

Configuration de la connexion à distance sur les routeurs RV160 et RV260

Objectif

La journalisation à distance peut être un outil efficace pour le débogage des problèmes de réseau. Les options de journalisation des routeurs RV160x et RV260x incluent : *local*, *e-mail* et *serveur distant*. Cet article illustre les étapes de configuration de la journalisation à distance sur un routeur RV160W. Avant de commencer, nous vous fournirons un contexte supplémentaire pour vous aider à déterminer si cet article est destiné à vous.

Conditions requises

- RV160x [[Guide d'administration du lien](#)]
- RV260x [[Guide d'administration du lien](#)]
- Un serveur ou un point de terminaison Syslog précédemment configuré, avec une adresse IP attribuée

Qui utiliserait la journalisation à distance ?

Cet article s'adresse à quelques types différents de personnes. Certains envisagent de créer un « pipeline » de données entre le RV160x/RV260x et un emplacement de cloud distant. Cela peut également s'appliquer à une personne qui envoie les journaux à un réseau interne ou à un point d'extrémité du réseau. Troisièmement, il se peut que vous souhaitiez vous enregistrer sur votre réseau par programme via un fournisseur tiers. La journalisation à distance a pour but l'analyse, la surveillance ou le stockage du contenu des journaux. Grâce à des techniques modernes d'exploration de données, ces fournisseurs pourraient tirer des enseignements des journaux. Que vous stockiez ou non les journaux en interne ou en externe, les besoins du « pipeline » ont des considérations différentes.

Ce gazoduc ressemble beaucoup à une ligne principale d'eau, il vaporisera des billes partout où vous le dirigez. Mais pour tirer de la valeur de ces journaux, certaines personnes choisissent d'utiliser une tierce partie pour contextualiser les journaux.

Si votre serveur Syslog n'est pas encore configuré

Il existe de nombreuses solutions pour configurer un serveur Syslog distant. Nous ne vous conseillerons pas l'un sur l'autre, voici quelques liens vers quelques options de bien-être.

- [Journaux Cisco Umbrella envoyés à AWS](#)
- [Serveur Syslog Red Hat](#)

Configuration de la journalisation à distance

Étape 1. Après vous être connecté au routeur, cliquez sur **System Configuration > Log**.



Getting Started



Status and Statistics



Administration



System Configuration

1

Initial Router Setup

System

Time

Log

2

Email

User Accounts

User Groups

Étape 2. Cochez la case **Activer** sous l'en-tête *Paramètres du journal*.



Log

Log settings

Log:

 Enable

Log Buffer:

1024

KB (Range: 1-4096, Default: 1024)

Severity:

Notification ▼

Category:

 All Kernel System Firewall Network VPI Users Wireless PnP

Save to USB Automatically:

 Enable

Étape 3. Les journaux ont huit niveaux d'impact différents. La sélection de la quantité d'information appropriée à vos fins variera. Gardez à l'esprit qu'au fil du temps, les répertoires contenant des journaux peuvent augmenter plus que vous ne l'aviez prévu. Reportez-vous à la liste ci-dessous pour connaître l'impact le plus important :

1. Débogage : consigne la plus grande quantité d'informations pour le dépannage.
2. Informations - Détails de l'impact sur les performances.
3. Notification - Condition normale mais significative.
4. Avertissement - fonctionnel mais en danger de basculer en mode erreur.
5. Erreur : la fonction ou la fonction n'est pas disponible en raison d'une erreur.
6. Conditions critiques - conditions essentielles.
7. Alerte : une action immédiate est requise.
8. Urgence : le périphérique est inutilisable ou inaccessible.

Note: Activez le débogage uniquement si vous travaillez activement avec les journaux.



Log

Log settings

Log: Enable

Log Buffer: 1024

Severity: Notification ▼

Category: Emergency

Alert

Critical

Error

Warning

Notification

Information

Debugging

Save to USB Automatically:

Email Server

Note: Soyez sélectif quant aux paramètres sélectionnés ici, mais vous pouvez les composer en fonction de vos besoins en faisant des expériences.

Étape 4. Les autres décisions de cette section nécessitent le même examen judiciaire. Toutes les catégories sélectionnées sont par défaut, ce que nous avons sélectionné.

1. Noyau
2. système
3. Pare-feu
4. Réseau
5. VPN
6. OpenVPN
7. Utilisateurs
8. Accès sans fil
9. PnP

Category:

All Kernel System Firewall Network VPN OpenVPN
 Users Wireless PnP

Note: Lorsque vous sélectionnez les catégories si vous utilisez un tiers pour analyser les journaux, vérifiez leur documentation pour les catégories à inclure.

Étape 5. Faites défiler la page jusqu'en bas (le cas échéant). Ensuite, cochez la case **Activer** sous l'en-tête *Serveurs syslog distants*.

Remote Syslog Servers

Syslog Servers:

Enable

Syslog Servers 1:

Syslog Servers 2:

Étape 6. Entrez l'**adresse IP** du serveur distant.

Remote Syslog Servers

Syslog Servers:

Enable

Syslog Servers 1:

192.168.4.25

(1.2.3.4, abc.com or fe08::10)

Syslog Servers 2:

(1.2.3.4, abc.com or fe08::10)

Note: Le serveur de journalisation distant doit être un point de terminaison valide pour la livraison des fichiers syslog.

Étape 7. (Facultatif) Pour la redondance, ajoutez une adresse IP supplémentaire.

Remote Syslog Servers

Syslog Servers: Enable

Syslog Servers 1: (1.2.3.4, abc.com or fe08::10)

Syslog Servers 2: (1.2.3.4, abc.com or fe08::10)

Étape 8. Cliquez sur **Apply** pour terminer la configuration.

cisco(admin) English

Étape 9. Veillez à **enregistrer** la configuration à partir de **running config > startup config**.

Conclusion

Dans ce guide de configuration, nous avons examiné la façon dont les routeurs RV160x/RV260x devaient envoyer des journaux à un point d'extrémité via une adresse IP. Notez que les journaux ne sont générés qu'après l'activation, ils ne sont pas générés par une méthode rétroactive.