BeyondTrust

Privileged Remote Access
Mise en place du serveur virtuel

TC:9/25/2020

Table des matières

Installation du serveur virtuel Privileged Remote Access

Ce guide est conçu pour vous conseiller lors de l'installation et de la configuration initiales de votre PRA Virtual Appliance BeyondTrust. Si vous avez besoin d'aide, contactez l'Assistance technique BeyondTrust à l'adresse www.beyondtrust.com/support.

Conditions pour les déploiements VMWare et Hyper-V

Avant de commencer l'installation de votre PRA Virtual Appliance BeyondTrust, consultez bien les conditions et les directives de taille qui suivent.

- VMware vCenter 5.1+ et versions matériel virtuel 9+
- Hyper-V 2012 R2 (autonome ou en tant que rôle) et matériel de première génération uniquement
- Au moins 124 Go de stockage disponible.

> Pour déterminer exactement la quantité de stockage disponible dont vous avez besoin pour votre environnement, consultez « Directives relatives à la taille du serveur virtuel Privileged Remote Access », page 4.

- Une partition de 32 Go pour le système d'exploitation BeyondTrust, et au moins 100 Go disponibles pour les journaux et les enregistrements.
- Les SAN à IP externe doivent être sur un réseau réservé 1 Gbit ou 10 Gbit avec des disques à 10 000 RPM ou plus.
- Une IP statique pour votre PRA Virtual Appliance
- Un enregistrement de DNS privé de type A effectuant une résolution vers l'IP statique de votre PRA Virtual Appliance. Un enregistrement d'adresse public et une IP publique seront également requis si les clients publics ont besoin d'un accès au serveur. L'enregistrement de DNS de type A est le nom de domaine complet (FDQN) de votre site (par ex. access.example.com).

  > ***Remarque :*** *Les « clients publics » incluent tous les logiciels clients (navigateurs, console d'accès BeyondTrust, client de point de terminaison, etc.) qui se connectent à partir d'adresses IP externes en dehors du ou des réseaux et VPN dans le réseau du Secure Remote Access Appliance.*

- Un serveur NTP valide qui est joignable par le serveur
- Vérifiez que l'heure du système entre le serveur ESXi hôte et le système d'exploitation de BeyondTrust sont synchronisés. Des variations de quelques secondes seulement peuvent potentiellement causer des problèmes de performance ou de connectivité.

Conditions pour Microsoft Azure

- Microsoft Azure Resource Manager (ARM)
- Si vous utilisez Microsoft Azure, vérifiez que les éléments suivants sont déjà en place avant le déploiement :
  - Un groupe de ressources
  - Un compte de stockage avec conteneur vhds
  - Un VNET et sous-réseau a été configuré

Directives relatives à la taille du serveur virtuel Privileged Remote Access

Les directives de taille pour la MV invitée suivantes doivent être utilisées pour apporter une assistance technique au PRA Virtual Appliance BeyondTrust.

Pour un maximum de 20 utilisateurs simultanés avec 1 000 Jump Clients et une session simultanée par utilisateur (petit), les besoins du VMware sont :

- 2 processeurs virtuels ; 2,5 GHz ou plus
- 4 Go de mémoire
- 24 Go de stockage disponible pour le système d'exploitation
- 100 Go de stockage disponible pour les journaux et les enregistrements

Pour un maximum de 300 utilisateurs simultanés avec 10 000 Jump Clients et une session simultanée par utilisateur (moyen), les besoins du VMware sont :

- 4 processeurs virtuels ; 2,5 GHz ou plus
- 8 Go de mémoire
- 24 Go de stockage disponible pour le système d'exploitation
- 500 Go sur disque dur secondaire pour les journaux et les enregistrements

Pour un maximum de 1 000 utilisateurs simultanés avec 25 000 Jump Clients et une session simultanée par utilisateur (grand), les besoins du VMware sont :

- 8 processeurs virtuels ; 2,5 GHz ou plus
- 16 Go de mémoire
- 24 Go de stockage disponible pour le système d'exploitation
- Disque secondaire de 100 Go résidant sur un magasin de données haute performance
- Disque tertiaire de 1 000 Go pour les journaux et les enregistrements

Remarque : *Si vous prévoyez plus de 1 000 utilisateurs simultanés, veuillez contacter l'Assistance technique BeyondTrust à l'adresse www.beyondtrust.com/support pour vous assurer que les ressources allouées répondront à vos besoins.*

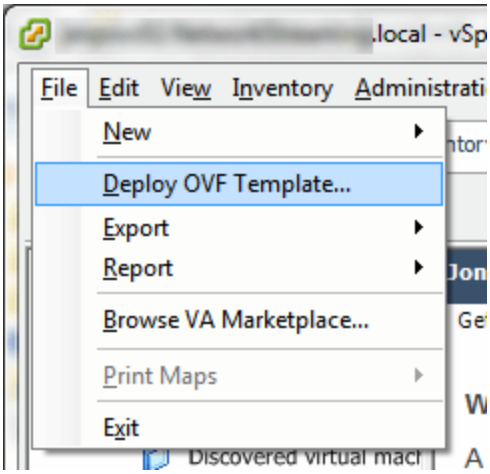
Remarque : *comme la quantité de données enregistrées varie grandement en fonction du type de données collectées, la durée de session, etc., il est impossible de définir quelle quantité d'espace de stockage est requise pour enregistrer les données pour un nombre de jours donnés. Si votre entreprise doit se conformer à des règles de rétention de données, BeyondTrust vous recommande d'estimer la quantité de stockage nécessaire en vous basant sur l'observation de vos propres banques de données, ou d'utiliser l'API BeyondTrust ou le client d'intégration pour extraire les données de session vers une banque externe.*

Remarque : *À des fins de résolution des problèmes, l'Assistance technique BeyondTrust peut demander à ce que des ressources réservées correspondant aux spécifications de ce document soient allouées à votre PRA Virtual Appliance BeyondTrust. En gardant cela à l'esprit, vous pouvez vous écarter de ces spécifications comme bon vous semble.*

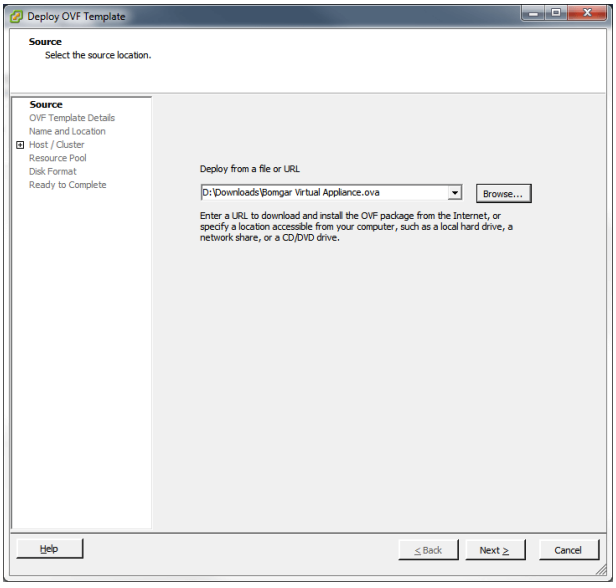
Déployer le Secure Remote Access Appliance BeyondTrust dans un environnement VMware

1. Ouvrez l'e-mail que vous avez reçu de l'Assistance technique BeyondTrust et cliquez sur le lien pour télécharger le fichier **BeyondTrust PRA Virtual Appliance.ova**

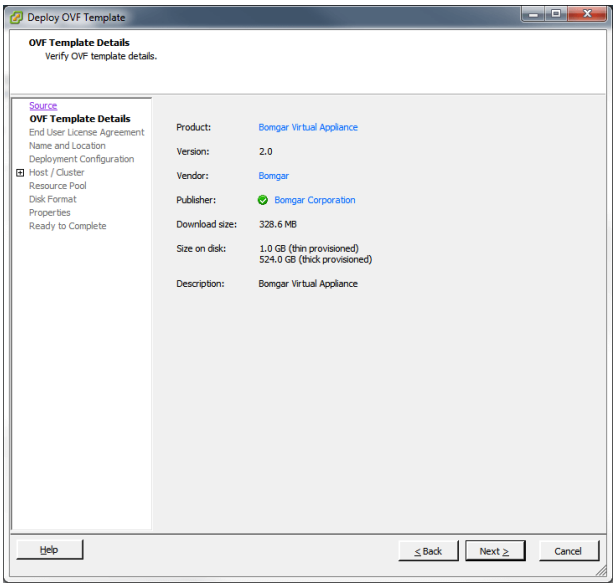
2. Connectez-vous à votre client d'infrastructure virtuelle. Vous devez utiliser un compte disposant d'autorisations pour déployer une machine virtuelle comme modèle OVF. Suivez le processus pour déployer un modèle OVF.



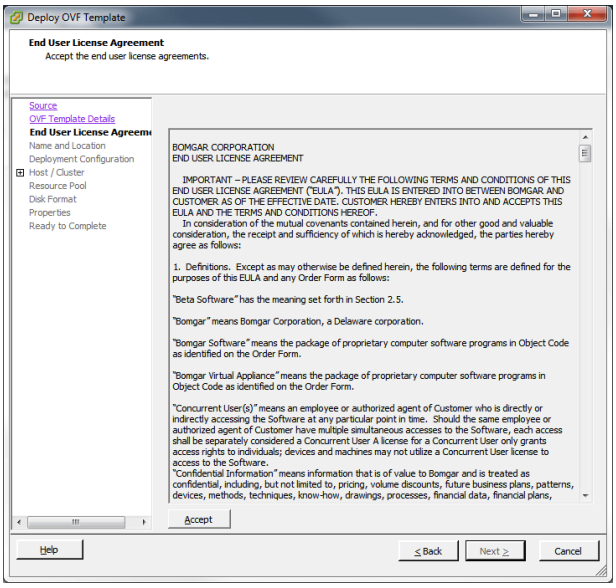
3. Dans la section **Source** de l'assistant de déploiement, sélectionnez le fichier **BeyondTrust Virtual Appliance.ova**.



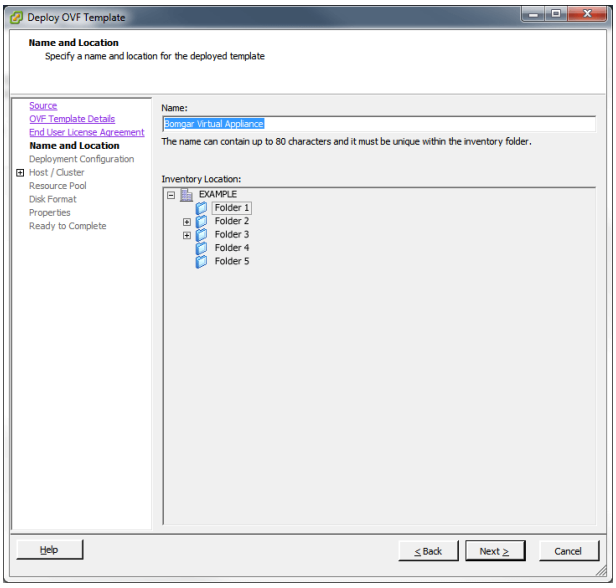
4. Consultez les détails du modèle OVF.



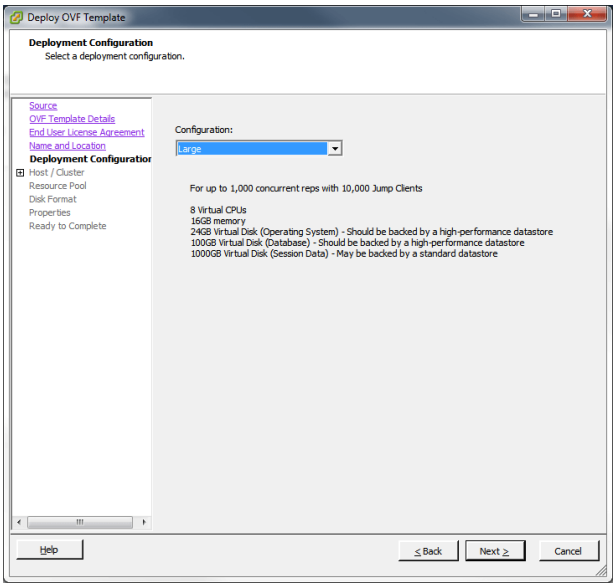
5. Lisez et acceptez le contrat de licence utilisateur final.



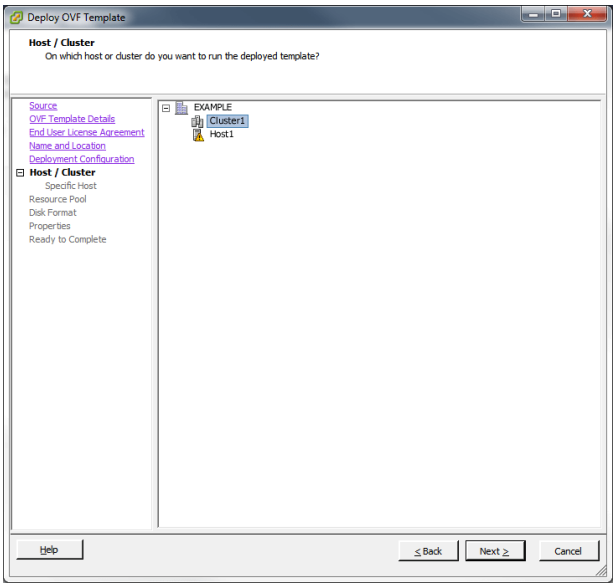
6. Indiquez un nom pour ce modèle OVF et sélectionnez un emplacement dans l'inventaire pour lequel vous disposez des droits.



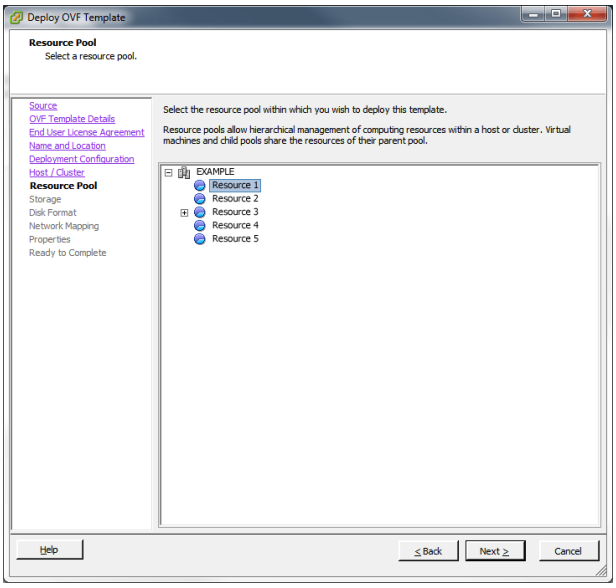
7. Sélectionnez une configuration entre **Petit**, **Moyen** ou **Grand**. Cette sélection définit vos allocations de ressources par défaut. Choisissez votre configuration en fonction de vos besoins d'utilisation et des ressources disponibles.



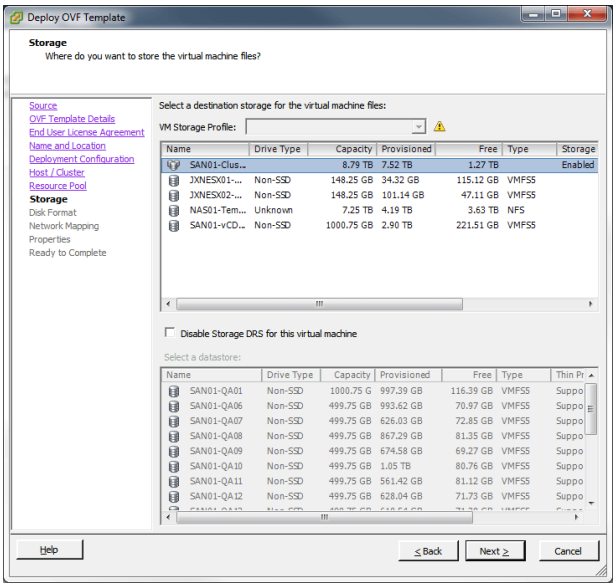
8. Choisissez l'hôte ou le cluster sur lequel vous souhaitez exécuter le PRA Virtual Appliance BeyondTrust. Sélectionnez un emplacement pour lequel vous disposez de droits.



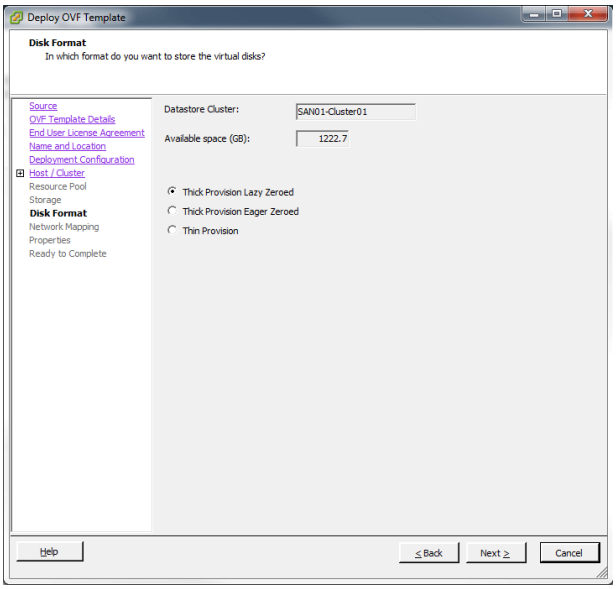
9. Sélectionnez un pool de ressources pour lequel vous disposez de droits.



10. Sélectionnez la banque de données sur laquelle vous souhaitez que le PRA Virtual Appliance s'exécute. C'est là que le système d'exploitation et les données de session sont stockés.

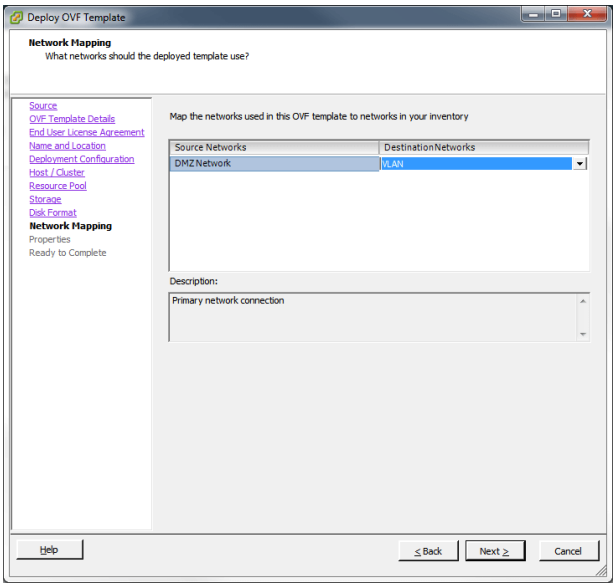


11. Choisissez comment les données seront provisionnées. Si vous n'êtes pas sûr de la sélection à effectuer, choisissez **Provisionnement standard avec zéro basique**.



> Pour plus d'informations sur les emplacements réseau, consultez Le Secure Remote Access Appliance dans le réseau à l'adresse www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/dmz.

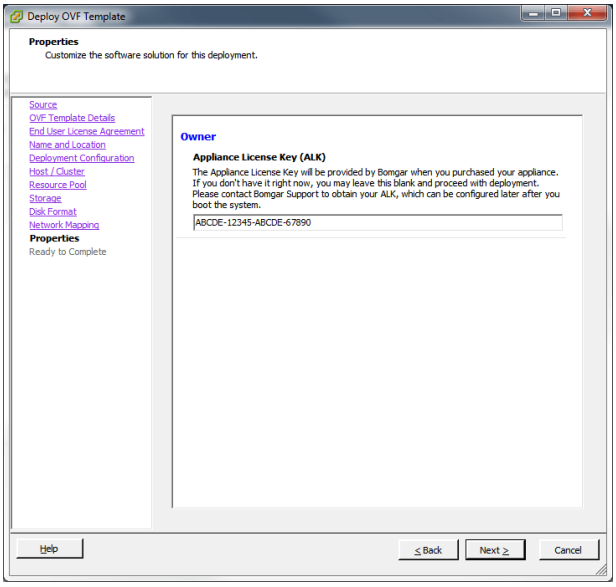
12. Sélectionnez la cartographie de réseau appropriée pour votre environnement. Votre PRA Virtual Appliance peut fonctionner n'importer où sur votre réseau avec un accès Internet. Cependant, si vous comptez accéder à des systèmes hors de votre réseau, BeyondTrust recommande pour une sécurité optimale que vous placiez le PRA Virtual Appliance dans une DMZ ou à l'extérieur de votre pare-feu interne. Les considérations sur l'emplacement réseau sont exposées dans le tableau ci-dessous.



Considérations pour l'emplacement réseau d'un Secure Remote Access Appliance

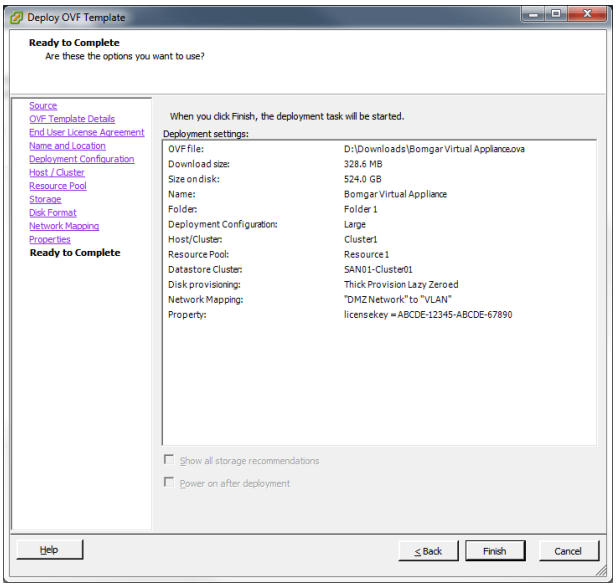
Emplacement réseau	Avantages/Inconvénients
Hors de votre pare-feu	Ne requiert pas que les ports 80 et 443 soient ouverts pour le trafic TCP entrant sur votre pare-feu. Simplifie grandement le processus d'installation, car les clients du technicien d'assistance et des clients sont construits pour renvoyer vers un DNS spécifique ; si votre DNS enregistré renvoie vers une adresse IP publique directement assignée à votre serveur, aucune installation additionnelle n'est nécessaire de votre part pour lancer une session.
DMZ	Peut nécessiter une configuration supplémentaire en fonction de votre (vos) routeur(s).
À l'intérieur de votre pare-feu	Nécessite une redirection de ports sur votre pare-feu et potentiellement une configuration supplémentaire de votre routage NAT et de votre DNS interne.

13. Reprenez l'e-mail que l'Assistance technique BeyondTrust vous a envoyé et copiez la clé de licence du serveur. Copiez la clé dans le champ dans l'assistant de déploiement.



Remarque : *si vous ne pouvez pas fournir de clé de licence du serveur à ce moment, vous pouvez la saisir manuellement plus tard, depuis la console de machine virtuelle. Il est recommandé que vous saisissiez la clé maintenant pour plus de simplicité.*

14. Vérifiez vos paramètres et cliquez sur **Terminé**.
15. Le PRA Virtual Appliance se déploiera à l'emplacement et avec les ressources que vous avez spécifiés.

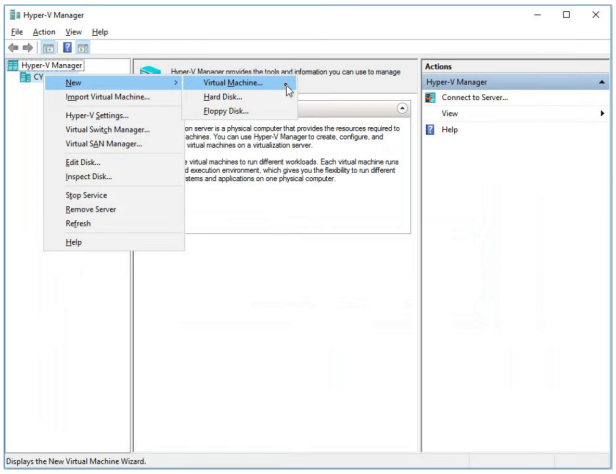


Déployer le Secure Remote Access Appliance BeyondTrust dans un environnement Hyper-V

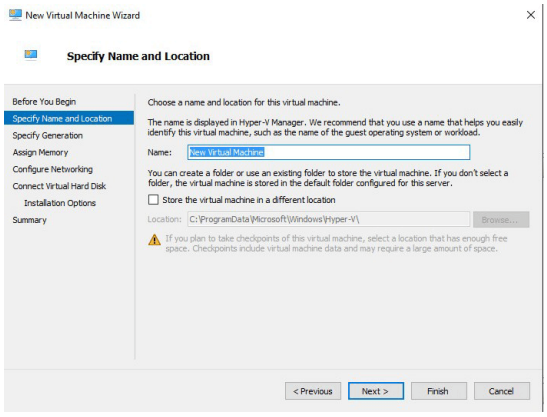
Configurer Hyper-V

1. Ouvrez l'e-mail que vous avez reçu de l'Assistance technique BeyondTrust et cliquez sur le lien pour télécharger le fichier **BeyondTrust PRA Virtual Appliance for Hyper-V .exe**. Enregistrez le fichier à un emplacement approprié pour qu'il puisse être importé sur votre hôte Hyper-V, puis faites un double-clic sur le fichier zip pour extraire votre PRA Virtual Appliance.

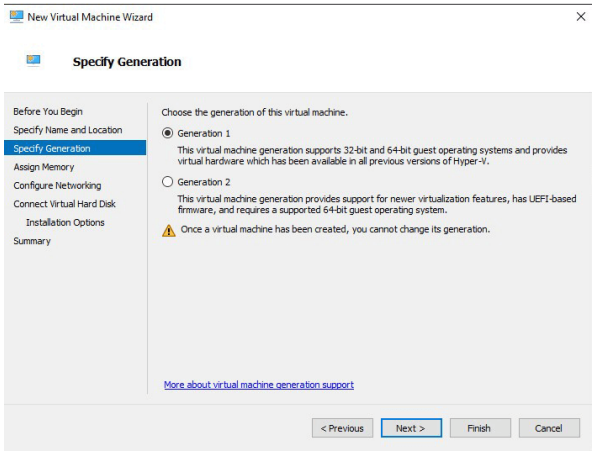
2. Lancez le gestionnaire Hyper-V.
3. Après vous être assuré que le serveur sur lequel vous souhaitez installer la PRA Virtual Appliance est présent, faites un clic droit dessus puis sélectionnez **Nouvelle** pour lancer l'**assistant de nouvelle machine virtuelle**.



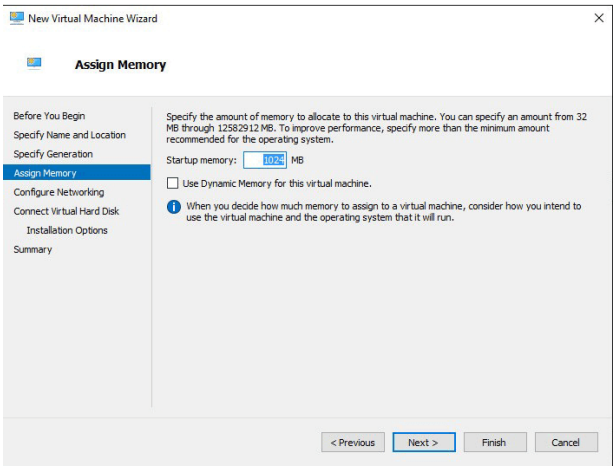
4. Saisissez un nom et choisissez un emplacement pour le PRA Virtual Appliance BeyondTrust. Cliquez ensuite sur **Suivant**.



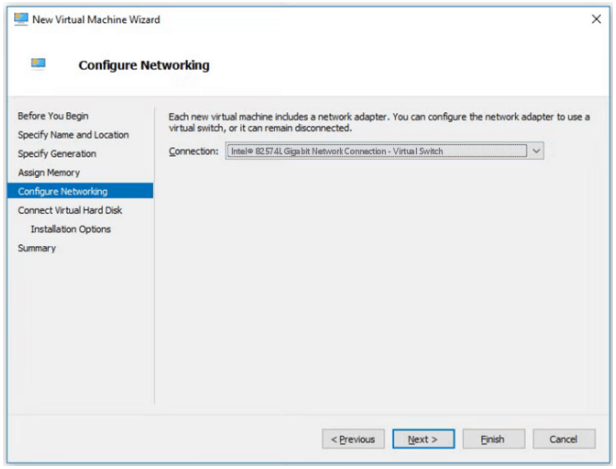
5. Sélectionnez **Génération 1** et cliquez sur **Suivant**.



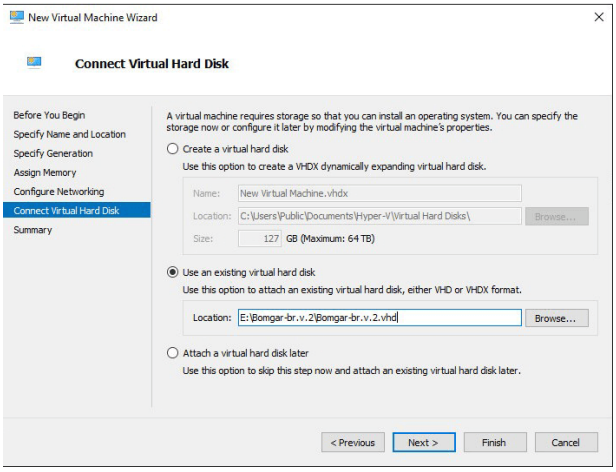
6. Saisissez **4096 Mo** pour un petit déploiement, ou **8192 Mo** pour toute autre taille. N'utilisez pas de mémoire dynamique. Cliquez sur **Suivant**.



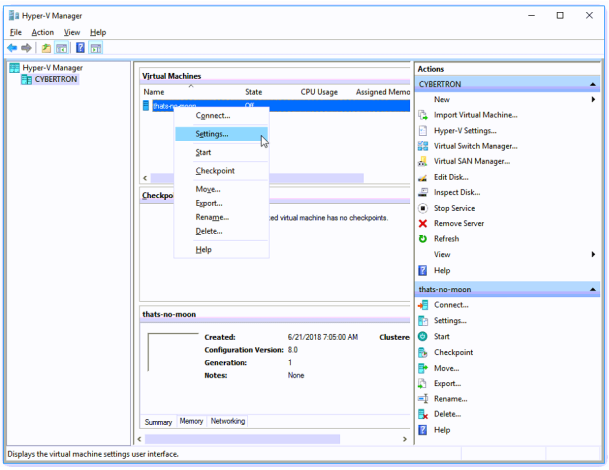
7. Depuis le menu déroulant **Connexion**, sélectionnez l'option d'interface réseau la plus adaptée à vos besoins, puis cliquez sur **Suivant**.



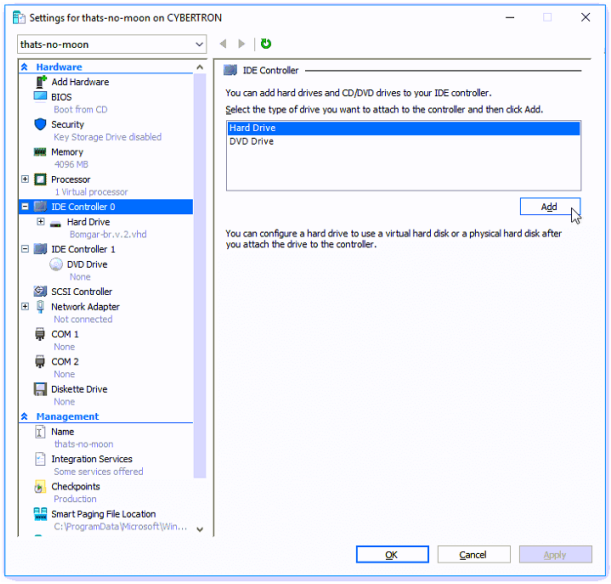
8. Sélectionnez **Utiliser un disque dur virtuel existant** puis sélectionnez le fichier **Bomgar-br.v.2.vhd** extrait plus tôt de l'archive téléchargée. BeyondTrust Corporation vous recommande de mettre le fichier DDV dans le même emplacement que la MV. Cliquez sur **Suivant**.



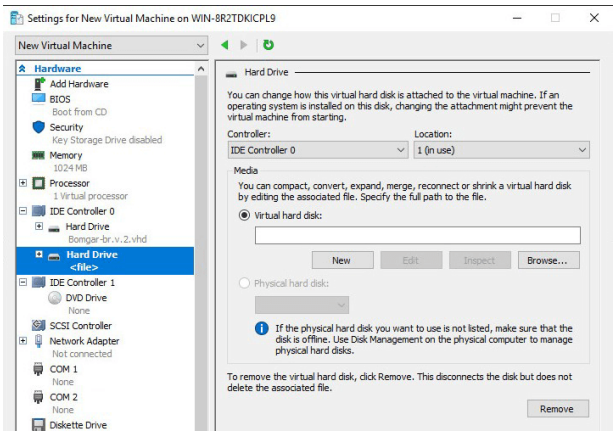
9. Vérifiez les détails de la MV sur la page **Résumé** puis cliquez sur **Terminer**.
10. Une fois la MV créée, faites un clic droit dessus puis sélectionnez **Paramètres**.



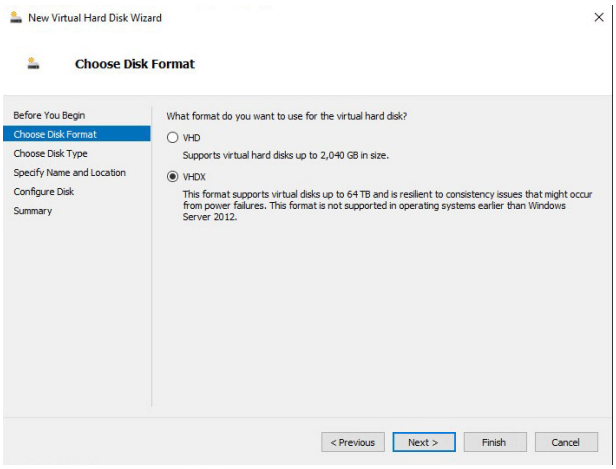
11. Cliquez sur **Contrôleur IDE 0** et sélectionnez **Disque dur**. Cliquez ensuite sur **Ajouter**.



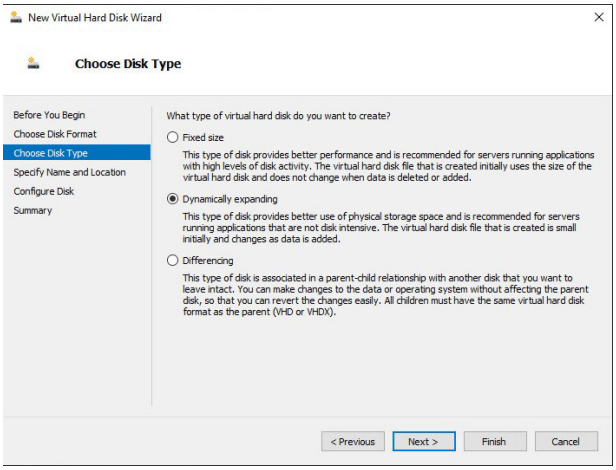
12. Cliquez sur le bouton **Nouveau** pour créer un nouveau disque dur virtuel. L'**assistant de création de nouveau disque dur virtuel** se lancera.



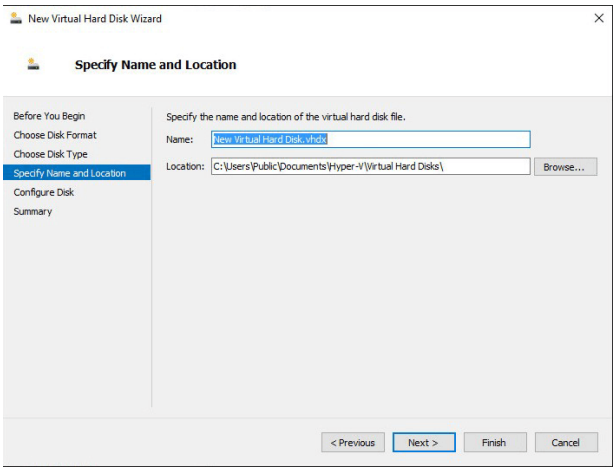
13. Sur la page **Choix du format du disque** sélectionnez **VHDX** puis cliquez sur **Suivant**.



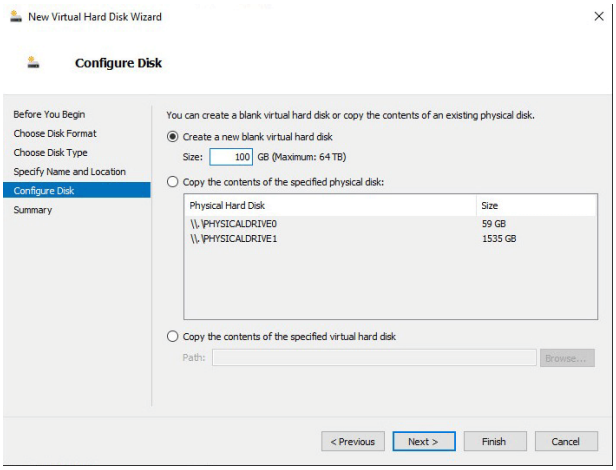
14. Choisissez le type de disque souhaité sur la page **Choix du type de disque** puis cliquez sur **Suivant**.



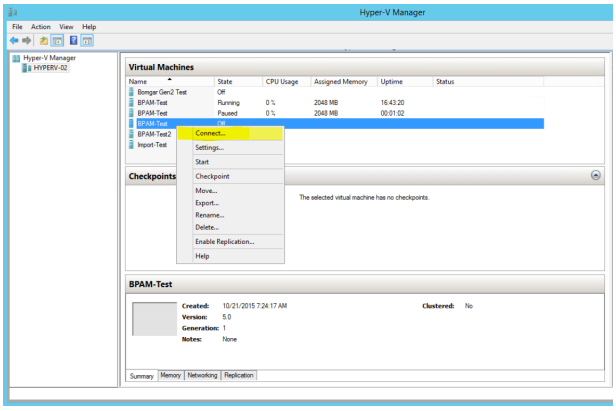
15. Sur la page **Spécification du nom et de l'emplacement**, fournissez un nom et un emplacement pour le fichier du disque dur virtuel. Cliquez sur **Suivant**.



16. Sélectionnez **Créer un nouveau disque dur virtuel vide** et définissez une taille de **100 Go**. Cliquez sur **Suivant**.

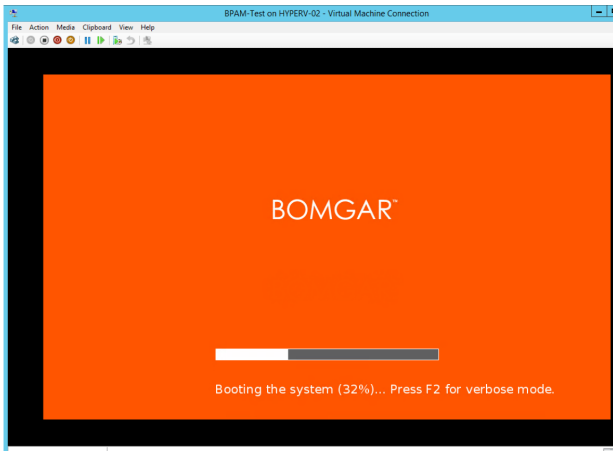


17. Vérifiez les options du disque dur sur la page **Résumé** puis cliquez sur **Terminer**.
18. Si vos exigences de taille concernent des machines virtuelles de taille moyenne ou supérieure, suivez les étapes ci-dessus pour créer un disque supplémentaire, puis définissez une taille de **500 Go**.
19. Enfin, faites un clic droit sur la machine virtuelle et sélectionnez

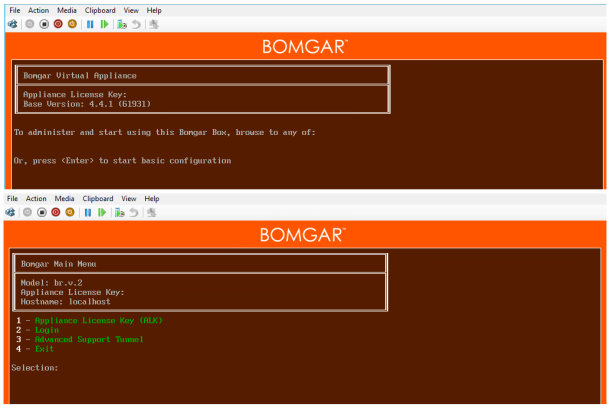


Configurer le PRA Virtual Appliance

1. Cliquez sur le bouton **Démarrer** pour lancer la machine virtuelle Hyper-V.

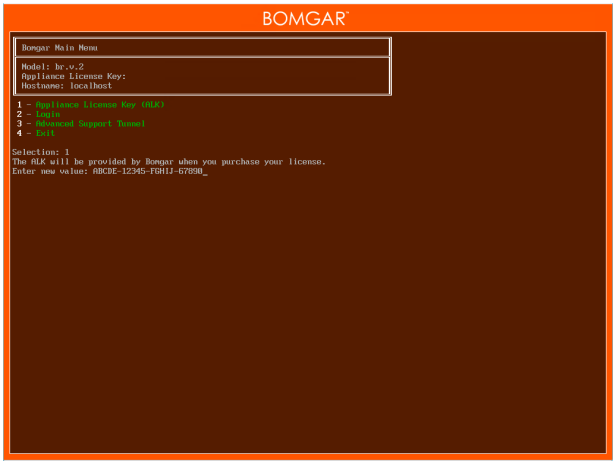


2. Sur l'écran de la configuration initiale de la console, appuyez sur **Entrée** puis sur **1** pour saisir la clé de licence du serveur.



3. Revenez à l'e-mail envoyé par l'assistance technique BeyondTrust, notez la clé de licence du serveur, saisissez-la ici et appuyez sur **Entrée**.

> ***Remarque :*** *si vous ne pouvez pas fournir de clé de licence du serveur à ce moment, vous pouvez la saisir manuellement plus tard, depuis la console de machine virtuelle. Il est recommandé que vous saisissiez la clé maintenant pour plus de simplicité.*



Considérations pour l'emplacement réseau d'un Secure Remote Access Appliance

Emplacement réseau	Avantages/Inconvénients
Hors de votre pare-feu	Ne requiert pas que les ports 80 et 443 soient ouverts pour le trafic TCP entrant sur votre pare-feu. Simplifie grandement le processus d'installation, car les clients du technicien d'assistance et des clients sont construits pour renvoyer vers un DNS spécifique ; si votre DNS enregistré renvoie vers une adresse IP publique directement assignée à votre serveur, aucune installation additionnelle n'est nécessaire de votre part pour lancer une session.
DMZ	Peut nécessiter une configuration supplémentaire en fonction de votre (vos) routeur(s).
À l'intérieur de votre pare-feu	Nécessite une redirection de ports sur votre pare-feu et potentiellement une configuration supplémentaire de votre routage NAT et de votre DNS interne.

Déployer le Secure Remote Access Appliance BeyondTrust dans un environnement Microsoft Azure

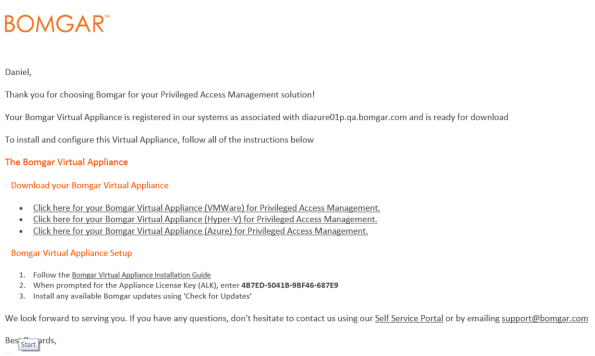
Les administrateurs qui souhaitent déployer le PRA Virtual Appliance BeyondTrust dans leur environnement Microsoft Azure doivent suivre les étapes suivantes.

IMPORTANT !

Remarque : *Vous devez disposer d'un compte Microsoft Azure et d'un environnement déjà configuré. Vous devez de plus installer le module Azure PowerShell sur votre machine, qui nécessitera peut-être une mise à niveau PowerShell. Pour plus d'informations sur l'installation et la configuration du module Azure PowerShell, veuillez consulter Installer et configurer Azure PowerShell à l'adresse https://docs.microsoft.com/en-us/powershell/azure/install-Az-ps?view=azps-1.8.0.*

Remarque : *BeyondTrust ne prend actuellement pas en charge l'utilisation de disques gérés par le script de déploiement pour Remote Support (RS) ou Privileged Remote Access (PRA) sur Azure.*

1. Ouvrez l'e-mail que vous avez reçu de l'Assistance technique BeyondTrust et sélectionnez le lien **Cliquez ici pour votre PRA Virtual Appliance BeyondTrust (Azure) pour Privileged Remote Access** afin de télécharger le fichier **BeyondTrustPAM_azure.exe**.


BOMGAR

Daniel,

Thank you for choosing Bomgar for your Privileged Access Management solution!

Your Bomgar Virtual Appliance is registered in our systems as associated with diazure01p.qa.bomgar.com and is ready for download

To install and configure this Virtual Appliance, follow all of the instructions below

The Bomgar Virtual Appliance

Download your Bomgar Virtual Appliance

- Click here for your Bomgar Virtual Appliance (VMWare) for Privileged Access Management.
- Click here for your Bomgar Virtual Appliance (Hyper-V) for Privileged Access Management.
- Click here for your Bomgar Virtual Appliance (Azure) for Privileged Access Management.

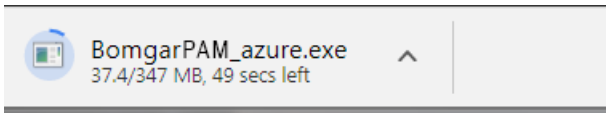
Bomgar Virtual Appliance Setup

1. Follow the Bomgar Virtual Appliance Installation Guide
2. When prompted for the Appliance License Key (ALK), enter **4B7ED-50418-9BF46-687E9**
3. Install any available Bomgar updates using 'Check for Updates'

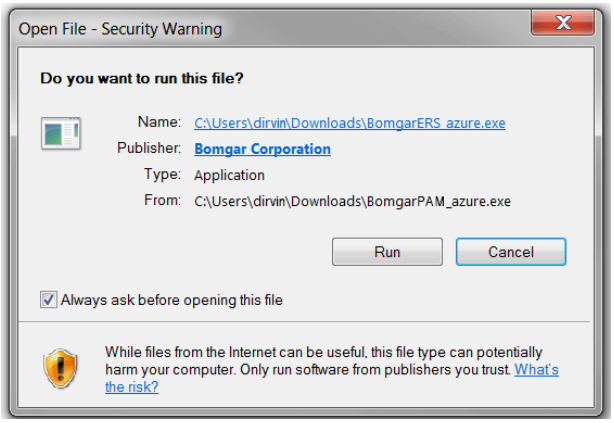
We look forward to serving you. If you have any questions, don't hesitate to contact us using our Self Service Portal or by emailing support@bomgar.com

Best regards,

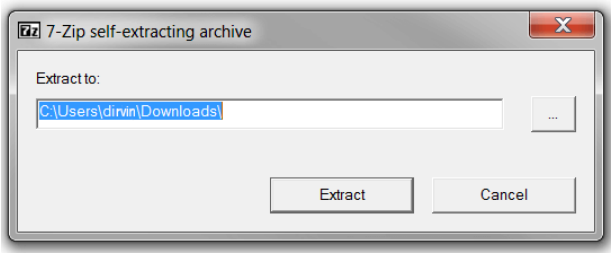
2. Cliquez sur le fichier **BeyondTrustPAM_azure.exe** dans votre navigateur pour lancer l'installation.



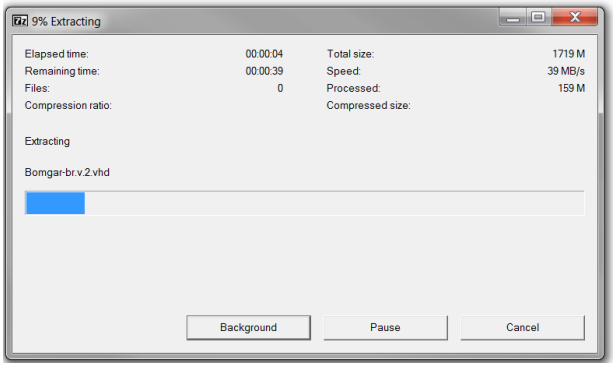
3. Si vous recevez un **Avertissement de sécurité**, cliquez sur **Exécuter**.



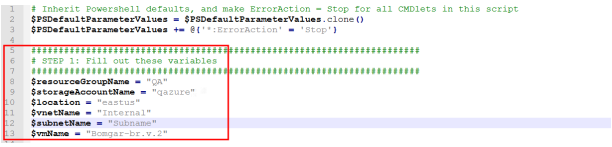
4. Choisissez où vous voulez extraire les fichiers. Cliquez sur **Extraire**.



5. Attendez que les fichiers soient extraits. Vous pouvez consulter le **Temps écoulé**, le **Temps restant** et la barre de progression bleue pour voir où en est l'extraction.



6. Une fois l'extraction terminée, les fichiers **BeyondTrustPAM_azure.exe**, **Deploy_AzureBeyondTrustVM.ps1** et **Bomgar-br.v.2.vhd** se trouveront à l'emplacement désigné pendant le processus d'extraction. Faites un clic droit sur le script PowerShell **Deploy_AzureBeyondTrustVM.ps1** et cliquez sur **Modifier**.
7. Une fois le script PowerShell ouvert, trouvez **ÉTAPE 1** et modifiez les variables suivantes en fonction de votre environnement Microsoft Azure :



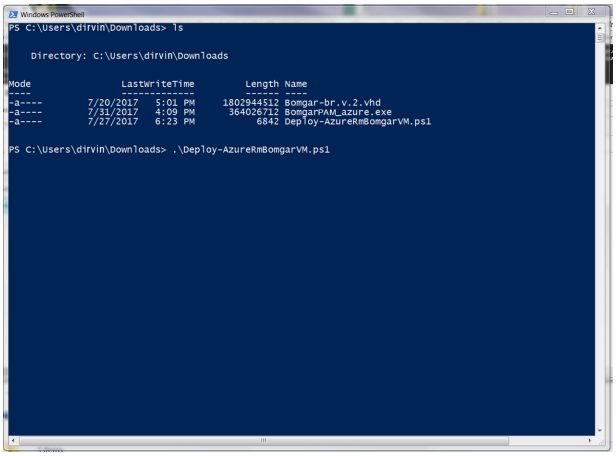
- **Nom de groupe de ressources**
- **Nom de compte de stockage**
- **Emplacement** (par exemple : westus)
- **Nom vnet**
- **Nom de sous-réseau**

> ***Remarque :*** *il n'est pas nécessaire de changer le* ***vmName****.*

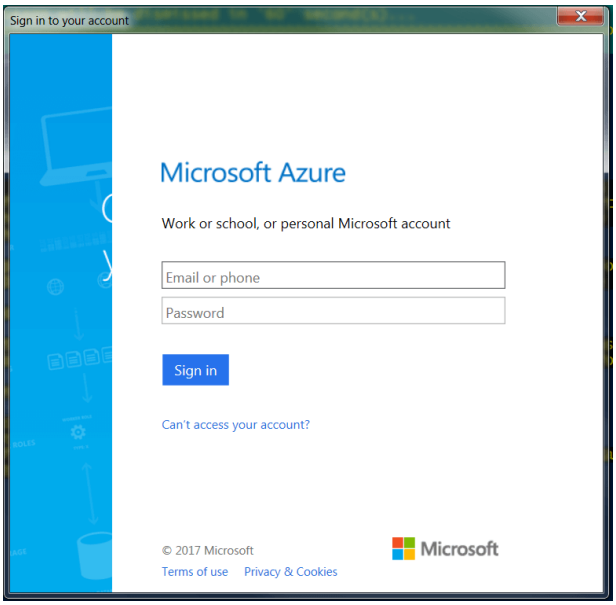
> ***Remarque :*** *Le compte de stockage utilisé pour le serveur virtuel Azure doit être d'usage général v1.*

8. Trouvez **ÉTAPE 2**. Dans le script Powershell fourni, enlevez le signe de commentaire de la taille de déploiement désirée sur votre serveur. Les options sont :
   - **Petit**
   - **Moyenne**
   - **Grand**

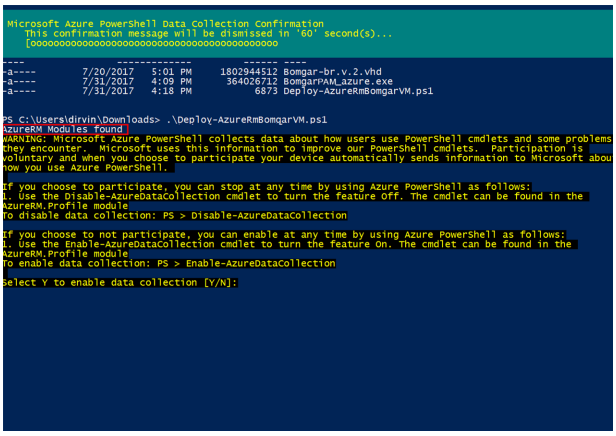
9. Enregistrez et exécutez le script dans **Windows PowerShell**.



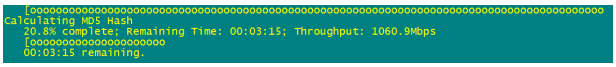
10. Saisissez vos informations d'authentification lorsqu'elles vous sont demandées et connectez-vous à votre compte **Microsoft Azure**.

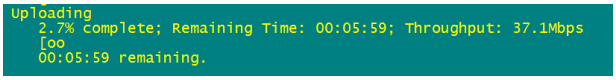


11. Dans **Windows PowerShell**, vous devriez recevoir un message indiquant les **modules AzureRM trouvés**. Vous pouvez à ce moment choisir d'aide Microsoft Azure dans la collecte de données.

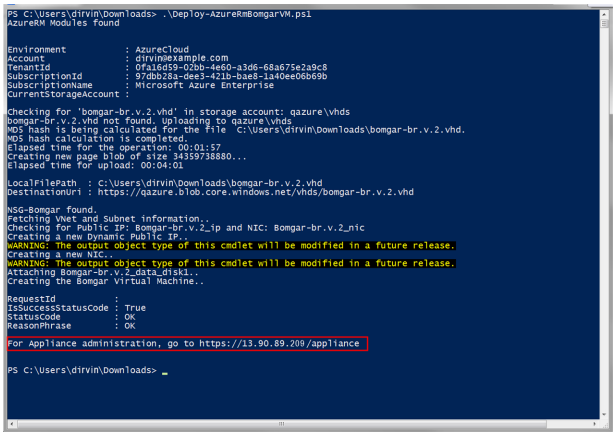


12. Le système configure ensuite un hachage MD5, envoie le serveur dans votre environnement Azure et configure une adresse IP publique pour votre PRA Virtual Appliance BeyondTrust.

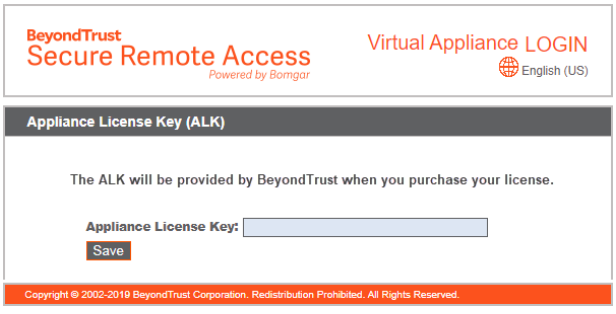




13. Il vous est ensuite demandé d'aller sur l'adresse IP configurée pour votre serveur. Le message est le suivant : **Pour administrer le serveur, allez à l'adresse https://xx.xx.xx.xxx/appliance**.



14. Sur la page /appliance, saisissez votre **clé de licence du serveur** fournie dans l'e-mail envoyé par l'Assistance technique BeyondTrust. Cliquez sur **Enregistrer**.
15. Pour configurer une URL persistante pour votre serveur, vous avez deux options :
    - Dans la console Azure, réglez l'IP externe du serveur sur « Statique ». Assignez ensuite votre entrée DNS à cette IP externe.
    - Vous pouvez aussi appliquer un nom de DNS dans Azure. Définissez un enregistrement CNAME pointant vers cette adresse.



Remarque : *aucune autre configuration du réseau ou de la console n'est nécessaire pour les serveurs basés sur Azure. Veuillez continuer pour Enregistrer et mettre à jour le serveur virtuel Privileged Remote Access*

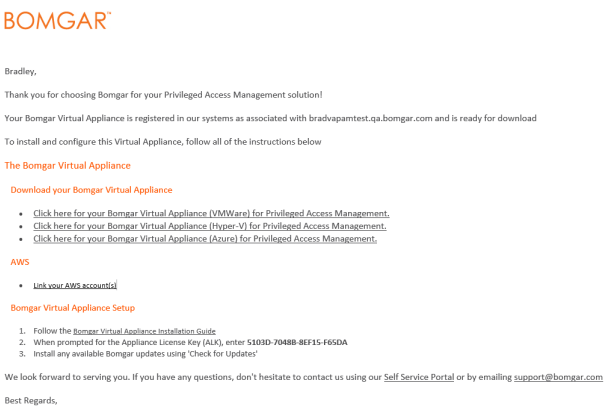
Déployer le Secure Remote Access Appliance BeyondTrust dans un environnement Amazon AWS

Les administrateurs qui souhaitent déployer le PRA Virtual Appliance Privileged Remote Access BeyondTrust dans leur environnement Amazon Web Services (AWS) doivent suivre les étapes suivantes.

IMPORTANT !

Vous devez posséder un compte Amazon AWS ainsi qu'un plan d'assistance déjà configuré. Vous êtes également responsable de l'enregistrement du nom d'hôte DNS de votre site.

1. Ouvrez l'e-mail que vous avez reçu de l'Assistance technique BeyondTrust et sélectionnez le lien **Connectez vos comptes AWS** pour être redirigé vers le site de BeyondTrust.


BOMGAR

Bradley,

Thank you for choosing Bomgar for your Privileged Access Management solution!

Your Bomgar Virtual Appliance is registered in our systems as associated with bradvapamtest.qa.bomgar.com and is ready for download

To install and configure this Virtual Appliance, follow all of the instructions below

The Bomgar Virtual Appliance

Download your Bomgar Virtual Appliance

- Click here for your Bomgar Virtual Appliance (VMWare) for Privileged Access Management.
- Click here for your Bomgar Virtual Appliance (Hyper-V) for Privileged Access Management.
- Click here for your Bomgar Virtual Appliance (Azure) for Privileged Access Management.

AWS

- Link your AWS account(s)

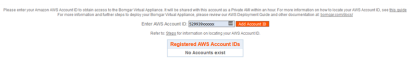
Bomgar Virtual Appliance Setup

1. Follow the Bomgar Virtual Appliance Installation Guide
2. When prompted for the Appliance License Key (ALK), enter **5103D-7048B-8EF15-F65DA**
3. Install any available Bomgar updates using 'Check for Updates'

We look forward to serving you. If you have any questions, don't hesitate to contact us using our Self Service Portal or by emailing support@bomgar.com

Best Regards,

2. Saisissez **l'identifiant de votre compte commercial AWS** ou de votre **compte gouvernemental AWS** dans la boîte de texte et cliquez sur **Ajouter un identifiant de compte**. Votre PRA Virtual Appliance sera partagé avec votre compte Amazon AWS en tant qu'Amazon Machine Image (AMI) privée dans un délai d'une heure. L'AMI sera partagée dans chacune de vos régions AWS.



Remarque : *si vous n'êtes pas sûr de savoir quel est votre identifiant de compte AWS, l'e-mail contient un lien vers une page d'aide d'Amazon expliquant comment le retrouver.*

3. Dans le tableau de bord AWS EC2, dans la **section AWS services**, cliquez sur le lien **EC2** pour lancer l'assistant.
4. Rendez-vous dans **Images > AMI**.
5. Dans le menu déroulant, cliquez sur **Images privées**.
6. Sélectionnez le PRA Virtual Appliance (par exemple, **Secure Remote Access Appliance - 5.2.0**) dans la liste d'AMI. Ceci est l'image de base du logiciel, qui devra ensuite être mise à jour et configurée.
7. Cliquez sur le bouton **Lancer**.
8. Choisissez un type d'instance. Nous prenons en charge tous les types d'instances t2 et m4. Référez-vous au tableau Licence et taille ci-dessous.
9. Cliquez sur **Suivant : Configurez les détails de l'instance**.
10. Après avoir configuré les détails de lancement de l'instance, cliquez sur **Suivant : Ajouter du stockage**.

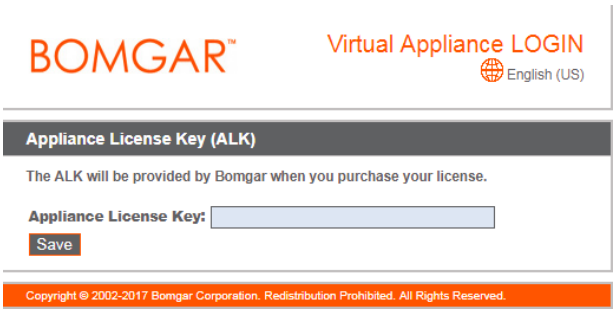
11. Sur la page **Ajouter du stockage**, configurez les tailles et volumes des disques que vous souhaitez inclure dans l'AMI. Nous vous recommandons de choisir **SSD d'usage général (gp2)** comme type pour les volumes racine et secondaire, mais vous pouvez choisir n'importe lequel des deux types de SSD (GP2 ou IO1). Si vous avez besoin d'un volume important pour des enregistrements, et que ce déploiement doit faire face à des impératifs de coûts, vous pouvez alors approvisionner un troisième disque et le configurer en tant que **Magnétique (standard)**. Pour connaître la taille recommandée des volumes des instances, référez-vous à la colonne **Disque AWS** dans le tableau Licence et taille ci-dessous. Vous pouvez activer l'option **Cryptage** si vous le souhaitez, bien que le produit Privileged Remote Access inclut également le cryptage des données stockées.

> Pour plus d'informations sur le chiffrement des données stockées, veuillez consulter la section Introduction au chiffrement des données stockées avec Privileged Remote Access BeyondTrust à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/how-to/data-at-rest-encryption/.

12. Cliquez sur **Suivant : Ajouter des balises**.
13. Cliquez sur **Suivant : Configurer le groupe de sécurité**.
14. L'assistant de lancement crée un groupe de sécurité que vous devez modifier ; autrement, vous pouvez créer un nouveau groupe de sécurité après avoir déployé l'image, afin que le site soit accessible à travers les ports 443 et 80. Pour procéder à cette opération, rendez-vous dans **Réseau & Sécurité > Groupes de sécurité** dans le **tableau de bord EC2**.
15. Cliquez sur **Vérifier et lancer**. Vérifiez les détails de votre instance puis cliquez sur **Lancer**.
16. Ignorez l'option de sélectionner ou créer une paire de clés, car l'instance n'autorisera pas l'accès SSH. À la place, sélectionnez **Continuer sans paire de clés**, cochez la case de confirmation, puis cliquez sur **Lancer les instances**.
17. Après le lancement du site, rendez-vous dans Instances > Instances dans le tableau de bord EC2 et localisez l'adresse **IP publique** assignée dans l'onglet **Description**. Ceci est l'adresse IP que vous utiliserez pour configurer votre serveur et votre registre DNS A.

> ***Remarque :*** *si vous interrompez ou arrêtez votre instance, vous n'êtes pas garanti de pouvoir récupérer la même adresse IP après redémarrage. Pour faciliter la gestion de votre DNS, nous vous recommandons d'acheter une adresse IP élastique.*

18. Dans un navigateur Web, rendez-vous sur https://[Adresse IP publique]/appliance.
19. Saisissez votre **clé de licence du serveur** fournie dans l'e-mail envoyé par l'Assistance technique BeyondTrust. Cliquez sur **Enregistrer**.



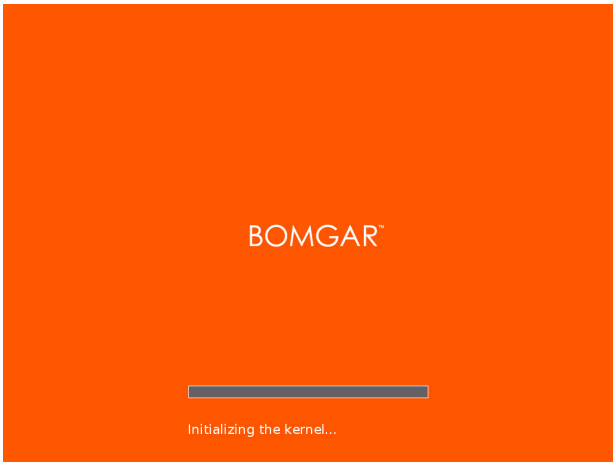
> ***Remarque :*** *aucune autre configuration du réseau ou de la console n'est nécessaire pour les serveurs basés sur Amazon AWS. Veuillez continuer pour Enregistrer et mettre à jour le serveur virtuel Privileged Remote Access*

Licence et taille

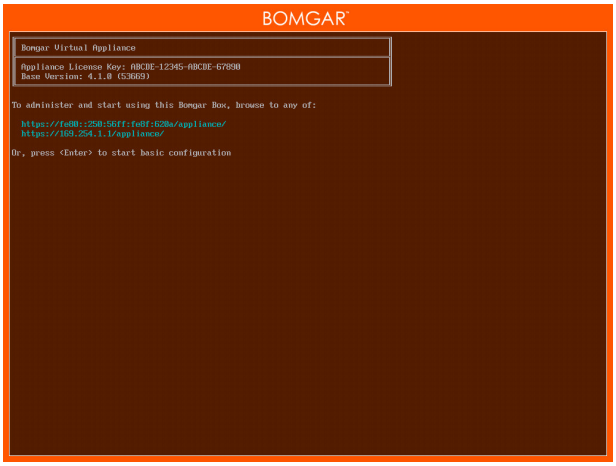
Taille d'approvisionnement	Nombre maximum de Jump Clients	Instance AWS	Disque AWS
Très petit	750	t2.medium	32/50
Petit	3 000	t2.medium	32/100
Moyenne	14 850	m4.xlarge	32/256
Grand		m4.2xlarge	32/1024

Premier démarrage d'un PRA Virtual Appliance Privileged Remote Access

1. Dans le client d'infrastructure virtuel, allez dans le dossier de MV que vous avez choisi ci-dessus et trouvez la nouvelle entrée pour le PRA Virtual Appliance. Faites un clic droit sur cette entrée, puis sélectionnez **Ouvrir console**. Cliquez ensuite sur le bouton de lecture pour démarrer votre PRA Virtual Appliance BeyondTrust.



2. Après le démarrage de votre PRA Virtual Appliance BeyondTrust, une ou plusieurs adresses IP seront affichées.

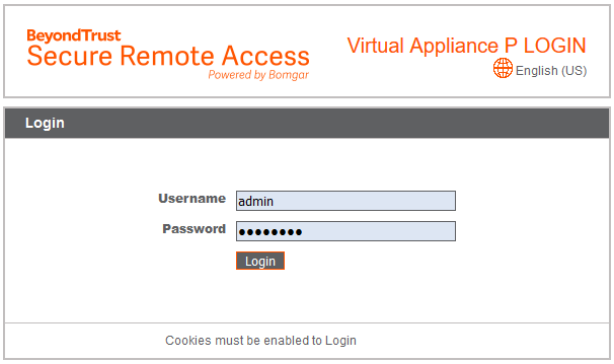


> ***Remarque :*** *si vous n'avez pas pu fournir de clé de licence du serveur lors du déploiement, appuyez sur Entrée pour entamer la configuration de base. La sélection 1 sur le prochain écran de menu vous permet de saisir manuellement la clé de licence du serveur. Revenez ensuite à l'écran principal.*

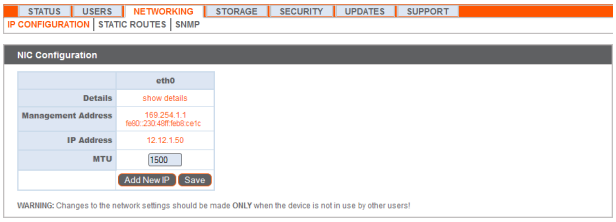
3. Depuis un ordinateur sur le même réseau, ouvrez un navigateur Internet et naviguez vers l'une des adresses IP données, suivie de **/appliance**. Si aucune des IP répertoriées n'est accessible, reportez-vous à « Administration avec la console de machine virtuelle Privileged Remote Access », page 31 pour assigner une adresse IP utilisable en utilisant l'interface de la console. Autrement, la portion VMware de la mise en place est terminée, et vous pouvez fermer la console VMware.

Configurer le PRA Virtual Appliance Privileged Remote Access

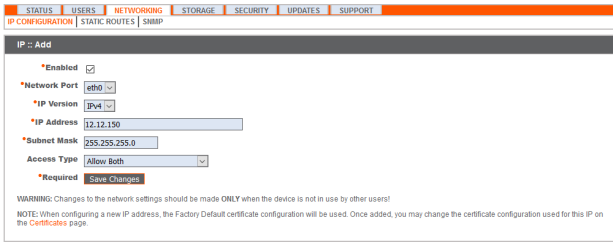
1. Dans l'interface **/appliance** de votre PRA Virtual Appliance BeyondTrust, connectez-vous en utilisant **admin** comme nom d'utilisateur et **password** comme mot de passe par défaut. Lors de votre première connexion, vous serez invité à changer de mot de passe.



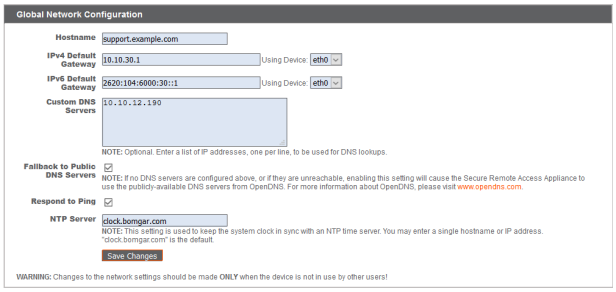
2. Allez ensuite sur **Réseau > Configuration IP**.
3. Sous la section **Configuration NIC**, cliquez sur **Ajouter nouvelle IP**.



4. Saisissez l'adresse IP statique et le masque de sous-réseau pour votre Secure Remote Access Appliance. Vous pouvez choisir si cette adresse IP prend en charge le trafic de session, le trafic internet, ou les deux. Cliquez ensuite sur **Enregistrer les modifications**.

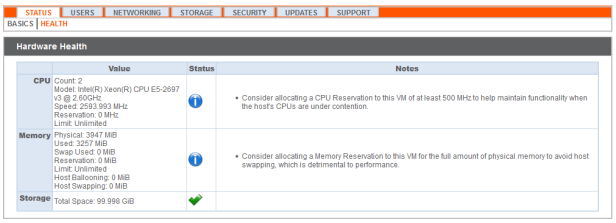


5. Dans la section **Configuration globale du réseau**, configurez le nom de la passerelle par défaut. La configuration des serveurs DNS n'est pas requise, mais elle est fortement recommandée. Après avoir saisi les informations requises, cliquez sur **Enregistrer les modifications**.



> ***Remarque :*** *des paramètres DNS valides sont nécessaires pour que la reprise en séquence et les mises à jour automatiques fonctionnent correctement. Pour vous aider à déterminer la configuration d'IP et de DNS appropriée pour votre réseau, consultez Le Secure Remote Access Appliance dans le réseau à l'adresse www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/dmz.*

6. Allez sur **État > Stockage** et cliquez sur **Formater ce disque** pour qu'il soit utilisé par le serveur.
7. Attendez que le formatage soit terminé, puis allez sur **État > Santé** pour vérifier que les besoins du PRA Virtual Appliance ont été satisfaits.



Pour plus d'informations, reportez-vous à « Consulter la santé du PRA Virtual Appliance Privileged Remote Access », page 32.

Référence d'URL

https://169.254.1.1/appliance/login.ns – Administration du serveur

https://access.example.com/login – Administration utilisateurs

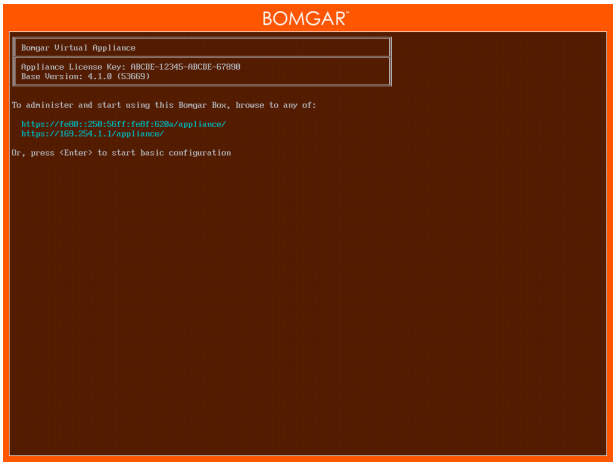
Enregistrer et mettre à jour le serveur virtuel Privileged Remote Access

Tant que vous n'aurez pas effectué les tâches de cette section, le serveur de mise à jour de BeyondTrust ne reconnaîtra pas le nouveau serveur, et vous ne pourrez pas naviguer vers l'interface /login.

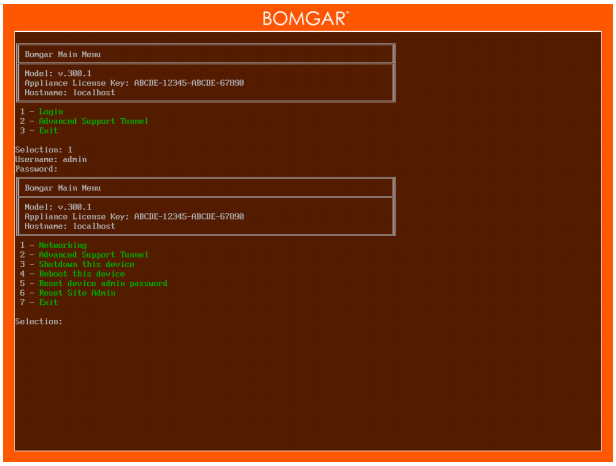
1. Obtenez un certificat SSL correspondant à votre nom de DNS. Transférez le certificat sur votre serveur. Pour des instructions détaillées, consultez le Guide de certificat SSL à l'adresse www.beyondtrust.com/docs/privileged-remote-access/how-to/sslcertificates.
2. Prenez une capture d'écran de l'onglet **/appliance > État > Bases**. Répondez à l'e-mail de téléchargement envoyé par l'assistance technique de l'Assistance technique BeyondTrust, en incluant dans votre e-mail cette capture d'écran ainsi que l'IP publique (le cas échéant), ou le certificat SSL du serveur. Si vous envoyez le certificat SSL, vérifiez qu'il est bien au format PKCS#7 (.p7b) ou DER (.cer). N'envoyez **pas** de PKCS#12 (.p12 et .pfx).
3. Attendez jusqu'à 24 heures que l'Assistance technique BeyondTrust enregistre le nouveau serveur et construise les packages logiciels nécessaires. Installez ensuite ces packages selon les instructions envoyées par l'Assistance technique BeyondTrust.
4. Une fois que vous avez installé la nouveau package de licence logicielle, votre interface /login sera accessible. Pour plus détails, consultez www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin.

Administration avec la console de machine virtuelle Privileged Remote Access

1. Après que vous avez fini de déployer votre PRA Virtual Appliance, vous pouvez lancer la console de machine virtuelle pour accéder à certaines fonctions administratives.
2. Le premier écran de la console de machine virtuelle présente les noms d'hôte et les adresses IP pour ce PRA Virtual Appliance. Pour effectuer des changements de configuration basiques depuis cette fenêtre, appuyez sur **Entrée**.



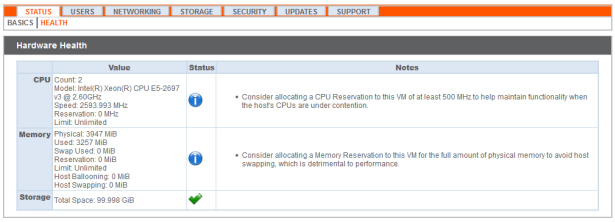
3. Faites votre choix dans le menu. Vous pouvez vous connecter pour effectuer des changements de configuration. Vous pouvez également saisir des codes d'assistance technique pour permettre la création d'un tunnel d'assistance technique initié par le serveur vers l'Assistance technique BeyondTrust afin de résoudre rapidement des problèmes complexes
4. Connectez-vous pour plus d'options. Vous pouvez configurer le réseau, autoriser un tunnel d'assistance technique avancé, éteindre ou redémarrer le PRA Virtual Appliance, ou réinitialiser le mot de passe du serveur ou le mot de passe administratif d'un site.



5. Sélectionnez **Réseau** pour gérer le nom d'hôte, les adresses IP, la passerelle par défaut et les serveurs DNS.
6. Choisissez une interface de réseau pour gérer sa vitesse ou la communication en duplex. Vous pouvez aussi ajouter ou modifier des adresses IP.

Consulter la santé du PRA Virtual Appliance Privileged Remote Access

1. Allez sur la page **État > Santé** dans l'interface d'administration /appliance. La page **Santé** vous donne des informations pour vous aider à garantir l'efficacité de votre installation de PRA Virtual Appliance BeyondTrust. Les informations présentées peuvent vous aider à résoudre les problèmes que vous pouvez rencontrer avec votre PRA Virtual Appliance.
2. Les informations en temps réel s'affichent dans trois catégories : **Processeur**, **Mémoire** et **Stockage**. Pour chaque catégorie, consultez **Valeur**, **État**, et toutes les **Notes** associées.



3. La **Valeur** montre les paramètres spécifiques du processeur, de la mémoire et du stockage associés à votre installation de PRA Virtual Appliance. Pour vous aider à évaluer rapidement les performances de votre installation, dans **État** vous pourrez voir une coche verte, un point d'exclamation bleu ou des croix rouges.

	Une coche verte vous montre immédiatement qu'une certaine catégorie est suffisamment configurée pour des performances de PRA Virtual Appliance optimales.
	Un point d'exclamation bleu indique que vous aurez peut-être besoin d'apporter des modifications pour améliorer les performances. Les changements suggérés sont indiqués dans la colonne **Notes** adjacente.
	Une croix rouge vous prévient d'une situation d'erreur de mémoire qui pourrait causer des problèmes pour votre PRA Virtual Appliance. Les changements suggérés pour corriger le problème associé à la croix rouge sont indiqués dans la colonne **Notes** adjacente, et peuvent nécessiter que vous contactiez l'Assistance technique BeyondTrust.

Questions fréquemment posées au sujet du PRA Virtual Appliance Privileged Remote Access

Vous trouverez ci-dessous certaines des questions fréquemment posées sur l'administration du PRA Virtual Appliance et des réponses à ces questions de la part de l'Assistance technique BeyondTrust.

VMware

Puis-je installer les outils VMware sur mon PRA Virtual Appliance BeyondTrust ?

Le PRA Virtual Appliance BeyondTrust est fourni avec les outils d'invité VMware déjà installés.

Est-ce qu'un décalage de temps entre mon hôte ESXi et PRA Virtual Appliance BeyondTrust peut causer des problèmes de connectivité ?

Oui, toute différence d'heure entre le PRA Virtual Appliance BeyondTrust et le serveur hôte ESXi peut causer des problèmes de connectivité. Pour empêcher ceci, spécifiez une source NTP valide dans l'interface /appliance du PRA Virtual Appliance, et vérifiez que votre hôte ESXi utilise une source NTP valide. VMware possède également une fonction pour synchroniser l'heure du système d'exploitation invité avec celle du serveur hôte ESXi. Si vous utilisez cette option, la source NTP dans le PRA Virtual Appliance BeyondTrust n'a PAS besoin d'être réglée. Il est recommandé d'utiliser une méthode ou l'autre, mais PAS les deux en même temps.

Quelle version de VMware est prise en charge pour héberger le PRA Virtual Appliance BeyondTrust ?

BeyondTrust certifie la prise en charge pour VMware vCenter 5.0+, Virtual Hardware Version 7+.

Est-ce que le PRA Virtual Appliance BeyondTrust requiert des ressources réservées dans VMware ?

À des fins de résolution de problèmes, un technicien de l'Assistance technique BeyondTrust peut demander à ce que le PRA Virtual Appliance BeyondTrust bénéficie de ressources réservées pour diagnostiquer de façon efficace un problème d'assistance technique.

Est-ce que BeyondTrust prend en charge la fonctionnalité d'instantané de VMware ?

BeyondTrust prend en charge la technologie de prise d'instantané seulement lors de situations de mises à niveau. L'instantané d'un PRA Virtual Appliance BeyondTrust éteint peut être pris avant une mise à niveau, et peut être utilisé pour revenir en arrière en cas d'échec de la mise à niveau

> ***Remarque :*** *BeyondTrust ne recommande pas et ne prend pas en charge la capture d'instantanés sur un PRA Virtual Appliance ou plusieurs en cours d'utilisation.*

Puis-je exécuter le PRA Virtual Appliance BeyondTrust dans mon environnement VMware en cluster ?

Oui, lorsque le PRA Virtual Appliance BeyondTrust est installé dans un cluster vSphere, il peut bénéficier de beaucoup des technologies à valeur ajoutée de VMware, comme VMotion, DRS et HA pour maximiser les performances et la durée de fonctionnement.

Puis-je spécifier un disque alternatif pour les enregistrements ?

Oui, dans certains cas vous souhaiterez peut-être séparer les disques pour les enregistrements si votre environnement VMware dispose d'un stockage hiérarchisé. Ajoutez un troisième disque à votre PRA Virtual Appliance BeyondTrust et redémarrez. Une fois que le PRA Virtual Appliance BeyondTrust a redémarré, le troisième disque sera provisionné et utilisé pour les enregistrements.

Le matériel virtuel de mon PRA Virtual Appliance BeyondTrust fonctionne actuellement sous une version plus ancienne et a besoin d'être mis à niveau. Quelles sont les recommandations de BeyondTrust pour les mises à niveau de version de matériel virtuel ?

BeyondTrust certifie la prise en charge pour VMware vCenter 5.0+, Virtual Hardware Version 7+.

Si votre configuration ne correspond pas à l'une des configurations ci-dessus, BeyondTrust recommande la mise à jour de la version du matériel virtuel de votre PRA Virtual Appliance BeyondTrust.

Pourquoi est-ce que le PRA Virtual Appliance n'arrive pas à importer avec l'erreur « Le package OVF nécessite la prise en charge des propriétés OVF » ?

Dans certaines circonstances, le PRA Virtual Appliance ne réussira pas à importer avec le message d'erreur « Le package OVF utilise des fonctions qui ne sont pas prises en charge lors du déploiement direct sur un hôte ESX. Détails ligne 88 : Élément 'Propriétés' non pris en charge. »

Cette erreur se produit lorsque l'hôte VMware recevant l'importation ne prend pas en charge les propriétés OVF. Plus particulièrement, cette erreur apparaîtra lorsque vous tentez d'importer le kit OVA de BeyondTrust (B300v v1) lors d'une connexion directe à un hôte ESXi via le client vSphere.

Pour corriger cette erreur et réussir à importer le kit OVA, connectez le client vSphere au serveur vCenter qui gère l'hôte ESXi, ou en utilisant vDirector.

Quelle est cette erreur : « Le fichier de certificat OVF n'est pas valide » ?

Lorsque vous importez un nouveau PRA Virtual Appliance BeyondTrust sur VMware en utilisant le package d'installation OVA, il est possible que VMware renvoie une erreur « Le fichier de certificat OVF n'est pas valide ». Ceci se produit lors d'une tentative d'importation du fichier OVF qui est inclus dans le fichier .ova du serveur. Ceci nécessiterait l'extraction du contenu du package OVA, et cela annulerait la validité de tout le package. Pour résoudre ce problème, téléchargez à nouveau le fichier OVA et importez-le sans extraire l'OVA. Si vous utilisez Internet Explorer, il peut être nécessaire de remplacer **.tar** par **.ova** dans l'extension du fichier téléchargé.

Le second disque virtuel doit-il être en provisionnement standard ou granulaire ?

Dans les versions actuelles, le modèle OVF choisit automatiquement le provisionnement standard pour le second et (le cas échéant) le troisième disque virtuel.

Selon la documentation ESXi et vCenter Server 5, le provisionnement granulaire alloue initialement uniquement l'espace réellement nécessaire à la machine virtuelle, et s'agrandit au besoin. En revanche, les deux formes de provisionnement standard allouent tout l'espace assigné du disque à la machine virtuelle à la création, le verrouillant à l'utilisation par une autre machine (voir « À propos des règles de provisionnement standard de disque virtuel » dans la documentation ESXi et vCenter Server 5 dans **Administration de machine virtuelle vSphere > Configuration de machines virtuelles > Configuration de disque virtuel** dans le centre de documentation vSphere à l'adresse vmware.com/support/pubs/). Bien que le serveur puisse opérer correctement avec un provisionnement granulaire, cela n'est pas le meilleur choix.

Pourquoi est-ce que le serveur virtuel se télécharge sous la forme d'un fichier .tar ?

Lorsque vous utilisez Internet Explorer, l'installeur OVA de BeyondTrust peut être téléchargé comme fichier « bomgar.tar » au lieu d'un fichier « bomgar.ova ». Pour installer le fichier selon le guide d'installation du PRA Virtual Appliance, remplacez simplement l'extension **.tar** par **.ova** et suivez le guide normalement.

Les disques durs virtuels peuvent-ils être stockés dans plusieurs banques de données ?

Certains clients dotés d'un PRA Virtual Appliance BeyondTrust peuvent souhaiter distribuer les différents disques de PRA Virtual Appliance parmi plusieurs banques de données VMware. BeyondTrust prend en charge cette configuration, et donc nos serveurs devraient fonctionner convenablement lorsque leurs disques virtuels se situent chacun dans une banque de données différente.

Hyper-V

Quelle version de Hyper-V est prise en charge pour héberger le PRA Virtual Appliance BeyondTrust ?

BeyondTrust certifie la prise en charge Hyper-V 2012 R2 (standalone), ainsi que Microsoft Server 2012 R2 avec le rôle Hyper-V activé.

Est-ce que BeyondTrust prend en charge la fonctionnalité d'instantané de Hyper-V ?

BeyondTrust prend en charge la technologie de prise d'instantané seulement lors de situations de mises à niveau. L'instantané d'un PRA Virtual Appliance BeyondTrust éteint peut être pris avant une mise à niveau, et peut être utilisé pour revenir en arrière en cas d'échec de la mise à niveau

Puis-je spécifier un disque alternatif pour les enregistrements ?

Oui, dans certains cas vous souhaiterez peut-être séparer les disques pour les enregistrements si votre environnement Hyper-V dispose d'un stockage hiérarchisé. Ajoutez un troisième disque à votre PRA Virtual Appliance BeyondTrust et redémarrez. Une fois que le PRA Virtual Appliance BeyondTrust a redémarré, le troisième disque sera provisionné et utilisé pour les enregistrements.

Le matériel virtuel de mon PRA Virtual Appliance BeyondTrust fonctionne actuellement sous une version plus ancienne et a besoin d'être mis à niveau. Quelles sont les recommandations de BeyondTrust pour les mises à niveau de version de matériel virtuel ?

Pour Hyper-V, BeyondTrust ne prend pour le moment en charge que les machines virtuelles de génération 1. L'image VA est fournie comme MV de génération 1.

Si votre configuration ne correspond pas à la configuration ci-dessus, BeyondTrust vous recommande de mettre à jour la version du matériel virtuel de votre PRA Virtual Appliance BeyondTrust.

Microsoft Azure

Est-ce que le modèle de déploiement Azure Classic est pris en charge ?

Non. Le seul modèle pris en charge est Azure Resource Manager (ARM).

Dois-je configurer le scripte Windows PowerShell différemment si je dispose d'un compte de stockage Premium ?

Oui. Si vous avez un compte de stockage Premium, vous devez modifier l'information **vmSize** de l'**ÉTAPE 2** du script pour indiquer **Premium** et la taille qui convient.

Puis-je utiliser des fonctions Azure supplémentaires de l'agent Linux Azure avec mon PRA Virtual Appliance BeyondTrust ?

BeyondTrust ne prend pas en charge ces fonctions à l'heure actuelle.

Dois-je saisir mon adresse IP publique dans l'interface BeyondTrust /appliance ?

Non. La couche réseau Azure associe l'IP publique à l'IP privée. Le PRA Virtual Appliance BeyondTrust attribue l'IP privée en utilisant DHCP.

Est-ce que la reprise en séquence est nécessaire ? Est-ce que la reprise en séquence est prise en charge pour Microsoft Azure ?

Bien que le risque de temps d'indisponibilité soit bien moins élevé dans Azure, il est toujours possible d'avoir besoin d'un serveur de reprise en séquence. La reprise en séquence est prise en charge dans Azure. Cependant, le partage d'IP ne fonctionne pas avec la mise en réseau d'Azure. Une modification de l'entrée DNS sera nécessaire pour effectuer une reprise en séquence vers un serveur de sauvegarde.

Ai-je besoin d'une IP statique pour mon PRA Virtual Appliance BeyondTrust ?

Attribuer une IP statique est le moyen le plus simple de s'assurer qu'il n'y a pas de problème de DNS lors d'un redémarrage, et pour garantir que les points d'intégration qui nécessitent une adresse IP fonctionnent correctement. Cependant, attribuer un enregistrement CNAME pour l'entrée de DNS de votre serveur devrait suffire pour la plupart des déploiements.

Problèmes généraux

Est-ce qu'un PRA Virtual Appliance d'évaluation peut être converti en version de production ?

Oui, le PRA Virtual Appliance existant peut être converti en version de production.

Une fois les licences du PRA Virtual Appliance achetées, l'Assistance technique BeyondTrust construit un package de désinstallation pour le PRA Virtual Appliance d'évaluation et un package d'installation pour le PRA Virtual Appliance de production.

Si vous avez créé des fournisseurs de sécurité et des comptes utilisateur sur le serveur d'évaluation, créez une sauvegarde grâce à **/login > Gestion** et restaurez cette sauvegarde sur le PRA Virtual Appliance de production.

Les ressources disponibles peuvent-elles être modifiées ?

Il est possible d'ajouter des ressources additionnelles à un PRA Virtual Appliance BeyondTrust, et il est possible de réduire la mémoire et les cycles de processeur disponibles ; cependant, il n'est pas possible de réduire le stockage disponible de façon sûre, et rien de tout cela ne doit être effectué lorsque le serveur est allumé. Après avoir éteint le serveur et avoir effectué vos changements, le serveur devrait reconnaître les modifications au prochain démarrage.

Un PRA Virtual Appliance a deux ou trois disques durs virtuels, en fonction de la configuration que vous avez sélectionnée lors du déploiement : petit, moyen ou grand. Les déploiements petits et moyens ont deux disques, tandis que les grands en ont deux. Le premier disque est utilisé pour la racine du système d'exploitation dans les trois cas, et le second disque pour les données de site /login et les enregistrements dans les déploiements petits et moyens.

Dans les déploiements grands, les enregistrements sont déplacés du deuxième au troisième disque. Si votre PRA Virtual Appliance était à l'origine déployé avec deux disques durs virtuels, vous pouvez en ajouter un troisième plus tard, et le serveur stockera automatiquement les enregistrements de session sur celui-ci. Le serveur n'utilisera pas plus de trois disques.

1. Éteindre le PRA Virtual Appliance BeyondTrust.
2. Ajuster l'allocation de RAM et/ou du processeur et/ou augmenter l'espace disque utilisant VMware.
3. Allumer le PRA Virtual Appliance BeyondTrust.

Le PRA Virtual Appliance peut-il se replier sur un niveau de stockage plus lent ?

Les organisations peuvent choisir d'établir le stockage d'un PRA Virtual Appliance par le biais d'un stockage hiérarchisé dans un SAN. Le stockage « Niveau rapide 1 » fait en général référence à des structures qui utilisent la technologie SSD pour les données auxquelles on accède fréquemment, et le stockage « lent » fait en général référence aux données placées dans des technologies de type SAS, NL-SAS ou SATA. L'un ou l'autre fonctionnera avec BeyondTrust, mais certaines configurations de stockage ne sont pas prises en charge lors de l'utilisation de deux serveurs en reprise en séquence.

Dans les cas où le PRA Virtual Appliance principal possède un stockage en SSD / stockage de niveau 1, ces règles s'appliquent au serveur de secours :

- Un grand PRA Virtual Appliance doit être provisionné avec du stockage de même niveau.
- Un PRA Virtual Appliance petit ou moyen peut avoir un stockage plus limité s'ils sont appuyés par des disques à 10 000 ou 15 000.
- Aucun PRA Virtual Appliance de sauvegarde ne peut avoir de vitesse de disque inférieure à 10 000 / 15 000.

Les spécifications exactes pour petit, moyen et grand sont décrites dont notre document Directives relatives à la taille du serveur virtuel Privileged Remote Access à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/virtual/sizing.htm. Il est important de noter que BeyondTrust ne nécessite aucun niveau particulier pour qu'un

PRA Virtual Appliance démarre simplement et fonctionne en isolement. Le stockage hiérarchisé ne devient un problème que lorsque seulement deux serveurs sont utilisés en reprise en séquence.

Le clonage d'un PRA Virtual Appliance est-il pris en charge ?

Après l'installation d'un PRA Virtual Appliance BeyondTrust dans un environnement ESX ou ESXi, l'administrateur peut souhaiter cloner le serveur. Cloner une machine virtuelle crée un double de la machine virtuelle avec la même configuration et les mêmes logiciels installés que l'original. Cette fonction d'ESX et d'ESXi n'est pour l'instant pas prise en charge par le PRA Virtual Appliance BeyondTrust.

Est-ce que le PRA Virtual Appliance prend en charge le gestionnaire de récupération de site (SRM) vCenter ?

Le gestionnaire de récupération de site (SRM) de vCenter se sert de la réplication de vSphere pour fournir une récupération de sinistre. Les administrateurs qui exécutent BeyondTrust dans un système vCenter voudront peut-être tirer parti de ceci avec un PRA Virtual Appliance BeyondTrust. Bien que BeyondTrust est censé fonctionner avec le SRM de vCenter, effectuer une restauration depuis une réplication comme cela serait pour le serveur l'équivalent de débrancher la prise, et il y aurait donc un risque de corruption de fichiers système, ce qui pourrait se traduire par une potentielle perte de données.

Mentions pour logiciels Open Source

Pour obtenir des informations sur les droits d'auteurs et les mentions des logiciels open source utilisés dans le matériel et les logiciels BeyondTrust, veuillez consulter l'Index des attributions à l'adresse www.beyondtrust.com/docs/privileged-remote-access/updates/attributions.