  
Network & storage  
connected servers  
in ScienceDMZ







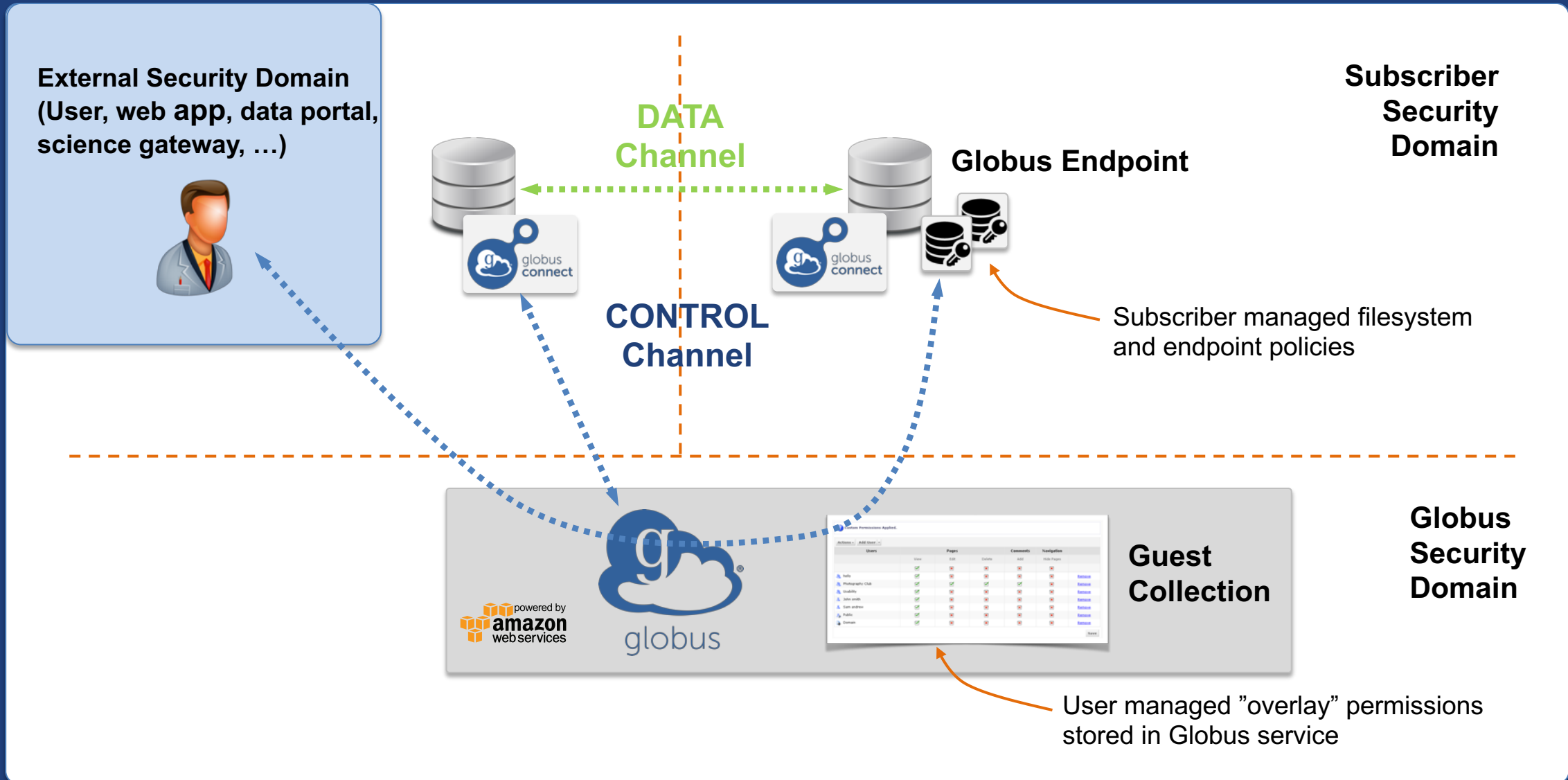
# Conceptual architecture: Mapped collections







# Conceptual architecture: Guest Collections





# Globus Connect Server v5 Milestones

v5.3: ...

v5.x: v4 feature parity+

v5.2: High assurance

v5.1: POSIX guest collections, HTTPS

- Multi DTN support
- Additional storage types
- Custom IdPs
- ...

Other features

v5.0: Google Drive





# High Assurance features

- **Additional authentication assurance**
  - Per storage gateway policy on frequency of authentication with specific identity for access to data (timeout)
  - Ensure that user authenticates with the specific identity that gives them access within session (decoupling linked identities)
- **Session/device isolation**
  - Authentication context is per application, per session (~browser session)
- **Enforces encryption of all user data in transit**
- **Audit logging**



# Globus security features – endpoint

- **Data remain at institution, not hosted by Globus**
- **Integrity checks of transferred data**
- **High availability and redundancy**
- **Encryption**
  - All communications and data in transit are encrypted (data in flight)
    - Transfers are encrypted using OpenSSL libraries installed at the endpoint and TLS 1.2 or higher. The cipher used for a transfer is negotiated between the source and destination endpoints and depends on the preference-ordered list of OpenSSL ciphers (default HIGH) on each endpoint.
  - All data stored by Globus is encrypted at rest (**service**)
    - All Globus operational and log data stored in AWS are encrypted at rest, using either AWS Key Management Service encryption or AWS service-specific encryption options.
- **Access Control**
  - Identities provided and managed by institution
  - Acts as identity broker only, does not access or store any institutional user credentials
  - Institution controls all access policies (at multiple levels)
    - who can access what data and with what permissions
    - who can share what data and with what permissions
    - all access policies can be changed or revoked at any time



# Globus security features - service

- **Secure operations**
  - Intrusion detection and prevention
  - Performance and health monitoring
  - Logging
  - Secure remote access, access control
  - Uniform configuration management and change control
  - Backups and disaster recovery
  - All data stored by Globus is encrypted at rest
- **Use AWS best practices for securing environment**
  - Virtual Private Clouds – host security
  - AWS security groups – network security
  - AWS IAM (identity and access management) best practices – individual security



# Additional authentication assurance



userX@anl.gov



userX@anl.gov

globus File Manager

Collection: NCAR RDA Dataset Archive

Path: /ds314.2/2000\_2009/

File Name	Date	Size	Type
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1:4...	259.21 MB	file
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1:4...	234.33 MB	file
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1:4...	259.21 MB	file
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1:4...	250.92 MB	file
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1:4...	259.21 MB	file
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1:4...	250.92 MB	file
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1:4...	259.21 MB	file
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1:4...	259.21 MB	file
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1:5...	259.21 MB	file
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1:51...	250.92 MB	file
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1:51...	259.21 MB	file
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1:5...	250.92 MB	file
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1:5...	250.21 MB	file

THE UNIVERSITY OF CHICAGO

JAGGAER

Welcome!

Please log in to JAGGAER Production Environment.

To securely logout, you must quit your browser.

CNetID / UCHADID:

Password:

[Forgot your password?](#)

Need help with your CNetID or UCHADID? If you are a University of Chicago faculty member, student, or staff member you may use myaccount.uchicago.edu to change your password, recertify your



# Additional authentication assurance



userX@anl.gov



userX@uchicago.edu

The screenshot shows the Globus File Manager interface for userX@anl.gov. The interface includes a sidebar with navigation options, a main content area displaying a file list, and a right-hand menu with various actions. The file list shows a collection of files named 'clmforc.WFDEI.c2017.0.5x0....' with columns for date, size, and type. The right-hand menu includes options like 'Permissions', 'Transfer or Sync to...', 'New Folder', 'Rename', 'Delete Selected', 'Preview (limited)', 'Download (https)', 'Open (https)', 'Get Link', 'Show Hidden Items', and 'Deactivate'.

The screenshot shows the Globus File Manager interface for userX@uchicago.edu. The interface includes a sidebar with navigation options, a main content area displaying a file list, and a right-hand menu with various actions. The file list shows a collection of folders named 'bester', 'dpowers', 'mlink', 'ranantha', 'read\_only', 'sjmartin', 'tuecke', and 'vas' with columns for date, size, and type. The right-hand menu includes options like 'Permissions', 'Transfer or Sync to...', 'New Folder', 'Rename', 'Delete Selected', 'Preview (limited)', 'Download (https)', 'Open (https)', 'Get Link', and 'Show Hidden Items'.



# Re-authentication timeout



globus File Manager

Collection: NCAR RDA Dataset Archive

Path: /ds314.2/2000\_2009/

File Name	Date	Size	Type
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1.4...	259.21 MB	file
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1.4...	234.33 MB	file
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1.4...	259.21 MB	file
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1.4...	250.92 MB	file
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1.4...	259.21 MB	file
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1.4...	250.92 MB	file
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1.4...	259.21 MB	file
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1.4...	250.92 MB	file
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1.5...	259.21 MB	file
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1.51...	250.92 MB	file
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1.51...	259.21 MB	file
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1.5...	250.92 MB	file
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1.5...	250.21 MB	file

Permissions, Transfer or Sync to..., New Folder, Rename, Delete Selected, Preview (limited), Download (https), Open (https), Get Link, Show Hidden Items, Deactivate

globus File Manager

Collection: GCSv5.2 Globus Demo HA Mapped Collection

Path: /

Folder Name	Date	Size	Type
bester	9/1/2018 5:44pm	6 B	folde
dpowers	9/2/2018 3:24pm	30 B	folde
mmlink	9/1/2018 5:44pm	6 B	folde
ranantha	9/1/2018 5:44pm	6 B	folde
read_only	9/1/2018 6:17pm	30 B	folde
sjmartin	9/1/2018 5:44pm	6 B	folde
tuecke	9/3/2018 10:40a...	22 B	folde
vas	9/24/2018 1:16pm	6 B	folde

Permissions, Transfer or Sync to..., New Folder, Rename, Delete Selected, Preview (limited), Download (https), Open (https), Get Link, Show Hidden Items





# Application Instance Isolation

Authenticated in browser session (app instance 1)



The screenshot shows the Globus File Manager interface. The top navigation bar includes the Globus logo, a hamburger menu, and the text "File Manager". Below this, there are "Panels" and "Bookmark Manager" options. The main content area displays a "Collection" of "GCSv5.2 Globus Demo HA Mapped Collection" with a "Path" of "/". A table lists several folders with their creation dates, sizes, and types. A sidebar on the left shows "RECENTLY USED ENDPOINTS" including "UChicago RCC Midway", "petrel#testbed", "GCSv5.2 Globus Demo HA Mapped Collection", "5.1 Home Shares - Vas", "5.1 Sandbox - Vas", "Amazon S3 Gateway - Vas", "ESnet Read-Only Test DTN at Sunnyvale", "Vas Laptop", and "POSIX Sandbox - Vas". A right-hand menu contains actions like "Permissions", "Transfer or Sync to...", "New Folder", "Rename", "Delete Selected", "Preview (limited)", "Download (https)", "Open (https)", "Get Link", and "Show Hidden Items".

Folder Name	Created	Size	Type
bester	9/1/2018 5:44pm	6 B	folde
dpowers	9/2/2018 3:24pm	30 B	folde
mmlink	9/1/2018 5:44pm	6 B	folde
ranantha	9/1/2018 5:44pm	6 B	folde
read_only	9/1/2018 6:17pm	30 B	folde
sjmartin	9/1/2018 5:44pm	6 B	folde
tuecke	9/3/2018 10:40a...	22 B	folde
vas	9/24/2018 1:16pm	6 B	folde



Re-authentication required in CLI session (app instance 2)



```
(globus-cli) - $ globus
Usage: globus [OPTIONS] COMMAND [ARGS]...

Options:
  -v, --verbose           Control level of output
  -h, --help             Show this message and exit.
  -F, --format [unix|json|text] Output format for stdout. Defaults to text
  --jmespath, --jq TEXT  A JMESPath expression to apply to json output. Takes precedence over any specified '--format' and forces the format to be json processed by this expression
  --map-http-status TEXT Map HTTP statuses to any of these exit codes: 0,1,50-99. e.g. "404=50,403=51"

Commands:
  bookmark      Manage endpoint bookmarks
  config        Manage your Globus config file. (Advanced Users)
  delete        Submit a delete task (asynchronous)
  endpoint      Manage Globus endpoint definitions
  get-identities Lookup Globus Auth Identities
  list-commands List all CLI Commands
  login         Log into Globus to get credentials for the Globus CLI
  logout        Logout of the Globus CLI
  ls            List endpoint directory contents
  mkdir         Make a directory on an endpoint
  rename        Rename a file or directory on an endpoint
  rm            Delete a single path; wait for it to complete
  session       Manage your CLI auth session
  task         Manage asynchronous tasks
  transfer      Submit a transfer task (asynchronous)
  update        Update the Globus CLI to its latest version
  version       Show the version and exit
  whoami        Show the currently logged-in primary...
```



# Application Instance Isolation



The screenshot shows the desktop version of the Globus File Manager. The interface includes a sidebar with navigation options, a main content area with search and path fields, and a file list table. The file list contains multiple files with names like 'clmforc.WFDEI.c2017.0.5x0....' and various metadata such as dates and sizes. A context menu is open on the right side of the file list, showing options like 'Permissions', 'Transfer or Sync to...', 'New Folder', 'Rename', 'Delete Selected', 'Preview (limited)', 'Download (https)', 'Open (https)', 'Get Link', 'Show Hidden Items', and 'Deactivate'.

File Name	Date	Size	Type
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1:4...	259.21 MB	file
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1:4...	234.33 MB	file
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1:4...	259.21 MB	file
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1:4...	250.92 MB	file
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1:4...	259.21 MB	file
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1:4...	250.92 MB	file
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1:4...	259.21 MB	file
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1:4...	250.92 MB	file
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1:5...	259.21 MB	file
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1:51...	250.92 MB	file
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1:51...	259.21 MB	file
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1:5...	250.92 MB	file
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1:5...	250.21 MB	file

The screenshot shows the mobile version of the Globus File Manager app. The interface is optimized for a smaller screen, with a search bar and path field at the top. The file list shows several files with names like '100KB.dat', '10KB.dat', '10MB.dat', and '1KB.dat', along with their respective sizes and dates. The bottom of the screen features a navigation bar with icons for back, forward, upload, bookmark, and refresh.

File Name	Date	Size
100KB.dat	9/18/2018 1:19am	100 KB
10KB.dat	9/18/2018 1:19am	10 KB
10MB.dat	9/18/2018 1:19am	10 MB
1KB.dat	9/18/2018 1:19am	1 KB



# Application Instance Isolation



File Manager

Collection: NCAR RDA Dataset Archive

Path: /ds314.2/2000\_2009/

select all	up one folder	refresh list	columns	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Permissions
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Transfer or Sync to...
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	New Folder
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Rename
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Delete Selected
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Preview (limited)
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Download (https)
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Open (https)
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Get Link
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Show Hidden Items
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Deactivate

RECENTLY USED ENDPOINTS

- globuspublish#trial\_data
- UChicago RCC Midway
- petrel#testbed
- GCSv5.2 Globus Demo HA Mapped Collection
- 5.1 Home Shares - Vas
- 5.1 Sandbox - Vas
- Amazon S3 Gateway - Vas
- ESnet Read-Only Test DTN at Sunnyvale
- Vas Laptop
- POSIX Sandbox - Vas
- Globus Tutorial Endpoint 1
- NCAR RDA Dataset Archive
- Globus Tutorial Endpoint 2

app.globus.org

File Manager

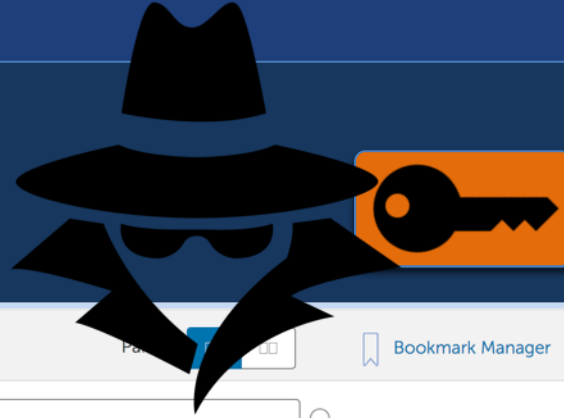
Collection: UChicago RCC Midway

Path: /-/

select all	Sort	
<input type="checkbox"/>	<input type="checkbox"/>	100KB.dat
<input type="checkbox"/>	<input type="checkbox"/>	10KB.dat
<input type="checkbox"/>	<input type="checkbox"/>	10MB.dat
<input type="checkbox"/>	<input type="checkbox"/>	1KB.dat



# Application Instance Isolation



globus File Manager

Collection: NCAR RDA Dataset Archive

Path: /ds314.2/2000\_2009/

**ACCESS DENIED**

File Name	Size	Type
clmforc.WFDEI.c2017.0.5x0...	259.21 MB	file
clmforc.WFDEI.c2017.0.5x0...	250.92 MB	file
clmforc.WFDEI.c2017.0.5x0...	259.21 MB	file
clmforc.WFDEI.c2017.0.5x0...	250.92 MB	file
clmforc.WFDEI.c2017.0.5x0...	259.21 MB	file
clmforc.WFDEI.c2017.0.5x0...	250.92 MB	file
clmforc.WFDEI.c2017.0.5x0...	259.21 MB	file
clmforc.WFDEI.c2017.0.5x0...	250.92 MB	file
clmforc.WFDEI.c2017.0.5x0...	259.21 MB	file
clmforc.WFDEI.c2017.0.5x0...	250.92 MB	file



app.globus.org File Manager

Collection: UChicago RCC Midway

Path: /-/

File Name	Size	Type
100KB.dat	100 KB	file
10KB.dat	10 KB	file
10MB.dat	10 MB	file
1KB.dat	1 KB	file



# Application Instance Isolation



File Manager

Collection: NCAR RDA Dataset Archive

Path: /ds314.2/2000\_2009/

select all	up one folder	refresh list	columns	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Permissions
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Transfer or Sync to...
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	New Folder
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Rename
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Delete Selected
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Preview (limited)
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Download (https)
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Open (https)
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Get Link
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Show Hidden Items
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Deactivate

Permissions

Transfer or Sync to...

New Folder

Rename

Delete Selected

Preview (limited)

Download (https)

Open (https)

Get Link

Show Hidden Items

Deactivate

File Manager

Collection: UChicago RCC Midway

Path: /-/

select all	Sort	
<input type="checkbox"/>	<input type="checkbox"/>	100KB.dat
<input type="checkbox"/>	<input type="checkbox"/>	10KB.dat
<input type="checkbox"/>	<input type="checkbox"/>	10MB.dat
<input type="checkbox"/>	<input type="checkbox"/>	1KB.dat



# Application Instance Isolation

The screenshot shows the Globus File Manager web interface. The left sidebar lists 'RECENTLY USED ENDPOINTS' including 'globuspublish#trial\_data', 'UChicago RCC Midway', 'petrel#testbed', 'GCSv5.2 Globus Demo HA Mapped Collection', '5.1 Home Shares - Vas', '5.1 Sandbox - Vas', 'Amazon S3 Gateway - Vas', 'ESnet Read-Only Test DTN at Sunnyvale', 'Vas Laptop', 'POSIX Sandbox - Vas', 'Globus Tutorial Endpoint 1', 'NCAR RDA Dataset Archive', and 'Globus Tutorial Endpoint 2'. The main content area shows the 'File Manager' for the 'NCAR RDA Dataset Archive' collection at the path '/ds314.2/2000\_2009/'. A table of files is displayed with columns for file name, date, and size. A large green checkmark is overlaid on the interface, and a key icon is visible in the top right corner.

File Name	Date	Size	Type
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1:4...	259.21 MB	file
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1:4...	234.33 MB	file
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1:4...	259.21 MB	file
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1:4...	250.92 MB	file
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1:4...	259.21 MB	file
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1:4...	250.92 MB	file
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1:4...	259.21 MB	file
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1:4...	250.92 MB	file
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1:4...	259.21 MB	file
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1:5...	259.21 MB	file
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1:51...	250.92 MB	file
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1:51...	259.21 MB	file
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1:5...	250.92 MB	file
clmforc.WFDEI.c2017.0.5x0....	2/19/2018 1:5...	259.21 MB	file

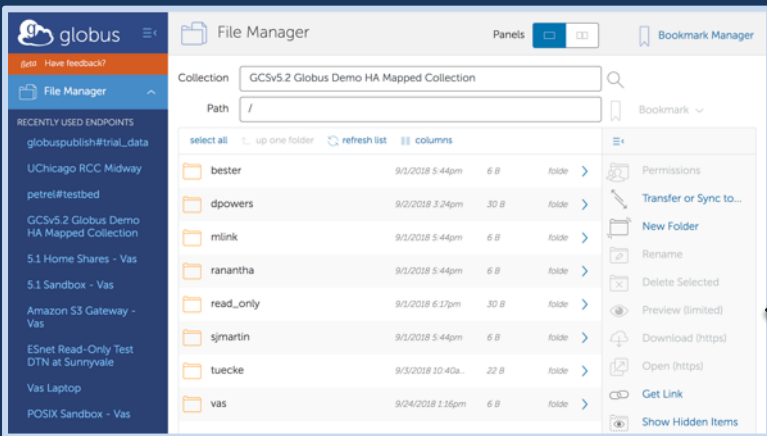


The screenshot shows the Globus File Manager mobile app interface. The top bar shows the time '10:45' and battery level '48%'. The main content area shows the 'File Manager' for the 'UChicago RCC Midway' collection at the path '/-/'. A list of files is displayed with columns for file name, date, and size. A large red 'X' is overlaid on the interface, and a hacker icon is visible in the top right corner.

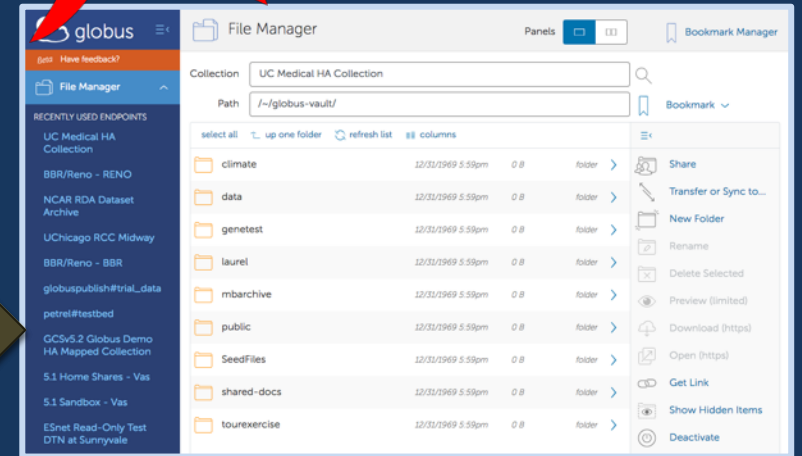
File Name	Date	Size
100KB.dat	9/18/2018 1:19am	100 KB
10KB.dat	9/18/2018 1:19am	10 KB
10MB.dat	9/18/2018 1:19am	10 MB
1KB.dat	9/18/2018 1:19am	1 KB

# Async transfer between HA collections

Mapped Collection  
HA timeout: 4hrs



Mapped Collection  
HA timeout: 2hrs

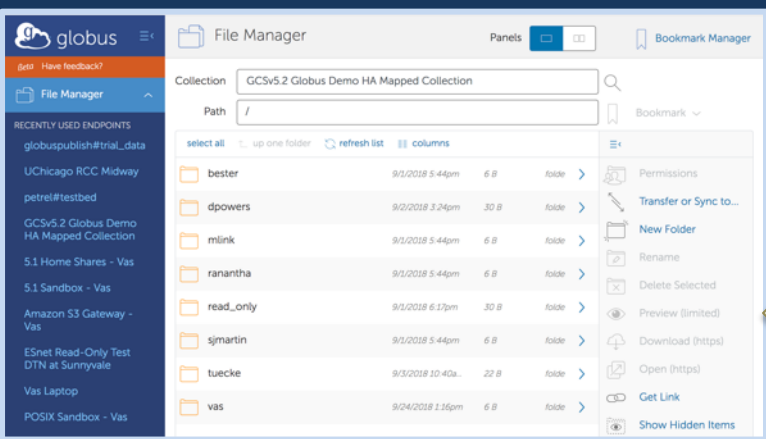




# Async transfer between HA collections



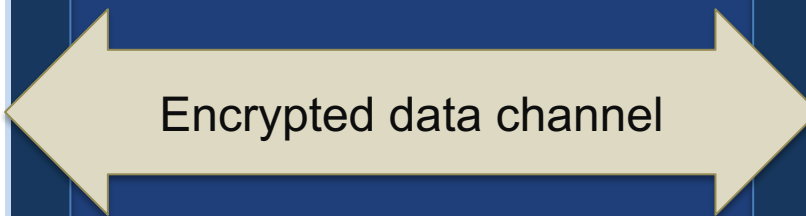
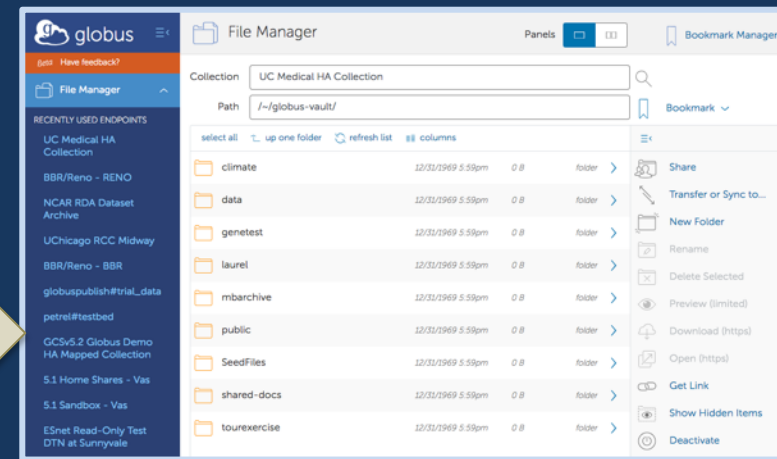
Mapped Collection  
HA timeout: 4hrs



Re-authentication  
required after 2hrs  
during long-running  
transfer



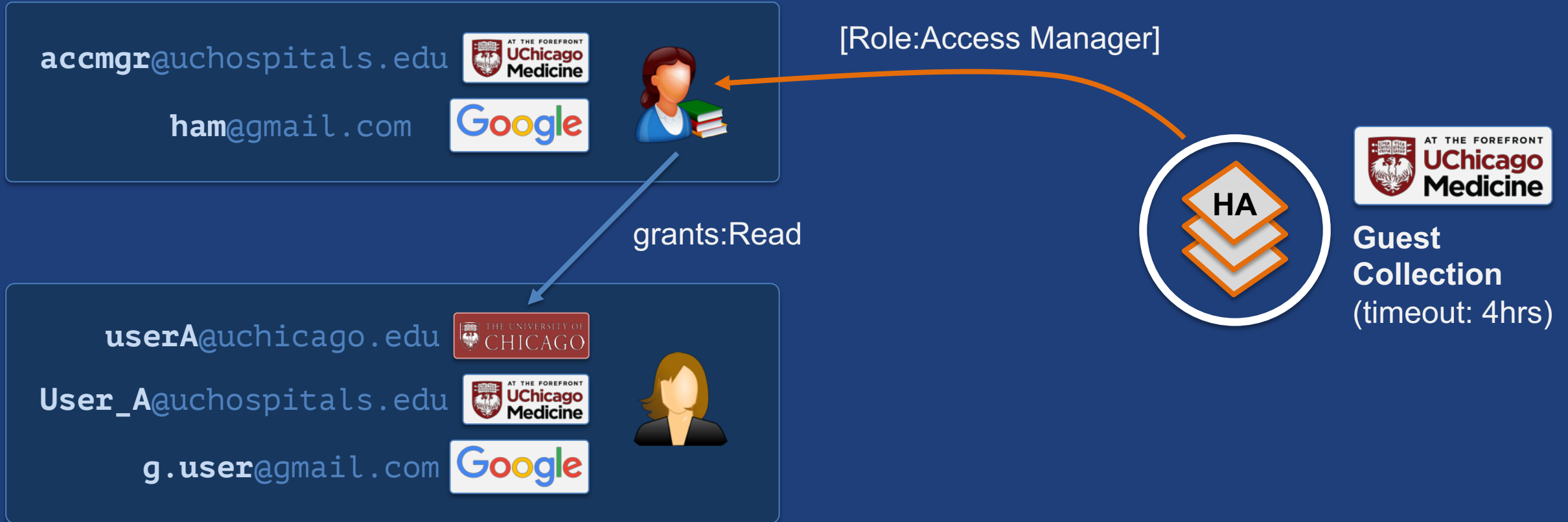
Mapped Collection  
HA timeout: 2hrs











# Example user flow: Guest collection





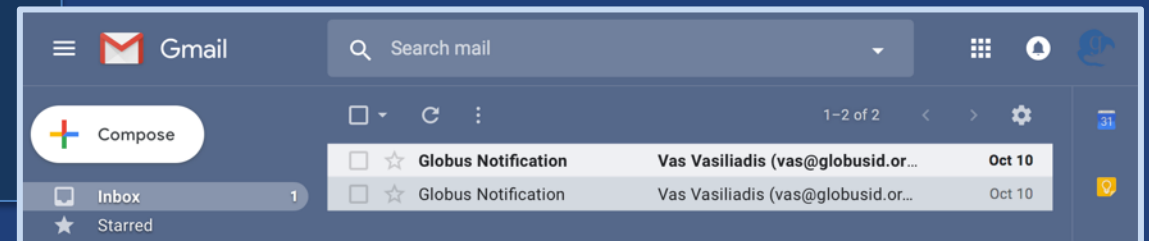
# Example user flow: Guest collection

accmgr@uchospitals.edu    
ham@gmail.com 

userA@uchicago.edu   
User\_A@uchospitals.edu    
g.user@gmail.com 



Guest  
Collection  
(timeout: 4hrs)



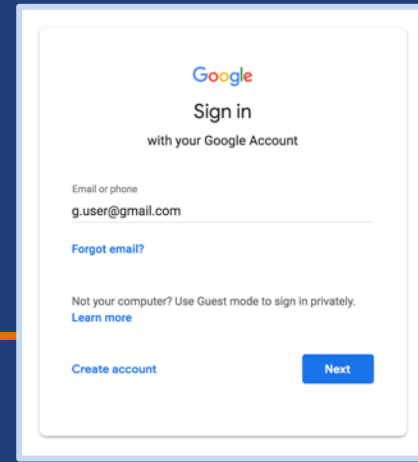






# Example user flow: Guest collection

acmgr@uchospitals.edu  
ham@gmail.com



userA@uchicago.edu  
User\_A@uchospitals.edu  
g.user@gmail.com



Google  
Sign in  
with your Google Account

Email or phone  
g.user@gmail.com

Forgot email?

Not your computer? Use Guest mode to sign in privately.  
[Learn more](#)

Create account Next



Guest Collection  
(timeout: 4hrs)





# Example user flow: Guest collection

acmgr@uchospitals.edu



ham@gmail.com



userA@uchicago.edu



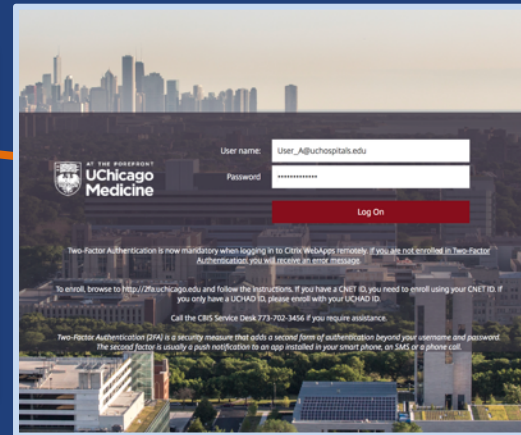
User\_A@uchospitals.edu



g.user@gmail.com



redirect → UC Medicine







Guest Collection (timeout: 4hrs)



# Example user flow: Guest collection

accmgr@uchospitals.edu    
ham@gmail.com 

userA@uchicago.edu   
User\_A@uchospitals.edu    
g.user@gmail.com 



Guest Collection  
(timeout: 4hrs)

[Permission:Read]



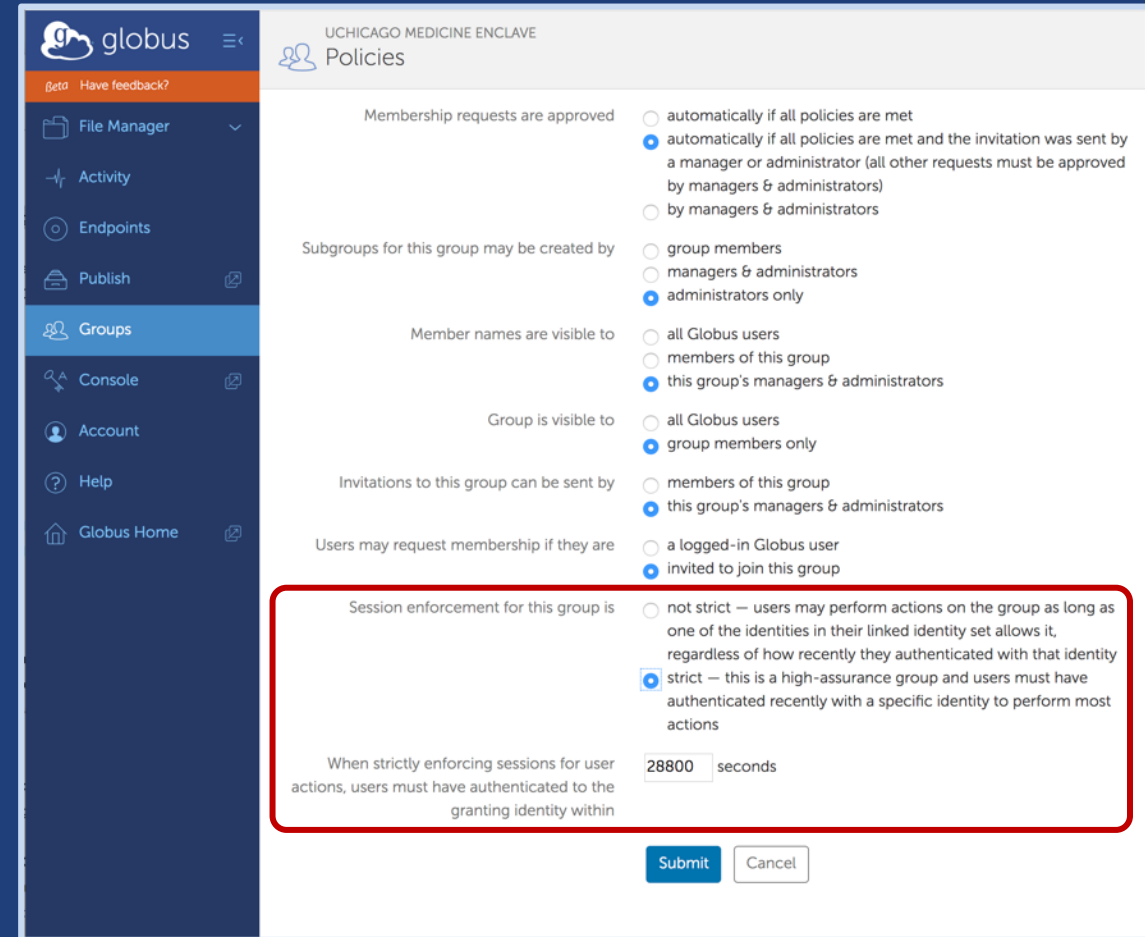


# Example management flows

- **Managing High Assurance endpoints requires authentication with authorized identity, within session**
  - Endpoint configuration
  - Globus Groups used to provide access to high assurance data
  - Management Console access (e.g. to review logs)

# Groups accessing HA guest collections

- **Policy options**
  - High assurance – (not) strict
  - Authentication assurance timeout
- **Additional restrictions**
  - Invitations can only be issued by administrator or manager
  - Changes to group policies require specific identity within session/ authentication assurance timeout
  - Subgroups inherit HA policy



The screenshot shows the 'Policies' configuration page for a group named 'UCHICAGO MEDICINE ENCLAVE'. The left sidebar contains navigation options: File Manager, Activity, Endpoints, Publish, Groups (selected), Console, Account, Help, and Globus Home. The main content area lists various policy settings with radio button options:

- Membership requests are approved:  automatically if all policies are met,  automatically if all policies are met and the invitation was sent by a manager or administrator (all other requests must be approved by managers & administrators),  by managers & administrators
- Subgroups for this group may be created by:  group members,  managers & administrators,  administrators only
- Member names are visible to:  all Globus users,  members of this group,  this group's managers & administrators
- Group is visible to:  all Globus users,  group members only
- Invitations to this group can be sent by:  members of this group,  this group's managers & administrators
- Users may request membership if they are:  a logged-in Globus user,  invited to join this group
- Session enforcement for this group is:  not strict — users may perform actions on the group as long as one of the identities in their linked identity set allows it, regardless of how recently they authenticated with that identity,  strict — this is a high-assurance group and users must have authenticated recently with a specific identity to perform most actions
- When strictly enforcing sessions for user actions, users must have authenticated to the granting identity within:  seconds

At the bottom, there are 'Submit' and 'Cancel' buttons.



# New Globus Connect Server installation flow

- **Install GCSv5.2+ binaries**
- **Register the endpoint at [developers.globus.org](https://developers.globus.org)**
- **Add connectors**
- **Add storage gateways**
  - Set as high assurance, configure authentication assurance timeout
  - Set policy on type of collections supported
- **Add mapped collection**
  - User must login with identity from configured domain
  - Local account determined by removing the TLD: `username@example1.org` → `username` is local account

<https://docs.globus.org/globus-connect-server-v5-installation-guide/> for installation instructions

<https://docs.globus.org/high-assurance/> for instructions on how to create a high assurance collection





# Audit log on DTN via GCSv5.2

```
#INTERACTIVE BROWSING, ATTEMPT TO ACCESS A NON-EXISTENT FILE
t=S ts=2018-02-05T15:47:26Z ref=dd66bfc2-0a8b-11e8-9441-065bf8bb5752 c_ip=cli.globusonline.org:36988 auth=GSIFTP+SHARING
p_usr=gcsweb s_usr=mlink@globus.org r=/ g_tid=none g_eid=b1419262-0a88-11e8-a749-0a448319c2f8 g_uid=mlink g_oid=b83ef3aa-
d274-11e5-a441-1717a57f7cc7
t=O ts=2018-02-05T15:47:29Z ref=dd66bfc2-0a8b-11e8-9441-065bf8bb5752 op=STAT c_path=/My%20Drive/b.txt s_path=c_path
t=E ts=2018-02-05T15:47:30Z ref=dd66bfc2-0a8b-11e8-9441-065bf8bb5752 op=STAT c_path=/My%20Drive/b.txt s_path=c_path
d_ip=0.0.0.0 len=0 res=GlobusError:%20v=1%20c=PATH_NOT_FOUND%0AGridFTP-Path:%20"/My%20Drive/b.txt"%0A

#FORCED TRANSFER FAILURE, FOLLOWED BY RETRY. NOTE INCOMPLETE LEN VALUE.
t=S ts=2018-02-05T16:27:44Z ref=7e845df6-0a91-11e8-91e1-065bf8bb5752 c_ip=ec2-54-237-254-199.compute-
1.amazonaws.com:60884 auth=GSIFTP+SHARING p_usr=gcsweb s_usr=mlink@globus.org r=/ g_tid=79cf7700-0a91-11e8-a74a-
0a448319c2f8 g_eid=b1419262-0a88-11e8-a749-0a448319c2f8 g_uid=mlink g_oid=b83ef3aa-d274-11e5-a441-1717a57f7cc7
t=O ts=2018-02-05T16:27:44Z ref=7e845df6-0a91-11e8-91e1-065bf8bb5752 op=STAT c_path=/My%20Drive/test7 s_path=c_path
t=O ts=2018-02-05T16:27:46Z ref=7e845df6-0a91-11e8-91e1-065bf8bb5752 op=RETR c_path=/My%20Drive/test7 s_path=c_path
t=E ts=2018-02-05T16:27:48Z ref=7e845df6-0a91-11e8-91e1-065bf8bb5752 op=RETR c_path=/My%20Drive/test7 s_path=c_path
d_ip=76.16.213.112 len=3145728 res=globus_ftp_control_data_write%20failed.%0AHandle%20not%20in%20the%20proper%20state%0A
t=O ts=2018-02-05T16:27:48Z ref=7e845df6-0a91-11e8-91e1-065bf8bb5752 op=CKSM c_path=/My%20Drive/test7 s_path=c_path
#RETRY
t=S ts=2018-02-05T16:28:25Z ref=96eee906-0a91-11e8-a41c-065bf8bb5752 c_ip=ec2-54-237-254-199.compute-
1.amazonaws.com:34996 auth=GSIFTP+SHARING p_usr=gcsweb s_usr=mlink@globus.org r=/ g_tid=79cf7700-0a91-11e8-a74a-
0a448319c2f8 g_eid=b1419262-0a88-11e8-a749-0a448319c2f8 g_uid=mlink g_oid=b83ef3aa-d274-11e5-a441-1717a57f7cc7
t=O ts=2018-02-05T16:28:25Z ref=96eee906-0a91-11e8-a41c-065bf8bb5752 op=STAT c_path=/My%20Drive/test7 s_path=c_path
t=O ts=2018-02-05T16:28:28Z ref=96eee906-0a91-11e8-a41c-065bf8bb5752 op=RETR c_path=/My%20Drive/test7 s_path=c_path
t=E ts=2018-02-05T16:28:32Z ref=96eee906-0a91-11e8-a41c-065bf8bb5752 op=RETR c_path=/My%20Drive/test7 s_path=c_path
d_ip=76.16.213.112 len=10223616 res=ok
t=O ts=2018-02-05T16:28:32Z ref=96eee906-0a91-11e8-a41c-065bf8bb5752 op=CKSM c_path=/My%20Drive/test7 s_path=c_path
```



# Globus Connect Personal (GCP)

- **New version for high assurance data handling**
- **Allow user to choose an identity for use with the endpoint**
  - Using GCP for data access requires that identity be in session
  - Guest collections will work as they do with GCS
- **Additional logging**



# New subscription levels

- **High Assurance**
  - 33% uplift on Standard subscription and on premium connectors used for high assurance data
- **BAA**
  - All High Assurance features + BAA with University of Chicago
  - 50% uplift on Standard subscription and on premium connectors used under a BAA
- **Separate subscription ID issued**

Features (click ⓘ for description)	Basic	Starter	Standard	High Assurance ⓘ	HIPAA BAA ⓘ
File transfer ⓘ	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
Managed endpoints ⓘ	None	1	Unlimited	Unlimited	Unlimited
Management console ⓘ	–	✓	✓	✓	✓
Usage reports ⓘ	–	✓	✓	✓	✓
Support for Globus Connect, Web, CLI ⓘ	–	✓	✓	✓	✓
File sharing ⓘ	–	✓	✓	✓	✓
Globus Plus users ⓘ	–	–	✓	✓	✓
Data publication ⓘ	–	–	✓	✓	✓
Application integration support ⓘ	–	–	✓	✓	✓
HTTPS support ⓘ	–	–	✓	✓	✓
Session/Device Isolation ⓘ	–	–	–	✓	✓
Additional authentication assurance ⓘ	–	–	–	✓	✓
Comprehensive audit logging ⓘ	–	–	–	✓	✓
Business Associate Agreement ⓘ	–	–	–	–	✓
Support service level ⓘ	–	Monday-Friday, 9am-5pm Central; 1-business day response			
Named support contacts ⓘ	–	1	5		
Pricing	Free	Contact us for subscription pricing or request details on pricing for Globus with protected data support			

# Webinar: Managing Protected Data with Globus

- Rachana Ananthakrishnan, Head of Products
- October 24, 2018 - 11:00 CDT
- **Web Site Link**
  - <https://www.globus.org/events/webinar-managing-protected-data>
- **Registration Page**
  - <https://www.eventbrite.com/e/webinar-managing-protected-data-with-globus-tickets-49899367351>