

Guide utilisateur ProPM Agent

Cette documentation aide les clients Azure à utiliser ProPM Agent sans confusion entre usage quotidien, administration projet, administration plateforme et diagnostic support.

The screenshot shows the ProPM Agent dashboard. At the top, there's a header with the project name 'Azure Bay Hotel & Convention Cent' and a language selector set to 'Français'. Below the header, there's a navigation sidebar on the left with options like 'Tableau de bord', 'Projets', 'Espace de travail', 'Connaissance', 'Agents', 'Rapports & artefacts', 'Journal IA', 'Centre de commande portefeuille', and 'Administration de la plateforme'. The main content area is titled 'Tableau de bord' and features a 'CENTRE DE PILOTAGE PROJET' section with four key metrics: 12 PROJETS, 9 CONNAISSANCE, 8 AGENTS ACTIFS, and 3 SIGNAUX OUVERTS. There are also buttons for 'Ouvrir l'espace de travail' and 'Journal IA'. A right-hand panel shows 'PROJET ACTUEL' and 'CONNAISSANCE' counts.

Export PDF

Télécharger le PDF français

Commencer par le bon parcours

VOTRE SITUATION	OUVREZ D'ABORD	OBJECTIF
Je découvre ProPM Agent	Publics, rôles et périmètres	Choisir le bon parcours de lecture
Je dois me connecter	Démarrage	Accéder à l'application et comprendre les états vides
Je veux voir l'état du projet	Tableau de bord	Lire les métriques, raccourcis et activités récentes

VOTRE SITUATION	OUVREZ D'ABORD	OBJECTIF
Je dois choisir ou créer un projet	Projet actif et création de projet	Fixer le contexte de travail
Je veux ajouter ou retrouver des documents	Connaissance, documents et imports	Téléverser, importer et rechercher des preuves
Je veux interroger l'IA	Agents	Choisir un agent, lancer un run et lire les résultats
Je dois relire un livrable	Documents PM et artefacts	Relire, approuver, télécharger, publier ou ajouter à la connaissance
Je dois auditer une exécution	Journal IA	Retrouver le run et le fournisseur IA effectif
Je dois traiter une alerte	Signaux et notifications	Lire, reporter, fermer ou transformer un signal
Je dois proposer ou approuver une action	Actions et approbations	Comprendre le workflow approved puis executed

Parcours par profil

PROFIL	PAGES PRINCIPALES
Utilisateur métier	Démarrage → Tableau de bord → Connaissance → Agents → Documents PM
Project Manager	Projet actif → Signaux → Actions et approbations → Journal IA
Propriétaire de projet	Contrôle d'accès et rôles → Projets et espace de travail → Gouvernance → Connecteurs
PMO ou direction	Portfolio → Documents PM → Journal IA
Administrateur Azure ou tenant	Administration Azure et Entra → Fournisseur IA → Intégrations plateforme → Licences, plans et mises à jour
Support ou audit	Support, audit et diagnostic → Journal IA → Maintenance, support et FAQ

Chaîne de travail à retenir

Le flux courant est : **projet actif** → **connaissance** → **agent** → **sortie structurée** → **artefact** → **Document PM** → **Download / Publish / Add to knowledge** → **Journal IA**.

Une conversation d'agent ne crée pas automatiquement un document final partagé. Un Document PM doit être relu, gouverné et publié ou ajouté à la connaissance selon les droits et politiques du projet.

Concepts essentiels

TERME	DÉFINITION COURTE
Projet actif	Projet actuellement appliqué aux pages Knowledge, Agents, Documents PM, Signaux et Journal IA
All projects	Portée limitée aux projets déjà accessibles par le même compte
Rattachement projet	Lien qui rend une intégration plateforme utilisable dans un projet donné
Sortie structurée	Résultat d'un run d'agent, distinct d'un document final
Document PM	Livrable projet relu, versionné et gouverné
Fournisseur IA effectif	Fournisseur réellement utilisé par un run, visible dans le Journal IA
Entitlement	Blocage opérationnel lié à licence, rôle, politique, intégration ou santé

Administration Azure et plateforme

Les détails Azure, Entra, fournisseur IA, connecteurs, licences et mises à jour sont séparés du guide utilisateur final :

SUJET	PAGE
Déployer et finaliser l'accès	Administration Azure et Entra
Configurer Save / Validate / Test / Activate	Fournisseur IA
Définir, valider et rattacher les intégrations	Intégrations plateforme
Gérer seats, plan Marketplace et updates	Licences, plans et mises à jour

Support

Pour un incident, fournissez l'URL, le projet actif, l'heure, l'action tentée, le message affiché et les identifiants visibles comme Run ID ou Trace ID. Ne partagez jamais de secret, clé, jeton ou payload sensible.

- [Support, audit et diagnostic](#)
- [Maintenance, support et FAQ](#)
- [Glossaire](#)

Publics, rôles et périmètres

[Accueil](#) · Publics, rôles et périmètres

Objectif

Cette page sert de point d'entrée éditorial. Elle explique quel parcours lire selon votre responsabilité dans ProPM Agent et sépare clairement l'usage quotidien, l'administration projet, l'administration Azure et le support.

Pour qui

PROFIL	USAGE DE CETTE PAGE
Utilisateur métier	Comprendre quelles pages lire pour travailler dans un projet sans détails Azure internes
Propriétaire de projet	Identifier les pages de configuration projet, rôles, connaissance, gouvernance et intégrations
Administrateur Azure ou tenant	Accéder aux pages de déploiement, fournisseur IA, licences, intégrations plateforme et mises à jour
Support ou auditeur	Retrouver les pages de diagnostic, Journal IA, traces et informations à fournir

Les quatre niveaux de documentation

NIVEAU	À UTILISER POUR	À ÉVITER DANS CE NIVEAU
Utilisateur final	Se connecter, choisir un projet, lire le tableau de bord, chercher une preuve, lancer un agent, gérer un Document PM	Variables Azure, secrets, charges JSON, détails d'infrastructure
Propriétaire de projet	Membres, rôles, catégories, intégrations projet, politiques, actions et approbations	Authentification détaillée des connecteurs et secrets
Administrateur Azure et plateforme	Marketplace, Entra, fournisseur IA, licences, intégrations plateforme, mises à jour	Procédures métier quotidiennes trop détaillées
Support et audit	Run ID, Trace ID, fournisseur IA effectif, activité, symptômes et escalade	Secrets, clés, endpoints internes ou payloads sensibles

Parcours recommandé par rôle

RÔLE	COMMENCER PAR	PUIS
Nouvel utilisateur	Démarrage	Interface et navigation, Tableau de bord, Projet actif
Contributeur projet	Connaissance, documents et imports	Agents, Sorties structurées, Documents PM
Project Manager	Projet actif	Signaux et notifications, Actions et approbations
Project Owner	Contrôle d'accès et rôles	Projets et espace de travail, Gouvernance, décisions et actions
PMO ou direction	Portfolio	Journal IA pour la traçabilité si nécessaire
Administrateur tenant	Administration Azure et Entra	Fournisseur IA, Licences et mises à jour
Support client	Support, audit et diagnostic	Journal IA, Maintenance, support et FAQ

Convention sur les libellés UI

Cette documentation utilise le terme français lorsqu'il est clair, puis ajoute le libellé exact de l'interface si celui-ci reste en anglais. Exemple : **Ajouter à la connaissance** ([Add to knowledge](#)), **Tous les projets** ([All projects](#)), **Fournisseur IA effectif** ([Effective AI Provider](#)).

Règles de sécurité documentaire

- Ne copiez jamais de secret, clé, jeton ou mot de passe dans une demande support.
- Ne partagez pas de payload complet si une capture ciblée suffit.
- Masquez les noms de personnes, documents sensibles et données client dans les captures.
- Fournissez plutôt l'URL de la page, l'heure, le projet, le message visible et les identifiants de support affichés.

Suite

- Pour l'usage quotidien, ouvrez [Tableau de bord](#).
- Pour administrer Azure, ouvrez [Administration Azure et Entra](#).

- Pour un incident, ouvrez [Support, audit et diagnostic](#).

Démarrage

Accueil · Démarrage

ProPM Agent
Cockpit de livraison IA

PROJET ACTUEL
Tous les projets
Choisir un projet

Tableau de bord
Projets
Espace de travail
Connaissance
Agents
Rapports & artefacts
Journal IA
Centre de commande portefeuille
Administration de la plateforme

Utilisateur
mock.user@contoso.c...

Tous les projets

Océan

Français

Aide

Santé

Appuyez sur Ctrl+K / ⌘K pour les commandes

Projets
Parcourir et gérer les espaces de travail projet.

Projets de démonstration par défaut installés + Créer un projet

AIDE

Répertoire des projets

La page Projets liste les projets accessibles et permet d'en ouvrir un dans l'espace de travail actif.

Répertoire des projets

Formulaire de création de projet

Identifiant du projet

Nom du projet

Description du projet

Import de projet démo

Rechercher...

Dernier usage

Enregistrer la vue

Exporter

NOM	CRÉATEUR	MON RÔLE	STATUT	CRÉÉ	ACTIONS
Azure Bay Hotel & Convention Center demo-hotel-001 Demo construction program: 220-room upscale hotel, conference center, and wellness facilities in Tunis. Projet de démonstration par défaut	Michael Carter michael.carter@NovaBizLLC.onmicrosoft.com	Project Admin	active	21/04/2026 15:08:04	Espace de travail Supprimer la démo
North Delta Gas Compression & Export Upgrade demo-energy-001 Demo oil & gas capital program: brownfield compression upgrade, shutdown execution, and export reliability improvements. Projet de démonstration par défaut	Jennifer Walker jennifer.walker@NovaBizLLC.onmicrosoft.com	Project Admin	active	20/04/2026 15:08:04	Espace de travail Supprimer la démo

Objectif

Cette page aide un nouvel utilisateur à ouvrir ProPM Agent, se connecter avec Microsoft Entra ID, sélectionner le projet actif et reconnaître les états vides courants.

Pour qui

PROFIL	USAGE DE CETTE PAGE
Utilisateur métier	Première connexion et sélection du projet
Project Manager	Vérifier l'accès au bon projet
Propriétaire de projet	Orienter les nouveaux membres
Administrateur Azure	Lire seulement le renvoi vers la page admin si l'URL ou Entra n'est pas prêt

Avant de commencer

- Vous avez reçu l'URL ProPM Agent de votre organisation.
- Vous disposez d'un compte Microsoft Entra ID autorisé.
- Vous devez être membre d'au moins un projet ou disposer du droit de créer un projet.
- Vous utilisez un navigateur moderne.

Si l'application n'est pas encore déployée ou si l'accès Entra n'est pas finalisé, l'administrateur doit d'abord suivre [Administration Azure et Entra](#).

Première connexion

1. Ouvrez l'URL ProPM Agent fournie par votre organisation.
2. Sélectionnez **Sign in** ou le bouton de connexion Microsoft.
3. Choisissez le compte professionnel attendu.
4. Acceptez le consentement si votre organisation l'autorise et si l'écran le demande.
5. Attendez le retour dans ProPM Agent.
6. Vérifiez que votre nom ou profil apparaît dans la barre supérieure.
7. Sélectionnez un projet actif si l'application le demande.

Sélectionner ou créer le premier projet

1. Ouvrez le sélecteur de projet ou la page **Projects**.
2. Sélectionnez le projet fourni par votre équipe.
3. Si vous êtes autorisé à créer un projet, utilisez **Create project**.
4. Vérifiez ensuite le projet actif dans la barre supérieure.
5. Ouvrez [Tableau de bord](#) pour confirmer que les données du projet s'affichent.

États vides courants

ÉTAT	SIGNIFICATION	ACTION RECOMMANDÉE
Aucun projet disponible	Votre compte n'est pas encore membre d'un projet	Demandez au Project Owner de vous ajouter
Aucun projet actif	Vous êtes connecté mais aucun contexte n'est sélectionné	Sélectionnez un projet

ÉTAT	SIGNIFICATION	ACTION RECOMMANDÉE
Page vide avec message de rôle	Votre rôle ne permet pas l'action	Demandez le rôle adapté
Connexion en boucle	Consentement, tenant ou configuration Entra à vérifier	Contactez l'administrateur tenant
Boutons grisés	Rôle, politique ou intégration insuffisants	Ouvrez Contrôle d'accès et rôles

Résultat attendu

- Vous êtes connecté à ProPM Agent.
- Un projet actif est visible.
- Le tableau de bord charge les données du projet.
- Vous savez qui contacter si l'accès ou le rôle manque.

Si cela ne fonctionne pas

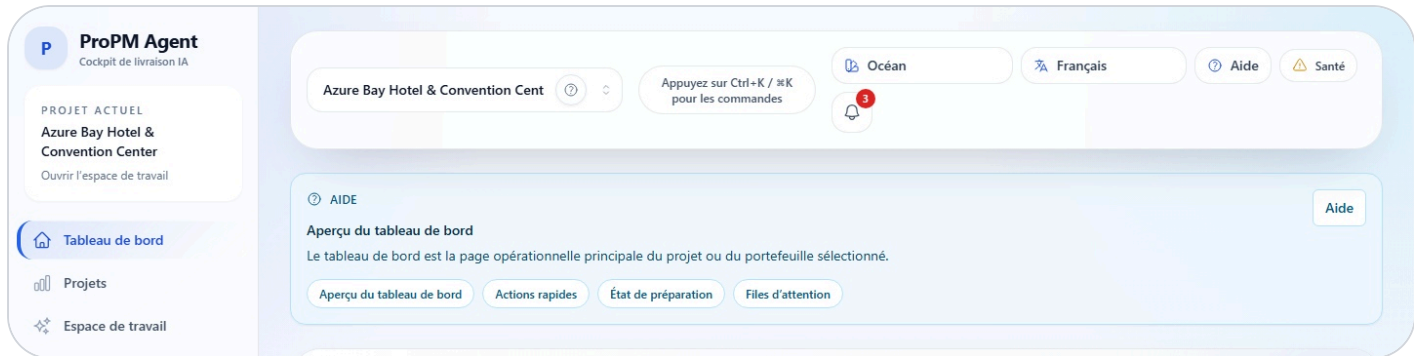
SYMPTÔME	CAUSE PROBABLE	ACTION RECOMMANDÉE
URL inaccessible	Déploiement ou réseau non prêt	Contactez l'administrateur Azure
Microsoft refuse la connexion	Compte, tenant ou consentement incorrect	Contactez l'administrateur tenant
Aucun projet n'apparaît	Vous n'avez pas encore été ajouté	Contactez le Project Owner
Une exécution IA ne démarre pas	Fournisseur IA ou santé plateforme à vérifier	Ouvrez Support, audit et diagnostic

Suite

- Pour découvrir l'interface, ouvrez [Interface et navigation](#).
- Pour choisir le contexte de travail, ouvrez [Projet actif et création de projet](#).
- Pour un incident, ouvrez [Support, audit et diagnostic](#).

Interface et navigation

Accueil · Interface et navigation



Objectif

Cette page explique comment se repérer dans ProPM Agent : navigation principale, projet actif, centre de notifications, indicateur de santé, palette de commandes, langue, thème et aide.

Pour qui

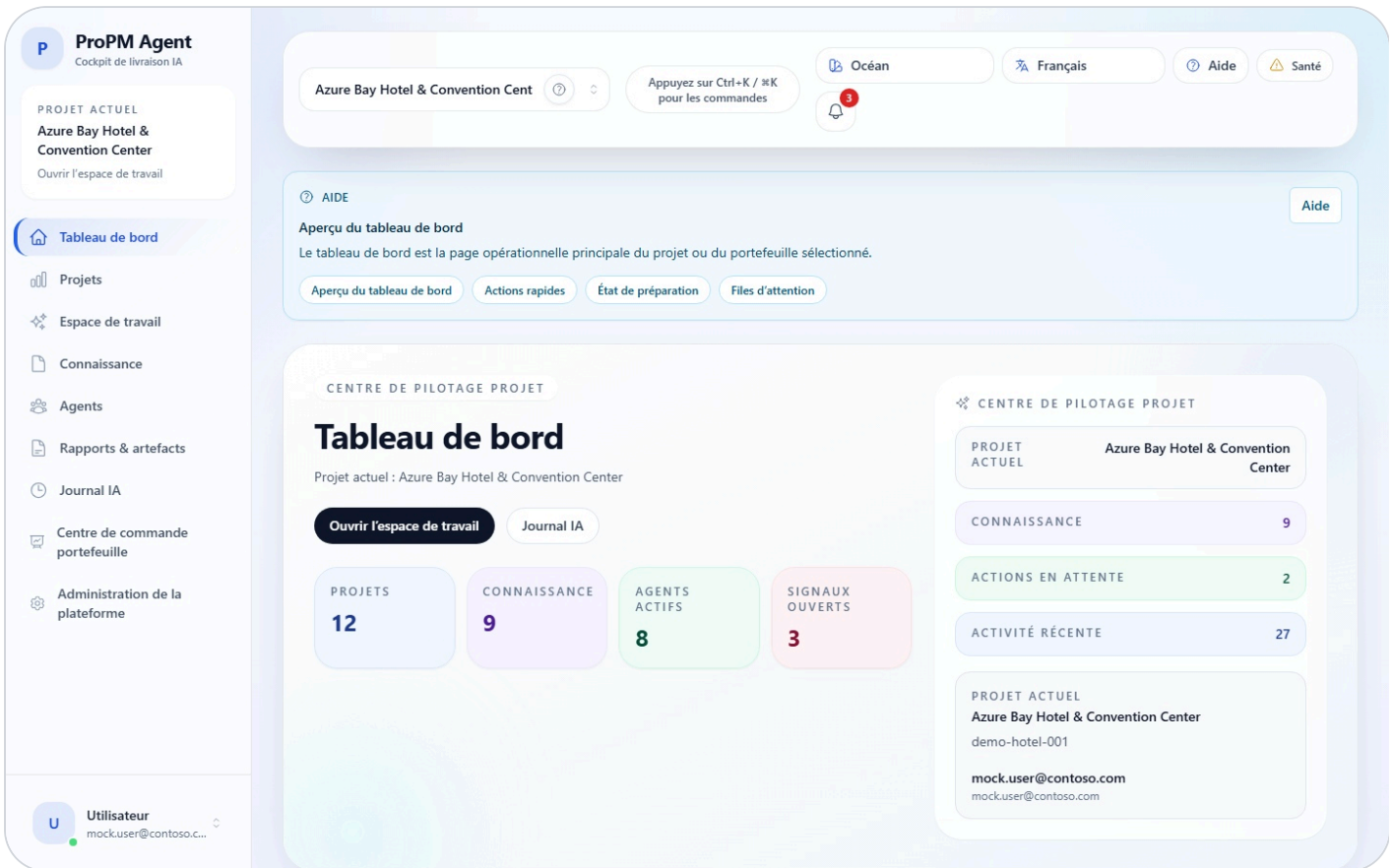
PROFIL	USAGE DE CETTE PAGE
Utilisateur métier	Trouver la bonne page et comprendre les états vides
Project Manager	Changer de projet avant d'agir et suivre les notifications
Propriétaire de projet	Diagnostiquer rapidement rôle, projet, santé ou intégration
Support	Collecter les premiers indices sans entrer dans l'administration technique

Avant de commencer

- Vous êtes connecté à ProPM Agent.
- Votre compte a accès à au moins un projet.
- Vous savez quel projet vous devez consulter.

Vue d'ensemble

ZONE	USAGE PRINCIPAL
Barre latérale	Ouvrir les grands domaines : Dashboard, Projets, Connaissance, Agents, Documents PM, Journal IA, Portfolio, Administration
Barre supérieure	Changer de projet, ouvrir la palette, consulter notifications, santé, langue, thème et aide
Surface centrale	Afficher les données du projet actif ou de l'administration choisie
États vides	Signaler un projet absent, un rôle insuffisant, un filtre actif ou une donnée non encore créée



Ouvrir la bonne surface

BESOIN	PAGE À OUVRIR
Lire l'état général du projet	Tableau de bord
Sélectionner ou créer un projet	Projet actif et création de projet

BESOIN	PAGE À OUVRIR
Ajouter ou rechercher des documents	Connaissance, documents et imports
Lancer un run IA	Agents
Relire un livrable	Documents PM et artefacts
Auditer un run	Journal IA
Traiter un signal	Signaux et notifications
Proposer ou approuver une action	Actions et approbations

Changer de projet actif

1. Ouvrez le sélecteur de projet dans la barre supérieure.
2. Recherchez le projet par nom si la liste est longue.
3. Sélectionnez le projet voulu.
4. Vérifiez que son nom apparaît dans la barre supérieure.
5. Ouvrez **Tableau de bord** pour confirmer que les métriques correspondent.
6. Reprenez ensuite votre action dans **Connaissance, Agents, Documents PM, Signaux** ou **Journal IA**.

Impact du projet actif

SURFACE	EFFET DU PROJET ACTIF
Connaissance	Limite les documents, imports et résultats de recherche au projet
Agents	Lance les runs dans le contexte du projet sélectionné
Documents PM	Affiche les artefacts et livrables du projet
Journal IA	Filtre les runs et activités du projet
Signaux	Affiche les alertes, digests, brouillons et actions du projet

[All projects](#) n'est pas un projet sélectionnable dans la barre supérieure. C'est une portée contrôlée, par exemple pour certains agents personnalisés, limitée aux projets déjà accessibles par le même compte.

Utiliser la palette de commandes

1. Appuyez sur **Ctrl+K** sous Windows/Linux ou **Cmd+K** sous macOS.
2. Saisissez le nom d'une page ou d'une action.
3. Sélectionnez l'entrée voulue.
4. Vérifiez le projet actif si vous ouvrez une page projet.

La palette accélère la navigation, mais elle ne donne pas de droits supplémentaires.

Utiliser le centre de notifications

1. Ouvrez l'icône de cloche dans la barre supérieure.
2. Lisez les notifications non lues.
3. Sélectionnez une notification pour ouvrir la page liée, si une navigation est fournie.
4. Utilisez **Mark all read** ou **Marquer tout comme lu** pour vider le compteur sans supprimer l'historique local.
5. Utilisez **Clear** ou **Tout effacer** uniquement si vous n'avez plus besoin de la liste locale.
6. Si la notification ouvre une page vide, vérifiez le projet actif et vos droits.

Comprendre l'indicateur de santé

ÉTAT OU INDICE	LECTURE PRATIQUE	ACTION RECOMMANDÉE
API saine	Les services répondent	Continuer le travail normal
API dégradée	Certaines pages peuvent charger lentement ou rester vides	Patienter, relever l'heure et réessayer
Temps réel dégradé	Notifications et mises à jour peuvent arriver en retard	Rafraîchir la page si nécessaire
Auth à vérifier	La session ou le tenant demande une attention	Revenir à Démarrage
Latence élevée	Les actions peuvent sembler lentes	Éviter les doubles clics et attendre la fin des traitements
Message bloquant	Une page peut être indisponible si l'API live n'est pas saine	Ouvrir Support, audit et diagnostic

Quand escalader

Escaladez au support ou à l'administrateur lorsque l'indicateur de santé reste dégradé après rafraîchissement, lorsqu'un run n'est pas créé dans le Journal IA, ou lorsqu'une action critique reste bloquée malgré un projet actif et un rôle attendu.

Langue, thème et aide

- La langue modifie l'interface et les libellés disponibles, pas les données projet.
- Le thème clair/sombre est une préférence de confort locale.
- L'aide ouvre les repères intégrés et les liens vers la documentation.
- Certaines préférences comme le projet récent, la langue, le thème ou l'état lu des notifications peuvent rester locales au navigateur.

Résultat attendu

- Vous savez quel projet est actif.
- Vous pouvez ouvrir la bonne page sans parcourir toute la navigation.
- Vous savez distinguer notification, état vide, rôle insuffisant et santé dégradée.

Suite

- [Tableau de bord](#)
- [Projet actif et création de projet](#)
- [Support, audit et diagnostic](#)

Tableau de bord

Accueil · Tableau de bord

ProPM Agent
Cockpit de livraison IA

PROJET ACTUEL
Azure Bay Hotel & Convention Center
Ouvrir l'espace de travail

Tableau de bord

- Projets
- Espace de travail
- Connaissance
- Agents
- Rapports & artefacts
- Journal IA
- Centre de commande portefeuille
- Administration de la plateforme

Utilisateur
mock.user@contoso.c...

Azure Bay Hotel & Convention Cent

Appuyez sur Ctrl+K / ⌘K pour les commandes

Océan

Français

Aide

Santé

AIDE

Aperçu du tableau de bord

Le tableau de bord est la page opérationnelle principale du projet ou du portefeuille sélectionné.

Aperçu du tableau de bord

Actions rapides

État de préparation

Files d'attente

CENTRE DE PILOTAGE PROJET

Tableau de bord

Projet actuel : Azure Bay Hotel & Convention Center

Ouvrir l'espace de travail

Journal IA

Métrique	Valeur
PROJETS	12
CONNAISSANCE	9
AGENTS ACTIFS	8
SIGNAUX OUVERTS	3

CENTRE DE PILOTAGE PROJET

PROJET ACTUEL: Azure Bay Hotel & Convention Center

CONNAISSANCE: 9

ACTIONS EN ATTENTE: 2

ACTIVITÉ RÉCENTE: 27

PROJET ACTUEL: Azure Bay Hotel & Convention Center
demo-hotel-001

mock.user@contoso.com

Ordre de lecture du tableau de bord

Commencez par le contexte projet, puis lisez l'état, l'activité et les raccourcis disponibles.

1 Projet actif

Toutes les métriques, runs et documents dépendent du projet sélectionné.

2 Métriques projet

Lisez avancement, blocages, risques et signaux de preuves manquantes.

3 Santé et alertes

Vérifiez santé plateforme, notifications et messages avant diagnostic.

4 Activité récente

Relisez runs, imports, documents et actions pour comprendre les changements.

5 Raccourcis d'action

Ouvrez connaissance, agents, Documents PM ou actions depuis le contexte courant.

Si la page paraît vide, vérifiez d'abord le projet actif et votre rôle

Objectif

Le tableau de bord donne une synthèse du projet actif : activité récente, connaissance, agents, Documents PM, signaux, actions et raccourcis vers les pages de travail.

Pour qui

PROFIL	USAGE DE CETTE PAGE
Utilisateur métier	Comprendre l'état du projet et ouvrir la bonne page
Project Manager	Prioriser les documents, signaux, actions et runs récents
Propriétaire de projet	Vérifier si le projet est prêt à être utilisé
Administrateur	Diagnostiquer seulement si l'état indique un problème global

Avant de commencer

- Vous êtes connecté à ProPM Agent.
- Un projet actif est sélectionné, sauf si vous consultez volontairement l'état vide.
- Votre rôle vous donne accès au projet.

Lire le tableau de bord

1. Ouvrez la page **Dashboard** ou **Tableau de bord**.
2. Vérifiez le nom du **projet actif** dans la barre supérieure.
3. Lisez les cartes de synthèse : agents, documents, runs, Documents PM, signaux et actions.
4. Consultez l'activité récente pour repérer ce qui a changé depuis votre dernière visite.
5. Utilisez les raccourcis vers **Workspace**, **Knowledge**, **Agents**, **PM Docs** ou **AI Log** selon la prochaine action.

Quand aucun projet n'est sélectionné

ÉTAT AFFICHÉ	SIGNIFICATION	ACTION RECOMMANDÉE
Aucun projet actif	Les pages projet n'ont pas de contexte	Sélectionnez un projet depuis le sélecteur ou ouvrez Projet actif
Aucun projet disponible	Votre compte n'a pas encore accès à un projet	Demandez à un Project Owner de vous ajouter
Accès refusé	Vous êtes connecté mais pas autorisé sur cette surface	Vérifiez votre rôle avec le propriétaire du projet

Interpréter les métriques

ZONE	LECTURE PRATIQUE
Agents	Agents disponibles ou exécutions récentes dans le projet actif
Documents	Contenus indexés, en cours d'ingestion ou en erreur
Runs	Exécutions d'agents et activité IA récente
Drafts / Finals	Documents PM en brouillon, en revue ou finalisés
Signaux	Alertes ou opportunités à traiter
Actions	Actions proposées, approuvées, bloquées ou exécutées

Utiliser l'activité récente

L'activité récente sert à répondre à trois questions : qu'est-ce qui vient d'être importé, quelle exécution a produit un résultat, et quelle action attend une décision. Si une entrée semble incohérente, ouvrez [Journal IA](#) pour vérifier le run et le fournisseur IA effectif.

Si cela ne fonctionne pas

SYMPTÔME	CAUSE PROBABLE	ACTION RECOMMANDÉE
Le tableau de bord reste vide	Aucun projet actif ou rôle insuffisant	Sélectionnez un projet puis vérifiez votre rôle
Les chiffres semblent anciens	Données non rafraîchies ou ingestion en cours	Patiencez, puis ouvrez la page concernée
Une carte est visible mais non cliquable	Permission manquante	Demandez le rôle adapté au Project Owner
Une erreur globale est affichée	Santé API ou fournisseur non opérationnel	Relevez le message et ouvrez Support, audit et diagnostic

Suite

- Pour choisir ou créer un projet, ouvrez [Projet actif et création de projet](#).
- Pour alimenter le projet, ouvrez [Connaissance, documents et imports](#).
- Pour traiter les alertes, ouvrez [Signaux et notifications](#).

Projet actif et création de projet

Accueil · Projet actif et création de projet

ProPM Agent
Cockpit de livraison IA

PROJET ACTUEL
Tous les projets
Choisir un projet

Tableau de bord
Projets
Espace de travail
Connaissance
Agents
Rapports & artefacts
Journal IA
Centre de commande portefeuille
Administration de la plateforme

Utilisateur
mock.user@contoso.c...

Tous les projets

Appuyez sur Ctrl+K / ⌘K pour les commandes

Océan Français Aide Santé

Projets Projets de démonstration par défaut installés + Créer un projet

Parcourir et gérer les espaces de travail projet.

AIDE Aide

Répertoire des projets
La page Projets liste les projets accessibles et permet d'en rouvrir un dans l'espace de travail actif.

Répertoire des projets Formulaire de création de projet Identifiant du projet Nom du projet Description du projet Import de projet démo

Rechercher... Dernier usage Enregistrer la vue Exporter

NOM	CRÉATEUR	MON RÔLE	STATUT	CRÉÉ	ACTIONS
Azure Bay Hotel & Convention Center demo-hotel-001 Demo construction program: 220-room upscale hotel, conference center, and wellness facilities in Tunis. Projet de démonstration par défaut	Michael Carter michael.carter@NovaBizLLC.onmicrosoft.com	Project Admin	active	21/04/2026 15:08:04	Espace de travail Supprimer la démo
North Delta Gas Compression & Export Upgrade demo-energy-001 Demo oil & gas capital program: brownfield compression upgrade, shutdown execution, and export reliability improvements. Projet de démonstration par défaut	Jennifer Walker jennifer.walker@NovaBizLLC.onmicrosoft.com	Project Admin	active	20/04/2026 15:08:04	Espace de travail Supprimer la démo

Objectif

Cette page explique comment sélectionner le projet actif, créer un nouveau projet et vérifier que les pages Knowledge, Agents, Documents PM et Journal IA utilisent le bon contexte.

Pour qui

PROFIL	USAGE DE CETTE PAGE
Utilisateur métier	Sélectionner le bon projet avant de travailler
Project Manager	Créer un projet lorsque le rôle le permet
Propriétaire de projet	Initialiser le projet et déléguer les premiers accès
Support	Vérifier qu'un état vide n'est pas simplement lié au mauvais projet

Avant de commencer

- Vous êtes connecté avec un compte Microsoft Entra ID autorisé.
- Votre compte a accès à au moins un projet, ou dispose du droit de créer un projet.
- Si vous ne voyez aucun projet attendu, contactez le propriétaire de projet.

Sélectionner un projet actif

1. Ouvrez le sélecteur de projet dans la barre supérieure.
2. Recherchez le projet par nom si la liste est longue.
3. Sélectionnez le projet voulu.
4. Vérifiez que le nom du projet s'affiche dans la barre supérieure.
5. Ouvrez **Tableau de bord** ou **Workspace** pour confirmer que les données correspondent.

Créer un projet

1. Ouvrez **Projects** ou **Projets**.
2. Sélectionnez **Create project** si le bouton est disponible.
3. Renseignez le nom, la description et les paramètres demandés.
4. Choisissez la langue de données par défaut si le champ est proposé.
5. Ajoutez les langues additionnelles uniquement si le projet contient réellement des sources multilingues.
6. Validez la création.
7. Vérifiez que le projet devient disponible dans la liste et peut être sélectionné comme projet actif.

Résultat attendu

- Le projet apparaît dans la liste des projets.
- Le projet actif est visible dans la barre supérieure.
- Le tableau de bord affiche les données du projet sélectionné.
- Les pages **Connaissance**, **Agents**, **Documents PM**, **Signaux** et **Journal IA** s'ouvrent dans ce contexte.

Comprendre **All projects**

All projects ne désigne pas un super-projet. Ce libellé indique une portée disponible sur tous les projets auxquels le même compte a déjà accès. Il ne contourne ni les rôles, ni les permissions, ni les limites tenant.

Projet mémorisé localement

ProPM Agent peut mémoriser localement le dernier projet actif dans le navigateur. Si vous changez de navigateur, d'appareil ou de profil utilisateur, vous pouvez devoir sélectionner à nouveau le projet.

Si cela ne fonctionne pas

SYMPTÔME	CAUSE PROBABLE	ACTION RECOMMANDÉE
Le bouton de création est absent	Rôle insuffisant	Demandez le rôle adapté au Project Owner
Le projet n'apparaît pas	Vous n'êtes pas membre du projet	Demandez l'ajout au projet
Les pages projet restent vides	Aucun projet actif	Sélectionnez le projet dans la barre supérieure
Les données ne correspondent pas	Mauvais projet actif	Changez de projet puis rechargez la page
Certains boutons sont grisés	Rôle ou politique insuffisante	Ouvrez Contrôle d'accès et rôles

Suite

- Pour ajouter des membres, ouvrez [Contrôle d'accès et rôles](#).
- Pour alimenter le projet, ouvrez [Connaissance, documents et imports](#).
- Pour vérifier la synthèse, ouvrez [Tableau de bord](#).

Connaissance, documents et imports

Accueil · Connaissance, documents et imports

ProPM Agent
Cockpit de livraison IA

PROJET ACTUEL
Azure Bay Hotel & Convention Center
Ouvrir l'espace de travail

Tableau de bord
Projets
Espace de travail
Connaissance
Agents
Rapports & artefacts
Journal IA
Centre de commande portefeuille
Administration de la plateforme

Utilisateur
mockuser@contoso.c...

Azure Bay Hotel & Convention Cent ⓘ

Appuyez sur Ctrl+K / ⌘K pour les commandes

Océan

Français

Aide

Santé

Connaissance

Preuves projet préchargées, états d'ingestion de démonstration et recherche contextuelle pour Azure Bay Hotel & Convention Center

AIDE

Aperçu de Knowledge

La page Knowledge permet d'importer, téléverser, parcourir et rechercher la connaissance du projet.

Aperçu de Knowledge Téléversement de document Téléverser un fichier local Sources d'import Importer depuis une source approuvée Recherche de connaissance

Comment interpréter les statuts et métadonnées de Knowledge

Indexed signifie recherchable. Ingesting signifie que l'élément existe mais que la recherche peut arriver avec un délai. et Failed signifie qu'un support ou une nouvelle tentative est nécessaire. Source label et source system aident à juger la provenance, tandis que Trace ID sert surtout de repère support et audit plutôt que de clé fonctionnelle au quotidien.

Le mode démo conserve aussi le périmètre projet pour la connaissance. Utilisez les documents préchargés, simulez un téléversement, puis recherchez des extraits étayés avant de réutiliser les contenus ailleurs.

Rechercher dans la connaissance projet préchargée ⓘ

Rechercher par nom de fichier, catégorie ou statut... **Rechercher**

Examinez les extraits, liens sources et indices de fraîcheur avant de transformer la preuve en artefacts.

Aucun résultat pour le moment.

Rechercher des documents...

General 6 affichés

Téléverser un document de démonstration

Actualiser la bibliothèque

Objectif

Cette page explique comment alimenter la connaissance du projet, vérifier l'indexation, importer depuis une source approuvée et lire les résultats de recherche avec citations.

Pour qui

PROFIL	USAGE DE CETTE PAGE
Contributeur	Téléverser des documents et vérifier leur statut
Project Manager	Importer depuis une source approuvée et contrôler la fraîcheur
Lecteur ou auditeur	Rechercher une preuve et lire les citations
Administrateur	Intervenir seulement si un connecteur ou fournisseur d'ingestion est bloqué

Avant de commencer

- Un projet actif est sélectionné.
- Votre rôle autorise le téléversement, l'import ou la recherche.
- Les documents ne contiennent pas d'informations qui ne doivent pas être partagées dans le projet.

Téléverser un document

1. Ouvrez **Knowledge** ou **Connaissance**.
2. Sélectionnez **Upload** ou **Téléverser**.
3. Choisissez le fichier à ajouter.
4. Renseignez la catégorie ou les métadonnées demandées.
5. Lancez l'envoi.
6. Vérifiez que le document apparaît dans la liste.
7. Attendez que le statut passe à **Indexed** avant de l'utiliser comme preuve.

Importer depuis une source approuvée

1. Ouvrez **Knowledge**.
2. Sélectionnez l'action d'import si elle est disponible.
3. Choisissez la source approuvée, par exemple SharePoint, Jira, Confluence, Azure DevOps ou Blob selon votre environnement.
4. Sélectionnez le périmètre proposé par l'interface.
5. Lancez l'import.
6. Ouvrez l'historique d'import pour suivre les éléments importés, ignorés ou en erreur.

Comprendre les statuts

STATUT	SIGNIFICATION	ACTION RECOMMANDÉE
Indexed	Le contenu est prêt pour la recherche et les agents	Utilisez le document dans vos recherches ou runs
Ingesting	Le document est en cours de traitement	Patientez puis rafraîchissez la liste
Failed	Le traitement a échoué	Vérifiez le format, le contenu, la source et contactez le support si nécessaire

STATUT	SIGNIFICATION	ACTION RECOMMANDÉE
Not visible	Le document n'est pas dans le projet actif	Vérifiez le projet actif, les filtres et vos droits

Rechercher une preuve

1. Ouvrez **Knowledge**.
2. Saisissez une question, un terme métier ou un identifiant de document.
3. Filtrez par catégorie, source ou fraîcheur si les filtres sont disponibles.
4. Ouvrez un résultat pertinent.
5. Lisez le snippet, la citation, le score, le `source label` et le `source system` si affichés.
6. Si la preuve est destinée à une décision, vérifiez que la source est récente et cohérente avec le contexte.

Résultat attendu

- Les documents importants sont visibles dans le projet actif.
- Les documents exploitables sont au statut **Indexed**.
- Les recherches affichent des citations et sources compréhensibles.
- Les agents peuvent s'appuyer sur les documents indexés.

Si cela ne fonctionne pas

SYMPTÔME	CAUSE PROBABLE	ACTION RECOMMANDÉE
Le téléversement est refusé	Format, taille ou rôle non autorisé	Vérifiez le message et demandez le rôle adapté
Le statut reste Ingesting	Traitement encore en cours ou file d'attente	Patientez puis rafraîchissez
Le statut passe Failed	Fichier illisible, source inaccessible ou contenu non exploitable	Essayez un fichier plus simple ou contactez le support
Les résultats sont hors sujet	Mauvais projet, filtre trop large ou documents obsolètes	Vérifiez le projet actif et affinez la recherche

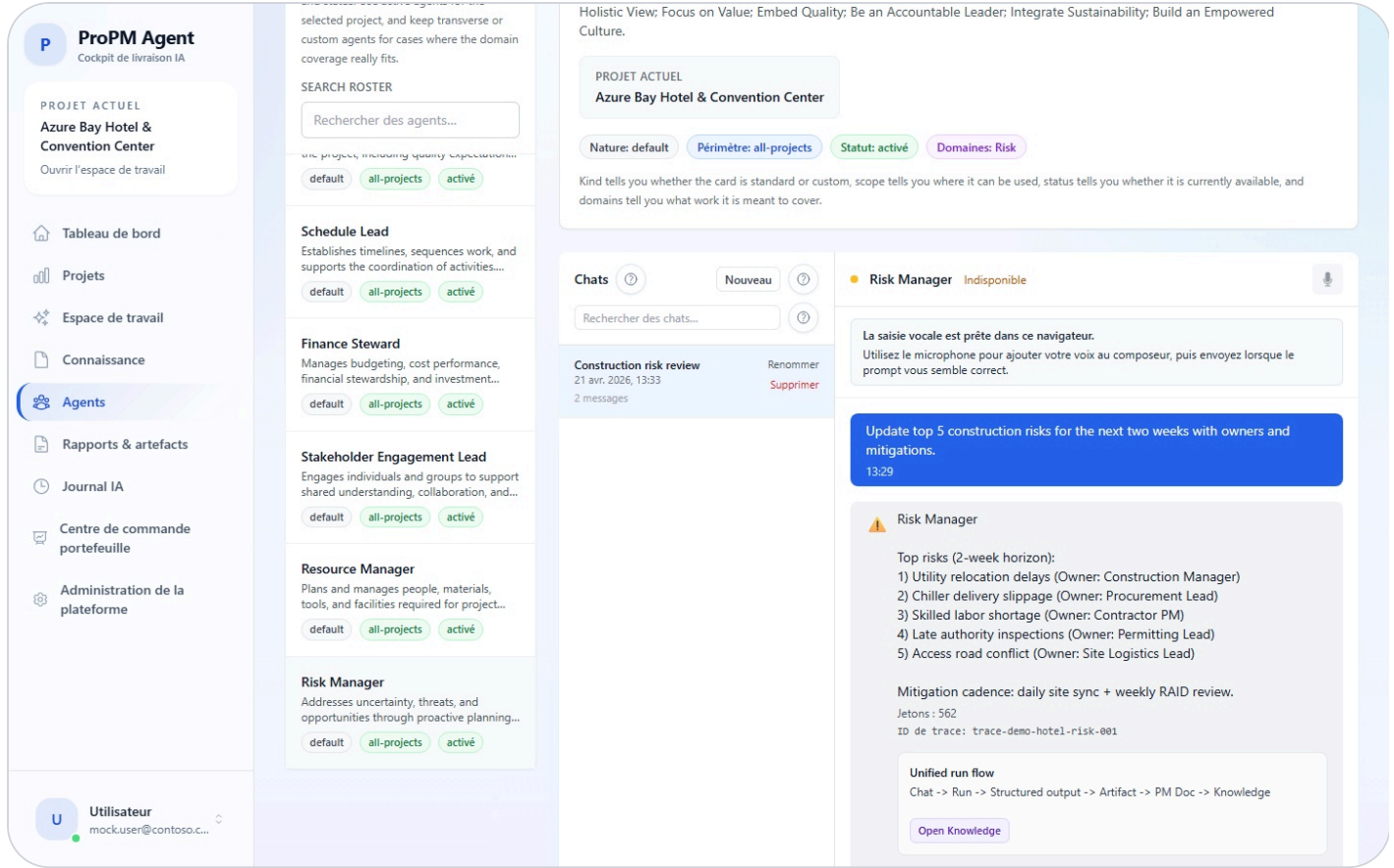
SYMPTÔME	CAUSE PROBABLE	ACTION RECOMMANDÉE
Une source d'import est absente	Fournisseur non rattaché au projet	Demandez au Project Owner de vérifier les intégrations projet

Suite

- Pour interroger les documents, ouvrez [Agents](#).
- Pour lire correctement les citations, ouvrez [Sorties structurées, preuves et fraîcheur](#).
- Pour un problème d'import avancé, ouvrez [Support, audit et diagnostic](#).

Agents

Accueil · Agents



Objectif

Cette page explique comment choisir un agent, lancer une exécution, comprendre les sessions locales et créer un agent personnalisé lorsque votre rôle le permet.

Pour qui

PROFIL	USAGE DE CETTE PAGE
Contributeur	Lancer un agent standard et lire la réponse
Project Manager	Choisir l'agent adapté au besoin métier
Propriétaire de projet	Encadrer les agents personnalisés et leur portée
Auditeur	Comprendre qu'un run doit être vérifié dans le Journal IA

Avant de commencer

- Un projet actif est sélectionné.
- La connaissance utile au projet est indexée.
- Votre rôle autorise l'exécution d'agents ou la création d'agents personnalisés.

Choisir un agent standard

BESOIN	AGENT À PRIVILÉGIÉ
Coordonner une analyse transverse	Orchestrator
Relire décisions, politiques ou approbations	Governance
Clarifier périmètre, livrables ou exigences	Scope
Analyser planning, jalons ou dépendances	Schedule
Suivre budget, coûts ou écarts financiers	Finance
Préparer communication et parties prenantes	Stakeholders
Examiner capacité, charge ou ressources	Resources
Identifier risques, problèmes et plans de réponse	Risk

Lancer un run d'agent

1. Ouvrez **Agents**.
2. Vérifiez le projet actif.
3. Sélectionnez l'agent adapté.
4. Rédigez une demande précise avec l'objectif, le contexte et le format attendu.
5. Ajoutez les documents ou références utiles si l'interface le propose.
6. Lancez le run.
7. Lisez la réponse, les citations, la fraîcheur et le niveau de confiance.
8. Ouvrez le lien vers le **Journal IA** si vous devez auditer l'exécution.

Résultat attendu

- Le run produit une réponse structurée ou une synthèse exploitable.

- Les preuves et citations sont visibles lorsque le modèle s'appuie sur la connaissance.
- Les actions aval disponibles sont affichées, par exemple copier, ouvrir l'artefact, créer un Document PM ou consulter le Journal IA.

Comprendre les sessions locales

Les sessions de chat peuvent être conservées localement dans le navigateur. Elles ne constituent pas une archive centrale partagée. Un changement de navigateur, d'appareil ou de profil peut donc afficher un historique différent.

Créer un agent personnalisé

1. Ouvrez **Agents**.
2. Sélectionnez l'action de création d'agent personnalisé si elle est disponible.
3. Donnez un nom clair et un objectif métier.
4. Choisissez la portée : projet courant ou **All projects** si votre rôle l'autorise.
5. Décrivez les consignes, sources et limites d'usage.
6. Enregistrez l'agent.
7. Lancez un premier test sur une demande simple.
8. Supprimez ou désactivez l'agent s'il ne doit plus être utilisé.

Points d'attention

- Une réponse d'agent n'est pas automatiquement un Document PM final.
- Une sortie sans preuve doit être relue avec prudence.
- La saisie vocale est une option de confort dépendante du navigateur.
- Pour une décision externe, relisez les preuves et ouvrez [Documents PM et artefacts](#) si un livrable doit être gouverné.

Si cela ne fonctionne pas

SYMPTÔME	CAUSE PROBABLE	ACTION RECOMMANDÉE
Aucun agent n'est disponible	Rôle insuffisant ou projet non sélectionné	Vérifiez le projet actif et votre rôle

SYMPTÔME	CAUSE PROBABLE	ACTION RECOMMANDÉE
La réponse ignore les documents	Documents non indexés ou question trop vague	Vérifiez la connaissance et reformulez
Le run échoue	Fournisseur IA non opérationnel ou limite temporaire	Ouvrez Journal IA puis contactez le support si nécessaire
L'agent personnalisé est invisible	Portée ou droits insuffisants	Vérifiez la portée et les permissions

Suite

- Pour interpréter les preuves, ouvrez [Sorties structurées, preuves et fraîcheur](#).
- Pour transformer un résultat en livrable, ouvrez [Documents PM et artefacts](#).
- Pour auditer le fournisseur effectif, ouvrez [Journal IA](#).

Sorties structurées, preuves et fraîcheur

[Accueil](#) · Sorties structurées, preuves et fraîcheur

make procurement and schedule owners explicit before the first controls review.
Responsable: Procurement Lead Niveau: program Échéance: 2026-01-13

Hypothèses

- Authority inspection slots remain available through the planned enabling-works window.

Informations manquantes

- Confirm final sponsor attendance and decision authority for the kickoff SteerCo.

Points de vigilance

- Long-lead equipment exposure should remain visible until procurement awards are contractually locked.

Preuves

Project Charter

blob://demo/demo-hotel-001/01-project-charter.md

Récent Autorité 5

Authorize and govern the delivery of a 220-room upscale urban hotel, conference center, and wellness facilities.

Système: Knowledge

Master Schedule

blob://demo/demo-hotel-001/04-master-schedule.md

Vieillissant Autorité 4

Commissioning complete remains targeted for 2028-03-15 with a recovery trigger when SPI < 0.95.

Système: Schedule

Relire une sortie structurée avant réutilisation

Suivez les étapes dans l'ordre : chaque sortie IA reste un brouillon tant que la relecture humaine n'est pas terminée.

1

Résumé et constats

Lisez le message principal, puis distinguez les faits vérifiables de l'interprétation IA.

2

Décisions à prendre

Repérez ce qui demande approbation, arbitrage, revue projet ou validation d'un responsable.

3

Preuves et citations

Ouvrez les sources citées et vérifiez qu'elles soutiennent réellement la conclusion.

4

Fraîcheur

Classez les informations avant usage : Récent Vieillissant Ancien Conflit

5

Confiance

Utilisez le score comme un signal de priorisation, jamais comme une approbation automatique.

6

Informations manquantes

Complétez la connaissance, demandez une source ou gardez la réponse en exploration.

7

Actions aval

Choisissez seulement après vérification : Document PM, Journal IA, action d'approbation ou suivi projet.

Relecture humaine obligatoire avant publication

Aucune sortie IA ne doit devenir un livrable final sans contrôle des preuves, du contexte et de la décision.

Objectif

Cette page explique comment relire une sortie structurée produite par un agent avant de l'utiliser dans une décision, un Document PM, une publication ou une action gouvernée.

Pour qui

PROFIL	USAGE DE CETTE PAGE
Utilisateur métier	Lire une réponse IA sans la surinterpréter
Project Manager	Vérifier preuves, fraîcheur, confiance et informations manquantes

PROFIL	USAGE DE CETTE PAGE
Propriétaire de projet	Décider si une revue, un Document PM ou une action gouvernée est nécessaire
Auditeur ou support	Comprendre les repères de traçabilité et le lien vers le Journal IA

Avant de commencer

- Un projet actif est sélectionné.
- La sortie vient d'un run d'agent ou d'un flux de revue identifié.
- Vous avez accès aux preuves ou au Journal IA si l'analyse demande une traçabilité.

Lire une sortie structurée

1. Lisez le **Résumé** pour comprendre le message principal.
2. Lisez les **Constats** et **Décisions à prendre**.
3. Ouvrez les **Preuves** et citations.
4. Vérifiez la **Fraîcheur des sources**.
5. Lisez la **Confiance** et les **Informations manquantes**.
6. Décidez si la sortie reste exploratoire, devient un Document PM ou doit être escaladée.

Zones à repérer sur la capture

ZONE	CE QU'ELLE APPORTE
Résumé	Lecture rapide du résultat
Constats	Faits ou motifs identifiés
Décisions	Points demandant arbitrage humain
Preuves	Sources qui justifient la réponse
Fraîcheur	État temporel des sources utilisées
Confiance	Indice de solidité à relire avec les preuves
Actions aval	Copie, artefact, Document PM, Journal IA ou action gouvernée selon le contexte

Décider quoi faire

SITUATION OBSERVÉE	RISQUE	DÉCISION RECOMMANDÉE
Preuve absente	Le résultat n'est pas justifiable	Ne pas publier ; demander une source ou relancer avec contexte
Source stale	Source trop ancienne	Rafraîchir, réimporter ou confirmer manuellement
Source conflicting	Sources contradictoires	Arbitrer humainement et documenter la décision
Source unavailable	Preuve non récupérée	Traiter comme alerte, pas comme preuve exploitable
Confiance faible	Résultat incertain	Garder en exploration ou demander une revue
Informations manquantes	Hypothèses fortes	Compléter la connaissance ou reformuler la demande
Action externe proposée	Impact hors ProPM Agent	Passer par Actions et approbations
Livrable à partager	Besoin de version et gouvernance	Ouvrir Documents PM et artefacts

États de fraîcheur

ÉTAT	SIGNIFICATION PRATIQUE	RÉACTION RECOMMANDÉE
fresh	Source assez récente pour un usage normal	Relecture normale
aging	Source encore exploitable mais à surveiller	Vérifier avant diffusion large
stale	Source trop ancienne	Rafraîchir ou confirmer
conflicting	Source contradictoire	Arbitrage humain obligatoire
unavailable	Source non confirmée	Ne pas l'utiliser comme preuve principale

Relecture humaine obligatoire

Une sortie IA doit être relue avant publication, décision externe, communication sponsor, notification client, ticket externe ou action gouvernée. La confiance n'est pas une approbation et la fraîcheur n'est pas une preuve à elle seule.

Passer vers un Document PM

Transformez la sortie en Document PM lorsque le résultat doit être partagé, versionné, approuvé, publié, téléchargé ou ajouté à la connaissance. Le flux recommandé est :

run → sortie structurée → artefact → version → Document PM → Download / Publish / Add to knowledge.

Consultez [Documents PM et artefacts](#) pour la revue, le diff, la lignée et les actions aval.

Repères support et audit

Les champs comme [Trace ID](#), [Structured output ID](#) ou [Context snapshot ID](#) sont utiles au support et à l'audit, mais ne doivent pas remplacer la lecture métier des preuves. Pour une enquête, ouvrez [Journal IA](#) et [Support, audit et diagnostic](#).

Résultat attendu

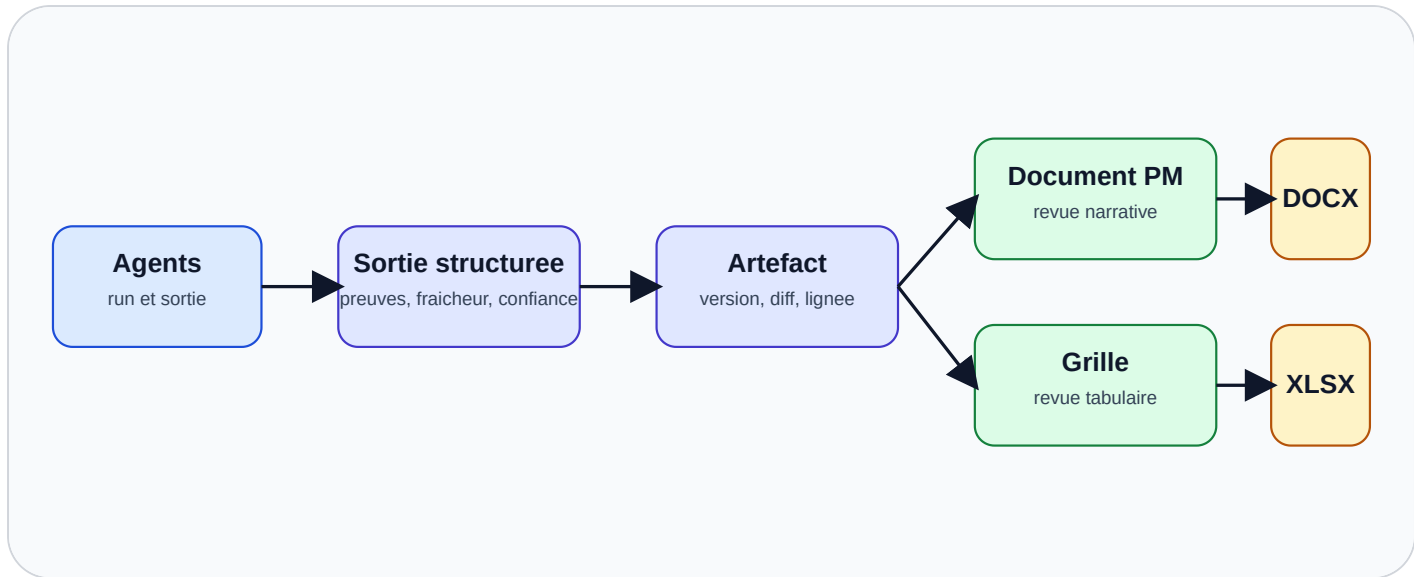
- Vous savez si la sortie est exploitable, exploratoire ou bloquée.
- Vous avez vérifié les preuves et leur fraîcheur.
- Vous savez quand créer un Document PM ou ouvrir une action gouvernée.

Suite

- [Agents](#)
- [Documents PM et artefacts](#)
- [Journal IA](#)
- [Support, audit et diagnostic](#)

Documents PM et artefacts

[Accueil](#) · Documents PM et artefacts



Objectif

Cette page explique le parcours de revue des artefacts et Documents PM : retrouver un livrable, relire le contenu, comparer les versions, télécharger, publier ou ajouter à la connaissance.

Pour qui

PROFIL	USAGE DE CETTE PAGE
Contributeur	Relire un brouillon et préparer une correction
Project Manager	Valider le contenu et télécharger un document
Propriétaire de projet	Approuver, publier ou encadrer les versions
Auditeur	Comprendre l'origine et la lignée d'un document

Avant de commencer

- Un projet actif est sélectionné.
- Un run, une sortie structurée ou une action a produit un artefact ou un Document PM.

- Votre rôle autorise la revue, l’approbation ou la publication selon l’action visée.

Comprendre le flux

Le flux documentaire le plus courant est : **run** → **sortie structurée** → **artefact** → **version** → **Document PM** → **Download / Publish / Add to knowledge**.

TERME	LECTURE PRATIQUE
Sortie structurée	Résultat d’un agent, encore à relire
Artefact	Objet gouverné issu d’un run ou d’une revue
Version	État précis d’un artefact avec historique et diff
Document PM	Document projet prêt à être relu, téléchargé, publié ou réinjecté dans la connaissance

Retrouver un Document PM

1. Ouvrez **PM Docs, Reports** ou **Rapports & artefacts** selon le libellé visible.
2. Vérifiez le projet actif.
3. Filtrez par statut, type, date ou auteur si les filtres sont disponibles.
4. Ouvrez le document à relire.
5. Consultez le contenu, les métadonnées, la lignée et les actions disponibles.

Relire et sauvegarder un DOCX ou Markdown

1. Ouvrez le document.
2. Relisez le titre, le résumé, les sections et les preuves.
3. Corrigez le contenu dans l’éditeur si votre rôle le permet.
4. Enregistrez les modifications.
5. Consultez le diff pour vérifier ce qui a changé.
6. Demandez ou appliquez l’approbation selon la gouvernance du projet.

Relire un XLSX ou une grille

1. Ouvrez le document tabulaire.
2. Vérifiez les colonnes, totaux, dates et hypothèses.

3. Corrigez uniquement les cellules modifiables.
4. Enregistrez puis rouvrez la version pour confirmer le résultat.
5. Téléchargez le fichier seulement après revue.

Télécharger, publier ou ajouter à la connaissance

ACTION	EFFET	À UTILISER QUAND
Download	Télécharge une copie locale	Vous devez partager ou archiver hors plateforme selon votre processus
Publish	Publie vers une destination gouvernée	Le projet a une destination validée, par exemple SharePoint
Add to knowledge	Réinjecte le document dans la connaissance projet	Le document relu doit devenir une source pour les recherches et agents futurs

Résultat attendu

- Le document est relu avant usage externe.
- Le diff explique les changements entre versions.
- La lignée permet de retrouver le run ou la source d'origine.
- Les actions de publication respectent les rôles, politiques et intégrations disponibles.

Si cela ne fonctionne pas

SYMPTÔME	CAUSE PROBABLE	ACTION RECOMMANDÉE
Le document est introuvable	Mauvais projet actif ou filtre trop restrictif	Vérifiez le projet et réinitialisez les filtres
Le bouton Publish est absent	Destination non rattachée ou rôle insuffisant	Vérifiez les intégrations projet et la politique
Add to knowledge échoue	Document non finalisé ou permission manquante	Relisez le statut et votre rôle
Le diff semble inattendu	Version de référence incorrecte	Ouvrez la lignée et comparez les versions

Suite

- Pour auditer le run d'origine, ouvrez [Journal IA](#).
- Pour publier vers SharePoint, consultez [Connecteurs et intégrations](#).
- Pour comprendre les preuves, ouvrez [Sorties structurées, preuves et fraîcheur](#).

Journal IA

Accueil · Journal IA

ProPM Agent
Cockpit de livraison IA

PROJET ACTUEL
Azure Bay Hotel & Convention Center
Ouvrir l'espace de travail

- Tableau de bord
- Projets
- Espace de travail
- Connaissance
- Agents
- Rapports & artefacts
- Journal IA**
- Centre de commande portefeuille
- Administration de la plateforme

Utilisateur
mock.user@contoso.c...

Azure Bay Hotel & Convention Cent

Appuyez sur Ctrl+K / ⌘K pour les commandes

Océan

Français

Aide

Santé

Journal IA Actualiser

Runs et chronologie d'activité pour ce projet.

AIDE Aide

Aperçu du journal IA
AI Log fournit une piste d'audit pour les exécutions, les événements d'activité, les artefacts, la fraîcheur et la transparence fournisseur.

Aperçu du journal IA Filtres d'exécution Audit des événements Identifiants de run

Runs Activité

Rechercher agent/statut/id de run... Tous les agents Tous les statuts

3 affichés

Créé	Agent	Statut	Coût	ID d'exécution	Actions
2026-04-21 08:50:50	Schedule	Terminé	884 jetons • 3 appels	run-003	Détails
2026-04-21 07:50:50	Risk	Terminé	917 jetons • 3 appels	run-002	Détails
2026-04-21 06:50:50	Orchestrator	Terminé	1432 jetons • 5 appels	run-001	Détails

Objectif

Le Journal IA sert à vérifier ce qui s'est réellement passé pendant une exécution : run, activité, fournisseur IA effectif, horodatage, utilisateur, projet, statut et identifiants utiles au support.

Pour qui

PROFIL	USAGE DE CETTE PAGE
Utilisateur avancé	Retrouver une exécution récente
Project Manager	Vérifier l'origine d'un résultat ou d'un Document PM
Auditeur	Confirmer le fournisseur IA effectif et les traces
Support	Collecter les identifiants nécessaires sans exposer de secret

Avant de commencer

- Un projet actif est sélectionné si l'analyse porte sur un projet.
- Vous connaissez l'heure approximative, l'agent, le document ou l'action concernée.
- Votre rôle permet d'ouvrir le Journal IA ou les détails de run.

Retrouver un run

1. Ouvrez **AI Log** ou **Journal IA**.
2. Sélectionnez l'onglet **Runs**.
3. Filtrez par projet, statut, agent, utilisateur ou période si les filtres sont disponibles.
4. Ouvrez le run concerné.
5. Vérifiez le statut, l'heure, le fournisseur IA effectif et les liens vers l'artefact ou le Document PM.

Vérifier le fournisseur IA effectif

1. Ouvrez le détail du run.
2. Recherchez le champ **Effective AI Provider** ou son équivalent.
3. Comparez-le au fournisseur attendu par l'administrateur.
4. Notez toute divergence visible.
5. En cas d'écart répété, demandez à l'administrateur de vérifier [Fournisseur IA](#).

Lire l'activité

1. Ouvrez l'onglet **Activity** si disponible.
2. Repérez les événements liés au run.
3. Relevez uniquement les identifiants utiles : Run ID, Trace ID, Artifact ID ou Context snapshot ID si affichés.
4. Ne copiez pas de payload complet si l'interface contient des données sensibles.
5. Fournissez une capture ciblée au support si nécessaire.

Fournisseur sélectionné vs fournisseur effectif

TERME	SIGNIFICATION
Fournisseur sélectionné au déploiement	Intention initiale renseignée pendant Azure Marketplace
Fournisseur configuré	Paramétrage actuel dans l'administration plateforme
Fournisseur IA effectif	Fournisseur réellement utilisé par un run donné

Une divergence peut être normale pendant une migration, un test, une désactivation temporaire ou une erreur de configuration. Le run réel fait foi pour l'audit.

Si cela ne fonctionne pas

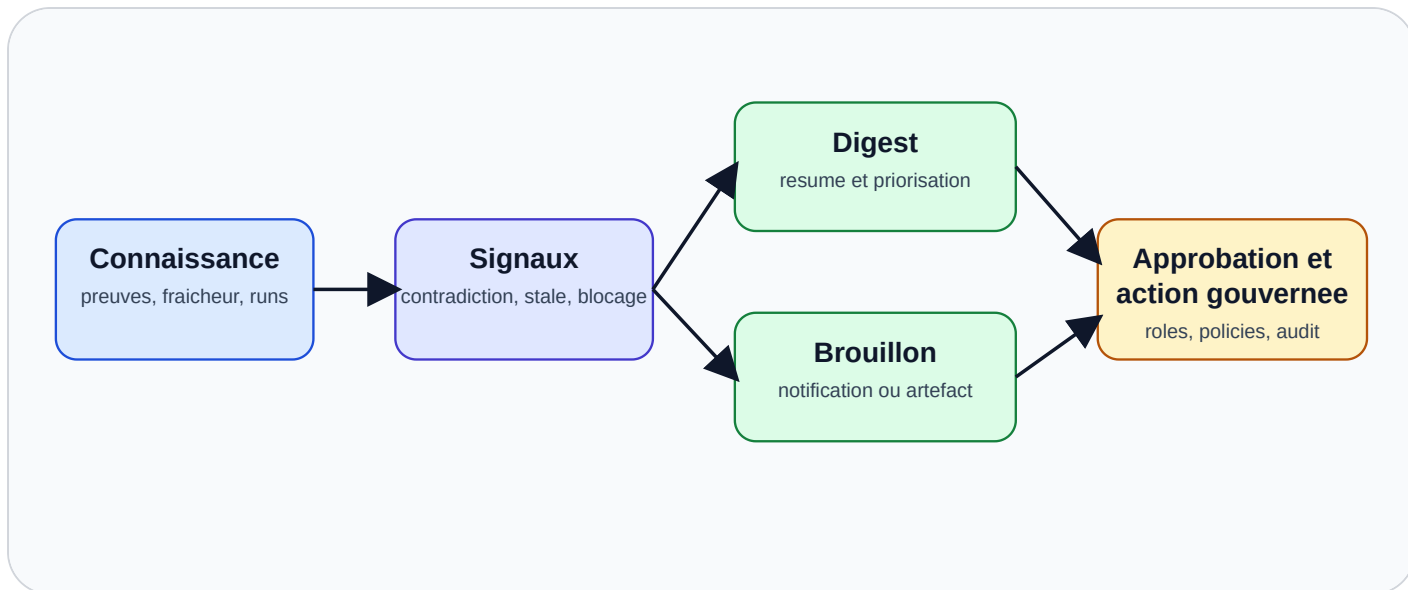
SYMPTÔME	CAUSE PROBABLE	ACTION RECOMMANDÉE
Aucun run trouvé	Mauvais projet, période ou filtre	Vérifiez le projet actif et élargissez la période
Le run est en erreur	Fournisseur IA, droits ou données d'entrée	Relevez le message et le Run ID
Le fournisseur effectif est inattendu	Configuration modifiée ou non activée	Ouvrez Fournisseur IA
Les détails sont trop techniques	Page support/audit avancée nécessaire	Ouvrez Support, audit et diagnostic

Suite

- Pour les informations à fournir au support, ouvrez [Support, audit et diagnostic](#).
- Pour gérer le fournisseur IA, ouvrez [Fournisseur IA](#).
- Pour comprendre un Document PM issu du run, ouvrez [Documents PM et artefacts](#).

Signaux et notifications

[Accueil](#) · Signaux et notifications



Objectif

Cette page explique comment traiter les signaux et notifications opérationnelles sans confondre alerte, brouillon, digest et action gouvernée.

Pour qui

PROFIL	USAGE DE CETTE PAGE
Contributeur	Lire un signal et comprendre son contexte
Project Manager	Traiter, reporter, fermer ou transformer un signal en brouillon
Propriétaire de projet	Vérifier les règles et escalader vers une action gouvernée
Support	Comprendre si un signal est bloqué par l'état projet ou la politique

Avant de commencer

- Un projet actif est sélectionné.
- Votre rôle permet de consulter les signaux du projet.
- Les données projet et la connaissance sont suffisamment à jour pour interpréter le signal.

Lire un signal

1. Ouvrez **Signals**, **Inbox** ou la zone de signaux du **Workspace**.
2. Vérifiez la sévérité, le statut, le mode et la date.
3. Ouvrez le détail du signal.
4. Lisez les preuves, sources et recommandations.
5. Décidez si le signal doit être traité, reporté, fermé ou transformé en brouillon/action.

Actions courantes

ACTION	EFFET	QUAND L'UTILISER
Refresh	Recharge ou recalcule les signaux visibles	Après nouvel import ou changement important
Generate digest draft	Prépare un digest de synthèse	Avant une communication de suivi
Create draft	Crée un brouillon exploitable	Quand le signal doit devenir un message ou livrable
Snooze 24h	Reporte temporairement le signal	Quand une réponse est attendue sous peu
Dismiss	Ferme le signal	Quand il est non pertinent ou déjà traité

Comprendre les notification drafts

Un brouillon de notification peut être **in-app**, retenu, planifié ou soumis à approbation selon la politique. Le fait qu'un brouillon existe ne signifie pas qu'un message externe a été envoyé.

Centre de notifications

1. Ouvrez l'icône de notifications dans la barre supérieure.
2. Sélectionnez une notification pour ouvrir la page liée.
3. Utilisez **Mark all read** pour marquer les éléments comme lus si le bouton est disponible.
4. Utilisez **Clear** uniquement lorsque vous n'avez plus besoin de la liste locale.

Résultat attendu

- Le signal est compris avec ses preuves.
- Les éléments non prioritaires sont reportés ou fermés.
- Les éléments importants deviennent un brouillon, une action ou une escalade claire.
- Les notifications ne remplacent pas la revue du projet actif.

Si cela ne fonctionne pas

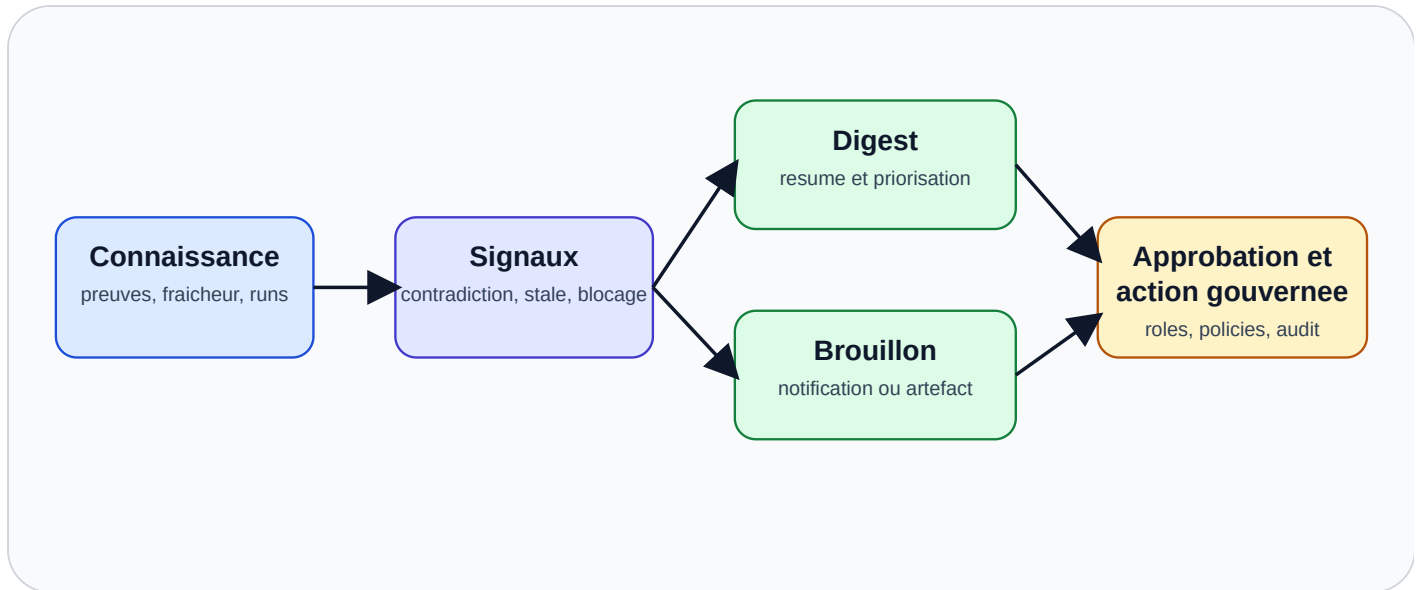
SYMPTÔME	CAUSE PROBABLE	ACTION RECOMMANDÉE
Aucun signal visible	Projet récent, filtre actif ou rôle insuffisant	Réinitialisez les filtres et vérifiez le rôle
Refresh ne change rien	Données inchangées ou calcul déjà à jour	Vérifiez la connaissance et l'activité récente
Create draft est bloqué	Politique, rôle ou destination manquante	Ouvrez Actions et approbations
Une notification mène à une page vide	Mauvais projet actif ou accès insuffisant	Sélectionnez le bon projet et vérifiez les droits

Suite

- Pour transformer un signal en action, ouvrez [Actions et approbations](#).
- Pour configurer les politiques, ouvrez [Gouvernance, décisions et actions](#).
- Pour diagnostiquer une notification bloquée, ouvrez [Support, audit et diagnostic](#).

Gouvernance, décisions et actions

[Accueil](#) · Gouvernance, décisions et actions



Objectif

Cette page explique, de manière simple, comment ProPM Agent passe :

1. d'un **signal** détecté ;
2. à une **décision** ;
3. puis à une **action gouvernée** ;
4. éventuellement soumise à **approbation** ;
5. avant d'être **exécutée** et **tracée**.

Cette page vous aide à comprendre clairement :

- ce qu'est une **politique de gouvernance** ;
- ce que signifient `allow`, `require_approval` et `deny` ;
- ce que signifient `observe`, `draft`, `propose` et `execute` ;
- comment utiliser **Actions & approbations** pas à pas ;
- pourquoi une action peut être visible mais bloquée.

Vue très simple du flux

Dans ProPM Agent, le chemin normal est le suivant :

1. un **signal** attire l'attention ;
2. l'équipe le relit ;

3. la **gouvernance** décide ce que chaque rôle a le droit de faire ;
4. si une sortie externe est nécessaire, une **action** est créée ;
5. si le projet l'exige, l'action passe en **approbation** ;
6. l'action est ensuite **exécutée** ou **rejetée** ;
7. la trace reste visible dans l'**activité** et le **Journal IA**.

Partie 1 — Comprendre les signaux

Un **signal** est une alerte structurée qui dit : « **ce sujet mérite d'être regardé** ».

Exemples de signaux

Un signal peut remonter :

- une **fraîcheur** des sources insuffisante ;
- une **contradiction** entre plusieurs preuves ;
- un **blocage** projet ;
- une suite à donner qui mérite une **notification**, une **décision** ou une **action externe**.

Ce que l'utilisateur voit généralement sur une carte de signal

Une carte de signal peut afficher :

- un **titre** ;
- un **résumé** ;
- une **explication** ;
- une **sévérité** ;
- un **statut** ;
- un **mode** ;
- un nombre de **preuves** ou de redéclenchements ;
- des actions comme **Create draft**, **Snooze 24h** ou **Dismiss** selon le rôle.

Pas à pas conseillé pour traiter un signal

Quand vous ouvrez un signal, gardez cet ordre :

1. lisez le **résumé** ;
2. relisez ensuite l'**explication** ;
3. vérifiez les **preuves** et la **fraîcheur** ;

4. décidez si le sujet demande seulement une surveillance, un brouillon ou une action réelle ;
5. si une sortie externe devient nécessaire, passez à **Actions & approbations**.

Statuts utiles d'un signal

STATUT	CE QUE CELA VEUT DIRE
open	le sujet reste actif et demande encore de l'attention
snoozed	le sujet est mis en pause temporairement
dismissed	le sujet est retiré de la file active
resolved	le sujet est considéré comme traité

Modes utiles d'un signal

MODE	LECTURE SIMPLE
inform	le signal informe, sans exiger d'action immédiate
suggest	le signal suggère une prochaine étape
draft	le signal est déjà orienté vers un brouillon ou une préparation
request_approval	le signal appelle une revue gouvernée ou une approbation

Partie 2 — Politiques de gouvernance

Qu'est-ce qu'une politique de gouvernance ?

Une **politique de gouvernance** est une règle qui répond à la question :
 « **Qui a le droit de faire quoi, sur quel connecteur, et avec quel niveau de contrôle ?** »

Autrement dit, la gouvernance empêche qu'une action externe parte sans cadre clair.

Ce qu'une politique décide

Une politique répond en général à quatre questions :

1. **Qui ?** — quel rôle est concerné ;
2. **Sur quoi ?** — quel connecteur, quel type d'action ou quelle destination est concerné ;
3. **Jusqu'où ?** — simple observation, brouillon, proposition ou exécution ;
4. **Avec quel effet ?** — autorisé, autorisé avec approbation, ou refusé.

Exemple très simple

Une politique peut vouloir dire :

- le **Contributeur** peut préparer un brouillon Teams ;
- le **Chef de projet** peut proposer une publication SharePoint ;
- le **Propriétaire du projet** doit approuver avant exécution ;
- personne d'autre ne peut exécuter directement cette publication.

Comprendre les niveaux : **observe**, **draft**, **propose**, **execute**

Le **niveau** décrit jusqu'où un rôle peut aller dans le flux.

NIVEAU	CE QUE L'UTILISATEUR PEUT FAIRE	CE QU'IL NE PEUT PAS ENCORE FAIRE	EXEMPLE SIMPLE
observe	voir l'information, suivre le sujet, consulter la file	créer une action ou un brouillon	un lecteur suit les signaux sans préparer de sortie
draft	préparer un brouillon, un texte, une intention d'action	soumettre officiellement l'action à la file	un contributeur prépare un message Teams mais ne le propose pas
propose	soumettre une vraie demande d'action dans la file gouvernée	exécuter directement l'action	un chef de projet propose un ticket Jira
execute	lancer l'exécution réelle si les autres conditions sont remplies	contourner la politique ou les approbations imposées	un propriétaire de projet publie un artefact vers SharePoint

Lecture très simple

- **observe** = je regarde ;
- **draft** = je prépare ;

- **propose** = je demande officiellement ;
- **execute** = je lance réellement.

Comprendre les effets : **allow**, **require_approval**, **deny**

L'**effet** décrit ce que la plateforme fait quand un rôle atteint ce niveau.

EFFET	CE QUE CELA VEUT DIRE	CONSÉQUENCE PRATIQUE
allow	l'action est autorisée à ce niveau	le flux peut avancer sans étape d'approbation supplémentaire, si le reste est prêt
require_approval	l'action est possible, mais doit être approuvée	la file d'approbation devient obligatoire avant exécution
deny	l'action est interdite pour ce rôle ou ce périmètre	l'utilisateur ne peut pas aller plus loin sur ce flux

Lecture très simple

- **allow** = oui ;
- **require_approval** = oui, mais après validation humaine ;
- **deny** = non.

Comment lire une ligne de politique

Prenons cette lecture :

- **Rôle** : Chef de projet
- **Connecteur** : SharePoint publish
- **Niveau** : **execute**
- **Effet** : **require_approval**

Cela veut dire :

- le Chef de projet peut aller jusqu'à la demande d'exécution ;
- mais la publication ne part pas immédiatement ;
- une approbation est nécessaire avant l'exécution réelle.

Exemples concrets de politiques

CAS MÉTIER	RÔLE	NIVEAU RECOMMANDÉ	EFFET RECOMMANDÉ	POURQUOI
publication d'un compte rendu vers SharePoint	Chef de projet	execute	require_approval	la sortie est externe et doit être relue
création d'un ticket Jira depuis un blocage	Chef de projet	propose	allow ou require_approval	le projet peut demander un ticket sans forcément l'ouvrir automatiquement
message Teams interne de faible risque	Contributeur	execute ou propose	allow	communication rapide à faible impact
e-mail Outlook à des sponsors	Contributeur	propose	require_approval	communication plus sensible et plus formelle
webhook vers un outil tiers	Propriétaire du projet	execute	require_approval	sortie technique à garder très contrôlée
connecteur non prêt ou non autorisé	tous sauf admin	observe ou aucun usage	deny	on évite tout départ accidentel

Pas à pas pour configurer une politique de gouvernance

Suivez cet ordre simple.

Étape 1 — Ouvrir la bonne surface

Depuis l'**Espace de travail** du projet, ouvrez **Politiques de gouvernance**.

Étape 2 — Choisir le flux à contrôler

Demandez-vous d'abord :

- s'agit-il d'une **publication** ;
- d'un **ticket** ;
- d'un **message** ;
- d'un **webhook** ;

- d'une autre action externe ?

Étape 3 — Choisir le rôle concerné

Définissez ensuite quel rôle peut agir :

- **Contributeur** ;
- **Chef de projet** ;
- **Propriétaire du projet** ;
- ou autre rôle présent dans votre configuration.

Étape 4 — Choisir le niveau d'action

Décidez si ce rôle doit seulement :

- observer ;
- préparer un brouillon ;
- proposer ;
- ou exécuter.

Étape 5 — Choisir l'effet

Décidez si ce niveau doit être :

- autorisé directement (`allow`) ;
- autorisé avec approbation (`require_approval`) ;
- ou refusé (`deny`).

Étape 6 — Vérifier le connecteur ou la destination concernée

Une bonne politique ne suffit pas si le connecteur :

- n'est pas prêt techniquement ;
- n'est pas ouvert au projet ;
- ou n'a pas la bonne destination d'artefact.

Étape 7 — Tester avec un rôle non administrateur

Le meilleur contrôle est pratique :

1. connectez-vous avec un rôle métier réaliste ;
2. ouvrez **Actions & approbations** ;
3. vérifiez ce qui est visible, autorisé ou bloqué ;

4. ajustez la politique si le comportement n'est pas celui attendu.

Politiques de gouvernance
 Configurez les connecteurs gouvernés, destinations, politiques d'action, profils de rendu, contraintes de fraîcheur et digests de notification.

CONNECTEURS
3

DESTINATIONS
2

POLITIQUES D'ACTION
2

PROFILS DE RENDU
2

PARAMÈTRES DE NOTIFICATION
1

Review and save each governance object independently so connector posture, routing destinations, action boundaries, rendering behavior, and notification rules stay easy to audit.

TYPES D' ACTIONS GOUVERNÉES

Publier l'artefact dans SharePoint
Envoyer un message Teams
Envoyer un message Outlook
Créer un ticket Jira
Créer un ticket Azure DevOps
Créer un suivi calendrier

Connecteurs 3 configurés

Statut, mode d'exécution, environnement et posture de périmètre pour les actions adossées à des connecteurs.

Microsoft Graph / SharePoint
 graph-sharepoint-primary • Microsoft Graph / SharePoint

Activé
Simulation
Fraîcheur : Fresh

Nom ? Type de connecteur ?

Microsoft Graph / SharePoint Microsoft Graph / SharePoint

Description ?

Statut ? Mode d'exécution ?

Activé Simulation

Environment ? Référence de fixture ?

Jira Activé Simulation Fraîcheur : Vieillissant

jira-primary • Jira

Nom ? Type de connecteur ?

Jira Jira

Description ?

Statut ? Mode d'exécution ?

Activé Simulation

Environment ? Référence de fixture ?

Règles simples pour bien configurer la gouvernance

- utilisez **allow** sur **execute** seulement pour les flux faibles en risque ;
- utilisez **require_approval** dès qu'un contenu sort du projet ou modifie un système externe ;
- utilisez **deny** quand le connecteur n'est pas prêt, pas autorisé ou trop sensible ;
- gardez les règles cohérentes avec les rôles réellement attribués ;
- testez toujours un cas réel avant de considérer la politique comme prête.

Erreurs fréquentes à éviter

ERREUR	BONNE LECTURE
« Je vois le connecteur, donc je peux l'utiliser »	faux : la visibilité ne garantit pas l'autorisation ni la santé technique
« propose veut dire que l'action part »	faux : propose veut dire que la demande entre dans la file gouvernée
« execute veut dire sans contrôle »	faux : execute peut encore être combiné avec require_approval
« deny veut dire panne »	faux : deny est souvent une décision de gouvernance normale

Partie 3 — Actions & approbations

L'écran **Actions & approbations** sert à transformer une intention en **action gouvernée réelle**.

Comment lire cette file
 L'absence d'éléments peut être normale lorsque rien n'a encore été proposé. Lisez les prérequis bloqués, les attentes d'approbation, les demandes exécutables et l'historique d'exécution comme des états distincts plutôt qu'une simple file vide générique.

Actions & approbations

Proposez des actions gouvernées adossées à des connecteurs, gardez-les en attente d'approbation et exécutez-les uniquement après revue.

Form draft **En attente d'approbation** Ready to execute Exécuté Rejected / failed

<p>EXECUTION PREREQUISITES Clear At least one compatible execution option is operational, so the proposal path is open.</p>	<p>PENDING APPROVAL 1 Requests proposed but still waiting for governance approval.</p>	<p>READY TO EXECUTE 1 Approved requests that are waiting for controlled execution.</p>	<p>EXECUTED HISTORY 0 Completed governed actions retained as execution history and audit evidence.</p>
---	--	--	--

Proposer une action gouvernée

Les types d'actions pris en charge restent sensibles aux politiques, à la fraîcheur et au périmètre des connecteurs. L'exécution externe ne contourne jamais l'approbation sur cette surface.

Execution readiness 1 available • 0 blocked

Only enterprise-approved execution options appear here. Technical connector setup remains in Platform Administration.

[Open Platform Administration](#) [Review project integrations](#)

Type d'action: **Publier l'artefact dans SharePoint**

Execution option: **Microsoft Graph / SharePoint — Microsoft Graph / SharePoint**

Mode: Mock

Titre: **Approuver la publication SharePoint du brief hebdomadaire**

Justification: **Expliquez pourquoi cette action externe est nécessaire et quelles preuves la justifient.**

Quatre lectures canoniques à retenir

Dans l'interface, cette surface se lit plus facilement à travers quatre états distincts :

LECTURE CANONIQUE	CE QUE CELA VEUT DIRE
Prérequis d'exécution	des options d'exécution compatibles peuvent exister, mais leur usage opérationnel reste bloqué ou indisponible
En attente d'approbation	une demande gouvernée a été proposée et attend encore une décision
Prêt à exécuter	la demande est déjà en état approved , mais l'exécution contrôlée reste une étape séparée
Historique d'exécution	l'action a réellement été exécutée et reste visible comme historique d'audit

Une demande en état **approved** n'est donc pas encore une demande en état **executed**.

Quand tout est correctement prêt, que devrait-on voir ?

Dans un cas nominal, l'utilisateur autorisé retrouve en général :

- au moins un **type d'action** pertinent ;
- une **option d'exécution compatible et saine** ;
- un **rattachement projet** réellement actif ;
- une **politique** qui autorise la proposition ou route vers l'approbation ;
- une file où les demandes passent ensuite par **pending approval**, **approved**, **executed** ou **rejected** selon le cas.

Si un de ces maillons manque, l'écran peut paraître vide, incomplet ou purement informatif sans qu'il s'agisse forcément d'une panne.

Ce que l'utilisateur voit dans cet écran

Un utilisateur y retrouve généralement :

- un formulaire **Proposer une action gouvernée** ;
- le choix du **type d'action** ;
- le choix du **connecteur d'exécution** ou de l'**option d'exécution** ;
- un résumé de **préparation** indiquant ce qui est disponible ou bloqué ;
- des champs comme **titre, justification, destination, message, description du ticket** ;
- une **file d'approbation et d'exécution** avec les demandes déjà soumises.

Pas à pas — créer une action gouvernée

Étape 1 — Ouvrir l'écran

Dans l'**Espace de travail**, ouvrez **Actions & approbations**.

Étape 2 — Choisir le type d'action

Sélectionnez d'abord l'intention métier. Les types d'action visibles incluent notamment :

- **Publish artifact to SharePoint** ;
- **Send Teams message** ;
- **Send Outlook message** ;
- **Create Jira ticket** ;
- **Create Azure DevOps ticket** ;
- **Webhook** selon la configuration du tenant.

Étape 3 — Vérifier l'option d'exécution compatible

L'interface recherche ensuite les **options d'exécution compatibles**.

Choisissez une option :

- **saine** ;
- **autorisée** ;
- réellement ouverte à votre projet.

Si aucune option saine n'apparaît, la vérification porte souvent sur :

- du connecteur lui-même ;
- de son état de santé ;
- du rattachement projet ;
- de la politique ;
- ou de votre permission.

Étape 4 — Lire la préparation

La zone **Préparation d'exécution** sert à vérifier que vous n'êtes pas en train de préparer une action théorique seulement.

En pratique :

- **available / healthy** = option exploitable ;
- **blocked by health** = connecteur à vérifier côté plateforme ;
- **blocked by policy** = le cadre de gouvernance bloque encore le passage ;
- **blocked by entitlement** = libellé hérité pour un blocage non lié au plan ; vérifiez configuration, binding, policy, permission, approbation ou health ;
- aucune option visible = connecteur compatible absent, binding projet manquant ou option non ouverte à votre rôle.

Lecture pédagogique d'un écran qui semble vide

Quand **Actions & approbations** ne propose rien d'exécutable, distinguez d'abord trois cas avant de conclure à une panne :

1. la disponibilité des options d'exécution n'a pas pu être chargée ;
2. des options compatibles existent mais restent bloquées ou non saines ;
3. aucun connecteur compatible n'est encore configuré pour ce type d'action.

Dans les trois cas, cet état doit être distingué d'une file simplement vide parce qu'aucune action n'a encore été proposée.

CE QUE VOUS VOYEZ	RAISON DOMINANTE POSSIBLE	RÉFLEXE UTILE
aucun connecteur sélectionnable	aucun connecteur compatible et sain n'est prêt	vérifier Intégrations du projet puis Administration de la plateforme
action visible mais bouton bloqué	permission, policy ou approbation requise	contrôler le rôle puis la gouvernance
file visible mais rien ne part	la demande reste en attente d'approbation ou d'exécution aval	relire le statut réel de la file
connecteur présent mais inutilisable	binding projet, health, configuration, policy ou permission insuffisants	vérifier la chaîne complète plateforme → projet → policy

Rappelez-vous aussi que seules les options d'exécution approuvées côté entreprise/projet apparaissent ici. La préparation technique du connecteur reste dans **Administration de la plateforme**, tandis que l'exposition au projet se lit dans **Intégrations du projet**.

Étape 5 — Renseigner le titre et la justification

Complétez ensuite :

- un **titre clair** ;
- une **justification** courte mais utile ;
- les champs spécifiques au type d'action choisi.

La justification doit répondre à deux questions :

1. **Pourquoi cette action est-elle nécessaire ?**
2. **Sur quelles preuves ou décisions s'appuie-t-elle ?**

Étape 6 — Compléter les champs métier

Les champs changent selon le type d'action.

TYPE D'ACTION	CHAMPS FRÉQUEMMENT ATTENDUS
Publication SharePoint	titre, justification, <code>artifact ID</code> , destination, profil de rendu, format
Message Teams	titre, justification, corps du message
Message Outlook	titre, justification, destinataires, objet, corps du message
Ticket Jira	titre, justification, description du ticket, éventuellement clé projet / board
Ticket Azure DevOps	titre, justification, description, type de ticket selon le connecteur
Webhook	titre, justification et données utiles au système cible

Étape 7 — Proposer l'action

Une fois les champs remplis, soumettez la demande.

À ce stade, l'action n'est pas forcément déjà partie. Elle peut d'abord entrer dans la **file d'approbation**.

Étape 8 — Revue par l'approbateur

Si la politique impose `require_approval`, un approbateur doit relire :

- le titre ;
- la justification ;
- le connecteur utilisé ;
- la charge utile ou le détail métier ;
- l'éventuel artefact ou brouillon lié.

Étape 9 — Approbation, rejet ou exécution

Selon la politique et le rôle de l'approbateur, la demande peut être :

- **approuvée** ;
- **rejetée** ;
- puis **exécutée** si tout est prêt.

Étape 10 — Vérifier la trace finale

Après exécution, vérifiez :

- la file d'actions ;

- l'activité projet ;
- le **Trace ID** s'il est affiché ;
- le **Journal IA** si le flux s'y reflète ;
- la présence de l'artefact, du ticket ou du message côté outil cible.

Comment lire les statuts d'action

STATUT	CE QUE CELA VEUT DIRE
draft	la demande est encore préparatoire
pending approval	l'approbation est attendue avant suite réelle
approved	la demande a été acceptée
executed	l'action a réellement été lancée
rejected	la demande a été refusée
failed	l'action a été lancée mais n'a pas abouti correctement
cancelled	la demande a été annulée

Exemple pas à pas — publication d'un artefact vers SharePoint

Situation

L'équipe a relu un **brief hebdomadaire** et veut le publier dans SharePoint.

Parcours

1. ouvrir **Actions & approbations** ;
2. choisir **Publish artifact to SharePoint** ;
3. sélectionner une option **SharePoint publish** saine ;
4. renseigner le **titre** de l'action ;
5. ajouter une **justification**, par exemple : « version relue et approuvée pour diffusion hebdomadaire » ;
6. renseigner l'**artefact ID** ;

7. choisir la **destination SharePoint** ;
8. choisir le **profil de rendu** ou le **format** si demandé ;
9. proposer l'action ;
0. si la politique l'exige, attendre l'approbation ;
1. exécuter ;
2. contrôler que l'artefact est bien publié côté SharePoint et tracé dans ProPM Agent.

Exemple pas à pas — créer un ticket Jira

Situation

Un signal remonte un blocage récurrent avec impact planning.

Parcours

1. ouvrir **Actions & approbations** ;
2. choisir **Create Jira ticket** ;
3. sélectionner un connecteur Jira disponible ;
4. saisir un titre clair, par exemple : « Blocage fournisseur sur lot critique » ;
5. compléter la **description** du ticket ;
6. ajouter la **justification** et les preuves utiles ;
7. proposer la demande ;
8. laisser l'approbateur relire si la politique impose `require_approval` ;
9. exécuter ;
0. vérifier ensuite la référence externe ou le ticket créé.

Exemple pas à pas — envoyer un message Teams ou Outlook

Situation

Le projet doit informer un groupe interne ou un sponsor d'une revue terminée.

Parcours Teams

1. choisir **Send Teams message** ;
2. sélectionner le connecteur Teams autorisé ;
3. rédiger un message court et compréhensible ;
4. ajouter la justification si le flux est gouverné ;
5. proposer, faire approuver si besoin, puis exécuter.

Parcours Outlook

1. choisir **Send Outlook message** ;
2. sélectionner le connecteur Outlook ;
3. renseigner les **destinataires** ;
4. compléter l'**objet** et le **corps** du message ;
5. proposer, faire approuver si besoin, puis exécuter.

Différence pratique

- **Teams** convient bien à une communication collaborative interne ;
- **Outlook** convient mieux à une communication plus formelle et plus ciblée.

Exemple pas à pas — webhook vers un outil tiers

Situation

L'entreprise veut déclencher un flux interne vers un outil maison.

Parcours

1. choisir le type d'action ou le flux lié au **Webhook** ;
2. sélectionner l'option d'exécution webhook compatible ;
3. renseigner le titre et la justification ;
4. compléter les données utiles au système cible ;
5. proposer la demande ;
6. faire approuver si la politique l'exige ;
7. exécuter ;
8. contrôler le résultat côté système cible et côté audit ProPM Agent.

Pourquoi une action peut être visible mais non exécutable

Une action peut être visible dans l'interface mais rester bloquée si :

- le connecteur compatible n'est pas sain ;
- le projet ne dispose pas du bon binding ;
- la politique du projet interdit ce niveau d'action ;
- votre rôle ne permet pas de proposer ou d'exécuter ;
- une approbation est encore en attente ;
- le connecteur, le binding, la policy, la permission, l'approbation ou l'état health bloque le flux.

Que faire si aucune option d'exécution n'apparaît

Suivez cet ordre :

1. vérifiez d'abord **Politiques de gouvernance** ;
2. vérifiez ensuite **Intégrations du projet** ;
3. ouvrez ensuite **Administration de la plateforme** ;
4. contrôlez enfin la **configuration**, le **binding**, la **permission** et l'état de santé du connecteur.

Scénario complet — du signal à l'action exécutée

Cas simple

1. un signal `open` remonte un blocage ;
2. l'équipe relit le résumé, l'explication et les preuves ;
3. elle décide qu'un ticket Jira est nécessaire ;
4. la politique autorise le **Chef de projet** à `propose` mais impose `require_approval` ;
5. le Chef de projet crée la demande dans **Actions & approbations** ;
6. le **Propriétaire du projet** approuve ;
7. l'action passe à **executed** ;

8. le ticket externe et la trace interne restent alignés.

Ce scénario résume bien la logique du produit : **voir, décider, contrôler, exécuter, tracer**.

Bonnes pratiques

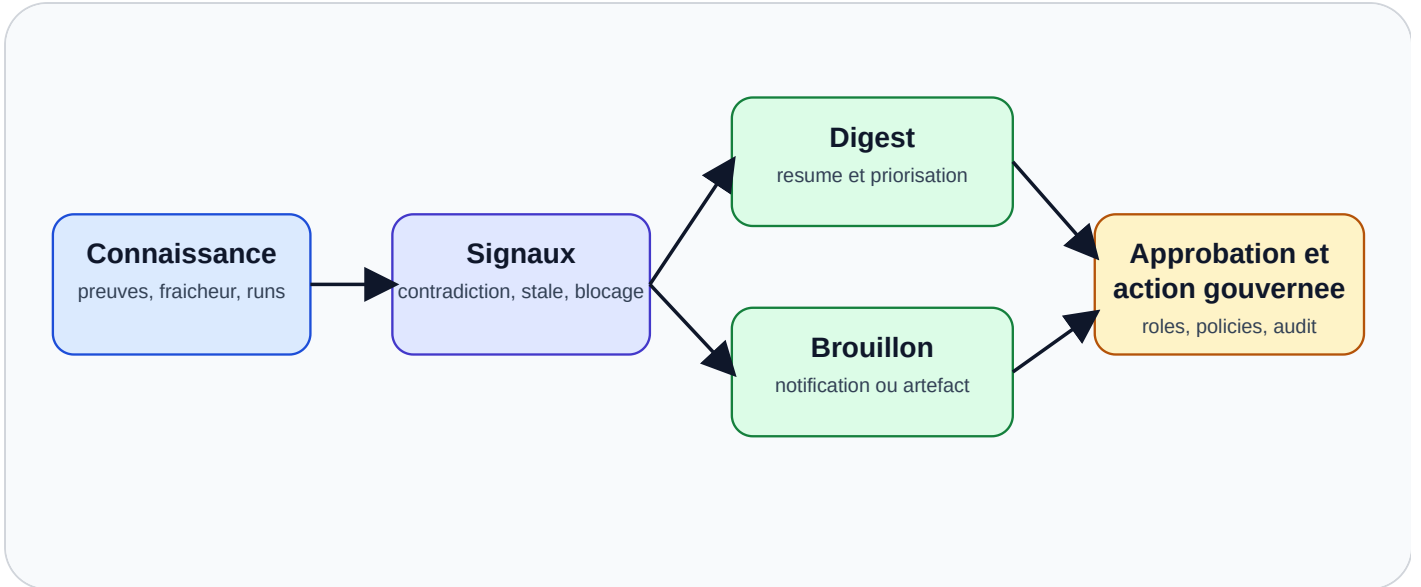
- ne confondez jamais **brouillon** et **exécution réelle** ;
- utilisez les politiques pour limiter les sorties sensibles ;
- demandez une approbation dès qu'un contenu quitte le projet ou modifie un système externe ;
- vérifiez toujours les preuves avant de proposer une action ;
- utilisez le **Journal IA** et la file d'actions comme référence commune d'audit.

Suite

- [Connecteurs et intégrations](#)
- [Journal IA](#)
- [Actions et approbations](#)
- [Maintenance, support et FAQ](#)

Actions et approbations

[Accueil](#) · Actions et approbations



Objectif

Cette page explique le workflow opérationnel des actions gouvernées : proposer une action, la faire approuver, la rejeter si nécessaire et comprendre quand elle est réellement exécutée.

Pour qui

PROFIL	USAGE DE CETTE PAGE
Contributeur autorisé	Proposer une action selon la politique
Project Manager	Préparer une action depuis un signal ou un Document PM
Propriétaire de projet	Approuver, rejeter ou exécuter selon la gouvernance
Support	Identifier la raison d'un blocage

Avant de commencer

- Un projet actif est sélectionné.
- L'action est liée à un signal, un Document PM, un connecteur ou une destination disponible.

- Le connecteur externe est validé et rattaché au projet si l'action sort de ProPM Agent.
- Votre rôle est autorisé par la politique de gouvernance.

Proposer une action

1. Ouvrez le signal, le Document PM ou la page qui propose l'action.
2. Sélectionnez l'action disponible, par exemple publier vers SharePoint ou créer un ticket Jira.
3. Vérifiez le contenu, la destination et le résumé.
4. Ajoutez une justification si l'interface la demande.
5. Soumettez l'action.
6. Vérifiez le statut : brouillon, proposée, en attente d'approbation ou bloquée.

Approuver ou rejeter

1. Ouvrez **Actions & approvals** ou **Actions et approbations**.
2. Filtrez les actions en attente.
3. Ouvrez le détail de l'action.
4. Vérifiez les preuves, la destination, l'impact et le demandeur.
5. Sélectionnez **Approve** pour autoriser ou **Reject** pour refuser.
6. Ajoutez une raison claire lorsque c'est demandé.

Exécuter une action

Une action **approved** n'est pas forcément **executed**. L'approbation donne l'autorisation. L'exécution correspond à l'envoi réel vers la destination ou au changement effectif dans le système cible.

1. Ouvrez l'action approuvée.
2. Vérifiez que le connecteur est prêt et que le mode live est activé si une action externe est attendue.
3. Lancez l'exécution si le bouton est disponible.
4. Vérifiez le statut final et la trace associée.

Raisons fréquentes de blocage

BLOPAGE	EXPLICATION	ACTION RECOMMANDÉE
Rôle insuffisant	Votre rôle ne peut pas proposer ou approuver cette action	Demandez une délégation au Project Owner
Politique require approval	Une approbation est obligatoire	Attendez ou relancez l'approbateur
Politique deny	L'action est interdite pour ce contexte	Revoyez la politique ou choisissez une autre action
Connecteur non rattaché	La plateforme connaît le connecteur mais pas le projet	Vérifiez les intégrations projet
Santé non prête	Le connecteur ou fournisseur n'est pas opérationnel	Demandez une validation administrateur
Mode live inactif	L'action ne peut pas créer d'objet externe réel	Vérifiez le mode avec l'administrateur

Résultat attendu

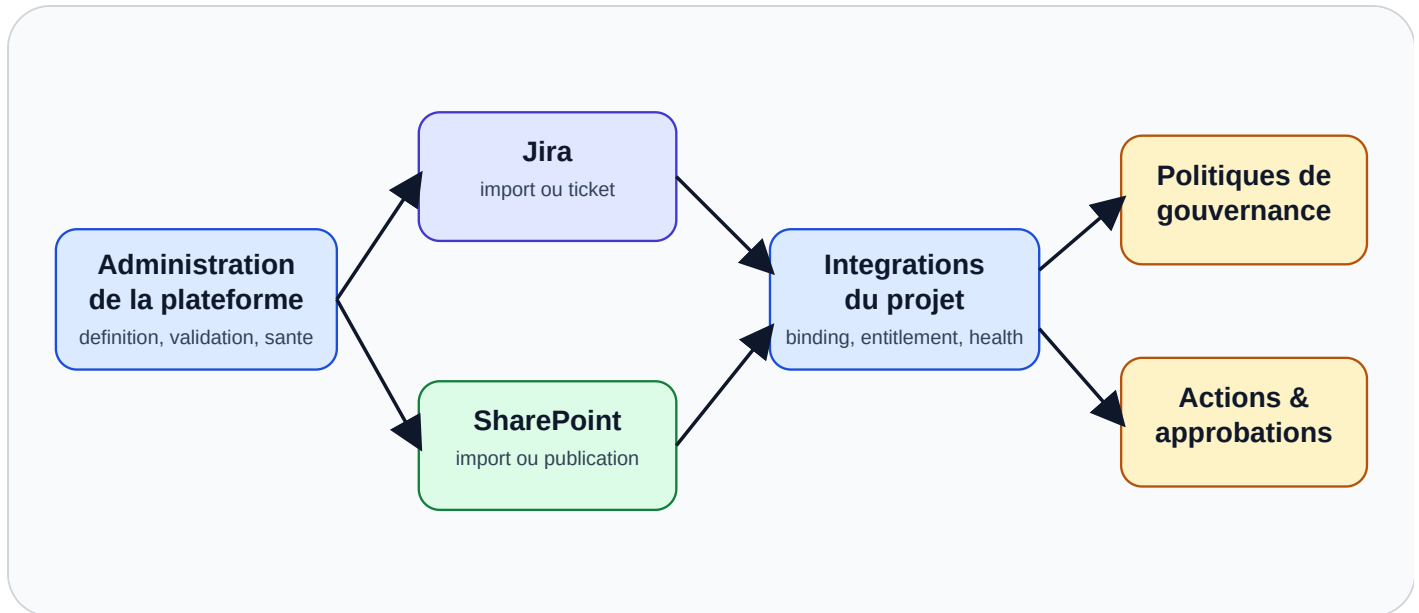
- Le demandeur comprend le statut de l'action.
- L'approbateur voit les preuves avant décision.
- Une action approuvée n'est exécutée que lorsque les conditions sont réunies.
- Les actions externes ne créent réellement des objets que si le connecteur live est validé et autorisé.

Suite

- Pour publier un Document PM, ouvrez [Documents PM et artefacts](#).
- Pour comprendre les connecteurs, ouvrez [Connecteurs et intégrations](#).
- Pour auditer l'action, ouvrez [Journal IA](#).

Connecteurs et intégrations

[Accueil](#) · Connecteurs et intégrations



Objectif

Cette page explique les connecteurs côté utilisateur et Project Owner. Les champs techniques, secrets et authentifications détaillées sont traités dans l'administration sécurisée, pas dans le guide utilisateur final.

Pour qui

PROFIL	USAGE DE CETTE PAGE
Utilisateur métier	Comprendre pourquoi un connecteur est visible ou bloqué
Project Manager	Importer depuis une source approuvée ou proposer une action
Propriétaire de projet	Vérifier rattachement, politique et destination
Administrateur plateforme	Utiliser plutôt Intégrations plateforme

Trois usages à distinguer

USAGE	EXEMPLE	PAGE LIÉE
Importer vers la connaissance	Importer documents SharePoint, tickets Jira ou pages Confluence	Connaissance
Publier un livrable	Publier un Document PM vers SharePoint	Documents PM
Créer une action externe	Créer un ticket Jira ou envoyer une notification	Actions et approbations

Checklist avant usage

Un connecteur est utilisable uniquement si les conditions suivantes sont réunies :

CONDITION	VÉRIFICATION
Plateforme prête	L'intégration est définie et validée par l'administrateur
Projet rattaché	Le projet actif utilise cette intégration
Politique compatible	La gouvernance autorise l'action ou demande une approbation
Rôle suffisant	Votre rôle peut importer, proposer, approuver ou publier
Santé OK	Le connecteur est prêt et non bloqué
Mode live actif	Les actions externes réelles sont autorisées si nécessaire

Importer depuis une source approuvée

1. Ouvrez [Connaissance](#).
2. Choisissez l'action d'import.
3. Sélectionnez la source disponible.
4. Lancez l'import.
5. Consultez l'historique d'import et les statuts.
6. Vérifiez que les documents deviennent **Indexed**.

Publier vers SharePoint

1. Ouvrez [Documents PM et artefacts](#).
2. Sélectionnez le Document PM relu.
3. Vérifiez la destination proposée.
4. Soumettez la publication si votre rôle le permet.
5. Attendez l'approbation si la politique l'exige.
6. Vérifiez le statut final et la trace dans le Journal IA ou l'activité.

Créer un ticket Jira depuis un signal

1. Ouvrez [Signaux et notifications](#).
2. Sélectionnez le signal pertinent.
3. Choisissez l'action de création de ticket si elle est disponible.
4. Vérifiez le titre, la description, la priorité et les preuves.
5. Soumettez l'action.
6. Suivez l'approbation puis l'exécution dans [Actions et approbations](#).

Si cela ne fonctionne pas

SYMPTÔME	CAUSE PROBABLE	ACTION RECOMMANDÉE
Connecteur visible mais inutilisable	Non rattaché au projet ou santé non prête	Demandez au Project Owner ou à l'admin plateforme
Action externe bloquée	Politique, rôle ou mode live	Ouvrez Actions et approbations
Import incomplet	Source, filtre ou droits source insuffisants	Vérifiez l'historique d'import
Publication absente	Destination non configurée	Vérifiez Intégrations plateforme

Suite

- Pour l'administration, ouvrez [Intégrations plateforme](#).
- Pour les actions, ouvrez [Actions et approbations](#).
- Pour le support, ouvrez [Support, audit et diagnostic](#).

Projets et espace de travail

Accueil · Projets et espace de travail

ProPM Agent
Cockpit de livraison IA

PROJET ACTUEL
Azure Bay Hotel & Convention Center
Ouvrir l'espace de travail

Tableau de bord
Projets
Espace de travail
Connaissance
Agents
Rapports & artefacts
Journal IA
Centre de commande portefeuille
Administration de la plateforme

Utilisateur
mock.user@contoso.c...

Azure Bay Hotel & Convention Cent ?

Appuyez sur Ctrl+K / ⌘K pour les commandes

Océan

Français

Aide

Santé

Azure Bay Hotel & Convention Center ? ID projet demo-hotel1-001

Demo construction program: 220-room upscale hotel, conference center, and wellness facilities in Tunis.

Statut : active Data language: English Contrôles d'administration démo activés

Comment cet espace utilise le contexte projet
Workspace est ancré à un seul projet actif à la fois. Le projet sélectionné ici devient le contexte mémorisé pour Agents, Knowledge, Reports et AI Log jusqu'à ce que vous changiez de projet ou que vous l'effaciez depuis le répertoire Projects.

AIDE
L'espace de travail est votre hub central pour gérer les projets, configurer les agents et surveiller les activités de gestion de projet pilotées par l'IA. Aide

Aperçu de l'espace de travail Résumé du projet Lancement d'exécution Historique & Continuité Transparence opérationnelle Flux d'exécution & de révision

Console d'exécution ?

OUVRIR LES SURFACES LIÉES ?

Agents Documents PM

Ouvrir la connaissance Journal IA

Sorties structurées Preuves + fraîcheur Révision de brouillon Actions soumises à approbation

CONTINUITÉ DES CHATS ENREGISTRÉS ?

Le projet de démonstration contient des conversations enregistrées sur la page Agents. Ouvrez d'abord un ancien chat, puis démarrez-en un nouveau pour comparer la continuité.

VOIX ?

Utilisez le microphone sur la page Agents lorsque votre navigateur prend en charge la reconnaissance vocale. Si la voix n'est pas disponible, le même flux fonctionne toujours avec des invites saisies.

Objectif

Cette page explique la différence entre **Projets**, **Espace de travail** et **Agents**, puis détaille les réglages projet réellement visibles dans l'application.

Trois surfaces à distinguer

SURFACE	QUAND L'UTILISER
Projets	Créer un projet, ouvrir un projet existant, changer de contexte
Espace de travail	Lire le résumé projet, la transparence opérationnelle, les signaux et les réglages de niveau projet
Agents	Lancer un échange en direct avec un agent et lire la sortie structurée du run

En pratique, **Projets** sert à entrer dans le bon contexte, **Espace de travail** à le configurer et **Agents** à l'exploiter.

Le rôle exact du projet actif

Le **projet actif** est le contexte actuellement appliqué aux pages de travail projet. Concrètement, il détermine :

- les documents visibles dans **Connaissance** ;
- les runs lancés dans **Agents** ;
- les PM Docs, artefacts et diff visibles dans **Rapports & artefacts** ;
- les runs et événements affichés dans **Journal IA** ;
- les signaux, intégrations et politiques affichés dans **Espace de travail**.

Il ne faut donc pas confondre :

- **projet actif** : contexte opérationnel courant ;
- **Portfolio** : vue de comparaison multi-projets ;
- **All projects** : portée éventuelle d'un agent personnalisé visible dans plusieurs projets pour le même compte.

Créer un projet

Le formulaire contient les champs suivants :

- **ID projet** ;
- **Nom** ;
- **Description** ;
- **Langue de données par défaut** ;
- **Langues de données supplémentaires**.

Recommandations de saisie :

- choisissez un ID lisible et durable ;
- ne confondez pas **langue de données projet** et **langue d'interface** ;
- définissez correctement le périmètre avant d'ouvrir la connaissance ou les agents.

Créateur du projet : droits initiaux et délégation

À la création, le **créateur du projet** démarre avec le rôle **Propriétaire du projet** et l'ensemble des permissions projet disponibles. En pratique, c'est donc lui qui peut ouvrir le projet, vérifier la configuration initiale et **déléguer ensuite les rôles** au reste de l'équipe.

Délégation recommandée juste après la création

1. ouvrez **Contrôle d'accès** ;
2. ajoutez au moins un autre **Propriétaire du projet** ou un **Chef de projet** de confiance ;
3. créez si besoin des rôles personnalisés ciblés plutôt que de multiplier les propriétaires ;
4. attribuez ensuite les rôles aux contributeurs, lecteurs et auditeurs ;
5. relisez enfin les **Politiques de gouvernance** et les **Intégrations du projet** pour aligner droits, connecteurs et validations.

Ce que la plateforme protège encore

- l'entrée du **créateur** reste protégée ;
- le rôle du créateur reste fixe dans l'interface ;
- la délégation se fait par attribution de rôles supplémentaires, pas par suppression de la protection du créateur ;
- pour le détail RBAC, voir [Contrôle d'accès et rôles projet](#).

Ouvrir et changer de projet

Un projet peut être ouvert depuis :

- la page **Projets** ;
- le **sélecteur de projet** de la barre supérieure ;
- le contexte récemment mémorisé dans le navigateur.

Lorsque vous changez de projet, les surfaces suivantes se recalent : **Connaissance, Agents, Documents PM / Rapports & artefacts, Journal IA**, les signaux et les réglages projet.

Ce changement de projet modifie donc réellement le **contexte actif** utilisé par la recherche documentaire, les conversations agents, les rapports et les traces associées. Le dernier projet retenu peut être mémorisé localement par le navigateur pour faciliter la reprise, mais cette mémoire locale n'est pas un réglage partagé à toute la plateforme.

L'espace de travail : centre de pilotage du projet

L'**Espace de travail** réunit dans une même surface :

- le **résumé projet** ;
- des raccourcis vers **Agents, Documents PM** et **Journal IA** ;
- une vue de **transparence opérationnelle** ;
- les **signaux** du projet ;
- les onglets de réglage de niveau projet.

L'**Espace de travail** ne présente plus de carte **voix** dédiée. Quand une saisie vocale existe encore dans certains environnements, elle est disponible dans **Agents**, pas comme point d'entrée séparé de l'espace de travail.

Transparence opérationnelle et préparation

L'espace de travail ne sert pas seulement à résumer le projet. Il permet aussi de voir si le projet est prêt à agir :

- présence ou absence de signaux ;
- activité récente ;
- raccourcis vers les brouillons ou livrables liés ;
- préparation des intégrations projet quand elles existent ;
- exposition du fournisseur IA effectif sans ouvrir la configuration tenant.

Utilisez cette zone pour comprendre **pourquoi** une action ou un import peut être disponible, à confirmer ou bloqué.

Moyen Ouvert Suggest

Créer un brouillon Reporter 24 h

Contradictory status signals detected

A narrative source and an operational source disagree on the current dependency posture.

Pourquoi il a été généré : Generated because the current narrative implies the dependency is stable while another source still reports an active watchpoint.

1 références de preuve Déclenché 3 fois

ÉTAPES SUIVANTES SUGGÉRÉES

- Capture the contradiction explicitly in the next briefing artifact.

knowledge: Récent connector:primavera-primary: Contradictoire

Dernière détection : 21/04/2026 14:04:58

Moyen Reporté Draft

Créer un brouillon Reporter 24 h

Approved publication follow-up pending

A reviewed artifact still needs its governed publication follow-up.

Pourquoi il a été généré : Generated because the approved draft has not yet been pushed through the governed publication path.

1 références de preuve

ÉTAPES SUIVANTES SUGGÉRÉES

- Review the action queue and publish the approved artifact if it is ready.

artifacts: Vieillissant actions: Vieillissant

Dernière détection : 21/04/2026 13:19:58 • Reporté jusqu'au 22/04/2026 02:49:58

DERNIER DIGEST ?

Hotel proactive digest Généré 21/04/2026 14:29:58

High-priority signals currently focus on stale schedule evidence, an explicit contradiction, and delayed follow-up on a reviewed artifact.

2 signaux résumés 1 brouillons préparés

[Élevé] **Schedule freshness degraded** Schedule evidence is older than the latest project narrative and should be reviewed before publication.

[Moyen] **Contradictory status signals detected** A narrative source and an operational source disagree on the current dependency posture.

Comment arrivent les signaux, digests et brouillons

Dans l'interface, le panneau de signaux du projet relit trois flux partagés pour le **projet actif** :

- les **signaux** courants ;
- les **digests** récents ;
- les **brouillons de notification** liés à ces signaux.

Lecture utile :

- l'ouverture de l'espace de travail recharge l'état partagé déjà connu pour ce projet ;
- **Refresh** demande explicitement au système de réévaluer le projet et de tirer les derniers signaux proactifs ;

- **Generate digest draft** construit une nouvelle synthèse groupée et peut préparer des notifications `in_app` ;
- ces éléments ne sont donc pas de simples notes locales du navigateur.

Onglets de niveau projet

ONGLET	À QUOI IL SERT
Configuration des agents	Paramétrer les agents pour ce projet
Contrôle d'accès	Gérer membres, rôles et permissions de niveau projet
Catégories de documents	Adapter la taxonomie documentaire du projet et la propager aux surfaces documentaires du projet
Politiques de gouvernance	Définir connecteurs, destinations, politiques d'action, profils de rendu et préférences de notification de niveau projet
Intégrations du projet	Relier au projet les intégrations prêtes et autorisées
Actions & approbations	Gérer les demandes d'action, validations et exécution gouvernée

Configuration des agents

Les paramètres confirmés au niveau projet sont :

- `status` ;
- `temperature` ;
- `max tokens` .

Contraintes visibles

- `temperature` est attendue entre **0** et **2** ;
- `max tokens` doit être un entier supérieur ou égal à **1**.

Historique de configuration

L'interface expose aussi un historique par version avec au minimum :

- numéro de version ;
- statut ;
- température ;

- max tokens ;
- date de création ;
- auteur ;
- **Trace ID** associé.

Configuration des agents du projet ?

Activez/désactivez les agents et ajustez les paramètres par projet.

Examinez la configuration d'exécution effective de chaque agent, modifiez une ligne à la fois et utilisez l'historique pour confirmer ce qui a changé.

STATUT 8 8 activés	DÉSACTIVÉ 0 0 désactivés	MODIFIER 0 0 lignes modifiées
--	--	---

Enregistrez les changements ligne par ligne afin que chaque ajustement reste traçable. Utilisez Réinitialiser pour annuler les modifications non enregistrées avant l'enregistrement.

Agent	Version	Statut ?	Température ?	Jetons max. ?	Actions ?
Virtual Project Manager default Routes your request to the right performance-domain specialist agents, then synthesizes a single value-focused answer. Principles: Adopt a Holistic View; Focus on Value; Embed Quality; Be an Accountable Leader; Integrate Sustainability; Build an Empowered Culture.	En attente du premier enregistrement	activé ▼	0.2 <small>Actuel : 0.2</small>	1024 <small>Actuel : Non défini</small>	Enregistrer Réinitialiser Historique
Governance Lead default Ensures appropriate oversight, decision making, compliance, and alignment with organizational policies. Principles: Adopt a Holistic View; Focus on Value; Embed Quality; Be an Accountable Leader; Integrate Sustainability; Build an Empowered Culture.	En attente du premier enregistrement	activé ▼	0.2 <small>Actuel : 0.2</small>	1024 <small>Actuel : Non défini</small>	Enregistrer Réinitialiser Historique
Scope Lead default Defines and manages the boundaries of the project, including quality expectations. Principles: Adopt a Holistic View; Focus on Value; Embed Quality; Be an Accountable Leader; Integrate Sustainability; Build an Empowered Culture.	En attente du premier enregistrement	activé ▼	0.2 <small>Actuel : 0.2</small>	1024 <small>Actuel : Non défini</small>	Enregistrer Réinitialiser Historique
Schedule Lead default Establishes timelines, sequences work, and	En attente du premier enregistrement	activé ▼	0.2 <small>Actuel : 0.2</small>	1024 <small>Actuel : Non défini</small>	Enregistrer Réinitialiser

Contrôle d'accès

L'onglet **Contrôle d'accès** administre les membres et rôles projet. Il supporte :

- les rôles standards ;
- les rôles personnalisés ;
- les garde-fous RBAC ;
- la lecture seule pour les profils non autorisés à modifier.

Voir la page dédiée : [Contrôle d'accès et rôles projet](#).

Catégories de documents

Cet onglet sert à aligner la classification documentaire avec le projet. En pratique, la taxonomie projet influence les catégories proposées lors des téléversements et certains sélecteurs documentaires utilisés ensuite dans les surfaces projet.

Effet concret d'une mise à jour

Quand la liste des catégories est modifiée avec succès :

- le sélecteur de catégorie de téléversement dans **Connaissance** est mis à jour ;
- les sélecteurs et filtres de catégorie dans **Documents PM** se recalent quand ils utilisent cette taxonomie partagée ;
- le changement reste limité au **projet courant**.

Exemples pratiques

Gardez une taxonomie courte et stable. Par exemple, au lieu de multiplier les variantes proches, préférez quelques catégories cohérentes comme :

- charte projet ;
- registre des risques ;
- rapport de statut ;
- plan achats ;
- plan de communication.

L'objectif n'est pas d'encoder la version du document dans la catégorie, mais de garder un classement réutilisable entre **Connaissance** et **Documents PM**.

Catégories de documents ?

Configurez la liste des catégories utilisée dans tout le projet (uploads Knowledge + catégories des PM Docs).

Nouvelle catégorie ?

ex. Architecture Ajouter ? Réinitialiser les valeurs par défaut ?

Status / SteerCo RAID Architecture Requirements Design Test Plan Release Notes Meeting Notes Vendor

Finance Security Operations Business Case Benefits Management Plan Project Charter Change Management Plan

Communications Management Plan Procurement Management Plan Quality Management Plan Resource Management Plan Risk Management Plan

Schedule Management Plan Scope Management Plan Stakeholder Engagement Plan Assumption Log Issue Log Lessons Learned Register

Milestone List Risk Register Stakeholder Register Status Report

Astuce : gardez une liste courte et stable. Vous pourrez toujours marquer les uploads avec une catégorie personnalisée plus tard via les métadonnées.

Politiques de gouvernance

Cet onglet fixe les règles qui encadrent les décisions, validations et comportements de gouvernance du projet. Utilisez-le avant de publier un livrable ou d'autoriser une action externe gouvernée.

Sous-surfaces visibles dans Politiques de gouvernance

SOUS-SURFACE	CE QU'ELLE RÈGLE
Connecteurs d'exécution	Type de connecteur, statut, mode d'exécution, environnement, scopes et paramètres de contexte
Destinations des artefacts	Destination cible d'un artefact, connecteur associé, caractère actif ou par défaut
Politiques d'action	Rôle concerné, connecteur ciblé, niveau d'action (<code>observe</code> , <code>draft</code> , <code>propose</code> , <code>execute</code>), effet (<code>allow</code> , <code>require_approval</code> , <code>deny</code>) et scopes autorisés
Profils de rendu	Profils de rendu et format de sortie utilisés lors des publications gouvernées
Préférences de notification	Canal, type de notification, mode de digest, seuil de sévérité et activation de la préférence

Exemples de réglages utiles

- exiger une approbation explicite avant une publication vers **SharePoint** ;
- autoriser la création de ticket **Jira** seulement au niveau `propose` pour certains rôles ;
- préparer des préférences `signal_digest` en `in_app` pour le suivi interne ;
- laisser les notifications externes `email` , `teams` ou `webhook` dans un chemin approuvé seulement lorsque le connecteur est sain ;
- choisir des profils de rendu séparés pour les publications **DOCX** et **XLSX**.

Scénario crédible — projet sensible / diffusion gouvernée

Pour un projet où toute diffusion externe doit être contrôlée, un réglage cohérent ressemble souvent à ceci :

- Destinations des artefacts** : destination SharePoint active avec profil de rendu connu ;
- Politiques d'action** : `allow` pour `observe` et `draft`, mais `require_approval` pour `execute` sur les publications et notifications externes ;
- Connecteurs d'exécution** : connecteurs externes visibles seulement pour les rôles réellement autorisés ;
- Préférences de notification** : `signal_digest` en `daily` pour l'équipe, `signal_alert` seulement pour les cas les plus sensibles ;
- Intégrations du projet** : rattachements activés uniquement pour les connecteurs déjà validés au niveau plateforme.

Cette combinaison évite qu'un brouillon, un digest ou une action apparaisse comme directement diffusable alors que le projet attend encore une approbation humaine.

Politiques de gouvernance

Configurez les connecteurs gouvernés, destinations, politiques d'action, profils de rendu, contraintes de fraîcheur et digests de notification.

CONNECTEURS
3

DESTINATIONS
2

POLITIQUE D'ACTION
2

PROFILS DE RENDU
2

PARAMÈTRES DE NOTIFICATION
1

Review and save each governance object independently so connector posture, routing destinations, action boundaries, rendering behavior, and notification rules stay easy to audit.

TYPES D' ACTIONS GOUVERNÉES

Pублиer l'artefact dans SharePoint
Envoyer un message Teams
Envoyer un message Outlook
Créer un ticket Jira
Créer un ticket Azure DevOps
Créer un suivi calendrier

Connecteurs 3 configurés

Statut, mode d'exécution, environnement et posture de périmètre pour les actions adossées à des connecteurs.

Microsoft Graph / SharePoint
graph-sharepoint-primary • Microsoft Graph / SharePoint

Activé Simulation Fraîcheur : Fresh

Nom ? Type de connecteur ?

Microsoft Graph / SharePoint Microsoft Graph / SharePoint

Description ?

Statut ? Mode d'exécution ?

Activé Simulation

Environnement ? Référence de fixture ?

Jira Activé Simulation Fraîcheur : Vieillissant

jira-primary • Jira

Nom ? Type de connecteur ?

Jira Jira

Description ?

Statut ? Mode d'exécution ?

Activé Simulation

Environnement ? Référence de fixture ?

Intégrations du projet

Cet onglet sépare les intégrations **techniquement définies** au niveau plateforme de celles qui sont **réellement utilisables** par le projet.

Comment lire cet onglet

L'onglet **Intégrations du projet** n'est pas l'endroit où l'on configure toute la technique du tenant. Il sert surtout à lire la **préparation opérationnelle** projet : ce qui est visible pour ce projet, ce qui est prêt, et ce qui reste bloqué avec une raison explicite.

On y retrouve plusieurs familles d'informations :

- **Connecteurs d'exécution** : options de sortie gouvernée vers des systèmes externes ;
- **Fournisseurs d'ingestion** : sources d'import consommées ensuite par **Connaissance** ;
- **Transparence d'exécution IA** : fournisseur IA effectif et fournisseur sélectionné au déploiement ;
- **Posture licences** : plan actif, licences commandées, licences utilisées et licences restantes visibles.

Ce que montre l'écran Intégrations du projet

L'écran sépare la préparation technique de la disponibilité projet :

- la configuration plateforme, le rattachement projet, la politique, la permission, l'état de santé et la disponibilité de licence pour l'accès à l'app sont des **causes distinctes**. Un connecteur peut rester visible en lecture seule pour expliquer pourquoi il est bloqué au lieu de laisser croire qu'il manque ;
- la configuration technique reste dans **Administration de la plateforme**. Les responsables des paramètres projet peuvent rattacher les intégrations activées et prêtes, tandis que les informations sensibles restent centralisées dans l'administration sécurisée.

ZONE	CE QUE VOUS POUVEZ VOIR	COMMENT AGIR
Connecteurs d'exécution	une liste courante parfois vide, puis un catalogue disponible au rattachement avec Asta Powerproject schedule sync, Azure DevOps delivery project, Jira delivery workspace, Microsoft Project schedule sync, Microsoft Teams collaboration, Outlook executive notifications, SharePoint publication library, Smartsheet portfolio workspace, Webhook event delivery et Wrike delivery workspace	utilisez Bind to project seulement pour les connecteurs déjà activés et prêts au niveau plateforme
Fournisseurs d'ingestion	des fournisseurs comme Smartsheet sheet import et Azure Data Factory evidence pipeline marqués Healthy , puis des fournisseurs disponibles comme SharePoint knowledge import, Azure Blob document ingest, Confluence knowledge import, Jira issue import, SFTP document intake, Microsoft Project schedule import, Wrike task import et Asta Powerproject schedule import	utilisez Validate binding pour vérifier un fournisseur rattaché, Disable pour le fermer côté projet, ou Bind to project pour un fournisseur approuvé

Les cartes fournisseur peuvent afficher **Ready**, **Healthy** ou **Not configured**. **Not configured** signifie que le fournisseur existe dans le catalogue plateforme, mais qu'il manque encore une source, des identifiants ou une validation de préparation avant l'usage projet.

Pour les champs obligatoires, les probes, le mapping des actions et les limites d'exécution réelle, utilisez la page [Connecteurs et intégrations](#). **Ready** ou **Healthy** indique une préparation cohérente, mais ne prouve pas à lui seul qu'un ticket, un message ou un import externe complet a déjà été exécuté.

Causes de blocage affichées

Une intégration projet ou une option d'import peut être bloquée pour cause de :

- politique ;
- permission ;
- état de santé à vérifier ;
- définition plateforme absente ou désactivée ;
- rattachement projet désactivé ou non configuré ;
- configuration ou validation spécifique au fournisseur incomplète.

Comment interpréter un blocage de rattachement

CAUSE VISIBLE	LECTURE PRATIQUE	RÉFLEXE RECOMMANDÉ
entitlement	libellé hérité pour une intégration bloquée, pas une différence de fonctionnalité Marketplace	vérifiez configuration, validation, état de santé, rattachement, politique, rôle et disponibilité de licence en cas de blocage d'accès

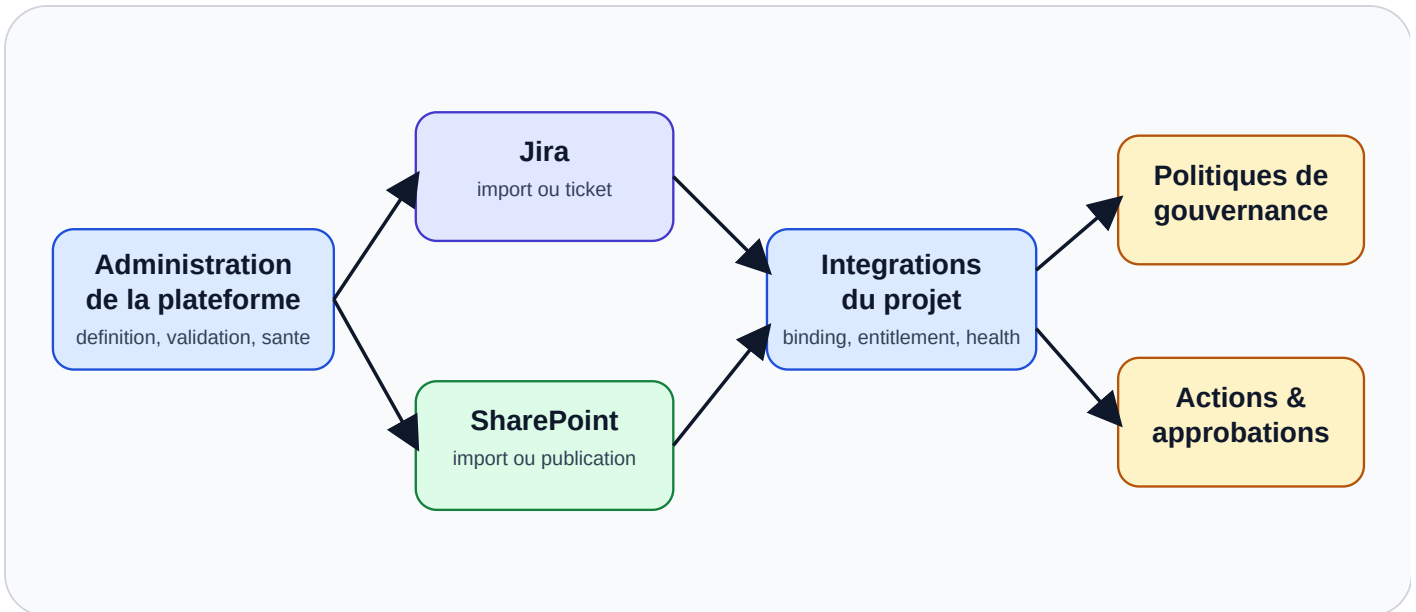
CAUSE VISIBLE	LECTURE PRATIQUE	RÉFLEXE RECOMMANDÉ
policy	la gouvernance projet interdit ou limite ce flux	relisez Politiques de gouvernance avant de modifier le rattachement
permission	le connecteur existe mais votre rôle ne permet pas de l'activer ou de l'utiliser	contrôlez le rôle projet dans Contrôle d'accès et rôles projet
health	la définition plateforme existe mais sa préparation ou sa disponibilité demandent une vérification	ouvrez l' Administration de la plateforme pour confirmer la définition technique
définition absente ou désactivée	rien n'est réellement prêt au niveau tenant	demandez d'abord la mise en place ou la réactivation plateforme
rattachement projet absent	la plateforme est prête mais le projet ne consomme pas encore l'intégration	activez explicitement le rattachement côté projet

Lecture pratique du rattachement et des licences

- **rattachement** : le connecteur ou fournisseur existe au niveau plateforme, mais il faut encore le rattacher et l'ouvrir au projet pour qu'il soit consommable dans ce projet ;
- **licence** : elle détermine si l'utilisateur dispose d'une licence disponible pour accéder à l'app. Les plans Marketplace ne débloquent ni ne bloquent des familles de connecteurs différentes ;
- un connecteur visible mais bloqué ne signifie donc pas qu'il est cassé : l'interface peut justement le laisser visible pour expliquer la raison du blocage.

Si un blocage persiste, ouvrez ensuite **Administration de la plateforme** pour vérifier la définition technique, puis revenez sur le projet pour confirmer le rattachement et la préparation.

Jira, SharePoint et chaîne des connecteurs



Gardez cette logique simple :

1. **Intégrations de la plateforme** définit le connecteur ou le fournisseur d'ingestion ;
2. **Intégrations du projet** expose seulement le rattachement approuvé et prêt ;
3. **Politiques de gouvernance** décide ce que chaque rôle peut observer, préparer, proposer ou exécuter ;
4. **Actions & approbations** applique ensuite ces règles lors de la demande réelle ;
5. **Documents PM** et **Journal IA** conservent la trace du flux.

Voir la page dédiée : [Connecteurs et intégrations](#).

Actions & approbations

Cet onglet transforme une recommandation en opération contrôlée.

Les états réels à retenir

Dans l'interface, la file et les cartes de synthèse distinguent surtout quatre états :

ÉTAT VISIBLE	LECTURE PRATIQUE
Prérequis d'exécution	des connecteurs compatibles peuvent exister, mais l'exécution reste bloquée par santé, configuration, rattachement, permission, politique, approbation ou préparation indisponible
En attente d'approbation	la demande a été proposée et attend encore une décision de gouvernance
Prêt à exécuter	la demande est en état <code>approved</code> , mais l'exécution reste une étape distincte

ÉTAT VISIBLE	LECTURE PRATIQUE
Historique d'exécution	l'action a réellement été exécutée et reste visible comme historique / preuve d'audit

Une action peut donc être en état **approved** sans être encore en état **executed**.

Comment lire un onglet qui paraît vide ou incomplet

La visibilité de l'onglet ne signifie pas qu'une action est déjà exécutable. Quand rien de concret ne semble disponible, la lecture la plus utile est souvent :

1. aucun **connecteur d'exécution compatible et sain** n'est prêt pour ce type d'action ;
2. le **rattachement projet** n'expose pas encore l'option au projet ;
3. une **policy** autorise la consultation mais pas la proposition ou l'exécution ;
4. votre **permission** permet de voir la file, mais pas d'agir ;
5. une approbation est requise et aucune décision n'a encore été prise.

Quand tout est correctement prêt, on s'attend au minimum à voir :

- un type d'action compatible ;
- au moins une option d'exécution saine ;
- un rattachement projet valide ;
- une policy cohérente ;
- un utilisateur autorisé à proposer, approuver ou exécuter selon le cas.

Ce qu'il faut lire dans **Execution préparation**

Le bloc **Execution préparation** n'administre pas toute la plateforme. Il résume simplement ce qui est actuellement proposable dans ce projet.

Lecture utile :

- **available / healthy** : option théoriquement utilisable ;
- **blocked by health** : le connecteur existe mais n'est pas dans un état opérationnel suffisant ;
- **blocked by entitlement** : libellé hérité indiquant un blocage ; vérifiez plutôt configuration, validation, rattachement, politique, rôle et disponibilité de licence si l'accès à l'app est bloqué ;
- **blocked by policy** : la gouvernance du projet bloque le passage ;
- **blocked by permission** : votre rôle ne suffit pas ;

- aucune option visible : aucun connecteur compatible approuvé n'est actuellement exposé au projet.

Lecture seule ou accès refusé

- **lecture seule** : l'onglet reste visible mais l'enregistrement est bloqué ;
- **accès refusé** : la route ou l'action n'est pas disponible pour votre compte.

Cette différence est particulièrement importante pour **Contrôle d'accès**, **Intégrations du projet** et les réglages de gouvernance.

Parcours recommandé après création d'un projet

1. ouvrez l'**Espace de travail** ;
2. vérifiez d'abord le **créateur**, les **membres** et les **rôles** si le projet est collaboratif ;
3. ajustez ensuite les **catégories de documents** ;
4. relisez les **Politiques de gouvernance** avant toute diffusion externe ;
5. reliez uniquement les **Intégrations du projet** réellement prêtes ;
6. chargez ensuite la **Connaissance** ;
7. passez enfin aux **Agents**, aux **Documents PM** et aux **Actions & approbations**.

Deux scénarios de paramétrage utiles

Scénario 1 — projet neuf minimal

Pour un projet qui démarre, gardez un ordre simple :

1. ajoutez les membres indispensables et vérifiez leurs rôles ;
2. créez une taxonomie documentaire courte dans **Catégories de documents** ;
3. activez seulement les intégrations déjà validées et vraiment nécessaires ;
4. préparez une gouvernance minimale, par exemple un digest interne et une destination d'artefact par défaut ;
5. chargez ensuite la **Connaissance** avant d'ouvrir les agents.

Ce scénario évite d'ouvrir trop tôt des connecteurs ou des règles de diffusion qui ne seront pas utilisés immédiatement.

Scénario 2 — projet sensible / diffusion gouvernée

Pour un projet exposé à des notifications externes ou à une publication documentaire formelle :

1. limitez les rôles ayant accès aux connecteurs externes ;
2. préparez une destination SharePoint ou équivalent dans **Destinations des artefacts** ;
3. appliquez `require_approval` sur les niveaux d'action qui peuvent produire une diffusion externe ;
4. privilégiez `signal_digest` pour le suivi courant et réservez les alertes instantanées aux cas critiques ;
5. ne rendez visibles dans **Intégrations du projet** que les rattachements dont la préparation et la politique sont déjà conformes.

Ce second scénario aligne lecture des signaux, diffusion, approbation et exécution réelle au lieu de laisser l'équipe traiter chaque écran comme une surface indépendante.

Suite

- [Contrôle d'accès et rôles projet](#)
- [Connaissance, documents et imports](#)
- [Gouvernance, décisions et actions](#)
- [Connecteurs et intégrations](#)
- [Administration Azure et plateforme](#)

Contrôle d'accès et rôles projet

Accueil · Contrôle d'accès et rôles projet

RBAC

Contrôle d'accès basé sur les rôles pour ce projet. Des rôles par défaut sont fournis ; vous pouvez créer des rôles personnalisés.

Créateur: Michael Carter Vous: mock.user@contoso.com

Rôles & permissions

Développez un rôle pour voir et modifier ses permissions.

Nouveau rôle ?

 Créer ?

Propriétaire du projet

Intégré

Accès complet au projet.

Voir le projet Modifier le projet Voir les documents Télécharger des documents Supprimer des documents Rechercher des documents Voir les documents PM

Modifier les documents PM +6 de plus

Chef de projet

Intégré

Peut exécuter des agents et gérer le travail quotidien du projet.

Voir le projet Voir les documents Télécharger des documents Rechercher des documents Voir les documents PM Modifier les documents PM Exporter les documents PM

Exécuter des agents +1 de plus

Contributeur

Intégré

Peut contribuer au contenu et exécuter des agents.

Voir le projet Voir les documents Télécharger des documents Rechercher des documents Voir les documents PM Modifier les documents PM Exporter les documents PM

Exécuter des agents

Lecteur

Intégré

Accès en lecture seule.

Voir le projet Voir les documents Rechercher des documents Voir les documents PM Exporter les documents PM

Auditeur

Intégré

Accès en lecture seule orienté audit.

Voir le projet Voir les documents Rechercher des documents Voir les documents PM Exporter les documents PM Voir RBAC

Membres

?

Attribuez des rôles aux utilisateurs (par e-mail) pour ce projet.

Contrôle d'accès projet

Attribuez d'abord des rôles métier, puis affinez le périmètre seulement quand le besoin le justifie.



1 Membres

Ajoutez les utilisateurs ou groupes au projet actif avant d'attribuer les permissions.

2 Rôles standards

Commencez par Propriétaire, Chef de projet, Contributeur, Lecteur ou Auditeur.

3 Rôles personnalisés

Utilisez-les seulement si les rôles standards sont trop larges, trop étroits ou non conformes.

4 Garde-fous RBAC

Prévenez auto-blocage, élévation imprévue, contournement de politique et accès excessif.

5 Trace d'audit

Conservez qui a changé l'accès, quand, et pourquoi le périmètre a été modifié.

Si un bouton est grisé, vérifiez rôle, politique et intégration

Un blocage vient généralement du rôle projet, d'une règle RBAC ou d'une intégration non autorisée.

Objectif

Cette page explique comment administrer les membres et rôles d'un projet ProPM Agent sans exposer les permissions techniques comme langage principal.

Pour qui

PROFIL	USAGE DE CETTE PAGE
Propriétaire de projet	Ajouter des membres, attribuer les rôles et créer des rôles personnalisés
Project Manager	Comprendre pourquoi une action est disponible, grisée ou absente
Auditeur	Vérifier la logique d'accès sans modifier le projet
Support	Identifier un blocage lié au rôle, au créateur ou à une auto-modification interdite

Avant de commencer

- Un projet actif est sélectionné.
- Vous connaissez le rôle métier que la personne doit jouer.
- Le compte à ajouter existe dans le tenant ou a été invité comme compte externe si nécessaire.
- Vous disposez du droit de gérer les membres ou les rôles.

Rôles standards

RÔLE	USAGE MÉTIER HABITUEL
Propriétaire du projet	Administre le projet, les membres, les rôles et les réglages sensibles
Chef de projet	Pilote le travail quotidien, les livrables, signaux et actions selon politique
Contributeur	Alimente la connaissance, lance des agents et contribue aux livrables autorisés
Lecteur	Consulte les informations sans modifier le projet
Auditeur	Relit les preuves, runs, lignée et traces selon les droits d'audit

Matrice simplifiée

ACTION COURANTE	PROPRIÉTAIRE	CHEF DE PROJET	CONTRIBUTEUR	LECTEUR	AUDITEUR
Lire le projet	Oui	Oui	Oui	Oui	Oui
Rechercher dans la connaissance	Oui	Oui	Oui	Oui	Oui
Lancer un agent	Oui	Oui	Oui	Non par défaut	Non par défaut
Préparer un livrable	Oui	Oui	Oui	Non	Non
Approuver ou publier selon politique	Oui	Selon politique	Selon politique	Non	Non

ACTION COURANTE	PROPRIÉTAIRE	CHEF DE PROJET	CONTRIBUTEUR	LECTEUR	AUDITEUR
Gérer membres et rôles	Oui	Non par défaut	Non	Non	Non
Auditer runs et traces	Oui	Oui	Selon rôle	Lecture limitée	Oui

Ajouter un membre

1. Ouvrez **Workspace** ou **Espace de travail**.
2. Ouvrez **Access control** ou **Contrôle d'accès**.
3. Sélectionnez l'onglet **Members** ou **Membres**.
4. Saisissez l'adresse e-mail du membre.
5. Choisissez le rôle standard ou personnalisé.
6. Enregistrez.
7. Vérifiez que la ligne du membre apparaît avec le rôle attendu.

Résultat attendu

- Le membre apparaît dans la liste.
- Le rôle affiché correspond à la délégation voulue.
- Le membre peut sélectionner le projet après reconnexion ou rafraîchissement.

Si l'ajout échoue

SYMPTÔME	CAUSE PROBABLE	ACTION RECOMMANDÉE
E-mail refusé	Format invalide ou compte non reconnu	Vérifiez l'adresse et l'invitation Entra si compte externe
Bouton grisé	Votre rôle ne permet pas de gérer les membres	Demandez l'action à un Propriétaire du projet
Membre ajouté mais projet invisible	Session non rafraîchie ou mauvais tenant	Demandez au membre de se reconnecter
Rôle impossible à choisir	Rôle supprimé, protégé ou indisponible	Choisissez un rôle standard ou recréez le rôle personnalisé

Créer un rôle personnalisé

1. Ouvrez **Roles and permissions** ou **Rôles et permissions**.
2. Sélectionnez l'action de création.
3. Donnez un nom métier clair.
4. Ajoutez une description qui explique le contexte d'usage.
5. Activez uniquement les capacités nécessaires.
6. Enregistrez le rôle.
7. Testez-le avec un utilisateur non critique avant diffusion large.

Propriétaire du projet Intégré

Accès complet au projet.

Voir le projet Modifier le projet Voir les documents Télécharger des documents Supprimer des documents Rechercher des documents Voir les documents PM
Modifier les documents PM +6 de plus

<input checked="" type="checkbox"/> Voir le projet Voir l'espace de travail et les métadonnées du projet.	<input checked="" type="checkbox"/> Modifier le projet Modifier les données et la configuration au niveau du projet.
<input checked="" type="checkbox"/> Voir les documents Voir les documents et les connaissances du projet.	<input checked="" type="checkbox"/> Télécharger des documents Télécharger des documents de projet.
<input checked="" type="checkbox"/> Supprimer des documents Supprimer des documents de projet.	<input checked="" type="checkbox"/> Rechercher des documents Rechercher dans les documents et les connaissances du projet.
<input checked="" type="checkbox"/> Voir les documents PM Voir les documents de gestion de projet.	<input checked="" type="checkbox"/> Modifier les documents PM Modifier les documents de gestion de projet.
<input checked="" type="checkbox"/> Exporter les documents PM Exporter les documents de gestion de projet.	<input checked="" type="checkbox"/> Exécuter des agents Exécuter des agents de projet et des workflows d'assistant.
<input checked="" type="checkbox"/> Configurer des agents Configurer des agents et des paramètres de projet.	<input checked="" type="checkbox"/> Voir RBAC Voir les paramètres de contrôle d'accès basé sur les rôles.
<input checked="" type="checkbox"/> Gérer RBAC Gérer les paramètres de contrôle d'accès basé sur les rôles.	<input checked="" type="checkbox"/> Manage project settings Manage project-level settings (categories, configs).

Les rôles intégrés sont en lecture seule. Créez un rôle personnalisé si vous avez besoin d'autorisations différentes.

Modifier un rôle personnalisé

1. Ouvrez le rôle dans **Rôles et permissions**.
2. Relisez sa description et les capacités activées.
3. Ajustez les capacités nécessaires.
4. Enregistrez.
5. Vérifiez l'impact sur les membres qui utilisent déjà ce rôle.

Supprimer un rôle personnalisé

1. Vérifiez qu'aucun membre n'utilise encore le rôle.
2. Remplacez ce rôle sur les membres concernés si nécessaire.

3. Utilisez l'action de suppression.
4. Confirmez que le rôle disparaît de la liste.

Un rôle système ne peut pas être supprimé. Un rôle personnalisé encore attribué est normalement bloqué pour éviter de retirer des droits de manière ambiguë.

Changer ou retirer un membre

1. Ouvrez la ligne du membre.
2. Changez le rôle via le sélecteur disponible, ou utilisez l'action de retrait.
3. Enregistrez.
4. Vérifiez que la liste affiche le nouvel état.

Vous ne pouvez pas vous auto-supprimer ou vous auto-rétrograder depuis cette page. L'entrée du créateur du projet reste également protégée.

Annexe admin : permissions techniques

Les libellés comme `project:read`, `agent:run`, `members:manage`, `roles:manage` ou `settings:manage` peuvent apparaître dans certains écrans ou exports. Ils servent au diagnostic RBAC avancé. Pour l'usage quotidien, raisonnez d'abord en rôles métier et en actions attendues.

Lecture seule vs accès refusé

ÉTAT	SIGNIFICATION	ACTION RECOMMANDÉE
Page visible mais contrôles grisés	Vous pouvez consulter mais pas modifier	Demandez le rôle approprié
Action absente	Le rôle ne permet pas cette action	Vérifiez la délégation avec le Project Owner
Erreur à l'enregistrement	Garde-fou serveur ou contrainte de rôle	Vérifiez créateur, auto-modification, rôle système ou rôle encore attribué

Suite

- [Projet actif et création de projet](#)

- Gouvernance, décisions et actions
- Actions et approbations
- Support, audit et diagnostic

Portfolio

Accueil · Portfolio

P ProPM Agent
Cockpit de livraison IA

PROJET ACTUEL
Azure Bay Hotel & Convention Center
Ouvrir l'espace de travail

- Tableau de bord
- Projets
- Espace de travail
- Connaissance
- Agents
- Rapports & artefacts
- Journal IA
- Centre de commande portefeuille**
- Administration de la plateforme

U Utilisateur
mock.user@contoso.c...

Azure Bay Hotel & Convention Cent ⓘ

Appuyez sur Ctrl+K / ⌘K pour les commandes

Océan

Français

Aide

Santé

3

Centre de commande du portefeuille

Gérer les projets Actualiser la comparaison

Comparez les projets sélectionnés avec des signaux configurables, des explications narratives et des preuves détaillées au lieu d'un tableau de bord fixe rouge-orange-vert.

AIDE Aide

Aperçu du portefeuille

La comparaison de portefeuille aide à comparer plusieurs projets à l'aide d'un modèle de signaux léger et configurable.

Aperçu du portefeuille Cohortes enregistrées Sélection des projets Profil de signaux Sévérité minimale Seuil global d'anomalie Résultats de comparaison

État de préparation de la comparaison

Comment interpréter Portfolio

Portfolio est une surface transverse de comparaison pour les revues de type PMO. Des résultats vides ou calmes peuvent signifier une sélection restrictive, des preuves limitées ou des projets réellement stables. Il faut donc le lire comme une aide comparative à la décision et non comme un verdict universel de santé.

Use this page for cross-project comparison and PMO-style triage. Use a project workspace when you need one project's documents, approvals, or execution context.

Cohortes ⓘ

Enregistrez des groupes de projets réutilisables avec un profil de comparaison.

Cohorte enregistrée ⓘ

Comparaison ad hoc

Nom de la cohorte ⓘ

Cohorte de revue de livraison

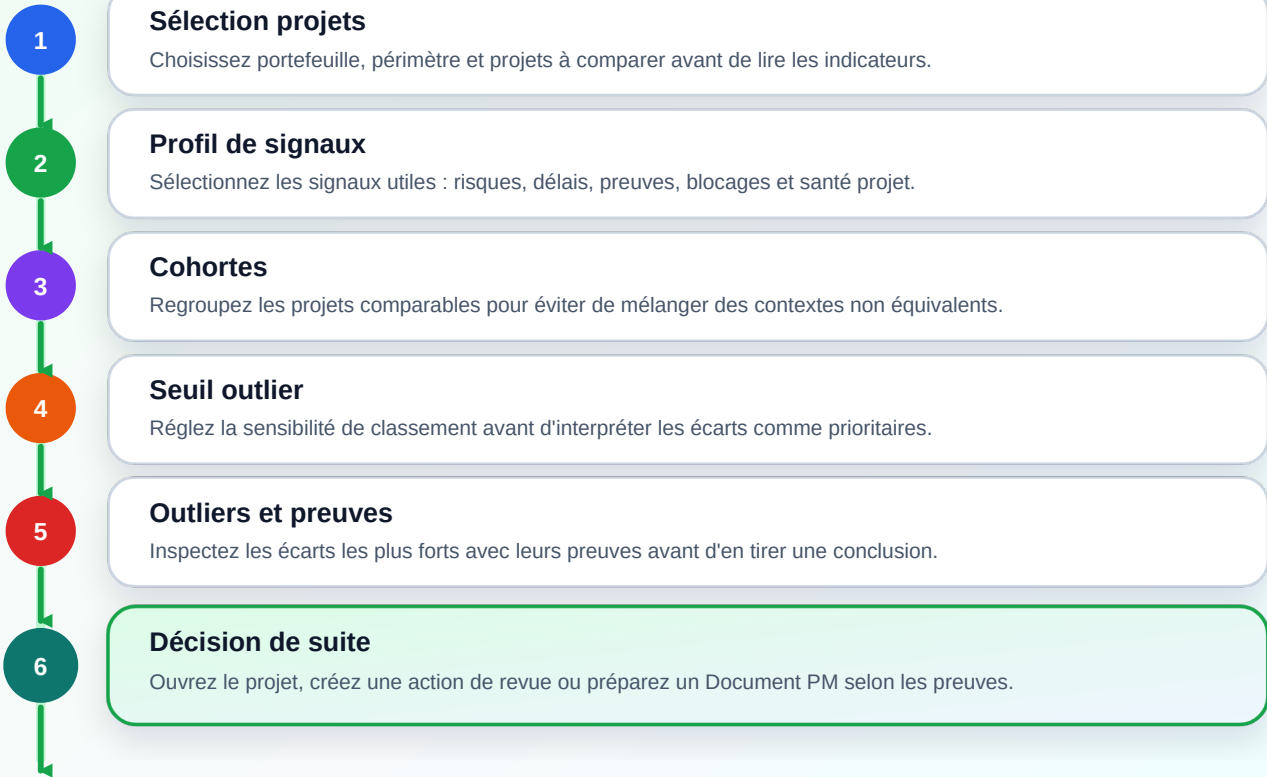
Comparison ready ⓘ

12 sur 12 sélectionnés • 7 signaux selected • Sévérité minimale: Afficher toutes les sévérités

PROJECTS COMPARED 12 Accessible projects in the current comparison	OUTLIERS 4 Projects exceeding the active signal profile	SIGNALS ENABLED 7 Comparative indicators currently applied	EVIDENCE GAPS 46 Signal / project combinations reported as unavailable
--	---	--	--

Workflow de revue Portfolio

Comparez les projets seulement après validation du périmètre, du profil de signaux, du seuil et des preuves.



Un outlier est une priorité de revue, pas une conclusion automatique

La décision finale dépend des preuves, du contexte projet et de la validation humaine.

Objectif

La page **Portfolio** aide les PMO et responsables de portefeuille à comparer plusieurs projets avec les mêmes signaux, puis à identifier les projets qui méritent une analyse prioritaire.

Pour qui

PROFIL	USAGE DE CETTE PAGE
PMO	Comparer plusieurs projets et préparer une revue portefeuille
Direction projet	Identifier les projets atypiques ou en tension
Project Manager	Comprendre pourquoi son projet ressort dans une comparaison

PROFIL	USAGE DE CETTE PAGE
Auditeur	Vérifier les preuves manquantes, contradictions et signaux indisponibles

Avant de commencer

- Vous avez accès à plusieurs projets.
- Les projets à comparer ont suffisamment de données, signaux ou preuves.
- Les seuils et poids doivent être adaptés à l'objectif de la revue.

Mots clés

TERME	SIGNIFICATION
Projects	Projets sélectionnés pour la comparaison
Signal profile	Ensemble de signaux, poids, seuils et sévérité minimale
Overall outlier threshold	Seuil global à partir duquel un projet ressort comme atypique
Refresh comparison	Recalcule la comparaison avec les paramètres courants
Reset defaults	Restaure les valeurs par défaut du profil
Cohorte	Configuration sauvegardée de projets et paramètres de comparaison
Snapshot	Résultat horodaté d'une comparaison à un moment donné

Sélectionner les projets

1. Ouvrez **Portfolio**.
2. Dans **Projects**, sélectionnez les projets à comparer.
3. Utilisez **Select all** si tous les projets accessibles doivent entrer dans la revue.
4. Utilisez **Clear all** pour repartir d'une sélection vide.
5. Vérifiez que les projets sélectionnés appartiennent au même objectif de pilotage.

Régler le profil de signaux

1. Ouvrez **Signal profile**.

2. Activez uniquement les signaux utiles à la revue.
3. Réglez le poids de chaque signal.
4. Réglez le seuil à partir duquel le signal devient significatif.
5. Choisissez la sévérité minimale pour réduire le bruit.
6. Réglez **Overall outlier threshold**.
7. Lancez **Refresh comparison**.

Exemples de profils PMO

REVUE	SIGNAUX À RENFORCER	OBJECTIF
Revue hebdomadaire delivery	schedule_pressure , blocker_density , activity_change	Repérer dérives et blocages opérationnels
Revue risques	contradiction_count , freshness_issues , blocker_density	Identifier preuves faibles et contradictions
Revue coûts	cost_pressure , failed_runs , activity_change	Voir les tensions budgétaires ou de consommation
Revue qualité des preuves	freshness_issues , contradiction_count , failed_runs	Prioriser les projets dont la base de preuve est fragile

Créer une cohorte

1. Sélectionnez les projets.
2. Réglez le profil de signaux.
3. Ouvrez l'éditeur de cohorte.
4. Donnez un nom clair, par exemple `Revue PMO hebdo delivery`.
5. Enregistrez.
6. Vérifiez que la cohorte est disponible pour une prochaine session.

Cohortes ⓘ

Enregistrez des groupes de projets réutilisables avec un profil de comparaison.

Cohorte enregistrée ⓘ

Comparaison ad hoc ▼

Nom de la cohorte ⓘ

Cohorte de revue de livraison

Description ⓘ

Projets actuellement examinés ensemble pour la santé de livraison du portefeuille.

Enregistrer la cohorte

Supprimer la cohorte

Modifier, supprimer ou recharger une cohorte

ACTION	ÉTAPES
Modifier	Chargez la cohorte, ajustez projets ou signaux, enregistrez à nouveau
Supprimer	Ouvrez la cohorte et utilisez l'action de suppression si disponible
Recharger	Sélectionnez la cohorte sauvegardée puis lancez Refresh comparison
Repartir des valeurs par défaut	Utilisez Reset defaults avant d'enregistrer une nouvelle cohorte

Une cohorte préconfigurée peut varier selon les environnements. Ne l'interprétez pas comme un modèle imposé si elle ne correspond pas à votre gouvernance.

Lire un outlier

Un **outlier** est un projet qui ressort selon les poids, seuils et signaux actifs. Ce n'est pas un verdict automatique.

Exemple métier

Un projet ressort fortement car `schedule_pressure` et `freshness_issues` dépassent les seuils. Lecture recommandée :

1. ouvrez le détail du projet dans Portfolio ;
2. vérifiez quels signaux expliquent le score ;
3. lisez les preuves et leur fraîcheur ;
4. ouvrez [Tableau de bord](#) ou [Signaux et notifications](#) pour le projet ;
5. ouvrez [Connaissance](#) si les preuves sont absentes ou anciennes ;
6. ouvrez [Journal IA](#) si le problème porte sur les runs ou le fournisseur IA effectif.

Signaux indisponibles et evidence gaps

Un signal indisponible ne signifie pas absence de risque. Il indique un manque de preuve ou de données exploitables pour calculer l'indicateur. Traitez les **evidence gaps** comme une demande de vérification, pas comme un feu vert.

Quand Portfolio paraît vide ou calme

SITUATION	LECTURE PROBABLE	ACTION RECOMMANDÉE
Aucun projet	Accès insuffisant ou sélection vide	Vérifiez les projets accessibles
Aucun outlier	Seuil trop élevé ou situation stable	Ajustez le seuil ou confirmez la stabilité
Résumé inexploitable	Données projet insuffisantes	Ouvrez la connaissance ou le tableau de bord
Snapshot ancien	Comparaison non recalculée récemment	Lancez Refresh comparison

Calcul et horodatage

Portfolio charge les projets accessibles, applique le profil de signaux, calcule les écarts et affiche un snapshot horodaté. Gardez l'explication simple : les poids expriment

l'importance relative, les seuils déclenchent l'attention et le score global sert à prioriser l'analyse.

Suite

- [Tableau de bord](#)
- [Signaux et notifications](#)
- [Journal IA](#)
- [Support, audit et diagnostic](#)

Déploiement Azure Marketplace

[Accueil](#) · Déploiement Azure Marketplace

Objectif

Cette page détaille le déploiement de **ProPM Agent** depuis **Azure Marketplace**. Elle explique les deux écrans principaux du formulaire Azure, le rôle de chaque champ visible et les contrôles à réaliser avant de cliquer sur **Review + create**.

Les captures ci-dessous correspondent au formulaire **Create ProPM-50**. Le nom affiché peut changer selon le plan Marketplace choisi, par exemple ProPM-50, ProPM-100 ou un autre plan disponible.

Pour qui

PROFIL	USAGE DE CETTE PAGE
Administrateur Azure	Créer la Managed Application depuis Azure Marketplace
Administrateur tenant	Préparer les groupes Entra et le premier accès administrateur
Administrateur plateforme	Comprendre les paramètres à finaliser après installation
Support	Vérifier le parcours sans demander de secret ni de variable interne
Utilisateur métier	Non, utiliser plutôt Démarrage

Avant de commencer

Préparez ces informations avant d'ouvrir le formulaire Marketplace.

INFORMATION	POURQUOI ELLE EST NÉCESSAIRE
Abonnement Azure cible	Il porte la transaction Marketplace et les ressources déployées
Groupe de ressources cible	Il organise l'objet Managed Application côté client
Région Azure cible	Elle détermine l'emplacement principal du déploiement
Nom d'application	Il identifie l'instance ProPM Agent dans Azure

INFORMATION	POURQUOI ELLE EST NÉCESSAIRE
Groupe de ressources managé	Il reçoit les ressources internes gérées par l'application
Group Object IDs Entra	Ils donnent l'accès administrateur à la plateforme
Utilisateurs bootstrap éventuels	Ils aident au premier accès ou à la récupération contrôlée
Fournisseur IA initial	Il indique la famille IA à préparer pour cette instance
Origines CORS éventuelles	Elles autorisent des domaines web additionnels si nécessaire
Plan réseau VNet CIDR	Il évite les conflits avec le réseau de l'organisation
Mot de passe initial	Il doit être généré et conservé comme secret

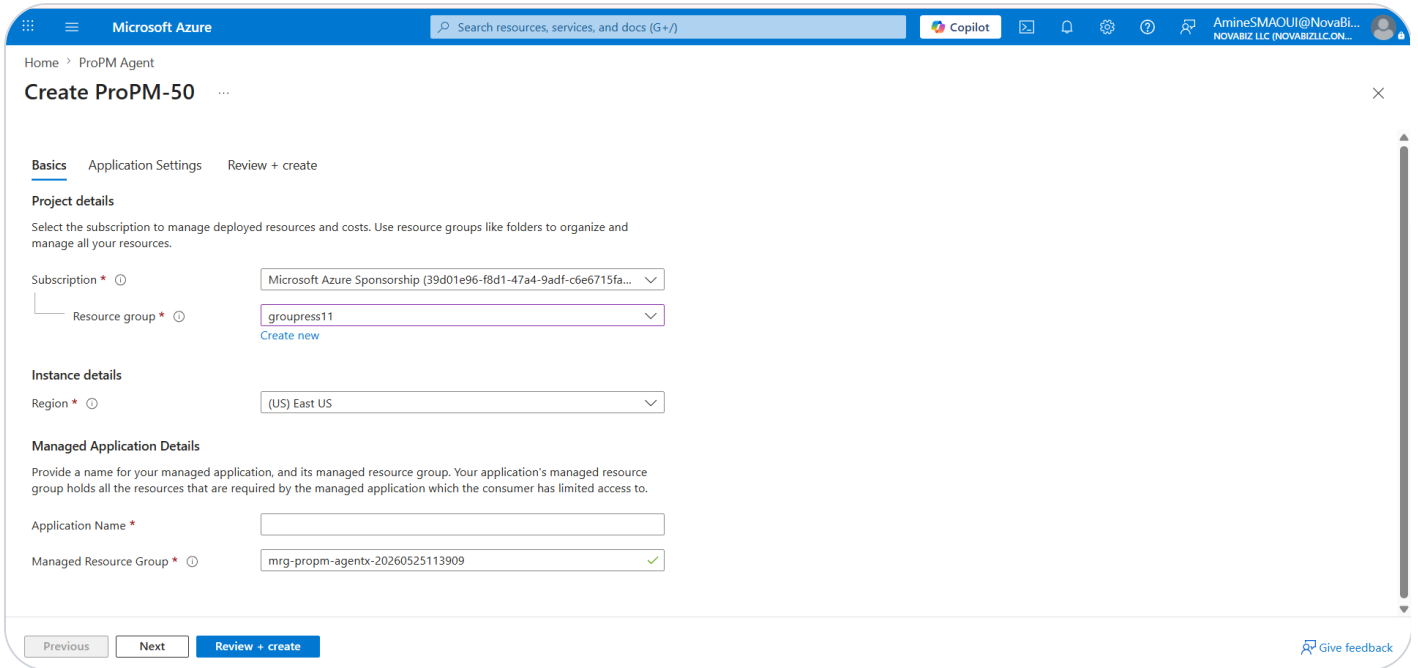
Ne copiez pas de mot de passe, secret, clé API, jeton ou valeur confidentielle dans la documentation ou dans une demande support non sécurisée.

Parcours de déploiement

1. Ouvrez l'offre ProPM Agent dans Azure Marketplace.
2. Sélectionnez le plan Marketplace voulu.
3. Remplissez l'onglet **Basics**.
4. Cliquez sur **Next**.
5. Remplissez l'onglet **Application Settings**.
6. Cliquez sur **Review + create**.
7. Corrigez les erreurs de validation éventuelles.
8. Lancez la création.
9. Attendez la fin du provisionnement Azure.
0. Ouvrez l'URL publiée et finalisez l'administration dans ProPM Agent.


Ecran 1 - Basics

L'onglet **Basics** définit le périmètre Azure du déploiement : abonnement, groupe de ressources, région et noms Azure de la Managed Application.



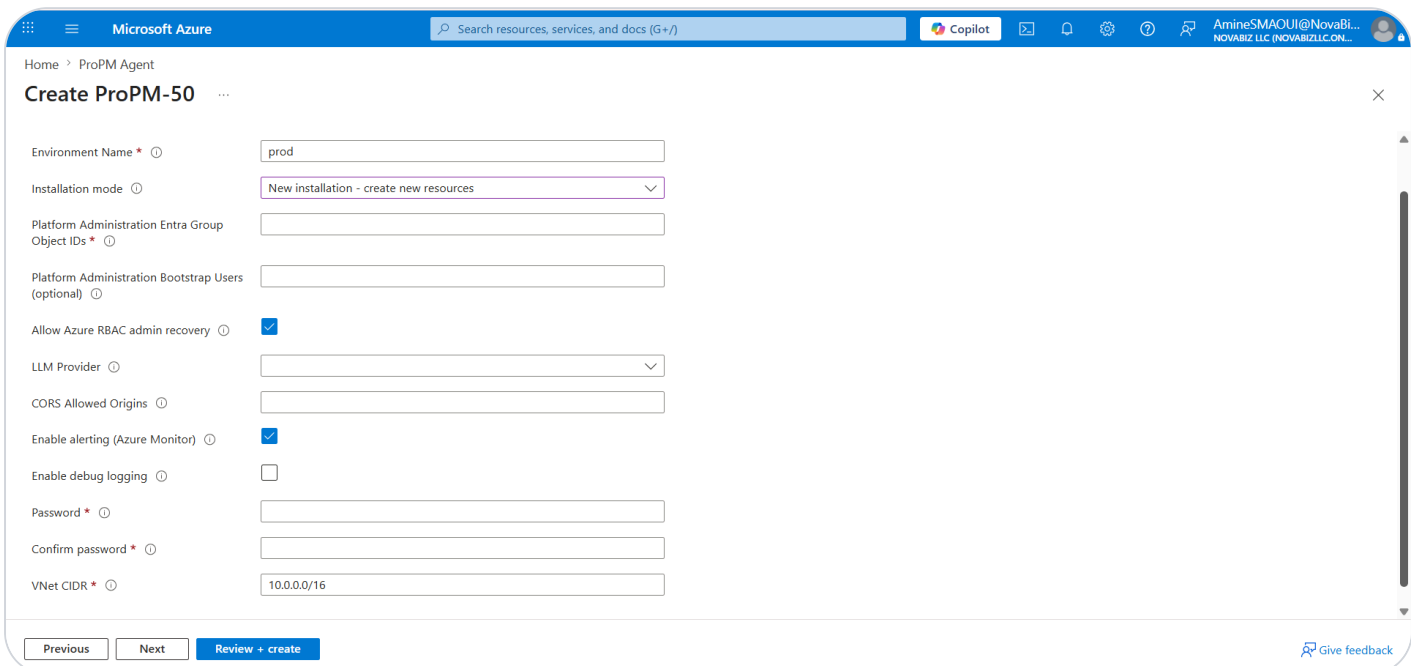
Champs de l'onglet Basics

CHAMP	OBLIGATOIRE	QUE RENSEIGNER	IMPACT ET RECOMMANDATIONS
Subscription	Oui	L'abonnement Azure qui recevra l'application managée et la facturation Marketplace.	Utilisez un abonnement où vous avez les droits de déployer une Managed Application et de créer ou sélectionner des groupes de ressources. Vérifiez aussi les règles internes de coûts et de gouvernance.
Resource group	Oui	Le groupe de ressources côté client qui contiendra l'objet Managed Application.	Vous pouvez choisir un groupe existant ou cliquer sur Create new . Ce groupe n'est pas le groupe managé interne qui contient les ressources techniques de ProPM Agent.
Create new	Non	Action Azure pour créer un nouveau groupe de ressources si aucun groupe adapté n'existe.	Donnez un nom clair, par exemple lié à l'environnement et à la région. Evitez les noms temporaires si l'instance est destinée à la production.
Region	Oui	La région Azure principale du déploiement.	Choisissez une région autorisée par votre organisation, proche des utilisateurs et compatible avec vos contraintes de résidence de données. Gardez une cohérence avec les ressources réseau et IA prévues.
Application Name	Oui	Le nom visible de l'instance Managed Application ProPM Agent.	Utilisez un nom stable et lisible, par exemple <code>propm-prod-eus</code> . Ce nom sert à reconnaître l'instance dans Azure. N'y mettez pas de secret ni de donnée client sensible.

CHAMP	OBLIGATOIRE	QUE RENSEIGNER	IMPACT ET RECOMMANDATIONS
Managed Resource Group	Oui	Le groupe de ressources managé qui recevra les ressources internes déployées par l'application.	Azure propose souvent un nom généré. Gardez un nom unique et reconnaissable. Ce groupe est géré par l'application ; les accès directs peuvent être limités selon le modèle Managed Application.
Previous	Non	Retourne à l'étape précédente du formulaire.	Aucun déploiement n'est lancé par ce bouton.
Next	Non	Passé à l'onglet suivant quand les champs requis sont suffisamment renseignés.	Utilisez-le pour continuer vers Application Settings . Si Azure bloque, relisez les champs obligatoires marqués par  .
Review + create	Non	Lance la validation Azure finale avant création.	Utilisez-le seulement après avoir rempli les paramètres d'application. Azure affiche ensuite les erreurs ou avertissements à corriger avant le lancement réel.

Ecran 2 - Application Settings

L'onglet **Application Settings** configure l'environnement ProPM Agent lui-même : identité d'administration, mode d'installation, fournisseur IA initial, CORS, supervision, journalisation, mot de passe initial et réseau.



The screenshot shows the 'Create ProPM-50' configuration page in the Microsoft Azure portal. The page is titled 'Create ProPM-50' and includes the following fields and options:

- Environment Name ***: Text input field containing 'prod'.
- Installation mode**: Dropdown menu set to 'New installation - create new resources'.
- Platform Administration Entra Group Object IDs ***: Text input field.
- Platform Administration Bootstrap Users (optional)**: Text input field.
- Allow Azure RBAC admin recovery**: Checkmark is checked.
- LLM Provider**: Dropdown menu.
- CORS Allowed Origins**: Text input field.
- Enable alerting (Azure Monitor)**: Checkmark is checked.
- Enable debug logging**: Checkmark is unchecked.
- Password ***: Text input field.
- Confirm password ***: Text input field.
- VNet CIDR ***: Text input field containing '10.0.0/16'.

At the bottom of the page, there are three buttons: 'Previous', 'Next', and 'Review + create' (highlighted in blue). A 'Give feedback' link is also visible in the bottom right corner.

Champs de l'onglet Application Settings

CHAMP	OBLIGATOIRE	QUE RENSEIGNER	IMPACT ET RECOMMANDATIONS
Environment Name	Oui	Un nom court pour l'environnement, par exemple <code>dev</code> , <code>test</code> , <code>uat</code> ou <code>prod</code> .	Ce nom aide à identifier l'environnement dans les ressources, la configuration et les échanges support. Utilisez une valeur courte, stable, sans secret et cohérente avec votre convention interne.
Installation mode	Selon le scénario	Le mode d'installation. Pour une première installation, gardez New installation - create new resources .	Ce mode crée une nouvelle instance avec de nouvelles ressources. N'utilisez un mode d'attachement à des ressources existantes que pour un scénario de changement de plan, mise à jour majeure ou reprise explicitement préparé.
Platform Administration Entra Group Object IDs	Oui	Les Object IDs des groupes Entra autorisés à administrer la plateforme.	Renseignez les Object IDs des groupes, pas seulement leurs noms d'affichage. Ces groupes déterminent qui pourra accéder à Platform Administration après déploiement. Préférez des groupes dédiés plutôt que des groupes trop larges.
Platform Administration Bootstrap Users (optional)	Non	Des utilisateurs de démarrage ou de récupération, si votre procédure le prévoit.	Utilisez ce champ pour sécuriser le premier accès quand les groupes Entra ne sont pas encore pleinement opérationnels. Gardez la liste minimale et contrôlée.
Allow Azure RBAC admin recovery	Non	Case à cocher permettant une récupération administrateur via Azure RBAC.	Laissez activé si votre modèle d'exploitation prévoit qu'un administrateur Azure autorisé puisse récupérer l'accès plateforme. Désactivez seulement si votre gouvernance impose une séparation stricte et documentée.

CHAMP	OBLIGATOIRE	QUE RENSEIGNER	IMPACT ET RECOMMANDATIONS
LLM Provider	Recommandé	La famille de fournisseur IA initiale : Azure OpenAI, OpenAI, OpenRouter ou OpenAI-compatible selon les choix disponibles.	Ce choix exprime l'intention initiale du déploiement. Il ne prouve pas que le fournisseur est déjà opérationnel. Après installation, finalisez le fournisseur dans Platform Administration > AI Provider Settings avec Save , Validate , Test puis Activate .
CORS Allowed Origins	Selon le scénario	Les origines web additionnelles autorisées, par exemple https://portal.contoso.com .	Laissez vide si aucune origine supplémentaire n'est nécessaire. Évitez les jokers trop larges. Les valeurs doivent être des origines complètes avec schéma https:// , domaine et port si nécessaire.
Enable alerting (Azure Monitor)	Non	Active ou désactive les alertes Azure Monitor créées pour l'environnement.	Recommandé pour la production afin de détecter les incidents. Vérifiez ensuite les destinataires, règles d'action et règles de coûts dans Azure Monitor.
Enable debug logging	Non	Active des journaux plus détaillés.	Gardez désactivé en production sauf demande de diagnostic. Le debug peut augmenter le volume de logs et exposer plus de détails techniques aux administrateurs autorisés.
Password	Oui	Le mot de passe initial demandé par le formulaire de déploiement.	Générez un mot de passe fort et stockez-le dans un coffre ou un gestionnaire de secrets approuvé. Ne l'envoyez pas par e-mail, chat ou ticket non sécurisé.
Confirm password	Oui	La même valeur que Password .	Azure valide que les deux champs correspondent. En cas d'erreur, saisissez à nouveau les deux valeurs depuis la source sécurisée.

CHAMP	OBLIGATOIRE	QUE RENSEIGNER	IMPACT ET RECOMMANDATIONS
VNet CIDR	Oui	La plage réseau privée réservée au déploiement, par exemple <code>10.0.0.0/16</code> .	Choisissez une plage qui ne chevauche pas vos réseaux existants, vos peerings, VPN ou plages futures prévues. Faites valider ce champ par l'équipe réseau avant la création, car il est difficile à changer après déploiement.
Previous	Non	Retourne à l'onglet Basics .	Utile pour corriger abonnement, groupe, région ou noms avant la validation finale.
Next	Non	Passe à l'étape suivante du formulaire.	Utilisez-le si vous voulez suivre l'ordre des onglets avant la validation.
Review + create	Non	Lance la validation finale de tous les paramètres.	Azure ne crée pas encore les ressources tant que vous n'avez pas confirmé la création après validation. Corrigez toutes les erreurs avant de lancer.

Choisir le champ LLM Provider

Le champ **LLM Provider** sélectionne la famille IA que l'environnement doit utiliser au départ. Ce n'est pas la fin de la configuration IA.

CHOIX	QUAND LE CHOISIR	CE QU'IL RESTE À FAIRE APRÈS INSTALLATION
Azure OpenAI	L'organisation veut rester dans l'écosystème Azure, Entra et gouvernance Microsoft.	Confirmer endpoint, région ou modèle disponible, paramètres Azure OpenAI, tests et activation.
OpenAI	L'organisation utilise directement les API OpenAI.	Renseigner l'URL, le modèle, la clé ou référence de secret, puis exécuter Save, Validate, Test, Activate .
OpenRouter	L'organisation veut accéder à plusieurs modèles via un point d'entrée unique.	Renseigner Base URL, clé ou référence de secret, modèle par défaut, puis valider et activer.
OpenAI-compatible	L'organisation utilise une passerelle ou un endpoint compatible OpenAI.	Renseigner endpoint exact, mode d'authentification, modèle ou déploiement attendu, puis tester réellement la compatibilité.

Règle simple : le déploiement **désigne** le fournisseur IA ; l'administration ProPM Agent le **rend opérationnel**.

Validation avant Review + create

Avant de lancer la création, contrôlez ces points.


CONTRÔLE	RÉSULTAT ATTENDU
Abonnement et groupe de ressources	Ils correspondent à l'environnement cible et aux règles de gouvernance
Région	Elle respecte résidence de données, disponibilité et stratégie réseau
Application Name	Le nom est clair, stable et non confidentiel
Managed Resource Group	Le nom est unique et reconnaissable
Group Object IDs Entra	Les IDs sont ceux des groupes prévus pour l'administration plateforme
Bootstrap Users	La liste est vide ou strictement limitée aux comptes prévus
RBAC recovery	Le choix est aligné avec la procédure de récupération administrateur
LLM Provider	Le fournisseur initial est cohérent avec la stratégie IA
CORS	Seules les origines nécessaires sont autorisées
Alerting	Activé pour les environnements qui doivent être supervisés
Debug logging	Désactivé sauf diagnostic encadré
Password	Stocké dans un coffre et jamais partagé en clair
VNet CIDR	Validé par l'équipe réseau et sans chevauchement connu

Après le déploiement

1. Attendez que le provisionnement Azure soit terminé.
2. Ouvrez l'URL publiée de ProPM Agent.
3. Connectez-vous avec un compte autorisé par les groupes Entra ou par la procédure bootstrap.
4. Vérifiez l'accès à **Platform Administration**.

5. Ouvrez les paramètres du fournisseur IA.
6. Exécutez **Save, Validate, Test** puis **Activate** pour le fournisseur retenu.
7. Vérifiez les licences et le plan Marketplace.
8. Réalisez un premier test fonctionnel avec un utilisateur standard.
9. Consultez le [Journal IA](#) après un run pour confirmer le fournisseur réellement utilisé.

Blocages fréquents

SYMPTÔME	CAUSE PROBABLE	ACTION RECOMMANDÉE
Azure refuse de passer à l'étape suivante	Champ obligatoire vide ou valeur invalide	Relisez tous les champs marqués  et les messages sous les champs
L'administrateur ne voit pas Platform Administration	Object ID Entra erroné ou groupe non propagé	Vérifiez l'Object ID du groupe et l'appartenance du compte
Conflit réseau après validation	VNet CIDR déjà utilisé ou chevauchant	Choisissez une autre plage avec l'équipe réseau
Fournisseur IA non utilisable après création	Le déploiement a seulement sélectionné la famille IA	Finalisez le fournisseur dans l'administration avec Save, Validate, Test, Activate
Trop de logs ou coûts inattendus	Debug logging ou alerting activés sans cadrage	Ajustez les paramètres Azure Monitor et désactivez le debug hors diagnostic

Suite

- Pour finaliser l'accès Entra, ouvrez [Administration Azure et Entra](#).
- Pour configurer le fournisseur IA, ouvrez [Fournisseur IA](#).
- Pour vérifier licences, plans et mises à jour, ouvrez [Licences, plans et mises à jour](#).
- Pour inviter les utilisateurs, envoyez [Démarrage](#).

Administration Azure et Entra

[Accueil](#) · Administration Azure et Entra

Objectif

Cette page s'adresse aux administrateurs Azure et tenant. Elle explique le parcours de déploiement Marketplace, la finalisation de l'accès Entra et les contrôles fonctionnels à réaliser avant d'inviter les utilisateurs.

Pour qui

PROFIL	USAGE DE CETTE PAGE
Administrateur Azure	Déployer la solution depuis Marketplace
Administrateur tenant	Valider l'accès Entra et les groupes autorisés
Support client	Vérifier les prérequis sans exposer de secret
Utilisateur métier	Non, sauf pour comprendre qui contacter

Avant de commencer

- Vous disposez des droits Azure nécessaires sur l'abonnement cible.
- Vous connaissez le tenant Entra et les groupes qui administreront ProPM Agent.
- Vous avez choisi la région, le plan Marketplace et la famille de fournisseur IA initiale.
- Les informations sensibles restent dans Azure ou l'administration sécurisée.

Déployer depuis Azure Marketplace

1. Ouvrez l'offre ProPM Agent dans Azure Marketplace.
2. Sélectionnez le plan et l'abonnement.
3. Renseignez le groupe de ressources, la région et les paramètres demandés.
4. Déclarez les groupes ou administrateurs Entra prévus.
5. Choisissez la famille de fournisseur IA initiale.
6. Lancez le déploiement.
7. Attendez la fin du provisionnement.

8. Récupérez l'URL publiée de l'application.

Finaliser l'accès Entra

1. Ouvrez l'URL de ProPM Agent avec un compte administrateur autorisé.
2. Validez le consentement Entra si l'organisation le demande.
3. Vérifiez que les administrateurs attendus accèdent à **Platform Administration**.
4. Invitez ensuite les premiers propriétaires de projet.
5. Demandez aux utilisateurs finaux de suivre [Démarrage](#), pas cette page.

Contrôles post-déploiement

CONTRÔLE	RÉSULTAT ATTENDU
Application accessible	La page de connexion puis l'accueil s'ouvrent
Entra opérationnel	Le compte autorisé se connecte sans boucle
Administration visible	Les administrateurs voient Platform Administration
Fournisseur IA à finaliser	Les paramètres IA sont visibles mais doivent être validés/testés
Licences lisibles	Le plan et les licences apparaissent dans l'administration

Ce qui relève d'autres pages

SUJET	PAGE
Save, Validate, Test, Activate du fournisseur IA	Fournisseur IA
Connecteurs et fournisseurs d'ingestion	Intégrations plateforme
Seats, licences et Refresh Marketplace plan	Licences, plans et mises à jour
Diagnostic avancé	Support, audit et diagnostic

Points d'attention

- Le fournisseur choisi pendant le déploiement est une intention initiale, pas la preuve du fournisseur réellement utilisé.

- Les utilisateurs métier n'ont pas besoin de connaître les variables Azure ou détails d'infrastructure.
- Ne copiez jamais de secret, clé, jeton ou configuration confidentielle dans une documentation ou une demande support.

Suite

- Configurez le fournisseur IA dans [Fournisseur IA](#).
- Vérifiez les licences dans [Licences, plans et mises à jour](#).
- Préparez les intégrations dans [Intégrations plateforme](#).

Fournisseur IA

Accueil · Fournisseur IA

P **ProPM Agent**
Cockpit de livraison IA

PROJET ACTUEL
Azure Bay Hotel & Convention Center
Ouvrir l'espace de travail

- Tableau de bord
- Projets
- Espace de travail
- Connaissance
- Agents
- Rapports & artefacts
- Journal IA
- Centre de commande portefeuille
- Administration de la plateforme**

U **Utilisateur**
mock.user@contoso.c...

Vue d'ensemble | Intégrations de la plateforme | Paramètres du fournisseur IA | Audit & activité

Connecteurs d'exécution ⚡
0
0 actifs • 0 dégradés / invalides

Fournisseurs d'ingestion ⬇️
0
0 actifs • 0 dégradés / invalides

Fournisseur IA effectif ⚡
Unavailable
Sélectionné par le déploiement :
Unavailable

Plan d'abonnement 🛡️
Unavailable
0 utilisés • 0 disponibles

Règles de fonctionnement de l'administration

L'interface applique les règles backend de lecture seule ou modifiable issues de allowed_actions et read_only_reason.

- Les intégrations de la plateforme restent réparties entre connecteurs d'exécution et fournisseurs d'ingestion.
- Les valeurs sensibles restent masquées ; seuls des champs API sans risque pour les métadonnées sont affichés.
- Les fournisseurs IA sélectionnés par le déploiement et effectifs sont affichés séparément.
- L'état de l'abonnement et des droits est rendu à partir de SubscriptionAdministrationView.

Plan du tenant et utilisateurs licenciés

La vue d'ensemble affiche le plan actuel du tenant. Les licences achetées et les utilisateurs dont l'accès repose actuellement sur une licence consommée.

PLAN ACTUEL
Unavailable
Le plan et le total des licences achetées sont synchronisés depuis l'abonnement Microsoft Marketplace actif lorsque l'accès fulfillment est configuré.

UTILISATION DES LICENCES
0 / 0
Aucun utilisateur supplémentaire du tenant ne peut se connecter tant qu'un administrateur n'a pas retiré un utilisateur licencié.

Règle de connexion
À chaque accès authentifié, l'application vérifie si cet utilisateur possède déjà une licence. Sinon, une licence disponible est consommée automatiquement, sauf si l'utilisateur a été retiré explicitement et doit être réattribué.

Fenêtre de retrait utilisateur
Retraits d'utilisateurs restants sur les prochaines 24 heures : 0.

Utilisateurs licenciés déjà connectés

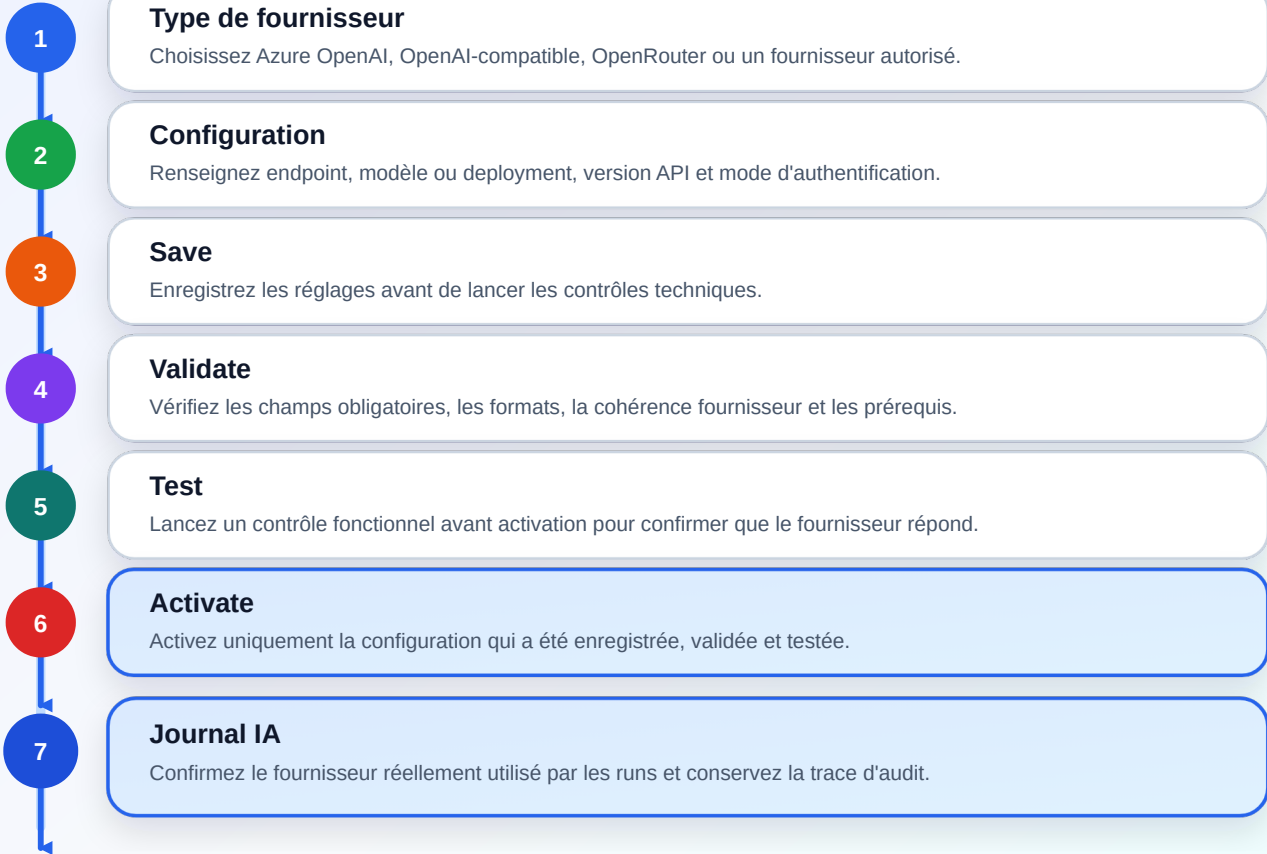
À chaque accès authentifié, l'application vérifie si l'utilisateur possède déjà une licence. Les utilisateurs retirés restent bloqués jusqu'à ce qu'un administrateur les réattribue, et les nouveaux utilisateurs sont bloqués lorsque toutes les licences achetées sont déjà consommées.

Activité administrative récente

L'historique d'activité et de validation reste consultable en mode modifiable comme en lecture seule.

Paramètres du fournisseur IA

Suivez la séquence d'administration : une configuration IA n'est fiable qu'après validation, test et activation contrôlée.



Ne copiez jamais secrets, clés API ou jetons dans un ticket

Utilisez des références sécurisées et contactez le support seulement avec des informations non sensibles.

Objectif

Cette page explique comment administrer le fournisseur IA de ProPM Agent et distinguer le fournisseur sélectionné au déploiement du fournisseur IA effectif observé dans un run.

Pour qui

PROFIL	USAGE DE CETTE PAGE
Administrateur tenant	Configurer et activer le fournisseur IA
Administrateur Azure	Fournir les informations Azure OpenAI ou fournisseur compatible
Support	Diagnostiquer une erreur de validation ou de test

PROFIL	USAGE DE CETTE PAGE
Utilisateur métier	Non, sauf pour savoir qui contacter

Avant de commencer

- Vous avez accès à **Platform Administration**.
- Vous connaissez le fournisseur à utiliser : Azure OpenAI, OpenRouter, OpenAI-compatible ou autre fournisseur exposé par votre environnement.
- Les secrets sont disponibles dans les outils d'administration sécurisés, pas dans cette documentation.

Comprendre les quatre actions

ACTION	RÔLE	ÉCHEC FRÉQUENT
Save	Enregistre la configuration saisie	Champ obligatoire manquant
Validate	Vérifie la cohérence de configuration	Endpoint, modèle ou authentification invalide
Test	Lance une vérification fonctionnelle	Fournisseur inaccessible ou déploiement absent
Activate	Rend la configuration active pour les runs	Validation ou test non réussi

Configurer le fournisseur

1. Ouvrez **Platform Administration**.
2. Sélectionnez **AI Provider Settings** ou **Paramètres du fournisseur IA**.
3. Choisissez le type de fournisseur.
4. Renseignez les champs demandés par l'interface.
5. Enregistrez avec **Save**.
6. Lancez **Validate**.
7. Lancez **Test**.
8. Activez avec **Activate** lorsque les contrôles sont réussis.
9. Lancez un run simple puis vérifiez le fournisseur effectif dans [Journal IA](#).

Azure OpenAI

Pour Azure OpenAI, l'administrateur doit vérifier les éléments fonctionnels suivants dans l'interface : endpoint, modèle ou deployment, version d'API, mode d'authentification et disponibilité réelle du déploiement côté Azure. Les clés, secrets et références sécurisées ne doivent pas être copiés dans les tickets utilisateurs.

Fournisseur sélectionné vs fournisseur effectif

SITUATION	LECTURE
Déploiement Marketplace	Choix initial de famille fournisseur
AI Provider Settings	Configuration actuellement enregistrée et activée
Journal IA	Preuve du fournisseur réellement utilisé par un run

Le Journal IA est la référence pour l'audit d'un résultat produit.

Erreurs fréquentes

SYMPTÔME	CAUSE PROBABLE	ACTION RECOMMANDÉE
Validate échoue	Champ incohérent ou fournisseur inaccessible	Corrigez la configuration puis relancez Validate
Test échoue	Modèle ou deployment indisponible	Vérifiez le fournisseur côté Azure ou plateforme externe
Activate est indisponible	Validation ou test non terminé	Terminez les étapes précédentes
Le run utilise un autre fournisseur	Configuration non activée, cache ou bascule temporaire	Vérifiez l'historique puis le Journal IA

Suite

- Pour confirmer un run réel, ouvrez [Journal IA](#).
- Pour l'administration des connecteurs, ouvrez [Intégrations plateforme](#).
- Pour un incident, ouvrez [Support, audit et diagnostic](#).

Intégrations plateforme

[Accueil](#) · Intégrations plateforme

Objectif

Cette page explique la différence entre intégration plateforme, rattachement projet, politique de gouvernance et usage réel par les utilisateurs.

Pour qui

PROFIL	USAGE DE CETTE PAGE
Administrateur plateforme	Définir et valider les intégrations
Propriétaire de projet	Demander ou vérifier un rattachement projet
Project Manager	Comprendre pourquoi un connecteur visible peut être inutilisable
Support	Identifier le niveau où l'intégration est bloquée

Avant de commencer

- Vous avez accès à **Platform Administration** pour la configuration globale.
- Le projet concerné existe et son propriétaire est identifié.
- Les secrets et informations d'authentification sont gérés dans les outils sécurisés prévus.

Les quatre niveaux à vérifier

NIVEAU	QUESTION À POSER
Plateforme	Le connecteur ou fournisseur d'ingestion est-il défini et validé ?
Projet	L'intégration est-elle rattachée au projet actif ?
Gouvernance	La politique autorise-t-elle l'action ou impose-t-elle une approbation ?
Exécution	La santé, le mode live et les droits permettent-ils l'action réelle ?

Définir et valider une intégration

1. Ouvrez **Platform Administration**.
2. Sélectionnez **Platform Integrations**.
3. Choisissez **Execution Connectors** ou **Ingestion Providers**.
4. Créez ou ouvrez la définition d'intégration.
5. Renseignez les champs demandés par l'interface.
6. Enregistrez la définition.
7. Lancez la validation.
8. Consultez l'historique de validation.
9. Désactivez l'intégration si elle ne doit plus être proposée.

Rattacher à un projet

1. Ouvrez le projet concerné.
2. Accédez aux intégrations projet.
3. Sélectionnez l'intégration validée côté plateforme.
4. Choisissez **Bind to project** ou le libellé équivalent.
5. Validez le rattachement.
6. Vérifiez la préparation, la santé et les actions disponibles.

Table de readiness

ÉTAT	SIGNIFICATION	ACTION RECOMMANDÉE
Ready	L'intégration est préparée pour l'usage prévu	Tester le parcours métier
Healthy	La vérification de santé est positive	Autoriser l'usage selon la politique
Not configured	La définition est incomplète ou absente	Compléter la configuration plateforme
Not bound	Le projet n'utilise pas encore l'intégration	Rattacher l'intégration au projet
Blocked	Rôle, politique, santé ou mode live bloque l'usage	Lire le détail puis corriger le niveau concerné

Points d'attention

- Un connecteur visible n'est pas forcément utilisable.

- Une définition plateforme ne suffit pas pour agir dans un projet.
- Une action externe ne crée réellement un objet que si le mode live est activé, validé et autorisé.
- Les champs techniques et secrets ne doivent pas être documentés dans le guide utilisateur final.

Suite

- Pour l'usage métier des connecteurs, ouvrez [Connecteurs et intégrations](#).
- Pour proposer ou approuver une action, ouvrez [Actions et approbations](#).
- Pour diagnostiquer un blocage, ouvrez [Support, audit et diagnostic](#).

Licences, plans et mises à jour

Accueil · Licences, plans et mises à jour

The screenshot displays the ProPM Agent administration dashboard. The top navigation bar includes 'Vue d'ensemble', 'Intégrations de la plateforme', 'Paramètres du fournisseur IA', and 'Audit & activité'. The main content area is divided into several sections:

- PROJET ACTUEL:** Azure Bay Hotel & Convention Center. Status: 0 actifs • 0 dégradés / invalides.
- Connecteurs d'exécution:** 0 actifs • 0 dégradés / invalides.
- Fournisseurs d'ingestion:** 0 actifs • 0 dégradés / invalides.
- Fournisseur IA effectif:** Unavailable. Sélectionné par le déploiement : Unavailable.
- Plan d'abonnement:** Unavailable. 0 utilisés • 0 disponibles.
- Règles de fonctionnement de l'administration:** L'interface applique les règles backend de lecture seule ou modifiable issues de allowed_actions et read_only_reason.
 - Les intégrations de la plateforme restent réparties entre connecteurs d'exécution et fournisseurs d'ingestion.
 - Les valeurs sensibles restent masquées ; seuls des champs API sans risque pour les métadonnées sont affichés.
 - Les fournisseurs IA sélectionnés par le déploiement et effectifs sont affichés séparément.
 - L'état de l'abonnement et des droits est rendu à partir de SubscriptionAdministrationView.
- Plan du tenant et utilisateurs licenciés:** La vue d'ensemble affiche le plan actuel du tenant, les licences achetées et les utilisateurs dont l'accès repose actuellement sur une licence consommée.
 - PLAN ACTUEL:** Unavailable. Le plan et le total des licences achetées sont synchronisés depuis l'abonnement Microsoft Marketplace actif lorsque l'accès fulfillment est configuré.
 - UTILISATION DES LICENCES:** 0 / 0. Aucun utilisateur supplémentaire du tenant ne peut se connecter tant qu'un administrateur n'a pas retiré un utilisateur licencié.
 - Règle de connexion:** À chaque accès authentifié, l'application vérifie si cet utilisateur possède déjà une licence. Sinon, une licence disponible est consommée automatiquement, sauf si l'utilisateur a été retiré explicitement et doit être réattribué.
 - Fenêtre de retrait utilisateur:** Retraits d'utilisateurs restants sur les prochaines 24 heures : 0.
- Utilisateurs licenciés déjà connectés:** À chaque accès authentifié, l'application vérifie si l'utilisateur possède déjà une licence. Les utilisateurs retirés restent bloqués jusqu'à ce qu'un administrateur les réattribue, et les nouveaux utilisateurs sont bloqués lorsque toutes les licences achetées sont déjà consommées.
- Activité administrative récente:** L'historique d'activité et de validation reste consultable en mode modifiable comme en lecture seule.

Objectif

Cette page explique les opérations administrateur liées au plan Marketplace, aux licences utilisateur, au changement de plan, au rattachement de données existantes et aux mises à jour applicatives.

Pour une simple mise à jour in-place des images applicatives, utilisez **Deployment & Updates** lorsque la surface est disponible. Pour un changement de plan ou une mise à jour majeure qui doit conserver les données existantes, créez un nouveau déploiement Azure Marketplace et sélectionnez **Attach existing ProPM data resources**.

Pour qui

PROFIL	USAGE DE CETTE PAGE
Administrateur tenant	Lire les sièges commandés, utilisés et restants
Administrateur Azure	Changer de plan ou rattacher des données existantes

PROFIL	USAGE DE CETTE PAGE
Support	Vérifier un blocage de licence ou update
Utilisateur métier	Non, sauf pour comprendre pourquoi l'accès peut être refusé

Avant de commencer

- Vous avez accès à **Platform Administration**.
- Azure Marketplace reste la source officielle pour l'achat, le prix et la facturation.
- Les utilisateurs à libérer ou réaffecter sont identifiés.
- Pour un rattachement de données existantes, vous connaissez la Managed Application ProPM précédente et son Resource ID complet.

Comprendre les compteurs

COMPTEUR	SIGNIFICATION
Ordered seats	Capacité commandée côté Marketplace
Included seats	Licences incluses dans le plan
Supplemental seats	Licences supplémentaires achetées
Used seats	Utilisateurs actuellement comptabilisés
Remaining seats	Licences encore disponibles

Gérer les utilisateurs licenciés

1. Ouvrez **Platform Administration**.
2. Restez dans **Overview**.
3. Ouvrez **Tenant plan and licensed users**.
4. Consultez la liste des utilisateurs connectés/licenciés.
5. Identifiez un utilisateur à libérer si la politique client le permet.
6. Utilisez **Release user** uniquement si l'utilisateur n'a plus besoin d'accès.
7. Vérifiez que le compteur restant est mis à jour.

Rafraîchir le plan Marketplace

1. Ouvrez **Tenant plan and licensed users**.
2. Sélectionnez **Refresh Marketplace plan**.
3. Attendez la synchronisation.
4. Vérifiez les compteurs affichés.

Refresh Marketplace plan synchronise les informations connues. Il n'achète pas de licences, ne change pas le plan et ne modifie pas la facturation.

Changer de plan ou faire une mise à jour majeure avec données existantes

Utilisez ce flux lorsqu'un nouveau déploiement Marketplace est nécessaire mais que les données ProPM existantes doivent être conservées, par exemple pour un changement commercial de plan ou une mise à jour majeure non applicable in-place. Ce n'est pas une migration manuelle de base de données. Le nouveau tier applicatif se connecte aux ressources de données utilisées par le déploiement ProPM précédent.

Parcours général

1. Ouvrez Azure Marketplace.
2. Sélectionnez le plan ProPM Agent cible.
3. Créez un nouveau déploiement ProPM Agent.
4. Dans **Application Settings**, sélectionnez **Attach existing ProPM data resources**.
5. Renseignez le Resource ID de la Managed Application ProPM précédente.
6. Laissez les overrides optionnels vides sauf demande support ou architecture particulière.
7. Configurez le cutover, l'administration, le CORS, la supervision, le mot de passe et le réseau.
8. Sélectionnez **Review + create**.
9. Validez la nouvelle instance avant de supprimer ou désactiver l'ancienne.

Écran de mise à jour 1 - Rattacher les données existantes

Cette partie de **Application Settings** identifie le déploiement précédent et les ressources de données existantes à réutiliser.

Home > ProPM Agent

Create ProPM Agent ...

Environment Name * ⓘ

Installation mode ⓘ

Attach mode creates a new Marketplace Managed Application and application tier for the selected plan, but connects it to the resources used by an existing ProPM deployment. Enter the previous Managed Application resource ID so ProPM can read its recorded deployment outputs and discover the actual data resources, including when the previous deployment is also an attach deployment. Keep the previous deployment stopped or read-only during cutover to avoid two app tiers writing to the same data.

Previous ProPM Managed Application resource ID * ⓘ

Advanced overrides: leave the resource IDs below empty to auto-discover the ProPM resources from the previous deployment outputs. Fill a field only if the previous deployment outputs are unavailable or the data resources are externally managed.

Existing Storage account resource ID (optional override) ⓘ

Existing Azure AI Search service resource ID (optional override) ⓘ

Existing SQL server resource ID (optional override) ⓘ

Existing SQL database name (optional override) ⓘ

Existing Cosmos DB account resource ID (optional override) ⓘ

Existing Document Intelligence account resource ID (optional override) ⓘ

Existing Service Bus namespace resource ID (optional override) ⓘ

Champs de rattachement des données existantes

CHAMP	OBLIGATOIRE	QUE RENSEIGNER	RECOMMANDATIONS
Environment Name	Oui	Nom court de l'environnement, par exemple <code>prod</code> , <code>uat</code> ou <code>test</code> .	Utilisez une valeur stable, non confidentielle, qui identifie le nouveau tier applicatif. Gardez la convention de nommage interne.

CHAMP	OBLIGATOIRE	QUE RENSEIGNER	RECOMMANDATIONS
Installation mode	Oui	Attach existing ProPM data resources.	Ce mode crée une nouvelle Managed Application Marketplace et un nouveau tier applicatif, puis les connecte aux données ProPM existantes. Utilisez New installation uniquement pour un environnement vide.
Previous ProPM Managed Application resource ID	Oui	Resource ID Azure complet de la Managed Application ProPM précédente.	Copiez le champ Id complet depuis la page Properties de l'ancienne Managed Application. Ne renseignez pas seulement le nom de l'application, le groupe de ressources ou le managed resource group.
Existing Storage account resource ID (optional override)	Non	Resource ID du compte de stockage existant, uniquement si l'auto-découverte ne peut pas être utilisée.	Laissez vide dans le cas standard. Renseignez seulement si les outputs du déploiement précédent sont indisponibles, si les ressources sont gérées hors standard ou si le support ProPM le demande.
Existing Azure AI Search service resource ID (optional override)	Non	Resource ID du service Azure AI Search existant.	Laissez vide sauf si la découverte standard ne peut pas identifier le service de recherche.
Existing SQL server resource ID (optional override)	Non	Resource ID du serveur SQL existant.	Utilisez seulement pour une topologie SQL personnalisée ou gérée hors standard. Ce champ identifie le serveur SQL, pas le nom de la base.
Existing SQL database name (optional override)	Non	Nom de la base SQL existante.	Utilisez avec prudence, uniquement si le nom de base ne peut pas être découvert depuis le déploiement précédent.
Existing Cosmos DB account resource ID (optional override)	Non	Resource ID du compte Cosmos DB existant.	Laissez vide sauf besoin explicite de pointer vers un compte Cosmos DB existant précis.
Existing Document Intelligence account resource ID (optional override)	Non	Resource ID du compte Document Intelligence existant.	Utilisez seulement si le déploiement précédent utilise une ressource Document Intelligence externe ou personnalisée.

CHAMP	OBLIGATOIRE	QUE RENSEIGNER	RECOMMANDATIONS
Existing Service Bus namespace resource ID (optional override)	Non	Ressource ID du namespace Service Bus existant.	Laissez vide dans le cas standard pour réutiliser le namespace découvert.
Previous	Non	Retourne à l'étape précédente du formulaire.	Ne lance aucun déploiement.
Next	Non	Passer à l'étape suivante du formulaire.	Utilisez-le après avoir rempli les champs requis.
Review + create	Non	Lance la validation Azure avant création.	Utilisez-le seulement après avoir complété les paramètres suivants.

Écran de mise à jour 2 - Cutover et paramètres plateforme

Cette partie contrôle la sécurité du cutover, l'administration plateforme, la reprise du fournisseur IA, le CORS, la supervision, la confirmation du mot de passe SQL et le réseau.

☰
Microsoft Azure
🔍 Search resources, services, and docs (G+)

Home > ProPM Agent

Create ProPM Agent ⋮

Existing Event Grid topic resource ID (optional override) ⓘ

Block previous deployment during cutover ⓘ

Platform Administration Entra Group Object IDs * ⓘ

Platform Administration Bootstrap Users (optional) ⓘ

Allow Azure RBAC admin recovery ⓘ

Reuse previous AI provider configuration ⓘ

AI provider fields are hidden for this update. ProPM will reuse the previous deployment's AI provider metadata and the existing Platform Administration configuration stored with your attached data. You can change AI settings after deployment from Platform Administration.

CORS Allowed Origins ⓘ

Enable alerting (Azure Monitor) ⓘ

Enable debug logging ⓘ

One secure SQL input is still required for attach updates: enter the existing ProPM SQL admin password so the new application tier can connect to the reused database. This password is not exposed by ARM outputs and cannot be read from the previous Managed Application because the managed resource group is protected by Azure deny assignments.

Password * ⓘ

Confirm password * ⓘ

VNet CIDR * ⓘ

Previous
Next
Review + create

Champs cutover et plateforme

CHAMP	OBLIGATOIRE	QUE RENSEIGNER	RECOMMANDATIONS
Existing Event Grid topic resource ID (optional override)	Non	Resource ID du topic Event Grid existant.	Laissez vide sauf si l'auto-découverte ne trouve pas le topic ou si le support demande de le renseigner.

CHAMP	OBLIGATOIRE	QUE RENSEIGNER	RECOMMANDATIONS
Block previous deployment during cutover	Non, recommandé pour le cutover	Cochez la case pour empêcher les changements dans l'ancien déploiement pendant la validation.	Cette option évite que deux tiers applicatifs écrivent dans les mêmes données. Sinon, gardez l'ancien déploiement arrêté ou en lecture seule par une autre méthode contrôlée.
Platform Administration Entra Group Object IDs	Oui	Object IDs des groupes Entra autorisés à administrer la nouvelle instance.	Renseignez les Object IDs des groupes, pas leurs noms d'affichage. Vérifiez que ce sont bien les administrateurs attendus.
Platform Administration Bootstrap Users (optional)	Non	Utilisateurs bootstrap ou de récupération si votre procédure le prévoit.	Gardez une liste minimale. À utiliser seulement pour le premier accès ou une récupération contrôlée.
Allow Azure RBAC admin recovery	Non	Case permettant la récupération administrateur via Azure RBAC.	Laissez activé si votre modèle d'exploitation l'autorise. Désactivez seulement si la gouvernance impose une séparation stricte.
Reuse previous AI provider configuration	Recommandé	Cochez si le nouveau déploiement doit réutiliser la configuration IA précédente.	Quand l'option est active, les champs IA sont masqués pour cette mise à jour. Vous pourrez changer les paramètres IA plus tard depuis Platform Administration .
CORS Allowed Origins	Selon le scénario	Origines web additionnelles, par exemple https://portal.contoso.com .	Laissez vide si aucune origine additionnelle n'est nécessaire. Évitez les jokers trop larges.
Enable alerting (Azure Monitor)	Non	Active ou désactive les alertes Azure Monitor.	Recommandé en production. Vérifiez les destinataires et règles d'action après déploiement.
Enable debug logging	Non	Active des journaux plus détaillés.	Gardez désactivé sauf diagnostic encadré, car cela peut augmenter le volume de logs et exposer plus de détails techniques aux administrateurs.

CHAMP	OBLIGATOIRE	QUE RENSEIGNER	RECOMMANDATIONS
Password	Oui	Mot de passe administrateur SQL ProPM existant.	Les mises à jour attachées exigent encore cette saisie sécurisée pour que le nouveau tier applicatif se connecte à la base réutilisée. Utilisez vos procédures approuvées de gestion des secrets.
Confirm password	Oui	Même valeur que Password .	Azure vérifie que les deux valeurs correspondent. En cas d'erreur, ressaisissez les deux champs depuis la source sécurisée.
VNet CIDR	Oui	Plage réseau privée du nouveau déploiement, par exemple <code>10.0.0.0/16</code> .	Faites valider par l'équipe réseau. Évitez tout chevauchement avec réseaux existants, peerings, VPN ou plages prévues.

Avant Review + create

CONTRÔLE	RÉSULTAT ATTENDU
Previous Managed Application ID	Resource ID Azure complet de l'ancienne Managed Application ProPM
Overrides	Vides sauf impossibilité de découverte ou demande support
Ancien déploiement	Bloqué, arrêté ou en lecture seule pendant le cutover
Groupes admin	Object IDs Entra corrects pour la nouvelle instance
Reprise fournisseur IA	Activée si la configuration précédente doit être reprise
Mot de passe SQL	Mot de passe administrateur SQL ProPM saisi via une gestion sécurisée
VNet CIDR	Validé et sans chevauchement
Review + create	Validation Azure réussie avant lancement de création

Après le nouveau déploiement

1. Attendez la fin du provisionnement Azure.
2. Ouvrez la nouvelle URL ProPM Agent.

3. Vérifiez la connexion administrateur.
4. Vérifiez utilisateurs, projets, documents, connaissance, rapports, agents et intégrations.
5. Vérifiez la configuration du fournisseur IA et lancez un test si nécessaire.
6. Vérifiez le plan Marketplace et les compteurs de licences.
7. Basculez les utilisateurs vers le nouveau déploiement seulement après validation.
8. Conservez temporairement l'ancien déploiement si votre plan de cutover le prévoit.
9. Ne supprimez pas les ressources de données réutilisées tant que le nouveau déploiement en dépend.

Vérifier les mises à jour applicatives

Utilisez **Deployment & Updates** pour vérifier et appliquer les mises à jour in-place des images applicatives lorsque la surface est disponible. Lancez ces updates pendant une fenêtre maîtrisée et conservez les informations de support si un rollback est nécessaire.

N'utilisez pas **Deployment & Updates** pour les changements commerciaux de plan, les nouveaux achats Marketplace, les mises à jour majeures exigeant une nouvelle Managed Application ou les cutovers vers des données existantes.

Si cela ne fonctionne pas

SYMPTÔME	CAUSE PROBABLE	ACTION RECOMMANDÉE
Compteurs inchangés après refresh	Marketplace non encore synchronisé ou aucun changement acheté	Vérifiez Azure Marketplace puis relancez plus tard
Utilisateur bloqué malgré licence	Rôle projet ou accès Entra manquant	Vérifiez Entra et Contrôle d'accès
Release user indisponible	Droit administrateur insuffisant	Demandez l'action au tenant admin
Update bloquée	Fenêtre, santé ou prérequis non satisfaits	Ouvrez Support, audit et diagnostic
Nouveau déploiement attaché invalide	Ressource ID précédent erroné, override incorrect ou mot de passe SQL invalide	Corrigez les champs Azure Marketplace avant création ou contactez le support

Suite

- Pour déployer, ouvrez [Administration Azure et Entra](#).
- Pour vérifier le fournisseur IA après changement, ouvrez [Fournisseur IA](#).
- Pour les incidents, ouvrez [Support, audit et diagnostic](#).

Fournisseurs IA et intégrations plateforme

Accueil · Fournisseurs IA et intégrations plateforme

ProPM Agent
Cockpit de livraison IA

PROJET ACTUEL
Azure Bay Hotel & Convention Center
Ouvrir l'espace de travail

Tableau de bord
Projets
Espace de travail
Connaissance
Agents
Rapports & artefacts
Journal IA
Centre de commande portefeuille
Administration de la plateforme

Utilisateur
mock.user@contoso.c...

Vue d'ensemble | Intégrations de la plateforme | Paramètres du fournisseur IA | Audit & activité

Connecteurs d'exécution
0
0 actifs • 0 dégradés / invalides

Fournisseurs d'ingestion
0
0 actifs • 0 dégradés / invalides

Fournisseur IA effectif
Unavailable
Sélectionné par le déploiement : Unavailable

Plan d'abonnement
Unavailable
0 utilisés • 0 disponibles

Règles de fonctionnement de l'administration
L'interface applique les règles backend de lecture seule ou modifiable issues de allowed_actions et read_only_reason.

- Les intégrations de la plateforme restent réparties entre connecteurs d'exécution et fournisseurs d'ingestion.
- Les valeurs sensibles restent masquées ; seuls des champs API sans risque pour les métadonnées sont affichés.
- Les fournisseurs IA sélectionnés par le déploiement et effectifs sont affichés séparément.
- L'état de l'abonnement et des droits est rendu à partir de SubscriptionAdministrationView.

Plan du tenant et utilisateurs licenciés
La vue d'ensemble affiche le plan actuel du tenant. Les licences achetées et les utilisateurs dont l'accès repose actuellement sur une licence consommée.

PLAN ACTUEL
Unavailable
Le plan et le total des licences achetées sont synchronisés depuis l'abonnement Microsoft Marketplace actif lorsque l'accès fulfillment est configuré.

UTILISATION DES LICENCES
0 / 0
Aucun utilisateur supplémentaire du tenant ne peut se connecter tant qu'un administrateur n'a pas retiré un utilisateur licencié.

Règle de connexion
À chaque accès authentifié, l'application vérifie si cet utilisateur possède déjà une licence. Sinon, une licence disponible est consommée automatiquement, sauf si l'utilisateur a été retiré explicitement et doit être réattribué.

Fenêtre de retrait utilisateur
Retraits d'utilisateurs restants sur les prochaines 24 heures : 0.

Utilisateurs licenciés déjà connectés
À chaque accès authentifié, l'application vérifie si l'utilisateur possède déjà une licence. Les utilisateurs retirés restent bloqués jusqu'à ce qu'un administrateur les réattribue, et les nouveaux utilisateurs sont bloqués lorsque toutes les licences achetées sont déjà consommées.

Activité administrative récente
L'historique d'activité et de validation reste consultable en mode modifiable comme en lecture seule.

Cette page a été scindée

La préparation technique de la plateforme est maintenant documentée dans deux pages dédiées pour éviter de mélanger fournisseur IA, connecteurs et usage projet.

Où aller maintenant

BESOIN	PAGE RECOMMANDÉE
Configurer Save / Validate / Test / Activate du fournisseur IA	Fournisseur IA
Vérifier le fournisseur IA réellement utilisé	Journal IA
Définir et valider des connecteurs ou fournisseurs d'ingestion	Intégrations plateforme
Comprendre l'usage métier des connecteurs	Connecteurs et intégrations
Diagnostiquer un blocage	Support, audit et diagnostic

Règle à retenir

La plateforme décide ce qui est techniquement disponible. Le projet décide ce qui est rattaché. La gouvernance décide qui peut agir. Le Journal IA prouve le fournisseur réellement utilisé par un run.

Plan du tenant, utilisateurs licenciés et mises à jour applicatives

Accueil · Plan du tenant, utilisateurs licenciés et mises à jour applicatives

The screenshot displays the ProPM Agent administration dashboard for the 'Azure Bay Hotel & Convention Center' project. The interface is divided into several sections:

- Navigation:** A sidebar on the left contains menu items like 'Tableau de bord', 'Projets', 'Espace de travail', 'Connaissance', 'Agents', 'Rapports & artefacts', 'Journal IA', 'Centre de commande portefeuille', and 'Administration de la plateforme' (highlighted).
- Summary Cards:** At the top right, four cards provide key metrics:
 - Connecteurs d'exécution:** 0 actifs, 0 dégradés / invalides.
 - Fournisseurs d'ingestion:** 0 actifs, 0 dégradés / invalides.
 - Fournisseur IA effectif:** Unavailable (Selected by deployment: Unavailable).
 - Plan d'abonnement:** Unavailable (0 utilisés, 0 disponibles).
- Règles de fonctionnement de l'administration:** A section detailing backend rules for API actions and permissions.
- Plan du tenant et utilisateurs licenciés:** A central section explaining the current plan status (Unavailable) and license usage (0/0). It includes sub-sections for 'PLAN ACTUEL' and 'Règle de connexion'.
- Utilisateurs licenciés déjà connectés:** A section describing the state of licensed users and their connection status.
- Activité administrative récente:** A section for viewing recent administrative activity and validation history.

Cette page a été scindée

Le contenu sur le plan tenant, les utilisateurs licenciés et les mises à jour est maintenant centralisé dans [Licences, plans et mises à jour](#).

Où aller maintenant

BESOIN	PAGE RECOMMANDÉE
Comprendre ordered, included, supplemental, used et remaining seats	Licences, plans et mises à jour
Libérer un utilisateur licencié	Licences, plans et mises à jour
Rafraîchir le plan Marketplace	Licences, plans et mises à jour
Changer de plan ou rattacher des données existantes	Licences, plans et mises à jour

BESOIN	PAGE RECOMMANDÉE
Vérifier les mises à jour applicatives	Licences, plans et mises à jour

Règles importantes

- Azure Marketplace reste la source officielle pour le plan, le prix et la facturation.
- **Refresh Marketplace plan** synchronise les informations connues mais n'achète rien.
- Les détails d'infrastructure relèvent de l'administration avancée ou du support, pas du guide utilisateur final.

Sécurité et conformité

[Accueil](#) · Sécurité et conformité

Objectif

Cette page explique les principes de sécurité et conformité à connaître comme utilisateur, Project Owner, administrateur tenant ou support client.

Pour qui

PROFIL	USAGE DE CETTE PAGE
Utilisateur métier	Comprendre les bonnes pratiques de partage, preuves et IA
Project Owner	Encadrer accès, rôles, gouvernance et publications
Administrateur tenant	Vérifier identité, licences, fournisseur IA et intégrations
Support ou auditeur	Collecter les traces utiles sans exposer d'informations sensibles

Identité et accès

- La connexion s'appuie sur Microsoft Entra ID dans les environnements Azure.
- L'accès à un projet dépend de l'appartenance au projet et du rôle attribué.
- Un utilisateur peut être connecté à l'application sans voir de projet si aucun accès projet ne lui a été accordé.
- Les rôles projet contrôlent les actions : lecture, agents, Documents PM, membres, gouvernance, actions et audit.

Isolation tenant et projet

- Le tenant définit le périmètre organisationnel.
- Le projet actif limite les documents, runs, signaux, actions et Documents PM affichés.
- **All projects** ne contourne pas les droits : il reste limité aux projets déjà accessibles par le même compte.
- Portfolio compare uniquement les projets accessibles par l'utilisateur.

Données et confidentialité

- Ne téléversez que les documents autorisés pour le projet.
- Masquez les données sensibles dans les captures support.
- Ne copiez jamais de secret, clé, jeton ou mot de passe dans une note, un prompt, une action ou un ticket.
- Vérifiez la destination avant **Publish** ou toute action externe.

Traçabilité et audit

ÉLÉMENT	OÙ LE VÉRIFIER	USAGE
Run	Journal IA	Retrouver une exécution IA
Fournisseur IA effectif	Journal IA	Confirmer le fournisseur réellement utilisé
Document PM	Documents PM et artefacts	Relire version, diff, lignée et actions aval
Action gouvernée	Actions et approbations	Voir proposition, approbation et exécution
Trace ID	Support, audit et diagnostic	Corréler un incident avec le support

Usage responsable de l'IA

- Relisez toujours les sorties IA avant décision ou publication.
- Vérifiez preuves, fraîcheur, contradictions et informations manquantes.
- Ne traitez pas la confiance comme une approbation automatique.
- Utilisez les Documents PM pour les livrables qui doivent être versionnés, approuvés ou publiés.
- Escaladez les contradictions importantes au Project Owner ou au PMO.

Connecteurs et actions externes

Une action externe réelle exige généralement : intégration plateforme validée, rattachement projet, politique compatible, rôle suffisant, santé correcte et mode live actif si applicable. Une action visible dans l'interface ne garantit pas qu'un ticket, message ou fichier externe sera créé.

Checklist avant publication ou diffusion externe

1. Le projet actif est correct.
2. Les preuves sont identifiables et assez fraîches.
3. Les contradictions sont arbitrées.
4. Le Document PM est relu et versionné.
5. La politique autorise l'action ou l'approbation est obtenue.
6. La destination externe est correcte.
7. Les informations sensibles non nécessaires sont retirées.

Suite

- [Sorties structurées, preuves et fraîcheur](#)
- [Documents PM et artefacts](#)
- [Actions et approbations](#)
- [Support, audit et diagnostic](#)

Limitations connues

[Accueil](#) · Limitations connues

Objectif

Cette page clarifie les limites connues afin d'éviter les attentes incorrectes et les escalades inutiles.

Limites d'usage utilisateur

SUJET	LIMITATION	CONTOURNEMENT OU BONNE PRATIQUE
Historique de chat	Peut être local au navigateur	Utiliser Documents PM, artefacts et Journal IA pour la trace partagée
Projet actif	Les pages projet changent selon le projet sélectionné	Vérifier la barre supérieure avant chaque action
All projects	Ne donne pas accès à tous les projets du tenant	Vérifier les accès projet réels
Réponse d'agent	N'est pas automatiquement un livrable final	Relire puis passer par Documents PM si nécessaire
Confiance IA	N'est pas une approbation	Vérifier preuves, fraîcheur et contradictions
Source unavailable	N'est pas une preuve exploitable	Réouvrir la source ou demander un réimport

Limites d'intégrations

SUJET	LIMITATION	BONNE PRATIQUE
Connecteur visible	Peut ne pas être utilisable	Vérifier plateforme, projet, politique, rôle, santé
Action approved	Peut ne pas être exécuté	Vérifier l'exécution dans Actions et Journal IA
Mode live	Requis pour créer des objets externes réels	Demander confirmation à l'administrateur
Import	Peut finir avant indexation complète	Attendre le statut Indexed

SUJET	LIMITATION	BONNE PRATIQUE
Publication	Dépend d'une destination validée	Vérifier le rattachement et la politique

Limites administration Azure

SUJET	LIMITATION	BONNE PRATIQUE
Fournisseur sélectionné au déploiement	Ne prouve pas le fournisseur utilisé par un run	Vérifier le fournisseur effectif dans Journal IA
Refresh Marketplace plan	Synchronise mais n'achète rien	Acheter ou changer le plan dans Azure Marketplace
Changement de plan	Peut nécessiter un nouveau déploiement avec données existantes	Suivre Licences, plans et mises à jour
Pages admin	Peuvent être visibles en lecture seule	Vérifier rôle administrateur tenant

Limites Portfolio

- Un outlier n'est pas un verdict automatique.
- Un signal indisponible indique un manque de preuve, pas une absence de risque.
- Les seuils et poids doivent être adaptés à la revue PMO.
- Un snapshot ancien doit être recalculé avec **Refresh comparison**.

Suite

- [Support, audit et diagnostic](#)
- [Portfolio](#)
- [Fournisseur IA](#)

Maintenance, support et FAQ

Accueil · Maintenance, support et FAQ

ProPM Agent
Cockpit de livraison IA

PROJET ACTUEL
Azure Bay Hotel & Convention Center
Ouvrir l'espace de travail

Tableau de bord
Projets
Espace de travail
Connaissance
Agents
Rapports & artefacts
Journal IA
Centre de commande portefeuille
Administration de la plateforme

Utilisateur
mock.user@contoso.c...

Azure Bay Hotel & Convention Cent ⓘ

Appuyez sur Ctrl+K / ⌘K pour les commandes

Océan

Français

Aide

Santé

Journal IA Actualiser

Runs et chronologie d'activité pour ce projet.

AIDE Aide

Aperçu du journal IA
AI Log fournit une piste d'audit pour les exécutions, les événements d'activité, les artefacts, la fraîcheur et la transparence fournisseur.

Aperçu du journal IA Filtres d'exécution Audit des événements Identifiants de run

Runs Activité

Rechercher agent/statut/id de run... Tous les agents Tous les statuts

3 affichés

Créé	Agent	Statut	Coût	ID d'exécution	Actions
2026-04-21 08:50:50	Schedule	Terminé	884 jetons • 3 appels	run-003	Détails
2026-04-21 07:50:50	Risk	Terminé	917 jetons • 3 appels	run-002	Détails
2026-04-21 06:50:50	Orchestrator	Terminé	1432 jetons • 5 appels	run-001	Détails

Objectif

Cette FAQ aide à reconnaître les symptômes courants et à ouvrir la bonne page sans exposer de détails internes ou sensibles.

Pour qui

PROFIL	USAGE DE CETTE PAGE
Utilisateur métier	Comprendre quoi vérifier avant de demander de l'aide
Project Owner	Distinguer rôle, projet, politique et intégration
Administrateur tenant	Identifier quand passer aux pages admin
Support	Collecter les informations utiles à l'investigation

Avant de commencer

- Vérifiez le projet actif.
- Notez l'heure approximative du problème.
- Conservez le message affiché et une capture masquée si nécessaire.
- Ne partagez jamais de secret, clé, jeton ou payload sensible.

Coordonnées NovaBiz

Pour joindre le support NovaBiz :

- Email : support@navabiz.pro
- Adresse : NovaBiz, 131 Continental Dr, Suite 305, Newark, DE 19713, United States

Symptôme vers première action

SYMPTÔME	PREMIÈRE ACTION	PAGE UTILE
Connexion impossible	Vérifier compte, tenant, consentement et URL	Démarrage
Aucun projet visible	Vérifier appartenance au projet et rôle	Projet actif
Page vide	Vérifier projet actif, filtre et rôle	Interface et navigation
Document non indexé	Vérifier statut Indexed , Ingesting ou Failed	Connaissance
Agent sans réponse	Vérifier si un run existe dans le Journal IA	Journal IA
Réponse incomplète	Vérifier preuves, fraîcheur et informations manquantes	Sorties structurées
Fournisseur IA non opérationnel	Vérifier fournisseur effectif et page admin IA	Fournisseur IA
Connecteur bloqué	Vérifier plateforme, projet, politique, santé	Connecteurs
Action en attente	Vérifier approbation, politique et exécution	Actions et approbations
Licence indisponible	Vérifier seats restants et utilisateur licencié	Licences, plans et mises à jour

FAQ accès et projet

La connexion Microsoft réussit mais aucun projet n'apparaît

Le compte est authentifié mais n'est probablement pas encore membre d'un projet, ou le projet actif n'est pas sélectionné. Demandez au Project Owner de vérifier votre présence dans [Contrôle d'accès et rôles](#).

Une page est visible mais tous les boutons sont grisés

Vous êtes probablement en lecture seule. Ce n'est pas une panne : le rôle permet de consulter mais pas de modifier. Vérifiez le rôle attendu avec le Project Owner.

Le projet actif change-t-il les résultats ?

Oui. Connaissance, Agents, Documents PM, Signaux et Journal IA dépendent du projet actif. Vérifiez-le dans la barre supérieure avant toute enquête.

FAQ connaissance et agents

Un document est visible mais pas retrouvable dans la recherche

Il peut encore être en traitement. Attendez le statut **Indexed** avant de l'utiliser comme preuve. Si le statut passe **Failed**, consultez [Connaissance, documents et imports](#).

Un agent répond sans preuve visible

Traitez la réponse comme exploratoire. Avant diffusion ou décision, vérifiez les preuves, la fraîcheur et les informations manquantes dans [Sorties structurées, preuves et fraîcheur](#).

L'historique de chat a disparu

La continuité de chat peut être locale au navigateur. Elle n'est pas une archive centrale partagée. Les Documents PM, artefacts, actions et runs tracés restent côté plateforme selon vos droits.

FAQ Documents PM et actions

Quelle différence entre Download, Publish et Add to knowledge ?

ACTION	EFFET
Download	Télécharge une copie locale
Publish	Publie vers une destination gouvernée
Add to knowledge	Réinjecte un document relu dans la connaissance projet

Une action est approved mais rien ne s'est passé

approved signifie que l'action est autorisée. **executed** signifie que l'action a réellement été lancée. Vérifiez l'état dans [Actions et approbations](#).

Un connecteur est visible mais inutilisable

Un connecteur doit être défini côté plateforme, rattaché au projet, autorisé par la politique, sain, et utilisable par votre rôle. Consultez [Connecteurs et intégrations](#).

FAQ Portfolio

Aucun outlier n'apparaît

Cela peut signifier que le seuil global est élevé, que la sélection est trop restrictive, que les preuves manquent ou que la situation est réellement stable. Ouvrez [Portfolio](#) et vérifiez le snapshot, les projets sélectionnés et le profil de signaux.

Un signal est indisponible

Indisponible ne veut pas dire sans risque. Cela signale souvent un manque de preuve ou de données exploitables.

Support et audit avancé

Pour une enquête, fournissez uniquement les informations utiles : URL, projet actif, heure, action tentée, message affiché, Run ID, Trace ID ou Action ID si visibles. Les

identifiants comme [Trace ID](#), [Context snapshot ID](#) ou [Structured output ID](#) sont des repères de support, pas des informations nécessaires à tous les utilisateurs. Pour le détail, ouvrez [Support, audit et diagnostic](#).

Suite

- [Support, audit et diagnostic](#)
- [Journal IA](#)
- [Glossaire](#)

Support, audit et diagnostic

[Accueil](#) · Support, audit et diagnostic

Objectif

Cette page centralise les informations à collecter lorsqu'un utilisateur rencontre un problème : accès, projet, connaissance, agents, fournisseur IA, connecteurs, actions, licences ou mise à jour.

Pour qui

PROFIL	USAGE DE CETTE PAGE
Utilisateur métier	Savoir quoi transmettre au support
Project Owner	Vérifier rôle, projet, politique et intégrations
Administrateur	Ajouter les contrôles fournisseur, licences ou plateforme
Support ou auditeur	Reconstituer le contexte sans demander de secret

Avant de commencer

- Reproduisez le problème si possible.
- Notez l'heure approximative et le fuseau horaire.
- Vérifiez le projet actif.
- Préparez une capture sans données sensibles.

Coordonnées NovaBiz

Pour joindre le support NovaBiz :

- Email : support@navabiz.pro
- Adresse : NovaBiz, 131 Continental Dr, Suite 305, Newark, DE 19713, United States

Checklist à transmettre

INFORMATION	EXEMPLE UTILE
URL de la page	Page visible au moment de l'erreur
Projet actif	Nom du projet concerné
Utilisateur concerné	Compte ou groupe, sans mot de passe
Heure	Date, heure et fuseau horaire
Action tentée	Téléverser, lancer un agent, publier, approuver
Message affiché	Texte exact ou capture masquée
Identifiants visibles	Run ID, Trace ID, Artifact ID, Action ID si présents

Ne jamais transmettre

- Mot de passe, secret, clé API ou jeton.
- Payload complet contenant des données client sensibles.
- Capture contenant des documents confidentiels non masqués.
- Configuration d'infrastructure détaillée sans demande explicite du support.

Diagnostic rapide par domaine

SYMPTÔME	PREMIÈRE VÉRIFICATION	PAGE UTILE
Connexion impossible	Tenant, compte Entra, consentement, licence	Démarrage
Aucun projet visible	Projet actif, appartenance, rôle	Projet actif
Document non indexé	Statut Knowledge, format, historique import	Connaissance
Agent sans réponse	Run dans Journal IA, fournisseur effectif	Journal IA
Document PM bloqué	Statut, diff, rôle, gouvernance	Documents PM
Action en attente	Approbation, politique, connecteur, mode live	Actions et approbations

SYMPTÔME	PREMIÈRE VÉRIFICATION	PAGE UTILE
Connecteur bloqué	Plateforme, projet, politique, santé	Intégrations plateforme
Licence refusée	Seats restants, utilisateur licencié	Licences et mises à jour

Utiliser les IDs de support

ID	OÙ LE TROUVER	USAGE
Run ID	Journal IA	Retrouver une exécution d'agent
Trace ID	Message d'erreur ou détail support	Corréler une erreur technique
Artifact ID	Document PM ou artefact	Identifier un livrable
Action ID	Actions & approbations	Identifier une action gouvernée
Context snapshot ID	Détail de run si affiché	Comprendre le contexte utilisé

Lire un payload avancé

Certains écrans d'audit peuvent afficher une activité ou un payload technique. Ne le copiez pas intégralement par défaut. Relevez le statut, les IDs, l'heure, le message d'erreur et le fournisseur effectif. Le support demandera un extrait précis si nécessaire.

Résultat attendu

Une demande support complète permet de reproduire ou d'analyser l'incident sans exposer de secrets et sans demander à l'utilisateur métier des détails Azure internes.

Suite

- Pour les runs IA, ouvrez [Journal IA](#).
- Pour les FAQ courantes, ouvrez [Maintenance, support et FAQ](#).
- Pour clarifier un terme, ouvrez [Glossaire](#).

Glossaire

[Accueil](#) · [Glossaire](#)

Convention de libellés

Le glossaire utilise le terme français principal, puis le libellé exact de l'interface lorsqu'il évite une ambiguïté. Exemple : **Ajouter à la connaissance** ([Add to knowledge](#)) ou **Fournisseur IA effectif** ([Effective AI Provider](#)). Les termes marqués **support/admin** ne sont pas nécessaires au parcours utilisateur quotidien.

A

Action gouvernée

Action préparée dans ProPM Agent puis soumise à rôle, politique, approbation ou connecteur avant exécution.

Add to knowledge / Ajouter à la connaissance

Action qui réinjecte un Document PM relu dans la connaissance du projet pour les recherches et agents futurs.

Agent

Assistant spécialisé qui travaille dans le contexte du projet actif et peut produire une sortie structurée avec preuves.

All projects / Tous les projets

Portée limitée aux projets auxquels le même compte a déjà accès. Ce n'est pas un super-projet.

Approvals / approbations

Étape de validation humaine avant exécution ou diffusion d'une action gouvernée.

Artefact

Objet gouverné issu d'un run ou d'une revue, utilisé pour version, diff, lignée ou Document PM.

C

Centre de commande portefeuille / Portfolio

Surface de comparaison multi-projets. Le terme principal de cette documentation est **Portfolio** ; **Centre de commande portefeuille** désigne la même surface lorsque le libellé UI le montre.

Citation

Référence affichée avec une réponse, un résultat de recherche ou un run pour justifier le contenu.

Cohorte

Configuration sauvegardée de projets, signaux, poids et seuils dans Portfolio.

Confiance

Indice de solidité d'une sortie structurée. Elle doit toujours être lue avec les preuves et la fraîcheur.

Connaissance

Espace projet où les documents sont téléversés, importés, indexés, recherchés et utilisés par les agents.

Context snapshot / capture de contexte

Terme **support/admin**. Capture du contexte utilisé pendant un run, utile pour audit et diagnostic.

D

Diff

Comparaison entre deux versions d'artefact ou de Document PM.

Digest

Synthèse de signaux pouvant servir de base à un brouillon de notification ou à une revue projet.

Document PM / PM Doc

Livrable projet relu, versionné et gouverné, pouvant être téléchargé, publié ou ajouté à la connaissance.

Download / Télécharger

Action qui produit une copie locale d'un document ou artefact.

E

Effective AI Provider / fournisseur IA effectif

Fournisseur réellement utilisé par un run donné. La valeur de référence se lit dans le Journal IA.

Entitlement

Terme **support/admin**. Blocage opérationnel lié à licence, rôle, politique, intégration, santé ou configuration. Ce n'est pas un niveau fonctionnel de plan Marketplace.

Evidence gap / manque de preuve

Signal indiquant que les preuves sont insuffisantes ou indisponibles pour conclure.

F

Fraîcheur

État temporel d'une preuve : `fresh`, `aging`, `stale`, `conflicting` ou `unavailable`.

Fournisseur d'ingestion

Source approuvée qui importe du contenu vers la connaissance projet.

Fournisseur IA sélectionné au déploiement

Intention initiale choisie pendant Azure Marketplace. Elle peut différer du fournisseur IA effectif observé dans un run.

H

Health / santé

État de disponibilité d'un composant, connecteur, fournisseur ou service visible dans l'interface.

J

Journal IA / AI Log

Page qui expose les runs, activités, statuts, fournisseur IA effectif et identifiants utiles à l'audit.

L

Lecture seule

État où une page reste visible mais non modifiable.

Lignée / lineage

Chaîne de traçabilité entre run, sortie structurée, artefact, version, Document PM et preuves.

LLM deployment name

Terme **support/admin**. Nom de déploiement modèle utilisé dans certains paramètres fournisseur IA.

P

Palette de commandes

Accès rapide aux pages et actions, généralement via `Ctrl+K` ou `Cmd+K`.

Pending approval / en attente d'approbation

État d'une action ou version qui attend une validation humaine.

Projet actif

Projet actuellement appliqué aux pages Tableau de bord, Connaissance, Agents, Documents PM, Signaux, Actions et Journal IA.

Publish / Publier

Action qui diffuse un Document PM ou artefact vers une destination gouvernée, par exemple SharePoint.

R

Rattachement projet (**binding)**

Lien qui rend une intégration plateforme réellement utilisable dans un projet donné.

Readiness / préparation

Niveau de préparation d'un projet, d'une intégration ou d'un flux gouverné.

Refresh Marketplace plan

Action admin qui synchronise les informations Marketplace connues par ProPM Agent. Elle n'achète pas de licence et ne change pas de plan.

Run

Exécution enregistrée d'un agent ou d'un traitement IA.

S

Siège / seat

Unité de licence utilisateur dans les déploiements qui limitent l'accès par capacité commandée.

Signal

Élément proactif qui attire l'attention sur un risque, une contradiction, un blocage ou une opportunité.

Source label

Libellé lisible de provenance d'une preuve ou d'un document.

Source system

Système source affiché avec une preuve ou un résultat.

Structured output / sortie structurée

Résultat formaté d'un run pouvant inclure résumé, constats, décisions, preuves, confiance et actions.

T

Tableau de bord

Page de synthèse du projet actif : métriques, activité récente, signaux, actions et raccourcis.

Trace ID

Terme **support/admin**. Identifiant utile pour corrélér un incident, un run ou un événement.

V

Validate / validation

Étape admin qui vérifie la cohérence d'une configuration avant test ou activation.

Version d'artefact

État historisé d'un artefact utilisé pour diff, approbation, publication et lignée.

W

Watchpoint / point de vigilance

Point d'attention signalé dans une sortie structurée, souvent lié à un risque ou une contradiction.

Suite

- [Publics, rôles et périmètres](#)
- [Support, audit et diagnostic](#)
- [Sécurité et conformité](#)

Connaissance et agents

[Accueil](#) · Connaissance et agents

Cette page a été scindée

La documentation **Connaissance et agents** est désormais séparée en procédures plus courtes afin de distinguer l'alimentation documentaire, l'usage des agents, la lecture des preuves et la production de livrables.

Où aller maintenant

BESOIN	PAGE RECOMMANDÉE
Téléverser, importer ou rechercher des documents	Connaissance, documents et imports
Choisir un agent, lancer un run ou créer un agent personnalisé	Agents
Lire les citations, la fraîcheur et la confiance	Sorties structurées, preuves et fraîcheur
Transformer un résultat en livrable gouverné	Documents PM et artefacts
Auditer une exécution ou vérifier le fournisseur IA effectif	Journal IA

Rappel important

Un document indexé peut alimenter les recherches et agents du projet actif. Une réponse d'agent reste une sortie à relire : elle ne devient Document PM que lorsqu'elle passe par le flux de revue et de gouvernance.

Page legacy portefeuille et administration

[Accueil](#) · Page legacy portefeuille et administration

Cette page est conservée pour compatibilité

L'ancienne page **Portefeuille et administration technique** a été remplacée par des pages spécialisées afin de séparer le guide utilisateur, l'administration projet, l'administration Azure et le diagnostic support.

Où aller maintenant

BESOIN	PAGE RECOMMANDÉE
Comparer les projets, cohortes, profils de signaux et outliers	Portfolio
Déployer depuis Azure Marketplace et finaliser Entra	Administration Azure et Entra
Configurer Save / Validate / Test / Activate du fournisseur IA	Fournisseur IA
Définir, valider ou rattacher des connecteurs	Intégrations plateforme
Gérer seats, plan Marketplace, refresh et mises à jour	Licences, plans et mises à jour
Diagnostiquer avec Run ID, Trace ID ou Journal IA	Support, audit et diagnostic

Règle produit sur les plans Marketplace

Les plans Marketplace n'expliquent pas, à eux seuls, qu'une action soit disponible ou bloquée. En cas de blocage, vérifiez plutôt licences restantes, rôle, accès projet, rattachement, politique, santé et fournisseur IA effectif.

Pages liées

- [Publics, rôles et périmètres](#)
- [Journal IA](#)
- [Maintenance, support et FAQ](#)

Rapports, Journal IA et traçabilité

[Accueil](#) · Rapports, Journal IA et traçabilité

Cette page a été scindée

Le contenu **Rapports, Journal IA et traçabilité** est désormais séparé pour clarifier les parcours : revue documentaire d'un côté, audit et diagnostic de l'autre.

Où aller maintenant

BESOIN	PAGE RECOMMANDÉE
Retrouver, relire, télécharger ou publier un Document PM	Documents PM et artefacts
Comprendre le diff, les versions et la lignée	Documents PM et artefacts
Retrouver un run, une activité ou le fournisseur IA effectif	Journal IA
Préparer une demande support avec Run ID ou Trace ID	Support, audit et diagnostic

Rappel important

La traçabilité utile se lit dans deux endroits complémentaires : **Documents PM et artefacts** pour le cycle de vie du livrable, et **Journal IA** pour le détail d'exécution.