Comprendre les performances du connecteur Active Directory

Table des matières

Introduction

Ce document décrit les performances du connecteur Active Directory pour le DNS Umbrella.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur Umbrella DNS.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Aperçu

Le service Umbrella Connector est utilisé pour surveiller les événements de connexion utilisateur/ordinateur dans le cadre de l'intégration Active Directory d'Umbrella. Le service OpenDNS Connector lit les informations de connexion dans le journal des événements de sécurité de chaque contrôleur de domaine AD de son site.

Dans les environnements où les événements de connexion des utilisateurs sont fréquents, il est important de revoir ces consignes de performances. Pour une identification précise de l'utilisateur, le service Connector doit pouvoir récupérer rapidement les informations de connexion.

Nombre maximal d'événements/seconde

Il n'y a pas de limite stricte au nombre d'événements pouvant être traités. Le service Umbrella Connector est testé pour prendre en charge 850 événements continus par seconde sur tous les contrôleurs de domaine d'un « site ». Il repose sur un environnement de travaux pratiques dédié sans logiciel tiers en cours d’exécution. Les résultats réels peuvent varier en fonction de la latence du réseau et d'autres goulots d'étranglement.

Les clients peuvent déterminer un nombre approximatif d'événements/s en lisant la section « Événements par seconde » plus loin dans cet article.

Nouvelles fonctionnalités

Pour les clients effectuant des déploiements plus importants avec une fréquence élevée d'événements de connexion, Umbrella propose de nouvelles fonctionnalités axées sur les performances. En plus des recommandations générales sur les performances, veuillez lire les directives plus loin dans cet article sur l'équilibrage de charge, la communication parallèle et la connexion Direct Event Log Reader.

Recommandations de performances

Dimensionnement du connecteur

Le serveur exécutant le service Connecteur Active Directory doit disposer des ressources processeur et mémoire spécifiées dans le Guide de dimensionnement de la documentation Umbrella.

Connecteur dédié

Bien que le service Connecteur puisse être installé directement sur un contrôleur de domaine, Cisco Umbrella recommande que le connecteur soit installé sur un serveur membre dédié au service Connecteur. Aucun autre logiciel tiers ne doit être installé sur ce serveur membre. Pour en savoir plus sur le processus d'installation, consultez la documentation d'Umbrella.

Sites parapluie

Dans la mesure du possible, les déploiements Umbrella doivent être répartis en « sites » qui limitent les composants qui communiquent sur le réseau. Le service Connector ne peut communiquer qu'avec les composants du même site Umbrella. Cette fonctionnalité doit toujours être utilisée lorsque les utilisateurs disposent d'un déploiement réparti sur de vastes zones géographiques.

En général, un site parapluie est créé pour chaque emplacement physique. Les sites Umbrella doivent inclure ces règles dans la documentation Umbrella.

Une utilisation appropriée des sites Umbrella peut améliorer considérablement le déploiement et empêcher les composants de communiquer sur le réseau étendu.

Latence réseau

Les événements de connexion peuvent être transférés au connecteur sur le réseau. Il est important qu'il existe une connexion haut débit entre le connecteur et chaque contrôleur de domaine afin de réduire les délais liés au réseau. Le connecteur peut être positionné aussi près que possible du ou des contrôleurs de domaine et du ou des appareils virtuels.

Nombre de connecteurs

Un connecteur est requis pour chaque site Umbrella. Il est possible d'avoir plusieurs connecteurs dans un site Umbrella, mais cela n'est nécessaire qu'à des fins de redondance. Le fait d'avoir des connecteurs supplémentaires impose une charge supplémentaire aux contrôleurs de domaine car ils dupliquent la même fonction que le premier connecteur. Umbrella recommande un maximum de 2 connecteurs pour chaque site Umbrella.

Taille du journal des événements

Les journaux d'événements de sécurité Windows volumineux peuvent avoir un impact négatif sur les performances de cette opération WMI. Umbrella recommande de limiter la taille du journal des événements. Les meilleures performances sont obtenues avec un fichier journal de moins de 512 Mo, mais vous pouvez l'ajuster en fonction de vos besoins en matière de rétention des journaux. La taille du fichier journal peut être réglée à l'aide des instructions suivantes :

1. Ouvrez l'application Observateur d'événements (eventvwr.msc).

2. Accédez à Journaux Windows > Système

3. Cliquez avec le bouton droit sur le journal système et sélectionnez Propriétés.

4. Réglez la taille maximale du fichier journal comme vous le souhaitez et sélectionnez OK.

Logiciels tiers

Un certain nombre d'autres produits logiciels utilisent également WMI, ce qui peut créer un goulot d'étranglement dans WMI sur le contrôleur de domaine. Cela peut inclure :

- Logiciel de sécurité/d'analyse tiers qui surveille les journaux d'événements
- Transfert du journal des événements Windows
- Intégration SIEM et autres logiciels de surveillance des journaux d'événements

Si l'un de ces logiciels n'est plus nécessaire, nous vous recommandons de le désactiver. Ce problème peut également être atténué à l'aide de la méthode « Connexion directe au lecteur du journal des événements » décrite dans l'annexe.

Logiciel antivirus

Exclure ce dossier et ces fichiers exécutables de l'analyse antivirus :

```
C:\Program Files (x86)\OpenDNS\OpenDNS Connector
C:\Program Files (x86)\OpenDNS\OpenDNS Connector\OpenDNSAuditService.exe
C:\Program Files (x86)\OpenDNS\OpenDNS Connector\<VERSION>OpenDNSAuditClient.exe
```

Contrôleurs de domaine supplémentaires

Le système de notification WMI du contrôleur de domaine met en file d'attente et traite chaque entrée du journal des événements, puis les envoie aux abonnés WMI. Il s'agit en fait d'un mécanisme de transmission où les événements sont envoyés par le contrôleur de domaine. Ainsi, il peut y avoir un goulot d'étranglement des performances sur le contrôleur de domaine lui-même, ce qui affecte la rapidité d'envoi des événements.

Ce goulot d'étranglement peut être atténué en ajoutant des contrôleurs de domaine supplémentaires à votre environnement AD. Umbrella a testé un seul contrôleur de domaine jusqu'à 850 événements/s.

Exceptions de compte de service

Réduisez le nombre de connexions Active Directory détectées par Umbrella en excluant les comptes de service. Ces comptes doivent être exclus de toute façon pour une application correcte de la stratégie. Vous pouvez également exclure des serveurs et d'autres périphériques qui n'utilisent pas les stratégies utilisateur AD, mais qui peuvent avoir un grand nombre d'ouvertures de session utilisateur.

Correctifs WMI

Assurez-vous que le contrôleur de domaine et le serveur de connecteurs sont à jour avec les derniers correctifs Microsoft. Voici des exemples de correctifs qui résolvent les problèmes de performances WMI connus.

Limites de mémoire et de poignée WMI

WMI contient ses propres limites internes qui peuvent créer un goulot d'étranglement. Cela est particulièrement vrai lorsque d'autres logiciels effectuent également des opérations WMI intensives. Un exemple de la façon d'augmenter ces limites se trouve dans la documentation Microsoft.

Umbrella Support n'est pas en mesure de vous indiquer les limites correctes pour votre environnement. Contactez Microsoft pour obtenir de l'aide.

Équilibrage de charge CC

Umbrella prend désormais en charge une fonctionnalité d'équilibrage de charge utile lorsqu'un site comporte plusieurs contrôleurs de domaine et un grand nombre d'événements de connexion. Dans ce scénario, des connecteurs supplémentaires sont installés et des contrôleurs de domaine sont ensuite affectés à un connecteur via un groupe d'équilibrage de charge.

Dans un environnement simple, l'équilibrage de charge fonctionne comme suit :

- DC_A et DC_B sont affectés au groupe d'équilibrage de charge_1 qui est géré par Connector_1.
- DC_C et DC_D sont affectés au groupe d'équilibrage de charge 2 qui est géré par Connector_2.
- Les appareils virtuels reçoivent toujours des événements des deux connecteurs, ils sont donc toujours informés de tous les événements de connexion.
- Si la redondance est requise, un connecteur supplémentaire peut être installé dans chaque groupe d'équilibrage de charge.

Cette fonctionnalité présente les avantages suivants :

- La charge de travail de chaque connecteur est considérablement réduite. Chaque connecteur gère un plus petit nombre de contrôleurs de domaine.
- Cela est généralement utile dans les cas où le délai de réception des événements d'un contrôleur de domaine est élevé.

L'équilibrage de charge peut évoluer pour être utilisé dans des environnements multisites complexes avec de nombreux contrôleurs de domaine. Il n'y a aucun inconvénient à utiliser l'équilibrage de charge au-delà de l'installation de connecteurs supplémentaires.

À ce stade, la fonctionnalité d'équilibrage de charge doit être activée par la prise en charge d'Umbrella. Veuillez contacter l'assistance Umbrella pour discuter de vos besoins.

Appliance virtuelle Communication parallèle

Le connecteur peut désormais envoyer des événements de connexion à plusieurs appliances virtuelles en parallèle, plutôt que d'utiliser la méthode série par défaut. Cela est utile lorsqu'un site comporte plusieurs appliances virtuelles et un grand nombre d'événements de connexion.

Cette fonctionnalité présente les avantages suivants :

- Réduit le délai d'envoi des informations de connexion en présence de plusieurs appliances. Un événement peut être envoyé à toutes les appliances à la fois.
- Empêche un problème de communication ou une panne avec une appliance ayant un effet d'entraînement pour les autres appliances. Une file d'attente d'événements distincte est gérée pour chaque événement.

Cette fonctionnalité est désormais activée automatiquement, mais uniquement lorsque le serveur respecte les recommandations relatives au processeur et à la mémoire .

Transmission accélérée des événements de connexion des utilisateurs

Le connecteur peut désormais transmettre les événements de connexion utilisateur par lots, ce qui augmente considérablement le nombre d'événements par seconde pouvant être envoyés à l'appliance virtuelle (par seconde). Ceci est particulièrement important pour les connecteurs qui communiquent avec des appliances virtuelles sur des sites distants.

Cette fonction peut désormais être activée automatiquement, mais elle présente les caractéristiques suivantes :

- La communication parallèle (ci-dessus) doit être activée. Le serveur doit respecter les recommandations relatives au processeur et à la mémoire.
- ADC version 1.8+ requise
- Connecteur version 3.2.0+ requis

Connexion du lecteur du journal des événements direct

La version 1.4+ du connecteur Active Directory prend en charge une nouvelle méthode pour se connecter directement au journal des événements de sécurité du ou des contrôleurs de domaine sans utiliser de requête WMI. Cela élimine WMI en tant qu'« intermédiaire » et améliore considérablement les performances dans les cas où WMI est un goulot d'étranglement. Ceci est particulièrement utile dans les scénarios où les contrôleurs de domaine individuels traitent un grand nombre d'événements de connexion.

Cette fonction fonctionne à l'aide d'un mécanisme d'extraction dans lequel le connecteur extrait de nouveaux événements toutes les 5 secondes, de sorte qu'il existe un court délai (par exemple, 5 secondes) dans l'identification de l'utilisateur correct.

Cette optimisation est désormais activée par défaut. Pour plus d'informations sur cette fonctionnalité, contactez le support Umbrella.

Événements par seconde

Il est possible de compter le nombre d'événements récents sur un contrôleur de domaine pour estimer les événements par seconde. Umbrella recommande de le faire aux heures de pointe :

1. Ouvrez l'application Observateur d'événements (eventvwr.msc).

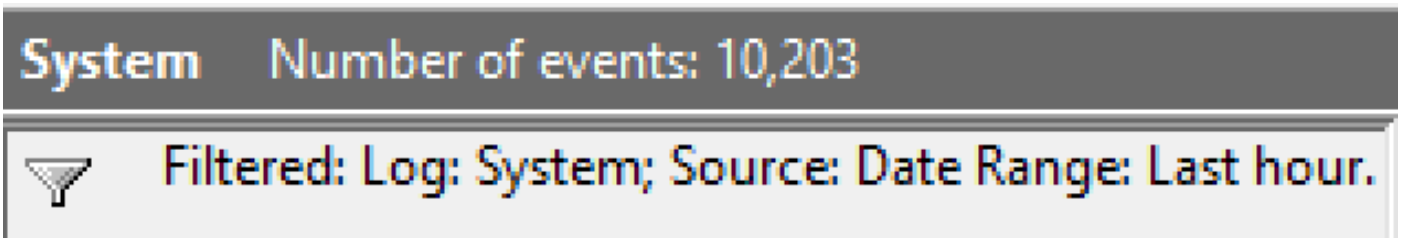
2. Accédez à Journaux Windows > Système.

3. Sélectionnez Filtrer le journal actuel et sélectionnez les événements enregistrés dans Dernière heure.

4. Cliquez sur OK.

Une fois le filtre chargé, le journal des événements peut afficher le nombre d'événements au cours de la dernière heure. Cette valeur peut être divisée par 3 600 pour estimer les événements par seconde.

360024901511



360024894112

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.