Business

Annexe technique au Descriptif de Service Managed Applications – OS managé

Table des matières

1 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.

Conditions Générales désigne les conditions générales relatives aux Services de Cloud du Prestataire.

Environnement désigne un espace privé virtuel de ressources sur le IaaS auquel seuls les Utilisateurs authentifiés par login et mot de passe peuvent avoir accès. Les actions de création, destruction, modification, listage de ces ressources et des fonctionnalités associés sont limitées à ces seuls Utilisateurs.

Environnement d'Administration Client désigne l'environnement dans lequel est hébergé le Service du Client (build et déploiement). Les actions de création, destruction, modification, listage des ressources et des Fonctionnalités associées sont limitées au Prestataire.

Environnement Client désigne l'environnement dans lequel sont déployés les conteneurs du Client. Les actions de création, destruction, modification, listage des ressources et des fonctionnalités associées sont attribuées au Prestataire et au Client. Le Client peut utiliser ce tenant pour exécuter des applications et utiliser des fonctionnalités IaaS.

RACI désigne la définition des responsabilités entre le Client et le Prestataire. R = Responsable, A = Autorité redevable, C= Consulté, I = Informé.

Tenant désigne un espace privé virtuel de ressources sur le IaaS auquel seuls les Utilisateurs authentifiés par login et mot de passe peuvent avoir accès. Les actions de création, destruction, modification, listage de ces ressources et des Fonctionnalités associés sont limitées à ces seuls Utilisateurs. Pour les IaaS en technologie VMware, le Tenant est également appelé « Organisation ».

Tenant Managé désigne le Tenant dans lequel est hébergé le Service du Client. Les actions de création, destruction, modification, listage des ressources et des Fonctionnalités associées sont limitées au Prestataire.

Token désigne l'unité d'œuvre utilisée pour exprimer les prix applicables aux changements demandés par le Client, tels qu'indiqués dans la Fiche Tarifaire.

2 Objet

Le présent descriptif de service a pour objet de définir les conditions dans lesquelles le Prestataire fournit le service «Managed OS» (ci-après le « Service ») au Client.
Le présent descriptif est rattaché au document « Managed Applications – Descriptif de Service ».

3 Présentation du Service

3.1 Aperçu du Service

Le service d'OS managé assure l'administration, la supervision, le patching et la sécurisation des systèmes d'exploitation Linux et Windows hébergés sur Cloud Avenue, vCoD ou toute autre infrastructure.

Dans le cadre du service d'OS managé, nous assurons également la gestion complète du système d'exploitation d'une VM (Machine Virtuelle) hébergée sur une infrastructure Cloud Public IaaS de la liste ci-dessous.

1. Cloud Avenue (le Prestataire)
2. Flexible Engine (le Prestataire)
3. AWS (Partenaire)
4. Microsoft Azure (Partenaire)
5. Google Cloud (Partenaire)

- Nous assurons également la gestion complète du système d'exploitation d'un serveur physique hébergé uniquement sur les IaaS du Prestataire (Cloud Avenue et Flexible Engine).

Nous intervenons pendant les 2 phases :

6. Mise en service
7. Maintien en conditions opérationnelles

La liste des OS supportés :

OS	Distribution et version
Linux	- RedHat Enterprise - CentOS - Ubuntu - Debian
Windows	- Windows Server

Le client a la responsabilité de gérer vos applications et Middleware et de vérifier le bon fonctionnement.

4 Pré-requis

4.1 Bastion sécurisé

Le service de Bastion est un pré-requis à l'ensemble des services managés Managed Applications dont l'OS managé.
L'usage du Bastion MASERPAM est obligatoire pour tout accès à privilèges au sein du service Managed OS.

4.1.1 La solution Bastion (MASERPAM)

Obligation d'usage du Bastion MASERPAM.

Un bastion est une solution de sécurité qui permet de protéger les accès pour les comptes à privilèges au sein d'un système d'information afin d'administrer les services hébergés.

Le Bastion MASERPAM est une solution de sécurité protégeant les accès aux comptes à privilèges dans un système d'information. Reposant sur CyberArk Alero/Remote Access, il s'appuie sur un coffre-fort sécurisé (Vault) où sont stockés et chiffrés identifiants, secrets, certificats et clés sensibles. Chaque accès est temporaire, tracé et enregistré afin de garantir sécurité, conformité et responsabilité.

L'utilisation du Bastion MASERPAM constitue un prérequis obligatoire pour l'ensemble des services Managed Applications (Managed OS, Managed Database, Managed Middleware, Managed Applications), quel que soit l'environnement d'hébergement (Cloud Avenue, vCoD ou autre infrastructure).

Ce dispositif garantit la sécurité, la confidentialité et la traçabilité des accès à privilèges, conformément aux exigences de conformité (HDS, PSSI, PGSSI-S) et aux engagements de qualité de service.

L'accès direct aux ressources managées sans passer par le Bastion est strictement interdit.

Pour les services relevant du périmètre IaaS / console vCoD (CAV), l'usage du Bastion MASERPAM n'est pas imposé contractuellement à ce jour mais reste fortement recommandé, en particulier pour les comptes utilisateurs disposant de privilèges d'administration.

L'utilisateur s'authentifie auprès du bastion et obtient un accès temporaire aux ressources demandées. L'accès est surveillé et enregistré, ce qui permet de suivre les actions effectuées par l'utilisateur.

En résumé, un bastion est une solution de sécurité qui permet de réduire les risques de compromission des comptes à privilèges et de renforcer la sécurité globale du système d'information.

4.1.2 Aperçu du Service

Dans le cadre des projets Cloud hébergés sur la plateforme Cloud Avenue, Le Prestataire met en œuvre un Bastion sécurisé pour les Clients qui nécessitent un accès à privilèges pour l'administration de leur système d'information.

L'usage d'un Bastion est un prérequis :

- Pour satisfaire aux exigences de cybersécurité,
- Pour maintenir la confidentialité et la protection des données à accès privilégiés,
- Pour garantir les engagements de qualité de service souscrits notamment en traçant les actions des différents acteurs intervenant sur le système.

Le Prestataire impose l'utilisation d'un Bastion d'administration pour effectuer toutes les actions sur les services que nous opérons.

Le Prestataire s'occupe intégralement et de manière exclusive de la gestion du Bastion d'administration qui fournit :

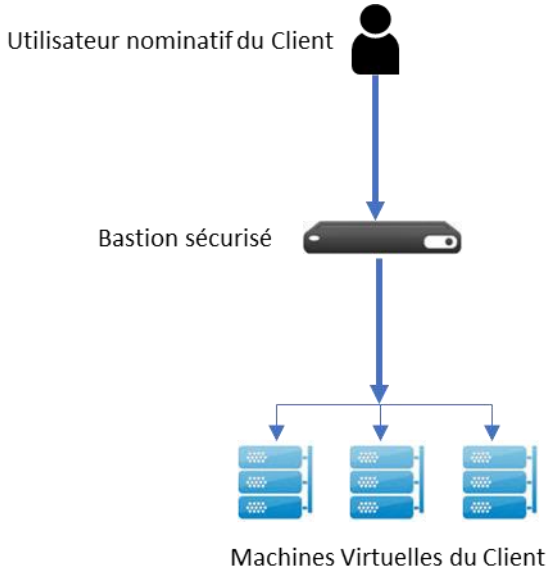
- Un accès centralisé à la plateforme/au service,
- Une gestion des utilisateurs,
- Une gestion des privileges,
- Une gestion des secrets,
- Une traçabilité des actions réalisées au travers du bastion.

4.1.3 Fonctionnalités principales

- Authentification forte biométrique via CyberArk Alero
- Accès sans VPN via interface web sécurisée (RDP, SSH)
- Option HTTPS avec connecteur dédié (OTC spécifique)
- Gestion centralisée des identifiants, secrets et certificats (Vault)
- Journalisation complète et enregistrement vidéo des sessions (consultables uniquement par BSO)
- Rotation automatique des mots de passe et clés d'accès

4.1.4 Schéma fonctionnel de la solution

Ce schéma d'architecture fonctionnelle illustre comment le Bastion sécurisé est utilisé pour protéger l'accès à des machines virtuelles, en fournissant une couche de contrôle et de sécurité supplémentaire pour les utilisateurs nommés.



4.1.5 Unités d'œuvres (UO) et tarificaiton

La tarification du Service Bastion sécurisé est composée comme suit :

- D'une UO **obligatoire** pour les Clients ayant souscrit un Managed Tenant – small couvrant le socle de service du bastion. Le socle de service bastion est inclus dans les souscriptions Managed Tenant – medium et large.
- D'une UO **obligatoire** avec un prix OTC/MRC pour 2 utilisateurs **nominatifs** du Client pour l'accès aux ressources (VM, Applications) du Client via le Bastion sécurisé. Cette UO couvre le service de Bastion et les licences nécessaires pour 2 utilisateurs nominatifs.
- D'une UO **en option** avec un prix OTC/MRC par utilisateur **nominatif** supplémentaire du Client pour l'accès aux ressources (VM, Applications) du Client via le Bastion sécurisé. Cette UO couvre le service de Bastion et les licences nécessaires pour 1 utilisateur nominatif

5 Services inclus

Dans le cadre du service OS Managé, nous assurons la gestion des composants d'infrastructures. Certains services sont inclus avec l'OS Managé et d'autres sont proposés en option.

5.1.1 Antivirus

Dans le cadre du service OS Managé proposé pour une VM ou un serveur physique hébergés sur une infrastructure Cloud, nous déployons l'antivirus Trend Micro Deep Security et nous gérons les mises à jour, le paramétrage et la supervision.

Cet antivirus scanne et détecte les virus, les Spyware et les chevaux de Troie en temps réel (Lors de l'accès au fichier). En cas de détection d'un virus, l'élément est automatiquement mis en quarantaine pour analyse, ou supprimé dans le cas où la première action n'est pas possible.

5.1.2 Scan de vulnérabilité

Dans le cadre du Service Managé le Prestataire fait un scan de vulnérabilité régulièrement pour garantir la sécurité des assets dont il est responsable. Ce service permet au Client d'être au niveau de sécurité recommandé et d'atténuer efficacement les risques. Les corrections de vulnérabilité sont prises en charge par les équipes du Prestataire dans le périmètre du service souscrit par le Client (Managed OS, Managed DB ou Managed application).

Le Prestataire utilise des outils de sécurité pour évaluer le réseau, les applications et l'infrastructure à la recherche de faiblesses qui pourraient être exploitées par des acteurs malveillants.

Un rapport détaillé par tenant est mis à disposition tous les trimestres dans l'espace Client décrivant les top 10 vulnérabilités identifiées ainsi que des étapes de remédiation recommandées sous la responsabilité du Client.

Sur instruction du Client les remédiations sous sa responsabilité pourront être traitées et pourront donner lieu à un devis par le Prestataire au Client.

5.1.3 Sauvegarde

Pour assurer le rétablissement du service en cas de problèmes, nous préconisons à minima une sauvegarde Snapshot avec 6 jours de rétention. Les sauvegardes sont réalisées en HNO et l'exploitation de la sauvegarde est assurée selon le niveau de support souscrit.

Une durée de rétention différente peut être choisie selon la disponibilité du backup de l'infrastructure Cloud hébergeant le service.

5.1.4 Supervision

Nous assurons la supervision suivante pour les VMs ou serveurs Physiques que nous gérons. Le tableau ci-dessous présente le type de supervision et les actions associées.

Type	Supervision	Action
Manuelle	Surveiller les fichiers système (dépôts Linux...)	En cas de dysfonctionnement, l'équipe opérationnelle est prévenue via un ticket pour résoudre le problème en heures ouvrées.
Manuelle	Surveiller l'obsolescence des OS.	En cas d'obsolescence, on vous prévient et l'équipe commerciale pour lancer un projet de mise à jour.
Automatique	Surveiller la mise à jour des agents et des bases de signalements (antivirus / patch de sécurité).	En cas de dysfonctionnement, l'équipe opérationnelle est prévenue via un ticket pour résoudre le problème en heures ouvrées.
Automatique	Surveiller la disponibilité de l'OS	En cas d'alerte (OS hors service), l'équipe opérationnelle est prévenue via un ticket pour résoudre le problème en heures ouvrées.
Automatique	Surveiller la performance de l'OS	En cas d'alerte sur la performance (sur base d'un seuil défini), l'équipe opérationnelle est prévenue via un ticket pour résoudre le problème en heures ouvrées.
Automatique	Surveiller en 24x7 la présence virale et son confinement.	En cas d'alerte, l'équipe opérationnelle est prévenue via un ticket pour résoudre le problème en heures ouvrées. Les actions seront à valider avec vous.

5.1.5 Log management

Sur Cloud Avenue un service de log management centralisé est proposé et se décompose de la façon suivante :

- **Collecte des logs :** Le service collecte automatiquement les logs générés issus des OS Managés et des composants sécurité souscrits par le Client.
- **Stockage des logs :** Les logs collectés sont stockés de manière sécurisée et durable dans un emplacement centralisé. Le Prestataire propose une durée de rétention standard, d'autres durées de rétention pourront faire l'objet d'une proposition spécifique du Prestataire au Client.
- **Usage des logs :** Les logs sont à usage interne pour les équipes d'administration du Prestataire.
- **Mise à disposition des logs :** Sur demande de changement, le Prestataire réalise un export des logs pour le Client.

5.1.6 Reporting - Option

Nous proposons 2 niveaux de reporting :

- Usage : rapport sur les d'infrastructures, état des services, capacitaire, performance et consommation.
- ITSM : rapports sur le change management, incident management, SLA

5.1.6.1 *Usage*

Les rapports d'usage présentent l'état de votre infrastructure Cloud managés sur une plage de temps choisie. Ces rapports accessibles depuis l'Espace Client Cloud

Les indicateurs disponibles sont :

Ressource	Indicateurs
Serveur (VM ou physique)	- Disponibilité du serveur - Utilisation CPU - Nombre de process

	- Utilisation mémoire - Utilisation de l'espace SWAP - Utilisation file système - Utilisation bande passante - Statut du serveur (Eteint, En veille, En service)

5.1.6.2 *ITSM*

Les rapports ITSM présentent l'état du service managés sur une plage de temps choisie. Ces rapports accessibles depuis l'Espace Client Cloud.

Disponibilité de service	
Service	**Indicateur**
Nom su service	- Nombre d'incidents sur la période choisie classées par niveau de priorité (P1, P2, P3, P4) - Durée de résolution pour chaque incident - Liste des incidents où l'engagement GTR n'est pas respecté - Liste des incidents où l'engagement GTI n'est pas respecté - Liste des incidents selon le statut (ouverts, pris en charge, en cours de résolution, résolu,..) - Evolution mensuelle sur 1 an.

Incidents	
Service	**Indicateur**
Nom du service	- Engagement GTD (garantie taux de disponibilité) contractuel - GTD mesuré - Evolution mensuelle sur 1 an.

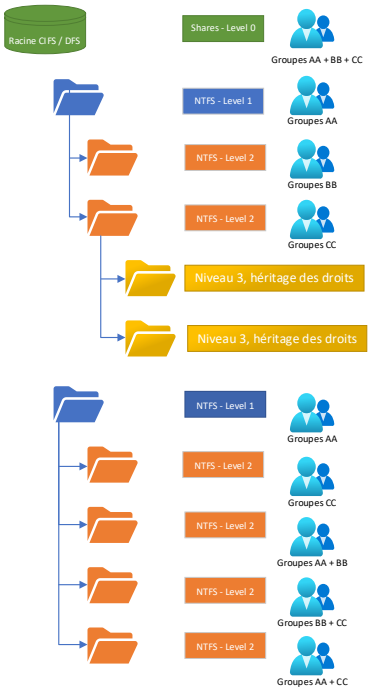
Demandes de changement	
Service	**Indicateur**
Nom du service	- Nombre de demandes sur la période choisie classées par type - Durée de traitement pour chaque demande - Liste des demandes où l'engagement GTT (garantie temps de traitement) n'est pas respecté - Liste des demandes selon le statut (ouverts, pris en charge, en cours de traitement, traité,..) - Evolution mensuelle sur 1 an. - Consommation des tokens du forfait

6 Services optionnels

6.1 Managed Filer

Avec ce service, en fonction de la solution technique choisie, nous assurons la gestion de fichiers pour répondre aux besoins de stockage et de partage de données du client. Nous prenons en charge la configuration, la surveillance et la maintenance de votre système de fichiers, vous permettant ainsi de vous concentrer sur votre activité principale. Notre service inclus la gestion des autorisations d'accès, la sauvegarde régulière des données, la gestion de la capacité de stockage et la résolution des problèmes techniques.

Le Managed Filer inclut la mise en place de la sécurisation des accès sur les Shares et le système de fichiers NTFS sur les deux premiers niveaux de l'arborescence du système de fichiers distribué (CIFS, DFS & DFS-R). La mise en place de la sécurisation de l'arborescence sera effectuée via des groupes Active Directory pré-renseigné par le client et communiqué aux opérationnels du Prestataire préalablement.



7 Conditions de prix

7.1 Prix

La tarification du Service OS Managé est composée :

- Des frais d'accès au service « Managed OS » 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 socle d'infrastructure et du service « Managed OS » indexé sur le nombre de serveurs.
- Le prix des licences

Les tarifs du Service n'incluent pas :

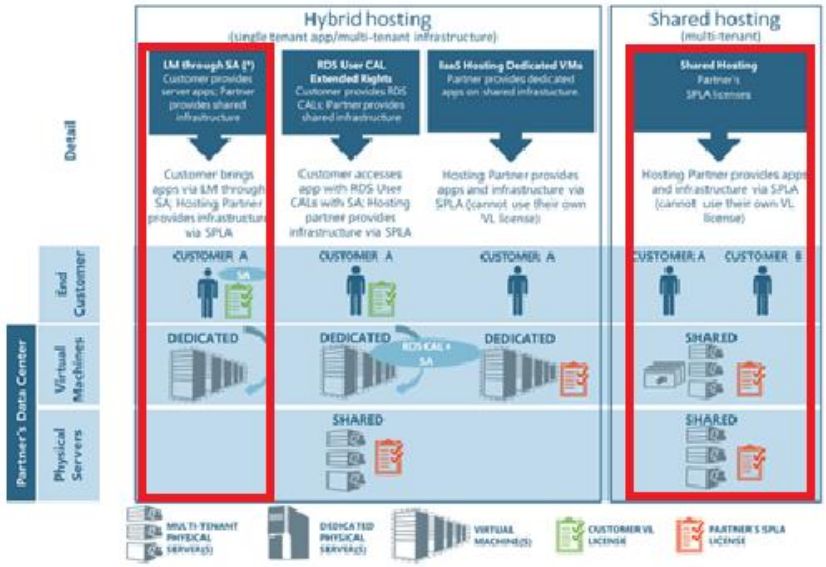
1. Le prix de l'infrastructure que vous devez souscrire par ailleurs auprès du fournisseur de IaaS selon les tarifs en vigueur.
2. Les demandes de changement.
3. Le prix des licences

Pour l'option « Managed Filer », la tarification est composée :

- Des frais de mise en service intégrant toutes les tâches d'implémentation et indexé sur le nombre de filers.
- D'un récurrent mensuel couvrant les activités liées au maintien en condition opérationnelle du filer indexé sur le volume réservé (en Go).

7.2 Licences

Le client dispose de 2 modes pour contractualiser les licences comme illustré dans le schéma ci-dessous :



1. BYOL (bring your own licence), fournir ses propres licences (Licence Mobility through SA, hybrid hosting). Dans ce mode, le client doit souscrire au programme mobility et disposer d'une Software assurance active.
   - Souscrire les licences auprès du Prestataire dans le cadre de son contrat SPLA (Shared Hosting multitenant).

8 Accès au Service

8.1 Prérequis

Le Service « Managed OS » s'appuie sur un service de IaaS, auquel vous devez également souscrire. Dans ce cadre, nous gérons le Tenant est les ressources associées.

Pour les systèmes dans un Active Directory, nous devons disposer d'un compte de type Administrateur pour effectuer nos actes de Managed OS nous accordant alors les accès au système de fichiers, la configuration registre, configuration système et le déploiement de nos outils (supervision, sauvegarde/restauration, gestion des correctifs, remédiation).

Pour les systèmes sous Linux (CentOS, RHEL), nous devons disposer d'un compte équivalent Root/Sudoer sur les machines couvertes par le Managed OS. Ce compte est nécessaire pour y lancer les Pipeline Ansible et déployer les correctifs.

8.2 Mise en Service

Nous réalisons les tâches suivantes pour mettre en place le service sur un serveur :

ID	Tâches	Le Prestataire	Client
Tenant			
1	Fournir les accès du tenant		A
2	Définir des politiques relatives aux systèmes d'exploitation, des procédures et des services système	A – R	V
3	Définir la configuration technique des systèmes d'exploitation, conformément aux services demandés (Version, langues, configuration système fichiers, paramètres système…)	R	A – R
4	Configurer le tenant sur le IaaS choisi	A - R	
5	Normaliser un OS en cas de lift and shift.	A - R	
6	Configurer la zone de services permettant de livrer tous les services	A - R	
7	Donner les accès clients aux services (espace client cloud, ITSM)	A - R	I - V
8	Fournir les éléments requis pour la mise en service des serveurs selon une SRF (service request form)	V	A
9	Installer les systèmes d'exploitation sur les serveurs	A – R	V

ID	Tâches	Le Prestataire	Client
10	Configurer les services : OS, supervision, sauvegarde standard, antivirus	A - R	V
11	Définir les indicateurs de performances du matériel et des systèmes d'exploitation, les seuils et les quotas	A – R	R
12	Développer et documenter des procédures de contrôles conformes au service souscrit	A - R	I
R : Réalisateur – A : Accountable (Responsable) – C : Consulté – I : Informé – V : Valideur			

8.3 Maintien en conditions opérationnelles

Nous assurons les opérations pour le maintien en conditions opérationnelles de l'OS.

Les dispositions prises dans le cadre de cet objectif peuvent être de nature préventive ou curative.

Le tableau ci-dessous présente les tâches et responsabilités associées pour l'exploitation des services présentés au §3.

ID	Tâches	Le Prestataire	Client
1	Exploiter le système de supervision	A – R	
2	Traiter les alertes et les incidents et escalader, tel que décrit dans les procédures	A – R	
3	Appliquer des mesures préventives pour la surveillance proactive et des fonctionnalités d'auto-rétablissement, afin de minimiser les pannes impactant la fourniture des services	A – R	
4	Résoudre les incidents systèmes, conformément à l'accord sur les niveaux de services	A – R	I
5	Surveiller les seuils et taux d'occupation et prendre les mesures qui s'imposent en cas de dépassement	A - R	R – V
6	Surveiller le bon fonctionnement des composants systèmes, conformément aux seuils définis	A – R	
7	Surveiller l'évolution des performances et la consommation des ressources, afin d'anticiper tout problème éventuel	A – R	I
8	Établir des rapports sur des événements, sur demande et conformément au processus de gestion des changements	A – R	V
9	Conseiller du matériel approprié pour de nouvelles configurations ou l'amélioration de configurations existantes, afin d'atteindre les niveaux de services souscrits	A – R	C
10	Administrer et maintenir les configurations matérielles et la configuration des systèmes d'exploitation, les paramètres, et les fichiers ressources systèmes	A – R	
11	Gérer les fichiers licences logicielles des systèmes d'exploitation et les clés utilisateurs	A – R	C
12	Effectuer la maintenance corrective du matériel et des systèmes d'exploitation : Gestion des patchs, gestion des interventions.	A – R	
13	Mettre à jour et surveiller les paramètres de configuration du matériel et des systèmes d'exploitation : Processeur, mémoire, systèmes de stockage, quotas disques, profils utilisateurs…	A – R	V
14	Analyser les journaux des systèmes d'exploitation	A – R	
15	Surveiller les indicateurs de performances du matériel et des systèmes d'exploitation, les seuils et les quotas	A – R	
16	Détecter et analyser tout état anormal du matériel et des systèmes d'exploitation, et prendre les actions correctives qui s'imposent	A – R	
17	Appliquer les changements, conformément au processus de gestion des changements	A – R	R
18	Effectuer des analyses de tendances proactives, afin d'identifier les problèmes récurrents	A – R	C – I
19	Suivre et signaler tout problème récurrent ou panne et fournir une liste des conséquences liées aux problèmes en cas d'impact sur l'activité du Client	A – R	I
20	Recommander des solutions pour résoudre tout problème récurrent ou panne	A – R	C
R : Réalisateur – A : Accountable (Responsable) – C : Consulté – I : Informé – V : Valideur			

9 Support

Nous présentons ci-dessous le support spécifique que nous apportons à l'OS Managé.

9.1 Gestion des patchs

Les correctifs apportés par l'éditeur du système d'exploitation sont effectués une fois par mois. L'OS est entièrement sauvegardé avant l'application d'un patch.

Pour réduire le risque sur le service et permettre au client de mesurer l'impact d'un patch, il peut diviser ses unités de service OS en 2 groupes : "patch 1er groupe" et "patch 2ème groupe".

Le Prestataire informe le client de la semaine et du jour où le patch est appliqué pour le « patch 1er groupe » : du lundi au jeudi de la première semaine ou de la deuxième semaine ou de la troisième semaine ou de la quatrième semaine. Le patch est toujours effectué pour le "patch 2ème groupe" la semaine suivant le "patch 1er groupe".

Les patchs sont déployés automatiquement à l'aide d'outils spécialisés en dehors des heures de travail du créneau choisi. Les défaillances éventuelles sont ensuite corrigées pendant les heures ouvrées.

Si notre supervision détecte une erreur après l'application d'un patch, l'équipe opérationnelle ouvre un ticket d'incident et le traite avec la possibilité de restaurer si nécessaire depuis la dernière sauvegarde OS.

9.2 Gestion des changements

La gestion des changements pour le service OS Managé s'inscrit dans le modèle commun de nos services managés. Vous disposez d'un catalogue de demandes standards présenté au chapitre 8.

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

1- Demande aisément qualifiable

   L'équipe opérationnelle vous 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 votre accord, la demande sera réalisée. Vous serez facturé :
   - 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 vous fait un retour vous indiquant de vous rapprocher de votre contact commercial.

Annexe 1 – Catalogue des demandes standard

Catalogue	Catégorie	Description	Nombre tokens
Managed Services : OS	OS	Créer/Etendre/Supprimer un Filesystem	1
		Installer un composant (patch, tool, prerequestite)	2
		Configurer l'OS (noyau, groupes, utilisateurs, sudo)	2
		Demande de droit administrateur temporaire 48h	3
		Démarrer/Arrêter un process	1
		Démarrer/Arrêter un serveur	1
		Autre demande	3
		Ajouter un OS managé	6
		Supprimer un OS managé	1
		Modifier la configuration de l'antivirus	2
Managed Services : Infra	Infrastructure	Demander un changement IAAS	2
		Modifier les ressources d'un OS managé (CPU, RAM, Storage, réseau)	2
Managed Services : Common	Non-Standard	Demander une cotation pour un change non-standard	
		Accepter la proposition de prix pour un change non-standard	
	DNS	Ajout d'entrée	1
		Modification d'une entrée	2
		Suppression d'une entrée	1
		Autres	3
	Communication	Demander de l'information	2
		Fournir une information au Prestataire	
	Certificat	Installer un certificat fourni	2
		Regénérer une clé de certificat	2
		Supprimer un certificat	2
	Backup	Demander un backup ou une restoration	2
		Mettre à jour la politique de sauvegarde	2
		Sauvegarde occasionnelle	1
		Modifier paramètre sauvegarde	1
		Restauration données	3
		Test de restauration de données	3
	Service	Supprimer une unité de service managée	2
		Créer une unité de service managée	3
	Vulnérabilité	Demande explication et recommandation pour une vulnérabilité	1
		Demande de scan par tenant	
Services optionnels			
Managed Filer		Création quota	2
		Augmentation quota	2
		Création share	2
		Suppression share	2
		Sécurisation NTFS jusqu'à 2 niveaux : share	5