Remote Management of Windows using Samba

Jelmer Vernooij
Samba Team

1 May 2006

Who am I?

- CS Student at the University of Utrecht (Netherlands)
- Part-time .NET and embedded systems developer
- Samba developer. I work mostly on Samba 4 these days, in this area:
  - pidl, the IDL Compiler and DCE/RPC
  - DCOM implementation and research
  - Registry implementation
  - Build system (building shared libraries)

Remote management from Windows

- Single-purpose tools: regedit, usrmgr, eventlog, etc..
- All in one: MMC
- Scriptable: VBScript
- Protocols involved
  - RAP
  - DCE/RPC
  - WMI / DCOM
  - LDAP

DCE/RPC introduction

- Used for IPC in Windows since NT
- Works over several protocols, most commonly:
  - “ncalrpc” (local)
  - TCP/IP
  - SMB (\\HOST\IPC$)
  - IPX
- Different authentication mechanisms
- Full implementations in Samba 3 and Samba 4

IDL files

Samba 4 uses “Interface Definition Language” files and autogenerates parsers from them

```
[  uuid("894de0c0-0d55-11d3-a322-00c04fa321a1"), version(1.0),
  endpoint("ncacn_np:[\\pipe\\InitShutdown]"),
  pointer_default(unique)
] interface initshutdown {
        typedef [public] struct {
                [value(strlen_m(r->name->name)*2)] uint16 name_len;
                [value(strlen_m_term(r->name->name)*2)] uint16 name_size;
                initshutdown_String_sub *name;
        } initshutdown_String;

        WERROR initshutdown_Init(       [in,unique] uint16 *hostname,
                [in,unique] initshutdown_String *message,
                [in] uint32 timeout,
                [in] uint8 force_apps,
                [in] uint8 reboot );
```

Interesting RPC interfaces

- winreg: remote registry editing
- initshutdown: reboot, shutdown
- svcctl: start/stop/list services
- atsvc: cron / at
- srvsvc: shares
- samr: user management
- eventlog: system events log

Interesting, but unimplemented

- wkssvc: start a join remotely, get client version, change name
- ntsvcs (Plugin and play): enumerate devices, detect devices, disable devices
- dnsserver / winstation: remote management of servers
- efs: encrypted file system support
- file system replication

Easy access using Samba4

- RPC interfaces are exposed as shared libraries
  - already used by one project (OpenChange)
- GTK+ frontends already exist for some interfaces
- Python bindings for some interfaces
- Server-side is implemented for some interfaces as well
  - Transparent management of Windows and Samba workstations

DCOM / WMI

- DCOM
  - Distributed Component Object Model
  - built on top of DCE/RPC
  - available since NT4
- WMI
  - implementation of WBEM
  - built on top of DCOM

DCOM / WMI - (Dis)advantages

- Advantages
  - Once implemented, easier to extend
  - Allows interesting things, more options than RPC
- Several disadvantages:
  - Disabled by default in newer Windows versions (considered a security threat)
  - Very complicated, a lot of work to implement
  - Superseded by .NET and others

Conclusion

- Comments? Questions?
- Which APIs would you like to see available?
- Slides up at http://samba.org/~jelmer/