



CONCEVOIR UN SERVEUR LOCAL MULTIUTILISATEUR

Guide détaillé du matériel, de l'architecture et de l'installation
pour plus de 100 utilisateurs

Albertho Lapierre
Créateur et formateur

Architecture Windows Server RDS • Sécurité • Licences • Sauvegardes • Déploiement

Note au lecteur

Ce guide présente une architecture de référence pour un centre de formation, une école ou une organisation comptant plus de 100 utilisateurs simultanés. Les applications sont installées et exécutées sur des serveurs locaux, tandis que les utilisateurs s'y connectent depuis des ordinateurs du réseau.

Les capacités proposées sont des points de départ. Le dimensionnement final dépend des logiciels, du nombre d'onglets de navigateur, de la vidéo, de l'impression, des périphériques et des habitudes réelles. Un essai de charge est donc obligatoire avant l'ouverture générale.

Décision centrale

Pour ce besoin, la solution recommandée est une ferme Windows Server Remote Desktop Services, et non un unique serveur partagé. Cette séparation réduit les interruptions, répartit la charge et facilite l'évolution.

La compatibilité des applications, les prix et les droits de licence doivent être confirmés auprès des éditeurs et d'un revendeur agréé avant tout achat. Ce document ne remplace pas un devis technique ni un avis juridique sur les licences.

Sommaire

Note au lecteur	1
1. Comprendre le système	3
2. Architecture générale	4
3. Dimensionnement matériel	5
4. Comptes, profils et données	6
5. Applications et expérience utilisateur	7
6. Réseau local	8
7. Sécurité	9
8. Licences	10
9. Sauvegarde et continuité	11
10. Déploiement par étapes	12
11. Exploitation quotidienne	13
12. Budget et achats	14
13. Liste de contrôle finale	14
14. Nomenclature matérielle détaillée	15
15. Installation physique et réseau	17
16. Installation des hôtes et du domaine	18
17. Installation détaillée de RDS et des applications	20
18. Tests, ouverture et maintenance	21
Conclusion	22
Références officielles	22

1. Comprendre le système

Chaque utilisateur voit son propre environnement, mais le traitement principal est effectué dans la salle des serveurs.

1.1 Le principe

L'utilisateur ouvre un poste du centre, saisit son identifiant et lance une connexion distante. Le serveur vérifie son compte, crée une session isolée, charge son profil et lui présente un bureau ou des applications. Le clavier, la souris et l'affichage circulent sur le réseau; les logiciels et les fichiers restent centralisés.

- 1 Ouvrir le client de connexion sur un ordinateur autorisé.
- 2 S'authentifier avec un compte personnel.
- 3 Recevoir automatiquement une session sur un serveur disponible.
- 4 Utiliser Office, le navigateur et les logiciels publiés.
- 5 Enregistrer les documents dans les emplacements centralisés puis fermer la session.

1.2 RDS, RemoteApp et VDI

Approche	Description	Usage conseillé
RDS - bureau partagé	Plusieurs utilisateurs disposent chacun d'une session sur le même système Windows Server.	Choix principal pour Office, Web, gestion et formation classique.
RemoteApp	Une application distante apparaît presque comme une application locale.	Comptabilité, gestion ou application précise sans bureau complet.
VDI	Chaque personne obtient une machine virtuelle de bureau distincte.	Logiciels incompatibles avec RDS, personnalisation forte ou isolation supérieure.

Recommandation

Utiliser RDS et RemoteApp pour la majorité des utilisateurs. Réserver la VDI à une minorité dont les logiciels ne peuvent pas fonctionner dans une session partagée.

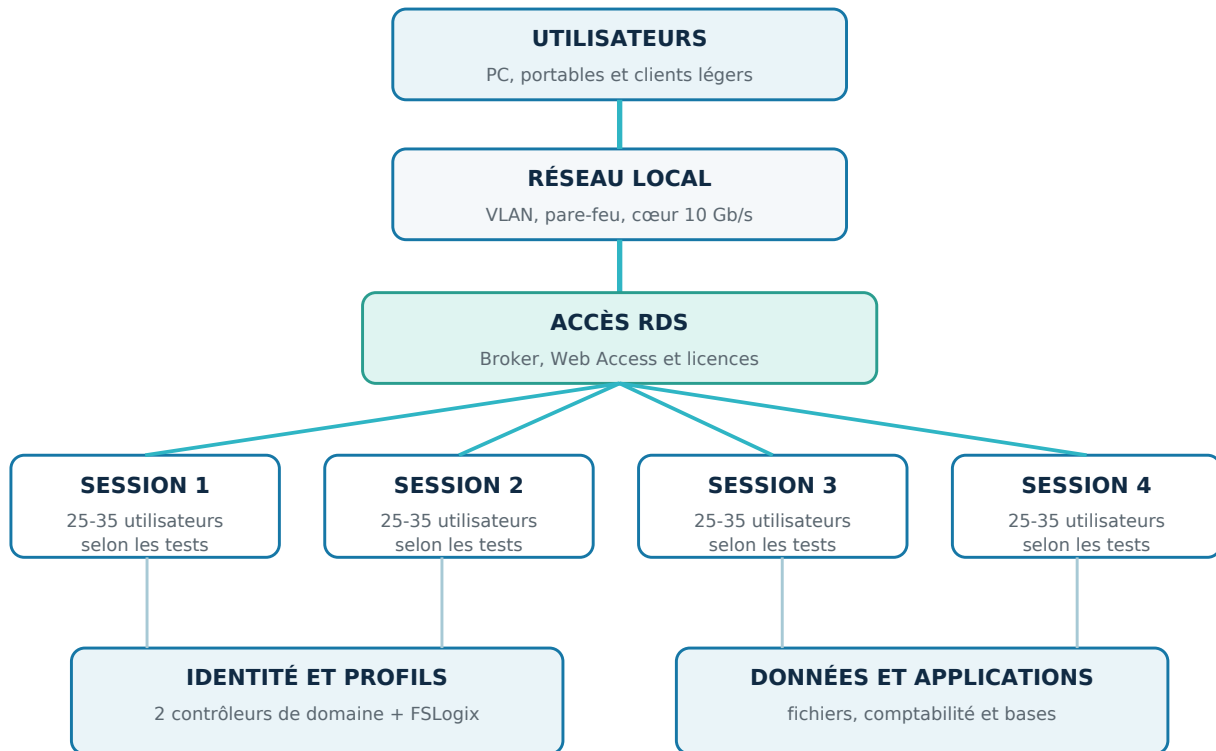
1.3 Ce que la centralisation apporte

- Installation et mise à jour des applications à un nombre limité d'endroits.
- Comptes, permissions et règles de sécurité administrés de façon cohérente.
- Accès au même profil depuis différents ordinateurs du réseau.
- Données mieux contrôlées et sauvegardées.
- Postes clients moins puissants et plus faciles à remplacer.

La centralisation concentre aussi le risque: une panne de stockage, d'électricité ou de réseau peut toucher tout le monde. C'est pourquoi la redondance, les sauvegardes et la surveillance ne sont pas facultatives.

2. Architecture générale

Pour 100 à 150 sessions, la disponibilité provient de plusieurs serveurs qui se partagent les rôles.



Architecture logique recommandée pour 100 à 150 utilisateurs simultanés

2.1 Les rôles principaux

Rôle	Mission
Active Directory et DNS	Authentifier les personnes et ordinateurs, appliquer les stratégies et résoudre les noms internes.
RD Connection Broker	Diriger les nouvelles connexions, équilibrer la charge et reconnecter un utilisateur à sa session existante.
RD Session Host	Exécuter les bureaux et applications des utilisateurs.
RD Web Access / RemoteApp	Présenter les ressources autorisées aux utilisateurs.
RD Licensing	Distribuer et suivre les licences d'accès RDS.
RD Gateway	Sécuriser un éventuel accès extérieur par HTTPS; inutile si tout accès reste strictement local.
Fichiers et profils	Conserver documents, dossiers partagés et profils FSLogix.
Base de données	Héberger séparément la comptabilité et les applications transactionnelles.

2.2 Pourquoi un seul serveur est insuffisant

- Une panne matérielle interromprait toutes les classes et tous les services.
- La maintenance imposerait une fermeture complète.
- Les charges Office, Web et base de données se concurrenceraient.
- Une infection ou un incident de stockage aurait un rayon d'impact maximal.
- L'ajout de capacité serait plus difficile.

Principe N+1

La plateforme doit pouvoir absorber la panne ou la maintenance d'un hôte sans perdre le service essentiel. La capacité restante peut être moins confortable, mais elle doit permettre de continuer à travailler.

3. Dimensionnement matériel

Les chiffres ci-dessous constituent une base de conception; les mesures du pilote déterminent la configuration finale.

3.1 Hôtes physiques de virtualisation

Trois hôtes physiques sont recommandés. En fonctionnement normal, la charge est répartie; si un hôte tombe, les deux autres accueillent les machines virtuelles prioritaires.

Composant	Minimum recommandé par hôte	Pourquoi
Processeur	24 à 32 cœurs physiques au total	Absorber sessions, virtualisation et pointe de charge.
Mémoire	256 Go ECC, extensible à 512 Go	La RAM limite souvent plus vite que le processeur.
Stockage local	NVMe professionnel en RAID 10	Faible latence et tolérance à la panne d'un disque.
Réseau	2 interfaces 10 Gb/s + gestion séparée	Débit, redondance et séparation des trafics.
Alimentation	Deux alimentations + onduleur en ligne	Éviter qu'un câble ou bloc d'alimentation arrête l'hôte.
Support	Garantie professionnelle sur site	Réduire la durée d'une panne matérielle.

3.2 Machines virtuelles initiales

Fonction	Quantité	Configuration de départ
Contrôleurs de domaine	2	4 vCPU, 8 à 16 Go RAM chacun
Broker, Web et licences	2 légers ou 1 + reprise	4 à 8 vCPU, 16 Go RAM
Serveurs de sessions	4	12 à 16 vCPU, 64 à 96 Go RAM chacun
Fichiers et profils	1 service protégé	8 à 12 vCPU, 32 à 64 Go RAM
Comptabilité / base	1 séparé	Selon exigences de l'éditeur
Sauvegarde / supervision	1	4 à 8 vCPU, 16 Go RAM

Commencer avec environ 25 à 35 utilisateurs par serveur de sessions. Un usage comportant vidéo, visioconférence, nombreuses pages Web ou applications lourdes peut réduire fortement ce nombre.

3.3 Capacité de stockage

La capacité doit inclure les profils, documents, bases, versions de sauvegarde, images de machines virtuelles et croissance pluriannuelle. Les profils ne doivent pas devenir des dépôts illimités.

- Définir un quota de profil et rediriger les gros dossiers vers un espace de fichiers.
- Séparer stockage de production et dépôt de sauvegarde.
- Utiliser des disques et contrôleurs adaptés aux écritures simultanées.
- Maintenir au moins 20 à 25 % d'espace libre pour les performances et opérations de maintenance.

3.4 Cas nécessitant un GPU

Le montage vidéo, la CAO, la 3D, l'imagerie ou certains simulateurs ne doivent pas être supposés compatibles avec la ferme standard. Ils peuvent nécessiter des hôtes avec GPU, des licences spécialisées ou des postes de travail dédiés.

Test obligatoire

Un processeur ou un serveur plus coûteux ne corrige pas une incompatibilité logicielle. Tester chaque application avec plusieurs comptes en même temps avant de généraliser.

4. Comptes, profils et données

L'identité centralisée permet à chacun de retrouver ses ressources tout en maintenant une séparation claire des responsabilités.

4.1 Active Directory

Active Directory Domain Services centralise les utilisateurs, les ordinateurs, les groupes et les règles. Deux contrôleurs de domaine distincts sont nécessaires afin qu'une panne n'empêche pas toutes les authentifications.

Unité organisationnelle	Exemples de groupes	Accès typique
Étudiants	Classe, session, filière	Applications pédagogiques et dossier personnel
Formateurs	Département, matière	Supports de cours, imprimantes et dossiers de classe
Administration	Accueil, admissions, direction	Gestion scolaire et documents administratifs
Comptabilité	Comptables, direction financière	Logiciel et données comptables seulement
Informatique	Support, administrateurs	Outils d'administration selon le principe du moindre privilège

4.2 Politiques de groupe

- Interdire l'installation de logiciels par les étudiants.
- Bloquer l'accès aux paramètres sensibles et aux outils d'administration.
- Configurer les imprimantes et lecteurs réseau par groupe.

- Verrouiller automatiquement une session inactive.
- Appliquer les navigateurs, mises à jour, antivirus et règles de pare-feu.
- Limiter la redirection de presse-papiers, lecteurs USB ou disques locaux lorsque les données sont sensibles.

4.3 Profils FSLogix

FSLogix conserve le profil de l'utilisateur dans un conteneur central. Le profil suit la personne même si le Broker la dirige vers un serveur de sessions différent. Il faut surveiller la taille des profils et exclure les caches inutiles.

- Stockage rapide et hautement disponible.
- Permissions strictes: chaque utilisateur ne lit que son propre profil.
- Quotas, nettoyage et supervision de la croissance.
- Sauvegarde cohérente et procédure de réparation d'un profil endommagé.

4.4 Dossiers personnels et partagés

Séparer le profil Windows, le dossier personnel, les dossiers de classe et les données administratives. Ne pas placer la base comptable dans un dossier partagé ordinaire si l'éditeur prévoit un serveur de base de données.

Règle pratique

Les permissions sont accordées aux groupes, jamais individuellement sans raison documentée. Cette méthode rend les arrivées, départs et changements de classe beaucoup plus sûrs.

5. Applications et expérience utilisateur

La réussite dépend autant de la compatibilité logicielle que de la puissance du matériel.

5.1 Microsoft Office et navigateurs

Office peut être publié dans le bureau RDS ou comme RemoteApp. Pour Microsoft 365 Apps dans un environnement admissible, utiliser l'activation d'ordinateur partagé. Les navigateurs doivent être configurés par politique: extensions autorisées, page d'accueil, téléchargements et conservation des données.

- Tester Word, Excel, PowerPoint, Access et les macros réellement utilisées.
- Limiter les extensions de navigateur non approuvées.
- Définir une stratégie pour les téléchargements et fichiers temporaires.
- Désactiver la synchronisation personnelle non autorisée.
- Tester imprimantes, scanners et formats de documents.

5.2 Logiciels de formation

Question à poser à l'éditeur	Pourquoi
Le logiciel est-il certifié pour Windows Server et RDS?	Certaines applications refusent les systèmes serveur ou plusieurs sessions.
Quelle licence couvre 100 utilisateurs simultanés?	Une licence monoposte ne devient pas multiutilisateur parce que le logiciel est centralisé.
Où résident les données et la base?	Le stockage et la sauvegarde doivent respecter l'architecture prévue.
Le logiciel exige-t-il GPU, USB ou pilote spécial?	Les périphériques et accélérations ne se redirigent pas toujours correctement.
Comment sont appliquées les mises à jour?	Une mise à jour peut interrompre toutes les classes si elle n'est pas testée.

5.3 Comptabilité et gestion

Créer un groupe d'accès dédié et publier l'application uniquement à ce groupe. Héberger la base sur un serveur distinct lorsque l'éditeur le demande. Restreindre exportations, presse-papiers, impressions et dossiers locaux selon la sensibilité des informations.

Séparation des tâches

Le personnel informatique administre la plateforme, mais ne doit pas utiliser quotidiennement le logiciel avec un compte administrateur. Le personnel comptable ne reçoit aucun droit d'administration du serveur.

5.4 Sessions et confort

- Prévenir avant la fermeture automatique des sessions déconnectées.
- Conserver une session déconnectée pendant une durée raisonnable, puis la fermer.
- Limiter les applications au démarrage.
- Surveiller les ouvertures de session lentes.
- Mettre à disposition une procédure simple pour changer de mot de passe et signaler un problème.

6. Réseau local

Un réseau bien segmenté protège les données et empêche les utilisateurs, les caméras et le Wi-Fi invité de perturber les serveurs.

6.1 Infrastructure

- Commutateurs administrables Gigabit pour les postes.
- Liaisons 10 Gb/s entre hôtes, stockage et cœur de réseau.
- Câblage Cat6 ou Cat6A correctement testé et étiqueté.
- Deux chemins réseau pour les services critiques lorsque le budget le permet.

- Points d'accès Wi-Fi professionnels gérés centralement.
- Pare-feu professionnel entre Internet et les réseaux internes.

6.2 Segmentation par VLAN

VLAN	Exemples	Accès autorisé
Serveurs	RDS, AD, fichiers, bases	Seulement les ports nécessaires depuis les réseaux autorisés
Étudiants	Salles de cours	RDS, impression pédagogique et Internet filtré
Formateurs	Bureaux et salles	RDS, partages de cours et impression
Administration	Accueil et direction	Applications administratives autorisées
Wi-Fi invité	Visiteurs	Internet seulement
Caméras / objets	Caméras, contrôleurs	Serveur de gestion uniquement; aucun accès aux données
Gestion	Interfaces des serveurs et commutateurs	Administrateurs autorisés seulement

6.3 Câble ou Wi-Fi

Les postes fixes qui dépendent du serveur doivent être câblés. Le Wi-Fi reste utile pour les appareils mobiles, mais il varie avec les interférences, le nombre de clients et la construction du bâtiment. Une étude radio est nécessaire pour une couverture professionnelle.

La connexion RDS consomme généralement moins de bande passante qu'une application exécutée localement, mais elle réagit fortement à la latence, aux pertes de paquets et aux microcoupures.

6.4 Services réseau

- DNS interne fourni par les contrôleurs de domaine.
- DHCP redondant ou protégé, avec réservations documentées.
- Synchronisation horaire fiable pour l'authentification.
- Qualité de service si voix, vidéo et RDS partagent les mêmes liaisons.
- Journalisation du pare-feu et supervision des commutateurs.

7. Sécurité

Le but n'est pas seulement d'empêcher une intrusion; il faut aussi réduire l'impact d'un compte compromis ou d'une erreur humaine.

7.1 Principes obligatoires

- Un compte nominatif par personne; aucun mot de passe partagé.
- Comptes administrateurs séparés des comptes de travail quotidien.
- Moindre privilège et accès accordé par groupe.
- Authentification multifacteur pour l'administration et tout accès extérieur.
- Mises à jour testées puis déployées selon un calendrier.

- Antivirus/EDR géré centralement et alertes suivies.
- Journalisation des connexions, échecs et actions sensibles.
- Chiffrement des sauvegardes et protection des clés.

7.2 Accès extérieur

Si l'utilisation est strictement locale, ne publier aucun service RDP sur Internet. Si un accès à distance devient nécessaire, passer par RD Gateway en HTTPS, ajouter une authentification multifacteur et limiter les groupes autorisés.

Interdiction importante

Ne jamais transférer directement le port RDP 3389 du pare-feu vers un serveur de sessions. Cette exposition facilite les attaques automatiques et augmente fortement le risque.

7.3 Sécurité physique

- Salle verrouillée, sèche, ventilée et sans accès public.
- Détection de température, fumée, fuite d'eau et ouverture de porte.
- Onduleurs surveillés et extinction automatique contrôlée.
- Groupe électrogène testé en charge.
- Inventaire, numéros de série et schéma de câblage conservés.
- Accès physique journalisé pour les intervenants.

7.4 Départs et changements

Le jour du départ d'un utilisateur, désactiver son compte, révoquer les sessions, récupérer les équipements, transférer les données professionnelles autorisées et conserver ou supprimer les informations selon la politique de l'établissement.

8. Licences

La licence technique permettant au logiciel de fonctionner n'est pas nécessairement le droit légal de l'utiliser en multiutilisateur.

8.1 Éléments à budgéter

Famille	Éléments à confirmer
Windows Server	Édition, nombre de cœurs couverts, droits de virtualisation.
Windows Server CAL	CAL par utilisateur ou par appareil pour accéder aux services Windows Server.
RDS CAL	CAL RDS par utilisateur ou par appareil pour chaque accès aux Session Hosts.
Microsoft Office	Édition ou abonnement admissible pour RDS et règles d'activation partagée.
Formation	Droits d'installation sur serveur et nombre de connexions simultanées.
Comptabilité	Utilisateurs nommés ou concurrents, modules, base de données et support.
Virtualisation / sauvegarde	Licence de l'hyperviseur, protection des VM et stockage de sauvegarde.

8.2 Par utilisateur ou par appareil

Modèle	Souvent intéressant lorsque	Attention
Par utilisateur	Une même personne se connecte depuis plusieurs appareils.	Chaque utilisateur concerné doit être correctement licencié.
Par appareil	Des postes fixes sont utilisés en rotation par beaucoup d'étudiants.	Chaque appareil qui accède au service doit être couvert.

Avant l'achat

Demander un relevé écrit des droits d'usage et des références exactes à un revendeur Microsoft agréé ainsi qu'à chaque éditeur. Conserver les contrats, factures et clés dans un emplacement sécurisé.

9. Sauvegarde et continuité

Le RAID maintient le fonctionnement après certaines pannes de disque; il ne protège ni contre la suppression, ni contre un rançongiciel, ni contre un incendie.

9.1 Règle 3-2-1

Copie	Emplacement	Objectif
Production	Stockage principal protégé	Service quotidien
Deuxième copie	NAS ou dépôt de sauvegarde distinct	Restauration rapide après erreur ou panne
Troisième copie	Hors bâtiment ou cloud, chiffrée et isolée	Sinistre, vol ou rançongiciel

9.2 Calendrier indicatif

Élément	Fréquence	Conservation initiale
Bases comptables	Plusieurs fois par jour selon activité	Versions quotidiennes et mensuelles
Fichiers utilisateurs	Chaque jour; plus fréquent si critique	30 jours ou selon politique
Machines virtuelles	Chaque jour	Plusieurs points récents
Configuration AD et systèmes	Régulière et après changement majeur	Au moins plusieurs versions
Copie hors site	Chaque jour ou selon connectivité	Immuable lorsque possible

9.3 Tester la restauration

- Restaurer chaque mois un échantillon de fichiers.
- Tester périodiquement une restauration complète dans un réseau isolé.
- Vérifier que les sauvegardes sont lisibles et que les mots de passe sont disponibles.
- Mesurer le temps nécessaire pour remettre le service essentiel en fonction.
- Documenter les responsabilités et numéros de contact.

Une sauvegarde non testée est une hypothèse

Le rapport vert d'un logiciel de sauvegarde ne prouve pas que l'organisation pourra reprendre ses activités. Seule une restauration réussie le démontre.

10. Déploiement par étapes

Le projet doit progresser du laboratoire vers la charge réelle; ouvrir directement à 100 personnes rend les problèmes difficiles à isoler.



Progression recommandée : valider chaque étape avant d'augmenter le nombre d'utilisateurs

10.1 Plan d'exécution

- 1 Inventorier les utilisateurs, postes, imprimantes, logiciels, licences, données et périphériques.
- 2 Classer les applications: compatible RDS, à tester, exigeant GPU, ou à maintenir sur poste dédié.
- 3 Produire le schéma réseau, le plan d'adressage, les VLAN et la liste des flux autorisés.
- 4 Acheter l'infrastructure, les garanties, les onduleurs et les licences confirmées.
- 5 Installer les hôtes de virtualisation et configurer réseau, stockage et supervision.
- 6 Déployer deux contrôleurs de domaine puis créer groupes, comptes et politiques.
- 7 Installer fichiers, profils FSLogix, Broker, licences et premiers Session Hosts.
- 8 Installer les applications selon les procédures propres à RDS et aux éditeurs.
- 9 Ouvrir un pilote à 10 utilisateurs représentatifs, puis corriger les problèmes.
- 10 Tester à 30, 60 puis 100 utilisateurs en mesurant performances et expérience.
- 11 Former le support, documenter les opérations et préparer le plan de retour arrière.
- 12 Déployer par classe ou département et surveiller étroitement les premières semaines.

10.2 Critères d'acceptation

Domaine	Exemples de critères
Connexion	Ouverture stable, temps acceptable et reconnexion à la bonne session.
Applications	Fonctions essentielles, impression, export et périphériques validés.
Performance	CPU, RAM, stockage et réseau restent dans des marges sûres en pointe.
Sécurité	Permissions, segmentation, journaux, mises à jour et MFA testés.
Continuité	Panne d'un hôte simulée et services prioritaires maintenus.
Sauvegarde	Restauration réelle de fichiers, base et système documentée.
Support	Procédures comprises et incidents correctement escaladés.

11. Exploitation quotidienne

Une bonne installation peut se dégrader rapidement sans surveillance, entretien et responsabilité clairement attribuée.

11.1 Tableau de bord

- Nombre de sessions actives, déconnectées et en échec.
- CPU, mémoire et latence disque par serveur de sessions.
- Temps d'ouverture de session et taille des profils.
- Capacité libre du stockage et croissance hebdomadaire.
- Santé des hôtes, alimentations, RAID, onduleurs et températures.
- État des sauvegardes et date du dernier test de restauration.
- Mises à jour en attente et alertes de sécurité.
- Saturation, erreurs et pertes sur le réseau.

11.2 Cycle de maintenance

Fréquence	Actions
Chaque jour	Vérifier alertes critiques, sauvegardes, stockage, sécurité et disponibilité.
Chaque semaine	Examiner performances, sessions anormales, comptes et incidents répétés.
Chaque mois	Tester restauration, appliquer les mises à jour après validation, revoir capacité.
Chaque trimestre	Tester basculement, vérifier droits, licences, documentation et onduleurs.
Chaque année	Réévaluer capacité, contrats, cycle de vie, risques et plan de continuité.

11.3 Assistance aux utilisateurs

Créer un point de contact unique. Chaque incident doit préciser l'utilisateur, l'ordinateur, l'heure, l'application, le message affiché et si d'autres personnes sont touchées. Cette discipline accélère le diagnostic.

- Niveau 1: mot de passe, impression, session bloquée, instructions de base.

- Niveau 2: profils, politiques, applications et analyse des journaux.
- Niveau 3: infrastructure, stockage, réseau, sécurité et éditeurs.

12. Budget et achats

Comparer le coût total sur plusieurs années, pas seulement le prix d'achat des serveurs.

12.1 Catégories budgétaires

Catégorie	Inclure
Calcul	Trois hôtes, RAM de réserve, cartes réseau, garantie.
Stockage	Production, profils, bases, NAS de sauvegarde, disques de réserve.
Réseau	Cœur 10 Gb/s, commutateurs, modules, câbles, pare-feu, Wi-Fi.
Électricité	Onduleurs, batteries, groupe électrogène, climatisation, surveillance.
Licences	Windows Server, CAL, RDS CAL, Office, logiciels, base, sauvegarde.
Services	Conception, installation, migration, tests, formation, support.
Exploitation	Internet, électricité, renouvellements, pièces, sécurité et temps humain.

12.2 Demande de devis

Fournir le même cahier des charges à plusieurs intégrateurs afin de comparer des propositions équivalentes. Exiger un schéma, une nomenclature détaillée, les références de licences, les garanties, les limites de capacité et les services inclus.

Éviter le faux prix bas

Une proposition qui omet les CAL RDS, la sauvegarde hors site, la redondance ou les tests paraîtra moins chère, mais ne répondra pas réellement au besoin.

13. Liste de contrôle finale

Cette liste sert à valider la conception avant la commande, puis l'ouverture du service.

13.1 Avant de commander

- Nombre d'utilisateurs simultanés confirmé par catégorie.
- Applications et périphériques inventoriés.
- Compatibilité RDS confirmée par écrit.
- Licences et droits multiutilisateurs chiffrés.
- Capacité N+1 démontrée dans la proposition.
- Stockage, croissance et sauvegardes dimensionnés.
- Électricité, climatisation et sécurité physique évaluées.
- Architecture réseau et VLAN documentés.

- Support et garantie définis.

13.2 Avant l'ouverture

- Deux contrôleurs de domaine opérationnels.
- Comptes, groupes et politiques testés.
- Profils et dossiers accessibles avec les bonnes permissions.
- Applications validées par les responsables métiers.
- Charge testée progressivement jusqu'au niveau cible.
- Panne d'un hôte et restauration testées.
- Aucun RDP direct exposé à Internet.
- Supervision et alertes reçues par une personne responsable.
- Documentation et formation du support terminées.
- Plan de communication disponible en cas d'interruption.

13.3 Après le lancement

- Revoir les mesures chaque jour pendant les deux premières semaines.
- Corriger les lenteurs à partir de données, pas d'impressions isolées.
- Limiter les changements simultanés afin de pouvoir identifier leur effet.
- Recueillir les difficultés des étudiants, formateurs et services administratifs.
- Planifier la prochaine extension avant d'atteindre les limites de capacité.

14. Nomenclature matérielle détaillée

Cette proposition est dimensionnée comme point de départ pour 100 à 150 utilisateurs simultanés. Les références définitives doivent être validées par les mesures du pilote.

14.1 Trois serveurs physiques identiques

Élément	Quantité et spécification recommandées	Observation
Châssis	3 serveurs rack 2U	Choisir une gamme professionnelle avec garantie sur site.
Processeur	1 CPU de 24 à 32 cœurs physiques par serveur	Un seul processeur puissant peut réduire la complexité de licence.
Mémoire	384 Go ECC par serveur, extensible à 512 Go ou plus	Conserver une marge suffisante après la panne d'un hôte.
Démarrage	2 SSD professionnels de 960 Go en RAID 1	Réservés à Windows Server et Hyper-V.
Données	4 à 6 NVMe de 3,84 To par serveur	Modèles entreprise avec protection contre la perte d'alimentation.
Réseau rapide	2 ports 25 Gb/s	Stockage, machines virtuelles et migration.
Gestion / secours	2 ports 1 ou 10 Gb/s	Gestion distante, maintenance et chemin secondaire.
Administration distante	iDRAC, iLO ou équivalent	Console indépendante du système d'exploitation.
Alimentation	2 blocs redondants 800 à 1 400 W	Chaque bloc connecté à un PDU différent.
Sécurité	TPM 2.0 et Secure Boot	Protection de démarrage et préparation au chiffrement.

Familles d'équipements possibles: Dell PowerEdge, HPE ProLiant DL380, Lenovo ThinkSystem SR650 ou serveur professionnel équivalent. Le choix final dépend de la disponibilité, de la garantie et de la capacité locale de réparation.

Pourquoi 384 Go de RAM?

Avec plusieurs Session Hosts, les services d'identité, les profils et les applications de gestion, 256 Go par hôte peut devenir insuffisant lors de la panne d'un serveur. La mémoire supplémentaire assure une meilleure continuité.

14.2 Réseau, postes et salle technique

Matériel	Quantité indicative	Caractéristiques essentielles
Commutateurs centraux	2	Niveau 3, 12 à 24 ports 10/25 Gb/s, VLAN, MLAG ou empilage.
Commutateurs d'accès	4 x 48 ports	Gigabit, administrables, uplinks 10 Gb/s; PoE+ si nécessaire.
Pare-feu	2 en haute disponibilité ou 1 + réserve	VLAN, VPN, journaux, prévention d'intrusion et MFA.
Points d'accès Wi-Fi	8 à 15 après étude radio	Wi-Fi 6/6E, gestion centrale, PoE+, réseaux séparés.
Ordinateurs clients	100 à 150	8 Go RAM, SSD 128/256 Go, Gigabit, Windows 11 Pro.
Armoire	1 x 42U	Fermée, mise à la terre, PDU A/B et organisation des câbles.
Onduleur	8 à 10 kVA à confirmer par calcul	Technologie en ligne, 15 à 30 minutes, supervision réseau.
Climatisation	Dédiée et dimensionnée	Fonctionnement continu, contrôle de température et humidité.

14.3 Serveur de sauvegarde

- Processeur de 8 à 16 cœurs et 64 à 128 Go de RAM.
- Deux interfaces 10 Gb/s.
- Huit à douze disques professionnels, pour 60 à 120 To bruts selon la conservation.
- RAID 6 ou technologie équivalente, avec snapshots protégés ou stockage immuable.
- Alimentations redondantes et comptes d'administration différents de la production.
- Troisième copie chiffrée hors du bâtiment, sur bande ou dans un stockage distant.

15. Installation physique et réseau

L'installation commence par la salle, l'électricité et le câblage. Les logiciels viennent seulement après la validation de cette base.

15.1 Préparer la salle

- 1 Installer l'armoire rack et vérifier sa mise à la terre.
- 2 Installer la climatisation dédiée et les capteurs de température, humidité, fumée et ouverture de porte.
- 3 Installer l'onduleur, les deux PDU et le groupe électrogène avec transfert automatique.
- 4 Préparer les panneaux de brassage Cat6A et étiqueter chaque prise et câble.
- 5 Contrôler l'accès physique à la salle et conserver un registre d'intervention.

Éviter fenêtres, poussière, humidité, conduite d'eau et installation directement au sol. L'onduleur se place généralement en bas du rack, les serveurs au centre et les commutateurs près des panneaux de brassage.

15.2 Raccordements redondants

- Alimentation A de chaque serveur vers PDU A; alimentation B vers PDU B.
- Première interface rapide vers le commutateur central 1; seconde vers le commutateur central 2.
- Interface de gestion distante placée dans le VLAN de gestion.
- Chemins distincts pour gestion, stockage, migration, utilisateurs et sauvegarde.
- Tous les ports, câbles et adresses documentés dans un registre de configuration.

15.3 Plan VLAN indicatif

VLAN	Usage	Exemple d'adressage
10	Gestion des serveurs et équipements	10.10.10.0/24
20	Cluster et migration	10.10.20.0/24
30	Stockage	10.10.30.0/24
40	Serveurs et machines virtuelles	10.10.40.0/24
50	Administration	10.10.50.0/24
60	Formateurs	10.10.60.0/24
70	Étudiants	10.10.70.0/23
80	Wi-Fi invité	10.10.80.0/23
90	Caméras et équipements connectés	10.10.90.0/24
100	Sauvegarde	10.10.100.0/24

Important

Ces adresses sont des exemples. Le plan définitif doit être approuvé et documenté avant la configuration du DHCP, du DNS et du pare-feu.

15.4 Règles de circulation

- Étudiants vers les serveurs RDS: autoriser uniquement les services nécessaires.
- Étudiants vers la gestion des serveurs: interdire.
- Wi-Fi invité vers tous les réseaux internes: interdire.
- Caméras vers RDS, fichiers et comptabilité: interdire.
- Administration vers comptabilité: autoriser seulement pour les groupes concernés.
- Sauvegarde vers production: autoriser uniquement les flux requis par le logiciel de sauvegarde.

16. Installation des hôtes et du domaine

Les exemples de commandes servent de guide à un administrateur qualifié. Les noms, adresses et paramètres doivent être adaptés au plan réel.

16.1 Préparer les trois hôtes

- 1 Mettre à jour BIOS, contrôleur RAID, cartes réseau et contrôleur de gestion.
- 2 Activer virtualisation matérielle, TPM 2.0 et Secure Boot.
- 3 Configurer les deux SSD de démarrage en RAID 1.
- 4 Attribuer les noms HV01, HV02 et HV03 ainsi que des adresses fixes.
- 5 Installer Windows Server et les pilotes approuvés par le fabricant.

- 6 Installer uniquement Hyper-V, clustering, outils de supervision et agents de sauvegarde nécessaires.

Exemple PowerShell:

```
Install-WindowsFeature Hyper-V, Failover-Clustering  
-IncludeManagementTools -Restart
```

Valider ensuite la configuration matérielle et réseau:

```
Test-Cluster -Node HV01,HV02,HV03
```

Ne créer le cluster que si les contrôles ne signalent aucun problème bloquant. Storage Spaces Direct exige des disques, pilotes et cartes réseau compatibles.

Séparation stricte

Ne jamais installer Office, la comptabilité ou les applications des utilisateurs directement sur les hôtes Hyper-V.

16.2 Créer Active Directory

Créer DC01 sur le premier hôte, lui attribuer une adresse fixe et installer le rôle AD DS:

```
Install-WindowsFeature AD-Domain-Services -IncludeManagementTools
```

Créer ensuite une forêt, par exemple avec un sous-domaine que l'organisation contrôle:

```
Install-ADDSForest -DomainName "ad.alapierreentreprises.org" -InstallDNS
```

Créer DC02 sur un autre hôte physique, le joindre au domaine et l'ajouter comme contrôleur DNS et Global Catalog. Vérifier la réplication, la résolution DNS et la synchronisation horaire.

Nom du domaine

ad.alapierreentreprises.org est un exemple cohérent avec le site de l'organisation. Vérifier la propriété du domaine et le plan DNS avant de l'adopter.

16.3 Créer les unités et groupes

- Unités: Étudiants, Formateurs, Administration, Comptabilité, Ordinateurs, Serveurs et Comptes de service.
- Groupes par classe, filière, matière et département.
- Comptes administratifs séparés des comptes de travail quotidien.
- Permissions accordées aux groupes et non directement aux utilisateurs.
- Procédure de création, changement de rôle, désactivation et archivage des comptes.

17. Installation détaillée de RDS et des applications

Le déploiement RDS distribue les sessions sur plusieurs serveurs et reconnecte chaque utilisateur à son environnement.

17.1 Déployer les rôles RDS

- 1 Ajouter toutes les machines RDS dans le Gestionnaire de serveur.
- 2 Choisir Ajouter des rôles et fonctionnalités.
- 3 Sélectionner Installation des Services Bureau à distance.
- 4 Choisir Déploiement standard, puis Déploiement de bureaux basé sur une session.
- 5 Affecter RD Connection Broker et RD Web Access à RDS-BRK01.
- 6 Ajouter RDS-SH01 comme premier Session Host, puis les autres après validation.
- 7 Ajouter RD Licensing, activer le serveur et installer les CAL appropriées.
- 8 Créer les collections de sessions et y associer les groupes autorisés.

Collections suggérées: BUREAU-ETUDIANTS, BUREAU-FORMATEURS, APPLICATIONS-ADMIN et COMPTABILITE.

Pour une meilleure disponibilité, ajouter ensuite un second Broker et configurer les certificats selon la conception choisie.

17.2 Installer les applications

Les quatre Session Hosts doivent recevoir les mêmes versions, paramètres et mises à jour. Pour une application traditionnelle qui ne gère pas automatiquement le mode serveur de sessions:

change user /install

Installer l'application

change user /execute

- Confirmer que l'édition Microsoft Office autorise RDS et l'activation partagée nécessaire.
- Tester Word, Excel, PowerPoint, Access, macros, compléments et impression.
- Limiter extensions, téléchargements et synchronisations personnelles des navigateurs.
- Demander à chaque éditeur une confirmation écrite de compatibilité et de licence multiutilisateur.
- Publier la comptabilité en RemoteApp et héberger sa base sur APP01 si l'éditeur le prévoit.

17.3 Profils et dossiers

Créer des emplacements distincts, par exemple:

\\FILE01\Profils\$

\\FILE01\Etudiants\$

\\FILE01\Formateurs\$

\\FILE01\Administrations\$

- Activer les conteneurs de profils FSLogix par stratégie de groupe.
- Définir quotas, exclusions de cache et surveillance de la taille.
- Donner à chaque utilisateur uniquement l'accès à son propre profil.
- Séparer profil Windows, documents, supports de cours et données comptables.

17.4 Politiques et sécurité

- Activer Network Level Authentication.
- Verrouiller les sessions inactives et fermer les sessions déconnectées après le délai prévu.
- Interdire l'installation de logiciels aux étudiants.
- Contrôler presse-papiers, lecteurs locaux, USB, imprimantes et téléchargements.
- Déployer antivirus/EDR, journaux, mises à jour et alertes centralisés.
- Pour un accès extérieur, utiliser RD Gateway, certificat public et MFA; ne jamais exposer directement le port 3389.

18. Tests, ouverture et maintenance

Une ouverture progressive permet de mesurer les limites avant qu'elles ne perturbent toutes les classes.

18.1 Montée en charge

- 1 Commencer avec cinq administrateurs et formateurs.
- 2 Ouvrir à dix utilisateurs pilotes représentatifs.
- 3 Passer à trente utilisateurs et corriger les défauts.
- 4 Tester soixante sessions avec les applications réelles.
- 5 Atteindre cent sessions et simuler une période de pointe.
- 6 Valider la charge cible complète et la panne d'un hôte.

Mesure	Ce qu'il faut observer
Connexion	Temps d'ouverture, échecs et reconnexion à la bonne session.
CPU et mémoire	Pointes, files d'attente et marge restante après une panne.
Stockage	Latence, files d'attente, capacité libre et croissance.
Réseau	Débit, pertes de paquets, erreurs de ports et latence.
Profil	Taille, temps de montage, erreurs et profils temporaires.
Applications	Stabilité, impression, export, audio, vidéo et périphériques.

18.2 Calendrier de protection

Élément	Fréquence recommandée
Base comptable	Toutes les 2 à 4 heures selon l'activité
Fichiers et profils	Chaque jour, davantage si les données sont critiques
Machines virtuelles	Chaque nuit
Copie hors site	Chaque jour ou dès que la connectivité le permet
Test de restauration de fichiers	Chaque mois
Test complet de reprise	Chaque trimestre

Condition d'ouverture

Le service ne doit pas être déclaré prêt avant une restauration réussie, une simulation de panne d'hôte et un test de charge représentatif.

Conclusion

La meilleure plateforme n'est pas un seul serveur très puissant, mais un ensemble équilibré, mesurable et récupérable.

Pour plus de 100 utilisateurs utilisant Microsoft Office, des navigateurs, des logiciels de formation, de comptabilité et de gestion, une ferme Windows Server RDS constitue la base la plus cohérente. Trois hôtes de virtualisation, quatre serveurs de sessions, deux contrôleurs de domaine, des profils FSLogix, un stockage protégé et une stratégie de sauvegarde 3-2-1 offrent une architecture évolutive.

La réussite repose ensuite sur quatre disciplines: valider chaque logiciel, licencier correctement, tester la charge réelle et préparer la reprise après incident. L'établissement peut ainsi centraliser ses ressources sans transformer la salle des serveurs en point unique de défaillance.

Recommandation finale

Construire un pilote représentatif, mesurer avec de vrais utilisateurs, puis déployer par vagues. Cette méthode protège le budget, les cours et les données.

Références officielles

Les liens suivants servent de point de départ. Les conditions de produit et de licence peuvent évoluer; vérifier les versions en vigueur avant tout achat.

Microsoft Learn - Vue d'ensemble de Remote Desktop Services

<https://learn.microsoft.com/windows-server/remote/remote-desktop-services/remote-desktop-services-overview>

Microsoft Learn - Licences RDS et CAL

<https://learn.microsoft.com/windows-server/remote/remote-desktop-services/rds-client-access-license>

Microsoft Learn - Active Directory Domain Services

<https://learn.microsoft.com/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-do>

main-services-overview

Microsoft Learn - FSLogix

<https://learn.microsoft.com/fslogix/overview>

Microsoft Learn - Activation d'ordinateur partagé pour Microsoft 365 Apps

<https://learn.microsoft.com/deployoffice/overview-shared-computer-activation>

Microsoft Learn - Remote Desktop Gateway

<https://learn.microsoft.com/windows-server/remote/remote-desktop-services/rds-roles>

© 2026 Albertho Lapierre. Document de formation et de planification technique.