Dépannage des erreurs Umbrella pour Active Directory et les VA

Table des matières

- Introduction
- Problème
- Environnement
- Résolution
  - Appareils virtuels
    - "Cette VA est enregistrée mais n'a jamais été synchronisée"
    - "Cette VA était en cours de synchronisation à un moment donné, mais s'est arrêtée depuis"
    - "Cette appliance virtuelle était précédemment connectée à un ou plusieurs connecteurs, mais n'est désormais connectée à aucun connecteur."
    - "Cet appareil virtuel est connecté à certains, mais pas à tous les connecteurs de ce site"
    - "Les requêtes DNS transmises par cette appliance virtuelle à Umbrella ne sont pas chiffrées"
    - "Aucun domaine local n'est configuré pour cette appliance virtuelle"
    - "Cette VA n'est pas redondante sur son site (plus de 2 VA requis par site)"
    - "Un grand pourcentage de requêtes DNS vers cette VA échoue"
  - Connecteurs AD
    - "Ce connecteur a été enregistré mais n'a jamais été synchronisé"
    - "Ce connecteur était en cours de synchronisation à un moment donné, mais s'est arrêté depuis"
    - "Ce connecteur n'a pas de VA ou pas de DC auquel se connecter."
    - "Ce connecteur n'a pas de contrôleur de domaine auquel se connecter"
    - "Le connecteur peut se connecter à un ou plusieurs contrôleurs de domaine, mais il ne s'y est pas encore connecté."
    - "Le connecteur est connecté à certains DC, mais pas à tous"
    - "Le connecteur a été connecté une fois, mais n'est actuellement connecté à aucun des contrôleurs de domaine disponibles"
    - "Le connecteur peut se connecter à un ou plusieurs VA, mais il ne s'y est pas encore connecté."
    - "Le connecteur signale des erreurs de délai d'attente lors de la tentative de connexion à certaines VA"
    - "Le connecteur est connecté à certains, mais pas à tous les VA"
    - "Le connecteur a été connecté une fois, mais n'est actuellement connecté à aucun des VA disponibles"
    - "Le connecteur ne synchronise pas les événements en parallèle avec les VA. Le traitement des événements peut être plus lent que prévu."
    - "Le connecteur signale des abandons lors d'une tentative d'envoi d'événements à certaines VA"
  - Contrôleurs de domaine
    - "Était connecté à un ou plusieurs connecteurs, mais n'est plus connecté à aucun"
    - "Ce contrôleur de domaine ne s'est jamais connecté à un connecteur"
    - "Ce contrôleur de domaine n'a pas de connecteurs auxquels se connecter"
    - "Ce contrôleur de domaine est connecté à certains connecteurs, mais pas à tous"
    - "L'état WMI de ce contrôleur de domaine est inactif. Le contrôleur de domaine ne répond pas à la connexion WMI du connecteur."
- Causes
- Autres informations utiles

Introduction

Ce document décrit le dépannage des erreurs Umbrella pour Active Directory et les appliances virtuelles.

Problème

Ce document présente les messages courants d'erreur, d'avertissement et d'information sur la page Sites et Active Directory et fournit des étapes de résolution.

Un ou plusieurs messages d'erreur, d'avertissement ou d'information apparaissent sur la page Paramètres Umbrella > Sites et Active Directory pour les appareils virtuels, les connecteurs Active Directory (AD) ou les contrôleurs de domaine (DC).

Environnement

La page Sites Umbrella et Active Directory se trouve dans Paramètres > Sites et Active Directory.

- Les composants concernés sont les appareils virtuels (VA), les connecteurs AD et les contrôleurs de domaine.
- La prise en charge de DNSCrypt est disponible dans VA version 1.5.x ou ultérieure.
- Si le connecteur est déployé sur Windows Server (WS) 2012 ou version ultérieure et que la synchronisation avec Umbrella a été interrompue, vérifiez qu'il exécute la version 1.6.31 ou version ultérieure.
- Les connecteurs version 1.6.31 ou ultérieure fonctionnent sur WS 2008/2008 R2 s'ils exécutent .NET version 4.5.2 ou ultérieure, mais le redéploiement sur un serveur pris en charge est recommandé.
- Cisco a annoncé la fin de vie de TLS (Transport Layer Security) 1.0/1.1. Les versions Windows non prises en charge (Windows Server 2008, 2008 R2 ou Windows 7) ne prennent pas en charge TLS 1.2 par défaut. Réinstallez le connecteur sur une version de serveur prise en charge (Windows Server 2012 ou version ultérieure).
- Pour envoyer des informations d'événement de connexion à une appliance virtuelle, un connecteur doit être installé sur le même site que le contrôleur de domaine (DC).
- Les sites doivent contenir au moins un élément de chaque type de composant lorsque le message le signale.
- Le service Umbrella Connector est testé pour prendre en charge 10 ressources (contrôleurs de domaine et appliances virtuelles) par processeur.
- Le service Umbrella Connector est testé pour prendre en charge environ 850 événements continus (sans limite matérielle) par seconde sur tous les contrôleurs de domaine d'un site Umbrella.

Résolution

Utilisez la section qui correspond au type de composant affiché dans Paramètres > Sites et AD, puis sélectionnez le texte exact du message.

- Appliances virtuelles : État de l'enregistrement/de la synchronisation VA, association du connecteur, DNSCrypt, domaines locaux, redondance et messages d'échec de requête DNS.
- Connecteurs AD : Enregistrement/état de synchronisation du connecteur, connectivité DC/VA, délais d'expiration, traitement parallèle et messages d'abandon d'événement.
- Contrôleurs de domaine : Messages d'association de connecteur et de connectivité WMI.

Appareils virtuels

"Cette VA est enregistrée mais n'a jamais été synchronisée"

1. Attendez jusqu'à 10 minutes que la synchronisation soit terminée.
2. Assurez-vous que les exigences réseau sont respectées. Voir Guide du flux de communication Active Directory : Connectors > Virtual Appliances > DC and the Cloud.
3. Si le problème persiste, collectez les journaux et ouvrez un dossier d'assistance.

"Cette VA était en cours de synchronisation à un moment donné, mais s'est arrêtée depuis"

Suivez ces étapes pour restaurer la synchronisation VA et confirmer la connectivité requise.

1. Si l'AV a été supprimé, supprimez-le du tableau de bord Umbrella : Instructions de retrait - Umbrella Insights.
2. Confirmez la configuration réseau requise. Voir Guide du flux de communication Active Directory : Connectors > Virtual Appliances > DC and the Cloud.
3. Ouvrez un dossier d'assistance si le problème persiste.

"Cette appliance virtuelle était précédemment connectée à un ou plusieurs connecteurs, mais n'est désormais connectée à aucun connecteur."

1. Si des connecteurs ont été supprimés, ignorez ce message et supprimez l'entrée Connector obsolète du tableau de bord.
2. Confirmez la configuration réseau requise. Voir Guide du flux de communication Active Directory : Connectors > Virtual Appliances > DC and the Cloud.

3. Ouvrez un dossier d'assistance si le problème persiste.

"Cet appareil virtuel est connecté à certains, mais pas à tous les connecteurs de ce site"

1. Si des connecteurs ont été supprimés, ignorez ce message et supprimez le connecteur du tableau de bord.
2. Confirmer les conditions préalables : Guide de l'utilisateur Virtual Appliance : Conditions préalables.
3. Collecter les journaux : Prise en charge des journaux du connecteur Active Directory.
4. Ouvrez un dossier d'assistance si le problème persiste.

"Les requêtes DNS transmises par cette appliance virtuelle à Umbrella ne sont pas chiffrées"

DNSCrypt chiffre les paquets DNS transférés de l'appliance virtuelle (VA) vers les résolveurs DNS publics Umbrella et est activé par défaut.

1. Vérifiez que l'appliance virtuelle exécute la version 1.5.x ou une version ultérieure. La prise en charge de DNSCrypt est disponible dans la version 1.5.x ou ultérieure. S'il n'existe qu'un seul VA et qu'il n'est pas mis à niveau, mettez-le à niveau : Mettre à jour les appliances virtuelles.
2. Examinez les politiques de pare-feu et d'inspection pour vous assurer que la sonde DNSCrypt sur le port 53 (UDP/TCP) n'est pas bloquée ou modifiée. Si un système de prévention des intrusions (IPS) ou un système de détection des intrusions (IDS) effectue une inspection approfondie des paquets et attend uniquement le trafic DNS, l'analyse peut échouer.
3. Pour les déploiements ASA (Adaptive Security Appliance), consultez les directives d'inspection des paquets référencées dans la documentation de déploiement.
4. Si l'avertissement persiste, collectez les journaux : Fournir une assistance avec les journaux du connecteur AD, puis ouvrir un dossier d'assistance.
5. Vérifiez que l'avertissement s'efface dans Paramètres > Sites et Active Directory pour l'appliance virtuelle concernée.

Plus de détails : Nouvel avertissement VA : Activation de DNSCrypt sur votre appliance virtuelle.

"Aucun domaine local n'est configuré pour cette appliance virtuelle"

1. Assurez-vous que les domaines locaux sont configurés : Transfert DNS local.

"Cette VA n'est pas redondante sur son site (plus de 2 VA requis par site)"

1. Installez un second VA pour une haute disponibilité. Reportez-vous à la documentation de déploiement de votre appliance virtuelle Umbrella pour obtenir des conseils sur l'exécution de deux appliances virtuelles par site.

"Un grand pourcentage de requêtes DNS vers cette VA échoue"

1. Collectez les journaux de la VA et du connecteur appropriés et ouvrez un dossier d'assistance.
2. Vérifiez que le taux d'échec de la requête DNS revient à la normale et que l'erreur disparaît dans Paramètres > Sites et Active Directory pour l'appliance virtuelle concernée.

Connecteurs AD

"Ce connecteur a été enregistré mais n'a jamais été synchronisé"

Procédez comme suit pour confirmer que la synchronisation initiale s'est terminée correctement :

1. Attendez jusqu'à 10 minutes que la synchronisation soit terminée.
2. Assurez-vous que les exigences réseau sont respectées : Intégrations des identités : Conditions préalables.
3. Collecter les journaux : Prise en charge des journaux du connecteur Active Directory.
4. Ouvrez un dossier d'assistance si le problème persiste.

"Ce connecteur était en cours de synchronisation à un moment donné, mais s'est arrêté depuis"

1. Assurez-vous que les exigences réseau sont respectées. Voir Guide du flux de communication Active Directory : Connectors > Virtual Appliances > DC and the Cloud.
2. Cisco a annoncé la fin de vie de TLS 1.0/1.1. Les versions Windows non prises en charge (Windows Server 2008, 2008 R2 ou Windows 7) ne prennent pas en charge TLS 1.2 par défaut. Réinstallez le connecteur sur une version de serveur prise en charge (Windows Server 2012 ou version ultérieure).
3. Si le connecteur est déployé sur WS 2012 ou version ultérieure et que la synchronisation avec Umbrella a été interrompue, assurez-vous qu'il exécute la version 1.6.31 ou version ultérieure.
4. Les connecteurs version 1.6.31 ou ultérieure fonctionnent sur WS 2008/2008 R2 s'ils exécutent .NET version 4.5.2 ou ultérieure, mais le redéploiement sur un serveur pris en charge est recommandé.
5. Collecter les journaux : Prise en charge des journaux du connecteur Active Directory.
6. Ouvrez un dossier d'assistance si le problème persiste.

"Ce connecteur n'a pas de VA ou pas de DC auquel se connecter."

1. Assurez-vous que le site contient au moins un composant de chaque type.
2. Consultez la documentation de configuration : Intégrations des identités : Conditions préalables et intégration à Active Directory > Étape 2 : Préparez votre environnement Active Directory.

"Ce connecteur n'a pas de contrôleur de domaine auquel se connecter"

1. Assurez-vous que le site contient au moins un composant de chaque type.
2. Consultez la documentation de configuration : Préparez Votre Environnement Active Directory.

"Le connecteur peut se connecter à un ou plusieurs contrôleurs de domaine, mais il ne s'y est pas encore connecté."

1. Attendez jusqu'à 10 minutes que la synchronisation soit terminée.
2. Assurez-vous que les conditions préalables sont remplies : Intégrations des identités : Conditions préalables.
3. Collecter les journaux : Prise en charge des journaux du connecteur Active Directory.
4. Ouvrez un dossier d'assistance si le problème persiste.

"Le connecteur est connecté à certains DC, mais pas à tous"

1. Confirmer les conditions préalables : Intégrations des identités : Conditions préalables.
2. Collecter les journaux : Prise en charge des journaux du connecteur Active Directory.
3. Ouvrez un dossier d'assistance si le problème persiste.

"Le connecteur a été connecté une fois, mais n'est actuellement connecté à aucun des contrôleurs de domaine disponibles"

1. Confirmer les conditions préalables : Intégrations des identités : Conditions préalables.
2. Collecter les journaux : Prise en charge des journaux du connecteur Active Directory.
3. Ouvrez un dossier d'assistance si le problème persiste.

"Le connecteur peut se connecter à un ou plusieurs VA, mais il ne s'y est pas encore connecté."

1. Retirez tous les VA inutilisés du tableau de bord.

2. Attendez jusqu'à 10 minutes pour la synchronisation après la suppression.
3. Assurez-vous que les exigences réseau sont respectées : Intégrations des identités : Conditions préalables.
4. Collecter les journaux : Prise en charge des journaux du connecteur Active Directory.
5. Ouvrez un dossier d'assistance si le problème persiste.

"Le connecteur signale des erreurs de délai d'attente lors de la tentative de connexion à certaines VA"

1. Si l'appliance virtuelle ne se trouve pas sur le même réseau local que le connecteur, envisagez de séparer le déploiement à l'aide des sites Umbrella : Connectez plusieurs domaines Active Directory à Umbrella.
2. Supprimez les VA inutilisées du tableau de bord.
3. Attendez jusqu'à 10 minutes pour la synchronisation après la suppression.
4. Assurez-vous que les exigences réseau sont respectées : Intégrations des identités : Conditions préalables.
5. Collecter les journaux : Prise en charge des journaux du connecteur Active Directory.
6. Ouvrez un dossier d'assistance si le problème persiste.

"Le connecteur est connecté à certains, mais pas à tous les VA"

1. Supprimez les VA inutilisées du tableau de bord.
2. Attendez jusqu'à 10 minutes pour la synchronisation après la suppression.
3. Assurez-vous que les exigences réseau sont respectées. Voir Guide du flux de communication Active Directory : Connectors > Virtual Appliances > DC and the Cloud.
4. Collecter les journaux : Prise en charge des journaux du connecteur Active Directory.
5. Ouvrez un dossier d'assistance si le problème persiste.

"Le connecteur a été connecté une fois, mais n'est actuellement connecté à aucun des VA disponibles"

1. Supprimez les VA inutilisées du tableau de bord.
2. Attendez jusqu'à 10 minutes pour la synchronisation après la suppression.
3. Assurez-vous que les exigences réseau sont respectées : Guide du flux de communication Active Directory : Connectors > Virtual Appliances > DC and the Cloud.
4. Collecter les journaux : Prise en charge des journaux du connecteur Active Directory.
5. Ouvrez un dossier d'assistance si le problème persiste.

"Le connecteur ne synchronise pas les événements en parallèle avec les VA. Le traitement des événements peut être plus lent que prévu."

1. Notez que le service Umbrella Connector est testé pour prendre en charge 10 ressources (contrôleurs de domaine et appareils virtuels) par processeur.
2. Mettez à niveau le serveur avec le nombre requis de CPU en fonction du nombre de contrôleurs de domaine et d'appliances virtuelles dans le site Umbrella.
3. Collecter les journaux : Prise en charge des journaux du connecteur Active Directory.
4. Ouvrez un dossier d'assistance si le problème persiste.

"Le connecteur signale des abandons lors d'une tentative d'envoi d'événements à certaines VA"

Suivez ces étapes pour réduire les abandons d'événements et restaurer la livraison stable des événements.

1. Vérifiez si le taux total d'événements sur tous les contrôleurs de domaine du site Umbrella dépasse la capacité continue testée d'environ 850 événements par seconde.
2. Si le taux d'événements dépasse cette capacité testée, augmentez les coeurs de CPU sur l'hôte Connector pour améliorer le débit de traitement.
3. Si les abandons persistent, activez l'équilibrage de charge avec deux connecteurs ou plus pour partager la charge du contrôleur de domaine. Cette fonctionnalité avancée doit être activée en ouvrant un dossier d'assistance avec l'assistance Umbrella.

Contrôleurs de domaine

"Était connecté à un ou plusieurs connecteurs, mais n'est plus connecté à aucun"

1. Si le connecteur a été supprimé, redéployez-le ou supprimez le contrôleur de domaine.
2. Confirmez la configuration réseau requise. Voir Guide du flux de communication Active Directory : Connectors > Virtual Appliances > DC and the Cloud.
3. Collecter les journaux : Prise en charge des journaux du connecteur Active Directory.
4. Ouvrez un dossier d'assistance si le problème persiste.

"Ce contrôleur de domaine ne s'est jamais connecté à un connecteur"

1. Pour envoyer des informations sur les événements d'ouverture de session à une appliance virtuelle, un connecteur doit être installé sur le même site que le contrôleur de domaine (DC). Voir Connexion d'Active Directory à Umbrella.
2. Collecter les journaux : Prise en charge des journaux du connecteur Active Directory.
3. Ouvrez un dossier d'assistance si le problème persiste.

"Ce contrôleur de domaine n'a pas de connecteurs auxquels se connecter"

1. Pour envoyer des informations sur les événements d'ouverture de session à une appliance virtuelle, un connecteur doit être installé sur le même site que le contrôleur de domaine (DC). Voir Connexion d'Active Directory à Umbrella.
2. Si vous réinstallez le connecteur ou si vous le déplacez d'une machine à une autre, ignorez ce message.

"Ce contrôleur de domaine est connecté à certains connecteurs, mais pas à tous"

1. Vérifier les autorisations : Autorisations requises pour l'utilisateur Cisco_Connector.
2. Collecter les journaux : Prise en charge des journaux du connecteur Active Directory.
3. Ouvrez un dossier d'assistance si le problème persiste.

"L'état WMI de ce contrôleur de domaine est inactif. Le contrôleur de domaine ne répond pas à la connexion WMI du connecteur."

1. Il peut s'agir d'un problème temporaire dû à la charge du contrôleur de domaine.
2. Vérifiez si la connexion WMI (Windows Management Instrumentation) peut être établie à l'aide de l'outil WBEMTest.
3. Réduisez la charge sur le contrôleur de domaine en arrêtant les autres applications inutilisées qui surveillent les événements de sécurité.
4. Redémarrez le service Connector pour établir une nouvelle connexion WMI après avoir réduit la charge CC.
5. Collecter les journaux : Prise en charge des journaux du connecteur Active Directory.
6. Ouvrez un dossier d'assistance si le problème persiste.

Causes

- Messages d'avertissement DNSCrypt (VA) : DNSCrypt est activé par défaut pour chiffrer les paquets DNS transférés de l'appliance virtuelle (VA) vers les résolveurs DNS publics Umbrella. Si les politiques de pare-feu ou d'inspection bloquent ou modifient la sonde DNSCrypt sur le port 53 (UDP/TCP), la sonde échoue. Si un système de prévention des intrusions (IPS) ou un système de détection des intrusions (IDS) effectue une inspection approfondie des paquets et attend uniquement le trafic DNS, l'analyse échoue.
- Messages d'arrêt de synchronisation du connecteur (connecteur AD) : Cisco a annoncé la fin de vie de TLS (Transport Layer Security) 1.0/1.1. Les versions Windows non prises en charge (Windows Server 2008, 2008 R2 ou Windows 7) ne prennent pas en charge TLS 1.2 par défaut, ce qui entraîne l'arrêt de la synchronisation des connecteurs.
- Messages de performances du connecteur (connecteur AD) : Le service Umbrella Connector est testé pour prendre en charge 10 ressources (contrôleurs de domaine et appliances virtuelles) par processeur. Lorsque cette taille est dépassée, le traitement des événements est plus lent que prévu.

- Messages d'avertissement de suppression d'événement (connecteur AD) : Le service Umbrella Connector est testé pour prendre en charge environ 850 événements continus (sans limite matérielle) par seconde sur tous les contrôleurs de domaine d'un site Umbrella. Si le débit global dépasse cette capacité testée, le connecteur abandonne les événements.
- Messages d'erreur WMI-down (contrôleur de domaine) : L'état WMI est désactivé lorsque le contrôleur de domaine est en charge et ne répond pas à la connexion WMI du connecteur.

Autres informations utiles

- Examiner le flux d'intégration d'Umbrella Active Directory
- Envoyer les journaux du connecteur Active Directory à la prise en charge Umbrella

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.