

Descriptif de Service

Managed RDS

Table des matières

[1 Définitions 2](#_Toc134204829)

[2 Objet 2](#_Toc134204830)

[3 Présentation du Service 2](#_Toc134204831)

[4 Fonctionnalités 2](#_Toc134204832)

[4.1 Collection RDS 3](#_Toc134204833)

[4.2 Remote Desktop Session Host (RDSH) 3](#_Toc134204834)

[4.3 Remote Desktop Connection Broker (RDCB) 4](#_Toc134204835)

[4.4 Remote Desktop Web Access (RDWEB) 4](#_Toc134204836)

[4.5 Remote Desktop Licence Server (RDLIC) 4](#_Toc134204837)

[4.6 Remote Desktop Gateway (RDGTW) 4](#_Toc134204838)

[4.7 Certificats SSL 4](#_Toc134204839)

[5 Architecture 4](#_Toc134204840)

[6 Services optionnels 5](#_Toc134204841)

[6.1 User Profile Disk (UPD) 5](#_Toc134204842)

[7 Conditions de prix 5](#_Toc134204843)

[7.1 Prix 5](#_Toc134204844)

[8 Accès au Service 5](#_Toc134204845)

[8.1 Prérequis 5](#_Toc134204846)

[8.2 Mise en service 6](#_Toc134204847)

[8.3 Maintien en conditions opérationnelles 7](#_Toc134204848)

[9 Support 7](#_Toc134204849)

[9.1 Gestion des changements 7](#_Toc134204850)

[9.1.1 Demandes au catalogue 8](#_Toc134204851)

[9.1.2 Demandes hors catalogue 8](#_Toc134204852)

[10 Annexe1 8](#_Toc134204853)

Liste des figures

**Aucune entrée de table d'illustration n'a été trouvée.**

Liste des tableaux

**Aucune entrée de table d'illustration n'a été trouvée.**

# Définitions

En complément des définitions des Conditions Générales et des Conditions Spécifiques Intégration Maintenance et Prestations associées, les définitions spécifiques suivantes s’appliquent à ce Descriptif de Service.

**AD :** Active Directory (AD), est l’annuaire LDAP de Microsoft, présent sous forme de rôle, qui fournit une gestion de point d'accès unique et cohérente pour les utilisateurs, les applications et les périphériques. Toutes les données sont hiérarchiques, répliquées et extensibles.

# Objet

Le présent descriptif de service a pour objet de définir les conditions dans lesquelles Orange Business fournit le service «Managed RDS» (ci-après le « Service ») au Client.

Le présent descriptif est rattaché au document « Managed Applications – Descriptif de Service ».

# Présentation du Service

Dans le cadre de ce service, nous assurons la gestion de votre RDS hébergé sur une infrastructure Cloud Public IaaS de la liste ci-dessous.

Orange Business

* Cloud Avenue
* Flexible Engine

Partenaire

* AWS (prévu dans la roadmap)
* Microsoft Azure (prévu dans la roadmap)
* Google Cloud (prévu dans la roadmap)

Le « Managed RDS » s’appuie sur des services complémentaires :

* Un Managed AD
* Des certificats SSL de serveur autosignés ou délivrés par une autorité de certification reconnue

Les prérequis pour cette offre :

* Souscrire à une offre d’infrastructure IaaS pour l’hébergement du service RDS selon les recommandations d’Orange Business.
* Souscrire à l’offre OS Managé pour les VMs où sont hébergés les composants
* Souscrire à l’offre Managed AD pour l’AD nécessaire à la livraison du service RDS

# Fonctionnalités

Le schéma suivant illustre les fonctionnalités qui constituent le service.



* Collection RDS
* Remote Desktop Session Host
* Remote Desktop Connection Broker
* Remote Desktop Gateway
* Remote Desktop Web Access
* Remote Desktop License server

## Collection RDS

Une Collection RDS permet de regrouper les serveurs Hôtes de Session Bureau à distance (RDSH : Remote Desktop Session Host) en des fermes séparées (RDS Farm). Un serveur RDSH ne peut pas appartenir à 2 Collections à la fois.

La collection de sessions est uniquement supportée avec 2 types en fonction des ressources qui y sont publiées :

* Bureaux à distance
* Programmes RemoteApp

Ces 2 types de ressources ne peuvent être mélangés dans la même collection. Un serveur RDSH affecté à une Collection héberge soit des RemoteApp, soit des bureaux à distance mais pas les 2.

Pour une collection de sessions, on désigne :

* Les utilisateurs ou les groupes d’utilisateurs ayant accès à la collection.
* En option, un espace de stockage partagé dans lequel sont stockés les profils utilisateurs

## Remote Desktop Session Host (RDSH)

Les RDSH sont déployés sur des serveurs et ont pour rôle d’exécuter toutes les applications basées sur des sessions et de fournir des bureaux publiés aux utilisateurs. Les utilisateurs accèdent aux applications ou aux bureaux publiés en lançant des logiciels clients (mstsc) disponible sous Windows, MacOS, iOS ou Android. Cet accès peut aussi se faire via un navigateur supporté en utilisant le « web client ».

## Remote Desktop Connection Broker (RDCB)

Le RDCB a plusieurs rôles. Il permet d’équilibrer la charge entre les différents services publiés sur les serveurs RDSH. Il gère les reconnexions des utilisateurs pour retrouver leurs sessions de travail suite à une coupure réseau, par exemple. Il garde également une trace de chaque session utilisateur connectée à la ferme RDS dans une base de données. Parmi les informations stockées, on retrouve un identifiant de session par utilisateur, le nom d’utilisateur et le nom du serveur auquel ce dernier est connecté. En cas de reconnexion à une session, le RD Connection Broker redirigera l’utilisateur vers son ancienne session déjà existante.

## Remote Desktop Web Access (RDWEB)

Le RDWEB permet aux utilisateurs d’accéder à leurs bureaux distants et aux « Remote App » au travers d’un portail web apporté. Lorsqu’une application est publiée et qu’un utilisateur a eu l’autorisation de s’en servir, elle apparait dans sa page d’accueil du site Web après authentification. Ce composant s’appuie sur le composant « Internet Information Services (IIS) ».

Le protocole HTTPS est utilisé entre les clients et le RDWEB offrant ainsi un canal chiffré de communication. Des certificats SSL délivrés par une autorité de certification et reconnus par les postes client doivent être installés sur le serveur et les postes client. À des fins de développement et de test, il peut s'agir d'un certificat autogénéré et autosigné. Le nom du certificat doit correspondre au nom de domaine pleinement qualifié (FQDN) utilisé pour accéder au RDWEB Access. Les FQDN possibles comprennent le nom DNS externe pour l'adresse IP publique et l'enregistrement DNS CNAME pointant vers l'adresse IP publique.

Des machines virtuelles RDWEB supplémentaires peuvent être ajoutées à une ferme RD Web Access afin d'augmenter la disponibilité du service et de l'adapter à un plus grand nombre d'utilisateurs. Une ferme RDWEB Access avec plusieurs machines virtuelles est configurée avec un Load-Balancer externe.

## Remote Desktop Licence Server (RDLIC)

Le RDLIC permet aux utilisateurs de se connecter aux serveurs RD Session Host qui hébergent les bureaux et les applications publiées. Ce serveur de licence RDLIC une fois activé requiert l’installation de « Client Access Licence » de type « User » ou de « Client Access Licence » de type « Device ». Quel que soit le type de CAL requises, il faut installer autant de CAL que d’utilisateurs uniques ou que d’équipements uniques. Le nombre d’utilisateurs connectés en même temps n’est pas la valeur qui sert de base au dénombrement du nombre de CALs nécessaire.

## Remote Desktop Gateway (RDGTW)

Le RDGTW fournit une connexion sécurisée aux serveurs Windows, par l'intermédiaire du protocole RDP, auquel s'ajoute la connexion à la passerelle sécurisée par le protocole TLS

## Certificats SSL

Chaque serveur utilisé dans la solution RDS a un certificat numérique qui est utilisé pour mettre en œuvre le protocole SSL (Secure Sockets Layer) et prouver son identité aux clients. Les certificats par défaut sont des certificats auto-signés qui ne sont pas reconnus des clients. Il faut donc installer des certificats délivrés par une autorité de certification reconnue.

4 certificats sont utilisés pour le service RDS:

* RD Connection Broker – Publication
* RD Connection Broker - Activer l'authentification unique
* RD Accès Web
* RD Gateway

# Architecture

Le schéma suivant illustre l’architecture préconisée pour rendre le service RDS.



# Services optionnels

## User Profile Disk (UPD)

Le disque de profil utilisateur (UPD) permet de stocker le profil de chaque utilisateur des services Bureau à distance ( %USERPROFILE% ) dans un fichier VHDX (disque virtuel) distinct. Un tel disque de profil est connecté lorsque l'utilisateur se connecte à Windows et sera déconnecté lorsque l'utilisateur se déconnecte (les modifications apportées au profil étant enregistrées).

# Conditions de prix

## Prix

La tarification du Service est composée :

* Des frais d’accès au service « Managed RDS » intégrant toutes les tâches mentionnées dans le RACI d’implémentation et indexé sur le nombre de serveurs et de fonctionnalités à configurer.
* D’un récurrent mensuel couvrant les activités liées au maintien en condition opérationnelle du service « Managed RDS » indexé sur le nombre de fonctionnalités et de serveurs (minimum 2).

Les tarifs du Service n’incluent pas :

* Le prix de l’infrastructure que vous devez souscrire par ailleurs auprès du fournisseur de IaaS selon les tarifs en vigueur.
* Les demandes de changement.

# Accès au Service

## Prérequis

Le Service « Managed RDS » s’appuie sur un service de IaaS, auquel vous devez également souscrire selon nos recommandations et nous confier le Service « Managed OS » inhérent.

A noter, que le service IaaS correspondant à l’AD sera facturé dès sa mise en service, sans attendre la recette du services Managed RDS.

## Mise en service

Orange Business s’appuie sur un document SRF (Service Request Form) que vous devez remplir pour la mise en service.

Ce document a pour but de présenter les paramétrages standards que nous appliquons et de recueillir vos besoins (éléments variables) afin de finaliser l’architecture à déployer.

Ce document permet de recueillir des éléments concernant deux parties :

1. Architecture physique du service RDS
* Le nombre de VM minimum
* La localisation des VMs
* Le dimensionnement en vCPU, vRAM, disque de chaque VM
* Plan d’adressage
1. Les éléments logiques de la configuration du service.
* Le nom de chaque VM
* L’OS requis sur les serveurs des différentes fonctionnalités

Le tableau ci-dessous présente les tâches et responsabilités associées pour l’implémentation des services présentés au §4.

|  | Tâches | Orange Business | CLIENT |
| --- | --- | --- | --- |
| 1 | Fourniture des éléments de configuration variables dans la SRF | C | R |
| 2 | Construction et Présentation de la SRF | R |  |
| 3 | Validation de la SRF |  | R |
| Infrastructure |
| 4 | Fournir les FQDN suivants : RDCB = DNS « round robin name » du RDCBRDWEB = Nom porté par le Load-BalancerDécrire les tests de la recette fonctionnelle de fin de BUILD  | R | I |
| 5 | Déployer les rôles RDSH, RDCB, RDWEB, RDCLIConfigurer les certificats SSL d’une ferme RDSOuvrir les flux nécessaires entre les VMs, le LB et les utilisateurs | R |  |
| 6 | Déployer haute disponibilité pour RDCB, RDLIC et RDWEBConfigurer VIP HTTPS sur Load-Balancer et installer certificat | R |  |
| 7 | Configurer les Collections selon le design de la proposition ou le design du client | R |  |
| 8 | Installer les applications sur les RDSH en mode multi-user | I | R |
| 9 | Fournir les configurations (chemin du binaire et paramètres si applicable) des Publications des RemoteApp pour toutes les collections.  | I | R |
| 10 | Publier « calculatrice » en RemoteApp dans toutes les collections | R |  |
| 11 | Mise en place des sondes de supervision OS Managé sur l’ensemble des serveurs RDSMise en place des sondes avec test de vie sur les services Windows de RDS (hors applicatif), accessibilité du service HTTPS RDWEBMise en place des sondes sur le service SQL SE Mise en place des indicateurs techniques « OS Managé » sur l’ensemble de la ferme | R |  |
| 12 | Configuration de la sauvegarde, de la supervision et du stockage sécurisé des mots de passe | R |  |
| Remote App |
| 13 | Installer les applications sur les RDSH en mode multi-user | I | R |
| 14 | Publier les RemoteApp Helios du client suivant les configurations données par le client  | R | I |
| 15 | Recette fonctionnelle des tests fournis en entrée de BUILD | I | R |
| R : Réalisateur – A : Accountable (Responsable) – C : Consulté – I : Informé – V : Valideur |

Les critères d’acceptance de la mise en service de l’Infrastructure :

* Publication de la « calculatrice » en RemoteApp
* Tests concluants pour les collections témoins.

Les critères d’acceptance de la mise en service de l’Infrastructure :

* Tests fonctionnels concluants.

## Maintien en conditions opérationnelles

Nous assurons les opérations pour le maintien en conditions opérationnelles du RDS en complément des OS requis pour rendre le service.

Les dispositions prises dans le cadre de cette activité peuvent être de nature préventive ou curative.

Le tableau ci-dessous présente les tâches et responsabilités associées pour l’exploitation des services présentés au §4.

|  | Tâches | Orange | CLIENT |
| --- | --- | --- | --- |
| 1 | MCO des fonctionnalités du service RDS | R |  |
| 2 | Sauvegarde (décrite dans le paragraphe qui suit) | R |  |
| 3 | Expression de besoin pour toute demande hors catalogue | C,I | R |
| 4 | Evolution de l’architecture physique et logique du service RDS | R | C,I |
| 5 | Signaler toute évolution des besoins du service RDS afin d’ajuster le gabarit des VMs  | C,I | R |
| 6 | Supervision des services Windows RDS (RDWEB, RDCB, SQL, RDLIC) hors services applicatifs (décrite dans le paragraphe qui suit) | R |  |
| 7 | Applications des patches OS (RDS est inclus dans l’OS) sur la plage d’intervention en Heure ouvrée la plus appropriée choisie par le client.  | R |  |
| 8 | Application des patches dans les RDSH et la supervision de ces services.  |  | R |
| 9 | Demandes d’évolution ou demande de modification de la configuration des éléments de l’architecture RDS (hors catalogue) | R |  |
| 10 | Etude des demandes d’évolution et réalisation effectuées dans le cadre de la gestion des changements | R |  |
| R : Réalisateur – A : Accountable (Responsable) – C : Consulté – I : Informé – V : Valideur |

#### Supervision

En plus de la supervision proposée dans le cadre du service « OS Managé » souscrit en prérequis, nous assurons la supervision suivante pour votre Managed RDS :

* Nous surveillons les services et nous analysons les données collectées sur la performance de l’environnement pour actions préventives.
* Nous surveillons des métriques pour déclencher des alertes en cas de problèmes critiques.
* Nous traitons les alertes remontées pas la supervision.

#### Sauvegarde

Une sauvegarde standard est assurée au niveau OS Managé, pour garantir la disponibilité du service en cas de problèmes.

#### Administration

Sur base des outils de supervision nous suivons les métriques d’usage du RDS. Ces métriques nous permettent :

* De suivre le comportement du service en temps-réel
* De lancer proactivement du troubleshooting suite à la détection d’une alerte de supervision
* De suivre les tendances sur des échelles de temps plus longues

# Support

Nous présentons ci-dessous le support spécifique que nous apportons dans le cadre du service.

## Gestion des changements

La gestion des changements s’inscrit dans le modèle commun de nos services managés.

### Demandes au catalogue

Les demandes de changement sont présentées dans l’Annexe 1. Elles sont classées selon 3 niveaux de complexité comme présenté dans le tableau ci-dessous. Pour chaque niveau un nombre de tokens est associé.

|  |  |  |
| --- | --- | --- |
| **Changement AD** | **Critère(s) de qualification** | **Nombre de Tokens**  |
| **Simple**  | * Nécessite de 1 à 3 tâche(s) pour le traitement
 | 1  |
| **Complexe**  | * Nécessite 4 tâches pour le traitement

Ou | 2 |
|  | * Nécessite une tâche complexe pour le traitement
 |

Nous préparons la réalisation d’un changement en concertation avec vous. Une fois la demande est traitée, vous serez prévenu pour valider et clôturer la demande.

### Demandes hors catalogue

Vous pouvez faire une demande hors catalogue et fournir les détails de votre besoin. Nous organiserons un point téléphonique d’une ½ h avec vous pour s’assurer de la bonne compréhension du besoin. 2 cas se présentent alors :

* Si le besoin fonctionnel est immédiatement qualifiable en tâches simples, moyennes ou complexes tel que défini au catalogue, la demande de Changement est finalement reclassée en demande au catalogue et peut être traitée par les équipes opérationnelles.
* Si le besoin fonctionnel n’est pas immédiatement traduisible en tâches simples ou complexes et que cela nécessitera une étude approfondie avec une durée et un délai de réalisation, une estimation du nombre de Tokens nécessaire pour l’étude sera faite. Cette étude est sans garantie de résultat compte-tenu de la très grande diversité de besoins fonctionnels qui peuvent être exprimés. En cas d’accord, l’étude est réalisée et aboutit à une faisabilité ou pas. En cas de faisabilité, celle-ci s’accompagne d’une évaluation des charges afférentes à sa réalisation. Ces charges seront qualifiées en demandes de changement simple ou complexe selon les critères énoncés plus haut.

# Annexe1

|  |  |  |
| --- | --- | --- |
| N° Tâche | Nom des tâches | Catégorie |
| RDS01 | Suppression d'une typologie de bureaux virtuels (groupes métiers…) | Simple |
| RDS02 | Création d'un nouveau bureau utilisateur (typologie de bureau existante) | Simple |
| RDS03 | Modification spécifique d'un bureau utilisateur (personnalisation) | Simple |
| RDS04 | Suppression d'une personnalisation spécifique d'un bureau utilisateur | Simple |
| RDS05 | Suppression d'une typologie de bureaux virtuels (groupes métiers…) | Simple |
| RDS06 | Création d'un nouveau bureau utilisateur (typologie de bureau existante) | Simple |
| RDS07 | Première analyse expert pour qualifier un besoin hors catalogue ou fonctionnel | Simple |