LA POLITIQUE « INACTIVITÉ »

La politique « Inactivité » : ce qui ne sert plus

Inactivité met sous les yeux du responsable de chaque objet, et de chaque identité, la **dernière activité** que la source de l'éditeur enregistre : connexions, requêtes, accès, rapports d'usage. Elle la compare à la durée que **vous** fixez. Le responsable décide de garder, d'archiver, de désactiver ou de supprimer, et sa 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 : ce qui reste ouvert après l'usage
2 Une question à part
3 La philosophie : cinq partis pris
4 Le signal et le réglage qui lui répond
5 Comment la dernière activité est établie
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 : ce qui reste ouvert après l'usage

Un site de projet a servi dix-huit mois, puis le projet s'est terminé. Une clé d'accès a été créée pour un script de migration, lancé une seule fois. Un prestataire invité n'est plus revenu depuis la fin de sa mission. Une machine virtuelle de test tourne toujours, sans que personne ne s'y connecte.

Aucun de ces objets n'est en faute : chacun a eu un usage légitime. Mais tous gardent leurs accès, leurs données et leur coût après la fin de cet usage. Ils ne déclenchent aucune alerte, et personne ne pense à les fermer. C'est **l'inactivité** : l'écart entre ce qui existe encore et ce qui sert encore.

02 Une question à part

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

POLITIQUE	LA QUESTION	LE FAIT LU	FRONTIÈRE
Inactivité	L'objet, ou l'identité, sert-il encore ?	Une date de dernière activité, donnée par une source d'activité	L'**usage**, daté
Orphan	Quelqu'un en répond-il encore ?	L'absence ou le départ du propriétaire	Un objet actif peut être orphelin ; un objet inactif peut avoir un propriétaire
Data Lifecycle	La donnée est-elle gardée selon sa règle de conservation ?	Rétention, gel, archivage	Une archive légale est inactive **par nature** : la garder est la bonne décision
Guests	Chaque invité garde-t-il un motif d'accès ?	Des personnes externes	Inactivité lit la dernière connexion de l'invité ; Guests juge son **motif**
Privileged Access	Ce privilège est-il justifié ?	Les rôles élevés	Un compte d'accès d'urgence est inactif **à dessein**

Inactivité couvre les **ressources** (sites, équipes, dépôts, bases, machines, files de messages) et les **identités** (utilisateurs, invités, administrateurs, clés, jetons, rôles, applications autorisées, appareils). La question est la même : « dernière utilisation ». Seul change le geste qui suit : on archive une ressource, on désactive ou on révoque une identité.

03 La philosophie : cinq partis pris

01 **Une activité, pas une modification.**

Seule une source d'**activité** fait foi : une connexion, une requête, une invocation, un accès, un rapport d'usage. Une date de modification n'en est pas une. Une synchronisation, un provisionnement ou un processus système la déplacent sans aucun usage. Une date de création n'en est pas une non plus. La gestion d'un objet par un administrateur (l'arrêter, le reconfigurer) n'est pas son usage.

02 **Quand il n'y a pas de source d'activité, le dire.**

Certaines ressources n'ont qu'une date de modification : des sous-sites, des notes, des paramètres. Pour celles-là seulement, REVIEWIT lit la dernière modification, et le verdict le dit en toutes lettres : « aucune source d'activité pour cette ressource · dernière modification le … ». Une modification ancienne prouve l'inactivité. Une modification récente ne prouve pas l'usage.

03 **Ne jamais dater ce que la source n'a pas vu.**

Beaucoup de sources ne gardent qu'une période : 90 jours, six mois, quinze mois. Quand rien n'y apparaît, REVIEWIT ne pose pas de date inventée. Il écrit « aucune activité depuis au moins le … ». Quand la source regarde moins loin que la durée de la campagne, le critère est **non concluant** : il ne dit ni conforme ni en écart.

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

Trois mois sans usage, c'est beaucoup pour une clé d'accès et peu pour un site d'archives. REVIEWIT ne tranche pas : vous fixez la durée, le relecteur décide. Un objet inactif peut l'être à dessein : archive, objet saisonnier, accès d'urgence. Le relecteur le garde avec un motif, et ce motif est tracé.

05 **Une date, jamais un détail.**

REVIEWIT retient la date de la dernière activité et sa source. Il ne conserve ni le détail des événements (quelle page, quel fichier, quelle adresse), ni un profil d'activité, ni un contenu. Pour une personne, la date de dernière connexion est une donnée personnelle : REVIEWIT n'en garde que la date, au service de la revue de l'accès, jamais d'un suivi de l'activité individuelle.

04 Le signal et le réglage qui lui répond

CE QUE PORTE L'OBJET	SENS
Dernière activité	La date la plus récente où la source d'activité de l'éditeur a vu l'objet servir
Dernière modification	Pour une ressource sans source d'activité seulement : la date de la dernière modification, en repli
Début de la période lue	Pour une source qui ne garde qu'une période : la date depuis laquelle la source a regardé
Création	La date de création de l'objet, ou d'ajout de l'identité, quand l'éditeur la donne

Le réglage de la campagne est la durée d'inactivité : 3, 6, 9, 12 mois, ou 18 mois et plus. Un objet sans activité depuis plus longtemps que cette durée est en écart.

05 Comment la dernière activité est établie

C'est la question la plus fréquente : *d'où vient la date, et que se passe-t-il quand la source oublie ?*

01 **Chaque ressource a une source nommée**

Rapport d'usage, métrique de la plateforme, horodatage de dernière utilisation, journal d'audit : la source est celle que l'éditeur documente, et le verdict la cite.

02 **Plusieurs sources : la plus récente gagne**

Quand une ressource en a plusieurs, REVIEWIT retient la plus récente des dates.

03 **La mémoire d'une collecte à l'autre**

Une activité vue en mars reste connue en juillet, même quand la source ne la garde plus. REVIEWIT conserve la plus récente date déjà observée, avec la source qui l'a donnée. Au fil des collectes, la profondeur dépasse celle que l'éditeur garde. Rien n'est fabriqué : chaque date a été vue.

04 **Un objet absent de la source n'est pas inactif**

Il n'est pas évaluable. C'est le cas d'un objet créé après l'arrêté du rapport, ou d'un objet que la source ne liste pas.

05 Les rapports d'usage Microsoft 365 et les noms masqués

Par défaut, Microsoft masque les noms des utilisateurs, des groupes et des sites dans ses rapports d'usage. Les objets ne s'apparient alors plus. Avant chaque rapport, la collecte lit ce réglage. S'il est actif, le rapport n'est pas lu : la collecte le dit, nomme le réglage à changer dans le centre d'administration Microsoft 365, et ne pose aucune date. Pour lire ce réglage, la connexion a besoin d'une permission facultative, ReportSettings.Read.All. Sans elle, la collecte le signale et repère le masquage à la forme des identifiants. Rien n'est bloqué.

06 Les délais des éditeurs

Un rapport d'usage arrive avec 24 à 72 heures de retard, un journal d'audit avec quelques heures. La date de dernière activité est donc celle de l'arrêté du rapport, pas celle de la minute de la collecte.

SOURCE	PÉRIODE GARDÉE PAR L'ÉDITEUR
Rapports d'usage Microsoft 365	180 jours au plus
Métriques de la plateforme Azure	93 jours
Métriques AWS (CloudWatch)	15 mois
Journaux d'audit Google Workspace	6 mois ; rapports d'usage : 15 mois
Dernière connexion (Entra ID, Okta, Google, Jira), dernière utilisation (clés et rôles AWS, jetons GitHub et Jira), dernier push (GitHub), dernier accès (secrets AWS)	Conservée sur l'objet, sans limite (400 jours pour les rôles AWS)

06 Ressource par ressource

Inactivité s'offre aujourd'hui sur les ressources ci-dessous. Chacune a une source d'activité ou, quand elle n'en a pas, une date de modification de repli. Une ressource sans aucune date ne propose pas Inactivité. C'est le cas des appartenances à un groupe, des groupes de sécurité, des stratégies, des règles réseau, des unités d'organisation et des canaux Teams : l'activité d'une personne se lit sur son identité, pas sur son appartenance.

SOLUTION	RESSOURCE	CE QUI FAIT FOI
Microsoft 365	Sites SharePoint, OneDrive	Rapport d'usage des sites et de OneDrive : dernière activité sur les fichiers et les pages
Microsoft 365	Équipes Teams, communautés Viva Engage	Rapport d'activité des équipes ; rapport d'activité des communautés
Microsoft 365	Groupes Microsoft 365, boîtes aux lettres partagées	Rapport d'activité des groupes ; rapport d'usage des boîtes aux lettres
Microsoft 365	Sous-sites, espaces Loop, applications, flux et environnements Power Platform, dossiers publics, Bookings	*Repli* : dernière modification
Entra ID	Invités	Dernière connexion réussie (licence Entra ID P1)
Entra ID	Appareils inscrits	Dernière connexion approximative ; l'éditeur ne la met à jour qu'environ toutes les deux semaines
Azure	Machines virtuelles, disques, applications web et de fonctions, comptes de stockage, bases SQL, Cosmos DB et Redis, registres de conteneurs et Container Apps, Logic Apps, Service Bus et Event Hubs, API Management, coffres de clés, comptes Azure AI, Data Factory, espaces Log Analytics	Métriques de la plateforme : requêtes, transactions, connexions, exécutions, trafic ; 93 jours
AWS	Utilisateurs IAM, compte racine	Dernière utilisation du mot de passe et des clés (rapport d'identifiants)
AWS	Clés d'accès, rôles IAM	Dernière utilisation de la clé ; dernière utilisation du rôle (400 jours)
AWS	Accès inutilisés	Dernier accès rapporté par l'analyseur d'accès inutilisés d'IAM Access Analyzer, quand le client l'a créé
AWS	Secrets, WorkSpaces	Dernier accès au secret ; dernière connexion d'un utilisateur

SOLUTION	RESSOURCE	CE QUI FAIT FOI
AWS	Instances EC2, fonctions Lambda, bases RDS, files SQS, sujets SNS, Step Functions, flux Kinesis, points de terminaison SageMaker	Métriques CloudWatch : invocations, requêtes, connexions, lectures et écritures ; 15 mois pour la plupart
Google Workspace	Utilisateurs, invités	Dernière connexion
Google Workspace	Drives partagés, sites Google	Dernière utilisation active du drive (rapports d'usage, 15 mois) ; consultations au journal d'audit de Drive (6 mois)
Google Workspace	Appareils Chrome et mobiles	Dernière synchronisation de l'appareil
Google Workspace	Groupes, notes Keep, liens de partage	*Repli* : dernière modification
Okta	Utilisateurs, utilisateurs suspendus	Dernière connexion
Asana	Projets	*Repli* : dernière modification
GitHub	Dépôts	Dernier push
GitHub	Jetons d'accès fins, autorisations d'applications OAuth	Dernière utilisation du jeton ; dernier accès de l'application (organisation sous SAML SSO)
Jira	Utilisateurs	Dernière activité du compte dans les produits Atlassian
Jira	Jetons d'API	Dernière utilisation du jeton (Atlassian Guard)
Exchange Server	Boîtes aux lettres partagées	Dernier accès à la boîte
SharePoint Server, Exchange Server	Sites, sous-sites, dossiers publics	*Repli* : dernière modification

Ce qui viendra ensuite. D'autres sources d'activité sont documentées par les éditeurs et rejoindront la politique au fil des versions : canaux Slack, membres Dropbox, utilisateurs Asana, applications Okta, boîtes Gmail et espaces Chat, d'autres métriques Azure et AWS. Tant qu'une ressource n'a pas sa source, l'assistant ne lui propose pas Inactivité.

Une écriture peut être un usage. Un push sur un dépôt, un déploiement, une exécution sont des gestes : ils comptent comme activité. La date de dernière mise à jour d'un ticket, d'un élément ou d'une version est un horodatage que des automatisations déplacent : elle ne vaut qu'en repli.

Ce qui coûte chez l'éditeur. Certaines sources sont payantes ou à activer par le client. C'est le cas du tableau de bord de stockage avancé ou des événements de données de la piste d'audit d'AWS pour les buckets S3, des journaux de diagnostic, et de l'analyseur d'accès inutilisés. REVIEWIT les lit quand le client les a, et ne les exige jamais.

07 Le verdict

RÉSULTAT	QUAND	CE QUE LIT LE RELECTEUR
Actif	Une activité est plus récente que la durée de la campagne	« Dernière activité le 12/09/2026 · rapport d'usage »
Inactif	La dernière activité est plus ancienne que la durée ; ou la source n'a rien vu depuis plus longtemps que la durée ; ou l'objet n'a jamais servi depuis sa création	« Aucune activité depuis au moins le 08/08/2026 » · « Jamais utilisée depuis sa création le 03/01/2025 »
Non concluant	La source regarde moins loin que la durée de la campagne, et n'a rien vu	« Aucune activité sur les 90 jours que la source conserve ; la durée de 6 mois ne peut pas être vérifiée »
Trop récent	L'objet a été créé depuis moins longtemps que la durée, sans activité qui conclue	« Créé le 20/10/2026, trop récent pour être jugé »
Non évaluable	L'objet n'apparaît pas dans la source	La fiche le montre sans juger

Trois règles de lecture :

01 **Jamais une conformité par défaut**
Un objet sans date n'est pas déclaré actif : il n'est pas évaluable, et la fiche le dit.

02 **« Au moins » est un fait**
« Aucune activité depuis au moins 90 jours » dépasse une durée de 3 mois : l'objet est inactif. Il ne dépasse pas une durée de 6 mois : le critère reste ouvert, il est non concluant.

03 **Le repli est annoncé**
Pour une ressource jugée sur sa dernière modification, le verdict le dit, et le relecteur sait qu'une modification récente ne prouve pas l'usage.

08 Ce que fait le relecteur

Le relecteur est, en principe, le **propriétaire de l'objet** ou le responsable de l'identité. Il voit la date de la dernière activité, sa source, la période lue et la date de création. Il a quatre gestes :

- **Garder**, avec un motif : archive, objet saisonnier, accès d'urgence, compte racine. Le motif est conservé et ressort à la campagne suivante.
- **Archiver ou désactiver** : l'objet reste, mais ne sert plus.
- **Supprimer ou révoquer** : la clé, le jeton, l'invité, la ressource.
- **Escalader**, avec les mécanismes habituels de la revue.

Le geste lui-même chez l'éditeur est suivi par la remédiation. Il n'est pas demandé au relecteur de juger une activité que la source ne compte pas, ni de changer la conservation des journaux ou le masquage des rapports : c'est l'affaire de l'administrateur de l'éditeur.

09 Ce que la politique ne fait pas

- Elle ne supprime rien et ne dit jamais qu'un objet est « à supprimer » : elle rend l'inactivité visible, datée et décidée.
- Elle ne chiffre aucune économie de licences, de stockage ou de coût cloud.
- Elle ne détecte pas toute activité : elle lit celle que la source de l'éditeur compte, avec ses périodes et ses délais.
- Elle ne distingue pas toujours l'usage humain de l'activité d'un processus. Une sauvegarde, une supervision ou un compte système peuvent tenir un objet « actif » ; le relecteur, qui connaît l'usage, en juge.
- Elle ne suit pas l'activité des personnes : elle revoit des accès qui ne servent plus.

10 Mettre en œuvre une campagne

01 **Choisir le workspace et la ressource**

Inactivité s'offre aux ressources qui portent une date de dernière activité ou, à défaut, de dernière modification. L'assistant ne la propose pas sur une ressource sans date, et dit pourquoi : « pas de source d'activité pour cette ressource ».

02 **Vérifier la connexion**

Pour Microsoft 365, accordez la permission facultative ReportSettings.Read.All : la collecte peut alors dire si les rapports d'usage masquent les noms. Certaines sources dépendent de l'offre du client (Entra ID P1 pour la dernière connexion des invités, Atlassian Guard pour les jetons Jira) : sans elle, la date manque et l'objet n'est pas évaluable.

03 **Régler la durée d'inactivité dans le panneau Inactivité. Elle doit tenir compte de la période que garde la source : une durée de 6 mois sur une ressource lue par des métriques de 93 jours reste non concluante tant que la mémoire de REVIEWIT n'a pas dépassé cette période.**

04 **Désigner les relecteurs**

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

05 **Lire les résultats, puis laisser les relecteurs garder, archiver, désactiver ou supprimer. Une première campagne courte, à 3 mois, sur les clés et les jetons, fait souvent apparaître les accès les plus faciles à fermer.**

Exemple. Deux cent quarante clés d'accès et jetons, collectés avec leur dernière utilisation. Une durée de 3 mois en fait ressortir trente-et-un : dix-neuf n'ont pas servi depuis plus d'un an, sept n'ont jamais servi depuis leur création, cinq ont été créés il y a moins de trois mois et sont « trop récents pour être jugés ». Les propriétaires révoquent vingt-quatre clés et en gardent deux, avec un motif : un accès d'urgence et une migration annuelle.

Autre exemple. Cent quarante sites SharePoint, lus par le rapport d'usage des sites. Une durée de 12 mois fait ressortir trente-huit sites sans activité. Trois sites créés le mois dernier sont trop récents, et deux sites absents du rapport ne sont pas évaluables. Les propriétaires archivent vingt-neuf sites de projets terminés, gardent six archives sous conservation légale, et en suppriment trois.

11 Glossaire

Activité	un usage enregistré par une source de l'éditeur (connexion, requête, invocation, accès, rapport d'usage, push, déploiement).
Source d'activité	le rapport, la métrique, l'horodatage ou le journal que l'éditeur documente et que REVIEWIT cite dans le verdict.
Repli sur la modification	pour une ressource qui n'a aucune source d'activité, la date de dernière modification, annoncée comme telle.
Période lue	la durée que la source conserve ; au-delà, l'éditeur ne sait plus rien.

Non concluant	la source regarde moins loin que la durée de la campagne et n'a rien vu ; REVIEWIT ne tranche pas.
Trop récent	l'objet existe depuis moins longtemps que la durée de la campagne.
Mémoire d'activité	la plus récente date d'activité déjà observée, conservée par REVIEWIT d'une collecte à l'autre.

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.