

**FOSDEM'24**

Brussels

3 & 4 February 2024

# Automated Integration of FreeIPA with AD and External IdP



Thomas Woerner

Principal Software Engineer / Red Hat

Rafael Jeffman

Senior Software Engineer / Red Hat

# What is this talk about?

- Automated FreeIPA deployment and configuration to integrate with Microsoft Active Directory (AD)
- Automated configuration and use of External Identity Providers (External IdP)

# Automated FreeIPA deployment

- Deployment using <https://github.com/rjeffman/freeipa-ad-trust.git> as a base
  - Change `ipaserver_timezone` and `winserver_timezone` and IP addresses as needed in `inventory.yaml`

- Documentation and playbooks will be added to ansible-freeipa web page soon

<https://www.freeipa.org/ansible-freeipa.github.io/>

- Preparation of the controller (Fedora)

```
dnf install python3-winrm.noarch
```

```
ansible-galaxy collection install ansible.windows  
ansible-galaxy collection install community.windows
```

```
git clone https://github.com/rjeffman/freeipa-ad-trust.git  
cd freeipa-ad-trust/
```

- Ensure timezone and time is correct on all machines

# Microsoft AD setup

- Preparation of Windows
- Windows AD setup

Might be needed to disable IPv6 in 01-windows-ad-setup.yml:

```
- name: Disable ms_tcpip6 for all interfaces
  community.windows.win_net_adapter_feature:
    interface: '*'
    state: disabled
    component_id:
      - ms_tcpip6
```

```
ansible-playbook -i inventory.yaml 01-windows-ad-setup.yml
```

# FreeIPA server setup

Enable DNS auto reverse  
Disable DNSSEC validation

```
ipaserver:  
  vars:  
    ipaserver_auto_reverse: yes  
    ipaserver_no_dnssec_validation: yes
```

```
ansible-playbook -i inventory.yaml 02-ipa-setup.yml  
ansible-playbook -i inventory.yaml 03-nslookup-test.yml  
ansible-playbook -i inventory.yaml 04-add-trust.yml
```

# Login as AD admin

```
$ ssh AD\\administrator@server.lin.ipa.test
(AD\\administrator@server.lin.ipa.test) Password:
Last login: Sun Feb  4 11:53:19 2024 from 192.168.153.1
[administrator@ad.ipa.test@server ~]$ klist
Ticket cache: KCM:325600500:99540
Default principal: Administrator@AD.IPA.TEST

Valid starting    Expires          Service principal
02/04/2024 11:54:16  02/04/2024 21:54:16  krbtgt/AD.IPA.TEST@AD.IPA.TEST
    renew until 02/05/2024 11:54:16
[administrator@ad.ipa.test@server ~]$ id
uid=325600500(administrator@ad.ipa.test) gid=325600500(administrator@ad.ipa.test)
groups=325600500(administrator@ad.ipa.test),325600512(domain
admins@ad.ipa.test),325600513(domain users@ad.ipa.test),325600518(schema
admins@ad.ipa.test),325600519(enterprise admins@ad.ipa.test),325600520(group policy
creator owners@ad.ipa.test)
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023

[administrator@ad.ipa.test@server ~]$ ipa user-add testuser --first=f --last=l
ipa: ERROR: Insufficient access: Invalid credentials
```

# Enable AD administrator to act as an IPA admin

```
---
- name: Enable AD administrator to act as a FreeIPA admin.
  hosts: ipaserver
  become: false
  gather_facts: false

  tasks:
  - name: Ensure idoverride for administrator@ad.ipa.test in 'default trust view'
    ipaidoverrideuser:
      ipadmin_password: SomeADMINpassword
      idview: default trust view
      anchor: administrator@ad.ipa.test

  - name: Ensure idoverride for administrator@ad.ipa.test is part of admins group
    ipagroup:
      ipadmin_password: SomeADMINpassword
      name: admins
      idoverrideuser: administrator@ad.ipa.test
```

...

# Use AD administrator as an IPA admin

```
[administrator@ad.ipa.test@server ~]$ ipa user-add testuser --first=f --last=l
```

```
-----  
Added user "testuser"
```

```
-----  
  User login: testuser  
  ...  
  Principal name: testuser@LIN.IPA.TEST  
  ...
```

```
[administrator@ad.ipa.test@server ~]$ ipa user-del testuser
```

```
-----  
Deleted user "testuser"
```



# Client deployment

**Important:** Use proper AD administrator Administrator@AD.IPA.TEST

Change inventory.yml

```
ipaclients:
  hosts:
    client1.lin.ipa.test:
      ansible_user: root
  vars:
    ipaclient_configure_dns_resolver: yes
    ipaclient_dns_servers: 192.168.122.251
    ipadmin_principal: Administrator@AD.IPA.TEST
    ipadmin_password: SomeW1Npassword
```

Deploy client:

```
---
- name: Deploy IPA client
  hosts: ipaclients
  become: true

  roles:
  - role: ipaclient
    state: present
```

...

# Replica deployment

**Temporary work a round:** Disable replica connection check

Add to inventory.yml

```
ipareplicas:
  hosts:
    replica1.lin.ipa.test:
      ansible_user: root
  vars:
    ipareplica_skip_conncheck: yes
    ipaclient_dns_servers: 192.168.122.251
    ipaadmin_principal: Administrator@AD.IPA.TEST
    ipaadmin_password: SomeW1Npassword
```

Deploy Replica:

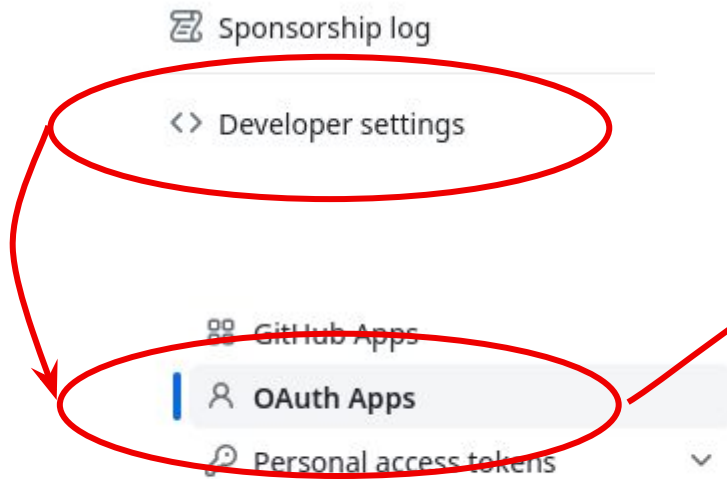
```
---
- name: Deploy IPA replica
  hosts: ipareplicas
  become: true

  roles:
  - role: ipareplica
    state: present
...
```

# External IdP configuration

- FreeIPA can be integrated with external identity providers (IdP)
- The integration requires configuration of FreeIPA as an OAuth client for the external IdP, add external IdP to FreeIPA, and configure users to authenticate through external IdP
- Example: Using Github as external IdP
  - Configure a new OAuth application on Github
  - Configure FreeIPA to use Github as external IdP
  - Configure FreeIPA user to authenticate through Github

# Create Github OAuth App



## No OAuth applications

OAuth applications are used to access the GitHub API. [Read the docs](#) to find out more.

Register a new application

# Create Github OAuth App



Confirm access



Signed in as @rafasgj



Security key

When you are ready, authenticate using the button below.

Use security key

## Register a new OAuth application

Application name \*

freeipa\_fosdem

Something users will recognize and trust.

Homepage URL \*

https://fosdem.ipa.test/ipa

The full URL to your application homepage.

Application description

A FreeIPA demo for FOSDEM.

This is displayed to all users of your application.

Authorization callback URL \*

https://fosdem.ipa.test/ipa

Your application's callback URL. Read our [OAuth documentation](#) for more information.

Enable Device Flow

Allow this OAuth App to authorize users via the Device Flow. Read the [Device Flow documentation](#) for more information.

Register application

Cancel

This is important!


# Create Github OAuth App

General

Optional features

Advanced

freeipa\_fosdem

 rafasgj owns this application. [Transfer ownership](#)



You can list your application in the [GitHub Marketplace](#) so that other users can discover it. [List this application in the Marketplace](#)

0 users [Revoke all user tokens](#)

**Client ID**  
546dff6fe371425452df

**Client secrets** [Generate a new client secret](#)

Make sure to copy your new client secret now. You won't be able to see it again.

  7b82da05d6fcd00b443492a96ab1cd02a95f461b [Copy](#)  
Added 1 minute ago by rafasgj  
Never used [Delete](#)

Client secret

You cannot delete the only client secret. Generate a new client secret first.

# Add IdP to FreeIPA

```
1  ---
2  - name: Setup external IdP
3    hosts: ipaserver
4    become: false
5    gather_facts: false
6
7    tasks:
8      - name: Ensure an external provider for Github is available
9        ipaidp:
10         ipaadmin_password: SomeADMINpassword
11         name: github_idp
12         provider: github
13         client_id: 481789d5cd3ca6b3f03f
14         secret: 979a1511df376e371c407760619148b82a2c4a6d
15         idp_user_id: 'id'
```

# Add user with external IdP

```
10     - name: Retrieve Github user id
11       ansible.builtin.uri:
12         url: "https://api.github.com/users/{{ github_login }}"
13         method: GET
14         headers:
15           Accept: "application/vnd.github.v3+json"
16       register: user_data
17
18     - name: Ensure user exists with IdP configuration
19       ipauser:
20         ipadmin_password: SomeADMINpassword
21         name: rafasgj
22         first: Rafael
23         last: Jeffman
24         userauthtype: idp
25         idp: github_idp
26         idp_user_id: "{{ user_data.json.id }}"
```

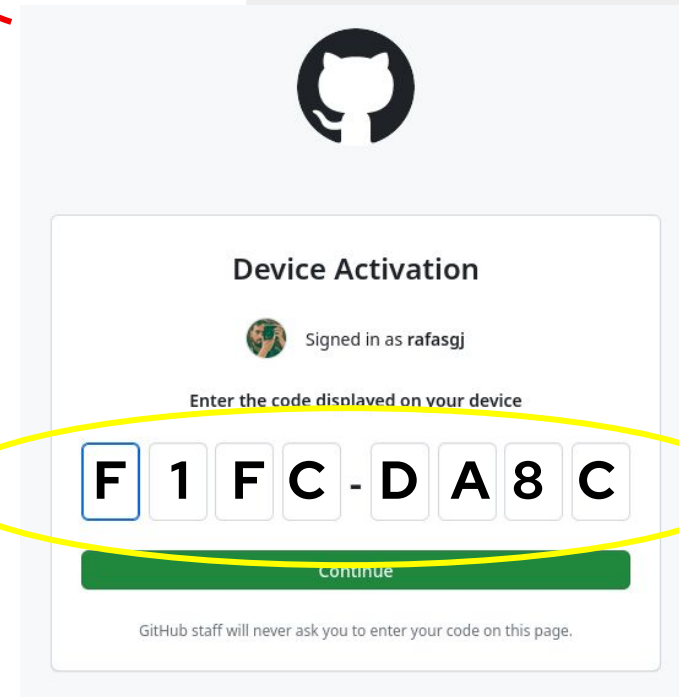


# User authentication

```
CentOS Stream 9
Kernel 5.14.0-412.el9.x86_64 on an x86_64

Activate the web console with: systemctl enable --now cockpit.socket

cs9 login: rafasgj
Authenticate with PIN F1FC-DABC at https://github.com/login/device and press ENTER.
Last login: Sat Feb  3 03:28:32 from 192.168.122.1
[rafasgj@cs9 ~]$
```



The image shows a GitHub Device Activation screen. At the top is the GitHub logo. Below it, the text reads "Device Activation". Underneath, there is a small globe icon and the text "Signed in as rafasgj". The main instruction is "Enter the code displayed on your device". Below this instruction is a row of seven input boxes containing the characters "F", "1", "F", "C", "-", "D", "A", "8", "C". A green "Continue" button is located below the input boxes. At the bottom, there is a small disclaimer: "GitHub staff will never ask you to enter your code on this page." Two yellow ovals highlight the PIN input area and the "Continue" button. Two red arrows originate from the PIN input area: one points to the terminal window on the left, and the other points to the terminal window on the right.

# Questions?