

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

Conception et déploiement d'un accès sécurisé

RAPPORT TYPE • SCÉNARIO FICTIF

PRÉPARÉ POUR
DATE

Groupe industriel Orivane
2026-08-07

Accès aux applications et besoins de l'entreprise

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 Groupe industriel Orivane compte 2 400 employés, 180 partenaires externes et 36 applications internes. Sofia Caron dirige Nacre Access sous ACC-2608. Le projet limite l'accès de chaque personne aux applications dont elle a besoin, sans ouvrir tout le réseau interne. Les équipes doivent pouvoir travailler depuis chaque établissement. Les partenaires restent limités aux services autorisés. Un accès de secours est prévu en cas de panne des services centraux.

Chaque autorisation vise une application et une tâche précises. La passerelle vérifie l'identité, la conformité de l'appareil et la validité de la session. L'application vérifie ensuite ses propres droits d'accès. Franchir la passerelle ne donne donc pas le droit de tout faire dans l'application.

CONTRAINTE	SOLUTION PRÉVUE
Anciens protocoles	Limiter chaque connecteur aux services approuvés. Garder un accès réseau direct seulement si l'application ne peut pas passer par la passerelle.
Appareils partenaires	Séparer ressources et sessions partenaires; une identité externe valide ne vaut pas accès d'employé.
Administration	Exiger un compte d'administration distinct et un appareil approuvé. Les sessions de travail ordinaires ne donnent aucun droit d'administration.
Disponibilité	Installer les connecteurs sur des infrastructures indépendantes et tester séparément la disponibilité du service qui décide des accès.

Le dispositif est prêt lorsque les utilisateurs accomplissent leurs tâches, que les accès sont traçables et que les autres ressources restent inaccessibles. Les applications peuvent utiliser des connecteurs différents. Une panne ne doit jamais ouvrir un accès sans restriction.

Applications et règles d'accès convenues

Le registre ACC-036 du 7 août identifie les 36 applications. Orivane ID fournit les identités; Nacre Access décide si l'accès demandé est autorisé. Les six connecteurs acc-mtl-01/02, acc-iad-01/02 et acc-dub-01/02 desservent Montréal, Ashburn et Dublin. Les deux connecteurs de chaque ville sont installés sur des infrastructures indépendantes.

RESSOURCE	RÈGLES D'ACCÈS
LedgerFlow / Tessa Lin	orders.orivane.example; HTTPS 443; groupe LF-OrderOps; appareils des employés gérés par Orivane. Session de huit heures, inactivité de 15 minutes, révocation en cinq minutes.
Partspan / Samir Okafor	partners.orivane.example; HTTPS 443; groupe PS-Suppliers. Accès des partenaires Neralis Automation approuvé jusqu'au 30 septembre; aucune découverte DNS interne.
ToolVault / Amira Chen	git.orivane.example; HTTPS 443 et SSH 22 limité. Dépôts d'ingénierie seulement; déploiement au moyen d'un compte de service distinct.
MillWatch / Marc Bellamy	millwatch.orivane.example; TCP 8443 via acc-mtl-02. EX-019 autorise l'accès de 20 opérateurs d'usine jusqu'au 30 septembre.
Accès privilégié	Amira Chen utilise a.chen-admin sur ORV-LT-0421 géré. Authentification de moins de 15 minutes; cible nacre-admin; session maximale de 30 minutes.

Socle de politiques et soutien

La politique access-2.3 exige un état de conformité de l'appareil datant de moins de cinq minutes pour accéder aux données internes. Sans cette information, l'accès est refusé. Une exception permet à Lucien Armand, de Neralis Automation, de consulter ses commandes Partspan sur un appareil non géré après authentification forte. Il ne peut ni exporter des données ni voir celles d'autres fournisseurs. Sofia Caron approuve les droits et Maya Dufresne révisé les exceptions. Julien Voss traite les incidents ACC-DENY.

Inventaire des ressources et politiques

CLASSE DE RESSOURCES	NOMBRE	RESPONSABLE DE POLITIQUE
Applications Web de l'entreprise	20	Le responsable de l'application définit les rôles et approuve les accès partenaires.
Services d'ingénierie	8	L'ingénierie définit les actions des dépôts et systèmes de compilation.
Consoles d'administration	5	Sécurité et responsable système approuvent ensemble les privilèges.
Services anciens	3	Le responsable documente les limites du protocole et les protections supplémentaires.

L'inventaire totalise 36 applications. ACC-036 précise nom d'hôte, classification, protocole, population, responsable, connecteurs, dépendances et reprise pour chaque entrée. Ces renseignements sont requis avant la migration. Une application sans responsable reste hors du déploiement de production.

Une politique est un changement applicatif

Chaque modification de politique est numérotée et fait l'objet d'une révision. Le demandeur décrit la tâche, les personnes concernées et la durée de l'accès. Le responsable de l'application approuve les droits; l'équipe de sécurité en vérifie les limites. L'appartenance au groupe « tous les employés » ne justifie pas, à elle seule, un accès.

Chaque partenaire a un répondant chez Orivane et une date de fin d'accès. À la fin du contrat, ce répondant vérifie les groupes et les rôles à retirer. Il faut aussi révoquer les jetons propres aux applications : retirer l'accès à la passerelle ne les désactive pas.

Décisions d'accès et révocation

Nacre Access vérifie l'identité, les droits et les exigences applicables à l'appareil. Partspan décide ensuite si l'utilisateur peut effectuer l'action demandée. Chaque refus doit fournir un motif utile. Une information manquante ne doit pas élargir les droits.

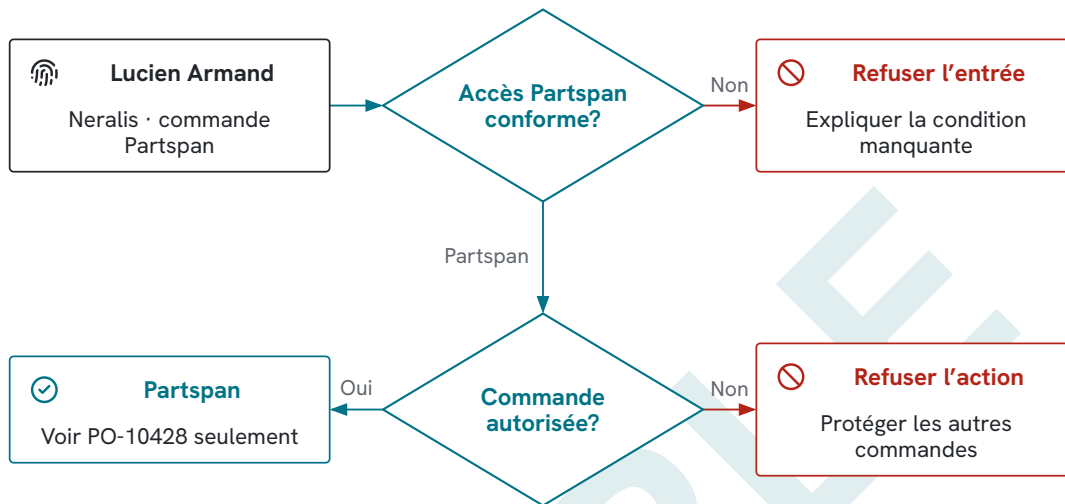


Figure 1 Deux vérifications : entrer dans l'application, puis effectuer l'action.

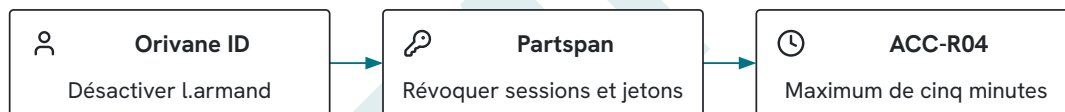


Figure 2 Le retrait d'un accès doit aussi fermer les sessions et désactiver les jetons.

Preuves d'acceptation requises

- ✓ Une tâche autorisée réussit; les ressources sans lien restent refusées.
- ✓ Un utilisateur désactivé ne crée aucun nouvel accès; le délai de fermeture de ses sessions est mesuré.
- ✓ Une panne de connecteur ou d'identité ne rouvre pas l'ancien accès large.

Flux de décision et matrice de politiques

Chaque demande précise l'utilisateur, l'application et l'action souhaitée. Nacre Access vérifie les droits actuels et le contexte, puis achemine la demande vers la seule application autorisée. Celle-ci contrôle les droits sur les données visées. Un identifiant commun permet de suivre ces étapes dans les journaux sans y copier les jetons de session.

PROFIL	CONTEXTE REQUIS	ACCÈS PERMIS
Mila Renaud / employée	Groupe approuvé, authentification forte et appareil géré pour les données internes.	Applications désignées et rôle applicatif propre.
Lucien Armand / Neralis	Répondant désigné, droit temporaire, authentification approuvée et règle d'appareil propre à la ressource.	Espace partenaire seulement; aucune découverte des services internes.
Amira Chen / admin	Identité privilégiée distincte, appareil approuvé, authentification récente et contexte de changement.	Console d'administration désignée; aucun rôle implicite de lecture de données.
ledgerflow-release	Identifiant de service, destinataire du jeton défini et droits limités à l'action requise.	Une interface de service; aucun accès interactif d'employé.
Elias Moreno / reprise	Identité indépendante approuvée, cible limitée et autorisation consignée.	Actions de reprise de la dépendance touchée seulement.

Inconnu ne signifie pas conforme

Si l'état de l'appareil est inconnu, trop ancien ou contradictoire, l'appareil n'est pas considéré comme conforme. La politique précise les accès limités qui restent possibles et leur durée. Les opérations d'administration sont refusées sans les vérifications requises. Une exception peut autoriser une tâche précise jusqu'à une date donnée; elle ne rend pas l'appareil conforme.

Sessions, révocation et pannes

Retirer un accès demande d'agir dans plusieurs systèmes. Désactiver un compte bloque les nouvelles connexions, mais une session ouverte ou un jeton peut encore fonctionner. ACC-R04 mesure la révocation à Nacre Access et à l'application : cinq minutes pour LedgerFlow et Partspan, 60 secondes pour nacre-admin. MillWatch ne peut pas fermer une session active; EX-019 exige donc l'arrêt du connecteur dans les dix minutes.

PANNE OU ÉVÉNEMENT	COMPORTEMENT REQUIS
Utilisateur désactivé	Bloquer les nouvelles connexions, fermer les sessions si possible et révoquer les jetons. Mesurer le délai de retrait complet dans chaque application.
Appareil non conforme	Réévaluer l'accès là où le système le permet et vérifier le comportement des connexions déjà ouvertes.
Connecteur perdu	Utiliser seulement un connecteur sain et autorisé; conserver les limites de destination et consigner la panne.
Service de décision indisponible	Refuser les nouveaux accès sensibles. Les décisions PolicyShelf peu sensibles expirent après 60 secondes; aucun cache pour les privilèges.
Fournisseur d'identité en panne	Utiliser la reprise indépendante pour restaurer le service; ne pas publier un accès réseau sans restriction.

Accès de reprise

Les accès de secours doivent fonctionner même si le service de connexion habituel est en panne. Leur utilisation exige une approbation et déclenche une notification par un canal indépendant. Après l'intervention, les identifiants sont renouvelés et leur utilisation est révisée. La procédure couvre aussi le DNS, la synchronisation de l'heure et les certificats.

Déploiement par groupes et période de transition

Migrer selon les dépendances et les rôles, sans basculer toute l'organisation à une date unique. Le groupe pilote doit inclure un partenaire et un administrateur. Il faut aussi tester le refus d'un appareil non géré et le retrait des accès d'une personne. Un essai limité à l'équipe plateforme ne couvrirait pas ces situations.

GROUPE	CRITÈRES D'ENTRÉE ET DE SORTIE
10 août / Montréal	120 employés et 20 partenaires Neralis; PolicyShelf, ShiftBoard, FieldNotes et Partspan. Sofia Caron accepte A1-A7 avant expansion.
17 août / Services régionaux	1 680 employés et 160 partenaires; 16 autres applications Web. Julien Voss confirme le soutien; plus de 99 % des tâches réussissent sur cinq jours.
24 août / Ingénierie Nacre	580 employés; huit services d'ingénierie et cinq consoles. Amira Chen teste la séparation des droits d'administration et les sessions prolongées.
31 août / Intégration usine	20 employés; MillWatch, BatchTrace Bridge et ForgeLink. Marc Bellamy est responsable d'EX-019-021; retrait des routes le 30 septembre.

Retirer l'ancien accès

Pour chaque application, un responsable fixe la date de retrait de l'ancien accès réseau. Le laisser ouvert permettrait de contourner les nouvelles règles. Avant de le retirer, vérifier qui l'utilise et pour quels services. Après le retrait, confirmer que les anciennes adresses et les anciens protocoles ne permettent plus d'entrer. Tout retour arrière doit être approuvé et limité dans le temps.

Catalogue des essais d'acceptation

ESSAI	EXERCICE	PREUVE REQUISE
A1	Mila Renaud crée la commande LedgerFlow LF-260810-17.	Décision et action applicative corrélées; autres ressources refusées.
A2	Lucien Armand tente de découvrir nacre-admin depuis Partspan.	Service partenaire fonctionnel; noms et destinations internes sans accès élargi.
A3	Utilisateur approuvé, appareil inconnu.	Ressource sensible refusée avec motif utile; soutien capable de diagnostiquer sans contourner.
A4	Désactiver l.armand pendant une session Partspan.	Nouveaux accès bloqués; sessions et jetons mesurés selon l'objectif propre à l'application.
A5	Arrêter acc-mtl-01, puis isoler le service de politique Nacre Access.	Comportement conforme à la matrice; aucune route de repli sans restriction.
A6	Tester les comptes d'administration et de service.	Un jeton d'employé ne peut obtenir les droits d'un administrateur ou d'un service; seules les actions prévues sont permises.
A7	Restaurer la dépendance d'identité.	Reprise indépendante fonctionnelle, journalisée, puis fermée et revue.

Pour chaque essai, consigner la politique, l'application, le profil, l'état de l'appareil, l'heure et les résultats attendus et observés. Les journaux donnent les motifs et un identifiant de suivi, sans jetons ni données personnelles inutiles. Analyser les échecs à la passerelle et dans l'application.

Exploitation et limites de conception

Le centre de services aide les utilisateurs à s'inscrire et analyse les premiers motifs de refus. Les responsables d'applications approuvent les droits, la sécurité autorise les exceptions et l'équipe plateforme maintient les connecteurs et le service de décision. Toute modification qui touche plusieurs équipes doit être examinée ensemble.

Le tableau de bord distingue les pannes d'application, les échecs de connexion, les refus d'accès et les connecteurs défaillants. De nombreux refus peuvent indiquer que la protection fonctionne ou que le déploiement pose problème. Avant d'assouplir une règle, vérifier les applications touchées et les tâches que les utilisateurs arrivent à accomplir.

Décisions requises avant mise en œuvre

- Sofia Caron joint les mesures ACC-R04 avant le 10 août : cinq minutes pour les applications de l'entreprise et 60 secondes pour les privilèges.
- Samir Okafor approuve le rôle de consultation Partspan; les appareils non gérés ne peuvent exporter ni atteindre LedgerFlow.
- Nadia Bellerose accepte la suspension des nouvelles tâches d'administration pendant une panne d'Orivane ID; Elias Moreno autorise la reprise indépendante.
- Marc Bellamy clôt EX-019-021 le 30 septembre après les essais d'arrêt de connecteur pour MillWatch, BatchTrace Bridge et ForgeLink.

Référence et risque résiduel

[NIST SP 800-207](#) éclaire la séparation entre autorisation de ressource et emplacement réseau. Cette conception ne neutralise pas un appareil approuvé compromis, ne répare pas l'autorisation applicative et ne garantit pas une révocation immédiate. Ces limites figurent aux essais et procédures d'incident. Populations et choix sont fictifs.