

**UNIVERSIDADE FEDERAL DE SANTA MARIA
CENTRO DE TECNOLOGIA
CIÊNCIA DA COMPUTAÇÃO**

**IMPLANTAÇÃO DE UM AMBIENTE DE TI
GERENCIÁVEL E INTEGRADO AO
OSTICKET NO CCSH/UFSM**

TRABALHO DE GRADUAÇÃO

Kevin Vinícius Teixeira Costa

Santa Maria, RS, Brasil

2014

IMPLANTAÇÃO DE UM AMBIENTE DE TI GERENCIÁVEL E INTÉGRADO AO OSTICKET NO CCSH/UFSM

Kevin Vinícius Teixeira Costa

Trabalho de Graduação apresentado ao curso de Ciência da Computação da
Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para
a obtenção do grau de

Bacharel em Ciência da Computação

Orientador: Prof.^a Dr.^a Roseclea Duarte Medina

**Trabalho de Graduação N° 390
Santa Maria, RS, Brasil**

2014

Universidade Federal de Santa Maria
Centro de Tecnologia
Curso de Ciência da Computação

A Comissão Examinadora, abaixo assinada,
aprova o Trabalho de Graduação

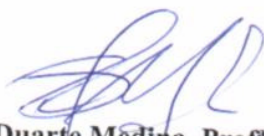
**IMPLANTAÇÃO DE UM AMBIENTE DE TI GERENCIÁVEL E INTEGRADO
AO OSTICKET NO CCSH/UFMS**

elaborado por

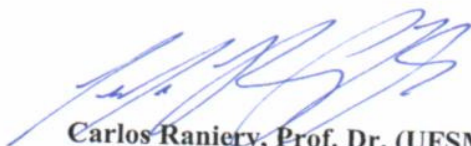
Kevin Vinícius Teixeira Costa

como requisito para obtenção do grau de
Bacharel em Ciência da Computação

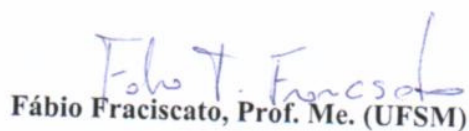
COMISSÃO EXAMINADORA:



Roseclea Duarte Medina, Profª. Drª. (Presidente/Orientador)



Carlos Raniery, Prof. Dr. (UFMS)



Fábio Fraciscato, Prof. Me. (UFMS)

Santa Maria, 16 de Dezembro de 2014.

"Wololo"

— AGE OF EMPIRES: PRIEST

RESUMO

Trabalho de Graduação
Ciência da Computação
Universidade Federal de Santa Maria

IMPLANTAÇÃO DE UM AMBIENTE DE TI GERENCIÁVEL E INTEGRADO AO OSTICKET NO CESH/UFMS

AUTOR: KEVIN VINÍCIUS TEIXEIRA COSTA

ORIENTADOR: ROSECLEA DUARTE MEDINA

Local da Defesa e Data: Santa Maria, 16 de Dezembro de 2014.

A gerência de redes é hoje uma área muito importante para infraestruturas computacionais, com a finalidade de haver uma otimização dos recursos disponíveis e minimização dos custos de manutenção. Assim, este trabalho tem o objetivo de implantar um ambiente gerenciável para o Centro de Ciências Sociais e Humanas da Universidade Federal de Santa Maria, a fim de permitir um melhor controle e maior segurança dos computadores e dispositivos da rede, com algumas de suas funções de forma remota através do site RemoteAD. Também foi instalado um sistema de help desk, chamado de osTicket, para abertura de chamados de suporte e registro de conhecimento em uma base de dados, melhorando e organizando o atendimento aos diversos setores da unidade universitária. A implantação resultou em melhorias na gerência e controle de computadores e dispositivos, e na geração de históricos de chamados e conhecimento adquirido.

Palavras-chave: Gerência de redes. Ticketing. Remota. Active Directory.

LISTA DE TABELAS

Tabela 4.1 – Divisão de conta de usuário por arquitetura	28
--	----

LISTA DE FIGURAS

Figura 2.1 – Exemplo de um diretório AD (MICROSOFT, 2014a)	16
Figura 2.2 – Exemplo genérico de uma hierarquia LDAP (OPENLDAP, 2003)	18
Figura 2.3 – Exemplo de aplicação de políticas de grupo em unidades organizacionais diferentes (MICROSOFT, 2014b)	19
Figura 4.1 – Diagrama de caso de uso com a interação entre atores e suas ações (autoria própria).....	24
Figura 4.2 – Diagrama de atividade para a melhoria contínua do sistema (BRIGANÓ; BARROS, 2010)	26
Figura 4.3 – Estrutura em árvore do diretório do AD para o CCSH (setas azuis), juntamente com suas respectivas políticas (setas verdes) (autoria própria)	27
Figura 4.4 – Console de administração do WSUS exibindo estatísticas e dados atuais sobre o status das máquinas (autoria própria)	30
Figura 4.5 – Lista de atualizações necessárias e aprovadas em alguns grupos (autoria própria).....	31
Figura 4.6 – Report Viewer mostrando a estatística de uma máquina que está atualizada (autoria própria).....	32
Figura 4.7 – Tela inicial dos tickets em abertos que estão em andamento (autoria própria)	35
Figura 4.8 – Tela exibindo os agentes responsáveis pela abertura e resolução dos tickets (autoria própria).....	35
Figura 4.9 – Tela mostrando a base de conhecimento atual, já com algumas entradas (autoria própria).....	36
Figura 4.10 – Diagrama de Atividades do sistema (autoria própria)	37
Figura 4.11 – Interface inicial para cada categoria escolhida (autoria própria)	39
Figura 4.12 – Menu de opções no estilo drop down em dispositivos móveis (autoria própria)	39
Figura A.1 – Exibição dos controladores de domínio disponíveis para o AD (autoria própria)	49
Figura A.2 – Área de trabalho padrão para laboratórios e salas de aula (autoria própria)...	49
Figura C.1 – Extensões ativas do PHP (autoria própria)	51

SUMÁRIO

1 INTRODUÇÃO	10
1.1 Motivação	10
1.2 Objetivos	11
2 REVISÃO BIBLIOGRÁFICA	12
2.1 Conceituação de gerência de redes de computadores	12
2.2 Cenário atual	14
2.3 Trabalhos correlatos	15
2.4 Conceituação das ferramentas e protocolos utilizados	16
2.4.1 Active Directory Domain Services (AD)	16
2.4.1.1 Usuários do AD	17
2.4.1.2 LDAP	17
2.4.1.3 Domínio	18
2.4.2 Controlador de Domínio	18
2.4.3 Fully Qualified Domain Name (FQDN)	18
2.4.4 Group Policy Object (GPO)	18
2.4.5 Windows Server Update Services (WSUS)	20
2.4.6 WPKG	21
2.4.7 Internet Information Services (IIS)	21
3 METODOLOGIA	22
3.1 Hardware utilizado	22
3.2 Ferramentas utilizadas	22
3.3 Cenário de desenvolvimento	23
4 PROPOSTA IMPLEMENTADA	24
4.1 Planejamento do modelo de gerência	25
4.1.1 Criação do diretório	26
4.1.2 Criação dos usuários	28
4.1.3 WSUS	29
4.1.4 Automatização de implantação e atualização de <i>software</i> utilizando WPKG e PSE- XEC	33

4.2 Utilização do sistema de emissão de ticket e abertura de chamados com base de conhecimento integrada osTicket.....	34
4.3 Implementação de website para manipulação remota de operações de manutenção do AD – RemoteAD	36
5 CONSIDERAÇÕES FINAIS.....	41
5.1 Trabalhos futuros	42
REFERÊNCIAS	43
ANEXOS	48

1 INTRODUÇÃO

Com o avanço da tecnologia no mundo moderno, e à medida que as redes de computadores e a quantidade de dispositivos aumentam, tornando-se cada vez mais importantes para as organizações, cresce a necessidade da utilização de ferramentas capazes de gerenciar com eficácia os equipamentos que estão a ela conectados (ZANELATTO et al., 2010). O crescimento das redes institucionais, de órgãos públicos e de empresas, fez com que se tornassem mais complexas com o passar do tempo, apresentando-se com um mal dimensionamento, enorme heterogeneidade de dispositivos conectados e vários problemas de segurança (SOARES, 2012). O gerenciamento de redes é feito pelo setor de Tecnologia de Informação (TI), presente hoje em empresas e organizações de qualquer porte.

De acordo com (TORRES, 2011), a TI surgiu como uma fusão entre as áreas de informática e de telecomunicações, viabilizando a comunicação e assim integrando todas as áreas existentes dentro de uma organização através da rede. Segundo ele, “Os assuntos relacionados à área de TI são um ponto crucial na gestão das organizações devido à importância das redes de comunicação e das informações integradas no apoio para que empresas atinjam seus objetivos estratégicos.”.

Segundo (LÔBO, 2011), com as empresas cada vez mais dependentes da Tecnologia da Informação para crescer, torna-se imprescindível um melhor gerenciamento da TI a fim de que os altos investimentos realizados nesse setor possam agregar valor às empresas.

Houve, assim, uma mobilização para a criação de metodologias, padrões e técnicas para contornar dos potenciais problemas de TI, surgindo posteriormente diversos *frameworks* que continham essa finalidade. O autor (MORAES; MARIANO, 2014) cita alguns deles como exemplos, como: ITIL, CobIT, CMMI, PMBOK, BSC e ISO 20000.

O modelo ITIL (Information Technology Infrastructure Library) é um padrão e referência mundial no quesito de boas práticas na área de gestão de TI, abordando todos os assuntos que são importantes no fornecimento e prestação de serviços de informação, auxiliando no atendimento ou nas necessidades do cliente (QUEIROZ, 2012).

1.1 Motivação

A motivação para este trabalho surgiu ao verificar-se a situação da infraestrutura de TI do Centro de Ciências Sociais e Humanas (CCSH) na UFSM no período anterior ao ano de

2014, onde foi encontrada uma situação precária e insustentável de gerência instalada, não havendo controle algum sobre computadores, usuários, permissões, processos computacionais, segurança, e registro de suporte. Frequentemente havia relatos de problemas com equipamentos, devido a infecção por malware, erros, falhas de *hardware/software*, problemas de conexão, entre outros. Esse cenário é comum em vários locais da UFSM.

O Centro de Processamento de Dados (CPD) possui metodologias próprias para a tentativa de contorno dos diversos problemas de TI da universidade, porém, com a grande demanda de atendimento e com o crescimento alavancado da rede da instituição, não é suficiente para o gerenciamento local do Centro.

1.2 Objetivos

Este trabalho de conclusão de curso tem como objetivo implantar, dentro do Centro de Ciências Sociais e Humanas, um ambiente gerenciável de TI executado em um ecossistema organizacional Microsoft, o qual provê uma gama de ferramentas, serviços e utilitários para que seja possível a centralização, integração e manipulação dos diversos recursos e equipamentos pertencentes à rede. Foi construído um diretório de objetos e, nele, integrado computadores, usuários e políticas para um melhor controle do ambiente. Juntamente com o diretório, houve a instalação de ferramentas para gerenciar e aumentar a automação de atualizações de softwares.

Também será feita a instalação e integração do osTicket, um sistema de help desk para abertura de chamados, prestação de suporte técnico e registro de conhecimento, bem como uma central de gerência web para a realização das principais tarefas via internet, batizada de RemoteAD.

Todo o conjunto abrangerá laboratórios de informática, salas de aula, e parte dos funcionários e bolsistas do Centro.

Espera-se, ao final desse trabalho, integrar diversas soluções com a finalidade de suprir os inúmeros problemas atualmente relevantes no CCSH, como controle e eliminação de vírus e malwares, manutenção e atualização preventiva das máquinas, atendimento e controle de chamados de suporte e gerência remota do ambiente, de uma forma a otimizar tempo e recursos humanos.

2 REVISÃO BIBLIOGRÁFICA

2.1 Conceituação de gerência de redes de computadores

A gerência de redes está associada ao controle das atividades e monitoramento do uso dos recursos, englobando métodos para configurar, controlar, monitorar, corrigir falhas e administrar redes de computadores e telecomunicações (MARTINS et al., 2002).

Existem algumas subdivisões dentro do conceito de gerência de redes de computadores, propostas por diferentes órgãos reguladores de padrões.

O gerenciamento de redes, de acordo com a Internet Engineering Task Force (IETF), utiliza o protocolo SNMP, que possui seu funcionamento baseado na pilha de protocolos TCP/IP e tem o objetivo de ser simples e flexível. Utiliza a base de dados MIB (*Management Information Base*), onde estão os objetos que serão gerenciados e manipulados pelos agentes. O SNMP possui os seguintes elementos: dispositivos gerenciados, agentes (contendo a MIB), e o sistema de gerenciamento central. Os agentes têm o papel de atender às requisições do gerente, comunicando-se com a base de dados MIB e enviando a esse gerente os dados quando necessário. O protocolo SNMP não garante consistência de dados, pois utiliza o protocolo UDP para comunicação e transporte de informações (IETF, 1990), podendo, também, ser utilizado sobre o protocolo TCP para comunicação segura (IETF, 2002).

Sob a visão da ISO, o gerenciamento de redes deve ser robusto, orientado a objetos e seguro. Com isso, foi definido o padrão OSI/ISO, o qual funciona com base na pilha OSI e define a gestão de rede em cinco categorias, chamado de FCAPS (acrônimo para cada categoria), são elas: Gerenciamento de Falhas, Gerenciamento de Configuração, Gerenciamento de Contabilidade, Gerenciamento de Performance e Gerenciamento de Segurança.

O autor (SIMÕES, 2010) explica essas cinco categorias a seguir.

- Gerenciamento de Falhas - tem como objetivo manter a rede funcional e sem falhas, monitorando, diagnosticando, corrigindo e isolando falhas de modo pró-ativo.
- Gerenciamento de Configuração - consiste na descoberta de rede, os dispositivos que lhe pertencem que serão monitorados, assim como os recursos e serviços.
- Gerenciamento de Contabilidade - é a forma que a organização tem de garantir o lucro a partir dos serviços que disponibilizam.

- Gerenciamento de Desempenho - implica que se monitore a rede, realizando ajustes e alterações a fim de manter um desempenho dentro dos padrões sem influenciar negativamente seus utilizadores.
- Gerenciamento de Segurança - divide-se: em gestão da segurança e segurança da gestão, sendo o primeiro relacionado às operação e utilização feitas somente por pessoas autorizadas, sendo limitado e restrita o uso para os demais; e a segunda relativa à segurança da rede, com a utilização de mecanismos de defesa e monitoramento de pacotes para detectar anomalias e ameaças.

O trabalho tem o foco na realização do Gerenciamento de Segurança de forma superficial, de forma a aperfeiçoar a segurança do local com a aplicação de novas políticas de acesso, maiores restrições e proteção contra ameaças.

De acordo com (MAGALHÃES; PINHEIRO, 2007),

O Gerenciamento de Serviços de TI visa alocar adequadamente os recursos disponíveis e gerenciá-los de forma integrada, fazendo com que a qualidade do conjunto seja percebida pelos seus clientes e usuários, evitando-se a ocorrência de problemas na entrega e na operação dos serviços de Tecnologia da Informação.

Para os autores, a fim de se alcançar esse objetivo, uma tática adotada é o gerenciamento dos processos de TI de acordo com o modelo ITIL.

O ITIL (Information Technology Infrastructure Library) é um modelo desenvolvido pelo CCTA (Central Computer and Telecommunications Agency), no final dos anos 80, e classifica-se como um conjunto de melhores práticas às áreas de TI, propiciando a construção de um caminho entre o nível “Caótico” e o nível “Valor” (LÔBO, 2011). É usado como referência para aperfeiçoar a governança e os serviços de TI, pois cada vez mais esses serviços dão suporte aos principais processos das empresas (SANTOS, 2014a).

O ITIL v3 sugere um ciclo de vida composto de 5 fases (BRIGANÓ; BARROS, 2010), sendo elas:

- Estratégia do Serviço: Analisa a viabilidade do serviço para a organização, levando-se em conta os serviços que já existem ou que possam surgir.
- Desenho do Serviço: O serviço pensado é modelado no que diz respeito aos seus recursos, práticas, técnicas, conhecimento e tempo, para que a implantação seja possível em um momento posterior.

- **Transição de Serviço:** Todos os recursos planejados são providenciados e alocados, para que o serviço opere com o mínimo de intercorrências possível.
- **Operação de Serviço:** O serviço começa a ser utilizado para suprir as demandas existentes.
- **Melhoria Contínua do Serviço:** Resume-se em acompanhar o serviço e verificar a necessidade de mudanças, correções e melhorias.

Para (LUNARDI, 2008), manter os recursos e serviços de TI alinhados à estratégia organizacional, gerenciando a inovação, os riscos e as mudanças, e estimando impactos de novos projetos tecnológicos, são atribuições da governança de TI.

2.2 Cenário atual

Há três paradigmas para gerenciamento de redes de computadores, são eles: centralizado, hierárquico e cooperativo, divididos em duas categorias, podendo ser fracamente distribuídos ou fortemente distribuídos (ROSA, 2007).

Para o paradigma centralizado, existe uma central de gerência, instalada em servidores ou estações de trabalho, e contam com um gerente, um banco de dados, e um processo de gerência com apenas um ponto de acesso.

Para o paradigma hierárquico, utiliza-se, além de um servidor central, servidores clientes, que podem atuar como gestores das mesmas tarefas (ROSA, 2007).

O paradigma cooperativo usa como estratégia a combinação das duas metodologias anteriores, com suas respectivas vantagens, porém distribuindo a base de dados para diversos servidores espalhados, evitando a dependência de um único sistema. O processamento de informações ocorre com delegação horizontal, não havendo necessariamente uma hierarquia envolvida. (ROSA, 2007).

Há ferramentas e protocolos que suportam os três paradigmas, não ficando restritos a um deles apenas. Tem-se como exemplo: IBM Netview (IBM, 2014), HP Network Node Manager (HP, 2014a), Cisco Prime (CISCO, 2014), Trauma Zero (IVIRTUA, 2014), Nagios (NAGIOS, 2014), HP Business Technology Optimization (HP, 2014b), EBX5 (ORCHESTRA, 2014), Zabbix (ZABBIX, 2014), SNMP (IETF, 1990), RMON (IETF, 1991), etc.

A utilização de outras ferramentas, juntamente com uma gerência centralizada, hierárquica ou cooperativa aumentam a capacidade e o controle do administrador sobre o ambiente.

Pode-se citar algumas como:

- PSEXEC é um utilitário que permite executar comandos de terminal remotamente através da rede, sem a necessidade de se fazer presente no local de interesse. Semelhante ao SSH dos sistemas Unix.
- Wake-On-Lan é um pequeno programa que envia Magic Packets pela rede para “acordar” um computador que esteja previamente configurado aceitar esses pacotes.

2.3 Trabalhos correlatos

O autor (SANTOS, 2014b) utilizou o protocolo LDAP e autenticação Kerberos para transformar computadores que executam Linux em Controladores de Domínio, e assim atuar juntamente com servidores Windows no Active Directory, permitindo autenticações dos usuários e edição da estrutura do diretório.

Sua aplicação pode permitir que, em ambientes que utilizam a gerência de recursos baseada em LDAP, haja uma comunicação entre diferentes plataformas, permitindo que sistemas Unix-like se comuniquem com plataformas com um sistema Microsoft. No presente trabalho, essa aplicação pode permitir que hajam substituições futuras dos sistemas operacionais dos servidores para distribuições Linux sem causar um grande impacto na funcionalidade do diretório.

Os autores (BRIGANÓ; BARROS, 2010) implantaram um sistema automatizado de service desk aplicando conceitos do ITIL e PMBOK no Centro de Ciências Exatas da Universidade Estadual de Londrina, onde foram coletados dados quantitativos e estatísticos da situação anterior do suporte, e criando um modelo genérico para adaptá-lo às necessidades do Departamento onde estava localizado. Foi utilizada a ferramenta Eventum, que desempenhou toda a automação de atividades pertencentes a um sistema de service desk.

Essa implantação, junto com o seu uso contínuo, foi importante para realizar os refinamentos e correções necessárias no ambiente, que, posteriormente, fora disponibilizado para os demais departamentos do local. Uma breve referência sobre a utilização da metodologia ITIL e dos processos de implantação dos autores foram estudadas para aplicar neste trabalho, e pode permitir, futuramente, uma possível mudança do sistema de help desk instalado para um sistema de service desk com novas amplitudes, prioridades e tarefas.

2.4 Conceituação das ferramentas e protocolos utilizados

A seguir, serão conceituadas as ferramentas e protocolos que compõem este trabalho, para uma melhor compreensão da solução proposta. Cada ferramenta e protocolo apresentado se faz presente na proposta deste trabalho, agindo direta ou indiretamente na formação e operação do ambiente.

2.4.1 Active Directory Domain Services (AD)

Criado pela Microsoft, é um diretório de objetos armazenado em uma base de dados, o qual é executado em um servidor promovido a controlador de domínio (DC), substituindo o antigo diretório SAM utilizado em sistemas Windows NT 4.0. Nesse diretório são cadastrados os recursos da rede que irão fazer parte desse domínio, tais como: computadores, usuários, impressoras, servidores, compartilhamentos, periféricos, etc, permitindo ao administrador controlar, centralizar e agrupar esses objetos (THOMPSON, 2010). A Figura 2.1 representa genericamente uma estrutura Active Directory com os triângulos representando os domínios, organizados hierarquicamente; a elipse representando uma floresta, a qual é um agrupamento de domínios; e alguns componentes internos de um domínio, tais como: grupos, computadores, usuários, unidades organizacionais e fila de impressão.

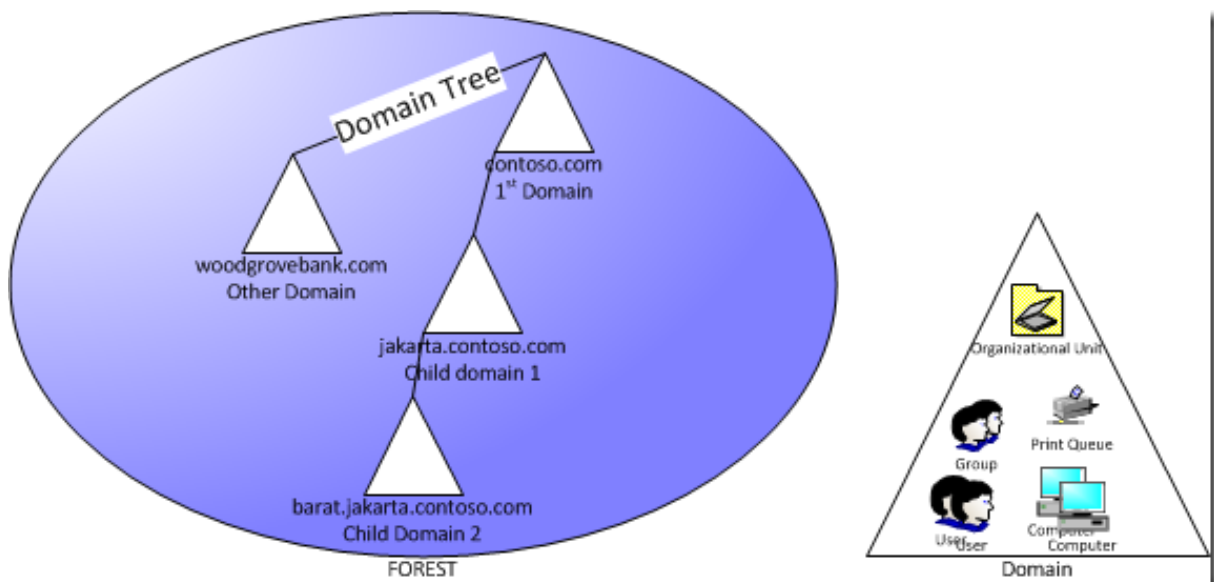


Figura 2.1 – Exemplo de um diretório AD (MICROSOFT, 2014a)

O AD usa o protocolo LDAP para organizar hierarquicamente os recursos internos, e faz a autenticação dos mesmos através do protocolo Kerberos versão 5, que utiliza um autenticador

para validar os tickets dos clientes e autorizá-los a usar os recursos da rede (OLIVEIRA, 2013).

2.4.1.1 Usuários do AD

Podem ser de dois tipos: usuário Administrador e usuário Padrão/Limitado (muito semelhante aos sistemas Unix/Linux), e são considerados um tipo de objeto pelo protocolo LDAP, contendo seus atributos, e assim armazenados no diretório. Um usuário do diretório pode acessar sua conta em qualquer computador que esteja cadastrado no AD, sem necessidade de ser criada uma conta para cada máquina onde aquele usuário irá utilizar. Porém o administrador pode alterar essa regra, podendo restringir um usuário a certas máquinas.

2.4.1.2 LDAP

Significa Lightweight Directory Access Protocol, e foi publicado primeiramente como RFC 1777 (IETF, 1995). Esse protocolo é o sucessor do DAP, criado na década de 1980, e o substituiu por questões de consumo de banda e pilha de rede utilizada. A partir de agora usa a pilha TCP/IP ao invés da OSI, usada no DAP (THOMPSON, 2010).

Esse protocolo é multiplataforma e formado por um conjunto de protocolos cliente/servidor utilizado para acessar um determinado diretório e suas informações, bem como com a possibilidade de navegação, leitura, escrita e consulta. O protocolo aborda um diretório formado por diversas nomenclaturas, representando hierarquias (OPENLDAP, 2003), tais como:

- UID: UserID – Identificador único obrigatório, semelhante a uma chave primária;
- DN: Distinguished Name – Identificador único para um objeto, abrange o caminho completo da árvore até o objeto em questão;
- RDN: Relative Distinguished Name – Identificador relativo de um objeto, abrange apenas o UID;
- DC: Domain Component – Subdivisões do domínio da aplicação;
- OU: Organizational Unit – Unidade Organizacional, agrupamento de objetos que contém finalidades semelhantes;
- CN: Common Name – apelido do usuário;
- Entre outros.

A Figura 2.2 ilustra a estrutura de um diretório LDAP tradicional (esquerda) e para a internet (direita).

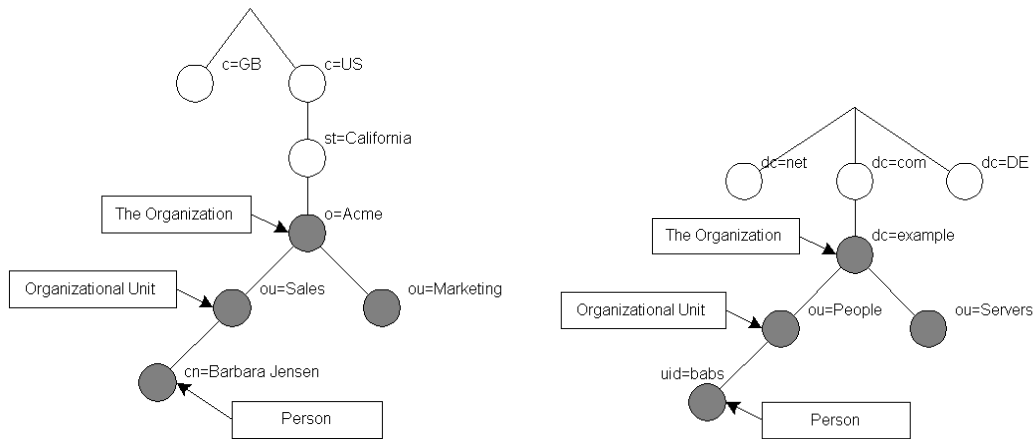


Figura 2.2 – Exemplo genérico de uma hierarquia LDAP (OPENLDAP, 2003)

2.4.1.3 Domínio

Representa um perímetro administrativo para os objetos do AD, compartilhando as mesmas regras, políticas, e relações de confiança com outros domínios (THOMPSON, 2010). Um domínio pode ter milhões de objetos em seu interior (MICROSOFT, 2003).

2.4.2 Controlador de Domínio

É um servidor do AD que possui privilégios para guardar o diretório, alterá-lo, pesquisá-lo, e gerenciar as autenticações de computadores e usuários na rede (MICROSOFT, 2005a). Nem todo o servidor incluso no diretório necessita ser um controlador de domínio.

2.4.3 Fully Qualified Domain Name (FQDN)

Um FQDN é o nome de domínio completo para um host específico na rede, e consiste em duas partes: o nome do host e o nome do domínio (UNIVERSITY, 2014). Por exemplo, para um computador nomeado “foo” e um domínio nomeado “bar.com”, o FQDN da máquina será foo.bar.com.

2.4.4 Group Policy Object (GPO)

Permite que políticas e configurações específicas sejam aplicadas nas máquinas e nos usuários do AD. Cada política é aplicada a uma ou várias Unidades Organizacionais (OUs), encadeando-se e aplicando-se com uma precedência conforme a ordem em que seja ajustada (MICROSOFT, 2011a). A Figura 2.3 exibe um diretório AD (representado pelo triângulo),

suas OUs (representadas pelas elipses) e as políticas (representadas pelos quadriláteros). Na parte de baixo da mesma é exibida a ordem em que as políticas são aplicadas em duas OUs, Servers e Marketing.

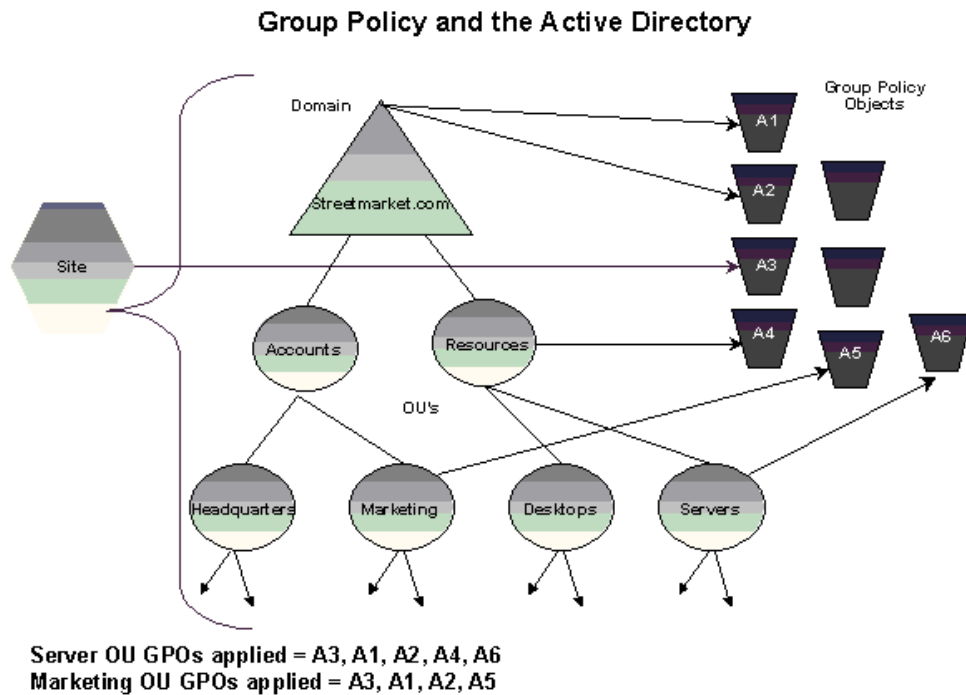


Figura 2.3 – Exemplo de aplicação de políticas de grupo em unidades organizacionais diferentes (MICROSOFT, 2014b)

A política A3 está sendo aplicada em todo o conjunto (*site*), abrangendo o domínio e suas OUs. Logo após a aplicação de A3, as políticas A1 e A2, da mesma forma, são impostas em todas as OUs filhas, pois estão em um escopo global do domínio e abrangem toda as suas subárvores. Descendo-se um nível da hierarquia, existe a política A4, a qual está aplicada na OU *Resources*, e essa mesma política será herdada por todo e qualquer objeto dentro dessa OU e não afetará as outras unidades que estão no mesmo nível, tal como a OU *Accounts*. Por fim, no nível das unidades folhas, é aplicada a política A5 na OU *Marketing* e A6 na OU *Servers*.

Um exemplo prático de algumas funções que podem ser configurados no GPO são: proibir o acesso a certas funções do computador, bloquear o acesso a certas URLs na internet, definir programas que serão inicializados e permitidos em cada máquina, não permitir a execução de certos tipos de arquivos, entre inúmeros outros.

2.4.5 Windows Server Update Services (WSUS)

É uma ferramenta que gerencia, controla e autoriza as atualizações do sistema operacional Windows para os clientes do AD. É composto por 3 componentes (MICROSOFT, 2011b):

- Site da Microsoft: Permite que sejam baixadas as atualizações e seus metadados;
- Servidor WSUS: É a máquina que oferece a interface para o administrador, e onde será armazenado os binários baixados, seus metadados, e onde se realiza todas as operações internas a fim de distribuir e aplicar atualizações às máquinas clientes;
- Windows Update: *Software* instalado em qualquer cliente Windows e que tem como finalidade baixar atualizações diretamente da Microsoft ou de um servidor WSUS.

As atualizações são compostas de duas partes:

- Binário: Arquivo da atualização propriamente dito, o qual será executado e instalado nas máquinas alvo;
- Metadados: Informações requeridas para instalar a atualização, contém as propriedades da atualização, regras de aplicabilidade, para determinar se alguma delas necessita ou não ser instalado em um determinado computador, e informações de instalação, que disponibiliza as opções de linha de comando.

O WSUS apresenta seguintes vantagens:

- Integração completa com o AD;
- Gerência centralizada de atualizações aprovadas e recusadas;
- Agrupamento e separação de máquinas;
- Gerador de relatórios contendo estatísticas sobre êxito ou falha na instalação das atualizações através do *software* Report Viewer;
- Fácil replicação para demais servidores WSUS na rede, sendo todas as aprovações e binários e metadados sincronizados entre eles;
- Economia de banda externa quando a máquina realiza o download das atualizações, pois irá verificar no servidor WSUS e não na internet.

Como desvantagem, o WSUS ocupa grande espaço em disco rígido, dependendo da quantidade de atualizações relevantes e necessárias.

2.4.6 WPKG

Consiste em um serviço de instalação e atualização automática de *softwares* de terceiros em computadores clientes através de configurações em arquivos XML e execução por scripts.

2.4.7 Internet Information Services (IIS)

É uma plataforma para hospedagem de sites, serviços e aplicativos nativa do sistema operacional servidor. Integra serviços FTP e frameworks como ASP.NET, PHP e WCF (MICROSOFT, 2012).

3 METODOLOGIA

Este trabalho foi modelado em três partes: a montagem do ambiente com suas ferramentas, a implantação do sistema de help desk e a criação da central de gerência via web. Na primeira parte, são detalhadas a instalação dos servidores que atuarão como pilares do ambiente, a criação e configuração do diretório, usuários, ferramentas de manutenção, e integração das máquinas à infraestrutura. A segunda parte terá como alvo a implantação e execução do sistema de help desk osTicket, justificando a escolha do *software* e detalhando alguns passos do processo. A terceira parte abrangerá a criação do website RemoteAD que tem como finalidade a gerência remota do ambiente.

3.1 Hardware utilizado

Foram utilizados dois desktops workstations que atuarão como servidores do ambiente. O servidor principal (HP) contém um processador AMD Phenom II X4 com 4 núcleos operando a 3.2GHz, 4GB de memória RAM, e 500GB de disco rígido. O servidor reserva (DELL) contém um processador Intel Core i5-3570 com 4 núcleos operando a 3.4GHz, 12GB de memória RAM, e 1TB de disco rígido. As duas máquinas executarão o sistema Windows Server 2008 R2 Enterprise Service Pack 1. O servidor com *hardware* mais fraco foi empregado como principal em função da disponibilidade no momento da instalação, sendo o novo servidor adquirido instantes depois.

3.2 Ferramentas utilizadas

As ferramentas que foram utilizadas, descritas na seção 2.4, para a realização dessa primeira etapa são: Active Directory Domain Services (AD), Group Policy Object (GPO), Windows Server Update Services (WSUS), WPKG e PSEXEC.

As ferramentas acima foram escolhidas dentre diversas analisadas, e a decisão de escolha foi influenciada principalmente pela unificação de plataforma, integração de serviços e sua fácil configuração. Optou-se pelo uso primeiramente de ferramentas gratuitas, para não haver investimento financeiro, porém o sistema operacional dos servidores é um *software* comercial, e foi em período de avaliação.

Para a segunda etapa, onde será inicializado o serviço de help desk, foram utilizadas as

seguintes ferramentas: Internet Information Services (IIS), Servidor PHP, osTicket e MySQL.

A terceira etapa utilizou, para a implementação do website de gerência, as ferramentas e framework seguintes: Internet Information Services (IIS) e ASP.NET.

3.3 Cenário de desenvolvimento

O local de desenvolvimento foi no Centro de Ciências Sociais e Humanas da Universidade Federal de Santa Maria, onde existem laboratórios de informática com 99 computadores, salas de aula com 36 computadores, e secretarias e direção com 18 computadores. Há dois tipos de usuários na unidade universitária: Alunos e funcionários.

Este trabalho não cobriu todos os computadores do CCSH, pelo motivo da falta de maior controle sobre a rede pelo baixo número de funcionários e bolsistas para a instalação, implantação e manutenção.

4 PROPOSTA IMPLEMENTADA

Após observar e analisar os diversos problemas que atingiam parte dos computadores do CCSH, tais como: vírus, lentidão, erros, sistemas vulneráveis e desatualizados; foi elaborada uma proposta para minimizar os mesmos, com a criação de um protótipo envolvendo a instalação de um modelo de gerência e modelo de suporte. O ambiente contém três atores principais: o Administrador, o Agente e o Usuário.

O Administrador, o qual tem o controle universal do ambiente, tem acesso às ferramentas de atualização do sistema operacional e *softwares* (WSUS e WPKG), controle sobre o diretório e seus objetos (Active Directory), seus recursos e políticas (Group Policy Object), permissão para usar o website de gerência remota (RemoteAD), bem como a abertura e fechamento de chamados de suporte (osTicket). O Agente, que é o bolsista que irá realizar o suporte, possui permissões apenas para a abertura, resolução, e fechamento de chamados (osTicket), não ficando responsável pela operações de atualização e controle do diretório. O Usuário, o qual é o aluno ou funcionário, poderá realizar a abertura de chamados (osTicket) e autenticar-se como usuário da rede através de um computador cadastrado no AD. A Figura 4.1 exibe um diagrama de caso de uso com a interação dos atores que foram abordados e suas possíveis ações.

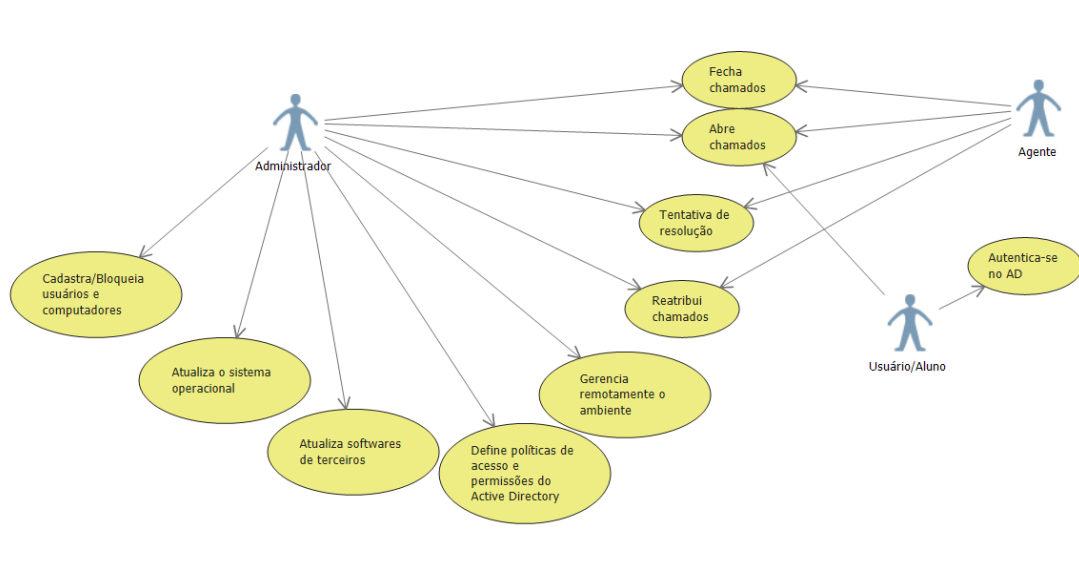


Figura 4.1 – Diagrama de caso de uso com a interação entre atores e suas ações (autoria própria)

4.1 Planejamento do modelo de gerência

Inicialmente houve um planejamento e analisou-se as fases do ITIL para o desenvolvimento do trabalho. A seguir serão descritas cada fase no contexto proposto.

- **Estratégia do Serviço:** Houve um estudo prévio do cenário para análise dos problemas e das necessidades da unidade universitária, para que a implantação do sistema de gerenciamento pudesse ocorrer de uma maneira natural.
- **Desenho do Serviço:** As tarefas foram divididas conforme o tempo e o pessoal disponíveis, selecionando quais técnicas, *softwares* e paradigmas serão escolhidos para posteriormente.
- **Transição de Serviço:** Etapa onde se adquiriu os recursos, servidores, periféricos e *softwares* em questão, para início da implantação e instalação dos componentes. Houve também o treinamento dos administradores e bolsistas para a operação dos serviços que serão prestados.
- **Operação de Serviço:** Após a transição, o ambiente está pronto para começar sua operação, com a equipe do laboratório analisando os dados e status dos serviços, e colhendo *feedback* a partir dos resultados.
- **Melhoria Contínua do Serviço:** Para esta etapa, verifica-se a necessidade de mudanças e melhorias na implantação, através de informações extraídas do dia-a-dia do setor. A Figura 4.2 exhibe esse processo.

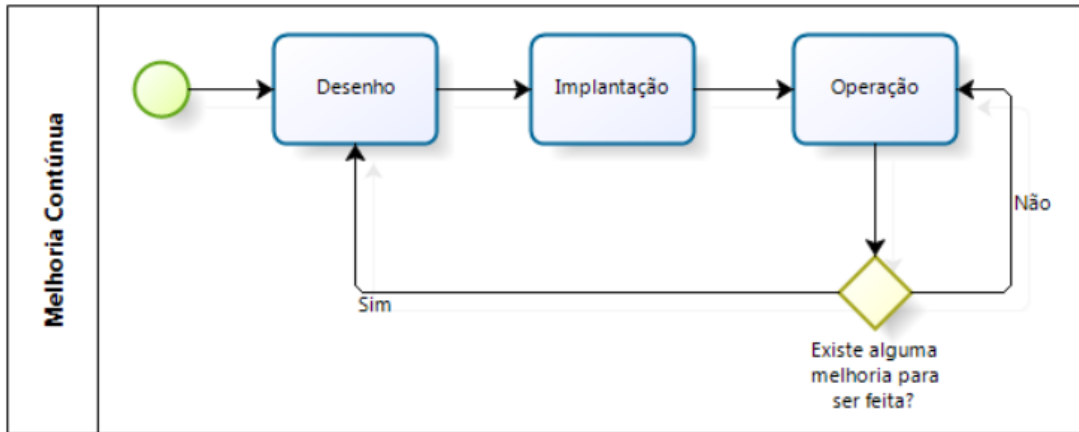


Figura 4.2 – Diagrama de atividade para a melhoria contínua do sistema (BRIGANÓ; BARROS, 2010)

4.1.1 Criação do diretório

Para começar o projeto, instalou-se o AD nos dois servidores iniciais, configurando-se para que agissem como réplicas entre si, permitindo assim que sejam aplicadas alterações de qualquer natureza no diretório em um modo bidirecional, garantindo o funcionamento do mesmo caso uma das máquinas esteja inoperante. Em seguida, houve instalação de dois servidores DNS, aplicados em ambas as máquinas, operando igualmente em réplicas como feito no AD. O serviço de DNS é necessário para a correta operação do diretório.

Os nomes dados aos servidores são: “WIN-AD” (principal), “WIN-BACKUP” (réplica e backup).

O próximo passo foi promover ambos os servidores para se tornarem Controladores de Domínio, para que fossem capazes de criar o domínio que abrigará o diretório propriamente dito. O nome do domínio escolhido foi: “server0.ccsb.br”, e todas as máquinas que forem integradas terão o seu FQDN com este final.

A partir desse momento, foram criadas as Unidades Organizacionais (OUs) para cada setor do CCSH. Essas OUs são agrupamento de objetos para atribuição de uma ou várias políticas de grupo (GPO). A Figura 4.3 descreve a estrutura da árvore das OUs criadas e suas respectivas GPOs. Como especificado anteriormente, uma GPO será aplicada no diretório em que está designada e em todos os seus subdiretórios.

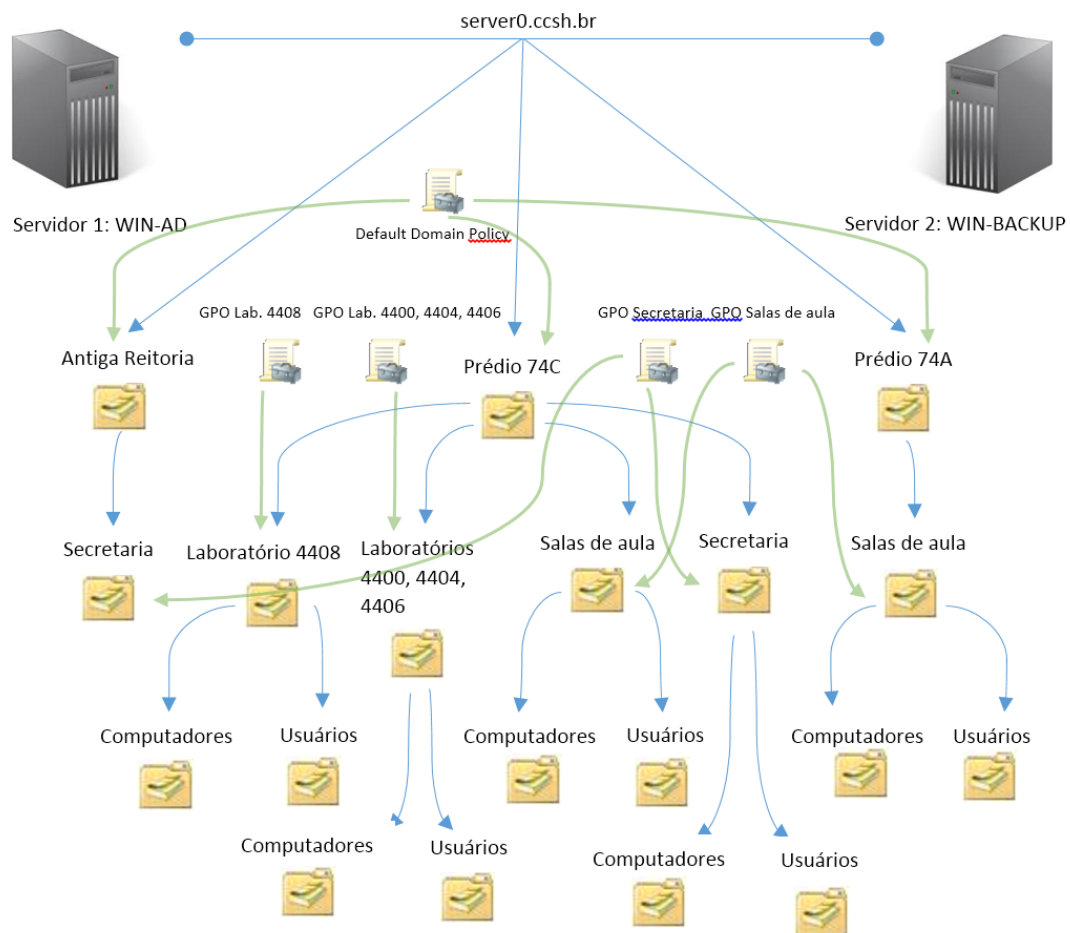


Figura 4.3 – Estrutura em árvore do diretório do AD para o CCSH (setas azuis), juntamente com suas respectivas políticas (setas verdes) (autoria própria)

A figura mostra a hierarquia LDAP de uma estrutura de diretório do Active Directory. Existem os dois servidores centrais que mantêm o controle e a consistência do diretório, e a partir do domínio criado, ocorrem diversas ramificações representando as Unidades Organizacionais (OU). Para o fluxo das setas azuis, foi dividido entre três unidades principais, representando cada prédio do CCSH onde a implantação foi aplicada. Para a próxima ramificação, dividiu-se entre os setores internos do CCSH em cada unidade, abrangendo os laboratórios, salas de aula, e secretaria. E por fim, as unidades organizacionais das folhas da árvore, dividem-se entre Computadores (abrangendo os computadores cadastrados do setor indicado pelo OU pai) e Usuários (abrangendo os usuários cadastrados do setor indicado pelo OU pai).

Por outro lado, o fluxo das setas verdes representam a hierarquia de políticas de grupo (GPO) aplicadas em cada OU. Inicia-se com o GPO mais genérico e padrão do sistema, chamado de *Default Domain Policy*, o qual é aplicado em todas as unidades raiz. Um nível abaixo se encontram as GPOs específicas para cada setor, tendo para os laboratórios, salas de aula e

secretarias, e vão ser aplicadas na subárvore de OUs correspondente. Cada GPO pode ser reutilizado para diferentes subárvores de OUs, não sendo necessária duplicação e cópias adicionais.

Integrou-se ao diretório todos os computadores presentes em salas de aula, auditórios e laboratórios do CCSH, incluindo algumas máquinas que são usados por alunos com bolsa de estudos e funcionários, totalizando 153 máquinas, divididas em seus respectivos OUs conforme o local e a aplicação da estação de trabalho.

4.1.2 Criação dos usuários

No ambiente atual de ensino da UFSM, normalmente não são usados usuários individuais para cada funcionário ou aluno, mas sim, genéricos. Um exemplo disso é o usuário “pccli”, o qual é usado na maioria dos Centros e Unidades Administrativas dentro da instituição.

Tendo esse fato em mente, manteve-se usuários do AD genéricos da mesma forma, diferenciando apenas os usuários usados pelos servidores públicos dos usuários de alunos.

Para suprir a atual necessidade, criou-se 12 usuários, dividindo-os conforme as duas colunas centrais da Tabela 4.1:

Tabela 4.1 – Divisão de conta de usuário por arquitetura

Usuário X Arquitetura	Máquinas 32-bits	Máquinas 64-bits	Perfil Viajante Mandatário
Administrador	"kevin"	"kevin"	Não
Funcionários e bolsistas	"pccli"	"pccli"	Não
Laboratório 4408	"lab4408"	-	Sim
Laboratório 4406	"lab4406"	"lab4406_64"	Sim
Laboratório 4404	"lab4404"	"lab4404_64"	Sim
Laboratório 4400	"lab4400"	"lab4400_64"	Sim
Sala de aula - 74C	"sala74c"	"sala74c_64"	Sim
Sala de aula - 74A	"sala74a"	-	Sim

Todos os usuários, com exceção de “pccli” e “kevin”, foram configurados para usar Mandatory Roaming Profile (perfil viajante mandatário) (MICROSOFT, 2005b). O perfil é chamado de “viajante” porque é transferida pela rede sempre que um usuário se autentica no AD, e é chamado “mandatário” pois não pode ser sobrescrito e alterado por usuários com privilégios limitados, apenas pelo administrador.

Essa funcionalidade permite que a pasta pessoal do usuário, contendo o perfil, ícones, plano de fundo, preferências, documentos, entre outros, resida no servidor principal, sendo fixo, somente leitura, e a cada inicialização de uma máquina cliente é transferida para a mesma,

sobrescrevendo o perfil local antigo com uma nova imagem. É um modelo útil para desfazer quaisquer alterações e personalizações que usuários por ventura consigam fazer nas máquinas, agindo semelhantemente aos *softwares* de gerência descentralizados, como o Shadow Defender por exemplo, porém a nível de perfil e não a nível de sistema.

O grande número de usuários diferentes pode ser justificado pelos problemas entre arquiteturas 32-bits e 64-bits em relação ao perfil viajante mandatório usado, e também pela diferentes configurações e *softwares* que cada local oferece. Ao se usar um perfil 32-bits em um ambiente 64-bits, percebeu-se problemas com atalhos, redirecionamentos e inconsistências.

Com a criação dos usuários concluída, o próximo passo exhibe a manipulação do serviço de atualização para manter os sistemas clientes atualizados utilizando a ferramenta WSUS.

4.1.3 WSUS

Para o WSUS (serviço de atualização dos sistemas Windows), primeiramente deve-se escolher as plataformas que irão ser atualizadas, para que o servidor faça o download necessário. Foram eleitas, levando-se em consideração a atual situação e necessidade do CCSH, as plataformas: Windows (XP, 7, 8 e 8.1, Server 2008 R2, Server 2012 R2), Office (2010 e 2013), Runtimes do Visual Studio (2005-2013), Silverlight, SQL Server (2000-2012).

Dividiu-se os 154 computadores cadastrados no AD em 8 grupos de atualização, conforme seu local de atuação, sendo eles: Secretaria, Salas de aula (74A e 74C), Laboratórios (4408, 4406, 4404 e 4400).

A Figura 4.4 mostra os grupos formados do lado esquerdo do console de administração, e do lado direito algumas estatísticas e gráficos sobre a atual situação das máquinas. Pode-se ver que 30 computadores estão necessitando de atualizações e 420 delas são necessárias nessas máquinas. Essa ferramenta permite ao gerente um grande dinamismo sobre a situação, pois oferece uma visão global das máquinas que estão necessitando de atualizações em apenas uma única interface.

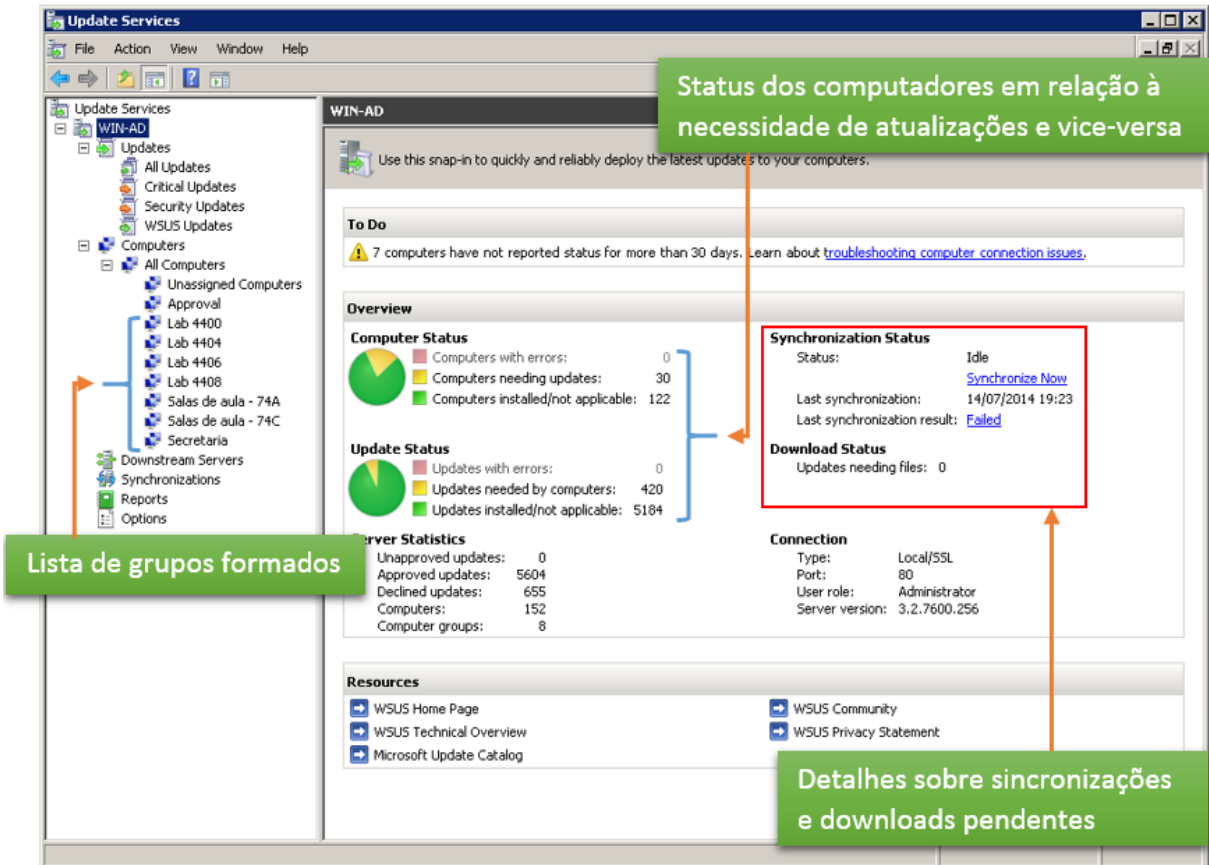


Figura 4.4 – Console de administração do WSUS exibindo estatísticas e dados atuais sobre o status das máquinas (autoria própria)

Por padrão, os computadores clientes não são redirecionados para o servidor WSUS automaticamente a fim de realizar a instalação das atualizações. Para que os mesmos tomem esse servidor como referência, é preciso alterar algumas regras nos GPOs aplicado na(s) sua (s) OU(s) (MICROSOFT, 2011c), tais como:

- Automatic Updates detection frequency: Enabled, configurado para reportar status para o servidor a cada 22 horas e verificar se há atualizações pendentes e aprovadas para o seu grupo;
- Configure Automatic Updates: Enabled, e configurado para a opção ‘4’, onde o download e instalação das atualizações são feitas automaticamente todas as sextas-feiras às 16h;
- Specify intranet Microsoft Update service location: Enabled, onde é inserido o site da intranet do WSUS para ser possível a localização pelos clientes que são aplicados por essa política de grupo, nesse caso: “http://WIN-AD”;

- Turn on recommended updates via Automatic Updates: Enabled, ativa o download das atualizações recomendadas pela Microsoft na lista de instalação;

Conforme as máquinas irão atualizando suas GPOs internas, se configuram automaticamente para usar o servidor local como referência para a transferência de atualizações do Windows Update.

As Figuras 4.5 e 4.6 mostram, respectivamente, a lista de atualizações baixadas que são necessárias e sua taxa de instalação bem sucedida em relação ao total de máquinas, e o *software* Report Viewer exibindo estatísticas de atualização específicas do computador da sala 2364 do Centro, o qual não contém pendências.

The screenshot displays the 'Update Services' console. The left pane shows a tree view with 'Update Services' expanded to 'All Updates'. The main pane shows a table of updates with columns for Title, Classification, Install... (percentage and count), and Approval. A red box highlights the table. Below the table, a detailed view for a selected update (KB2485376) is shown, including a status pie chart, description, and additional details. A green box highlights this detailed view.

Estadística de uma atualização selecionada, tais como: número de máquinas pendentes, sua severidade e dados técnicos específicos

Title	Classification	Install...	Approval
Security Update for Windows 7 (KB2485376)	Security Updates	99% Install (1/10)	
Security Update for Microsoft Outlook 2010 (KB2837597) 32-Bit Edition	Security Updates	91% Install (6/10)	
Definition Update for Microsoft Office 2010 (KB982726) 32-Bit Edition	Definition Updates	91% Install (6/10)	
Update for Microsoft Office 2010 (KB2597087) 32-Bit Edition	Critical Updates	91% Install (6/10)	
Update for Microsoft Office 2010 (KB2589352) 32-Bit Edition	Critical Updates	91% Install (6/10)	
Security Update for Microsoft Office 2010 (KB2553284) 32-Bit Edition	Security Updates	91% Install (6/10)	
Security Update for Microsoft Office 2010 (KB2760781) 32-Bit Edition	Security Updates	91% Install (6/10)	
Security Update for Windows 7 (KB2876331)	Security Updates	91% Install (6/10)	
Cumulative Security Update for ActiveX Killbits for Windows 7 (KB2900986)	Security Updates	91% Install (6/10)	
Update for Root Certificates for Windows 7 [November 2013] (KB931125)	Updates	91% Install (6/10)	
Update for Windows 7 (KB2893519)	Updates	91% Install (6/10)	
Security Update for Windows 7 (KB2868626)	Security Updates	91% Install (6/10)	
Security Update for Windows 7 (KB2868725)	Security Updates	91% Install (6/10)	
Security Update for Windows 7 (KB2862152)	Security Updates	91% Install (6/10)	
Security Update for Windows 7 (KB2864202)	Security Updates	91% Install (6/10)	
Security Update for Windows 7 (KB2862335)	Security Updates	91% Install (6/10)	
Security Update for Windows 7 (KB2847311)	Security Updates	91% Install (6/10)	
Cumulative Security Update for Internet Explorer 8 for Windows 7 (KB287...	Security Updates	99% Install (1/10)	
Security Update for Windows 7 (KB2868038)	Security Updates	91% Install (6/10)	
Security Update for Windows 7 (KB2884256)	Security Updates	91% Install (6/10)	

Lista de atualizações disponíveis, junto de sua categoria, e em quais grupos cada uma deve ser instalada

Status:

Computers with errors:	0
Computers needing this update:	1
Computers installed/not applicable:	151
Computers with no status:	0

MSRC severity: Critical
MSRC number: MS11-007
Release date: terça-feira, 8 de fevereiro de 2011
KB article numbers: 2485376

Description:
 A security issue has been identified that could allow an unauthenticated user to execute arbitrary code on affected systems. You can help protect your system by installing this update from Microsoft Update.

Additional Details:
More information: <http://go.microsoft.com/fwlink/?LinkId=161610>
Removable: Yes
Restart behavior: Can request restart
May request user input: No
Must be installed exclusively: No
Microsoft Software License Terms: This update does not have a license.

Figura 4.5 – Lista de atualizações necessárias e aprovadas em alguns grupos (autoria própria)

The screenshot shows the 'Update Services' console. The main pane displays a table titled 'All Computers (152 computers of 152 shown, 152 total)'. The table has the following columns: Name, IP Address, Operating System, Installed..., and Last Status Report. Two rows are highlighted with a red border:

Name	IP Address	Operating System	Installed...	Last Status Report
sala2364.server0.ccsb.br	2804:0:4000:800c:8c23...	Windows 7 Professional	97%	06/10/2014 13:59
sala4424.server0.ccsb.br	2804:0:4000:800c:789...	Windows 7 Professional	100%	06/10/2014 13:58

Below the table, the 'Computer Detailed Status Report' for 'sala2364.server0.ccsb.br' is shown. It includes the following details:

- Operating System: Windows 7 Professional
- Service Pack: 1
- Language: pt-BR
- IP Address: 2804:0:4000:800c:8c23:2b20:604b:3de7
- Last Status Reported: 10/6/2014 1:59 PM

The 'Status Summary' for this computer shows:

- 0 updates failed to install
- 0 updates have not been installed
- 5427 updates have been installed or are not applicable
- 0 updates have unknown status

Two green callout boxes provide additional context:

- The top callout box points to the table and contains the text: 'Dados do computador da sala 2364 exibidos no software Report Viewer, como: sistema, idioma, IP, data de reporte, e estatísticas de atualização'.
- The bottom callout box points to the detailed report and contains the text: 'Detalhes específicos da máquina em questão'.

Figura 4.6 – Report Viewer mostrando a estatística de uma máquina que está atualizada (autoria própria)

Verificou-se que o WSUS contribuiu muito para monitorar e visualizar o estado atual das atualizações dos equipamentos, minimizando assim que vírus, malwares e ataques virtuais se infiltrem nesses sistemas. A sua utilização também evita que seja executado um trabalho manual a fim de realizar a mesma tarefa em todos os dispositivos, já que é necessário apenas aprovar as atualizações baixadas e cada computador terá um tempo limite para realizar a sua instalação.

4.1.4 Automatização de implantação e atualização de *software* utilizando WPKG e PSEXEC

Um problema frequente em ambientes computacionais grandes é em relação à distribuição de *software* nas máquinas feita de maneira eficiente e rápida. O autor (DEARLE, 2007) conceitua a implantação de *software* como sendo a etapa depois da aquisição e antes da execução.

Em muitas situações, esse processo é feito manualmente, remota ou presencialmente, demandando um tempo considerável dependendo da quantidade de *softwares* e da quantidade de estações de trabalho.

Da mesma forma, no período anterior a implantação, o tempo necessário para realizar esta tarefa era grande, pois a equipe contém apenas dois funcionários e um bolsista no período diurno.

Para minimizar o problema de instalação de *softwares* em massa nos laboratórios de maneira manual, foram pesquisadas diversas ferramentas que tinham como função automatizar o processo de implantação de *software*. Foram comparados os seguintes aplicativos: Group Policy Object (gratuito, nativo e integrado ao AD), WPKG (gratuito) (WPKG, 2014), PDQ Deploy (comercial) (ARSENAL, 2014).

Foi escolhido o *software* WPKG como solução apropriada, pois o mesmo apresenta vantagens em relação aos concorrentes, como no fato de ser gratuito e open-source, aceitar uma grande variedade de instaladores diferentes e não possuir limite de *softwares* ou máquinas para implantação.

O *software* escolhido também possui desvantagens em relação aos outros analisados, tais como: ausência de interface gráfica, e configuração manual dos *softwares* e computadores via arquivos XML.

Um exemplo de uso desse *software* se dá para a atualização periódica de toda a gama de programas instalados nos computadores dos laboratórios e salas de aula, os quais incluem: plug-ins, comunicadores instantâneos, leitor de PDF, pacote de codecs, descompactadores, antivírus, etc, evitando assim, da mesma forma que o WSUS, a atualização custosa em termos de tempo e eficiência, e garantindo todos os programas em suas últimas versões disponíveis quando necessário.

O detalhes de uso do *software* WPKG estão descritos no Anexo B.

4.2 Utilização do sistema de emissão de ticket e abertura de chamados com base de conhecimento integrada osTicket

Uma necessidade presente na atual administração do laboratório de informática é um histórico dos registros, atendimentos e soluções de eventuais problemas em diversas partes do Centro. Sua concretização resultaria em um melhor controle sobre toda e qualquer manutenção e suporte prestados no ambiente, otimizando assim o processo de aprendizagem para novos bolsistas e redirecionando a força de trabalho conforme a necessidade aplicada.

Foram analisadas diversas ferramentas de ticketing, dentre elas, pagas e gratuitas. Coletou-se uma lista com as seguintes opções e verificou-se os recursos e limitações de cada uma: RT Request Tracker 4.2.8 (gratuito) (PRACTICAL, 2014), osTicket 1.9.4 (gratuito) (OSTICKET, 2014), OTRS 3.3.9 (gratuito) (SERVICES, 2014), GLPI 0.84.7 (gratuito) (GLPI, 2014), Web Help Desk 12.0.1 (comercial) (SOLARWINDS, 2014), Kayako 4.66 (comercial) (KAYAKO, 2014).

O *software* osTicket foi o escolhido para ser implantado como sistema de help desk do CCSH. Ele apresenta as principais vantagens em relação aos concorrentes: Gratuito, open-source, contém base de conhecimento integrada, fácil instalação e uso, boa documentação e comunidade ativa, interface limpa e agradável, multiplataforma.

Ao entrar na sua página inicial, o osTicket solicita ao administrador para que se realize a configuração inicial do ambiente recém implantado, requisitando alguns dados do administrador e do banco de dados a ser utilizado, assim como senhas de acesso para tarefas administrativas.

Foram modificadas algumas opções no painel de administração para adequar o sistema de ticketing à realidade do Centro, cadastrando funcionários e bolsistas da informática como membros da equipe de suporte, e cadastrando usuários, como por exemplo a Direção do CCSH, que solicitam os pedidos de suporte, auxílio e manutenção. Assim o sistema está em pleno funcionamento, aguardando a abertura de novos tickets e instruções na base de conhecimento. As Figuras 4.7 e 4.8 mostram o painel do ponto de vista do agente e do ponto de vista do administrador respectivamente.

A Figura 4.7 exhibe a lista de chamados abertos, podendo ser ordenada de vários modos, e contendo o assunto, o usuário que realizou o chamado, sua prioridade e a atribuição a um técnico. Já na Figura 4.8, é exibida a lista dos agentes cadastrados, e que integram a equipe. Nota-se que um dos agentes está com status bloqueado, significando que o mesmo deixou de fazer parte da equipe de suporte e não tem mais acesso ao sistema de ticketing.

Bem-vindo, Kevin. | [Painel de Administração](#) | [Minhas Preferências](#) | [Sair](#)

Painel de Controle Usuários **Tickets** Base de Conhecimento

[Aberto \(2\)](#) [Meus Tickets \(2\)](#) [Atrasado \(2\)](#) [Resolvido \(5\)](#) [Fechado \(1\)](#) [Novo Ticket](#)

 [avançado] ⓘ

🔄 **Tickets Abertos — Mostrando 1 - 2 de 2**

Ticket	Data	Assunto	De	Prioridade	Atribuído a
<input type="checkbox"/> 000011	02/10/2014 09:28	PC- travado no iniciar. (5) ⓘ	Marília	Normal	Kevin Costa
<input type="checkbox"/> 000010	02/10/2014 08:31	PC desconfigurado - sala: 4226 (6) ⓘ	Beloni Gomes	Normal	Kevin Costa

Selecionar: Todos Nenhum Alternar

Página: [1] Exportar ⓘ

Copyright © 2006-2014 Sistema de chamados do CCSH - UFSM All Rights Reserved.

Figura 4.7 – Tela inicial dos tickets em abertos que estão em andamento (autoria própria)

Bem-vindo, Kevin. | [Painel do Agente](#) | [Minhas Preferências](#) | [Sair](#)

Painel de Controle Configurações Gerenciar E-mails **Agentes**

[Agentes](#) [Equipes](#) [Grupos](#) [Departamentos](#)

Agentes

— Todos os Departamentos — — Todos os grupos — — Todas as equipes — [Adicionar Novo Agente](#)

Mostrando 1 - 5 de 5 agentes

Nome	Usuário	Status	Grupo	Departamento	Criado	Último Login
<input type="checkbox"/> Anderson Flores	anderson	Ativo	Domadores de Leões	Atendimento	23/09/2014	02/10/2014 13:27
<input type="checkbox"/> Kevin Costa	kevin	Ativo	Domadores de Leões	Atendimento	23/09/2014	06/10/2014 13:37
<input type="checkbox"/> Nikollas Kaue	nikollas	Bloqueado	Domadores de Leões	Atendimento	23/09/2014	24/09/2014 17:54
<input type="checkbox"/> Oberdan Lopes	oberdan	Ativo	Domadores de Leões	Atendimento	23/09/2014	03/10/2014 08:19
<input type="checkbox"/> Patricia Mattos	patricia	Ativo	Domadores de Leões	Atendimento	23/09/2014	

Selecionar: Todos Nenhum Alternar

Página: [1]

Figura 4.8 – Tela exibindo os agentes responsáveis pela abertura e resolução dos tickets (autoria própria)

A Figura 4.9 exibe a base de conhecimento criada para armazenamento de novas soluções e manuais que ajudarão futuros alunos bolsistas na resolução de problemas.

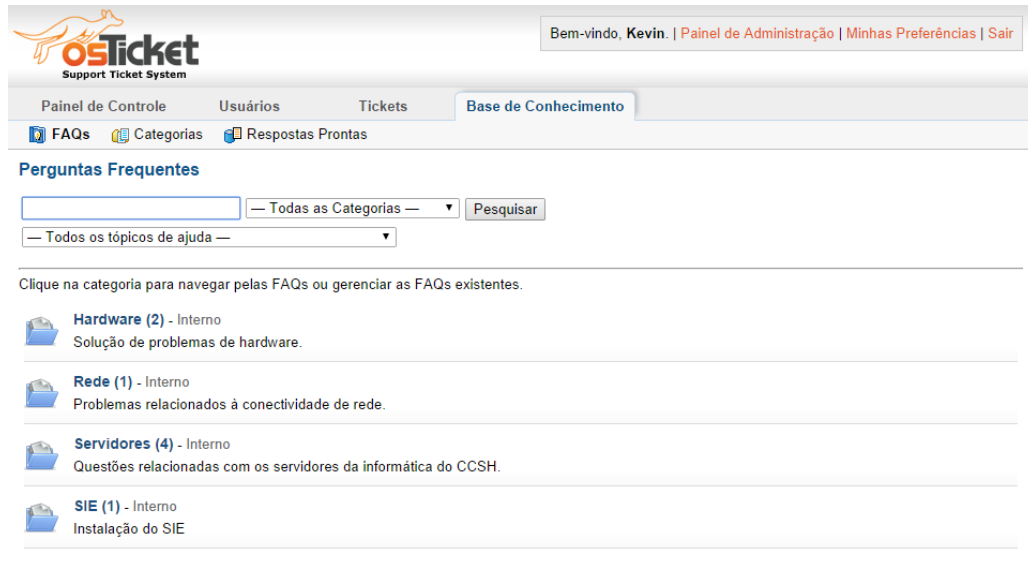


Figura 4.9 – Tela mostrando a base de conhecimento atual, já com algumas entradas (autoria própria)

Pode-se afirmar que o sistema de ticketing auxiliou consideravelmente no registro de ocorrências e na distribuição dos agentes de suporte de modo otimizado, os quais eram antes inexistentes. O suporte a uma base de conhecimento integrada é outro elemento muito importante no contexto atual, pois como há uma alta rotatividade de pessoas dentro das equipes técnicas, o conhecimento desta acaba se perdendo e com isso é necessário um novo treinamento para os novos técnicos.

Assim, é possível reter a expertise de cada integrante do grupo nesse banco de dados, e possibilitar que o conhecimento adquirido seja distribuído entre novos integrantes, que, no caso do CCSH, são alunos bolsistas, e que frequentemente trocam de projetos ou acabam concluindo a graduação.

O requisitos e detalhes de instalação do *software* osTicket estão descritos no Anexo C.

4.3 Implementação de website para manipulação remota de operações de manutenção do AD – RemoteAD

Em muitos sistemas computacionais, problemas não tem hora ou data para ocorrer, podendo aparecer nos momentos mais inesperados e nas situações mais inusitadas. Para evitar transtornos, uma boa alternativa é contar com mecanismos que permitam o acesso e a gerência remota de recursos, podendo ser acessada de qualquer lugar. Para isso, foi implementado um website, batizado de RemoteAD, o qual tem a finalidade de gerenciar alguns recursos do Active

Directory da internet.

O website foi construído utilizando os frameworks ASP.NET 4.5 (linguagem C#) para o back-end, e os frameworks JQuery 2.1.1 e Bootstrap 3.3.1 para o front-end, na IDE Visual Studio 2013. A hospedagem foi feita no IIS, juntamente com o osTicket, porém, aberto na porta 8080.

O framework ASP.NET foi escolhido por ser nativo ao sistema operacional e pela sua simples integração com o Active Directory, não sendo necessário o download adicional de nenhuma ferramenta. Os frameworks Bootstrap e JQuery foram escolhidos por possuírem uma ampla comunidade e suportarem uma grande gama de navegadores de internet, permitindo a construção de interfaces de websites e aplicativos web responsivas e dinâmicas, podendo serem dimensionadas para vários dispositivos e formatos de tela. O website RemoteAD foi construído focando-se primeiramente em dispositivos móveis, podendo, porém, ser utilizado em desktops e notebooks.

A Figura 4.10 mostra o funcionamento do site em um diagrama de atividades.

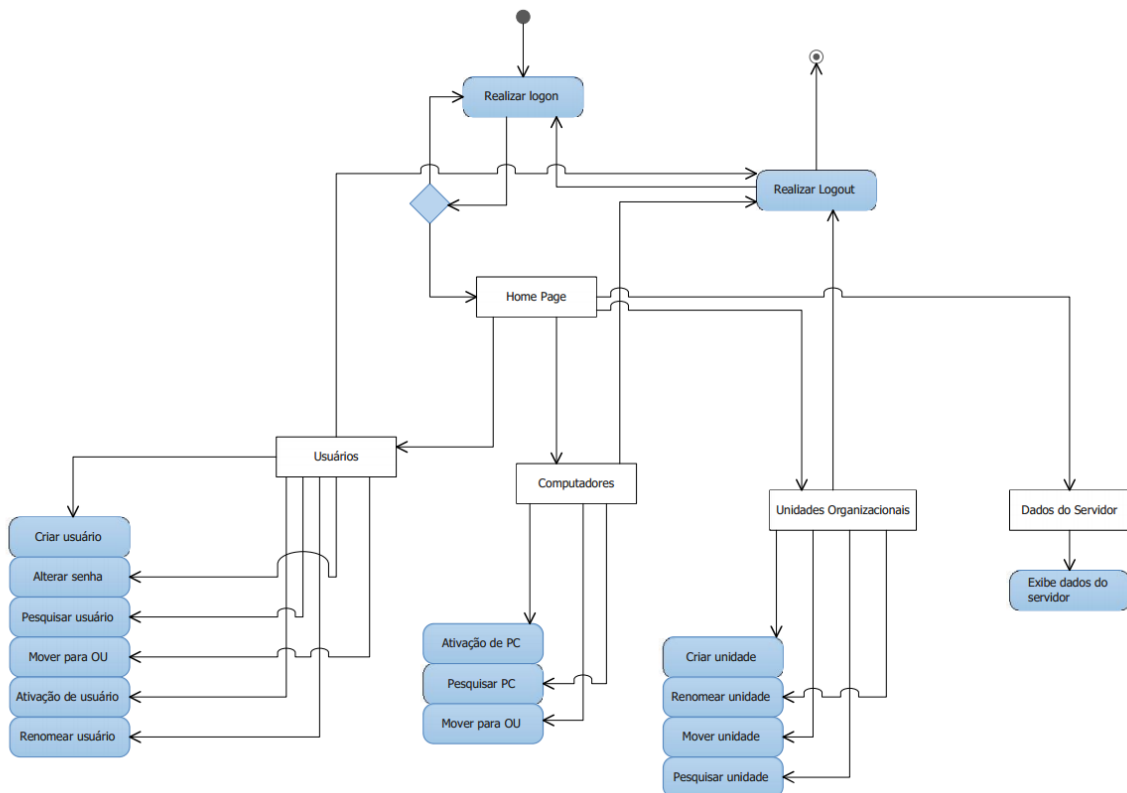


Figura 4.10 – Diagrama de Atividades do sistema (autoria própria)

A interface foi dividida em cinco Web Forms (arquivos com extensão .aspx) e uma Razor View (arquivos com extensão .cshtml), tendo cada Web form sua classe específica. Contam com

as seguintes funcionalidades:

- Users.aspx – interface que trata das operações feitas com usuários do AD, permitindo criar, renomear, alterar senha, pesquisar usuários existentes, ativar/desativar usuário, e mover usuário para uma OU diferente;
- Computers.aspx – Interface responsável pelo tratamento das operações feitas com computadores do AD, sendo possível pesquisar computadores cadastrados, mover computadores para outra OU, e ativar/desativar computador;
- OrganizationalUnits.aspx – Interface responsável pelas operações feitas com as Unidades Organizacionais (OU) do AD, permitindo a criação de novas OU, renomear uma OU, pesquisar OUs existentes, e mover uma OU de uma unidade para outra;
- Default.aspx – Interface que abrange a tela inicial do *software*, oferecendo as opções para o administrador e redirecionando-o para uma das opções acima, ou realizar o Logout;
- Logon.aspx – Interface para autenticação do administrador;
- ServerStats.cshtml – Exibe dados e detalhes do servidor onde o site está hospedado.

Internamente, o website se comunica com o diretório através da API nativa do Active Directory Services, disponível para uso. A API contém o namespace chamado System.DirectoryServices, o qual permite que seja feita uma gerência de recursos através de aplicativos e da web, independentemente do tamanho da rede (MICROSOFT, 2014c).

A parte lógica do *software* é composta por sete classes (arquivos com extensão .cs), as quais acessam a API nativa e utilizam os métodos e classes internas da mesma. São elas abaixo:

- AccountMaintenance.cs – Classe responsável pelas operações com contas de usuário, contendo métodos para manipular contas existentes;
- Authentication.cs – Classe responsável pela autenticação de usuários administradores no sistema, atuando primeiramente no logon e realizando a verificação das credenciais fornecidas;
- Fetch.cs – Classe que executa as respectivas buscas no diretório solicitadas pelos outros métodos e classes, retornando os dados para os mesmos;

- `GetterIPDomain.cs` – Classe auxiliar para a verificação do endereço IP do servidor e do domínio que será utilizado;
- `GroupManagement.cs` – Classe responsável pela verificação de grupo de privilégio para usuários, e para novas atribuições e promoções de privilégios para usuários existentes;
- `LDAPObjectState.cs` – Classe que contém as tarefas de ativação e desativação de usuários e computadores, e exibir avisos e confirmações na página para o administrador;
- `OuMaintenance.cs` – Classe para a manipulação de Unidades Organizacionais.

As Figuras 4.11 e 4.12 mostram, respectivamente, a lista de tarefas possíveis de serem realizadas, e o menu *drop down* de dentro da categoria "Usuários", exibindo as opções.

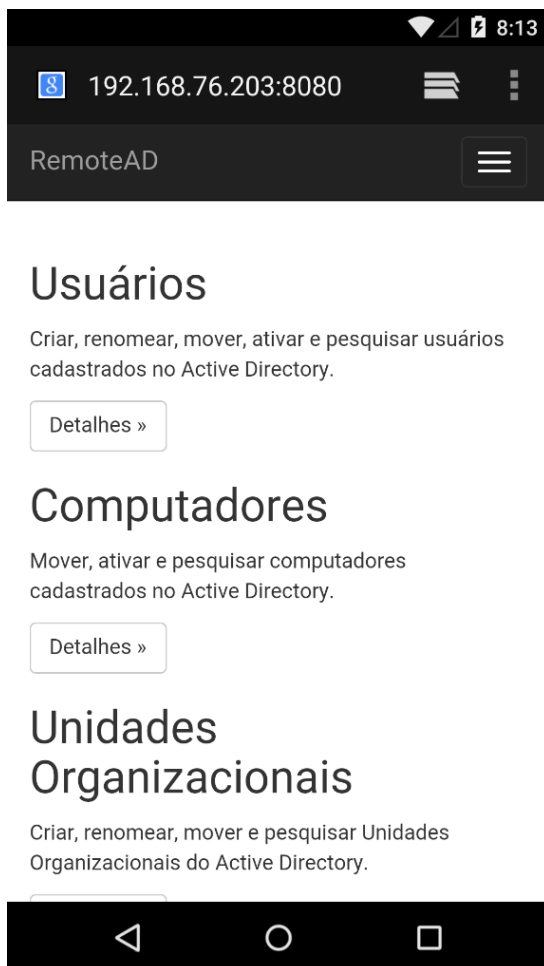


Figura 4.11 – Interface inicial para cada categoria escolhida (autoria própria)

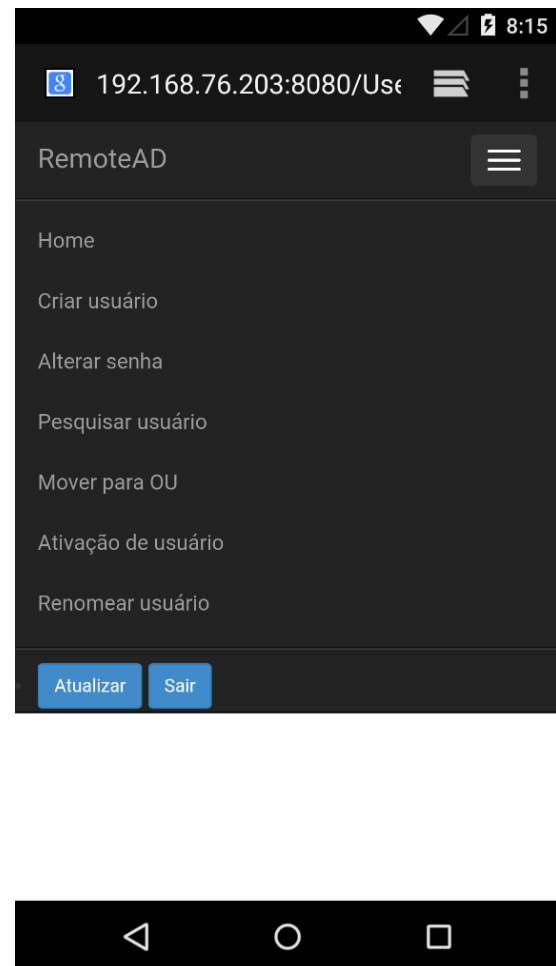


Figura 4.12 – Menu de opções no estilo drop down em dispositivos móveis (autoria própria)

As operações permitidas no website são em menor número em relação as operações possíveis diretamente no servidor, e, para maior segurança, apenas administradores do AD podem

acessar a ferramenta e obter controle sobre os recursos.

A implementação permite a manipulação de usuários, computadores e unidades organizacionais. Para usuários, tem-se a possibilidade de cadastrar novas contas com privilégios não administrativos no diretório, realizar alteração de senha, pesquisar um usuário específico, mover um determinado usuário para uma OU, ativar ou desativar usuário e renomear usuário. Para computadores, é possível realizar a pesquisa de computadores, mover uma máquina para uma OU, e ativar ou desativar computadores. Por fim, para unidades organizacionais, há a possibilidade de criação de novas OUs, pesquisa de OUs existentes, renomear OUs, e mover uma OU para outra unidade.

Algumas operações não são permitidas pelo website, tais como: exclusão de usuários, cadastro e exclusão de computadores, exclusão de OUs, alteração de atributos do objeto, entre outras.

Essa implementação se faz importante no campo da universidade no quesito de mobilidade dos técnicos, tanto dentro da unidade universitária quanto na extensão do campus da universidade, evitando deslocamentos desnecessários e custosos, e possibilitando o acesso e manipulação do diretório mesmo em momentos fora do expediente de trabalho.

5 CONSIDERAÇÕES FINAIS

A gerência de redes de computadores se eleva hoje como uma área muito importante tanto para empresas privadas quanto públicas, pois, cada vez mais, pessoas estão conectadas e dependentes da rede, e seu correto funcionamento, para a realização de suas tarefas e atividades com segurança, e para isso um bom gerenciamento se faz necessário para garantir um serviço de qualidade.

Com o advento da computação móvel, dos dispositivos vestíveis e da computação em nuvem, suprimir essa gerência pode acarretar consequências negativas para seus utilizadores e para a equipe que realiza sua manutenção. Garantir o correto funcionamento da infraestrutura lógica do ambiente se tornou essencial para manter uma rede organizada, padronizada, economizar recursos e tempo da equipe de TI, e manter a satisfação dos clientes e funcionários em um bom nível.

Este trabalho apresentou a implantação e instalação de algumas técnicas de gerência integradas em um ambiente acadêmico e predominantemente laboratorial, exibindo o funcionamento principal das suas ferramentas e utilitários, a fim de minimizar os diversos problemas, necessidades e deficiências encontrados no CCSH previamente, e melhorar a qualidade de uso dos recursos por parte dos alunos e funcionários. Para enfrentar os problemas de infecções por vírus, surgimento de erros e lentidão, falta de padronização e equipamentos desatualizados, aumentou-se o controle sobre os computadores e usuários nos setores com a criação de um diretório, onde definiu-se políticas de acesso, reforçou-se a segurança das máquinas, e impediu-se a sua total manipulação pelos seus utilizadores. Da mesma forma, foi estabelecida uma central de atualização de softwares e sistemas operacionais, para manter as máquinas atualizadas constantemente.

Essas medidas resultaram em uma boa diminuição nas ocorrências de problemas, passando de frequentes para esporádicos e ocasionando uma maior satisfação dos usuários, conforme a observação diária de chamados e solicitações de suporte. Também houve um melhor controle sobre a infraestrutura instalada, permitindo fácil acesso e menor esforço de manutenção pelos técnicos.

Para o controle remoto do diretório, construiu-se um website, batizado de RemoteAD, com a finalidade de permitir manipulação de objetos do AD em uma interface web de qualquer local com conexão a internet.

Por fim, foi implantado um sistema de emissão de tickets para abertura de chamados, chamado de osTicket, a fim de permitir a documentação dos serviços de suporte prestados pela equipe de TI local e construir uma base de conhecimento permanente para qualquer agente aperfeiçoar seu aprendizado ou aprender novas técnicas e soluções.

5.1 Trabalhos futuros

Não foi possível, no entanto, implantar alguns aspectos na gerência abordada, tais como o monitoramento completo do tráfego da rede e seu mapeamento, feita, por exemplo, com o *software* Nagios em conjunto com o *software* Cacti.

Outro aprimoramento possível, é a criação de uma conta de usuário para cada aluno conforme sua matrícula na universidade, cadastrando-o no diretório, e criando um perfil salvo em um *Storage* dedicado, a fim de que esse aluno possa acessar seus dados de qualquer lugar da instituição de ensino em um computador que esteja cadastrado no AD.

Para o *software* osTicket, este pode ser melhor integrado ao Active Directory, para realizar a coleta direta dos arquivos de log das máquinas com problema que forem referenciadas na solicitação, e adicionar essas informações ao corpo do chamado, mantendo informações importantes para o agente, e o auxiliando com mais detalhes na resolução do problema.

Tratando-se do website RemoteAD, pode-se realizar seu aperfeiçoamento, a fim de adicionar novas funções e mecanismos de controle, tais como: visualização de eventos de sistema, status atual dos computadores, última data de utilização, execução de scripts remotos personalizados para uma seleção específica de máquinas, entre outros.

REFERÊNCIAS

ARSENAL, A. **Deploy Software Quickly with PDQ Deploy**. Disponível em: <<http://www.adminarsenal.com/pdq-deploy>>, Acesso em: 01/10/2014.

BRIGANÓ, U.; BARROS, R. A Implantação de um Service Desk: um estudo de caso aplicando conceitos do itil e do pmbok. In: XXXVIII CONGRESSO BRASILEIRO DE EDUCAÇÃO EM ENGENHARIA–COBENGE. **Anais...** [S.l.: s.n.], 2010.

CISCO. **Cisco Prime for IT and Service Providers**. Disponível em: <<http://www.cisco.com/c/en/us/products/cloud-systems-management/prime.html>>, Acesso em: 27/11/2014.

DEARLE, A. Software deployment, past, present and future. In: FUTURE OF SOFTWARE ENGINEERING, 2007. **Anais...** [S.l.: s.n.], 2007. p.269–284.

GLPI. **GLPI Free It And Asset Management Software**. Disponível em: <<http://www.glpi-project.org/spip.php?lang=en>>, Acesso em: 03/10/2014.

HP. **NETWORK NODE MANAGER i**. Disponível em: <<http://www8.hp.com/br/pt/software-solutions/network-node-manager-i-network-management-software/>>, Acesso em: 27/11/2014.

HP. **HP BTO Software - Applications Portfolio**. Disponível em: <http://www.hp.com/hpinfo/newsroom/press_kits/2010/HPSoftwareUniverseBarcelona2010/HP_Applications_Portfolio_brochure.pdf>, Acesso em: 27/11/2014.

IBM. **IBM - Tivoli NetView**. Disponível em: <<http://www-03.ibm.com/software/products/pt/tivnetv/>>, Acesso em: 27/11/2014.

IETF. **SNMP over Ethernet**. Disponível em: <<https://www.ietf.org/rfc/rfc1157.txt>>, Acesso em: 27/11/2014.

IETF. **Remote Network Monitoring Management Information Base**. Disponível em: <<http://www.rfc-editor.org/rfc/rfc1271.txt>>, Acesso em: 27/11/2014.

IETF. **Lightweight Directory Access Protocol**. Disponível em: <<https://www.ietf.org/rfc/rfc1777.txt>>, Acesso em: 04/10/2014.

IETF. **Simple Network Management Protocol (SNMP) over Transmission Control Protocol (TCP) Transport Mapping**. Disponível em: <<https://tools.ietf.org/html/rfc3430>>, Acesso em: 23/12/2014.

IVIRTUA. **iVirtua Suite Trauma Zero**. Disponível em: <<http://www.ivirtuagroup.com.br/pt/produtos/ivirtua-suite-trauma-zero>>, Acesso em: 27/11/2014.

KAYAKO. **Simple, scalable customer service software**. Disponível em: <<http://www.kayako.com/>>, Acesso em: 03/10/2014.

LUNARDI, G. L. Um estudo empírico e analítico do impacto da governança de TI no desempenho organizacional. , [S.l.], 2008.

LÔBO, J. S. **CONTEXTO DE EXPERTISE E LOCALIZAÇÃO INFLUENCIANDO A GERÊNCIA DE TI**. 2011. Dissertação (Mestrado em Ciência da Computação) — Universidade Federal de Santa Maria.

MAGALHÃES, I. L.; PINHEIRO, W. B. Gerenciamento de Serviços de TI na Prática. **São Paulo: Novatec**, [S.l.], 2007.

MARTINS, P. J. et al. Comparação dos paradigmas cliente/servidor e agentes móveis. , [S.l.], 2002.

MICROSOFT. **What Are Domains and Forests?** Disponível em: <[http://technet.microsoft.com/en-us/library/cc759073\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc759073(v=ws.10).aspx)>, Acesso em: 05/10/2014.

MICROSOFT. **Domain controllers**. Disponível em: <[http://technet.microsoft.com/en-us/library/cc759623\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc759623(v=ws.10).aspx)>, Acesso em: 08/10/2014.

MICROSOFT. **Create a mandatory user profile**. Disponível em: <[http://technet.microsoft.com/en-us/library/cc786301\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc786301(v=ws.10).aspx)>, Acesso em: 07/10/2014.

MICROSOFT. **Group Policy for Beginners**. Disponível em: <[http://technet.microsoft.com/en-us/library/hh147307\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/hh147307(v=ws.10).aspx)>, Acesso em: 09/10/2014.

MICROSOFT. **Overview of Windows Server Update Services 3.0 SP2.** Disponível em: <[http://technet.microsoft.com/en-us/library/dd939931\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/dd939931(v=ws.10).aspx)>, Acesso em: 08/10/2014.

MICROSOFT. **Configure Automatic Updates using Group Policy.** Disponível em: <[http://technet.microsoft.com/en-us/library/dd939933\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/dd939933(v=ws.10).aspx)>, Acesso em: 07/10/2014.

MICROSOFT. **Visão geral do Servidor Web (IIS).** Disponível em: <<http://technet.microsoft.com/pt-br/library/hh831725.aspx>>, Acesso em: 06/10/2014.

MICROSOFT. **Active Directory: concepts part 2.** Disponível em: <<http://social.technet.microsoft.com/wiki/contents/articles/16969.active-directory-concepts-part-2.aspx>>, Acesso em: 26/11/2014.

MICROSOFT. **Step-by-Step Guide to Understanding the Group Policy Feature Set.** Disponível em: <<http://technet.microsoft.com/library/bb742376>>, Acesso em: 26/11/2014.

MICROSOFT. **Namespace System.DirectoryServices.** Disponível em: <[http://msdn.microsoft.com/pt-br/library/system.directoryservices\(v=vs.110\).aspx](http://msdn.microsoft.com/pt-br/library/system.directoryservices(v=vs.110).aspx)>, Acesso em: 08/11/2014.

MORAES, E. A. P.; MARIANO, S. R. H. Governança em tecnologia da informação: um estudo de caso de uma empresa de transporte ferroviário-[doi: 10.5102/un.gti.v4i1.2834](https://doi.org/10.5102/un.gti.v4i1.2834). **Universitas: Gestão e TI**, [S.l.], v.4, n.1, 2014.

NAGIOS. **Nagios - The Industry Standard In IT Infrastructure Monitoring.** Disponível em: <<http://www.nagios.org/>>, Acesso em: 27/11/2014.

OLIVEIRA, H. Análise da integração entre o Kerberos eo OpenLDAP. , [S.l.], 2013.

OPENLDAP. **Introduction to OpenLDAP Directory Services.** Disponível em: <<http://www.openldap.org/doc/admin22/intro.html>>, Acesso em: 05/10/2014.

ORCHESTRA. **EBX5 Multidomain Master Data Management Software.** Disponível em: <<http://www.orchestranetworks.com/product/>>, Acesso em: 27/11/2014.

OSTICKET. **osTicket Support Ticketing System.** Disponível em: <<http://www.osticket.com/>>, Acesso em: 03/10/2014.

PRACTICAL, B. **RT**: request tracker. Disponível em: <<http://bestpractical.com/rt/>>, Acesso em: 03/10/2014.

QUEIROZ, A. P. d. N. C. Análise da implantação da governança de TI, de acordo com as definições da biblioteca ITIL, um estudo de caso. , [S.l.], 2012.

ROSA, D. M. d. **Suporte a Cooperação em Sistemas de Gerenciamento de Redes Utilizando Tecnologias Peer-to-Peer**. 2007. Dissertação (Mestrado em Ciência da Computação) — UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL.

SANTOS, A. L. A. d. M. Análise do processo de change management utilizando as boas práticas do ITIL. , [S.l.], 2014.

SANTOS, M. d. Uso de LDAP implementado em software livre para integrar a autenticação dos controladores de domínio MS-Active Directory e Samba/Linux. , [S.l.], 2014.

SERVICES, O. O. T. R. **OTRS**. Disponível em: <<http://www.otrs.com/>>, Acesso em: 03/10/2014.

SIMÕES, J. M. B. Monitorização automática de redes de computadores: estudo e proposta de uma nova solução. , [S.l.], 2010.

SOARES, D. D. S. SiViCS: um sistema para visualização e coleta de switches: proposta de ferramenta integrada ao sistema de gerência de redes da ufrgs. , [S.l.], 2012.

SOLARWINDS. **Web Help Desk**. Disponível em: <<http://www.webhelpdesk.com/>>, Acesso em: 03/10/2014.

THOMPSON, M. A. **Windows Server 2008 R2**: instalação, configuração e administração de redes. first.ed. [S.l.]: Erica, 2010.

TORRES, J. O. A. d. L. Proposta de uma solução de Business Intelligence para a gestão da produção de serviços de tecnologias da informação com base no padrão de gerência de redes ISO/IEC 74984. , [S.l.], 2011.

UNIVERSITY, I. **What is a fully qualified domain name (FQDN)?** Disponível em: <<https://kb.iu.edu/d/aiuv>>, Acesso em: 03/10/2014.

WPKG. **Main Page**. Disponível em: <<http://wpkg.org/>>, Acesso em: 01/10/2014.

ZABBIX. **Zabbix - The Enterprise-class Monitoring Solution for Everyone**. Disponível em: <<http://www.zabbix.com/>>, Acesso em: 27/11/2014.

ZANELATTO, A. W. et al. Redes de Computadores-Desenvolvimento de Um Sistema de Apoio a Gerência de Falhas Baseado em Casos-Antifail. **Anais SULCOMP**, [S.l.], v.5, n.1, 2010.

ANEXOS

ANEXO A – Figuras complementares

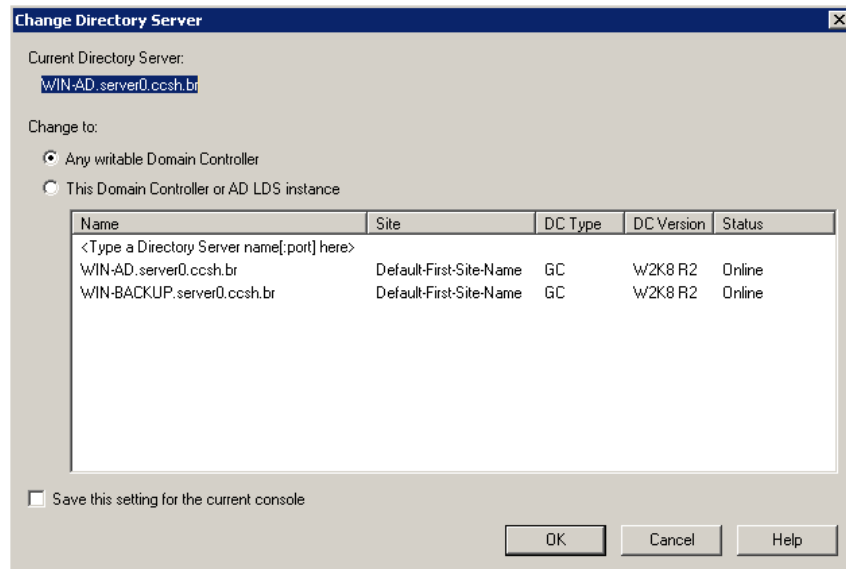


Figura A.1 – Exibição dos controladores de domínio disponíveis para o AD (autoria própria)



Figura A.2 – Área de trabalho padrão para laboratórios e salas de aula (autoria própria)

ANEXO B – Detalhes de funcionamento do WPKG

O WPKG é composto pelos seguintes arquivos:

- wpkg.js (parser responsável pela execução nos clientes);
- config.xml (onde são configuradas as opções de região, linguagem e caixas de diálogo);
- packages.xml (onde são especificados como cada *software* deve ser instalado);
- profiles.xml (onde são especificados quais *softwares* serão instalados em cada perfil);
- hosts.xml (onde são atribuídos computadores a determinados perfis).

O *software* PSEXEC foi utilizado para executar o parser “wpkg.js” remotamente nas máquinas através de arquivos batch. Cada arquivo executa uma instância do PSEXEC chamando o parser em cada computador especificado, como no exemplo abaixo:

Arquivo: “PSEXEC WPKG 4400.bat”

```
psexec -d \\lab74c01 -s cmd /c “cscript \\win-backup\wpkg\wpkg.js /synchronize /quiet /nonotify”
```

Argumentos:

-d: executa o PSEXEC paralelamente em cada computador, sem esperar o término de execução em cada uma;

\\lab74c01: Indica o nome da máquina alvo;

-s: Abre o processo como o usuário administrador SYSTEM, o qual possui altos privilégios;

cmd /c “cscript...”: Script a ser executado a fim de instanciar o parser do WPKG e iniciar o processo de instalação ou atualização dos *softwares*.

ANEXO C – Detalhes de instalação do osTicket

Os requisitos necessários para implantação do *software* escolhido, segundo a fabricante, são:

- Web server: Apache ou IIS;
- PHP: versão 5.3 ou superior;
- SGBD: MySQL 5.0 ou superior, MariaDB versão 5.5 ou superior.

Para o setup local foi utilizado o IIS versão 7.5, PHP versão 5.6 Non Thread Safe 64-bits, com gerenciamento via IIS, e MySQL versão 5.6.

Na Figura C.1 são exibidas as alterações que foram feitas no arquivo “php.ini” para integração do PHP com IIS.

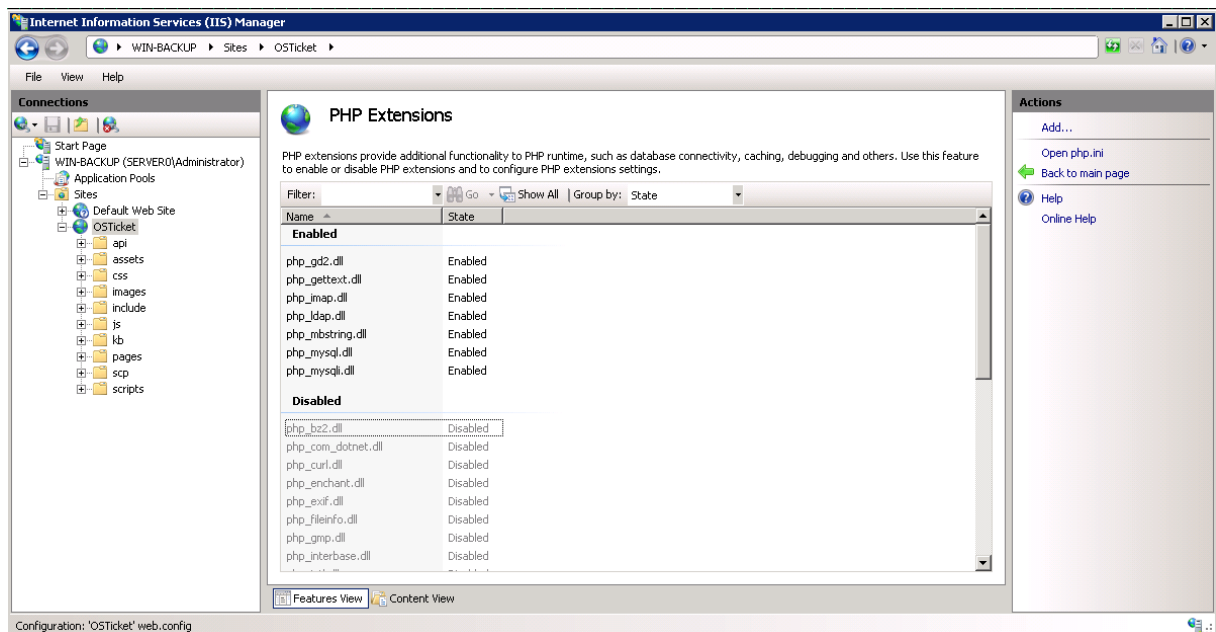


Figura C.1 – Extensões ativas do PHP (autoria própria)

O *software* osTicket foi instalado no diretório “C:\osticket”. Para uma primeira configuração, cria-se um novo banco de dados dentro do MySQL para que sejam armazenados os tickets e a base conhecimento do programa.

Um novo site para o *software* foi criado no IIS, com os redirecionamentos de IP e portas necessários.