Estudo e Implementação de Sistema de Gestão de Credenciais de Autenticação de Alta Disponibilidade

Fernando Emanuel Azevedo Reis

Orientadores

Professor Doutor Osvaldo Arede dos Santos

Dissertação apresentada à Escola Superior de Tecnologia de Castelo Branco do Instituto Politécnico de Castelo Branco para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Desenvolvimento de Software e Sistemas Interativos, realizada sob a orientação científica do Professor Doutor Osvaldo Arede dos Santos, do Instituto Politécnico de Castelo Branco.

fevereiro 2017

Composição do júri

Presidente do júri

Prof. Doutor Fernando Reinaldo Silva Garcia Ribeiro

Vogais

Prof. Doutor Carlos Manuel da Silva Rabadão

Professor Coordenador, Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Leiria

Prof. Doutor Vasco Nuno da Gama de Jesus Soares

Professor Adjunto, Escola Superior de Tecnologia de Castelo Branco do Instituto Politécnico de Castelo Branco

Dedicatória

A todos os que sempre me ajudaram durante toda a minha vida.

Agradecimentos

A todos os meus amigos e colegas que de alguma forma me ajudaram e incentivaram na realização deste trabalho.

Um agradecimento especial à Sara e ao meu orientador pelo seu trabalho e incentivo.

Resumo

A gestão de credenciais de acesso em instituições com alguma dimensão sempre foi difícil de organizar e manter, devido aos diversos perfis de utilizadores, aos diferentes tipos de sistemas que delas necessitam para autenticarem os seus utilizadores e às mudanças frequentes nos sistemas informáticos que são usados nestas instituições.

Uma vez que praticamente todos os sistemas informáticos de uma instituição dependem do subsistema de autenticação para funcionar, é importante que este apresente um elevado nível de disponibilidade e um desempenho que não comprometa a operacionalidade dos sistemas, mesmo quando o número de utilizadores é elevado.

Neste trabalho é proposta uma solução centralizada de gestão de credenciais para o Instituto Politécnico de Castelo Branco, capaz de armazenar e gerir a informação referente aos diferentes perfis de utilizadores, de forma redundante e com um desempenho capaz de responder às necessidades de autenticação da instituição. São testados e avaliados tanto a capacidade de tolerância a falhas como o desempenho, e discutidos os respetivos resultados.

Palavras chave

Armazenamento de credenciais, perfis de utilizador, redundância

Abstract

Managing access credentials in institutions of some size has always been difficult to organize and maintain because of the various user profiles, different types of systems that need them to authenticate their users, and the frequent changes in the computer systems used in these Institutions.

Considering that almost every computer system in an institution depends on the authentication subsystem to operate, it is important that it has a high level of availability and a performance that won't compromise the system's operationality, even when the number of users is high.

This work proposes a centralized credential management solution for the Polytechnic Institute of Castelo Branco, capable of storing and managing the information of the different user profiles, in a redundant manner and with a performance capable of responding to the authentication needs of the institution. Both fault tolerance and performance are tested and evaluated, and the corresponding results are discussed.

Keywords

Credentials storage, user profiles, redundancy

Índice geral

Índice de figuras

Lista de tabelas

Lista de abreviaturas, siglas e acrónimos

ACL - *Access Control List*

AD – *Active Directory*

DAP - *Directory Access Protocol*

DIT - *Directory Information Tree*

DN - *Distinguished Name*

IANA - *Internet Assigned Numbers Authority*

IDP – *Identity Provider*

IPCB - Instituto Politécnico de Castelo Branco

LDAP - *Lightweight Directory Access Protocol*

LDIF - LDAP *Data Interchange Format*

OID – *Object Identifier*

PDCA - *PLAN - DO - CHECK - ACT* ou *Adjust*

PEAP – *Protected Extensible Authentication Protocol*

PEN – *Private Enterprise Number*

RADIUS - *Remote Authentication Dial In User Service*

RFC - *Request for Comments*

SaaS - *Software as a Service*

SIGA – Sistema Integrado de Gestão Administrativa

SP – *Service Provider*

SSL - *Secure Sockets Layer*

SSO – *Single Sign-On*

TCP/IP - *Transmission Control Protocol / Internet Protocol*

TLS - *Transport Layer Security*

UML - *Unified Modeling Language*

UUID - *Universally Unique Identifier*

VPN - *Virtual Private Network*

VRRP - *Virtual Router Redundancy Protocol*

CAPÍTULO 1 - INTRODUÇÃO

1.1 Contexto e motivação

A gestão e armazenamento de credenciais de utilizadores em organizações de média ou grande dimensão sempre foi complexa uma vez que existe um elevado número de utilizadores com um conjunto de informações associadas com grande diferença entre si. Por outro lado, a existência de um vasto leque de serviços disponíveis, cada qual com o seu tipo/forma de autenticação, aumenta ainda mais a complexidade dos serviços que armazenam toda a informação relativa aos utilizadores e aos serviços aos quais estes acedem.

Tipicamente, a informação relativa às credenciais (utilizador e palavra-passe) dos utilizadores é acompanhada por informação extra para permitir identificar corretamente o utilizador perante o processo de autenticação nos diversos serviços, organização do repositório de credenciais e informação de base que permite identificar a entidade a quem pertencem as credenciais.

No que diz respeito ao processo de negócio, a incorreta gestão das credenciais de utilizadores pode ser lesiva pois do ponto de vista de segurança, torna-se difícil garantir políticas capazes de lidar com os requisitos atuais de um mundo ligado entre si pela internet.

O *Lightweight Directory Access Protocol* (LDAP) existe desde o início dos anos 90 (Butcher, 2007) e foi criado para permitir as mesmas funcionalidades do protocolo *Directory Access Protocol* (DAP) sobre o protocolo *Transmission Control Protocol / Internet Protocol* (TCP/IP) permitindo, no entanto, a interligação com os diretórios X.500. Este protocolo define a forma como a informação é representada, acedida, importada e exportada utilizando *LDAP Data Interchange Format* (LDIF) mas não define como deve ser armazenada.

Pretende-se, com este trabalho, definir uma estrutura de armazenamento de toda a informação relativa ao processo de autenticação e autorização dos utilizadores, garantindo redundância e robustez em caso de falha, utilizando tecnologias *open-source*. Pretende-se ainda, definir políticas de gestão desta informação por forma a garantir que a mesma está atualizada e de acordo com o estado atual da entidade a que se refere.

1.2 Objetivos do trabalho

Esta dissertação tem por objetivo estudar e implementar um sistema de gestão de credenciais para o Instituto Politécnico de Castelo Branco (IPCB) tendo por base os seguintes requisitos:

Como requisito fundamental deste trabalho temos a alta disponibilidade de todo o sistema. Uma vez que muitos serviços informáticos do IPCB dependem do sistema de autenticação, este tem que estar sempre em funcionamento, caso contrário, serviços como a rede sem fios, a gestão académica, a *Virtual Private Network* (VPN) e outros deixarão de funcionar.

A interligação com os serviços existentes para que os mesmos possam aceder à informação de autenticação quando os utilizadores lhes acedem. Os serviços atualmente em funcionamento no IPCB e que requerem informação de autenticação são:

- *Remote Authentication Dial In User Service* (RADIUS), responsável pela autenticação na rede sem fios e VPN;
- Shibboleth *Identity Provider*/ SimpleSAMLphp, fornecem a solução de identidade federada;
- Sistema de Gestão Académica, que como o próprio nome indica, tem a gestão da informação académica do IPCB;
- Office 365, sistema de email, OneDrive e outros serviços na nuvem disponibilizados pela Microsoft;
- *Active Directory* (AD), autenticação dos utilizadores nos computadores, bem como em servidores de ficheiros;

O sistema deve, ainda, ficar preparado para que seja fácil configurar novos serviços para que utilizem a informação de autenticação nele contida.

A segurança é determinante para um sistema deste tipo, pois, tratando-se de informação de credenciais de utilizadores, muito sensível, o seu acesso de ser o mais restrito possível, por forma a evitar acessos não autorizados. A segurança tem ainda um caracter especial, pois o utilizador tem apenas uma palavra-passe para acesso a todos os serviços que dependem do sistema de gestão de credenciais.

O sistema de gestão de credenciais deve ser adequado à organização a que se destina, sob pena de ser muito difícil, ou mesmo impossível, configurar os serviços para o utilizarem. A adequação é obtida através do uso de *objectclasses* e atributos criados de forma a representarem a realidade da organização, nomeadamente, que representem os diversos perfis dos utilizadores existentes.

Por forma a aferir a adequabilidade do sistema à realidade do IPCB, devem ser efetuados testes de desempenho e disponibilidade, garantindo assim, que o mesmo tem capacidade de resposta aos pedidos solicitados, bem como, apresenta a robustez requerida para uma solução deste tipo.

Por fim, pretende-se apresentar uma solução baseada em tecnologias *open-source* por forma a evitar custos desnecessários e aproveitar o conhecimento existente no IPCB.

1.3 Cronograma do trabalho

A Figura 1 apresenta o cronograma do trabalho com a definição das atividades que serão desenvolvidas e a sua sequência de realização.

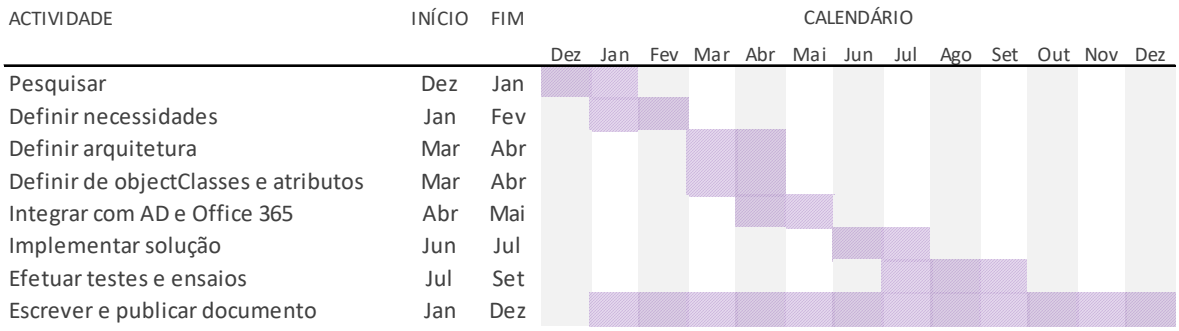

Figura 1 – Cronograma 2015/2016

Atividade 1: consiste na pesquisa de soluções de servidor de diretório LDAP de código aberto com a capacidade de implementar redundância *multi-master*. Nesta pesquisa, a facilidade de configuração e manutenção é também um fator a ter e conta.

Atividade 2: análise e estudo das necessidades no que diz respeito à informação a armazenar (atributos), aplicações a fornecer credenciais e garantias de disponibilidade.

Atividade 3: definição da arquitetura do serviço de diretório LDAP no que diz respeito à configuração do serviço, configuração da sincronização entre servidores, definição de *objectclasses* e outras funcionalidades que possam ser necessárias.

Atividade 4: compreende o registo na *Internet Assigned Numbers Authority* (IANA) do identificador único do IPCB e a definição, no formato da solução escolhida, dos atributos e *objectclasses* conforme as necessidades identificadas anteriormente.

Atividade 5: definição do processo de sincronização entre o diretório LDAP e o *Active Directory* e entre o diretório LDAP e o serviço Office 365.

Atividade 6: consiste na implementação de uma solução de diretório LDAP totalmente funcional com redundância *multi-master*, atributos e *objectclasses* definidos anteriormente.

Atividade 7: realização de testes e ensaios sobre a solução proposta, nomeadamente testes de desempenho e disponibilidade para aferir até que ponto a sincronização entre servidores é suficientemente rápida para o funcionamento em produção no IPCB e se oferece garantias de alta disponibilidade.

Atividade 8: redação da dissertação com base em todas as tarefas anteriores. Esta atividade tem a duração da quase totalidade do calendário pois é um trabalho contínuo.

1.4 Estrutura da dissertação

No capítulo inicial é feita a introdução e apresentados o contexto e motivação, os objetivos, o cronograma e, por fim, a estrutura da dissertação.

No segundo capítulo são apresentados conceitos, trabalhos relacionados e tecnologias existentes relevantes para este trabalho.

No capítulo 3 é apresentada a arquitetura proposta para fazer face às necessidades do Instituto Politécnico de Castelo Branco.

No quarto capítulo são apresentados os resultados dos testes de desempenho e disponibilidade, bem como a sua estrutura.

Por fim, no capítulo 5 é apresentada a conclusão da dissertação, bem como o trabalho futuro.

CAPÍTULO 2 - ESTADO DA ARTE

Neste capítulo são apresentados conceitos referentes à autenticação, autorização e contabilização, bem como os tipos de replicação propostos no *Request for Comments* (RFC) 4533.

São, ainda, apresentados trabalhos relacionados com a solução proposta e apresentados os aspetos mais relevantes dos mesmos.

Por fim, são apresentadas algumas soluções de armazenamento de credenciais existentes no mercado.

2.1 Conceitos

Neste subcapítulo são apresentados conceitos relevantes à solução proposta, nomeadamente, autenticação, contabilização e replicação.

2.1.1 Autenticação e contabilização

A autenticação (Boston University Information Services & Technology, 2016) compreende a validação por parte do servidor de que o utilizador a ser autenticado é quem apresenta ser, normalmente através do binómio utilizador/palavra-passe, mas podem, alternativamente, ser utilizadas outras formas de autenticação, como a impressão digital, o scan de retina, reconhecimento de voz, entre outros.

A autenticação de um cliente implica, normalmente, o envio por parte do servidor de um certificado que é validado por uma terceira parte de confiança que garante que o servidor é da entidade de quem apresenta ser.

Importa ainda mencionar que a autenticação não é responsável por definir a que dados tem o utilizador acesso ou que tarefas pode executar.

Um dos tipos de autenticação muito utilizado atualmente no ambiente académico é a autenticação federada (Buecker et al., 2005; Stallings, 2007), em que as credenciais dos utilizadores estão armazenadas na sua instituição de origem (*Identity Provider*), mas que com base em relações de confiança entre instituições, podem autenticar-se em aplicações disponibilizadas por outras instituições (*Service Provider*) sendo apenas transmitidos os dados necessários à execução da aplicação em questão.

A autenticação distribuída (Kaufman, 1993) atende ao facto de que um utilizador pode aceder a um serviço num computador na rede que por sua vez acede a outros computadores em busca de recursos necessários à execução do serviço inicial.

Normalmente este tipo de autenticação utiliza mecanismos criptográficos no seu funcionamento.

Na autenticação centralizada as credenciais estão armazenadas num repositório central, por exemplo um diretório LDAP (Wahl, et al., 1997), que é consultado pelos serviços em que o utilizador se tenta autenticar.

Esta autenticação tem benefícios acrescidos no que diz respeito à gestão das credenciais pois, estando estas num único sítio torna-se mais fácil a sua gestão.

Pode-se argumentar que a autenticação centralizada oferece alguns perigos acrescidos pois ao ser comprometida a informação todas as credenciais ficam vulneráveis, no entanto existem mecanismos que oferecem a proteção adequada.

Por último, a autenticação local, que como o próprio nome indica, pressupõe que as credenciais dos utilizadores estejam armazenadas no próprio destino da autenticação, normalmente routers, computadores ou servidores.

A autorização é o processo pelo qual é validada a permissão de acesso a ficheiros ou recursos existentes num determinado servidor ou serviço.

Na solução apresentada neste documento, a autorização é realizada ao nível do acesso do utilizador aos diversos dados existentes numa entrada, no acesso à entrada propriamente dita e por fim a um ramo da árvore de diretório.

Por fim o processo de contabilização, que tem como intuito a contabilização dos recursos acedidos pelos utilizadores durante a sessão autenticada. Como exemplo deste processo podemos considerar os clientes dos operadores móveis de telecomunicações que têm plafons de tráfego mensal associados aos seus tarifários. Na solução proposta, o processo de contabilização é realizado sob a forma de registos de acesso (*access logs*) onde são guardadas todas as informações referentes às ações efetuadas sobre os servidores que compõem a solução. Estes registos são guardados em servidor próprio independente, garantindo assim o acesso aos mesmos em situações de falha grave.

2.1.2 Replicação

O RFC 4533 (Zeilenga and Choi, 2006), define dois tipos de replicação entre serviços LDAP. No primeiro, *refreshOnly*, o servidor, que atua como cliente, liga-se ao segundo servidor em intervalos de tempo definidos para atualizar a informação. O segundo, *refreshAndPersist*, tem um funcionamento diferente, pois o servidor, que atua como cliente, fica ligado ao segundo servidor e recebe as atualizações sempre que as entradas são atualizadas, criadas ou removidas.

Uma vez que um pedido de sincronização de um servidor cliente é essencialmente uma procura estendida, o segundo servidor atua sobre este da mesma forma que

qualquer outro, estando o mesmo sujeito às mesmas permissões de acesso que qualquer outro pedido de uma outra qualquer aplicação. Não é configurada nenhuma informação específica sobre o servidor que atua como cliente de replicação.

De referir que não é obrigatório sincronizar toda a *Directory Information Tree* (DIT), pode-se sincronizar apenas um ramo ou então usar outro critério de acordo com o critério de pesquisa.

Replicação refreshOnly

Neste tipo de replicação, o cliente inicia a ligação com o servidor. Caso seja a primeira vez, o cliente indica que não tem *SyncCookie* (contém a *contextCSN* que é, basicamente, um selo temporal indicando a última vez que foi feita a sincronização) e é feita a pesquisa de acordo com o critério de procura. De seguida é feita sincronização de todas as entradas resultantes da pesquisa. Caso não seja a primeira vez que ocorre a sincronização então o cliente envia um *SyncCookie* que indica os limites da sessão de sincronização ao servidor.

O servidor responde com uma ou duas fases:

Fase presente (*present*):

1. Envia toda a informação relativa a todas as entradas que foram alteradas desde a última sincronização, incluindo o *Distinguished Name* (DN) e o *Universally Unique Identifier* (UUID) - atributo que contém o ID único universal de cada entrada - para o cliente;
2. Envia o DN e UUID das entradas que não foram alteradas desde a última sincronização.

Fase remoção (*delete*):

Envia o DN e UUID das entradas que foram removidas desde a última sincronização.

Por último, o servidor envia um *SyncCookie* atualizado e a ligação é terminada.

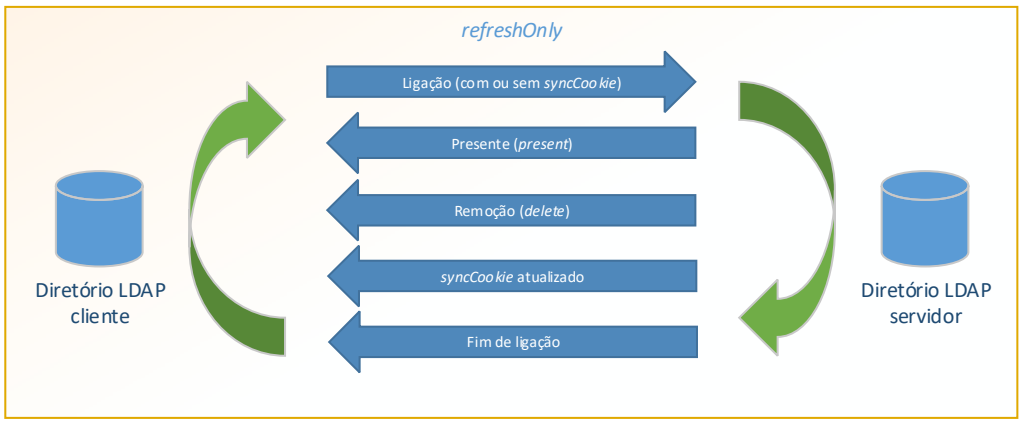

Figura 2 - Replicação *refreshOnly*

A Figura 2 representa o processo de replicação *refreshOnly*, sendo possível observar as duas fases deste processo (*present* e *delete*). Podemos também observar, que se trata de um processo cíclico.

Dependendo da configuração efetuada, o intervalo de tempo entre sincronizações pode ser reduzido. No entanto, na sincronização inicial a fase presente pode demorar a ser executada, pois caso existam poucas entradas alteradas são na mesma transferidos o DN e UUID de todas as entradas. Em grandes DIT tal pode ser um problema.

Existe na memória do servidor um log de sessão (*session log*) que, dependendo do tempo que este cobre, pode ignorar a fase presente, aumentando consideravelmente a velocidade de sincronização, por exemplo, quando não são alteradas ou criadas entradas. Caso o log de sessão não seja suficiente para cobrir o tempo desde a última sincronização então é feita um ressincronização total incluindo a fase presente.

Replicação refreshAndPersist

Este tipo de sincronização é idêntico ao anterior. No entanto, no fim da sincronização inicial, o servidor mantém a ligação. Assim, ao serem realizadas operações sobre as entradas, a informação é atualizada imediatamente.

Em atualizações ou adições de entradas é transferida toda a informação das entradas envolvidas na operação.

O *SyncCookie* é atualizado periodicamente.

A ligação entre o cliente e o servidor é mantida de forma permanente. Caso exista uma falha é feita uma religação.

.

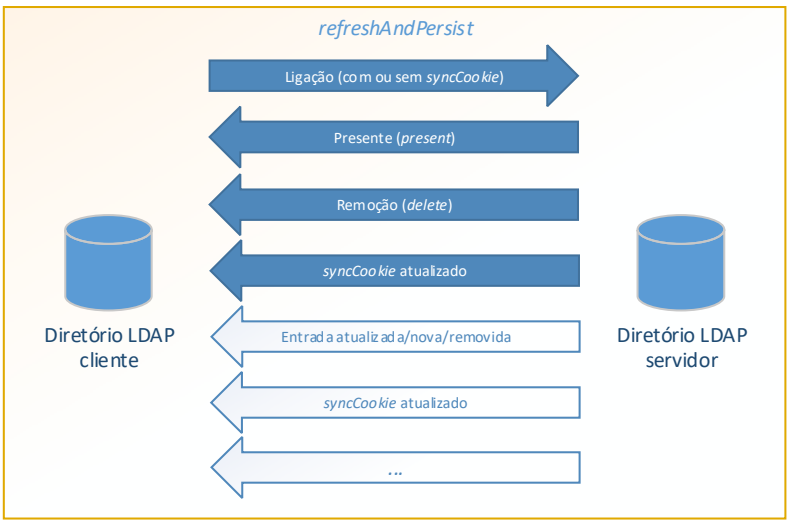

Figura 3 - Replicações *refreshAndPersist*

Na Figura 3 podemos observar o processo de replicação *refreshAndPersist*. Tal como no processo de replicação *refreshOnly*, é possível observar as duas fases (*present* e *delete*), no entanto, não se trata de um processo cíclico. As setas de fundo claro representam a permanência da ligação depois do processo de sincronização inicial.

2.2 Tecnologias existentes

Os diretórios LDAP são bases de dados utilizadas para armazenamento de credenciais, pois o seu desempenho e estrutura de armazenamento são perfeitas para o tipo de função que se pretende, ou seja, rapidez na resposta a pedidos de procura (as autenticações são procuras no diretório) e uma estrutura, em árvore, que é facilmente adaptável à realidade da empresa ou instituição.

Existem no mercado várias soluções de diretório LDAP, no entanto, na comunidade *open-source*, a mais utilizada é OpenLDAP Server (OpenLDAP Foundation, 2017). Esta solução é bastante simples de configurar para a maioria das necessidades e apresenta um conjunto de funcionalidades bastante extenso. É também uma das soluções de diretório mais antigas existentes no mercado.

Ainda no âmbito das soluções *open-source* existem outras soluções, como o 389 Directory Server (Red Hat, Inc., 2017), o Apache DS (The Apache Software Foundation, 2016) e o OpenDJ (ForgeRock, 2017) mas não tem a base de implementação do OpenLDAP.

Relativamente às soluções comerciais, o *Active Directory* (Microsoft, 2016) é a solução mais utilizada a nível mundial, pois é parte integrante do ambiente Windows, quando utilizado em ambiente de rede. Do ponto de vista de características, é uma solução muito completa e a integração com os restantes produtos deste fabricante é total.

Outras soluções comerciais existentes no mercado são o NetIQ eDirectory (Micro Focus, 2017), o IBM Security Directory Suite (IBM, 2016) e o Oracle Unified Directory (Oracle, n.d.), no entanto o público alvo destas soluções é o mercado das grandes empresas visto que são estas que necessitam das funcionalidades implementadas por estas soluções. Os valores envolvidos no seu licenciamento, bem como o esforço de configuração, invalidam o acesso a estas soluções por pequenas empresas e instituições.

Por fim, o Microsoft Azure AD (Microsoft, 2016a). É uma solução de diretório na nuvem, com funcionalidades como o *Single Sign-On* (SSO) e autenticação *multi-factor*, em que é necessário mais do que uma validação para autenticar o utilizador. Um dos grandes benefícios de utilizar esta solução é a sua integração com os mais diversos serviços existentes na nuvem, como por exemplo o DropBox (Dropbox, n.d.) ou o Office365 (Paul, 2013) e com o *Active Directory*, o que permite integrar os utilizadores locais com aplicações na nuvem.

O Microsoft Azure AD é uma solução bastante recente, no entanto, tem sido bastante desenvolvida e o número de funcionalidades apresentadas cresce a um ritmo bastante elevado, o que mostra a vontade desta empresa em apostar em soluções na nuvem.

2.2.1 *ObjectClasses* eduPerson e eduOrg

As *objectclasses*[1] eduPerson e eduOrg foram criadas pela comunidade Internet2 com o objetivo de criar uma lista de atributos e definições comuns a instituições de ensino superior em todo o mundo. Tem atributos, como por exemplo eduPersonAffiliation, que representa o tipo de relação do utilizador com a instituição ou então eduPersonPrincipalName que representa o id do utilizador associado ao seu domínio no formato utilizador@domínio como no serviço de correio eletrónico.

Na solução apresentada apenas é usada a *objectclass* eduPerson e alguns dos seus atributos.

2.2.2 Registo dos *Object Identifiers* (OID) na *Internet Assigned Numbers Authority* (IANA)

Ao criar um novo *schema* (conjunto de *objectclasses* e atributos) são definidos os atributos e *objectclasses* que lhe pertencem. Uma vez que cada atributo e *objectclass* devem ter um identificador único OID global que o distinga de qualquer outro objeto, é necessário (The OpenLDAP Project, 2016) solicitar à IANA um *Private Enterprise Number* (PEN) por forma a evitar colisões com objetos de outros *schemas*. Não se deve em caso algum utilizar OID de outras entidades sob pena de ocorrerem colisões e consequentemente perda de informação.

O pedido é gratuito e para o efetuar basta aceder ao endereço http://pen.iana.org/pen/PenApplication.page e preencher os dados solicitados.

Foi atribuído ao Instituto Politécnico de Castelo Branco o PEN 22567, que pode ser consultado no endereço http://www.iana.org/assignments/enterprise-numbers/enterprise-numbers.

[1] Relativamente a vários termos usados na estrutura de dados LDAP, foi tomada a decisão de manter a designação original em Inglês pelo facto de não ser usual encontrar estes termos traduzidos para Português

2.3 Trabalho relacionado

Em *Research and Design of Campus Network Unified Identity Authentication System Based on Kerberos* (Wang and Wang, 2012) os autores utilizam um servidor LDAP como repositório de informação pois este é otimizado para procuras. É ainda, importante referir, que é também utilizado um serviço Kerberos (MIT, 2016) para autenticação dos utilizadores. Na solução proposta, uma vez que a autenticação dos utilizadores nos computadores é feita a um dominio Windows (*Active Directory*) que implementa o serviço Kerberos, torna-se desnecessária a implementação de um outro serviço Kerberos.

O OpenLDAP permite utilizar diversas bases de dados (*Database Backend*) para armazenar os dados das entradas e da estrutura da árvore, sendo que, o back-BDB (Oracle, 2016) é a base de dados utilizada na maioria das configurações, até porque é a configurada por omissão em grande parte das distribuições de Linux, nas quais o OpenLDAP é fornecido.

Em *Enhancing the Performance of OpenLDAP Directory Server with Multiple Caching* (Choi et al., 2003) é apresentada uma solução para aumentar o desempenho do OpenLDAP através da configuração/optimização de memórias intermédias (*cache*) utilizando back-BDB.

Por fim, em *MDB: A Memory-Mapped Database and Backend for OpenLDAP* (Chu, 2011) é apresentada uma nova base de dados que faz um uso intensivo da memória para conseguir desempenhos elevados e ao mesmo tempo eliminar a complexidade da configuração, nomeadamente cache, como proposto noutras bases de dados. Esta base de dados é a utilizada na solução proposta, exactamente por causa do desempenho que apresenta.

2.4 Síntese

Neste capítulo foram apresentados conceitos referentes aos diversos tipos de autenticação existentes, bem como os tipos de replicação propostos no RFC 4533.

Foram ainda apresentados trabalhos relacionados com a solução proposta e salientados alguns aspetos considerados mais relevantes dos mesmos.

Por forma a perceber melhor o mercado de soluções de diretório, foram apresentadas algumas soluções de armazenamento de credenciais existentes no mercado.

Por fim, foi feita uma breve apresentação das *objectclasses* eduPerson e eduOrg e o processo de obtenção de um PEN à IANA.

CAPÍTULO 3 - ARQUITETURA PROPOSTA

Neste capítulo será apresentada a proposta de solução para a gestão de credenciais dos utilizadores, nomeadamente a arquitetura geral, a visão geral do serviço, a organização lógica dos dados, a sincronização com o *Active Directory* e Office 365 e a interligação do serviço LDAP com os restantes serviços.

3.1 Arquitetura geral

Por forma a garantir a máxima robustez, a arquitetura geral é composta por dois servidores OpenLDAP (cluster) configurados em modo *multi-master* (ZYTRAX, Inc., 2016a), o que garante a alta disponibilidade pretendida para um serviço com um elevado nível de dependências.

A figura abaixo mostra a ligação entre o cluster OpenLDAP e os serviços que lhe acedem para obter informação relevante ao processo de autenticação. À esquerda estão representados os serviços que consultam a informação e à direita os serviços que, de alguma forma, contribuem com informação de autenticação.

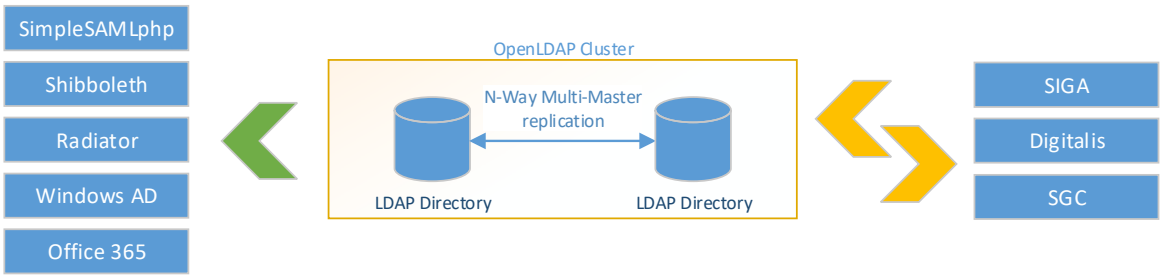

Figura 4 - Esquema de interligação com os serviços

A autenticação da rede sem fios e do serviço de VPN é realizada através do serviço de autenticação RADIUS que pode utilizar qualquer um dos servidores LDAP para verificar as credenciais dos utilizadores bem como o seu perfil.

Os serviços de *Single Sign-On* e identidade federada simpleSAMLphp (UNINETT, 2016) e Shibboleth (Internet2, 2017) podem também utilizar qualquer um dos servidores LDAP para autenticar os utilizadores e obter os atributos a distribuir às aplicações.

A sincronização das credenciais dos utilizadores existentes no diretório LDAP com o serviço Office 365 e Windows *Active Directory* é feita através de scripts em Powershell (Microsoft, 2017) que são executados a cada 2 minutos e apenas no sentido OpenLDAP – Windows *Active Directory* e OpenLDAP – Office 365. A implementação deste passo intermédio obriga à encriptação dos atributos x-pt-ipcb-adEncriptedPassword e x-pt-ipcb-o365EncriptedPassword utilizando certificados digitais para garantir que a confidencialidade destes atributos não é violada.

O SIGA – Sistema Integrado de Gestão Administrativa (IPCB, 2016) faz a sua autenticação através do Cluster LDAP, mas é também fonte de informação relativamente aos funcionários e docentes através da página de registo disponibilizada a estes colaboradores.

O sistema de gestão académica da Digitalis (Digitalis, 2017) faz um uso intensivo do cluster, pois necessita de um ramo privado para guardar uma série de atributos relevantes ao seu funcionamento, bem como de acesso de escrita a alguns atributos específicos do utilizador. É ainda fonte de informação relativa aos alunos que se inscrevem através da página de registo disponibilizada para o efeito.

O Sistema de Gestão de Credenciais tem acesso de escrita nos atributos que o utilizador pode alterar, nomeadamente a palavra-passe, o número de telefone e nome a exibir (displayName), uma vez que é um sítio web de acesso ao utilizador para que este possa alterar estes dados.

3.2 Visão geral do serviço

A solução apresentada tem por base dois servidores OpenLDAP (OpenLDAP Foundation, 2017) configurados em *N-Way Multi-Master replication* (The OpenLDAP Project, 2016; Zeilenga and Choi, 2006; ZYTRAX, Inc., 2016a) de forma a garantir a mais elevada disponibilidade possível utilizando este serviço. *N-Way Multi-Master replication* faz com que toda a informação seja replicada para todos os servidores (Masters) garantindo assim que estão todos sempre atualizados com a mesma informação. Esta configuração tem como principais benefícios:

- Garantia de funcionamento em caso de falha de um dos servidores;
- Elimina pontos únicos de falha;
- Funcionamento robusto em recuperação de falhas.

Esta configuração tem as suas desvantagens, sendo que a maior se prende com o facto de, em caso de recuperação, a informação ser toda trocada entre os diversos servidores que compõem o cluster, o que poderá originar constrangimentos de rede. No entanto, na solução apresentada, esta desvantagem é desprezável pois existem apenas dois servidores.

Por forma a adaptar a estrutura de dados à realidade do IPCB, é utilizada a *objectclass* standard do OpenLDAP inetOrgPerson, que tem como superior a *objectclass* organizationalPerson que, por sua vez, tem como superior a *objectclass* person. Foi também utilizada a *objectclass* eduPerson pois define informação utilizada no mundo académico que também é armazenada na solução apresentada. Por último, foram criadas diversas *objectclasses* para definir informação específica do IPCB, sendo que as mesmas foram criadas para armazenar/definir informação dos diversos serviços existentes:

- x-pt-ipcb-digitalis: define os atributos relativos ao sistema de gestão académica Digitalis;
- x-pt-ipcb-wifi: define os atributos relativos à autenticação na rede sem fios;
- x-pt-ipcb-siga: define os atributos relativos ao SIGA;
- x-pt-ipcb-active-directory: define os atributos relativos ao *Active Directory*;
- x-pt-ipcb-o365: define os atributos relativos ao Office 365;
- x-pt-ipcb-civilIdentity: define os atributos relativos à identificação civil dos utilizadores;
- x-pt-ipcb-institutional: define os atributos relativos a dados referentes ao IPCB;
- x-pt-ipcb-outside: define os atributos relativos a utilizadores que não pertencem ao ambiente académico;
- x-pt-ipcb-idp: define os atributos relativos aos sistemas de SSO e identidade federada simpleSAMLphp e Shibboleth.

Por forma a garantir a segurança da informação, é proposta segurança a dois níveis: na ligação, em que é obrigatório que toda a informação que circula entre os diversos serviços e o servidor OpenLDAP seja encriptada; na árvore de diretório, cujo acesso aos diversos atributos, entradas e ramos da árvore são protegidas por listas de controlo de acesso (ACL).

3.2.1 Funcionalidades do serviço

O serviço tem como principal funcionalidade o armazenamento das credenciais dos utilizadores para posterior acesso aquando da autenticação destes em serviços que dependam deste como repositório de credenciais.

Esta concentração das credenciais dos utilizadores num único sítio permite que qualquer alteração realizada sobre estas seja automaticamente aplicada a todos os serviços que dependem do diretório LDAP, por exemplo, ao alterar a palavra passe de um utilizador, todas as autenticações realizadas pelos serviços que utilizem o diretório LDAP como repositório de credenciais terão de utilizar a nova palavra passe sob pena de não realizarem a autenticação.

Com o constante aumento de serviços a disponibilizar aos utilizadores, utilizando um repositório central de credenciais (diretório LDAP) consegue-se garantir um elevado nível de integridade e simplicidade na gestão de credenciais dos utilizadores.

Outra das funcionalidades diz respeito à autenticação propriamente dita, ou seja, existem duas formas de realizar a autenticação dos utilizadores no serviço LDAP:

- Procura na árvore;
- Ligação (*bind*).

A primeira funciona como uma simples procura de um conjunto de atributos nas entradas do diretório, por exemplo, procurar uma entrada em que o utilizador e a palavra-passe sejam iguais aos que pretendemos encontrar. Esta forma de autenticação necessita de um utilizador no serviço LDAP com permissões para fazer procuras nos atributos específicos para realizar a procura relativa à autenticação, levando a mesma que a ser feita em dois passos:

1. Ligação ao diretório LDAP com um utilizador com permissões de leitura nos atributos específicos;
2. Procura do conjunto de atributos com os valores pretendidos.

Um exemplo deste tipo de autenticação é a autenticação na rede sem fios utilizando PEAP em que é procurado um agrupamento dos atributos x-pt-ipcb-wifiNThash e x-pt-ipcb-wifiUsername com os valores do utilizador e *hash* da palavra passe. Se for encontrado, então o utilizador está autenticado caso contrário o utilizador não está autenticado.

A autenticação por ligação (*bind*) utiliza o DN do próprio utilizador e a sua palavra passe para fazer a ligação ao diretório LDAP. Caso consiga ligar-se, então o utilizador está autenticado caso contrário o utilizado não está autenticado.

Por vezes o DN do utilizador não está disponível de forma direta o que obriga à realização de uma procura na árvore antes de se tentar a autenticação propriamente dita, levando a que também seja novamente necessário um utilizador no serviço LDAP com permissões para fazer procuras nos atributos e fazendo com que a mesma seja realizada em três passos:

1. Ligação ao diretório LDAP com um utilizador com permissões de leitura nos atributos específicos;
2. Procura do DN cujo atributo utilizador seja igual ao que pretendemos autenticar;
3. Ligação ao diretório (*bind*).

Seja qual das duas formas de autenticação a ser realizada, o serviço LDAP, quando configurado corretamente, com as *caches* e índices otimizados para os dados que armazena, consegue dar respostas bastante rápidas, pois foi concebido para responder a operações de leitura da forma mais rápida possível, pois são as operações realizadas em maior número quando se efetua autenticação de utilizadores

3.2.2 Arquitetura do serviço

Para garantir a tolerância a falhas do serviço LDAP são usados dois servidores, implementados em máquinas virtuais, em execução em dois servidores físicos independentes, de forma a que, caso um dos servidores físicos tenha uma falha, o serviço continue a funcionar corretamente.

Configuração *N-Way Multi-Master*

Esta configuração usa um dos processos de sincronização *refreshOnly* ou *refreshAndPersist*, implementados através do módulo (*overlay*) syncprov, para sincronizar as entradas entre os servidores, dando origem a uma solução *multi-master*, ou seja, tolerante a falhas e robusta.

De forma simples, um serviço LDAP atua como cliente quando existem entradas alteradas num dos membros do grupo (Figura 5).

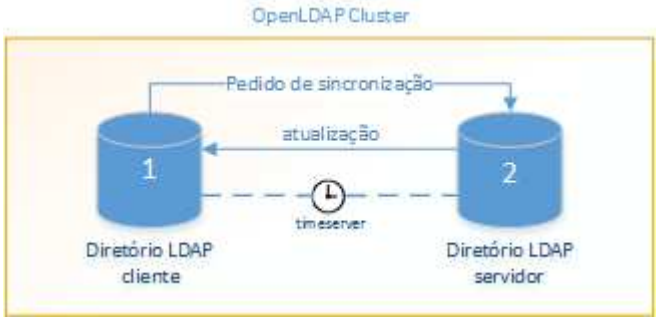

Figura 5 - *N-Way Multi-Master* serviço como cliente

E como servidor quando as entradas são alteradas nele próprio (Figura 6).

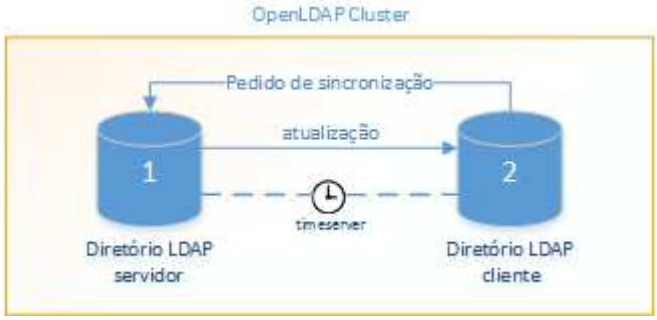

Figura 6 - *N-Way Multi-Master* serviço como servidor

Para garantir que a sincronização ocorre sem problemas, é obrigatório que ambos os *hosts* utilizem o mesmo servidor de tempo (*timeserver*), sob pena de originar perda de dados.

A sincronização que mais se adequa a esta configuração é a *refreshAndPersist* pois a sincronização é imediata, o que diminui as inconsistências entre as DITs.

Na Figura 7 podemos observar o funcionamento desta configuração: ambos os serviços LDAP atuam como clientes e como servidores em cada um dos *hosts*.

Figura 7 - *N-Way Multi-Master* serviço como cliente e servidor

Para tirar partido desta configuração, os clientes devem ser configurados com os dois *hosts* OpenLDAP (suportado na grande maioria). Assim, em caso de falha de um *host* é feita a ligação com o outro.

3.2.3 *Overlays*

Um único servidor OpenLDAP pode conter diversas DIT que são configuradas no ramo cn=config sob a forma de base de dados. Para cada base de dados é criado um ramo que irá conter todas as configurações a ela referentes. O DN ramo criado tem o formato olcDatabase={Z}T,cn=config, em que Z representa a ordem de criação da base de dados e T o tipo da base de dados (ex. olcDatabase={2}mdb,cn=config).

As *overlays* (The OpenLDAP Project, 2016) são módulos que são ativados no ramo cn=module{0},cn=config, bastando para isso apenas adicionar um atributo olcModuleLoad com o nome do módulo a ativar (ex. olcModuleLoad ={0}syncprov). O valor 0 representa a ordem com que os módulos foram adicionados. Por sua vez, a configuração dos módulos é feita dentro da entrada referente à base de dados à qual o módulo será aplicado.

Na solução apresentada nesta dissertação foram usadas as seguintes *overlays*:

- Syncprov: fazer a sincronização da informação entre os servidores;
- Memberof: atualizar o atributo memberOf das entradas pertencentes a um grupo sempre que este for atualizado;
- Refint: atualizar as entradas de um grupo (ou outras) sempre que uma entrada é removida ou atualizada;
- Dynlist: criar listas de entradas dinâmicas baseadas num filtro;
- Constraint: aplicar regras sobre os valores que os atributos podem ter;
- Unique: garantir que os valores atributos são únicos.

3.2.4 Segurança

O OpenLDAP possui diversos mecanismos de segurança (Butcher, 2007; The OpenLDAP Project, 2016; ZYTRAX, Inc., 2016b) ao seu dispor para garantir que informação é acedida e por quem/o quê lhe acede. No desenho da solução apresentada foi considerada a segurança nas ligações ao servidor, através da configuração de ligações seguras TLS/SSL e a segurança no acesso à informação propriamente dita, ou seja, os atributos, entradas e ramos da estrutura em árvore que compõem todo o diretório.

Relativamente à segurança da ligação, é utilizada encriptação TLS/SSL nos portos 389 e 636, sendo que no porto 389 a ligação é efetuada de forma desencriptada e depois é negociada a encriptação (StartTLS), enquanto que no porto 636 é criado um túnel SSL e a comunicação LDAP é feita através desse túnel.

Por forma a garantir que os serviços que necessitam de aceder à informação armazenada no diretório LDAP apenas acedem aos atributos que necessitam, é criada uma entrada com o *objectclass* estrutural account e com o *objectclass* auxiliar simpleSecurityObject, que representa o serviço, por exemplo o serviço Radiator que é utilizado para autenticar os utilizadores da rede sem fios. É este utilizador que é empregue nas listas de controlo de acesso (ACL) com as permissões específicas para cada atributo, entrada, ramo ou totalidade do diretório

A configuração das ACL tem algumas particularidades, sendo que a mais importante tem que ver com ser centrada no objeto (atributo, entrada, ramo ou toda a árvore) sobre o qual serão dadas permissões e não no utilizador ao qual serão dadas as permissões.

Para melhor perceber a forma como são estruturadas as permissões, são aqui demonstradas as ACL que permitem o acesso do serviço Radiator aos atributos userPassword, x-pt-ipcb-wifiLMhash, x-pt-ipcb-wifiNThash e x-pt-ipcb-wifiUsername necessários para que o utilizador se autentique na rede sem fios:

Acesso de leitura à base do diretório por todos os utilizadores:

```
access to dn.base=""
by * read
```

Acesso de leitura ao ramo cn=Subchema por todos os utilizadores para que possam aceder às definições de *objectclass* e atributos do diretório:

```
access to dn.base="cn=Subschema"
by * read
```

Acesso de leitura à base da árvore por utilizadores autenticados:

```
access to dn.base="dc=ipcb,dc=pt"
by users read
```

Acesso de leitura ao ramo ou=People,dc=ipcb,dc=pt pelo utilizador uid=srv_radiator,ou=Services,dc=ipcb,dc=pt:

```
access to dn.base="ou=People,dc=ipcb,dc=pt"
by dn="uid=srv_radiator,ou=Services,dc=ipcb,dc=pt" read
```

Acesso de leitura aos atributos userPassword, x-pt-ipcb-wifiLMhash, x-pt-ipcb-wifiNThash e x-pt-ipcb-wifiUsername em todas as entradas criadas no ramo ou=People,dc=ipcb,dc=pt (dn.one) pelo próprio utilizador, dono dos atributos, e pelo utilizador uid=srv_radiator,ou=Services,dc=ipcb,dc=pt e acesso de autenticação a todos os utilizadores não autenticados:

```
access to dn.one="ou=People,dc=ipcb,dc=pt"
attrs=userPassword,x-pt-ipcb-wifiLMhash,x-pt-ipcb-wifiNThash,x-pt-ipcb-wifiUsername
by dn="uid=srv_radiator,ou=Services,dc=ipcb,dc=pt" read
by dn.children="ou=Admins,dc=ipcb,dc=pt" write
by anonymous auth
by self read
```

Acesso de leitura aos restantes atributos (atributos não considerados na ACL anterior) em todas as entradas criadas no ramo ou=People,dc=ipcb,dc=pt (dn.one) pelo próprio utilizador, dono dos atributos e acesso de autenticação a todos os utilizadores não autenticados:

```
access to dn.one="ou=People,dc=ipcb,dc=pt"
by dn.children="ou=Admins,dc=ipcb,dc=pt" write
by anonymous auth
by self read
```

Acesso de ligação do utilizador uid=srv_radiator,ou=Services,dc=ipcb,dc=pt a partir do endereço IP 193.137.66.131:

```
access to dn.base="uid=srv_radiator,ou=Services,dc=ipcb,dc=pt"
by peername.ip=193.137.66.131 anonymous auth
```

Aplicando os dois métodos de segurança mencionados consegue-se garantir um nível de segurança muito eficiente, tanto na ligação entre os serviços e o servidor como no acesso à informação de cada utilizador por parte dos serviços.

3.3 Organização lógica dos dados

Um diretório LDAP armazena a informação (The OpenLDAP Project, 2016; ZYTRAX, Inc., 2016) de forma hierárquica organizada sob a forma de uma árvore (DIT). A informação é armazenada em atributos (*atributes*), que por sua vez são agrupados em *objectclasses*. A definição das *objectclasses* e dos atributos é armazenada em esquemas (*schemas*).

A forma como está organizada a informação é muito importante, pois a aplicação de permissões de acesso está muito dependente desta organização.

A DIT tem como raiz a entrada dc=ipcb,dc=pt que irá conter toda a informação relativa aos utilizadores.

Por forma a manter a organização da árvore, existe um ramo chamado ou=people,dc=ipcb,dc=pt que contém todas as entradas relativas aos utilizadores existentes. Cada utilizador representa uma entrada neste ramo e esta está organizada de uma forma modular, pois com base no ciclo de vida de um utilizador, este pode assumir vários papéis ao logo da sua vida alternando entre aluno, docente, funcionário, aluno simples, docente contratado, etc. Existem muitas combinações para o perfil do utilizador num dado tempo da sua vida, pelo que a estrutura modular é a que mais se adequa à realidade em causa.

Qualquer entrada em qualquer ramo da DIT tem, obrigatoriamente, que ser composta por uma, e só uma, *objectclass* estrutural (*structural object class*) e nenhuma ou várias *objectclasses* auxiliares (*auxiliary object class*). Um dos atributos da entrada é escolhido para a identificar, dando origem a um DN que identifica essa entrada em toda a árvore ex. uid=joao.santos,ou=people,dc=ipcb,dc=pt.

Todas as entradas neste ramo têm por base a *objectclass* estrutural inetOrgPerson (OID: 2.16.840.1.113730.3.2.2) que é composta pelos atributos comuns a todos utilizadores como o nome completo, ultimo nome, id de utilizador, palavra passe e outros. A esta *objectclass* estrutural podem ser adicionadas várias *objectclasses* auxiliares, o que permite atingir a modularidade pretendida.

3.3.1 Atributos

Os atributos são unidades onde se guarda a informação e podem ter vários nomes e/ou abreviações (ex. *surname*, sn). Outro aspeto importante é o facto de poderem ser de valor único ou multi-valor. Com exceção do atributo *objectclass*, uma entrada não pode ter atributos que não estejam definidos numa *objectclass*.

Como é comum em bases de dados, os atributos são de um determinado tipo consoante os dados que se pretende armazenar. O OpenLDAP permite utilizar os seguintes tipos na criação dos atributos (Tabela 1):

Tabela 1 - Atributos criados

Designação:	x-pt-ipcb-digitalis-studentNumber
Tipo:	DirectoryString
Cardinalidade:	Multi-valor
Descrição:	Número de aluno na plataforma Digitalis
Designação:	x-pt-ipcb-digitalis-courseNumber

Tipo:	DirectoryString
Cardinalidade:	Multi-valor
Descrição:	Número do curso na plataforma Digitalis
Designação:	x-pt-ipcb-digitalis-facultyStaffNumber
Tipo:	DirectoryString
Cardinalidade:	Multi-valor
Descrição:	Número de docente ou funcionário na plataforma Digitalis
Designação:	x-pt-ipcb-digitalis-individualID
Tipo:	DirectoryString
Cardinalidade:	Valor único
Descrição:	Número de único do aluno, docente ou funcionário na plataforma Digitalis
Designação:	x-pt-ipcb-digitalisUsername
Tipo:	DirectoryString
Cardinalidade:	Valor único
Descrição:	Nome de utilizador na plataforma Digitalis
Designação:	x-pt-ipcb-LMhash
Tipo:	IA5 String (tamanho máximo de 32 caracteres)
Cardinalidade:	Valor único
Descrição:	Hash Microsoft LAN Manager da palavra passe
Designação:	x-pt-ipcb-NThash
Tipo:	IA5 String (tamanho máximo de 32 caracteres)
Cardinalidade:	Valor único
Descrição:	Hash Microsoft NT LAN Manager da palavra passe
Designação:	x-pt-ipcb-wifiUsername
Tipo:	DirectoryString
Cardinalidade:	Valor único
Descrição:	Nome de utilizador da rede sem fios
Designação:	x-pt-ipcb-sigaId
Tipo:	DirectoryString
Cardinalidade:	Multi-valor
Descrição:	Nome de utilizador do Sistema Integrado de Gestão Administrativa. Uma entrada pode ter mais do que um valor deste atributo pois um utilizador pode, por exemplo, ser funcionário e aluno ao mesmo tempo.
Designação:	x-pt-ipcb-studentOrganicUnit
Tipo:	DirectoryString
Cardinalidade:	Multi-valor
Descrição:	Unidade orgânica a que o aluno pertence. Podem existir vários valores deste atributo pois o aluno pode pertencer a várias unidades orgânicas, por exemplo, estar matriculado em cursos de duas escolas.
Designação:	x-pt-ipcb-facultyOrganicUnit
Tipo:	DirectoryString
Cardinalidade:	Multi-valor
Descrição:	Unidade orgânica a que o docente pertence. Podem existir vários valores deste atributo pois o docente pode pertencer a várias unidades orgânicas, por exemplo, lecionar em cursos de duas escolas.
Designação:	x-pt-ipcb-staffOrganicUnit

Tipo:	DirectoryString
Cardinalidade:	Multi-valor
Descrição:	Unidade orgânica a que o funcionário pertence. Podem existir vários valores deste atributo pois o funcionário pode pertencer a várias unidades orgânicas.
Designação:	x-pt-ipcb-adEncriptedPassword
Tipo:	DirectoryString
Cardinalidade:	Valor único
Descrição:	Palavra passe do utilizador encriptada utilizando certificados digitais.
Designação:	x-ipcb-adAction
Tipo:	DirectoryString
Cardinalidade:	Valor único
Descrição:	Ação a realizar sobre a conta do utilizador. Este atributo pode ter os seguintes valores: create, update e delete.
Designação:	x-pt-ipcb-adDeletionDate
Tipo:	GeneralizedTime
Cardinalidade:	Valor único
Descrição:	Data para a remoção do utilizador.
Designação:	x-pt-ipcb-o365StaffFacultyMail
Tipo:	DirectoryString
Cardinalidade:	Multi-valor
Descrição:	Endereço de email institucional do docente ou funcionário. Este atributo pode ter mais do que um valor, pois o docente ou funcionário pode ter mais do que uma conta de email, por exemplo, um membro da direção.
Designação:	x-pt-ipcb-o365StudentMail
Tipo:	DirectoryString
Cardinalidade:	Valor único
Descrição:	Endereço de email institucional do aluno.
Designação:	x-pt-ipcb-o365EncriptedPassword
Tipo:	DirectoryString
Cardinalidade:	Valor único
Descrição:	Palavra passe do utilizador encriptada utilizando certificados digitais.
Designação:	x-pt-ipcb-o365Action
Tipo:	DirectoryString
Cardinalidade:	Valor único
Descrição:	Ação a realizar sobre a conta do utilizador. Este atributo pode ter os seguintes valores: create, update.
Designação:	x-pt-ipcb-PTcivilId
Tipo:	DirectoryString
Cardinalidade:	Valor único
Descrição:	Número de identificação civil português
Designação:	x-pt-ipcb-PTfiscalId
Tipo:	DirectoryString
Cardinalidade:	Valor único
Descrição:	Número de identificação fiscal português
Designação:	x-pt-ipcb-otherId
Tipo:	DirectoryString

Cardinalidade:	Multi-valor
Descrição:	Qualquer outro código de identificação legal (passaporte, autorização de residência e etc.)
Designação:	x-pt-ipcb-birthDate
Tipo:	GeneralizedTime
Cardinalidade:	Valor único
Descrição:	Data de nascimento
Designação:	x-pt-ipcb-studentOrganicUnit
Tipo:	DirectoryString
Cardinalidade:	Multi-valor
Descrição:	Unidades orgânicas às quais o aluno pertence
Designação:	x-pt-ipcb-facultyOrganicUnit
Tipo:	DirectoryString
Cardinalidade:	Multi-valor
Descrição:	Unidades orgânicas às quais o docente pertence
Designação:	x-pt-ipcb-staffOrganicUnit
Tipo:	DirectoryString
Cardinalidade:	Multi-valor
Descrição:	Unidades orgânicas às quais o funcionário pertence
Designação:	x-pt-ipcb-outsideType
Tipo:	DirectoryString
Cardinalidade:	Valor único
Descrição:	Tipo de utilizador externo (estagiário, convidado, recorrente e outros que sejam necessários)
Designação:	x-pt-ipcb-outsideOrganicUnit
Tipo:	DirectoryString
Cardinalidade:	Multi-valor
Descrição:	Unidades orgânicas às quais o utilizador externo pertence
Designação:	x-pt-ipcb-outsideDeletionDate
Tipo:	GeneralizedTime
Cardinalidade:	Valor único
Descrição:	Data para remoção a entrada do utilizador externo
Designação:	x-pt-ipcb-idpUsername
Tipo:	DirectoryString
Cardinalidade:	Valor único
Descrição:	Nome de utilizador no serviço de identificação federada

Neste documento estão representados apenas os atributos que foram criados especificamente para esta solução de armazenamento de credenciais.

3.3.2 *Objectclasses*

As *objectclasses* são grupos de atributos em que é definido, atributo a atributo, se é obrigatório ou opcional. Numa entrada da DIT só é possível guardar dados em atributos se estes estiverem definidos numa *objectclass* adicionada a essa entrada.

Para manter a organização da informação de forma modular, foram criadas *objectclasses* para agrupar a informação de acordo com a necessidade da aplicação que dela vai necessitar, por exemplo x-pt-ipcb-digitalis. Foram ainda criadas *objectclasses* que agrupam os atributos pelo tipo de informação, por exemplo x-pt-ipcb-civilIdentity, que agrupa informação relativa à identificação civil do utilizador.

x-pt-ipcb-digitalis

Esta *objectclass* define os atributos utilizados pelo sistema de gestão académica Digitalis. Um aluno, docente ou funcionário necessita destes atributos na sua entrada para que este sistema funcione convenientemente.

Atributos obrigatórios:

- userPassword
- x-pt-ipcb-digitalis-individualID
- x-pt-ipcb-digitalisUsername

Atributos opcionais:

- x-pt-ipcb-digitalis-studentNumber
- x-pt-ipcb-digitalis-courseNumber
- x-pt-ipcb-digitalis-facultyStaffNumber

x-pt-ipcb-wifi

Esta *objectclass* define os atributos utilizados pela autenticação da rede sem fios e do sistema de VPN. Para se autenticar na rede sem fios ou na VPN com um cliente Windows é necessária a existência de dois *hashes* gerados a partir da palavra passe do utilizador.

Atributos obrigatórios:

- x-pt-ipcb-LMhash
- x-pt-ipcb-NThash
- x-pt-ipcb-wifiUsername
- userPassword

Sendo todos os atributos obrigatórios e dado o seu carácter especial, esta *objectclass* deve ser adicionada a uma entrada de utilizador em dois momentos: a criação e a alteração do atributo userPassword (pertence à *objectclass* inetOrgPerson), pois é o único momento em que se tem acesso à palavra-passe sem estar encriptada de forma não reversível.

x-pt-ipcb-siga

Esta *objectclass* define os atributos utilizados pelo SIGA. Devido a limitações deste sistema, não pôde ser utilizado o atributo email ou uid para definir o *username* do utilizador que se autentica. Assim, foi definido um atributo para realizar esta tarefa.

Atributos obrigatórios:

- x-pt-ipcb-sigaId
- userPassword

x-pt-ipcb-active-directory

Esta *objectclass* define os atributos utilizados pelo script de manipulação dos utilizadores no *Active Directory*. A inexistência desta *objectclass* na entrada do utilizador significa que esta será ignorada pelo script.

Atributos obrigatórios:

- uid
- edupersonPrimaryAffiliation

Atributos opcionais:

- x-pt-ipcb-studentOrganicUnit
- x-pt-ipcb-facultyOrganicUnit
- x-pt-ipcb-staffOrganicUnit
- x-pt-ipcb-adEncriptedPassword
- x-ipcb-adAction
- x-pt-ipcb-adDeletionDate

x-pt-ipcb-o365

Esta *objectclass* define os atributos utilizados pelo *script* de manipulação dos utilizadores no serviço Office 365. A inexistência desta *objectclass* na entrada do utilizador significa que esta será ignorada pelo *script* e consequentemente não será criada ou atualizada a sua conta (ou contas, caso seja aluno e docente ou funcionário) no serviço Office 365.

Atributos obrigatórios:

- edupersonPrimaryAffiliation

Atributos opcionais:

- x-pt-ipcb-studentOrganicUnit
- x-pt-ipcb-facultyOrganicUnit
- x-pt-ipcb-staffOrganicUnit
- x-pt-ipcb-staffFacultyMail

- x-pt-ipcb-studentMail
- x-pt-ipcb-o365EncriptedPassword
- x-pt-ipcb-o365Action

x-pt-ipcb-civilIdentity

Esta *objectclass* define os atributos necessários para guardar a identificação civil dos utilizadores.

Atributos opcionais:

- x-pt-ipcb-PTcivilId
- x-pt-ipcb-PTfiscalId
- x-pt-ipcb-otherId
- x-pt-ipcb-birthDate

x-pt-ipcb-institutional

Esta *objectclass* define os atributos necessários para guardar a informação das unidades orgânicas onde pertencem os alunos, docentes e funcionários.

Atributos opcionais:

- x-pt-ipcb-studentOrganicUnit
- x-pt-ipcb-facultyOrganicUnit
- x-pt-ipcb-staffOrganicUnit

x-pt-ipcb-outside

Esta *objectclass* compreende todos os atributos que não têm uma organização específica, mas que são necessários para a gestão do ciclo de vida do utilizador

É composta pelos seguintes atributos:

- x-pt-ipcb-outsideType
- x-pt-ipcb-outsideDeletionAlertDate
- x-pt-ipcb-outsideDeletionDate

x-pt-ipcb-idp

Esta *objectclass* define os atributos utilizados pelo serviço de autenticação federada.

Atributos obrigatórios:

- x-pt-ipcb-idpUsername
- userPassword

3.4 Sincronização com *Active Directory*

O AD é uma solução de armazenamento de credenciais da Microsoft, que tem por base um diretório LDAP, com o objetivo de integrar as credenciais dos utilizadores de todos os produtos deste fabricante. Esta solução não é *open-source* e é bastante fechada no que à customização diz respeito.

Uma vez que a grande maioria dos computadores do IPCB estão instalados com sistemas operativos Microsoft (Windows 7, 8, 8.1 e 10) que não autenticam diretamente num diretório LDAP *standard*, como o OpenLDAP, torna-se necessário implementar um AD central e sincronizar as credenciais com o diretório LDAP central para que as credenciais sejam as mesmas em todos os serviços da instituição.

Para operacionalizar a sincronização foi definida a *objectclass* x-pt-ipcb-activeDirectory que, em conjunto com a *objectclass* inetOrgPerson armazenam a informação relevante para este processo.

É necessário que o processo de sincronização entre o LDAP e o AD seja feito no sentido LDAP –> AD. A razão desta configuração prende-se com o facto de que o diretório LDAP central concentra a autenticação de diversos serviços (Wifi, IDP, Digitalis e etc.) enquanto o AD apenas de um: a autenticação dos utilizadores ao entrarem num computador com o sistema operativo Windows. Existe ainda outro problema que obriga a esta configuração: não é possível obter a palavra-passe desencriptada dos utilizadores no momento em que estes a criam/alteram, o que invalida a autenticação na rede sem fios utilizando PEAP pois esta é necessária para gerar os valores (*hashes*) dos atributos x-pt-ipcb-LMhash e x-pt-ipcb-NThash.

No AD as credenciais devem estar armazenadas dentro de 3 unidades organizacionais:

- Staff
- Faculty
- Student

Devem existir grupos que representem as unidades orgânicas do IPCB de forma a que os utilizadores sejam adicionados a estes grupos para depois terem acesso recursos partilhados como pastas partilhadas ou impressoras:

- PSC
- ESA
- ESALD
- ESART
- ESE
- ESG
- EST

A sincronização com o AD deve ser feita como representado na Figura 8:

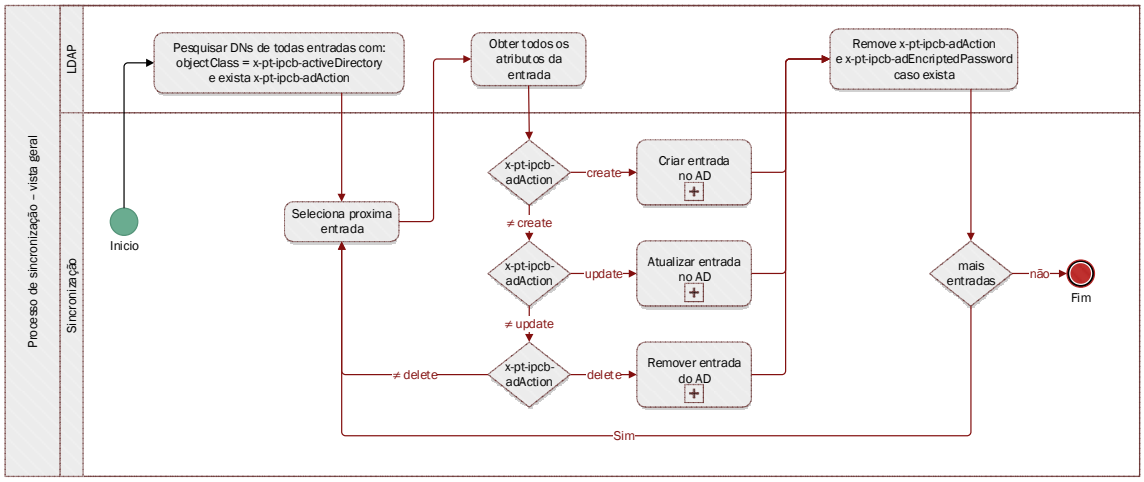

Figura 8 - Processo de sincronização com o AD

De acordo com a Figura é necessário:

1. Obter todas as entradas com a *objectclass* x-pt-ipcb-activeDirectory em que exista o atributo x-pt-ipcb-adAction.
2. Para cada entrada obter todos os seus atributos;
3. Caso o atributo x-pt-ipcb-adAction contenha o valor:
    a. *create*: deve ser criada a entrada no AD (detalhado abaixo);
    b. *update*: deve ser atualizada a entrada no AD (detalhado abaixo);
    c. *delete*: a entrada deve ser removida do AD (detalhado abaixo);
4. Após qualquer operação de sincronização os atributos x-pt-ipcb-adAction e x-pt-ipcb-adEncriptedPassword (caso exista) devem ser removidos da entrada do utilizador em questão, exceto no caso de remoção uma vez que a entrada é totalmente removida.

Olhando em pormenor ao subprocesso de criação de uma entrada no AD (Figura 9):

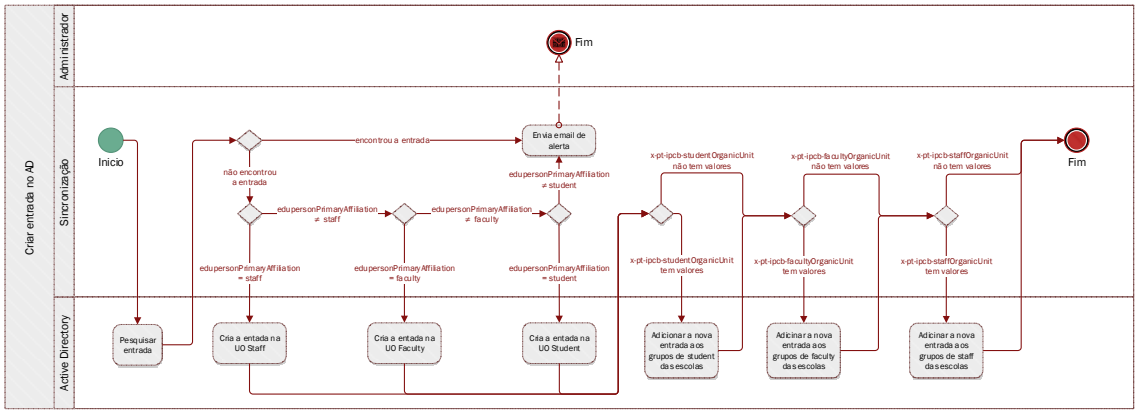

Figura 9 - Subprocesso de criação de entrada no AD

De acordo com o esquema apresentado o subprocesso de entrada engloba:

1. Procurar a entrada no AD a ver se já existe:
    a. Caso exista, deve ser enviado um email de alerta ao administrador do sistema e de seguida terminar o subprocesso;

2. Criar a entrada no AD em que o utilizador tem o valor contido no atributo uid com a palavra-passe existente em x-pt-ipcb-adEncriptedPassword, reviamente desencriptada, bem como a respetiva pasta de utilizador (*home*), que deverá ter como nome o valor contido em uid. A entrada deve ser criada na unidade organizacional de acordo com o valor contido no atributo eduPersonPrimaryAffiliation:
    a. *student*: a entrada deve ser criada na unidade organizacional Student;
    b. *faculty*: a entrada deve ser criada na unidade organizacional Faculty;
    c. *staff*: a entrada deve ser criada na unidade organizacional Staff;
3. Uma entrada não tem obrigatoriamente de conter todos os 3 atributos: x-pt-ipcb-studentOrganicUnit, x-pt-ipcb-facultyOrganicUnit e x-pt-ipcb-staffOrganicUnit. Se o utilizador for, por exemplo, apenas aluno só terá o atributo x-pt-ipcb-studentOrganicUnit;
4. A entrada deve ser adicionada aos grupos das unidades orgânicas de acordo com os valores contidos nos atributos x-pt-ipcb-studentOrganicUnit, x-pt-ipcb-facultyOrganicUnit e x-pt-ipcb-staffOrganicUnit.

Olhando em pormenor ao subprocesso de atualização de uma entrada no AD (Figura 10):

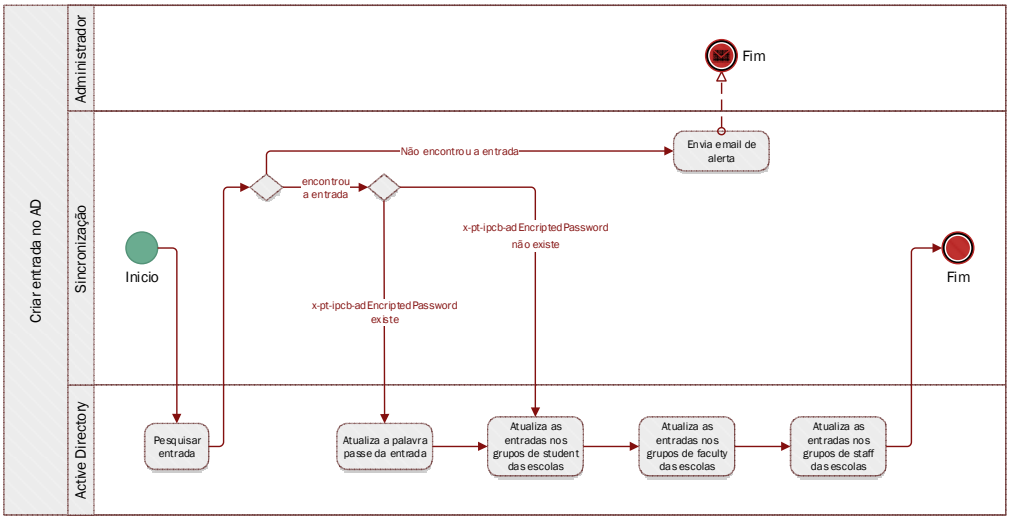

Figura 10 - Subprocesso de atualização de uma entrada no AD

No caso do subprocesso de atualização teremos:

1. Procurar a entrada no AD para verificar se existe:
    a. Caso não exista, deve ser enviado um email de alerta ao administrador do sistema e de seguida terminar o subprocesso;
2. Se o atributo x-pt-ipcb-adEncriptedPassword existir então a palavra passe deve ser alterada;
3. Os grupos a que a entrada pertence devem ser atualizados de acordo com os valores contidos nos atributos x-pt-ipcb-studentOrganicUnit, x-pt-ipcb-facultyOrganicUnit e x-pt-ipcb-staffOrganicUnit.

Olhando em pormenor ao subprocesso de remoção de uma entrada no AD (Figura 11):

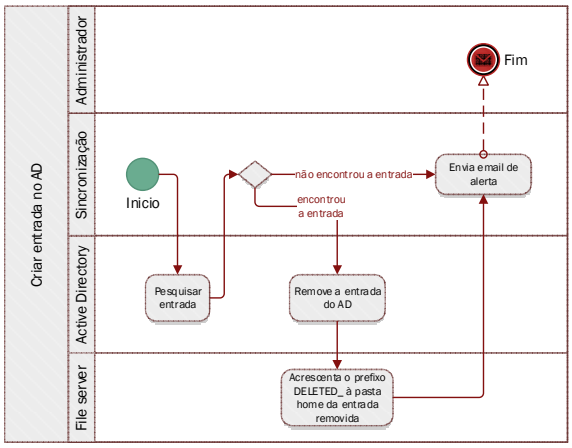

Figura 11 - Subprocesso de remoção de uma entrada no AD

No subprocesso de remoção encontramos as seguintes etapas:

1. Procurar a entrada no AD para verificar se existe:
    a. Caso não exista, deve ser enviado um email de alerta ao administrador do sistema e de seguida terminar o subprocesso;
2. A entrada deve ser removida do AD;
3. Deve ser acrescentado à pasta do utilizador (*home*) o prefixo DELETED_;
4. Deve ser enviado um email de alerta ao administrador do sistema, a notificar esta operação e de seguida terminar o subprocesso.

3.5 Sincronização com Office 365

O Office365 é uma solução de *Software as a Service* (SaaS) composto por um conjunto de serviços on-line, dos quais o correio eletrónico é o mais conhecido. Atualmente o Office 365 disponibiliza um conjunto muito vasto de serviços, entre os quais o OneDrive (armazenamento na nuvem), o OneNote, o Office On-line instalável, o SharePoint e muitos mais.

O IPCB foi uma das primeiras instituições de ensino superior do país a adotar esta solução. Na altura era conhecida por Live@Edu e só disponibilizava o serviço de correio eletrónico que era baseado na plataforma do serviço de email Hotmail.

Da mesma forma que outras sincronizações, para operacionalizar a sincronização foi definida a *objectclass* x-pt-ipcb-o365 que, em conjunto com a *objectclass* inetOrgPerson armazena a informação relevante para este processo.

Tal como como a sincronização com o *AD*, a sincronização com o Office 365 é feita apenas no sentido LDAP –> Office365 pelas mesmas razões.

A solução Office 365 do IPCB é composta por 2 domínios: ipcb.pt e ipcbcampus.pt. O primeiro para docentes e funcionários e o segundo para alunos.

Nas contas de correio eletrónico do serviço Office 365 existem 15 campos especiais, com o nome de CustomAttributeX (Em que X tem um valor entre 1 e 15), que podem ser utilizados para guardar informação relevante associada a cada conta. Na solução do IPCB estes campos são depois utilizados para associar a conta de correio eletrónico às listas de distribuição de correio eletrónico das escolas a que pertence.

As contas de correio eletrónico disponibilizadas à comunidade académica do IPCB são vitalícias pelo que não é considerada a ação de remover uma conta.

A sincronização com o Office365 deve ser feita de acordo com a Figura 12:

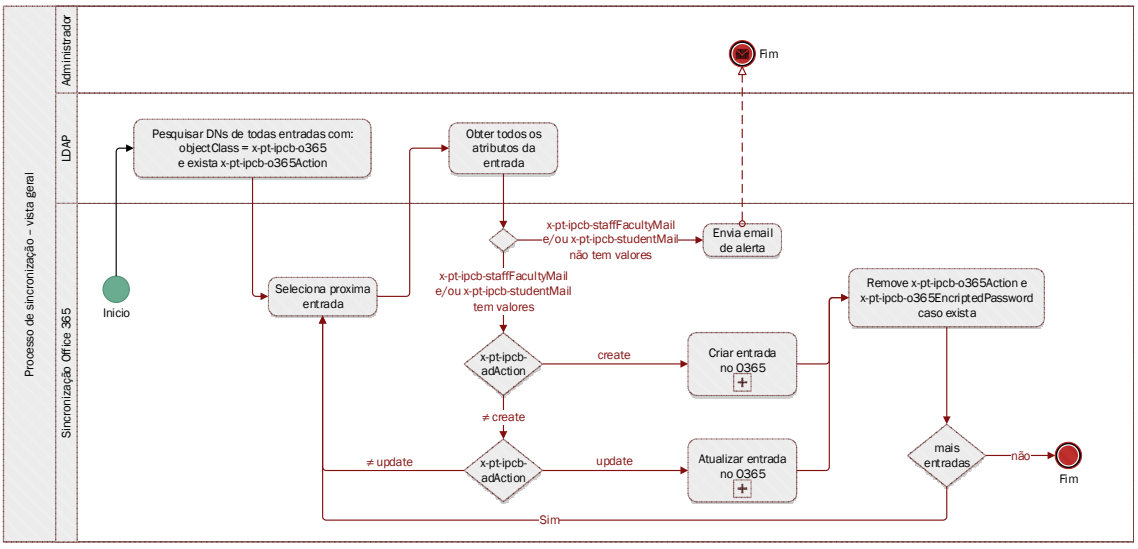

Figura 12 - Processo de sincronização com o Office 365

Neste esquema é possível algumas ações na sincronização:

1. Obter todas as entradas com a *objectclass* x-pt-ipcb-o365, em que exista o atributo x-pt-ipcb-o365Action;
2. Para cada entrada obter todos os seus atributos;
3. Caso o atributo x-pt-ipcb-o365Action contenha o valor:
    a. *create*: deve ser criada a entrada no AD (detalhado abaixo);
    b. *update*: deve ser atualizada a entrada no AD (detalhado abaixo);
4. Após qualquer operação de sincronização o atributo x-pt-ipcb-o365Action e x-pt-ipcb-o365EncriptedPassword (caso exista) devem ser removidos da entrada do utilizador em questão.

Olhando em pormenor ao subprocesso de criação de uma entrada no Office 365 (Figura 13):

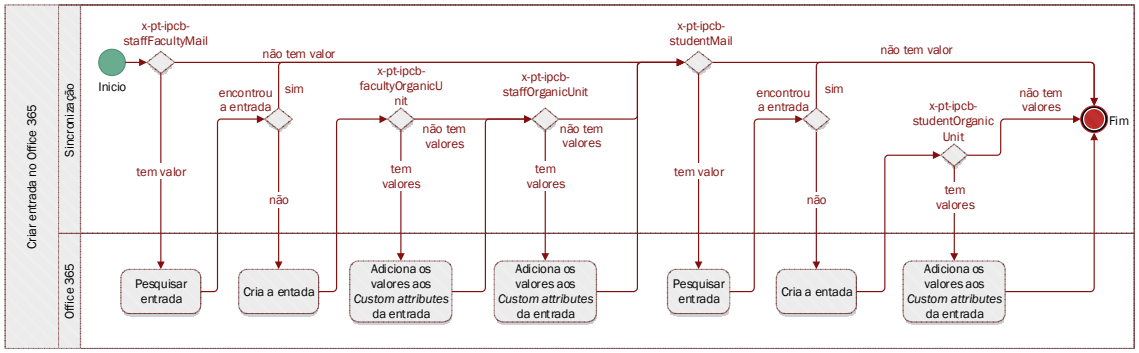

Figura 13 - Subprocesso de criação de uma entrada no Office 365

1. Verificar se a entrada tem o atributo x-pt-ipcb-staffFacultyMail existe/tem valor;
    a. Caso não exista/não tenha valor, verificar o atributo x-pt-ipcb-studentMail (ponto 5)
2. Procurar a entrada no Office 365 a ver se já existe;
    a. Caso exista, verificar o atributo x-pt-ipcb-studentMail (ponto 5)
3. Criar a entrada no Office 365 em que o endereço de correio eletrónico conta tem o valor contido em x-pt-ipcb-staffFacultyMail com a palavra-passe existente em x-pt-ipcb-o365EncriptedPassword, previamente desencriptada. O valor do atributo eduPersonPrimaryAffiliation deve ser adicionado ao CustomAtribute1 da entrada;
4. Caso existam valores nos atributos x-pt-ipcb-facultyOrganicUnit e x-pt-ipcb-staffOrganicUnit devem, também, ser adicionados aos CustomAttributes da entrada;
5. Verificar se a entrada tem o atributo x-pt-ipcb-studentMail existe/tem valor:
    a. Caso não exista/não tenha valor, deve terminar.
6. Procurar a entrada no Office 365 a ver se já existe;
    a. Caso exista, deve terminar.
7. Criar a entrada no Office 365 em que o endereço de correio eletrónico tem o valor contido em x-pt-ipcb-studentMail com a palavra-passe existente em x-pt-ipcb-o365EncriptedPassword, previamente desencriptada. O valor do atributo eduPersonPrimaryAffiliation deve ser adicionado ao CustomAtribute1 da entrada.
8. Caso existam valores no atributo x-pt-ipcb-studentOrganicUnit, devem também ser adicionados aos CustomAttributes da entrada.

Olhando em pormenor ao subprocesso de atualização de uma entrada no Office 365 (Figura 14):

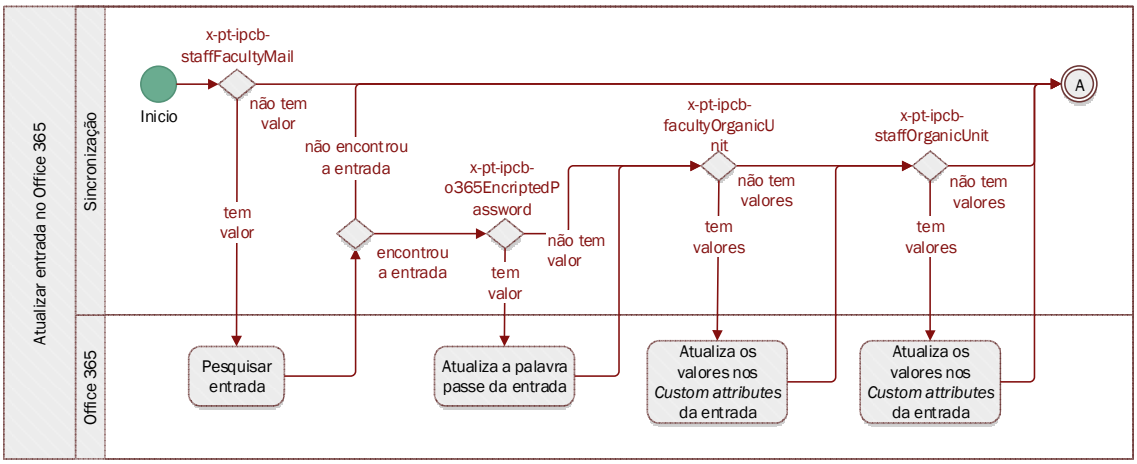

Figura 14 - Subprocesso de atualização de uma entrada no Office 365

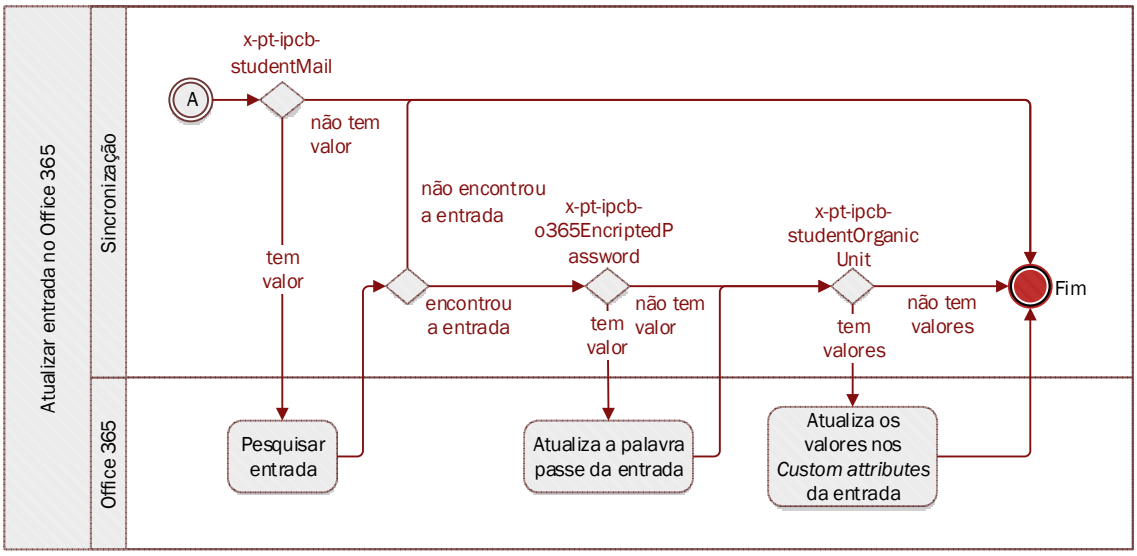

Figura 15 - Subprocesso de atualização de uma entrada no Office 365 (cont.)

1. Verificar se a entrada tem o atributo x-pt-ipcb-staffFacultyMail existe/tem valor;
    a. Caso não exista/não tenha valor, verificar o atributo x-pt-ipcb-studentMail (ponto 5);
2. Procurar a entrada no Office 365 a ver se já existe;
    a. Caso não exista, verificar o atributo x-pt-ipcb-studentMail (ponto 5);
3. Caso o atributo x-pt-ipcb-o365EncriptedPassword exista, atualizar a palavra passe da conta;
4. Caso existam valores nos atributos x-pt-ipcb-facultyOrganicUnit e x-pt-ipcb-staffOrganicUnit devem, também, ser atualizados os CustomAttributes da entrada.
5. Verificar se a entrada tem o atributo x-pt-ipcb-studentMail (Figura 15) existe/tem valor;
    a. Caso não exista/não tenha valor, deve terminar;
6. Procurar a entrada no Office 365 a ver se já existe;
    a. Caso não exista, terminar;

7. Caso o atributo x-pt-ipcb-o365EncriptedPassword exista, atualizar a palavra passe da conta;
8. Caso existam valores nos atributos x-pt-ipcb-studentOrganicUnit devem, também, ser atualizados os CustomAttributes da entrada.

3.6 Interligação com os serviços

Se no caso do AD e do Office 365 os atributos dos utilizadores são sincronizados com estes serviços, uma vez que não é possível fazer com que estes se liguem ao diretório LDAP para autenticarem os utilizadores, nos restantes serviços não é feita qualquer sincronização visto que, estes para autenticarem os utilizadores e obterem atributos, consultam diretamente o diretório LDAP, sendo esta a solução pretendida.

3.6.1 RADIUS

O serviço RADIUS é fornecido pelo software servidor Radiator da empresa OSC - Open System Consultants Pty Ltd (OSC, 2017), que é utilizado para a autenticação dos utilizadores na rede sem fios e na VPN.

Esta autenticação é realizada quando o utilizador se liga na rede sem fios ou na VPN e tem por objetivo validar as suas credenciais. No momento da autenticação o servidor RADIUS liga-se ao diretório LDAP e compara o utilizador autenticado com o atributo x-pt-ipcb-wifiUsername e a palavra passe com o atributo userPassword ou com os atributos x-pt-ipcb-LMhash e x-pt-ipcb-NThash consoante o tipo de autenticação utilizada, TTLS ou PEAP na autenticação da rede sem fios e MS-CHAP v2 na autenticação da VPN.

3.6.2 Shibboleth/simpleSAMLphp

O Shibboleth e o SimpleSAMLphp são dois softwares servidor cuja função é providenciar identidade (*Identity Provider* - IDP) e informação extra sobre os utilizadores aos provedores de serviços (SP) que os utilizem para autenticação.

Uma vez que ambos os servidores providenciam SSO, o acesso ao diretório LDAP pode ser feito em dois momentos; quando o utilizador acede a um SP (ex. acede a um site em que a autenticação é feita através do IDP) ou então quando um utilizador já autenticado acede a outro SP fazendo uso das capacidades de SSO do IDP. Seja qual o for o momento, do ponto de vista do diretório LDAP o acesso é feito da mesma forma e estes dois servidores Shibboleth e o SimpleSAMLphp têm acesso a todos os atributos,

exceto os que armazenam as palavras passe ou *hashes* das mesmas, ou seja, userPassword, x-pt-ipcb-LMhash e x-pt-ipcb-NThash.

O funcionamento da autenticação é idêntico ao do serviço RADIUS. No entanto, o atributo que armazena o utilizador é o x-pt-ipcb-idpUsername e password é o userPassword.

3.6.3 Sistema de gestão académica

O sistema de gestão académica é providenciado por um software servidor da empresa Digitalis Informática e faz um uso intensivo do diretório LDAP, não só para autenticação, que se processa da mesma forma que os servidores IDP, ainda que com atributos diferentes (x-pt-ipcb-digitalisUsername), mas para armazenar diferente informação como o número de aluno (x-pt-ipcb-digitalis-studentNumber) o código de curso (x-pt-ipcb-digitalis-courseNumber), o número de docente ou funcionário (x-pt-ipcb-digitalis-facultyStaffNumber) e o identificador individual do aluno (x-pt-ipcb-digitalis-individualID).

Esta aplicação requer ainda, para funcionar corretamente, um ramo com permissões de escrita e leitura de forma a ser permitido criar entradas com informação diversa durante o seu funcionamento. As credenciais utilizadas para escrita neste ramo são as mesmas que as que lhe permitem aceder aos restantes ramos da árvore, no entanto, neste ramo podem criar, alterar e remover entradas.

3.6.4 Sistema de e-learning e SIGA

O sistema de e-Learning e o SIGA são serviços distintos, o primeiro usa um software servidor Moodle, de código aberto, e o segundo foi desenvolvido pelo Instituto Superior de Engenharia do Porto, no entanto a sua forma de interagirem com o diretório LDAP é idêntica, ou seja, quando um utilizador se autentica nestes serviços é feita uma ligação ao diretório LDAP e são comparados os atributos: x-pt-ipcb-sigaId e userPassword no caso do SIGA e x-pt-ipcb-staffFacultyMail ou x-pt-ipcb-studentMail e userPassword no caso do Moodle, não sendo utilizada mais informação do diretório LDAP.

3.7 Síntese

Neste capítulo foi apresentada a forma como os serviços, cujas credenciais dependem da solução apresentada, interagem com a mesma, assim como as funcionalidades da solução apresentada e a sua arquitetura incluindo os tipos de replicação existentes.

Foram identificados os módulos (*overlays*) do servidor OpenLDAP usados na solução e a forma como a segurança (encriptação na ligação ao servidor e listas de controlo de acesso) é assegurada na solução apresentada.

Posteriormente, foi apresentada a organização lógica dos dados na árvore de diretório, bem como os atributos e *objectclasses* implementados para permitir o armazenamento da informação (credenciais) pretendida.

Foram também explicadas as sincronizações das credenciais armazenadas na solução com o *Active Directory* e com o Office 365, ambos da Microsoft, bem como a interligação com os restantes serviços.

CAPÍTULO 4 – TESTES

Pretende-se, com a realização de testes de desempenho, validar se a solução apresentada, dois servidores OpenLDAP configurados em *N-Way Multi-Master replication*, tem a capacidade suficiente para dar resposta às necessidades do IPCB.

Com os testes de disponibilidade, prende-se observar se a solução proposta é capaz de dar garantias de alta disponibilidade. Este requisito é obrigatório pois é central a toda a solução proposta.

4.1 Cenário de testes

O cenário de teste utilizado foi escolhido tendo por base a realidade do IPCB, ou seja, todos os servidores do IPCB são virtualizados utilizando VMware ESXi 6.0 Update 2, pelo que os testes foram realizados em cima desta plataforma já que a implementação da solução será feita exatamente no mesmo ambiente.

Foram criadas 3 máquinas virtuais com 4 vCPU (o servidor físico tem 2 CPU Intel(R) Xeon(R) CPU X5650 2.67GHz cada um com 6 núcleos) e 2 GB de memória RAM. Duas destas máquinas virtuais foram configuradas com OpenLDAP em *N-Way Multi-Master replication*. A terceira máquina virtual tem por função realizar testes às primeiras duas.

4.2 Testes ao desempenho

Para realizar os testes foram criados dois scripts. Um *script*, utilizando a linguagem de programação Python, que realiza as operações sobre um dos servidores e pesquisa sobre o outro, aferindo assim os tempos de sincronização entre os servidores para as operações ADD, MODIFY e DELETE. Não foram realizados testes sobre a operação SEARCH, uma vez que esta não provoca interações entre os dois servidores. O segundo script, criado em linguagem de *scripting* Bash, tem o propósito de executar o *script* Python o número de vezes indicado, ou seja, executar os testes para uma determinada quantidade de entradas 100 vezes, aumentando assim a precisão dos valores.

O *script* desenvolvido em Python 2.7.5, sistema operativo Linux Centos 7 necessita de 3 parâmetros de entrada para ser executado: total de entradas, total de testes e o teste corrente. O *script* apresenta o seguinte funcionamento:

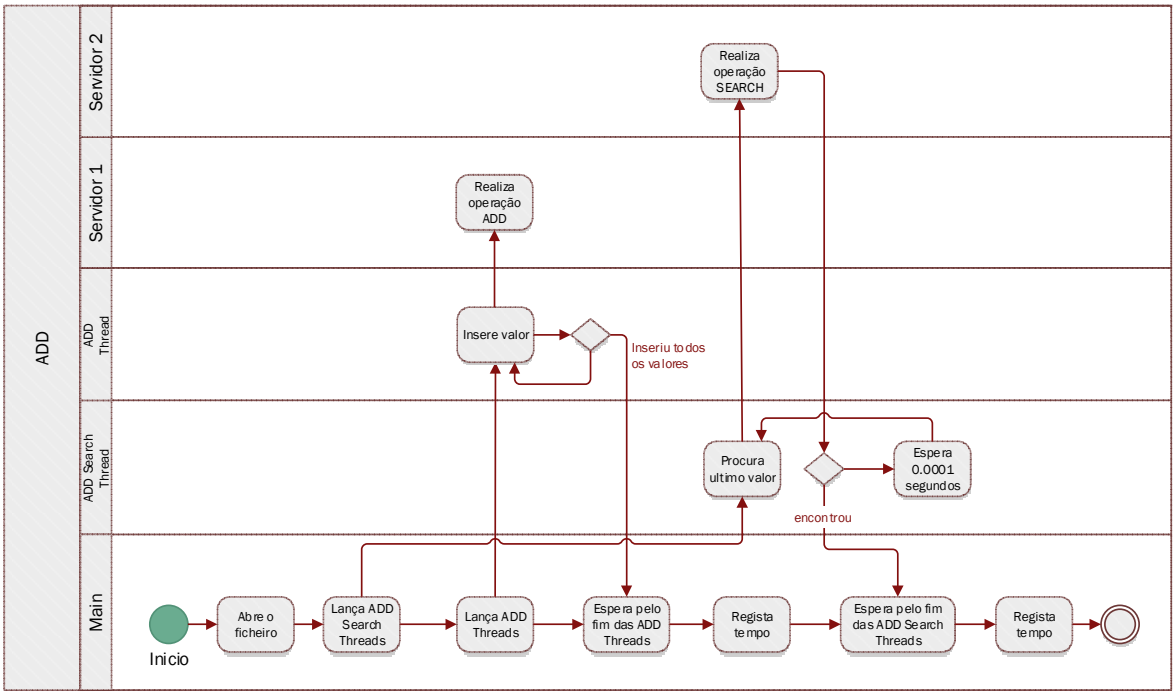

Figura 16 - Processo de teste da operação ADD

Como se pode observar na Figura 16:

Em primeiro lugar, são lançadas as *threads* de procura no segundo servidor ADDSRC e de seguida começa a inserção dos valores no primeiro servidor.

A *thread* ADDSRC termina quando o último valor a ser inserido no primeiro servidor for encontrado no segundo servidor.

Por fim, é registado o tempo das duas operações ADD e ADDSRC no ficheiro e são aguardados 5 segundos, para que os servidores estabilizem, terminando todas as operações que possam estar por realizar.

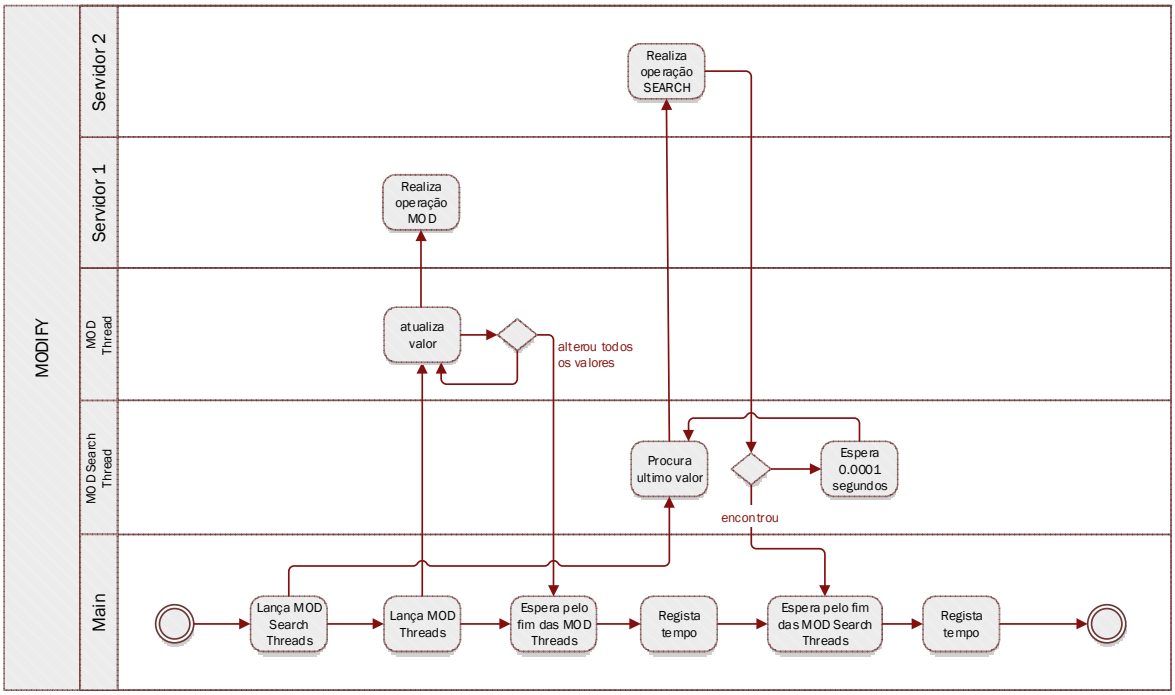

Figura 17 - Processo de teste da operação MODIFY

De seguida (Figura 17), são lançadas as *threads* de procura MODSRC no segundo servidor e começa a alteração dos valores no primeiro servidor.

A *thread* MODSRC termina quando o último valor a ser alterado no primeiro servidor for encontrado no segundo servidor.

Novamente, é registado o tempo das duas operações MOD e MODSRC no ficheiro e aguardados 5 segundos, para estabilização dos servidores.

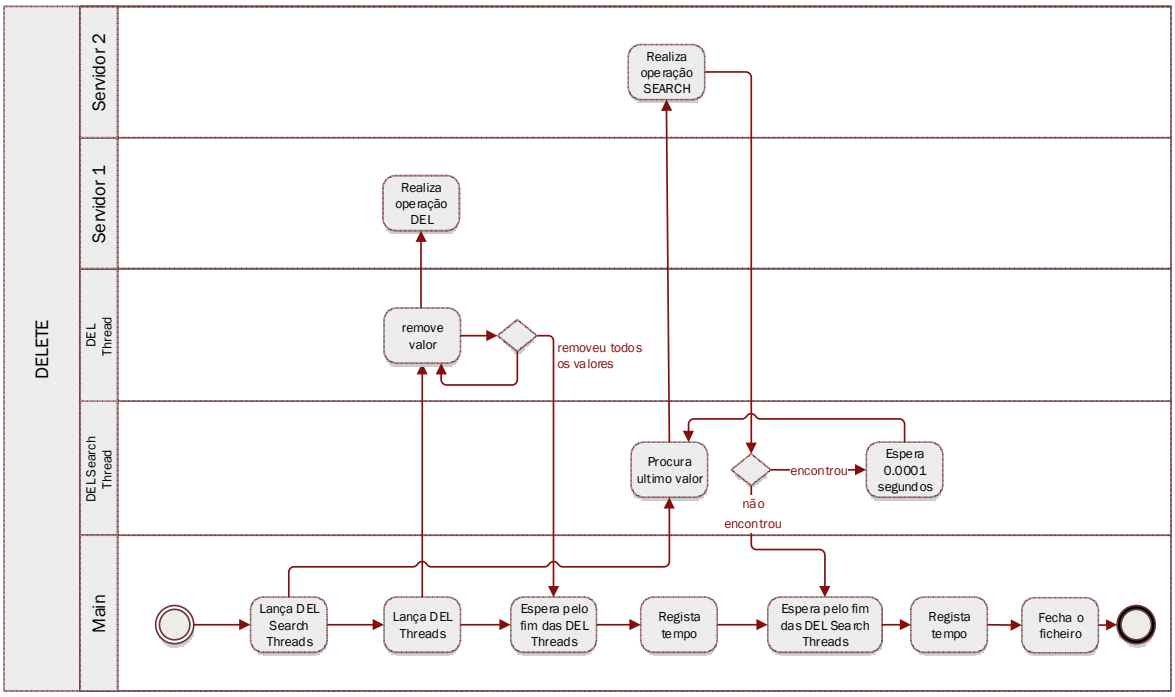

Figura 18 - Processo de teste da operação DELETE

Por último (Figura 18), são lançadas as *threads* de procura no segundo servidor DELSRC e começa a remoção dos valores no primeiro servidor.

A *thread* DELSRC termina quando o último valor a ser removido no primeiro servidor não for encontrado no segundo servidor.

Por fim, é registado o tempo das duas operações DEL e DELSRC no ficheiro, fechando-o.

O *script* em Bash cria os cabeçalhos do ficheiro .csv e tem um ciclo que chama o script em Python 100 vezes.

O resultado final da execução dos scripts de testes é um ficheiro .csv com os seguintes dados por coluna:

- Operação: ADD, ADDSRC, MOD, MODSRC, DEL, DELSRC;
- Teste: o número do teste a ser executado;
- Total_entradas: total de entradas do teste a ser executado;
- Tempo: tempo em formato HH:MM:SS.ms.

As operações ADDSRC, MODSRC e DELSRC representam as operações de pesquisa no segundo servidor, ou seja, as operações ADD, MOD e DEL são realizadas sobre um servidor e sobre o segundo servidor é pesquisado se os valores já foram sincronizados.

Para a realização dos testes de desempenho foram escolhidas as seguintes quantidades de entradas 1000, 10000, 20000, 50000 e 100000, sendo que para estas quantidades foram realizados 100 testes por cada, totalizando 1500 (3 operações * 5 quantidades * 100 testes) testes.

No gráfico abaixo (Figura 19) podem observar-se os tempos obtidos com a realização dos testes para cada uma das operações bem como da sua sincronização:

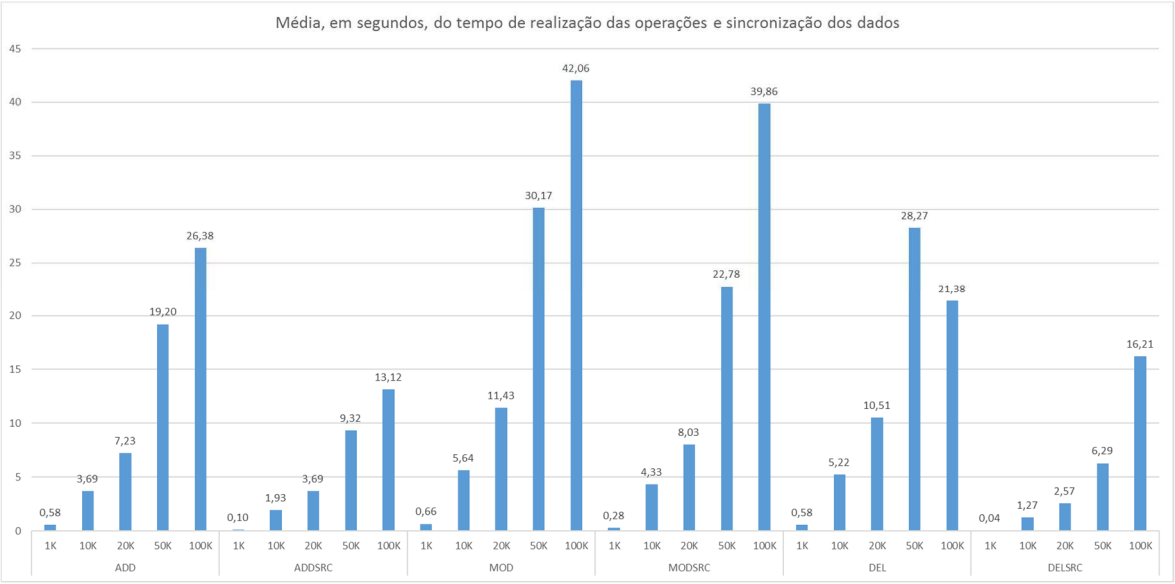

Figura 19 - Tempo de realização de operação e sincronização

Como se pode observar, as operações ADD, MOD e DEL, bem como as pesquisas ADDSRC, MODSRC e DELSRC têm perfis idênticos, sendo que mais entradas demoram mais tempo a ser processadas. A operação DEL com 100000 entradas é a única exceção, possivelmente devido ao facto de os testes terem sido realizados no sistema de virtualização do IPCB, que se encontra em produção com partilha de recursos por diversas máquinas virtuais, o que pode originar estrangulamentos no seu acesso.

Relativamente ao tempo de sincronização entre os servidores, constata-se que as operações de sincronização (ADDSRC, MODSRC e DELSRC) são realizadas em menos tempo do que as operações que lhe dão origem (ADD, MOD e DEL).

Uma vez que o mais importante, do ponto de vista funcional, é o tempo total que demora a realizar as operações, incluindo a sincronização dos dados com o segundo servidor, no gráfico (Figura 20) podem observar-se os tempos totais das operações:

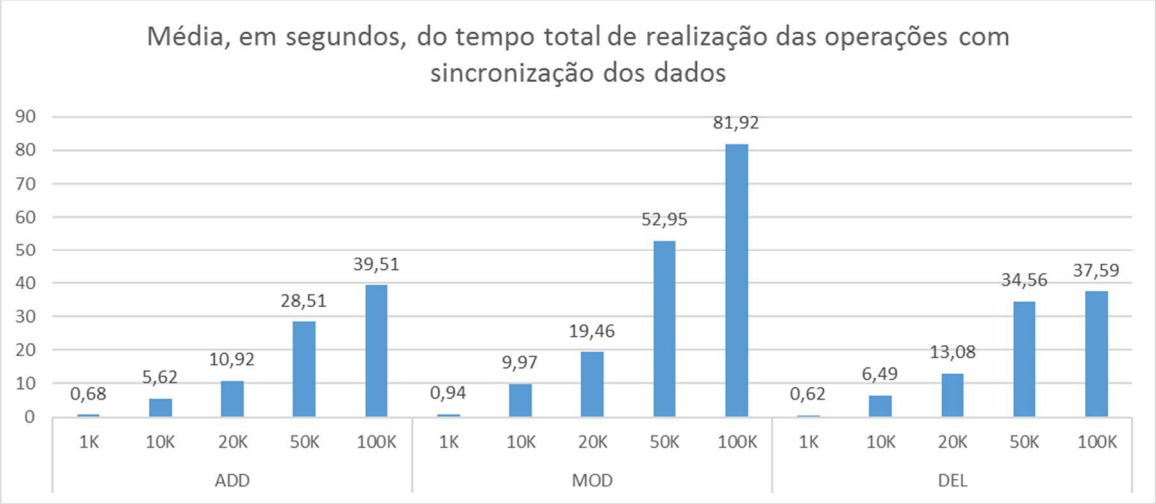

Figura 20 - Tempo total de realização das operações

Podemos verificar que os tempos totais respeitam o mesmo perfil no gráfico de tempos de operação e sincronização, não existindo exceções. Assim, mais uma vez, para mais entradas mais tempo de processamento.

O número de operações por segundo permite uma visão bastante mais clara dos valores de desempenho obtidos com a realização dos testes. Assim, temos os mesmos dados, mas de uma perspetiva diferente, como se pode ver no gráfico (Figura 21):

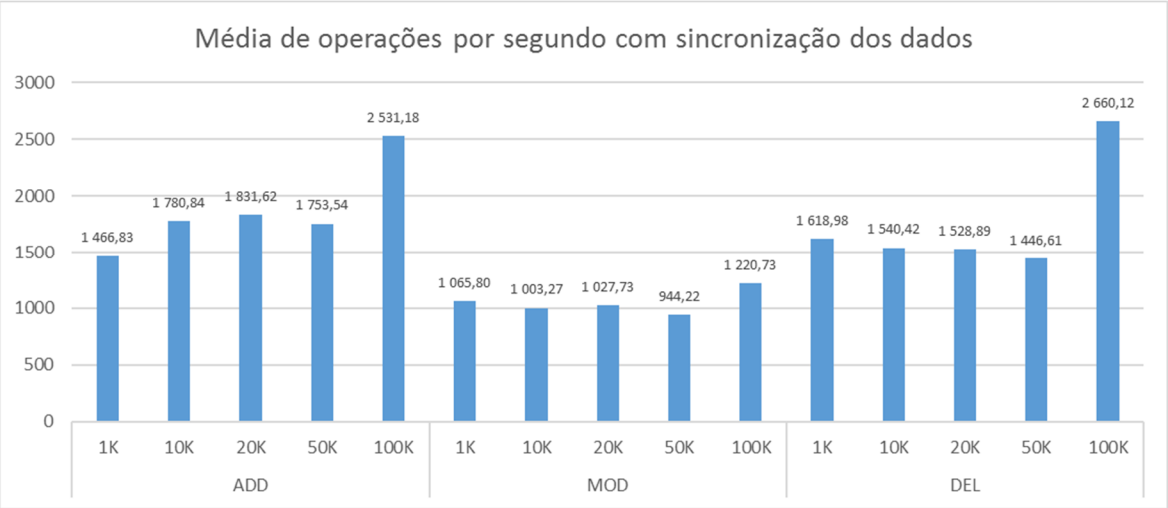

Figura 21 - Operações realizadas por segundo

Observando os dados, conclui-se que a configuração apresentada permite em média realizar 1873 operações ADD por segundo, 1052 operações MOD por segundo e 1759 operações DEL por segundo. Podemos concluir que dada a dimensão de utilizadores do IPCB, aproximadamente 4000 alunos e 520 funcionários, o sistema apresenta um desempenho muito acima do necessário para o correto funcionamento dos serviços que dele dependem.

4.3 Testes de disponibilidade

Com estes testes pretende-se verificar, se em caso de falha de um dos servidores, os clientes continuam a realizar as operações sobre o cluster, garantindo assim a alta disponibilidade pretendida na solução apresentada.

É importante clarificar que a disponibilidade do sistema não é garantida após concluído o processo de ligação (*bind*) a um servidor, ou seja, depois de estar ligado num servidor e este falhar - essa sessão será perdida. Isto acontece porque o OpenLDAP não sincroniza a informação da sessão, apenas os dados do diretório. No entanto, ao ligar-se novamente, terá acesso aos dados no segundo servidor.

No ambiente onde se insere, autenticação de utilizadores, a perda de ligação não representa problema, pois a grande maioria dos serviços que ligam ao diretório estão configurados de forma a fazerem mais do que uma tentativa de ligação ou então a ligarem novamente caso falhe a uma sessão estabelecida.

Para a realização dos testes foi desenvolvido um *script* que simula um serviço cliente que necessita de aceder ao cluster, utilizando a linguagem de programação Python, que realiza uma simples operação de pesquisa. Repetindo a execução deste script, e de forma alternada, desligando os servidores, consegue-se aferir se o sistema garante a alta disponibilidade caso se consiga sempre obter os resultados da pesquisa:

```
#!/usr/bin/python

import sys, ldap, ldif

def main(argv):

  HOSTS = "ldaps://ldap2.si.ipcb.pt:636/ ldaps://ldap1.si.ipcb.pt:636/"
  USER = "cn=Manager,dc=ipcb,dc=pt"
  PASS = "FAKE PASS"

  BASEDN = "ou=People, dc=ipcb, dc=pt"
  SEARCHSCOPE = ldap.SCOPE_SUBTREE
  ATTRIBUTES = ['dn','uid','givenName','sn','cn']
  SEARCHFILTER = "uid=fereis"

  try:

    con = ldap.initialize( HOSTS )
    con.set_option( ldap.OPT_NETWORK_TIMEOUT, 1 )
    con.set_option( ldap.OPT_PROTOCOL_VERSION, ldap.VERSION3 )
    con.simple_bind_s( USER , PASS )

    results = con.search_s( BASEDN , SEARCHSCOPE, SEARCHFILTER, ATTRIBUTES )
    ldif_writer = ldif.LDIFWriter(sys.stdout)

    print "\nRESULTS:\n"
    for dn,entry in results:
      ldif_writer.unparse(dn,entry)

    con.unbind_s()

  except ldap.LDAPError, e:
    print e
    return None

if __name__ == "__main__":
   main(sys.argv[1:])
```

Para obter o resultado pretendido são necessárias algumas configurações específicas por forma a garantir a alta disponibilidade.

Uma vez que ambos os servidores utilizam encriptação SSL/TLS para garantir a segurança da ligação, e esta obriga à utilização de certificados digitais, não é possível implementar protocolos, como o VRRP, para gerar um endereço virtual que redireciona os pedidos para o servidor em funcionamento, sob pena de gerar um erro de certificado. Assim é necessário configurar os dois servidores do cluster na linha que indica a que servidores será efetuada a ligação:

```
HOSTS = "ldaps://ldap2.si.ipcb.pt:636/ ldaps://ldap1.si.ipcb.pt:636/"
```

É também necessário configurar o tempo de espera (*timeout*) de rede para que, caso o primeiro servidor da lista falhe se tente o mais rapidamente possível ligar ao segundo servidor:

```
con.set_option( ldap.OPT_NETWORK_TIMEOUT, 1 )
```

A configuração do tempo de espera de rede pode necessitar de ajuste caso o cluster esteja muito sobrecarregado com pedidos.

Para comprovar a que servidor o script se ligou em cada um dos testes foi utilizado o comando tcpdump (Tcpdump/Libpcap, 2017) que permite ver, em tempo real, o tráfego em trânsito na interface de rede do servidor.

O primeiro teste foi realizado com os dois servidores em funcionamento configurados pela ordem ldap1.si.ipcb.pt, ldap2.si.ipcb.pt:

```
    22:01:22.181398 IP ldap-tests.si.ipcb.pt.48340 > ldap1.si.ipcb.pt.ldaps: Flags [S], seq
3723471897, win 29200, options [mss 1460,sackOK,TS val 79161193 ecr 0,nop,wscale 7], length
0
    22:01:22.181606 IP ldap1.si.ipcb.pt.ldaps > ldap-tests.si.ipcb.pt.48340: Flags [S.], seq
1780889595, ack 3723471898, win 28960, options [mss 1460,sackOK,TS val 12241000 ecr
79161193,nop,wscale 7], length 0
    22:01:22.181656 IP ldap-tests.si.ipcb.pt.48340 > ldap1.si.ipcb.pt.ldaps: Flags [.], ack
1, win 229, options [nop,nop,TS val 79161193 ecr 12241000], length 0
    22:01:22.383164 IP ldap-tests.si.ipcb.pt.48340 > ldap1.si.ipcb.pt.ldaps: Flags [P.], seq
1:156, ack 1, win 229, options [nop,nop,TS val 79161395 ecr 12241000], length 155
    22:01:22.383318 IP ldap1.si.ipcb.pt.ldaps > ldap-tests.si.ipcb.pt.48340: Flags [.], ack
156, win 235, options [nop,nop,TS val 12241202 ecr 79161395], length 0
    22:01:22.386994 IP ldap1.si.ipcb.pt.ldaps > ldap-tests.si.ipcb.pt.48340: Flags [P.], seq
1:3111, ack 156, win 235, options [nop,nop,TS val 12241206 ecr 79161395], length 3110
    22:01:22.387036 IP ldap-tests.si.ipcb.pt.48340 > ldap1.si.ipcb.pt.ldaps: Flags [.], ack
3111, win 277, options [nop,nop,TS val 79161399 ecr 12241206], length 0
    22:01:22.392621 IP ldap-tests.si.ipcb.pt.48340 > ldap1.si.ipcb.pt.ldaps: Flags [P.], seq
156:282, ack 3111, win 277, options [nop,nop,TS val 79161404 ecr 12241206], length 126
    22:01:22.394488 IP ldap1.si.ipcb.pt.ldaps > ldap-tests.si.ipcb.pt.48340: Flags [P.], seq
3111:3162, ack 282, win 235, options [nop,nop,TS val 12241213 ecr 79161404], length 51
    22:01:22.394666 IP ldap-tests.si.ipcb.pt.48340 > ldap1.si.ipcb.pt.ldaps: Flags [P.], seq
282:359, ack 3162, win 277, options [nop,nop,TS val 79161406 ecr 12241213], length 77
    22:01:22.394911 IP ldap1.si.ipcb.pt.ldaps > ldap-tests.si.ipcb.pt.48340: Flags [P.], seq
3162:3205, ack 359, win 235, options [nop,nop,TS val 12241214 ecr 79161406], length 43
    22:01:22.395067 IP ldap-tests.si.ipcb.pt.48340 > ldap1.si.ipcb.pt.ldaps: Flags [P.], seq
359:482, ack 3205, win 277, options [nop,nop,TS val 79161407 ecr 12241214], length 123
    22:01:22.395348 IP ldap1.si.ipcb.pt.ldaps > ldap-tests.si.ipcb.pt.48340: Flags [P.], seq
3205:3376, ack 482, win 235, options [nop,nop,TS val 12241214 ecr 79161407], length 171
    22:01:22.395382 IP ldap1.si.ipcb.pt.ldaps > ldap-tests.si.ipcb.pt.48340: Flags [P.], seq
3376:3419, ack 482, win 235, options [nop,nop,TS val 12241214 ecr 79161407], length 43
    22:01:22.395456 IP ldap-tests.si.ipcb.pt.48340 > ldap1.si.ipcb.pt.ldaps: Flags [.], ack
3419, win 326, options [nop,nop,TS val 79161407 ecr 12241214], length 0
    22:01:22.395719 IP ldap-tests.si.ipcb.pt.48340 > ldap1.si.ipcb.pt.ldaps: Flags [P.], seq
482:518, ack 3419, win 326, options [nop,nop,TS val 79161407 ecr 12241214], length 36
    22:01:22.395762 IP ldap-tests.si.ipcb.pt.48340 > ldap1.si.ipcb.pt.ldaps: Flags [FP.], seq
518:549, ack 3419, win 326, options [nop,nop,TS val 79161407 ecr 12241214], length 31
    22:01:22.395904 IP ldap1.si.ipcb.pt.ldaps > ldap-tests.si.ipcb.pt.48340: Flags [.], ack
550, win 235, options [nop,nop,TS val 12241215 ecr 79161407], length 0
    22:01:22.395940 IP ldap1.si.ipcb.pt.ldaps > ldap-tests.si.ipcb.pt.48340: Flags [F.], seq
3419, ack 550, win 235, options [nop,nop,TS val 12241215 ecr 79161407], length 0
    22:01:22.395964 IP ldap-tests.si.ipcb.pt.48340 > ldap1.si.ipcb.pt.ldaps: Flags [.], ack
3420, win 326, options [nop,nop,TS val 79161408 ecr 12241215], length 0
```

Como se pode observar, o script, em execução no servidor ldap-tests.si.ipcb.pt, não contacta o servidor ldap2.si.ipcb.pt, pois consegue ligar-se logo no primeiro servidor pelo que não tem de tentar o segundo.

No segundo teste, a ordem foi invertida, ficando ldap2.si.ipcb.pt, ldap1.si.ipcb.pt:

```
22:02:09.092048 IP ldap-tests.si.ipcb.pt.49676 > ldap2.si.ipcb.pt.ldaps: Flags [S], seq
4150947303, win 29200, options [mss 1460,sackOK,TS val 79208104 ecr 0,nop,wscale 7], length
0
```

```
22:02:09.092295 IP ldap2.si.ipcb.pt.ldaps > ldap-tests.si.ipcb.pt.49676: Flags [S.], seq
440208922, ack 4150947304, win 28960, options [mss 1460,sackOK,TS val 78519298 ecr
79208104,nop,wscale 7], length 0
22:02:09.092333 IP ldap-tests.si.ipcb.pt.49676 > ldap2.si.ipcb.pt.ldaps: Flags [.], ack 1,
win 229, options [nop,nop,TS val 79208104 ecr 78519298], length 0
22:02:09.318574 IP ldap-tests.si.ipcb.pt.49676 > ldap2.si.ipcb.pt.ldaps: Flags [P.], seq
1:156, ack 1, win 229, options [nop,nop,TS val 79208330 ecr 78519298], length 155
22:02:09.318769 IP ldap2.si.ipcb.pt.ldaps > ldap-tests.si.ipcb.pt.49676: Flags [.], ack 156,
win 235, options [nop,nop,TS val 78519524 ecr 79208330], length 0
22:02:09.322679 IP ldap2.si.ipcb.pt.ldaps > ldap-tests.si.ipcb.pt.49676: Flags [P.], seq
1:3111, ack 156, win 235, options [nop,nop,TS val 78519528 ecr 79208330], length 3110
22:02:09.322751 IP ldap-tests.si.ipcb.pt.49676 > ldap2.si.ipcb.pt.ldaps: Flags [.], ack 3111,
win 277, options [nop,nop,TS val 79208334 ecr 78519528], length 0
22:02:09.331011 IP ldap-tests.si.ipcb.pt.49676 > ldap2.si.ipcb.pt.ldaps: Flags [P.], seq
156:282, ack 3111, win 277, options [nop,nop,TS val 79208343 ecr 78519528], length 126
22:02:09.333373 IP ldap2.si.ipcb.pt.ldaps > ldap-tests.si.ipcb.pt.49676: Flags [P.], seq
3111:3162, ack 282, win 235, options [nop,nop,TS val 78519539 ecr 79208343], length 51
22:02:09.333654 IP ldap-tests.si.ipcb.pt.49676 > ldap2.si.ipcb.pt.ldaps: Flags [P.], seq
282:359, ack 3162, win 277, options [nop,nop,TS val 79208345 ecr 78519539], length 77
22:02:09.333990 IP ldap2.si.ipcb.pt.ldaps > ldap-tests.si.ipcb.pt.49676: Flags [P.], seq
3162:3205, ack 359, win 235, options [nop,nop,TS val 78519540 ecr 79208345], length 43
22:02:09.334174 IP ldap-tests.si.ipcb.pt.49676 > ldap2.si.ipcb.pt.ldaps: Flags [P.], seq
359:482, ack 3205, win 277, options [nop,nop,TS val 79208346 ecr 78519540], length 123
22:02:09.334564 IP ldap2.si.ipcb.pt.ldaps > ldap-tests.si.ipcb.pt.49676: Flags [P.], seq
3205:3376, ack 482, win 235, options [nop,nop,TS val 78519540 ecr 79208346], length 171
22:02:09.334601 IP ldap2.si.ipcb.pt.ldaps > ldap-tests.si.ipcb.pt.49676: Flags [P.], seq
3376:3419, ack 482, win 235, options [nop,nop,TS val 78519540 ecr 79208346], length 43
22:02:09.334656 IP ldap-tests.si.ipcb.pt.49676 > ldap2.si.ipcb.pt.ldaps: Flags [.], ack 3419,
win 326, options [nop,nop,TS val 79208346 ecr 78519540], length 0
22:02:09.335005 IP ldap-tests.si.ipcb.pt.49676 > ldap2.si.ipcb.pt.ldaps: Flags [P.], seq
482:518, ack 3419, win 326, options [nop,nop,TS val 79208347 ecr 78519540], length 36
22:02:09.335057 IP ldap-tests.si.ipcb.pt.49676 > ldap2.si.ipcb.pt.ldaps: Flags [P.], seq
518:549, ack 3419, win 326, options [nop,nop,TS val 79208347 ecr 78519540], length 31
22:02:09.335088 IP ldap-tests.si.ipcb.pt.49676 > ldap2.si.ipcb.pt.ldaps: Flags [F.], seq 549,
ack 3419, win 326, options [nop,nop,TS val 79208347 ecr 78519540], length 0
22:02:09.335267 IP ldap2.si.ipcb.pt.ldaps > ldap-tests.si.ipcb.pt.49676: Flags [.], ack 549,
win 235, options [nop,nop,TS val 78519541 ecr 79208347], length 0
22:02:09.335376 IP ldap2.si.ipcb.pt.ldaps > ldap-tests.si.ipcb.pt.49676: Flags [F.], seq
3419, ack 550, win 235, options [nop,nop,TS val 78519541 ecr 79208347], length 0
22:02:09.335411 IP ldap-tests.si.ipcb.pt.49676 > ldap2.si.ipcb.pt.ldaps: Flags [.], ack 3420,
win 326, options [nop,nop,TS val 79208347 ecr 78519541], length 0
```

Podemos observar novamente, que o script se ligou no primeiro servidor (ldap2.si.ipcb.pt) ignorando completamente o segundo servidor (ldap1.si.ipcb.pt).

Por fim, desligamos o primeiro servidor da lista ldap2.si.ipcb.pt, ldap1.si.ipcb.pt e observamos o comportamento do script:

```
    22:03:18.744944 IP ldap-tests.si.ipcb.pt.49678 > ldap2.si.ipcb.pt.ldaps: Flags [S], seq
3984996379, win 29200, options [mss 1460,sackOK,TS val 79277757 ecr 0,nop,wscale 7], length
0
    22:03:19.748025 IP ldap-tests.si.ipcb.pt.48346 > ldap1.si.ipcb.pt.ldaps: Flags [S], seq
789746256, win 29200, options [mss 1460,sackOK,TS val 79278760 ecr 0,nop,wscale 7], length 0
    22:03:19.748246 IP ldap1.si.ipcb.pt.ldaps > ldap-tests.si.ipcb.pt.48346: Flags [S.], seq
1277160684, ack 789746257, win 28960, options [mss 1460,sackOK,TS val 12358567 ecr
79278760,nop,wscale 7], length 0
    22:03:19.748289 IP ldap-tests.si.ipcb.pt.48346 > ldap1.si.ipcb.pt.ldaps: Flags [.], ack
1, win 229, options [nop,nop,TS val 79278760 ecr 12358567], length 0
    22:03:19.980426 IP ldap-tests.si.ipcb.pt.48346 > ldap1.si.ipcb.pt.ldaps: Flags [P.], seq
1:156, ack 1, win 229, options [nop,nop,TS val 79278992 ecr 12358567], length 155
    22:03:19.980635 IP ldap1.si.ipcb.pt.ldaps > ldap-tests.si.ipcb.pt.48346: Flags [.], ack
156, win 235, options [nop,nop,TS val 12358799 ecr 79278992], length 0
    22:03:19.984404 IP ldap1.si.ipcb.pt.ldaps > ldap-tests.si.ipcb.pt.48346: Flags [P.], seq
1:3111, ack 156, win 235, options [nop,nop,TS val 12358803 ecr 79278992], length 3110
```

```
    22:03:19.984449 IP ldap-tests.si.ipcb.pt.48346 > ldap1.si.ipcb.pt.ldaps: Flags [.], ack
3111, win 277, options [nop,nop,TS val 79278996 ecr 12358803], length 0
    22:03:19.992773 IP ldap-tests.si.ipcb.pt.48346 > ldap1.si.ipcb.pt.ldaps: Flags [P.], seq
156:282, ack 3111, win 277, options [nop,nop,TS val 79279004 ecr 12358803], length 126
    22:03:19.994618 IP ldap1.si.ipcb.pt.ldaps > ldap-tests.si.ipcb.pt.48346: Flags [P.], seq
3111:3162, ack 282, win 235, options [nop,nop,TS val 12358813 ecr 79279004], length 51
    22:03:19.994847 IP ldap-tests.si.ipcb.pt.48346 > ldap1.si.ipcb.pt.ldaps: Flags [P.], seq
282:359, ack 3162, win 277, options [nop,nop,TS val 79279006 ecr 12358813], length 77
    22:03:19.995090 IP ldap1.si.ipcb.pt.ldaps > ldap-tests.si.ipcb.pt.48346: Flags [P.], seq
3162:3205, ack 359, win 235, options [nop,nop,TS val 12358814 ecr 79279006], length 43
    22:03:19.995299 IP ldap-tests.si.ipcb.pt.48346 > ldap1.si.ipcb.pt.ldaps: Flags [P.], seq
359:482, ack 3205, win 277, options [nop,nop,TS val 79279007 ecr 12358814], length 123
    22:03:19.995590 IP ldap1.si.ipcb.pt.ldaps > ldap-tests.si.ipcb.pt.48346: Flags [P.], seq
3205:3376, ack 482, win 235, options [nop,nop,TS val 12358814 ecr 79279007], length 171
    22:03:19.995614 IP ldap1.si.ipcb.pt.ldaps > ldap-tests.si.ipcb.pt.48346: Flags [P.], seq
3376:3419, ack 482, win 235, options [nop,nop,TS val 12358814 ecr 79279007], length 43
    22:03:19.995693 IP ldap-tests.si.ipcb.pt.48346 > ldap1.si.ipcb.pt.ldaps: Flags [.], ack
3419, win 326, options [nop,nop,TS val 79279007 ecr 12358814], length 0
    22:03:19.996043 IP ldap-tests.si.ipcb.pt.48346 > ldap1.si.ipcb.pt.ldaps: Flags [P.], seq
482:518, ack 3419, win 326, options [nop,nop,TS val 79279008 ecr 12358814], length 36
    22:03:19.996101 IP ldap-tests.si.ipcb.pt.48346 > ldap1.si.ipcb.pt.ldaps: Flags [FP.], seq
518:549, ack 3419, win 326, options [nop,nop,TS val 79279008 ecr 12358814], length 31
    22:03:19.996198 IP ldap1.si.ipcb.pt.ldaps > ldap-tests.si.ipcb.pt.48346: Flags [.], ack
550, win 235, options [nop,nop,TS val 12358815 ecr 79279008], length 0
    22:03:19.996248 IP ldap1.si.ipcb.pt.ldaps > ldap-tests.si.ipcb.pt.48346: Flags [F.], seq
3419, ack 550, win 235, options [nop,nop,TS val 12358815 ecr 79279008], length 0
    22:03:19.996274 IP ldap-tests.si.ipcb.pt.48346 > ldap1.si.ipcb.pt.ldaps: Flags [.], ack
3420, win 326, options [nop,nop,TS val 79279008 ecr 12358815], length 0
```

Podemos observar, a negrito, que ocorreu uma tentativa de ligação ao primeiro servidor (ldap2.si.ipcb.pt), mas como não houve resposta passado um segundo, como fora configurado no tempo de espera da rede, o script ligou-se no segundo servidor (ldap2.si.ipcb.pt), garantindo a alta disponibilidade, como proposto.

O resultado do script em todos os testes foi sempre o mesmo, sendo que no último teste, demorou mais um segundo do que nos restantes testes:

```
RESULTS:

dn: uid=fereis,ou=People,dc=ipcb,dc=pt
cn: Fernando Emanuel Azevedo Reis
givenName: Fernando
sn: Reis
uid: fereis
```

Através dos testes realizados, podemos concluir que a solução proposta é uma solução de alta disponibilidade, pois a execução do script retornou sempre os resultados esperados mesmo com a falha de um dos servidores.

4.4 Síntese

O presente capítulo compreende a realização de testes de desempenho e disponibilidade à solução apresentada, nomeadamente a capacidade para responder

ao caso específico do IPCB. Os testes foram realizados em sistemas em produção no IPCB para que os resultados obtidos sejam os mais próximos possíveis da realidade.

Foram apresentados os diagramas de atividade *Unified Modeling Language* (UML) dos scripts desenvolvidos bem como a sua explicação.

Relativamente ao desempenho da solução proposta, foram apresentados os resultados dos testes realizados através de gráficos, que mostram que o sistema proposto cumpre os requisitos de desempenho.

Por fim foram realizados os testes de disponibilidade que confirmam que a solução proposta permite garantir a disponibilidade do serviço mesmo em caso de falha de um dos servidores.

CAPÍTULO 5 - CONCLUSÕES E TRABALHO FUTURO

5.1 Conclusões

Tendo em conta os resultados obtidos, conclui-se que é possível implementar um sistema de armazenamento de credenciais, com tecnologia *open-source*, muito robusto, com tolerância a falhas e com elevada capacidade de resposta.

Através do registo de OID na IANA, é possível implementar interoperabilidade entre diretórios LDAP de diferentes organizações. Apesar de não existir esta necessidade, a solução apresentada está preparada para a implementar, pois todos os atributos e *objectclasses* têm um OID único no mundo que pertence ao IPCB.

Relativamente aos atributos e *objectclasses* criados e a sua relação com a informação a armazenar, conclui-se que apresentam um elevado nível de modularidade, exatamente o que se pretendia, permitindo adicionar ou remover informação relativa aos serviços durante todo o ciclo de vida das credenciais.

O tipo de sincronização utilizada entre os dois servidores LDAP, *multi-master*, oferece as garantias de disponibilidade necessárias a uma solução deste tipo, garantindo a distribuição dos dados das credenciais por todos os servidores de uma forma robusta e rápida. A utilização de pesquisas idênticas às utilizadas pelos clientes no processo de sincronização demonstra a simplicidade e robustez da solução.

Relativamente ao desempenho da solução apresentada, a mesma apresenta valores muito acima do necessário para uma instituição com a dimensão do IPCB. O número de operações por segundo apresentado, superior a 1000 em qualquer uma das operações, permite um funcionamento com desempenhos muito acima do necessário, o que garante os tempos de resposta durante a longa duração que esta solução necessita de estar em funcionamento.

Por fim, com os testes de disponibilidade, ficou comprovado que a solução proposta oferece garantias de alta disponibilidade, ficando este requisito base preenchido.

5.2 Trabalho futuro

O desenvolvimento da solução proposta neste documento tem por base a realidade do IPCB, pelo que a sua implementação e início de funcionamento em ambiente de produção é muito importante por forma a garantir o armazenamento robusto das credenciais dos seus utilizadores, bem como desempenho no acesso às mesmas.

Tendo em conta que uma instituição de ensino superior está em constante mutação, quer com a adesão a novos projetos ou pela implementação de novos serviços, utilizando como base o modelo PDCA (Figura 22), fazer modificações na solução

proposta será uma constante, pelo que a utilização do modelo irá permitir a melhoria contínua do sistema.

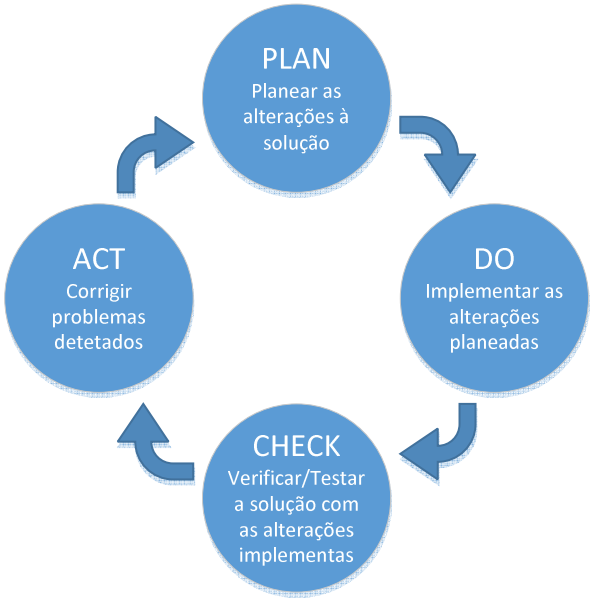

Figura 22 - Ciclo PDCA

A criação de novas *objectclasses*/atributos pertence à fase de (PLAN) do modelo. Já a sua instalação, bem como a adequação das entradas existentes às novas *objectclasses*/atributos, quer pela simples adição dos mesmos, com a respetiva informação, a cada entrada ou pela alteração de *objectclasses*/atributos existentes pertence à fase de (DO). A verificação da adequabilidade das novas *objectclasses*/atributos ao que se pretende pertence à fase (CHECK), e por último a correção de anomalias pertence à fase (ACT).

BIBLIOGRAFIA

Boston University Information Services & Technology, 2016. Understanding Authentication, Authorization, and Encryption. [online]. Available at: <https://www.bu.edu/tech/about/security-resources/bestpractice/auth/> [Accessed 15 Dec. 2016].

Buecker, A., Filip, W., Hinton, H., Hippenstiel, H.P., Hollin, M., Neucom, R., Weeden, S. and Westman, J., 2005. Federated Identity Management and Web Services Security with IBM Tivoli Security Solutions. 2rd ed. IBM.

Butcher, M., 2007. Mastering OpenLDAP. Birmingham: Packt Publishing Ltd.

Choi, J.H., Franke, H., Box, P.O., Heights, Y. and Zeilenga, K., 2003. Enhancing the Performance of OpenLDAP Directory Server with Multiple Caching. [online] Available at: <http://www.openldap.org/pub/jchoi/backbdb-perf.pdf> [Acessed 2 Jun. 2016].

Chu, H., 2011. MDB: A Memory-Mapped Database and Backend for OpenLDAP. [online] Available at: <https://www.openldap.org/pub/hyc/mdm-paper.pdf> [Acessed 2 Jun. 2016].

Digitalis, 2016. Portfolio. [online] Available at: <http://www.digitalis.pt/#sp-portfolio-wrapper> [Acessed 30 Jan. 2017].

Dropbox, n.d. What is Dropbox?. [online] Available at: <https://www.dropbox.com/help/6642> [Acessed 2 Feb. 2017].

ForgeRock, 2017. OpenDJ – Directory Services. [online] Available at: <https://forgerock.org/opendj/> [Acessed 23 Jan. 2017].

IBM, 2016. IBM Security Directory Suite. [online] <http://www-03.ibm.com/software/products/pt/ibm-security-directory-suite> [Acessed 3 Feb. 2017].

Internet2, 2017. Shibboleth | Internet2. [online] Available at: <http://www.internet2.edu/products-services/trust-identity/shibboleth/> [Acessed 30 Jan. 2017].

IPCB, 2016. Serviços Online. [online] Available at: <http://www.ipcb.pt/ipcb/serviços-online> [Acessed 30 Jan. 2017].

Kaufman, C., 1993. Distributed Authentication Security Service. IETF RFC 1507. Available at: <https://tools.ietf.org/html/rfc1507>.

Micro Focus, 2017. NetIQ eDirectory. [online] Available at: <https://www.netiq.com/products/edirectory/> [Acessed 3 Feb. 2017].

Microsoft, 2016. Active Directory. [online] Available at: <https://msdn.microsoft.com/en-us/library/bb742424.aspx> [Acessed 25 Jan. 2017].

Microsoft, 2016a. What is Azure Active Directory?. [online] Available at: <https://docs.microsoft.com/en-us/azure/active-directory/active-directory-whatis> [Acessed 20 Feb. 2016].

Microsoft, 2017. Microsoft Shell. [online] Available at: <https://msdn.microsoft.com/en-us/powershell/mt173057.aspx> [Acessed 30 Jan. 2017].

MIT, 2016. Kerberos: The Network Authentication Protocol. [online] Available at: <https://web.mit.edu/kerberos/> [Acessed 2 Feb. 2017].

OpenLDAP Foundation, 2017. OpenLDAP Software. [online] Available at: <https://www.openldap.org/software/> [Acessed 20 Feb. 2016].

Oracle, 2016. Oracle Berkeley DB 12c. [online] Available at: <http://www.oracle.com/technetwork/database/database-technologies/berkeleydb/overview/index.html> [Acessed 2 Feb. 2017].

Oracle, n.d. Oracle Unified Directory. [online] <http://www.oracle.com/technetwork/middleware/id-mgmt/overview/oud-433568.html> [Acessed 2 Feb. 2017].

OSC, 2017. Radiator RADIUS Server. [online] Available at: <http://www.open.com.au/radiator/> [Acessed 31 Jan. 2017].

Paul, I., 2013. Office 2013 vs. Office 365: Should you buy or rent?. PCWorld. [online] Available at: <http://www.pcworld.com/article/2026703/office-365-vs-office-2013-should-you-rent-or-own-.html> [Acessed 31 Jan. 2017].

Red Hat, Inc., 2017. 389 Directory Server. [online] Available at: <http://directory.fedoraproject.org/> [Acessed 23 Jan. 2017].

Stallings, W., 2007. Understanding federated identity. [online] Network World. Available at: <http://www.networkworld.com/article/2285444/tech-primers/understanding-federated-identity.html> [Accessed 22 Dec. 2016].

Tcpdump/Libpcap, 2017. TCPDUMP/LIBPCAP public repository. [online] Available at: <http://www.tcpdump.org/> [Acessed 2 Fev. 2017].

The Apache Software Foundation, 2016. Apache Directory. [online] Available at: <http://directory.apache.org/apacheds/> [Acessed 20 Jan. 2017].

The OpenLDAP Project, 2016. OpenLDAP Software 2.4 Administrator's Guide. [pdf] The OpenLDAP Project. Available at: <https://www.openldap.org/doc/admin24/OpenLDAP-Admin-Guide.pdf> [Acessed 20 Feb. 2016].

UNINETT, 2016. SimpleSAMLphp. [online] Available at: <https://simplesamlphp.org/> [Acessed 30 Jan. 2017].

Wahl, M., Howes, T. and Kille, S., 1997. Lightweight Directory Access Protocol (v3). IETF RFC 2251. Available at: <http://www.ietf.org/rfc/rfc2251.txt>.

Wang, Z., Wang, Y., 2012. Research and Design of Campus Network Unified Identity Authentication System Based on Kerberos. *Advanced Materials Research*, [online] 546–547, pp.1086–1089. Available at: <http://www.scientific.net/AMR.546-547.1086>.

Zeilenga, K. and Choi, J.H., 2006. The Lightweight Directory Access Protocol (LDAP) Content Synchronization Operation. IETF RFC 4533. Available at: <https://www.ietf.org/rfc/rfc4533.txt>.

ZYTRAX, Inc., 2016. Chapter 2 LDAP Concepts & Overview. [online] Available at: <http://www.zytrax.com/books/ldap/ch2/> [Acessed 20 Feb. 2016].

ZYTRAX, Inc., 2016a. Chapter 7 Replication & Referral. [online] Available at: <http://www.zytrax.com/books/ldap/ch7/> [Acessed 20 Feb. 2016].

ZYTRAX, Inc., 2016b. Chapter 15 LDAP Security. [online] Available at: <http://www.zytrax.com/books/ldap/ch15/> [Acessed 20 Feb. 2016].