Configurez les configurations de journal système sur le routeur de gamme RV34x

Objectif

Les événements de système sont des activités qui peuvent exiger l'attention et les actions nécessaires d'être pris pour exploiter le système sans à-coup et pour empêcher des pannes. Ces événements sont enregistrés en tant que logs. Les logs système permettent à l'administrateur de maintenir les événements particuliers qui ont lieu sur le périphérique.

Les configurations de log définissent les règles et les destinations de sortie se connectantes pour des messages, des notifications, et d'autres informations pendant que de divers événements sont enregistrés sur le réseau. Cette caractéristique informe le personnel responsable de sorte qu'une mesure nécessaire soit prise quand un événement se produit. Des logs peuvent également leur être envoyés par l'intermédiaire des alertes par courrier électronique.

Cet article vise à afficher te comment configurer les configurations de journal système comprenant le serveur d'email, et aux configurations de serveur distant sur le routeur de gamme RV34x.

Périphériques applicables

- Gamme RV34x

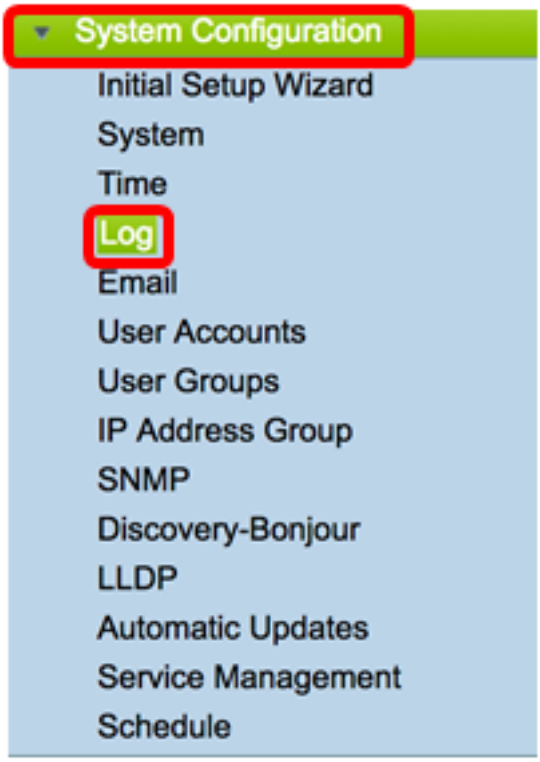
Version de logiciel

- 1.0.01.14

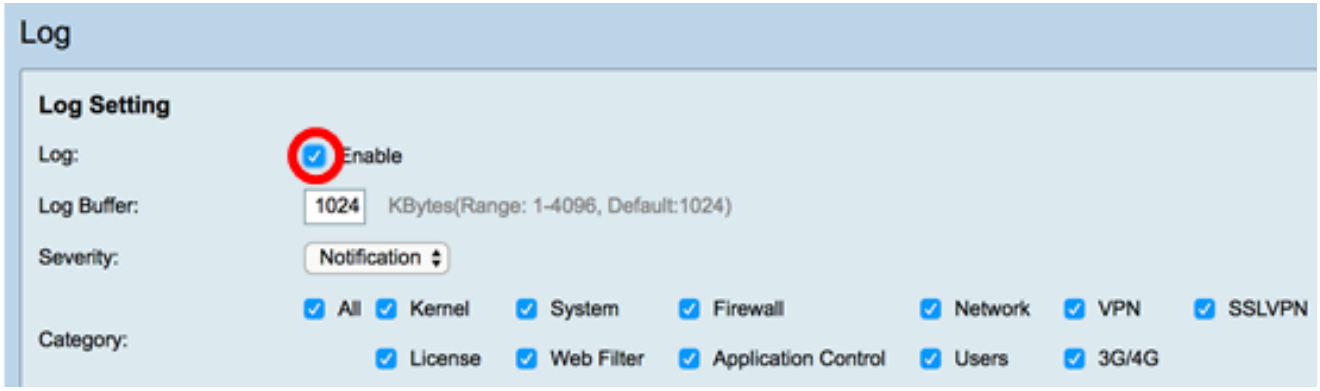
Configurez les configurations de log système

Configuration de log

Étape 1. Ouvrez une session à l'utilitaire basé sur le WEB et choisissez la **configuration système > le log**.

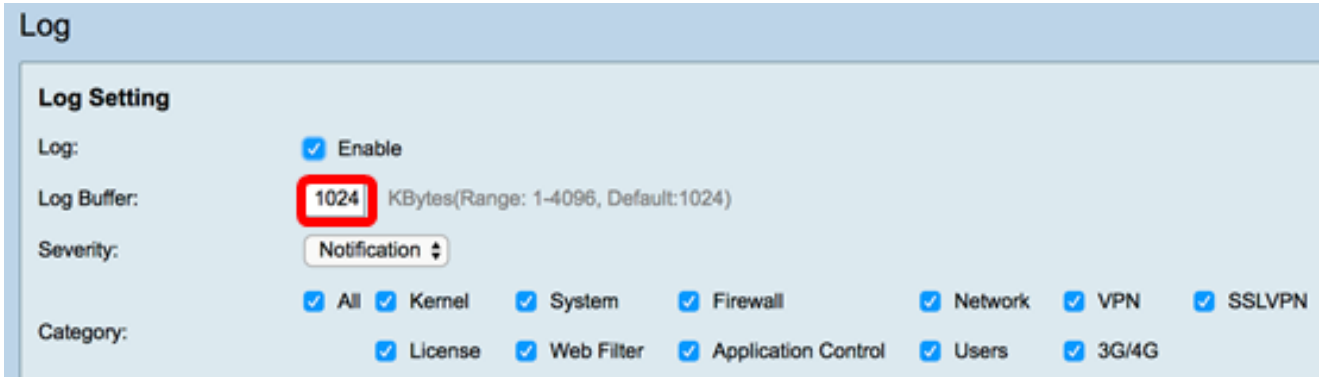


Étape 2. Dans le log plaçant la zone, cochez la case d'**enable** pour que le log reçoive des mises à jour au sujet du réseau.



Étape 3. Dans le domaine de *mémoire tampon de log*, écrivez la taille dans les kilo-octets (KO) que la mémoire tampon locale a pour des logs. La taille de mémoire tampon détermine combien de logs peuvent être enregistrés localement sur le routeur. La plage est de 1 à 4096. La valeur par défaut est 1024.

Remarque: Pour cet exemple, la valeur est laissée au par défaut.



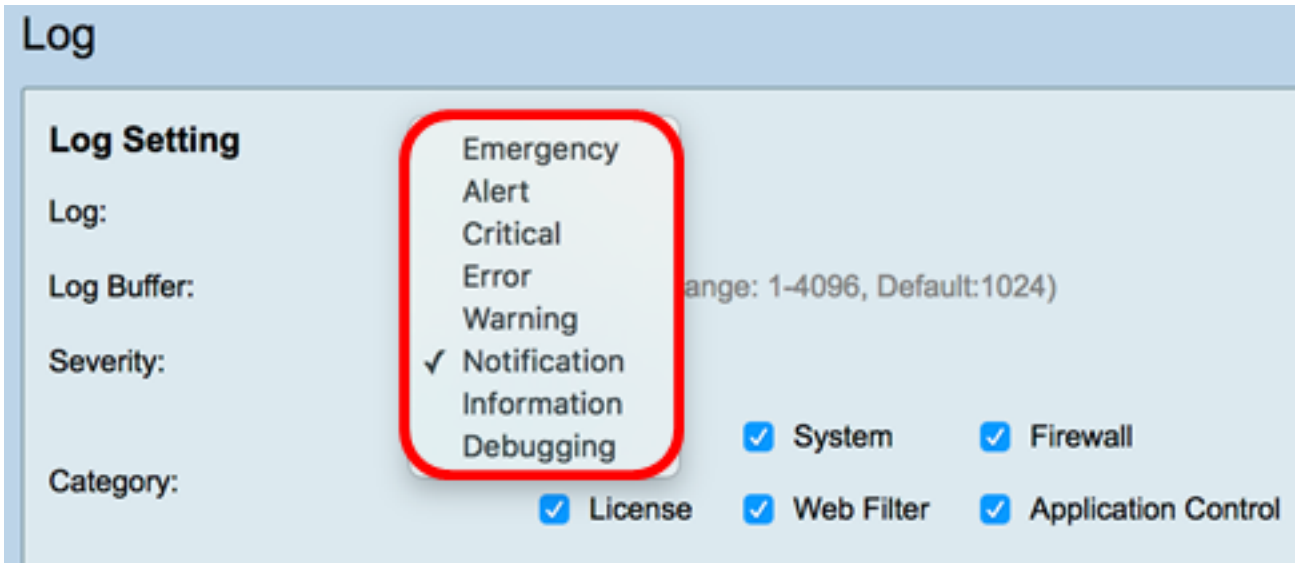
Étape 4. Choisissez une option de la liste déroulante de sévérité. La sévérité choisie est y compris tous les niveaux supérieurs, ainsi des logs sont réduites pour tous les niveaux

d'importance du niveau supérieur au niveau choisi.

Les options sont :

- Urgence — Niveau 0 ; Le message est enregistré si un périphérique est en baisse ou inutilisable. Le message est normalement annoncé à tous les processus.
- Alerte — Niveau 1 ; Le message est enregistré s'il y a une défaillance sérieuse de périphérique, telle qu'un cas en lequel toutes les caractéristiques de périphérique cessent de fonctionner.
- Essentiel — Niveau 2 ; Le message est enregistré s'il y a une défaillance essentielle de périphérique, telle que deux ports ne fonctionnant pas correctement tandis que les ports restants fonctionnent correctement.
- Erreur — Niveau 3 ; Le message est enregistré s'il y a une erreur dans un périphérique tel qu'un port unique étant hors ligne.
- Avertissement — Niveau 4 ; Le message est enregistré si un périphérique fonctionne correctement mais un problème opérationnel se pose.
- Niveau de notification 5 ; Le message est enregistré si un périphérique fonctionne correctement mais un avis de système se produit. Il s'agit de la configuration par défaut.
- Les informations — Niveau 6 ; Le message est enregistré si une condition qui n'est pas une erreur existe sur le périphérique mais peut exiger l'attention ou la manipulation spéciale.
- Débogage — Niveau 7 ; Fournit toutes les informations de débogage détaillées.

Remarque: Pour cet exemple, le par défaut est choisi.



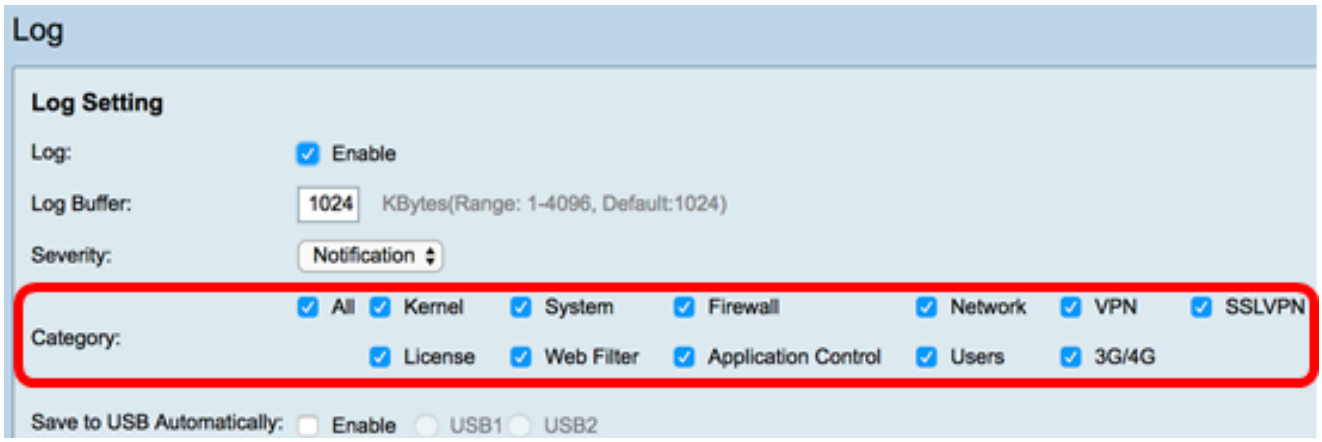
Étape 5. Vérifiez les catégories applicables pour recevoir des mises à jour et des notifications. Les options sont :

- Entièrement cette option active toutes les options.
- Noyau — Logs impliquant le code de noyau.
- Logs système impliquant des applications du l'utilisateur-espace telles que le Protocole NTP (Network Time Protocol), la session, et le protocole DHCP (DHCP).
- Journaux du pare-feu déclenchés par des violations, des règles, des attaques, et filtrage selon le contenu de Pare-feu.
- Réseau — Les logs ont associé à l'acheminement, au DHCP, au réseau étendu (WAN), au réseau local (RÉSEAU LOCAL), et au QoS.
- VPN — Le réseau privé virtuel (VPN) a associé des logs comprenant des exemples comme la

panne d'établissement de tunnel VPN, panne de passerelle VPN, et ainsi de suite.

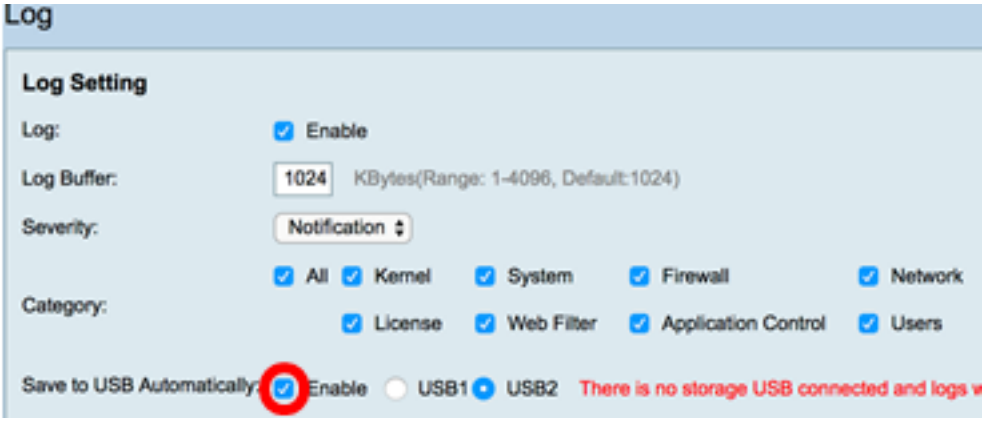
- SSLVPN — Logs liés à Secure Sockets Layer (SSL) VPN.
- Permis — Logs comportant des violations de permis.
- Filtre Web — Se connecte connexe aux événements qui ont déclenché le filtrage de Web.
- Contrôle d'application — Logs liés au contrôle d'application.
- Utilisateurs — Logs liés aux activités d'utilisateur.
- 3G/4G — Se connecte des dongles 3G/4G/USB qui sont branchés au routeur.

Remarque: Dans cet exemple, tout est choisi.



Contrôle (facultatif) d'étape 6. la case d'**enable** pour la sauvegarde à l'USB automatiquement pour sauvegarder des logs à un USB. Ceci est désactivé par défaut.

Remarque: Si le routeur le détecte qu'un USB n'est pas connecté afin de cette caractéristique soit fonctionnel, une ligne de texte rouge sera évident près de la case d'option USB2 déclarant qu'il n'y a aucune mémoire USB connectée et des logs seront enregistrés seulement après qu'un périphérique de stockage valide est connecté.



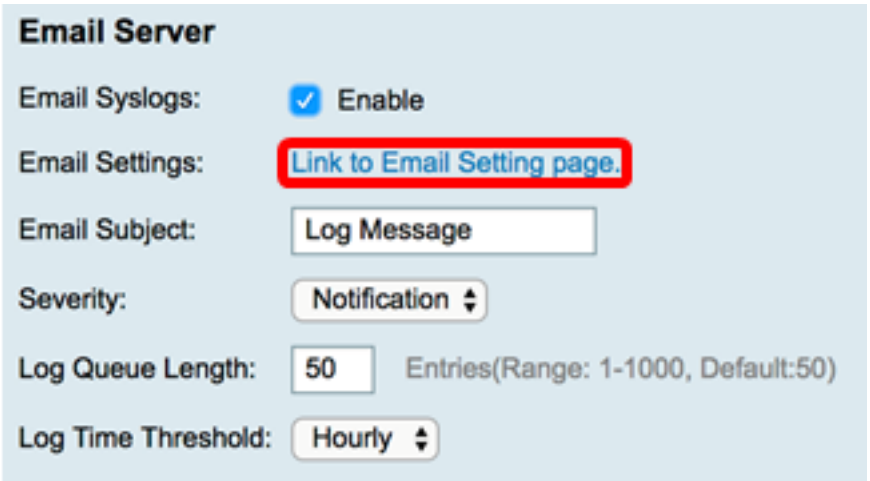
Étape 7. Choisissez une case d'option du port USB où le lecteur est connecté.

Remarque: Pour cet exemple, l'USB2 est choisi.

Serveur de mail

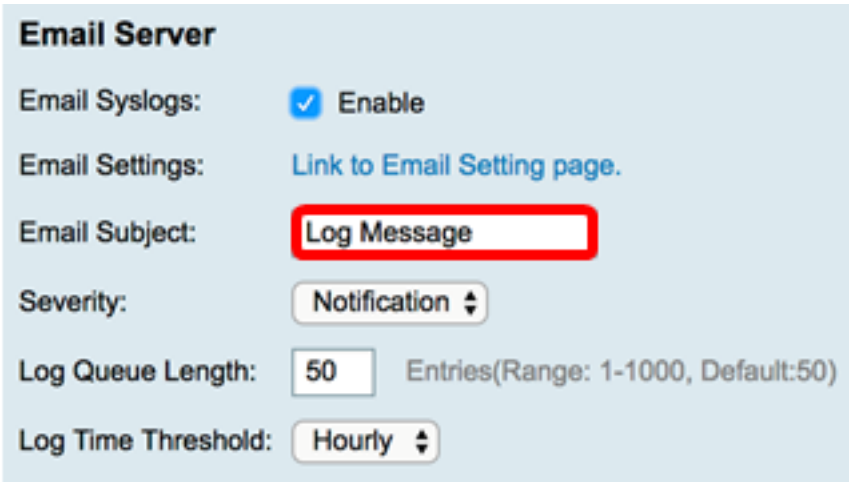
Étape 8. Cochez la case d'**enable** pour que les Syslog d'email permettent au routeur pour envoyer des alertes par courrier électronique pour les événements réseau ou le comportement spécifiques qui peuvent affecter la représentation, Sécurité, ou pour l'élimination des imperfections.

Étape 9. Pour configurer des configurations d'email, le lien de clic envoyer la page de configuration et a cliquez ici pour des instructions sur la façon dont configurer les configurations d'email sur le routeur de gamme RV34x.



Étape 10. Dans le *champ Subject d'email*, écrivez un sujet pour que l'email soit envoyé à l'adresse e-mail.

Remarque: Pour cet exemple, le message de log est utilisé.

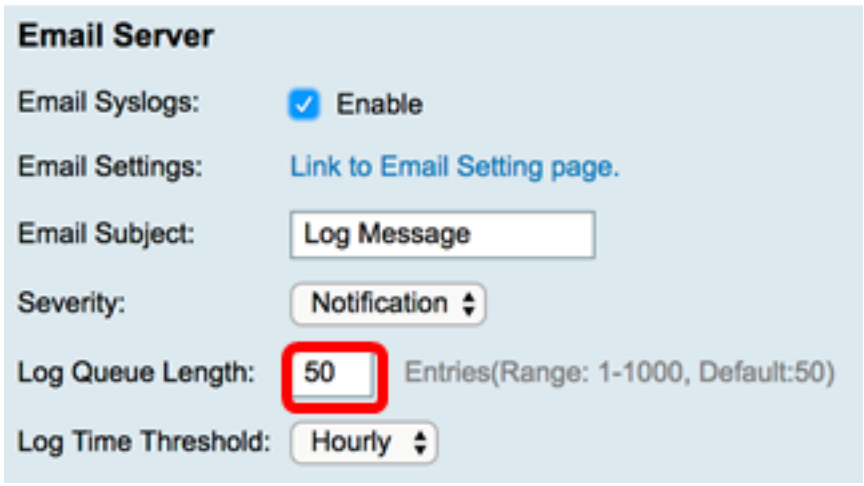


Étape 11. De la liste déroulante de sévérité, choisissez une sévérité. La sévérité choisie est y compris tous les niveaux supérieurs, ainsi des logs sont réduites pour tous les niveaux d'importance du niveau supérieur au niveau choisi. Les options sont notification, avertissement, erreur, essentielles, vigilantes, et urgence.

Remarque: Pour cet exemple, la notification est utilisée.

Étape 12. Dans le domaine de *longueur de file d'attente de log*, écrivez le nombre d'entrées qui doivent être faites avant que le log soit envoyé dans le destinataire de courriel. Le par défaut est 50.

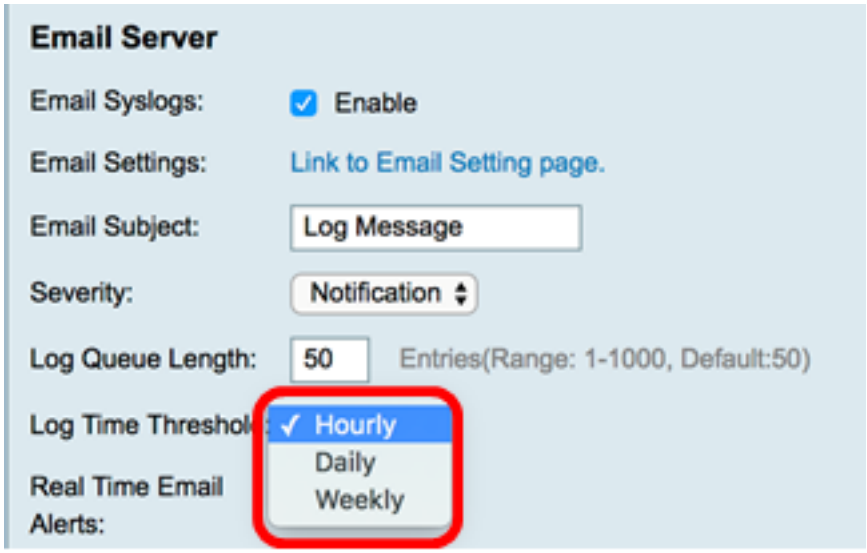
Remarque: Pour cet exemple, le par défaut est utilisé.



Étape 13. De la liste déroulante de seuil de temps de log, choisissez l'intervalle auquel le

routeur envoie le log à l'email. Les options sont horaires, quotidiennes, et hebdomadaires.

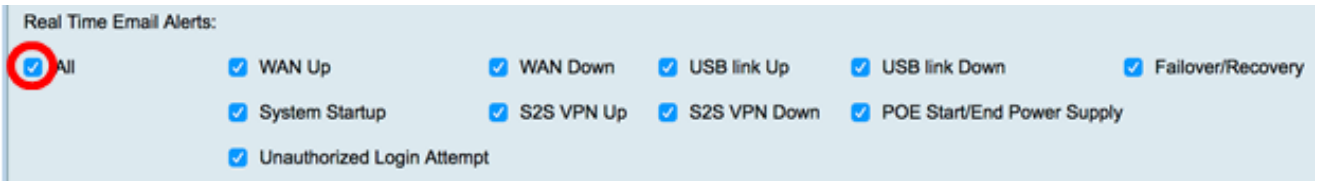
Remarque: Pour cet exemple, d'heure en heure est choisi.



Étape 14. Vérifiez les cases des événements qui déclencheront une alerte par courrier électronique en temps réel. Les options sont comme suit :

- Entièrement vérifie toutes les cases et permet au routeur d'envoyer des alertes en temps réel à l'email.
- WAN — L'alerte envoyée pour envoyer au sujet du lien WAN est en hausse.
- WAN vers le bas — Alerte envoyée pour envoyer au sujet du lien WAN allant vers le bas.
- Relier USB — Alerte envoyée pour envoyer au sujet du lien USB allant.
- Lien USB vers le bas — Alerte envoyée pour envoyer au sujet du lien USB allant vers le bas.
- Basculement/reprise — L'alerte envoyée pour envoyer au sujet du routeur allant dans le mode de reprise ou du routeur a recouru au dongle 3G/4G USB pour se connecter à l'Internet.
- Démarrage du système — Alerte envoyée pour envoyer au sujet du routeur démarrant.
- S2S VPN vers le bas — Alerte envoyée pour envoyer que le site à site VPN est.
- S2S VPN vers le bas — Alerte envoyée pour envoyer que le site à site VPN est vers le bas.
- Tentative non autorisée de procédure de connexion — L'alerte est envoyée à l'email au sujet d'une tentative non autorisée de procédure de connexion sur le routeur.

Remarque: Pour cet exemple, tout est vérifié.

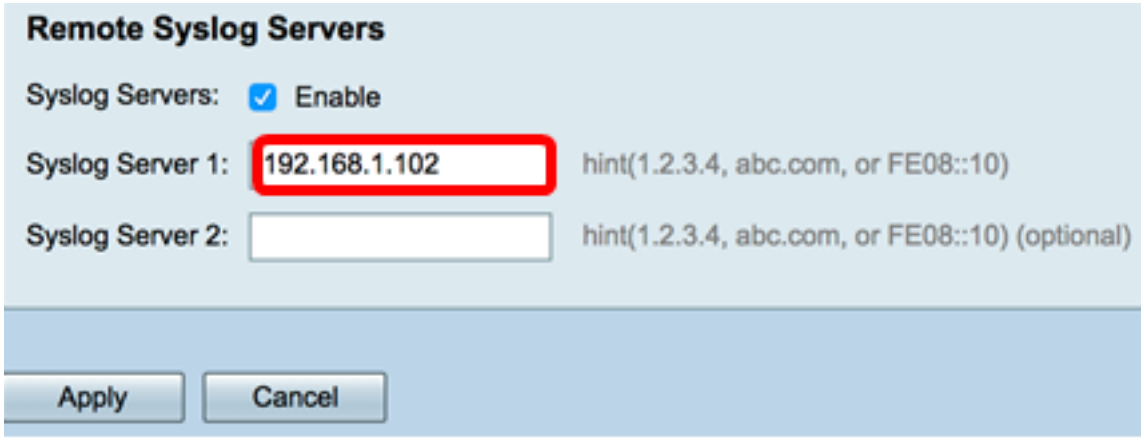


Serveurs de Syslog distant

Étape 15. Cochez la case d'**enable** pour des serveurs de Syslog.

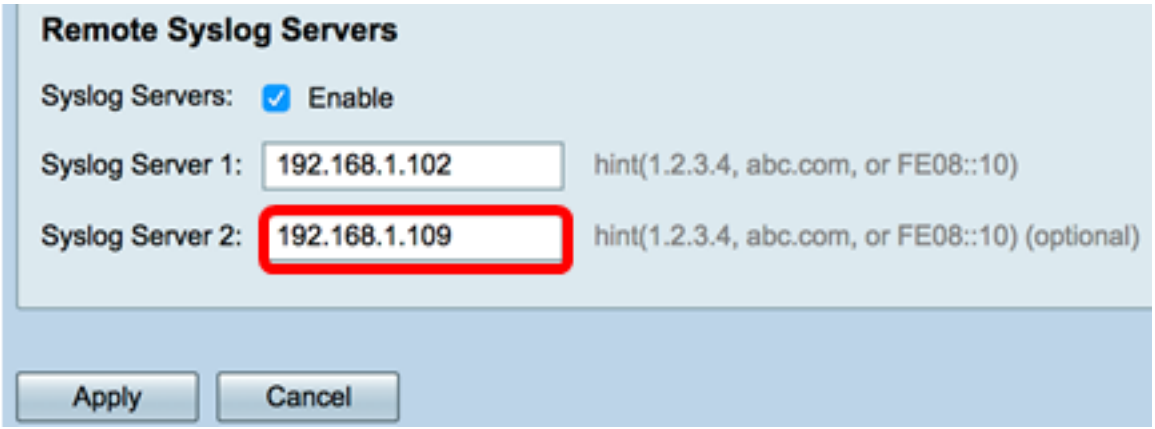
Étape 16. Dans le domaine du *serveur 1 de Syslog*, écrivez l'adresse IP du serveur distant de Syslog où les événements loggés seront enregistrés.

Remarque: Pour cet exemple, 192.168.1.102 est utilisé comme adresse du serveur distante de Syslog.

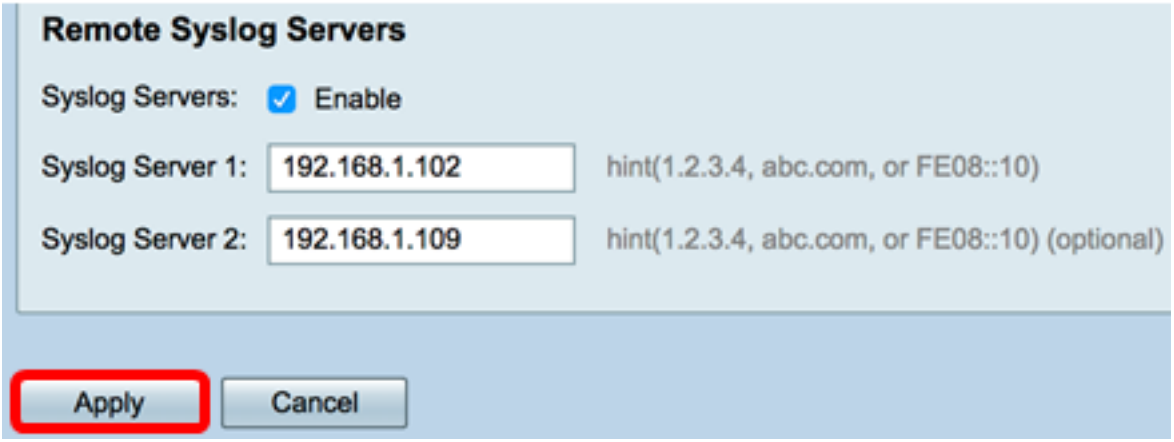


Étape 17. (Facultatif) dans le domaine du *serveur 2 de Syslog*, écrivez l'adresse IP de sauvegarde du serveur distant de Syslog.

Remarque: Dans cet exemple, 192.168.1.109 est utilisé.



Étape 18. Cliquez sur **Apply**.



Étape 19. (Facultatif) pour sauvegarder la configuration de manière permanente, allez à la page de copie/save configuration ou cliquez sur 

l'icône à la partie supérieure de la page.

Vous devriez avoir maintenant avec succès configuré les configurations de journal système sur le routeur de gamme RV34x.