LA POLITIQUE « OVERSHARED »

# La politique « Overshared » : l'audience interne trop large

Overshared met sous les yeux du responsable de chaque objet l'audience **interne** que l'éditeur rend vérifiable : un accès ouvert à toute l'organisation, des groupes jugés trop larges, le nombre de liens d'organisation, le nombre de personnes. Cette audience est comparée aux seuils que **vous** fixez. Le responsable confirme l'audience ou la réduit, et sa décision est tracée.

VERSION
1.3 · Novembre 2026

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

DIFFUSION
Confidentiel · Clients REVIEWIT

DANS CETTE FICHE


1 Le problème : un accès que personne n'a décidé
2 Une question à part
3 La philosophie : cinq partis pris
4 Les quatre signaux et les réglages qui leur répondent
5 Comment l'audience est dénombrée
6 Ressource par ressource
7 Le verdict
8 Ce que fait le relecteur
9 Ce que la politique ne fait pas
10 Mettre en œuvre une campagne
11 Glossaire


## 01 Le problème : un accès que personne n'a décidé

Un site d'équipe est créé pour douze personnes. Trois ans plus tard, il porte quarante liens « personnes de votre organisation » sur ses fichiers, un groupe « Tous les salariés » a été ajouté aux membres pour dépanner un projet, et personne ne s'en souvient. Rien n'est sorti de l'entreprise, aucun invité n'est entré, le site est toujours déclaré « privé ». Et pourtant ses contenus sont à portée de cinq mille personnes.

C'est le **sur-partage** : l'écart entre l'audience voulue d'un objet et l'audience qui peut effectivement l'atteindre. Il s'installe par petits gestes légitimes, il ne déclenche aucune alerte, et il reste invisible tant qu'un outil de recherche ou un assistant ne rend pas trouvable ce qui était seulement accessible. Les assistants d'entreprise ne créent aucun accès : ils révèlent ceux qui existent déjà.

## 02 Une question à part

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

| POLITIQUE | LA QUESTION | LE FAIT LU | FRONTIÈRE |
|---|---|---|---|
| Privacy | La visibilité déclarée est-elle celle voulue ? | Un réglage de l'objet : public ou privé | Ce que l'objet **annonce** |
| External Sharing | Le partage hors de l'organisation est-il justifié ? | Le niveau de partage externe, les liens « tout le monde » | La **frontière de l'organisation** |
| Guests | Chaque invité garde-t-il un motif d'accès ? | Des personnes externes nommées | Une **personne externe** |
| Membership, Permissions | Chaque détenteur doit-il rester, à ce niveau ? | Un accès nominatif | Une **personne**, une à une |
| **Overshared** | Qui, dans l'organisation, peut effectivement atteindre l'objet, et est-ce plus large que son usage ? | Un octroi à toute l'organisation, des liens d'organisation, une audience dénombrée | **L'audience interne effective**, prise en bloc |

Un objet « privé » peut être ouvert à tous : Privacy le dit conforme, Overshared le voit. Une revue nominative ne voit pas la revendication « tout le monde », qui n'est pas une personne : Overshared la lit. Quand le réglage de visibilité de l'éditeur signifie par lui-même « toute l'organisation » (un projet public à l'espace de travail, un dépôt interne, un canal public), c'est Privacy qui le juge et Overshared ne le rejuge pas : Overshared ne retient que des **octrois** et des **audiences mesurées**.

## 03 La philosophie : cinq partis pris

**01** **Mesurer ce qui se vérifie, ne jamais supposer.**

Chaque signal vient d'une source que l'éditeur documente : une liste de membres, un compte de membres, un rapport d'administration. Un signal que l'éditeur ne donne pas n'est pas écrit, et le critère correspondant n'est pas évalué. *Absent n'est jamais zéro.*

**02** **Un minimum vérifiable, et dire s'il est complet.**

Le nombre de personnes d'une audience est toujours un **plancher prouvé**, accompagné d'un indicateur de complétude. Quand un groupe n'a pas pu être développé, ou qu'un accès est ouvert à toute l'organisation, le nombre reste un minimum et l'objet le dit. Un minimum au-dessus du seuil est un fait ; un minimum sous le seuil, incomplet, ne vaut pas conformité.

**03** **Le seuil appartient à l'organisation.**

« Trop » dépend de l'usage : trois cents personnes pour un site de direction, trois mille pour l'intranet d'une division. REVIEWIT ne fixe aucun seuil numérique par défaut ; il tranche seulement le fait binaire, l'accès ouvert à toute l'organisation, et laisse les nombres au client.

04 **Le verdict dit ce que l'audience est ; la décision reste au responsable.**

Une audience large peut être voulue : intranet, site de communication, communauté de toute l'entreprise. Le relecteur confirme avec un motif, demande la réduction ou escalade. Chaque décision est tracée et opposable.

05 **Des agrégats, jamais des contenus.**

Les signaux sont un texte d'octroi et des nombres. REVIEWIT ne lit aucun fichier, aucun message, ne juge pas la sensibilité d'un contenu et ne conserve pas le détail élément par élément d'un rapport d'administration. L'étiquette de confidentialité n'est connue que par son identifiant.

## 04 Les quatre signaux et les réglages qui leur répondent

| SIGNAL PORTÉ PAR L'OBJET | SENS | RÉGLAGE DE LA CAMPAGNE | ÉCART SI |
|---|---|---|---|
| **Accès à toute l'organisation** (OrgWideAccess) | Les octrois à l'organisation entière, dans les mots de l'éditeur, avec le rôle et le chemin : « Tout le monde sauf les utilisateurs externes · Modifier · via Membres du site » | Autoriser l'accès à toute l'organisation (oui/non, non par défaut) | Un octroi est présent et n'est pas autorisé |
| **Groupes de l'audience** (AudienceGroups) | Les groupes d'annuaire qui donnent accès, nommés | Groupes jugés trop larges, choisis dans votre annuaire (« Tous les salariés », un groupe dynamique) | Un des groupes choisis donne accès |
| **Liens d'organisation** (OrgLinkCount) | Le nombre de liens actifs « personnes de votre organisation », tel qu'un rapport d'administration le compte, avec sa date d'arrêté | Nombre maximal de liens d'organisation | Le nombre dépasse le maximum |
| **Taille de l'audience** (AudienceSize, et sa complétude) | Le nombre de personnes qui peuvent atteindre l'objet, plancher prouvé | Audience maximale | Le nombre dépasse le maximum, même si le compte est incomplet |

Un dernier réglage, le **mode d'écart**, dit ce qu'un écart fait au verdict global : en mode strict, un critère en écart rend l'objet non conforme ; en mode souple, chaque écart reste visible critère par critère et le verdict global reste conforme. Le mode souple sert à une première campagne d'observation.

# 05 Comment l'audience est dénombrée

C'est la question la plus fréquente : *qui calcule l'audience, et les groupes imbriqués comptent-ils ?*

Le seuil, personne ne le calcule : c'est votre réglage. L'audience, c'est la **collecte** qui la mesure, au moment du passage, avec les mêmes règles pour toutes les ressources :

- **Une personne nommée compte une fois**, par son identité résolue. Une identité que l'éditeur ne permet pas de résoudre rend l'audience incomplète.
- **Un groupe d'annuaire est nommé, puis compté** par le nombre d'utilisateurs qu'il atteint **en traversant ses sous-groupes** jusqu'aux personnes. Les groupes imbriqués sont donc pris en compte. Comme les membres de plusieurs groupes se recouvrent, leur somme ne prouverait rien : REVIEWIT retient le plus grand des comptes, et marque l'audience incomplète. Un groupe qui ne peut pas être compté reste nommé ; rien n'est inventé.
- **Un accès ouvert à toute l'organisation est rapporté, jamais compté.** Il rend l'audience incomplète : le nombre de personnes est alors « au moins N ».
- **Les liens d'organisation** ne se lisent pas par les interfaces de programmation : ils viennent du rapport d'administration de l'éditeur, que vous importez dans REVIEWIT comme **import complémentaire**. Chaque valeur porte la date d'arrêté du rapport, affichée avec le critère, et cesse d'être prise en compte au-delà de soixante jours.

L'audience est ainsi lue **au niveau de l'objet collecté** : le site, l'équipe, la communauté, l'espace. Le détail fichier par fichier n'est pas couvert ; le rapport d'administration l'agrège par objet, c'est ce que l'import complémentaire apporte.

# 06 Ressource par ressource

| RESSOURCE | CE QUI EST MESURÉ | GROUPES IMBRIQUÉS | AUDIENCE COMPLÈTE ? |
|---|---|---|---|
| Site SharePoint | Les personnes des octrois du site, les groupes accordés nommés et comptés, l'accès à toute l'organisation ; les liens d'organisation par l'import du rapport d'autorisations de site | Oui, par le compte transitif des groupes | Non dès qu'un groupe ou un accès à toute l'organisation est présent |
| OneDrive | Les liens d'organisation et le nombre d'utilisateurs ayant accès, par l'import du même rapport | Sans objet | Selon le rapport |
| Équipe Teams | Les personnes de la liste des membres de l'équipe (propriétaires, membres, invités) | Sans objet : les membres d'une équipe sont des personnes, un groupe Microsoft 365 ne contient pas de groupe | Oui, si chaque membre est nommé |
| Communauté Viva Engage | Les membres du groupe Microsoft 365 lié | Sans objet, même raison | Oui ; une communauté ouverte à tout le réseau sans liste de membres n'a **pas** d'audience et n'est pas évaluée |
| Espace Power BI | Les groupes d'annuaire qui ont accès à l'espace, nommés ; le nombre de liens ouverts à toute l'organisation, tel que l'éditeur le rapporte | Non dépliés : l'espace est jugé sur ses octrois, pas sur un dénombrement | Sans objet : aucun nombre de personnes n'est calculé |
| Dossier public Exchange | Le droit **par défaut** du dossier quand il l'ouvre à toute l'organisation, rendu dans les mots de l'éditeur avec le chemin (« Default · Author · \Annonces internes ») ; les groupes d'annuaire qui ont un droit sur le dossier, nommés | Non dépliés | Sans objet : le dossier est jugé sur l'octroi ; un accès anonyme est collecté à part et ne relève pas d'Overshared |
| Boîte partagée Exchange | Les personnes qui ont l'**accès complet** à la boîte, dénombrées ; les groupes accordés en accès complet, nommés. Les droits « envoyer en tant que » et « envoyer de la part de » ne lisent pas la boîte et ne comptent pas | Non dépliés : un groupe accordé rend l'audience incomplète | Oui tant qu'aucun groupe n'est accordé ; « au moins N » sinon |

| RESSOURCE | CE QUI EST MESURÉ | GROUPES IMBRIQUÉS | AUDIENCE COMPLÈTE ? |
|---|---|---|---|
| Bucket S3, snapshot RDS, table DynamoDB (AWS) | Les **findings d'accès interne** d'IAM Access Analyzer sur l'objet : un accès ouvert à **toute l'organisation** ou à une **unité d'organisation** (politique de ressource à principal « * » conditionnée par l'identifiant ou le chemin d'organisation), rendu « Organisation o-… · s3:GetObject, s3:ListBucket » ; les autres principaux internes trouvés (rôles, utilisateurs, comptes), nommés avec leurs actions. L'accès public reste une question de visibilité, le partage à un autre compte hors organisation une question de partage externe | Sans objet : un principal IAM n'est pas déplié | Sans objet : aucun nombre de personnes n'est calculé ; sans analyseur d'accès interne chez le client, les deux signaux sont vides et l'objet est hors champ |
| Drive partagé Google | Une permission de type **domaine** sur le Drive, rendue « Domaine votre-domaine · Lecteur » ; les groupes accordés, nommés ; les personnes nommées, dénombrées. Les gestionnaires du Drive répondent | Non dépliés : un groupe ou le domaine rend l'audience incomplète | Oui tant qu'aucun groupe ni le domaine n'est présent ; « au moins N » sinon |
| Site Google | Une permission de type domaine sur le fichier du site ; la portée de publication reste une question de visibilité (Privacy) | Sans objet | Sans objet |
| Mon Drive (Google) | Le nombre de fichiers dont un lien est ouvert au domaine, compté par le passage des liens partagés et daté ; les fichiers ne sont jamais nommés | Sans objet | Sans objet |
| Canal Slack | Le nombre de membres du canal, tel que Slack le rend ; complet quand il est rendu, incomplet pour un canal privé que l'application ne voit pas | Sans objet : les membres d'un canal sont des personnes | Oui quand Slack rend le compte |
| Équipe Asana | Le nombre de membres de l'équipe | Sans objet | Oui |
| Projet Asana | Les membres directs, plus l'équipe quand le projet lui est partagé ; l'équipe partagée, nommée | Non dépliée : une équipe partagée rend l'audience incomplète | Oui sans équipe partagée ; « au moins N » sinon |
| Dépôt GitHub | La permission de base de l'organisation quand elle n'est pas « none », rendue sur chaque dépôt « Membres de l'organisation · read, write ou admin » ; les équipes qui ont accès, nommées | Non dépliées | Sans objet : aucun nombre de personnes n'est calculé |

| RESSOURCE | CE QUI EST MESURÉ | GROUPES IMBRIQUÉS | AUDIENCE COMPLÈTE ? |
|---|---|---|---|
| Filtre ou tableau de bord Jira | Un partage à **tous les utilisateurs connectés**, rendu « Tous les utilisateurs connectés · Lecture » ; les partages à un groupe ou à un projet, nommés. Un partage public reste une question de partage externe | Non dépliés | Sans objet |

Une équipe Teams et son site SharePoint sont deux objets : un groupe de sécurité ajouté à la main dans le site se lit sur le site, pas sur l'équipe. Chacun est évalué avec sa propre audience.

**Qui répond pour une boîte partagée.** Exchange n'enregistre aucun propriétaire pour une boîte partagée. REVIEWIT retient le propriétaire que **vous déclarez** dans l'un des attributs personnalisés de la boîte (`owner: prenom.nom@votre-domaine`), sinon les détenteurs de l'accès complet. La campagne dit lequel des deux a servi. Une boîte sans l'un ni l'autre, un dossier public sans propriétaire, une communauté sans liste de membres **sortent de la campagne** comme orphelins et sont signalés : REVIEWIT ne désigne jamais un relecteur par défaut.

## 07 Le verdict

| CRITÈRE | ATTENDU | OBSERVÉ |
|---|---|---|
| Accès à toute l'organisation | « Aucun accès ouvert à toute l'organisation » ou « autorisé pour cette campagne » | Le texte de l'octroi, ou « aucun » |
| Groupes jugés trop larges | « Aucun des groupes choisis » | Les groupes trouvés |
| Liens d'organisation | « Au plus N liens », avec la date d'arrêté du rapport | Le nombre |
| Taille de l'audience | « Au plus N personnes » | « N personnes » si l'audience est complète, « au moins N personnes » sinon |

Trois règles de lecture :

01 **Hors champ, dit comme tel**

Un objet qui ne porte aucun des quatre signaux n'a pas de verdict Overshared : la fiche le montre sans juger, elle n'affiche jamais une conformité par défaut.

02 **Un plancher au-dessus du seuil est un écart**

Même incomplète, une audience d'« au moins 40 personnes » dépasse un seuil de 30.

03 **Un plancher sous le seuil, incomplet, n'est pas évalué**

« Au moins 12 personnes » pour un seuil de 30 ne prouve rien : le critère est laissé ouvert plutôt que d'affirmer une conformité.

## 08 Ce que fait le relecteur

Le relecteur est, en principe, le **propriétaire de l'objet** : il connaît l'usage, il a souvent ouvert l'accès lui-même. Il voit l'octroi, le chemin, les groupes, les nombres et leurs dates. Il a trois gestes :

- **Confirmer l'audience**, avec un motif : intranet, site de communication, communauté d'entreprise. Le motif est conservé et ressort à la campagne suivante.
- **Demander la réduction** : retirer l'octroi, convertir les liens, sortir un groupe. La réduction est un geste d'écriture chez l'éditeur, suivi par la remédiation.
- **Escalader**, avec les mécanismes habituels de la revue.

Il ne lui est pas demandé de juger la sensibilité d'un contenu qu'il ne voit pas dans REVIEWIT, ni de changer les réglages du tenant : c'est l'affaire de l'administrateur de l'éditeur.

## 09 Ce que la politique ne fait pas

- Elle n'élimine pas le sur-partage : elle le rend visible, mesuré et décidé.
- Elle ne certifie aucune préparation à un assistant d'entreprise : elle y aide.
- Elle ne détecte pas les contenus sensibles et ne lit aucun contenu.
- Elle ne couvre pas le détail élément par élément d'un objet ; elle lit l'objet, et le rapport d'administration qui l'agrège.
- Elle ne modifie rien chez l'éditeur : la réduction d'une audience est une décision, puis une remédiation.

# 10 Mettre en œuvre une campagne

01 **Choisir le workspace et la ressource**

Overshared s'offre aux workloads qui portent au moins un des quatre signaux : pour Microsoft 365, SharePoint, OneDrive, Teams, Viva Engage, Power BI et Exchange (dossiers publics, boîtes partagées) ; pour Google Workspace, Google Drive et Sites ; pour Slack, les conversations ; pour Asana, les projets et les équipes ; pour GitHub, les dépôts ; pour Jira, les objets partagés ; pour AWS, le stockage (buckets S3) et les bases de données (snapshots RDS, tables DynamoDB). Le panneau n'offre que les critères que la ressource porte, et dit lesquels : pour une boîte partagée, l'audience et les groupes ; pour un dossier public, l'accès à toute l'organisation et les groupes ; pour une équipe, la seule audience.

02 **Importer le rapport d'administration si la campagne porte sur les liens d'organisation (sites, OneDrive) : Subscription Manager › Collecter › Importer un rapport, format « Import complémentaire ». Voir la fiche « L'import complémentaire ».**

03 **Régler la politique dans le panneau Overshared : l'accès à toute l'organisation autorisé ou non, les groupes jugés trop larges choisis dans l'annuaire, le nombre maximal de liens, l'audience maximale, le mode d'écart. Les nombres laissés vides ne sont pas évalués.**

04 **Désigner les relecteurs**

les propriétaires de l'objet, avec un relecteur de repli pour les objets sans propriétaire.

05 **Lire les résultats critère par critère, puis laisser les relecteurs confirmer ou réduire. Une première campagne en mode souple permet d'observer la distribution des audiences avant de fixer les seuils d'une campagne stricte.**

*Exemple.* Cinquante-six équipes Teams, toutes dénombrées avec une audience complète, de deux à dix-huit personnes. Une audience maximale de quinze fait ressortir six équipes publiques : le club de course, l'afterwork, le comité des fêtes, la communauté Power Platform, les nouveaux arrivants et l'équipe de toute l'entreprise. Leurs propriétaires confirment les cinq premières comme communautés voulues et la sixième comme équipe d'entreprise ; la campagne a établi, et tracé, que ces audiences sont assumées.

*Autre exemple.* Vingt-huit boîtes partagées. Trois portent un propriétaire déclaré, qui devient leur seul relecteur ; deux sont accordées en accès complet au groupe « Partage Finance » et une au groupe « Accès Paie », que la campagne juge trop larges ; une n'a ni propriétaire déclaré ni accès complet. La campagne compte vingt-sept boîtes et cinq écarts, et signale la vingt-huitième comme orpheline. Les relecteurs de la comptabilité confirment le groupe, puisque la boîte est celle du service ; celui du recrutement demande que le groupe de la paie soit retiré.

# 11 Glossaire

| | |
|---|---|
| **Audience interne** | l'ensemble des personnes de l'organisation qui peuvent atteindre un objet, par un accès direct, un groupe ou un lien. |
| **Accès à toute l'organisation** | un octroi dont le bénéficiaire est l'organisation entière (« Tout le monde sauf les utilisateurs externes », « Tous »), quel que soit le chemin. |
| **Lien d'organisation** | un lien de partage que toute personne de l'organisation peut ouvrir. |
| **Plancher prouvé** | le nombre de personnes que REVIEWIT a pu nommer ou compter ; l'audience réelle est au moins celle-là. |
| **Import complémentaire** | l'ajout, à des objets déjà collectés, des colonnes qu'un rapport d'administration est seul à connaître, avec sa date d'arrêté. |
| **Mode d'écart** | strict, un écart rend l'objet non conforme ; souple, les écarts sont visibles et le verdict global reste conforme. |

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.