Manual do Usuário: Nova Padronização e Acesso SSH no LAMCAD

Manual com o objetivo de orientar os usuários e administradores de máquinas virtuais (VMs) do **LAMCAD** sobre a nova padronização do serviço SSH. Esta é uma importante medida de segurança preventiva implementada para reduzir a superfície de ataque nas VMs dos clientes, protegendo seus dados e pesquisas contra acessos não autorizados.

---

1. O que muda no seu acesso? 🔄

As novas VMs serão entregues com as diretrizes de segurança do LAMCAD, determinando que:

- **Bloqueio de Senhas:** A autenticação convencional por senha foi desativada no servidor SSH (`PasswordAuthentication no`), exceto quando o cliente estiver conectado às redes da UFG.
- **Acesso por Chaves:** O acesso só é permitido utilizando chaves criptográficas públicas e privadas (`PubkeyAuthentication yes`).
- **Acesso Root Bloqueado:** O login direto como usuário `root` está desabilitado (`PermitRootLogin no`).
- **Apenas Usuários Autorizados:** Apenas usuários explicitamente permitidos terão acesso liberado no servidor.
- **Serviço SSHGuard:** O serviço `sshguard` é instalado por padrão para proteger contra ataques de força bruta, monitorando registros de acesso e bloqueando automaticamente endereços IP que apresentem tentativas de login suspeitas ou repetidas.

---

2. Como Gerar e Proteger seu Par de Chaves SSH 🔑

Se você ainda não possui um par de chaves SSH (uma chave pública e uma privada), siga as instruções abaixo para criá-lo.

Passo 2.1: Gerando a chave no Linux, macOS ou Windows (PowerShell)

Abra o seu terminal (ou `PowerShell`) e execute o comando abaixo. Recomendamos a criptografia moderna **ED25519**:

```
ssh-keygen -t ed25519 -C "seu_email@dominio.com"
```

Durante o processo de geração:

1. O sistema perguntará onde salvar a chave (pressione Enter para aceitar o caminho padrão ou outro de seu interesse: `~/.ssh/id_ed25519`).

2. **Defina uma Passphrase (Senha Forte):** O sistema solicitará uma *passphrase*. **Nunca deixe este campo em branco!** Isso garante que, mesmo que alguém roube seu arquivo de chave privada, não poderá usá-lo sem a senha.

🛡️ ***Nota:*** *Uma senha forte deve conter uma combinação de letras maiúsculas e minúsculas, números, caracteres especiais e no mínimo 12 dígitos.*

Boas Práticas de Segurança e Armazenamento:

- 🔒 **Chave Privada (`id_ed25519`):** É o seu segredo. Nunca compartilhe, envie por e-mail, ou suba em repositórios (como GitHub/GitLab). Ela deve ficar exclusivamente no seu computador pessoal.
- 🔓 **Chave Pública (`id_ed25519.pub`):** Esta é a chave que você enviará para os servidores onde deseja se conectar. Ela pode ser compartilhada livremente.
- 💾 **Backup Seguro:** Guarde um backup seguro de suas chaves em um gerenciador de senhas confiável (como Bitwarden or KeepassXC) ou em um armazenamento criptografado offline.

---

3. Simplificando o Acesso com o arquivo config ⚡

Para evitar digitar comandos longos e lembrar portas ou IPs todas as vezes, você pode criar atalhos de conexão.

Como criar o arquivo de atalhos (Todos os Sistemas):

Crie ou edite o arquivo chamado `config` dentro da pasta oculta `.ssh` no seu diretório de usuário.

- **No Linux / macOS:** O caminho é `~/.ssh/config`
- **No Windows:** O caminho é `C:\Users\SEU_USUARIO\.ssh\config`

Abra o arquivo em um editor de texto e adicione o seguinte bloco de configuração:

```
Host vm-lamcad
    HostName IP_OU_DOMINIO_DA_SUA_VM
    User SEU_USUARIO
    Port 22 # Ou 42112, caso sua VM utilize esta porta padrão
    IdentityFile ~/.ssh/id_ed25519
    AddKeysToAgent yes
```

Nota: *Caso o arquivo já exista, você pode simplesmente adicionar este bloco ao final dele. A opção* ***`AddKeysToAgent yes`*** *ajuda a manter a passphrase carregada no agente SSH para facilitar as conexões subsequentes.*

Como conectar agora:
Basta abrir o terminal e digitar apenas o atalho definido no campo Host:
`ssh vm-lamcad`

---

4. Guia por Sistema Operacional do Cliente 💻

4.1 No Windows

Para obter a melhor experiência no Windows, uma sugestão é o uso do aplicativo oficial **Terminal do Windows (Windows Terminal)**.

- **Instalação do Aplicativo Recomendado:** Baixe e instale gratuitamente na Microsoft Store através deste link oficial: Terminal do Windows - Microsoft Store.
- **Como acessar:** Abra o Terminal do Windows, certifique-se de estar usando uma aba do *PowerShell* ou do *Prompt de Comando*, e utilize os comandos nativos do OpenSSH (como o `ssh vm-lamcad` configurado no passo anterior).

4.2 No Linux / macOS

- Estes sistemas já trazem o cliente OpenSSH instalado de fábrica de maneira nativa.
- Basta abrir o terminal padrão de sua preferência e utilizar os comandos citados nas seções 2 e 3.

---

5. Seção do Administrador: Como padronizar manualmente VMs não integradas ⚙️

Se você possui uma Máquina Virtual (VM) com sistema operacional **Debian, Ubuntu ou Rocky Linux** ofertados pelo LAMCAD e que ainda não recebeu a automação centralizada do LAMCAD via Ansible, siga este passo a passo para aplicar manualmente a padronização de segurança.

Passo A: Copiar sua Chave Pública para a VM

Antes de bloquear o acesso por senha, você precisa garantir que a sua chave pública SSH está instalada na VM. No seu computador local, envie a chave executando:

```
ssh-copy-id -i ~/.ssh/id_ed25519.pub -p PORTA_SSHD
SEU_USUARIO@IP_DA_VM
```

(Insira sua senha atual da VM para confirmar a transferência).

Passo B: Configurar as permissões corretas da pasta SSH

Conecte-se na VM e certifique-se de que os arquivos de chaves possuem permissões extremamente restritivas para que o SSH funcione de forma segura:

```
chmod 700 /home/SEU_USUARIO/.ssh
chmod 600 /home/SEU_USUARIO/.ssh/authorized_keys
```

```
chown -R SEU_USUARIO:SEU_USUARIO /home/SEU_USUARIO/.ssh
```

Passo C: Modificar as diretivas do Servidor SSH

Com o intuito de aplicar a padronização oficial do **LAMCAD**, orientamos a elaboração de um arquivo de parametrização específico no diretório de inclusão **`sshd_config.d`**. Tal procedimento assegura a integridade do arquivo principal **`/etc/ssh/sshd_config`**, mantendo-o organizado.

1. Inicialmente, certifique-se de que a instrução a seguir esteja ativa (sem o caractere de comentário **`#`**) no topo do seu arquivo **`/etc/ssh/sshd_config`**:
2. **Verificação de Inclusão:**
   `Include /etc/ssh/sshd_config.d/*.conf`

3. Prossiga com a criação do arquivo de configuração dedicada para o ambiente LAMCAD:
4. **Criação do Arquivo:**
   `sudo nano /etc/ssh/sshd_config.d/99-lamcad-standard.conf`

5. Insira o bloco de diretrizes padrão estabelecido por nossa equipe de infraestrutura:

Atenção: Na diretiva `AllowUsers` do bloco abaixo, substitua os usuários de exemplo pelos nomes reais das contas de usuário que devem ter acesso ao servidor, separando-os apenas por espaços em branco.

Bloco de Configuração:

```
# ====================================================================
# Configurações Padronizadas de Segurança - LAMCAD
# ====================================================================

# --- Autenticação ---
Protocol 2
UsePAM yes
MaxAuthTries 4
LoginGraceTime 60
# Lista de usuários autorizados, separados por espaço em branco
AllowUsers usuario1 usuario2 usuario3
PermitRootLogin no
PermitEmptyPasswords no
PubkeyAuthentication yes
PasswordAuthentication no
AuthenticationMethods publickey
KbdInteractiveAuthentication no
ChallengeResponseAuthentication no

# --- Segurança Fina ---
X11Forwarding no
AllowTcpForwarding yes
```

```
AllowAgentForwarding no
AllowStreamLocalForwarding no
PermitUserEnvironment no
GatewayPorts no
PermitTunnel no
PermitUserRC no
StrictModes yes

# --- Sessões e Limites ---
UseDNS no
MaxSessions 10
MaxStartups 10:30:60
ClientAliveInterval 300
ClientAliveCountMax 3
LogLevel VERBOSE

# --- Banners ---
PrintMotd no
Banner none
PrintLastLog yes

# --- Exceção para Redes Internas da UFG ---
# Permite autenticação por senha caso a conexão tenha origem dentro da
UFG
Match Address 200.137.192.0/19,200.137.244.0/22,2001:12f0:0c0b::/48
    PasswordAuthentication yes
    AuthenticationMethods password publickey
```

Nota: *Para efetuar a gravação no editor Nano, utilize* ***Ctrl + O*** *seguido de* ***Enter****, finalizando a edição com* ***Ctrl + X****.*

Entendendo as Principais Diretivas de Segurança Aplicadas 🛡️

Para melhor compreensão das mudanças efetuadas em sua VM, destacamos os principais parâmetros implementados:

- **`PasswordAuthentication no:`** Inabilita o uso de senhas convencionais, mitigando riscos de intrusão por ataques de força bruta.
- **`PubkeyAuthentication yes:`** Estabelece a autenticação via chaves criptográficas como o padrão obrigatório de segurança.
- **`AuthenticationMethods publickey:`** Restringe o acesso exclusivamente ao método de desafio por chave pública.
- **`PermitRootLogin no:`** Bloqueia o acesso direto como **root**. Deve-se acessar com usuário comum e elevar privilégios via **sudo**.
- **`PermitEmptyPasswords no:`** Impede que contas sem credenciais definidas sejam exploradas remotamente.
- **`KbdInteractiveAuthentication no:`** Desabilita entradas interativas de teclado, reforçando a exclusividade do acesso por chave.

- **`Match Address:`** Regra de exceção para redes da UFG, permitindo temporariamente o uso de senha em conexões originadas no ambiente acadêmico interno.

Passo D: Validar a sintaxe e reiniciar o serviço

Antes de reiniciar o SSH, valide se não há erros de sintaxe no arquivo de configuração:
`sudo sshd -t`

Se o comando não retornar nenhuma mensagem de erro, reinicie com segurança o serviço correspondente à sua distribuição:

- **No Debian e Ubuntu:**

  ```
  sudo systemctl restart ssh
  ```

- **No Rocky Linux:**

  ```
  sudo systemctl restart sshd
  ```

Atenção Administrador: Mantenha sua sessão SSH atual aberta! Abra um novo terminal em seu computador pessoal e tente se conectar utilizando sua chave. Apenas feche a sessão antiga quando tiver certeza absoluta de que o login por chave está funcionando com sucesso. Caso tenha dúvidas ou precise de auxílio nesta configuração pode entrar em contato com a equipe Técnica do LAMCAD.