opentext™

LIVRE BLANC

OpenText™ Server Backup pour une sécurité et un contrôle accrus

OpenText™ Server Backup offre plusieurs couches de protection et de résilience des données sur une infrastructure évolutive et sécurisée



Sommaire

Sécurité	4
Détection	5
Chiffrement	5
Architecture	6
Fiabilité/durabilité des données	8
Disponibilité des données	8
Conformité	9
Confidentialité	11
Prochaines étapes	12

OpenText™ Cybersecurity fournit aux partenaires une solution de sauvegarde dans le cloud puissante et facile à gérer, OpenText™ Server Backup. Il comprend des fonctions de configuration, de gestion et de prise en charge des activités de sauvegarde de serveur. Grâce à un programme d'installation d'agent facile à utiliser, les utilisateurs peuvent enregistrer leurs serveurs et utiliser le portail centralisé pour créer des tâches de sauvegarde répondant à leurs besoins en matière de protection. Les options et configurations de sauvegarde incluent :

- Sauvegarde de fichiers/dossiers
- Sauvegarde d'applications (SQL, Exchange, Oracle)
- Sauvegarde de l'état du système
- Sauvegarde au niveau image
- Sauvegarde du chemin UNC
- Sauvegarde sur site
- Sauvegarde cloud
- Sauvegarde hybride (cloud et sur site)

La sauvegarde sur emplacements multiples offre différentes options pour récupérer les données et éviter la perte de données. OpenText™ Server Backup offre à la fois une protection robuste et des processus de récupération simples.



Sécurité

OpenText™ Server Backup offre les fonctions de contrôle et de visibilité dont les administrateurs informatiques ont besoin pour assurer la séparation logique des tâches entre les clients, les partenaires et les équipes d'exploitation OpenText™. En arrière-plan, une infrastructure éprouvée, sécurisée et sophistiquée est conçue pour protéger les données pendant le transport et le stockage.

Contrôle et visibilité

Grâce aux outils essentiels disponibles dans un portail multi-locataire, OpenText™ Cybersecurity permet aux administrateurs de personnaliser la configuration d'OpenText™ Server Backup pour répondre aux besoins de l'entreprise. Les principales caractéristiques sont les suivantes :

- Hiérarchie de « sites enfants » distincte pour prendre en charge l'administration autonome de clients individuels
- Accès basé sur les rôles pour les administrateurs
- Portail intuitif permettant de regrouper les actifs de sauvegarde de manière logique
- Chiffrement distinct par tâche de sauvegarde pour une confidentialité étendue
- Coffres-forts de données (et informations d'identification) séparés de manière logique désignés par client
- Rapports historiques agrégés

La hiérarchie multi-locataire d'OpenText™ Server Backup assure la séparation logique des tâches administratives et de gestion des données, garantissant ainsi que les données restent privées et sous le contrôle du client.

Contrôle d'accès

L'accès à l'agent de sauvegarde et au portail de sauvegarde, pour la configuration et la planification de l'administration (configuration des tâches) ou pour le lancement des sauvegardes et des restaurations (transfert de données), est strictement contrôlé. Les exigences strictes en matière de nom d'utilisateur et de mot de passe peuvent être (et devraient être) renforcées par l'authentification à deux facteurs (2FA).

Authentification à deux facteurs

Lorsqu'elle est configurée, l'authentification de compte à deux facteurs fournit une couche de sécurité supplémentaire lors de la connexion au portail OpenText™ Server Backup. Les utilisateurs peuvent configurer l'authentification de compte à deux facteurs à tout moment en saisissant un numéro de téléphone dans leurs paramètres de profil. Les utilisateurs pour lesquels une authentification de compte à deux facteurs est configurée sont invités à saisir un code périodiquement (tous les 30 jours) lorsqu'ils se connectent au portail, lorsqu'ils souhaitent réinitialiser leurs mots de passe et lorsqu'ils se connectent au portail à partir d'un nouveau navigateur Web. Les utilisateurs ont la possibilité de recevoir des codes d'authentification par SMS ou par appels vocaux automatisés.

Enregistrement de l'agent

Chaque agent de sauvegarde déployé pour protéger les serveurs sources doit être enregistré auprès du portail. Ce processus nécessite un accès administratif au serveur et une authentification via un ensemble d'informations d'identification du portail, qui sont gérées dans le compte administrateur du portail.

Détection

Le ransomware est un fléau pour toutes les entreprises. La détection des ransomwares potentiels dans les environnements Windows et VMware vSphere signale automatiquement les anomalies et propose des fonctions d'alerte à plusieurs niveaux, telles que des avertissements sur le tableau de bord, des vues des menaces et des notifications automatiques par e-mail. Si cela est confirmé, les données non compromises peuvent être rapidement restaurées et récupérées.

Chiffrement

Le chiffrement des données est au coeur du modèle de sécurité des données. Server Backup utilise le chiffrement par clé privée AES-256 bits pour toutes les tâches, avec une clé de chiffrement créée pour chaque tâche comme suit :

- Le client fournit un mot de passe de chiffrement, qui est stocké de manière chiffrée sur l'agent dans l'environnement du client.
- Le mot de passe de chiffrement fourni par le client est utilisé pour générer la clé de chiffrement AES-256.
    - Ce mot de passe n'est pas stocké dans le système de l'interface utilisateur ni lu par l'agent lorsque l'interface utilisateur charge les paramètres de la tâche à partir d'un agent.
- Les données sont chiffrées sur le système du client à l'aide du mot de passe de chiffrement fourni par le client avant d'être envoyées au coffre-fort.
- Les données sont transmises sur un canal chiffré séparément.
- Lors de la restauration, les données sont renvoyées chiffrées depuis le coffre-fort et déchiffrées sur le système du client.
    - La clé de chiffrement n'est pas stockée dans le coffre-fort ni transmise à OpenText.



OpenText™ recommande aux clients de toujours choisir avec soin des mots de passe de chiffrement forts et aléatoires. De plus, pour détecter les logiciels malveillants et les empêcher d'accéder à l'agent, nous vous recommandons d'installer un logiciel de protection fiable des points d'accès.

IMPORTANT : le mot de passe de chiffrement est requis pour la restauration des données. Stockez-le en toute sécurité. En cas d'oubli du mot de passe, les restaurations ne seront pas possibles. Si l'administrateur modifie ce mot de passe de chiffrement pour une tâche existante, cela forcera une nouvelle sauvegarde complète (c'est-à-dire une réinitialisation). Les points de reprise plus anciens nécessiteront le mot de passe précédent. Il est impératif de conserver l'historique des mots de passe et la date de toute modification.

Transport Layer Encryption

La seconde mise en oeuvre d'AES protège les paquets envoyés entre l'agent du serveur source et le coffre-fort de données. Dans ce cas, le paquet complet est chiffré et envoyé au serveur sur lequel il est traité. L'agent établit la connexion avec le serveur sur un port TCP/IP prédéterminé. Ce port peut être personnalisé en fonction des paramètres et préférences du réseau. Lors de la connexion entre l'agent et le serveur, il existe une liaison initiale pour s'assurer que la connexion est autorisée.

Vulnerability Remediation

OpenText™ utilise régulièrement des analyses de vulnérabilité, notamment des analyses au niveau du code et des analyses au niveau des applications. Tous les résultats sont régulièrement examinés, et tout problème de sécurité est trié et résolu rapidement. Pour plus d'informations, consultez notre rapport SOC 2 Type 2, disponible sur demande lorsque les clients signent un accord de non-divulgation (NDA).

Architecture

OpenText™ Server Backup est conçu avec plusieurs couches de protection, notamment le transfert sécurisé des données, le chiffrement, la configuration réseau et les contrôles au niveau des applications, répartis sur une infrastructure évolutive et sécurisée. Le système lui-même est composé de composants modulaires (portail, coffre-fort de données et agents) isolés les uns des autres afin de promouvoir la disponibilité et la robustesse du service.

Infrastructure Resilience

OpenText™ Server Backup repose sur plus de 20 ans de fiabilité logicielle renforcée. Nos datacenters sont conçus et construits selon les normes du secteur avec plusieurs couches de tolérance aux pannes au niveau des composants et des systèmes :

- Composants de calcul et de stockage redondants N+1
- Configurations de serveur et installations en rack redondantes
- Plusieurs onduleurs avec batterie de secours pour garantir une alimentation propre et stable
- Générateurs d'urgence, qui sont automatiquement activés en cas de coupure de courant

- Réseaux routés de diverses manières fournis par plusieurs fournisseurs
- Mesures de protection physique, y compris, mais sans s'y limiter :
  - Unités de refroidissement indépendantes redondantes
  - Contrôle de la température et de l'humidité
  - Refroidisseurs alimentant les unités CRAC
  - Système de détection de fumée précoce
  - Système d'extinction d'incendie à base de gaz
- Plans de reprise d'activité pour les composants critiques de l'infrastructure, par exemple :
  - Bases de données du coffre-fort sauvegardées localement, deux fois par jour
  - Sauvegardes de la base de données du coffre-fort local, qui sont copiées hors site au moins toutes les huit heures
  - Copies hors site sauvegardées une fois par jour
- OpenText™ prend différentes mesures pour protéger les données :
  - Plusieurs copies de chaque octet, ce qui protège contre les pannes de disque ou de noeud
  - Les snapshots quotidiens de données sont stockés pendant quatre jours
  - Restrictions d'accès physique dans toutes les installations OpenText™
  - L'accès est contrôlé par le personnel de sécurité sur site et tous les accès sont enregistrés
  - La surveillance des installations comprend toutes les portes périphériques, les alarmes de sécurité, la surveillance numérique et les caméras vidéo qui surveillent et enregistrent les entrées et les sorties pour empêcher toute activité non autorisée



Fiabilité/durabilité des données

L'intégrité des données est essentielle pour tout service de sauvegarde. OpenText™ Server Backup dispose de fonctions robustes de fiabilité des données présentes dans le service pour garantir la fiabilité des données sur les connexions distantes.

Quick File Scanning (QFS)

OpenText™ Server Backup utilise une technologie propriétaire brevetée appelée Quick File Scanning pour examiner les métadonnées d'un fichier et déterminer s'il a changé depuis la dernière sauvegarde. Cette capacité à analyser rapidement des datasets volumineux et à rechercher uniquement les fichiers présentant des modifications est essentielle à l'efficacité de la solution et à la réduction de l'impact des workloads de sauvegarde sur le réseau.

DeltaProTM – Delta Processing

En plus de l'utilisation de QFS pour identifier les fichiers modifiés, notre traitement de données exclusif et breveté DeltaProTM nous permet de trouver les modifications par bloc au sein des fichiers modifiés. La combinaison de la technologie QFS et de la technologie DeltaProTM permet une optimisation élevée du traitement des données pour aider les entreprises à réduire la fenêtre potentielle de perte de données tout en réduisant l'impact sur le réseau.

Protocole BRTP (Backup/Restore Transfer Protocol)

Outre DeltaProTM, l'agent OpenText™ Server Backup effectue des sauvegardes et des restaurations à distance en établissant d'abord une connexion sécurisée avec le coffre-fort de données à l'aide de TCP/IP. Il met ensuite en oeuvre le protocole BRTP (Backup/Restore Transfer Protocol) propriétaire pour transférer les informations de contrôle et les données réelles vers le coffre-fort de données. Cela permet de garantir un séquençage d'ordre d'écriture précis, même sur les connexions intermittentes.

Disponibilité des données

OpenText™ Server Backup est une solution entièrement hébergée, gérée par une équipe d'exploitation expérimentée. Travaillant sur plusieurs fuseaux horaires, les équipes chargées des opérations et du support restent disponibles 24 h/24, 7 j/7.

Le service peut parfois être indisponible en raison de mises à niveau et d'autres procédures de maintenance. Ces événements sont planifiés et une notification ainsi qu'une fenêtre de maintenance sont communiquées à l'avance.

- **Maintenance planifiée.** OpenText™ effectue une maintenance planifiée tous les trimestres et tous les mois pour appliquer les correctifs de système d'exploitation et de sécurité. Les partenaires et les clients reçoivent un préavis de sept jours.
- **Maintenance non planifiée.** OpenText™ peut effectuer des opérations de maintenance non planifiées pour résoudre certaines nouvelles vulnérabilités ou modifications d'applications et d'infrastructure qui pourraient être nécessaires dans un avenir proche. Les partenaires et les clients reçoivent un préavis d'un à six jours.
- **Maintenance d'urgence.** OpenText™ peut effectuer une maintenance d'urgence pour résoudre des problèmes susceptibles d'avoir un impact critique sur le service et nécessitant une résolution immédiate. Il n'y a pas d'avis préalable à une maintenance d'urgence.

Les partenaires et les clients peuvent vérifier l'état du service en consultant la section Server Backup de notre page d'état à l'adresse https://status.carbonite.com.

Conformité

OpenText™ s'engage chaque année auprès d'une société d'audit tierce indépendante pour fournir une attestation de conformité aux exigences SOC 2 Type 2. OpenText™ exploite un cadre de contrôle basé sur le respect de plusieurs réglementations standard du secteur, notamment :

- Loi fédérale HIPAA (Health Insurance Portability and Accountability Act)
- Loi FERPA (Family Educational Rights and Privacy Act)
- Loi GLBA (Gramm-Leach-Bliley)

En outre, OpenText™ Server Backup est certifié ISO 27001 et respecte les processus PCI pour les transactions de paiement des clients.



Contrôles du système et de l'organisation (SOC)

Les partenaires et les clients peuvent demander le rapport d'attestation du SOC actuel via leur représentant de compte (NDA actuel requis). Les contrôles SOC validés et mis en place pour tous les services OpenText™ Server Backup répondent aux meilleures pratiques du secteur en matière de services cloud, telles que définies par la Cloud Security Alliance (CSA). Parmi ceux-ci, on peut citer, sans s'y limiter :

- Sécurité des applications et des interfaces
- Chiffrement et gestion des clés
- Interopérabilité et portabilité
- Assurance d'audit et conformité
- Gouvernance et gestion des risques
- Sécurité des périphériques sans fil
- Gestion de la continuité des activités et résilience opérationnelle
- Ressources humaines
- Gestion des incidents de sécurité, découverte électronique et analyse du cloud
- Contrôle des modifications et gestion de la configuration
- Gestion des identités et des accès
- Gestion de la supply chain, transparence et responsabilité
- Sécurité des données et administration du cycle de vie des informations
- Sécurité de l'infrastructure et de la virtualisation
- Gestion des menaces et des vulnérabilités
- Sécurité du datacenter

Loi fédérale HIPAA (Health Insurance Portability and Accountability Act)

La loi fédérale américaine HIPAA (Health Insurance Portability and Accountability Act) spécifie la manière dont les organismes de soins médicaux doivent traiter les données médicales protégées (DMP). Il ne s'agit pas seulement d'organismes de soins médicaux qui sont concernés par la législation fédérale sur les soins de santé. Toute entreprise qui traite des informations médicales protégées doit se conformer aux exigences fédérales en matière de sécurisation des dossiers médicaux électroniques (DME). Cela inclut les cabinets juridiques et comptables, ainsi que les entreprises d'hébergement Web, pour n'en citer que quelques-uns.

En vertu de la réglementation, OpenText™ se considère comme assurant les fonctions d'un partenaire commercial et a amélioré son programme de conformité pour faciliter la gestion d'une infrastructure conforme à la loi HIPAA. Chaque fois que cela est nécessaire, OpenText conclura un Accord de partenariat commercial (Business Associate Agreement), garantissant contractuellement que nous nous conformerons à la loi HIPAA en ce qui concerne les données médicales protégées. En outre, OpenText™ fait appel à des fournisseurs prêts à conclure des accords conformes à la loi HIPAA, garantissant ainsi les mêmes normes strictes. OpenText™ a conçu des solutions conformes aux plus de 40 mesures de protection de la confidentialité et de la sécurité requises par la loi HIPAA.

Souveraineté des données

Pour les clients opérant dans des secteurs réglementés ou dans des pays disposant de lois sur la protection des données, il est important de connaître l'emplacement géographique de leurs données. Les offres OpenText™ au sein du portefeuille Server Backup comprennent les installations géographiques spécifiques suivantes pour les entreprises qui doivent conserver et gérer des données dans une région particulière en raison d'un cadre réglementaire :

- U.S. x2
- Canada
- Royaume-Uni
- Pays-Bas

Règlement général sur la protection des données (RGPD)

OpenText™ Server Backup comprend des solutions technologiques pour sécuriser les données personnelles, garantir leur résidence et limiter l'accès pour les utilisateurs non autorisés. OpenText™ Server Backup aide à prendre en charge la conformité au Règlement général sur la protection des données (RGPD) pour les organisations de l'UE, notamment :

Rectification

OpenText™ Server Backup est conçu pour capturer automatiquement toutes les modifications apportées aux données sources. Ainsi, s'il est nécessaire de corriger ou de compléter les données en production, ces modifications seront automatiquement reflétées dans la prochaine sauvegarde périodique sans qu'aucune intervention manuelle supplémentaire ne soit nécessaire.



Effacement

Les périodes de conservation des données sont facilement configurables pour supprimer les anciens datasets après une période prédéterminée. Par exemple, si la période de conservation est définie sur 30 jours et que le nombre de datasets conservés est configuré sur 30, toutes les anciennes sauvegardes dépassant les 30 datasets spécifiés seront supprimées à la fin de cette période.

Confidentialité

OpenText™ Server Backup utilise le chiffrement par clé privée AES-256 bits pour toutes les tâches et les données, avec une clé de chiffrement créée pour chaque tâche. Le client fournit un mot de passe de chiffrement, qui est stocké de manière chiffrée sur l'agent dans l'environnement du client. Le mot de passe de chiffrement fourni par le client est utilisé pour générer la clé de chiffrement AES-256. Le mot de passe de chiffrement n'est pas stocké dans le système d'interface utilisateur ni transmis à OpenText. Cela limite encore l'accès aux données. Les données sont transmises à OpenText™ sur un canal chiffré séparément.

OpenText™ recommande aux clients de toujours choisir avec soin des mots de passe de chiffrement forts et aléatoires. De plus, pour détecter les logiciels malveillants et les empêcher d'accéder à l'agent, nous vous recommandons d'installer un logiciel de protection fiable des points d'accès.

Registres de traitement

Pour répondre aux exigences de conservation des données, OpenText propose divers rapports qui peuvent être planifiés et envoyés par e-mail aux utilisateurs. Par exemple :

- **Rapport d'état quotidien.** Ce rapport contient des informations sur l'état des sauvegardes au cours des dernières 24 heures, y compris les sauvegardes manquées et les tâches en cours pour les ordinateurs qui exécutent les derniers agents.
- **Rapport de sauvegarde détaillé.** Ce rapport fournit des informations détaillées sur chaque exécution d'une sauvegarde au cours d'une période donnée, y compris la quantité de données sauvegardées, la quantité de données modifiées depuis la dernière sauvegarde et la réussite ou l'échec de la sauvegarde.
- **Rapport détaillé sur les activités.** Ce rapport fournit des informations sur les activités d'un site au cours d'une période donnée, y compris les sauvegardes et les restaurations.
- **Rapports récapitulatifs d'utilisation**, etc.

Pour plus d'informations sur le RGPD et sur la manière dont il peut affecter une entreprise, rendez-vous sur : https://www.carbonite.com/what-is-carbonite/gdpr

Confidentialité

Lorsque les gouvernements ou les forces de l'ordre font une demande légale de données clients auprès d'OpenText™, nous nous engageons à faire preuve de transparence et à limiter ce que nous divulguons. Nous pensons que les clients doivent contrôler leurs propres données. L'organisation ne divulguera pas les données hébergées dans un service cloud à un gouvernement ou à un organisme chargé de l'application des lois, sauf sur instruction des clients ou lorsque la loi l'exige. Lorsqu'une demande de données client émanant d'un gouvernement ou d'un organisme chargé de l'application des lois est reçue, nous essayons toujours de rediriger le tiers pour obtenir les données demandées auprès de nos clients.

OpenText™ n'a pas d'accès direct aux données clients. Sans le mot de passe de chiffrement de la tâche fourni par le client ou l'accès au système de l'agent (contrôlé par le client), nous ne pouvons pas déchiffrer les données de sauvegarde.

Pour plus d'informations, veuillez consulter : https://www.carbonite.com/terms-of-use/privacy-policy

Prochaines étapes

OpenText™ Cybersecurity réunit les meilleures solutions de sa catégorie pour aider votre entreprise à rester cyberrésiliente. Nous pouvons vous aider à prévenir les menaces et à vous en protéger, et vous permettre d'atténuer les risques en détectant et en réagissant rapidement, puis en récupérant les données en toute simplicité. Vous réduisez ainsi leur impact et assurez votre conformité au regard de l'évolution des réglementations. OpenText™ Server Backup offre aux entreprises une solution de sauvegarde et de restauration simple et fiable qui préserve en toute sécurité la confidentialité, l'intégrité et la disponibilité des données tout en minimisant les interruptions de service pour vos opérations quotidiennes.

Pour plus d'informations, contactez votre responsable de compte ou le service commercial. Pour en savoir plus, consultez le site d'OpenText.

Copyright © 2025 Open Text • 06.25 | 262-FR0166-001