A view on how to improve Samba user experience

Alexander Bokovoy // Samba Team, Red Hat

SambaXP 2018 // Göttingen, Germany

A starting note

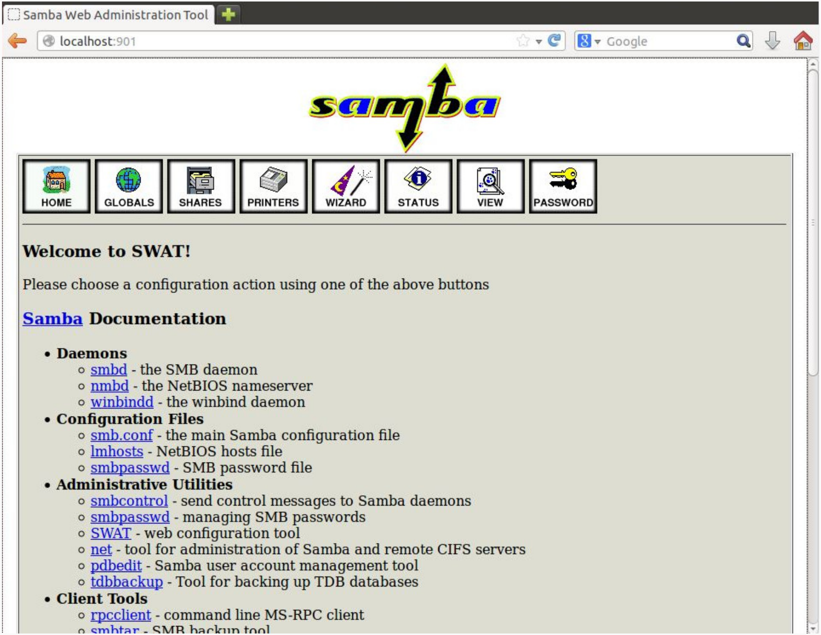
- This talk represents unfinished work and thoughts
- Nothing in this talk can be taken for granted
- A goal is to have a discussion

A starting note

- This talk represents unfinished work and thoughts
- Nothing in this talk can be taken for granted
- A goal is to have a discussion

- About me
    - Samba Team member
    - Engineer at Red Hat
    - Focused on identity management and interoperability

Samba administration until version 4.1



Welcome to SWAT!

Please choose a configuration action using one of the above buttons

Samba Documentation

- **Daemons**
  - smbd - the SMB daemon
  - nmbd - the NetBIOS nameserver
  - winbindd - the winbind daemon
- **Configuration Files**
  - smb.conf - the main Samba configuration file
  - lmhosts - NetBIOS hosts file
  - smbpasswd - SMB password file
- **Administrative Utilities**
  - smbcontrol - send control messages to Samba daemons
  - smbpasswd - managing SMB passwords
  - SWAT - web configuration tool
  - net - tool for administration of Samba and remote CIFS servers
  - pdbedit - Samba user account management tool
  - tdbbackup - Tool for backing up TDB databases
- **Client Tools**
  - rpcclient - command line MS-RPC client
  - smbtar - SMB backup tool

Samba administration until version 4.1

- SWAT: web daemon for editing `smb.conf` and viewing documentation
- SWAT: constant source of CVEs for Samba
- Samba Team is not a group of stellar web programmers
    - programming is hard, no matter which area
- SWAT was removed in Samba 4.1

How complex is it to manage Samba?

- Five main server roles:
  - Standalone server
  - Domain member server
  - Classic primary domain controller
  - Classic backup domain controller
  - Active Directory domain controller
- File share configuration
  - Applies to all five roles
  - allows 133 different options per share
- Global configuration
  - 339 different options

That was just `smb.conf` configuration

- Databases beyond `smb.conf`
  - identity information backend
  - secrets database
  - account policy database
  - SMB identity to POSIX group mapping
  - NetBIOS browsing details database
  - Kerberos keytabs
- Utilites
  - `net`
  - `samba-tool`
  - `smbcontrol` (an instant messaging app)
  - …

Role differences

- Each role has own slightly different initial configuration sequence
  - domain member: create `smb.conf` and `krb5.conf`, then run `net ads join`
  - ad dc: remove `smb.conf`, run `samba-tool domain provision`, then copy `krb5.conf`
  - in both cases one needs to configure the system services too
- No machine-readable definition of the configuration differences
  - quickly leads to myths on the Internet
  - does not help with a clear scenario definition
  - harder to understand to newcomers

Role differences

- Each role has own slightly different initial configuration sequence
  - domain member: create `smb.conf` and `krb5.conf`, then run `net ads join`
  - ad dc: remove `smb.conf`, run `samba-tool domain provision`, then copy `krb5.conf`
  - in both cases one needs to configure the system services too
- No machine-readable definition of the configuration differences
  - quickly leads to myths on the Internet
  - does not help with a clear scenario definition
  - harder to understand to newcomers
- A typical confusion

```
[11:14] <cart_man> Ho everyone. I am desperately trying to mount which should be
        a simple Samba mount to a linux system. The only way I get it to work
        is when I run sudo smbclient -U user[%pass] -L //192.168.xxx.xxx  ; and then
        sudo mount -t cifs -o username=user,password=pass //192.168.xxx.xxx/Sync /tv/Sync
        on my local setup. But when I try and mount cifs on already setup machine
        I get ( ERROR NT_STATUS_IO_TIMEOUT ) and when I try the mount cifs
        without smbclient it gives me an error -> mount error(115): Operation now in progress
```

Operating system integration requirements

- Samba services have multiple uses
    - Domain controllers and members
    - A “simple” SMB network client
    - Identity mapping for POSIX environment
- Even basic use case requires to go beyond Samba own configuration

Operating system integration requirements

- Samba services have multiple uses
  - Domain controllers and members
  - A “simple” SMB network client
  - Identity mapping for POSIX environment
- Even basic use case requires to go beyond Samba own configuration
- In practice, we have to deal with pre-defined scenarios that affect multiple software stacks

Operating system integration requirements

- Samba services have multiple uses
  - Domain controllers and members
  - A “simple” SMB network client
  - Identity mapping for POSIX environment
- Even basic use case requires to go beyond Samba own configuration
- In practice, we have to deal with pre-defined scenarios that affect multiple software stacks
- e.g. Domain member:

Operating system integration requirements

- Samba services have multiple uses
    - Domain controllers and members
    - A “simple” SMB network client
    - Identity mapping for POSIX environment
- Even basic use case requires to go beyond Samba own configuration
- In practice, we have to deal with pre-defined scenarios that affect multiple software stacks
- e.g. Domain member:
    - winbindd configuration

Operating system integration requirements

- Samba services have multiple uses
    - Domain controllers and members
    - A “simple” SMB network client
    - Identity mapping for POSIX environment
- Even basic use case requires to go beyond Samba own configuration
- In practice, we have to deal with pre-defined scenarios that affect multiple software stacks
- e.g. Domain member:
    - winbindd configuration
    - Identity mapping (`/etc/nsswitch.conf`)

Operating system integration requirements

- Samba services have multiple uses
    - Domain controllers and members
    - A “simple” SMB network client
    - Identity mapping for POSIX environment
- Even basic use case requires to go beyond Samba own configuration
- In practice, we have to deal with pre-defined scenarios that affect multiple software stacks
- e.g. Domain member:
    - winbindd configuration
    - Identity mapping (`/etc/nsswitch.conf`)
    - PAM authentication against a domain controller

Operating system integration requirements

- Samba services have multiple uses
  - Domain controllers and members
  - A “simple” SMB network client
  - Identity mapping for POSIX environment
- Even basic use case requires to go beyond Samba own configuration
- In practice, we have to deal with pre-defined scenarios that affect multiple software stacks
- e.g. Domain member:
  - winbindd configuration
  - Identity mapping (`/etc/nsswitch.conf`)
  - PAM authentication against a domain controller
  - optionally: Samba file server configuration

Not a Samba Team problem?

- We cannot replace actual OS distribution development teams
    - we hope they scale more than we do
    - at least, with the help of our software

Not really.

Not really

- a wide spectre of Samba deployments:
    - ‘I am learning my way through GUI’
    - manual configuration for ‘my own machine’
    - reproducible deployments with automated tools
- We see both extremes on practice

Not really

- a wide spectre of Samba deployments:
    - ‘I am learning my way through GUI’
    - manual configuration for ‘my own machine’
    - reproducible deployments with automated tools
- We see both extremes on practice
    - Millenials have grown up, and

Not really

- a wide spectre of Samba deployments:
  - ‘I am learning my way through GUI’
  - manual configuration for ‘my own machine’
  - reproducible deployments with automated tools
- We see both extremes on practice
  - Millenials have grown up, and
  - Migrations from environments with a different management paradigm do happen

Not really

- a wide spectre of Samba deployments:
    - ‘I am learning my way through GUI’
    - manual configuration for ‘my own machine’
    - reproducible deployments with automated tools
- We see both extremes on practice
    - Millenials have grown up, and
    - Migrations from environments with a different management paradigm do happen
    - Cloud deployments don’t have eyes, only blind sockets

Millenials have grown up

- Android and iOS brought computers to masses
- They also changed administration experience expectations
- One can use complex systems without understanding their components
- Everyone can be a devops engineer too

Migrations from Windows

- Windows shops do migrate to Linux
- Admins have quite a different background and experience
- Some might have never encountered POSIX before
- A crash course down to low details doesn’t always produce expected results
    - Support costs for distributions and upstream actually higher
        - support cases get filed for any minute detail
        - people ask “silly” questions on the user lists

Management consoles

- SWAT was a management console for Samba
  - too low-level but still …
- NAS vendors all have their own automation
  - hides low-level stuff and automate scenarios
  - Does not focus on complex scenarios though
- Windows Server has had few iterations

Management consoles

- SWAT was a management console for Samba
    - too low-level but still …
- NAS vendors all have their own automation
    - hides low-level stuff and automate scenarios
    - Does not focus on complex scenarios though
- Windows Server has had few iterations
    - Project Honolulu is a latest one

Management consoles

- SWAT was a management console for Samba
    - too low-level but still …
- NAS vendors all have their own automation
    - hides low-level stuff and automate scenarios
    - Does not focus on complex scenarios though
- Windows Server has had few iterations
    - Project Honolulu is a latest one
- Cockpit is an open source approach in the same area

Management consoles

- SWAT was a management console for Samba
    - too low-level but still …
- NAS vendors all have their own automation
    - hides low-level stuff and automate scenarios
    - Does not focus on complex scenarios though
- Windows Server has had few iterations
    - Project Honolulu is a latest one
- Cockpit is an open source approach in the same area
    - but more on that later

Robots have no eyes, only blind sockets

- Robots get programmed by people so they are better off than novices

Robots have no eyes, only blind sockets

- Robots get programmed by people so they are better off than novices
- Robots like predictable input

Robots have no eyes, only blind sockets

- Robots get programmed by people so they are better off than novices
- Robots like predictable input
- Robots like predictable output

Robots have no eyes, only blind sockets

- Robots get programmed by people so they are better off than novices
- Robots like predictable input
- Robots like predictable output

Robots have no eyes, only blind sockets

- Robots get programmed by people so they are better off than novices
- Robots like predictable input
- Robots like predictable output

```
# testparm -d0
Load smb config files from /etc/samba/smb.conf
Loaded services file OK.
ERROR: Invalid idmap range for domain *!

Server role: ROLE_DOMAIN_PDC

Press enter to see a dump of your service definitions
<blinking cursor>
```

or

```
# samba-tool user getpassword administrator --attributes virtualClearTextUTF8
dn: CN=Administrator,CN=Users,DC=r28ad,DC=example,DC=com

Got password OK
<where is a password?>
```

Management consoles, take two

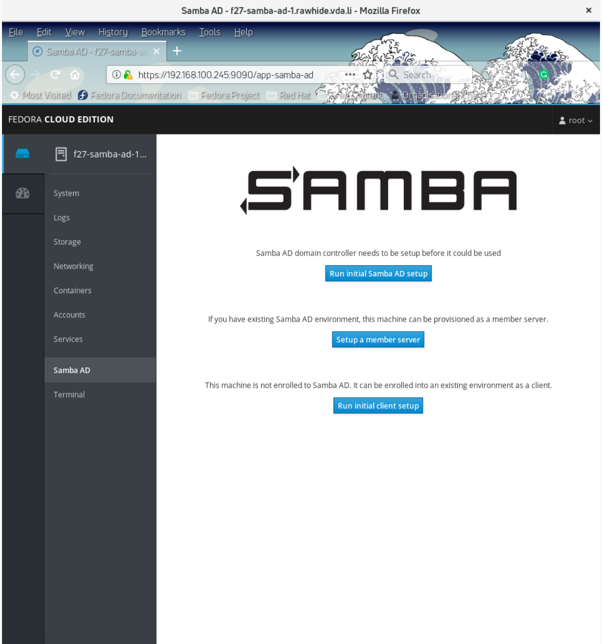
- Management console allows to automate *some* tasks
    - Does basic configuration as an ‘atomic’ operation
    - Allows people to explore capabilities of the generated configuration
    - … sometimes breaks when there are unexpected manual edits

Management consoles, take two

- Management console allows to automate *some* tasks
  - Does basic configuration as an ‘atomic’ operation
  - Allows people to explore capabilities of the generated configuration
  - … sometimes breaks when there are unexpected manual edits
- Management console needs automated input and output
  - It is a C-3PO while `samba-tool` or `net` are R2-D2
- We can talk to R2-D2 directly but somehow prefer translators (and magic)

Magic (demo)

Magic (demo)



Samba AD - f27-samba-ad-1.rawhide.vda.li - Mozilla Firefox

Samba AD domain controller needs to be setup before it could be used

Run initial Samba AD setup

If you have existing Samba AD environment, this machine can be provisioned as a member server.

Setup a member server

This machine is not enrolled to Samba AD. It can be enrolled into an existing environment as a client.

Run initial client setup

What was that?

- Cockpit management console for Fedora 28
- Samba AD Cockpit application
    - prototype
    - deploys Samba AD domain controller
    - or shows its state

What was that?

- Cockpit management console for Fedora 28
- Samba AD Cockpit application
  - prototype
  - deploys Samba AD domain controller
  - or shows its state
- Behind the (web) interface
  - Runs `samba-tool domain provision`
  - Copies generated Kerberos configuration
  - Starts samba
  - Runs `samba-tool domain info`

Cockpit application

- An HTML and JavaScript code
- Uses predefined Cockpit API
- Part of Cockpit app, socket-activated and authenticated
- Cockpit session is like an SSH session
    - Properly authenticated, can use `sudo`, if allowed
    - All you can do in SSH session can be done by a Cockpit app
        - even to a remote Cockpit server

Interaction of robots

- Parsing low-level utility output is easy
  - but we really should consider providing machine-readable output
  - and machine-writable input
- It is all text, just easier to explain to humans
- But a management console needs to re-interpret it in a context
- Some level of a tagged and easy to parse response would be nice
  - No, no XML
- JSON is “good enough” for transformations
  - we already started to provide audit logs in JSON output

samba-tool drs showrepl --json

```
# samba-tool drs showrepl --json
[
    {
        ”result”: {
            ”info”: ”
Default-First-Site-Name \AD-DC-28
DSA Options: 0x00000001
DSA object GUID: 44a3ce06-fdc3-4bc8-be92-768a681df782
DSA invocationId: 56bce630-7686-477f-af46-da7e02dc3311
”,
            ”data”: {
                ”site”: ”Default-First-Site-Name”,
                ”server”: ”AD-DC-28”,
                ”objectGUID”: ”44a3ce06-fdc3-4bc8-be92-768a681df782”,
                ”invocationId”: ”56bce630-7686-477f-af46-da7e02dc3311”,
                ”options”: 0x00000001
            }
        }
    },
    {
        ”info”: ”==== INBOUND NEIGHBORS ====\n\n”
    },
    {
        ”info”: ”==== OUTBOUND NEIGHBORS ====\n\n”
    },
    {
        ”info”: ”==== KCC CONNECTION OBJECTS ====\n\n”
    }
]
```

What is this `--json` switch

- A work in progress to add `--json` to all commands in `samba-tool`
- Would allow to transform all output from a plain-text to a machine-readable format
- Transparent for internal commands
  - output is collected, then rendered in a chosen format
  - applies to informative messages and errors too
- Output can easily be understood and transformed by a robot

What about predictable input?

- Interactive input is often required
- Passwords, names, etc
- Perhaps, allowing for JSON input would help
  - no need to prompt
  - `echo $PASSWORD | samba-tool ...` goes away
  - can be more secure for data passes

Predictable input, take two

- If input can be serialized, a sequence of calls to tools can be serialized too
- Sounds similar to how Ansible or other configuration management tools behave
    - requires someone to document the sequence-as-a-code
- An example of how a predictable input is used: **varlink**
    - varlink interface: varlink.org
    - a JSON input and a method call definition
    - LWN article: https://lwn.net/Articles/742675/

Imaginary use

- Imagine `samba-tool domain provision` call over varlink with a predictable input

```
{
  ”method”: ”org.samba.samba-tool.domain.provision”,
  ”parameters”: {
    ”options”: {
      ”use-rfc2307”: ”true”,
      ”realm”: ”${options.realm}”,
      ”domain”: ”${options.domain}”,
      ”server-role”: ”${options.setup_type}”,
      ”adminpass”: ”${options.adminpw}”,
      ”dns-backend”: ”SAMBA_INTERNAL”
    }
  }
}
```

Final thoughts

- Samba is used by people
- And robots
- Robots increasingly consume Samba artefacts
- Parsing human-oriented output is a waste of resources for robots
- We can do better (for robots and humans)
- A little magic can help both

Thanks!