Proposta para resolução do problema a baixo:

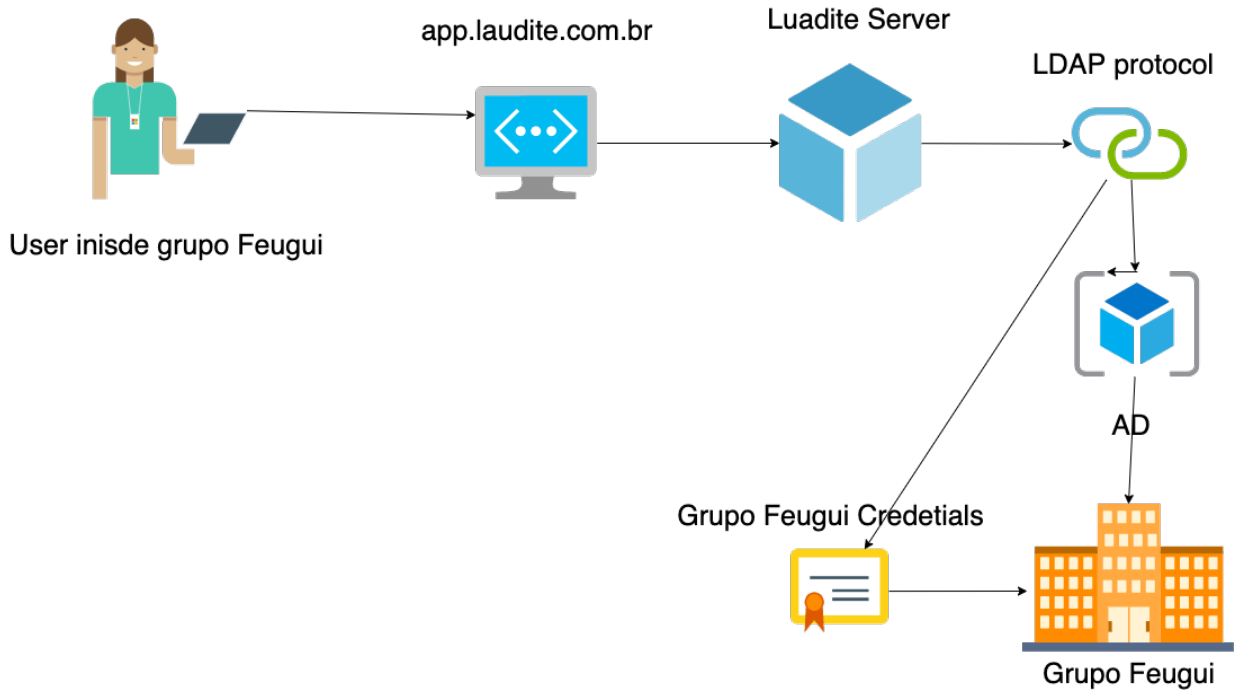
Uma grande empresa chamada "Grupo Feugui" que gostaria de integrar com o web app Laudite (vue.js - node.js - kubernetes - google cloud).
Contudo, a empresa exige que façamos o login no web app via AD (active directory), permitindo que seus usuários ao fazerem o login no Windows, ao acessar o site do Laudite (app.laudite.com.br) já estejam autenticados e autorizados. Lembrando, não iremos fazer parte da intranet deles, eles irão acessar o web app na internet pública.

Nesse contexto laudite não tem acesso a intranet do grupo Feugui, o que não lhe da a possiblidade de acessa seus usuário no AD.
Em uma autenticação padrão é comum termos um endpoint para auth e uma DB para persistir e verificar o payload vindo do frontend (requisição). Já nesse problema é diferente , nos não precisamos necessariamente de persistir os dados desses usuário e nem até mesmo de uma DB **(mas por questões de performances e consistência necessitamos persistir essa informação)** para tal ,nesse modelo o Grupo Feugui já tem seus users persistidos no AD server da empresa . O que se procura é um jeito de acessar o AD da empresa e verificar as credencias desses users vindo do frontend (laudit cliente app),sendo que não estamos na intranet deles, seu users vão acessar nosso web app através da internet. Para a solução deste problema acebei encontrando três: alternativas:

1- Protocolo LDAP
2- SSO-SAML
3- Azure AD Identity provider

Protocolo LDAP:
LDAP(Lightweight Directory Access Protocol) – é um protocol aberto e de múltiplas-plataform usado para serviço de autenticação de diretórios. LDAP fornece a linguagem de comunição que as empresas usam para comunicar com o serviço de diretórios de outros servidores. Resumindo LDAP é uma forma de conversar com active Directory. Para que isso aconteça é necessário uma relação de Orgazination-to-service provider ,nesse caso passaria existir uma relação entre o grupo Feugui e Laudite, dando a possiblidade da Laudite acessar AD service do Grupo Feugui através do protocolo LDAP, Nessa relação grupo Feugui forneceria o mínimo de informação para o acesso via LDAP. Desse jeito o server da Laudite teria um endpoint dedicado para lidar com requisições do active directory do grupo Feugui , usando o protocolo LDAP e tendo o mínimo de informação do grupo Feugui para acessar o AD service deles através do LDAP é possível

verificar e autenticar um user ,tentando acessar o web app da Laudite dentro do grupo Feugui.



SSO- SAML (Single Sign-on),(Security Assertion Markup Language)

No modelo traditional de requisição , temos um server e um cliente . Já no modelo baseado em SSO , temos uma entidade a mais .

Cliente,Server,Identity Provider(idp)

Como esse modelo se adaptaria ao problema:
O modelo acima (SSO) seria o ideal para este problema , uma vez que pretende-se acessar o web app laudite , mas mantendo os usarios já existentes dentro de uma intranet (org).

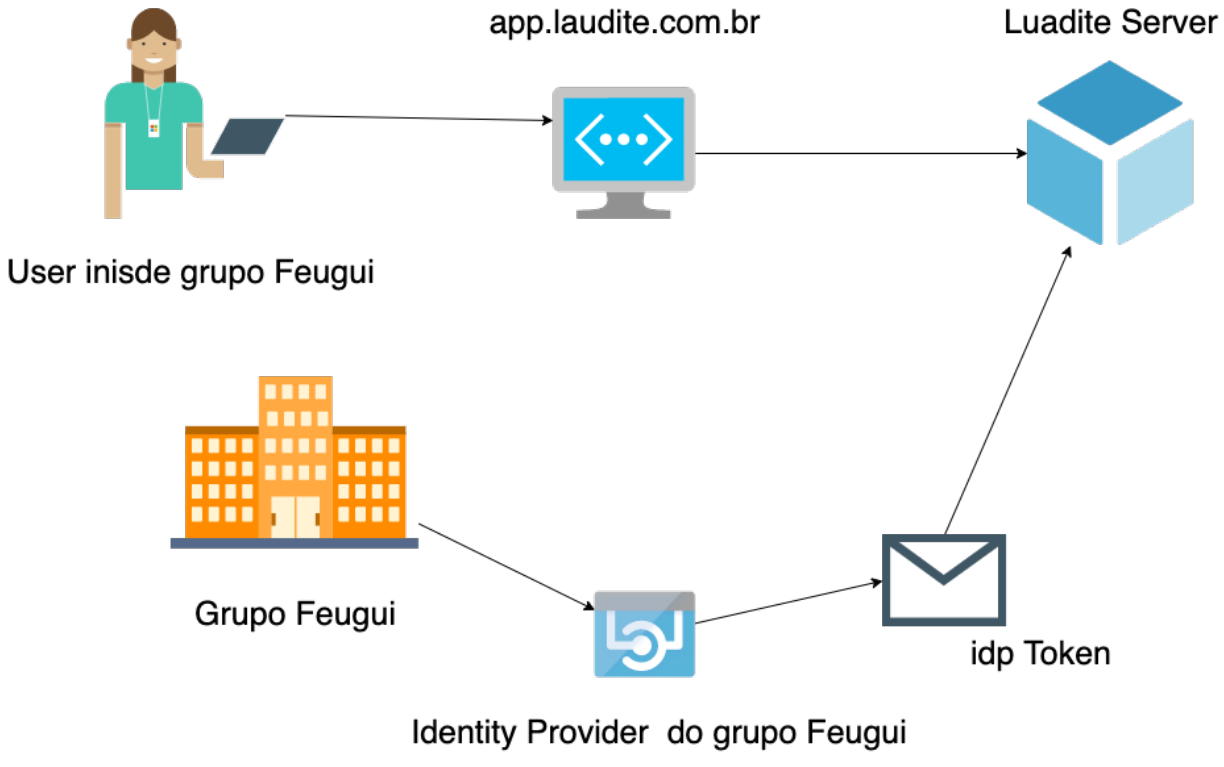
Servidor da laudite tem implementado authN e authZ de seus usuários , mas para os user do grupo Feugui que precisam re-usar as informações de seus usuários como isso seria resolvido?

O Cliente app da laudite pode ser acessado via rede public (internet) e nos precisamos manter os dados dos users do grupo Feugui acessa da sua intranet .

É aqui onde entra o Identity provider , como disse anteriormente , existe uma relação Business-to-consumer e Employer-to-employee. Como funcionaria?:

1- O user interno do grupo Feugui acessa a aplicação da laudite , o app cliente da laudite oferece ao grupo Feugui a possiblidade de logar com AD ,em que na qual o user so precisar fornecer seu dados uma vez, o nome de usuários pode ser adquirido automático , daí so precisaríamos da password do user.
2- É mandado uma requisição para um endpoint dedicado a autenticação AD, é aqui onde entra o papel do idp(identity provider) , o server da laudite recebendo essa request ela vai se comunicar com o idp service do Grupo Feugui passando as credencias que foram dadas , daí o idp service do Grupo Feugui verifica a autenticação do payload passado {username , password} o idp do grupo Feugui confirma que tais informação {username, password} é pertencentes a um de seu usuários no seu AD(Active Directory) ,daí o idp do Grupo Feugui vai emitir um token para o server da Laudite que por sua ves via mandar esse token para app cliente da Laudite que iniciou a requisição tendo verificado a autenticação desse usuário o app cliente da Laudite redireciona para a dashboard Laudite com as informações provenientes do idp (Identity provider) .

   Nesse modelo podemos ver o quão seguro e rápido foi o processo , a laudite não precisou de fazer parte da intranet para acessar os dados do AD do grupo Feugui, todo trabalho foi feito pela relação entre grupo Feugui (idp service) e Laudite (AD Auth service)



Azure Active Directory Identity Provider

Em ambientes cloud é possível o mesmo cenário.
Esse modelo funciona da sequinte forma , é criado um app service associado ao AD da empresa. Esse mesmo app service tem os previlegios de acessar direitamente o AD e verificar as credencias do user realizando a requisição. Nesse modelo existe uma relação de B2C , em que o app front da laudite comunica com o app service do AADidp(Azure active directory Identity provider) , gerando assim um código e um payload ,podendo ser persistido no backend da laudite caso necessário.

Source Microsoft SAML based Auth.