Acronis

Statuts des Plans

- Les statuts des plans de protection et de réplication sont affichés avec un code couleur spécifique pour chaque état :
- OK (vert) : Le plan fonctionne normalement.
- Avertissement (orange) et Erreur (orange foncé) : Indiquent des problèmes qui nécessitent une attention, l'erreur étant plus grave.
- Critique (rouge) : Signale un problème majeur nécessitant une intervention immédiate.
- En cours d'exécution (bleu) : Le plan est activement en train de s'exécuter.
- Désactivé (gris) : Le plan n'est pas actif.

Gestion des Plans de Protection

- L'onglet "Gestion > Plans de protection" permet de voir les informations sur les plans existants, de réaliser diverses opérations comme exécuter, stopper, modifier, ou supprimer des plans, et de créer de nouveaux plans.

Sauvegarde d’Applications dans le Cloud

- Les plans de sauvegarde "cloud à cloud" sont conçus pour sauvegarder des applications exécutées dans le cloud, utilisant le stockage cloud comme lieu de sauvegarde.
- Des limitations sont mises en place pour éviter la surutilisation, limitant le nombre d'exécutions de sauvegardes à 10 par heure pour

chaque organisation, avec une réduction à une exécution par heure après atteinte de la limite.

Analyse des Sauvegardes

- Un plan d'analyse de sauvegarde peut être créé pour inspecter les sauvegardes à la recherche de malwares, y compris les ransomwares. Ce plan utilise un agent cloud qui exécute automatiquement l'analyse selon les emplacements de sauvegarde spécifiés.

Traitement des Données Hors Hôte

- Ces plans permettent de réaliser des opérations de réplication, de validation, de nettoyage et de conversion de sauvegardes en machines virtuelles, en utilisant différents agents de protection, et peuvent être programmés pour les heures creuses afin de réduire l'utilisation de la bande passante.

Réplication de Sauvegarde

- Pour créer un plan de réplication de sauvegarde, il faut spécifier un agent qui aura accès aux emplacements source et de réplication. Il est possible de choisir entre répliquer toutes les sauvegardes, uniquement les sauvegardes complètes, ou seulement la dernière sauvegarde. La configuration des règles de rétention pour l'emplacement cible est également nécessaire, définissant comment et combien de temps les sauvegardes répliquées seront conservées.

Désinstallation d'agents

Lorsque vous désinstallez un agent d'une ressource, cette ressource est supprimée automatiquement de la console Cyber Protect. Si la ressource reste affichée après que vous avez désinstallé l'agent, en raison d'un problème réseau, par exemple, supprimez cette ressource manuellement de

la console. Pour en savoir plus sur la procédure à suivre, reportez-vous à "Suppression de ressources de la console Cyber Protect".

Sauvegarde

La sauvegarde avec agent est une sauvegarde créée par un agent de protection installé sur la ressource ou sur un support de démarrage. La sauvegarde sans agent n'est disponible que pour les machines virtuelles. Elle est effectuée au niveau de l'hyperviseur par un agent qui peut sauvegarder et restaurer toutes les machines virtuelles de l'environnement. Aucun agent n'est installé sur les machines virtuelles protégées. Pour plus d'informations sur les différences entre les sauvegardes avec et sans agent, voir « Sauvegarde avec et sans agent »

Restauration

La restauration avec agent est effectuée par un agent installé sur la ressource ou sur un support de démarrage. La restauration sans agent ne prend en charge que les machines virtuelles en tant que cibles. Elle est effectuée au niveau de l'hyperviseur par un agent qui peut sauvegarder et restaurer toutes les 59 ©Acronis International GmbH, 2003-2024machines virtuelles de l'environnement. Il n'est pas nécessaire de créer manuellement une machine cible vers laquelle la sauvegarde est restaurée.

Activation de l'Autoprotection

Au sein d'un plan de protection, activez le module "Protection contre les virus et les malwares" (connu sous le nom de module Active Protection pour les éditions Cyber Backup). Assurez-vous que l'interrupteur "Autoprotection" est activé.

2. Configurer la Protection par Mot de Passe :

- Activez l'interrupteur "Protection par mot de passe".

- Un mot de passe unique est généré, que vous devez copier et conserver en lieu sûr, car il ne sera pas récupérable une fois la fenêtre fermée.
- Ce mot de passe est nécessaire pour toute désinstallation ou modification des composants de l'Agent pour Windows protégé.

3. Enregistrement des Changements :

- Après avoir configuré le mot de passe, cliquez sur "Fermer" puis "Terminé" dans le volet Autoprotection.
- Enregistrez les modifications apportées au plan de protection.

4. Restrictions et Compatibilité :

- Cette fonctionnalité est uniquement disponible pour les versions de l'Agent pour Windows version 15.0.25851 ou ultérieure.
- Les machines doivent être en ligne pour que cette protection soit effective.
- Bien que le plan de protection puisse être appliqué à des machines macOS, aucune protection par mot de passe ne sera activée sur ces systèmes.
- Les machines Linux ne peuvent pas utiliser ce plan de protection.
- Un seul plan de protection avec protection par mot de passe peut être appliqué à une même machine Windows à la fois.

5. Modification du Mot de Passe :

- Si le mot de passe est perdu ou oublié, il est possible de modifier le plan de protection pour créer un nouveau mot de passe suivant une procédure similaire à celle de l'activation initiale.