



Serviço de Directoria para a Universidade do Minho

Índice

- 1- [Enquadramento](#)
- 2- [Objectivos](#)
- 3- [Princípios](#)
- 4- [Serviços de Directoria Comerciais Existentes no Mercado](#)
- 5- [X.500 Directory Access Protocol \(DAP\)](#)
- 6- [Limitações do X.500](#)
- 7- [LDAP \(Lightweight Directory Access Protocol\)](#)

1. Enquadramento

O ambiente ao nível das TIC na Universidade do Minho é tecnologicamente variado e suportado por vários grupos em diferentes Unidades Orgânicas usando uma variedade de ferramentas para efectuar a gestão e permitir o acesso aos conteúdos que são disponibilizadas para todos os utilizadores, alunos, funcionários docentes e não docentes. Até ao momento esta estratégia funcionou, embora existisse a nítida sensação de que seria necessário disponibilizar um Serviço de Único de Directoria capaz de efectuar a autenticação de forma centralizada de todos aqueles que utilizam as diferentes plataformas.

Actualmente proliferam Serviços de Directoria, sem qualquer mais valia para a Instituição e para todos aqueles que usam e partilham recursos comuns. Acresce o facto de que a simples manutenção e suporte a estes serviços, tem custos elevadíssimos, com o senão acrescido de fornecer informação que muitas vezes está desactualizada ou puramente incorrecta, pois a informação é redundante e nem sempre se encontra actualizada em relação aos repositórios centrais.

Com a entrada em funcionamento do projecto Campus Virtual, e com a disponibilização de novos conteúdos e a necessidade de disponibilizar estes conteúdos em qualquer local dos Campi de forma segura, a necessidade de se adoptar um Serviço de Directoria capaz de fornecer a infra-estrutura de suporte à identidade controlando o acesso e autenticação, fornecendo conteúdos personalizados e um conjunto de outros aspectos de gestão do relacionamento entre as fontes de informação e os utilizadores que as usam tornou-se essencial. Sendo um repositório central de informação organizacional, onde a se disponibiliza uma única vista lógica dos utilizadores, recursos e de outros objectos que compõem um sistema mais amplo e distribuído. Este Serviço de Directoria permitirá aos

utilizadores e aplicações acederem aos recursos existentes de forma transparente. Este serviço é estruturante e indispensável na gestão diária dos processos administrativos e de apoio ao ensino, na Universidade do Minho.



2. Objectivos

Os objectivos que se consideram ser necessários para se concretizar o Serviço de Directoria são os seguintes:

- Criar um Serviço de Directoria Único para a Universidade do Minho, que facilite a identificação e a autenticação dos utilizadores e que fazendo a sua gestão e controlo no acesso aos recursos disponibilizados numa forma unificada e eficiente.
- Permitir a partilha livre de recursos entre os diferentes utilizadores, sejam eles alunos, funcionários docentes ou não docentes e convidados externos da Universidade de uma forma personalizada.
- Criar um serviço com um desenho simples e flexível que permitirá minimizar o suporte e a administração necessários. O ideal seria que as necessidades ao nível administrativo (pessoal técnico necessário) não aumentem para fazer frente ao esperado aumento de necessidades ao nível da gestão da identificação de utilizadores e recursos computacionais.
- Manter a o nível actual de controlo descentralizado de software e hardware ao nível das diferentes Unidades Orgânicas.
- Garantir que o tempo necessário para se criar um perfil de utilizador e dar-lhe acesso aos recursos que necessita e que pode aceder é maior ou igual ao tempo que se irá gastar com o Serviço de Directoria implementado, ou seja a implementação deste serviço não pode causar atrasos nos processos actuais.
- Fornecer e requerer diversos níveis de segurança.
- Utilizar soluções comerciais standard na implementação, se possível com aplicações práticas e funcionais em organizações similares, tendo em consideração as boas práticas e experiências adquiridas por essas organizações.



3. Princípios

O Serviço de Directoria a criar na Universidade do Minho deve ter em conta os seguintes princípios:

- **Deve ser Escalável:** Que tamanho terá? Qual será o grau de escalabilidade necessário para o Serviço de Directoria, de forma que corresponda às necessidades actuais mas também a necessidades futuras? Funcionará este Serviço da forma desejada quando as necessidades de identificação crescerem exponencialmente?
- **Deve ser Compatível:** Funcionará este serviço com as aplicações actuais? Suportará serviços de acesso a directorias standard? Funcionará nas nossas plataformas preferidas?

- **Deve estar Sempre Disponível:** Que mecanismos asseguraram que este serviço estará constantemente disponível? Será que atingirá os nossos objectivos de disponibilidade? É à prova de erros de serviço ou à corrupção de dados? Possui mecanismos de recuperação em caso de desastre?
- **Deve ser Manuseável:** Que ferramentas e serviços possui para efectuar a gestão pro-activa e monitorização do sistema? É capaz de se conectar de forma transparente às consolas de gestão de rede? Será que as ferramentas de gestão se adaptam às necessidades da Organização?
- **Deve ser Seguro:** Será que o sistema permite dar o acesso privilegiado a utilizadores enquanto nega redundantemente o acesso a intrusos com fins maliciosos? O sistema possuirá meios para garantir a total privacidade e confidencialidade dos dados armazenados?

Ao possuir estas 5 características, tendo no entanto em atenção que algumas das características indicadas poderão ter um pesos diferentes, teremos a garantia que o Serviço de Directoria seleccionado para ser implementado, terá as características necessárias para fazer frente às necessidades presentes e futuras da Universidade do Minho.



4. Serviços de Directoria Comerciais Existentes no Mercado

Existem diversos Serviços de Directoria no mercado, alguns dos quais com experiências muito bem sucedidas em Universidades, quer na Europa(Oxford University, University of Leicester, University of York) quer nos Estados Unidos(Colorado University, Iowa University, Wayne State University, University of Hawaii, MIT, University of Michigan, University of Yale). Destacam-se cinco fornecedores de Serviços de Directoria:

Comerciais:

Microsoft – Active Directory
 Sun – Sun One (Open Net Environment) Directory Server
 Sun – iPlanet Directory Server
 Novell – eDirectory
 Isode – M-Vault
 Netscape Directory Server

Open-Source:

OpenLdap
 Connexitor Directory Services
 Directory Administrator

Existem estudos no mercado efectuados por empresas (pelas próprias e por empresas supostamente independentes) que garantem que determinado produto é superior ao outro, no entanto, parece ser mais importante, a análise detalhada de cada uma das opções disponíveis, e se a solução a adoptar responde na totalidade ou não às necessidades que foram anteriormente identificadas.

Ao nível do ensino, encontraram-se diversas instalações, quer no Reino-Unido quer nos Estados Unidos, com produtos acima citados. Três das razões invocadas, e que levaram (em ambos os casos) pela adopção de um produto em detrimento do outro foram:

- Tipo de parque informático instalado – Qual é a predominância de tecnologia (Microsoft, Sun ou Linux). São levantadas questões de interoperabilidade, pois normalmente os meios universitários são dados a grande heterogeneidade ao nível do equipamento informático e sistemas operativos em uso, não perdendo no entanto o foco principal da questão, que é, ter de servir o máximo de população possível, com grande eficácia, de forma transparente e com custos de implementação e manutenção técnica e humana reduzidos.
- Suporte – Questões relativas ao apoio técnico pré e pós implementação são focadas com bastante ênfase.
- Custos: Não só da implementação do Serviço de Directoria, mas também do parque informático, bem como da formação necessária ao nível técnico para operar com o Serviço de Directoria.

Uma das conclusões retiradas da literatura revista, foi que todos os serviços de directoria analisados usam um protocolo comum – o LDAP (Lightweight Directory Access Protocol), terminando aqui as suas semelhanças. As análises realizadas aos produtos das empresas acima citados são no mínimo contraditórios, pois são efectuados pelas próprias empresas.

Um outro facto relevante e retirado dos artigos revistos, é que, a fase de selecção e discussão em algumas das organizações (Universidades também) demorou de 3 a 6 meses, com o apoio de consultores externos às próprias instituições na demonstração local e perante os cenários apresentados, dos produtos que comercializam.

Relativamente aos produtos Open-Source, pode-se dizer que existem alguns produtos disponíveis, tendo no entanto um senão, que é facto de existir falta de suporte e documentação técnica em abundância, nem centros de formação adequados. Também não foi possível determinar instalações relevantes (em grandes instituições) de Serviços de Directoria com produtos do tipo Open-Source.



5. X.500 Directory Access Protocol (DAP)

X.500, Directory Access Protocol (DAP) é uma forma standard de desenvolver uma directoria electrónica constituída por pessoas numa determinada organização de forma que possam fazer parte de uma directoria global disponível para qualquer um em qualquer parte.

Na arquitectura de directoria X.500 um cliente faz query's recebendo respostas de um ou mais servidores a partir do Serviço de Directoria, através do DAP (Directory Access Protocol), controlando a comunicação entre o cliente e o servidor.

O Directory System Agent (DSA) é a Base de Dados onde a informação da Directoria é armazenada. Esta Base de Dados é Hierárquica na forma, desenhada para responder de uma forma muita rápida às questões que lhe são colocadas.

O programa de acesso disponível aos utilizadores é um Directory User Agent (DUA). DUA inclui um Whois, Finger e programas que oferecem uma componente gráfica na sua utilização.

O Directory System Protocol (DSP) controla a interacção entre uma ou mais DSA's e entre a DUA e a DSA. Isto é feito de tal forma que um utilizador pode aceder a uma determinada informação na Directoria sem saber exactamente a localização da física dessa mesma informação.

O X.500 oferece as seguintes características base:

- **Manutenção Descentralizada:** Cada site que se encontra a correr o X.500 é responsável unicamente pela parte local da Directoria. Assim os updates e a manutenção podem ser feitos instantaneamente.
- **Um FrameWork de Informação Estruturada:** O X.500 define um FrameWork de Informação usado na Directoria permitindo extensões locais.
- **Standard – Base dos Serviços de Directoria:** X.500 pode ser usado para construir aplicações que exijam informação de directoria (email, ferramentas de procura, etc), ou aceder a informação global de uma forma unificada.
- **Mecanismos de Procura Poderosos:** X.500 oferece mecanismos de procura muito poderosos que permitem aos utilizadores construir de uma forma arbitrária querys extremamente complexas.
- **Um Name-Space Único:** Tal como o DNS, o X.500 dá um único e homogéneo Name-Space aos utilizadores. O Name-Space do X.500 é mais flexível e expansível que o DNS.



6. Limitações do X.500

O X.500 é criticado por ser demasiado complexo para a maior parte das implementações, devido à forma como está estruturada a informação na sua Base de Dados. Talvez seja esta a razão principal, para que existam tão poucas instalações puras de X.500.



7. LDAP (Lightweight Directory Access Protocol)

Para resolver este problema de “complexidade excessiva” a Universidade de Michigan, desenvolveu uma versão baseada em TCP/IP do DAP, chamada de Lightweight Directory Access Protocol (LDAP) também conhecida por X.500-Light, para ser usada na Internet. O LDAP (actualmente com na versão 3) oferece as mesmas funcionalidades básicas do DAP, sem a complexidade e o peso excessivo do DAP, podendo ser usada para questionar Serviços de Directoria

Proprietários bem como de serviços X.500 abertos (Como complemento ao próprio DAP).

Com o passar dos anos, grande parte das produtoras de software relacionadas com Email e Serviços de Directoria, expressaram o seu interesse no LDAP, tornando-se o protocolo de eleição para a Internet, ao nível do Email e Serviços de Directoria.

•
—