Manual do Usuário: Nova Padronização e Acesso RDP no LAMCAD

Este manual tem como objetivo orientar pesquisadores, alunos e administradores de Máquinas Virtuais (VMs) com sistema operacional **Windows Server** hospedadas no **LAMCAD** sobre a nova padronização de segurança para acesso à Área de Trabalho Remota (RDP). Essa medida preventiva visa eliminar a exposição direta do protocolo RDP na internet pública, mitigando riscos de ataques de força bruta, exploração de vulnerabilidades, varreduras automatizadas e sequestro de dados (*ransomware*).

1. O que muda no seu acesso? 🔄

Em conformidade com a política de *hardening* e redução de superfície de ataque do LAMCAD, o modelo de acesso aos servidores Windows Server foi reformulado:

- **Bloqueio da Porta Pública RDP (TCP 3389):** A porta de conexão remota foi totalmente bloqueada no firewall de borda da infraestrutura. Não é mais possível conectar diretamente pelo IP público ou domínio externo da VM sem intermediação de rede privada.
- **Acesso Exclusivo via VPN Privada (Tailscale):** O acesso remoto só é permitido através do IP privado virtualizado (faixa `100.x.x.x`) atribuído pela malha de VPN da plataforma Tailscale.
- **Nativo Multiusuário e Simultâneo:** Por padrão, o Windows Server já suporta nativamente até duas conexões simultâneas de administração RDP com contas de usuário distintas sem necessidade de configurações adicionais.
- **Descentralização com *Node Sharing*:** Os pesquisadores responsáveis pelas VMs possuem autonomia para conceder ou revogar o acesso de colaboradores da pesquisa via convites seguros utilizando o console web oferecido pela Tailscale, sem depender da intermediação constante da equipe de TI.

⚠️ **Importante para Administradores de Projetos:** Até que o LAMCAD disponibilize um serviço corporativo interno de VPN unificado, o uso do **Tailscale no plano *Free Tier*** foi homologado como a solução oficial temporária. O plano gratuito oferece capacidade para até 100 dispositivos e compartilhamento sem limites de usuários por máquina.

2. Visão Geral da Arquitetura e Viabilidade Técnica 🛠️

A solução baseia-se em um modelo ***Zero Trust Mesh VPN***. A conexão entre o computador do pesquisador e o Windows Server ocorre de forma criptografada de ponta a ponta, sem a necessidade de abertura de portas no roteador ou de configurações de NAT públicas.

Componente	Configuração / Função	Benefício de Segurança
Windows Server	Agente Tailscale em *Unattended Mode* (Modo Autônomo)	O serviço inicia automaticamente no boot antes do logon, garantindo persistência sem depender de sessão gráfica aberta.
Firewall de Borda	Regra de Bloqueio Drop/Deny para a porta 3389 na interface WAN	Elimina completamente o tráfego não solicitado de ataques de força bruta vindos da internet pública.
Clientes (Estações)	Tailscale instalado no Windows, Linux (Debian, Ubuntu, Rocky Linux) ou macOS	Acesso seguro via IP 100.x.x.x nativo pelo cliente RDP (MSTSC, Remmina, etc.).
Gestão de Acesso	Recurso de *Node Sharing* (Compartilhamento de Nós)	Sem compartilhamento de senhas da conta VPN; revogação de acessos individuais em 1 clique.

3. Configuração do Servidor (Seção do Administrador da VM) ⚙️

Se você é o pesquisador responsável pela VM Windows Server e precisa padronizar sua máquina antes do desligamento da regra pública no firewall de borda, siga o procedimento abaixo.

Passo 3.1: Instalação do Agente e Ativação do *Unattended Mode*

1. Crie uma conta gratuita no portal oficial do Tailscale (https://login.tailscale.com/) obrigatoriamente usando seu e-mail pessoal, pois **o uso de e-mail institucional não funcionará**, visto que a UFG não dá suporte a este serviço, ou utilize uma das opções de *Single Sign On* disponíveis.
2. Acesse o Windows Server, baixe e execute o instalador oficial do Tailscale para Windows https://tailscale.com/download/windows.
3. Após a instalação, será sugerido que faça o login inicial no aplicativo para vincular a VM à sua conta do Tailscale, utilize a conta que foi criada no passo 1 anterior.
4. No Windows Server, clique com o botão direito no ícone do Tailscale próximo ao relógio, vá em ***Preferences*** e marque a opção ***Run unattended***, como visto na Figura 1. Isso

garante que o serviço de VPN inicie automaticamente com o sistema operacional.

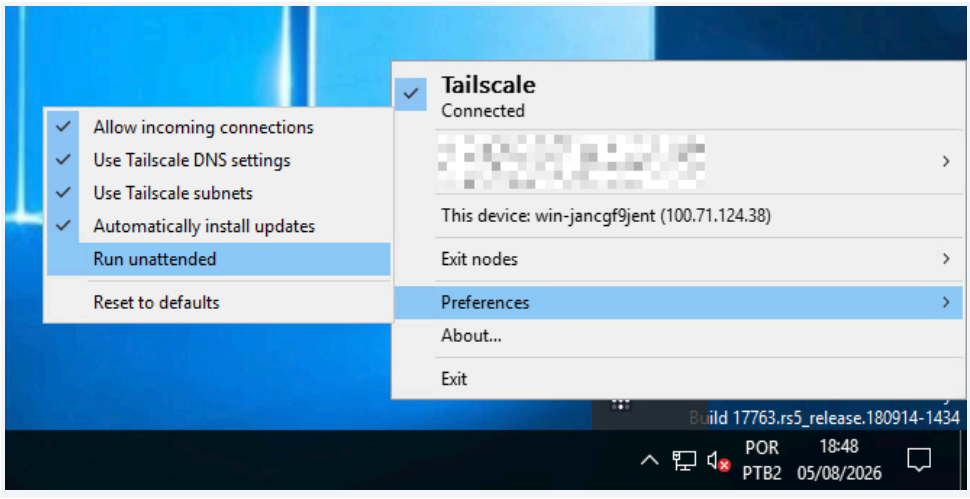

Figura 1: Ativar a opção *Run unattended* para inicializar automáticamente no boot

5. Acesse o painel web do Tailscale (*Admin Console*), localize a VM na aba *Machines*, abra as opções (três pontos) e marque **Disable Key expiry** (Figura 2) para evitar a perda automatizada de conexão após alguns meses.

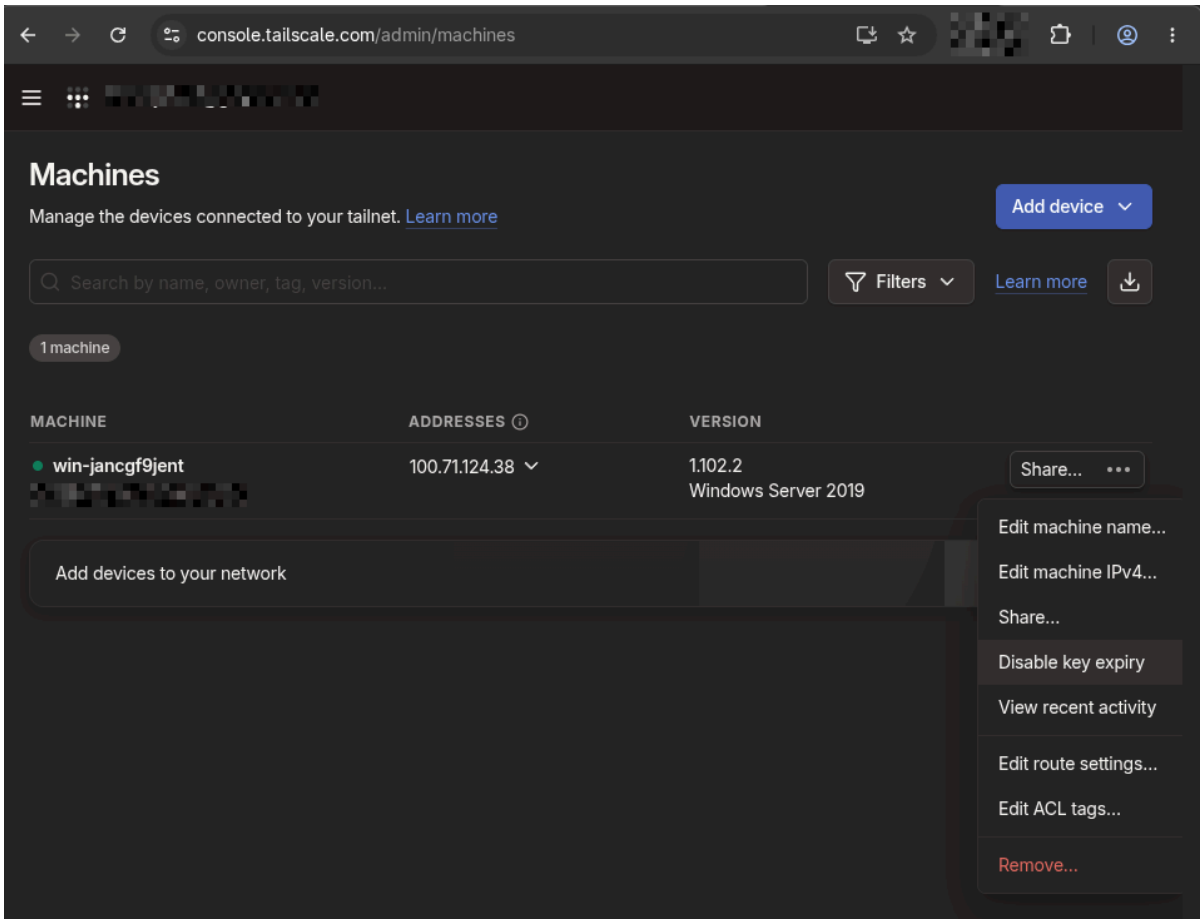

Figura 2: Desabilitar a automação que expira a chave de acesso do *endpoint* criado.

Passo 3.2: Gestão de Usuários Locais para Acesso Simultâneo

Como o Windows Server permite nativamente 2 sessões simultâneas de administração, basta criar usuários locais distintos para cada pesquisador e adicioná-los ao grupo de acesso remoto, caso não queiram compartilhar contas locais:

1. Acesse o **Gerenciamento do Computador** (`compmgmt.msc`) > **Usuários e Grupos Locais** > **Usuários**.
2. Crie a conta para o colaborador (ex: user1) definindo uma senha forte, caso ainda não tenha uma conta.
3. Adicione esta conta ao grupo local **Usuários do Sistema Remoto** (*Remote Desktop Users*), como detalhado na Figura 3.

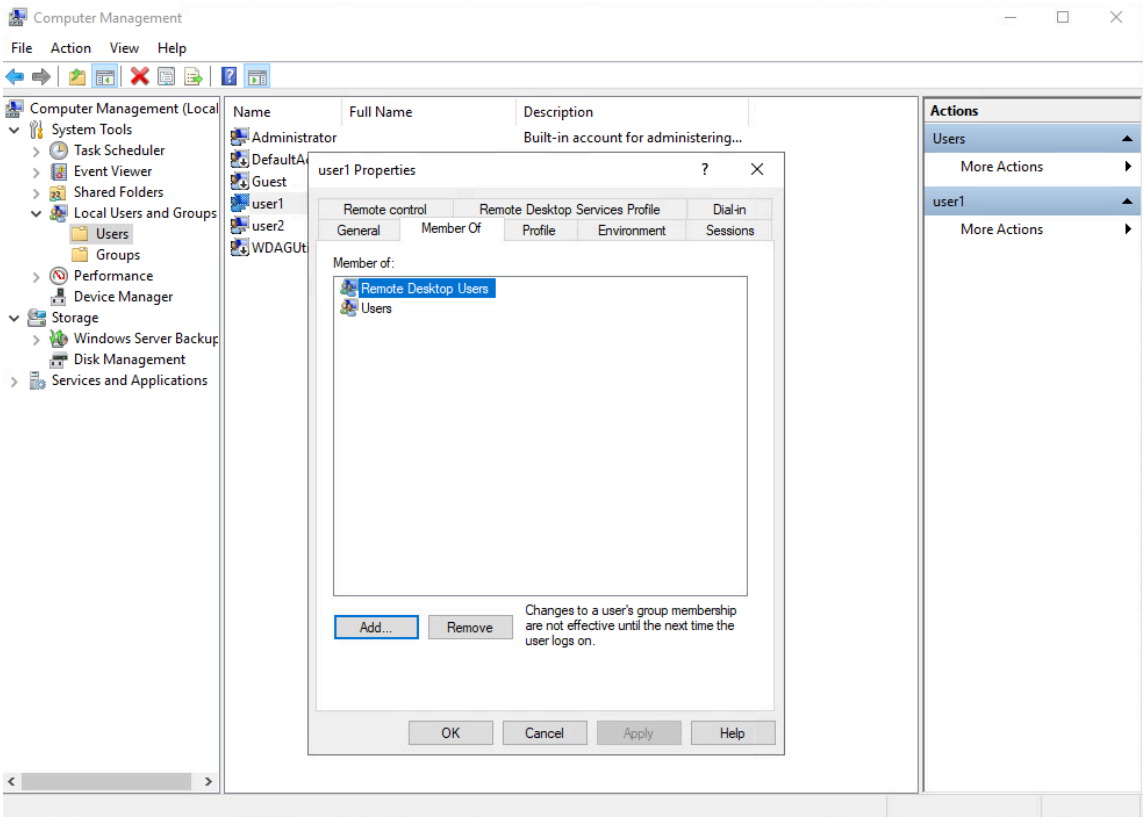

Figura 3: Janela do 'compmgmt.msc' exibindo o grupo 'Remote Desktop Users' com os usuários do projeto adicionados.

Passo 3.3: Compartilhando o Acesso com Outros Pesquisadores (*Node Sharing*)

Para conceder acesso aos membros do laboratório sem compartilhar a sua senha pessoal do Tailscale:

1. Acesse o painel web do Tailscale no seu computador pessoal (*Admin Console* >

Machines).
2. Localize a VM do laboratório e clique no botão ***Share...***.
3. Gere o link único de convite ou insira o e-mail do colaborador e envie para ele.

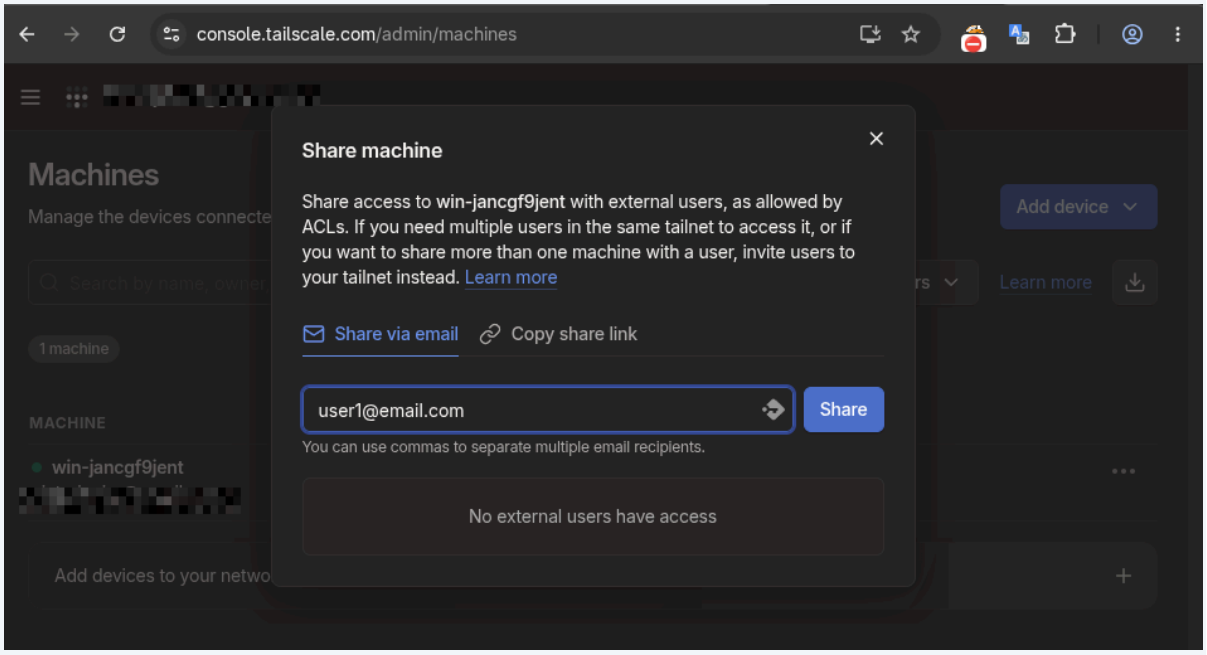

Figura 4: Painel Admin Console do Tailscale destacando a opção 'Share' na máquina servidor e o modal de geração do link de convite.

💡 **Vantagem do *Node Sharing* no Plano Gratuito:** Não há limitação no número de usuários com quem você pode compartilhar uma VM individual via *Node Sharing* no plano Free Tier. Cada pesquisador utiliza sua própria conta gratuita para autenticar.

4. Guia de Conexão do Cliente por Sistema Operacional 💻

4.1 No Windows (Cliente)

1. Crie uma conta gratuita no Tailscale e instale o aplicativo cliente no seu computador pessoal, caso ainda não tenha uma conta criada.
2. Abra o link de convite enviado pelo responsável da VM para aceitar o compartilhamento da máquina.
3. Abra o aplicativo nativo **Conexão de Área de Trabalho Remota** (`mstsc.exe`).
4. No campo *Computador*, insira o IP do Tailscale da VM Windows Server configurada no Passo 3.1 (ex: `100.x.x.x`).
5. Insira seu usuário e senha do Windows Server configurados pela equipe da pesquisa e clique em **Conectar**.

4.2 No Linux (Debian, Ubuntu e Rocky Linux)

Em distribuições Linux, a conexão é feita instalando e habilitando o serviço do Tailscale via terminal e utilizando o cliente RDP **Remmina** ou outro de sua preferência.

1. Instalação e Ativação do Tailscale:

- **No Ubuntu / Debian:**
```
curl -fsSL https://tailscale.com/install.sh | sh
sudo systemctl enable --now tailscaled
sudo tailscale up
```

- **No Rocky Linux / RHEL:**
```
sudo dnf config-manager --add-repo
https://pkgs.tailscale.com/stable/rhel/8/tailscale.repo
sudo dnf install -y tailscale
sudo systemctl enable --now tailscaled
sudo tailscale up
```

(Acesse a URL gerada no terminal pelo comando `tailscale up` no seu navegador para autorizar o dispositivo).

2. Instalação do Remmina e Conexão RDP:

- **Ubuntu / Debian:** `sudo apt install remmina remmina-plugin-rdp -y`
- **Rocky Linux:** `sudo dnf install remmina -y`

Abra o Remmina, selecione o protocolo **RDP**, digite o IP do Tailscale (`100.x.x.x`) no campo de endereço e insira as credenciais do Windows Server para conectar.

4.3 No macOS

1. Baixe o **Tailscale** na Mac App Store e realize o login.
2. Baixe o aplicativo oficial **Microsoft Remote Desktop** na Mac App Store.
3. Adicione um novo PC inserindo o IP `100.x.x.x` do Tailscale e conecte-se com suas credenciais do servidor.

5. Boas Práticas e Recomendações de Segurança 🛡️

- **Contas de Usuário Individuais:** Crie sempre usuários locais distintos no Windows Server para cada pesquisador (ex: pesquisador.joao, pesquisador.maria) e adicione-os ao grupo *Usuários do Sistema Remoto*. Evite o uso compartilhado da conta Administrador.
- **Senhas Fortes:** Mantenha senhas complexas (mínimo de 16 caracteres contendo letras maiúsculas, minúsculas, números e caracteres especiais) em todos os usuários com permissão de login remoto.
- **Revogação Imediata:** Ao término de um projeto de pesquisa ou desligamento de um colaborador, o responsável pela VM deve acessar o painel do Tailscale e revogar o compartilhamento da máquina correspondente de imediato.