Protegendo contas privilegiadas com ferramentas *open source*

TLP:CLEAR

PALESTRANTE

ANDRÉ TORRES

WHOAMI

- ✓ Auditor de cibersegurança (2010)
  - ✓ APF – crimes cibernéticos (2005-2010)

- ✓ Bacharel em Ciência da Computação pela Universidade de Brasília (UnB). Pós-graduado em Segurança da Informação (UPIS) e em Governança de Tecnologia da Informação e Comunicação no Setor Público (UnB).

- ✓ Experiência nas áreas de gestão de incidentes e vulnerabilidades, segurança em infraestrutura do AD, ofensiva e auditoria.

- ✓ Consultor de cibersegurança e instrutor de cursos de AD, ADCS, Purple Team

andretorresbr

O desafio da gestão de acesso privilegiado

Atacante **não** mais **hackeia**, ele **acessa**

79% dos ataques de ransomware usaram identidades como vetor de acesso inicial

Descoberta foi documentada no State of Ransomware 2026 da Sophos, anunciada hoje (15) pela empresa. De acordo com os executivos da companhia, esse cenário é fruto de uma coordenação maior de diversos eventos maliciosos a partir da Inteligência Artificial, exigindo que a Cibersegurança caminhe com mais urgência à defesa interconectada

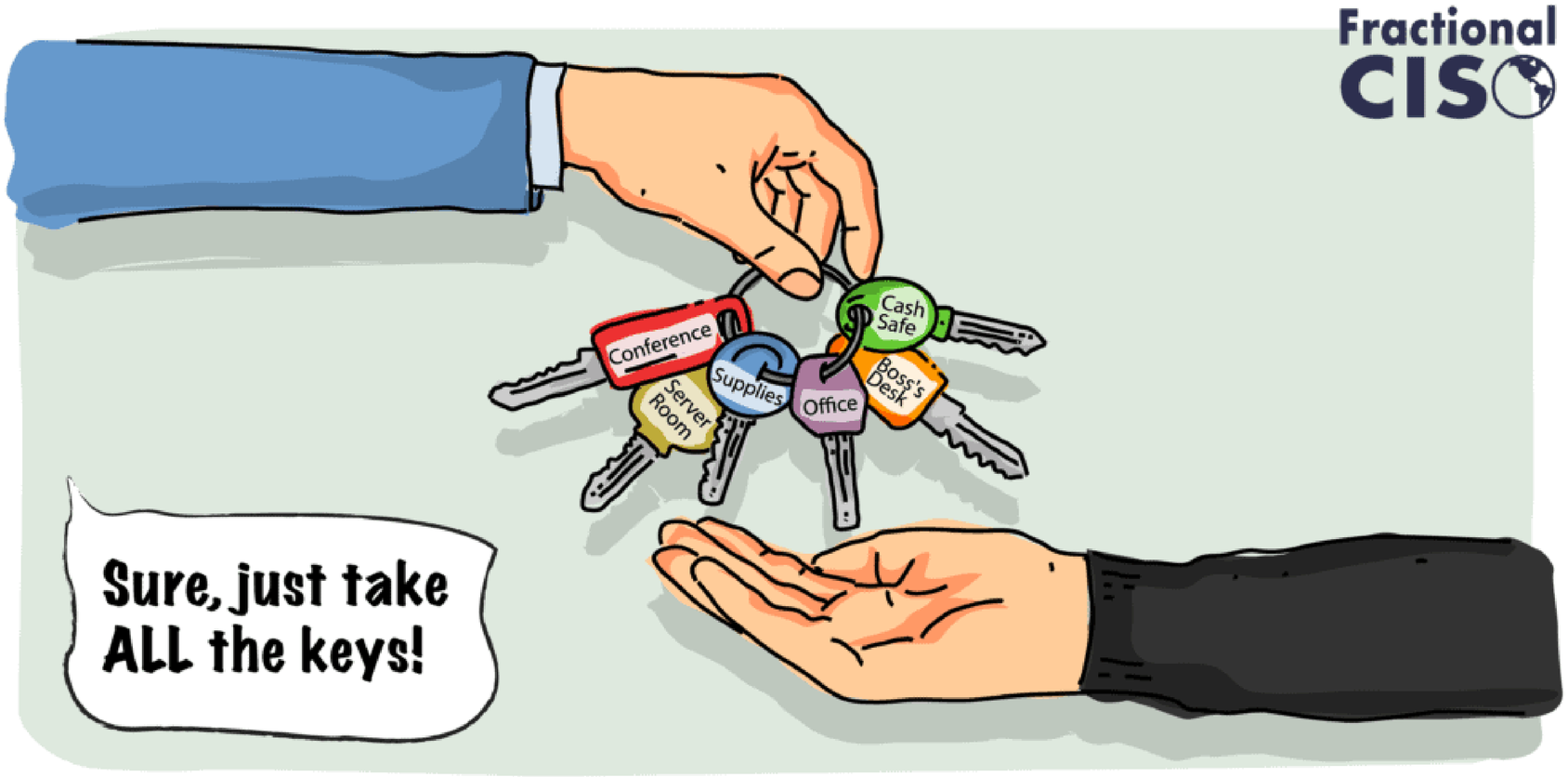
Por: Matheus Bracco julho 15, 2026 Destaques

O desafio da gestão de acesso privilegiado

- Dificuldades da gestão de contas privilegiadas
  - Senhas fracas

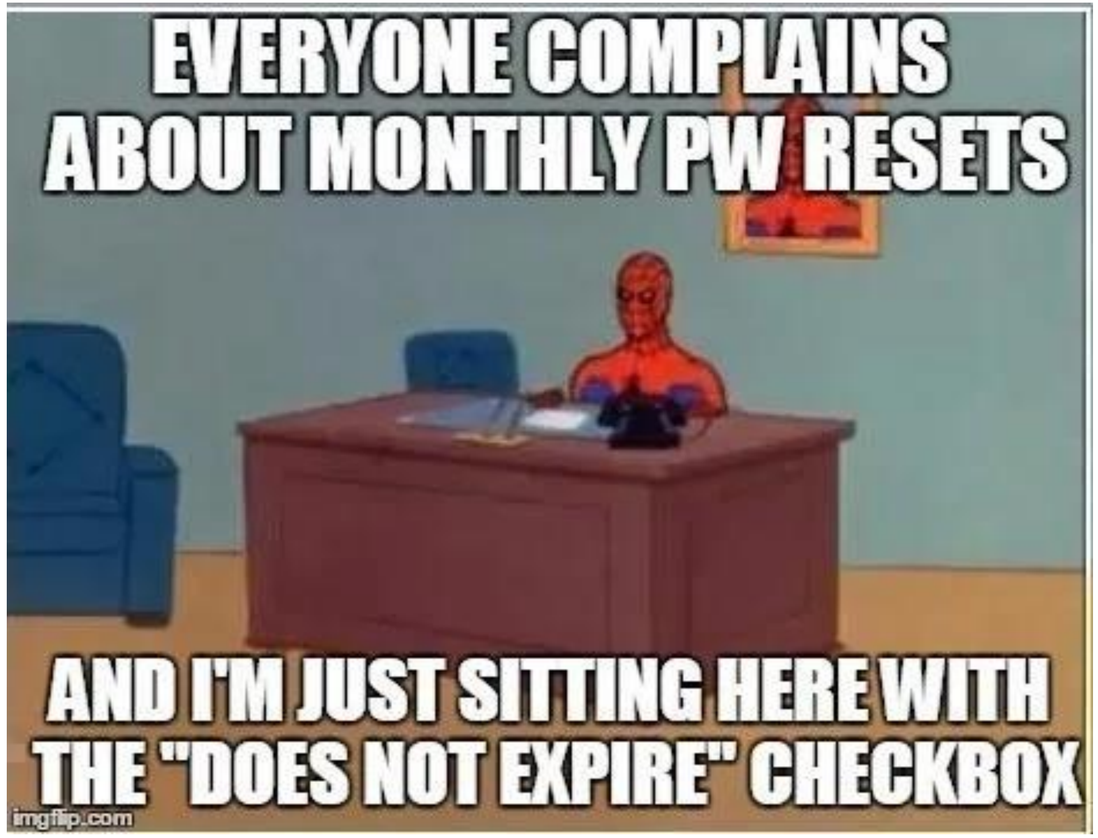
O desafio da gestão de acesso privilegiado

- Dificuldades da gestão de contas privilegiadas
  - Excesso de privilégios + privilégios constantes



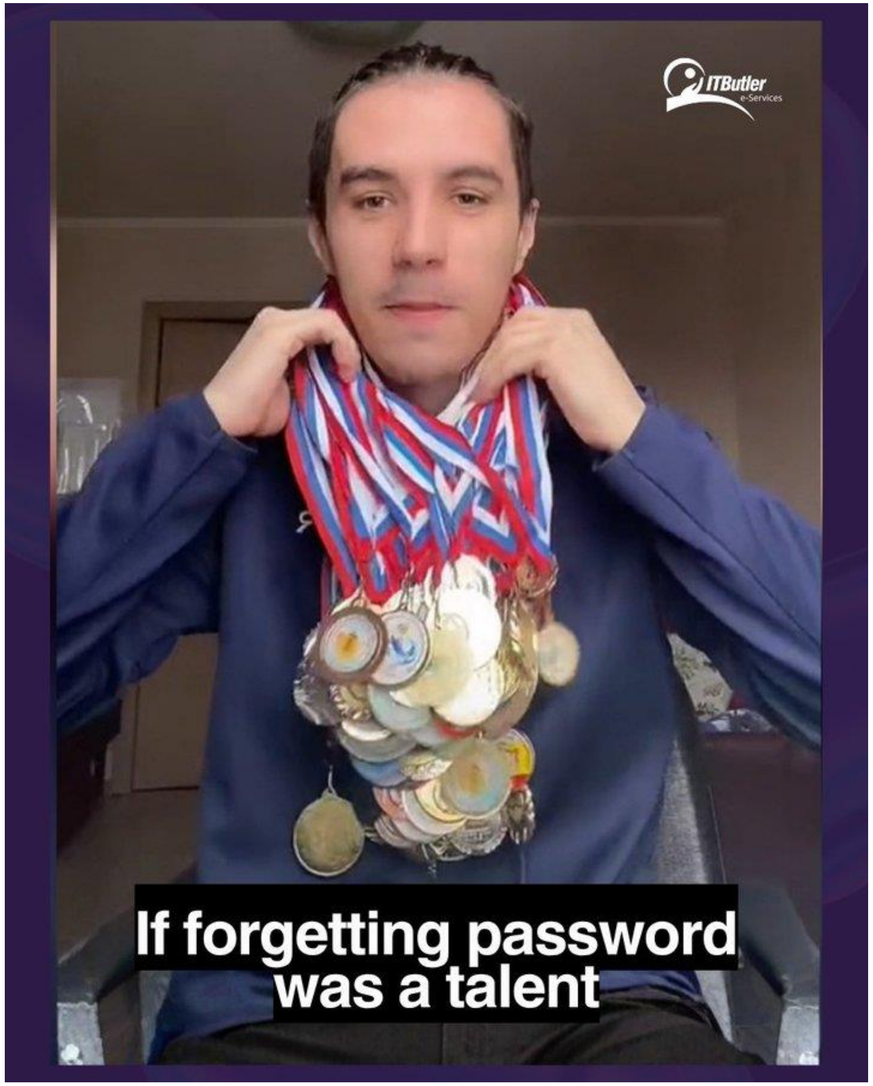
O desafio da gestão de acesso privilegiado

- Dificuldades da gestão de contas privilegiadas
  - Senhas imutáveis, sequenciais ou raramente modificadas

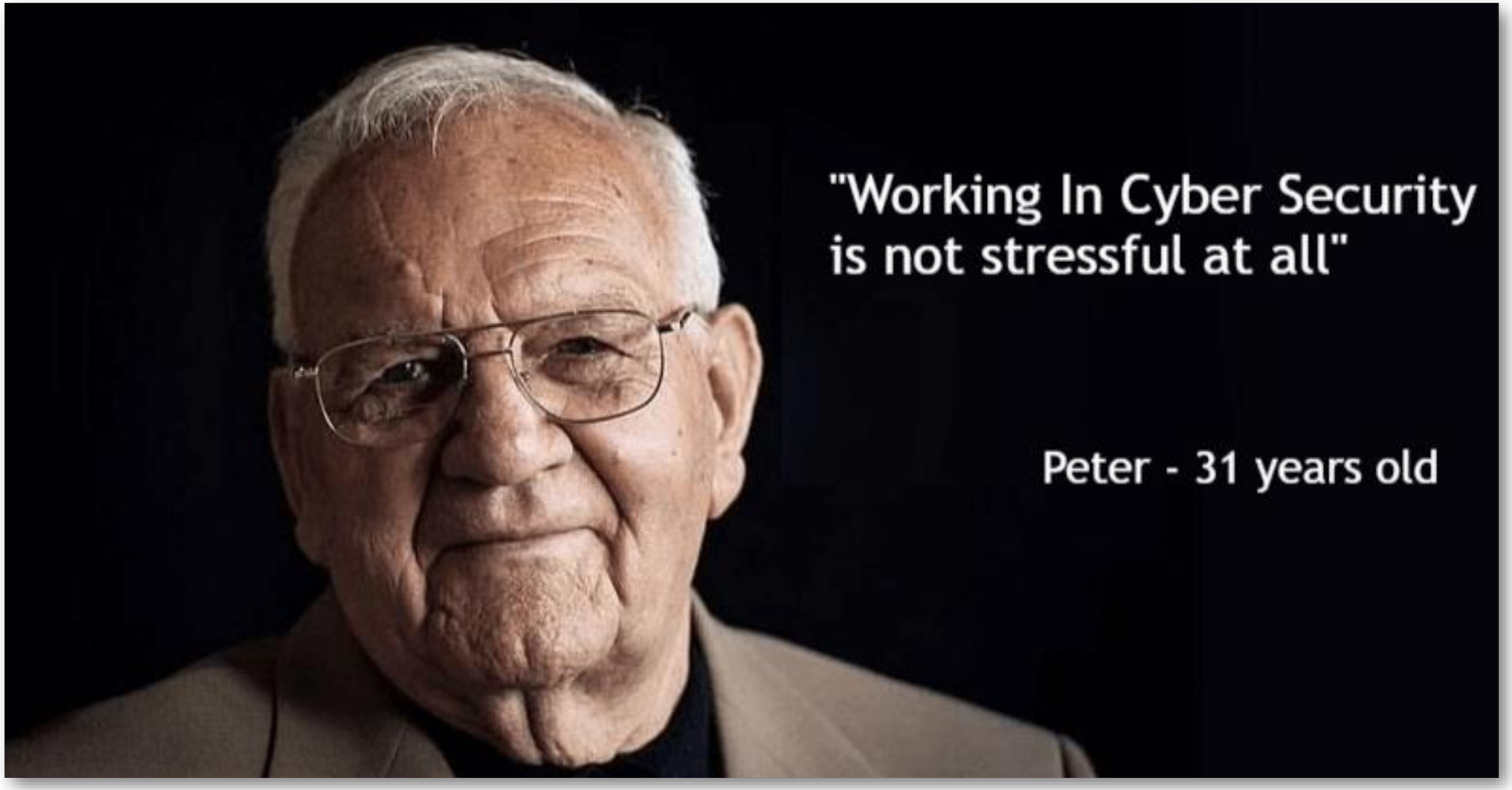


O desafio da gestão de acesso privilegiado

- Dificuldades da gestão de contas privilegiadas
  - **Se não for fraca, onde armazená-las?**
- Na vida **pessoal**, usamos gerenciadores de senhas
  - Bitwarden, LastPass, 1Password, etc
- E na vida **corporativa**?



O desafio da gestão de acesso privilegiado



Agenda

- Active Directory (AD) e a importância do Tiering
- A solução: HashiCorp Vault (cofre de segredos)
- Autenticação segura: Authentik IdP
- Demonstração: o cofre em ação
- Conclusão e próximos passos

Active Directory (AD) e a importância do Tiering

3 **Autorização**

Concedendo acesso a recursos com base em funções e políticas.

2 **Autenticação**

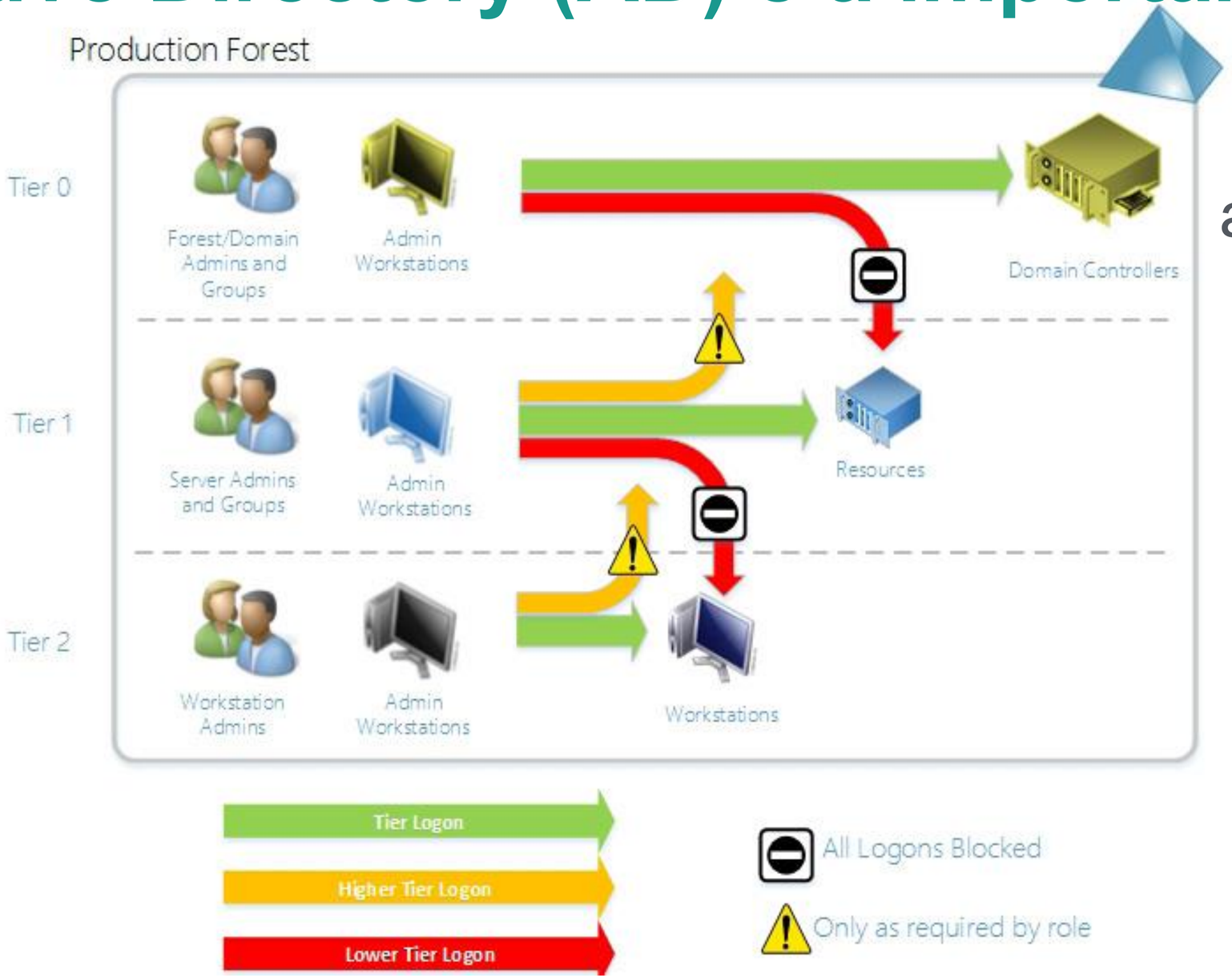
Valida a identidade do usuário através de senhas, biometria ou outros fatores.

1 **Identificação**

Estabelece a identidade do usuário através de identificadores únicos.

Active Directory

Active Directory (AD) e a importância do Tiering



andre.torres_da

andre.torres_a

andre.torres

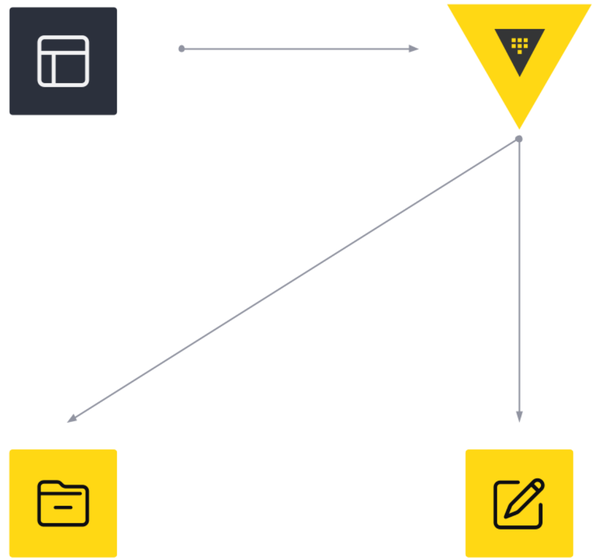
A solução: HashiCorp Vault (cofre de segredos)

- Ferramenta aberta para gerenciamento e acesso a **secrets**
  - 2023 mudou licença para BSL, fork *OpenBao*
  - Armazena chaves de API, usuários + senhas, certificados, tokens, etc
- Provê interface de acesso unificada aos secrets
  - Controle de acesso: quem pode acessar uma secret
  - Logs de auditoria detalhado: quem acessou o que
- Centralização de secrets que antes estavam espalhados em estações de devs e servidores (*secret sprawl*)

HashiCorp Vault

A solução: HashiCorp Vault (cofre de segredos)

- Gerenciamento de secrets
  - **Estáticos** (“*KeePass corporativo com API*”)
    - Armazena secrets no cofre de forma criptografada
    - Não expiram ou revogam a credencial
    - Credenciais permanentes
    - Ex: credencial de um usuário permanente no SGBD
  - **Dinâmicos** (JIT)
    - Criação de secrets no momento e com vida curta
    - Credenciais temporárias (TTL)
    - Ex: credencial temporária de SGBD para uma operação específica



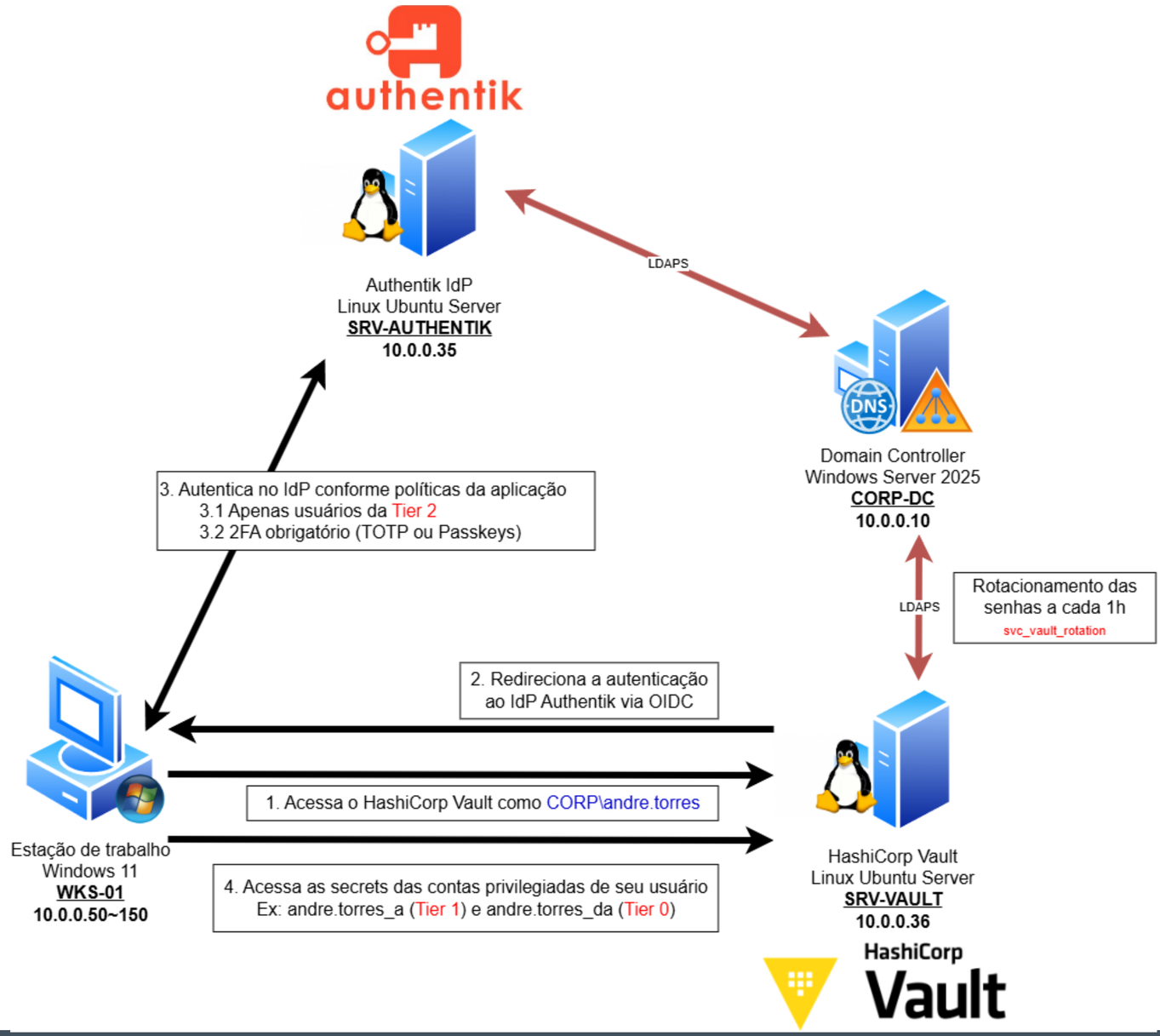
A solução: HashiCorp Vault (cofre de segredos)

- Secrets engines
  - Plugins de gerenciamento de soluções
  - Banco de dados (PostgreSQL, MySQL, MongoDB, MSSQL, Oracle, Snowflake, etc)
  - Plataformas Cloud (AWS, Azure, GCP)
  - Orquestração (Kubernetes, Nomad)
  - Redes e acesso (Consul, RabbitMQ, SSH)
  - TOTP
  - PKI
  - LDAP/S

HashiCorp Vault

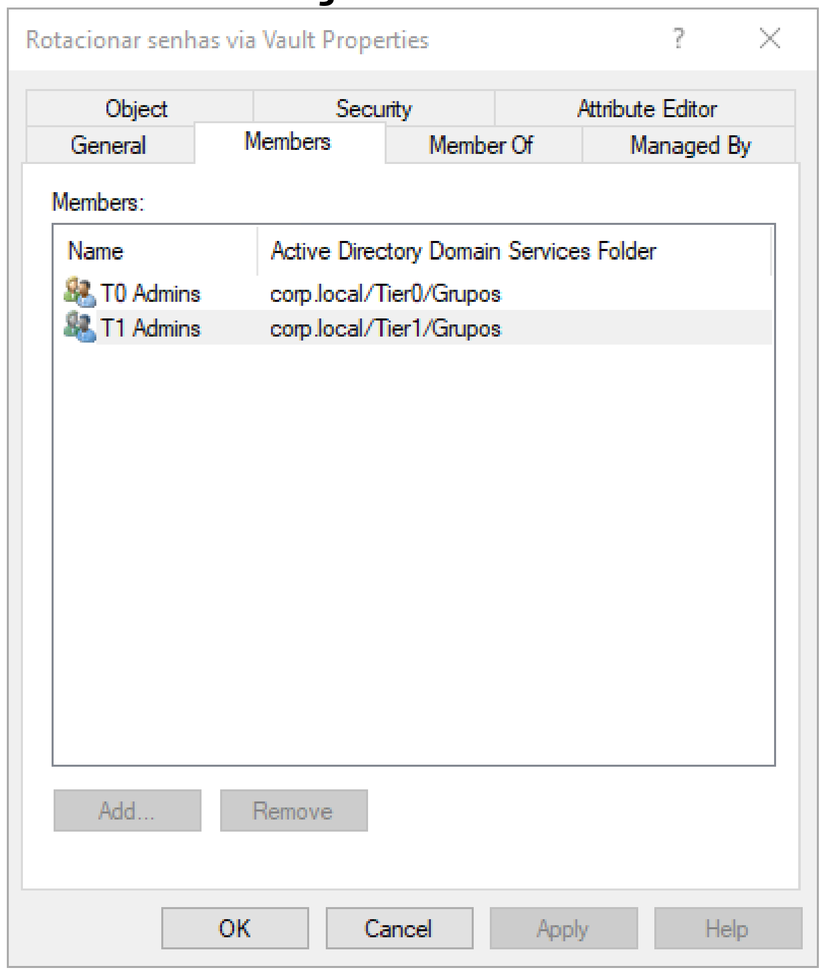
A solução: HashiCorp Vault (cofre de segredos)

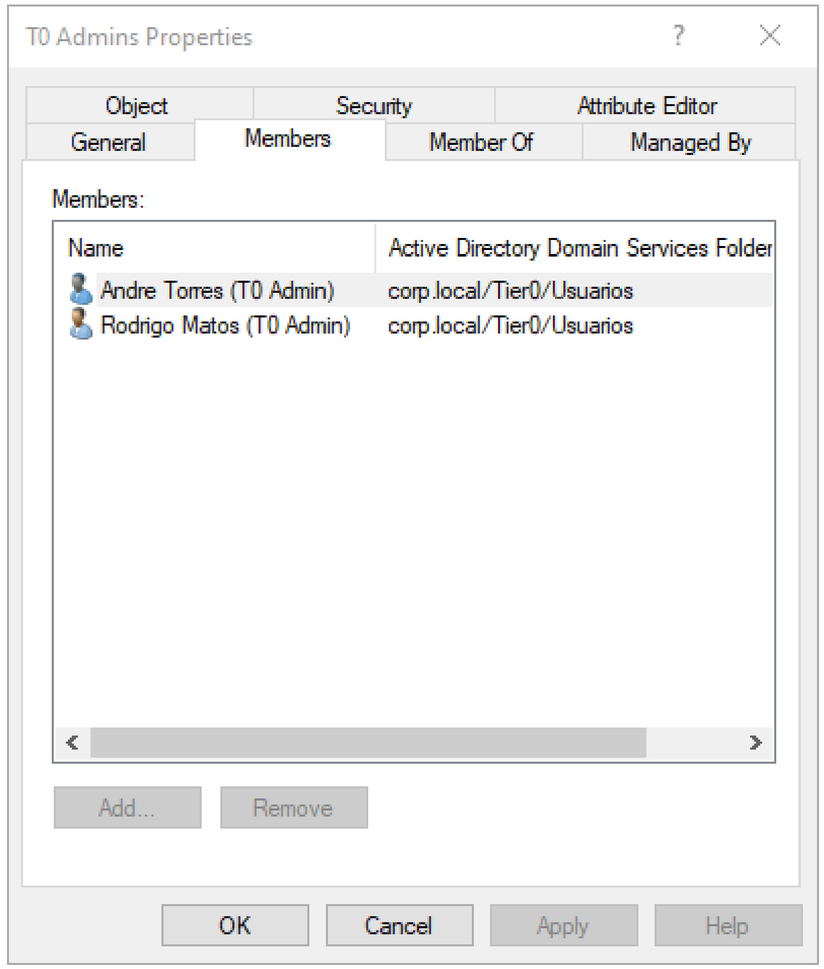
- Secrets engine escolhida: **LDAP/S**
  - Rotação das senhas de contas privilegiadas (Tier 0 e Tier 1) a cada 1h
  - Senhas complexas de 64 caracteres
  - Usuário **username** só tem acesso à senha de suas contas **username_a** e **username_da** via Vault

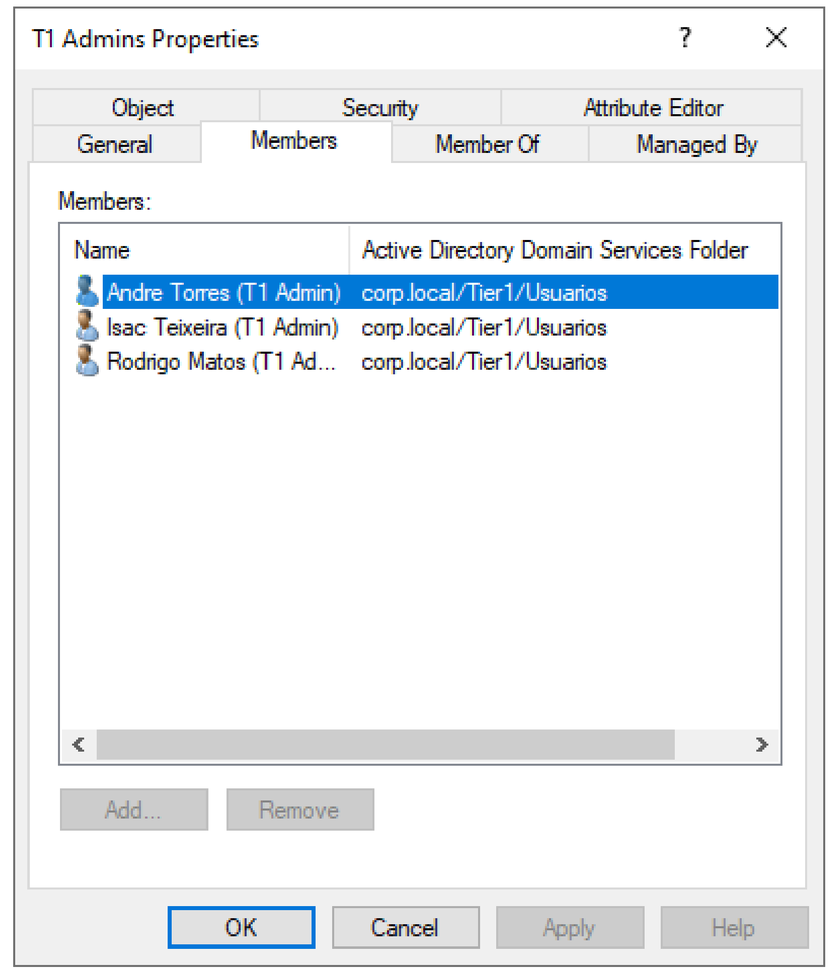


A solução: HashiCorp Vault (cofre de segredos)

- Para um usuário ter sua senha rotacionada, basta incluí-lo no grupo de rotação de senhas







A solução: HashiCorp Vault (cofre de segredos)

- Script de sincronismo
  - Executa a cada 6hs
  - Varre os membros do grupo do AD e garante que todos estão sendo gerenciados pelo Vault
    - Se algum usuário foi inserido no grupo, insere no Vault
    - Se algum usuário foi removido do grupo, remove do Vault

```
root@srv-vault:/opt/vault/sync# vault list corp.local/static-role/
Keys
----
andre.torres_a
andre.torres_da
isac.teixeira_a
rodrigo.matos_a
rodrigo.matos_da
root@srv-vault:/opt/vault/sync#
```

A solução: HashiCorp Vault (cofre de segredos)

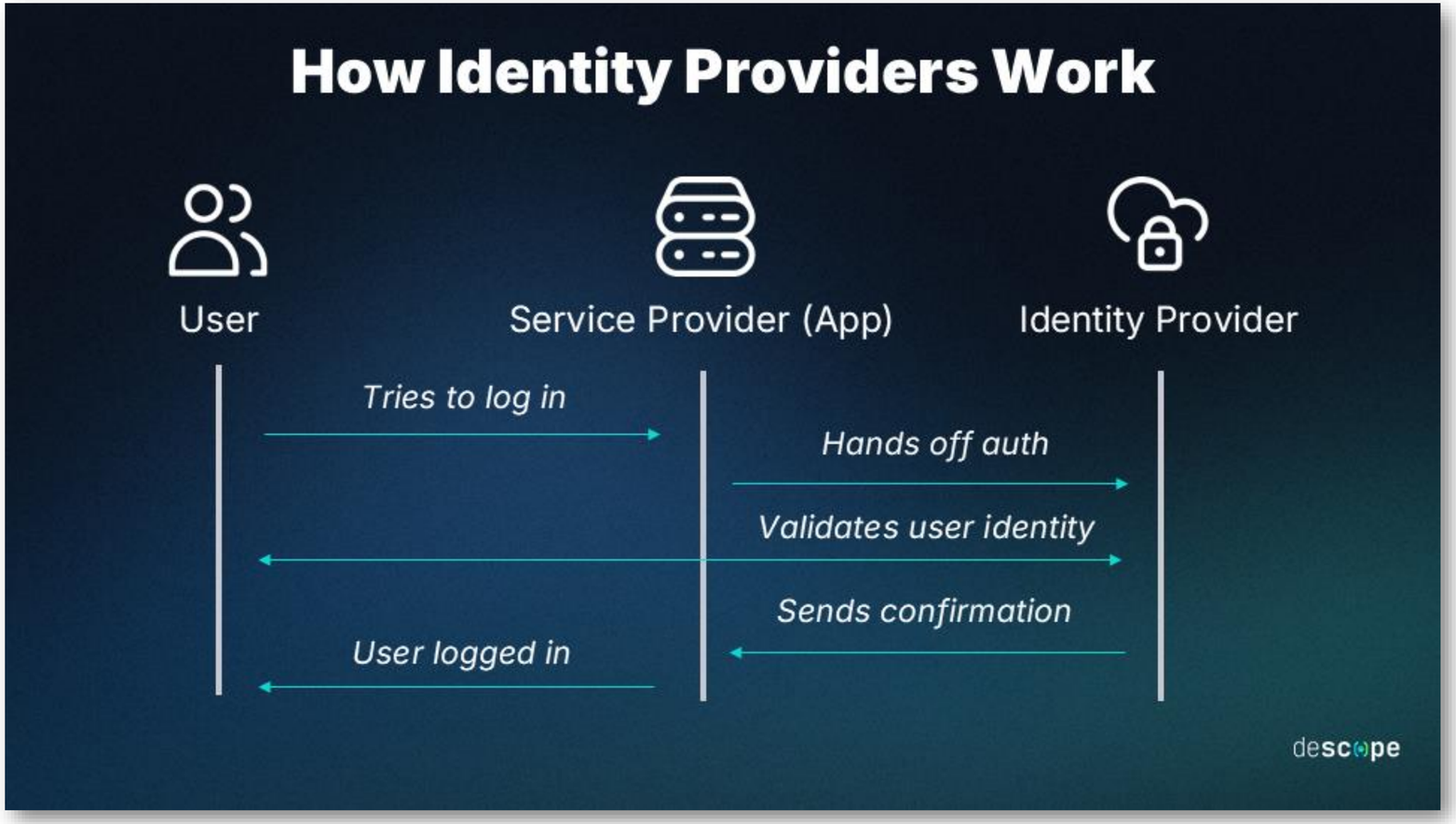
- Script de sincronismo

```
root@srv-vault:/opt/vault/sync# cat logs/2026/06/2026-06-10.log

============================================================
--- INÍCIO DA SINCRONIZAÇÃO AD/VAULT (Wed Jun 10 18:00:01 -03 2026) ---
============================================================
--- Autenticando no Vault via AppRole ---
[SUCESSO] Autenticado e token de curta duração obtido.
Buscando contas de serviço recursivamente no grupo 'Rotacionar senhas via Vault' (DN: CN=Rotacionar senhas via Vault,OU=Papeis,OU=Tier0,DC=corp,DC
=local)...
Contas de Serviço encontradas para Static Roles:
andre.torres_a
isac.teixeira_a
rodrigo.matos_a
andre.torres_da
rodrigo.matos_da
--- Processando criação de Static Roles ---
  -> Processando role: andre.torres_a
    [INFO] Static role andre.torres_a já existe. Pulando criação.
  -> Processando role: isac.teixeira_a
    [INFO] Static role isac.teixeira_a já existe. Pulando criação.
  -> Processando role: rodrigo.matos_a
    [INFO] Static role rodrigo.matos_a já existe. Pulando criação.
  -> Processando role: andre.torres_da
    [INFO] Static role andre.torres_da já existe. Pulando criação.
  -> Processando role: rodrigo.matos_da
    [INFO] Static role rodrigo.matos_da já existe. Pulando criação.
--- Processando limpeza de Static Roles obsoletas ---
============================================================
--- FIM DA SINCRONIZAÇÃO AD/VAULT (Wed Jun 10 18:00:02 -03 2026) ---
============================================================
--- Revogando token AppRole ---
root@srv-vault:/opt/vault/sync#
```

A solução: HashiCorp Vault (cofre de segredos)

- Como proteger o acesso ao Vault?
  - Autenticação OAuth2/OIDC com Identity Provider (IdP) - MFA seguro

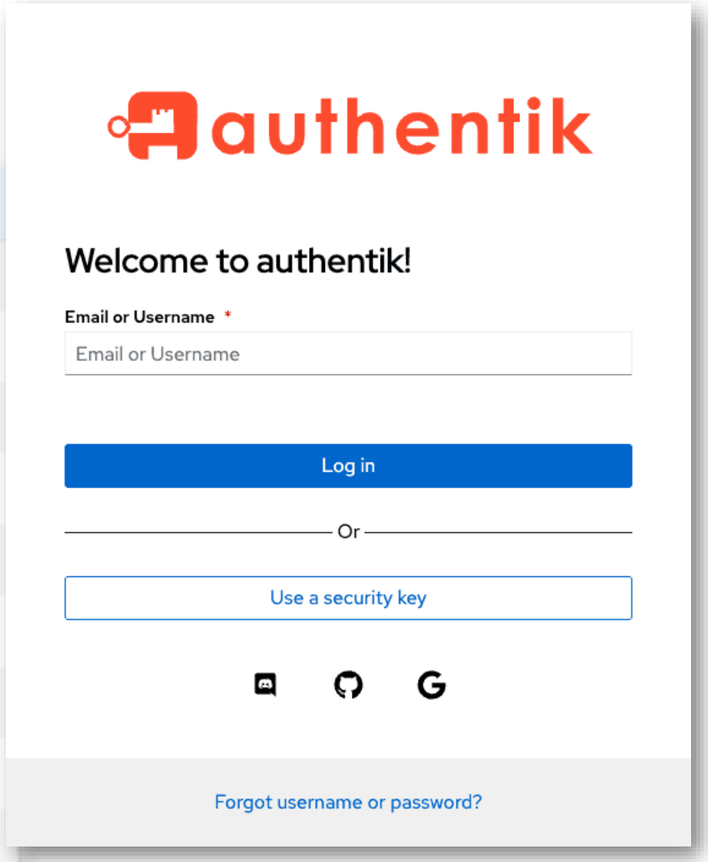


Fonte: https://www.descope.com/learn/post/identity-provider

Autenticação segura: Authentik IdP

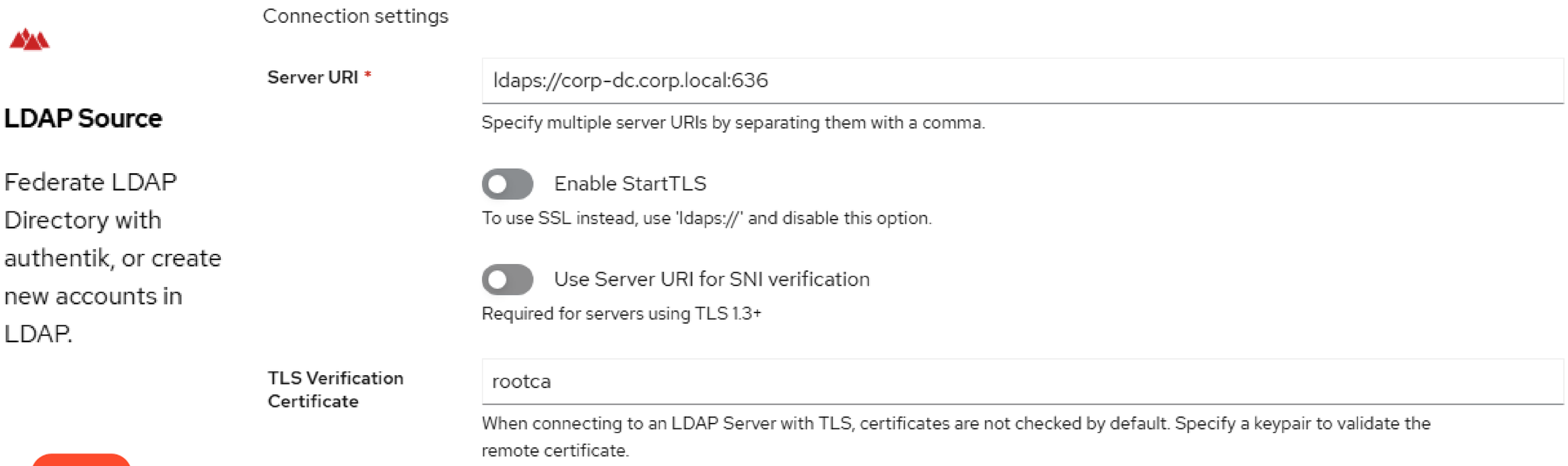
- Soluções abertas de IdP: Keycloak, Authelia, Authentik

Core Capabilities	authentik	Okta	Microsoft ADFS	Azure/Entra ID	Keycloak	Duo	Authelia
Self-host Anywhere	✓	✗	⚠	✗	✓	✗	✓
MFA ⓘ	✓	✓	✗	✓	✓	✓	✓
Conditional Access	✓	✓	✓	⚠	✓	⚠	✓
Open-source/Source Available	✓	✗	✗	✗	✓	✗	✓
Application Proxy	✓	✗	⚠	✓	⚠	✗	✗
FIPS Compliance	✓	⚠	✓	✓	✓	⚠	✗
Enterprise Support	✓	✓	✗	✓	⚠	✓	✗
WebAuthn (Passkeys)	✓	✓	✓	✓	✓	✓	✓
GeoIP / Impossible Travel	✓	✓	✓	✓	✗	✓	✗
Remote Access (RDP, VNC, SSH)	✓	✗	✗	✗	✗	✗	✗
OIDC Back-Channel Logout	✓	✗	✗	✗	✓	✗	✗



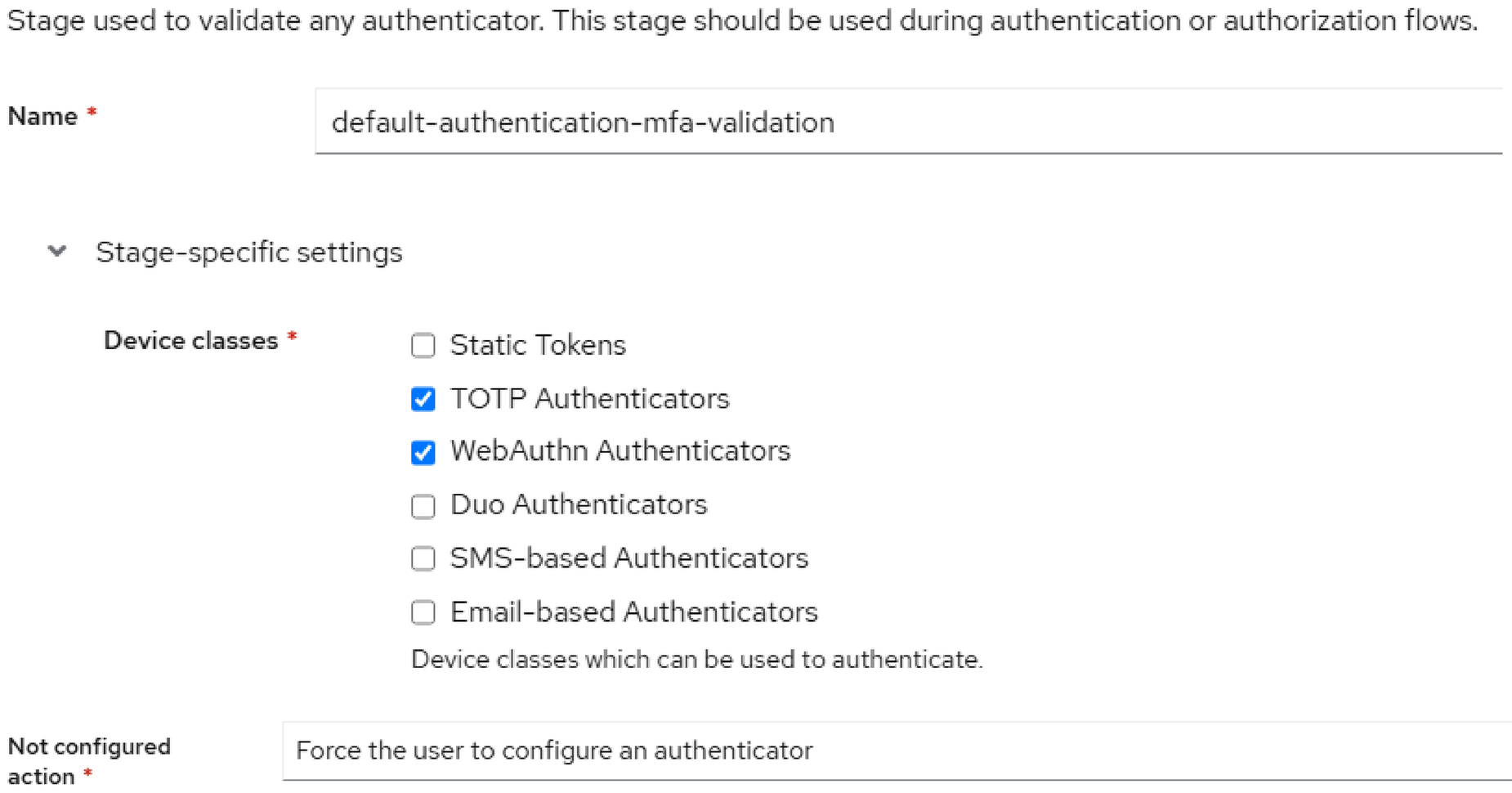
Autenticação segura: Authentik IdP

- Autenticação LDAPs integrada ao Active Directory



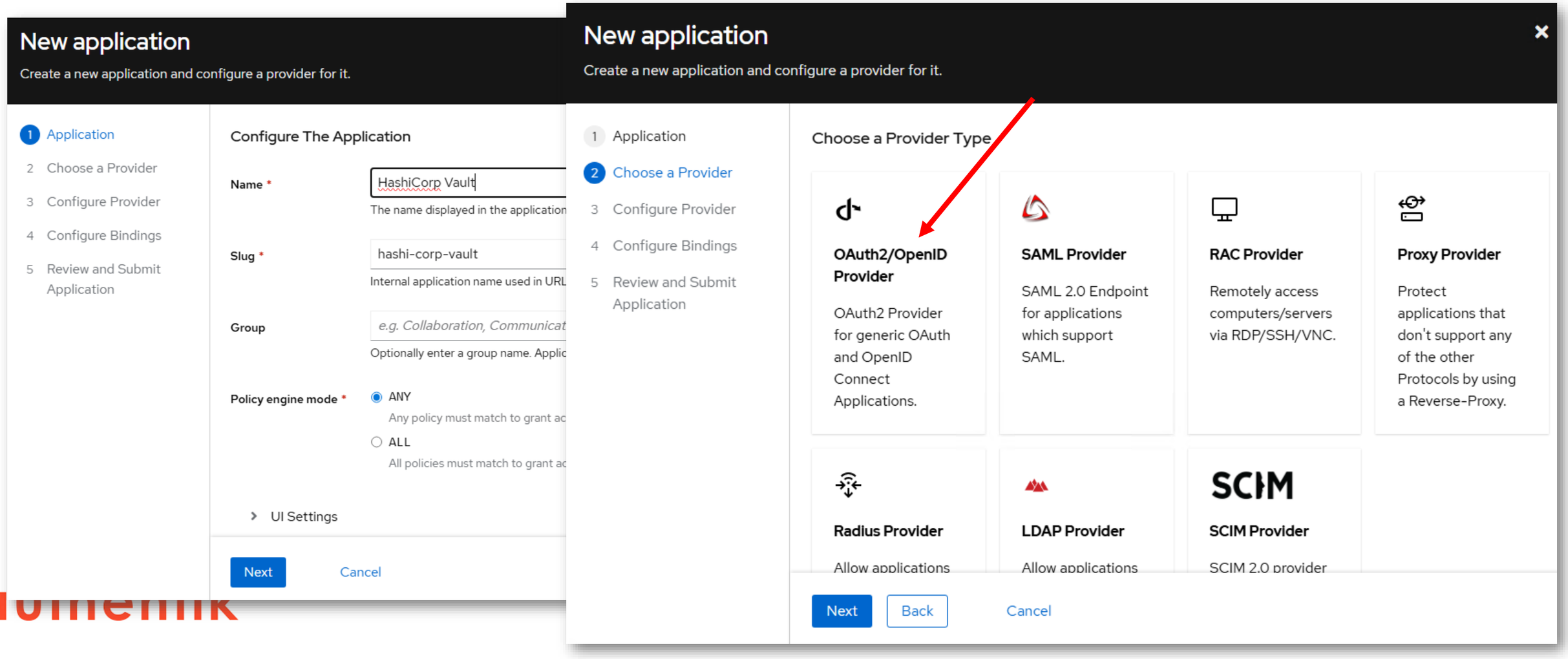
Autenticação segura: Authentik IdP

- Enforcement de MFA para todos os usuários



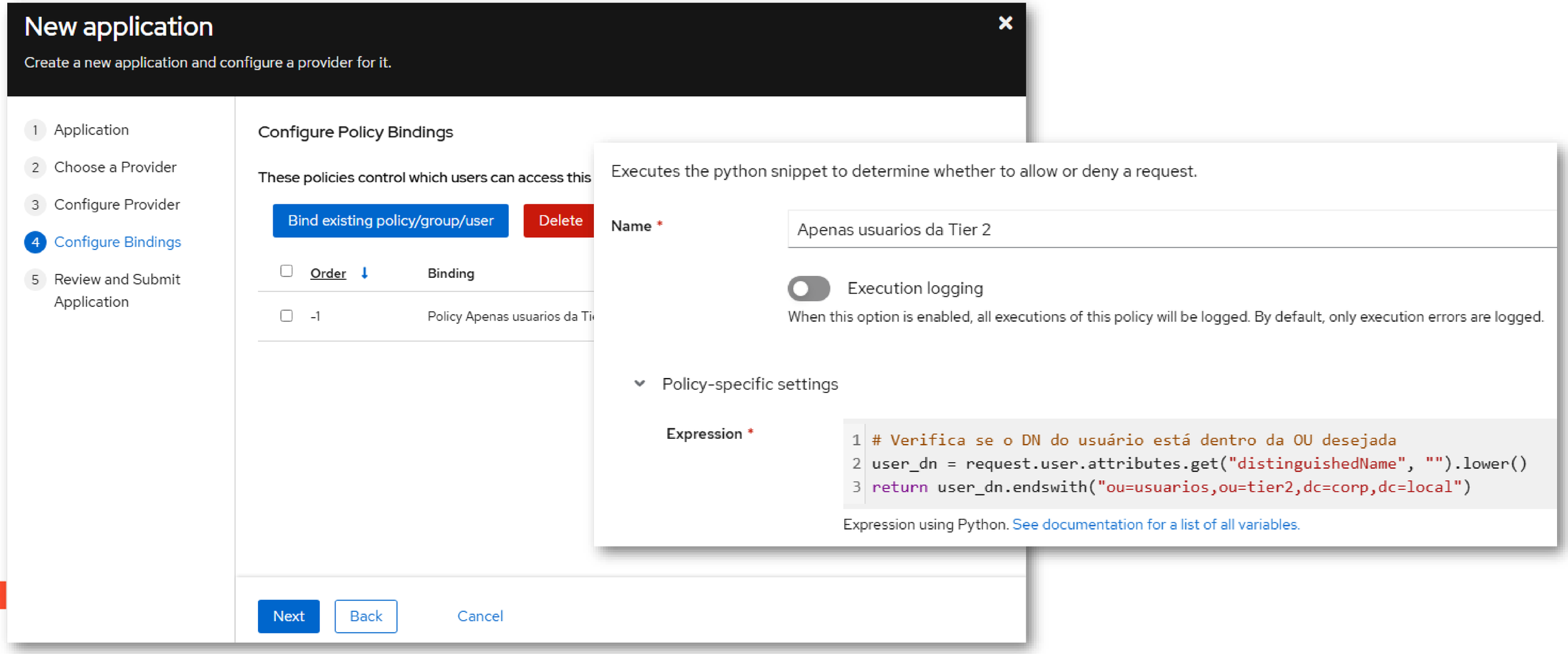
Autenticação segura: Authentik IdP

- Criação de Application e Provider OIDC no Authentik



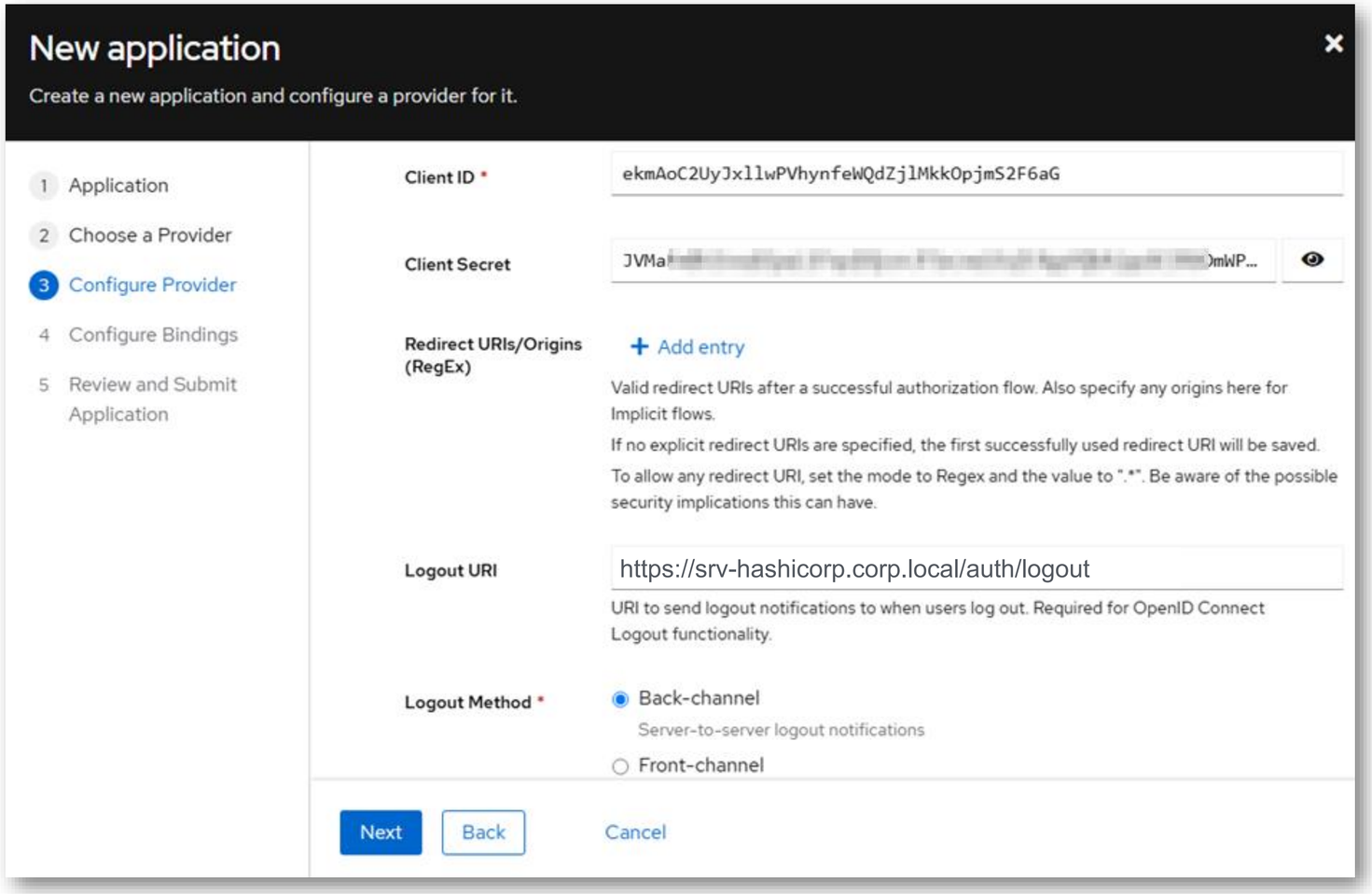
Autenticação segura: Authentik IdP

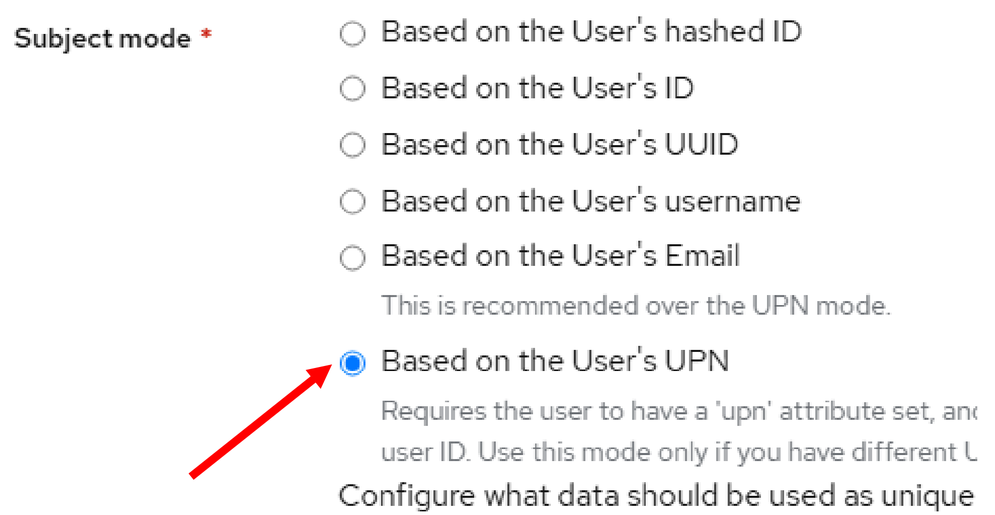
- Restrição via policy: apenas usuários Tier 2 se autenticam no Vault



Integração LAM + Authentik com 2FA

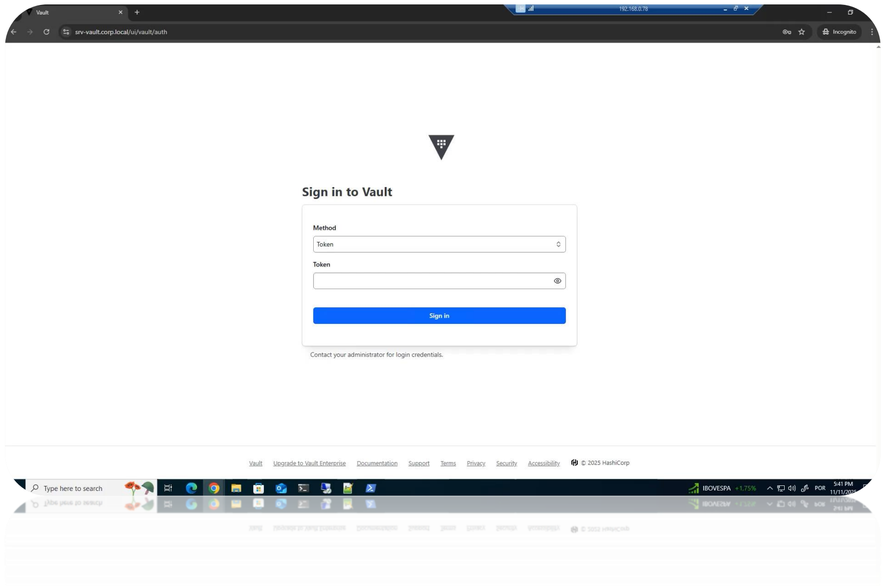
- Criação de Application e Provider OIDC no Authentik





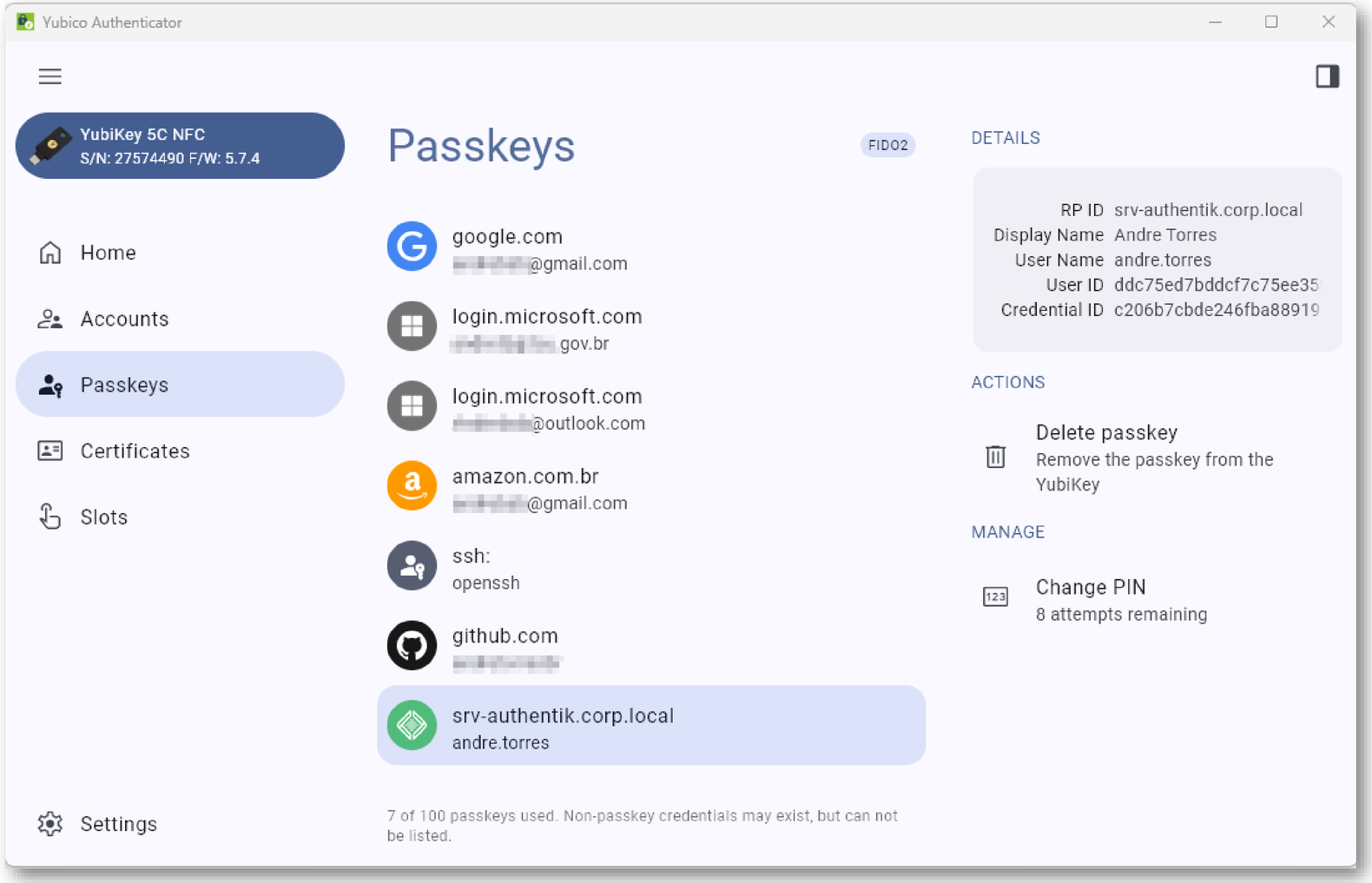
Demonstração: o cofre em ação

- Cenário: acesso válido às credenciais usando Passkey



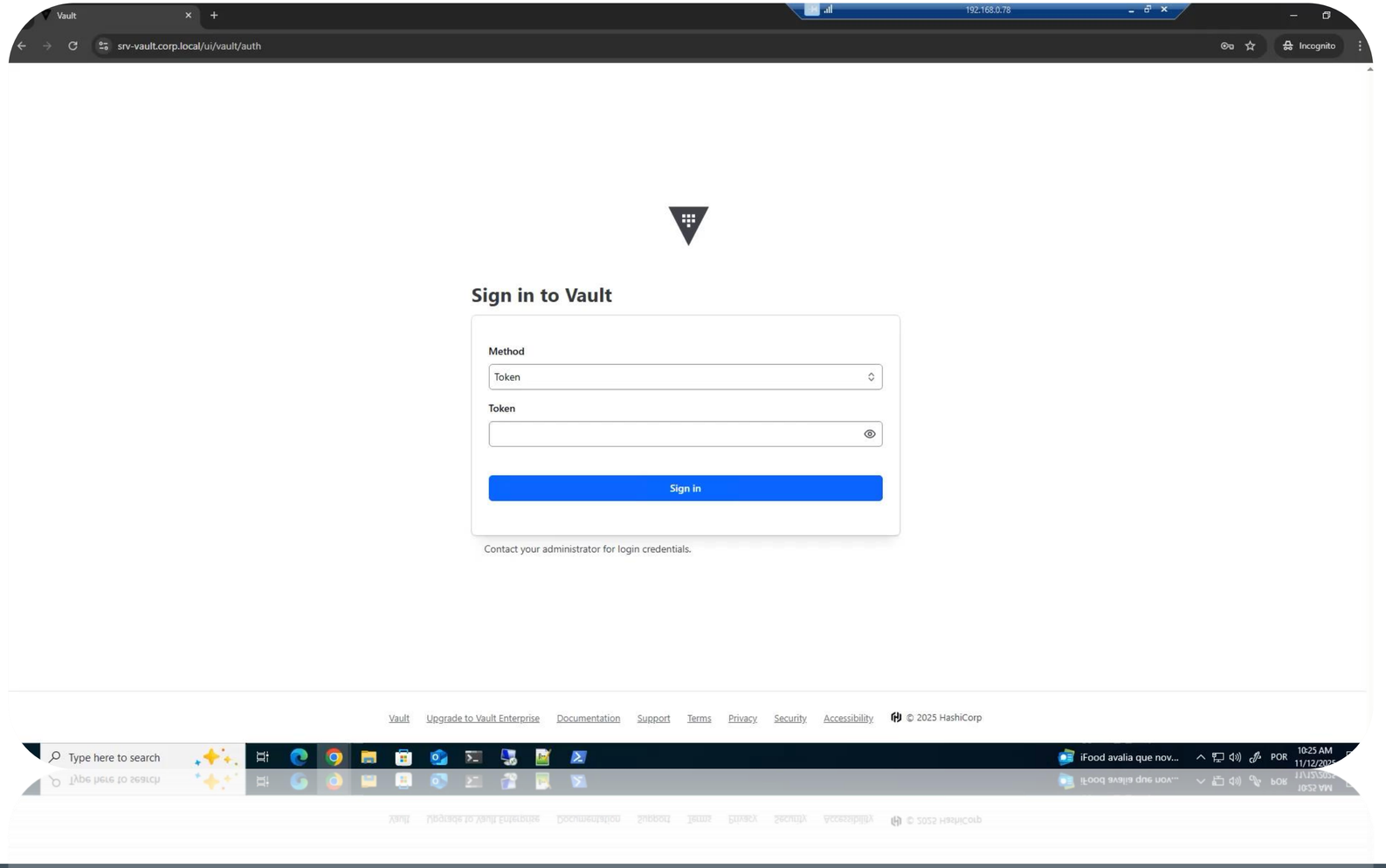
Demonstração: o cofre em ação

- Cenário: acesso válido às credenciais usando Passkey



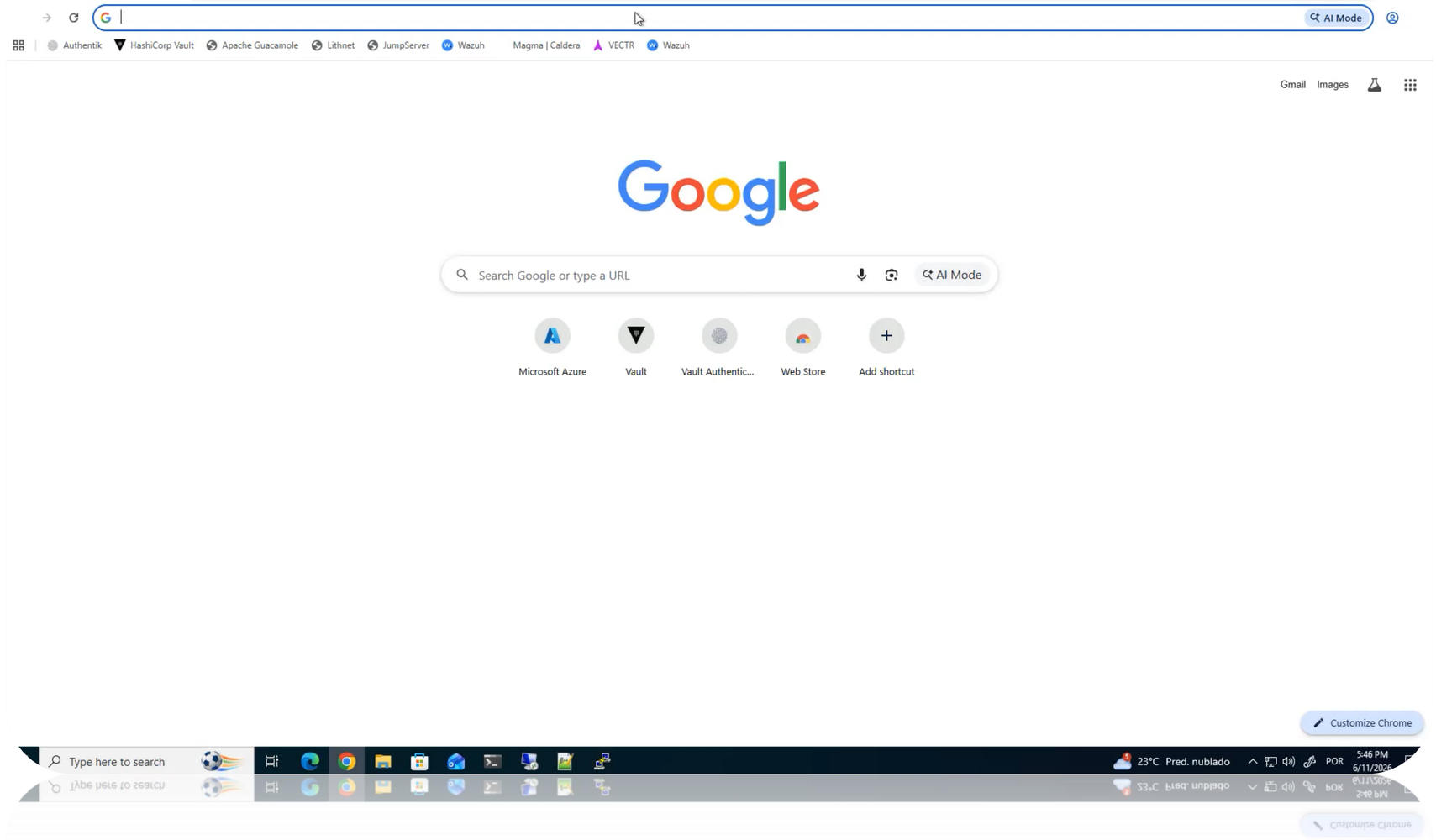
Demonstração: o cofre em ação

- Cenário: primeiro acesso de um usuário



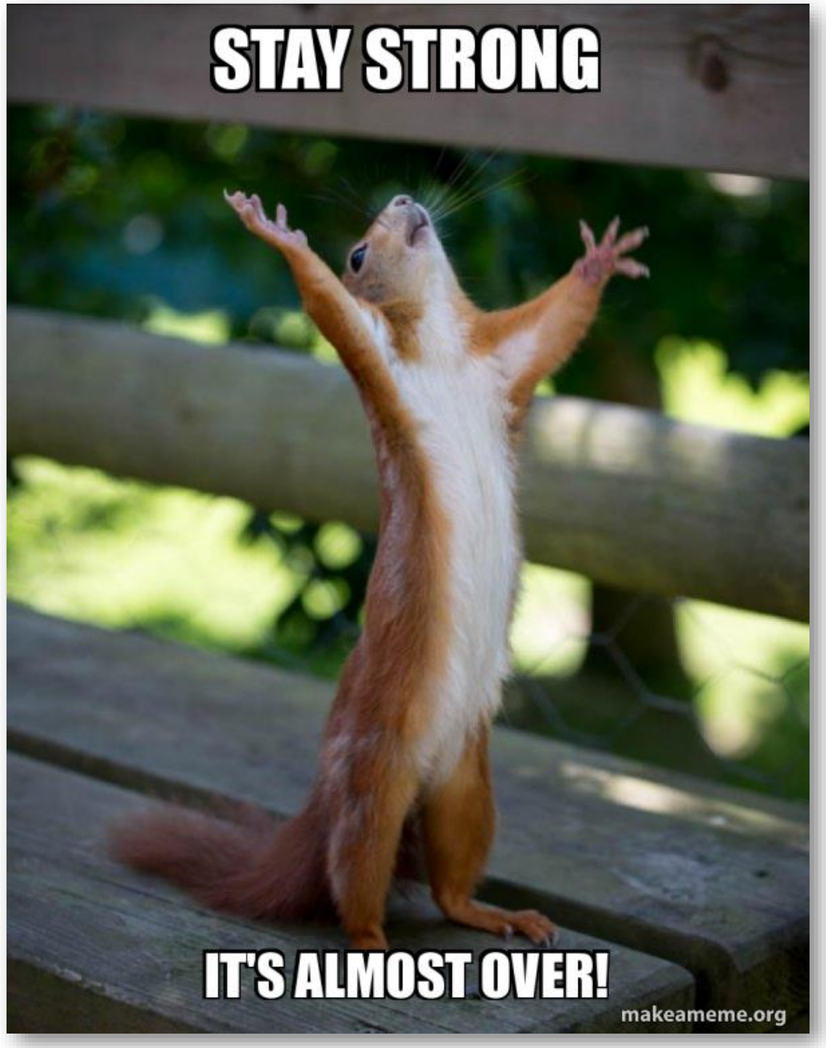
Demonstração: o cofre em ação

- Cenário: usando **outro IdP** (Entra ID)

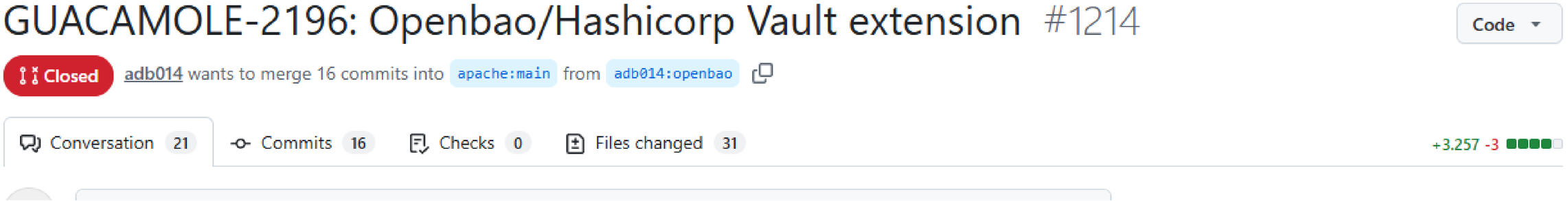


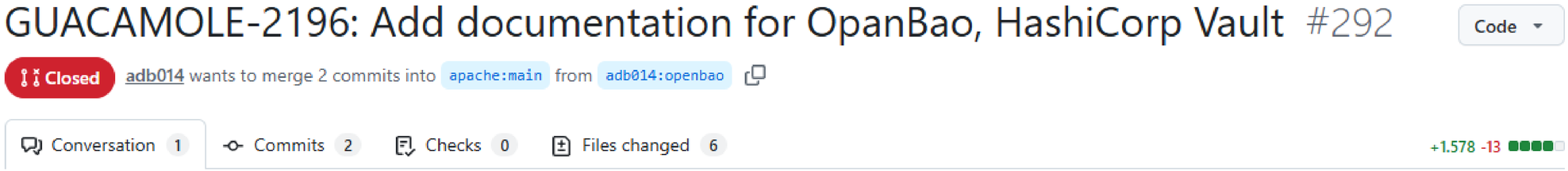
Conclusão e próximos passos

- Gestão de senhas de contas privilegiadas ✓
  - Senhas temporárias (1h) e complexas
- Problema ✗
  - Se máquina do cliente está comprometida, senhas são vazadas (*clipboard*)
- Como resolver?
  - PAW (raro)
  - Integração do Vault com ferramentas de acesso remoto
    - Ex: Apache Guacamole ou JumpServer



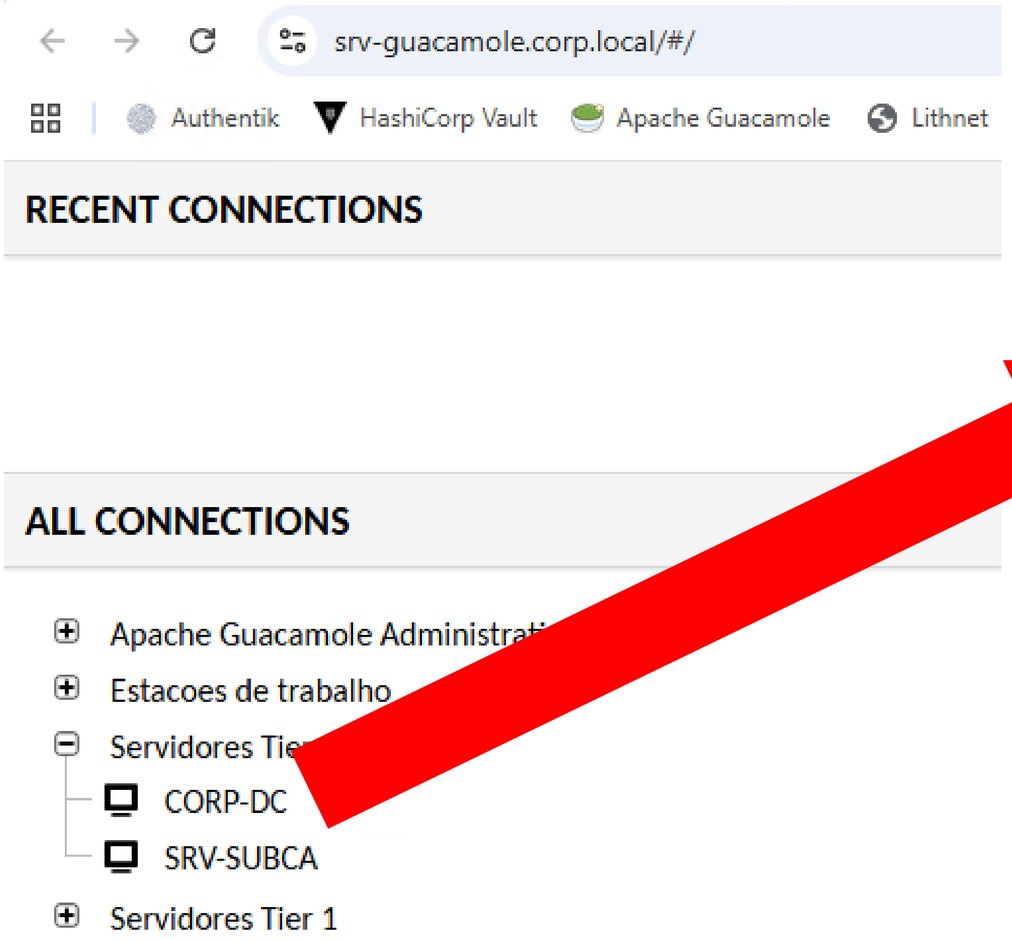
O jogo ainda não terminou...





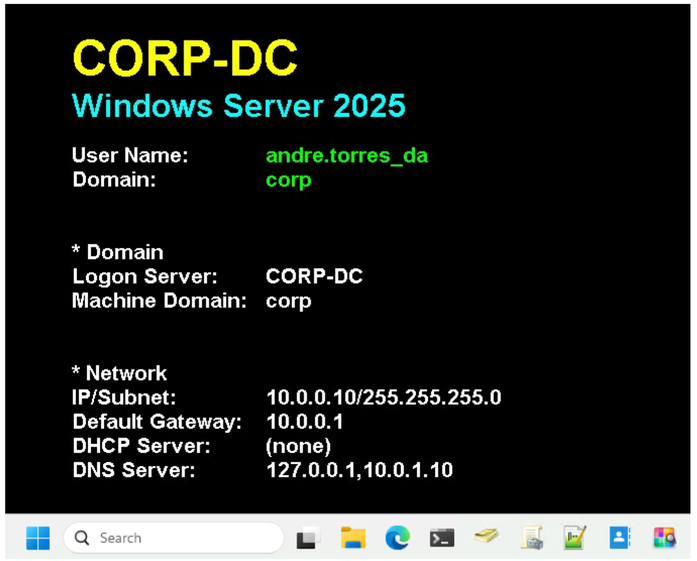
O jogo ainda não terminou...

Usuário: andre.torres



Usuário: ${GUAC_USERNAME}_da

Senha: HashiCorp Vault



Obrigado ☺

André Torres
https://www.linkedin.com/in/andretorresbr/