



BeyondTrust


Serveur virtuel Guide d'installation

Table des matières

Mise à niveau du logiciel BeyondTrust	3
Mise à niveau d'un serveur d'accès à distance sécurisé unique à l'aide des mises à jour automatiques	6
Mise à niveau d'un serveur d'accès à distance sécurisé unique à l'aide des mises à jour manuelles	8
Mise à niveau de deux serveurs d'accès à distance sécurisé dans une configuration de reprise en séquence	10
Mise à niveau synchrone de deux serveurs partageant une relation de reprise en séquence	11
Sauvegarde et synchronisation	11
Mise à jour du serveur A	12
Vérification et test	13
Mise à jour du serveur B	13
Restauration d'une relation de reprise en séquence	13
Mise à niveau asynchrone de deux serveurs partageant une relation de reprise en séquence	15
Sauvegarde et synchronisation	15
Mise à jour du serveur B	16
Vérification et test	17
Définition du serveur B en tant que serveur principal	17
Mise à jour du serveur A	18
Restauration d'une relation de reprise en séquence	19
Mise à niveau de plusieurs serveurs d'accès à distance sécurisé dans un cluster Atlas 20	
Avec la reprise en séquence configurée	20
Sans reprise en séquence configurée	22
Mise à niveau de matériel BeyondTrust	24
Avis de non-responsabilité, limitations associées à la licence et assistance technique ..	26

Mise à niveau du logiciel BeyondTrust

Vous trouverez des informations détaillées sur chaque version du logiciel d'assistance technique à distance BeyondTrust dans le [Journal des modifications du produit](#).

 **Remarque :** Si votre logiciel BeyondTrust n'a pas été mis à jour depuis un certain temps et qu'il est dépassé de plusieurs révisions par rapport à la dernière version, il vous faudra probablement installer plusieurs versions intermédiaires avant d'installer la dernière. Reportez-vous au troisième point pour plus de détails.

Préparation de la mise à jour

- Avant de procéder à la mise à jour, créez toujours une sauvegarde de vos paramètres et de votre configuration depuis **/login > Gestion > Gestion du 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 votre mise à niveau prête, BeyondTrust vous préviendra par e-mail pour en lancer la procédure.
- Si votre serveur n'a pas été mis à jour depuis plusieurs mois ou plusieurs années, il est peu probable qu'il puisse être mis à niveau directement avec la dernière version de BeyondTrust en une seule installation. Dans ce cas, certains paquets de mise à jour peuvent être grisés dans la liste des mises à jour et nécessiter l'installation préalable d'un autre paquet. Sélectionnez **Installer cette mise à jour** sur le package disponible pour activer la mise à jour correspondante.
 - Si vous n'êtes pas sûr des mises à jour à installer ou dans quel ordre le faire, contactez l'assistance technique BeyondTrust à l'adresse beyondtrust.com/docs/index.htm#support en fournissant une capture d'écran de votre page **/appliance > État > Caractéristiques** afin de déterminer les mises à jour spécifiques nécessaires pour votre serveur.
 - Dans les cas où des mises à jour BeyondTrust intermédiaires doivent être installées avant la version la plus récente, les logiciels clients BeyondTrust ne devraient pas se mettre à jour automatiquement, à moins qu'on leur laisse le temps de récupérer les mises à jour intermédiaires. BeyondTrust recommande donc que vous attendiez au moins 24 heures après l'installation de chaque paquet contenant le préfixe « BeyondTrust ».
 - Les mises à jour de base ne nécessitent pas de temps d'attente, mais elles sont en général requises pour les paquets « BeyondTrust ». Les mises à jour de base sont ainsi habituellement installées immédiatement avant les paquets « BeyondTrust ».
 - S'il est impossible de réserver 24 heures pour que les mises à jour automatiques du client se fassent, l'alternative à la mise à jour automatique consiste à premièrement retirer tous les logiciels clients, y compris les consoles des techniciens d'assistance, Jump Clients, Jumpoints, boutons d'assistance technique, agents de connexion, etc. Installez chaque mise à niveau « BeyondTrust » et mise à niveau de base en séquence jusqu'à la dernière version en date. Redémarrez ensuite manuellement tous les logiciels clients.
- 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 17).

- En cas de problème lors de la mise à jour de base, ne redémarrez pas le serveur d'accès à distance sécurisé. 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'effectuer 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.



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. À défaut, la majorité de vos Jump Clients existants peuvent apparaître hors ligne.

- Les consoles du technicien d'assistance installées devront être mises à niveau après la mise à niveau du site. Généralement, cela se fait automatiquement à la prochaine exécution de la console du technicien d'assistance par un technicien d'assistance.
 - les consoles du technicien d'assistance précédemment déployées sur des ordinateurs verrouillées à l'aide de [MSI](#) peuvent nécessiter un redéploiement une fois la mise à niveau achevée.
 - Si la fonction de console du technicien d'assistance ou de Jump Client extractible a été activée pour votre site par l'assistance technique BeyondTrust, vous pouvez télécharger un installateur MSI afin de mettre à jour les consoles du technicien d'assistance et les Jump Clients avant de mettre à niveau le serveur. Pour ce faire, recherchez manuellement ou automatiquement les mises à jour disponibles. Cliquez sur le lien **Installeurs de console du technicien d'assistance** ou **Installeurs de Jump Client** pour télécharger l'installateur MSI à des fins de distribution. 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** et/ou la **Bande passante maximale pour les mises à niveau simultanées de Jump Client** sur une valeur plus basse.

- Les Jump Clients actifs et passifs font la queue pour se mettre à jour lors de leur premier enregistrement auprès du serveur suite à la mise à jour de ce dernier. Ces événements 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 à la console du technicien d'assistance, 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 portera la mention **Mise à niveau en attente**, et ses numéros de version et de révision seront affichés dans le panneau des détails. Vous pouvez modifier un Jump Client obsolète, mais vous ne pouvez pas effectuer un Jump vers celui-ci. Si vous tentez d'effectuer un Jump, ce Jump Client sera déplacé au début de la file d'attente de mise à niveau.
- Si votre serveur d'accès à distance sécurisé est obsolète, plusieurs mises à jour peuvent s'avérer nécessaires pour atteindre la version actuelle. Dans ce cas, BeyondTrust recommande d'attendre au moins 24 heures entre les mises à jour afin de permettre la mise à niveau des Jump Clients. La durée nécessaire à la mise à jour des Jump Clients passifs peut être supérieure à 24 heures en fonction de la durée pendant laquelle les systèmes hôte restent hors ligne.



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.

- Vous saurez que la mise à jour a réussi lorsque le Jump Client apparaîtra comme étant en ligne dans la console du technicien d'assistance ou sur la page **/login > État > Informations**. Il existe un moyen efficace pour s'assurer que tous les Jump Clients ont bien été mis à jour. Connectez-vous à la console du technicien d'assistance avec un compte administrateur disposant des droits de modification sur tous les Jump Clients du système. Exportez la liste des Jump Clients. Dans le rapport ainsi généré, triez les Jump Clients par **Détails de statut**, puis vérifiez que toutes les dates sont postérieures à celle de la dernière mise à niveau du serveur d'accès à distance sécurisé.
- Si vous procédez à plusieurs installations sans laisser suffisamment de temps pour la mise à jour des Jump Clients, ces derniers peuvent nécessiter un redéploiement manuel.
- Après une mise à niveau, les boutons d'assistance technique sont automatiquement mis à jour lors de leur première utilisation.
- De même, les Jumpoints déployés sont automatiquement mis à jour.
- Les agents de connexion BeyondTrust se mettent automatiquement à jour après les mises à niveau du site.
- Les clients d'intégration BeyondTrust ne sont pas automatiquement mis à jour après les mises à niveau du site. Les clients d'intégration doivent être réinstallés manuellement. Les programmes d'installation des clients d'intégration sont disponibles sur la page **Téléchargements** à l'adresse beyondtrust.com/docs/index.htm#support.
- Lors de la mise à niveau, il est nécessaire de recréer tous les packages d'installateur précédemment générés pour les boutons d'assistance technique, les Jump Clients et les consoles des techniciens d'assistance. Les clients eux-mêmes sont mis à jour selon la procédure décrite ci-dessus. Toutefois, les fichiers d'installation pour ces clients deviennent obsolètes après la mise à niveau du serveur utilisé pour leur génération.

Mise à niveau d'un serveur d'accès à distance sécurisé unique 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 serveur d'accès à distance sécurisé (/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. À défaut, la majorité de vos Jump Clients existants peuvent apparaître hors ligne.

Updates :: Check

When Bomgar releases updates to your software periodically, use this interface to view available updates and install select updates.

There are updates available to be installed

– Available Updates

Base Software 3.3.2	Install This Update
Bomgar-12.2.0	
3.2.4 does not satisfy 12.2.0's requirements. Please install any other available package by clicking "Install this Update".	
<ul style="list-style-type: none">◦ Primary Hostname: support.example.com◦ Licenses: 15◦ Expires: Never	



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

En cas d'échec des mises à jour automatiques, consultez la FAQ de dépannage relative à la recherche des mises à jour à l'adresse www.beyondtrustcorp.service-now.com/csm/SolutionFAQ.aspx?id=377. Si vous n'arrivez toujours pas à effectuer les mises à jour automatiques, consultez « Mise à niveau d'un serveur d'accès à distance sécurisé unique à l'aide des mises à jour manuelles », page 8.

Mise à niveau d'un serveur d'accès à distance sécurisé unique à l'aide des 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 serveur d'accès à distance sécurisé et allez sur la page **Mises à jour**. À partir de la version Base 3.3.2, cliquez sur le lien **Clé de téléchargement du serveur** pour générer une clé de serveur unique ; pour les versions antérieures, contactez l'assistance technique BeyondTrust pour demander cette clé. Envoyez ensuite cette clé au serveur de mise à jour BeyondTrust (<https://update.bomgar.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 !

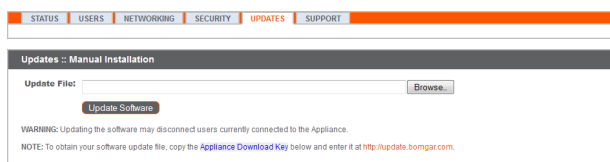
Lorsque vous effectuez une mise à niveau vers le progiciel d'un site récemment créé, vérifiez que tous les magasins de certificats sont gérés de façon appropriée et sont à jour avant de passer à une nouvelle version de BeyondTrust. À défaut, la majorité de vos Jump Clients existants peuvent apparaître hors ligne.

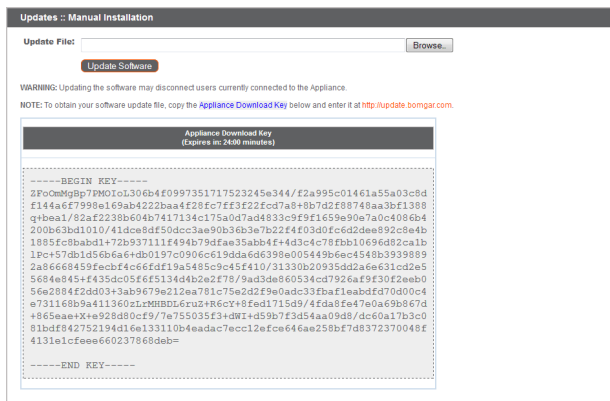


Remarque : préparez-vous à installer les mises à jour du logiciel directement après le téléchargement. Une fois qu'une mise à jour a été téléchargée, elle n'apparaît plus sur votre liste de mises à jour disponibles. Si vous avez besoin de retélécharger une mise à jour, contactez l'assistance technique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



Remarque : si une erreur se produit, vérifiez que l'heure donnée sur la page **/appliance > État > Caractéristiques** est correcte. De nombreuses fonctions du serveur d'accès à distance sécurisé, 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 d'accès à distance sécurisé 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 serveurs 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 serveurs 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'effectuer 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 serveurs 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. Si vous rencontrez des problèmes lors de la mise à jour de base, ne relancez pas le serveur d'accès à distance sécurisé. 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 > Gestion du logiciel**.

STATUS	MY ACCOUNT	CONFIGURATION	JUMP™	REP CONSOLE	USERS & SECURITY	REPORTS	PUBLIC PORTALS	LOCALIZATION	MANAGEMENT
	SOFTWARE MANAGEMENT	SECURITY	SITE CONFIGURATION	EMAIL CONFIGURATION	OUTBOUND EVENTS	CLUSTER	FAILOVER	API CONFIGURATION	SUPPORT

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

Software :: Backup Settings

Backup Password

Confirm Password

Include logged history
NOTE: Unchecking this box will exclude logged session reporting data from the backup.

[Download Backup](#)

The backup file will include all your configuration and logged data except for session recordings and some large files from the file store. The backup will only include files from the file store less than 200KB in size and no more than 50 files total.

You can optionally provide a password to protect the backup file. Then select 'Download Backup' to save a secure copy of your software configuration. You will need to provide this password when you restore from the backup file.

If the Backup Password is lost, you will not be able to restore from the backup file.

NOTE: Bomgar™ recommends backing up your site configuration each time you change the settings.
In the event of a hardware failure, a backup file will allow Bomgar™ to provide you access to temporary hosted services while retaining the settings from your most recent backup.
NOTE: If you would like to have your site automatically backed up on a recurring basis, see the following site: <http://www.bomgar.com/autobackup/>.

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**.

Falover :: Backup Site Instance Status

This is the Backup site instance for support.example.com

[Sync Now](#) The last data-sync was successfully pulled at August 10, 2012 03:46:18 PM CDT. [Refresh Status](#)

[Become Primary](#) Check this box to pull a data-sync from the site instance at (site2.example.com) while becoming the primary.

NOTE: Execute this command only when the existing primary has stopped responding or when maintenance is necessary on the primary site. After the step is successfully performed, reconfigure DNS or reassign the floating IP to point to the new primary site instance. If the current peer site instance can be contacted, it will be swapped as well.

[Break Falover Relationship](#) NOTE: This command will break the falover relationship with the existing falover peer instance. No configuration other than the relationship will be lost on either site instance. To reestablish the falover relationship, you will simply have to enter the hostname and SSL port of the peer appliance and press the Establish Relationship button.

Mise à jour du serveur A

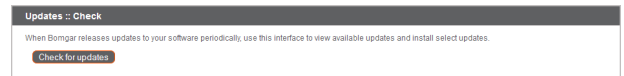
Mettez à jour le **serveur A** à l'aide de la méthode automatique ou manuelle.

Automatique

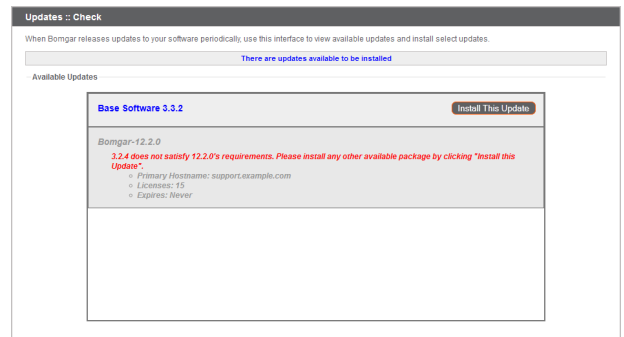
Dans la plupart des cas, les utilisateurs de BeyondTrust peuvent télécharger et installer des mises à jour sans l'aide de l'assistance technique BeyondTrust. Pour consulter les mises à jour disponibles, sélectionnez **/appliance > Mises à jour**.



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 la FAQ de dépannage relative à la recherche des mises à jour à l'adresse beyondtrustcorp.service-now.com/csm.

Mises à jour manuelles

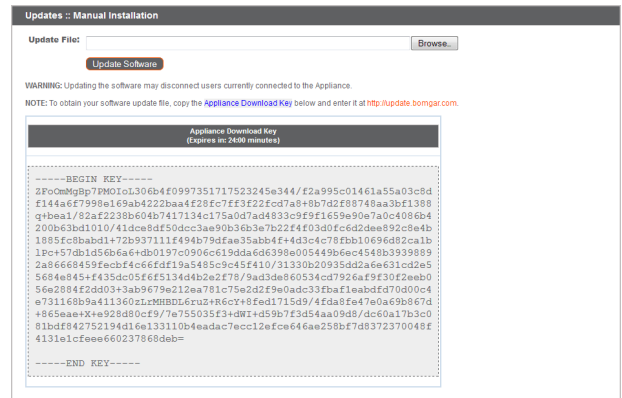
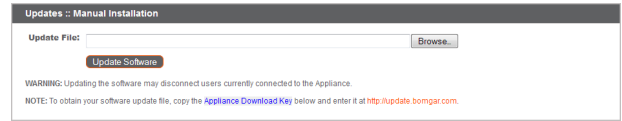
Si vous ne pouvez pas utiliser les mises à jour automatiques (par exemple, si votre serveur réside sur un réseau restreint), effectuez les mises à jour manuellement.

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



À partir de la version Base 3.3.2, cliquez sur le lien **Clé de téléchargement du serveur** pour générer une clé de serveur unique ; pour les versions antérieures, contactez l'assistance technique BeyondTrust pour demander cette clé. Envoyez ensuite cette clé au serveur de mise à jour BeyondTrust (<https://update.bomgar.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. Les consoles du technicien d'assistance installées devront être mises à niveau après la mise à niveau du site. Cela se produit en général automatiquement la prochaine fois que le technicien d'assistance lancera la console du technicien d'assistance. 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 de technicien d'assistance 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 du technicien d'assistance ou de Jump Client extractible a été activée pour votre site par l'assistance technique BeyondTrust, vous pouvez télécharger un installateur MSI afin de mettre à jour les consoles du technicien d'assistance et les Jump Clients avant de mettre à niveau le serveur. Pour ce faire, recherchez manuellement ou automatiquement les mises à jour disponibles. Cliquez sur le lien **Installeurs de console du technicien d'assistance** ou **Installeurs de Jump Client** pour télécharger l'installateur MSI à des fins de distribution. 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.

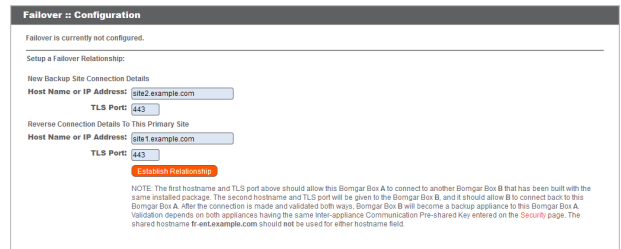
Restauration d'une relation de reprise en séquence

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** permet d'indiquer la façon dont le serveur principal doit se connecter au serveur de sauvegarde. La section **Rapporter les informations de connexion à ce site primaire** concerne le serveur de sauvegarde, et indique la façon dont il doit se connecter au serveur principal. Vous devez spécifier un nom d'hôte ou une adresse IP valide, ainsi que le numéro de port TLS. Une fois terminé, cliquez sur **Établir une relation** pour établir la relation.



Failover :: Configuration

Failover is currently not configured.

Setup a Failover Relationship:

New Backup Site Connection Details

Host Name or IP Address:

TLS Port:


Reverse Connection Details To This Primary Site

Host Name or IP Address:

TLS Port:

Establish Relationship

NOTE: The first hostname and TLS port above should allow this Bomgar Box A to connect to another Bomgar Box B that has been built with the same installed package. The second hostname and TLS port will be given to the Bomgar Box B, and it should allow B to connect back to this Bomgar Box A. After the connection is made and validated both ways, Bomgar Box B will become a backup appliance to the Bomgar Box A. Validation depends on both appliances having the same inter-appliance Communication Pre-shared Key entered on the Security page. The shared hostname B-site1.example.com should not be used for either hostname field.

 **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 l'opération terminée, la page **Reprise en séquence** indique la date et l'heure de la dernière synchronisation de données.

La synchronisation de reprise en séquence synchronise tous les comptes d'utilisateurs, tous les paramètres de configuration de **/login**, les fichiers du magasin de fichiers, les journaux et les enregistrements. Toutes ces informations qui existent sur le serveur de sauvegarde seront écrasées par celles sur le serveur primaire. Si le serveur primaire est le nœud primaire dans un cluster Atlas, le serveur de sauvegarde deviendra automatiquement le nouveau nœud maître de sauvegarde primaire de ce cluster.

Mise à niveau asynchrone de deux serveurs 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'effectuer 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. Si vous rencontrez des problèmes lors de la mise à jour de base, ne relancez pas le serveur d'accès à distance sécurisé. 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 > Gestion du logiciel**.

	STATUS	MY ACCOUNT	CONFIGURATION	JUMP™	REP CONSOLE	USERS & SECURITY	REPORTS	PUBLIC PORTALS	LOCALIZATION	MANAGEMENT
	SOFTWARE MANAGEMENT	SECURITY	SITE CONFIGURATION	EMAIL CONFIGURATION	OUTBOUND EVENTS	CLUSTER	FAILOVER	API CONFIGURATION	SUPPORT	

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

Software :: Backup Settings

Backup Password

Confirm Password

Include logged history
NOTE: Unchecking this box will exclude logged session reporting data from the backup.

[Download Backup](#)

The backup file will include all your configuration and logged data except for session recordings and some large files from the file store. The backup will only include files from the file store less than 200KB in size and no more than 50 files total.

You can optionally provide a password to protect the backup file. Then select "Download Backup" to save a secure copy of your software configuration. You will need to provide this password when you restore from the backup file.

If the Backup Password is lost, you will not be able to restore from the backup file.

NOTE: Bomgar™ recommends backing up your site configuration each time you change the settings.
In the event of a hardware failure, a backup file will allow Bomgar™ to provide you access to temporary hosted services while retaining the settings from your most recent backup.
NOTE: If you would like to have your site automatically backed up on a recurring basis, see the following site: <http://www.bomgar.com/autobackup/>.

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**.

Fallover :: Backup Site Instance Status

This is the Backup site instance for support.example.com

[Sync Now](#) The last data-sync was successfully pulled at August 10, 2012 03:45:18 PM CDT. [Refresh Status](#)

[Become Primary](#) Check this box to pull a data-sync from the site instance at (site2.example.com) while becoming the primary.

NOTE: Execute this command only when the existing primary has stopped responding or when maintenance is necessary on the primary site. After the sweep is successfully performed, reconfigure DNS or reassign the floating IP to point to the new primary site instance. If the current peer site instance can be contacted, it will be swapped as well.

[Break Fallover Relationship](#) NOTE: This command will break the fallover relationship with the existing/fallover peer instance. No configuration other than the relationship will be lost on either site instance. To reestablish the fallover relationship, you will simply have to enter the hostname and SSL port of the peer appliance and press the Establish Relationship button.

Mise à jour du serveur B

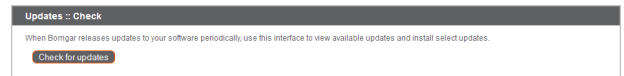
Mettez à jour le **serveur B** à l'aide de la méthode automatique ou manuelle.

Automatique

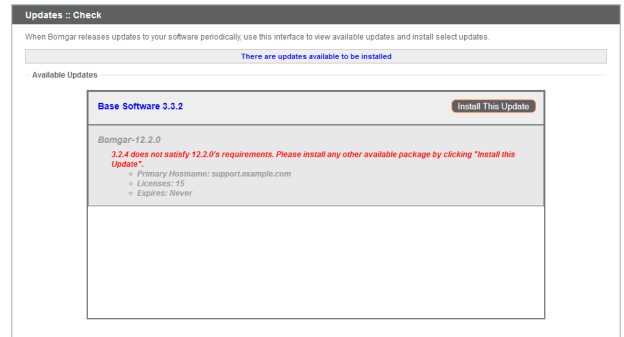
Dans la plupart des cas, les utilisateurs de BeyondTrust peuvent télécharger et installer des mises à jour sans l'aide de l'assistance technique BeyondTrust. Pour consulter les mises à jour disponibles, sélectionnez **/appliance > Mises à jour**.



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 la FAQ de dépannage relative à la recherche des mises à jour à l'adresse beyondtrustcorp.service-now.com/csm.

Mises à jour manuelles

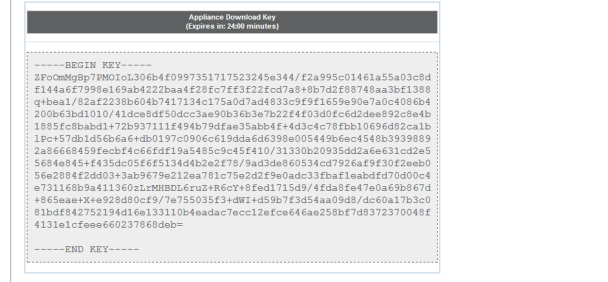
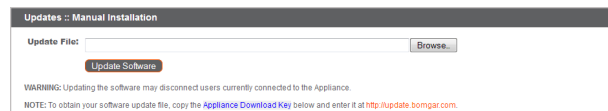
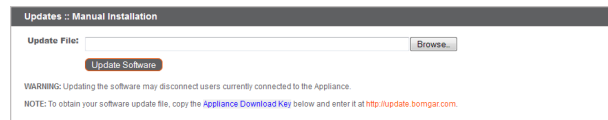
Si vous ne pouvez pas utiliser les mises à jour automatiques (par exemple, si votre serveur réside sur un réseau restreint), effectuez les mises à jour manuellement.

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



À partir de la version Base 3.3.2, cliquez sur le lien **Clé de téléchargement du serveur** pour générer une clé de serveur unique ; pour les versions antérieures, contactez l'assistance technique BeyondTrust pour demander cette clé. Envoyez ensuite cette clé au serveur de mise à jour BeyondTrust (<https://update.bomgar.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 du technicien d'assistance sur l'un des ordinateurs. Les consoles du technicien d'assistance installées devront être mises à niveau après la mise à niveau du site. Cela se produit en général automatiquement la prochaine fois que le technicien d'assistance lancera la console du technicien d'assistance. 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 du technicien d'assistance 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 du technicien d'assistance ou de Jump Client extractible a été activée pour votre site par l'assistance technique BeyondTrust, vous pouvez télécharger un installateur MSI afin de mettre à jour les consoles du technicien d'assistance et les Jump Clients avant de mettre à niveau le serveur. Pour ce faire, recherchez manuellement ou automatiquement les mises à jour disponibles. Cliquez sur le lien **Installeurs de console du technicien d'assistance** ou **Installeurs de Jump Client** pour télécharger l'installateur MSI à des fins de distribution. 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 d'assistance technique distantes effectuées 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

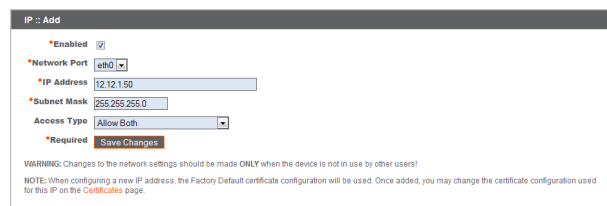
Sur le **serveur A**, sélectionnez **/appliance > Réseau > Configuration IP**.



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

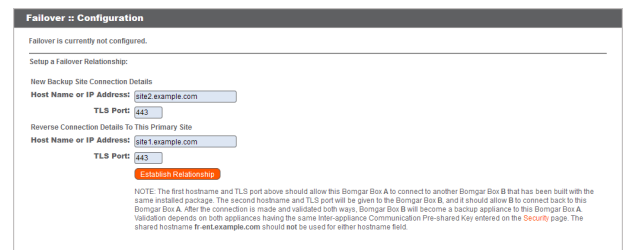
Sur le **serveur B**, sélectionnez **/login > Gestion > Reprise en séquence**.


STATUS	MY ACCOUNT	CONFIGURATION	JUMP™	REP CONSOLE	USERS & SECURITY	REPORTS	PUBLIC PORTALS	LOCALIZATION	MANAGEMENT
SOFTWARE MANAGEMENT	SECURITY	SITE CONFIGURATION	EMAIL CONFIGURATION	OUTBOUND EVENTS	CLUSTER	FAILOVER	API CONFIGURATION	SUPPORT	

 **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** permet d'indiquer la façon dont le serveur principal doit se connecter au serveur de sauvegarde. La section **Rapporter les informations de connexion à ce site primaire** concerne le serveur de sauvegarde, et indique la façon dont il doit se connecter au serveur principal. Vous devez spécifier un nom d'hôte ou une adresse IP valide, ainsi que le numéro de port TLS. 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 l'opération terminée, la page **Reprise en séquence** indique la date et l'heure de la dernière synchronisation de données.

La synchronisation de reprise en séquence synchronise tous les comptes d'utilisateurs, tous les paramètres de configuration de **/login**, les fichiers du magasin de fichiers, les journaux et les enregistrements. Toutes ces informations qui existent sur le serveur de sauvegarde seront écrasées par celles sur le serveur primaire. Si le serveur primaire est le nœud primaire dans un cluster Atlas, le serveur de sauvegarde deviendra automatiquement le nouveau nœud maître de sauvegarde primaire de ce cluster.

Mise à niveau de plusieurs serveurs d'accès à distance sécurisé dans un cluster Atlas

Mettre à niveau des clusters Atlas BeyondTrust est plus complexe que mettre à niveau des paires de reprise en séquence ou des serveurs individuels. Pour savoir comment installer et configurer Atlas, consultez le [Guide de configuration d'Atlas](http://www.beyondtrust.com/docs/remote-support/how-to/atlas) à l'adresse www.beyondtrust.com/docs/remote-support/how-to/atlas. La section suivante explique comment mettre à niveau des clusters Atlas.

Avec la reprise en séquence configurée

Ces étapes partent du principe qu'il y a deux nœuds maîtres opérant selon une configuration de reprise en séquence. Ceux-ci sont appelés **Serveur A** (le nœud maître principal de la paire de reprise en séquence) et **Serveur B** (le nœud maître de secours). Si la reprise en séquence n'est pas configurée et qu'il n'y a pas de nœud maître de secours, passez à la section « **Sans reprise en séquence configurée** », page 22.



Remarque : le processus de reprise en séquence provoque un temps d'indisponibilité. Pensez à prévoir cela.

Préparation

1. Sur le **serveur A**, sélectionnez **/appliance > Gestion > Gestion du logiciel**.
 - a. Téléchargez les mises à jour disponibles, mais ne les installez pas.
 - b. Cliquez sur **Distribuer au cluster** pour envoyer le paquet à tous les autres nœuds.



Remarque : cela n'installe pas de logiciel, mais le prépare à l'être.

2. Sur le **serveur A**, allez sur **/login > Gestion > Cluster**.
 - a. Identifiez la moitié des nœuds de trafic à désactiver temporairement par région géographique.
 - b. Sur les nœuds identifiés, décochez **Accepte les nouvelles connexions de clients**. Ces derniers sont appelés des nœuds de trafic hors ligne.
3. Sur chaque nœud de trafic hors ligne, allez sur **/login > État > Informations**.
4. En regardant le tableau des **Clients connectés**, attendez que toutes les connexions des clients d'utilisateur et des consoles du technicien d'assistance soient fermées. Cette période d'attente empêche l'interruption de sessions existantes.

Mettre à niveau la sauvegarde

1. Sur le **Serveur B**, allez sur **/appliance > Mises à jour**.
2. Cliquez sur le bouton **Installer** pour mettre à niveau le logiciel vers la dernière version en vous assurant d'installer les mises à jour dans le bon ordre.



Remarque : les mises à jour pour le logiciel de base sont en général installées avant la concession de licences pour les mises à jour logicielles. Si vous n'êtes pas sûr de l'ordre, contactez l'assistance technique de BeyondTrust avant d'installer une mise à jour. Le serveur redémarre automatiquement pendant le processus de mise à jour du logiciel de base.

Avec la mise à jour du logiciel, le serveur B définit automatiquement tous les nœuds de trafic comme n'acceptant pas les nouvelles connexions de client dans la configuration de cluster.



Remarque : n'apportez pas de changement à la configuration du **Serveur A** pendant cette mise à niveau. Ces changements seraient écrasés à la première synchronisation de données après la mise à niveau.

3. Répétez le processus de mise à niveau ci-dessus pour chaque nœud de trafic hors ligne. Une fois cela fait, le **Serveur A** et la moitié des nœuds de trafic devraient disposer de l'ancienne version de BeyondTrust. Le **Serveur B** et l'autre moitié des nœuds de trafic devraient disposer de la nouvelle version.

Mettre le nouveau primaire en production



Remarque : Ce processus de reprise en séquence provoque un temps d'indisponibilité. Pensez à prévoir cela.

1. Sur le **serveur A**, allez sur **/login > Gestion > Reprise en séquence**.
2. Cochez **Devenir une sauvegarde même si le site pair ne peut être contacté**.
3. Cliquez sur le bouton **Devenir sauvegarde**.



Remarque : ce processus pousse le serveur de sauvegarde à prendre le rôle primaire dans la paire de reprise en séquence.

4. Si nécessaire, faites passer le DNS et/ou le NAT sur le serveur B. Si le partage d'adresses IP de reprise en séquence est configuré, les paramètres du DNS ou du NAT n'auront pas besoin d'être modifiés ; le partage des adresses IP se désactive automatiquement sur le serveur A à la place.
5. Passez au **Serveur B** et allez sur **/login > Gestion > Reprise en séquence**.
6. Cliquez sur **Devenir la principale**.
7. Décochez **Activer les opérations de sauvegarde**.

Remettre les nœuds de trafic mis à niveau en ligne

1. Sur le **Serveur B**, allez sur **/login > Gestion > Cluster**.
2. Pour chaque nœud de trafic mis à niveau, cochez la case **Accepte les nouvelles connexions de clients**.
3. Dans la section **Cluster :: État**, cliquez sur **Synchroniser maintenant**.

Mettre à niveau le reste du déploiement

1. Sur chaque nœud de trafic qui n'a pas encore été mis à niveau, allez sur **/appliance > Mises à jour**.
2. Cliquez sur **Installer** pour mettre à niveau vers la nouvelle version, en faisant attention d'installer les mises à jour dans le bon ordre. Attendez la fin de l'installation des mises à jour.
3. Passez au **Serveur B** et allez sur **/login > Gestion > Cluster**.
4. Pour chaque nœud de trafic mis à niveau à l'étape précédente, cochez **Accepte les nouvelles connexions de clients**.

Mettre à niveau le serveur A

1. Sur le **Serveur A**, allez sur **/appliance > Mises à jour**.
2. Cliquez sur **Installer** pour mettre à niveau vers la nouvelle version, en faisant attention d'installer les mises à jour dans le bon ordre.

Rétablir la configuration du cluster

1. Sur le **serveur A**, allez sur **/login > Gestion > Reprise en séquence**.
2. Cochez **Activer les opérations de sauvegarde**.
3. Passez au **Serveur B** et allez sur **/login > Gestion > Cluster**.
4. Dans la section **Cluster :: État**, cliquez sur **Synchroniser maintenant**.

Sans reprise en séquence configurée

Préparation

1. Allez sur **/login > Gestion > Gestion du logiciel**.
 - a. Téléchargez les mises à jour disponibles, mais ne les installez pas.
 - b. Cliquez sur **Distribuer au cluster** pour envoyer le paquet à tous les autres nœuds.



Remarque : cela n'installe pas de logiciel, mais le prépare à l'être.

2. Allez sur **/login > Gestion > Cluster**.
 - a. Identifiez la moitié des nœuds de trafic à désactiver temporairement par région géographique.
 - b. Sur les nœuds identifiés, décochez **Accepte les nouvelles connexions de clients**. Ces derniers sont appelés des nœuds de trafic hors ligne.
3. Sur chaque nœud de trafic hors ligne, allez sur **/login > État > Informations**.
4. En regardant le tableau des **Clients connectés**, attendez que toutes les connexions des clients d'utilisateur et des consoles du technicien d'assistance soient fermées. Cette période d'attente empêche l'interruption de sessions existantes.

Mise à niveau des nœuds hors ligne

1. Sur chaque nœud de trafic hors ligne, allez sur **/appliance > Mises à jour**.
2. Cliquez sur le bouton **Installer** pour mettre à niveau le logiciel vers la dernière version en vous assurant d'installer les mises à jour dans le bon ordre.



Remarque : les mises à jour pour le logiciel de base sont en général installées avant la concession de licences pour les mises à jour logicielles. Si vous n'êtes pas sûr de l'ordre, contactez l'assistance technique de BeyondTrust avant d'installer une mise à jour. Le serveur redémarre automatiquement pendant le processus de mise à jour du logiciel de base.

Mise à niveau du nœud maître

1. Sur le nœud maître, allez sur **/appliance > Mises à jour**.
2. Cliquez sur le bouton **Installer** pour mettre à niveau le logiciel vers la dernière version en vous assurant d'installer les mises à jour dans le bon ordre. Avec la mise à jour du logiciel, le nœud maître définit automatiquement tous les nœuds de trafic comme n'acceptant pas les nouvelles connexions de client dans la configuration de cluster.

Remettre les nœuds de trafic mis à niveau en ligne

1. Sur le nœud maître, allez sur **/login > Gestion > Cluster**.
2. Pour chaque nœud de trafic mis à niveau, cochez la case **Accepte les nouvelles connexions de clients**.
3. Dans la section **Cluster :: État**, cliquez sur **Synchroniser maintenant**.

Mettre à niveau le reste du déploiement

1. Sur chaque nœud de trafic qui n'a pas encore été mis à niveau, allez sur **/appliance > Mises à jour**.
2. Cliquez sur **Installer** pour mettre à niveau vers la nouvelle version, en faisant attention d'installer les mises à jour dans le bon ordre. Attendez la fin de l'installation des mises à jour.

Rétablir la configuration du cluster

1. Passez au nœud maître et allez sur **/login > Gestion > Cluster**.
2. Pour chaque nœud de trafic mis à niveau à l'étape précédente, cochez **Accepte les nouvelles connexions de clients**.
3. Dans la section **Cluster :: État**, cliquez sur **Synchroniser maintenant**.

Mise à niveau de matériel BeyondTrust

Lorsque vous mettez à niveau votre serveur d'accès à distance sécurisé d'un serveur physique à un autre, ou entre un serveur physique et un serveur virtuel, 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 du serveur virtuel BeyondTrust : www.beyondtrust.com/docs/remote-support/getting-started/deployment/virtual
 - Installation du matériel du serveur d'accès à distance sécurisé : www.beyondtrust.com/docs/remote-support/getting-started/deployment/hardware

2. Sauvegardez les paramètres logiciels actuels de votre serveur.
 - a. Sur votre serveur actuel, sélectionnez **/login > Gestion > Gestion du 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.



Remarque : Pour tous les détails sur les certificats SSL et BeyondTrust, rendez-vous sur www.beyondtrust.com/docs/remote-support/how-to/sslcertificates.

- 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. Assignez une adresse IP au certificat.
 - a. Sur votre nouveau serveur, sélectionnez **/appliance > Sécurité > Certificats**.
 - b. Dans la section **Sécurité :: Certificats**, trouvez l'entrée pour votre certificat SSL. Elle comporte en général un champ **Transmis à** contenant le nom de domaine complet de votre serveur (par exemple : support.example.com).
 - c. Confirmez qu'il n'existe pas d'avertissement répertorié pour le nouveau certificat. Si vous voyez un avertissement, reportez-vous à la FAQ 755 du Centre d'assistance technique en libre-service BeyondTrust pour savoir comment résoudre l'avertissement : beyondtrustcorp.service-now.com/csm/ssc/SolutionFAQ.aspx?id=755.
 - d. Une fois tous les avertissements résolus, cliquez sur le lien **Assigner IP** dans la ligne du certificat. En bas de la page, vérifiez les adresses IP à assigner, puis cliquez sur le bouton **Enregistrer configuration**.

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 > Gestion du 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'assistance technique à distance 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 de 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. BEYONDTRUST, son logo, et JUMP sont des marques déposées de BeyondTrust Corporation. Les autres marques déposées sont la propriété de leurs détenteurs respectifs.

Limitations associées à la licence

Une licence d'assistance technique à distance BeyondTrust permet à un technicien d'assistance à la fois d'intervenir sur un nombre illimité d'ordinateurs distants, avec et sans surveillance. 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.

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, veuillez contacter l'assistance technique de BeyondTrust : [beyondtrust.com/docs/index.htm#support](https://www.beyondtrust.com/docs/index.htm#support).

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