LES 10 PRINCIPAUX ÉVÉNEMENTS DE SÉCURITÉ À SURVEILLER DANS AZURE AD ET OFFICE 365

Découvrez les lacunes des outils d'audit natifs et surmontez-les

Quest

Votre organisation est-elle véritablement plus en sécurité depuis que vous exécutez vos applications dans le Cloud ?

Plus efficace, très certainement. Mais plus en sécurité ?

Les utilisateurs peuvent toujours réaliser des actions à haut risque dans le Cloud, et les informations d'identification des comptes peuvent toujours être compromises. Depuis des années, Microsoft avertit les administrateurs que des dizaines de millions de comptes AD sont la cible quotidienne de cyberattaques.[1] Qui plus est, 34 % des violations de données impliquent une personne interne au réseau.[2]

Malheureusement, les outils d'audit natifs d'Office 365 et Azure AD laissent beaucoup à désirer en matière d'audit des modifications apportées aux rôles, groupes, applications, partages et boîtes aux lettres. Leurs fonctionnalités de recherche sont limitées et les événements d'audit ne sont conservés que pendant un certain temps.

Office 365 et Azure AD offrent des capacités de recherche limitées et ne conservent les événements d'audit que pendant un certain temps.

Cet e-book met en lumière dix événements de sécurité que les administrateurs suivent de très près pour préserver la sécurité de leur environnement Azure AD et Office 365. Il explore les informations d'audit qu'ils peuvent trouver à l'aide des outils et consoles natifs, et identifie les écueils les plus fréquents associés à une extraction native des rapports. Pour finir, dévoile une solution susceptible de les aider à surmonter certaines de ces restrictions liées à l'audit natif.

1 Fontana, John, « Active Directory czar rallies industry for better security, identity », ZDNet, juin 2015, https://www.zdnet.com/article/active-directory-czar-rallies-industry-for-better-security-identity/

2 « 2019 Data Breach Investigations Report », Verizon, mai 2019, https://enterprise.verizon.com/resources/reports/dbir/2019/summary-of-findings/

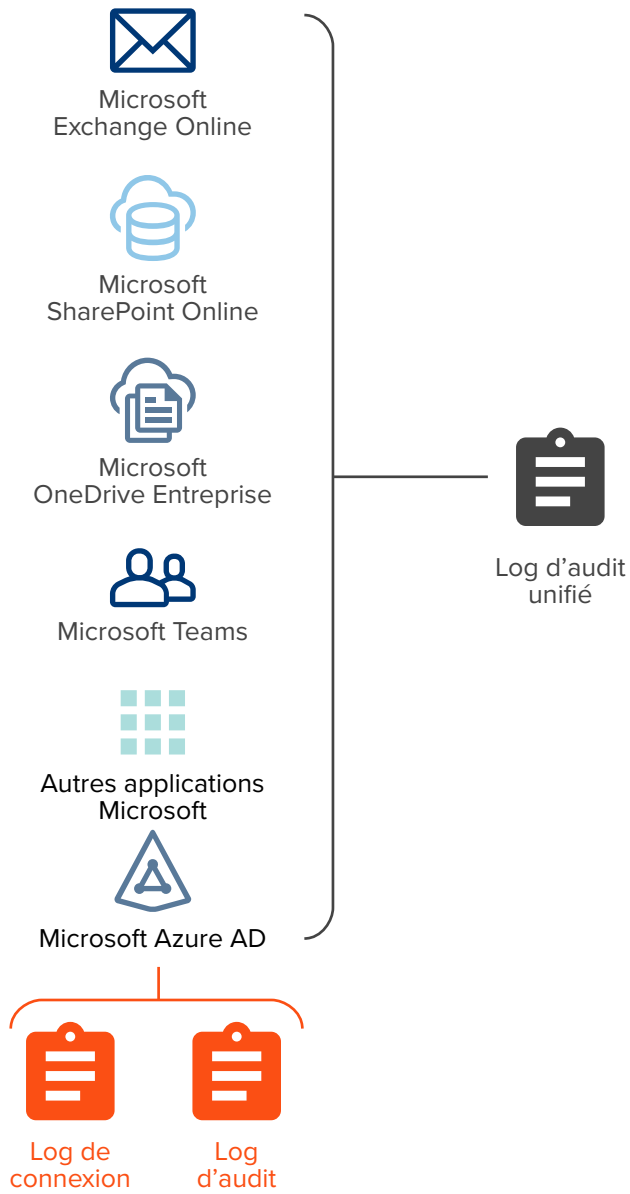


Figure 1 : Log d'audit unifié (pour la recherche dans le log d'audit Office 365)

Comment fonctionne l'audit natif dans Azure et Office 365 ?

La gestion et la sécurisation d'un environnement Cloud exigent tout d'abord de pouvoir suivre les événements de connexion et déconnexion d'un utilisateur.

Pour obtenir ces renseignements localement, les administrateurs système qui essaient de suivre les utilisateurs doivent examiner plusieurs logs sur chaque contrôleur de domaine Windows et mettre en relation les événements d'audit sur les logs de plusieurs serveurs.

Dans le Cloud, les administrateurs doivent mettre en relation de manière similaire deux logs dans Azure AD : le log d'audit qui contient tous les événements de modification, et le log de connexion qui contient tous les événements d'authentification (voir Figure 1). Ils y accèdent par le Portail Azure ou par PowerShell.

Quant à Office 365, chaque application (Exchange Online, SharePoint Online, OneDrive Entreprise, etc.) écrit dans ce qui deviendra le log d'audit unifié Office 365, contenant tous les événements au niveau de l'administrateur et de l'utilisateur. Le log d'audit unifié inclut également des événements du log d'audit Azure et du log de connexion.

Les administrateurs savent quels types de données sont conservés dans les logs. Mais extraire ces données et les utiliser pour gérer et sécuriser leur environnement est une autre affaire.

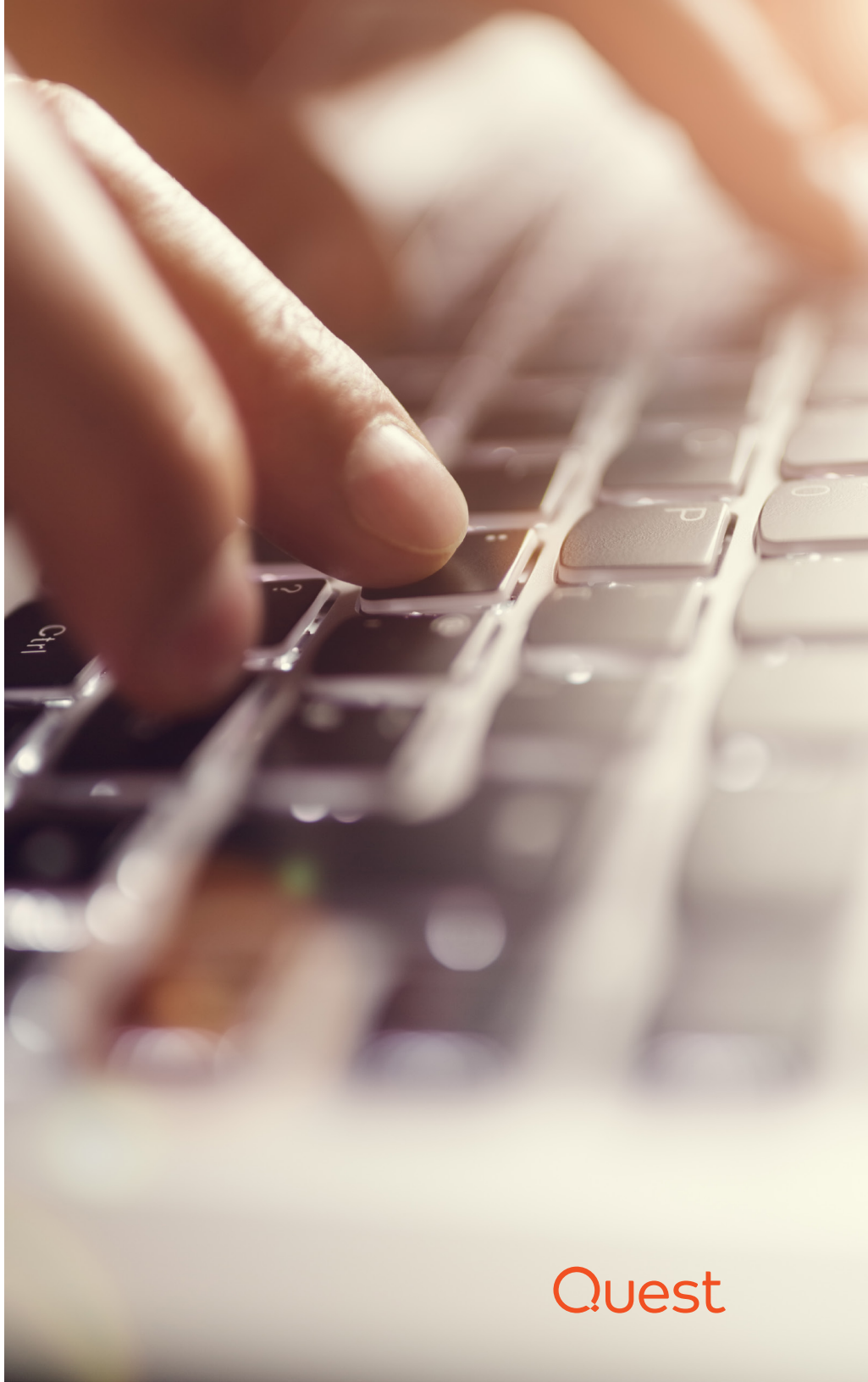
Quest

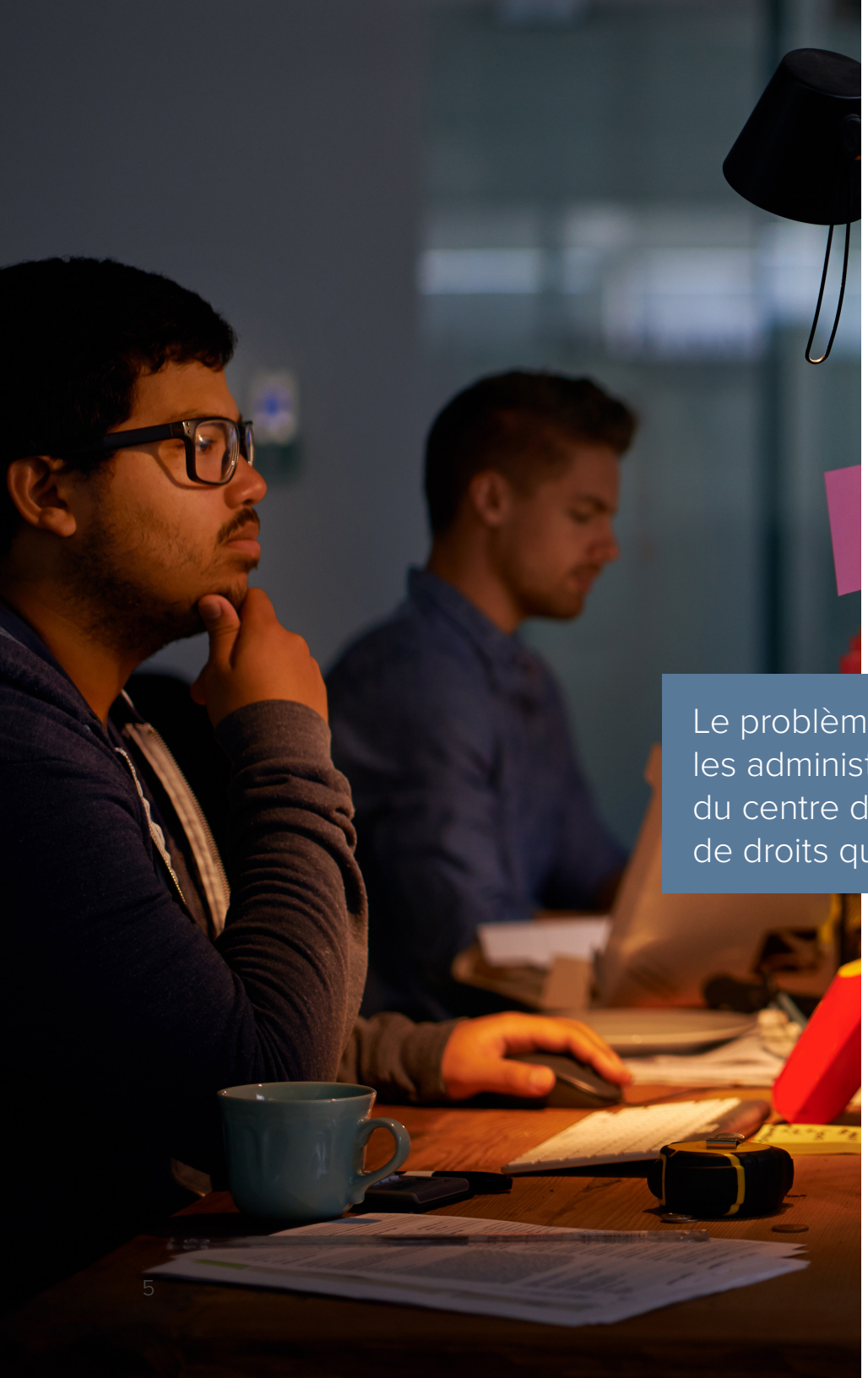
Les administrateurs savent où se trouvent les logs, ainsi que le type de données qu'ils contiennent. Mais extraire ces données et les utiliser pour gérer et sécuriser leur environnement est une autre affaire.

LES LACUNES DES OUTILS D'AUDIT NATIFS

Les audits dans Azure et Office 365 comportent de nombreuses restrictions.

- Pour les organisations qui exploitent des environnements hybrides, il n'est pas possible de rechercher une activité d'audit dans les charges de travail locales et dans le Cloud depuis un affichage unique.
- De même, les stratégies d'audit pour les charges de travail locales doivent être configurées séparément de celles des charges de travail dans le Cloud. Il est aussi impossible de surveiller les stratégies d'audit en cas d'évolution ou de désactivation par d'autres administrateurs.
- Un décalage d'au moins 24 heures peut intervenir dans le traitement de certaines entrées des logs d'audit et leur ajout au log d'audit unifié.
- Dans Azure, les logs sont conservés pour une durée qui varie en fonction de la charge de travail et du type d'abonnement. Cela peut être un facteur restrictif lorsque le service informatique enquête sur des incidents. Tout comme cela peut être source d'incertitude pour certaines exigences de conformité.
- Les événements sont formatés différemment selon le type d'événement et selon que celui-ci s'est produit dans le Cloud ou localement. En l'absence de format normalisé, les logs consultables depuis les consoles natives sont difficiles à interpréter.
- Il est possible d'accéder aux événements d'audit pour Azure et Office 365 depuis PowerShell. De plus, Azure et Office 365 proposent tous deux un portail Web pour accéder aux événements d'audit. Toutefois, celui-ci n'affiche que 15 événements à la fois, et qui plus est, en raison du décalage qui intervient dans leur traitement, tous les événements d'audit pertinents ne sont pas nécessairement affichés en même temps.





1. Modifications apportées aux rôles importants

Dans une infrastructure locale, plusieurs groupes au sein d'AD, tels que les Administrateurs de domaines, les Opérateurs de compte et les Administrateurs de serveur, sont considérés comme importants en raison des droits avancés qu'ils confèrent. Dans le Cloud, cela s'applique également aux rôles dans le locataire Azure.

Le problème est que, au fil du temps, les utilisateurs tels que les administrateurs, opérateurs, responsables et techniciens du centre d'assistance acquièrent progressivement bien plus de droits que ce qu'ils devraient. Par conséquent, une gestion prudente inclut la possibilité de signaler et alerter sur les changements qui interviennent dans ces groupes et rôles.

Le problème est que, au fil du temps, les utilisateurs tels que les administrateurs, opérateurs, responsables et techniciens du centre d'assistance acquièrent progressivement bien plus de droits que ce qu'ils devraient.

TROUVER DES RÔLES DANS LE LOG D'AUDIT AZURE

Dans le Cloud, la première étape consiste à identifier les rôles importants dans le portail Azure. Dans la section **Logs d'audit** sous Azure Active Directory, une recherche sur le service **Core Directory** et la catégorie **RoleManagement** renvoie tous les changements apportés dans le locataire, comme le montre la Figure 2. Malheureusement, il n'est pas possible de rechercher directement les rôles dits importants. Les administrateurs doivent examiner chaque événement d'audit séparément pour savoir quel rôle a été modifié.

Quest

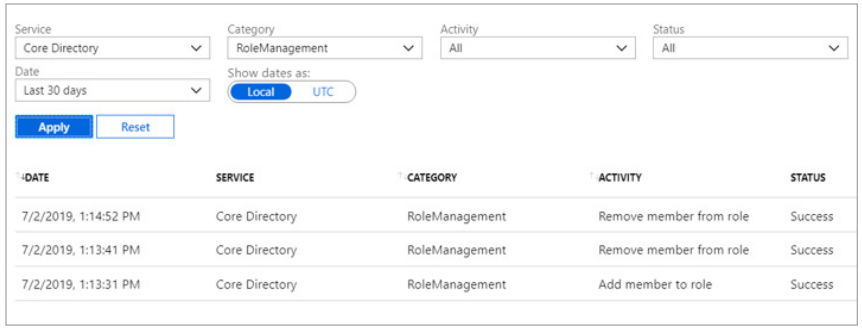


Figure 2 : Recherche sur les rôles dans le portail Azure

Une autre option consiste à exporter et analyser les résultats sous forme de feuille de calcul Microsoft Excel. Cela exige d'être non seulement abonné à Office 365, mais aussi à Azure.

TROUVER DES RÔLES DANS LE LOG D'AUDIT UNIFIÉ

Les informations peuvent aussi être recueillies au moyen d'une recherche dans le log d'audit unifié via le Centre de sécurité et conformité Office 365. (Ces recherches sont effectuées dans les logs d'Azure AD, ainsi que dans les logs de tous les outils Office 365, comme nous l'avons expliqué précédemment. De telles recherches peuvent être plus longues qu'avec le seul log d'audit Azure.)

Ces recherches renvoient toutes les activités individuelles liées à l'administration des rôles dans une plage de dates donnée (voir Figure 3), ce qui est un avantage par rapport aux recherches dans le log d'audit Azure.

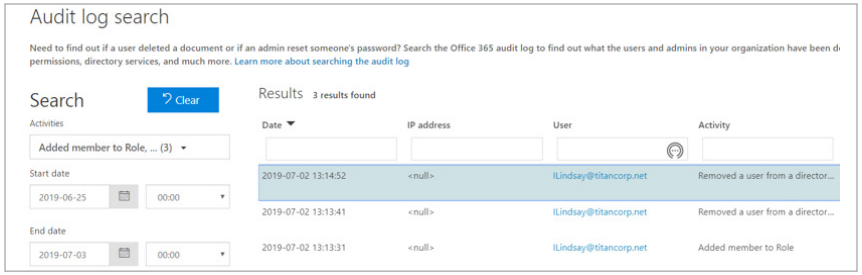


Figure 3 : Recherche dans le log d'audit unifié

Ici, toutefois, le détail de l'audit complet se trouve dans un fichier JSON imbriqué. Identifier le rôle modifié implique donc de consulter tous les détails. Il est possible d'exporter les données vers un outil comme Excel, mais comme le montre la colonne AuditData dans la Figure 4, le format JSON ne permet pas de filtrer facilement les rôles modifiés.

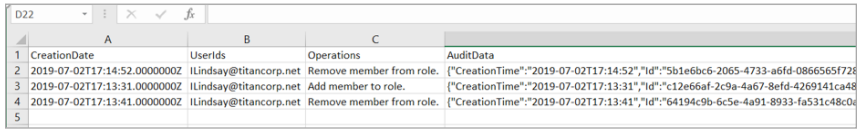


Figure 4 : Résultats de la recherche affichés dans Microsoft Excel

Quest

2. Modifications apportées aux groupes

Les groupes dans AD ont longtemps été indispensables pour octroyer l'accès aux ressources. C'est encore vrai dans le Cloud, avec quelques complications.

- Azure autorise davantage de types de groupes. Par exemple, les utilisateurs peuvent créer des groupes depuis des applications comme Outlook et Teams.
- Les groupes Office 365, tout comme ceux créés depuis Teams, génèrent d'autres ressources Azure pour prendre en charge l'application.[3]
- Azure AD B2B permet de créer facilement des groupes en vue de collaborer avec les clients et les fournisseurs. Mais cela s'accompagne aussi du risque de voir un utilisateur accorder un accès fortuit à un tiers.

Azure AD B2B permet de créer facilement des groupes en vue de collaborer avec les clients et les fournisseurs. Mais cela s'accompagne aussi du risque de voir un utilisateur accorder un accès fortuit à un tiers.

3 Pour plus d'informations, consultez l'e-book « Frequently Asked Questions: Office 365 Groups » (Forum aux questions : les groupes Office 365) https://www.quest.com/whitepaper/frequently-asked-questions-office-365-groups8134485/

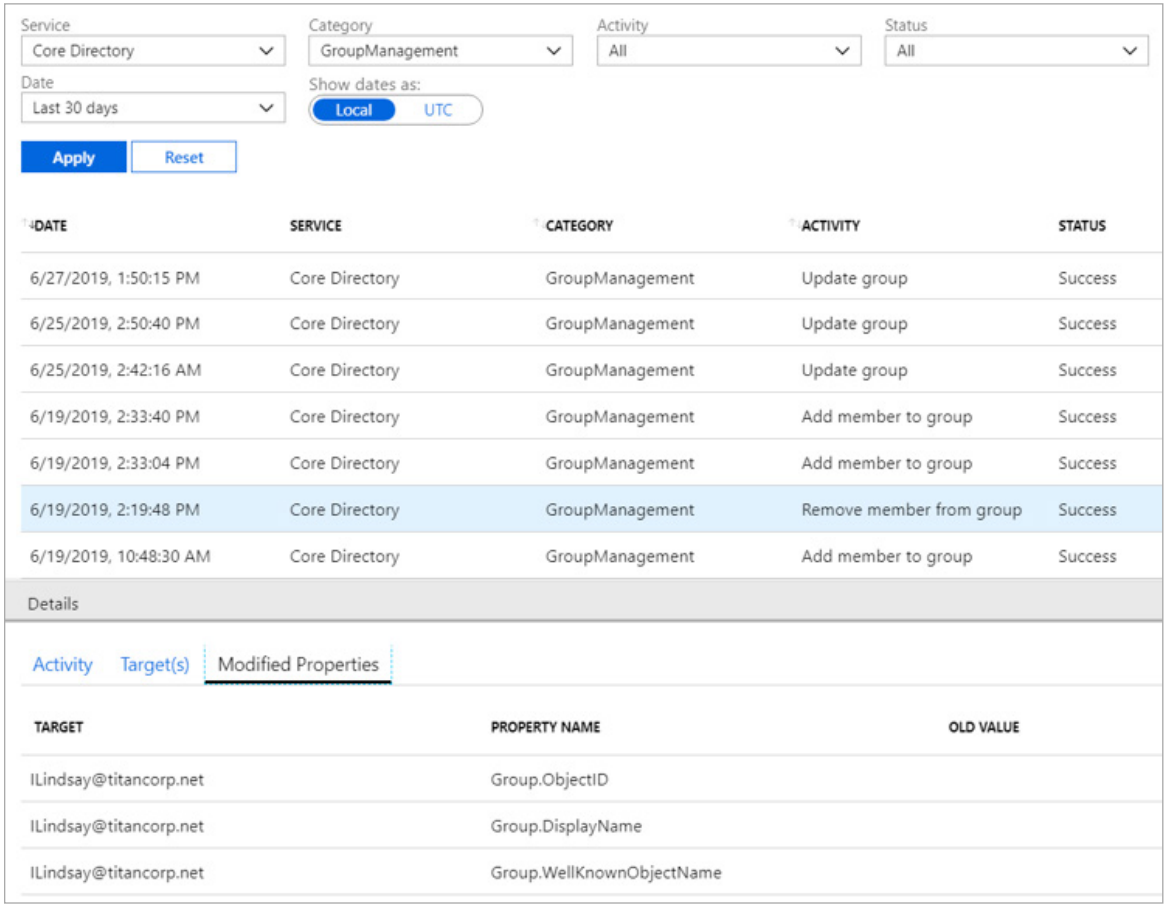


Figure 4 : Recherche sur des groupes dans le portail Azure

TROUVER DES GROUPES DANS LE LOG D'AUDIT AZURE

Tout comme pour les changements apportés aux rôles, le portail Azure est la première étape logique pour suivre les groupes. Dans la section **Logs d'audit** sous Azure Active Directory, une recherche sur le service **Core Directory** et la catégorie **GroupManagement** renvoie toutes les modifications apportées dans le locataire (haut de la Figure 4). Là encore, il n'est pas possible de rechercher directement les groupes dits importants. Qui plus est, le groupe modifié n'est pas initialement affiché. Les administrateurs doivent donc examiner dans le détail l'événement d'audit dans l'onglet Propriétés modifiées (bas de la Figure 4) pour trouver le groupe modifié.

Une autre option consiste à exporter et analyser les résultats dans une feuille de calcul Microsoft Excel, ce qui exige d'avoir souscrit un abonnement non seulement à Office 365, mais aussi à Azure.

Quest

TROUVER DES GROUPES DANS LE LOG D'AUDIT UNIFIÉ

Tout comme pour les modifications apportées aux rôles, les informations sur les modifications apportées aux groupes peuvent être recueillies dans le Centre de sécurité et conformité Office 365 (voir Figure 2) à partir d'une recherche dans le log d'audit sur toutes les **activités d'administration du groupe Azure AD**. Une recherche lancée sur les filtres **Membre ajouté au groupe** et **Membre supprimé du groupe** (voir Figure 5) affiche les changements d'appartenance.

Mais cette procédure ne permet toujours pas les recherches directes sur seulement quelques groupes. Vous devez rechercher les modifications apportées à tous les groupes, puis examiner les données. Et une fois encore, le détail de l'audit complet se trouve dans un fichier JSON imbriqué. Identifier le groupe modifié implique donc de consulter tous les détails. Il est possible d'exporter les données vers un outil comme Excel, mais le format JSON ne permet pas de filtrer facilement les groupes modifiés.

Figure 5 : Modification des propriétés dans le log d'audit unifié

Quest

3. Modifications apportées aux applications

Azure AD autorise l'installation simplifiée de nombreuses applications SaaS ainsi que l'accès à des applications locales.

Si les applications SaaS ne sont pas difficiles à configurer, elles peuvent facilement devenir inutilisables si les modifications ne sont pas effectuées correctement. Qui plus est, les modifications non documentées entraînent une perte de temps, de productivité et de rentabilité avant que les problèmes soient résolus. C'est pourquoi être en mesure de suivre les modifications apportées aux applications est un impératif commercial.

> Être en mesure de suivre les modifications apportées aux applications est un impératif commercial.

TROUVER DES MODIFICATIONS APPORTÉES AUX APPLICATIONS DANS LE LOG D'AUDIT AZURE

Dans le portail Azure, la première étape pour trouver les modifications apportées à une application donnée se trouve sous Azure Active Directory dans la section **Logs d'audit** de l'application en question. Le problème avec cette méthode est qu'elle nécessite un grand nombre d'explorations manuelles et répétitives pour trouver les modifications.

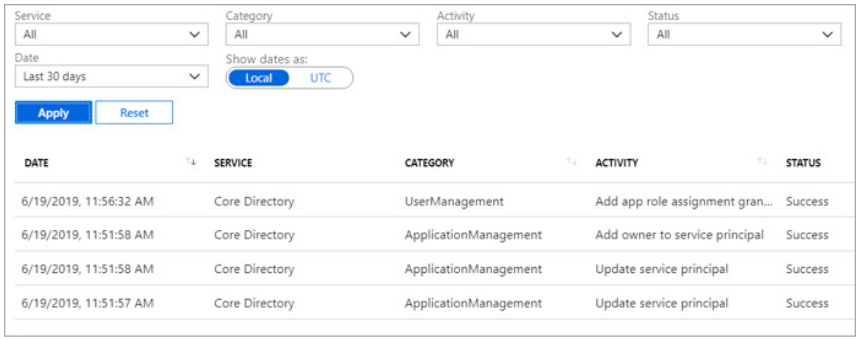


Figure 6 : Modifications apportées à l'application dans le log d'audit Azure

Comme le montre la colonne Catégorie de la Figure 6, les événements d'audit proviennent des catégories **ApplicationManagement** et **UserManagement**.

L'exploration de la catégorie **ApplicationManagement** produit la liste présentée en Figure 7.

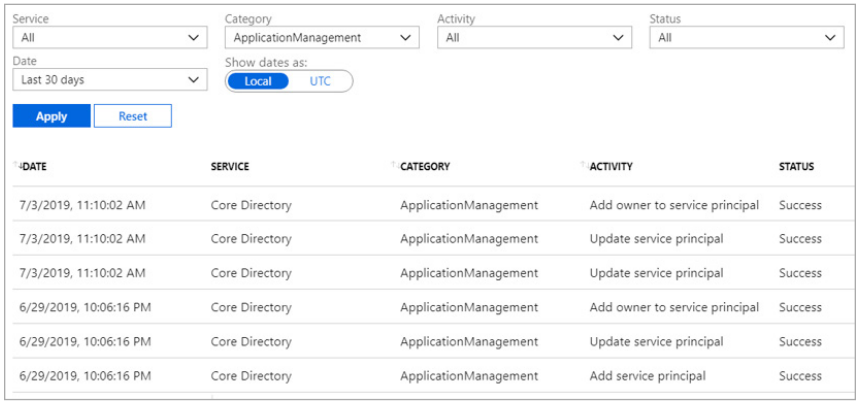


Figure 7 : Recherche sur la catégorie ApplicationManagement

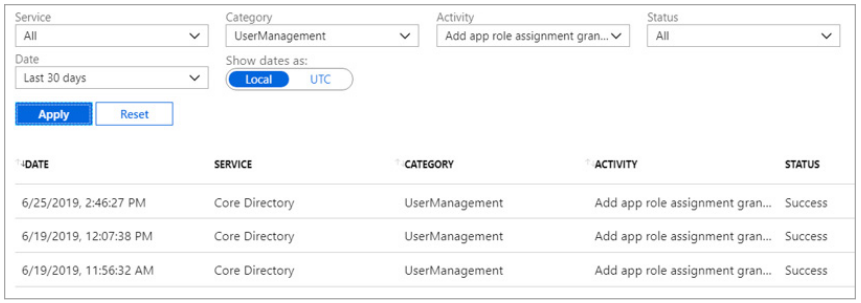


Figure 8 : Recherche sur la catégorie UserManagement

Pour explorer les modifications apportées à une application liées à la catégorie **UserManagement**, il est nécessaire de basculer vers cette catégorie, puis de sélectionner cinq activités différentes dans la liste déroulante **Activité** :

- Ajouter un octroi d'attribution de rôle pour l'application à l'utilisateur (voir Figure 8)
- Créer un mot de passe pour l'application pour l'utilisateur
- Supprimer un mot de passe pour l'application pour l'utilisateur
- Supprimer l'attribution de rôle pour l'application de l'utilisateur
- Examiner l'affectation d'application

Il n'existe donc aucun moyen facile de rechercher toutes les modifications apportées à une application ou de générer une liste contenant celles que vous souhaitez.

Quest

4. Création de ressources

Presque chaque migration vers le Cloud entraîne la création de ressources, dont certaines (comme un site Microsoft Teams) créent leur propre ensemble de ressources, comme des groupes Office 365 et des ressources SharePoint. Parvenir à suivre le type et le nombre de ressources ainsi créées aidera les administrateurs à réduire la charge onéreuse et chronophage que représente leur gestion.

TROUVER DES RESSOURCES CRÉÉES DANS LE LOG D'AUDIT AZURE

Tenez compte des ressources associées à la création des utilisateurs et des groupes. Le meilleur endroit pour découvrir les ressources consommées (ajouts, suppressions, mises à jour, changements de licences, attributions de rôle dans une application) est le log d'audit Azure Active Directory sur le portail Azure.

Malheureusement, il n'est possible de rechercher qu'une seule Catégorie à la fois (**UserManagement** [voir Figure 9], puis **GroupManagement**). Les administrateurs sont donc contraints d'exécuter plusieurs requêtes pour réunir toutes les informations.

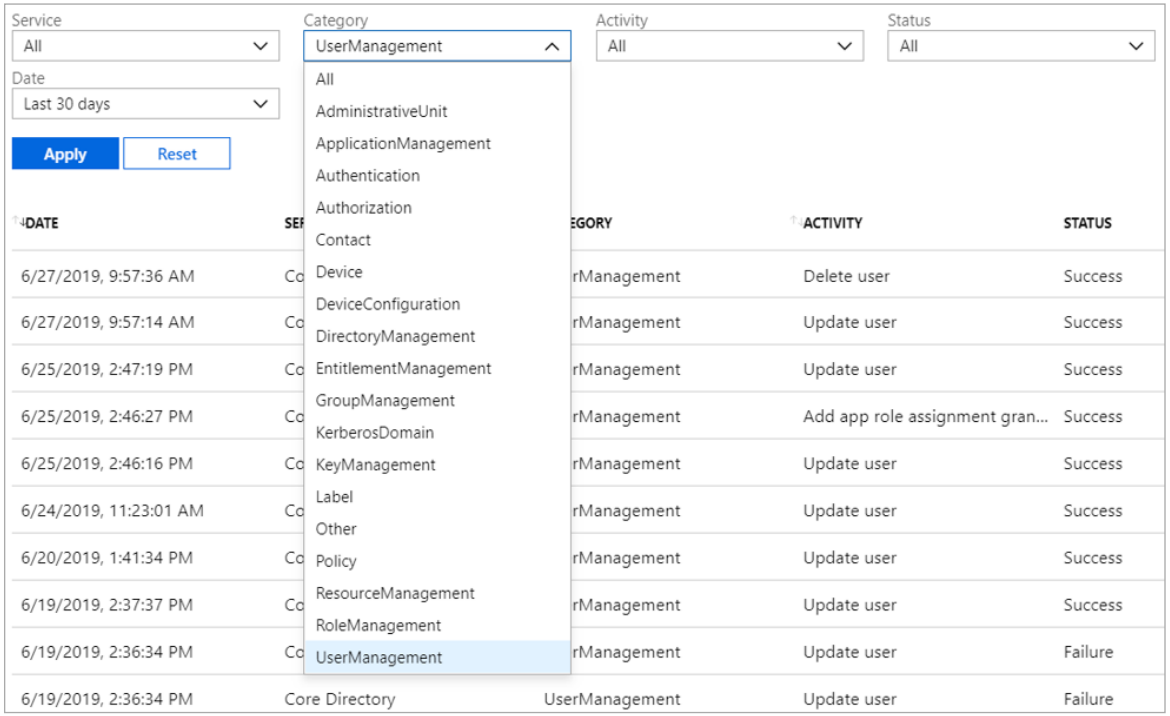


Figure 9 : Ressources créées répertoriées dans le log d'audit Azure

Parvenir à suivre le type et le nombre de ressources ainsi créées aidera les administrateurs à réduire la charge onéreuse et chronophage que représente leur gestion.

Quest

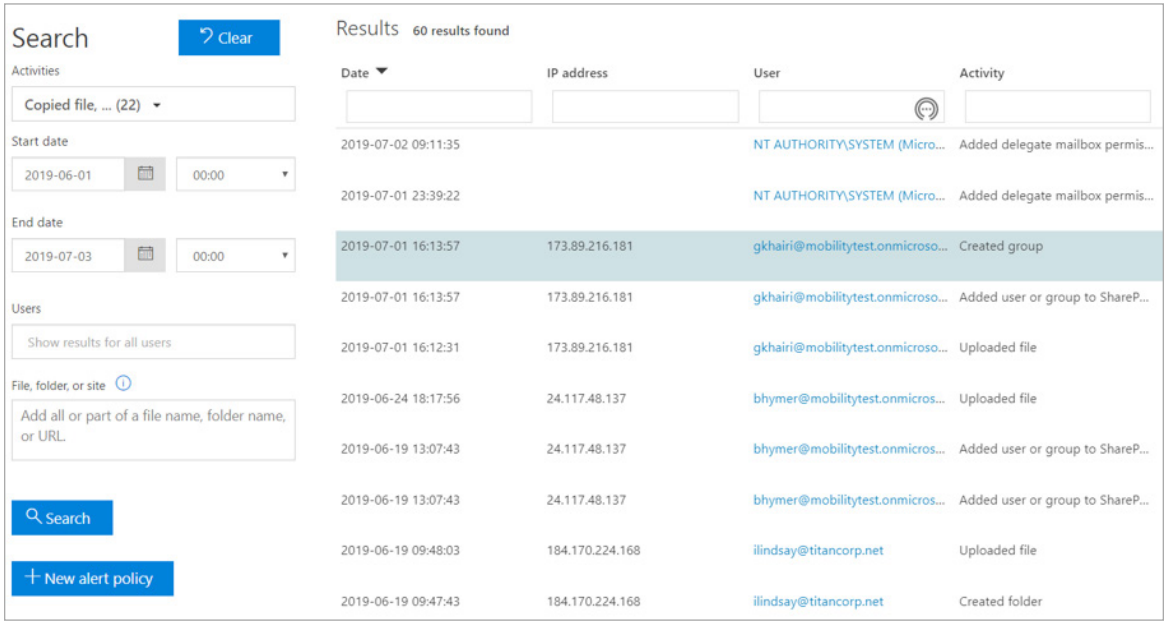


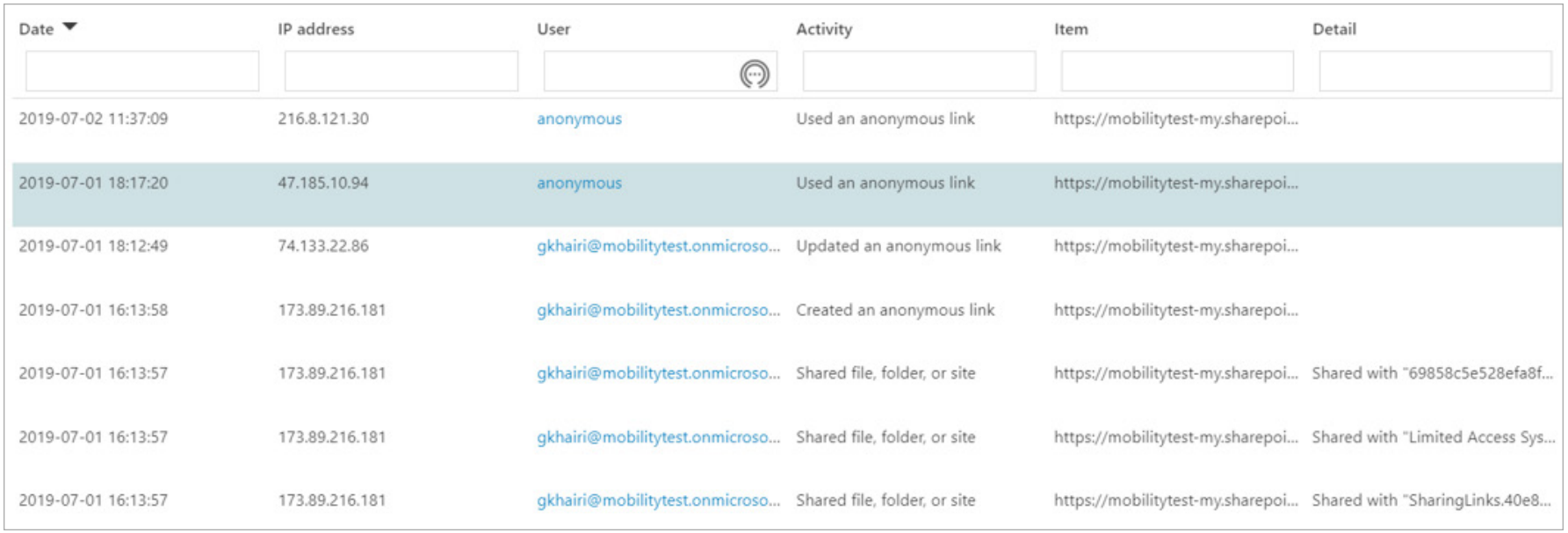
Figure 10 : Ressources créées répertoriées dans le log d'audit unifié

TROUVER DES RESSOURCES CRÉÉES DANS LE LOG D'AUDIT UNIFIÉ

La recherche dans le log d'audit dans le portail Centre de sécurité et conformité Office 365 (voir Figure 10) permet d'afficher plusieurs ressources :

- Fichiers : copiés, déplacés, chargés, renommés, restaurés
- Dossiers : créés, renommés, déplacés, restaurés
- Sites SharePoint : liste créée, élément de liste créée
- Autorisations du site : administrateur de collection de site ajouté, utilisateur ou groupe ajouté à un groupe SharePoint, groupe créé
- Exchange : élément de boîte aux lettres créé, autorisation de boîte aux lettres ajoutée
- Sway : Sway créé
- Teams : équipe créée, onglet ajouté, connecteur ajouté, canal ajouté, membres ajoutés, robot ajouté

Plusieurs requêtes sont nécessaires pour avoir une vision d'ensemble de ces ressources. Et, comme avec n'importe quelle autre recherche dans les événements d'audit Office 365, les détails seront consignés dans le fichier JSON imbriqué, ce qui les rend moins accessibles que les résultats d'une requête simple.



Date	IP address	User	Activity	Item	Detail
2019-07-02 11:37:09	216.8.121.30	anonymous	Used an anonymous link	https://mobilitytest-my.sharepoi...	
2019-07-01 18:17:20	47.185.10.94	anonymous	Used an anonymous link	https://mobilitytest-my.sharepoi...	
2019-07-01 18:12:49	74.133.22.86	gkhairi@mobilitytest.onmicroso...	Updated an anonymous link	https://mobilitytest-my.sharepoi...	
2019-07-01 16:13:58	173.89.216.181	gkhairi@mobilitytest.onmicroso...	Created an anonymous link	https://mobilitytest-my.sharepoi...	
2019-07-01 16:13:57	173.89.216.181	gkhairi@mobilitytest.onmicroso...	Shared file, folder, or site	https://mobilitytest-my.sharepoi...	Shared with "69858c5e528efa8f...
2019-07-01 16:13:57	173.89.216.181	gkhairi@mobilitytest.onmicroso...	Shared file, folder, or site	https://mobilitytest-my.sharepoi...	Shared with "Limited Access Sys...
2019-07-01 16:13:57	173.89.216.181	gkhairi@mobilitytest.onmicroso...	Shared file, folder, or site	https://mobilitytest-my.sharepoi...	Shared with "SharingLinks.40e8...

Figure 11 : Partage d'activité répertorié dans le log d'audit unifié

5 et 6. Partages de fichiers importants et de données anonymes

La migration vers SharePoint Online et OneDrive Entreprise introduit de nouveaux types de risques, en particulier autour du partage de données. Comme nous l'avons indiqué précédemment, les utilisateurs peuvent accidentellement partager des données sensibles en incluant un utilisateur B2B d'une autre entreprise sans s'en rendre compte. Par exemple, un utilisateur non autorisé qui obtient un lien de partage des données sur OneDrive peut accéder au fichier de manière anonyme.

L'inconvénient avec la généralisation du partage est l'augmentation des risques. Pour le service informatique, être en mesure de générer

Un utilisateur non autorisé qui obtient un lien de partage des données sur OneDrive peut accéder au fichier de manière anonyme.

des rapports Azure AD sur le partage de données devient encore plus important avec la migration dans le Cloud des entreprises. Celles-ci ont d'excellentes raisons de bloquer ou de contrôler étroitement le partage de certains types de fichiers.

TROUVER DES DEMANDES D'ACCÈS ET DE PARTAGE DANS LE LOG D'AUDIT UNIFIÉ

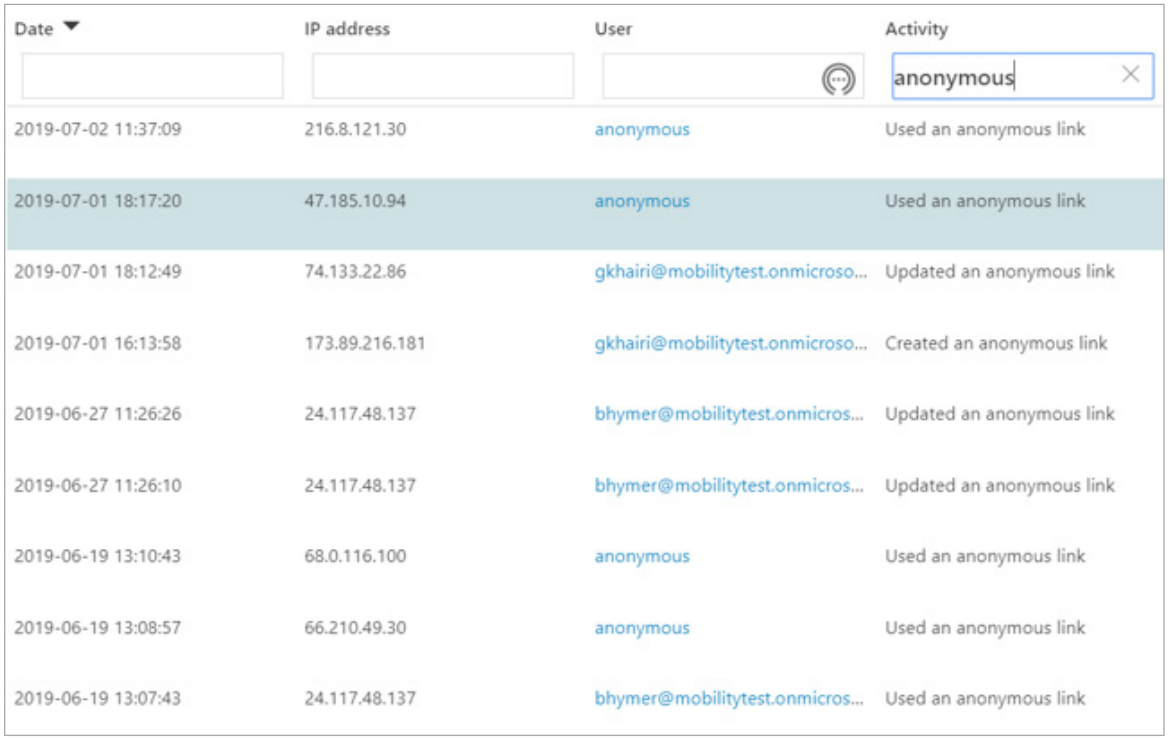
La recherche dans le log d'audit dans le Centre de sécurité et conformité Office 365 renvoie des informations sur les fichiers, dossiers et sites partagés. La Figure 11 décrit les résultats d'une recherche sur les **Activités de demande d'accès et de partage**.

Le problème est que cette requête renvoie toutes les données de ces activités. Une requête plus efficace et utile limiterait les résultats aux extensions des fichiers partagés, par exemple CER, DER, CRT, PEM, PFX, P7B, P7C, P12, PPK, PUB, SPC, STL, CRL, SSH, EVT, EXE, BAT, PIF. Ou elle limiterait les résultats aux extensions de fichier Microsoft Office, à savoir PPT, PPTX, XLS, XLSX, DOC, DOCX, etc. La recherche dans le log d'audit ne le permet pas.

Une autre option consiste à exporter le sur-ensemble de données depuis le champ **AuditData** du log d'audit unifié sous forme de feuille de calcul. Néanmoins, certaines manipulations de données restent nécessaires pour affiner le résultat aux seuls partages en question.

Les requêtes concernant les partages anonymes, qui nous intéressent tout particulièrement, sont plus faciles. Il suffit en effet de saisir le mot « anonyme » dans le filtre Activité, comme le montre la Figure 12.

Le filtre Utilisateur défini sur anonyme renvoie tous les fichiers qui ont été consultés de manière anonyme. L'application de filtre sur les colonnes **UserIds** ou **Operations** dans les événements d'audit exportés renvoie des résultats similaires.



Date	IP address	User	Activity
			anonymous
2019-07-02 11:37:09	216.8.121.30	anonymous	Used an anonymous link
2019-07-01 18:17:20	47.185.10.94	anonymous	Used an anonymous link
2019-07-01 18:12:49	74.133.22.86	gkhairi@mobilitytest.onmicroso...	Updated an anonymous link
2019-07-01 16:13:58	173.89.216.181	gkhairi@mobilitytest.onmicroso...	Created an anonymous link
2019-06-27 11:26:26	24.117.48.137	bhymer@mobilitytest.onmicros...	Updated an anonymous link
2019-06-27 11:26:10	24.117.48.137	bhymer@mobilitytest.onmicros...	Updated an anonymous link
2019-06-19 13:10:43	68.0.116.100	anonymous	Used an anonymous link
2019-06-19 13:08:57	66.210.49.30	anonymous	Used an anonymous link
2019-06-19 13:07:43	24.117.48.137	bhymer@mobilitytest.onmicros...	Used an anonymous link

Figure 12 : Résultats de la recherche sur une activité de partage anonyme

7. E-mails, transfert des messages entrants

En soit, le transfert d'e-mails entrants à d'autres destinataires n'est ni bien ni mal. Il peut arriver que le destinataire d'un message ait besoin de partager des informations contenues dans un message avec des fournisseurs ou des clients externes. Des consultants et prestataires contractuels intervenant localement peuvent préférer transférer des messages et consolider tous leurs e-mails dans un seul et même compte. Les utilisateurs peuvent transférer les messages manuellement et un transfert automatique peut être configuré sur une boîte aux lettres par un utilisateur (via ForwardSMTP) ou un administrateur (via ForwardAlias).

Un transfert automatique peut être parfaitement inoffensif, mais un administrateur avisé gardera un œil sur les modifications qui impliquent un transfert d'e-mail afin de contrer toute modification laissant supposer qu'il s'agit d'une activité malveillante.

Malheureusement, les logs d'audit dans Azure Active Directory et Office 365 ne permettent pas de rechercher directement les modifications liées au transfert d'e-mails.

Malheureusement, les logs d'audit dans Azure Active Directory et Office 365 ne permettent pas de rechercher directement ces modifications. Au contraire, ils exigent d'exporter l'intégralité du log dans Exchange Online, puis de rechercher les événements d'audit exportés avec **{"name":"DeliverToMailboxAndForward","value":"True"}** dans le champ Paramètres du détail de l'audit pour retourner les événements souhaités.

Quest

8. E-mail, activité non-propriétaire

L'activité de courrier électronique non-propriétaire est courante dans les grandes entreprises, avec les assistants administratifs qui ont accès aux comptes de courrier des cadres qu'ils assistent, ou des employés qui partagent une même boîte aux lettres. Si un compte non-propriétaire est compromis, un cybercriminel peut avoir accès à des informations sensibles.

Dans le contexte de l'administration d'Exchange Online, les administrateurs peuvent réaliser presque toutes les activités avec leurs droits, notamment s'octroyer l'accès pour consulter les boîtes aux lettres d'autres cadres. Si chaque organisation fait confiance à ses administrateurs pour gérer et mettre à jour les systèmes, elle doit faire attention aux activités malveillantes.

Les administrateurs peuvent réaliser presque toutes les activités avec leurs droits, notamment s'octroyer l'accès pour consulter les boîtes aux lettres d'autres cadres.

TROUVER UNE ACTIVITÉ DE COURRIER ÉLECTRONIQUE NON-PROPRIÉTAIRE DANS LE LOG D'AUDIT UNIFIÉ

Les informations sur l'activité non-propriétaire sont disponibles uniquement dans le log d'audit unifié, comme le montre la Figure 13. Pour rechercher les types d'activités que la plupart des utilisateurs non-propriétaires effectuent sur une boîte aux lettres, il convient d'inclure :

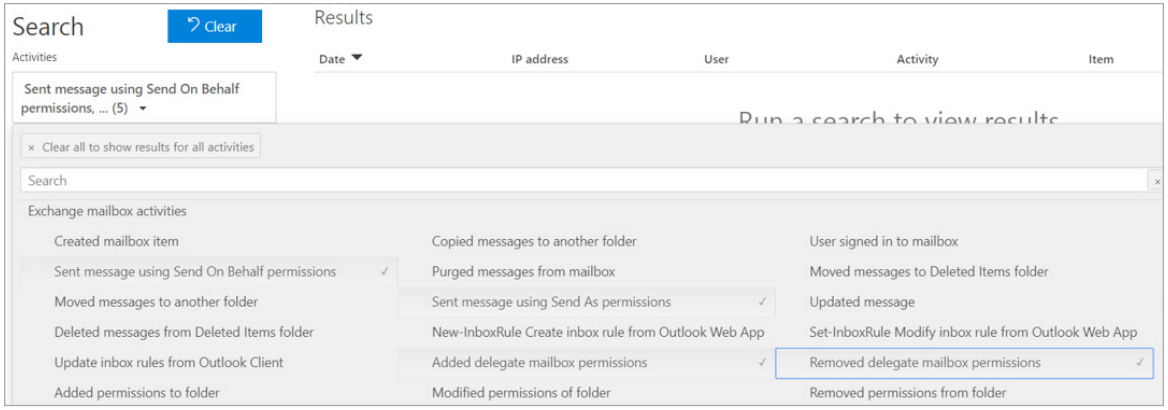


Figure 13 : Activité de courrier électronique non-propriétaire dans le log d'audit unifié

Figure 14 : Détail de la colonne AuditData

- Message envoyé à l'aide d'une autorisation Envoyer de la part de
- Utilisateur ajouté ou supprimé avec un accès délégué au calendrier/dossier
- Message envoyé à l'aide d'une autorisation Envoyer en tant que
- Autorisation de boîte aux lettres déléguée ajoutée
- Autorisation de boîte aux lettres déléguée supprimée

Il convient toutefois de noter que des activités comme l'ajout, la suppression ou le déplacement de dossiers et de messages ne sont pas couvertes, pas plus que les modifications apportées à certaines autorisations, pour ne citer que quelques exemples. Lancer des requêtes pour toutes les **activités de la boîte aux lettres** et exporter les résultats dans une feuille de calcul est le seul moyen de procéder à une recherche exhaustive.

Mais l'étape suivante, à savoir trouver les événements d'audit lorsque les catégories **LogonUserSid** et **MailboxOwnerMasterSid** ne correspondent pas, est une tâche ardue, car les informations sont imbriquées dans la colonne **AuditData** avec le reste des informations sur l'événement (voir Figure 14).[4]

4 Consultez également le livre blanc « Auditing Privileged Operations and Mailbox Access in Office 365 Exchange Online » (Audit des opérations à privilèges et des accès aux boîtes aux lettres), https://www.quest.com/docs/auditing-privileged-operations-and-mailbox-access-in-office-365-white-paper-24932.pdf

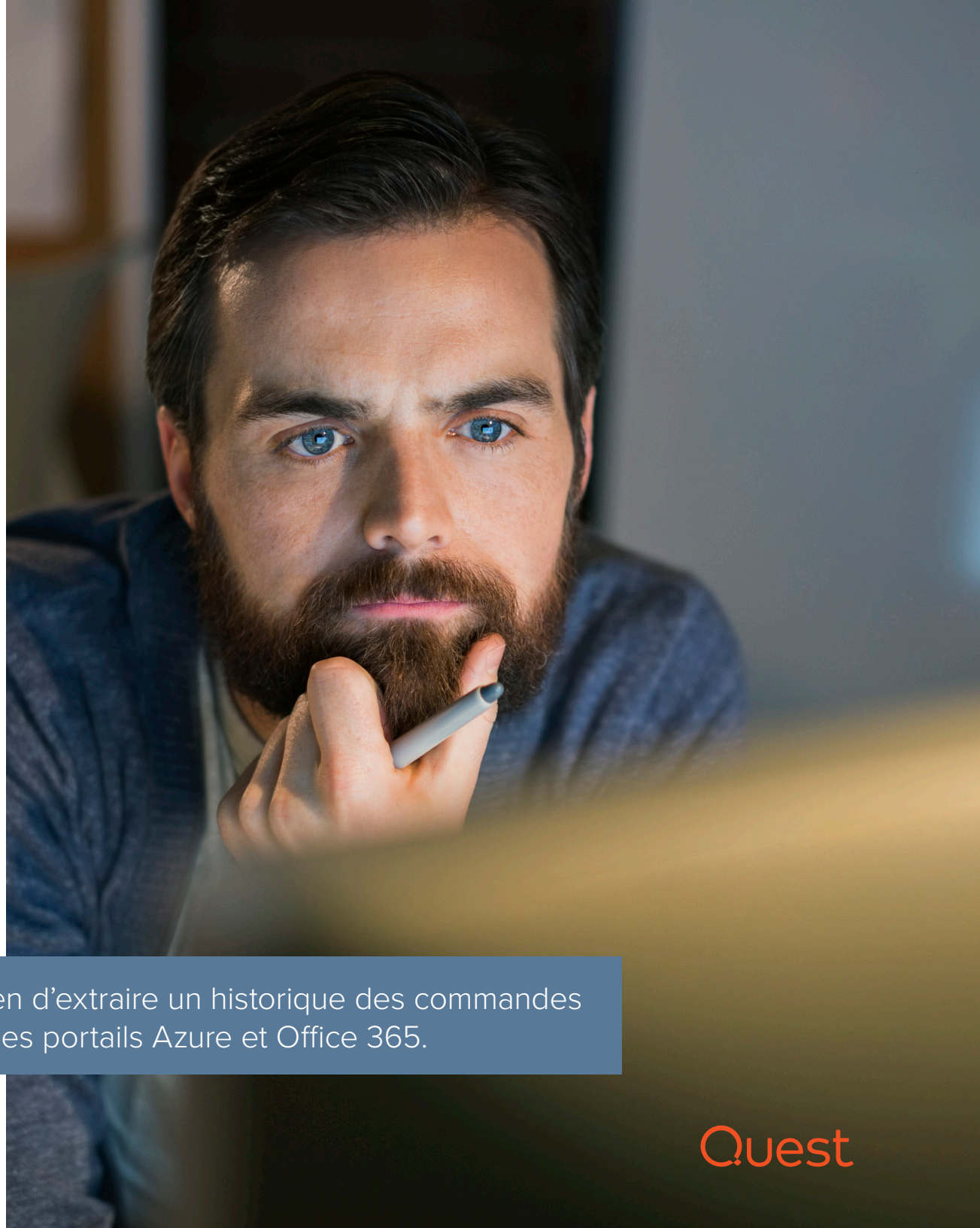
Quest

9. Historique des commandes d'administration

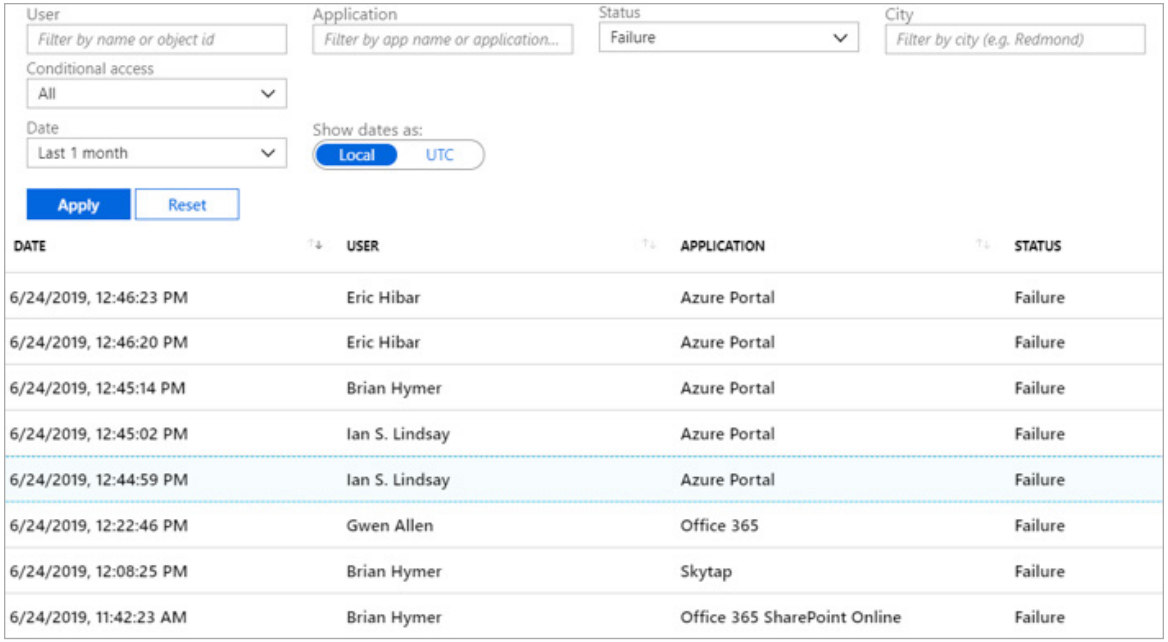
Microsoft propose des outils d'administration comme Microsoft Management Console (MMC) pour la gestion locale et des portails Web pour la gestion dans le Cloud. Microsoft met de plus en plus en avant sa solution PowerShell comme principale méthode d'administration. Dans les faits, de nombreuses instances MMC exécutent des commandes PowerShell d'après des événements passés à partir de l'interface utilisateur. Exchange en est un parfait exemple.

Toutefois, aussi important qu'il puisse être de s'assurer que les commandes sont correctement exécutées, il est pratiquement impossible de suivre l'historique des commandes. Par exemple, il est bon de suivre les événements d'autorisation de l'application et toutes les modifications apportées aux stratégies d'accès conditionnel dans Azure AD. Un accès en lecture/écriture à des objets octroyé à la mauvaise application peut être source de vulnérabilité.

Le problème est qu'il n'existe actuellement aucun moyen d'extraire un historique des commandes d'administration exécutées depuis les portails Azure et Office 365.



Il n'existe actuellement aucun moyen d'extraire un historique des commandes d'administration exécutées depuis les portails Azure et Office 365.



DATE	USER	APPLICATION	STATUS
6/24/2019, 12:46:23 PM	Eric Hibar	Azure Portal	Failure
6/24/2019, 12:46:20 PM	Eric Hibar	Azure Portal	Failure
6/24/2019, 12:45:14 PM	Brian Hymer	Azure Portal	Failure
6/24/2019, 12:45:02 PM	Ian S. Lindsay	Azure Portal	Failure
6/24/2019, 12:44:59 PM	Ian S. Lindsay	Azure Portal	Failure
6/24/2019, 12:22:46 PM	Gwen Allen	Office 365	Failure
6/24/2019, 12:08:25 PM	Brian Hymer	Skytap	Failure
6/24/2019, 11:42:23 AM	Brian Hymer	Office 365 SharePoint Online	Failure

Figure 15 : Recherche sur les échecs de connexion dans Azure AD

Des échecs répétés peuvent indiquer une activité malveillante, car des acteurs mal intentionnés essaient d'entrer les mots de passe d'utilisateur par force brute.

10. Échecs de connexion

Que ce soit localement ou dans le Cloud, le suivi des échecs de connexion fait partie du travail de l'administrateur. Les utilisateurs verrouillés hors de leur compte sont frustrés, car ils comprennent rarement pourquoi ou comment ils se retrouvent dans cette situation. Les connexions hybrides depuis Azure AD exacerbent encore le problème en ajoutant une autre source potentielle au verrouillage. Mais des échecs répétés peuvent indiquer une activité malveillante, car des acteurs mal intentionnés essaient d'entrer les mots de passe d'utilisateur par force brute.

Localement, les informations sur les événements d'échec de connexion sont conservées dans les logs de sécurité sur tous les contrôleurs de domaine. Dans le Cloud, ces informations se trouvent dans les événements d'audit de tous les locataires Azure. Comme le montre la Figure 15, une recherche sur un **Échec** dans l'écran **Connexions** sous **Surveillance** dans Azure AD pour chaque locataire renvoie les événements d'échec de connexion.

Toutefois, la collecte de tous les événements d'échec de connexion n'est que le début. La tâche suivante consiste à analyser toutes les informations pour établir des modèles, une tâche rendue compliquée par l'absence de détails dans les résultats de la recherche.

Quest

Conclusion : la solution On Demand Audit de Quest

Au vu des lacunes que montrent les outils natifs dans la génération de rapports Office 365 et Azure, que diriez-vous si vous pouviez éviter d'avancer à l'aveuglette ?

La suite Quest On Demand Audit Hybrid Suite pour Office 365 centralise l'affichage de l'activité des utilisateurs sur des environnements Microsoft hybrides. Elle expose toutes les modifications effectuées, que ce soit sur des instances AD ou Azure AD locales ou sur des charges de travail Office 365 comme Exchange Online, SharePoint Online et OneDrive Entreprise. Plutôt que de passer au peigne fin les pics partiels dans les logs d'audit, vous pouvez utiliser une recherche réactive sur des années de données pour enquêter et créer des rapports sur des événements depuis une fenêtre unique. Son intégration à la solution Power BI de Microsoft vous permet de générer des rapports via une visualisation interactive des données, comme le montre la Figure 16.

La suite On Demand Audit Hybrid Suite procure un accès granulaire et délégué qui permet aux utilisateurs d'obtenir les renseignements nécessaires sans avoir à modifier la configuration ou à paramétrer une nouvelle infrastructure. En quelques clics seulement, vous pouvez offrir à vos équipes de sécurité et de conformité, à vos ingénieurs du centre d'assistance, à vos responsables informatiques et même à vos auditeurs et partenaires externes exactement les rapports dont ils ont besoin, et rien de plus.

Pour en savoir plus, rendez-vous sur quest.com/on-demand.

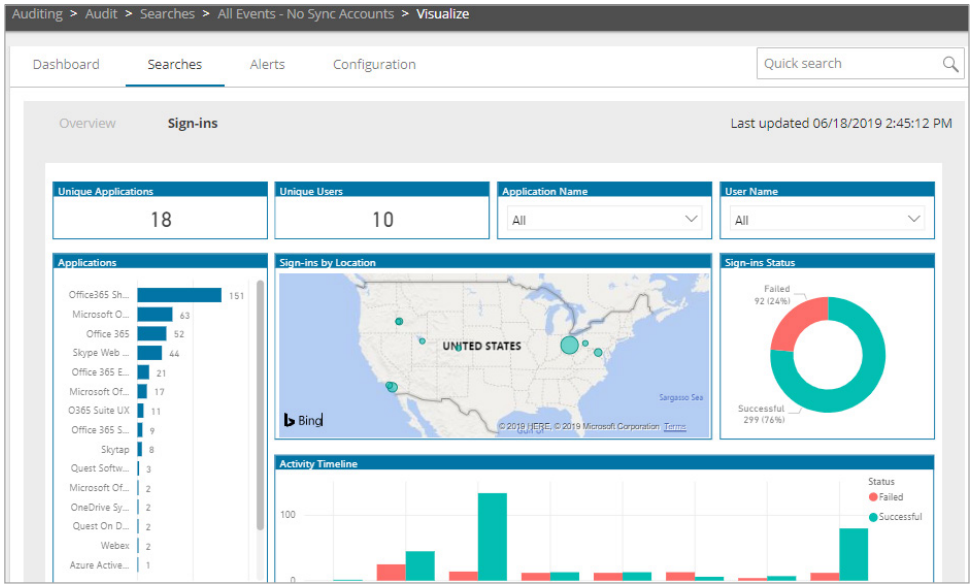


Figure 16 : On Demand Audit

La suite On Demand Audit Hybrid Suite procure un accès granulaire et délégué qui permet aux utilisateurs d'obtenir les renseignements nécessaires sans avoir à modifier la configuration ou à paramétrer une nouvelle infrastructure.

Quest

PROFIL DE QUEST

Quest fournit des solutions logicielles adaptées au monde de l'informatique d'entreprise en rapide évolution. Nous simplifions les défis associés à l'explosion des données, à l'expansion dans le Cloud, aux datacenters hybrides, aux menaces de sécurité et aux exigences de conformité. Nous fournissons des solutions à 130 000 entreprises dans 100 pays, dont 95 % des entreprises du classement Fortune 500 et 90 % des entreprises du classement Global 1000. Depuis 1987, nous développons une gamme de solutions qui couvre désormais la gestion des bases de données, la protection des données, la gestion des accès et des identités, la gestion des plateformes Microsoft et la gestion unifiée des terminaux. Avec Quest, les entreprises consacrent moins de temps à la gestion informatique et plus de temps à l'innovation. Pour en savoir plus, consultez le site www.quest.com.

En cas de questions sur l'utilisation de ce document, nous vous invitons à contacter :

www.quest.com/fr-fr/company/contact-us.aspx

Ebook-SecurityEventsToMonitor-US-GM-FR-WL-40070

© 2019 Quest Software Inc. TOUS DROITS RÉSERVÉS.

Ce guide contient des informations propriétaires protégées par des droits d'auteur. Les logiciels présentés dans ce guide sont concédés sous licence logicielle ou dans le cadre d'un accord de confidentialité. Ces logiciels peuvent être utilisés ou copiés conformément aux dispositions de l'accord applicable. Toute reproduction ou transmission de ce guide sous quelque forme ou par quelque moyen que ce soit (électronique ou mécanique, notamment par photocopie ou par enregistrement), à des fins autres que l'usage personnel par l'acheteur, est interdite sans l'autorisation écrite préalable de Quest Software Inc.

Les informations fournies dans ce document sont liées aux produits Quest Software. Aucune licence de droit de propriété intellectuelle, expresse ou implicite, par préclusion ou autre, n'est accordée par le présent document ou en relation avec la vente de produits Quest Software. SAUF STIPULATION EXPRESSE DANS LES CONDITIONS GÉNÉRALES MENTIONNÉES DANS LE CONTRAT DE LICENCE DE CE PRODUIT, QUEST DÉCLINE TOUTE RESPONSABILITÉ QUELLE QU'ELLE SOIT ET N'ACCORDE AUCUNE GARANTIE EXPRESSE, IMPLICITE OU LÉGALE QUANT À SES PRODUITS, NOTAMMENT, MAIS SANS S'Y LIMITER, LA GARANTIE IMPLICITE DE QUALITÉ MARCHANDE, D'ADÉQUATION À UN USAGE PARTICULIER ET D'ABSENCE DE CONTREFAÇON. LA SOCIÉTÉ QUEST SOFTWARE NE PEUT EN AUCUN CAS ÊTRE TENUE RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, CONSÉCUTIFS, PUNITIFS, SPÉCIAUX OU FORTUITS (NOTAMMENT, MAIS SANS S'Y LIMITER, CEUX DÉCOULANT D'UNE PERTE DE BÉNÉFICES, D'UNE INTERRUPTION D'ACTIVITÉ OU D'UNE PERTE D'INFORMATIONS) ATTRIBUABLES À L'UTILISATION OU À L'IMPOSSIBILITÉ D'UTILISER LE PRÉSENT DOCUMENT, MÊME SI QUEST SOFTWARE A ÉTÉ AVERTIE DE L'ÉVENTUALITÉ DE TELS DOMMAGES. Quest Software ne se soumet à aucune déclaration ou garantie quant à l'exactitude ou l'exhaustivité du contenu du présent document et se réserve le droit de modifier les spécifications et les descriptions de produits à tout moment et sans préavis. Quest Software ne saurait s'engager à actualiser les informations contenues dans le présent document.

Brevets

Chez Quest Software, nous sommes fiers de notre technologie de pointe. Des brevets ou des brevets en attente peuvent s'appliquer à ce produit. Pour obtenir des informations récentes sur les brevets applicables à ce produit, veuillez consulter notre site Web à l'adresse suivante : www.quest.com/legal.

Marques

Quest et le logo Quest sont des marques et des marques déposées de Quest Software, Inc. Pour obtenir la liste complète des produits Quest, rendez-vous sur le site www.quest.com/legal/trademark-information.aspx. Toutes les autres marques commerciales sont la propriété de leurs détenteurs respectifs.

Quest