



# Group Policy Integration





# Task

# Project Goals

- Provide seamless Active Directory domain integration.
- Design and implement graphical interfaces with familiar look to Windows administrators.
- Be portable across multiple architectures like AMD64 machines, Raspberry Pi 3&4 and Baikal machines (Aarch64), Elbrus (e2k VLIW), YADRO (POWER), MIPS and others.

P. S.: e2k is a very exotic platform where is a few new programming language compilers exist. For example, there is no Golang compiler at the moment.



# The Beginning: «GPO applier»

The project started at the end of 2019 and looked like: «Hey, we want to read zeros and ones from Registry.pol file in GPOs and perform some actions. Let's write the PoC and present it to the team». The resulting project is called GPOA and is located here: <https://github.com/altlinux/gpupdate>



# The Beginning: «GPO applier»

```
root@clw0: /root
Файл Действия Правка Вид Справка
nir  nir@comp-core-i7-...eb053d: /home/nir  root@clw0: /root
clw0 ~ # LC_ALL=C gpoa --loglevel 0 administrator
2021-05-05 14:59:27.215|[D00001]| The GPOA process was started for user|{"username": "root", "uid": 0
2021-05-05 14:59:27.215|[D00015]| Username for frontend is determined|{"username": "administrator"}
2021-05-05 14:59:27.215|[D00003]| Initializing plugin manager|{}
2021-05-05 14:59:27.216|[W00005]| ADP package is not installed - plugin will not be initialized|{}
2021-05-05 14:59:27.865|[D00018]| Found AD domain via CLDAP query|{"domain": "domain.alt"}
2021-05-05 14:59:27.865|[D00009]| Initializing Samba backend for domain|{"domain": "domain.alt"}
2021-05-05 14:59:27.897|[D00017]| Kerberos ticket check succeed|{"output": "Ticket cache: FILE:/var/c
\nValid starting Expires Service principal\n05/05/21 14:59:27 05/06/21 00:59:27 krbt
2021-05-05 14:59:27.915|[D00019]| Setting info|{"varname": "domain", "value": "domain.alt"}
2021-05-05 14:59:27.919|[D00021]| Set operational SID|{"sid": "S-1-5-21-3312666625-3281714301-2478023
2021-05-05 14:59:27.919|[D00019]| Setting info|{"varname": "machine_name", "value": "CLW0$"}
2021-05-05 14:59:27.920|[D00019]| Setting info|{"varname": "machine_sid", "value": "S-1-5-21-33126666
2021-05-05 14:59:27.923|[D00021]| Set operational SID|{"sid": "S-1-5-21-3312666625-3281714301-2478023
2021-05-05 14:59:27.923|[D00020]| Initializing cache|{"cache_file": "sqlite:///var/cache/gpupdate/re
2021-05-05 14:59:27.926|[D00020]| Initializing cache|{"cache_file": "sqlite:///var/cache/gpupdate/gp
2021-05-05 14:59:27.928|[D00007]| Cache directory determined|{"cachedir": "/var/cache/samba"}
2021-05-05 14:59:28.565|[D00045]| GPO update started|{}
2021-05-05 14:59:28.565|[D00048]| Establishing connection with AD DC|{}
2021-05-05 14:59:28.619|[D00047]| Retrieving list of GPOs to replicate from AD DC|{}
2021-05-05 14:59:28.632|[I00001]| Got GPO list for username|{"username": "CLW0$"}
2021-05-05 14:59:28.632|[I00002]| Got GPO|{"gpo_name": "Local Policy", "gpo_uid": "Local Policy"}
2021-05-05 14:59:28.632|[I00002]| Got GPO|{"gpo_name": "Default Domain Policy", "gpo_uid": "{31B2F34
2021-05-05 14:59:28.632|[I00002]| Got GPO|{"gpo_name": "AD GPO Test - Allow Login", "gpo_uid": "{4A6
2021-05-05 14:59:28.633|[D00049]| Started GPO replication from AD DC|{}
2021-05-05 14:59:28.733|[D00050]| Finished GPO replication from AD DC|{}
2021-05-05 14:59:28.733|[D00046]| GPO update finished|{}
2021-05-05 14:59:28.734|[D00025]| Re-caching Local Policy|{}
2021-05-05 14:59:28.734|[D00036]| Loading PReg from XML|{"polfile": "/usr/share/local-policy/default/
2021-05-05 14:59:28.740|[D00024]| Looking for preference in machine part of GPT|{"setting": "shortcut
```

# Privilege escalation problems

The next project was:

<https://github.com/altlinux/oddjob-gpupdate>

The goal of the project was to allow any user to trigger GPO update for machine. It is a D-Bus service which triggers the actual GPO «applier».

# Local settings

The last repository developed is:  
<https://github.com/altlinux/local-policy>

Which is a distribution-specific «Default Policy» templates. They are needed to establish default distribution settings «The Samba Way».

We also have a set of distro-specific ADMX/ADML files:  
<https://github.com/altlinux/admx-basealt>



# GUI for Domain: Design Approaches

Despite numerous requests to implement Web UI we've decided to do it the classic way: C++ with Qt5. The rationale behind this decision was:

- No need to setup web server and database.
- Kerberos tickets are stored on operator's machine.
- Ability to look like RSAT.





# «Domain Editor» GUI (ADMC)

It all started from: «Now we can somehow apply GPOs. Let's try to implement LDAP editor for Samba database!»

There was a need for secure and easy UI to edit users and machines, assign GPOs and search for various elements. The project started at the beginning of 2020 and, after a year of efforts, it is located at:

<https://github.com/altlinux/admc>

The project had the goal to rethink the design approach behind RSAT and don't try to implement the software 1 to 1. We tried to make it as simple and effective as possible.



# «Domain Editor» GUI (ADMC)

The screenshot shows the ADMC (Active Directory Management Console) interface. The window title is "ADMC". The menu bar includes "File", "Action", "Navigation", "View", "Preferences", and "Help". The left pane shows a tree view of the domain structure, with "Users" selected. The main pane displays a table of 19 objects.

Users: 19 objects

Name	Class	Description	Distinguished name
Administrator	User	Built-in account f...	CN=Administrator,CN=Users,DC=domain,DC=alt
Allowed RO...	Security Group - ...	Members in this ...	CN=Allowed RODC Password Replication Group,CN=User...
Cert Publis...	Security Group - ...	Members of this ...	CN=Cert Publishers,CN=Users,DC=domain,DC=alt
Denied RO...	Security Group - ...	Members in this ...	CN=Denied RODC Password Replication Group,CN=Users...
DnsAdmins	Security Group - ...	DNS Administrat...	CN=DnsAdmins,CN=Users,DC=domain,DC=alt
DnsUpdate...	Security Group - ...	DNS clients who ...	CN=DnsUpdateProxy,CN=Users,DC=domain,DC=alt
Domain Ad...	Security Group - ...	Designated admi...	CN=Domain Admins,CN=Users,DC=domain,DC=alt
Domain Co...	Security Group - ...	All workstations ...	CN=Domain Computers,CN=Users,DC=domain,DC=alt
Domain Co...	Security Group - ...	All domain contr...	CN=Domain Controllers,CN=Users,DC=domain,DC=alt
Domain Gu...	Security Group - ...	All domain guests	CN=Domain Guests,CN=Users,DC=domain,DC=alt
Domain Users	Security Group - ...	All domain users	CN=Domain Users,CN=Users,DC=domain,DC=alt
Enterprise ...	Security Group - ...	Designated admi...	CN=Enterprise Admins,CN=Users,DC=domain,DC=alt
Enterprise ...	Security Group - ...	Members of this ...	CN=Enterprise Read-only Domain Controllers,CN=Users,...
Group Polic...	Security Group - ...	Members in this ...	CN=Group Policy Creator Owners,CN=Users,DC=domain,...
Guest	User	Built-in account f...	CN=Guest,CN=Users,DC=domain,DC=alt
RAS and IA...	Security Group - ...	Servers in this gr...	CN=RAS and IAS Servers,CN=Users,DC=domain,DC=alt
Read-only ...	Security Group - ...	Members of this ...	CN=Read-only Domain Controllers,CN=Users,DC=domai...
Schema Ad...	Security Group - ...	Designated admi...	CN=Schema Admins,CN=Users,DC=domain,DC=alt
adgpotest	User		CN=adgpotest,CN=Users,DC=domain,DC=alt

Ready



## WIP: GPO Editor

Our team is working on GPO editor with ADMX file support. The technological stack is similar to ADMC: C++ and Qt5.



# Future Plans

# World-Conquering Plans

- Merge GPO «applier» code into Samba upstream.
- Implement bindings for Samba registry. samba-regedit is a nice utility.
- Release first GPO editor UI.
- Implement FreeIPA domain integration and policy application.



**Contacts**

Тел.: +7 (495) 123-47-99

[basealt.ru](http://basealt.ru)

E-mail: [sales@basealt.ru](mailto:sales@basealt.ru)

**Offices:**

Moscow,  
75 Butyrskaya street

Saint-Petersburg,  
27 Kolomyazhskiy prospect

Saratov,  
44A Oktyabrskaya street

Obnynsk,  
45 Korolyova street