

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

MARIA EDUARDA GUEDES DE OLIVEIRA

PESQUISA AOS PROTOCOLOS XMPP, DNS, NFS E BITTORRENT

GUARAPUAVA

2024

MARIA EDUARDA GUEDES DE OLIVEIRA

PESQUISA AOS PROTOCOLOS XMPP, DNS, NFS E BITTORRENT

SEARCH TO THE PROTOCOLS XMPP, DNS, NFS AND BITTORRENT

Trabalho entregue do curso de graduação
apresentado como requisito parcial para a obtenção
de nota do 2º semestre em Sistema de Tecnologia
para Internet, Universidade Tecnológica Federal do
Paraná (UTFPR).

GUARAPUAVA

2024

SUMÁRIO

INTRODUÇÃO.....	4
FUNCIONAMENTO.....	5
XMPP.....	5
DNS.....	5
NFS.....	5
BITTORRENT.....	5
CARACTERÍSTICAS.....	6
XMPP (Extensible Messaging and Presence Protocol):.....	6
DNS sobre HTTPS (DoH):.....	6
NFS (Network File System):.....	7
BitTorrent:.....	7
VANTAGENS E DESVANTAGENS DE CADA PROTOCOLO.....	7
XMPP (Extensible Messaging and Presence Protocol):.....	7
Vantagens:.....	7
Desvantagens:.....	8
DNS sobre HTTPS (DoH):.....	8
Vantagens:.....	8
Desvantagens:.....	8
NFS (Network File System):.....	8
Vantagens:.....	8
Desvantagens:.....	9
BitTorrent:.....	9
Vantagens:.....	9
Desvantagens:.....	9
AMBIENTE DE APLICAÇÃO DE CADA PROTOCOLO:.....	9
XMPP (Extensible Messaging and Presence Protocol):.....	9
DNS sobre HTTPS (DoH):.....	10
NFS (Network File System):.....	10
BitTorrent:.....	10
FUNCIONAMENTO DE CADA PROTOCOLO.....	11
XMPP (Extensible Messaging and Presence Protocol):.....	11
DNS sobre HTTPS (DoH):.....	11
NFS (Network File System):.....	12
BitTorrent:.....	12
REFERÊNCIAS.....	13
LINK DO REPOSITÓRIO GITHUB.....	13

INTRODUÇÃO

XMPP (Extensible Messaging and Presence Protocol): XMPP é um protocolo aberto e extensível para troca de mensagens e presença em tempo real na internet. Ele foi originalmente desenvolvido para permitir a comunicação instantânea (IM) entre pessoas, mas também suporta uma ampla gama de funcionalidades adicionais, como voz sobre IP (VoIP), videoconferência e IoT (Internet das Coisas). XMPP utiliza um modelo cliente-servidor e é conhecido por sua descentralização e interoperabilidade entre diferentes serviços e redes.

DNS sobre HTTPS (DoH): DNS sobre HTTPS é uma extensão do protocolo DNS que permite a resolução de nomes de domínio de forma segura e privada através do protocolo HTTPS. Ele protege a privacidade dos usuários ao criptografar as consultas DNS, dificultando que terceiros, como provedores de internet, interceptem ou manipulem os dados de resolução de DNS. DoH facilita o acesso à internet de forma mais segura, especialmente em redes públicas ou onde a privacidade é uma preocupação.

NFS (Network File System): NFS é um protocolo de sistema de arquivos distribuído que permite que computadores em uma rede acessem diretórios e arquivos em outros sistemas de forma transparente. Ele facilita o compartilhamento de recursos de armazenamento entre sistemas operacionais Unix-like, permitindo que um sistema monte um sistema de arquivos remoto como se fosse local. NFS é amplamente utilizado em ambientes onde o armazenamento centralizado e o acesso a arquivos de forma eficiente são necessários, como em redes corporativas e servidores de arquivos.

BitTorrent: BitTorrent é um protocolo peer-to-peer utilizado para compartilhamento de arquivos pela internet. Ele permite que os usuários compartilhem partes de arquivos entre si, ao invés de dependerem exclusivamente de um único servidor centralizado. O BitTorrent divide os arquivos em pequenas partes, distribuindo-as entre os peers (pares) da rede. Isso resulta em downloads mais rápidos e eficientes, especialmente para arquivos grandes, além de aliviar a carga nos servidores tradicionais. O protocolo BitTorrent é amplamente utilizado para distribuição de conteúdo digital, incluindo filmes, música, software e jogos.

FUNCIONAMENTO

XMPP

Seu funcionamento no Linux, o XMPP é geralmente implementado através de clientes de mensagens instantâneas como Pidgin, Empathy, ou programas específicos como o Gajim. Esses clientes se conectam a servidores XMPP, como o Prosody, ejabberd ou Openfire, que são instalados e configurados em servidores Linux. Os clientes XMPP permitem trocar mensagens instantâneas, presença, e até mesmo realizar chamadas de voz e vídeo, dependendo das capacidades do servidor e do cliente utilizados.

DNS

No Linux, o suporte ao DNS sobre HTTPS pode variar de acordo com o sistema operacional e a configuração do navegador ou aplicativo. Muitos navegadores modernos suportam DoH nativamente, onde as consultas DNS são criptografadas e enviadas através do protocolo HTTPS para servidores DoH compatíveis. Além disso, é possível configurar resolvers DNS que suportam DoH, como o systemd-resolved, para que todas as consultas DNS do sistema sejam feitas através de HTTPS.

NFS

O NFS é bem suportado e amplamente utilizado no Linux para compartilhamento de arquivos entre sistemas. No servidor, é necessário configurar e exportar diretórios através do arquivo `/etc/exports`, especificando quais sistemas e usuários têm permissão para acessar esses recursos compartilhados. Nos clientes Linux, os sistemas de arquivos remotos são montados usando o comando `mount` ou configurados no `/etc/fstab` para montagem automática durante a inicialização do sistema. O NFS permite acesso transparente a arquivos e diretórios em sistemas remotos como se fossem locais.

BITTORRENT

No Linux, há vários clientes BitTorrent disponíveis, como o Transmission, qBittorrent, Deluge, entre outros. Esses clientes permitem que os usuários baixem e compartilhem arquivos usando o protocolo BitTorrent. Para baixar um arquivo via

BitTorrent, você geralmente precisa de um arquivo .torrent que contém informações sobre os peers e o arquivo a ser baixado. O cliente BitTorrent então se conecta aos peers para baixar partes do arquivo simultaneamente, enquanto também compartilha as partes já baixadas com outros peers. É possível controlar a largura de banda, prioridades de download e outras configurações através desses clientes.

CARACTERÍSTICAS

XMPP (Extensible Messaging and Presence Protocol):

Aberto e Extensível: XMPP é um protocolo aberto, definido pelo RFC 6120 e 6121, e é extensível através de extensões (XEPs) que adicionam funcionalidades como transferência de arquivos, criptografia, entre outras.

Comunicação em Tempo Real: Suporta troca de mensagens instantâneas, presença (disponibilidade de usuários), e notificações em tempo real.

Descentralizado: Permite a operação descentralizada, com servidores XMPP interoperáveis que podem ser configurados para se comunicarem diretamente uns com os outros.

Segurança: Pode suportar criptografia TLS para proteção das comunicações.

Aplicações: Além de mensagens instantâneas, é utilizado para VoIP, videoconferência, IoT, entre outros.

DNS sobre HTTPS (DoH):

Criptografia: Todas as consultas DNS são criptografadas usando HTTPS, o que protege a privacidade dos usuários contra interceptações e manipulações.

Privacidade: Evita que provedores de internet e terceiros monitorem ou modifiquem as consultas DNS realizadas pelos usuários.

Compatibilidade: Pode ser integrado em navegadores web e outros aplicativos para garantir que todas as solicitações DNS sejam feitas através de HTTPS.

Implementações: Existem várias implementações de servidores DoH e suporte crescente em navegadores e sistemas operacionais.

NFS (Network File System):

Compartilhamento de Arquivos: Permite que sistemas Unix-like compartilhem diretórios e arquivos de forma transparente através da rede.

Montagem Remota: Os sistemas de arquivos NFS são montados nos clientes Linux como se fossem locais, facilitando o acesso a dados centralizados.

Performance: Oferece boa performance para acesso a arquivos, especialmente em redes locais de alta velocidade.

Segurança: Pode ser configurado com controles de acesso e autenticação para garantir a segurança dos dados compartilhados.

BitTorrent:

Distribuição Peer-to-Peer: Os arquivos são compartilhados diretamente entre os usuários (peers) da rede, sem depender de um servidor centralizado.

Divisão de Arquivos: Os arquivos são divididos em pequenas partes, facilitando o download simultâneo de múltiplas partes de diferentes peers.

Eficiência: Permite downloads rápidos e eficientes, pois vários peers contribuem com partes do arquivo simultaneamente.

Popularidade: Ampla utilização para distribuição de grandes arquivos como filmes, música, software e jogos, aliviando a carga em servidores convencionais.

VANTAGENS E DESVANTAGENS DE CADA PROTOCOLO

XMPP (Extensible Messaging and Presence Protocol):

Vantagens:

- **Interoperabilidade:** Funciona com uma ampla variedade de clientes e servidores, permitindo comunicação entre diferentes plataformas.
- **Extensibilidade:** Pode ser estendido através de XEPs para suportar novas funcionalidades conforme necessário.
- **Descentralização:** Permite a operação de servidores independentes, oferecendo maior controle e privacidade para os usuários.
- **Segurança** Suporta criptografia TLS para proteger as comunicações.

Desvantagens:

- Complexidade de Implementação: Configurar e manter servidores XMPP pode exigir conhecimentos técnicos avançados.
- Variedade de Implementações: A interoperabilidade entre diferentes implementações nem sempre é perfeita, podendo causar problemas de compatibilidade.
- Competição de Protocolos: A popularidade de plataformas de mensagens centralizadas como WhatsApp e Telegram diminuiu o uso de XMPP em certos contextos.

DNS sobre HTTPS (DoH):

Vantagens:

- Privacidade Reforçada: Protege contra a monitoração e manipulação de consultas DNS por provedores de internet e outros intermediários.
- Segurança: Criptografa todas as consultas DNS, aumentando a segurança das comunicações online.
- Integração com HTTPS: Utiliza a infraestrutura existente de HTTPS, o que facilita a implementação e adoção.

Desvantagens:

- Complexidade Operacional: Configurar servidores DoH e garantir a compatibilidade com diferentes plataformas pode ser complexo.
- Controvérsias de Privacidade: Alguns argumentam que DoH pode dificultar a aplicação de políticas de segurança em redes corporativas ou educacionais.

NFS (Network File System):

Vantagens:

- Eficiência: Oferece bom desempenho para acesso a arquivos em redes locais de alta velocidade.
- Integração com Sistemas Unix-like: Totalmente integrado com sistemas operacionais Unix-like, facilitando o compartilhamento de recursos.
- Simplicidade de Uso: Montagem de sistemas de arquivos remotos é transparente para os usuários.

Desvantagens:

- **Segurança**:** NFS tradicionalmente não possui criptografia embutida, exigindo configurações adicionais para proteger dados sensíveis.
- **Complexidade de Configuração:** Configurar e manter servidores NFS pode ser complicado, especialmente em ambientes grandes.

BitTorrent:

Vantagens:

- **Distribuição Eficiente:** Permite downloads rápidos e eficientes ao distribuir a carga entre vários peers.
- **Redução de Custo de Banda:** Reduz a carga nos servidores centrais ao distribuir o tráfego entre os usuários.
- **Resiliência:** A natureza descentralizada do protocolo torna a rede mais resistente a falhas e censura.

Desvantagens:

- **Legalidade e Pirataria:** Muitos conteúdos distribuídos via BitTorrent podem violar direitos autorais, o que gera controvérsias legais.
- **Reputação Negativa:** O uso generalizado para compartilhamento ilegal de conteúdo afeta a percepção pública do protocolo.
- **Segurança:** A autenticidade e integridade dos arquivos baixados podem ser um problema se não verificados adequadamente.

AMBIENTE DE APLICAÇÃO DE CADA PROTOCOLO:

XMPP (Extensible Messaging and Presence Protocol):

- **Ambiente de Uso:** XMPP é frequentemente utilizado em ambientes que requerem comunicação instantânea, presença e colaboração em tempo real.

Em empresas onde a comunicação interna entre funcionários é crucial, especialmente em equipes distribuídas ou com necessidade de comunicação segura.

Em instituições educacionais para comunicação entre alunos e professores, e para suporte técnico.

Para comunicação entre dispositivos na Internet das Coisas, devido à sua capacidade de suportar mensagens e presença.

DNS sobre HTTPS (DoH):

- Ambiente de Uso: DoH é utilizado principalmente em ambientes onde a privacidade e segurança das comunicações DNS são prioritárias.

Navegadores web modernos estão cada vez mais integrando suporte a DoH para proteger consultas DNS contra espionagem e manipulação.

Em ambientes corporativos ou educacionais onde políticas de privacidade estritas são aplicadas.

Para proteger contra sniffing de DNS e outros ataques em redes Wi-Fi públicas.

NFS (Network File System):

- Ambiente de Uso**: NFS é comumente utilizado em ambientes que necessitam compartilhar arquivos entre sistemas Unix-like de forma eficiente e transparente.

Em ambientes corporativos e data centers onde há necessidade de armazenamento compartilhado acessível por múltiplos sistemas.

Em ambientes de desenvolvimento de software, onde arquivos de código e recursos precisam ser compartilhados entre desenvolvedores.

Para centralizar backups de dados em um servidor NFS acessível por várias máquinas.

BitTorrent:

- BitTorrent é amplamente utilizado em ambientes onde a distribuição eficiente de grandes volumes de dados é necessária, mesmo com largura de banda limitada.

Para distribuição de conteúdo digital como filmes, música, software e jogos de forma descentralizada.

Para distribuir grandes imagens de ISO de sistemas operacionais e outros softwares de código aberto.

Em plataformas de jogos e aplicativos onde grandes atualizações precisam ser distribuídas eficientemente para milhares de usuários.

FUNCIONAMENTO DE CADA PROTOCOLO

XMPP (Extensible Messaging and Presence Protocol):

O XMPP opera em um modelo cliente-servidor. Aqui estão os passos básicos do funcionamento:

1. Um cliente XMPP se conecta a um servidor XMPP através de um canal de comunicação seguro (geralmente TLS/SSL).
2. O cliente envia suas credenciais de login (nome de usuário e senha) ao servidor para autenticação.
3. Após autenticado, o cliente pode enviar sua presença ao servidor, indicando seu status online, offline, ocupado, etc.
4. Os clientes podem trocar mensagens instantâneas, arquivos, iniciar chamadas de voz ou vídeo, tudo isso através do servidor XMPP.
5. O protocolo é extensível através de XEPs (XMPP Extension Protocols), que adicionam funcionalidades adicionais como transferência de arquivos, conferências multiusuário, entre outros.

DNS sobre HTTPS (DoH):

Funcionamento: DoH permite que consultas DNS sejam criptografadas e enviadas através de HTTPS. Aqui está como funciona:

1. Consulta DNS: O cliente (como um navegador web) precisa resolver um nome de domínio em um endereço IP.
2. Solicitação HTTPS: Em vez de enviar a consulta DNS em texto simples, o cliente envia a consulta criptografada para um servidor DoH através de uma conexão HTTPS.
3. Resposta Criptografada: O servidor DoH responde com a resposta DNS criptografada, que o cliente decodifica para obter o endereço IP desejado.
4. Proteção de Privacidade: Esse processo protege contra interceptação e manipulação das consultas DNS, garantindo maior privacidade para o usuário final.

NFS (Network File System):

NFS permite que sistemas Unix-like acessem e compartilhem arquivos através da rede. Aqui está como funciona em alto nível:

1. Servidor NFS: Um sistema configurado como servidor NFS exporta (compartilha) diretórios ou sistemas de arquivos específicos.
2. Montagem NFS: Um cliente NFS monta (faz o acesso) a esses sistemas de arquivos remotos como se fossem locais.
3. Acesso Transparente: Uma vez montado, o sistema operacional cliente pode acessar e manipular arquivos no sistema de arquivos NFS remoto da mesma forma que se fossem locais.
4. Controle de Acesso: O servidor NFS define permissões de acesso aos arquivos compartilhados, permitindo ou negando acesso com base nas configurações de segurança.

BitTorrent:

Funcionamento: BitTorrent é um protocolo peer-to-peer para distribuição de arquivos. Aqui estão os passos básicos do seu funcionamento:

1. Divisão do Arquivo: O arquivo a ser compartilhado é dividido em pequenos pedaços (chunks).
2. Meta-Informação: Um arquivo .torrent é criado, contendo informações sobre os pedaços e trackers (servidores que auxiliam na conexão de peers).
3. Conexão com Peers: Um cliente BitTorrent se conecta a outros peers que estão compartilhando o mesmo arquivo. Ele pode obter endereços IP desses peers a partir de um tracker ou de outros peers conhecidos (peer exchange).
4. Download e Upload: O cliente BitTorrent baixa partes do arquivo de múltiplos peers simultaneamente (download). Ao mesmo tempo, ele também envia partes do arquivo que já baixou para outros peers (upload).
5. Reconstrução do Arquivo: Após baixar todas as partes, o cliente BitTorrent reconstrói o arquivo completo.

REFERÊNCIAS

AWS. **O que é o DNS?** Disponível em: <<https://aws.amazon.com/pt/route53/what-is-dns/>>. Acesso em 29 de junho 2024.

Digital Ocean. **Como configurar uma montagem NFS no Ubuntu 20.04.** Brian Boucheron, 2020. Disponível em:<<https://www.digitalocean.com/community/tutorials/how-to-set-up-an-nfs-mount-on-ubuntu-20-04-pt>>. Acesso em 26 de junho de 2024.

W2 Websites. **O que é XMPP Server?** Disponível em: <<https://w2websites.com/glossario/o-que-e-xmpp-server/>>. Acesso em 27 de junho de 2024.

LINK DO REPOSITÓRIO GITHUB

<https://github.com/mariagued/protocolos>

LINK DO VÍDEO YOUTUBE

<https://youtu.be/kEtaFJAui44>