Systèmes de fichiers réseau
Stockage objet

Module Admin Sys Réseau – S26E02

Philippe Latu / Université de Toulouse
inetdoc.net

Le système de fichiers réseau fournit une abstraction aux systèmes.

Le stockage objet fournit une abstraction aux applications.

Le plan

- Forces et Faiblesses
- Topologie d’un réseau de stockage
- Système de fichiers virtuel
- Appels de procédures RPC
- Système de fichiers NFS
- Système de fichiers SMB
- Stockage Objet

Forces / Faiblesses
des systèmes de fichiers réseau

Les forces des systèmes de fichiers réseau

- Partage « 1 producteur vers n consommateurs »
  - Stockage à grande échelle
    - Nombreux clients hétérogènes
  - Point de ressource unique → Le **serveur NAS**
    - Limitation du nombre de copies / Moins d'incohérences
    - Instantanés / Sauvegardes faciles à gérer
- Gestion des verrous côté serveur
  - N conteneurs d'applications pour 1 même stockage persistant

Les faiblesses des systèmes de fichiers réseau

- Performances
  - Coût CPU élevé côté serveur
  - Sensibilité aux ruptures de communication
  - Mobilité « limitée » côté client
  - Sensibilité à la latence et à la gigue réseau
    - Éviter les applications transactionnelles
- Sécurité
  - Gestion des autorisations d’accès depuis les clients

Topologie d’un réseau de stockage

Topologie type : premier plan / arrière-plan

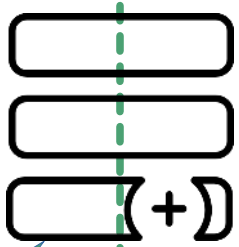
frontend | *backend*

Relations au réseau de stockage

Hôte ↔ Hôte

Client ↔ Serveur

Application ↔ Système de fichiers

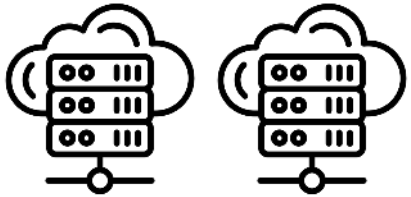


Relations : SAN ou VFS noyau

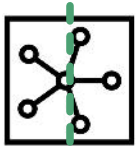
Hôte ↔ stockage

Système de fichiers ↔ périphérique

Application ↔ périphérique



Service de stockage NAS



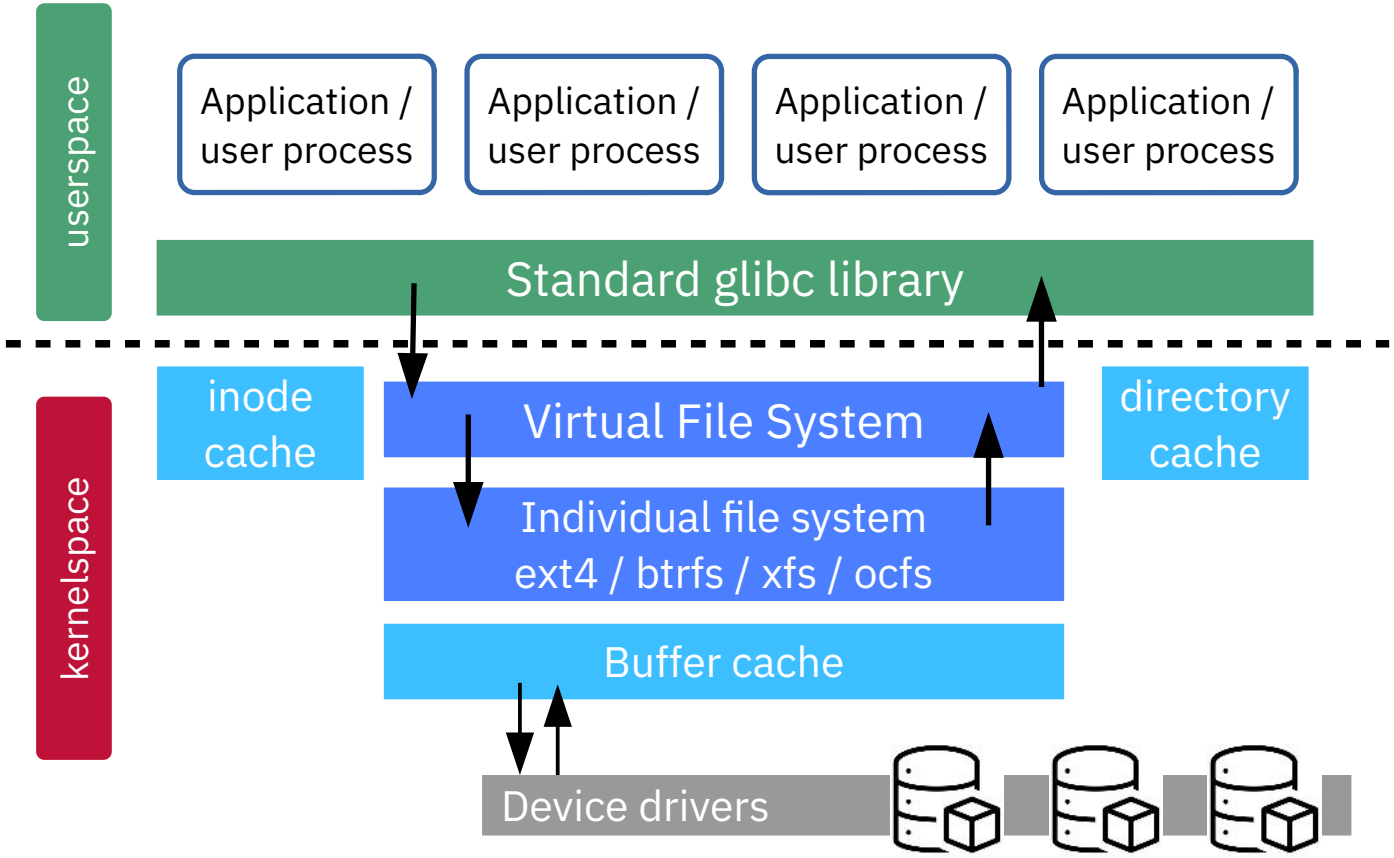
Système de fichiers virtuel

Pourquoi virtualiser le système de fichiers à l’échelle d’un système ?

Systèmes de fichiers virtuels

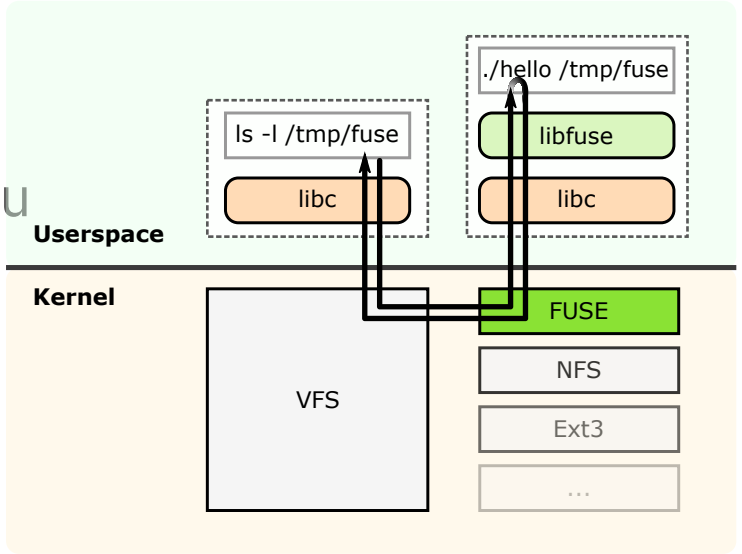
- Définition → Virtual File System (VFS)
  - Service du noyau → interface applications ↔ périphériques
  - Bibliothèque standard → API à l'échelle d'un système unique
- Objectifs
  - Accès transparent pour les applications
  - Contrôle d'accès uniforme → permissions / contrôle d'accès
  - Schéma de nommage cohérent entre serveurs et clients
  - Performances d'accès uniformes

Définition VFS noyau Linux



Définition VFS espace utilisateur → FUSE

- Portabilité
  - Entre systèmes : Linux/MacOS/*BSD
  - API : plusieurs langages et gestion du contrôle d'accès
  - Métadonnées système uniquement
- Objectifs
  - Performances élevées
  - Développements et évolutions rapides



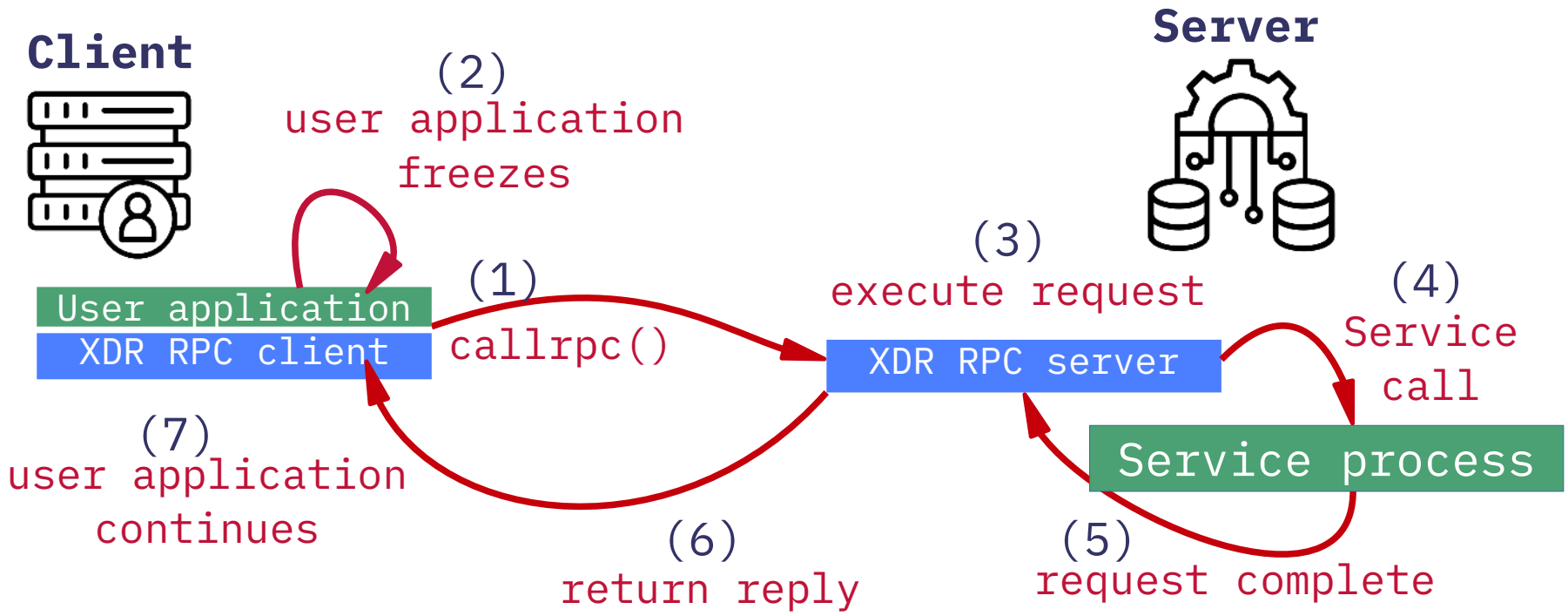
Source Wikipedia

Appels de procédures à distance

Remote procedure calls (RPCs) are a fundamental building block for constructing distributed systems. By abstracting the complexities of network communication, RPC enables developers to concentrate on their application logic rather than on the intricacies of interprocess or intermachine messaging.

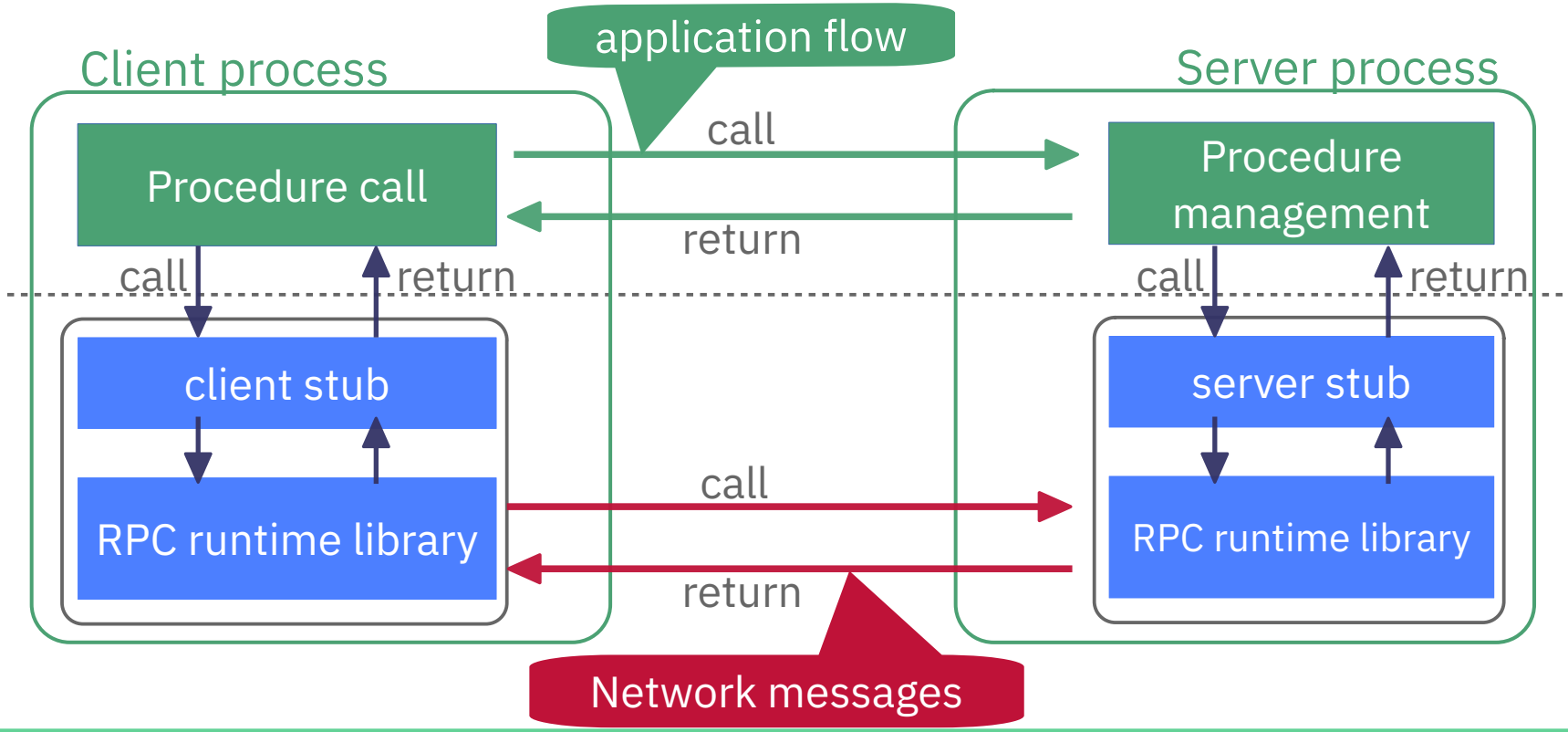
Remote Procedure Call (RPC) 1/2

Les étapes d'un appel de procédure



Remote Procedure Call (RPC) 2/2

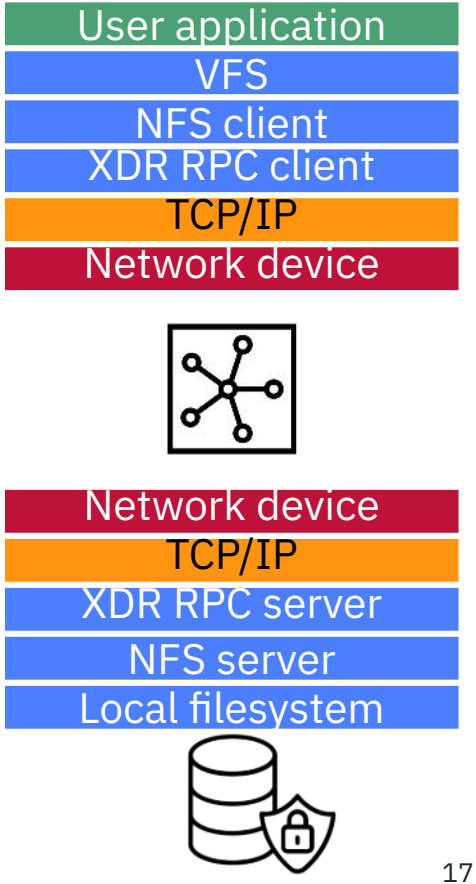
Modélisation des flux



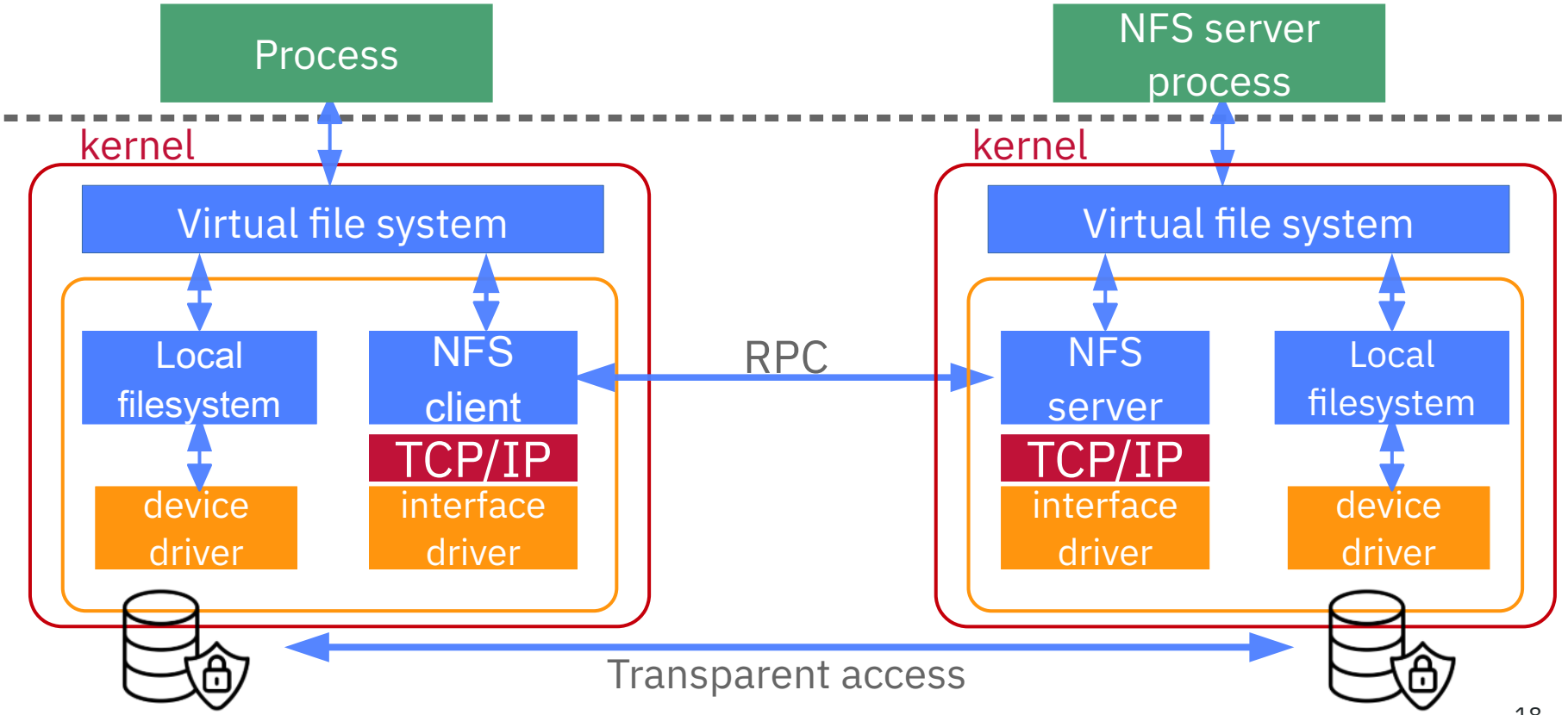
Système de fichiers réseau NFS

Network File System → NFS

- NFSv2 1983
  - Protocole UDP et réseaux locaux
  - Performances médiocres en écriture
- NFSv3 1995
  - Exportation de systèmes de fichiers POSIX 64 bits
  - Protocoles UDP et TCP toujours avec multiplexage de ports
  - Performances améliorées en écriture
- NFSv4.0 2003 – RFC 3530
  - Protocole avec état (stateful) → suppression du montage/verrouillage séparés
  - Communications sur un port unique tcp/2049 → filtrage simplifié
  - Appels de procédures groupés → compound RPC
  - Chiffrement des flux via RPCSEC_GSS / Kerberos
- NFSv4.2 2016
  - Copie de fichiers côté serveur (server-side copy)
  - Fichiers creux (sparse files) et réservation d'espace
  - Étiquetage de sécurité (Labeled NFS / contrôle d'accès obligatoire)



Network File System → NFS



Network File System → NFS

Pile de protocoles et mécanismes de sécurisation

	Historique (Kerberos/GSS-API)	Actuel (RPC-with-TLS)
Version de protocole	NFSv4 RFC 3530	NFSv4.x (v3 à v4.2)
Authentification	Kerberos v5 RFC 4120	Certificats x.509 (TLS 1.3) mTLS optionnel
Sécurité RPC	RPC_GSS RFC 5403 + SPKM/LIPKEY RFC 2847	RPC-with-TLS RFC 9289 (option xprtsec=tls/mtls)
Session	RPC RFC 5531 + XDR RFC 4506	RPC RFC 5531 + XDR RFC 4506 (chiffrés via kTLS)
Transport	TCP port 2049	TCP port 2049

Network File System → NFS

Fonctions principales

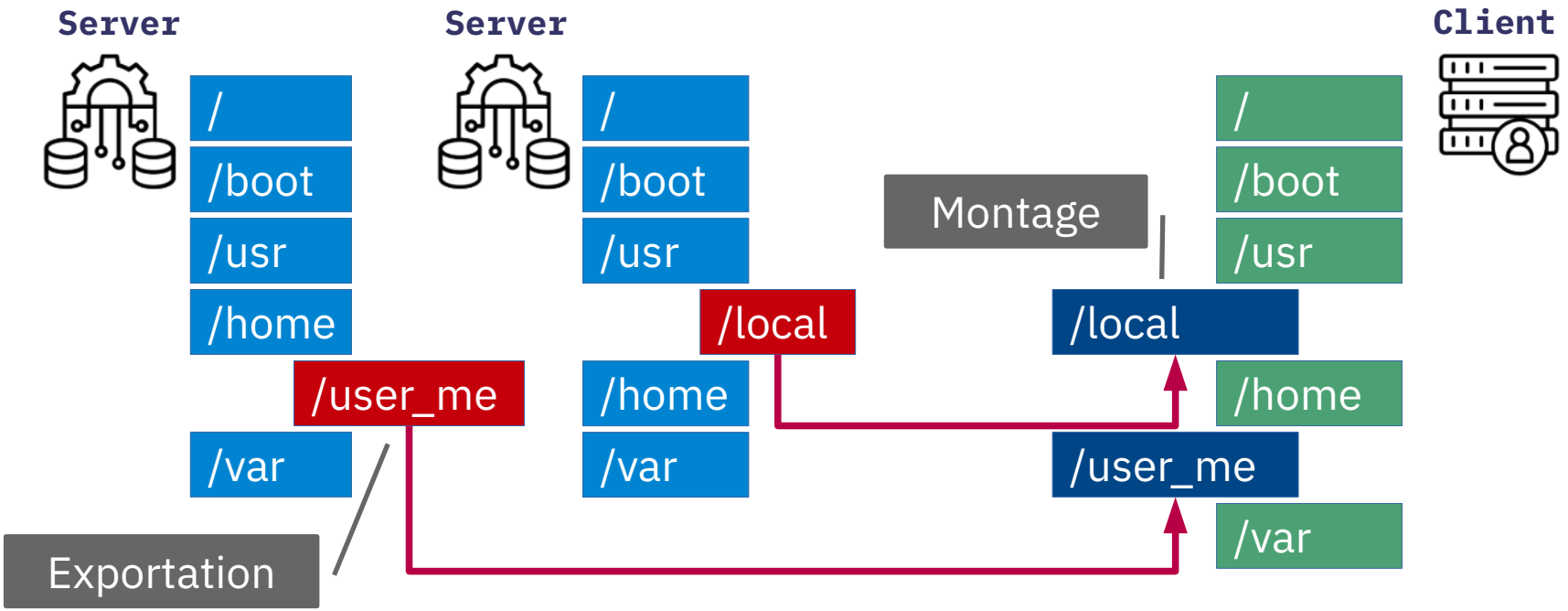
- Système de fichiers distribué
  - Accès et Nommage identiques entre serveurs et clients
- Modèle client/serveur
  - Serveur → répertoires locaux accessibles aux clients
  - Clients → montage des répertoires distants
- Hiérarchique par nature → chaînes de répertoires et fichiers

Usages

- Partage de répertoires : utilisateurs, données et applications qui sont exécutées localement
- Clouds publics et stockage hybride → version NFS prise en charge
  - GCP NetApp Volumes → NFSv4.2
  - AWS Elastic File System (EFS) → NFSv4.1
  - Azure NetApp Files → NFSv4.1

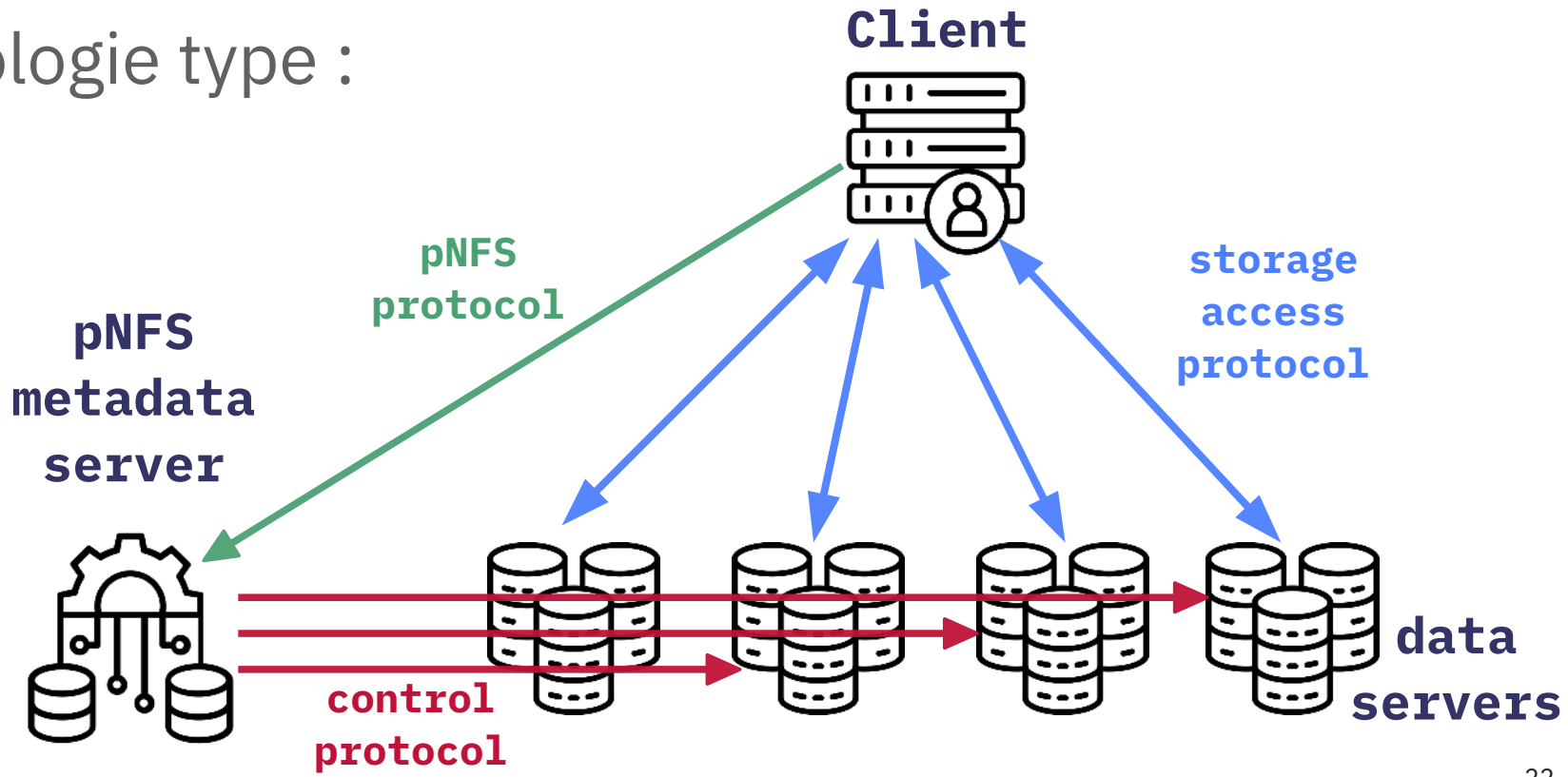
Network File System → NFS

Nommage et arborescence Unix :



Parallel Network File System → pNFS

Topologie type :



Parallel Network File System → pNFS

- Transaction type *parallel* NFS
  - Client → demande la lecture ou l'écriture d'un fichier
  - Serveur pNFS
    → autorise l'accès au fichier
    → envoie le plan de répartition du fichier au client
  - Client → lit ou écrit directement sur tous les serveurs
- Performances nettement améliorées
  - Plus de relation strictement point-à-point avec le serveur
  - Amélioration des accès aux fichiers de grande taille
  - Répartition de charge entre clients et serveurs
- Espace de nommage unique préservé

Système de fichiers réseau SMB

Server Message Block → SMB

- SMB 3.0
  - Windows Server 2012
  - Optimisé pour les applications serveur
- SMB 3.1.1
  - Windows Server 2016/2019/2022
  - Chiffrement AES-128/AES-256 (GCM, CCM, GMAC)
  - Négociation de dialecte sécurisée
- Fonctions SMB Windows Server 2025
  - Signature SMB activée par défaut
  - Chiffrement SMB forcé par défaut
  - SMB over QUIC

Server Message Block

Pile de protocoles

	Après Windows 2000 (avant patchs récents)	Après 2024 (actuel)
Version de protocole	SMB 2.x / 3.x	SMB 3.1.1 (fonctionnalités avancées)
Session	Raw access	Raw access / Audits améliorés / Multichannel
Transport	TCP 445	TCP 445 + ports alternatifs + QUIC (UDP 443)
Sécurité	Signature, début du chiffrement (SMB3)	AES-GCM/CCM / signature forte / audit QUIC
Parefeu	Règles autorisant TCP 445 / 137-139 si SMB1 autorisé	Plus de 137-139, stricte, liste de ports définis

Usages du chiffrement

Usages du chiffrement

Type de chiffrement	Objectif	Systèmes de fichiers NFS et/ou SMB	Exemples de mise en œuvre
Données en transit	Protéger les échanges réseau contre l'interception	SMB 3.x / NFSv4.x + Kerberos krb5p ou RPC-with-TLS (RFC 9289)	SMB 3.1.1 (AES-GCM/CCM) / NFSv4.2 avec Kerberos krb5p ou RPC-with-TLS (xprtsec=tls, sans Kerberos)
Données au repos	Sécuriser les données stockées	NFS & SMB sur solutions modernes (cloud, appliances)	Azure Files, NetApp ONTAP, Windows BitLocker
Bout en bout du serveur au client	Assurer la confidentialité et l'intégrité de bout en bout	Depuis SMB 3.1.1 / NFSv4.x avec RPC-with-TLS (RFC 9289)	SMB 3.1.1 natif + négociation automatique d'AES / NFSv4.x + RPC-with-TLS (mTLS, certificats x.509)

Stockage en mode Objet

Stockage en mode Objet → principes

- Communications directes entre application et stockage
  - Trouver/Chercher des données à partir d'expressions rationnelles
  - Stockage cloud = base de données
- Distinction données - métadonnées
  - Requêtes complexes → Big Data
  - Exemple : recherche de données similaires à l'aide de la classification des métadonnées

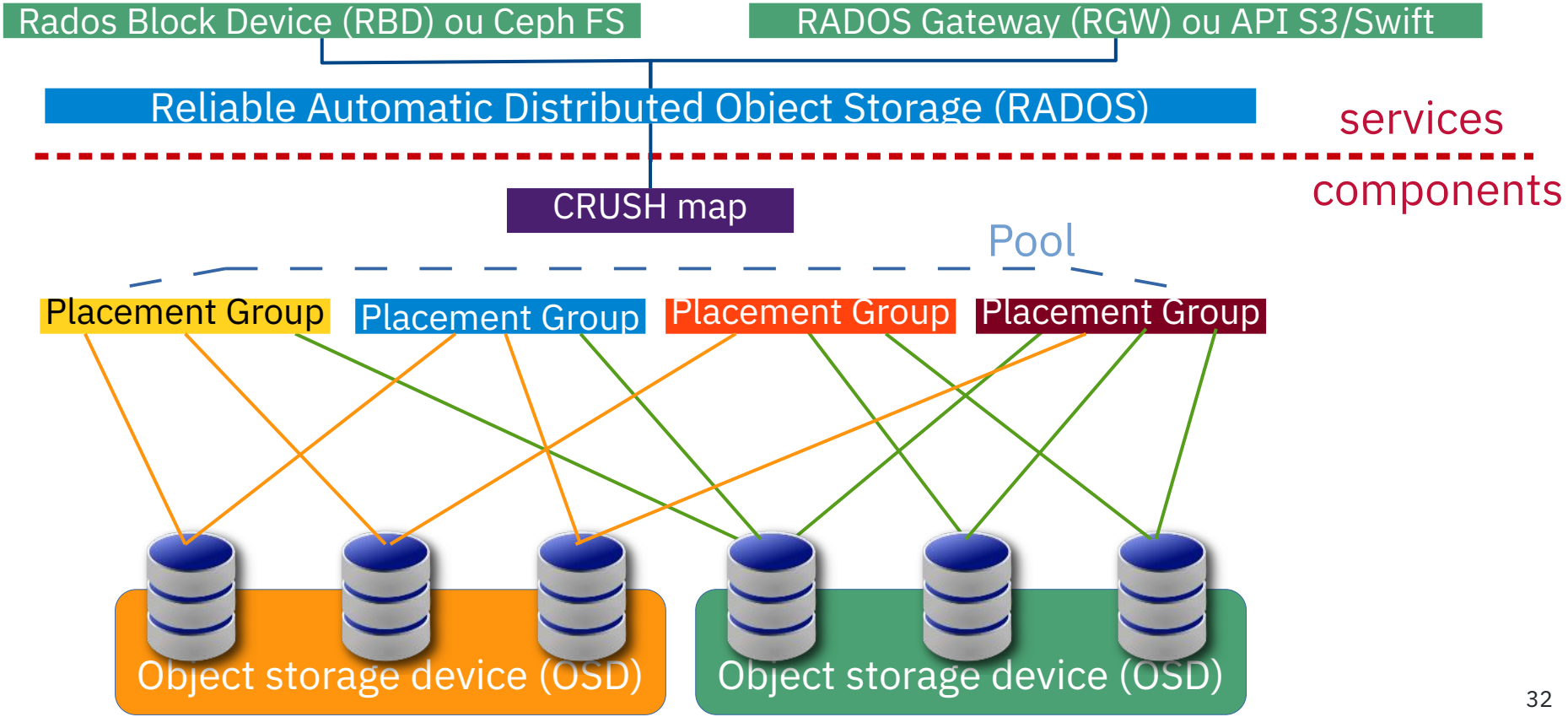
Metadata

Data

Stockage en mode Objet → accès aux objets

- Un serveur stocke un objet sur un seul nœud
  - Algorithmes de sélection basés sur la topologie
- Politique de stockage
  - Algorithmes basés sur l'occupation des nœuds, les performances et les métadonnées système
- Schémas de nommage cohérents
  - Accès global uniforme
- Réplication
  - Entre nœuds et/ou sites en fonction des accès

Stockage en mode Objet → Ceph



Stockage en mode Objet → Ceph

Composant / Service	Rôle	Description / Usage
OSD (Object Storage Device)	Volume de stockage	DAS / SAN /NAS Nombre d'OSDs → réplication + tolérance aux pannes
Pool	Groupe logique	Groupe de *Placements Groups* Stratégie de performance (*tiering*)
CRUSH map	Distribution des objets	Cartes de distribution des objets vers les OSDs Une cartographie par pool
RADOS	Stockage partagé	Transformation données ↔ objets Stockage partagé performant
RBD (RADOS Block Device)	Service bloc	Découpage en bandes (*stripes*) Images de conteneurs ou de Vms (Incus / Proxmox)
RGW (RADOS Gateway)	Service objet (API s3 / Swift)	Passerelle REST compatible S3/Swift Accès direct depuis les applications (buckets, objets, *upload multipart*)

Pour conclure

On reprend...

Systèmes de fichiers réseau et protocoles (NFS, SMB)

- Partage de données à grande échelle avec des clients hétérogènes
  - Solutions NAS populaires
  - Réduction du nombre de copies et sauvegardes faciles
- Défis de performances
  - Sensibilité réseau et mobilité limitée
  - Enjeux spécifiques de sécurité et d'accès côté client
- Topologies associant backend (SAN/VFS noyau) et frontend (NAS)
  - Architecture client/serveur avec montage distant des répertoires
  - Accès unifiés via VFS (kernel ou FUSE) pour obtenir des performances uniformes
- Protocoles
  - NFSv4.2 pour Unix/Linux
  - SMB3.1.1 pour Windows
  - Évolutions orientées sécurité → chiffrement, authentification forte
  - Évolutions orientées performances → parallélisme pour pNFS et RDMA + multicanal pour SMB

Stockage objet et enjeux de sécurité

- Stockage objet (Ceph)
  - Séparation entre données et métadonnées
  - Indexation/Recherche avancée → gestion de gros volumes et usages Big Data ou cloud
- Accès direct application-stockage
  - Cohérence de nommage
  - Réplication entre sites et le placement intelligent (CRUSH dans Ceph)
  - Optimisation de l'efficacité, de la résilience et de l'intégrité des données
- Sécurité des systèmes de fichiers
  - Chiffrement en transit → NFSv4.2+Kerberos/TLS et SMB 3.x (AES-GCM/CCM)
  - Protection au repos → solutions cloud, BitLocker et confidentialité de bout en bout
- Intégration dans le cloud
  - Flexibilité accrue et nouvelles stratégies d'accès
  - Sauvegardes automatisées
  - Environnements distribués.