ManageEngine®

EventLog Analyzer

Les bonnes critiques et recommandations

Pré requis Systèmes

Pré requis CPU et RAM

Les pré requis nécessaires pour La CPU (processeur et vitesse) et la taille de la RAM dépendent du taux de log, de la taille moyenne des logs enregistrés, et du nombre de serveurs qui envoient l'ensemble des informations vers le collecteur log EventLog Analyser.

Pré requis de la capacité de stockage

Les pré requis nécessaires pour l'espace disque dépendent du volume de logs, collecté par jour, et qui doivent être archivés par EventLog Analyzer.

Jusqu'à 50 machines

Tx de log	Spécification vitesse, CPU	RAM	Volume Log	capacité disque
100/sec	processeur Pentium 41 GHz,	512 MB	1.5 GB/jour	150 GB
300/sec	Processeur 1 GHz, Pentium 4 machine dédiée	1GB	4.5 GB/jour	450 GB
500/sec	v1.5 GHz, Pentium Dual Core machine dédiée	2GB	7 GB/jour	720 GB

Jusqu'à 100 machines

Tx log	spécification vitesse, CPU	RAM	Volume log	capacité Disque
100/sec	Processeur Pentium 4 1 GHz,	1 GB	3 GB/jour	300 GB
300/sec	1.5 GHz, Pentium Dual Core machine dédiée	2 GB	9 GB/jour	900 GB
500/sec	1.5 GHz, Pentium Dual Core machine dédiée	4 GB	15 GB/jour	1500 GB

Jusqu'à 200 machines

Tx Log	spécification vitesse CPU	RAM	Volume log	capacité disk
100/sec	1.5 GHz, Pentium Dual Core machine dédiée	2 GB	6 GB/jour	600 GB
300/sec	1.5 GHz, Pentium Dual Core machine dédiée	4 GB	18 GB/jour	1800 GB
500/sec	2 GHz, Pentium Quad Core machine dédiée	8 GB	30 GB/jour	3000 GB

Note: pour 200 machines, et un taux de log qui dépasse 300/sec, l'équipe technique de EventLog Analyzer vous recommande d'utiliser une base de données MS SQL.

Jusqu'à 500 machines

Tx Log	Spécification vitesse, CPU	RAM	Volume Log	Capacité disque
100/sec	1.5 GHz, Pentium Dual Core machine dédiée	4 GB	15 GB/jour	1500 GB
300/sec	2 GHz, Pentium Quad Core machine dédiée	8 GB	45 GB/jour	4500 GB
500/sec	2 GHz, Pentium Quad Core machine dédiée	16 GB	75 GB/jour	7500 GB

Au delà de 500 machines

Si votre déploiement nécessite un fort volume de collecte des serveurs comme plus de 500 machines dans ce cas il faudra se rapprocher de nos équipes techniques pour vous fournir plus de précisions sur les pré requis.

Optimiser la capacité disque

Contrôle de l'évolution de l'espace disque

EventLog Analyzer a deux sources de données principales qui consomment de l'espace disque. Une est la base de données et l'autre est le stockage des fichiers d'archive. Les logs de données, sont pour la base de données MySQL, sont stockés dans le répertoire *<EventLog Analyzer Home>/mysql* MySQL et les fichiers d'archives sont stockées dans le répertoire archive *<EventLog Analyzer Home>/archive*

Optimisation de l'espace disque pour la base de données.

EventLog Analyzer stocke les données de logs dans la base de données pour analyser et générer des rapports. Mais les journaux (logs) ne peuvent pas être toujours conservés dans la base de données. Cela augmente non seulement la consommation d'espace disque dur, mais également affecte les performances de la base de données. Les logs dans la base de données sont régulièrement stockés dans les archives. La durée du temps de conservation les données dans la base de données est configurable. La valeur par défaut est de 32 jours. Modifiez cette valeur pour optimiser le stockage

Optimisation de l'espace disque pour l'archivage

EventLog Analyzer stocke une copie des fichiers de logs collectés de toutes les machines configurés dans le répertoire de l'archive, donc la taille de ce dossier d'archive augmente indéfiniment.

Vous pouvez contrôler l'évolution de l'espace disque en suivant les recommandations ci-dessous:

• Changer le dossier d'archivage en l'affectant à un autre endroit. Pour cela utiliser

Les paramètres > fichiers archivés> Archive dans le menu Paramètres de EventLog Analyzer accessible par le client web.

• Vous pouvez conserver les deux zones d'archivage et de garder la zone d'échange (swap) périodiquement. Transférer le contenu de l'archive dormante vers le lecteur de bande ou vers une zone de stockage à haute capacité comme un SAN, afin d'avoir un stockage sur du long terme

• Vous pouvez assigner différents lecteur dédié (s) pour les fichiers logs archivés et de surmonter la limitation d'espace disque

Sécuriser EventLog Analyzer

Installation et configuration

Il est recommandé d'installer EventLog Analyzer en tant que service. Quand il est installé en tant que service, chaque fois que vous démarrez le système, le service EventLog Analyzer démarrera automatiquement sans une intervention manuelle. Par défaut EventLog Analyzer sera installé en tant que service. Même si vous avez installé EventLog Analyzer en tant qu'une l'application, vous pouvez revenir sur le mode service par une procédure simple.

• Le compte utilisateur de l'OS a besoin de toutes les autorisations sur tous les répertoires et sous-répertoires dans le répertoire seulement d'installation de EventLog Analyzer.
• Il n'est pas nécessaire d'installer EventLog Analyzer avec un compte utilisateur comme root (sous Linux). Mais, il est nécessaire d'installer EventLog Analyzer avec un compte utilisateur en tant qu'Administrateur (sous Windows). Veuillez à ce que toute l'installation est faite en utilisant ce même compte utilisateur..
• Pour l'installation et le fonctionnement de l'application ou du service, le même compte utilisateur doit être utilisé.
L'installation de l'application utilisant que le compte root, cela risque de ne pas fonctionner avec un autre compte après l'installation.

Précautions pour le répertoire d'installation de EventLog Analyzer

- Exclure le répertoire d'installation de EventLog Analyzer »AdventNet» (ce pourrait être dans C: \ AdventNet ou D: \ AdventNet) lors du système de sauvegarde mais aussi lors du scan de l'anti-virus, car cela peut corrompre les tables de la base de données MySQL

Configuration Utilisateur

- Assurez-vous de modifiez par défaut le mot de passe **admin** et **guest** depuis l'interface web web de EventLog Analyser

Sécurisation des communications client/serveur

Si vous souhaitez sécuriser les communications client-serveur de EventLog Analyzer, vous pouvez mettre en œuvre Socket Layer sécurisé (SSL).

Consultez les documents d'aide ainsi que la procédure détaillée décrivant comment configurer et sécuriser les communications client/serveur via le protocole SSL les données sont fournis à partir de ce lien ci-dessous:

http://www.manageengine.com/products/eventlog/help/appendix/eventflow_ssl_support.html

Les bonnes pratiques pour la base de données

Sécurisation de la base de données après l'installation pour Mysql

Pour une simple installation, EventLog Analyzer utilise la base de données MySQL par défaut avec le compte utilisateur "root" sans mot de passe. Vous pouvez renforcer la sécurisation de l'installation de base de données MySQL, en lui associant un mot de passe pour l'utilisateur «root».
Il est recommandé d'attribuer un mot de passe pour l'utilisateur root par défaut.

Consultez la Foire aux questions relatives à la procédure détaillée pour attribuer / modifier le mot de passe de la base de données MySQL cliquer sur le lien ci-dessous.

http://www.manageengine.com/products/eventlog/faq.html # 17_2

Sécurisation de la base de données après l'installation pour MS SQL

Pour la base de données MS SQL, il n'est pas nécessaire d'attribuer de mot de passe, parce que pendant l'installation du produit lui-même, vous devez fournir un compte valide MS SQL avec les informations d'identification utilisateur, en dehors des autres paramètres.

Optimisation des performances de la base de données MySQL

Pour de meilleur performance, vous pouvez configurer vos paramètres de votre base de donnée MySQL afin d'adapter la base avec la taille RAM du serveur EventLog Analyzer

Consultez les documents d'aide pour la procédure détaillée pour configurer les paramètres de MySQL donnée dans le lien ci-dessous:

http://www.manageengine.com/products/eventlog/system_requirement.html # mysql

Utiliser une base de données sur un autre serveur, ce qui optimise les performances

Le serveur EventLog Analyzer et la base de données MySQL peut être installé dans des machines distinctes, ce qui évite une hausse de la charge CPU lors de d'un fort volume de collecte des logs

Recommandation pour la sauvegarde des données

Sauvegarde des données de EventLog Analyzer

Il est recommandé de sauvegarder les données de la base d'EventLog Analyzer tous les quinze jours, afin que les données ne soient pas perdues en cas de désastre.

Avant de réaliser la sauvegarde des données d'EventLog Analyzer, il est recommandé d'arrêter les services du serveur EventLog Analyzer.

MySQL

copier manuellement le dossier et les fichiers suivants ou utiliser un logiciel tiers de sauvegarde.

<EventLog Analyzer Home>/mysql/

Note: réaliser une sauvegarde complète du répertoire incluant les fichiers et les sous répertoires

MS SQL

Concernant la procédure de sauvegarde se référent à la base de données MS SQL, utiliser le lien ci-dessous

http://support.microsoft.com/kb/930615

Nous vous suggérons également de prendre une copie du dossier d'archives, situé sous <EventLog Analyzer/archive/, si vous souhaitez libérer de l'espace sur le disque dur.

Vous pouvez suivre les étapes ci-dessus une fois tous les quinze jours et de les restaurer en cas de problème.

Note: assurez-vous que le numéro de build est le même lors de la restauration, si non, revenir vers le support qui vous aidera dans votre restauration des données. L'équipe support intégrera dans la prochaine version du produit l'automatisation du processus de sauvegarde

Recommandations et bonnes pratiques pour le support

Procédure pour créer un fichier d'information de support (SIF) et envoyer le SIF au support de EventLog Analyzer

Nous recommandons à l'utilisateur de créer un fichier d'information de support (SIF) et l'envoyer aux équipes supports de eventloganalyzer-support@manageengine.com

Les instructions pour la création du SIF sont les suivante:

• Se connecter en utilisant le Web-client et cliquez sur l'onglet 'Support'.
• Cliquez sur le lien 'Créer un fichier d'information sur les fichiers pour le Support »dans cette page.
• Attendez pendant 30-40 secondes et à nouveau cliquez sur l'onglet "support".
• Maintenant, vous trouverez de nouveaux liens "Télécharger" et charger" vers le serveur FTP.
• Vous pouvez soit télécharger le SIF en cliquant sur le lien "Télécharger", puis envoyer le fichier téléchargé SIF à eventloganalyzer-support@manageengine.com ou cliquez sur charger vers le serveur FTP et fournir tous les détails des données nécessaires du fichier téléchargé.

Procédure pour créer le SIF et envoyer ce fichier à ZOHO Corp, si le client web ne permet pas d'accéder au serveur EventLog Analyzer

Si vous ne parvenez pas à créer un fichier SIF à partir de l'interface utilisateur apr le client web, vous pouvez zipper les fichiers sous le répertoire «logs» situé dans *<EventLog Analyzer Home>\server\default\log* \(chemin par défaut) et envoyer le fichier zip en le chargeant " dans le lien ftp suivant:

http://bonitas.adventnet.com/upload/index.jsp?to=eventloganalyzer-support @ manageengine.com

http://bonitas.adventnet.com/upload/index.jsp?to=eventloganalyzer-support@manageengine.com