



Sécurité des workloads

Cloud Insights

NetApp
April 16, 2024

Sommaire

- Sécurité des workloads 1
 - À propos de la sécurité des charges de travail du stockage 1
 - Mise en route 1
 - Alertes 44
 - Médecine légale 50
 - Stratégies de réponse automatisées 59
 - Stratégies de types de fichiers autorisées 61
 - Intégration avec la protection ONTAP autonome contre les ransomwares 62
 - Intégration avec l'accès ONTAP refusée 65
 - Blocage de l'accès utilisateur 67
 - Sécurité des charges de travail : simulation d'une attaque 73
 - Configuration des notifications par e-mail pour les alertes, les avertissements et l'état de santé du collecteur d'agents/de sources de données 76
 - API de sécurité du workload 77

Sécurité des workloads

À propos de la sécurité des charges de travail du stockage

La sécurité des charges de travail du stockage Cloud Insights (anciennement Cloud Secure) vous aide à protéger vos données avec des informations exploitables sur les menaces internes. Elle assure la visibilité et le contrôle centralisés sur tous les accès aux données de l'entreprise à l'échelle des environnements de cloud hybride, afin de garantir l'atteinte des objectifs de sécurité et de conformité.



La sécurité des charges de travail n'est pas disponible dans l'édition fédérale de Cloud Insights.

Visibilité

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

Remplacez les outils et les processus manuels qui n'offrent pas de visibilité opportune et exacte sur l'accès aux données et leur contrôle. La sécurité des charges de travail fonctionne de façon unique sur les systèmes de stockage cloud et sur site pour vous avertir en temps réel des comportements malveillants des utilisateurs.

La protection

Protégez les données de l'entreprise contre les activités abusives ou les usurpations d'identité à l'aide de fonctionnalités avancées de machine learning et de détection des anomalies.

Vous alerte en cas d'accès anormal aux données au moyen du machine learning avancé et de la détection des anomalies du comportement des utilisateurs.

La conformité

Assurez la conformité aux règles de l'entreprise en vérifiant l'accès des utilisateurs aux données critiques stockées dans des infrastructures sur site ou dans le cloud.

Mise en route

Mise en route de la sécurité des charges de travail

Certaines tâches de configuration doivent être effectuées avant de pouvoir utiliser la sécurité de la charge de travail pour surveiller l'activité des utilisateurs.



La sécurité des charges de travail n'est pas disponible dans l'édition fédérale de Cloud Insights.

Le système Workload Security utilise un agent pour collecter les données d'accès des systèmes de stockage et des informations utilisateur à partir des serveurs Directory Services.

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

Tâche	Informations associées
Configurer un agent	"Exigences de l'agent" "Ajouter un agent" "Vidéo : déploiement de l'agent"
Configurer un connecteur de répertoire utilisateur	"Ajouter un connecteur de répertoire utilisateur" "Vidéo : connexion Active Directory"
Configurer des collecteurs de données	Cliquez sur Workload Security > Collectors Cliquez sur le collecteur de données à configurer. Voir la section référence du fournisseur du Data Collector de la documentation. "Vidéo : connexion SVM ONTAP"
Créer des comptes d'utilisateurs	"Gérer les comptes d'utilisateurs"
Dépannage	"Vidéo : dépannage"

La sécurité des charges de travail peut également s'intégrer à d'autres outils. Par exemple : ["voir ce guide"](#) De l'intégration avec Splunk.

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

Vous devez ["Installez un agent"](#) afin d'obtenir des informations à partir de vos collecteurs de données. Avant d'installer l'agent, vous devez vous assurer que votre environnement répond aux exigences relatives au système d'exploitation, au processeur, à la mémoire et à l'espace disque.



La sécurité des workloads de stockage n'est pas disponible dans l'édition fédérale de Cloud Insights.

Composant	Configuration Linux requise
Système d'exploitation	<p>Un ordinateur exécutant une version sous licence de l'une des versions suivantes :</p> <p>Red Hat Enterprise Linux 7.x, 8.x 64 bits, SELinux CentOS 7.x 64 bits, SELinux CentOS 8 Stream, SELinux Ubuntu 20 à 22 64 bits Rocky 8.x 64 bits, Rocky 9.x 64 bits, SELinux SUSE Linux Enterprise Server 15 SP3, SUSE Linux Enterprise Server 15 SP4, SELinux sur SUSE 15 SP3</p> <p>Cet ordinateur ne doit pas exécuter d'autres logiciels au niveau de l'application. Un serveur dédié est recommandé.</p>

Composant	Configuration Linux requise
Commandes	le dézipper est requis pour l'installation. En outre, la commande « <code>udo su -</code> » est requise pour l'installation, l'exécution de scripts et la désinstallation.
CPU	4 cœurs de processeurs
Mémoire	16 GO DE RAM
Espace disque disponible	<p>L'espace disque doit être alloué de la manière suivante : /Opt/netapp 35 Go (minimum)</p> <p>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.</p> <p>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 Data Collector peut échouer si les utilisateurs locaux n'ont pas l'autorisation de ce dossier. voir la "dépannage" pour plus de détails.</p>
Le réseau	Connexion Ethernet de 100 Mbit/s à 1 Gbit/s, adresse IP statique, connectivité IP à tous les périphériques et port requis à l'instance de sécurité de la charge de travail (80 ou 443).

Remarque : l'agent de sécurité de charge de travail peut être installé sur la même machine qu'une unité d'acquisition Cloud Insights et/ou un agent. Toutefois, il est recommandé de les installer sur des machines distinctes. Si ces derniers 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 à la fois sur le système ONTAP et sur l'ordinateur Agent à l'aide de **NTP (Network Time Protocol)** ou **SNTP (simple Network Time Protocol)**.

Règles d'accès au réseau cloud

Pour les environnements de sécurité de la charge de travail **basés aux États-Unis** :

Protocole	Port	Source	Destination	Description
TCP	443	Agent de sécurité des charges de travail	<site_name>.cs01.cloudinsights.netapp.com <site_name>.c01.cloudinsights.netapp.com <site_name>.c02.cloudinsights.netapp.com	Accès à Cloud Insights
TCP	443	Agent de sécurité des charges de travail	gateway.c01.cloudinsights.netapp.com 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 des charges de travail	<site_name>.cs01-eu-1.cloudinsights.netapp.com <site_name>.c01-eu-1.cloudinsights.netapp.com <site_name>.c02-eu-1.cloudinsights.netapp.com	Accès à Cloud Insights
TCP	443	Agent de sécurité des charges de travail	gateway.c01.cloudinsights.netapp.com agentlogin.cs01-eu-1.cloudinsights.netapp.com	Accès aux services d'authentification

Pour les environnements de sécurité de la charge de travail **APAC** :

Protocole	Port	Source	Destination	Description
TCP	443	Agent de sécurité des charges de travail	<site_name>.cs01-ap-1.cloudinsights.netapp.com <site_name>.c01-ap-1.cloudinsights.netapp.com <site_name>.c02-ap-1.cloudinsights.netapp.com	Accès à Cloud Insights

Protocole	Port	Source	Destination	Description
TCP	443	Agent de sécurité des charges de travail	gateway.c01.cloudinsights.netapp.com agentlogin.cs01-app-1.cloudinsights.netapp.com	Accès aux services d'authentification

Règles dans le réseau

Protocole	Port	Source	Destination	Description
TCP	389 (LDAP) 636 (LDAPS/Start-tls)	Agent de sécurité des charges de travail	URL du serveur LDAP	Connectez-vous à LDAP
TCP	443	Agent de sécurité des charges de travail	Adresse IP de gestion du cluster ou du SVM (selon la configuration du collecteur SVM)	Communication de l'API avec ONTAP
TCP	35000 - 55000	Adresses IP des LIF de données des SVM	Agent de sécurité des charges de travail	Communication de 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 que ONTAP lui envoie des événements, y compris tout pare-feu sur l'agent de sécurité de la charge de travail lui-même (le cas échéant).
TCP	7	Agent de sécurité des charges de travail	Adresses IP des LIF de données des SVM	Echo from Agent to SVM Data LIFs
SSH	22	Agent de sécurité des charges de travail	Gestion du cluster	Nécessaire pour le blocage des utilisateurs CIFS/SMB.

Dimensionnement du système

Voir la "[Vérificateur de taux d'événement](#)" pour plus d'informations sur le dimensionnement.

Installation de l'agent de sécurité de charge de travail

La sécurité des charges de travail (anciennement Cloud Secure) collecte des données d'activité utilisateur en utilisant un ou plusieurs agents. Les agents se connectent aux terminaux de votre environnement et collectent les données envoyées à la couche SaaS de sécurité de la charge de travail pour analyse. Voir ["Exigences de l'agent"](#) Pour configurer une machine virtuelle agent.



La sécurité des charges de travail n'est pas disponible dans l'édition fédérale de Cloud Insights.

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 l'ordinateur. Si les paramètres d'autorisation n'autorisent pas la création d'un utilisateur local et nécessitent à la place Active Directory, un utilisateur avec le nom d'utilisateur `cssys` doit être créé dans le serveur Active Directory.
- Vous pouvez en savoir plus sur la sécurité Cloud Insights ["ici"](#).

Procédure d'installation de l'agent

1. Connectez-vous en tant qu'administrateur ou responsable de compte à votre environnement de sécurité de la charge de travail.
2. Sélectionnez **collecteurs > agents > +Agent**

Le système affiche la page Ajouter un agent :

Add an Agent X

Cloud Secure collects device and user data using one or more Agents installed on local servers. Each Agent can host multiple Data Collectors, which send data to Cloud Secure for analysis.

Which Operating system are you using ?

CentOS RHEL

Close

3. Vérifiez que le serveur 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 supportées (i)*.
5. Si votre réseau utilise un serveur proxy, définissez les détails du serveur proxy en suivant les instructions de la section Proxy.

Agent Server Requirements

Linux Versions Supported: [?](#) Minimum Server Requirements: [?](#)

Need Help?

1. If a proxy server is used, please enter these proxy server settings after editing in your proxy variables.



```
token='eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJvbmV0aw1lVG9rZW5JZCdk1Zi05YjU0WFJlLTQwNDYtNDk1Zi05YjU1LTdhYjZlODhmNDVlMyIsInJvbnZlclVybkBwluIl0sInNlcnZlclVybkCI6Imh0dHBzOi8vZnc3MzRZW5JZCdk1Zi05YjU0WFJlLTQwNDYtNDk1Zi05YjU1LTdhYjZlODhmNDVlMyIsInJvbnZlclVybkBwluIl0sInNlcnZlclVybkCI6Imh0dHBzOi8vZnc3M3YmJmLTJhMDI0YjYjMC00ODY2LWYwN2JhMDI0YjYjcwMSIsIm1hdCI6MTY2Mz
```



- ✔ New agent detected!

1. Vous devez configurer un "Collecteur d'annuaire d'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. En cas de problème de sécurité concernant la plage de ports, vous pouvez utiliser une plage de ports inférieure, 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 plate-forme :

CentOS 7.x/RHEL 7.x :

1. `sudo iptables-save | grep 35000`

Sortie d'échantillon :

```
-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)

Sortie d'échantillon :

```
35000-55000/tcp
```

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 contient aucune information pertinente.	Cette erreur se produit lors du démarrage de l'agent. L'erreur n'est pas consignée 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 <code>journalctl -u cloudsecure-agent.service</code> commande. Cette commande peut être utilisée pour résoudre le problème plus loin.
L'installation de l'agent échoue avec 'cette distribution linux n'est pas prise en charge. Fermeture de l'installation'.	Cette erreur apparaît lorsque vous tentez d'installer l'agent sur un système non pris en charge. Voir "Exigences de l'agent" .

Problème :	Résolution :
L'installation de l'agent a échoué avec l'erreur : "-bash : unzip : commande introuvable"	Installez unzip, puis exécutez de nouveau la commande d'installation. Si Yum est installé sur la machine, essayez "yum install unzip" pour installer le logiciel dézip. Ensuite, copiez à nouveau la commande à partir de l'interface utilisateur d'installation de l'agent et collez-la dans l'interface de ligne de commande pour exécuter à nouveau l'installation.
L'agent a été installé et était en cours d'exécution. Toutefois, l'agent s'est arrêté soudainement.	SSH vers l'ordinateur Agent. Vérifiez l'état du service agent via <code>sudo systemctl status cloudsecure-agent.service</code> . 1. Vérifiez si les journaux affichent un message "Impossible de démarrer le service du démon de sécurité de la charge de travail" . 2. Vérifiez si l'utilisateur cssys existe dans l'appareil Agent ou non. Exécutez les commandes suivantes une par une avec l'autorisation root et vérifiez si l'utilisateur et le groupe cssys existent. <code>sudo id cssys</code> <code>sudo groups cssys`</code> 3. Si aucune règle n'existe, une stratégie de surveillance centralisée peut avoir supprimé l'utilisateur de cssys. 4. Créez l'utilisateur et le groupe cssys manuellement en exécutant les commandes suivantes. <code>`sudo useradd cssys</code> <code>`sudo groupadd cssys`</code> 5. Redémarrez le service agent après cela en exécutant la commande suivante : <code>`sudo systemctl restart cloudsecure-agent.service`</code> 6. S'il n'est toujours pas en cours d'exécution, vérifiez 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 autres collecteurs.
L'interface utilisateur indique que l'agent est à l'état NON CONNECTÉ.	Étapes de redémarrage de l'agent. 1. SSH vers l'ordinateur Agent. 2. Redémarrez le service agent après cela en exécutant la commande suivante : <code>sudo systemctl restart cloudsecure-agent.service`</code> 3. Vérifier l'état du service agent via <code>`sudo systemctl status cloudsecure-agent.service</code> . 4. L'agent doit passer à l'état CONNECTÉ.

Problème :	Résolution :
<p>La machine virtuelle de l'agent 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 signé par Zscaler CA de sorte que l'agent ne fait pas confiance à la communication.</p>	<p>Désactivez l'inspection SSL dans le proxy Zscaler pour l'url *.cloudinsights.netapp.com. Si Zscaler procède à l'inspection SSL et remplace les certificats, la sécurité de la charge de travail ne fonctionnera pas.</p>
<p>Lors de l'installation de l'agent, l'installation se bloque après le décompression.</p>	<p>La commande chmod 755 -RF est défectueuse. La commande échoue lorsque la commande d'installation de l'agent est exécutée par un utilisateur non-root sudo qui a des fichiers dans le répertoire de travail, appartenant à un autre utilisateur et que 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 "cloudssécurisée". 2. Allez à ce répertoire. 3. Copiez et collez le "jeton=..... .. /cloudsecure-agent-install.sh", commande d'installation et appuyez sur entrée. 4. L'installation doit pouvoir continuer.</p>
<p>Si l'agent n'est toujours pas en mesure de se connecter à Saas, veuillez ouvrir un dossier auprès du support NetApp. Fournissez le numéro de série Cloud Insights pour ouvrir un dossier et joindre les journaux au dossier comme indiqué.</p>	<p>Pour joindre des journaux au cas : 1. Exécutez le script suivant avec l'autorisation root et partagez le fichier de sortie (cloudSecure-agent-symptômes.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. groupes cssys c. cat /etc/os-release</p>
<p>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 de l'état de service instantané prise de l'instantané de la structure d'annuaire de l'agent /Opt/netapp/cloudSecure/agent/bin/cloudSecure-agent-symptôme-Collector.sh: Ligne 52: Zip: Commande introuvable ERREUR: Échec de la création /tmp/cloudsecure-agent-symptoms.zip</p>	<p>L'outil de fermeture à glissière n'est pas installé. Installer l'outil zip en exécutant la commande "yum install zip". Puis exécutez à nouveau le cloudsecure-agent-symptom-collector.sh.</p>

Problème :	Résolution :
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 du manque d'autorisations. La solution serait de créer l'utilisateur cssys et d'ajouter son répertoire de connexion manuellement à l'aide de la commande suivante : <code>sudo useradd nom_utilisateur -m -d HOME_DIR</code> -m : Créez le répertoire de base de l'utilisateur s'il n'existe pas. -D : le nouvel utilisateur est créé en utilisant HOME_DIR comme valeur du répertoire de connexion de l'utilisateur. Par exemple, <code>sudo useradd cssys -m -d /cssys</code> , ajoute un utilisateur cssys et crée son répertoire de connexion sous root.
L'agent n'est pas en cours d'exécution après l'installation. <code>Systemctl status cloudsecure-agent.service</code> montre ce qui suit: [Root@demo ~]# <code>systemctl status cloudsecure-agent.service</code> agent.service – Workload Security Agent Daemon Service chargé: Chargé (/usr/lib/systemd/system/cloudsecure-agent.service; activé; fournisseur prédéfini: Disabled) active: Activation (redémarrage automatique) (résultat: Exit-code) depuis tue 2021-08-03 21 25889:12:26 Pbin/Security/ID_fr = démarrage/ID_de l'agent_Cloud/n/n_1/n_1/126 = uned/n_1/n_1/n_1_1_1_1_1_1_1_1_1_3_3_1 25889 (code=fermé, état=126), août 03 21:12:26 système de démonstration[1] : cloudsecure-agent.service: processus principal fermé, code=fermé, état=126/n/a août 03 21:12:26 système de démonstration[1] : l'unité cloudsecure-agent.service a entré l'état en échec. Aug 03 21:12:26 DEMO system[1]: cloudsecure-agent.service failed.	Ceci peut échouer car cssys l'utilisateur n'est peut-être pas autorisé à installer. Si /opt/netapp est un montage NFS et si l'utilisateur cssys n'a pas accès à ce dossier, l'installation échoue. Cssys est un utilisateur local créé par le programme d'installation de Workload Security qui n'a peut-être pas l'autorisation d'accéder au partage monté. Pour ce faire, essayez d'accéder à /opt/netapp/cloudSecure/agent/bin/cloudSecure-agent à l'aide de cssys user. S'il renvoie "permission refusée", l'autorisation d'installation n'est pas présente. Au lieu d'un dossier monté, installez-le sur un répertoire local de la machine.
L'agent était 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 modifier la configuration du proxy de l'agent ?	Vous pouvez modifier le fichier agent.properties pour ajouter les détails du proxy. Procédez comme suit : 1. Passez au dossier contenant le fichier de propriétés : <code>cd /opt/netapp/cloudSecure/conf</code> 2. À l'aide de votre éditeur de texte favori, ouvrez le fichier <code>agent.properties</code> 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 : <code>sudo systemctl redémarrez cloudsecure-agent.service</code>

Suppression d'un agent de sécurité de charge de travail

Lorsque vous supprimez un agent de sécurité de charge de travail, tous les collecteurs de données associés à l'agent doivent être supprimés en premier.

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 autre agent, vous devez créer une sauvegarde des configurations Data Collector 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 de sécurité de la charge de travail.

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

Procédure de suppression d'un agent :

1. SSH dans le VM agent 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'annuaire d'utilisateurs Active Directory (AD)

La sécurité des charges de travail peut être configurée pour collecter des attributs utilisateur à partir des serveurs Active Directory.

Avant de commencer

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

Procédure de configuration d'un collecteur d'annuaire d'utilisateurs

1. Dans le menu sécurité de la charge de travail, cliquez sur :
Collecteurs > collecteurs d'annuaire d'utilisateurs > + collecteur d'annuaire d'utilisateurs et sélectionnez **Active Directory**

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

Configurez le collecteur d'annuaire d'utilisateurs en entrant les données requises dans les tableaux suivants :

Nom	Description
Nom	Nom unique du répertoire utilisateur. Par exemple <i>GlobalADCollector</i>
Agent	Sélectionnez un agent configuré dans la liste
IP/Nom de domaine du serveur	Adresse IP ou nom de domaine complet (FQDN) du serveur hébergeant le répertoire actif
Nom de la forêt	Niveau forestier de la structure du répertoire. Le nom de forêt permet les deux formats suivants : <i>x.correct.z</i> ⇒ nom de domaine direct comme vous l'avez sur votre SVM. [Exemple : <i>hq.companynome.com</i>] <i>DC=x,DC=y,DC=z</i> ⇒ noms distinctifs relatifs [exemple : <i>DC=hq,DC=companynome,DC=com</i>] ou vous pouvez spécifier les éléments suivants : <i>Ou=engineering,DC=hq,DC=companynome,DC=com</i> [to filter by Specific UO Engineering] <i>CN=username,ou=engineering,DC=companynome,DC=netapp,DC=com</i> [to get only user with <username> from ou <engineering>] <i>_CN=Acrobat,CN=Users,CN=company=ID=DC=ID=ID=ID=ici=ID=ID=ID=entreprise,DC=ID=ici=ID=s=ID=ID=s=s=s=s=ici=ID_a_a_a_c,c=ID=s=s=noms_a_a_c=noms_c=</i>
Lier DN	L'utilisateur est autorisé à rechercher dans le répertoire. Par exemple : <i>username@companynome.com</i> ou <i>username@domainname.com</i> En outre, l'autorisation lecture seule du domaine est requise. L'utilisateur doit être membre du groupe de sécurité <i>contrôleurs de domaine en lecture seule</i> .
LIER le mot de passe	Mot de passe du serveur d'annuaire (c'est-à-dire mot de passe pour le nom d'utilisateur utilisé dans Bind DN)
Protocole	Idap, Idaps, Idap-start-tls
Ports	Sélectionnez le port

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

Attributs	Nom d'attribut dans le serveur d'annuaire
Afficher le nom	nom
SID	id d'objet
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 électronique	e-mail
Numéro de téléphone	téléphone
Rôle	titre
Pays	co
État	état
Service	service
Photo	miniature
Gestionnaire DN	gestionnaire
Groupes	Membre

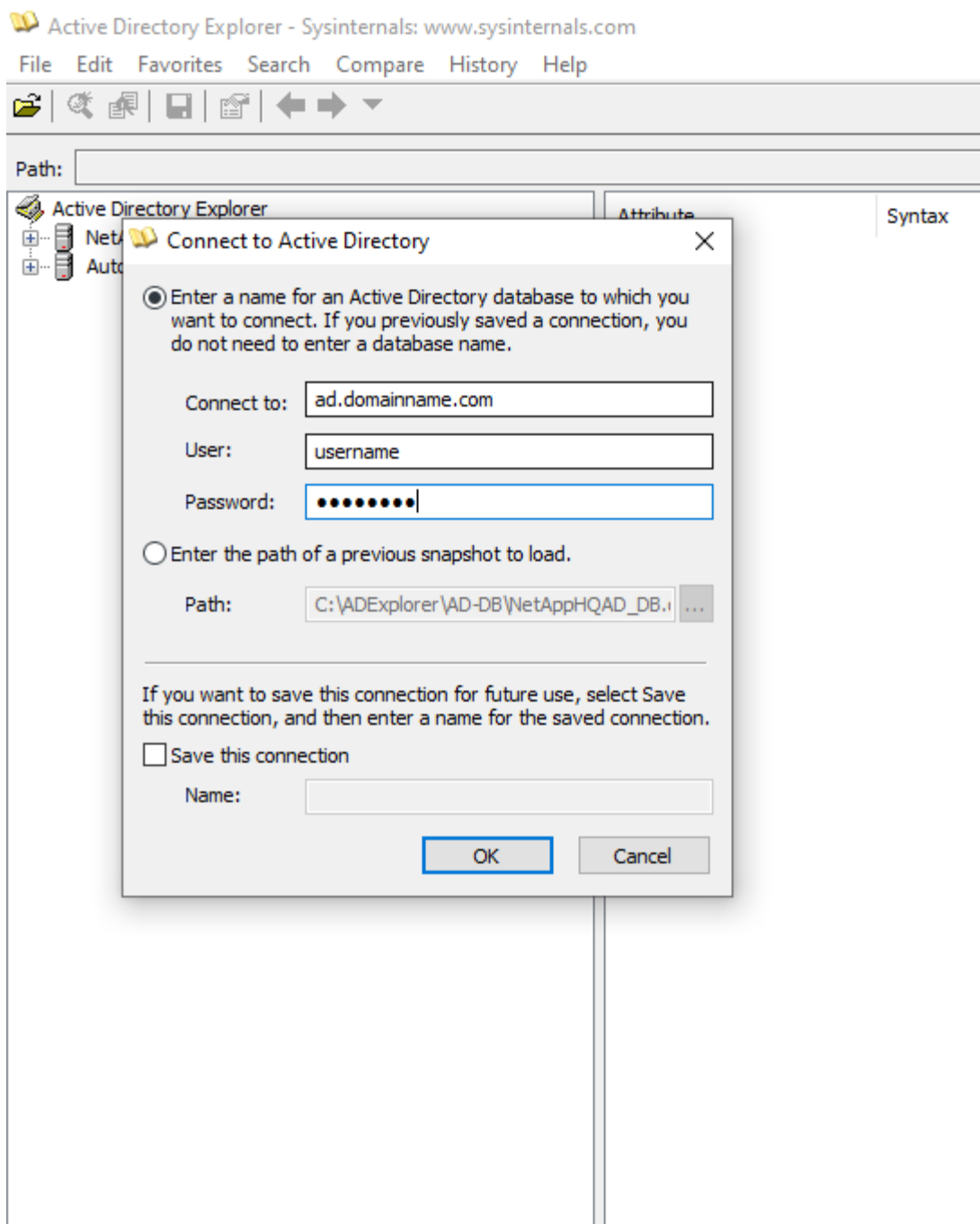
Test de la configuration du collecteur d'annuaire d'utilisateurs

Vous pouvez valider les autorisations utilisateur LDAP et les définitions d'attributs en suivant les procédures suivantes :

- Utilisez la commande suivante pour valider l'autorisation utilisateur LDAP de la sécurité de la charge de travail :

```
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 l'Explorateur AD pour naviguer dans 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 exécuter à nouveau.
 - Installer "[Explorateur D'ANNONCES](#)" Sur n'importe quel ordinateur Windows pouvant se connecter à AD Server.
 - 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'annuaire utilisateur

Le tableau suivant décrit les problèmes connus et les solutions qui peuvent survenir pendant la configuration du collecteur :

Problème :	Résolution :
L'ajout d'un connecteur de répertoire utilisateur donne l'état "erreur". 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 de répertoire utilisateur donne 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 ne s'affichent pas dans la page profil utilisateur de sécurité de la charge de travail.	Ceci est probablement dû à une incohérence entre les noms des attributs facultatifs ajoutés dans CloudSecure et les noms réels des attributs dans Active Directory. Modifiez et fournissez le ou les noms d'attribut facultatifs appropriés.
Data Collector à l'état d'erreur avec « Impossible de récupérer les utilisateurs LDAP. Raison de l'échec : impossible de se connecter sur le serveur, la connexion est nulle »	Redémarrez le collecteur en cliquant sur le bouton <i>Restart</i> .
L'ajout d'un connecteur de répertoire utilisateur donne l'état "erreur".	Assurez-vous que vous avez fourni des valeurs valides pour les champs requis (serveur, nom-forêt, nom-bind, mot-de-passe-bind). Assurez-vous que l'entrée bind-DN est toujours fournie en tant que 'Administrateur@<nom_domaine_forêt>' ou en tant que compte d'utilisateur disposant de privilèges d'administrateur de domaine.
L'ajout d'un connecteur d'annuaire utilisateur a pour résultat l'état « RECOMMANDE ». Affiche l'erreur "Impossible de définir l'état du collecteur,raison de la commande TCP [Connect(localhost:35012,None,List(),About(,secondes),true)] a échoué en raison de java.net.ConnectionException:Connection refusé."	IP ou FQDN incorrect fourni pour le serveur AD. Modifiez et fournissez l'adresse IP ou le nom de domaine complet approprié.
L'ajout d'un connecteur de répertoire utilisateur donne 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 nom de domaine complet approprié.
L'ajout d'un connecteur de répertoire utilisateur donne l'état "erreur". L'erreur indique : « Impossible de charger les paramètres. Motif : la configuration de la source de données présente une erreur. Raison spécifique : /Connector/conf/application.conf: 70: ldap.ldap-port a une CHAÎNE de type plutôt QUE DU NOMBRE”	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 données facultatives, les données d'attributs facultatives ne sont pas extraites d'AD.	Ceci est probablement dû à une incohérence entre les attributs facultatifs ajoutés dans CloudSecure et les noms réels des attributs 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 se produira-t-elle ?	LA synchronisation AD se produit immédiatement après le redémarrage du collecteur. La récupération des données utilisateur d'environ 300 000 utilisateurs prend environ 15 minutes. De plus, elle est mise à jour 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 d'actualisation non prévue. Si le locataire est supprimé, les données seront supprimées.
Le connecteur de répertoire utilisateur indique 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: AcceptSecurityContext error, data 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.	Ceci est probablement dû à un problème de mappage d'attribut avec Active Directory. 1. Modifiez le collecteur Active Directory particulier qui recherche les informations de l'utilisateur à partir d'Active Directory. 2. Avis sous attributs facultatifs, il existe un nom de champ "Numéro de téléphone" mappé sur l'attribut Active Directory 'Numéro de téléphone'. 4. Maintenant, utilisez l'outil Explorateur Active Directory comme décrit ci-dessus pour naviguer dans Active Directory et voir le nom d'attribut correct. 3. Assurez-vous que dans Active Directory il y a un attribut appelé «téléphone» qui a en effet le numéro de téléphone de l'utilisateur. 5. Disons dans Active Directory qu'il a été modifié en "numéro de téléphone". 6. Puis modifiez le collecteur de répertoire d'utilisateurs CloudSecure. Dans la section des attributs facultatifs, remplacer «téléphone» par «numéro de téléphone». 7. Enregistrez le collecteur Active Directory, le collecteur redémarre et affiche le numéro de téléphone de l'utilisateur dans la page de profil utilisateur.
Si le certificat de cryptage (SSL) est activé sur le serveur Active Directory (AD), le collecteur d'annuaire de l'utilisateur de sécurité de charge de travail ne peut pas se connecter au serveur AD.	Désactivez le cryptage du serveur AD avant de configurer un collecteur d'annuaire utilisateur. Une fois les informations utilisateur extraites, elles seront disponibles pendant 13 mois. Si le serveur AD est déconnecté après avoir récupéré les détails de l'utilisateur, les nouveaux utilisateurs dans AD ne seront pas extraits. Pour récupérer à nouveau, le collecteur d'annuaire de l'utilisateur 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 d'Active Directory de CloudInsights Security. Pour supprimer l'utilisateur, le locataire complet doit être supprimé.

Configuration d'un collecteur de serveur d'annuaire LDAP

Vous configurez la sécurité de la charge de travail pour collecter les attributs utilisateur à partir des serveurs d'annuaire LDAP.

Avant de commencer

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

Procédure de configuration d'un collecteur d'annuaire d'utilisateurs

1. Dans le menu sécurité de la charge de travail, cliquez sur :
Collecteurs > collecteurs d'annuaire d'utilisateurs > + collecteur d'annuaire d'utilisateurs et sélectionnez **serveur d'annuaire LDAP**

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

Configurez le collecteur d'annuaire d'utilisateurs en entrant les données requises dans les tableaux suivants :

Nom	Description
Nom	Nom unique du répertoire utilisateur. Par exemple <i>GlobalLDAPCollector</i>
Agent	Sélectionnez un agent configuré dans la liste
IP/Nom de domaine du serveur	Adresse IP ou nom de domaine complet (FQDN) du serveur hébergeant le serveur d'annuaire LDAP
Base de recherche	La base de recherche du serveur LDAP Search base permet les deux formats suivants : x. <i>correct.z</i> ⇒ nom de domaine direct tel que vous l'avez sur votre SVM. [Exemple : <i>hq.companyname.com</i>] <i>DC=x,DC=y,DC=z</i> ⇒ noms distinctifs relatifs [exemple : <i>DC=hq,DC=companyname,DC=com</i>] ou vous pouvez spécifier les éléments suivants : <i>Ou=engineering,DC=hq,DC=companyname,DC=com</i> [to filter by Specific UO Engineering] <i>CN=username,ou=engineering,DC=companyname,DC=netapp, DC=com</i> [to get only user with <username> from ou <Engineering>] <i>_CN=Acrobat,CN=Users,CN=company=ID=Users,DC=Company=Company=Company=s==Company=Company=s=Company=Company=Company=s=ID=s,DC=ID=s=ID=s=s=s=</i>
Lier DN	L'utilisateur est autorisé à rechercher dans le répertoire. Par exemple : <i>uid=ldapuser,cn=Users,cn=Accounts,dc=domain,dc=companyname,dc=com</i> <i>uid=john,cn=Users,cn=comptes,dc=dorp,dc=Company,dc=com</i> pour un utilisateur john@dorp.company.com . <i>dorp.company.com</i>

--comptes	--utilisateurs
--jean	--anna
LIER le mot de passe	Mot de passe du serveur d'annuaire (c'est-à-dire mot de passe pour le nom d'utilisateur utilisé dans Bind DN)
Protocole	ldap, ldaps, ldap-start-tls
Ports	Sélectionnez le port

Entrez les attributs requis du serveur d'annuaire suivants si les noms d'attribut par défaut ont été modifiés dans le serveur d'annuaire LDAP. Le plus souvent, ces noms d'attributs sont *NOT* modifiés dans LDAP Directory Server, auquel cas vous pouvez simplement continuer avec le nom d'attribut par défaut.

Attributs	Nom d'attribut dans le serveur d'annuaire
Afficher le nom	nom
NON-IXID	numéro uidnumber
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 électronique	e-mail
Numéro de téléphone	téléphone
Rôle	titre
Pays	co
État	état
Service	numéro du département
Photo	photo
Gestionnaire DN	gestionnaire
Groupes	Membre

Test de la configuration du collecteur d'annuaire d'utilisateurs

Vous pouvez valider les autorisations utilisateur LDAP et les définitions d'attributs en suivant les procédures suivantes :

- Utilisez la commande suivante pour valider l'autorisation utilisateur LDAP de la sécurité de la charge de travail :

```
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 l'Explorateur LDAP 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 exécuter à nouveau.

- Installez LDAP Explorer Ou Java LDAP Explorer Sur n'importe quel ordinateur Windows qui peut se connecter au serveur LDAP.
- Connectez-vous au serveur LDAP à l'aide du nom d'utilisateur/mot de passe du serveur d'annuaire LDAP.

The screenshot shows a 'Configuration' dialog box for LDAP. It has five tabs: Configuration, Server, Connection, Option, and SSL/TLS. The 'Configuration' tab is active. It contains the following fields and controls:

- User DN:** A text box containing 'cn=admin,d'.
- Password:** A text box with masked characters '*****'.
- Use SSL port:** Two radio buttons, 'Yes' and 'No', with 'No' selected.
- Use TLS:** Two radio buttons, 'Yes' and 'No', with 'No' selected.
- Base DN:** A text box containing 'dc=workgro'.
- Anonymous login:** An unchecked checkbox.
- Store password:** A checked checkbox.
- Test connection:** A button located below the Base DN field.
- Guess value:** A button located to the right of the Base DN field.
- Buttons:** 'Ok' and 'Annuler' (Cancel) buttons at the bottom.

Dépannage des erreurs de configuration du collecteur d'annuaire LDAP

Le tableau suivant décrit les problèmes connus et les solutions qui peuvent survenir pendant la configuration du collecteur :

Problème :	Résolution :
L'ajout d'un connecteur d'annuaire LDAP entraîne l'état "erreur". Erreur indique : "informations d'identification non valides fournies pour le serveur LDAP".	Nom unique de liaison ou mot de passe de liaison incorrect ou base de recherche fournie. Modifiez et fournissez les informations correctes.
L'ajout d'un connecteur d'annuaire LDAP entraîne 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 fournie incorrecte. Modifiez et fournissez le nom de forêt correct.
Les attributs facultatifs de l'utilisateur de domaine ne s'affichent pas dans la page profil utilisateur de sécurité de la charge de travail.	Ceci est probablement dû à une incohérence entre les noms des attributs facultatifs ajoutés dans CloudSecure et les noms réels des attributs dans Active Directory. Les champs sont sensibles à la casse. Modifiez et fournissez le ou les noms d'attribut facultatifs appropriés.
Data Collector à l'état d'erreur avec « Impossible de récupérer les utilisateurs LDAP. Raison de l'échec : impossible de se connecter sur le serveur, la connexion est nulle »	Redémarrez le collecteur en cliquant sur le bouton <i>Restart</i> .
L'ajout d'un connecteur d'annuaire LDAP entraîne l'état "erreur".	Assurez-vous que vous avez fourni des valeurs valides pour les champs requis (serveur, nom-forêt, nom-bind, mot-de-passe-bind). 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 « recommande ». Affiche l'erreur "Impossible de déterminer l'état de santé du collecteur d'où une nouvelle tentative"	Assurez-vous que l'adresse IP du serveur et la base de recherche correcte sont fournies ///
Lors de l'ajout du répertoire LDAP, l'erreur suivante s'affiche : « Impossible de déterminer l'état du collecteur dans 2 tentatives, essayez de redémarrer le collecteur à nouveau (Code d'erreur : AGENT008) »	Assurez-vous que l'adresse IP du serveur et la base de recherche appropriées sont fournies
L'ajout d'un connecteur d'annuaire LDAP entraîne l'état « recommande ». Affiche l'erreur "Impossible de définir l'état du collecteur,raison de la commande TCP [Connect(localhost:35012,None,List(),About(,secondes),true)] a échoué en raison de java.net.ConnectionException:Connection refusé."	IP ou FQDN incorrect fourni pour le serveur AD. Modifiez et fournissez l'adresse IP ou le nom de domaine complet approprié. ////
L'ajout d'un connecteur d'annuaire LDAP entraîne l'état "erreur". L'erreur indique "échec de l'établissement de la connexion LDAP".	Adresse IP ou FQDN incorrecte fournie pour le serveur LDAP. Modifiez et fournissez l'adresse IP ou le nom de domaine complet approprié. 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 entraîne l'état "erreur". L'erreur indique : « Impossible de charger les paramètres. Motif : la configuration de la source de données présente une erreur. Raison spécifique : /Connector/conf/application.conf: 70: ldap.ldap-port a une CHAÎNE de type plutôt QUE DU NOMBRE »	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 données facultatives, les données d'attributs facultatives ne sont pas extraites d'AD.	Ceci est probablement dû à une incohérence entre les attributs facultatifs ajoutés dans CloudSecure et les noms réels des attributs dans Active Directory. Modifiez et fournissez le nom d'attribut obligatoire ou facultatif correct.
Après le redémarrage du collecteur, quand la synchronisation LDAP se produira-t-elle ?	La synchronisation LDAP se produit immédiatement après le redémarrage du collecteur. La récupération des données utilisateur d'environ 300 000 utilisateurs prend environ 15 minutes. De plus, elle est mise à jour automatiquement toutes les 12 heures.
Les données utilisateur sont synchronisées de LDAP à CloudSecure. Quand les données seront-elles supprimées ?	Les données utilisateur sont conservées pendant 13 mois en cas d'actualisation non prévue. Si le locataire est supprimé, les données seront supprimées.
LDAP Directory Connector affiche 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: AcceptSecurityContext error, data 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.	Ceci est probablement dû à un problème de mappage d'attribut avec Active Directory. 1. Modifiez le collecteur Active Directory particulier qui recherche les informations de l'utilisateur à partir d'Active Directory. 2. Avis sous attributs facultatifs, il existe un nom de champ "Numéro de téléphone" mappé sur l'attribut Active Directory 'Numéro de téléphone'. 4. Utilisez l'outil Explorateur Active Directory 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 y a un attribut appelé «téléphone» qui a en effet le numéro de téléphone de l'utilisateur. 5. Disons dans l'annuaire LDAP qu'il a été modifié en «téléphone». 6. Puis modifiez le collecteur de répertoire d'utilisateurs CloudSecure. Dans la section des attributs facultatifs, remplacer «téléphone» par «numéro de téléphone». 7. Enregistrez le collecteur Active Directory, le collecteur redémarre et affiche le numéro de téléphone de l'utilisateur dans la page de profil utilisateur.

Problème :	Résolution :
Si le certificat de cryptage (SSL) est activé sur le serveur Active Directory (AD), le collecteur d'annuaire de l'utilisateur de sécurité de charge de travail ne peut pas se connecter au serveur AD.	Désactivez le cryptage du serveur AD avant de configurer un collecteur d'annuaire utilisateur. Une fois les informations utilisateur extraites, elles seront disponibles pendant 13 mois. Si le serveur AD est déconnecté après avoir récupéré les détails de l'utilisateur, les nouveaux utilisateurs dans AD ne seront pas extraits. Pour récupérer à nouveau, le collecteur d'annuaire de l'utilisateur doit être connecté à AD.

Configuration du SVM Data Collector de ONTAP

La sécurité de la charge de travail utilise des collecteurs de données pour collecter les données d'accès des fichiers et des utilisateurs à partir de terminaux.

Avant de commencer

- Ce collecteur de données est pris en charge avec les éléments suivants :
 - Data ONTAP 9.2 et versions ultérieures Pour des performances optimales, utilisez une version Data ONTAP supérieure à 9.13.1.
 - Protocole SMB version 3.1 et antérieure.
 - Protocole NFS version 4.0 et antérieure
 - FlexGroup est pris en charge à partir de ONTAP 9.4 et versions ultérieures
 - ONTAP Select est pris en charge
- Seuls les SVM de type données sont pris en charge. Les SVM avec Infinite volumes ne sont pas pris en charge.
- SVM possède 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 des collecteurs de données.
- Assurez-vous que vous disposez d'un connecteur d'annuaire utilisateur correctement configuré. Dans le cas contraire, les événements affichent des noms d'utilisateur codés et non le nom réel de l'utilisateur (tel qu'il est stocké dans Active Directory) dans la page « activités approfondies ».
- Pour des performances optimales, il est recommandé de configurer le serveur FPolicy sur le même sous-réseau que le système de stockage.
- Vous devez ajouter un SVM à l'aide de l'une des deux méthodes suivantes :
 - En utilisant l'IP du cluster, le nom du SVM et le nom d'utilisateur et mot de passe de Cluster Management. **c'est la méthode recommandée.**
 - Le nom du SVM doit être exactement comme indiqué dans ONTAP et est sensible à la casse.
 - En utilisant SVM Vserver Management IP, Nom d'utilisateur et Mot de passe
 - Si vous ne pouvez pas ou n'êtes pas disposé à utiliser le nom d'utilisateur et le mot de passe administrateur complet Cluster/SVM Management, vous pouvez créer un utilisateur personnalisé avec des privilèges moins importants comme indiqué dans la ["Une note sur les autorisations"](#) section ci-dessous. Cet utilisateur personnalisé peut être créé pour l'accès au SVM ou au cluster.
 - o vous pouvez également utiliser un utilisateur AD avec un rôle qui possède au moins les

autorisations de csrole, comme indiqué dans la section "Une note sur les autorisations" ci-dessous. Reportez-vous également à la ["Documentation ONTAP"](#).

- S'assurer que les applications correctes sont définies pour le SVM en exécutant la commande suivante :

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

Exemple de résultat

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

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

Le système renvoie le nom du Vserver, le nom du serveur CIFS et les champs supplémentaires.

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

Voir ["Exigences de l'agent"](#) pour des informations de configuration. Cela s'applique aux agents et agents installés sur site dans le Cloud.

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

Conditions préalables au blocage de l'accès utilisateur

Gardez les points suivants à l'esprit pendant ["Blocage de l'accès utilisateur"](#):

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

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

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

Pour *csuser* avec les identifiants du cluster, effectuez la procédure suivante dans 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
```

Remarque sur les autorisations

Autorisations lors de l'ajout via Cluster Management IP :

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

Pour créer le nouvel utilisateur, connectez-vous à ONTAP à l'aide du nom d'utilisateur/mot de passe de l'administrateur de gestion des clusters 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 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
```

Autorisations pour l'intégration ARP ONTAP :

```
security login rest-role create -role arwrole -api /api/storage/volumes
-access readonly -vserver <cluster_name>
security login rest-role create -api /api/security/anti-ransomware -access
readonly -role arwrole -vserver <cluster_name>
security login create -user-or-group-name csuser -application http
-authmethod password -role arwrole
```

Autorisations d'accès ONTAP refusées :

```
security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <cluster_name>
security login create -user-or-group-name csuser -application http
-authmethod password -role csrestrole
```

Remarque : si un rôle REST est déjà ajouté—soit *arwrole* soit *csrestrole*--il n'est pas nécessaire d'ajouter un deuxième rôle REST. Vous pouvez simplement ajouter les autorisations d'API comme dans l'exemple ci-dessous.

Exemple : *csrestrole* est déjà présent. Il nous suffit donc d'activer la protection contre les ransomware et de donner des autorisations d'API au *csrestrole* existant :

```
security login rest-role create -role csrestrole -api /api/storage/volumes
-access readonly -vserver <cluster_name>
security login rest-role create -api /api/security/anti-ransomware -access
readonly -role arwrole -vserver <cluster_name>
```

Autorisations lors de l'ajout via Vserver Management IP :

Si vous ne pouvez pas utiliser l'utilisateur administrateur de gestion du cluster pour permettre à Workload Security d'accéder au collecteur de données du SVM ONTAP, vous pouvez créer un nouvel utilisateur nommé « csuser » avec les rôles, comme indiqué 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 de la sécurité Workload pour utiliser l'IP de gestion Vserver.

Pour créer le nouvel utilisateur, connectez-vous à ONTAP à l'aide du nom d'utilisateur/mot de passe de l'administrateur de gestion des clusters et exécutez les commandes suivantes sur le serveur ONTAP. Pour faciliter la gestion, copiez ces commandes dans un éditeur de texte et remplacez <vservname> par votre nom de Vserver avant d'exécuter les commandes suivantes sur ONTAP :

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

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

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

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

Autorisations d'accès ONTAP refusées :

```
security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <svm_name>
security login create -user-or-group-name csuser -application http
-authmethod password -role csrestrole -vserver <svm_name>
```

Autorisations pour la protection anti-ransomware autonome de ONTAP

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

Si vous utilisez un utilisateur personnalisé (par exemple, *csuser*) avec les autorisations accordées à l'utilisateur, suivez les étapes ci-dessous pour donner les autorisations à la sécurité de la charge de travail afin de collecter des informations relatives à ARP à partir de ONTAP.

Pour *csuser* avec les informations d'identification du cluster, effectuez les opérations suivantes à partir de la ligne de commande ONTAP :

```
security login rest-role create -role arwrole -api /api/storage/volumes
-access readonly -vserver <cluster_name>
security login rest-role create -api /api/security/anti-ransomware -access
readonly -role arwrole -vserver <cluster_name>
security login create -user-or-group-name csuser -application http
-authmethod password -role arwrole
```

Pour plus d'informations, consultez à propos de ["Intégration avec la protection ONTAP autonome contre les ransomwares"](#)

Autorisations d'accès ONTAP refusées

Si le Data Collector 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 les autorisations données 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 les *ccsuser* avec des informations d'identification *cluster*, exécutez les commandes suivantes à partir de la ligne de commande ONTAP. Notez que *csrestrole* est un rôle personnalisé et *csuser* est un utilisateur personnalisé ONTAP.

```
security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <cluster_name>
security login create -user-or-group-name csuser -application http
-authmethod password -role csrestrole
```

Pour les *csuser* avec *SVM* credentials, exécuter les commandes suivantes depuis la ligne de commande ONTAP :

```
security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <svm_name>
security login create -user-or-group-name csuser -application http
-authmethod password -role csrestrole -vserver <svm_name>
```

Pour plus d'informations, consultez à propos de ["Intégration avec l'accès ONTAP refusée"](#)

Configurer le collecteur de données

Étapes de configuration

1. Connectez-vous en tant qu'administrateur ou responsable de compte à votre environnement Cloud Insights.
2. Cliquez sur **sécurité de la charge de travail > collecteurs > +collecteurs de données**

Le système affiche les collecteurs de données disponibles.

3. Placez le curseur de la souris sur la vignette **NetApp SVM et cliquez sur *+Monitor**.

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

Champ	Description
Nom	Nom unique pour le Data Collector
Agent	Sélectionnez un agent configuré dans la liste.
Se connecter via l'IP de gestion pour :	Sélectionnez IP de cluster ou IP de gestion SVM
Adresse IP de gestion cluster / SVM	L'adresse IP du cluster ou du SVM, en fonction de votre choix ci-dessus.
Nom du SVM	Le nom du SVM (ce champ est requis lors de la connexion via IP du cluster)
Nom d'utilisateur	Nom d'utilisateur pour accéder au SVM/Cluster lors de l'ajout via IP du cluster les options sont : 1. Cluster-admin 2. 'csuser' 3. UTILISATEUR AD ayant le rôle similaire à celui de csuser. Lors de l'ajout via SVM IP, les options sont les suivantes : 4. vsadmin 5 'csuser' 6. AD-username ayant le rôle similaire à csuser.
Mot de passe	Mot de passe du nom d'utilisateur ci-dessus
Filtrer les partages/volumes	Choisissez d'inclure ou d'exclure des partages/volumes de la collection d'événements
Entrez les noms de partage complets à exclure/inclure	Liste de partages séparés par des virgules à exclure ou inclure (le cas échéant) de la collection d'événements
Entrez les noms complets des volumes à exclure/inclure	Liste de volumes séparés par des virgules à exclure ou inclure (le cas échéant) de la collection d'événements

Surveiller l'accès au dossier	Lorsque cette case est cochée, active les événements pour la surveillance de l'accès aux dossiers. Notez que la création/le renommage et la suppression de dossiers seront contrôlés même si cette option n'est pas sélectionnée. L'activation de cette option augmente le nombre d'événements surveillés.
Définir la taille de la mémoire tampon d'envoi ONTAP	Définit la taille du tampon d'envoi de la Fpolicy ONTAP. Si une version antérieure à ONTAP 9.8p7 est utilisée et qu'un problème de performances est détecté, la taille de la mémoire tampon d'envoi ONTAP peut être modifiée pour améliorer les performances de ONTAP. Contactez le support NetApp si vous ne voyez pas cette option et souhaitez l'explorer.

Une fois que vous avez 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 Metro Cluster

Il est recommandé d'utiliser les éléments suivants pour Metro Cluster :

1. Connectez deux collecteurs de données, un sur le SVM source et un autre sur le SVM de destination.
2. Les collecteurs de données doivent être connectés par *Cluster IP*.
3. À tout moment, un collecteur de données doit être en cours d'exécution, un autre sera en erreur.

Le collecteur de données actuel de la SVM "en cours d'exécution" s'affiche sous la forme *running*. Le collecteur de données actuel de la SVM 'ssup' sera *Error*.

4. Chaque fois qu'il y a un basculement, l'état du collecteur de données passe de 'en cours d'exécution' à 'erreur' et vice versa.
5. Le collecteur de données passe de l'état erreur à l'état en cours d'exécution pendant deux minutes.

Politique de service

Si vous utilisez une stratégie de service de ONTAP version 9.9.1, afin de vous connecter au Data Source Collector, 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 ONTAP antérieures à 9.9.1, *data-fpolicy-client* n'a pas besoin d'être défini.

Collecteur de données Play-Pause

2 nouvelles opérations sont maintenant affichées dans le menu kebab du collecteur (PAUSE et REPRISE).

Si le Data Collector est à l'état *running*, vous pouvez suspendre la collection. Ouvrez le menu « trois points » du collecteur et sélectionnez PAUSE. Lorsque le collecteur est en pause, aucune donnée n'est collectée à partir de ONTAP et aucune donnée n'est envoyée du collecteur vers ONTAP. Cela signifie qu'aucun événement Fpolicy ne circule de ONTAP vers le collecteur de données et de là vers Cloud Insights.

Notez que si de nouveaux volumes, etc. Sont créés sur ONTAP alors que le collecteur est en pause, la sécurité des workloads ne recueillera pas les données et ces volumes, etc. Ne seront pas reflétés dans les tableaux de bord ou les tableaux.

Gardez à l'esprit les éléments suivants :


- La suppression des snapshots ne se fera pas conformément aux paramètres configurés sur un collecteur en pause.
- Les événements EMS (comme ONTAP ARP) ne seront pas traités sur un collecteur en pause. En d'autres termes, si ONTAP identifie une attaque par ransomware, Cloud Insights Workload Security ne pourra pas acquérir cet événement.
- Les e-mails de notification de santé NE seront PAS envoyés pour un collecteur en pause.
- Les actions manuelles ou automatiques (telles que instantané ou blocage utilisateur) ne sont pas prises en charge sur un collecteur en pause.
- Lors des mises à niveau d'agent ou de collecteur, des redémarrages/redémarrages de machine virtuelle d'agent ou du redémarrage du service d'agent, un collecteur en pause restera à l'état *Pause*.
- Si le collecteur de données est à l'état *Error*, le collecteur ne peut pas être remplacé par l'état *Papersed*. Le bouton Pause est activé uniquement si l'état du collecteur est *running*.
- Si l'agent est déconnecté, le collecteur ne peut pas être remplacé par l'état *Papersed*. Le collecteur passe à l'état *stopped* et le bouton Pause est désactivé.

Dépannage

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

En cas d'erreur, cliquez sur *more detail* dans la colonne *Status* pour obtenir des détails sur l'erreur.

Installed Data Collectors

Name	Status	Type	Agent
9.8_vs1	 Error more detail	ONTAP SVM	agent-11

Problème :	Résolution :
<p>Data Collector s'exécute pendant un certain temps et s'arrête après un temps aléatoire, en échouant avec: "Message d'erreur: Le connecteur est à l'état d'erreur. Nom du service : audit. Cause de la panne : serveur fpolicy externe surchargé. »</p>	<p>Le taux d'événement de ONTAP était beaucoup plus élevé que ce que l'Agent Box peut traiter. Par conséquent, la connexion a été interrompue. Vérifiez le trafic maximal dans CloudSecure lorsque la déconnexion s'est produite. Vous pouvez effectuer cette vérification à partir de la page CloudSecure > activités approfondies > toutes les activités. Si le pic de trafic agrégé est supérieur à ce que l'Agent Box peut traiter, reportez-vous à la page Event Rate Checker sur la taille du déploiement collecteur dans une boîte d'agent. 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 après le redimensionnement de l'interface utilisateur.</p>

Problème :	Résolution :
<p>Le collecteur signale un message d'erreur : "aucune adresse IP locale trouvée sur le connecteur qui peut atteindre les interfaces de données de la SVM".</p>	<p>Cela est probablement dû à un problème de réseau côté ONTAP. Procédez comme suit :</p> <ol style="list-style-type: none"> 1. S'assurer qu'il n'y a pas de pare-feu sur la lif de données du SVM ou sur la lif de gestion qui bloquent la connexion du SVM. 2. Lorsque vous ajoutez un SVM via une IP de gestion du cluster, veillez à ce que la lif de données et la lif de gestion de la SVM soient pingable à partir de la machine virtuelle de l'agent. En cas de problème, vérifier la passerelle, le masque de réseau et les routes de la lif. <p>Vous pouvez également essayer de vous connecter au cluster via ssh à l'aide de l'IP de gestion de cluster et envoyer une requête ping à l'IP de l'agent. Assurez-vous que l'adresse IP de l'agent peut faire l'objet d'un ping :</p> <pre>Network ping -vserver <vserver name> -destination <Agent IP> -lif <Lif Name> -show-detail</pre> <p>Si vous ne pouvez pas effectuer de ping, assurez-vous que les paramètres réseau dans ONTAP sont corrects, de sorte que l'ordinateur de l'agent puisse effectuer des requêtes ping.</p> <ol style="list-style-type: none"> 3. Si vous avez essayé de vous connecter via Cluster IP et qu'il ne fonctionne pas, essayez de vous connecter directement via SVM IP. Voir ci-dessus pour les étapes de connexion via SVM IP. 4. Lors de l'ajout du collecteur via les identifiants SVM IP et vsadmin, vérifiez si le LIF du SVM a le rôle de gestion et Data est activé. Dans ce cas, le ping vers la LIF du SVM va fonctionner, mais SSH vers la LIF du SVM ne fonctionnera pas. Si oui, créer une LIF SVM Mgmt uniquement et tenter de se connecter via cette LIF de management SVM uniquement. 5. Si elle ne fonctionne toujours pas, créez une nouvelle LIF de SVM et essayez de vous connecter via cette LIF. Vérifiez que le masque de sous-réseau est correctement défini. 6. Débogage avancé : <ol style="list-style-type: none"> A) démarrez une trace de paquet dans ONTAP. b) essayez de connecter un collecteur de données au SVM à partir de l'interface utilisateur CloudSecure. c) attendez que l'erreur s'affiche. Arrêtez la trace de paquet dans ONTAP. d) Ouvrez la trace de paquet à partir de ONTAP. Il est

Problème :	Résolution :
<p>Message : « Impossible de déterminer le type de ONTAP pour [nom d'hôte : <adresse IP>. Motif : erreur de connexion au système de stockage <adresse IP> : l'hôte est injoignable (hôte inaccessible) »</p>	<p>1. Vérifier que l'adresse IP de gestion du SVM ou l'IP de gestion du cluster correcte a été fournie. 2. SSH au SVM ou au Cluster auquel vous souhaitez vous connecter. Une fois connecté, assurez-vous que le SVM ou le nom du cluster est correct.</p>
<p>Message d'erreur : « le connecteur est en état d'erreur. service.name: Vérification. Cause de la panne : le serveur fpolicy externe est terminé. »</p>	<p>1. Il est fort probable qu'un pare-feu bloque les ports nécessaires dans l'ordinateur de l'agent. Vérifier que la plage de ports 35000-55000/tcp est ouverte pour que l'ordinateur agent se connecte à partir du SVM. Assurez-vous également qu'aucun pare-feu n'est activé à partir du blocage de la communication côté ONTAP vers l'agent. 2. Tapez la commande suivante dans la zone Agent et vérifiez que la plage de ports est ouverte. <code>_Sudo iptables-save</code></p>

Problème :	Résolution :
<p>grep 3500*_ la sortie d'échantillon doit ressembler à : -A IN_public_allow -p tcp -m tcp --dport 35000 -m conntrack -ctstate NEW -j ACCEPT</p> <p>3. Connectez-vous au SVM, entrez les commandes suivantes et vérifiez qu'aucun pare-feu n'est défini pour bloquer la communication avec ONTAP. <i>service système pare-feu show services système firewall policy show</i> "Vérifiez les commandes du pare-feu"</p> <p>Côté ONTAP. 4. SSH vers le SVM/Cluster que vous souhaitez contrôler. Ping de la boîte agent depuis la lif de données du SVM (avec prise en charge des protocoles CIFS et NFS) et vérifier le fonctionnement du ping : <i>_Network ping -vserver <nom vserver> -destination <agent IP> -lif <nom LIF> -show-detail</i> si impossible d'accéder, assurez-vous que les paramètres réseau dans ONTAP sont corrects, afin que la machine agent soit pingable.</p> <p>5. si un seul SVM est ajouté deux fois à un locataire via 2 collecteurs de données, cette erreur s'affiche. 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 affiche l'état « EN COURS d'EXÉCUTION » et commence à recevoir des événements du SVM. En réalité, dans un locataire, 1 SVM ne doit être ajouté qu'une seule fois, via 1 Data Collector. 1 SVM ne doit pas être ajouté deux fois via 2 collecteurs de données.</p> <p>6. Dans les cas où le même SVM a été ajouté dans deux environnements de sécurité des charges de travail (locataires) différents, le dernier sera toujours réussir. Le second collecteur configure fpolicy avec sa propre adresse IP et commence le lancement du premier. Ainsi, le collecteur du premier arrête de recevoir des événements et son service d'audit passe en état d'erreur. Pour éviter cela, configurer chaque SVM sur un seul environnement.</p> <p>7. Cette erreur peut également se produire si les stratégies de service ne sont pas correctement configurées. Avec ONTAP 9.8 ou version ultérieure, pour se connecter au Data Source Collector, le service client Data-fpolicy est requis avec le service de données Data-nfs et/ou Data-cifs. De plus, le service data-fpolicy-client doit être associé aux lif de données pour le SVM surveillé.</p>	<p>Aucun événement n'est visible sur la page activité.</p>

Problème :	Résolution :
<p>1. Vérifier si le collecteur ONTAP est à l'état "EN FONCTIONNEMENT". Si oui, assurez-vous alors que certains événements cifs sont générés sur les machines virtuelles client cifs en ouvrant certains fichiers. 2. Si aucune activité n'est constatée, veuillez vous connecter au SVM et saisir la commande suivante. <SVM>event log show -source fpolicy Vérifiez qu'il n'y a aucune erreur liée à fpolicy. 3. Si aucune activité n'est constatée, veuillez vous connecter à la SVM. Entrez la commande suivante <SVM> fpolicy show Vérifiez si la politique fpolicy nommée avec le préfixe « cloudSecure_ » a été définie et que le statut est « on ». Si non défini, 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.</p>	<p>Le SVM Data Collector est en état d'erreur et le message d'erreur est "l'agent n'a pas pu se connecter au collecteur"</p>
<p>1. Il est fort probable que l'agent est surchargé et qu'il ne peut pas se connecter aux collecteurs de sources de données. 2. Vérifiez le nombre de collecteurs de sources de données 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 significativement élevé, installez un autre agent et déplacez certains des collecteurs de sources de données vers le nouvel agent.</p>	<p>SVM Data Collector affiche le message d'erreur comme « fpolicy.server.connectError: nœud n'a pas pu établir de connexion avec le serveur FPolicy « 12.195.15.146 » (motif : « Select Timed out ») »</p>
<p>Le pare-feu est activé au niveau du SVM/Cluster. Le moteur fpolicy ne peut donc pas se connecter au serveur fpolicy. Les interfaces de ligne de commande de ONTAP qui peuvent être utilisées pour obtenir plus d'informations sont les suivantes : journal des événements show -source fpolicy qui affiche le journal des erreurs show -source fpolicy -champs événement,action,description qui affiche plus de détails."Vérifiez les commandes du pare-feu" Côté ONTAP.</p>	<p>Message d'erreur : "le connecteur est en 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 : up) trouvée sur le SVM ».</p>
<p>Assurez-vous qu'il existe une interface opérationnelle (ayant le rôle de protocole de données et de données en tant que CIFS/NFS.</p>	<p>Le collecteur de données passe à l'état erreur, puis PASSE à l'état D'EXÉCUTION après un certain temps, puis revient à l'état erreur. Ce cycle se répète.</p>
<p>Cela se produit généralement dans le scénario suivant : 1. Plusieurs collecteurs de données sont ajoutés. 2. Les collecteurs de données qui montrent ce type de comportement auront 1 SVM ajouté à ces collecteurs de données. Signification : 2 collecteurs de données ou plus sont connectés à 1 SVM. 3. S'assurer que 1 collecteur de données se connecte à 1 seul SVM. 4. Supprimer les autres collecteurs de données qui sont connectés au même SVM.</p>	<p>Le connecteur est en état d'erreur. Nom du service : audit. Motif de l'échec : échec de la configuration (politique sur la SVM svmname. Motif : valeur non valide spécifiée pour l'élément « shres-à-inclure » dans « fpolicy.policy.scope-modifier : « fédérale »</p>

Problème :	Résolution :
Les noms des partages doivent être indiqués sans guillemets. Modifiez la configuration du SVM DSC de ONTAP pour corriger les noms de partage. <i>Inclure et exclure des partages</i> n'est pas destiné à une longue liste de noms de partage. Utilisez le filtrage par volume à la place si vous avez un grand nombre de partages à inclure ou exclure.	Il existe des fpolicies existantes dans le Cluster qui ne sont pas utilisées. Que faut-il faire avant l'installation de la sécurité des charges de travail ?
Il est recommandé de supprimer tous les paramètres fpolicy existants non utilisés même s'ils sont à l'état déconnecté. La sécurité des charges de travail crée fpolicy avec le préfixe « cloudSecure_ ». Toutes les autres configurations fpolicy non utilisées peuvent être supprimées. Commande CLI pour afficher la liste fpolicy : <i>fpolicy show</i> étapes à supprimer les configurations fpolicy : <i>fpolicy disable -vserver <svmname> -policy-name <policy_name> _fpolicy</i> <i>policy delete -vserver <svmname> -policy-name <policy_FPolicy_name> _vmname></i> <i>_vmnom_moteur_vserver__vmname></i> <i>-vserver_policy_mvmname></i> <i>-vserver_mvmnom_machine_machine_vmnom_vserv</i> <i>er_vmname></i>	Après avoir activé la sécurité des charges de travail, les performances ONTAP sont affectées : la latence devient sporadique, l'IOPS s'avère sporadique faible.
Lors de l'utilisation de ONTAP avec Workload Security, des problèmes de latence sont parfois visibles dans ONTAP. Plusieurs raisons peuvent être à l'origine de cette situation, comme indiqué dans les points suivants : " 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.	Le collecteur de données est en erreur, affiche ce message d'erreur. "Erreur : le connecteur est en état d'erreur. Nom du service : audit. Motif de l'échec : échec de la configuration de la règle sur le SVM svm_test. Motif : valeur manquante pour le champ zapi : événements. «
Commencez par un nouveau SVM avec uniquement le service NFS configuré. Ajoutez un collecteur de données SVM ONTAP dans la sécurité des charges de travail. CIFS est configuré en tant que protocole autorisé pour la SVM lors de l'ajout du SVM Data Collector de ONTAP dans Workload Security. Attendez que le collecteur de données de la sécurité de la charge de travail affiche une erreur. Étant donné que le serveur CIFS n'est PAS configuré sur le SVM, cette erreur comme indiquée sur la gauche est indiquée par Workload Security. Modifiez le collecteur de données du SVM ONTAP et décochez la case CIFS en tant que protocole autorisé. Enregistrer le collecteur de données. Il démarre alors que seul le protocole NFS est activé.	Data Collector affiche le message d'erreur : "erreur : échec de la détermination de la santé du collecteur dans 2 tentatives, essayez de redémarrer le collecteur à nouveau (Code d'erreur : AGENT008)".

Si vous rencontrez toujours des problèmes, accédez aux liens d'assistance mentionnés dans la page **aide > support**.

Configuration de Cloud Volumes ONTAP et d'Amazon FSX pour NetApp ONTAP Collector

La sécurité de la charge de travail utilise des collecteurs de données pour collecter les données d'accès des fichiers et des utilisateurs à partir de terminaux.

Configuration du stockage Cloud Volumes ONTAP

Consultez la documentation OnCommand Cloud Volumes ONTAP pour configurer une instance AWS à un seul nœud/haute disponibilité pour héberger l'agent de sécurité workloads :<https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/index.html>

Une fois la configuration terminée, suivre les étapes de configuration de votre SVM :https://docs.netapp.com/us-en/cloudinsights/task_add_collector_svm.html

Plateformes prises en charge

- Cloud Volumes ONTAP, pris en charge dans tous les fournisseurs de services cloud disponibles, là où il est disponible. Par exemple : Amazon, Azure et Google Cloud.
- ONTAP, Amazon FSX

Configuration de l'ordinateur agent

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

Vous trouverez ci-dessous les étapes d'installation d'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 la charge de travail :

Procédez comme suit pour configurer la machine à utiliser en tant qu'agent de sécurité de la charge de travail :

Étapes

1. Connectez-vous à la console AWS, accédez à la page EC2-instances et sélectionnez *Launch instance*.
2. Sélectionnez une ami RHEL ou CentOS avec la version appropriée, comme indiqué sur 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 de Cloud ONTAP.
4. Sélectionnez *t2.XLarge* (4 cpu virtuels 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 package YUM :
 - a. Installez les packages Linux natifs *wget* et *unzip*.

Installez l'agent de sécurité de la charge de travail

1. Connectez-vous en tant qu'administrateur ou responsable de compte à votre environnement Cloud 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 installation de l'agent.
5. Collez la commande installation de l'agent dans l'instance RHEL EC2 à laquelle vous êtes connecté. Cela installe l'agent de sécurité de la charge de travail, fournissant ainsi tous les "Conditions préalables de l'agent" sont satisfaits.

Pour plus de détails, consultez le lien suivant : 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	Solution
L'erreur "sécurité de la charge de travail : échec de la détermination du type de ONTAP pour le collecteur de données Amazon FSxN" est indiquée par le Data Collector. Le client ne peut pas ajouter un nouveau collecteur de données Amazon FSxN à la sécurité de la charge de travail. La connexion au cluster FSxN sur le port 443 de l'agent est en cours de temporisation. Les règles requises sont activées pour permettre la communication entre le pare-feu et les groupes de sécurité AWS. Un agent est déjà déployé et se trouve également dans le même compte AWS. Ce même agent est utilisé pour connecter et surveiller les dispositifs NetApp restants (et tous fonctionnent).	Résoudre ce problème en ajoutant le segment réseau LIF fsxadmin à la règle de sécurité de l'agent. Autorisé tous les ports si vous n'êtes pas sûr des ports.

Gestion des utilisateurs

Les comptes utilisateurs de la sécurité des charges de travail sont gérés via Cloud Insights.

Cloud Insights fournit quatre niveaux de compte utilisateur : propriétaire, administrateur, utilisateur et invité du compte. Chaque compte se voit attribuer 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 charge de travail suivants :

Rôle	Accès à la sécurité du workload
Administrateur	Peut exécuter toutes les fonctions de sécurité de la charge de travail, y compris celles pour les alertes, les analyses approfondies, les collecteurs de données, les stratégies de réponse automatisées et les API pour la sécurité de la charge de travail. Un administrateur peut également inviter d'autres utilisateurs, mais peut uniquement attribuer des rôles de sécurité de la charge de travail.

Utilisateur	Peut afficher et gérer des alertes et afficher des informations judiciaires. Le rôle de l'utilisateur peut modifier l'état des alertes, ajouter une note, effectuer des instantanés manuellement et limiter l'accès des utilisateurs.
Invité	Peut afficher les alertes et les analyses approfondies. Le rôle invité ne peut pas modifier le statut des alertes, ajouter une note, effectuer des instantanés manuellement ou restreindre l'accès des utilisateurs.

Étapes

1. Connectez-vous à la sécurité des charges de travail
2. Dans le menu, cliquez sur **Admin > gestion des utilisateurs**

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

3. Sélectionnez le rôle souhaité pour chaque utilisateur.

Lors de l'ajout d'un nouvel utilisateur, il suffit de sélectionner le rôle souhaité (généralement utilisateur ou invité).

Vous trouverez plus d'informations sur les comptes utilisateur et les rôles dans le Cloud Insights ["Rôle utilisateur"](#) documentation :

Vérificateur de taux d'événements SVM (Guide de dimensionnement des agents)

Le vérificateur de taux d'événement est utilisé pour vérifier le taux d'événement combiné NFS/SMB au sein du SVM avant d'installer un collecteur de données SVM ONTAP, afin de voir le nombre de SVM qu'un ordinateur Agent peut surveiller. Utilisez le vérificateur de taux d'événements comme guide de dimensionnement pour vous aider à planifier votre environnement de sécurité.

Un agent peut prendre en charge jusqu'à 50 collecteurs de données.

Besoins :

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



Lors de l'exécution de ce script, aucun SVM Data Collector de ONTAP ne doit s'exécuter pour le SVM pour lequel le taux d'événement est déterminé.

Étapes :

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 l'installation de `_sshpass_` 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
```

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

```
"Svm svm_rate is generating 100 events/sec".
```

Chaque SVM Data Collector de ONTAP peut être associé à un seul SVM, ce qui signifie que chaque collecteur de données sera en mesure de recevoir le nombre d'événements qu'un seul SVM génère.

Gardez à l'esprit les éléments suivants :

A) utilisez ce tableau comme guide de dimensionnement général. 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 l'ordinateur agent	Nombre de collecteurs de données SVM	Taux d'évènement maximal que l'Agent machine peut traiter
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 total de vos événements, ajoutez les événements générés pour tous les SVM pour 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 un tampon de taux d'évènement de 30 %.

B + C doit être inférieur À A, sinon la machine Agent ne sera pas en mesure de surveiller.

En d'autres termes, le nombre de collecteurs de données pouvant 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 la xref:{relative_path}concept_cs_agent_requirements.html["Exigences de l'agent"] pour connaître les conditions préalables et les conditions requises supplémentaires.

Exemple

Disons que nous avons trois SVM générant des taux d'événements de 100, 200 et 300 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_<nom du SVM>.log* dans le répertoire de travail actuel.

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

- Des identifiants, IP ou nom de SVM incorrects sont fournis.
- un serveur fpolicy existant avec le même nom, numéro de séquence, etc. Fournit une erreur.
- Le script s'arrête brusquement en cours d'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	Réponse
----------	---------

Si je exécute ce script sur un SVM déjà configuré pour Workload Security, utilise-t-il simplement la configuration fpolicy existante sur le SVM ou configure-t-il une configuration temporaire et exécute-t-il le processus ?	L'Event Rate Checker peut s'exécuter correctement, même pour un SVM déjà configuré pour Workload Security. Il ne devrait y avoir aucun impact.
Puis-je augmenter le nombre de SVM sur lesquels le script peut être exécuté ?	Oui. Il vous suffit de modifier le script et de changer le nombre max de SVM de 5 à n'importe quel nombre souhaitable.
Si j'augmente le nombre de SVM, augmente-t-il le temps d'exécution du script ?	Non Le script s'exécute pendant 5 minutes au 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 changer le nombre max de SVM de 5 à n'importe quel nombre souhaitable.
Si j'augmente le nombre de SVM, augmente-t-il le temps d'exécution du script ?	Non Le script s'exécute pendant 5 min au maximum, même si le nombre de SVM est augmenté.
Que se passe-t-il si j'exécute Event Rate Checker avec un agent existant ?	L'exécution d'Event Rate Checker sur un agent existant peut entraîner une augmentation de la latence sur le SVM. Cette augmentation sera temporaire pendant l'exécution du vérificateur de taux d'événement.

Alertes

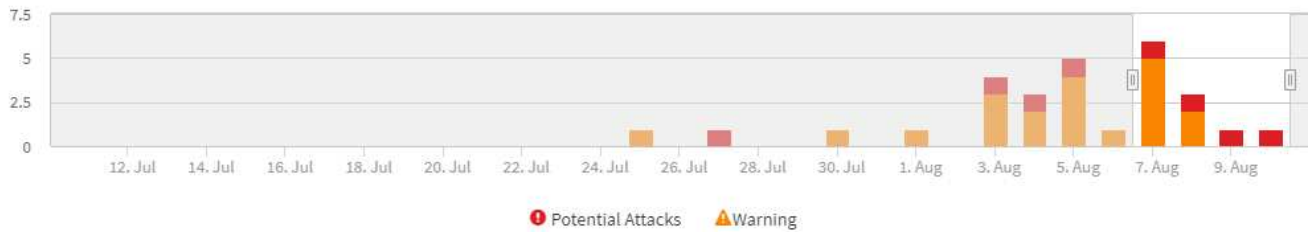
La page alertes de sécurité de la charge de travail affiche un calendrier des attaques et/ou avertissements récents et vous permet d'afficher les détails de chaque problème.



La sécurité des charges de travail n'est pas disponible dans l'édition fédérale de Cloud Insights.



Filter By Status New



⚠ Potential Attacks (3)

Potential Attacks	Detected ↓	Status	User	Evidence	Action Taken
Ransomware Attack	5 hours ago Aug 10, 2020 4:38 AM	New	Iris McIntosh	> 700 Files Encrypted	Snapshots Taken
Ransomware Attack	a day ago Aug 9, 2020 3:51 AM	New	Christy Santos	> 500 Files Encrypted	Snapshots Taken
Ransomware Attack	2 days ago Aug 8, 2020 4:29 AM	New	Safwan Langley	> 700 Files Encrypted	Snapshots Taken

⚠ Warnings (7)

Abnormal Behaviour	Detected ↓	Status	User	Change	Action Taken
User Activity Rate	2 days ago Aug 8, 2020 7:49 PM	New	Iris McIntosh	↑ 192.46%	None
User Activity Rate	2 days ago Aug 8, 2020 7:32 PM	New	Jenny Bryan	↑ 73.64%	None
User Activity Rate	3 days ago Aug 7, 2020 8:07 PM	New	Szymon Owen	↑ 189.88%	None

Alerte

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

Pour chaque alerte, les éléments suivants s'affichent :

Attaques potentielles:

- Le type *attaque potentielle* (par exemple, ransomware ou sabotage)
- Date et heure de l'attaque potentielle *Detected*
- Le *Status* de l'alerte :
 - **Nouveau** : il s'agit de la valeur par défaut pour les nouvelles alertes.
 - **En cours** : l'alerte est en cours d'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 comme un comportement faux positif ou attendu.

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

A modal dialog box titled "Change Status To". It contains a dropdown menu with "In Progress" selected. Below the dropdown is a section titled "Add a Note" with a text input field containing the placeholder text "Enter notes or updates here". At the bottom of the dialog are two buttons: "Cancel" and "Save".

- Le *User* dont le comportement a déclenché l'alerte
- *Evidence* de l'attaque (par exemple, un grand nombre de fichiers ont été cryptés)
- La *action entreprise* (par exemple, un instantané a été créé)

Avertissements:

- Le *comportement anormal* qui a déclenché l'avertissement
- La date et l'heure auxquelles le comportement a été *déecté*
- Le *Status* de l'alerte (Nouveau, en cours, etc.)
- Le *User* dont le comportement a déclenché l'alerte
- Une description de *change* (par exemple, une augmentation anormale de l'accès aux fichiers)
- La *action entreprise*

Options de filtre

Vous pouvez filtrer les alertes en procédant comme suit :

- Le *Status* de l'alerte
- Texte spécifique dans la *Note*
- Type de *attaques/Avertissements*
- Le *User* 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 en fonction du type d'attaque ou d'alerte. Par exemple, une page

de détails sur les attaques par ransomware peut afficher les informations suivantes :

Section Récapitulatif :

- Type d'attaque (ransomware, sabotage) et ID d'alerte (attribué par la sécurité de la charge de travail)
- Date et heure de détection de l'attaque
- Action entreprise (par exemple, un instantané automatique a été effectué. L'heure de l'instantané s'affiche immédiatement sous la section récapitulative)
- État (Nouveau, en cours, etc.)

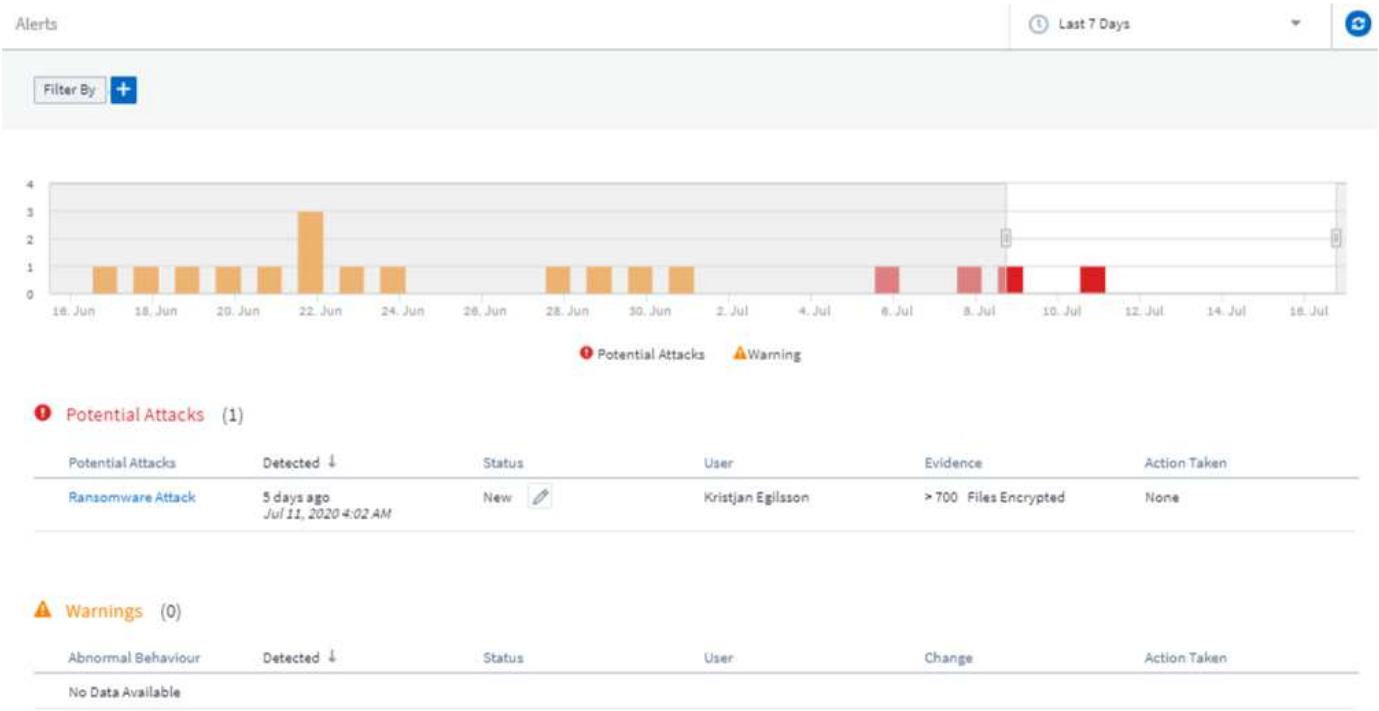
Section des résultats d'attaque :

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

Section utilisateurs associés :

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

Page alertes (cet exemple montre une attaque par ransomware potentielle)
:



Page détaillée (cet exemple montre une attaque par ransomware potentielle)
:



POTENTIAL ATTACK: AL_305
Ransomware Attack

Detected
5 days ago
Jul 11, 2020 4:02 AM

Action Taken
None

Status
New

Total Attack Results

1	0	4173
Affected Volumes	Deleted Files	Encrypted Files

4173 Files have been copied, deleted, and potentially encrypted by 1 user account.

This is potentially a sign of ransomware attack.
The extension "crypt" was added to each file.

Encrypted Files

Activity per minute



Related Users



Kristjan Egilsson
Accountant
Finance

4173
Encrypted Files

Detected
5 days ago
Jul 11, 2020 4:02 AM

Action Taken
None



Username
us035

Email
Egilsson@netapp.com

Phone
387224312607

Department
Finance

Manager
Lyndsey Maddox

Top Activity Types

Activity per minute
Last access location: 10.197.144.115

[View Activity Detail](#)



Prendre une action instantané

La sécurité des charges de travail protège vos données en prenant automatiquement un instantané en cas de détection d'une activité malveillante, ce qui garantit la sauvegarde sécurisée de vos données.

Vous pouvez définir "[stratégies de réponse automatisées](#)" cette opération prend un snapshot en cas d'attaque par ransomware ou d'autre activité anormale de l'utilisateur. Vous pouvez également prendre un instantané manuellement à partir de la page d'alerte.

Cliché automatique pris

:

Potential Attack Detail / Ransomware Attack

Jul 26, 2020
2:38 AM - 5:38 AM

POTENTIAL ATTACK: AL_307
Ransomware Attack

Detected
4 days ago
Jul 26, 2020 3:38 AM

Action Taken
Snapshots Taken

Status
In Progress

Last snapshots taken by
Amit Schwartz
Jul 30, 2020 2:54 PM

How To:
[Restore Entities](#)

Re-Take Snapshots

Total Attack Results

1
Affected Volumes

0
Deleted Files

5148
Encrypted Files

5148 Files have been copied, deleted, and potentially encrypted by 1 user account.

This is potentially a sign of ransomware attack.
The extension "crypt" was added to each file.

Encrypted Files
Activity per minute

Related Users

Ewen Hall
Developer Engineering

5148
Encrypted Files

Detected
4 days ago
Jul 26, 2020 3:38 AM

Action Taken
Snapshots Taken

Instantané manuel

Cloud Insights

Abhi Basu Thakur

MONITOR & OPTIMIZE

Alerts / **Nabilah Howell** had an abnormal change in activity rate

Jul 23, 2020 - Jul 26, 2020
1:44 AM - 1:44 AM

CLOUD SECURE

ALERTS

FORENSICS

ADMIN

HELP

WARNING: AL_306
Nabilah Howell had an abnormal change in activity rate.

Detected
5 days ago
Jul 25, 2020 1:44 PM

Action Taken
None

Status
New

Recommendation: Setup an Automated Response Policy
An Automated Response Policy will trigger measures to contain the damage automatically when a future attack is detected. Try it now.

Take Snapshots

How To:
[Restore Entities](#)

Nabilah Howell's Activity Rate Change

Typical
122.8
Activities Per Minute

Alert
210
Activities Per Minute

↑ 71%

Nabilah Howell's activity rate grew 71% over their typical average.

Activity Rate
Activity per 5 minutes

Notifications d'alerte

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

Stratégie de conservation

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

mois seront supprimés. Si l'environnement de sécurité de la charge de travail est supprimé, toutes les données associées à l'environnement sont également supprimées.

Dépannage

Problème :	Essayer :
Dans certains cas, ONTAP effectue des copies Snapshot par jour toutes les heures. Les snapshots de sécurité des workloads (WS) l'affecteront-ils ? Le snapshot de la station de travail prend-il la place du snapshot horaire ? Le snapshot horaire par défaut sera-t-il arrêté ?	Les snapshots de sécurité de la charge de travail n'affectent pas les snapshots horaires. Les instantanés WS ne prennent pas l'espace horaire de snapshot et doivent continuer comme précédemment. Le snapshot horaire par défaut n'est 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 échoue et la sécurité de la charge de travail affiche un message d'erreur signalant que le snapshot est plein. L'utilisateur doit définir des règles de snapshot pour supprimer les snapshots les plus anciens, sinon les snapshots ne seront pas effectués. Dans ONTAP 9.3 et versions antérieures, un volume peut contenir jusqu'à 255 copies Snapshot. Dans ONTAP 9.4 et versions ultérieures, un volume peut contenir jusqu'à 1023 copies Snapshot. Pour plus d'informations, consultez la documentation ONTAP sur " Définition de la règle de suppression Snapshot ".
La sécurité de la charge de travail ne peut pas prendre de snapshots du tout.	Assurez-vous que le rôle utilisé pour créer des instantanés dispose de lien : proper droits affectés . Assurez-vous que <i>csrole</i> est créé avec les droits d'accès appropriés pour la prise de snapshots : Security login role create -vserver <vservename> -role csrole -cmddirname « volume snapshot » -Access All
Les snapshots échouent pour les alertes plus anciennes sur les SVM qui ont été supprimées de la sécurité des charges de travail, puis rajoutées à nouveau. Pour les nouvelles alertes qui se produisent après l'ajout d'un SVM, des snapshots sont réalisés.	Ce scénario est rare. Si vous rencontrez ce problème, connectez-vous à ONTAP et prenez manuellement les snapshots pour les anciennes alertes.
Dans la page <i>Alert Details</i> , le message "Last tentative failed" (dernière tentative échouée) s'affiche sous le bouton <i>prendre snapshot</i> . Lorsque vous passez la souris sur l'erreur, "la commande Invoke API a expiré pour le collecteur de données avec ID" s'affiche.	Cela peut se produire lorsqu'un collecteur de données est ajouté à la sécurité de la charge de travail via SVM Management IP, si le LIF du SVM est dans <i>Disabled</i> state dans ONTAP. Activez la LIF particulière dans ONTAP et déclenchez <i>Take snapshot manuellement</i> à partir de la sécurité des charges de travail. L'action Snapshot va alors réussir.

Médecine légale

Analyse - toute l'activité

La page toutes les activités vous aide à comprendre les actions effectuées sur les entités de l'environnement de sécurité de la charge de travail.

Examen de toutes les données d'activité

Cliquez sur **Forensics > activité Forensics** et cliquez sur l'onglet **toutes les activités** pour accéder à la page toutes les activités. Cette page présente les activités de votre environnement et présente les informations suivantes :

- Graphique indiquant *Historique des activités* (accessible par minute/par 5 minutes/10 minutes en fonction de 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 de temps agrandie. Lorsque vous effectuez un zoom avant, un bouton s'affiche pour permettre à l'utilisateur d'effectuer un zoom arrière.

- Un graphique de *types d'activités*. Pour obtenir les données de l'historique d'activité par type d'activité, cliquez sur le lien du libellé de l'axe X correspondant.
- Un graphique d'activité sur *types d'entité*. Pour obtenir les données de l'historique d'activité par type d'entité, cliquez sur le lien du libellé de l'axe X correspondant.
- Une liste des données *All Activity*

Le tableau **toutes les activités** indique 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 « vitesse »



- Le **temps** où une entité a été consultée, y compris l'année, le mois, le jour et l'heure du dernier accès.
- Le **utilisateur** qui a accédé à l'entité avec un lien vers le "[Informations utilisateur](#)".
- L'activité * réalisée par l'utilisateur. Les types pris en charge sont les suivants :
 - **Changer la propriété du groupe** - la propriété du groupe est de fichier ou de dossier est modifiée. Pour plus de détails sur la propriété du groupe, reportez-vous à la section "[ce lien](#)."
 - **Changer propriétaire** - la propriété du fichier ou du dossier est remplacée par un autre utilisateur.
 - **Modifier l'autorisation** - l'autorisation de fichier ou de dossier est modifiée.
 - **Créer** - Créer un fichier ou un dossier.
 - **Supprimer** - Supprimer le fichier ou le dossier. Si un dossier est supprimé, *delete* events sont obtenus pour tous les fichiers de ce dossier et de ces sous-dossiers.
 - **Lire** - le fichier est lu.
 - **Read Metadata** - uniquement sur l'activation de l'option de surveillance de dossier. 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.
 - **Ecrire** - les données sont écrites dans un fichier.
 - **Write Metadata** - les métadonnées de fichier sont écrites, par exemple, les autorisations modifiées.
 - **Autre changement** - tout autre événement qui n'est pas décrit ci-dessus. Tous les événements non mappés sont mappés au type d'activité "autre changement". Applicable aux fichiers et dossiers.

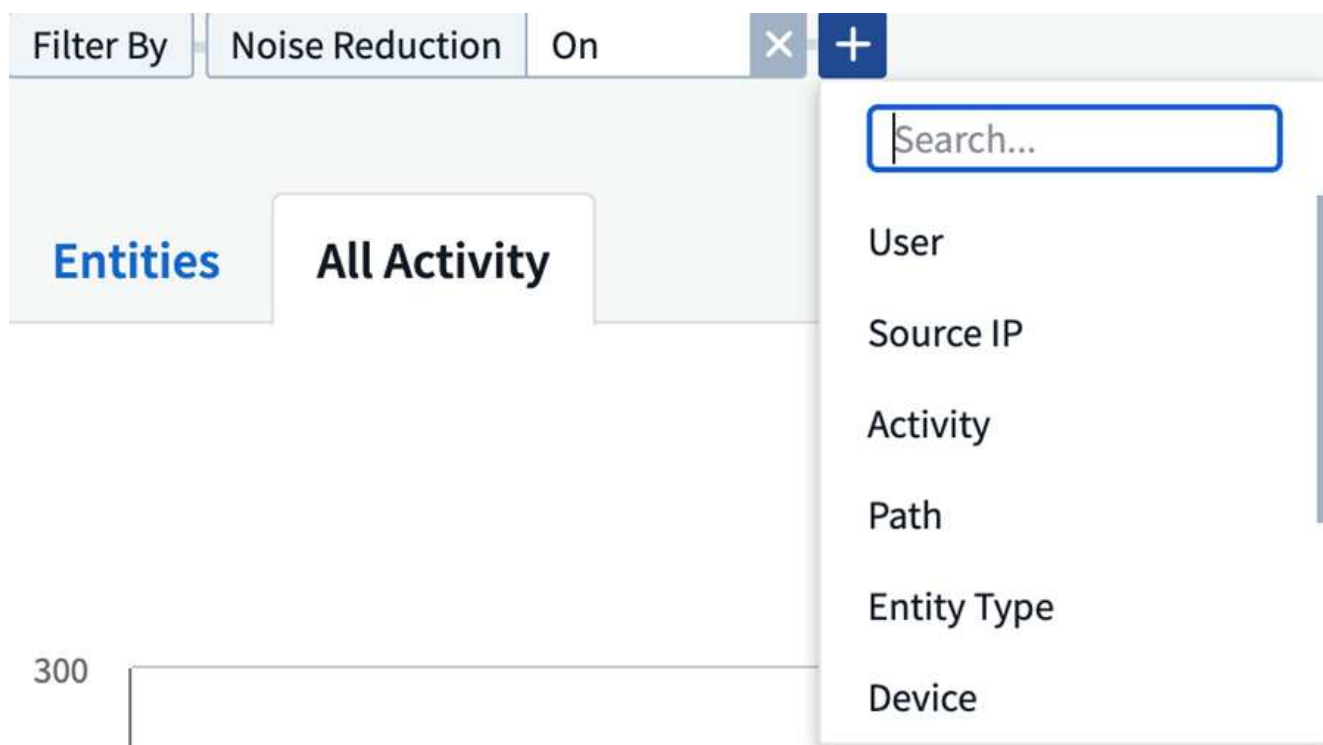
- Le **chemin** vers l'entité avec un lien vers le "[Données de détail d'entité](#)"
- Le **Type d'entité**, y compris l'extension d'entité (c.-à-d. fichier) (.doc, .docx, .tmp, etc.)
- Le **périphérique** où résident les entités
- Le **Protocole** utilisé pour récupérer des événements.
- Le **chemin d'origine** utilisé pour renommer les événements lorsque le fichier d'origine a été renommé. Par défaut, cette colonne n'est pas visible dans le tableau. Utilisez le sélecteur de colonne pour ajouter cette colonne à la table.
- Le **Volume** où résident les entités. Par défaut, cette colonne n'est pas visible dans le tableau. Utilisez le sélecteur de colonne pour ajouter cette colonne à la table.

Filtrage des données d'historique d'activité Forensic

Vous pouvez utiliser deux méthodes pour filtrer les données.

1. Placez le pointeur de la souris sur le champ du tableau et cliquez sur l'icône de filtre qui s'affiche. La valeur est ajoutée aux filtres appropriés dans la liste *Filter by* supérieure.
2. Filtrez les données en entrant dans le champ *Filter by* :

Sélectionnez le filtre approprié dans le widget filtre par en haut 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 Forensic en utilisant les champs suivants :

- Le type **activité**.
- **Source IP** à partir de laquelle l'entité a été accédée. Vous devez fournir une adresse IP source valide en

guillemets doubles, par exemple "10.1.1.1." Les adresses IP incomplètes telles que "10.1.1.", "**10.1..***", etc. Ne fonctionneront pas.

- **Protocole** pour extraire des activités spécifiques au protocole.
- **Nom d'utilisateur** de l'utilisateur effectuant l'activité. Vous devez fournir le nom d'utilisateur exact pour 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 par l'utilisateur au cours des 2 dernières heures. Il est également utilisé pour filtrer les fichiers temporaires (par exemple, les fichiers .tmp) auxquels l'utilisateur a accès.

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

- **Type d'entité**, utilisant l'extension d'entité (fichier)
- **Chemin** de l'entité
- **Utilisateur** exécutant l'activité
- **Périphérique** (SVM) où résident les entités
- **Volume** où résident les entités
- Le **chemin d'origine** utilisé pour renommer les événements lorsque le fichier d'origine a été renommé.

Les champs précédents sont soumis aux éléments suivants lors du filtrage :

- La valeur exacte doit se trouver dans les guillemets : exemple : « searchtext »
- Les chaînes de caractères génériques ne doivent pas contenir de guillemets : par exemple : searchtext, *searchtext*, filtrera les chaînes contenant 'contour d'oreille'.
- Chaîne avec un préfixe, par exemple : searchtext* , recherchera toutes les chaînes commençant par 'contour d'oreille'.

Tri des données d'historique d'activité Forensic

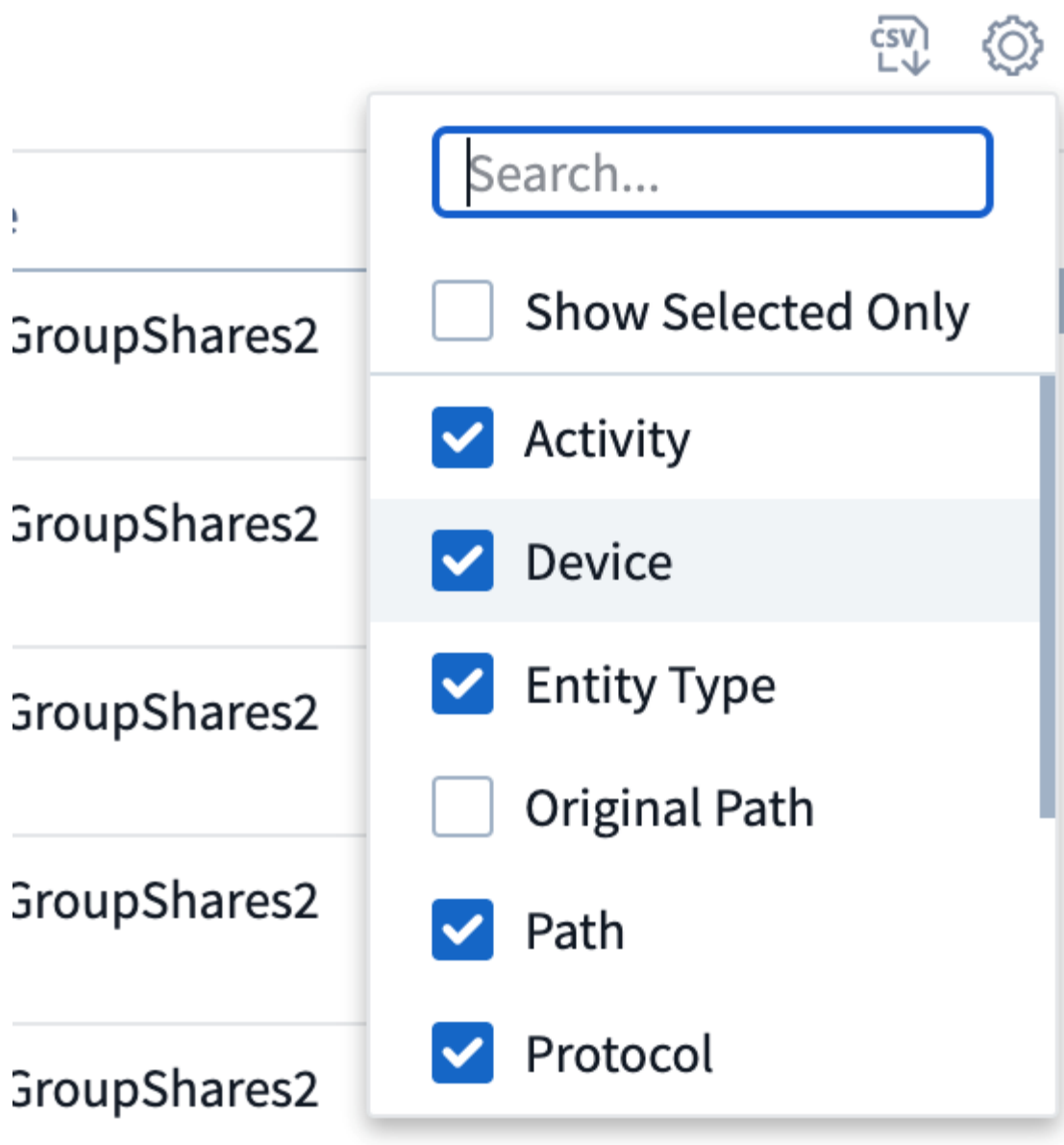
Vous pouvez trier les données de l'historique d'activité par *Time*, *User*, *Source IP*, *Activity*, *Path* et *Entity Type*. Par défaut, la table est triée par ordre décroissant *time*, ce qui signifie que les dernières données seront affichées en premier. Le tri est désactivé pour les champs *Device* et *Protocol*.

Exportation de toute l'activité

Vous pouvez exporter l'historique des activités dans un fichier .CSV en cliquant sur le bouton *Export* au-dessus de la table Historique des activités. Notez que seuls les 100,000 premiers enregistrements sont exportés. Selon la quantité de données, l'exportation peut prendre de quelques secondes à plusieurs minutes.

Sélection de colonne pour toutes les activités

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



Conservation de l'historique des activités

L'historique des activités est conservé pendant 13 mois pour les environnements de sécurité active de la charge de travail.

Applicabilité des filtres dans la page Forensics

Filtre	Ce qu'il fait	Exemple	Quels filtres s'appliquent ?	Non applicable pour quels filtres	Résultat
* (Astérisque)	permet de rechercher tout	Auto*03172022	Utilisateur, CHEMIN, Type d'entité, Type de périphérique, Volume, Chemin d'origine		Renvoie toutes les ressources commençant par "Auto" et se terminant par "03172022"

? (point d'interrogation)	permet de rechercher un nombre spécifique de caractères	AutoSabotageUser1_03172022 ?	Utilisateur, Type d'entité, périphérique, volume		Renvoie AutoSabotageUser1_03172022A, AutoSabotageUser1_03172022AB, AutoSabotageUser1_031720225, etc
OU	vous permet de spécifier plusieurs entités	AutoSalotageUser1_03172022 OU AutoRansomUser4_03162022	Utilisateur, domaine, Nom d'utilisateur, CHEMIN, Type d'entité, Périphérique, chemin d'origine		Renvoie AutoSalotageUser1_03172022 OU AutoRansomUser4_03162022
PAS	permet d'exclure du texte des résultats de la recherche	PAS AutoRansomUser4_03162022	Utilisateur, domaine, Nom d'utilisateur, CHEMIN, Type d'entité, CHEMIN d'origine, Volume	Périphérique	Renvoie tout ce qui ne commence pas par "AutoRansomUser4_03162022"
Aucune	Recherche les valeurs NULL dans tous les champs	Aucune	Domaine		renvoie les résultats où le champ cible est vide

Chemin d'accès / chemin d'origine recherche

Les résultats de la recherche avec et sans / seront différents

/AutoDir1/AutoFile	Fonctionne
AutoDir1/AutoFile	Ne fonctionne pas
/AutoDir1/AutoFile (Dir1)	Dir1 la sous-chaîne partielle ne fonctionne pas
"/AutoDir1/AutoFile03242022"	La recherche exacte fonctionne
Auto*03242022	Ne fonctionne pas
AutoSabotageUser1_03172022 ?	Ne fonctionne pas
/AutoDir1/AutoFile03242022 OU /AutoDir1/AutoFile03242022	Fonctionne
NON /AutoDir1/AutoFile03242022	Fonctionne
NON /AutoDir1	Fonctionne
NON /AutoFile03242022	Ne fonctionne pas
*	Affiche toutes les entrées

Dépannage

Problème	Essayez
Dans la table “toutes les activités”, sous la colonne ‘utilisateur’, le nom d’utilisateur est indiqué comme suit : “ldap:HQ.COMPANYNAME.COM:S-1-5-21-3577637-1906459482-1437260136-1831817” ou “ldap:Default:80038003”	<p>Raisons possibles :</p> <ol style="list-style-type: none">1. Aucun groupe de répertoires d'utilisateurs n'a encore été configuré. Pour en ajouter un, accédez à Workload Security > Collectors > User Directory Collectors et cliquez sur +User Directory Collector. Choisissez <i>Active Directory</i> ou <i>LDAP Directory Server</i>.2. Un collecteur d'annuaire d'utilisateurs a été configuré, mais il s'est arrêté ou est à l'état d'erreur. Accédez à collecteurs > collecteurs d'annuaire d'utilisateurs et vérifiez l'état. Reportez-vous à la "Dépannage de l'utilisateur Directory Collector" section de la documentation pour des conseils de dépannage. <p>Après la configuration correcte, le nom sera automatiquement résolu dans les 24 heures. Si elle n'est toujours pas résolue, vérifiez si vous avez ajouté le collecteur de données utilisateur approprié. Assurez-vous que l'utilisateur fait bien partie du serveur Active Directory/LDAP d'annuaire ajouté.</p>
Certains événements NFS n'apparaissent pas dans l'interface utilisateur.	<p>Vérifier ce qui suit :</p> <ol style="list-style-type: none">1. Un collecteur d'annuaire utilisateur pour serveur AD avec un jeu d'attributs POSIX doit être exécuté avec l'attribut unixid activé à partir de l'interface utilisateur.2. Tout utilisateur effectuant un accès NFS doit s'afficher lorsqu'il recherche dans la page utilisateur à partir de l'interface utilisateur.3. Les événements bruts (événements pour lesquels l'utilisateur n'est pas encore découvert) ne sont pas pris en charge par NFS.4. L'accès anonyme à l'exportation NFS ne sera pas surveillé.5. S'assurer que la version NFS est utilisée dans un niveau inférieur à NFS4.1.

Après avoir saisi des lettres contenant un caractère générique comme l'astérisque (*) dans les filtres des pages Forensics <i>All Activity</i> ou <i>Entités</i> , les pages se chargent très lentement.	<p>Un astérisque (*) dans la chaîne de recherche recherche tout. Cependant, les chaînes de caractères génériques comme <i>*<searchTerm></i> ou <i>*<searchTerm>*</i> entraînent une requête lente. Pour obtenir de meilleures performances, utilisez plutôt des chaînes de préfixe, au format <i><searchTerm>*</i> (en d'autres termes, ajoutez l'astérisque (*) <i>après</i> un terme de recherche). Exemple : utilisez la chaîne <i>testvolume*</i>, plutôt que <i>*testvolume</i> ou <i>*test*volume</i>.</p> <p>Utilisez une recherche basée sur des préfixes pour voir toutes les activités sous un dossier donné de manière récursive (recherche hiérarchique). par exemple <i>/path1/path2/path3</i> ou <i>"/path1/path2/path3"</i> répertoriera toutes les activités récursivement sous <i>/path1/path2/path3</i>. Vous pouvez également utiliser l'option « Ajouter au filtre » sous l'onglet toutes les activités.</p>
J'ai rencontré une erreur « Echec de la demande 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.

Page entités judiciaires

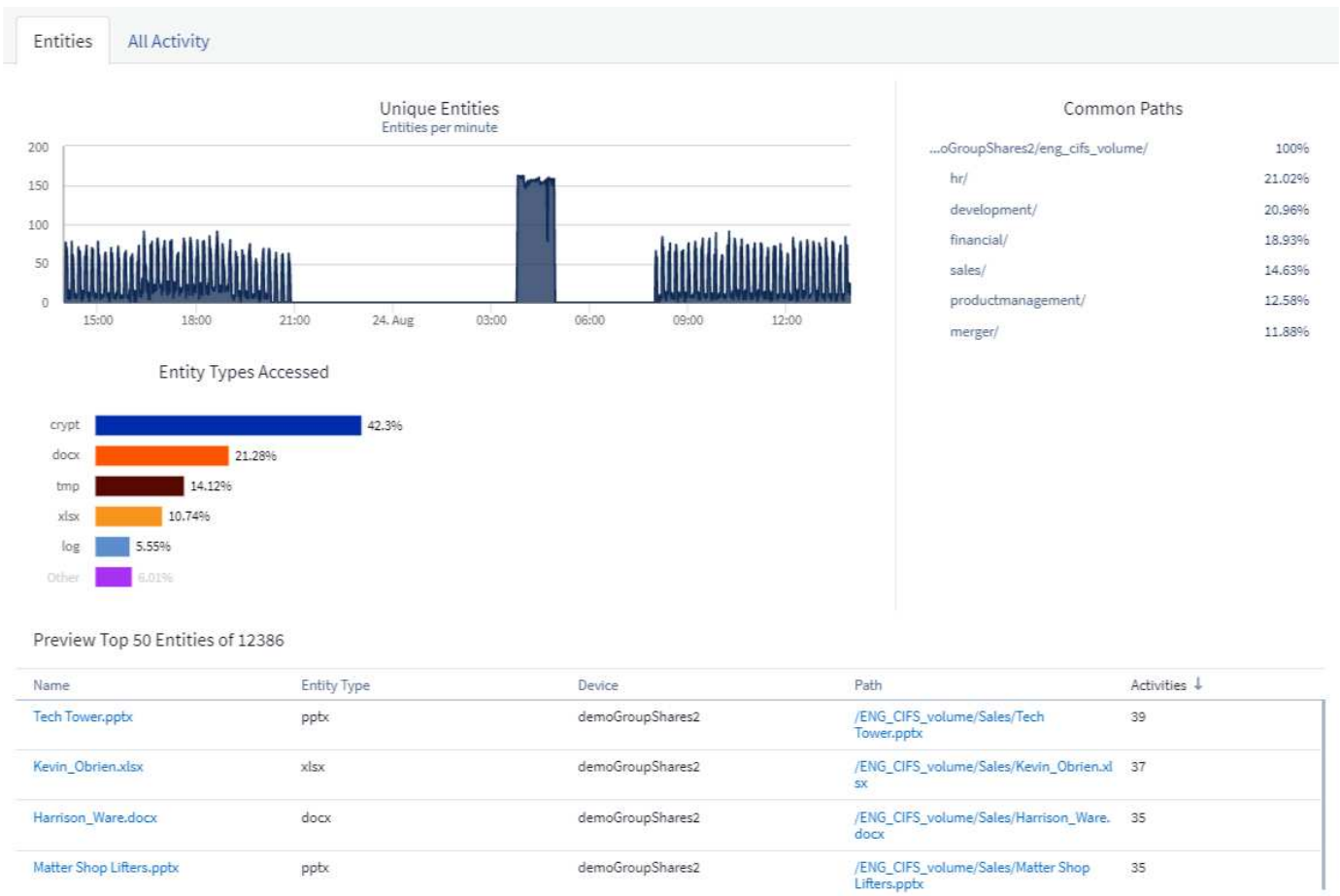
La page entités judiciaires fournit des informations détaillées sur l'activité de l'entité dans votre environnement.

Examen des informations sur l'entité

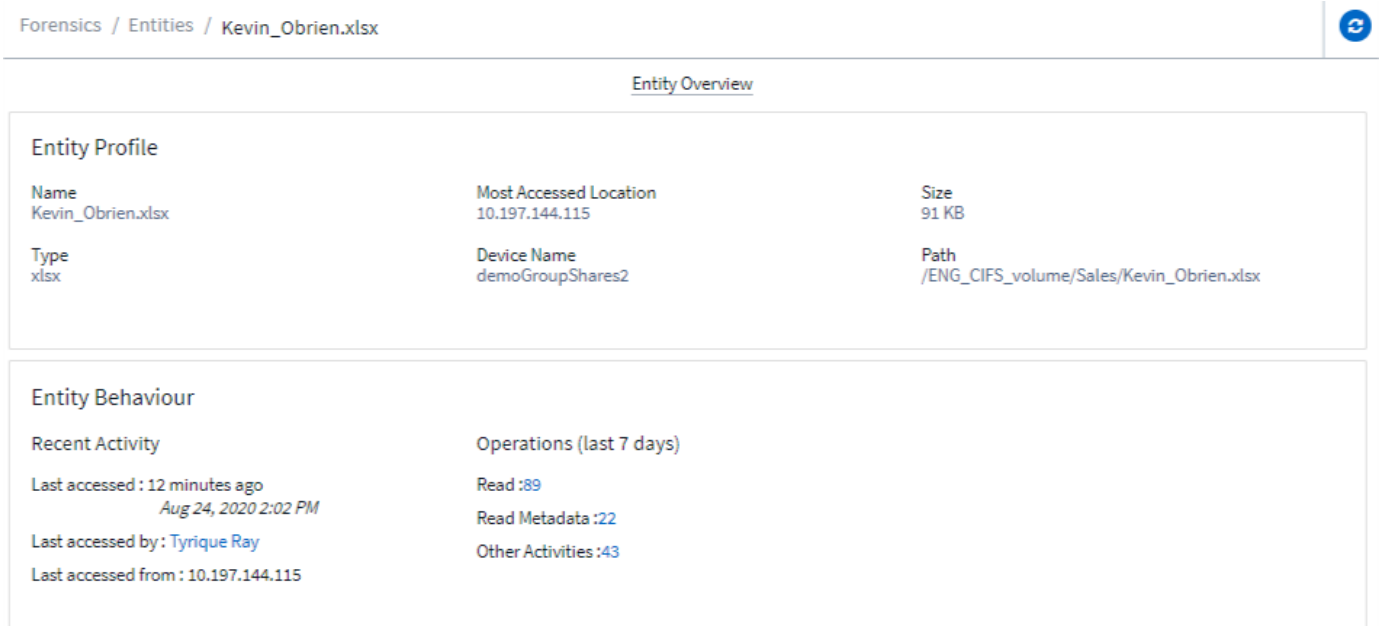
Cliquez sur **Forensics > activités médico-légales** et cliquez sur l'onglet *entités* pour accéder à la page entités.

Cette page présente l'activité de l'entité dans votre environnement, en soulignant les informations suivantes : *

- Un graphique montrant *unique entités* accédées par minute
- * Un graphique de *types d'entités accédées*
- * Une ventilation des *chemins communs*
- * Une liste des *50 principales entités* sur le nombre total d'entités



Un clic sur une entité dans la liste ouvre une page de présentation pour l'entité, affichant un profil de l'entité avec des détails tels que le nom, le type, le nom du périphérique, l'adresse IP la plus utilisée et le chemin d'accès, ainsi que le comportement de l'entité comme l'utilisateur, l'adresse IP, et heure du dernier accès à l'entité.



Vue d'ensemble de l'utilisateur judiciaire

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 électronique de l'utilisateur
- Responsable de l'utilisateur
- Contact téléphonique de l'utilisateur
- Emplacement 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.

Stratégie de conservation

S'il n'est pas actualisé à nouveau, la liste des utilisateurs est conservée pendant 13 mois. Au bout de 13 mois, les données seront supprimées. Si votre environnement de sécurité des workloads est supprimé, toutes les données associées à l'environnement sont supprimées.

Stratégies de réponse automatisées

Les stratégies de réponse déclenchent des actions telles que la prise d'un instantané ou la restriction de l'accès de l'utilisateur en cas d'attaque ou de comportement anormal de l'utilisateur.



La sécurité des charges de travail n'est pas disponible dans l'édition fédérale de Cloud Insights.

Vous pouvez définir des stratégies sur des périphériques spécifiques ou sur tous les périphériques. Pour définir une stratégie de réponse, sélectionnez **Admin > Automated Response Policies** et cliquez sur le

bouton **+Policy** approprié. Vous pouvez créer des stratégies pour les attaques ou les avertissements.

Add Attack Policy

Policy Name*

Unique New Policy Name

For Attack Type(s) *

☐ Ransomware Attack

☐ Data Destruction - File Deletion

On Device

All Devices

+ Another Device

Actions

☒ Take Snapshot ?

☐ Block User File Access ?

Time Period

12 hours

Cancel Save

Vous devez enregistrer la police avec un nom unique.

Pour désactiver une action de réponse automatisée (par exemple, prendre un instantané), il suffit d'annuler l'action et d'enregistrer la stratégie.


Lorsqu'une alerte est déclenchée par rapport aux périphériques spécifiés (ou à tous les périphériques, si elle est sélectionnée), la stratégie de réponse automatique prend un instantané de vos données. Vous pouvez voir l'état des snapshots sur le ["Page de détails de l'alerte"](#).

Voir la ["Limiter l'accès des utilisateurs"](#) Pour plus d'informations sur la restriction de l'accès des utilisateurs par IP.

Vous pouvez modifier ou interrompre une stratégie de réponse automatique en sélectionnant l'option dans le menu déroulant de la stratégie.

Le service de sécurité des charges de travail supprime automatiquement les snapshots une fois par jour en fonction des paramètres de suppression de Snapshot.

Snapshot Purge Settings



Define purge periods to automatically delete snapshots taken by Cloud Secure.

Attack Automated Response

Delete Snapshot after 30 Days ▼

Warning Automated Response

Delete Snapshot after 7 Days ▼

User Created

Delete Snapshot after 30 Days ▼


CancelSave

Stratégies de types de fichiers autorisées

Si une attaque par ransomware 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 *allowed file types* pour éviter des alertes inutiles.

Accédez à **Workload Security > Politiques** et allez à l'onglet *Allowed File Type Policies*.

Allowed File Types Policies

Ransomware alerts will not be triggered for the following file types: 

.abc X

.123 X

*.safe X

Une fois ajoutée à la liste *allowed file types* list, aucune alerte d'attaque par ransomware ne sera générée pour ce type de fichier autorisé. Notez que la règle *allowed File types* ne s'applique qu'à la détection des ransomware.

Par exemple, si un fichier nommé *test.txt* est renommé *test.txt.abc* et que Workload Security détecte une attaque par ransomware en raison de l'extension *.abc*, l'extension *.abc* peut être ajoutée à la liste *allowed file types* list. Après leur ajout à cette liste, les attaques par ransomware ne seront plus générées contre les fichiers portant 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 des types ".a*c", ".p*f" ne sont pas prises en charge.

Intégration avec la protection ONTAP autonome contre les ransomwares

La fonction ONTAP de protection autonome contre les ransomwares (Autonomous ransomware protection, ARP) utilise l'analyse des workloads dans les environnements NAS (NFS et SMB) pour détecter et avertir de manière proactive les anomalies d'activité dans les fichiers qui peuvent indiquer une attaque par ransomware.

Vous trouverez des détails supplémentaires et des exigences de licence concernant ARP ["ici"](#).

La sécurité des charges de travail s'intègre à ONTAP pour recevoir des événements ARP et fournir une couche d'analyse et de réponses automatiques supplémentaires.

La sécurité des charges de travail reçoit les événements ARP de ONTAP et effectue les opérations suivantes :

1. Met en corrélation les événements de cryptage des volumes avec l'activité des utilisateurs pour identifier qui est à l'origine des dommages.
2. Met en œuvre des politiques de réponse automatique (si définies)
3. Offre des fonctionnalités d'analyse :
 - Permettre aux clients de mener des enquêtes sur les violations de données.
 - Identifier les fichiers affectés, ce qui permet de les récupérer plus rapidement et de mener des enquêtes sur les violations de données.

Prérequis

1. Version minimale de ONTAP : 9.11.1
2. Volumes compatibles ARP. Des détails sur l'activation de ARP sont disponibles ["ici"](#). ARP doit être activé via OnCommand System Manager. La sécurité des charges de travail ne peut pas activer ARP.
3. Le collecteur de sécurité de la charge de travail doit être ajouté via l'IP du cluster.
4. Des informations d'identification au niveau du cluster sont nécessaires pour que cette fonctionnalité fonctionne. En d'autres termes, les identifiants au niveau du cluster doivent être utilisés lors de l'ajout de la SVM.

Autorisations utilisateur requises

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

Si vous utilisez un utilisateur personnalisé (par exemple, *csuser*) avec les autorisations accordées à l'utilisateur, suivez les étapes ci-dessous pour donner les autorisations à la sécurité de la charge de travail afin de collecter des informations relatives à ARP à partir de ONTAP.

Pour *csuser* avec les informations d'identification du cluster, effectuez les opérations suivantes à partir de la ligne de commande ONTAP :

```
security login rest-role create -role arwrole -api /api/storage/volumes
-access readonly -vserver <cluster_name>
security login rest-role create -api /api/security/anti-ransomware -access
readonly -role arwrole -vserver <cluster_name>
security login create -user-or-group-name csuser -application http
-authmethod password -role arwrole
```

En savoir plus sur la configuration d'autres ["Autorisations ONTAP"](#).

Alerte exemple

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



POTENTIAL ATTACK: AL_1315
Ransomware Attack

Detected
5 months ago
Oct 20, 2022 3:06 AM

Action Taken
Access Blocked on 5 SVMs
Snapshots Taken

Status
New

Blocked permanently by
auto response policy

Last snapshots taken by
auto response policy
Oct 20, 2022 3:09 AM

How To:
Restore Entities

Change Block Period

Re-Take Snapshots

Unblock User

Total Attack Results

1 Affected Volumes | 83 Deleted Files | 81 Encrypted Files

81 Files have been copied, deleted, and potentially encrypted by 1 user account.

The extension "osiris" was added to each file.

High Confidence Detection
Ransomware behavior and in-file encryption activities were detected.

Encrypted Files

Activity per minute



E Encryption activity in files

Related Users



Jamelia Graham
Business Partner
HR

User/IP Access
Blocked

81 Encrypted Files

Detected
5 months ago
Oct 20, 2022 3:06 AM

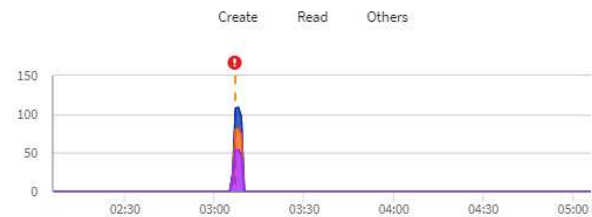
Username
us024
Domain
cslab.netapp.com
Email
Graham@netapp.com
Phone
9251140014

Department
HR
Manager
Iwan Holt
Location
WA

Top Activity Types

Activity per minute
Last accessed from: 10.193.113.247

View Activity Detail



Access Limitation History for This User (3)

Time	Action	Duration	Action Taken by	Response	Blocked IPs on NFS
Oct 20, 2022 3:09 AM	Block more detail	Never Expires		Automatic	none
Mar 10, 2022 4:59 AM	Unblock		system	Blocking Expired	10.197.144.115
Mar 10, 2022 3:57 AM	Block more detail	1h		Automatic	10.197.144.115

Affected Devices/Volumes

Device ↑	Volume	Encrypted Files	Associated Snapshot Taken
subprod_rtp	stargazer	81	Oct 20, 2022 3:09 AM cloudsecure_attack_auto Automatic _1666249787062 Take Snapshot

Une bannière de confiance élevée indique que l'attaque a montré un comportement par ransomware avec les activités de chiffrement de fichiers. Le graphique fichiers chiffrés indique l'horodatage auquel l'activité de chiffrement de volume a été détectée par la solution ARP.

Limites

Si un SVM n'est pas surveillé par la sécurité des charges de travail, mais que des événements ARP sont générés par ONTAP, les événements sont tout de même reçus et affichés par la sécurité des charges de travail. Cependant, les informations judiciaires liées à l'alerte, ainsi que le mappage des utilisateurs, ne seront pas capturées ni 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 s'affichent 24 heures avant la réception des e-mails par Cloud Insights Workload Security.	Lorsque ONTAP envoie l'événement <i>ransomware Detected</i> à la sécurité de la charge de travail Cloud Insights (c'est-à-dire la sécurité des charges de travail), l'e-mail est envoyé. L'événement contient une liste d'attaques et de ses horodatages. L'interface utilisateur de la sécurité de la charge de travail affiche l'horodatage d'alerte du premier fichier attaqué. ONTAP envoie l'événement <i>ransomware détecté</i> à Cloud Insights lorsqu'un certain nombre de fichiers sont encodés. Par conséquent, il peut y avoir une différence entre l'heure d'affichage de l'alerte dans l'interface utilisateur et l'heure d'envoi de l'e-mail.

Intégration avec l'accès ONTAP refusée

La fonction ONTAP de refus d'accès utilise l'analyse de la charge de travail dans les environnements NAS (NFS et SMB) pour détecter de manière proactive les opérations de fichiers qui ont échoué et pour signaler ces échecs (c'est-à-dire qu'un utilisateur tente d'effectuer une opération pour laquelle il n'a pas l'autorisation nécessaire). Ces notifications d'échec d'opération de fichier, en particulier en cas de défaillances liées à la sécurité, aideront encore davantage à bloquer les attaques internes dès les premiers stades.

Cloud Insights Workload Security s'intègre à ONTAP pour recevoir les événements de refus d'accès et fournir une couche supplémentaire d'analytique et de réponse automatique.

Prérequis

- Version minimale de ONTAP : 9.13.0.
- Un administrateur de Workload Security doit activer la fonctionnalité accès refusé lors de l'ajout d'un nouveau collecteur ou de la modification d'un collecteur existant, en cochant la case *Monitor Access Denied Events* sous Advanced Configuration.

Autorisations utilisateur requises

Si le Data Collector 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 les autorisations données 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 les *ccsuser* avec des informations d'identification *cluster*, exécutez les commandes suivantes à partir de la ligne de commande ONTAP. Notez que *csrestrole* est un rôle personnalisé et *csuser* est un utilisateur personnalisé ONTAP.

```
security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <cluster_name>
security login create -user-or-group-name csuser -application http
-authmethod password -role csrestrole
```

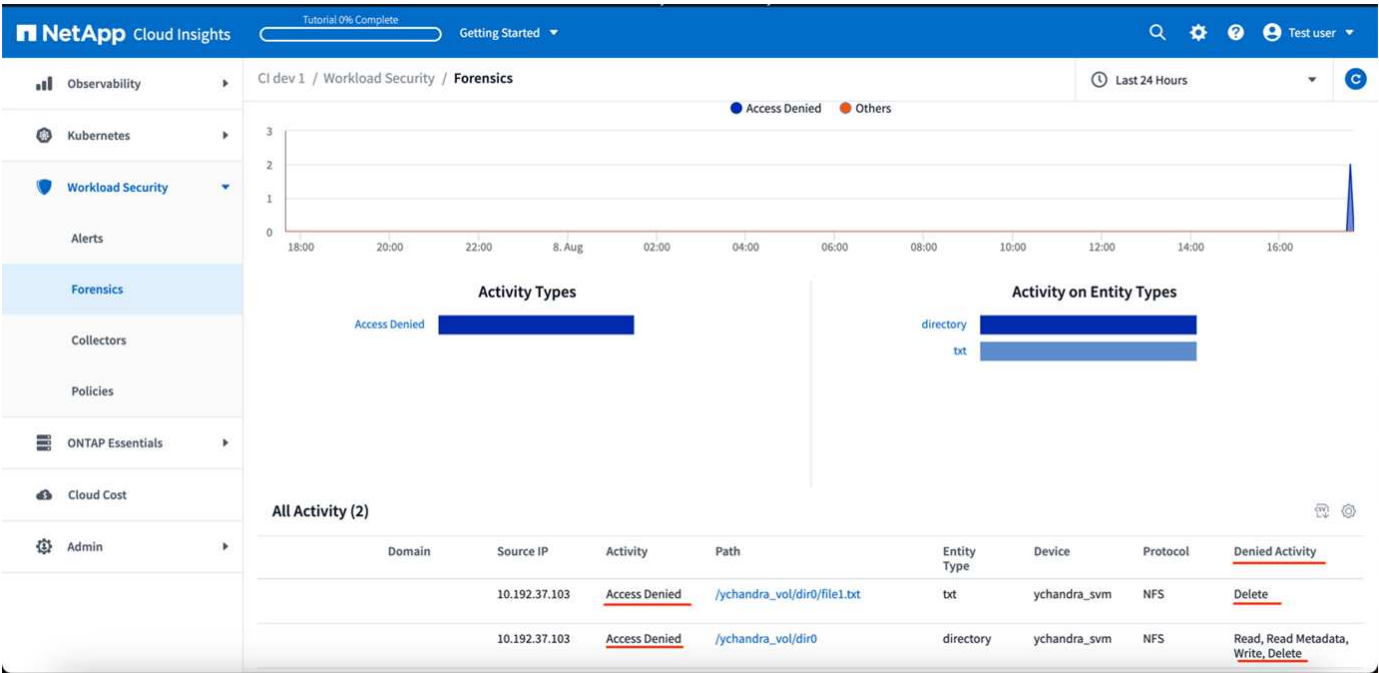
Pour les *csuser* avec *SVM* credentials, exécuter les commandes suivantes depuis la ligne de commande ONTAP :

```
security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <svm_name>
security login create -user-or-group-name csuser -application http
-authmethod password -role csrestrole -vserver <svm_name>
```

En savoir plus sur la configuration d'autres ["Autorisations ONTAP"](#).

Événements d'accès refusé

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



Blocage de l'accès utilisateur

Une fois qu'une attaque est détectée, Workload Security peut arrêter l'attaque en bloquant l'accès des utilisateurs au système de fichiers. L'accès peut être bloqué automatiquement à l'aide de politiques de réponse automatique ou manuellement à partir des pages d'alerte ou d'informations utilisateur.



La sécurité des charges de travail n'est pas disponible dans l'édition fédérale de Cloud Insights.

Lorsque vous bloquez l'accès utilisateur, vous devez définir une période de blocage. Une fois la période sélectionnée terminée, l'accès utilisateur est automatiquement restauré. Le blocage des accès est pris en charge à la fois pour les protocoles SMB et NFS.

L'utilisateur est directement bloqué pour le protocole SMB et l'adresse IP des machines hôtes à l'origine de l'attaque sera bloquée pour NFS. Ces adresses IP de la machine seront bloquées lors de l'accès à l'un des SVM contrôlés par la sécurité des charges de travail.

Disons, par exemple, que la sécurité des charges de travail gère 10 SVM, et la stratégie de réponse automatique est configurée pour quatre de ces SVM. Si l'attaque provient de l'un des quatre SVM, l'accès de l'utilisateur sera bloqué dans les 10 SVM. Une copie Snapshot est toujours effectuée sur la SVM d'origine.

Si quatre SVM avec un SVM configuré pour SMB, un SVM pour NFS et les deux autres configurés pour NFS et SMB, tous les SVM seront bloqués si l'attaque provient de l'un des quatre SVM.

Conditions préalables au blocage de l'accès utilisateur

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

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

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

Pour *csuser* avec les identifiants du cluster, effectuez la procédure suivante dans 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 SVM Data Collector de ONTAP"](#) page également.

Comment activer la fonction ?

- Dans Workload Security, accédez à **Workload Security > Politiques > Automated Response Policies**. Choisissez **+stratégie d'attaque**.
- Sélectionnez (cochez) *bloquer l'accès aux fichiers utilisateur*.

Comment configurer le blocage automatique des accès utilisateur ?

- Créez une nouvelle stratégie d'attaque ou modifiez une stratégie d'attaque existante.
- Sélectionnez les SVM sur lesquels la règle d'attaque doit être contrôlée.
- Cliquez sur la case à cocher "bloquer l'accès aux fichiers utilisateur". La fonction sera activée lorsque cette option est sélectionnée.
- Sous "time period", sélectionnez la durée jusqu'à laquelle le blocage doit être appliqué.
- Pour tester le blocage automatique de l'utilisateur, 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 s'affiche en haut de l'écran si un utilisateur est bloqué.
- Cliquez sur la bannière pour accéder à la page "utilisateurs", où la liste des utilisateurs bloqués peut être affichée.

- Dans la page “utilisateurs”, il y a une colonne intitulée “accès utilisateur/IP”. Dans cette colonne, l’état actuel du blocage de l’utilisateur s’affiche.

Limitez et gérez l’accès des utilisateurs manuellement

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

Historique des limitations d’accès utilisateur

Dans la page des détails de l’alerte et de l’utilisateur, dans le panneau utilisateur, vous pouvez afficher un audit de l’historique des limites d’accès de l’utilisateur : heure, action (Bloc, débloquent), durée, action effectuée par, Manuel/automatique et adresses IP concernées pour NFS.

Comment désactiver cette fonction ?

Vous pouvez à tout moment désactiver la fonction. Si le système contient des utilisateurs restreints, vous devez d’abord restaurer leur accès.

- Dans Workload Security, accédez à **Workload Security > Politiques > Automated Response Politiques**. Choisissez **+stratégie d’attaque**.
- Désélectionner (décocher) *bloquer l’accès aux fichiers utilisateur*.

La fonction sera masquée de toutes les pages.

Restaurez manuellement les adresses IP pour NFS

Procédez comme suit pour restaurer manuellement des adresses IP à partir de ONTAP si votre essai de sécurité de la charge de travail expire ou si l’agent/collecteur est arrêté.

1. Lister toutes les export policy sur un SVM.

```

contrail-qa-fas8020::> export-policy rule show -vserver <svm name>

```

Vserver	Policy Name	Rule Index	Access Protocol	Client Match	RO Rule
svm0	default	1	nfs3, nfs4, cifs	cloudsecure_rule, 10.11.12.13	never
svm1	default	4	cifs, nfs	0.0.0.0/0	any
svm2	test	1	nfs3, nfs4, cifs	cloudsecure_rule, 10.11.12.13	never
svm3	test	3	cifs, nfs, flexcache	0.0.0.0/0	any

4 entries were displayed.

2. Supprimez les règles de toutes les règles de la SVM qui ont "cloudSecure_rule" comme client Match en spécifiant son RuleIndex respectif. La règle de sécurité de la charge de travail est généralement de 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>

```

Vserver	Policy Name	Rule Index	Access Protocol	Client Match	RO Rule
svm0	default	4	cifs, nfs	0.0.0.0/0	any
svm2	test	3	cifs, nfs, flexcache	0.0.0.0/0	any

2 entries were displayed.

Restaurez manuellement les utilisateurs pour SMB

Procédez comme suit pour restaurer manuellement des utilisateurs à partir de ONTAP si votre version d'évaluation de la sécurité de la charge de travail expire ou si l'agent/collecteur est arrêté.

Vous pouvez obtenir la liste des utilisateurs bloqués dans la sécurité de la charge de travail à partir de la page liste des utilisateurs.

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

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

```
Vserver:    <vservename>
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 étaient 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 débloquent l'utilisateur :

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

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

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

Dépannage

Problème	Essayez
Certains utilisateurs ne sont pas limités, bien qu'il y ait une attaque.	1. Assurez-vous que le Data Collector et l'Agent des SVM sont à l'état <i>running</i> . La sécurité de charge de travail ne pourra pas envoyer de commandes si le Data Collector et l'agent sont arrêtés. 2. Ceci est dû au fait que l'utilisateur a peut-être accédé au stockage à partir d'un ordinateur avec une nouvelle adresse IP qui n'a pas été utilisée auparavant. La restriction s'effectue via l'adresse IP de l'hôte par l'intermédiaire de laquelle l'utilisateur accède au stockage. Vérifiez dans l'interface utilisateur (Détails de l'alerte > Historique des limitations d'accès pour cet utilisateur > adresses IP affectées) 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, alors l'utilisateur pourra toujours accéder au stockage via l'adresse IP non restreinte. Si l'utilisateur tente d'accéder aux hôtes dont les adresses IP sont restreintes, alors le stockage ne sera pas accessible.
Si vous cliquez manuellement sur restreindre l'accès, « les adresses IP de cet utilisateur ont déjà été restreintes » s'affiche.	L'adresse IP à restreindre est déjà restreinte par un autre utilisateur.
La politique n'a pas pu être modifiée. Motif : non autorisé pour cette commande.	Vérifiez si vous utilisez <i>csuser</i> , les autorisations sont accordées à l'utilisateur comme indiqué ci-dessus.
Le blocage de l'utilisateur (adresse IP) pour NFS fonctionne, mais pour SMB / CIFS, un message d'erreur s'affiche : « échec de la transformation entre SID et DomainName. Délai d'expiration du motif : le socket n'est pas établi »	Ceci peut se produire est <i>csuser</i> n'a pas l'autorisation d'exécuter ssh. (Vérifiez la connexion au niveau du cluster, puis assurez-vous que l'utilisateur peut effectuer ssh). le rôle <i>csuser</i> requiert ces autorisations. https://docs.netapp.com/us-en/cloudinsights/cs_restrict_user_access.html#prerequisites-for-user-access-blocking Pour <i>csuser</i> avec les informations d'identification du cluster, effectuez les opérations suivantes à partir de la ligne de commande ONTAP : sécurité 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 authentifiez" -all security login Rôle create -role csrole -cmddirname "vserver name-mapping" -Access all si <i>csuser</i> n'est pas utilisé et si admin user au niveau du cluster est utilisé, assurez-vous que l'utilisateur admin a les droits ssh à ONTAP.

Sécurité des charges de travail : simulation d'une attaque

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



La sécurité des charges de travail n'est pas disponible dans l'édition fédérale de Cloud Insights.

À noter avant de commencer

- Le script de simulation d'attaque par ransomware fonctionne uniquement sur Linux.
- Le script est fourni avec les fichiers d'installation de l'agent de sécurité de la charge de travail. Il est disponible sur n'importe quelle machine sur laquelle un agent de sécurité de la charge de travail est installé.
- Vous pouvez exécuter le script sur l'agent de sécurité de la charge de travail lui-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.

Avoir au moins 1,000 fichiers d'exemple

Ce script doit s'exécuter sur un SVM avec un dossier qui a des fichiers à chiffrer. Nous vous recommandons d'avoir au moins 1,000 fichiers dans ce dossier et tous les sous-dossiers. Les fichiers ne doivent pas être vides. Ne créez pas les fichiers et ne les cryptez pas à l'aide du même utilisateur. La sécurité de la charge de travail considère cette activité à faible risque et ne génère donc pas d'alerte (c'est-à-dire que le même utilisateur modifie les fichiers qu'il/elle vient de créer).

Voir ci-dessous pour les instructions à ["créer par programmation des fichiers non vides"](#).

Consignes avant d'exécuter le simulateur :

1. Assurez-vous que les fichiers chiffrés ne sont pas vides.
2. Assurez-vous de crypter > 50 fichiers. Un petit nombre de fichiers sera ignoré.
3. Ne pas exécuter une attaque avec le même utilisateur plusieurs fois. Au bout de quelques reprises, Workload Security apprendra ce comportement d'utilisateur et suppose qu'il s'agit du comportement normal de l'utilisateur.
4. Ne pas crypter les fichiers que le même utilisateur vient de créer. La modification d'un fichier qui vient d'être créé par un utilisateur n'est pas considérée comme une activité risquée. Utilisez plutôt les fichiers créés par un autre utilisateur OU attendez quelques heures entre la création et le cryptage des fichiers.

Préparez le système

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

Pour monter l'exportation NFS sous Linux :

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

Ne montez pas NFS version 4.1 ; il n'est pas pris en charge par Fpolicy.

Pour monter CIFS sous Linux :

```
mount -t cifs //10.193.77.91/sharedfolderincluster  
/root/destinationfolder/ -o username=raisa  
Configurez ensuite un Data Collector :
```

1. Configurez l'agent de sécurité de la charge de travail si ce n'est déjà fait.
2. Configurer le collecteur de données du SVM s'il n'a pas encore été effectué

Exécutez le script du simulateur de ransomware

1. Connectez-vous (ssh) à l'agent de sécurité de la charge de travail.
2. Accédez à : `/opt/netapp/cloudSecure/agent/install`
3. Appelez le script du simulateur sans paramètres pour voir l'utilisation :

```
# pwd  
/opt/netapp/cloudsecure/agent/install  
# ./ransomware_simulator.sh  
Error: Invalid directory provided.  
Usage: ./ransomware_simulator.sh [-e] [-d] [-i <input_directory>]  
-e to encrypt files (default)  
-d to restore files  
-i <input_directory> - Files under the directory to be encrypted
```

```
Encrypt command example: ./ransomware_simulator.sh -e -i  
/mnt/audit/reports/  
Decrypt command example: ./ransomware_simulator.sh -d -i  
/mnt/audit/reports/
```

Crypter vos fichiers de test

Pour crypter les fichiers, exécutez la commande suivante :

```
# ./ransomware_simulator.sh -e -i /root/for/  
Encryption key is saved in /opt/netapp/cloudsecure/cloudsecure-agent-  
1.251.0/install/encryption-key,  
which can be used for restoring the files.  
Encrypted /root/for/File000.txt  
Encrypted /root/for/File001.txt  
Encrypted /root/for/File002.txt  
...
```

Restaurez les fichiers

Pour décrypter, exécutez la commande suivante :

```
[root@scspa2527575001 install]# ./ransomware_simulator.sh -d -i /root/for/  
File /root/for/File000.txt is restored.  
File /root/for/File001.txt is restored.  
File /root/for/File002.txt is restored.  
...
```

Exécutez le script plusieurs fois

Après avoir généré une attaque par ransomware pour un utilisateur, passez à un autre utilisateur pour générer une attaque supplémentaire. La sécurité des charges de travail apprend le comportement des utilisateurs et ne déclenche pas d'alerte lorsque les attaques par ransomware sont répétées dans les mêmes délais par le même utilisateur.

Créez des fichiers par programmation

Avant de créer les fichiers, vous devez d'abord arrêter ou interrompre le traitement du collecteur de données. Effectuez les étapes ci-dessous avant d'ajouter le collecteur de données à l'agent. Si vous avez déjà ajouté le collecteur de données, il vous suffit de modifier le collecteur de données, de saisir un mot de passe non valide et de l'enregistrer. Le collecteur de données sera temporairement à l'état d'erreur. REMARQUE : veillez à noter le mot de passe d'origine !



L'option recommandée est à "[mettre le collecteur en pause](#)" avant de créer vos fichiers.]

Avant d'exécuter la simulation, vous devez d'abord ajouter des fichiers à chiffrer. Vous pouvez soit copier manuellement les fichiers à crypter dans le dossier cible, soit utiliser un script (voir l'exemple ci-dessous) pour créer les fichiers par programmation. Quelle que soit la méthode utilisée, copiez au moins 1,000 fichiers.

Si vous choisissez de créer les fichiers par programmation, procédez comme suit :

1. Connectez-vous à la boîte Agent.
2. Monter une exportation NFS depuis le SVM du filer vers la machine Agent. CD dans ce dossier.
3. Dans ce dossier, créez un fichier nommé createfiles.sh
4. Copiez les lignes suivantes dans ce fichier.

```
for i in {000..1000}
do
    echo hello > "File${i}.txt"
done
echo 3 > /proc/sys/vm/drop_caches ; sync
```

5. Enregistrez le fichier.
6. Assurez-vous que l'autorisation d'exécution est autorisée sur le fichier :

```
chmod 777 ./createfiles.sh
. Exécutez le script :
```

```
./createfiles.sh
```

1000 fichiers seront créés dans le dossier actuel.

7. Réactiver le collecteur de données

Si vous avez désactivé le collecteur de données à l'étape 1, modifiez le collecteur de données, saisissez le mot de passe correct et enregistrez. Assurez-vous que le collecteur de données est à nouveau en cours d'exécution.

8. Si vous avez interrompu le collecteur avant de suivre ces étapes, assurez-vous de ["reprendre le collecteur"](#).

Configuration des notifications par e-mail pour les alertes, les avertissements et l'état de santé du collecteur d'agents/de sources de données

Pour configurer les destinataires d'alertes de sécurité de la charge de travail, cliquez sur **Admin > Notifications** et entrez une ou plusieurs adresses électroniques dans les sections appropriées pour chaque destinataire.



La sécurité des charges de travail n'est pas disponible dans l'édition fédérale de Cloud Insights.

Alertes et avertissements d'attaque potentielle

Pour envoyer des notifications *attaque potentielle* alerte, entrez les adresses e-mail des destinataires dans la section *Envoyer alertes d'attaque potentielles*. Les notifications par e-mail sont envoyées à la liste des destinataires des alertes pour chaque action de l'alerte.

Pour envoyer des notifications *Warning*, entrez les adresses e-mail des destinataires dans la section *Send Warning Alerts*.

Surveillance de l'état de santé des agents et des Data Collector

Vous pouvez surveiller l'état des agents et des sources de données grâce aux notifications.

Afin de recevoir des notifications si un agent ou un collecteur de source de données ne fonctionne pas, entrez les adresses électroniques des destinataires dans la section *Data Collection Health Alerts*.

Gardez à l'esprit les éléments suivants :

- Les alertes d'intégrité ne seront envoyées qu'une fois que l'agent/le collecteur cesse de générer des rapports pendant au moins une heure.
- Une seule notification par e-mail est envoyée aux destinataires prévus dans une période donnée de 24 heures, même si l'agent ou le collecteur de données est déconnecté pendant une période plus longue.
- En cas de défaillance d'un agent, une alerte est envoyée (pas une par collecteur). Cet e-mail inclura une liste de tous les SVM affectés.
- L'échec de la collecte de répertoire actif est signalé comme un avertissement ; elle n'a aucun impact sur la détection de ransomware.
- La liste mise en route comprend maintenant une nouvelle phase *configurer les notifications par e-mail*.

Réception de notifications de mise à niveau d'agent et de Data Collector

- Entrez les ID d'e-mail dans le champ « Data Collection Health Alerts » (alertes d'état de la 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 Data Collector sont envoyées aux ID d'e-mail un jour avant la mise à niveau prévue.

Dépannage

Problème:	Essayez ceci:
Les ID d'e-mail sont présents dans les « alertes d'intégrité du Data Collector », mais je ne reçois pas de notifications.	Les e-mails de notification sont envoyés depuis le domaine NetApp Cloud Insights, c'est-à-dire depuis <i>accounts@service.cloudinsights.netapp.com</i> . Certaines entreprises bloquent les e-mails entrants s'ils proviennent d'un domaine externe. Assurez-vous que les notifications externes provenant des domaines NetApp Cloud Insights sont blanches.

API de sécurité du workload

L'API de sécurité des charges de travail permet aux clients NetApp et aux éditeurs de logiciels indépendants d'intégrer la sécurité des charges de travail à d'autres applications, comme les CMDB ou d'autres systèmes de gestion des tickets.



La sécurité des charges de travail n'est pas disponible dans l'édition fédérale de Cloud Insights.

Conditions requises pour l'accès à l'API :

- Un modèle de token d'accès API est utilisé pour accorder l'accès.
- La gestion des tokens API est effectuée par les utilisateurs de la sécurité de la charge de travail dotés du rôle d'administrateur.

Documentation API (swagger)

Pour obtenir les dernières informations sur l'API, connectez-vous à la sécurité de la charge de travail et accédez à **Admin > API Access**. Cliquez sur le lien **API Documentation**. La documentation API est basée sur swagger, qui fournit une brève description et des informations d'utilisation de l'API et vous permet de l'essayer dans votre environnement.

Jetons d'accès à l'API

Avant d'utiliser l'API de sécurité de la charge de travail, 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 token d'accès :

- Cliquez sur **Admin > accès API**
- Cliquez sur **+jeton d'accès API**
- Saisissez **Nom de token**
- Spécifiez **expiration du token**



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

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

Les jetons accordent un accès général aux API du point de vue du client, et gèrent l'accès aux API dans le cadre de leur propre environnement.

L'application reçoit un token d'accès après l'authentification et l'autorisation de l'accès, puis transmet le token d'accès en tant qu'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 l'étendue accordée lors de l'autorisation.

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

Par exemple, utilisez les éléments suivants pour récupérer des actifs de stockage :

```
curl https://<tenant_host_name>/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 à l'API.

Vous trouverez des informations détaillées dans le lien *API Documentation* sous **Admin > API Access**.

Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.