ID Mapping of Active Directory users with

Sumit Bose
Red Hat
sbose@redhat.com

is a client for FreeIPA

sssd

freeIPA

identity | policy | audit

sssd

Integrated Solution

freeIPA
identity | policy | audit

=

389
directory server

NTP

DNS

SAMBA

sssd

Identity

Who you are

sssd

FREE IPA

Identity | Policy | IPA Server

Users | User Groups | Hosts | Host Groups | Netgroups | Services | DNS | Certificates | Realm Dom

USERS

Refresh | Delete | Add | Disable | Enable

	User login	First name	Last name	Status	UID	Emai
☐	admin		Administrator	✔ Enabled	747400000	
☐	migration-test	Migration	Test	✔ Enabled	747400013	migrat test@

Showing 1 to 4 of 4 entries.

FREE IPA

Identity | Policy | IPA Server

Users | User Groups | Hosts | Host Groups | Netgroups | Services | DNS | Certificates | Realm Dom

USER GROUPS

Refresh Delete Add

	Group name	GID
☐	admins	747400000
☐	editors	747400002
☐	ipausers	
☐	trust admins	

Showing 1 to 4 of 4 entries.

FREE IPA

Identity | Policy | IPA Server

Users | User Groups | Hosts | Host Groups | Netgroups | Services | DNS | Certificates | Realm Dom

HOSTS

Refresh | Delete | + Add

	Host name	Description
	ipa20-devel.ipa20.devel	

Showing 1 to 1 of 1 entries.

FREE IPA

Identity | Policy | IPA Server

Users | User Groups | Hosts | Host Groups | Netgroups | Services | DNS | Certificates | Realm Dom

HOST GROUPS

Refresh | Delete | + Add

	Host-group	Description
☐	myhosts	Group for my hosts

Showing 1 to 1 of 1 entries.

FREE IPA

Identity | Policy | IPA Server

Users | User Groups | Hosts | Host Groups | Netgroups | Services | DNS | Certificates | Realm Dom

NETGROUPS

Refresh | Delete | + Add

	Netgroup name	Description
☐	ngtest	test entgroup

Showing 1 to 1 of 1 entries.

FREE IPA

Identity | Policy | IPA Server

Users | User Groups | Hosts | Host Groups | Netgroups | Services | DNS | Certificates | Realm Dom

SERVICES

Refresh | Delete | + Add

	Principal
	DNS/ipa20-devel.ipa20.devel@IPA20.DEVEL
	HTTP/ipa20-devel.ipa20.devel@IPA20.DEVEL
	cifs/ipa20-devel.ipa20.devel@IPA20.DEVEL
	ldap/ipa20-devel.ipa20.devel@IPA20.DEVEL

Showing 1 to 4 of 4 entries.

FREE IPA

Identity | Policy | IPA Server

Users | User Groups | Hosts | Host Groups | Netgroups | Services | DNS | Certificates | Realm Dom

DNS ZONES | DNS GLOBAL CONFIGURATION

DNS ZONES

Refresh | Delete | Add | Disable | Enable

	Zone name	Status
☐	122.168.192.in-addr.arpa.	✔ Enabled
☐	ipa20.devel	✔ Enabled

Showing 1 to 2 of 2 entries.

FREE IPA

Identity | Policy | IPA Server

Users | User Groups | Hosts | Host Groups | Netgroups | Services | DNS | Certificates | Realm Dom

CERTIFICATES

Refresh

Betreff

Serial Number	Betreff
1	CN=Certificate Authority,O=IPA20.DEVEL
2	CN=OCSP Subsystem,O=IPA20.DEVEL
3	CN=ipa20-devel.ipa20.devel,O=IPA20.DEVEL
4	CN=CA Subsystem,O=IPA20.DEVEL

10 certificates matched

https://ipa20-devel.ipa20.devel/ipa/ui/index.html#identity/cert

VT100 anyone ?

```
$ ipa user-find admin
--------------
1 user matched
--------------
  User login: admin
  Last name: Administrator
  Home directory: /home/admin
  Login shell: /bin/bash
  UID: 747400000
  GID: 747400000
  Account disabled: False
  Password: True
  Kerberos keys available: True
----------------------------
Number of entries returned 1
----------------------------
```

sssd

Policy

What you are allowed to do

sssd

FREE IPA

Identity | Policy | IPA Server

Host Based Access Control | Sudo | Automount | Password Policies | Kerberos Ticket Policy | SELinux User M

HBAC RULES | HBAC SERVICES | HBAC SERVICE GROUPS | HBAC TEST

HBAC RULES

Refresh | Delete | Add | Disable | Enable

	Rule name	Status
☐	allow_all	✔ Enabled
☐	hbac_test	✔ Enabled

Showing 1 to 2 of 2 entries.

FREE IPA

Identity | Policy | IPA Server

Host Based Access Control | Sudo | Automount | Password Policies | Kerberos Ticket Policy | SELinux User M

SUDO RULES | SUDO COMMANDS | SUDO COMMAND GROUPS

SUDO RULES

Refresh | Delete | Add | Disable | Enable

	Rule name	Status
☐	allow_reboot	✔ Enabled

Showing 1 to 1 of 1 entries.

FREE IPA

Identity | Policy | IPA Server

Host Based Access Control | Sudo | Automount | Password Policies | Kerberos Ticket Policy | SELinux User M

AUTOMOUNT LOCATIONS

Refresh | Delete | + Add

	Ort
	default

Showing 1 to 1 of 1 entries.

FREE IPA

Identity | Policy | IPA Server

Host Based Access Control | Sudo | Automount | Password Policies | Kerberos Ticket Policy | SELinux User M

PASSWORD POLICIES

Refresh | Delete | + Add

	Group	Priority
	global_policy	

Showing 1 to 1 of 1 entries.

FREE IPA

Identity | Policy | IPA Server

Host Based Access Control | Sudo | Automount | Password Policies | Kerberos Ticket Policy | SELinux User M

SELINUX USER MAPS

Refresh | Delete | Add | Disable | Enable

	Rule name	SELinux User	Status
☐	testmap2	staff_u:s0-s0:c0.c1023	✔ Enabled

Showing 1 to 1 of 1 entries.

Audit

What you have done

sssd

IPA Server

PAM

InfoPipe

automount

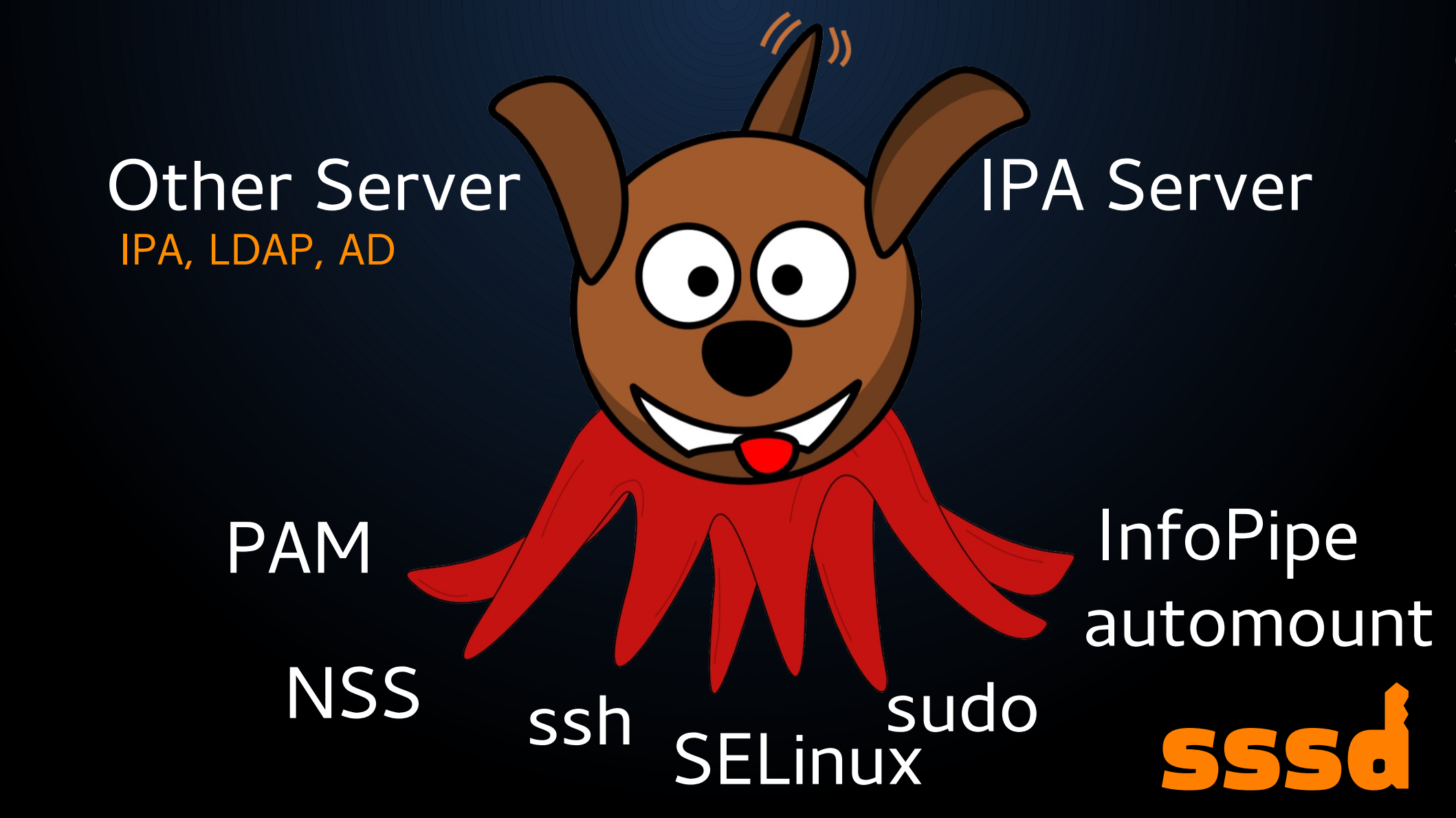
NSS

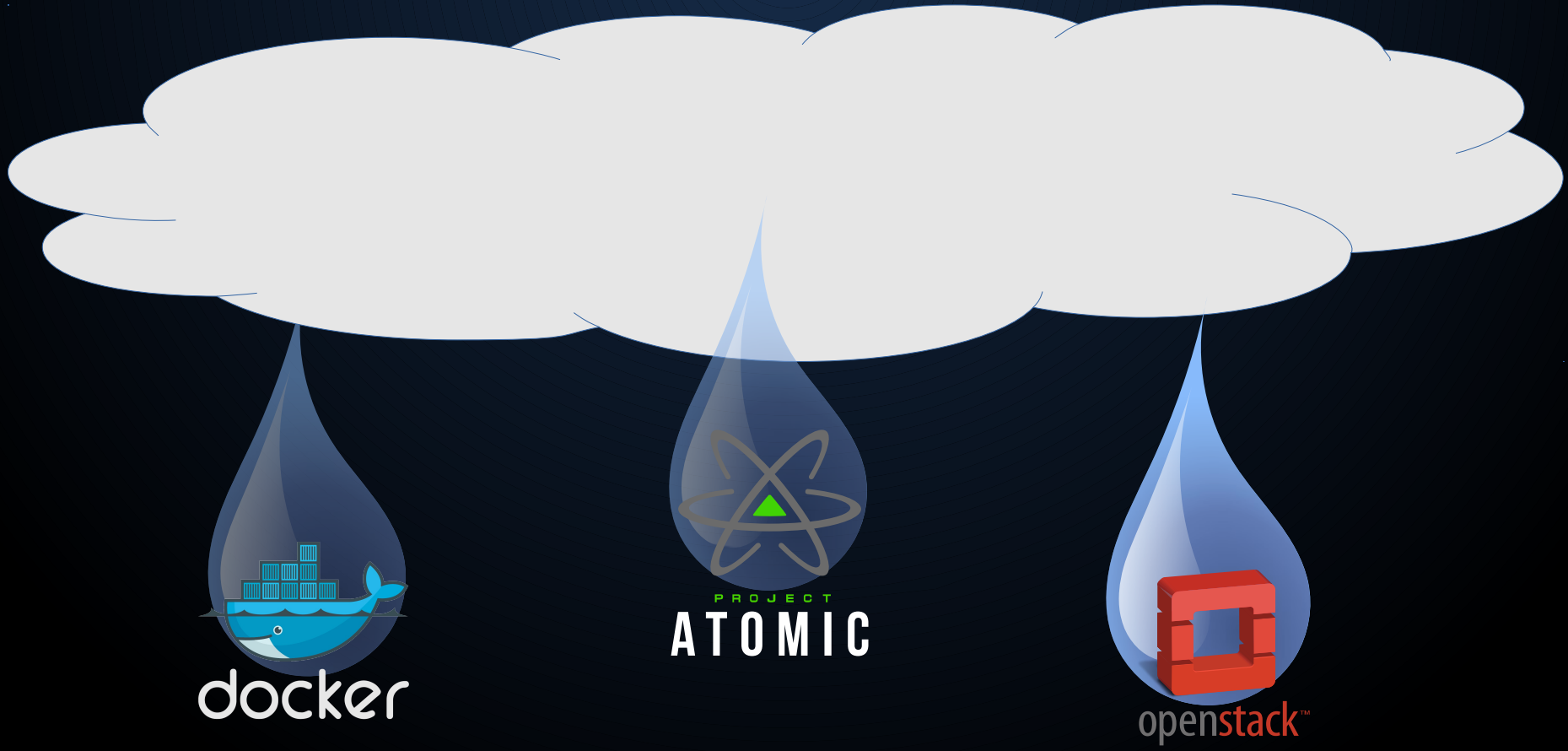
ssh

SELinux

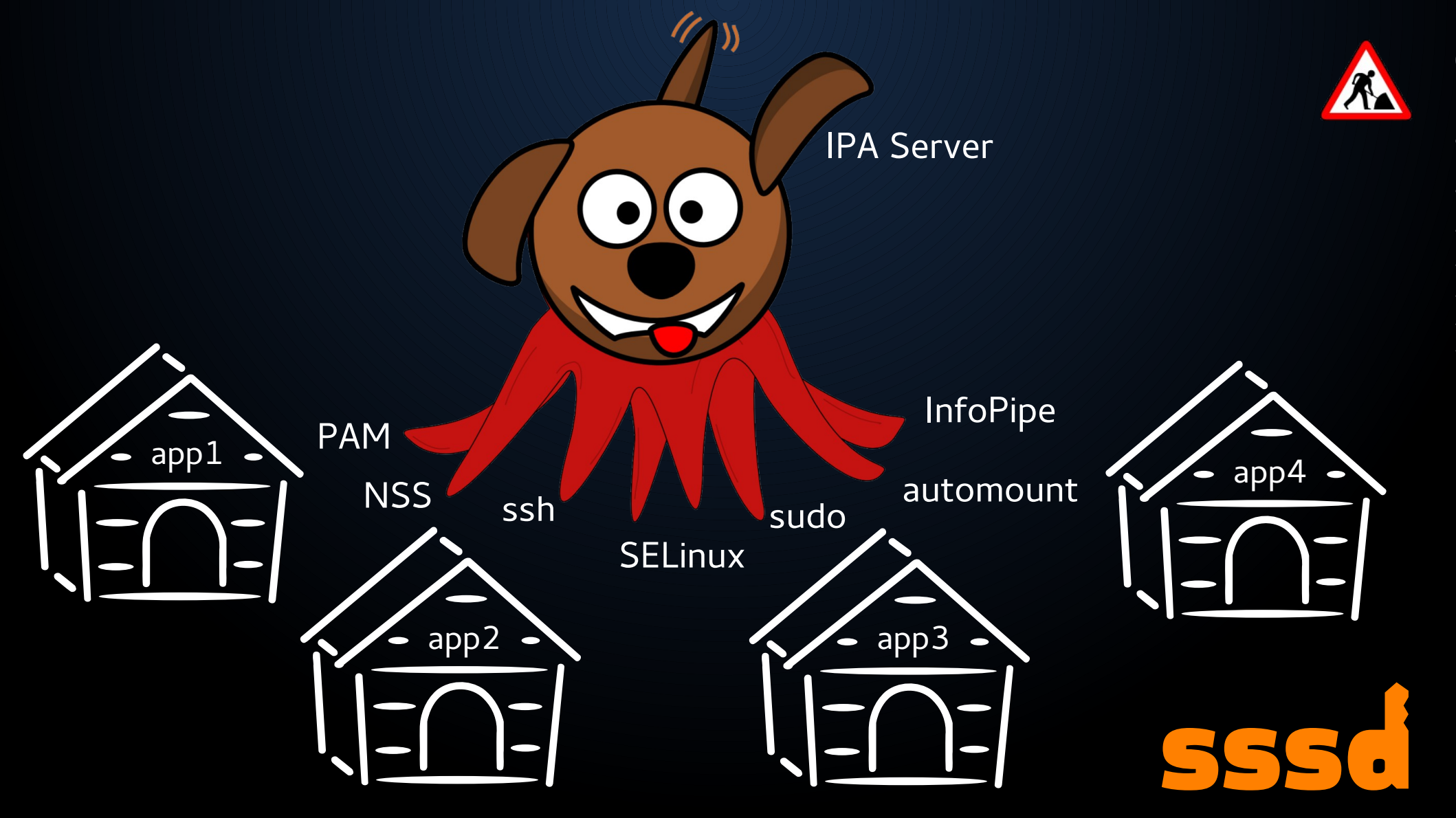
sudo

sssd


Other Server
IPA, LDAP, AD
IPA Server
PAM
InfoPipe
automount
NSS
ssh
SELinux
sudo
sssd



sssd


IPA Server
PAM
NSS
ssh
SELinux
sudo
automount
InfoPipe
app1
app2
app3
app4
sssd

	to Micro Servers	
11:30 am - 12:15 pm	**Julien Kerihuel (OpenChange)** OpenChange: Beyond Technical Fulfillment	**Martin Schwenke (IBM)** Scaling IP address handling in CTDB
12:15 pm - 1:15 pm	**lunch**	
1:15 pm - 2:00 pm	**Dan Shearer** The Big News that Never Quite Happen	* **Ingo Meents (IBM)** * Experiences of Applying Samba in Enterprise NAS Products
2:00 pm - 2:45 pm	**David Disseldorp (SUSE)** Elasto cloud storage	**Alexander Werth (IBM)** Recent improvements in using NFS4 ACLs with Samba
2:45 pm - 3:00 pm	**break**	
3:00 pm - 3:45 pm	* **Simo Sorce (Red Hat)** * OpenStack and Samba	
3:45 pm - 4:30 pm	**Jeremy Allison (Google)** Asynchronous smbd - the future of fileserving	
4:30 pm - end :-)	**Samba Team** panel discussion	

Tomorrow

Forest Trust

Active Directory

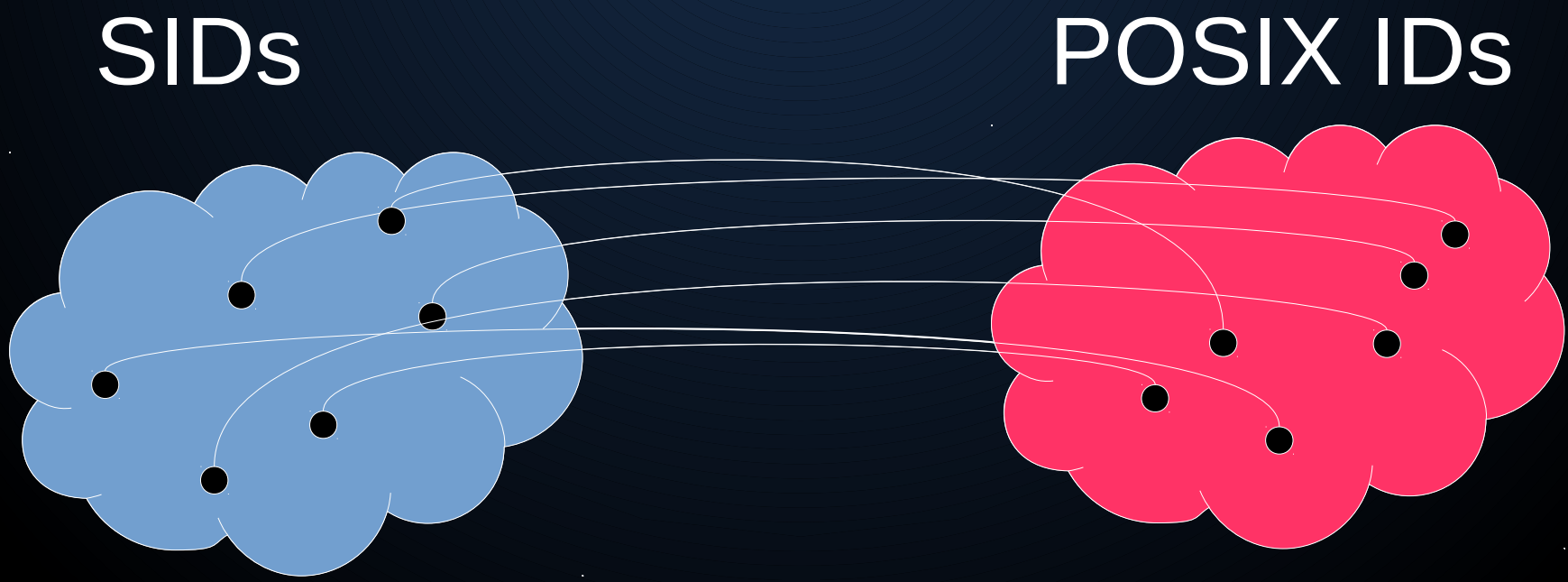
freeIPA

identity | policy | audit

sssd

		Track 1	Track 2
Thu, 15th	9:00 am - 9:45 am	**Andreas Schneider (Red Hat)** Testing your full software stack on a single host with cwrap	**Michael Adam (SerNet)** To winbind or not to winbind - that is NOT the question!
	9:45 am - 10:30 am	**Nadezhda Ivanova (Symas)** Samba4 with OpenLDAP Backend - It's Alive!	**Alexander Bokovoy (Red Hat)** Trusting Active Directory with FreeIPA: a story beyond Samba
	10:30 am - 10:45 am	**break**	
	10:45 am - 11:30 am	* **Kai Blin (MPG)** * µSamba - Scaling Samba Down to Micro Servers	**Amitay Isaacs (IBM)** Sustaining CTDB Development
	11:30 am - 12:15 pm	**Julien Kerihuel (OpenChange)** OpenChange: Beyond Technical Fulfillment	**Martin Schwenke (IBM)** Scaling IP address handling in CTDB
	12:15 pm - 1:15 pm	**lunch**	
	1:15 pm - 2:00 pm	**Dan Shearer**	* **Ingo Meents (IBM)** *

Tomorrow

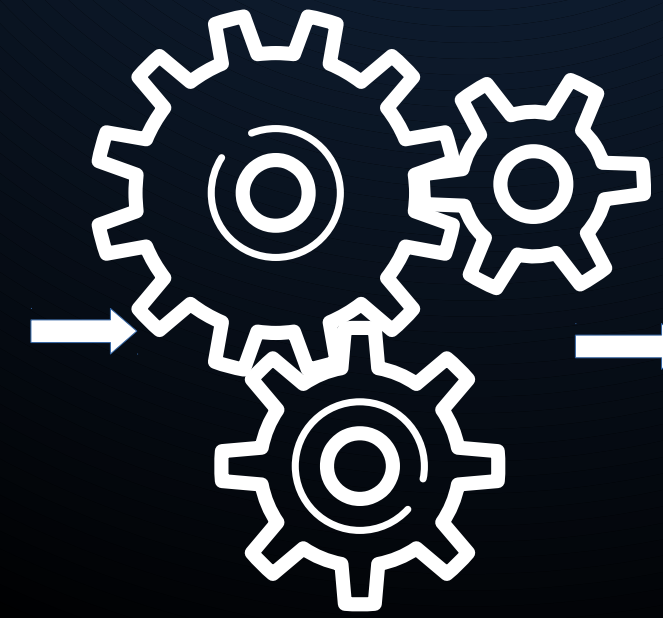


ID-Mapping

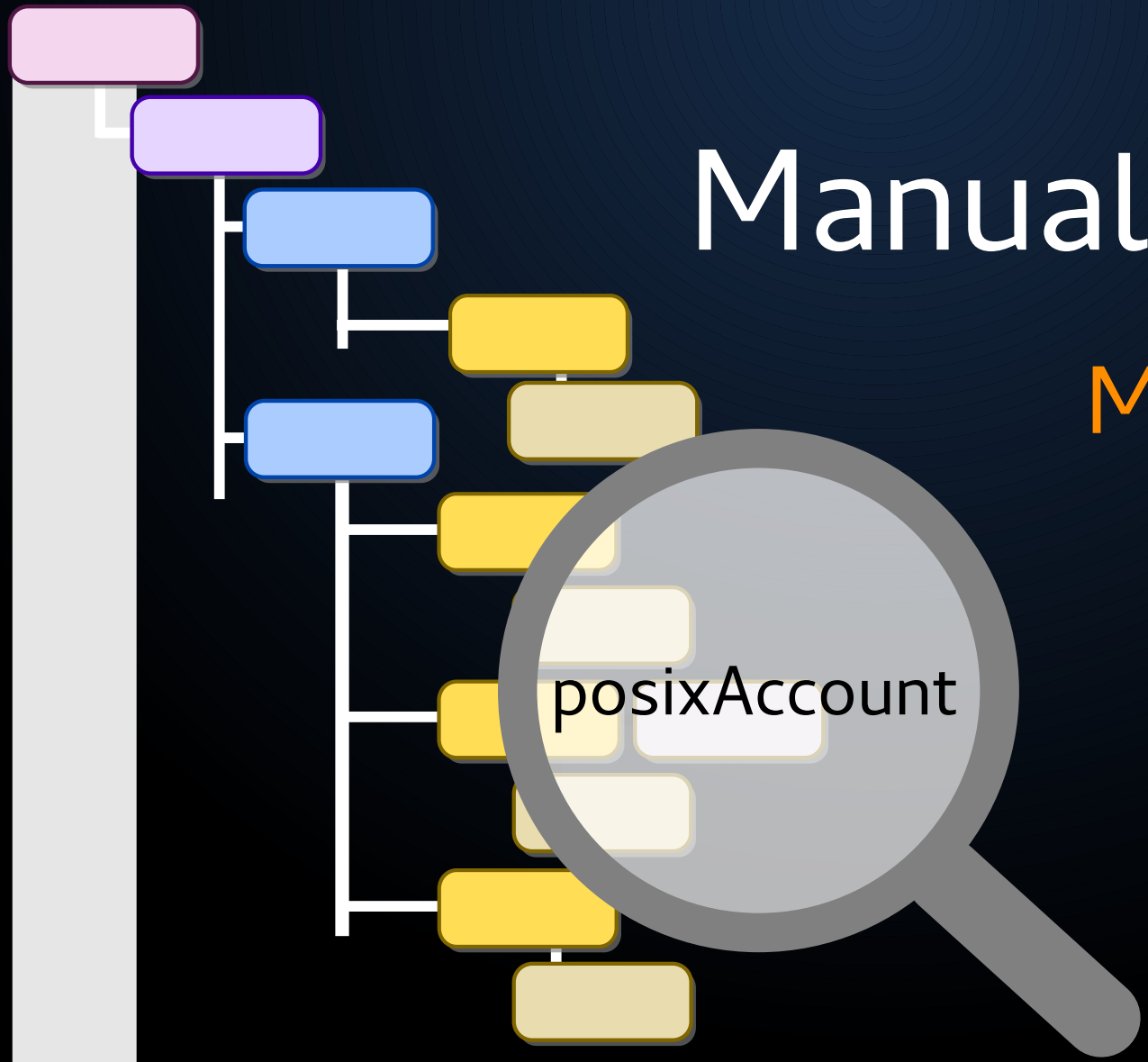
sssd


$10^{28} : 1$
128bits
32bits
sssd

Algorithmic Mapping

SID →  → POSIX ID

sssd



Manual Mapping

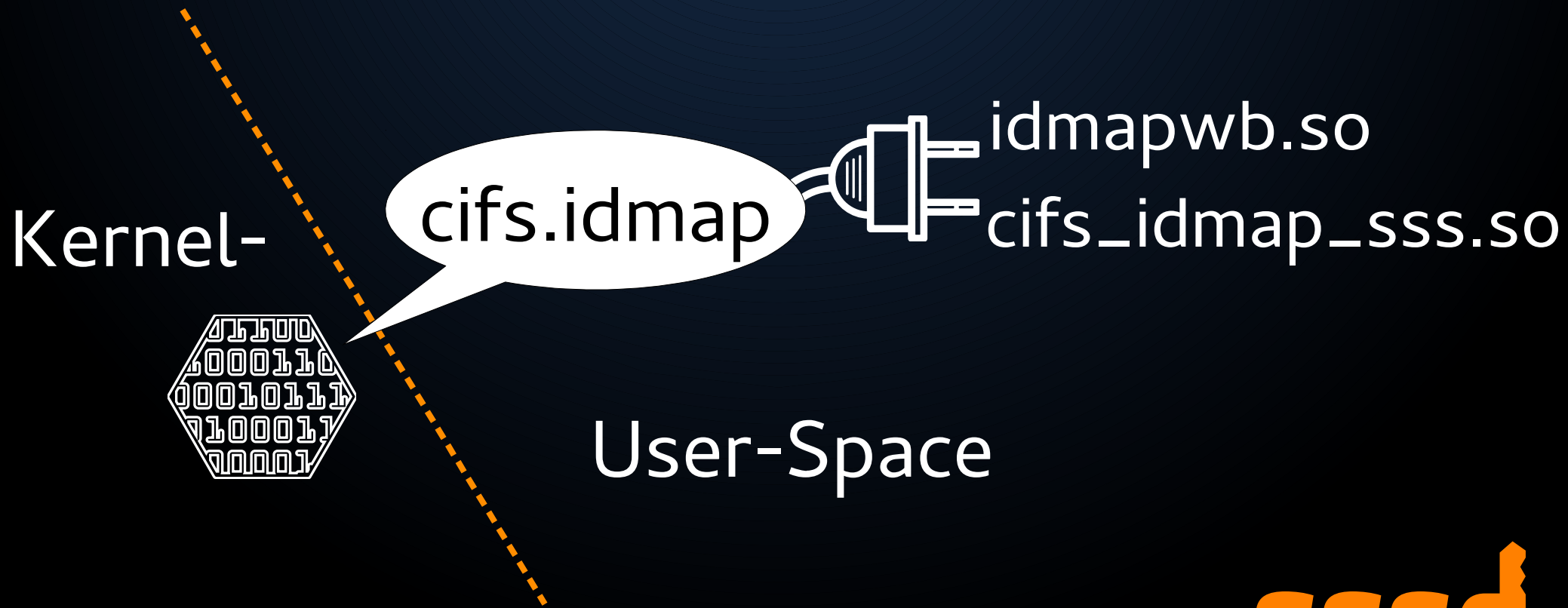
Managed in AD

sssd

FreeIPA CIFS-Client

sssd

cifs-utils



sssd

FreeIPA CIFS-Server

Samba File-Server

SAMBA

smbd wbinfo

winbindd

libwbclient.so.0

sssd

Samba File-Server

On a FreeIPA Client

smbd wbinfo

libwbclient-sssd.so.0

sssd

		Track 1	Track 2
Thu, 15th	9:00 am - 9:45 am	**Andreas Schneider (Red Hat)** Testing your full software stack on a single host with cwrap	**Michael Adam (SerNet)** To winbind or not to winbind - that is NOT the question!
	9:45 am - 10:30 am	**Nadezhda Ivanova (Symas)** Samba4 with OpenLDAP Backend - It's Alive!	**Alexander Bokovoy (Red Hat)** Trusting Active Directory with FreeIPA: a story beyond Samba
	10:30 am - 10:45 am	**break**	
	10:45 am - 11:30 am	*** Kai Blin (MPG) *** µSamba - Scaling Samba Down to Micro Servers	**Amitay Isaacs (IBM)** Sustaining CTDB Development
	11:30 am - 12:15 pm	**Julien Kerihuel (OpenChange)** OpenChange: Beyond Technical Fulfillment	**Martin Schwenke (IBM)** Scaling IP address handling in CTDB
	12:15 pm - 1:15 pm	**lunch**	
	1:15 pm - 2:00 pm	**Dan Shearer**	*** Ingo Meents (IBM) ***

Tomorrow

libwbclient-sssd

common

ID/SID lookup

utilities

authentication

sssd

libwbclient-sssd

Limitations

sssd

Next Plans

pam_winbind.so
libnss_winbind.so

socket → winbindd

pam_sss.so
libnss_sss.so

socket → sssd

sssd

Unified PAM/nss Client

pam_socket.so
libnss_socket.so

winbindd

sssd

sssd

Thank you :-)

Any questions please?