Sécurité de la charge de travail

Data Infrastructure Insights

NetApp
February 19, 2026

Sommaire

Sécurité de la charge de travail

À propos de la sécurité des charges de travail de stockage

Data Infrastructure Insights Storage Workload Security (anciennement Cloud Secure) aide à protéger vos données grâce à des informations exploitables sur les menaces internes. Il offre une visibilité et un contrôle centralisés de tous les accès aux données de l'entreprise dans les environnements de cloud hybride pour garantir que les objectifs de sécurité et de conformité sont atteints.

Visibilité

Bénéficiez d'une visibilité et d'un contrôle centralisés de l'accès des utilisateurs à vos données d'entreprise critiques stockées sur site ou dans le cloud.

Remplacez les outils et les processus manuels qui ne parviennent pas à fournir une visibilité rapide et précise sur l'accès et le contrôle des données. Workload Security fonctionne de manière unique sur les systèmes de stockage cloud et sur site pour vous fournir des alertes en temps réel sur le comportement malveillant des utilisateurs.

Protection

Protégez les données de l'organisation contre toute utilisation abusive par des utilisateurs malveillants ou compromis grâce à l'apprentissage automatique avancé et à la détection des anomalies.

Vous alerte de tout accès anormal aux données grâce à l'apprentissage automatique avancé et à la détection des anomalies du comportement des utilisateurs.

Conformité

Assurez la conformité de l'entreprise en auditant l'accès des utilisateurs à vos données d'entreprise critiques stockées sur site ou dans le cloud.

Commencer

Premiers pas avec la sécurité des charges de travail

Workload Security vous aide à surveiller l'activité des utilisateurs et à détecter les menaces de sécurité potentielles dans votre environnement de stockage. Avant de pouvoir commencer la surveillance, vous devez configurer les agents, les collecteurs de données et les services d'annuaire afin d'établir les bases d'une surveillance de sécurité complète.

Le système Workload Security utilise un agent pour collecter les données d'accès des systèmes de stockage et les informations utilisateur des serveurs des services d'annuaire.

Vous devez configurer les éléments suivants avant de pouvoir commencer à collecter des données :

Tâche	Informations connexes

Configurer un agent	"Exigences relatives aux agents" "Ajouter un agent"
Configurer un connecteur d'annuaire utilisateur	"Ajouter un connecteur d'annuaire utilisateur"
Configurer les collecteurs de données	Cliquez sur **Sécurité de la charge de travail > Collecteurs**. Cliquez sur le collecteur de données que vous souhaitez configurer. Consultez la section « Référence du fournisseur de collecteurs de données » de la documentation pour obtenir des informations sur les collecteurs.
Créer des comptes utilisateurs	"Gérer les comptes utilisateurs"

Workload Security peut également s'intégrer à d'autres outils. Par exemple,"voir ce guide" sur l'intégration avec Splunk.

Exigences relatives à l'agent de sécurité de la charge de travail

Déployez les agents de sécurité des charges de travail sur des serveurs dédiés répondant aux exigences minimales en matière de système d'exploitation, de processeur, de mémoire et d'espace disque afin de garantir des performances optimales de surveillance et de détection des menaces. Ce guide spécifie la configuration matérielle et réseau requise avant "installation de votre Workload Security Agent", notamment les distributions Linux prises en charge, les règles de connectivité réseau et les recommandations de dimensionnement du système.

Composant	Exigences Linux
Système opérateur	Un ordinateur exécutant une version sous licence de l'un des systèmes d'exploitation suivants : * AlmaLinux 9.4 (64 bits) à 9.5 (64 bits), 10 (64 bits), y compris SELinux * CentOS Stream 9 (64 bits) * Debian 11 (64 bits), 12 (64 bits), y compris SELinux * OpenSUSE Leap 15.3 (64 bits) à 15.6 (64 bits) * Oracle Linux 8.10 (64 bits), 9.1 (64 bits) à 9.6 (64 bits), y compris SELinux * Red Hat Enterprise Linux 8.10 (64 bits), 9.1 (64 bits) à 9.6 (64 bits), 10 (64 bits), y compris SELinux * Rocky 9.4 (64 bits) à 9.6 (64 bits), y compris SELinux * SUSE Linux Enterprise Server 15 SP4 (64 bits) à 15 SP6 (64 bits), y compris SELinux * Ubuntu 20.04 LTS (64 bits), 22.04 LTS (64 bits), 24.04 LTS (64 bits) Cet ordinateur ne doit exécuter aucun autre logiciel de niveau application. Un serveur dédié est recommandé.
Commandes	'unzip' est requis pour l'installation. De plus, la commande « sudo su – » est requise pour l'installation, l'exécution de scripts et la désinstallation.
processeur	4 cœurs de processeur
Mémoire	16 Go de RAM

Composant	Exigences Linux
Espace disque disponible	L'espace disque doit être alloué de cette manière : /opt/netapp 36 Go (minimum 35 Go d'espace libre après la création du système de fichiers) Remarque : il est recommandé d'allouer un peu d'espace disque supplémentaire pour permettre la création du système de fichiers. Assurez-vous qu'il y a au moins 35 Go d'espace libre dans le système de fichiers. Si /opt est un dossier monté à partir d'un stockage NAS, assurez-vous que les utilisateurs locaux ont accès à ce dossier. L'installation de l'agent ou du collecteur de données peut échouer si les utilisateurs locaux ne disposent pas de l'autorisation d'accéder à ce dossier. voir le"dépannage" section pour plus de détails.
Réseau	Connexion Ethernet 100 Mbps à 1 Gbps, adresse IP statique, connectivité IP à tous les appareils et un port requis pour l'instance Workload Security (80 ou 443).

Remarque : l'agent Workload Security peut être installé sur la même machine qu'une unité d'acquisition et/ou un agent Data Infrastructure Insights . Cependant, il est recommandé de les installer sur des machines séparées. Dans le cas où ceux-ci sont installés sur la même machine, veuillez allouer de l'espace disque comme indiqué ci-dessous :

Espace disque disponible	50-55 Go Pour Linux, l'espace disque doit être alloué de cette manière : /opt/netapp 25-30 Go /var/log/netapp 25 Go

Recommandations supplémentaires

- Il est fortement recommandé de synchroniser l'heure sur le système ONTAP et sur la machine Agent à l'aide du **Network Time Protocol (NTP)** ou du **Simple Network Time Protocol (SNTP)**.

Règles d'accès au réseau cloud

Pour les environnements de sécurité des charges de travail **basés aux États-Unis** :

Protocole	Port	Source	Destination	Description
TCP	443	Agent de sécurité de la charge de travail	<nom_site>.cs01.cloudinsights.netapp.com <nom_site>.c01.cloudinsights.netapp.com <nom_site>.c02.cloudinsights.netapp.com	Accès aux Data Infrastructure Insights
TCP	443	Agent de sécurité de la charge de travail	agentlogin.cs01.cloudinsights.netapp.com	Accès aux services d'authentification

Pour les environnements de sécurité des charges de travail **basés en Europe** :

Protocole	Port	Source	Destination	Description
TCP	443	Agent de sécurité de la charge de travail	<nom_site>.cs01-eu-1.cloudinsights.netapp.com <nom_site>.c01-eu-1.cloudinsights.netapp.com <nom_site>.c02-eu-1.cloudinsights.netapp.com	Accès aux Data Infrastructure Insights
TCP	443	Agent de sécurité de la charge de travail	agentlogin.cs01-eu-1.cloudinsights.netapp.com	Accès aux services d'authentification

Pour les environnements de sécurité des charges de travail **basés sur la région APAC** :

Protocole	Port	Source	Destination	Description
TCP	443	Agent de sécurité de la charge de travail	<nom_site>.cs01-ap-1.cloudinsights.netapp.com <nom_site>.c01-ap-1.cloudinsights.netapp.com <nom_site>.c02-ap-1.cloudinsights.netapp.com	Accès aux Data Infrastructure Insights
TCP	443	Agent de sécurité de la charge de travail	agentlogin.cs01-ap-1.cloudinsights.netapp.com	Accès aux services d'authentification

Règles du réseau

Protocole	Port	Source	Destination	Description
TCP	389 (LDAP) 636 (LDAP / start-tls)	Agent de sécurité de la charge de travail	URL du serveur LDAP	Se connecter à LDAP
TCP	443	Agent de sécurité de la charge de travail	Adresse IP de gestion du cluster ou du SVM (selon la configuration du collecteur SVM)	Communication API avec ONTAP

Protocole	Port	Source	Destination	Description
TCP	35000 - 55000	Adresses IP LIF des données SVM	Agent de sécurité de la charge de travail	Communication d' ONTAP à l'agent de sécurité de la charge de travail pour les événements Fpolicy. Ces ports doivent être ouverts vers l'agent de sécurité de la charge de travail pour ONTAP puisse lui envoyer des événements, y compris tout pare-feu sur l'agent de sécurité de la charge de travail lui-même (le cas échéant). NOTEZ que vous n'avez pas besoin de réserver **tous** ces ports, mais les ports que vous réservez pour cela doivent être dans cette plage. Il est recommandé de commencer par réserver environ 100 ports, et d'augmenter si nécessaire.

Protocole	Port	Source	Destination	Description
TCP	35000-55000	IP de gestion de cluster	Agent de sécurité de la charge de travail	Communication de l'IP de gestion du cluster ONTAP à l'agent de sécurité de la charge de travail pour les **événements EMS**. Ces ports doivent être ouverts vers l'agent de sécurité de la charge de travail pour ONTAP puisse lui envoyer des **événements EMS**, y compris tout pare-feu sur l'agent de sécurité de la charge de travail lui-même (le cas échéant). NOTEZ que vous n'avez pas besoin de réserver **tous** ces ports, mais les ports que vous réservez pour cela doivent être dans cette plage. Il est recommandé de commencer par réserver environ 100 ports, et d'augmenter si nécessaire.
SSH	22	Agent de sécurité de la charge de travail	Gestion des clusters	Nécessaire pour le blocage des utilisateurs CIFS/SMB.

Dimensionnement du système

Voir le"Vérificateur de taux d'événements" documentation pour obtenir des informations sur le dimensionnement.

Déployer des agents de sécurité de charge de travail

Les agents de sécurité des charges de travail sont essentiels pour surveiller l'activité des utilisateurs et détecter les menaces potentielles à la sécurité de votre infrastructure de stockage. Ce guide fournit des instructions d'installation étape par étape, les meilleures pratiques pour la gestion des agents (y compris les fonctionnalités de pause/reprise et d'épinglage/désépinglage) et les exigences de configuration post-déploiement. Avant de

commencer, assurez-vous que votre serveur d'agent répond aux exigences suivantes : "exigences système".

Avant de commencer

- Le privilège sudo est requis pour l'installation, l'exécution de scripts et la désinstallation.
- Lors de l'installation de l'agent, un utilisateur local *cssys* et un groupe local *cssys* sont créés sur la machine. Si les paramètres d'autorisation ne permettent pas la création d'un utilisateur local et nécessitent plutôt Active Directory, un utilisateur avec le nom d'utilisateur *cssys* doit être créé sur le serveur Active Directory.
- Vous pouvez en savoir plus sur la sécurité de Data Infrastructure Insights"ici" .

Meilleures pratiques

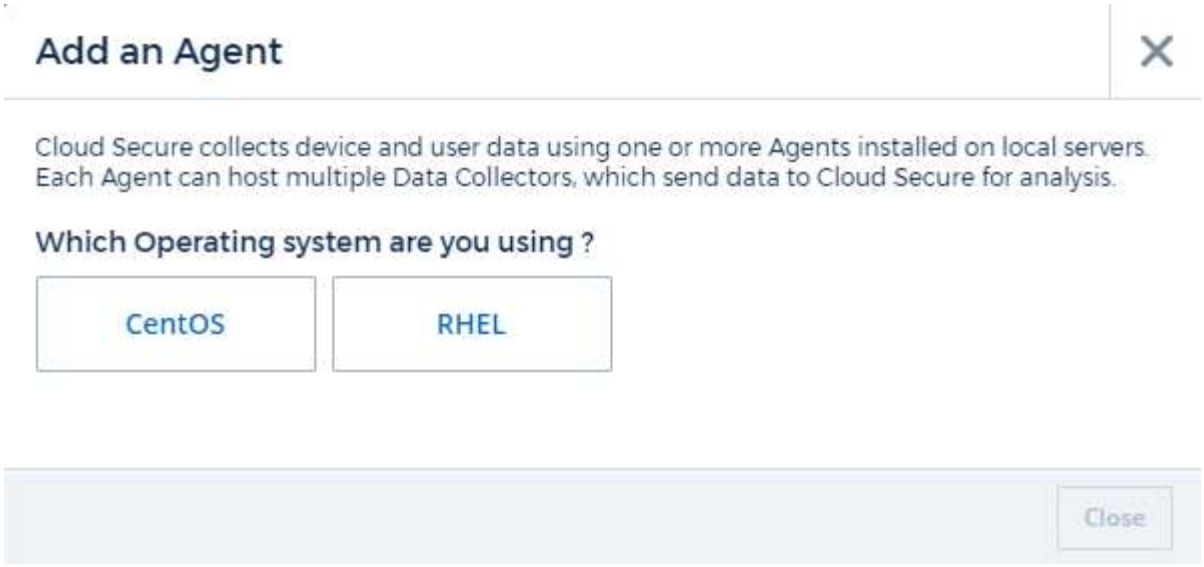
Gardez les points suivants à l'esprit avant de configurer votre agent Workload Security.

Pause et reprise	Pause : Supprime les politiques fpolicies d' ONTAP. Généralement utilisé lorsque les clients effectuent des opérations de maintenance prolongées pouvant prendre beaucoup de temps, comme le redémarrage des machines virtuelles d'agents ou le remplacement du stockage. Résumé : Ajoute à nouveau fpolicies à ONTAP.
Épingler et désépingler	Unpin récupère immédiatement la dernière version (si disponible) et met à jour l'agent et le collecteur. Durant cette mise à niveau, fpolicies se déconnectera puis se reconnectera. Cette fonctionnalité est conçue pour les clients qui souhaitent contrôler le calendrier des mises à jour automatiques. Voir ci-dessous pourInstructions pour épingler/déépingler .
Approche recommandée	Pour les configurations importantes, il est conseillé d'utiliser Pin et Unpin plutôt que de mettre en pause les collecteurs. Il n'est pas nécessaire de faire une pause et de reprendre pendant l'utilisation de l'épinglage et du désépinglage. Les clients peuvent conserver leurs agents et collecteurs épinglés et, dès réception d'une notification par e-mail concernant une nouvelle version, disposent d'un délai de 30 jours pour mettre à jour sélectivement leurs agents un par un. Cette approche minimise l'impact de la latence sur les politiques fpolicies et offre un meilleur contrôle sur le processus de mise à niveau.

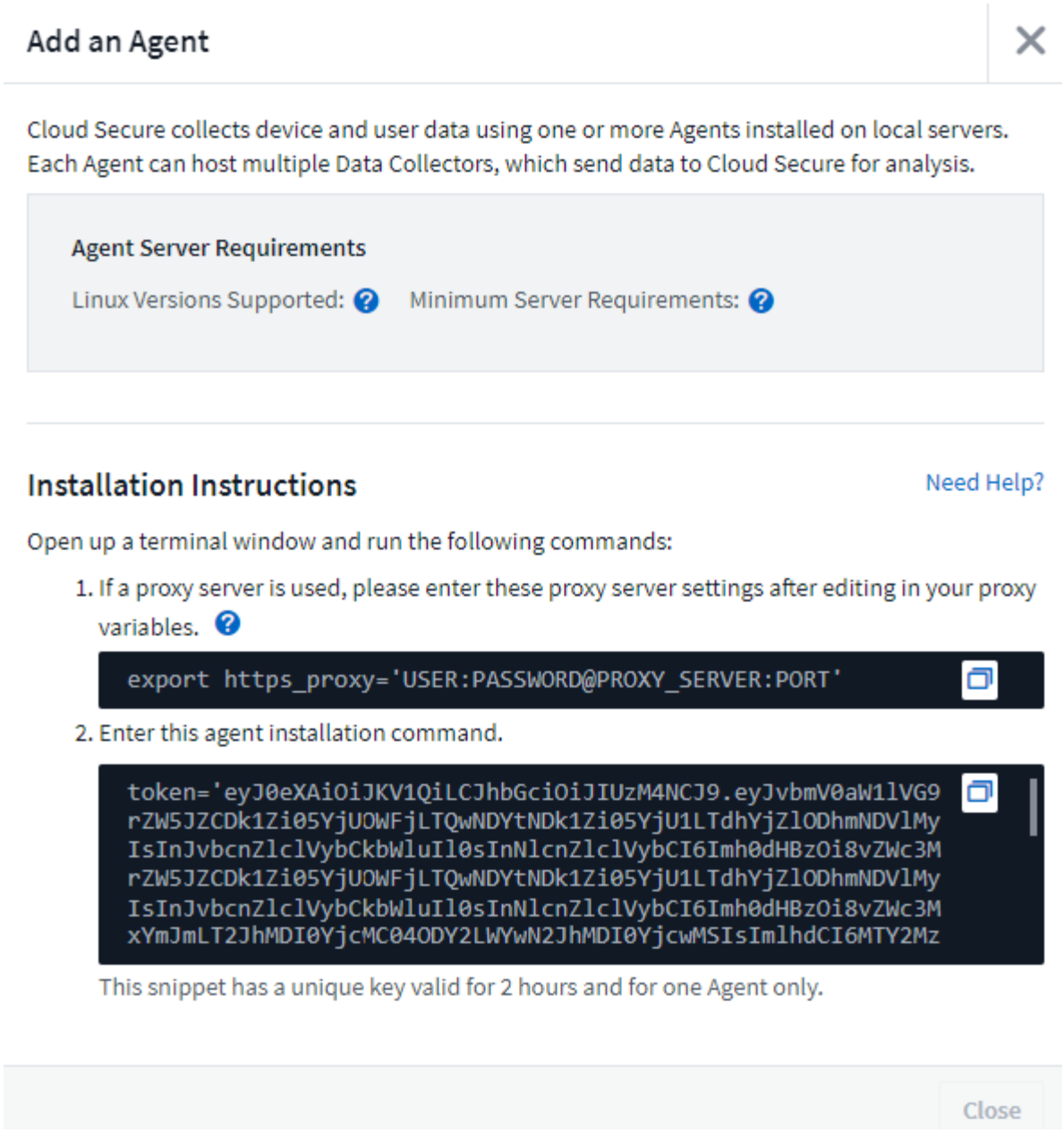
Étapes pour installer l'agent

1. Connectez-vous en tant qu'administrateur ou propriétaire de compte à votre environnement Workload Security.
2. Sélectionnez **Collecteurs > Agents > +Agent**

   Le système affiche la page Ajouter un agent :



3. Vérifiez que le serveur d'agent répond à la configuration système minimale requise.
4. Pour vérifier que le serveur d'agent exécute une version prise en charge de Linux, cliquez sur *Versions prises en charge (i)*.
5. Si votre réseau utilise un serveur proxy, veuillez définir les détails du serveur proxy en suivant les instructions de la section Proxy.



6. Cliquez sur l'icône Copier dans le presse-papiers pour copier la commande d'installation.
7. Exécutez la commande d'installation dans une fenêtre de terminal.
8. Le système affiche le message suivant lorsque l'installation se termine avec succès :

Après avoir terminé

1. Vous devez configurer un"Collecteur d'annuaires utilisateurs" .
2. Vous devez configurer un ou plusieurs collecteurs de données.

Configuration du réseau

Exécutez les commandes suivantes sur le système local pour ouvrir les ports qui seront utilisés par Workload Security. S'il existe un problème de sécurité concernant la plage de ports, vous pouvez utiliser une plage de ports plus petite, par exemple *35000:35100*. Chaque SVM utilise deux ports.

Étapes

1. `sudo firewall-cmd --permanent --zone=public --add-port=35000-55000/tcp`
2. `sudo firewall-cmd --reload`

Suivez les étapes suivantes en fonction de votre plateforme :

CentOS 7.x / RHEL 7.x:

1. `sudo iptables-save | grep 35000`

Exemple de sortie :

```
 -A IN_public_allow -p tcp -m tcp --dport 35000:55000 -m conntrack
-ctstate NEW,UNTRACKED -j ACCEPT
*CentOS 8.x / RHEL 8.x*:
```

1. `sudo firewall-cmd --zone=public --list-ports | grep 35000`(pour CentOS 8)

Exemple de sortie :

```
35000-55000/tcp
```

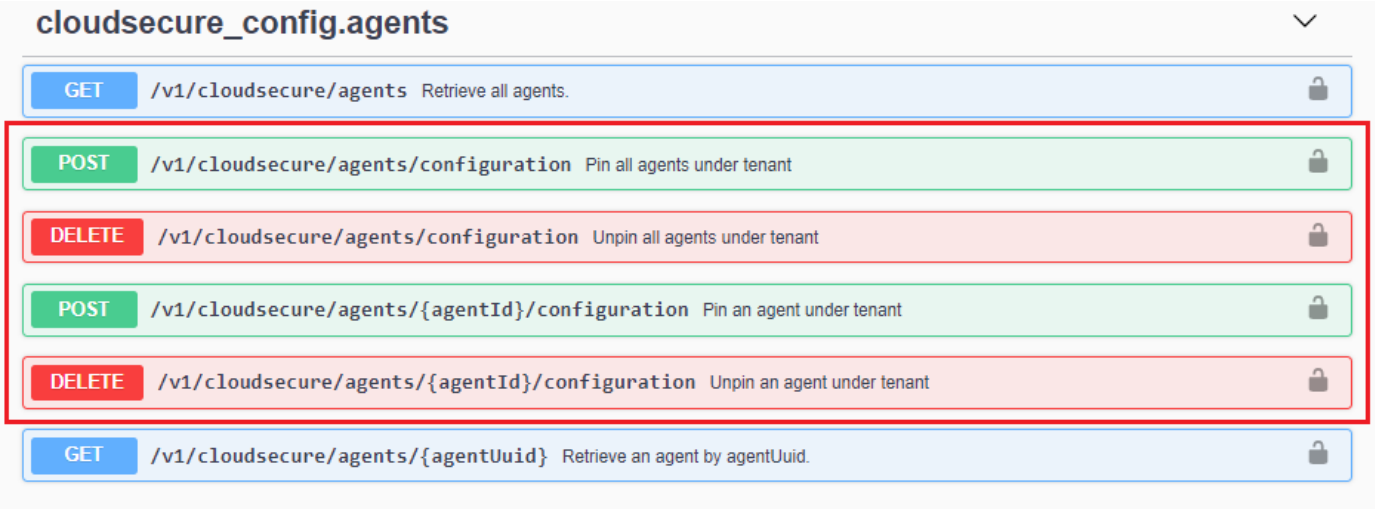
« Épingler » un agent sur la version actuelle

Par défaut, Data Infrastructure Insights Workload Security met à jour automatiquement les agents. Certains clients peuvent souhaiter suspendre la mise à jour automatique, ce qui laisse un agent à sa version actuelle jusqu'à ce que l'un des événements suivants se produise :

- Le client reprend les mises à jour automatiques de l'agent.
- 30 jours sont passés. Notez que les 30 jours commencent le jour de la mise à jour la plus récente de l'agent, et non le jour où l'agent est mis en pause.

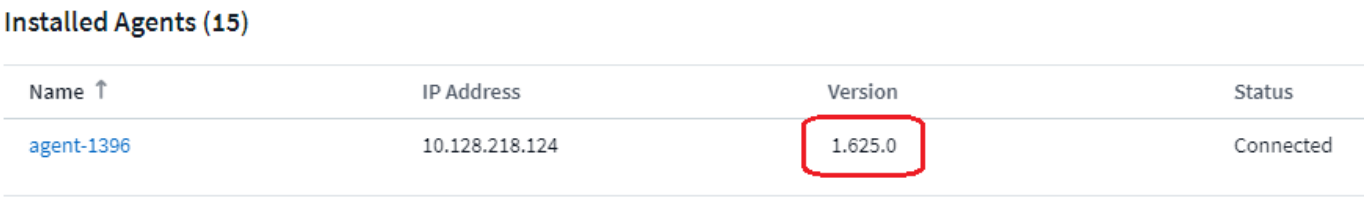
Dans chacun de ces cas, l'agent sera mis à jour lors de la prochaine actualisation de Workload Security.

Pour suspendre ou reprendre les mises à jour automatiques des agents, utilisez les API *cloudsecure_config.agents* :



Notez que l'action de pause ou de reprise peut prendre jusqu'à cinq minutes pour prendre effet.

Vous pouvez afficher vos versions d'agent actuelles sur la page **Sécurité de la charge de travail > Collecteurs**, dans l'onglet **Agents**.



Dépannage des erreurs de l'agent

Les problèmes connus et leurs résolutions sont décrits dans le tableau suivant.

Problème:	Résolution:
L'installation de l'agent ne parvient pas à créer le dossier /opt/netapp/cloudsecure/agent/logs/agent.log et le fichier install.log ne fournit aucune information pertinente.	Cette erreur se produit lors de l'amorçage de l'agent. L'erreur n'est pas enregistrée dans les fichiers journaux car elle se produit avant l'initialisation de l'enregistreur. L'erreur est redirigée vers la sortie standard et est visible dans le journal de service à l'aide de l' `journalctl -u cloudsecure-agent.service` commande. Cette commande peut être utilisée pour résoudre le problème plus en détail. est
L'installation de l'agent échoue avec le message « Cette distribution Linux n'est pas prise en charge. Sortie de l'installation'.	Cette erreur apparaît lorsque vous tentez d'installer l'agent sur un système non pris en charge. Voir "Exigences relatives aux agents" .
L'installation de l'agent a échoué avec l'erreur : « -bash : unzip : commande introuvable »	Installez, décompressez, puis exécutez à nouveau la commande d'installation. Si Yum est installé sur la machine, essayez « yum install unzip » pour installer le logiciel de décompression. Après cela, recopiez la commande depuis l'interface utilisateur d'installation de l'agent et collez-la dans l'interface de ligne de commande pour exécuter à nouveau l'installation.

Problème:	Résolution:
L'agent a été installé et était en cours d'exécution. Cependant, l'agent s'est arrêté soudainement.	Connectez-vous en SSH à la machine de l'agent. Vérifiez l'état du service de l'agent via `sudo systemctl status cloudsecure-agent.service` . 1. Vérifiez si les journaux affichent un message « Échec du démarrage du service démon Workload Security ». 2. Vérifiez si l'utilisateur cssys existe ou non dans la machine Agent. Exécutez les commandes suivantes une par une avec l'autorisation root et vérifiez si l'utilisateur et le groupe cssys existent. `sudo id cssys` `sudo groups cssys` 3. S'il n'en existe aucun, une politique de surveillance centralisée peut avoir supprimé l'utilisateur cssys. 4. Créez l'utilisateur et le groupe cssys manuellement en exécutant les commandes suivantes. `sudo useradd cssys` `sudo groupadd cssys` 5. Redémarrez ensuite le service de l'agent en exécutant la commande suivante : `sudo systemctl restart cloudsecure-agent.service` 6. Si le problème persiste, veuillez vérifier les autres options de dépannage.
Impossible d'ajouter plus de 50 collecteurs de données à un agent.	Seuls 50 collecteurs de données peuvent être ajoutés à un agent. Il peut s'agir d'une combinaison de tous les types de collecteurs, par exemple, Active Directory, SVM et d'autres collecteurs.
L'interface utilisateur indique que l'agent est dans l'état NOT_CONNECTED.	Étapes pour redémarrer l'agent. 1. Connectez-vous en SSH à la machine de l'agent. 2. Redémarrez ensuite le service de l'agent en exécutant la commande suivante : `sudo systemctl restart cloudsecure-agent.service` 3. Vérifiez l'état du service de l'agent via `sudo systemctl status cloudsecure-agent.service` . 4. L'agent doit passer à l'état CONNECTÉ.
L'agent VM est derrière le proxy Zscaler et l'installation de l'agent échoue. En raison de l'inspection SSL du proxy Zscaler, les certificats de sécurité de la charge de travail sont présentés comme s'ils étaient signés par Zscaler CA, de sorte que l'agent ne fait pas confiance à la communication.	Désactivez l'inspection SSL dans le proxy Zscaler pour l'URL *.cloudinsights.netapp.com. Si Zscaler effectue une inspection SSL et remplace les certificats, Workload Security ne fonctionnera pas.

Problème:	Résolution:
Lors de l'installation de l'agent, l'installation se bloque après la décompression.	La commande « chmod 755 -Rf » échoue. La commande échoue lorsque la commande d'installation de l'agent est exécutée par un utilisateur sudo non root qui possède des fichiers dans le répertoire de travail, appartenant à un autre utilisateur, et les autorisations de ces fichiers ne peuvent pas être modifiées. En raison de l'échec de la commande chmod, le reste de l'installation ne s'exécute pas. 1. Créez un nouveau répertoire nommé « cloudsecure ». 2. Allez dans ce répertoire. 3. Copiez et collez la commande d'installation complète « token=…… … ./cloudsecure-agent-install.sh » et appuyez sur Entrée. 4. L'installation devrait pouvoir se poursuivre.
Si l'agent ne parvient toujours pas à se connecter à Saas, veuillez ouvrir un dossier auprès du support NetApp . Fournissez le numéro de série Data Infrastructure Insights pour ouvrir un dossier et joignez les journaux au dossier comme indiqué.	Pour joindre des journaux au dossier : 1. Exécutez le script suivant avec l'autorisation root et partagez le fichier de sortie (cloudsecure-agent-symptoms.zip). a. /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh 2. Exécutez les commandes suivantes une par une avec l'autorisation root et partagez la sortie. a. id cssys b. groups cssys c. cat /etc/os-release
Le script cloudsecure-agent-symptom-collector.sh échoue avec l'erreur suivante. [root@machine tmp]# /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh Collecte du journal de service Collecte des journaux d'application Collecte des configurations d'agent Prise d'un instantané de l'état du service Prise d'un instantané de la structure du répertoire de l'agent ……. ……. /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh : ligne 52 : zip : commande introuvable ERREUR : Échec de la création de /tmp/cloudsecure-agent-symptoms.zip	L'outil Zip n'est pas installé. Installez l'outil zip en exécutant la commande « yum install zip ». Exécutez ensuite à nouveau cloudsecure-agent-symptom-collector.sh.
L'installation de l'agent échoue avec useradd : impossible de créer le répertoire /home/cssys	Cette erreur peut se produire si le répertoire de connexion de l'utilisateur ne peut pas être créé sous /home, en raison d'un manque d'autorisations. La solution de contournement serait de créer un utilisateur cssys et d'ajouter son répertoire de connexion manuellement à l'aide de la commande suivante : *sudo useradd user_name -m -d HOME_DIR* -m : Créez le répertoire personnel de l'utilisateur s'il n'existe pas. -d : Le nouvel utilisateur est créé en utilisant HOME_DIR comme valeur pour le répertoire de connexion de l'utilisateur. Par exemple, *sudo useradd cssys -m -d /cssys*, ajoute un utilisateur *cssys* et crée son répertoire de connexion sous root.

Problème:	Résolution:
L'agent ne s'exécute pas après l'installation. *Systemctl status cloudsecure-agent.service* affiche ce qui suit : [root@demo ~]# systemctl status cloudsecure-agent.service agent.service – Workload Security Agent Daemon Service Loaded: loaded (/usr/lib/systemd/system/cloudsecure-agent.service; enabled; vendor preset: disabled) Active: activation (redémarrage automatique) (Result: exit-code) since Tue 2021-08-03 21:12:26 PDT; Il y a 2 s Processus : 25889 ExecStart=/bin/bash /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent (code=exited status=126) PID principal : 25889 (code=exited, status=126), 03 août 21:12:26 démo systemd[1] : cloudsecure-agent.service : processus principal terminé, code=exited, status=126/n/a 03 août 21:12:26 démo systemd[1] : l'unité cloudsecure-agent.service est entrée en état d'échec. 03 août 21:12:26 démo systemd[1] : cloudsecure-agent.service a échoué.	Cela peut échouer car l'utilisateur *cssys* n'a peut-être pas l'autorisation d'installer. Si /opt/netapp est un montage NFS et si l'utilisateur *cssys* n'a pas accès à ce dossier, l'installation échouera. *cssys* est un utilisateur local créé par le programme d'installation de Workload Security qui n'est peut-être pas autorisé à accéder au partage monté. Vous pouvez le vérifier en essayant d'accéder à /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent en utilisant l'utilisateur *cssys*. Si le message « Autorisation refusée » est renvoyé, l'autorisation d'installation n'est pas présente. Au lieu d'un dossier monté, installez-le dans un répertoire local sur la machine.
L'agent a été initialement connecté via un serveur proxy et le proxy a été défini lors de l'installation de l'agent. Le serveur proxy a maintenant changé. Comment la configuration du proxy de l'agent peut-elle être modifiée ?	Vous pouvez modifier le fichier agent.properties pour ajouter les détails du proxy. Suivez ces étapes : 1. Accédez au dossier contenant le fichier de propriétés : cd /opt/netapp/cloudsecure/conf 2. À l'aide de votre éditeur de texte préféré, ouvrez le fichier *agent.properties* pour le modifier. 3. Ajoutez ou modifiez les lignes suivantes : AGENT_PROXY_HOST=scspa1950329001.vm.netapp.com AGENT_PROXY_PORT=80 AGENT_PROXY_USER=pxuser AGENT_PROXY_PASSWORD=pass1234 4. Enregistrez le fichier. 5. Redémarrez l'agent : sudo systemctl restart cloudsecure-agent.service

Suppression d'un agent de sécurité de charge de travail

Lorsque vous supprimez un agent Workload Security, tous les collecteurs de données associés à l'agent doivent d'abord être supprimés.

Suppression d'un agent

La suppression d'un agent supprime tous les collecteurs de données associés à l'agent. Si vous prévoyez de configurer les collecteurs de données avec un agent différent, vous devez créer une sauvegarde des configurations du collecteur de données avant de supprimer l'agent.

Avant de commencer

1. Assurez-vous que tous les collecteurs de données associés à l'agent sont supprimés du portail Workload Security.

   Remarque : ignorez cette étape si tous les collecteurs associés sont à l'état ARRÊTÉ.

Étapes pour supprimer un agent :

1. Connectez-vous à la machine virtuelle de l'agent via SSH et exécutez la commande suivante. Lorsque vous y êtes invité, entrez « y » pour continuer.

```
sudo /opt/netapp/cloudsecure/agent/install/cloudsecure-agent-
uninstall.sh
Uninstall CloudSecure Agent? [y|N]:
```

2. Cliquez sur **Sécurité de la charge de travail > Collecteurs > Agents**

   Le système affiche la liste des agents configurés.

3. Cliquez sur le menu d'options de l'agent que vous supprimez.
4. Cliquez sur **Supprimer**.

   Le système affiche la page **Supprimer l'agent**.

5. Cliquez sur **Supprimer** pour confirmer la suppression.

Configuration d'un collecteur d'annuaires utilisateurs Active Directory (AD)

Workload Security peut être configuré pour collecter les attributs utilisateur à partir des serveurs Active Directory.

Avant de commencer

- Vous devez être administrateur ou propriétaire de compte Data Infrastructure Insights pour effectuer cette tâche.
- Vous devez disposer de l'adresse IP du serveur hébergeant le serveur Active Directory.
- Un agent doit être configuré avant de configurer un connecteur d'annuaire utilisateur.

Étapes pour configurer un collecteur d'annuaires utilisateurs

1. Dans le menu Sécurité de la charge de travail, cliquez sur : **Collecteurs > Collecteurs d'annuaires utilisateurs > + Collecteur d'annuaires utilisateurs** et sélectionnez **Active Directory**

   Le système affiche l'écran Ajouter un répertoire d'utilisateurs.

Configurez le collecteur d'annuaires utilisateurs en saisissant les données requises dans les tableaux suivants :

Nom	Description
Nom	Nom unique pour le répertoire utilisateur. Par exemple *GlobalADCollector*
Agent	Sélectionnez un agent configuré dans la liste
IP du serveur/nom de domaine	Adresse IP ou nom de domaine complet (FQDN) du serveur hébergeant l'annuaire actif

Nom de la forêt	Niveau de forêt de la structure du répertoire. Le nom de forêt autorise les deux formats suivants : *x.y.z* ⇒ nom de domaine direct tel que vous l'avez sur votre SVM. [Exemple : hq.companyname.com] *DC=x,DC=y,DC=z* ⇒ Noms distinctifs relatifs [Exemple : DC=hq,DC= companyname,DC=com] Ou vous pouvez spécifier comme suit : *OU=engineering,DC=hq,DC= companyname,DC=com* [pour filtrer par UO spécifique engineering] *CN=username,OU=engineering,DC=companyname, DC=netapp, DC=com* [pour obtenir uniquement l'utilisateur spécifique avec <username> de l'UO <engineering>] *CN=Acrobat Users,CN=Users,DC=hq,DC=companyname,DC=com ,O= companyname,L=Boston,S=MA,C=US* [pour obtenir tous les utilisateurs Acrobat au sein des utilisateurs de cette organisation] Les domaines Active Directory approuvés sont également pris en charge.
Lier DN	L'utilisateur est autorisé à rechercher dans le répertoire. Par exemple : *username@companyname.com* ou *username@domainname.com*. De plus, l'autorisation de lecture seule du domaine est requise. L'utilisateur doit être membre du groupe de sécurité *Contrôleurs de domaine en lecture seule*.
Mot de passe BIND	Mot de passe du serveur d'annuaire (c'est-à-dire le mot de passe du nom d'utilisateur utilisé dans Bind DN)
Protocole	ldap, ldaps, ldap-start-tls
Ports	Sélectionner le port

Saisissez les attributs requis du serveur d'annuaire suivants si les noms d'attributs par défaut ont été modifiés dans Active Directory. Le plus souvent, ces noms d'attributs ne sont pas modifiés dans Active Directory, auquel cas vous pouvez simplement continuer avec le nom d'attribut par défaut.

Attributs	Nom d'attribut dans Directory Server
Nom d'affichage	nom
SID	objectid
Nom d'utilisateur	sAMAccountName

Cliquez sur Inclure les attributs facultatifs pour ajouter l'un des attributs suivants :

Attributs	Nom d'attribut dans le serveur d'annuaire
Adresse email	mail
Numéro de téléphone	numéro de téléphone
Rôle	titre

Pays	co
État	État
Département	département
Photo	vignettephoto
GestionnaireDN	directeur
Groupes	membreDe

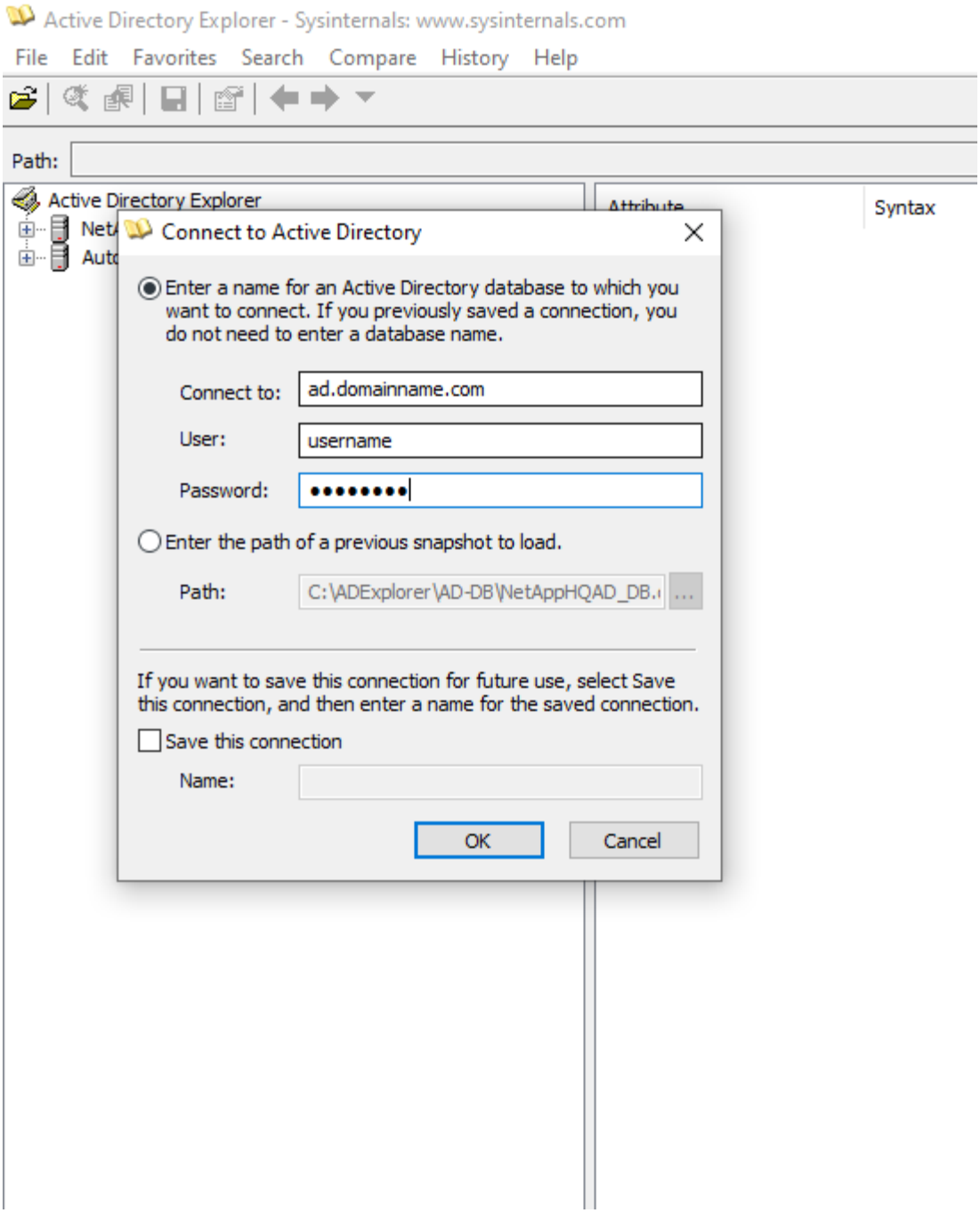
Test de la configuration de votre collecteur d'annuaires utilisateurs

Vous pouvez valider les autorisations utilisateur et les définitions d'attributs LDAP à l'aide des procédures suivantes :

- Utilisez la commande suivante pour valider l'autorisation de l'utilisateur LDAP de Workload Security :

  ```
  ldapsearch -o ldif-wrap=no -LLL -x -b "dc=netapp,dc=com" -h 10.235.40.29 -p
  389 -D Administrator@netapp.com -W
  ```

- Utilisez AD Explorer pour parcourir une base de données AD, afficher les propriétés et les attributs des objets, afficher les autorisations, afficher le schéma d'un objet, exécuter des recherches sophistiquées que vous pouvez enregistrer et réexécuter.
  - Installer"Explorateur AD" sur n'importe quelle machine Windows pouvant se connecter au serveur AD.
  - Connectez-vous au serveur AD à l'aide du nom d'utilisateur/mot de passe du serveur d'annuaire AD.



Dépannage des erreurs de configuration du collecteur d'annuaires utilisateurs

Le tableau suivant décrit les problèmes connus et les résolutions qui peuvent survenir lors de la configuration du collecteur :

Problème:	Résolution:
L'ajout d'un connecteur d'annuaire utilisateur génère l'état « Erreur ». L'erreur indique : « Informations d'identification non valides fournies pour le serveur LDAP ».	Nom d'utilisateur ou mot de passe incorrect fourni. Modifiez et fournissez le nom d'utilisateur et le mot de passe corrects.

Problème:	Résolution:
L'ajout d'un connecteur d'annuaire utilisateur génère l'état « Erreur ». L'erreur indique : « Impossible d'obtenir l'objet correspondant à DN=DC=hq,DC=domainname,DC=com fourni comme nom de forêt. »	Nom de forêt incorrect fourni. Modifiez et fournissez le nom de forêt correct.
Les attributs facultatifs de l'utilisateur de domaine n'apparaissent pas dans la page Profil utilisateur de Workload Security.	Cela est probablement dû à une incompatibilité entre les noms des attributs facultatifs ajoutés dans CloudSecure et les noms d'attributs réels dans Active Directory. Modifiez et fournissez le(s) nom(s) d'attribut facultatif(s) correct(s).
Collecteur de données dans un état d'erreur avec « Échec de la récupération des utilisateurs LDAP ». Motif de l'échec : Impossible de se connecter au serveur, la connexion est nulle.	Redémarrez le collecteur en cliquant sur le bouton *Redémarrer*.
L'ajout d'un connecteur d'annuaire utilisateur génère l'état « Erreur ».	Assurez-vous d'avoir fourni des valeurs valides pour les champs obligatoires (serveur, nom de forêt, DN de liaison, mot de passe de liaison). Assurez-vous que l'entrée bind-DN est toujours fournie sous la forme « Administrateur@<domain_forest_name> » ou sous la forme d'un compte utilisateur avec des privilèges d'administrateur de domaine.
L'ajout d'un connecteur d'annuaire utilisateur entraîne l'état « RÉESSAI ». Affiche l'erreur « Impossible de définir l'état du collecteur, raison pour laquelle la commande TCP [Connect(localhost:35012,None,List(),Some(,seconds),true)] a échoué en raison de java.net.ConnectionException : connexion refusée. »	IP ou FQDN incorrect fourni pour le serveur AD. Modifiez et fournissez l'adresse IP ou le FQDN correct.
L'ajout d'un connecteur d'annuaire utilisateur génère l'état « Erreur ». L'erreur indique : « Échec de l'établissement de la connexion LDAP ».	IP ou FQDN incorrect fourni pour le serveur AD. Modifiez et fournissez l'adresse IP ou le FQDN correct.
L'ajout d'un connecteur d'annuaire utilisateur génère l'état « Erreur ». L'erreur indique : « Échec du chargement des paramètres. Motif : la configuration de la source de données comporte une erreur. Raison spécifique : /connector/conf/application.conf : 70 : ldap.ldap-port est de type STRING plutôt que NUMBER »	Valeur incorrecte pour le port fourni. Essayez d'utiliser les valeurs de port par défaut ou le numéro de port correct pour le serveur AD.
J'ai commencé avec les attributs obligatoires, et cela a fonctionné. Après avoir ajouté les attributs facultatifs, les données des attributs facultatifs ne sont pas récupérées à partir d'AD.	Cela est probablement dû à une incompatibilité entre les attributs facultatifs ajoutés dans CloudSecure et les noms d'attributs réels dans Active Directory. Modifiez et fournissez le nom d'attribut obligatoire ou facultatif correct.

Problème:	Résolution:
Après le redémarrage du collecteur, quand la synchronisation AD aura-t-elle lieu ?	La synchronisation AD se produira immédiatement après le redémarrage du collecteur. Il faudra environ 15 minutes pour récupérer les données utilisateur d'environ 300 000 utilisateurs, et elles sont actualisées automatiquement toutes les 12 heures.
Les données utilisateur sont synchronisées d'AD vers CloudSecure. Quand les données seront-elles supprimées ?	Les données utilisateur sont conservées pendant 13 mois en cas de non actualisation. Si le locataire est supprimé, les données seront supprimées.
Le connecteur d'annuaire utilisateur génère l'état « Erreur ». "Le connecteur est en état d'erreur. Nom du service : usersLdap. Motif de l'échec : échec de la récupération des utilisateurs LDAP. Motif de l'échec : 80090308 : LdapErr : DSID-0C090453, commentaire : erreur AcceptSecurityContext, données 52e, v3839	Nom de forêt incorrect fourni. Voir ci-dessus comment fournir le nom de forêt correct.
Le numéro de téléphone n'est pas renseigné dans la page de profil utilisateur.	Cela est probablement dû à un problème de mappage d'attributs avec Active Directory. 1. Modifiez le collecteur Active Directory particulier qui récupère les informations de l'utilisateur à partir d'Active Directory. 2. Notez que sous les attributs facultatifs, il existe un nom de champ « Numéro de téléphone » mappé à l'attribut Active Directory « telephonenumber ». 4. Maintenant, utilisez l'outil Active Directory Explorer comme décrit ci-dessus pour parcourir Active Directory et voir le nom d'attribut correct. 3. Assurez-vous que dans Active Directory, il existe un attribut nommé « telephonenumber » qui contient bien le numéro de téléphone de l'utilisateur. 5. Disons que dans Active Directory, il a été modifié en « numéro de téléphone ». 6. Modifiez ensuite le collecteur d'annuaires utilisateurs CloudSecure. Dans la section des attributs facultatifs, remplacez « telephonenumber » par « phonenumber ». 7. Enregistrez le collecteur Active Directory, le collecteur redémarrera et récupérera le numéro de téléphone de l'utilisateur et l'affichera dans la page de profil utilisateur.
Si le certificat de chiffrement (SSL) est activé sur le serveur Active Directory (AD), le collecteur d'annuaires d'utilisateurs Workload Security ne peut pas se connecter au serveur AD.	Désactivez le chiffrement du serveur AD avant de configurer un collecteur d'annuaires utilisateurs. Une fois les détails de l'utilisateur récupérés, ils resteront là pendant 13 mois. Si le serveur AD est déconnecté après avoir récupéré les détails de l'utilisateur, les utilisateurs nouvellement ajoutés dans AD ne seront pas récupérés. Pour effectuer une nouvelle récupération, le collecteur d'annuaires utilisateurs doit être connecté à AD.
Les données d'Active Directory sont présentes dans CloudInsights Security. Vous souhaitez supprimer toutes les informations utilisateur de CloudInsights.	Il n'est pas possible de supprimer UNIQUEMENT les informations utilisateur Active Directory de CloudInsights Security. Afin de supprimer l'utilisateur, le locataire complet doit être supprimé.

Configuration d’un collecteur de serveur d’annuaire LDAP

Vous configurez Workload Security pour collecter les attributs utilisateur à partir des serveurs d’annuaire LDAP.

Avant de commencer

- Vous devez être administrateur ou propriétaire de compte Data Infrastructure Insights pour effectuer cette tâche.
- Vous devez disposer de l’adresse IP du serveur hébergeant le serveur d’annuaire LDAP.
- Un agent doit être configuré avant de configurer un connecteur d’annuaire LDAP.

Étapes pour configurer un collecteur d’annuaires utilisateurs

1. Dans le menu Sécurité de la charge de travail, cliquez sur : **Collecteurs > Collecteurs d’annuaires utilisateurs > + Collecteur d’annuaires utilisateurs** et sélectionnez **Serveur d’annuaire LDAP**

   Le système affiche l’écran Ajouter un répertoire d’utilisateurs.

Configurez le collecteur d’annuaires utilisateurs en saisissant les données requises dans les tableaux suivants :

Nom	Description
Nom	Nom unique pour le répertoire utilisateur. Par exemple *GlobalLDAPCollector*
Agent	Sélectionnez un agent configuré dans la liste
IP du serveur/nom de domaine	Adresse IP ou nom de domaine complet (FQDN) du serveur hébergeant le serveur d’annuaire LDAP
Base de recherche	Base de recherche du serveur LDAP Search Base autorise les deux formats suivants : *x.y.z* ⇒ nom de domaine direct tel que vous l’avez sur votre SVM. [Exemple : hq.companyname.com] *DC=x,DC=y,DC=z* ⇒ Noms distinctifs relatifs [Exemple : DC=hq,DC= companyname,DC=com] Ou vous pouvez spécifier comme suit : *OU=engineering,DC=hq,DC= companyname,DC=com* [pour filtrer par UO spécifique engineering] *CN=username,OU=engineering,DC=companyname, DC=netapp, DC=com* [pour obtenir uniquement l’utilisateur spécifique avec <username> de l’UO <engineering>] *CN=Acrobat Users,CN=Users,DC=hq,DC=companyname,DC=com ,O= companyname,L=Boston,S=MA,C=US* [pour obtenir tous les utilisateurs Acrobat au sein des utilisateurs de cette organisation]

Lier DN	L'utilisateur est autorisé à rechercher dans le répertoire. Par exemple : uid=ldapuser,cn=users,cn=accounts,dc=domain,dc=companyname,dc=com uid=john,cn=users,cn=accounts,dc=dorp,dc=company,dc=com pour un utilisateur john@dorp.company.com. dorp.company.com
--comptes	--utilisateurs
--John	--Anna
Mot de passe BIND	Mot de passe du serveur d'annuaire (c'est-à-dire le mot de passe du nom d'utilisateur utilisé dans Bind DN)
Protocole	ldap, ldaps, ldap-start-tls
Ports	Sélectionner le port

Saisissez les attributs requis du serveur d'annuaire suivants si les noms d'attributs par défaut ont été modifiés dans le serveur d'annuaire LDAP. Le plus souvent, ces noms d'attributs ne sont pas modifiés dans le serveur d'annuaire LDAP, auquel cas vous pouvez simplement continuer avec le nom d'attribut par défaut.

Attributs	Nom d'attribut dans Directory Server
Nom d'affichage	nom
UNIXID	numéro d'identifiant utilisateur
Nom d'utilisateur	uid

Cliquez sur Inclure les attributs facultatifs pour ajouter l'un des attributs suivants :

Attributs	Nom d'attribut dans le serveur d'annuaire
Adresse email	mail
Numéro de téléphone	numéro de téléphone
Rôle	titre
Pays	co
État	État
Département	numéro de département
Photo	photo
GestionnaireDN	directeur
Groupes	membreDe

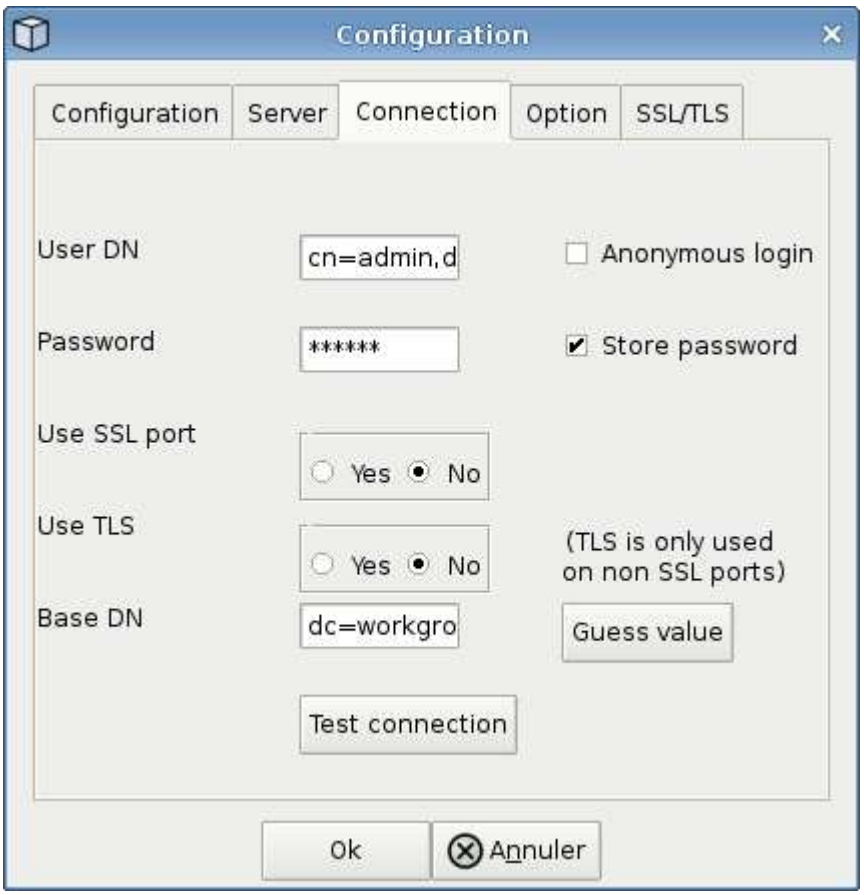
Test de la configuration de votre collecteur d'annuaires utilisateurs

Vous pouvez valider les autorisations utilisateur et les définitions d'attributs LDAP à l'aide des procédures suivantes :

- Utilisez la commande suivante pour valider l'autorisation de l'utilisateur LDAP de Workload Security :

```
 ldapsearch -D "uid=john
,cn=users,cn=accounts,dc=dorp,dc=company,dc=com" -W -x -LLL -o ldif-
wrap=no -b "cn=accounts,dc=dorp,dc=company,dc=com" -H
ldap://vmwipaapp08.dorp.company.com
* Utilisez LDAP Explorer pour naviguer dans une base de données LDAP,
afficher les propriétés et les attributs des objets, afficher les
autorisations, afficher le schéma d'un objet, exécuter des recherches
sophistiquées que vous pouvez enregistrer et réexécuter.
```

- Installer LDAP Explorer(http://ldaptool.sourceforge.net/) ou Java LDAP Explorer(http://jxplorer.org/) sur n'importe quelle machine Windows pouvant se connecter au serveur LDAP.
- Connectez-vous au serveur LDAP en utilisant le nom d'utilisateur/mot de passe du serveur d'annuaire LDAP.



Dépannage des erreurs de configuration du collecteur d'annuaires LDAP

Le tableau suivant décrit les problèmes connus et les résolutions qui peuvent survenir lors de la configuration du collecteur :

Problème:	Résolution:
L'ajout d'un connecteur d'annuaire LDAP génère l'état « Erreur ». L'erreur indique : « Informations d'identification non valides fournies pour le serveur LDAP ».	Nom unique de liaison, mot de passe de liaison ou base de recherche incorrects fournis. Modifiez et fournissez les informations correctes.
L'ajout d'un connecteur d'annuaire LDAP génère l'état « Erreur ». L'erreur indique : « Impossible d'obtenir l'objet correspondant à DN=DC=hq,DC=domainname,DC=com fourni comme nom de forêt. »	Base de recherche incorrecte fournie. Modifiez et fournissez le nom de forêt correct.
Les attributs facultatifs de l'utilisateur de domaine n'apparaissent pas dans la page Profil utilisateur de Workload Security.	Cela est probablement dû à une incompatibilité entre les noms des attributs facultatifs ajoutés dans CloudSecure et les noms d'attributs réels dans Active Directory. Les champs sont sensibles à la casse. Modifiez et fournissez le(s) nom(s) d'attribut facultatif(s) correct(s).
Collecteur de données dans un état d'erreur avec « Échec de la récupération des utilisateurs LDAP ». Motif de l'échec : Impossible de se connecter au serveur, la connexion est nulle.	Redémarrez le collecteur en cliquant sur le bouton *Redémarrer*.
L'ajout d'un connecteur d'annuaire LDAP génère l'état « Erreur ».	Assurez-vous d'avoir fourni des valeurs valides pour les champs obligatoires (serveur, nom de forêt, DN de liaison, mot de passe de liaison). Assurez-vous que l'entrée bind-DN est toujours fournie sous la forme uid=ldapuser,cn=users,cn=accounts,dc=domain,dc=companyname,dc=com.
L'ajout d'un connecteur d'annuaire LDAP entraîne l'état « RETRYING ». Affiche l'erreur « Échec de la détermination de l'état du collecteur, réessayez donc »	Assurez-vous que l'adresse IP du serveur et la base de recherche correctes sont fournies ////
Lors de l'ajout d'un annuaire LDAP, l'erreur suivante s'affiche : « Échec de la détermination de l'état du collecteur après 2 tentatives. Veuillez redémarrer le collecteur (code d'erreur : AGENT008) »	Assurez-vous que l'adresse IP du serveur et la base de recherche correctes sont fournies
L'ajout d'un connecteur d'annuaire LDAP entraîne l'état « RETRYING ». Affiche l'erreur « Impossible de définir l'état du collecteur, raison pour laquelle la commande TCP [Connect(localhost:35012,None,List(),Some(,seconds),true)] a échoué en raison de java.net.ConnectionException : connexion refusée. »	IP ou FQDN incorrect fourni pour le serveur AD. Modifiez et fournissez l'adresse IP ou le FQDN correct. ////
L'ajout d'un connecteur d'annuaire LDAP génère l'état « Erreur ». L'erreur indique : « Échec de l'établissement de la connexion LDAP ».	IP ou FQDN incorrect fourni pour le serveur LDAP. Modifiez et fournissez l'adresse IP ou le FQDN correct. Ou valeur incorrecte pour le port fourni. Essayez d'utiliser les valeurs de port par défaut ou le numéro de port correct pour le serveur LDAP.

Problème:	Résolution:
L'ajout d'un connecteur d'annuaire LDAP génère l'état « Erreur ». L'erreur indique : « Échec du chargement des paramètres. Motif : la configuration de la source de données comporte une erreur. Raison spécifique : /connector/conf/application.conf : 70 : ldap.ldap-port est de type STRING plutôt que NUMBER »	Valeur incorrecte pour le port fourni. Essayez d'utiliser les valeurs de port par défaut ou le numéro de port correct pour le serveur AD.
J'ai commencé avec les attributs obligatoires, et cela a fonctionné. Après avoir ajouté les attributs facultatifs, les données des attributs facultatifs ne sont pas récupérées à partir d'AD.	Cela est probablement dû à une incompatibilité entre les attributs facultatifs ajoutés dans CloudSecure et les noms d'attributs réels dans Active Directory. Modifiez et fournissez le nom d'attribut obligatoire ou facultatif correct.
Après le redémarrage du collecteur, quand la synchronisation LDAP aura-t-elle lieu ?	La synchronisation LDAP se produira immédiatement après le redémarrage du collecteur. Il faudra environ 15 minutes pour récupérer les données utilisateur d'environ 300 000 utilisateurs, et elles sont actualisées automatiquement toutes les 12 heures.
Les données utilisateur sont synchronisées depuis LDAP vers CloudSecure. Quand les données seront-elles supprimées ?	Les données utilisateur sont conservées pendant 13 mois en cas de non actualisation. Si le locataire est supprimé, les données seront supprimées.
Le connecteur d'annuaire LDAP génère l'état « Erreur ». "Le connecteur est en état d'erreur. Nom du service : usersLdap. Motif de l'échec : échec de la récupération des utilisateurs LDAP. Motif de l'échec : 80090308 : LdapErr : DSID-0C090453, commentaire : erreur AcceptSecurityContext, données 52e, v3839	Nom de forêt incorrect fourni. Voir ci-dessus comment fournir le nom de forêt correct.
Le numéro de téléphone n'est pas renseigné dans la page de profil utilisateur.	Cela est probablement dû à un problème de mappage d'attributs avec Active Directory. 1. Modifiez le collecteur Active Directory particulier qui récupère les informations de l'utilisateur à partir d'Active Directory. 2. Notez que sous les attributs facultatifs, il existe un nom de champ « Numéro de téléphone » mappé à l'attribut Active Directory « telephonenumber ». 4. Maintenant, utilisez l'outil Active Directory Explorer comme décrit ci-dessus pour parcourir le serveur d'annuaire LDAP et voir le nom d'attribut correct. 3. Assurez-vous que dans l'annuaire LDAP, il existe un attribut nommé « telephonenumber » qui contient bien le numéro de téléphone de l'utilisateur. 5. Disons que dans l'annuaire LDAP, il a été modifié en « numéro de téléphone ». 6. Modifiez ensuite le collecteur d'annuaires utilisateurs CloudSecure. Dans la section des attributs facultatifs, remplacez « telephonenumber » par « phonenumber ». 7. Enregistrez le collecteur Active Directory, le collecteur redémarrera et récupérera le numéro de téléphone de l'utilisateur et l'affichera dans la page de profil utilisateur.

Problème:	Résolution:
Si le certificat de chiffrement (SSL) est activé sur le serveur Active Directory (AD), le collecteur d'annuaires d'utilisateurs Workload Security ne peut pas se connecter au serveur AD.	Désactivez le chiffrement du serveur AD avant de configurer un collecteur d'annuaires utilisateurs. Une fois les détails de l'utilisateur récupérés, ils resteront là pendant 13 mois. Si le serveur AD est déconnecté après avoir récupéré les détails de l'utilisateur, les utilisateurs nouvellement ajoutés dans AD ne seront pas récupérés. Pour récupérer à nouveau, le collecteur de répertoires utilisateurs doit être connecté à AD.

Configuration du collecteur de données ONTAP SVM

Le collecteur de données ONTAP SVM permet à Workload Security de surveiller les activités d'accès aux fichiers et aux utilisateurs sur les machines virtuelles de stockage NetApp ONTAP (SVM). Ce guide vous guide à travers la configuration et la gestion du collecteur de données SVM pour fournir une surveillance de sécurité complète de votre environnement ONTAP .

Avant de commencer

- Ce collecteur de données est pris en charge avec les éléments suivants :
  - Data ONTAP 9.2 et versions ultérieures. Pour de meilleures performances, utilisez une version Data ONTAP supérieure à 9.13.1.
  - Protocole SMB version 3.1 et antérieure.
  - Versions NFS jusqu'à NFS 4.1 inclus (notez que NFS 4.1 est pris en charge avec ONTAP 9.15 ou version ultérieure).
  - Flexgroup est pris en charge à partir d' ONTAP 9.4 et des versions ultérieures
  - FlexCache est pris en charge pour NFS avec ONTAP 9.7 et les versions ultérieures.
  - FlexCache est pris en charge pour SMB avec ONTAP 9.14.1 et les versions ultérieures.
  - ONTAP Select est pris en charge
- Seuls les types de données SVM sont pris en charge. Les SVM avec des volumes infinis ne sont pas pris en charge.
- SVM comporte plusieurs sous-types. Parmi ceux-ci, seuls *default*, *sync_source* et *sync_destination* sont pris en charge.
- Un agent"doit être configuré" avant de pouvoir configurer les collecteurs de données.
- Assurez-vous que vous disposez d'un connecteur d'annuaire utilisateur correctement configuré, sinon les événements afficheront les noms d'utilisateur codés et non le nom réel de l'utilisateur (tel que stocké dans Active Directory) dans la page « Analyse forensique des activités ».
- ONTAP Persistent Store est pris en charge à partir de la version 9.14.1.
- Pour des performances optimales, vous devez configurer le serveur FPolicy pour qu'il soit sur le même sous-réseau que le système de stockage.
- Pour connaître les meilleures pratiques et recommandations complètes concernant la configuration de la stratégie FPolicy de sécurité des charges de travail, consultez le document suivant :"Article de la base de connaissances sur les meilleures pratiques FPolicy" .

- Vous devez ajouter un SVM en utilisant l'une des deux méthodes suivantes :
  - En utilisant l'adresse IP du cluster, le nom SVM et le nom d'utilisateur et le mot de passe de gestion du cluster. ***C'est la méthode recommandée.***
    - Le nom SVM doit être exactement tel qu'il est affiché dans ONTAP et est sensible à la casse.
  - En utilisant l'adresse IP, le nom d'utilisateur et le mot de passe de gestion du serveur virtuel SVM
  - Si vous ne pouvez pas ou ne souhaitez pas utiliser le nom d'utilisateur et le mot de passe complets de gestion du cluster/SVM de l'administrateur, vous pouvez créer un utilisateur personnalisé avec des privilèges moindres comme mentionné dans le« Une note sur les autorisations » section ci-dessous. Cet utilisateur personnalisé peut être créé pour l'accès SVM ou Cluster.
    - Vous pouvez également utiliser un utilisateur AD disposant d'un rôle possédant au moins les autorisations du rôle csrole, comme indiqué dans la section « Remarque concernant les autorisations » ci-dessous. Voir également le"Documentation ONTAP" .
- Assurez-vous que les applications correctes sont définies pour le SVM en exécutant la commande suivante :

```
clustershell:> security login show -vserver <vservername> -user-or-group
-name <username>
```

Exemple de sortie :

```
Vserver: svmname
                                                                  Second
User/Group                  Authentication                 Acct   Authentication
Name           Application  Method        Role Name        Locked Method
-------------- -----------  ------------- ---------------- ------ --------------
vsadmin        http         password      vsadmin          no     none
vsadmin        ontapi       password      vsadmin          no     none
vsadmin        ssh          password      vsadmin          no     none
3 entries were displayed.
```

- Assurez-vous que le SVM dispose d'un serveur CIFS configuré : clustershell:> `vserver cifs show`

  Le système renvoie le nom du serveur virtuel, le nom du serveur CIFS et des champs supplémentaires.

- Définissez un mot de passe pour l'utilisateur SVM vsadmin. Si vous utilisez un utilisateur personnalisé ou un utilisateur administrateur de cluster, ignorez cette étape. clustershell:> `security login password -username vsadmin -vserver svmname`
- Déverrouillez l'utilisateur SVM vsadmin pour l'accès externe. Si vous utilisez un utilisateur personnalisé ou un utilisateur administrateur de cluster, ignorez cette étape. clustershell:> `security login unlock -username vsadmin -vserver svmname`
- Assurez-vous que la politique de pare-feu du LIF de données est définie sur « mgmt » (et non sur « données »). Ignorez cette étape si vous utilisez un LIF de gestion dédié pour ajouter le SVM. clustershell:> `network interface modify -lif <SVM_data_LIF_name> -firewall-policy mgmt`
- Lorsqu'un pare-feu est activé, vous devez définir une exception pour autoriser le trafic TCP pour le port à l'aide du collecteur de données Data Data ONTAP .

Voir"Exigences relatives aux agents" pour les informations de configuration. Ceci s'applique aux agents sur site et aux agents installés dans le Cloud.

- Lorsqu'un agent est installé dans une instance AWS EC2 pour surveiller une SVM Cloud ONTAP , l'agent et le stockage doivent se trouver dans le même VPC. S'ils se trouvent dans des VPC distincts, il doit y avoir un itinéraire valide entre les VPC.

Tester la connectivité pour les collecteurs de données

La fonctionnalité de connectivité de test (introduite en mars 2025) vise à aider les utilisateurs finaux à identifier les causes spécifiques des échecs lors de la configuration des collecteurs de données dans Data Infrastructure Insights (DII) Workload Security. Cela permet aux utilisateurs de corriger eux-mêmes les problèmes liés à la communication réseau ou aux rôles manquants.

Cette fonctionnalité aidera les utilisateurs à déterminer si tous les contrôles liés au réseau sont en place avant de configurer un collecteur de données. De plus, il informera les utilisateurs des fonctionnalités auxquelles ils peuvent accéder en fonction de la version ONTAP , des rôles et des autorisations qui leur sont attribués dans ONTAP.

La connectivité de test n'est pas prise en charge pour les collecteurs d'annuaires utilisateurs

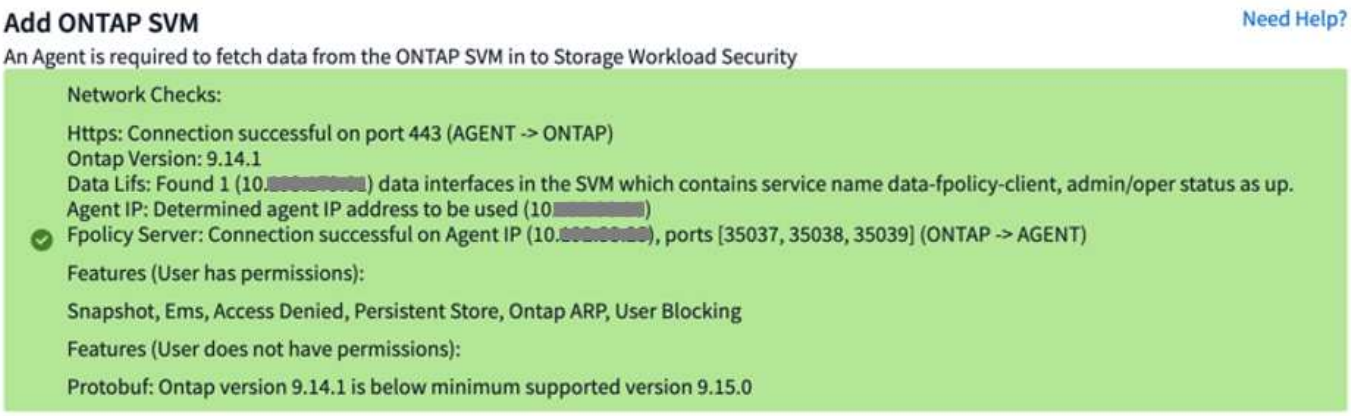
Conditions préalables aux tests de connexion

- Les informations d'identification au niveau du cluster sont nécessaires pour que cette fonctionnalité fonctionne pleinement.
- La vérification de l'accès aux fonctionnalités n'est pas prise en charge en mode SVM.
- Si vous utilisez les informations d'identification d'administration de cluster, aucune nouvelle autorisation n'est nécessaire.
- Si vous utilisez un utilisateur personnalisé (par exemple, *csuser*), fournissez les autorisations obligatoires et les autorisations spécifiques aux fonctionnalités que vous souhaitez utiliser.

Assurez-vous de revoir leAutorisations section ci-dessous également.

Tester la connexion

L'utilisateur peut accéder à la page d'ajout/modification du collecteur, saisir les détails du niveau du cluster (en mode cluster) ou les détails du niveau SVM (en mode SVM) et cliquer sur le bouton **Tester la connexion**. Workload Security traitera ensuite la demande et affichera un message de réussite ou d'échec approprié.



Points à noter pour ONTAP Multi Admin Verify (MAV)

Certaines fonctionnalités, telles que la création et la suppression d'instantanés ou le blocage des utilisateurs (SMB), peuvent ne pas fonctionner en fonction des commandes MAV ajoutées dans votre version de ONTAP.

Suivez les étapes ci-dessous pour ajouter des exclusions à vos commandes MAV afin de permettre à Workload Security de créer ou de supprimer des instantanés et de bloquer des utilisateurs.

Commandes pour autoriser la création et la suppression d'instantanés :

```
multi-admin-verify rule modify -operation "volume snapshot create" -query
"-snapshot !*cloudsecure_*"
multi-admin-verify rule modify -operation "volume snapshot delete" -query
"-snapshot !*cloudsecure_*"
```

Commande pour autoriser le blocage des utilisateurs :

```
multi-admin-verify rule delete -operation set
```

Conditions préalables au blocage de l'accès utilisateur

Gardez à l'esprit les points suivants pour"Blocage de l'accès utilisateur" :

Les informations d'identification au niveau du cluster sont nécessaires pour que cette fonctionnalité fonctionne.

Si vous utilisez les informations d'identification d'administration de cluster, aucune nouvelle autorisation n'est nécessaire.

Si vous utilisez un utilisateur personnalisé (par exemple, *csuser*) avec des autorisations accordées à l'utilisateur, suivez les étapes de"Blocage de l'accès utilisateur" pour donner des autorisations à Workload Security pour bloquer l'utilisateur.

Remarque sur les autorisations

Autorisations lors de l'ajout via Cluster Management IP :

Si vous ne pouvez pas utiliser l'utilisateur administrateur de gestion de cluster pour autoriser Workload Security à accéder au collecteur de données ONTAP SVM, vous pouvez créer un nouvel utilisateur nommé « csuser » avec les rôles indiqués dans les commandes ci-dessous. Utilisez le nom d'utilisateur « csuser » et le mot de passe « csuser » lors de la configuration du collecteur de données Workload Security pour utiliser l'adresse IP de gestion de cluster.

Remarque : vous pouvez créer un rôle unique à utiliser pour toutes les autorisations de fonctionnalités pour un utilisateur personnalisé. S'il existe un utilisateur existant, supprimez d'abord l'utilisateur et le rôle existants à l'aide de ces commandes :

```
security login delete -user-or-group-name csuser -application *
security login role delete -role csrole -cmddirname *
security login rest-role delete -role csrestrole -api *
security login rest-role delete -role arwrole -api *
```

Pour créer le nouvel utilisateur, connectez-vous à ONTAP avec le nom d'utilisateur/mot de passe de l'administrateur de gestion de cluster et exécutez les commandes suivantes sur le serveur ONTAP :

```
security login role create -role csrole -cmddirname DEFAULT -access
readonly
```

```
security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
security login role create -role csrole -cmddirname "volume snapshot"
-access all -query "-snapshot cloudsecure_*"
security login role create -role csrole -cmddirname "event catalog"
-access all
security login role create -role csrole -cmddirname "event filter" -access
all
security login role create -role csrole -cmddirname "event notification
destination" -access all
security login role create -role csrole -cmddirname "event notification"
-access all
security login role create -role csrole -cmddirname "security certificate"
-access all
security login role create -role csrole -cmddirname "cluster application-
record" -access all
security login create -user-or-group-name csuser -application ontapi
-authmethod password -role csrole
security login create -user-or-group-name csuser -application ssh
-authmethod password -role csrole
security login create -user-or-group-name csuser -application http
-authmethod password -role csrole
```

Autorisations lors de l'ajout via Vserver Management IP :

Si vous ne pouvez pas utiliser l'utilisateur administrateur de gestion de cluster pour autoriser Workload Security à accéder au collecteur de données ONTAP SVM, vous pouvez créer un nouvel utilisateur nommé « csuser » avec les rôles indiqués dans les commandes ci-dessous. Utilisez le nom d'utilisateur « csuser » et le mot de passe « csuser » lors de la configuration du collecteur de données Workload Security pour utiliser l'adresse IP de gestion du serveur virtuel.

Remarque : vous pouvez créer un rôle unique à utiliser pour toutes les autorisations de fonctionnalités pour un utilisateur personnalisé. S'il existe un utilisateur existant, supprimez d'abord l'utilisateur et le rôle existants à l'aide de ces commandes :

```
security login delete -user-or-group-name csuser -application * -vserver
<vservername>
security login role delete -role csrole -cmddirname * -vserver
<vservername>
security login rest-role delete -role csrestrole -api * -vserver
<vservername>
```

Pour créer le nouvel utilisateur, connectez-vous à ONTAP avec le nom d'utilisateur/mot de passe de l'administrateur de gestion de cluster et exécutez les commandes suivantes sur le serveur ONTAP . Pour plus de simplicité, copiez ces commandes dans un éditeur de texte et remplacez <vservername> par le nom de votre Vserver avant d'exécuter ces commandes sur ONTAP:

```
security login role create -vserver <vservername> -role csrole -cmddirname
DEFAULT -access none
```

```
security login role create -vserver <vservername> -role csrole -cmddirname
"network interface" -access readonly
security login role create -vserver <vservername> -role csrole -cmddirname
version -access readonly
security login role create -vserver <vservername> -role csrole -cmddirname
volume -access readonly
security login role create -vserver <vservername> -role csrole -cmddirname
vserver -access readonly
```

```
security login role create -vserver <vservername> -role csrole -cmddirname
"vserver fpolicy" -access all
security login role create -vserver <vservername> -role csrole -cmddirname
"volume snapshot" -access all
```

```
security login create -user-or-group-name csuser -application ontapi
-authmethod password -role csrole -vserver <vservername>
security login create -user-or-group-name csuser -application http
-authmethod password -role csrole -vserver <vservername>
```

Mode Protobuf

Workload Security configurera le moteur FPolicy en mode protobuf lorsque cette option est activée dans les paramètres *Configuration avancée* du collecteur. Le mode Protobuf est pris en charge dans ONTAP version 9.15 et ultérieure.

Vous trouverez plus de détails sur cette fonctionnalité dans le"Documentation ONTAP" .

Des autorisations spécifiques sont requises pour protobuf (certaines ou toutes peuvent déjà exister) :

Mode cluster :

```
 security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
Mode serveur virtuel :
```

```
security login role create -vserver <vservername> -role csrole -cmddirname
"vserver fpolicy" -access all
```

Autorisations pour la protection autonome contre les ransomwares ONTAP et accès ONTAP refusé

Si vous utilisez les informations d'identification d'administration de cluster, aucune nouvelle autorisation n'est nécessaire.

Si vous utilisez un utilisateur personnalisé (par exemple, *csuser*) avec des autorisations accordées à l'utilisateur, suivez les étapes ci-dessous pour accorder des autorisations à Workload Security afin de collecter des informations liées à ARP à partir d' ONTAP.

Pour plus d'informations, lisez à propos de"Intégration avec ONTAP Accès refusé"

et"Intégration avec la protection autonome contre les ransomwares ONTAP"

Configurer le collecteur de données

Étapes de configuration

1. Connectez-vous en tant qu'administrateur ou propriétaire de compte à votre environnement Data Infrastructure Insights .
2. Cliquez sur **Sécurité de la charge de travail > Collecteurs > +Collecteurs de données**

   Le système affiche les collecteurs de données disponibles.

3. Passez la souris sur la mosaïque * NetApp SVM et cliquez sur **+Surveiller**.

Le système affiche la page de configuration ONTAP SVM. Saisissez les données requises pour chaque champ.

Champ	Description
Nom	Nom unique pour le collecteur de données
Agent	Sélectionnez un agent configuré dans la liste.
Connectez-vous via l'IP de gestion pour :	Sélectionnez l'adresse IP du cluster ou l'adresse IP de gestion SVM
Adresse IP de gestion du cluster / SVM	L'adresse IP du cluster ou du SVM, selon votre sélection ci-dessus.
Nom de SVM	Le nom du SVM (ce champ est obligatoire lors de la connexion via l'IP du cluster)
Nom d'utilisateur	Nom d'utilisateur pour accéder au SVM/Cluster Lors de l'ajout via l'IP du cluster, les options sont : 1. Administrateur de cluster 2. 'csutilisateur' 3. Utilisateur AD ayant un rôle similaire à csuser. Lors de l'ajout via SVM IP, les options sont : 4. vsadmin 5. 'csutilisateur' 6. Nom d'utilisateur AD ayant un rôle similaire à csuser.
Mot de passe	Mot de passe pour le nom d'utilisateur ci-dessus
Filtrer les parts/volumes	Choisissez d'inclure ou d'exclure les actions/volumes de la collecte d'événements
Saisissez les noms de partage complets à exclure/inclure	Liste séparée par des virgules des partages à exclure ou à inclure (selon le cas) de la collecte d'événements
Saisissez les noms de volumes complets à exclure/inclure	Liste séparée par des virgules des volumes à exclure ou à inclure (selon le cas) de la collecte d'événements
Surveiller l'accès aux dossiers	Lorsque cette option est cochée, elle active les événements pour la surveillance de l'accès aux dossiers. Notez que la création/le changement de nom et la suppression des dossiers seront surveillés même sans cette option sélectionnée. L'activation de cette option augmentera le nombre d'événements surveillés.
Définir la taille du tampon d'envoi ONTAP	Définit la taille du tampon d'envoi ONTAP Fpolicy. Si une version ONTAP antérieure à 9.8p7 est utilisée et qu'un problème de performances est constaté, la taille du tampon d'envoi ONTAP peut être modifiée pour obtenir de meilleures performances ONTAP . Contactez le support NetApp si vous ne voyez pas cette option et souhaitez l'explorer.

Après avoir terminé

- Dans la page Collecteurs de données installés, utilisez le menu d'options à droite de chaque collecteur pour modifier le collecteur de données. Vous pouvez redémarrer le collecteur de données ou modifier les attributs de configuration du collecteur de données.

Configuration recommandée pour MetroCluster

Ce qui suit est recommandé pour MetroCluster:

1. Connectez deux collecteurs de données, l'un au SVM source et l'autre au SVM de destination.
2. Les collecteurs de données doivent être connectés par *Cluster IP*.
3. À tout moment, le collecteur de données du SVM « en cours d'exécution » s'affichera comme *Running*. Le collecteur de données du SVM « arrêté » actuel s'affichera comme *Arrêté*.
4. À chaque basculement, l'état du collecteur de données passe de *Running* à *Stopped* et vice versa.
5. Il faudra jusqu'à deux minutes au collecteur de données pour passer de l'état *Arrêté* à l'état *En cours d'exécution*.

Politique de service

Si vous utilisez la stratégie de service avec ONTAP **version 9.9.1 ou plus récente**, afin de vous connecter au collecteur de sources de données, le service *data-fpolicy-client* est requis avec le service de données *data-nfs* et/ou *data-cifs*.

Exemple:

```
Testcluster-1:*> net int service-policy create -policy only_data_fpolicy
-allowed-addresses 0.0.0.0/0 -vserver aniket_svm
-services data-cifs,data-nfs,data,-core,data-fpolicy-client
(network interface service-policy create)
```

Dans les versions d' ONTAP antérieures à 9.9.1, *data-fpolicy-client* n'a pas besoin d'être défini.

Collecteur de données de lecture-pause

Si le collecteur de données est à l'état *En cours d'exécution*, vous pouvez suspendre la collecte. Ouvrez le menu « trois points » du collecteur et sélectionnez PAUSE. Pendant que le collecteur est en pause, aucune donnée n'est collectée à partir d' ONTAP et aucune donnée n'est envoyée du collecteur à ONTAP. Cela signifie qu'aucun événement Fpolicy ne circulera d' ONTAP vers le collecteur de données, et de là vers Data Infrastructure Insights.

Notez que si de nouveaux volumes, etc. sont créés sur ONTAP alors que le collecteur est en pause, Workload Security ne collectera pas les données et ces volumes, etc. ne seront pas reflétés dans les tableaux de bord ou les tables.

Un collecteur ne peut pas être mis en pause s'il a des utilisateurs restreints. Restaurez l'accès utilisateur avant de suspendre le collecteur.

Gardez à l'esprit les points suivants :

- La purge des instantanés ne se produira pas selon les paramètres configurés sur un collecteur en pause.
- Les événements EMS (comme ONTAP ARP) ne seront pas traités sur un collecteur suspendu. Cela signifie que si ONTAP identifie une attaque de falsification de fichier, Data Infrastructure Insights Workload Security ne pourra pas acquérir cet événement.
- Les e-mails de notifications de santé ne seront PAS envoyés pour un collecteur en pause.

- Les actions manuelles ou automatiques (telles que le snapshot ou le blocage d'utilisateur) ne seront pas prises en charge sur un collecteur en pause.
- Lors des mises à niveau de l'agent ou du collecteur, des redémarrages/redémarrages de la machine virtuelle de l'agent ou du redémarrage du service de l'agent, un collecteur en pause restera dans l'état *Paused*.
- Si le collecteur de données est dans l'état *Erreur*, le collecteur ne peut pas être modifié en état *En pause*. Le bouton Pause ne sera activé que si l'état du collecteur est *Running*.
- Si l'agent est déconnecté, le collecteur ne peut pas être modifié en état *Paused*. Le collecteur passera à l'état *Arrêté* et le bouton Pause sera désactivé.

Magasin persistant

Le magasin persistant est pris en charge avec ONTAP 9.14.1 et versions ultérieures. Notez que les instructions de nom de volume varient d' ONTAP 9.14 à 9.15.

Le magasin persistant peut être activé en sélectionnant la case à cocher dans la page d'édition/ajout du collecteur. Après avoir coché la case, un champ de texte s'affiche pour accepter le nom du volume. Le nom du volume est un champ obligatoire pour activer le magasin persistant.

- Pour ONTAP 9.14.1, vous devez créer le volume avant d'activer la fonctionnalité et fournir le même nom dans le champ *Nom du volume*. La taille de volume recommandée est de 16 Go.
- Pour ONTAP 9.15.1, le volume sera créé automatiquement avec une taille de 16 Go par le collecteur, en utilisant le nom fourni dans le champ *Nom du volume*.

Des autorisations spécifiques sont requises pour le magasin persistant (certaines ou toutes ces autorisations peuvent déjà exister) :

Mode cluster :

```
security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
security login role create -role csrole -cmddirname "job show" -access
readonly
```

Mode serveur virtuel :

```
security login role create -vserver <vservername> -role csrole -cmddirname
"vserver fpolicy" -access all
security login role create -vserver <vservername> -role csrole -cmddirname
"job show" -access readonly
```

Migrer les collecteurs

Vous pouvez facilement migrer un collecteur Workload Security d'un agent à un autre, permettant ainsi un équilibrage efficace de la charge des collecteurs entre les agents.

Prérequis

- L'agent source doit être dans l'état *connecté*.
- Le collecteur à migrer doit être dans l'état *running*.

Note:

- Migrate est pris en charge pour les collecteurs de données et d'annuaires d'utilisateurs.
- La migration d'un collecteur n'est pas prise en charge pour les locataires gérés manuellement.

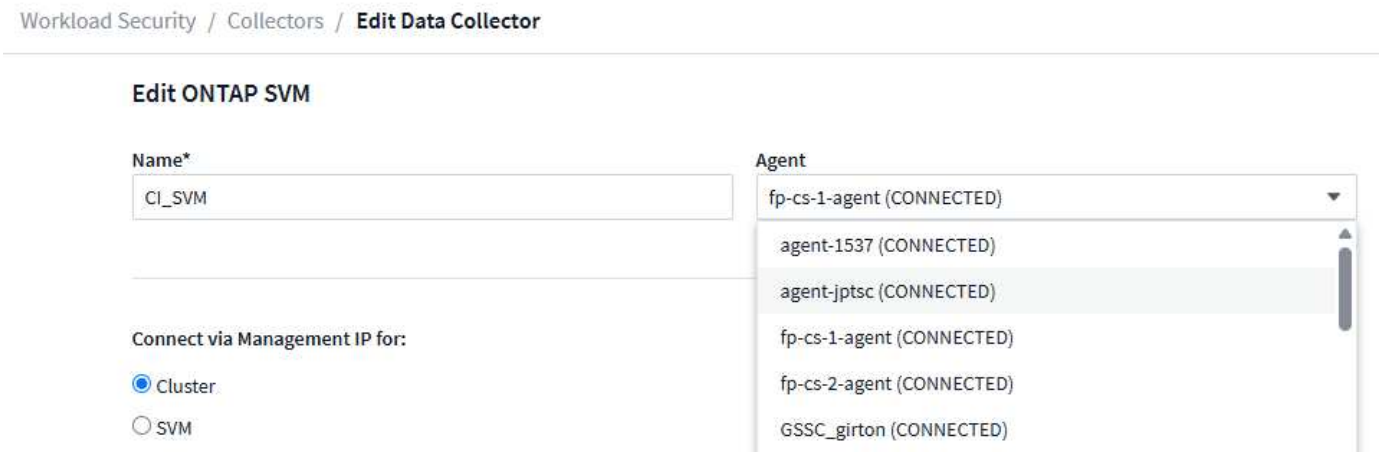
Migrer le collecteur

Pour migrer un collecteur, suivez ces étapes :

1. Accédez à la page « Modifier le collecteur ».
2. Sélectionnez un agent de destination dans la liste déroulante des agents.
3. Cliquez sur le bouton « Enregistrer le collecteur ».

Workload Security traitera la demande. Une fois la migration réussie, l'utilisateur sera redirigé vers la page de la liste des collecteurs. En cas d'échec, un message approprié sera affiché sur la page d'édition.

Remarque : toutes les modifications de configuration précédemment effectuées sur la page « Modifier le collecteur » resteront appliquées lorsque le collecteur sera migré avec succès vers l'agent de destination.



Dépannage

Voir le"Dépannage du collecteur SVM" page pour des conseils de dépannage.

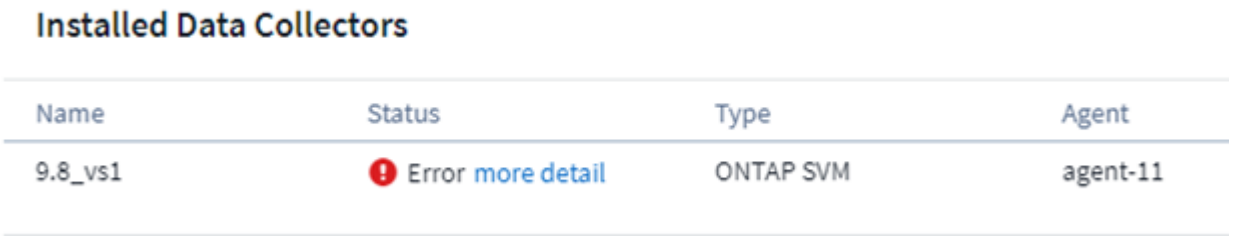
Dépannage du collecteur de données ONTAP SVM

Workload Security utilise des collecteurs de données pour collecter les données d'accès aux fichiers et aux utilisateurs à partir des appareils. Vous trouverez ici des conseils pour résoudre les problèmes liés à ce collecteur.

Voir le"Configuration du collecteur SVM" page pour obtenir des instructions sur la configuration de ce collecteur.

En cas d'erreur, vous pouvez cliquer sur *plus de détails* dans la colonne *Statut* de la page Collecteurs de

données installés pour obtenir des détails sur l'erreur.



Les problèmes connus et leurs résolutions sont décrits ci-dessous.

Problème : le collecteur de données s'exécute pendant un certain temps et s'arrête après un temps aléatoire, échouant avec : « Message d'erreur : le connecteur est en état d'erreur. Nom du service : audit. Motif de l'échec : serveur fpolicy externe surchargé. **Essayez ceci :** le taux d'événements d' ONTAP était bien supérieur à ce que la boîte d'agent peut gérer. La connexion a donc été interrompue.

Vérifiez le trafic de pointe dans CloudSecure lorsque la déconnexion s'est produite. Vous pouvez le vérifier à partir de la page **CloudSecure > Analyse forensique des activités > Toutes les activités**.

Si le trafic agrégé de pointe est supérieur à ce que l'Agent Box peut gérer, reportez-vous à la page du vérificateur de taux d'événements pour savoir comment dimensionner le déploiement du collecteur dans une Agent Box.

Si l'agent a été installé dans la boîte Agent avant le 4 mars 2021, exécutez les commandes suivantes dans la boîte Agent :

```
echo 'net.core.rmem_max=8388608' >> /etc/sysctl.conf
echo 'net.ipv4.tcp_rmem = 4096 2097152 8388608' >> /etc/sysctl.conf
sysctl -p
```

Redémarrez le collecteur à partir de l'interface utilisateur après le redimensionnement.

{vider}

Problème : le collecteur signale le message d'erreur : « Aucune adresse IP locale trouvée sur le connecteur pouvant atteindre les interfaces de données du SVM ». **Essayez ceci :** cela est probablement dû à un problème de réseau côté ONTAP . Veuillez suivre ces étapes :

1. Assurez-vous qu'il n'y a pas de pare-feu sur le LIF de données SVM ou sur le LIF de gestion qui bloque la connexion depuis le SVM.
2. Lors de l'ajout d'un SVM via une adresse IP de gestion de cluster, assurez-vous que la durée de vie des données et la durée de vie de gestion du SVM sont pingables à partir de la machine virtuelle de l'agent. En cas de problème, vérifiez la passerelle, le masque de réseau et les routes du lif.

   Vous pouvez également essayer de vous connecter au cluster via ssh à l'aide de l'adresse IP de gestion du cluster et d'envoyer une requête ping à l'adresse IP de l'agent. Assurez-vous que l'adresse IP de l'agent est pingable :

```
network ping -vserver <vserver name> -destination <Agent IP> -lif <Lif
Name> -show-detail
```

Si le ping n'est pas possible, assurez-vous que les paramètres réseau dans ONTAP sont corrects, afin que la machine de l'agent soit pingable.

3. Si vous avez essayé de vous connecter via l'IP du cluster et que cela ne fonctionne pas, essayez de vous connecter directement via l'IP SVM. Veuillez consulter ci-dessus les étapes de connexion via l'IP SVM.
4. Lors de l'ajout du collecteur via l'adresse IP SVM et les informations d'identification vsadmin, vérifiez si le rôle Données plus Gestion du SVM est activé. Dans ce cas, le ping vers le SVM Lif fonctionnera, mais le SSH vers le SVM Lif ne fonctionnera pas. Si oui, créez un Lif de gestion SVM uniquement et essayez de vous connecter via ce Lif de gestion SVM uniquement.
5. Si cela ne fonctionne toujours pas, créez un nouveau Lif SVM et essayez de vous connecter via ce Lif. Assurez-vous que le masque de sous-réseau est correctement défini.
6. Débogage avancé :
   a. Démarrer une trace de paquets dans ONTAP.
   b. Essayez de connecter un collecteur de données au SVM à partir de l'interface utilisateur CloudSecure.
   c. Attendez que l'erreur apparaisse. Arrêtez le suivi des paquets dans ONTAP.
   d. Ouvrez la trace des paquets depuis ONTAP. Il est disponible à cet endroit

```
 https://<cluster_mgmt_ip>/spi/<clustername>/etc/log/packet_traces/
.. Assurez-vous qu'il existe un SYN d' ONTAP vers la boîte Agent.
.. S'il n'y a pas de SYN d' ONTAP , il s'agit d'un problème de pare-
feu dans ONTAP.
.. Ouvrez le pare-feu dans ONTAP, afin ONTAP puisse connecter la
boîte d'agent.
```

7. Si cela ne fonctionne toujours pas, veuillez consulter l'équipe réseau pour vous assurer qu'aucun pare-feu externe ne bloque la connexion d' ONTAP au boîtier Agent.
8. Si aucune des solutions ci-dessus ne résout le problème, ouvrez un dossier avec"Assistance Netapp" pour obtenir de l'aide.

{vider}

Problème : Message : « Échec de la détermination du type ONTAP pour [nom d'hôte : <adresse IP>. Raison : Erreur de connexion au système de stockage <Adresse IP> : L'hôte est inaccessible (Hôte inaccessible)"
Essayez ceci :

1. Vérifiez que l'adresse IP de gestion SVM ou l'adresse IP de gestion de cluster correcte a été fournie.
2. Connectez-vous en SSH au SVM ou au cluster auquel vous souhaitez vous connecter. Une fois connecté, assurez-vous que le nom du SVM ou du cluster est correct.

{vider}

Problème : Message d'erreur : « Le connecteur est dans un état d'erreur. Service.nom : audit. Motif de l'échec : serveur fpolicy externe arrêté. **Essayez ceci :**

1. Il est très probable qu'un pare-feu bloque les ports nécessaires sur la machine agent. Vérifiez que la plage de ports 35000-55000/tcp est ouverte pour que la machine agent se connecte à partir du SVM. Assurez-vous également qu'aucun pare-feu n'est activé côté ONTAP bloquant la communication avec la machine agent.
2. Tapez la commande suivante dans la zone Agent et assurez-vous que la plage de ports est ouverte.

   ```
   sudo iptables-save | grep 3500*
   ```

   Un exemple de sortie devrait ressembler à :

   ```
    -A IN_public_allow -p tcp -m tcp --dport 35000 -m conntrack -ctstate
   NEW -j ACCEPT
   . Connectez-vous à SVM, entrez les commandes suivantes et vérifiez
   qu'aucun pare-feu n'est configuré pour bloquer la communication avec
   ONTAP.
   ```

   ```
   system services firewall show
   system services firewall policy show
   ```

   "Vérifier les commandes du pare-feu"du côté ONTAP .

3. Connectez-vous en SSH au SVM/cluster que vous souhaitez surveiller. Envoyez une requête ping à la boîte Agent à partir de la bibliothèque de données SVM (avec prise en charge des protocoles CIFS et NFS) et assurez-vous que la requête ping fonctionne :

   ```
   network ping -vserver <vserver name> -destination <Agent IP> -lif <Lif
   Name> -show-detail
   ```

   Si le ping n'est pas possible, assurez-vous que les paramètres réseau dans ONTAP sont corrects, afin que la machine de l'agent soit pingable.

4. Si un seul SVM est ajouté deux fois à un locataire via 2 collecteurs de données, cette erreur s'affichera. Supprimez l'un des collecteurs de données via l'interface utilisateur. Redémarrez ensuite l'autre collecteur de données via l'interface utilisateur. Ensuite, le collecteur de données affichera le statut « EN COURS D'EXÉCUTION » et commencera à recevoir des événements de SVM.

   Fondamentalement, dans un locataire, 1 SVM ne doit être ajouté qu'une seule fois, via 1 collecteur de données. 1 SVM ne doit pas être ajouté deux fois via 2 collecteurs de données.

5. Dans les cas où le même SVM a été ajouté dans deux environnements de sécurité de charge de travail différents (locataires), le dernier réussira toujours. Le deuxième collecteur configurera fpolicy avec sa propre adresse IP et expulsera le premier. Ainsi, le collecteur du premier cessera de recevoir des événements et son service « audit » entrera en état d'erreur. Pour éviter cela, configurez chaque SVM sur

un seul environnement.

6. Cette erreur peut également se produire si les stratégies de service ne sont pas configurées correctement. Avec ONTAP 9.8 ou version ultérieure, pour se connecter au collecteur de sources de données, le service data-fpolicy-client est requis avec le service de données data-nfs et/ou data-cifs. De plus, le service data-fpolicy-client doit être associé aux données lif pour le SVM surveillé.

{vider}

Problème : Aucun événement n'est visible sur la page d'activité. **Essayez ceci :**

1. Vérifiez si le collecteur ONTAP est à l'état « RUNNING ». Si oui, assurez-vous que certains événements cifs sont générés sur les machines virtuelles clientes cifs en ouvrant certains fichiers.
2. Si aucune activité n'est observée, connectez-vous au SVM et entrez la commande suivante.

   ```
   <SVM>event log show -source fpolicy
   ```

   Veuillez vous assurer qu'il n'y a pas d'erreurs liées à fpolicy.

3. Si aucune activité n'est visible, veuillez vous connecter au SVM. Entrez la commande suivante :

   ```
   <SVM>fpolicy show
   ```

   Vérifiez si la politique fpolicy nommée avec le préfixe « cloudsecure_ » a été définie et si le statut est « on ». Si cette option n'est pas définie, il est fort probable que l'agent ne puisse pas exécuter les commandes dans la SVM. Veuillez vous assurer que toutes les conditions préalables décrites au début de la page ont été respectées.

{vider}

Problème : Le collecteur de données SVM est en état d'erreur et le message d'erreur est « L'agent n'a pas réussi à se connecter au collecteur » **Essayez ceci :**

1. Il est fort probable que l'agent soit surchargé et ne parvienne pas à se connecter aux collecteurs de sources de données.
2. Vérifiez combien de collecteurs de sources de données sont connectés à l'agent.
3. Vérifiez également le débit de données dans la page « Toutes les activités » de l'interface utilisateur.
4. Si le nombre d'activités par seconde est considérablement élevé, installez un autre agent et déplacez certains des collecteurs de sources de données vers le nouvel agent.

{vider}

Problème : le collecteur de données SVM affiche le message d'erreur suivant : « fpolicy.server.connectError : le nœud n'a pas pu établir de connexion avec le serveur FPolicy « 12.195.15.146 » (raison : « Sélection

expirée ») » **Essayez ceci :** le pare-feu est activé dans SVM/Cluster. Le moteur fpolicy ne peut donc pas se connecter au serveur fpolicy. Les CLI dans ONTAP qui peuvent être utilisées pour obtenir plus d'informations sont :

```
event log show -source fpolicy which shows the error
event log show -source fpolicy -fields event,action,description which
shows more details.
```

"Vérifier les commandes du pare-feu"du côté ONTAP .

{vider}

Problème : Message d'erreur : « Le connecteur est dans un état d'erreur. Nom du service : audit. Motif de l'échec : Aucune interface de données valide (rôle : données, protocoles de données : NFS ou CIFS ou les deux, état : actif) trouvée sur la SVM. **Essayez ceci :** Assurez-vous qu'il existe une interface opérationnelle (ayant un rôle de données et un protocole de données comme CIFS/NFS).

{vider}

Problème : le collecteur de données passe à l'état d'erreur, puis passe à l'état d'exécution après un certain temps, puis revient à l'état d'erreur. Ce cycle se répète. **Essayez ceci :** Cela se produit généralement dans le scénario suivant :

1. Plusieurs collecteurs de données ont été ajoutés.
2. Les collecteurs de données qui présentent ce type de comportement auront 1 SVM ajouté à ces collecteurs de données. Cela signifie que 2 ou plusieurs collecteurs de données sont connectés à 1 SVM.
3. Assurez-vous qu'un seul collecteur de données se connecte à un seul SVM.
4. Supprimez les autres collecteurs de données connectés au même SVM.

{vider}

Problème : le connecteur est dans un état d'erreur. Nom du service : audit. Motif de l'échec : échec de la configuration (politique sur SVM svmname. Motif : Valeur non valide spécifiée pour l'élément « shares-to-include » dans « fpolicy.policy.scope-modify : « Federal » **Essayez ceci :** *Les noms de partage doivent être indiqués sans guillemets. Modifiez la configuration DSC ONTAP SVM pour corriger les noms de partage.

Inclure et exclure des partages n'est pas destiné à une longue liste de noms de partages. Utilisez plutôt le filtrage par volume si vous avez un grand nombre d'actions à inclure ou à exclure.

{vider}

Problème : il existe des fpolicies existantes dans le cluster qui ne sont pas utilisées. Que faut-il faire avec ceux-ci avant l'installation de Workload Security ? **Essayez ceci :** Il est recommandé de supprimer tous les paramètres fpolicy inutilisés existants, même s'ils sont dans un état déconnecté. Workload Security créera

fpolicy avec le préfixe « cloudsecure_ ». Toutes les autres configurations fpolicy inutilisées peuvent être supprimées.

Commande CLI pour afficher la liste fpolicy :

```
 fpolicy show
Étapes pour supprimer les configurations fpolicy :
```

```
fpolicy disable -vserver <svmname> -policy-name <policy_name>
fpolicy policy scope delete -vserver <svmname> -policy-name <policy_name>
fpolicy policy delete -vserver <svmname> -policy-name <policy_name>
fpolicy policy event delete -vserver <svmname> -event-name <event_list>
fpolicy policy external-engine delete -vserver <svmname> -engine-name
<engine_name>
```

{vider}

Problème : Après l'activation de la sécurité des charges de travail, les performances ONTAP sont affectées : la latence devient sporadiquement élevée et les IOPS deviennent sporadiquement faibles. **Essayez ceci :** Lors de l'utilisation ONTAP avec Workload Security, des problèmes de latence peuvent parfois être observés dans ONTAP. Plusieurs raisons peuvent expliquer cela, comme indiqué ci-dessous :"1372994" , "1415152" , "1438207" , "1479704" , "1354659" . Tous ces problèmes sont résolus dans ONTAP 9.13.1 et versions ultérieures ; il est fortement recommandé d'utiliser l'une de ces versions ultérieures.

{vider}

Problème : le collecteur de données affiche le message d'erreur : « Erreur : échec de la détermination de l'état du collecteur en 2 tentatives, essayez de redémarrer le collecteur (code d'erreur : AGENT008) ». **Essayez ceci :**

1. Sur la page Collecteurs de données, faites défiler vers la droite du collecteur de données générant l'erreur et cliquez sur le menu à 3 points. Sélectionnez *Modifier*. Saisissez à nouveau le mot de passe du collecteur de données. Enregistrez le collecteur de données en appuyant sur le bouton *Enregistrer*. Le collecteur de données redémarrera et l'erreur devrait être résolue.
2. Il se peut que la machine Agent ne dispose pas de suffisamment de CPU ou de RAM, c'est pourquoi les DSC échouent. Veuillez vérifier le nombre de collecteurs de données ajoutés à l'agent dans la machine. Si le nombre est supérieur à 20, veuillez augmenter la capacité du processeur et de la RAM de la machine Agent. Une fois le CPU et la RAM augmentés, les DSC passeront automatiquement en état d'initialisation puis en état d'exécution. Consultez le guide des tailles sur"cette page" .

{vider}

Problème : le collecteur de données génère une erreur lorsque le mode SVM est sélectionné. **Essayez ceci :** lors de la connexion en mode SVM, si l'IP de gestion du cluster est utilisée pour se connecter au lieu de l'IP de

gestion SVM, la connexion échouera. Assurez-vous que l'adresse IP SVM correcte est utilisée.

{vider}

Problème : le collecteur de données affiche un message d'erreur lorsque la fonction Accès refusé est activée : « Le connecteur est en état d'erreur. Nom du service : audit. Motif de l'échec : échec de la configuration de fpolicy sur SVM test_svm. Motif : l'utilisateur n'est pas autorisé. **Essayez ceci :** l'utilisateur ne dispose peut-être pas des autorisations REST nécessaires à la fonctionnalité Accès refusé. Veuillez suivre les instructions sur"cette page" pour définir les autorisations.

Redémarrez le collecteur une fois les autorisations définies.

{vider}

Problème : Le collecteur est en état d'erreur avec le message : Le connecteur est en état d'erreur. Raison de l'échec : Échec de la configuration du stockage persistant sur la SVM <Nom de la SVM>. Raison : Impossible de trouver un agrégat approprié pour le volume « <volumeName> » dans le SVM « <SVM Name> ». Motif : Les informations de performance pour l'agrégat « <aggregateName> » ne sont actuellement pas disponibles. Patientez quelques minutes et réessayez la commande. Nom du service : audit. Raison de l'échec : impossible de configurer le magasin persistant sur la SVM <SVM name="">.</SVM> Reason: Unable to find a suitable aggregate for volume "<volumeName>" in SVM "<SVM Name>". Motif : Les informations sur les performances pour <aggregateName>l'agrégat « » ne sont actuellement pas disponibles.</aggregateName> Attendez quelques minutes et réessayez la commande.

Essayez ceci : Attendez quelques minutes, puis redémarrez le Collecteur.

{vider}

Si vous rencontrez toujours des problèmes, contactez les liens d'assistance mentionnés dans la page **Aide > Assistance**.

Configuration du collecteur Cloud Volumes ONTAP et Amazon FSx for NetApp ONTAP

Surveillez l'accès aux fichiers et aux utilisateurs sur votre infrastructure de stockage cloud en configurant les collecteurs de données Workload Security pour Cloud Volumes ONTAP et Amazon FSx for NetApp ONTAP. Ce guide fournit des instructions étape par étape pour déployer des agents dans AWS et les connecter à vos instances de stockage cloud.

Configuration du stockage Cloud Volumes ONTAP

Consultez la documentation OnCommand Cloud Volumes ONTAP pour configurer une instance AWS à nœud unique / HA pour héberger l'agent de sécurité de la charge de travail :https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/index.html[]

Une fois la configuration terminée, suivez les étapes pour configurer votre SVM :https://docs.netapp.com/us-en/cloudinsights/task_add_collector_svm.html[]

Plateformes prises en charge

- Cloud Volumes ONTAP, pris en charge par tous les fournisseurs de services cloud disponibles, partout où ils sont disponibles. Par exemple : Amazon, Azure, Google Cloud.
- ONTAP Amazon FSx

Configuration de la machine agent

La machine agent doit être configurée dans les sous-réseaux respectifs des fournisseurs de services cloud. Pour en savoir plus sur l'accès au réseau, consultez les [Exigences relatives à l'agent].

Vous trouverez ci-dessous les étapes d'installation de l'agent dans AWS. Des étapes équivalentes, applicables au fournisseur de services cloud, peuvent être suivies dans Azure ou Google Cloud pour l'installation.

Dans AWS, procédez comme suit pour configurer la machine à utiliser comme agent de sécurité de charge de travail :

Suivez les étapes suivantes pour configurer la machine à utiliser comme agent de sécurité de charge de travail :

Étapes

1. Connectez-vous à la console AWS et accédez à la page EC2-Instances et sélectionnez *Lancer l'instance*.
2. Sélectionnez une AMI RHEL ou CentOS avec la version appropriée comme mentionné dans cette page :https://docs.netapp.com/us-en/cloudinsights/concept_cs_agent_requirements.html[]
3. Sélectionnez le VPC et le sous-réseau dans lesquels réside l'instance Cloud ONTAP .
4. Sélectionnez *t2.xlarge* (4 vcpus et 16 Go de RAM) comme ressources allouées.
    a. Créez l'instance EC2.
5. Installez les packages Linux requis à l'aide du gestionnaire de packages YUM :
    a. Installez *wget* et *unzip* les packages Linux natifs.

Installer l'agent Workload Security

1. Connectez-vous en tant qu'administrateur ou propriétaire de compte à votre environnement Data Infrastructure Insights .
2. Accédez à Workload Security **Collectors** et cliquez sur l'onglet **Agents**.
3. Cliquez sur **+Agent** et spécifiez RHEL comme plate-forme cible.
4. Copiez la commande d'installation de l'agent.
5. Collez la commande d'installation de l'agent dans l'instance RHEL EC2 à laquelle vous êtes connecté. Cela installe l'agent Workload Security, fournissant tous les"Prérequis de l'agent" sont respectées.

Pour les étapes détaillées, veuillez vous référer à ce lien : https://docs.netapp.com/us-en/cloudinsights/task_cs_add_agent.html#steps-to-install-agent

Dépannage

Les problèmes connus et leurs résolutions sont décrits dans le tableau suivant.

Problème	Résolution

L'erreur « Sécurité de la charge de travail : échec de détermination du type ONTAP pour le collecteur de données Amazon FxSN » est affichée par le collecteur de données. Le client ne peut pas ajouter de nouveau collecteur de données Amazon FSxN dans Workload Security. La connexion au cluster FSxN sur le port 443 depuis l'agent expire. Les groupes de sécurité du pare-feu et AWS ont les règles requises activées pour permettre la communication. Un agent est déjà déployé et se trouve également dans le même compte AWS. Ce même agent est utilisé pour connecter et surveiller les périphériques NetApp restants (et ils fonctionnent tous).	Résolvez ce problème en ajoutant le segment réseau LIF fsxadmin à la règle de sécurité de l'agent. Autorisez tous les ports si vous n'êtes pas sûr des ports.

Gestion des utilisateurs

Les comptes d'utilisateurs de Workload Security sont gérés via Data Infrastructure Insights.

Data Infrastructure Insights propose quatre niveaux de compte utilisateur : propriétaire du compte, administrateur, utilisateur et invité. À chaque compte sont attribués des niveaux d'autorisation spécifiques. Un compte utilisateur disposant de privilèges d'administrateur peut créer ou modifier des utilisateurs et attribuer à chaque utilisateur l'un des rôles de sécurité de la charge de travail suivants :

Rôle	Accès à la sécurité de la charge de travail
Administrateur	Peut exécuter toutes les fonctions de sécurité de la charge de travail, y compris celles pour les alertes, l'analyse médico-légale, les collecteurs de données, les politiques de réponse automatisées et les API pour la sécurité de la charge de travail. Un administrateur peut également inviter d'autres utilisateurs, mais ne peut attribuer que des rôles de sécurité de la charge de travail.
Utilisateur	Peut afficher et gérer les alertes et consulter les analyses médico-légales. Le rôle utilisateur peut modifier l'état de l'alerte, ajouter une note, prendre des instantanés manuellement et restreindre l'accès utilisateur.
Invité	Peut afficher les alertes et les analyses médico-légales. Le rôle d'invité ne peut pas modifier l'état de l'alerte, ajouter une note, prendre des instantanés manuellement ou restreindre l'accès des utilisateurs.

Étapes

1. Connectez-vous à Workload Security
2. Dans le menu, cliquez sur **Admin > Gestion des utilisateurs**

   Vous serez redirigé vers la page de gestion des utilisateurs de Data Infrastructure Insights.

3. Sélectionnez le rôle souhaité pour chaque utilisateur.

Lors de l'ajout d'un nouvel utilisateur, sélectionnez simplement le rôle souhaité (généralement Utilisateur ou Invité).

Vous trouverez plus d'informations sur les comptes d'utilisateurs et les rôles dans Data Infrastructure Insights."Rôle de l'utilisateur" documentation.

Vérificateur de taux d'événements : Guide de dimensionnement des agents

Déterminez la taille optimale des machines Agent en mesurant les débits d'événements NFS et SMB générés par vos SVM avant de déployer les collecteurs de données. Le script Event Rate Checker vous aide à comprendre les limites de capacité (maximum 50 collecteurs de données par Agent) et garantit que votre infrastructure Agent peut gérer le volume d'événements attendu pour une détection fiable des menaces.

Exigences:

- IP de cluster
- Nom d'utilisateur et mot de passe de l'administrateur du cluster

Lors de l'exécution de ce script, aucun collecteur de données ONTAP SVM ne doit être en cours d'exécution pour le SVM pour lequel le taux d'événements est déterminé.

Mesures:

1. Installez l'agent en suivant les instructions de CloudSecure.
2. Une fois l'agent installé, exécutez le script *server_data_rate_checker.sh* en tant qu'utilisateur sudo :

```
 /opt/netapp/cloudsecure/agent/install/svm_event_rate_checker.sh
. Ce script nécessite que _sshpass_ soit installé sur la machine Linux.
Il existe deux façons de l'installer :
```

   a. Exécutez la commande suivante :

```
 linux_prompt> yum install sshpass
.. Si cela ne fonctionne pas, téléchargez _sshpass_ sur la machine
Linux à partir du Web et exécutez la commande suivante :
```

```
linux_prompt> rpm -i sshpass
```

3. Fournissez les valeurs correctes lorsque vous y êtes invité. Voir ci-dessous pour un exemple.
4. L'exécution du script prendra environ 5 minutes.
5. Une fois l'exécution terminée, le script imprimera le taux d'événements à partir du SVM. Vous pouvez vérifier le taux d'événements par SVM dans la sortie de la console :

```
“Svm svm_rate is generating 100 events/sec”.
```

Chaque collecteur de données Ontap SVM peut être associé à un seul SVM, ce qui signifie que chaque collecteur de données pourra recevoir le nombre d’événements générés par un seul SVM.

Gardez à l’esprit les points suivants :

A) Utilisez ce tableau comme guide général de dimensionnement. Vous pouvez augmenter le nombre de cœurs et/ou de mémoire pour augmenter le nombre de collecteurs de données pris en charge, jusqu’à un maximum de 50 collecteurs de données :

Configuration de la machine agent	Nombre de collecteurs de données SVM	Taux maximal d’événements que la machine agent peut gérer
4 cœurs, 16 Go	10 collecteurs de données	20 000 événements/sec
4 cœurs, 32 Go	20 collecteurs de données	20 000 événements/sec

B) Pour calculer le nombre total d’événements, additionnez les événements générés pour tous les SVM de cet agent.

C) Si le script n’est pas exécuté pendant les heures de pointe ou si le trafic de pointe est difficile à prévoir, conservez une marge de taux d’événements de 30 %.

B + C doit être inférieur à A, sinon la machine Agent ne parviendra pas à surveiller.

En d’autres termes, le nombre de collecteurs de données qui peuvent être ajoutés à une seule machine agent doit être conforme à la formule ci-dessous :

```
 Sum of all Event rate of all Data Source Collectors + Buffer Event rate
of 30% < 20000 events/second
Voir lelink:concept_cs_agent_requirements.html["Exigences relatives aux
agents"] page pour les prérequis et exigences supplémentaires.
```

Exemple

Disons que nous avons trois SVMS générant des taux d’événements de 100, 200 et 300 événements par seconde, respectivement.

Nous appliquons la formule :

```
 (100+200+300) + [(100+200+300)*30%] = 600+180 = 780events/sec
780 events/second is < 20000 events/second, so the 3 SVMs can be monitored
via one agent box.
```

La sortie de la console est disponible sur la machine Agent dans le nom de fichier *fpolicy_stat_<SVM Name>.log* dans le répertoire de travail actuel.

Le script peut donner des résultats erronés dans les cas suivants :

- Des informations d'identification, une adresse IP ou un nom SVM incorrects sont fournis.
- Une fpolicy déjà existante avec le même nom, le même numéro de séquence, etc. donnera une erreur.
- Le script s'arrête brusquement pendant son exécution.

Un exemple d'exécution de script est présenté ci-dessous :

```
[root@ci-cs-data agent]#
/opt/netapp/cloudsecure/agent/install/svm_event_rate_checker.sh
```

```
Enter the cluster ip: 10.192.139.166
Enter the username to SSH: admin
Enter the password:
Getting event rate for NFS and SMB events.
Available SVMs in the Cluster
------------------------------
QA_SVM
Stage_SVM
Qa-fas8020
Qa-fas8020-01
Qa-fas8020-02
audit_svm
svm_rate
vs_new
vs_new2
```

```
-----------------------------
Enter [1/5] SVM name to check (press enter to skip): svm_rate
Enter [2/5] SVM name to check (press enter to skip): audit_svm
Enter [3/5] SVM name to check (press enter to skip):
Enter [4/5] SVM name to check (press enter to skip):
Enter [5/5] SVM name to check (press enter to skip):
Running check for svm svm_rate...
Running check for svm audit_svm...
Waiting 5 minutes for stat collection
Stopping sample svm_rate_sample
Stopping sample audit_svm_sample
fpolicy stats of svm svm_rate is saved in fpolicy_stat_svm_rate.log
Svm svm_rate is generating 100 SMB events/sec and 100 NFS events/sec
Overall svm svm_rate is generating 200 events/sec
fpolicy stats of svm audit_svm is saved in fpolicy_stat_audit_svm.log
Svm audit_svm is generating 200 SMB events/sec and 100 NFS events/sec
Overall svm audit_svm is generating 300 events/sec
```

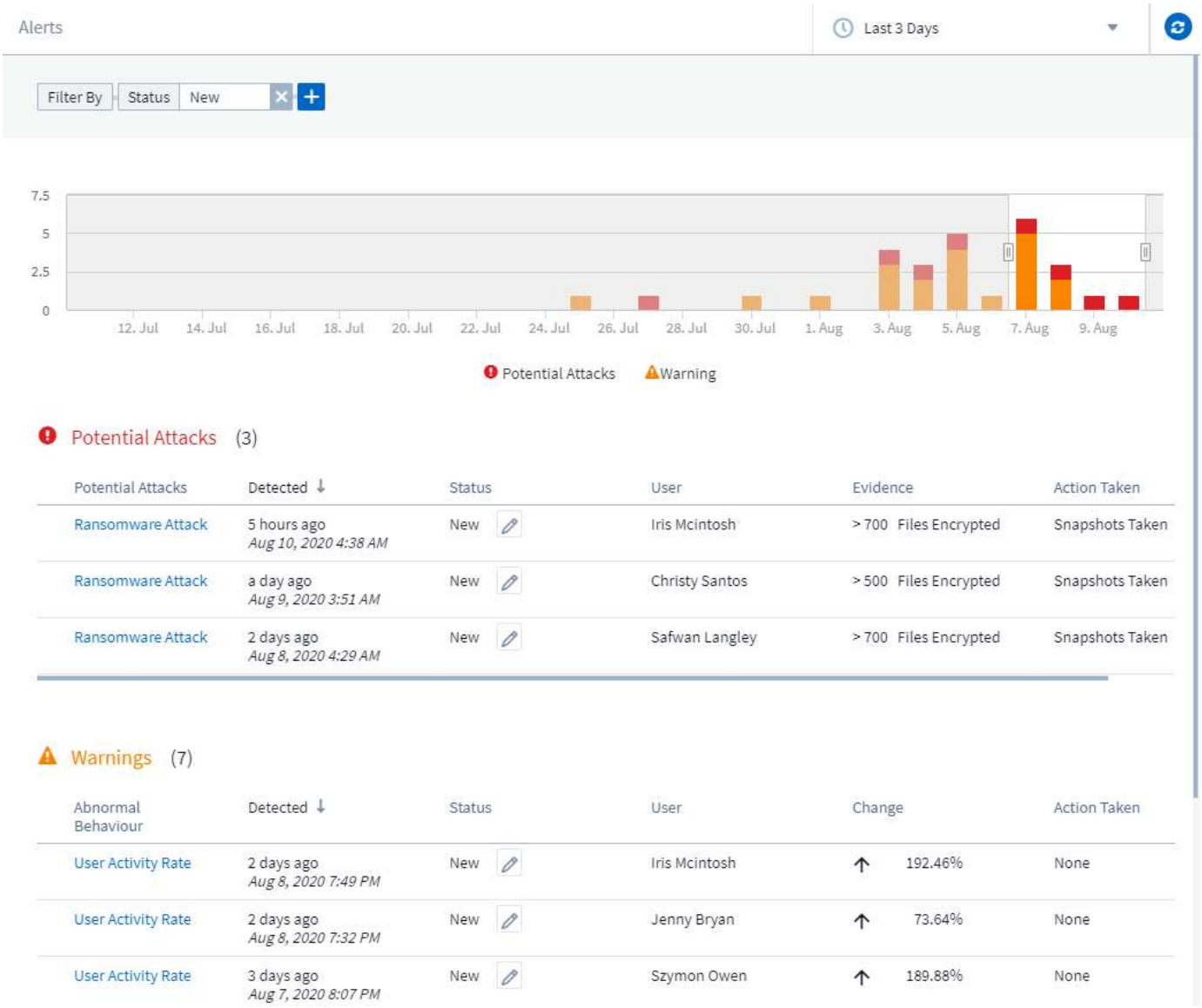
```
[root@ci-cs-data agent]#
```

Dépannage

Question	Répondre
Si j'exécute ce script sur un SVM déjà configuré pour Workload Security, utilise-t-il simplement la configuration fpolicy existante sur le SVM ou en configure-t-il un temporaire et exécute-t-il le processus ?	Le vérificateur de taux d'événements peut fonctionner correctement même pour un SVM déjà configuré pour la sécurité de la charge de travail. Il ne devrait y avoir aucun impact.
Puis-je augmenter le nombre de SVM sur lesquels le script peut être exécuté ?	Oui. Modifiez simplement le script et modifiez le nombre maximal de SVM de 5 à n'importe quel nombre souhaité.
Si j'augmente le nombre de SVM, cela augmentera-t-il le temps d'exécution du script ?	Non. Le script s'exécutera pendant 5 minutes maximum, même si le nombre de SVM est augmenté.
Puis-je augmenter le nombre de SVM sur lesquels le script peut être exécuté ?	Oui. Vous devez modifier le script et modifier le nombre maximal de SVM de 5 à n'importe quel nombre souhaité.
Si j'augmente le nombre de SVM, cela augmentera-t-il le temps d'exécution du script ?	Non. Le script s'exécutera pendant 5 minutes maximum, même si le nombre de SVM augmente.
Que se passe-t-il si j'exécute le vérificateur de taux d'événements avec un agent existant ?	L'exécution du vérificateur de taux d'événements sur un agent déjà existant peut entraîner une augmentation de la latence sur le SVM. Cette augmentation sera de nature temporaire pendant l'exécution du vérificateur de taux d'événements.

Comprendre et examiner les alertes

La page « Alertes de sécurité des charges de travail » fournit une chronologie complète des menaces et avertissements détectés, ainsi que des outils d'investigation détaillés. Consultez les détails des alertes, gérez les mises à jour de statut, filtrez par critères et suivez les activités des utilisateurs pour enquêter efficacement sur les incidents de sécurité et y répondre.



Alerte

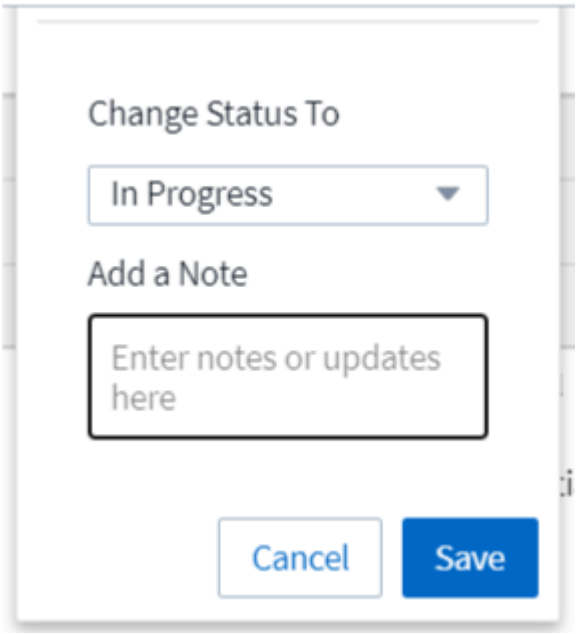
La liste des alertes affiche un graphique indiquant le nombre total d'attaques potentielles et/ou d'avertissements qui ont été émis dans la période sélectionnée, suivi d'une liste des attaques et/ou des avertissements qui se sont produits dans cette période. Vous pouvez modifier la plage horaire en ajustant les curseurs d'heure de début et d'heure de fin dans le graphique.

Les éléments suivants sont affichés pour chaque alerte :

Attaques potentielles :

- Le type d'attaque potentielle (par exemple, falsification de fichiers ou sabotage)
- La date et l'heure auxquelles l'attaque potentielle a été *détectée*
- Le *Statut* de l'alerte :
  - **Nouveau** : il s'agit de la valeur par défaut pour les nouvelles alertes.
  - **En cours** : L'alerte fait l'objet d'une enquête par un ou plusieurs membres de l'équipe.
  - **Résolu** : L'alerte a été marquée comme résolue par un membre de l'équipe.
  - **Rejeté** : l'alerte a été rejetée en tant que faux positif ou comportement attendu.

    Un administrateur peut modifier le statut de l'alerte et ajouter une note pour faciliter l'enquête.



- L'utilisateur dont le comportement a déclenché l'alerte
- *Preuve* de l'attaque (par exemple, un grand nombre de fichiers ont été chiffrés)
- L'action entreprise (par exemple, un instantané a été pris)

Avertissements :

- Le *Comportement anormal* qui a déclenché l'avertissement
- La date et l'heure auxquelles le comportement a été *détecté*
- Le *Statut* de l'alerte (Nouveau, En cours, etc.)
- L'utilisateur dont le comportement a déclenché l'alerte
- Une description du *Changement* (par exemple, une augmentation anormale de l'accès aux fichiers)
- L'action entreprise

Options de filtrage

Vous pouvez filtrer les alertes selon les critères suivants :

- Le *Statut* de l'alerte

- Texte spécifique dans la *Note*
- Le type d'*attaques/avertissements*
- L'utilisateur dont les actions ont déclenché l'alerte/l'avertissement

La page Détails de l'alerte

Vous pouvez cliquer sur un lien d'alerte sur la page de la liste des alertes pour ouvrir une page de détails pour l'alerte. Les détails de l'alerte peuvent varier selon le type d'attaque ou d'alerte. Par exemple, une page de détails sur une attaque par falsification de fichiers peut afficher les informations suivantes :

Section récapitulative :

- Type d'attaque (falsification de fichiers, sabotage) et ID d'alerte (attribué par la sécurité des charges de travail)
- Date et heure de détection de l'attaque
- Action entreprise (par exemple, un instantané automatique a été pris). L'heure de l'instantané est indiquée immédiatement sous la section récapitulative))
- Statut (Nouveau, En cours, etc.)

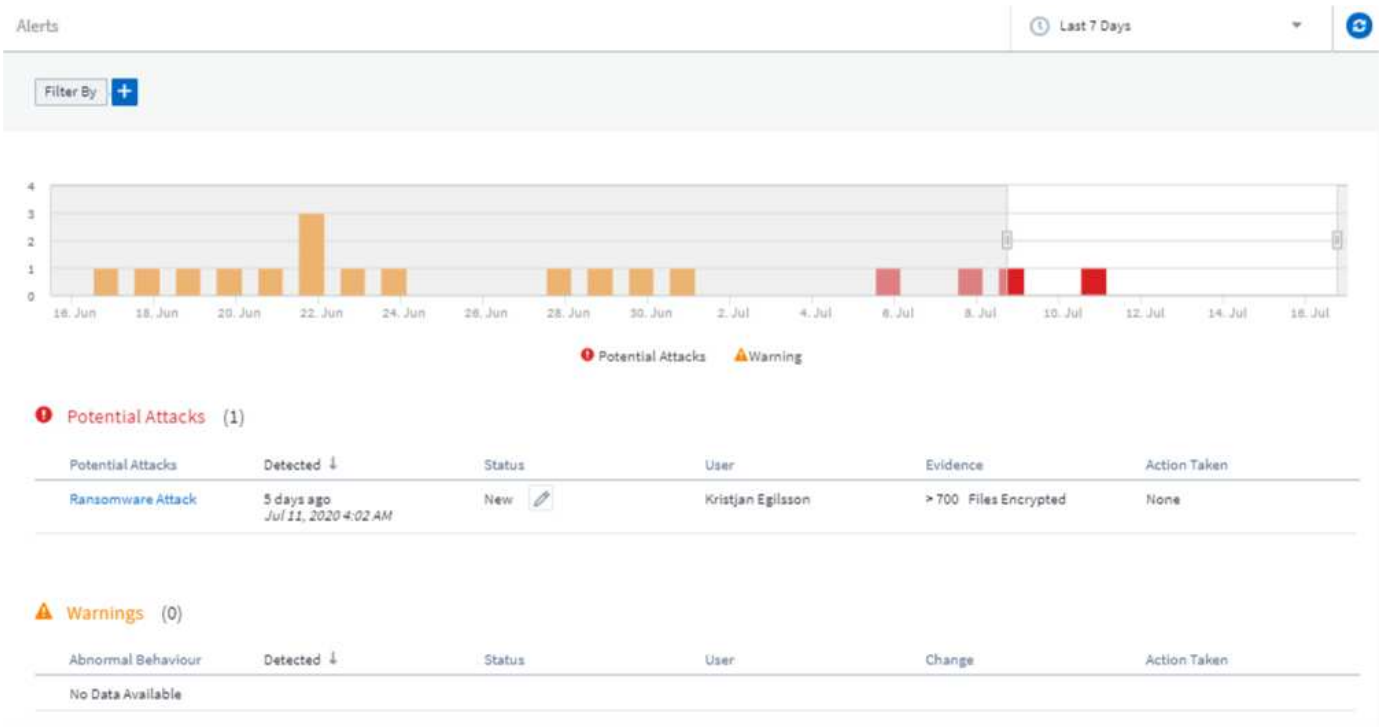
Section Résultats d'attaque :

- Nombre de volumes et de fichiers affectés
- Un résumé d'accompagnement de la détection
- Un graphique montrant l'activité du fichier pendant l'attaque

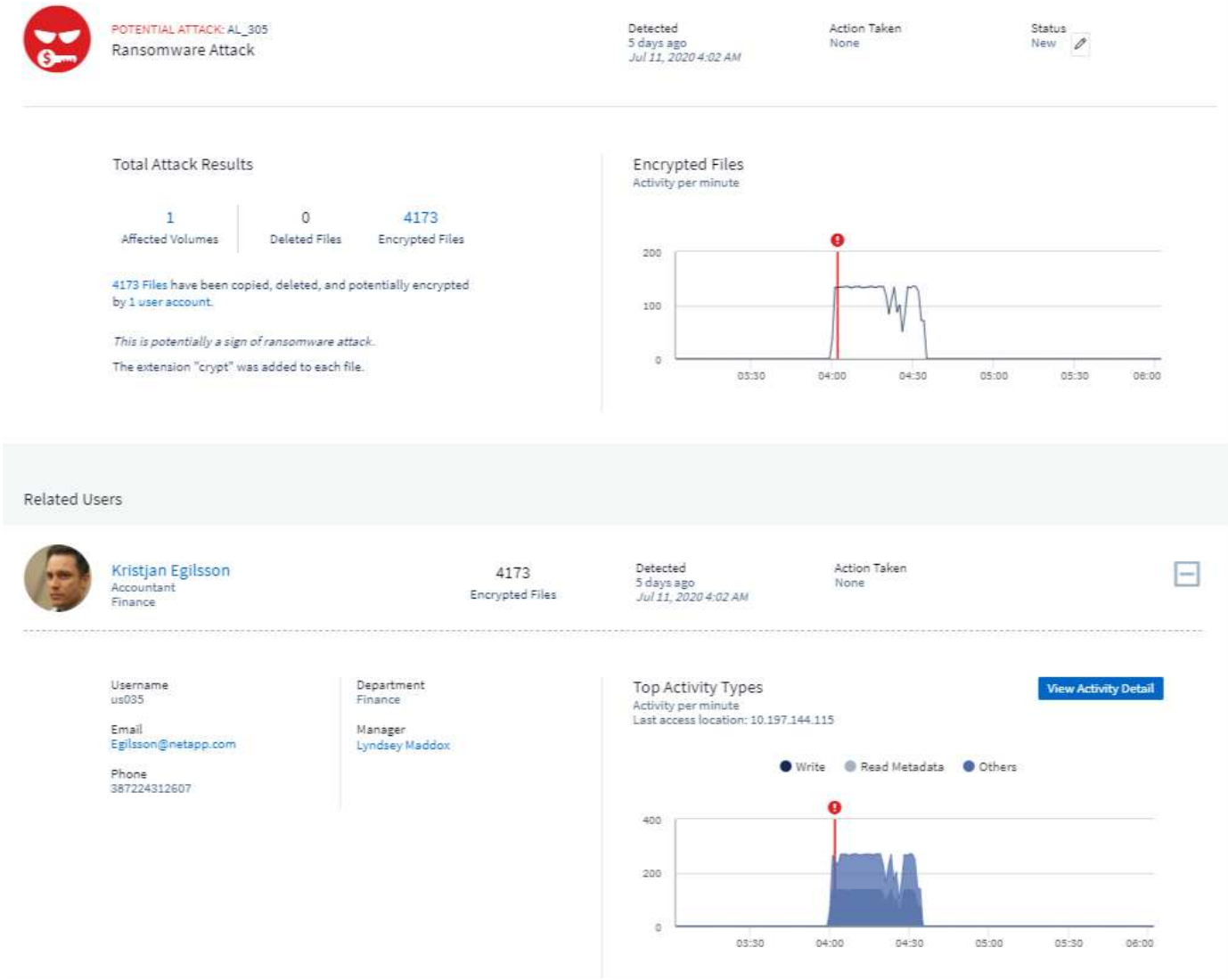
Section Utilisateurs associés :

Cette section affiche des détails sur l'utilisateur impliqué dans l'attaque potentielle, y compris un graphique de l'activité principale de l'utilisateur.

Page d'alertes (cet exemple illustre une potentielle attaque par falsification de fichiers) :



Page de détails (cet exemple illustre une attaque potentielle par falsification de fichiers) :

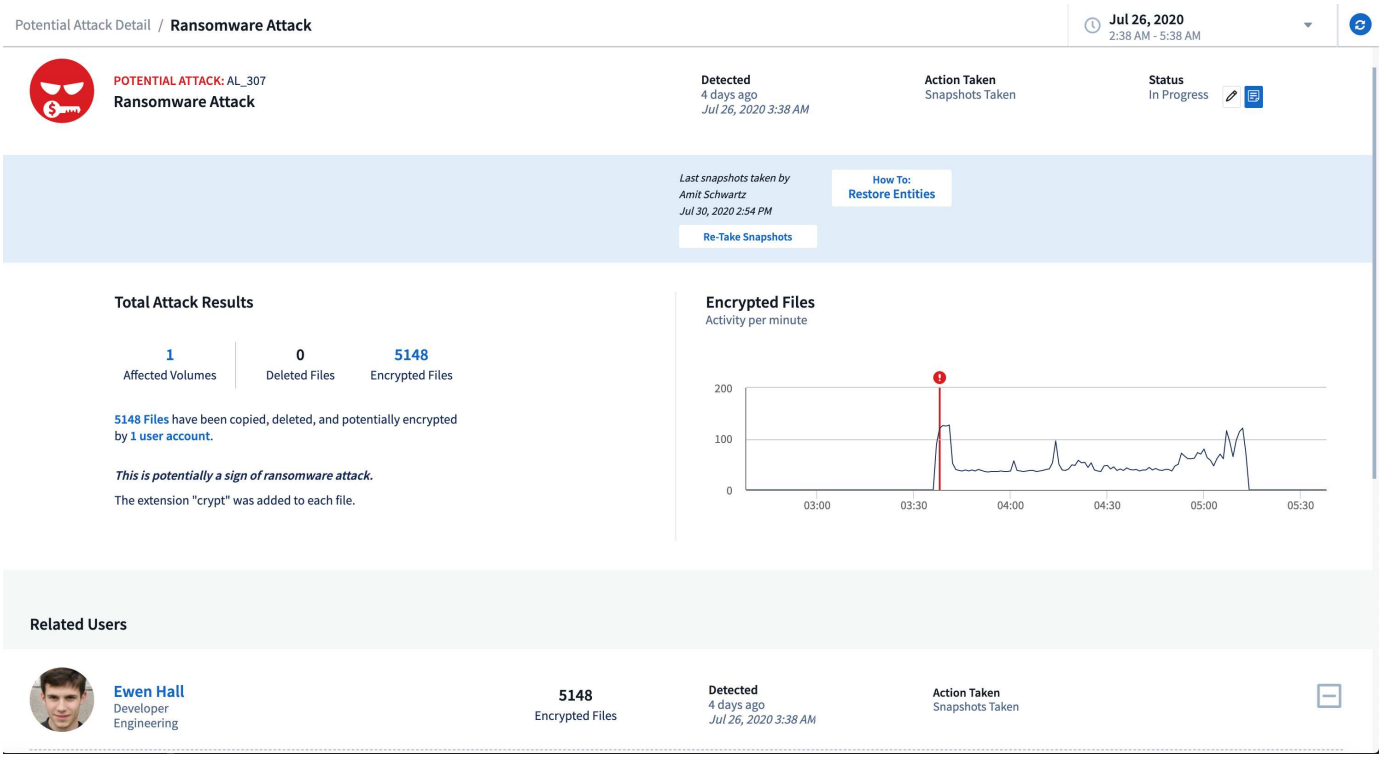


Prendre un instantané **Action**

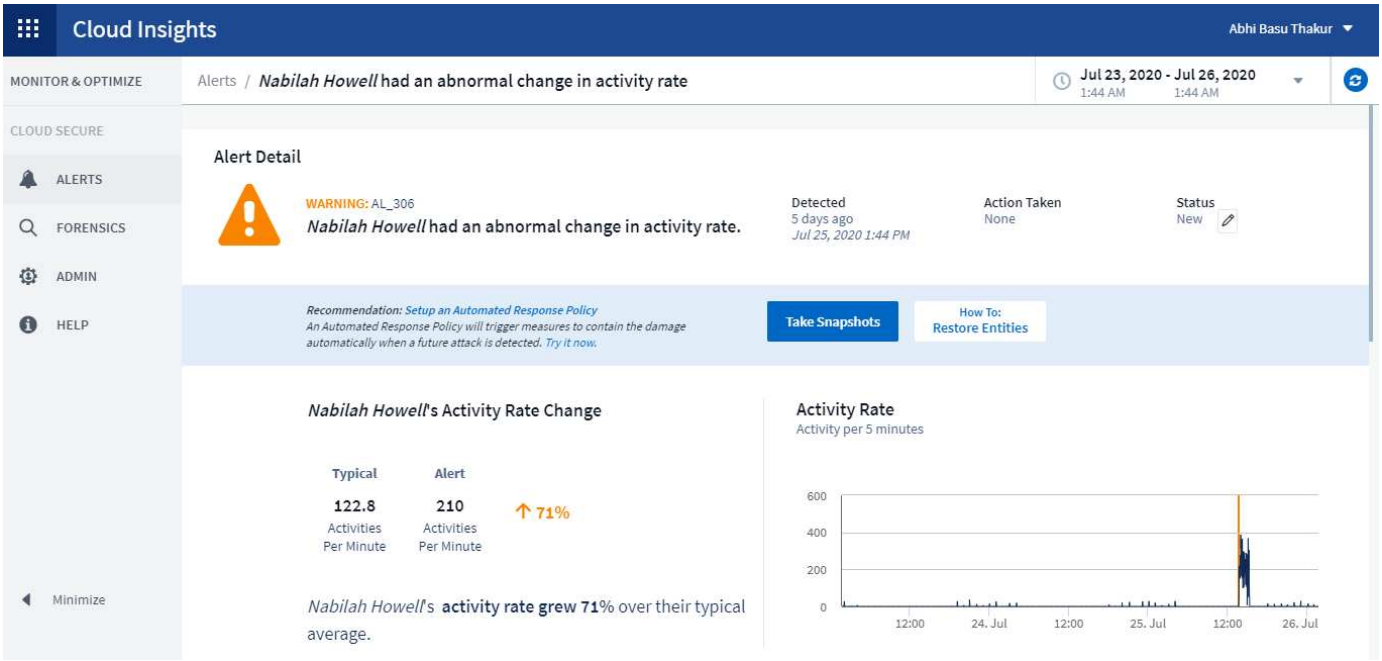
Workload Security protège vos données en prenant automatiquement un instantané lorsqu'une activité malveillante est détectée, garantissant ainsi que vos données sont sauvegardées en toute sécurité.

Vous pouvez définir "politiques de réponse automatisées" qui prennent un instantané lorsqu'une attaque par falsification de fichiers ou toute autre activité anormale de l'utilisateur est détectée. Vous pouvez également prendre une capture d'écran manuellement depuis la page d'alerte.

Capture d'écran automatique
prise :



Instantané manuel :



Notifications d’alerte

Les notifications par courrier électronique des alertes sont envoyées à une liste de destinataires d’alertes pour chaque action sur l’alerte. Pour configurer les destinataires des alertes, cliquez sur **Admin > Notifications** et saisissez une adresse e-mail pour chaque destinataire.

Politique de conservation

Les alertes et avertissements sont conservés pendant 13 mois. Les alertes et avertissements datant de plus

de 13 mois seront supprimés. Si l'environnement Workload Security est supprimé, toutes les données associées à l'environnement sont également supprimées.

Dépannage

Problème:	Essayez ceci:
Il existe une situation dans laquelle ONTAP prend des instantanés toutes les heures par jour. Les snapshots de Workload Security (WS) l'affecteront-ils ? Le snapshot WS prendra-t-il la place du snapshot horaire ? L'instantané horaire par défaut sera-t-il arrêté ?	Les instantanés de sécurité de la charge de travail n'affecteront pas les instantanés horaires. Les instantanés WS n'occuperont pas l'espace d'instantané horaire et cela devrait continuer comme avant. L'instantané horaire par défaut ne sera pas arrêté.
Que se passera-t-il si le nombre maximal de snapshots est atteint dans ONTAP?	Si le nombre maximal de snapshots est atteint, la prise de snapshots suivante échouera et Workload Security affichera un message d'erreur indiquant que le snapshot est plein. L'utilisateur doit définir des politiques d'instantanés pour supprimer les instantanés les plus anciens, sinon les instantanés ne seront pas pris. Dans ONTAP 9.3 et les versions antérieures, un volume peut contenir jusqu'à 255 copies Snapshot. Dans ONTAP 9.4 et versions ultérieures, un volume peut contenir jusqu'à 1 023 copies Snapshot. Consultez la documentation ONTAP pour plus d'informations sur"définition de la politique de suppression des instantanés" .
Workload Security n'est pas en mesure de prendre des instantanés.	Assurez-vous que le rôle utilisé pour créer des instantanés dispose du lien : https://docs.netapp.com/us-en/cloudinsights/task_add_collector_svm.html#a-note-about-permissions [droits appropriés attribués]. Assurez-vous que *csrole* est créé avec les droits d'accès appropriés pour prendre des instantanés : security login role create -vserver <vservername> -role csrole -cmddirname "volume snapshot" -access all
Les instantanés échouent pour les alertes plus anciennes sur les SVM qui ont été supprimées de Workload Security, puis rajoutées. Pour les nouvelles alertes qui se produisent après le nouvel ajout de SVM, des instantanés sont pris.	C'est un scénario rare. Si vous rencontrez ce problème, connectez-vous à ONTAP et prenez manuellement les instantanés des alertes les plus anciennes.
Dans la page *Détails de l'alerte*, le message d'erreur « La dernière tentative a échoué » s'affiche sous le bouton *Prendre un instantané*. Le survol de l'erreur affiche « La commande d'appel de l'API a expiré pour le collecteur de données avec l'ID ».	Cela peut se produire lorsqu'un collecteur de données est ajouté à Workload Security via SVM Management IP, si le LIF du SVM est à l'état *désactivé* dans ONTAP. Activez le LIF particulier dans ONTAP et déclenchez *Prendre un instantané manuellement* à partir de Workload Security. L'action Snapshot réussira alors.

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.

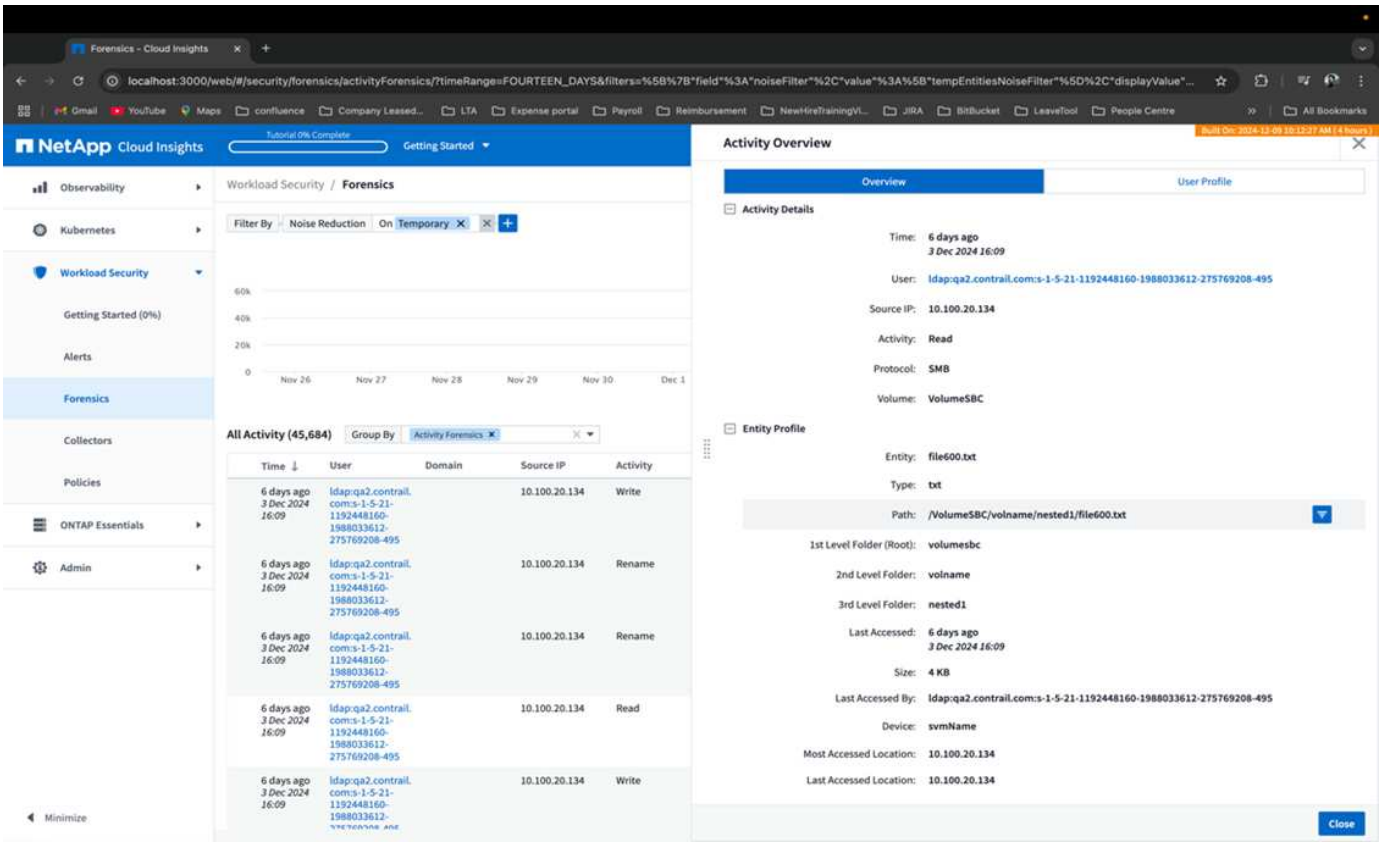
Le tableau **Toutes les activités** affiche les informations suivantes. Notez que toutes ces colonnes ne sont pas affichées par défaut. Vous pouvez sélectionner les colonnes à afficher en cliquant sur l'icône « engrenage ».

- 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.

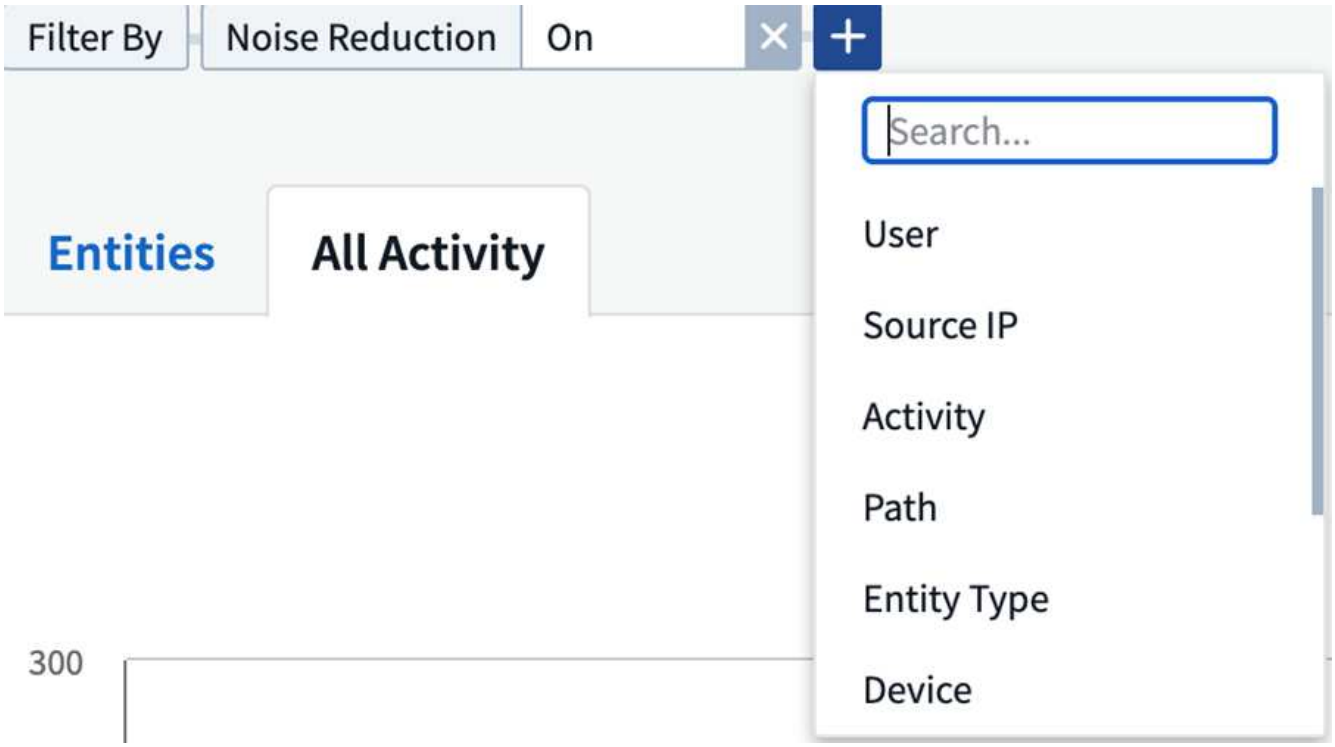
- Le nombre d'activités est affiché sous forme de lien hypertexte ; la sélection de cette option ajoutera le groupe sélectionné en tant que filtre. Le tableau d'activité sera mis à jour en fonction de ce filtre.
- Notez que si vous modifiez le filtre, modifiez la plage horaire ou actualisez l'écran, 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.

Expression de filtre appliquée par l'utilisateur	Résultat attendu	Évaluation des performances	Commentaire
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

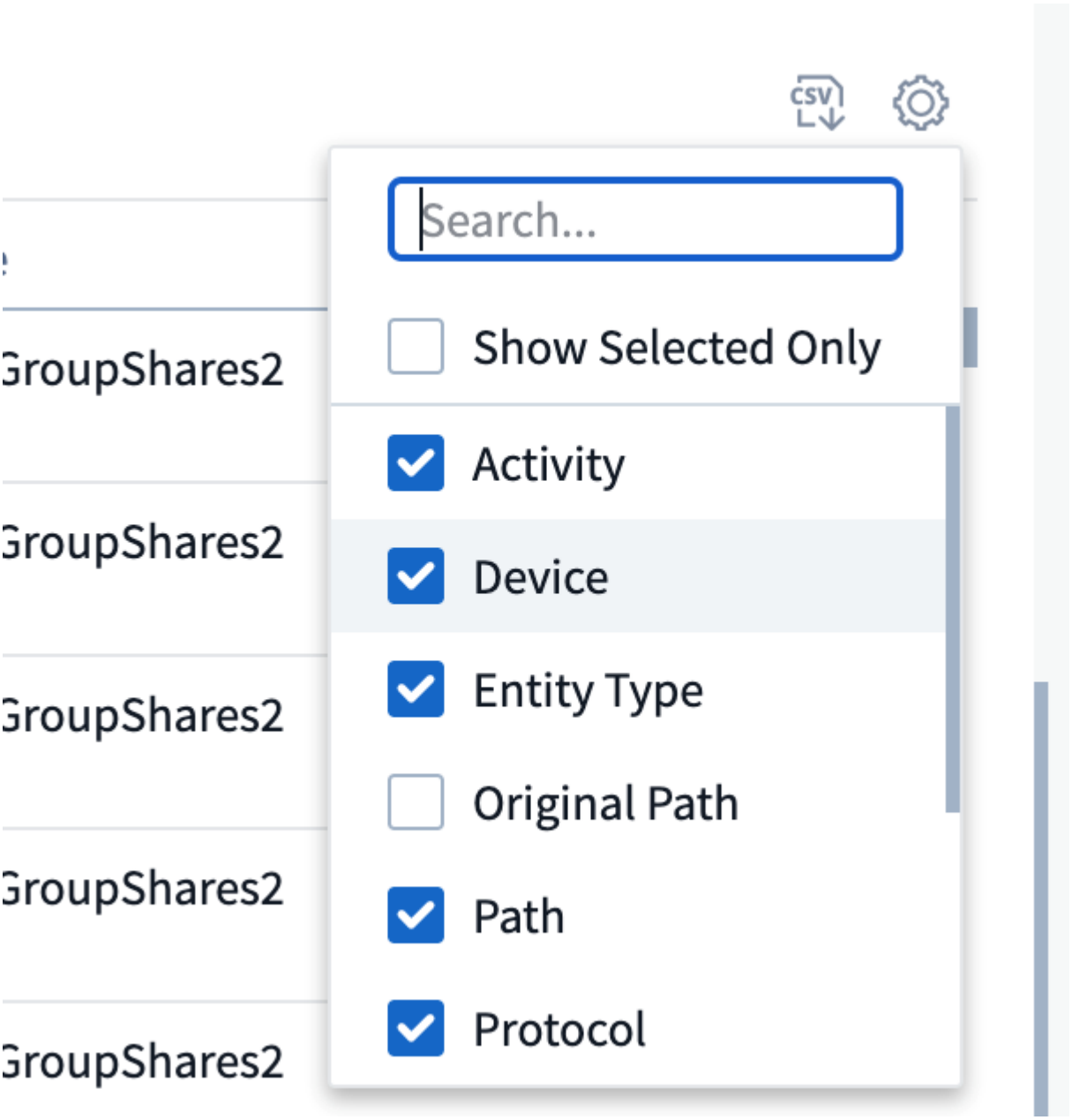
1. **Lancer l'exportation** : Sélectionnez la durée et les filtres souhaités pour l'exportation et cliquez sur le bouton Exporter.
2. **Attendez que l'exportation soit terminée** : Le temps de traitement peut varier de quelques minutes à quelques heures. Vous devrez peut-être actualiser la page d'analyse 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.

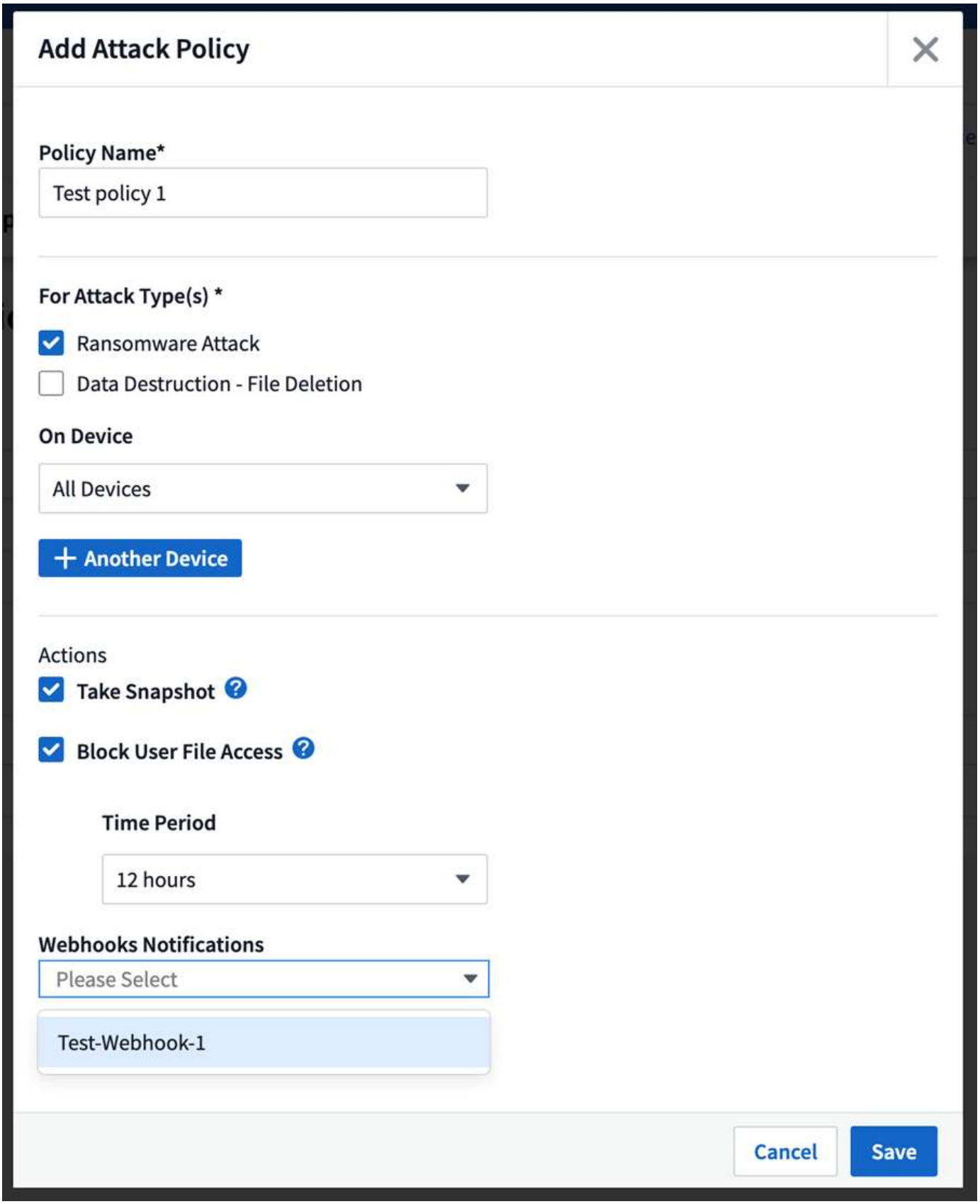
Politique de conservation

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.

Politiques de réponse automatisées

Les politiques de réponse déclenchent des actions telles que la prise d’un instantané ou la restriction de l’accès des utilisateurs en cas d’attaque ou de comportement anormal des utilisateurs.

Vous pouvez définir des politiques sur des appareils spécifiques ou sur tous les appareils. Pour définir une politique de réponse, sélectionnez **Admin > Politiques de réponse automatisées** et cliquez sur le bouton **+Politique** approprié. Vous pouvez créer des politiques pour les attaques ou pour les avertissements.



Vous devez enregistrer la politique sous un nom unique.

Pour désactiver une action de réponse automatisée (par exemple, Prendre un instantané), décochez simplement l'action et enregistrez la politique.

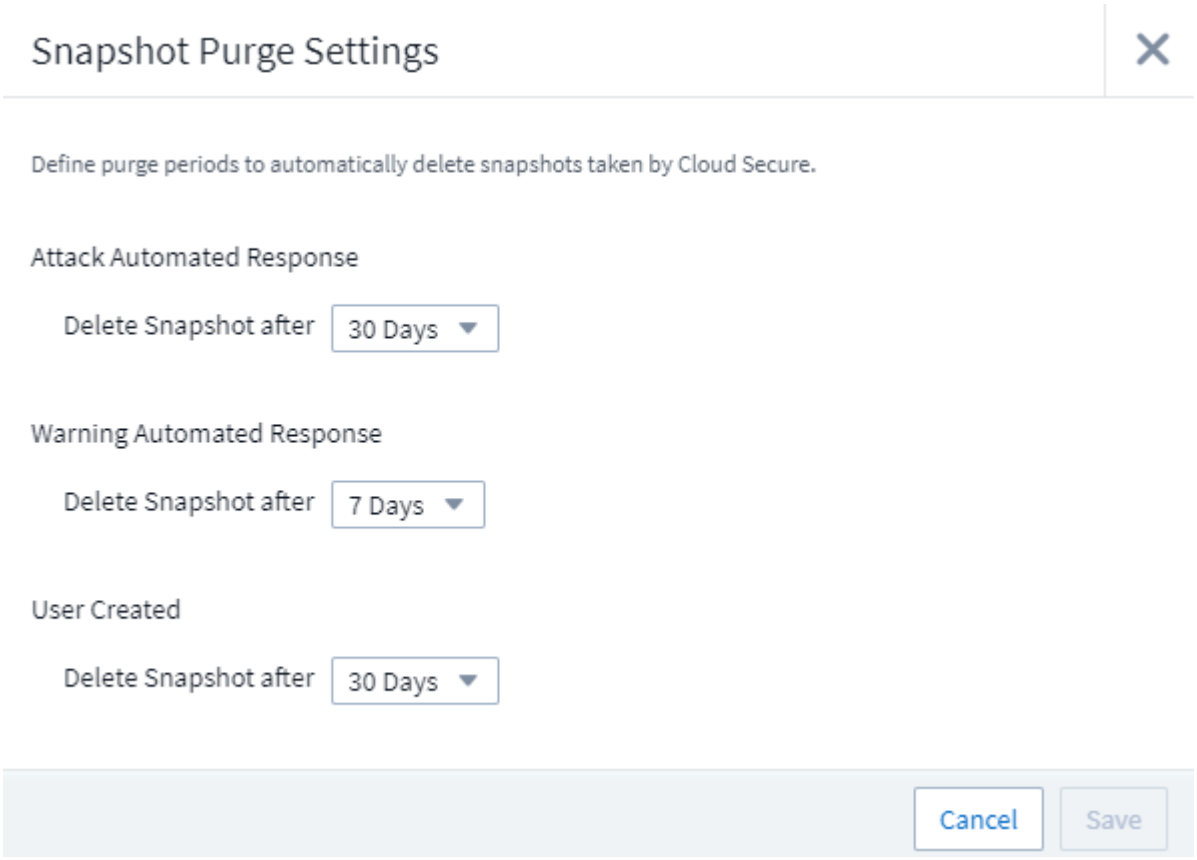
Lorsqu'une alerte est déclenchée sur les appareils spécifiés (ou tous les appareils, s'ils sont sélectionnés), la politique de réponse automatisée prend un instantané de vos données. Vous pouvez voir l'état de l'instantané sur le"Page de détails de l'alerte" .

Voir le"Restreindre l'accès des utilisateurs" page pour plus de détails sur la restriction de l'accès des utilisateurs par IP.

Vous pouvez attacher un ou plusieurs webhooks à une politique pour être averti lorsqu'une alerte est créée et qu'une action est entreprise. Il est recommandé de ne pas ajouter plus de 10 webhooks à une politique. Gardez à l'esprit que si une politique est suspendue, les notifications de webhook ne seront pas déclenchées.

Vous pouvez modifier ou suspendre une politique de réponse automatisée en choisissant l'option dans le menu déroulant de la politique.

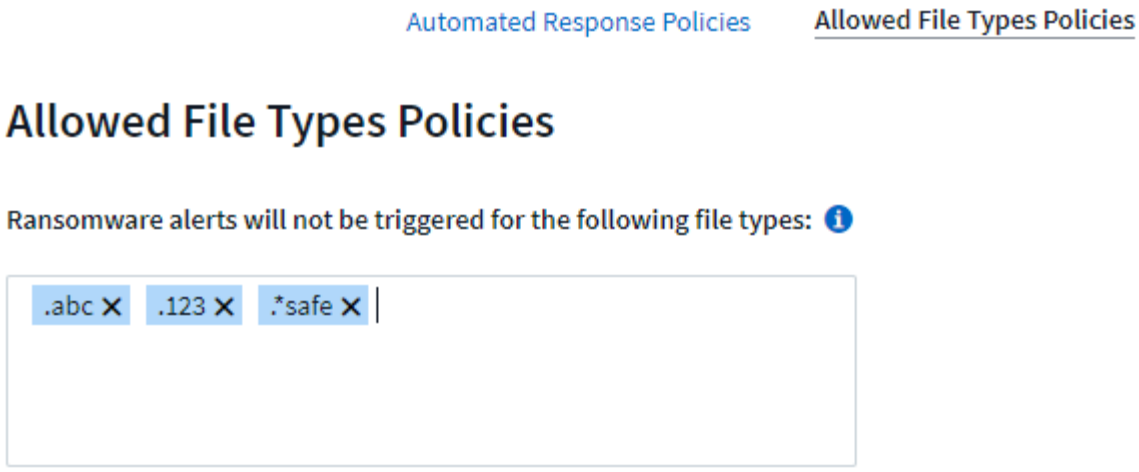
Workload Security supprimera automatiquement les instantanés une fois par jour en fonction des paramètres de purge des instantanés.



Politiques relatives aux types de fichiers autorisés

Si une attaque par falsification de fichier est détectée pour une extension de fichier connue et que des alertes sont générées sur l'écran Alertes, cette extension de fichier peut être ajoutée à une liste de types de fichiers autorisés afin d'éviter les alertes inutiles.

Accédez à **Sécurité de la charge de travail > Politiques** et accédez à l'onglet *Politiques de type de fichier autorisées*.



Une fois ajouté à la liste des *types de fichiers autorisés*, aucune alerte d'attaque par falsification de fichiers ne sera générée pour ce type de fichier autorisé. Notez que la politique relative aux *Types de fichiers autorisés* ne s'applique qu'à la détection des falsifications de fichiers.

Par exemple, si un fichier nommé *test.txt* est renommé en *test.txt.abc* et que Workload Security détecte une attaque par falsification de fichier en raison de l'extension *.abc*, l'extension *.abc* peut être ajoutée à la liste des *types de fichiers autorisés*. Après leur ajout à la liste, les attaques par falsification de fichiers ne seront plus générées contre les fichiers ayant l'extension *.abc*.

Les types de fichiers autorisés peuvent être des correspondances exactes (par exemple, « .abc ») ou des expressions (par exemple, « .**type », « .type** » ou « **type** »). Les expressions de types « .a*c », « .p*f » ne sont pas prises en charge.

Intégration avec la protection autonome contre les ransomwares ONTAP

La fonction de protection autonome ONTAP utilise l'analyse de la charge de travail dans les environnements NAS (NFS et SMB) pour détecter et signaler de manière proactive toute activité anormale dans les fichiers pouvant indiquer des attaques malveillantes ou des modifications de données non autorisées.

Des détails supplémentaires et des exigences de licence concernant ARP peuvent être trouvés"ici" .

Workload Security s'intègre à ONTAP pour recevoir les événements ARP et fournir une couche d'analyse supplémentaire et de réponses automatiques.

Workload Security reçoit les événements ARP d' ONTAP et entreprend les actions suivantes :

1. Met en corrélation les événements de chiffrement de volume avec l'activité de l'utilisateur pour identifier qui cause les dommages.
2. Implémente des politiques de réponse automatique (si définies)
3. Fournit des capacités d'investigation médico-légale :
   - Permettre aux clients de mener des enquêtes sur les violations de données.
   - Identifiez les fichiers affectés, ce qui permet une récupération plus rapide et la réalisation d'enquêtes sur les violations de données.

Prérequis

1. Version minimale ONTAP : 9.11.1
2. Volumes compatibles ARP. Vous trouverez des détails sur l'activation d'ARP."ici" . ARP doit être activé via OnCommand System Manager. Workload Security ne peut pas activer ARP.
3. Le collecteur de sécurité de la charge de travail doit être ajouté via l'adresse IP du cluster.
4. Les informations d'identification au niveau du cluster sont nécessaires pour que cette fonctionnalité fonctionne. En d'autres termes, les informations d'identification au niveau du cluster doivent être utilisées lors de l'ajout du SVM.

Autorisations utilisateur requises

Si vous utilisez les informations d'identification d'administration de cluster, aucune nouvelle autorisation n'est nécessaire.

Si vous utilisez un utilisateur personnalisé (par exemple, *csuser*) avec des autorisations accordées à l'utilisateur, suivez les étapes ci-dessous pour accorder des autorisations à Workload Security afin de collecter des informations liées à ARP à partir d' ONTAP.

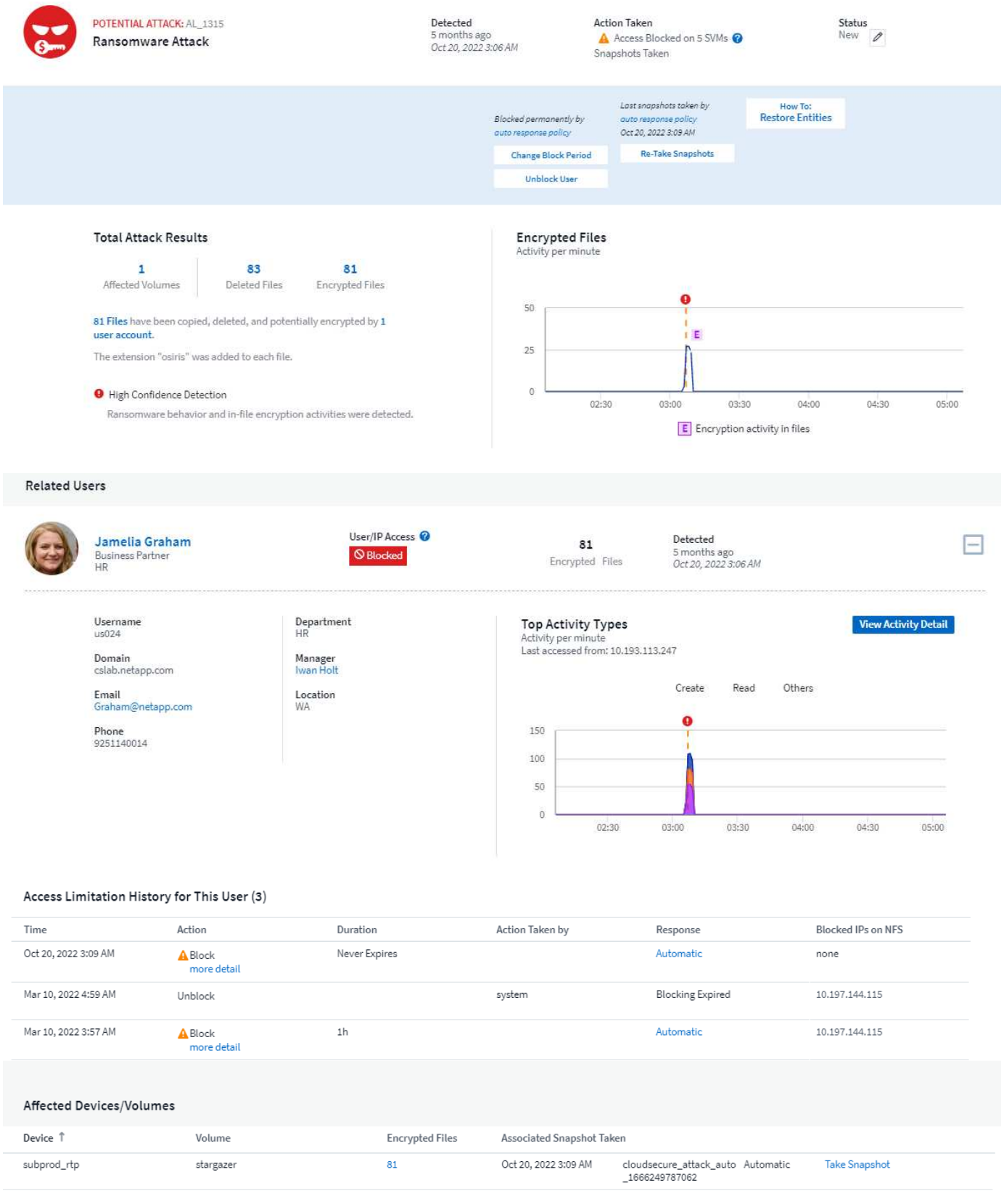
Pour *csuser* avec les informations d'identification du cluster, procédez comme suit à partir de la ligne de commande ONTAP :

```
security login role create -role csrole -cmddirname "volume" -access
readonly
security login role create -role csrole -cmddirname "security anti-
ransomware volume" -access readonly
```

En savoir plus sur la configuration d'autres"Autorisations ONTAP" .

Exemple d'alerte

Un exemple d'alerte générée en raison d'un événement ARP est présenté ci-dessous :



Un bandeau de confiance élevée indique que l'attaque a démontré un comportement de falsification de fichiers ainsi que des activités de chiffrement de fichiers. Le graphique des fichiers chiffrés indique l'horodatage auquel l'activité de chiffrement du volume a été détectée par la solution ARP.

Limites

Dans le cas où un SVM n'est pas surveillé par Workload Security, mais qu'il existe des événements ARP générés par ONTAP, les événements seront toujours reçus et affichés par Workload Security. Cependant, les informations médico-légales liées à l'alerte, ainsi que la cartographie des utilisateurs, ne seront pas capturées ou affichées.

Dépannage

Les problèmes connus et leurs résolutions sont décrits dans le tableau suivant.

Problème:	Résolution:
Les alertes par e-mail sont reçues 24 heures après la détection d'une attaque. Dans l'interface utilisateur, les alertes sont affichées 24 heures avant la réception des e-mails par Data Infrastructure Insights Workload Security.	Lorsque ONTAP envoie l'événement *Ransomware Detected* à Data Infrastructure Insights Workload Security (c'est-à-dire Workload Security), l'e-mail est envoyé. L'événement contient une liste d'attaques et leurs horodatages. L'interface utilisateur de sécurité de la charge de travail affiche l'horodatage d'alerte du premier fichier attaqué. ONTAP envoie l'événement *Ransomware Detected* à Data Infrastructure Insights lorsqu'un certain nombre de fichiers sont codés. Par conséquent, il peut y avoir une différence entre le moment où l'alerte s'affiche dans l'interface utilisateur et le moment où l'e-mail est envoyé.

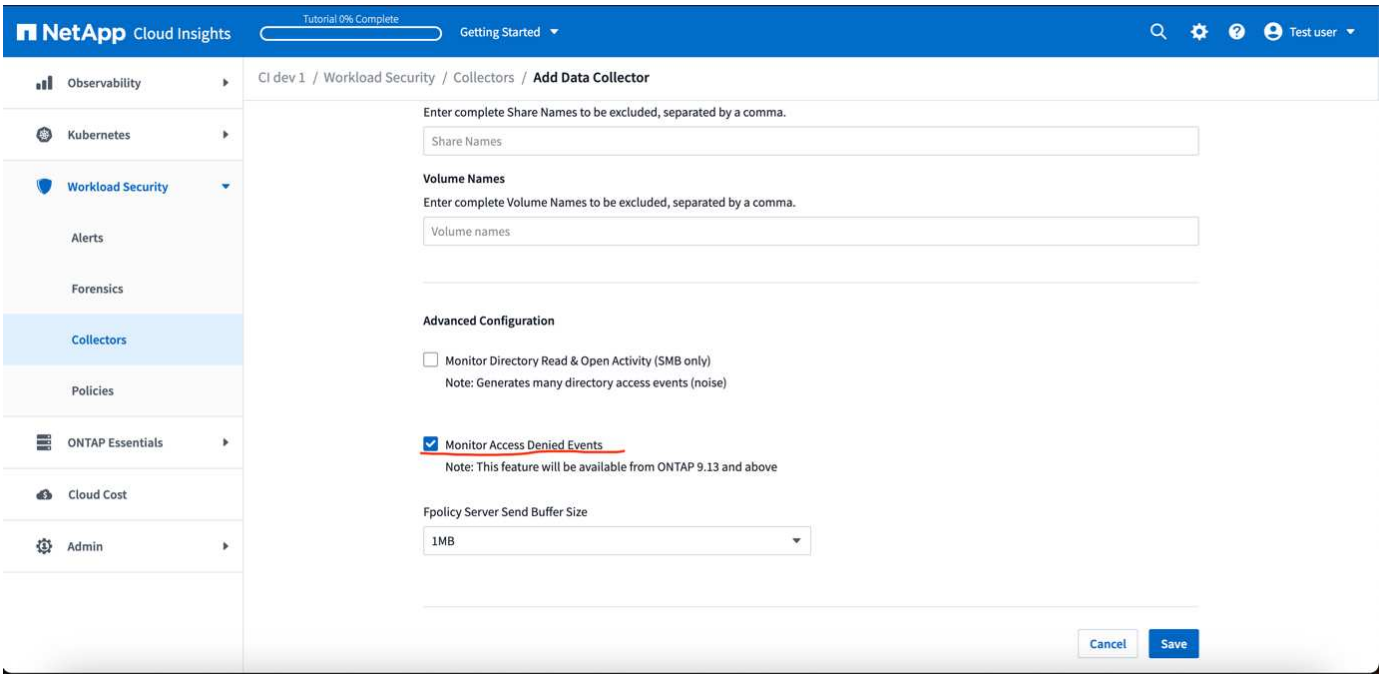
Intégration avec ONTAP Accès refusé

La fonctionnalité ONTAP Access Denied utilise l'analyse de la charge de travail dans les environnements NAS (NFS et SMB) pour détecter et avertir de manière proactive des opérations de fichiers ayant échoué (c'est-à-dire un utilisateur essayant d'effectuer une opération pour laquelle il n'a pas l'autorisation). Ces notifications d'échec d'opération de fichier, en particulier dans les cas de défaillances liées à la sécurité, contribueront davantage à bloquer les attaques internes à un stade précoce.

Data Infrastructure Insights Workload Security s'intègre à ONTAP pour recevoir les événements d'accès refusé et fournir une couche d'analyse et de réponse automatique supplémentaire.

Prérequis

- Version minimale ONTAP : 9.13.0.
- Un administrateur de sécurité de la charge de travail doit activer la fonctionnalité Accès refusé lors de l'ajout d'un nouveau collecteur ou de la modification d'un collecteur existant, en sélectionnant la case à cocher *Surveiller les événements d'accès refusé* sous Configuration avancée.



Autorisations utilisateur requises

Si le collecteur de données est ajouté à l'aide des informations d'identification d'administration du cluster, aucune nouvelle autorisation n'est nécessaire.

Si le collecteur est ajouté à l'aide d'un utilisateur personnalisé (par exemple, *csuser*) avec des autorisations accordées à l'utilisateur, suivez les étapes ci-dessous pour donner à Workload Security l'autorisation nécessaire pour s'inscrire aux événements d'accès refusé avec ONTAP.

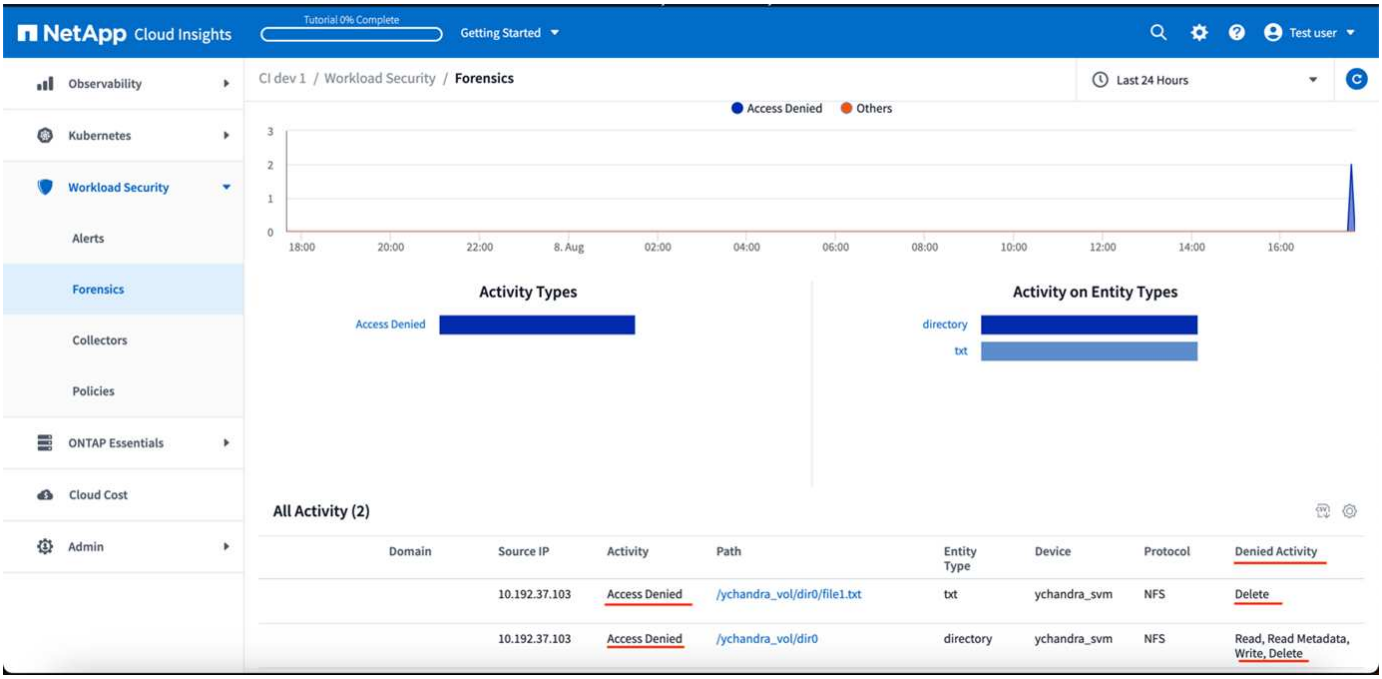
Pour csuser avec les informations d'identification *cluster*, exécutez les commandes suivantes à partir de la ligne de commande ONTAP . Notez que cette autorisation existe peut-être déjà.

```
 security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
Pour csuser avec les informations d'identification _SVM_, exécutez les
commandes suivantes à partir de la ligne de commande ONTAP .  Notez que
cette autorisation existe peut-être déjà.
```

```
 security login role create -vserver <vservername> -role csrole
-cmddirname "vserver fpolicy" -access all
En savoir plus sur la configuration
d'autreslink:task_add_collector_svm.html["Autorisations ONTAP"] .
```

Événements d'accès refusé

Une fois les événements acquis à partir du système ONTAP , la page Forensics de sécurité de la charge de travail affichera les événements d'accès refusé. En plus des informations affichées, vous pouvez afficher les autorisations utilisateur manquantes pour une opération particulière en ajoutant la colonne *Activité souhaitée* au tableau à partir de l'icône d'engrenage.



Bloquer l’accès des utilisateurs pour stopper les attaques

Interrompez immédiatement les attaques détectées en bloquant l’accès des utilisateurs compromis afin d’empêcher toute nouvelle atteinte aux données ou toute exfiltration de données. La sécurité des charges de travail permet à la fois le blocage automatique via des politiques de réponse automatisées et l’intervention manuelle à partir des pages d’alerte ou de détails de l’utilisateur, vous offrant ainsi un contrôle flexible sur votre réponse de sécurité. Les restrictions d’accès s’appliquent automatiquement à tous les volumes de stockage surveillés et sont limitées dans le temps pour la restauration automatique.

L’utilisateur est directement bloqué pour SMB et l’adresse IP des machines hôtes à l’origine de l’attaque sera bloquée pour NFS. Ces adresses IP de machine ne pourront pas accéder aux machines virtuelles de stockage (SVM) surveillées par Workload Security.

Par exemple, disons que Workload Security gère 10 SVM et que la stratégie de réponse automatique est configurée pour quatre de ces SVM. Si l’attaque provient de l’une des quatre SVM, l’accès de l’utilisateur sera bloqué dans les 10 SVM. Un instantané est toujours pris sur le SVM d’origine.

S’il existe quatre SVM, dont une configurée pour SMB, une configurée pour NFS et les deux autres configurées pour NFS et SMB, toutes les SVM seront bloquées si l’attaque provient de l’une des quatre SVM.

Conditions préalables au blocage de l’accès utilisateur

Les informations d’identification au niveau du cluster sont nécessaires pour que cette fonctionnalité fonctionne.

Si vous utilisez les informations d’identification d’administration de cluster, aucune nouvelle autorisation n’est nécessaire.

Si vous utilisez un utilisateur personnalisé (par exemple, *csuser*) avec des autorisations accordées à l’utilisateur, suivez les étapes ci-dessous pour accorder des autorisations à Workload Security afin de bloquer

l'utilisateur.

Pour csuser avec les informations d'identification du cluster, procédez comme suit à partir de la ligne de commande ONTAP :

```
security login role create -role csrole -cmddirname "vserver export-policy
rule" -access all
security login role create -role csrole -cmddirname set -access all
security login role create -role csrole -cmddirname "vserver cifs session"
-access all
security login role create -role csrole -cmddirname "vserver services
access-check authentication translate" -access all
security login role create -role csrole -cmddirname "vserver name-mapping"
-access all
```

Assurez-vous de consulter la section Autorisations du"Configuration du collecteur de données ONTAP SVM" page aussi.

Comment activer la fonctionnalité ?

- Dans Sécurité de la charge de travail, accédez à **Sécurité de la charge de travail > Politiques > Politiques de réponse automatisée**. Choisissez **+Politique d'attaque**.
- Sélectionnez (cochez) *Bloquer l'accès aux fichiers utilisateur*.

Comment configurer le blocage automatique de l'accès des utilisateurs ?

- Créez une nouvelle politique d'attaque ou modifiez une politique d'attaque existante.
- Sélectionnez les SVM sur lesquelles la politique d'attaque doit être surveillée.
- Cochez la case « Bloquer l'accès aux fichiers des utilisateurs ». La fonctionnalité sera activée lorsque cette option est sélectionnée.
- Sous « Période », sélectionnez la durée jusqu'à laquelle le blocage doit être appliqué.
- Pour tester le blocage automatique des utilisateurs, vous pouvez simuler une attaque via un"script simulé" .

Comment savoir s'il y a des utilisateurs bloqués dans le système ?

- Dans la page des listes d'alertes, une bannière en haut de l'écran sera affichée au cas où un utilisateur serait bloqué.
- En cliquant sur la bannière, vous serez redirigé vers la page « Utilisateurs », où la liste des utilisateurs bloqués peut être consultée.
- Dans la page « Utilisateurs », il y a une colonne nommée « Accès utilisateur/IP ». Dans cette colonne, l'état actuel du blocage de l'utilisateur sera affiché.

Restreindre et gérer manuellement l'accès des utilisateurs

- Vous pouvez accéder aux détails de l'alerte ou à l'écran des détails de l'utilisateur, puis bloquer ou restaurer manuellement un utilisateur à partir de ces écrans.

Historique des limitations d’accès des utilisateurs

Dans la page des détails de l’alerte et des détails de l’utilisateur, dans le panneau utilisateur, vous pouvez afficher un audit de l’historique des limitations d’accès de l’utilisateur : heure, action (bloquer, débloquer), durée, action entreprise par, manuel/automatique et adresses IP affectées pour NFS.

Comment désactiver la fonctionnalité ?

À tout moment, vous pouvez désactiver la fonctionnalité. S’il y a des utilisateurs restreints dans le système, vous devez d’abord restaurer leur accès.

- Dans Sécurité de la charge de travail, accédez à **Sécurité de la charge de travail > Politiques > Politiques de réponse automatisée**. Choisissez **+Politique d’attaque**.
- Décochez (désélectionnez) *Bloquer l’accès aux fichiers utilisateur*.

La fonctionnalité sera masquée sur toutes les pages.

Restaurer manuellement les adresses IP pour NFS

Utilisez les étapes suivantes pour restaurer manuellement toutes les adresses IP d' ONTAP si votre essai de Workload Security expire ou si l’agent/collecteur est en panne.

1. Répertoriez toutes les politiques d’exportation sur un SVM.

```
contrail-qa-fas8020:> export-policy rule show -vserver <svm name>
             Policy          Rule    Access   Client                RO
Vserver      Name            Index   Protocol Match                 Rule
------------ --------------- ------  -------- ---------------------
---------
svm0         default         1       nfs3,    cloudsecure_rule,     never
                                     nfs4,    10.11.12.13
                                     cifs
svm1         default         4       cifs,    0.0.0.0/0             any
                                     nfs
svm2         test            1       nfs3,    cloudsecure_rule,     never
                                     nfs4,    10.11.12.13
                                     cifs
svm3         test            3       cifs,    0.0.0.0/0             any
                                     nfs,
                                     flexcache
4 entries were displayed.
```

2. Supprimez les règles de toutes les stratégies sur la SVM qui ont « cloudsecure_rule » comme correspondance client en spécifiant son RuleIndex respectif. La règle de sécurité de la charge de travail sera généralement à 1.

```
 contrail-qa-fas8020:*> export-policy rule delete -vserver <svm name>
-policyname * -ruleindex 1
. Assurez-vous que la règle de sécurité de la charge de travail est
supprimée (étape facultative pour confirmer).
```

```
contrail-qa-fas8020:*> export-policy rule show -vserver <svm name>
             Policy          Rule    Access   Client                RO
Vserver      Name            Index   Protocol Match                 Rule
------------ --------------- ------  -------- ---------------------
---------
svm0         default         4       cifs,    0.0.0.0/0             any
                                     nfs
svm2         test            3       cifs,    0.0.0.0/0             any
                                     nfs,
                                     flexcache
2 entries were displayed.
```

Restaurer manuellement les utilisateurs pour SMB

Utilisez les étapes suivantes pour restaurer manuellement tous les utilisateurs d' ONTAP si votre essai de Workload Security expire ou si l'agent/collecteur est en panne.

Vous pouvez obtenir la liste des utilisateurs bloqués dans Workload Security à partir de la page de la liste des utilisateurs.

1. Connectez-vous au cluster ONTAP (où vous souhaitez débloquer les utilisateurs) avec les informations d'identification *admin* du cluster. (Pour Amazon FSx, connectez-vous avec les informations d'identification FSx).
2. Exécutez la commande suivante pour répertorier tous les utilisateurs bloqués par Workload Security for SMB dans tous les SVM :

```
vserver name-mapping show -direction win-unix -replacement " "
```

```
Vserver:   <vservername>
Direction: win-unix
Position Hostname         IP Address/Mask
-------- ---------------- ----------------
1        -                -                Pattern: CSLAB\\US040
                                           Replacement:
2        -                -                Pattern: CSLAB\\US030
                                           Replacement:
2 entries were displayed.
```

Dans la sortie ci-dessus, 2 utilisateurs ont été bloqués (US030, US040) avec le domaine CSLAB.

1. Une fois que nous avons identifié la position à partir de la sortie ci-dessus, exécutez la commande suivante pour débloquer l'utilisateur :

```
 vserver name-mapping delete -direction win-unix -position <position>
. Confirmez que les utilisateurs sont débloqués en exécutant la
commande :
```

```
vserver name-mapping show -direction win-unix -replacement " "
```

Aucune entrée ne doit être affichée pour les utilisateurs précédemment bloqués.

Dépannage

Problème	Essayez ceci
Certains utilisateurs ne sont pas restreints, même s'il y a une attaque.	1. Assurez-vous que le collecteur de données et l'agent pour les SVM sont à l'état *Running*. Workload Security ne pourra pas envoyer de commandes si le collecteur de données et l'agent sont arrêtés. 2. Cela est dû au fait que l'utilisateur a peut-être accédé au stockage à partir d'une machine avec une nouvelle IP qui n'a pas été utilisée auparavant. La restriction s'effectue via l'adresse IP de l'hôte via lequel l'utilisateur accède au stockage. Consultez l'interface utilisateur (Détails de l'alerte > Historique des limitations d'accès pour cet utilisateur > IP affectées) pour obtenir la liste des adresses IP restreintes. Si l'utilisateur accède au stockage à partir d'un hôte dont l'adresse IP est différente des adresses IP restreintes, l'utilisateur pourra toujours accéder au stockage via l'adresse IP non restreinte. Si l'utilisateur tente d'accéder à partir des hôtes dont les adresses IP sont restreintes, le stockage ne sera pas accessible.
Cliquer manuellement sur Restreindre l'accès donne le message « Les adresses IP de cet utilisateur ont déjà été restreintes ».	L'adresse IP à restreindre est déjà restreinte pour un autre utilisateur.
La politique n'a pas pu être modifiée. Motif : non autorisé pour cette commande.	Vérifiez si vous utilisez csuser, les autorisations sont accordées à l'utilisateur comme mentionné ci-dessus.

Problème	Essayez ceci
Le blocage des utilisateurs (adresse IP) pour NFS fonctionne, mais pour SMB / CIFS, je vois un message d'erreur : « La transformation SID en DomainName a échoué. Raison du délai d'attente : le socket n'est pas établi »	Cela peut arriver si *csuser* n'a pas l'autorisation d'exécuter ssh. (Assurez-vous de la connexion au niveau du cluster, puis assurez-vous que l'utilisateur peut exécuter ssh). Le rôle *csuser* nécessite ces autorisations. https://docs.netapp.com/us-en/cloudinsights/cs_restrict_user_access.html#prerequisites-for-user-access-blocking Pour *csuser* avec les informations d'identification du cluster, procédez comme suit à partir de la ligne de commande ONTAP : security login role create -role csrole -cmddirname "vserver export-policy rule" -access all security login role create -role csrole -cmddirname set -access all security login role create -role csrole -cmddirname "vserver cifs session" -access all security login role create -role csrole -cmddirname "vserver services access-check authentication translate" -access all security login role create -role csrole -cmddirname "vserver name-mapping" -access all Si *csuser* n'est pas utilisé et si l'utilisateur admin au niveau du cluster est utilisé, assurez-vous que l'utilisateur admin dispose de l'autorisation ssh sur ONTAP.
J'obtiens le message d'erreur *SID translate failed. Raison : 255 : Erreur : échec de la commande : non autorisé pour cette commandeErreur : « access-check » n'est pas une commande reconnue*, alors qu'un utilisateur aurait dû être bloqué.	Cela peut se produire lorsque *csuser* ne dispose pas des autorisations correctes. Voir "Conditions préalables au blocage de l'accès utilisateur" pour plus d'informations. Après avoir appliqué les autorisations, il est recommandé de redémarrer le collecteur de données ONTAP et le collecteur de données de l'annuaire utilisateur. Les commandes d'autorisation requises sont répertoriées ci-dessous. ---- création du rôle de connexion de sécurité -role csrole -cmddirname "règle de politique d'exportation vserver" -access all création du rôle de connexion de sécurité -role csrole -cmddirname set -access all création du rôle de connexion de sécurité -role csrole -cmddirname "session cifs vserver" -access all création du rôle de connexion de sécurité -role csrole -cmddirname "traduction d'authentification de vérification d'accès aux services vserver" -access all création du rôle de connexion de sécurité -role csrole -cmddirname "mappage de noms vserver" -access all ----

Sécurité des charges de travail : simulation de falsification de fichiers

Vous pouvez utiliser les instructions de cette page pour simuler une falsification de fichiers à des fins de test ou de démonstration de la sécurité des charges de travail à l'aide du script de simulation de falsification de fichiers inclus.

Choses à noter avant de commencer

- Le script de simulation de falsification de fichiers fonctionne uniquement sous Linux. Le script de simulation doit également générer des alertes à haute fiabilité dans le cas où l'utilisateur aurait intégré ONTAP ARP à Workload Security.
- Workload Security détectera les événements et les alertes générés avec NFS 4.1 uniquement si la version ONTAP est 9.15 ou supérieure.
- Le script est fourni avec les fichiers d'installation de l'agent Workload Security. Il est disponible sur toute machine sur laquelle un agent Workload Security est installé.
- Vous pouvez exécuter le script sur la machine de l'agent Workload Security elle-même ; il n'est pas nécessaire de préparer une autre machine Linux. Cependant, si vous préférez exécuter le script sur un autre système, copiez simplement le script et exécutez-le là-bas.
- Les utilisateurs peuvent opter pour le script Python ou Shell en fonction de leurs préférences et des exigences système.
- Le script Python nécessite des installations préalables. Si vous ne souhaitez pas utiliser Python, utilisez le script shell.

Directives :

Ce script doit être exécuté sur une SVM contenant un dossier avec un nombre substantiel de fichiers à chiffrer, idéalement 100 ou plus, y compris les fichiers dans les sous-dossiers. Assurez-vous que les fichiers ne sont pas vides.

Pour générer l'alerte, mettez temporairement le collecteur en pause avant la création des données de test. Une fois les fichiers d'échantillon générés, reprenez le collecteur et lancez le processus de cryptage.

Mesures:

Préparez le système :

Tout d'abord, montez le volume cible sur la machine. Vous pouvez monter une exportation NFS ou CIFS.

Pour monter l'exportation NFS sous Linux :

```
mount -t nfs -o vers=4.0 10.193.177.158:/svmvol1 /mntpt
mount -t nfs -o vers=4.0 Vserver data IP>:/nfsvol /destinationlinuxfolder
```

Ne montez pas la version NFS 4.1 ; elle n'est pas prise en charge par Fpolicy.

Pour monter CIFS sous Linux :

```
mount -t cifs //10.193.77.91/sharedfolderincluster
/root/destinationfolder/ -o username=raisa
```

Activer la protection autonome contre les ransomwares ONTAP (facultatif) :

Si la version de votre cluster ONTAP est 9.11.1 ou supérieure, vous pouvez activer le service ONTAP Ransomware Protection en exécutant la commande suivante sur la console de commande ONTAP .

```
 security anti-ransomware volume enable -volume [volume_name] -vserver
[svm_name]
Ensuite, configurez un collecteur de données :
```

1. Configurez l'agent Workload Security si ce n'est pas déjà fait.
2. Configurez un collecteur de données SVM si ce n'est pas déjà fait.
3. Assurez-vous que le protocole de montage est sélectionné lors de la configuration du collecteur de données.

Générez les fichiers d'exemple par programmation :

Avant de créer les fichiers, vous devez d'abord arrêter ou"mettre en pause le collecteur de données" traitement.

Avant d'exécuter la simulation, vous devez d'abord ajouter les fichiers à chiffrer. Vous pouvez soit copier manuellement les fichiers à crypter dans le dossier cible, soit utiliser l'un des scripts inclus pour créer les fichiers par programmation. Quelle que soit la méthode utilisée, assurez-vous qu'au moins 100 fichiers sont présents à crypter.

Si vous choisissez de créer les fichiers par programmation, vous pouvez utiliser le Shell ou Python :

Coquille:

1. Connectez-vous à la boîte Agent.
2. Montez un partage NFS ou CIFS depuis la SVM du fichier vers la machine Agent. CD dans ce dossier.
3. Copiez le script du répertoire d'installation de l'agent (%AGENT_INSTALL_DIR/agent/install/ransomware_simulation/shell/create_dataset.sh) vers l'emplacement de montage cible.
4. Exécutez la commande suivante à l'aide des scripts dans le répertoire monté (par exemple /root/demo) pour créer le dossier et les fichiers du jeu de données de test :

```
 './create_dataset.sh'
. Cela créera 100 fichiers non vides avec différentes extensions dans le
dossier de montage sous un répertoire appelé « test_dataset ».
```

Python:

Script Python Prérequis :

- Installez Python (si ce n'est pas déjà fait).
  - Téléchargez Python 3.5.2 ou supérieur depuis https://www.python.org/ .
  - Pour vérifier l'installation de Python, exécutez `python --version` .
  - Le script Python a été testé sur des versions aussi anciennes que la 3.5.2.
- Installez pip s'il n'est pas déjà installé :

- Téléchargez le script get-pip.py depuis https://bootstrap.pypa.io/ .
- Installer pip en utilisant `python get-pip.py` .
- Vérifiez l'installation de pip avec `pip --version` .

- Bibliothèque PyCryptodome :
  - Le script utilise la bibliothèque PyCryptodome.
  - Installer PyCryptodome avec `pip install pycryptodome` .
  - Confirmez l'installation de PyCryptodome en exécutant `pip show pycryptodome` .

Script de création de fichier Python :

1. Connectez-vous à la boîte Agent.
2. Montez un partage NFS ou CIFS depuis la SVM du fichier vers la machine Agent. CD dans ce dossier.
3. Copiez le script du répertoire d'installation de l'agent (%AGENT_INSTALL_DIR/agent/install/ransomware_simulation/python/create_dataset.py) vers l'emplacement de montage cible.
4. Exécutez la commande suivante à l'aide des scripts dans le répertoire monté (par exemple /root/demo) pour créer le dossier et les fichiers du jeu de données de test :

```
 'python create_dataset.py'
. Cela créera 100 fichiers non vides avec différentes extensions à
l'intérieur du dossier de montage sous un répertoire appelé
« test_dataset »
```

Reprendre le collecteur

Si vous avez mis le collecteur en pause avant de suivre ces étapes, assurez-vous de reprendre le collecteur une fois les fichiers d'exemple créés.

Générez les fichiers d'exemple par programmation :

Avant de créer les fichiers, vous devez d'abord arrêter ou"mettre en pause le collecteur de données" traitement.

Pour générer une alerte de falsification de fichier, vous pouvez exécuter le script inclus qui simulera une alerte de falsification de fichier dans Workload Security.

Coquille:

1. Copiez le script du répertoire d'installation de l'agent (%AGENT_INSTALL_DIR/agent/install/ransomware_simulation/shell/simulate_attack.sh) vers l'emplacement de montage cible.
2. Exécutez la commande suivante à l'aide des scripts dans le répertoire monté (par exemple /root/demo) pour crypter l'ensemble de données de test :

```
 './simulate_attack.sh'
. Cela cryptera les fichiers d'exemple créés sous le répertoire
« test_dataset ».
```

Python:

1. Copiez le script du répertoire d'installation de l'agent (%AGENT_INSTALL_DIR/agent/install/ransomware_simulation/python/simulate_attack.py) vers l'emplacement de montage cible.
2. Veuillez noter que les prérequis Python sont installés conformément à la section Prérequis du script Python
3. Exécutez la commande suivante à l'aide des scripts dans le répertoire monté (par exemple /root/demo) pour crypter l'ensemble de données de test :

```
 'python simulate_attack.py'
. Cela cryptera les fichiers d'exemple créés sous le répertoire
« test_dataset ».
```

Générer une alerte dans Workload Security

Une fois l'exécution du script du simulateur terminée, une alerte s'affichera sur l'interface Web dans quelques minutes.

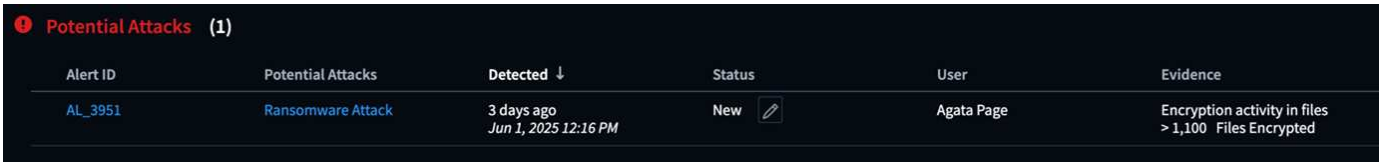
Remarque : si toutes les conditions suivantes sont remplies, une alerte de haute confiance sera générée.

1. Version ONTAP du SVM surveillée supérieure à 9.11.1
2. Protection autonome contre les ransomwares ONTAP configurée
3. Le collecteur de données de sécurité de la charge de travail est ajouté en mode Cluster.

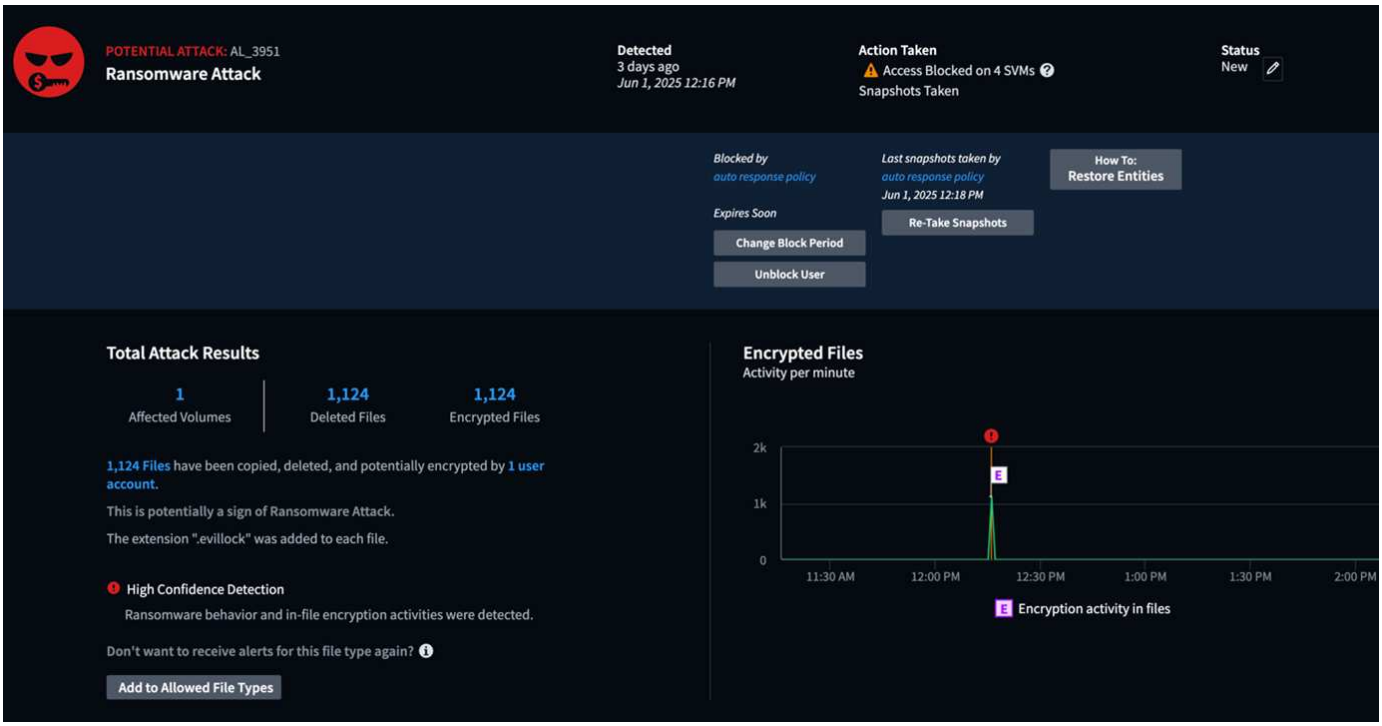
Workload Security détecte les schémas de falsification de fichiers en fonction du comportement de l'utilisateur, tandis ONTAP ARP détecte les activités de falsification de fichiers en fonction des activités de chiffrement dans les fichiers.

Si les conditions sont remplies, Workload Security marque les alertes comme alerte de haute confiance.

Exemple d'alerte de haute confiance sur la page de liste des alertes :



Exemple de détail d'alerte de haute confiance :



Déclenchement de l’alerte plusieurs fois

Workload Security analyse le comportement des utilisateurs et ne génère pas d’alertes en cas d’attaques répétées de falsification de fichiers survenant dans un délai de 24 heures pour un même utilisateur.

Pour générer une nouvelle alerte avec un utilisateur différent, veuillez suivre à nouveau les mêmes étapes (création de données de test puis cryptage des données de test).

Configuration des notifications par e-mail pour les alertes, les avertissements et l’état de santé de l’agent/collecteur de sources de données

Les notifications par e-mail vous permettent de rester informé des attaques potentielles, des alertes de sécurité et des problèmes de santé de l’infrastructure dès leur apparition. Configurez les adresses e-mail des destinataires dans les paramètres Admin > Notifications pour recevoir des alertes en temps réel adaptées aux responsabilités de chaque destinataire.

Alertes et avertissements d’attaque potentielle

Pour envoyer des notifications d’alerte d’attaque potentielle, saisissez les adresses e-mail des destinataires dans la section *Envoyer des alertes d’attaque potentielle*. Des notifications par courrier électronique sont envoyées à la liste des destinataires de l’alerte pour chaque action sur l’alerte.

Pour envoyer des notifications d’avertissement, saisissez les adresses e-mail des destinataires dans la section Envoyer des alertes d’avertissement.

Surveillance de la santé des agents et des collecteurs de données

Vous pouvez surveiller la santé des agents et des sources de données via des notifications.

Afin de recevoir des notifications dans le cas où un agent ou un collecteur de sources de données ne fonctionne pas, saisissez les adresses e-mail des destinataires dans la section *Alertes de santé de la collecte de données*.

Gardez à l'esprit les points suivants :

- Les alertes de santé ne seront envoyées qu'après que l'agent/collecteur aura cessé de signaler pendant au moins une heure.
- Une seule notification par e-mail est envoyée aux destinataires prévus au cours d'une période donnée de 24 heures, même si l'agent ou le collecteur de données est déconnecté pendant une durée plus longue.
- En cas de défaillance d'un Agent, une seule alerte sera envoyée (pas une par collecteur). L'e-mail comprendra une liste de tous les SVM concernés.
- L'échec de la collecte Active Directory est signalé comme un avertissement ; il n'a pas d'incidence sur la détection des menaces.
- La liste de configuration de mise en route inclut désormais une nouvelle phase *Configurer les notifications par e-mail*.

Notifications de mise à niveau de l'agent récepteur et du collecteur de données

- Saisissez les identifiants de messagerie dans les « Alertes de santé de collecte de données ».
- La case à cocher « Activer les notifications de mise à niveau » devient activée.
- Les notifications par e-mail de mise à niveau de l'agent et du collecteur de données sont envoyées aux identifiants de messagerie un jour avant la mise à niveau prévue.

Dépannage

Problème:	Essayez ceci :
Les identifiants de messagerie sont présents dans les « Alertes de santé du collecteur de données », mais je ne reçois pas de notifications.	Les e-mails de notification sont envoyés depuis le domaine NetApp Data Infrastructure Insights , c'est-à-dire depuis *accounts@service.cloudinsights.netapp.com*. Certaines entreprises bloquent les e-mails entrants s'ils proviennent d'un domaine externe. Assurez-vous que les notifications externes des domaines NetApp Data Infrastructure Insights sont sur liste blanche.

Notifications Webhook

Notifications de sécurité de la charge de travail à l'aide de webhooks

Les webhooks permettent aux utilisateurs d'envoyer des notifications d'alerte critiques ou d'avertissement à diverses applications à l'aide d'un canal webhook personnalisé.

De nombreuses applications commerciales prennent en charge les webhooks comme interface d'entrée standard, par exemple : Slack, PagerDuty, Teams et Discord. En prenant en charge un canal webhook

générique et personnalisable, Workload Security peut prendre en charge bon nombre de ces canaux de diffusion. Des informations sur la configuration des webhooks peuvent être trouvées sur les sites Web des applications respectives. Par exemple, Slack fournit"ce guide utile" .

Vous pouvez créer plusieurs canaux webhook, chaque canal ciblant un objectif différent, des applications distinctes, des destinataires différents, etc.

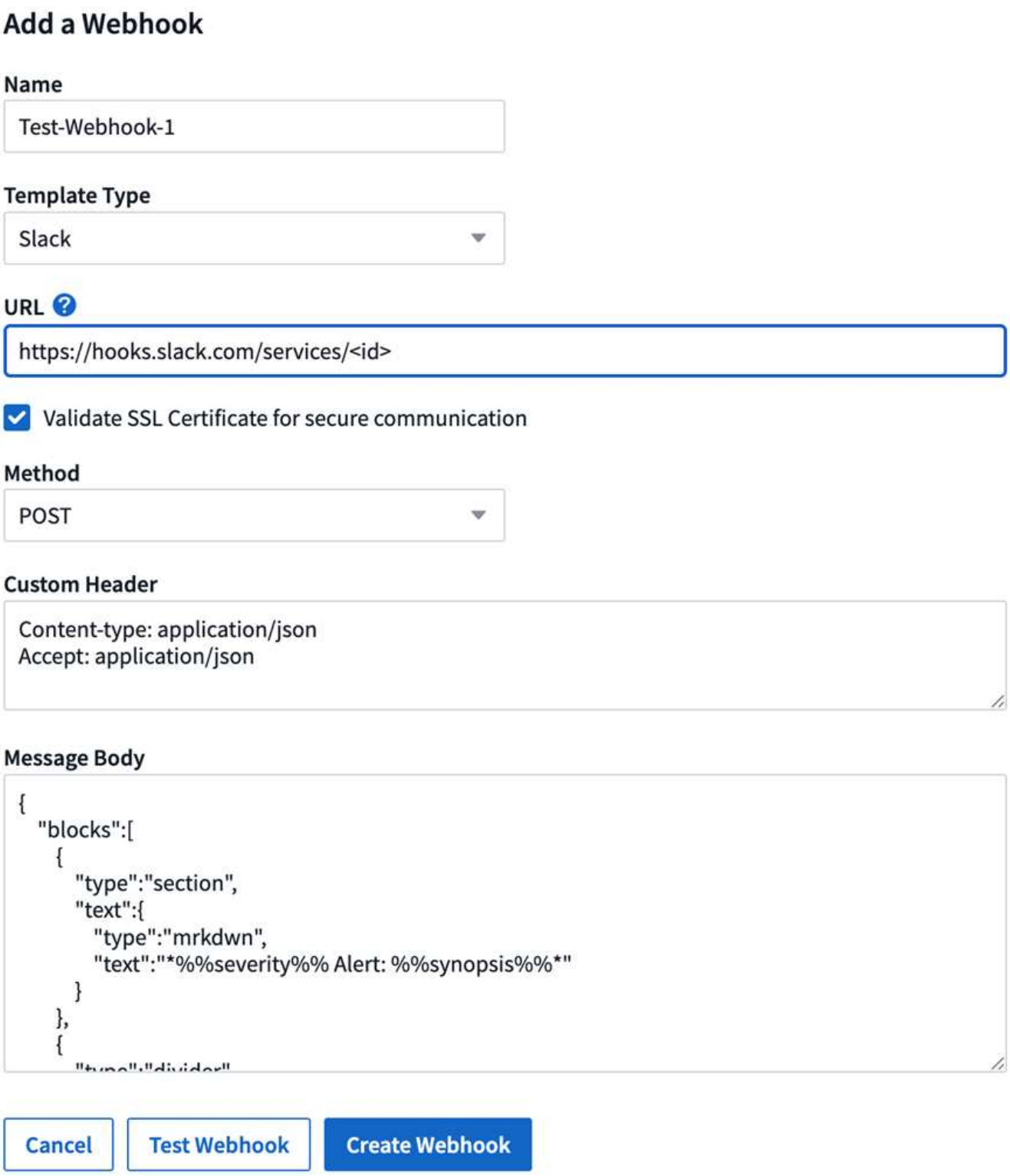
L'instance de canal webhook est composée des éléments suivants

Nom	Description
URL	URL cible du webhook, y compris le préfixe http:// ou https:// ainsi que les paramètres d'URL
Méthode	GET/POST - La valeur par défaut est POST
En-tête personnalisé	Spécifiez ici les en-têtes personnalisés
Corps du message	Mettez le corps de votre message ici
Paramètres d'alerte par défaut	Répertorie les paramètres par défaut du webhook
Paramètres et secrets personnalisés	Les paramètres et secrets personnalisés vous permettent d'ajouter des paramètres uniques et des éléments sécurisés tels que des mots de passe

Créer un webhook

Pour créer un Webhook de sécurité de charge de travail, accédez à Admin > Notifications et sélectionnez l'onglet « Webhooks de sécurité de charge de travail ». L'image suivante montre un exemple d'écran de création de webhook Slack.

Remarque : l'utilisateur doit être un administrateur de Workload Security pour créer et gérer les Webhooks de Workload Security.



- Saisissez les informations appropriées pour chacun des champs et cliquez sur « Enregistrer ».
- Vous pouvez également cliquer sur le bouton « Tester le Webhook » pour tester la connexion. Notez que cela enverra le « Corps du message » (sans substitutions) à l'URL définie selon la méthode sélectionnée.
- Les webhooks SWS comprennent un certain nombre de paramètres par défaut. De plus, vous pouvez créer vos propres paramètres ou secrets personnalisés.

Paramètres : que sont-ils et comment les utiliser ?

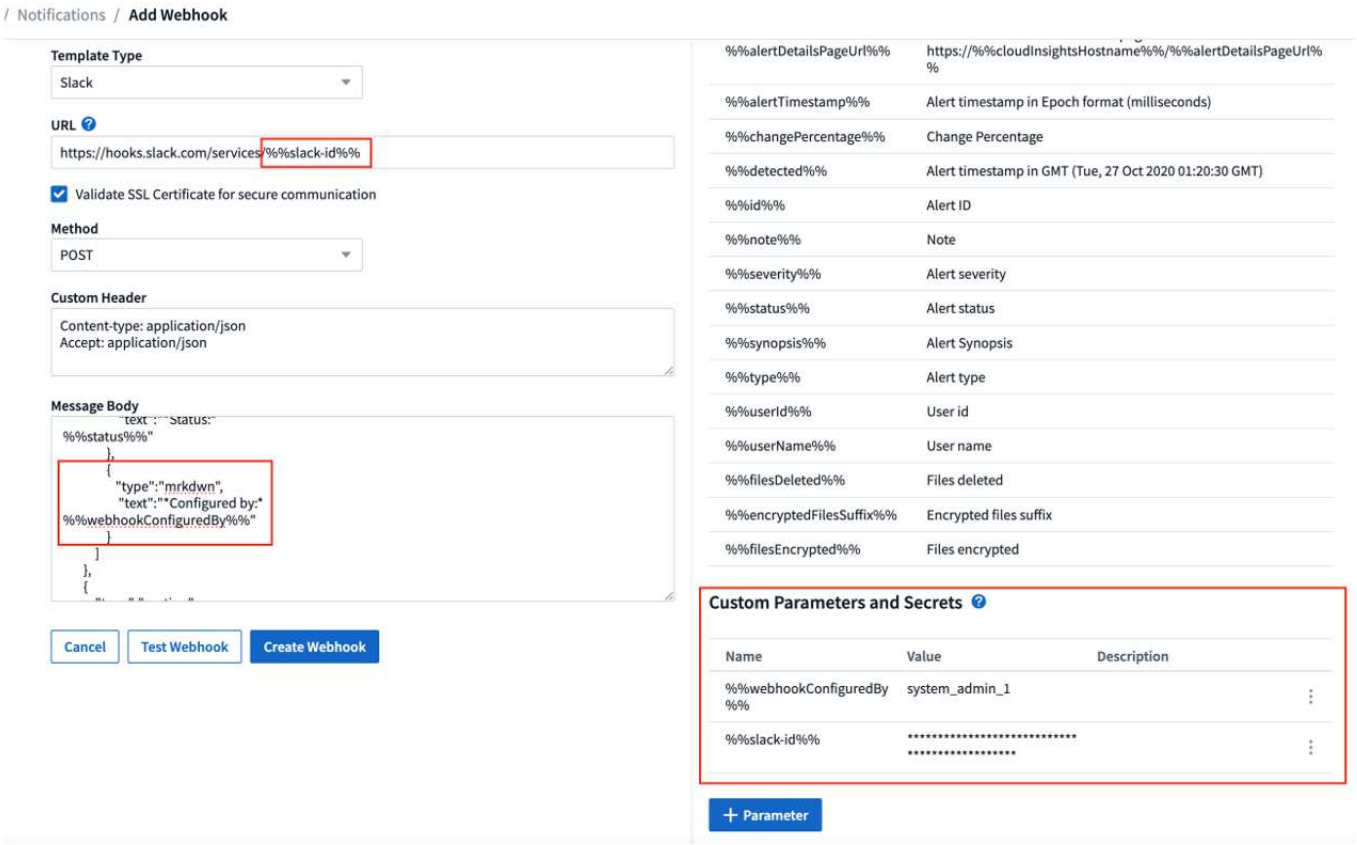
Les paramètres d'alerte sont des valeurs dynamiques renseignées par alerte. Par exemple, le paramètre *%%severity%%* sera remplacé par le type de gravité de l'alerte.

Notez que les substitutions ne sont pas effectuées lorsque vous cliquez sur le bouton « Tester le Webhook » ; le test envoie une charge utile qui affiche les espaces réservés du paramètre (*%%<param-name>%%*) mais ne les remplace pas par des données.

Paramètres et secrets personnalisés

Dans cette section, vous pouvez ajouter tous les paramètres personnalisés et/ou secrets que vous souhaitez. Un paramètre personnalisé ou un secret peut figurer dans l'URL ou le corps du message. Les secrets permettent à l'utilisateur de configurer un paramètre personnalisé sécurisé comme un mot de passe, une clé API, etc.

L'exemple d'image suivant montre comment les paramètres personnalisés sont utilisés dans la création de webhook.



Page de liste des webhooks de sécurité de la charge de travail

Sur la page de liste des Webhooks, les champs Nom, Créé par, Créé le, Statut, Sécurisé et Dernier signalement sont affichés. Remarque : la valeur de la colonne « statut » continuera de changer en fonction du résultat du dernier déclencheur de webhook. Voici quelques exemples de résultats d'état.

Statut	Description
OK	Notification envoyée avec succès.

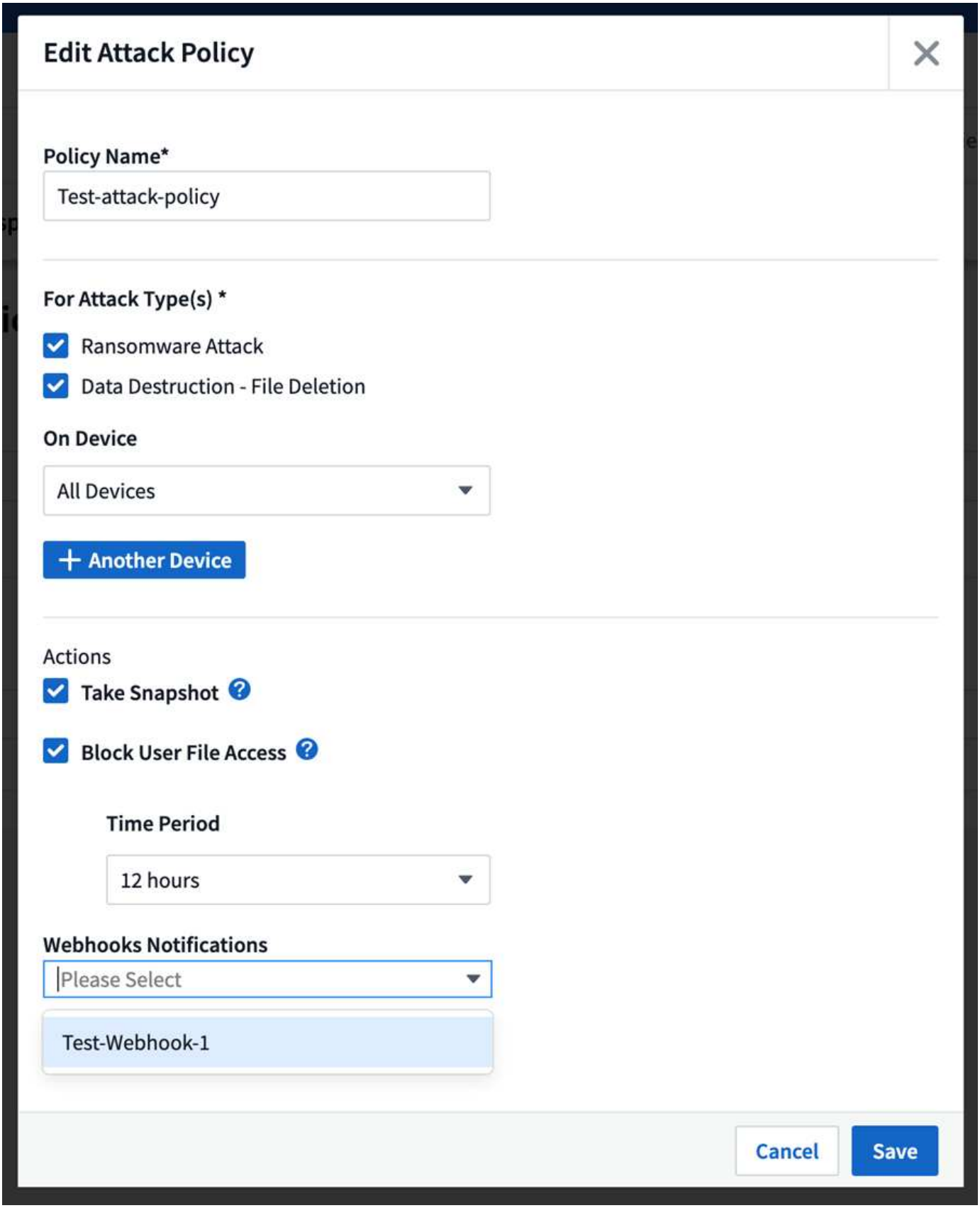
403	Interdit.
404	URL non trouvée.
400	Mauvaise demande. Vous pouvez voir ce statut s'il y a une erreur dans le corps du message, par exemple : • Json mal formaté. • Fourniture d'une valeur non valide pour les clés réservées. Par exemple, PagerDuty accepte uniquement les valeurs critiques/avertissements/erreurs/informations pour « Gravité ». Tout autre résultat peut donner un statut 400. • Erreurs de validation spécifiques à l'application. Par exemple, Slack autorise un maximum de 10 champs dans une section. L'inclusion de plus de 10 peut entraîner un statut 400.
410	La ressource n'est plus disponible

La colonne « Dernier signalement » indique l'heure à laquelle le webhook a été déclenché pour la dernière fois.

À partir de la page de liste des webhooks, les utilisateurs peuvent également modifier/dupliquer/supprimer les webhooks.

Configurer la notification Webhook dans la politique d'alerte

Pour ajouter une notification webhook à une politique d'alerte, accédez à - Sécurité de la charge de travail > Politiques - et sélectionnez une politique existante ou ajoutez une nouvelle politique. Dans la section *Actions* > liste déroulante *Notifications Webhook*, sélectionnez les webhooks requis.



Les notifications Webhook sont liées aux politiques. Lorsque l'attaque (RW/DD/WARN) se produit, l'action configurée (Prendre un instantané / blocage de l'utilisateur) sera effectuée, puis la notification webhook associée sera déclenchée.

Remarque : les notifications par e-mail sont indépendantes des politiques, elles seront déclenchées comme d'habitude.

- Si une politique est suspendue, les notifications webhook ne seront pas déclenchées.
- Plusieurs webhooks peuvent être attachés à une seule politique, mais il est recommandé de ne pas attacher plus de 5 webhooks à une politique.

Exemples de webhooks de sécurité de charge de travail

Webhooks pour"Mou"

Webhooks pour"PagerDuty" Webhooks pour"Équipes" Webhooks pour"Discorde"

Exemple de webhook de sécurité de charge de travail pour Discord

Les webhooks permettent aux utilisateurs d'envoyer des notifications d'alerte à diverses applications à l'aide d'un canal webhook personnalisé. Cette page fournit un exemple de configuration de webhooks pour Discord.

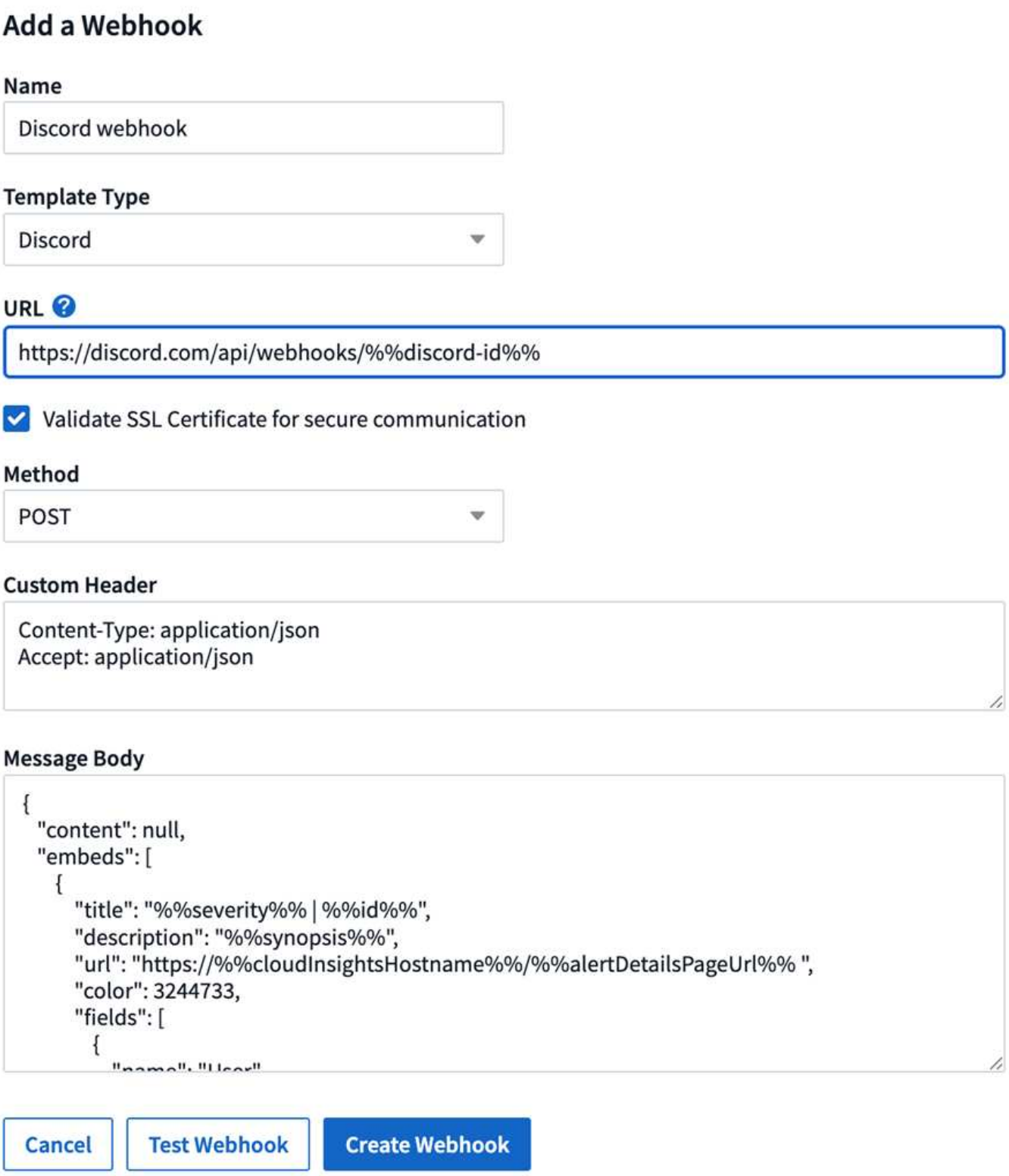
Cette page fait référence à des instructions de tiers, qui sont susceptibles d'être modifiées. Reportez-vous à la"Documentation Discord" pour les informations les plus récentes.

Configuration de Discord :

- Dans Discord, sélectionnez le serveur, sous Canaux texte, sélectionnez Modifier le canal (icône en forme d'engrenage)
- Sélectionnez **Intégrations > Afficher les webhooks** et cliquez sur **Nouveau webhook**
- Copiez l'URL du Webhook. Vous devrez coller ceci dans la configuration du webhook Workload Security.

Créer un webhook de sécurité de charge de travail :

1. Accédez à Admin > Notifications et sélectionnez l'onglet *Webhooks de sécurité de la charge de travail*. Cliquez sur « + Webhook » pour créer un nouveau webhook.
2. Donnez au webhook un nom significatif.
3. Dans la liste déroulante *Type de modèle*, sélectionnez **Discord**.
4. Collez l'URL Discord ci-dessus dans le champ *URL*.



Afin de tester le webhook, remplacez temporairement la valeur de l'URL dans le corps du message par n'importe quelle URL valide (telle que *https://netapp.com*), puis cliquez sur le bouton *Tester le Webhook*. Discord exige qu'une URL valide soit fournie pour que la fonctionnalité Test Webhook fonctionne.

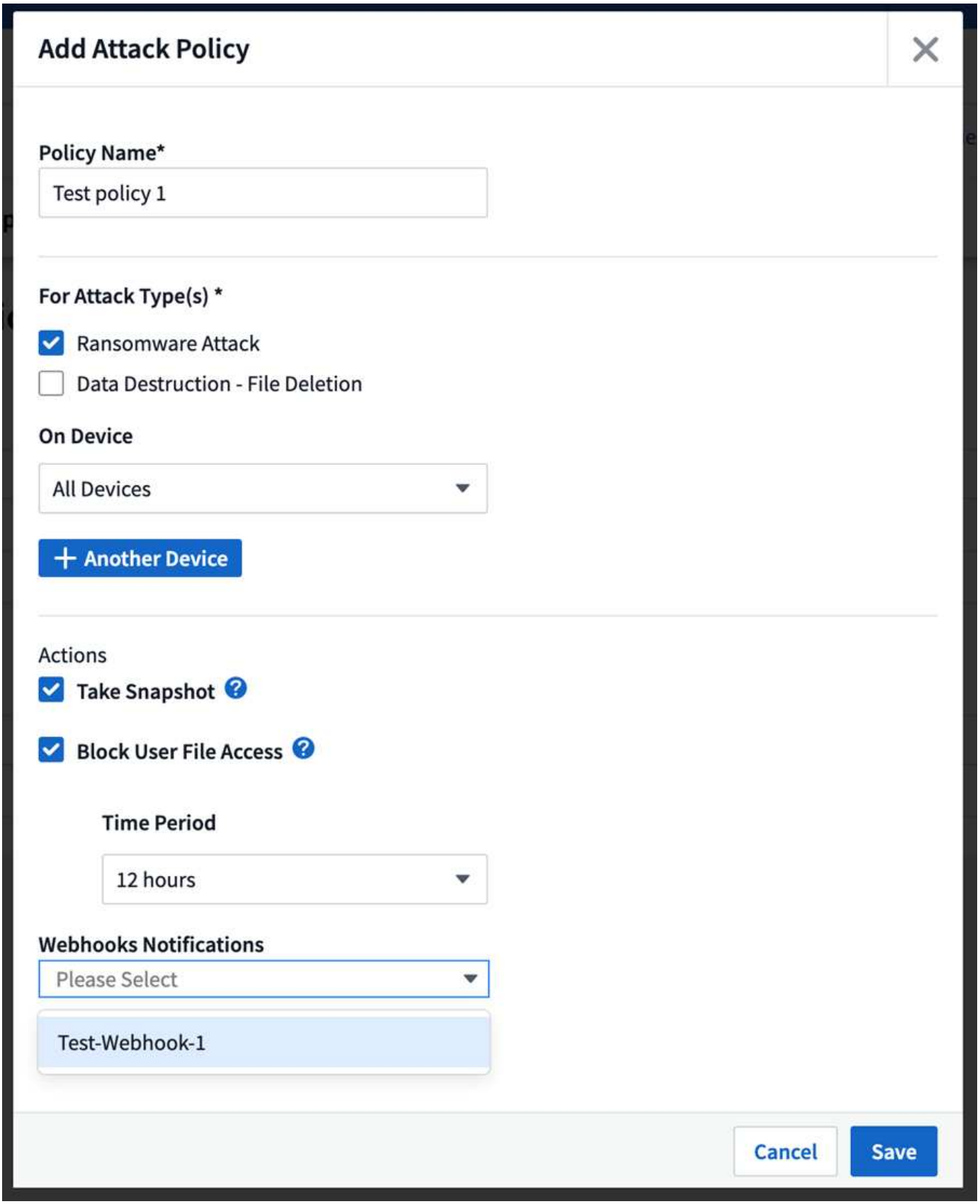
Assurez-vous de réinitialiser le corps du message une fois le test terminé.

Notifications via Webhook

Pour notifier les événements via le webhook, accédez à *Sécurité de la charge de travail > Politiques*. Cliquez sur *+Politique d'attaque* ou *+Politique d'avertissement*.

- Saisissez un nom de politique significatif.
- Sélectionnez les types d'attaque requis, les périphériques auxquels la stratégie doit être associée et les actions requises.
- Sous la liste déroulante *Notifications Webhooks*, sélectionnez les webhooks Discord requis et enregistrez.

Remarque : les webhooks peuvent également être attachés à des politiques existantes en les modifiant.



Exemple de webhook de sécurité de charge de travail pour PagerDuty

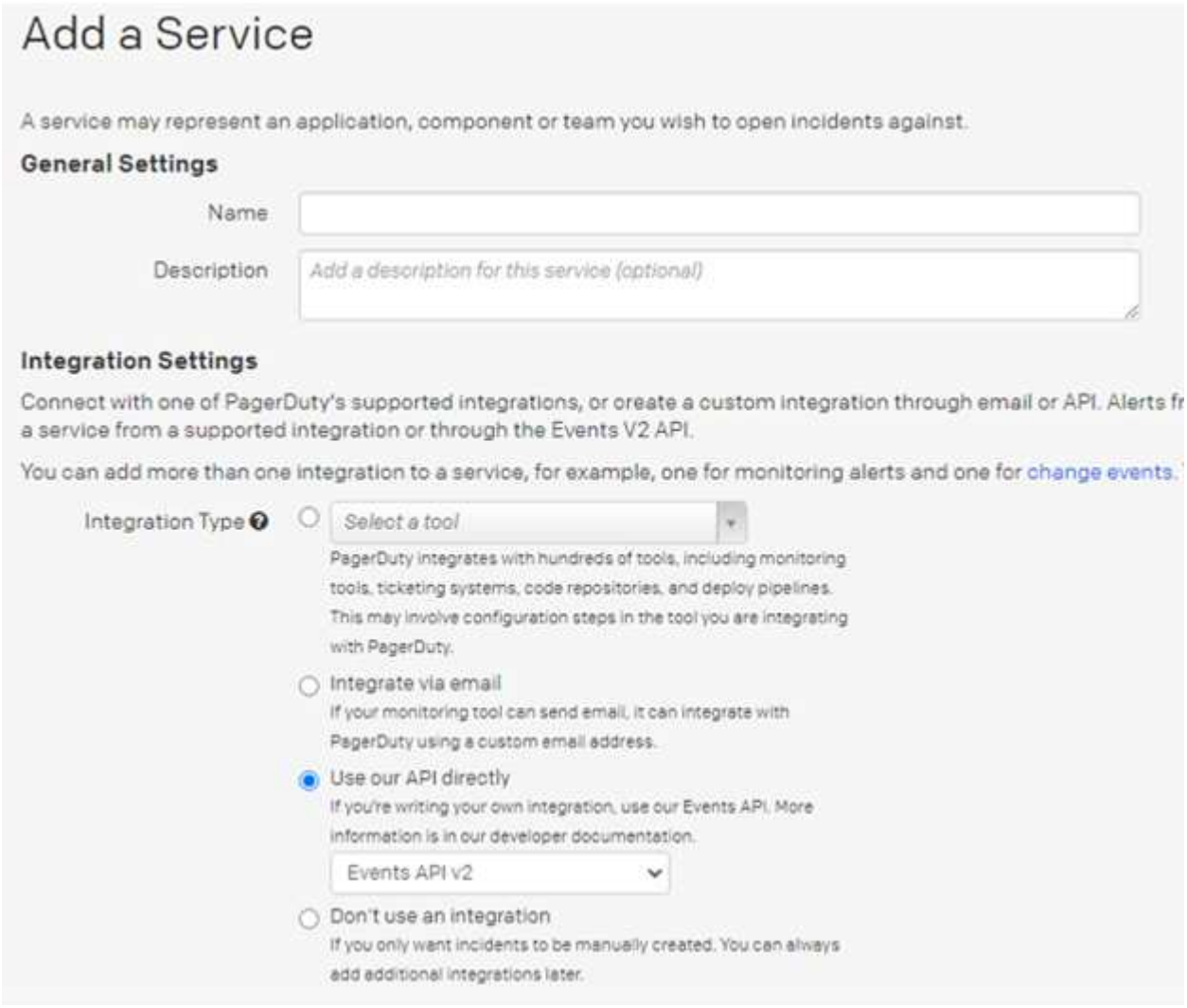
Les webhooks permettent aux utilisateurs d'envoyer des notifications d'alerte à diverses applications à l'aide d'un canal webhook personnalisé. Cette page fournit un exemple de

configuration de webhooks pour PagerDuty.

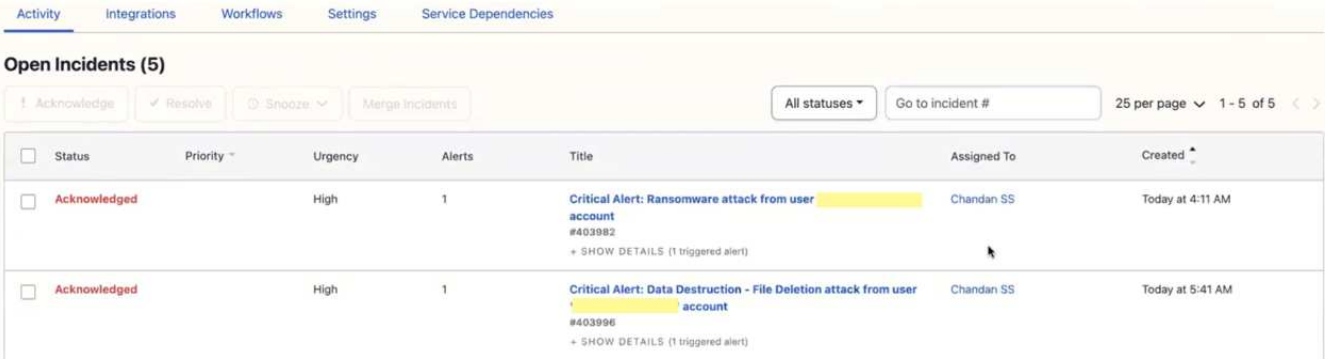
Cette page fait référence à des instructions de tiers, qui sont susceptibles d'être modifiées. Reportez-vous à la"Documentation de PagerDuty" pour les informations les plus récentes.

Configuration de PagerDuty :

1. Dans PagerDuty, accédez à **Services > Répertoire des services** et cliquez sur le bouton **+Nouveau service**.
2. Saisissez un *Nom* et sélectionnez *Utiliser directement notre API*. Sélectionnez *Ajouter un service*.

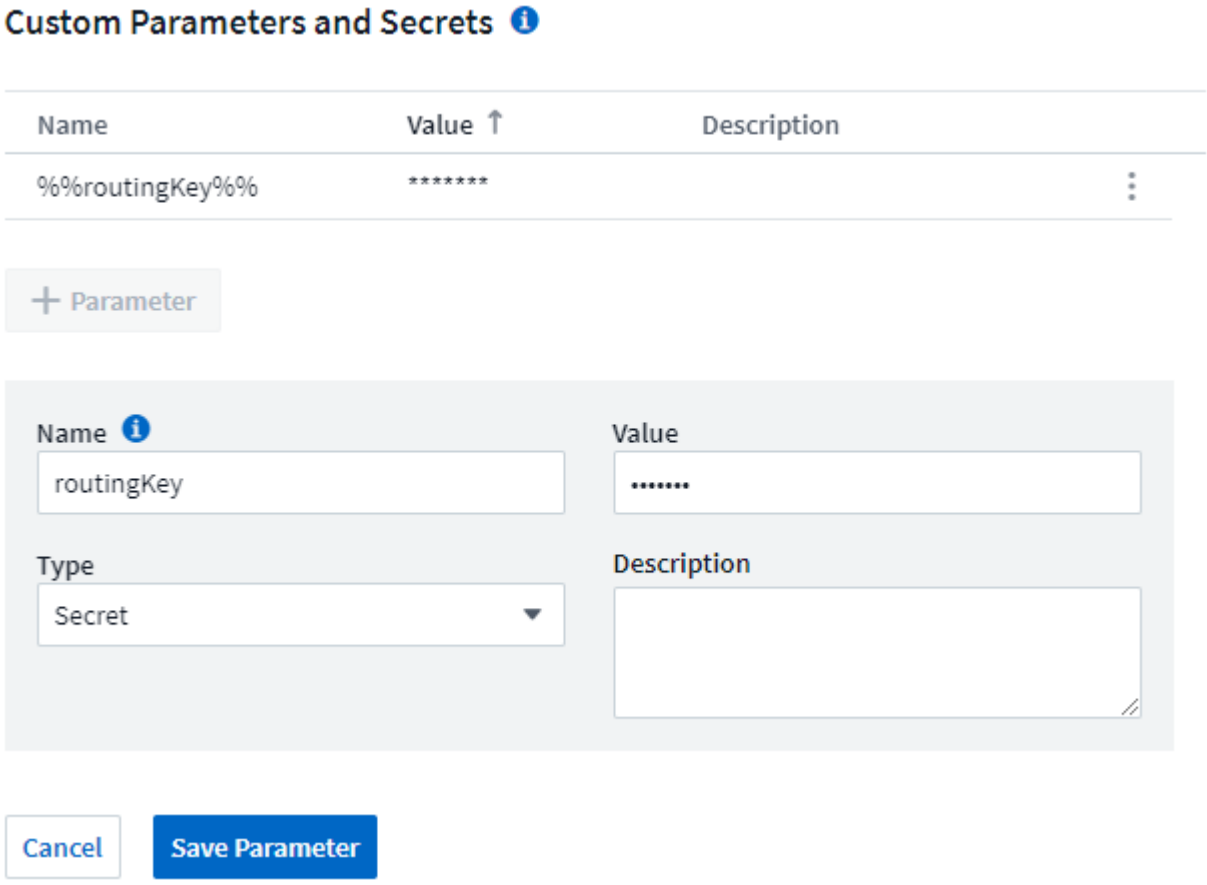


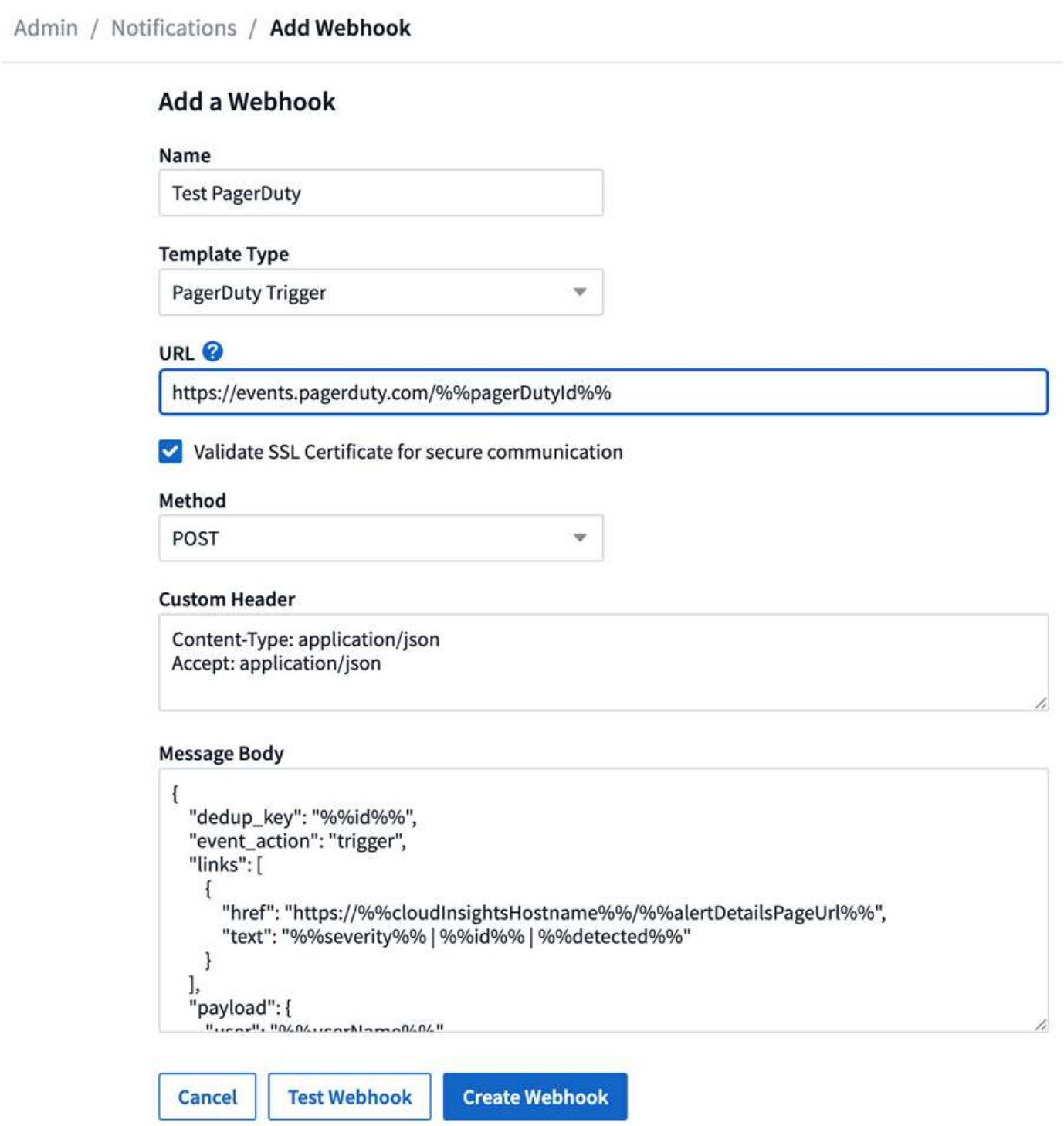
3. Sélectionnez l'onglet *Intégrations* pour voir la **Clé d'intégration**. Vous aurez besoin de cette clé lorsque vous créerez le webhook Workload Security ci-dessous.
4. Accédez à **Incidents** ou **Services** pour afficher les alertes.



Créer un Webhook PagerDuty de sécurité de charge de travail :

- Accédez à Admin > Notifications et sélectionnez l'onglet *Webhooks de sécurité de la charge de travail*. Sélectionnez « + Webhook » pour créer un nouveau webhook.
- Donnez au webhook un nom significatif.
- Dans la liste déroulante *Type de modèle*, sélectionnez *Déclencheur PagerDuty*.
- Créez un secret de paramètre personnalisé nommé *routingKey* et définissez la valeur sur la clé d'intégration PagerDuty *Integration Key* créée ci-dessus.

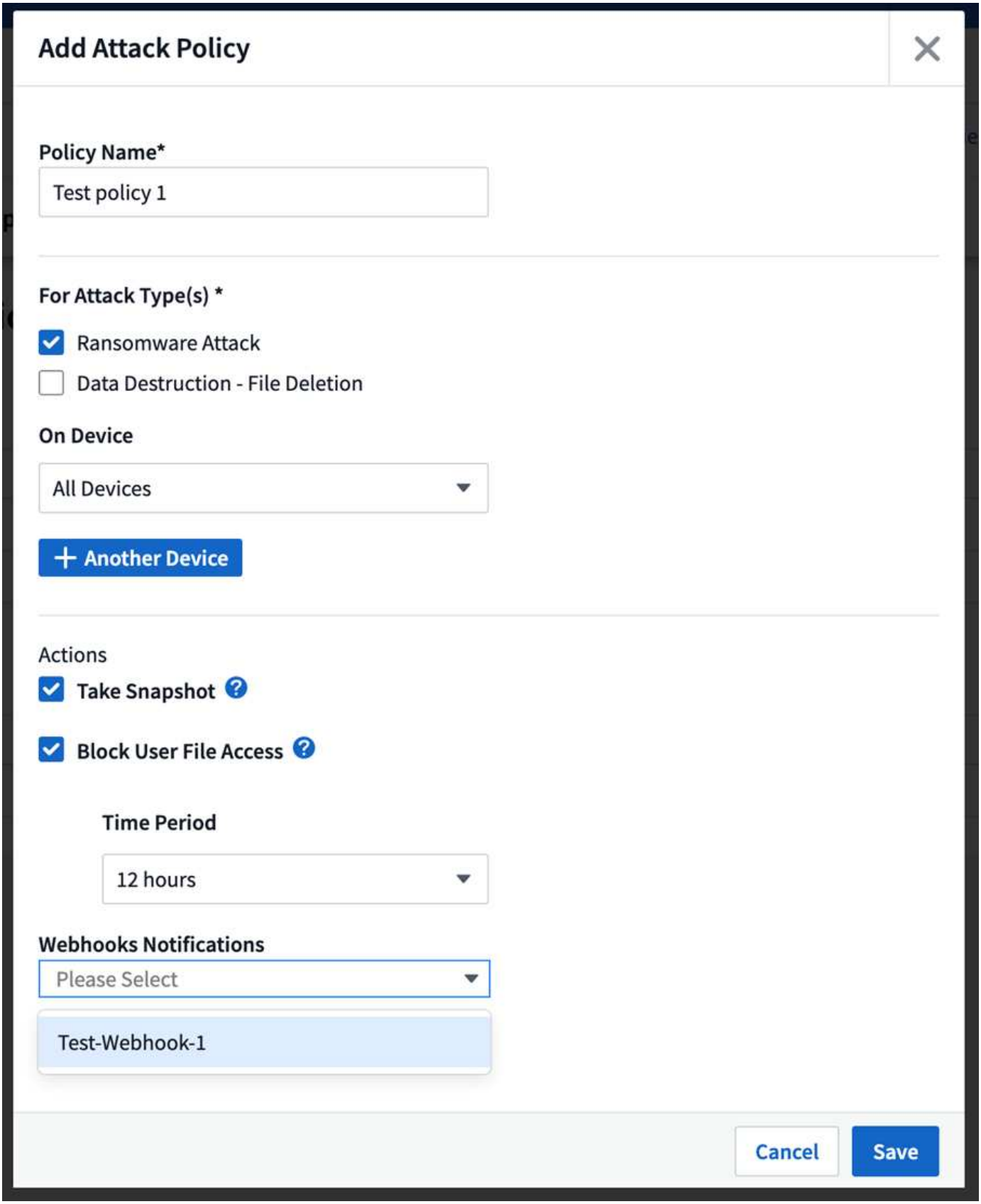




Notifications via Webhook

- Pour notifier les événements via le webhook, accédez à *Sécurité de la charge de travail > Politiques*. Sélectionnez *+Politique d'attaque* ou *+Politique d'avertissement*.
- Saisissez un nom de politique significatif.
- Sélectionnez les types d'attaque requis, les périphériques auxquels la politique doit être attachée et les actions requises.
- Sous la liste déroulante *Notifications Webhooks*, sélectionnez les webhooks PagerDuty requis. Sauvegarder la politique.

Remarque : les webhooks peuvent également être attachés à des politiques existantes en les modifiant.



Exemple de webhook de sécurité de charge de travail pour Slack

Les webhooks permettent aux utilisateurs d'envoyer des notifications d'alerte à diverses applications à l'aide d'un canal webhook personnalisé. Cette page fournit un exemple de configuration de webhooks pour Slack.

Cette page fait référence à des instructions de tiers, qui sont susceptibles d'être modifiées. Consultez la documentation Slack pour obtenir les informations les plus récentes.

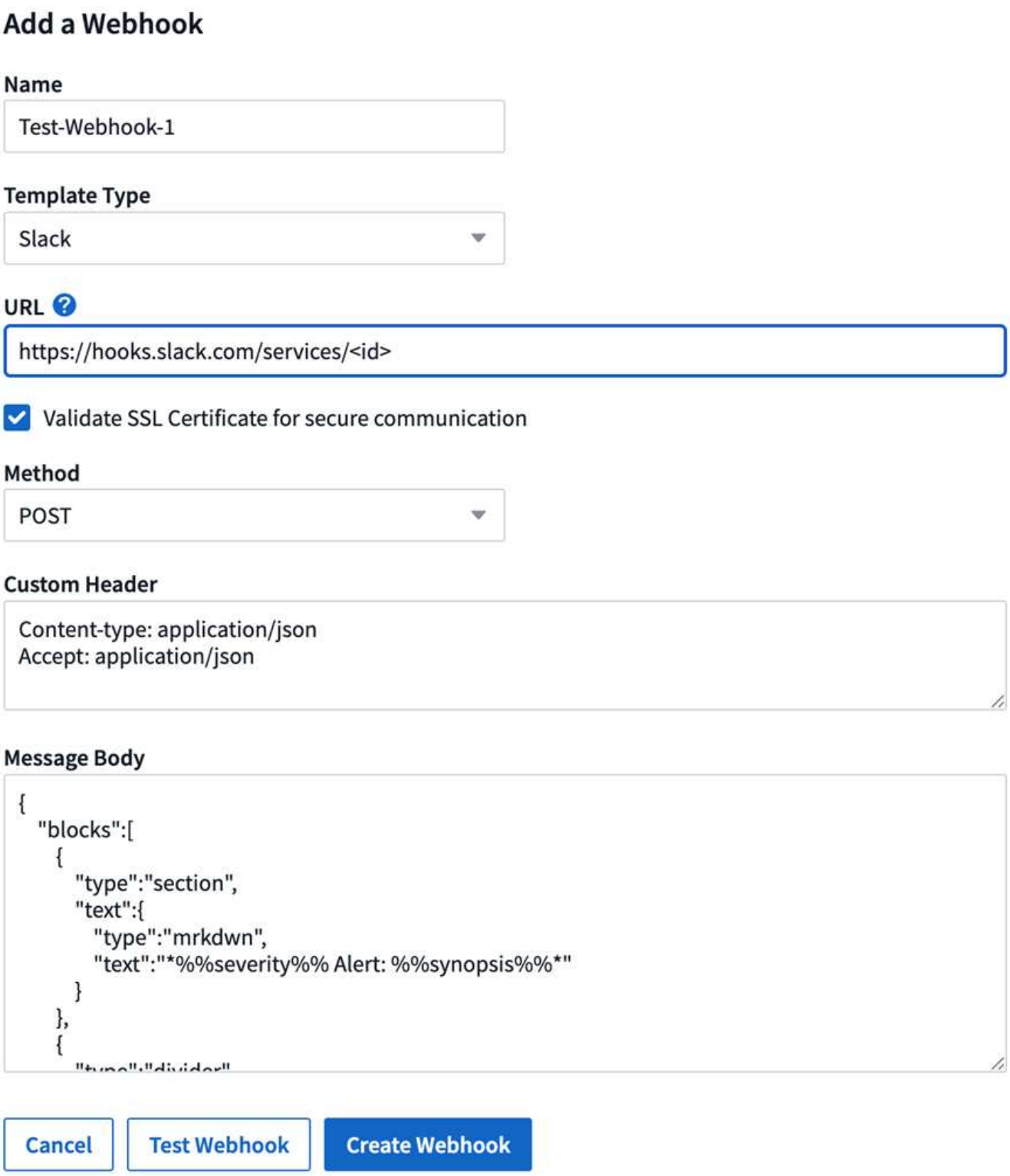
Exemple de Slack

- Aller à https://api.slack.com/apps et créez une nouvelle application. Donnez-lui un nom significatif et sélectionnez un espace de travail.

- Accédez à Webhooks entrants, cliquez sur *Activer les Webhooks entrants*, sélectionnez *Ajouter un nouveau Webhook* et sélectionnez le canal sur lequel publier.
- Copiez l'URL du Webhook. Cette URL sera fournie lors de la création d'un webhook Workload Security.

Créer un webhook Slack pour la sécurité de la charge de travail

1. Accédez à Admin > Notifications et sélectionnez l'onglet *Webhooks de sécurité de la charge de travail*. Sélectionnez _+ *Webhook* pour créer un nouveau webhook.
2. Donnez au webhook un nom significatif.
3. Dans la liste déroulante *Type de modèle*, sélectionnez *Slack*.
4. Collez l'URL copiée ci-dessus.

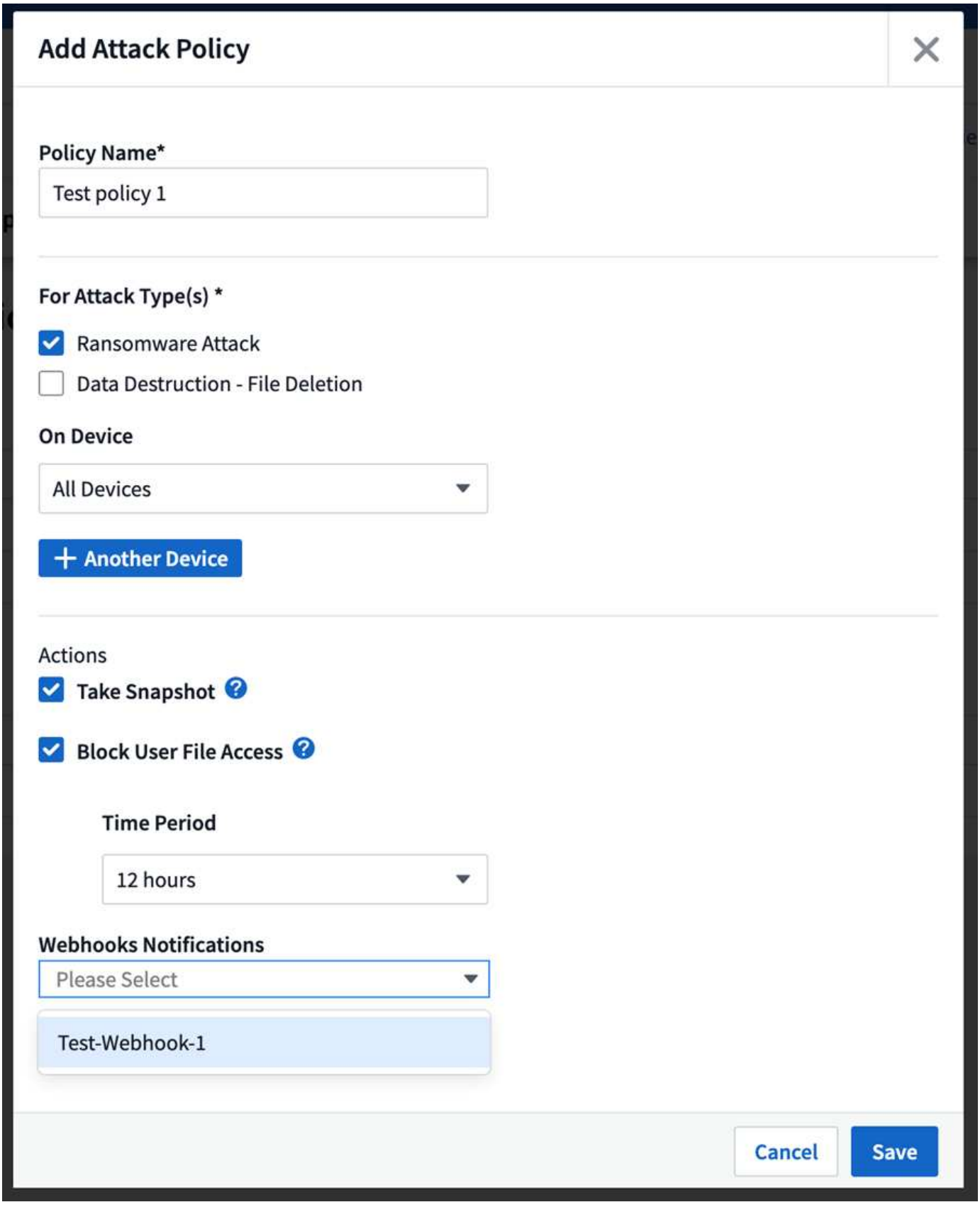


Notifications via webhook

- Pour notifier les événements via le webhook, accédez à *Sécurité de la charge de travail > Politiques*. Cliquez sur *+Politique d'attaque* ou *+Politique d'avertissement*.
- Saisissez un nom de politique significatif.
- Sélectionnez les types d'attaque requis, les appareils auxquels la politique doit être attachée et les actions requises.

- Sous la liste déroulante *Notifications Webhooks*, sélectionnez les webhooks requis. Sauvegarder la politique.

Remarque : les webhooks peuvent également être attachés à des politiques existantes en les modifiant.



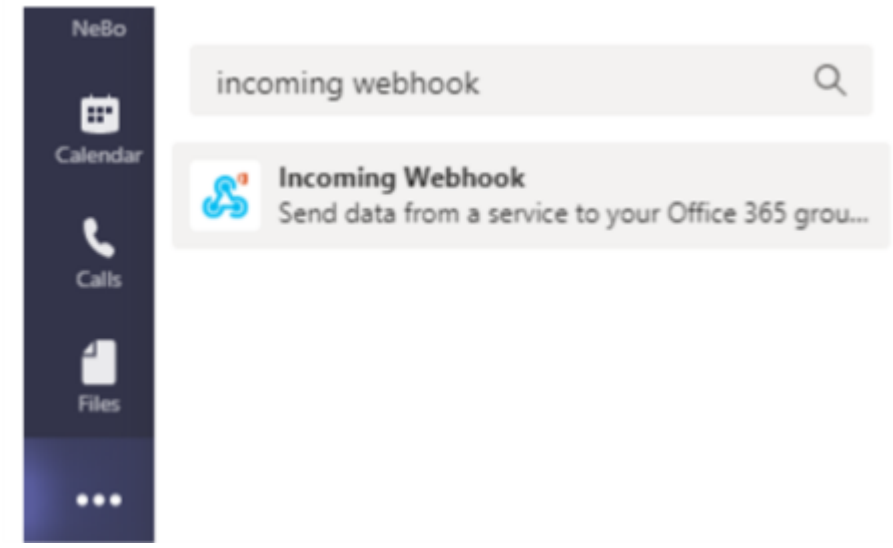
Exemple de webhook de sécurité de charge de travail pour Microsoft Teams

Les webhooks permettent aux utilisateurs d'envoyer des notifications d'alerte à diverses applications à l'aide d'un canal webhook personnalisé. Cette page fournit un exemple de configuration de webhooks pour Teams.

Cette page fait référence à des instructions de tiers, qui sont susceptibles d'être modifiées. Reportez-vous à la"Documentation des équipes" pour les informations les plus récentes.

Configuration des équipes :

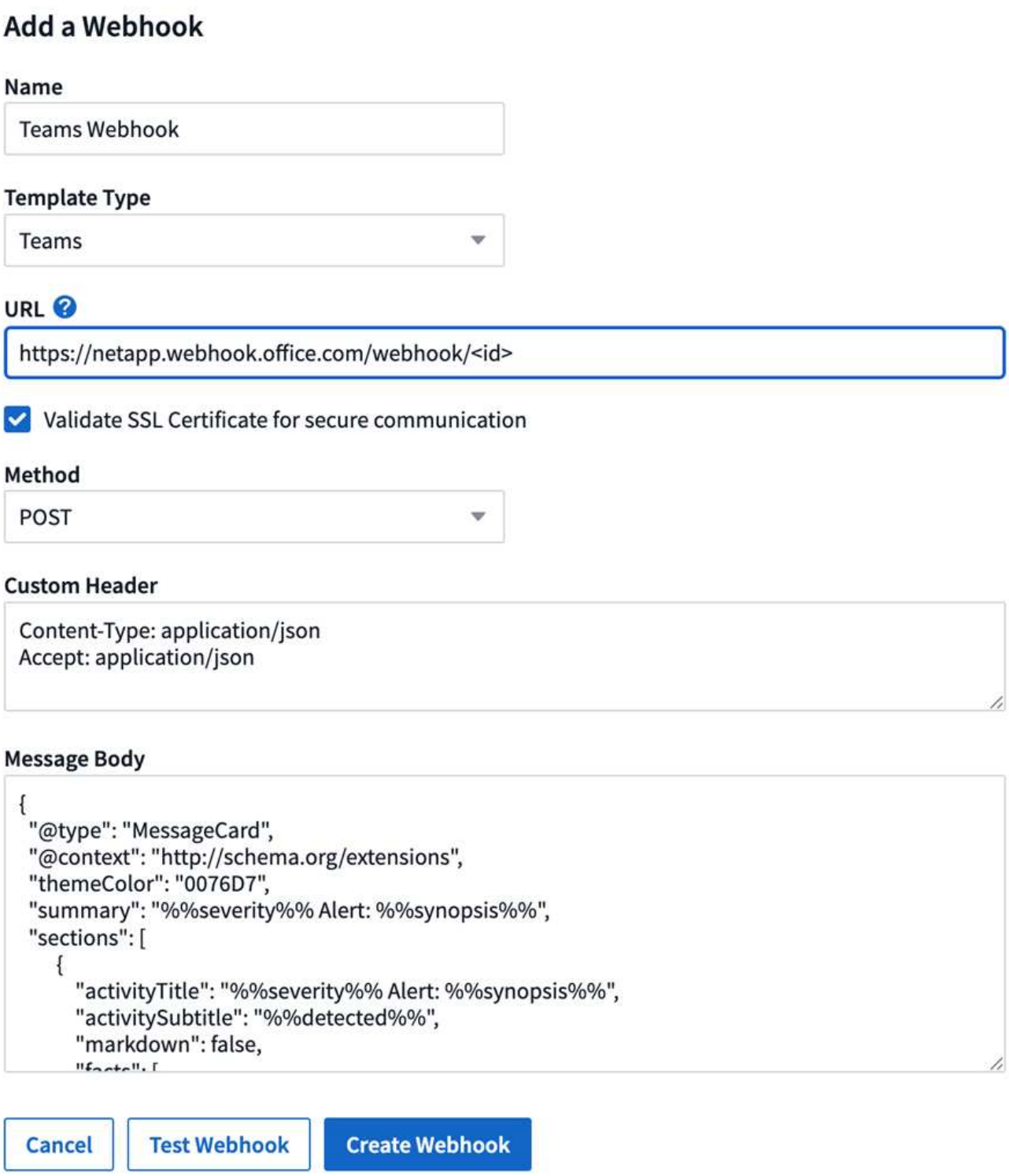
1. Dans Teams, sélectionnez le kebab et recherchez Webhook entrant.



2. Sélectionnez **Ajouter à une équipe > Sélectionner une équipe > Configurer un connecteur**.
3. Copiez l'URL du Webhook. Vous devrez coller ceci dans la configuration du webhook Workload Security.

Créer un webhook pour les équipes de sécurité de la charge de travail :

1. Accédez à Admin > Notifications et sélectionnez l'onglet *« Webhooks de sécurité de la charge de travail »*. Sélectionnez _+ *Webhook* pour créer un nouveau webhook.
2. Donnez au webhook un nom significatif.
3. Dans la liste déroulante *Type de modèle*, sélectionnez **Équipes**.



4. Collez l'URL ci-dessus dans le champ *URL*.

Étapes pour créer une notification Teams avec un modèle Adaptive Card

1. Remplacez le corps du message par le modèle suivant :

```
{
"type": "message",
"attachments": [
```

```
{
  "contentType": "application/vnd.microsoft.card.adaptive",
  "content": {
    "$schema": "http://adaptivecards.io/schemas/adaptive-card.json",
    "type": "AdaptiveCard",
    "version": "1.2",
    "body": [
      {
        "type": "TextBlock",
        "text": "%%severity%% Alert: %%synopsis%%",
        "wrap": true,
        "weight": "Bolder",
        "size": "Large"
      },
      {
        "type": "TextBlock",
        "text": "%%detected%%",
        "wrap": true,
        "isSubtle": true,
        "spacing": "Small"
      },
      {
        "type": "FactSet",
        "facts": [
          {
            "title": "User",
            "value": "%%userName%%"
          },
          {
            "title": "Attack/Abnormal Behavior",
            "value": "%%type%%"
          },
          {
            "title": "Action taken",
            "value": "%%actionTaken%%"
          },
          {
            "title": "Files encrypted",
            "value": "%%filesEncrypted%%"
          },
          {
            "title": "Encrypted files suffix",
            "value": "%%encryptedFilesSuffix%%"
          },
          {
            "title": "Files deleted",
```

```
                "value": "%%filesDeleted%%"
              },
              {
                "title": "Activity Change Rate",
                "value": "%%changePercentage%%"
              },
              {
                "title": "Severity",
                "value": "%%severity%%"
              },
              {
                "title": "Status",
                "value": "%%status%%"
              },
              {
                "title": "Notes",
                "value": "%%note%%"
              }
            ]
          }
        ],
        "actions": [
          {
            "type": "Action.OpenUrl",
            "title": "View Details",
            "url":
"https://%%cloudInsightsHostname%%/%%alertDetailsPageUrl%%"
          }
        ]
      }
    }
  ]
}
```

2. Si vous utilisez Power Automate Flows, les paramètres de requête dans l'URL sont au format encodé. Vous devez décoder l'URL avant de la saisir.
3. Cliquez sur « Test Webhook » pour vous assurer qu'il n'y a pas d'erreurs.
4. Enregistrez le webhook.

Notifications via Webhook

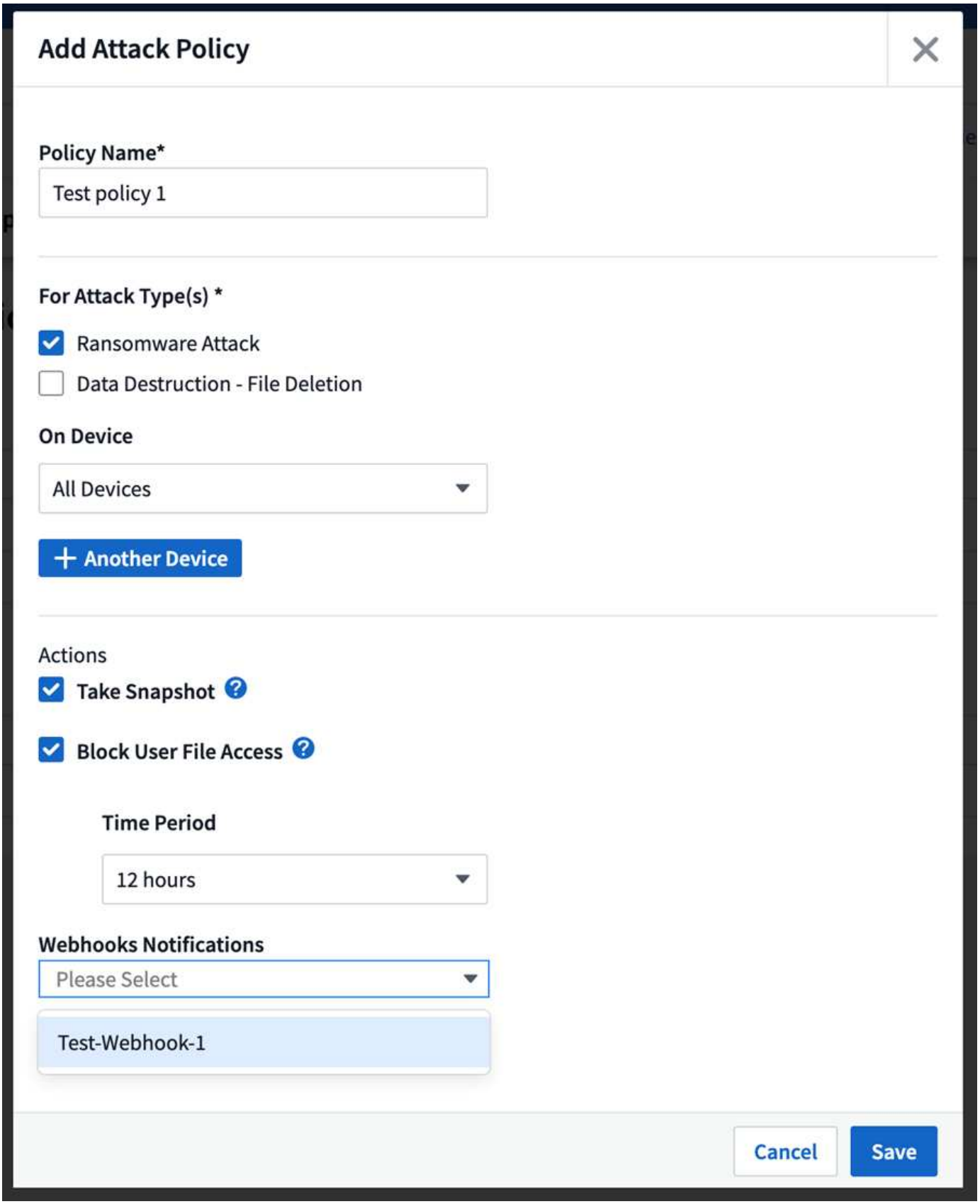
Pour notifier les événements via le webhook, accédez à *Sécurité de la charge de travail > Politiques*. Sélectionnez *+Politique d'attaque* ou *+Politique d'avertissement*.

- Saisissez un nom de politique significatif.
- Sélectionnez les types d'attaque requis, les périphériques auxquels la stratégie doit être associée et les

actions requises.

- Sous la liste déroulante *Notifications Webhooks*, sélectionnez les webhooks Teams requis. Sauvegarder la politique.

Remarque : les webhooks peuvent également être attachés à des politiques existantes en les modifiant.



API de sécurité de la charge de travail

Intégrez Workload Security à votre écosystème d'entreprise à l'aide d'une API REST

protégée par une authentification sécurisée basée sur des jetons. Récupérez les données d'activité forensique, gérez les jetons d'accès API et développez des intégrations personnalisées avec les CMDB, les systèmes de gestion des tickets et d'autres applications. La documentation Swagger interactive fournit des spécifications complètes de l'API et vous permet de tester les points de terminaison directement.

Conditions requises pour l'accès à l'API :

- Un modèle de jeton d'accès API est utilisé pour accorder l'accès.
- La gestion des jetons API est effectuée par les utilisateurs de Workload Security avec le rôle d'administrateur.

Documentation de l'API (Swagger)

Les dernières informations sur l'API sont disponibles en vous connectant à Workload Security et en accédant à **Admin > Accès API**. Cliquez sur le lien **Documentation API**. La documentation de l'API est basée sur Swagger, qui fournit une brève description et des informations d'utilisation de l'API et vous permet de l'essayer sur votre locataire.

Si vous appelez l'API Forensics Activity, utilisez l'API cloudsecure_forensics.activities.**v2**. Si vous effectuez plusieurs appels à cette API, assurez-vous que les appels se produisent de manière séquentielle et non en parallèle. Plusieurs appels parallèles peuvent entraîner l'expiration du délai d'attente de l'API.

Jetons d'accès API

Avant d'utiliser l'API Workload Security, vous devez créer un ou plusieurs **jetons d'accès API**. Les jetons d'accès accordent des autorisations de lecture. Vous pouvez également définir l'expiration de chaque jeton d'accès.

Pour créer un jeton d'accès :

- Cliquez sur **Admin > Accès API**
- Cliquez sur **+Jeton d'accès API**
- Entrez **Nom du jeton**
- Spécifiez **Expiration du jeton**

Votre jeton ne sera disponible que pour la copie dans le presse-papiers et l'enregistrement pendant le processus de création. Les jetons ne peuvent pas être récupérés après leur création, il est donc fortement recommandé de copier le jeton et de l'enregistrer dans un endroit sûr. Vous serez invité à cliquer sur le bouton Copier le jeton d'accès API avant de pouvoir fermer l'écran de création de jeton.

Vous pouvez désactiver, activer et révoquer les jetons. Les jetons désactivés peuvent être activés.

Les jetons accordent un accès général aux API du point de vue du client, en gérant l'accès aux API dans le cadre de leur propre locataire.

L'application reçoit un jeton d'accès après qu'un utilisateur s'est authentifié et a autorisé l'accès avec succès, puis transmet le jeton d'accès comme identifiant lorsqu'il appelle l'API cible. Le jeton transmis informe l'API

que le porteur du jeton a été autorisé à accéder à l'API et à effectuer des actions spécifiques en fonction de la portée qui a été accordée lors de l'autorisation.

L'en-tête HTTP où le jeton d'accès est transmis est **X-CloudInsights-ApiKey:**

Par exemple, utilisez ce qui suit pour récupérer les ressources de stockage :

```
 curl https://<Workload Security tenant>/rest/v1/cloudsecure/activities -H
'X-CloudInsights-ApiKey: <API_Access_Token>'
Où _<API_Access_Token>_ est le jeton que vous avez enregistré lors de la
création de la clé d'accès API et _<Workload Security Tenant>_ est l'URL
du locataire de votre environnement Workload Security.
```

Des informations détaillées peuvent être trouvées dans le lien *Documentation API* sous **Admin > Accès API**.

Script pour extraire des données via l'API

Les agents Workload Security incluent un script d'exportation pour faciliter les appels parallèles à l'API v2 en divisant la plage horaire demandée en lots plus petits.

Le script se trouve dans */opt/netapp/cloudsecure/agent/export-script*. Un fichier README dans le même répertoire fournit des instructions d'utilisation.

Voici un exemple de commande pour appeler le script :

```
python3 data-export.py --tenant_url <Workload Security tenant>
--access_key %ACCESS_KEY% --path_filter "<dir path>" --user_name "<user>"
--from_time "01-08-2024 00:00:00" --to_time "31-08-2024 23:59:59"
--iteration_interval 12 --num_workers 3
```

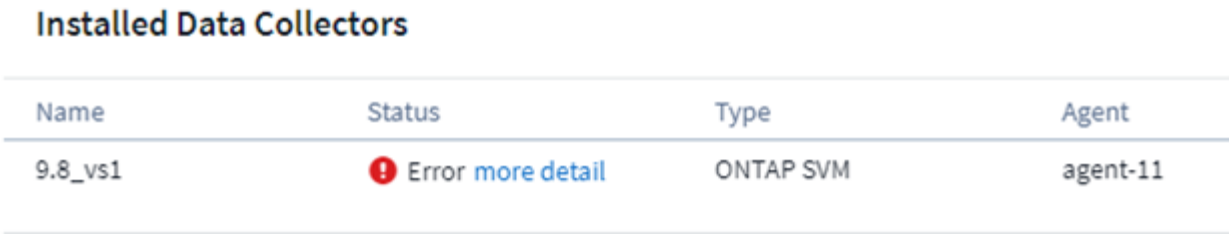
Paramètres clés : - `--iteration_interval 12` : Divise la plage horaire demandée en intervalles de 12 heures. - `--num_workers 3` : Récupère ces intervalles en parallèle à l'aide de 3 threads.

Dépannage du collecteur de données ONTAP SVM

Workload Security utilise des collecteurs de données pour collecter les données d'accès aux fichiers et aux utilisateurs à partir des appareils. Vous trouverez ici des conseils pour résoudre les problèmes liés à ce collecteur.

Voir le"Configuration du collecteur SVM" page pour obtenir des instructions sur la configuration de ce collecteur.

En cas d'erreur, vous pouvez cliquer sur *plus de détails* dans la colonne *Statut* de la page Collecteurs de données installés pour obtenir des détails sur l'erreur.



Les problèmes connus et leurs résolutions sont décrits ci-dessous.

Problème : le collecteur de données s'exécute pendant un certain temps et s'arrête après un temps aléatoire, échouant avec : « Message d'erreur : le connecteur est en état d'erreur. Nom du service : audit. Motif de l'échec : serveur fpolicy externe surchargé. **Essayez ceci :** le taux d'événements d' ONTAP était bien supérieur à ce que la boîte d'agent peut gérer. La connexion a donc été interrompue.

Vérifiez le trafic de pointe dans CloudSecure lorsque la déconnexion s'est produite. Vous pouvez le vérifier à partir de la page **CloudSecure > Analyse forensique des activités > Toutes les activités**.

Si le trafic agrégé de pointe est supérieur à ce que l'Agent Box peut gérer, reportez-vous à la page du vérificateur de taux d'événements pour savoir comment dimensionner le déploiement du collecteur dans une Agent Box.

Si l'agent a été installé dans la boîte Agent avant le 4 mars 2021, exécutez les commandes suivantes dans la boîte Agent :

```
echo 'net.core.rmem_max=8388608' >> /etc/sysctl.conf
echo 'net.ipv4.tcp_rmem = 4096 2097152 8388608' >> /etc/sysctl.conf
sysctl -p
```

Redémarrez le collecteur à partir de l'interface utilisateur après le redimensionnement.

{vider}

Problème : le collecteur signale le message d'erreur : « Aucune adresse IP locale trouvée sur le connecteur pouvant atteindre les interfaces de données du SVM ». **Essayez ceci :** cela est probablement dû à un problème de réseau côté ONTAP . Veuillez suivre ces étapes :

1. Assurez-vous qu'il n'y a pas de pare-feu sur le LIF de données SVM ou sur le LIF de gestion qui bloque la connexion depuis le SVM.
2. Lors de l'ajout d'un SVM via une adresse IP de gestion de cluster, assurez-vous que la durée de vie des données et la durée de vie de gestion du SVM sont pingables à partir de la machine virtuelle de l'agent. En cas de problème, vérifiez la passerelle, le masque de réseau et les routes du lif.

   Vous pouvez également essayer de vous connecter au cluster via ssh à l'aide de l'adresse IP de gestion du cluster et d'envoyer une requête ping à l'adresse IP de l'agent. Assurez-vous que l'adresse IP de l'agent est pingable :

```
network ping -vserver <vserver name> -destination <Agent IP> -lif <Lif
Name> -show-detail
```

Si le ping n'est pas possible, assurez-vous que les paramètres réseau dans ONTAP sont corrects, afin que la machine de l'agent soit pingable.

3. Si vous avez essayé de vous connecter via l'IP du cluster et que cela ne fonctionne pas, essayez de vous connecter directement via l'IP SVM. Veuillez consulter ci-dessus les étapes de connexion via l'IP SVM.
4. Lors de l'ajout du collecteur via l'adresse IP SVM et les informations d'identification vsadmin, vérifiez si le rôle Données plus Gestion du SVM est activé. Dans ce cas, le ping vers le SVM Lif fonctionnera, mais le SSH vers le SVM Lif ne fonctionnera pas. Si oui, créez un Lif de gestion SVM uniquement et essayez de vous connecter via ce Lif de gestion SVM uniquement.
5. Si cela ne fonctionne toujours pas, créez un nouveau Lif SVM et essayez de vous connecter via ce Lif. Assurez-vous que le masque de sous-réseau est correctement défini.
6. Débogage avancé :
   a. Démarrer une trace de paquets dans ONTAP.
   b. Essayez de connecter un collecteur de données au SVM à partir de l'interface utilisateur CloudSecure.
   c. Attendez que l'erreur apparaisse. Arrêtez le suivi des paquets dans ONTAP.
   d. Ouvrez la trace des paquets depuis ONTAP. Il est disponible à cet endroit

```
 https://<cluster_mgmt_ip>/spi/<clustername>/etc/log/packet_traces/
.. Assurez-vous qu'il existe un SYN d' ONTAP vers la boîte Agent.
.. S'il n'y a pas de SYN d' ONTAP , il s'agit d'un problème de pare-
feu dans ONTAP.
.. Ouvrez le pare-feu dans ONTAP, afin ONTAP puisse connecter la
boîte d'agent.
```

7. Si cela ne fonctionne toujours pas, veuillez consulter l'équipe réseau pour vous assurer qu'aucun pare-feu externe ne bloque la connexion d' ONTAP au boîtier Agent.
8. Si aucune des solutions ci-dessus ne résout le problème, ouvrez un dossier avec"Assistance Netapp" pour obtenir de l'aide.

{vider}

Problème : Message : « Échec de la détermination du type ONTAP pour [nom d'hôte : <adresse IP>. Raison : Erreur de connexion au système de stockage <Adresse IP> : L'hôte est inaccessible (Hôte inaccessible)"
Essayez ceci :

1. Vérifiez que l'adresse IP de gestion SVM ou l'adresse IP de gestion de cluster correcte a été fournie.
2. Connectez-vous en SSH au SVM ou au cluster auquel vous souhaitez vous connecter. Une fois connecté, assurez-vous que le nom du SVM ou du cluster est correct.

{vider}

Problème : Message d'erreur : « Le connecteur est dans un état d'erreur. Service.nom : audit. Motif de l'échec : serveur fpolicy externe arrêté. **Essayez ceci :**

1. Il est très probable qu'un pare-feu bloque les ports nécessaires sur la machine agent. Vérifiez que la plage de ports 35000-55000/tcp est ouverte pour que la machine agent se connecte à partir du SVM. Assurez-vous également qu'aucun pare-feu n'est activé côté ONTAP bloquant la communication avec la machine agent.
2. Tapez la commande suivante dans la zone Agent et assurez-vous que la plage de ports est ouverte.

   ```
   sudo iptables-save | grep 3500*
   ```

   Un exemple de sortie devrait ressembler à :

   ```
    -A IN_public_allow -p tcp -m tcp --dport 35000 -m conntrack -ctstate
   NEW -j ACCEPT
   . Connectez-vous à SVM, entrez les commandes suivantes et vérifiez
   qu'aucun pare-feu n'est configuré pour bloquer la communication avec
   ONTAP.
   ```

   ```
   system services firewall show
   system services firewall policy show
   ```

   "Vérifier les commandes du pare-feu"du côté ONTAP .

3. Connectez-vous en SSH au SVM/cluster que vous souhaitez surveiller. Envoyez une requête ping à la boîte Agent à partir de la bibliothèque de données SVM (avec prise en charge des protocoles CIFS et NFS) et assurez-vous que la requête ping fonctionne :

   ```
   network ping -vserver <vserver name> -destination <Agent IP> -lif <Lif
   Name> -show-detail
   ```

   Si le ping n'est pas possible, assurez-vous que les paramètres réseau dans ONTAP sont corrects, afin que la machine de l'agent soit pingable.

4. Si un seul SVM est ajouté deux fois à un locataire via 2 collecteurs de données, cette erreur s'affichera. Supprimez l'un des collecteurs de données via l'interface utilisateur. Redémarrez ensuite l'autre collecteur de données via l'interface utilisateur. Ensuite, le collecteur de données affichera le statut « EN COURS D'EXÉCUTION » et commencera à recevoir des événements de SVM.

   Fondamentalement, dans un locataire, 1 SVM ne doit être ajouté qu'une seule fois, via 1 collecteur de données. 1 SVM ne doit pas être ajouté deux fois via 2 collecteurs de données.

5. Dans les cas où le même SVM a été ajouté dans deux environnements de sécurité de charge de travail différents (locataires), le dernier réussira toujours. Le deuxième collecteur configurera fpolicy avec sa propre adresse IP et expulsera le premier. Ainsi, le collecteur du premier cessera de recevoir des événements et son service « audit » entrera en état d'erreur. Pour éviter cela, configurez chaque SVM sur

un seul environnement.

6. Cette erreur peut également se produire si les stratégies de service ne sont pas configurées correctement. Avec ONTAP 9.8 ou version ultérieure, pour se connecter au collecteur de sources de données, le service data-fpolicy-client est requis avec le service de données data-nfs et/ou data-cifs. De plus, le service data-fpolicy-client doit être associé aux données lif pour le SVM surveillé.

{vider}

Problème : Aucun événement n'est visible sur la page d'activité. **Essayez ceci :**

1. Vérifiez si le collecteur ONTAP est à l'état « RUNNING ». Si oui, assurez-vous que certains événements cifs sont générés sur les machines virtuelles clientes cifs en ouvrant certains fichiers.
2. Si aucune activité n'est observée, connectez-vous au SVM et entrez la commande suivante.

   ```
   <SVM>event log show -source fpolicy
   ```

   Veuillez vous assurer qu'il n'y a pas d'erreurs liées à fpolicy.

3. Si aucune activité n'est visible, veuillez vous connecter au SVM. Entrez la commande suivante :

   ```
   <SVM>fpolicy show
   ```

   Vérifiez si la politique fpolicy nommée avec le préfixe « cloudsecure_ » a été définie et si le statut est « on ». Si cette option n'est pas définie, il est fort probable que l'agent ne puisse pas exécuter les commandes dans la SVM. Veuillez vous assurer que toutes les conditions préalables décrites au début de la page ont été respectées.

{vider}

Problème : Le collecteur de données SVM est en état d'erreur et le message d'erreur est « L'agent n'a pas réussi à se connecter au collecteur » **Essayez ceci :**

1. Il est fort probable que l'agent soit surchargé et ne parvienne pas à se connecter aux collecteurs de sources de données.
2. Vérifiez combien de collecteurs de sources de données sont connectés à l'agent.
3. Vérifiez également le débit de données dans la page « Toutes les activités » de l'interface utilisateur.
4. Si le nombre d'activités par seconde est considérablement élevé, installez un autre agent et déplacez certains des collecteurs de sources de données vers le nouvel agent.

{vider}

Problème : le collecteur de données SVM affiche le message d'erreur suivant : « fpolicy.server.connectError : le nœud n'a pas pu établir de connexion avec le serveur FPolicy « 12.195.15.146 » (raison : « Sélection

expirée ») » **Essayez ceci :** le pare-feu est activé dans SVM/Cluster. Le moteur fpolicy ne peut donc pas se connecter au serveur fpolicy. Les CLI dans ONTAP qui peuvent être utilisées pour obtenir plus d'informations sont :

```
event log show -source fpolicy which shows the error
event log show -source fpolicy -fields event,action,description which
shows more details.
```

"Vérifier les commandes du pare-feu"du côté ONTAP .

{vider}

Problème : Message d'erreur : « Le connecteur est dans un état d'erreur. Nom du service : audit. Motif de l'échec : Aucune interface de données valide (rôle : données, protocoles de données : NFS ou CIFS ou les deux, état : actif) trouvée sur la SVM. **Essayez ceci :** Assurez-vous qu'il existe une interface opérationnelle (ayant un rôle de données et un protocole de données comme CIFS/NFS).

{vider}

Problème : le collecteur de données passe à l'état d'erreur, puis passe à l'état d'exécution après un certain temps, puis revient à l'état d'erreur. Ce cycle se répète. **Essayez ceci :** Cela se produit généralement dans le scénario suivant :

1. Plusieurs collecteurs de données ont été ajoutés.
2. Les collecteurs de données qui présentent ce type de comportement auront 1 SVM ajouté à ces collecteurs de données. Cela signifie que 2 ou plusieurs collecteurs de données sont connectés à 1 SVM.
3. Assurez-vous qu'un seul collecteur de données se connecte à un seul SVM.
4. Supprimez les autres collecteurs de données connectés au même SVM.

{vider}

Problème : le connecteur est dans un état d'erreur. Nom du service : audit. Motif de l'échec : échec de la configuration (politique sur SVM svmname. Motif : Valeur non valide spécifiée pour l'élément « shares-to-include » dans « fpolicy.policy.scope-modify : « Federal » **Essayez ceci :** *Les noms de partage doivent être indiqués sans guillemets. Modifiez la configuration DSC ONTAP SVM pour corriger les noms de partage.

Inclure et exclure des partages n'est pas destiné à une longue liste de noms de partages. Utilisez plutôt le filtrage par volume si vous avez un grand nombre d'actions à inclure ou à exclure.

{vider}

Problème : il existe des fpolicies existantes dans le cluster qui ne sont pas utilisées. Que faut-il faire avec ceux-ci avant l'installation de Workload Security ? **Essayez ceci :** Il est recommandé de supprimer tous les paramètres fpolicy inutilisés existants, même s'ils sont dans un état déconnecté. Workload Security créera

fpolicy avec le préfixe « cloudsecure_ ». Toutes les autres configurations fpolicy inutilisées peuvent être supprimées.

Commande CLI pour afficher la liste fpolicy :

```
 fpolicy show
Étapes pour supprimer les configurations fpolicy :
```

```
fpolicy disable -vserver <svmname> -policy-name <policy_name>
fpolicy policy scope delete -vserver <svmname> -policy-name <policy_name>
fpolicy policy delete -vserver <svmname> -policy-name <policy_name>
fpolicy policy event delete -vserver <svmname> -event-name <event_list>
fpolicy policy external-engine delete -vserver <svmname> -engine-name
<engine_name>
```

{vider}

Problème : Après l'activation de la sécurité des charges de travail, les performances ONTAP sont affectées : la latence devient sporadiquement élevée et les IOPS deviennent sporadiquement faibles. **Essayez ceci :** Lors de l'utilisation ONTAP avec Workload Security, des problèmes de latence peuvent parfois être observés dans ONTAP. Plusieurs raisons peuvent expliquer cela, comme indiqué ci-dessous :"1372994" , "1415152" , "1438207" , "1479704" , "1354659" . Tous ces problèmes sont résolus dans ONTAP 9.13.1 et versions ultérieures ; il est fortement recommandé d'utiliser l'une de ces versions ultérieures.

{vider}

Problème : le collecteur de données affiche le message d'erreur : « Erreur : échec de la détermination de l'état du collecteur en 2 tentatives, essayez de redémarrer le collecteur (code d'erreur : AGENT008) ». **Essayez ceci :**

1. Sur la page Collecteurs de données, faites défiler vers la droite du collecteur de données générant l'erreur et cliquez sur le menu à 3 points. Sélectionnez *Modifier*. Saisissez à nouveau le mot de passe du collecteur de données. Enregistrez le collecteur de données en appuyant sur le bouton *Enregistrer*. Le collecteur de données redémarrera et l'erreur devrait être résolue.
2. Il se peut que la machine Agent ne dispose pas de suffisamment de CPU ou de RAM, c'est pourquoi les DSC échouent. Veuillez vérifier le nombre de collecteurs de données ajoutés à l'agent dans la machine. Si le nombre est supérieur à 20, veuillez augmenter la capacité du processeur et de la RAM de la machine Agent. Une fois le CPU et la RAM augmentés, les DSC passeront automatiquement en état d'initialisation puis en état d'exécution. Consultez le guide des tailles sur"cette page" .

{vider}

Problème : le collecteur de données génère une erreur lorsque le mode SVM est sélectionné. **Essayez ceci :** lors de la connexion en mode SVM, si l'IP de gestion du cluster est utilisée pour se connecter au lieu de l'IP de

gestion SVM, la connexion échouera. Assurez-vous que l'adresse IP SVM correcte est utilisée.

{vider}

Problème : le collecteur de données affiche un message d'erreur lorsque la fonction Accès refusé est activée : « Le connecteur est en état d'erreur. Nom du service : audit. Motif de l'échec : échec de la configuration de fpolicy sur SVM test_svm. Motif : l'utilisateur n'est pas autorisé. **Essayez ceci :** l'utilisateur ne dispose peut-être pas des autorisations REST nécessaires à la fonctionnalité Accès refusé. Veuillez suivre les instructions sur"cette page" pour définir les autorisations.

Redémarrez le collecteur une fois les autorisations définies.

{vider}

Problème : Le collecteur est en état d'erreur avec le message : Le connecteur est en état d'erreur. Raison de l'échec : Échec de la configuration du stockage persistant sur la SVM <Nom de la SVM>. Raison : Impossible de trouver un agrégat approprié pour le volume « <volumeName> » dans le SVM « <SVM Name> ». Motif : Les informations de performance pour l'agrégat « <aggregateName> » ne sont actuellement pas disponibles. Patientez quelques minutes et réessayez la commande. Nom du service : audit. Raison de l'échec : impossible de configurer le magasin persistant sur la SVM <SVM name="">.</SVM> Reason: Unable to find a suitable aggregate for volume "<volumeName>" in SVM "<SVM Name>". Motif : Les informations sur les performances pour <aggregateName>l'agrégat « » ne sont actuellement pas disponibles.</aggregateName> Attendez quelques minutes et réessayez la commande.

Essayez ceci : Attendez quelques minutes, puis redémarrez le Collecteur.

{vider}

Si vous rencontrez toujours des problèmes, contactez les liens d'assistance mentionnés dans la page **Aide > Assistance**.

Informations sur le copyright

Informations sur les marques commerciales