

Síťové souborové systémy

Michal Moudrý

24. listopadu 2018

Abstrakt

Tento dokument obsahuje zpracované zadání na téma síťové souborové systémy, jež se zabývá protokoly síťových souborových systémů, jako například NFS či SMB. Dále se práce zaměřuje na využití daných systémů, mezi které jsem vybral použití v NAS serverech, ovšem jsou v této práci rozebrány i klasické souborové systémy (FS). Cílem této práce je obecné seznámení se souborovými systémy a protokoly umožňující sdílení souborů v počítačové síti. Součástí této práce je i praktická část, která má za účel simulaci operace nasazení části disku serveru na klienta a analyzovat síťový provoz na portu serveru během dané operace.

1 Úvod

Předmětem této semestrální práce je popis technologie síťových souborových systémů a jejich protokolů, dále také jejich využití a analýza komunikace mezi NFS serverem a klientem za pomoci nástroje Tshark v rámci virtuální počítačové sítě hostované na cloudové platformě Azure.

Tento dokument se skládá z teoretické části, tedy kapitola č. 2, kde jsou popsány souborové systémy obecně, včetně dvou příkladů, následně jsou popsány distribuované souborové systémy v podkapitole č. 2.2. Poslední dvě podkapitoly č. 2.3 a 2.4 pojednávají o protokolech a využití souborových systémů. Po teoretické části následuje praktická část, ve které se nachází podkapitola č. 3.1 o specifikaci virtuální sítě a hostů, pak podkapitola č. 3.2 o analýze provozu mezi klientem a serverem při nasazování části disku.

2 Teoretická část

Tato kapitola pojednává o obecně o souborových systémech, tedy k čemu takové systémy slouží a jaké mohou mít vlastnosti, dále také jejich interakce s operačním systémem, ale také o distribuovaných souborových systémech a síťových souborových systémech. Účelem této kapitoly je obecné seznámení se souborovými systémy, společně s nejčastěji používanými protokoly a možným využitím síťových FS.

2.1 Souborové systémy

Souborové systémy jsou takové systémy, které určují, jakým způsobem budou data a metadata organizována na vnější paměti (pevný disk, paměťová karta, flash disk, ...), ale také informace pro přístup uživatele k daným datům (soubory, složky). Pro tuto organizaci využívají souborové systémy datové struktury, jako například pole bloků nebo struktury, jež jsou založené na stromové struktuře.[1, 2]

Co se týče souborových systémů a jejich interakce s operačním systémem, tak operační systém volá FS pro získání přístupu k jejich funkcím, jako například verzování či šifrování. Samozřejmě může být hned několik souborových systémů na jednom zařízení a proto OS obsahuje virtuální souborový systém (VFS), který umožňuje existenci více FS a poskytuje k nim jednotné rozhraní, přičemž cílem VFS je zlehčení přenositelnosti mezi operačními systémy.[3]

2.1.1 NTFS

Jedná se o žurnálovací souborový systém vyvinutý společností Microsoft, který je hojně využíván produkty dané společnosti. Žurnálovací souborové systémy využívají soubor se záznamy („logy“) jednotlivých operacích pro provedení nedokončených operací v případě výpadku systému, což má za výsledek vysokou spolehlivost FS.[2]

Co se týče bezpečnosti, tak NTFS využívá Access Control List (ACL), což je list oprávnění uživatelů či skupin uživatelů k souborům nebo složkám. NTFS využívá technologie Encrypted File System (EFS) pro ukládání zašifrovaných dat na vnější paměti.[2]

2.1.2 ZFS

Identicky jako NTFS je ZFS žurnálovací souborový systém, ale byl vyvinut společností Sun Microsystems a byl vydán pod open-source licenci. Přestože byl tento FS vyvinut původně pro operační systém Solaris, tak ho lze nalézt na BSD a několika různých distribucích Linuxu a dalších operačních systémech.[4]

Mezi hlavní funkce a vlastnosti tohoto systému patří proměnlivá velikost paměťových bloků, komprese dat, kdy ZFS implementuje kompresi dat a tím zrychluje některé diskové operace. Další funkcí je kontrola dat, kdy ZFS provádí kontrolu dat za účelem udržení jejich konzistence, kdy ukládá 64bitové kontrolní součty na vnější paměti zařízení, aby mohl následně tuto operaci provádět.[4]

2.2 Distribuované souborové systémy

Byly prvním případem využití modelu klient a server s distribucí výpočtu. Prostředí v takovém to systému je složeno z klientů a jednoho či více serverů, přičemž server na své vnější paměti má data a klienti posílají požadavky na daná data pomocí protokolových zpráv (např. ACCESS operace u NFS). Výhodou

této konfigurace je sdílení dat mezi několika klienty najednou, dále také jednodušší administrace, kdy třeba nastavení verzování dokumentů lze nakonfigurovat z menšího počtu serverů než klientů.[5]

Jedním z prvních distribuovaných systémů byl Sun Network File System, jež byl vyvinut společností Sun Microsystems. Významným aspektem tohoto systému byl jeho samotný vývoj, kdy společnost Sun Microsystems vytvořila protokol pro komunikaci mezi serverem a klientem, dnes známý jako NFS, který nebyl proprietární, a tedy ostatní výrobci mohli dělat jejich NFS servery, což mělo za výsledek velkou rozšířenost protokolu NFS.[5]

2.3 Protokoly síťových souborových systémů

2.3.1 NFS

Network File System (NFS) je protokol od společnosti Sun Microsystems, jehož účel je poskytnutí vzdáleného přístupu k datům, která jsou sdílena zařízením v síti. Velkou výhodou tohoto protokolu je jeho snadná přenositelnost mezi jinými operačními systémy, transportními protokoly či architekturami sítě a je tedy nezávislý na těchto částech. Nezávislost tohoto protokolu byla dosažena pomocí Remote Procedure Call (RPC), což je rozhraní k službám na vzdálených zařízeních. Další výhodou je otevřenost, kdy existuje mnoho implementací protokolu NFS.[6]

Tento protokol má celkem 4 hlavní verze, přičemž specifikace druhé verze (NFSv2) byla publikována roku 1989, kde byly popsány základy NFS protokolu, jako například jeho procedury a parametry a některé z nich již byly v té době zastaralé. Další verzí byla třetí (NFSv3), která byla specifikována roku 1995, přičemž v této verzi byla přidána podpora větších souborů a zlepšení bezpečnosti v podobě kontroly přístupu na serveru. Čtvrtá verze NFS (NFSv4) byla původně specifikována roku 2000, kde mezi hlavní změny patřilo zlepšení výkonosti protokolu, dále vylepšení bezpečnosti, což zahrnovalo podporu protokolu RPCSEC_GSS, následně byla přidána možnost rozšíření protokolu. Ovšem specifikace čtvrté verze byla roku 2003 upravena, přestože definice protokolu je v částech stejná, tak jsou představeny změny jako přidání podmínek chyb a vysvětlivek pro práci s atributy majitelů a skupin.[6, 7, 8, 9]

2.3.2 SMB/CIFS

SMB protokol byl původně vyvinut společností IBM a následně byl upravován společnostmi jako Microsoft, IBM nebo Intel. Stejně jako NFS má protokol Server Message Block (SMB), také známý jako Microsoft SMB Protocol, za účel poskytnout vzdálený přístup ke sdíleným datům v síti. Kromě základní funkcionality poskytuje SMB i jiné funkce jako například tisk přes síť, notifikace o změnách souborů či adresářů nebo podpora oplock, což je zámek, který umožňuje lokální cachování dat.[10, 11]

CIFS protokol poskytuje to samé co SMB, ale samotný význam tohoto protokolu se v průběhu let změnil, kdy původně označoval verzi standardu SMB

pro Windows NT 4.0 a Windows 2000 nebo také označuje dialekt SMB, tedy označuje Windows NT LAN Manager (NTLM) dialekt protokolu SMB. Protokol CIFS je kompletně „stateful“, což znamená, že si udržuje stavy o věcech jako například bezpečnostní kontexty atd.[10, 12, 13]

2.4 Využití síťových souborových systémů

Existuje mnoho využití síťových souborových systémů, ale v rámci této podkapitoly je popsáno využití v Network Attached Storage (NAS) serverech.

NAS servery je označení zařízení, jež poskytuje přístup ke sdíleným datům v síti, primárně v lokální, což umožňuje spravovat data na jednom centralizovaném místě a lze tedy říci, že se jedná o privátní cloudové řešení. Tyto servery využívají pro sdílení dat již zmíněné protokoly, jako NFS nebo CIFS, ale také mohou sloužit jako FTP servery, a tak podporovat protokoly jako FTP a SFTP.

Z hardwarového hlediska tyto servery jsou převážně v HTPC skříních a sestávají se většinou z několika pevných disků, operační paměti a procesoru, přičemž mají RJ-45 port nebo porty pro fyzické připojení do sítě.

3 Praktická část

V rámci této kapitoly jsou obsaženy podkapitoly zabývající se praktickou částí semestrální práce, mezi které patří podkapitola, kde je specifikována virtuální síť, konfigurace hostů v dané síti a také analýza síťového provozu na NFS serveru.

3.1 Specifikace virtuální sítě

V rámci praktické části jsem vytvořil virtuální síť za pomoci cloudové platformy Microsoft Azure a v dané síti jsou dva virtuální stroje řady B, konkrétně jednotky B1s, přičemž tato řada se vyznačuje nízkými náklady a flexibilním využíváním procesorů, konkrétní specifikace hardwaru je uvedena v tabulce č. 1. Tuto velikost jsem zvolil, protože pro potřeby simulace nebylo třeba výkonnějších strojů.

Ohledně použití jednotlivých virtuálních strojů, tak stroj s privátní IP adresou 10.0.0.4 je NFS server a stroj s privátní IP adresou 10.0.0.5 je NFS klient. Samotné stroje mají i veřejné IP adresy a názvy DNS a DNS servery jsou poskytovány cloudovou platformou Azure a co se týče zabezpečení sítě, tak je nastaven přístup přes porty 80 a 22.[15]

Komponenta	Parametr
Počet procesorů	1
Řada procesorů	Intel Haswell
Frekvence procesorů	2,4 GHz
Velikost operační paměti	1 GB
Typ vnější paměti	SSD
Velikost 1 SSD disku	30 GB
Operační systém	Linux

Tabulka 1: Parametry jednoho virtuálního stroje

3.2 Analýza síťového provozu

V rámci zadání práce je úkolem analyzovat vybrané řešení a vybral jsem si řešení, kdy v jedné síti je host, jenž má roli NFS serveru a druhý host je klientem, který bude nasazovat část disku serveru. Ovšem jsem analýzu neprovedl za využití programu Wireshark, ale za pomoci jeho konzolové ekvivalenty Tshark, protože jsem ani na jediný virtuální stroj nenainstaloval grafické uživatelské rozhraní.

Příkaz pro spuštění analýzy a část výstupu příkazu je možné vidět na obrázku č. 1, přičemž je výstup filtrován pomocí IP adresy klienta, tedy 10.0.0.5 a výsledkem je komunikace mezi NFS serverem a klientem, což zahrnuje dotazy na server a odpovědi serveru pro operace na připojeném uložišti.

Pro detailnější přehled celé komunikace slouží příložený .pcap soubor s názvem Tshark-log.pcap (cesta: /Přílohy/Tshark-log.pcap), kde je uvedena veškerá komunikace na portu serveru a pro zobrazení komunikace mezi klientem a serverem je zapotřebí použít filtr „ip.addr == 10.0.0.5“. V daném souboru lze vidět například NFS operaci ACCESS, kdy se jedná o pakety číslo 2779 a 2780, tedy klient 10.0.0.5 zjišťuje povolené oprávnění k souboru a server 10.0.0.4 mu odpoví, že všechny operace kromě EXECUTE je možno provést.

4 Závěr

Předmětem této práce bylo popsat technologii síťových souborových systémů, včetně jejich protokolů a uvést příklad využití souborového systému a tyto aspekty práce jsou vypracovány v kapitole č. 2. Dalším požadavkem byla analýza komunikace mezi NFS serverem a klientem, kdy pro dosažení tohoto výsledku byl využit nástroj Tshark a cloudová platforma Azure, tato část a postup analýzy jsou uvedeny v kapitole č. 3, včetně popisu virtuálních strojů a virtuální sítě.

Co se týče dalšího rozšíření práce, tak by šlo přidat do teoretické části podkapitoly s příklady distribuovaných souborových systémů, jako Google File System, dále by bylo možné více rozvést více do detailu kapitoly o souborových systémech a jejich aspektech. Také by šlo doplnit praktickou část o analýzu provozu mezi klientem a serverem, ale za využití třeba protokolu SMB.

5 Přílohy

```
root@02:~# $ sudo tshark -i eth0 -Y "ip.addr == 10.0.0.5"
Running as user "root" and group "root". This could be dangerous.
tshark: Lua: Error during loading:
[string "/usr/share/wireshark/init.lua"]:32: dofile has been disabled due to running Wireshark as superuser. See https://wiki.wireshark.org/help_in_running_Wireshark_as_an_unprivileged_user.
Capturing on 'eth0'
227 6.974461259 10.0.0.5 → 10.0.0.4 NFS 258 V4 Call ACCESS FH: 0x91af3f8c, [Check: RD LU MD XT DL]
228 6.974584758 10.0.0.4 → 10.0.0.5 NFS 238 V4 Reply (Call In 227) ACCESS, [Access Denied: MD XT DL], [Allowed: RD LU]
229 6.975285450 10.0.0.5 → 10.0.0.4 TCP 66 952 → 2049 [ACK] Seq=193 Ack=173 Win=430 Len=0 TSval=2485791455 Tsecr=1294087943
230 6.975302050 10.0.0.5 → 10.0.0.4 NFS 274 V4 Call LOOKUP DH: 0x91af3f8c/10.0.0.4:
231 6.975352249 10.0.0.4 → 10.0.0.5 NFS 166 V4 Reply (Call In 230) LOOKUP Status: NFS4ERR_NOENT
232 6.975806044 10.0.0.5 → 10.0.0.4 NFS 250 V4 Call GETATTR FH: 0x91af3f8c
233 6.975832243 10.0.0.4 → 10.0.0.5 NFS 310 V4 Reply (Call In 232) GETATTR
234 6.977928619 10.0.0.5 → 10.0.0.4 NFS 210 V4 Call SECINFO_NO_NAME
235 6.977957319 10.0.0.4 → 10.0.0.5 NFS 250 V4 Reply (Call In 234) SECINFO_NO_NAME
236 6.981015683 10.0.0.5 → 10.0.0.4 NFS 222 V4 Call PUTROOTFH | GETATTR
237 6.981066582 10.0.0.4 → 10.0.0.5 NFS 330 V4 Reply (Call In 236) PUTROOTFH | GETATTR
238 6.981489478 10.0.0.5 → 10.0.0.4 NFS 234 V4 Call GETATTR FH: 0x62d40c52
239 6.981509278 10.0.0.4 → 10.0.0.5 NFS 234 V4 Reply (Call In 238) GETATTR
240 6.981961072 10.0.0.5 → 10.0.0.4 NFS 234 V4 Call GETATTR FH: 0x62d40c52
241 6.981987972 10.0.0.4 → 10.0.0.5 NFS 234 V4 Reply (Call In 240) GETATTR
242 6.982651064 10.0.0.5 → 10.0.0.4 NFS 234 V4 Call GETATTR FH: 0x62d40c52
243 6.982776363 10.0.0.4 → 10.0.0.5 NFS 234 V4 Reply (Call In 242) GETATTR
244 6.983569054 10.0.0.5 → 10.0.0.4 NFS 234 V4 Call GETATTR FH: 0x62d40c52
245 6.983598953 10.0.0.4 → 10.0.0.5 NFS 234 V4 Reply (Call In 244) GETATTR
246 6.984131047 10.0.0.5 → 10.0.0.4 NFS 226 V4 Call GETATTR FH: 0x62d40c52
247 6.984186647 10.0.0.4 → 10.0.0.5 NFS 186 V4 Reply (Call In 246) GETATTR
248 6.984965938 10.0.0.5 → 10.0.0.4 NFS 234 V4 Call GETATTR FH: 0x62d40c52
249 6.985060137 10.0.0.4 → 10.0.0.5 NFS 234 V4 Reply (Call In 248) GETATTR
250 6.985325933 10.0.0.5 → 10.0.0.4 NFS 230 V4 Call GETATTR FH: 0x62d40c52
251 6.985361833 10.0.0.4 → 10.0.0.5 NFS 310 V4 Reply (Call In 250) GETATTR
252 6.986546619 10.0.0.5 → 10.0.0.4 NFS 238 V4 Call ACCESS FH: 0x62d40c52, [Check: RD LU MD XT DL]
253 6.986601319 10.0.0.4 → 10.0.0.5 NFS 238 V4 Reply (Call In 252) ACCESS, [Access Denied: MD XT DL], [Allowed: RD LU]
254 6.987222511 10.0.0.5 → 10.0.0.4 NFS 246 V4 Call LOOKUP DH: 0x62d40c52/home
255 6.987256811 10.0.0.4 → 10.0.0.5 NFS 358 V4 Reply (Call In 254) LOOKUP
```

Obrázek 1: Ukázka výstupu programu Tshark

Reference

- [1] Arpaci-Dusseau, Remzi a Arpaci-Dusseau, Andrea. File System Implementation. Operating Systems: Three Easy Pieces. [online] 29. 8. 2018. [cit. 3. 11. 2018]. Dostupné z: <http://pages.cs.wisc.edu/~remzi/OSTEP/file-implementation.pdf>
- [2] Microsoft. What Is NTFS? Microsoft Docs. [online] 10. 8. 2009. [cit. 4. 11. 2018]. Dostupné z: <https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778410%28v%3dws.10%29>
- [3] ABD-EL-MALEK, Michael, et al. File system virtual appliances. ACM Transactions on Storage [online]. 2012, 8(3), 1-26 [cit. 3. 11. 2018]. DOI: 10.1145/2339118.2339120. ISSN 15533077. Dostupné z: <http://dl.acm.org/citation.cfm?doid=2339118.2339120>
- [4] Krěmář, Petr. Co umí souborový systém ZFS. root.cz. [online] 29. 8. 2006. [cit. 22. 11. 2018]. Dostupné z: <https://www.root.cz/clanky/co-umi-souborovy-system-zfs/>
- [5] Arpaci-Dusseau, Remzi a Arpaci-Dusseau, Andrea. Network File System (NFS). Operating Systems: Three Easy Pieces. [online] 29. 8. 2018. [cit. 3. 11. 2018]. Dostupné z: <http://pages.cs.wisc.edu/~remzi/OSTEP/dist-nfs.pdf>

- [6] Sun Microsystems, Inc. NFS: Network File System Protocol Specification. RFC 1094 - NFS: Network File System Protocol Specification. [online] 1989. [cit. 21. 11. 2018]. Dostupné z: <https://tools.ietf.org/html/rfc1094>
- [7] Callaghan, B., Pawlowski, B. a Staubach, P. NFS Version 3 Protocol Specification. RFC 1813 - NFS Version 3 Protocol Specification. [online] 1995. [cit. 21. 11. 2018]. Dostupné z: <https://tools.ietf.org/html/rfc1813>
- [8] Shepler, S, et al. NFS version 4 Protocol. RFC 3010 - NFS version 4 Protocol. [online] 2000. [cit. 21. 11. 2018]. Dostupné z: <https://tools.ietf.org/html/rfc3010>
- [9] Shepler, S, et al. Network File System (NFS) version 4 Protocol. RFC 3530 - Network File System (NFS) version 4 Protocol. [online] 2003. [Citace: 21. 11. 2018]. Dostupné z: <https://tools.ietf.org/html/rfc3530>
- [10] Microsoft. Microsoft SMB Protocol and CIFS Protocol Overview. Microsoft Docs. [online] 31. 5. 2018. [cit. 21. 11. 2018]. Dostupné z: <https://docs.microsoft.com/en-us/windows/desktop/fileio/microsoft-smb-protocol-and-cifs-protocol-overview>
- [11] Microsoft. Opportunistic Locks. Microsoft Docs. [online] 31. 5. 2018. [cit. 21. 11. 2018]. Dostupné z: <https://docs.microsoft.com/en-us/windows/desktop/fileio/opportunistic-locks>
- [12] Microsoft. [MS-CIFS]: Introduction. Microsoft Developer Network. [online] [cit. 22. 11. 2018]. Dostupné z: <https://msdn.microsoft.com/en-us/library/ee441901.aspx?f=255&MSPPErrors=-2147217396>
- [13] Microsoft. [MS-CIFS]: Overview. Microsoft Developer Network. [online] [cit. 22. 11. 2018]. Dostupné z: <https://msdn.microsoft.com/en-us/library/ee441722.aspx>
- [14] Ptáčník, Jiří. Kam ukládat filmy, hudbu a fotky? Na datové úložiště NAS. digilidi.cz. [online] 15. 12. 2016. [cit. 22. 11. 2018]. Dostupné z: <https://www.digilidi.cz/datove-uloziste-nas>
- [15] Sanders, Corey. Introducing B-Series, our new burstable VM size. Microsoft Azure. [online] 11. 9. 2017. [cit. 26. 10. 2018]. Dostupné z: <https://azure.microsoft.com/en-us/blog/introducing-b-series-our-new-burstable-vm-size/>