

ALLVIS

Uppsala University official storage of scientific Data

Allvis is a wise dwarf in the nordic mythology but in the modern world it is an acronym: all visdom (eng. all wisdom). Here we gather our scientists findings for the good (and gain) of future generations.



But what is a mythological being to do in the probably most secular region, in the probably most secular country in the world?

He has got an urgent need to modernize, re-vitalize and re-invent himself!

One set of precreated folders

Working material

Arbetsmaterial

- **A1** Administrative data
- **A2** Drafts
- **A3** Calculations
- **A4** Processed data
- **A5** Reference and source material
- **A6** Presentations
- **A7** Miscellaneous

Deselectable

Gallringsbart

- **G1** Experiment protocols
- **G2** Gathered data
- **G3** Processed data
- **G4** Media
- **G5** Questionnaire surveys

- **G6** Code Lists for identification

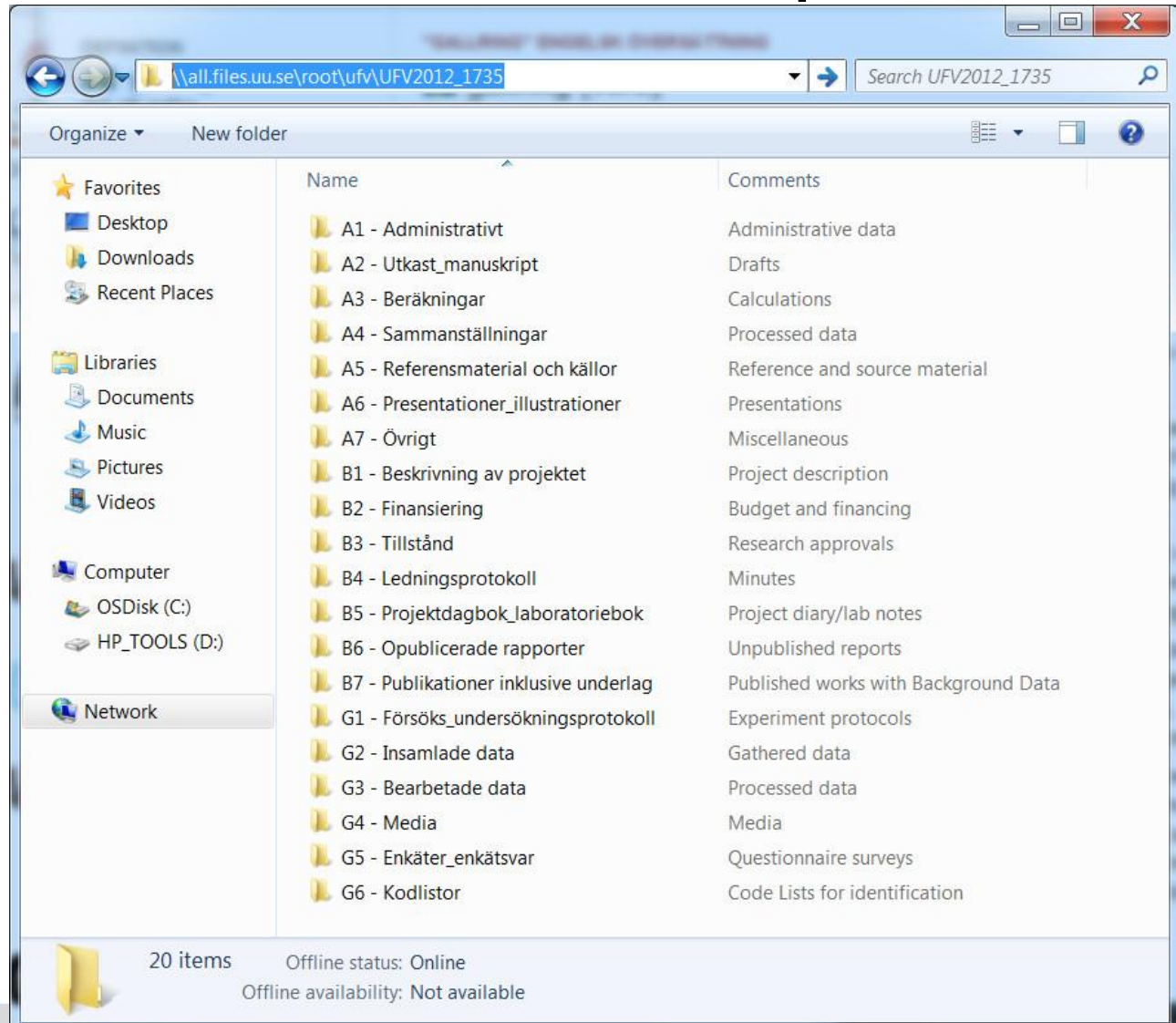
Preserve

Bevaras permanent

- **B1** Project description
- **B2** Budget and financing
- **B3** Research approvals
- **B4** Minutes
- **B5** Project diary/lab notes

- **B6** Unpublished reports
- **B7** Published works and Background Data

View from Windows Explorer



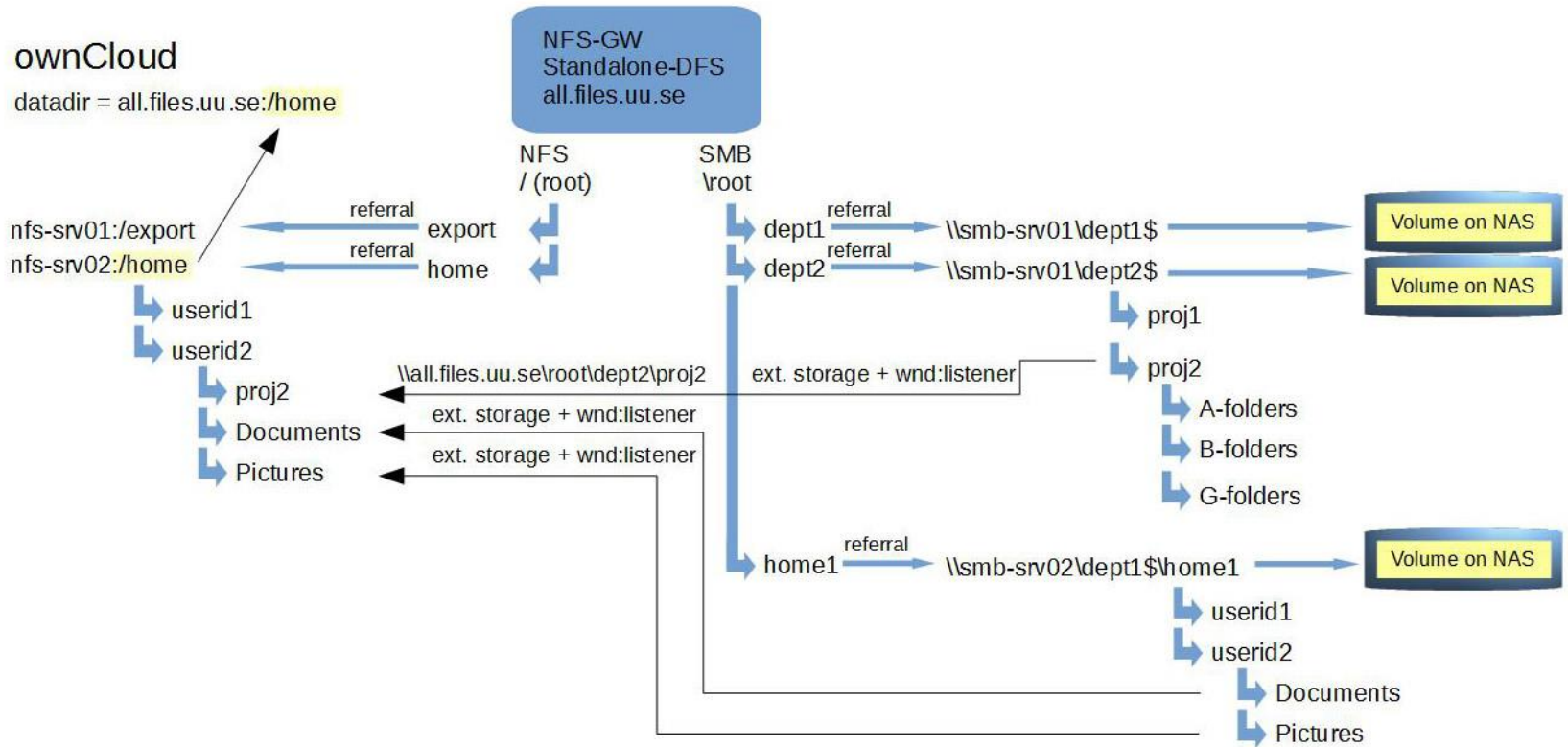
The screenshot shows a Windows Explorer window displaying a network share. The address bar shows the path `\\all.files.uu.se\root\ufv\UFV2012_1735`. The search bar contains the text `Search UFV2012_1735`. The left sidebar shows the navigation pane with 'Network' selected. The main pane displays a list of 20 folders with their names and comments.

Name	Comments
A1 - Administrativt	Administrative data
A2 - Utkast_manuskript	Drafts
A3 - Beräkningar	Calculations
A4 - Sammanställningar	Processed data
A5 - Referensmaterial och källor	Reference and source material
A6 - Presentationer_illustrationer	Presentations
A7 - Övrigt	Miscellaneous
B1 - Beskrivning av projektet	Project description
B2 - Finansiering	Budget and financing
B3 - Tillstånd	Research approvals
B4 - Ledningsprotokoll	Minutes
B5 - Projektdagbok_laboratoriebok	Project diary/lab notes
B6 - Opublicerade rapporter	Unpublished reports
B7 - Publikationer inklusive underlag	Published works with Background Data
G1 - Försöks_undersökningsprotokoll	Experiment protocols
G2 - Insamlade data	Gathered data
G3 - Bearbetade data	Processed data
G4 - Media	Media
G5 - Enkäter_enkät svar	Questionnaire surveys
G6 - Kodlistor	Code Lists for identification

20 items Offline status: Online
Offline availability: Not available



ALLVIS

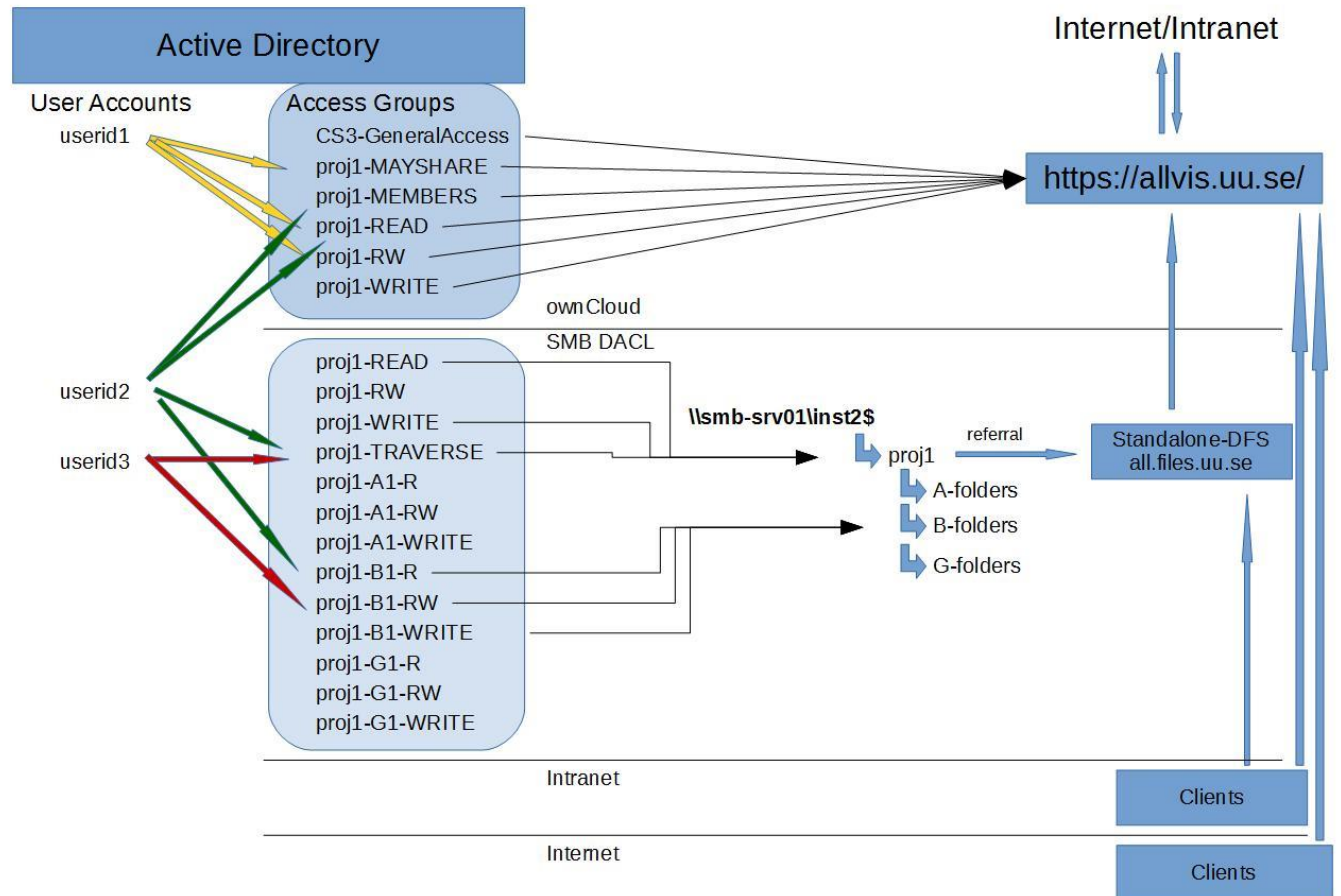


/home/userid = placeholder for ext. storage
- Documents
- Projectfolder(s)

/home/userid = minimal size to accomodate folders above



ALLVIS





UPPSALA
UNIVERSITET

Sharing



Areas of concern

Logons with NTLM are very chatty and costly.

The following steps present an outline of NTLM noninteractive authentication. The first step provides the user's NTLM credentials and occurs only as part of the interactive authentication (logon) process.

1. (Interactive authentication only) A user accesses a client computer and provides a domain name, user name, and password. The client computes a cryptographic *hash* of the password and discards the actual password.
2. The client sends the user name to the server (in *plaintext*).
3. The server generates a 16-byte random number, called a *challenge* or *nonce*, and sends it to the client.
4. The client encrypts this challenge with the hash of the user's password and returns the result to the server. This is called the *response*.
5. The server sends the following three items to the domain controller:
 - User name
 - Challenge sent to the client
 - Response received from the client
6. The domain controller uses the user name to retrieve the hash of the user's password from the Security Account Manager database. It uses this password hash to encrypt the challenge.
7. The domain controller compares the encrypted challenge it computed (in step 6) to the response computed by the client (in step 4). If they are identical, authentication is successful.



UPPSALA
UNIVERSITET

Areas of concern

Concerns/challenges

Is there a way to eliminate (the effects) NTLM?





UPPSALA
UNIVERSITET

Areas of concern

Concerns/challenges

Is there a way to eliminate (the effects) NTLM?

Potential solutions:

Don't use SMB!





UPPSALA
UNIVERSITET

Areas of concern

Concerns/challenges

Is there a way to mitigate (the effects) NTLM?



Areas of concern

Concerns/challenges

Is there a way to mitigate (the effects) NTLM?

Potential solutions:

1. Very much has already been done, see https://github.com/owncloud/core/tree/master/apps/files_external/3rdparty/icewind/smb



The screenshot shows a web browser displaying the GitHub repository page for the SMB wrapper. The browser's address bar shows the URL <https://github.com/owncloud/>. The page title is "SMB". Below the title, there are three status indicators: "coverage 89%" (yellow), "build passing" (green), and "Scrutinizer 9.66" (green). The description of the repository is "PHP wrapper for `smbclient` and `libsmbclient-php`". Below the description, there are two bullet points:

- Reuses a single `smbclient` instance for multiple requests
- Doesn't leak the password to the process list

Areas of concern

Concerns/challenges

Is there a way to mitigate (the effects) NTLM?

Potential solutions:

Smbclient uses `/etc/samba/smb.conf` for its configuration.

Most Visited Suggested Sites Getting Started Web Slice Gallery Dokument - Forskning...

[Samba] libsmbclient.so and /etc/samba/smb.conf

Jeremy Allison [jra at samba.org](mailto:jra@samba.org)

Mon Oct 24 17:04:28 UTC 2016

- Previous message: [\[Samba\] libsmbclient.so and /etc/samba/smb.conf](#)
- Next message: [\[Samba\] define share without name](#)
- Messages sorted by: [\[date\]](#) [\[thread\]](#) [\[subject\]](#) [\[author\]](#)

On Sat, Oct 22, 2016 at 04:45:04PM +0200, Davor Vusir via samba wrote:

```
> Hello!  
>  
> When using functions from libsmbclient.so, is the configuration in  
> /etc/samba/smb.conf honored?
```

Yes, that's where it gets the config info from.

```
[global]
```

```
workgroup = AD  
realm = AD.UU.SE  
security = ADS  
client signing = yes  
client use spnego = yes
```

```
kerberos method = secrets and keytab
```

```
idmap config *:backend = tdb  
idmap config *:range = 2200000001-220010  
idmap config AD:backend = ad  
idmap config AD:schema_mode = rfc2307  
idmap config AD:range = 1000-2200000000
```

Areas of concern

Concerns/challenges

Is there a way to mitigate (the effects) NTLM?

Potential solutions:

Smbclient uses `/etc/samba/smb.conf` for its configuration.

2. Steer smbclient towards one or more DC:s using "**password server = dc1, dc2**" on oC-server1, "**password server = dc2, dc1**" on oC-server2...

Eventually in conjunction with both oC-servers, file servers and DC:s in the same AD site.

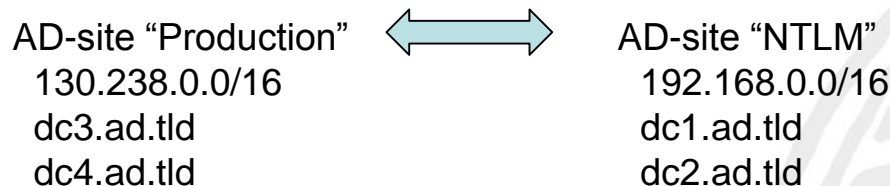
Areas of concern

Concerns/challenges

Is there a way to mitigate (the effects) NTLM?

Potential solutions:

Smbclient uses `/etc/samba/smb.conf` for its configuration.



Windows with IP’s belonging
to “production” site

OC-server1: “password server = dc1, dc2”
OC-server2: “password server = dc2, dc1”

Windows binds to a DC in the same AD-site.

Samba based Linux servers can be configured to use a specific DC.

Areas of concern

Concerns/challenges

Is there a way to mitigate (the effects) NTLM?

Potential solutions:

Smbclient uses `/etc/samba/smb.conf` for its configuration.

2. Steer smbclient towards one or more DC:s using "**password server = dc1, dc2**" on oC-server1, "**password server = dc2, dc1**" on oC-server2...

Eventually in conjunction with both oC-servers, file servers and DC:s in the same AD site.

Sidenote: use of "hidden" oC-servers for SMB notifications/wnd:listener to take load off public web servers?



Areas of concern

Concerns/challenges

Is there a way to mitigate (the effects) NTLM?

Potential solutions:

3. Increase **MaxConcurrentApi**, see <https://support.microsoft.com/en-us/kb/2688798>

Enable **LsaLookupRestrictIsolatedNameLevel**, see <https://support.microsoft.com/en-us/kb/818024>, in certain Domain Trusts scenarios.

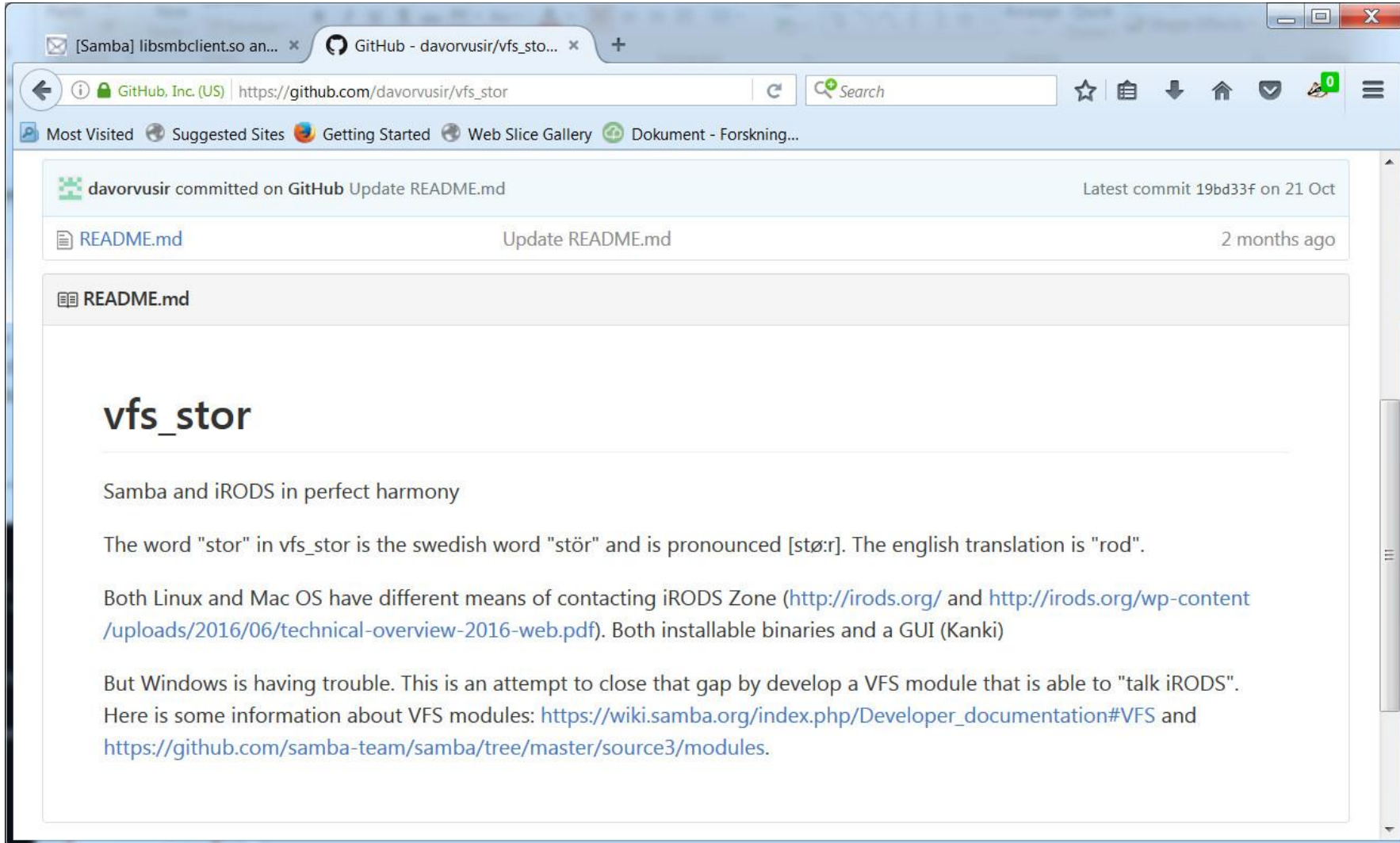


ALLVIS

Summary

1. Create a Global Name Space using both MS-DFS and NFS-gateway
2. Connect ownCloud-servers to DFS/NFS-GW and utilize referrals technology
3. Allows clients to use GNS to access and use the file shares for bulk ingest, continuous deposit from probes etc
4. Allows use of AD-groups for access and (re-)share control
 - a) Develop an oC-app that allows a user to edit group membership
5. Makes "Previous versions" an alternative to oC's file versions.
 - a) Develop an oC-app that enumerates VSS and presents the files
6. Dedicate oC-servers for SMB notifications
7. Make head room for excessive load from NTLM authentications
 - a) Dedicate domain controllers
 - b) Edit Windows Registry
 - c) Tweak /etc/samba/smb.conf

Windows and iRODS



[Samba] libsmbclient.so an... x GitHub - davorvusir/vfs_sto... x +

GitHub, Inc. (US) | https://github.com/davorvusir/vfs_stor Search

Most Visited Suggested Sites Getting Started Web Slice Gallery Dokument - Forskning...

davorvusir committed on GitHub Update README.md Latest commit 19bd33f on 21 Oct

README.md Update README.md 2 months ago

README.md

vfs_stor

Samba and iRODS in perfect harmony

The word "stor" in `vfs_stor` is the swedish word "stör" and is pronounced [stø:r]. The english translation is "rod".

Both Linux and Mac OS have different means of contacting iRODS Zone (<http://irods.org/> and <http://irods.org/wp-content/uploads/2016/06/technical-overview-2016-web.pdf>). Both installable binaries and a GUI (Kanki)

But Windows is having trouble. This is an attempt to close that gap by develop a VFS module that is able to "talk iRODS". Here is some information about VFS modules: https://wiki.samba.org/index.php/Developer_documentation#VFS and <https://github.com/samba-team/samba/tree/master/source3/modules>.

ALLVIS

Uppsala University official storage of scientific Data

Thank you!



Davor Vusir
davor.vusir@uadm.uu.se