

IBM QRadar on Cloud

Ce Descriptif de Services détaille le Service Cloud qu'IBM fournit au Client. Le terme « Client » signifie la partie contractante et des destinataires et utilisateurs autorisés du Service Cloud. Le Devis et l'Autorisation d'Utilisation sont fournis séparément sous la forme de Documents de Transaction.

1. Service Cloud

1.1 IBM QRadar on Cloud 100 EPS

L'Offre IBM QRadar on Cloud fournit une solution de sécurité interne avancée à partir de l'IBM Cloud basé sur le produit IBM Security QRadar SIEM. Elle permet aux Clients de collecter, de corrélérer et de stocker les événements générés à partir des environnements Cloud et sur site et de gérer la sécurité et les menaces comme ils le feraient avec un produit QRadar SIEM déployé sur site. Dans le cadre de l'offre, IBM assure également la surveillance de l'infrastructure 24 heures sur 24 et 7 jours sur 7 et applique le dernier niveau de logiciel ou les correctifs critiques chaque fois qu'ils sont disponibles.

Le présent Service Cloud inclut quatre vingt dix (90) jours de stockage actif et consultable.

1.2 Modules ou services facultatifs

1.2.1 IBM QRadar on Cloud 1K EPS Temporary Upgrade

Cette offre est une mise à niveau de service qui fournit une capacité supplémentaire de 1000 EPS pour la collecte et le traitement des événements de journal, mais uniquement pour un nombre provisoire de mois. Le Client peut acheter plusieurs unités de cette mise à niveau, à concurrence du niveau EPS maximum pouvant être pris en charge par l'offre. Cette partie a pour objectif de permettre à un Client qui nécessite une couverture pendant les périodes de pointe durant l'année de répondre à ces exigences par le biais d'une mise à niveau de capacité temporaire. A l'issue de la période, ces augmentations de capacité temporaires seront supprimées de l'environnement du Client.

1.2.2 IBM QRadar on Cloud Data Capacity 100 EPS

Un stockage supplémentaire ainsi qu'une extension de la période d'analyse sont ajoutés après la mise à jour des capacités des données. La mise à niveau de la capacité fournit aux clients jusqu'à 1 année complète de données stockées pour chaque mise à niveau de 100 EPS achetée.

1.2.3 IBM QRadar on Cloud Flows Add-On

S'intègre à IBM QRadar SIEM et aux processeurs de flux pour permettre la visibilité des réseaux de la couche 7 et des analyses de flux aidant le Client à détecter les activités sur son réseau et à y réagir.

1.2.4 IBM QRadar on Cloud Vulnerability Management Add-On

Permet la détection proactive des vulnérabilités de sécurité d'application et de périphérique réseau, afin d'ajouter du contexte et de prendre en charge la hiérarchisation des activités de remise en état et d'atténuation.

1.2.5 IBM QRadar on Cloud Log Archival

Permet au Client d'archiver les données d'événement à partir du Service Cloud pendant la période souscrite. IBM collaborera avec le Client pour inscrire les événements désignés dans le stockage d'objets à des fins d'archivage. Sur demande du Client, IBM remontera jusqu'à trente (30) jours de données d'événement archivés du Service Cloud dans un délai de trois (3) jours ouvrables après ladite requête. Le Client pourra consulter lesdites données pendant 48 heures avant qu'elles ne soient renvoyées vers le stockage d'objets d'archives. Le Client peut effectuer jusqu'à deux requêtes tous les trois mois. La mise à niveau de la capacité fournit aux Clients jusqu'à 1 année complète de données stockées pour chaque mise à niveau de 100 EPS achetée.

1.2.6 IBM QRadar on Cloud Optimization Service

Pour ce service d'abonnement à distance, IBM organisera une réunion d'examen avec le Client afin de vérifier l'état actuel du Service Cloud et de fournir des résultats au Client via un rapport QRadar on Cloud Health Status, ce qui permettra d'identifier les points à améliorer, le cas échéant.

En outre, IBM fournira au Client, s'il le demande, les services de consultation suivants, jusqu'à huit (8) jours pendant une période d'un an:

- aider à l'ajout de sources de journal additionnelles au Service Cloud ;
- configurer des recherches, des rapports et des tableaux de bord additionnels ;
- réaliser un réglage additionnel sur le déploiement QRadar existant ;
- fournir un transfert de connaissances sur les sujets QRadar pertinents.

1.3 Services de Configuration

Les services de configuration suivants sont réalisés à distance et doivent être commandés séparément. Chaque service commandé expire quatre vingt dix (90) jours après l'achat, sauf indiqué autrement, quel que soit le nombre d'heures utilisées (le cas échéant). Les services comprennent un responsable d'engagement IBM désigné qui programmera et prendra les appels.

1.3.1 IBM QRadar on Cloud Deployment Service

Ce service propose quarante (40) jours de services professionnels pendant lesquels IBM réalisera certaines des tâches suivantes:

IBM réalisera un examen de l'architecture SIEM qui pourra durer jusqu'à seize heures afin de définir les exigences de rapport du Client. IBM communiquera ses conclusions au Client dans un rapport de l'architecture de solution qui aidera à définir et à stocker les exigences du Client.

Ce rapport contiendra:

- les exigences définies par le Client pour être conforme, les exigences en matière de renseignement de sécurité et de vérification.
- les exigences en matière de renseignement de sécurité, les cas d'utilisation et les applications qu'IBM peut assister pour la mise en place (jusqu'à dix (10) cas d'utilisation et deux (2) applications).
- les informations de haut niveau sur le journal du Client et les sources de flux qui nécessitent la prise en charge des cas d'utilisation.
- les études de l'infrastructure du réseau, tels que les pare-feux et les ports.

En fonction du rapport de l'architecture de la solution et si le temps restant le permet, IBM réalisera les tâches suivantes :

- la configuration de l'ensemble des événements pour trois (3) instances maximum des dix (10) types de source du journal maximum dans le Service Cloud. Cette activité inclura le transfert des connaissances vers le personnel approprié du Client afin qu'il puisse ajouter plus de sources de journal que nécessaires. Seules les sources de journal prises en charge par QRadar Device Support Modules (DSM) feront partie de ce service.
- Réglage initial qui inclut a) l'activation des règles prêtes à l'emploi, les recherches sauvegardées, les graphiques et les rapports de séries temporelles accumulés ; b) l'identification et la suppression des sources de bruit et c) la configuration du stockage hors ligne via NFS, CIFS ou iSCSI.
- mise en place des dix (10) cas d'utilisation et des deux (2) applications à partir d'IBM QRadar App Exchange établis dans le document d'architecture de solution.

1.3.2 IBM QRadar on Cloud Custom Service

Le présent service proposera le développement d'un analyseur/uDSM unique et personnalisé pour la prise en charge des types de source de journal par défaut du Client qui doivent être envoyés au Service Cloud et qui doivent comprendre les tâches suivantes:

- création d'un analyseur personnalisé pour un type de source de journal non-standard (tâche effectuée à distance) ;
- création, configuration et cartographie d'uDSM ;
- déploiement et test d'uDSM personnalisé ; et
- analyse de vingt cinq types de messages maximum pour la source de journal.

2. Protection du Contenu et des Données

La Fiche Technique relative au Traitement et à la Protection des données (« Fiche Technique ») contient des informations spécifiques au Service Cloud concernant le type de Contenu autorisé à être traité, les activités de traitement impliquées, les dispositifs de protection des données et les détails de conservation et de retour de Contenu. Les détails ou clarifications et dispositions, y compris les responsabilités du Client, concernant l'utilisation du Service Cloud et les dispositifs de protection de données, le cas échéant, sont énoncés dans la présente clause. Plusieurs Fiches Techniques peuvent être applicables à l'utilisation du Service Cloud par le Client, en fonction des options sélectionnées par le Client. La Fiche Technique n'est disponible qu'en anglais. Elle n'est pas disponible dans la langue locale. En dépit des pratiques des lois ou coutumes locales, les parties attestent qu'elles comprennent l'anglais qui est une langue appropriée pour l'acquisition et l'utilisation des Services Cloud. La ou les Fiches Techniques ci-dessous s'appliquent au Service Cloud et ses options disponibles. Le Client accepte i) qu'IBM peut, à son entière discrétion, modifier de temps en temps la Fiche Technique et ii) que de telles modifications remplaceront les versions précédentes. Les modifications apportées à la Fiche Technique auront pour objectif i) d'améliorer ou de clarifier les engagements existants ii) de conserver la conformité aux normes actuelles et aux lois applicables ou iii) de fournir des engagements supplémentaires. La sécurité du service Cloud ne sera en aucun cas affectée par les modifications apportées à la Fiche Technique.

Lien(s) vers la ou les Fiches Techniques applicables :

<https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=FB0F42F0750011E6865BC3F213DB63F7>

Le Client est tenu de prendre les mesures nécessaires pour commander, activer ou utiliser les dispositifs de protection de données disponibles pour un Service Cloud et reconnaît être responsable de l'utilisation des Services Cloud si le Client ne parvient pas à prendre lesdites mesures, notamment à se conformer à toute obligation de protection de données ou autre exigence légale relative au Contenu.

L'Addendum d'IBM relatif au Traitement de Données à caractère Personnel, disponible sur <http://ibm.com/dpa> (DPA), et la ou les Annexe(s) DPA s'appliquent et sont référencés dans le Contrat, si et dans la mesure où le Règlement Général Européen sur la Protection des Données (EU/2016/679) (RGPD) s'applique aux Données à caractère personnel figurant dans le Contenu. La ou les Fiches Techniques applicables pour ce Service Cloud constitueront la ou les Annexes DPA. Si le DPA s'applique, l'obligation d'IBM d'informer les Sous-traitants ultérieurs des modifications et le droit du Client à s'opposer à de telles modifications s'appliquent comme défini dans le DPA.

3. Accord Relatif aux Niveaux 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, comme indiqué dans une Autorisation d'Utilisation. Le SLA ne constitue pas une garantie. Il n'est disponible que pour le Client et ne peut être utilisé que dans les environnements de production.

3.1 Crédits de Disponibilité

Le Client doit consigner un ticket de support de Gravité 1 auprès du centre d'assistance technique IBM dans les 24 heures suivant la première fois où le Client a eu connaissance d'un impact critique sur les activités et de l'indisponibilité du Service Cloud. Le Client doit raisonnablement aider IBM dans le cadre du diagnostic et de la résolution des problèmes.

Une demande de ticket de support pour non-respect d'un SLA doit être soumise dans les trois jours ouvrables suivant la fin du mois contractuel. Le dédommagement relatif à une réclamation de SLA valide sera un avoir sur une future facture du Service Cloud en fonction de la période de temps pendant laquelle le traitement du système de production pour le Service Cloud n'est pas disponible (« Durée d'Indisponibilité »). La Durée d'Indisponibilité est calculée depuis le moment où le Client signale l'événement jusqu'au moment où le Service Cloud est restauré ; elle ne comprend pas les périodes d'indisponibilité pour les raisons suivantes : indisponibilité de maintenance programmée ou annoncée, causes échappant au contrôle d'IBM, incidents liés au contenu, à la technologie, aux conceptions ou aux instructions du Client ou d'un tiers, plateformes et configurations système non prises en charge ou autres erreurs du Client, incident de sécurité du fait du Client ou test de sécurité mené par le Client. IBM appliquera le dédommagement correspondant le plus élevé, en fonction de la disponibilité cumulée du Service Cloud pendant chaque mois contractuel, comme indiqué dans le tableau ci-dessous. Le

dédommagement total relatif à tout mois contractuel ne pourra pas dépasser dix (10 %) d'un douzième (1/12ème) de la redevance annuelle du Service Cloud.

3.2 Niveaux de Service

Disponibilité du Service Cloud pendant un mois contractuel

Disponibilité pendant un mois contractuel	Indemnisation (% de redevance d'abonnement mensuelle* pour le mois contractuel objet d'une réclamation)
Inférieure à 99,9 %	2 %
Inférieure à 99 %	5 %
Inférieure à 95 %	10 %

* Si le Service Cloud a été acquis auprès d'un Partenaire Commercial IBM, la redevance d'abonnement mensuelle sera calculée sur le prix en vigueur à ce moment-là pour le Service Cloud concerné pendant le mois contractuel qui fait l'objet d'une réclamation, avec une réduction de cinquante pour cent (50 %). IBM accordera une remise directement au Client.

La disponibilité, exprimée en pourcentage, est calculée comme suit : le nombre total de minutes d'un mois contractuel moins le nombre total de minutes de la Durée d'Indisponibilité au cours d'un mois contractuel, divisé par le nombre total de minutes d'un mois contractuel.

4. Support Technique

Le support technique destiné au Service Cloud est fourni par e-mail, sur les forums en ligne et par le biais d'un système de notification de problème en ligne. Le guide de support Software as a Service (SaaS) d'IBM, disponible en ligne à l'adresse https://www-01.ibm.com/software/support/saas_support_guide.html contient les coordonnées des personnes à contacter ainsi que des informations et processus relatifs au support technique. Le support technique est offert avec le Service Cloud et n'est pas disponible en tant qu'offre distincte.

5. Droits d'Utilisation et Informations de Facturation

5.1 Unités de mesure des redevances

Le Service Cloud est disponible en fonction des unités de mesure de redevance indiquées dans le Document de Transaction :

- 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 d'Utilisation suffisants sont nécessaires pour couvrir chaque Engagement.
- Evénements par Seconde (EPS) est une unité de mesure par laquelle l'Offre Cloud Service peut être acquise. Un Evénement est une occurrence d'un événement caractéristique, qui est traitée par ou relative à l'utilisation du Service Cloud. Des Droits d'Utilisation suffisants doivent être obtenus pour couvrir le nombre d'Evénements par seconde à collecter et à traiter par le Service Cloud pendant la période de mesure indiquée dans l'Autorisation d'Utilisation (« PoE ») ou le Document de Transaction du Client.
- Dix Mille Flux par Minute est une unité de mesure par laquelle le Service Cloud peut être acquis. Un Flux est un enregistrement de communications entre deux hôtes. Tous les paquets contenant les mêmes IP source, IP de destination, port source, port de destination et protocole sont combinés pour former un enregistrement de Flux. Des droits d'utilisation suffisants sont nécessaires pour couvrir le nombre maximal de Flux dans un intervalle d'une minute, arrondi à la Dizaine de Milliers près, gérés ou traités par le Service Cloud pendant la période de mesure indiquée dans l'Autorisation d'Utilisation (« PoE ») ou le Document de Transaction du Client.
- 256 Ressources est une unité de mesure par laquelle le Service Cloud peut être acquis. Un Actif correspond à toute ressource matérielle ou à tout élément de valeur à gérer, y compris les équipements de production, les installations et le transport, ainsi que le matériel et les logiciels informatiques. Tout élément ou ressource ayant un identifiant unique dans le Service Cloud est un Actif distinct. Des Droits d'Utilisation suffisants sont nécessaires pour couvrir les Actifs, arrondis à 256 unités près, accessibles ou gérés par le Service Cloud pendant la période de mesure indiquée

dans l'Autorisation d'Utilisation (« PoE ») ou le Document de Transaction du Client. Chaque droit d'utilisation de 256 Actifs représente 256 Actifs.

5.2 Redevances de Configuration

Une redevance de configuration unique sera facturée au tarif indiqué dans le Document de Transaction pour chaque service de configuration commandé.

5.3 Fréquence de facturation

En fonction de la fréquence de facturation sélectionnée, IBM facturera au Client les redevances exigibles au début de la période de la fréquence de facturation, à l'exception des redevances dues pour dépassement et des frais d'utilisation qui seront facturés à terme échu.

6. Durée et Options de Renouvellement

La durée du Service Cloud commence à la date à laquelle IBM notifie au Client que ce dernier a accès au Service Cloud, comme décrit dans l'Autorisation d'Utilisation. L'Autorisation d'Utilisation indiquera si le Service Cloud est renouvelé automatiquement, s'il se poursuit en continu ou s'il prend fin à l'issue de la durée.

Pour un renouvellement automatique, le Service Cloud est automatiquement renouvelé pour la durée indiquée dans l'Autorisation d'Utilisation, sauf si le Client notifie par écrit, au moins 90 jours avant la date d'expiration de la durée, son intention de ne pas renouveler. Les renouvellements sont soumis à une augmentation de prix annuelle tel que spécifié dans le devis. En cas de renouvellement automatique à la suite d'une notification de retrait du Service Cloud de la part d'IBM, la durée de renouvellement prend fin au plus tôt à la fin de la durée de renouvellement actuelle ou à la date du retrait annoncé.

Pour une utilisation en continu, le Service Cloud continuera d'être disponible mois par mois jusqu'à ce que le Client notifie la résiliation moyennant un préavis écrit de 90 jours. Le Service Cloud demeure disponible jusqu'à la fin du mois suivant ladite période de 90 jours.

7. Dispositions Additionnelles

7.1 Dispositions générales

Le Client ne pourra pas utiliser les Services Cloud, seuls ou conjointement avec d'autres services ou produits, à l'appui de l'une quelconque des activités à haut risque suivantes : conception, construction, contrôle ou maintenance d'installations nucléaires, de systèmes de transport en commun, de systèmes de contrôle du trafic aérien, de systèmes de contrôle automobiles, de systèmes d'armement, de systèmes de navigation ou de communication aériennes ou toute autre activité où toute défaillance du Service Cloud pourrait entraîner un risque matériel de mort ou de blessures corporelles graves.

7.2 Logiciels d'Activation

Ce Service Cloud comprend des logiciels d'activation, qui ne doivent être utilisés qu'en rapport avec l'utilisation du Service Cloud par le Client et uniquement pendant la durée du Service Cloud. Si les logiciels d'activation sont accompagnés d'un contrat de licence distinct, la durée dudit contrat de licence est également applicable, dans les limites stipulées dans la présente Clause. Dans le cas d'un conflit, les dispositions du présent Descriptif de Services prévalent sur ledit contrat de licence qui accompagne les logiciels d'activation. Le logiciel d'activation est fourni « EN L'ETAT ». Le Client n'est autorisé à installer et utiliser qu'un maximum de 10 copies des Logiciels d'Activation.

7.3 Données sécurisées

IBM peut collecter des indicateurs d'activités potentiellement malveillantes dans le Contenu du Client à des fins d'utilisation dans des contextes d'intelligence des cybermenaces, notamment des URL, des adresses IP, des domaines ainsi que des hachages de fichiers. IBM peut, en retour, avertir le Client si ces indicateurs révèlent un risque de cybermenace élevé pour le Client.