

### IBM Cognos Controller on Cloud

Voici la Description de Service de la Commande du Client :

#### 1. Service Cloud

L'offre de Services Cloud est décrite ci-dessous et spécifiée dans un Bon de Commande pour les offres autorisées sélectionnées. Le Bon de Commande est constitué du Devis fourni et de l'Autorisation d'Utilisation (ci-après dénommée « PoE ») qui confirme la date de début et la durée des Services Cloud. La facturation commencera suite à la mise à disposition du Service Cloud.

##### 1.1 IBM Cognos Controller User on Cloud

IBM Cognos Controller est un logiciel de consolidation financière qui prend en charge les processus de clôture, de consolidation et de rapport. Cette offre permet aux utilisateurs de produire des résultats financiers, de créer des rapports financiers et de gestion et fournit une vue professionnelle des principaux ratios et unités de mesure financiers.

IBM Cognos Controller User on Cloud permet de consolider et d'administrer le système et d'établir des rapports au niveau du système.

##### 1.2 IBM Cognos Controller Jump Start on Cloud

Le service à distance IBM Cognos Controller Jump Start on Cloud inclut jusqu'à 80 heures d'accompagnement et d'assistance, y compris l'identification facilitée d'un cas d'utilisation IBM Cognos Controller on Cloud (CCoC) initial, l'accompagnement sur la planification de projet et le lancement d'une implémentation IBM CCoC, l'accompagnement sur des pratiques avérées permettant la création de rapports IBM CCoC, ainsi que l'accompagnement sur la gestion et l'administration d'IBM CCoC. Les services sont acquis par Engagement et arrivent à expiration 90 jours suivant leur acquisition, que toutes les heures aient été utilisées ou non.

##### 1.3 IBM Cognos Controller Additional Non-Production Instance

Cette offre ajoute d'autres instances de Non-Production d'IBM Cognos Controller. Elle ne peut être utilisée que dans le cadre des activités du Client non destinées à la production, y compris, sans que cette liste soit limitative, pour les activités de test, d'optimisation de performances, de diagnostic d'incident, de tests de performances, de transfert, d'assurance qualité et/ou pour développer, à l'aide d'interfaces de programmation d'application publiées, des ajouts ou extensions de l'offre utilisés en interne.

#### 2. Description de la sécurité

##### 2.1 Règles de sécurité

IBM dispose d'une équipe chargée de la sécurité des informations et applique également des règles de confidentialité et de sécurité qui sont communiquées aux employés IBM. IBM exige une formation à la confidentialité et la sécurité pour le personnel qui prend en charge les centres de données IBM. Les règles et normes de sécurité IBM sont examinées et réévaluées tous les ans. Les incidents de sécurité IBM sont traités conformément à une procédure détaillée de réponse après incident.

##### 2.2 Contrôle d'accès

L'accès aux données client, si nécessaire, n'est autorisé que par les représentants agréés du service de support IBM, conformément aux principes de répartition des tâches. Le personnel IBM utilise l'authentification à deux facteurs auprès d'un hôte de gestion de « passerelle » intermédiaire. Toutes les connexions sont des canaux chiffrés lors de l'accès aux données client. Tous les accès aux données client et le transfert des données vers ou hors de l'environnement d'hébergement sont consignés. L'utilisation du WIFI est interdite dans les centres de données IBM qui prennent en charge ce Service Cloud.

##### 2.3 Intégrité et Disponibilité des Services

Les modifications des logiciels d'application et des systèmes d'exploitation sont régies par la procédure de gestion des modifications d'IBM. Les modifications des règles de pare-feu sont également régies par la procédure de gestion des modifications et sont examinées par le personnel de sécurité IBM avant d'être mises en oeuvre. IBM surveille le centre de données 24 heures sur 24 et 7 jours sur 7. Le scannage de vulnérabilité interne et externe est régulièrement effectué par des administrateurs autorisés

et des fournisseurs tiers pour aider à détecter et résoudre les risques potentiels liés à la sécurité des systèmes. Les systèmes de détection de logiciel malveillant (antivirus, détection d'intrusion, scannage de vulnérabilité et prévention contre les intrusions) sont utilisés dans tous les centres de données IBM. Les services de centre de données d'IBM prennent en charge de nombreux protocoles de distribution d'informations pour la transmission de données sur les réseaux publics. Exemples : HTTPS/SFTP/FTPS/S/MIME et VPN de site à site. Les données de sauvegarde destinées au stockage hors site sont chiffrées avant le transport.

## **2.4 Consignation des Activités**

IBM gère des journaux de ses activités pour les systèmes, applications, référentiels de données, middleware et unités d'infrastructure de réseau qui sont capables de et configurés pour consigner l'activité. Pour minimiser la possibilité de falsification et pour permettre l'analyse centralisée, la gestion d'alertes et la génération de rapports, l'activité est consignée en temps réel dans des référentiels de journaux centralisés. Les données sont signées pour empêcher la contrefaçon. Les journaux sont analysés en temps réel et via des rapports d'analyse périodiques pour détecter les comportements anormaux. Le personnel des opérations est averti des anomalies et contacté, si nécessaire, un spécialiste de sécurité joignable 24 heures sur 24 et 7 jours sur 7.

## **2.5 Sécurité physique**

IBM gère des normes de sécurité physique conçues pour restreindre l'accès physique non autorisé aux centres de données IBM. Seuls des points d'accès limité existent dans les centres de données ; ils sont contrôlés par l'authentification à deux facteurs et surveillés par des caméras de surveillance. L'accès n'est autorisé qu'au personnel autorisé dont l'accès est approuvé. Le personnel des opérations vérifie l'approbation et émet un badge d'accès accordant l'accès nécessaire. Les employés auxquels ces badges sont destinés doivent restituer leurs autres badges d'accès et ne peuvent être en possession du badge d'accès au centre de données que pendant la durée de leur activité. L'utilisation des badges est consignée. Les visiteurs non IBM sont enregistrés dès leur arrivée dans les locaux et sont accompagnés lorsqu'ils se trouvent dans les locaux. Les zones de livraison et les plateformes de chargement ainsi que tous les autres lieux d'entrée des personnes non autorisées sont contrôlés et isolés.

## **2.6 Conformité**

IBM certifie que ses pratiques en matière de protection de la vie privée sont conformes à celles de l'accord Safe Harbor du Département du Commerce des États-Unis : avertissement, choix, transfert ultérieur, accès et exactitude, sécurité et mise en oeuvre. IBM effectue annuellement des audits SSAE 16 (ou leur équivalent) conformes aux normes de l'industrie dans ses centres de données de production. IBM passe en revue les activités liées à la sécurité et la confidentialité quant à leur conformité aux besoins métier d'IBM. Des évaluations et des audits sont effectués régulièrement par IBM pour confirmer le respect des règles de sécurité des informations. Les employés d'IBM et les employés des fournisseurs suivent tous les ans une formation à la sensibilisation et à la sécurité de la main d'oeuvre. Les membres du personnel sont informés tous les ans de leurs objectifs de travail et de leurs responsabilités quant au respect de l'éthique professionnelle, la confidentialité et les obligations de sécurité d'IBM.

## **3. Engagement de niveau de service**

IBM fournit l'Accord relatif aux Niveaux de Service (ci-après dénommé « Accord relatif aux Niveaux de Service » ou « SLA ») de disponibilité ci-dessous pour le Service Cloud. Le Client reconnaît que l'Accord relatif aux Niveaux de Service ne constitue pas une garantie pour le Client.

### **3.1 Définitions**

- a. « Contact Agréé » signifie la ou les personnes que le Client a indiquées à IBM et qui sont autorisées à soumettre des Réclamations aux termes du présent « Accord relatif aux Niveaux de Service ».
- b. « Crédit de Disponibilité » signifie la réparation fournie par IBM pour une Réclamation validée. Le Crédit de Disponibilité sera appliqué sous la forme d'un avoir ou d'une remise sur une future facture des redevances d'abonnement au Service Cloud.
- c. « Réclamation » signifie une réclamation que le Client soumet à IBM, conformément à l'Accord relatif aux Niveaux de Service, selon laquelle un Niveau de Service n'a pas été satisfait pendant un Mois Contractuel.

- d. « Client » signifie une entité s'abonnant au Service directement auprès d'IBM, qui ne manque pas à ses obligations importantes, y compris les obligations de paiement, au titre de son contrat avec IBM pour le Service.
- e. « Mois Contractuel » signifie chaque mois complet pendant la durée du Service, mesuré entre le premier jour du mois à minuit (heure de l'Est des États-Unis) et le dernier jour du mois à 23h59 (heure de l'Est des États-Unis).
- f. « Durée d'Indisponibilité » signifie une période de temps pendant laquelle le traitement du système de production pour le Service Cloud s'est arrêté et que les utilisateurs du Client ne peuvent pas utiliser tous les aspects du Service Cloud pour lequel ils disposent des droits. La Durée d'Indisponibilité ne comprend pas la période pendant laquelle le Service Cloud n'est pas disponible pour les raisons suivantes :
  - (1) indisponibilité de maintenance programmée ou annoncée ;
  - (2) événements ou causes échappant au contrôle d'IBM (par exemple, catastrophes naturelles, pannes Internet, maintenance d'urgence, etc.) ;
  - (3) incidents liés aux applications, équipements ou données du Client ou d'un tiers ;
  - (4) non-respect des configurations système requises et des plateformes prises en charge pour l'accès au Serveur ; ou
  - (5) conformité d'IBM à toute conception, spécification ou instruction fournie à IBM par le Client ou par un tiers pour le compte du Client.
- g. « Événement » signifie une circonstance ou un ensemble de circonstances réunies, donnant lieu au non-respect d'un Niveau de Service.
- h. « Niveau de Service » signifie la norme exposée ci-dessous permettant à IBM de mesurer le niveau de service qu'elle fournit au titre du présent Accord relatif aux Niveaux de Service (ou « SLA »).

### 3.2 Crédits de Disponibilité

- a. Pour pouvoir soumettre une Réclamation, le Client doit consigner un ticket de support de Gravité 1 (comme défini ci-dessous dans la section Support Technique) pour chaque événement auprès du centre d'assistance technique IBM, dans les 24 heures suivant la première fois où le Client a eu connaissance que l'Événement a eu une incidence sur l'utilisation du Service Cloud par le Client. Le Client doit fournir toutes les informations nécessaires relatives à l'Événement et collaborer de manière raisonnable avec IBM lors du diagnostic et de la résolution de l'Événement.
- b. Le Client doit soumettre sa Réclamation pour un Crédit de Disponibilité au plus tard dans les trois (3) jours ouvrables suivant la fin du Mois Contractuel au cours duquel la Réclamation a eu lieu.
- c. Les Crédits de Disponibilité sont basés sur la Durée d'Indisponibilité mesurée depuis la première fois que le Client a signalé des problèmes relatifs à la Durée d'Indisponibilité. Pour chaque Réclamation valide, IBM appliquera le Crédit de Disponibilité applicable le plus élevé, en fonction du Niveau de Service Obtenu lors de chaque Mois Contractuel, comme indiqué dans le tableau ci-dessous. IBM ne sera pas redevable de plusieurs Crédits de Disponibilité pour le même Événement au cours du même Mois Contractuel.
- d. Le nombre total de Crédits de Disponibilité accordés pour tout Mois Contractuel ne dépassera en aucun cas dix pour-cent (10 %) d'un douzième (1/12ème) de la redevance annuelle que le Client paie à IBM pour le Service Cloud.

### 3.3 Niveaux de service

Disponibilité du Service Cloud pendant un Mois Contractuel

Disponibilité pendant un Mois Contractuel	Crédit de Disponibilité (% de Redevance d'Abonnement Mensuel pour le Mois Contractuel objet d'une Réclamation)
99 % – 99,75 %	2 %
95 % – 98,99 %	5%
Inférieur à 95,0 %	10 %

La disponibilité, exprimée en pourcentage, est calculée comme suit : (a) le nombre total de minutes d'un Mois Contractuel moins (b) le nombre total de minutes de la Durée d'Indisponibilité au cours d'un Mois Contractuel, divisé par (c) le nombre total de minutes d'un Mois Contractuel.

Exemple : 476 minutes de Durée d'Indisponibilité totale pendant un Mois Contractuel

Au total 43 200 minutes dans un Mois Contractuel de 30 jours - 476 minutes de Durée d'Indisponibilité = 42 724 minutes <hr style="width: 50%; margin: 0 auto;"/> Au total 43 200 minutes dans un Mois Contractuel de 30 jours	= 5 % de Crédit de Disponibilité pour 98,9 % de disponibilité pendant le Mois Contractuel
---	--

### 3.4 Autres informations relatives à ce SLA

Ce SLA n'est fourni qu'aux clients d'IBM et ne s'applique pas aux réclamations des utilisateurs, invités, participants et invités autorisés du Client concernant le Service Cloud ou à tout service bêta ou d'essai fourni par IBM. Le SLA ne s'applique qu'aux Services Cloud destinés à la production. Il ne s'applique pas aux environnements hors production, y compris et de façon non limitative, aux environnements de test, de reprise après incident, d'assurance qualité ou de développement.

## 4. Autorisation d'Utilisation et Informations de Facturation

### 4.1 Unités de Mesure des Prix

Les Services Cloud sont mis à disposition en fonction d'une des unités de mesure de redevance suivantes indiquées dans le Bon de Commande :

- a. Instance : unité de mesure par laquelle le Service Cloud peut être acquis. Une Instance est l'accès à une configuration spécifique du Service Cloud. Des Droits d'Utilisation suffisants doivent être obtenus pour chaque instance du Service Cloud mise à disposition à des fins d'accès et d'utilisation pendant la période de mesure indiquée dans le Bon de commande.
- b. Utilisateur Autorisé : unité de mesure par laquelle le Service Cloud peut être acquis. Un Utilisateur Autorisé est un individu unique qui a le droit d'accéder au Service Cloud. Le Client doit se procurer des autorisations distinctes et dédiées pour chaque Utilisateur Autorisé accédant à l'offre de Services Cloud directement ou indirectement (par exemple, via un logiciel de multiplexage, un périphérique ou un serveur d'applications), par quelque moyen que ce soit, pendant la période de mesure indiquée dans le Bon de commande. L'autorisation d'un Utilisateur Autorisé est unique et ne peut être partagée ni réaffectée à d'autres fins que le transfert définitif de l'autorisation d'un Utilisateur Autorisé à un autre individu. Le Service Cloud permet au Client de proposer un accès aux utilisateurs en dehors de son Entreprise. Ces utilisateurs sont considérés comme des Utilisateurs Autorisés et doivent posséder les autorisations appropriées.
- c. Engagement : unité de mesure par laquelle les services peuvent être acquis. Un Engagement comprend des services professionnels et/ou de formation relatifs au Service Cloud. Des droits suffisants sont nécessaires pour couvrir chaque Engagement.

### 4.2 Redevances et Facturation

Le montant à régler pour le Service Cloud est indiqué dans un Bon de commande.

### 4.3 Redevances de Configuration

Les frais de configuration seront indiqués dans un Bon de commande.

### 4.4 Redevances Mensuelles Partielles

La redevance mensuelle partielle est un tarif journalier au prorata. Les redevances mensuelles partielles sont calculées sur la base des jours restants du mois partiel à compter de la date à laquelle le Client est informé par IBM que son accès au Service Cloud est disponible.

### 4.5 Redevances des options à la demande

Les options On-Demand incluses dans le Bon de Commande ne seront pas facturées au Client tant que celui-ci ne demande pas l'activation du composant On-Demand. Une fois ce dernier activé, le Client sera facturé au prix indiqué dans le Bon de Commande.

## 5. Durée et options de renouvellement

### 5.1 Durée

La durée du Service Cloud commence à la date à laquelle IBM notifie au Client que ce dernier a accès au Service Cloud décrit dans le Bon de Commande. La partie PoE ou le Bon de Commande confirmera la date exacte de début et de fin de la durée. Le Client est autorisé à augmenter son niveau d'utilisation du Service Cloud pendant la durée en contactant IBM ou le Partenaire Commercial IBM du Client. IBM confirmera dans le Bon de Commande le niveau d'utilisation accru.

### 5.2 Options de renouvellement de la Durée des Services Cloud

Le Bon de commande du Client indiquera si le Service Cloud sera renouvelé à la fin de la durée, en désignant la durée par l'une des options suivantes :

#### 5.2.1 Renouvellement Automatique

Si le Bon de commande du Client indique que le renouvellement est automatique, le Client est autorisé, moyennant une demande écrite, à résilier la durée du Service Cloud arrivant à expiration, au moins quatre-vingt-dix (90) jours avant la date d'expiration de la durée stipulée dans le Bon de commande. Si IBM ou le Partenaire Commercial IBM du Client ne reçoit pas ladite notification de résiliation avant la date d'expiration, la durée arrivant à expiration sera automatiquement renouvelée pour une durée d'un an ou pour la même durée que celle d'origine, telle qu'elle est stipulée dans l'Autorisation d'Utilisation.

#### 5.2.2 Facturation Continue

Lorsque le Bon de Commande indique que la facturation du Client est continue, le Client continuera à avoir accès au Service Cloud à l'issue de sa période d'abonnement et sera facturé en continu pour l'utilisation du Service Cloud. Pour cesser d'utiliser le Service Cloud et mettre fin au processus de facturation continue, le Client doit fournir à IBM ou à son Partenaire Commercial IBM une notification écrite de quatre-vingt-dix (90) jours demandant l'annulation de son Service Cloud. Une fois l'accès du Client annulé, le Client sera facturé pour toutes les redevances d'accès impayées jusqu'au mois au cours duquel l'annulation a pris effet.

#### 5.2.3 Renouvellement requis

Lorsque le Bon de Commande indique que le renouvellement du Client est de type « résiliation », le Service Cloud sera résilié à la fin de la durée et l'accès du Client au Service Cloud sera supprimé. Pour continuer d'utiliser le Service Cloud au-delà de la date de fin, le Client doit passer une commande auprès de son ingénieur commercial IBM ou Partenaire Commercial IBM pour acheter une nouvelle période d'abonnement.

## 6. Support Technique

Le support technique du Service Cloud est disponible pendant la période d'abonnement.

**Les horaires de disponibilité du service d'assistance par téléphone et par e-mail sont les suivants :**

Ticket de Support ou E-Mail : A tout moment, les tickets sont traités conformément aux niveaux de gravité attribués. Les niveaux de gravité entre 2 et 4 seront traités pendant les heures ouvrables.

Numéro de téléphone : de 9 heures à 17 heures du lundi au vendredi (sauf jours fériés respectés par la société IBM).

**Assistance après les horaires de travail :**

Le service d'Assistance Après les Horaires de Travail (hors des horaires de travail normaux indiqués ci-dessus) n'est disponible que pour les problèmes de gravité 1 pendant les jours ouvrables, les week-ends et les jours fériés.

**Numéro d'urgence du service d'assistance aux Etats-Unis : 1-877-465-5444.**

**E-mail :** [vsupport@ca.ibm.com](mailto:vsupport@ca.ibm.com)

Pour consigner un ticket par e-mail, les clients doivent utiliser l'adresse Varicent/IBM provisoire.

**Portail Web de support :** <http://support.varicent.com>

Voir le lien ci-dessous vers le guide de support technique : <http://www-1.ibm.com/software/analytics/varicent/customercenter/saas.html>.

Niveau de gravité	Définition de la gravité	Objectifs de temps de réponse	Couverture de temps de réponse
1	<b>Impact critique sur les activités/indisponibilité du service :</b> Une fonctionnalité critique est inutilisable ou une interface critique est défaillante. Cela s'applique généralement à un environnement de production et indique l'impossibilité d'accès aux services, ce qui donne lieu à un impact critique sur les opérations. Cette condition nécessite une solution immédiate.	Sous 1 heure	24 heures sur 24 et 7 jours sur 7
2	<b>Impact significatif sur les activités :</b> L'utilisation d'un dispositif ou d'une fonction du service est gravement restreinte ou le Client risque de ne pas respecter des délais.	Sous 2 heures ouvrables	Heures ouvrables du lundi au vendredi
3	<b>Impact mineur sur les activités :</b> Indique que le service ou la fonctionnalité est utilisable et qu'il ne s'agit pas d'un impact critique sur les opérations.	Sous quatre heures ouvrables	Heures ouvrables du lundi au vendredi
4	<b>Impact minime sur les activités :</b> Une demande d'information ou une demande non technique	Sous 1 jour ouvrable	Heures ouvrables du lundi au vendredi

## 7. Conformité Safe Harbor

IBM n'a pas déterminé la conformité de ce Service Cloud aux normes américano-européennes et américano-suisse « US-EU » et « US-Swiss » Safe Harbor Frameworks.

## 8. Informations supplémentaires

### 8.1 Sites Bénéficiaires Dérivés

Le cas échéant, les taxes sont fonction du(es) site(s) que le Client identifie comme bénéficiant des Services Cloud. IBM appliquera les taxes en fonction de l'adresse professionnelle indiquée lors de la commande d'un Service Cloud comme étant le site bénéficiaire principal, sauf si le Client fournit des informations supplémentaires à IBM. Le Client est responsable de la mise à jour de ces informations et est tenu de fournir les éventuelles informations à IBM.

### 8.2 Informations Personnelles sur la Santé Interdites

Le Service Cloud n'est pas conçu pour être conforme à la loi HIPAA et ne doit pas être utilisé pour la transmission et le stockage des informations personnelles sur la santé.

### 8.3 Cookies

Le Client reconnaît et accepte qu'IBM pourra, dans le cadre du fonctionnement et du support normaux du Service Cloud, collecter des informations personnelles auprès du Client (employés et sous-traitants du Client) liées à l'utilisation du Service Cloud, par le biais de processus de suivi et d'autres technologies. Cela permet à IBM de rassembler des statistiques et informations d'utilisation relatives à l'efficacité du Service Cloud pour améliorer l'acquis utilisateur et/ou personnaliser les interactions avec le Client. Le Client confirme qu'il obtiendra ou a obtenu l'accord permettant à IBM de traiter les informations personnelles collectées pour le but susmentionné chez IBM, d'autres sociétés d'IBM et leurs sous-traitants, quel que soit l'endroit où IBM et ses sous-traitants exercent leurs activités, conformément à la loi applicable. IBM se conformera aux demandes des employés et sous-traitants du Client pour l'accès, la mise à jour, la correction ou la suppression de leurs informations personnelles collectées.

### 8.4 Reprise après Incident et Sauvegarde de Contenu

Ce Service Cloud comprend également les services de reprise après incident et de sauvegarde de contenu suivants :

Dans l'hypothèse où se produirait un événement défini comme un événement de « Force Majeure », tel que catastrophe naturelle, acte de terrorisme, mouvement social, incendie, inondation, tremblement de terre, émeute, guerre, mesures gouvernementales, ordonnances de restriction, virus, attaque par saturation et toute autre action malveillante, incident de connectivité des utilitaires ou du réseau ou toute

autre cause pouvant induire une indisponibilité du Service Cloud échappant au contrôle raisonnable d'IBM, IBM s'efforcera de restaurer l'accès du Client au Service Cloud comme suit :

- a. Option standard : IBM fournira les matériels, les logiciels et l'infrastructure réseau dans le réseau du centre de données d'IBM nécessaires pour permettre au Client d'accéder à nouveau au Service Cloud sous un délai de 14 jours.
- b. Option Premium : IBM fournira les matériels, les logiciels et l'infrastructure réseau dans le réseau du centre de données d'IBM nécessaires pour permettre au Client d'accéder à nouveau au Service Cloud sous un délai de 5 jours.

L'environnement sera restauré à partir de la dernière sauvegarde du Contenu, comme décrit ci-dessous, avec une perte limitée à 24 heures de Contenu sur le jeu de données du Contenu restauré.

Les sauvegardes sont réalisées quotidiennement et copiées sur un emplacement hors site dans l'hypothèse ou un événement de Force Majeure se produirait à l'emplacement principal. IBM conserve les sauvegardes en continu : tous les sept jours, une sauvegarde de base de données complète est réalisée et une sauvegarde différentielle comparative est effectuée chacun des jours suivants de la semaine. IBM conservera les sauvegardes différentielles quotidiennes des sept derniers jours et les quatre précédentes sauvegardes intégrales (couvrant une période de 28 jours d'activité). Lorsqu'une nouvelle sauvegarde intégrale est créée, l'ancienne version est supprimée. Les sauvegardes sont chiffrées lors du stockage sur un système d'archivage basé sur disques et durant les transmissions vers l'emplacement hors site.