Hệ thống tệp AFS

VẼ HÌNH ẢNH MÂY LÂU TRƯỚC KHI NÓ LÀ XU HƯỚNG

Richard Brittain, 2021/08/22 Dartmouth College
Research Cyberinfrastructure.

Các từ viết tắt

bạn Địa điểm

u Máy kinh doanh quốc tế của IBM

u Học viện MIT Mass. của Công nghệ u Hệ thống tập tin u Hệ thống tập tin AFS Andrew u Hệ thống tệp mạng NFS u Hệ thống tệp công nghệ mới NTFS u Khối tin nhắn máy chủ SMB

u Hệ thống tệp Internet chung CIFS u Mạng diện rộng WAN

u Mạng cục bộ LAN

u Mạng vùng lưu trữ SAN u Kênh sợi quang FC

u Mảng dự phòng RAID của các đĩa độc lập u Máy chủ tên miền DNS

u Giao thức điều khiển truyền dẫn TCP

u Giao thức gói dữ liệu người dùng UDP u Lệnh gọi thủ tục từ xa RPC

u Dịch vụ ứng dụng u Trung tâm phân phối khóa KDC u Máy chủ cơ sở dữ liệu Bảo vệ PTS

u Cơ sở dữ liệu vị trí ổ đĩa VLDB

u Kiểm soát truy cập

u Danh sách kiểm soát truy cập ACL

u RO Chỉ đọc

u RW Đọc+Ghi

Về tôi

u Lớn lên ở Newcastle Upon Tyne, Vương

quốc Anh u Đại học Oxford (sinh viên ngành

Vật lý) u Đại học Southampton; Đại học Cornell; Trường cao đẳng Dartmouth

u Sinh viên tốt nghiệp u

Vật lý vô tuyến cực quang; thí nghiệm tên lửa âm thanh; lĩnh vực làm việc trong
Iceland, Na Uy, Alaska, Canada, Nam Cực. Hệ thống thu thập dữ liệu

bạn Lập trình viên FORTRAN

Đại học Dartmouth

u Sự nghiệp chuyển sang Unix Sysadmin và Hỗ trợ Nghiên cứu, Máy tính
Dịch vụ.

Dòng thời gian của các hệ thống tập tin mạng

u 1983 SMB1 (IBM); Dự án Andrew bắt đầu tại CMU; điện toán phân tán u 1988 Kerberos 4 (MIT); AFS (Carnegie-Mellon); AFS đến Dartmouth; Dự án Northstar u 1989 CMU sinh ra Transarc Corp để tiếp thị AFS; NFS2 (Mặt Trời)

u 1990 Richard đến Dartmouth

u 1993 Kerberos 5 (MIT); Dự án Arla (tương thích với AFS) bắt đầu ở Thụy Điển; NTFS (Microsoft) u 1994 IBM mua lại Transarc u 1995 NFS3 (Sun) u 1996 SMB1 -> CIFS (MS) u 2000 IBM phát hành mã AFS, OpenAFS 1.0; NFS4.0 (IETF) u 2006 SMB2 (MS)

u 2009 Auristor thành lập

u 2010 NFS4.1 (IETF, Panasas) u

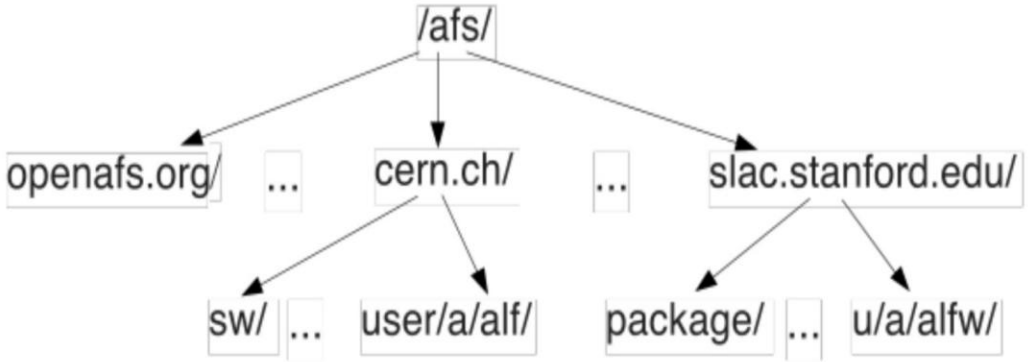
2021 OpenAFS 1.8.8 (bản phát hành hiện tại)

Các tính năng cốt lõi của AFS

- Hoàn toàn là một sản phẩm phần mềm
  - Được hỗ trợ trên nhiều loại phần cứng
- AFS sử dụng Kerberos v5 để xác thực
- Phần mềm máy khách AFS
  - Trình quản lý bộ đệm
    - Universal mount /afs/cell (\\afs\cell)
- Máy chủ siêu dữ liệu AFS
  - Tính năng sẵn sàng cao; cơ sở dữ liệu phân tán
  - Dịch vụ ủy quyền (PTS) và Vị trí dữ liệu (VLDB)
- Máy chủ tập tin
  - Nhiều máy chủ; mạng phân tán; độc lập vị trí dữ liệu (đám mây!); mạng LAN và mạng LAN

AFS như một hệ thống tập tin trên toàn thế giới

- "AFS is a distributed filesystem that enables co-operating hosts (clients and servers) to efficiently share filesystem resources across both local area and wide area networks" (AFSWiki)



- openafs.org, cern.ch etc. are AFS Cells

- Cấp tổ chức cao nhất là Tế bào
- Các ô thường được đặt tên theo tên miền DNS
- Với thông tin xác thực phù hợp, khách hàng có thể xem các ô khác
- Vì những lý do cũ, di động của Dartmouth là Northstar.dartmouth.edu
- Mọi thứ trong một ô chia sẻ (các) lĩnh vực xác thực giống nhau
- Người dùng chính là EDU, phòng nghiên cứu, một số tập đoàn lớn

AFS sử dụng tại Dartmouth

u Ban đầu được sử dụng làm thư mục chính cho nhóm máy trạm Unix trong khuôn viên trường (Project Northstar; Trường Thayer và tài trợ của IBM)

u Cài đặt và phân phối phần mềm; phát triển phần mềm ngoại khóa u Thế hệ thứ nhất

u 1 MB hạn ngạch nhà

u 300 MB trên mỗi máy chủ tệp, tổng dung lượng < 1GB

u Máy chủ web cung cấp nội dung từ AFS (Caligari, hay còn gọi là rcweb)

u Thư mục nhà dùng chung cho các máy chủ Unix nghiên cứu độc lập trước đây

u 2008 Được đặt tên là RStor

u Dung lượng lưu trữ nghiên cứu lên tới 2TB; 50GB gia đình u

Phần cứng mở rộng, RAID

u Thanh

toán u Hệ thống sao lưu được phát triển cục bộ được cải thiện (kết xuất vos sang NetBackup)

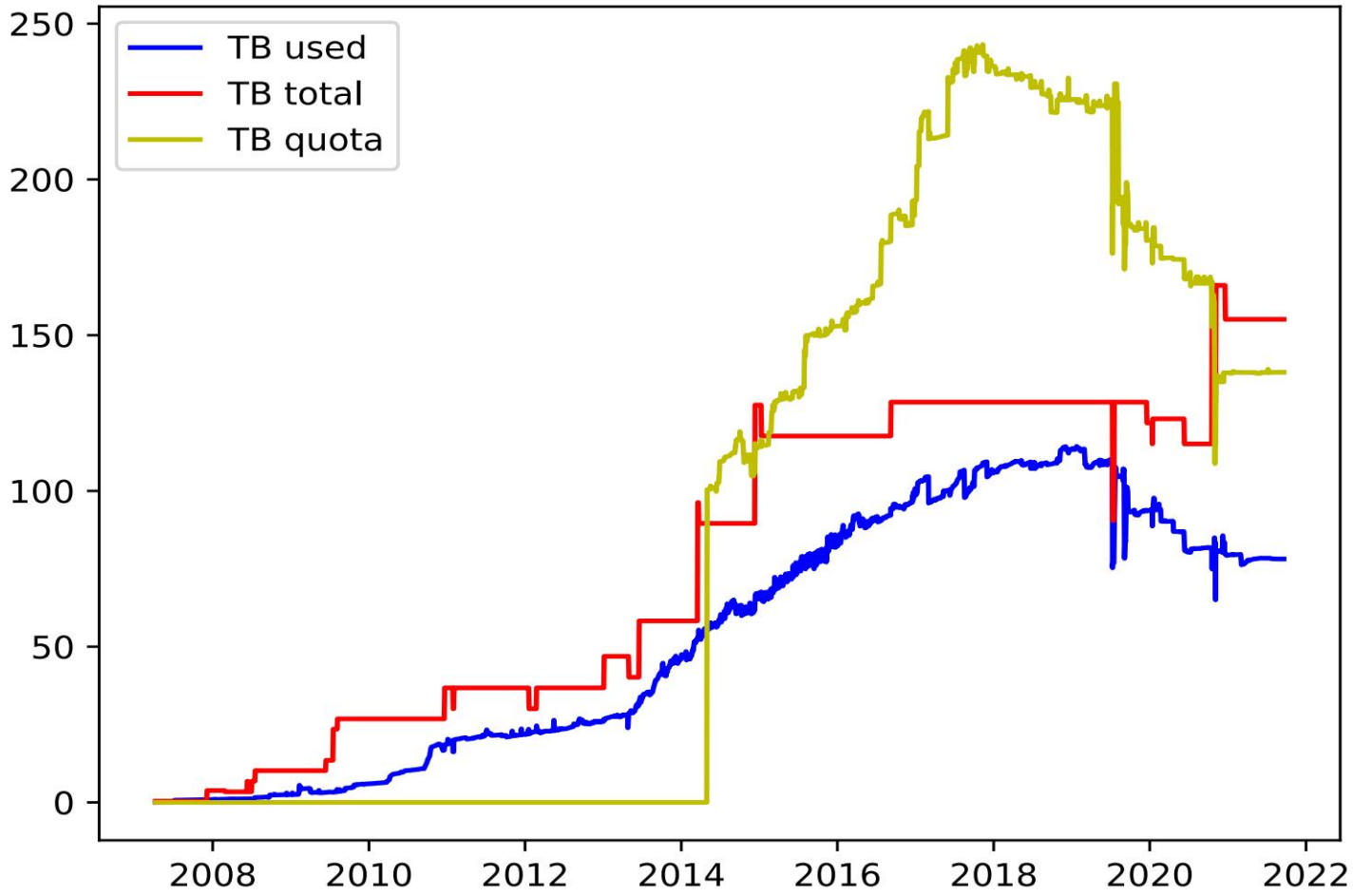
u Tin tưởng hai vùng Kerberos như nhau u Vùng

RSTOR Kerberos (tên người dùng cũ, MIT Kerberos) u Vùng KIEWIT Kerberos

(NetID, MS Active Directory)

u Bộ phận PBS điều hành một chi bộ độc lập (dbic.dartmouth.edu)

Theo thời gian: AFS/RStor tại Dartmouth



- 20 năm đầu tiên chúng tôi không lưu số liệu sử dụng
- Ít nhất 6 thế hệ phần cứng máy chủ
- Từ năm 2008, chúng tôi giữ các số liệu tóm tắt hàng ngày như một phần của quá trình sao lưu
- 2013, chúng tôi giảm giá
- Giữa năm 2014, chúng tôi đã thêm tổng thông tin hạn ngạch
- Trong năm 2017, chúng tôi bắt đầu di chuyển dữ liệu sang DartFS

Kiến trúc: tổng quan

- Máy chủ tệp được hỗ trợ trên hầu hết các biến thể của Unix và hầu hết các khối khả dụng lưu trữ (đĩa cục bộ, RAID cục bộ, FC SAN)
  - Máy chủ triển khai ổ đĩa, thư mục và tệp có siêu dữ liệu (ACL) và nội dung tệp. Không phụ thuộc vào các tính năng của hệ thống tệp hệ điều hành máy chủ. Không được mã hóa, nhưng rất tối nghĩa
    - Các phiên bản đầu tiên sử dụng các nút để tối ưu hóa
- Chi phí thấp cho mỗi khách hàng. Tỷ lệ máy khách:máy chủ cao
- Đơn vị lưu trữ là Khối lượng.
  - Thường là 1 cho mỗi người dùng; 1 cho mỗi dự án, 1 cho mỗi ứng dụng cài đặt
  - Được gắn trong cây hệ thống tập tin
- Khối lượng là đơn vị cho hạn ngạch, di chuyển máy chủ và sao lưu
  - Di chuyển trực tiếp giữa các máy chủ
- Tên di động, VolID, vnode kết hợp với một mã định danh duy nhất trên toàn cầu của một tệp
- Khối lượng được sao chép, nhiều RO, một RW; đồng bộ hóa theo yêu cầu

Kiến trúc: khách hàng

u Trình quản lý bộ đệm máy khách (mô-đun hạt nhân) trình bày một hệ thống tệp được gắn với hầu hết các ngữ nghĩa POSIX

u Sử dụng Kerberos để xác thực người dùng và máy chủ tệp

u Có thể tận dụng nhiều vùng Kerberos

u Sử dụng DNS để khám phá các máy chủ siêu dữ liệu (KDC, PTS, VLDB) u Sử dụng VLDB để khám phá vị trí của tệp.

u Lưu trữ các khối tệp trên đĩa cục bộ

u Khách hàng trạng thái

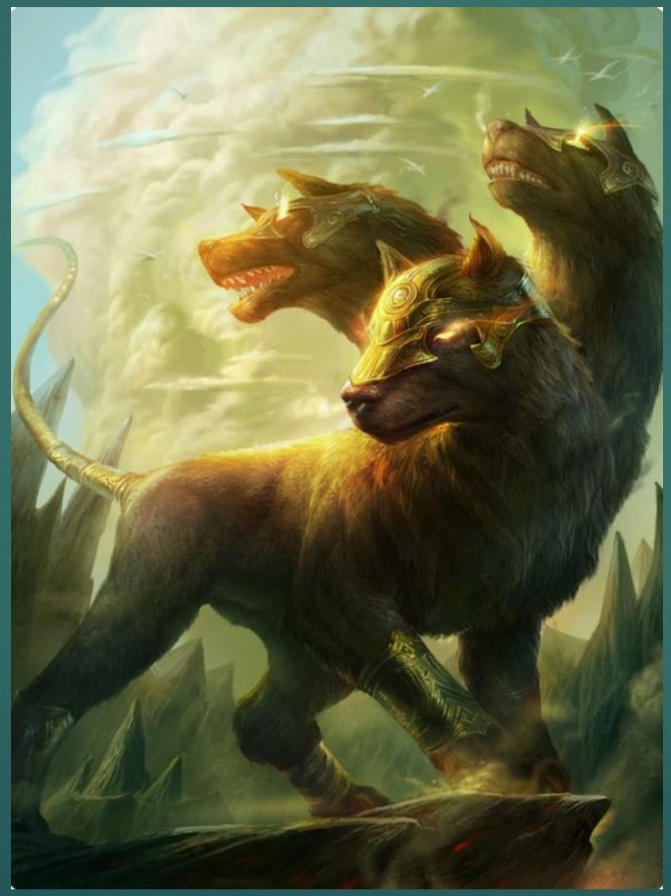
u Sử dụng gọi lại để duy trì tính nhất quán (yếu)

u Ghi vào bộ đệm cục bộ, xóa vào máy chủ khi đóng () hoặc khi bộ đệm đầy u Chế độ xem lưu trữ giống hệt nhau từ mỗi máy khách u Máy khách chọn giữa các ổ đĩa được sao chép khi khả dụng u Tất cả lưu lượng truy cập đều do máy khách khởi tạo ngoại trừ các cuộc gọi lại u Root cục bộ KHÔNG có quyền truy cập thành mã thông báo (nói chung), vì vậy không có quyền truy cập vào trang chủ AFS thư mục

Kiến trúc: máy chủ

- Có thể thực hiện thay đổi cấu hình từ bất kỳ máy khách nào
  - Hiếm khi cần đăng nhập trực tiếp vào máy chủ
- Các tập có thể được di chuyển từ máy chủ này sang máy chủ khác trong khi hoạt động
  - Cân bằng lại lưu lượng truy cập
  - Thêm máy chủ mới
  - Xả máy chủ để bảo trì
- Máy chủ tệp không thể truy cập dữ liệu của chính chúng, trừ khi máy khách được cài đặt
- Máy chủ siêu dữ liệu được định cấu hình là cơ sở dữ liệu sao chép có tính sẵn sàng cao
  - Triển khai cơ sở dữ liệu PTS, ánh xạ danh tính Kerberos thành số UID, và thành viên nhóm
  - Triển khai cơ sở dữ liệu VLDB, ánh xạ các điểm gắn kết trong hệ thống tệp tới máy chủ tập tin
  - 3 máy ảo nhỏ (không phải tất cả trên cùng một máy chủ!)
- RPC/UDP, Giao thức tùy chỉnh (UBIK)

Xác thực: Kerberos



Tổng quan về Kerberos:

u Được mọi người sử dụng hàng ngày với xác thực Active Directory

u Xác thực AFS tận dụng rõ ràng các tính năng của Kerberos

u Kerberos cung cấp xác thực; không ủy quyền u MS Active

Directory làm mờ các dòng đó. Với AFS, kiểm soát truy cập máy chủ tệp và máy chủ PTS cung cấp ủy quyền

u Xác thực lẫn nhau của các bên đáng tin cậy trong môi trường không đáng tin

cậy u Xác thực bạn với tư cách là người dùng và cũng là dịch vụ bạn kết

nối với u Đăng nhập một lần: xác thực với nhiều dịch vụ sau lần đầu tiên mua lại chứng chỉ.

u Kerberos v5 sử dụng mã hóa khóa đối xứng u Mã

hóa khóa công khai có thể được sử dụng để xác thực ban đầu u

Tạo và phân phối khóa phiên an toàn

TGT và vé dịch vụ

u Xác thực ban đầu tạo Vé cấp vé (TGT). So sánh nó với hộ chiếu; thời gian giới hạn; tái tạo; chứng minh danh tính cho người khác mà không cần thêm tài liệu nào u Không bao giờ có mật khẩu, thậm chí mã hóa u TGT được sử dụng để lấy Vé dịch vụ cho một ứng dụng cụ thể. Cái này

chứa khóa máy chủ ứng dụng được mã hóa

u Nếu TGT là hộ chiếu, Phiếu dịch vụ là tem thị thực u

Phiếu dịch vụ được xuất trình tới Máy chủ ứng dụng, máy chủ này xác thực khóa mã hóa kèm theo và xác thực ứng dụng khách

u AFS sử dụng một dạng vé dịch vụ đặc biệt (Mã thông báo) được đính kèm với mọi hoạt động của hệ thống tập tin

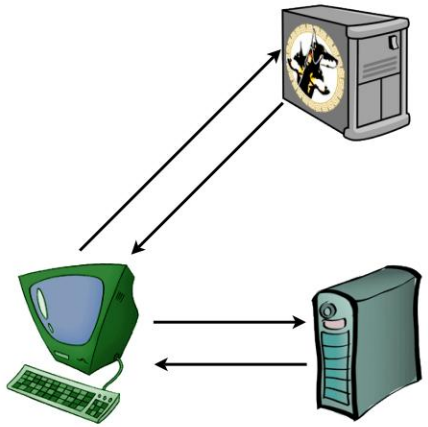
u Khi đăng nhập để nghiên cứu máy chủ Linux bằng NetID, mã thông báo AFS là vé Active Directory được

tạo tự động là 10 giờ. trọn đời, tái tạo lên đến 30 ngày

Xác thực cho một dịch vụ

Xác thực cho một dịch vụ

- Khách hàng yêu cầu phiếu dịch vụ từ KDC
- KDC trả lại vé dịch vụ và khóa phiên, được mã hóa bằng mật khẩu của người dùng
- Khách hàng gửi vé dịch vụ và trình xác thực đến ứng dụng
- Ứng dụng trả về dấu thời gian của trình xác thực, được mã hóa bằng khóa phiên
  - do đó chứng minh rằng nó biết khóa phiên và đọc trình xác thực



Danh sách kiểm soát truy cập (ACL)

u ACL NFS4 và SMB bị ảnh hưởng nhiều bởi thiết kế AFS ACL

u Mô hình cấp phép trong DartFS cũng tương tự nhưng phức tạp hơn

u 7 bit quyền được coi là đủ (NFS4/SMB có 14) u AFS ACL

chỉ trên các thư mục - không phải trên mỗi tệp u Các tệp

luôn kế thừa các quyền của thư mục mẹ u Tạo một thư mục

ban đầu kế thừa các quyền của thư mục mẹ u Các quyền áp dụng cho các

cá nhân hoặc nhóm

bit quyền

Cờ kiểm soát truy cập

bạn đang đọc nội dung tập tin

u l tra cứu (đọc nội dung thư mục, duyệt thư mục) u w ghi nội dung tệp (và nối thêm) u tôi chèn vào thư mục (tạo tệp) u d xóa khỏi thư mục (xóa tệp)

bạn k khóa tập tin

bạn là quản trị viên (thay đổi ACL, ngầm định cho chủ sở hữu)

u Các bit POSIX (ls -l) không chính xác, nhưng hiếm khi xảy ra sự cố

u chmod +x hoạt động để thiết lập bit thực thi

u Quyền hạn có thể

Các nhóm

- Nhóm hệ thống
  - Hệ thống: bất kỳ người dùng nào (công khai)
  - Hệ thống:authuser (như người dùng tên miền)
  - Hệ thống: quản trị viên (như root)
- Không gian tên nhóm mỗi người dùng
  - tên người dùng của bạn : tên nhóm
  - Người dùng quản lý các nhóm của riêng họ
- Các nhóm có thể được lồng vào nhau

P

u PAG (Nhóm xác thực quy trình)

u Thông tin đăng nhập riêng biệt cho các nhóm quy trình trên cùng một máy tính

u Một mã thông báo trên mỗi ô trên

mỗi PAG u Nếu không có PAG, trình quản lý bộ đệm sẽ sử dụng UID cục bộ để nhận
dạng, do đó, tài khoản gốc có thể chuyển đổi UID và đánh cắp mã thông báo

u MacOS không có PAG

u Windows có 1 PAG cho mỗi phiên đăng nhập u

Linux đang cố gắng hết sức để không thể có PAG cho bảng điều khiển máy tính để bàn

Sự cố với AFS

- Giới hạn âm lượng 2TB (hạn ngạch)
- Hiệu suất không thể bão hòa các liên kết 10Gb.
  - Mảng đĩa và mạng hiện nhanh hơn mạng và phần mềm máy chủ giao thức
- Khả năng song song hóa kém của các quy trình trong một máy chủ tệp nhất định
- Máy khách để bàn (MacOS, Windows) ngày càng khó xây dựng
  - Các tính năng bảo mật trên máy tính để bàn
  - Không thể làm việc với hỗ trợ thương mại để xây dựng và phân phối trình cài đặt đã ký (Auristor, Sine Nomine)
- Thiếu các công cụ sao lưu gốc. Bản gốc sao lưu gốc là một kết xuất âm lượng có thể được gửi tới NetBackup, v.v.
- Mã hóa tệp chậm (không tận dụng hệ điều hành hoặc phần cứng hiện đại)
- Các công cụ quản trị hơi rắc rối
  - Rất nhiều công cụ được đóng góp để giúp mọi việc trở nên dễ dàng hơn

Tương lai của AFS

- OpenAFS vẫn tốt, nhưng hiện tại chủ yếu hướng đến Linux
- Auristor. Viết lại thương mại, tương thích ngược, nhiều cái mới
  các tính năng và loại bỏ hầu hết các hạn chế
- Mô-đun hạt nhân Red Hat (máy khách tối thiểu)
- Máy khách MacOS và Windows từ Auristor

Tình trạng hiện tại của Northstar Cell