Mise en route

Data Infrastructure Insights

NetApp
January 17, 2025

Sommaire

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.

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 **sécurité de la charge de travail > collecteurs** cliquez sur le collecteur de données que vous souhaitez configurer. Reportez-vous à la section Data Collector Vendor Reference 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" lors de l'intégration avec Splunk.

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

Vous devez pour "Installez un agent"obtenir des informations 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.

Composant	**Configuration Linux requise**
Système d'exploitation	Un ordinateur exécutant une version sous licence de l'un des éléments suivants : * CentOS 8 64 24,04 11 9,4 Stream (64 20.04 64 64 64 bits), CentOS 9 22.04 10 9.3 Stream, SELinux * openSUSE Leap 64 à 9.2 (64 bits) * Oracle Linux 8.8 - 9.1, 9.4 à 9.4 (64 bits) * Red Hat Enterprise Linux 8.6 à 8.6, 8.8 à 9.1 (15.3 bits), SELinux * 15.5 - 9.4 bits (15 bits) et Linux * 15 bits (64 bits) Un serveur dédié est recommandé.

Composant	Configuration Linux requise
Commandes	le dézipper est requis pour l'installation. En outre, la commande « udo su – » 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	L'espace disque doit être alloué de la manière suivante : /opt/NetApp 36 Go (minimum 35 Go d'espace libre après la création du système de fichiers) Remarque : il est recommandé d'allouer un peu d'espace disque supplémentaire pour permettre la création du système de fichiers. Assurez-vous qu'il y a au moins 35 Go d'espace libre dans le système de fichiers. Si /opt est un dossier monté à partir d'un stockage NAS, assurez-vous que les utilisateurs locaux ont accès à ce dossier. L'installation de l'agent ou du collecteur de données peut échouer si les utilisateurs locaux n'ont pas l'autorisation de ce dossier. Reportez-vous à la section pour plus de détails."dépannage"
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 Workload Security peut être installé sur la même machine qu'un agent et/ou une unité d'acquisition Data Infrastructure Insights. 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 aux informations exploitables de l'infrastructure de données

Protocole	Port	Source	Destination	Description
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 aux informations exploitables de l'infrastructure de données
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 aux informations exploitables de l'infrastructure de données
TCP	443	Agent de sécurité des charges de travail	gateway.c01.cloudinsights.netapp.com agentlogin.cs01-ap-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). NOTEZ que vous n'avez pas besoin de réserver **tous** de ces ports, mais que les ports que vous réservez pour ce port doivent être compris dans cette plage. Il est recommandé de commencer par réserver ~100 ports et d'augmenter si nécessaire.
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

Pour plus d'informations sur le dimensionnement, reportez-vous à la "Vérificateur de taux d'événement"documentation.

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 périphériques de votre locataire et collectent les données qui sont envoyées à la couche SaaS de sécurité de la charge de travail pour analyse. Reportez-vous à la section "Exigences de l'agent" pour configurer une machine virtuelle d'agent.

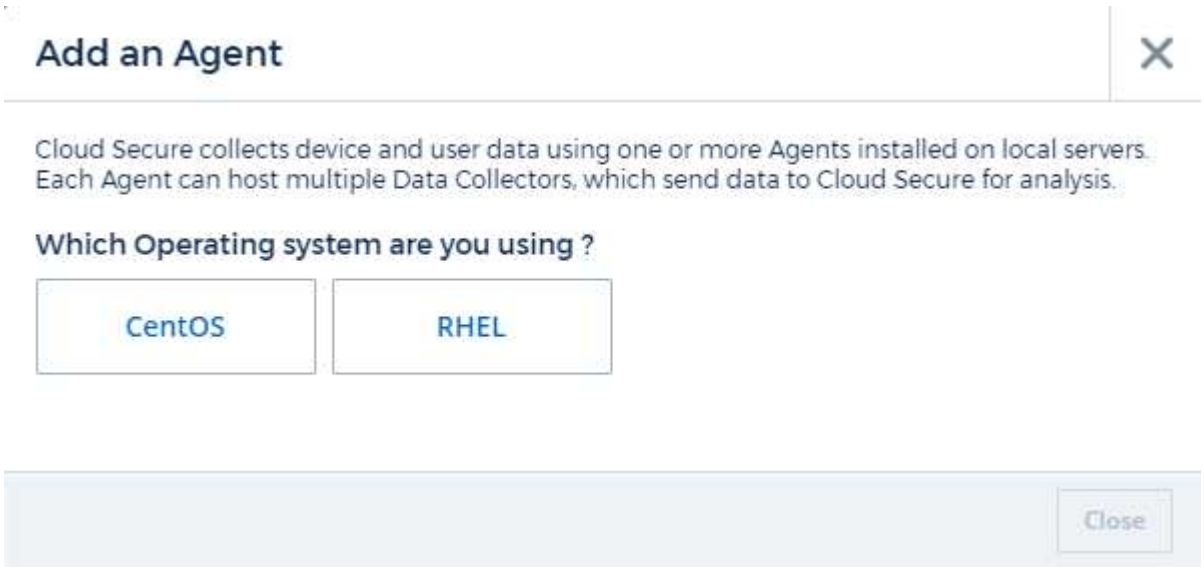
Avant de commencer

- 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 lire à propos de la sécurité Data Infrastructure Insights "ici".

Procédure d'installation de l'agent

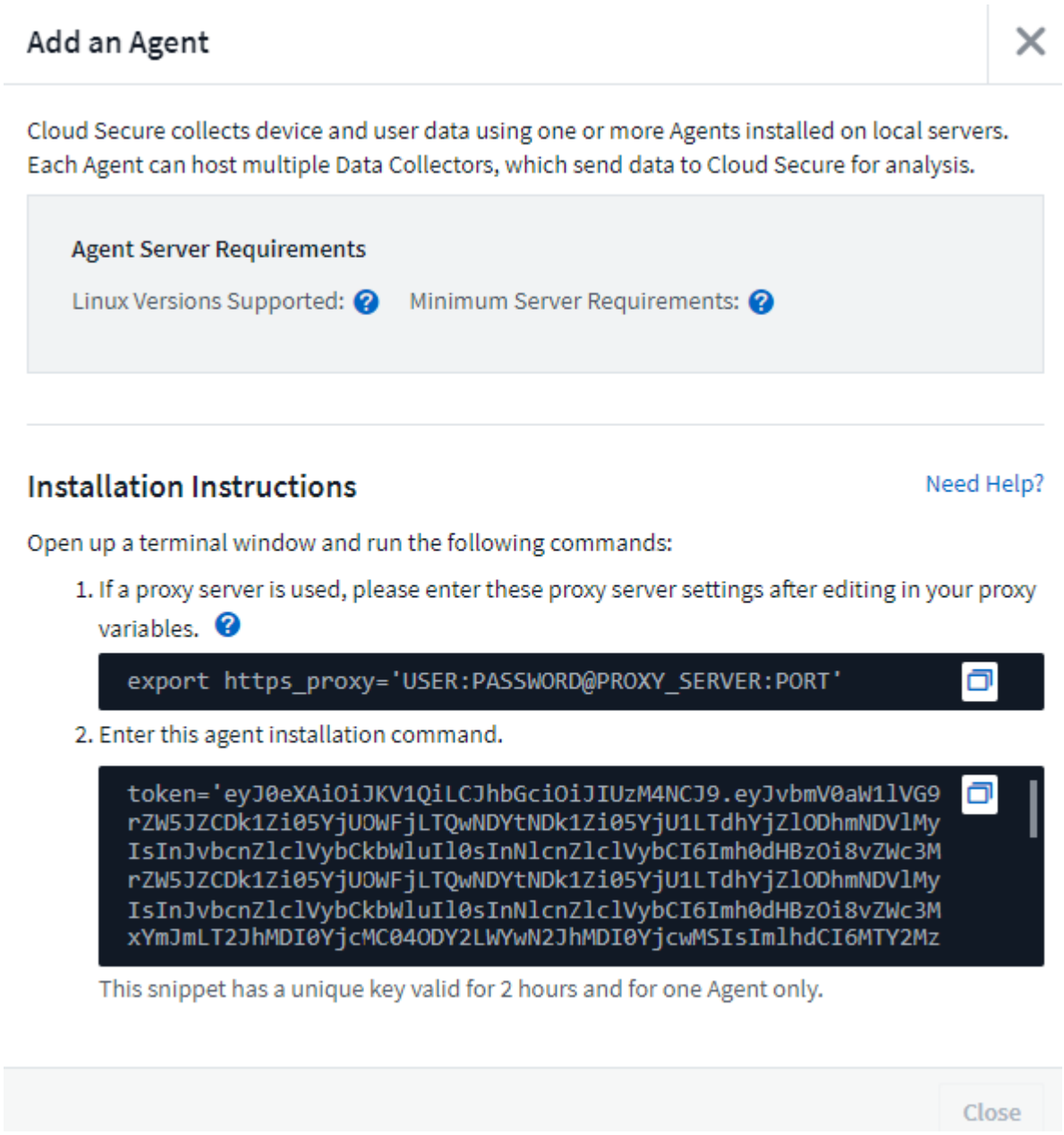
1. Connectez-vous en tant qu'administrateur ou responsable de compte à votre environnement de sécurité de la charge de travail.
2. Sélectionnez **collecteurs > agents > +Agent**

   Le système affiche la page Ajouter un agent :



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.



6. Cliquez sur l'icône Copier dans le presse-papiers pour copier la commande d'installation.
7. Exécutez la commande d'installation dans une fenêtre de terminal.
8. Une fois l'installation terminée, le système affiche le message suivant :

Et pour finir

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
```

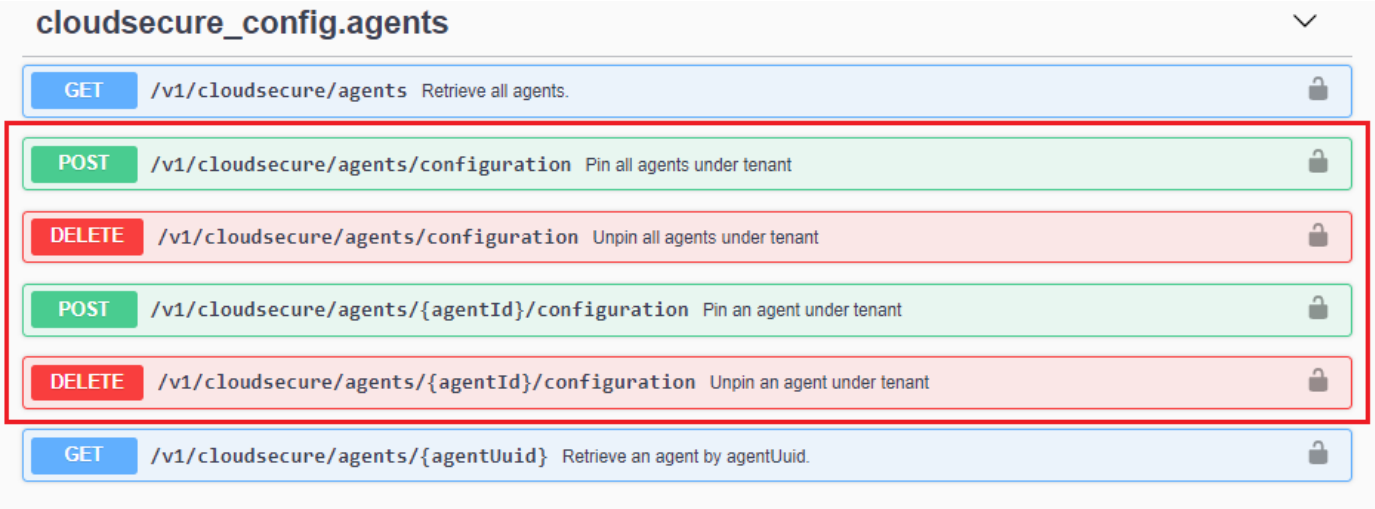
« Épingler » un agent à la version actuelle

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

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

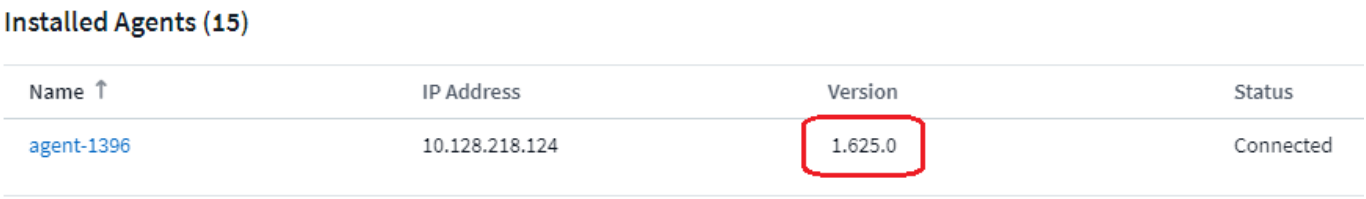
Dans chacun de ces cas, l'agent sera mis à jour lors de la prochaine actualisation de la sécurité de la charge de travail.

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



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

Vous pouvez afficher les versions actuelles de vos agents sur la page **Workload Security > Collectors**, dans l'onglet **agents**.



Dépannage des erreurs de l'agent

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

Problème :	Résolution :
L'installation de l'agent ne parvient pas à créer le dossier /opt/netapp/cloudSecure/agent/logs/agent.log et le fichier install.log ne 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 la `journalctl -u cloudsecure-agent.service` commande. Cette commande peut être utilisée pour résoudre le problème. est
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 de l'agent via `sudo systemctl status cloudsecure-agent.service`. 1. Vérifiez si les journaux affichent un message « Impossible de démarrer le service démon Workload Security » . 2. Vérifiez si l'utilisateur cssys existe dans la machine Agent ou non. Exécutez les commandes suivantes une par une avec l'autorisation root et vérifiez si l'utilisateur et le groupe cssys existent. `sudo id cssys` `sudo groups cssys` 3. S'il n'en existe aucun, une stratégie de surveillance centralisée peut avoir supprimé l'utilisateur cssys. 4. Créez manuellement un utilisateur et un groupe cssys en exécutant les commandes suivantes. `sudo useradd cssys` `sudo groupadd cssys` 5. Redémarrez ensuite le service d'agent en exécutant la commande suivante : `sudo systemctl restart cloudsecure-agent.service` 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 ensuite le service d'agent en exécutant la commande suivante : `sudo systemctl restart cloudsecure-agent.service` 3. Vérifiez l'état du service de l'agent via `sudo systemctl status cloudsecure-agent.service`. 4. L'agent doit passer à l'état CONNECTÉ.
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.	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.

Problème :	Résolution :
Lors de l'installation de l'agent, l'installation se bloque après le décompression.	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 « cloudsecure ». 2. Accédez à ce répertoire. 3. Copiez et collez la commande d'installation complète "token=…… ./cloudsecure-agent-install.sh" et appuyez sur entrée. 4. L'installation doit pouvoir continuer.
Si l'agent n'est toujours pas en mesure de se connecter à Saas, veuillez ouvrir un dossier auprès du support NetApp. Fournir le numéro de série Data Infrastructure Insights pour ouvrir un dossier de demande de support et joindre les journaux au dossier comme indiqué.	Pour joindre des journaux au cas : 1. Exécutez le script suivant avec l'autorisation root et partagez le fichier de sortie (cloudsecure-agent-symptomes.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
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	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.
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 : *sudo useradd nom_utilisateur -m -d HOME_DIR* -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, *sudo useradd cssys -m -d /cssys*, ajoute un utilisateur *cssys* et crée son répertoire de connexion sous root.

Problème :	Résolution :
L'agent n'est pas en cours d'exécution après l'installation. *Systemctl status cloudsecure-agent.service* NetApp 126 26 affiche les éléments suivants : [root@demo ~]# systemctl status cloudsecure-agent.service agent.service 26 03 21 cloudsecure-agent.service – Workload Security Agent Daemon Service loaded: Loaded (/usr/lib/systemd/system/cloudsecure-agent.service; cloudsecure-agent.service: 12 Enabled; vendor preset: Disabled) Active: Activating (auto-restart) (result: Code-exit) depuis Mar 25889-126:126:26:03 21:12 PDT; 2s/basso. Démarrer/08-03 21:2021:25889:12(used). 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 : cd /opt/netapp/cloudSecure/conf 2. À l'aide de votre éditeur de texte favori, ouvrez le fichier *agent.properties* pour le modifier. 3. Ajoutez ou modifiez les lignes suivantes : AGENT_PROXY_HOST=scspa1950329001.vm.NetApp.com AGENT_PROXY_PORT=80 AGENT_PROXY_user=pxuser AGENT_PROXY_PASSWORD=pass1234 4. Enregistrez le fichier. 5. Redémarrez l'agent : sudo systemctl restart cloudsecure-agent.service

Suppression d'un agent de sécurité de charge de travail

Lorsque vous supprimez un agent 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 un administrateur Data Infrastructure Insights ou un 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 **Collectors > User Directory Collectors > + User Directory Collector** 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 *GlobalADCollector*
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 : *x. correct.z* ⇒ nom de domaine direct comme vous l'avez sur votre SVM. [Exemple : hq.companyname.com] *DC=x,DC=y,DC=z* ⇒ noms distinctifs relatifs [exemple : DC=hq,DC= companyname,DC=com] ou vous pouvez spécifier les éléments suivants : *Ou=engineering,DC=hq,DC= companyname,DC=com* [to filter by Specific UO Engineering] *CN=username,ou=engineering,DC=companyname, DC=netapp, DC=com* [to get only user with <username> from ou <engineering>] _CN=Acrobat,CN=Users,CN=company=ID=DC=ID=ID=ID=ici=ID=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=
Lier DN	L'utilisateur est autorisé à rechercher dans le répertoire. Par exemple : *username@companyname.com* ou *username@domainname.com* en outre, l'autorisation domaine en lecture seule est requise. L'utilisateur doit être membre du groupe de sécurité *contrôleurs de domaine en lecture seule*.
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 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

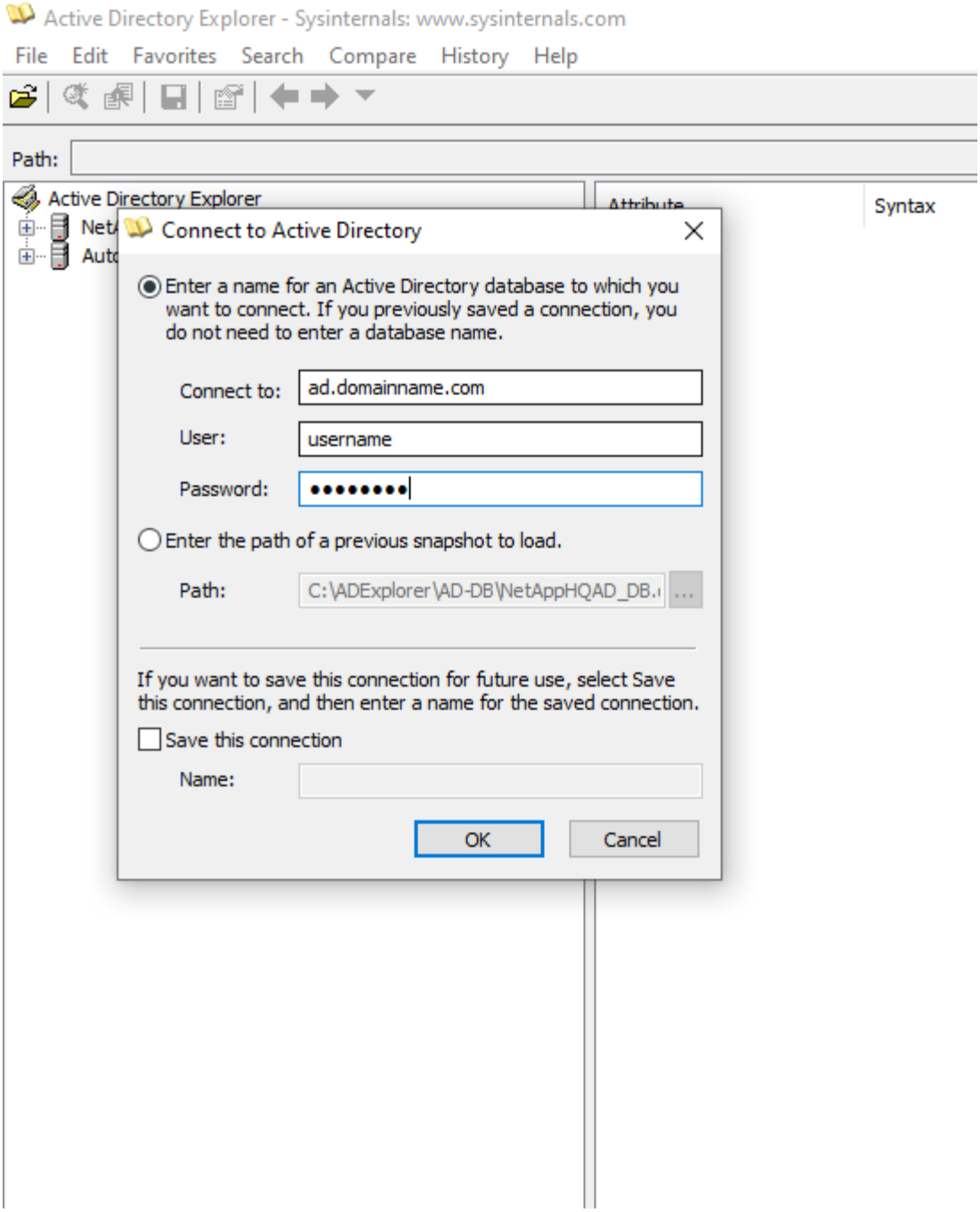
Test de la configuration du collecteur d'annuaire d'utilisateurs

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.
  - Installez "Explorateur D'ANNONCES" sur n'importe quelle machine Windows pouvant se connecter au serveur AD.
  - Connectez-vous au serveur AD à l'aide du nom d'utilisateur/mot de passe du serveur d'annuaire AD.



Dépannage des erreurs de configuration du collecteur d'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 *Restart*.
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(,seconds),true)] a échoué en raison de java.net.ConnectionException:Connection refusé."	Adresse IP ou FQDN incorrecte fournie 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".	Adresse IP ou FQDN incorrecte fournie 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 de AD 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.
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 qui extrait les informations de l'utilisateur depuis Active Directory. 2. Remarque sous attributs facultatifs, un nom de champ "Numéro de téléphone" est mappé à l'attribut Active Directory 'numéro de téléphone'. 4. Veuillez maintenant utiliser l'outil Explorateur Active Directory comme décrit ci-dessus pour parcourir Active Directory et voir le nom d'attribut correct. 3. Assurez-vous que, dans Active Directory, il existe un attribut nommé 'telephonenumber' qui a effectivement le numéro de téléphone de l'utilisateur. 5. Disons dans Active Directory qu'il a été modifié en 'phonenumber'. 6. Modifiez ensuite 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 obtient le numéro de téléphone de l'utilisateur et affiche le même numéro 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 un administrateur Data Infrastructure Insights ou un 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 **Collectors > User Directory Collectors > + User Directory Collector** et sélectionnez **LDAP Directory Server**

   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 *GlobalLDAPCollector*
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. correct.z* ⇒ nom de domaine direct tel que vous l’avez sur votre SVM. [Exemple : hq.companyname.com] *DC=x,DC=y,DC=z* ⇒ noms distinctifs relatifs [exemple : DC=hq,DC=companyname,DC=com] ou vous pouvez spécifier les éléments suivants : *Ou=engineering,DC=hq,DC=companyname,DC=com* [to filter by Specific UO Engineering] *CN=username,ou=engineering,DC=companyname, DC=netapp, DC=com* [to get only user with <username> from ou <Engineering>] _CN=Acrobat,CN=Users,CN=company=ID=Users,DC=Company=Company=Company=s==Company=Company=s=Company=Company=Company=s=s=Company=s=s=s=s=s=Company=Company=s=ID=s,DC=ID=s=ID=s=s=s=

Lier DN	L'utilisateur est autorisé à rechercher dans le répertoire. Par exemple : uid=ldapuser,cn=Users,cn=accounts,dc=domain,dc=companyname,dc=com uid=john,cn=users,cn=accounts,dc=dorp,dc=Company,dc=com pour un utilisateur john@dorp.company.com. dorp.company.com
--comptes	--utilisateurs
--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

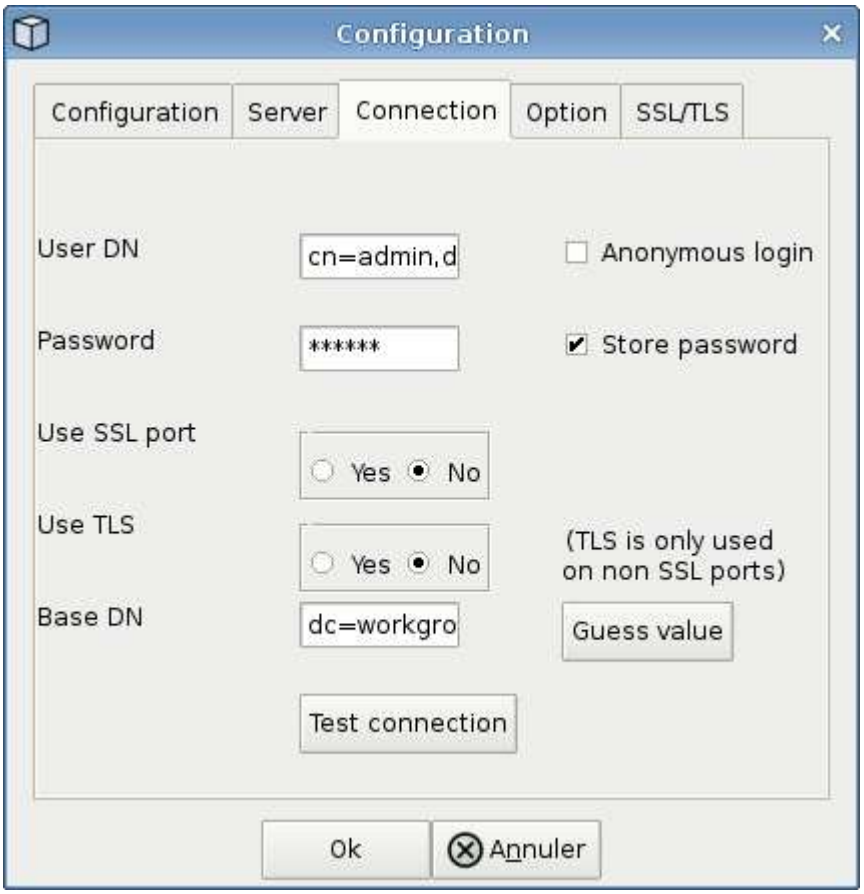
Test de la configuration du collecteur d'annuaire d'utilisateurs

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



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 *Restart*.
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 sont correctes ///
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(,seconds),true)] a échoué en raison de java.net.ConnectionException:Connection refusé."	Adresse IP ou FQDN incorrecte fournie 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 qui extrait les informations de l'utilisateur depuis Active Directory. 2. Remarque sous attributs facultatifs, un nom de champ "Numéro de téléphone" est mappé à l'attribut Active Directory 'numéro de téléphone'. 4. Veuillez maintenant utiliser 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 existe un attribut nommé 'telephonenumber' qui a effectivement le numéro de téléphone de l'utilisateur. 5. Disons dans l'annuaire LDAP qu'il a été modifié en "phonenumber". 6. Modifiez ensuite 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 obtient le numéro de téléphone de l'utilisateur et affiche le même numéro 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.
  - NFS versions jusqu'à NFS 4.1 avec ONTAP 9.15.1 ou version ultérieure incluse.
  - 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 ».
- • Le magasin permanent ONTAP est pris en charge à partir de 9.14.1.
- 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 utiliser le nom d'utilisateur et le mot de passe complets de gestion du cluster/SVM, vous pouvez créer un utilisateur personnalisé avec un Privileges inférieur, 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 de l'ONTAP".

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

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

Exemple de résultat :

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

- 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 admin du cluster, ignorez cette étape. Clustershell:::> `security login password -username vsadmin -vserver svmname`
- Déverouiller l'utilisateur SVM vsadmin pour l'accès externe Si vous utilisez un utilisateur personnalisé ou un utilisateur admin du cluster, ignorez cette étape. Clustershell:::> `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 en cas d'utilisation d'une lif de gestion dédiée pour ajouter le SVM. Clustershell::> `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 plus d'informations sur la 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 à l'esprit les "Blocage de l'accès utilisateur"points suivants :

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
security login create -user-or-group-name csuser -application http
-authmethod password -role csrole
```

Autorisations lors de l'ajout via Vserver Management IP :

Si vous ne pouvez pas utiliser l'utilisateur administrateur de gestion 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 <vservername> par votre nom de Vserver avant d'exécuter les commandes suivantes sur ONTAP :

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

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

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

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

Mode protobuf

La sécurité de la charge de travail configure le moteur FPolicy en mode protobuf lorsque cette option est activée dans les paramètres *Advanced Configuration* du collecteur. Le mode Protobuf est pris en charge dans ONTAP version 9.15 et ultérieure.

Vous trouverez plus de détails sur cette fonction dans le "Documentation de l'ONTAP".

Des autorisations spécifiques sont requises pour le protobuf (certaines ou toutes ces autorisations existent peut-être déjà) :

Mode cluster :

```
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
```

Mode SVM :

```
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 ONTAP et accès ONTAP refusées

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 plus d'informations, consultez à propos de "Intégration avec l'accès ONTAP refusée"

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

Configurer le collecteur de données

Étapes de configuration

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

   Le système affiche les collecteurs de données disponibles.

3. 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 de 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 MetroCluster

Les recommandations suivantes sont recommandées pour MetroCluster :

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 avec ONTAP **version 9.9.1 ou ultérieure**, pour 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 les informations d'infrastructure de données.

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 identifie une attaque par ransomware, ONTAP ne pourra pas acquérir les connaissances nécessaires sur l'infrastructure de données avec Workload Security.
- 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.

Stockage persistant

Le stockage persistant est pris en charge avec ONTAP 9.14.1 et les versions ultérieures. Notez que les instructions relatives au nom du volume varient de ONTAP 9.14 à 9.15.

Le stockage persistant peut être activé en cochant la case dans la page de modification/ajout du collecteur. Une fois la case cochée, un champ de texte permettant d'accepter le nom du volume s'affiche. Le nom du volume est un champ obligatoire pour activer le stockage permanent.

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

Des autorisations spécifiques sont requises pour le stockage permanent (certaines ou toutes ces autorisations existent peut-être déjà) :

Mode cluster :

```
security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <cluster-name>
security login rest-role create -role csrestrole -api /api/cluster/jobs/
-access readonly -vserver <cluster-name>
```

Mode SVM :

```
security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <vserver-name>
security login rest-role create -role csrestrole -api /api/cluster/jobs/
-access readonly -vserver <vserver-name>
```

Dépannage

Reportez-vous "Dépannage du collecteur SVM"à la page pour obtenir des conseils de dépannage.

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

Pour configurer une instance AWS HA à un seul nœud ou pour héberger l'agent Workload Security, reportez-vous à la documentation OnCommand Cloud Volumes ONTAP : https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/index.html

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

Plateformes prises en charge

- Cloud Volumes ONTAP, pris en charge 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 un 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 Data Infrastructure Insights.
2. Accédez à Workload Security **Collectors** et cliquez sur l'onglet **agents**.
3. Cliquez sur **+Agent** et spécifiez RHEL comme plate-forme cible.
4. Copiez la commande installation de l'agent.
5. Collez la commande installation de l'agent dans l'instance RHEL EC2 à laquelle vous êtes connecté. Ceci installe l'agent Workload Security, à condition que tous les "Conditions préalables de l'agent" soient satisfaits.

Pour des étapes détaillées, veuillez vous reporter au 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 FxSN" 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 utilisateur Workload Security sont gérés via les informations exploitables de l’infrastructure de données.

Data Infrastructure Insights offre quatre niveaux de compte utilisateur : propriétaire de compte, administrateur, utilisateur et invité. 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 transféré à la page gestion des utilisateurs de Data Infrastructure 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).

Pour plus d'informations sur les comptes et les rôles utilisateur, reportez-vous à la documentation Data Infrastructure Insights"Rôle utilisateur".

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
```

3. Indiquez les valeurs correctes lorsque vous y êtes invité. Voir un exemple ci-dessous.
4. L'exécution du script prend environ 5 minutes.

5. Une fois l'exécution terminée, le script imprime le taux d'évènement à partir du SVM. Vous pouvez vérifier le taux d'événement 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'événement 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'événement 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
Reportez-vous
xref:{relative_path}concept_cs_agent_requirements.html["Exigences de
l'agent"]à la page pour connaître les conditions requises 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'exécutera pendant 5 minutes maximum, même si le nombre de SVM sera 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'exécutera pendant 5 min maximum, même si le nombre de SVM sera 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.