

Ubuntu Debullshit



Aqui podemos entender as dúvidas mais comuns dos usuários e apresentá-las de forma clara e organizada.

Script: `ubuntu-debullshit.sh`

Perguntas Frequentes (FAQ)

Boa parte das coisas que os scripts de "desbotificação" fazem, podem ser feitos na instalação prestando atenção nos textos do instalador.

Sumário

Remoção dos pacotes gnome-power-manager e o gnome-logs.....	3
Governança de TI e a Remoção de Pacotes.....	3
Conclusão.....	4
Adição de repositórios de terceiros para temas.....	4
1. Segurança e Controle de Versões.....	4
2. Transparência e Auditoria.....	4
3. Gerenciamento de Dependências.....	5
4. Facilidade de Manutenção e Suporte.....	5
5. Eficiência Operacional.....	5
6. Licenciamento e Conformidade Legal.....	5
7. Redução de Riscos.....	5
Conclusão.....	6
Instalação de pacote do Debian no Ubuntu para tema.....	6
1. Compatibilidade de Tema.....	6
2. Consistência Visual e User Experience.....	6
3. Gerenciamento e Controle.....	7
4. Suporte e Estabilidade.....	7
5. Padronização.....	7
Conclusão:.....	8
Remoção do pacote Livepatch.....	8
1. Controle Total sobre as Atualizações.....	8
2. Rastreabilidade e Auditoria.....	8
3. Evita Atualizações Automáticas Inesperadas.....	9
4. Gerenciamento de Risco e Compatibilidade.....	9
5. Planejamento de Capacidade e Recursos.....	9
6. Custo de Licenciamento.....	9
Em resumo:.....	9
Remoção do pacote Update Manager.....	10
1. Desempenho e Consumo de Recursos.....	10
2. Automação e Controle.....	10
3. Segurança e Transparência.....	10
4. Customização e Flexibilidade.....	10
5. Impacto de Erros e Problemas.....	11
Resumo.....	11
Desabilitar as atualizações automáticas de forma gráfica.....	12
1. Controle e Visibilidade.....	12
2. Monitoramento e Auditoria.....	12
3. Segurança.....	12
4. Gerenciamento de Patches.....	12
Como Implementar.....	13
Ubuntu com GNOME em equipamento com recursos limitados.....	13
Desativar o serviço de localização.....	15
Remoção do repositório de parceiros do Ubuntu.....	19
Desativar o Ubuntu Repor.....	21
Remoção do Appport.....	24
Remoção do Snap e SnapD.....	27
Remoção dos avisos sobre o Ubuntu Pro.....	30
Desfazer as alterações do script.....	33

Remoção dos pacotes **gnome-power-manager** e o **gnome-logs**

1- O Script remove o **gnome-power-manager** e o **gnome-logs**. No que manter esses pacotes, vai contra uma boa política de governança de TI?

R:

A remoção de pacotes como **gnome-power-manager** e **gnome-logs** pode ser uma decisão válida, dependendo das necessidades específicas da infraestrutura de TI e das diretrizes de governança adotadas pela organização. Vamos analisar os dois pacotes mencionados:

1. **gnome-power-manager**: Este é um gerenciador de energia para o ambiente GNOME, responsável por controlar configurações de energia, como suspensão, brilho de tela e gerenciamento de bateria. Em ambientes corporativos, pode ser preferível desativar ou remover esse tipo de ferramenta, especialmente em servidores ou estações de trabalho onde a gestão de energia é controlada de forma centralizada ou por ferramentas específicas de gerenciamento de hardware. No entanto, em estações de trabalho pessoais ou em configurações que exigem gerenciamento de energia eficiente, mantê-lo pode ser útil.
2. **gnome-logs**: Este é um visualizador de logs simples para o GNOME, usado para exibir mensagens de log do sistema e aplicativos. Em um ambiente de governança de TI, o gerenciamento de logs é fundamental para monitoramento, auditoria e conformidade. Em vez de remover completamente, pode-se optar por configurar ou utilizar outras ferramentas de logs mais avançadas ou específicas, como *syslog*, *journald*, ou soluções externas de monitoramento.

Governança de TI e a Remoção de Pacotes

No contexto de governança de TI, as decisões sobre a remoção de pacotes devem ser orientadas por políticas de segurança, manutenção e gerenciamento de sistemas. A decisão de remover esses pacotes poderia ser considerada contra as boas práticas se:

- **Logs essenciais não forem monitorados adequadamente**: Se a remoção do **gnome-logs** impedir o acesso a logs importantes para auditoria e monitoramento, isso pode ser um risco de segurança e uma violação da política de governança.
- **Gerenciamento de energia não for centralizado**: Se o ambiente de TI não centraliza o gerenciamento de energia e o controle de consumo e eficiência energética for importante, a remoção do **gnome-power-manager** pode interferir no controle adequado desses parâmetros.

Porém, se a organização tiver ferramentas alternativas para monitoramento de logs e gerenciamento de energia (como soluções corporativas ou ferramentas personalizadas), a remoção desses pacotes pode ser totalmente aceitável.

Conclusão

Manter ou remover esses pacotes não vai, por si só, contra uma boa política de governança de TI. O que importa é garantir que haja alternativas adequadas para as funcionalidades fornecidas por esses pacotes, e que a governança de TI tenha controle sobre os processos de gerenciamento de energia e logs. Se houver alternativas que atendam às necessidades de segurança, conformidade e gerenciamento centralizado, a remoção pode ser uma decisão válida.

Adição de repositórios de terceiros para temas

2- O Script adiciona um outro repositórios de terceiros para temas, o que é irônico, já que teve uma reclamação sobre o repositório Canonical Partners. No que incluir um repositório para temas ajuda numa boa governança de TI?

R:

Incluir um repositório específico para temas pode ajudar numa boa governança de TI de várias maneiras. A governança de TI envolve garantir que os sistemas e processos de tecnologia da informação sejam eficientes, seguros, bem geridos e em conformidade com as políticas organizacionais. Ao incluir um repositório para temas, você está criando um controle mais rigoroso sobre as atualizações, a segurança, a qualidade e a conformidade dos pacotes utilizados na infraestrutura da organização. Aqui estão alguns benefícios específicos para a governança de TI:

1. Segurança e Controle de Versões

- **Atualizações regulares e controle de versões:** Repositórios específicos para temas geralmente oferecem atualizações frequentes e seguras. Isso ajuda a manter os sistemas protegidos contra vulnerabilidades, pois os temas frequentemente recebem correções de bugs e patches de segurança.
- **Controle de versões:** Com um repositório centralizado, a TI tem maior controle sobre quais versões dos temas estão sendo usadas em toda a organização. Isso assegura que os temas mais recentes e seguros sejam implementados, evitando o uso de versões desatualizadas que possam ter falhas de segurança.

2. Transparência e Auditoria

- **Rastreabilidade:** Repositórios bem geridos possibilitam o rastreamento de quais pacotes estão sendo utilizados, facilitando a auditoria e a identificação de problemas. Isso garante que a equipe de TI possa identificar rapidamente se algum tema está causando problemas de desempenho ou segurança.
- **Conformidade:** Ao usar repositórios oficiais ou bem mantidos, é possível garantir que o uso de temas está em conformidade com as políticas de TI e as regulamentações de segurança da organização, reduzindo o risco de não conformidade.

3. Gerenciamento de Dependências

- **Evitar conflitos e dependências não gerenciadas:** Ao centralizar os temas em um repositório controlado, você facilita o gerenciamento das dependências de pacotes. Isso ajuda a evitar conflitos entre pacotes ou dependências quebradas, que poderiam causar problemas no funcionamento do sistema.
- **Consistência no ambiente de TI:** Ter um repositório definido para temas assegura que todos os sistemas na organização usem as mesmas versões de temas, promovendo consistência e evitando a instalação de versões incompatíveis em diferentes máquinas.

4. Facilidade de Manutenção e Suporte

- **Gestão centralizada:** Usar repositórios específicos para temas torna a manutenção de pacotes e temas mais fácil, pois a TI pode atualizar, modificar ou remover pacotes de forma centralizada, sem precisar de intervenções manuais em diversos sistemas.
- **Suporte ativo e documentação:** Muitos repositórios de terceiros oferecem suporte técnico e documentação atualizada, facilitando a resolução de problemas. Isso também ajuda a TI a manter a infraestrutura com recursos e suporte de qualidade.

5. Eficiência Operacional

- **Automatização de processos:** Ao integrar repositórios específicos para temas, é possível automatizar a instalação e a atualização de pacotes, o que reduz o tempo gasto pela equipe de TI com tarefas manuais e melhora a eficiência operacional.
- **Melhoria no gerenciamento de mudanças:** A TI pode implementar um controle mais rigoroso sobre quando e como os temas são atualizados, minimizando os riscos associados a mudanças não planejadas ou a falhas durante atualizações de temas.

6. Licenciamento e Conformidade Legal

- **Licenciamento e conformidade com a lei:** Muitos repositórios de terceiros disponibilizam temas com licenciamento claro e em conformidade com as normas de propriedade intelectual. Isso garante que a organização esteja em conformidade com as leis de direitos autorais e não corra o risco de usar software não licenciado ou ilegal.

7. Redução de Riscos

- **Redução de erros humanos:** Centralizando a gestão dos temas em repositórios confiáveis e bem definidos, a TI minimiza a possibilidade de erros humanos ao instalar ou atualizar temas, garantindo maior estabilidade no ambiente de TI.
- **Melhor gestão de riscos:** Repositórios bem geridos permitem uma abordagem proativa na identificação de temas obsoletos ou vulneráveis, reduzindo riscos de falhas operacionais ou brechas de segurança.

Conclusão

Incluir um repositório específico para temas ajuda a melhorar a governança de TI, proporcionando maior segurança, controle de versões, rastreabilidade, eficiência operacional, conformidade legal e redução de riscos. Essa abordagem centralizada facilita a gestão, manutenção e atualização de pacotes, promovendo um ambiente de TI mais seguro, eficiente e bem controlado.

Instalação de pacote do Debian no Ubuntu para tema

3- E ainda instala um pacote do Debian no Ubuntu. Tudo bem, que alguns pacotes do Debian são compatíveis com o Ubuntu, mas não acho que isso é a favor de uma boa governança de TI para as empresas

R:

<https://github.com/polkaulfield/ubuntu-debullshit/issues/6>

Instalar pacotes de tema do Debian no Ubuntu pode ser considerado menos problemático do que a instalação de pacotes de software ou aplicativos, mas ainda assim não é uma prática recomendada em um contexto de **boa governança de TI** para empresas. Vamos analisar os motivos:

1. Compatibilidade de Tema

- **Temas gráficos** (como temas de ícones, GTK, ou papéis de parede) geralmente têm menos risco de causar falhas ou instabilidade em sistemas comparado a pacotes de software. No entanto, mesmo pacotes de tema podem não ser 100% compatíveis entre as versões do Debian e do Ubuntu, já que o Ubuntu tem seus próprios ajustes e preferências para temas. Em alguns casos, o tema pode não se comportar corretamente ou causar problemas de aparência em alguns aplicativos.
- **Dependências de tema:** Embora pacotes de tema não possuam tantas dependências críticas como softwares, ainda assim pode haver problemas com dependências específicas que são tratadas de maneira diferente em cada distribuição, o que pode impactar a experiência do usuário.

2. Consistência Visual e User Experience

- **Manutenção da consistência:** Em um ambiente corporativo, uma das boas práticas de governança de TI é garantir uma experiência de usuário consistente. Isso inclui garantir que o visual do sistema seja uniforme em todos os dispositivos e máquinas. Misturar temas de diferentes distribuições pode prejudicar essa consistência visual, principalmente se a aparência não for testada amplamente ou se houver variações no comportamento entre diferentes versões do Ubuntu e do Debian.

- **Preferência corporativa:** Empresas muitas vezes escolhem temas específicos para garantir que todos os sistemas e aplicativos sigam a mesma linha visual, tanto para questões estéticas quanto para a experiência do usuário. Ao instalar pacotes de temas de Debian no Ubuntu, pode-se acabar desviando dos padrões adotados pela empresa.

3. Gerenciamento e Controle

- **Fonte confiável:** Em governança de TI, é importante que todos os pacotes utilizados sejam provenientes de fontes confiáveis e bem mantidas. O repositório oficial do Ubuntu é uma fonte segura e controlada, enquanto o pacote de tema do Debian pode ter sido testado principalmente para a versão do Debian e pode não ser otimizado ou mantido para o Ubuntu.
- **Segurança:** Embora pacotes de tema em si geralmente não apresentem riscos de segurança diretos, qualquer pacote que seja instalado fora dos repositórios oficiais do sistema operacional deve ser cuidadosamente avaliado. Pacotes não oficiais podem, em alguns casos, conter scripts ou alterações inesperadas.

4. Suporte e Estabilidade

- **Suporte oficial:** Como mencionado, o Ubuntu tem suporte oficial e um repositório mantido pela Canonical, enquanto o Debian tem seu próprio ciclo de manutenção. Ao usar pacotes de tema do Debian, você perde o suporte técnico oficial do Ubuntu, o que pode ser um problema em empresas que dependem de garantias de suporte, especialmente para sistemas críticos.
- **Estabilidade e atualizações:** Misturar pacotes de diferentes distribuições pode dificultar o gerenciamento de atualizações e a resolução de problemas, caso o sistema venha a ter problemas gráficos ou de interface. A governança de TI visa uma operação estável e previsível, e adicionar elementos que não são oficialmente testados no Ubuntu pode tornar o sistema mais suscetível a problemas no futuro.

5. Padronização

- **Facilidade de gestão:** Empresas que aplicam boas práticas de governança de TI frequentemente buscam padronização em seus ambientes. Usar pacotes de diferentes distribuições pode criar uma situação onde os sistemas não são facilmente gerenciados, atualizados ou auditados de forma centralizada. Um tema de Debian no Ubuntu pode ser um pequeno detalhe, mas contribui para uma falta de padronização no longo prazo.

Conclusão:

Embora instalar pacotes de tema do Debian no Ubuntu **não seja uma violação grave de governança de TI**, essa prática pode não ser a mais indicada para empresas que buscam uma governança sólida e controlada. **Boas práticas de TI** envolvem garantir **consistência, segurança e controle**, e misturar pacotes de distribuições diferentes, mesmo que não seja crítico em termos de funcionamento do sistema, pode ser uma violação desses princípios.

Se for necessário usar temas específicos, o ideal seria buscar temas amplamente compatíveis e testados tanto para o Ubuntu quanto para o Debian, ou ainda criar uma solução personalizada que seja controlada e validada internamente pela equipe de TI da empresa.

Remoção do pacote Livepatch

4- O Script também remove o Livepatch, com a desculpa de aumentar a privacidade. Bom, manter o Livepatch, sim seria uma boa em empresas, já que aplica atualizações importantes sem ter que reiniciar o computador. No que remover o Livepatch melhora na governança de TI de uma empresa?

R:

A remoção do **Livepatch** pode trazer melhorias para a governança de TI de uma empresa de algumas maneiras, dependendo do contexto e das necessidades específicas da organização. Vamos analisar os pontos principais.

1. Controle Total sobre as Atualizações

- **Livepatch** aplica patches de segurança sem a necessidade de reiniciar o sistema, mas isso pode ocorrer de maneira automática e invisível, o que pode dificultar o controle sobre quais patches foram aplicados e quando.
- **apt update && apt -y upgrade**, por outro lado, oferece maior transparência no processo de atualização. A equipe de TI pode decidir quando aplicar os patches, testar as atualizações antes de aplicá-las em produção, e verificar se o sistema foi atualizado corretamente.

2. Rastreabilidade e Auditoria

- Usando **apt update && apt -y upgrade**, a governança de TI pode manter logs claros sobre as atualizações realizadas no sistema, facilitando a auditoria.
- Com o **Livepatch**, as atualizações de segurança podem ser aplicadas sem a intervenção ou monitoramento explícito da equipe de TI, o que pode tornar o processo menos rastreável e dificultar a auditoria, o que é uma preocupação para empresas que precisam de conformidade regulatória.

3. Evita Atualizações Automáticas Inesperadas

- Com o **Livepatch**, o sistema pode receber patches sem que a equipe de TI saiba exatamente o que foi alterado. Isso pode ser problemático em ambientes onde a governança exige a aprovação explícita de atualizações.
- Com os comandos **apt update && apt -y upgrade**, você tem mais controle e pode realizar atualizações de forma programada, por exemplo, fora do horário de pico, minimizando o impacto em produção.

4. Gerenciamento de Risco e Compatibilidade

- O **Livepatch** é uma solução automática que pode ser útil para correções críticas de segurança. No entanto, ele pode não ser a solução ideal se houver riscos de compatibilidade com outras aplicações ou serviços no sistema. O uso do **apt update && apt -y upgrade** permite que você teste as atualizações antes de aplicá-las, garantindo que a compatibilidade e a estabilidade do sistema sejam mantidas.

5. Planejamento de Capacidade e Recursos

- Com o **Livepatch**, o processo de atualização acontece sem reinicializações, mas isso pode ocultar o consumo de recursos do sistema ou mudanças que podem afetar o desempenho. Com o **apt update && apt -y upgrade**, a equipe de TI pode planejar as atualizações, avaliar o impacto nos recursos e até mesmo realizar testes de carga para garantir que a performance não seja comprometida.

6. Custo de Licenciamento

- **Livepatch** geralmente tem um custo associado a sua utilização, dependendo do plano da Canonical. Removê-lo pode resultar em uma economia de custos, especialmente em empresas que não têm uma necessidade crítica de aplicar patches sem reiniciar.
- Utilizando apenas o **apt update && apt -y upgrade**, as atualizações ficam dentro do escopo das soluções que já estão sendo pagas, sem necessidade de licenciamento adicional.

Em resumo:

A remoção do **Livepatch** pode melhorar a governança de TI de uma empresa ao garantir maior controle sobre as atualizações, maior rastreabilidade e maior previsibilidade dos impactos no sistema. Além disso, permite um processo de atualização mais controlado e alinhado com os requisitos de conformidade, segurança e compatibilidade da empresa.

Remoção do pacote Update Manager

5- Remove o Update Manager, que atualiza o sistema de forma gráfica. No que manter isso seria contra uma boa governança de TI?

R:

Manter o **Update Manager** em um ambiente de TI, especialmente em servidores ou sistemas que exigem alta disponibilidade e controle rigoroso de recursos, pode ser considerado contra uma boa governança de TI por várias razões:

1. Desempenho e Consumo de Recursos

O **Update Manager** normalmente opera com uma interface gráfica, o que pode consumir mais recursos do sistema, como CPU e memória, especialmente se houver bugs ou falhas na aplicação. Esse consumo pode afetar o desempenho geral da máquina, o que não é desejável, especialmente em servidores ou sistemas críticos. A atualização automática via linha de comando (como o `apt update && apt -y upgrade` com monitoramento) permite que o processo seja feito de forma mais eficiente e sem a sobrecarga gráfica.

2. Automação e Controle

O método `apt update && apt -y upgrade` via cron, com monitoramento das saídas de erros — oferece maior controle e automação. A governança de TI valoriza a capacidade de monitorar, auditar e responder rapidamente a qualquer problema que ocorra durante o processo de atualização. Utilizando cron e logs, você pode personalizar a frequência das atualizações, controlar o momento em que elas ocorrem e verificar os erros de forma centralizada, sem a necessidade de interação manual ou da sobrecarga de um processo gráfico.

3. Segurança e Transparência

Com o processo automatizado via cron e logs, é possível auditar de maneira mais eficaz o que aconteceu durante a atualização e se algo deu errado. No **Update Manager**, caso ocorra algum erro, ele pode não ser tão transparente quanto a execução direta na linha de comando, podendo esconder falhas ou falhas parciais no processo de atualização.

4. Customização e Flexibilidade

Utilizando scripts e a linha de comando, você tem maior flexibilidade para personalizar como as atualizações são feitas, além de poder fazer ajustes finos (como excluir pacotes específicos ou evitar certas atualizações) diretamente no cron ou no script que você utiliza. O **Update Manager** não oferece a mesma flexibilidade e, em muitos casos, pode aplicar atualizações de forma indiscriminada.

5. Impacto de Erros e Problemas

Como o **Update Manager** é uma aplicação gráfica, ele pode ser suscetível a erros visuais ou de interface que não são evidentes em logs ou em monitoramento automatizado. Caso haja um bug ou falha no próprio **Update Manager**, isso pode levar a problemas difíceis de diagnosticar rapidamente. Em contraste, o método automatizado via cron gera logs e alertas claros sobre erros, permitindo uma reação mais rápida.

Resumo

A principal razão pela qual manter o **Update Manager** pode ser contra uma boa governança de TI é a questão da **gestão eficiente dos recursos, controle de processos e auditoria de segurança**. A abordagem de usar **cron e logs** oferece **automação, controle total, transparência** e um **uso mais eficiente de recursos**, que são princípios fundamentais de boas práticas de governança de TI. O **Update Manager**, por ser uma ferramenta gráfica, pode comprometer o desempenho, tornar o processo menos transparente e difícil de monitorar de forma eficaz.

Desabilitar as atualizações automáticas de forma gráfica

6- O seu Script, ele também desabilita as atualizações automáticas. Me diz: No que desabilitar as atualizações automáticas ajuda numa boa governança de TI?

R:

Desabilitar as atualizações automáticas de forma gráfica e usar comandos manuais como `apt update` && `apt -y upgrade` via cron, com monitoramento das saídas de erros para um arquivo de log, pode ser uma boa prática em termos de governança de TI, especialmente em ambientes corporativos e servidores críticos. Aqui estão algumas razões pelas quais essa abordagem pode ser vantajosa:

1. Controle e Visibilidade

- **Atualizações automáticas** podem aplicar atualizações de pacotes sem a supervisão necessária, o que pode gerar incompatibilidades ou até falhas inesperadas. Ao realizar as atualizações manualmente, você tem controle sobre o que está sendo atualizado e pode verificar os pacotes que estão sendo instalados.
- **Logs detalhados:** Com um arquivo de log, você pode monitorar todas as atualizações e erros, ajudando a identificar qualquer problema antes que ele afete os usuários ou o sistema.

2. Monitoramento e Auditoria

- Com o monitoramento das saídas de erro, você pode auditar o processo de atualização e garantir que não ocorra nenhuma falha não detectada. Além disso, a criação de logs facilita a rastreabilidade das ações realizadas, importante para auditorias de segurança ou compliance.
- **Centralização do log:** Caso seja necessário, os logs podem ser enviados para uma central de monitoramento (ex. Syslog) ou um sistema de SIEM para análise mais profunda.

3. Segurança

- Em ambientes com políticas de segurança rigorosas, é importante testar e validar as atualizações antes de aplicá-las em produção. Atualizações automáticas podem incluir atualizações de segurança, mas também podem incluir mudanças que afetam a compatibilidade do sistema.
- Usar um cron com um script customizado oferece a flexibilidade de aplicar as atualizações em momentos controlados e agendados, além de permitir o uso de procedimentos de validação antes de fazer uma atualização mais ampla.

4. Gerenciamento de Patches

- Em algumas situações, pode ser necessário realizar atualizações de forma mais controlada e priorizada, em vez de aceitar atualizações automáticas para todos os pacotes. Isso ajuda a evitar a instalação de patches não testados em ambientes críticos.

- **Testes de pacotes:** Antes de rodar o comando de upgrade em produção, você pode testar as atualizações em ambientes de homologação para garantir que não haja impacto.

Como Implementar

1. Desabilitar atualizações automáticas gráficas:

- Se você estiver utilizando uma interface gráfica, geralmente as atualizações automáticas podem ser desabilitadas através das configurações do "Software Updater" ou "Atualizações de Software" no seu sistema operacional.
- Em sistemas baseados em Debian/Ubuntu, você pode desabilitar as atualizações automáticas editando o arquivo `/etc/apt/apt.conf.d/20auto-upgrades` e definindo os valores para 0:

Ubuntu com GNOME em equipamento com recursos limitados

7- O Script faz sentido em máquinas muito fracas. Agora, dizer que isso é para empresas e não para usuários domésticos, é mentira.

R:

Existem muitas empresas de pequeno e médio porte que utilizam máquinas antigas para servidores Linux.

Quando você está lidando com um equipamento com recursos limitados, otimizar o Ubuntu com o GNOME para desempenho pode ser crucial. O GNOME é uma interface gráfica que exige bastante do hardware, então existem algumas estratégias que você pode adotar para melhorar o desempenho do sistema.

1. Usar uma versão mais leve do Ubuntu ou trocar de interface gráfica dele (i3WM, FluxBox, OpenBox...)

O Ubuntu padrão com GNOME pode ser pesado para máquinas fracas. Considerar uma versão mais leve pode ser uma boa solução. O Ubuntu MATE, Xubuntu ou Lubuntu são variantes com ambientes gráficos mais leves, como o MATE, XFCE e LXQt, que exigem menos recursos.

Se preferir continuar com o GNOME, ainda existem opções para melhorar o desempenho, sem a necessidade de trocar de distribuição ou ambiente gráfico.

2. Instalar o GNOME no modo "Minimal"

O GNOME pode ser configurado para consumir menos recursos. Você pode instalar o GNOME de uma forma mais "minimalista", sem algumas das funcionalidades extras. Isso pode ser feito instalando o GNOME sem muitas extensões.

```
# apt update && apt install -y gnome-shell
```

Evite instalar outras extensões ou plugins que não são essenciais.

3. Desativar efeitos gráficos

O GNOME vem com vários efeitos gráficos que podem consumir muitos recursos. Você pode desativar a maioria desses efeitos para melhorar o desempenho.

Vá para Configurações > Aparência > Desempenho e ajuste as configurações de efeitos gráficos. Desabilite animações em Configurações > Acessibilidade > Mostrar animações (desmarque a opção).

4. Reduzir os processos e serviços em segundo plano

Alguns serviços em segundo plano consomem muitos recursos. Você pode desabilitar serviços que não são necessários:

Systemd-analyze: Use esse comando para ver quanto tempo o seu sistema está demorando para inicializar e quais serviços estão gastando mais tempo:

```
systemd-analyze blame
```

Desabilitar serviços desnecessários: Desative os serviços que você não precisa, por exemplo, o bluetooth ou impressoras, se não for necessário.

5. Gerenciar programas de inicialização

Muitos programas são configurados para iniciar automaticamente ao ligar o computador. Você pode desabilitar os desnecessários para liberar recursos.

Abra o Aplicativos de Sessão ou `gnome-session-properties` e desmarque os aplicativos que você não usa frequentemente.

6. Instalar e usar o zswap (troca comprimida)

O zswap pode melhorar o desempenho em máquinas com pouca RAM. Ele utiliza a troca comprimida, o que reduz o impacto no disco rígido ao utilizar o swap.

Habilite o zswap:

```
sudo nano /etc/default/grub
```

No arquivo, localize a linha `GRUB_CMDLINE_LINUX_DEFAULT` e adicione `zswap.enabled=1` no final. Depois, atualize o GRUB:

```
sudo update-grub
```

7. Usar um gerenciador de pacotes leve

Se você está usando muitos pacotes e softwares pesados, vale a pena considerar substituir alguns deles por alternativas mais leves.

Navegador: O Firefox pode ser substituído pelo Chromium ou Midori, que são mais leves.

Editor de texto: Use Geany ou Mousepad em vez de editores mais pesados como o Gedit.

8. Monitorar o uso de recursos

Use ferramentas como htop ou System Monitor para monitorar o uso de CPU, memória e discos. Você pode descobrir quais processos estão consumindo muitos recursos e, então, agir para otimizar ou matar os processos desnecessários.

9. Usar um kernel mais leve

Em alguns casos, a instalação de um kernel mais leve pode ajudar, principalmente se você não precisar de suporte para muitas funcionalidades. Você pode instalar o Linux Lowlatency ou Linux LTS, que são opções mais otimizadas para desempenho.

10. Considerar a utilização de uma swap maior

Se a máquina tem pouca RAM, você pode ajustar a área de swap. Isso ajuda quando a RAM se esgota, evitando travamentos no sistema. Aumentar o swap para um arquivo ou partição maior pode ser benéfico.

Essas estratégias podem ajudar a otimizar o Ubuntu com GNOME para um hardware mais fraco. Se o desempenho ainda não for suficiente, considere mudar para um ambiente gráfico mais leve (como o XFCE, i3WM, FluxBox ou OpenBox...) ou até uma distribuição mais otimizada para máquinas antigas, como o Lubuntu ou Xubuntu.

Desativar o serviço de localização

8- Por que desativar o serviço de localização do Ubuntu ajuda numa boa governança de TI?

R:

Desativar o serviço de localização no Ubuntu pode ser uma prática útil em uma boa governança de TI por várias razões, especialmente em relação à segurança, privacidade e controle sobre os dados. Aqui estão alguns pontos principais que explicam por que isso pode ser benéfico:

1. Proteção da Privacidade

O serviço de localização pode coletar dados sobre a posição geográfica do dispositivo, como a localização baseada em GPS ou na rede, o que pode ser uma preocupação de privacidade. Ao desativá-lo, você evita a coleta e transmissão desses dados, garantindo que informações sensíveis sobre a localização do usuário ou da organização não sejam compartilhadas sem consentimento.

2. Redução de Riscos de Segurança

Embora a localização em si não seja uma ameaça imediata, serviços que rastreiam a posição podem ser vulneráveis a exploits ou ataques cibernéticos. Se o serviço de localização estiver ativo e não for necessário, pode representar uma superfície adicional de ataque. Desativá-lo reduz a chance de exploração por partes externas mal-intencionadas.

3. Controle de Dados

Muitas empresas preferem ter controle sobre todos os dados que circulam em seus sistemas. O serviço de localização, se ativado, pode enviar dados de localização para serviços de terceiros ou servidores externos, algo que pode ser indesejado em ambientes corporativos onde a coleta e o uso de dados precisam ser monitorados e regulados de acordo com as políticas de segurança e privacidade da organização.

4. Conformidade com Regulamentações de Privacidade

Em alguns setores e regiões, existem regulamentações rigorosas de privacidade, como o GDPR na União Europeia, que exige que as empresas gerenciem e protejam dados pessoais de forma rigorosa. A localização pode ser considerada um dado pessoal, e desativar o serviço de localização pode ser uma maneira de minimizar o risco de violar essas leis.

5. Otimização de Recursos

Embora não seja a principal razão, desativar serviços desnecessários pode resultar em um uso mais eficiente de recursos do sistema. O serviço de localização pode consumir poder de processamento e largura de banda, mesmo que de forma leve, e desativá-lo pode liberar recursos para outras funções mais essenciais.

6. Políticas de Segurança Corporativa

Em muitas organizações, o rastreamento da localização de dispositivos não é necessário para as operações diárias. A governança de TI muitas vezes envolve garantir que apenas os serviços essenciais estejam ativos nos dispositivos corporativos, limitando a quantidade de dados que podem ser acessados ou transmitidos externamente. Isso pode ajudar a manter a integridade dos sistemas e evitar a exposição desnecessária de informações.

Como desativar o serviço de localização no Ubuntu:

Você pode desativar a funcionalidade de localização através das configurações do sistema ou com comandos no terminal.

Via Interface Gráfica:

Abra as Configurações.

Vá para a seção Privacidade.

Selecione Localização e desative o serviço.

Via Terminal:

No terminal, você pode desativar o serviço de localização com o seguinte comando:

```
sudo systemctl stop location.service  
sudo systemctl disable location.service
```


Conclusão:

Desativar o serviço de localização no Ubuntu é uma prática simples, mas importante, em termos de segurança e governança de TI, pois ajuda a proteger a privacidade dos usuários, reduz o risco de vazamento de dados sensíveis, facilita a conformidade com regulamentações e reduz a exposição a vulnerabilidades.

A remoção do pacote geoclue no Ubuntu pode ser uma ação importante dentro de uma boa governança de TI, especialmente em organizações que buscam aumentar a segurança, a privacidade e o controle sobre os dados no ambiente corporativo. O geoclue é um serviço de localização que fornece informações sobre a posição geográfica do dispositivo com base em diferentes fontes, como GPS, redes Wi-Fi, IP, entre outros.

Aqui estão algumas razões pelas quais a remoção do pacote geoclue pode ajudar numa boa governança de TI:

1. Proteção de Privacidade

O geoclue pode coletar dados de localização, o que pode representar uma ameaça à privacidade. Dependendo da configuração do sistema e dos serviços que o utilizam, a localização pode ser compartilhada com terceiros sem o devido consentimento ou controle. Ao remover o geoclue, você evita que o sistema colete e envie dados de localização para servidores externos, protegendo a privacidade dos usuários.

2. Redução de Superfícies de Ataque

O geoclue é um serviço que pode ser vulnerável a ataques, como qualquer outro serviço em execução no sistema. Ao removê-lo, você reduz a superfície de ataque do sistema operacional, o que diminui a possibilidade de exploração de vulnerabilidades associadas a esse pacote. Isso é especialmente relevante em ambientes corporativos, onde a segurança e a proteção de dados são prioridades.

3. Conformidade com Regulamentações de Privacidade

Muitas organizações precisam seguir regulamentações rigorosas de privacidade, como o GDPR (Regulamento Geral de Proteção de Dados) na União Europeia ou outras legislações locais sobre proteção de dados. A localização é considerada um dado pessoal e sensível em muitas jurisdições, e o uso do geoclue pode envolver a coleta e o armazenamento de dados de localização sem o devido controle e consentimento. Remover o geoclue ajuda a evitar possíveis violações de privacidade e facilita a conformidade com essas regulamentações.

4. Controle de Dados

Em muitas organizações, é importante manter controle sobre os dados gerados e transmitidos pelos dispositivos corporativos. O geoclue pode enviar dados de localização para servidores externos, o que pode ser indesejado em ambientes onde o tráfego de dados é rigorosamente monitorado e controlado. A remoção do pacote impede que dados de localização sejam enviados para fora da rede corporativa, garantindo maior controle sobre o que é compartilhado.

5. Otimização de Recursos

Embora o impacto de desempenho seja geralmente pequeno, o serviço de localização pode consumir recursos do sistema, como CPU e rede, ao tentar determinar a localização do dispositivo. Em sistemas onde não é necessária essa funcionalidade, remover o geoclue pode liberar recursos para outras tarefas mais críticas, o que pode ser um fator relevante em dispositivos com recursos limitados.

6. Prevenção de Riscos Não Necessários

Em algumas organizações, o rastreamento de localização pode ser uma funcionalidade desnecessária, especialmente se o dispositivo não precisar dessas informações para sua operação diária. Manter o geoclue ativo quando não há necessidade de uso pode representar um risco desnecessário. A remoção do pacote ajuda a evitar funcionalidades que não agregam valor e ainda podem introduzir riscos.

Como remover o pacote geoclue:

Se você decidir que a remoção do geoclue é apropriada para a sua organização, o processo é simples.

No terminal, você pode remover o pacote com o seguinte comando:

```
sudo apt remove geoclue
```

Se você quiser garantir que todos os pacotes dependentes também sejam removidos, use:

```
sudo apt autoremove
```

Isso remove o geoclue e qualquer outro pacote que não seja mais necessário após a remoção.

Conclusão:

A remoção do pacote geoclue ajuda na boa governança de TI ao proteger a privacidade dos usuários, reduzir a exposição a vulnerabilidades de segurança, facilitar a conformidade com regulamentações de privacidade e garantir maior controle sobre os dados. É uma prática recomendada, especialmente em ambientes corporativos, onde a segurança e a privacidade dos dados são prioridades.

Remoção do repositório de parceiros do Ubuntu

9- Remove o repositório de parceiros do Ubuntu ajuda numa boa governança de TI?

Remover o repositório de parceiros do Ubuntu pode ser uma prática útil dentro de uma boa governança de TI, especialmente em ambientes corporativos ou em sistemas que exigem um controle rigoroso sobre os pacotes e fontes de software. Aqui estão algumas razões pelas quais essa ação pode ser benéfica:

1. Maior Controle sobre Fontes de Software

O repositório de parceiros do Ubuntu (geralmente partner no arquivo de fontes de pacotes) contém pacotes de software de terceiros que são fornecidos por empresas parceiras da Canonical, como o Google, Adobe, entre outros. Ao remover esse repositório, você assegura que os pacotes instalados em seu sistema provêm de fontes confiáveis e controladas pela organização, reduzindo a possibilidade de instalar software de fontes não autorizadas ou potencialmente inseguras.

2. Segurança e Integridade

Pacotes de repositórios de terceiros podem ser menos auditados em termos de segurança e, por vezes, podem ser mais suscetíveis a vulnerabilidades. Além disso, o fornecimento de atualizações e patches de segurança pode não ser tão rápido quanto os pacotes oficiais dos repositórios da distribuição. Ao remover os repositórios de parceiros, você pode evitar o risco de instalar pacotes que possam introduzir vulnerabilidades ou problemas de compatibilidade no sistema.

3. Prevenção de Riscos Legais e de Conformidade

Em muitas organizações, a conformidade com regulamentações de segurança e privacidade, como o GDPR ou outras normas, é uma prioridade. O uso de pacotes de terceiros pode apresentar riscos em relação ao cumprimento dessas regulamentações, especialmente quando se trata de software que coleta dados de usuários ou se comunica com servidores externos. A remoção dos repositórios de parceiros ajuda a minimizar o risco de instalar software que possa coletar dados de forma inadequada ou que não esteja em conformidade com as políticas corporativas.

4. Redução da Superfície de Ataque

O uso de repositórios externos, incluindo os de parceiros, pode aumentar a superfície de ataque de um sistema. Qualquer vulnerabilidade presente em pacotes de terceiros pode representar um vetor de ataque adicional. Ao desabilitar ou remover esses repositórios, você reduz a quantidade de software de terceiros no sistema, diminuindo a possibilidade de exploração de falhas de segurança.

5. Estabilidade e Compatibilidade

O software proveniente de repositórios de parceiros pode, às vezes, ter problemas de compatibilidade com os pacotes oficiais do Ubuntu. Pode haver dependências conflitantes, ou até mesmo versões de pacotes que não são totalmente compatíveis com o restante do sistema. Ao remover os repositórios de parceiros, você pode garantir que o software instalado seja mantido dentro dos limites das versões e pacotes oficiais, aumentando a estabilidade do sistema.

6. Simplificação do Gerenciamento de Pacotes

Em ambientes corporativos, a administração e auditoria de pacotes e atualizações precisam ser bem controladas. Ao remover repositórios de parceiros, você simplifica o gerenciamento de pacotes, garantindo que apenas fontes oficiais e auditadas sejam usadas. Isso facilita a gestão de atualizações, correções e auditabilidade do sistema.

Como remover o repositório de parceiros no Ubuntu:

Para remover o repositório de parceiros, você pode editar o arquivo de fontes de pacotes do APT ou desmarcar a opção em um gerenciador gráfico de repositórios, como o Software & Updates. Aqui está como fazer isso via terminal:

Abra o terminal e edite o arquivo de fontes de pacotes:

```
sudo nano /etc/apt/sources.list
```

Localize as linhas que fazem referência ao repositório de parceiros, que geralmente se parecem com isto:

```
deb http://archive.canonical.com/ubuntu YOUR_UBUNTU_VERSION_HERE partner
```

Comente essas linhas adicionando um # no início de cada linha ou exclua-as.

Salve o arquivo e saia do editor.

Atualize a lista de pacotes:

sudo apt update

Alternativa Gráfica:

Se você preferir uma interface gráfica, pode usar o aplicativo Software & Updates do Ubuntu:

Abra Software & Updates.

Vá para a aba Other Software.

Desmarque a linha relacionada ao repositório de parceiros (Canonical Partners).

Clique em Fechar e depois confirme se deseja recarregar a lista de pacotes.

Conclusão:

Remover o repositório de parceiros do Ubuntu pode ser uma boa prática em termos de governança de TI, especialmente em ambientes corporativos que exigem controle rigoroso de fontes de software, segurança e conformidade com regulamentações. Isso ajuda a garantir que apenas pacotes oficiais e auditados sejam usados, minimizando os riscos associados à segurança, privacidade e integridade do sistema.

Desativar o Ubuntu Repor

10 - O que desativar o Ubuntu Report ajuda numa boa governança de TI?

Desativar o Ubuntu Report (também conhecido como Apport), que é o sistema de relatórios de falhas e bugs do Ubuntu, pode ser uma prática importante dentro de uma boa governança de TI, especialmente em ambientes corporativos e sistemas que precisam garantir a segurança, a privacidade e o controle sobre os dados coletados. Aqui estão as principais razões pelas quais desativar o Ubuntu Report pode ser benéfico:

1. Proteção da Privacidade

O Ubuntu Report, através do Apport, coleta informações detalhadas sobre o sistema, incluindo logs de falhas, dados sobre pacotes instalados e configurações do sistema. Em algumas situações, esses relatórios podem incluir informações sensíveis, como detalhes sobre o hardware ou configurações específicas do sistema, que podem ser usadas para identificar usuários ou vulnerabilidades.

Desativar o Ubuntu Report ajuda a proteger a privacidade dos usuários, evitando o envio involuntário de dados que podem ser sensíveis ou confidenciais.

2. Controle de Dados

Em muitas organizações, é crucial manter controle sobre os dados que são enviados para fora da rede corporativa. O Ubuntu Report pode enviar informações de falhas e bugs para os servidores da Canonical, o que pode ser indesejável em ambientes com políticas rigorosas de controle de dados. Ao desativá-lo, a organização pode evitar o envio de dados que possam ser irrelevantes ou que possam violar as políticas de privacidade e segurança da empresa.

3. Conformidade com Regulamentações de Privacidade

Em algumas jurisdições e setores, existem regulamentações de proteção de dados, como o GDPR (Regulamento Geral de Proteção de Dados) da União Europeia, que exigem que as empresas protejam e gerenciem os dados pessoais de forma rigorosa. O envio de relatórios de falhas pode potencialmente incluir dados pessoais ou informações sobre o comportamento do usuário, o que poderia entrar em conflito com essas regulamentações. Desativar o Ubuntu Report ajuda a reduzir o risco de violações e facilita o cumprimento das leis de privacidade.

4. Segurança

Embora o Ubuntu Report tenha como objetivo melhorar a qualidade e a confiabilidade do sistema, ele pode enviar informações sobre falhas de segurança que podem ser analisadas e, em alguns casos, usadas por atacantes para explorar vulnerabilidades. Embora a Canonical tenha medidas para proteger a integridade desses dados, em um ambiente corporativo, é mais seguro desativar o envio de relatórios de falhas para reduzir a exposição do sistema a ataques baseados em informações de falhas.

5. Prevenção de Exposição Involuntária

Algumas falhas e bugs podem expor informações sobre a arquitetura do sistema, pacotes instalados ou outros detalhes que poderiam ser usados de forma maliciosa se caírem nas mãos erradas.

Desativar o Ubuntu Report reduz a chance de essas informações serem enviadas para fora da rede corporativa sem o controle adequado.

6. Redução de Dependência de Serviços Externos

Para muitas organizações, manter todos os processos e serviços internos sob controle é uma prioridade. O Ubuntu Report depende de servidores externos para enviar os relatórios de falhas, o que pode ser visto como uma dependência desnecessária de um serviço externo. Desativando o Ubuntu Report, a organização mantém o controle completo sobre o processo de coleta de dados de falhas.

7. Economia de Recursos de Rede e Sistema

Embora o impacto seja geralmente pequeno, a coleta e envio de relatórios pode consumir largura de banda da rede e recursos do sistema. Desativar o Ubuntu Report pode ajudar a liberar recursos de rede e processamento, especialmente em sistemas com recursos limitados.

Como desativar o Ubuntu Report:

Você pode desativar o Ubuntu Report de duas formas principais: via terminal ou via interface gráfica.

Via Terminal:

Abra o terminal e edite o arquivo de configuração do Apport:

```
sudo nano /etc/default/apport
```

Localize a linha `enabled=1` e altere para `enabled=0`:

```
enabled=0
```

Salve o arquivo e saia do editor.

Para garantir que o Apport pare de coletar relatórios, você pode desabilitar o serviço:

```
sudo systemctl stop apport.service
```

```
sudo systemctl disable apport.service
```

Via Interface Gráfica:

Abra Configurações do Sistema.

Vá até a seção Privacidade.

Em Relatórios de Erros, desmarque a opção para enviar relatórios automaticamente.

Conclusão:

Desativar o Ubuntu Report (Apport) em um ambiente corporativo ou em sistemas críticos pode ser uma boa prática de governança de TI, pois ajuda a proteger a privacidade dos usuários, garantir o controle sobre os dados enviados, evitar a exposição involuntária de informações sensíveis, e reduzir o risco de falhas de segurança ou problemas de conformidade com regulamentações de privacidade. Ao desabilitar o envio de relatórios de falhas, você mantém o controle sobre o que está sendo compartilhado e minimiza os riscos associados ao envio de dados para servidores externos.

Remoção do Apport

11 - O que a remoção do Apport no Ubuntu ajuda numa boa governança de TI?

A remoção do Apport no Ubuntu pode ser relevante para uma boa governança de TI por diversos motivos, principalmente no contexto de segurança, performance e controle sobre os sistemas. O Apport é um sistema de coleta de relatórios de falhas no Ubuntu, utilizado para enviar informações sobre crashes e erros de software aos desenvolvedores para análise. Porém, em ambientes de produção ou em organizações que precisam de maior controle sobre os sistemas, a remoção do Apport pode trazer algumas vantagens, como:

1. Segurança:

Evita o envio de dados sensíveis: Apport pode coletar informações sobre o sistema e o software no momento de falhas, o que inclui detalhes que podem ser confidenciais, como arquivos de configuração, credenciais ou caminhos de diretórios. A remoção do Apport reduz o risco de vazamento acidental de dados sensíveis para servidores externos.

Controle sobre o que é compartilhado: Ao desabilitar ou remover o Apport, a organização tem maior controle sobre o que é enviado aos desenvolvedores, garantindo que nenhum dado sensível seja compartilhado sem a devida autorização ou processamento de segurança.

2. Desempenho e Recursos do Sistema:

Redução de uso de recursos: O Apport pode consumir recursos do sistema, principalmente durante eventos de falha. A remoção ou desativação do Apport pode liberar recursos do sistema, como CPU e memória, permitindo uma maior eficiência e desempenho, especialmente em servidores e ambientes de produção.

Redução de ruído em ambientes de produção: Em ambientes críticos, como servidores, a geração constante de relatórios de falhas pode gerar “ruído” nos logs, dificultando a identificação de problemas reais de produção. A remoção do Apport pode ajudar a reduzir essa sobrecarga.

3. Conformidade e Política de Governança:

Alinhamento com políticas de privacidade e governança: Algumas organizações têm políticas rigorosas sobre o envio de dados para fora de seus sistemas. A remoção do Apport pode garantir que a empresa esteja em conformidade com as regulamentações de privacidade, como a LGPD (Lei Geral de Proteção de Dados) no Brasil ou o GDPR na Europa, já que a coleta de dados não será feita automaticamente sem um controle rigoroso.

Controle sobre os relatórios de falhas: A governança de TI pode preferir controlar manualmente os relatórios de falhas, como parte de um processo de gestão de incidentes mais formal, em vez de depender de uma ferramenta automática que pode não ter o mesmo nível de rastreabilidade ou aprovações internas.

4. Estabilidade e Minimização de Riscos:

Evitar possíveis falhas em ambientes críticos: Em sistemas de produção ou críticos, a geração de relatórios automáticos pode não ser desejada, já que o Apport pode gerar falhas adicionais ao tentar capturar detalhes do erro, o que pode afetar ainda mais a estabilidade do sistema.

Menos complexidade: A remoção do Apport simplifica o sistema ao eliminar uma camada adicional de processamento. Isso pode reduzir a complexidade, o que é benéfico para a manutenção e governança.

Considerações Finais:

A remoção do Apport pode ser uma boa prática em ambientes de TI corporativa, especialmente quando o foco está na segurança, controle de dados, e performance do sistema. No entanto, em ambientes de desenvolvimento ou testes, o Apport pode ser útil para coletar informações detalhadas sobre falhas e erros de software. Portanto, a decisão de remover ou desativar o Apport depende do ambiente e das necessidades específicas da organização.

Se precisar de mais detalhes sobre como desabilitar ou configurar o Apport no Ubuntu, posso te ajudar com isso também!

Remoção do Snap e SnapD

12- O que a remoção do Snap e SnapD no Ubuntu ajuda numa boa governança de TI?

A remoção do Snap e do Snapd no Ubuntu pode ser vantajosa para uma boa governança de TI, dependendo dos objetivos de controle, segurança, desempenho e conformidade de uma organização. O Snap é uma tecnologia de pacotes para software, que visa simplificar a instalação e atualização de aplicativos no Ubuntu e outras distribuições Linux. Já o Snapd é o serviço responsável por gerenciar os pacotes Snap no sistema.

Aqui estão os principais motivos pelos quais a remoção do Snap e do Snapd pode ser relevante para a boa governança de TI:

1. Segurança e Controle de Software

Controle centralizado de pacotes: No Ubuntu, o Snap permite que aplicativos sejam instalados de maneira independente do sistema e sem necessidade de pacotes tradicionais como DEBs. Isso pode ser vantajoso em termos de isolamento e controle de dependências, mas em ambientes corporativos, pode ser difícil garantir que as versões e os pacotes Snap sejam compatíveis e seguros.

Preocupações com a segurança do Snapd: O Snapd é responsável por gerenciar os pacotes Snap, e, em alguns casos, pode ser considerado um vetor de ataque devido à sua necessidade de comunicação constante com servidores externos. A remoção do Snapd elimina esse risco, uma vez que o sistema deixa de depender de serviços que podem ser explorados para comprometer o sistema.

Isolamento inadequado: Embora os pacotes Snap ofereçam uma forma de "isolamento" para os aplicativos, alguns profissionais de TI acreditam que esse isolamento não é suficiente, principalmente quando se trata de permissões de acesso a arquivos e recursos do sistema. Remover o Snap e o Snapd dá um controle mais direto sobre como os aplicativos são instalados e isolados no sistema.

2. Desempenho e Consumo de Recursos

Uso de recursos do sistema: O Snapd pode consumir recursos do sistema, principalmente durante a instalação ou atualização de pacotes Snap. Além disso, cada pacote Snap vem com suas próprias dependências, o que pode levar a um maior consumo de espaço em disco e memória. Remover o Snap pode melhorar o desempenho do sistema ao reduzir o consumo de recursos desnecessários.

Desempenho de aplicativos Snap: Alguns usuários relatam que aplicativos instalados como Snap podem ter um desempenho inferior em comparação com seus equivalentes em pacotes DEB ou Flatpak, devido ao overhead de execução e do próprio formato Snap. A remoção pode ajudar a melhorar o desempenho geral do sistema.

3. Gerenciamento e Manutenção Simplificados

Simplificação da gestão de pacotes: A remoção do Snap e Snapd pode simplificar o gerenciamento de pacotes em um ambiente corporativo, uma vez que se concentra apenas em pacotes DEB ou outras tecnologias de gerenciamento de pacotes como APT. Isso pode ser vantajoso em termos de facilidade de manutenção, especialmente quando se utiliza ferramentas de gerenciamento de configuração ou automação, como Ansible ou Puppet, que são mais otimizadas para pacotes tradicionais.

Menos atualizações automáticas: O Snap pode atualizar automaticamente os pacotes em segundo plano, o que pode ser indesejável em ambientes de produção, onde as atualizações precisam ser gerenciadas de maneira controlada e testada. A remoção do Snap evita esse tipo de comportamento e coloca o controle das atualizações de software diretamente nas mãos da equipe de TI.

4. Conformidade e Auditoria

Conformidade com políticas de TI e governança: Em muitas organizações, as políticas de TI exigem controle rigoroso sobre o software instalado nos sistemas, garantindo que os pacotes estejam de acordo com normas de segurança e licenciamento. O uso de Snap pode dificultar a rastreabilidade, uma vez que os pacotes Snap não são gerenciados de maneira tradicional e podem ser atualizados automaticamente, sem o conhecimento ou autorização da equipe de TI.

Auditoria mais clara: Com o Snap removido, é mais fácil auditar e rastrear quais pacotes estão instalados no sistema, pois a instalação de software se dá de maneira mais transparente e previsível, usando pacotes DEB ou repositórios oficiais. Isso facilita a conformidade com regulamentações de segurança, como a ISO 27001 ou GDPR, que exigem controles rigorosos sobre o software usado em um sistema.

5. Minimização de Riscos e Complexidade

Redução de dependências externas: O Snap precisa se comunicar com servidores externos para atualizar pacotes e obter informações. Isso pode ser um risco de segurança, principalmente em ambientes corporativos que preferem limitar a comunicação com fontes externas, seja por questões de segurança ou de controle.

Simplificação do ambiente de TI: Remover o Snap pode reduzir a complexidade do ambiente de TI, pois elimina uma camada adicional de gerenciamento e interação com pacotes. Em vez disso, a organização pode se concentrar em soluções mais tradicionais ou amplamente aceitas (como APT ou Flatpak), facilitando o treinamento da equipe e a integração com outras ferramentas.

6. Maior Controle sobre o Software Instalado

Instalação de software personalizada: Em um ambiente corporativo, muitas vezes é necessário configurar o software de uma maneira específica ou instalar versões personalizadas de certos aplicativos. Os pacotes Snap são frequentemente mais fechados e podem não oferecer o mesmo nível de flexibilidade ou personalização que os pacotes tradicionais DEB ou código-fonte.

Considerações Finais:

A remoção do Snap e do Snapd no Ubuntu pode melhorar a governança de TI, proporcionando maior controle, segurança e desempenho, além de simplificar a gestão e conformidade com as políticas corporativas. No entanto, o Snap oferece benefícios, como a facilidade de instalação e atualização de pacotes de software, além de isolamento e segurança para os aplicativos. Portanto, a decisão de remover ou manter o Snap depende das necessidades específicas de cada organização, incluindo o nível de controle desejado e o tipo de infraestrutura que a empresa utiliza.

Se você precisar de mais detalhes sobre como remover o Snap e Snapd no Ubuntu, posso te fornecer um guia para isso também!

Remoção dos avisos sobre o Ubuntu Pro

13- O que a remoção dos avisos sobre o Ubuntu Pro ajuda numa boa governança de TI?

A remoção ou desativação dos avisos sobre o Ubuntu Pro pode ser uma estratégia de governança de TI interessante em certos contextos, principalmente em ambientes corporativos que buscam maior controle, eficiência e conformidade. O Ubuntu Pro é uma oferta da Canonical, que proporciona suporte e atualizações estendidas para versões LTS do Ubuntu, mas o sistema exibe notificações sobre essa disponibilidade, incentivando os administradores a ativar o serviço.

Aqui estão algumas maneiras de como a remoção desses avisos pode contribuir para uma boa governança de TI:

1. Redução de Ruído e Sobrecarga de Notificações

Menos distração para os administradores de TI: Em ambientes onde a equipe de TI precisa focar em tarefas específicas e problemas críticos de produção, os avisos sobre o Ubuntu Pro podem ser vistos como uma distração. Removê-los pode ajudar a reduzir o “ruído” nas notificações do sistema, permitindo que a equipe se concentre no que é mais importante, sem ser constantemente alertada sobre serviços opcionais.

Limpeza de notificações em sistemas gerenciados: Quando você tem um grande número de servidores ou estações de trabalho gerenciados centralizadamente, esses avisos podem se tornar um incômodo se não houver uma intenção clara de ativar o Ubuntu Pro. A remoção ou desativação desses avisos pode manter as notificações mais organizadas e relevantes.

2. Controle Centralizado e Conformidade com Políticas Internas

Alinhamento com as políticas de governança: Se uma organização tem uma política de não usar serviços de pagamento ou de manter todos os sistemas dentro de uma estrutura controlada, os administradores podem remover ou desabilitar os avisos do Ubuntu Pro para garantir que os usuários ou administradores não ativem acidentalmente o serviço sem passar pelo processo de avaliação ou aprovação interna.

Prevenção de ativações não autorizadas: Em algumas organizações, pode ser necessário garantir que o Ubuntu Pro não seja ativado sem uma análise completa de custo-benefício ou uma aprovação formal. A remoção dos avisos pode ajudar a evitar que um serviço pago seja ativado sem a devida autorização, o que pode levar a custos desnecessários ou não planejados.

3. Otimização do Desempenho e Menos Interrupções

Evitar processamento desnecessário: Embora os avisos em si não sejam pesados em termos de recursos, a interação com o sistema (ou a frequência de alertas) pode ser um pequeno fator de sobrecarga. Remover ou desativar esses avisos pode resultar em menos interações desnecessárias do sistema com o usuário, contribuindo para uma experiência mais suave e eficiente.

Menos pop-ups e interrupções: Em sistemas críticos ou de produção, as interrupções frequentes para avisos podem afetar a fluidez do trabalho. Para manter a estabilidade do ambiente de TI e reduzir interrupções nas operações, a remoção de avisos ajuda a garantir que os administradores se concentrem apenas nas questões essenciais.

4. Facilidade de Gerenciamento em Grandes Ambientes

Gestão de servidores e estações de trabalho em larga escala: Em ambientes corporativos com um grande número de servidores ou estações de trabalho, gerenciar as notificações em cada máquina pode ser um desafio. A remoção dos avisos sobre o Ubuntu Pro pode ser uma maneira de padronizar o comportamento dos sistemas, tornando mais fácil para a equipe de TI controlar e configurar os dispositivos sem a preocupação com notificações que não são relevantes.

Automatização e scripts de configuração: Se a organização utilizar ferramentas de automação (como Ansible, Puppet, Chef, ou SaltStack) para gerenciar a configuração de sistemas, desabilitar esses avisos de forma centralizada pode ser facilmente integrado aos scripts de configuração, garantindo consistência entre todos os sistemas sem a necessidade de interação manual.

5. Controle de Custos

Evitar ativação não planejada do Ubuntu Pro: O Ubuntu Pro oferece benefícios como suporte estendido e segurança adicional, mas pode ter custos associados, especialmente em grandes volumes de máquinas. Remover os avisos ajuda a evitar que administradores ou usuários ativem o serviço sem uma análise cuidadosa dos custos e benefícios. Isso pode ser útil em ambientes onde a organização quer controlar rigorosamente os custos com software e serviços.

Evitar custos inesperados: A remoção dos avisos pode ser uma forma de evitar que o Ubuntu Pro seja ativado sem que a organização tenha orçado esse custo ou que tenha realizado uma avaliação detalhada sobre a necessidade do serviço. Isso pode ser especialmente relevante em grandes implementações, onde cada serviço adicional tem implicações financeiras.

6. Padronização e Consistência no Ambiente de TI

Mantendo uma configuração consistente entre as máquinas: Em empresas que buscam manter um nível alto de padronização em seus ambientes de TI, pode ser preferível desabilitar notificações sobre serviços opcionais como o Ubuntu Pro, já que isso garante que todas as máquinas tenham o mesmo comportamento e não sejam desviadas para ativar funcionalidades diferentes, a menos que isso seja decidido de forma centralizada.

Gestão simplificada: Ao remover esses avisos, a equipe de TI pode gerenciar os sistemas de maneira mais simplificada, sem a necessidade de verificar constantemente se houve qualquer interação com as notificações do Ubuntu Pro, mantendo um controle mais direto sobre os sistemas e seus estados.

Considerações Finais:

A remoção ou desativação dos avisos sobre o Ubuntu Pro pode trazer benefícios significativos em termos de controle, eficiência e conformidade, especialmente em grandes ambientes corporativos, onde o foco está em reduzir distrações, manter a segurança e controlar custos. No entanto, para algumas organizações, os benefícios do Ubuntu Pro — como suporte estendido, atualizações de segurança e acesso a ferramentas empresariais — podem ser valiosos. A decisão de remover esses avisos deve ser tomada com base nas necessidades específicas da organização, levando em consideração tanto os requisitos operacionais quanto financeiros.

Se precisar de ajuda para desabilitar esses avisos ou quiser entender mais sobre o Ubuntu Pro, estou à disposição!

Desfazer as alterações do script

14- O script **NÃO** tem opção para **DESFAZER as alterações**?

R: Cria uma imagem do sistema antes de usar o script.

Ex:

dd

parclone

Clonezilla: <https://clonezilla.org/downloads.php>

Rescuezilla: <https://rescuezilla.com/>

<https://fostips.com/command-remove-snaps-install-vanilla-gnome-ubuntu/>

Sinceramente, estou completamente farto de hardware com defeito e ataques puramente teóricos que nunca se manifestaram na prática.

Linus Torvalds.