FIT-LDAP: Um Serviço de Diretório Tolerante a Falhas e Intrusões

Rayol Neto[1], Bruno Barreto[1], Diego Kreutz[2], Aldri Santos[3], Eduardo Feitosa[1]

[1]ETSS/IComp/UFAM, Manaus, Brasil

[2]SnT/University of Luxembourg, Luxembourg

[3]NR2/UFPR, Paraná, Brasil

{rayol,begb,efeitosa}@icomp.ufam.edu.br, diego.kreutz@uni.lu, aldri@inf.ufpr.br

Abstract. *Directory services (e.g., LDAP) are often used to keep sensitive information (e.g., data and user credentials) for critical systems such as domain control servers, DNS servers, access control services and public key infrastructure (PKI). In this paper, we present the first fault- and intrusion-tolerant directory service. Our system architecture leverages different techniques of distributed systems, dependability and security. We demonstrated the feasibility of the proposed architecture through a prototype implementation. The results show that our directory service performs good enough to sustain the requirements of IT infrastructures with more than 136K users.*

Resumo. *Serviços de diretório (e.g., LDAP) são frequentemente utilizados para manter informações sensíveis (e.g., dados e credenciais de usuários) em sistemas críticos como serviços de controle de domínio, servidores DNS, mecanismos de controle de acesso e infra-estrutura de chaves públicas. Este artigo apresenta a primeira arquitetura e mecanismos para prover serviços de diretórios tolerante a falhas e intrusões. Para atingir este objetivo são empregadas diferentes técnicas de sistemas distribuídos, dependabilidade e segurança. A viabilidade da solução proposta é demonstrada através da implementação e avaliação de um protótipo que utiliza protocolos e técnicas avançadas de tolerância a falhas e intrusões. Os resultados demonstram que a solução proposta é boa o suficiente para suportar as demandas de infra-estruturas de TI com mais de 136K usuários.*

1. Introdução e Motivação

A dependência de acesso rápido, seguro e garantido a dados críticos, como dados e credenciais de usuários, vem aumentando a um ritmo constante. Dois dos fatores que tem contribuído para esse cenário são: a integração e a interoperabilidade entre sistemas; e a horizontalização das infraestruturas de autenticação e autorização. Um exemplo clássico dos dois primeiros são os mecanismos de *single-sign-on* (SSO), que permitem a um usuário utilizar diferentes serviços com um único processo de autenticação. Isso, naturalmente, aumenta os riscos e falhas associadas aos serviços básicos de segurança.

Os serviços de diretórios, ou simplesmente diretórios, representam a solução mais comumente utilizada para atender essa demanda de integração, interoperabilidade e horizontalização de serviços de segurança essenciais. Os diretórios são tipicamente caracterizados como banco de dados especializados em

consultas, onde os dados são armazenados de forma flexível e hierárquica. Embora existam diferentes soluções de diretórios como eDirectory, Active Directory, NIS e StreeTalk [Howes et al. 2003], LDAP (*Lightweight Directory Access Protocol*) [Sermersheim 2006] é o protocolo mais difundido e utilizado no suporte à segurança e interoperabilidade de sistemas. LDAP é um protocolo de aplicação aberto e amplamente suportado pela indústria para acessar e manter informações em serviços de diretório distribuídos. Exemplos de sistemas que comumente utilizam diretórios LDAP são serviços de rede como e-mail, DNS e DHCP [Vasiliadis et al. 2007, Borsato et al. 2003], mecanismos de controle de acesso [Zhou and Meinel 2004, Park et al. 2002], infraestruturas de chave pública (PKI) [Karatsiolis et al. 2004], soluções de interoperabilidade de sistemas [Flechl and Field 2008, Kreutz and Charao 2009], entre outros [Ardizzone et al. 2011, Flechl and Field 2008].

Entre as principais características que levaram a ampla adoção dos diretórios LDAP estão a flexibilidade, a eficiência das consultas e o suporte nativo a replicação, ou seja, sua capacidade de simplificar a escalabilidade e a disponibilidade dos serviços de diretório. Entretanto, considerando o presente e o futuro cenário de ameaças persistentes [Tankard 2011, Kushner 2013] e o estado de guerra digital, a segurança e a dependabilidade de sistemas críticos, como diretórios LDAP, tomam novas proporções. No contexto atual, o caminho para proteger infraestruturas de TI contra as ameaças digitais avançadas é a cyber resiliência [Goche and Gouveia 2014, Boyd 2014]. Similarmente, a academia vem investigando a resiliência a situações extremas, que pode ser definida como tolerância a intrusões, como forma de promover a segurança automática de sistemas [Verissimo et al. 2006], i.e., tornar os sistemas robustos o suficiente para suportar as novas ameaças digitais [Ficco and Rak 2012, Kreutz et al. 2014a].

O LDAP suporta nativamente a replicação de dados, permitindo a operação em três diferentes modos, um único mestre (*SingleMaster*), mestres espelho (*MirrorMode*) e múltiplos mestres (*MultiMaster*). Entretanto, todas as três configurações suportam apenas falhas por parada. Devido a essa limitação, novas técnicas começaram a ser investigadas para criar serviços de diretório LDAP capazes de tolerar falhas arbitrárias, i.e., quaisquer tipos de anomalia de funcionamento dos sistemas, canais de comunicação ou infraestrutura de TI em si. Um dos recursos frequentemente utilizados para prover tolerância a falhas arbitrária são os protocolos BFT (*Byzantine Fault Tolerance*). A forma mais comum de implementar estes protocolos é através da replicação ativa ou de máquina de estados [Bessani et al. 2014b], que oferece consistência forte e favorece a disponibilidade.

Algumas soluções de diretórios LDAP tolerantes a falhas arbitrárias já foram propostas, como é o caso do bftLDAP [Wang et al. 2006] e do HBFTLDAP [Hou et al. 2006]. Entretanto, as soluções existentes toleram apenas falhas arbitrárias não-maliciosas. Elas não toleram falhas arbitrárias maliciosas, como ataques constantes, ameaças avançadas persistentes e intrusões. Os protocolos BFT, por si só, não são o suficiente para tolerar ataques constantes e intrusões [Bessani 2011, Brandão and Bessani 2012]. Outras técnicas e mecanismos são necessários para tolerar ameaças avançadas, como recuperação proativa e reativa, diversidade, rejuvenescimento, controle de exaustão de recursos e componentes confiáveis

[Verissimo et al. 2006, Sousa et al. 2007, Bessani 2011].

Tomando a diversidade de sistemas como um exemplo, as soluções existentes suportam apenas uma única implementação de serviços de diretório LDAP (e.g., OpenLDAP) em todas as réplicas. Isso significa que um atacante precisa descobrir apenas uma única vulnerabilidade no serviço de diretórios utilizado para comprometer todas as réplicas ao mesmo tempo (e.g., ataque paralelo). Da mesma forma, um simples bug na implementação do diretório irá potencialmente afetar todas as instâncias LDAP ao mesmo tempo, uma vez que a execução das réplicas é baseada em máquina de estados. Portanto, diversidade é um componente de suma importância para tolerar falhas arbitrárias e intrusões.

Com objetivo de contribuir para o avanço no desenvolvimento de diretórios LDAP robustos e capazes de enfrentar os ataques frequentes e constantes e as novas ameaças persistentes avançadas, este artigo propõe o FIT-LDAP, o primeiro serviço de diretório cyber resiliente, i.e., tolerante a falhas e intrusões, que combina diferentes técnicas de sistemas distribuídos, dependabilidade e segurança. A arquitetura do FIT-LDAP é baseada num modelo funcional e artefatos de sistemas demonstrados anteriormente como eficazes para o desenvolvimento de serviços de autenticação e autorização (por exemplo, RADIUS e OpenID) resilientes [Kreutz et al. 2014d, Kreutz et al. 2014b, Kreutz et al. 2014a]. Entre os componentes essenciais para tolerar falhas arbitrárias e intrusões estão os protocolos de replicação de máquinas de estado, as técnicas de diversidade e rejuvenescimento de sistemas, a recuperação pró-ativa e reativa e a diversidade de infraestruturas.

Um protótipo do FIT-LDAP foi implementado como prova de conceito. Ele utiliza um dos mais avançados protocolos de replicação de máquinas de estado para tolerar falhas arbitrárias, o BFT-SMaRt [Bessani et al. 2014b]. Este protocolo já foi utilizado anteriormente na implementação de outros serviços resilientes, como o R-RADIUS [Malichevskyy et al. 2012], o R-OpenID [Kreutz et al. 2014b], o C2FS [Bessani et al. 2014a] e provedores de identidade num modelo cloud-of-clouds [Kreutz and Feitosa 2014]. Os resultados demonstram que o FIT-LDAP é capaz de comportar as demandas de infraestruturas de TI, tolerando falhas e intrusões.

As principais contribuições desta proposta são: (1) uma arquitetura para serviços de diretório cyber resilientes; (2) componentes e protocolos para tolerar falhas arbitrárias, de forma transparente e eficiente, em diretórios LDAP; (3) mecanismos como diversidade e recuperação pró-ativa e reativa para tolerar falhas arbitrárias e intrusões; (4) uma solução genérica que pode ser utilizada em diferentes ambientes como uma única máquina física, múltiplas máquinas físicas, múltiplos data centers e múltiplas infraestruturas de nuvens; (5) uma análise de desempenho que demonstra que o FIT-LDAP satisfaz as necessidades de ambientes de produção como, por exemplo, uma universidade com mais de 136K usuários.

Este artigo está organizado da seguinte maneira. A Seção 2 descreve a arquitetura e os elementos de projeto do FIT-LDAP, bem com sua implementação. Em seguida, a Seção 3 apresenta os resultados experimentais da arquitetura proposta, incluindo uma discussão sobre falhas toleradas pelo FIT-LDAP. A Seção 4 discute os trabalhos relacionados e os compara com a solução proposta. Por fim, a Seção 5 apresenta as considerações finais.

2. FIT-LDAP

2.1. Arquitetura

Recentemente, foram propostos e sistematizados um modelo funcional, artefatos de sistema e técnicas essenciais necessárias para o projeto, implementação e implantação de infraestruturas de autenticação e autorização (AAI) mais seguras e confiáveis [Kreutz et al. 2014d, Kreutz et al. 2014a]. A arquitetura do FIT-LDAP, ilustrada na Figura 1, segue e estende o modelo proposto para serviços de diretórios LDAP. Os componentes e mecanismos adotados, descritos na arquitetura e implementação, permitem ao FIT-LDAP tolerar falhas arbitrárias e intrusões em serviços de diretório LDAP. O modelo funcional da arquitetura pode ser resumido em quatro elementos: (a) cliente; (b) gateway; (c) réplicas SMR (***S**tate **M**achine **R**eplication*); e (d) serviços de diretório LDAP. O conjunto dos gateways, réplicas e serviços de diretório LDAP formam a infraestrutura do FIT-LDAP.

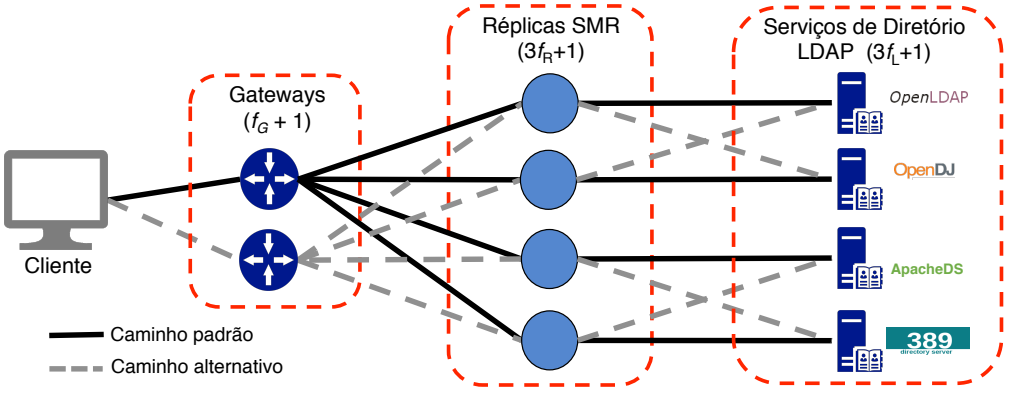

Figura 1. Arquitetura proposta para o serviço de diretório LDAP replicado.

O cliente representa um usuário ou serviço que tenta acessar alguma informação do diretório LDAP. Em termos práticos, o cliente é uma aplicação de autenticação, por exemplo.

Em relação a outras soluções como o BFTLDAP [Shoker and Bahsoun 2012], o FIT-LDAP apresenta um novo componente, mais simples e transparente, o gateway. Uma das principais funções do gateway é manter compatibilidade com os clientes existentes. Em outras palavras, o gateway é visto com um servidor LDAP convencional pelos clientes, ou seja, não é necessário qualquer tipo de modificação nos clientes.

A segunda função do gateway é mascarar o protocolo de replicação BFT-SMaRt e outros mecanismos utilizados para tolerar falhas arbitrárias e intrusões em diretórios LDAP. Ao receber a requisição do cliente, o gateway simplesmente encapsula os dados no protocolo BFT e envia para as $3f + 1$ réplicas do sistema. Similarmente, a resposta das réplicas é enviada aos respectivos clientes. Em outras palavras, o gateway atua de forma análoga a um gateway de rede, repassando dados de um lado para outro sem a necessidade dos processos comunicantes conhecerem os diferentes segmentos de rede. Por fim, o gateway podem também agregar funcionalidades adicionais, como a função de barreira de defesa (e.g, firewall), limitando as atividades maliciosas dos clientes.

O papel das réplicas SMR é processar as requisições dos clientes de forma determinista e ordenada. Por isso da necessidade de protocolos de replicação de máquinas de estado, como é o caso do BFT-SMaRt. As réplicas podem conectar-se a um único ou múltiplos servidores LDAP. Caso a conexão com um servidor falhe, a réplica SMR utiliza automaticamente a conexão com o próximo servidor LDAP da lista. Tanto a réplica quanto o serviço de diretórios LDAP podem ser instanciados na mesma máquina por questões de desempenho e segurança. No caso de ambos os componentes estarem na mesma máquina, não é necessário a utilização de canais cifrados (e.g., LDAPS) entre a réplica e o servidor LDAP, por exemplo.

Finalmente, o serviço de diretório LDAP pode ser parte integrante do domínio local ou ainda um serviço prestado por terceiros, i.e., localizado geograficamente em outro domínio. Essa flexibilidade aumenta a robustez do FIT-LDAP, uma vez que múltiplas infraestruturas físicas podem ser utilizadas para aumentar a disponibilidade do sistema e a resistência contra diferentes tipos de ataques. Múltiplos domínios e infraestruturas físicas são um importante aliado contra ameaças avançadas, para aumentar a disponibilidade do sistema, para evitar problemas de *vendor lock-in* em provedores de nuvem, entre outros [Kreutz et al. 2014d, Kreutz et al. 2014c, Kreutz and Feitosa 2014].

Duas das principais características, que também representam um diferencial em relação às soluções existentes, são o suporte a diversidade de diretórios LDAP e a capacidade de tirar proveito das vantagens de diferentes cenários de implantação. Ambas as características contribuem para aumentar a disponibilidade do sistema e tolerar falhas arbitrárias (de uma maneira geral e abrangente) e intrusões.

Diversidade de diretórios LDAP. O princípio básico da diversidade é evitar que falhas comuns (e.g., bugs de software ou hardware) e vulnerabilidades possam ser exploradas por atacantes. Como exemplo prático, assumindo um sistema replicado de diretórios LDAP para tolerar falhas arbitrárias que utilize o mesmo serviço LDAP em todas as réplicas, como é o caso do bftLDAP, HBFTLDAP e BFTLDAP, uma única vulnerabilidade na implementação do serviço permitirá ao usuário malicioso realizar um ataque paralelo e comprometer simultaneamente todas as réplicas. Similarmente, um bug de implementação também irá (potencialmente) afetar todas as réplicas ao mesmo tempo uma vez que protocolos de replicação de máquinas de estado são utilizados nas réplicas. De forma similar, o conceito de diversidade pode ser aplicado a diferentes níveis, desde hardware (e.g., utilizar diferentes infraestruturas físicas) até sistemas operacionais, bibliotecas e aplicações.

No caso do FIT-LDAP, o conceito de diversidade é estendido a todos os componentes do sistema (gateway, réplica e serviço LDAP). É assumido que a diversidade pode ser atingida com diferentes: (i) sistemas operacionais; (ii) implementações do serviço LDAP (e.g., OpenLDAP, Apache DS, 389Directory e OpenDJ); (iii) hypervisors (e.g., Xen, VirtualBox e VMWare); e (iv) infraestruturas físicas (e.g, diferentes máquinas físicas, data centers ou provedores de nuvem). A arquitetura e implementação do FIT-LDAP foram especialmente pensadas para os casos (ii) e (iv), ou seja, o suporte a múltiplas implementações LDAP e infraestruturas físicas. As outras formas de diversidade podem ser consideradas como comuns, ou seja, facilmente aplicáveis às soluções existentes uma vez que não interferem na arquitetura e nem na implementação do sistema.

Suporte a implantação em diferentes cenários. O FIT-LDAP foi arquitetado e implementado para permitir que os gateways, as réplicas e os serviços de diretório LDAP sejam instanciados em quaisquer lugar. Mais especificamente, diferentes máquinas físicas em um único domínio, múltiplas máquinas físicas em diferentes domínios, múltiplos data centers, ou ainda múltiplos provedores de nuvem. Essa característica permite ao sistema tolerar uma vasta gama de falhas físicas (e.g., problemas de conexão de rede, falhas de energia e falhas de disco) e lógicas (e.g., erros de configuração de sistemas/redes e ataques de negação de serviço). Adicionalmente, a implantação em múltiplas infraestruturas físicas contribui para garantir altos níveis de disponibilidade e fornecer mecanismos extras de proteção contra diferentes tipos de ataques de exaustão de recursos, DDoS em grande escala, e assim por diante [Kreutz et al. 2014d, Kreutz et al. 2014c, Kreutz and Feitosa 2014]. Cabe também ressaltar que a implantação do sistema em diferentes infraestruturas físicas permite atingir níveis de desempenho bons o suficiente para suportar demandas corriqueiras de instituições de diferentes portes, como universidades com mais de 200K usuários [Niedermayer et al. 2014, Kreutz and Feitosa 2014].

2.2. Modelo e Suposições

Em primeiro lugar, é assumido um modelo de sincronia parcial [Dwork et al. 1988], ou seja, o sistema pode se comportar de forma assíncrona por algum tempo, até que se torne síncrono, i.e., com limites de tempo de processamento e comunicação. Este é um requisito essencial para garantir o término dos protocolos de consenso, um alicerce fundamental para a implementação de replicação máquina de estado.

É assumido que os gateways conseguem comunicar-se com todas as réplicas SMR através do protocolo BFT-SMaRt. Ao receber um pacote de um cliente, o gateway encapsula os dados no protocolo BFT e enviada para as réplicas. O gateway aguarda a resposta correta (igual) de $2f_R + 1$ réplicas antes de responder ao cliente.

Com relação ao modelo de falhas, são assumidas falhas arbitrárias de até f_G gateways e falhas arbitrárias nas réplicas SMR (f_R) e serviços LDAP (f_L). Não é assumido nada em relação aos clientes, ou seja, o sistema suporta um número ilimitado de clientes.

Por último, em relação ao modelo de ameaça, assume-se que um atacante pode: (i) comprometer simultaneamente até f_G gateways, f_R réplicas, e f_L diretórios LDAP, respectivamente; (ii) interceptar e injetar mensagens em até f_G gateways, f_R réplicas, e f_L diretórios LDAP; e (iii) alterar mensagens em trânsito. O FIT-LDAP considera um modelo de ameaça onde o atacante pode ter controle dos canais de comunicação entre os elementos do sistema. No entanto, é assumido que o atacante não é capaz de quebrar quaisquer mecanismos criptográficos sem obter as chaves criptográficas adequadas. Um atacante pode ainda ter o controle da rede por algum tempo, mas não pode controlar toda a rede durante todo o tempo. Esta é uma suposição razoável, já que todos os elementos do sistema, incluindo réplicas, podem estar em execução em diferentes infraestruturas físicas e, consequentemente, é altamente improvável que um atacante obtenha controle sobre os canais de comunicação ou recursos em lugares distintos.

2.3. Implementação

Na implementação do FIT-LDAP foi utilizada a biblioteca UnboundID LDAP [UnboundID 2015] (versão 0.9.8), que suporta a versão 3 do protocolo LDAP, e a biblioteca BFT-SMaRt [bft smart 2015] para replicação de máquina de estados. Esta biblioteca fornece um conjunto de módulos e protocolos de comunicação para assegurar canais de comunicação seguros e eficientes entre as réplicas.

A Figura 2 ilustra a implementação do FIT-LDAP. Os clientes comunicam-se com os gateways através de TCP/IP, assim como ocorre com servidores LDAP tradicionais. Para fins de testes, foi implementada uma aplicação cliente utilizando a biblioteca UnboundID LDAP. Esta aplicação realiza operações (e.g., consultas) no diretório LDAP.

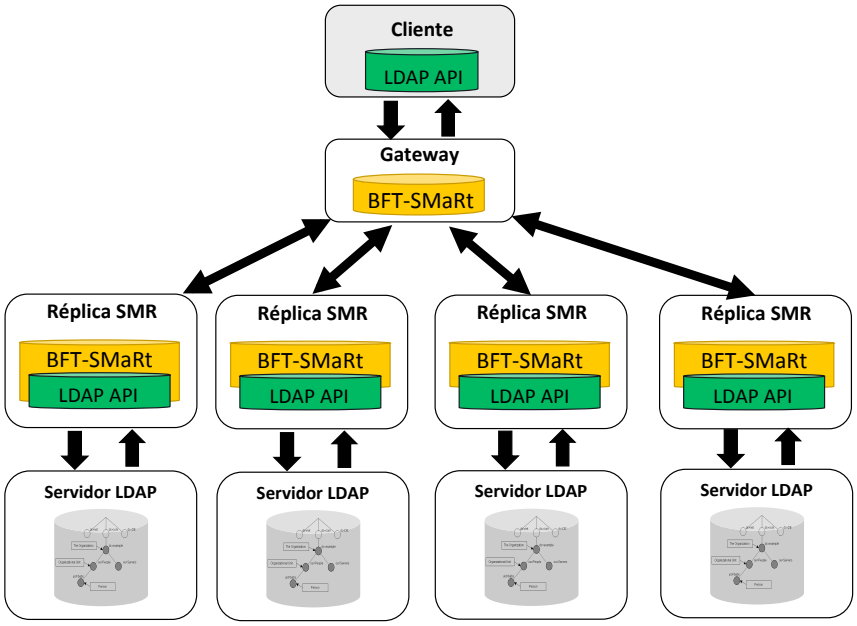

Figura 2. Elementos de implementação do diretório LDAP replicado.

O gateway recebe as conexões dos clientes (via TCP, na porta 389) e simplesmente as repassa a interface BFT proxy do BFT-SMaRt. O BFT proxy envia, de forma ativa, uma cópia das requisições dos clientes para cada réplicas SMR. De maneira similar, respostas vindas das réplicas são enviados aos clientes através dos canais TCP/IP previamente estabelecidos.

Uma réplica SMR mantém um arcabouço de conexões com um ou mais serviços de diretório LDAP. Ao receber a requisição do cliente, encaminhada pelo gateway, a réplica encaminha a requisição para o(s) respectivo(s) servidor(es) LDAP. O servidor LDAP pode ser qualquer implementação LDAP disponível, desde que suporte a versão 3 do protocolo.

Após executar a operação requisitada, a réplica SMR encaminha a resposta do serviço LDAP ao gateway. Ao receber $2f_R + 1$ respostas idênticas, o gateway envia a resposta ao respectivo cliente. Caso não hajam $2f_R + 1$ respostas idênticas, o proxy BFT reenvia a requisição original às réplicas SMR.

3. Avaliação

Esta seção apresenta uma avaliação de desempenho do FIT-LDAP e uma análise resumida dos diferentes tipos de falhas e ataques.

3.1. Desempenho

Para a avaliação de desempenho do FIT-LDAP foi utilizando um ambiente composto por seis máquinas virtuais (VMs), como resumido na Tabela 1. Uma para executar os clientes e uma segunda para executar um gateway. Adicionalmente, mais quatro VMs para executar as réplicas SMR e os serviços de diretório LDAP, sendo uma réplica e um serviço de diretório por VM.

Tabela 1. Ambiente utilizado para o teste

Tipo	# VMs	# vCPUs	Memória	Disco	Rede
Clientes	1	8	8	15GB	Gigabit Ethernet
Gateway	1	4	4	15GB	Gigabit Ethernet
Replicas	4	4	4	15GB	Gigabit Ethernet

Para os testes foram utilizadas duas implementações LDAP, o OpenLDAP (versão 2.4.31) e o OpenDJ xpress (versão 2.5.0). Cada uma das quatro instâncias de serviços de diretório foi povoada com 45000 entradas. Duas réplicas SMR foram conectadas ao servidor OpenLDAP, enquanto que as outras duas foram conectadas ao servidor OpenDJ xpress.

Vazão do sistema. O desempenho do FIT-LDAP foi medido em duas configurações distintas, uma utilizando apenas o OpenLDAP em todas as réplicas e a outra utilizando diversidade (OpenLDAP e OpenDJ). A Figura 3 apresenta os resultados dos experimentos no ambiente sem diversidade. Foram utilizados 10, 25, 50 e 100 clientes simultâneos, executados na VM clientes (Tabela 1). Cada cliente foi configurado para realizar 1.000 operações de busca com tamanhos de mensagem variando de 1byte a 512bytes. Conforme outros trabalhos de avaliação de desempenho de diretórios LDAP, um dos tamanhos de mensagens mais comuns é de 488 bytes [Wang et al. 2008], o qual foi incluído nas avaliações realizadas. Para cada configuração de cliente, foram realizadas 5 execuções.

Como pode ser observado na Figura 3, a diferença de desempenho é pequena com a variação dos tamanhos das mensagens e o número de clientes. Tal fato é explicado por uma das características da biblioteca BFT-SMaRt, que é operar garantindo o ordenamento total das mensagens (*Total Order Multicast*) [Bessani et al. 2014b]. Durante a execução normal, os clientes enviam seus pedidos para todas as réplicas, em lote, e esperam por suas respostas. O ordenamento total é realizado através de uma sequência de instâncias de consenso entre as réplicas.

No melhor caso, com 100 clientes e mensagens de 64 bytes, a vazão do sistema chega próximo a 1400 operações por segundo. Cabe ressaltar que o FIT-LDAP atinge um desempenho de 1400 operações/s no pior caso (levando em conta operações de leitura e escrita em SMR), que são operações totalmente ordenadas e serializadas nas réplicas. Essa vazão é o suficiente para suportar ambientes de TI, como universidades, com mais de 136K usuários, conforme números relatados em trabalhos anteriores [Niedermayer et al. 2014, Kreutz et al. 2014a]. Este tipo de operação é

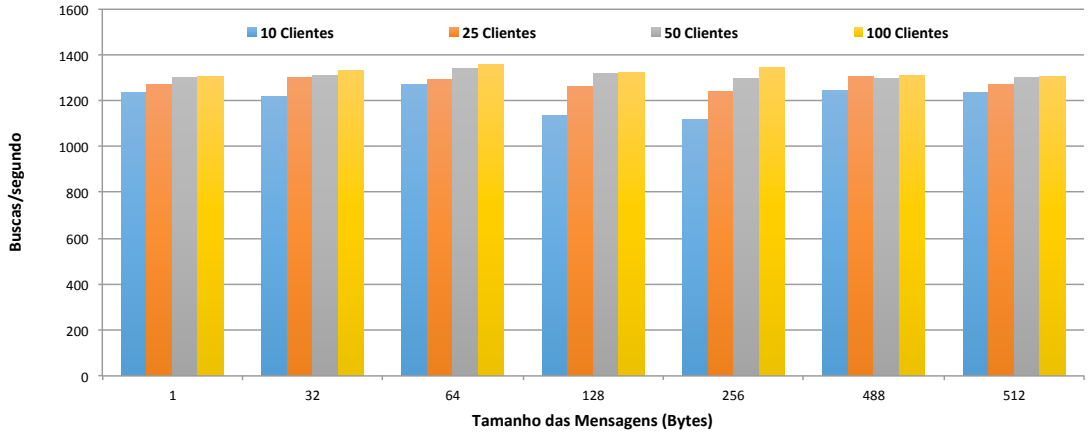

Figura 3. Vazão do FIT-LDAP sem diversidade.

necessário somente para operações de escrita, para manter a consistência forte dos dados. As operações de leitura, como é o caso das buscas, podem ser executadas de forma não ordenada e não serializada. O BFT-SMaRt suporta este tipo de operação. Um dos trabalhos futuro é avaliar os limites do sistema em termos de escalabilidade e desempenho.

A Figura 4 mostra os resultados do sistema no ambiente com diversidade (2 servidores OpenLDAP e 2 servidores OpenDJ). Como pode ser observado, a vazão do sistema é similar à do ambiente sem diversidade. Devido a isso, pode-se concluir que a diversidade de diretórios LDAP não causa nenhum impacto significativo no desempenho do sistema.

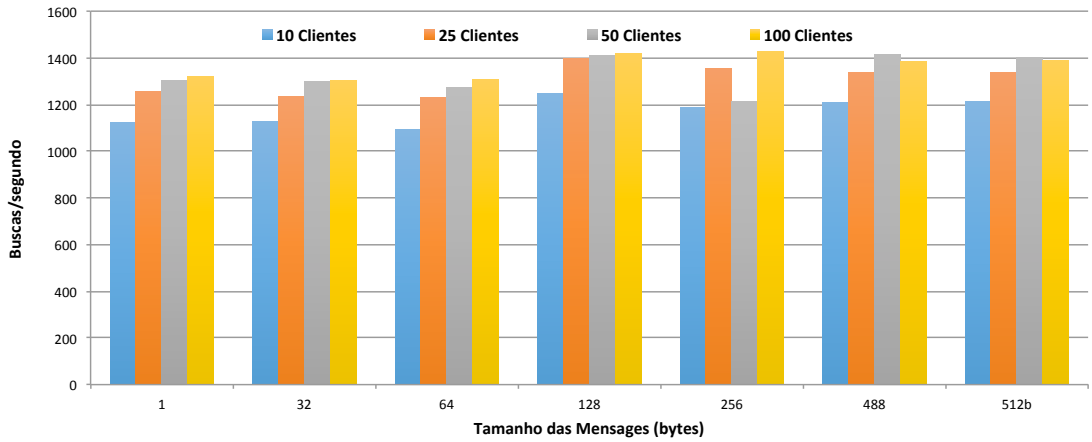

Figura 4. Vazão do FIT-LDAP com diversidade (OpenLDAP e OpenDJ).

3.2. Falhas e Ataques

Servidores de diretório LDAP tradicionais (e.g., OpenLDAP e OpenDJ) não toleram falhas arbitrárias. Soluções como o bftLDAP, HBFTLDAP e BFTLDAP suportam apenas parcialmente falhas arbitrárias (vide Seção 4). Já o FIT-LDAP, além de tolerar falhas arbitrárias nas réplicas, suporta diversidade de serviços de diretório, o que

permite tolerar quaisquer falhas arbitrárias no sistema (e.g., bugs de implementação dos servidores LDAP).

Como o FIT-LDAP utiliza o mesmo modelo funcional do R-RADIUS e do R-OpenID [Kreutz et al. 2014d, Kreutz et al. 2014a] e, também, os mesmos protocolos de tolerância a falhas, como é o caso do BFT-SMaRt, ele tolera os mesmos tipos de falhas e ataques. Em outras palavras, o FIT-LDAP suporta simultaneamente falhas arbitrárias em até f_G gateways e f_R réplicas. As falhas arbitrárias incluem quaisquer anomalias de protocolo, falhas de infraestruturas e ataques como negação de serviço e exaustão de recursos. O impacto desse tipo de falhas e ataques no sistema já foi demostrado anteriormente [Kreutz et al. 2014a, Kreutz et al. 2014c].

4. Trabalhos Relacionados

Tolerância a falhas é um dos pontos cobertos pela especificação do protocolo LDAP [Harrison 2006]. Tomando como exemplo o OpenLDAP [OpenLDAP 2014], é comum implementações do LDAP oferecerem três esquemas de replicação, *Single-Master*, *MirrorMode* e *MultiMaster*. O primeiro, mais simples, é baseados no modelo mestre e escravos, ou seja, um único processo mestre e múltiplos processos escravos. Enquanto que as escritas de dados podem ser realizadas somente no processo mestre, as leituras podem ser realizadas em todos os processos. Naturalmente, as escritas ficam comprometidas no caso de falha do processo mestre. No modelo *SingleMaster* tanto o processo mestre quanto os escravos toleram apenas falhas por parada.

O modelo *MirrorMode* é similar ao *SingleMaster*, com a diferença de ter dois processos mestre que cooperam na atualização dos dados. Portanto, as escritas ficam comprometidas somente quando os dois mestres falharem. Finalmente, no modelo *MultiMaster* todos os processos são mestres, ou seja, suportam operações de escrita. Os dados escritos num processo mestre são replicados para os outros os demais servidores. Assim como no caso do modelo *SingleMaster*, os modelos *MirrorMode* e *MultiMaster* suportam apenas falhas por paragem. Além disso, em todos os modelos, escritas realizadas num processo mestre falho são comprometidas. Caso o processo falhe durante a escrita, os dados serão perdidos. Em outras palavras, os clientes precisam tratar falhas dos processos mestre, ou seja, re-encaminhar os pedidos de escrita para eventuais processos mestre não falhos.

Apesar dos modelos de replicação do LDAP ajudarem a aumentar o desempenho e a disponibilidade do serviço, eles não oferecem efetivo suporte à resiliência e confiabilidade do serviço no caso de falhas da sincronização entre os processos ou no caso de falhas arbitrarias [Shoker and Bahsoun 2012]. O bftLDAP é uma das primeiras soluções a propor protocolos de tolerância a falhas arbitrárias, como o CLBFT, para garantir a consistência dos dados entre as réplicas e a disponibilidade do serviço no caso de falhas arbitrárias [Wang et al. 2006]. O bftLDAP utiliza o modelo tradicional de $3f + 1$ réplicas para tolerar f falhas simultâneas sem comprometer a operação do serviço. Os testes realizados com o bftLDAP apontaram que a replicação dos dados utilizando o CLBFT leva a uma sobrecarga de até 42,29% (para operação de busca) em relação a um serviço LDAP simples, i.e., que não tolera falhas arbitrárias.

Um segundo exemplo de implementação tolerante a falhas arbitrárias é o HBFTLDAP [Hou et al. 2006]. Apesar do HBFTLDAP criar um serviço de di-

retório hierárquico tolerante a falhas, com o objetivo de atingir garantir maior escalabilidade, os resultados, em termos de desempenho, são idênticos ao bftLDAP. Mais recentemente, diferentes protocolos para tolerar falhas arbitrárias em serviços LDAP foram testados, como o PBFT, Chain, Zyzzyva e o Quorum [Shoker and Bahsoun 2012]. Considerando apenas funções de busca, as implementações BFTLDAP com os protocolos PBFT e Zyzzyva atingiram um desempenho similar ao do OpenLDAP. Este apresenta um desempenho 5% melhor que o BFTLDAP/Zyzzyva e 10% melhor que o BFTLDAP/PBFT para mensagens pequenas. No caso de mensagens maiores, a diferença de desempenho reduz ainda mais, ou seja, as implementações com suporte a falhas arbitrárias atingem praticamente o mesmo número de operações por segundo do OpenLDAP.

A Tabela 2 resume as principais características das soluções existentes, bem como da solução proposta. Enquanto que o OpenLDAP necessita $f+1$ réplicas para tolerar falhas por parada, todas as soluções que toleram falhas arbitrárias (parcialmente ou totalmente) utilizam $3f+1$ réplicas para tolerar f falhas sem comprometer a operação do serviço. A única solução projetada para suportar múltiplas implementações (e.g., OpenLDAP, OpenDJ e ApacheDS) de serviços LDAP é o FIT-LDAP. As demais soluções, como bftLDAP, HBFTLDAP e BFTLDAP, utilizam apenas o OpenLDAP e suportam apenas parcialmente falhas arbitrárias. Tomando como exemplo um bug de implementação no serviço LDAP, com exceção da solução proposta, nenhuma das soluções existentes é capaz de efetivamente suportar esse tipo de falha. A única solução projetada para tolerar intrusões é o FIT-LDAP.

Tabela 2. Comparação dos trabalhos relacionados e abordagem proposta

Solução	Tipos de Falhas Toleradas	Protocolo de Replicação	Serviço LDAP	# réplicas	Tolerância a Intrusão
OpenLDAP *SingleMaster*	Por parada (*)	Syncrepl	OpenLDAP	$f+1$	não
OpenLDAP *MirrorMode*	Por parada	Syncrepl	OpenLDAP	$f+1$	não
OpenLDAP *MultiMaster*	Por parada	Syncrepl	OpenLDAP	$f+1$	não
bftLDAP	Por parada e parcialmente arbitrárias	CLBFT	OpenLDAP (2.1.22)	$3f+1$	não
HBFTLDAP	Por parada e parcialmente arbitrárias	CLBFT	OpenLDAP (2.1.22)	$3f+1$	não
BFTLDAP	Por parada e parcialmente arbitrárias	PBFT, Zyzzyva	OpenLDAP (2.4)	$3f+1$	não
FIT-LDAP	Por parada e arbitrárias	BFT-SMaRt	Múltiplos	$3f+1$	sim
(*) A parada do servidor Master interrompe a operação de escrita.					

Resumidamente, os principais diferenciais do FIT-LDAP, quando comparado às soluções existentes, são: (1) maior disponibilidade, resistindo a diferentes tipos de falhas físicas e lógicas (e.g., bugs de implementação e ataques paralelos); (2) resistência a ataques de exaustão de recursos, uma vez que as réplicas podem ser instanciadas em diferentes máquinas físicas e/ou domínios administrativos; e (3) capacidade de tirar vantagem de ambientes multi-data center e multi-cloud, usufruindo dos respectivos mecanismos de defesa dessas infraestruturas, como mecanismos de mitigação

de ataques de negação de serviços [Prince 2013, Kreutz and Feitosa 2014].

5. Conclusão

Este artigo apresentou o FIT-LDAP, o primeiro serviço de diretório tolerante a falhas arbitrárias e intrusões, que combina diferentes técnicas de sistemas distribuídos, dependabilidade e segurança. Como forma de validar a arquitetura proposta, foi implementado e avaliado um protótipo.

Os resultados de desempenho do FIT-LDAP demonstram que a solução pode ser utilizada em infra-estruturas de TI, como universidades, com mais de 136K usuários. Além disso, a solução proposta é a única a tolerar falhas arbitrárias e intrusões. Um dos componentes essenciais para atingir este objetivo é o uso da diversidade de serviços de diretório LDAP, o que garante maior robustez e resistência ao sistema.

Com trabalhos futuros podem ser relacionados testes da arquitetura em outros ambientes, identificar os limites de desempenho e escalabilidade do sistema (e.g., incluindo operações de busca sem ordenação total e serialização) e aumentar a diversidade através de outras implementações de serviços de diretórios.

Referências

Ardizzone, V., Barbera, R., Calanducci, A., Fargetta, M., Ingrà, E., La Rocca, G., Monforte, S., Pistagna, F., Rotondo, R., and Scardaci, D. (2011). A european framework to build science gateways: Architecture and use cases. In *Proceedings of the 2011 TeraGrid Conference: Extreme Digital Discovery*, TG '11, pages 43:1–43:2, New York, NY, USA. ACM.

Bessani, A. (2011). From byzantine fault tolerance to intrusion tolerance (a position paper). In *Dependable Systems and Networks Workshops (DSN-W), 2011 IEEE/IFIP 41st International Conference on*, pages 15–18.

Bessani, A., Mendes, R., Oliveira, T., Neves, N., Correia, M., Pasin, M., and Verissimo, P. (2014a). Scfs: a shared cloud-backed file system. In *Proc. of the 2014 USENIX Annual Technical Conference*.

Bessani, A., Sousa, J., and Alchieri, E. (2014b). State machine replication for the masses with bft-smart. In *Dependable Systems and Networks (DSN), 2014 44th Annual IEEE/IFIP International Conference on*, pages 355–362.

bft smart (2015). Bft-smart. `http://bft-smart.github.io/library/`.

Borsato, L., Gaudet, M., Hamilton, I., Anderson, R., and Waters, G. (2003). Trusted network binding using ldap (lightweight directory access protocol). US Patent 6,654,891.

Boyd, A. (2014). It security shifts from prevention to resiliency. `http://goo.gl/01poFz`.

Brandão, L. and Bessani, A. (2012). On the reliability and availability of replicated and rejuvenating systems under stealth attacks and intrusions. *Journal of the Brazilian Computer Society*, 18(1):61–80.

Dwork, C., Lynch, N. A., and Stockmeyer, L. (1988). Consensus in the Presence of Partial Synchrony. *J. ACM*, 35(2):288–322.

Ficco, M. and Rak, M. (2012). Intrusion tolerance of stealth dos attacks to web services. In Gritzalis, D., Furnell, S., and Theoharidou, M., editors, *Information*

Security and Privacy Research, volume 376 of *IFIP Advances in Information and Communication Technology*, pages 579–584. Springer Berlin Heidelberg.

Flechl, M. and Field, L. (2008). Grid interoperability: joining grid information systems. *Journal of Physics: Conference Series*, 119(6):062030.

Goche, M. and Gouveia, W. (2014). Why cyber security is not enough: You need cyber resilience. `http://goo.gl/jNZ3Bw`.

Harrison, R. (2006). Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms. RFC 4513 (Proposed Standard).

Hou, H., Wang, X., and Wu, M. (2006). Hierarchical byzantine fault tolerant secure ldap. In *IEEE SMC'06*, pages 3844–3849.

Howes, T. A., Smith, M. C., and Good, G. S. (2003). *Understanding and Deploying LDAP Directory Services*. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 2 edition.

Karatsiolis, V., Lippert, M., and Wiesmaier, A. (2004). Using ldap directories for management of pki processes. In *Public Key Infrastructure*, pages 126–134. Springer.

Kreutz, D., Bessani, A., Feitosa, E., and Cunha, H. (2014a). Towards secure and dependable authentication and authorization infrastructures. In *Dependable Computing (PRDC), 2014 IEEE 20th Pacific Rim International Symposium on*, pages 43–52. IEEE.

Kreutz, D. and Charao, A. (2009). Flexvaps: a system for managing virtual appliances in heterogeneous virtualized environments. In *Network Operations and Management Symposium, 2009. LANOMS 2009. Latin American*, pages 1–12.

Kreutz, D. and Feitosa, E. (2014). Identity providers-as-a-service built as cloud-of-clouds: challenges and opportunities. In *Position Papers of the 2014 Federated Conference on Computer Science and Information Systems*, pages 101–108.

Kreutz, D., Feitosa, E., and Cunha, H. (2014b). Provedores de identidade resilientes e confiáveis. In *Anais do XXXII SBRC - XV WTF*, pages 174–187.

Kreutz, D., Feitosa, E., Cunha, H., Niedermayer, H., and Kinkelin, H. (2014c). Increasing the resilience and trustworthiness of openid identity providers for future networks and services. In *ARES 2014*, pages 317–324.

Kreutz, D., Malichevskyy, O., Feitosa, E., Barbosa, K. R. S., and Cunha, H. (2014d). System design artifacts for resilient identification and authentication infrastructures. In *ICNS*. IARIA.

Kushner, D. (2013). The real story of stuxnet. *IEEE Spectrum*, 50(3):48–53.

Malichevskyy, O., Kreutz, D., Pasin, M., and Bessani, A. (2012). O vigia dos vigias: um serviço radius resiliente. In *INForum*.

Niedermayer, H., Kreutz, D., Feitosa, E., Malichevskyy, O., Bessani, A., Fraga, J., Cunha, H. A., and Kinkelin, H. (2014). Trustworthy and resilient authentication service architectures. Technical report, SecFuNet Consortium.

OpenLDAP (2014). OpenLDAP Software 2.4 Administrator's Guide.

Park, J., Ahn, G.-J., and Sandhu, R. (2002). Role-based access control on the web using ldap. In Olivier, M. and Spooner, D., editors, *Database and Application Security XV*, volume 87 of *IFIP - The International Federation for Information Processing*, pages 19–30. Springer US.

Prince, M. (2013). The DDoS that almost broke the internet. `http://goo.gl/oeDrMY`.

Sermersheim, J. (2006). Lightweight Directory Access Protocol (LDAP): The Protocol. RFC 4511 (Proposed Standard).

Shoker, A. and Bahsoun, J.-P. (2012). Towards byzantine resilient directories. In *Proceedings of NCA '12*, pages 52–60.

Sousa, P., Bessani, A. N., Correia, M., Neves, N. F., and Verissimo, P. (2007). Resilient intrusion tolerance through proactive and reactive recovery. In *Proceedings of PRDC '07*, pages 373–380.

Tankard, C. (2011). Advanced Persistent threats and how to monitor and deter them. *Network Security*, (8).

UnboundID (2015). Unboundid ldap sdk for java. `https://www.ldap.com/unboundid-ldap-sdk-for-java`.

Vasiliadis, D., Rizos, G., Stergiou, E., and Margariti, S. (2007). A trusted network model using the lightweight directory access protocol. In *Proceedings of AIC*, pages 252–256.

Verissimo, P., Neves, N., Cachin, C., Poritz, J., Powell, D., Deswarte, Y., Stroud, R., and Welch, I. (2006). Intrusion-tolerant middleware: the road to automatic security. *Security Privacy, IEEE*, 4(4):54–62.

Wang, X., Hou, H., and Zhuang, Y. (2006). Secure byzantine fault tolerant ldap system. In *Proceedings of IMSCCS '06*, pages 34–39.

Wang, X., Schulzrinne, H., Kandlur, D., and Verma, D. (2008). Measurement and analysis of ldap performance. *Networking, IEEE/ACM Transactions on*, 16(1):232–243.

Zhou, W. and Meinel, C. (2004). Implement role based access control with attribute certificates. In *Advanced Communication Technology, 2004. The 6th International Conference on*, volume 1, pages 536–540.

