UKG Dimensions dans le Cloud Google

Sécurité, confidentialité et technologie

Introduction

Les entreprises sont de plus en plus nombreuses à transférer leurs technologies métier vers le Cloud. Elles veulent donc s'assurer que les fournisseurs respectent, voire dépassent, les normes du secteur en matière de sécurisation de leurs applications hébergées. UKG™ (Ultimate Kronos Group) vous garantit que votre solution hébergée sera en ligne et disponible, les technologies les plus récentes étant utilisées pour la sécurisation et la maintenance de l'application.

UKG s'engage à concevoir et à déployer des systèmes et des processus de gestion des temps et de planification afin de protéger la confidentialité des informations personnelles dans toutes les phases du cycle de vie des données.

Certifications et contrôles

UKG Dimensions™ (anciennement Workforce Dimensions™) est déployé sur la plate-forme Google™ Cloud (GCP), laquelle a obtenu les certifications ISO 27001, 27017 et 27018. Chaque année, GCP fait l'objet d'un audit réalisé par un cabinet indépendant, selon les critères SSAE 18 SOC 2 de l'AICPA. La plate-forme a démontré sa conformité à la norme « HIGH » FedRAMP et a obtenu une autorisation de fonctionnement à ce niveau. L'application et le service UKG Dimensions ont obtenu les certifications ISO 27001, 27018 et 27017. UKG Dimensions fait également l'objet d'un audit annuel sur la base des exigences SSAE 18 des Trust Services Principles de l'AICPA en matière de sécurité, de confidentialité, de disponibilité, d'intégrité du traitement et de respect de la vie privée. Les rapports UKG Dimensions SOC 2 Type II et Google Cloud Platform SOC 2 sont disponibles sur demande, moyennant l'exécution d'un accord mutuel de confidentialité.

Confidentialité

Leader technologique des solutions de gestion des temps et de planification, UKG comprend les pressions réglementaires auxquelles nos clients sont confrontés dans le domaine en constante évolution de la vie privée. Conformément à notre philosophie centrée sur le client, UKG s'engage à concevoir et à déployer des systèmes et des processus de gestion des temps et de planification afin de protéger la confidentialité des informations personnelles dans toutes les phases du cycle de vie des données, dans le respect des instructions formulées par nos clients, de notre politique de confidentialité publiée et des lois applicables.

Culture de confidentialité

Le respect de la confidentialité des données commence au niveau de l'équipe de direction d'UKG. L'engagement et le soutien de la direction ont contribué à sensibiliser davantage les employés et à améliorer les processus pour la protection des données et la confidentialité des informations personnelles.

Enregistrements relatifs au traitement des données

Le processus d'inventaire des données mis en place par UKG a pour but d'enregistrer, avec une grande précision, les activités de traitement réalisées au nom de ses clients.

Traitement des données

UKG applique des mesures techniques et structurelles afin d'accompagner ses clients dans leurs obligations en matière de sécurité et de conformité, telles que stipulées dans le RGPD (Règlement Général sur la Protection des Données) de l'Union européenne.

Évaluations d'impact sur la confidentialité

Au fur et à mesure de l'évolution de ses produits et processus, UKG continuera d'évaluer la confidentialité des données et d'identifier les aspects problématiques au moyen du système UKG d'inventaire et de classification des données.

Gestion des risques au niveau des fournisseurs

Le gestion des risques au niveau des fournisseurs d'UKG inclut un contrôle et des engagements contractuels visant à garantir la conformité des tiers avec les principes du RGPD de l'Union européenne en matière de traitement des données.

Gestion des incidents

Le plan UKG d'intervention en cas d'incidents de cybersécurité (UKG Cybersecurity Incident Response Plan) permet de gérer les incidents impliquant des informations personnelles avec le niveau de réponse le plus strict.

Chiffrement : protocoles et cryptographie

Données pendant leurs transferts : les communications entre applications Web, mobiles, interfaces de programmation d'applications (API) et terminaux sont protégées par le protocole TLS (Transport Layer Security). De plus, UKG prend en charge les terminaux des clients qui se connectent avec TLS 1.2.

Les services de protocole sécurisé de transfert de fichiers (SFTP) utilisent le protocole de transfert Secure Shell pour fournir un point de contact générique aux clients qui envoient et reçoivent des fichiers vers et depuis UKG Dimensions. En outre, le chiffrement des fichiers PGP est assuré en standard pour toutes les intégrations de fichiers plats.

Données pendant leur stockage : UKG sécurise les données au niveau du stockage pour les environnements de production et hors production du client, pour les données dans GCP, en utilisant le chiffrement Advanced Encryption Standard 256 bits.

Des mesures de sécurité strictes ont été mises en place afin de protéger les données des clients au moyen de protocoles de chiffrement et de la cryptographie.

Sécurité du réseau

Toutes les connexions Internet franchissent des pare-feu redondants afin d'appliquer des contrôles d'accès et d'assurer la surveillance et la traçabilité du trafic. UKG configure les règles des pare-feu sur l'option « deny all » (tout refuser) par défaut. Les ports et protocoles requis sont ouverts en fonction d'un objectif professionnel défini. Les proxies de réseau interdisent tout trafic d'application non nécessaire.

Des systèmes de détection et de prévention des intrusions sur le réseau sont mis en œuvre pour atténuer les risques d'intrusion et les attaques de logiciels malveillants. Des analyses de vulnérabilité de l'environnement et de l'application hébergés sont effectuées, les résultats sont examinés et les vulnérabilités sont corrigées conformément au rapport UKG SOC 2.

La transmission électronique de fichiers entre l'environnement et les clients est autorisée avec l'utilisation du protocole SFTP et des API. Les paramètres de durcissement sur les serveurs de production sont contrôlés par rapport aux normes de durcissement définies.

Contrôles d'accès aux applications

UKG Dimensions applique une stratégie de déploiement multi-locataire, où les données des clients sont séparées par schéma de base de données. Tous les accès des locataires sont contrôlés par une passerelle API sécurisée, et le trafic est résolu par l'ID du locataire.

L'accès d'un utilisateur au système UKG Dimensions est contrôlé au moyen de profils d'accès configurables. Les profils d'accès suivants déterminent ce qu'un utilisateur peut voir et faire et se composent de deux éléments, qui vous permettent de définir précisément l'accès au système en fonction des exigences spécifiques de son poste au sein de votre entreprise :

Profils d'accès aux fonctions : ce profil détermine les fonctions qu'un utilisateur peut exécuter dans le système et ce qu'il peut faire.

Profils d'affichage et d'accès aux données : ces profils déterminent non seulement les catégories de paie, les règles de travail et les rapports qu'un utilisateur peut utiliser dans le système, mais aussi les contrôles d'affichage, qui affectent la façon dont un utilisateur visualise les composants d'UKG Dimensions. Ils contrôlent également les employés auxquels un responsable peut accéder.

Authentification

UKG Dimensions prend en charge le protocole SAML 2.0, norme du secteur, pour l'intégration du SSO.

Le service d'authentification d'UKG Dimensions fournit un service SSO fédéré à haute disponibilité pour la connexion des utilisateurs à UKG Dimensions , et ce depuis les postes de travail de l'entreprise cliente, les dispositifs professionnels utilisés à domicile et les appareils mobiles.

Le service d'authentification UKG Dimensions prend également en charge l'authentification de base pour les clients qui n'ont pas migré vers le SSO. Les noms d'utilisateurs et les mots de passe sont stockés dans le système UKG Dimensions pour les clients utilisant l'authentification de base. Les clients peuvent décider que certains (par exemple, les responsables) utiliseront le SSO et que les autres utilisateurs (non responsables) utiliseront l'authentification de base.

Accès et authentification

L'accès des utilisateurs à UKG Dimensions est contrôlé au moyen de profils d'accès configurables, tandis que l'authentification s'appuie sur le SSO.

Évolutivité

UKG Dimensions présente une architecture de services distribués et tire parti de micro-services au sein d'une plate-forme multi-couche.

UKG Dimensions offre des capacités d'automatisation et de gestion du Cloud pour approvisionner et configurer l'infrastructure sous-jacente à la solution logicielle. Ceci permet de faire évoluer les services horizontalement et/ou verticalement, indépendamment les uns des autres, en fonction de l'utilisation réelle ou prévue.

UKG recueille un volume important d'indicateurs de performance sur l'infrastructure et les applications afin d'évaluer la demande globale de services, ainsi que l'intégrité et les performances de l'environnement. Ces mesures sont exploitées, à la fois de façon passive et active, à diverses fins opérationnelles.

UKG utilise régulièrement la capacité de gestion du Cloud, et l'appuie sur des données quantitatives et qualitatives issues de la surveillance. Les services sont adaptés de façon appropriée à la charge réelle et prévue du système.

Performances

UKG Dimensions est soumis à un processus rigoureux d'évaluation des performances au cours du développement, avec des seuils de pointe pour le trafic interactif, le trafic d'intégration (API) et les calculs et analyses en arrière-plan. La solution a été imaginée et conçue pour offrir des performances élevées, afin de répondre aux besoins de nos clients dans tous les secteurs d'activités et pour un large éventail d'effectifs. Ce processus d'évaluation des performances est intégré au cycle de vie du développement logiciel et s'applique aussi bien aux fonctionnalités nouvelles qu'aux fonctionnalités existantes.

Dans les environnements orientés clients, les temps de réponse sont régulièrement contrôlés au moyen d'une combinaison de surveillance synthétique des transactions à partir de plusieurs emplacements géographiques (représentant l'expérience de la base client) et de surveillance interne (représentant la partie UKG de l'expérience).

Les outils internes de surveillance des performances applicatives offrent une visibilité depuis la périphérie du réseau UKG dans le Cloud jusqu'au niveau des données. Les ingénieurs d'UKG peuvent ainsi localiser précisément tout problème de performance. Les données agrégées, issues de ces différents outils de surveillance, sont régulièrement examinées par des équipes d'ingénierie et d'exploitation spécialisées, afin de s'assurer qu'UKG Dimensions répond aux attentes de nos clients et aux normes de performances élevées d'UKG, voire dépasse celles-ci.

Processus d'évaluation des performances

UKG Dimensions est soumis à un processus rigoureux d'évaluation des performances au cours du développement. La solution a été imaginée et conçue pour offrir des performances élevées, afin de répondre aux besoins de nos clients dans tous les secteurs d'activités et pour un large éventail d'effectifs.

Haute disponibilité

L'architecture UKG Dimensions intègre la haute disponibilité et la résilience dans les couches de la solution afin de garantir le SLA de 99,75 % d'UKG. Tous les composants de service des couches web, applications et middleware sont mis en miroir sur plusieurs instances de serveur afin d'assurer la redondance. Des technologies d'équilibrage des charges et le clustering des logiciels sont mis en œuvre pour accroître la disponibilité.

UKG Dimensions s'appuie sur les meilleurs micro-services afin de créer une véritable plate-forme distribuée, garantissant une haute disponibilité. Ces services permettent un meilleur enclavement des défaillances ; si un micro-service tombe en panne, les autres continuent de fonctionner. UKG permet d'ajouter d'autres services, et ceux-ci peuvent être répartis sur plusieurs nœuds, voire sur plusieurs centres de données, pour répondre à une demande accrue.

Toutes les bases de données UKG Dimensions utilisent le clustering de bases de données avec une réplication synchrone ou asynchrone en continu entre les serveurs de bases de données et les zones Google.

Service et disponibilité

Les services UKG Dimensions sont conçus pour fonctionner en utilisant plusieurs centres de données dans le Cloud (zones) dans une zone géographique (région). En cas d'interruption du service, l'objectif du temps de reprise est de 24 heures et l'objectif de point de reprise est de 4 heures.

Reprise après sinistre

Le programme de reprise après sinistre d'UKG dans le Cloud (UKG Cloud Disaster Recovery Program) a été élaboré et est géré afin d'assurer l'adéquation permanente avec le programme de gestion de la continuité des activités d'UKG (UKG Business Continuity Management Program), qui définit les exigences relatives aux plans de reprise après sinistre et aux stratégies de gestion de crise d'UKG.

Les services UKG Dimensions sont conçus pour fonctionner en utilisant plusieurs centres de données dans le Cloud (zones) dans une zone géographique (région). Le programme de reprise après sinistre d'UKG dans le Cloud est basé sur une stratégie de basculement « tout ou rien ». Si les services UKG Dimensions du client sont indisponibles et ne peuvent pas être rétablis dans un délai acceptable, l'ensemble de la pile sera basculée, en cas d'incident grave, vers la région de reprise après sinistre (DR).

Une fois que les services ont été restaurés dans la région DR, cet environnement continuera en tant que région de production. Dans le but de maintenir la continuité du service standard de reprise après sinistre d'UKG Dimensions, UKG préparera une nouvelle région de reprise après sinistre dans le cadre du processus de reprise après sinistre de la production.

L'objectif de temps de reprise (RTO) est de 24 heures, et l'objectif de point de reprise (RPO) est de 4 heures.

Centres de données de pointe

UKG Dimensions est déployé dans GCP. La sécurité et la protection des données sont au premier plan des critères de conception et font partie intégrante de toutes les opérations de Google. Dans tous les centres de données Google, la sécurité physique inclut un modèle de sécurité à plusieurs niveaux qui utilise des dispositifs de protection tels que des alarmes, des barrières d'accès aux véhicules, des clôtures de périmètre, des détecteurs de métaux et des dispositifs biométriques. Les centres de données de Google sont surveillés 24 heures sur 24 et 7 jours sur 7 par des caméras haute résolution, à l'intérieur comme à l'extérieur.

Les mesures de sécurité sont encore renforcées dans les zones qui sont plus proches du centre de données lui-même. Moins d'1 % des employés de Google mettront un jour les pieds dans un centre de données de Google. Seuls les employés autorisés de Google exerçant certains rôles spécifiques peuvent accéder à ces espaces. L'accès au centre de données est uniquement possible par un couloir de sécurité équipé d'un système de contrôle d'accès multifacteur, nécessitant des badges de sécurité et des données biométriques pour entrer.

Le Cloud Google s'exécute sur une plate-forme technologique qui a été pensée, conçue et créée pour fonctionner en toute sécurité. Google est un innovateur dans le domaine des technologies de gestion du matériel, des logiciels, des réseaux et des systèmes. À partir de cette expertise, l'entreprise a conçu ses serveurs, son système d'exploitation propriétaire et ses centres de données géographiquement distribués selon les principes de la « défense en profondeur ». Ceci a donné lieu à une infrastructure informatique plus sûre et plus facile à gérer que les technologies plus traditionnelles.

La « défense en profondeur » décrit les multiples couches de défense qui protègent le réseau de Google contre les attaques extérieures. Seuls les services et protocoles autorisés qui respectent les exigences de sécurité de Google peuvent le franchir, tout le reste étant automatiquement rejeté. Des pare-feu et des listes de contrôle d'accès conformes aux normes industrielles assurent la ségrégation du réseau. Tout le trafic est acheminé via des serveurs Google Front End (GFE) personnalisés afin de détecter et d'arrêter les demandes malveillantes et les attaques par déni de service distribué (DDoS). En outre, les serveurs GFE ne sont autorisés à communiquer qu'avec une liste contrôlée de serveurs en interne. Cette configuration de « refus par défaut » empêche les serveurs GFE d'accéder à des ressources non souhaitées. Les journaux sont régulièrement examinés afin d'identifier toute exploitation d'erreurs de programmation. L'accès aux dispositifs en réseau est limité au personnel autorisé.

Les centres de données de Google disposent de systèmes d'alimentation et de contrôles environnementaux redondants. Chaque composant critique dispose d'une source d'alimentation principale et d'une source d'alimentation alternative, chacune ayant la même puissance. Les générateurs diesel de secours sont capables de fournir suffisamment d'énergie électrique pour faire fonctionner chaque centre de données à pleine capacité.

Les systèmes de refroidissement maintiennent une température de fonctionnement constante pour les serveurs et autres équipements, ce qui réduit les risques d'interruptions de service.

Les équipements de détection et d'extinction des incendies permettent d'éviter les dommages au matériel. Les détecteurs de chaleur, d'incendie et de fumée déclenchent des alarmes sonores et visuelles dans les zones concernées, sur les consoles des opérations de sécurité et au niveau des postes de télésurveillance.

Cloud Google

Google est un innovateur dans le domaine des technologies de gestion du matériel, des logiciels, des réseaux et des systèmes. Le Cloud Google s'exécute sur une plate-forme technologique qui a été pensée, conçue et créée pour fonctionner en toute sécurité.

Surveillance des systèmes et gestion des vulnérabilités

UKG a déployé plusieurs couches de sécurité, en commençant par le périmètre du système, notamment des pare-feu technologiques de nouvelle génération, des systèmes de prévention des intrusions, des systèmes de détection des intrusions (IDS), la surveillance des journaux et des logiciels antivirus. L'environnement fait l'objet d'une surveillance permanente.

Les systèmes de gestion des informations et des événements de sécurité fusionnent les sources de données (par exemple, les journaux d'applications, les journaux de pare-feu, les journaux des IDS) pour une analyse et une alerte granulaires. En plus de la génération d'alertes IDS, un tableau de bord de sécurité facilite les analyses. Il est à la disposition du personnel de sécurité d'UKG. Des mesures de détection et de prévention sont appliquées à plusieurs niveaux.

Matériel et équipements de stockage

Google assure le suivi de l'emplacement et de l'état de tous les équipements de stockage dans ses centres de données. Google met également à niveau le matériel obsolète afin d'améliorer la vitesse de traitement et l'efficacité énergétique ou pour augmenter la capacité de stockage.

Nettoyage des supports et destruction des données

Google assure le suivi de l'emplacement et de l'état de tous les équipements de stockage dans ses centres de données, de l'acquisition à la destruction en passant par l'installation et la mise hors service, grâce à des étiquettes d'actifs qui sont enregistrées dans la base de données des actifs de Google. Les supports de stockage physique peuvent être mis hors service pour toute une série de raisons. Si un composant échoue à un test de performance à un moment quelconque de son cycle de vie, il est retiré de l'inventaire et mis hors service. Google met également à niveau le matériel obsolète afin d'améliorer la vitesse de traitement et l'efficacité énergétique ou pour augmenter la capacité de stockage.

Que le matériel soit déclassé en raison d'une panne, d'une mise à niveau ou pour toute autre raison, les supports de stockage sont mis hors service en appliquant les mesures de protection appropriées. Les disques durs Google utilisent des technologies telles que le cryptage intégral du disque pour protéger les données au repos lors de la mise hors service. Lorsqu'un disque dur est mis hors service, les personnes autorisées devront soit : 1) vérifier que le disque est effacé en écrasant le disque avec des zéros et en exécutant un processus de vérification pour s'assurer que le disque ne contient aucune donnée ; ou 2) utiliser un outil pour écraser et déformer le disque ou le déchiqueter en petits morceaux.

À propos d'UKG

Chez UKG (Ultimate Kronos Group), our purpose is people™. Fruit d'une fusion qui a donné naissance à l'une des plus grandes entreprises Cloud au monde, UKG estime que les organisations doivent se concentrer sur leurs employés pour réussir. Proposées par l'un des principaux fournisseurs, à l'échelle mondiale, de solutions de gestion du capital humain, de la paie, de la prestation de services RH et de gestion des temps et de planification, UKG propose les solutions primées Pro, Dimensions et Ready afin d'aider des dizaines de milliers d'organisations, dans tous les secteurs et dans toutes les régions du monde, à obtenir de meilleurs résultats commerciaux, à améliorer l'efficacité des RH, à rationaliser le processus de paie et à faire du travail une expérience plus agréable et plus connectée pour tous. UKG compte plus de 12 000 employés dans le monde entier et est connue pour sa culture d'intégration sur le lieu de travail. L'entreprise a remporté de nombreux prix pour sa culture, ses produits et ses services, notamment en se classant plusieurs années de suite dans la liste des *100 meilleurs employeurs*. Pour en savoir plus, visitez le site ukg.com.

UKG

Our purpose is people