

Annexe technique au Descriptif de Service Managed Applications RDS managé

Table des matières

1	DEFINITIONS	2
2	OBJET	2
3	PRESENTATION DU SERVICE	2
4	FONCTIONNALITES	2
4.1	COLLECTION RDS	3
4.2	REMOTE DESKTOP SESSION HOST (RDSH)	3
4.3	REMOTE DESKTOP CONNECTION BROKER (RDCB)	4
4.4	REMOTE DESKTOP WEB ACCESS (RDWEB)	4
4.5	REMOTE DESKTOP LICENCE SERVER (RDLIC)	4
4.6	REMOTE DESKTOP GATEWAY (RDGTW)	4
4.7	CERTIFICATS SSL	4
5	INFRASTRUCTURE	4
6	SERVICES OPTIONNELS	6
6.1	USER PROFILE DISK (UPD)	6
7	CONDITIONS DE PRIX	7
7.1	PRIX	7
8	ACCES AU SERVICE	7
8.1	PREREQUIS	7
8.2	MISE EN SERVICE	7
8.3	MAINTIEN EN CONDITIONS OPERATIONNELLES	8
8.3.1	<i>Supervision</i>	8
8.3.2	<i>Sauvegarde</i>	9
8.3.3	<i>Administration</i>	9
9	SUPPORT	9
9.1	GESTION DES CHANGEMENTS	9
9.1.1	<i>Demandes au catalogue</i>	9
9.1.2	<i>Demandes hors catalogue</i>	9
10	ANNEXE1	9

1 Définitions

En complément des définitions des Conditions Générales, des Conditions Spécifiques Intégration Maintenance et Prestations associées, du Descriptif de Service Managed Applications, les définitions spécifiques suivantes s'appliquent à cette Annexe Technique.

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.

2 Objet

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

La présente est rattachée au document « Managed Applications – Descriptif de Service ».

3 Présentation du Service

Dans le cadre de ce service, le Prestataire assure la gestion du RDS Client 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 :

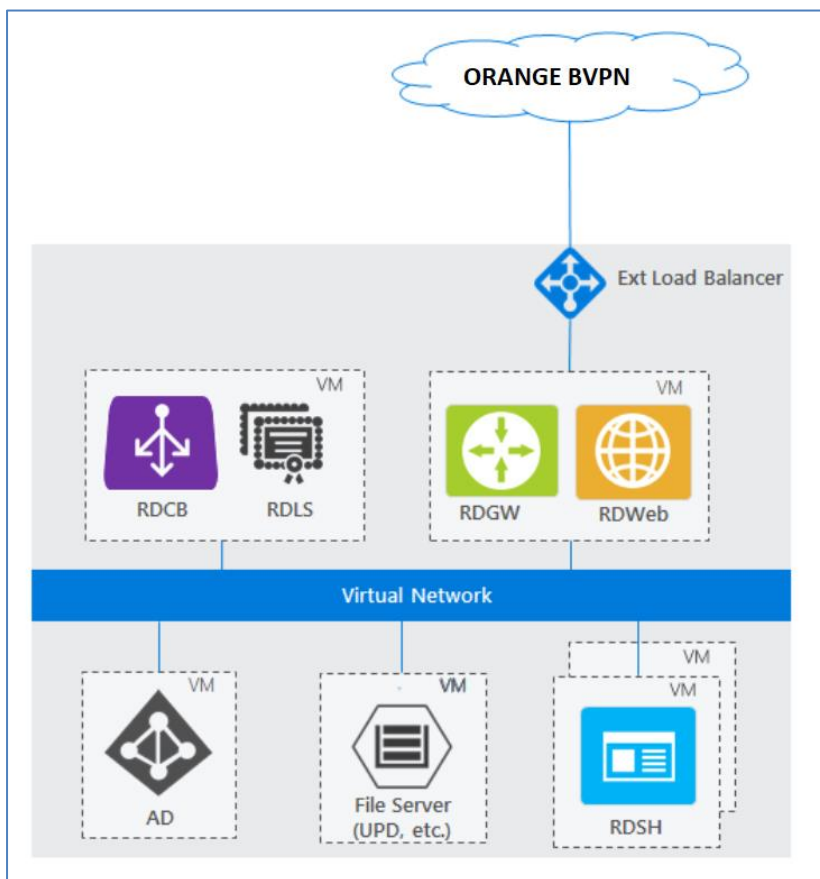
- Un Managed AD
- Des certificats SSL de serveur autosignés ou délivrés par une autorité de certification reconnue

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

4 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

4.1 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

4.2 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 ».

4.3 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.

4.4 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 apparaît 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.

4.5 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.

4.6 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

4.7 Certificats SSL

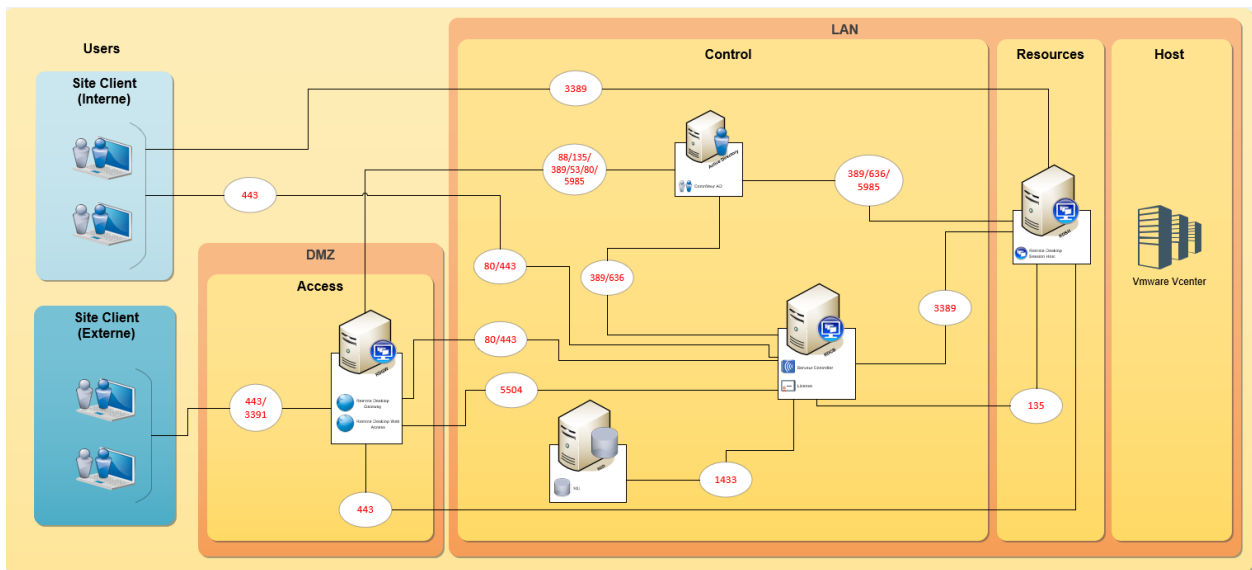
Chaque serveur utilisé dans la solution RDS a un certificat numérique qui est utilisé pour mettre en œuvre le protocole SSL (Secure Sockets Layer) et prouver son identité aux clients. Les certificats par défaut sont des certificats auto-signés qui ne sont pas reconnus des clients. Il faut donc installer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

5 Infrastructure

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



Le choix de l'infrastructure à souscrire sur Cloud Avenue pour proposer le service dépend du nombre d'utilisateurs, des usages prévus et du niveau de support requis, standard ou premium. Tel que présenté dans l'annexe qualité de service, le niveau de support premium permet d'avoir une haute disponibilité et un délai de rétablissement du service plus rapide en cas d'incident.

Le Tenant Cloud Avenue inclut l'accès réseau vers Internet uniquement avec une capacité minimum de 10Mbits. Selon l'usage mentionné par le client, les ajustements de bande passante peuvent faire l'objet d'une réévaluation des quotas et facturation. Les besoins d'adduction réseau du client vers Cloud Avenue, peuvent nécessiter une souscription additionnelle d'un lien haute performance / sécurité peut être intégré à l'offre.

A titre d'exemple, ci-dessous 2 simulations avec les 2 niveaux de support :

1- Maximum 100 utilisateurs

VM	Fonctionnalités	Spécifications				Quantité		Commentaire
		CPU	Ram (Go)	Disk1 (Go)	Disk2 (Go)	Standard	Premium	
Broker	RD Broker, Licence	4	8	100	20	1	2	
RD	RD Gateway, RD Web Access	4	4	100	NA	1	2	
RDSH		4	20	100	20	N + 1 (pour le test)	N + 1 (pour le test)	12 utilisateurs par serveur RDSH, à ajuster en fonction des usages.
FS	File Server	4	8	100	(standard user size (500 Mo) X number of hosted users) x 1.2	1	2	
BDD	Base de données SQL	4	16	100	C:\OS 100Go	1	1	Express, standard ou entreprise

VM	Fonctionnalités	Spécifications				Quantité		Commentaire
		CPU	Ram (Go)	Disk1 (Go)	Disk2 (Go)	Standard	Premium	
					D:\SOURCES 30Go			
AD	Active Directory	2	8	150 (50 pour backup local)	30	1	1	

2- Maximum entre 100 et 300 utilisateurs

VM	Fonctionnalités	Spécifications				Quantité		Commentaire
		CPU	Ram (Go)	Disk1 (Go)	Disk2 (Go)	Standard	Premium	
Broker	RD Broker, Licence	4	8	100	20	1	2	
RD	RD Gateway, RD Web Access	4	4	100	NA	1	2	
RDSH		4	20	100	20	N + 1 (pour le test)	N + 1 (pour le test)	12 utilisateurs par serveur RDSH, à ajuster en fonction des usages.
FS	File Server	4	8	100	(standard user size (500 Mo) X number of hosted users) x 1.2	1	2	
BDD	Base de données SQL	4	16	100	C:\OS 100Go D:\SOURCES 30Go	1	1	Express, standard ou entreprise
AD	Active Directory	2	8	150 (50 pour backup local)	30	1	1	

6 Services optionnels

6.1 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).

7 Conditions de prix

7.1 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 le Client doit souscrire par ailleurs auprès du fournisseur de IaaS selon les tarifs en vigueur.
- Les demandes de changement.

8 Accès au Service

8.1 Prérequis

Le Service « Managed RDS » s'appuie sur un service de IaaS, auquel le Client doit également souscrire selon les recommandations du Prestataire et lui 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.

8.2 Mise en service

Le Prestataire 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 paramètres 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
2. 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 RDCB RDWEB = Nom porté par le Load-Balancer Décrire les tests de la recette fonctionnelle de fin de BUILD	R	I
5	Déployer les rôles RDSH, RDCB, RDWEB, RDCLI Configurer les certificats SSL d'une ferme RDS Ouvrir les flux nécessaires entre les VMs, le LB et les utilisateurs	R	

Tâches		Orange Business	CLIENT
6	Déployer haute disponibilité pour RDCB, RDLIC et RDWEB (pour le niveau premium) Configurer 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 une application / bureau de test en RemoteApp dans toutes les collections	R	
11	Mise en place des sondes de supervision OS Managé sur l'ensemble des serveurs RDS Mise en place des sondes avec test de vie sur les services Windows de RDS (hors applicatif), accessibilité du service HTTPS RDWEB Mise 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 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.

8.3 Maintien en conditions opérationnelles

Le Prestataire assure 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)	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			

8.3.1 Supervision

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

- Analyse des données collectées sur la performance de l'environnement pour actions préventives.
- Métriques pour déclencher des alertes en cas de problèmes critiques.
- Traitement les alertes remontées par la supervision.

8.3.2 Sauvegarde

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

8.3.3 Administration

Sur base des outils de supervision le Prestataire suit les métriques d'usage du RDS qui permettent de :

- Suivre le comportement du service en temps-réel
- Lancer proactivement du troubleshooting suite à la détection d'une alerte de supervision
- Suivre les tendances sur des échelles de temps plus longues

9 Support

Dans le cadre du support, le Prestataire assure :

9.1 Gestion des changements

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

9.1.1 Demandes au catalogue

Les demandes de changement sont présentées dans le § « Catalogue de changement ». Le Prestataire prépare la réalisation d'un changement en concertation avec le client. Une fois la demande est traitée, le client sera prévenu pour valider et clôturer la demande.

9.1.2 Demandes hors catalogue

Pour une demande hors catalogue, l'équipe opérationnelle évalue sa faisabilité, 2 cas de figure se présentent:

1- Demande aisément qualifiable

L'équipe opérationnelle fait un retour sur le nombre de Tokens nécessaire pour la réalisation et si applicable les ressources d'infrastructure nécessaires et la charge de service récurrente qui en résultent. Après l'accord du Client, la demande sera réalisée et les éléments suivants facturés :

- le nombre de Tokens débité sur votre forfait si vous en avez souscrit un ou hors forfait,
- les ressources d'infrastructure additionnelles selon votre contrat d'infrastructure Cloud,
- la charge de service récurrent

2- Demande à qualification spécifique

L'équipe opérationnelle fait un retour au Client lui indiquant de se rapprocher de son contact commercial.

10 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