

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

Évaluation de la sécurité du socle infonuagique

RAPPORT TYPE • SCÉNARIO FICTIF

PRÉPARÉ POUR
DATE

Groupe industriel Orivane
2026-07-10

Note de décision

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 regroupe les comptes AWS, les règles d'accès et les services réseau du Groupe industriel Orivane. Les applications sont séparées des services partagés, mais deux faiblesses doivent être corrigées avant d'élargir la plateforme. Le serveur de compilation nacre-build-03, accessible par Internet, peut utiliser le rôle ReleaseDeploy de LedgerFlow. Les administrateurs des applications peuvent aussi modifier la destination de leurs journaux d'audit. Un attaquant pourrait ainsi modifier le logiciel en production et masquer ses traces.

L'évaluation couvre les 48 comptes AWS : politiques, accès, déploiement, réseau, protection des données et reprise. Nous recommandons de maintenir les services actuels, de retirer les accès inutiles entre comptes et de vérifier que les actions interdites sont bloquées avant d'ajouter des applications.

Décisions attendues

DÉCISION	MOTIF
Suspendre l'expansion	Maintenir les services; différer les nouveaux comptes de production jusqu'à la validation du socle.
Limiter les droits de déploiement	Séparer compilation et mise en production avant de modifier les droits de journalisation ou les identifiants.
Prévoir les essais de reprise	Réserver du temps aux responsables applicatifs pour une restauration isolée et la validation des dépendances.

Orivane : mandat et documents examinés

Nadia Bellerose, directrice des technologies de l'information, a demandé l'évaluation ORV-SEC-2607 avant l'expansion de Nacre. Orivane fabrique des composants industriels et assure leur distribution et leur entretien. L'entreprise emploie 2 400 personnes dans 18 établissements au Canada, aux États-Unis et en Europe. Elle compte six divisions : Mouvement, Emballage, Matériaux, Distribution, Service sur le terrain et Services administratifs.

DOSSIER	DONNÉES DE RÉFÉRENCE
Période	Du 29 juin au 10 juillet 2026; documents recueillis jusqu'à 16 h UTC le 10 juillet. Collecte en lecture seule et essais d'accès en environnement isolé.
Inventaire	INV-0710.csv : 48 comptes actifs; orv-mgmt, orv-secops, orv-log et 45 comptes de plateforme et d'applications. Aucun compte suspendu.
Régions approuvées	ca-central-1 (Montréal), us-east-1 (Virginie du Nord), eu-west-1 (Irlande). Recherche de ressources dans les autres régions activées.
Identités	IAM-0709 : 312 politiques de confiance IAM; 94 relations d'accès entre comptes, dont 24 rôles de déploiement en production.
Réseau	NET-0708 : 57 rattachements VPC, neuf tables de transit et 126 flux approuvés.
Reprise	BKP-0709 : 24 plans de sauvegarde de production. L'exercice de reprise LedgerFlow REC-0709 s'arrête avant la validation du traitement des commandes.

Responsables de la revue

Elias Moreno est responsable de Nacre; Maya Dufresne, des opérations de sécurité; Jonah Patel, du routage; et Léa Mercier, de la reprise. Tessa Lin valide le traitement des commandes dans LedgerFlow. Les documents examinés sont regroupés sous ORV-SEC-2607 dans le dépôt documentaire d'Orivane. Les conclusions portent sur la version nacre-1.3.2.

Environnement et portée de l'évaluation

Orivane exploite 48 comptes AWS pour six unités d'affaires dans trois régions approuvées. Tous les comptes figurent à l'inventaire et à la revue des politiques. L'examen du code applicatif, la sécurité physique et l'évaluation de la sécurité des fournisseurs sont exclus. Cette couverture ne constitue ni une certification ni une découverte exhaustive des vulnérabilités.

PÉRIMÈTRE DE COMPTES	COMPTES
Gestion	1
Sécurité et archives	2
Réseautique régionale	3
Services partagés	6
Charges de production	24
Hors production	12

Méthodes utilisées

DOMAINE	MÉTHODE DE REVUE
Organisation	Politiques en vigueur et classement de tous les comptes; examen distinct des exceptions du compte de gestion.
Identité et livraison	Confiance des rôles, droits de déploiement, attributs de fédération et accès d'urgence approuvés.
Réseau et données	Connexions permises par les routes et pare-feu, accès privés, droits sur les compartiments de stockage et les clés, gestion des sauvegardes.
Exploitation	Livraison des journaux, acheminement des alertes, admission des comptes et séquence de reprise applicative représentative.

Sans preuve, nous ne pouvons pas confirmer qu'un contrôle fonctionne. L'examen d'une configuration et un essai en conditions réelles apportent des renseignements différents; les deux sont nécessaires.

Périmètres et méthode de priorisation

Les employés passent par Orivane ID; le groupe Nacre-Platform reçoit des sessions d'administration de 60 minutes. Les groupes approuvés obtiennent des rôles temporaires dans les comptes de charges. Le compte orv-ci exécute nacre-build-03; ledgerflow-release déploie vers orv-ledgerflow-prod. Le transit régional donne accès au DNS et à la gestion partagés. Les journaux quittent les comptes de charges pour une archive distincte, tout comme les copies de reprise.

Le découpage des comptes n'est qu'un point de départ. La séparation doit être appliquée dans les droits d'accès, le routage et la gestion des sauvegardes. Un compte de production sur réseau privé peut rester exposé par son rôle de déploiement.

Chemins d'attaque représentatifs

CHEMIN	CONDITION PRÉALABLE ET CONSÉQUENCE
P1 / livraison	Compromettre un exécuteur → utiliser son rôle de confiance → utiliser un rôle de déploiement en production → modifier un artefact applicatif. Aucune connexion utilisateur supplémentaire n'est requise.
P2 / preuves	Obtenir l'administration d'une charge → modifier la livraison des journaux ou l'accès à sa clé → créer une lacune de surveillance. La conservation des archives existantes doit être vérifiée séparément.
P3 / reprise	Compromettre un rôle de charge → atteindre l'administration des sauvegardes → supprimer les copies récupérables. La réussite d'une tâche ne prouve pas l'isolement.

Preuves requises avant clôture

- ✓ Vérifier les droits de l'identité source et les règles d'accès du rôle cible.
- ✓ Tester une action interdite et une opération autorisée.
- ✓ Consigner la version testée, le résultat et le nom de la personne qui l'a vérifié.

Droits de déploiement : situation actuelle et correction

Ces schémas isolent le chemin de livraison de SEC-01. Les flèches indiquent autorité ou action, pas connectivité réseau. Elles n’impliquent aucun droit automatique sur journaux ou sauvegardes.

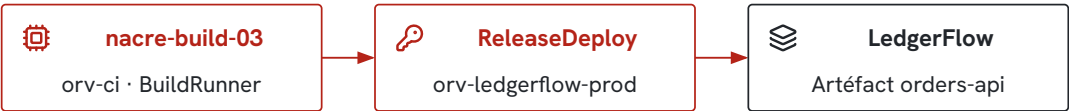


Figure 1 Le serveur de compilation peut modifier la production.

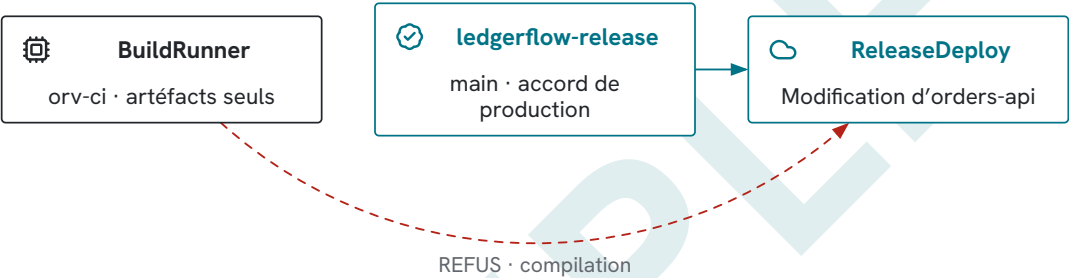


Figure 2 Contrôle proposé : la production accepte le contexte de livraison approuvé.

Niveaux de gravité

GRAVITÉ	SENS DANS CETTE ÉVALUATION
⚠ ÉLEVÉE	Accès permettant d’agir sur la production ou la reprise au-delà des droits prévus. Trois constats.
⚠ MOYENNE	Faiblesse dont les effets dépendent d’une autre défaillance ou d’un élément non vérifié. Trois constats.
ⓘ FAIBLE	Faiblesse circonscrite de portée immédiate limitée. Aucun constat ici.

La gravité dépend des accès possibles, des privilèges requis, des effets potentiels et de la capacité à détecter l’attaque. Un schéma décrit un scénario; seul un essai encadré permet de confirmer les accès.

Constats : administration de la plateforme

 SEC-01

 ÉLEVÉE

Le serveur de compilation peut déployer en production

Selon IAM-0709, neuf des 24 rôles de production sont accessibles à orv-ci/BuildRunner. L'essai ID-17 confirme que nacre-build-03 peut utiliser ReleaseDeploy pour modifier orders-api; aucun fichier de production n'a été changé. Protéger la branche du dépôt ne bloque donc pas ce serveur s'il est compromis.

Séparer les identifiants de compilation et de déploiement. Limiter le rôle cible au processus de livraison approuvé et aux seules actions requises. Vérifier qu'un jeton de compilation est refusé, même pour un fichier valide. Le processus approuvé et ses responsables doivent toujours être protégés.

 SEC-02

 ÉLEVÉE

Les administrateurs peuvent arrêter leurs journaux

Dans six comptes de production, WorkloadAdmin peut arrêter l'envoi des journaux vers orv-log. AUD-12 confirme un StopLogging permis pour orv-dockline-prod. Un attaquant peut ainsi interrompre les nouvelles traces; les objets déjà archivés restent protégés. Le stockage central ne suffit pas à protéger la collecte.

Confier la collecte à l'équipe de sécurité et surveiller l'envoi depuis un compte distinct. Tester une tentative d'arrêt, une perte d'accès aux clés et une panne d'envoi. Prévoir un accès de secours indépendant pour corriger une erreur de politique.

 SEC-03

 MOYENNE

Les exceptions expirées restent actives

Sept exceptions sur onze sont échues. EX-014 permet encore un point d'accès public après le déplacement d'orv-partsdesk-test de Sandbox à NonProduction le 2 juillet; l'échéance du 30 juin n'a déclenché aucune revue. Une permission temporaire peut survivre à son responsable ou sortir du périmètre prévu. Exiger un responsable, une échéance et un essai des politiques effectives à chaque déplacement; une ancienne étiquette d'inventaire ne suffit pas.

Constats : isolation des applications et reprise

⚠ SEC-04

⚠ ÉLEVÉE

Les mêmes droits donnent accès aux applications et aux sauvegardes

Les 24 charges de production ont une sauvegarde planifiée. Selon BKP-0709, WorkloadAdmin peut utiliser RecoveryAdmin pour 18 applications, dont LedgerFlow et Dockline, et supprimer leurs copies. Une sauvegarde réussie confirme la création d'une copie, mais pas sa protection contre un attaquant ayant ces droits.

Séparer l'administration de reprise, valider la conservation et exiger une seconde autorité pour les changements destructifs. Restaurer une application représentative dans un compte isolé, avec clés et dépendances. Une copie protégée que l'équipe ne peut déchiffrer ne prouve pas la capacité de reprise.

⚠ SEC-05

⚠ MOYENNE

Le réseau partagé relie des environnements à isoler

La table nacre-tgw-shared de ca-central-1 importe 12 rattachements hors production et huit de production. NET-31 atteint le sous-réseau LedgerFlow depuis orv-partsdesk-test; le pare-feu refuse TCP 5432. Les pare-feu bloquent certains flux, mais les routes ne respectent pas la séparation prévue. Une modification ultérieure pourrait exposer des services au-delà de la portée envisagée.

Pour chaque connexion autorisée, préciser la source, la destination et le service, puis configurer les routes et les pare-feu en conséquence. Vérifier l'aller et le retour, le DNS et l'inspection. Garder des exceptions explicites pour les services partagés; une séparation qui casse la résolution de noms n'est pas viable.

⚠ SEC-06

⚠ MOYENNE

Un déploiement réussi ne suffit pas à autoriser la production

ACF-218 déclare orv-cartonspec-prod prêt malgré l'absence de test des journaux et de responsable des coûts. Nacre-1.3.2 ne prévoit aucune vérification indépendante avant la mise en production. Exiger des essais d'actions autorisées et interdites ainsi qu'un approbateur désigné. Garder tout compte non conforme en quarantaine jusqu'à sa correction.

Séquence de correction et responsabilités

Les fenêtres ci-dessous proposent une séquence après approbation, sans constituer une promesse de livraison. Les responsables doivent confirmer accès, dépendances et fenêtres avant de s'engager. Le confinement précède les changements généraux; l'acceptation est jointe au dossier de mise en œuvre.

FENÊTRE	RESPONSABLE ET ACTION	PREUVE DE CLÔTURE
13 juillet	Elias Moreno : séparer compilation et livraison. SEC-01 .	Jeton de compilation refusé; livraison approuvée réussie; refus transmis à la surveillance.
14 juillet	Maya Dufresne : protéger la collecte et alerter sur ses lacunes. SEC-02 .	Désactivation refusée; panne contrôlée signalée par un canal indépendant.
20 juillet	Léa Mercier : séparer les copies et prouver le déchiffrement. SEC-04 .	Suppression refusée à l'administrateur de charge; restauration isolée avec dépendances et validation.
22 juillet	Jonah Patel : limiter le transit aux flux approuvés. SEC-05 .	Flux interdits refusés dans les deux sens; DNS et trafic permis fonctionnels.
24 juillet	Elias Moreno : retirer les exceptions échues et contrôler l'admission. SEC-03 , SEC-06 .	Politiques revérifiées au déplacement; échec laissant le compte en quarantaine; responsabilité consignée.

Sécurité des changements

Tester chaque politique dans un compte pilote. Conserver politiques effectives et attributions avant modification. Confirmer une identité d'urgence et une autorisation de retour arrière indépendantes avant de restreindre l'administration. Arrêter si une livraison approuvée, les journaux ou un service essentiel échouent. Rétablir la dernière configuration sûre; rouvrir un chemin exposé exige une acceptation explicite et temporaire du risque.

Dossier de validation et limites

Maya Dufresne a revu l'index ORV-SEC-2607 le 10 juillet. La collecte est complète; les essais de vérification après correction restent à faire sous CHG-2613 à CHG-2617. Les lignes identifient les dossiers recueillis et les preuves de clôture encore requises.

DOSSIER DE VÉRIFICATION	CONTENU REQUIS
E1 / INV-0710	Inventaire rapproché de l'organisation; régions non examinées et comptes suspendus indiqués séparément.
E2 / IAM-0709	Droits de l'appelant, confiance et contexte de session pour chaque chemin; tentatives permises et refusées.
E3 / AUD-12	Configuration de collecte, droits d'archive et de clé, événement reçu et alerte indépendante de panne.
E4 / NET-0708	Matrice de flux approuvée, routes et règles effectives, essais de connexions autorisées et interdites.
E5 / REC-0709	Responsabilité des copies, refus de suppression, restauration isolée, accès aux clés et validation applicative.
E6 / ACF-218	Demande de compte, socle effectif, échéance des exceptions et décision signée d'admission ou de quarantaine.

Ce que la conclusion ne couvre pas

L'évaluation n'établit ni l'autorisation applicative, ni la résilience à pleine charge, ni la sécurité des fournisseurs, ni l'absence de compromission. L'échantillon doit être élargi si l'inventaire révèle un autre mode de déploiement. Un constat est clos seulement après vérification du contrôle et de ses preuves; une modification fusionnée ne suffit pas.

Cadre de référence

Les domaines couverts s'appuient sur le [pilier Sécurité du cadre AWS Well-Architected](#). Le scénario, les constats et les priorités sont des exemples originaux, pas des conclusions fournies par ce cadre.