Memorial de customizações para uso geral de sistemas corporativos, governamentais, jurídicos, prescrições eletrônicas com tokens

1. DESCRIÇÃO

Descreve-se aqui os processos planejados, executados e documentados como o núcleo de boas práticas operacionais sob responsabilidade da TI, aliado ao uso eficiente dos recursos disponíveis para facilitar a instalação ou reinstalação do sistema operacional.

2. OBJETIVO

O objetivo é garantir que seja reproduzido em todos os computadores dos usuários os mesmos procedimentos de manutenção de forma padronizada e rápida. Há os procedimentos obrigatoriamente realizados pelo administrador responsável pelo ambiente e os procedimentos inerentes ao técnico na bancada. É recomendado que o administrador execute todos os processos e transfira as atividades executivas específicas aos técnicos para completar o ciclo.

3. PROCEDIMENTOS REALIZADOS PELO ADMINISTRADOR

A) Preparação de um desktop/notebook (mínimo um I3, 6G RAM, SSD 240G) pela execução do script preparatório nfs-server.sh que instala o KVM-Linux e o nfs-server (Ver o tutorial 1-PrepararNotebookComNFS-Server.pdf);

B) Download das ISOs das versões estáveis do Clonezilla e do Linux Zorin OS para inicializar no gerenciador de máquinas virtuais VMM (do KVM-linux);

C) Configuração do modelo de máquina virtual (BIOS ou UEFI) com no mínimo 2 (4 melhor) vCPUs virtuais – 2GB(4GB melhor) RAM - HD virtual, dinamicamente alocado de 74 GB - <ver no google Gigabytes X Gibi bytes e digite 80 na caixa gigabytes>). Como criar o HD virtual para uma nova VM KVM no modelo thin provisioning com alocação dinâmica de espaço <qemu-img create -f qcow2 vm/vm.qcow2 74G> supondo que na pasta atual exista a subpasta vm (Ver o tutorial 2-ConfigurarVMnoKVM.pdf);

D) Realizar a instalação padronizada (sem particionamentos extras) para permitir ao clonezilla **expandir** e usar todo o espaço do **SSD** o que proporciona **maior durabilidade** do mesmo;

E) Instalação do Zorin OS na VM modelo (Ver o tutorial 3-InstalarSOnoKVMLinux.pdf) e customização através da execução do script run.sh. Recomenda-se realizar a atualização {executar no terminal como administrador sh /etc/aptcacher.sh} e a gerar a imagem no nfs-server (Ver tutorial 4-BackupDoHDemImagem.pdf) uma vez por mês para mantê-lo atualizado;

F) Exclusão de todas as linguagens, exceto inglês e português na opção Suporte a Idiomas, SFC;

G) Configuração do BleachBit como root com a manutenção das opções English, Português e Português do Brasil nas Preferências dentro da aba Idiomas e respectiva limpeza do sistema. Reproduzir a configuração no ambiente do usuário final;

H) Inicialização da VM customizada com a ISO do Clonezilla para

geração da imagem customizada no nfs-server informando o IP do mesmo;

I) Alterar as permissões (chmod e chown) da pasta /partimag/ e copiar a pasta da imagem customizada do nfs-server primário (notebook/desktop) para o nfs-server de produção(SFC), disponibilizando-o aos técnicos no IP do nfs-server;
J) Preparar um pendrive de boot com o utilitário VENTOY para inicializar com a ISO baixada do Clonezilla.

4. PROCEDIMENTOS REALIZADOS PELO TÉCNICO NA BANCADA

A) Se For o Caso, execute um backup e o anote todos os requisitos do usuário, antes de inicializar o computador em manutenção com o pendrive botável do VENTOY para a restaurar a imagem a partir do nfs-server de produção com o Clonezilla (Ver o tutorial 5-RecoveryImagemDoNFS-server.pdf);
B) Remover o pendrive e re-inicializar o computador pelo sistema operacional restaurado;
C) Criar um novo usuário no Zorin OS. No gerenciador XFCE, clicar no botão <Configurações avançadas> da janela de <Configurações de usuários>, na aba <Privilégios de usuários> selecionar e marcar tudo (Ver o tutorial 7-AdicionanovousuarioComum.pdf);
D) Verificar as conexões de rede do usuário final e restaurar o backup a partir do ProxmoxBackupServer (via comando pxar extract), SFC;
E) Consultar as anotações, reconfigurar as necessidades específicas da estação conforme planilha de requisitos funcionais de cada usuário final:
   a) instalar a nova impressora, mantendo a impressora PDF;
   b) redefinir a nova impressora como padrão;
   c) instalar o emulador HOD no Mozilla ESR;
   d) abrir o terminal PW3270 e configurá-lo no IP 10.67.4.20 e porta padrão da região;
   e) configurar a ferramenta RECOLL para substituir o localizador da Adobe PDF reader, proibido em ambiente corporativo, para localizar sequências de caracteres alfanuméricos ou palavras em contidos nos documentos;
   f) (re)configurar o acesso das pastas compartilhadas, (re)mapeá-las e RENOMEAR EM MAIÚSCULAS o atalho correspondente no gerenciador de arquivos;
   g) verificar o conectividade da internet (abra o terminal e teste o ping no DNS e/ou no FIREWALL/PROXY do provedor);
   h) configurar o digitalizador do aplicativo Epson Scan2 para o endereço IP da impressora EPSON específica na rede, SFC;
   i) restaurar o backup do favoritos no navegador Mozilla, SFC;
   j) A limpeza do SSD/HD com o utilitário BleachBit no usuário final está agendada para ocorrer todo dia 20 de cada mês. A limpeza do sistema ocorre a cada 63 dias via crontab;
   k) Checar o funcionamento das aplicações legadas no ambiente do usuário final. Caso algum usuário ou vírus corrompa o ambiente pré-configurado tentando instalar alguma aplicação Windows, basta remover a pasta oculta .wine e reexecutar o procedimento;
   l) Solicitar ao usuário final que relate se o **ícone** da solução de segurança **corporativa** não estiver visível, o que pode demorar até

um dia em virtude de downloads externos de atualizações;

m) Verificar se os drivers dos tokens estão listados no navegador via ícone Dispositivos de segurança...;
n) desativar aplicações auto iniciados <HP System Tray Service>, <Miniaplicativo Blueman> se não for notebook, e <Screensaver> em Sessão e Inicialização para todas as estações Zorin OS.

5. BENEFÍCIOS ESPERADOS DA CUSTOMIZAÇÃO

Os recursos providos e descritos sumariamente estão disponíveis **após a criação de um novo usuário não administrador**:

A) Reabilitação automática de impressoras pausadas, minimizando visitas de suporte ao usuário;
B) Gerenciamento remoto de impressoras USB compartilhadas no navegador WEB para o administrador, via endereço IP da estação onde está a porta USB;
C) Desativação (nos parâmetros do CUPS) do anúncio por broadcast de impressoras compartilhadas para evitar a poluição na rede;
D) Os nomes dos hosts são atribuído dinamicamente através do servidor DNSmasq, via cadastro do IP e MAC reservado juntamente com o nome do hostname definidos no serviço de DHCP;
E) Possibilidade de pré-configuração da página inicial no Mozilla Firefox SFC (definido na variável site no arquivo adv.ips/gac.ips/hgu.ips) reabilitando das linhas da seção “APLICA A PERSONALIZAÇÃO CORPORATIVA AO MOZILLA STANDARD” no arquivo script4om.sh;
F) Geração dinâmica e integração de senhas e passkeys no KeepassXC com navegadores;
G) Disponibilidade do wine stable (com HOLD, exceto perfil doméstico) para executar ferramentas corporativas legadas no Zorin OS;
H) Disponibilidade do JAVA no Firefox ESR para o HOD do SERPRO, sites e-CAC, GOV.BR, contratos e pregões no governo, assinatura da prescrição eletrônica no CERTILLION, assinatura de processos do PJE, etc;
I) Disponibilidade do terminal PW3270 para acesso ao HOD;
J) Uso da ferramenta RECOLL para localização de sequências de caracteres alfanuméricos ou palavras em documentos;
K) O mozilla ESR autentica em tokens DXSafe, G&D STARSIGN, SAFENET e ALADDIN, **quando criado um segundo usuário**;
L) Disponibilidade do navegador MS EDGE para acessar o conectividade social v2 instalando os plugins listados em no site contabilplay “como-instalar-o-kriptonita-no-microsoft-edge-para-uso-da-conectividade-social-icp-v2”;
M) Disponibilidade do limpador de arquivos BleachBit, similar ao Ccleaner programado no crontab;
N) Disponibilidade de terminais remotos ao usuário final através do protocolo spice via remote-viewer de VM instaladas no Proxmox VE;
O) Monitoramento on-line da saúde do HD/SSD via smartctl;
P) Instalação e atualização automática dos certificados para sites GovBR e do proxy no mozilla do usuário final (em alguns casos deve-se cadastrar o site no painel do java run-time);
Q) Disponibilidade do serviço ssh para manutenção remota (limitado a faixa da rede local informado no arquivo com extensão .ips);
R) Inclusão de dicionários temáticos para profissionais no LibreOffice;

S) Autorreconhecimento da maioria de impressoras Canon, Samsung, Brother, Epson e HP (HP antigas, vide orientações abaixo);
T) O assinador do SERPRO **deve ser instalado no usuário administrador** para assinatura de documentos e acesso as páginas web da Receita conjugado ao JAVA (alguns sites exigem cadastro no java);
U) O assinador do CFM **deve ser instalado no usuário final** para assinatura de receitas e acesso as páginas web conforme manual;
V) O assinador PJE OFFICE PRO **deve ser instalado no usuário final** para assinatura de documentos dos tribunais e acesso as páginas web conforme manual;
W) O Mozilla Firefox ESR quando executado no login de um **segundo usuário** (**não administrador**) onde o drivers de tokens são carregados e reconhecidos pelo navegador, permitem autenticar em sites como o SIAFI, CFM, Tribunais de Justiça, Receita Federal, GOV.BR.
X) Os assinadores exigem os drivers dos tokens carregados no segundo usuário para a assinatura ou verificação de assinaturas, conforme a aplicação.

6. OBSERVAÇÕES

A) Sugere-se uma infraestrutura provisionada com um Proxmox-VE (PVE) e um PROXMOX BACKUP SERVER (PBS). O PVE pode prover recursos de virtualização para os serviços de DHCP/DNS/nome de hosts/NTP, página da web interna, serviço de banco de dados, serviço de gestão de atendimento, serviço de compartilhamento de arquivos autenticado, serviço de gestão de preços praticados no mercado, serviço de gestão de escalas, serviço de gerenciamento de boletins, etc. O PBS provê backup automatizado para todas as VM do PVE e via script para todos os desktops. Os backups dos desktops podem ser recuperados via download na página autenticada do PBS e extraídos pelo comando: pxar extract <archive> [<target>] [OPTIONS].
B) Ao prover um ambiente de rede com um servidor de DHCP com reserva de IP, preferencialmente provido pelo DNSMasq, que informa o IP do servidor de horário, nome do host e provisiona cache de DNS para a rede local, todos os endereços MAC das estações da rede devem estar previamente cadastrados com o respectivo IP e o hostname (com 14 caracteres alfabéticos não acentuados) para que o Clonezilla recupere o IP e se comunique com o IP do servidor NFS. Informe aos técnicos o IP do NFS-SERVER e o caminho onde está a imagem a ser clonada com o Clonezilla. Este SETUP é recomendado para todos os ambientes de rede, pois automatiza muitas tarefas, facilita o processo e minimiza o tempo total que a estação fica em manutenção. Caso a rede local trabalhe com IP fixo, selecionar a opção <<static>> em [Escolha o modo de configuração de rede para esta placa de rede: eth0] da janela | Configuração de rede | e informar sempre o mesmo IP reservado só para manutenção.
C) A escolha do Zorin OS (scripts compatibilizados até versão 17.3), após testes com outros sistemas, deu-se por sua maior estabilidade com sistemas legados Windows (a instalação do WINE 4.0.X em modo HOLD, que pode ser superado, com pequenas alterações, via

Phoenicis PlayOnLinux ou com o Bottles) e disponibilidade de drivers dos tokens, o que reflete em maior compatibilidade com o ambiente corporativo. Os scripts devem funcionar, com pequenos ajustes, nos sabores ?buntu (18.04 ao 22.04) e derivados. Novas versões com a solução das dependências de drivers e as especifidades do gerenciador de janela.

D) Para instalar impressoras HP 1020 e similares, conecte o computador à internet **sem proxy** para baixar o plugin (conecte o celular ao computador via cabo USB e ative a **<Ancoragem via USB>** no celular. No Linux será criado uma nova **<Rede ethernet (usb0)>** e uma nova **<Conexão cabeada>**. Clique sobre a conexão para torná-la ativa). Ligue a impressora e conecte o cabo USB a ambos os equipamentos. Abra a aplicação Impressoras. Aguarde até o plugin acionar o mecanismo da nova impressora. Imprimir a página do teste e no caso de falha, testar estes drivers nesta sequência (1)-PDF, (2)-Postscript e (3)-PCL Laser.

E) Ao instalar uma impressora conectada via RJ-45 ou wi-fi, procure-a na lista pelo endereço IP, clique sobre o endereço IP numérico e aguarde. Siga as orientações. Nomear <seção_função-MODELO_DA_IMPRESSORA>. Caso necessário testar os drivers nesta sequência (1)-PDF, (2)-Postscript e (3)-PCL Laser.

F) Ao instalar impressoras remotas USB, abra o navegador e digite na caixa de pesquisa o endereço http://IP:631 da estação onde estiver fisicamente conectado o cabo. Clique na aba Impressoras e clique sobre o nome da impressora a ser instalada. Copie o link da impressora da barra de endereços para a caixa <Digite o URi do dispositivo> na janela Nova impressora e avance até que seja solicitado o nome. Sugere-se seção_função-MODELO_DA_IMPRESSORA. Caso necessário testar os drivers nesta sequência (1)-PDF, (2)-Postscript e (3)-PCL Laser. Para instalar no Windows siga estas mesmas orientações.

G) O gerenciador de impressão e de compartilhamento de impressoras é realizado no aplicativo system-config-printer. Abra um terminal e digite o comando para abri-lo. Acessar o menu [Servidor], opção [Configurações] e ativar as 5 caixas para que as impressoras locais sejam compartilhadas com o Windows, por exemplo. No caso de impressoras remotas de rede, deixar ativado somente a caixa [Permitir administração remota]. O compartilhamento de impressoras locais é gerenciado no menu Servidor. O controle granular e efetivo do compartilhamento ou não de uma impressora específica é realizado por meio da ativação/desativação da opção [Compartilhada], acessado via botão direito sobre o ícone da impressora instalada. Recomenda-se desativar a opção se for uma impressora remota (evita a poluição na rede com visualizações múltiplas da mesma impressora) e ativar a opção [Compartilhada] para impressoras instaladas localmente, como por USB.

H) Caso os drivers dos TOKENS no usuário (não Administrador) final (DXToken, G&D StarSign, modelos novos da SAFENET/ALADDIN) sejam removidos acidentalmente, como usuário final, abra o terminal e execute **<sh /usr/bin/zorin-tokens-autostart>**.

I) Ícone de instalação do Assinador SERPRO WEB funcional no navegador MOZILLA, conforme ajuda em

https://tutorial.assinadorserpro.estaleiro.serpro.gov.br/html/demo_59.html.

J) Todos os scripts e arquivos de parâmetros são zipados durante a customização para posterior auditoria de segurança no próprio sistema operacional em /etc/skel.

K) Verifique periodicamente as funcionalidades dos scripts para manter atualizados as aplicações, ferramentas e utilitários com a versão do S.O. customizado.

L) Link dos scripts para aplicar em uma instalação em HD ou VM: https://drive.google.com/drive/folders/187bEL4f0feeYIpuYWtGfd2QIl8orTylp?usp=drive_link

M) **Customize a instalação para sua organização editando as variáveis siscofis e site nos arquivo /etc/om.ips conforme faixa de sua rede local ou edite o perfil (adv.ips/gac.ips/hgu.ips) e execute no terminal como root o comando** <sh run.sh #> sendo # a opção do perfil editado 1 para adv.ips, 2 para gac.ips e 3 para hgu.ips.

Os procedimentos acima são operacionalizados via scripts e consolida uma técnica da prática de segurança conhecida como **Linha de Base** para redes de computadores e abrange como o ambiente é configurado e definido. Uma Linha de base é um ponto de referência fixo. Esse ponto de referência pode ser usado para comparar as mudanças feitas em um ambiente. Para otimização operacional, este ponto compreende a geração da imagem de uma instalação padronizada com todas as configurações predefinidas como bloqueios, políticas e recursos de segurança implementados. Esta Linha de Base é replicada via clonagem para novas instalações. A configuração e a instalação adequada pode melhorar muito a segurança e o desempenho de um ambiente. Segue-se alguns exemplos de hardening e ações para o estabelecimento de uma Linha de Base neste pacote abrangido na coletânea de scripts disponível no link acima: restrição do acesso remoto, gerenciamento de backup, ativação automática do Endpoint de segurança corporativo, limpeza automatizada do cache de navegação para minorar a mineração de dados para futuros ataques, atualização automática. Os arquivos PDF do link documentam a execução dos procedimentos e caso alguma atualização cause rupturas na execução, convido-o a realizar pesquisas para a devida compreensão de como deve ser executado novas versões.