BeyondTrust

Privileged Remote Access
Guide de mise à niveau

TC:9/25/2020

Table des matières

Mise à niveau du logiciel Privileged Remote Access BeyondTrust

Vous trouverez des informations détaillées sur chaque version du logiciel Privileged Remote Access BeyondTrust dans le Journal des modifications du produit.

Préparation de la mise à jour

- Avant de procéder à la mise à niveau, créez toujours une sauvegarde de vos paramètres et de votre configuration depuis **/login > Gestion > Logiciel**. Il est également conseillé d'exporter et d'enregistrer en local une copie des certificats SSL et de la clé privée, afin de garantir la continuité en cas d'échec de la mise à niveau.
- Pour les principales versions logicielles, les clients titulaires de contrats de maintenance en cours sont placés dans un calendrier de déploiement. Une fois que votre mise à niveau est prête, BeyondTrust vous alertera par e-mail pour lancer la procédure de mise à niveau.
- L'installation demande généralement entre 15 minutes et une heure. Toutefois, si vous stockez une grande quantité de données sur votre serveur (par ex. des enregistrements de session), l'installation peut durer beaucoup plus longtemps.
- BeyondTrust vous conseille de procéder aux mises à niveau au cours des fenêtres de maintenance programmées. Votre site BeyondTrust sera temporairement indisponible pendant la mise à niveau. Tous les utilisateurs connectés seront déconnectés et les sessions actives seront fermées.
- BeyondTrust recommande également de tester la mise à jour dans un environnement contrôlé avant de la déployer en production. Il est préférable de procéder à un test si vous disposez de deux serveurs en relation de reprise en séquence et lorsque vous effectuez une mise à jour asynchrone. (Voir « Vérification et test », page 13).
- En cas de problème lors de la mise à jour de la base, ne redémarrez pas le Secure Remote Access Appliance. Veuillez contacter l'Assistance technique BeyondTrust.
- Si vous disposez de deux serveurs définis dans une configuration de reprise en séquence, vous devez choisir entre la mise à jour synchrone et la mise à jour asynchrone.
    - Dans le cas de la mise à jour synchrone, le serveur principal est mis à jour en premier et conserve son rôle. Cette méthode implique un certain temps d'arrêt ; elle est recommandée pour les déploiements et scénarios simples qui peuvent être mis hors ligne le temps de la mise à jour.
    - Lors d'une mise à jour asynchrone, le serveur de sauvegarde est mis à jour en premier, puis adopte le rôle de serveur principal. Cette méthode permet un temps d'arrêt minimal, et est recommandée pour les déploiements importants et les scénarios reposant sur le maintien d'un temps de fonctionnement maximal. Ceci implique une certaine complexité, puisqu'il peut s'avérer nécessaire de modifier le réseau afin d'effecteur une reprise en séquence vers le serveur de sauvegarde.

Mises à niveau client

Seules certaines mises à niveau impliquent une mise à jour du logiciel client. Les mises à jours logicielles de base et les composants de licence additionnels ne nécessitent pas de mettre à jour le logiciel client. À l'inverse, les mises à jour de version de site requièrent des mises à jour. La plupart des mises à jour client s'effectuent automatiquement. Cependant, la procédure de mise à jour pour chaque type de client est présentée ci-après.

- Toute console d'accès installée devra être mise à niveau après la mise à niveau du site. Généralement, cela se fait automatiquement au prochain lancement de la console d'accès par l'utilisateur.

IMPORTANT !

Lorsque vous effectuez une mise à niveau vers le progiciel d'un site récemment créé, vérifiez que tous les magasins de certificats sont gérés de façon appropriée et sont à jour avant de passer à une nouvelle version de BeyondTrust. Si vous ne le faites pas, une majorité de vos Jump Client existants pourraient apparaître hors ligne.

  - les consoles d'accès précédemment déployées sur des ordinateurs verrouillés à l'aide de MSI peuvent nécessiter un redéploiement une fois la mise à niveau achevée.
  - Si la fonction de console d'accès ou de Jump Client extractible a été activée pour votre site par l'Assistance technique BeyondTrust, vous pouvez télécharger un installeur MSI afin de mettre à jour toute console d'accès et les Jump Clients avant de mettre à niveau le serveur. Pour ce faire, recherchez manuellement ou automatiquement les mises à jour disponibles. Notez que les clients mis à jour ne seront en ligne qu'une fois leur serveur mis à jour. Il n'est pas nécessaire de désinstaller le client d'origine avant de déployer le nouveau, car celui-ci devrait remplacer automatiquement l'installation d'origine. Il est cependant préférable de conserver une copie de l'ancien MSI afin de supprimer les installations obsolètes une fois le serveur mis à jour, au cas où cette suppression s'avère nécessaire. Le nouveau MSI n'en est pas capable.

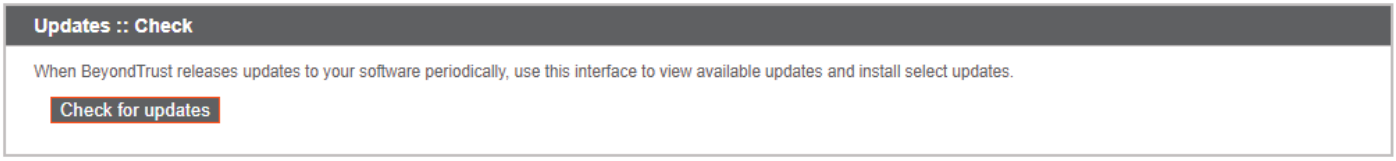
- Après une mise à niveau, les Jump Clients déployés sont automatiquement mis à jour.
  - Selon la bande passante disponible et le matériel utilisé, un trop grand nombre de mises à jour de Jump Clients simultanées peut entraîner la saturation du serveur, paralysant ainsi sévèrement le serveur et le réseau. Pour réguler la quantité de bande passante et de ressources utilisées par les mises à jour de Jump Client, allez dans **/login > Jump > Jump Clients**, et réglez le **Nombre maximal de mises à niveau de Jump Clients simultanées** sur une valeur plus basse.
  - Les Jump Clients actifs et passifs se mettent en file d'attente pour se mettre à jour lors de leur premier enregistrement auprès du serveur suite à la mise à jour de ce dernier. Ces évènements d'enregistrement se produisent à intervalles réguliers en partance de l'hôte des Jump Clients sur le port TCP 443 vers le serveur. Les Jump Clients actifs s'enregistrent immédiatement après qu'une mise à jour a été effectuée sur le serveur. Les Jump Clients passifs s'enregistrent au démarrage lors de l'établissement d'une connexion depuis la console d'accès, lorsqu'on leur dit de s'enregistrer depuis l'icône de la barre des tâches, et au moins une fois toutes les 24 heures.
  - Si un Jump Client n'a pas encore été mis à jour, il reçoit l'étiquette **Mise à niveau en attente**, et son numéro de version et de révision s'affiche dans le panneau de détails. Vous pouvez modifier un Jump Client obsolète, mais vous ne pouvez pas effectuer de Jump vers lui. Si vous tentez d'effectuer un Jump, ce Jump Client sera déplacé au début de la file d'attente de mise à niveau.
- De même, les Jumpoints déployés sont automatiquement mis à jour.

Remarque : *lors de la mise à niveau vers une nouvelle version logicielle, prévoyez du temps pour que tous les Jump Clients se reconnectent avant de passer aux autres processus de mise à niveau.*

- Les agents de connexion BeyondTrust se mettent automatiquement à jour après les mises à niveau de site.
- De même, les clients d'intégration BeyondTrust ne sont pas automatiquement mis à jour après les mises à niveau de site. Ils nécessitent également une réinstallation manuelle. Les installeurs des clients d'intégration sont disponibles sur la page **Téléchargements** à l'adresse beyondtrustcorp.service-now.com/csm.
- Lors de la mise à niveau, il sera nécessaire de recréer tous les packages d'installeur précédemment générés pour les Jump Clients et toute console d'accès. Les clients eux-mêmes sont mis à jour selon la procédure décrite ci-avant. Toutefois, les fichiers d'installation pour ces clients deviennent obsolètes après la mise à jour du serveur utilisé pour leur génération.

Mise à niveau d'un seul Secure Remote Access Appliance à l'aide des mises à jour automatiques

Dans la plupart des cas, les utilisateurs de BeyondTrust peuvent télécharger et installer des mises à jour sans l'aide de l'Assistance technique BeyondTrust. Pour voir si une mise à niveau est disponible, connectez-vous à votre Secure Remote Access Appliance (/appliance). Cliquez sur **Rechercher les mises à jour** sur la page **Mises à jour**.



Si une mise à jour logicielle est disponible, elle s'affichera sous **Mises à jour disponibles**. Lorsque vous cliquez sur **Installer cette mise à jour**, le serveur téléchargera et installera automatiquement la nouvelle version du logiciel BeyondTrust.

IMPORTANT !

Lorsque vous effectuez une mise à niveau vers le progiciel d'un site récemment créé, vérifiez que tous les magasins de certificats sont gérés de façon appropriée et sont à jour avant de passer à une nouvelle version de BeyondTrust. Si vous ne le faites pas, une majorité de vos Jump Client existants pourraient apparaître hors ligne.

***Remarque :** certains packages nécessitent l'installation préalable d'un autre package. Installez le package disponible pour activer celui qui en dépend.*

Si vous n'arrivez toujours pas à effectuer les mises à jour automatiques, consultez « Mise à niveau d'un seul Secure Remote Access Appliance avec les mises à jour manuelles », page 6.

Mise à niveau d'un seul Secure Remote Access Appliance avec les mises à jour manuelles

Si vous ne pouvez pas utiliser les mises à jour automatiques (par exemple, si votre serveur réside sur un réseau restreint), effectuez les mises à jour manuellement.

Connectez-vous à votre Secure Remote Access Appliance et allez sur la page **Mises à jour**. Cliquez sur le lien de la **Clé de téléchargement du serveur** pour générer une clé de serveur unique. Envoyez cette clé au serveur de mise à jour BeyondTrust (https://btupdate.com) à partir d'un système non restreint. Téléchargez toutes les mises à jour disponibles sur un périphérique de stockage amovible, puis transférez-les sur un système à partir duquel vous pouvez gérer votre serveur.

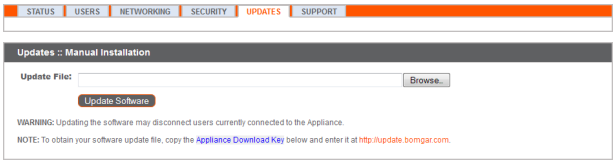
Sur la page **Mises à jour**, accédez au fichier à partir de la section **Installation manuelle**, puis cliquez sur le bouton **Mettre à jour le logiciel** pour terminer l'installation. Le serveur installera la nouvelle version du logiciel BeyondTrust.

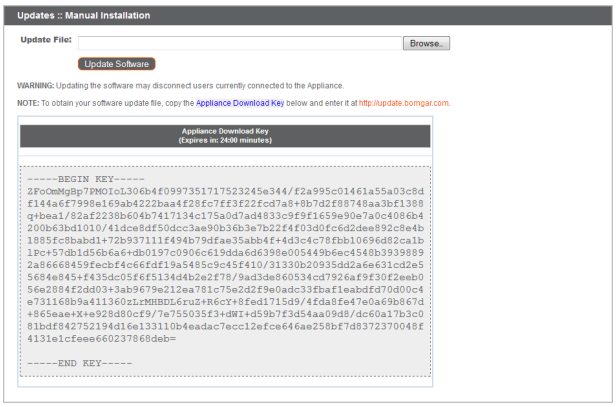
IMPORTANT !

Lorsque vous effectuez une mise à niveau vers le progiciel d'un site récemment créé, vérifiez que tous les magasins de certificats sont gérés de façon appropriée et sont à jour avant de passer à une nouvelle version de BeyondTrust. Si vous ne le faites pas, une majorité de vos Jump Client existants pourraient apparaître hors ligne.

***Remarque :** préparez-vous à installer les mises à jour du logiciel directement après le téléchargement. Une fois qu'une mise à jour a été téléchargée, elle n'apparaît plus sur votre liste de mises à jour disponibles. Si vous avez besoin de retélécharger une mise à jour, contactez l'Assistance technique BeyondTrust.*

***Remarque :** si une erreur se produit, vérifiez que l'heure donnée sur la page **/appliance > État > Caractéristiques** est correcte. De nombreuses fonctions du Secure Remote Access Appliance, comme la clé de téléchargement du serveur, reposent sur le fait que l'heure est bien réglée. Si l'heure n'est pas la bonne, veuillez vérifier le paramètre NTP sur la page **Réseau > Configuration IP**.*





Mise à niveau de deux serveurs dans une configuration de reprise en séquence

IMPORTANT !

BeyondTrust conseille de planifier les fenêtres de maintenance pendant les heures de faible trafic.

Il existe deux alternatives de mise à niveau dans un environnement de reprise en séquence : la mise à niveau synchrone et la mise à niveau asynchrone.

Mise à niveau synchrone de deux Secure Remote Access Appliances partageant une relation de reprise en séquence

Dans le cas de la mise à jour synchrone, le serveur principal est mis à jour en premier et conserve son rôle. Cette méthode implique un certain temps d'arrêt ; elle est recommandée pour les déploiements et scénarios simples qui peuvent être mis hors ligne le temps de la mise à jour.

Avantage : aucun événement de reprise en séquence.
Inconvénient : temps d'arrêt prolongé du site de production.

Mise à niveau asynchrone de deux Secure Remote Access Appliances partageant une relation de reprise en séquence

Lors d'une mise à jour asynchrone, le serveur de sauvegarde est mis à jour en premier, puis adopte le rôle de serveur principal. Cette méthode permet un temps d'arrêt minimal, et est recommandée pour les déploiements importants et les scénarios reposant sur le maintien d'un temps de fonctionnement maximal. Ceci implique une certaine complexité, puisqu'il peut s'avérer nécessaire de modifier le réseau afin d'effecteur une reprise en séquence vers le serveur de sauvegarde.

Avantage : temps d'arrêt minimal en production.
Inconvénient : requiert une activité de reprise en séquence.

Remarques

1. Sélectionnez l'alternative de reprise en séquence qui correspond le mieux à vos exigences en matière de temps d'arrêt et de continuité.
2. Prévoyez deux fenêtres de maintenance distinctes dans lesquelles effectuer la mise à niveau.
3. La durée du processus de mise à niveau sera identique sur les deux serveurs.
4. Entre les deux fenêtres de maintenance, prévoyez une période intermédiaire suffisamment longue pour permettre la confirmation de la nouvelle version logicielle dans votre environnement de production mais suffisamment brève pour minimiser le risque lié à l'absence temporaire de configuration de reprise en séquence.

Mise à niveau synchrone de deux Secure Remote Access Appliances partageant une relation de reprise en séquence

Dans le cas de la mise à jour synchrone, le serveur principal est mis à jour en premier et conserve son rôle. Cette méthode implique un certain temps d'arrêt ; elle est recommandée pour les déploiements et scénarios simples qui peuvent être mis hors ligne le temps de la mise à jour.

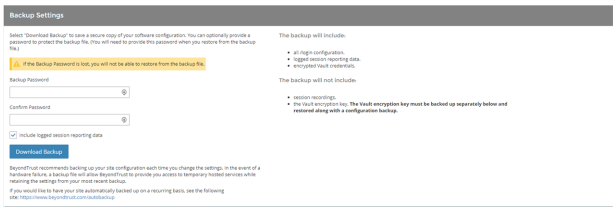
BeyondTrust vous conseille de procéder aux mises à niveau au cours des fenêtres de maintenance programmées. Votre site BeyondTrust sera temporairement indisponible pendant la mise à niveau. Tous les utilisateurs connectés seront déconnectés et les sessions actives seront fermées. Prévoyez deux fenêtres de maintenance distinctes dans lesquelles effectuer la mise à niveau. L'installation demande généralement entre 15 minutes et une heure. Toutefois, si vous stockez une grande quantité de données sur votre serveur (par ex. des enregistrements de session), l'installation peut durer beaucoup plus longtemps. Entre les deux fenêtres de maintenance, prévoyez une période intermédiaire suffisamment longue pour permettre la confirmation de la nouvelle version logicielle dans votre environnement de production, mais suffisamment brève pour minimiser le risque lié à l'absence temporaire de configuration de reprise en séquence. BeyondTrust recommande également de tester la mise à jour dans un environnement contrôlé avant de la déployer en production. En cas de problème lors de la mise à jour de la base, ne redémarrez pas le Secure Remote Access Appliance. Veuillez contacter l'Assistance technique BeyondTrust.

Les instructions suivantes supposent d'utiliser le **serveur A** comme serveur principal (le serveur auquel correspond le nom d'hôte principal) et le **serveur B** comme serveur de sauvegarde.

Sauvegarde et synchronisation

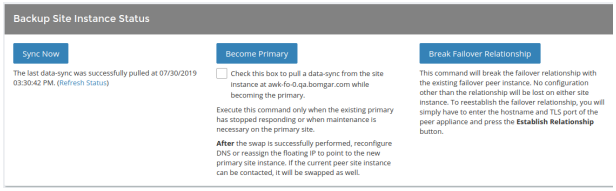
Avant toute mise à niveau, effectuez une sauvegarde de vos paramètres logiciels BeyondTrust actuels. Sur le **serveur A**, sélectionnez **/login > Gestion > Logiciel**.

Cliquez sur **Télécharger la sauvegarde**, puis enregistrez le fichier de sauvegarde à un emplacement sécurisé.



Allez dans **/login > Gestion > Reprise en séquence**, cliquez sur **Synchroniser maintenant** et attendez que la synchronisation soit terminée.

Une fois la synchronisation terminée, cliquez sur **Rompre les relations de reprise en séquence**.



Mise à jour du serveur A

Mettez à jour le **serveur A** à l'aide de la méthode automatique ou manuelle.

Automatique

Dans la plupart des cas, les utilisateurs de BeyondTrust peuvent télécharger et installer des mises à jour sans l'aide de l'Assistance technique BeyondTrust. Pour consulter les mises à jour disponibles, sélectionnez **/appliance > Mises à jour**.

Cliquez ensuite sur **Rechercher les mises à jour**.

Si une mise à jour logicielle est disponible, elle s'affichera sous **Mises à jour disponibles**. Lorsque vous cliquez sur **Installer cette mise à jour**, le serveur téléchargera et installera automatiquement la nouvelle version du logiciel BeyondTrust.

> ***Remarque :*** *Les mises à jour logicielles « BeyondTrust » dépendent souvent d'une ou plusieurs mises à jour du « logiciel de base ». Installez les mises à jour du logiciel de base disponibles pour activer les mises à jour BeyondTrust qui en dépendent. Téléchargez ensuite une sauvegarde et installez immédiatement les mises à jour logicielles BeyondTrust avant de faire quoi que ce soit d'autre, comme une reprise en séquence ou l'installation de mises à jour sur un autre serveur.*

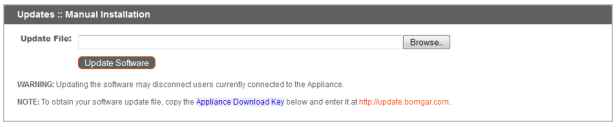
En cas d'échec des mises à jour automatiques, veuillez consulter le portail d'assistance technique pour obtenir de plus amples informations.

Mises à jour manuelles

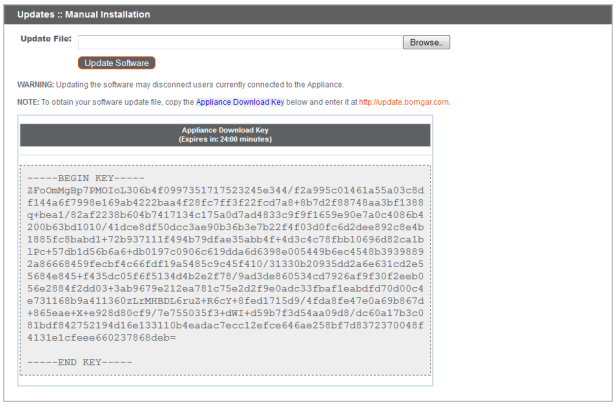
Si vous ne pouvez pas utiliser les mises à jour automatiques (par exemple, si votre serveur réside sur un réseau restreint), effectuez les mises à jour manuellement.

Allez dans **/appliance > Mises à jour**.

Cliquez sur le lien de la **Clé de téléchargement du serveur** pour générer une clé de serveur unique. Envoyez cette clé au serveur de mise à jour BeyondTrust (https://btupdate.com) à partir d'un système non restreint. Téléchargez toutes les mises à jour disponibles sur un périphérique de stockage amovible, puis transférez-les sur un système à partir duquel vous pouvez gérer votre serveur.



Sur la page **Mises à jour**, accédez au fichier à partir de la section **Installation manuelle**, puis cliquez sur le bouton **Mettre à jour le logiciel** pour terminer l'installation. Le serveur installera la nouvelle version du logiciel BeyondTrust.



> ***Remarque :*** *préparez-vous à installer les mises à jour du logiciel directement après le téléchargement. Une fois qu'une mise à jour a été téléchargée, elle n'apparaît plus sur votre liste de mises à jour disponibles. Si vous avez besoin de retélécharger une mise à jour, contactez l'Assistance technique BeyondTrust.*

Vérification et test

Une fois la mise à jour terminée, vérifiez que l'opération s'est correctement déroulée et que le logiciel fonctionne normalement. Toute console d'accès installée devra être mise à niveau après la mise à niveau du site. Généralement, cela se fait automatiquement au prochain lancement de la console d'accès par l'utilisateur. Pour connaître la version logicielle d'une console, connectez-vous à la

console et cliquez sur **Aide > À propos**. Assurez-vous également de pouvoir établir une connexion à un ordinateur distant par le biais d'une session.

> ***Remarque :*** *les consoles d'accès précédemment déployées sur des ordinateurs verrouillés à l'aide de MSI peuvent nécessiter un redéploiement une fois la mise à niveau achevée. Si la fonction de console d'accès ou de Jump Client extractible a été activée pour votre site par l'Assistance technique BeyondTrust, vous pouvez télécharger un installeur MSI afin de mettre à jour toute console d'accès et les Jump Clients avant de mettre à niveau le serveur. Pour ce faire, recherchez manuellement ou automatiquement les mises à jour disponibles. Notez que les clients mis à jour ne seront en ligne qu'une fois leur serveur mis à jour. Il n'est pas nécessaire de désinstaller le client d'origine avant de déployer le nouveau, car celui-ci devrait remplacer automatiquement l'installation d'origine. Il est cependant préférable de conserver une copie de l'ancien MSI afin de supprimer les installations obsolètes une fois le serveur mis à jour, au cas où cette suppression s'avère nécessaire. Le nouveau MSI n'en est pas capable.*

Mise à jour du serveur B

Mettez à jour le **serveur B** à l'aide de la méthode automatique ou manuelle, comme défini précédemment. Vérifiez ensuite la bonne exécution de la mise à jour.

Restauration d'une relation de reprise en séquence

Sur le **serveur A**, sélectionnez **/login > Gestion > Reprise en séquence**.

> ***Remarque :*** *pour pouvoir configurer une connexion valide, les deux serveurs doivent présenter des clés inter-serveurs identiques. Accédez à la page **/login > Gestion > Sécurité** pour vérifier la clé de chaque serveur.*

Rétablissez la relation de reprise en séquence avec le serveur de sauvegarde en utilisant le **serveur B** en tant que serveur de sauvegarde et le **serveur A** en tant que serveur principal.

La définition de la relation entre les deux serveurs doit être effectuée via la page **Reprise en séquence** du serveur devant agir en tant que serveur principal. Les adresses saisies permettent d'établir la relation, afin que les serveurs puissent se connecter l'un à l'autre à n'importe quel moment. La section **Informations de connexion du nouveau site de sauvegarde** indique au serveur principal comment se connecter au serveur qui deviendra le serveur de sauvegarde. Les champs **Rapporter les informations de connexion à ce site primaire** sont fournis au serveur de sauvegarde et lui disent comment se connecter à son serveur principal. Vous devez spécifier un nom d'hôte ou une adresse IP valide, ainsi qu'un numéro de port TLS pour ces champs. Une fois terminé, cliquez sur **Établir une relation** pour établir la relation.

> ***Remarque :*** *chaque fois que cela s'avère possible, BeyondTrust recommande d'utiliser l'adresse IP unique de chacun des serveurs lors de la configuration de ces paramètres.*

Une fois la relation établie, les onglets superflus sont supprimés du site de sauvegarde. La synchronisation initiale des données démarre après environ 60 secondes, mais vous pouvez également cliquer sur **Synchroniser maintenant** pour forcer la synchronisation et transférer les informations les plus récentes du serveur principal dans la mémoire du serveur de sauvegarde. Le processus de synchronisation en lui-même peut durer de quelques secondes à plusieurs heures, en fonction de la quantité de données à traiter. Une fois la synchronisation terminée, la page **Reprise en séquence** affiche la date et l'heure de la dernière synchronisation de données.

Mise à niveau asynchrone de deux Secure Remote Access Appliances partageant une relation de reprise en séquence

Lors d'une mise à jour asynchrone, le serveur de sauvegarde est mis à jour en premier, puis adopte le rôle de serveur principal. Cette méthode permet un temps d'arrêt minimal, et est recommandée pour les déploiements importants et les scénarios reposant sur le maintien d'un temps de fonctionnement maximal. Ceci implique une certaine complexité, puisqu'il peut s'avérer nécessaire de modifier le réseau afin d'effecteur une reprise en séquence vers le serveur de sauvegarde.

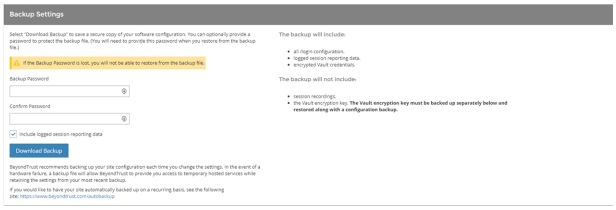
BeyondTrust vous conseille de procéder aux mises à niveau au cours des fenêtres de maintenance programmées. Votre site BeyondTrust sera temporairement indisponible pendant la mise à niveau. Tous les utilisateurs connectés seront déconnectés et les sessions actives seront fermées. Prévoyez deux fenêtres de maintenance distinctes dans lesquelles effectuer la mise à niveau. L'installation demande généralement entre 15 minutes et une heure. Toutefois, si vous stockez une grande quantité de données sur votre serveur (par ex. des enregistrements de session), l'installation peut durer beaucoup plus longtemps. Entre les deux fenêtres de maintenance, prévoyez une période intermédiaire suffisamment longue pour permettre la confirmation de la nouvelle version logicielle dans votre environnement de production, mais suffisamment brève pour minimiser le risque lié à l'absence temporaire de configuration de reprise en séquence. BeyondTrust recommande également de tester la mise à jour dans un environnement contrôlé avant de la déployer en production. En cas de problème lors de la mise à jour de la base, ne redémarrez pas le Secure Remote Access Appliance. Veuillez contacter l'Assistance technique BeyondTrust.

Les instructions suivantes supposent d'utiliser le **serveur A** comme serveur principal (le serveur auquel correspond le nom d'hôte principal) et le **serveur B** comme serveur de sauvegarde.

Sauvegarde et synchronisation

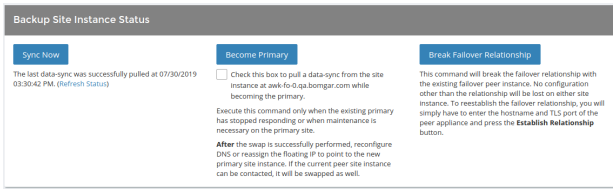
Avant toute mise à niveau, effectuez une sauvegarde de vos paramètres logiciels BeyondTrust actuels. Sur le **serveur A**, sélectionnez **/login > Gestion > Logiciel**.

Cliquez sur **Télécharger la sauvegarde**, puis enregistrez le fichier de sauvegarde à un emplacement sécurisé.



Allez dans **/login > Gestion > Reprise en séquence**, cliquez sur **Synchroniser maintenant** et attendez que la synchronisation soit terminée.

Une fois la synchronisation terminée, cliquez sur **Rompre les relations de reprise en séquence**.



Mise à jour du serveur B

Mettez à jour le **serveur B** à l'aide de la méthode automatique ou manuelle.

Automatique

Dans la plupart des cas, les utilisateurs de BeyondTrust peuvent télécharger et installer des mises à jour sans l'aide de l'Assistance technique BeyondTrust. Pour consulter les mises à jour disponibles, sélectionnez **/appliance > Mises à jour**.

Cliquez ensuite sur **Rechercher les mises à jour**.

Si une mise à jour logicielle est disponible, elle s'affichera sous **Mises à jour disponibles**. Lorsque vous cliquez sur **Installer cette mise à jour**, le serveur téléchargera et installera automatiquement la nouvelle version du logiciel BeyondTrust.

> ***Remarque :*** *Les mises à jour logicielles « BeyondTrust » dépendent souvent d'une ou plusieurs mises à jour du « logiciel de base ». Installez les mises à jour du logiciel de base disponibles pour activer les mises à jour BeyondTrust qui en dépendent. Téléchargez ensuite une sauvegarde et installez immédiatement les mises à jour logicielles BeyondTrust avant de faire quoi que ce soit d'autre, comme une reprise en séquence ou l'installation de mises à jour sur un autre serveur.*

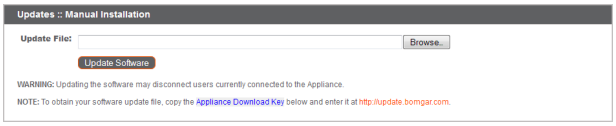
En cas d'échec des mises à jour automatiques, veuillez consulter le portail d'assistance technique pour obtenir de plus amples informations.

Mises à jour manuelles

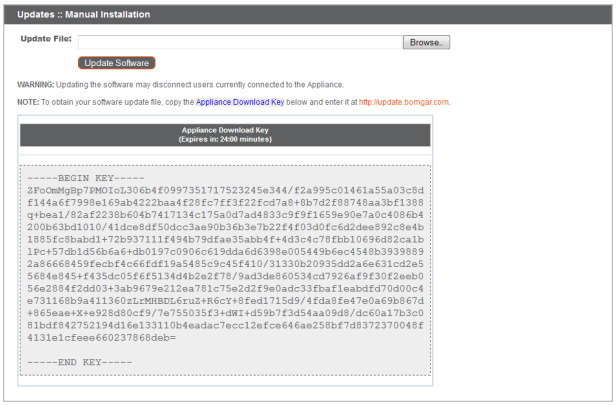
Si vous ne pouvez pas utiliser les mises à jour automatiques (par exemple, si votre serveur réside sur un réseau restreint), effectuez les mises à jour manuellement.

Allez dans **/appliance > Mises à jour**.

Cliquez sur le lien de la **Clé de téléchargement du serveur** pour générer une clé de serveur unique. Envoyez cette clé au serveur de mise à jour BeyondTrust (https://btupdate.com) à partir d'un système non restreint. Téléchargez toutes les mises à jour disponibles sur un périphérique de stockage amovible, puis transférez-les sur un système à partir duquel vous pouvez gérer votre serveur.



Sur la page **Mises à jour**, accédez au fichier à partir de la section **Installation manuelle**, puis cliquez sur le bouton **Mettre à jour le logiciel** pour terminer l'installation. Le serveur installera la nouvelle version du logiciel BeyondTrust.



> ***Remarque :*** *préparez-vous à installer les mises à jour du logiciel directement après le téléchargement. Une fois qu'une mise à jour a été téléchargée, elle n'apparaît plus sur votre liste de mises à jour disponibles. Si vous avez besoin de retélécharger une mise à jour, contactez l'Assistance technique BeyondTrust.*

Vérification et test

Une fois la mise à jour terminée, vérifiez que l'opération s'est correctement déroulée et que le logiciel fonctionne normalement.

Sur au moins deux machines locales ayant accès au **serveur B**, modifiez le fichier d'hôtes de sorte que le nom d'hôte de votre site renvoie vers l'adresse IP du **serveur B**. Lancez la console d'accès. Toute console d'accès installée devra être mise à niveau après la mise à niveau du site. Généralement, cela se fait automatiquement au prochain lancement de la console d'accès par l'utilisateur. Pour connaître la version logicielle d'une console, connectez-vous à la console et cliquez sur **Aide > À propos**. Assurez-vous également de pouvoir établir une connexion à un ordinateur distant par le biais d'une session.

> ***Remarque :*** *les consoles d'accès précédemment déployées sur des ordinateurs verrouillés à l'aide de MSI peuvent nécessiter un redéploiement une fois la mise à niveau achevée. Si la fonction de console d'accès ou de Jump Client extractible a été activée pour votre site par l'Assistance technique BeyondTrust, vous pouvez télécharger un installeur MSI afin de mettre à jour toute console d'accès et les Jump Clients avant de mettre à niveau le serveur. Pour ce faire, recherchez manuellement ou automatiquement les mises à jour disponibles. Notez que les clients mis à jour ne seront en ligne qu'une fois leur serveur mis à jour. Il n'est pas nécessaire de désinstaller le client d'origine avant de déployer le nouveau, car celui-ci devrait remplacer automatiquement l'installation d'origine. Il est cependant préférable de conserver une copie de l'ancien MSI afin de supprimer les installations obsolètes une fois le serveur mis à jour, au cas où cette suppression s'avère nécessaire. Le nouveau MSI n'en est pas capable.*

Définition du serveur B en tant que serveur principal

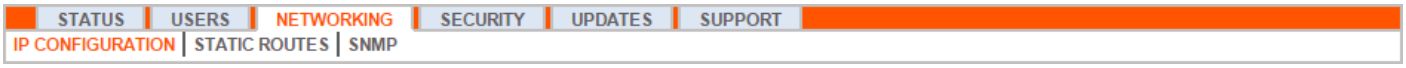
Définissez le **serveur B** en tant que serveur principal, conformément aux étapes précédemment déterminées dans le plan de reprise en séquence : modification de l'adresse IP partagée, modification de l'entrée DNS ou modification de l'entrée NAT.

> ***Remarque :*** *Si vous utilisez le client d'intégration BeyondTrust et que vous l'avez configuré d'après l'adresse IP plutôt que d'après le nom d'hôte, vérifiez qu'il peut extraire les données du **serveur B** après avoir défini le **serveur B** comme serveur principal.*

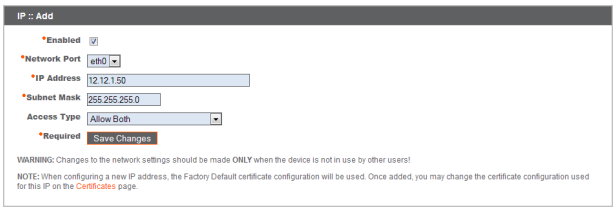
> ***Remarque :*** *les données des sessions réalisées sur l'un des serveurs tandis que la reprise en séquence n'est pas activée seront automatiquement synchronisées une fois la relation de reprise en séquence rétablie.*

Modification de l'adresse IP partagée

Sur le **serveur A**, sélectionnez **/appliance > Réseau > Configuration IP**.



Cliquez sur l'adresse IP partagée pour la modifier, puis décochez la case **Activé**. Cliquez ensuite sur **Enregistrer les modifications**.



Sélectionnez à présent **/appliance > Réseau > Configuration IP** sur le **serveur B**. Il est judicieux d'afficher préalablement cette page dans un autre onglet de navigation.

Cliquez sur l'adresse IP partagée pour la modifier, puis cochez la case **Activé**. Cliquez ensuite sur **Enregistrer les modifications**.

Dès que le changement est fait, vous pouvez reprendre des activités normales. Toutes les demandes pour votre site seront prises en charge par le **serveur B**.

Modification de l'entrée DNS

Accédez au contrôleur DNS et trouvez l'entrée DNS de votre site BeyondTrust. Modifiez l'entrée pour qu'elle pointe vers l'adresse IP du **serveur B**. Une fois l'entrée DNS propagée, vous pouvez reprendre vos activités normales. Toutes les demandes pour votre site seront prises en charge par le **serveur B**.

Modification de l'entrée NAT

Accédez au contrôleur NAT et trouvez l'entrée NAT de votre site BeyondTrust. Modifiez l'entrée pour qu'elle pointe vers l'adresse IP du **serveur B**. Une fois la modification effectuée, vous pouvez reprendre vos activités normales. Toutes les demandes pour votre site seront prises en charge par le **serveur B**.

Mise à jour du serveur A

> ***Remarque :*** *Chaque environnement varie en fonction de l'utilisateur, et bien que BeyondTrust teste chacune des fonctions, il nous est impossible d'essayer l'ensemble des scénarios qu'un utilisateur est susceptible de rencontrer. Veuillez confirmer que le logiciel BeyondTrust fonctionne correctement dans votre environnement avant de mettre à jour le serveur A.*

Mettez à jour le **serveur A** à l'aide de la méthode automatique ou manuelle, comme défini précédemment. Vérifiez ensuite la bonne exécution de la mise à jour.

Restauration d'une relation de reprise en séquence

Sur le **serveur B**, sélectionnez **/login > Gestion > Reprise en séquence**.

> ***Remarque :*** *pour pouvoir configurer une connexion valide, les deux serveurs doivent présenter des clés inter-serveurs identiques. Accédez à la page* ***/login > Gestion > Sécurité*** *pour vérifier la clé de chaque serveur.*

Rétablissez la relation de reprise en séquence avec le serveur de sauvegarde, en utilisant le **serveur A** en tant que serveur de sauvegarde et le **serveur B** en tant que serveur principal.

La définition de la relation entre les deux serveurs doit être effectuée via la page **Reprise en séquence** du serveur devant agir en tant que serveur principal. Les adresses saisies permettent d'établir la relation, afin que les serveurs puissent se connecter l'un à l'autre à n'importe quel moment. La section **Informations de connexion du nouveau site de sauvegarde** indique au serveur principal comment se connecter au serveur qui deviendra le serveur de sauvegarde. Les champs **Rapporter les informations de connexion à ce site primaire** sont fournis au serveur de sauvegarde et lui disent comment se connecter à son serveur principal. Vous devez spécifier un nom d'hôte ou une adresse IP valide, ainsi qu'un numéro de port TLS pour ces champs. Une fois terminé, cliquez sur **Établir une relation** pour établir la relation.

> ***Remarque :*** *chaque fois que cela s'avère possible, BeyondTrust recommande d'utiliser l'adresse IP unique de chacun des serveurs lors de la configuration de ces paramètres.*

Une fois la relation établie, les onglets superflus sont supprimés du site de sauvegarde. La synchronisation initiale des données démarre après environ 60 secondes, mais vous pouvez également cliquer sur **Synchroniser maintenant** pour forcer la synchronisation et transférer les informations les plus récentes du serveur principal dans la mémoire du serveur de sauvegarde. Le processus de synchronisation en lui-même peut durer de quelques secondes à plusieurs heures, en fonction de la quantité de données à traiter. Une fois la synchronisation terminée, la page **Reprise en séquence** affiche la date et l'heure de la dernière synchronisation de données.

Mise à niveau du matériel BeyondTrust

Lorsque vous mettez à niveau votre Secure Remote Access Appliance d'un serveur physique à un autre, ou entre un serveur physique et un PRA Virtual Appliance, vous devez à la fois installer le nouveau serveur et transférer les données depuis le serveur d'origine.

1. Installez le nouveau serveur selon le guide de mise en place approprié.
   - Installation de PRA Virtual Appliance BeyondTrust : www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/virtual/index .htm
   - Installation matérielle de Secure Remote Access Appliance : www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/hardware index.htm
2. Sauvegardez les paramètres logiciels actuels de votre serveur.
   a. Sur votre serveur actuel, sélectionnez **/login > Gestion > Logiciel**.
   b. Dans la section **Logiciel :: Paramètres de sauvegarde**, cliquez sur le bouton **Télécharger la sauvegarde**.
   c. Enregistrez le fichier de sauvegarde dans un emplacement sécurisé.
3. Importez votre chaîne de certificat SSL existante dans le nouveau serveur.
   a. Sur votre serveur actuel, sélectionnez **/appliance > Sécurité > Certificats**.
   b. Dans la section **Sécurité :: Certificats**, cochez la case à côté du certificat assigné à l'adresse IP active. Sélectionnez ensuite **Exporter** dans le menu déroulant situé en haut de la section.

      Remarque : *exporter des certificats ne les supprime pas du serveur.*

   c. Sur la page **Sécurité :: Certificats :: Exportation**, cochez les options pour inclure le certificat, la clé privée et la chaîne de certificat. Il est fortement recommandé que vous définissiez une phrase secrète pour la clé privée.
   d. Sur votre nouveau serveur, sélectionnez **/appliance > Sécurité > Certificats**.
   e. Dans la section **Sécurité :: Installation d'un certificat**, cliquez sur le bouton **Importer**.
   f. Naviguez jusqu'au fichier de certificat que vous avez exporté auparavant, puis cliquez sur **Transférer**.
4. Choisissez un certificat par défaut pour servir vos clients.
   a. Sur votre nouveau serveur, sélectionnez **/appliance > Sécurité > Certificats**.
   b. Dans la section **Sécurité :: Certificats**, trouvez l'entrée pour votre certificat SSL. Il comporte en général un champ **Remis à** contenant le nom de domaine complet de votre serveur (par ex. access.example.com).
   c. Confirmez qu'il n'existe pas d'avertissement répertorié pour le nouveau certificat. S'il y a un avertissement, veuillez accéder au Portail d'assistance technique pour obtenir de l'aide.
   d. Une fois tous les avertissements résolus, cliquez sur le bouton radio dans la colonne **Par défaut** du certificat que vous souhaitez servir à vos clients.
5. Installez le nouveau progiciel.
   a. Sur votre nouveau serveur, allez dans **/appliance > Mises à jour**.
   b. Cliquez sur **Rechercher les mises à jour** ou utilisez la **Clé de téléchargement du serveur**, suivant les instructions à l'écran.
   c. Cliquez sur **Installer cette mise à jour**. Un CLUF devra être signé avant l'installation.

6. Importez vos paramètres de configuration logicielle depuis votre ancien serveur.
    a. Connectez-vous à l'interface /login de votre nouveau serveur. Les informations d'authentification initiales sont **admin** et **password**.
    b. Allez sur **/login > Gestion > Logiciel**.
    c. Dans la section **Logiciel :: Restaurer les paramètres**, naviguez jusqu'au fichier de sauvegarde que vous avez téléchargé auparavant, puis cliquez sur **Transférer une sauvegarde** pour restaurer la sauvegarde sur le nouveau serveur.

Vous pouvez alors mettre à jour votre serveur DNS pour qu'il dirige le trafic vers les adresses IP du nouveau serveur, et vous pouvez commencer à tester l'session d'accès sur votre nouveau serveur. Une fois que vous avez confirmé qu'il fonctionne correctement, vous pouvez renvoyer l'ancien serveur s'il est physique, ou le supprimer s'il est virtuel. Pour renvoyer un serveur physique, suivez ces étapes :

1. Connectez-vous à l'interface Web **/appliance** de l'ancien serveur.
2. Allez sur la page **Statut > Bases** et cliquez sur **Rétablir la version par défaut du serveur**.
3. Attendez la fin de la réinitialisation, puis cliquez sur **Éteindre ce serveur**.
4. Emballez le serveur pour l'expédition.
5. Collez l'étiquette d'expédition de retour BeyondTrust sur le colis et contactez votre expéditeur pour qu'il vienne le récupérer. Si vous n'avez pas d'étiquette d'expédition, contactez l'Assistance technique BeyondTrust.

Avis de non-responsabilité, limitations associées à la licence et assistance technique

Avis de non-responsabilité

Ce document est fourni exclusivement à titre informatif. BeyondTrust Corporation peut modifier ce contenu sans préavis. Le présent document n'est pas garanti être dépourvu d'erreurs, ni ne fait l'objet d'autres garanties ou conditions, orales ou implicites en vertu de la loi, y compris des garanties et conditions implicites de qualité marchande ou d'adéquation à des fins données. BeyondTrust Corporation décline spécifiquement toute responsabilité concernant le présent document et aucune obligation contractuelle n'est formulée, directement ou indirectement, par le présent document. Les technologies, fonctionnalités, services et processus décrits aux présentes peuvent faire l'objet de modifications sans préavis.

Tous droits réservés. Les autres marques déposées identifiées sur cette page sont la propriété de leurs propriétaires respectifs. BeyondTrust n'est pas une banque à charte, une société de fiducie ou une institution de dépôt. Elle n'est pas autorisée à accepter des dépôts ou des comptes en fiducie et n'est ni sous licence ni gouvernée par une autorité bancaire nationale ou fédérale.

Limitations associées à la licence

Une licence Privileged Remote Access BeyondTrust permet à un technicien d'assistance à la fois d'intervenir sur un nombre illimité d'ordinateurs distants, en mode surveillé ou non surveillé. Même si plusieurs comptes peuvent partager la même licence, il faut deux licences ou plus (une pour chacun des techniciens Service client présents) pour permettre à plusieurs techniciens Service client d'intervenir simultanément.

Une licence Privileged Remote Access BeyondTrust vous permet d'accéder à un système de point de terminaison. Bien que cette licence puisse être transférée d'un système à un autre si vous n'avez plus besoin d'accéder au premier, deux licences ou plus (une par point de terminaison) sont requises pour permettre l'accès à plusieurs points de terminaison à la fois.

Assistance technique

Chez BeyondTrust, nous nous engageons à fournir une qualité de service optimale en veillant à ce que nos clients disposent de tout ce qui est nécessaire à une productivité maximale. Si vous avez besoin d'aide, contactez l'Assistance technique BeyondTrust à l'adresse www.beyondtrust.com/support.

Pour bénéficier de l'assistance technique, vous devez souscrire chaque année un plan de maintenance.