Uma Ferramenta para a Administração de Serviços de Diretório Distribuídos Baseados no OpenLDAP

Fernando William Cruz, Giovanni Almeida Santos, Raissa Dantas Freire de Medeiros, Lucas Araújo Pereira, Márcio Carlos Braga, Roberto Diener

Universidade Católica de Brasília - UCB
QS 07 Lote 01 – Águas Claras – 71966-700 – Taguatinga – DF – Brasil

{fwcruz,giovanni,raissad}@ucb.br, lucas@sisnetti.com.br,
marcio@tecnolink.com.br, robertodiener@brturbo.com

Abstract. *The LDAP free administration tools present some limitations. In general, they allow object management in a centralized directory server, but they do not provide a suitable manner to deal with distributed directories. This paper proposes a free administration tool for an OpenLDAP-based distributed directory service, which allows the graphical management of objects, partitions, replicas, schemas and ACLs, without the direct access to OpenLDAP configuration files by the service administrator.*

Resumo. *As ferramentas livres para administração de serviços de diretório LDAP atualmente existentes são bastante limitadas, permitindo apenas a gerência de objetos em servidores isolados. Esse artigo propõe uma ferramenta para administração de serviços de diretório distribuídos baseados no OpenLDAP. Seu uso permite gerenciar graficamente não apenas objetos, mas também partições, réplicas, esquemas e ACLs sem a necessidade de manipulação direta dos arquivos de configuração do diretório.*

1. Introdução

Serviço de diretório é uma tecnologia que serve como suporte para a realização de atividades tais como nomeação, localização e segurança, dentre outras, relacionadas à gestão da infraestrutura de recursos (usuários, impressoras, servidores, etc.) nas organizações.

Nesse contexto, é possível perceber diversos tipos de serviços de diretórios. Dentre esses, destacam-se o X.500, que faz parte do modelo de referência OSI/ISO [1], e o LDAP [2], que é considerado um padrão *de facto* para serviços de diretório na Internet. Esses protocolos ganharam aceitação em relação aos demais pelo fato de serem padrões abertos e de permitirem a incorporação completa de serviços que sempre foram realizados por sistemas operacionais de rede [8].

Existem diversas implementações desses protocolos disponíveis atualmente, mas, no mundo do código aberto, a implementação do LDAP de maior aceitação é o OpenLDAP [3]. Tal implementação é bastante utilizada em plataformas Linux para construção de serviços de diretório distribuídos. Em comparação com outras soluções de diretórios, o OpenLDAP apresenta um bom grau de tolerância a falhas e um bom desempenho [6].

Contudo, administrar um serviço de diretório baseado no OpenLDAP ainda é uma tarefa complexa. Há diversas ferramentas disponíveis – dentre as quais se destaca o phpLDAPadmin [4] - contudo, elas apresentam algumas limitações:

i. Não facilitam a configuração do serviço de diretório, a qual é feita diretamente via arquivos que possuem uma sintaxe específica. Isso inclui a definição de esquemas, configuração de ACLs (*Access Control Lists*), administração de réplicas e partições.

ii. Em geral, as corporações possuem objetos espalhados fisicamente em diferentes servidores, mas não há o suporte adequado para a administração gráfica de objetos distribuídos. Não é possível, por exemplo, que um administrador altere, remova ou acrescente objetos numa partição remota se ele não é usuário local daquela partição, mesmo que ele tenha autorização para tal. Na verdade, essa é uma característica do LDAP, mas há mecanismos para tornar a administração de objetos distribuídos transparente [3].

iii. Não suportam autenticação de usuários em um serviço de diretório distribuído.

Sendo assim, esse artigo propõe uma ferramenta gráfica para a administração de serviços de diretório baseados no OpenLDAP, tendo como foco a gerência de objetos, partições, réplicas e esquemas em um ambiente distribuído. Na próxima seção, será detalhada a arquitetura da solução proposta. Nas seções 3 e 4, são descritos os módulos que compõem a solução e suas funcionalidades. Na seção 5, são descritos trabalhos futuros já vislumbrados.

2. Arquitetura da Ferramenta de Administração de Diretórios Distribuída (ADD)

Visando resolver os aspectos abordados na seção anterior com relação à melhoria da administração do OpenLDAP e a sua gestão em ambientes distribuídos, propõe-se o ADD[1], cuja arquitetura está descrita na Figura 1.

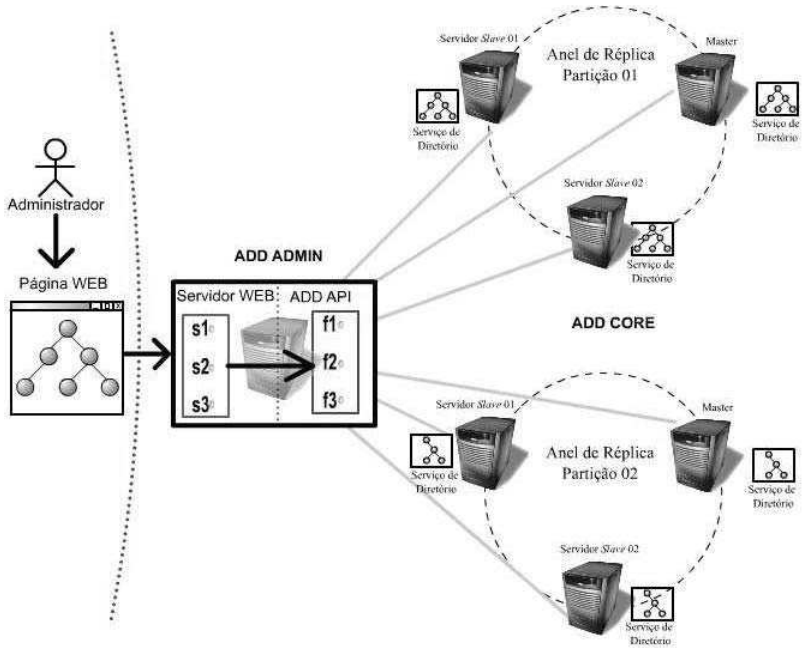

Figura 1. Arquitetura da Ferramenta de Administração de Diretórios Distribuída

Na Figura 1, os objetos da árvore de diretório estão distribuídos em duas partições - 01 e 02, cada uma suportada por um anel de réplica (que emprega um esquema de replicação *single-master*

[1] O ADD faz parte do GATI (Gerência de Ambiente de Tecnologia da Informação), um ambiente de administração integrado que inclui outros módulos (que não são objeto desse documento) e está sendo desenvolvido pelo CESMIC/UCB em convênio com a Itautec.

[5]), cujo controle está centralizado num único ponto. Em relação ao anel, um dos servidores desempenha o papel de mestre (*master)*, aceitando operações de escrita e leitura, e os demais representam réplicas apenas de leitura (*slaves*). O mestre é responsável pela atualização das réplicas, de forma a garantir a sincronização da base de objetos entre eles. Todos os servidores de cada anel de réplica têm o OpenLDAP instalado.

A arquitetura proposta é formada por dois módulos principais, de acordo com o que está descrito a seguir:

- ADD ADMIN: Instalado num servidor que possibilita efetuar operações administrativas sobre o serviço de diretórios via WEB. Composto de funcionalidades que tratam da interface com o administrador (s1, s2 e s3) e por uma API de gerência (representada na Figura 1 por f1, f2 e f3). As funcionalidades associadas a essa interface fazem chamadas ao ADD API em atendimento às requisições do usuário. O ADD API, por sua vez, faz requisições aos servidores de diretório via LDAP ou, quando isso não é suficiente, invoca o ADD CORE diretamente.
- ADD CORE: Composto de funções que executam do lado dos servidores de diretório. Seu objetivo é realizar operações sobre o serviço OpenLDAP propriamente dito, envolvendo tarefas como reinicialização do servidor OpenLDAP e modificação de arquivos de configuração.

O ADD ADMIN usa a linguagem Java (e tecnologias associadas, como JSP e Servlets) na sua implementação, enquanto o ADD CORE é baseado em C. A seguir, serão descritas as principais funcionalidades do ADD ADMIN e ADD CORE.

3. ADD ADMIN

Além da interface com o administrador, o ADD ADMIN possui uma API que é composta por cinco sub-módulos, a saber:

- *Objeto Admin* - responsável pela administração dos objetos armazenados no diretório. Permite que sejam feitas operações de inclusão, alteração e remoção de objetos, independente da partição em que estejam localizados. Além disso, objetos podem ser copiados ou movidos dentro da árvore, inclusive para pontos localizados em partições distintas.
- *Partição Admin* – provê funcionalidades associadas à gerência de partições do serviço de diretório. Esse sub-módulo permite a criação e remoção de partições, cuidando da redistribuição dos objetos entre as mesmas.
- *Replica Admin* – permite administrar os servidores que compõem os anéis de réplica que suportam as partições, podendo incluir, remover e visualizar *status* dos servidores, converter master em réplica e vice-versa, reiniciar o serviço OpenLDAP, entre outras atividades.
- *ACL Admin* – facilita a administração das permissões que os usuários têm sobre os objetos contidos no diretório. Tais permissões podem ser aplicadas num objeto específico, sendo automaticamente propagadas para todas as sub-árvores ou sub-partições existentes, promovendo a herança de direitos na árvore distribuída. Além disso, abstrai a sintaxe do OpenLDAP para a configuração de ACLs.
- *Esquema Admin* – provê a gerência de esquemas do serviço de diretório, permitindo que estes possam ser incluídos, removidos ou modificados. As modificações somente podem ser feitas na partição raiz do diretório e são automaticamente propagadas para as demais partições, com o objetivo de manter a consistência das informações.

Nas funcionalidades acima, são resolvidas as questões inicialmente apontadas como restrições das ferramentas administrativas disponíveis. Está embutido no ADD um mecanismo de localização de objetos que permite o login do administrador num serviço distribuído, independente da partição da qual ele faz parte. Operações sobre objetos de partições diferentes daquela em que o administrador foi

inicialmente autenticado são possíveis via *SASL Proxy Authorization* [2] [5]. Os sub-módulos do ADD API (em conjunto com o ADD CORE) também dispensam a manipulação direta dos arquivos de configuração do OpenLDAP por parte do administrador. A lista completa das funcionalidades e um protótipo da interface do ADD podem ser encontrados em [7].

4. ADD CORE

O ADD CORE interage diretamente com os servidores OpenLDAP, em atendimento a chamadas remotas do ADD API. Nesse sentido, é ele quem efetivamente realiza modificações nos arquivos de configuração do serviço de diretório.

Algumas de suas funcionalidades incluem: configurar partições, acrescentar servidores num anel de réplica, incluir diretivas de esquemas e de ACLs no arquivo *slapd.conf* [3], dentre outras.

5. Trabalhos Futuros

Numa primeira fase a ser concluída em setembro próximo, todas as funcionalidades descritas neste documento estarão implementadas. Além disso, alguns melhoramentos são vislumbrados desde já para uma outra fase a ser iniciada em outubro. O principal deles é o suporte a várias partições em uma única máquina servidora e à administração das mesmas. Com relação à gerência de esquemas, esta deverá incluir checagem automática de integridade, evitando que o administrador realize operações indevidas (por exemplo, a alteração de um esquema que afeta objetos já existentes no diretório). A gerência de réplicas fornecerá suporte ao esquema multimaster [2] [5] em adição ao esquema single-master.

6. Agradecimentos

Agradecemos ao SERPRO pelo provimento de informações indispensáveis à realização desse trabalho durante a fase de levantamento de requisitos da solução aqui proposta. Agradecemos ainda a Itautec pelo apoio financeiro e parceria junto a Universidade Católica de Brasília.

7. Referências Bibliográficas

[1] Yeong, W., Howes, T. and Kille, S. *X.500 Directory Access Protocol*, RFC 1487, IETF, July 1993.

[2] Wahl, M., Coulbeck, A., Howes, T. and Kille, S. *Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions*, RFC 2252, IETF, December 1997.

[3] The Open Source LDAP suite, *http://www.openldap.org*. Fevereiro, 2004.

[4] The phpLDAPadmin tool, *http://phpldapadmin.sourceforge.net*. Fevereiro, 2004.

[5] Howes, T. A., Smith, M. C., Good, G. S. *Understanding and Deploying LDAP Directory Services, 2nd Edition*, Addison-Wesley, 2003.

[6] Thornton, E. J., Mundy, D. and Chadwick, D. W. *A Comparative Performance Analysis of 7 Lightweight Directory Access Protocol Directories*, IS Institute, University of Salford, Inglaterra, May 2003.

[7] Medeiros, R., Santos, G. , Cruz, F., Pereira, L. and Diener, R. *Especificação Técnica – Serviço de Diretórios*, Relatório Técnico 04-002B, Centro de Excelência em Servidores de Missão Crítica (CESMIC), Universidade Católica de Brasília, Abril 2004.

[8] Tanembaum A. S., Steen M. *Distributed Systems Principles and Paradigms*.Prentice Hall, 2002.