AUTODESK

Livre blanc sur la sécurité d'Autodesk® Fusion 360

Octobre 2022

Sommaire

1. Introduction

Autodesk® Fusion 360™ est le premier outil en son genre de CAO, FAO et IAO 3D. Il rassemble vos processus de développement de produits sur une seule plateforme Cloud compatible avec Mac et PC. Fusion 360 permet d'explorer rapidement et facilement vos idées de conception grâce à son jeu d'outils intégré et sécurisé allant de la conception à la fabrication, qui prend en charge les navigateurs Web et les appareils mobiles.

1.1 Objectif et portée du document

L'objectif de ce document est d'expliquer les opérations d'Autodesk, le processus de développement de logiciels et les mesures de sécurité mises en œuvre dans l'environnement. Dans ce document, « Autodesk Fusion 360 » fait référence au logiciel client Fusion 360 et au logiciel d'accès par navigateur Fusion 360.

Le cadre de sécurité d'Autodesk est basé sur les normes du secteur afin d'assurer la confidentialité, l'intégrité et la disponibilité des informations du client.

Fusion 360 est conçu pour offrir une haute disponibilité et une grande évolutivité, offrant ainsi à nos clients un service Cloud rapide et résilient. L'hébergeur Cloud d'Autodesk est Amazon Web Services (AWS), un des leaders du marché dans le domaine des infrastructures Cloud. Autodesk s'appuie sur le modèle de responsabilité partagée des fournisseurs d'hébergement AWS, qui inclut une infrastructure composée du matériel, des logiciels, de la mise en réseau et des installations qui exécutent les services Cloud AWS. (Pour en savoir plus, consultez la page suivante : https://aws.amazon.com/fr/compliance/shared-responsibility-model/).

2. Sécurité Autodesk

Le cadre de sécurité d'Autodesk est basé sur les normes du secteur pour garantir des pratiques de sécurité cohérentes, ce qui nous permet de créer des systèmes sécurisés tant dans leur conception que dans leur utilisation sur le long terme.

- **Une conception sécurisée** : la sécurité est intégrée à nos produits de A à Z. Elle est essentielle pour garantir l'investissement de nos clients dans les produits et services Autodesk. Nous intégrons la sécurité dans toutes les phases du développement logiciel.

- **Une utilisation sécurisée** : la sécurité est intégrée directement à notre infrastructure. Notre approche globale comprend le déploiement d'outils de protection des points de terminaison, des exigences standardisées et durcies en matière de correctifs, des contrôles de la gestion des identités et des accès, ainsi que des activités de sécurité offensives.

- **Une sécurité pérennisée :** la sécurité chez Autodesk est axée sur trois objectifs principaux qui protègent la confidentialité, l'intégrité et la disponibilité (CID) des informations :

    - Confidentialité : les informations sont accessibles uniquement aux personnes autorisées.
    - Intégrité : les informations sont exhaustives et précises.
    - Disponibilité : les données sont accessibles et disponibles pour les clients.

Le responsable de la sécurité (CSO) est responsable du développement, de la mise en œuvre et de la gouvernance de la stratégie et du programme de sécurité. Il veille à ce que les politiques et les normes de sécurité soient appliquées à l'ensemble des produits et environnements Autodesk. Les actions de l'équipe chargée des opérations de sécurité et le responsable de la sécurité sont soutenus par les dirigeants et le conseil d'administration d'Autodesk.

3. Ingénierie Fusion 360

L'équipe d'ingénierie de Fusion 360 est chargée de concevoir, de mettre en œuvre et de tester le logiciel client Fusion 360 et l'application des services Cloud.

La conception, le codage, les tests et la maintenance de Fusion 360 reposent sur un processus de développement logiciel agile. Pendant les phases de conception, les architectes produisent et révisent des documents de conception détaillés pour évaluer la fonctionnalité et l'évolutivité

de la conception. Lors des phases de mise en œuvre, les ingénieurs logiciel et les architectes procèdent à des révisions par des pairs afin de détecter les écarts vis-à-vis des pratiques de développement d'applications de Fusion 360. Tout le code développé pendant le processus est soumis à un test unitaire fonctionnel, et aucun témoignage utilisateur n'est considéré comme valable tant que le personnel en charge de l'assurance qualité n'a pas vérifié l'applicabilité des critères Définition et Terminé. Les tests de performance de Fusion 360 sont également intégrés au cycle de développement. L'équipe de Fusion 360 effectue des tests de charge tout au long des phases de développement pour identifier au plus tôt les modifications qui ont un impact négatif sur les performances.

3.1 Formation des employés

Dans le cadre du processus de formation lors de l'embauche, les employés d'Autodesk doivent s'engager à comprendre l'importance de la sécurité des informations. Ils doivent lire, comprendre et suivre un cours de formation sur le Code de conduite de l'entreprise. Ce code exige que chaque employé mène ses activités de façon légale, éthique, intègre et respectueuse de l'autre et des utilisateurs, partenaires et concurrents de l'entreprise.

Les employés d'Autodesk sont tenus de suivre les directives de l'entreprise en matière de confidentialité, d'éthique professionnelle, d'utilisation appropriée et de normes professionnelles. Les nouveaux employés doivent signer un accord de confidentialité. Le nouveau processus d'insertion des employés met l'accent sur la confidentialité des données des clients.

Pour mettre en œuvre les meilleures pratiques en matière de sécurité, Autodesk a mis en place un programme annuel de certification de la sécurité des logiciels (SSCP) pour tous les utilisateurs occupant des postes relatifs à l'ingénierie et à l'infrastructure Cloud.

4. Sécurité des produits Fusion 360

Autodesk Fusion 360 intègre des fonctionnalités de sécurité qui vont de la communication avec les services Cloud aux fonctionnalités de sécurité/collaboration au niveau des produits que les utilisateurs contrôler.

4.1 Sécurité des communications

Toutes les communications entre Autodesk Fusion 360 et les services Cloud requièrent des connexions HTTPS sécurisées.

4.2 Chiffrement et clés

La communication entre Fusion 360 et les services backend au sein de ces derniers s'effectue via un canal chiffré.

4.3 Authentification

Des informations d'identification constituées d'un ID Autodesk, d'un ID utilisateur et d'un mot de passe sont requises pour accéder à Autodesk Fusion 360. Les informations d'identification sont sécurisées lors de la transmission réseau et stockées uniquement sous forme de hachage salé.

Fusion 360 offre aux utilisateurs finaux la possibilité d'utiliser l'authentification multifacteur lors de la connexion. Les utilisateurs qui choisissent d'activer cette fonctionnalité peuvent utiliser leur appareil personnel sécurisé autorisé (par exemple, un téléphone portable) pour recevoir un code à utiliser avec leur mot de passe.

4.4 Sécurité des données

Toutes les conceptions Fusion 360 sont enregistrées dans le Cloud sur un espace de stockage chiffré. La solution de stockage utilise la norme Advanced Encryption Standard 256 bits (AES-256) pour chiffrer les données.

En local, les conceptions mises en cache dépendent des autorisations de niveau utilisateur du système d'exploitation pour le contrôle d'accès.

4.5 Contrôle des versions des conceptions

Pour chaque conception, Autodesk Fusion 360 conserve un historique des versions. Le contrôle des versions protège l'intégrité des données en permettant aux utilisateurs de revenir aux versions antérieures et en fournissant une liste vérifiable des informations sur chaque modification de fichier.

4.6 Sécurité de la collaboration basée sur les hubs et les groupes

Les projets permettent d'accorder ou de limiter simplement l'accès aux conceptions Autodesk Fusion 360 à un ensemble de collaborateurs. Les invitations à des projets sont approuvées par le propriétaire ou le modérateur du projet, ce qui garantit un contrôle strict des membres qui accordent l'accès aux nouveaux utilisateurs.

Les entreprises peuvent opter pour les hubs d'équipe, qui leur permettent d'exercer un contrôle sur la propriété et l'accès à tous les projets créés par les membres. Les paramètres de confidentialité du projet, tels que les projets ouverts, fermés et secrets, permettent un contrôle poussé de la collaboration. Avec les hubs d'équipe, les membres peuvent choisir de restreindre l'accès aux collaborateurs qui ont été invités au projet. Les hubs d'équipe permettent également aux administrateurs des clients de désactiver les comptes des anciens employés et de transférer la propriété du projet à d'autres membres de l'équipe.

4.7 Partage public

Grâce au partage public, les utilisateurs peuvent collaborer avec des intervenants externes qui ne disposent pas d'un ID Autodesk ou de droits d'accès à Fusion 360. Les utilisateurs de Fusion 360 créent un lien qui fournit un accès en lecture seule à la conception. Les utilisateurs ont également la possibilité d'activer les fonctionnalités de téléchargement/exportation. À tout moment, l'utilisateur peut révoquer le partage public offert par ce lien.

5. Infrastructure Cloud

L'équipe Infrastructure Cloud est chargée de définir et d'exécuter les procédures de gestion des versions d'application, des mises à niveau du matériel et des systèmes d'exploitation, de surveillance de l'état du système et des autres activités requises pour la maintenance d'Autodesk Fusion 360.

5.1 Haute disponibilité

Autodesk Fusion 360 est conçu pour atteindre un niveau de disponibilité élevé en utilisant des systèmes redondants dans son infrastructure de support et en répartissant la charge sur une flotte d'instances évolutive.

5.2 Réplication et redondance des données

La réplication des données client est effectuée entre les zones de disponibilité (AZ) d'Amazon Web Services (AWS). La réplication limite la possibilité de perte de données ou de retard de reprise du service si un basculement vers un centre de données de sauvegarde est requis.

5.3 Redondance du système d'alimentation

Les centres de données AWS contiennent des systèmes d'alimentation électrique redondants pour assurer le fonctionnement 24 heures sur 24, 7 jours sur 7. Des onduleurs assurent automatiquement la sauvegarde des systèmes électriques principaux en cas de panne. Les générateurs de chaque centre de données fournissent une alimentation de sauvegarde à long terme en cas de panne.

5.4 Redondance de la connectivité Internet

Un système hétérogène redondant permet de maintenir la connexion Internet à chacun des centres de données.

Le logiciel client Autodesk Fusion 360 dispose également d'un mode hors ligne grâce auquel les utilisateurs peuvent continuer à accéder à leurs conceptions et à travailler sur des copies locales lorsqu'ils ne sont pas connectés à Internet.

5.5 Sécurité de l'infrastructure physique

L'application Autodesk Fusion 360 s'exécute sur des centres de données sécurisés AWS, protégés contre les accès physiques non autorisés et les risques environnementaux par une série de contrôles de sécurité. Certains des contrôles physiques et environnementaux sont présentés ci-dessous. Une présentation complète des processus de sécurité d'AWS est disponible ici.

5.6 Contrôle de l'accès aux installations

Les centres de données AWS sont surveillés 24 heures sur 24 et 7 jours sur 7 par un personnel de sécurité physique professionnel. Le périmètre de chaque centre de données ainsi que les pièces qui contiennent les équipements informatiques et de sauvegarde sont protégés par la vidéosurveillance. Les données de vidéosurveillance sont conservées au format numérique, ce qui permet de visualiser les activités récentes à la demande. Les entrées du centre de données

sont protégées par des portiques qui limitent l'accès à une seule personne à la fois. Tous les visiteurs et les fournisseurs doivent présenter une pièce d'identité pour être admis et sont escortés à tout moment par un personnel autorisé. Seuls les employés ayant des besoins commerciaux légitimes bénéficient d'un accès au centre de données et toutes les visites sont consignées par voie électronique.

5.7 Prévention incendie

Des systèmes de détection et de suppression des incendies tels que des détecteurs de fumée et canalisations sensibles aux variations thermiques sont installés dans chaque centre de données pour protéger les salles contenant des équipements informatiques et des systèmes de sauvegarde. Des capteurs de détection de fumée sont installés au plafond et sous un sol surélevé.

5.8 Contrôleurs climatiques

Les contrôleurs climatiques des centres de données protègent les serveurs, les routeurs et les autres équipements en cas de défaillance si des seuils limites stricts des conditions environnementales sont dépassés. La surveillance est assurée par les systèmes et par le personnel afin d'éviter des conditions dangereuses, telles que la surchauffe. Les systèmes de contrôle effectuent automatiquement des ajustements qui maintiennent la température et d'autres mesures environnementales dans des plages acceptables.

6. Gestion des incidents d'exploitation

Autodesk a une politique de gestion des incidents qui définit les meilleures pratiques pour la résolution des incidents. La politique de gestion des incidents d'Autodesk met l'accent sur la consignation des étapes de correction et l'utilisation de l'analyse des causes profondes afin de créer une liste des procédures à utiliser en cas de problème. L'objectif de la politique de gestion des incidents d'Autodesk n'est pas seulement de clore rapidement et efficacement les incidents, mais aussi de collecter et de distribuer des informations sur ces derniers de manière à améliorer en permanence les processus et de pouvoir répondre aux questions futures sur la base des connaissances accumulées.

7. Gestion des correctifs

L'équipe Infrastructure Cloud dispose d'une stratégie de gestion des correctifs qui permet d'assurer un déploiement efficace des correctifs. Dans la mesure du possible, l'automatisation est appliquée pour vérifier la présence de nouveaux correctifs et préparer des listes de déploiement pouvant être approuvées par le personnel autorisé des infrastructures Cloud. La stratégie d'application de correctifs définit également des critères permettant de déterminer l'impact d'un correctif sur la stabilité des systèmes. Si un patch est identifié comme ayant un impact potentiellement élevé, un test de régression est effectué avant son déploiement. La gestion des modifications effectue le suivi du déploiement des correctifs sur les systèmes de production.

8. Gestion des modifications

L'équipe Infrastructure Cloud a une politique de gestion des modifications qui inclut les activités suivantes :

- **Formulaire de demande de modification.** Un formulaire doit être envoyé pour toutes les modifications. Celui-ci inclut le nom de l'initiateur de la modification, la priorité de la modification, la justification commerciale de la modification et une date de mise en œuvre de la modification demandée.

- **Plans de sauvegarde.** L'équipe Infrastructure Cloud crée des plans de sauvegarde détaillés avant le déploiement, afin que l'état du système puisse être restauré si une modification entraîne une interruption du service. Ces plans incluent des instructions exécutables définies dans des scripts qui restaurent l'état du système en effectuant un minimum d'étapes manuelles.

- **Fenêtres de maintenance définies.** L'équipe Infrastructure Cloud spécifie des fenêtres de maintenance planifiée, d'urgence et étendues. Elle planifie la maintenance pendant les heures creuses.

- **Plan de test.** L'équipe Infrastructure Cloud définit un ensemble de tests pour vérifier que les fonctionnalités sont accessibles après le déploiement d'une modification.

- **Exécution du test.** Une fois le déploiement terminé, l'équipe d'assurance qualité d'Autodesk Fusion 360 et d'Infrastructure Cloud effectue des tests pour vérifier que les fonctionnalités identifiées comme étant à risque restent disponibles.

9. Gestion des capacités

L'accès des clients aux services Cloud étant fourni à la demande via un modèle en libre-service, les tendances du trafic sont très variables et soumises à des pics d'utilisation. En cas de pic, la disponibilité d'un service peut être affectée négativement si le pool de ressources informatiques qui alimentent le service est épuisé. Pour maintenir un niveau élevé de disponibilité, l'équipe Infrastructure Cloud met en œuvre une stratégie de gestion des capacités. Ces pratiques sont les suivantes :

- **Enregistrement fréquent de l'utilisation des ressources.** L'utilisation des ressources d'Autodesk Fusion 360 est collectée à intervalles réguliers sur un ensemble de composants d'infrastructure, notamment les instances virtuelles, les volumes de stockage virtuels et les périphériques réseau virtuels. Les statistiques d'utilisation sont stockées dans un répertoire de gestion de la capacité.

- **Planification de la capacité.** L'équipe Infrastructure Cloud se sert de la gestion de la capacité pour générer un plan détaillé qui documente les niveaux actuels d'utilisation et modélise les niveaux futurs en fonction de l'analyse statistique et de l'impact des améliorations à venir apportées aux fonctionnalités de l'entreprise. Le plan de capacité est mis à jour si nécessaire ou si des modifications importantes sont détectées dans les schémas d'utilisation.

- **Allocation des ressources.** Les ressources de calcul sont allouées à la demande des clients. Des ressources de calcul préchauffées sont toujours disponibles. En cas de pic d'activité, les nouvelles ressources sont instanciées. Par exemple, la disponibilité pour des ressources du navigateur Autodesk Fusion est généralement atteinte en moins de 10 minutes.

- **Contrôle des activités.** Les tableaux de bord et les alertes d'activité sont définis dans les services principaux, ce qui permet aux ingénieurs d'observer l'activité du système et d'effectuer des analyses et des examens post-incident.

10. Alertes et surveillance

Pour fournir le délai moyen de résolution le plus court possible, Autodesk utilise des systèmes automatisés qui surveillent Fusion 360 et valident l'intégrité du service. Chaque composant, de la base de données aux services, est contrôlé individuellement.

En cas d'événement affectant le service, des alertes sont générées et l'équipe Infrastructure Cloud est avertie par un processus de remontée d'informations.

L'état de santé du service détaille également l'interaction entre les services Autodesk. Un service comme Autodesk Fusion 360 est très sensible au service ACM (contrôle d'accès). Chaque service doit être résilient lorsqu'un service dépendant tombe en panne et doit être en mesure d'entrer en défaillance de façon contrôlée lorsqu'il ne peut plus fonctionner, sans que cela n'entraîne une perte de données pour le client.

L'état du service Fusion 360 est affiché publiquement dans le service de tableau de bord sur l'état général d'Autodesk : https://health.autodesk.com.

11. Temps d'arrêt nul lors des déploiements

Lorsque des correctifs sont appliqués à l'environnement de production, une approche de déploiement bleu/vert est adoptée pour le navigateur Autodesk Fusion et d'autres services Fusion 360. Cela permet de s'assurer que les clients ne subissent aucune interruption du service.

12. Contrôles opérationnels d'Autodesk Fusion 360

Autodesk Fusion 360 protège les données sensibles des clients contre les accès non autorisés.

- **Restrictions physiques imposées aux centres de données.** Les restrictions physiques appliquées aux centres de données empêchent les personnes non autorisées d'accéder au matériel et aux systèmes de sauvegarde utilisés par Autodesk Fusion 360.
- **Vérifications des antécédents.** Les employés ayant un accès physique aux ressources informatiques et aux systèmes de sauvegarde utilisés par Autodesk Fusion 360 doivent être soumis à un contrôle de leurs antécédents.
- **Réplication des données.** La réplication des données copie les données client dans des centres de données redondants afin de maintenir la continuité de l'activité en cas de basculement entre des installations.
- **Technologies redondantes**. Des technologies redondantes telles que les équilibreurs de charge et les bases de données en cluster limitent les points de défaillance uniques.

13. Sécurité Autodesk

L'équipe sécurité d'Autodesk est un groupe de spécialistes dédiés à la sécurité des informations, qui se concentre sur l'identification et l'application des pratiques de sécurité au sein de l'environnement Cloud d'Autodesk. L'équipe est notamment chargée des tâches suivantes :

- Examen de la sécurité de l'implémentation et de la conception de l'infrastructure Cloud d'Autodesk
- Définition et vérification de la mise en œuvre des stratégies de sécurité, notamment la gestion des identités et des accès, la gestion des mots de passe et la gestion des vulnérabilités
- Vérification du respect des procédures de sécurité établies en procédant à des examens et à des audits internes
- Identification et mise en œuvre de technologies sécurisant les informations du client
- Appel à des experts tiers en sécurité pour effectuer des évaluations de la sécurité des informations

- Surveillance des services Cloud pour détecter d'éventuels problèmes de sécurité et réaction aux incidents en fonction des besoins
- Révision annuelle de la politique de sécurité d'Autodesk

13.1 Analyses de vulnérabilité et test d'intrusion

Les services Fusion 360 sont soumis à un test d'intrusion annuel et à des analyses régulières pour détecter les menaces et les vulnérabilités liées à la sécurité. L'application est également soumise à une analyse statique et à des analyses de bibliothèques tierces. Les analyses de sécurité et les tests d'intrusion couvrent une large gamme de vulnérabilités définies par le projet Open Web Application Security Project (OWASP) et le SANS top 25.

13.2 Sécurité réseau

La sécurité réseau est mise en œuvre à l'aide d'une combinaison de contrôles physiques et logiques, notamment un chiffrement, des pare-feux et des procédures de sécurisation renforcée des systèmes. En outre, AWS fournit des contrôles de sécurité réseau qui protègent leurs centres de données physiques. Pour en savoir plus, consultez les meilleures pratiques en matière de sécurité, d'identité et de conformité.

13.3 Chiffrement

Tout le trafic du réseau est chiffré lorsqu'il est transmis via Internet vers le périmètre de l'environnement Cloud d'Autodesk. Les informations sensibles, telles que les informations d'identification, les informations de session de l'application, les jetons d'accès et les profils utilisateur, sont chiffrées au repos.

13.4 Confidentialité

Autodesk est transparent sur la manière dont les données personnelles des clients sont collectées et utilisées. Pour en savoir plus, consultez la Déclaration de confidentialité d'Autodesk.

14. Ressources

Les ressources suivantes fournissent des informations générales sur Autodesk et d'autres sujets abordés dans la section principale de ce document.

- **Autodesk** : pour en savoir plus sur Autodesk, visitez le site https://www.autodesk.fr.
- **Centre de confiance Autodesk** : pour en savoir plus sur le Centre de confiance Autodesk, visitez le site https://www.autodesk.fr/trust/overview.
- **Autodesk Fusion 360** : pour en savoir plus sur Fusion 360, visitez le site https://www.autodesk.fr/products/fusion-360/overview.