

IBM QRadar on Cloud

Ce Descriptif de Services détaille le Service Cloud. Les bons de commande applicables contiennent les prix et des détails supplémentaires concernant la commande du Client.

1. Service Cloud

1.1 Offres

Le Client peut faire son choix parmi les offres disponibles ci-dessous.

1.1.1 IBM QRadar on Cloud

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 et est autorisé par lots de 100 Événements par seconde (EPS).

1.2 Services Optionnels

1.2.1 IBM QRadar on Cloud Temporary Upgrade

Cette offre est une mise à niveau de service qui fournit une capacité supplémentaire de 1 000 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. À 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

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 capacité fournit aux Clients jusqu'à 1 année complète de données d'événement 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.

Le présent Service Cloud inclut quatre-vingt-dix (90) jours de stockage actif et consultable et est autorisé par lots de 10 000 Flux par minute (FPM).

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 Flows Add-On Data Capacity

Un stockage supplémentaire ainsi qu'une extension de la période d'analyse sont ajoutés après la mise à jour des capacités des données en fournissant au Client jusqu'à 1 année complète de données de flux stockées pour chaque mise à niveau de 10 000 FPM achetée.

1.2.7 IBM QRadar on Cloud Flows Add-On Log Archival

Cette offre permet aux Clients d'archiver les données de flux à partir du Service Cloud pendant la période souscrite. IBM collaborera avec le Client pour inscrire les enregistrements de flux désignés dans le stockage d'objets à des fins d'archivage. Sur demande du Client, IBM remontera jusqu'à trente (30) jours de données de flux archivés vers l'instance du Service Cloud du Client 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 10 000 FPM achetée.

1.2.8 IBM QRadar on Cloud for Non-Production Environment

L'offre IBM QRadar on Cloud for Non-Production Environment fournit une instance de test dédiée du Service Cloud. 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 un environnement de test dédié. 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 Client ne pourra utiliser ce Service Cloud qu'à des fins de test hors production.

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

1.3 Services d'Accélération

1.3.1 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 ; et
- fournir un transfert de connaissances sur les sujets QRadar pertinents.

1.3.2 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.

a. IBM QRadar on Cloud Deployment Services

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 ; et
- les études de l'infrastructure du réseau, tels que les firewalls 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.

b. **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. **Fiches Techniques sur le Traitement et la Protection des Données**

L'Addendum d'IBM relatif au Traitement de Données à caractère personnel, disponible sur <http://ibm.com/dpa> (DPA) et la ou les Fiches Techniques (désignées par fiche(s) technique(s) ou Annexe(s) DPA) dans les liens ci-dessous contiennent des informations additionnelles sur la protection des données pour les Services Cloud et leurs options concernant les types de Contenus pouvant être traités, les activités de traitement impliquées, les dispositifs de protection des données et les détails de conservation et de retour de Contenu. Le DPA s'applique aux Données à caractère personnel du Contenu dans la mesure où i) Le Règlement Général Européen sur la Protection des Données (UE/2016/679) (RGPD) ; ou ii) d'autres lois relatives à la protection des données identifiées sur <http://www.ibm.com/dpa/dpl> s'appliquent.

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

3. **Niveaux de Service et Support Technique**

3.1 **Accord Relatif aux Niveaux de Service**

IBM fournit au Client l'Accord relatif aux Niveaux de Service (« SLA ») de disponibilité ci-dessous. IBM appliquera le dédommagement correspondant le plus élevé, en fonction de la disponibilité cumulée du Service Cloud, comme indiqué dans le tableau ci-dessous. Le pourcentage de disponibilité est calculé comme suit : le nombre total de minutes d'un mois contractuel moins le nombre total de minutes d'indisponibilité du Service au cours du mois contractuel, divisé par le nombre total de minutes du mois contractuel. La définition de l'indisponibilité du Service, la procédure de réclamation et les moyens de contacter IBM concernant les problèmes de disponibilité de service figurent dans le guide de support de Services Cloud d'IBM à l'adresse https://www.ibm.com/software/support/saas_support_overview.html.

Disponibilité	Avoir (% de redevance d'abonnement mensuelle*)
Inférieure à 99,9 %	2 %
Inférieure à 99,0 %	5 %
Inférieure à 95,0 %	10 %

* La redevance d'abonnement est le prix contractuel pour le mois objet de la réclamation.

3.2 Support Technique

Le support technique destiné au Service Cloud, y compris les coordonnées des personnes à contacter, les niveaux de gravité, les heures de disponibilité, les temps de réponse ainsi que d'autres informations et processus relatifs au support technique sont disponibles en sélectionnant le Service Cloud dans le guide de support IBM disponible à l'adresse <https://www.ibm.com/support/home/pages/support-guide/>.

4. Montant des Redevances

4.1 Unités de mesure des redevances

Les unités de mesure des redevances du Service Cloud sont indiquées dans le Document de Transaction.

Les unités de redevances suivantes s'appliquent à ce Service Cloud :

- Un Engagement est un service professionnel ou de formation relatif aux Services Cloud.
- Les Evénements par seconde correspondent au nombre d'occurrences d'un événement caractéristique par seconde, qui est traité par ou relatif à l'utilisation des Services Cloud.
- Les Flux par minute correspondent au nombre de flux par minute gérés ou traités par les Services Cloud. Un Flux est un enregistrement de communications entre deux hôtes. Les paquets contenant les mêmes IP source, IP de destination, port source, port de destination et protocole sont combinés pour former un seul enregistrement de Flux.
- Un Actif correspond à une ressource ou un élément de valeur tangible identifié de manière unique qui doit être accessible aux Services Cloud ou gérés par ces derniers.

5. Dispositions Additionnelles

Pour les Contrats de Services Cloud (ou des contrats Cloud de base équivalents) signés avant le 1er janvier 2019, les dispositions énoncées à l'adresse <https://www.ibm.com/acs> s'appliquent.

5.1 Logiciels d'Activation

Le Service Cloud contient le Logiciel d'Activation suivant :

Logiciel d'Activation	Dispositions de licence applicables (le cas échéant)
Data Gateway	Le Client n'est autorisé à installer et utiliser qu'un maximum de dix (10) copies de Data Gateway.

6. Dispositions dérogatoires

6.1 Utilisation de Données

La disposition suivante prévaut sur toute disposition contraire dans la clause « Contenu et protection des données » des conditions cadre de Service Cloud entre les parties : IBM n'utilisera ou ne communiquera pas les résultats découlant de l'utilisation du Service Cloud par le Client qui sont exclusivement liés au Contenu (Observations) du Client ou qui identifient le Client de quelque autre manière. IBM utilisera cependant le Contenu et d'autres informations issues du Contenu (à l'exception des analyses) dans le cadre du Service Cloud en vue d'améliorer le Service Cloud. IBM peut également partager des identificateurs de menaces et d'autres informations de sécurité intégrées au Contenu à des fins de détection des menaces et de protection.