

PC-SAMPLE-NET-01 / FR / V1.1

Conception et bascule du réseau hybride

RAPPORT TYPE • SCÉNARIO FICTIF

PRÉPARÉ POUR
DATE

Groupe industriel Orivane
2026-08-14

Réseau : mandat et besoins à couvrir

Ce rapport présente un scénario fictif. L'entreprise Orivane, les personnes, les fournisseurs, les systèmes et les résultats ont été inventés. Les noms de technologies réelles servent uniquement à décrire le contexte technique. Aucun contenu ne provient d'un mandat client. Les adresses utilisent le domaine réservé .example.

Le réseau Nacre relie les 18 établissements d'Orivane, les centres de données MTL-DC1 à Montréal et IAD-DC2 à Ashburn, ainsi que trois régions AWS. Jonah Patel est responsable du projet NET-2608 et du changement CHG-2648. Le réseau doit soutenir les commandes d'entrepôt, le travail de bureau et les applications de l'entreprise. En cas de panne, les connexions de secours doivent maintenir les mêmes restrictions d'accès.

La conception distingue le trafic des utilisateurs, la réplication des données, les transferts volumineux et l'administration. La capacité doit répondre à la demande de pointe même lorsque la liaison principale tombe en panne. Le débit annoncé ne suffit pas à le démontrer. Les dépendances des applications doivent être documentées avant de fixer la date de bascule.

EXIGENCE	CONSÉQUENCE POUR L'ACCEPTATION
Connexions limitées	Flux approuvés fonctionnels et flux interdits refusés en exploitation normale comme en relève.
Routes prévisibles	Routes principale et de secours définies dans les deux sens; aucune ambiguïté de priorité pour les connexions en cours.
Reprise indépendante	Accès d'administration indépendant du réseau principal et retour arrière autorisé même en cas de panne.
Panne observable	Surveillance distinguant transport, routes, DNS et application.

L'achat de circuits, la correction du câblage et la refonte applicative sont exclus. Si ces travaux sont nécessaires, ils doivent être terminés par un responsable désigné avant la bascule.

Sites, fournisseurs et dossier de changement

MTL-DC1 occupe Vela Quay à Montréal; IAD-DC2, Stonebridge à Ashburn. Ils s'ajoutent aux 18 sites ci-dessous. Les points de raccordement AWS sont ca-central-1, us-east-1 et eu-west-1. Jonah Patel effectue les changements, Amira Chen les vérifie, Tessa Lin valide les commandes LedgerFlow et Elias Moreno dirige l'intervention.

PARC	EMPLACEMENTS INSCRITS
Canada	MTL-01 Montréal; QC-02 Québec; TOR-03 Toronto; OTT-04 Ottawa; HAM-05 Hamilton; YYC-06 Calgary.
États-Unis	IAD-07 Ashburn; RIC-08 Richmond; CMH-09 Columbus; DTW-10 Detroit; PIT-11 Pittsburgh; BOS-12 Boston.
Europe	DUB-13 Dublin; ORK-14 Cork; LIM-15 Limerick; GWY-16 Galway; MAN-17 Manchester; RTM-18 Rotterdam.

Liaisons et fournisseurs

FOURNISSEUR	SERVICE ET DOSSIER D'EXPLOITATION
Veyra Fiber	Ethernet privé 10 Gb/s par centre : VF-MTL-4401 et VF-IAD-4402. Préférence BGP 200. Priya Nordin, responsable; incident VF-260814-06.
TernRoute Networks	Internet 5 Gb/s par centre : TR-MTL-8821 et TR-IAD-8822, avec IPsec vers Nacre. Préférence 100. Mateo Silva, centre d'exploitation réseau; dossier TR-11842.
Mistral Mobile	Gestion LTE indépendante : MM-MTL-091 et MM-IAD-092. Elias Moreno autorise les interventions de secours; essai OOB-0813.
Fenêtre	CHG-2648 : 22 août, 01 h-03 h UTC. MTL-01 d'abord; QC-02/TOR-03 après l'accord de Tessa Lin. Décision avant 01 h 40 UTC.

Plan d'adressage, routage et dépendances

Les plages ci-dessous constituent le plan d'adressage du scénario. Avant de réserver ces adresses, vérifier les réseaux existants, les routes des partenaires, les accès distants et les conteneurs pour éviter les chevauchements. Une route qui regroupe plusieurs plages ne doit être annoncée que par l'équipe qui les gère toutes. Le trafic vers les adresses inutilisées doit être rejeté.

DOMAINE	BLOC RÉSERVÉ	RÈGLE DE SEGMENTATION
Sites d'affaires	10.64.0.0/12	Subdivision par site et fonction; appareils d'entrepôt sans accès de bureau implicite.
Centres de données	10.80.0.0/12	Domaines distincts pour applications, bases de données et gestion.
ca-central-1	10.96.0.0/12	Rattachements séparés pour production, hors production et services partagés.
us-east-1	10.112.0.0/12	Routes interrégionales explicites pour applications et reprise.
eu-west-1	10.128.0.0/12	Mêmes règles de séparation; la présence dans une région n'accorde aucun accès supplémentaire.

Politique de routage

RP-17 encadre l'échange de routes par le protocole BGP. Les numéros de réseau sont 65010 pour Orivane et 64520/64530 pour les liaisons fournisseurs. Des listes limitent les routes reçues et annoncées à 200 préfixes par voisin. La préférence locale favorise Veyra à 200, puis TernRoute à 100. Documenter aussi la route par défaut. Toute route annoncée par un partenaire doit correspondre aux plages qu'il est autorisé à gérer.

Avant le gel de conception

Vérifier les chevauchements d'adresses, les routes de retour, la traduction d'adresses, la taille maximale des paquets et les adresses sources réellement vues par les applications. Consigner les résultats : un schéma cohérent ne garantit pas que ces éléments fonctionnent ensemble.

Liaisons réseau et contrôles d'accès

Les liaisons Ethernet de Veyra Fiber et les tunnels chiffrés IPsec de TernRoute appliquent les mêmes règles d'accès à Nacre. Elles ne relient pas librement la production, les environnements de test et les services partagés. Les essais doivent vérifier les routes de retour et le suivi des connexions par les pare-feu sur les deux liaisons.

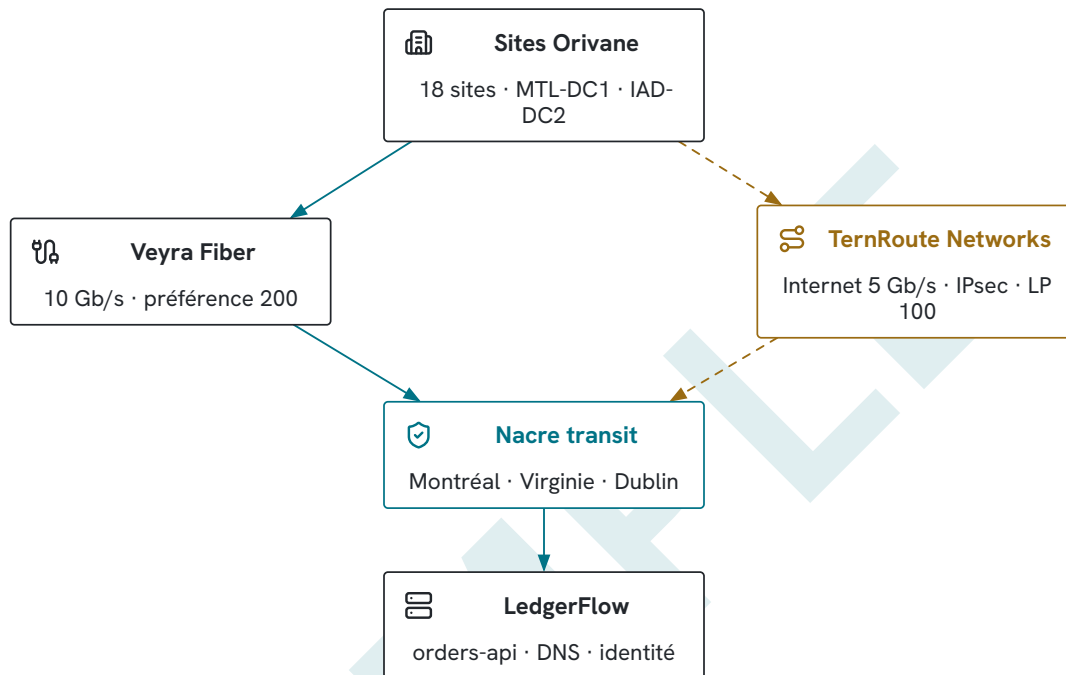


Figure 1 Chemins Veyra Fiber et TernRoute. L'ombre indique la diversité des conduits IAD encore à prouver.

Preuves exigées en relève

- ✓ La liaison de secours absorbe la demande de pointe tout en respectant les objectifs des applications.
- ✓ Flux permis et refusés conservent la même politique dans les deux sens.
- ✓ DNS, certificats et transaction métier fonctionnent depuis les segments réels.
- ✓ L'accès d'administration indépendant reste disponible si la liaison de production tombe en panne.

Flux de services et conception DNS

SOURCE	DESTINATION	USAGE PERMIS
MTL-01 / VLAN 120	API LedgerFlow	10.64.1.0/24 → 10.96.10.0/24, TCP 443. Aucun accès direct aux bases ou à l'administration.
MTL-01 / VLAN 210	Orivane ID / nacre-dns-ca	Services publiés d'authentification et de résolution; aucun accès général au réseau d'administration.
API LedgerFlow	ledgerflow-db	10.96.10.0/24 → 10.96.20.0/24, TCP 5432; inspection symétrique au retour.
orv-recovery	LedgerSafe / ledgerflow-dr	Flux temporaires avec responsable et étape de fermeture.
Hors production	Production	Refus sauf dépendance approuvée représentée dans routage et pare-feu.

La résolution fait partie du chemin

Jonah Patel gère la zone DNS prod.orivane.example. MTL-DC1 envoie les requêtes à nacre-dns-ca, 10.96.0.10 et 10.96.0.11; us.orivane.example utilise 10.112.0.10 et 10.112.0.11; eu.orivane.example, 10.128.0.10 et 10.128.0.11. La durée de conservation des réponses en cache (TTL) passe à 60 secondes, 24 heures avant CHG-2648. Les requêtes vers un service privé doivent atteindre le résolveur régional et retourner l'adresse prévue pour l'utilisateur. Éviter les règles qui renvoient les requêtes d'un résolveur à l'autre en boucle. Vérifier la durée de cache des réponses valides et des noms introuvables.

Tester depuis les segments réels avec la chaîne de résolution de production. Une résolution sur le portable d'un ingénieur ne valide ni les entrepôts ni les hôtes de reprise. Vérifier noms de certificats, redirections et découverte des services. Garder les anciens enregistrements seulement pendant la coexistence approuvée.

Pannes et validation de capacité

Deux fournisseurs peuvent utiliser le même conduit, la même alimentation ou des équipements communs. Il faut donc vérifier le parcours physique des deux liaisons. VF-DIV-0812 confirme des entrées distinctes à Montréal. Mateo Silva doit fournir le plan DIV-118 d'Ashburn le 18 août. La bascule réseau a été validée, mais l'indépendance physique des liaisons d'Ashburn reste à confirmer.

PANNE	RÉPONSE ATTENDUE	PREUVE
VF-MTL-4401	Retirer Veyra; préférer TR-MTL-8821 avec préférence locale 100.	Convergence, application, sessions et utilisation du chemin secondaire.
Nœud d'inspection	Utiliser un chemin sain ou arrêter les flux; aucun contournement silencieux.	Essais de connexions autorisées et interdites pendant la panne, y compris le suivi du trafic de retour.
Résolveur régional	Utiliser le résolveur de secours prévu, avec les mêmes réponses pour les zones privées.	Requêtes par segment, expiration du cache et reconnexion applicative.
Centre de données	Activer uniquement les dépendances de reprise approuvées.	Seules les routes prévues sont diffusées; le responsable valide le service de secours et ses données.
Gestion	Utiliser le canal hors bande indépendant.	Accès opérateur, configuration conservée et autorité de retour vérifiée.

Résultats des essais de capacité

CAP-0812 fait passer 3,1 Gb/s par TR-MTL-8821. La perte de paquets est de 0,08 % et les routes se stabilisent en 8,4 secondes. Dans LedgerFlow, 95 % des réponses arrivent en moins de 620 ms (p95). Les limites sont de 0,1 %, 15 secondes, 900 ms au p95 et moins de 4 Gb/s en continu. Refaire l'essai pendant CHG-2648 en tenant compte du chiffrement, de l'inspection et de la réplication. L'essai ne couvre pas la perte simultanée des deux centres. Un ping réussi ne suffit pas à autoriser la bascule.

Poursuivre, suspendre ou revenir en arrière

Chaque étape exige une décision. Les essais techniques doivent réussir et Tessa Lin doit valider LedgerFlow avant de passer aux sites suivants. Un échec suspend la suite. Avant tout retour arrière, il faut aussi vérifier que l'ancienne configuration convient encore aux données et aux accès autorisés.

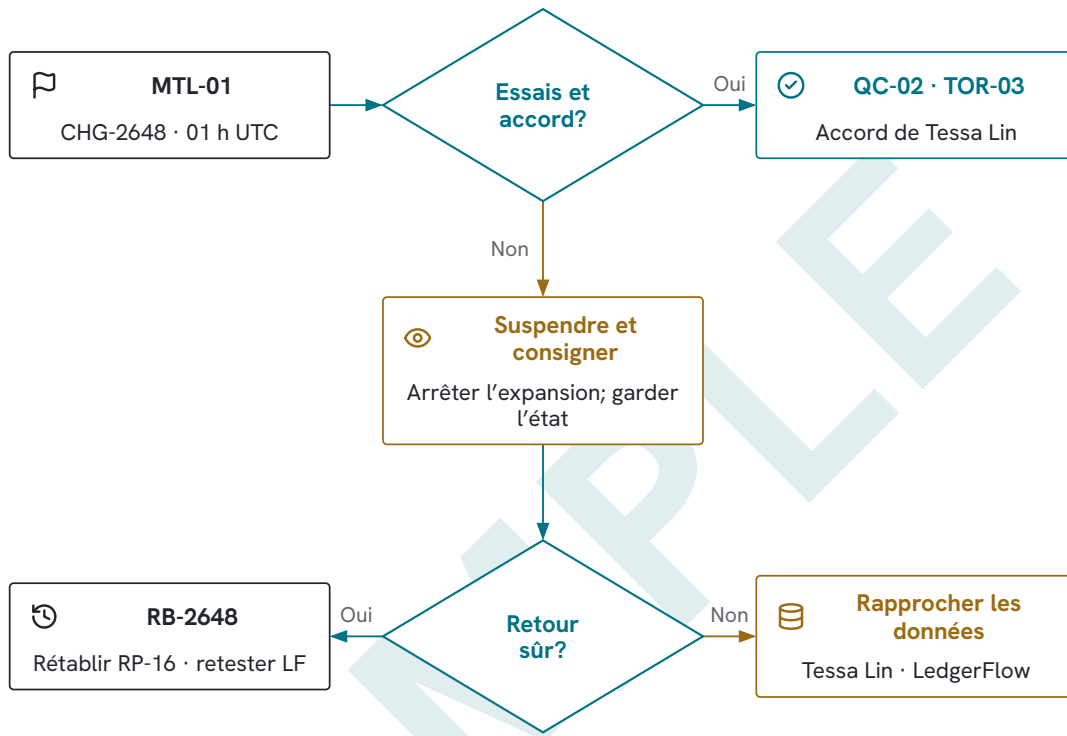


Figure 2 Les points de décision réservent le temps nécessaire au retour arrière et à la vérification des données.

Avant le début des opérations

- ✓ Les routes prévues, la configuration en vigueur et la procédure de retour arrière sont sauvegardées.
- ✓ Opérateur, vérificateur et responsable de décision sont présents.
- ✓ Le temps restant couvre validation, décision et reprise éprouvée.

Procédure de bascule

CHG-2648 commence à MTL-01 le 22 août à 01 h UTC. Jonah Patel effectue les changements, Amira Chen les vérifie et Tessa Lin valide le résultat. Elias Moreno consigne la décision à 01 h 40. La fenêtre se termine à 03 h; RB-2648 commence avant 02 h 10 pour garder 50 minutes de validation.

POINT	ACTION	POINT DE CONTRÔLE
21 août / 17 h	Geler le routage, conserver la configuration effective, vérifier le hors bande et répéter la reprise.	Préalables acceptés.
00 h 30 UTC	Confirmer la disponibilité des équipes, les routes, la surveillance et l'absence de changements concurrents.	Début autorisé par le gestionnaire.
01 h 00 UTC	Appliquer routes et règles préparées au seul périmètre pilote.	État effectif vérifié par le second opérateur.
01 h 10 UTC	Tester DNS, flux permis et refusés, puis la commande LF-TEST-0822-0042 et son accusé Dockline.	Comportement validé par le responsable.
01 h 25 UTC	Tester la liaison de secours selon le plan approuvé.	Aucun accès imprévu, aucune perte ni surcharge inattendue.
01 h 40 UTC	Passer à QC-02/TOR-03, maintenir MTL-01 ou lancer RB-2648.	Décision explicite; aucune expansion automatique.

Ne pas comprimer la validation pour rattraper un retard. Si la fenêtre ne permet plus vérification et retour, reporter la prochaine cohorte. Conserver l'état observé avant dépannage pour distinguer la bascule prévue des corrections d'urgence.

Retour arrière et limites des données

Le retour arrière s'impose si un accès interdit s'ouvre, si l'accès d'administration est perdu, si un test de commande échoue de façon persistante ou si la liaison de secours dépasse sa capacité. Jonah Patel suspend la suite, sauvegarde les routes et les compteurs, puis informe Elias Moreno. L'ancienne configuration ne peut être rétablie qu'après vérification de ses dépendances et de ses risques.

Un retour réseau redirige le trafic, mais n'annule ni écritures, ni état répliqué, ni messages acceptés. Si l'emplacement actif des données a changé, le responsable applicatif autorise leur rapprochement avant le retour du trafic. Ce point d'arrêt s'applique même si le réseau peut revenir en quelques secondes.

ÉTAPE	VÉRIFICATION
Arrêter les cohortes	Geler routes et DNS supplémentaires; conserver une autorité de changement.
Rétablir l'état approuvé	Réappliquer règles et préférences précédentes revues, jamais une permission générale.
Vérifier les sessions	Confirmer inspection à état, adresses traduites et reconnexion applicative.
Valider le service	Répéter flux permis et refusés et transaction métier depuis les segments touchés.
Fermer la fenêtre	Consigner état final, symptômes, responsabilités et prochaine revue avant de libérer les équipes.

L'exercice préalable fixe l'heure limite de décision. Pour poursuivre le dépannage après cette heure, Elias Moreno doit approuver une prolongation en tenant compte de la fatigue des équipes, du temps de reprise restant et des effets sur les activités.

Preuves de transfert et contrôles d'exploitation

DOSSIER	CONTENU
Socle de conception	Responsabilité des plages, politiques de routes, flux approuvés et dépendances.
Mise en œuvre	Configurations revues, états effectifs avant/après et dossier de retour.
Acceptation	DNS par source, flux permis et refusés, transaction métier et mesures en relève.
Exploitation	Alertes, identifiants de circuits, escalade fournisseur, hors bande et entretien.
Exceptions	Traductions d'adresses en cas de chevauchement, anciennes routes conservées, pannes non testées et dates de révision.

Contrôles récurrents

Signaler les changements du nombre de routes, les routes par défaut inattendues et les pannes de tunnel, de DNS ou d'accès d'administration. Tester régulièrement les applications depuis plusieurs établissements. Refaire les essais de secours après tout changement majeur du réseau ou des applications. Des liaisons affichées comme disponibles ne garantissent pas que les utilisateurs peuvent travailler.

Hypothèses à prouver

L'exemple suppose des plages sans chevauchement, un hors bande disponible et des responsables capables de valider les données. CAP-0812 prouve la relève MTL. La diversité IAD reste ouverte dans DIV-118; Jonah Patel la valide avant le 18 août et la vague IAD. Le [pilier Fiabilité du cadre AWS Well-Architected](#) offre un cadre général, sans valider cette topologie fictive ni fournir ses cibles de capacité.