

Distrito Linux Tails

Eduardo H. Machado¹, Rosialdo Q. Vicente¹, Venícius J. Oliveira¹

¹ Universidade Federal de Roraima (UFRR)

Campus Paricarana – Boa Vista – RR – Brazil

edu.hen.fm@gmail.com, rosialdovideinho3@gmail.com,
veniciusjoliveira@gmail.com

Abstract. *This report describes a security-focused Linux distribution, Tails Linux. It gives a broader vision towards Tails, from its visual aspects to its daemons and packages. It also goes over Tails' most distinguishing features, which sets it apart from other distributions, like its integration with Tor networks and amnesic storage.*

Resumo. *Este relatório descreve uma distribuição Linux com foco em segurança, Tails Linux. Ele fornece uma visão geral acerca da Tails, desde seus aspectos visuais até suas daemons e pacotes. Ele também trata das características mais distinguíveis da Tails, que a diferencia de outras distribuições, como sua integração com a rede Tor e seu armazenamento amnésico.*

1. Visão Geral e Objetivos da Distribuição

A distribuição Tails (The Amnesic Incognito Live System) do Linux visa oferecer um ambiente seguro e portátil para o usuário, usando de recursos como: rede Tor; armazenamento amnésico; e aplicativos com criptografia de ponta. Isso permite que o usuário mantenha seu anonimato e navegue pela internet deixando o mínimo de rastros possíveis. Ela também se propõe a ser um sistema completamente gratuito e open-source.

2. Ambiente Gráfico

O ambiente gráfico utilizado pela Tails é o GNOME, que é amplamente utilizado pela comunidade Linux, oferecendo um alto nível de customização, por meio de suas extensões, e suporte, por meio tanto da comunidade quanto da sua robusta documentação.

No entanto, quando comparada com outras GUIs (Graphical User Interfaces), como o XFCE, KDE e Cinnamon, temos que o GNOME é mais custoso em recursos do sistema, o que pode levar a uma pior performance.

3. Papéis de Parede, Ícones e Cores

Os papéis de parede padrões da Tails são os mesmos da Debian, sua distribuição base. Já o pacote de ícones presente na distribuição é o Adwaita, muito comum dentro da comunidade também. No mais, suas cores de destaque são o roxo e o verde.

4. Requisitos Mínimos e Instalação

4.1. Requisitos Mínimos

Os requisitos mínimos para o uso da Tails são 2 GB de RAM, um processador de 64 bits compatível com x86-64 e um pendrive USB ou DVD de no mínimo 8 GB.

4.2. Instalação

Sua instalação pode ser realizada a partir de diferentes sistemas operacionais, como Windows, Linux e MacOS. O processo é simples, basta baixar a imagem da Tails diretamente do site, verificá-la, instalar em um pendrive USB ou DVD usando BalenaEtcher (Windows e MacOS) ou Gnome Disks (Linux), reiniciar o computador e fazer boot pelo dispositivo removível.

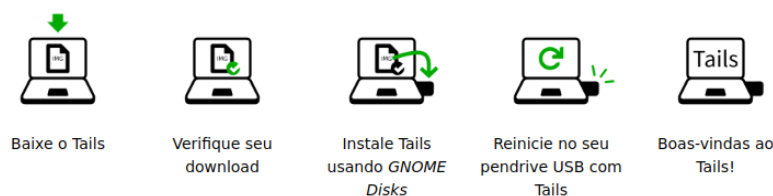


Figura 1. Exemplo de passo a passo para instalação a partir do Linux

5. Vantagens e Facilidades

A maior vantagem obtida quando se usa a Tails é sua extrema segurança, começando pelo modo de uso, que é através de um pendrive USB ou DVD, para deixar menos rastros, permitindo que ele possa ser inicializado em qualquer aparelho se estiver com as configurações necessárias.

Além disso, temos também que toda conexão à internet realizada por meio da Tails passa por 3 retransmissões na rede Tor, tornando muito complexo o rastreamento do usuário, e permitindo acessar conteúdos restringidos por censura local.

Não obstante a isso, Tails oferece uma gama de aplicativos seguros para realizar operações do dia a dia, com criptografia de ponta. Quando unimos isso ao armazenamento amnésico, que esquece todos os dados utilizados localmente durante aquela sessão, temos um sistema muito seguro.

Por fim, Tails é gratuito, open-source e extremamente transparente em suas operações, como é possível concluir por meio das finanças e contrato social disponíveis na documentação. Além destes, também é possível confirmar sua confiança por meio de seus patrocinadores, usuários e assinaturas.

6. Pacotes

Os gerenciadores de pacotes padrões da Tails são DPKG e APT. Esses gerenciadores são padrões de distribuições baseadas em Debian, com o APT servindo de front-end para o DPKG, oferecendo recursos como instalação de dependências de um pacote.

A Tails, recém instalada, acompanha cerca de 1900 pacotes, como foi verificado usando o comando `apt list --installed | wc -l`. Como o nosso foco não é descrever pacote por pacote, mas sim fornecer uma visão geral sobre a distribuição, foram escolhidos os aplicativos/pacotes mais interessantes para análise abaixo.

6.1. LibreOffice

Envolve uma série de ferramentas de escritório, como editores de texto, planilhas e slides, por exemplo. É importante ressaltar que as ferramentas fornecidas pelo LibreOffice são totalmente gratuitas e de código aberto, tornando-as uma boa opção para um sistema seguro.

6.2. Thunderbird

O Thunderbird é um aplicativo com código aberto que oferece muitas utilidades na questão de segurança, como a criptografia de e-mails, aviso de possíveis links e e-mails maliciosos e proteção contra golpes.

6.3. Kleopatra

Kleopatra é um gerenciador de certificados que pode armazenar certificados e chaves OpenPGP, de uso comum entre usuários da Tails. Tem versões para Windows e Linux.

6.4. KeePassXC

Essa aplicação de código aberto permite que o usuário gerencie suas senhas no computador de forma segura e com criptografia, podendo ser usado em diferentes sistemas como Linux e Windows.

6.5. Tor Browser

Com esse navegador podemos usar a internet via rede Tor, e com isso obtemos várias vantagens do ponto de vista da segurança, como, por exemplo, não armazenar o histórico de navegação e passar por 3 retransmissores durante a conexão para impedir o rastreamento da navegação.

6.6. VeraCrypt

Com esse programa conseguimos criptografar a memória do computador e criar um disco virtual criptografado.

6.7. OnionShare

OnionShare é uma ferramenta que permite o envio de arquivos, hospedagem de sites e bate papo de forma anônima, tudo feito pela rede Tor, trazendo mais segurança e privacidade para o compartilhamento de dados.

6.8. LUKS

Outro software que se propõe a fazer uma criptografia do disco rígido. Ele é multiplataforma e também possibilita o gerenciamento de senhas.

6.9. GtkHash

GtkHash é um aplicativo gráfico que passa um texto por uma das várias funções de hashing fornecidas.

6.10. Pidgin

Este aplicativo permite se conectar a múltiplos servidores de chat simultaneamente, como IRC e XMPP. Ele é completamente gratuito e open-source.

6.11. mat2

Essa ferramenta, que também é uma biblioteca em Python, permite fazer a remoção de metadados de outros arquivos, como fotos, documentos e vídeos, por exemplo.

6.12. Feather

Esse aplicativo é uma carteira de Monero rápida, segura e de fácil uso. Além disso, é multiplataforma, livre e de código aberto.

6.13. Electrum

Esse aplicativo é uma carteira de Bitcoin fácil, segura e rápida que oferece diversas ferramentas para gerenciar seu dinheiro. Não obstante a isso, é gratuito e de código aberto.

6.14. Audacity

Audacity é um aplicativo de gravação e edição de áudio em múltiplas tracks. Além de ser grátis e open-source, ainda fornece suporte para múltiplos sistemas operacionais.

6.15. GIMP

Esse aplicativo lida com edição de imagens raster. Seria o equivalente a um Adobe Photoshop, porém grátis e open-source.

6.16. Inkscape

Inkscape é uma ferramenta de criação de imagens vetoriais. Seria o equivalente a um Adobe Illustrator, porém grátis e open-source.

7. Kernel

A versão do kernel da Tails mais atual no momento da escrita deste trabalho, versão 5.2, verificada através do comando `uname -r`, é 5.10.0-15-amd64. Essa versão atualmente se encontra como LTS (Long Term Support).

De acordo com o site It's Foss, essa versão traz diversas melhorias em relação aos anteriores, das quais, algumas das mais interessantes são: melhorias em compatibilidade com processadores; adição de suporte a novos processadores e placas de vídeo; melhorias em performance em questões de armazenamento; prevenção contra novos ataques; e melhor compatibilidade com drivers.

8. Histórico

A distribuição não parece oferecer muitas vantagens para as empresas, mas é utilizada por pessoas que não querem ser rastreadas, o que pode incluir desde pessoas num país com uma censura muito rígida até criminosos cibernéticos. De acordo com a Wired, um caso famoso de uso da Tails é o de Edward Snowden, que o utilizou durante o escândalo de compartilhamento de dados confidenciais dos EUA (Estados Unidos da América).

8.1. Tails 1.0

Após quase 5 anos de desenvolvimento, o sistema operacional ganhou a sua versão 1.0, demonstrando a maior maturidade desde a sua concepção, no 36º lançamento estável do Sistema. Algumas das características da versão foram atualizações automáticas, suporte para pontes Tor, falsificação de endereço MAC, entre outros.

8.2. Tails 2.0

Nessa versão foi implementado o recurso para corrigir o indicador de força da senha dos discos GNOME. Outras mudanças foram atualizações do navegador Tor, remoção da Claws Mail como cliente de e-mail padrão, sendo substituído pelo Icedove. Houveram correções de desempenho da Tails Upgrader, que tornava as atualizações automáticas muito lentas para serem aplicadas. Ela também parou de oferecer a opção de abrir arquivos baixados por aplicativos externos no navegador Tor.

8.3. Tails 3.0

A Tails 3.0 foi baseada na versão 9 do Debian. Nessa versão, a Tails parou de funcionar em computadores de 32 bits, passando a funcionar apenas em computadores de 64 bits, decisão esta que foi tomada por questões de segurança. O Tor foi atualizado para a versão 7.0 (baseado no Firefox), que é multiprocesso, abrindo caminho para o conteúdo sandboxing.

8.4. Tails 4.0

Temos agora a Tails 4.0 baseada no Debian 10. Essa versão trouxe atualizações na maioria dos softwares padrões da Tails, como também importantes melhorias na usabilidade e desempenho. Foi a versão com maior número de mudanças e correções de problemas de segurança. Os principais softwares atualizados foram o OnionShare, da versão 0.9.2 para 1.3.2, e o Tor. Além disso, o KeePassX foi substituído pelo KeePassXC.

8.5. Tails 5.0

A versão mais recente da Tails é a 5.0. nessa versão a Tails é baseada no Debian 11. Ela trouxe versões novas de vários softwares incluídos na Tails e novas ferramentas OpenPGP. Foi adicionado o Kleopatra para substituir o Applet OpenPGP, porque o Applet OpenPGP não estava mais sendo mantido ativamente, enquanto o Kleopatra fornece recursos semelhantes em uma única ferramenta e está sendo desenvolvido de forma mais ativa.

9. Segurança

Como o foco da distribuição é segurança, a Tails oferece um dos ambientes mais seguros tratando de sistemas Linux, fornecendo diversas ferramentas para manter o anonimato do usuário, como: Tor para conectar e navegar pela internet; Thunderbird para e-mails criptografados; OnionShare para compartilhar arquivos pela rede Tor; entre outras.

A Tails também tem armazenamento amnésico por padrão, não salvando dados localmente, a não ser que explicitamente requerido pelo usuário. Além disso, sua portabilidade permite um fácil descarte, permitindo se tornar praticamente irracional. Todas essas características, em conjunto, tornam a Tails uma das distribuições mais seguras do ecossistema Linux.

10. Documentação

A documentação da Tails é extensa, porém tem um foco em seus aplicativos e como usufruir destes, deixando o usuário um pouco desamparado em relação a troubleshooting. Mas, considerando que a distribuição é do tipo portátil, similar a dispositivos plug-and-play, a maioria de seus problemas deve ser relacionada ao boot do sistema, o que é tratado na documentação. Abaixo se encontram os principais tópicos discutidos na documentação.

10.1. Informações Gerais

Essa seção trata de temas mais abrangentes, como os requisitos de sistema, avisos sobre o uso da Tails, acesso ao seu código fonte, registros das finanças para desenvolvimento, missões e valores defendidos pelos desenvolvedores e agradecimentos.

10.2. Baixar, instalar e atualizar

Essa seção nos traz como realizar a instalação da Tails a partir de outros sistemas, como gravá-lo em um DVD, como iniciá-lo numa máquina virtual, como obter suas imagens ISO, como atualizar a partir de um pendrive e como resetar um pendrive.

10.3. Primeiros Passos com Tails

Essa seção é sobre questões de acessibilidade e sobre alguns dos recursos mais exclusivos da Tails, como a definição da senha de administração por sessão, gerenciamento do armazenamento persistente, instalação de programas adicionais, uso do GNOME, como reportar um erro e como desligar o sistema.

10.4. Internet Anônima e Sem Censura

Essa seção é primordialmente sobre redes, principalmente a rede Tor, tratando sobre como se conectar ao Wi-Fi, como se conectar à rede Tor e como usar o navegador Tor. Ela também trata do uso de aplicativos específicos, como OnionShare para compartilhamento de arquivos, Thunderbird para acessar e-mails e ler notícias, Electrum para realizar transações com criptomoedas e Pidgin e OTR para chats.

10.5. Criptografia e Privacidade

Essa seção fala sobre o uso de aplicativos específicos para segurança, como KeePassXC para gerenciar senhas, Kleopatra para criptografar textos e arquivos, LUKS para criar e usar volumes criptografados, VeraCrypt para usar volumes criptografados, GtkHash para calcular somas de verificação e o uso do teclado de tela.

10.6. Trabalhe com Documentos Importantes

Essa seção é voltada para ferramentas de escritório e/ou trabalho, como aplicativos de texto, planilhas, gráficos, áudio, vídeo e impressão. No mais, também é tratada a remoção de metadados usando mat2.

10.7. Tópicos Avançados

Essa última seção aborda tópicos mais específicos, como opções de boot avançadas, acesso a discos rígidos internos, virtualização da Tails, uso do armazenamento persistente, habilitação de dispositivos sem fio, defesa contra ataques cold boot e uso de Dino e Feather.

11. Hardware

Os requisitos mínimos para operação da Tails incluem: 2 GB de RAM; pendrive USB ou DVD com 8 GB; e processador compatível com arquitetura x86-64. Apesar disso, há alguns hardwares específicos que não funcionam ou podem apresentar incompatibilidades com a Tails, como os apresentados abaixo.

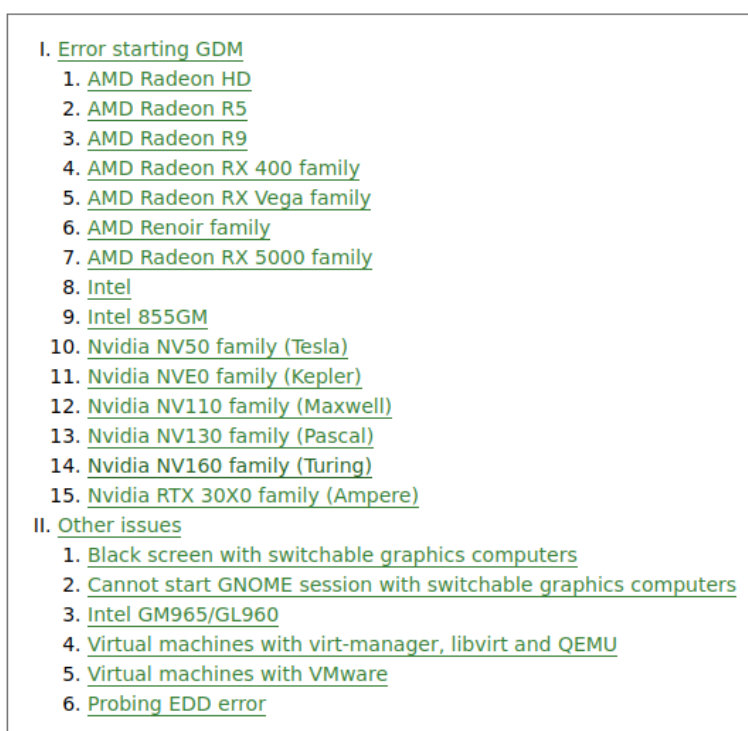
- 
- The image shows a screenshot of a document with a list of hardware compatibility issues. The list is organized into two main sections: 'I. Error starting GDM' and 'II. Other issues'. Each section contains a numbered list of specific hardware models or configurations that may cause problems. The text is in a standard font, and the list items are underlined.
- I. [Error starting GDM](#)
 - 1. [AMD Radeon HD](#)
 - 2. [AMD Radeon R5](#)
 - 3. [AMD Radeon R9](#)
 - 4. [AMD Radeon RX 400 family](#)
 - 5. [AMD Radeon RX Vega family](#)
 - 6. [AMD Renoir family](#)
 - 7. [AMD Radeon RX 5000 family](#)
 - 8. [Intel](#)
 - 9. [Intel 855GM](#)
 - 10. [Nvidia NV50 family \(Tesla\)](#)
 - 11. [Nvidia NVE0 family \(Kepler\)](#)
 - 12. [Nvidia NV110 family \(Maxwell\)](#)
 - 13. [Nvidia NV130 family \(Pascal\)](#)
 - 14. [Nvidia NV160 family \(Turing\)](#)
 - 15. [Nvidia RTX 30X0 family \(Ampere\)](#)
 - II. [Other issues](#)
 - 1. [Black screen with switchable graphics computers](#)
 - 2. [Cannot start GNOME session with switchable graphics computers](#)
 - 3. [Intel GM965/GL960](#)
 - 4. [Virtual machines with virt-manager, libvirt and QEMU](#)
 - 5. [Virtual machines with VMware](#)
 - 6. [Probing EDD error](#)

Figura 2. Hardware que pode apresentar incompatibilidade com Tails

- Tails não funciona com modelos de Mac que usam o chip [Apple M1](#).
- Tails não funciona com computadores 32-bits desde o [Tails 3.0](#) (junho de 2017).
- Tails não funciona na maioria dos tablets e smartphones.

Figura 3. Hardware no qual Tails não funciona

12. Suporte para Tecnologias Modernas

O suporte a algumas tecnologias modernas também foi analisada na Tails, como TPM2 (Trusted Platform Module 2.0), Secure Boot e Descriptografia de Armazenamento Automatizado. Os resultados obtidos são discutidos abaixo.

12.1. TPM2

TPM2 se trata de uma criptoprocessador que protege o hardware por meio de chaves criptográficas. Ela se popularizou quando se tornou necessário tê-la para instalar o Windows 11, dando acesso a serviços como Windows Hello, escanamento biométrico e reconhecimento facial, de acordo com o site de notícias MiniTool.

Na Tails, para verificar o suporte a TPM2, foi utilizado o comando `[-c /dev/tpmrm0] && echo "TPM 2.0"`. Este comando verifica a existência de uma pasta no sistema que indica a presença do suporte ao TPM2, e foi constatado por meio dele que a pasta não existe na Tails, logo não há suporte para TPM2.

12.2. Secure Boot

De acordo com a Microsoft, Secure Boot é um padrão que apenas deixa sistemas confiáveis realizarem boot no PC. Isso é avaliado por meio do software de boot, como os drivers de firmware UEFI, as aplicações EFI e o sistema operacional. O PC inicia se, e somente se, todas as assinaturas forem válidas.

Na Tails, para verificar o suporte ao Secure Boot, foi utilizado o comando `mokutil -sb-state`. Este comando retorna se o sistema está com o Secure Boot ativado ou se houve alguma falha ao tentar lê-lo. No caso da Tails, nos é retornado que o sistema não oferece suporte a variáveis EFI, o que significa que não há suporte a Secure Boot.

12.3. Descriptografia de Armazenamento Automatizado

Descriptografia de Armazenamento Automatizado se refere à capacidade de descriptografar discos automaticamente. Para realizar tal tarefa, é necessário haver suporte para LVM (Logical Volume Management), o que pode ser verificado usando os comandos `lvm` ou `lvdisplay`.

Na Tails, ambos os comandos não fazem parte do sistema, o que nos leva a concluir que a distribuição não oferece suporte para tais operações.

13. Daemons

A Tails, recém instalada, imediatamente após o boot, tem cerca de 175 daemons rodando, como foi verificado usando o comando `ps -ef | wc -l`. Novamente, como nosso foco é apenas fornecer uma visão geral acerca da distribuição, não serão fornecidas

explicações detalhadas sobre cada daemon. Mas, em poucas palavras, as daemons ativas são relacionadas à inicialização do sistema, sua operação, drivers e à rede Tor.

14. Interpretador de Comandos

O interpretador de comandos serve de interface entre o usuário e o kernel do sistema, possibilitando a execução de comandos via terminal e a criação de scripts. Entre os mais famosos interpretadores de comandos, temos o bash (Bourne-Again Shell) e o zsh (Z Shell), que apresentam diferentes conveniências para o usuário do sistema.

Na Tails, os interpretadores de comandos disponíveis são o sh (Shell), o bash (Bourne-Again Shell) e o mksh (MirBSD Korn Shell), sendo que os dois últimos são sucessores do sh, com o bash sendo o interpretador padrão, como na maioria das distribuições Linux. Eles oferecem mais recursos que seu predecessor, mas em compensação não têm a mesma portabilidade que o sh.

15. Edições ou Spin-offs

Após uma ampla busca, não foram encontradas outras edições ou spin-offs da Tails. O que talvez venha a se caracterizar como tal é a distribuição que a precedeu, Incognito, que foi uma distribuição voltada para segurança, com apenas 3 versões, descontinuada em 2008.

References

Finley, Klint. (2014) “Out in the Open: Inside the Operating System Edward Snowden Used to Evade the NSA”, <https://www.wired.com/2014/04/tails/>, July.

Sarah. (2021) “What Is A TPM 2.0 And Why Does Windows 11 Require It [MiniTool Tips]”, <https://www.minitool.com/news/why-windows-11-needs-tpm-2.html>, July.

Microsoft. (2022) “Secure Boot”, <https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-secure-boot>, July.

Das, Shaswata. (2020) “Oh, Yeah! Linux Kernel 5.10 LTS is Finally Here Before the End of 2020 With Interesting Performance Improvements”, <https://news.itsfoss.com/kernel-5-10-release/>, July.

Tails. (2022), “Documentação”, <https://tails.boum.org/doc/index.pt.html>, July.