Business

Annexe technique au Descriptif de Service Managed Applications – AD 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.

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.

AD DS : Active Directory Domain Services est le service proposé dans ce document.

Domaines active directory : Les domaines sont les principales unités de sécurité et de gestion dans Active Directory. Ils permettent de regrouper les utilisateurs et les ressources en fonction de critères tels que leur localisation géographique, leur service ou leur entreprise. Les domaines sont organisés en une arborescence hiérarchique qui permet de gérer les utilisateurs et les ressources de manière centralisée.

Unités d'organisation (OU) : Les unités d'organisation (OU) sont des conteneurs logiques qui permettent de regrouper des objets tels que les utilisateurs, les groupes et les ordinateurs dans un domaine. Les OUs peuvent être utilisées pour gérer les stratégies de sécurité, les paramètres de configuration et les autorisations d'accès pour les utilisateurs et les groupes.

Les groupes active directory : Les groupes dans Active Directory permettent de regrouper des utilisateurs en fonction de leur rôle ou de leur service. Les groupes peuvent être utilisés pour gérer les autorisations d'accès aux ressources et pour faciliter la gestion des utilisateurs.

Les utilisateurs active directory : Les utilisateurs sont les objets les plus importants dans Active Directory. Ils représentent les personnes qui utilisent les ressources d'un réseau. Les informations relatives à un utilisateur, comme son nom d'utilisateur, son mot de passe et ses autorisations d'accès, sont stockées dans Active Directory.

IaaS (Infrastructure as a Service). Il s'agit d'un modèle de service cloud computing qui fournit aux utilisateurs des ressources informatiques de base telles que des ordinateurs virtuels, du stockage et des réseaux, ainsi que des fonctionnalités telles que la gestion et la mise à l'échelle, sans qu'ils aient besoin de gérer les infrastructures physiques elles-mêmes. Les entreprises peuvent utiliser un IaaS pour bénéficier d'une plus grande flexibilité, de coûts réduits et d'une meilleure évolutivité pour leurs activités informatiques.

AGPM (Advanced Group Policy Management) est un outil de gestion de stratégies de groupe pour les environnements Windows. Il permet de stocker, contrôler et gérer les GPO (Group Policy Objects) dans un référentiel centralisé, tout en fournissant des processus de flux de travail pour la création, la modification, la révision, l'approbation et le déploiement des GPO. Les fonctionnalités d'AGPM comprennent la comparaison de versions de GPO, la gestion des autorisations, la vérification de conformité et l'historique des modifications.

2 Objet

La présente annexe technique a pour objet de définir les conditions dans lesquelles le Prestataire fournit le service «Managed AD» (ci-après le « Service ») au Client.
La présente annexe technique est rattachée au document « Managed Applications – Descriptif de Service ».

3 Présentation du Service

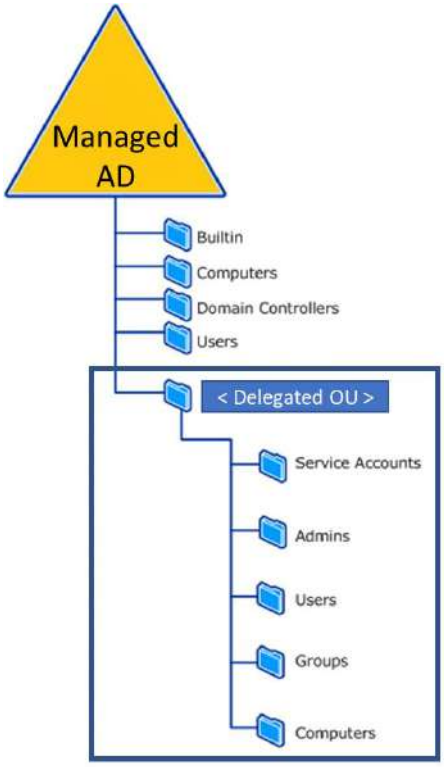
Dans le cadre de ce service, le Prestataire assure la gestion de l'AD DS hébergé sur une infrastructure Cloud Public IaaS de la liste ci-dessous.

Orange Business
- Cloud Avenue
- Flexible Engine

Partenaire
- AWS (prévu dans la roadmap)
- Microsoft Azure (prévu dans la roadmap)
- Google Cloud (prévu dans la roadmap)

Comme illustré dans le schéma ci-dessous, le Client a une délégation sur une ou plusieurs 'OU' lui permettant d'administrer les comptes utilisateurs et ordinateurs et le Prestataire a en charge les activités suivantes :

- Le choix des composants nécessaires pour votre Managed AD
- La mise en place du service
- La maintenance
- La configuration et la surveillance des services AD
- La gestion des GPO (hors OU déléguée) et la gestion des services AD
- La sauvegarde standard de l'AD



Les prérequis pour cette offre :

- Souscrire à l'offre OS Managé pour les VMs où est hébergée l'AD du Client
- Infrastructure composée d'un minimum de 2 VMs selon les recommandations de Microsoft
- AD mono-forêt, mono-domaine
- Respecter les bonnes pratiques et les recommandations d'Orange Business

4 Services optionnels

4.1 Audit sécurité

Le Prestataire réalise avec l'outil de PingCastle un contrôle mensuel pour évaluer la sécurité d'un Active Directory. Cet outil analyse les domaines active directory et fournit un score qui reflète la sécurité de l'environnement AD Client. Plus le score PingCastle est bas, plus l'AD est sécurisé.

L'analyse prend en compte plusieurs facteurs, tels que par exemple :

- la complexité des mots de passe et leur durée de vie
- la configuration de l'authentification à deux facteurs.
- les comptes utilisateurs / ordinateurs / comptes à pouvoir
- relations d'approbations / délégations / privilèges / GPOs / certificats
- type de chiffrement supportés / obsolescence de systèmes, de protocoles
- les sauvegardes / les politiques d'audit

A l'issue de l'analyse, PingCastle génère un score de conformité et un rapport dans une console centralisée. Sur base du rapport, le Prestatire préconise des recommandations pour améliorer la sécurité de l'active directory et des systèmes

gérés par celui-ci. Ces recommandations aident à protéger le domaine Client contre les menaces internes/externes et les usages frauduleux de comptes équivalents administrateurs.

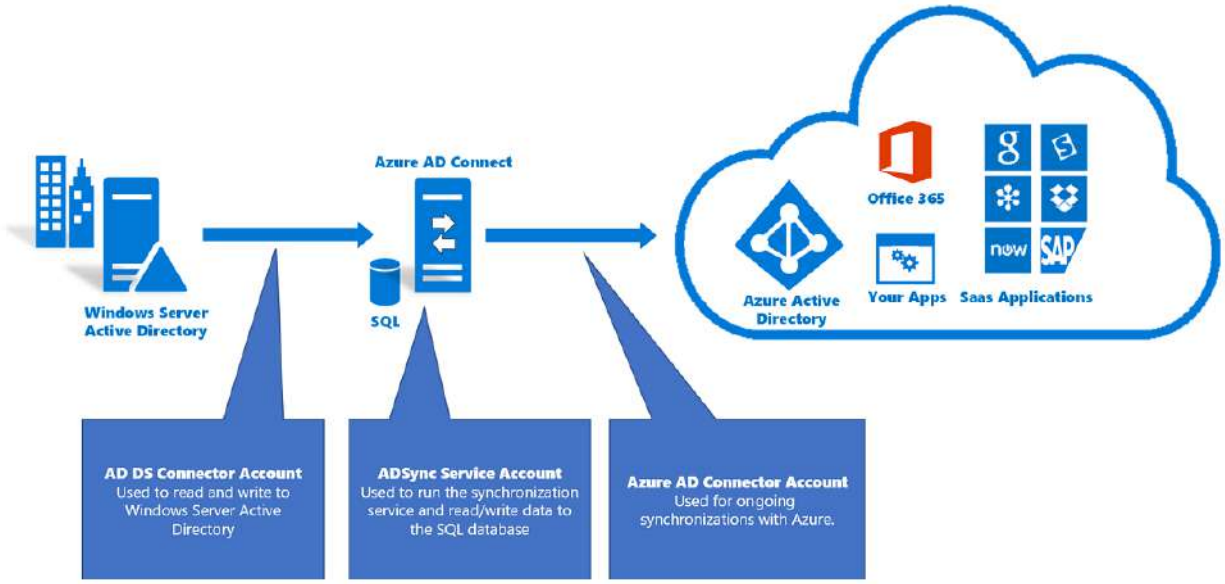
A noter, il n'existe pas de score PingCastle "acceptable" spécifique qui s'applique à tous les contextes. Cependant, en général, un score PingCastle inférieur à 50 est considéré comme une bonne indication de la sécurité de votre Active Directory.

Prérequis

L'intégration de PingCastle dans l'environnement Active Directory consiste à installer et à configurer le logiciel sur un serveur contrôleur de domaine. Une fois installé, PingCastle peut scanner tous les contrôleurs de domaine dans l'environnement pour détecter les faiblesses de sécurité potentielles.

4.2 Azure AD Connect

Avec cette option le Prestataire assure la synchronisation de l'AD Managé du Client sur un IaaS Orange Business vers son Azure AD via le composant Azure AD Connect .



Ce service permet aux utilisateurs identifiés dans l'AD Managé d'utiliser facilement des ressources définis dans l'Azure AD du Client sans réauthentification comme :

- Office 365
- Exchange Online
- Sharepoint Online
- Teams
- Ou utiliser Azure AD comme source fiable externe d'authentification pour les applications SaaS (ServiceNow, Google, Salesforce, SAP, etc.)

Pour accéder à cette option il faut héberger le service Azure AD Connect dans le domaine Active Directory managé du Client et configurer la connexion avec son Tenant Azure.

Prérequis

1- **Infrastructure**

Ci-dessous les prérequis minimums pour l'Azure AD Connect.

Forest version	Windows Server Min	vCPU	RAM	Disque 1	Disque 2	Classe
Min 2003	Windows 2016 member domain	2	6	100	70	Silver

Nombre d'objets dans Active Directory	vCPU	RAM	Disque 1	Disque 2
Moins de 10 000	2	6	100	70
Entre 10 000 et 50 000	4	6	100	70
Entre 50 000 et 100 000	6	16	100	100
Entre 100 000 et 300 000	8	32	100	300
Entre 300 000 et 600 000	8	32	100	450
Plus de 600 000	8	32	100	500

A Noter, à partir de 100 000 objets, la version Standard de SQL Server 2019 est requise. Pour des raisons de performance, il est préférable de l'installer localement. Les valeurs présentées dans le tableau ci-dessus sont valides uniquement pour l'installation d'Azure AD Connect. Si SQL Server est installé sur le même serveur, de la mémoire, des lecteurs et des capacités processeurs supplémentaires sont nécessaires.

L'usage de Domain Controller en ReadOnly de l'AD Managé n'est pas permis. Le Prestataire héberge avec le service Azure AD Connect des Domain Controller en lecture écriture.

Dans sa documentation Microsoft liste les adresses et hosts public qui doivent être accessible depuis le serveur Azure AD Connect pour fonctionner correctement avec le Tenant Client chez Azure.
Cette liste est construite par famille de produit et doit donc être intégrée dans le Parefeu du Client ou à défaut autorisée dans son Proxy. En plus, le serveur nécessite l'usage du TLS 1.2 minimum pour fonctionner.

2- Droits d'accès pour la gestion de l'Azure AD Connect

L'installation du service nécessite les droits suivants :

- **Compte d'administrateur local** : l'administrateur qui installe Azure AD Connect et qui a des autorisations d'administrateur local sur l'ordinateur. Cela sera un compte Administrateur Orange dans le domaine du client.
- **Compte d'administrateur d'entreprise AD DS** : utilisé de façon facultative pour créer le compte de connecteur AD DS requis.
- **Compte d'administrateur général Azure AD.** Utilisé pour créer le compte de connecteur Azure Active Directory et configurer Azure Active Directory. Nous devrons avoir un accès Global Administrator sur le Tenant Azure du Customer pour mener à bien nos actions.
- **Compte d'administrateur système SQL** (facultatif) : utilisé pour créer la base de données ADSync lors de l'utilisation de la version complète de SQL Server. L'instance SQL Server peut être locale ou distante de l'installation d'Azure AD Connect et nous nous référerons aux abaques des Database Manager.

L'administration du service nécessite les droits suivants :

- **Compte de connecteur AD DS** : utilisé pour lire et écrire des informations dans Windows Server Active Directory à l'aide de services de domaine Active Directory (AD DS).
- **Compte de service ADSync :** utilisé pour exécuter le service de synchronisation et accéder à la base de données SQL Server.
  Compte de connecteur Azure AD. Utilisé pour écrire des informations dans Azure AD.

3- Mise en place de la sécurité renforcée

Comme une partie ou la totalité de l'annuaire Active Directory est exposé sur Internet, nous préconisons de mettre en place l'authentification renforcée Multi Factor Authentication (MFA).
Le niveau de service minimum pour le MFA est celui de Microsoft Azure pour tous les comptes Azure AD sans aucune discrimination.
Les plans Azure AD P1 et P2 sont disponibles en option tarifée auprès d'Orange Business et Microsoft et apportent une granularité dans le verrouillage des accès, l'usage discriminatoire par compte, horaire, emplacement géographique, adresse IP ou périphérique de connexion. Pour une couverture de service SaaS plus large nous proposons le service OKTA présenté ci-dessous.

5 Conditions de prix

5.1 Prix

La tarification du Service est composée :

- Des frais d'accès au service « Managed AD » intégrant toutes les tâches mentionnées dans le RACI d'implémentation et indexé sur le nombre de contrôleurs de domaine à installer (minimum 2)
- D'un récurrent mensuel couvrant les activités liées au maintien en conditions opérationnelles du service « Managed AD » indexé sur le nombre de contrôleurs de domaine (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.

6 Accès au Service

6.1 Prérequis

Le Service « Managed AD » 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 service managé Managed AD.

6.2 Mise en service

Le Prestataire s'appuie sur un document SRF (Service Request Form) que le Client doit remplir pour la mise en service.

Ce document a pour but de présenter les paramétrages standards que le Prestataire applique et de recueillir les besoins Client (éléments variables) afin de finaliser l'architecture à déployer.

Ce document permet de recueillir des éléments concernant deux parties :

1. Architecture physique de l'Active Directory
   - Le nombre de VM minimum
   - La localisation des VMs
   - Le dimensionnement en vCPU, vRAM, disque de chaque VM
   - Plan d'adressage des contrôleurs de domaine
2. Les éléments logiques de la configuration du service.
   - Le nom de chaque VM
   - Le niveau fonctionnel de la forêt et du domaine
   - L'OS requis sur les contrôleurs de domaine
   - Nom du domaine
   - Le nom du site « active directory » par défaut « Default First Site »
   - Le nom des OUs de 1er niveau soit en prenant ceux choisis par le client, soit en prenant en compte une liste de noms issus des pratiques courantes d'Orange Business
   - Le nom de l'OU sur laquelle une délégation personnalisée sera faite

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

	Tâches	OBS	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
4	Déploiement et installation du rôle Active Directory et du rôle de serveur DNS	R	
5	Configuration du rôle selon les invariants OBS (cf. bonnes pratiques)	R	I
6	Configuration des éléments variables de l'architecture physique présents dans la SRF (OU, GPO, …)	R	I
7	Configuration des éléments variables de l'architecture logique présents dans la SRF (OU, GPO, …)		
8	Installation et configuration de l'outil PingCastle (option)	R	
9	Ouverture des flux entre les serveurs membres et les contrôleurs de domaine	R	I
10	Fourniture d'un compte de domaine héritant de la délégation de l'OU désignée par le client	R	I
11	Configuration de la sauvegarde, de la supervision et du stockage sécurisé des mots de passe	R	
12	Configuration des indicateurs techniques : disponibilité, occupation vCPU, ram, disque	R	I
13	Audit par Ping Castle, partage et application des recommandations	R	

Tâches		OBS	CLIENT
R : Réalisateur – A : Accountable (Responsable) – C : Consulté – I : Informé – V : Valideur			

6.3 Maintien en conditions opérationnelles

Le Prestataire assure les opérations pour le maintien en conditions opérationnelles de l'AD en complément des OS requis pour rendre le service.

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.

	Tâches	OBS	CLIENT
1	MCO des Services Windows AD : contrôleur de domaine, DNS, rôle FSMO, AD DS, Kerberos, Netlogon, réplication	R	
2	Services Windows AD : création des GPO et leur modification (hors OU déléguée) – via le processus de Gestion des changements	R	
3	Services Windows AD : Création, modification et suppression des comptes utilisateurs, des comptes ordinateurs, des groupes AD (hors OU déléguée) – via le processus de Gestion des changements	R	
5	Gestion des autorisations applicatives		R
6	Services Windows AD : Création, modification et suppression des comptes utilisateurs, des comptes ordinateurs, des groupes AD (uniquement OU déléguée) – via le processus de Gestion des changements		R
7	Services Windows AD : création des GPO et leur modification dans le cadre de Gestion des changements (uniquement OU déléguée) – via le processus de Gestion des changements		R
8	Utilisation de la délégation sur l'OU désignée		R
9	Supervision (décrite dans le paragraphe qui suit)	R	
10	Sauvegarde (décrite dans le paragraphe qui suit)	R	
11	Restauration du service AD – via le processus de Gestion des changements	R	
12	Expression de besoin pour toute demande hors catalogue de changements	C,I	R
13	Etude des demandes d'évolution et réalisation effectuées dans le cadre de la gestion des changements	R	
14	Maintien en condition opérationnelle de la relation d'approbation externe (applicable au service du domaine d'infrastructure dédié)		A,R
15	Evolution de l'architecture physique et logique du service AD	R	C,I
16	Signaler toute évolution des besoins l'Active Directory afin d'ajuster le gabarit des VMs ou le nombre de contrôleurs de domaine rendant le service	C,I	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, le Prestataire assure la supervision suivante pour l'AD Managé :

- Les services clés tels que les contrôleurs de domaine, les serveurs DNS et les services de réplication pour assurer leur disponibilité en continu. Les données sur la performance de l'environnement sont collectées et stockées pour analyse.
- Les métriques clés qui peuvent déclencher des alertes en cas de problèmes critiques, tels que les erreurs de réplication ou les temps de réponse lents des requêtes DNS.
- Le traitement des alertes remontées pas la supervision.

Sauvegarde

En plus de la sauvegarde assurée au niveau OS Managé, pour garantir la disponibilité du service en cas de problèmes, le Prestataire réalise une sauvegarde de l'Active Directory Managé via la fonctionnalité Windows Backup sur un disque dédié afin de permettre une restauration plus facile. La rétention de la sauvegarde sera liée à la volumétrie du système et des objets de l'Active Directory, elle pourra être augmentée si nécessaire en augmentant la volumétrie du disque dédié à cette sauvegarde. La sauvegarde est effectuée durant la fenêtre horaire suivante : 22h00 à 6h00.

Le Prestataire surveille la solution de sauvegarde pour garantir sa bonne exécution. En cas de besoin, le Prestataire décide en concertation avec le Client la restauration d'une copie de sauvegarde. Des mécanismes de protection apportées par la technologie Active Directory protègent des effacements accidentels de certaines données, la mise en place de ces mécanismes fait partie des bonnes pratiques que nous appliquons lors du déploiement du service.

Administration

Sur base des outils de supervision le Prestataire suit les métriques d'usage de l'AD. Ces métriques lui 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

7 Support

Nous présentons ci-dessous le support spécifique que nous apportons au service Managed AD.

7.1 Gestion des changements

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

7.1.1 Demandes au catalogue

Les demandes de changement sont présentées dans le § 8 « Catalogue de changements ». Elles sont classées selon 2 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 ▪ Nécessite une tâche complexe pour le traitement	2

Le Prestataire prépare la réalisation d'un changement en concertation avec le Client. Une fois la demande est traitée, le Client est prévenu pour valider et clôturer la demande.

7.1.2 Demandes hors catalogue

Le Client peut faire une demande hors catalogue et fournir les détails. Le Prestataire organise si nécessaire un point téléphonique d'une ½ h avec le Client 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 AD 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.

8 Catalogue de changements

N° Tâche	Nom des tâches	Catégorie
AD0001	Création compte utilisateur	Simple
AD0002	Suppression compte utilisateur	Simple
AD0004	Renommer un compte utilisateur	Simple
AD0005	Déplacer un compte utilisateur	Simple
AD0006	Activer ou désactiver un utilisateur	Simple
AD0007	Trouver un compte d'utilisateur	Simple
AD0008	Réinitialiser les mots de passe	Simple
AD0009	Verrouiller uncomptes	Simple
AD0010	Débloquer un compte	Simple
AD0011	Définir la date d'expiration d'un compte	Simple
AD0012	Modifier l'appartenance à un groupe d'utilisateurs	Simple
AD0014	Rajouter un membre à un groupe	Simple
AD0017	Supprimer un membre d'un groupe	Simple
AD0018	Supprimer un groupe	Simple
AD0019	Renommer un groupe	Simple
AD0021	Trouver un groupe	Simple
AD0022	trouver des groupes dans lesquels un utilisateur est membre	Simple
AD0023	Définir une date d'expiration pour un groupe sur un compte	Simple
AD0024	Créer un compte ordinateur	Simple
AD0025	Ajouter 1 compte d'ordinateur dans un groupe	Simple
AD0026	Supprimer 1 compte d'ordinateur	Simple
AD0028	Désactiver 1 compte d'ordinateur	Simple
AD0029	Activer 1 compte d'ordinateur	Simple
AD0035	Trouver un dossier partagé	Simple
AD0036	Trouver une imprimante	Simple
AD0003	Modifier les propriétés d'un compte utilisateur	Simple
AD0013	Création d'un groupe	Simple
AD0015	Changer la portée du groupe	Simple
AD0016	Modifier les propriétés d'un groupe	Simple
AD0020	Utilisation des groupes pour attribuer des droits aux ressources	Simple
AD0032	Suppression d'une file d'impression (pas dans l'AD)	Simple
AD0034	Suppression des dossiers partagés	Simple
AD0102	Lier l'objet de stratégie de groupe à l'unité d'organisation	Simple
AD0110	Création d'une unité d'organisation	Simple
AD0114	Suppression d'objets dans les OU- unités organisationnelles	Simple
AD0219	Afficher les détenteurs du rôle de maître d'opérations en cours	Simple
AD0223	Identification des serveurs du catalogue global	Simple
AD0224	Première analyse expert AD pour qualifier un besoin hors catalogue ou fonctionnel	Simple
AD0130	Supprimer 1 approbation	Simple
AD0027	Réinitialiser un compte d'ordinateur	Simple

AD0030	Configurer un ordinateur pour l'utilisation d'un nom DNS différent	Simple
AD0033	Publier un dossier partagé	Simple
AD0111	Suppression d'une OU	Simple
AD0113	Ajouter 1 objet à 1 OU	Simple
AD0123	Restaurer un objet de la corbeille	Simple
AD0146	Valider une approbation	Simple
AD0178	Installation 1 outil d'administration de serveur distant pour AD	Simple
AD0204	Déterminer si un contrôleur de domaine est un serveur DNS	Simple
AD0249	Ajout d'un sous-réseau	Simple
AD0250	Associer un objet de sous-réseau existant à un site	Simple
AD0258	Supprimer un objet serveur d'un site	Simple
AD0263	Déterminer si un serveur est un serveur tête de pont préféré	Simple

N° Tâche	Nom des tâches	Complexité
AD0105	Générer le jeu résultant d'objets de stratégie de groupe	Complexe
AD0106	Sauvegardez l'objet de stratégie de groupe sur le système de fichiers à l'aide de l'option Sauvegarde GPMC.	Complexe
AD0031	Publier une imprimante	Complexe
AD0108	Ajustez certaines des valeurs de l'objet de stratégie de groupe lorsqu'il est déplacé vers le domaine de production	Complexe
AD0109	Importation avec GPMC dans le domaine de production	Complexe
AD0112	Délégation des permissions d'administration	Complexe
AD0115	Création d'un filtre WMI	Complexe
AD0116	Déterminer la durée de rétention des objets supprimés	Complexe
AD0120	Activer la corbeille Active Directory	Complexe
AD0122	Déléguer une opération de la corbeille Active Directory	Complexe
AD0133	Suppression de l'approbation de la forêt	Complexe
AD0138	Activer l'authentification sélective sur une approbation externe	Complexe
AD0139	Activer l'authentification sélective sur une approbation de forêt	Complexe
AD0140	Activer l'authentification à l'échelle du domaine sur une approbation externe	Complexe
AD0141	Activer l'authentification à l'échelle de la forêt sur une approbation de forêt	Complexe
AD0147	Réinitialiser le mot de passe d'une relation d'approbation	Complexe
AD0148	Sauvegarde d'Active Directory et des composants associés	Complexe
AD0166	Sauvegarde de l'objet de stratégie de groupe sur le système de fichiers à l'aide de l'option Sauvegarde GPMC.	Complexe
AD0167	Restaurer une GPO	Complexe
AD0179	Nettoyer les métadonnées	Complexe
AD0188	Mettre à jour l'objet membre de la réplication DFS ou FRS	Complexe
AD0193	Vérifier les performances du processeur	Complexe
AD0194	Vérifier l'utilisation de la mémoire	Complexe
AD0195	Vérifier la longueur de la file d'attente du disque	Complexe
AD0196	Vérifier les compteurs NTDS	Complexe
AD0197	Vérifier la bande passante totale	Complexe
AD0198	Vérifier l'utilisation de l'espace disque	Complexe
AD0227	Vérifier l'état du volume système partagé	Complexe
AD0203	Déterminer si le contrôleur de domaine est un serveur tête de pont préféré	Complexe
AD0210	Vérification du transfert d'un rôle de maître d'opérations	Complexe
AD0216	Déterminer le propriétaire du rôle ISTG pour un site	Complexe
AD0224	Vérifier l'état de préparation du catalogue global	Complexe
AD0225	Surveiller la progression de la réplication du catalogue global	Complexe
AD0226	Vérifier les enregistrements DNS du catalogue global	Complexe
AD0229	Modifier le quota alloué au dossier de stockage intermédiaire	Complexe
AD0230	Déplacement de la zone de transit SYSVOL	Complexe
AD0231	Déplacement manuel de SYSVOL	Complexe
AD0232	Modifier le chemin d'accès du SYSVOL	Complexe
AD0235	Vérifier l'état des partages SYSVOL et Netlogon	Complexe
AD0240	Configuration d'une source de temps pour la forêt	Complexe
AD0241	Configuration de l'heure sur l'émulateur PDC de la racine de la forêt	Complexe

AD0242	Configuration d'une source de temps fiable sur un ordinateur autre que le PDC	Complexe
AD0244	Activer la journalisation du débogage du service de temps Windows	Complexe
AD0245	Ajout d'un nouveau site active directory	Complexe
AD0246	Créer l'objet d'un site	Complexe
AD0247	Créer un objet de lien d'un site	Complexe
AD0248	Créer un objet de sous-réseau	Complexe
AD0251	Etablir la Liaison de sites via la réplication	Complexe
AD0252	changer les propriétés de liaison d'un site	Complexe
AD0253	Déplacement d'un contrôleur de domaine vers un autre site	Complexe
AD0254	Supprimer un site	Complexe
AD0255	Configurer un contrôleur de domaine en tant que serveur tête de pont préféré	Complexe
AD0256	Configurer un contrôleur de domaine pour qu'il ne soit pas un serveur préféré	Complexe
AD0259	Supprimer un objet de lien d'un site	Complexe
AD0260	Suppression de l'objet d'un site	Complexe
AD0261	Surpression d'un objet sous-réseau	Complexe
AD0262	Configurez le coût de liaison de site pour établir une priorité pour la réplication	Complexe
AD0264	Afficher la liste de tous les serveurs têtes de pont préférés	Complexe
AD0265	Déplacer un objet serveur vers un nouveau site	Complexe
AD0266	Vérifier qu'une IP correspond à un sous-réseau et déterminer l'association de site	Complexe
AD0267	Vérifier que la réplication a réussi sur un contrôleur de domaine	Complexe
AD0268	Vérifier l'état de préparation du catalogue global	Complexe
AD0269	Vérifier le journal du service d'annuaire	Complexe
AD0270	Vérifier le journal de réplication DFS	Complexe
AD0271	Créer un rapport DFS-R	Complexe
AD0272	Effectuer un « GPRESULT »	Complexe