Storage Management with Active Directory Group Policies

Introduction

- Aimed at developers of storage-based products
- Covers information that will help implementors leverage existing Active Directory infrastructure

Nomenclature

- Client – a CIFS domain member, including a storage device

Why Group Policies?

- Distributed
- Some existing user familiarity
- Configuration can be global and granular
- Extensible

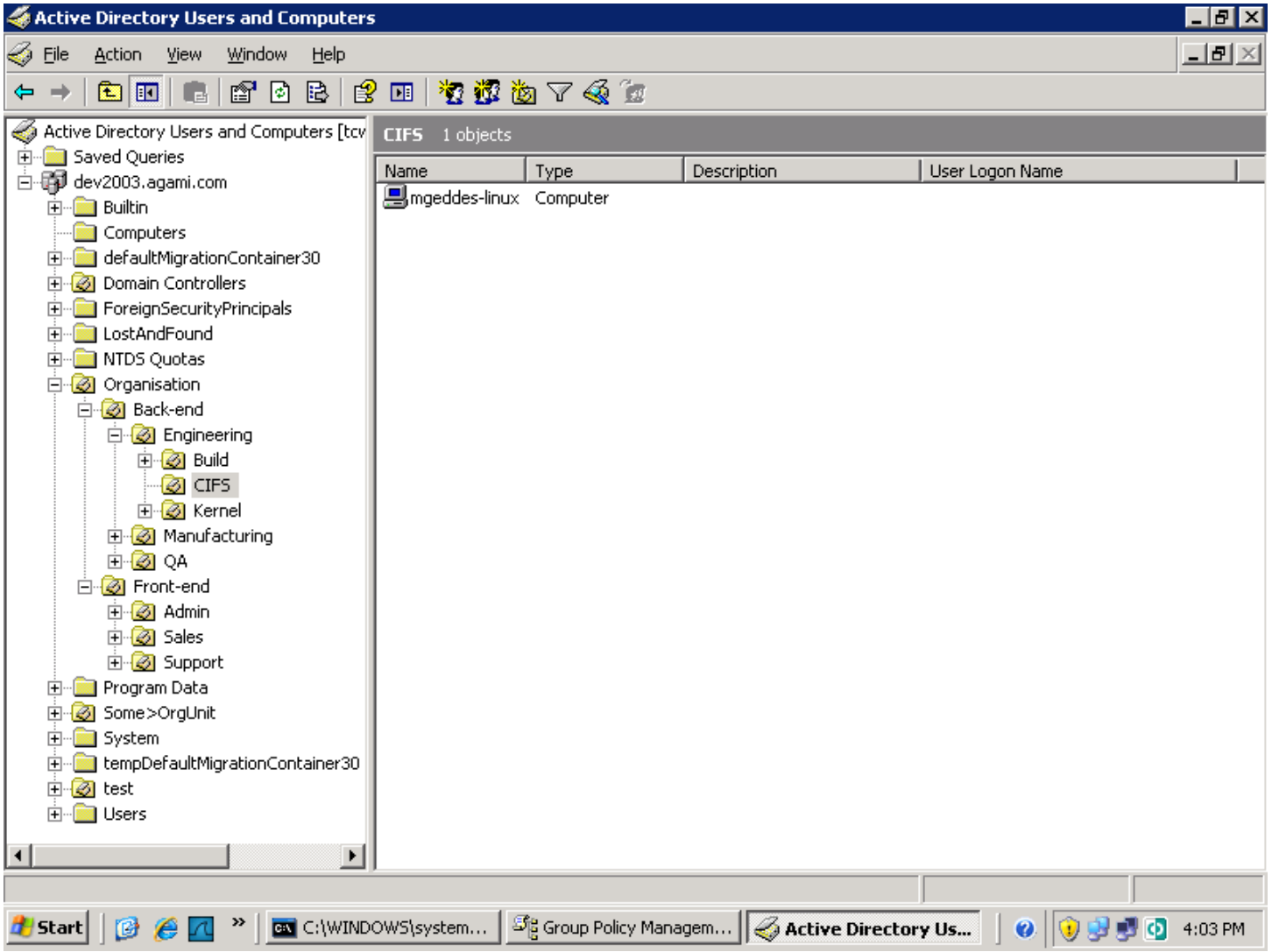
Group Policies Overview

- Essentially a set of parameters and registry entries applied to client machines

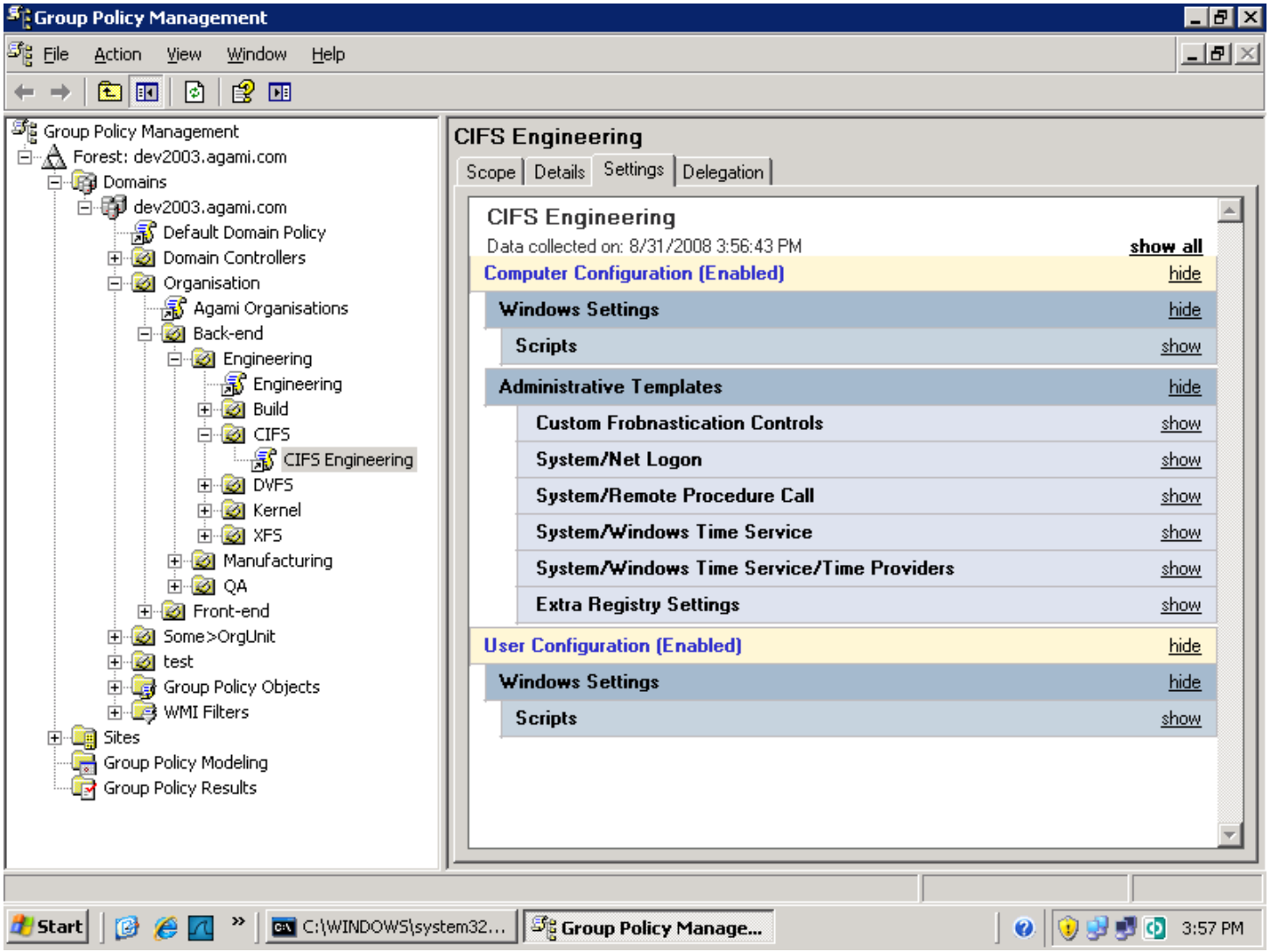
Group Policies Overview

- Administrator creates Group Policy Objects
  - Stored on domain controllers
  - Created from parameters defined in template files
- Administrator links objects to organizationalUnits (OUs) in Active Directory

Group Policies Overview



Group Policies Overview



Group Policies Overview

- Client queries Active Directory (over LDAP) for list of relevant Group Policies links
- Client retrieves matching Group Policies Objects from DC(s)
- Client applies configuration locally

LDAP Queries

- Find default naming context to use as base DN
- Query all entries down to machine account. Applied in order from root to machine account:
  - Eg: cn=somehost,ou=Computers,dc=snia,dc=org
- Looking for *gPLink* attribute

LDAP Queries

- Each *gPLink* returned is a *distinguishedName* (*DN*)
- For each *gPlink*, retrieve entry's *gPCFileSysPath* attribute
- *gPCFileSysPath* is a UNC path to group policy objects on DCs' SYSVOL share

gPLink

dn: OU=CIFS, OU=Engineering, OU=Backend, OU=Organisation, DC=dev200
DC=agami,DC=com
objectClass: top
objectClass: organizationalUnit
ou: CIFS
name: CIFS
objectGUID:: iM/wwrq4NkuLyfPfV1i7aQ==
objectCategory: CN=Organizational-
Unit,CN=Schema,CN=Configuration,DC=dev2003,DC=agami,DC=com
gPLink: [LDAP://cn={ECFD9B0F-129F-413C-9021-
F7C087B4F084},cn=policies,cn=system,DC=dev2003,DC=agami,DC=com;
]

gPCFileSysPath

dn: CN={ECFD9B0F-129F-413C-9021-F7C087B4F084},CN=Policies,CN=System,DC=dev2003,DC=agami,DC=com
objectClass: groupPolicyContainer
cn: {ECFD9B0F-129F-413C-9021-F7C087B4F084}
displayName: CIFS Engineering
gPCFunctionalityVersion: 2
gPCFileSysPath: \\dev2003.agami.com\SysVol\dev2003.agami.com\Policies\{ECFD9B0F-129F-413C-9021-F7C087B4F084}

gPCFileSysPath

dn: CN={ECFD9B0F-129F-413C-9021-F7C087B4F084},CN=Policies,CN=System,DC=dev2003,DC=agami,DC=com
objectClass: groupPolicyContainer
cn: {ECFD9B0F-129F-413C-9021-F7C087B4F084}
displayName: CIFS Engineering
gPCFunctionalityVersion: 2
gPCFileSysPath: \\dev2003.agami.com\SysVol\dev2003.agami.com\Policies\{ECFD9B0F-129F-413C-9021-F7C087B4F084}

GPO Files

- A set for users and a set for machines – the former less relevant to us
- GptTmpl.inf
- Registry.pol
- Scripts directory

Scripts directory

- Contains administrator-specified scripts to be run by client
- Because these scripts are interpreted by the client, they can be sets of device-specific CLI commands
- Not mentioned in [MS-GPOL]

GptTmpl.inf

- Unicode .ini-style file:

```
[Unicode]
Unicode=yes
[Event Audit]
AuditSystemEvents = 1
AuditLogonEvents = 1
...
```

- Contains audit parameters, LSA privilege settings, registry entries and filesystem permissions

GptTmpl.inf

- [] to denote different sections

  [Privilege Rights]

  SeBackupPrivilege = *S-1-5-19

  SeRestorePrivilege = *S-1-5-19

  SeDiskOperatorPrivilege =

  SeAuditPrivilege = *S-1-5-19,*S-1-5-20

- Actually called Gpt.ini in [MS-GPOL]

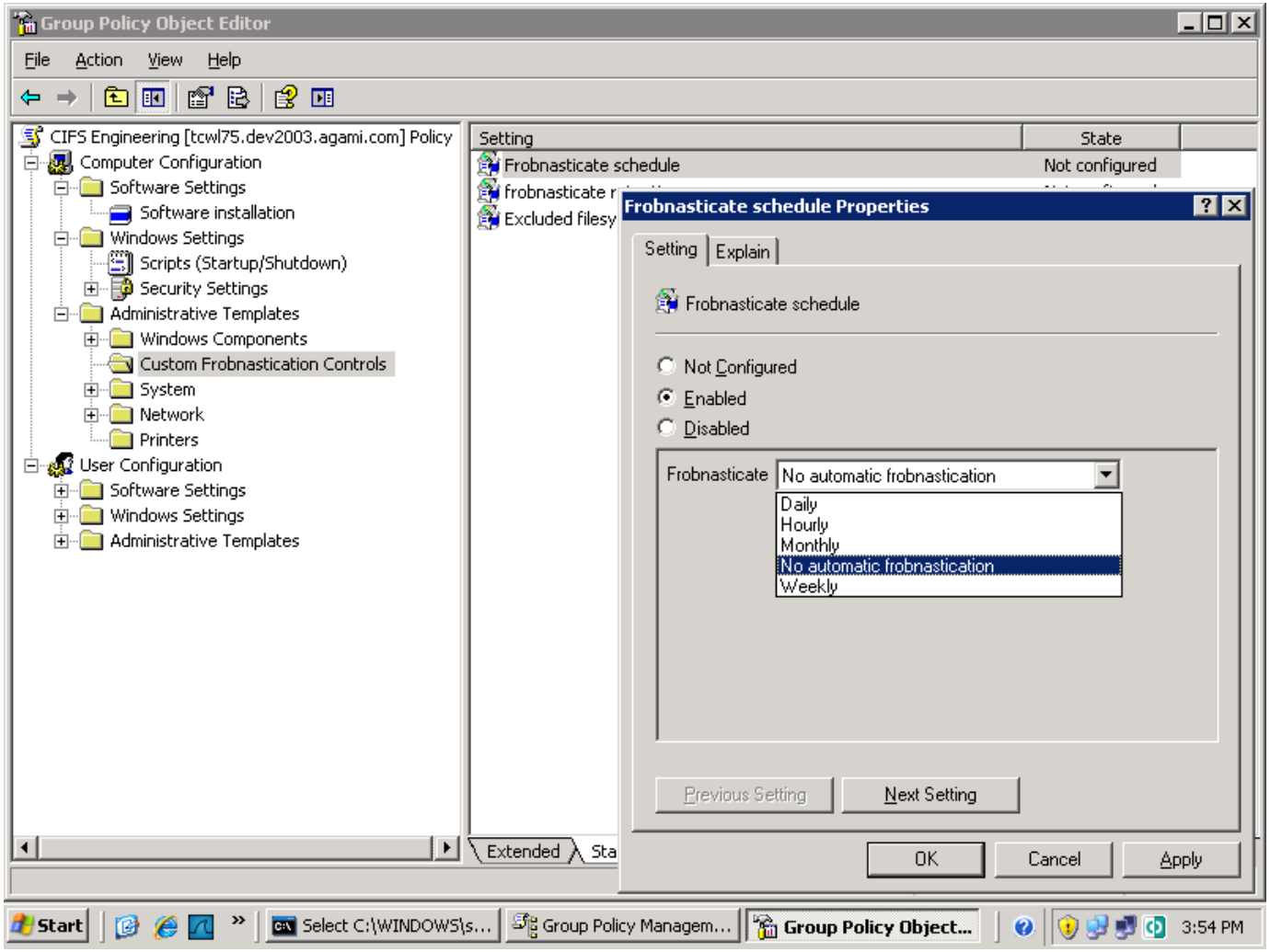
Registry.pol

- Contains the registry entries not part of the subset handled by GptTmpl.inf
- Binary Unicode file
  - 8-byte header (signature and version)
  - Records made up of:
    - Key name
    - Value
    - Type
    - Size
- Not mentioned in [MS-GPOL]

Client-side template

- Templates allow custom parameters to be configured using the same infrastructure
- A storage device/application vendor can use it to extend Group Policies
- Consists of two sections:
  - [strings] section that defines user-visible strings
  - Policy template section that defines what user sees and what is set in GPO

Client-side templates



Client-side templates


```
POLICY !!schedulename
  EXPLAIN !!scheduledesc
  PART !!schedulepartlabel DROPDOWNLIST REQUIRED VALUENAME
     "frobnasticateSchedulePolicy"
    ITEMLIST
      NAME !!sched_none VALUE NUMERIC 0 DEFAULT
      NAME !!sched_hourly VALUE NUMERIC 1
      NAME !!sched_daily VALUE NUMERIC 2
      NAME !!sched_weekly VALUE NUMERIC 3
      NAME !!sched_monthly VALUE NUMERIC 4
    END ITEMLIST
  END PART
END POLICY
```

Example custom parameters

- Filesystem snapshot policy
- Replication sync/async policy
- Heartbeat and other timeouts
- Default filesystem security
- Windows Privilege support in LSA
- Any policy-based information