Dépannage des problèmes de migration

Dépannage de l'outil de migration de pare-feu sécurisé

Une migration échoue généralement lors du Check Point chargement du fichier de configuration de ou lors du transfert de la configuration migrée verscentre de gestion.

Voici certains des scénarios courants où le processus de migration échoue pour une configuration Check Point :

- Fichiers manquants dans le fichier Check Point Config.zip.
- Les fichiers non valides sont détectés par l'outil de migration de pare-feu sécurisé dans le fichier Check Point Cofig.zip
- Si le fichier de configuration de Check Point est d'un type de fichier compressé autre que .zip.

Offre groupée de soutien pour l'outil de migration de pare-feu sécurisé

L'outil de migration Secure Firewall offre la possibilité de télécharger un ensemble d'assistance pour extraire des informations de dépannage précieuses comme les fichiers journaux, la base de données et les fichiers de configuration. Procédez comme suit:

1. Sur l'écran **Migration terminée**, cliquez sur le bouton **Soutien technique**.

   La page de soutien technique apparaît.

2. Cochez la case **Offre groupée de soutien**, puis sélectionnez les fichiers de configuration à télécharger.

Remarque Les fichiers journaux et dB sont choisis pour téléchargement par défaut.

3. Cliquez sur **Télécharger**.

   Le fichier d'assistance est téléchargé sous la forme d'un fichier .zip dans votre chemin d'accès local. Extrayez le dossier Zip pour voir les fichiers journaux, la base de données et les fichiers de configuration.

4. Cliquez sur **Envoyer** pour envoyer les détails de la panne à l'équipe technique.

   Vous pouvez aussi joindre les fichiers d'assistance téléchargés à votre courriel.

5. Cliquez sur **Visiter la page TAC** pour créer une demande TAC dans la page de soutien de Cisco

Remarque Vous pouvez soumettre une demande TAC en tout temps durant la migration à partir de la page de soutien technique.

Journaux et autres fichiers utilisés pour le dépannage

Vous pouvez trouver des informations utiles pour identifier et résoudre les problèmes dans les fichiers suivants.

Fichier	Emplacement
Fichier de journalisation	<migration_tool_folder>\journaux
Rapport pré-migration	<migration_tool_folder>\ressources
Rapport post-migration	<migration_tool_folder>\ressources
fichier non analysé	<migration_tool_folder>\ressources

Résolution de problèmes liée aux échecs de chargement des fichiers Check Point

Si le chargement de votre fichier de configuration Check Point échoue, c'est généralement parce que l'outil de migration Cisco Secure Firewall n'a pas pu analyser une ou plusieurs lignes du fichier.

Vous pouvez trouver des informations sur les erreurs qui ont causé l'échec du chargement et de l'analyse aux emplacements suivants :

- Fichier non analysé : Examinez la fin du fichier pour repérer la dernière ligne ignorée du fichier de configuration de Check Point qui a été analysée avec succès.
- Fichier inattendu : Fichier non valide détecté pour Check Point. Par exemple, lors de la compression à l'aide de Mac OS, les fichiers système Mac sont créés. Supprimez les fichiers Mac.
- (Pour r75 à r77.30 seulement) Fichiers incorrectement nommés : Lorsque les fichiers de la politique de sécurité et ceux de la politique NAT ne sont pas nommés correctement pour Check Point. Renommez correctement les fichiers ACL et NAT.
- Fichiers manquants : Il manque certains fichiers dans le fichier config.zip de Check Point. Ajoutez les fichiers requis.

Remarque Pour r77, extrayez manuellement le fichier de configuration manquant. Pour en savoir plus, consultez Export the Check Point Configuration Files for r77 [exporter les fichiers de configuration Check Point pour r77].

Pour r80, utilisez Live Connect pour extraire le fichier de configuration approprié pour l'outil de migration de Cisco Secure Firewall. Pour en savoir plus, consultez Export the Check Point Configuration Files for r80 [exporter les fichiers de configuration Check Point pour r80].

Exemple de résolution de problèmes pour Check Point : Impossible de trouver le membre du groupe d'objets (pour les versions r75 à r77.30 seulement)

Dans cet exemple, le chargement et l'analyse du fichier de configuration Check Point ont échoué en raison d'une erreur dans la configuration d'un élément.

Étape 1 Consultez les messages d'erreur pour identifier le problème.

Cet échec a généré les messages d'erreur suivants :

Emplacement	Message d'erreur
Message de l'outil de migration Cisco Secure Firewall	Les fichiers de configuration Check Point ont été analysés et comportent des erreurs. Consultez la section sur les erreurs du rapport prémigration pour connaître les erreurs d'analyse et le rapport postmigration pour connaître les erreurs de transmission qui sont survenues pendant l'étape de transmission.
Fichier de journalisation	[ERROR | objectGroupRules] > "ERROR, SERVICE_GROUP_RULE not applied for port-group object [services_epacity_nt_abc] as CheckPoint object [ica] does not exist in <service> table;" [INFO | objectGroupRules] > "Parsing object-group service:[services_gvxs06]" [INFO | objectGroupRules] > "Parsing object-group service:[services_iphigenia]" [INFO | objectGroupRules] > "Parsing object-group service:[Services_KPN_ISP]"

Étape 2 Ouvrez le fichier Check Point `services.xml`.

Étape 3 Cherchez le groupe d'objets dont le nom est services_gvxs06.

Étape 4 Créez le membre manquant pour le groupe d'objets au moyen du tableau de bord intelligent.

Étape 5 Exporter de nouveau le fichier de configuration. Pour en savoir plus, consultez Export the Check Point Configuration Files [exporter les fichiers de configuration Check Point].

Étape 6 S'il n'y a plus d'erreurs, chargez le nouveau fichier de configuration Check Point compressé dans l'outil de migration Cisco Secure Firewall pour poursuivre la migration.

Exemple de résolution de problèmes pour Check Point (r80) concernant Live Connect

Exemple 1 : Demandez des détails sur le gestionnaire de sécurité Check Point.

Dans cet exemple, l'outil de migration Cisco Secure Firewall demande des détails pour le gestionnaire de sécurité Check Point.

Consultez les messages d'erreur pour identifier le problème. Cet échec a généré les messages d'erreur suivants :

Emplacement	Message d'erreur
Message de l'outil de migration Cisco Secure Firewall	Filtrer les demandes de détails pour le gestionnaire de sécurité Check Point.
Fichier de journalisation	[ERREUR | connect_cp]> « Unable to extract the Extracted-objects.json file due to credentials with insufficient privileges, time-out issues and so on. Refer Secure Firewall migration tool UG for more info » [impossible d'extraire le fichier Extracted-objects.json en raison des données d'identification ayant des privilèges insuffisants, des délais d'expiration, etc. Consultez le guide de l'utilisateur de l'outil de migration Cisco Secure Firewall pour en savoir plus.] 127.0.0.1 - - [20/Jul/2020 17:20:43] "POST /api/CP/connect HTTP/1.1" 500 -

Vos informations d'authentification sont erronées. Suivez les étapes mentionnées pour préparer les données d'identification. Les données d'identification utilisées doivent avoir un profil Shell */bin/bash* sur Check Point Gaia pour le gestionnaire de sécurité Check Point. Les mêmes données d'identification doivent être repérées sur l'application de console Check Point Smart pour le gestionnaire de sécurité Check Point ayant des privilèges de superutilisateur dans le cadre d'un déploiement normal. Les privilèges doivent être « super utilisateur » si vous utilisez un déploiement multidomaine. Pour en savoir plus, consultez la section Pre-stage the Check Point (r80) Devices for Configuration Extraction Using Live Connect [préparer les appareils Check Point (r80) pour l'extraction de la configuration au moyen de Live Connect].

Exemple 2 : Mauvais format de fichier

Dans le présent exemple, l'outil de migration Cisco Secure Firewall est bloqué en raison d'un mauvais format de fichier.

Consultez les messages d'erreur pour identifier le problème. Cet échec a généré les messages d'erreur suivants :

Emplacement	Message d'erreur
Message de l'outil de migration Cisco Secure Firewall	Bloqué

Emplacement	Message d'erreur
Fichier de journalisation	[ERROR | cp_device_connection] > "Bad file format" 2020-07-20 17:10:57,347 [ERROR | connect_cp] > "Unable to download .tar file". 127.0.0.1 - - [20/Jul/2020 17:10:57] "GET /api/CP/generate_tar_file?package=Standard HTTP/1.1" 500 -

Vos informations d'authentification sont erronées. Suivez les étapes mentionnées pour préparer les données d'identification. Les données d'identification utilisées doivent avoir un profil Shell */bin/bash* sur Check Point Gaia pour le gestionnaire de sécurité Check Point. Les mêmes données d'identification doivent être repérées sur l'application de console Check Point Smart pour le gestionnaire de sécurité Check Point ayant des privilèges de superutilisateur. Les privilèges de super utilisateur doivent être octroyés si vous utilisez un déploiement multidomaine. Pour en savoir plus, consultez la section Pre-stage the Check Point (r80) Devices for Configuration Extraction Using Live Connect [préparer les appareils Check Point (r80) pour l'extraction de la configuration au moyen de Live Connect].

Exemple 3 : La fonction VSX bloquée n'est PAS prise en charge par Threat Defense

Ici, dans l'exemple, l'outil de migration Cisco Secure Firewall échoue en raison du blocage de la fonction VSX dans la protection contre les menaces.

Consultez les messages d'erreur pour identifier le problème. Cet échec a généré les messages d'erreur suivants :

Emplacement	Message d'erreur
Message de l'outil de migration Cisco Secure Firewall	La fonction VSX bloquée n'est PAS prise en charge par FTD.
Fichier de journalisation	[ERROR | config_upload] > "VSX Feature is UNSUPPORTED in FTD" Recherche de la source (appel le plus récent)

Description du problème : Cette erreur se produit, car la commande **fw vsx stat** est obsolète à partir de la version r80.40 de Check Point.

Voici comment contourner le problème :

1. Décompressez le fichier zip *config.zip*.
2. Ouvrez le fichier *networking.txt*.

   Voici un exemple de l'exemple de sortie :

   ```
   firewall> fw vsx stat
   Deprecated command, Please see sk144112 for alternative
   Deprecated commands: cphaprob cpinfo cplic fw ips raidconfig fwaccel
   ```

   Faites le remplacement manuellement, comme suit :

   ```
   firewall> fw vsx stat
   VSX is not supported on this platform
   ```

3. Sélectionnez tous les fichiers et compressez-les de sorte qu'ils aient l'extension .zip.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.