Internet Of Things

23 a 27 de Outubro

XIV SESINFO

Segunda-Feira (23/10)
Administração e Monitoração de Servidores

Terça-Feira (24/10)
Construindo mais que sites com Joomla!

Quarta-Feira (25/10)
Programação em sistemas embarcados

Quinta-Feira (26/10)
Segurança da Informação

Sexta-Feira (27/10)
Virtualização com XenServer

Inscrições em: https://goo.gl/forms/JoPBTqpae1LbiNGB3

Entrada:
1Kg Alimento não-perecível
Local: FAFRAM - Ituverava/SP

FAFRAM
ITUVERAVA - SP

R. Domingos Nunes Macedo, s/n - Aeroporto, Ituverava - SP

Administração e Monitoração de Servidores

MsC. Eng. Ali Faiez Taha

aftaha@usp.br

Administrar Servidores

- Tarefa dos Sysadmins
- **Manter servidores em ordem**
- ***Diversidade de Sistemas Operacionais***
- ***Diversidade de Serviços de Rede***
- Usuários
- Administração dos Recursos

Administrar recursos

- **Administração, manutenção e proteção do Sistema Operacional, Softwares e Serviços de Rede.**
- **No Breaks e Backup.**
- Serviços de Backup, Banco de Dados, Servidores WEB, etc.
- **Disponibilidade, Redundância e Resiliência**
- **Escalabilidade**
- Gerenciamento dos Servidores

Servidores Dedicados

- **Escolha do Hardware e do Software**
- Linux / BSD / Mac / Windows
- **Capacidade de Memória, CPUs, Discos, Motherboards, Taxa de utilização, etc.**
- Compartilhamento de Recursos: NFS, Banco de Dados, SMB, WEB, FTP, Proxy, SSH, etc.
- Servidores a instalar, especificações, custos, capacidade e limites.
- **Licenças de Software e Hardware.**

Servidores Cloud

- Servidores dedicados: **Máquinas físicas, totalmente dedicadas com hardware de alta performance para comportar altas requisições.**
- Cloud Computing: **Fracionamento de um conjunto de recursos disponível em dezenas de servidores e Storages, permitindo escalabilidade, garantia de performance e disponibilidade do ambiente.**
- Servidor compartilhado: **É partilhado por uma rede de usuários. O espaço e recursos são repartidos com vários clientes – espaço em disco, CPU, memória e banda de internet.**

Monitoração dos Servidores

- **Administração dos serviços e recursos exige monitoração constante.**
- **Domínio dos diversos tipos de ferramentas de monitoração.**
- Preocupação constante com **vulnerabilidades de Softwares,** falhas, ataques via Rede de Dados, Hackers, Vírus, Malwares e outras pragas.
- **Proteção física e lógica.**
- Firewalls, acesso restrito, segurança física, **Sala Cofre**, Guarda noturno, Hackers.

Itens a monitorar

- **Uso de CPU, discos, Hardware, Rede, Memória, Taxa de uso dos processadores, Swap, Cache, Temperatura, Ventoinhas, refrigeração, etc.**

- **Tráfego das Interfaces de rede, picos, uso da banda da rede de dados, tipo de tráfego, endereços IP, MacAddress, resolução DNS, NetBIOS, abusos, TCP/IP, anomalias, tráfego estranho, etc.**

- **Monitoração constante de usuários, serviços de rede, softwares instalados, comportamento do servidor, arquivos de senhas, compartilhamento de arquivos, permissões, logs, logs, logs, logs...**

Ferramentas de Monitoração

Monitoração de Servidores Linux

- **Via linha de comando:** Top, htop, Atop, Apachetop, Mytop, Ftptop, Powertop, Iotop
- **Ferramentas para Desktop:** Ntopng, iftop, jnettop, bandwidthd, etherape, MRTG, traceroute, IPTState, netstat, sockstat, nmap, tcpdump, Justsniffer, etc.
- **Monitoramento da Infraestrutura:** OpenNMS, Sysusage, Nagios, Cacti, Munin, Zenoss, Zabbix, Nmon, Glances, Saidar, RRDTool, Monit, NetSNMP, Mpstat, pmap, etc.
- **Monitoramento de Logs:** GoAccess, LogWatch, Swatch, MultiTail, etc.
- **Monitoramento do Servidor:** Whowatch, strace, acct, psacct, Dtrace, Webmin, stat, ulimit, cpulimit, lsof, etc.
- **Recomendadas:** Collectd, Observium, Nload, SmokePing, MobaXterm, Shinken Monitoring.

https://www.serverdensity.com/monitor/linux/how-to/

Integridade do Servidor

- **Alteração em Sistema de Arquivos e Softwares instalados**

Auditar com Tripwire

- **Serviços de rede estranhos**

www.sectools.org

Administração do Linux

- **Atualização do S.O. - Será que precisa recompilar o Kernel e todos os programas fontes do Linux ?**
- Fontes seguras de Softwares – **conheça a origem dos Softwares que utiliza.**
- **Atualização e aplicação de patches de segurança – fique atento pois tem muitas falhas em Softwares.**
- **Conheça o Searchsploit - www.exploit-db.com/search/ - e fique sabendo como são as invasões por exploração de programas, sistemas e sites vulneráveis.**
- **Analisar os diversos tipos de vulnerabilidades** – Um dia você fica craque e faz um Software a prova de falhas.

- **Como fazer a atualização dos Softwares instalados ? E do Sistema Operacional ? Será que é fácil atualizar uma versão muito antiga dum Sistema Operacional ? E se estiver em produção ?**
- **Fica bom depois de atualizar tudo ? Quem garante a integridade dos dados ?**

- **Atenção aos alertas pelas comunidades de segurança – Bons amigos e bons conhecimentos.**
- **Auditoria constante – pense nisso !!!**
- **Uso de ferramentas IDS, HIDS, NIDS – Detectar tentativas de intrusão**
- ***Firewall – Será que precisa mesmo num simples servidor ou é só para usar em Redes ?***
- **Limitar acessos – Quem pode se conectar ao servidor ?**
- ***Procure garantir a Integridade, Confidencialidade e Autenticidade dos dados***
- **Redes VPN – Circuito fechado entre as redes de uma empresa.**

Integridade do Sistema Operacional

- Integridade do Sistema em produção e do Backup.
- Espaço em disco, Programas de inicialização, Registro do Sistema, Histórico de Softwares, DLLs compartilhadas, arquivos corrompidos, etc.
- Necessidade de aplicação de patches.
- Chaves de registro.
- No Linux, use o Tripwire. Verificador de integridade de arquivos com MD5SUM, SHA, SHA256, etc.
- **Ferramentas Administrativas e de monitoração embutidas no Sistema Operacional Windows. Monitor de Recursos e gerenciamento de tarefas.**
- **Verificador de Arquivos do Sistema, SFC.exe**
- **Performance Monitor no S.O. Windows.**

Sistema de Logs

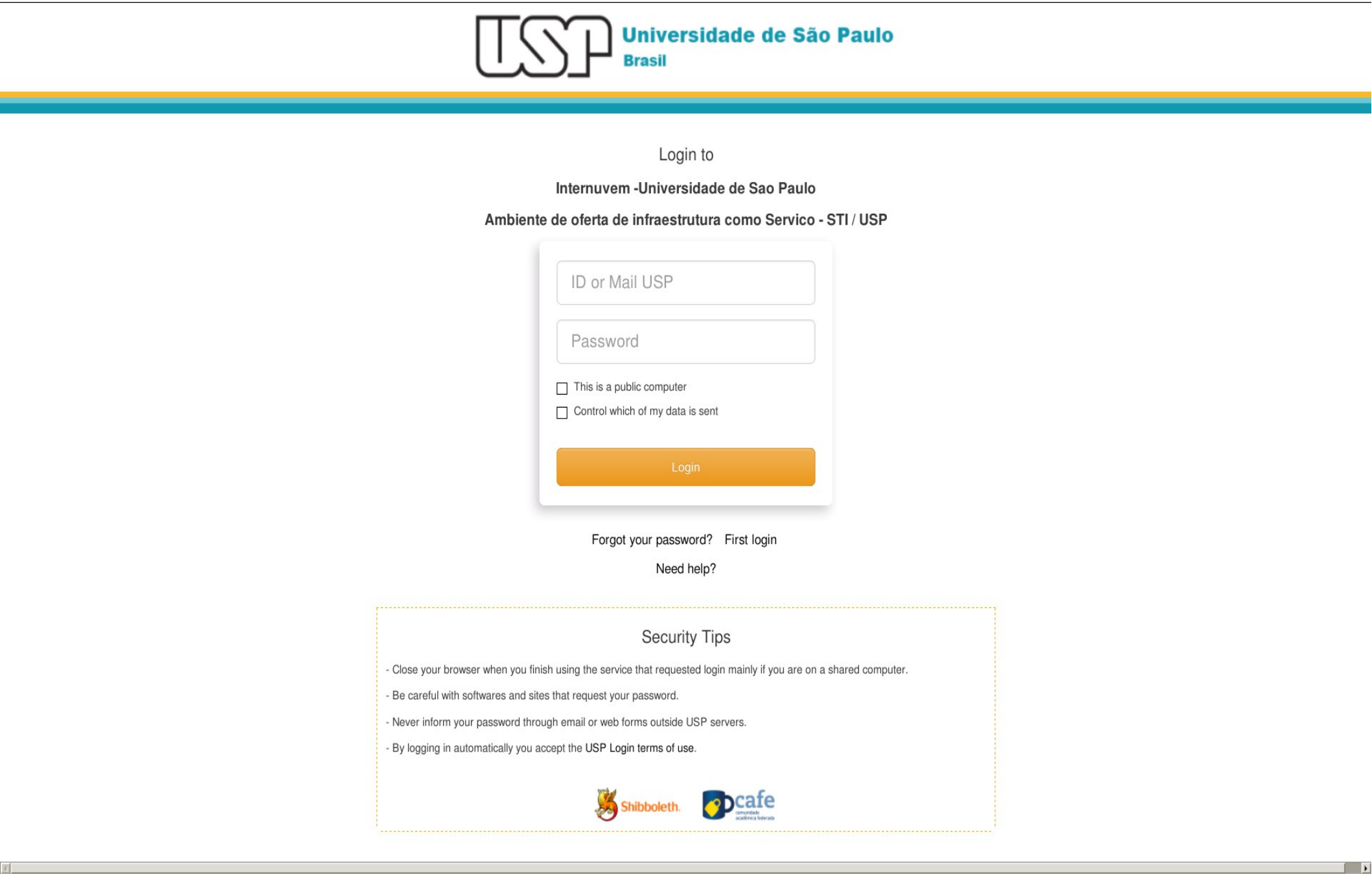
- Registro de atividades, falhas, acessos e erros de aplicações do Sistema Operacional e dos programas em execução.
- **Unix / Linux: Diretório /var/log** **Windows: Visualizador de Eventos**
- Ferramentas para gerenciamento de logs : **Fluentd, LogPacker, Logstash, Graylog, Logagent-js**
- Daemon Syslog responsável pelo gerenciamento dos logs. Muitos tipos e formatos de logs.
- **Sawmill – Analisador de logs – www.sawmill.net**
- **Fundamental para eventos de (in)segurança.**
- Falhas em configuração e execução de serviços são registradas em arquivos de log.
- Uso de comandos em busca de expressões regulares nos logs: **grep e egrep**
- /var/log/httpd.access, httpd.error = Logs do Servidor Web Apache
- /var/log/daemon.log = logs de serviços em geral
- /var/log/syslog: logs do sistema
- /var/log/auth.log: logs de autenticação

Servidores em Nuvem

Nuvem-USP

- Integração de Sistemas Administrativos, E-Mails, Desktops, Autenticação Única, Máquinas Virtuais.
- Implementada em 2012 com apoio da Fapesp, com o objetivo de auxiliar na gestão da tecnologia da informação (TI) da USP, a interNuvem atende tanto às demandas dos pesquisadores da Universidade – que necessitam de recursos de computação de alto desempenho e de armazenamento de dados para a realização de suas pesquisas –, como também da administração da instituição.
- Recursos de Hardware devidamente controlados e limitados.
- Alta disponibilidade e segurança pois são hospedados em Datacenters com infraestrutura redundante
- Atualização de Softwares automática.
- Capacidade de atender a demanda por Máquinas Virtuais e armazenamento de dados de pesquisadores
- http://jornal.usp.br/ciencias/nuvem-computacional-da-usp-e-aberta-a-comunidade-cientifica/

Autenticação Senha Única USP



Perguntas