

Centralising Authorization in PostgreSQL

Experimenting with LDAP synchronization

Structure of this talk...

- A summary of my experience with implementing a simple form of Centralized Authorisation
- A step by step approach

Authentication versus Authorisation

PostgreSQL LDAP Authentication

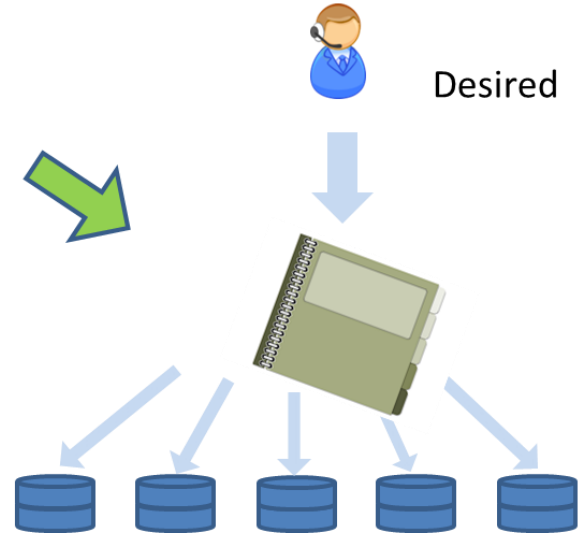
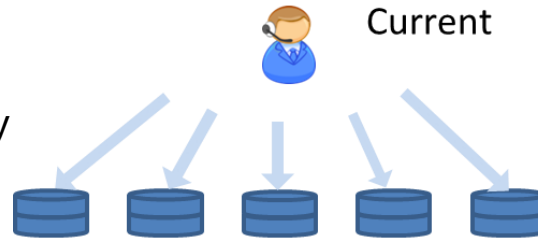
```
ldap ldapserver=servername.ad.company.au ldaptls=1  
ldapbasedn="ou=AU,dc=ad,dc=company,dc=au" ldapbinddn="cn=Gary  
Evans,ou=consultant,ou=ThirdParty Contractors,ou=Users,  
ou=AU,dc=ad,dc=corelogic,dc=asia" ldapbindpasswd="<the password>"  
ldapsearchattribute=sAMAccountName
```

Benefits of a centralized approach

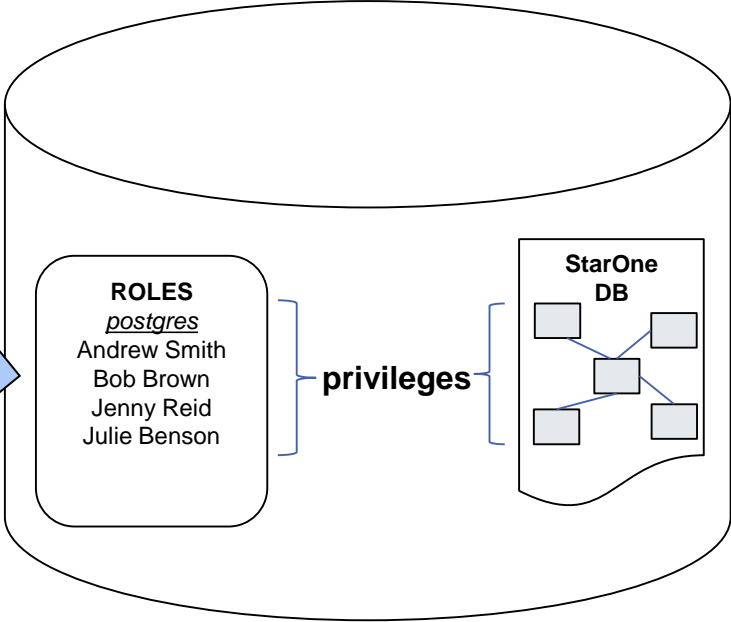
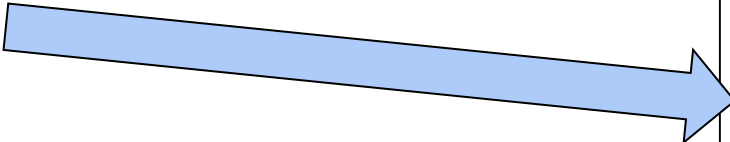
- Single point of control of database users

- Adding a user can be done by help desk

- Less error prone

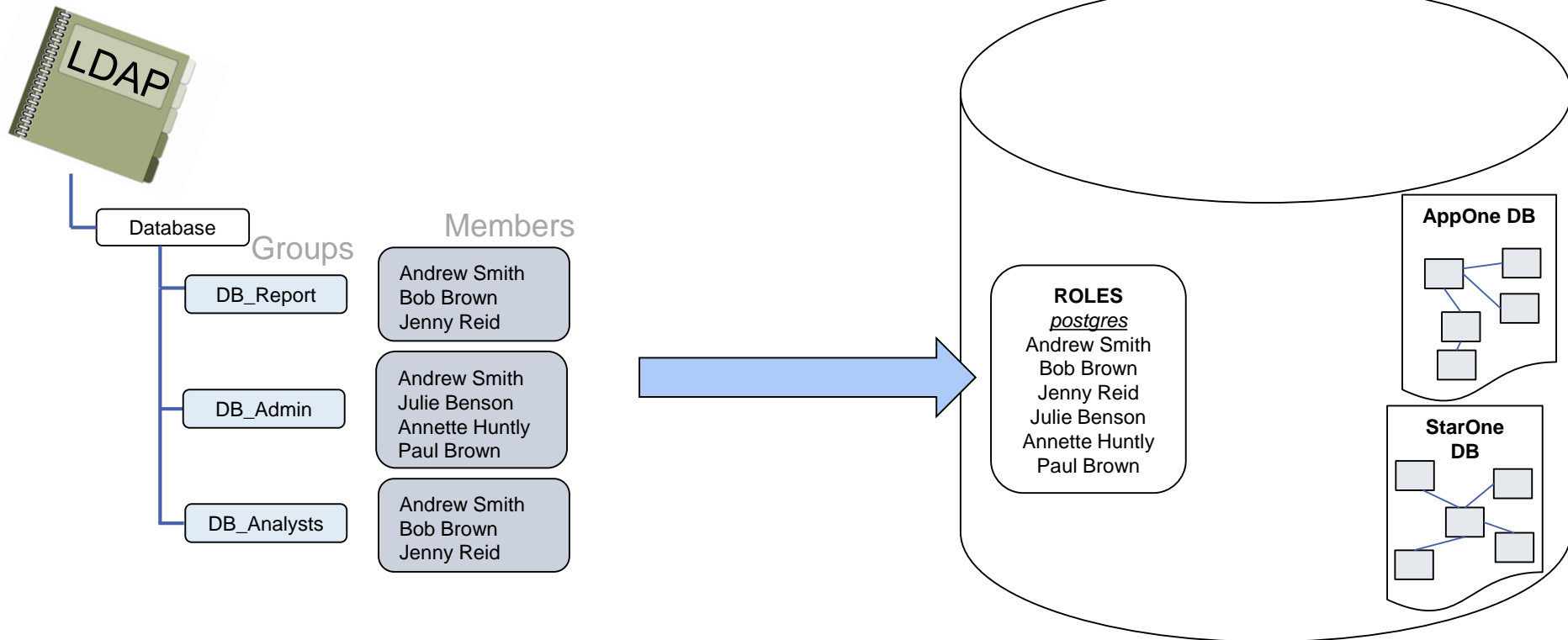


Synchronisation Approach

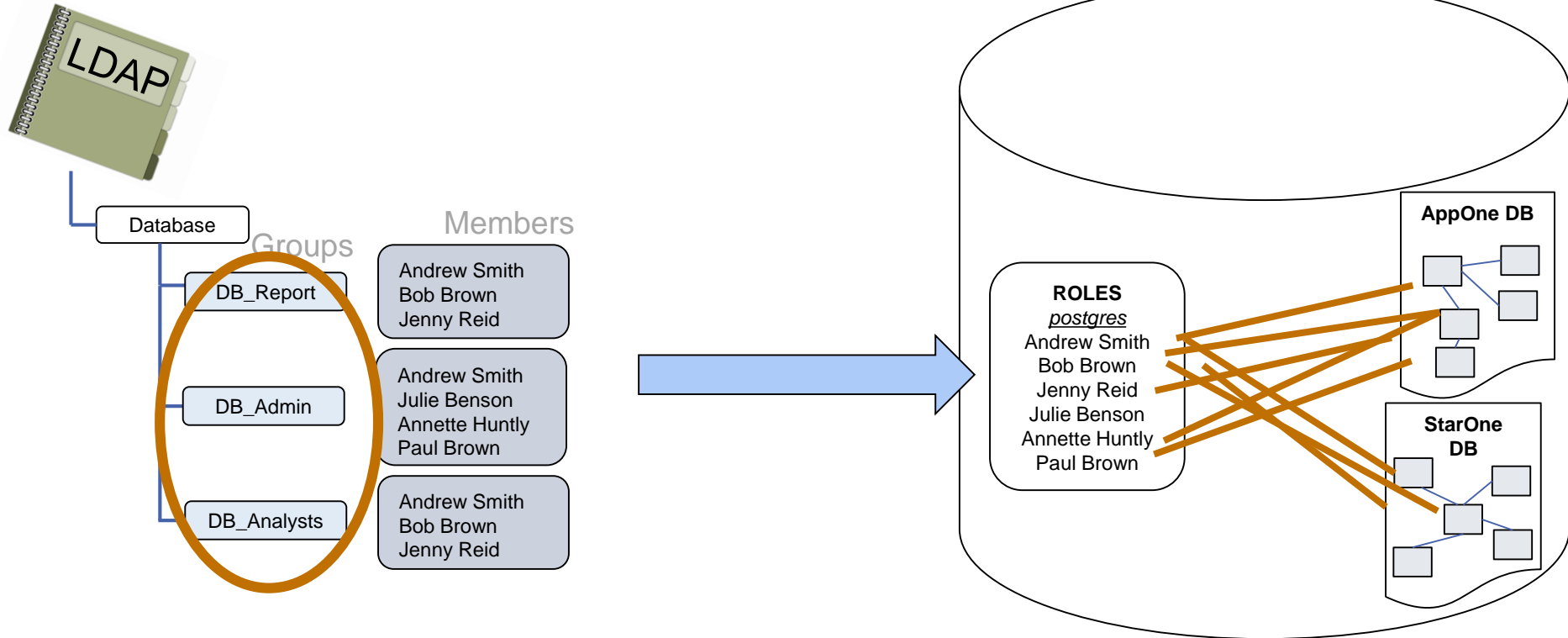


```
ldapsearch -Z -LLL -h ldapservername -D
gevans@ldapservername -w password
-b dc=ad,dc=companyname,dc=aus
'(&(objectClass=user)(memberOf=CN="${ADRow[0]}"
,OU=SQL,OU=Groups,OU=AU,DC=ad,DC=ccompany
name,DC=aus))' sAMAccountName |
sed -e 's/sAMAccountName: \([a-zA-Z]*\)^1/;tx;d;:x'
```

Synchronisation Approach

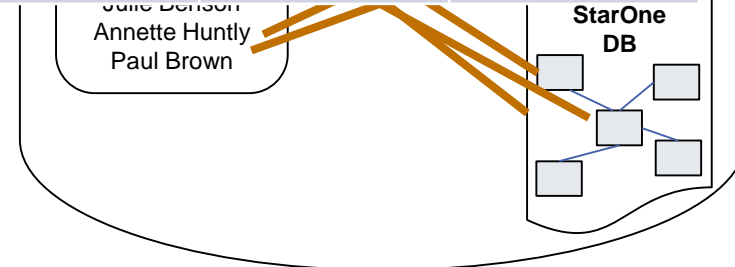
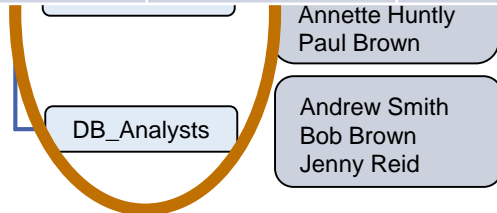


Synchronisation Approach



Synchronisation Approach

ID	Hostname	Dbname	ADGroup	Dbrole	Enabled	CRUD
1	Serverone	AppOne	DB_Report	Read_only	True	F,T,F,F
2	Serverone	StarOne	DB_Report	Reporting	True	F,T,T,F
3	Serverone	AppOne	DB_Admin	Admin_user	True	T,T,T,T
4	Serverone	StarOne	DB_Analysts	Analyst	True	F,T,F,F
5						



Synchronisation Approach

```
{PSQL} ${DBMONITOR//HOST/localhost}/schemaname -qtAX --field-separator ' '\
-c "SELECT distinct adgroup FROM mapping WHERE enabled = true and hostname='${hostname}'" |
while read -a ADRow ; do
    for adname in $(ldapsearch -Z -LLL -h ldapservername -D gevans@ldapservername -w password -b
dc=ad,dc=companyname,dc=aus
'(&(objectClass=user)(memberOf=CN="${ADRow[0]}",OU=SQL,OU=Groups,OU=AU,DC=ad,DC=companyname,DC=aus))' sAMAccountName | sed -e 's/sAMAccountName: \([a-zA-Z]*\)\/1;/tx;d;:x')
    do
        {PSQL} ${PGMONITOR//HOST/$hostname}/ schemaname -qtAX --field-separator ' '\
        -c "CREATE ROLE ${adname} with LOGIN;"

        {PSQL} ${PGMONITOR//HOST/localhost}/ schemaname -qtAX --field-separator ' '\
        -c "SELECT distinct dbrole FROM mapping where enabled = true and
        hostname='${hostname}' and adgroup = '${adname}' | while read -a DBRRow ; do

            {PSQL} ${PGMONITOR//HOST/$hostname}/performance -qtAX --field-separator ' '\
            -c "GRANT ${DBRRow} TO ${adname};"

        done
    done
done
```

Synchronisation Approach

```
{PSQL} ${DBMONITOR//HOST/localhost}/schemaname -qtAX --field-separator ' '\
-c "SELECT distinct adgroup FROM mapping WHERE enabled = true and hostname='${hostname}' |
while read -a ADRow ; do

    for adname in $(ldapsearch -Z -LLL -h ldapservername -D gevens@ldapservername -w password -b
dc=ad,dc=companyname,dc=aus
'(&(objectClass=user)(memberOf=CN="${ADRow[0]}",OU=SQL,OU=Groups,OU=AU,DC=ad,DC=ccompanyname,DC=aus))' sAMAccountName | sed -e 's/sAMAccountName: \([a-zA-Z]*\)\/1;/tx;d;:x')

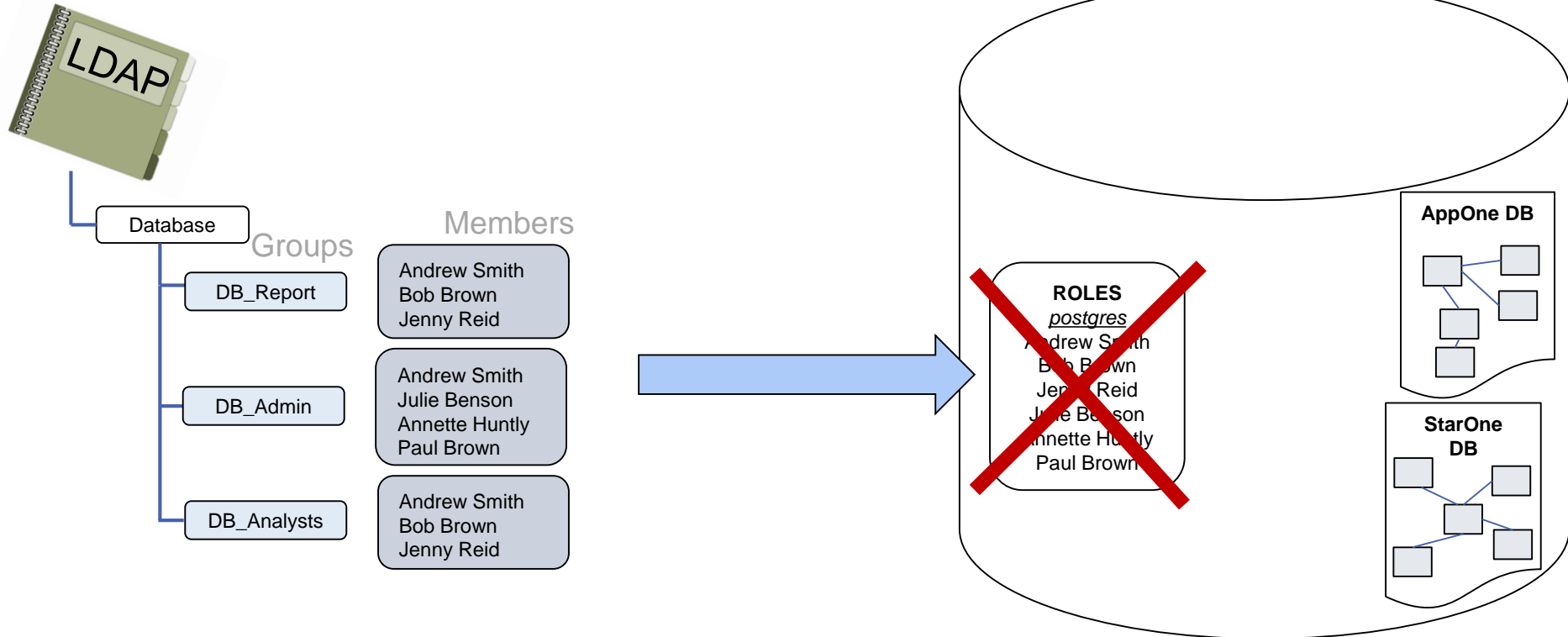
    do
        {PSQL} ${PGMONITOR//HOST/$hostname}/schemaname -qtAX --field-separator ' '\
        -c "CREATE ROLE ${adname} with LOGIN;"

        {PSQL} ${PGMONITOR//HOST/localhost}/performance -qtAX --field-separator ' '\
        -c "SELECT distinct dbrole FROM mapping where enabled = true and
hostname='${hostname}' and adgroup = '${adname}' | while read -a DBRRow ; do

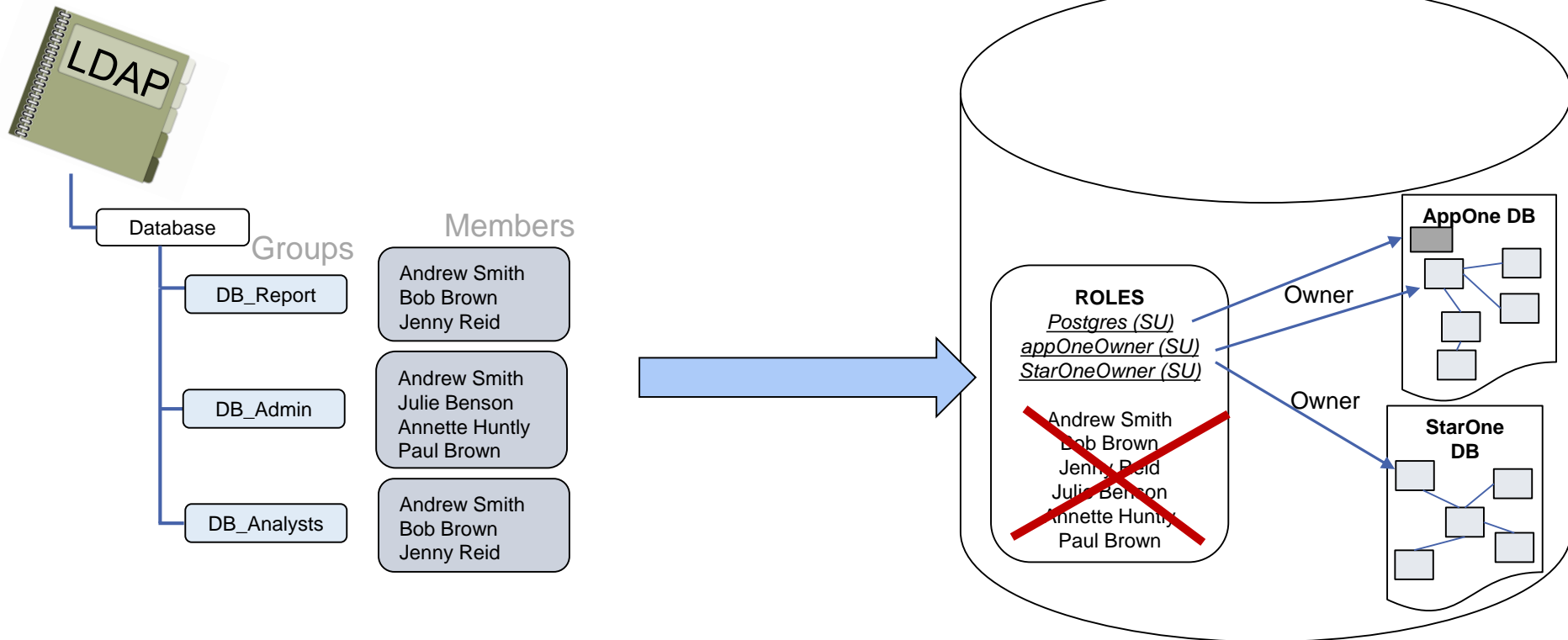
            {PSQL} ${PGMONITOR//HOST/$hostname}/schemaname -qtAX --field-separator ' '\
            -c "GRANT ${DBRRow} TO ${adname};"

        done
```

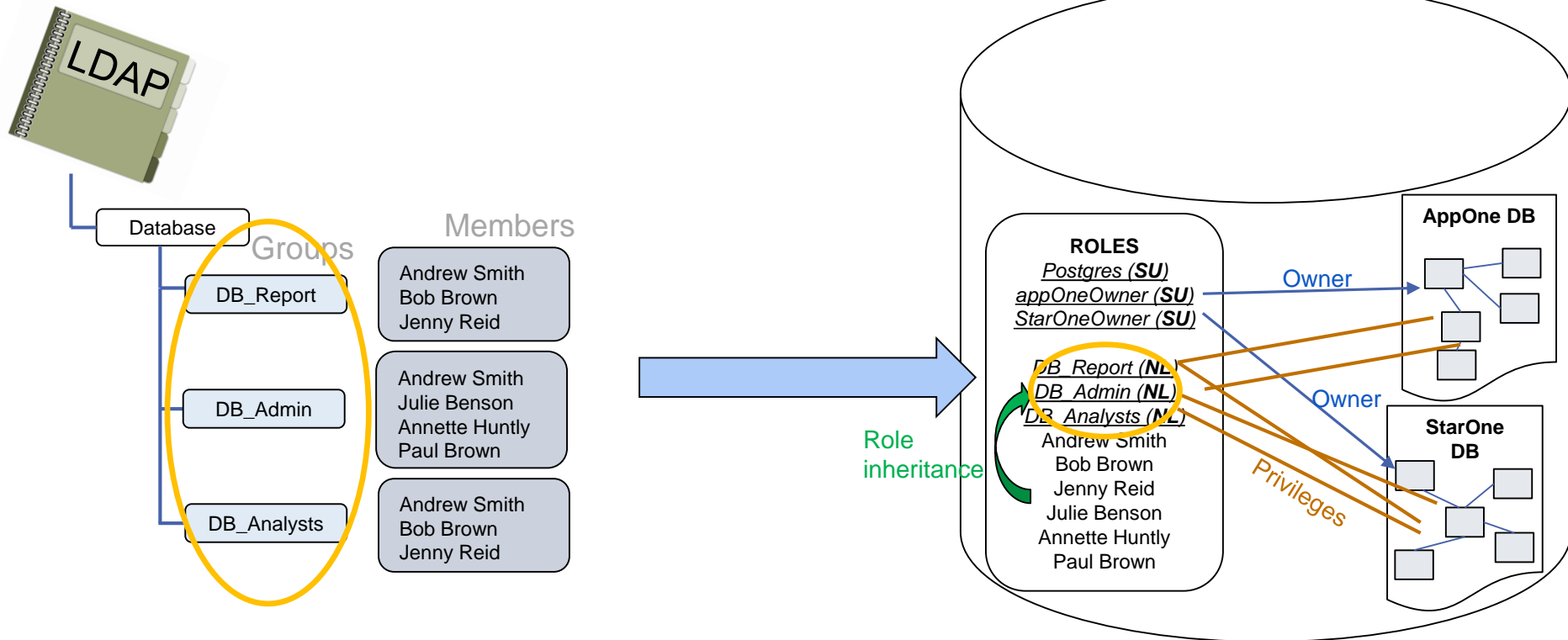
Synchronisation Approach



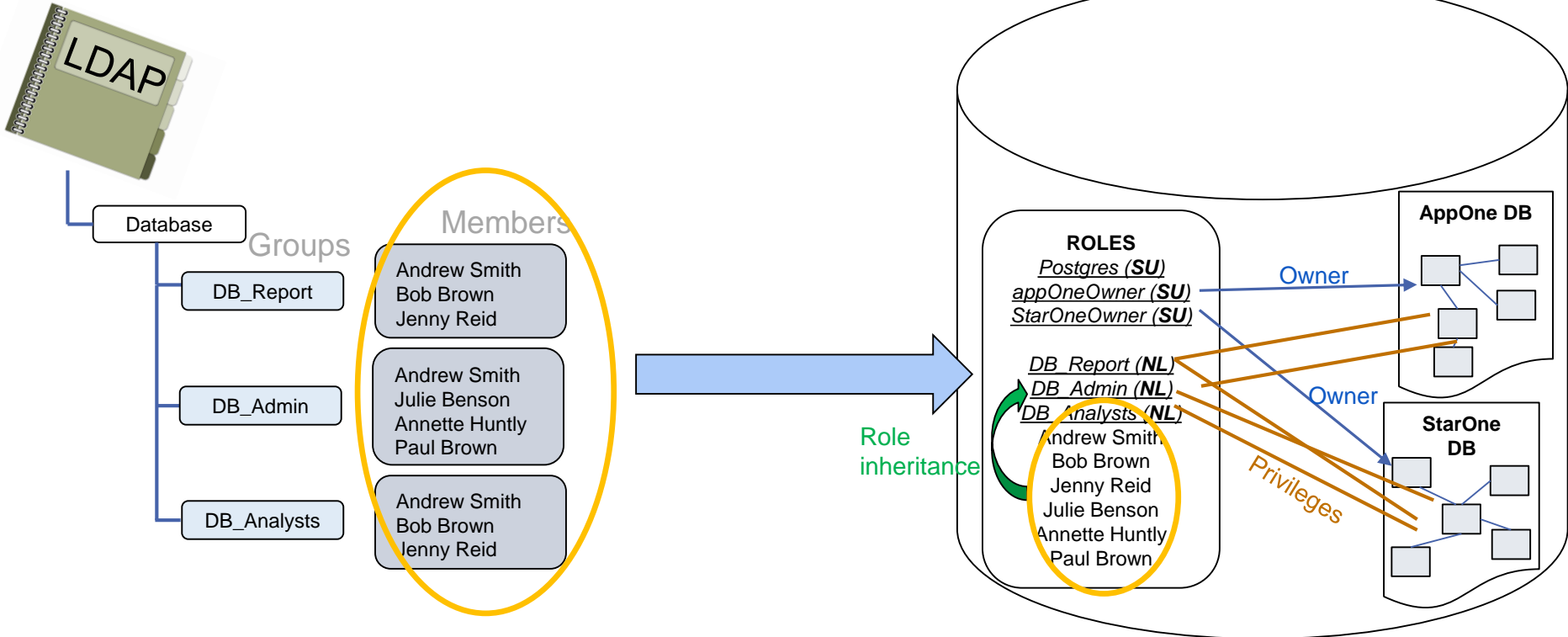
Synchronisation Approach



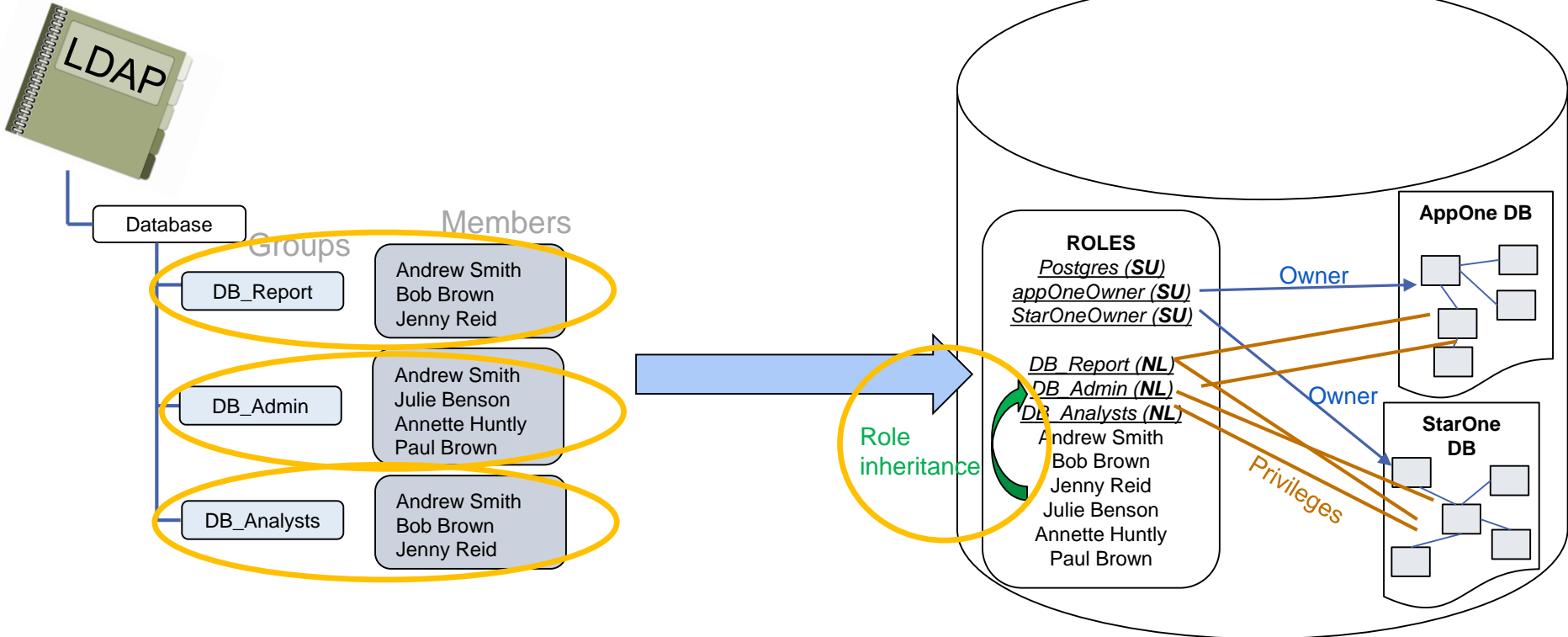
Synchronisation Approach



Synchronisation Approach



Synchronisation Approach



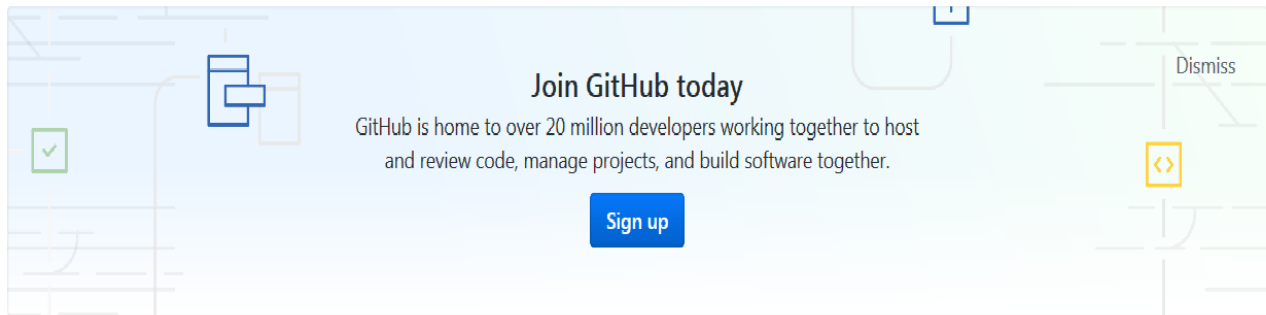
Existing tool

Pg-ldap-sync

larskanis / pg-ldap-sync

Watch 5 Star 50 Fork 13

Code Issues 5 Pull requests 1 Projects 0 Insights



Dismiss

Join GitHub today

GitHub is home to over 20 million developers working together to host and review code, manage projects, and build software together.

Sign up

Use LDAP permissions in PostgreSQL <http://github.com/larskanis/pg-ldap-sync>

47 commits 1 branch 2 releases 1 contributor

Branch: master New pull request Find file Clone or download

larskanis Update README.rdoc Latest commit 55b3e31 on Jan 14, 2016