Guide de dépannage et FAQ sur CX Cloud Agent

Table des matières

Introduction

Déploiement

- Q. La redirection d'URL tocloudfront.net est-elle un comportement attendu lors de la connexion au domaine principal du cloud CX ?
- Q. Avec l'option « Réinstaller », l'utilisateur peut-il déployer le nouvel agent cloud CX avec une nouvelle adresse IP ?
- Q. Quels formats de fichier sont disponibles pour l'installation ?
- Q. Dans quel environnement l'installable peut-il être déployé ?
- Q. CX Cloud Agent peut-il détecter une adresse IP dans un environnement DHCP ?
- Q. CX Cloud Agent prend-il en charge les configurations IPv4 et IPv6 ?
- Q. Pendant la configuration IP, l'adresse IP est-elle validée ?
- Q. Combien de temps faut-il pour le déploiement OVA et la configuration IP ?
- Q. Existe-t-il des limites en ce qui concerne les types de matériel ?
- Q. Le code d'appariement peut-il être généré à tout moment ?
- Q. Quelles sont les exigences en matière de bande passante entre Cisco DNA Centers (jusqu'à 10 clusters ou 20 non-clusters) et CX Cloud Agent ?
- Q. Comment accéder aux syslog de l'agent pour surveiller la machine virtuelle (VM) de l'agent cloud CX ?

Versions et correctifs

- Q. Quels sont les différents types de versions répertoriés pour la mise à niveau de CX Cloud Agent ?
- Q. Où trouver la dernière version de CX Cloud Agent et comment mettre à niveau CX Cloud Agent existant ?

Configuration de l'authentification et du proxy

- Q. Quel est l'utilisateur par défaut de l'application CX Cloud Agent ?
- Q. Comment le mot de passe est-il défini pour l'utilisateur par défaut ?
- Q. Existe-t-il une option permettant de réinitialiser le mot de passe après le jour 0 ?
- Q. Quelles sont les politiques de mot de passe pour configurer CX Cloud Agent ?
- Q. Comment puis-je confirmer l'accessibilité de Secure Shell (SSH) à un périphérique à partir de CX Cloud Agent ?
- Q. Comment puis-je confirmer l'accessibilité SNMP à un périphérique à partir de CX Cloud Agent ?
- Q. Comment définir le mot de passe Grub ?
- Q. Quel est le délai d'expiration du mot de passe xcadminpassword ?
- Q. Le système désactive-t-il le compte après plusieurs tentatives de connexion infructueuses ?
- Q. Comment générer une phrase de passe ?
- Q. L'hôte proxy prend-il en charge à la fois le nom d'hôte et IP ?

Protocole SSH (Secure Shell)

- Q. Quels sont les chiffrements pris en charge par l'interpréteur de commandes ssh ?
- Q. Comment puis-je me connecter à la console ?

Q. Les connexions SSH sont-elles consignées ?

Q. Quel est le délai d'inactivité de la session ?

Ports et services

Q. Quels ports restent ouverts sur CX Cloud Agent ?

Connexion de CX Cloud Agent avec Cisco DNA Center et d'autres ressources

Q. Quel est l'objectif et la relation entre Cisco DNA Center et CX Cloud Agent ?

Q. Où les utilisateurs peuvent-ils fournir des informations détaillées sur Cisco DNA Center concernant CX Cloud Agent ?

Q. Combien de centres Cisco DNA peuvent être ajoutés ?

Q. Comment supprimer un Cisco DNA Center connecté de CX Cloud Agent ?

Q. Quel rôle l'utilisateur de Cisco DNA Center peut-il jouer ?

Q. Comment les modifications apportées à CX Cloud Agent sont-elles reflétées dans les informations d'identification du DNA Center connecté ?

Q. Comment les informations relatives au Cisco DNA Center et aux fichiers d'amorçage sont-elles stockées dans CX Cloud Agent ?

Q. Existe-t-il des limitations à la saisie de plages IP lors de l'ajout d'autres ressources ?

Q. Un sous-réseau public peut-il être utilisé pour le déploiement de CX Cloud Agent v2.4 pour le cluster et le sous-réseau personnalisé de service ?

Q. À quelle fréquence l'opération de redécouverte peut-elle être lancée ?

Q. Quel est le workflow d'ajout de « Autres ressources en tant que source de données » lors du téléchargement d'un fichier d'amorçage ?

Q. Quel type de cryptage est utilisé lors de l'accès à l'API Cisco DNA Center à partir de CX Cloud Agent ?

Q. Quelles sont les opérations effectuées par CX Cloud Agent sur l'agent Cisco DNA Center Cloud intégré ?

Q. Quelles données par défaut sont collectées à partir de Cisco DNA Center et téléchargées sur le serveur principal ?

Q. Quelles données supplémentaires sont collectées à partir de Cisco DNA Center et téléchargées vers le back-end Cisco ?

Q. Comment les données d'inventaire sont-elles téléchargées vers le serveur principal ?

Q. Quelle est la fréquence de chargement des stocks ?

Q. L'utilisateur peut-il replanifier l'inventaire ?

Q. Quand le délai d'attente de connexion se produit-il entre Cisco DNA Center et Cloud Agent ?

Analyse de diagnostic utilisée par l'agent CX Cloud

Q. Quelles commandes d'analyse sont exécutées sur le périphérique ?

Q. Où les résultats de l'analyse sont-ils stockés et profilés ?

Q. Les doublons (par nom d'hôte ou IP) dans Cisco DNA Center sont-ils ajoutés au diagnostic scan lorsque la source Cisco DNA Center est branchée ?

Q. Que se passe-t-il lorsque l'une des commandes scans échoue ?

Q. Que se passe-t-il lorsque plusieurs balayages se chevauchent ?

Journaux du système de l'agent CX Cloud

Q. Quelles informations de santé sont envoyées au portail Cloud CX ?

Q. Quels sont les détails du système et du matériel collectés ?

Q. Comment les données d'intégrité sont-elles envoyées au back-end ?

Q. Quelle est la politique de conservation des journaux de données d'intégrité de CX Cloud Agent dans le back-end ?

Q. Quels types de téléchargements sont disponibles ?

Dépannage

Réponses aux échecs de collecte

Réponses aux échecs de l'analyse diagnostique

Introduction

Ce document inclut une foire aux questions et des scénarios de dépannage que les utilisateurs peuvent rencontrer lorsqu'ils travaillent avec CX Cloud Agent.

Déploiement

Q. La redirection d'URL vers cloudfront.net est-elle un comportement attendu lors de la connexion au domaine principal du cloud CX ?

R. Oui, pour certains scénarios de déploiement spécifiques, la redirection vers cloudfront.net est attendue. L'accès sortant doit être autorisé avec la redirection activée sur le port 443 pour ces FQDN.

Q. Avec l'option « Réinstaller », l'utilisateur peut-il déployer le nouvel agent cloud CX avec une nouvelle adresse IP ?

A. Oui

Q. Quels sont les formats de fichiers disponibles pour l'installation ?

A. OVA et VHD

Q. Dans quel environnement l'installable peut-il être déployé ?

A. Pour OVA

- VMware ESXi version 5.5 ou ultérieure
- Oracle Virtual Box 5.2.30 ou version ultérieure

Pour VHD

- Hyperviseur Windows 2012 à 2016

Q. CX Cloud Agent peut-il détecter une adresse IP dans un environnement DHCP ?

R. Oui, l’attribution de l’adresse IP pendant la configuration IP est détectée. Cependant, le changement d'adresse IP prévu pour CX Cloud Agent à l'avenir n'est pas pris en charge. Il est recommandé aux clients de réserver l'adresse IP pour CX Cloud Agent dans leur environnement DHCP.

Q. CX Cloud Agent prend-il en charge les configurations IPv4 et IPv6 ?

R. Non, seul IPV4 est pris en charge.

Q. Pendant la configuration IP, l’adresse IP est-elle validée ?

R. Oui, la syntaxe d’adresse IP et l’attribution d’adresses IP en double sont validées.

Q. Combien de temps faut-il pour le déploiement OVA et la configuration IP ?

R. Le déploiement OVA dépend de la vitesse du réseau qui copie les données. La configuration IP prend environ 8 à 10 minutes, y compris la création de Kubernetes et de conteneurs.

Q. Existe-t-il des limites en ce qui concerne les types de matériel ?

R. La machine hôte sur laquelle OVA est déployé doit répondre aux exigences fournies dans le cadre de la configuration du portail CX. L’agent cloud CX a été testé avec VMware/Virtual box fonctionnant sur un matériel équipé de processeurs Intel Xeon E5 avec un ratio vCPU à CPU fixé à 2: 1. Si un processeur moins puissant ou un rapport plus élevé est utilisé, les performances peuvent se dégrader.

Q. Le code d'appariement peut-il être généré à tout moment ?

R. Non, le code de jumelage ne peut être généré que lorsque l'agent cloud CX n'est pas enregistré.

Q. Quelles sont les exigences en matière de bande passante entre Cisco DNA Centers (pour 10 clusters ou 20 non-clusters maximum) et CX Cloud Agent ?

R.La bande passante n'est pas une contrainte lorsque CX Cloud Agent et Cisco DNA Center se trouvent sur le même réseau LAN/WAN dans l'environnement du client. La bande passante réseau minimale requise est de 2,7 Mbit/s pour les collections d'inventaire de 5 000 périphériques +13000 points d'accès pour une connexion d'agent à Cisco DNA Center. Si les syslogs sont collectés pour des analyses de niveau 2, la bande passante minimale requise est de 3,5 Mbits/s pour 5 000 périphériques +13000 points d'accès pour l'inventaire, 5 000 syslogs et 2 000 périphériques pour les analyses, tous exécutés en parallèle à partir de CX Cloud Agent.

Q. Comment accéder aux syslogs de l'agent pour surveiller la machine virtuelle (VM) de l'agent cloud CX ?

R. Les journaux système de la machine virtuelle de l'agent sont accessibles à partir de la connexion de la machine virtuelle locale via les deux chemins suivants :

/var/log/syslog.1 (accessible via les connexions cxcadmin et cxcroot)

/var/log/syslog (accès via root)

Versions et correctifs

Q. Quels sont les différents types de versions répertoriés pour la mise à niveau de

CX Cloud Agent ?

R. Voici l'ensemble des versions de CX Cloud Agent qui sont répertoriées :

- Ax0 (où x est la plus récente version majeure des fonctionnalités de production, exemple : 1.3.0)
- A.x.y (où A.x.0 est obligatoire et une mise à niveau incrémentielle doit être lancée, x est la dernière version de la fonctionnalité majeure de production et y est le dernier correctif de mise à niveau actif, par exemple : 1.3.1)
- A.x.y-z (où A.x.0 est obligatoire et une mise à niveau incrémentielle doit être initiée, x est la dernière version majeure de la fonctionnalité de production, et y est le dernier correctif de mise à niveau actif, et z est le correctif ponctuel qui est un correctif instantané pour une très courte période de temps, par exemple : 1.3.1-1)

où A est une version à long terme répartie sur 3 à 5 ans.

Q. Où trouver la dernière version de CX Cloud Agent et comment mettre à niveau CX Cloud Agent existant ?

R. Pour localiser et mettre à niveau vers la dernière version de CX Cloud Agent :

1. Connectez-vous au portail Cloud CX et accédez au Centre d'administration. La fenêtre Sources de données s'ouvre.
2. Sélectionnez CX Cloud Agent pour ouvrir la vue détaillée et cliquez sur l'onglet Software.
3. Faites une sélection dans la liste déroulante Choisir la version du logiciel à mettre à niveau et cliquez sur Installer la mise à jour.

Configuration de l’authentification et du proxy

Q. Quel est l'utilisateur par défaut de l'application CX Cloud Agent ?

A. cxcadmin.

Q. Comment le mot de passe est-il défini pour l'utilisateur par défaut ?

R. Les mots de passe sont définis lors de la configuration du réseau.

Q. Existe-t-il une option permettant de réinitialiser le mot de passe après le jour 0 ?

R. Aucune option spécifique n'est fournie par CX Cloud Agent pour réinitialiser le mot de passe, mais vous pouvez utiliser les commandes Linux pour réinitialiser le mot de passe pour cxcadmin.

Q. Quelles sont les politiques de mot de passe pour configurer CX Cloud Agent ?

R. Les stratégies de mot de passe sont :

- Âge maximal (durée) défini sur 90 jours

- Âge minimum (durée) défini sur 8 jours
- Longueur maximale : 127 caractères
- Au moins un caractère majuscule et un caractère minuscule doivent être inclus
- Doit contenir au moins un caractère spécial (par exemple, !$%^&*()_+|~-=\`{}[]:";'<>?,/)
- Les caractères suivants ne sont pas autorisés
    - Caractères spéciaux de 8 bits (par exemple, £, √Å √´, √¥, √ë,, √ü)
    - Espaces
- Ne doit pas être le dernier 10 mots de passe récemment utilisés
- Ne doit pas contenir d'expression régulière
- Ne doit pas contenir les mots ou dérivés suivants : cisco, sanjose et sanfran

Q. Comment confirmer l'accessibilité de Secure Shell (SSH) à un périphérique à partir de CX Cloud Agent ?

A. Pour confirmer l'accessibilité SSH :

1. Connectez-vous en tant qu'utilisateur cxcroot.
2. Exécutez la commande suivante pour activer le port SSH dans Iptables :

   Iptables -A OUTPUT -p tcp -m tcp —dport 22 -j ACCEPT

3. Exécutez la commande suivante pour confirmer l'accessibilité SSH :

   ssh user@ip-address:port

Pour désactiver les ports SSH activés ci-dessus dans CX Cloud Agent :

1. Exécutez la commande suivante pour obtenir le numéro de ligne du port SSH activé dans les iptables :

   iptables -L OUTPUT —numéro-ligne | dpt grep | grep ssh | awk '{print $1}'

2. Exécutez la commande suivante pour supprimer le numéro de ligne obtenu :

   iptables -L OUTPUT <Numéro de ligne>

Q. Comment puis-je confirmer l'accessibilité SNMP à un périphérique à partir de CX Cloud Agent ?

R. Pour confirmer l'accessibilité SNMP :

1. Connectez-vous en tant qu'utilisateur cxcroot.
2. Exécutez la commande suivante pour activer les ports SNMP dans les Iptables :

   iptables -A OUTPUT -p udp -m udp —dport 161 -j ACCEPT

   iptables -A OUTPUT -p udp -m udp —dport 161 -j ACCEPT

3. Exécutez la commande snmpwalk/snmpget suivante pour confirmer l'accessibilité SNMP :

snmpwalk -v2c -c adresse IP cisco

Pour désactiver les ports SNMP activés ci-dessus dans CX Cloud Agent :

1. Exécutez la commande suivante pour obtenir les numéros de ligne des ports SNMP activés (deux numéros de ligne sont générés en réponse) :

iptables -L OUTPUT —numéro-ligne | dpt grep | grep ssh | awk '{print $1}'

2. Exécutez la commande suivante pour supprimer les numéros de ligne (dans l'ordre décroissant) :

iptables -L OUTPUT <Numéro de ligne2>

iptables -L OUTPUT <Numéro de ligne1>

Q. Comment définir le mot de passe Grub ?

R. Pour définir le mot de passe Grub :

1. Exécutez .ssh en tant que cxcroot et fournissez le jeton [contactez l'équipe d'assistance pour obtenir le jeton cxcroot].
2. Exécutez sudo su pour fournir le même jeton.
3. Exécutez la commande grub-mkpasswd-pbkdf2 et définissez le mot de passe Grub. Le hachage du mot de passe fourni sera imprimé, copiez le contenu.
4. vi dans le fichier /etc/grub.d/00_header.
5. Accédez à la fin du fichier et remplacez la sortie de hachage suivie du contenu password_pbkdf2 root ***** par le hachage obtenu pour le mot de passe obtenu à l’étape 3.
6. Enregistrez le fichier à l'aide de la commande : wq ! .
7. Exécutez la commande update-grub.

Q. Quel est le délai d'expiration du mot de passe cxcadmin ?

R. Le mot de passe expire dans 90 jours.

Q. Le système désactive-t-il le compte après plusieurs tentatives de connexion infructueuses ?

R. Oui, le compte est désactivé après cinq (5) tentatives consécutives infructueuses. La période de verrouillage est de 30 minutes.

Q. Comment générer une phrase de passe ?

A. Pour générer une phrase de passe :

1. Exécutez .ssh et connectez-vous en tant qu'utilisateur cxcadmin.
2. Exécutez la commande remoteaccount cleanup -f.
3. Exécutez la commande remoteaccount create.

Q. L’hôte proxy prend-il en charge le nom d’hôte et IP ?

R. Oui, mais pour utiliser le nom d'hôte, l'utilisateur doit fournir l'adresse IP DNS (Domain Name Server) lors de la configuration du réseau.

Protocole SSH (Secure Shell)

Q. Quels sont les chiffrements pris en charge par l’interpréteur de commandes SSH ?

R. Les chiffrements suivants sont pris en charge :

- chacha20-poly1305@openssh.com
- aes256-gcm@openssh.com
- aes128-gcm@openssh.com
- aes256-ctr
- aes192-ctr
- aes128-ctr

Q. Comment puis-je me connecter à la console ?

A. Pour vous connecter :

1. Connectez-vous en tant qu'utilisateur cxcadmin
2. Fournissez le mot de passe cxcadmin

Q. Les connexions SSH sont-elles consignées ?

R. Oui, ils sont consignés dans le fichier "var/logs/audit/audit.log".

Q. Quel est le délai d’inactivité de la session ?

R. Le délai d'expiration de la session SSH se produit si CX Cloud Agent est inactif pendant cinq (5) minutes.

Ports et services

Q. Quels ports restent ouverts sur CX Cloud Agent ?

R. Les ports suivants sont disponibles :

- Port sortant : l'agent cloud CX déployé peut se connecter au back-end Cisco comme indiqué dans le tableau sur le port HTTPS 443 ou via un proxy pour envoyer des données à Cisco comme indiqué dans le tableau ci-dessous. L’agent CX Cloud déployé peut se connecter au centre Cisco DNA sur le port HTTPS 443.

AMÉRIQUE	EMEA	APJC
cloudsso.cisco.com	cloudsso.cisco.com	cloudsso.cisco.com
api-cx.cisco.com	api-cx.cisco.com	api-cx.cisco.com
agent.us.csco.cloud	agent.emea.csco.cloud	agent.apjc.csco.cloud
ng.acs.agent.us.csco.cloud	ng.acs.agent.emea.csco.cloud	ng.acs.agent.apjc.csco.cloud

Remarque : en plus des domaines répertoriés, lorsque les clients EMEA ou APJC réinstallent CX Cloud Agent, le domaine agent.us.csco.cloud doit être autorisé dans le pare-feu du client.
Le domaine agent.us.csco.cloud n'est plus nécessaire après une réinstallation réussie.

Remarque : assurez-vous que le trafic de retour doit être autorisé sur le port 443.

- Inbound port: pour la gestion locale de CX Cloud Agent, 514 (Syslog) et 22 (ssh) doivent être accessibles. Les clients doivent autoriser le port 443 de leur pare-feu à recevoir des données du cloud CX.

Connexion de CX Cloud Agent avec Cisco DNA Center et d'autres ressources

Q. Quel est l'objectif et la relation entre Cisco DNA Center et CX Cloud Agent ?

R. Cisco DNA Center est l'agent cloud qui gère les périphériques réseau des locaux du client. CX Cloud Agent collecte les informations d'inventaire des périphériques à partir du Cisco DNA Center configuré et télécharge les informations d'inventaire disponibles dans la **vue des ressources** de CX Cloud.

Q. Où les utilisateurs peuvent-ils fournir des informations détaillées sur Cisco DNA Center concernant CX Cloud Agent ?

R. Pendant la configuration de l'agent cloud du jour 0 - CX, les utilisateurs peuvent ajouter les détails de Cisco DNA Center à partir du portail Cloud CX. Pendant les opérations du jour N, les utilisateurs peuvent ajouter des centres Cisco DNA supplémentaires à partir de Admin Settings > Data Source.

Q. Combien de centres Cisco DNA peuvent être ajoutés ?

R. Il est possible d'ajouter dix (10) clusters Cisco DNA Center ou 20 clusters non Cisco DNA Center.

Q. Comment **supprimer un Cisco DNA Center connecté de CX Cloud Agent ?**

R. Pour retirer un Cisco DNA Center connecté de CX Cloud Agent, contactez le Centre d'assistance technique (TAC) pour ouvrir un dossier

d'assistance à partir du portail CX Cloud.

Q. Quel rôle l’utilisateur de Cisco DNA Center peut-il jouer ?

R. Le rôle d'utilisateur peut être **admin** ou **observer**.

Q. Comment **les modifications apportées à CX Cloud Agent sont-elles reflétées dans les informations d'identification du DNA Center connecté** ?

R. Exécutez la commande *cxcli agent modifyController* à partir de la console CX Cloud Agent :

Contactez le support pour tout problème lors de la mise à jour des informations d'identification Cisco DNA Center.

Q. Comment les détails de Cisco DNA Center **et des fichiers d'amorce** sont-ils stockés dans CX Cloud Agent ?

R. Toutes les données, y compris les informations d'identification des contrôleurs connectés à CX Cloud Agent (par exemple, Cisco DNA Center) et les ressources connectées directement (par exemple, via un fichier d'amorce, une plage IP), sont chiffrées à l'aide de AES-256 et stockées dans la base de données CX Cloud Agent qui est protégée par un ID utilisateur et un mot de passe sécurisés.

Q. **Existe-t-il des restrictions à la saisie de plages IP lors de l’ajout d’autres ressources ?**

R. Oui, CX Cloud Agent n'est pas en mesure de gérer les opérations de détection pour des plages d'adresses IP de sous-réseau plus étendues. Cisco recommande d'utiliser des plages de sous-réseaux réduites limitées à 10 000 adresses IP.

Q. **Un sous-réseau public peut-il être utilisé pour le déploiement de CX Cloud Agent v2.4 pour le cluster et le sous-réseau personnalisé de service ?**

R. Cisco déconseille l'utilisation d'un sous-réseau IP public pour les raisons suivantes :

- **Risques de sécurité** : les adresses IP publiques exposent les clusters et les services à Internet, augmentant ainsi le risque d'accès non autorisé, d'attaques et de violations potentielles des données.
- **Conflits d'adresses IP** : l'utilisation de sous-réseaux IP publics peut entraîner des conflits d'adresses IP, en particulier si les mêmes adresses IP sont attribuées ailleurs sur Internet, ce qui entraîne des problèmes de connectivité et un comportement inattendu.
- **Complexité de la configuration réseau** : la gestion des stratégies réseau, des règles de pare-feu et du routage devient plus complexe lorsque vous traitez des adresses IP publiques. Cela peut entraîner des erreurs de configuration et une surcharge de maintenance accrue.

Un sous-réseau IP public peut être utilisé s’il est attribué uniquement à une organisation du client et configuré sur le réseau du client.

Q. **À quelle fréquence l'opération de redécouverte peut-elle être lancée ?**

R. L'opération de redécouverte ne doit être effectuée que si le réseau du client a été modifié (par exemple, après l'ajout ou la suppression de périphériques sur le réseau).

Q. **Quel est le workflow d'ajout de « Autres ressources en tant que source de données » lors du téléchargement d'un fichier d'amorçage ?**

R. Le workflow est le suivant :

- Téléchargez le fichier d'amorçage dans CX Cloud.
- Le fichier de départ est temporairement stocké dans le compartiment Cisco Cloud AWS S3 (avec le cryptage SSE activé).
- Le fichier d'amorçage est envoyé à l'agent cloud CX et le fichier d'amorçage est supprimé du compartiment S3
- CX Cloud Agent traite les entrées du fichier d'amorce et chiffre les informations d'identification à l'aide d'une clé AES 256 (cette clé est unique pour chaque CX Cloud Agent). Ces informations d'identification chiffrées sont stockées dans la base de données CX Cloud Agent.
- Le fichier d'amorçage est supprimé de CX Cloud Agent une fois que les entrées du fichier d'amorçage sont traitées.

Q. Quel type de cryptage est utilisé lors de l'accès à l'API Cisco DNA Center à partir de CX Cloud Agent ?

R. HTTPS sur TLS 1.2 est utilisé pour la communication entre Cisco DNA Center et CX Cloud Agent.

Q. Quelles sont les opérations effectuées par CX Cloud Agent sur l'agent Cisco DNA Center Cloud intégré ?

R. CX Cloud Agent collecte des données sur les périphériques réseau auprès de Cisco DNA Center et utilise l'interface du canal d'exécution des commandes Cisco DNA Center pour communiquer avec les périphériques finaux et exécuter les commandes CLI (commande show). Aucune commande de modification de configuration n’est exécutée.

Q. Quelles données par défaut sont collectées à partir de Cisco DNA Center et téléchargées sur le serveur principal ?

A.

- Entité de réseau
- Modules
- show version
- configuration
- Informations sur l’image du périphérique
- Étiquettes

Q. Quelles données supplémentaires sont collectées à partir de Cisco DNA Center et téléchargées vers le back-end Cisco ?

R. Reportez-vous à ce document pour plus d'informations.

Q. Comment les données d'inventaire sont-elles téléchargées vers le serveur principal ?

R. CX Cloud Agent télécharge les données d'inventaire via le protocole TLS 1.2 vers le serveur principal Cisco.

Q. Quelle est la fréquence de chargement des stocks ?

R. La collecte est déclenchée selon le planning défini par l'utilisateur et est téléchargée vers le serveur principal Cisco.

Q. L'utilisateur peut-il replanifier l'inventaire ?

R. Oui, une option est disponible dans **Centre d'administration > Sources de données** pour modifier les informations de planification.

Q. Quand le délai d'attente de connexion se produit-il entre Cisco DNA Center et Cloud Agent ?

R. Les délais d'attente sont classés comme suit :

- Pour la connexion initiale, le délai d'attente est de 300 secondes maximum. Si la connexion n'est pas établie entre Cisco DNA Center et Cloud Agent dans un délai maximal de cinq (5) minutes, la connexion est interrompue.
- Pour les mises à jour récurrentes, standard ou non : le délai de réponse est de 1 800 secondes. Si la réponse n'est pas reçue ou ne peut pas être lue dans les 30 minutes, la connexion est interrompue.

Analyse de diagnostic utilisée par l’agent CX Cloud

Q. Quelles commandes d’analyse sont exécutées sur le périphérique ?

R. Les commandes qui doivent être exécutées sur le périphérique pour le balayage sont déterminées dynamiquement pendant le processus de balayage. L'ensemble de commandes peut changer au fil du temps, même pour le même périphérique (et ne contrôle pas l'analyse diagnostique).

Q. Où les résultats de l'analyse sont-ils stockés et profilés ?

R. Les résultats analysés sont stockés et profilés dans le back-end Cisco.

Q. Les doublons (par nom d’hôte ou IP) dans Cisco DNA Center sont-ils ajoutés au diagnostic scan lorsque la source Cisco DNA Center est branchée ?

R. Non, les doublons sont filtrés de sorte que seuls les périphériques uniques soient extraits.

Q. Que se passe-t-il lorsque l’une des commandes scans échoue ?

R. L'analyse du périphérique s'arrête complètement et est marquée comme ayant échoué.

Q. **Que se passe-t-il lorsque plusieurs balayages se chevauchent ?**

R. L'exécution simultanée de plusieurs analyses de diagnostic peut ralentir le processus d'analyse et entraîner des échecs d'analyse. Cisco recommande de planifier des analyses de diagnostic ou de lancer des analyses à la demande au moins 6 à 7 heures à l'écart des calendriers de collecte d'inventaire afin qu'elles ne se chevauchent pas.

Journaux du système de l’agent CX Cloud

Q. Quelles informations de santé sont envoyées au portail Cloud CX ?

R. Journaux d'application, état du Pod, détails de Cisco DNA Center, journaux d'audit, détails du système et détails du matériel.

Q. Quels sont les détails du système et du matériel collectés ?

A. Exemple de résultat :

system_details":{
"os_details":{
"containerRuntimeVersion":"docker://19.3.12",
"kernelVersion":"5.4.0-47-generic",
"kubeProxyVersion":"v1.15.12",
"kubeletVersion":"v1.15.12",
"machineID":"81edd7df1c1145e7bcc1ab4fe778615f",
"operatingSystem":"linux",
"osImage" :"Ubuntu 20.04.1 LTS",
"systemUID" :"42002151-4131-2ad8-4443-8682911bdadb"
},
"hardware_details":{
"total_cpu":"8",
"cpu_used":"12.5%",
"total_memory":"16007MB",
"free_memory" :"994 Mo",
"hdd_size":"214G",
"free_hdd_size":"202G"
}
}
}

Q. Comment les données d'intégrité sont-elles envoyées au back-end ?

R. Avec CX Cloud Agent, le service d'intégrité (facilité de maintenance) transmet les données au back-end Cisco.

Q. Quelle est la politique de conservation des journaux de données d'intégrité de CX Cloud Agent dans le back-end ?

R. La politique de conservation des journaux de données d'intégrité de CX Cloud Agent dans le back-end est de 120 jours.

Q. Quels types de téléchargements sont disponibles ?

A.

- Chargement des stocks

- Téléchargement Syslog
- Chargement de l'état de l'agent, y compris du chargement de l'état

    1. Santé des services - Toutes les cinq (5) minutes
    2. Podlog - Toutes les (1) heures
    3. Journal d'audit - Toutes les (1) heures

Dépannage

Problème : impossible d'accéder à l'adresse IP configurée.

Solution : exécutez ssh en utilisant l'IP configurée. Si la connexion expire, la raison possible est une mauvaise configuration IP. Dans ce cas, procédez à une réinstallation en configurant une adresse IP valide. Vous pouvez le faire via le portail avec l'option de réinstallation fournie dans la Admin Centerpage.

Problème : comment puis-je vérifier que les services sont opérationnels après l'enregistrement ?

Solution : suivez les étapes ci-dessous pour vérifier que les pods sont opérationnels :

- ssh à l'adresse IP configurée comme cxcadmin
- Indiquez le mot de passe
- Exécutez la commande *kubectl get pods*

Les modules peuvent être dans n'importe quel état (En cours d'exécution, Initialisation ou Création de conteneur). Au bout de 20 minutes, les modules doivent être à l'état En cours d'exécution.

Si state is **n'est pas en cours d'exécution** ou **Pod Initializing**, vérifiez la description pod à l'aide de la commande *kubectl description pod <podname>*.

Le résultat contient des informations sur l'état du pod.

Problème : comment vérifier si l'intercepteur SSL est désactivé au niveau du proxy client ?
Solution : exécutez la commande curl indiquée ici pour vérifier la section du certificat du serveur. La réponse contient les détails du certificat du serveur web console.

curl -v —header 'Autorisation : xxxxxx de base' https://concsoweb-prd.cisco.com/

* Certificat de serveur :

* sujet : C=US ; ST=California ; L=San Jose ; O=Cisco Systems, Inc. ; CN=concsoweb-prd.cisco.com

* date de début : 16 février 11:55:11 2021 GMT

* date d'expiration : 16 février 12:05:00 2022 GMT

* subjectAltName : l'hôte « concsoweb-prd.cisco.com » correspond à « concsoweb-prd.cisco.com » du certificat

* émetteur : C=US ; O=HydrantID (Avalanche Cloud Corporation) ; CN=HydrantID SSL CA G3

* Vérification du certificat SSL OK.

> GET / HTTP/1.1

Problème : les commandes kubectl ont échoué et l'erreur est « La connexion au serveur X.X.X.X:6443 a été refusée - avez-vous spécifié le bon hôte ou port »
Solution :

- Vérifiez la disponibilité des ressources. [exemple : CPU, mémoire].
- Attendez que le service Kubernetes démarre.

Problème : comment obtenir les détails de l'échec de la collecte pour une commande/un périphérique ?

Solution :

- Exécutez kubectl get pods et obtenez le nom de la zone de collecte.
- Exécutez kubectl logs <collectionPodName> pour obtenir les détails spécifiques à la commande/au périphérique.

Problème : la commande kubectl ne fonctionne pas avec l'erreur "[authentication.go : 64] Impossible d'authentifier la demande en raison d'une erreur : [x509 : le certificat a expiré ou n'est pas encore valide, x509 : le certificat a expiré ou n'est pas encore valide]"

Solution : exécutez les commandes indiquées ici en tant qu'utilisateur *cxcroot*

rm /var/lib/rancher/k3s/server/tls/dynamic-cert.json
systemctl restart k3s
kubectl —insecure-skip-tls-verify=true delete secret -n kube-system k3s-service
systemctl restart k3s

Réponses aux échecs de collecte

La collecte peut avoir échoué en raison de toute contrainte ou de tout problème rencontré avec le contrôleur ajouté ou les périphériques présents

dans le contrôleur.

Le tableau ci-dessous contient l'extrait d'erreur pour les cas d'utilisation observés sous le microservice Collection pendant le processus de collecte.

Scénario	Extrait de journal dans le micro-service de collecte
Si le périphérique demandé est introuvable dans le centre Cisco DNA	{ "commande" : "show version", "status" : "Failed", "commandResponse" : "", "errorMessage" : " Aucun périphérique trouvé portant l'id 02eb08be-b13f-4d25-9d63-eaf4e882f71a " }
Si le périphérique demandé n'est pas accessible à partir du centre Cisco DNA	{ "commande" : "show version", "status" : "Failed", "commandResponse" : "", "errorMessage" : "Une erreur s'est produite lors de l'exécution de la commande : show version\nErreur de connexion au périphérique [Hôte : 172.21.137.221:22]Pas de route vers l'hôte : Pas de route vers l'hôte " }
Si le périphérique demandé n'est pas accessible à partir du centre Cisco DNA	{ "commande" : "show version", "status" : "Failed", "commandResponse" : "", "errorMessage" : "Une erreur s'est produite lors de l'exécution de la commande : show version\nErreur de connexion au périphérique [Hôte : X.X.X.X]Délai de connexion dépassé : /X.X.X.X:22 : Délai de connexion dépassé : /X.X.X.X:22" }
Si la commande demandée n'est pas disponible dans le périphérique	{ "command" : "show run-config", "status" : "Success", "commandResponse" : " Une erreur s'est produite lors de l'exécution de la commande : show run-config\n\nshow run-config\n ^\n% Entrée non valide détectée au niveau du marqueur \u0027^\u0027.\n\nXXCT5760#", "errorMessage" : ""

Scénario	Extrait de journal dans le micro-service de collecte
	}

Si le périphérique demandé ne dispose pas de SSHv2 et que Cisco DNA Center tente de le connecter à SSHv2	{
	"commande" : "show version",
	"status" : "Failed",
	"commandResponse" : "",
	"errorMessage" : "Une erreur s'est produite lors de l'exécution de la commande : show version\nSSH2 channel closed : Remote party uses incompatible protocol, it is not SSH-2 compatible."
	}

Si la commande est désactivée dans le micro-service de collecte	{
	"commande" : "config paging disable",
	"status" : "Command_Disabled",
	"commandResponse" : "La collection de commandes est désactivée",
	"errorMessage" : ""
	}

Si la tâche du gestionnaire de commandes échoue, et que l'URL de tâche n'est pas renvoyée par le centre Cisco DNA	{
	"commande" : "show version",
	"status" : "Failed",
	"commandResponse" : "",
	"errorMessage" : "La tâche du lanceur de commandes a échoué pour le périphérique %s. L'URL de la tâche est vide."
	}

Si la tâche de gestionnaire de commandes n'a pas pu être créée dans le centre Cisco DNA	{
	"commande" : "show version",
	"status" : "Failed",
	"commandResponse" : "",
	"errorMessage" : "La tâche du lanceur de commandes a échoué pour le périphérique %s, RequestURL : %s. Aucun détail de tâche."
	}

Si le microservice de collecte ne reçoit pas de réponse pour une requête Command Runner de	{ "commande" : "show version", "status" : "Failed",

Scénario	Extrait de journal dans le micro-service de collecte
Cisco DNA Center	"commandResponse" : "", "errorMessage" : "Échec de la tâche d'exécution de commande pour le périphérique %s, RequestURL : %s." }

Si le centre Cisco DNA ne termine pas la tâche dans le délai imparti configuré (cinq minutes par commande dans le micro-service de collecte)	{
	"commande" : "show version",
	"status" : "Failed",
	"commandResponse" : "",
	"errorMessage" : "Délai d'attente de l'opération. Échec de la tâche d'exécution de commande pour le périphérique %s, RequestURL : %s. Aucun détail de progression."
	}

Si la tâche Command Runner a échoué et que l'ID de fichier est vide pour la tâche soumise par Cisco DNA Center	{
	"commande" : "show version",
	"status" : "Failed",
	"commandResponse" : "",
	"errorMessage" : "La tâche du lanceur de commandes a échoué pour le périphérique %s, RequestURL : %s. L'ID de fichier est vide."
	}

Si la tâche Command Runner a échoué et que la balise d'ID de fichier n'est pas renvoyée par Cisco DNA Center	{
	"commande" : "show version",
	"status" : "Failed",
	"commandResponse" : "",
	"errorMessage" : "La tâche du lanceur de commandes a échoué pour le périphérique %s, RequestURL : %s. Aucun détail d'ID de fichier."
	}

Si l'appareil n'est pas admissible à l'exécution du gestionnaire de commandes	{
	"commande" : "config paging disable",
	"status" : "Failed",
	"commandResponse" : "",
	"errorMessage" : "Les périphériques demandés ne sont pas dans l'inventaire, essayez avec d'autres périphériques disponibles dans l'inventaire"
	}

Scénario	Extrait de journal dans le micro-service de collecte

Si le gestionnaire de commandes est désactivé pour l'utilisateur	{
	"commande" : "show version",
	"status" : "Failed",
	"commandResponse" : "",
	"errorMessage" : "{\"message\":\"Le rôle ne dispose pas d'autorisations valides pour accéder à l'API\"}\n"
	}

Réponses aux échecs de l'analyse diagnostique

Les échecs d'analyse et les causes peuvent provenir de l'un des composants répertoriés.

Lorsque les utilisateurs lancent une analyse à partir du portail, il arrive qu'elle se traduise par « failed: Internal server error ».

La cause du problème est l'un des composants répertoriés

- Point de contrôle
- Passerelle de données de réseau
- Connecteur
- Analyse de diagnostic
- Micro-service d'agent CX Cloud [devicemanager, collection]
- Centre Cisco DNA
- APIX
- Mashery
- Accès Ping
- IRONBANK
- IRONBANK GW
- Broker Big Data (BDB)

Pour afficher les journaux :

- Connectez-vous à la console CX Cloud Agent.

    - Exécuter.kubectl get pods
- Obtenez le nom du pod de la collection, du connecteur et de la facilité de maintenance.
- Pour vérifier les journaux de microservice de collecte, de connexion et de maintenance.

- Exécuter kubectl logs <collectionpodname>
- Exécuter kubectl logs <connector>
- Exécuter kubectl logs <servicability>

Le tableau ci-dessous affiche l'extrait d'erreur qui se produit dans les journaux du microservice de collecte et du microservice de servicabilité en raison des problèmes/contraintes avec les composants.

Scénario	Extrait de journal dans le micro-service de collecte

Le périphérique peut être accessible et pris en charge, mais les commandes à exécuter sur ce périphérique sont répertoriées en bloc sur le microservice Collection	{
	"commande" : "config paging disable",
	"status" : "Command_Disabled",
	"commandResponse" : "La collection de commandes est désactivée",
	}

Si le périphérique pour une analyse n'est pas disponible. Se produit dans un scénario, en cas de problème de synchronisation entre les composants tels que le portail, l'analyse diagnostique, le composant CX et le Cisco DNA Center	Aucun périphérique portant l'ID 02eb08be-b13f-4d25-9d63-eaf4e882f71a
Si le périphérique qui doit être analysé est occupé (dans un scénario), le même périphérique fait partie d'un autre travail, et aucune demande parallèle du centre Cisco DNA n'est traitée pour le périphérique	Tous les périphériques demandés sont déjà interrogés par le programme d'exécution de commandes dans une autre session. Essayez d'autres périphériques
Si le périphérique n'est pas pris en charge pour l'analyse	Les périphériques demandés ne sont pas dans l'inventaire, essayez avec d'autres périphériques

Scénario	Extrait de journal dans le micro-service de collecte
	disponibles dans l'inventaire
Si le périphérique tenté pour l'analyse est inaccessible	"Une erreur s'est produite lors de l'exécution de la commande : show udi\nErreur de connexion au périphérique [Hôte : x.x.x.x:22] Pas de route vers l'hôte : Pas de route vers l'hôte

Si le centre Cisco DNA n’est pas joignable à partir de l’agent Cloud ou si le microservice de collecte de l’agent Cloud ne reçoit pas de réponse à une demande du gestionnaire de commandes du centre Cisco DNA	{
	"commande" : "show version",
	"status" : "Failed",
	"commandResponse" : "",
	"errorMessage" : "Échec de la tâche d'exécution de commande pour le périphérique %s, RequestURL : %s."
	}

Scénario	Extrait de journal dans le micro-service de l’agent de point de contrôle
Si des détails de planification sont manquants dans la demande d’analyse	Échec de l'exécution de la requête {"message":"23502 : la valeur null de la colonne \"schedule\" ne respecte pas la contrainte non null"}
Si les détails du périphérique sont manquants dans la demande d’analyse	Impossible de créer la stratégie d'analyse. Aucun périphérique valide dans la demande
Si la connexion entre le CPA et la connectivité est interrompue	Échec de l'exécution de la requête
Si le périphérique qui doit être analysé n’est pas disponible dans les analyses de diagnostic	Impossible d'envoyer la demande à analyser. Raison = {\"message\":\"Le périphérique avec Hostname=x.x.x.x' est introuvable\"}

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.