GPOs from source

GPO as code, GPO Ops

SambaXP 2026

Kees van Vloten

About me

Kees van Vloten

- Freelancer in infrastructure automation
- Using Samba in infrastructure since the 90’s
- Started in 2020 with integrations on Samba-AD

Agenda

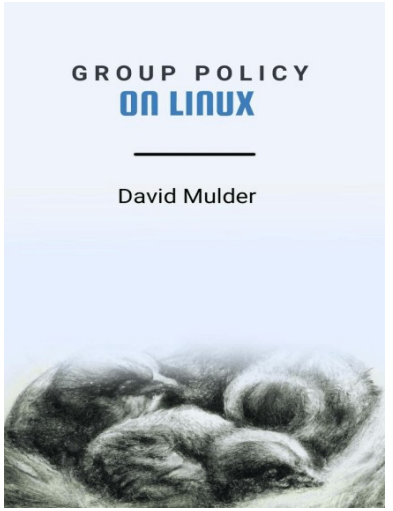
- History, today
- Why from source?
- Components of a GPO
- Achievements
- Questions

History

- Early implementations used netlogon share
  - Windows 9x/me: `config.pol`
  - Windows NT4: `ntconfig.pol`
- Current style GPOs exist since Windows 2000
- Evolved a lot since
  - Formats changed
  - Components were added
  - Client-side extensions

Today / challenges

- Dispersed storage:
  - Files in multiple formats
  - LDAP records
  - Permissions
- Not well documented, but:
  - Fragmented online sources
  - David Mulder
  - Reverse engineering



Why from source?

- Backup
- Versioning
- GPOs portable over domains
- Identify GPOs by name (not by uuid)
- Documentation

Components of a GPO

- Filesystem
  - directories
  - .ini / .inf-files
  - .xml-files
  - registry.pol files
- LDAP
  - GPO, 3 records
  - WMI, 1 record (optional)
- Permissions
  - Link to LDAP object
  - Permissions in filesystem and LDAP

Filesystem

- `Sysvol` share in `Policies`
- GPO directory `{<uuid>}`
- Subdirs for `machine` for `user` files
- Some settings in `GPT.ini`

Filesystem - ini files

- UTF-16, CR-LF newlines
- File extension .ini, .inf (others?)

```
[Unicode]
Unicode=yes
[Version]
signature="$CHICAGO$"
Revision=1
[Registry Values]
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount=1,"0"
```

- Directory requirement, even empty dirs

```
{C14317E3-D51B-47AA-83A9-33D0B0764EE4}
{C14317E3-D51B-47AA-83A9-33D0B0764EE4}/User
{C14317E3-D51B-47AA-83A9-33D0B0764EE4}/Machine
{C14317E3-D51B-47AA-83A9-33D0B0764EE4}/Machine/Scripts
{C14317E3-D51B-47AA-83A9-33D0B0764EE4}/Machine/Scripts/Startup
{C14317E3-D51B-47AA-83A9-33D0B0764EE4}/Machine/Scripts/Shutdown
{C14317E3-D51B-47AA-83A9-33D0B0764EE4}/Machine/Microsoft
{C14317E3-D51B-47AA-83A9-33D0B0764EE4}/Machine/Microsoft/Windows NT
{C14317E3-D51B-47AA-83A9-33D0B0764EE4}/Machine/Microsoft/Windows NT/SecEdit
{C14317E3-D51B-47AA-83A9-33D0B0764EE4}/Machine/Microsoft/Windows NT/SecEdit/GptTmpl.inf
{C14317E3-D51B-47AA-83A9-33D0B0764EE4}/GPT.INI
```

- Specific client-side extensions in LDAP
- GPMC: hardcoded UI

Filesystem - xml files

- UTF-8, LF newlines
- File extension .xml
- Changed date requirement

```
<?xml version="1.0" encoding="utf-8"?>
<NTServices clsid="{2CFB484A-4E96-4b5d-A0B6-093D2F91E6AE}">
    <NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}"
               name="CscService"
               image="4"
               changed="2026-04-14 10:48:40"
               uid="{FD6EE9C7-0DA3-465A-ADC9-E4D8957F607A}">
        <Properties startupType="DISABLED" serviceName="CscService" timeout="30"/>
    </NTService>
</NTServices>
```

- Directory requirement

```
{0CC52383-DEE7-494A-8AD9-C7AAD7760BA8}
{0CC52383-DEE7-494A-8AD9-C7AAD7760BA8}/User
{0CC52383-DEE7-494A-8AD9-C7AAD7760BA8}/Machine
{0CC52383-DEE7-494A-8AD9-C7AAD7760BA8}/Machine/Preferences
{0CC52383-DEE7-494A-8AD9-C7AAD7760BA8}/Machine/Preferences/Services
{0CC52383-DEE7-494A-8AD9-C7AAD7760BA8}/Machine/Preferences/Services/Services.xml
{0CC52383-DEE7-494A-8AD9-C7AAD7760BA8}/GPT.INI
```

- Specific client-side extensions in LDAP
- GPMC: hardcoded UI

Filesystem – registry.pol

- Binary registry file
- Simple directory tree

```
{2BC07843-D60D-444E-972A-C23A62A0203E}
{2BC07843-D60D-444E-972A-C23A62A0203E}/User
{2BC07843-D60D-444E-972A-C23A62A0203E}/User/Registry.pol
{2BC07843-D60D-444E-972A-C23A62A0203E}/Machine
{2BC07843-D60D-444E-972A-C23A62A0203E}/Machine/Registry.pol
{2BC07843-D60D-444E-972A-C23A62A0203E}/GPT.INI
```

- One client-side extension in LDAP:
  `[{35378EAC-683F-11D2-A89A-00C04FBBCFA2}`
  `{D02B1F72-3407-48AE-BA88-E8213C6761F1}]`
- GPMC flexible UI
- Properties from .admx, .adml files on sysvol share in:
  - .admx: `Policies/PolicyDefinions`
  - .adml: `Policies/PolicyDefinions/en-US`

Filesystem – registry.pol

- Samba-tool:
  - `samba-tool gpo load {<uuid>} -replace -content <file>`
  - `samba-tool gpo show {<uuid>}`
- Json:

```
[
    {
        "keyname": "Software\\Policies\\Microsoft\\Windows\\FileHistory",
        "valuename": "Disabled",
        "class": "MACHINE",
        "type": "REG_DWORD",
        "data": 1
    },
    {
        "keyname": "Software\\Microsoft\\Windows\\CurrentVersion\\WindowsBackup",
        "valuename": "DisableMonitoring",
        "class": "MACHINE",
        "type": "REG_DWORD",
        "data": 1
    }
]
```

Filesystem – GPT.INI

- UTF-16, CR-LF newlines
- Settings and version

```
[General]
Version=196613
displayName=gpo_windows-desktop_os_cached_credentials
```

- Version: 32-bits number
  - Machine policy: lower 16-bits (version 5)
  - User policy: upper 16-bits (version 3)
- Samba-tool shows display-name and version:
  - `samba-tool gpo show {<uuid>}`
  - `samba-tool gpo listall`

LDAP

- 3 GPO records:
  - Top-level record contains settings
  - DN: `CN={<uuid>},CN=Policies,CN=System,DC=samdom,DC=com`
  - Subs for `Machine` and `User`, merely placeholders

- 1 WMI-filter record (optional):
  - Contains code of WMI-filter
  - DN: `CN={<uuid>},CN=SOM,CN=WMIPolicy,CN=System,DC=samdom,DC=com`

LDAP - GPO

- GPO top-level record

```
dn: CN={B45B56F9-B730-4086-A8EC-0A162395BEF9},CN=Policies,CN=System,DC=virtualhosting,DC=lan
objectClass: top
objectClass: container
objectClass: groupPolicyContainer
cn: {B45B56F9-B730-4086-A8EC-0A162395BEF9}
instanceType: 4
whenCreated: 20260415133529.0Z
uSNCreated: 5810
showInAdvancedViewOnly: TRUE
name: {B45B56F9-B730-4086-A8EC-0A162395BEF9}
objectGUID: ec07743a-ebd4-4453-ad19-e353c6da98d1
objectCategory: CN=Group-Policy-Container,CN=Schema,CN=Configuration,DC=virtualhosting,DC=lan
displayName: gpo_demo_windows_os_cached_credentials
gPCFileSysPath: \\virtualhosting.lan\sysvol\virtualhosting.lan\Policies\{B45B56F9-B730-4086-A8EC-0A162395BEF9}
gPCFunctionalityVersion: 2
flags: 0
gPCMachineExtensionNames: [{827D319E-6EAC-11D2-A4EA-00C04F79F83A}{803E14A0-B4FB-11D0-A0D0-00A0C90F574B}]
gPCUserExtensionNames: [{35378EAC-683F-11D2-A89A-00C04FBBCFA2}{D02B1F72-3407-48AE-BA88-E8213C6761F1}]
versionNumber: 65537
gPCWQLFilter: [virtualhosting.lan;{0A8E728E-52A5-4D24-BF01-7A002E6BA7DE};0]
whenChanged: 20260415134039.0Z
uSNChanged: 5818
distinguishedName: CN={B45B56F9-B730-4086-A8EC-0A162395BEF9},CN=Policies,CN=System,DC=virtualhosting,DC=lan
```

- Samba-tool shows DN, flags, extensions:
  `samba-tool gpo show {<uuid>}`
- Ldbsearch shows GPO LDAP records:
  `ldbsearch -H /var/lib/samba/private/sam.ldb -b '<dn>'`

LDAP - WMI-filter

- WMI-filter record

```
dn: CN={0A8E728E-52A5-4D24-BF01-7A002E6BA7DE},CN=SOM,CN=WMIPolicy,CN=System,DC=virtualhosting,DC=lan
objectClass: top
objectClass: msWMI-Som
cn: {0A8E728E-52A5-4D24-BF01-7A002E6BA7DE}
instanceType: 4
whenCreated: 20260415132913.0Z
uSNCreated: 5793
showInAdvancedViewOnly: TRUE
name: {0A8E728E-52A5-4D24-BF01-7A002E6BA7DE}
objectGUID: a4c5c3bb-f528-4d2b-8698-a4909d95bc94
objectCategory: CN=ms-WMI-Som,CN=Schema,CN=Configuration,DC=virtualhosting,DC=lan
msWMI-ID: {0A8E728E-52A5-4D24-BF01-7A002E6BA7DE}
msWMI-Name: wmi_win10
msWMI-Parm2: 1;3;10;84;WQL;root\CIMv2;select * from Win32_OperatingSystem where Version like "10.0.1%"
whenChanged: 20260415132914.0Z
uSNChanged: 5794
distinguishedName: CN={0A8E728E-52A5-4D24-BF01-7A002E6BA7DE},CN=SOM,CN=WMIPolicy,CN=System,DC=virtualhosting,DC=lan
```

- Ldbsearch shows all WMI-filter records:

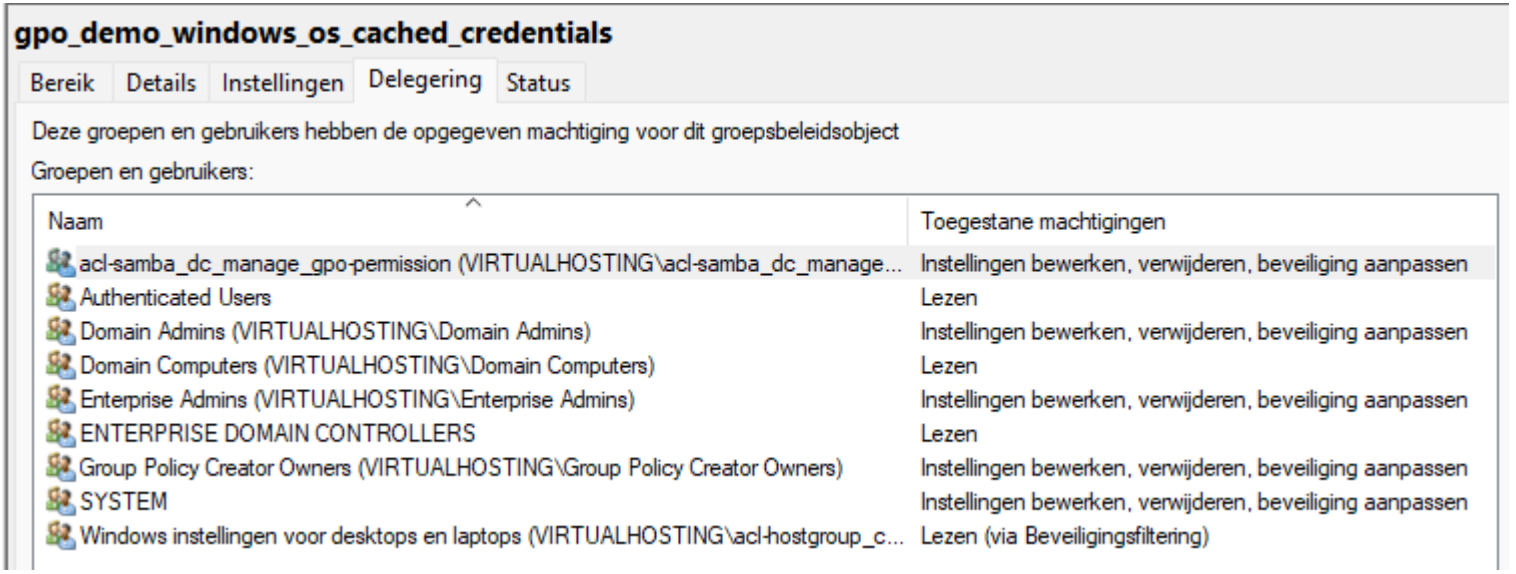
```
ldbsearch -H /var/lib/samba/private/sam.ldb -b
'CN=SOM,CN=WMIPolicy,CN=System,DC=samdom,DC=com'
```

Permissions

- Link:
  - Links GPO to an LDAP container
  - Sets the root of the GPO's scope
  - Samba-tool:
    `samba-tool gpo setlink <link-dn> {<uuid>}`
- Permissions:
  - Filesystem ACLs: delegation
  - LDAP ACLs: delegation + security filtering

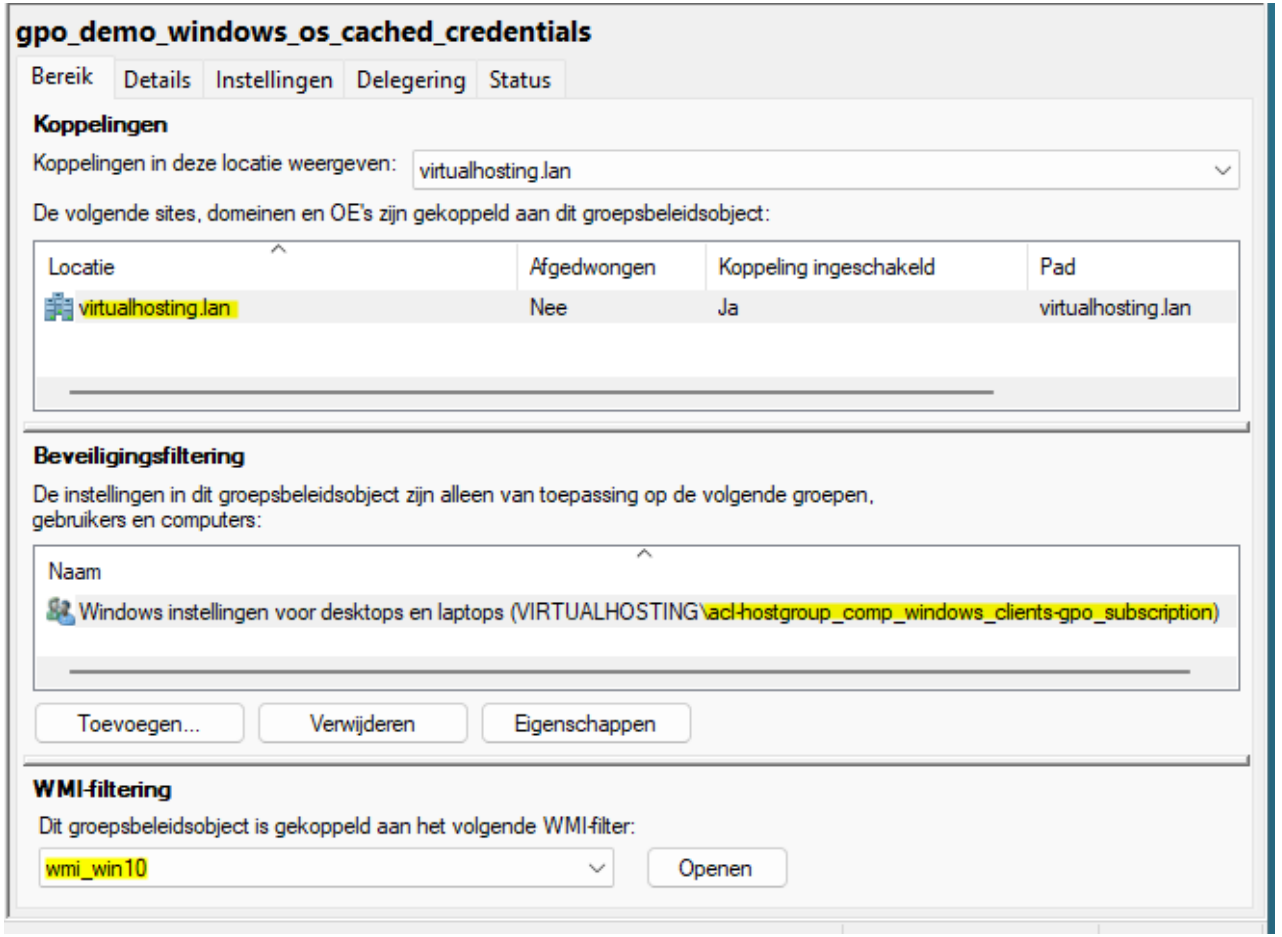
Permissions - delegation

- Who can read, edit, etc.
- LDAP- and filesystem ACLs identical
- GPMC:



Permissions - scope

- Scope = link + security filter + WMI
- GPMC:



Permissions - filesystem

- Apply GPO top-level with inheritance
- Posix-ACLs (`setfacl`) are insufficient for Windows
- Sysvol replication must support and trigger on acls, xattrs
- Use samba: `smbcacls //<dc-host>/sysvol -set --propagate-inheritance`
- Limitations of SMB on DC: `samba-tool ntacl sysvolreset`
- ACLs for smbcacls:

```
REVISION:1
OWNER:<netbios-name>\Domain Admins,
GROUP:<netbios-name>\Domain Admins,
ACL:CREATOR OWNER:ALLOWED/OI|CI|IO/FULL,
ACL:NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS:ALLOWED/OI|CI/READ,
ACL:NT AUTHORITY\Authenticated Users:ALLOWED/OI|CI/READ,
ACL:NT AUTHORITY\SYSTEM:ALLOWED/OI|CI/FULL,
ACL:<netbios-name>\Domain Admins:ALLOWED/OI|CI/FULL,
ACL:<netbios-name>\Enterprise Admins:ALLOWED/OI|CI/FULL,
ACL:<netbios-name>\Group Policy Creator Owners:ALLOWED/OI|CI/FULL,
<for group in security-filter-groups>
ACL:<netbios-name>\<group>:ALLOWED/OI|CI/READ,
<endfor>
```

Permissions - LDAP

- Apply GPO top-level DN
- Uses SDDL format
- Read ACLs: `samba-tool dsacl get -objecdn='<dn>'`
- Replace ACLs:

```
cat << EOF | ldbmodify -H /var/lib/samba/private/sam.ldb
dn: <dn>
changetype: modify
replace: nTSecurityDescriptor
nTSecurityDescriptor: <acls>
EOF
```

Get SID for each security-filter group:

```
ldbsearch -H /var/lib/samba/private/sam.ldb -s sub -b
'DC=samdom,DC=com' '(&(objectClass=group)(sAMAccountName=<group>))'
objectSid
```

Permissions - LDAP

- ACLs for ldbmodify:

```
O:DAG:DAD:PAR
(A;CI;CCDCLCSWRPWPDTLOSDRCWDWO;;;DA)(A;CI;CCDCLCSWRPWPDTLOSDRCWDWO;;;EA)
(A;CIIO;CCDCLCSWRPWPDTLOSDRCWDWO;;;CO)(A;;CCDCLCSWRPWPDTLOSDRCWDWO;;;DA)
(A;CI;CCDCLCSWRPWPDTLOSDRCWDWO;;;SY)
(A;CI;LCRPLORC;;;ED)
(A;CI;LCRPRC;;;<security-filter-sids[0]>)
(A;CI;LCRPRC;;;AU)
(A;CI;CCDCLCRPWPSDRCWDWO;;;PA)
<if len(security-filter-sids)== 1>
(A;CI;LCRPRC;;;DC)
<else>
<for security-filter-sid in security-filter-sids[1:]>
(A;CI;LCRPRC;;;<security_filter_sid>)
<endfor><endif>
<for security-filter-sid in security-filter-sids>
(OA;CI;CR;dacfd8f-ffb3-11d1-b41d-00a0c968f939;;<security-filter-sid>)
<endfor>
S:AI
(OU;CIIOIDSA;WP;f30e3bbe-9ff0-11d1-b603-0000f80367c1;
bf967aa5-0de6-11d0-a285-00aa003049e2;WD)
(OU;CIIOIDSA;WP;f30e3c00-9ff0-11d1-b603-0000f80367c1;
bf967aa5-0de6-11d0-a285-00aa003049e2;WD)
```

Achievements - pseudo code

```
Create wmi-filter: ldbmodify
Create gpo: samba-tool gpo create
Set smb acls:
    samba-tool ntacl sysvolreset
    smbcacls <dc-host>/sysvol<gpo-root-dir> --set

Create dirs: smbclient <dc-host>/sysvol -c ‘mkdir <path>’

If ini-file:
    Convert: todos;iconv -f utf-8 -t utf-16
    Upload: smbclient <dc-host>/sysvol -c ‘put <file>’

If xml-file:
    Insert change-date in xml-file
    Upload: smbclient <dc-host>/sysvol -c ‘put <file>’

If regpol-file:
    samba-tool gpo load {<uuid>} -replace -content <json-file>

Update ldap:
    Attributes: ldbmodify client-extensions, flags, wmi-filter
    Permissions: ldbmodify nTSecurityDescriptor

Increase version number:
    In gpt.ini like ini-file
    In ldap: ldbmodify versionNumber

Link GPO: samba-too gpo setlink <link-dn> {<uuid>}
```

Achievements

- Specification file:
  - Combine security-filter groups to gpo descriptions
- Files / templates:
  - Ini-files, xml-files, registry.pol.json files
  - Optionally as jinja2 template
- Variables:
  - Variables for template rendering
- Implementation of the pseudo code
- Store in git

Thank you

- Questions?

- Reach out via:
  - Github: https://github.com/kvvloten
  - Linked-in: https://linkedin.com/in/keesvanvloten/
  - Email: keesvanvloten@gmail.com