criminalistique

Data Infrastructure Insights

NetApp
February 11, 2026

Sommaire

criminalistique

Forensic - Toutes les activités

La page Toutes les activités vous aide à comprendre les actions effectuées sur les entités dans l'environnement Workload Security.

Examen de toutes les données d'activité

Cliquez sur **Forensics > Forensics d'activité** et cliquez sur l'onglet **Toutes les activités** pour accéder à la page Toutes les activités. Cette page fournit un aperçu des activités de votre locataire, en mettant en évidence les informations suivantes :

- Un graphique montrant *l'historique des activités* (basé sur la plage horaire globale sélectionnée)

  Vous pouvez zoomer sur le graphique en faisant glisser un rectangle dans le graphique. La page entière sera chargée pour afficher la plage horaire zoomée. Lors d'un zoom avant, un bouton s'affiche qui permet à l'utilisateur de dézoomer.

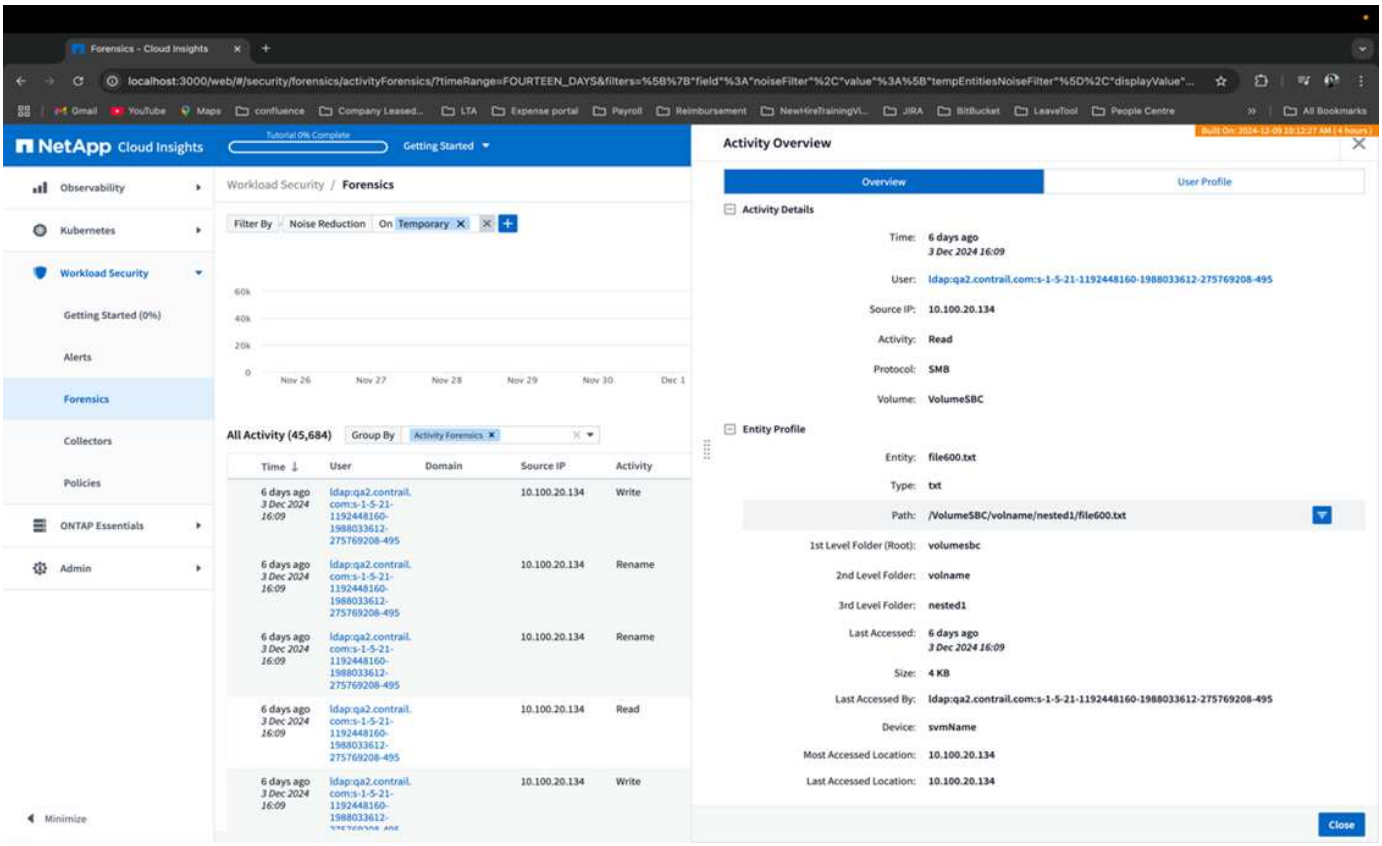
- Une liste des données *Toutes les activités*.
- Un groupe par liste déroulante offrira la possibilité de regrouper l'activité par utilisateurs, dossiers, type d'entité, etc.
- Un bouton de chemin commun sera disponible au-dessus du tableau, en cliquant dessus, nous pourrons accéder à un panneau coulissant avec les détails du chemin de l'entité.

Le tableau **Toutes les activités** affiche les informations suivantes. Notez que toutes ces colonnes ne sont pas affichées par défaut. Vous pouvez sélectionner les colonnes à afficher en cliquant sur l'icône « engrenage ».

- L'**heure** à laquelle une entité a été consultée, y compris l'année, le mois, le jour et l'heure du dernier accès.
- L'**utilisateur** qui a accédé à l'entité avec un lien vers le"Informations utilisateur" comme un panneau coulissant.
- L'**activité** effectuée par l'utilisateur. Les types pris en charge sont :
  - **Modifier la propriété du groupe** - La propriété du groupe du fichier ou du dossier est modifiée. Pour plus de détails sur la propriété du groupe, veuillez consulter"ce lien."
  - **Changer de propriétaire** - La propriété du fichier ou du dossier est transférée à un autre utilisateur.
  - **Modifier l'autorisation** - L'autorisation du fichier ou du dossier est modifiée.
  - **Créer** - Créer un fichier ou un dossier.
  - **Supprimer** - Supprimer le fichier ou le dossier. Si un dossier est supprimé, les événements *delete* sont obtenus pour tous les fichiers de ce dossier et de ses sous-dossiers.
  - **Lecture** - Le fichier est lu.
  - **Lire les métadonnées** - Uniquement lors de l'activation de l'option de surveillance des dossiers. Sera généré lors de l'ouverture d'un dossier sous Windows ou de l'exécution de « ls » dans un dossier sous Linux.
  - **Renommer** - Renommer le fichier ou le dossier.
  - **Écriture** - Les données sont écrites dans un fichier.

    - **Écrire des métadonnées** - Les métadonnées du fichier sont écrites, par exemple, l'autorisation est modifiée.
    - **Autre changement** - Tout autre événement non décrit ci-dessus. Tous les événements non mappés sont mappés au type d'activité « Autre changement ». Applicable aux fichiers et dossiers.
- Le **Chemin** est le chemin d'*entité*. Il doit s'agir soit du chemin d'entité exact (par exemple, "*/home/userX/nested1/nested2/abc.txt*") OU de la partie répertoire du chemin pour la recherche récursive (par exemple, "*/home/userX/nested1/nested2/*"). REMARQUE : les modèles de chemin d'expression régulière (par exemple, *nested*) ne sont PAS autorisés ici. Alternativement, des filtres de niveau de dossier de chemin individuel, comme mentionné ci-dessous, peuvent également être spécifiés pour le filtrage de chemin.
- Le **dossier de 1er niveau (racine)** est le répertoire racine du chemin d'entité en minuscules.
- Le **dossier de 2e niveau** est le répertoire de deuxième niveau du chemin d'entité en minuscules.
- Le **dossier de 3e niveau** est le répertoire de troisième niveau du chemin d'entité en minuscules.
- Le **dossier de 4e niveau** est le répertoire de quatrième niveau du chemin d'entité en minuscules.
- Le **Type d'entité**, y compris l'extension d'entité (c'est-à-dire de fichier) (.doc, .docx, .tmp, etc.).
- L'**Appareil** où résident les entités.
- Le **Protocole** utilisé pour récupérer les événements.
- Le **chemin d'origine** utilisé pour les événements de renommage lorsque le fichier d'origine a été renommé. Cette colonne n'est pas visible dans le tableau par défaut. Utilisez le sélecteur de colonne pour ajouter cette colonne au tableau.
- Le **Volume** où résident les entités. Cette colonne n'est pas visible dans le tableau par défaut. Utilisez le sélecteur de colonne pour ajouter cette colonne au tableau.
- Le **Nom de l'entité** est le dernier composant du chemin de l'entité ; pour le type d'entité tel que fichier, il s'agit du nom du fichier.

La sélection d'une ligne de tableau ouvre un panneau coulissant avec le profil utilisateur dans un onglet et l'aperçu de l'activité et de l'entité dans un autre onglet.



La méthode *Group by* par défaut est *Activity forensics*. Si vous sélectionnez une méthode *Group By* différente (par exemple, Type d'entité), la table *Group By* de l'entité s'affiche. Si aucune sélection n'est effectuée, *Grouper par* **tout** est affiché.

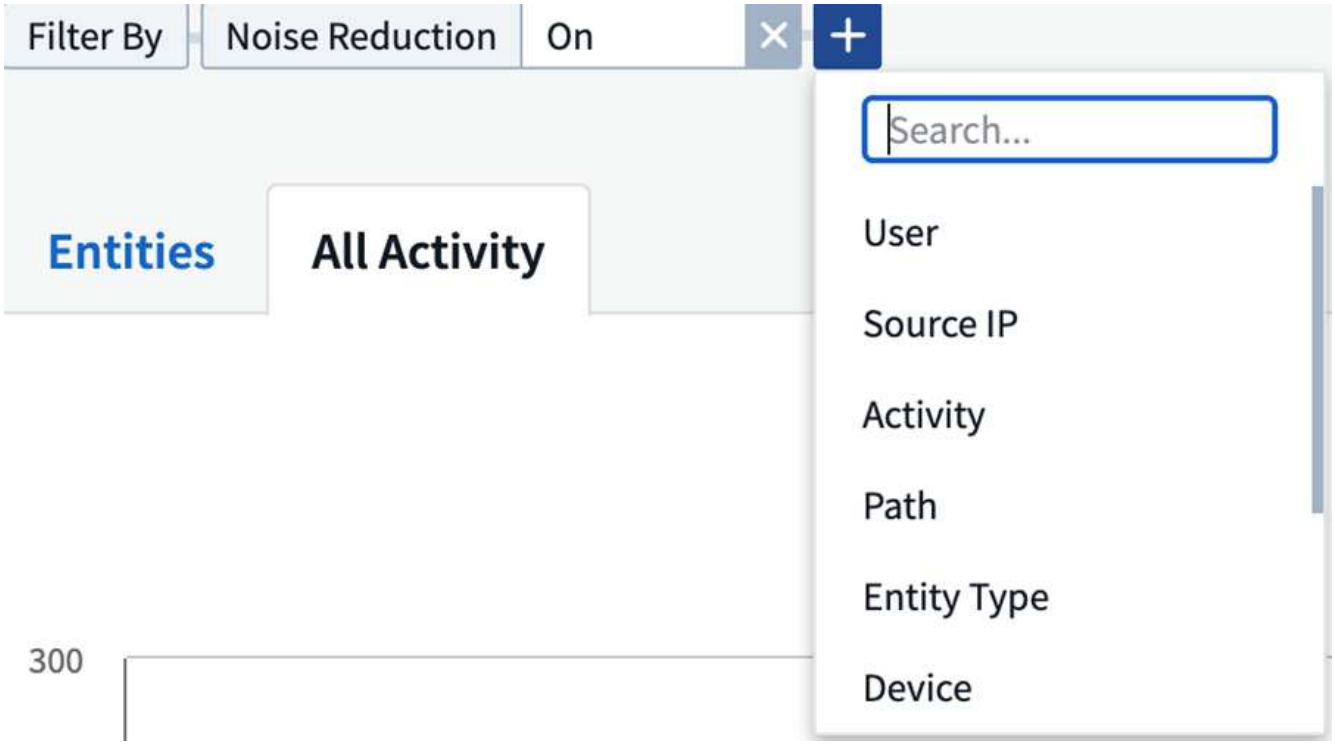
- Le nombre d'activités est affiché sous forme de lien hypertexte ; la sélection de cette option ajoutera le groupe sélectionné en tant que filtre. Le tableau d'activité sera mis à jour en fonction de ce filtre.
- Notez que si vous modifiez le filtre, modifiez la plage horaire ou actualisez l'écran, vous ne pourrez pas revenir aux résultats filtrés sans redéfinir le filtre.
- Veuillez noter que lorsque le nom de l'entité est sélectionné comme filtre, la liste déroulante Grouper par sera désactivée ; de plus, lorsque l'utilisateur est déjà sur l'écran Grouper par, le nom de l'entité comme filtre sera désactivé.

Filtrage des données d'historique des activités médico-légales

Il existe deux méthodes que vous pouvez utiliser pour filtrer les données.

- Le filtre peut être ajouté à partir du panneau coulissant. La valeur est ajoutée aux filtres appropriés dans la liste supérieure *Filtrer par*.
- Filtrer les données en saisissant dans le champ *Filtrer par* :

  Sélectionnez le filtre approprié dans le widget supérieur « Filtrer par » en cliquant sur le bouton **[+]** :



Entrez le texte de recherche

Appuyez sur Entrée ou cliquez en dehors de la zone de filtre pour appliquer le filtre.

Vous pouvez filtrer les données d'activité médico-légale selon les champs suivants :

- Le type **Activité**.
- **Protocole** pour récupérer les activités spécifiques au protocole.
- **Nom d'utilisateur** de l'utilisateur effectuant l'activité. Vous devez fournir le nom d'utilisateur exact à filtrer. La recherche avec un nom d'utilisateur partiel ou un nom d'utilisateur partiel préfixé ou suffixé par « * » ne fonctionnera pas.
- **Réduction du bruit** pour filtrer les fichiers créés au cours des 2 dernières heures par l'utilisateur. Il est également utilisé pour filtrer les fichiers temporaires (par exemple, les fichiers .tmp) auxquels l'utilisateur accède.
- **Domaine** de l'utilisateur effectuant l'activité. Vous devez fournir le **domaine exact** à filtrer. La recherche d'un domaine partiel, ou d'un domaine partiel préfixé ou suffixé par un caractère générique ('*'), ne fonctionnera pas. *None* peut être spécifié pour rechercher un domaine manquant.

Les champs suivants sont soumis à des règles de filtrage spéciales :

- **Type d'entité**, utilisant l'extension d'entité (fichier) - il est préférable de spécifier le type d'entité exact entre guillemets. Par exemple *"txt"*.
- **Chemin** de l'entité - Il doit s'agir soit du chemin exact de l'entité (par exemple, "*/home/userX/nested1/nested2/abc.txt*"), soit de la partie du répertoire du chemin pour la recherche récursive (par exemple, "*/home/userX/nested1/nested2/*"). REMARQUE : les modèles de chemin d'expression régulière (par exemple, *nested*) ne sont PAS autorisés ici. Les filtres de chemin de répertoire (chaîne de chemin se terminant par /) jusqu'à 4 répertoires de profondeur sont recommandés pour des résultats plus rapides. Par exemple, "*/home/userX/nested1/nested2/*". Voir le tableau ci-dessous pour plus de détails.

- Dossier de 1er niveau (racine) - répertoire racine du chemin d'entité comme filtres. Par exemple, si le chemin d'accès de l'entité est /home/userX/nested1/nested2/, alors home OU « home » peut être utilisé.
- Dossier de 2e niveau - Répertoire de 2e niveau des filtres de chemin d'entité. Par exemple, si le chemin d'accès de l'entité est /home/userX/nested1/nested2/, alors userX OU « userX » peut être utilisé.
- Dossier de 3e niveau – Répertoire de 3e niveau des filtres de chemin d'entité.
- Par exemple, si le chemin d'accès de l'entité est /home/userX/nested1/nested2/, alors nested1 OU « nested1 » peut être utilisé.
- Dossier de 4e niveau - Répertoire Répertoire de 4e niveau des filtres de chemin d'entité. Par exemple, si le chemin d'accès de l'entité est /home/userX/nested1/nested2/, alors nested2 OU « nested2 » peut être utilisé.
- **Utilisateur** effectuant l'activité - il est préférable de spécifier l'utilisateur exact entre guillemets. Par exemple, *"Administrateur"*.
- **Appareil** (SVM) où résident les entités
- **Volume** où résident les entités
- Le **chemin d'origine** utilisé pour les événements de renommage lorsque le fichier d'origine a été renommé.
- **IP source** à partir de laquelle l'entité a été accédée.
  - Vous pouvez utiliser les caractères génériques * et ?. Par exemple : 10.0.0.**, 10.0?.0.10, 10.10**
  - Si une correspondance exacte est requise, vous devez fournir une adresse IP source valide entre guillemets, par exemple « 10.1.1.1 ». Les adresses IP incomplètes avec des guillemets doubles tels que « 10.1.1. », « 10.1..* », etc. ne fonctionneront pas.
- Le **Nom de l'entité** - le nom de fichier du chemin de l'entité en tant que filtres. Par exemple, si le chemin de l'entité est /home/userX/nested1/testfile.txt, le nom de l'entité est testfile.txt. Veuillez noter qu'il est recommandé de spécifier le nom exact du fichier entre guillemets ; essayez d'éviter les recherches avec caractères génériques. Par exemple, « testfile.txt ». Notez également que ce filtre de nom d'entité est recommandé pour les plages de temps plus courtes (jusqu'à 3 jours).

Les champs précédents sont soumis aux conditions suivantes lors du filtrage :

- La valeur exacte doit être entre guillemets : Exemple : « searchtext »
- Les chaînes génériques ne doivent contenir aucun guillemet : Exemple : searchtext, *searchtext*, filtrera toutes les chaînes contenant « searchtext ».
- Chaîne avec un préfixe, exemple : searchtext*, recherchera toutes les chaînes commençant par « searchtext ».

Veuillez noter que tous les champs de filtre sont sensibles à la casse. Par exemple : si le filtre appliqué est de type Entité avec une valeur comme « searchtext », il renverra des résultats avec un type Entité comme « searchtext », « SearchText », « SEARCHTEXT »

Exemples de filtres d'analyse médico-légale des activités :

Expression de filtre appliquée par l'utilisateur	Résultat attendu	Évaluation des performances	Commentaire
Chemin = "/home/userX/nested1/nested2/"	Recherche récursive de tous les fichiers et dossiers sous un répertoire donné	Rapide	Les recherches dans les répertoires jusqu'à 4 répertoires seront rapides.
Chemin = "/home/userX/nested1/"	Recherche récursive de tous les fichiers et dossiers sous un répertoire donné	Rapide	Les recherches dans les répertoires jusqu'à 4 répertoires seront rapides.
Chemin = "/home/userX/nested1/test"	Correspondance exacte où la valeur du chemin correspond à /home/userX/nested1/test	Ralentissez	La recherche exacte sera plus lente à effectuer que les recherches dans l'annuaire.
Chemin = "/home/userX/nested1/nested2/nested3/"	Recherche récursive de tous les fichiers et dossiers sous un répertoire donné	Ralentissez	Les recherches dans plus de 4 répertoires sont plus lentes.
Tout autre filtre non basé sur le chemin. Il est recommandé que les filtres de type d'utilisateur et d'entité soient entre guillemets, par exemple : Utilisateur = Administrateur ; Type d'entité = txt ;		Rapide	
Nom de l'entité = "test.log"	Correspondance exacte où le nom du fichier est test.log	Rapide	Comme c'est une correspondance exacte
Nom de l'entité = *test.log	Noms de fichiers se terminant par test.log	Lent	En raison du caractère générique, cela peut être lent.
Nom de l'entité = test*.log	Les noms de fichiers commencent par test et se terminent par .log	Lent	En raison du caractère générique, cela peut être lent.
Nom de l'entité = test.lo	Noms de fichiers commençant par test.lo Par exemple : il correspondra à test.log, test.log.1, test.log1	Ralentissez	En raison du caractère générique à la fin, cela peut être lent.
Nom de l'entité = test	Noms de fichiers commençant par test	Le plus lent	En raison du caractère générique à la fin et de la valeur plus générique utilisée, cela peut être plus lent.

NOTE:

1. Le nombre d'activités affiché à côté de l'icône Toutes les activités est arrondi à 30 minutes lorsque la plage horaire sélectionnée s'étend sur plus de 3 jours. Par exemple, une plage horaire du *1er septembre 10h15 au 7 septembre 10h15* affichera le nombre d'activités du 1er septembre 10h00 au 7 septembre 10h30.
2. De même, les mesures de comptage affichées dans le graphique de l'historique des activités sont arrondies à 30 minutes lorsque la plage de temps sélectionnée s'étend sur plus de 3 jours.

Tri des données d'historique des activités médico-légales

Vous pouvez trier les données de l'historique des activités par *Heure, Utilisateur, IP source, Activité, _, _Type d'entité*, Dossier de 1er niveau (Racine), Dossier de 2e niveau, Dossier de 3e niveau et Dossier de 4e niveau. Par défaut, le tableau est trié par ordre décroissant *Time*, ce qui signifie que les données les plus récentes seront affichées en premier. Le tri est désactivé pour les champs *Device* et *Protocol*.

Guide de l'utilisateur pour les exportations asynchrones

Aperçu

La fonctionnalité Exportations asynchrones de Storage Workload Security est conçue pour gérer les exportations de données volumineuses.

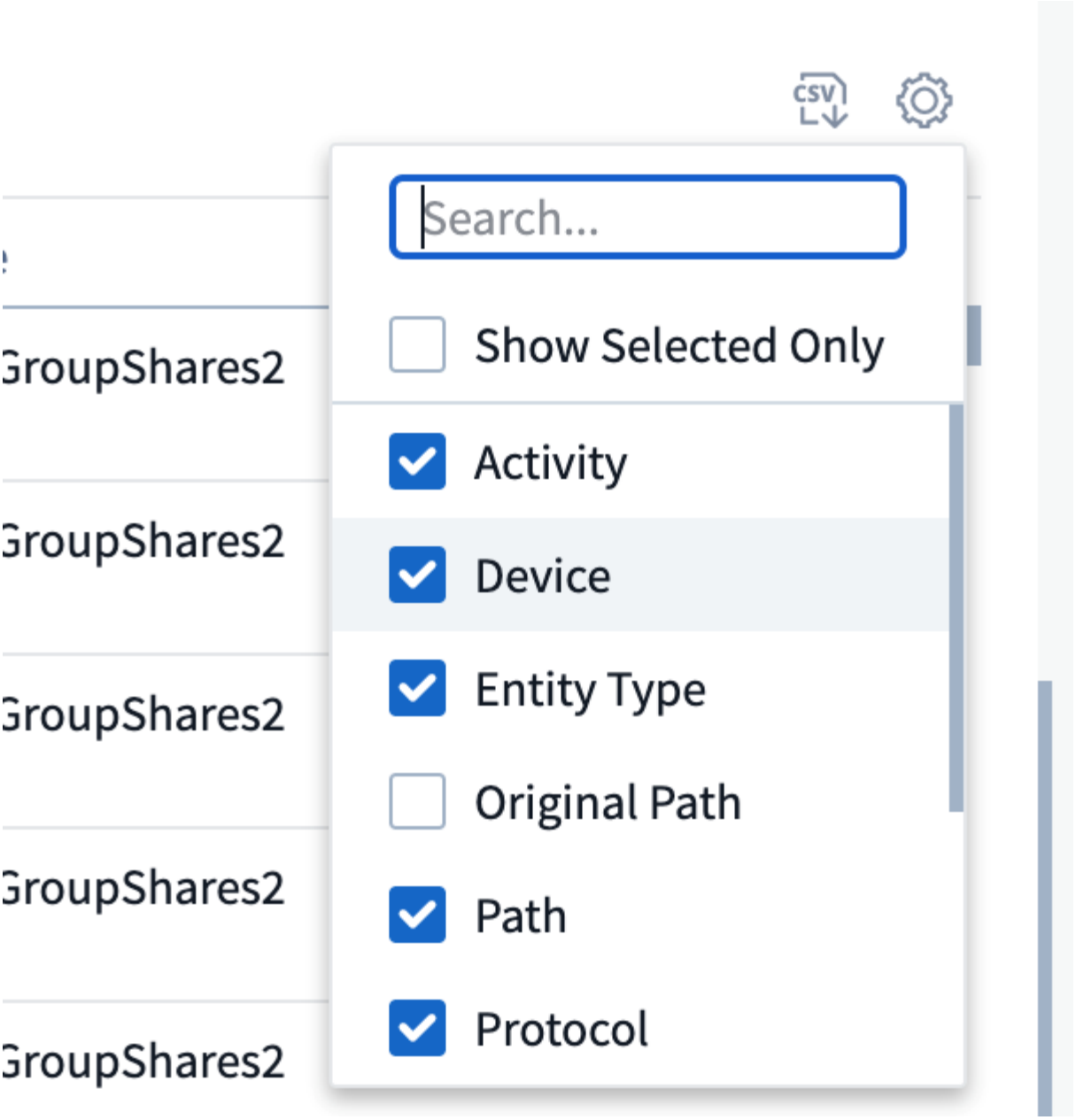
Guide étape par étape : Exportation de données avec des exportations asynchrones

1. **Lancer l'exportation** : Sélectionnez la durée et les filtres souhaités pour l'exportation et cliquez sur le bouton Exporter.
2. **Attendez que l'exportation soit terminée** : Le temps de traitement peut varier de quelques minutes à quelques heures. Vous devrez peut-être actualiser la page d'analyse médico-légale plusieurs fois. Une fois le travail d'exportation terminé, le bouton « Télécharger le dernier fichier CSV d'exportation » sera activé.
3. **Télécharger** : Cliquez sur le bouton « Télécharger le dernier fichier d'exportation créé » pour obtenir les données exportées au format .zip. Ces données seront disponibles au téléchargement jusqu'à ce que l'utilisateur lance une autre exportation asynchrone ou que 3 jours se soient écoulés, selon la première éventualité. Le bouton restera activé jusqu'à ce qu'une autre exportation asynchrone soit lancée.
4. **Limites**:
    - Le nombre de téléchargements asynchrones est actuellement limité à 1 par utilisateur pour chaque tableau d'activités et d'analyse des activités et à 3 par locataire.
    - Les données exportées sont limitées à un maximum de 1 million d'enregistrements pour la table Activités ; tandis que pour Grouper par, la limite est d'un demi-million d'enregistrements.

Un exemple de script permettant d'extraire des données médico-légales via l'API est présent dans */opt/netapp/cloudsecure/agent/export-script/* sur l'agent. Consultez le fichier readme à cet endroit pour plus de détails sur le script.

Sélection de colonnes pour toutes les activités

Le tableau *Toutes les activités* affiche les colonnes sélectionnées par défaut. Pour ajouter, supprimer ou modifier les colonnes, cliquez sur l'icône d'engrenage à droite du tableau et sélectionnez dans la liste des colonnes disponibles.



Conservation de l'historique des activités

L'historique des activités est conservé pendant 13 mois pour les environnements Workload Security actifs.

Applicabilité des filtres dans la page médico-légale

Filtre	Ce qu'il fait	Exemple	Applicable à ces filtres	Non applicable pour ces filtres	Résultat
* (Astérisque)	vous permet de rechercher tout ce que vous voulez	Auto*03172022 Si le texte de recherche contient un trait d'union ou un trait de soulignement, indiquez l'expression entre parenthèses. Par exemple, (svm*) pour rechercher svm-123	Utilisateur, type d'entité, périphérique, volume, chemin d'accès d'origine, dossier de premier niveau, dossier de deuxième niveau, dossier de troisième niveau, dossier de quatrième niveau, nom d'entité, adresse IP source		Renvoie toutes les ressources commençant par « Auto » et se terminant par « 03172022 »
? (point d'interrogation)	vous permet de rechercher un nombre spécifique de caractères	AutoSabotageUser1_03172022 ?	Utilisateur, Type d'entité, Appareil, Volume, Dossier de 1er niveau, Dossier de 2e niveau, Dossier de 3e niveau, Dossier de 4e niveau, Nom de l'entité, IP source		renvoie AutoSabotageUser1_03172022A, AutoSabotageUser1_03172022B, AutoSabotageUser1_031720225, etc.
OU	vous permet de spécifier plusieurs entités	AutoSabotageUser1_03172022 OU AutoRansomUser4_03162022	Utilisateur, domaine, type d'entité, chemin d'origine, nom d'entité, adresse IP source		renvoie l'un des éléments suivants : AutoSabotageUser1_03172022 OU AutoRansomUser4_03162022

Filtre	Ce qu'il fait	Exemple	Applicable à ces filtres	Non applicable pour ces filtres	Résultat
PAS	vous permet d'exclure du texte des résultats de recherche	NOT AutoRansomUser4_03162022	Utilisateur, domaine, type d'entité, chemin d'accès d'origine, dossier de premier niveau, dossier de deuxième niveau, dossier de troisième niveau, dossier de quatrième niveau, nom d'entité, adresse IP source	Appareil	renvoie tout ce qui ne commence pas par « AutoRansomUser4_03162022 »
Aucune	recherche les valeurs NULL dans tous les champs	Aucune	Domaine		renvoie les résultats lorsque le champ cible est vide

Recherche de chemin

Les résultats de recherche avec et sans / seront différents

"/AutoDir1/AutoFile03242022"	Seule la recherche exacte fonctionne ; renvoie toutes les activités avec un chemin exact comme /AutoDir1/AutoFile03242022 (insensible à la casse)
"/AutoDir1/ "	Fonctionne ; renvoie toutes les activités avec un répertoire de 1er niveau correspondant à AutoDir1 (insensible à la casse)
"/AutoDir1/AutoFile03242022/"	Fonctionne ; renvoie toutes les activités avec un répertoire de 1er niveau correspondant à AutoDir1 et un répertoire de 2e niveau correspondant à AutoFile03242022 (insensible à la casse)
/AutoDir1/AutoFile03242022 OU /AutoDir1/AutoFile03242022	Ça ne marche pas
PAS /AutoDir1/AutoFile03242022	Ça ne marche pas
PAS /AutoDir1	Ça ne marche pas
NON /AutoFile03242022	Ça ne marche pas
*	Ça ne marche pas

Modifications de l'activité de l'utilisateur SVM racine local

Si un utilisateur SVM racine local effectue une activité, l'adresse IP du client sur lequel le partage NFS est monté est désormais prise en compte dans le nom d'utilisateur, qui sera affiché sous la forme root@<adresse-ip-du-client> dans les pages d'activité médico-légale et d'activité utilisateur.

Par exemple:

- Si SVM-1 est surveillé par Workload Security et que l'utilisateur root de ce SVM monte le partage sur un client avec l'adresse IP 10.197.12.40, le nom d'utilisateur affiché dans la page d'activité médico-légale sera *root@10.197.12.40*.
- Si le même SVM-1 est monté sur un autre client avec l'adresse IP 10.197.12.41, le nom d'utilisateur affiché dans la page d'activité médico-légale sera *root@10.197.12.41*.

*• Ceci est fait pour séparer l'activité de l'utilisateur root NFS par adresse IP. Auparavant, toute l'activité était considérée comme effectuée uniquement par l'utilisateur *root*, sans distinction d'IP.

Dépannage

Problème	Essayez ceci
Dans le tableau « Toutes les activités », sous la colonne « Utilisateur », le nom d'utilisateur est affiché comme suit : « ldap:HQ.COMPANYNAME.COM:S-1-5-21-3577637-1906459482-1437260136-1831817 » ou « ldap:default:80038003 »	Les raisons possibles pourraient être : 1. Aucun collecteur d'annuaire utilisateur n'a encore été configuré. Pour en ajouter un, accédez à **Sécurité de la charge de travail > Collecteurs > Collecteurs d'annuaires utilisateurs** et cliquez sur **+Collecteur d'annuaires utilisateurs**. Choisissez *Active Directory* ou *LDAP Directory Server*. 2. Un collecteur d'annuaires utilisateurs a été configuré, mais il s'est arrêté ou est dans un état d'erreur. Veuillez vous rendre dans **Collecteurs > Collecteurs du répertoire utilisateur** et vérifier le statut. Reportez-vous à la"Dépannage du collecteur d'annuaires utilisateurs" section de la documentation pour des conseils de dépannage. Après une configuration correcte, le nom sera automatiquement résolu dans les 24 heures. Si le problème n'est toujours pas résolu, vérifiez si vous avez ajouté le bon collecteur de données utilisateur. Assurez-vous que l'utilisateur fait bien partie du serveur d'annuaire Active Directory/LDAP ajouté.
Certains événements NFS ne sont pas visibles dans l'interface utilisateur.	Vérifiez les points suivants : 1. Un collecteur d'annuaires utilisateurs pour le serveur AD avec des attributs POSIX définis doit être exécuté avec l'attribut unixid activé à partir de l'interface utilisateur. 2. Tout utilisateur effectuant un accès NFS doit être visible lors d'une recherche dans la page utilisateur de l'interface utilisateur 3. Les événements bruts (événements pour lesquels l'utilisateur n'est pas encore découvert) ne sont pas pris en charge pour NFS 4. L'accès anonyme à l'exportation NFS ne sera pas surveillé. 5. Assurez-vous que la version NFS utilisée est la version 4.1 ou inférieure. (Notez que NFS 4.1 est pris en charge avec ONTAP 9.15 ou version ultérieure.)

Après avoir tapé quelques lettres contenant un caractère générique comme un astérisque (*) dans les filtres des pages Forensics *All Activity* ou *Entities*, les pages se chargent très lentement.	Un astérisque (*) dans la chaîne de recherche recherche tout. Cependant, les chaînes génériques de début telles que *<*searchTerm*>* ou *<*searchTerm*>** entraîneront une requête lente. Pour obtenir de meilleures performances, utilisez plutôt des chaînes de préfixe, au format <*searchTerm*>* (en d'autres termes, ajoutez l'astérisque (*) *après* un terme de recherche). Exemple : utilisez la chaîne *testvolume**, plutôt que **testvolume* ou **test*volume*. Utilisez une recherche de répertoire pour voir toutes les activités sous un dossier donné de manière récursive (recherche hiérarchique). Par exemple, "/path1/path2/path3/" répertoriera toutes les activités de manière récursive sous /path1/path2/path3. Vous pouvez également utiliser l'option « Ajouter au filtre » sous l'onglet Toutes les activités.
Je rencontre une erreur « La demande a échoué avec le code d'état 500/503 » lors de l'utilisation d'un filtre de chemin.	Essayez d'utiliser une plage de dates plus petite pour filtrer les enregistrements.
L'interface utilisateur médico-légale charge les données lentement lors de l'utilisation du filtre *path*.	Les filtres de chemin de répertoire (chaîne de chemin se terminant par /) jusqu'à 4 répertoires de profondeur sont recommandés pour des résultats plus rapides. Par exemple, si le chemin du répertoire est /Aaa/Bbb/Ccc/Ddd, essayez de rechercher « /Aaa/Bbb/Ccc/Ddd/ » pour charger les données plus rapidement.
L'interface utilisateur médico-légale charge les données lentement et rencontre des échecs lors de l'utilisation du filtre de nom d'entité.	Veuillez essayer avec des plages de temps plus petites et avec une recherche de valeur exacte avec des guillemets doubles. Par exemple, si entityPath est "/home/userX/nested1/nested2/nested3/testfile.txt", essayez avec "testfile.txt" comme filtre de nom d'entité.

Présentation de l'utilisateur forensique

Les informations relatives à chaque utilisateur sont fournies dans la vue d'ensemble de l'utilisateur. Utilisez ces vues pour comprendre les caractéristiques des utilisateurs, les entités associées et les activités récentes.

Profil utilisateur

Les informations du profil utilisateur incluent les coordonnées et l'emplacement de l'utilisateur. Le profil fournit les informations suivantes :

- Nom de l'utilisateur
- Adresse e-mail de l'utilisateur
- Gestionnaire des utilisateurs
- Contact téléphonique de l'utilisateur

- Localisation de l’utilisateur

Comportement de l’utilisateur

Les informations sur le comportement de l’utilisateur identifient les activités et opérations récentes effectuées par l’utilisateur. Ces informations comprennent :

- Activité récente
  - Emplacement du dernier accès
  - Graphique d’activité
  - Alertes
- Opérations des sept derniers jours
  - Nombre d’opérations

Intervalle de rafraîchissement

La liste des utilisateurs est actualisée toutes les 12 heures.

Politique de conservation

Si elle n’est pas actualisée à nouveau, la liste des utilisateurs est conservée pendant 13 mois. Après 13 mois, les données seront supprimées. Si votre environnement Workload Security est supprimé, toutes les données associées à l’environnement sont supprimées.

Informations sur le copyright

Informations sur les marques commerciales