Xerox® Digital Alternatives
Guide d'utilisation du logiciel de sécurité et d'évaluation

Octobre 2016
Version 2.0.xx

Ce document fait régulièrement l'objet de modifications. Les inexactitudes techniques et les erreurs typographiques seront corrigées dans les prochaines versions.

Historique des révisions

Date	Numéro de version	Description
Octobre 2016	2.0.xx	• Mise à jour d'après publication concernant le chiffrement en cours des adresses électroniques
Janvier 2016	2.0	• Ajout des nouvelles fonctionnalités de Digital Alternatives 2.0
Mai 2015	1.2	• Ajout de la fonctionnalité de déploiement sur cloud privé de Digital Alternatives 1.2
Mars 2015	1.1	• Réorganisation majeure conformément au modèle de la documentation de sécurité interne • Mises à jour de la version 1.1, incluant la présentation de la prise en charge du cloud
Août 2014	1.0	Première version

Sommaire

Figures

1 Introduction

Aperçu du produit

Xerox® Digital Alternatives est un service logiciel qui prend en charge la lecture, l'annotation et le partage numériques de documents. Sitôt enregistré sur le client Digital Alternatives d'un utilisateur, un document est automatiquement répliqué sur tous les PC et périphériques iPad de l'utilisateur sur lesquels le client Digital Alternatives est installé. Divers utilisateurs peuvent également se partager le document annoté via l'application, ainsi que par voie de messagerie.

Xerox® Digital Alternatives est constitué de cinq composants essentiels.

Composant	Description
Serveur local de Xerox® Digital Alternatives	• Effectue les tâches d'authentification. • Réplique les documents sur les autres périphériques de l'utilisateur et sur les périphériques d'autres utilisateurs.
Logiciel End User Client	• S'installe sur le PC Windows®, l'iPad® ou les tablettes Android™ prises en charge, ou sur l'ordinateur Apple Macintosh® de l'utilisateur final. • Affiche les documents à des fins de consultation et d'annotation.
Xerox® CompleteView® Reporting Data Communicator	• Transmet les données d'utilisation du serveur local de Digital Alternatives à la plateforme de rapports Digital Alternatives CompleteView® hébergée au sein de Xerox.
Digital Alternatives CompleteView Reporting	• Utilise les informations d'utilisation Digital Alternatives récupérées sur le serveur local de Xerox® Digital Alternatives pour analyser les avantages de l'utilisation pour le client d'après les paramètres standard du secteur. Hébergé au sein du réseau Xerox.
Serveur central de Digital Alternatives sur Internet	• Stocke les informations de compte et les données de licence utilisées par le serveur local et les clients.

Méthodes de déploiement du serveur local de Xerox® Digital Alternatives

Implémentation sur site

Grâce à la méthode d'implémentation sur site, ce composant effectue toutes les tâches d'authentification avec le service d'annuaire informatique Active Directory® du client au nom de l'utilisateur de Xerox® Digital Alternatives. L'utilisateur fournit les informations d'identification par le biais de l'application End User Client de Xerox® Digital Alternatives. Le serveur local de Xerox® Digital Alternatives effectue une autre tâche capitale, à savoir la réplication des documents sur les autres périphériques de l'utilisateur, ainsi que sur ceux d'autres utilisateurs en cas de partage des documents. Le serveur local de Xerox® Digital Alternatives procède également à une recherche d'adresses globale au profit de l'application

End User Client de Xerox® Digital Alternatives lors du partage de documents avec d'autres utilisateurs de Digital Alternatives. Par ailleurs, si un document est partagé avec un utilisateur qui ne possède pas Digital Alternatives, le serveur local de Xerox® Digital Alternatives envoie le document par le biais du serveur de messagerie du client pour l'application End User Client de Xerox® Digital Alternatives. Le serveur local de Xerox® Digital Alternatives s'interface avec le serveur central sur Internet pour fournir des documents sur demande à des utilisateurs situés à l'extérieur de l'infrastructure réseau du client.

Implémentation sur cloud privé

Xerox offre la possibilité d'héberger le serveur local au sein du réseau en cloud privé de Xerox® au nom du client de Digital Alternatives. Dans ce cas, toute installation du logiciel serveur sur site est inutile, et le client ne s'occupe plus de gérer le serveur physique puisque Xerox en assume l'entière responsabilité. Grâce à la méthode de déploiement en cloud privé, une connexion VPN dédiée s'impose entre le réseau du client et l'environnement en cloud privé de Xerox®. Un accès aux ressources Active Directory et Exchange LDAP du client depuis le serveur d'applications en cloud privé assuré en toute sécurité par le biais de la connexion VPN établie est également requis. La méthode d'implémentation sur cloud privé prend en charge les mêmes fonctionnalités de serveur local que la méthode d'implémentation sur site.

Mode d'emploi du guide

Le présent guide a pour but d'aider les représentants commerciaux de Xerox ou de ses partenaires à fournir aux services informatiques de leurs prospects des informations sur Digital Alternatives en matière de sécurité afin de contribuer à la certification du déploiement de Xerox® Digital Alternatives dans l'environnement des clients. Les clients et le personnel de Xerox pourront utiliser ce guide dans le cadre du processus d'évaluation avant-vente, d'analyse après-vente et d'acceptation. Les protocoles de test et les critères d'acceptation réels dépendront des formalités ou de la documentation requise du client. Ce document contient des informations relatives à l'impact potentiel de Xerox® Digital Alternatives sur la sécurité, l'infrastructure informatique de l'entreprise, le trafic réseau, les ressources et la planification requise.

Utilisez ce guide principalement pendant l'implémentation et après la signature du contrat, mais également au cours des activités avant-vente et d'évaluation sous réserve de la signature d'un accord de confidentialité.

Public visé

Ce guide s'adresse au service informatique, au service chargé de la sécurité et au service de gestion du client, ainsi qu'à l'équipe de direction. Avant de certifier Xerox® Digital Alternatives, les clients et le personnel Xerox concerné doivent parfaitement maîtriser les éléments suivants :

- L'environnement informatique du site où Xerox® Digital Alternatives sera installé
  - En cas d'hébergement du serveur local sur cloud privé, il importe de comprendre la nature de la connectivité VPN et ses aspects en matière de sécurité.
- Toutes les restrictions imposées sur les applications qui sont déployées sur le réseau
- Le système d'exploitation Microsoft® Windows Server®
- Le système de base de données Microsoft SQL Server®

Limites appliquées à ce guide

La solution Xerox® Digital Alternatives offre plusieurs possibilités de configuration et possède un grand nombre de fonctionnalités. Ce guide présente les implémentations standard et un environnement informatique type. Si l'environnement informatique du client diffère de celui décrit dans ce guide, l'équipe informatique du client et le représentant Xerox devront identifier les différences et résoudre tous les problèmes éventuels.

Les informations contenues dans ce guide portent sur la version 2.0 de Xerox® Digital Alternatives. Bien que les informations demeurent en grande partie les mêmes tout au long du cycle de vie du logiciel, certaines données fournies peuvent faire l'objet d'une révision et nécessiteront à ce titre des mises à jour régulières. Les services informatiques doivent se procurer la version adéquate auprès du représentant Xerox.

Nouveautés de la version 2.0

La version 2.0 de Digital Alternatives offre un certain nombre de nouvelles fonctionnalités.

- Divers flux de travail documentaires intégrés permettent aux clients d'effectuer des tâches courantes telles que la consultation, l'approbation et la signature de documents entre les utilisateurs de Digital Alternatives.
- L'intégration avec le service de signature électronique DocuSign® permet aux utilisateurs d'envoyer des documents pour signature à l'aide de leur compte DocuSign existant en vue d'obtenir des signatures numériques légales.
- Digital Alternatives propose désormais une intégration native avec la plateforme de gestion de contenu Xerox® DocuShare®, qui permet d'importer et d'exporter des documents via la solution de gestion de contenu électronique DocuShare.
- Par ailleurs, le logiciel client Digital Alternatives est désormais pris en charge sur deux nouvelles plateformes d'hébergement, les tablettes Google Android et les ordinateurs Apple Macintosh.

Flux de travail documentaires Digital Alternatives

Digital Alternatives propose une fonction intégrée de gestion de flux de travail documentaires. Les utilisateurs peuvent envoyer des documents au sein de Digital Alternatives à un autre utilisateur à des fins de consultation, de signature ou d'approbation. Chaque fonction de flux de travail informe le destinataire des nouvelles demandes de flux de travail. Dès que le destinataire de la demande a terminé la tâche qui lui a été assignée, le document traité est estampillé avec la date de réalisation, puis automatiquement renvoyé au demandeur accompagné de commentaires.

Toute personne externe au système Digital Alternatives peut demander des flux de travail. Dans ce cas, le document est envoyé en pièce jointe d'un courrier électronique, mais n'est pas renvoyé au demandeur au sein de Digital Alternatives une fois traité.

Intégration avec le service de signature électronique DocuSign®

Pour les clients qui possèdent un compte de signature électronique DocuSign d'entreprise, les utilisateurs de Digital Alternatives peuvent envoyer un document à un destinataire à des fins de signature à l'aide du compte DocuSign de l'expéditeur. Le document est automatiquement chargé sur le compte DocuSign de l'expéditeur, où le destinataire reçoit un courrier électronique de DocuSign l'informant d'une demande de signature en attente. Sitôt le document chargé sur DocuSign, la demande de signature est traitée au sein de DocuSign. Une fois que le destinataire a traité la demande de signature, le document signé n'est pas automatiquement renvoyé au compte Digital Alternatives de l'expéditeur, mais est conservé dans DocuSign.

Intégration avec le système de gestion de contenu électronique Xerox® DocuShare®

Digital Alternatives peut charger et télécharger des documents sur un système DocuShare configuré au sein de l'application cliente Digital Alternatives. Pour accéder à DocuShare, l'utilisateur doit posséder un compte utilisateur DocuShare natif indépendant du compte utilisateur avec lequel il accède à Digital Alternatives. L'application cliente Digital Alternatives doit par ailleurs avoir un accès réseau direct au serveur DocuShare afin que l'accès intégré fonctionne. L'utilisation de cette fonctionnalité peut donc s'avérer impossible pour les utilisateurs qui travaillent en dehors de leur réseau d'entreprise, à moins que leurs périphériques clients soient connectés à ce réseau via une connexion VPN.

Nouvelles plateformes d'hébergement d'applications clientes : Google Android et Apple Macintosh

L'application cliente Digital Alternatives prend en charge les ordinateurs Apple Macintosh et certaines tablettes Google Android, outre les ordinateurs Windows et tablettes Apple® iPad existants. Consultez le guide d'administration de Xerox® Digital Alternatives pour obtenir une liste des périphériques pris en charge par l'application cliente Digital Alternatives.

Gestion des licences logicielles

La gestion des licences logicielles s'effectue au niveau du compte client stocké sur le serveur central de Digital Alternative. Ni le logiciel End User Client ni le serveur local ne font l'objet d'une licence spécifique ; en revanche, la première fois qu'un nouvel utilisateur final client se connecte à son compte Digital Alternatives, le nombre global de postes sous licence disponibles tel que géré dans le serveur central diminue d'une unité. Cette connexion initiale d'un client est appelée « intégration ». La désinstallation du logiciel End User Client n'incrémente pas le nombre de licences affectées au sein du serveur central. Sitôt que les clients intégrés ont épuisé le nombre de licences disponibles sur le serveur central, vous devez vous procurer d'autres postes sous licence auprès de Xerox.

Il est possible de récupérer les postes sous licence d'un utilisateur à l'autre en désactivant le compte d'un utilisateur dans le serveur local afin de l'empêcher d'utiliser Digital Alternatives. Lorsqu'un utilisateur est désactivé, les licences affectées à son compte sont récupérées et rajoutées aux postes sous licence disponibles pouvant être affectés à un autre utilisateur au sein du compte client.

Conformité et certification des applications

Implémentation - Service informatique chez le client

Au final, il appartient au service informatique du client de certifier et d'accepter le déploiement et le fonctionnement de la solution Xerox® Digital Alternatives sur le réseau. Le client peut disposer d'un processus de certification informel, limité à l'étude de la documentation de Xerox® Digital Alternatives et à une démonstration Xerox. Le client peut, sinon, disposer d'un processus plus formel qui exige l'installation proprement dite et une analyse réalisée sur la base de critères et d'un protocole de test définis. Le client doit déterminer les critères de certification et collaborer avec l'équipe Xerox pour définir la marche à suivre et les délais.

Les données utilisateur stockées sur les serveurs locaux implémentés au sein du réseau du client ne sont pas transférées vers les serveurs externes, à l'exception des données d'utilisation, qui sont périodiquement exportées vers les serveurs de rapports Xerox (composants de l'offre disponibles en option et limités aux données utilisateur répertoriées dans le Tableau 1 : Données utilisateur stockées dans Digital Alternatives).

Implémentation – Sur cloud privé

Xerox est chargée de certifier et d'approuver le déploiement de la solution Xerox® Digital Alternatives au sein de l'environnement en cloud privé d'un client donné. Xerox peut, sur demande, communiquer au client les procédures de certification et d'approbation de cette implémentation.

Les données utilisateur stockées sur les serveurs locaux implémentés au sein du réseau en cloud privé ne sont pas transférées vers les serveurs externes, à l'exception des données d'utilisation, qui sont périodiquement exportées vers les serveurs de rapports Xerox® (composants de l'offre disponibles en option et limités aux données utilisateur répertoriées dans le Tableau 1 : Données utilisateur stockées dans Digital Alternatives).

Pour les clients européens qui optent pour la méthode d'implémentation sur cloud privé, les serveurs sont situés sur l'un des sites d'hébergement européens indiqués dans le Tableau 2 : Sites d'hébergement du cloud privé.

Implémentation - Fournisseur de services Xerox® Digital Alternatives agréé

Le fournisseur de services Xerox® Digital Alternatives agréé peut participer au processus de certification et aider à déterminer les caractéristiques et fonctions de Xerox® Digital Alternatives nécessaires et la fréquence des activités de Xerox® Digital Alternatives.

Fonctions et responsabilités opérationnelles courantes

Dans le cadre du processus de certification du client, l'équipe chargée des comptes Xerox, également appelée « équipe des opérations », l'analyste sur le terrain qui prendra part au déploiement initial et à la maintenance, et le service informatique du client doivent définir les fonctions et responsabilités du traitement continu de l'installation du logiciel Xerox® Digital Alternatives :

- Responsabilité de la gestion du système
  - Le service informatique du client est responsable de la prise en charge du matériel serveur. Il est par ailleurs chargé de l'installation des mises à jour périodiques du logiciel du système d'exploitation Microsoft®.
- Responsabilité de la sauvegarde du référentiel de documents et de la base de données du serveur local
  - Le service informatique du client est chargé d'effectuer des sauvegardes périodiques de la base de données SQL Server® à laquelle fait appel Xerox® Digital Alternatives. Il est également responsable des sauvegardes périodiques du référentiel de documents.
- Responsabilité du contrôle de l'intégrité du matériel du serveur local
  - Le service informatique du client est chargé de contrôler l'intégrité du matériel et du système d'exploitation des serveurs locaux, à savoir pannes des composants matériels, problèmes de capacité d'espace disque, problèmes de connectivité réseau et erreurs du système d'exploitation.
- Mises à jour du logiciel du serveur local
  - Le fournisseur de services Xerox® Digital Alternatives agréé, en collaboration avec le service informatique du client, est chargé de planifier et d'exécuter les mises à niveau du logiciel du serveur local dès que celles-ci sont disponibles.

2 Architecture

Xerox® Digital Alternatives est constitué de cinq composants essentiels.

Composant	Description
Serveur local de Xerox® Digital Alternatives	• Effectue les tâches d'authentification. • Réplique les documents sur les autres périphériques de l'utilisateur et sur les périphériques d'autres utilisateurs.
Logiciel End User Client	• S'installe sur le PC Windows®, l'iPad® ou les tablettes Android™ prises en charge, ou sur l'ordinateur Apple Macintosh® de l'utilisateur final. • Affiche les documents à des fins de consultation et d'annotation.
CompleteView® Reporting Data Communicator	• Transmet les données d'utilisation du serveur local de Digital Alternatives à la plateforme de rapports Digital Alternatives CompleteView® hébergée au sein de Xerox.
Digital Alternatives CompleteView Reporting	• Utilise les informations d'utilisation Digital Alternatives récupérées sur le serveur local de Xerox® Digital Alternatives pour analyser les avantages de l'utilisation pour le client d'après les paramètres standard du secteur. Hébergé au sein du réseau Xerox.
Serveur central de Digital Alternatives sur Internet	• Stocke les informations de compte et les données de licence utilisées par le serveur local et les clients.

Composants du système

Application End User Client de Xerox® Digital Alternatives

Ce logiciel, qui peut être installé sur l'ordinateur Windows, l'iPad, la tablette Android ou l'ordinateur Apple Macintosh d'un utilisateur, affiche les documents et enregistre une copie locale dans le référentiel de documents local Xerox® Digital Alternatives de l'utilisateur. Les utilisateurs font appel au client lorsqu'ils souhaitent accéder à leurs documents. Il est impossible d'accéder aux documents locaux sans utiliser l'application End User Client de Digital Alternatives. Tous les documents stockés dans Digital Alternatives sont convertis en fichiers PDF. Les documents stockés au sein de l'application cliente sont automatiquement synchronisés avec le compte serveur local de l'utilisateur. L'utilisateur peut afficher les documents stockés sur son compte, ainsi que les documents que d'autres utilisateurs ont partagés avec lui.

Application de serveur local Xerox® Digital Alternatives

L'application de serveur local installée par un fournisseur de services Xerox® Digital Alternatives agréé requiert l'accès à un serveur de base de données SQL Server® et au serveur Web des services d'informations Internet Windows. Le serveur local coordonne les échanges de documents entre les périphériques d'un utilisateur, ou avec d'autres utilisateurs lors de la réception d'une demande de partage de documents entre deux utilisateurs. Chaque

application cliente Digital Alternatives interagit avec l'application de serveur local lors de l'authentification de l'utilisateur, mais aussi lors de l'importation ou de la modification d'un document. L'hébergement des serveurs d'applications sur des machines virtuelles distinctes est pris en charge.

Lorsque les comptes utilisateur sont définis et authentifiés à l'aide du serveur Active Directory du client, les informations d'identification qu'un utilisateur fournit au logiciel client à des fins d'authentification sont transférées vers le serveur local pour une authentification avec le serveur Active Directory du client. Cette communication entre le serveur local et le serveur Active Directory du client s'effectue via le protocole LDAP (Lightweight Directory Access Protocol).

Application Reporting Data Communicator

Le composant logiciel Reporting Data Communicator, installé séparément sur le serveur local de Xerox® Digital Alternatives, extrait les informations d'utilisation du client de la base de données de rapports du serveur local, puis les envoie aux serveurs Analytiques des utilisateurs CompleteView de Digital Alternatives hébergés au sein de Xerox. Les serveurs de rapports CompleteView utilisent ces données pour créer des rapports analytiques d'utilisation. Le logiciel Reporting Data Communicator est configuré de sorte que les informations d'identification personnelle ne soient pas transférées aux serveurs CompleteView de Digital Alternatives. Le guide d'administration de Digital Alternatives explique comment configurer Reporting Data Communicator pour envoyer les données de rapport aux serveurs Analytiques des utilisateurs CompleteView de Digital Alternatives. Tous les rapports de Digital Alternatives sont accessibles via le serveur de rapports CompleteView de Digital Alternatives hébergé par Xerox. Aucun rapport n'est disponible directement auprès du serveur local de Digital Alternatives.

Il est possible de configurer le logiciel Data Communicator de façon à exclure les informations d'identification personnelle lors du chargement des données sur le serveur de rapports CompleteView. Il est par ailleurs possible de configurer Data Communicator lors de l'implémentation du serveur en vue d'occulter certains éléments de données considérés comme informations personnelles. Le tableau suivant indique les éléments de données envoyés et les éléments de données occultés si aucune information personnelle ne doit être partagée avec le serveur de rapports de Xerox® Digital Alternatives.

Élément de données	Digital Alternatives	Digital Alternatives sans informations personnelles
UserID	Envoyé tel quel	Envoyé tel quel
Username	Envoyé tel quel	Occulté
Email	Envoyé tel quel	Occulté
Documents	Envoyé tel quel	Envoyé tel quel
StorageUsed	Envoyé tel quel	Envoyé tel quel
Quota	Envoyé tel quel	Envoyé tel quel
DeviceID	Envoyé tel quel	Envoyé tel quel
ClientTypeID	Envoyé tel quel	Envoyé tel quel
Type	Envoyé tel quel	Envoyé tel quel
ActivityTypeID	Envoyé tel quel	Envoyé tel quel
ActivitySubTypeID	Envoyé tel quel	Envoyé tel quel
ActivityID	Envoyé tel quel	Envoyé tel quel
Key	Envoyé tel quel	Envoyé tel quel

Élément de données	Digital Alternatives	Digital Alternatives sans informations personnelles
Value	Envoyé tel quel	Envoyé tel quel
DocumentName	Envoyé tel quel	Occulté
Pages	Envoyé tel quel	Envoyé tel quel
IsColor	Envoyé tel quel	Envoyé tel quel
DateUTC	Envoyé tel quel	Envoyé tel quel
Description	Envoyé tel quel	Envoyé tel quel
ActivityKeyValuePairID	Envoyé tel quel	Envoyé tel quel
OnboardDateUTC	Envoyé tel quel	Envoyé tel quel
RecType	Envoyé tel quel	Envoyé tel quel

Tableau 1 : Données utilisateur stockées dans Digital Alternatives

Les serveurs sont hébergés sur le site d'hébergement sur cloud privé Xerox®. La communication entre ces serveurs et Data Communicator est établie via le protocole sécurisé HTTPS à l'aide du port 443. Les serveurs CompleteView disposent d'une interface Web sécurisée, qui permet aux utilisateurs autorisés d'utiliser la fonctionnalité de création de rapports CompleteView. Les utilisateurs peuvent afficher uniquement les données des comptes Digital Alternatives auxquels ils sont autorisés à accéder. Les comptes Data Communicator peuvent uniquement envoyer des données à un compte CompleteView spécifique configuré à cet effet.

Serveur central de Xerox® Digital Alternatives

Le serveur central de Digital Alternatives est hébergé au sein du réseau en cloud Microsoft Azure désigné pour Xerox. Seul le personnel d'assistance de Xerox® MPS Application chargé de la création et de la maintenance des comptes utilisateur au sein du serveur central peut accéder au serveur central de Digital Alternatives. Toutes les communications que le serveur local et le logiciel client envoient au serveur central sont établies via l'interface de protocole HTTPS sécurisée.

Ce composant stocke les informations de compte et les données de licence utilisées par le serveur local et les clients. Le serveur central gère le compte client de Digital Alternatives, c'est-à-dire l'ID de client généré par le serveur central pour chaque implémentation du client Digital Alternatives, ainsi que le ou les domaines de messagerie associés auxquels les utilisateurs du client font appel lorsqu'ils accèdent à leur compte Digital Alternatives. Les adresses électroniques, chiffrées, des utilisateurs qui ont installé le logiciel client et qui se sont connectés à Digital Alternatives sont les seules informations utilisateur stockées sur le serveur central. Aucune autre information utilisateur n'est enregistrée sur le serveur central.

Les quotas des postes utilisateur sous licence pour chaque implémentation sont gérés au sein du compte client de Digital Alternatives. Consultez le guide d'administration de Xerox® Digital Alternatives pour plus d'informations sur la méthode de gestion des licences.

Les schémas ci-dessous illustrent les deux scénarios de déploiement des composants du serveur local Digital Alternatives. Dans le cadre d'une implémentation sur site, nous implémentons le serveur local Digital Alternatives au sein de l'environnement informatique du client, où le client procure les serveurs Windows, y compris Microsoft SQL Server. Dans le cadre d'une implémentation sur cloud privé, Xerox fournit les hôtes et le serveur SQL Server au sein de son réseau en cloud privé, et une connexion VPN entre le réseau en cloud privé de Xerox® et le réseau informatique du client.

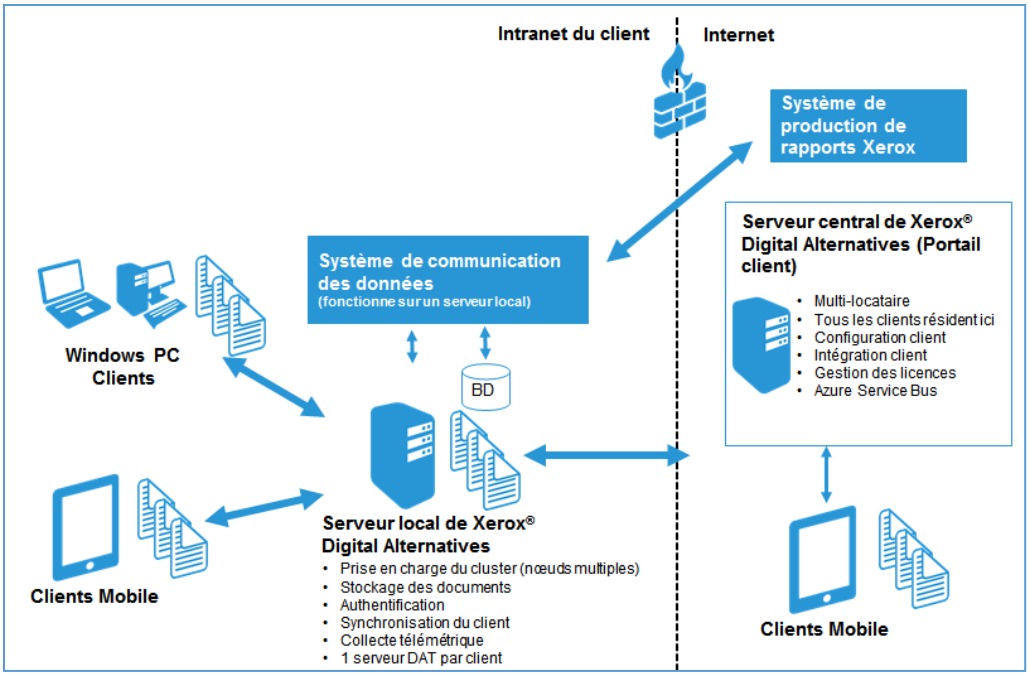

Figure 1 : Implémentation sur site

Dans l'implémentation sur cloud privé, nous établissons une connexion VPN dédiée interentreprises entre le serveur d'applications au sein du réseau des services Xerox et le réseau du client qui assure l'accès par le serveur d'applications aux connexions Active Directory et Exchange LDAP du client. Par ailleurs, la connexion VPN permet aux utilisateurs équipés du logiciel client Digital Alternatives de se connecter au serveur d'applications via le réseau du client.

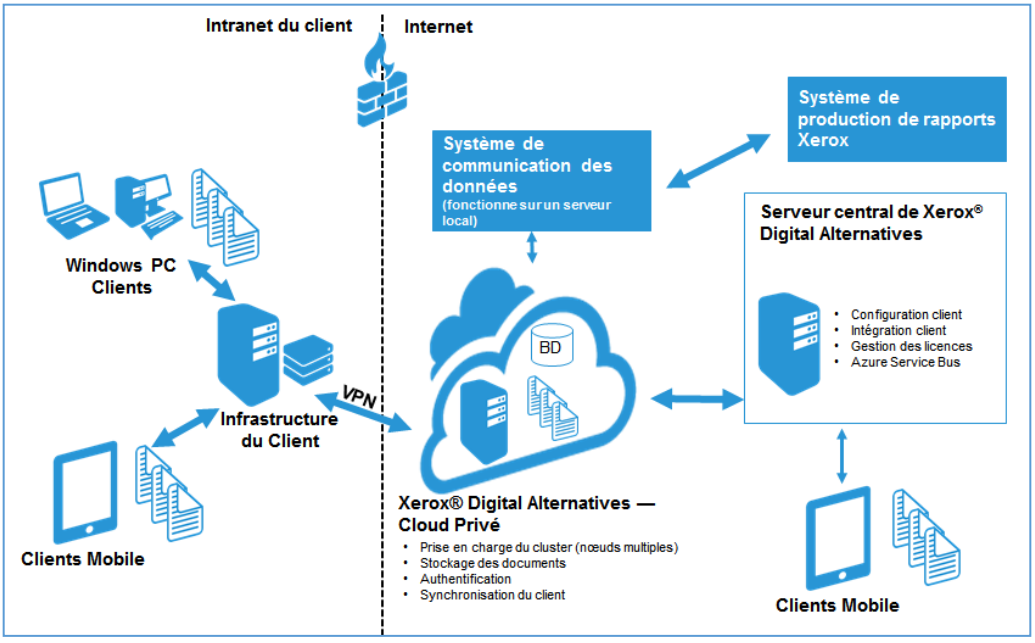

Figure 2 : Implémentation sur cloud privé

Modèles de déploiement du serveur local

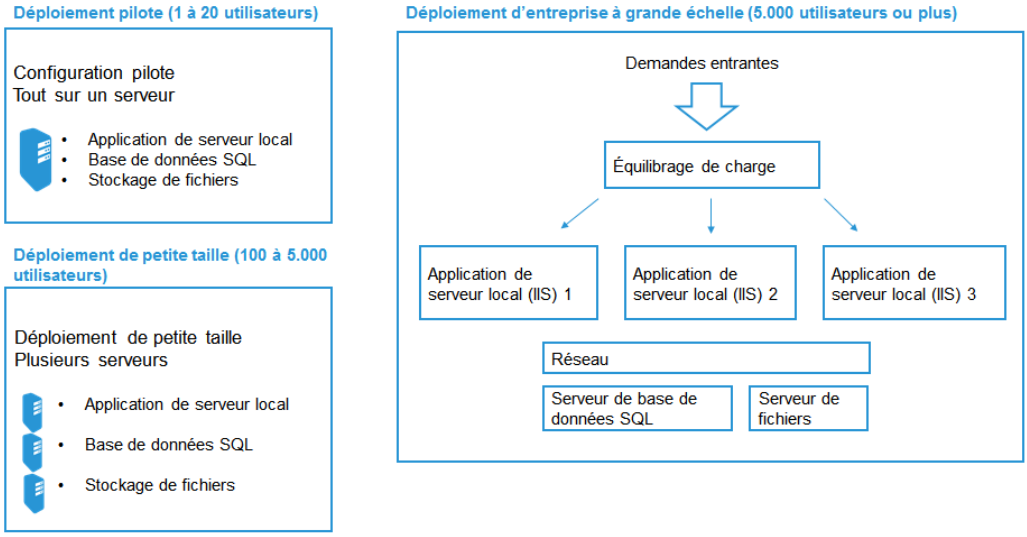

Figure 3 : Modèle de déploiement du serveur local

3 Environnements solution/application

Matériel et logiciels requis

Les logiciels et le matériel requis pour le serveur local et les composants du logiciel client dans la solution Digital Alternatives sont détaillés dans les sections ci-après. Par ailleurs, le document cible le serveur local, mais n'omet pas de parler également des composants PC et iPad.

Configuration requise pour l'installation du serveur local

Systèmes d'exploitation pris en charge

- Windows® 2008 Standard
- Windows® 2008 Entreprise
- Windows® 2008 R2 Standard
- Windows® 2008 R2 Entreprise
- Windows® 2012
- Windows® 2012 R2

Autres logiciels requis

- Microsoft® .NET Framework v4.5.2
- Planificateur de tâches Windows
- Microsoft Message Queuing (MSMQ)

Configuration minimale requise pour le matériel

- RAM : 8 Go
- Processeur : Double cœur 1,20 GHZ
- Disque dur : 260 Go

L'installation nécessite 100 Mo d'espace disponible pour le logiciel, ce qui exclut le stockage du référentiel de documents. Le serveur d'applications (Web) doit appliquer le certificat de serveur au serveur Web IIS du serveur afin d'activer le protocole HTTPS pour les communications chiffrées SSL (Secure Sockets Layer) avec les applications clientes. Toutes les communications entre les composants de l'application Digital Alternatives sont basées sur le protocole HTTPS.

Il est possible d'installer Reporting Data Communicator sur un nœud d'application du serveur local.

Composant	Configuration minimale	Souhaité/Recommandé
Système d'exploitation	Windows Server® 2008 R2	Windows Server 2008 R2 ou Windows Server 2012
Serveur Web	IIS version 7.5	IIS version 7.5 pour Server 2008 R2 ou IIS version 8 pour Server 2012
Mémoire virtuelle	8 Go	
Accès COM+ réseau	Non requis	Non requis
Accès DTC réseau	Non requis	Non requis
Composants d'accès	Requis (groupés avec Microsoft® .NET 4.5 Framework)	Requis (groupés avec Microsoft® .NET 4.5 Framework)
Microsoft .Net Framework	4.5.2	.NET 4.5.2
Serveur de base de données	Microsoft SQL Server® 2008 R2	SQL Server 2012
Authentification SQL	Requis avec l'accès au compte admin	Requis avec l'accès au compte admin
Droits d'administration de serveur	Requis	Requis

Ressources requises pour tous les déploiements

Le service informatique du client doit fournir les ressources suivantes nécessaires au serveur local de Digital Alternatives.

SMTP (serveur de courrier sortant) : les informations sur le serveur SMTP du client sont requises pour que le serveur local de Xerox® Digital Alternatives envoie les notifications de partage. Si le protocole SMTP exige une authentification de l'utilisateur, les informations d'identification de l'utilisateur du compte de service sont utilisées. Le serveur local utilise l'interface entre le protocole SMTP existant du client et le serveur de messagerie MS Exchange existant du client. Le port 25 (TCP) est le paramètre le plus courant pour l'interaction entre les relais de messagerie SMTP et Digital Alternatives, mais il est possible de le remplacer au moment de configurer le serveur local en fonction des exigences du serveur de messagerie du client.

Connexion LDAP pour la recherche d'adresses globale : principal serveur de recherche d'annuaire des utilisateurs chez le client. Permet d'accéder aux adresses électroniques pour la vérification du propriétaire de la messagerie pendant l'intégration. Il est également utilisé pour la recherche d'adresses globale. Le port 389 (TCP) est utilisé par défaut, sauf si le service informatique du client nous demande de faire appel à un autre ID de port.

Connexion(s) LDAP pour l'authentification : les utilisateurs de Xerox® Digital Alternatives sont authentifiés via l'authentification de domaine de réseau Microsoft® Windows. Le serveur local de Xerox® Digital Alternatives peut détecter automatiquement une adhésion dans un domaine donné (via le compte de service fourni), de sorte que les domaines et les serveurs apparaissent automatiquement sur l'écran de configuration. Sinon, il est possible d'ajouter les domaines et les connexions LDAP manuellement. Le port 389 (TCP) est utilisé par défaut, sauf si le service informatique du client nous demande de faire appel à un autre ID de port.

Compte de service : le service informatique du client doit créer un compte de service que doivent utiliser les trois services de maintenance de l'application sur le serveur et les pools d'applications IIS. Les trois services de maintenance installés avec l'application de serveur local sont les suivants :

- Xerox.Digital.MaintenanceService : chargé de supprimer périodiquement les documents identifiés par les utilisateurs de Digital Alternatives
- Xerox.Digital.QueueService : chargé d'interagir avec MS Queuing pour l'exécution des travaux
- Xerox.Digital.RelayService : chargé d'interagir avec le serveur central pour obtenir des informations de licence et de s'interfacer avec le serveur central pour une mise à jour à distance des documents du client

Il doit s'agir d'un compte de domaine doté de droits d'administration locaux sur le ou les nœuds du serveur local de Xerox® Digital Alternatives. Si le protocole SMTP utilisé exige une authentification de l'utilisateur, les nom d'utilisateur et mot de passe du compte de service sont utilisés. Ce compte de service doit être affranchi de toute expiration de mot de passe, car un mot de passe expiré affecte le fonctionnement du serveur local. Consultez le guide d'administration du serveur local de Xerox® Digital Alternatives pour plus de détails sur la configuration correcte du compte de service du serveur local. Ce compte est requis au moment de l'installation du serveur local.

Accès Internet : l'accès au serveur central de Xerox® Digital Alternatives est indispensable. Le port https requis est le port 443.

Configuration requise pour PC client Xerox® Digital Alternatives

Installation

La configuration minimale requise pour l'installation est la suivante (selon la configuration système requise et les besoins du client, du matériel supplémentaire peut être nécessaire).

- Système d'exploitation pris en charge :
  - Windows® 7 (Professionnel, Édition Intégrale, Entreprise)
  - Windows® 7 x64 (Professionnel, Édition Intégrale, Entreprise)
  - Windows® 8
  - Windows® 8 x64
  - Windows® 8.1 (Professionnel, Édition Intégrale)
  - Windows® 10 (Édition Familiale, Professionnel, Entreprise)
- Processeur Intel® Pentium® 4 ou ultérieur
- Mémoire physique (RAM) : 2 Go minimum (4 Go recommandé)
- Espace libre sur le disque dur : 250 Mo pour l'application seule. 5 Go minimum recommandé pour le stockage de documents.
  Remarque : les utilisateurs qui gèrent de gros volumes de documents peuvent avoir besoin d'un espace disque plus important.
- Microsoft® .NET Framework 4.5 s'impose comme condition préalable pour tous les systèmes d'exploitation pris en charge.

Sécurité

- L'application cliente et le serveur local de Digital Alternatives utilisent l'authentification de domaine Active Directory du client.
- Les utilisateurs utiliseront leur propre connexion au domaine Windows.
- Pour l'application du PC client, Internet Explorer doit être configuré avec un serveur proxy pour un accès initial au serveur central externe. L'interaction entre le PC client et le serveur central s'effectue via le protocole HTTPS à l'aide du port 443. Le serveur proxy du client doit autoriser la communication de protocole HTTPS vers le serveur central de Digital Alternatives lors de l'installation initiale du logiciel du PC client.
- Le serveur local de Xerox® Digital Alternatives doit être connecté au(x) serveur(s) d'authentification de domaine du client. Consultez la section Ressources requises pour tous les déploiements pour obtenir de plus amples informations.

Remarque : après l'installation, l'accès Internet est requis afin que les utilisateurs puissent :

- intégrer la solution du logiciel client Xerox® Digital Alternatives au serveur central et à leur client serveur local installé pour la première fois.
- réauthentifier leur client Xerox® Digital Alternatives auprès de leur serveur local (lorsque celui-ci est externe au réseau de leur entreprise) à l'expiration du jeton de sécurité ou du mot de passe de leur client ; si l'application cliente est externe et n'a pas accès à Internet (notamment si elle est en mode Avion), le logiciel client ne s'ouvre pas tant que la connexion Internet n'est pas rétablie ou que le logiciel n'a pas de nouveau accès au réseau interne du client.
  - Les jetons de sécurité expirent toutes les 8 heures.

Configuration requise pour iPad client Xerox® Digital Alternatives

Installation

- Système d'exploitation iOS 7, 8 ou 9.
- iPad 2 et plus récent, y compris iPad mini™ (avec et sans écran Retina) iPhone non pris en charge.

Sécurité :

- L'iPad client utilise l'authentification de domaine Active Directory du client.
- Le serveur local de Xerox® Digital Alternatives doit être connecté au(x) serveur(s) d'authentification de domaine du client. De plus amples informations à ce sujet sont fournies dans une autre section.

Remarque : après l'installation, l'accès Internet est requis afin que les utilisateurs puissent :

a. intégrer la solution Xerox® Digital Alternatives à leur client pour la première fois.
b. réauthentifier leur client Xerox® Digital Alternatives à l'expiration de leur jeton ou mot de passe.
   - Les jetons d'authentification expirent toutes les 8 heures.
c. Pour la synchronisation et le partage, vous pouvez utiliser Internet ou l'intranet du client.

Configuration requise pour Android client Xerox® Digital Alternatives

Installation

Fabricants et versions du système d'exploitation Android pris en charge :

Périphérique	Versions du système d'exploitation prises en charge
Asus Memo Pad 7	v4.4.2 (KitKat®)
Google (Asus) Nexus 9	v5.0 et v5.1.1(Lollipop)
Google (Asus) Nexus 7	v4.1(Jelly Bean), v4.4.2 (KitKat®), v5.0/5.1/5.1.1 (Lollipop)
Samsung Galaxy Tab 4	v4.4.2 (KitKat®)
Samsung Galaxy Tab S	v4.4.2 (KitKat®), v5.0/5.1/5.1.1 (Lollipop)

Sécurité :

- L'application cliente Android utilise l'authentification de domaine Active Directory du client.
- Le serveur local de Xerox® Digital Alternatives doit être connecté au(x) serveur(s) d'authentification de domaine du client. De plus amples informations à ce sujet sont fournies dans une autre section.

Configuration requise pour Apple Macintosh client Xerox® Digital Alternatives

Installation

- Versions du système d'exploitation Apple prises en charge : OS X 10.10 (Yosemite) et OS X 10.11 (El Capitan).

Sécurité :

- L'application cliente Apple Macintosh utilise l'authentification de domaine Active Directory du client.
- Le serveur local de Xerox® Digital Alternatives doit être connecté au(x) serveur(s) d'authentification de domaine du client.

4 Considérations concernant le cloud privé

Considérations concernant l'implémentation sur cloud privé

Établissement d'une connectivité interentreprises (B2B)

Dans le cas d'une implémentation sur cloud privé, nous devons établir une connexion B2B dédiée entre le réseau du client et le réseau en cloud privé de Xerox® de façon à ce que le serveur local du client hébergé sur le cloud privé puisse interagir avec le serveur Active Directory du client. La solution VPN en cloud privé permet par ailleurs aux utilisateurs du client d'interagir avec le serveur local hébergé sur le cloud privé, comme ci celle-ci était installée au sein du réseau du client. Une implémentation standard inclut une solution VPN de site à site qui établit une connexion privée entre le pare-feu du client et le pare-feu du cloud privé. Plusieurs facteurs doivent être pris en considération pour une implémentation efficace de la solution VPN en cloud privé.

Adresse IP et numéro de port du serveur Active Directory du client

Le serveur en cloud privé de Digital Alternatives doit présenter les informations d'identification d'un utilisateur intégré au serveur Active Directory du client à l'aide de son interface LDAP (Lightweight Directory Access Protocol) via la connexion B2B.

Adresse IP et numéro de port de l'interface LDAP d'Exchange Server du client

Lorsqu'un utilisateur final consulte le carnet d'adresses global de son entreprise au sein de Digital Alternatives, le serveur local récupère ces informations en accédant au serveur Exchange Server du client via son interface LDAP. Le port 389 (TCP) est généralement utilisé, mais le service informatique du client peut utiliser un autre numéro de port.

Règle de traduction d'adresses de réseau des adresses IP du client dans le pare-feu

En raison de l'éventuelle similitude entre les adresses IP internes utilisées par le client pour ses périphériques réseau et les adresses de réseaux d'un autre client au sein de Xerox, le client doit fournir une règle de traduction d'adresses de réseau (NAT) pour mapper la communication de l'adresse IP sortante avec le serveur en cloud privé de Digital Alternatives. Par exemple, il est courant que les périphériques réseau du client utilisent les plages d'adresses 192.168.1.XXX ou 10.10.1.XXX pour l'adressage interne. Comme l'application cliente de chaque client communique avec le serveur en cloud privé au moment de la synchronisation des documents, l'ensemble du trafic sortant du client doit apparaître pour Xerox comme une unique source IP entrante représentant tout le trafic du client vers le serveur en cloud privé avec lequel interagir.

Sécurité des documents au sein du serveur local dans le cloud

Les documents importés dans Digital Alternatives sont stockés sous forme de fichiers PDF non chiffrés dans le référentiel de documents au sein du serveur local. L'accès à ce référentiel de documents, ainsi qu'à l'application et au serveur de base de données, est réservé au personnel informatique chargé du cloud privé de Xerox® dont les tâches consistent, entre autres, à administrer ces serveurs et à en assurer la maintenance. La prévention d'un accès direct au référentiel de documents par des utilisateurs ou des membres non autorisés du personnel informatique chargé du cloud privé de Xerox® est assurée au moyen d'autorisations Windows spécifiées dans le répertoire contenant les documents. Nous appliquons donc des pratiques sûres eu égard à la sécurité des documents et aux informations d'identification personnelle lors du stockage de documents confidentiels dans un système cloud.

Sécurité physique du cloud privé

Xerox fait appel à plusieurs data centers pour héberger son application et ses données, assurant ainsi une redondance essentielle. Tous les data centers sont équipés de systèmes de sécurité physique, respectent des politiques d'accès rigoureuses, et disposent de chambres fortes et de cages de protection sécurisées. Xerox prend toutes les mesures de sécurité nécessaires pour préserver la confidentialité des informations de ses clients. Xerox possède des moyens de protection administratifs, techniques et physiques qui permettent de répondre aux exigences de conformité de l'entreprise des clients.

- Les data centers emploient des méthodes d'authentification à deux facteurs, qui incluent l'authentification biométrique et des moyens de protection disponibles 24 h sur 24, 7 jours sur 7.
- Xerox figure dans le rapport SSAE 16 de type II.
- Les sites de stockage sont munis de systèmes d'alimentation sans interruption et de sauvegarde, ainsi que de systèmes de prévention contre les incendies/inondations.
- Les data centers qui hébergent le cloud privé de Digital Alternatives sont conformes aux normes ISO 27001, HIPAA, PCI-DSS et aux directives SOX.
- Nous surveillons en permanence notre réseau privé et effectuons de fréquentes évaluations des menaces de sécurité et d'intrusion pour garantir la protection des données.
- Plusieurs connexions à la dorsale Internet assurent un routage redondant et une connectivité haute performance.
- Les instances du cloud privé de Digital Alternatives sont hébergées dans les data centers de Xerox qui sont épaulés par des sites secondaires de reprise après sinistre, tous conformes à la norme ISO 27001 :

Data centers aux États-Unis		Data centers en Europe	
Site principal	**Site secondaire (reprise après sinistre)**	**Sites principaux**	**Site secondaire (reprise après sinistre)**
Lexington, KY, États-Unis	Sandy, UT, États-Unis	Telford, R.-U.	Newport, R.-U.
		Paris, France	Tours, France

Tableau 2 : Sites d'hébergement du cloud privé

- Les sites secondaires de reprise après sinistre prennent le relai lorsque les sites principaux tombent en panne. Une fois activé, le site secondaire prend la relève à partir de la sauvegarde de nuit du site principal.
- Aucun renseignement ni aucun document client n'est hébergé dans l'environnement Microsoft Azure. Concernant le cloud privé de Digital Alternatives, tous les renseignements et documents des clients sont stockés dans les data centers gérés par Xerox.
- Les régulations effectuées dans le data center sur cloud privé sont les suivantes :
  - Régulation des conditions ambiantes (climatisation, extinction des incendies, etc.)
  - Systèmes d'alimentation redondante/de réserve
  - Connexions réseau/Internet redondantes B2B et B2C

Gestion de l'accès au cloud privé

Seuls les comptes utilisateur qui prennent en charge la maintenance continue des serveurs sur la base des demandes d'accès sont autorisés à accéder aux serveurs sur cloud privé. Les utilisateurs Xerox chargés de la maintenance du serveur sur cloud privé demandent l'accès à la gouvernance du cloud privé après avoir reçu l'aval de leur responsable. Dès que la gouvernance du cloud privé analyse la demande, elle peut ou pas donner son approbation. L'équipe d'implémentation désignée par la gouvernance est chargée de toutes les implémentations d'accès. L'accès à l'instance de base de données et au référentiel de documents du client est limité à un sous-ensemble d'utilisateurs autorisés à accéder à l'implémentation du cloud privé du client.

Contrôle d'accès logique du cloud privé

Le cloud privé de Xerox® entretient un cadre stratégique de sécurité des informations grâce à des évaluations régulières des menaces, des vulnérabilités et de l'impact sur les activités auxquels les systèmes d'information protégés peuvent être soumis de la part d'un éventail d'agresseurs et d'imprévus. Nous examinons ce cadre au moins deux fois par an. Ce cadre englobe la sécurité des informations à l'échelle de l'entreprise, ainsi que les questions propres à l'environnement d'hébergement sur le cloud privé de Digital Alternatives. Xerox met également en œuvre un jeu complet de stratégies, de procédures et d'outils pour garantir la conformité permanente avec les directives de sécurité internes et externes.

Les utilisateurs du client ne disposent pas de comptes utilisateur leur permettant de se connecter à distance à leurs serveurs locaux hébergés. Seuls les utilisateurs Xerox devant accéder aux serveurs sur cloud privé à des fins de maintenance peuvent s'y connecter.

Identification et authentification du cloud privé

Le cloud privé de Digital Alternatives dispose d'un connecteur LDAP qui permet au serveur local hébergé d'utiliser le serveur LDAP ou Active Directory d'entreprise d'un client pour authentifier les utilisateurs de Digital Alternatives.

Les clients qui s'authentifient auprès de Digital Alternatives sur leur logiciel client doivent spécifier leurs informations de connexion sur le logiciel client de façon à les transférer au serveur local via la connexion VPN sur cloud privé. À son tour, le serveur local authentifie l'interface LDAP Active Directory du client à l'aide des informations d'identification spécifiées via la connexion VPN sur cloud privé. Dès que le serveur Active Directory du client valide ces informations d'identification, le logiciel du client est autorisé à interagir avec le serveur local hébergé.

Transmission des données du cloud privé

Pour renforcer la sécurité des données, Xerox fait appel au chiffrement des données lors du transit depuis et vers le cloud privé de Digital Alternatives.

- Chiffrement au transfert avec SSL avec AES 256 bits sur le port 443

Audit et consignation

Xerox peut fournir sur demande des rapports d'audit pour la plupart des actions ou activités ayant lieu au sein de l'administration de Digital Alternatives.

Les accès utilisateur aux serveurs locaux sont consignés au sein des serveurs sur cloud privé à l'aide de la fonction standard de journalisation des accès utilisateur Windows, qui consigne par défaut les accès utilisateur des deux dernières années. Les données d'accès utilisateur sont stockées localement sur le serveur local et occupent normalement moins de 80 Mo d'espace disque.

À la demande du client, Xerox peut fournir un fichier texte contenant tous les accès utilisateur consignés.

Délai d'expiration de l'application

L'authentification de l'utilisateur doit être renouvelée toutes les huit heures. Lorsqu'une session expire sur le logiciel client Digital Alternatives, l'utilisateur doit se réauthentifier.

Sécurité de l'application

La solution Digital Alternatives a été développée conformément aux normes de développement de logiciels de Xerox, qui incluent des révisions de conception et de code, ainsi que des bibliothèques de logiciels standard telles que Microsoft .NET Framework.

Toutes les communications entre les composants de Digital Alternatives font appel à des technologies de chiffrement pour sécuriser les données du client.

Poursuite des activités/reprise après sinistre

Xerox conserve des sauvegardes de toutes les données, ainsi que du matériel redondant pour minimiser les répercussions sur les activités suite aux pannes de matériel, à l'indisponibilité des sites, aux catastrophes naturelles ou autres imprévus. Nous testons tous les ans les plans et outils de reprise après sinistre sur une installation de référence en direct de Digital Alternatives. La reprise après sinistre inclut une fonction de basculement sur site pour chaque emplacement, tel que défini dans le tableau des data centers : Tableau 2 : Sites d'hébergement du cloud privé.

5 Gestion/protection des données

Stockage des documents

Tous les documents des utilisateurs de Xerox® sont conservés sur le serveur de documents de Xerox® Digital Alternatives. Le serveur de documents de Xerox® Digital Alternatives, ainsi que le serveur local et le serveur de base de données, se trouvent dans les locaux ou bien sont hébergés en toute sécurité sur le cloud Xerox. Les documents sont stockés sans être chiffrés sur le serveur de documents de Digital Alternatives. L'accès aux documents est protégé par un accès Windows et un accès au serveur sur le domaine du client, et seul un nombre limité d'utilisateurs au sein du site d'hébergement peut accéder aux documents. En guise de protection supplémentaire, les documents réels sont stockés avec un nom de fichier et une extension obscurcis. Les documents sont supprimés non pas automatiquement, mais par les utilisateurs eux-mêmes. Il n'y a pas de nettoyage automatique de documents. Chaque utilisateur dispose d'un espace alloué spécifique pour stocker ses documents sur le serveur de fichiers de Xerox® Digital Alternatives (paramétrage du quota d'utilisateurs dans l'interface utilisateur d'administration). Aucun document d'utilisateur de Xerox® Digital Alternatives n'est stocké sur le serveur central de Xerox® Digital Alternatives.