

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

Conception et transfert du socle infonuagique

RAPPORT TYPE • SCÉNARIO FICTIF

PRÉPARÉ POUR
DATE

Groupe industriel Orivane
2026-07-24

Mandat de conception

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.

Nacre fournira aux six divisions d'Orivane une base commune pour exploiter leurs 24 applications : gestion des accès, réseau et reprise après incident. La plateforme comprendra 48 comptes AWS dans trois régions approuvées. Chaque application de production aura son propre compte; les services partagés seront administrés séparément.

Le présent document décrit la conception, les décisions à respecter et les vérifications nécessaires avant que l'équipe d'exploitation prenne le relais. Un déploiement réussi ne suffit pas. Pour chaque contrôle, il faut désigner un responsable, détecter les pannes et prévoir une procédure de reprise.

Priorités de conception

PRIORITÉ	CHOIX RETENU
Droits d'administration limités	Les équipes déploient leurs services sans administrer politiques organisationnelles, archives ou copies de reprise.
Approbation uniforme des comptes	Chaque compte suit les mêmes étapes : demande, configuration, vérification et attribution des responsabilités.
Changement réversible	Un déploiement peut être arrêté par vague; sa reprise ne dépend pas de l'identité en réparation.
Coûts visibles	Chaque application a un responsable des coûts et des alertes budgétaires. Le budget prévu n'autorise pas à lui seul une dépense.

La conception des applications, les licences et l'exploitation continue ne font pas partie de ce mandat. Les interfaces et les procédures livrées précisent comment ces activités s'intègrent à la plateforme.

Paramètres du projet Nacre

Nadia Bellerose est la commanditaire du projet NCRE-26. Elias Moreno dirige la plateforme et Maya Dufresne approuve les mesures de sécurité. Cette conception du 24 juillet donne suite à l'évaluation ORV-SEC-2607. Elle définit la configuration commune nacre-1.4.0 et autorise les travaux. La mise en production reste conditionnelle aux vérifications décrites ici.

INTERFACE	SOCLE CONVENU
Autorité des comptes	Les politiques de l'organisation sont gérées dans orv-mgmt. orv-secops reçoit les détections; orv-log conserve les preuves. orv-recovery est l'un des six comptes de services partagés.
Livraison	Dépôt platform.orivane.example/nacre; modules 1.4.0; manifeste accounts-0724.yaml; changements CHG-2620-2625.
Régions	ca-central-1 : fabrication et distribution canadiennes; us-east-1 : distribution américaine et reprise; eu-west-1 : activités européennes.
Identité et noms	Fédération Orivane ID; groupe privilégié Nacre-Platform; zones prod.orivane.example et lab.orivane.example gérées par Jonah Patel.
Objectifs de service	LedgerFlow et Dockline : RTO 60 min, RPO 15 min. ForgeTrack et MarginLedger : RTO 4 h, RPO 1 h, à confirmer par un exercice de reprise.
Allocation	Enveloppe de planification de 185 000 CAD par mois; six centres de coûts suivis par Celia Hart. Alertes à 70 %, 90 % et 100 %, sans autoriser la dépense.

Le RTO fixe le délai maximal de rétablissement du service. Le RPO fixe la perte de données acceptable, exprimée en durée. Un exercice de reprise doit confirmer ces deux objectifs.

Responsabilités et dossiers

Tessa Lin est responsable de LedgerFlow, Marc Bellamy de ForgeTrack et Léa Mercier de la reprise. Amira Chen vérifie les comptes avant leur mise en production. DEC-024 justifie le choix d'un compte par application. L'exception EX-019 autorise l'ancien point d'accès MillWatch jusqu'au 30 septembre, sans prolongation automatique.

Topologie des comptes et décisions

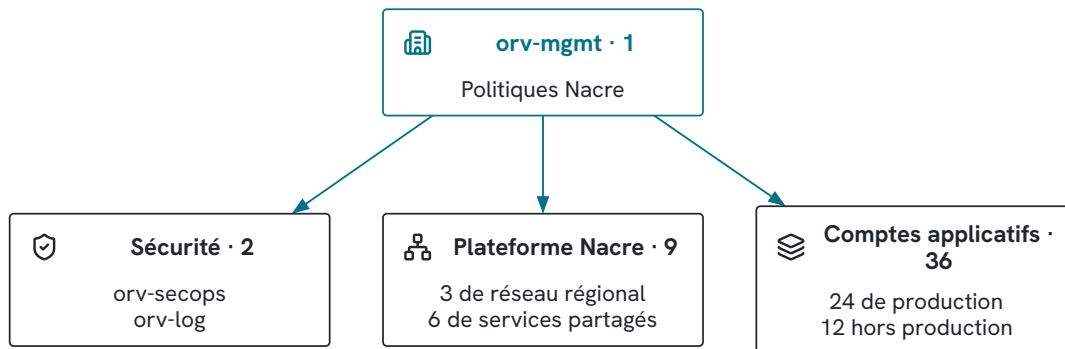


Figure 1 Groupes de comptes et portée des politiques. Les flèches indiquent la gouvernance, pas l'accès réseau.

Le total est de 48 comptes. Chaque charge possède ici son compte de production; le hors production est regroupé par équipe et sensibilité. Les régions sont des lieux de déploiement, pas des comptes supplémentaires. Le compte de gestion n'héberge aucune charge d'affaires.

ADR-01 / Isoler la production par responsabilité

Un compte par application permet d'attribuer clairement les droits, les coûts et les responsabilités en cas d'incident. Un compte par division demanderait moins de gestion, mais réunirait les droits de déploiement et de reprise de plusieurs applications. Le projet retient donc des comptes séparés et automatise leur configuration. Les comptes partagés hors production ne peuvent contenir de données de production sans exception approuvée.

ADR-02 / Centraliser les politiques, répartir la livraison

L'équipe plateforme maintient les règles communes et les outils de gestion des comptes. Les équipes applicatives configurent leurs services et approuvent leurs déploiements. Les politiques de l'organisation limitent les droits possibles, mais n'accordent aucun accès. Chaque application conserve ses propres règles. Le compte de gestion exige des procédures plus strictes que les autres comptes.

Identité et responsabilité des contrôles

Les employés se connectent par Orivane ID et reçoivent des accès temporaires. L'administration, les déploiements automatisés et les interventions d'urgence utilisent des rôles distincts, décrits dans la documentation. Aucun compte administrateur n'est partagé. Chaque accès privilégié a un responsable et une date de révision.

CONTRÔLE	RESPONSABLE	PREUVE AVANT TRANSFERT
Politique organisationnelle	Maya Dufresne approuve; l'automatisation applique la version revue.	Changements interdits refusés dans un compte pilote; politique effective conservée.
Identité de livraison	Tessa Lin approuve les permissions LedgerFlow.	Livraison approuvée réussie; compilation et dépôt sans lien refusés.
Journaux et détection	Maya Dufresne gère orv-log et le suivi des alertes SecOps.	Événement reçu et traité; panne de livraison signalée séparément.
Autorité de reprise	Léa Mercier approuve les accès et suppressions dans orv-recovery.	Restauration isolée sans identifiants d'administration de la charge.
Accès d'urgence	Elias Moreno autorise; Maya Dufresne révise ensuite.	Accès de secours testé; notification et renouvellement consignés.

Les limites de permission en pratique

L'administrateur plateforme ne devient pas automatiquement lecteur des données applicatives. L'identité de livraison peut modifier l'infrastructure approuvée sans affaiblir sa propre confiance. Une exception précise la permission élargie, le responsable et l'échéance. Son renouvellement exige la preuve que la contrainte persiste; elle n'est pas un second socle permanent.

Interfaces réseau et données

Dans chaque région, les routes séparent la production, les environnements de test et les services partagés. Le DNS, qui résout les noms des services, et l'inspection du trafic sont accessibles aux seules applications autorisées. Cet accès n'ouvre pas l'ensemble des sous-réseaux partagés. Les connexions entre régions doivent répondre à un besoin documenté de l'application ou de sa reprise.

SOURCE	DESTINATION	CONTRAT
LedgerFlow	nacre-dns-ca	Résolveurs et zones approuvés seulement; requêtes et échecs de transfert observables.
API LedgerFlow	ledgerflow-db	TCP 5432 depuis le sous-réseau API, avec retour symétrique; chaque côté approuve les changements.
orv-partsdesk-test	LedgerFlow prod	Refus par défaut; essai synthétique après chaque modification de routage.
ledgerflow-release	API AWS	Identité limitée, politique de terminaison régionale et contexte de changement journalisé.
orv-recovery	Coffre LedgerSafe	Autorité indépendante; le trafic de reprise n'hérite pas de la connectivité normale.

ADR-03 / Centraliser l'inspection avec un responsable

L'inspection centrale uniformise les politiques, mais ajoute des dépendances communes de débit et de disponibilité. La dimensionner selon le trafic concurrent et éprouver sa dégradation avant de la rendre obligatoire. Un flux qui ne la tolère pas exige un contrôle local approuvé, pas un contournement caché. La classification et les clés restent des responsabilités applicatives.

Validation des comptes et traitement des échecs

Le processus garde les comptes créés hors production jusqu'à la vérification indépendante du socle déployé. Un échec produit une quarantaine réversible. Les corrections reprennent le même processus versionné; modifier une étiquette d'inventaire ne permet pas l'admission.

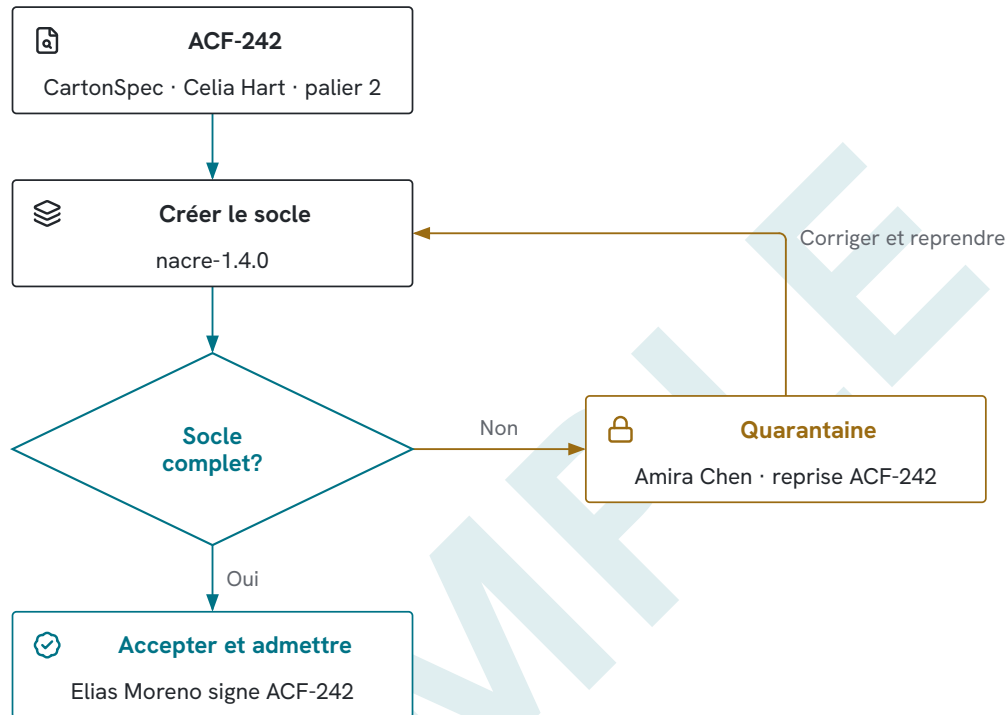


Figure 2 L'admission est une décision explicite avec une boucle de correction.

Vérifications avant mise en production

- ✓ Un système indépendant reçoit les journaux et signale toute panne d'envoi.
- ✓ Les actions approuvées réussissent; identités et flux interdits restent refusés.
- ✓ Responsable, coûts, échéance des exceptions et version déployée sont consignés.

Cycle des comptes et livraison du socle

Toute demande de compte doit préciser le responsable, l'environnement, la sensibilité des données, les régions, le centre de coûts et les objectifs de reprise. Aucun compte ne passe en production sans responsables désignés.

ÉTAPE	ACTION	CONDITION DE SORTIE
1 / approuver	Revoir responsabilité, placement et exceptions.	Un approbateur accepte le contrat de compte.
2 / créer	Créer le compte et appliquer le socle revu.	L'automatisation reprend sans dupliquer les ressources après un échec.
3 / relier	Configurer identité, journaux, DNS et flux permis.	Événements et sondes visibles depuis des observateurs indépendants.
4 / vérifier	Tester les actions autorisées et les refus attendus.	Preuves liées à la version déployée; échec laissant le compte en quarantaine.
5 / admettre	Transférer responsabilité de la charge et des coûts.	Responsable acceptant procédures et alertes avant la première livraison.
6 / retirer	Retirer accès et dépendances; conserver les dossiers requis.	Conservation ou suppression des données approuvée; routes, budgets et inventaire mis à jour.

Évolution du socle

Numéroter chaque version de la configuration commune. La déployer d'abord dans des comptes pilotes, puis hors production et enfin en production. Conserver les paramètres propres aux applications à part. Le suivi des écarts distingue les exceptions approuvées des modifications non vérifiées. Une mise à jour automatique ne doit pas retirer une règle ajoutée pour contenir un incident.

Vagues de migration et conditions d'arrêt

Les 24 applications migreront en trois vagues, les 11 août, 25 août et 8 septembre. La répartition ci-dessous pourra changer si plusieurs applications partagent des données ou un service dont elles dépendent. Avant chaque migration, il faut vérifier les données, les accès, les certificats, le DNS et la reprise dans la fenêtre prévue.

VAGUE	CHARGES	PREUVE D'ADMISSION
11 août · Alder	4	PolicyShelf, ShiftBoard, FieldNotes, CartonSpec. Amira Chen vérifie reconstruction et retour sans écritures de production.
25 août · Birch	8	ToolVault, LabelWorks, GradeBook, MillWatch, RouteDesk, FreightLens, PartsDesk, PeopleDeck. Prouver identité, routes et alertes.
8 sept. · Cedar	12	ForgeTrack, AlloyPlan, PackFlow, LinePulse, StockBridge, BatchTrace, LedgerFlow, Dockline, ServiceAtlas, WarrantyDesk, MarginLedger, Partspan. Tester la restauration des données et du service.

Conditions d'arrêt d'une migration

Arrêter si les journaux n'arrivent plus, si un privilège inattendu apparaît, si un flux interdit s'ouvre ou si la reprise manque l'objectif approuvé. Les applications non touchées conservent leur configuration validée. Le responsable de l'incident décide de revenir en arrière, d'isoler le problème ou de le corriger. L'outil de déploiement ne peut pas prendre cette décision sur la seule base d'un délai écoulé.

Avant de migrer un service qui conserve des données, noter le dernier point de restauration et les transactions possibles après la bascule. Revenir à l'ancienne infrastructure n'annule ni les écritures ni les messages déjà transmis. Si le retour risque de perdre des transactions, suspendre les nouvelles écritures et appliquer la procédure de rapprochement avant de rediriger le trafic.

- **Responsables de l'approbation**

Elias Moreno approuve le socle. Tessa Lin approuve le comportement de LedgerFlow et l'intégrité des données. Aucun ne signe pour l'autre.

Transfert et acceptation opérationnelle

LIVRABLE	ESSAI D'ACCEPTATION
Dépôt plateforme	Un autre ingénieur crée un compte pilote avec la procédure, sans l'aide de l'auteur.
Décisions d'architecture	Les responsables expliquent périmètres, exceptions et conséquences de leur modification.
Preuves des contrôles	Essais permis et refusés d'identité, de réseau et de politique liés à la version déployée.
Procédures d'exploitation	L'équipe de garde reçoit une alerte, identifie le responsable et effectue un diagnostic sûr.
Dossier de reprise	Un service est restauré isolément avec clés, dépendances et validation applicative.
Inventaire et coûts	Chaque compte actif a des responsables pour l'application et les coûts, un état à jour et une date de révision des exceptions.

Décisions ouvertes au transfert

Au 24 juillet, deux vérifications bloquent encore la vague Cedar : rétablir ForgeTrack en quatre heures lors de REC-2619 et valider le transfert des alertes DNS dans CHG-2625. Léa Mercier et Jonah Patel doivent présenter les résultats le 31 juillet. Le dossier de transfert précise les éléments manquants, les responsables et la prochaine révision. La garantie du travail livré ne comprend pas un service permanent de surveillance ou de garde.

Référence et hypothèses

Le [pilier Fiabilité du cadre AWS Well-Architected](#) fournit un cadre général pour changements et reprise. Topologie, répartition des charges, migration et acceptation sont des exemples originaux. Dimensionnement, conservation légale et objectifs de service doivent être établis avant une mise en œuvre réelle.