Bonnes pratiques de sauvegarde et restauration avec SharePoint

AvePoint®
Unleashing the Power of SharePoint™

Ce livre blanc a été conçu pour aider les administrateurs chargés de la gestion des déploiements Microsoft® SharePoint® à planifier et mettre en œuvre une stratégie de protection des données complète, fiable, efficace et adaptée aux besoins de l'entreprise. Il expose notamment les points à prendre en considération pour la planification, les recommandations et la mise en œuvre de la sauvegarde et la restauration avec SharePoint, puis passe brièvement en revue les fonctionnalités individuelles de la solution DocAve® *Backup and Restore*.

Table des matières

Résumé

Les entreprises, quelle que soit leur taille, sont de plus en plus nombreuses à adopter Microsoft SharePoint comme plateforme standard pour la collaboration en ligne, les services de portail et autres services essentiels à leur métier. Mais à mesure que les utilisateurs finaux ont recours à SharePoint dans leurs tâches quotidiennes, les entreprises doivent faire face à la croissance exponentielle du volume de données stratégiques stockées sur cette plateforme ainsi qu'à l'encombrement général qu'elles représentent. Toute entreprise souhaitant rester compétitive se doit donc d'être vigilante et de se préparer à tout désastre imprévu en se dotant de solutions robustes pour la sauvegarde et la restauration de ses données.

Compte tenu du caractère complexe et ramifié du modèle de déploiement SharePoint, mais aussi des contraintes de plus en plus lourdes pesant sur les ressources informatiques, les entreprises ont besoin d'une solution de récupération efficace et complète, qui protège tout l'éventail de données et de composants de leurs fermes SharePoint. Cette solution doit être à même de satisfaire les cahiers des charges et les contrats de niveau de service (SLA) les plus stricts et présenter la modularité nécessaire pour rester performante à mesure que s'étend l'empreinte de SharePoint.

DocAve *Backup and Restore* répond à ces défis en fournissant une solution de sauvegarde et de restauration granulaire, hautement fiables, du niveau de l'élément jusqu'à celui de la plateforme. Le présent livre blanc définit les points à prendre en compte dans la planification et l'implémentation des procédures de protection et de récupération des données avec SharePoint, puis passe brièvement en revue les caractéristiques de DocAve *Backup and Restore*. Il est conçu pour aider les administrateurs chargés de la gestion des déploiements SharePoint à planifier et mettre en œuvre une stratégie de protection des données complète, fiable, efficace et adaptée à l'entreprise.

La réussite du déploiement de SharePoint passe par une gestion efficace, une protection solide, des protocoles de conformité diligents et une disponibilité de chaque instant. Les entreprises s'en remettent de plus en plus à SharePoint pour stocker leurs actifs numériques stratégiques. Ces exigences deviennent des catalyseurs essentiels pour optimiser la production et minimiser le risque d'interruption de l'activité et de perte de données ainsi que les coûts associés. Toute organisation opérant dans un environnement 24/7 doit donc se poser une question fondamentale : à quel point suis-je préparée à faire face à une interruption de cet environnement si essentiel à ma mission ? La réussite dans l'univers actuel, si contraignant, impose aux entreprises d'être convenablement équipées pour assurer un accès constant et ininterrompu à leurs actifs numériques stratégiques.

Mise en place d'un plan de sauvegarde SharePoint efficace

Quelle confiance accordez-vous à la stratégie de reprise actuellement en place pour protéger votre environnement SharePoint ? Une stratégie de reprise SharePoint bien pensée doit viser les objectifs suivants :

- réduction des fenêtres de sauvegarde ;
- respect des objectifs de temps de récupération (RTO) et de point de récupération (RPO) ;
- protection complète de tous les composants de la ferme SharePoint.

Réduction des fenêtres de sauvegarde

Avec l'augmentation rapide du volume de données à sauvegarder au sein du référentiel SharePoint des entreprises aujourd'hui, effectuer les sauvegardes dans les délais est un défi majeur. Une sauvegarde qui s'éternise entraîne souvent un cortège d'effets indésirables : baisse des performances, mobilisation improductive des ressources système et risque accru de perte de données, du fait de la réduction des points de restauration. Ce n'est pas tout : les fichiers ouverts résidant dans la mémoire du système ayant toutes les chances d'être exclus de cette sauvegarde, une procédure trop longue peut se traduire par une plus grande quantité de données incohérentes. Pour réduire les fenêtres de sauvegarde, plusieurs tactiques peuvent être mises en œuvre, séparément ou conjointement :

- réduire le volume des données à sauvegarder ;
- procéder à des sauvegardes incrémentielles ;
- effectuer les tâches de sauvegarde selon un rythme plus approprié à l'entreprise.

La stratégie qui convient le mieux à une entreprise donnée reprend généralement des éléments de ces trois grandes tactiques : passons-les brièvement en revue.

L'une des façons les plus efficaces de réduire les fenêtres de sauvegarde consiste à réduire la quantité de données SharePoint à inclure dans une sauvegarde configurée. Pour ce faire — sans compromettre la protection des actifs numériques — les entreprises doivent déterminer de façon granulaire le caractère critique pour leur activité de chaque site, liste et/ou bibliothèque de documents au sein de leur déploiement. Une fois établi le caractère critique de chacun de ces éléments, il devient possible de leur associer un degré de protection adéquat (c'est-à-dire une fréquence d'exécution de sauvegarde). Ce processus de catégorisation permet aux entreprises de bien différencier leurs données, de sorte que les contenus considérés comme les plus critiques seront sauvegardés plus fréquemment tandis que les données relativement moins importantes seront sauvegardées de façon plus espacée.

La deuxième tactique pour minimiser les fenêtres consiste à espacer les sauvegardes complètes. Une sauvegarde incrémentiélle ne porte que sur les contenus modifiés depuis la sauvegarde précédente, ce

qui permet de réduire considérablement la taille du fichier de sauvegarde créé. Les données restent donc protégées, mais le temps d'exécution et, par là, les fenêtres de sauvegarde, sont réduits.

La dernière tactique que nous aborderons pour réduire les fenêtres de sauvegarde consiste à optimiser la gestion du temps. Quand une sauvegarde est exécutée en dehors des heures de production, les ressources réseau peuvent être entièrement affectées à cette tâche alors qu'une sauvegarde effectuée pendant la production oblige à partager ces ressources avec les utilisateurs finaux et les autres process de l'infrastructure. Il n'est pourtant pas impossible de programmer des tâches de sauvegarde pendant les heures de production, à condition toutefois d'opter pour une méthodologie de sauvegarde « légère », qui ne surcharge pas le système. Cette tactique suppose évidemment la possibilité de programmer ses sauvegardes. Toute stratégie solide de protection des données doit donc comporter des outils permettant une exécution différée.

Respect des objectifs de temps de récupération et de point de récupération

L'un des principaux objectifs de la stratégie de protection des données et de reprise d'activité est de minimiser les interruptions des opérations. L'analyse des tactiques visant à assurer cette continuité doit avoir comme impératif fondamental la restauration des données perdues ou endommagées. La principale préoccupation est de récupérer ses données de façon que le travail puisse reprendre. L'interruption de l'accès aux contenus hébergés sur SharePoint est souvent lourd de conséquences pour la création de valeur, la productivité des utilisateurs finaux et autres objectifs fondamentaux des entreprises. La reprise de l'activité est paramétrée entre autres par deux grandes mesures : l'objectif de temps de récupération (*recovery time objective*, RTO) et l'objectif de point de récupération (*recovery point objective*, RPO).

- **objectif de durée de récupération** (RTO) : délai sous lequel un process opérationnel doit être restauré après un sinistre ou une perte de données pour éviter que les conséquences résultant de l'interruption de l'activité n'atteignent des proportions inacceptables ;
- **objectif de point de récupération** (RPO) : quantité acceptable de données perdues, exprimée en intervalle de temps.

Il arrive que la perte de données résulte d'un sinistre matériel — incendie ou inondation, par exemple — ou d'un dysfonctionnement du matériel. Pour faire face à ces situations, les administrateurs doivent impérativement se doter d'une stratégie de récupération au niveau de la plateforme ; nous y reviendrons plus loin. Mais, le plus souvent, la perte de contenus résulte d'une suppression accidentelle ou d'une corruption localisée et peut donc être résolue sans passer par une restauration complète du système. Les administrateurs SharePoint peuvent alors minimiser le délai de récupération et remplir l'objectif RTO convenant à leur activité en mettant en œuvre des stratégies de récupération à un niveau granulaire. Si seule une petite partie des données nécessite une récupération, la restauration complète du système à partir d'une sauvegarde complète est inadaptée : beaucoup trop longue, elle mobilise inutilement les ressources système. Dans ces circonstances, une stratégie de récupération optimale doit plutôt permettre de ne cibler et restaurer que les objets perdus ou endommagés liés directement à la production. Ce contrôle granulaire de la récupération de données est un élément clé pour atteindre les objectifs RTO les plus exigeants.

Atteindre un objectif RPO adapté à une activité relève aussi de la fréquence des sauvegardes. Les stratégies sont donc essentiellement centrées sur l'intervalle entre deux sauvegardes, aussi bien pour les pertes de données dues à un sinistre matériel que celles liées à un incident ciblé. Les administrateurs doivent donc mettre en œuvre des procédures de protection des données assurant des sauvegardes à des intervalles compatibles avec la perte de données maximum admissible par l'entreprise. Les contraintes varient avec les besoins de chacun, mais si le RPO est de 60 minutes, il faudra pouvoir procéder à une sauvegarde toutes les heures et retrouver des données le cas échéant.

Quand on parle des objectifs RTO et RPO et comme nous allons le voir plus loin, il est important de bien garder à l'esprit que la véritable protection des données ne porte pas uniquement sur la récupération du contenu brut, mais aussi de l'ensemble des métadonnées associées, des historiques des versions et des autorisations d'accès. SharePoint étant par essence une plateforme collaborative, les RPO et RTO définis doivent inclure une récupération des données haute fidélité pour être réellement efficaces. Les administrateurs doivent veiller à ce que leur stratégie de protection des données prévoie la préservation complète de toutes les métadonnées associées aux contenus.

Un support complet pour tous les composants de la ferme

Une ferme SharePoint ne se compose pas uniquement des sites et contenus hébergés par les bases de données SQL Server, mais aussi d'autres éléments qu'il convient de sauvegarder de façon adéquate pour assurer une protection complète face aux sinistres. Il s'agit notamment des bases de données de configuration et d'administration centrale, des applications Internet, des fournisseurs de services partagés (SSP), de l'index de recherche, des configurations IIS et d'autres paramètres personnalisables susceptibles de résider sur des serveurs frontaux, communément appelés le « 12 Hive » pour SharePoint 2007 et le «14 Hive » pour SharePoint 2010. Sans une protection soigneuse de ces composants, la récupération complète d'un environnement SharePoint exigerait un temps d'immobilisation plus long, une reconfiguration complexe et un très grand nombre de tâches manuelles, avec le risque d'erreur humaine que cela comporte. Il est donc recommandé que toute stratégie de reprise d'activité fournisse une protection à l'ensemble des composants de la ferme SharePoint.

Maintenant que nous avons passé en revue les principaux paramètres dont une entreprise doit tenir compte dans son plan de protection des données SharePoint, nous pouvons nous pencher plus en détail sur l'anatomie de la plateforme SharePoint et ses contenus et évoquer les moyens d'assurer une bonne protection pour chacun de ces éléments.

Déterminer les actifs à protéger

Tous les éléments d'un environnement SharePoint doivent être protégés, mais aucune stratégie particulière ne constitue de solution universelle pour tout le déploiement. Les stratégies doivent au contraire s'appliquer aux différents aspects du déploiement en tenant compte de leur fonction, de leur importance pour l'activité et du moyen de restauration. La première étape consiste à distinguer ses actifs SharePoint selon le modèle suivant :

- **Contenu:** c'est l'ensemble des collections de sites, listes, bibliothèques de documents, éléments de listes, documents, fils de discussion, etc., résidant dans SharePoint. Stocké sur une base de données de contenu SQL Server, le contenu est accessible et consultable par l'utilisateur final, que celui-ci soit administrateur, propriétaire de site, propriétaire de contenu ou utilisateur à droits limités. Du point de vue de l'entreprise/activité, le contenu regroupe les actifs les plus critiques de SharePoint : prospects, contacts, états financiers de l'entreprise et autres données sensibles. La perte de ces contenus serait à coup sûr très préjudiciable.
- **Composants de plateforme:** c'est l'ensemble des éléments d'infrastructure nécessaires au fonctionnement de SharePoint. Ces composants représentent l'architecture fonctionnelle de SharePoint et l'utilisateur final n'y a en principe pas accès : bases de données de configuration et d'administration centrale, applications Internet, fournisseurs de services partagés (SSP dans SharePoint 2007, SSA dans SharePoint 2010), index de recherche, configurations IIS, solutions déployées et autres paramètres configurables résidant sur chacun des serveurs frontaux. La gestion et la configuration de ces éléments est généralement du ressort de l'administrateur SharePoint. La perte de ces données est susceptible d'entraîner une interruption de l'accès à la plateforme.

Pour développer une stratégie de sauvegarde adéquate, il est recommandé d'aborder séparément ces deux catégories d'actifs SharePoint. Pour faire simple, disons que les stratégies de protection appropriées à une catégorie ne le sont pas forcément pour l'autre. L'examen des questions abordées dans la partie précédente montre clairement qu'en dépit d'une grande simplicité d'exécution, une sauvegarde de type snapshot pour toute la ferme ne saurait suffire à fournir la protection requise (en termes de RTO et RPO) pour le contenu d'une entreprise standard. Inversement, une stratégie capable de récupérer le contenu peut ne pas permettre de restaurer rapidement les composants complexes de la plateforme et des configurations associées. Tout plan de reprise d'activité solide doit donc fournir un support optimal pour protéger à la fois le contenu et les composants de plateforme plus complexes.

Analyser la taxonomie SharePoint

Bien concevoir sa taxonomie est une condition préalable à l'efficacité de tout déploiement SharePoint. La mise en œuvre d'une taxonomie des contenus efficace fait que le collaborateur est mieux équipé pour tirer parti de SharePoint et organiser les informations non structurées. Une taxonomie bien conçue se met en œuvre de

façon claire et relativement simple, à condition d'être bien planifiée. Pour éviter toute prolifération anarchique des contenus, une série de tâches simples peuvent encadrer une taxonomie efficace : regroupement logique des sites et sous-sites ; catégorisation adéquate des bibliothèques de documents et des listes ; ciblage de l'information en fonction des différentes catégories d'utilisateurs.

Le changement est la seule constante du monde dans lequel évoluent les entreprises de nos jours et une taxonomie bien définie dans SharePoint permet de cadrer efficacement l'organisation des informations, toujours plus nombreuses et toujours changeantes. Les nombreuses dimensions d'une taxonomie bien pensée facilitent non seulement l'accès à l'information pour l'utilisateur final, mais peuvent aussi simplifier grandement la stratégie de sauvegarde dédiée au contenu. Les administrateurs peuvent élaborer leurs plans de sauvegarde granulaire de façon plus efficace quand ceux-ci ciblent des sous-séries de sites, sous-sites ou bibliothèques dont les contenus sont regroupés logiquement par taxonomie. Ce faisant, les administrateurs peuvent attribuer comme il se doit les ressources système et sauvegarde nécessaires pour protéger les différentes catégories de contenus fonctionnels. Le contenu SharePoint considéré comme le plus important pour l'activité (applications de productivité des ventes, par exemple) peut être sauvegardé en priorité tandis que les contenus relativement moins importants (manuels des sites, par exemple) seront sauvegardés à intervalles plus espacés.

Nous reviendrons plus en détail sur ce point en passant en revue les procédures concrètes et les outils disponibles pour cibler et exécuter des sauvegardes en fonction de l'importance des contenus.

Déterminer le volume du contenu

La croissance des contenus fait peser un poids toujours plus important sur les stratégies de sauvegarde existantes. La « stratégie de sauvegarde idéale » est donc toujours une cible mouvante, qu'il s'agit de réévaluer à intervalles réguliers. Il est impératif d'analyser régulièrement et en détail les environnements SharePoint afin de connaître précisément la quantité et le type de contenus à protéger. Il faut pour cela tenir compte de divers facteurs, dont :

- la nature de chaque base de données de contenu : sa taille totale et le type de contenus stockés (éléments de liste, documents, fils de discussion, fichiers mp3, etc.) ;
- le taux de changement des contenus : fréquence d'utilisation/d'accès et volume de données générées par semaine ou par mois.

Tout en considérant les facteurs ci-dessus, il convient de garder à l'esprit que les contenus issus d'une base de données particulière peuvent être sauvegardés vers un environnement de stockage hiérarchisé. Pour mettre en œuvre une stratégie de sauvegarde optimale, les objets de contenu doivent être traités de façon granulaire. Il faut donc disposer d'outils de sauvegarde offrant ce type de précision.

Définir ses contrats de niveau de service

Comme nous l'avons brièvement évoqué plus haut, pour être viable, une stratégie de protection des contenus et de la plateforme SharePoint nécessite l'élaboration d'un contrat de niveau de service (*service level agreement*, SLA) approprié à l'activité. C'est bien souvent l'aspect le plus délicat de l'élaboration d'une stratégie de protection, car il suppose de formuler des conditions générales — sous forme de RTO et RPO — en concertation avec la direction de l'entreprise et les utilisateurs finaux. Un document formel doit être élaboré, qui rassemble les exigences convenues par rapport aux performances de SharePoint. Pour l'administrateur, ces contrats remplissent une double fonction :

- ils font office de principes directeurs pour les détails d'un plan de sauvegarde ;
- ils justifient les exigences de budget et d'attribution de ressources pour l'implémentation dudit plan.

Tout au long de l'élaboration de ce document formel, l'administrateur doit aussi être celui qui ramène ses collaborateurs à la réalité : bien souvent, la direction et les utilisateurs finaux ont des attentes irréalistes sur les niveaux de service faisables. Dans ces circonstances, le niveau souhaité ne correspond pas au degré d'engagement (ressources financières et temps) que ces parties sont prêtes à investir. Les directeurs et utilisateurs finaux exigent souvent une garantie « zéro-perte de données » ou « zéro-interruption », mais sans attribuer l'énergie et les ressources nécessaires pour atteindre ces objectifs. C'est donc souvent à l'administrateur qu'il incombe de les informer sur le coût réel d'un contrat de niveau de service donné.

En plus des mesures explicites (RTO et RPO), un SLA pour SharePoint bien pensé doit définir les catégories suivantes :

- *Parties prenantes* – Ces personnes et groupes de personnes ne se limitent pas à la direction et aux utilisateurs finaux,mais englobent aussi le personnel appelé à jouer un rôle décisif en cas de sinistre. Les fonctions du personnel informatique doivent être clairement définies et les canaux de communication appropriés doivent être mis en place par et entre toutes les parties impliquées (direction, utilisateurs finaux, personnel informatique, etc.).
- *Scénarios de reprise d'activité* – Tous les types de scénarios de reprise envisageables doivent être définis de façon explicite et aussi détaillée que possible. Ces scénarios devront à tout le moins répondre aux questions suivantes : que faire en cas d'effondrement de l'environnement de production tout entier ? Si un site unique est perdu, comment procéder à sa restauration ? Les documents perdus peuvent-ils être récupérés sans une restauration de la ferme tout entière ? Si un long temps d'immobilisation a été prévu, les documents critiques peuvent-ils être restaurés sur un système de fichiers accessible de façon temporaire ?
- *Intégrité des données* – Les utilisateurs finaux doivent savoir à quoi s'en tenir quand des contenus sont restaurés dans un environnement SharePoint. Le document de SLA doit donc définir de façon explicite ce que l'utilisateur peut attendre en termes de préservation des métadonnées, autorisations d'accès et versions. Pour des considérations de productivité et de conformité, la direction doit quant à elle comprendre de façon explicite les implications sur la sécurité et les contenus (et leurs métadonnées).

- *Mesurabilité* – Tous les services décrits dans un document de SLA doivent l'être en termes mesurables. S'agissant du RPO et du RTO, la disponibilité du service doit être définie en pourcentage du temps utilisable, tandis que le délai de récupération doit être égal au temps moyen estimé avant restauration des contenus pour l'utilisateur final. Il peut être utile de représenter la disponibilité de la plateforme en fonction de l'intervalle moyen entre deux défaillances (*mean time between failures*, MTBF) et du temps moyen de réparation (*mean time to recover*, MTTR) :

$$disponibilité = \frac{MTBF}{(MTBF+MTTR)}$$

Comme on le voit, réduire le MTTR a pour effet de maximiser la disponibilité. Cette équation met en lumière l'importance des stratégies offrant une possibilité de restauration granulaire des contenus. Une autre question à se poser est de déterminer la quantité de contenus que l'utilisateur final doit s'attendre à perdre en cas d'immobilisation. Cette quantité est fonction de la fréquence des sauvegardes prévue par chaque plan. Si une bibliothèque de documents est protégée par un plan de sauvegarde incrémentiélle s'exécutant toutes les heures, les utilisateurs finaux peuvent s'attendre à perdre au maximum l'équivalent d'une heure de données en cas de sinistre.

Si tous ces facteurs ont été pris en compte, le SLA fera office de précieux plan directeur et de guide de référence pour toutes les parties prenantes en cas de perte de données ou de défaillance de la plateforme. Un SLA est toutefois un document « vivant » qui, pour être efficace, ne doit pas rester immobile trop longtemps. Il convient donc de le réviser régulièrement, en tenant compte de l'évolution du volume de données et du caractère critique pour l'activité de chaque ensemble de données : c'est vital si l'on veut conserver une protection optimale des données et des stratégies de reprise d'activité dans un environnement où les déploiements et l'organisation évoluent sans cesse.

DocAve *Backup and Restore* fournit une protection des données du spectre complet des composants de Microsoft SharePoint, du niveau de l'élément jusqu'à celui de la plateforme,. Cette solution « best-of-breed » protège des environnements SharePoint tout entiers, depuis des éléments et sites isolés jusqu'aux applications Internet, bases de données de contenu, serveurs d'index et configurations IIS. DocAve *Backup and Restore* assure une récupération à l'identique de l'ensemble des métadonnées, sécurités, historiques des versions et présentations personnalisés. Une programmation des sauvegardes granulaire permet aux organisations de catégoriser leurs données et d'exécuter les tâches en intégrant les contraintes de leur activité et les emplois du temps de leurs structures. En outre, DocAve *Backup and Restore* détecte automatiquement les nouveaux contenus SharePoint et exécute des sauvegardes programmées ou à la demande, complètes, incrémentiélles ou différentielles de ces contenus. Avec DocAve *Backup and Restore*, les entreprises ont la certitude que leur environnement SharePoint bénéficie d'une protection optimale et que leurs SLA sont respectés.

Aperçu de l'architecture système de DocAve

DocAve *Backup and Restore* fait appel à des composants redondants et entièrement distribués pour assurer un temps d'utilisation continu et un basculement pour tout process DocAve en cours d'exécution. Tout en utilisant un modèle agent-serveur qui lui permet de se déployer sur un très grand nombre d'instances et de versions de SharePoint, chacun de ces composants individuels peut être décomposé en services pour une nouvelle répartition de la charge de travail, avec gestion et contrôle centralisés depuis une interface Web unique, accessible partout, sur les réseaux internes de l'entreprise comme sur les réseaux externes. Cette architecture est représentée à la figure 1 ci-dessous.

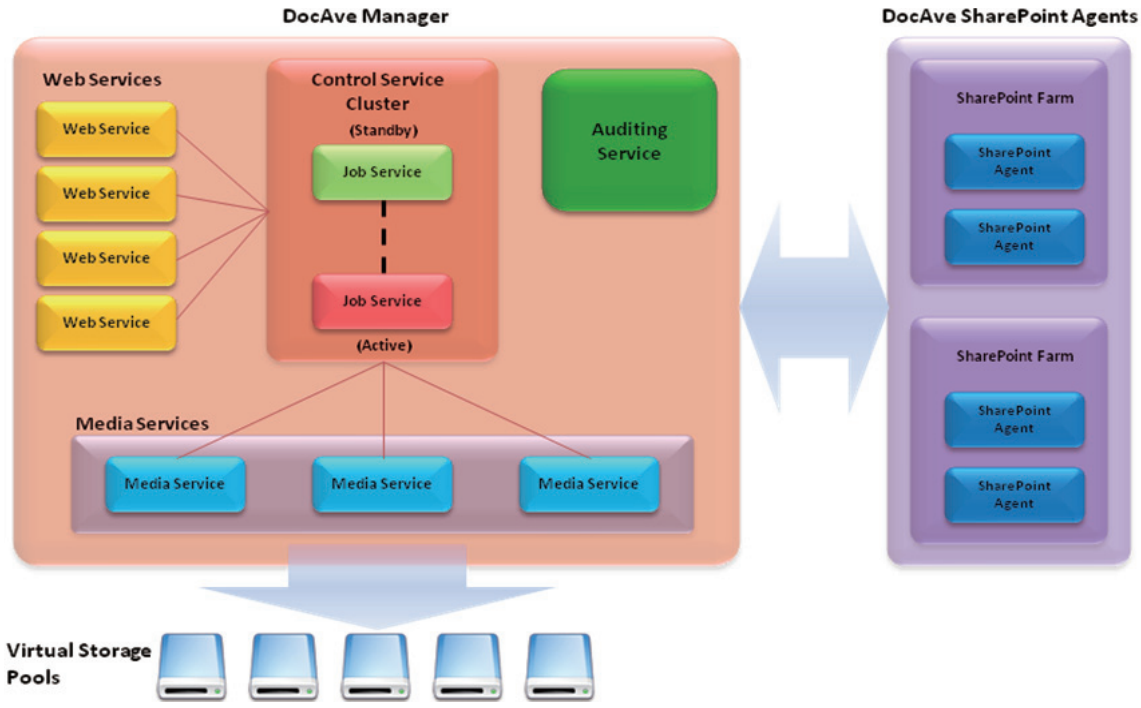

Figure 1 : Architecture système entièrement distribuée de DocAve v5

La solution se compose de trois éléments principaux, chacun conçu pour optimiser la répartition de la charge de travail tout en fournissant une fonction de sauvegarde et de restauration souple, intelligente et granulaire.

Comme on le voit sur la figure ci-dessus, le service DocAve Manager se compose de services Internet à équilibrage de charge, traitant les requêtes/réponses et d'un binôme de services de contrôle actif/passif. Cette architecture haute disponibilité du service de contrôle permet à DocAve de basculer sur le serveur de secours pour continuer à exécuter les tâches en attente.

DocAve Manager

DocAve Manager administre de façon centrale toutes les tâches exécutées par la plateforme logicielle DocAve et permet aux administrateurs de contrôler les routines, de programmer des tâches, de visualiser et d'intervenir sur tout état anormal résultant des agents. Ce gestionnaire peut être installé sur tout matériel opérant sous Microsoft Windows et doté d'une puissance de traitement appropriée et d'un accès aux agents membres à travers le réseau. Il est toutefois recommandé d'installer DocAve Manager sur un système à haute disponibilité, même s'il fournit lui-même un cluster de services de contrôle actif/passif pour assurer une disponibilité continue. L'architecture haute disponibilité du service de contrôle permet à DocAve de basculer sur un serveur de secours pour continuer à exécuter les tâches en attente. DocAve Manager est également le processus serveur chargé de fournir l'interface Web de DocAve au navigateur de l'utilisateur final. Les agents client de DocAve communiquent avec lui via des messages de commande XML légers et des connexions TCP/IP, ce qui permet à un seul gestionnaire de contrôler plusieurs agents et de représenter un réseau distribué de serveurs SharePoint sur plusieurs fermes.

DocAve Media Service

DocAve Media Service est conçu pour fournir des ressources de calcul dédiées pour lire et écrire sur les supports de stockage. Pour les déploiements fortement distribués, il est recommandé de déployer le ou les Media Service(s) à proximité des serveurs Internet frontaux et du support physique de stockage, mais sur un matériel distinct. Il est également recommandé d'héberger le(s) Media Service(s) sur des matériels à haute disponibilité. Il est possible de distribuer plusieurs Media Services dédiés sur plusieurs environnements SharePoint pour gérer une charge de travail supplémentaire et ainsi améliorer la performance globale des tâches de sauvegarde et de récupération. Media Services prend aussi en charge la capacité de persistance des données sur différents supports de stockage logique. Media Services peut être associé à une série limitée de supports de stockage virtuel, de sorte que DocAve puisse attribuer automatiquement les process de sauvegarde via les Media Services désignés. DocAve peut ainsi poursuivre l'optimisation des pools de stockage en fonction de l'activité de l'entreprise ainsi que des SLA en vigueur.

DocAve Agent

Chaque DocAve Client Agent est un composant client léger et spécifique d'une application. S'agissant du DocAve *Backup and Restore*, l'agent est hébergé sur chacun des serveurs de la ferme SharePoint (frontal, applicatif, index, SQL). Ses opérations sont contrôlées par DocAve Manager via des commandes XML sur réseau. L'agent lit et transmet les données sélectionnées via le serveur SharePoint.

Il est possible de faire communiquer entre eux plusieurs agents DocAve, ce qui permet de transférer des données entre environnements SharePoint. Des capacités uniques au sein de l'architecture DocAve veillent à ce que la communication entre agents puisse supporter des canaux de données très bruyants, voire intermittents. Les bons résultats obtenus lors de tests de performances de transfert de données et autres stress-tests très contraignants ont mis en évidence la capacité de tolérance aux pannes de DocAve au niveau des paquets de données.

Points à prendre en compte pour les déploiements à grande échelle

Pour les fermes SharePoint de grandes dimensions, l'architecture distribuée de DocAve *Backup and Restore* permet d'accompagner le développement des besoins de l'entreprise. Il est possible d'optimiser les performances et la gestion des déploiements à grande échelle en tenant compte des points suivants.

Prendre en compte les recommandations d'architecture et les limites de SharePoint

La première étape pour assurer une modularité efficace des plans de protection des données et de récupération est de déployer l'environnement SharePoint en fonction des recommandations de Microsoft, à consulter sur TechNet (http://technet.microsoft.com/fr-fr/library/cc262787.aspx). L'article décrit divers scénarios de tests de la performance et les valeurs indicatives correspondantes pour le déploiement des environnements SharePoint. Ces valeurs définissent un grand nombre de points importants à prendre en considération, notamment :

- limites de la taille de chaque base de données de contenu ;
- nombre maximum de collections de sites par application Web ou base de données de contenu ;
- nombre maximum de documents par bibliothèque de documents.

Ces valeurs indicatives aident les administrateurs à fournir à leur direction et aux utilisateurs finaux des temps de réponse de plateforme précis pour les opérations les plus courantes. Même si chaque déploiement particulier entraîne inévitablement des temps de réponse variables en pratique, ces valeurs indicatives fournissent une base sur laquelle élaborer des estimations pertinentes.

Limiter la taille des sauvegardes par plan

Comme on l'a vu plus haut, le volume de données à sauvegarder est inversement proportionnel à la durée de l'intervalle de sauvegarde qui suit. Une fenêtre plus longue peut entraîner une baisse de la performance, la mobilisation improductive de ressources système et un risque accru de pertes de données ou de données incohérentes. Pour prévenir ce type de problèmes, la règle générale consiste à plafonner chaque plan de sauvegarde à 50 Go de données. Les capacités granulaires de DocAve *Backup and Restore* et le nombre illimité de plans de sauvegarde offrent toute la souplesse nécessaire pour supporter ce type de scénario de déploiement.

Tirer parti de plusieurs Media Services

DocAve *Backup and Restore* supporte le déploiement de plusieurs Media Services DocAve sur différents matériels physiques. À mesure que SharePoint se développe et que de nouveaux contenus exigent des sauvegardes, la probabilité d'avoir besoin de plusieurs tâches de sauvegarde simultanées s'accroît. Afin d'optimiser l'écriture par Media Services des données de sauvegarde sur le support de stockage, il est recommandé de déployer des Media Services supplémentaires pour limiter la charge de chaque serveur média à cinq tâches en parallèle. En outre, du fait que les Media Services doivent être déployés à proximité des serveurs frontaux et des sites de stockage physiques, il est également vivement conseillé de déployer au moins un Media Service par zone géographique.

Utiliser des groupes d'agents à équilbrage des charge

DocAve *Backup and Restore* intègre la capacité de traiter les agents au sein de groupes. En cas de ferme SharePoint fortement distribuée, il est préférable de déployer et d'habiliter un agent au sein de chaque serveur frontal à charge équilibrée, de façon que DocAve puisse automatiquement assigner une tâche de sauvegarde au serveur le moins chargé et ainsi accélérer toute tâche déjà en cours.

Optimiser les plans de sauvegarde

Une fois DocAve *Backup and Restore* déployé, plusieurs approches sont recommandées pour l'implémentation des plans de sauvegarde. En utilisant à plein les capacités intégrées dans DocAve — granularité, création de pools de stockage et planification automatisée de sauvegarde grâce à une matrice — les administrateurs peuvent fournir une protection plus robuste et honorer les SLA même les plus exigeants.

Évaluer ses besoins de stockage

Après avoir déterminé tous les actifs au sein de l'environnement SharePoint nécessitant une protection et calculé à la fois le volume et l'importance critique de ces contenus, l'étape suivante consiste à élaborer des plans de sauvegarde spécifiques dans DocAve *Backup and Restore*. Il faut tout d'abord veiller à ce que les ressources de stockage adéquates soient bien en place pour supporter les routines de protection de données anticipées. Pour déterminer ses besoins de stockage, on se posera les questions suivantes :

- Quel est le matériel nécessaire pour héberger le logiciel de sauvegarde et combien d'espace de stockage une sauvegarde complète va-t-elle occuper ?
- Quelles autres options de sécurités seront implémentées sur le support de stockage ?
- Comment définir les règles d'élagage pour obtenir le meilleur usage possible de ce précieux espace de stockage quand les sauvegardes ne seront plus nécessaires ?

Répondre à ces questions par des estimations précises est une condition clé pour optimiser ses plans de sauvegarde. Cela influe aussi sur la fréquence possible des tâches de sauvegarde complète et sur celle des sauvegardes incrémentiélles dans l'intervalle. De même, en groupant les ressources de stockage disponibles, il est possible de gérer plusieurs volumes en tant que destination unique de sauvegarde pour gérer plus efficacement les sauvegardes de données les plus lourdes.

Estimer l'espace de stockage pour les sauvegardes DocAve

La quantité réelle d'espace de stockage physique nécessaire pour les sauvegardes SharePoint dépend de deux paramètres :

- le volume de données (contenu plus composants de plateforme) ;
- les règles d'élagage de DocAve, qui définissent le nombre de cycles de sauvegarde à conserver.

Les SLA doivent spécifier la longueur et le nombre de sauvegardes à conserver pour supporter convenablement la récupération des divers contenus à protéger. Ces périodes de temps sont étroitement liées aux besoins en ressources de stockage décrites plus haut.

Pour estimer ses besoins en espace de stockage, on peut partir de l'équation suivante :

$$\textit{espace de stockage nécessaire} \cong 1{,}5\ S \times C + S$$

où S représente le volume de données à sauvegarder et C, le nombre de cycles de sauvegarde à conserver.

- Pour chaque cycle de sauvegarde conservé, veillez à ce que soit attribué l'espace de stockage correspondant à un cycle de sauvegarde complète de toutes les données plus la moitié pour tenir compte de toute mise à jour de données pendant le cycle.
- En utilisant DocAve *Backup and Restore*, il est possible de procéder aux tâches d'élagage avant ou après une sauvegarde : il faut donc prévoir de l'espace de stockage supplémentaire pour tenir compte du ou des cycle(s) de sauvegarde complète supplémentaire(s) qui sera/seront exécuté(s) avant l'élagage.

Un autre facteur influant sur l'attribution de l'espace de stockage est le recours à la compression. Utilisée de façon efficace, la compression des fichiers de sauvegarde permet de réduire jusqu'à 75 % les besoins en stockage. En revanche, certains fichiers déjà compressés, au format JPEG ou MP3, par exemple, ne peuvent être réduits de façon significative.

Un dernier facteur à prendre en compte pour l'évaluation des besoins en espace de stockage est le degré d'optimisation parmi les divers plans de sauvegarde. Les contenus sélectionnés pour une sauvegarde peuvent souvent figurer également dans d'autres plans de sauvegarde en chevauchement. Ces contenus risquent donc d'être sauvegardés deux fois. Éliminer les sauvegardes redondantes (c'est-à-dire optimiser les plans de sauvegarde pour supprimer les doublons) permet de récupérer de l'espace de stockage et de réduire les coûts en conséquence.

Configurer des plans de sauvegarde orientés business

SharePoint est une plateforme technologique orientée métier : les solutions de protection des données et de récupération doivent toujours tenir compte des besoins de l'activité. De nombreuses entreprises croient peut-être avoir un plan de reprise complet en place, mais « avoir un plan » ne suffit pas. Encore faut-il qu'il soit applicable à la situation réelle de l'entreprise et à ses besoins et qu'il ait été convenablement validé. Faute de cette validation, il sera difficile de remplir les conditions du SLA en vigueur et de maintenir les process critiques pour l'activité.

Toutes les données ne sont pas égales

Les décisions les plus délicates à prendre pour un administrateur SharePoint au cours de la phase de conception d'une architecture appropriée pour la sauvegarde sont liées à la programmation des sauvegardes en fonction des divers types de données. Pour ce faire, il convient d'évaluer deux critères :

- le caractère critique du contenu pour l'activité ;
- la fréquence d'utilisation de ce contenu.

Un bon moyen de visualiser ces critères et la façon dont ils sont liés est de les représenter sur un diagramme à deux axes (*SharePoint Backup Planning Criticality Matrix*) avec le caractère critique pour l'activité sur l'axe des abscisses et la fréquence d'utilisation sur celui des ordonnées (figure 2). Comme on le voit dans l'exemple ci-dessous, les informations sur les prospects et clients sauvegardéss dans une application de productivité des ventes dans SharePoint sont extrêmement importantes pour l'entreprise : elles revêtent un caractère vital et tout temps d'immobilisation ou perte de ces données est lourd de conséquences. Ce type de contenu est par ailleurs très fréquemment mis à jour, jusqu'à plusieurs fois par heure. Cela signifie qu'il faudra un plan de sauvegarde plus dynamique pour minimiser le volume de données perdues, compte tenu de la fréquence des modifications. Sur le diagramme, ce type de contenu correspond à la cellule située tout en haut à droite. À l'inverse, les contenus mis à jour très peu souvent — une fois tous les six mois, par exemple — et d'importance relativement réduite pour les process opérationnels se trouveront à l'autre extrémité du tableau. Dans notre exemple, il s'agit des guides pour les employés et de la politique de congés, généralement considérés comme moins sensibles et modifiés moins souvent que les prospects ou les informations financières de l'entreprise.

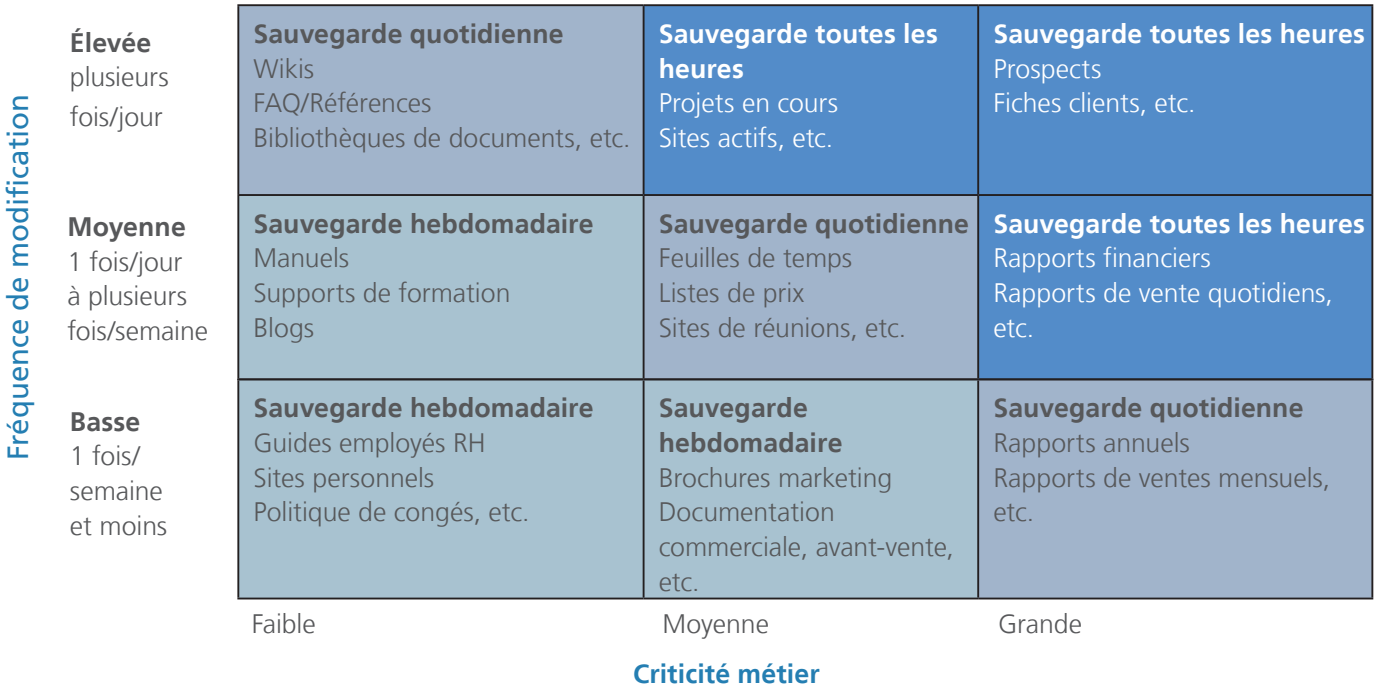

Figure 2 : matrice de planification des sauvegardes SharePoint
(SharePoint Backup Planning Criticality Matrix)

Une fois le caractère critique de tous les contenus évalué, élaborer un plan de sauvegarde devient relativement simple. DocAve permet aux administrateurs de définir un nombre illimité de plans de sauvegarde, comprenant chacun jusqu'à six planifications configurables. Chaque programme peut exécuter une sauvegarde complète, différentielle ou incrémentiélle une fois par heure, par jour, par semaine ou par mois. Les administrateurs disposent ainsi de toute la souplesse possible pour créer une combinaison idéale de programmes de sauvegarde couvrant l'intégralité de l'environnement SharePoint.

Dans l'exemple ci-dessus, le contenu lié à l'application de productivité des ventes peut être protégé par un plan de sauvegarde unique et dédié. Avec ce plan, créé avec DocAve, tous les contenus liés à l'application — collection entière de sites, listes individuelles ou bibliothèques de documents — peuvent être sélectionnés de façon granulaire et plusieurs sauvegardes programmées. Un premier plan consisterait en une sauvegarde totale tous les dimanches soirs. Un deuxième couvrirait toutes les mises à jour par une sauvegarde incrémentiélle toutes les heures.

Pour rester dans cet exemple, le site des RH (cellule tout en bas à gauche) peut être protégé par un plan de sauvegarde distinct exécutant une sauvegarde complète toutes les semaines et des sauvegardes incrémentiélles tous les mercredis soirs.

En appliquant cette démarche à tous les autres sites de l'environnement SharePoint, on peut créer un système de sauvegarde modulaire et flexible qui s'exécute au rythme de l'entreprise, évite les sauvegardes redondantes et assure la sécurité et l'intégrité de tout le contenu de SharePoint.

À partir du concept illustré par le diagramme de la figure 2 (ci-dessus), le module DocAve *Backup and Restore* propose une seconde matrice (*Business Criticality Matrix*, figure 3, ci-dessous) pour classer automatiquement le contenu de SharePoint en fonction de son importance et de sa fréquence d'utilisation. Cette classification automatique permet d'optimiser les ressources de stockage et les ressources système et d'exécuter des sauvegardes conditionnelles à partir d'analyses en temps réel des données au niveau des éléments.

En utilisant DocAve *Backup and Restore*, les propriétaires de contenu ont la possibilité de spécifier l'importance d'un site donné : le logiciel l'affecte alors automatiquement à la cellule correspondant à son importance et à sa fréquence d'accès. En fonction de l'activité des utilisateurs finaux, DocAve ajuste automatiquement le classement de chaque site au sein de la matrice si l'un de ces deux critères évolue. Pour chaque cellule, les administrateurs peuvent appliquer des plans de sauvegarde plus dynamiques (une fois par jour ou une fois par heure, par exemple) aux contenus couverts par des SLA plus contraignants.

Figure 3 : Diagramme de sauvegarde DocAve 5.0

En automatisant le processus de classification et en effectuant un suivi de l'utilisation de SharePoint, DocAve permet d'honorer les contrats de niveau de service différenciés et d'optimiser l'usage des ressources.

Granularité des sauvegardes

Les plans de sauvegarde peuvent être créés au niveau des collections de sites, des sites ou des éléments individuels. La sélection du niveau qui convient dépend de plusieurs facteurs.

Le premier concerne la granularité avec laquelle différencier les données pour les sauvegardes. Il peut arriver que les sites soient déjà organisés de façon logique : associer un plan de sauvegarde à chaque collection de sites ou site individuel est alors une procédure simple. Cela permet aussi de réduire le nombre de plans de sauvegarde à gérer et de limiter ainsi le risque de doublons.

Le deuxième facteur concerne les options de restauration appropriées au contenu. DocAve *Backup and Restore* indexe les fichiers de sauvegarde pour la restauration en fonction du « niveau » de récupération choisi. Une sauvegarde au niveau du site, par exemple, ne permettra la restauration que de sites entiers, tandis qu'une sauvegarde au niveau des éléments permettra de restaurer les éléments de contenu pris séparément ou les différentes versions d'un même élément. Il faut garder en tête que les plans de sauvegarde au niveau des éléments couvrent aussi des sites ou des collections de sites entiers, ainsi que les sites imbriqués créés. En somme, la sélection du niveau approprié de sauvegarde dépend d'une part du niveau de granularité nécessaire à la restauration et de l'autre du temps attribué (défini par le SLA) pour l'exécution de la tâche de sauvegarde[1]. Il est recommandé de toujours commencer par les sauvegardes au niveau des éléments, puisqu'elles fournissent non seulement une souplesse optimale dans la différenciation des données, mais aussi une capacité de restauration au niveau des éléments ou des versions d'élément.

Le dernier facteur à prendre en compte pour déterminer le niveau de sauvegarde est la nature exacte des données à restaurer à chaque niveau. Les fichiers générés par les sauvegardes au niveau du site sont généralement plus lourds que ceux des sauvegardes au niveau des éléments, puisqu'ils englobent la totalité des actifs du site en question. Il faut envisager l'impact sur l'attribution des ressources de stockage, sachant que les tâches de sauvegarde incrémentiélle de sites entiers s'exécuteront à nouveau même si un seul élément de contenu a été modifié depuis la sauvegarde complète précédente.

[1]Compte tenu de la nécessité d'indexage pendant les sauvegardes au niveau des éléments, le temps nécessaire pour l'exécution de ce type de sauvegarde est plus important que pour une sauvegarde au niveau du site pour un même site. En cas de sauvegarde incrémentiélle, toutefois, la sauvegarde au niveau du site peut prendre plus de temps, sachant que la tâche va essayer de sauvegarder le site tout entier même si la différence ne porte que sur un seul document.

Accès filtré aux données de sauvegarde

L'accès filtré à la restauration des données de sauvegarde de SharePoint aide les entreprises à répartir la charge de travail administratif qui pesait jusque alors sur les seuls administrateurs de ferme. Ceci permet d'optimiser les ressources informatiques et de réduire les objectifs RTO et RPO.

DocAve propose non seulement des outils pour exécuter des captures en temps réel des événements de suppression au niveau du site (la fonctionnalité SiteBin de DocAve *Backup and Restore*), mais fournit aussi un accès filtré à DocAve pour les propriétaires de collections de sites ainsi qu'une fonction *Restore Webpart* sécurisée elle aussi. SiteBin exécute une capture en temps réel des sites supprimés de SharePoint, ce qui permet de réduire à zéro le RPO d'un site effacé par erreur. Les propriétaires de sites et les administrateurs peuvent aussi procéder à des restaurations directes de leurs propres contenus par le biais de DocAve ou d'un webpart installé sur DocAve directement dans SharePoint pour assurer une reprise d'activité dans les meilleurs délais et minimiser la perte de données en cas de suppression accidentelle. Les permissions AD des propriétaires de collections de site peuvent être intégrées à DocAve pour veiller à ce que leur accès soit limité aux contenus dont ils sont propriétaires. Si l'on exploite cet outil pour récupérer un site unique, une liste/bibliothèque, un élément ou un document d'un site effacé, l'utilisateur final n'est plus obligé de passer par l'administrateur de ferme ou l'administrateur DocAve.

Déléguer en toute sécurité la restauration des données

De nombreuses tâches administratives jusqu'à maintenant dévolues aux administrateurs de fermes peuvent être déléguées à condition de disposer de fonctionnalités de restauration filtrées sur les droits (security-trimmed). Au-delà de l'économie de ressources informatiques, cela améliore également le temps et le point de restauration.

DocAve propose non seulement des outils pour intercepter en temps réel les suppressions de sites ou de collections de sites (DocAve SiteBin), mais permet également à chaque propriétaire de collection de site de restaurer lui-même ses données via un Webpart dédié à cet effet. DocAve SiteBin réalise une capture en temps réel des sites à l'instant où ils sont supprimés de SharePoint, garantissant un RPO de zéro pour un site accidentellement supprimé. Les propriétaires et administrateurs de sites peuvent également restaurer leur propre contenu via DocAve ou via un web part directement installé dans SharePoint. Il est possible d'intégrer les permissions AD à DocAve pour que chaque responsable de collection de site ne puisse restaurer des données que dans ses propres sites. Ainsi, des tâches comme la restauration d'un site, d'un élément, d'un document ou d'une liste peuvent se faire sans intervention des administrateurs de ferme.

Prévoir les scénarios de récupération possibles

Une fois leurs plans de sauvegarde bien en place pour fournir une protection adéquate à l'environnement SharePoint, les administrateurs doivent prévoir les différents scénarios de récupération possibles. Ici encore, la granularité est un élément clé, puisqu'une tâche de récupération quelle qu'elle soit doit non seulement remplir les critères du SLA convenu, mais aussi présenter l'impact minimum sur l'activité de l'environnement.

Il est important de garder à l'esprit le fait que les procédures de récupération peuvent aussi être déléguées à d'autres utilisateurs dotés des permissions d'accès nécessaires à DocAve. Le personnel d'assistance informatique, par exemple, voire les propriétaires du site ou du contenu eux-mêmes, peuvent parfois procéder à des tâches simples de récupération d'éléments perdus ou endommagés. La récupération complète de la plateforme reste quant à elle du seul ressort du ou des administrateur(s) SharePoint.

Voici une liste de quelques événements courants à prévoir, qui peuvent nécessiter une récupération :

- *Défaillance matérielle* – La défaillance matérielle entraîne généralement un temps d'immobilisation de l'environnement. Il est important dans ce cas d'être prêt à mettre en ligne une ferme SharePoint en stand-by dans les meilleurs délais possibles, conformément aux conditions convenues dans le SLA. Si l'environnement de production a été configuré en haute disponibilité, il est possible de minimiser la perte de données grâce aux technologies pour mettre à jour les contenus sur l'environnement de stand-by (DocAve *High Availability* possède cette fonction). Dans le cas contraire, une solution temporaire consistera à exécuter une restauration des contenus « out-of-place » vers un environnement SharePoint distant.

- *Erreur humaine* – Il peut arriver qu'un utilisateur, un développeur ou un administrateur efface accidentellement un contenu, supprime des collections de sites entières ou commette une erreur en modifiant une configuration. Ces erreurs sont la principale raison à l'origine de la récupération d'un site ou d'un contenu.
- *Virus, corruption de données, etc.* – La fonction native *Recycle Bin* de SharePoint ne saurait mettre les utilisateurs finaux à l'abri d'une corruption de contenu. Le fichier corrompu devra être écrasé par un fichier de sauvegarde intact.
- *Destruction d'un centre de données* – La destruction d'un centre de données impose une récupération complète de la plateforme, probablement sur une ferme SharePoint séparée, pouvant être mise en ligne sur un site à part. Pour mieux faire face à un sinistre de ce type, il est également possible d'opter pour une stratégie de haute disponibilité en recourant à des technologies telles que le *mirroring SQL* ou le *log shipping* pour créer un environnement SharePoint pour une reprise à chaud. Dans ce cas, la perte de données sera fonction de la fréquence de la copie de contenus.

Avec ses fonctionnalités de sauvegarde et restauration automatisées et orientés métier et son interface graphique avec points de restauration, DocAve est bien parti pour changer en profondeur une fois encore la façon dont les administrateurs gèrent et protègent SharePoint.

Comme nous l'avons déjà vu, le contenu est l'actif le plus important de tout déploiement SharePoint, puisqu'il représente la propriété intellectuelle essentielle aux opérations. Mais un autre facteur joue un rôle essentiel : c'est l'infrastructure sous-jacente au déploiement SharePoint, qui regroupe un grand nombre de composants de niveau plateforme, étroitement reliés les uns aux autres pour créer un environnement de travail. Compte tenu du nombre très élevé de ces « pièces en mouvement » dans une plateforme SharePoint, il suffit qu'un seul composant présente une défaillance pour que l'environnement tout entier soit affecté.

DocAve *Backup and Restore* assure une protection complète non seulement du contenu hébergé par la ou les base(s) de données, mais aussi de tout l'éventail des composants de niveau ferme avec leurs configurations. La base de données de configuration, les applications web, les serveurs de recherche et d'index, les configurations IIS et autres objets du système de fichiers au niveau du serveur web frontal bénéficient ainsi d'une protection rapprochée.

Exécuter une sauvegarde complète de la ferme

Pour l'utilisateur de DocAve, la création d'une sauvegarde de niveau plateforme avec DocAve *Backup and Restore* ne diffère guère de celle aux niveaux collection de sites, site ou élément. Les administrateurs peuvent programmer des plans pour exécuter des sauvegardes complètes, incrémentiélles ou différentielles sur les serveurs où sont installés les agents DocAve. S'agissant d'une sauvegarde de niveau plateforme visant à mettre l'environnement à l'abri de tout sinistre, le ou les fichiers de sauvegarde ainsi créés doivent être stockés sur un site différent de celui de la ferme SharePoint de base : c'est ce qui permet de conserver l'accès aux sauvegardes SharePoint même si la ferme dans son ensemble n'est plus fonctionnelle. Les options telles que la rétention des données (élagage), leur cryptage et leur compression sont les mêmes que celles décrites dans la partie consacrée à la sauvegarde des contenus. Certaines options, toutefois, sont spécifiques à la sauvegarde de niveau plateforme.

Choix entre VDI et VSS

Pour la sauvegarde de niveau plateforme, DocAve *Backup and Restore* offre le choix entre l'application VDI (*virtual device interface*) pour SQL Server et la technologie de snapshot Microsoft Volume Shadow Copy Service (VSS). La VDI est une méthode de protection des bases de données SQL *basée sur les flux* tandis que le VSS exploite divers *VSS writers* issus de la plateforme Windows Server et des applications. Les deux technologies présentent plusieurs grandes différences, dont les administrateurs doivent avoir conscience avant de sélectionner la méthode de sauvegarde qui leur convient. Par exemple, le VSS étant une technologie de snapshot, il présente un impact minime sur les serveurs SQL de production et n'entraîne aucune interruption du process d'indexation pendant l'exécution d'une tâche de sauvegarde. En revanche, le VSS ne prend pas encore en charge les restaurations distantes : tous les composants de niveau ferme ne peuvent donc être restaurés qu'à leur emplacement d'origine.

Veuillez consulter le guide de l'utilisateur DocAve *Backup and Restore* pour un comparatif complet entre les technologies VDI et VSS.

Coexistence avec les sauvegardes SQL Server et IBM Tivoli

Les administrateurs de base de données ont généralement des plans de sauvegarde pour SQL Server afin de protéger la ou les base(s) de données en cas de sinistre. Ces serveurs de base de données sont ceux utilisés pour les applications personnalisées ou autres référentiels opérationnels, ainsi que toutes les bases de données de contenu et de configuration de SharePoint. Les sauvegardes de niveau plateforme de DocAve *Backup and Restore* peuvent coexister avec des utilitaires de sauvegarde de base de données institutionnels et prévenir automatiquement tout conflit. Il est donc recommandé de conserver ses sauvegardes SQL Server telles qu'elles sont et de ne protéger que les bases de données de contenu SharePoint avec DocAve.

façon holistique un environnement SharePoint entier par le biais d'une sauvegarde DocAve plutôt que d'avoir à gérer les sauvegardes ou la restauration de serveur SQL avec un utilitaire distinct.

En plus de cette fonction, DocAve permet aux administrateurs de restaurer un contenu directement à partir de sauvegardes du serveur SQL préexistantes, ainsi que de sauvegardes sur IBM Tivoli Storage et Microsoft Data Protection Manager (DPM). DocAve est également compatible avec EMC Centera Storage, qui identifie automatiquement les doublons pour une réduction supplémentaire de l'espace de stockage.

Identifier et sélectionner les composants à protéger

À l'instar de la fonction de sauvegarde aux niveaux collection de sites, site et élément, la sauvegarde par DocAve au niveau plateforme propose une arborescence affichant les divers composants disponibles à la sélection granulaire pour chaque plan. Ces composants de niveau plateforme sont notamment :

- la base de données de configuration de la ferme SharePoint ;
- les bases de données de contenu / applications web;
- la base de données de contenu d'administration centrale ;
- la base de données de configuration des paramètres de recherche globale ;
- pour SharePoint 2007 : les composants liés au fournisseurs de services partagés (SSP), notamment la base de données SSP, les bases de données Project Server, la base de données de recherche et l'index ;
- pour SharePoint 2010 : les composants liés aux applications de services partagés (SSA), y compris les métadonnées d'entreprise (managed metadata) et les bases de données associées ;
- les fichiers d'installation des solutions SharePoint ;
- les InfoPath Form Services et tous les modèles de formulaires installés sur le serveur web frontal et la configuration des Form Services ;
- la configuration et la base de données d'authentification unique (SSO) ;
- les composants de serveur web frontal, notamment les configurations IIS, les modèles SharePoint sous le « 12 hive » ou le « 14 hive », les fonctions personnalisées, les définitions de sites personnalisées et autres répertoires de système de fichiers ;
- le kit de formation SharePoint.

Concernant les composants des serveurs web frontaux, plusieurs configurations SharePoint ne sont pas stockées dans la base de données de configuration, mais hébergées sur le système de fichiers du serveur lui-même. Les configurations telles que la configuration SSL, l'authentification par formulaire et la configuration des Web Part sont situées dans le fichier de configuration IIS web.config. Les templates, définitions de site et fonctions personnalisés sont quant à eux déployés dans le « SharePoint hive »[2] . Ces personnalisations doivent être incluses dans les sauvegardes, de sorte que les administrateurs n'aient pas à les reprendre une fois l'environnement restauré. L'arborescence fournie par DocAve peut se développer dans le système de fichiers du serveur web frontal, si bien que toute autre dépendance externe à la configuration SharePoint peut également être protégée par le même plan de sauvegarde.

[2]Le « SharePoint Hive » est un dossier nommé « 12 » pour SharePoint 2007 ou « 14 » pour SharePoint 2010 et il se trouve à l'emplacement suivant : C:\Program Files\Common Files\Microsoft Shared\web server extensions\

Déterminer le degré de granularité de la restauration

L'arborescence des composants de SharePoint de DocAve permet aux administrateurs de zoomer pour sélectionner de façon granulaire les composants de chaque ferme à protéger pour chaque plan de sauvegarde. Les administrateurs ont ainsi toute latitude pour regrouper certaines applications web, bases de données de contenu et autres composants individuels dans leurs plans de sauvegarde personnalisés. En outre, DocAve leur permet de sélectionner simplement une ferme SharePoint tout entière pour que tout composant enfant qu'elle renferme soit automatiquement protégé par un plan de sauvegarde unique. Même les composants nouvellement créés sont automatiquement couverts par cette protection.

Quelle que soit la granularité avec laquelle les plans de sauvegarde sont définis, DocAve *Backup and Restore* permet d'indexer les sauvegardes de niveau plateforme pour une récupération au niveau des éléments, ou même des versions d'un élément, en autorisant la sélection du degré de granularité adéquat au moment de la définition du plan. Si ce degré de granularité de la restauration est défini à « site », le processus de sauvegarde indexera le fichier de sauvegarde pour qu'il permette une restauration au niveau du site. S'il est défini à « élément », il sera possible de restaurer jusqu'à des éléments individuels à partir d'une sauvegarde de ferme complète.

Processus de récupération de ferme complète

En cas de défaillance grave d'une ferme SharePoint, il peut être nécessaire de récupérer la ferme dans son intégralité en recourant à une sauvegarde de niveau plateforme. Cette procédure suppose que le système remplisse une série de conditions préalables :

- Windows Server 2008 R2 ou Windows Server 2008 avec Service Pack 2
- IIS avec ASP.NET activé ;
- NET Framework 3.0 ;
- Microsoft SharePoint Server 2010 installé, mais pas configuré (si une ferme existante a déjà des serveurs web frontaux déployés, ceux-ci doivent tous être déconnectés par le biais de l'Assistant Configuration des produits et technologies SharePoint) ;
- le niveau de patch de SharePoint doit rester le même ;
- le(s) nom(s) du serveur et la topologie doivent rester les mêmes ;
- la disposition des disques SQL Server doit rester la même ;
- utiliser le même compte domaine pour l'administration de SharePoint.

Si toutes ces conditions sont remplies, la ferme peut être récupérée par un simple chargement de la sauvegarde de plateforme appropriée par le biais de DocAve Restore Controller. En raison des dépendances entre les divers éléments de la ferme SharePoint, cette procédure de restauration se fait généralement par étapes. Pour que les serveurs web frontaux puissent être attachés, il faut tout d'abord que la base de données de configuration et les bases de données d'administration centrale aient été restaurées. Une fois cette étape achevée, les serveurs web frontaux peuvent être mis en ligne et connectés à la base de données de configuration restaurée à l'aide de l'Assistant Configuration SharePoint. Il est important de ne pas perdre de vue le fait que l'un de ces serveurs web frontaux devra héberger l'application web d'administration centrale.

Une fois les serveurs web frontaux mis en ligne, d'autres composants de niveau ferme peuvent à leur tour être restaurés : IIS personnalisés (authentification SSL ou par formulaire, web.config, etc.), solutions personnalisées, fournisseurs de services partagés, authentification unique, etc.

Veuillez noter que tout composant lié au front-end ainsi restauré (configuration IIS, définitions et fonctions de site personnalisées, etc.) doit l'être sur tous les serveurs web frontaux de la ferme SharePoint.

Pour tout complément d'information sur DocAve, veuillez consulter notre site : www.avepoint.com

AvePoint France
6 place de la Madeleine
75008 Paris
Call: +33 1 70 80 01 39
Email: SalesFR@avepoint.com