



Automatizando o gerenciamento de identidades centralizado com FreeIPA e Ansible

Rafael Jeffman

Senior Software Engineer / Red Hat

Thomas Woerner

Principal Software Engineer / Red Hat



O que é o FreeIPA?

- Identity, Policy , (- Audit)
- Sistema para gerenciamento centralizado de identidades e políticas de acesso.
- Oferece integração com Microsoft AD e provedores de identidade externos.
- Autenticação via SSSD
- Autorização e SSO via TGT Kerberos.
- Gerenciamento via CLI, WebUI e Ansible

O que é o ansible-freeipa?

- Provê módulos e *roles* Ansible para o FreeIPA
- Procura criar uma interface consistente de gerenciamento
- Comandos são agrupados em tarefas
- Utiliza contextos *server* e *client*
- Comandos idempotentes
- Executa em *batch mode* para maior otimização
(**em breve**)

Implantação com ansible-freeipa

Em inventory.yml:

```
ipaserver:
  hosts:
    server.lin.ipa.test:
      ansible_user: root
  vars:
    ipaserver_setup_kra: false
    ipaserver_setup_dns: true
    ipaserver_no_forwarders: true
    ipaserver_auto_reverse: true
    ipaserver_setup_adtrust: true
    ipaserver_netbios_name: IPA
    ipaserver_no_hbac_allow: true
```

Role para criar o servidor:

- role: ipaclient
state: present

Integração com MS AD

- Utilizando os playbooks de <https://github.com/rjeffman/freeipa-ad-trust.git>
 - Configure
 - ipaserver_timezone, winserver_timezone os endereços de IP no arquivo inventory.yaml

- Preparação do controlador

```
git clone https://github.com/rjeffman/freeipa-ad-trust.git
cd freeipa-ad-trust/
pip install -r requirements.txt
ansible-galaxy collection install -r requirements.yml
```

- É muito importante que os horários e as *time zones* dos *hosts* estejam corretos.

Configuração do Microsoft AD

- Preparação correta do windows (nome do servidor, DNS, configuração IP)
- Poderes necessário desabilitar o IPv6 no *playbook* `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
```

Configuração do FreeIPA

```
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 como 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~]$ 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~]$ 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~]$ ipa user-add testuser --first=f --last=l
ipa: ERROR: Insufficient access: Invalid credentials
```


Habilitando o administrador do AD para atuar como admin IPA

- name: Enable AD administrator to act as a FreeIPA admin.
hosts: ipaserver
tasks:
 - name: Ensure idoverride for administrator@ad.ipa.test
ipaoverrideuser:
 - ipaadmin_password: SomeADMINpassword
 - idview: default trust view
 - anchor: administrator@ad.ipa.test
- name: Ensure idoverride for administrator@ad.ipa.test is in admins group
ipagroup:
 - ipaadmin_password: SomeADMINpassword
 - name: admins
 - idoverrideuser: administrator@ad.ipa.test

Usando administrator como 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"
```

```
-----
```

Adicionando um Cliente

Important: Use o AD administrator corretamente: Administrator@AD.IPA.TEST

```
Em inventory.yml
  ipaclients:
    hosts:
      client1.lin.ipa.test:
        ansible_user: root
    vars:
      ipaclient_configure_dns_resolver: yes
      ipaclient_dns_servers: 192.168.122.251
      ipaadmin_principal: Administrator@AD.IPA.TEST
      ipaadmin_password: SomeW1Npassword
```

Playbook para criar o cliente:

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

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

Adicionando uma Réplica

Workaround temporário: Desabilitar a verificação de conexão.

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

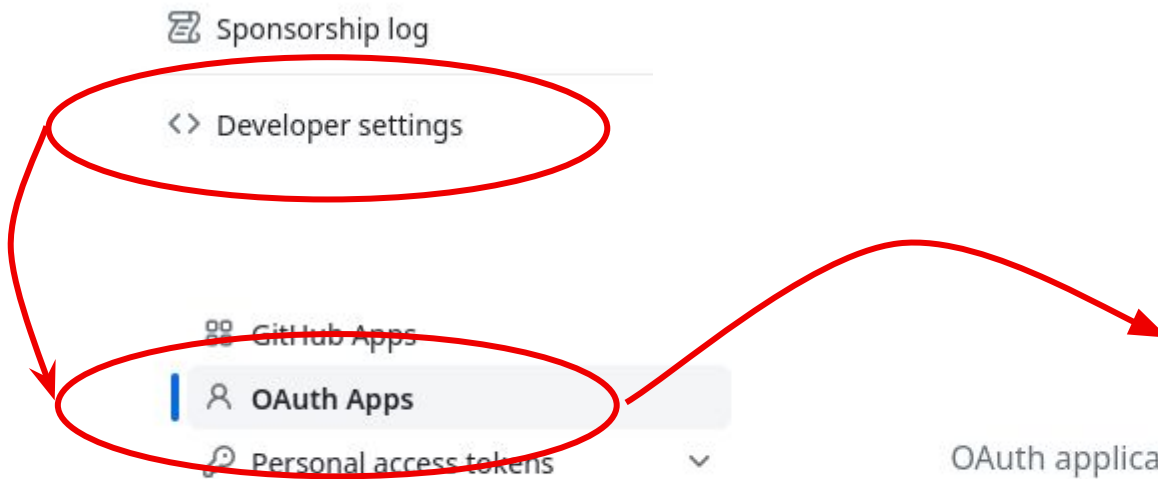
  roles:
    - role: ipareplica
      state: present
...
```

Utilizando External IdP

- FreeIPA pode ser integrado com provedores de identidade externos (IdP), como Entra ID, Github, Keycloak, Google.
- O FreeIPA deve ser configurado como um cliente OAuth
- O IdP deve ser adicionado ao FreeIPA
- Os usuários devem ser configurados para realizar a autenticação pelo IdP

Exemplo: Utilizando o Github como External IdP

Criar uma aplicação OAuth no Github



No OAuth applications

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

Register a new application

Criação da 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

Enter 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

MUITO IMPORTANTE


Criação da 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.

 Client secret

✓ 7b82da05d6fcd00b443492a96ab1cd02a95f461b


Added 1 minute ago by rafasgj

Never used

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

Delete

17



FreeIPA
Open Source Identity Management Solution

Adiciona o IdP ao FreeIPA

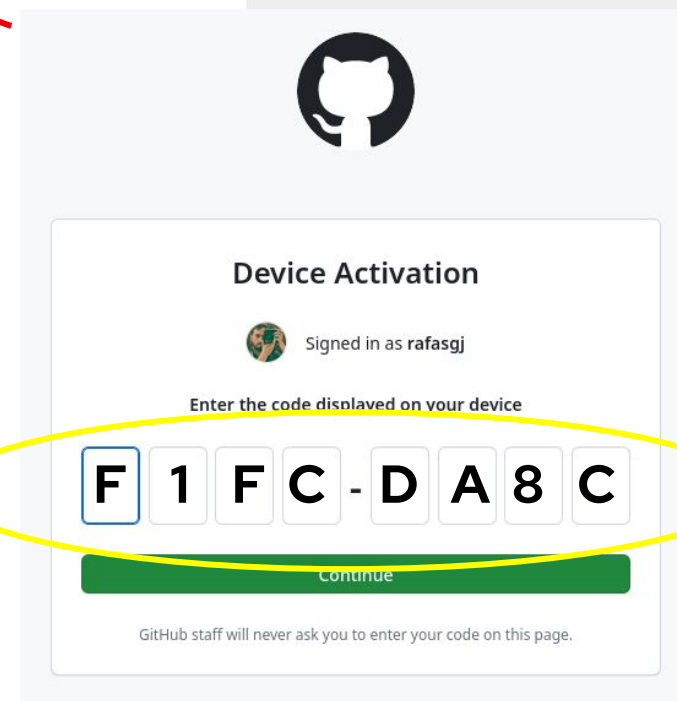
```
1  ---
2  - name: Setup external IdP
3    hosts: ipaserver
4    become: false
5    gather_facts: false
6
7    tasks:
8      - name: Ensure an external provider for Github is available
9        ipaidp:
10          ipaadmin_password: SomeADMINpassword
11          name: github_idp
12          provider: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

Adiciona user com 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         ipaadmin_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 }}"
```

Autenticação

```
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 "Device Activation" is centered. Underneath, there's a small profile picture and the text "Signed in as rafasgj". Below that, it says "Enter the code displayed on your device". The code is displayed in a row of boxes: F, 1, F, C, -, D, A, 8, C. The first box 'F' is highlighted with a blue border. Below the code boxes is a green "Continue" button. At the bottom, a small note says "GitHub staff will never ask you to enter your code on this page."

Seguindo em frente...

- Esta apresentação e seus playbooks:
 - <https://github.com/rjeffman/flisol2024>
- <https://freeipa.org>
 - [Quick Start Guide](#)
 - [Deployment Recommendations](#)
- Documentação do ansible-freeipa
 - <https://www.freeipa.org/ansible-freeipa.github.io>

Dúvidas?

<https://freeipa.org>

