LA POLITIQUE « OWNERSHIP »

La politique « Ownership » : qui répond de chaque objet

Ownership vérifie que chaque objet a **au moins le nombre de propriétaires que vous fixez**, des personnes de votre organisation si vous l'exigez. Chaque propriétaire est nommé avec **ce qui le désigne** : l'éditeur, votre étiquette, un rôle de gestion, ou un parent dont il hérite. Les propriétaires confirment, complètent ou corrigent la liste, et leur décision est tracée.

VERSION
1.0 · Novembre 2026

LECTEURS
responsable de la gouvernance des accès, administrateur de workspace, relecteur

DIFFUSION
Confidentiel · Clients REVIEWIT

DANS CETTE FICHE

1 Le problème : un objet dont personne ne répond
2 Une question à part
3 La philosophie : cinq partis pris
4 D'où vient le propriétaire
5 Qui compte comme propriétaire
6 Le réglage de la campagne
7 Ressource par ressource
8 Le verdict
9 Ce que fait le relecteur
10 Ce que la politique ne fait pas
11 Mettre en œuvre une campagne
12 Glossaire

01 Le problème : un objet dont personne ne répond

Un site d'équipe a été créé par une seule personne, qui a changé de service. Un dépôt de code n'est administré que par un compte de déploiement. Un canal de discussion a pour seul responsable un prestataire externe. Une base de données AWS n'a aucune étiquette : son seul « propriétaire » est celui du compte, qui ne la connaît pas.

Rien ne casse. Mais le jour où il faut décider de cet objet (ouvrir un accès, le fermer, l'archiver, répondre à un auditeur), personne n'est là pour le faire. Un seul propriétaire est un point unique de défaillance : son départ suffit à laisser l'objet sans responsable.

02 Une question à part

REVIEWIT pose à chaque politique une seule question, lisible dans un fait vérifiable. Ownership ne redouble aucune des politiques voisines :

POLITIQUE	LA QUESTION	LE FAIT LU	FRONTIÈRE
Ownership	L'objet a-t-il les propriétaires que sa règle exige ?	Les propriétaires, leur nombre, leur nature, leur source	La **règle** de propriété
Orphan	Qui reprend l'objet que personne ne possède plus ?	L'absence de propriétaire, ou son départ	Le **sauvetage** : nommer un nouveau propriétaire. Un objet à un seul propriétaire est en écart pour Ownership sans être orphelin
Membership	Chaque membre doit-il le rester ?	Les appartenances	Une appartenance n'a pas de propriétaire : c'est l'accès d'une personne
Privileged Access	Ce privilège est-il justifié ?	Les rôles élevés	Un administrateur du tenant n'est pas propriétaire de chaque objet : seul un rôle de gestion **sur l'objet** compte
Guests	Chaque invité garde-t-il un motif d'accès ?	Les personnes externes	Un invité **propriétaire** est jugé par Ownership ; son accès en général reste à Guests
Inactivité	L'objet sert-il encore ?	Une date d'activité	Un objet actif peut être mal possédé ; un objet bien possédé peut ne plus servir

Ownership couvre les **ressources** (sites, équipes, canaux, dépôts, bases, machines, dossiers) et les **identités non humaines** : clés, jetons, comptes de service, applications, rôles. Quelqu'un en répond. Une **personne**, elle, n'a pas de propriétaire : son responsable hiérarchique ou son parrain ne la possède pas. Les utilisateurs, invités et rôles d'administration restent à Membership, Guests et Privileged Access.

03 La philosophie : cinq partis pris

01 **Nommer la source, toujours.**

Un propriétaire n'a pas la même valeur selon ce qui le désigne. « Désigné par l'étiquette owner » se vérifie ; « déduit : créateur du canal » se discute. Le verdict dit donc, pour chaque objet, d'où vient la liste. Un propriétaire hérité ou déduit compte, mais il est signalé.

02 **Un inconnu n'est pas un « aucun ».**

Quand la source ne dit rien (un import sans la colonne des propriétaires, une lecture refusée par l'éditeur), l'objet n'est **pas évaluable**. REVIEWIT ne le déclare jamais « sans propriétaire » : ce serait un faux écart. « Aucun propriétaire » n'est écrit que lorsque la source l'affirme.

03 **Un propriétaire est quelqu'un qui peut répondre.**

Une personne de l'organisation compte. Un groupe compte pour un, nommé comme groupe : ses membres ne sont pas dépliés. Un compte de service, un robot ou une application ne comptent pas : ils ne peuvent pas répondre d'une décision. Ils restent nommés, pour que le relecteur les voie.

04 **Le seuil appartient à l'organisation, et la décision au propriétaire.**

Deux propriétaires par défaut, parce qu'un seul est un point unique de défaillance. Vous pouvez exiger de un à cinq propriétaires, et autoriser ou non les invités. REVIEWIT constate ; les propriétaires confirment ou corrigent.

05 **Un constat, jamais un score.**

Le verdict dit un compte et une liste : « 1 propriétaire valide sur 2 exigés, désigné ». Il ne dit jamais « orphelin », « à risque » ou « non gouverné », et ne suggère aucune action. Ownership n'ajoute aucune donnée sur les personnes : les noms des propriétaires sont déjà collectés et déjà montrés aux relecteurs.

04 D'où vient le propriétaire

C'est la question la plus fréquente : *qui REVIEWIT appelle-t-il « propriétaire », et sur quelle foi ?* Chaque objet porte la source de sa liste, écrite par la collecte ou par l'import, objet par objet.

SOURCE	CE QUE C'EST	EXEMPLES
Désigné	L'éditeur ou votre organisation **désigne** le propriétaire	Propriétaires d'un groupe Microsoft 365 ou Entra ID ; étiquette « owner » sur une ressource Azure ou AWS ; responsable d'une liste de distribution Exchange ; lead d'un projet Jira ; propriétaire d'un projet Asana ; titulaire d'un jeton
Rôle de gestion	Un rôle de **gestion sur l'objet**	Administrateur de collection de sites ; rôle Owner Azure sur la ressource ; administrateur d'un dépôt GitHub ; gestionnaire d'un drive partagé ou d'un espace Chat ; Channel Manager Slack ; mainteneur d'équipe GitHub ; administrateur d'équipe Asana
Hérité	Le propriétaire d'un **parent**	Étiquette du groupe de ressources ou de la souscription ; rôle Owner sur un parent ; propriétaire du compte AWS ; équipe d'un canal standard ; application d'un secret ; dépôt d'un environnement GitHub
Déduit	Une personne **liée à l'objet** sans le posséder	Créateur d'un canal ; détenteur de l'accès complet d'une boîte partagée ; installateur d'une application ; auteur
Aucun	La source affirme que l'objet n'a personne	Un groupe sans propriétaire, un espace sans gestionnaire

Quand un objet a plusieurs sources possibles, la plus forte l'emporte. Une ressource Azure étiquetée « owner » est **désignée**. Sans étiquette, son rôle Owner donne le propriétaire (**rôle de gestion**), et s'il n'est posé que sur le groupe de ressources, le propriétaire est **hérité**.

05 Qui compte comme propriétaire

IDENTITÉ	COMPTE	CE QUE MONTRE LE VERDICT
Personne de l'organisation	1	Son nom
Groupe	1	Le nom du groupe ; ses membres ne sont pas dépliés
Compte de service, robot, application	0	Nommé, non compté
Invité, personne externe	1 si vous autorisez les invités ; sinon écart « invité propriétaire »	Nommé comme invité
Identité que l'éditeur ne permet pas de résoudre	0	L'identifiant tel que l'éditeur le rend, non compté

L'invité se reconnaît sur l'**identité** elle-même (domaine externe, compte invité de l'éditeur), et non sur la liste des invités de l'objet. Un propriétaire parti, que la collecte ne résout plus, est montré « non résolu » et ne compte pas : le rendre au bon propriétaire est le travail d'Orphan.

06 Le réglage de la campagne

RÉGLAGE	SENS
Nombre minimum de propriétaires	De 1 à 5, **2 par défaut**. Un objet qui a moins de propriétaires valides est en écart
Rôles qui comptent	Sur une ressource qui a à la fois des propriétaires et des administrateurs (un site SharePoint, un Drive), vous choisissez lesquels comptent : les deux, les propriétaires seuls ou les administrateurs seuls. Ailleurs, le choix n'existe pas
Invités autorisés comme propriétaires	Décoché par défaut : un invité propriétaire est alors un écart, même si le nombre est atteint

07 Ressource par ressource

Ownership s'offre aujourd'hui sur **180 ressources de douze solutions**. Chacune porte une liste de propriétaires et sa source. L'assistant ne propose pas Ownership sur une ressource qui n'en a pas, et dit pourquoi : une appartenance à un groupe, une attribution de rôle, un constat d'analyse ou un utilisateur n'ont pas de propriétaire au sens de cette politique.

SOLUTION	RESSOURCES	CE QUI FAIT FOI
Microsoft 365	Sites et sous-sites SharePoint, OneDrive, équipes et canaux Teams, communautés Viva Engage, boîtes partagées, dossiers publics, Planner, Loop, Bookings, applications, flux et environnements Power Platform, espaces Power BI, environnements eDiscovery	Propriétaires du groupe (désignés) ; administrateurs de collection de sites et administrateurs Power BI (rôle) ; un canal standard et une application installée héritent de l'équipe ; une boîte partagée sans attribut de propriétaire a pour propriétaires déduits les détenteurs de l'accès complet
Entra ID	Groupes Microsoft 365, groupes de sécurité, listes de distribution, inscriptions d'applications, principaux de service, secrets et certificats, packages d'accès et catalogues, appareils inscrits	Propriétaires de l'objet (désignés) ; le responsable Exchange (ManagedBy) d'une liste de distribution ou d'un groupe à extension messagerie ; un secret hérite de son application, un package d'accès de son catalogue
Azure	Machines virtuelles et disques, applications web et de fonctions, stockage, bases SQL, Cosmos DB et Redis, conteneurs, coffres de clés, intégration, analyse, IA, exposition réseau, rôles personnalisés, délégations Lighthouse, autres ressources et périmètres	Étiquette « owner » de la ressource (désignée) ; rôle Owner sur la ressource (rôle) ; étiquette ou rôle Owner du groupe de ressources ou de la souscription (hérité)
AWS	67 ressources : calcul, conteneurs, bases, stockage, intégration, analyse, IA, exposition réseau, secrets et clés, identités d'application, utilisateurs, groupes, rôles et clés IAM, comptes, utilisateurs racine, jeux de permissions	L'étiquette que vous choisissez (désignée) ; à défaut, le propriétaire du compte ou l'utilisateur IAM (hérité). Les clés d'accès, les utilisateurs racine et les appartenances aux groupes IAM héritent toujours

Les solutions SaaS et les serveurs installés chez vous :

SOLUTION	RESSOURCES	CE QUI FAIT FOI
Google Workspace	Fichiers Drive, drives partagés, liens de partage, groupes, agendas, notes Keep, sites, espaces Chat, appareils mobiles et Chrome, projets et déploiements Apps Script, applications Marketplace, comptes de service	Propriétaire natif (désigné) ; gestionnaires d'un drive partagé ou d'un espace Chat (rôle) ; un déploiement Apps Script hérite des propriétaires du projet ; une application Marketplace a pour propriétaire déduit son installateur
GitHub	Organisations, dépôts, équipes, environnements, groupes d'exécuteurs, installations d'applications, packages, projets, jetons d'accès personnels	Propriétaires de l'organisation et administrateurs d'un dépôt (rôle), une équipe administratrice comptant pour un ; mainteneurs d'une équipe (rôle) ; un environnement hérite des administrateurs de son dépôt ; titulaire d'un jeton (désigné)
Slack	Canaux publics, privés et Slack Connect, groupes d'utilisateurs, workflows, applications installées, webhooks, jetons	Channel Managers d'un canal (rôle, sur Enterprise Grid) ; à défaut son créateur (déduit) ; collaborateurs d'un workflow (rôle) ; créateur ou installateur pour les groupes, applications et webhooks (déduit) ; titulaire d'un jeton (désigné)
Jira	Projets, projets de service, filtres, tableaux de bord, règles d'automatisation, jetons d'API	Lead du projet, propriétaire du filtre ou du tableau de bord, titulaire du jeton (désignés) ; auteur d'une règle d'automatisation
Asana	Projets, portefeuilles, objectifs, équipes	Propriétaire natif (désigné) ; administrateurs d'une équipe (rôle)
Okta	Groupes, applications, jetons d'API	Propriétaires de groupe et d'application (Okta Identity Governance) ; titulaire du jeton
Dropbox	Dossiers partagés, dossiers d'équipe, groupes, liens partagés	Propriétaire du dossier ; gestionnaires du groupe ; un dossier d'équipe hérite de l'équipe ; créateur d'un lien
SharePoint Server, Exchange Server	Sites et sous-sites, boîtes partagées, dossiers publics	Même règle que leurs équivalents Microsoft 365

Par collecte ou par import. La plupart de ces ressources sont lues par une connexion à l'éditeur. Certaines solutions passent aujourd'hui par l'import d'un fichier : AWS, Okta, Dropbox, SharePoint Server et Exchange Server. Le fichier porte alors une colonne des propriétaires et une colonne de leur source. Si la colonne de la source est vide, REVIEWIT applique la source habituelle de la ressource. Si la colonne des propriétaires manque, l'objet n'est pas évaluable.

AWS : posez une étiquette. AWS n'a pas de propriétaire natif. Sans étiquette, toutes les ressources d'un compte ont le même propriétaire, hérité du compte, et deux propriétaires de compte suffisent à rendre conformes des dizaines de ressources. Le verdict le dit (« hérité du compte »). Une étiquette « owner » par ressource donne un vrai propriétaire désigné.

Slack : le jeton d'administration. Les Channel Managers ne sont lisibles que sur Enterprise Grid, avec le jeton d'administration de la connexion. Sans lui, le propriétaire d'un canal est son créateur, et le verdict dit « déduit ».

08 Le verdict

RÉSULTAT	QUAND	CE QUE LIT LE RELECTEUR
Conforme	Le nombre de propriétaires valides atteint le minimum, et aucun invité interdit n'est propriétaire	« 2 propriétaires valides, désignés »
Écart	Moins de propriétaires valides que le minimum ; ou un invité est propriétaire alors que vous ne l'autorisez pas	« 1 propriétaire valide, hérité d'un parent — 1 non compté »
Non évaluable	La source ne dit pas qui possède l'objet : colonne absente à l'import, lecture refusée par l'éditeur	La fiche le montre sans juger

Trois règles de lecture :

01 **Le compte, puis la liste**
Le verdict dit combien de propriétaires valides l'objet a, de quelle source, combien d'administrateurs parmi eux et combien d'identités ne sont pas comptées. La liste nomme chacun.

02 **Hérité et déduit sont des faits, pas des fautes**
Un objet dont le propriétaire est hérité du compte peut être conforme. Le relecteur sait seulement que ce propriétaire ne connaît peut-être pas l'objet.

03 **Le risque qui reste**
Un propriétaire désigné peut être faux : une étiquette périmée, un lead qui a changé de poste. REVIEWIT ne le sait pas, le relecteur si. C'est pour cela que la source est nommée.

09 Ce que fait le relecteur

Les relecteurs sont les **propriétaires trouvés** : toute personne résolue qui répond de l'objet. Un objet sans propriétaire résolu va au relecteur de repli de la campagne. Le relecteur voit la liste, la source et la nature de chaque identité. Il a trois gestes :

- **Confirmer** la liste.
- **Compléter** : nommer un second propriétaire quand la règle en exige deux.

- **Corriger** : un nom déduit ou hérité n'est pas le bon.

Il ne peut pas rendre conforme un objet qui n'a qu'un propriétaire quand la règle en exige deux : il doit en nommer un second. L'ajout du propriétaire chez l'éditeur est suivi par la remédiation. Le sauvetage d'un objet sans aucun propriétaire est le travail d'Orphan.

10 Ce que la politique ne fait pas

- Elle ne change aucun propriétaire chez l'éditeur : elle rend la propriété visible, sourcée et confirmée.
- Elle ne juge pas les personnes : un compte désactivé ou supprimé est montré « non résolu », pas évalué.
- Elle ne déplie pas les groupes : un groupe propriétaire compte pour un, quel que soit le nombre de ses membres.
- Elle ne devine pas un propriétaire que la source ne donne pas : sans source, l'objet n'est pas évaluable.
- Elle ne compte pas les comptes de service, robots et applications comme propriétaires.

11 Mettre en œuvre une campagne

01 **Choisir le workspace et la ressource**
Ownership s'offre aux ressources qui portent une liste de propriétaires et sa source. L'assistant ne la propose pas ailleurs.

02 **Vérifier la connexion ou le fichier**
Pour les listes de distribution et les groupes à extension messagerie, la connexion Microsoft doit pouvoir lire Exchange : sans ce droit, leur responsable reste inconnu et l'objet n'est pas évaluable. Pour Slack, ajoutez le jeton d'administration si vous êtes sur Enterprise Grid. Pour un import, gardez les colonnes des propriétaires et de leur source.

03 **Régler la campagne dans le panneau Ownership : le nombre minimum (2 par défaut), les rôles qui comptent, les invités.**

04 **Désigner le relecteur de repli, pour les objets dont aucun propriétaire n'est résolu.**

05 **Lire les résultats, puis laisser les propriétaires confirmer, compléter ou corriger. Une première campagne sur les groupes et les sites fait souvent apparaître les objets à un seul propriétaire, les plus nombreux.**

Exemple. Cent quatre-vingts groupes Microsoft 365 et de sécurité. Avec un minimum de 2, quarante-six sont en écart : trente et un n'ont qu'un propriétaire, douze n'en ont aucun, trois ont pour seul propriétaire un principal de service, nommé et non compté. Sept listes de distribution ont pour propriétaire leur responsable Exchange, désigné. Les propriétaires nomment un second propriétaire sur trente-huit groupes ; les douze sans propriétaire passent au relecteur de repli, puis à Orphan.

Autre exemple. Deux cents ressources AWS importées d'un compte de production. Cent soixante n'ont pas d'étiquette « owner » : leurs deux propriétaires sont hérités du compte, et le verdict le dit sur chacune. Les quarante étiquetées ont un propriétaire désigné. L'équipe cloud décide d'étiqueter les bases et les buckets avant la campagne suivante.

12 Glossaire

Propriétaire	une identité qui répond de l'objet, désignée par l'éditeur, par votre organisation, par un rôle de gestion ou par un parent.
Propriétaire valide	un propriétaire qui compte, c'est-à-dire une personne ou un groupe de l'organisation (un invité si vous l'autorisez).
Source	ce qui désigne le propriétaire : désigné, rôle de gestion, hérité, déduit, aucun.
Hérité	le propriétaire d'un parent de l'objet (groupe de ressources, souscription, compte, équipe, application).
Déduit	une personne liée à l'objet sans le posséder (créateur, installateur, détenteur d'un accès complet).
Non résolu	une identité que l'éditeur rend sans qu'elle puisse être rattachée à une personne ou un groupe ; elle est montrée et ne compte pas.
Non évaluable	la source ne dit pas qui possède l'objet ; REVIEWIT ne tranche pas.

REVIEWIT

Cette fiche décrit la politique telle que REVIEWIT la met en œuvre à la date de publication. Les signaux lus dépendent de ce que chaque éditeur rend vérifiable ; ils peuvent évoluer avec les versions suivantes.