BeyondTrust

Privileged Remote Access 20.1
Interface d’administration

TC:9/30/2020

Table des matières

Interface d'admin Privileged Remote Access BeyondTrust

Ce guide offre un aperçu détaillé de **/login** et a pour objectif de vous aider à administrer les utilisateurs BeyondTrust et votre logiciel BeyondTrust. Le Secure Remote Access Appliance sert de point d'administration et de gestion central de votre logiciel BeyondTrust et vous permet de vous connecter depuis n'importe quel endroit disposant d'un accès internet pour télécharger la console d'accès.

Utilisez ce guide uniquement après que l'administrateur a procédé à l'installation et à la configuration initiales du Secure Remote Access Appliance, comme l'explique le Guide d'installation matérielle du Secure Remote Access Appliance à l'adresse www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/hardware/. Une fois BeyondTrust correctement installé, vous pouvez commencer immédiatement à accéder à vos points de terminaison. Si vous avez besoin d'aide, contactez l'Assistance technique BeyondTrust à l'adresse www.beyondtrust.com/support.

Connexion à l'interface d'administration PRA

Connexion

Connectez-vous à l'interface d'administration de l'utilisateur en allant à l'URL de votre serveur, suivie de **/login**. L'interface d'administration de l'utilisateur permet aux administrateurs de créer des comptes d'utilisateur et de configurer les paramètres du logiciel.

Bien que l'URL de votre serveur puisse être n'importe quel DNS enregistré, il est plus que probable qu'il s'agisse d'un sous-domaine du domaine principal de votre entreprise (par ex. access.example.com/login).

Nom d'utilisateur par défaut : **admin**

Mot de passe par défaut : **password**

Remarque : *Pour des raisons de sécurité, le nom d'utilisateur et le mot de passe d'administration utilisés pour l'interface /appliance sont différents de ceux utilisés pour l'interface /login et doivent être gérés séparément.*

Si l'authentification à deux facteurs est activée sur votre compte, saisissez le code de l'application d'authentification.

Remarque : *Les utilisateurs qui se connectaient à l'aide de codes obtenus par e-mail passent automatiquement à l'authentification 2FA. Ils ont toutefois la possibilité d'utiliser des codes e-mail jusqu'à ce qu'ils soient inscrits sur une application. Après une première utilisation de 2FA, l'option du code e-mail n'est plus disponible.*

Pour plus d'informations, consultez la section Connexion à la console d'accès PRA à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/login-to-the-access-console.htm.

Utiliser l'authentification de navigateur intégrée

Si Kerberos a été correctement configuré pour une authentification unique, vous pouvez cliquer sur le lien pour utiliser l'authentification de navigateur intégrée, ce qui vous permet d'entrer directement dans l'interface Web sans avoir à saisir vos informations d'authentification.

Vous avez oublié votre mot de passe ?

Ce lien est visible si la réinitialisation du mot de passe a été activée sur la page **/login > Gestion > Sécurité** et le serveur SMTP a été configuré pour votre site. Pour réinitialiser le mot de passe, cliquez sur le lien, saisissez et confirmez votre adresse e-mail, puis cliquez sur **Envoyer**. Si plusieurs utilisateurs partagent la même adresse e-mail, vous devez confirmer votre nom d'utilisateur. Vous recevrez alors un lien par e-mail qui vous renvoie à la page de connexion. Sur l'écran de connexion, saisissez et confirmez votre nouveau mot de passe, puis cliquez sur **Modifier le mot de passe**.

Accord de connexion

Les administrateurs peuvent restreindre l'accès à l'écran de connexion en activant un accord de connexion devant impérativement être validé pour pouvoir continuer. L'accord de connexion peut être activé et personnalisé sur la page **/login > Gestion > Configuration du Site**.

Administration Privileged Remote Access : État

Informations : Consultation des informations logicielles Privileged Remote Access BeyondTrust

État du site

La page principale de l'interface /login Privileged Remote Access de BeyondTrust permet d'avoir un aperçu général des informations sur les statistiques de votre Secure Remote Access Appliance. Lorsque vous contactez l'Assistance technique BeyondTrust pour des mises à jour de logiciel ou des résolutions de problèmes, il se peut que l'on vous demande d'envoyer par e-mail une capture d'écran de cette page.

Redémarrer le logiciel Privileged Remote Access

Vous pouvez redémarrer le logiciel BeyondTrust à distance. Ne redémarrez votre logiciel que si cela vous a été demandé par l'Assistance technique BeyondTrust.

Fuseau horaire

Un administrateur peut sélectionner le fuseau horaire approprié dans le menu déroulant. La date et l'heure du serveur seront ainsi définies en fonction de la région sélectionnée.

Télécharger le rapport d'utilisation des licences

Téléchargez un fichier zip contenant des informations détaillées (en anglais uniquement) sur votre utilisation de licences BeyondTrust. Ce fichier contient une liste de tous les éléments de Jump (sans compter les Jump Clients désinstallés), les comptes quotidiens d'opérations d'élément de Jump et d'utilisation de licences, et un résumé pour l'utilisation et la résiliation de licence pour le Secure Remote Access Appliance et son point de terminaison.

Logiciel client

Ceci est le nom d'hôte auquel les logiciels clients BeyondTrust se connectent. Si le nom d'hôte tenté par un logiciel client doit changer, prévenez l'Assistance technique BeyondTrust des changements requis afin qu'elle puisse créer une mise à jour logicielle.

Clients connectés

Consultez le nombre et le type de logiciels clients BeyondTrust connectés à votre Secure Remote Access Appliance.

> Pour en savoir plus sur le Secure Remote Access Appliance, veuillez consulter la section Vue d'ensemble du Secure Remote Access Appliance à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/index.htm.

Clients GIAPT

Consultez le nombre de gestionnaires d'informations d'authentification de point de terminaison BeyondTrust (GIAPT) connectés à votre Secure Remote Access Appliance. Vous pouvez également consulter les informations liées à l'emplacement et la durée de connexion de chaque GIAPT.

Remarque : *pour optimiser le temps de disponibilité, les administrateurs peuvent installer jusqu'à 5 GIAPT sur plusieurs machines Windows pour communiquer avec le même site sur le Secure Remote Access Appliance. Une liste des GIAPT connectés au site du serveur est disponible sur* ***/login > État > Information > Clients GIAPT****.*

Remarque : *lorsque plusieurs GIAPT sont connectés au site BeyondTrust, le Secure Remote Access Appliance achemine les demandes vers le GIAPT ayant été le plus longtemps connecté au serveur.*

Pour plus d'informations, veuillez consulter la section Connexion aux points de terminaison en utilisant l'injection d'informations d'authentification à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/web-access/credential-injection.htm.

Utilisateurs : Regarder les utilisateurs connectés et envoyez des messages

Utilisateurs connectés

Consultez une liste des utilisateurs connectés à la console d'accès, ainsi que l'heure de leur connexion et s'ils exécutent des sessions.

Terminer

Vous pouvez mettre fin à la connexion d'un utilisateur à la console d'accès.

Envoyer un message aux utilisateurs

Envoyez un message à tous les utilisateurs connectés dans une fenêtre contextuelle de la console d'accès.

Utilisateurs en disponibilité étendue

Regardez quels utilisateurs ont le mode disponibilité étendue activé.

Désactiver

Vous pouvez désactiver la disponibilité étendue d'un utilisateur.

Nouveautés : Consulter les informations relatives à la version du logiciel

Nouveautés

Passez facilement en revue les fonctionnalités de BeyondTrust disponibles avec chaque nouvelle version. Tenez-vous informé des nouvelles fonctions disponibles pour tirer le meilleur parti de votre déploiement BeyondTrust.

La première fois que vous vous connectez à l'interface d'administration après une mise à niveau du logiciel BeyondTrust, la page **Nouveautés** est mise en évidence et vous informe des nouvelles fonctions disponibles sur votre site. Vous devez être un administrateur pour voir cet onglet.

Les informations affichées sur la page **Nouveautés** sont également accessibles aux utilisateurs dans la console d'accès dans le menu **Aide > À propos**.

Pour plus d'informations, veuillez consulter la section Documentation relative à la mise à jour de Privileged Remote Access BeyondTrust à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/updates/index.htm.

Mon compte : Modification du mot de passe et du nom d'utilisateur, et téléchargement de la Console d'Accès ainsi que d'autres logiciels

Console d'accès Privileged Web BeyondTrust

Lancez la console d'accès Privileged Web, une console d'accès basée sur le Web. Accédez à des systèmes distants depuis votre navigateur sans avoir à télécharger et à installer complètement la console d'accès.

BeyondTrust Console d'Accès

Choisir une plate-forme

Choisissez le système d'exploitation sur lequel vous souhaitez installer ce logiciel. Ce menu déroulant sélectionne par défaut l'installeur approprié détecté pour votre système d'exploitation.

> Pour plus d'informations, veuillez consulter le Guide de la Privileged Web Access Console à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/web-access/index.htm.

Télécharger la Console d'Accès BeyondTrust

Télécharger l'installeur de la console d'accès BeyondTrust.

Pour les administrateurs système devant déployer l'installeur de la console sur un grand nombre de systèmes, l'installeur Microsoft peut être utilisé avec l'outil de gestion de système de votre choix. Dans votre invite de commande, lorsque vous composez la commande pour installer la console avec un MSI, modifiez pour indiquer le répertoire de téléchargement du MSI et saisissez la commande figurant à la page **Mon compte**.

Vous pouvez inclure des paramètres facultatifs pour l'installation du MSI.

- **INSTALLDIR=** accepte tout chemin d'accès à un répertoire valide dans lequel vous voulez installer la console.
- **RUNATSTARTUP=** accepte **0** (par défaut) ou **1**. Si vous saisissez 1, la console s'exécutera à chaque démarrage de l'ordinateur.
- **ALLUSERS=** accepte **""** ou **1** (par défaut). Si vous saisissez **1**, la console s'installera pour tous les utilisateurs de l'ordinateur ; sinon, elle s'installera uniquement pour l'utilisateur actuel.
- **SHOULDAUTOUPDATE=1** Si vous n'installez que pour l'utilisateur actuel, vous pouvez opter pour une mise à jour automatique de la console chaque fois que le site est mis à niveau en saisissant une valeur de 1 ; une valeur de **0** (par défaut) empêche la mise à jour automatique et la console devra être réinstallée manuellement lorsque le site sera mis à niveau. Si vous installez la console pour tous les utilisateurs, elle ne se mettra pas automatiquement à jour.

Modifier votre mot de passe

BeyondTrust vous recommande de changer régulièrement votre mot de passe.

Nom d'utilisateur, Mot de passe actuel, Nouveau mot de passe

Vérifiez que vous êtes connecté au compte dont vous souhaitez changer le mot de passe, puis saisissez votre mot de passe actuel. Créez et confirmez un nouveau mot de passe pour votre compte. Vous pouvez définir le mot de passe de votre choix, tant que la chaîne reste conforme à la règle définie sur la page **/login > Gestion > Sécurité**.

Modifiez vos paramètres d'e-mail

Adresse e-mail

Définissez une adresse e-mail où envoyer les notifications, comme les réinitialisations de mot de passe ou le mode Disponibilité étendue.

Mot de passe

Saisissez le mot de passe de votre compte /login, pas celui de votre e-mail.

Authentification à deux facteurs

Activer l'authentification à deux facteurs

Activez l'authentification à deux facteurs (2FA) pour améliorer le niveau de sécurité des utilisateurs accédant à /login et à la console d'accès BeyondTrust. Cliquez sur **Activer l'authentification à deux facteurs**, puis utilisez l'application d'authentification de votre choix, comme Google Authenticator, pour scanner le code QR sur la page. Vous pouvez aussi saisir manuellement le code alphanumérique sous le code QR dans votre appli d'authentification.

L'application enregistre automatiquement le compte et vous propose des codes. Saisissez votre mot de passe et le code généré par l'application sélectionnée, puis cliquez sur **Activer**. Veuillez noter qu'après avoir été généré, un code n'est valable que pendant 60 secondes. Une fois connecté, vous avez la possibilité de changer d'application d'authentification ou de désactiver l'authentification 2FA.

Remarque : *si votre administrateur a imposé l'option 2FA, il est impossible de la désactiver.*

Mode disponibilité étendue

Activer ou désactiver

Activez ou désactivez le mode Disponibilité étendue en cliquant sur le bouton **Activer/Désactiver**. Le mode disponibilité étendue vous permet de recevoir des invitations par e-mail de la part d'autres utilisateurs demandant de partager une session lorsque vous n'êtes pas connecté à la console.

Agent de bureau à distance

Téléchargez l'installeur de l'agent d'accès au bureau à distance

L'agent de bureau à distance doit être installé sur des serveurs Windows 64 bits dont les services Bureau à distance sont activés et qui ont besoin de lancer et d'injecter des informations d'authentification dans des applications définies par l'administrateur.

Carte à puce virtuelle

Pour tenter l'authentification par carte à puce virtuelle, l'utilisateur BeyondTrust doit disposer du pilote de carte à puce virtuelle BeyondTrust installé. L'ordinateur cible doit en outre être exécuté avec des droits accrus. Le pilote de carte à puce virtuelle BeyondTrust pour point de terminaison doit également être installé, ou il doit être accessible par la fonction Jump vers de la console d'accès.

> Pour plus d'informations et pour connaître les exigences, consultez le document Cartes à puce pour l'authentification à distance à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/how-to/smart-card/index.htm.

Choisir une architecture Windows

Sélectionnez pour télécharger l'installeur de carte à puce virtuelle pour le système d'utilisateur BeyondTrust ou le système de point de terminaison.

Télécharger l'installeur de la carte à puce virtuelle

Téléchargez l'installeur de la carte à puce virtuelle sélectionné ci-dessus. Une carte à puce virtuelle vous permet de vous authentifier sur un système distant à l'aide d'une carte à puce installée sur votre système local.

Configuration

Options : Gérer les options de connexion, enregistrer des sessions, accélérer les sessions

Options de session

Exiger des sessions terminées à la déconnexion ou fermeture

Si vous cochez **Exiger des sessions terminées à la déconnexion ou fermeture**, les utilisateurs ne pourront pas se déconnecter de la console s'ils ont des onglets de session ouverts.

Options de connexion

Délai de reconnexion

Déterminez le délai avant qu'un client de point de terminaison déconnecté puisse à nouveau se connecter.

Limiter l'accès physique au point de terminaison en cas de perte de la connexion du point de terminaison ou de déconnexion de l'ensemble des utilisateurs de la session

Si la connexion de la session est perdue, l'entrée souris et clavier du système distant peut être temporairement désactivée, pour reprendre lorsque la connexion est restaurée ou quand la session est terminée.

Comportement de fin de session

Si vous ne pouvez pas vous reconnecter dans le temps que vous avez défini dans **Délai de reconnexion**, choisissez l'action à effectuer. Pour empêcher un utilisateur final d'accéder à des privilèges non autorisés après une session avec des droits accrus, réglez le client pour qu'il déconnecte automatiquement l'utilisateur final de l'ordinateur Windows distant à la fin de la session, qu'il verrouille l'ordinateur distant, ou qu'il ne fasse rien. Ces règles ne s'appliquent pas aux sessions de partage de navigation.

Autoriser les utilisateurs à remplacer ce paramètre session par session

Vous pouvez autoriser un utilisateur à outrepasser le paramètre de fin de session dans l'onglet **Résumé** de la console au cours d'une session.

Options d'enregistrement de session d'accès

Activer l'enregistrement de partage d'écran

Choisissez si les sessions de partage d'écran doivent être automatiquement enregistrées sous forme de vidéos.

Résolution d'enregistrement de partage d'écran

Définissez la résolution à laquelle visionner l'enregistrement de session.

> ***Remarque :*** *tous les enregistrements sont enregistrés en format brut ; le choix de la résolution affecte uniquement la lecture.*

Activer l'enregistrement utilisateur pour le Jump en tunnel par protocole

Choisissez si les sessions de Jump en tunnel par protocole doivent automatiquement être enregistrées en vidéo. Comme les Jumps en tunnel par protocole nécessitent l'utilisation d'une application tierce de votre choix, tout le bureau de l'utilisateur est enregistré, incluant tous les moniteurs.

Résolution d'enregistrement de l'utilisateur

Définissez la résolution à laquelle visionner l'enregistrement de session.

> ***Remarque :*** *tous les enregistrements sont enregistrés en format brut ; le choix de la résolution affecte uniquement la lecture.*

Exiger le consentement de l'utilisateur avant le début de l'enregistrement

Choisissez si les utilisateurs doivent recevoir une invite leur indiquant que leur bureau peut être enregistré lors du début de la session de Jump en tunnel par protocole. Il est à noter que si un utilisateur ne donne pas son autorisation, la session de Jump en tunnel par protocole est interrompue.

Activer l'enregistrement de l'interpréteur de commandes

Choisissez si les sessions d'interpréteur de commandes doivent être automatiquement enregistrées sous forme de vidéos. L'activation de l'enregistrement d'interpréteur de commandes active également la mise à disposition de transcriptions textuelles des sessions d'interpréteur de commandes.

Résolution de l'enregistrement de l'interpréteur de commandes

Définissez la résolution à laquelle visionner l'enregistrement de session.

> ***Remarque :*** *tous les enregistrements sont enregistrés en format brut ; le choix de la résolution affecte uniquement la lecture.*

IMPORTANT !

Les paramètres d'enregistrement activés sur cette page peuvent être remplacés par une règle de Jump avec l'option ***Désactiver les enregistrements de session*** *sélectionnée. Cette option affecte le partage d'écran, l'enregistrement de Jump en tunnel par protocole et les enregistrements d'interpréteur de commandes.*

Activer l'enregistrement automatique des informations système

Choisissez si les informations système doivent être automatiquement récupérées depuis l'ordinateur distant au début de la session pour qu'elles soient disponibles plus tard dans les détails du rapport de session.

Activer les preuves de session

Choisissez si vous voulez la capacité supplémentaire de rechercher parmi les sessions en fonction des évènements de session, qui comprennent les messages instantanés, le transfert de fichier, les évènements de l'éditeur de registre et les évènements de changement de premier plan des fenêtres. Cette fonction est activée par défaut.

> ***Remarque :*** *si l'interpréteur de commandes est activé, les preuves de session vous permettent d'effectuer une recherche en profondeur des enregistrements de l'interpréteur de commandes. Lorsque vous recherchez une expression clé et qu'une correspondance est trouvée dans un enregistrement d'interpréteur de commandes, la vidéo sera automatiquement avancée jusqu'à ce moment. Aucun résultat de commande ou mot de passe n'est enregistré.*

Options pair-à-pair

Désactivé(e)

Ceci est le réglage par défaut. Désactive les connexions pair-à-pair. Pour activer cette fonction, vous devez choisir un serveur pour négocier la session. Lorsque le partage d'écran, le transfert de fichiers ou l'interpréteur de commandes est détecté, la connexion pair-à-pair est tentée. Si elle réussit, cela crée une connexion directe entre l'utilisateur et les systèmes clients, tout en continuant d'envoyer un second flux de données au serveur à des fins d'audit. Si pour une raison quelconque la connexion pair-à-pair ne peut pas être établie, le trafic de session redevient par défaut une connexion gérée par le serveur.

Utilisez un serveur pair-à-pair hébergé par BeyondTrust

Les clients BeyondTrust tentent d'atteindre une connexion pair-à-pair à travers le serveur hébergé par BeyondTrust. Ceci nécessite que vos clients BeyondTrust puissent envoyer des demandes de connexion sortantes UDP 3478 à stun.bomgar.com. Ce réglage devrait fonctionner dans la plupart des situations.

Utiliser le serveur comme serveur pair-à-pair

Si votre organisation requiert des paramètres de sécurité spécifiques pour le trafic, vous pouvez utiliser le serveur comme serveur pair-à-pair. Ceci nécessite que votre serveur puisse accepter les demandes de connexion entrantes UDP 3478 par vos clients BeyondTrust. Des paramètres de pare-feu supplémentaires sont nécessaires.

> Pour plus d'informations, veuillez consulter la section Administration du serveur : Définir des restrictions liées aux comptes, aux réseaux et aux ports, activer un serveur STUN, installer un protocole Syslog, activer un accord de connexion, réinitialiser un compte d'administrateur à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/web/security-appliance-administration.htm.

Logo du portail d'accès

Les administrateurs ont la possibilité de mettre en ligne une image de logo personnalisée sur des pages Web publiques. Cela permet aux utilisateurs externes de vérifier qu'ils se trouvent sur le site Web de votre organisation. De plus, cette mesure met en avant votre portail d'accès et votre marque.

L'image du logo est affichée sur les pages Web publiques suivantes :

- Accès à la page d'invitation au téléchargement (page affichée après avoir cliqué sur un lien dans une invitation d'accès envoyée par e-mail)
- URL des enregistrements publics (voir et télécharger)
- Réponses de disponibilité étendue (page affichée après avoir cliqué sur un lien dans une invitation de disponibilité étendue envoyée par e-mail)
- Autorisations d'approbation de Jump (page affichée après avoir cliqué sur un lien dans une approbation de Jump envoyée par e-mail)

Remarque : *les fichiers d'image du logo mis en ligne peuvent utiliser un format d'image standard quelconque. La taille de l'image logique ne doit pas excéder 250 pixels en largeur et 64 pixels en hauteur. Toutefois, BeyondTrust prend en charge les affichages à haute densité, ce qui permet une taille physique maximale de 500 pixels en largeur et de 128 pixels en hauteur.*

Équipes : Rassembler les utilisateurs en équipes

Gérer les équipes

Grouper des utilisateurs en équipes favorise l'efficacité en attribuant le leadership dans des groupes d'utilisateurs. Dans la console d'accès, chaque équipe apparaît comme une file d'attente séparée pour les sessions.

Ajouter une nouvelle équipe, modifier, supprimer

Créer une nouvelle équipe, modifier ou supprimer une équipe existante. La suppression d'une équipe ne supprime pas ses comptes d'utilisateurs, mais uniquement l'équipe à laquelle ils sont associés.

Ajouter ou modifier une équipe

Nom d'équipe

Créez un nom unique permettant d'identifier cette équipe.

Nom de code

Définissez également un nom de code, qui sera utilisé à des fins d'intégration. Dans le cas contraire, le système en crée un automatiquement.

Commentaires

Ajoutez des commentaires pour aider à identifier la fonction de cet objet.

Règles de groupe

Notez toutes les règles de groupe attribuant des membres à cette équipe. Cliquez sur le lien renvoyant vers la page **Règles de groupe** afin de vérifier les membres des règles ou d'en assigner.

Membres de l'équipe

Lancez une recherche pour ajouter des utilisateurs à cette équipe. Vous pouvez déterminer le rôle de chaque membre, tel que **Membre de l'équipe**, **Chef d'équipe** ou **Responsable d'équipe**. Ces rôles représentent une part significative de la fonction **Tableau de bord** de la console d'accès.

Dans le tableau ci-dessous, consultez les membres d'équipe existants. Vous pouvez filtrer la vue en saisissant un nom d'utilisateur dans la zone de filtre. Vous pouvez aussi modifier les paramètres d'un membre ou supprimer un membre de l'équipe.

Pour ajouter un groupe d'utilisateurs à une équipe, consultez **Utilisateurs et sécurité > Règles de groupe** et assignez ce groupe à une ou à plusieurs équipes dans un rôle donné.

Remarque : *Vous pouvez ne pas être en mesure de modifier ou de supprimer certains membres d'une équipe. Cela arrive lorsqu'on ajoute un utilisateur par le biais d'une règle de groupe.*

Cliquez sur le lien de la règle de groupe pour modifier la règle de façon globale. Les changements apportés à une règle de groupe s'appliquent également à l'ensemble des membres de cette règle de groupe.

Vous pouvez aussi ajouter un utilisateur à l'équipe, en ignorant ses paramètres tels qu'il sont définis ailleurs.

Paramètres du tableau de bord

Au sein d'une équipe, un utilisateur ne peut administrer que les personnes ayant un rôle inférieur au sien. Sachez toutefois que les rôles s'appliquent strictement au cas par cas pour chaque équipe. Ainsi, un utilisateur peut être en mesure d'administrer un autre utilisateur dans une équipe, sans pouvoir administrer ce même utilisateur dans une autre.

Surveillance des membres de l'équipe depuis le tableau de bord

Si l'option est activée, un chef ou responsable d'équipe peut surveiller les membres de l'équipe depuis le tableau de bord. Faites une sélection pour **désactiver** la possibilité de surveiller, ou choisissez **Console d'Accès uniquement** pour autoriser un chef ou responsable d'équipe à surveiller la console d'accès d'un membre de l'équipe. La surveillance affecte tous les responsables et chefs d'équipe de toutes les équipes du site.

Activer « Rejoindre session » et « Prendre le contrôle » sur le tableau de bord

Si cette option est cochée, un chef d'équipe peut rejoindre ou reprendre les sessions d'un membre de l'équipe. De la même façon, un responsable d'équipe peut administrer les membres et les chefs de l'équipe.

Champs personnalisés : Créer, modifier et supprimer des champs d'API personnalisés

Créez des champs d'API personnalisés pour collecter des informations sur votre client, ce qui vous permet d'intégrer BeyondTrust de manière plus poussée avec vos programmes existants. Les champs personnalisés doivent être utilisés en combinaison avec l'API BeyondTrust. Créer un nouveau champ, modifier ou supprimer un champ existant.

Ajouter ou modifier un champ d'API personnalisé

Nom affiché

Créez un nom unique pour identifier ce champ personnalisé. Ce nom est affiché dans la console d'accès dans les détails de session.

Nom de code

Définissez également un nom de code, qui sera utilisé à des fins d'intégration. Dans le cas contraire, le système en crée un automatiquement.

Afficher dans la Console d'Accès

Si vous cochez **Afficher dans la Console d'Accès**, ce champ et ses valeurs apparaîtront là où les détails de session personnalisés s'affichent dans la console d'accès.

Jump

Jump Clients : gérez les paramètres et installez des Jump Clients pour l'accès aux points de terminaison

Assistant de déploiement en masse de Jump Clients

L'assistant de déploiement en masse permet aux administrateurs et aux utilisateurs privilégiés de déployer des Jump Clients sur un ou plusieurs ordinateurs distants pour pouvoir y accéder ultérieurement en mode autonome.

> Pour plus d'informations, veuillez consulter Guide Jump Client Privileged Remote Access : Accès sans surveillance aux systèmes de n'importe quel réseau à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/how-to/jump-clients/index.htm.

Groupe de Jump

Dans le menu déroulant, indiquez si vous souhaitez attacher le Jump Client à votre liste personnelle d'éléments de Jump ou à un groupe de Jump partagé avec d'autres utilisateurs. Si vous l'attachez à votre liste personnelle d'éléments de Jump, vous serez le seul à pouvoir accéder à cet ordinateur distant par le biais de ce Jump Client. Si vous l'attachez au groupe de Jump partagé, ce Jump Client deviendra accessible à tous les membres de ce groupe de Jump.

Nom

Saisissez un nom pour le Jump Client.

Certains paramètres de l'assistant de déploiement en masse autorisent le remplacement, et vous permettent donc d'utiliser la ligne de commande pour définir des paramètres spécifiques au déploiement, avant l'installation.

Règle de Jump

Vous pouvez appliquer une règle de Jump à ce Jump Client. Les règles de Jump sont configurées sur la page **Jump > Règles de Jump** et déterminent les périodes pendant lesquelles un utilisateur peut accéder à ce Jump Client. Une règle de Jump peut également envoyer une notification lorsqu'on y accède, ou peut exiger l'approbation pour l'accès. Si aucune règle de Jump n'est appliquée, ce Jump Client est accessible sans restriction.

Type de connexion

Définissez le **type de connexion** sur **Active** ou **Passive** pour les Jump Clients déployés. Un Jump Client actif maintient une connexion continue au serveur, tandis qu'un Jump Client passif détecte les demandes de connexion.

Tenter une installation avec des droits accrus si le client offre cette possibilité

Si l'option **Tenter une installation avec des droits accrus si le client offre cette possibilité** est sélectionnée, le programme d'installation tente de s'exécuter avec les droits d'administration, en installant le Jump Client en tant que service système. Si la tentative d'installation avec des droits accrus échoue ou si cette option est désélectionnée, le programme d'installation s'exécute

avec des droits utilisateur, en installant le Jump Client en tant qu'application. Notez que cette option n'est valable que pour les systèmes d'exploitation Windows et Mac.

> ***Remarque :*** *un Jump Client attaché en mode utilisateur n'est disponible que lorsque cet utilisateur est connecté. À l'inverse, un Jump Client attaché en mode service, avec des droits accrus, permet un accès permanent au système, indépendamment de l'utilisateur connecté.*

L'installeur est valide pour

Le programme d'installation n'est valable que pendant la durée indiquée dans le menu déroulant **L'installeur est valide pour**. N'oubliez pas de laisser suffisamment de temps pour l'installation. En cas de tentative d'exécution de l'installeur de Jump Client une fois ce délai écoulé, l'installation échoue et un nouvel installeur de Jump Client doit être créé. De plus, si l'installateur est exécuté dans le temps imparti mais que le Jump Client n'est pas en mesure de se connecter au serveur durant cet intervalle, le Jump Client se désinstalle, et un nouvel installeur doit être lancé. Le délai de validité peut être défini sur un laps de temps allant de 10 minutes à 1 an. Ce délai n'affecte pas la durée pendant laquelle le Jump Client demeure actif.

En plus d'expirer après la période donnée par l'option **L'installeur est valide pour**, les packages de déploiement en masse de Jump Client deviennent non valides lorsque leur Secure Remote Access Appliance est mis à niveau. La seule exception à cette règle est les mises à jour directes qui modifient le nombre de licences ou leur date d'expiration. Toute autre mise à jour, même si elle ne change pas le numéro de version du serveur, rend non valides les installeurs de Jump Client d'avant la mise à niveau. Si ces installeurs sont des packages MSI, ils peuvent toujours être utilisés pour désinstaller les Jump Clients si nécessaire.

Une fois qu'un Jump Client a été installé, il reste en ligne et actif jusqu'à ce qu'il soit désinstallé du système local par un administrateur connecté, un utilisateur BeyondTrust depuis l'interface de Jump de la console d'accès ou par un script de désinstallation. Un utilisateur BeyondTrust ne peut supprimer un Jump Client que s'il a reçu les autorisations nécessaires de son admin dans l'interface /login.

Commentaires

Ajoutez des **commentaires** qui peuvent s'avérer utiles pour rechercher et identifier des ordinateurs distants. Il est à noter que les Jump Clients déployés avec cet installeur affichent les mêmes commentaires définis au préalable, sauf si vous cochez **Autoriser le remplacement pendant l'installation** et que vous utilisez les paramètres disponibles pour modifier l'installeur pour des installations individuelles.

Règle de session

Choisissez une règle de session à attribuer à ce Jump Client. Les règles de session sont configurées sur la page **Utilisateurs et sécurité > Règles de session**. Une règle de session attribuée à ce Jump Client a la priorité la plus élevée lors de la configuration des autorisations de session.

Proxy de Jumpoint

Si vous avez un ou plusieurs Jumpoints définis comme proxy, vous pouvez sélectionner un Jumpoint comme proxy pour ces connexions de Jump Client. Ainsi, lorsque ces Jump Clients sont installés sur des ordinateurs sans connexion Internet native, ils peuvent utiliser le Jumpoint pour se connecter au Secure Remote Access Appliance. Les Jump Clients doivent être installés sur le même réseau que le Jumpoint sélectionné comme proxy pour les connexions.

Demander des informations d'authentification d'accroissement de droits si nécessaire

Si l'option **Demander des informations d'authentification d'accroissement de droits si nécessaire** est sélectionnée, le programme d'installation invite l'utilisateur à indiquer les informations d'authentification d'un compte d'administration si le système

exige que ces informations d'authentification soient fournies de manière indépendante ; dans le cas contraire, le Jump Client est installé avec des droits d'utilisateur. Notez que cette option ne concerne que les installations avec droits accrus.

Balise

L'ajout d'une **balise** permet d'organiser vos Jump Clients en catégories à l'intérieur de la console d'accès.

Autoriser le remplacement lors de l'installation

Certains paramètres de l'assistant de déploiement en masse autorisent le remplacement, et vous permettent donc d'utiliser la ligne de commande pour définir des paramètres spécifiques au déploiement, avant l'installation.

Aide pour le déploiement en masse

Pour les administrateurs système devant déployer le programme d'installation de Jump Client sur un grand nombre de systèmes, l'exécutable Windows, Mac ou Linux, ou le MSI Windows peut être utilisé avec l'outil de gestion de système de votre choix. Vous pouvez inclure un chemin d'accès personnalisé valide pour le répertoire d'installation du Jump Client.

Vous pouvez également remplacer certains paramètres d'installation en fonction de vos besoins spécifiques. Ces paramètres peuvent être spécifiés pour le MSI et l'EXE en utilisant un outil d'administration système ou l'interface en ligne de commande. Lors de la configuration du remplacement de certaines options d'installation spécifiques pendant l'installation, vous pouvez utiliser les paramètres facultatifs suivants pour modifier l'installeur de Jump Client pour différentes installations. Notez que si un paramètre est passé en ligne de commande mais qu'il n'est pas marqué pour remplacement dans l'interface d'administration /login, l'installation échoue. Dans ce cas, consultez le journal des événements du système d'exploitation à la recherche des erreurs d'installation.

Paramètre de ligne de commande	Valeur	Description
--install-dir	<directory_path>	Spécifie un nouveau répertoire accessible en écriture dans lequel installer le Jump Client. Ce paramètre est pris en charge sur les systèmes Windows et Linux uniquement. En cas de définition d'un répertoire d'installation personnalisé, assurez-vous que ce répertoire n'existe pas déjà et que l'emplacement spécifié est disponible en écriture.
--jc-name	<name...>	Si le remplacement est autorisé, ce paramètre de ligne de commande définit le nom du Jump Client.
--jc-jump-group	utilisateur :<username>groupe de jump :<jumpgroup-code-name>	Si le remplacement est autorisé, ce paramètre de ligne de commande prévaut sur le groupe de Jump défini dans l'assistant de déploiement en masse.
--jc-session-policy	<session-policy-code-name>	Si le remplacement est autorisé, ce paramètre de ligne de commande définit la règle de session de ce Jump Client contrôlant la règle d'autorisation au cours d'une session d'accès.
--jc-jump-policy	<jump-policy-code-name>	Si le remplacement est autorisé, ce paramètre de ligne de commande définit la règle de Jump contrôlant l'accès au Jump Client.
--jc-tag	<tag-name>	Si le remplacement est autorisé, ce paramètre de ligne de commande définit l'étiquette du Jump Client.
--jc-comments	<comments ... >	Si le remplacement est autorisé, ce paramètre de ligne de

		commande définit les commentaires du Jump Client.
--silent		Avec cette commande, l'installeur n'affiche ni fenêtre, ni indicateur de chargement, ni erreur, ni aucune autre alerte visible.

Remarque : *lors du déploiement d'un installeur MSI sous Windows à l'aide de la commande msiexec, les paramètres ci-avant peuvent être spécifiés comme suit :*

1. *Suppression des tirets de début (--)*
2. *Conversion des tirets restants en tirets bas (_)*
3. *Attribution d'une valeur à l'aide du signe égal (=)*

Exemple MSI :

```
msiexec /i bomgar-scc-win32.msi KEY_INFO=w0dc3056g7ff8d1j68ee6wi6dhwzfefggyezh7c40jc90
jc_jump_group=jumpgroup:server_support jc_tag=servers
```

Lors du déploiement d'un installeur EXE, les paramètres ci-dessus peuvent être spécifiés comme suit :

- *Ajout de tirets*
- *Ajout d'une espace entre le paramètre et la valeur*

Exemple EXE :

```
bomgar-scc-[unique id].exe --jc_jump_group=jumpgroup:servers --jc-tag servers
```

Autres règles à prendre en compte :

- ***installdir*** *possède un tiret dans la version EXE, mais aucun dans la version MSI.*
- ***/quiet*** *est utilisé dans la version MSI à la place de* ***--silent*** *dans la version EXE.*

Statistiques des Jump Clients

Un administrateur peut choisir les statistiques à afficher pour tous les Jump Clients à l'échelle du site. Ces statistiques sont affichées dans la console d'accès ; elles comprennent le processeur, l'utilisateur de la console, le taux d'utilisation du disque, une miniature de l'écran distant et le temps de disponibilité.

Mise à niveau

Bande passante maximale pour les mises à niveau simultanées de Jump Client

Vous pouvez réguler la bande passante utilisée lors des mises à jour à l'aide du paramètre **Bande passante maximale pour les mises à niveau de Jump Client simultanées**.

Nombre maximum de mises à niveau de Jump Client simultanées

De même, définissez le nombre maximum de Jump Clients à mettre à jour en même temps. Notez que si vous avez déployé un grand nombre de Jump Clients, il se peut que vous deviez en limiter le nombre pour réguler la quantité de bande passante consommée.

> ***Remarque :*** *Ce paramètre n'affecte pas les mises à niveau de la console d'accès.*

Taux de connexions global pour les Jump Clients

Le paramètre de taux de connexions global est utilisé par les Jump Clients déconnectés comme indice pour savoir comment ils doivent tenter de se reconnecter.

Maintenance

Nombre de jours avant que les Jump Clients non connectés soient effacés automatiquement

Si un Jump Client est déconnecté et ne se reconnecte pas au Secure Remote Access Appliance pendant le nombre de jours spécifié par le paramètre **Nombre de jours avant que les Jump Clients non connectés soient effacés automatiquement**, il sera automatiquement désinstallé de l'ordinateur cible et supprimé de l'interface de Jump dans la console d'accès.

> ***Remarque :*** *ce paramètre est partagé avec le Jump Client en temps normal. Ainsi, même s'il ne parvient pas à communiquer avec le site, il se désinstalle au moment configuré. Si ce paramètre est modifié après qu'un Jump Client se soit déconnecté du serveur, il se désinstallera au moment configuré précédemment.*

Nombre de jours avant que les Jump Clients non connectés soient considérés comme perdus

Si un Jump Client est déconnecté et ne se reconnecte pas au Secure Remote Access Appliance pendant le nombre de jours spécifié par le paramètre **Nombre de jours avant que les Jump Clients non connectés soient effacés automatiquement**, il sera identifié comme perdu dans la console d'accès. Aucune action spécifique n'est effectuée sur le Jump Client à ce moment. Il n'est défini comme étant perdu qu'à des fins d'identification, afin qu'un administrateur puisse diagnostiquer la raison de la perte de connexion et faire le nécessaire pour remédier à la situation.

> ***Remarque :*** *pour vous permettre d'identifier les Jump Clients perdus avant qu'ils soient automatiquement supprimés, ce champ doit contenir un chiffre inférieur au champ de suppression ci-dessus.*

Comportement du Jump Client désinstallé

L'option **Comportement du Jump Client désinstallé** définit comment un Jump Client supprimé par un utilisateur final est géré par la console d'accès. Selon l'option du menu déroulant sélectionnée, l'élément supprimé peut être signalé comme désinstallé et maintenu dans la liste ou, au contraire, être retiré de la liste d'éléments de Jump dans la console d'accès. Si le Jump Client n'est pas en mesure de contacter le Secure Remote Access Appliance lors de l'installation, l'élément affecté se maintient hors ligne.

Divers

Type de connexion par défaut pour Jump Client

Définissez si le type de connexion de Jump Client par défaut doit être actif ou passif.

Port de Jump Client passif

L'option **Port de Jump Client passif** indique le port qu'un Jump Client passif doit utiliser pour détecter une commande de « réveil » émise par le serveur. Le port par défaut est **5832**. Vérifiez que la configuration du pare-feu autorise le trafic entrant sur ce port pour les hôtes présentant des Jump Clients passifs. Une fois activés, les Jump Clients se connectent toujours au serveur via le port 80 ou la sortie 443.

Autoriser l'utilisateur à tenter de réveiller les Jump Clients

Autoriser les utilisateurs à tenter de réveiller les Jump Clients offre un moyen de réveiller un Jump Client spécifique en transmettant des paquets Wake-on-LAN (WOL) par le biais d'un autre Jump Client du même réseau. Après chaque tentative, cette option devient indisponible pendant 30 secondes. Notez que la technologie WOL doit être activée sur l'ordinateur cible et le réseau associé pour que cela fonctionne. Les informations de passerelle par défaut du Jump Client sont utilisées pour déterminer si d'autres Jump Clients résident sur le même réseau. Lors de l'envoi d'un paquet WOL, l'utilisateur dispose d'une option avancée pour fournir un mot de passe pour les environnements WOL nécessitant un mot de passe WOL sécurisé.

Remarque : *les Jumps simultanés peuvent être autorisés ou refusés en configurant un Jump Client dans la section* ***Jump > Éléments de Jump > Paramètres de Jump****. Lorsqu'ils sont autorisés, plusieurs utilisateurs peuvent accéder au même Jump Client sans avoir à être invités à rejoindre une session par un autre utilisateur. Dans le cas contraire, un seul utilisateur à la fois est en mesure d'utiliser un Jump vers un Jump Client. S'il souhaite accéder à la session, un second utilisateur doit obtenir une invitation de la part de l'utilisateur ayant ouvert la session.*

Pour plus d'informations, consultez la section Gérer les paramètres du Jump Client à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/how-to/jump-clients/settings.htm.

Groupes de Jump : Définir les éléments de Jump accessibles aux utilisateurs

Groupes de Jump

Un groupe de Jump est une façon d'organiser les éléments de Jump : on attribue à certains membres un certain niveau d'accès à ces éléments. Les utilisateurs sont associés à des groupes de Jump depuis cette page ou depuis la page **Utilisateurs et sécurité > Règles de groupe**.

Ajouter un nouveau groupe de Jump, modifier, supprimer

Créez un nouveau groupe, modifiez un groupe existant ou supprimez un groupe existant.

Ajouter ou modifier un groupe

Nom

Créez un nom unique permettant d'identifier ce groupe. Ce nom est utile lorsqu'on ajoute des éléments de Jump à un groupe ou lorsqu'on souhaite savoir quels utilisateurs et quelles règles de groupe font partie d'un groupe de Jump.

Nom de code

Définissez également un nom de code, qui sera utilisé à des fins d'intégration. Dans le cas contraire, le système en crée un automatiquement.

Commentaires

Ajoutez une brève description pour résumer la fonction de ce groupe de Jump.

Règles de groupe

Cette option affiche une liste de règles de groupe qui associent des utilisateurs à ce groupe de Jump.

Utilisateurs autorisés

(missing or bad snippet)(missing or bad snippet)

> Pour plus d'informations, veuillez consulter la section Utiliser des groupes de Jump pour définir les éléments de Jump accessibles aux utilisateurs à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/how-to/jumpoint/jump-groups.htm.

Règles de Jump : Définir les plannings, les notifications et les approbations pour les éléments de Jump

Règles de Jump

Les règles de Jump Client sont utilisées pour contrôler à quels moments certains éléments de Jump sont accessibles en mettant en place des calendriers, en envoyant des notifications par e-mail lorsqu'un élément de Jump est en cours d'accès, ou en demandant l'approbation ou la saisie par l'utilisateur d'un ID de système de ticket avant l'accès à un élément de Jump.

Ajouter une nouvelle règle de Jump, modifier, supprimer

Créer une nouvelle règle, modifier ou supprimer une règle existante.

Ajouter ou modifier une règle

Nom affiché

Créez un nom unique permettant d'identifier cette règle. Ce nom doit permettre aux utilisateurs d'identifier cette règle lorsqu'on l'attribue à des éléments de Jump.

Nom de code

Définissez également un nom de code, qui sera utilisé à des fins d'intégration. Dans le cas contraire, le système en crée un automatiquement.

Description

Ajoutez une brève description pour résumer la fonction de cette règle.

Planning de Jump

Activé

Définissez un planning pour déterminer à quel moment l'accès aux éléments de Jump est autorisé selon cette règle. Définissez le fuseau horaire à utiliser pour ce planning, puis ajoutez une ou plusieurs entrées de planification. Pour chaque entrée, indiquez l'heure et la date de début ainsi que l'heure et la date de fin.

Ainsi, si la période commence à 8 h et se termine à 17 h, un utilisateur peut lancer une session à l'aide de cet élément de Jump durant cet intervalle, et il pourra également continuer à travailler après l'heure de fin. Cependant, toute tentative d'accéder à nouveau à cet élément de Jump après 17 heures déclenchera une notification indiquant que le planning ne permet pas à la session de commencer. Si nécessaire, l'utilisateur peut choisir d'outrepasser la restriction du planning et lancer la session malgré tout.

Forcer l'arrêt de la session lorsque le planning ne permet pas l'accès

Si un contrôle d'accès plus strict est requis, cochez **Forcer l'arrêt de la session**. Ceci force la déconnexion de la session à l'heure de fin définie. Dans ce cas, l'utilisateur reçoit des notifications récurrentes à partir de 15 minutes avant d'être déconnecté.

Notification de Jump

Avertir les destinataires en cas de démarrage d'une session

Si cette option est cochée, un e-mail de notification est envoyé aux destinataires désignés lorsqu'une session commence avec un élément de Jump utilisant cette règle de Jump. Lorsqu'un utilisateur tente de lancer une session avec un élément de Jump associé à cette règle, une invite lui indique qu'un e-mail de notification sera envoyé et lui demande s'il souhaite malgré tout démarrer la session.

Avertir les destinataires en cas d'arrêt d'une session

Si cette option est cochée, un e-mail de notification est envoyé aux destinataires désignés lorsqu'une session se termine pour un élément de Jump utilisant cette règle de Jump. Lorsqu'un utilisateur tente de lancer une session avec un élément de Jump associé à cette règle, une invite lui indique qu'un e-mail de notification sera envoyé à la fin de la session et lui demande s'il souhaite malgré tout démarrer la session.

Adresse(s) e-mail

Saisissez une ou plusieurs adresses auxquelles les e-mails doivent être envoyés. Séparez les adresses avec une espace. Cette fonction nécessite une configuration SMTP compatible avec votre serveur, que l'on peut paramétrer sur la page **/login > Gestion > Configuration e-mail**.

Nom affiché

Saisissez le nom du destinataire de l'e-mail. Ce nom apparaît sur l'invite que l'utilisateur reçoit avant une session avec un élément de Jump associé à cette règle.

Paramètres régionaux

Si plus d'une langue est activée sur ce site, sélectionnez la langue dans laquelle envoyer les e-mails.

Approbation de Jump

Exiger un ID de ticket avant le démarrage d'une session

Si cette option est cochée, l'utilisateur doit saisir un ID de ticket valide avant de pouvoir lancer une session d'accès. Lorsqu'un utilisateur tente d'accéder à un point de terminaison avec cette règle de Jump appliquée, l'utilisateur doit saisir un ID de ticket provenant de votre ITSM existant ou du processus d'approbation d'ID de ticket avant que l'accès soit accordé. Configurez l'ITSM ou l'intégration du système de ticket dans la section **Règles de Jump :: Système de ticket**.

Exiger l'approbation pour autoriser le démarrage d'une session

Si cette option est cochée, un e-mail d'approbation est envoyé aux destinataires désignés lorsqu'on essaie de lancer une session avec un élément de Jump utilisant cette règle de Jump. Lorsqu'un utilisateur tente de lancer une session avec un élément de Jump qui utilise cette règle, une invite demande à l'utilisateur de saisir une raison pour la demande et l'heure et la durée pour la demande.

Durée d'accès maximale

Définissez la durée maximale pendant laquelle un utilisateur peut demander l'accès à un élément de Jump utilisant cette règle. L'utilisateur peut demander un accès plus court, mais pas plus long que ce qui est défini ici.

L'approbation d'accès s'applique à

Lorsque l'approbation a été accordée à un élément de Jump, celui-ci devient disponible pour tout utilisateur pouvant le voir et en demander l'accès, ou seulement à l'utilisateur qui a demandé l'accès.

Adresse(s) e-mail

Saisissez une ou plusieurs adresses auxquelles les e-mails doivent être envoyés. Séparez les adresses avec une espace. Cette fonction nécessite une configuration SMTP compatible avec votre serveur, que l'on peut paramétrer sur la page **/login > Gestion > Configuration e-mail**.

Nom affiché

Saisissez le nom du destinataire de l'e-mail. Ce nom apparaît sur l'invite que l'utilisateur reçoit avant une session avec un élément de Jump associé à cette règle.

Paramètres régionaux

Si plus d'une langue est activée sur ce site, sélectionnez la langue dans laquelle envoyer les e-mails.

Désactiver les enregistrements

Désactiver les enregistrements

Si cette option est cochée, les sessions démarrées avec cette règle de Jump ne seront pas enregistrées lorsqu'on active les enregistrements sur la page **Configuration > Options**. Cette option affecte le partage d'écran, les enregistrements d'utilisateur pour le Jump en tunnel par protocole et les enregistrements d'interpréteur de commandes.

Modèle d'e-mail de notification

Objet

Personnalisez l'objet de cet e-mail. Cliquez sur le lien sous le champ **Corps** pour afficher les macros qui peuvent être utilisées pour personnaliser le texte dans vos e-mails selon vos souhaits.

Corps

Personnalisez le texte de cet e-mail. Cliquez sur le lien sous le champ **Corps** pour afficher les macros qui peuvent être utilisées pour personnaliser le texte dans vos e-mails selon vos souhaits.

Modèle d'e-mail d'approbation

Objet

Personnalisez l'objet de cet e-mail. Cliquez sur le lien sous le champ **Corps** pour afficher les macros qui peuvent être utilisées pour personnaliser le texte dans vos e-mails selon vos souhaits.

Corps

Personnalisez le texte de cet e-mail. Cliquez sur le lien sous le champ **Corps** pour afficher les macros qui peuvent être utilisées pour personnaliser le texte dans vos e-mails selon vos souhaits.

Système de ticket

URL du système de ticket

Dans **URL du système de ticket**, saisissez l'URL de votre système de ticket externe. Le Secure Remote Access Appliance envoie une demande sortante à votre système de ticket externe. L'URL doit être formatée pour HTTP ou HTTPS. Si une URL HTTPS est saisie, le certificat du site doit être vérifié pour une connexion valide. Si une règle de Jump nécessitant un ID de ticket existe, l'URL du système de ticket doit être saisie ; sinon, vous recevrez un message d'avertissement.

Transférer un certificat pour les connexions HTTPS

Cliquez sur **Choisir un certificat** pour transférer le certificat pour la connexion du système de ticket HTTPS au serveur. Si votre certificat a été transféré, le serveur l'utilisera lorsqu'il contactera le système externe. Si vous ne transférez pas un certificat et que l'option **Ignorer les erreurs des certificats SSL** ci-dessous est cochée, le Secure Remote Access Appliance aura la possibilité d'utiliser le magasin de certificats intégré lors de l'envoi de la demande.

Invite d'utilisateur

Dans **Invite d'utilisateur**, saisissez le texte de dialogue que vous souhaitez montrer aux utilisateurs de la console d'accès lorsqu'il leur est demandé de saisir l'ID de ticket requis pour l'accès.

Traiter l'ID de ticket comme une information sensible

Si cette case est cochée, l'ID du ticket sera considérée comme confidentielle, et des astérisques seront affichés à la place du texte. Vous devez utiliser une URL en HTTPS pour le système de ticket. Si une adresse en HTTP est saisie, un message d'erreur vous indique qu'il faut utiliser le protocole HTTPS.

Lorsque cette fonction est activée, il est impossible d'ignorer les problèmes liés aux certificats SSL en cochant la case **Ignorer les erreurs des certificats SSL**. Cela signifie que votre certificat SSL doit être valable. Si vous essayez de cocher l'option **Ignorer les erreurs des certificats SSL**, un message vous indique que vous ne pouvez pas ignorer les erreurs de certificat SSL.

Lorsque l'ID du ticket est confidentielle, les règles suivantes s'appliquent :

- Le bureau et les console d'accès Web affichent des astérisques au lieu du texte.
- Le ticket n'est enregistré nulle part par la console d'accès ou sur le serveur.

> Pour plus d'informations, veuillez consulter la section Créer des règles de Jump pour contrôler l'accès aux éléments de Jump à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/how-to/jumpoint/policies.htm.

Ignorer les erreurs des certificats SSL

Si cette option est cochée, le Secure Remote Access Appliance n'inclura **pas** les informations de validation du certificat lorsqu'il contactera le système de ticket externe. Laissez cette case décochée si vous transférez un certificat pour les connexions HTTPS sécurisées.

Rôles d'élément de Jump : créez des groupes d'autorisation pour les éléments de Jump

Rôles d'élément de Jump

(missing or bad snippet)

Ajouter un nouveau rôle d'élément de Jump, modifier, supprimer

Créez un nouveau rôle, modifiez un rôle existant ou supprimez un rôle existant.

Ajouter ou modifier un rôle d'élément de Jump

Nom

Créez un nom unique permettant d'identifier ce rôle. Ce nom est utile lorsqu'on associe un rôle d'élément de Jump à un utilisateur ou à un groupe d'utilisateurs dans un groupe de Jump.

Description

Ajoutez une brève description pour résumer la fonction de ce rôle.

Autorisations

Groupe de Jump ou éléments de Jump personnels

Créer et déployer de nouveaux éléments de Jump

Permet à l'utilisateur de créer des éléments de Jump et de les installer sur des systèmes distants.

Déplacer des éléments de Jump

Permet à l'utilisateur de déplacer des éléments de Jump d'un groupe de Jump à un autre groupe de Jump. Cette autorisation doit être activée sur les deux groupes de Jump.

Supprimer des éléments de Jump existants

Permet à l'utilisateur de supprimer des éléments de Jump.

Élément de Jump

Démarrer les sessions

Permet à l'utilisateur d'effectuer un Jump vers des ordinateurs distants.

Modifier une balise

Permet à l'utilisateur de modifier un champ de balise d'élément de Jump.

Modifier des commentaires

Permet à l'utilisateur de modifier un champ de commentaires d'élément de Jump.

Modifier une règle de Jump

Permet à l'utilisateur de définir, le cas échéant, la règle de Jump à associer à un élément de Jump.

Modifier une règle de session

Permet à l'utilisateur de définir, le cas échéant, la règle de session à associer à un élément de Jump. Toute modification de la règle de session peut affecter les autorisations associées à la session.

Modifier la connectivité et l'authentification

Permet à l'utilisateur de modifier la connexion et les informations d'authentification associées à un élément de Jump, notamment les champs comme le nom d'hôte, le Jumpoint, le port et le nom d'utilisateur, entre autres.

Modifier le comportement et l'expérience

Permet à l'utilisateur de modifier le comportement des éléments de Jump, notamment les champs comme le type de connexion, la taille de l'affichage et le type de terminal, entre autres.

> Pour plus d'informations, veuillez consulter la section Utiliser les rôles d'éléments de Jump pour configurer les groupes d'autorisation des éléments de Jump à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/how-to/jumpoint/jump-item-roles.htm.

Jumpoint : configuration d'un accès autonome à un réseau

Gestion de Jumpoint

La technologie Jump de BeyondTrust permet à un utilisateur d'accéder à des ordinateurs sur un réseau distant sans avoir à préinstaller un logiciel sur chaque machine. Il suffit d'installer un agent Jumpoint unique à n'importe quel endroit du réseau pour pouvoir accéder à chaque ordinateur de ce réseau en mode autonome.

Ajouter un nouveau Jumpoint, modifier, supprimer

Créer un nouveau Jumpoint, modifier ou supprimer un Jumpoint existant.

Redéployer

Désinstaller un Jumpoint existant et télécharger un installeur pour remplacer le Jumpoint existant par un nouveau. Les raccourcis de Jump associés au Jumpoint existant utiliseront le nouveau Jumpoint une fois qu'il est installé.

> ***Remarque :*** *lorsqu'un Jumpoint existant est remplacé, sa configuration n'est pas sauvegardée. Le nouveau Jumpoint doit être reconfiguré.*

Ajouter ou modifier un Jumpoint

Nom

Créez un nom unique permettant d'identifier ce Jumpoint. Ce nom doit aider les utilisateurs à trouver ce Jumpoint lorsqu'ils ont besoin de démarrer une session avec un ordinateur sur le même réseau.

Nom de code

Définissez également un nom de code, qui sera utilisé à des fins d'intégration. Dans le cas contraire, le système en crée un automatiquement.

Commentaires

Ajoutez une brève description pour résumer la fonction de ce Jumpoint. Cette description est utile lorsqu'on gère les Jumpoints.

Désactivé(e)

Si cette option est cochée, ce Jumpoint n'est pas disponible pour établir des connexions de Jump.

En cluster

Si cela est coché, vous pourrez ajouter plusieurs nœuds redondants du même Jumpoint sur différents systèmes hôtes. Ceci garantit que le Jumpoint sera toujours disponible tant qu'au moins un nœud est en ligne.

Activer la méthode de Shell Jump

Si vous souhaitez que les utilisateurs puissent se connecter à des appareils réseau SSH et Telnet à travers ce Jumpoint, cochez la case **Activer la méthode de Shell Jump**. Le filtrage de commandes peut être configuré pour empêcher l'utilisation accidentelle de commandes pouvant endommager les systèmes des points de terminaison.

> Pour plus d'informations sur le filtrage de commandes, veuillez consulter la section Utiliser un Shell Jump pour accéder à un appareil réseau distant à l'adresse www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/shell-jump.htm.

Activer la méthode de Jump en tunnel par protocole

Si l'option **Activer la méthode de Jump en tunnel par protocole** est cochée, les utilisateurs peuvent établir des connexions TCP depuis leurs systèmes vers des points de terminaison distants à travers ce Jumpoint.

Compte de service RDP

Sélectionnez le compte que doit utiliser le Jumpoint pour exécuter un client lancé par l'utilisateur sur le serveur RDP. Ceci vous permet de recueillir des informations supplémentaires sur l'événement depuis une session RDP lancée avec ce Jumpoint. Ce compte est uniquement utilisé sir l'élément de Jump RDP distant est configuré pour activer la fonctionnalité de **Preuves de session**.

> Pour plus d'informations sur la façon de configurer la fonctionnalité de **Preuves de session** dans la console d'accès, veuillez consulter Utiliser RDP pour accéder à un point de terminaison Windows distant à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/rdp.htm.

Règles de groupe

Cette option affiche une liste de règles de groupe permettant aux utilisateurs d'accéder à ce Jumpoint.

Utilisateurs autorisés

Nouveau nom de membre

Lancez une recherche pour ajouter des utilisateurs à ce Jumpoint. Selon leur niveau d'autorisation, les utilisateurs peuvent utiliser ce Jumpoint pour lancer une session ou créer des éléments de Jump se connectant via ce Jumpoint.

Le tableau du bas affiche les utilisateurs des Jumpoints existants. Vous pouvez filtrer la vue en saisissant une chaîne dans la zone de texte **Filtrer par nom**. Vous pouvez aussi supprimer l'utilisateur du Jumpoint.

Pour ajouter un groupe d'utilisateurs à un Jumpoint, consultez **Utilisateurs et sécurité > Règles de groupe** et associez ce groupe à un ou à plusieurs Jumpoints.

Remarque : *il est possible que l'option* ***Supprimer*** *de certains utilisateurs ait été désactivée. Cela arrive lorsqu'on ajoute un utilisateur par le biais d'une règle de groupe.*

Cliquez sur le lien de la règle de groupe pour modifier la règle de façon globale. Les changements apportés à une règle de groupe s'appliquent également à l'ensemble des membres de cette règle de groupe.

Vous pouvez aussi ajouter un utilisateur au Jumpoint, en ignorant ses paramètres tels qu'ils sont définis ailleurs.

Pour plus d'informations sur la configuration de Jumpoint, veuillez consulter Configurer et installer un Jumpoint PRA à l'adresse www.beyondtrust.com/docs/privileged-remote-access/how-to/jumpoint/installation.htm.

Éléments de Jump : Importer en masse des raccourcis de Jump et gérer en masse les paramètres des éléments de Jump

Assistant d'importation en masse de raccourcis de Jump

À travers un Jumpoint, des raccourcis de Jump peuvent être créés pour lancer une session d'accès standard, pour lancer une session en protocole de bureau à distance avec un système Windows, pour effectuer un Jump vers un site Web sur un navigateur distant, pour effectuer un Shell Jump vers un appareil réseau prenant en charge SSH ou Telnet, pour se connecter à un serveur VNC ou pour établir une connexion TCP à travers un Jump en tunnel par protocole.

Lors de la création d'un grand nombre de raccourcis de Jump, il peut être plus aisé de les importer par le biais d'une feuille de calcul plutôt que de les ajouter un par un dans la console d'accès.

> Pour plus d'informations, veuillez consulter la section Utiliser un raccourci de Jump pour effectuer un Jump vers un système distant à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/how-to/jumpoint/jump-shortcuts.htm.

Télécharger un modèle

Dans la liste déroulante de la **section Assistant d'importation en masse de raccourcis de Jump** de l'interface /login, sélectionnez le type d'élément de Jump que vous souhaitez ajouter, puis cliquez sur **Télécharger un modèle**. En utilisant le texte du modèle CSV comme en-têtes de colonnes, ajoutez les informations pour chaque raccourci de Jump que vous voulez importer. Si un champ obligatoire n'a pas été rempli, l'importation échoue. Les champs optionnels peuvent être remplis ou laissés vides.

Importer des raccourcis de Jump

Une fois que vous avez fini de remplir le modèle, utilisez **Importer des raccourcis de Jump** pour transférer le fichier CSV contenant les informations d'éléments de Jump. Vous pouvez transférer un fichier d'une taille maximale de 5 Mo à la fois. Seul un type d'élément de Jump peut être inclus dans chaque fichier CSV. Le fichier CSV doit utiliser le format décrit dans les tableaux ci-dessous.

Raccourci de Jump local

Champ	Description
Nom de l'hôte	Le nom d'hôte du point de terminaison auquel cet élément de Jump doit accéder. Cette chaîne contient 128 caractères au maximum.
Nom	Le nom d'hôte du point de terminaison auquel cet élément de Jump doit accéder. Ce nom identifie l'élément dans les onglets de la session. Cette chaîne contient 128 caractères au maximum.
Groupe de Jump	Le nom de code du groupe de Jump avec lequel cet élément de Jump doit être associé. ***Remarque :*** *lorsqu'on utilise la méthode d'importation, un élément de Jump ne peut pas être associé à une liste personnelle d'éléments de Jump.*
Balise (optionnelle)	Vous pouvez organiser vos éléments de Jump en catégories en ajoutant une balise. Cette chaîne

Champ	Description
	contient 1 024 caractères au maximum.
Commentaires (optionnel)	Vous pouvez ajouter des commentaires à vos éléments de Jump. Cette chaîne contient 1 024 caractères au maximum.
Règle de Jump (optionnelle)	Le nom de code d'une règle de Jump. Vous pouvez spécifier une règle de Jump pour gérer l'accès à cet élément de Jump.
Règle de session (optionnelle)	Le nom de code d'une règle de session. Vous pouvez spécifier une règle de session pour gérer les autorisations disponibles sur cet élément de Jump.
Règle d'accord de point de terminaison (facultative)	La valeur **accepter** accepte automatiquement l'accord de point de terminaison s'il expire et permet à la session de démarrer La valeur **rejeter** rejette automatiquement l'accord de point de terminaison et empêche la session de démarrer. La valeur **aucune demande** n'affiche aucun accord de point de terminaison, même si la fonctionnalité est configurée. Ce champ n'a aucun effet si l'accord de point de terminaison global n'est pas activé. Pour en savoir plus sur le paramétrage global, veuillez consulter Éléments de Jump : Importer en masse des raccourcis de Jump et gérer en masse les paramètres des éléments de Jump à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/jump-items.htm.

Raccourci de Jump distant

Champ	Description
Nom de l'hôte	Le nom d'hôte du point de terminaison auquel cet élément de Jump doit accéder. Cette chaîne contient 128 caractères au maximum.
Jumpoint	Le nom de code du Jumpoint à travers lequel l'on accède au point de terminaison.
Nom	Le nom d'hôte du point de terminaison auquel cet élément de Jump doit accéder. Ce nom identifie l'élément dans les onglets de la session. Cette chaîne contient 128 caractères au maximum.
Groupe de Jump	Le nom de code du groupe de Jump avec lequel cet élément de Jump doit être associé. ***Remarque :*** *lorsqu'on utilise la méthode d'importation, un élément de Jump ne peut pas être associé à une liste personnelle d'éléments de Jump.*
Balise (optionnelle)	Vous pouvez organiser vos éléments de Jump en catégories en ajoutant une balise. Cette chaîne contient 1 024 caractères au maximum.
Commentaires (optionnel)	Vous pouvez ajouter des commentaires à vos éléments de Jump. Cette chaîne contient 1 024 caractères au maximum.
Règle de Jump (optionnelle)	Le nom de code d'une règle de Jump. Vous pouvez spécifier une règle de Jump pour gérer l'accès à cet élément de Jump.
Règle de session (optionnelle)	Le nom de code d'une règle de session. Vous pouvez spécifier une règle de session pour gérer les autorisations disponibles sur cet élément de Jump.
Règle d'accord de point de terminaison	La valeur **accepter** accepte automatiquement l'accord de point de terminaison s'il expire et permet à la session de démarrer La valeur **rejeter** rejette automatiquement l'accord de point de terminaison et

Champ	Description
(facultative)	empêche la session de démarrer. La valeur **aucune demande** n'affiche aucun accord de point de terminaison, même si la fonctionnalité est configurée. Ce champ n'a aucun effet si l'accord de point de terminaison global n'est pas activé. Pour en savoir plus sur le paramétrage global, veuillez consulter Éléments de Jump : Importer en masse des raccourcis de Jump et gérer en masse les paramètres des éléments de Jump à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/jump-items.htm.

Raccourci de Jump VNC distant

Champ	Description
Nom de l'hôte	Le nom d'hôte du point de terminaison auquel cet élément de Jump doit accéder. Cette chaîne contient 128 caractères au maximum.
Jumpoint	Le nom de code du Jumpoint à travers lequel l'on accède au point de terminaison.
Port (optionnel)	Un numéro de port valide entre **100** et **65535**. Sélectionne par défaut **5900**.
Nom	Le nom d'hôte du point de terminaison auquel cet élément de Jump doit accéder. Ce nom identifie l'élément dans les onglets de la session. Cette chaîne contient 128 caractères au maximum.
Groupe de Jump	Le nom de code du groupe de Jump avec lequel cet élément de Jump doit être associé. ***Remarque :*** *lorsqu'on utilise la méthode d'importation, un élément de Jump ne peut pas être associé à une liste personnelle d'éléments de Jump.*
Balise (optionnelle)	Vous pouvez organiser vos éléments de Jump en catégories en ajoutant une balise. Cette chaîne contient 1 024 caractères au maximum.
Commentaires (optionnel)	Vous pouvez ajouter des commentaires à vos éléments de Jump. Cette chaîne contient 1 024 caractères au maximum.
Règle de Jump (optionnelle)	Le nom de code d'une règle de Jump. Vous pouvez spécifier une règle de Jump pour gérer l'accès à cet élément de Jump.

Raccourci de Jump RDP distant

Champ	Description
Nom de l'hôte	Le nom d'hôte du point de terminaison auquel cet élément de Jump doit accéder. Cette chaîne contient 128 caractères au maximum.
Jumpoint	Le nom de code du Jumpoint à travers lequel l'on accède au point de terminaison.
Nom d'utilisateur (optionnel)	Le nom d'utilisateur avec lequel se connecter.
Domaine (optionnel)	Le domaine où se trouve le point de terminaison.
Qualité (optionnelle)	La qualité à laquelle afficher le système distant. Peut être **basse** (niveaux de gris 2 bits pour une

Champ	Description
	consommation de bande passante minimale), **meilleure_perf** (par défaut - couleur 8 bits pour performances rapides), **perf_et_qual** (16 bits pour une qualité d'image et des performances moyennes), **meilleure_qual** (32 bits pour une résolution d'image maximale), ou **video_opt** (codec VP9 pour une vidéo plus fluide). Notez que ce réglage ne peut plus être modifié une fois la session RDP démarrée.
Session de console	**1** : Démarre une session de console. **0** : Démarre nouvelle session (par défaut).
Ignorer un certificat non approuvé (optionnel)	**1** : Ignore les avertissements de certificat. **0** : Affiche un avertissement si le certificat du serveur ne peut pas être vérifié.
Type de SecureApp	La méthode de lancement de SecureApp. Peut -être « none », « remote_app » (pour utiliser la fonctionnalité intégrée d'appli distante de RDP), « remote_desktop_agent » (pour utiliser l'agent d'accès au bureau à distance de BeyondTrust), ou « remote_desktop_agent_credentials » (pour utiliser l'agent d'accès au bureau à distance de BeyondTrust avec injection d'informations d'authentification). Si « remote_desktop_agent » ou « remote_desktop_agent_credentials » sont choisis, alors l'agent d'accès au bureau à distance de BeyondTrust doit être installé sur le système distant.>
Nom de l'appli distante	Le nom du programme d'appli distante. Cette chaîne contient 520 caractères au maximum.
Paramètres de l'appli distante	Une liste de paramètres séparés par des espaces à transmettre à l'appli distante. Les paramètres contenant des espaces peuvent être cités en utilisant des guillemets doubles. Cette chaîne contient 16 000 caractères au maximum.
Paramètres de l'exécutable distant	Une liste séparée par des espaces de paramètres à transmettre à l'exécutable distant qui sera lancé au moyen de l'agent d'accès au bureau à distance de BeyondTrust. Les paramètres contenant des espaces peuvent être cités en utilisant des guillemets doubles. Cela peut seulement être utilisé si le type de SecureApp utilise l'agent d'accès au bureau à distance de BeyondTrust.
Paramètres de l'exécutable distant	Une liste séparée par des espaces de paramètres à transmettre à l'exécutable distant qui sera lancé au moyen de l'agent d'accès au bureau à distance de BeyondTrust. Les paramètres contenant des espaces peuvent être cités en utilisant des guillemets doubles. Cela peut seulement être utilisé si le type de SecureApp utilise l'agent d'accès au bureau à distance de BeyondTrust.
Système cible	Le nom du système cible en cours d'accès par l'application distante. Cette valeur est utilisée pour limiter la liste d'informations d'authentification injectées à celles qui sont valides sur le système cible. Cette valeur peut seulement être utilisée si le type de SecureApp utilise l'agent d'accès au bureau à distance de BeyondTrust avec injection d'informations d'authentification.
Type d'informations d'authentification	Les types d'informations d'authentification qui seront injectées dans l'exécutable distant. Cette valeur dépendra de la banque de mots de passe à partir de laquelle les informations d'authentification seront récupérées. Cette valeur peut seulement être utilisée si le type de SecureApp utilise l'agent d'accès au bureau à distance de BeyondTrust avec injection d'informations d'authentification.
Nom	Le nom d'hôte du point de terminaison auquel cet élément de Jump doit accéder. Ce nom identifie l'élément dans les onglets de la session. Cette chaîne contient 128 caractères au maximum.
Groupe de Jump	Le nom de code du groupe de Jump avec lequel cet élément de Jump doit être associé. ***Remarque :*** *lorsqu'on utilise la méthode d'importation, un élément de Jump ne peut pas être associé à une liste personnelle d'éléments de Jump.*

Champ	Description
Balise (optionnelle)	Vous pouvez organiser vos éléments de Jump en catégories en ajoutant une balise. Cette chaîne contient 1 024 caractères au maximum.
Commentaires (optionnel)	Vous pouvez ajouter des commentaires à vos éléments de Jump. Cette chaîne contient 1 024 caractères au maximum.
Règle de Jump (optionnelle)	Le nom de code d'une règle de Jump. Vous pouvez spécifier une règle de Jump pour gérer l'accès à cet élément de Jump.

Raccourci de Shell Jump

Champ	Description
Nom de l'hôte	Le nom d'hôte du point de terminaison auquel cet élément de Jump doit accéder. Cette chaîne contient 128 caractères au maximum.
Jumpoint	Le nom de code du Jumpoint à travers lequel l'on accède au point de terminaison.
Nom d'utilisateur (optionnel)	Le nom d'utilisateur avec lequel se connecter.
Protocole	Peut être **ssh** ou **telnet**.
Port (optionnel)	Un numéro de port valide entre **1** et **65535**. Se règle par défaut sur **22** si le protocole est **ssh**, ou **23** si le protocole est **Telnet**.
Type de terminal (optionnel)	Peut être **xterm** (par défaut) ou **VT100**.
Persistance (optionnelle)	Le nombre de secondes entre chaque paquet envoyé pour empêcher une session inactive de s'arrêter. Peut être compris entre **0** et **300**. **Zéro** désactive la persistance (réglé par défaut).
Nom	Le nom d'hôte du point de terminaison auquel cet élément de Jump doit accéder. Ce nom identifie l'élément dans les onglets de la session. Cette chaîne contient 128 caractères au maximum.
Groupe de Jump	Le nom de code du groupe de Jump avec lequel cet élément de Jump doit être associé. ***Remarque :*** *lorsqu'on utilise la méthode d'importation, un élément de Jump ne peut pas être associé à une liste personnelle d'éléments de Jump.*
Balise (optionnelle)	Vous pouvez organiser vos éléments de Jump en catégories en ajoutant une balise. Cette chaîne contient 1 024 caractères au maximum.
Commentaires (optionnel)	Vous pouvez ajouter des commentaires à vos éléments de Jump. Cette chaîne contient 1 024 caractères au maximum.
Règle de Jump (optionnelle)	Le nom de code d'une règle de Jump. Vous pouvez spécifier une règle de Jump pour gérer l'accès à cet élément de Jump.
Règle de session (optionnelle)	Le nom de code d'une règle de session. Vous pouvez spécifier une règle de session pour gérer les autorisations disponibles sur cet élément de Jump.

Raccourci de Jump en tunnel par protocole

Champ	Description
Nom de l'hôte	Le nom d'hôte du point de terminaison auquel cet élément de Jump doit accéder. Cette chaîne contient 128 caractères au maximum.
Jumpoint	Le nom de code du Jumpoint à travers lequel l'on accède au point de terminaison.
Tunnels TCP	La liste d'une ou plusieurs définitions de tunnel. Une définition de tunnel est l'association d'un port TCP sur le système de l'utilisateur local à un port TCP sur le point de terminaison distant. Toute connexion établie sur le port local cause la création d'une connexion sur le port distant, permettant aux données de passer par ce tunnel entre le système local et le système distant. Plusieurs associations doivent être séparées par des points-virgules. Exemple : `auto->22;3306->3306` Dans l'exemple ci-dessus, un port local assigné aléatoirement est associé au port distant 22, et le port local 3306 est associé au port distant 3306.
Adresse locale (facultatif)	L'adresse à partir de laquelle la connexion est établie. Il peut s'agir de n'importe quelle adresse dans la sous-plage 127.x.x.x. L'adresse par défaut 127.0.0.1.
Nom	Le nom d'hôte du point de terminaison auquel cet élément de Jump doit accéder. Ce nom identifie l'élément dans les onglets de la session. Cette chaîne contient 128 caractères au maximum.
Groupe de Jump	Le nom de code du groupe de Jump avec lequel cet élément de Jump doit être associé. ***Remarque :*** *lorsqu'on utilise la méthode d'importation, un élément de Jump ne peut pas être associé à une liste personnelle d'éléments de Jump.*
Balise (optionnelle)	Vous pouvez organiser vos éléments de Jump en catégories en ajoutant une balise. Cette chaîne contient 1 024 caractères au maximum.
Commentaires (optionnel)	Vous pouvez ajouter des commentaires à vos éléments de Jump. Cette chaîne contient 1 024 caractères au maximum.
Règle de Jump (optionnelle)	Le nom de code d'une règle de Jump. Vous pouvez spécifier une règle de Jump pour gérer l'accès à cet élément de Jump.

Raccourci de Jump Web

Champ	Description
Nom	Le nom d'hôte du point de terminaison auquel cet élément de Jump doit accéder. Ce nom identifie l'élément dans les onglets de la session. Cette chaîne contient 128 caractères au maximum.
Jumpoint	Le nom de code du Jumpoint à travers lequel l'on accède au point de terminaison.
Groupe de Jump	Le nom de code du groupe de Jump avec lequel cet élément de Jump doit être associé.

Champ	Description
	Remarque : *lorsqu'on utilise la méthode d'importation, un élément de Jump ne peut pas être associé à une liste personnelle d'éléments de Jump.*
Balise (optionnelle)	Vous pouvez organiser vos éléments de Jump en catégories en ajoutant une balise. Cette chaîne contient 1 024 caractères au maximum.
Commentaires (optionnel)	Vous pouvez ajouter des commentaires à vos éléments de Jump. Cette chaîne contient 1 024 caractères au maximum.
Règle de Jump (optionnelle)	Le nom de code d'une règle de Jump. Vous pouvez spécifier une règle de Jump pour gérer l'accès à cet élément de Jump.
Règle de session (optionnelle)	Le nom de code d'une règle de session. Vous pouvez spécifier une règle de session pour gérer les autorisations disponibles sur cet élément de Jump.
URL	L'URL du site Web. L'URL doit commencer par **http** ou **https**.
Vérifier le certificat (facultatif)	**1** : Le certificat du site est validé avant le démarrage de la session. Si des problèmes surviennent, la session ne démarre pas. **0** : Le certificat du site n'est pas validé.
Format du nom d'utilisateur	passthru : transférez le nom d'utilisateur directement depuis le fournisseur d'informations d'authentification. username_only : si le nom d'utilisateur est au format UPN (nom d'utilisateur@domaine) ou DLLN (DOMAINE\nom d'utilisateur), le domaine est supprimé. Seul le nom d'utilisateur est injecté.
Indice de champ de nom d'utilisateur	Un sélecteur de requêtes façon CSS qui identifie le champ de nom d'utilisateur pour accompagner l'injection d'informations d'authentification initiale. Si cette valeur est fournie et qu'aucun élément correspondant n'est trouvé, l'injection d'informations d'authentification échoue.
Indice de champ de mot de passe	Un sélecteur de requêtes façon CSS qui identifie le champ de mot de passe pour accompagner l'injection d'informations d'authentification initiale. Si cette valeur est fournie et qu'aucun élément correspondant n'est trouvé, l'injection d'informations d'authentification échoue.
Indice de bouton d'envoi	Un sélecteur de requêtes façon CSS qui identifie le champ de bouton d'envoi (Soumettre) pour accompagner l'injection d'informations d'authentification initiale. Si cette valeur est fournie et qu'aucun élément correspondant n'est trouvé, l'injection d'informations d'authentification échoue.
Délai d'attente pour l'authentification	La durée pendant laquelle le client Jump Web doit attendre que l'authentification réussisse avant de se déconnecter. Les valeurs valides sont 1, 2, 3, 5, 10, 15, 30

Pour plus d'informations, veuillez consulter la section Utiliser un raccourci de Jump pour effectuer un Jump vers un système distant à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/how-to/jumpoint/jump-shortcuts.htm.

Accord d'utilisateur du point de terminaison

Activer la configuration de consentement de l'utilisateur du point de terminaison pour les éléments de Jump applicables

Activer un menu déroulant dans la console d'accès permettant de configurer les options d'accord de point de terminaison d'utilisateur pour chaque élément de Jump.

Titre

Personnalisez le titre de l'accord. L'utilisateur final voit cela dans la barre de titre de l'invite. Vous pouvez traduire ce texte dans les langues que vous avez activées. Pour revenir au texte par défaut, supprimez le texte du champ puis enregistrez le champ vide.

Texte

Saisissez le texte pour l'accord. Vous pouvez traduire ce texte dans les langues que vous avez activées. Pour revenir au texte par défaut, supprimez le texte du champ puis enregistrez le champ vide.

Délai d'attente d'acceptation

Si l'utilisateur n'accepte pas l'accord pendant le **Délai d'attente d'acceptation**, l'accord est accepté ou rejeté en fonction des propriétés de l'élément de Jump.

Comportement automatique

Choisissez **Acceptation automatique** ou **Refus automatique**. La valeur **Acceptation automatique** accepte automatiquement l'accord de point de terminaison s'il expire et permet à la session de démarrer La valeur **Refus automatique** rejette automatiquement l'accord de point de terminaison et empêche la session de démarrer.

Paramètres d'élément de Jump

Jumps simultanés

Pour : Jump Client, Jump local, Jump distant, VNC distant et Shell Jump.

Définissez cette option sur **Rejoindre une session existante** pour offrir à plusieurs utilisateurs le moyen d'accéder au même élément de Jump sans avoir à être invités à rejoindre une session active par un autre utilisateur. Le premier utilisateur à accéder à cet élément de Jump conserve la propriété de la session. Les utilisateurs dans une session de Jump partagée peuvent se voir et discuter.

Choisissez l'option **Interdire Jump** si vous souhaitez qu'un seul utilisateur à la fois soit en mesure d'effectuer un Jump vers un élément de Jump. S'il souhaite accéder à la session, un second utilisateur doit obtenir une invitation de la part de l'utilisateur ayant ouvert la session.

Ce réglage s'applique aux types d'éléments de Jump suivants : Jump Client, Jump local, Jump distant, VNC distant et Shell Jump.

Pour un RDP distant

Définissez cette option sur **Démarrer une nouvelle session** pour offrir à plusieurs utilisateurs le moyen d'accéder au même élément de Jump sans avoir à être invités à rejoindre une session active par un autre utilisateur. Pour les RDP distants, plusieurs utilisateurs peuvent accéder à un élément de Jump, mais chacun d'entre eux démarre une session indépendante.

Choisissez l'option **Interdire Jump** si vous souhaitez qu'un seul utilisateur à la fois soit en mesure d'effectuer un Jump vers un élément de Jump. S'il souhaite accéder à la session, un second utilisateur doit obtenir une invitation de la part de l'utilisateur ayant ouvert la session.

Ce paramètre ne s'applique qu'aux éléments de Jump de type RDP distant.

Filtrer les Shell Jump

Invites d'interpréteur reconnues

Saisissez des expressions régulières (une par ligne) qui seront comparées aux invites d'interpréteur de commandes sur vos systèmes de points de terminaison. Une expression régulière ne doit tenter de correspondre qu'à la dernière ligne d'une invite de plusieurs lignes.

Validation de correspondance d'invites d'interpréteur

Saisissez l'invite d'interpréteur d'un point de terminaison existant, et le retour indiquera si elle correspond à une expression régulière de la liste. Cette fonction vous permet de tester vos expressions régulières sans lancer de session.

Vault pour Privileged Remote Access

Détection : Détectez des domaines, des comptes et des points de terminaison

BeyondTrust Vault est un magasin d'informations d'authentification sur serveur permettant la détection et l'accès à des informations d'authentification privilégiées. Vous pouvez ajouter manuellement des informations d'authentification privilégiées, ou vous pouvez utiliser l'outil de détection intégré pour scanner et importer les comptes Active Directory et locaux dans BeyondTrust Vault.

> Pour plus d'informations, veuillez consulter le Livre blanc technique de BeyondTrust Vault à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/how-to/vault/index.htm.

Détection de domaine

Avec l'add-on BeyondTrust Vault, vous pouvez détecter les comptes Active Directory, les comptes locaux et les points de terminaison. Les Jumpoints sont utilisés pour scanner les points de terminaison et détecter les comptes associés à ces derniers.

> Pour en savoir plus sur les Jumpoints, veuillez consulter le Guide Jumpoint pour Privileged Remote Access BeyondTrust à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/how-to/jumpoint/index.htm.

Nom de DNS

Saisissez le nom DNS pour votre environnement.

Jumpoint

Choisissez un Jumpoint existant situé dans l'environnement où vous souhaitez détecter des comptes.

Compte de gestion

Sélectionnez le compte de gestion nécessaire au lancement de la tâche de détection. Choisissez d'utiliser un nouveau compte, lequel nécessitera la saisie d'un **nom d'utilisateur**, d'un **mot de passe** et d'une **confirmation du mot de passe**. Ou alors, choisissez d'utiliser un compte existant détecté lors d'une précédente tâche ou ajouté manuellement dans la section **Comptes**. Une fois qu'un compte est sélectionné, cliquez sur **Détection** pour lancer la tâche de détection.

Nom d'utilisateur

Saisissez un nom d'utilisateur valide à utiliser pour la détection (utilisateur@domaine).

Mot de passe

Saisissez un mot de passe valide à utiliser pour la détection.

Confirmer le mot de passe

Saisissez à nouveau le mot de passe pour confirmer.

> ***Remarque :*** *Vous pouvez définir les parties d'un domaine à utiliser pour exécuter une tâche de* ***détection/importation****. Une fois que vous sélectionnez les champs requis pour une* ***tâche de détection****, vous pouvez affiner la recherche en indiquant quelle unité organisationnelle cibler ou en saisissant des requêtes LDAP.*

Tâches de détection

Consultez les tâches de détection en cours pour un domaine spécifique, ou vérifiez les résultats des tâches de détection ayant réussi ou échoué.

Consulter les résultats

Consultez les résultats de la tâche de détection dans la section **Résultats de la détection**, incluant les points de terminaison détectés, les comptes locaux détectés et les comptes de domaine trouvés sur le domaine. Pour chaque élément détecté, un **nom** et une **description** seront fournis. Vous pouvez sélectionner quels points de terminaison et comptes à importer et stocker dans votre instance BeyondTrust Vault. Pour chaque élément de la liste que vous souhaitez importer, cochez la case à proximité et cliquez sur **Importer la sélection**.

Points de terminaison : consultez et gérez les systèmes détectés

Points de terminaison

Consultez les informations sur tous les points de terminaison détectés, telles que le nom et le nom de domaine du système, ainsi que les informations à propos des comptes associés à ces systèmes.

Recherche de points de terminaison

Recherchez un point de terminaison spécifique ou un groupe de points de terminaison sur la base du **nom**, du **nom d'hôte**, de la **description** ou du **nom du Jumpoint**.

Comptes

Consultez le nombre de comptes trouvés pendant la détection ainsi que les points de terminaison qui y sont associés. Cliquez sur l'option **Comptes** pour voir les comptes associés au système.

Modifier

Modifiez les informations du point de terminaison, à savoir le **nom**, la **description** et le **nom d'hôte**.

Supprimer

Supprimez le point de terminaison de la liste des **points de terminaison**.

Comptes : Gérez les comptes privilégiés utilisés sur les points de terminaison

Consultez et gérez les informations de tous les comptes détectés et ajoutés manuellement. Les informations disponibles incluent :

- **Type** : le type de compte, à savoir, si c'est un compte de domaine ou un compte local
- **Nom** : le nom du compte
- **Point de terminaison** : le point de terminaison auquel le compte est associé
- **Description** : Description brève au sujet du compte
- **Dernière extraction** : la dernière fois que le compte a été extrait
- **Âge du mot de passe** : l'âge du mot de passe

Sur la base de cette information, vous pouvez procéder à différentes actions, incluant l'extraction/l'archivage d'informations d'authentification et la rotation d'informations d'authentification.

Comptes

Ajouter un nouveau compte

Cliquez sur **Ajouter un nouveau compte** pour ajouter manuellement un nouveau compte à BeyondTrust Vault.

Chercher des comptes

Recherchez un compte ou groupe de comptes spécifique en fonction du **nom**, du **nom du point de terminaison** ou de la **description**.

Extraction/Archivage

Cliquez sur **Extraction** pour voir et utiliser des informations d'authentification. Lorsque sélectionné, l'invite du **Mot de passe du compte** apparaît, affichant les informations d'authentification pendant 60 secondes pour vous permettre de copier le mot de passe. Une fois l'invite fermée, l'option **Archivage** devient alors disponible. Lorsque vous avez fini d'utiliser le compte, cliquez sur **Archivage** pour archiver à nouveau le mot de passe dans le système.

> Pour plus d'informations, veuillez consulter Extraire des informations d'authentification depuis l'interface /login PRA à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/how-to/vault/check-out.htm.

...

Cliquez sur **...** pour voir plus d'actions, telles que **Rotation du mot de passe**, **Modifier** et **Supprimer**. Lorsque vous sélectionnez **Rotation du mot de passe**, le système procède automatiquement à une rotation ou un changement du mot de passe. Lorsque vous sélectionnez **Modifier**, vous pouvez seulement modifier les informations du compte. L'option **Supprimer** supprime le compte de la liste **Comptes**.

> Pour plus d'informations, veuillez consulter Rotation des informations d'authentification privilégiées avec BeyondTrust Vault à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/how-to/vault/rotation.htm.

Ajouter un compte

L'option **Ajouter un nouveau compte** vous permet d'ajouter des comptes sans avoir à lancer une tâche de détection. Au lieu de cela, vous pouvez saisir manuellement les informations à propos du compte. Cette option est utile dans les situations où un compte partagé ou une combinaison de nom d'utilisateur/mot de passe peut être utilisé pour accéder à de nombreux systèmes différents.

Nom

Saisissez un nom pour le compte.

Description

Saisissez une description brève et facile à mémoriser du compte.

Nom d'utilisateur

Fournissez le nom d'utilisateur du compte.

Authentification

Sélectionnez la méthode d'authentification pour le compte : **Mot de passe** ou **Clé privée SSH**.

> ***Remarque :*** *si vous sélectionnez une clé SSH pour authentification, vous devez fournir une clé privée pour le compte au format OpenSSH. Facultativement, vous pouvez inclure la phrase secrète associée à la clé privée.*

Mot de passe et confirmation du mot de passe

Si la méthode d'authentification sélectionnée est **Mot de passe**, vous devez saisir le mot de passe du compte et le confirmer.

Clé privée SSH

Si la méthode d'authentification **Clé privée SSH** est sélectionnée, vous devez saisir la clé privée SSH du compte.

Clé privée SSH

Fournissez les informations de la clé privée SSH.

Phrase secrète de clé SSH

Si applicable, saisissez la phrase secrète de la clé privée SSH.

Permettre les extractions simultanées

Si le compte peut être extrait et utilisé par de multiples utilisateurs ou sessions à la fois, sélectionnez cette option.

Utilisateurs du compte

Nouveau nom d'utilisateur

Sélectionnez les utilisateurs autorisés à accéder à ce compte puis cliquez sur **Ajouter**.

Nouveau rôle de membre

L'un de ces deux rôles peut être assigné aux utilisateurs :

- **Injecter** (valeur par défaut) : Les utilisateurs dotés de ce rôle peuvent utiliser ce compte dans des sessions Privileged Remote Access.
- **Injecter et extraire** : Les utilisateurs dotés de ce rôle peuvent utiliser ce compte dans des sessions Privileged Remote Access et peuvent extraire le compte sur **/login**. L'autorisation d'**extraction** n'a pas d'effet sur les comptes génériques SSH.

Remarque : *Le* ***rôle de compte Vault*** *est visible dans la liste des utilisateurs ajoutés au compte Vault.*

Remarque : *Lors d'une mise à niveau vers une installation Privileged Remote Access BeyondTrust avec la fonction Extraction configurable du Vault, toutes les* ***appartenances de compte Vault*** *existantes qui étaient configurées dans les règles de groupe avant la mise à niveau verront leur* ***rôle de compte Vault*** *défini par défaut sur* ***Injecter et extraire*** *après la mise à niveau.*

IMPORTANT !

Prévalence des rôles de compte Vault *: Les rôles de compte Vault peuvent être assignés à la fois aux utilisateurs et aux règles de groupe. Cela signifie qu'un même utilisateur peut avoir différents rôles pour un seul compte Vault. Un rôle peut être assigné par les règles de groupe de l'utilisateur, tandis qu'un autre peut l'être en vertu de l'accès explicite de l'utilisateur au compte Vault. Dans de tels cas, le système utilise le rôle le plus spécifique pour cet utilisateur. Par conséquent, le système autorisera le rôle assigné par la page* ***Modifier le compte Vault*** *à outrepasser le rôle assigné par la règle de groupe de l'utilisateur. Lorsque le rôle est remplacé de cette manière, le mot outrepassé apparaît sur la page* ***Modifier le compte Vault*** *en ce qui concerne les règles de groupe associées à l'utilisateur. Ce comportement est conforme avec l'ordre de prévalence pour les rôles d'élément de Jump.*

Remarque : *les comptes utilisateur avec la permission* ***Autorisé à administrer Vault*** *sont implicitement autorisés à accéder à tous les comptes Vault.*

Modifier un compte local

Nom

Consultez ou modifiez le nom utilisé pour le compte.

Description

Consultez ou modifiez la description du compte.

Nom d'utilisateur

Consultez le nom d'utilisateur associé au compte.

Mot de passe

Saisissez un nouveau mot de passe pour le compte, ou laissez le champ vide pour conserver le mot de passe existant. Confirmez le mot de passe saisi.

Âge du mot de passe

Consultez l'âge du mot de passe existant.

Rotation automatique des informations d'authentification

Définir des comptes locaux pour une rotation automatique après utilisation

Permettre les extractions simultanées

Si le compte peut être extrait et utilisé par de multiples utilisateurs ou sessions à la fois, sélectionnez cette option.

Nom du point de terminaison

Consultez quels points de terminaison sont associés au compte.

Nom d'hôte du point de terminaison

Consultez le nom d'hôte des points de terminaison associés.

Utilisateurs du compte

Sélectionnez les utilisateurs autorisés à accéder à ce compte puis cliquez sur **Ajouter**.

> ***Remarque :*** *les comptes utilisateur avec la permission* ***Autorisé à administrer Vault*** *sont implicitement autorisés à accéder à tous les comptes Vault.*

Modifier un compte de domaine

Nom

Consultez ou modifiez le nom utilisé pour le compte.

Description

Consultez ou modifiez la description du compte.

Nom d'utilisateur

Consultez le nom d'utilisateur associé au compte.

Mot de passe

Saisissez un nouveau mot de passe pour le compte, ou laissez le champ vide pour conserver le mot de passe existant. Confirmez le mot de passe saisi.

Âge du mot de passe

Consultez l'âge du mot de passe existant.

Rotation automatique des informations d'authentification

Si vous souhaitez qu'une rotation des informations d'authentification ait lieu de façon automatique après archivage, sélectionnez cette option.

Permettre les extractions simultanées

Si le compte peut être extrait et utilisé par de multiples utilisateurs ou sessions à la fois, sélectionnez cette option.

Nom unique

Consultez le nom unique du compte.

Utilisateurs du compte

Sélectionnez les utilisateurs autorisés à accéder à ce compte puis cliquez sur **Ajouter**.

> ***Remarque :*** *les comptes utilisateur avec la permission* ***Autorisé à administrer Vault*** *sont implicitement autorisés à accéder à tous les comptes Vault.*

Domaines : Ajoutez ou gérez des domaines

Ajoutez, consultez et gérez des informations à propos de vos domaines.

Domaines

Ajouter un domaine

Cliquez sur **Ajouter** pour ajouter manuellement un nouveau domaine à la liste des **domaines**.

Nom de domaine

Consultez le nom du domaine.

Jumpoint

Consultez le Jumpoint utilisé pour détecter des comptes et points de terminaison sur le domaine.

Compte de gestion

Consultez le compte de gestion associé au Jumpoint et au domaine.

Détecter

Cliquez sur **Détecter** pour que le Jumpoint commence à scanner et détecter des points de terminaison et des comptes sur le domaine.

Modifier

Cliquez sur **Modifier** pour modifier les informations du domaine.

Supprimer

Cliquez sur **Supprimer** pour supprimer ce domaine de la liste des **domaines**.

Ajouter un domaine

Nom DNS

Saisissez le **nom DNS** du domaine.

Jumpoint

Choisissez un Jumpoint existant situé dans l'environnement où vous souhaitez détecter des comptes.

Compte de gestion

Sélectionnez le compte de gestion nécessaire au lancement de la tâche de détection pour ce domaine. Choisissez d'utiliser un nouveau compte, lequel nécessitera un **nom d'utilisateur**, un **mot de passe** et une **confirmation du mot de passe**. Ou alors, choisissez d'utiliser un compte existant détecté lors d'une précédente tâche ou ajouté manuellement dans la section **Comptes**.

Modifier le domaine

Nom DNS

Consultez ou modifiez le **nom DNS** du domaine.

Jumpoint

Consultez ou modifiez les informations du Jumpoint du domaine.

Compte de gestion

Consultez ou modifiez le compte de gestion nécessaire au lancement de la tâche de détection pour ce domaine. Choisissez d'utiliser un nouveau compte, lequel nécessitera un **nom d'utilisateur**, un **mot de passe** et une **confirmation du mot de passe**. Ou alors, choisissez d'utiliser un compte existant détecté lors d'une précédente tâche ou ajouté manuellement dans la section **Comptes**.

Console d'accès

Paramètres de la console d'accès : gérez les paramètres par défaut de la console d'accès

Gestion des paramètres de la Console d'Accès

Vous pouvez configurer les paramètres par défaut de la console d'accès pour l'ensemble de votre base d'utilisateurs, afin d'obtenir une expérience utilisateur de console d'accès homogène et d'augmenter l'efficacité de votre équipe. Vous pouvez forcer des paramètres, permettre aux utilisateurs de les outrepasser, ou ne pas les gérer. Si vous sélectionnez **Non gérés**, la configuration BeyondTrust par défaut s'affiche à des fins d'examen.

Chaque paramètre d'**activation** et de **désactivation** inclut une option d'administration permettant l'application forcée du paramètre. Les paramètres forcés prennent effet lors de la prochaine connexion de l'utilisateur et ne permettent pas la configuration dans la console. Un paramètre forcé ne peut pas être outrepassé, sauf si un administrateur décoche l'option **Forcé** pour ce paramètre dans l'interface d'administration /login.

> Pour plus de détails sur la façon dont un utilisateur peut configurer des paramètres dans la console d'accès selon ses besoins, reportez-vous à Changer les paramètres et préférences dans la console d'accès à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/settings.htm.

Choisissez les paramètres par défaut pour vos utilisateurs, puis cliquez sur le bouton **Enregistrer** en haut de la page.

Notez que les paramètres enregistrés ne prennent effet qu'à la connexion à la console. Même si vous enregistrez et appliquez les modifications avec le bouton **Appliquer maintenant** situé en bas de page (voir plus loin), l'utilisateur n'utilisera les nouveaux paramètres qu'après connexion.

Si, par exemple, vous souhaitez définir des paramètres par défaut pour les nouveaux utilisateurs tout en conservant les paramètres définis pour les utilisateurs existants, enregistrez vos paramètres gérés sans les appliquer. De cette manière, toutes les nouvelles connexions à la console d'accès démarreront avec vos paramètres gérés par défaut. Les paramètres forcés seront appliqués aux utilisateurs existants à la prochaine connexion, mais tous les autres paramètres resteront identiques.

Paramètres globaux

Correcteur orthographique activé

Dans la section **Paramètres globaux**, vous pouvez choisir d'activer ou de désactiver le correcteur orthographique pour la messagerie instantanée. Le correcteur est actuellement disponible en anglais US uniquement.

Barre latérale de session configurable

Choisissez si vous souhaitez que l'icône de menu de session soit affichée, si la barre latérale peut être détachée, et si les widgets de la barre latérale de session peuvent être réorganisés et redimensionnés.

Alertes - Alertes de la messagerie instantanée

Alertes sonores - Émettre un signal sonore lors de la réception d'un message instantané

Choisissez si une alerte sonore doit retentir lorsque l'utilisateur reçoit un message instantané. Si cela n'est pas géré, ou si cela est activé mais non forcé, l'utilisateur peut désigner un son personnalisé au format WAV de 1 Mo maximum.

Alertes visuelles - Faire clignoter l'icône de l'application lors de la réception d'un message instantané

Choisissez si l'icône de l'application doit clignoter lorsque l'utilisateur reçoit un message instantané.

Afficher les messages d'état dans les fenêtres de messagerie instantanée des équipes

Choisissez si la messagerie instantanée de l'équipe doit inclure les messages de statut, comme la connexion et déconnexion des utilisateurs, ou seulement les messages instantanés entre les membres de l'équipe.

Notifications contextuelles

Messagerie instantanée de l'équipe

Choisissez si un utilisateur doit recevoir un avertissement contextuel pour les messages instantanés reçus dans une messagerie instantanée d'équipe.

Session d'accèss

Choisissez si un utilisateur doit recevoir un avertissement contextuel pour les messages instantanés reçus dans une session d'accès

Alertes - Alertes de la file d'attente

Alertes sonores - Émettre un signal sonore lors de l'ajout d'une session dans une file d'attente

Choisissez si une alerte sonore doit retentir lorsqu'une session arrive dans une des files d'attente d'un utilisateur.

Notifications contextuelles

Les notifications contextuelles s'affichent indépendamment de la console d'accès et par-dessus les autres fenêtres. Si les notifications contextuelles sont activées mais non forcées ou laissées non gérées, l'utilisateur pourra choisir la façon dont il reçoit des notifications.

File d'attente personnelle - Sessions partagées

Choisissez si un utilisateur doit recevoir une notification contextuelle pour les sessions partagées dans cette file d'attente.

Messagerie instantanée de l'équipe - Sessions partagées

Choisissez si un utilisateur doit recevoir une notification contextuelle pour les sessions partagées dans cette file d'attente.

Comportement contextuel - Emplacement et durée

Définissez l'emplacement et la durée par défaut des avertissements contextuels.

Session d'accèss

Demander automatiquement le partage d'écran

Déterminez si vous souhaitez que les sessions de vos utilisateurs commencent par un partage d'écran.

Détacher automatiquement

Choisissez si vous souhaitez que les sessions s'ouvrent sous forme d'onglets dans la console d'accès ou détacher les sessions automatiquement dans de nouvelles fenêtres.

Qualité par défaut

Définissez la qualité par défaut pour les sessions de partage d'écran.

Échelle par défaut

Définissez la taille d'écran par défaut pour les sessions de partage d'écran.

Passer automatiquement en mode plein écran au démarrage du partage d'écran

L'utilisateur peut passer automatiquement en mode plein écran au démarrage du partage d'écran.

Restreindre automatiquement la visibilité du point de terminaison lors du démarrage du partage d'écran

Au lancement du partage d'écran, le système distant peut voir son affichage et ses entrées à la souris et au clavier automatiquement restreints, fournissant un écran de confidentialité.

Interpréteur de commandes

Nombre de lignes d'historique de commande disponible

Vous pouvez définir le nombre de lignes à enregistrer dans l'historique de l'interpréteur de commandes. La valeur par défaut est de 500 lignes.

Enregistrer

Cliquez sur **Enregistrer** pour enregistrer tous les paramètres configurés. Le message de confirmation « **Le profil de paramètres a été enregistré.** » s'affiche alors dans le haut de la page. Tous les utilisateurs se connectant à la console d'accès après que vous avez enregistré un nouveau profil recevront les nouveaux paramètres en tant que paramètres par défaut.

Appliquer les paramètres Console d'Accès

Appliquer maintenant

Pour appliquer les paramètres par défaut à l'ensemble de votre base d'utilisateurs, cliquez sur **Appliquer maintenant**. Le message de confirmation « **Le profil de paramètres a été appliqué.** » s'affiche alors dans le haut de la page.

Suite à l'application de nouveaux paramètres pour votre base d'utilisateurs, ceux-ci recevront une alerte de confirmation lors de leur première connexion à la console d'accès après que vous avez appliqué les paramètres. Cette alerte leur indique que leurs paramètres ont été modifiés et leur permet uniquement d'accuser réception de l'alerte ou d'ouvrir leur fenêtre de paramètres de console d'accès pour voir les changements.

Liens personnalisés : Ajouter des raccourcis d'URL à la Console d'Accès

Liens personnalisés

Créer des liens vers des sites auxquels vos utilisateurs peuvent accéder lors des sessions. Par exemple un lien vers une base de connaissances pouvant faire l'objet d'une recherche, donner aux utilisateurs la possibilité de rechercher une solution au problème sur le système du point de terminaison, ou un système de gestion de la relation client (GRC).

Les liens créés ici deviennent disponibles par le bouton **Liens** de la console d'accès.

Ajouter un lien personnalisé, modifier, supprimer

Créer un nouveau lien, modifier ou supprimer un lien existant.

Ajouter ou modifier un lien existant

Nom

Créez un nom unique permettant d'identifier ce lien.

URL

Ajoutez l'URL vers laquelle ce lien personnalisé doit renvoyer. Cliquez sur le lien sous le champ **Corps** pour afficher les macros qui peuvent être utilisées pour personnaliser le texte dans vos e-mails selon vos souhaits.

> Pour plus d'informations, veuillez consulter la section Vue d'ensemble de session d'accès et outils à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/session-overview.htm.

Scripts prédéfinis : création de scripts pour le partage d'écran ou les sessions d'interpréteur de commandes

Scripts prédéfinis

Créez des scripts personnalisés à utiliser pour le partage d'écran et des sessions d'interpréteur de commandes. Le script s'affiche dans l'interface du partage d'écran ou de l'interpréteur de commandes lors de son exécution. L'exécution d'un script dans l'interface de partage d'écran affichera le script en cours d'exécution sur l'écran distant.

> Pour plus d'informations, veuillez consulter la section Vue d'ensemble de session d'accès et outils à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/session-overview.htm.

> Pour plus d'informations, veuillez consulter la section Ouvrir l'interpréteur de commandes sur le point de terminaison distant en utilisant la Console d'Accès à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/command-shell.htm.

Disponibilité d'équipe et filtres de catégorie

Filtrez votre affichage en sélectionnant une catégorie ou une équipe dans les listes déroulantes.

Ajouter un nouveau script prédéfini, modifier, supprimer

Créer un nouveau script, modifier ou supprimer un script existant.

Ajouter ou modifier un script prédéfini

Nom du script

Créez un nom unique permettant d'identifier ce script. Ce nom doit aider les utilisateurs à trouver le script qu'ils souhaitent exécuter.

Description

Ajoutez une brève description pour résumer la fonction de ce script. Cette description s'affiche à l'invite pour confirmer que l'utilisateur souhaite exécuter le script sélectionné.

Séquence de commande

Écrivez la séquence de commandes. Les scripts doivent être rédigés au format ligne de commande, comme pour la rédaction d'un fichier de lot ou d'un script d'interpréteur. Remarquez que seule la dernière ligne du script peut être interactive ; vous ne pouvez pas demander de saisie au milieu du script.

Dans le script lui-même, référencez un fichier de ressources associé à l'aide de **%RESOURCE_FILE%** en veillant à insérer les guillemets. Remarque : la séquence de commandes est sensible à la casse.

Vous pouvez accéder au répertoire temporaire du fichier de ressources à l'aide de **%RESOURCE_DIR%**. Lorsque vous exécutez un script avec un fichier de ressources associé, celui-ci est temporairement chargé sur l'ordinateur de l'utilisateur.

Disponibilité d'équipe

Sélectionnez les équipes qui doivent pouvoir utiliser cet élément.

Catégories

Sélectionnez la catégorie dans laquelle répertorier cet objet.

Fichier de ressources

Vous pouvez sélectionner un fichier de ressources à associer à ce script.

Catégories

Ajouter une catégorie, supprimer

Créer une nouvelle catégorie ou supprimer une catégorie existante.

Ressources

Choisir et transférer une ressource

Ajoutez les fichiers de ressources auxquels vous souhaitez avoir accès dans vos scripts. Vous pouvez transférer jusqu'à 100 Mo dans votre répertoire du fichier de ressources.

Supprimer

Supprimez un fichier de ressources existant.

Actions spéciales : création d'actions spéciales personnalisées

Actions spéciales

Créez des actions spéciales afin d'accélérer vos processus. Notez qu'il est possible de créer des actions spéciales pour les systèmes Windows, Mac et Linux.

Ajouter une action spéciale, modifier, supprimer

Créer une nouvelle action spéciale, modifier ou supprimer une action spéciale existante.

Ajouter ou modifier une action spéciale

Nom de l'action

Créez un nom unique permettant d'identifier cette action. Au cours d'une session, un utilisateur peut voir ce nom dans le menu déroulant d'actions spéciales.

Commande

Dans le champ **Commande**, entrez le chemin d'accès complet de l'application à exécuter. N'utilisez pas de guillemets, le système les ajoute automatiquement. Les systèmes Windows peuvent utiliser les macros prédéfinies. Si la commande n'est pas trouvable sur le système distant, cette action spéciale personnalisée n'apparaîtra pas dans la liste d'actions spéciales de l'utilisateur.

Arguments

Si la commande fournie accepte les arguments en ligne de commande, vous pourrez les ajouter ensuite. Les arguments peuvent utiliser des guillemets si nécessaire, et les arguments des systèmes Windows peuvent utiliser les macros prédéfinies.

> Pour plus d'informations sur les arguments Windows, recherchez « commutateurs de ligne de commande » sur le site Web docs.microsoft.com.

Confirmer

Si vous cochez la case **Confirmer**, les utilisateurs seront invités à confirmer qu'ils veulent exécuter cette action spéciale avant qu'elle se lance. Dans le cas contraire, la sélection de cette action spéciale dans le menu au cours d'une session entraîne son exécution immédiate.

Paramètres des actions spéciales

Afficher les actions spéciales préexistantes

Si vous souhaitez activer les actions spéciales par défaut fournies par BeyondTrust, cochez la case **Afficher les actions spéciales préexistantes**. Si vous ne souhaitez activer que vos actions spéciales personnalisées, décochez-la.

> ***Remarque :*** *l'action spéciale* ***Sécurité de Windows (Ctrl-Alt-Suppr)*** *ne peut pas être désactivée.*

Utilisateurs et sécurité

Utilisateurs : Ajouter des autorisations de compte pour un utilisateur ou un administrateur

Comptes utilisateurs

Affichez les informations sur tous les utilisateurs qui ont accès à votre Secure Remote Access Appliance, y compris les utilisateurs locaux et ceux qui y ont accès par l'intégration du fournisseur de sécurité.

Ajouter un utilisateur, modifier, supprimer

Créer un nouveau compte, modifier un compte existant, ou supprimer un compte existant. Vous ne pouvez pas supprimer votre propre compte.

Chercher des utilisateurs

Recherchez le compte d'un utilisateur à partir du nom d'utilisateur, du nom affiché ou de l'adresse e-mail.

Fournisseur de sécurité

Sélectionnez un type de fournisseur de sécurité depuis le menu déroulant pour filtrer la liste des utilisateurs par fournisseur de sécurité.

Synchroniser

Synchronisez les utilisateurs et les groupes associés avec un fournisseur de sécurité externe. La synchronisation se produit automatiquement une fois par jour. Cliquer sur ce bouton force une synchronisation manuelle.

Réinitialiser des échecs de connexion et déverrouiller un compte

Si un utilisateur échoue une ou plusieurs fois à se connecter, cliquez sur le bouton **Réinitialiser** pour son compte d'utilisateur afin de remettre le chiffre à 0.

Si un utilisateur se retrouve bloqué après un trop grand nombre d'échecs de connexion consécuritfs, cliquez sur le bouton **Déverrouiller le compte** pour que le compteur de son compte d'utilisateur soit remis à 0 et débloquer son compte.

Ajouter ou modifier un utilisateur

Nom d'utilisateur

Identificateur unique servant à vous connecter.

Nom affiché

Le nom d'utilisateur tel qu'affiché dans les discussions d'équipe, les rapports, etc.

Adresse e-mail

Définissez une adresse e-mail où envoyer les notifications, comme les réinitialisations de mot de passe ou le mode Disponibilité étendue.

Mot de passe

Le mot de passe utilisé avec le nom d'utilisateur pour la connexion. Vous pouvez définir le mot de passe de votre choix, tant que la chaîne reste conforme à la règle définie sur la page **/login > Gestion > Sécurité**.

Doit changer son mot de passe lors de la prochaine connexion

Si cette option est sélectionnée, l'utilisateur doit réinitialiser son mot de passe lors de sa prochaine connexion.

Le mot de passe n'expire jamais

Cochez cette case pour que le mot de passe de l'utilisateur n'expire jamais.

Date d'expiration du mot de passe

Saisissez une date pour l'expiration du mot de passe.

Composition

> ***Remarque :*** *dans un premier temps, la section* ***Appartenance*** *ne s'affiche pas lors de la création d'un nouvel utilisateur. Après l'enregistrement d'un nouvel utilisateur, une nouvelle section* ***Appartenance*** *affiche les règles de groupe ou les équipes auxquelles l'utilisateur a été associé.*

Membres associés à la règle de groupe

Liste des règles de groupe associées à l'utilisateur.

Appartenance à des équipes

Liste des équipes auxquelles l'utilisateur appartient.

Appartenance à un Jumpoint

Liste des Jumpoints auxquels l'utilisateur peut accéder.

Appartenances de groupe de Jump

Liste des groupes de Jump auxquels l'utilisateur appartient.

Paramètres du compte

Authentification à deux facteurs

L'authentification à deux facteurs (2FA) fait appel à une application d'authentification pour créer un code unique limité dans le temps et se connecter à l'interface d'administration et à la console d'accès. Lorsque **Requis** est sélectionné, l'utilisateur est invité à s'inscrire et à se servir de l'authentification 2FA à sa prochaine connexion. Lorsque **Optionnel** est sélectionné, l'utilisateur a la possibilité d'utiliser l'authentification 2FA, mais il n'y est pas contraint. **Cliquez sur Supprimer l'appli d'authentification actuelle** lorsque vous souhaitez qu'un utilisateur ne se connecte plus par le biais d'une appli d'authentification donnée.

> ***Remarque :*** *Les utilisateurs qui se connectaient à l'aide de codes obtenus par e-mail passent automatiquement à l'authentification 2FA. Ils ont toutefois la possibilité d'utiliser des codes e-mail jusqu'à ce qu'ils soient inscrits sur une application. Après une première utilisation de 2FA, l'option du code e-mail n'est plus disponible.*

Le compte n'expire jamais

Lorsque cette case est cochée, le compte n'expire jamais. Lorsque cette case n'est pas cochée, une date d'expiration du compte doit être définie.

Date d'expiration du compte

Avec ceci, le compte expirera après une date donnée.

Activation du compte

Vous permet de désactiver le compte pour que l'utilisateur ne puisse plus se connecter. Une désactivation ne supprime PAS le compte.

Commentaires

Ajoutez des commentaires pour aider à identifier la fonction de cet objet.

Autorisations générales

Administration

Privilèges administratifs

Accorde des droits d'administration complets à l'utilisateur.

Autorisé à administrer Vault

Autorise l'accès de l'utilisateur à Vault.

Paramètres de mot de passe

Permet à l'utilisateur de définir des mots de passe et de débloquer des comptes pour les utilisateurs locaux ne disposant pas de droits d'administrateur.

Modification d'un Jumpoint

Permet à l'utilisateur de créer ou de modifier des Jumpoints. Cette option n'affecte pas la capacité de l'utilisateur à accéder à des ordinateurs distants via un Jumpoint, qui est configurée par Jumpoint ou règle de groupe.

Modification d'équipe

Permet à l'utilisateur de créer ou de modifier des équipes.

Modification d'un groupe de Jump

Permet à l'utilisateur de créer ou de modifier les groupe de Jump.

Modification de script prédéfini

Permet à l'utilisateur de créer ou de modifier des scripts prédéfinis en vue de les utiliser dans des sessions de partage d'écran ou d'interpréteur de commandes.

Modification de lien personnalisé

Permet à l'utilisateur de créer ou de modifier des liens personnalisés.

Autorisé à consulter les rapports sur les sessions d'accès

Permet à l'utilisateur d'établir des rapports sur l'activité des session d'accès, en visualisant uniquement les sessions pour lesquelles il était le propriétaire principal de la session, uniquement les sessions pour les points de terminaison appartenant à un groupe de Jump dont l'utilisateur est membre, ou toutes les sessions.

Autorisé à voir les enregistrements de session d'accès

Permet à l'utilisateur de lire les enregistrements vidéo des sessions de partage d'écran et des sessions d'interpréteur de commandes.

Autorisé à consulter les rapports Vault

Permet à l'utilisateur de consulter ses propres événements Vault ou tous les événements Vault.

Autorisations d'accès

Accès

Autorisé à accéder aux points de terminaison

Permet à l'utilisateur d'utiliser la console d'accès pour exécuter des sessions. Si l'accès au point de terminaison est activé, les options relatives à l'accès au point de terminaison seront également disponibles.

Gestion de session

Autorisé à partager les sessions avec des équipes auxquelles il n'appartient pas

Permet à l'utilisateur d'inviter un ensemble moins limité d'utilisateurs pour partager des sessions, pas seulement des membres de son équipe. Combinée à la permission de disponibilité étendue, cette permission développe les capacités de partage de session.

> Pour plus d'informations, veuillez consulter la section Contrôler le point de terminaison à distance avec partage d'écran à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/screen-sharing.htm.

Autorisé à inviter des utilisateurs externes

Permet à l'utilisateur d'inviter un utilisateur tiers à participer à une session de manière ponctuelle.

> Pour plus d'informations, veuillez consulter la section Inviter un utilisateur externe à rejoindre une session d'accès à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/access-invite.htm.

Autorisé à activer le mode disponibilité étendue

Permet à l'utilisateur de recevoir des invitations par e-mail de la part d'autres utilisateurs demandant de partager une session, même lorsqu'il n'est pas connecté à la console d'accès.

> Pour plus d'informations, consultez la section Utiliser la disponibilité étendue pour rester accessible lorsque vous n'êtes pas connecté à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/extended-availability.htm.

Autorisé à modifier la clé externe

Permet à l'utilisateur de modifier la clé externe depuis le volet d'informations d'une session dans la console d'accès.

> Pour plus d'informations, veuillez consulter la section Vue d'ensemble de session d'accès et outils à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/session-overview.htm.

Partage d'écran d'utilisateur à utilisateur

Pour plus d'informations, veuillez consulter Partager votre écran avec un autre utilisateur à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/user-screensharing.htm.

Autorisé à montrer son écran aux autres utilisateurs

Permet à l'utilisateur de partager son écran avec un autre utilisateur sans que l'utilisateur récepteur ait besoin de rejoindre une session. Cette option est disponible même si l'utilisateur n'est pas dans une session.

Autorisé à accorder le contrôle lorsqu'il montre son écran à d'autres utilisateurs

Permet à l'utilisateur partageant son écran d'accorder le contrôle de son clavier et de sa souris à l'utilisateur regardant son écran.

Technologie Jump

Méthodes d'élément de Jump autorisées

Permet à l'utilisateur d'effectuer un Jump vers des ordinateurs en utilisant les **Jump Clients**, les **Jump locaux sur le réseau local**, les **Jump distants avec un Jumpoint**, les **VNC distants avec un Jumpoint**, les **RDP distants avec un Jumpoint**, les **Jump Web avec un Jumpoint**, les **Shell Jump avec un Jumpoint** et les **Jump en tunnel par protocole avec un Jumpoint**.

Rôles d'élément de Jump

Le rôle d'élément de Jump est un ensemble prédéfini d'autorisations relatives à la gestion et à l'utilisation d'un élément de Jump. Pour chaque paramètre, cliquez sur **Afficher** pour ouvrir le rôle d'élément de Jump dans un nouvel onglet.

Le rôle **Par défaut** n'est utilisé que lorsque **Utiliser les paramètres par défaut de l'utilisateur** est défini pour cet utilisateur dans un groupe de Jump.

Le rôle **Personnel** ne s'applique qu'aux éléments de Jump attachés à la liste personnelle d'éléments de Jump d'un utilisateur.

Le rôle **Équipe** ne s'applique qu'aux éléments de Jump attachés à la liste personnelle d'éléments de Jump d'un membre de l'équipe doté d'un rôle inférieur. Ainsi, un chef d'équipe peut visualiser les éléments de Jump d'un responsable ou d'un membre de son équipe, et un responsable d'équipe peut visualiser les éléments de Jump personnels d'un membre de son équipe.

Le rôle **Système** s'applique au reste des éléments de Jump du système. Pour la plupart des utilisateurs, ce rôle est en principe défini sur **Aucun accès**. S'il est défini sur une autre option, l'utilisateur est ajouté à des groupes de Jump auxquels il ne devrait pas être assigné, et, dans la console d'accès, il est en mesure de visualiser la liste personnelle d'éléments de Jump de membres n'appartenant pas à son équipe.

Pour plus d'informations, veuillez consulter la section Utiliser les rôles d'éléments de Jump pour configurer les groupes d'autorisation des éléments de Jump à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/how-to/jumpoint/jump-item-roles.htm.

autonomes et non autonomes

Définissez les règles de demande et d'autorisation devant s'appliquer aux sessions de cet utilisateur. Sélectionnez une règle de session existante ou définissez des autorisations personnalisées pour cet utilisateur. Notez que l'option **Non défini** entraîne l'utilisation de la règle globale par défaut. Ces autorisations peuvent être remplacées par une règle de niveau supérieur.

Description

Affichez la description d'une règle de permission de session prédéfinie.

Partage d'écran

Règles de partage d'écran

Permet à l'utilisateur de voir ou de contrôler l'écran distant. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

> Pour plus d'informations, veuillez consulter la section Contrôler le point de terminaison à distance avec partage d'écran à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/screen-sharing.htm.

Restrictions de partage d'applications

Limiter l'accès aux applications spécifiées sur le système distant avec **N'autoriser que les exécutables répertoriés** ou **Ne refuser que les exécutables répertoriés**. Vous pouvez aussi choisir d'autoriser ou de refuser l'accès au bureau.

> ***Remarque :*** *cette fonction ne s'applique qu'aux systèmes d'exploitation Windows et Linux et n'inclut pas les sessions Remote Desktop Protocol (RDP) ou VNC.*

Ajouter des exécutables

Si des restrictions de partage d'application sont imposées, un bouton **Ajouter des exécutables** apparaît. Cliquer sur ce bouton ouvre un dialogue qui vous permet de spécifier quels exécutables autoriser ou refuser, en fonction de vos objectifs.

Après avoir ajouté des exécutables, un ou deux tableaux affichent les noms ou hachages de fichier que vous avez sélectionnés pour la restriction. Un champ de commentaire modifiable permet d'écrire des notes d'administration.

Entrer les noms de fichier ou hachages SHA-256 (un par ligne)

Lorsque vous restreignez des exécutables, saisissez manuellement les noms ou hachages des fichiers exécutables que vous souhaitez autoriser ou refuser. Cliquez sur **Ajouter des exécutables** lorsque vous avez terminé pour ajouter les fichiers choisis à votre configuration.

Vous pouvez saisir jusqu'à 25 fichiers par dialogue. Si vous avez besoin d'en ajouter davantage, cliquez sur **Ajouter des exécutables** puis rouvrez le dialogue.

Rechercher un ou plusieurs fichiers

Lorsque vous restreignez des exécutables, sélectionnez cette option pour parcourir votre système et choisir les fichiers exécutables pour obtenir automatiquement leurs noms ou hachages. Si vous sélectionnez des fichiers de votre plate-forme locale et du système de cette manière, assurez-vous que les fichiers sont bien des exécutables. Aucune vérification au niveau du navigateur n'est effectuée.

Choisissez **Utiliser le nom de fichier** ou **Utiliser le hachage de fichier** pour que le navigateur obtienne les noms ou hachages des fichiers exécutables automatiquement. Cliquez sur **Ajouter des exécutables** lorsque vous avez terminé pour ajouter les fichiers choisis à votre configuration.

Vous pouvez saisir jusqu'à 25 fichiers par dialogue. Si vous avez besoin d'en ajouter davantage, cliquez sur **Ajouter des exécutables** puis rouvrez le dialogue.

Remarque : *cette option n'est disponible que dans les navigateurs modernes, pas dans les navigateurs plus anciens.*

Restrictions de point de terminaison autorisées

Définissez si l'utilisateur peut interrompre l'entrée souris et clavier du système distant. L'utilisateur peut aussi empêcher l'affichage du bureau distant.

Pour plus d'informations, veuillez consulter la section Contrôler le point de terminaison à distance avec partage d'écran à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/screen-sharing.htm.

Annotations

Règles d'annotation

Permet à l'utilisateur d'utiliser les outils d'annotation pour dessiner sur l'écran du système distant. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

Pour plus d'informations, veuillez consulter la section Utilisez les annotations pour dessiner sur l'écran distant du point de terminaison à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/annotations.htm.

Transfert de fichiers

Règles de transfert de fichiers

Permet à l'utilisateur d'envoyer des fichiers vers le système distant, de télécharger des fichiers depuis le système distant, ou les deux. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

Chemins accessibles sur le système de fichiers du point de terminaison

Permettre à l'utilisateur de transférer des fichiers de et vers n'importe quel répertoire sur le système distant ou uniquement les répertoires spécifiés.

Chemins accessibles sur le système de fichiers de l'utilisateur

Permettre à l'utilisateur de transférer des fichiers de et vers n'importe quel répertoire sur son système local ou uniquement les répertoires spécifiés.

> Pour plus d'informations, veuillez consulter la section Transfert de fichiers vers et depuis le point de terminaison de système distant à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/file-transfer.htm.

Interpréteur de commandes

Règles de l'interpréteur de commandes

Permet à l'utilisateur de saisir des commandes sur l'ordinateur distant par l'intermédiaire d'une interface en ligne de commande virtuelle. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

> ***Remarque :*** *l'accès à l'interpréteur de commandes ne peut pas être restreint lors de sessions de Shell Jump.*

Configurez le filtrage des commandes pour empêcher l'utilisation accidentelle de commandes pouvant endommager les systèmes des points de terminaison.

> Pour plus d'informations sur le filtrage de commandes, veuillez consulter la section Utiliser un Shell Jump pour accéder à un appareil réseau distant à l'adresse www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/shell-jump.htm.

> Pour plus d'informations, veuillez consulter la section Ouvrir l'interpréteur de commandes sur le point de terminaison distant en utilisant la console d'accès à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/command-shell.htm.

Informations système

Règles relatives aux informations système

Permet à l'utilisateur de consulter les informations système de l'ordinateur distant. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

Autorisé à utiliser les actions relatives aux informations système

Permet à l'utilisateur d'interagir avec les processus et les programmes sur le système distant sans avoir recours au partage d'écran. Le technicien d'assistance peut ainsi désinstaller des programmes, supprimer des processus ou encore démarrer, arrêter, mettre en pause, reprendre et redémarrer des services.

> Pour plus d'informations, veuillez consulter la section Consulter les informations système sur le point de terminaison distant à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/system-info.htm.

Accès au registre

Règles d'accès au registre

Permet à l'utilisateur d'agir sur le registre d'un système Windows distant sans avoir recours au partage d'écran. Le technicien d'assistance peut ainsi afficher, ajouter, supprimer, modifier, rechercher et importer/exporter des clés.

> Pour plus d'informations, veuillez consulter la section Accès à l'éditeur de registre distant sur le point de terminaison distant à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/registry-editor.htm.

Scripts prédéfinis

Règles de script prédéfini

Permet à l'utilisateur d'exécuter des scripts prédéfinis créés pour ses équipes. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

> Pour plus d'informations, veuillez consulter la section Ouvrir l'interpréteur de commandes sur le point de terminaison distant en utilisant la Console d'Accès à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/command-shell.htm.

Paramètres de disponibilité

Planning de connexion

Restreindre la connexion de l'utilisateur selon le planning suivant

Définissez un planning afin de déterminer les périodes pendant lesquelles les utilisateurs peuvent se connecter à la console d'accès. Définissez le fuseau horaire à utiliser pour ce planning, puis ajoutez une ou plusieurs entrées de planification. Pour chaque entrée, indiquez l'heure et la date de début ainsi que l'heure et la date de fin.

Par exemple, si la période définie commence à 8 h et se termine à 17 h, un utilisateur peut se connecter à n'importe quel moment au cours de cette période et peut continuer à travailler passée l'heure de fin. Il ne sera toutefois pas autorisé à se reconnecter après 17 h.

Forcer la déconnexion lorsque le planning ne permet pas l'ouverture d'une session

Si un contrôle d'accès plus strict est requis, cochez cette option. Ceci force la déconnexion de l'utilisateur à l'heure de fin définie. Dans ce cas, l'utilisateur reçoit des notifications récurrentes à partir de 15 minutes avant d'être déconnecté. Lorsque l'utilisateur est déconnecté, toutes les sessions possédées suivront les règles de récupération.

Rapport sur les comptes utilisateur

Exportez des informations détaillées sur vos utilisateurs à des fins d'audit. Collectez des informations détaillées sur l'ensemble des utilisateurs, sur les utilisateurs d'un fournisseur de sécurité spécifique ou sur les utilisateurs locaux uniquement. Les informations collectées incluent les données affichées sous le bouton « Afficher les détails », ainsi que les appartenances et les autorisations des équipes et des règles de groupe.

Comptes utilisateur pour réinitialisation des mots de passe : Autoriser les utilisateurs à gérer les mots de passe

Comptes utilisateurs

Les administrateurs peuvent déléguer, via une autorisation utilisateur, la réinitialisation des mots de passe des utilisateurs locaux et des comptes utilisateurs bloqués à des utilisateurs avec privilèges, sans leur accorder les droits d'administrateur complets. Notez que les utilisateurs locaux peuvent tout de même réinitialiser leurs propres mots de passe.

> ***Remarque :*** *cela n'a aucune incidence sur l'interface utilisateur pour les administrateurs disposant de l'autorisation* ***Autorisé à définir les mots de passe****.*

Lorsqu'un utilisateur privilégié non administrateur accède à la page **Utilisateurs et sécurité > Utilisateurs** dans l'interface d'administration /login, il verra une version limitée de l'écran **Utilisateurs** contenant des liens **Modifier le mot de passe** pour les utilisateurs non administrateurs. Les utilisateurs avec privilèges ne peuvent pas modifier ou supprimer des comptes utilisateur, et ne sont pas autorisés à réinitialiser les mots de passe administrateur, ni les mots de passe des utilisateurs fournisseurs de sécurité.

Chercher des utilisateurs

Recherchez le compte d'un utilisateur à partir du nom d'utilisateur, du nom affiché ou de l'adresse e-mail.

Réinitialiser des échecs de connexion et déverrouiller un compte

Si un utilisateur échoue une ou plusieurs fois à se connecter, cliquez sur le bouton **Réinitialiser** pour son compte d'utilisateur afin de remettre le chiffre à 0.

Si un utilisateur se retrouve bloqué après un trop grand nombre d'échecs de connexion consécuritfs, cliquez sur le bouton **Déverrouiller le compte** pour que le compteur de son compte d'utilisateur soit remis à 0 et débloquer son compte.

Modifier le mot de passe

Changez le mot de passe pour un utilisateur non administrateur.

Modifier le mot de passe

Nom d'utilisateur

Identificateur unique servant à vous connecter. Ce champ ne peut pas être modifié.

Noms affichés

Le nom d'utilisateur tel qu'affiché dans les discussions d'équipe, les rapports, etc. Ce champ ne peut pas être modifié.

Adresse e-mail

L'adresse e-mail à laquelle sont envoyées les notifications par e-mail, notamment les réinitialisations de mot de passe ou les alertes de mode disponibilité étendue. Ce champ ne peut pas être modifié.

Commentaires

Commentaires sur le compte. Ce champ ne peut pas être modifié.

Mot de passe

Le nouveau mot de passe à assigner à ce compte d'utilisateur. Vous pouvez définir le mot de passe de votre choix, tant que la chaîne reste conforme à la règle définie sur la page **/login > Gestion > Sécurité**.

Envoyer le lien de réinitialisation de mot de passe à l'utilisateur par e-mail

Envoyez un lien par e-mail à l'utilisateur pour réinitialiser le mot de passe de son compte. Cette fonction nécessite une configuration SMTP compatible avec votre serveur, que l'on peut paramétrer sur la page **/login > Gestion > Configuration e-mail**.

Doit changer son mot de passe lors de la prochaine connexion

Si cette option est sélectionnée, l'utilisateur doit réinitialiser son mot de passe lors de sa prochaine connexion.

Invitation d'accès : créez des profils pour inviter des utilisateurs externes à des sessions

E-mail d'invitation d'accès

Avec l'invitation d'accès, un utilisateur privilégié peut inviter un utilisateur externe à rejoindre une session de manière ponctuelle. Lorsque l'utilisateur crée l'invitation, il sélectionne un profil de sécurité pour déterminer le niveau de privilèges octroyé à l'utilisateur externe. Les profils de sécurité d'invitation d'accès sont configurés en tant que règles de session sur la page **Utilisateurs et sécurité > Règles de session** et doivent être activés pour pouvoir utiliser l'invitation d'accès.

L'e-mail d'invitation est envoyé aux utilisateurs externes lorsque vous les invitez à rejoindre une session.

Objet

Personnalisez l'objet de cet e-mail. Cliquez sur le lien sous le champ **Corps** pour afficher les macros qui peuvent être utilisées pour personnaliser le texte dans vos e-mails selon vos souhaits.

Corps

Personnalisez le texte de cet e-mail. Cliquez sur le lien sous le champ **Corps** pour afficher les macros qui peuvent être utilisées pour personnaliser le texte dans vos e-mails selon vos souhaits.

> Pour plus d'informations, veuillez consulter la section Inviter un utilisateur externe à rejoindre une session d'accès à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/access-invite.htm.

Fournisseurs de sécurité : Activation des connexions LDAP, Active Directory, RADIUS et Kerberos

Fournisseurs de sécurité

Vous pouvez configurer votre Secure Remote Access Appliance pour qu'il authentifie les utilisateurs d'après des serveurs LDAP, RADIUS ou Kerberos existants, et pour attribuer des privilèges d'après la hiérarchie et les paramètres de groupe préexistants déjà spécifiés dans vos serveurs. Kerberos permet une authentification unique, tandis que RSA et d'autres mécanismes d'authentification à deux facteurs par RADIUS fournissent un niveau de sécurité supplémentaire.

Ajouter un fournisseur

Depuis le menu déroulant **Ajouter**, sélectionnez LDAP, RADIUS, Kerberos, SAML ou SCIM pour ajouter une nouvelle configuration de fournisseur de sécurité.

Modifier l'ordre

Cliquez sur ce bouton pour déplacer les fournisseurs de sécurité afin de définir leur priorité. Vous pouvez déplacer des serveurs à l'intérieur d'une grappe ; les grappes peuvent être déplacées dans leur intégralité. Cliquez sur **Enregistrer l'ordre** pour que les changements de priorité prennent effet.

Désactiver

Désactiver la connexion de ce fournisseur de sécurité. Ceci est utile pour les maintenances planifiées, lorsque vous voulez qu'un serveur soit hors ligne mais non effacé.

Synchroniser

Synchronisez les utilisateurs et les groupes associés avec un fournisseur de sécurité externe. La synchronisation se produit automatiquement une fois par jour. Cliquer sur ce bouton force une synchronisation manuelle.

Afficher le journal

Affichez l'historique d'état pour la connexion d'un fournisseur de sécurité.

Dupliquer le nœud

Créez une copie d'une configuration de fournisseur de sécurité en cluster existante. Ceci sera ajouté en tant que nouveau nœud dans le même cluster.

Mettre à niveau vers un cluster

Mettez à niveau un fournisseur de sécurité sur un cluster de fournisseur de sécurité. Pour ajouter d'autres fournisseurs de sécurité à ce cluster, copiez un nœud existant.

Copier

Créez une copie d'une configuration de fournisseur de sécurité existante. Ceci sera ajouté comme fournisseur de sécurité de niveau principal et non pas comme faisant partie d'un cluster.

Modifier, supprimer

Modifier ou supprimer un élément existant.

Modifier le fournisseur de sécurité - LDAP

Paramètres généraux

Nom

Créez un nom unique permettant d'identifier ce fournisseur.

Activé

Si cette case est cochée, votre Secure Remote Access Appliance peut chercher ce fournisseur de sécurité lorsqu'un utilisateur tente de se connecter. Si elle n'est pas cochée, le fournisseur ne sera pas recherché.

Authentification utilisateur

Choisissez si ce fournisseur devrait être utilisé pour l'authentification d'utilisateurs. Si désélectionnées, les options spécifiques à l'authentification d'utilisateurs sont désactivées.

Approvisionnement de l'utilisateur

Par défaut, l'approvisionnement d'utilisateurs a lieu avec ce fournisseur. Si vous possédez un fournisseur SCIM en place, vous pouvez choisir d'approvisionner les utilisateurs à travers ce fournisseur à la place. Si ce fournisseur n'est pas utilisé pour l'authentification d'utilisateurs, alors **Ne pas approvisionner les utilisateurs** sera sélectionné.

> ***Remarque :*** *ce paramètre ne peut pas être modifié après que ce fournisseur de sécurité a été enregistré pour la première fois.*

Garder les informations d'utilisateur synchronisées avec le serveur LDAP

Cocher cette option fait en sorte que le nom d'utilisateur affiché reste le même que celui désigné sur le fournisseur de sécurité, plutôt que d'autoriser la modification du nom affiché sur BeyondTrust.

Paramètres d'autorisation

Synchronisation : Activer le cache d'objet LDAP

Si ceci est coché, les objets LDAP visibles pour le serveur sont mis en cache et synchronisés toutes les nuits, ou manuellement si désiré. Lorsque cette option est utilisée, un nombre plus faible de connexions est établi avec le serveur LDAP pour des raisons administratives, ce qui peut potentiellement améliorer la vitesse et l'efficacité.

Si cette option est décochée, les changements apportés au serveur LDAP sont disponibles immédiatement, sans besoin de synchronisation. Cependant, lorsque vous apportez des changements aux règles d'utilisateur à travers l'interface d'administration, quelques connexions LDAP courtes peuvent avoir lieu si c'est nécessaire.

Pour les fournisseurs qui avaient le paramètre de synchronisation activé, désactiver ou décocher l'option de synchronisation provoquera l'effacement de tous les enregistrements mis en cache qui ne sont pas en cours d'utilisation.

Rechercher des groupes

Choisissez d'utiliser ce fournisseur de sécurité uniquement pour l'authentification d'utilisateurs, seulement pour les recherches de groupes, ou pour les deux. Si l'option **Authentification utilisateur** ci-dessus n'est pas cochée, alors **Rechercher des groupes en utilisant ce fournisseur** sera sélectionné. L'option de rechercher des groupes en utilisant un fournisseur différent n'est disponible que si un autre fournisseur permettant la recherche de groupe a déjà été créé.

Règle de groupe par défaut *(Visible uniquement si l'authentification d'utilisateur est autorisée)*

Chaque utilisateur qui s'authentifie auprès d'un serveur externe doit être membre d'au moins une règle de groupe pour pouvoir s'authentifier sur votre Secure Remote Access Appliance, en se connectant sur l'interface /login ou sur la console d'accès. Vous pouvez sélectionner une règle de groupe par défaut à appliquer à tous les utilisateurs autorisés à s'authentifier auprès du serveur configuré.

Notez que si une règle par défaut est définie, alors n'importe quel utilisateur qui s'authentifie sur ce serveur peut potentiellement avoir accès au niveau de cette règle par défaut. Il est donc recommandé de définir le défaut sur une règle avec le minimum de privilèges, pour empêcher les utilisateurs d'obtenir des autorisations que vous ne souhaitez pas qu'ils aient.

> ***Remarque :*** *si un utilisateur est dans une règle de groupe par défaut et qu'il est ensuite spécifiquement ajouté à une autre règle de groupe, les paramètres pour la règle spécifique prendront toujours le pas sur les paramètres par celle par défaut, même si la règle spécifique a une priorité plus basse que celle par défaut, et même si les paramètres de la règle par défaut n'autorisent pas le remplacement.*

Paramètres de connexion

Nom de l'hôte

Saisissez le nom d'hôte du serveur sur lequel se trouve le magasin d'annuaire externe.

> ***Remarque :*** *si vous allez utiliser **LDAPS** ou **LDAP avec TLS**, le nom d'hôte doit correspondre au nom d'hôte utilisé dans le nom du sujet du certificat SSL public de votre serveur LDAP ou au composant DNS de son nom de sujet alternatif.*

Port

Spécifiez le port de votre serveur LDAP. Il s'agit généralement du port **389** pour LDAP ou du port **636** pour LDAPS. BeyondTrust permet également le catalogue global sur le port **3268** pour LDAP ou **3269** pour LDAPS.

Chiffrement

Sélectionnez le type de cryptage à utiliser lors de la communication avec le serveur LDAP. Pour des raisons de sécurité, **LDAPS** ou **LDAP avec TLS** est recommandé.

> ***Remarque :*** *le LDAP envoie et reçoit des données en texte clair depuis le serveur LDAP, ce qui peut exposer des informations de comptes utilisateurs confidentielles au reniflage de paquets. LDAPS, et LDAP avec un cryptage TLS, cryptent les données utilisateur lors de leur transfert ; ces méthodes sont donc recommandées, plutôt que le LDAP classique. Le LDAP avec TLS utilise la fonction StartTLS pour initier une connexion de LDAP en texte clair, mais la fait ensuite passer en connexion cryptée. Le LDAPS initie la connexion sur une connexion cryptée sans envoyer aucune donnée en texte clair.*

Si vous sélectionnez **LDAPS** ou **LDAP avec TLS**, vous devez transférer le certificat SSL racine utilisé par votre serveur LDAP. Ceci est nécessaire pour garantir la validité du serveur et la sécurité des données. Le certificat racine doit être au format PEM.

> ***Remarque :*** *Si le nom de sujet du certificat SSL public du serveur LDAP ou le composant DNS de son nom de sujet alternatif ne correspond pas à la valeur du champ **Nom de l'hôte**, le fournisseur sera considéré comme inaccessible. Vous pouvez cependant utiliser un certificat à caractère générique pour certifier plusieurs sous-domaines du même site. Par exemple, un certificat pour ***.example.com** certifiera à la fois **access.example.com** et **remote.example.com**.*

Informations d'authentification de liaison

Spécifiez un nom d'utilisateur et un mot de passe grâce auxquels votre Secure Remote Access Appliance peut se lier et effectuer une recherche sur le magasin d'annuaires LDAP.

Si votre serveur prend en charge les liaisons anonymes, vous aurez la possibilité de lier sans spécifier un nom d'utilisateur et un mot de passe. La liaison anonyme est considérée comme non sécurisée et est désactivée par défaut sur la plupart des serveurs LDAP.

Méthode de connexion

Si vous utilisez un magasin de répertoire externe sur le même réseau LAN que votre Secure Remote Access Appliance, il se peut que les deux systèmes puissent communiquer directement. Dans ce cas, vous pouvez laisser l'option **Proxy à partir du serveur via l'agent de connexion** décochée et poursuivre.

Comme votre magasin externe d'annuaires ne se trouve pas sur le même réseau que votre serveur cloud BeyondTrust, ils ne peuvent pas communiquer directement. L'utilisation d'un agent de connexion est donc nécessaire.

Si les deux systèmes ne peuvent pas communiquer directement, par exemple si votre serveur de répertoire externe se trouve derrière un pare-feu, vous devez utiliser un agent de connexion. Télécharger l'agent de connexion Win32 permet à votre serveur de répertoire et votre Secure Remote Access Appliance de communiquer par une connexion sortante chiffrée en SSL sans configuration de pare-feu. L'agent de connexion peut être téléchargé sur le serveur de répertoire ou sur un serveur séparé sur le même réseau que votre serveur de répertoire (recommandé).

Dans le cas ci-dessus, cochez **Proxy à partir du serveur via l'agent de connexion**. Créer un **Mot de passe de l'agent de connexion** à utiliser lors du processus d'installation de l'agent de connexion. Cliquez ensuite sur **Télécharger l'agent de connexion**, lancez l'installeur et suivez les instructions de l'assistant d'installation. Lors de l'installation, vous serez invité à saisir le nom du fournisseur de sécurité et le mot de passe de l'agent de connexion que vous avez créé ci-dessus.

> ***Remarque :*** *Les clients du cloud BeyondTrust doivent exécuter l'agent de connexion pour pouvoir utiliser un magasin externe d'annuaires.*

Nom d'utilisateur

Saisissez un nom d'utilisateur pour les informations d'authentification de liaison.

Mot de passe et confirmation du mot de passe

Saisissez et confirmez un mot de passe pour les informations d'authentification de liaison.

Type de répertoire

Pour aider à la configuration de la connexion réseau entre votre Secure Remote Access Appliance et votre fournisseur de sécurité, vous pouvez sélectionner un type de répertoire comme modèle. Ceci pré-remplit les champs de configuration ci-dessous avec des données standard, mais celles-ci doivent être modifiées pour correspondre à la configuration spécifique de votre fournisseur de sécurité. Le LDAP Active Directory est le type de serveur le plus commun, mais vous pouvez configurer BeyondTrust pour qu'il communique avec la plupart des types de fournisseurs de sécurité.

Paramètres du cluster *(Visible uniquement pour les clusters)*

Algorithme de sélection des membres

Sélectionnez la méthode de recherche des nœuds dans ce cluster.

Du haut vers le bas essaie en premier le serveur ayant la plus haute priorité dans le cluster. Si ce serveur n'est pas disponible ou si le compte n'est pas trouvé, le serveur ayant la priorité suivante est essayé. La recherche se déplace dans la liste des serveurs en cluster jusqu'à ce que le compte soit trouvé ou qu'il soit déterminé que le compte n'existe sur aucun des serveurs spécifiés et disponibles.

En alternance est conçu pour équilibrer la charge entre plusieurs serveurs. L'algorithme choisit aléatoirement quel serveur essayer en premier. Si ce serveur n'est pas disponible, ou si le compte n'est pas trouvé, un autre serveur aléatoire est essayé. La recherche se poursuit aléatoirement parmi les serveurs restants dans le cluster jusqu'à ce que le compte soit trouvé ou qu'il soit déterminé que le compte n'existe sur aucun des serveurs spécifiés et disponibles.

Délai de nouvelle tentative

Réglez la durée devant s'écouler avant de pouvoir tenter à nouveau d'utiliser un membre de cluster indisponible.

Paramètres de schéma d'utilisateur

Remplacer les valeurs de cluster *(Visible uniquement pour les nœuds du cluster)*

Si cette option n'est pas cochée, ce nœud de cluster utilisera les mêmes paramètres de schéma que le cluster. Si cette option n'est pas cochée, vous pouvez modifier les paramètres de schéma ci-dessous.

Nom unique de base de recherche

Déterminez le niveau dans la hiérarchie de votre annuaire, spécifiée par un nom unique, où le Secure Remote Access Appliance devra commencer à chercher des utilisateurs. En fonction de la taille de votre magasin d'annuaires et des utilisateurs nécessitant des comptes BeyondTrust, vous pourrez améliorer les performances en désignant l'unité organisationnelle spécifique dans votre magasin d'annuaires qui requiert l'accès. Si vous n'êtes pas sûr, ou si les utilisateurs recouvrent plusieurs unités organisationnelles, vous pouvez aussi spécifier le nom unique de la racine de votre magasin d'annuaires.

Requête utilisateur

Spécifiez les informations de requête que le Secure Remote Access Appliance doit utiliser pour trouver un utilisateur LDAP lorsque l'utilisateur tente de se connecter. Le champ **Requête utilisateur** accepte une requête LDAP standard (RFC 2254 – Représentation en chaîne des filtres de recherche LDAP). Vous pouvez modifier la chaîne de requête pour personnaliser la façon dont vos utilisateurs se connectent et quels types de noms d'utilisateurs sont acceptés. Pour spécifier quelle valeur à l'intérieur de la chaîne doit correspondre au nom d'utilisateur, remplacer cette valeur par *.

Requête de navigation

La requête de navigation influence la façon dont les résultats sont affichés lors de la navigation par règles de groupe. Ceci filtre les résultats afin que seuls certains d'entre eux soient affichés dans la liste déroulante de sélection de membres lors de l'ajout de membres dans une règle de groupe.

Classes d'objets

Spécifiez des classes d'objets valides pour un utilisateur dans votre magasin d'annuaires. Seuls les utilisateurs possédant une ou plusieurs de ces classes d'objets seront autorisés à s'authentifier. Ces classes d'objets sont également utilisées avec les noms d'attribut ci-dessous pour indiquer à votre Secure Remote Access Appliance le schéma que le serveur LDAP utilise pour identifier les utilisateurs. Vous pouvez indiquer plusieurs classes d'objets, une par ligne.

Noms d'attribut

Spécifiez les champs à utiliser pour l'identificateur unique, le nom affiché et l'adresse e-mail d'un utilisateur.

Identificateur unique

Ce champ nécessite un identificateur unique pour l'élément. Bien que le nom unique puisse servir d'identificateur, le nom unique d'un utilisateur peut changer fréquemment au cours de la vie de l'utilisateur, avec un changement de nom ou d'emplacement, ou avec le changement de nom du magasin LDAP. Ainsi, la plupart des serveurs LDAP incorporent un champ unique pour chaque élément qui ne change pas pour la durée de vie de l'utilisateur. Si vous utilisez le nom unique comme identifiant unique et que le nom unique d'un utilisateur change, cet utilisateur sera considéré comme un nouvel utilisateur, et tout changement apporté spécifiquement au compte utilisateur BeyondTrust de cet individu ne sera pas reporté sur le nouvel utilisateur. Si votre serveur LDAP n'inclut pas d'identificateur unique, utilisez un champ dont il est peu probable que la valeur soit identique pour un autre utilisateur.

E-mail

Cette valeur détermine quel champ doit être utilisé comme adresse e-mail de l'utilisateur.

Nom affiché

Cela détermine quel champ doit être utilisé comme nom affiché de l'utilisateur.

Paramètres de schéma de groupe *(Visible uniquement lors de recherches de groupe)*

Type de répertoire

Pour aider à la configuration de la connexion réseau entre votre Secure Remote Access Appliance et votre fournisseur de sécurité, vous pouvez sélectionner un type de répertoire comme modèle. Ceci pré-remplit les champs de configuration ci-dessous avec des données standard, mais celles-ci doivent être modifiées pour correspondre à la configuration spécifique de votre fournisseur de

sécurité. Le LDAP Active Directory est le type de serveur le plus commun, mais vous pouvez configurer BeyondTrust pour qu'il communique avec la plupart des types de fournisseurs de sécurité.

Nom unique de base de recherche

Déterminez le niveau dans la hiérarchie de votre annuaire, spécifiée par un nom unique, où le Secure Remote Access Appliance devra commencer à chercher des groupes. En fonction de la taille de votre magasin d'annuaires et des groupes nécessitant un accès au Secure Remote Access Appliance, vous pourrez améliorer les performances en désignant l'unité organisationnelle spécifique dans votre magasin d'annuaire qui requiert l'accès. Si vous n'êtes pas sûr, ou si les groupes recouvrent plusieurs unités organisationnelles, vous pouvez aussi spécifier le nom unique de la racine de votre magasin d'annuaire.

Requête de navigation

La requête de navigation influence la façon dont les résultats sont affichés lors de la navigation par règles de groupe. Ceci filtre les résultats afin que seuls certains d'entre eux soient affichés dans la liste déroulante de sélection de membres lors de l'ajout de membres dans une règle de groupe.

Classes d'objets

Spécifiez des classes d'objets valides pour un groupe dans votre magasin d'annuaires. Seuls les groupes possédant une ou plusieurs de ces classes d'objets seront retournés. Ces classes d'objets sont également utilisées avec les noms d'attribut ci-dessous pour indiquer à votre Secure Remote Access Appliance le schéma que le serveur LDAP utilise pour identifier les groupes. Vous pouvez saisir plusieurs classes d'objets de groupes, une par ligne.

Noms d'attribut

Spécifiez les champs à utiliser pour l'identificateur unique, et le nom affiché d'un groupe.

Identificateur unique

Ce champ nécessite un identificateur unique pour l'élément. Bien que le nom unique puisse servir d'identificateur, le nom unique d'un groupe peut changer fréquemment au cours de la vie du groupe, avec un changement d'emplacement, ou avec le changement de nom du magasin LDAP. Ainsi, la plupart des serveurs LDAP incorporent un champ unique pour chaque élément qui ne change pas pour la durée de vie du groupe. Si vous utilisez le nom unique comme identificateur unique et que le nom unique d'un groupe change, ce groupe sera considéré comme un nouveau groupe, et toutes les règles de groupes définies pour ce groupe ne seront pas reportées sur le nouveau groupe. Si votre serveur LDAP n'inclut pas d'identificateur unique, utilisez un champ dont il est peu probable que la valeur soit identique pour un autre groupe.

Nom affiché

Cette valeur détermine quel champ doit être utilisé comme nom affiché du groupe.

Relations utilisateurs-groupes

Ce champ appelle une requête pour déterminer quels utilisateurs appartiennent à quels groupes ou, inversement, quels groupes contiennent quels utilisateurs.

Effectuer une recherche de groupes récursive

Vous pouvez choisir d'effectuer une recherche de groupes récursive. Ceci lancera une requête pour un utilisateur, puis des requêtes pour tous les groupes auxquels l'utilisateur appartient, puis des requêtes pour tous les groupes auxquels ces groupes appartiennent, et ainsi de suite, jusqu'à ce que tous les groupes possibles associés à cet utilisateur aient été trouvés.

Lancer une recherche récursive peut avoir un impact considérable sur les performances, car le serveur continuera à émettre des requêtes jusqu'à ce qu'il trouve des informations sur tous les groupes. Si cela prend trop de temps, l'utilisateur ne pourra peut-être pas se connecter.

Une recherche non récursive n'émettra qu'une requête par utilisateur. Si votre serveur LDAP a un champ spécial contenant tous les groupes auxquels l'utilisateur appartient, la recherche récursive n'est pas nécessaire. La recherche récursive est également inutile si votre système de répertoire ne prend pas en charge les membres de groupes ou les groupes.

Tester les paramètres

Nom d'utilisateur et mot de passe

Saisissez un nom d'utilisateur et un mot de passe pour un compte qui existe sur le serveur que vous testez. Ce compte doit correspondre aux critères de connexion spécifiés dans la configuration ci-dessus.

Essayer d'obtenir des attributs d'utilisateur et des appartenances de groupes si les informations d'authentification sont acceptées

Si cette option est cochée, votre test d'informations d'authentification réussi tentera également de vérifier les attributs d'utilisateur et la recherche de groupe. Notez que pour que ces fonctions soient testées avec succès, elles doivent être prises en charge et configurées dans votre fournisseur de sécurité.

Démarrer le test

Si votre serveur est correctement configuré et que vous avez saisi un nom d'utilisateur et un mot de passe de test valides, vous recevrez un message de confirmation. Sinon, vous verrez un message d'erreur et un journal qui vous aidera à résoudre le problème.

Modifier le fournisseur de sécurité - RADIUS

Paramètres généraux

Nom

Créez un nom unique permettant d'identifier ce fournisseur.

Activé

Si cette case est cochée, votre Secure Remote Access Appliance peut chercher ce fournisseur de sécurité lorsqu'un utilisateur tente de se connecter. Si elle n'est pas cochée, le fournisseur ne sera pas recherché.

Conserver le nom affiché synchronisé avec le système distant

Cocher cette option fait en sorte que le nom d'utilisateur affiché reste le même que celui désigné sur le fournisseur de sécurité, plutôt que d'autoriser la modification du nom affiché sur BeyondTrust.

Paramètres d'autorisation

N'autoriser que les utilisateurs suivants

Vous pouvez choisir d'autoriser l'accès seulement aux utilisateurs spécifiés sur votre serveur RADIUS. Saisissez chaque nom d'utilisateur séparé par un saut de ligne. Une fois qu'ils auront été saisis, ces utilisateurs seront disponibles dans le dialogue **Ajouter membre de règle** lors de la modification de règle de groupe sur la page **/login > Utilisateurs et sécurité > Règles de groupe**.

Si vous laissez ce champ vide, tous les utilisateurs qui s'authentifient grâce à votre serveur RADIUS seront autorisés ; si vous les autorisez tous, vous devez aussi spécifier une règle de groupe par défaut.

Recherche de groupe LDAP

Si vous voulez que les utilisateurs de ce fournisseur de sécurité soient associés à leurs groupes sur un serveur LDAP séparé, choisissez un ou plusieurs serveurs de groupe LDAP à utiliser pour la recherche de groupe.

Règle de groupe par défaut

Chaque utilisateur qui s'authentifie auprès d'un serveur externe doit être membre d'au moins une règle de groupe pour pouvoir s'authentifier sur votre Secure Remote Access Appliance, en se connectant sur l'interface /login ou sur la console d'accès. Vous pouvez sélectionner une règle de groupe par défaut à appliquer à tous les utilisateurs autorisés à s'authentifier auprès du serveur configuré.

Notez que si une règle par défaut est définie, alors n'importe quel utilisateur qui s'authentifie sur ce serveur peut potentiellement avoir accès au niveau de cette règle par défaut. Il est donc recommandé de définir le défaut sur une règle avec le minimum de privilèges, pour empêcher les utilisateurs d'obtenir des autorisations que vous ne souhaitez pas qu'ils aient.

> ***Remarque :*** *si un utilisateur est dans une règle de groupe par défaut et qu'il est ensuite spécifiquement ajouté à une autre règle de groupe, les paramètres pour la règle spécifique prendront toujours le pas sur les paramètres par celle par défaut, même si la règle spécifique a une priorité plus basse que celle par défaut, et même si les paramètres de la règle par défaut n'autorisent pas le remplacement.*

Paramètres de connexion

Nom de l'hôte

Saisissez le nom d'hôte du serveur sur lequel se trouve le magasin d'annuaire externe.

Port

Spécifiez le port d'authentification pour votre serveur RADIUS. C'est en général le port **1812**.

Méthode de connexion

Si vous utilisez un magasin de répertoire externe sur le même réseau LAN que votre Secure Remote Access Appliance, il se peut que les deux systèmes puissent communiquer directement. Dans ce cas, vous pouvez laisser l'option **Proxy à partir du serveur via l'agent de connexion** décochée et poursuivre.

Comme votre magasin externe d'annuaires ne se trouve pas sur le même réseau que votre serveur cloud BeyondTrust, ils ne peuvent pas communiquer directement. L'utilisation d'un agent de connexion est donc nécessaire.

Si les deux systèmes ne peuvent pas communiquer directement, par exemple si votre serveur de répertoire externe se trouve derrière un pare-feu, vous devez utiliser un agent de connexion. Télécharger l'agent de connexion Win32 permet à votre serveur de répertoire et votre Secure Remote Access Appliance de communiquer par une connexion sortante chiffrée en SSL sans configuration de pare-feu. L'agent de connexion peut être téléchargé sur le serveur de répertoire ou sur un serveur séparé sur le même réseau que votre serveur de répertoire (recommandé).

Dans le cas ci-dessus, cochez **Proxy à partir du serveur via l'agent de connexion**. Créer un **Mot de passe de l'agent de connexion** à utiliser lors du processus d'installation de l'agent de connexion. Cliquez ensuite sur **Télécharger l'agent de connexion**, lancez l'installeur et suivez les instructions de l'assistant d'installation. Lors de l'installation, vous serez invité à saisir le nom du fournisseur de sécurité et le mot de passe de l'agent de connexion que vous avez créé ci-dessus.

Secret partagé

Fournissez un nouveau secret partagé pour que votre Secure Remote Access Appliance et votre serveur RADIUS puissent communiquer.

Délai d'attente (secondes)

Définissez la durée d'attente maximale d'une réponse du serveur. Notez bien que si la réponse est **Réponse-Accepter** ou **Réponse-Demande**, alors RADIUS attendra pendant l'intégralité de la durée spécifiée ici avant d'authentifier le compte. Il est ainsi conseillé de garder cette valeur à un niveau aussi bas que possible, en fonction de vos paramètres réseau. Une valeur idéale est de 3-5 secondes, la valeur maximum étant de trois minutes.

Paramètres du cluster *(Visible uniquement pour les clusters)*

Algorithme de sélection des membres

Sélectionnez la méthode de recherche des nœuds dans ce cluster.

Du haut vers le bas essaie en premier le serveur ayant la plus haute priorité dans le cluster. Si ce serveur n'est pas disponible ou si le compte n'est pas trouvé, le serveur ayant la priorité suivante est essayé. La recherche se déplace dans la liste des serveurs en cluster jusqu'à ce que le compte soit trouvé ou qu'il soit déterminé que le compte n'existe sur aucun des serveurs spécifiés et disponibles.

En alternance est conçu pour équilibrer la charge entre plusieurs serveurs. L'algorithme choisit aléatoirement quel serveur essayer en premier. Si ce serveur n'est pas disponible, ou si le compte n'est pas trouvé, un autre serveur aléatoire est essayé. La recherche se poursuit aléatoirement parmi les serveurs restants dans le cluster jusqu'à ce que le compte soit trouvé ou qu'il soit déterminé que le compte n'existe sur aucun des serveurs spécifiés et disponibles.

Délai de nouvelle tentative

Réglez la durée devant s'écouler avant de pouvoir tenter à nouveau d'utiliser un membre de cluster indisponible.

Tester les paramètres

Nom d'utilisateur et mot de passe

Saisissez un nom d'utilisateur et un mot de passe pour un compte qui existe sur le serveur que vous testez. Ce compte doit correspondre aux critères de connexion spécifiés dans la configuration ci-dessus.

Essayer d'obtenir des attributs d'utilisateur et des appartenances de groupes si les informations d'authentification sont acceptées

Si cette option est cochée, votre test d'informations d'authentification réussi tentera également de vérifier les attributs d'utilisateur et la recherche de groupe. Notez que pour que ces fonctions soient testées avec succès, elles doivent être prises en charge et configurées dans votre fournisseur de sécurité.

Démarrer le test

Si votre serveur est correctement configuré et que vous avez saisi un nom d'utilisateur et un mot de passe de test valides, vous recevrez un message de confirmation. Sinon, vous verrez un message d'erreur et un journal qui vous aidera à résoudre le problème.

Modifier le fournisseur de sécurité - Kerberos

Paramètres généraux

Nom

Créez un nom unique permettant d'identifier ce fournisseur.

Activé

Si cette case est cochée, votre Secure Remote Access Appliance peut chercher ce fournisseur de sécurité lorsqu'un utilisateur tente de se connecter. Si elle n'est pas cochée, le fournisseur ne sera pas recherché.

Conserver le nom affiché synchronisé avec le système distant

Cocher cette option fait en sorte que le nom d'utilisateur affiché reste le même que celui désigné sur le fournisseur de sécurité, plutôt que d'autoriser la modification du nom affiché sur BeyondTrust.

Retirer le domaine des noms principaux

Sélectionnez cette option pour supprimer la partie DOMAINE du nom principal d'utilisateur lors de la construction du nom d'utilisateur BeyondTrust.

Paramètres d'autorisation

Mode de gestion des utilisateurs

Sélectionnez les utilisateurs pouvant s'authentifier auprès de votre Secure Remote Access Appliance. **Autoriser tous les utilisateurs** autorise toute personne actuellement authentifiée par votre KDC. **Autoriser uniquement les noms principaux d'utilisateurs indiqués dans la liste** n'autorise que les noms principaux d'utilisateurs spécifiquement désignés. **Autoriser uniquement les noms principaux d'utilisateurs qui correspondent à la regex** autorise uniquement les utilisateurs correspondant à une expression régulière compatible Perl (PCRE).

Mode de gestion SPN : Autoriser uniquement les SPN indiqués dans la liste

Si la case n'est pas cochée, tous les Noms principaux du service (SPN) pour ce fournisseur de sécurité sont autorisés. Si la case est cochée, sélectionnez des SPN spécifiques dans une liste de SPN actuellement configurés.

Recherche de groupe LDAP

Si vous voulez que les utilisateurs de ce fournisseur de sécurité soient associés à leurs groupes sur un serveur LDAP séparé, choisissez un ou plusieurs serveurs de groupe LDAP à utiliser pour la recherche de groupe.

Règle de groupe par défaut

Chaque utilisateur qui s'authentifie auprès d'un serveur externe doit être membre d'au moins une règle de groupe pour pouvoir s'authentifier sur votre Secure Remote Access Appliance, en se connectant sur l'interface /login ou sur la console d'accès. Vous pouvez sélectionner une règle de groupe par défaut à appliquer à tous les utilisateurs autorisés à s'authentifier auprès du serveur configuré.

Notez que si une règle par défaut est définie, alors n'importe quel utilisateur qui s'authentifie sur ce serveur peut potentiellement avoir accès au niveau de cette règle par défaut. Il est donc recommandé de définir le défaut sur une règle avec le minimum de privilèges, pour empêcher les utilisateurs d'obtenir des autorisations que vous ne souhaitez pas qu'ils aient.

> ***Remarque :*** *si un utilisateur est dans une règle de groupe par défaut et qu'il est ensuite spécifiquement ajouté à une autre règle de groupe, les paramètres pour la règle spécifique prendront toujours le pas sur les paramètres par celle par défaut, même si la règle spécifique a une priorité plus basse que celle par défaut, et même si les paramètres de la règle par défaut n'autorisent pas le remplacement.*

Modifier le fournisseur de sécurité - SAML

Paramètres généraux

Nom

Ce nom unique aide à identifier votre fournisseur. Le nom de votre fournisseur SAML est auto-généré et ne peut pas être modifié pour le moment.

Activé

Si cette case est cochée, votre Secure Remote Access Appliance peut chercher ce fournisseur de sécurité lorsqu'un utilisateur tente de se connecter. Si elle n'est pas cochée, le fournisseur ne sera pas recherché.

Approvisionnement de l'utilisateur

Par défaut, l'approvisionnement d'utilisateurs a lieu avec ce fournisseur. Si vous possédez un fournisseur SCIM en place, vous pouvez choisir d'approvisionner les utilisateurs à travers ce fournisseur à la place.

> ***Remarque :*** *ce paramètre ne peut pas être modifié après que ce fournisseur de sécurité a été enregistré pour la première fois.*

Paramètres du fournisseur d'identité

Métadonnées de fournisseur d'identité

Le fichier de métadonnées contient toutes les informations nécessaires à l'installation initiale de votre fournisseur SAML et doit être téléchargé à partir de votre fournisseur d'identité. Enregistrez le fichier XML, puis cliquez sur **Choisir fichier** pour sélectionner et transférer le fichier sélectionné.

> ***Remarque :*** *les champs pour l'**ID d'entité**, l'**URL de service d'authentification unique** et le **Certificat** sont automatiquement remplis à partir du fichier de métadonnées du fournisseur d'identité. Si vous ne pouvez pas obtenir de fichier de métadonnées de votre fournisseur, ces informations peuvent être saisies manuellement.*

ID d'entité

Ceci est l'identifiant unique pour le fournisseur d'identité que vous utilisez.

URL de service d'authentification unique

Lorsque vous souhaitez vous connecter à BeyondTrust au moyen de SAML, c'est vers cette URL que vous serez automatiquement redirigé afin de pouvoir vous connecter.

Liaison de protocole URL SSO

Cela détermine si une requête HTTP POST a lieu ou si l'utilisateur est redirigé vers l'URL d'authentification. Cela devrait être laissé en tant que redirection, sauf dans le cas où cela serait requis par le fournisseur d'identité.

Certificat du serveur

Ce certificat est utilisé pour vérifier la signature de l'affirmation envoyée par le fournisseur d'identité.

Paramètres du fournisseur de service

Métadonnées de fournisseur de service

Téléchargez les métadonnées BeyondTrust, que vous devrez ensuite transférer à votre fournisseur d'identité.

ID d'entité

Ceci est votre URL BeyondTrust. Cela identifie de façon unique votre site auprès du fournisseur d'identité.

Clé privée

Si nécessaire, vous pouvez déchiffrer les messages envoyés par le fournisseur d'identité, s'ils prennent en charge et requièrent le chiffrement. Cliquez sur **Choisir le fichier** pour transférer la clé privée nécessaire au déchiffrement des messages envoyés par le fournisseur d'identité.

Paramètres d'approvisionnement d'utilisateurs *(Visible uniquement si ce fournisseur est utilisé pour l'approvisionnement d'utilisateurs)*

Attribut SAML d'utilisateur

Ces attributs sont utilisés pour approvisionner les utilisateurs à travers BeyondTrust. Les valeurs par défaut correspondent aux applications certifiées par BeyondTrust avec différents fournisseurs d'identité. Si vous créez votre propre connecteur SAML, vous aurez peut-être besoin de modifier les attributs pour les faire correspondre à ce qui est envoyé par votre fournisseur d'identité.

Paramètres d'autorisation *(Visible uniquement si ce fournisseur est utilisé pour l'approvisionnement d'utilisateurs)*

Recherches de groupe

Ceci est le nom de l'attribut SAML contenant les noms des groupes auxquels les utilisateurs devraient appartenir. Le nom par défaut des applications BeyondTrust est « Groupes ».

> ***Remarque :*** *si la valeur d'attribut contient plusieurs noms de groupes, vous devez spécifier le délimiteur utilisé pour séparer leurs noms. Si le délimiteur est laissé vide, la valeur d'attribut peut contenir plusieurs nœuds XML contenant chacun un nom différent.*

Groupes disponibles

Permet à une liste de groupes prédéfinie d'être associée au fournisseur de sécurité. Cette liste peut ensuite être utilisée pour associer un groupe à la règle de groupe appropriée.

Règle de groupe par défaut

Chaque utilisateur qui s'authentifie auprès d'un serveur externe doit être membre d'au moins une règle de groupe pour pouvoir s'authentifier sur votre Secure Remote Access Appliance, en se connectant sur l'interface /login ou sur la console d'accès. Vous

pouvez sélectionner une règle de groupe par défaut à appliquer à tous les utilisateurs autorisés à s'authentifier auprès du serveur configuré.

Notez que si une règle par défaut est définie, alors n'importe quel utilisateur qui s'authentifie sur ce serveur peut potentiellement avoir accès au niveau de cette règle par défaut. Il est donc recommandé de définir le défaut sur une règle avec le minimum de privilèges, pour empêcher les utilisateurs d'obtenir des autorisations que vous ne souhaitez pas qu'ils aient.

Remarque : *si un utilisateur est dans une règle de groupe par défaut et qu'il est ensuite spécifiquement ajouté à une autre règle de groupe, les paramètres pour la règle spécifique prendront toujours le pas sur les paramètres par celle par défaut, même si la règle spécifique a une priorité plus basse que celle par défaut, et même si les paramètres de la règle par défaut n'autorisent pas le remplacement.*

Pour plus d'informations, veuillez consulter la section SAML pour l'authentification unique à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/security-providers/saml/index.htm.

Modifier le fournisseur de sécurité - SCIM

Remarque : *pour que SCIM fonctionne, l'API SCIM doit être activée sur un compte API, et l'API doit être configurée sur votre fournisseur SCIM. La gestion des comptes API se fait sous* ***/login > Gestion > Configuration API****. Pour le moment, un seul fournisseur SCIM peut être créé. Une fois un fournisseur SCIM créé, l'option SCIM n'est plus disponible dans le menu déroulant* ***Créer un fournisseur****. L'approvisionnement d'utilisateurs SCIM utilise des utilisateurs et des objets de groupe SCIM 2.0. Pour plus d'informations sur le standard SCIM 2.0 veuillez consulter http://www.simplecloud.info/*

Remarque : *L'accès à distance privilégié prend désormais en charge les API SCIM pour des groupes d'utilisateurs. Une fois que vous avez paramétré un fournisseur SCIM dans /login ainsi que des utilisateurs et des groupes configurés dans votre solution SCIM, PRA reflète les mêmes groupes que ceux qui sont présents dans votre solution SCIM, vous permettant de sélectionner des règles de groupe pour chaque groupe SCIM.*

Paramètres généraux

Nom

Créez un nom unique permettant d'identifier ce fournisseur.

Activé

Si cette case est cochée, votre Secure Remote Access Appliance peut chercher ce fournisseur de sécurité lorsqu'un utilisateur tente de se connecter. Si elle n'est pas cochée, le fournisseur ne sera pas recherché.

Identifiant de requête d'utilisateur SCIM

Dans le menu déroulant, sélectionnez l'identificateur unique que SCIM devrait utiliser pour les requêtes des utilisateurs.

Identifiant de requête de groupe SCIM

Dans le menu déroulant, sélectionnez l'identificateur unique que SCIM devrait utiliser pour les requêtes des groupes.

Paramètres d'approvisionnement de l'utilisateur

Attribut d'utilisateur

Ces attributs sont utilisés pour approvisionner les utilisateurs à travers BeyondTrust. Les valeurs par défaut correspondent aux applications certifiées par BeyondTrust avec différents fournisseurs d'identité.

Paramètres d'autorisation

Identificateur unique

Saisissez l'attribut SCIM à utiliser en tant qu'identificateur unique au sein de BeyondTrust.

Règle de groupe par défaut

Chaque utilisateur qui s'authentifie auprès d'un serveur externe doit être membre d'au moins une règle de groupe pour pouvoir s'authentifier sur votre Secure Remote Access Appliance, en se connectant sur l'interface /login ou sur la console d'accès. Vous pouvez sélectionner une règle de groupe par défaut à appliquer à tous les utilisateurs autorisés à s'authentifier auprès du serveur configuré.

Notez que si une règle par défaut est définie, alors n'importe quel utilisateur qui s'authentifie sur ce serveur peut potentiellement avoir accès au niveau de cette règle par défaut. Il est donc recommandé de définir le défaut sur une règle avec le minimum de privilèges, pour empêcher les utilisateurs d'obtenir des autorisations que vous ne souhaitez pas qu'ils aient.

> ***Remarque :*** *si un utilisateur est dans une règle de groupe par défaut et qu'il est ensuite spécifiquement ajouté à une autre règle de groupe, les paramètres pour la règle spécifique prendront toujours le pas sur les paramètres par celle par défaut, même si la règle spécifique a une priorité plus basse que celle par défaut, et même si les paramètres de la règle par défaut n'autorisent pas le remplacement.*

Nom d'attribut

Saisissez le nom de l'attribut SCIM qui identifie les utilisateurs de façon unique.

Les groupes approvisionnés avec SCIM sont toujours identifiés de manière unique sans sensibilité à la casse grâce à leur nom pour les recherches de groupe.

Règles de session : configuration de règles de demande et d'autorisation de session

Règles de session

Les règles de session permettent de personnaliser les autorisations de sécurité des sessions pour correspondre à des scénarios spécifiques. Les règles de session peuvent être appliquées aux utilisateurs et aux Jump Clients.

La section **Règles de session** répertorie toutes les règles disponibles. Cliquez sur la flèche à côté du nom d'une règle pour voir rapidement où cette règle est utilisée, sa disponibilité pour les utilisateurs, les invitations d'accès et les Jump Clients, et les outils configurés.

Ajouter, modifier ou supprimer une règle de session

Créer une nouvelle règle, modifier ou supprimer une règle existante.

Copier

Pour accélérer la création de règles de groupe semblables, cliquez sur **Copier** pour créer une nouvelle règle avec des réglages identiques. Vous pouvez ensuite modifier cette nouvelle règle pour répondre à vos exigences spécifiques.

Ajouter ou modifier une règle de session

Nom affiché

Créez un nom unique permettant d'identifier cette règle. Ce nom facilite l'assignation d'une règle de session aux utilisateurs et aux Jump Clients.

Nom de code

Définissez également un nom de code, qui sera utilisé à des fins d'intégration. Dans le cas contraire, le système en crée un automatiquement.

Description

Ajoutez une brève description pour résumer la fonction de cette règle. La description s'affiche lors de l'application d'une règle à des comptes utilisateur, règles de groupe et invitations d'accès.

Disponibilité

Utilisateurs

Choisissez si cette règle peut être attribuée à des utilisateurs (comptes d'utilisateurs et règles de groupe).

Invitation d'accès

Choisissez si cette règle peut être sélectionnée par les utilisateurs lors de l'invitation d'utilisateurs externes à rejoindre une session.

Éléments de Jump

Choisissez si cette règle peut être associée à un élément de Jump.

Dépendants

Si cette règle de session est déjà utilisée, vous verrez le nombre d'utilisateurs et de Jump Clients utilisant cette règle.

Autorisations

Vous pouvez choisir d'activer ou de désactiver toutes les autorisations suivantes, ou encore de les définir sur **Non défini**. Les règles de session sont appliquées à une session de manière hiérarchisée, les Jump Clients étant prioritaires, suivis des utilisateurs, et enfin de la règle globale par défaut. S'il existe plusieurs règles s'appliquant à une session, la règle présentant la priorité la plus haute prévaut sur toutes les autres. Par exemple, si la règle appliquée à un Jump Client définit une autorisation, alors aucune autre règle ne peut modifier cette autorisation pour la session. Pour qu'une autorisation puisse être définie par une règle de niveau inférieur, elle doit être définie sur **Non défini**.

Indiquez les outils d'assistance technique devant être activés ou désactivés avec cette règle.

Partage d'écran

Règles de partage d'écran

Permet à l'utilisateur de voir ou de contrôler l'écran distant. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

Restrictions de point de terminaison autorisées

Définissez si l'utilisateur peut interrompre l'entrée souris et clavier du système distant. L'utilisateur peut aussi empêcher l'affichage du bureau distant.

Restrictions de partage d'applications

Limiter l'accès aux applications spécifiées sur le système distant avec **N'autoriser que les exécutables répertoriés** ou **Ne refuser que les exécutables répertoriés**. Vous pouvez aussi choisir d'autoriser ou de refuser l'accès au bureau.

> ***Remarque :*** *cette fonction ne s'applique qu'aux systèmes d'exploitation Windows et Linux et n'inclut pas les sessions Remote Desktop Protocol (RDP) ou VNC.*

Ajouter des exécutables

Si des restrictions de partage d'application sont imposées, un bouton **Ajouter des exécutables** apparaît. Cliquer sur ce bouton ouvre un dialogue qui vous permet de spécifier quels exécutables autoriser ou refuser, en fonction de vos objectifs.

Après avoir ajouté des exécutables, un ou deux tableaux affichent les noms ou hachages de fichier que vous avez sélectionnés pour la restriction. Un champ de commentaire modifiable permet d'écrire des notes d'administration.

Entrer les noms de fichier ou hachages SHA-256 (un par ligne)

Lorsque vous restreignez des exécutables, saisissez manuellement les noms ou hachages des fichiers exécutables que vous souhaitez autoriser ou refuser. Cliquez sur **Ajouter des exécutables** lorsque vous avez terminé pour ajouter les fichiers choisis à votre configuration.

Vous pouvez saisir jusqu'à 25 fichiers par dialogue. Si vous avez besoin d'en ajouter davantage, cliquez sur **Ajouter des exécutables** puis rouvrez le dialogue.

Rechercher un ou plusieurs fichiers

Lorsque vous restreignez des exécutables, sélectionnez cette option pour parcourir votre système et choisir les fichiers exécutables pour obtenir automatiquement leurs noms ou hachages. Si vous sélectionnez des fichiers de votre plate-forme locale et du système de cette manière, assurez-vous que les fichiers sont bien des exécutables. Aucune vérification au niveau du navigateur n'est effectuée.

Choisissez **Utiliser le nom de fichier** ou **Utiliser le hachage de fichier** pour que le navigateur obtienne les noms ou hachages des fichiers exécutables automatiquement. Cliquez sur **Ajouter des exécutables** lorsque vous avez terminé pour ajouter les fichiers choisis à votre configuration.

Vous pouvez saisir jusqu'à 25 fichiers par dialogue. Si vous avez besoin d'en ajouter davantage, cliquez sur **Ajouter des exécutables** puis rouvrez le dialogue.

> ***Remarque :*** *cette option n'est disponible que dans les navigateurs modernes, pas dans les navigateurs plus anciens.*

Autorisé à se connecter à l'aide d'informations d'authentification venant d'un gestionnaire d'informations d'authentification de point de terminaison

Activez la connexion d'un utilisateur à votre gestionnaire d'informations d'authentification de point de terminaison pour utiliser les informations d'authentification de vos magasins ou banques de mot de passe existants.

L'utilisation du gestionnaire d'informations d'authentification de point de terminaison nécessite un accord de services séparé avec BeyondTrust. Une fois qu'un accord de services est en place, vous pouvez télécharger le middleware requis auprès du portail d'assistance technique BeyondTrust.

> ***Remarque :*** *avant la version 15.2, cette fonction n'est disponible que dans les sessions lancées depuis un Jump Client aux droits accrus sur Windows®. À partir de la version 15.2, vous pouvez également utiliser un gestionnaire d'informations d'authentification de point de terminaison dans les sessions de Jump distants, les sessions de protocole de bureau à distance Microsoft®, les sessions VNC et les sessions de Shell Jump. Vous pouvez aussi utiliser cette fonction avec l'action Exécuter en tant que spécial dans une session de partage d'écran sur un système Windows®.*

Annotations

Règles d'annotation

Permet à l'utilisateur d'utiliser les outils d'annotation pour dessiner sur l'écran du système distant. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

Transfert de fichiers

Règles de transfert de fichiers

Permet à l'utilisateur d'envoyer des fichiers vers le système distant, de télécharger des fichiers depuis le système distant, ou les deux. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

Chemins accessibles sur le système de fichiers du point de terminaison

Permettre à l'utilisateur de transférer des fichiers de et vers n'importe quel répertoire sur le système distant ou uniquement les répertoires spécifiés.

Chemins accessibles sur le système de fichiers de l'utilisateur

Permettre à l'utilisateur de transférer des fichiers de et vers n'importe quel répertoire sur son système local ou uniquement les répertoires spécifiés.

Interpréteur de commandes

Règles de l'interpréteur de commandes

Permet à l'utilisateur de saisir des commandes sur l'ordinateur distant par l'intermédiaire d'une interface en ligne de commande virtuelle. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

Remarque : *l'accès à l'interpréteur de commandes ne peut pas être restreint lors de sessions de Shell Jump.*

Configurez le filtrage des commandes pour empêcher l'utilisation accidentelle de commandes pouvant endommager les systèmes des points de terminaison.

Pour plus d'informations sur le filtrage de commandes, veuillez consulter la section Utiliser un Shell Jump pour accéder à un appareil réseau distant à l'adresse www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/shell-jump.htm.

Informations système

Règles relatives aux informations système

Permet à l'utilisateur de consulter les informations système de l'ordinateur distant. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

Autorisé à utiliser les actions relatives aux informations système

Permet à l'utilisateur d'interagir avec les processus et les programmes sur le système distant sans avoir recours au partage d'écran. Le technicien d'assistance peut ainsi désinstaller des programmes, supprimer des processus ou encore démarrer, arrêter, mettre en

pause, reprendre et redémarrer des services.

Accès au registre

Règles d'accès au registre

Permet à l'utilisateur d'agir sur le registre d'un système Windows distant sans avoir recours au partage d'écran. Le technicien d'assistance peut ainsi afficher, ajouter, supprimer, modifier, rechercher et importer/exporter des clés.

Scripts prédéfinis

Règles de script prédéfini

Permet à l'utilisateur d'exécuter des scripts prédéfinis créés pour ses équipes. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

Exporter la règle

Vous pouvez exporter une règle de session à partir d'un site et importer ces autorisations dans une règle sur un autre site. Modifiez la règle que vous souhaitez exporter et faites défiler jusqu'au bas de la page. Cliquez sur **Exporter la règle** et enregistrez le fichier.

Importer une règle

Vous pouvez importer ces paramètres de règles vers les autres sites BeyondTrust prenant en charge l'importation de règles de session. Créez une nouvelle règle de session, puis accédez au bas de la page. Naviguez jusqu'au fichier de la règle, puis cliquez sur **Importer la règle**. Une fois le fichier de la règle chargé, la page s'actualisera pour vous permettre d'effectuer des modifications. Cliquez alors sur **Enregistrer la règle** pour rendre la règle disponible.

Enregistrer

Cliquez sur **Enregistrer** pour rendre la règle disponible.

Simulateur de règle de session

La priorisation des règles pouvant s'avérer complexe, vous pouvez utiliser le **simulateur de règle de session** pour déterminer le résultat. Vous pouvez également utiliser ce simulateur pour déterminer pourquoi une autorisation n'est pas disponible alors qu'elle devrait l'être.

Utilisateur

Commencez en sélectionnant l'utilisateur effectuant la session. Cette liste déroulante inclut les comptes utilisateur et les règles d'invitation d'accès.

Méthode de démarrage de session

Sélectionnez la méthode de démarrage de la session.

Jump Client/raccourci de Jump

Recherchez un Jump Client ou un raccourci de Jump par nom, commentaires, groupe de Jump ou balise.

Simuler

Cliquez sur **Simuler**. La zone située en dessous affiche en lecture seule les autorisations configurables par règle de session. Vous pouvez ainsi voir quelles autorisations sont accordées ou refusées d'après la hiérarchie de règles, ainsi que la règle associée à chaque autorisation.

Règles de groupe : application d'autorisations utilisateur à des groupes d'utilisateurs

Règles de groupe

La page **Règles de groupe** vous permet de définir des groupes d'utilisateurs qui partagent des privilèges communs.

Ajouter une nouvelle règle, modifier, supprimer

Créer une nouvelle règle, modifier ou supprimer une règle existante.

Modifier l'ordre

Cliquez sur ce bouton pour faire glisser et déposer les règles de groupe afin de définir leur priorité. Cliquez sur **Enregistrer l'ordre** pour que les changements de priorité prennent effet. Pour des raisons de gestion, l'ordre de priorité recommandé consiste à définir des règles pour des groupes d'utilisateurs plus spécifiques avec une priorité élevée (empêchant le remplacement), puis de définir des groupes de plus en plus larges avec une priorité inférieure.

Copier

Pour accélérer la création de règles de groupe semblables, cliquez sur **Copier** pour créer une nouvelle règle avec des réglages identiques. Vous pouvez ensuite modifier cette nouvelle règle pour répondre à vos exigences spécifiques.

Ajouter ou modifier une règle

Nom de la règle

Créez un nom unique permettant d'identifier cette règle.

Membres disponibles et membres de la règle

Pour attribuer des membres, cliquez sur le bouton **Ajouter** pour ouvrir une zone de sélection. Sélectionnez des utilisateurs dans votre système local, ou sélectionnez des utilisateurs ou des groupes entiers à partir des fournisseurs de sécurité configurés. Pour ajouter des utilisateurs et des groupes d'un magasin d'annuaires externe comme un LDAP, RADIUS ou Kerberos, vous devez d'abord configurer la connexion sur la page **/login > Utilisateurs et sécurité > Fournisseurs de sécurité**. Si une tentative d'ajout d'un utilisateur d'un fournisseur de sécurité configuré n'est pas valide, le message d'erreur de journal de synchronisation apparaîtra ici et dans le journal.

Paramètres du compte

Quels paramètres de compte cette règle de groupe doit-elle contrôler ?

Pour chaque paramètre, déterminez s'il est défini dans cette règle ou librement disponible à la configuration pour des utilisateurs individuels. Si cela est défini, vous ne pourrez pas modifier ce privilège pour un utilisateur individuel depuis la page de son compte utilisateur.

Si vous avez une règle qui définit une autorisation et que vous ne voulez pas que n'importe quelle règle puisse remplacer cette autorisation, vous devez indiquer que cette autorisation ne peut pas être remplacée, et la règle doit avoir une priorité supérieure à celle des autres règles qui définissent également ce paramètre.

Authentification à deux facteurs

L'authentification à deux facteurs (2FA) fait appel à une application d'authentification pour créer un code unique limité dans le temps et se connecter à l'interface d'administration et à la console d'accès. Lorsque **Requis** est sélectionné, l'utilisateur est invité à s'inscrire et à se servir de l'authentification 2FA à sa prochaine connexion. Lorsque **Optionnel** est sélectionné, l'utilisateur a la possibilité d'utiliser l'authentification 2FA, mais il n'y est pas contraint.

> ***Remarque :*** *Les utilisateurs qui se connectaient à l'aide de codes obtenus par e-mail passent automatiquement à l'authentification 2FA. Ils ont toutefois la possibilité d'utiliser des codes e-mail jusqu'à ce qu'ils soient inscrits sur une application. Après une première utilisation de 2FA, l'option du code e-mail n'est plus disponible.*

Expiration du compte

Lorsque cette case est cochée, le compte n'expire jamais. Lorsque cette case n'est pas cochée, une date d'expiration du compte doit être définie.

Activation du compte

Vous permet de désactiver le compte pour que l'utilisateur ne puisse plus se connecter. Une désactivation ne supprime PAS le compte.

Commentaires

Ajoutez des commentaires pour aider à identifier la fonction de cet objet.

Autorisations générales

Quels paramètres globaux cette règle de groupe doit-elle contrôler ?

Pour chaque paramètre, déterminez s'il est défini dans cette règle ou librement disponible à la configuration pour des utilisateurs individuels. Si cela est défini, vous ne pourrez pas modifier ce privilège pour un utilisateur individuel depuis la page de son compte utilisateur.

Si vous avez une règle qui définit une autorisation et que vous ne voulez pas que n'importe quelle règle puisse remplacer cette autorisation, vous devez indiquer que cette autorisation ne peut pas être remplacée, et la règle doit avoir une priorité supérieure à celle des autres règles qui définissent également ce paramètre.

Administration

Privilèges administratifs

Accorde des droits d'administration complets à l'utilisateur.

Privilèges administratifs Vault

Autorise l'accès de l'utilisateur à Vault.

Paramètres de mot de passe

Permet à l'utilisateur de définir des mots de passe et de débloquer des comptes pour les utilisateurs locaux ne disposant pas de droits d'administrateur.

Modification d'un Jumpoint

Permet à l'utilisateur de créer ou de modifier des Jumpoints. Cette option n'affecte pas la capacité de l'utilisateur à accéder à des ordinateurs distants via un Jumpoint, qui est configurée par Jumpoint ou règle de groupe.

Modification d'équipe

Permet à l'utilisateur de créer ou de modifier des équipes.

Modification d'un groupe de Jump

Permet à l'utilisateur de créer ou de modifier les groupe de Jump.

Modification de script prédéfini

Permet à l'utilisateur de créer ou de modifier des scripts prédéfinis en vue de les utiliser dans des sessions de partage d'écran ou d'interpréteur de commandes.

Modification de lien personnalisé

Permet à l'utilisateur de créer ou de modifier des liens personnalisés.

Rapport en cours

Accès aux sessions et rapports d'équipe

Permet à l'utilisateur d'afficher les rapports de session d'accès. Selon l'option sélectionnée, les utilisateurs peuvent afficher leurs sessions, leurs sessions de groupe de saut ou toutes les sessions.

Autorisé à consulter les rapports sur les sessions d'accès

Permet à l'utilisateur d'établir des rapports sur l'activité des session d'accès, en visualisant uniquement les sessions pour lesquelles il était le propriétaire principal de la session, uniquement les sessions pour les points de terminaison appartenant à un groupe de Jump dont l'utilisateur est membre, ou toutes les sessions.

Autorisé à voir les enregistrements de session d'accès

Permet à l'utilisateur de lire les enregistrements vidéo des sessions de partage d'écran et des sessions d'interpréteur de commandes.

Accès aux rapports Vault

Permet à l'utilisateur d'acceder aux rapportsVault. Selon l'option sélectionnée, les utilisateurs peuvent afficher leurs sessions ou toutes les sessions.

Autorisé à consulter les rapports Vault

Permet à l'utilisateur de consulter ses propres événements Vault ou tous les événements Vault.

Autorisations d'accès

Autorisé à accéder aux points de terminaison

Permet à l'utilisateur d'utiliser la console d'accès pour exécuter des sessions. Si l'accès au point de terminaison est activé, les options relatives à l'accès au point de terminaison seront également disponibles.

Gestion de session

Autorisé à partager les sessions avec des équipes auxquelles il n'appartient pas

Permet à l'utilisateur d'inviter un ensemble moins limité d'utilisateurs pour partager des sessions, pas seulement des membres de son équipe. Combinée à la permission de disponibilité étendue, cette permission développe les capacités de partage de session.

Autorisé à inviter des utilisateurs externes

Permet à l'utilisateur d'inviter un utilisateur tiers à participer à une session de manière ponctuelle.

Autorisé à activer le mode disponibilité étendue

Permet à l'utilisateur de recevoir des invitations par e-mail de la part d'autres utilisateurs demandant de partager une session, même lorsqu'il n'est pas connecté à la console d'accès.

Autorisé à modifier la clé externe

Permet à l'utilisateur de modifier la clé externe depuis le volet d'informations d'une session dans la console d'accès.

Partage d'écran d'utilisateur à utilisateur

Autorisé à montrer son écran aux autres utilisateurs

Permet à l'utilisateur de partager son écran avec un autre utilisateur sans que l'utilisateur récepteur ait besoin de rejoindre une session. Cette option est disponible même si l'utilisateur n'est pas dans une session.

Autorisé à accorder le contrôle lorsqu'il montre son écran à d'autres utilisateurs

Permet à l'utilisateur partageant son écran d'accorder le contrôle de son clavier et de sa souris à l'utilisateur regardant son écran.

Technologie Jump

Méthodes d'élément de Jump autorisées

Permet à l'utilisateur d'effectuer un Jump vers des ordinateurs en utilisant les **Jump Clients**, les **Jump locaux sur le réseau local**, les **Jump distants avec un Jumpoint**, les **VNC distants avec un Jumpoint**, les **RDP distants avec un Jumpoint**, les **Jump Web avec un Jumpoint**, les **Shell Jump avec un Jumpoint** et les **Jump en tunnel par protocole avec un Jumpoint**.

Rôles d'élément de Jump

Le rôle d'élément de Jump est un ensemble prédéfini d'autorisations relatives à la gestion et à l'utilisation d'un élément de Jump. Pour chaque paramètre, cliquez sur **Afficher** pour ouvrir le rôle d'élément de Jump dans un nouvel onglet.

Le rôle **Par défaut** n'est utilisé que lorsque **Utiliser les paramètres par défaut de l'utilisateur** est défini pour cet utilisateur dans un groupe de Jump.

Le rôle **Personnel** ne s'applique qu'aux éléments de Jump attachés à la liste personnelle d'éléments de Jump d'un utilisateur.

Le rôle **Équipe** ne s'applique qu'aux éléments de Jump attachés à la liste personnelle d'éléments de Jump d'un membre de l'équipe doté d'un rôle inférieur. Ainsi, un chef d'équipe peut visualiser les éléments de Jump d'un responsable ou d'un membre de son équipe, et un responsable d'équipe peut visualiser les éléments de Jump personnels d'un membre de son équipe.

Le rôle **Système** s'applique au reste des éléments de Jump du système. Pour la plupart des utilisateurs, ce rôle est en principe défini sur **Aucun accès**. S'il est défini sur une autre option, l'utilisateur est ajouté à des groupes de Jump auxquels il ne devrait pas être assigné, et, dans la console d'accès, il est en mesure de visualiser la liste personnelle d'éléments de Jump de membres n'appartenant pas à son équipe.

autonomes et non autonomes

Définissez les règles de demande et d'autorisation devant s'appliquer aux sessions de cet utilisateur. Sélectionnez une règle de session existante ou définissez des autorisations personnalisées pour cet utilisateur. Notez que l'option **Non défini** entraîne l'utilisation de la règle globale par défaut. Ces autorisations peuvent être remplacées par une règle de niveau supérieur.

Description

Affichez la description d'une règle de permission de session prédéfinie.

Partage d'écran

Règles de partage d'écran

Permet à l'utilisateur de voir ou de contrôler l'écran distant. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

> Pour plus d'informations, veuillez consulter la section Contrôler le point de terminaison à distance avec partage d'écran à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/screen-sharing.htm.

Restrictions de partage d'applications

Limiter l'accès aux applications spécifiées sur le système distant avec **N'autoriser que les exécutables répertoriés** ou **Ne refuser que les exécutables répertoriés**. Vous pouvez aussi choisir d'autoriser ou de refuser l'accès au bureau.

> ***Remarque :*** *cette fonction ne s'applique qu'aux systèmes d'exploitation Windows et Linux et n'inclut pas les sessions Remote Desktop Protocol (RDP) ou VNC.*

Ajouter des exécutables

Si des restrictions de partage d'application sont imposées, un bouton **Ajouter des exécutables** apparaît. Cliquer sur ce bouton ouvre un dialogue qui vous permet de spécifier quels exécutables autoriser ou refuser, en fonction de vos objectifs.

Après avoir ajouté des exécutables, un ou deux tableaux affichent les noms ou hachages de fichier que vous avez sélectionnés pour la restriction. Un champ de commentaire modifiable permet d'écrire des notes d'administration.

Entrer les noms de fichier ou hachages SHA-256 (un par ligne)

Lorsque vous restreignez des exécutables, saisissez manuellement les noms ou hachages des fichiers exécutables que vous souhaitez autoriser ou refuser. Cliquez sur **Ajouter des exécutables** lorsque vous avez terminé pour ajouter les fichiers choisis à votre configuration.

Vous pouvez saisir jusqu'à 25 fichiers par dialogue. Si vous avez besoin d'en ajouter davantage, cliquez sur **Ajouter des exécutables** puis rouvrez le dialogue.

Rechercher un ou plusieurs fichiers

Lorsque vous restreignez des exécutables, sélectionnez cette option pour parcourir votre système et choisir les fichiers exécutables pour obtenir automatiquement leurs noms ou hachages. Si vous sélectionnez des fichiers de votre plate-forme locale et du système de cette manière, assurez-vous que les fichiers sont bien des exécutables. Aucune vérification au niveau du navigateur n'est effectuée.

Choisissez **Utiliser le nom de fichier** ou **Utiliser le hachage de fichier** pour que le navigateur obtienne les noms ou hachages des fichiers exécutables automatiquement. Cliquez sur **Ajouter des exécutables** lorsque vous avez terminé pour ajouter les fichiers choisis à votre configuration.

Vous pouvez saisir jusqu'à 25 fichiers par dialogue. Si vous avez besoin d'en ajouter davantage, cliquez sur **Ajouter des exécutables** puis rouvrez le dialogue.

> ***Remarque :*** *cette option n'est disponible que dans les navigateurs modernes, pas dans les navigateurs plus anciens.*

Restrictions de point de terminaison autorisées

Définissez si l'utilisateur peut interrompre l'entrée souris et clavier du système distant. L'utilisateur peut aussi empêcher l'affichage du bureau distant.

> Pour plus d'informations, veuillez consulter la section Contrôler le point de terminaison à distance avec partage d'écran à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/screen-sharing.htm.

Annotations

Règles d'annotation

Permet à l'utilisateur d'utiliser les outils d'annotation pour dessiner sur l'écran du système distant. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

> Pour plus d'informations, veuillez consulter la section Utilisez les annotations pour dessiner sur l'écran distant du point de terminaison à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/annotations.htm.

Transfert de fichiers

Règles de transfert de fichiers

Permet à l'utilisateur d'envoyer des fichiers vers le système distant, de télécharger des fichiers depuis le système distant, ou les deux. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

Chemins accessibles sur le système de fichiers du point de terminaison

Permettre à l'utilisateur de transférer des fichiers de et vers n'importe quel répertoire sur le système distant ou uniquement les répertoires spécifiés.

Chemins accessibles sur le système de fichiers de l'utilisateur

Permettre à l'utilisateur de transférer des fichiers de et vers n'importe quel répertoire sur son système local ou uniquement les répertoires spécifiés.

> Pour plus d'informations, veuillez consulter la section Transfert de fichiers vers et depuis le point de terminaison de système distant à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/file-transfer.htm.

Interpréteur de commandes

Règles de l'interpréteur de commandes

Permet à l'utilisateur de saisir des commandes sur l'ordinateur distant par l'intermédiaire d'une interface en ligne de commande virtuelle. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

> ***Remarque :*** *l'accès à l'interpréteur de commandes ne peut pas être restreint lors de sessions de Shell Jump.*

Configurez le filtrage des commandes pour empêcher l'utilisation accidentelle de commandes pouvant endommager les systèmes des points de terminaison.

Pour plus d'informations sur le filtrage de commandes, veuillez consulter la section Utiliser un Shell Jump pour accéder à un appareil réseau distant à l'adresse www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/shell-jump.htm.

Pour plus d'informations, veuillez consulter la section Ouvrir l'interpréteur de commandes sur le point de terminaison distant en utilisant la console d'accès à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/command-shell.htm.

Informations système

Règles relatives aux informations système

Permet à l'utilisateur de consulter les informations système de l'ordinateur distant. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

Autorisé à utiliser les actions relatives aux informations système

Permet à l'utilisateur d'interagir avec les processus et les programmes sur le système distant sans avoir recours au partage d'écran. Le technicien d'assistance peut ainsi désinstaller des programmes, supprimer des processus ou encore démarrer, arrêter, mettre en pause, reprendre et redémarrer des services.

Pour plus d'informations, veuillez consulter la section Consulter les informations système sur le point de terminaison distant à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/system-info.htm.

Accès au registre

Règles d'accès au registre

Permet à l'utilisateur d'agir sur le registre d'un système Windows distant sans avoir recours au partage d'écran. Le technicien d'assistance peut ainsi afficher, ajouter, supprimer, modifier, rechercher et importer/exporter des clés.

Pour plus d'informations, veuillez consulter la section Accès à l'éditeur de registre distant sur le point de terminaison distant à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/registry-editor.htm.

Scripts prédéfinis

Règles de script prédéfini

Permet à l'utilisateur d'exécuter des scripts prédéfinis créés pour ses équipes. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

> Pour plus d'informations, veuillez consulter la section Ouvrir l'interpréteur de commandes sur le point de terminaison distant en utilisant la Console d'Accès à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/command-shell.htm.

Paramètres de disponibilité

Planning de connexion

Restreindre la connexion de l'utilisateur selon le planning suivant

Définissez un planning afin de déterminer les périodes pendant lesquelles les utilisateurs peuvent se connecter à la console d'accès. Définissez le fuseau horaire à utiliser pour ce planning, puis ajoutez une ou plusieurs entrées de planification. Pour chaque entrée, indiquez l'heure et la date de début ainsi que l'heure et la date de fin.

Par exemple, si la période définie commence à 8 h et se termine à 17 h, un utilisateur peut se connecter à n'importe quel moment au cours de cette période et peut continuer à travailler passée l'heure de fin. Il ne sera toutefois pas autorisé à se reconnecter après 17 h.

Forcer la déconnexion lorsque le planning ne permet pas l'ouverture d'une session

Si un contrôle d'accès plus strict est requis, cochez cette option. Ceci force la déconnexion de l'utilisateur à l'heure de fin définie. Dans ce cas, l'utilisateur reçoit des notifications récurrentes à partir de 15 minutes avant d'être déconnecté. Lorsque l'utilisateur est déconnecté, toutes les sessions possédées suivront les règles de récupération.

Composition

Ajouter une appartenance à des équipes

Lancez une recherche pour trouver les équipes auxquelles les membres de cette règle de groupe devraient appartenir. Vous pouvez définir les rôles **Membre de l'équipe**, **Chef d'équipe** ou **Responsable d'équipe**. Ces rôles représentent une part significative de la fonction **Tableau de bord** de la console d'accès. Cliquez sur **Ajouter**.

Les équipes ajoutées figurent dans un tableau. Il est possible de modifier le rôle d'un membre d'une équipe ou de supprimer l'équipe de la liste.

Supprimer une appartenance à des équipes

Recherchez les équipes dont les membres de cette règle de groupe devraient être supprimés, puis cliquez sur **Ajouter**. Les équipes supprimées figurent dans un tableau. Il est possible de supprimer une équipe de la liste.

Ajouter une appartenance à un Jumpoint

Recherchez les Jumpoints auxquels les membres de cette règle de groupe devraient pouvoir accéder, puis cliquez sur **Ajouter**. Les Jumpoints ajoutés figurent dans un tableau. Il est possible de supprimer un Jumpoint de la liste.

Supprimer une appartenance à un Jumpoint

Recherchez les Jumpoints dont les membres de cette règle de groupe ne devraient pas être supprimés, puis cliquez sur **Ajouter**. Les Jumpoints supprimés figurent dans un tableau. Il est possible de supprimer un Jumpoint de la liste.

Ajouter des appartenances de groupe de Jump

Recherchez les groupes de Jump auxquels les membres de cette règle de groupe devraient appartenir. Il est possible de paramétrer le rôle d'élément de Jump de chaque utilisateur pour définir son type d'autorisation vis-à-vis des éléments de Jump dans ce groupe de Jump. Vous pouvez aussi utiliser les rôles d'élément de Jump par défaut de l'utilisateur définis dans cette règle de groupe ou sur la page **Utilisateurs et sécurité > Utilisateurs**. Le rôle d'élément de Jump est un ensemble prédéfini d'autorisations relatives à la gestion et à l'utilisation d'un élément de Jump.

> Pour plus d'informations, veuillez consulter la section Utiliser les rôles d'éléments de Jump pour configurer les groupes d'autorisation des éléments de Jump à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/how-to/jumpoint/jump-item-roles.htm.

Vous pouvez aussi appliquer une règle de Jump pour gérer l'accès aux éléments de Jump dans ce groupe de Jump. Si vous sélectionnez **Défini sur les éléments de Jump**, la règle de Jump sera appliquée à l'élément de Jump lui-même. Les règles de Jump sont configurées sur la page **Jump > Règles de Jump** et déterminent les périodes pendant lesquelles un utilisateur peut accéder à cet élément de Jump. Une règle de Jump peut également envoyer une notification lorsqu'on y accède, ou peut exiger l'approbation pour l'accès. Si aucune règle de Jump n'est appliquée pour l'utilisateur ou l'élément de Jump, cet élément de Jump est accessible sans restriction.

> Pour plus d'informations, veuillez consulter la section Créer des règles de Jump pour contrôler l'accès aux éléments de Jump à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/how-to/jumpoint/policies.htm.

Les groupe de Jump ajoutés figurent dans un tableau. Il est possible de modifier les paramètres d'un groupe de Jump ou de supprimer le groupe de Jump de la liste.

Supprimer des appartenances de groupe de Jump

Recherchez les groupes de Jump dont les membres de cette règle de groupe devraient être supprimés, puis cliquez sur **Ajouter**. Les groupe de Jump supprimés figurent dans un tableau. Il est possible de supprimer un groupe de Jump de la liste.

Ajouter des appartenances à un compte Vault

Les utilisateurs peuvent voir leurs appartenances de groupe ajoutées par d'autres comptes Vault. Consultez les **comptes Vault** pour voir tous les membres de chaque groupe. Il est possible d'assigner aux comptes Vault l'un des deux rôles :

- **Injecter** (valeur par défaut) : Les utilisateurs dotés de ce rôle peuvent utiliser ce compte dans des sessions Privileged Remote Access.
- **Injecter et extraire** : Les utilisateurs dotés de ce rôle peuvent utiliser ce compte dans des sessions Privileged Remote Access et peuvent extraire le compte sur **/login**. L'autorisation d'**extraction** n'a pas d'effet sur les comptes génériques SSH.

> ***Remarque :*** *Activez l'autorisation* ***Ajouter des appartenances à un compte Vault*** *pour assigner un* ***rôle de compte Vault*** *dans une règle de groupe. Le* ***rôle de compte Vault*** *est visible dans la liste des comptes ajoutés à la règle de groupe.*

Enregistrer

Cliquez sur **Enregistrer la règle** pour activer la règle.

Exporter la règle

Vous pouvez exporter une règle de groupe à partir d'un site et importer ces autorisations dans une règle sur un autre site. Modifiez la règle que vous souhaitez exporter et faites défiler jusqu'au bas de la page. Cliquez sur **Exporter la règle** et enregistrez le fichier.

> ***Remarque :*** *lors de l'exportation d'une règle de groupe, seuls le nom de la règle, les paramètres du compte et les autorisations sont exportés. Les membres de la règle, les appartenances à des équipes et des Jumpoints ne sont pas inclus dans l'exportation.*

Importer une règle

Vous pouvez importer des paramètres de règles de groupe exportés dans les autres sites BeyondTrust prenant en charge l'importation de règles de groupe. Créez une nouvelle règle de groupe ou modifiez une règle existante dont vous souhaitez remplacer les autorisations, et faites défiler jusqu'à la section **Importer la règle** en bas de la page. Cliquez sur **Sélectionner un fichier de règle**, naviguez jusqu'au fichier de la règle, puis cliquez sur **Ouvrir**. Une fois le fichier de la règle chargé, la page s'actualisera pour vous permettre d'effectuer des modifications ; cliquez sur **Enregistrer** pour activer la règle de groupe.

> ***Remarque :*** *l'importation d'un fichier de règle dans une règle de groupe existante remplacera toutes les autorisations précédemment définies, sauf les membres de la règle, et les appartenances à des équipes et des Jumpoints.*

Keytab Kerberos : gestion du keytab Kerberos

Gestion du keytab Kerberos

BeyondTrust prend en charge une fonctionnalité d'authentification unique au moyen du protocole d'authentification Kerberos. Cela permet aux utilisateurs de s'authentifier sur le Secure Remote Access Appliance sans avoir à entrer leurs informations d'authentification. L'authentification Kerberos s'applique à la fois à l'interface Web /login et à la console d'accès.

Pour intégrer Kerberos à votre Secure Remote Access Appliance, Kerberos doit avoir été déployé ou être en cours de déploiement. Les conditions requises sont les suivantes :

- Vous devez avoir un centre de distribution de clés (KDC) opérationnel.
- Les horloges doivent être synchronisées sur tous les clients, le KDC et le Secure Remote Access Appliance. L'utilisation d'un serveur NTP (Network Time Protocol) est un moyen facile d'y parvenir.
- Vous devez avoir créé un nom principal du service (SPN) sur le KDC pour votre Secure Remote Access Appliance.

Noms principaux configurés

La section **Noms principaux configurés** répertorie tous les SPN disponibles pour chaque keytab transféré.

Une fois que des SPN sont disponibles, vous pouvez configurer un fournisseur de sécurité Kerberos depuis la page **Fournisseurs de sécurité** et définir les principaux utilisateurs pouvant s'authentifier sur le Secure Remote Access Appliance via Kerberos.

Importer un keytab

Transmettre le fichier

Exportez le keytab pour le SPN depuis votre KDC et chargez-le sur le Secure Remote Access Appliance dans la section **Importer un keytab** sur cette page.

Rapports

Accès : faites un rapport sur l'activité des sessions

Rapports d'accès

Les administrateurs et les utilisateurs avec privilèges peuvent générer de vastes rapports exhaustifs et appliquer des filtres spécifiques en vue de personnaliser les informations contenues dans les rapports en fonction des besoins précis.

Type de rapport

Générez des rapports d'activité d'après trois types de rapports distincts : **Session**, **Résumé** et **Preuves de session** (si l'option est activée).

Rapport de session

Voir toutes les sessions d'accès qui correspondent aux critères spécifiés dans les filtres de rapport. Les rapports de session comprennent des informations de session de base, ainsi que des liens vers les détails de session, les transcriptions de la messagerie instantanée, et les enregistrements vidéo des sessions de partage d'écran, de Jump en tunnel par protocole et d'interpréteur de commandes.

Les rapports de session détaillent la transcription complète de la discussion, le nombre de fichiers transférés et les actions spécifiques ayant été effectuées lors de la session. Les évènements de fenêtres qui présentent des changements visuels évidents dans une session sont capturés en tant qu'évènements dans les détails de session. Ceci inclut principalement les changements de fenêtre de premier plan, avec le nom de l'exécutable et le titre de sa fenêtre.

Les autres informations de session incluent la durée de la session, l'adresse IP des ordinateurs locaux et distants, et les informations sur le système distant (le cas échéant). Les rapports peuvent être consultés en ligne ou être téléchargés sur le système local.

Si l'enregistrement de session est activé, lisez une vidéo des sessions individuelles, avec une annotation précisant qui contrôlait la souris et le clavier à tout moment au cours de la session. Si l'enregistrement de Jump en tunnel par protocole est activé, consultez les enregistrements vidéo de tout le bureau de l'utilisateur. Si l'enregistrement de l'invite de commande est activé, consultez les enregistrements et/ou les transcriptions texte de tous les interpréteurs de commandes exécutés pendant la session. Tous les enregistrements sont conservés sur le serveur BeyondTrust dans un format brut et sont convertis dans un format compressé lors du visionnage ou du téléchargement.

Rapport récapitulatif

Les rapports récapitulatifs fournissent une vision d'ensemble de l'activité de session sur une certaine période, classée par utilisateur. Les statistiques regroupent le nombre total de sessions exécutées, le nombre moyen de sessions par jour de la semaine et leur durée moyenne.

Rapports de preuves de session :

Les rapports de preuves de sessions d'accès vous permettent de chercher des événements de session dans toutes les sessions d'accès, ainsi que de trouver des sessions contenant le texte ou la phrase indiqué dans le filtre. Cela permet de chercher dans les messages instantanés, les commandes d'interpréteur, les transferts de fichiers, les modifications du système de fichiers, les modifications de registre et les titres des fenêtres au premier plan.

Filtres

Appliquez des options de filtre selon les besoins en vue de générer des rapports encore plus personnalisés à partir des types de rapport de base. Activez un ou plusieurs filtres selon vos désirs, mais seules les sessions qui correspondent à tous les filtres sélectionnés s'afficheront.

Identifiant de session ou numéro de séquence

Cet identificateur unique exige que vous indiquiez l'identifiant (LSID) ou le numéro de séquence pour la session unique que vous recherchez. Ceci est souvent utile si vous possédez un système de tickets externe ou une intégration GRC. Vous ne pouvez pas combiner ce filtre à un autre.

Période

Sélectionnez une date de début pour l'extraction de données de rapport. Sélectionnez ensuite le nombre de jours pour lequel extraire votre rapport, ou une date de fin.

Point de terminaison

Filtrez les sessions par nom de l'ordinateur, adresse IP publique ou adresse IP privée.

Groupe de Jump

Filtrer les sessions par éléments de Jump appartenant à un groupe de Jump spécifique. Si cette option est sélectionnée, les options suivantes sont disponibles :

- Trouver toutes les sessions démarrées depuis des éléments de Jump appartenant à un groupe de Jump spécifique.
- Trouver toutes les sessions démarrées à partir d'éléments de Jump personnels pour un utilisateur spécifique.
- Trouver toutes les sessions dans votre groupe de Jump personnel.

Utilisateur

Sélectionnez un utilisateur depuis la case **Chercher un utilisateur** pour filtrer les sessions auxquelles un utilisateur spécifique a participé. Cochez **Correspond uniquement si l'utilisateur sélectionné est l'utilisateur principal pour la session** pour trouver uniquement les sessions dans lesquelles l'utilisateur était l'utilisateur principal.

Clé externe

Filtrez pour rapporter des sessions qui ont utilisé la même clé externe donnée.

N'inclure que les sessions terminées

Filtrez pour inclure uniquement les sessions qui ont été terminées. Ceci exclut les sessions toujours en cours.

Rapport sur l'activité d'équipe

Période

Sélectionnez une date de début pour l'extraction de données de rapport. Sélectionnez ensuite le nombre de jours pour lequel extraire votre rapport, ou une date de fin.

Équipe

Choisissez l'équipe dont vous souhaitez voir les journaux d'activité.

Affichez toutes les activités d'équipe qui correspondent aux critères spécifiés sur la page précédente. Les rapports d'activité d'équipe incluent des informations sur les utilisateurs lorsqu'ils se connectent et se déconnectent de la console d'accès, les messages instantanés échangés entre membres d'équipe, les actions de partage d'écran d'utilisateur à utilisateur telles qu'elles sont répertoriées dans la messagerie instantanée, et les fichiers partagés et téléchargés.

Vault : rapports sur le compte Vault et l'activité utilisateur

Rapport d'activité du compte Vault

Période

Sélectionnez une date de début pour l'extraction de données de rapport. Sélectionnez ensuite le nombre de jours pour lequel extraire votre rapport, ou une date de fin.

Compte

Pour voir tous les événements impliquant un compte Vault BeyondTrust stocké spécifique, saisissez le nom du compte, ou sélectionnez le compte dans la liste dynamique en fenêtre pop-up.

Utilisateur

Pour voir tous les événements impliquant un utilisateur privilégié spécifique, saisissez le nom d'utilisateur, ou sélectionnez le nom d'utilisateur dans la liste dynamique en fenêtre pop-up.

Pour plus d'informations, veuillez consulter le Livre blanc technique de BeyondTrust Vault à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/how-to/vault/index.htm.

Remarque : *si un utilisateur a été rendu anonyme en vue de satisfaire à des normes de conformité, le rapport d'**activité du compte Vault** pourrait afficher des pseudonymes pour les données utilisateurs ou indiquer que les informations ont été supprimées. Pour en savoir plus sur l'anonymisation des données et la suppression pour cause de mise en conformité, veuillez consulter la section Conformité : Anonymiser les données pour satisfaire aux normes de conformité à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/compliance.htm.*

Résultats de rapport d'activité de compte Vault

Étant donné que les utilisateurs peuvent obtenir un accès distinct pour utiliser et extraire des comptes, le **Rapport d'activité du compte Vault** distingue ces deux types d'activité. Cela permet aux administrateurs de faire la différence entre un utilisateur qui est en mesure d'afficher le mot de passe du compte et un utilisateur qui ne peut qu'injecter des informations d'identification dans une session.

Dans le **Rapport d'activité du compte Vault**, la colonne **Données** indique des informations associées avec l'événement. L'événement **Informations d'authentification extraites** contient un lien **Détails** dans la nouvelle colonne **Données** quand les informations d'authentification sont extraites lors d'une session. Ce lien redirige vers le **Rapport des détails de session d'assistance technique** dans laquelle les informations d'authentification ont été utilisées.

Remarque : *Si les informations d'authentification sont extraites depuis **/login**, alors aucun lien **Détails** n'est présent dans la colonne **Données**.*

Conformité : Anonymisez des données Privileged Remote Access pour répondre aux normes de conformité

IMPORTANT !

*L'onglet de **conformité** est désactivé par défaut. Si votre organisation souhaite disposer de cette fonction, veuillez contacter l'assistance technique BeyondTrust à l'adresse www.beyondtrust.com/docs/index.htm#support.*

Anonymisation de l'utilisateur

Les informations sur les utilisateurs ainsi que les actions effectuées pendant les sessions d'accès peuvent être rendues anonymes pour satisfaire aux règles de confidentialité et aux normes de conformité.

Pour anonymiser des données, saisissez le nom d'utilisateur, le nom affiché ou l'adresse e-mail puis sélectionnez l'utilisateur dans la liste. Cliquez sur **Rechercher une activité de technicien d'assistance**. Si des données sont trouvées, le système renvoie une liste des informations trouvées pour cet utilisateur, ainsi qu'un terme de remplacement généré aléatoirement proposé pour ces informations. Vous pouvez cliquer sur le terme proposé pour ouvrir le dialogue **Modifier un remplacement**. Dans ce dialogue, les données peuvent être anonymisées en saisissant un terme de remplacement préféré pour les données. Lorsque vous avez fini, cliquez sur **Modifier un terme de remplacement dans tout l'historique** pour remplacer le terme dans la section.

La liste se met à jour avec le nouveau terme de remplacement et affiche « Les sessions d'accès et les activités d'équipe de cet utilisateur seront signalées comme anonymisées à : [date et heure]. » Après avoir vérifié les termes de remplacement et l'horodatage, cliquez sur **Supprimer l'utilisateur et anonymiser** pour lancer le processus d'anonymisation pour tout le logiciel. Avant de lancer le processus d'anonymisation, vous devez saisir votre nom affiché.

IMPORTANT !

Tous les enregistrements de session sont effacés lors de l'anonymisation.

Anonymisation du point de terminaison

Les informations sur les points de terminaison auxquels l'on accède ainsi que les actions effectuées pendant les sessions d'accès peuvent être rendues anonymes pour satisfaire aux règles de confidentialité et aux normes de conformité.

Pour anonymiser les données, saisissez le nom du point de terminaison, son nom d'hôte ou son adresse IP dans le champ. Cochez la case **Correspondance partielle** si vous voulez que les correspondances partielles soient listées. Cliquez ensuite sur **Chercher l'activité du client**. Si des données sont trouvées, le système renvoie une liste des informations trouvées pour ce point de terminaison, ainsi qu'un terme de remplacement généré aléatoirement proposé pour ces informations. Vous pouvez cliquer sur le terme proposé pour ouvrir le dialogue **Modifier un remplacement**. Dans ce dialogue, les données peuvent être anonymisées en saisissant un terme de remplacement préféré pour les données. Lorsque vous avez fini, cliquez sur **Modifier un terme de remplacement dans tout l'historique** pour remplacer le terme dans la section.

La liste se met à jour avec le nouveau terme de remplacement et affiche « Les sessions d'accès sélectionnées seront signalées comme anonymisées à : [date et heure]. » Après avoir vérifié les termes de remplacement et l'horodatage, cliquez sur **Anonymiser les sessions sélectionnées** pour lancer le processus d'anonymisation pour tout le logiciel. Avant de lancer le processus d'anonymisation, vous devez saisir votre nom affiché.

Vous pouvez également choisir d'**Ajouter un élément personnalisé**. Ceci vous permet de saisir et de rechercher des informations personnalisées, comme des numéros de compte.

IMPORTANT !

Tous les enregistrements de session sont effacés lors de l'anonymisation.

État

Vérifiez les informations des tâches d'anonymisation, y compris les termes trouvés et les termes de remplacement, le type de données anonymisées et l'état de la tâche.

L'état de la tâche est automatiquement actualisé toutes les 15 secondes, et l'état des demandes terminées reste disponible pendant 24 heures.

Remarque : *Ces informations d'état sont également disponibles dans les rapports de session.*

Remarque : *pour les environnements où la reprise en séquence ou Atlas est configuré, l'anonymisation des données n'est terminée qu'une fois que tous les nœuds ou les serveurs de sauvegarde ont été synchronisés.*

Gestion

Logiciel : Téléchargement d'une sauvegarde et mise à niveau logicielle

Paramètres de sauvegarde

L'enregistrement régulier d'une copie de sauvegarde de vos paramètres logiciels fait partie des meilleures pratiques de la reprise après sinistre. BeyondTrust vous recommande de sauvegarder la configuration de votre Secure Remote Access Appliance chaque fois que vous en modifiez les paramètres. En cas de problème matériel, un fichier de sauvegarde accélère la reprise et, si nécessaire, permet à BeyondTrust de vous donner accès à des services hébergés temporairement tout en conservant les paramètres de votre plus récente sauvegarde.

Mot de passe de sauvegarde

Créez un mot de passe pour protéger votre fichier de sauvegarde logicielle. Si vous choisissez de définir un mot de passe, vous ne pouvez pas revenir à la sauvegarde sans fournir le mot de passe.

Inclure les données de rapport de l'historique enregistré

Si cette option est cochée, votre fichier de sauvegarde comportera les journaux de session. Si cette option est décochée, les données de rapport de session ne seront pas incluses dans la sauvegarde.

Télécharger la sauvegarde

Enregistrez une copie sécurisée de votre configuration logicielle. Enregistrez ce fichier dans un emplacement sûr.

Sauvegarder la clé de chiffrement Vault

La clé de chiffrement Vault est utilisée pour chiffrer et déchiffrer toutes les informations d'authentification stockées dans Vault sur le serveur. Si vous avez besoin de restaurer les données de configuration d'une sauvegarde sur un nouveau serveur, vous devez également restaurer la clé de chiffrement Vault à partir d'une sauvegarde pour être en mesure d'utiliser les informations d'authentification chiffrées Vault contenues dans la sauvegarde de la configuration.

Restaurer les paramètres

Configuration et fichier de sauvegarde de la clé de chiffrement Vault

Si vous avez besoin de rétablir une sauvegarde, naviguez jusqu'au dernier fichier de sauvegarde que vous avez enregistré.

Configuration et mot de passe de sauvegarde de la clé de chiffrement Vault

Si vous avez créé un mot de passe pour votre fichier de sauvegarde, saisissez-le ici.

Transférer une sauvegarde

Transférez le fichier de sauvegarde sur votre Secure Remote Access Appliance et restaurez les paramètres de votre site comme ils étaient sur la sauvegarde.

> Pour plus d'informations, veuillez consulter la section Procédures de sauvegarde à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/how-to/disaster-recovery/back-up-procedures.htm.

Envoyer la mise à jour

Sélectionnez un fichier de mise à jour logicielle pour envoyer manuellement les nouveaux packages de logiciels provenant de BeyondTrust. Vous serez invité à confirmer que vous souhaitez télécharger le progiciel. La section **Mise à jour téléchargée** affiche des informations supplémentaires pour vérifier que vous avez téléchargé les programmes. Cliquez sur **Installer** si vous souhaitez terminer l'installation, ou sur **Supprimer la mise à jour** si vous souhaitez effacer la zone de mise à jour. Si le progiciel mis à jour contient uniquement des licences supplémentaires, vous pouvez installer la mise à jour sans redémarrer le serveur. Une fois que vous avez confirmé que vous souhaitez procéder à l'installation, cette page affiche une barre de progression vous informant de la progression générale de l'installation. Les mises à jour effectuées ici mettent automatiquement à jour l'ensemble des sites et licences sur votre Secure Remote Access Appliance.

> ***Remarque :*** *L'administrateur de votre Secure Remote Access Appliance peut également utiliser la fonction* ***Rechercher les mises à jour*** *de l'interface serveur pour rechercher automatiquement et installer les nouveaux packages logiciels.*

Sécurité : gestion des paramètres de sécurité

Mots de passe

Longueur minimum du mot de passe

Définissez des règles pour la longueur des mots de passe des comptes d'utilisateurs locaux.

Exiger des mots de passe complexes

Définissez des règles pour la complexité des mots de passe des comptes d'utilisateurs locaux.

Expiration du mot de passe par défaut

Définissez à quelle fréquence les mots de passe des comptes d'utilisateurs locaux doivent expirer.

Autoriser la réinitialisation du mot de passe

Autorisez les utilisateurs ayant une adresse e-mail configurée à réinitialiser leurs mots de passe. Le lien fourni dans les e-mails de réinitialisation de mot de passe est valide jusqu'à ce qu'un des événements suivants se produise :

- Vingt-quatre heures se sont écoulées.
- Le lien a été cliqué, et le mot de passe a bien été réinitialisé.
- Le système envoie un autre lien à l'adresse e-mail.

Verrouillage du compte au bout de

Définissez le nombre de saisies incorrectes d'un mot de passe avant blocage du compte.

Durée du verrouillage du compte

Définissez la durée d'attente d'un utilisateur bloqué avant qu'il puisse se reconnecter. Vous pouvez aussi demander à un administrateur de débloquer son compte.

Console d'accès

Mettre fin à la session si le compte est en cours d'utilisation

Si un utilisateur essaie de se connecter à la console d'accès avec un compte en cours d'utilisation et que la case **Mettre fin à la session** est cochée, la connexion précédente est interrompue pour autoriser la nouvelle connexion.

Autoriser l'enregistrement des informations de connexion

Autorisez ou non la console d'accès à mémoriser les informations d'authentification d'un utilisateur.

Déconnecter un utilisateur inactif au bout de

Définissez le délai d'attente avant qu'un utilisateur inactif ne soit déconnecté d'une console d'accès, afin de permettre à un autre utilisateur d'y accéder.

Activer l'alerte et la notification de déconnexion sur les délais d'inactivité dépassés

Réglez cette option de sorte qu'une notification soit transmise à un utilisateur inactif 30 secondes avant qu'une déconnexion ne se produise. L'utilisateur recevra aussi une autre notification dès que la déconnexion se sera produite.

Supprimer un utilisateur d'une session après une période d'inactivité

Cette option oblige un utilisateur à abandonner la session après une période d'inactivité définie. Ceci aide les clients BeyondTrust à satisfaire aux initiatives de conformité en matière d'inactivité. L'utilisateur reçoit une notification 1 minute avant la déconnexion et a la possibilité de réinitialiser le délai d'attente.

Un utilisateur est considéré comme actif dans une session lorsqu'un fichier est en cours de transfert, par le biais de onglet de transfert ou de l'interface de la messagerie, ou lorsqu'il clique sur la souris ou qu'il appuie sur un bouton de l'onglet de session. Le simple déplacement de la souris n'est pas considéré comme une activité. Dès l'interruption d'une activité, le compteur d'inactivité est mis en marche.

Autoriser la Console d'Accès mobile et la Privileged Web Access Console à se connecter

Donnez aux utilisateurs la possibilité d'accéder à des systèmes distants à travers l'appli de la console d'accès BeyondTrust pour iOS et Android, ainsi qu'à travers la console d'accès Privileged Web, une console d'accès sur navigateur.

Mode de synchronisation du presse-papiers

Le **Mode de synchronisation du presse-papiers** détermine comment les utilisateurs sont autorisés à synchroniser les presse-papiers lors d'une session de partage d'écran. Les paramètres disponibles sont les suivants :

- **Non autorisé** : L'utilisateur ne peut pas accéder au presse-papiers de l'ordinateur distant ou le modifier.
- **Autorisé à envoyer manuellement le presse-papiers de l'utilisateur au client** : L'utilisateur peut cliquer sur un bouton pour envoyer le contenu du presse-papiers local vers celui de l'ordinateur distant.
- **Autorisé à envoyer manuellement le presse-papiers dans les deux sens** : L'utilisateur peut cliquer sur un bouton pour envoyer le contenu du presse-papiers local vers celui de l'ordinateur distant, ou pour copier le contenu du presse-papiers distant vers son presse-papiers local.
- **Envoyer automatiquement les changements du presse-papiers dans les deux sens** : Les contenus des presse-papiers local et distant restent automatiquement les mêmes.

> ***Remarque :*** *Vous DEVEZ redémarrer le logiciel sur la page d'état pour que ce paramètre prenne effet.*

Divers

Nombre de jours de conservation des informations enregistrées

Dans **Nombre de jours de conservation des informations enregistrées**, définissez la durée pendant laquelle les informations de journalisation doivent être stockées sur le serveur. Ces informations comprennent les données de rapport de la session ainsi que les

enregistrements. Vous pouvez conserver les données de rapport et d'enregistrement d'une session sur un Secure Remote Access Appliance pendant 90 jours au maximum. Il s'agit de la valeur par défaut pour une nouvelle installation. Il arrive que les enregistrements de certaines sessions ne soient pas disponibles, même lorsque la limite de conservation n'est pas dépassée. Les contraintes liées à l'espace du disque ou le paramètre **Nombre de jours de conservation des informations enregistrées** peuvent être à l'origine de ce problème.

Le Secure Remote Access Appliance exécute un script de maintenance chaque jour pour vérifier que l'utilisation du disque est inférieure à 90 %. Si cette limite est dépassée, le script supprime les enregistrements de session selon une formule donnée jusqu'à ce que l'utilisation du disque soit inférieure à 90 %. Si le paramètre **Nombre de jours de conservation des informations enregistrées** a été modifié récemment, il est possible qu'il ne soit pris en compte qu'après un délai de 24 heures.

> Lorsqu'on souhaite conserver les données ou les enregistrements au-delà du délai fixé, BeyondTrust conseille d'utiliser l'API de rapport (www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/api/reporting).

Clé pré-partagée de communication entre serveurs

Entrez un mot de passe dans le champ **Clé pré-partagée de communication entre instances** pour établir une relation de confiance entre deux serveurs. Des clés correspondantes sont requises pour la configuration de deux serveurs ou plus pour des fonctions, telles que la reprise en séquence ou le clustering. La clef doit comporter au moins 6 caractères et contenir au moins une lettre majuscule, une lettre minuscule, un chiffre et un caractère spécial.

Restrictions de réseau

Déterminez les réseaux IP pouvant accéder aux interfaces /login et /api ainsi qu'à la console d'accès BeyondTrust sur votre Secure Remote Access Appliance. Si vous activez des restrictions réseau, vous pouvez également définir les réseaux sur lesquels une console d'accès ou plusieurs peuvent être utilisées.

Interface d'administration (/login) et interface API (/api)

- **Toujours appliquer des restrictions réseau** : lorsque sélectionnée, vous avez la possibilité de créer soit une liste blanche contenant uniquement les réseaux autorisés, soit une liste noire contenant les réseaux auxquels l'accès est refusé. Lorsque cette option est sélectionnée, vous pouvez déterminer quelles restrictions, le cas échéant, devraient s'appliquer aux consoles d'accès bureau, mobile et Web.
- **Ne jamais appliquer de restrictions réseau** : lorsque sélectionnée, aucune restriction n'est appliquée et aucune autre option ne permet d'appliquer de restrictions pour les consoles bureau, mobile et Web.

Console d'accès bureau et mobile

- **Toujours appliquer des restrictions réseaux** : lorsque sélectionnée, elle hérite des restrictions réseau mises en place pour l'interface d'administration.
- **Ne jamais appliquer de restrictions réseau** : lorsque cette option est sélectionnée, aucune restriction n'est appliquée aux consoles bureau et mobile, mais vous avez la possibilité d'appliquer des restrictions pour la console d'accès.
- **N'appliquer des restrictions réseau que pour la première authentification d'un utilisateur** : cela applique les restrictions sélectionnées ci-dessus, mais seulement lors de la première connexion d'un utilisateur.

Console Web (/console)

- **Toujours appliquer des restrictions réseau** : lorsque cette option est sélectionnée, la console d'accès hérite des restrictions mises en place pour l'interface d'administration.
- **Ne jamais appliquer de restrictions réseau** : lorsque cette option est sélectionnée, aucune restriction n'est appliquée à la console d'accès, même si des restrictions sont en place pour les autres méthodes de console d'accès.

> Pour plus d'informations, veuillez consulter le Guide de la Privileged Web Access Console à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/web-access/index.htm.

Restrictions de ports pour l'interface Web d'administration

Définissez les ports d'accès à l'interface /login.

Configuration du site : configuration des ports HTTP et activation de l'accord de connexion

HTTP

Adresses de sites

Définissez les adresses DNS qui renvoient vers votre Secure Remote Access Appliance.

Port HTTP et port HTTPS

Il est possible pour les techniciens de réseaux expérimentés qui travaillent dans des environnements réseau non standard de changer les ports de trafic de BeyondTrust. Ces paramètres ne doivent être ajustés que lorsque des ports autres que les ports standard 80 et 443 sont utilisés pour l'accès Web.

Accord de connexion à /login

Activer l'accord de connexion

Vous pouvez activer un accord de connexion que les utilisateurs devront accepter pour pouvoir accéder à l'interface d'administration /login. Cet accord configurable permet de spécifier des restrictions et des règles de politique interne relatives aux connexions utilisateur.

Titre de l'accord

Personnalisez le titre de l'accord.

Texte de l'accord

Saisissez le texte pour l'accord de connexion.

Configuration e-mail : configuration de l'envoi des e-mails

Adresse e-mail

Remarque : *lorsqu'un serveur est désigné comme étant un serveur de sauvegarde ou un nœud de trafic, la configuration des e-mails pour ce serveur sera remplacée par celle définie sur le serveur maître principal.*

Adresse de l'expéditeur

Définissez l'adresse e-mail à partir de laquelle seront envoyés les messages automatiques de votre Secure Remote Access Appliance.

Serveur relais SMTP

Configurez votre Secure Remote Access Appliance pour qu'il fonctionne avec votre serveur relais SMTP, afin d'envoyer automatiquement des notifications par e-mail de certains événements.

Serveur relais SMTP

Indiquez le nom d'hôte ou l'adresse IP de votre serveur relais SMTP.

Port SMTP

Indiquez le port SMTP sur lequel contacter ce serveur.

Cryptage SMTP

Si votre serveur SMTP prend en charge le cryptage TLS, sélectionnez **TLS** ou **STARTTLS**. Sinon, sélectionnez **Aucun**.

Nom d'utilisateur SMTP

Si votre serveur SMTP requiert une authentification, indiquez un nom d'utilisateur.

Mot de passe SMTP

Si votre serveur SMTP requiert une authentification, indiquez un mot de passe.

Contact administrateur

Adresses e-mail du contact administrateur par défaut

Saisissez une ou plusieurs adresses auxquelles les e-mails doivent être envoyés. Séparez les adresses avec une espace.

Envoyer un avis de communication tous les jours

Vous pouvez demander à recevoir un avis de communication quotidien du Secure Remote Access Appliance pour vérifier le bon fonctionnement des alertes.

En plus de l'e-mail de test et des avis de communication qui peuvent être configurés ci-dessus, des e-mails sont envoyés pour les évènements suivants :

- Lors de toute opération de reprise en séquence, la version de produit du nœud principal ne correspond pas à la version de produit du nœud de sauvegarde.
- Lors d'un contrôle d'état de reprise en séquence, l'un des problèmes suivants est détecté.
    - Le serveur actuel est le nœud principal et une adresse IP partagée est configurée dans /login, mais l'interface réseau n'est pas activée.
    - Une adresse IP partagée est configurée dans /login, mais n'est pas répertoriée comme adresse IP dans /appliance.
    - Le nœud de sauvegarde n'a pas pu contacter ni le nœud principal ni aucune des adresses IP de test configurées sur la page **Gestion > Reprise en séquence**.
    - Le nœud de sauvegarde n'a pu contacter aucune des adresses IP de test configurées sur la page **Gestion > Reprise en séquence**.
    - Les opérations de sauvegarde du nœud de sauvegarde ont été désactivées sur la page **Gestion > Reprise en séquence**.
    - Le nœud de sauvegarde n'a pas réussi à se sonder lui-même, ce qui indique qu'il ne fonctionne pas correctement.
    - Le nœud de sauvegarde n'a pas réussi à contacter le nœud principal en utilisant le nom d'hôte du nœud principal.
    - La reprise en séquence automatique est désactivée, et le nœud de sauvegarde n'a pas réussi à sonder le nœud principal.
    - La reprise en séquence automatique est activée, et le nœud de sauvegarde n'a pas réussi à sonder le nœud principal. Le nœud de sauvegarde deviendra automatiquement le nœud principal si le nœud principal ne répond pas.
    - La reprise en séquence automatique est activée, et le nœud de sauvegarde devient automatiquement le nœud principal parce que le nœud principal est resté inactif pendant trop longtemps.
    - Le nœud principal n'a pas réussi à synchroniser des données avec le nœud de sauvegarde au cours des 24 dernières heures.

Envoyer un e-mail de test lorsque les paramètres sont enregistrés

Si vous souhaitez recevoir un e-mail de test pour vérifier immédiatement la bonne configuration de vos paramètres SMTP, cochez cette option avant de cliquer sur le bouton **Enregistrer**.

Événements sortants : configuration des événements déclenchant l'envoi de messages

Destinataires HTTP

Vous pouvez configurer votre Secure Remote Access Appliance pour qu'il envoie des messages à un serveur HTTP ou à une adresse e-mail lorsque différents événements sont déclenchés.

Les variables envoyées par le Secure Remote Access Appliance arrivent par la méthode HTTP POST et sont accessibles via la méthode utilisée pour récupérer les données POST dans votre langage de codage. Si le serveur ne vous adresse pas une réponse HTTP 200 pour indiquer la réussite de l'opération, le Secure Remote Access Appliance remet l'événement dans la file d'attente et réessaie ultérieurement.

Ajouter un nouveau destinataire HTTP, modifier, supprimer

Créer un nouveau destinataire, modifier ou supprimer un destinataire existant.

Ajouter ou modifier un destinataire HTTP

Nom

Créez un nom unique permettant d'identifier cet événement sortant.

URL

Saisissez une URL de destination pour ce gestionnaire d'événements sortants.

> ***Remarque :*** *Les clients du Cloud BeyondTrust doivent utiliser des URL commençant par HTTPS ; seul le port 443 est pris en charge.*

Activé

Cochez **Activé(e)** pour activer le gestionnaire d'événements. Décochez **Activé(e)** pour interrompre rapidement les messages pour le gestionnaire d'événements que vous avez mis en place, comme dans le cas d'un test d'intégration planifié.

Utiliser un certificat AC

Lorsque vous utilisez une connexion HTTPS, vous devez transférer le certificat racine de l'autorité de certificat annoncé par le serveur d'évènements sortants.

Envoyer des champs personnalisés

Lorsqu'activés, tous les champs personnalisés configurés dans la page **Champs Personnalisés** seront inclus dans l'événement sortant.

Événements à transmettre

Choisissez les événements qui doivent déclencher l'envoi de messages.

Intervalle entre tentatives

Définissez combien de fois il faut relancer après un échec de connexion.

Durée totale des tentatives

Si un événement continue d'échouer malgré les différentes tentatives, déterminez au bout de combien de temps abandonner.

Contact e-mail

Entrez une ou plusieurs adresses de messagerie auxquelles envoyer une notification en cas d'erreur.

Transmettre une alerte par e-mail

Déterminez au bout de combien de temps un e-mail doit être envoyé ; si le problème est résolu avant la fin de ce délai et si l'événement aboutit, aucune notification d'erreur n'est envoyée.

Retransmettre les alertes e-mail

Définissez à quelle fréquence envoyer des e-mails d'erreur si l'échec se prolonge.

Destinataires de messagerie

Ajouter un nouveau destinataire de messagerie, modifier, supprimer

Créer un nouveau destinataire, modifier ou supprimer un destinataire existant.

Statut actuel

Affiche un bref message d'état du serveur relais SMTP. Tant que le serveur peut envoyer des messages au serveur relais, l'état indiqué est **OK**. Sinon, vous devez revoir les paramètres de votre serveur relais SMTP.

Durée totale des tentatives

Si un événement continue d'échouer malgré les différentes tentatives, déterminez au bout de combien de temps abandonner.

Ajouter un destinataire

Avant de configurer le Secure Remote Access Appliance pour envoyer des messages d'événement à une adresse e-mail, vérifiez que votre Secure Remote Access Appliance est bien configuré pour utiliser le serveur relais SMTP. Accédez à la page **Gestion > Configuration e-mail** pour vérifier les paramètres.

Activé

Cochez **Activé(e)** pour activer le gestionnaire d'événements. Décochez **Activé(e)** pour interrompre rapidement les messages pour le gestionnaire d'événements que vous avez mis en place, comme dans le cas d'un test d'intégration planifié.

Nom

Créez un nom unique permettant d'identifier cet événement sortant.

Adresse e-mail

Saisissez l'adresse e-mail à laquelle doit être envoyée la notification des événements sélectionnés. Vous pouvez configurer jusqu'à dix adresses e-mail séparées par des virgules.

Clé externe requise

Si cette option est cochée, les e-mails ne seront envoyés que pour les sessions possédant une clé externe lors de la survenue de l'événement.

Événements à transmettre

Choisissez les événements qui doivent déclencher l'envoi de messages.

Objet

Personnalisez l'objet de cet e-mail. Cliquez sur le lien sous le champ **Corps** pour afficher les macros qui peuvent être utilisées pour personnaliser le texte dans vos e-mails selon vos souhaits.

Corps

Personnalisez le texte de cet e-mail. Cliquez sur le lien sous le champ **Corps** pour afficher les macros qui peuvent être utilisées pour personnaliser le texte dans vos e-mails selon vos souhaits.

Cluster : configuration de la technologie Atlas pour l'équilibrage de charge

État

Les déploiements géographiques à grande échelle tirent parti de la technologie de cluster BeyondTrust Atlas, établissant un site BeyondTrust unique sur plusieurs serveurs, appelés nœuds dans un cluster. Le nœud serveur maître/serveur principal est le site de la plupart des tâches d'administration. Le nœud de trafic est un Secure Remote Access Appliance qui participe à l'acheminement efficace de votre trafic d'assistance technique.

Sur le nœud maître principal, vous pouvez configurer le maître principal lui-même et les nœuds de trafic.

> Vous trouverez plus d'informations sur Atlas dans le Guide de la technologie BeyondTrust Atlas, disponible à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/how-to/atlas.

Statut actuel

Confirme le rôle de l'instance de site depuis laquelle vous avez accédé à la page.

Synchroniser maintenant

Synchronisez les serveurs en cluster.

Démanteler le cluster

Démantelez le cluster, ce qui supprime chaque serveur de son rôle dans le cluster.

Historique de l'état

Affichez ou masquez le journal des messages de serveur en cluster.

Nœuds de trafic

Méthode de sélection des nœuds de trafic

Ce menu est utilisé pour définir la sélection d'un nœud de trafic pour la connexion d'un technicien d'assistance ou d'un client d'utilisateur. Les méthodes disponibles pour définir la connexion sont les suivantes : **Aléatoire**, **Recherche d'enregistrement**, **Recherche d'enregistrement SRV**, **Anycast IP** et **Décalage horaire**. La méthode de connexion choisie dépend en grande partie de votre infrastructure réseau, entre autres considérations complexes.

Ajouter un nouveau nœud de trafic, Modifier un nœud, Supprimer un nœud

Créer un nouveau nœud, modifier un nœud existant, ou supprimer un nœud existant.

Accepte les nouvelles connexions de clients

Vérifiez que cette option est cochée sans quoi les clients ne pourront pas utiliser le nœud de trafic.

Ajouter le nœud de trafic

Nom

Créez un nom unique permettant d'identifier ce nœud.

Décalage horaire

S'utilise uniquement si la **méthode de sélection des nœuds de trafic** est définie sur **Décalage horaire**. Ce processus implique la détection du paramètre de fuseau horaire de la machine hôte et l'utilisation de ce paramètre pour associer le nœud de trafic approprié qui possède le décalage horaire le plus proche. Le décalage horaire est dérivé du paramètre de fuseau horaire du client par rapport au temps universel coordonné (UTC).

Adresse publique

Saisissez le nom d'hôte que vous avez mis comme DNS pour ce nœud, et le port sur lequel les clients vont communiquer avec le nœud.

Adresse interne

"Il peut s'agir de la même adresse que celle utilisée pour l'adresse publique. Des configurations avancées peuvent la définir en option sur un autre nom d'hôte pour une communication inter-serveur.

Préfixes d'adresse réseau

Cette zone peut rester vierge.

Pour les configurations avancées, saisissez les préfixes d'adresse réseau, à raison d'un par ligne, sous la forme **ip.add.re.ss [/masque de réseau]**. Le masque de réseau est facultatif et peut être fourni sous forme décimale pointée ou sous forme d'un entier représentant un ensemble de bits de masquage (bitmask). Si le masque de réseau n'est pas indiqué, une adresse IP unique est supposée.

Si ce champ est renseigné, le nœud maître tente d'assigner un client à ce nœud de trafic si l'adresse IP du client correspond à l'un des préfixes d'adresse réseau. Si l'adresse IP du client correspond à plusieurs préfixes d'adresse réseau de nœuds de trafic, le client est assigné au nœud de trafic ayant la plus longue correspondance de préfixe. Si les préfixes d'adresse réseau correspondants ont une longueur identique, l'un des nœuds de trafic correspondants est choisi aléatoirement. Si l'adresse IP d'un client ne correspond à aucun préfixe d'adresse réseau, le client utilisera la méthode de sélection configurée.

Configuration du nœud maître

Nœud maître primaire

Nom

Créez un nom unique permettant d'identifier ce nœud.
(missing or bad snippet)(missing or bad snippet)

Reprise de client maximum sur le maître

Permet au nombre de clients que vous définissez de revenir au maître pour contrôler le trafic si nécessaire.

Reprise en séquence : configuration d'un serveur de sauvegarde pour la reprise en séquence

Remarque : *Cette fonction n'est disponible que pour les clients possédant un Secure Remote Access Appliance dans leurs locaux. Les clients du Cloud BeyondTrust n'ont pas accès à cette fonction.*

Pour plus d'informations, veuillez consulter la section Configuration de la reprise en séquence Privileged Remote Access à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/how-to/failover/index.htm.

Configuration

Informations de connexion du nouveau site de sauvegarde

Nom de l'hôte ou adresse IP

Saisissez le nom d'hôte ou l'adresse IP du Secure Remote Access Appliance que vous souhaitez utiliser comme sauvegarde dans une relation de reprise en séquence.

Port

Saisissez le port TLS permettant à ce serveur principal de se connecter au serveur de sauvegarde.

Rapporter les informations de connexion à ce site primaire

Nom de l'hôte ou adresse IP

Saisissez le nom d'hôte ou l'adresse IP de ce Secure Remote Access Appliance que vous souhaitez utiliser comme serveur principal dans une relation de reprise en séquence.

Port

Saisissez le port TLS permettant au serveur de sauvegarde de se connecter au serveur principal.

État

Statut de cet hôte

Afficher le nom d'hôte de ce site, ainsi que son état d'instance de site principal ou d'instance de site de sauvegarde.

Statut de l'hôte pair

Afficher le nom d'hôte de ce site, ainsi que son état d'instance de site principal ou d'instance de site de sauvegarde. Afficher également la date et l'heure de la dernière vérification d'état.

Historique de l'état

Développez ou réduisez un tableau des évènements d'état qui se sont produits.

État de l'instance de site principal ou de sauvegarde

Un texte confirme que vous vous trouvez sur l'instance de site principal ou sur l'instance de site de sauvegarde de votre site hôte.

Synchroniser maintenant

Forcer manuellement une synchronisation de données du serveur principal vers le serveur de sauvegarde.

Devenir sauvegarde/principal

Alternez les rôles avec le serveur pair, ce qui force une reprise en séquence pour une opération de maintenance ou un événement de reprise en séquence connu.

Cochez cette case pour extraire une synchronisation des données de l'instance de site sur example.com tout en devenant la sauvegarde/principale.

Pour synchroniser les données du serveur pair avant d'échanger les rôles, cochez cette case. Si cette option est sélectionnée, tous les utilisateurs du serveur principal sont déconnectés pendant la synchronisation et aucune opération n'est possible pendant l'opération d'échange.

Cochez cette case pour devenir une sauvegarde même si l'instance du site pair sur example.com ne peut être contactée.

Sur l'instance de site principal, vous pouvez passer en site de sauvegarde même si le serveur pair ne peut être contacté. Si cette option est désélectionnée, la reprise en séquence est annulée si les deux serveurs ne peuvent être maintenus en synchronisation en termes de rôles de reprise en séquence (un serveur principal et un serveur de sauvegarde).

Par exemple, si vous savez que le serveur de sauvegarde est en ligne mais que le serveur principal ne peut le contacter en raison d'un problème de connexion réseau, vous pouvez sélectionner cette option afin de faire du serveur principal le serveur de sauvegarde en attendant de restaurer la connexion réseau. Dans cet exemple, vous devez également accéder au serveur de sauvegarde afin d'en faire le serveur principal.

Rompre les relations de reprise en séquence

Brisez la relation de la reprise en séquence, ce qui supprime chaque serveur de son rôle principal ou de sauvegarde.

Configuration de l'instance de site principal ou de sauvegarde

IP partagées

Contrôlez les adresses IP partagées que l'instance de site utilise au cas où une reprise en séquence viendrait à se produire. Il suffit pour cela de cocher la case de l'adresse IP de reprise en séquence. Si vous modifiez la relation entre les sites, les adresses IP sélectionnées seront désactivées lorsque le site principal deviendra site de sauvegarde, et seront activées lors de l'opération inverse. Vous devrez copier manuellement ce réglage sur le site pair, car il n'est pas partagé.

Paramètres de sauvegarde

Les paramètres que vous configurez ici deviennent actifs lorsque l'instance de site que vous configurez passe en mode sauvegarde.

Sur l'instance de site principal, sélectionnez **Paramètres de sauvegarde >** pour afficher ou masquer la page affichant les champs de configuration.

Activer les opérations de sauvegarde

Activez ou désactivez les sauvegardes de site.

Intervalle de synchronisation automatique des données

Vous pouvez contrôler l'intervalle de synchronisation automatique.

Limite de bande passante de la synchronisation des données

Définissez les paramètres de bande passante pour la synchronisation de données.

Activer la reprise en séquence automatique

Activer ou désactiver la reprise en séquence automatique.

Délai d'attente de l'instance du site principal

Déterminez l'intervalle avant qu'un site principal inaccessible passe en reprise en séquence.

IP test de connectivité réseau

Indiquez des adresses IP pour le site de sauvegarde, afin de déterminer si la sauvegarde ne peut pas atteindre le site principal, car le site principal est hors-ligne ou parce que la sauvegarde a perdu sa connexion réseau.

Configuration de l'API : activation de l'API XML et configuration de champs personnalisés

Configuration de l'API

Activer l'API XML

Vous pouvez choisir d'activer l'API XML BeyondTrust, qui permet d'exécuter des rapports et des commandes, comme le démarrage ou le transfert de sessions depuis des applications externes, ainsi que de sauvegarder automatiquement votre configuration logicielle.

Autoriser l'accès HTTP à l'API XML

Par défaut, l'accès à l'API s'effectue via une connexion SSL cryptée. Vous pouvez néanmoins autoriser un accès HTTP non crypté. Il est fortement recommandé de désactiver l'accès HTTP dans le cadre des meilleures pratiques de sécurité.

> ***Remarque :*** *cette option est obsolète depuis la version 16.1 et n'apparaît pas pour les nouveaux utilisateurs. Pour les utilisateurs se mettant à jour depuis une version antérieure à 16.1, l'option est toujours disponible si vous continuez à utiliser la méthode obsolète d'authentification à l'API avec un compte d'utilisateur. Si vous passez à la méthode préférée d'authentification avec un compte API, tout le trafic API doit se faire en HTTPS.*

Comptes d'API

Un compte API stocke tous les paramètres d'authentification et d'autorisation pour le client d'API. Au moins un compte d'API est nécessaire pour utiliser l'API, soit en conjonction avec le client d'intégration, soit avec une application tierce, soit avec votre propre logiciel.

> ***Remarque :*** *avant la version 16.1, un compte d'utilisateur était utilisé pour l'authentification à l'API. Cette méthode est désormais obsolète, mais elle est toujours prise en charge pour les clients qui l'utilisent.*

Ajouter un compte d'API, Modifier, Supprimer

Créer un nouveau compte, modifier un compte existant, ou supprimer un compte existant.

Ajouter ou modifier un compte d'API

Activé

Si cette option est cochée, ce compte est autorisé à s'authentifier auprès de l'API. Lorsqu'un compte est désactivé, tous les jetons OAuth associés au compte sont immédiatement désactivés.

Nom

Créez un nom unique permettant d'identifier ce compte.

Commentaires

Ajoutez des commentaires pour aider à identifier la fonction de cet objet.

Identifiant client OAuth

L'ID client OAuth est un identificateur unique généré par le serveur. Il ne peut pas être modifié. L'ID client est considérée comme information publique et peut donc être partagée sans compromettre la sécurité de l'intégration.

Secret de client OAuth

Le secret de client OAuth est généré par le serveur grâce à un générateur de nombres pseudo-aléatoire sécurisé cryptographiquement.

> ***Remarque :*** *le secret de client ne peut pas être modifié, mais il peut être généré à nouveau sur la page* ***Modifier****. Générer un nouveau secret de client et enregistrer le compte rend immédiatement invalides tous les jetons OAuth associés à ce compte. Tout appel d'API utilisant ces jetons ne pourra pas accéder à l'API.*

> ***Remarque :*** *L'ID client OAuth et le secret de client sont utilisés pour créer des jetons OAuth, nécessaires pour l'authentification à l'API.*

> Pour plus d'informations, veuillez consulter le Guide de l'API à l'adresse www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/api/index.htm.

Autorisations

Sélectionnez les zones de l'API que ce compte a le droit d'utiliser. Pour l'**API de commande**, choisissez de refuser l'accès, d'autoriser l'accès en lecture seule ou d'autoriser l'accès complet. Définissez également si ce compte peut utiliser **l'API de rapport**, **l'API de sauvegarde**, l'API de configuration et/ou **l'API du gestionnaire d'informations d'authentification de point de terminaison**.

L'API de configuration permet de gérer et de configurer des tâches fréquentes dans **/login**, ce processus pouvant être automatisé et étant compatible avec vos processus d'orchestration.

> Pour plus d'informations, veuillez consulter la section API de configuration d'un compte Vault à l'adresse www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/api/configuration-api.htm.

L'**API SCIM** permet l'approvisionnement d'utilisateurs d'un fournisseur de sécurité différent. En autorisant l'accès à l'API SCIM, l'option **Autoriser un jeton du porteur à long terme** devient disponible. Autoriser les jetons à long terme n'est pas recommandé, à moins que cela ne soit requis par votre client SCIM, étant donné que ces jetons du porteur n'expirent jamais. Comme toutes les autres autorisations de l'API exigent des jetons expirant au bout d'une heure, activer les jetons à long terme pour SCIM désactive toutes les autres autorisations de l'API.

Restrictions de réseau

Répertoriez les préfixes d'adresse réseau à partir desquels ce compte peut s'authentifier.

> ***Remarque :*** *les comptes API ne sont pas restreints par les préfixes réseau configurés sur la page* ***/login > Gestion > Sécurité****. Ils sont uniquement restreints par les préfixes de réseau configurés pour le compte d'API.*

Assistance technique : Contacter l'Assistance technique BeyondTrust

Comment contacter l'assistance technique BeyondTrust

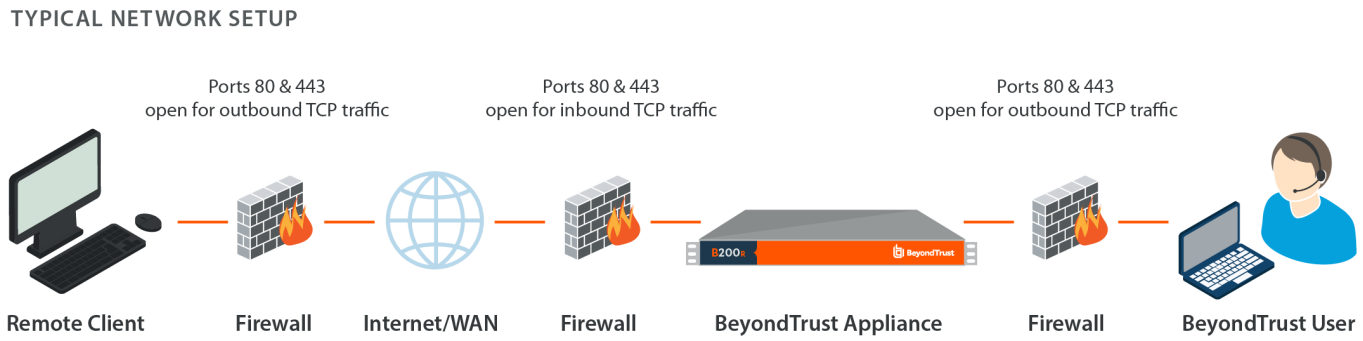
La page d'assistance technique contient toutes les coordonnées pour contacter le technicien d'assistance Assistance technique BeyondTrust.

Assistance technique avancée de BeyondTrust

Si un technicien de l'Assistance technique BeyondTrust doit accéder à votre serveur, il vous fournira des codes d'assistance technique, d'accès et de remplacement à saisir sur cette page pour créer un tunnel d'assistance technique entièrement crypté créé par le serveur et pointant vers BeyondTrust pour une résolution rapide des problèmes complexes.

Ports et pare-feu

Les solutions BeyondTrust sont conçues pour fonctionner en transparence au travers des pare-feu, et permettent une connexion avec tout ordinateur disposant d'une connexion à internet, partout dans le monde. Toutefois, avec certains réseaux hautement sécurisés, une configuration supplémentaire peut s'avérer utile.



- Les ports 80 et 443 doivent être ouverts au trafic TCP sortant sur les pare-feux de l'utilisateur et du système distant. Il est possible que davantage de ports soient disponibles en fonction de votre version. Ce schéma montre une configuration réseau type ; vous trouverez des informations supplémentaires dans le Guide d'installation matérielle du serveur.
- Des logiciels de sécurité internet tels que des pare-feu ne doivent pas bloquer le téléchargement des fichiers exécutables BeyondTrust. Sont concernés notamment McAfee Security, Norton Security et Zone Alarm. Si vous disposez d'un logiciel pare-feu, vous pouvez constater quelques problèmes de connexion. Afin d'éviter ces problèmes, configurez votre pare-feu de façon à autoriser les fichiers exécutables suivants, où {uid} est un identificateur unique composé de lettres et de chiffres :
  - bomgar-scc-{uid}.exe
  - bomgar-scc.exe
  - bomgar-pac-{uid}.exe
  - bomgar-pac.exe
  - bomgar-pec-{uid}.exe
  - bomgar-pec.exe

  Pour obtenir une assistance au niveau de la configuration de votre pare-feu, veuillez contacter le fabricant du logiciel du pare-feu.
- Des exemples de règles de pare-feu basées sur l'emplacement du serveur peuvent être trouvés à l'adresse www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/dmz/firewall-rules.htm.

Si vous ne parvenez toujours pas à établir une connexion, contactez l'Assistance technique BeyondTrust à l'adresse www.beyondtrust.com/support.

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

Avis de non-responsabilité

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

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

Limitations associées à la licence

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

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

Assistance technique

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

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