



le cnam
École d'ingénieurs eichnam



ESSILOR
MIEUX VOIR LE MONDE

Alexandre Labrousse
Ingénieur Informatique en Apprentissage
Spécialité Systèmes d'information
Master 2, FIP 3

Déploiement et Exploitation d'Oracle Enterprise Manager 12c

MÉMOIRE D'INGENIEUR

Sous la direction de

Tuteur pédagogique :
Monsieur Nicolas TRAVERS
Maître de Conférences en informatique
Enseignant-chercheur
CNAME - Paris

Maître d'apprentissage :
Monsieur Jean-Luc GUERIN
Administrateur Base de données Séniior
ESSILOR FRANCE

Année Universitaire 2015/2016

Alexandre Labrousse
Ingénieur Informatique en Apprentissage
Spécialité Systèmes d'information
Master 2, FIP 3

Déploiement et Exploitation d'Oracle Enterprise Manager 12c

MÉMOIRE D'INGENIEUR

Sous la direction de

Tuteur pédagogique :
Monsieur Nicolas TRAVERS
Maître de Conférences en informatique
Enseignant-chercheur
CNAM - Paris

Maître d'apprentissage :
Monsieur Jean-Luc GUERIN
Administrateur Base de données Séniior
ESSILOR FRANCE

Année Universitaire 2015/2016

Avant-propos

Le présent mémoire rentre dans le cadre de l'obtention du diplôme de fin d'étude du cycle ingénieur informatique du Conservatoire National des Arts et Métiers (CNAM), spécialité systèmes d'information.

A l'issue de mon rapport de recherche de deuxième année sur la *supervision informatique*, de nombreuses questions sont restées en suspens. En effet plusieurs aspects techniques, méthodologiques et fonctionnels de notre logiciel de supervision de base de données (OEM) restaient encore à découvrir. C'est donc naturellement qu'est venue l'idée du sujet de ce mémoire qui porte sur le déploiement de la nouvelle version d'Oracle Enterprise Manager Cloud Control entreprise durant cette dernière année de Master. En effet, Essilor a profité de l'arrivée de la nouvelle version de son principal logiciel de supervision pour bénéficier des améliorations liées à l'administration de ses bases et des nouvelles fonctionnalités proposées par le logiciel. Ce projet m'a donc permis de mettre en pratique les connaissances acquises durant les années précédentes chez Essilor. J'ai également pu appliquer les méthodologies de gestion de projet acquises au CNAM directement à cette mission.

Nous avons été confrontés à plusieurs difficultés lors de ce projet. En effet, la phase de conduite de changement destinée à rendre reproductible toutes les opérations techniques réalisées et à exploiter les nouvelles fonctionnalités par les équipes administrateurs base de données en Asie a représenté un vraie défi pour notre équipe.

Malgré les contraintes soulevées par le déploiement de la nouvelle version d'OEM, le calendrier prévisionnel a pu être respecté. Le déploiement s'est finalisé à la date prévue et la solution Cloud Control est utilisée par notre équipe pour superviser nos bases les plus stratégiques.

Remerciements

En préambule, je veux adresser tous mes remerciements aux personnes avec lesquelles j'ai pu échanger et qui m'ont aidé pour la rédaction de ce mémoire.

Je tenais à remercier tout d'abord mon tuteur d'apprentissage Monsieur Nicolas Travers. Je le remercie de m'avoir encadré, orienté, aidé et conseillé pour la rédaction de mon mémoire.

J'adresse mes sincères remerciements à toute l'équipe d'administrateurs base de données qui par leurs paroles, leurs écrits, leurs conseils et leurs critiques ont guidé mes réflexions durant ma mission.

Je remercie Monsieur Lamine Bouciouf qui m'a accordé son temps et a su me guider pendant la phase de réalisation du projet.

Enfin, je remercie Monsieur Luc Perrin-Turenne et Monsieur Jean-Luc Guerin pour les références qu'ils m'ont transmises au sujet de mes recherches.

Table des matières

<i>Avant-propos</i>	4
<i>Remerciements</i>	5
<i>Table des matières</i>	6
<i>Liste des figures</i>	9
<i>Liste des tableaux</i>	9
<i>Table des sigles et abréviations</i>	10
I <i>Introduction</i>	12
I.1 Présentation de l'entreprise	12
I.2 Présentation du département	14
I.3 Présentation du poste	15
I.4 Présentation de la mission	16
II <i>Définition du projet</i>	17
II.1 Expression du besoin	17
II.1.1 Note de cadrage	17
II.2 Etude d'avant-projet.....	20
II.2.1 Présentation du produit	20
II.2.2 Architecture technique d'OEM Cloud Control	20
II.3 Cahier des charges	23
II.3.1 Les contraintes.....	23
II.3.2 Critères de satisfaction	25
II.3.3 Détail des versions logicielles déployées	26
II.3.4 Budget & Délais	26
II.3.5 Cahier des charges fonctionnel	28
II.4 Etude de faisabilité	29
II.4.1 Etude Réseaux	29
II.4.2 Ressources allouées.....	30
II.4.3 Les risques et les impacts	31
III <i>La solution Oracle Enterprise Manager Cloud Control 12c</i>	33
III.1 Analyse de l'architecture d'OEM	33
III.1.1 Cloud Control Console	34
III.1.2 Oracle Management Agent.....	35
III.1.3 Gestion et découverte des cibles supervisées	36

III.1.4	Oracle Management Service.....	37
III.1.5	Oracle Management Repository.....	38
III.1.6	Flux de données.....	40
III.2	Les choix d'implémentation d'OEM Cloud Control 12c.....	42
III.2.1	Définition du nombre d'environnements Cloud Control mis en œuvre	44
III.2.2	Environnement de production Vs Environnement de non-production	44
III.2.3	Décision du choix d'architecture d'Oracle Cloud Control.....	45
III.2.4	Décision concernant sur le choix d'architecture de la base de données Repository..	46
III.2.5	Décision concernant le choix d'architecture d'Oracle Management Server	47
III.2.6	Décision concernant le choix de regroupement du serveur OMS et de la base OMR	48
III.3	Conclusion	49
IV	Réalisation.....	50
IV.1	Introduction.....	50
IV.1.1	Installation d'une base de données Repository.....	51
IV.1.2	Etape 1 : Installation du logiciel Grid Infrastructure (facultative).....	52
IV.1.3	Etape 2 : Installation du logiciel de base de données.....	53
IV.2	Configuration de la base de données Repository.....	57
IV.2.1	Renommage des fichiers de données Cloud Control.....	58
IV.2.2	Désactivation de l'optimisateur de récupération automatique des statistiques	58
IV.2.3	Création de groupes de redo logs additionnels	59
IV.2.4	Implémentation des HugePages	60
IV.2.5	Activation de la base de données Flashback (Flashback Database)	61
IV.2.6	Activation du Block Change Tracking.....	62
IV.3	Exécution du Kit de prérequis de OEM en mode indépendant	62
IV.3.1	Installation et Configuration d'Oracle Enterprise Manager Cloud Control	63
IV.3.2	Réactivation de l'optimisateur de récupération automatique des statistiques	63
IV.3.3	Mise en œuvre des variables d'environnement sur le serveur-hôte OMS	63
IV.3.4	Planification des purges périodiques des fichiers logs de Cloud Control	64
IV.3.5	Mise en place de la politique de sauvegarde des composants de Cloud Control	65
IV.4	Configuration de la console Cloud Control.....	65
IV.4.1	Mise en place des méthodes de notification.....	66
IV.5	Conclusion	69
V	Après Projet.....	70

V.1	Conduite du changement	70
V.1.1	Détails et explications de l'administration de Cloud Control	70
V.1.2	Analyse des améliorations d'administration	71
V.2	Maintenance opérationnelle	76
V.2.1	Alarmes, alertes et métriques de supervisions.....	76
V.2.2	Configuration des règles d'incidents dans OEM 12c	78
VI	Conclusion	79
	Glossaire	80
	Références Bibliographiques	81
	Annexes	82
	Table des matières.....	82
I.	11gR2 Database Installation (11.2.0.4) on Linux server x64	83
II.	Oracle Enterprise Manager Cloud Control 12c Installation.....	99
1.	Starting Cloud Control and all Its Components	106
2.	Stopping Cloud Control and all Its Components.....	107
III.	OEM 12c Agent installation & Database Discovery with Cloud Control.....	108
IV	Planning prévisionnel	119
	Implémentation et exploitation d'Oracle Enterprise Manager CC v12c.....	120
	Installing and exploiting Oracle Enterprise Manager CC v12c.....	120

Liste des figures

Figure 1: Présentation du département	14
Figure 2: Schéma du processus de notification	18
Figure 3: Planning prévisionnel	27
Figure 4: Architecture d'Oracle Enterprise Management Cloud Control 12c.....	33
Figure 5: Flux de données.....	40
Figure 7:Mise en place des adresses mails des administrateurs	67
Figure 8: Ecran de l'emploi du temps des notifications à l'œuvre chez Essilor Error! Bookmark not defined.	
Figure 9: Ecran de l'emploi du temps des notifications à l'œuvre chez Essilor	68
Figure 10: Ecran de mise en place de la période rotation chez Essilor.....	68
Figure 11: Fenêtre de création d'une accréditation	72
Figure 12: Fenêtre de création d'une accréditation	Error! Bookmark not defined.
Figure 13: Fenêtre de gestion de délégation des privilèges	73
Figure 14: Fenêtre d'audit de control OEM 12c	74

Liste des tableaux

Tableau 1: Prérequis réseaux minimum nécessaires de connexion	30
Tableau 2: Ordre de grandeur des sites supervisés.....	45
Tableau 3: Adéquation entre la taille du site supervisé et la taille recommandée des redo logs	56
Tableau 4: Statut actif de l'Auto Optimizer Stats Collection	59
Tableau 5: Hugepage	60
Tableau 6: Statut inactif de l'Auto Optimizer Stats Collection	63
Tableau 7: Commandes d'arrêt et de démarrage de l'agent.....	64
Tableau 8: Objectifs et méthodes déployées pour sécuriser OEM Cloud Control	75
Tableau 9: Seuils d'alertes OEM	77
Tableau 10: Règles d'incident OEM	78

Table des sigles et abréviations

- ASLM** : Application Service Level Management / Niveau de service d'application
- ASM** : Automatic Storage Management / Gestion de Stockage Automatique
- ASMM** : Automatic Shared Memory Management/Gestion du Partage de la Mémoire Automatique
- BP** : Best Practice / Meilleure méthode
- CC** : Cloud Control / OEM 12c
- CFC** : Cold Failover Cluster
- CNAM** : Conservatoire National des Arts et Métiers
- CPU** : Central Processing Unit / Unité Centrale de Calcul
- DBA** : Database Administrator / Administrateur Base de données
- DBCA** : Database Configuration Assistant / Assistant de Configuration de base de données
- DR** : Disaster Recovery / Récupération après Désastre
- ERP** : Enterprise Ressource Planning / Gestion des ressources d'entreprise
- EUS** : Enterprise User Security
- FMA** : Functional Maintenance Applicative / Equipe de Maintenance Fonctionnelle
- FRA** : Fast Recovery Area / Zone de Récupération Rapide
- GC** : Grid Control / OEM 10g
- GI** : Grid Infrastructure / Infrastructure Grid
- GigE** : Gigabit Ethernet
- HA** : High Availability / Haute Disponibilité
- HTTP/HTTPS** : Hypertext Transfer Protocol / Hypertext Transfer Protocol Secure
- ICMP** : Internet Control Message Protocol / Protocole de Control de Message Internet
- JDBC** : Java Database Connectivity / Connectivité de base de données Java
- MAA** : Maximum Availability Architecture / Architecture de Disponibilité Maximale
- NAS** : Network Attached Storage / Stockage Réseaux
- NC** : Named Credential / Accréditation nominative
- NLS** : National Language Support / Support de Langage National
- OAS** : Oracle Application Server / Serveur d'Application Oracle
- OCI** : Oracle Call Interface
- ODG** : Oracle Data Guard
- OEM** : Oracle Enterprise Manager
- OHS** : Oracle HTTP Server
- OMA** : Oracle Management Agent
- OMF** : Oracle Managed File
- OMR** : Oracle Management Repository / Base de données Repository
- OMS** : Oracle Management Server
- ORON** : Real Application Clusters (RAC) One Node
- OUI** : Oracle Universal Installer / Installateur Universel Oracle
- PSU** : Patch Set Update / Groupe de mises à jour
- RAC** : Real Application Cluster
- RAM** : Random Access Memory / Mémoire à Accès Aléatoire

RMAN : Oracle Recovery Manager / Gestionnaire de Récupération Oracle

SAN : Storage Array Networks / Réseau de Stockage

SGA : System Global Area / Zone Globale Système

SGBD : Système de Gestion de Base de données

SLA : Service Level Agreement / Contrat de niveau de service

SLB : Server Load Balancing / Serveur à Répartition des charges

SMTP : Simple Mail Transfer Protocol / Protocole de transfert de Mail

SSL : Secure Socket Layer

TMA : Tierce Maintenance Applicative / Equipe de Maintenance Technique

T-Center : Developer Team / Equipe de développeur

WLS : WebLogic Server

WWSCP : World Wide Supply Chain / Logistique

I Introduction

Dans le cadre de ma formation d'ingénieur informatique en apprentissage j'ai été recruté par ESSILOR en tant qu'apprenti administrateur de bases de données Oracle et Oracle Application pour une durée de trois ans.

J'ai été intégré au sein de l'équipe DBA Oracle (Administrateur de base de données) du département logistique WWSCP (World Wide Supply Chain Project) qui appartient à la branche logistique d'Essilor sur le site de Créteil.



Cette équipe est composée de six DBA Oracle (trois en France et trois en Asie) et d'un manager qui pilote l'activité de cette équipe.

Il s'agit d'une équipe opérationnelle qui est chargée de la maintenance de toutes les bases de données Oracle utilisées dans les applications gérées dans le département WWSCP.

Cette équipe joue un rôle clé au sein de ce département car elle gère notamment les bases de production. Ces bases sont stratégiques car elles sont directement liées à l'activité de ce département.

Je vais maintenant vous présenter le contexte de mon travail, l'équipe dans laquelle j'effectue mon apprentissage, ainsi que la mission qui m'a été confiée dans le cadre de ce mémoire.

I.1 Présentation de l'entreprise

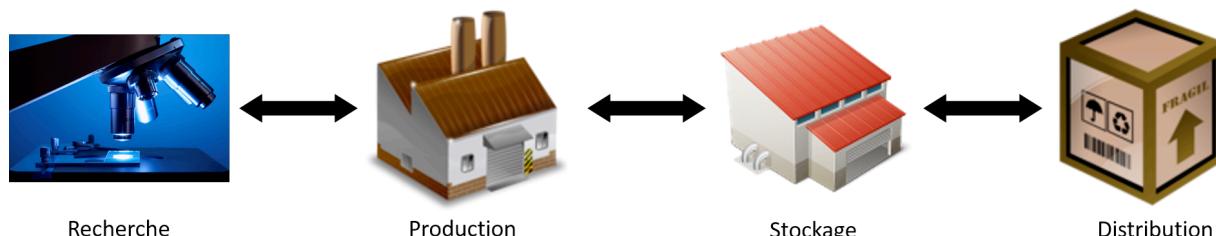
Activités

Essilor International, leader mondial de la production de verre ophthalmiques, doit sa position de leader tant à la qualité de ses produits que de ses services. En 2015, le chiffre d'affaire de la société a augmenté de 18.4 % par rapport à l'année 2014 avec 6 716 M€. Essilor fait partie de l'indice CAC40 depuis 2005.



Structure Organisationnelle

La majeure partie de l'activité d'Essilor s'oriente sur les 4 axes principaux suivants :



Ces axes sont gérés au travers de son système d'information qui a énormément évolué depuis la création de l'entreprise.

Système d'Information

Aujourd'hui, c'est lui qui coordonne les activités de l'entreprise, qui véhicule l'information au sein de l'organisation, et qui représente l'ensemble des ressources et systèmes du groupe ayant pour but :

- La saisie des informations
- Le stockage des informations
- Le traitement des informations
- La restitution des informations
- La transmission des informations
- etc.

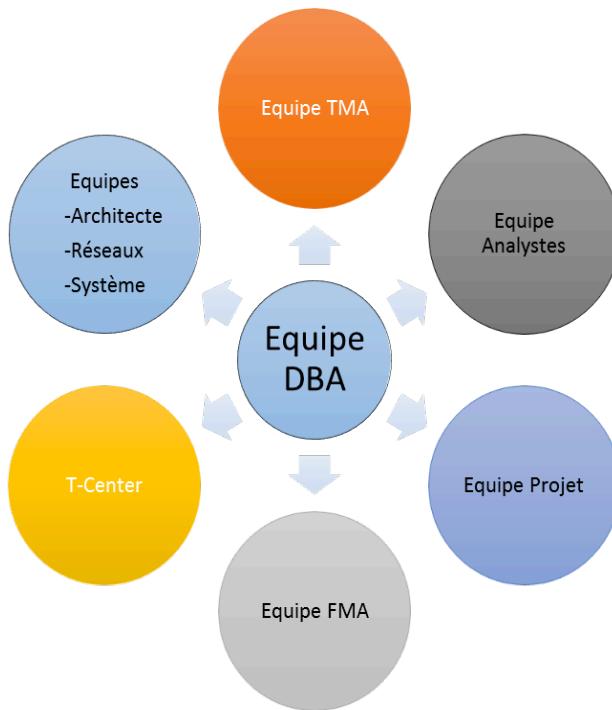
Différents supports sont utilisés pour matérialiser ces informations dans le SI tels que :

- Les bases de données (Oracle, SQL Server, etc.)
- Les serveurs de fichiers,
- Les intranets,
- Les GED,
- etc.



I.2 Présentation du département

Figure 1: Présentation du département



Chez Essilor, suite à une récente réorganisation des services, l'équipe DBA précédemment basée à Vincennes a rejoint le département WWSCP à Créteil Oudry ; *World Wide Supply Chain Project*, service dans lequel j'évolue dans le cadre de mon apprentissage à Essilor. Elle travaille conjointement avec les équipes Projets / TMA (*Tierce Maintenance Applicative*) et FMA (*Functional Maintenance Applicative*) qui sont notamment chargées du support technique et fonctionnel des applications.

De plus, avec les réattributions des responsabilités liées à l'augmentation de la taille de l'entreprise et de son internationalisation, le scope de bases de données gérées par l'équipe DBA s'est considérablement diversifié et élargi ; notamment par la gestion de nouvelles bases anciennement gérées par d'autres équipes travaillant pour l'essentiel à l'étranger.

Le scope couvert par les DBA (Administrateur de bases de données) comprend aujourd'hui un ensemble de bases de données fonctionnant sur plusieurs versions de SGBD (Système de Gestion de Base de Données) notamment Oracle et SQL Serveur, hébergées sur différents OS (Linux, Unix, Windows Server, ...), et sur différents sites (Asie, Europe, US, ...).

Notre équipe maintient plus d'une dizaine de base de données de production. Ces bases sont particulièrement surveillées car elles sont essentielles au fonctionnement de nos modules ERP Oracle Application. De plus nous gérons également des bases de données issues d'environnements de test et d'intégration qui sont principalement utilisés par le T-Center et la TMA.

I.3 Présentation du poste

Pour comprendre et apprendre le métier de DBA, il convient de connaître tout d'abord les différents rôles que l'administrateur base de données doit pouvoir gérer et maîtriser :

- **La conception du modèle de données** : bien qu'elle incombe normalement à l'analyste ou au concepteur, les principes de modélisation des données doivent être parfaitement maîtrisés par le DBA. En effet, les facteurs de dégradation des performances sont en premier lieu liés à la structuration des données.
- **La définition et la gestion des espaces de stockage** : Comme une base de données a besoin de beaucoup de place pour les données, il doit dimensionner les espaces de stockage physiques (ex : Disque dur) et logiques (ex : *Tablespaces*) de façon précise.
- **L'intégrité des données** : il vérifie ou aide à vérifier la cohérence des données de la base afin qu'elles ne rentrent pas en conflit avec les principes du système réel.
- **La gestion des incidents** : il doit créer et tester des solutions de maintien (procédures de récupération) afin d'assurer la continuité de la production en cas d'incidents.
- **Le maintien de la performance** : il doit s'assurer que l'accès aux données se fasse dans un temps raisonnable et que cette performance soit maintenue dans le temps.
- **L'optimisation** : il doit régulièrement et de manière proactive faire des campagnes de mesure afin de débusquer les problèmes de contention ou de temps de réponse avant qu'ils ne deviennent handicapants pour l'exploitation de l'entreprise.
- **Migration et mises à jour** : il doit régulièrement appliquer les mises à jour préconisées par les éditeurs (système et SGBD).

I.4 Présentation de la mission

Mon sujet de mémoire de fin d'étude d'ingénieur CNAM porte sur ma mission principale de cette troisième année d'ingénieur en entreprise. Celle-ci consiste au remplacement progressif de notre logiciel de supervision de bases de données Oracle Enterprise Manager (OEM).

Plus précisément, je vais procéder au remplacement de la version 10g existante de cet outil par sa version la plus récente en 12c.

Je vais directement intervenir dans la partie support du système d'information d'Essilor.

Le premier objectif qui m'a été donné par l'équipe DBA (Database Administrator ou Administrateur de base de données) est d'identifier puis de mettre en place tous les éléments permettant l'implémentation de la version 12c du logiciel, plans de maintenance inclus.

Ce nouvel outil permettrait de faire bénéficier dans un premier temps à l'équipe DBA d'une supervision des bases de données améliorée, de paramétrages plus fins du système d'envoi des alertes ainsi que de métriques plus détaillées pour faciliter la résolution des incidents. Ceci permettant d'optimiser la supervision des bases de données stratégiques de l'entreprise.

Le second objectif de cette mission est double. Je suis chargé d'analyser les nouvelles fonctionnalités du logiciel et de les communiquer à mon équipe afin de lui faire profiter de mes découvertes. Je dois également préparer la conduite du changement afin de faciliter la transition entre les deux versions d'Oracle Enterprise Manager.

Mon sujet se situe donc dans la continuité de mon rapport de recherche rédigé l'année précédente. En effet, celui-ci portait sur la supervision informatique dans lequel ont été développés les enjeux et les méthodologies de la supervision des bases de données ainsi que les potentielles améliorations fonctionnelles et ergonomiques qu'apporterait la montée d'Oracle Enterprise Manager en version 12c.

Cette mission m'a été confiée dans son intégralité, depuis la rédaction de l'expression du besoin jusqu'à la phase d'après projet avec la rédaction du plan de maintenance et du plan de conduite de changement.

Ce projet est soumis au contrôle de notre expert DBA Oracle qui est chargé de ma formation pour les parties techniques de la réalisation. Plus concrètement les phases d'installation de la base de données dépôt et du logiciel Oracle Enterprise Manager seront opérées sur un serveur Linux donné via une connexion à distance. Les étapes suivantes seront, quant à elles, effectuées directement sur l'interface OEM.

Je dispose également d'une documentation spécialisée destinée à me former et à découvrir les spécificités de la version 12c de ce nouvel outil.

Les aspects organisationnels de la mission sont, quant à eux, soumis à mon supérieur, manager d'équipe.

II Définition du projet

Nous allons maintenant définir complètement le référentiel du projet. Nous développerons les éléments du référentiel du projet suivant :

- L'expression du besoin
- L'étude d'avant-projet
- Le cahier des charges
- L'étude de faisabilité

Cette phase est particulièrement importante pour nous car elle va nous permettre de mettre en œuvre une démarche de conduite de projet organisée, cohérente et collective.

II.1 Expression du besoin

Dans le cadre de ma mission de cette troisième année en entreprise je suis chargé de mettre en œuvre toutes les étapes suivantes :

1^{ère} étape : Implémentation et mise en fonctionnement d'Oracle Enterprise Manager 12c

2^{ième} étape : Rédaction des procédures d'installation et de déploiement du logiciel

3^{ième} étape : Analyse et transmission à l'équipe DBA des nouvelles fonctionnalités phares de la nouvelle version de l'outil

4^{ième} étape : Mise en œuvre de la conduite du changement du logiciel

La date de fin de la mission est fixée pour la fin Juin 2016.

II.1.1 Note de cadrage

Nous expliquerons dans cette partie les principaux enjeux liés au déploiement de la nouvelle version d'OEM. Après avoir explicités les raisons de cette mission, nous nous intéresserons aux objectifs que nous nous sommes fixés permettant de répondre à la problématique exposée.

II.1.1.1 Contexte

En ce jour, le département *World Wide Supply Chain* (WWSCP ou Logistique) dans laquelle l'équipe DBA opère possède une architecture informatique hétérogène en raison du renouvellement progressif du parc informatique et logiciel d'Essilor (machines, systèmes d'exploitation, ordinateurs de bureau, licences logicielles etc.)

Comme toute société qui possède des systèmes informatiques, Essilor doit gérer l'obsolescence de ses systèmes et de ses applications.

En effet une partie de nos serveurs et de nos applications vieillissantes sont renouvelées progressivement. Essilor possède de ce fait des environnements techniques différents adaptés aux applications plus ou moins récentes fonctionnant sur nos systèmes.

En raison de l'hétérogénéité de ces environnements, notre parc de bases de données est également diversifié car elles sont hébergées sur des architectures techniques adaptées à ces applications.

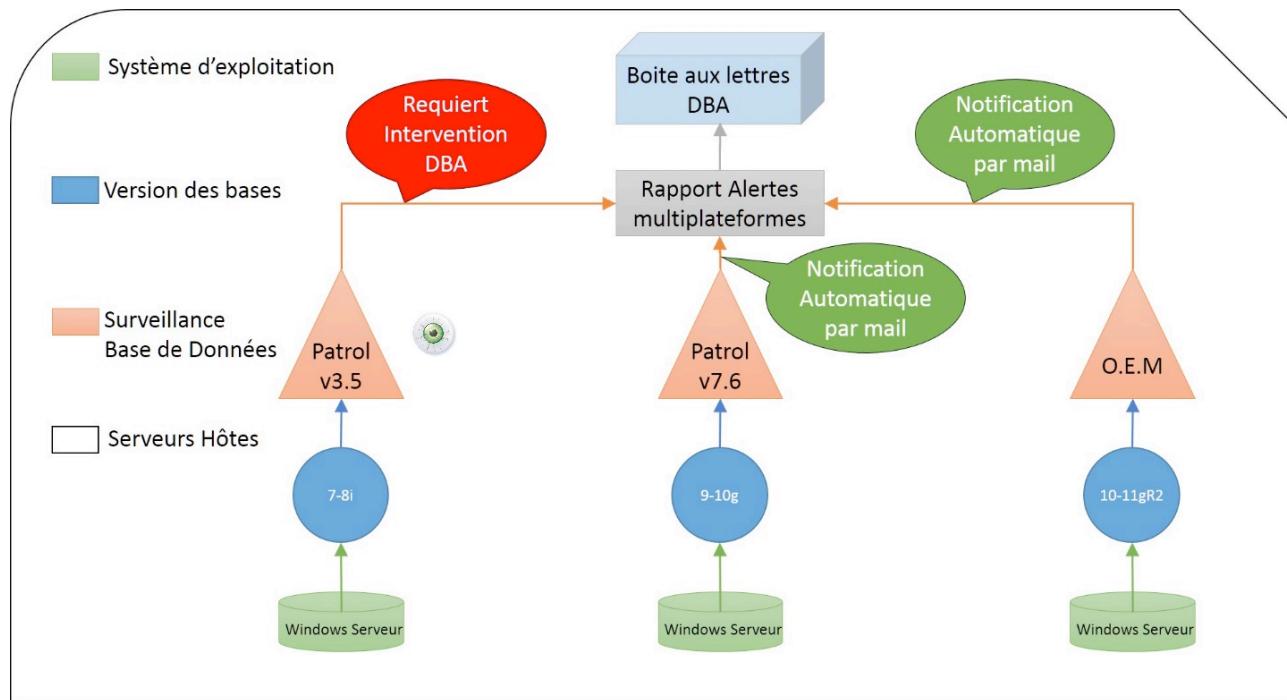
Nous possédons par conséquent des bases de données Oracle dont les versions vont des anciennes versions 7 jusqu'aux plus récentes en 11gR2.

Afin de faire face à la complexité engendrée par les problèmes d'accèsibilité, de réseau ou de performance et de faciliter la maintenance des bases de données, l'équipe DBA a dû mettre en place trois outils de surveillance qui sont destinés à alerter les administrateurs de tous dysfonctionnements et comportements anormaux des bases de données dont ils ont la charge :

- Patrol (logiciel de la société BMC Software)
 - Version v3.5 : assure la surveillance des bases Oracle : versions 7 à 8i
 - Version v7.6 : assure la surveillance des bases Oracle : versions 9i à 10g
- OEM (*Oracle Enterprise Manager*, logiciel de la société Oracle)
 - Version 11g : Assure la surveillance des bases 11gR2.

La Figure 2 résume le processus de notification existant des alertes provenant des logiciels Patrol et OEM.

Figure 2: Schéma du processus de notification



Note : L'encadré « Rapport Alertes multiplateformes » a fait l'objet de ma mission de suivi des alertes de ma première année de cycle ingénieur.

II.1.1.2 Problématique

Au cours de ces dernières années, le parc de bases de données a subi une forte augmentation pour répondre aux besoins croissants de l'entreprise. De façon parallèle, les besoins en termes de maintenabilité des bases de données se sont intensifiés et la performance de l'outil existant qui les supervise n'est aujourd'hui plus satisfaisante pour plusieurs raisons :

- I. La version de l'outil de supervision existant OEM v10g ne centralise pas les alertes et les incidents de toutes les bases de données qu'elle supervise. Plus précisément chaque DBA doit se connecter individuellement sur chaque serveur hébergeant la ou les bases en question pour effectuer son analyse ou ses modifications. Cela complique la tâche d'administration du DBA et engendre au même titre une perte de productivité.
- II. Un des objectifs sous-jacents de la mise à niveau d'OEM en sa version 12c est de remplacer à court terme le logiciel Patrol v3.5 et Patrol v7.6. Ceci aurait pour conséquence de simplifier l'architecture applicative de l'entreprise et de bénéficier par la même occasion d'un outil certifié unique pour toutes nos bases de données Oracle et Oracle application (ERP).

Notre équipe est donc confrontée à une problématique multiple :

Comment implémenter et exploiter OEM 12c au sein de notre environnement informatique tout en garantissant une supervision continue pour nos bases de données ?

II.1.1.3 Objectifs à atteindre

L'outil de surveillance de bases de données OEM envoie les alertes sous forme de mail dont les messages sont formatés de façon à rendre une information qui soit rapidement déchiffrable. Le remplacement des versions existantes de Patrol permettra donc de récupérer sous la même forme et via le même biais de communication tous les incidents et alertes de bases de données supervisées par notre équipe. Cette solution présente l'avantage de permettre à notre équipe de créer des filtres sur la messagerie qui leur est commune. De cette façon, chacun peut discriminer efficacement la criticité des alertes et des incidents en cours.

De plus, la montée de version *d'Oracle Enterprise Manager* fera bénéficier toute l'équipe de nombreuses nouvelles fonctionnalités destinées à simplifier et à améliorer l'efficience de notre travail. Ces nouvelles fonctionnalités seront explicitées en détail plus tard dans ce mémoire.

II.2 *Etude d'avant-projet*

Nous présenterons dans cette partie la manière dont fonctionne Oracle Enterprise Manager en étudiant ses éléments internes et leurs interactions. Nous nous pencherons également sur les différentes contraintes liées notamment aux prérequis du logiciel auxquels nous devrons répondre.

II.2.1 Présentation du produit

Oracle Enterprise Manager Cloud Control 12c (plus souvent référencé comme *Cloud Control*, CC, ou CC 12c) est une solution Oracle pour superviser un environnement informatique complet qu'il soit composé de produits Oracle ou non. L'outil *Cloud Control* réunit les informations concernant un système informatique en centralisant sa supervision dans un répertoire central. OEM CC affiche les informations aux administrateurs responsables dans une console web puis l'outil leur envoie des alertes basées sur des seuils plus ou moins critiques. Les superviseurs peuvent alors utiliser ces informations pour que Cloud Control opère les tâches permettant la supervision de tout le système informatique de l'entreprise.

OEM v12c est basé sur la technologie Oracle, une base de données Oracle et un serveur WebLogic de niveau intermédiaire (*Middle Tier*) qui héberge l'application OMS (*Oracle Management Service*). Pour résumer, une base de données Oracle va servir de base de données « dépôt » appelé aussi OMR (*Oracle Management Repository*), celle-ci va stocker toutes les données de métriques des cibles supervisées. Ces données sont collectées et transmises par des agents locaux appelés OMA (*Oracle Management Agents*). Ces agents envoient ces données au service OMS qui va envoyer à son tour ces informations à la base de données pour que celle-ci les stocke. Le service OMS va générer une page d'interface web aux administrateurs, celle-ci va servir de passerelle de communication entre les opérateurs CC et la base de données Dépôt.

II.2.2 Architecture technique d'OEM Cloud Control

L'installation et l'architecture d'Oracle Enterprise Manager GC v10g et de CC v12c ne sont pas les même car leurs composants diffèrent. De plus, les modes de fonctionnement du service OMS et de la base de données dépôt sont bien distincts :

II.2.2.1 Installation et architecture du logiciel OMS

La version 12 d'*Oracle Management Service* est basée sur un Serveur Weblogic Oracle (WLS) 11g R1 (10.3.5) tandis que la version 10g d'OMS est basée sur un serveur d'application Oracle (v 10.1.2.3). Cette amélioration d'architecture a renforcé la sécurité des flux de données entre les différents composants de Cloud Control.

II.2.2.2 Installation de la base de données dépôt

Dans les versions 11g et 12c d'OEM, l'installation de la base de données dépôt ou « Repository » est séparée de l'installation d'OEM. Dans la version GC 10g, une des options d'*Oracle Universal Installer* (OUI) était (en plus de l'installation d'OMS) de créer une nouvelle base de données 10g pour servir de base de dépôt. Les versions GC 11g et 12c de l'outil ne disposent pas d'une base de données intégrée pour servir de base *Repository*. Contrairement à la version 10g, nous avons donc tout d'abord préinstallé une base de données Oracle pour procéder à l'installation de la version 12c. Néanmoins, CC v12.1.0.4 propose un modèle dans l'assistant de configuration de bases de données (Database Configuration Assistant ou DBCA) qui créer une base *Repository* préconfigurée.

II.2.2.3 Prérequis de l'installation d'Oracle Cloud Control 12c

Avant de procéder à l'installation d'OEM 12c, nous devons d'abord installer une base de données certifiée pour héberger les données de supervision du logiciel contrairement à OEM Grid Control 10g où l'on devait choisir d'installer dans un premier temps une base de données Oracle 10g ou 11g par l'intermédiaire d'*Oracle Universal Installer*. Il s'agit ici d'une différence d'architecture substantielle entre la version v10g et les celles en v11g et v12c. Cela est dû au fait qu'Oracle propose à ce jour trop de types d'installations de bases de données différentes (groupes de patchs inclus) dans OEM v11g et v12c pour les inclure dans l'installateur de l'outil.

Les versions des bases de données et des groupes de patchs inclus les versions v11.2.0.1+, v11.1.0.7 et v10.2.0.5+.

Les types d'installation proposés sont variés :

- Un Oracle RAC (*Real Application Cluster*)
- Un Oracle RAC one-node (ORON)
- Une base de données unique : C'est le choix que notre équipe DBA a pris. Nous expliquerons les raisons de ce choix un peu plus loin dans ce mémoire.
- Un *Cold Failover Cluster* (CFC)

II.2.2.4 Différences concernant WLS

Dans la version 10g, le service OMS est une application de niveau intermédiaire basée sur la plateforme Java 2 Entreprise Edition (J2EE) qui génère l'interface utilisateur, c'est-à-dire la console GC. (J2EE est un environnement de développement et de déploiement d'applications d'entreprise). La couche intermédiaire de GC 10g qui utilise Oracle Application Server (OAS ou Oracle AS) 10g, contient 3 éléments :

1. *Oracle Application Server Containers* pour J2EE (OC4J) ou Serveurs Conteneurs d'applications Oracle
2. Oracle HTTP Server (OHS) ou Serveur HTTP Oracle
3. Oracle AS Web Cache

OHS déploie la version 10g du Management Service J2EE web Application.

OMS 10g quant à lui fait techniquement partie d'OC4J toutefois, la couche intermédiaire de GC 10g fait habituellement référence à OMS.

OracleAS Web Cache fournit un moyen supplémentaire de s'identifier dans la console GC.

Contrairement à la version 10g où OMS est déployé dans son propre conteneur OC4J, chacune des plateformes intergiciels GC v11 et CC 12c se composent d'une instance WLS dans laquelle un domaine d'application OMS est créé (appelé GCDomain).

De plus, *OracleAS Web Cache* n'est pas utilisé dans les versions GC v11g et CC v12c alors que celui-ci est exploité dans la version GC v10g. De ce fait, les versions 11g et 12c possèdent un avantage certain vis-à-vis de la version 10g pour plusieurs raisons :

OracleAS Web Cache ne s'avère finalement pas très utile dans GC v10g car ce dernier ne fournit qu'un très léger gain de performance par rapport à l'identification directe sur OHS depuis la console GC. La plupart des requêtes de la console étant ad hoc, celles-ci sont faites pour traiter des données dynamiques avec très peu de données en cache. Généralement, les données se limitent à des icônes, des items de menus, des en-têtes et pieds de page.

OracleAS Web Cache complique le diagnostic des problèmes de GC v10g.

Enfin, L'accès à la console OEM via le Web Cache n'est pas sécurisé (sur HTTP port 7777) lorsque l'on sort des sentiers battus. En effet, le processus de configuration pour sécuriser un tel accès n'est pas aisé et n'est pas documenté. Il s'agit ici d'une faille de sécurité pour les sites qui veulent utiliser Web Cache et qui ont besoin de renforcer la sécurité des communications entre tous les composants de GC v10g.

Bien qu'Oracle donne à ses clients le choix de construire leurs propres applications sur OC4J ou WLS, elle a choisi d'implémenter WLS dans sa solution Cloud Control , pour des raisons de sécurité et de maintenabilité logicielle.

II.3 Cahier des charges

Nous expliquerons dans cette partie quelles sont les contraintes et les attentes liées à Cloud Control.

II.3.1 Les contraintes

Nous allons nous intéresser maintenant aux contraintes nécessaires à l'installation et à l'exploitation de notre environnement Cloud Control. Nous allons mettre en lumière les décisions auxquelles notre équipe doit se confronter au niveau de l'architecture de l'outil.

Nous parlerons notamment de la question du nombre d'environnement CC 12c à installer ainsi que de l'architecture choisie de ses éléments.

Nous nous intéresserons ici aux prérequis des éléments de CC suivant :

- **Oracle Management Service** : Un service « OMS » doit être installé sur le serveur-hôte sur lequel l'installateur est exécuté.
- **Oracle Management Repository** : La base de données dépôt appelée aussi base dépôt ou « OMR » est créée à partir d'une base de données que vous devez avoir préinstallée.
- **Oracle Management Agent** : Un agent ou « OMA » est installé sur chaque serveur-hôte que vous voulez superviser avec Cloud Control. Il existe deux types d'agents : l'agent préinstallé et l'agent autonome.
- **Agent préinstallé** : L'installation de ces types d'agents (Chain-installed Agent) est couplée avec celle OMS, par conséquent, celle-ci est réalisée de façon automatique par l'installateur OUI. Comme n'importe quel agent, il supervise les cibles du serveur-hôte sur lequel il est installé dont OMS et la base Repository si ces derniers sont installés sur le même serveur-hôte.
- **Agent autonome** : Contrairement à l'agent préinstallé, les agents autonomes (Standalone Agents) doivent être installés manuellement sur tous les serveur-hôtes hébergeant des cibles supervisées excepté le serveur OMS lui-même sur lequel l'agent est préinstallé. Le déploiement d'agents autonomes doit être opéré après l'installation de la base Repository et du service OMS. Ces deux types d'agent exigent les mêmes prérequis. Une fois installés, ces agents sont en tout point identiques.
- **CC Console Client** : Il s'agit ici de la console client de Cloud Control. Celle-ci est réservée aux administrateurs de bases de données. Ces derniers se connectent à la console via un navigateur internet. La console est affichée par OMS et celle-ci n'a pas besoin d'être installée séparément. Les seuls prérequis nécessaires relatifs à la console concernent la bande passante du réseau et la latence maximale autorisée entre le poste client et OMS.

Les prérequis explicités ici s'appliquent aux serveurs-hôtes sur lesquels OMR, OMS et les agents préinstallés seront installés, à ceux où les agents autonomes seront déployés et aux postes clients chargés d'afficher la console Cloud Control. Tous ces prérequis représentent, en plus des autres bases de données qui hébergent la base de dépôt, l'ensemble de tous les prérequis nécessaires à l'installation et à l'exploitation d'un environnement CC 12c.

Les tâches de pré-installation s'organisent en quatre catégories :

- **Conception architecturale** : Le premier prérequis consiste à concevoir une architecture de CC qui prend en compte le nombre d'environnements CC à mettre en place et le nombre de serveurs OMS à installer. Nous devons également prendre en compte tous les critères de hautes disponibilités (HA) et des plans de récupération après sinistre.
- **Configuration réseaux** : Après s'être mis d'accord sur l'architecture de Cloud Control à déployer, la deuxième étape consiste à saisir les prérequis de la configuration réseaux en passant par les règles et les contraintes de nommage des serveurs-hôtes, les tests de connectivité entre les différents éléments de CC, la configuration des pare-feux et du système d'équilibrage (Load Balancing) des charges du serveur si un tel système est utilisé.
- **Prérequis matériel** : Cette catégorie fournit des spécifications concernant OMR, OMS et les serveurs-hôtes hébergeant les agents relatifs aux ressources (espace disque, RAM, swap et rapidité du CPU) nécessaires pour saisir les prérequis nécessaires à l'installation et à l'exploitation de CC.
- **Prérequis logiciel** : Nous devons tout d'abord vérifier que les plateformes OMS et OMR répondent aux prérequis nécessaires à la certification Cloud Control. Il faut créer les groupes systèmes, les utilisateurs et les répertoires. Il faut synchroniser les fuseaux horaires des serveurs-hôtes et saisir les prérequis des plateformes logicielles spécifiques.

Il est important de souligner que nous avons dû tout d'abord saisir les prérequis nécessaires à l'installation de OMR et OMS avant d'exécuter l'installateur de Cloud Control (Oracle Universal Installer). Toutefois, les prérequis nécessaires à l'installation des agents autonomes peuvent être retardés et être saisi après la phase d'installation de CC. Il est fortement conseillé de s'assurer au minimum que les prérequis des agents préinstallés (chain-installed agent) soient saisis sur les serveurs-hôtes sur lesquels les agents autonomes sont opérationnels. En effet, un certain nombre de ces prérequis sont relatifs aux exigences réseaux demandées qui sont la plupart du temps vérifiés par l'administrateur réseaux lui-même.

II.3.2 Critères de satisfaction

a. La centralisation des informations

Dans ce projet, le principal critère de satisfaction attendu par l'implémentation de cette nouvelle version d'OEM repose sur la centralisation des informations relatives aux bases de données supervisées. En effet jusqu'à maintenant il fallait configurer pour chaque base supervisée un ensemble de règles d'incidents et de notifications. Cela pouvait poser problème en termes de maintenabilité de ces bases de données. Grâce à la nouvelle interface fournie dans Cloud Control, il sera désormais possible de surveiller les activités de l'intégralité de nos bases de données via la même console utilisateur ce qui représente une amélioration substantielle dans le travail de maintenance quotidienne de notre équipe.

b. Fonctionnalités améliorées

Oracle Enterprise Manager 12c nous fera profiter des fonctionnalités améliorées. Voici deux exemples des améliorations attendus :

- **Amélioration du fonctionnement interne de Cloud Control** : Beaucoup d'opérations de contrôle des agents de supervisions sont maintenant disponibles. Par exemple le démarrage, le redémarrage et l'arrêt des agents sont dès à présent accessibles sur l'interface de gestion du système.
De plus, tous problèmes entre les agents de supervisions et le service Oracle Management sont désormais automatiquement détectés et peuvent être traités dans la section de traitement des incidents du système. Dans cette section, on peut accéder au support de test qui va établir pour vous le diagnostic du problème rencontré. Ce support peut par la suite utiliser le diagnostic établi pour l'envoyer au support Oracle qui pourra trouver une solution à ce problème. Cela a pour avantage de faire économiser du temps aux équipes support concernés de l'entreprise, notamment en matière de résolution des incidents.
- **Amélioration des métriques** : Les métriques de l'interface utilisateur ont été améliorées et permettent une meilleure navigation et un meilleur accès aux données de mesure. On a accès aussi aux métriques dont les alertes ont été le plus souvent déclenchées sur sept jours la nouvelle fonctionnalité de suggestion de seuils est maintenant disponible pour nous aider à affiner notre configuration.

c. Nouvelles fonctionnalités

J'ai par ailleurs lister les nouvelles fonctionnalités proposées, afin d'étudier l'évolution du métier de maintenance pour les DBA au sein de l'équipe d'Essilor. Deux nouveaux dispositifs sont disponibles :

- **Les actions correctives sur les incidents** : Nous pourrons effectuer des actions correctives sur des incidents dans un groupe ou un système depuis le tableau de bord système. Ces actions peuvent être assignées à des personnes et une liste de priorité peut être établie sur les incidents les plus urgents à résoudre.
- **La mise en place d'alertes sensibles au temps** : Différents seuils d'alertes pourront être configurés en fonction du temps. Par exemple, durant la journée, nous pourrons établir un seuil d'alerte relativement exigeant, pouvant détecter tout délai abnormal concernant l'émission de requêtes SQL par les utilisateurs. Mais en soirée, parce qu'un certain nombre de scripts tournent, nous pouvons baisser les seuils d'alertes car les enjeux ne sont pas les mêmes en journée et en soirée.

II.3.3 Détail des versions logicielles déployées

- Version du logiciel installé : Oracle Enterprise Manager Cloud Control 12c v12.1.0.4
- Version de la base de données installée : Oracle Database v11.2.0.4
- Version du modèle de base de données installée : DB Template v12.1.0.2
- Version des agents déployés sur les serveurs-cibles : Oracle Enterprise Agent v12.1.0.2.0

II.3.4 Budget & Délais

a. Budget Logiciel

Oracle Enterprise Manager est logiciel de gestion de bases de données proposé par Oracle en libre-service. Contrairement aux logiciels concurrents tels que *Patrol* utilisés pour superviser les bases de données Oracle v7i et v8i.

Bien qu'il soit gratuit, ce n'est pas le critère qui a été pris en compte quant à l'adoption de ce logiciel. D'autres critères plus importants tels que la disponibilité de documentations en ligne, la certification de prise en charge des bases Oracle (versions supérieures à 8i) par OEM et de la fiabilité d'Oracle ont été pris en compte.

b. Budget Humain

Les méthodes de déploiement et de configuration d'OEM ont été supervisées par l'expert DBA Oracle de notre équipe, un deuxième administrateur Oracle et moi-même pendant un peu plus de 6 mois.

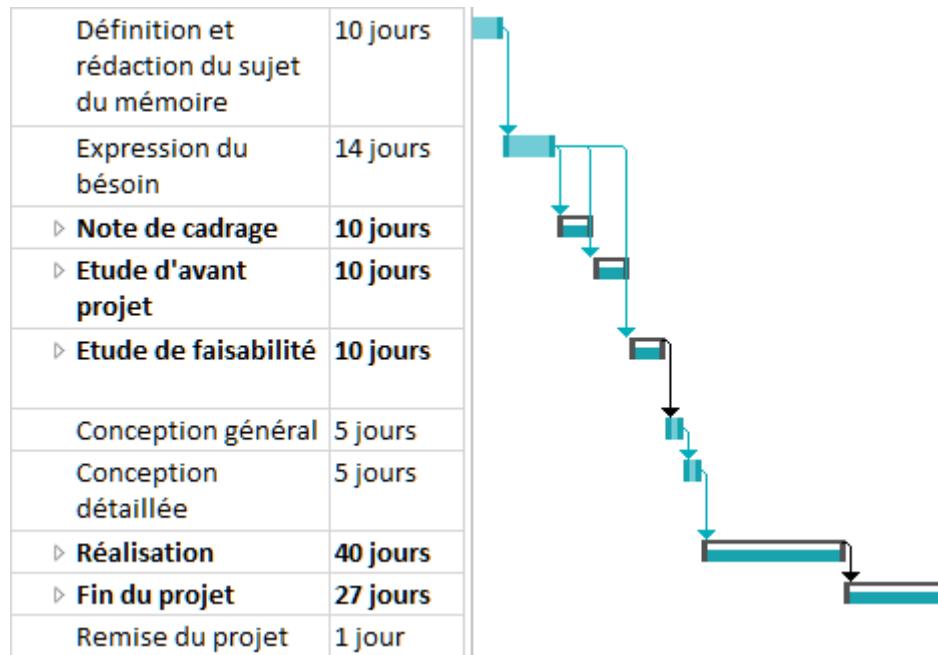
Pour des raisons de confidentialité, il n'est pas possible de fournir plus de détails vis-à-vis du budget alloué à ce projet.

c. Délais

Le détail du planning prévisionnel est fourni en annexe. Le projet a débuté le premier décembre 2015 et s'est réellement terminée le 20 mai 2016.

Voici un bref récapitulatif du planning prévisionnel des différentes phases du projet

Figure 3: Planning prévisionnel



II.3.5 Cahier des charges fonctionnel

Outre les besoins précédemment définis pour l'équipe de DBA en termes de maintenance, *Oracle Enterprise Manager Cloud Control* possède de nombreuses fonctionnalités. Il n'est pas possible de toutes les énumérer ici mais en voici une liste résumée :

- Fonctionnalités d'administration centralisée des bases de données pour la gestion des bases de données Oracle locales et distantes.
- Simplification des tâches du DBA grâce à une interface graphique intuitive.
- Exécution de tâches sans saisie manuelle de la syntaxe SQL, PL/SQL ou RMAN.
- Gestion des instances et des sessions de base de données Oracle.
- Gestion des objets de schéma, comme les index, les tables, les partitions, les vues et les procédures stockées.
- Gestion des utilisateurs de base de données et de leurs privilèges, profils et rôles.
- Gestion des exigences de la base de données en matière d'espace physique et d'espace logique, notamment la gestion des fichiers de contrôle, des espaces disque logiques et des fichiers de journalisation.
- Entrée et extraction de données dans les bases de données à l'aide des assistants de gestion des données.
- Impression et enregistrement des informations récapitulatives relatives à la base de données, comme l'ensemble des utilisateurs de base de données.
- Création et programmation des travaux de sauvegarde via les assistants de gestion des sauvegardes (disponibles si connectée à Oracle Management Server).
- Visualisation des dépendances pour les objets de la base de données.
- Visualisation et modification des données accessibles par l'intermédiaire des tables, des vues et des synonymes.
- Suppression rapide et facile de colonnes de table.
- Analyse des objets de base de données à l'aide d'assistants.
- Mise à disposition de plusieurs états prédéfinis qui permettent aux DBA de personnaliser, de programmer et de publier ces états vérifier l'état de la base.

II.4 Etude de faisabilité

A travers cette étude nous allons prouver que le projet est techniquement faisable et économiquement viable. Ainsi nous expliciterons dans cette partie les ressources techniques et humaines nécessaires à la réalisation de ce projet.

II.4.1 Etude Réseaux

Les études réseaux et matérielles ont été réalisées succinctement car le logiciel *Oracle Grid Control* 10g, qui est une ancienne version d'*Oracle Enterprise Manager*, est installé et utilisé sur nos systèmes depuis plus de cinq ans. Les éléments internes d'OEM 12c étant semblables à ceux de la version 10g, il n'a pas été nécessaire de faire des études réseaux et matériels approfondies pour implémenter la solution Cloud Control. Nous allons néanmoins exposer ici les prérequis réseaux à respecter pour implémenter une solution OEM quel que soit la version du produit déployée.

Pour calculer et donc connaitre le nombre d'environnements Cloud Control à installer en fonction de l'éloignement géographique des cibles supervisées il faut connaitre les prérequis réseaux nécessaires pour la communication entre les composants d'OEM 12c ainsi que la performance réseaux des serveurs hébergeant ces éléments. (Voir tableau n°1)

La gestion des erreurs réseaux de Cloud Control est robuste. Elle permet entre autres de tolérer des bugs et des interruptions réseaux entre les différents composants d'OEM. Toutefois, les problèmes réseaux entre un agent et OMS ou entre la console et OMS n'ont que très peu d'impact sur les performances globales de CC comparé à ceux pouvant affectés les communications entre OMS et OMR. La connexion d'un agent ou d'une console à OMS peut être interrompue sans impacter les fonctions du système Cloud Control. Néanmoins, un problème réseaux entre un OMS actif et OMR peut réduire les performances globales du système de supervision. La connexion de la console, le système de notification automatique, l'exécution des tâches et presque toutes les autres fonctions de CC peuvent être impactés.

En règle générale, la performance réseaux minimale requise entre les hôtes OMS et OMR dicte le choix d'implantation géographique de ces deux composants car les performances réseaux de communication entre les agents et le serveur OMS passent au second plan. Il n'existe pas de limitations spécifiques propres à l'application OEM car celle-ci a été conçue pour administrer plusieurs centaines de milliers de cibles par plus d'une centaine d'administrateurs.

Le *tableau 1* met en évidence la bande passante réseau minimale ainsi que la latence maximale à respecter entre un OMS actif, la base Repository et les agents OMA. Les prérequis nécessaires de connexion réseaux entre OMR et ses disques de stockages sont en général pris en compte lorsque l'hôte OMR n'est pas physiquement couplé avec ses propres équipements de stockage. Les serveurs-hôtes situés dans le Cloud (« Cloud hosting » ou « Cloud storage ») représentent un exemple concret de cette réalité.

Tableau 1: Prérequis réseaux minimum nécessaires de connexion

Connexion entre les éléments de Cloud Control	Bandé Passante Minimale Requise	Latence Maximale autorisée
Console Client <-> OMS	300 Kbps	300 ms
OMA <-> OMS	300 Kbps	300 ms
OMS <-> OMR	1 Gbps	30 ms
OMR <-> Stockage OMR	1 Gbps	10 ms

Remarque : Il semble important de souligner que les prérequis de connexion réseaux explicités ici se basent sur le postulat que le réseau est entièrement dédié au trafic de Cloud Control.

Ce même tableau montre à quel point la bande passante minimal et la latence maximale demandée sont bien plus exigeantes que celles requise entre les hôtes OMA et OMS. Il s'agit ici d'un différentiel de 10x pour la latence et de plus de 3000x pour la bande passante. Il est essentiel de connaître les ordres de grandeur des prérequis réseaux entre les différents composants d'OEM et de les comparer avec les performances réseaux de l'entreprise pour pouvoir allouer l'équipement adéquat au bon fonctionnement de Cloud Control. En raison des fortes exigences de connexion entre OMS et les tiers OMR, la plupart des sites réunissent au sein de leur(s) centre(s) de données (Datacenters) au moins un serveur-hôte dédié à OMS à celui dédié à OMR. Essilor possède un équipement réseau Gigabit Ethernet (GigE) ou supérieur. Nous sommes donc capables de répondre au prérequis de 1Gbps minimum demandé en bande passante entre les serveurs OMS et OMR.

II.4.2 Ressources allouées

Notre mission a nécessité de mettre en place un certain nombre de ressources matériels, logiciels et humaines. Voici le détail des ressources utilisées durant le projet.

II.4.2.1 Ressources matérielles et logicielles

- Mise à disposition d'un serveur Linux x64
- Création d'un File system de 100 Go sur le disque dur alloué au serveur
- Création d'un compte système utilisateur standard sur le serveur
- Xming. Logiciel destiné à lancer les exécutables DBCA (Database Configuration Assistant) pour la création de la base Repository et OUI (Oracle Universal Installer) pour lancer l'installation de Cloud Control
- Putty. Logiciel de prise de contrôle à distance pour se connecter sur le serveur destiné à héberger Oracle Enterprise Manager 12c.

II.4.2.2 Ressources humaines : les acteurs

- Expert Administrateur base de données Oracle : Il a joué le rôle de superviseur pendant toutes les phases du projet. Ses conseils et ses avertissements ont permis à notre équipe de résoudre certains points bloquants notamment sur la phase de configuration de Cloud Control.
- Un administrateur base de données senior : Il m'a donné les références dont j'avais besoin durant la phase de recherche des nouvelles fonctionnalités.
- Moi-même, apprenti administrateur base de données

II.4.3 Les risques et les impacts

Le remplacement de la version d'Oracle Enterprise Manager 10g par la version 12c entraîne un certain nombre de risques au niveau de la supervision des bases de production dont nous avons la charge. Voici les étapes auxquelles il a fallu être particulièrement vigilant au niveau des risques encourus :

1. Le rapatriement de nos bases de données sur la nouvelle version d'OEM
 - a. Désinstallation des anciens agents OEM 10g
 - b. Installation des nouveaux agents compatibles OEM 12c
2. La configuration des seuils d'alertes des métriques des bases de données
3. La configuration des notifications des incidents

II.4.3.1 Les risques associés

1. La perte des informations de supervision. L'enjeu principal de cette étape a consisté à maintenir la supervision continue de nos bases de données de production pendant la période de transition entre OEM 10g - OEM 12c.

Afin de se prémunir contre toute discontinuité de la surveillance de ces bases stratégiques, nous avons, dans un premier temps, testé nos procédures de déploiement des agents sur des serveurs qui hébergeaient des bases de données non-stratégiques pour l'entreprise. Nous avons également profité de ces premiers déploiements pour tester nos procédures de configuration des seuils d'alertes et des méthodes de notification. Ces étapes ayant été réalisées sans difficulté, notre équipe a opté pour :

- L'adoption immédiate et globale de Cloud Control pour nos bases de données non-stratégiques.
- Une transition lente et progressive de nos bases de données de production.

Nous avons donc gardé l'environnement OEM 10g pour nous prémunir contre d'éventuels bugs critiques de la nouvelle version 12c déployée. En effet nous aurions pu à tout moment décider de revenir à l'ancienne version du logiciel si de telles erreurs étaient survenues sur Cloud Control.

2. La survenance d'incidents sur les bases de données. Lorsque les seuils d'alertes sont mal configurés, certains problèmes peuvent ne pas être détectés à temps et le niveau de performance de nos applications et de nos bases de données en subit les conséquences. Cela peut nous mener à devoir arrêter une base de données pour la réparer (Downtime). Inversement, des seuils trop sensibles peuvent amener à ce que des alarmes soient déclenchées à cause de simples opérations de routine de nos systèmes. Dans de tels scénarios, les alarmes génèrent des alertes sans qu'aucun mal n'ait été fait au système.

Non-détection d'alertes et d'incidents. Si la méthode de notification des alertes et incidents est mal configurée, les administrateurs ne sont pas notifiés de l'apparition de problèmes au sein de leurs bases de données. Par conséquent, si des alertes sont générées, celles-ci ne seront pas traitées à temps et des incidents critiques peuvent survenir. De la même façon, si des incidents ne sont pas détectés, les performances globales des bases de données et des applications sont directement impactées et celles-ci peuvent cesser de fonctionner.

II.4.3.2 Les impacts associés

Le déploiement de Cloud Control nous a contraint à mettre en œuvre de nouvelles procédures.

- Procédure d'installation de la base Repository
- Procédure d'installation d'OEM 12c
- Procédure de déploiement des agents et d'ajout des bases de données dans OEM 12c
- Procédure de configuration de la méthode de notification par mail
- Procédure de configuration des seuils d'alertes de bases de données
- Procédure de création de règles d'incidents

Toutes ces procédures ont dû être réalisées en amont de la phase de déploiement grâce à la documentation que l'éditeur Oracle met en libre-service sur son site internet. Celles-ci ont été testées et validées par l'expert administrateur base de données Oracle de notre équipe et moi-même.

Cloud Control a fait l'objet d'une étude approfondie et d'un travail d'uniformisation des diverses configurations existantes des bases de données.

Ces procédures sont par la suite communiquées aux équipes DBA de Thaïlande et permettent de transmettre des nouvelles méthodes et de nouveaux savoir-faire.

La clarification de l'expression du besoin, la rédaction du cahier des charges et de l'étude de faisabilité nous a permis de mieux appréhender les enjeux de la mission. Nous pouvons maintenant analyser l'architecture d'OEM 12c pour comprendre le fonctionnement interne du logiciel.

III La solution Oracle Enterprise Manager Cloud Control 12c

Dans cette partie, nous analyserons tout d'abord l'architecture de Cloud Control et les différents choix de déploiement qui nous sont proposés. Nous serons ainsi capables de choisir l'architecture logicielle d'OEM la plus à même de répondre aux besoins liés à la maintenance de nos environnements informatiques. Pour ce faire, nous développerons les parties suivantes :

- Analyse de l'architecture d'OEM
- Les choix architecturaux de Cloud Control

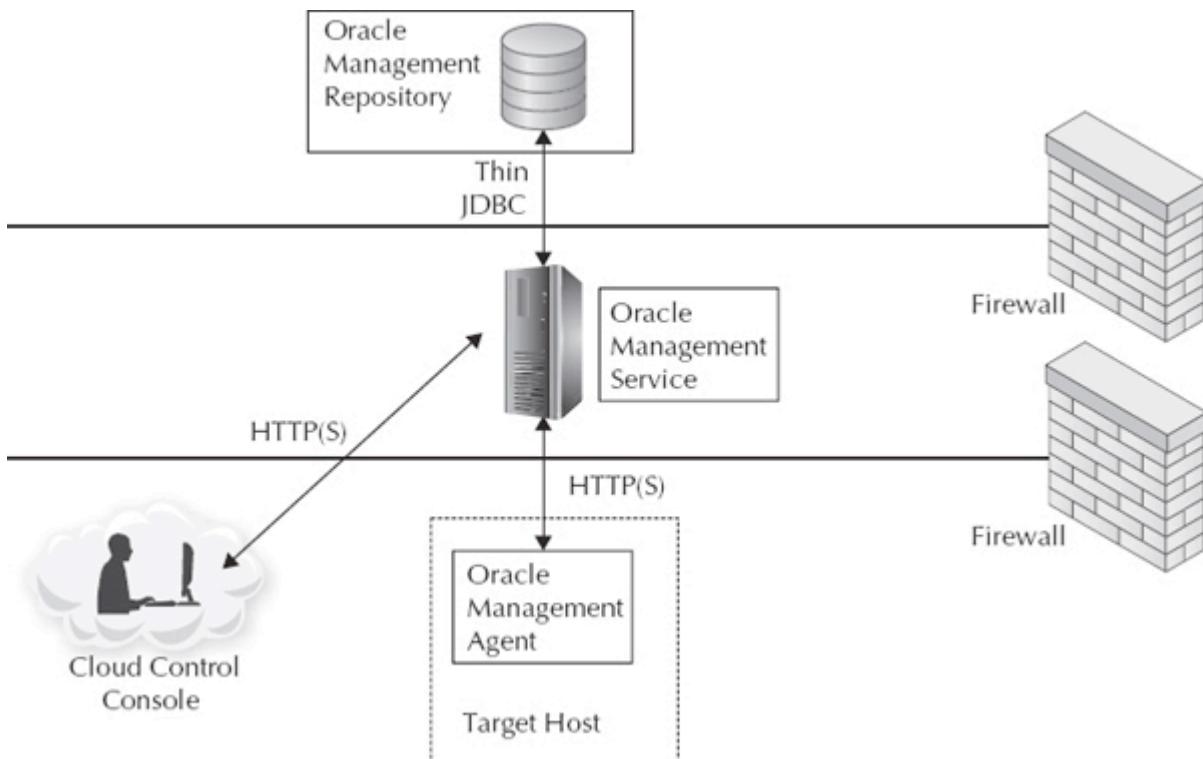
III.1 Analyse de l'architecture d'OEM

Nous allons examiner dans un premier temps quels sont les composants communs aux différentes versions de l'outil de supervision sorties à ce jour. La structure classique de Cloud Control se décompose en quatre composants principaux qui sont :

1. La console Cloud Control
2. L'agent d'Oracle Management (OMA)
3. Le service Oracle Management (OMS)
4. La base Repository (OMR)

Chaque composant peut être séparé par un firewall.

Figure 4: Architecture d'Oracle Enterprise Management Cloud Control 12c



III.1.1 Cloud Control Console

La console Cloud Control est une application basée sur un navigateur web au travers de laquelle nous pouvons superviser de façon centralisée les environnements informatiques. La page d'accueil donne une vue d'ensemble de l'infrastructure technique supervisée dans laquelle nous accédons à une cible bien précise administrée par le logiciel. La console CC est certifiée pour fonctionner avec les navigateurs internet les plus connus comme Internet Explorer, Firefox, Safari, Google Chrome mais aussi avec le plug-in Adobe Flash Player pour certaines autres fonctionnalités de la console.

La console n'a pas besoin d'être installée par nos soins, c'est le service OMS qui se charge d'afficher cette interface. Il suffit d'ouvrir un navigateur internet et de se connecter à la console via l'URL d'identification d'Entreprise Manager.

La console d'OEM nous permet donc de nous connecter quasiment partout via son navigateur internet. L'interface de la console étant codée en HTML, celle-ci utilise par défaut le protocole HTTPS (ou HTTP si l'accès est non-sécurisé) qui la rend donc fluide, facile d'accès et facilement configurable pour d'éventuels pare-feux.

La manière la plus courante de nous identifier à la console se fait par l'intermédiaire de la barre d'adresse du navigateur en utilisant le format suivant : <nom-serveur-hôte> :<port>/em. L'installation de Cloud Control restreint les accès du navigateur pour sécuriser les communications (SSL), cependant après l'installation, celle-ci vous permet d'établir des accès HTTP avec une configuration minimale.

Dans GC v10g, nous pouvions nous identifier directement via le serveur HTTP Oracle (OHS) ou indirectement via OracleAS Web Cache qui vous relayait ensuite à OHS. En revanche, dans les versions OEM 11g et CC 12c, vous ne pouvez le faire qu'à travers le serveur Apache WLS (WLS Apache Web Server) avec le protocole HTTPS et le port par défaut 7799. Il n'y a pas d'accès par le cache Web aux consoles GC 11g et CC 12c.

Dans la version 10g d'OEM, presque toutes les fonctionnalités de la console Java d'OEM v9i avaient été reprises et redéveloppées en code HTML. Pour exécuter les anciennes fonctionnalités des versions 9i propres aux clients lourds Java qui n'étaient pas encore disponibles dans la console de GC 10g comme la gestion avancée de la réPLICATION Oracle, nous devions télécharger le logiciel client Oracle 10g et installer les composants de la console Java d'Oracle GC 10g. La console Java d'OEM fonctionne de façon autonome, elle ne se connecte pas au service OMS. Dans GC 11g, il n'y a plus besoin d'installer une console Java en mode client lourd. Dans les versions GC 11g et CC 12c, toutes les fonctionnalités sont accessibles via leur console.

III.1.2 Oracle Management Agent

L'agent de supervision installé sur chaque serveur-hôte supervisé surveille ce dernier ainsi que toutes les cibles qu'il héberge. Celui-ci communique également toutes les informations relatives aux composants ciblés au service OMS provenant des produits Oracle ou de sociétés extérieures. Cloud Control peut superviser plus de 200 types de cibles différentes. Chaque instance d'un type de cible particulier présent sur le serveur-hôte compte comme une cible supervisée. Les types de cible les plus répandues sont par exemple les instances de bases de données, les *Listeners* (ou *Auditeur*), le serveur Oracle Application et le serveur-hôte hébergeant ces mêmes cibles.

Les plug-ins d'OEM permettent quant à eux de contrôler de façon spécifique des cibles Oracle et non-Oracle. Dans les versions Grid Control v10g et v11g, certains types de cibles couplées avec le produit sont maintenant packagés comme de simples plug-ins dans CC 12c. Cela permet aux équipes de développement Oracle de mettre à jour les plug-ins indépendamment des versions du produit lui-même. En effet, les plug-ins étant à la fois développés par la société Oracle et par des sociétés partenaires, ceux-ci sont non seulement utilisés dans les produits Oracle mais également dans beaucoup d'autres produits non-Oracle. Par exemple, les produits Microsoft SQL Server, Microsoft Active Directory, IBM WebSphere Application Server ainsi que d'autres produits les utilisent.

Le logiciel Cloud Control se monitor également lui-même par conséquent un agent OMA doit aussi fonctionner sur tous les nœuds hébergeant les services OMS et OMR. Sur chaque hôte surveillé, virtuel et non virtuel, seul un seul agent doit être opérationnel.

Oracle certifie son agent pour les versions actuelles 12c (v12.1.0.2) sur les serveurs-hôtes d'infrastructure 32-bit 64-bit en passant par les systèmes Linux x86-64 et x86, Oracle Solaris avec SPARC (64-bits), Oracle Solaris 64-bit, IBM Linux sur système Windows (x64 et x86) et HP-UX (Itanium, PA-RISC).

OMS fait partie du Framework d'Oracle Enterprise Manager, l'agent est codé dans le langage de programmation C pour des raisons de performance et de ressource. Les bibliothèques de programmation du cœur Oracle sont utilisées par un processus parallélisé (multithread) et ce sont Oracle Call Interface (OCI) et Oracle Secure Socket Layer (SSL) qui se chargent de le sécuriser par défaut. Pour comprendre de façon plus précise le fonctionnement de l'agent nous allons expliciter les étapes de découverte des cibles des agents à l'intérieur des serveur-hôtes sur lesquelles ils sont hébergés.

III.1.3 Gestion et découverte des cibles supervisées

Dans cette partie nous allons nous intéresser aux agents de supervision d'OEM. Les agents font partie intégrante d'OEM. Nous expliquerons leur fonctionnement et le rôle qu'ils jouent au sein d'OEM.

Il ne peut y avoir qu'un seul agent opérationnel au sein d'un serveur-hôte supervisé. Un agent OMS qui a été correctement installé commence par se surveiller lui-même puis vérifie l'état de son hôte, du service OMS si celui-ci est présent et des autres produits Oracle présents sur la machine (Listeners, Bases de données etc.). Il est à noter que l'agent lui-même et son hôte sont traités par Cloud Control comme des cibles à part entière. La découverte automatique des cibles commence dès que l'agent est installé et démarré. Les cibles qui n'ont pas été découvertes par l'agent peuvent être mises en lumière par la console OEM. Cette dernière méthode permet également de découvrir de nouvelles cibles de façon manuelle ou automatique.

Les cibles peuvent se décomposer en plusieurs types de catégories comme nous l'avons expliqué précédemment, cependant, un certain nombre de plug-ins de GC 11g n'ont pas encore été mis à jour pour CC 12c mais il est très probable qu'ils soient pris en charge dans un futur proche.

L'agent utilise un niveau de supervision par défaut pour la récolte des données des cibles surveillées. Ces données sont transmises au système de supervision. OMA envoie immédiatement les métriques d'alertes et émettent de façon périodique des informations de supervision au service OMS. L'agent effectue des tâches pour le compte de OMS qui peuvent être de différentes natures :

- Des tâches métiers appelés « jobs ». Ce sont des unités de travail créés pour automatiser des tâches administrateurs comme l'application de patchs ou l'implémentation de sauvegardes régulières.
- Des tâches de coupure qui arrêtent la récolte de données sur les cibles supervisés pour effectuer des maintenances planifiées. Ces coupures permettent d'obtenir une image plus juste et plus précise des performances de la cible supervisée car celle-ci permet non seulement de libérer des ressources supplémentaires pour le serveur mais elle autorise également l'arrêt planifié du service OMS. De ce fait, le contrat de niveau de service (Service Level Agreement) de la cible ne s'en retrouve pas affecté.

III.1.4 Oracle Management Service

Dans la version 10g, le service OMS est une application de niveau intermédiaire basée sur la plateforme Java 2 Entreprise Edition (J2EE) qui génère l'interface utilisateur, c'est-à-dire la console GC. Les agents transmettent les données relatives aux cibles supervisées au service OMS. Celui-ci traite les données entrantes avant de les envoyer à son tour à la base de données dépôt, plus communément appelée Repository (OMR). La couche intermédiaire de Cloud Control est composée d'une instance d'Oracle WebLogic Server v10.3.5 qui se charge de déployer l'application Web J2EE.

Nous devons installer OMS sur un ou plusieurs serveur-hôtes afin de pouvoir garantir pour notre environnement informatique supervisé, des niveaux de disponibilité et de flexibilité acceptables. Chaque service de supervision doit être opérationnel sur le serveur-hôte qu'il héberge. OMS et OMR peuvent se situer sur le même hôte mais, pour des raisons de performance, Oracle ne recommande pas cette configuration pour un environnement de production de plus de mille cibles. Tous les hôtes physiques d'OMS échangent de façon indépendante avec le service Oracle Management Service. En revanche, plusieurs hôtes d'OMS ayant un répertoire partagé peuvent se coordonner pour traiter la transmission des fichiers de chaque agent dans ce même répertoire.

Le service de supervision d'Oracle est déployé avec WLS v11gR1 (10.3 .5). Comme nous l'avons déjà expliqué, l'installation d'OMS est couplée avec l'installateur de CC 12c. Lorsqu'OUI créer un nouveau système de supervision, une instance de WLS est installée dans le sous-répertoire wlserver_10.3 du répertoire dédié à la couche intermédiaire de l'application. (Par exemple : /u01/app/Middleware). OMS est déployé dans un nouveau domaine appelé GCDomain dans l'instance WLS et n'utilise aucun domaine déjà existant de l'architecture en place. Pour comprendre de façon précise l'architecture d'un serveur OMS il faut d'abord comprendre le rôle que joue chacun des éléments qui la compose. WLS 10.3.5 (qui contient le serveur HTTP Oracle) et l'application J2EE d'OMS qui font partie du domaine de WLS Fusion réunissent à eux seuls ce que nous appelons communément « OMS ».

Tous les composants de ce service sont installés sur le même serveur indépendamment de la méthode d'installation de Cloud Control utilisée (via OUI ou installation silencieuse). On peut déployer néanmoins plusieurs OMS sur des serveurs-hôtes différents. En revanche, sur chacun de ces serveurs doivent être présents tous les composants d'OMS et doivent obligatoirement faire référence à la même base Repository pour un environnement Cloud Control donné. Chacun de ces services communiquent avec la base de dépôt via JDBC qui sert d'interface standard Java pour les connexions entre Java et les bases de données relationnelles.

III.1.5 Oracle Management Repository

Nous expliquerons ici le rôle et le fonctionnement de la base Repository au sein de l'architecture OEM. Celle-ci joue un rôle central et nécessite d'être étudiée pour comprendre ses possibilités de déploiement et de configuration.

La base de données dépôt agit comme un entrepôt de données pour Cloud Control. Celle-ci peut être préinstallée manuellement ou par le modèle EM dans l'assistant de configuration de base de données DBCA. Le Repository est créée par défaut par le schéma utilisateur SYSMAN, celui-ci contient les informations sur toutes les cibles de Cloud Control, schémas administrateurs compris. La base de données dépôt organise toutes ces données de façon à ce qu'OMS puisse accéder mais aussi afficher ces informations dans la console d'administration. Cloud Control n'utilise qu'une seule base centrale Repository. Celle-ci peut être une base de données simple ou issue d'un ensemble RAC et doit être en version 10gR2 (10.2.0.5), en 11gR1 (11.1.0.7.0) ou en 11gR2 (11.2.0.1+) qu'Oracle préconise.

Les consoles administrateur et agent communiquent avec OMS de façon directe ou par l'intermédiaire de scripts (en dehors des alertes). Ils utilisent les protocoles réseaux respectifs :

- Nous pouvons émettre des requêtes dans la console à travers le protocole HTTP(S) dans notre session de navigateur internet, celles-ci seront traitées par OMS. Le serveur va récupérer les données demandées par ces requêtes dans la base dépôt et les afficher directement dans la console.
- Les agents envoient les informations au serveur OMS via le protocole HTTP(S) et les transmet à son tour à OMR via JDBC (Java DataBase Connectivity). La base Repository retourne ces données à OMS via le même protocole et les relaient à l'agent OMA via un protocole d'écoute HTTP.

Toutes les consoles administrateurs ont accès aux informations présentes dans la base de données dépôt pour un niveau de droit d'accès donné. Les informations dont dispose la base Repository sont :

- Les détails de configurations des cibles supervisées.
- Les informations de disponibilité des cibles surveillées.
- L'historique des métriques et des informations relatives aux alertes.
- Les données concernant les temps de réponse des cibles.
- Les informations d'inventaire des patchs et des produits installés.

Toutes ces informations vont nous permettre :

- De superviser l'ensemble de nos environnements (Bases de données, serveurs d'application, serveur-hôtes etc.), les applications modélisées et les tâches automatisées.
- D'analyser les données de statuts et de performances.
- De mettre en place des niveaux de service applicatif (ASLM pour Application Service Level Management).
- De pister et d'effectuer des changements de configuration.
- Et de mener à bien beaucoup d'autres tâches pour superviser des systèmes d'information complexes fonctionnant de pair avec des technologies Oracle et non-Oracle.

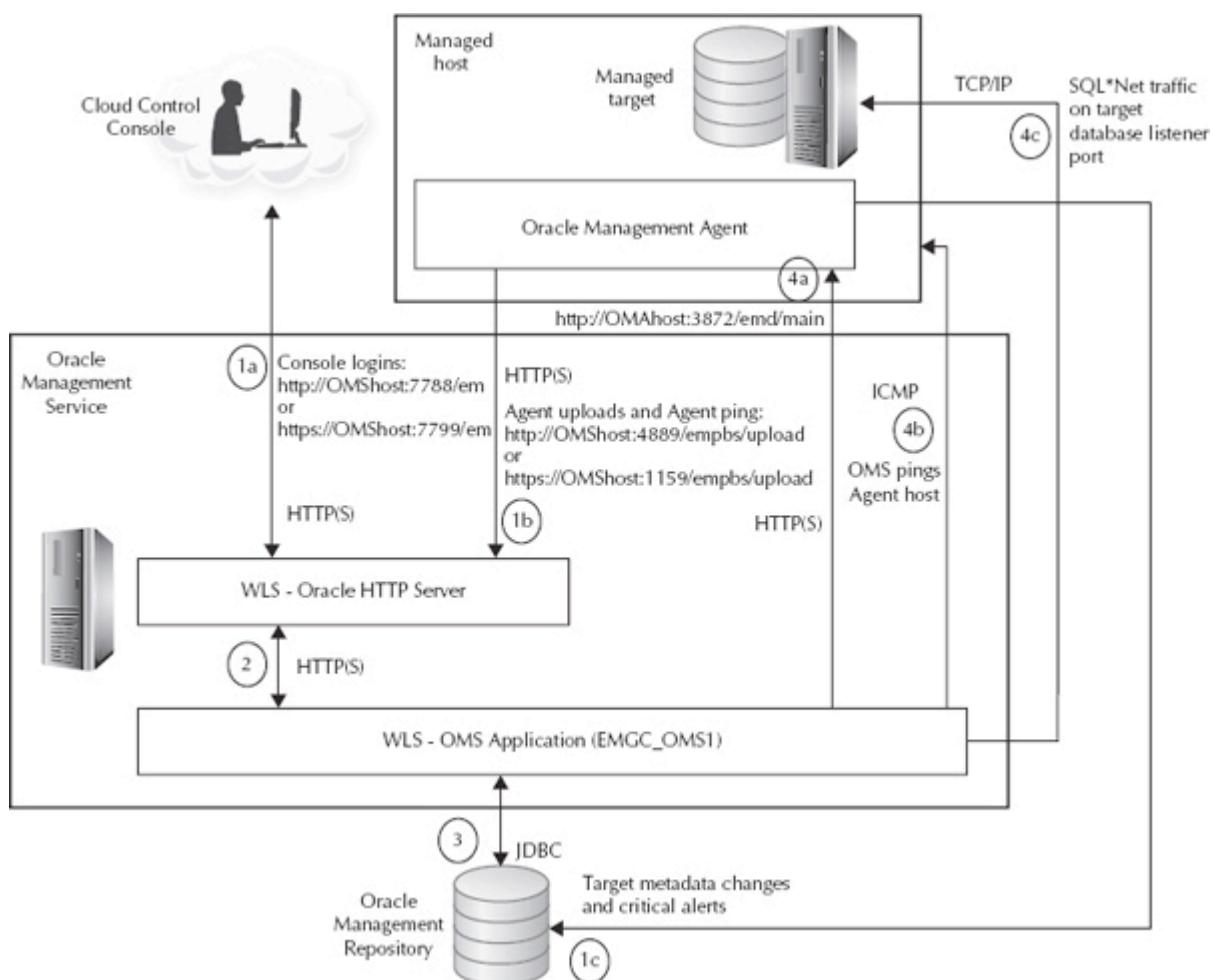
Nous allons maintenant examiner le schéma utilisateur de OMR ainsi que le schéma propriétaire, les « tablespaces » (segments logiques de bases de données) et des objets qui font partie de ces schémas. L'utilisateur SYSMAN correspond à la fois au schéma propriétaire et au compte par défaut du Super Administrateur. On ne peut supprimer ou renommer ce compte, celui-ci est utilisé pour :

- Effectuer la configuration de Cloud Control comme par exemple la création de privilèges, de rôles, de comptes administrateurs ou de règles de notifications.
- La découverte de nouvelles cibles
- La création de tâches génériques pouvant être exécutées sur tout hôte ou base de données.

III.1.6 Flux de données

Afin de mieux comprendre le modèle d'architecture de CC, nous allons maintenant nous intéresser à la façon dont les composants interagissent. Le diagramme ci-dessous montre les différentes interactions qui s'opèrent au sein de l'outil.

Figure 5: Flux de données



Nous allons procéder étape par étape en suivant le flux de données :

1°) La console OEM et les agents peuvent utiliser trois types de communications différents

a) Nous nous identifions dans la console en se connectant à l'adresse <http://<serveurhôteOMS>/<port>/em> via le serveur HTTP Oracle (OHS) du WLS. L'URL d'identification dépend de la sécurité de la connexion utilisée par l'administrateur.

- Connexion sécurisée : <https://<serveurhôteOMS>:7799/em>
- Connexion non-sécurisée : <http://<serveurhôteOMS>:7788/em>

- b) L'agent envoie les métriques qu'il récolte et les alertes qu'il détecte à l'URL du serveur HTTP Oracle du serveur WebLogic. OMA envoie également périodiquement des messages test appelés « Agent ping » à son service OMS lui faisant état de sa disponibilité. L'URL par défaut des deux types de communication se font via une connexion sécurisée ou non-sécurisée définie dans la propriété « REPOSITORY_URL » du fichier de configuration « emd.properties ».
 - Connexion sécurisée : <https://<serveurhôteOMS>:1159/empbs/upload>
 - Connexion non-sécurisée : <http://<serveurhôteOMS>:4889/empbs/upload>
- c) L'agent contourne le service OMS en se connectant directement à la base Repository pour lui rapporter tout changement des métadonnées des cibles supervisées et toutes alertes critiques.

2°) L'administrateur établit sa demande dans la console ou l'agent émet la demande à OMS pour la transmettre via le protocole HTTP ou HTTPS à l'application OMS

3°) Le service de supervision d'Oracle envoie la requête émise de la console ou de l'agent à la base de données dépôt via JDBC. Dès réception, OMS affiche le résultat de la requête dans la console administrateur.

4°) OMS communique avec OMA de plusieurs façons :

- a) OMS transmet directement les données à l'agent via HTTP(S) à l'agent intégré au Listener HTTP. Celui-ci écoute l'URL de l'agent à l'adresse : [http\(s\)://<OMAhost>:3872/emd/main](http(s)://<OMAhost>:3872/emd/main) (https par défaut), défini par la propriété « EMD_URL » localisée dans le fichier de configuration de l'agent « emd.properties ». OMS soumet également des tâches de différentes natures à travers cet URL.
- b) Si la communication OMS-Agent échoue, le service OMS va vérifier le statut du serveur-hôte sur lequel l'agent réside en lui envoyant des pings via des requêtes échos (Echo Requests) passant par le protocole Internet Control Message Protocol (ICMP).
- c) OMS envoie toute les requêtes SQL*NET aux ports TCP des Listeners des bases de données supervisées sur les serveurs-hôtes où les agents sont installés. (Ex : Application de patch sur une base de données)

Toutes ces informations peuvent être utiles pour identifier les sources possibles d'un problème donné.

A travers l'étude détaillée de l'architecture d'OEM, nous avons pu comprendre le fonctionnement interne de ses différents composants qui sont à l'origine de flux de données complexes. Cette analyse va maintenant nous permettre de comprendre les différents choix d'architecture que nous pouvons adopter pendant la phase de déploiement du logiciel.

III.2 Les choix d'implémentation d'OEM Cloud Control 12c

Avant d'installer Cloud Control, nous devons prendre des décisions clés concernant le choix d'architecture adopté par OEM 12c. De cette façon, nous nous assurons que le système sur lequel nous opèrerons répondra aux prérequis nécessaires à la supervision de l'infrastructure informatique d'Essilor. Nos décisions doivent prendre en compte des critères importants tels que le niveau de disponibilité nécessaire à l'environnement Cloud Control ainsi que le plan de récupération à adopter après désastre. Ces types de questions doivent peser sur le choix architectural de CC que nous implémenterons.

Afin de fournir un haut niveau de disponibilité (High Availability ou HA) et de reprise après sinistre (Disaster Recovery ou DR), nous avons besoin de faire appel aux services d'Oracle et/ou à d'autres technologies dont *Oracle Real Application Clusters* (RAC), *Oracle Automatic Storage Management* (ASM), *Storage Array Networks* (SAN) et *Network Attached Storage* (NAS), des solutions externes de récupération du cluster à froid (*Cold Failover Cluster* ou CFC), *Oracle Data Guard*, *Oracle Recovery Manager* (RMAN), *Oracle Flashback*, des pare-feux, des serveurs proxys et des serveurs de répartition de charges (*Server Load Balancing* ou SLB).

Nous n'avons pas besoin d'intégrer ces technologies HA et DR lorsque l'on installe pour la première fois *Oracle Cloud Control* mais il peut s'avérer plus facile de le faire en premier si certains prérequis de l'outil le demande. Il a fallu que nous prenions en compte des décisions préliminaires concernant l'architecture à adopter pour permettre à ces technologies d'être implémentées dans le futur.

Cette solution temporaire a pour but de donner le temps nécessaire à notre équipe DBA pour la mise en place d'une architecture Cloud Control HA/DR plus conforme. Une analyse coût/bénéfice doit être effectuée et prise en compte pour évaluer les économies de main-d'œuvre réalisées via la construction d'une architecture complète d'un système CC 12c vis-à-vis des coûts de reconfiguration des éléments de Cloud Control effectuée après mise en place de l'outil. Cette analyse a donc pour objectif d'arriver à une architecture finale de la façon la plus efficiente.

Aux bénéfices fournis par l'implémentation de CC s'ajoutent encore d'autres avantages que l'on peut tirer pour la reconfiguration des solutions HA/DR :

- Nous pouvons compter sur les fonctionnalités propres à Cloud Control pour améliorer les solutions de hautes disponibilités et de récupération après sinistre qui ont été déployées. Par exemple, OEM 12c peut aider à construire ou à convertir la base Repository pour *Oracle Real Application Cluster* qui bénéficie de meilleurs standards de disponibilités. Cet outil peut également créer dans un premier temps une base de données temporaire pouvant héberger les données de la base de dépôt et la placer dans un second temps dans une configuration Data Guard en tant que base primaire.

Cloud Control peut être utilisé pour définir et pister un Contrat de Niveau de Service (Service Level Agreement ou SLA) et de mesurer la disponibilité et la performance de l'outil vis-à-vis de ce même SLA. A partir de cette donnée, nous pourrions convenir quant à la nécessité d'implémenter des instances OMS supplémentaires ou de convertir la base Repository en RAC pour satisfaire le SLA mis en place.

- Il est possible de mettre en place un système Cloud control supervisant un environnement de production et de le reconfigurer pour qu'il supervise un autre type d'environnement. Cela se fait par la suppression des cibles de production et par la découverte et l'ajout de nouvelles cibles.

Que l'on décide de mettre en place un environnement Cloud Control basique en laissant de côté les éléments de configurations avancée ou d'installer un environnement CC avec les technologies HA et DR, nous devons prendre deux décisions clés concernant l'architecture d'OEM 12c avant de l'installer. Pour cela nous nous sommes posés les questions suivantes :

- Combien d'environnements Cloud Control devons-nous mettre en place ?
- Quel est le type d'installation dont nous avons besoin ?

III.2.1 Définition du nombre d'environnements Cloud Control mis en œuvre

Un environnement Cloud Control se définit par un système composé d'un ou plusieurs couples de serveurs-hôtes OMS et OMR associé(s) à des agents OMA sur les serveurs-cibles supervisés. Les environnements CC fonctionnent de manière indépendante. Ils ne communiquent pas entre eux et on ne peut pas les lier entre eux ou les sérialiser. La décision de la mise en place de plusieurs environnements de supervision OEM est dictée par plusieurs choix :

- Nous pouvons faire le choix d'utiliser deux environnements CC. Nous pouvons choisir par exemple de séparer la supervision de notre environnement de production de nos autres environnements moins stratégiques.
- Les limitations du réseau d'entreprise peuvent exiger l'instauration de plusieurs systèmes OEM.

III.2.2 Environnement de production Vs Environnement de non-production

L'élément décisif qui va déterminer le nombre d'environnements Cloud Control que nous utiliserons dépend du choix que nous aurons fait pour superviser nos environnements de production et de non-production. En effet si nous décidons de séparer leur supervision, le nombre d'environnements va augmenter. Nous sommes donc confrontés à deux choix de stratégie :

- Installer deux environnements Cloud Control, un pour les cibles de production et l'autre pour ceux de non-production et de gestion de l'instance de CC (Mises à jour, correctifs, etc.) pour tester les changements d'infrastructure d'OEM et de les appliquer sur l'instance dédiée à la production.
- Installer un seul environnement Cloud Control pour les univers de production et de non-production.

Il semble important de souligner que les entreprises utilisent souvent plusieurs instances d'OEM pour superviser des environnements de non-production également. Une pour le développement, une pour l'intégration etc. Toutefois, un environnement de supervision est dans la plupart des cas suffisant pour tester tout changement d'infrastructure de CC.

La meilleure pratique (Best Practice) reconnue est d'utiliser un système Cloud Control dédié pour superviser des cibles de production. Cette méthode empêche toutes cibles de non-production d'impacter sur le Framework Cloud Control de production.

Si nous faisons le choix de séparer la supervision de nos environnements de production et de non-production, l'usage est d'implémenter d'abord la solution OEM 12c pour les environnements de non-production. Nous devrions alors assigner un ou plusieurs serveurs pour démarrer les installations. Dès lors, nous devrions avoir décidé si ces serveurs-hôtes seront attribués à un environnement CC de production ou de non-production.

Nous allons maintenant développer deux sections où nous déterminerons dans un premier temps le nombre de serveurs OMS et de serveurs hébergeant OMR nécessaires. Nous nous intéresserons dans un second temps à la question de la réunion de ces deux composants sur le même serveur.

III.2.3 Décision du choix d'architecture d'Oracle Cloud Control

Les choix architecturaux de Cloud Control auxquels nous sommes confrontés doivent répondre aux questions essentielles concernant les diverses implémentations possibles d'OEM.

- Quelle architecture de base de données devons-nous utiliser pour la base Repository ?
- Quelle architecture OMS devons-nous déployer ?
- Avons-nous besoin que la base OMR et OMS soient sur le même nœud lorsque ces deux éléments sont physiquement au même endroit ?

Tableau 2: Ordre de grandeur des sites supervisés

Taille des sites monitorées par Cloud Control	Nombre de nœuds actifs OMR	Nombre de serveurs OMS actifs	Localiser OMR et OMS sur le même hôte	Nombre total de serveurs demandés pour OMR et OMS
Petit <1000 cibles <100 Agents <10 Sessions concurrentes utilisateur	1 (2-nœuds RAC si la technologie HA est requise)	1 (2 si HA requise)	Oui	1 (2 si HA requise)
Moyen 1000 - 10000 cibles 100 - 1000 agents 10 - 25 Sessions concurrentes utilisateur	2 nœuds RAC	2	Non	4
Grand >10000 cibles >1000 agents >25 Sessions concurrentes utilisateur	2 nœuds RAC	3 ou plus	Non	5 ou plus

Le tableau ci-dessus répond de façon résumée aux trois questions précédentes en listant les configurations recommandées par Oracle. Celles-ci sont données en fonction de la taille du site de production que l'on veut superviser. Cet ordre de grandeur est défini par trois variables qui sont le nombre de cibles, d'agents et de sessions concurrentes actives. Pour chaque taille de site, le tableau liste le nombre de serveurs OMS et OMR actifs * ainsi que le nombre total de serveurs requis pour une taille de site donnée. Ce nombre minimum de serveurs prend déjà en compte la solution où OMS et OMR sont sur le même serveur.

Remarque : Si nous avions besoin d'une haute disponibilité pour nos bases tierces OMR, nous en aurions également besoin pour les instances OMS (actives ou passives). En effet, OMR et OMS doivent fonctionner pour permettre à Cloud Control de rester opérationnel. Toutes les configurations listées ci-dessous prennent en considération ces éléments de HA.

III.2.4 Décision concernant sur le choix d'architecture de la base de données Repository

Nous pouvons installer OMR à partir de n'importe quelle version certifiée de base de données pour Repository sur une plateforme donnée. Néanmoins, Oracle nous recommande d'utiliser la version la plus récente de la v11gR2. L'architecture de la base OMR à adopter dépend des critères de haute disponibilité qui sont en vigueur chez Essilor et de la taille de notre environnement à superviser. Il existe deux choix d'architecture CC disponible : une qui ne dispose que d'une seule base Repository et une autre qui en dispose de plusieurs. Si nous avons besoin d'une haute disponibilité pour notre base ou si nous devons superviser un environnement informatique comprenant plus de 1000 cibles, Oracle nous recommanderait alors d'utiliser plusieurs instances de bases de dépôt. Cependant, nous ne nous situons pas dans ce cas, par conséquent une seule base Repository suffit. Nous avons donc le choix entre deux types de base de données uniques :

- **Standalone Database** : Une seule instance de base de données peut être utilisée. Celle-ci dispose de fichiers stockés sur le serveur.
- **Oracle Restart database** : Il s'agit d'une fonctionnalité des bases de données en version 11g. Celle-ci est utilisée sur des serveurs qui ne sont pas mis en grappe. Oracle Restart redémarre automatiquement les éléments de la base de données (instance, service, listener et instance ASM) après un échec d'un matériel ou d'un logiciel ou alors en cas de redémarrage intempestif du serveur-hôte.

Toutefois, bien que cette fonctionnalité puisse s'avérer utile, celle-ci n'est pas considérée comme une solution de haute disponibilité car il n'existe pas de seconde instance de Repository pouvant prendre le relais en cas de panne critique. Par conséquent, une base de données Oracle Restart doit être considérée comme une simple base de données pendant l'étape de dimensionnement de Cloud Control et d'évaluation des critères HA.

III.2.5 Décision concernant le choix d'architecture d'Oracle Management Server

Il existe plusieurs choix d'implémentation pour maintenir un haut niveau de disponibilité sur le serveur OMS. Ces solutions vont dépendre de nos besoins en termes de haute disponibilité.

Serveur OMS simple : Un seul serveur OMS peut suffire si l'environnement supervisé par OEM 12c est petit (inférieur à 1000 cibles) et s'il ne nécessite pas d'être hautement disponible. Ce cas correspond à celui d'Essilor.

Multiple Serveurs OMS : Si nous avons besoin d'une haute disponibilité pour notre serveur OMS, Nous devrions décider du nombre de serveurs OMS à implémenter et du mode de configuration dans lequel ils vont fonctionner. Il peut s'agir de configuration Actif/Actif ou Actif/Passif. Nous devrions également faire le choix de la localisation de ces serveurs OMS.

- Pour maintenir un haut niveau de disponibilité sur de petits sites, deux serveurs OMS sont requis. Ils peuvent être configurés en mode Actif/Actif ou Actif/Passif. (Deux serveurs sont en effet requis pour la HA car un des deux serveurs peut rester passif dans des environnements relativement petits car la charge des traitements effectués reste gérable pour une seule instance d'OMS).
- Pour les sites supervisés de tailles moyennes ou grandes, deux serveurs OMS en mode Actif/Actif suffisent. Toutefois, il existe également une solution réunissant les deux modes de configurations cités. On peut par exemple utiliser la configuration Actif/Passif sur chaque OMS déjà implantés en mode Actif/Actif. Si les serveurs OMS sont géographiquement éloignés l'un de l'autre, mettre en œuvre une solution CFC (Cold Failover Cluster) pour chaque OMS actif peut sembler redondant voire inutile étant donné que les serveurs OMS actifs fournissent déjà un bon niveau de HA. Cependant, le CFC a l'avantage de fournir une solution locale de HA.
- Il existe plusieurs facteurs pouvant justifier l'implémentation de plusieurs serveurs OMS. La flexibilité, la haute disponibilité et les besoins en termes de couverture réseaux représentent tous des raisons valables pour mettre au point une telle configuration. Le dernier facteur précédemment évoqué est particulièrement important car la communication Agent-OMS nécessite une bande passante d'au moins 300 Kbps et une latence maximale de 300 ms.

- Nous pourrions installer un serveur OMS actif ou passif à l'endroit où le dispositif de récupération après désastre (Disaster Recovery ou DR) est mis en place. Nous pourrions configurer une instance OMS de veille depuis le lieu de récupération prête à l'emploi en cas de désastre. Une instance active permettrait quant à elle de l'utiliser soit en SLB (Server Load-balancer) pour répartir les charges entre les différents serveurs OMS actifs soit en SLB géographique ayant l'avantage de donner plus de flexibilité vis-à-vis des contraintes réseaux concernant les communications OMS-Agent.

L'expert administrateur base de données Oracle de notre équipe et moi-même avons fait le choix de l'implémentation d'une instance unique OMS au sein de l'environnement Cloud Control étant donné le nombre modeste de cibles à superviser au sein de nos systèmes de production (<1000 cibles).

III.2.6 Décision concernant le choix de regroupement du serveur OMS et de la base OMR

Après avoir fait le choix des architectures d'OMS et d'OMR, nous sommes maintenant confrontés à la question de la réunion de ces éléments sur le même serveur-hôte. Il existe plusieurs solutions à cette question car celles-ci dépendent des choix architecturaux qui ont été pris concernant la base Repository et OMR :

- **Installation d'OMR et d'OMS sur des serveurs hôtes différents** : C'est la configuration adéquate pour des environnements Cloud Control de moyenne et de grande taille (>1000 cibles).
- **Installation d'OMR et d'OMS sur le même nœud** : OMS et OMR peuvent être installés sur le même nœud. Celui-ci peut être répliqué pour des raisons de haute disponibilité et/ou de flexibilité.
- **Installation d'OMR et d'OMS sur le même serveur-hôte** : Cette solution n'est appropriée que sur des environnements Cloud Control de petites tailles (<1000cibles) qui ne requiert pas d'une haute disponibilité. C'est la solution la plus adéquate pour l'environnement informatique d'Essilor.
- **Installation d'OMR et d'OMS sur de multiples nœuds** : Installer des instances OMS sur des nœuds de RAC OMR est une solution supportée par OEM 12c et appropriée pour des environnements CC de petites tailles. Toutefois, cette configuration peut présenter certains dangers pour des environnements Cloud Control de production de moyennes et de grandes tailles. En effet, il existe un danger de saturation des ressources disponibles des nœuds pour OMR et OMS pendant les périodes de fortes charges. C'est la raison pour laquelle les instances OMS doivent être installées sur des nœuds dédiés, séparés des nœuds de bases de données OMR pour des sites OEM de moyennes ou de grandes tailles.

Notre équipe DBA a fait le choix de l'installation d'OMR et d'OMS sur le même serveur hôte étant donné la petite taille de l'environnement Cloud Control supervisé. Les périodes de fortes charges étant facilement gérées par OEM, nous avons décidé de maintenir ce type de configuration pour OEM 12c.

III.3 Conclusion

Nous avons pu grâce à l'analyse des différentes architectures disponibles dans Cloud Control de choisir la configuration de déploiement la plus adapté aux besoins de notre entreprise. Nous avons finalement opté pour l'installation d'OMR et d'OMS sur le même serveur-hôte. Deux facteurs essentiels ont été pris en compte :

- La petite taille de nos environnements de supervisions
- L'absence de besoin en termes de haute disponibilité

Maintenant que nous avons choisi la méthode de déploiement de Cloud Control, nous pouvons passés à l'étape de réalisation du projet.

IV Réalisation

Dans les parties précédentes nous avons détaillé les prérequis liés à l'installation des différents composants d'OEM 12c et trouvé des solutions pour y répondre. Puis nous avons choisi, à travers une étude approfondie des différents choix d'implémentation proposé par Cloud Control, l'architecture OEM la plus adapté à nos besoins.

IV.1 Introduction

Nous allons maintenant nous intéresser aux processus d'installation d'une base de données 11gR2 préconfigurée pour héberger la base Repository (base de dépôt des données OEM) de OEM Cloud Control. Distinguons les étapes suivantes :

- **Partie I :** Cette première partie explicite les étapes nécessaires à l'installation d'une base de données en mode Repository, celle-ci se décompose en deux sous-parties :
 - Effectuer une installation logiciel simple (software-only) d'une base de données 11gR2 et lui appliquer le plus récent ensemble de patchs disponible (Patch Set Update ou PSU).
 - Créer une base de données via l'assistant de configuration de base de données (Database Configuration Assistant ou DBCA) avec le nouveau modèle nommé « DB11.2.0.4 EM seed database » qui préconfigure la base Repository avec tous ses objets.
- **Partie II :** Cette seconde partie décrit comment terminer la configuration de la base de données pour effectuer des opérations spécifiques à une base Repository.
 - Configuration des redo logs
 - Implémentation du HugePage
 - Activations de fonctionnalités avancées

Dans ces deux parties, nous allons expliciter toutes les étapes d'installation d'une base de données 11gR2 selon les meilleures pratiques de l'Architecture Oracle de Disponibilité Maximum (Oracle Maximum Availability Architecture ou MAA).

IV.1.1 Installation d'une base de données Repository

Avant de procéder à l'installation d'OEM 12c, nous devons dans un premier temps installer une base de données destinée à héberger OMR.

Nous allons expliquer les procédures à suivre concernant les installations de Grid Infrastructure (GI), de la base de données et de l'application de leur PSU respectif. Ceux-ci peuvent être appliquées sur des architectures de base de données indépendantes ou en grappe (RAC).

- **1^{er} étape** (facultative) : Installation de GI Oracle home avec son dernier PSU (Si nous avions recours à l'architecture de GI). Nous n'utiliserons pas cette solution toutefois nous avons jugé important d'inclure les procédures à suivre pour mettre en œuvre cette méthode.
- **2^{ème} étape** : Installation de la base de données Oracle 11gR2 avec son dernier PSU. Si nous utilisions GI, nous devrions appliquer le dernier PSU de GI sur la base de données car celui-ci contient également la même version du PSU pour la base de données elle-même.

Il est important de respecter l'ordre des étapes indiquées. Si nous utilisions GI, nous devrions procéder à l'installation de la base de données et de son PSU seulement après avoir installé et patché GI. Patcher le logiciel de base de données avant que celle-ci ne soit installée faciliterait le processus d'installation car cela permettrait de contourner les étapes de post-installation des composants. Il s'agit ici de la meilleure méthode (Best practice) concernant la création d'une base de données Oracle.

En règle générale, nous procéderions à l'installation de GI et de son dernier PSU puis refuserions l'étape de création de la base. Dans un second temps nous appliquerions GI avec son dernier PSU et ferions de même pour la base de données. Enfin, Nous lancerions DBCA en mode indépendant (standalone) pour enfin créer la base de données.

Remarque : Il est fortement recommandé par Oracle d'installer la dernière version certifiée de base de données et du PSU pour laquelle il existe un modèle Enterprise Manager dans DBCA pour profiter des dernières fonctionnalités de la version 11.2, des derniers correctifs de bugs et de l'utilisation d'*EM template*.

Bien que nous ayons opté pour une installation basique de bases de données (correspondant uniquement à la deuxième étape citée ci-dessus) pour héberger les données d'OMR, nous avons décidé d'explorer les opportunités que pourraient nous apporter l'architecture Grid Infrastructure. En effet, le seul fait de pouvoir redémarrer automatiquement tous les services d'une base de données après le redémarrage (prévu ou imprévu) d'un serveur représenterait une amélioration non négligeable concernant la disponibilité de nos bases de données. De ce fait, nous allons brièvement nous intéresser aux étapes d'installation de ce logiciel.

IV.1.2 Etape 1 : Installation du logiciel Grid Infrastructure (facultative)

La procédure d'installation de GI et de son dernier PSU peut différer selon le choix d'architecture adopté par la base de données (Simple ou en grappe) :

- Installation de GI sur serveur indépendant (Oracle Restart).
- Installation de GI sur un cluster de serveurs pour une configuration en RAC ou ORON.

Nous développerons ici brièvement les étapes fondamentales de ces procédures.

Durant toutes les étapes d'installation, nous devons prendre le soin de vérifier que la version de la base de données installée par GI et celle de Cloud Control implémentée au sein du système informatique sont certifiées pour fonctionner ensemble.

a. Installation de la dernière version logicielle GI 11gR2

Si nous choisissons d'utiliser Grid Infrastructure, nous devons installer la dernière version de l'outil disponible pour la plateforme du serveur sur lequel l'installation est mise en œuvre. Il faut de plus que nous nous assurons que la version du logiciel implémentée est certifiée pour fonctionner avec la Cloud Control 12c et qu'il existe la version équivalente pour la base *template*.

b. Installation du dernier PSU de GI pour le logiciel de la base de données 11.2.0.x

Après l'installation de la dernière version de Grid Infrastructure, il nous faut lui appliquer le dernier ensemble de correctifs (PSU).

IV.1.3 Etape 2 : Installation du logiciel de base de données

Nous allons expliciter la procédure classique de l'installation du logiciel de la base de données 11gR2.

Nous indiquerons cependant les options à suivre qui sont adaptées aux choix d'Essilor.

Option d'installation : Il nous faut choisir l'option « Installer uniquement le logiciel de base de données ». Comme nous l'avons déjà expliqué, nous devons d'abord appliquer le dernier PSU de la base de données avant d'installer la base de données elle-même (étape suivante).

Option d'installation Grid : Nous avons le choix entre trois options d'installation. Seul le choix en bleu est adapté au contexte et aux choix d'Essilor :

- Installation d'une seule instance de base de données (Single-instance database)
- Installation de bases de données en mode Oracle Real Application Clusters (mode grappe)
- Installation de bases de données RAC One Node (Une seule instance de base de données est activée parmi la grappe)

Nous avons maintenant accès aux éléments de configurations suivant via DBCA :

- Langage du produit : Il s'agit de l'étape de sélection de la langue, Essilor demande d'installer les produits Oracle en anglais afin d'être en accord avec la configuration effective sur les serveurs de Thaïlande.
- Type de la base de données : Pour les milieux professionnels comme le nôtre, il nous faut choisir la version Enterprise Edition mais ce n'est pas tout : nous devons cocher la case de partitionnement Oracle. C'est une option obligatoire car la base Repository crée un nombre conséquent de tables partitionnées et d'indexes dans le schéma SYSMAN afin de stocker les nombreuses métriques de supervision. Les autres éléments listés sont facultatifs.
- Localisation de l'installation : nous devons spécifier un certain nombre d'éléments concernant le chemin d'installation du logiciel et celui de la base Oracle :
 - Chemin d'installation de la base (Oracle Base) : **/u01/app/oracle**
 - Chemin d'installation logiciel (Software Location) :
/u01/app/oracle/product/11.2.0/db_1
- Groupe d'appartenance système (Operating System Groups) : Il nous faut spécifier les valeurs concernant les groupes d'appartenance système pour les groupes OSDBA et OSOPER :
 - Groupe d'administrateur base de données OSDBA : dbdb. Essilor a choisi la valeur dbdb.
 - Groupe des opérateurs OSOPER (Facultatif) : dbdb. Essilor ne spécifie pas ce champs
- Sommaire : Vérification des choix effectués et finalisation de l'installation.

IV.1.3.1 Installation du dernier PSU

Comme nous l'avons déjà mentionné, après l'installation du logiciel de base de données nous devons lui appliquer son PSU le plus récent. Une liste des PSU est disponible dans les notes MOS (My Oracle Support) n°7566671.1 au chapitre « Patchs Oracle Recommandés – Bases de données Oracle ».

IV.1.3.2 Modèle Enterprise Manager DBCA

Avant de commencer cette partie, il nous faut impérativement nous assurer que le logiciel Grid Infrastructure (si GI est choisi) ou que le logiciel de base de données ait été installé avec son PSU le plus récent. Cette dernière étape consiste à créer une base de données conforme pour servir de base dépôt (Repository) en faisant appel à l'assistant de configuration de base de données DBCA. Celui-ci est directement exécutable dans le répertoire \$ORACLE_HOME/bin.

Pour créer une instance unique (single instance) de base de données pour la base Repository, Oracle recommande d'utiliser son propre modèle de base de données nommée *EM template* que nous allons brièvement introduire.

Introduction au modèle EM template

En plus de créer la structure adéquate, EM template définit un certain nombre de propriétés qui vont s'aligner avec les prérequis de la base Repository. Par exemple, l'outil peut définir automatiquement les valeurs les plus compatibles concernant attributs de stockage, les paramètres d'initialisation etc.

Dans la première version de Cloud Control (v12.1.0.1), seul l'installateur de CC pouvait installer et configurer la base Repository. Toutefois, les versions CC 12.1.0.2 ou supérieurs contiennent en son sein un modèle DBCA préconfiguré appelé « DB11.2.0.3 EM seed database » ou « EM template » qui va nous permettre de créer une base de données 11.2.0.3 contenant une base Repository préconfigurée. De telles bases de données diffèrent des bases de données classiques tant dans leurs structures que dans leurs données. Dans ce cas précis, la base créée par le EM template issue de DBCA contiendra dès sa création une base de données Repository contenant :

- Tous les schémas requis par OEM Cloud Control 12c : *SYSMAN*, *SYSMAN_APM*, *SYSMAN_MDS*, *SYSMAN_OPSS* et *SYSMAN_RO*.
- Tous les espaces de stockages logiques (Tablespaces) : *MGMT_AD4J_TS*, *MGMT_TABLESPACE* et *MGMT_ECM_DEPOT_TS*)
- Les différents objets de bases de données.

Le modèle EM template apparaît dans l'outil DBCA dans la fenêtre des choix des modèles de bases de données à côté des autres templates standard.

Vis-à-vis de cette option, l'équipe DBA a opté pour suivre les recommandations d'Oracle et de sélectionner le modèle spécialement destiné à OEM 12c. En effet, faire le choix d'un modèle standard d'EM template pour une base Repository demanderait des étapes de configurations manuelles supplémentaires et fastidieuses dans les étapes d'installations et de post-installations de la base de données.

Cela impliquerait notamment de consulter la documentation oracle en ligne pour effectuer une série de scripts supplémentaires sur la base Repository. Cela aurait pour effet de ralentir considérablement l'étape de configuration d'OMR.

IV.1.3.3 Configuration de la base dépôt avec EM template

Avant l'avènement du modèle *EM template* pour les versions Cloud Control 12.1.0.2 et supérieures, il nous fallait sélectionner un modèle EM générique dans DBCA et configurer manuellement les propriétés de la base de données pour qu'elle puisse accueillir une base Repository. Par exemple, nous devions spécifiquement expliciter les paramètres d'initialisation et la taille des journaux d'évènements (Redo Log). Aujourd'hui, quasiment toutes les étapes de configuration de la base de données sont effectuées par l'assistant de configuration avec le template EM. Celui-ci est spécialement conçu pour créer une base de données avec les propriétés, les structures, les données et les objets adéquats pour servir de base Repository à Cloud Control. Néanmoins, il existe plusieurs prérequis et quelques bonnes pratiques qu'il nous reste à effectuer.

L'équipe DBA a fait le choix d'adopter la plupart des éléments de la configuration par défaut proposée par le template EM de l'outil DBCA pour des raisons de simplicité et de maintenabilité et d'adéquation avec nos besoins actuels. Nous nous intéresserons donc dans un premier temps aux options qui diffèrent vis-à-vis de la configuration par défaut puis, dans un deuxième temps, aux étapes de configuration de la base Repository que le template EM ne couvre pas.

IV.1.3.4 Paramètres d'initialisation

Choix sur le type de mémoire utilisé : Lors de la configuration de la base Repository via le logiciel DBCA, il est possible de choisir un certain nombre de paramètre d'initialisation dont celui de la mémoire. Lors de cette étape, nous avons le choix entre l'option de gestion automatique de la mémoire (Automatic Memory Management ou AMM) qui est coché par défaut et l'option de gestion automatique du partage de la mémoire (Automatic Shared Memory Management ou ASMM). Ces options sont toutes les deux des choix valides pour gérer la mémoire dédiée à la base Repository. Néanmoins, nous avons optés pour le type de mémoire ASMM car seul celui-ci permet l'implémentation de la configuration HugePages qui fait partie des meilleures pratiques (Best Practices ou BP) préconisées par Oracle. Bien qu'il s'agisse ici d'une configuration optionnelle, celle-ci permet de bénéficier d'un plus grand espace de mémoire partagé (System Global Area ou SGA) pour tous les processus Oracle. Par conséquent, le HugePages améliore les performances de la mémoire même pour des allocations mémoires très faibles (2 Go minimum).

Nous nous intéresserons plus en détails à la mise en place de cette configuration un peu plus loin dans cette partie.

Choix sur le jeu de caractère utilisé : Lors du choix du jeu de caractères (Character Set) utilisé par la base de données, le modèle EM Template choisi par défaut celui qui est utilisé par le système d'exploitation du serveur. Nous avons choisi comme Oracle le recommande, d'adopter le jeu de caractère Unicode qui permet de stocker plusieurs groupes de langages. Bien que la politique d'Essilor soit d'utiliser prioritairement l'anglais sur ses logiciels, notre équipe DBA a choisi cette option pour des raisons de flexibilité.

Redéfinition de la taille des groupes des Redo Logs : Lors du choix de l'allocation mémoire des groupes de redo logs, il nous faut spécifier à la fois le nombre de groupes à créer et le nombre de membres à utiliser dans chaque groupe.

Concernant la taille des fichiers redo que nous devons adopter, le modèle EM Template crée par défaut trois groupes de redo logs de 100 Mo. Notre équipe DBA a fait le choix d agrandir cette taille à 600 Mo pour respecter les recommandations d Oracle. En effet cette taille est plus appropriée avec le nombre de redo logs que peut générer un petit environnement de production qui change de fichiers logs toutes les 20 minutes. De plus agrandir la taille de ces fichiers diminuent les opérations de maintenance les concernant et améliore les performances de l écriture et de l archivage de la base de données.

Il est plus ais é de laisser l installateur DBCA cr éer des fichiers redo logs avec la bonne taille m émoire que de la modifier manuellement plus tard. La taille pr éconis e de ces fichiers d pend de l importance du syst ème supervis e par Cloud Control. Voici le tableau ici des recommandations d Oracle :

Tableau 3: Adéquation entre la taille du site supervisé et la taille recommandée des redo logs

Taille du site supervisée	Taille recommandée des fichiers Redo Log (Mo)
Petite	600
Moyenne	1024
Grande	1536

Lors de l étape de cr éation des groupes de redo logs, le mod èle EM Template propose par d faut de ne cr éer que trois groupes de ces fichiers. Cependant, nous avons opt es pour la cr éation d un groupe supplémentaire servant de de groupe tampon (Buffer group) et ce, malgr é la taille modeste de notre environnement à superviser. En effet, une base de donn ées en mode ARCHIVELOG restera en suspend si un groupe de redo logs est sollicité mais ne peut pas t re archivé.

Enfin, concernant le nombre de membres redo log à cr éer pour chacun de ces groupes, nous avons opt e pour le multiplexage des fichiers redo log et les fichiers de contrôle. Il s agit ici d une Best Practice recommandée par Oracle et que nous avons adoptée.

Rappel : Les fichiers redo logs permettent à la base de garder une trace de toutes les altérations de donn ées, ainsi en cas de crash de la base, ils permettent de rejouer les modifications apportées à la base. Ces fichiers doivent t re au moins au nombre de deux et nécessitent une attention toute particuli ère tant au niveau de la sauvegarde que de l optimisation des acc ès.

En mode ARCHIVELOG, les redo logs sont archivés afin de garder une trace de toutes les modifications apportées et non pas seulement dans la limite de la taille des fichiers de redo log.

Sauvegarde du Template EM : Apr ès ces étapes de configuration du template EM, nous avons choisi comme nous le propose l outil DBCA de sauvegarder ce mod èle au cas o ù nous aurions besoin de cr éer un deuxième environnement Cloud Control. En effet la mise en place de nouvelles bases aux Etats-Unis et en Asie nous forcera peut- t re de monter des environnements de

supervision entièrement dédiés à ces sites. De ce fait, sauvegarder ce Template présenterait l'avantage de ne pas repasser par les étapes de configuration du modèle lors de la mise en place d'une future base Repository.

IV.2 Configuration de la base de données Repository

L'étape de configuration de la base Repository a un double objectif : elle doit répondre aux prérequis imposés par l'installation d'OEM 12c et d'implémenter un certain nombre de fonctionnalités nécessaires au fonctionnement et à la fiabilité de la base Repository.

Les étapes de configuration de la base Repository qui suivent sont à effectuer après l'exécution de DBCA.

La première étape consiste à renommer les fichiers de données (Datafile) de Cloud Control pour qu'ils correspondent aux noms attendus par l'installateur de Cloud Control : *Oracle Universal Installer* ou CC OUI. De plus, ayant choisi le mode de gestion des données OMF (*Oracle Managed File*) nous devons désactiver l'optimisateur de récupération automatique des statistiques. Cette étape doit faire l'objet d'une attention toute particulière car elle peut bloquer le logiciel OUI de Cloud Control.

Les autres étapes de configuration ont pour principal objectif de suivre les *Best Practice* préconisés par Oracle en termes de disponibilité d'une base de données 11gR2 (*Maximum Availability Architecture* ou MAA). Ces meilleures méthodes sont décrites dans la documentation que fournit Oracle sur son site internet et sont aussi bien pertinentes pour une base Repository que pour une base de données standard.

Ces lignes directrices peuvent être mises en pratique à la fois sur des bases en mode Grappe (RAC) et sur des bases de données indépendantes. Voici donc les étapes de configurations additionnelles à effectuer sur la base Repository faisant partie des Best Practices reconnues par Oracle :

- 1) Renommage des fichiers de données Cloud Control destinés à aligner leur nom avec ceux attendus par l'installateur de Cloud Control OUI.
- 2) Désactivation de l'optimisateur de récupération automatique des statistiques.
- 3) Définition du paramètre d'initialisation compatible avec la version du patch appliquée à la base de données.
- 4) Création de groupes de redo logs additionnels (Ayant choisi le mode de gestion de stockage des données OMF, nous devons faire cette étape après avoir exécuté l'outil DBCA).
- 5) Vérification de l'adéquation de la configuration du système d'exploitation du serveur local avec la configuration NLS de la base de données Repository.
- 6) Vérification de l'adéquation des fuseaux horaires entre le système d'exploitation du serveur et celui de la base de données.
- 7) Implémentation du HugePages.
- 8) Activation du mode Flashback pour la base de données.
- 9) Activation du mode FORCE LOGGING.
- 10) Activation du Block Change Tracking pour la mise en place de sauvegarde incrémentale.
- 11) Exécution du Kit de prérequis de OEM en mode indépendant.

Seules les étapes en bleu feront l'objet d'explications détaillées.

L'ordre d'implémentation de ces étapes n'a pas d'importance car celles-ci sont indépendantes les unes des autres.

Pour des raisons de sécurité, nous avons choisi d'effectuer une sauvegarde de la base de données Repository. De cette façon, la base données et sa configuration pourront être restaurées en cas d'erreurs irrécupérables de la base de données durant les manipulations à suivre.

IV.2.1 Renommage des fichiers de données Cloud Control

Ayant sélectionné le mode de gestion Oracle-Managed File durant la création de la base de données dans l'onglet « Chemin de stockage » de DBCA, nous devons impérativement renommer les trois fichiers de données créés par cet outil pour qu'ils correspondent aux noms attendus par le logiciel installateur de Cloud Control. En effet, il ne nous est pas possible de renommer directement les fichiers de contrôle durant l'étape d'installation d'OEM Cloud Control. Voici la marche à suivre :

```
SQL> select tablespace_name, file_name from dba_data_files;
SQL> Alter tablespace MGMT_AD4J_TS offline;
SQL> !mv o1_mf_mgmt_ad4_8gmfqckg_.dbf mgmt._ad4j.dbf
SQL> Alter database rename file
'/orahome/app/oraoem/oradata/EMREP/datafile/o1_mf_mgmt_ad4_8gmfqckg_.dbf' to
'/orahome/app/oraoem/oradata/EMREP/datafile/mgmt._ad4j.dbf';
SQL> Alter tablespace MGMT_AD4J_TS online;
```

IV.2.2 Désactivation de l'optimisateur de récupération automatique des statistiques

Il s'agit ici de l'unique prérequis auquel l'outil DBCA ne peut pas répondre pendant la phase de création de la base de données. Il s'agit ici d'une opération de maintenance à laquelle nous avons implicitement adhéré lorsque nous avons laissé par défaut l'option « Activer les tâches de maintenance automatique » dans les options de gestion de DBCA.

Notre expert administrateur base de données Oracle et moi-même avons laissé cette option cochée car elle permet d'activer deux tâches (jobs) supplémentaires qui s'avèrent utiles pour administrer plus facilement la base Repository. Il s'agit des fonctions « Auto Space Advisor » et de « SQL Tuning Advisor ».

La requête suivante permet d'afficher l'état de ces fonctionnalités :

```
SQL> Select CLIENT_NAME, STATUS FROM DBA_AUTOTAST_CLIENT ;
```

Tableau 4: Statut actif de l'Auto Optimizer Stats Collection

CLIENT_NAME	STATUS
Auto Optimizer Stats collection	ENABLED*
Auto Space Advisor	ENABLED
SQL Tuning Advisor	ENABLED

*Activé

Pour désactiver l'optimisateur automatique de récolte des statistiques, nous devons exécuter les commandes suivantes puis vérifier à nouveau le statut de cette fonctionnalité en exécutant de nouveau la commande explicitée ci-dessus :

```
SQL> exec DBMS_AUTO_TASK_ADMIN.DISABLE;
SQL> client_name => 'auto optimizer stats collection',
SQL> operation => NULL,
SQL> window_name=> NULL);
```

IV.2.3 Crédit de groupes de redo logs additionnels

Lors de la création de la base de données, l'assistant DBCA ne crée que trois groupes de redo logs qui représente le nombre minimum requis pour effectuer des opérations sur une base Oracle. Ayant voulu suivre les meilleures méthodes préconisées par Oracle, nous avons créé un groupe de redo log supplémentaire ([Groupe 4](#)). Ayant opté pour l'option OMF, nous devons créer manuellement ce groupe additionnel car l'outil DBCA n'est pas encore capable de gérer cette étape création.

Voici le nom de l'utilisateur système et la commande SQL qui nous ont permis de créer ce nouveau groupe :

```
ALTER DATABASE ADD LOGFILE GROUP 4 SIZE 600;
```

Implémentation des HugePages

Sur la plupart des systèmes d'exploitations UNIX (Linux et AIX compris) et Windows, Oracle recommande aux administrateurs de configurer l'option des HugePages (Grandes Pages) pour des bases de données dont le SGA (System Global Area) est supérieure à 2 Go. Cette option nous permet également de mieux supporter l'allocation mémoire des instances ASM (Automatic Storage Management). La fonctionnalité HugePages est aussi connue sous le nom de « Large Pages » pour les systèmes AIX et Windows. Afin de rester dans le contexte d'Essilor, nous ne parlerons ici que des étapes d'implémentation de cette fonctionnalité sur un système Linux x64.

HugePages est une fonctionnalité intégrée dans les systèmes Linux depuis la version 2.6 qui permet d'utiliser de grandes quantités de mémoire SGA de façon optimale en s'assurant que la mémoire ne fait jamais appel au disque dur. HugePages nous permet d'utiliser des pages mémoires beaucoup plus importantes (2 Mo ou 4 Mo) comparées aux pages par défaut de taille de 4 Ko. Cela a pour principal avantage d'améliorer de façon conséquente les performances de la base de données sur Linux. Les avantages de cette fonctionnalité sont d'autant plus marqués que nous disposons de serveurs de grandes capacités dont la mémoire dépasse 100 Go.

Le seul point sur lequel nous devons prêter attention concerne la restriction sur le type de mémoire choisi durant l'étape de configuration de la mémoire de DBCA. En effet, comme nous l'avons explicité précédemment dans ce mémoire, HugePages ne peut pas être utilisé conjointement avec la gestion automatique de la mémoire (Automatic Memory Management ou AMM). Nous devons veiller à cocher le mode de gestion automatique de mémoire partagée (Automatic Shared Memory Management ou ASMM). Par conséquent, il a fallu peser les avantages et les inconvénients avant d'opter au final pour le mode ASMM. Deux critères ont été décisifs : le gain conséquent de performance souligné par Oracle et la grande quantité de mémoire dont nos serveurs disposaient. Nous avons pu de ce fait allouer plus de 100 Go sans inconvénients.

Pour vérifier si cette fonctionnalité est implémentée, il suffit de taper la commande suivante :

```
grep Huge /proc/meminfo
```

Le tableau suivant montre la différence de configuration entre le HugePage configuré et non configuré.

Tableau 5: Hugepage

HugePage non configurée		HugePage configurée chez Essilor	
AnonHugePages	53248 Ko	AnonHugePages	55296 Ko
HugePages_Total	0	HugePages_Total	2050
HugePages_Free	0	HugePages_Free	1551
HugePages_Rsvd	0	HugePages_Rsvd	1550
HugePages_Surp	0	HugePages_Surp	0
Hugepagesize	2048 Ko	Hugepagesize	2048

Les valeurs recommandées des propriétés du tableau sont définies dans le MOS ID 401749.1

IV.2.4 Activation de la base de données Flashback (Flashback Database)

La base de données Flashback nous permet de restaurer une base à un moment précis de son état antérieur sans utiliser le moindre media. Lorsqu'une base de données est active, Flashback Database écrit dans une zone tampon des images passées des blocks de données (Datablock) dans les fichiers logs de Flashback. Ceux-ci sont générés par défaut dans des tablespaces permanents localisés dans la zone de restauration rapide du système (Fast Recovery Area ou FRA). Les logs Flashback permettent à la base de données Flashback de gagner du temps sur la correction d'une erreur inattendue en restaurant la base originale dans un état précédent jugé plus fiable.

L'équipe DBA a donc adopté cette fonctionnalité pour lui donner plus de flexibilité lors d'erreurs critiques inattendues. En effet, l'expert DBA Oracle de notre équipe et moi-même avons déterminé qu'il est parfois plus judicieux de restaurer un état antérieur fiable plutôt que d'essayer de trouver la source de l'erreur et de la corriger. Ce type de restauration est d'autant plus efficace qu'il est rapide à mettre en œuvre.

Afin de mettre en œuvre cette fonctionnalité, il est indispensable d'activer le mode FORCE LOGGING.

IV.2.4.1 Activation du mode FORCE LOGGING

Pour finaliser l'activation de Flashback Database nous avons dû activer le mode FORCE LOGGING. Cette option permet de forcer l'écriture de redo log pour certains types de commande SQL n'en générant pas par défaut. Par exemple, les commandes de créations de table CREATE TABLE autorisent la clause NOLOGGING. Ceci a pour inconvénient majeur d'empêcher la restauration de cette table à un état antérieur.

Par conséquent, nous avons donc activé cette fonctionnalité pour permettre à la base de données Flashback de construire une image fidèle de la base Repository.

Pour activer la mode FORCE LOGGING, il suffit d'exécuter les commandes SQL suivantes :

```
SQL> shutdown immediate;  
SQL> startup mount;  
SQL> alter database FORCE LOGGING;  
SQL> alter database OPEN;
```

IV.2.5 Activation du Block Change Tracking

Lorsque l'on active cette fonctionnalité dans une base de données v11g, Oracle fait l'inventaire des chemins physiques de toutes les modifications de la base afin de créer une sauvegarde incrémentale dans le temps. De ce fait, le logiciel RMAN, qui est l'outil de gestion des sauvegardes et de restaurations des bases de données Oracle, utilise automatiquement cet inventaire pour déterminer les blocks de données qui doivent être lus pendant une sauvegarde incrémentale.

Dans un deuxième temps, RMAN accède à ces données pour les sauvegarder. Lorsque la fonctionnalité Block Change Tracking n'est pas activée, c'est l'intégralité du bloc de données qui doit être lu par RMAN. De plus, si une toute petite partie des données du bloc a été modifiée, c'est le bloc de données tout entier qui sera sauvegardé. Ceci a pour principal désavantage de grossir inutilement la taille des sauvegardes effectuées.

Nous avons donc décidé d'activer cette option qui permet d'optimiser la taille mémoire des sauvegardes effectuées.

Cette option s'active à partir d'un fichier binaire localisé dans la zone de récupération rapide du système (FRA). Ce fichier est localisé dans le même répertoire que les fichiers de la base de données.

Pour vérifier si cette fonctionnalité est activée il suffit d'exécuter la commande SQL suivante :

*SQL> Select * From V\$BLOCK_CHANGE_TRACKING;*

Voici comment procéder maintenant à l'activation :

SQL> Alter database enable BLOCK CHANGE TRACKING;

IV.2.6 Exécution du Kit de prérequis de OEM en mode indépendant

Le kit de prérequis Enterprise Manager est un logiciel qui vérifie de façon automatique si tous les prérequis nécessaires pour la base Repository ont été installés. En effet, nous devons nous assurer que tous ces prérequis sont satisfaits pour procéder à l'installation de Cloud Control. Ce kit permet également d'entreprendre certaines actions correctives quand un prérequis fait défaut.

L'installateur OUI d'OEM 12c exécute automatiquement ce kit mais nous pouvons également l'exécuter indépendamment de cet outil comme nous l'avons fait en exécutant la commande : emprereqkit

Notre expert DBA et moi-même avons pensé qu'il serait plus pratique de corriger les manquements signalés dans le rapport transmis par cette commande que de les résoudre à la volée pendant l'installation de Cloud Control.

La validation des prérequis par ce kit représente l'aboutissement des étapes de configuration de la base Repository. Il va maintenant falloir installer OEM 12c et le configurer à son tour pour bénéficier des fonctionnalités de notifications d'alertes et d'incidents.

IV.3 Installation et Configuration d'Oracle Enterprise Manager Cloud Control

Dans cette partie nous allons principalement nous intéresser aux étapes de configuration du système de supervision. Cela nous permettra notamment de bénéficier des fonctionnalités avancées de notification d'alerte et de configuration des seuils de métriques. Les étapes d'installation du logiciel et de l'agent sont consultables dans les annexes de ce mémoire. Voici donc les étapes de configuration que l'on a effectué pour OMS et OMR :

- Réactivation de l'optimisateur de récupération automatique des statistiques
- Mise en œuvre des variables d'environnement sur le serveur-hôte OMS
- Planification des purges périodiques des fichiers logs de Cloud Control
- Mise en place de la politique de sauvegarde des composants de Cloud Control

IV.3.1 Réactivation de l'optimisateur de récupération automatique des statistiques

Lors de l'étape de configuration de la base Repository, nous avions désactivé cette fonctionnalité afin de nous préparer à l'installation de Cloud Control. Une fois OEM déployé, il est important de réactiver l'optimisateur de récupération automatique des statistiques pour optimiser les plans d'exécution des commandes SQL. Pour ce faire, il suffit de procéder de la manière suivante :

```
SQL> exec DBMS_AUTO_TASK_ADMIN.ENABLE;
SQL> client_name => 'auto optimizer stats collection',
SQL> operation => NULL,
SQL> window_name=> NULL);
```

La requête suivante nous permet de vérifier le statut de cette fonctionnalité :

```
SQL> Select CLIENT_NAME, STATUS FROM DBA_AUTOTAST_CLIENT order by 1;
```

Tableau 6: Statut inactif de l'Auto Optimizer Stats Collection

CLIENT_NAME	STATUS
Auto Optimizer Stats collection	ENABLED*
Auto Space Advisor	ENABLED
SQL Tuning Advisor	ENABLED

*Activé

IV.3.2 Mise en œuvre des variables d'environnement sur le serveur-hôte OMS

Comme pour une grande majorité de logiciels informatiques, OEM Cloud Control est plus facile à administrer lorsque l'on peut définir des variables d'environnement qui viennent raccourcir et donc simplifier certaines écritures de chemins de répertoire (chemins absous). L'utilisation de ces variables d'environnement peut même s'avérer obligatoire lorsque l'on veut démarrer ou stopper un élément de Cloud Control.

Par exemple, pour stopper ou démarrer l'agent OMA, nous avons dû mettre en place les variables d'environnement suivantes :

```
export AGENT_HOME=/IDBO/oem/core/12.1.0.4.0
export ORACLE_HOME=/IDBO/oem/core/12.1.0.4.0
export PATH=$ORACLE_HOME/bin:$PATH
```

Il suffit maintenant de lancer les commandes d'arrêt ou de démarrage :

Tableau 7: Commandes d'arrêt et de démarrage de l'agent

Consignes administrateur	Commandes système	Réponses attendues du système
Démarrage de l'agent	emctl start agent	'Agent is Running and Ready '
Arrêt de l'agent	emctl stop agent	'Agent is not Running'
Statut de l'agent	emctl status agent	'Agent is Running and Ready '/ 'Agent is not Running '

IV.3.3 Planification des purges périodiques des fichiers logs de Cloud Control

Les fichiers logs générés par Cloud Control peuvent nous être utiles pour déboguer et résoudre certains problèmes d'accès à la console OEM et de transmission des données des agents. Tous les fichiers logs générés par OMS et WLS (WebLogic Server) dépassant une certaine taille génèrent, une fois arrivés à leur limite (5 Mo) de nouveaux fichiers et effacent les anciens fichiers logs de façon automatique. Cependant, toutes les anciens logs ne sont pas systématiquement effacés et requièrent une suppression manuelle de la part de l'administrateur.

Sans cette intervention, l'espace disque que nous avons alloué à OMS pourrait se saturer rapidement ce qui aurait pour conséquence d'arrêter les activités de supervision de Cloud Control comme l'envoie des alertes, la récolte des métriques et la transmission des données des agents.

Etant donné la taille modeste de notre environnement de supervision et de l'espace disque disponible sur notre serveur OMS, l'équipe DBA a planifiée une purge des anciens fichiers logs tous les trente jours.

Mise en place de la politique de sauvegarde des composants de Cloud Control

Afin de finaliser les étapes d'installation et de configuration d'OEM 12c, notre équipe a mis en place une politique de sauvegarde de Cloud Control pour se prémunir contre des défaillances matérielles, logicielles et humaines qui pourraient potentiellement nous amener à repasser par toutes les étapes d'installation et de configuration effectuées jusqu'à maintenant. Voici donc les différentes parties de notre politique de sauvegarde :

- Sauvegarde de la base Repository : La base de données OMR ainsi que son logiciel sont sauvegardés régulièrement selon les meilleures méthodes recommandées par Oracle dont voici le résumé :
 - Sauvegarde des répertoires Oracle homes et de l'Oracle Inventory dans la zone de sauvegarde du système d'exploitation du serveur.
 - Sauvegarde de la base de données hébergeant la base Repository avec le logiciel RMAN via la console Cloud Control ou via des scripts de lignes de commandes.
- Planification de sauvegardes régulières d'OMS :
 - Sauvegarde des répertoires Oracle homes et de l'Oracle Inventory dans la zone de sauvegarde du système d'exploitation du serveur.
 - Capture de la configuration d'OMS via l'utilisation des fonctionnalités emctl suivantes :
`Emctl exportconfig oms -dir <backup_dir> -sysman_pwd <pwd>`

Ainsi, en sauvegardant à la fois les données (datafile) et le logiciel de la base Repository, il est aisément de recréer une image fidèle de la base après la survenance d'un désastre.

IV.4 Configuration de la console Cloud Control

Une fois finalisée l'installation et la configuration d'OEM 12c, il nous faut mettre en œuvre les méthodes de supervision destinées à surveiller l'activité de notre environnement de production.

Les étapes de configuration de Cloud Control s'effectuent via sa console. Nous y accédons depuis un navigateur internet avec une URL indiquée par OEM lors de son installation. Ces étapes ont pour objectif d'activer les fonctionnalités de notification d'incidents survenus sur les bases de données supervisées.

IV.4.1 Mise en place des méthodes de notification

Les méthodes de notification représentent les mécanismes permettant de nous contacter lorsque certains évènements ont lieu. Par exemple, l'apparition d'alertes de métriques ou le changement de l'état d'une base sont des évènements qui doivent nous être notifiés en permanence afin de nous permettre d'administrer correctement nos bases de données. Nous avons fait le choix de notifications sous forme de mails destinés à la messagerie commune de notre équipe en France et à celle de Thaïlande qui travaille en collaboration avec nous en horaire décalé. Il existe d'autres moyens de notification (procédures PL/SQL ou scripts OS etc.) mais pour des raisons de simplicité et de maintenabilité nous avons décidé d'adopter ce moyen de communication.

Pour recevoir des notifications au sujet de certains évènements, l'administrateur doit en premier souscrire à des règles de notifications que nous expliquerons plus en détail dans la suite de ce mémoire. Dans ces règles, il est possible entre autres de définir les destinataires des notifications mais aussi la nature des évènements dont nous souhaitons nous tenir au courant. Pour ce faire, l'administrateur doit avoir configuré au préalable une méthode de notification.

a. Serveur Mail

Le mail reste la méthode de notification principale que nous utilisons chez Essilor, qu'il s'agisse de superviser des environnements de production ou de non-production. Pour mettre en place ce système, il faut qu'un super administrateur (notre expert DBA) définisse au moins un serveur mail à travers lequel Cloud Control puisse envoyer des notifications aux différents administrateurs. Le champ du serveur mail sortant (SMTP) sur la page présentée ci-dessous contiendra déjà une entrée si l'on a spécifié un serveur SMTP lors de l'installation de Cloud Control.

Pour que nous puissions fournir une haute disponibilité concernant la transmission de notifications il nous est possible de spécifier des serveurs mails additionnels.

Une fois que tous les champs sont spécifiés, il ne reste plus qu'à tester la configuration.

b. Spécification des adresses mails pour les utilisateurs

Maintenant que nous avons configuré le serveur mail sortant nous devons définir les adresses mails des administrateurs chargés de la maintenance des bases supervisées. L'image ci-dessous montre la section de la console utilisateur où l'on peut renseigner ces adresses.

The screenshot shows the Oracle Enterprise Manager interface for Cloud Control 12c. The main title bar reads "ORACLE Enterprise Manager Cloud Control 12c". The top navigation bar includes links for "Enterprise", "Targets", "Favorites", "History", "Setup", "SYSMAN", and search fields for "Search Target Name". The main content area is titled "Enterprise Manager Password & Email". Under this, there's a "Password" section with a note about changing the SYSMAN user password. Below it is the "E-mail Addresses" section, which contains a table with columns for "Select All", "Select None", "E-mail Address", and "Email Type (Message Format)". There are 7 rows in the table, each with a checked checkbox in the first column and an "Email (Long)" dropdown in the fourth column. At the bottom left of this section is a "TIP" note with a link to online help for message format samples. At the bottom right of the main content area are "Revert" and "Apply" buttons.

Pour finaliser cette étape, nous devons utiliser la fonctionnalité de test proposée par le produit pour s'assurer de l'intégrité des adresses renseignées.

c. Configuration de l'emploi du temps des notifications

A travers cette fonctionnalité, il nous est possible de définir pour chaque administrateur de notre équipe les adresses et les horaires pendant lesquelles ils recevront les notifications de Cloud Control. L'emploi du temps est configurable. Nous pouvons par exemple renseigner une adresse de notification différente pour chaque heure. En ce qui concerne notre équipe, nous avons laissé les notifications activées à toutes les heures durant toute la semaine, weekend compris pour l'adresse mail de l'expert DBA Oracle de notre équipe. En effet, celui-ci dirige les opérations de maintenance en France et en Thaïlande et de ce fait, il doit rester notifié en permanence.

L'emploi du temps proposé par Cloud Control autorise des rotations allant d'une à huit heures. Cela est d'autant plus pratique que beaucoup de professionnels de l'informatique travaillent sur une rotation de sept jours composée de cinq jours ouvrés et de deux jours de repos.

Voici la marche à suivre pour mener à bien cette étape :

1. Définir des horaires et de la rotation effectuée sur l'emploi du temps.
2. Renseigner la fréquence de rotation désirée
3. Modifier ou remplacer l'emploi du temps existant
4. Définir la date de début de l'emploi du temps à Lundi.
5. Choisir le fuseau horaire dans lequel l'administrateur se situe

Notification Schedule > Edit Schedule Definition: Time Period

Edit Schedule Definition: Time Period

Your notification schedule is a rotating schedule that repeats based on the frequency you specify. It will take effect immediately or can be deferred to a later start date. No notifications will be sent prior to the start date.

* Rotation Frequency: 1 Week

(*) Edit Existing Schedule

(*) Replace Existing Schedule

Start Date: Feb 5, 2016

Example: Oct 31, 2008

TIP: Your current schedule will be deleted. No e-mail notifications will be sent to you prior to the start date specified.

* Time Zone: (UTC+01:00) Oslo (CET)

Notification Schedule

A notification schedule is a rotating schedule used by Enterprise Manager to determine how to send e-mail notifications to administrators. Each administrator has exactly one notification schedule. When an alert needs to be e-mailed to an administrator, Enterprise Manager consults that administrator's notification schedule to determine the e-mail address to be used. In a notification schedule, an administrator can specify different e-mail addresses based on day of the week and time of the day. When sending e-mail notifications, Enterprise Manager will use the e-mail addresses appropriate for that day and time. Time periods that are left empty signify periods where no e-mail notifications should be sent. A notification schedule repeats every interval specified in the notification schedule definition.

Cancel Continue

Notification Schedule

You need to set up your notification schedule in order to receive e-mail notifications for alerts. For each day in the schedule, specify the e-mail addresses that should be used to send you e-mail notifications.

Administrator: SYSMAN

Rotation Frequency: 1 Week

Current Week

Time Zone: (UTC+01:00)

	May 23, 2016 Monday	May 24, 2016 Tuesday	May 25, 2016 Wednesday	May 26, 2016 Thursday	May 27, 2016 Friday	May 28, 2016 Saturday	May 29, 2016 Sunday
12:00 am - 1:00 am	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...
1:00 am - 2:00 am	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...
2:00 am - 3:00 am	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...
3:00 am - 4:00 am	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...
4:00 am - 5:00 am	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...
5:00 am - 6:00 am	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...
6:00 am - 7:00 am	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...
7:00 am - 8:00 am	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...
8:00 am - 9:00 am	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...
9:00 am - 10:00 am	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...
10:00 am - 11:00 am	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...
11:00 am - 12:00 pm	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...
12:00 pm - 1:00 pm	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...
1:00 pm - 2:00 pm	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...
2:00 pm - 3:00 pm	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...
3:00 pm - 4:00 pm	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...
4:00 pm - 5:00 pm	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...
5:00 pm - 6:00 pm	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...
6:00 pm - 7:00 pm	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...
7:00 pm - 8:00 pm	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...
8:00 pm - 9:00 pm	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...
9:00 pm - 10:00 pm	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...
10:00 pm - 11:00 pm	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...
11:00 pm - 12:00 am	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...	bouyou@rest...

Idle

Administrator: SYSMAN

Rotation Frequency: 1 Week

Current Week

Time Zone: (UTC+01:00)

View Week Containing: May 24, 2016

Example: Oct 31, 2008

Edit Schedule Definition

May 23, 2016 Monday

May 24, 2016 Tuesday

May 25, 2016 Wednesday

May 26, 2016 Thursday

May 27, 2016 Friday

May 28, 2016 Saturday

May 29, 2016 Sunday

Idle

Administrator: SYSMAN

Rotation Frequency: 1 Week

Current Week

Time Zone: (UTC+01:00)

View Week Containing: May 24, 2016

Example: Oct 31, 2008

Edit Schedule Definition

d. Sécurité de Cloud Control

La sécurité est une partie importante de l'administration d'Oracle Enterprise Manager. Celle-ci s'est beaucoup renforcée dans la version 12c vis-à-vis des versions 10g et 11g via l'apparition d'identifiants partagés.

Cette nouvelle fonctionnalité permet à certains priviléges dont nous disposons d'être attribués à plusieurs autres administrateurs (situés en Thaïlande). De ce fait, cela réduit considérablement le nombre de personnes se partageant les mêmes mots de passe. S'agissant ici d'une amélioration de sécurité substantielle, j'ai été chargé d'étudier ce sujet afin d'en expliquer les avantages à l'expert DBA oracle de notre équipe dans l'optique d'une future implémentation de cette fonctionnalité.

Nous nous intéresserons également aux améliorations concernant les commandes Sudo et PowerBroker.

IV.5 Conclusion

L'étape de configuration de Cloud Control nous a permis d'implémenter des fonctionnalités essentielles à la supervision de nos bases de données. En effet, les fonctionnalités de notification d'alertes et d'incidents sont celles que notre équipe utilise principalement pour surveiller l'activité de nos bases de production dans la version 10g d'OEM. Cependant, afin d'être notifier des évènements survenus sur nos bases de données supervisées, il est nécessaire que :

- La base Repository fonctionne correctement
- L'agent présent sur le serveur et les agents présents sur les serveurs-cibles fonctionnement également
- Le service OEM soit activé

Ne disposant pas de dispositifs de redondance, nous ne pouvons pas assurer en cas de sinistre la continuité de la supervision de nos bases de données. De ce fait, si un incident critique à lieu pendant la maintenance d'OMR ou d'OMS, nous ne serions pas notifiés de cet évènement. En revanche, nous disposons des sauvegardes nécessaires pour récupérer l'intégralité de notre base Repository si celle-ci venait à tomber en erreur.

V Après Projet

Maintenant que nous avons déployé et configuré OEM 12c, nous allons expliciter dans cette partie comment fonctionne l'administration d'OEM. Cette première étape est nécessaire pour comprendre par la suite les améliorations qui ont été apportées dans Cloud Control. Dans un second temps, nous donnerons les explications nécessaires à l'exploitation des nouvelles fonctionnalités d'administration de Cloud Control afin que les équipes de Thaïlande puissent en tirer parti.

V.1 Conduite du changement

Dans cette partie nous allons analyser les principales améliorations d'administration qui ont été apportées dans la version Cloud Control puis brièvement expliquer comment les exploiter.

Avant de commencer la phase d'analyse nous allons mettre en évidence les différents acteurs de l'administration d'Oracle Enterprise Manager afin de mieux comprendre le fonctionnement de l'outil dans sa globalité.

V.1.1 Détails et explications de l'administration de Cloud Control

Chaque utilisateur de Cloud Control est appelé administrateur. Il existe trois types d'utilisateur OEM : l'administrateur, le super administrateur et le propriétaire de la base Repository. Le compte SYSMAN est l'unique propriétaire de cette base de données. Le super administrateur a quant à lui tous les priviléges dont dispose un administrateur standard mais il dispose également de ceux permettant de gérer tous les administrateurs au sein de l'environnement Cloud Control.

Comme le recommande Oracle, chaque utilisateur de CC dispose au sein de notre équipe de son propre compte, composé d'un identifiant et d'un mot de passe qui lui appartient. Il existe trois types de rôles disponibles pour un administrateur : le concepteur et l'opérateur et le super administrateur :

- **Le Super Administrateur** : Un compte Super Administrateur est semblable à un compte administrateur standard, néanmoins celui-ci dispose de la capacité de gestion des comptes administrateurs de Cloud Control. Celui-ci dispose d'un accès total à toutes les cibles monitorées par OEM. De plus, le super administrateur dispose des droits de création et de modification de comptes administrateurs.
- **Le concepteur** : Un concepteur est un administrateur disposant des autorisations lui permettant de créer des modèles de procédures de déploiement, des plans et des modèles de correctifs.
- **L'opérateur** : un opérateur est un administrateur qui dispose de droits réduits sur les procédures de déploiement et les bibliothèques logiciels. Un opérateur déploie et utilise les procédures, les patchs et les modèles de correctifs. Il n'est pas censé modifier ni même créer ces procédures.

- **Le propriétaire de la base Repository :** Le propriétaire de la base Repository appartient à la classe des Supers Administrateurs et possède des droits additionnels lui permettant de gérer et de maintenir cette base. Par défaut, le compte SYSMAN est le propriétaire de cette base et son utilisation est réservée à des opérations de mise à jour ou de maintenance de la base Repository.

Au sein de notre équipe, nous disposons tous de comptes administrateurs nominatifs. L'expert DBA Oracle dispose quant à lui du compte Super Administrateur car il est le responsable des opérations en France.

V.1.2 Analyse des améliorations d'administration

Les accréditations

Les accréditations (credentials) sont au cœur de la sécurité d'OEM Cloud Control. Lorsque nous nous connectons à l'interface de l'outil, nous n'avons d'abord accès qu'à une vue basique des informations de supervision récoltées par les agents. Pour accéder à une vision complète de ces informations il est nécessaire que nous nous identifions à la base de données via une accréditation définie pour chaque compte utilisateur. Cela permet à nos développeurs de bases de données, à nos gestionnaires et à notre équipe administrateurs de se connecter à la base en utilisant nos accréditations respectives. C'est une mesure essentielle pour sécuriser et auditer OEM.

Les accréditations sont maintenant gérées de façon nominative. Plus précisément, celles-ci sont sauvegardées sous forme de noms ce qui facilite grandement leur gestion mais aussi leur partage. Les noms des accréditations sont sauvegardés et peuvent être utilisés pour se connecter sur des cibles supervisées. De plus, des accréditations préférentielles peuvent être utilisés pour un certain nombre de connexion par défaut et peuvent être sauvegardées dans la base Repository.

La nouvelle fonctionnalité de partage des accréditations présente plusieurs avantages :

- **Réduction du partage des mots de passe :** Notre expert DBA Oracle est maintenant la seul personne ayant besoin de connaître le mot de passe du compte system pour une base de données. Les informations de connexion sont cachées mais peuvent être partagées entre plusieurs autres administrateurs.
- **Mise en place de permission de groupe :** Il nous est possible de donner accès à une base de données à certains groupes d'utilisateurs uniquement. Par exemple, nous pouvons décider que tous les administrateurs concepteurs aient accès en lecture seulement à une base de données qui initialement leur était interdite.

Il s'agit ici d'une fonctionnalité qui nous a été particulièrement utile lors de la configuration des seuils d'alertes des métriques et des règles d'incidents. En effet, mon compte administrateur standard a pu hériter de certains droits du compte Super Administrateur de l'expert DBA de notre équipe. De ce fait, cela m'a permis de configurer avec son accord et ses préconisations un certain nombre de ces dispositifs.

Accréditations nominatives

Les accréditations nominatives (Named credentials ou NC) sont sauvegardées et associées à chaque administrateur dans la base Repository. Celles-ci peuvent contrôler selon leur nature les accès à une base de données, un serveur-hôte ou bien une application. Au cœur de l'accréditation sont définis un identifiant et un mot de passe qui sont associés au type de cible visé. Une accréditation nominative peut être utilisée sur une ou plusieurs cibles si les identifiants et les mots sont les mêmes pour chacune d'entre elles. Les NC peuvent être gérées dans OEM Cloud Control via la fenêtre « Security Named Credentials ». Nous pouvons y supprimer ou modifier les accréditations existantes ou encore en créer de nouvelles.

La création d'accréditation varie légèrement en fonction de l'authentification exigée par le type de cible sélectionné dans le « Target Type ».

Ce champ détermine également les propriétés qui seront disponibles dans la partie « propriété de l'accréditation »

The screenshot shows the Oracle Enterprise Manager Cloud Control 12c interface. The main title bar reads "ORACLE Enterprise Manager Cloud Control 12c". The top navigation bar includes "Enterprise", "Targets", "Favorites", and "History". The current page is "Security", with a timestamp "Page Refreshed May 25, 2016 12:53:06 AM CEST". The main content area is titled "Create Credential" under "Named Credentials > Create Credential". The form is divided into three sections: "General Properties", "Credential Properties", and "Access Control".

- General Properties:** Contains fields for "Credential name" (mandatory), "Credential description", "Authenticating Target Type" (set to "Host"), "Credential type" (set to "Host Credentials"), "Scope" (set to "Target"), "Target type" (set to "Host"), and "Target Name".
- Credential Properties:** Contains fields for "UserName" (mandatory), "Password" (mandatory), "Confirm Password", and "Run Privilege" (set to "None").
- Access Control:** A table with columns "Grantee", "Grantee Type", and "Privileges". It includes buttons for "Add Grant", "Change Privilege(s)", and "Revoke Grant". A note at the top says: "Click on 'Add Grant' to add users. Click on 'Remove Grant' to remove grants to users. Click on 'Change Privilege' to edit privilege for user(s).". The table currently shows "No access policy" and "Add a new grantee with default privilege".

Accréditations automatiques

Les accréditations automatiques sont stockées et assignées en général à des cibles spécifiques. Néanmoins, nous pouvons mettre en place ces accréditations pour des cibles ou des types de cibles plus générales via l'outil d'accréditation automatique « Preferred Credential ». Si ces types d'accréditations ne sont pas définies, nous sommes contraints d'entrer manuellement la bonne accréditation à chaque fois que nous désirons avoir accès à toutes les informations de la cible dont nous souhaitons nous renseigner (l'accès aux informations basiques n'exigent pas d'accréditations particulières).

Chez Essilor, la mise en place de ces accréditations est peu envisageable car chaque serveur-hôte, chaque base de données et chaque application requiert différents identifiants et mots de passe. Il faudrait par conséquent créer autant d'accréditations qu'il existe de cibles différentes. C'est la raison pour laquelle nous n'envisageons pas pour le moment de mettre en place un tel système.

Accréditations de supervision

Les accréditations de supervision sont utilisées par les agents OMA pour superviser des cibles spécifiques dans l'environnement OEM Cloud Control. Celles-ci peuvent être mis en œuvre par un Super Administrateur et fonctionner pour tous les agents si les identifiants de connexion sur les serveur-hôtes sont les mêmes. De manière générale, nous attribuons une accréditation spécifique pour chaque serveur sur lequel un agent est installé. L'accréditation est renseignée une seule fois lors de la phase de déploiement de l'agent sur le serveur-hôte.

Ces accréditations sont essentielles pour le bon fonctionnement de Cloud Control et sont faciles à maintenir. Il est indispensable que nous changeons les mots de passe des accréditations renseignées dans OEM lorsque nous changeons les mots de passe système (ou de base de données).

Cette remarque est d'autant plus importante que notre équipe met en application sa politique de changement de mots de passe pour renforcer la sécurité de ses systèmes.

Délégation de droits

La délégation de droits ou de priviléges permet aux utilisateurs système d'un serveur-cible d'obtenir un niveau de privilège supérieur via les commandes Sudo ou PowerBroker. Ces droits sont utilisés durant le processus de configuration de l'agent et dépendent de sa méthode d'installation. Toutefois, si l'on souhaite utiliser la fonctionnalité de délégation de priviléges après l'étape d'installation de l'agent, il est nécessaire de configurer cette délégation dans la section de gestion de délégation des priviléges.

Select	Details	Host	Status	Type	Agent	Agent Version	Operating System	Edit
<input type="checkbox"/>	> Show	dadvmn0630.us.oracle.com	(i)	None	dadvmn0630.us.oracle.com:11852	12.1.0.1.0	Linux	

Figure 11: Fenêtre d'audit de control OEM 12c

Cas pratique :

Prenons le cas d'un administrateur opérateur d'OEM voulant stopper ou démarrer un agent sur un serveur. Ce dernier ne dispose pas nécessairement des priviléges suffisant pour effectuer ces types d'opérations. En revanche, il est très probable que le Super Administrateur d'OEM dispose des priviléges suffisant sur ce même serveur. Grâce à l'outil de délégation des priviléges, l'administrateur opérateur pourra donc demander au Super administrateur de configurer cette fonctionnalité afin qu'il puisse hériter des droits dont il manque.

Dans notre équipe, tous nos membres possèdent des comptes utilisateurs disposant des droits suffisants à effectuer des opérations de maintenance sur les agents OMA. Cette fonctionnalité ne nous est donc pas nécessaire pour le moment.

Audit avec Cloud Control

La fonctionnalité d'audit de Cloud Control est destinée à surveiller son utilisation. Les informations de connexion et de déconnexion sont enregistrées et nous pouvons les consulter depuis la section « Audit Data » de Cloud Control. Afin que cette surveillance soit efficace, chacun des DBA Oracle doit se connecter avec son propre compte. En effet, dans le cas contraire, si tous les administrateurs s'identifient à la console OEM avec le compte super administrateur SYSMAN, il est impossible de connaître les réels utilisateurs de l'outil.

Chez Essilor, l'accès à OEM 12c reste très restreint car il n'existe que trois personnes qui ont accès à la console utilisateur :

Un expert DBA Oracle qui possède le compte Super Administrateur.

Un administrateur senior Oracle qui dispose d'un compte administrateur.

Moi-même qui dispose du compte utilisateur SYSMAN.

Grâce à cette fonctionnalité, il nous est très aisément de contrôler l'accès à OEM. Voici un exemple de ce que peut afficher cette fonctionnalité.

The screenshot shows the Oracle Enterprise Manager Cloud Control 12c interface. The top navigation bar includes links for Enterprise, Targets, Favorites, History, Setup, Help, and Log Out. The current user is identified as SYSMAN. The main content area is titled 'Audit Data' under the 'Security' category. A 'Simple Search' panel on the left allows filtering by Start Date (Sep 2, 2011), End Date (Sep 2, 2011), Operation (All), Administrator (SYSMAN), and Status (All). The search results table has columns for Timestamp, Administrator, Operation, Status, and Message. The table shows five entries related to SYSMAN's browser activity on Sep 2, 2011. At the bottom of the page, there are two tips: one about using wild card characters and another about case-insensitive searches.

Timestamp	Administrator	Operation	Status	Message
Sep 2, 2011 4:06:30 PM	SYSMAN (Browser)	EM Login	Success	SYSMAN Logged on successfully
Sep 2, 2011 1:01:03 PM	SYSMAN (Browser)	EM Logout	Success	SYSMAN Logged out successfully, session timed out
Sep 2, 2011 1:01:03 PM	SYSMAN (Browser)	EM Logout	Success	SYSMAN Logged out successfully, session timed out
Sep 2, 2011 1:00:11 PM	SYSMAN (Browser)	EM Login	Success	SYSMAN Logged on successfully
Sep 2, 2011 1:00:11 PM	SYSMAN (Browser)	EM Login	Success	SYSMAN Logged on successfully

TIP You can optionally use "_" and "%" wild card characters in search criteria and "\\" escape character to escape wild card characters
 TIP Searches are case-insensitive

Il s'agit ici d'un cas très simple n'affichant que les informations de connexion et de déconnexion d'une seule après-midi mais il est possible d'agrandir l'intervalle de temps à plusieurs années en configurant les champs adéquats (ici *Start Date* et *End Date*).

Sécurisation des transferts de données de Cloud Control

OEM Cloud Control dispose d'une multitude de fonctionnalités lui permettant d'assurer sa sécurité au niveau de son application et au niveau des éléments avec lesquels elle interagit. Celles-ci sont accessibles via la console de l'outil ou via des lignes de commandes (emctl sous OMS_HOME). Les éléments sous-jacents tels que la base de données Oracle 11g et OMS/Oracle HTTP Server possèdent leurs propres fonctionnalités de sécurité intégrées que Cloud Control coopte pour se protéger.

Tableau 8: Objectifs et méthodes déployées pour sécuriser OEM Cloud Control

Objectifs de sécurité de Cloud Control	Méthode choisie pour atteindre l'objectif
Protéger les données sensibles (mots de passe etc.)	Sécuriser la clé emkey
Fournir la possibilité d'auditer pour les sites qui en ont le besoin	Activer la fonctionnalité d'audit de Cloud Control
Refuser les utilisateurs non-autorisés à accéder à la console OEM ; donner les droits d'accès au personnel autorisé	Renforcer les droits d'accès des administrateurs
Adoption des standards de sécurité des entreprises pour sécuriser les éléments de CC et les serveurs-hôtes	Mettre en place des politiques de sécurité pour les éléments de CC et les serveurs-hôtes
Sécuriser le transfert des données entre les agents et le serveur OMS	Activer le Framework de sécurité « EM Framework Security »
Crypter les transmissions des données de la base Repository	Utiliser la fonctionnalité avancée de sécurité d'Oracle : « Oracle Advanced Security »
Sécuriser les données transférées entre le navigateur internet et la console OEM et restreindre le nombre d'utilisateur de la console	Renforcer la sécurité du serveur HTTP d'Oracle
Intégrer CC avec d'autres technologies Oracle permettant d'identifier les utilisateurs	Intégrer CC au sein d'EUS
Déployer CC lorsque les pare-feu sont mis en place	Configurer les propriétés dans le fichier de configuration de CC, renforcer la sécurité des serveurs proxy et configurer les pare-feu.

Le tableau ci-dessus fait la liste des objectifs de sécurité à atteindre et de la méthode à adopter les satisfaire. Ce bref récapitulatif a été utile pour évaluer et mettre en place un certain nombre de dispositifs de sécurité lors du déploiement de Cloud Control.

Les lignes en bleu montrent les objectifs atteints à ce jour par notre équipe DBA.

Les lignes en orange désignent les objectifs en cours de réalisation.

Les lignes en noir sont les objectifs qui restent à mettre en œuvre.

V.2 Maintenance opérationnelle

Il existe deux types de maintenance de Cloud Control : la maintenance opérationnelle et la maintenance physique du logiciel. La maintenance opérationnelle renvoie aux fonctionnalités que notre équipe doit implémenter pour automatiser les tâches de détection des problèmes et de notification des évènements qui se sont produits. Les environnements informatiques que nous avons la charge de maintenir sont composés de plusieurs centaines de cibles nécessitant une supervision constante. Nous ne pourrions donc pas gérer de tels environnements sans des logiciels de supervision comme OEM. En effet, le cœur de la maintenance opérationnelle de Cloud Control concerne à la fois la configuration des alarmes via les métriques de supervision et la configuration des règles d'incidents.

Après avoir défini brièvement les notions d'alarmes, d'alertes et de métriques dans OEM, nous expliquerons les raisons qui nous ont amenés à mettre en place des seuils d'alertes spécifiques à certaines cibles supervisées.

Nous expliquerons par la suite les règles d'incidents que nous avons créées pour superviser nos bases de données de production.

V.2.1 Alarmes, alertes et métriques de supervisions

Une alarme est un élément de configuration décrivant le changement d'état d'un système. Typiquement il met en évidence un changement indésirable à travers la fluctuation de points de données dans une série de données. Les alarmes sont composées de métriques de supervision, de mesures de dates et de temps et peuvent potentiellement déclencher d'autres alarmes.

Une alerte est une notification d'un problème potentiel, celui-ci peut prendre différentes formes : un e-mail, un SMS, un appel téléphonique. Une alerte est transmise par une alarme lorsque le système détecte, par l'intermédiaire du superviseur, qu'un de ses seuils d'alerte a été atteint. Par exemple, on peut configurer une alarme pour vous alerter quand le système dépasse 80 % d'utilisation CPU sur une période continue de 10 minutes.

Une métrique de supervision est attachée à une série de données et évalue cette dernière pour s'assurer qu'aucun seuil n'a été franchi. Le seuil est constitué de limites (exprimées sous la forme de nombre de points donné) et de la durée pour laquelle ce même seuil a été franchi. Lorsque les points de données sortent du cadre défini du seuil d'alerte, le seuil est dit atteint ou franchi et le superviseur passe de l'état normal (« Clear ») à l'état alerte (« Alert »). De la même manière,

lorsque les points de données reviennent dans le cadre les limites définies par le seuil d'alerte, le superviseur revient à l'état normal. Les états du superviseur sont utilisés comme des indicateurs clés lorsque l'on veut apprécier les états des alarmes.

Parmi toutes les métriques disponibles dans l'onglet de configuration des seuils d'alertes, nous avons décidé de mettre l'accent sur un type de métrique en particulier :

Tablespace Space Used (%) : L'espace alloué à un tablespace est égale à la somme des espaces mémoires occupés par ses fichiers de données. Cette métrique calcule l'espace utilisé pour chaque tablespace existant.

Les tablespaces font l'objet d'une attention particulière au sein de notre équipe car nous voulons surveiller leur agrandissement. Plus précisément nous voulons connaître comment évoluent les fichiers de données (Datafile) situés dans chaque tablespace. De cette façon nous pouvons connaître comment évoluent nos bases de données et détecter des activités anormales sur celles-ci. De plus, surveiller l'accroissement des tablespaces nous permet de mieux anticiper les problèmes éventuels de stockage matériel.

Nous avons décidé de mettre en place la configuration suivante pour tous nos tablespaces (Voir ligne « All others ») :

Metric	Comparison Operator	Warning Threshold	Critical Threshold
▽ Tablespace Full			
▽ Tablespace Space Used (%)			
APPS_TS_MEDIA	>=	85	90
APPS_TS_TX_DATA	>=	94	97
APPS_TS_TX_IDX	>=	94	97
All others	>=	85	90

Nous avons modifié les seuils par défaut du champ « All others » qui était initialement à 94-97. Nous avons descendu les seuils d'alertes « Warning » et « Critical » à 85-90 pour donner plus de flexibilité à nos équipes. Nous voulons dans la mesure du possible éviter d'entreprendre des modifications dans des situations de stress.

Deux tablespaces font l'objet d'une attention particulière :

- APPS_TS_MEDIA : Ce tablespace stocke tous les documents liés à l'ERP Oracle Application
- APPS_TS_TX_IDX : Ce tablespace stocke les indexes de la base de données.

Ce sont des tablespaces qui évoluent très lentement dans le temps, nous avons donc gardé la configuration initiale d'OEM uniquement pour ces deux tablespaces.

V.2.2 Configuration des règles d'incidents dans OEM 12c

Pour profiter des notifications d'alertes et d'incidents, il nous a fallu créer des règles d'incidents.

Pour ce faire, nous avons copié et modifié le premier ensemble de règles que propose par défaut Cloud Control (voir Tableau 10).

Tableau 10: Règles d'incident OEM

Incident management rule set for all targets 	Rule set to create and manage incidents for all targets
Create incident for critical metric alerts	Rule to create incidents for critical metric alert events.
Clear metric alert events older than 7 days	Rule to clear metric alert events older than 7 days.
Create incident for compliance score violations	Rule to create incidents for compliance score violation events.
Clear job status change events older than 7 days	Rule to clear job status change events corresponding to terminal job status which are older than 7 days.
Create incident for target monitoring disruption	Rule to create incidents for critical target monitoring disruption.
Create incident for critical Service Level Agreement alerts	Rule to create incidents for critical service level agreement alert events.
Incident creation rule for down and agent unreachable	Rule to create target availability incidents when a agent or host goes into down or agent unreachable state.
Incident creation rule for a Target Down availability state	Rule to create incident when a target goes down.
Incident creation Rule for target error	Rule to create target availability error incidents for all targets.
Rule to create incident after 2 minutes for down and agent unreachable	Rule to create target availability incidents when the Agent or host stays unreachable for more than 2 minutes.
Clear adp alerts after 7 days without incidents	Rule to clear up ADP events older than 7 days
Create incidents for critical or fatal business application alerts	Rule to create incidents for critical or fatal business application alerts from RUEI.

Ces règles permettent d'automatiser les fonctions comme la notification d'évènements, la création d'incidents et la purge d'évènements selon des scénarios que nous pouvons configurer.

Parmi cet ensemble de règles, nous nous intéresserons en particulier à règle de création d'incident pour les alertes critiques des métriques (« Create incident for critical metric alerts »). Nous avons en effet effectué un certain nombre de modifications sur cette règle pour l'adapter aux besoins d'Essilor :

Répétition des notifications d'alertes : A cause de certains impératifs de production, nous ne pouvons pas toujours traiter immédiatement les alertes émises par OEM. Afin de s'assurer que toutes les alertes sont résolues au jour le jour, nous avons instauré en guise de rappel une répétition des alertes existantes sur nos bases de données toutes les huit heures. Cette fréquence de rappel permet à nos équipes en Thaïlande qui travaillent à des horaires décalés par rapport à nous d'intervenir également sur les alertes qui n'ont pas pu être traitées à temps pendant nos horaires de travail.

Notification des alertes : Nous avons configuré la règle de création d'incident afin de ne recevoir uniquement les alertes d'avertissement (Warning), les alertes critiques (Critical) et les purges (Clear). De plus, nous avons différencié les destinataires de ces alertes en fonction de leur priorité. Plus précisément, les alertes d'avertissement et les purges sont uniquement envoyés aux équipes support (TMA, Analystes) et les alertes critiques sont envoyés aux équipes DBA de France et de Thaïlande ainsi qu'au centre d'assistance Essilor (Helpdesk). Cela nous permet de prioriser la résolution des alertes et des incidents survenus et de répartir selon les différents niveaux de compétences la charge de travail.

VI Conclusion

Nous avons exposé dans ce mémoire les méthodes d'implémentation et d'exploitation de la solution Cloud Control pour satisfaire nos besoins en termes de supervision de nos bases de données de production.

Il en résulte une réflexion et une méthodologie clairement définies pour identifier nos besoins d'architecture OEM, satisfaire les prérequis, installer les composants de l'outil mais aussi identifier et mettre en œuvre nos impératifs de supervision.

En effet, nous avons dans un premier temps étudié les différentes possibilités d'architecture des composants de Cloud Control ce qui a permis à notre équipe de définir l'infrastructure interne du logiciel la plus adaptée au contexte Essilor.

Nous avons ensuite mené une analyse approfondie vis-à-vis de la configuration de la base Repository et des nouvelles fonctionnalités proposées dans la version 12c afin d'améliorer la fiabilité de nos bases et de faciliter les opérations de maintenance de nos bases de données.

Enfin, nous avons mis en évidence les impératifs de supervision auxquels notre équipe doit répondre en termes de méthode de notification et de configuration des seuils d'alertes et des règles d'incidents. Ce travail nous a permis de reproduire et d'améliorer les méthodes de supervision existantes dans la version Cloud Control.

Le travail réalisé dans la phase de conduite de changement a permis aux équipes de Thaïlande de comprendre le fonctionnement du nouvel outil et de leur transmettre les connaissances nécessaires afin qu'ils puissent pleinement exploiter les principales fonctionnalités du produit.

Cette mission a donc permis de remplacer la version existante d'Oracle Enterprise Manager Grid Control par la version Cloud Control tout en assurant la continuité de la supervision de nos bases de données. De plus, l'implémentation et l'exploitation de ce nouvel outil nous a permis d'automatiser certaines routines manuelles de surveillance autrefois opérées par les membres de notre équipe. Nous pouvons donc conclure que le changement de version d'OEM s'est traduit par une amélioration substantielle de la qualité de maintenance de nos bases de supervision.

Toutefois, nous devrons continuer de maintenir nos logiciels de supervision additionnels Patrol v3.5 et Patrol 7.6 car Cloud Control ne permet pas de maintenir nos bases de données Oracle v7 et v8. Par conséquent, nos bases de données ne bénéficient pas toutes des mêmes niveaux de fonctionnalités et de supervision. Pour remédier à ce problème, nous mettrons à jour ces bases de données dans le cadre d'un futur projet.

Glossaire

- accréditations automatiques, 72
- accréditations de supervision, 73
- accréditations nominatives, 72
- Administrateur de base de données, 12
- Agent autonome, 23
- agent de supervision, 35
- Agent préinstallé, 23
- audit, 74
- base de données dépôt, 38
- concepteur, 70
- Conservatoire National des Arts et Métiers, 4
- Console Client, 23
- Contrat de Niveau de Service, 43
- découverte des cibles, 36
- délégation de droits, 73
- EM template, 54
- Essilor International, 12
- GCDomain, 37
- JDBC, 37
- jobs, 36
- Les accréditations, 71
- Listeners, 35
- niveaux de service applicatif, 39
- opérateur, 70
- Oracle Enterprise Manager Cloud Control 12c, 20
- Oracle Restart database, 46
- Oracle WebLogic Server, 37
- plug-ins, 35
- PowerBroker, 73
- processus parallélisé, 35
- schéma utilisateur, 38
- Standalone Database, 46
- Sudo, 73
- Super Administrateur, 70
- SYSMAN, 71
- World Wide Supply Chain, 17

Références Bibliographiques

- Site Internet d'Oracle (Anglais uniquement) :
http://docs.oracle.com/cd/E24628_01/index.htm
Consulté de Décembre 2015 à fin Janvier 2016
- Monitoring & Alerting de Stawek Ligus
Publié par O'Reilly Media
ISBN 10:1-4493-3347-8
- Oracle 10g Administration by Razvan Bizoi
Publié par :Tsoft, Groupe Eyrolles, 2006,
ISBN : 2-212-12055-9
ISBN 13 : 978-2-212-12055-4
- Oracle Essentials for Oracle Database 12c
Publié par : O'REILLY
ISBN-13 : 978-1449343033
ISBN-10 : 1449343031
- Oracle Enterprise Manager Cloud Control 12c Deep Dive by Michael New
Publié par McGraw-Hill Professional
ISBN-10: 0071790578
ISBN-13: 978-0071790574

Annexes

Table des matières

I.	11gR2 Database Installation (11.2.0.4) on Linux server x64	83
II.	Oracle Enterprise Manager Cloud Control 12c Installation.....	99
1.	Starting Cloud Control and all Its Components	106
2.	Stopping Cloud Control and all Its Components.....	107
III.	OEM 12c Agent installation & Database Discovery with Cloud Control.....	108
IV	Planning prévisionnel	119

I. 11gR2 Database Installation (11.2.0.4) on Linux server x64

1. User Creation:

Start putty with Xming

And do as shown below:

```
mkdir -p /IDBO/oem12c/ker1/11.2.0 IDBO
```

```
mkdir -p /IDBO/tmp0/tmp
```

```
export TEMP=/IDBO/tmp0/tmp
```

```
export TMPDIR=/IDBO/tmp0/tmp
```

```
export TMP=/IDBO/tmp0/tmp
```

```
export ORACLE_HOME=/IDBO/ker1/11.2.0
```

```
DISPLAY=192.168.1.128:0.0;
```

```
export DISPLAY
```

```
/etc
```

```
cp -p oraInst.loc oraInst.loc_IIC1
```

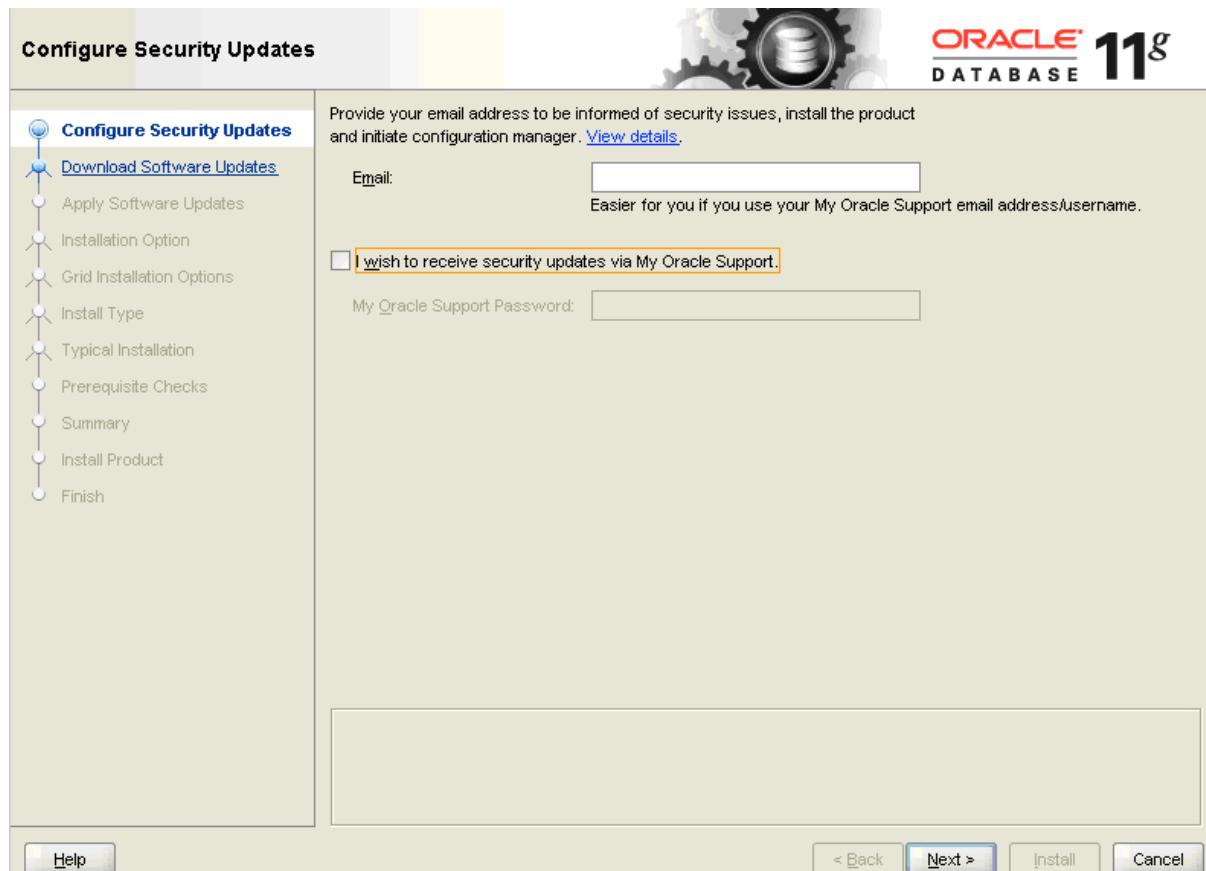
```
vi oraInst.loc
```

```
cp -p oraInst.loc oraInst.loc_IDBO
```

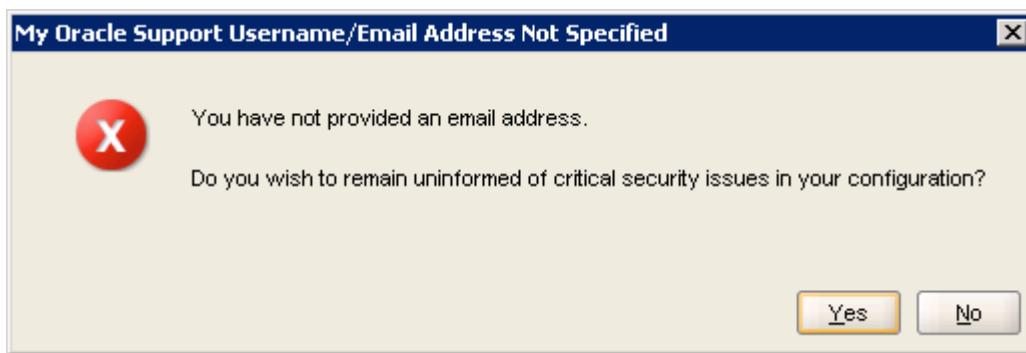
```
./runInstaller
```

```
cd /oraclestg/oracleRDBMS/11.2.0.3_Linux/database
```

Follow the installation instructions as below:

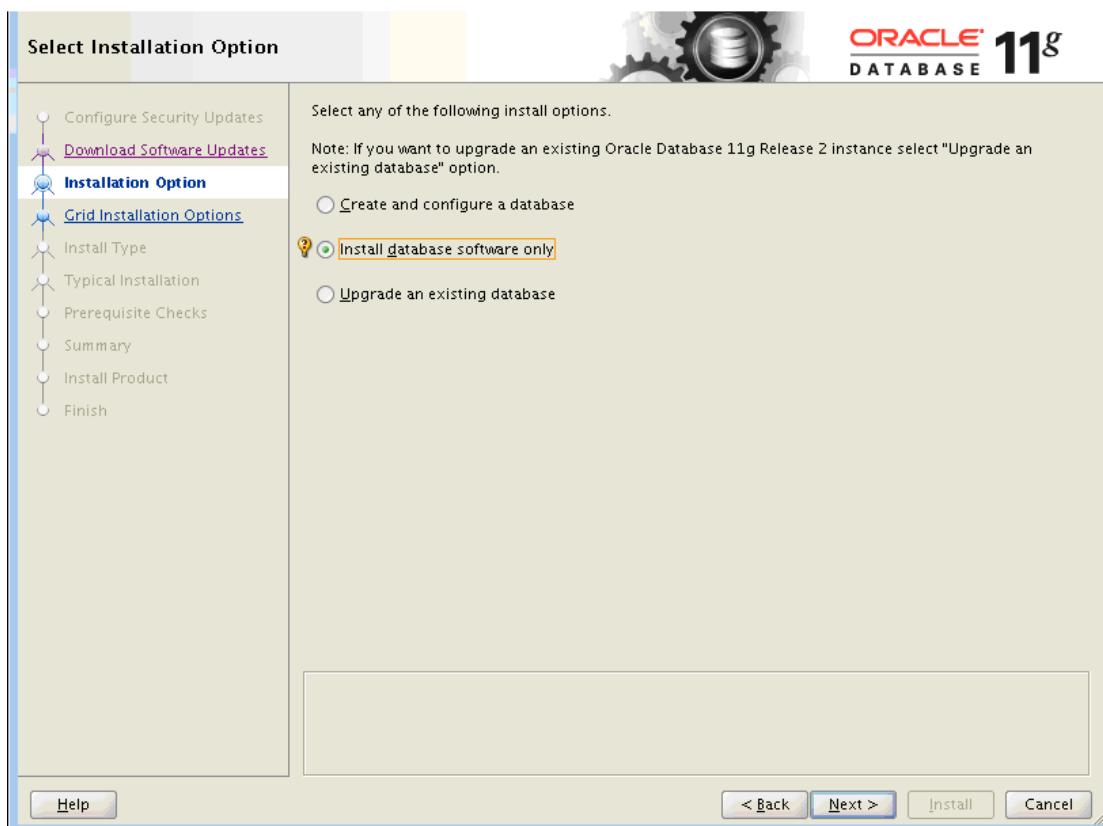


Don't do anything, just click on "Next"!

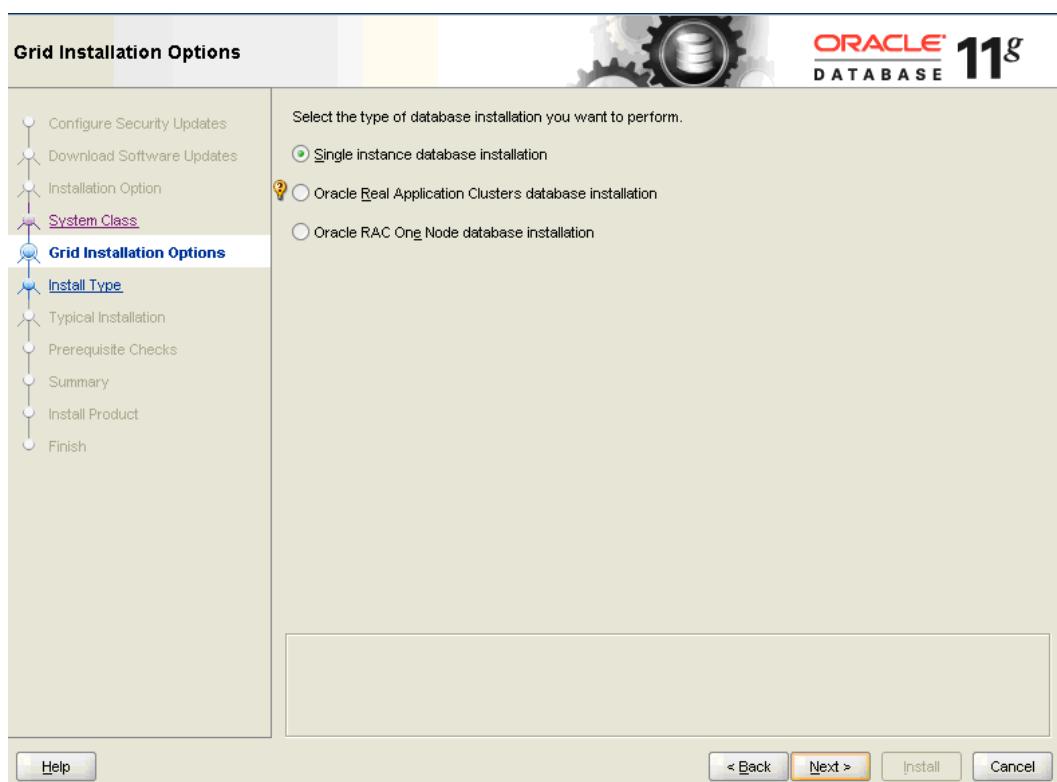


A warning message appears, click on "Yes"

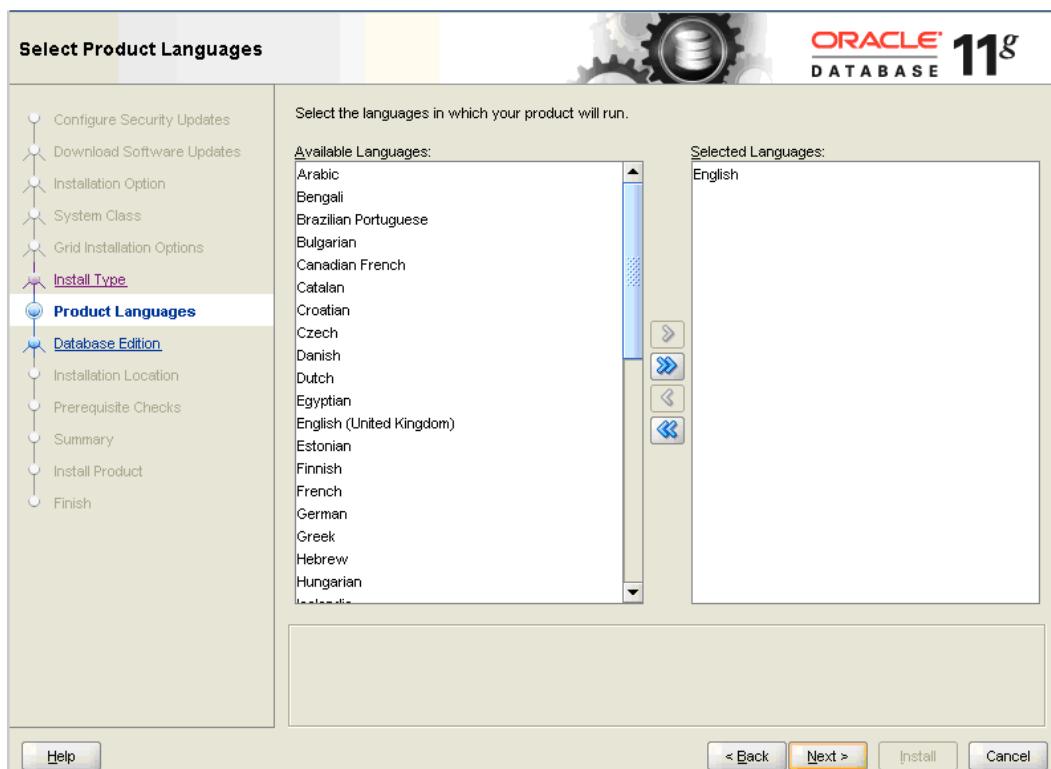
Select « Skip software updates



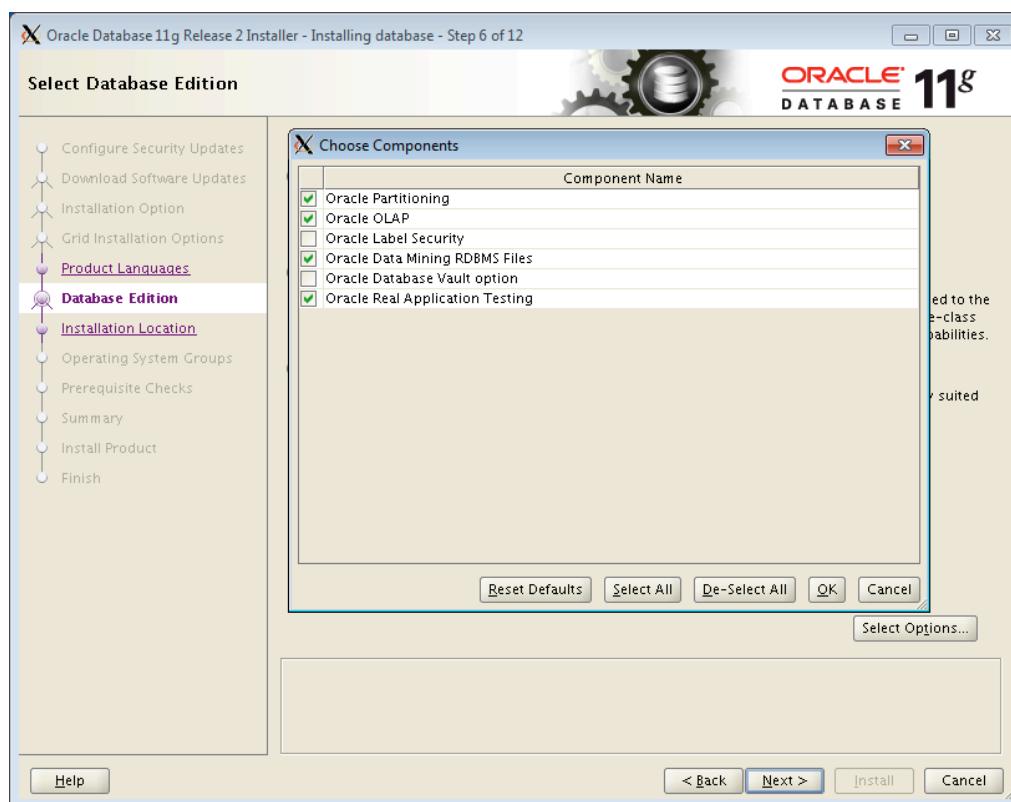
Select « Install database only », Click on “Next”



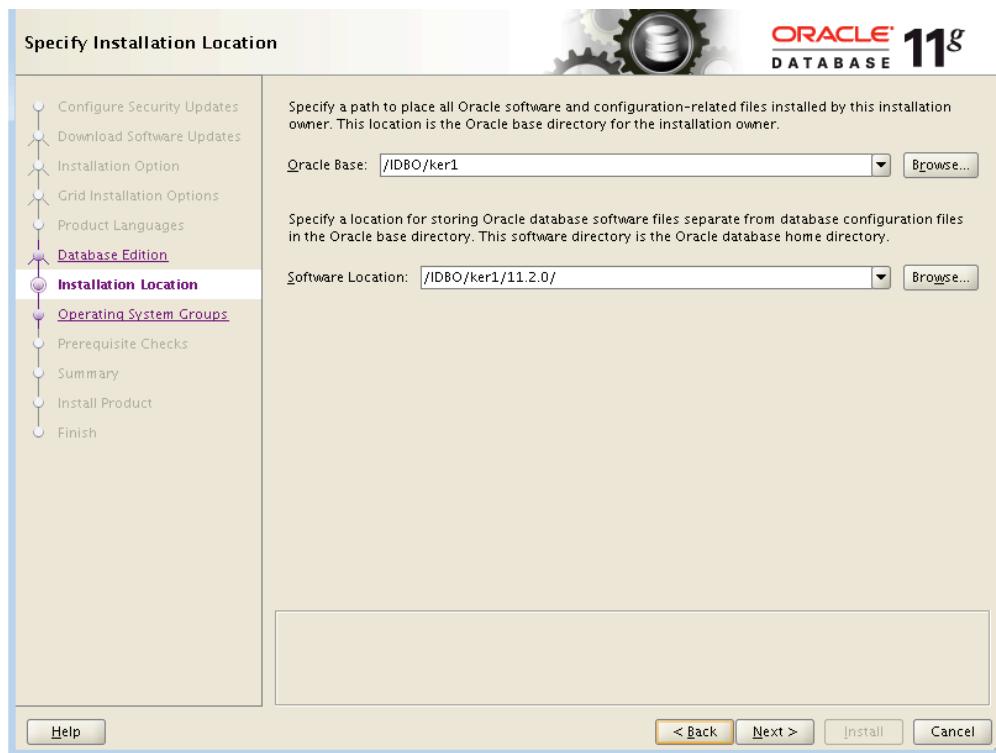
Select « Single instance installation », click on « Next »



Just click on « Next »

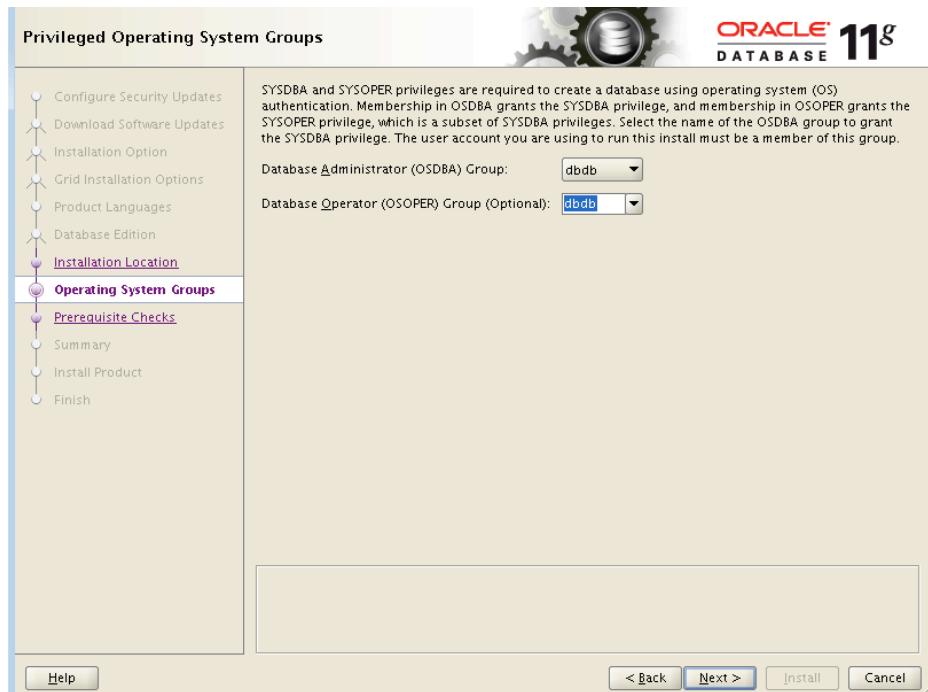


Select « Enterprise Edition », De-Select all the options and Click on OK and Next



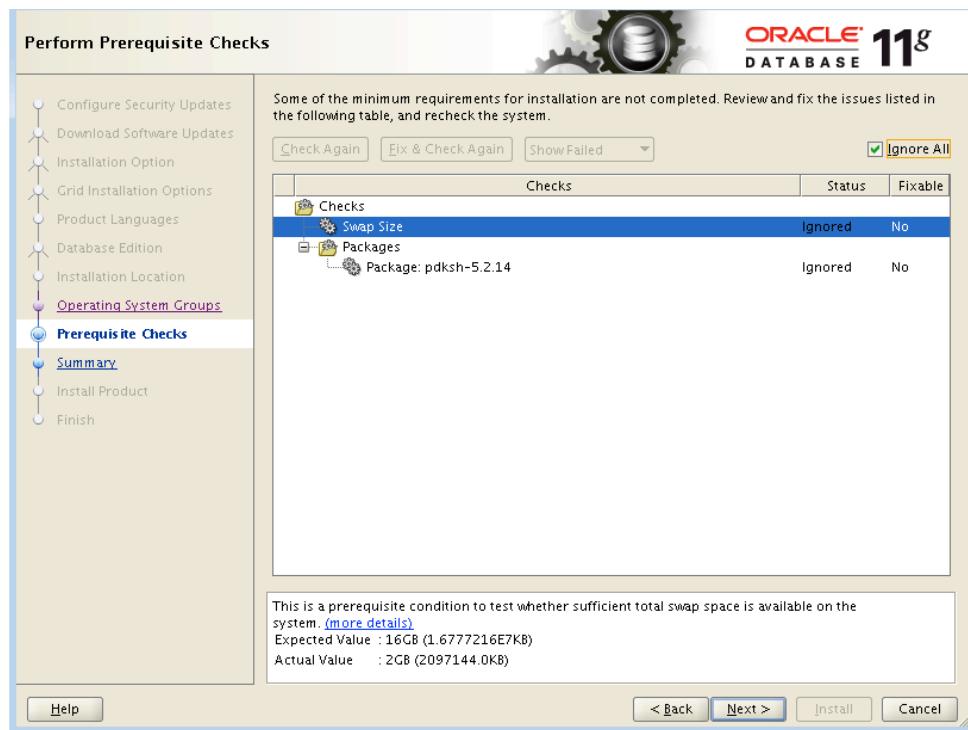
Oracle Base path is : D:\oracle\ora11g\database_SID (database_SID = IDBO for example)

Software location is: IDBO/ker1/11.2.0

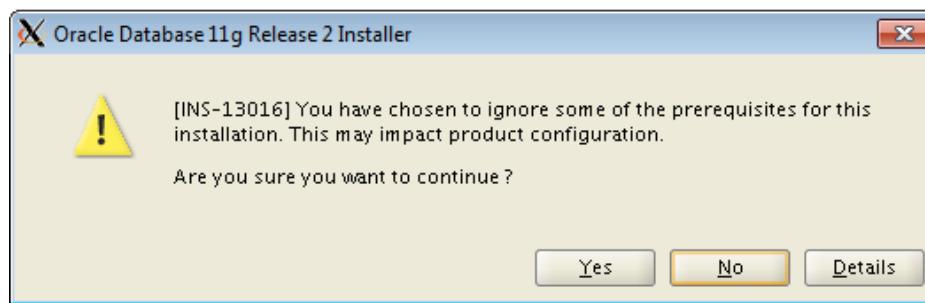


Database Administrator group : dbdb

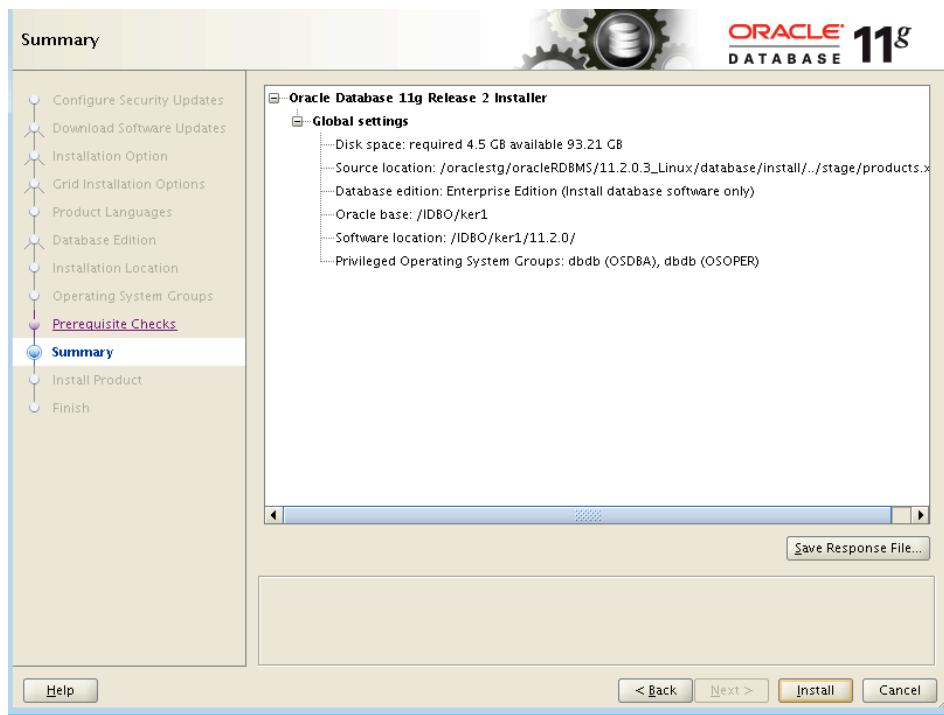
Database Operator Group : dbdb



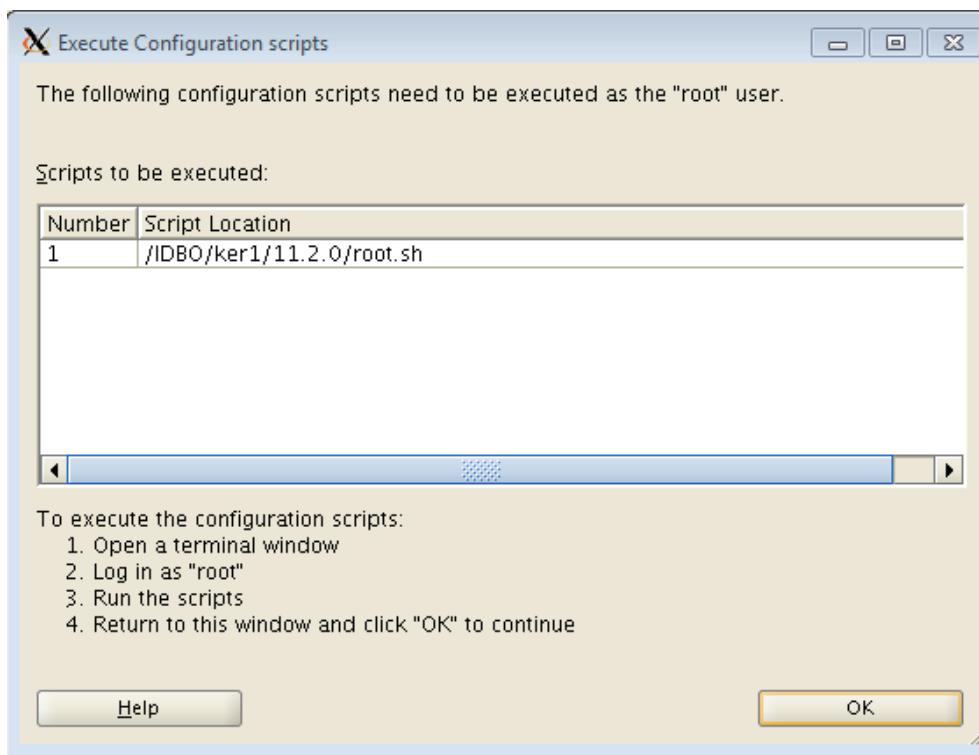
Select "Ignore All" Option to continue



A Warning window appears, click on "Yes"



Click on “Install”



Don't do anything yet

Do as shown below

Picture Version

The screenshot shows a terminal window titled 'root@freo1124: /IDBO/ker1/11.2.0'. It displays the output of a shell script running as root. The script performs several tasks: changing to the Oracle home directory, setting environment variables (ORACLE_OWNER to orIDBO, ORACLE_HOME to /IDBO/ker1/11.2.0), prompting for a local bin directory (which is left blank), and updating the /etc/oratab file. It also handles oraenv and coraenv files. Finally, it runs product-specific root actions.

```
root@freo1124:/IDBO/ker1/11.2.0
(root@freo1124:/oraclestg/oracleRDBMS/11.2.0.3_Linux/database)cd $ORACLE_HOME
(root@freo1124:/root)
(root@freo1124:/root)
(root@freo1124:/root)
(root@freo1124:/root)
Performing root user operation for Oracle 11g

The following environment variables are set as:
    ORACLE_OWNER= orIDBO
    ORACLE_HOME= /IDBO/ker1/11.2.0

Enter the full pathname of the local bin directory: [/usr/local/bin]:
The contents of "dbhome" have not changed. No need to overwrite.
The contents of "oraenv" have not changed. No need to overwrite.
The contents of "coraenv" have not changed. No need to overwrite.

Entries will be added to the /etc/oratab file as needed by
Database Configuration Assistant when a database is created
Finished running generic part of root script.
Now product-specific root actions will be performed.
Finished product-specific root actions.
(root@freo1124:/IDBO/ker1/11.2.0)
```

Text Version

```
(root@freo1124:/root)cd /IDBO/ker1/11.2.0/
(root@freo1124:/IDBO/ker1/11.2.0)
(root@freo1124:/IDBO/ker1/11.2.0)./root.sh

Performing root user operation for Oracle 11g
```

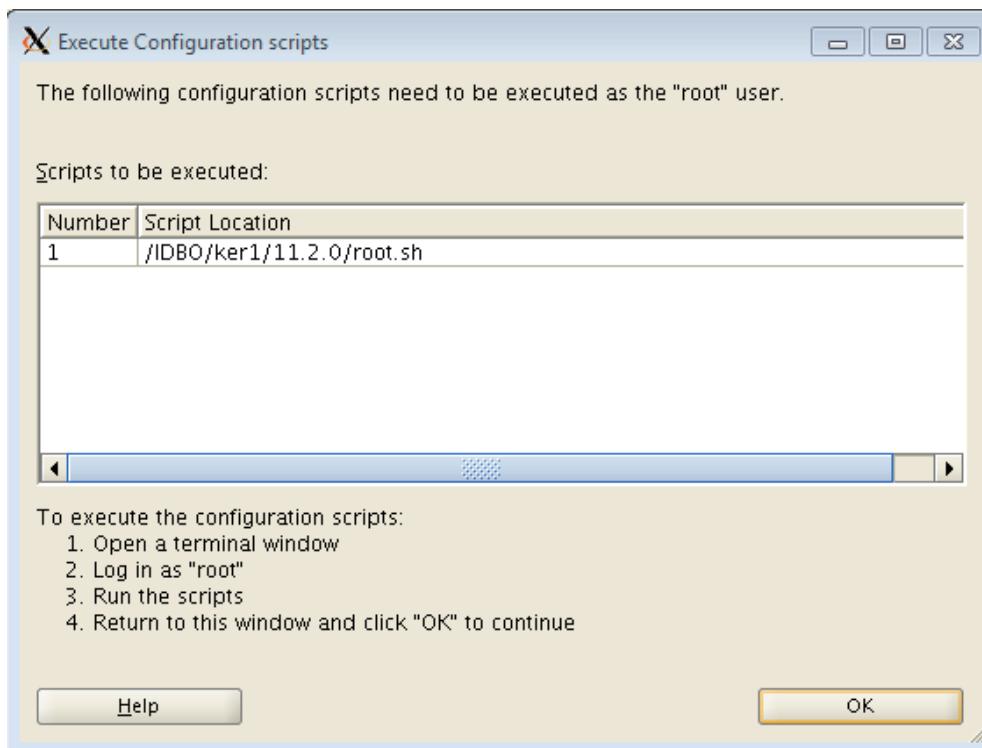
The following environment variables are set as:

```
ORACLE_OWNER= orIDBO
ORACLE_HOME= /IDBO/ker1/11.2.0
```

Enter the full pathname of the local bin directory:
[/usr/local/bin]:

The contents of "dbhome" have not changed. No need to overwrite.
The contents of "oraenv" have not changed. No need to overwrite.
The contents of "coraenv" have not changed. No need to overwrite.

Entries will be added to the /etc/oratab file as needed by
Database Configuration Assistant when a database is created
Finished running generic part of root script.
Now product-specific root actions will be performed.
Finished product-specific root actions.



Now you can click on Ok

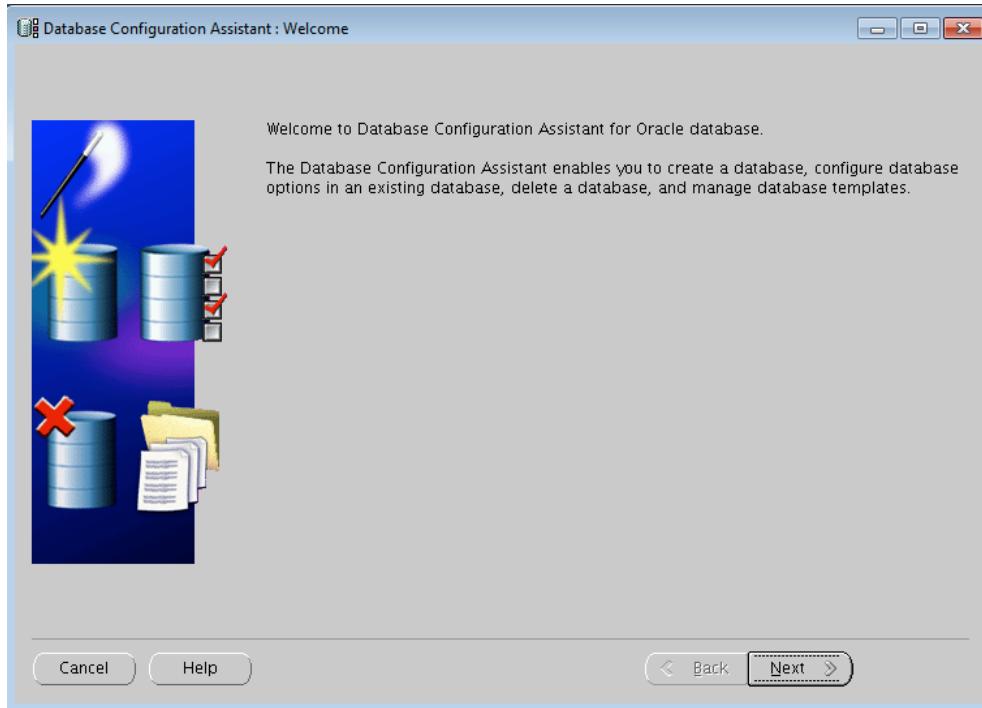


The installation has finished! You can close the program

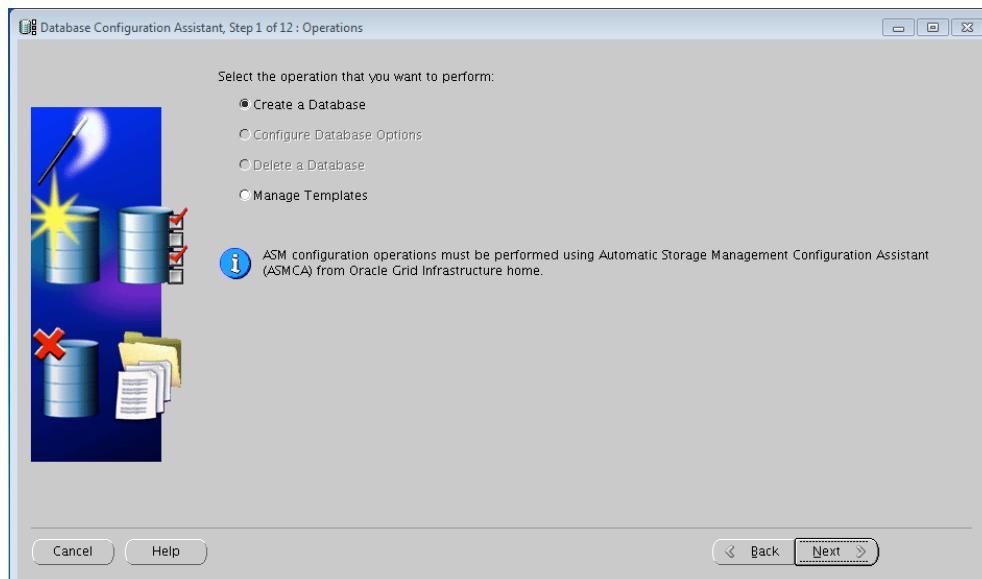
Now, you'll have to run the following commands :

```
export PATH=$ORACLE_HOME/bin:$PATH
```

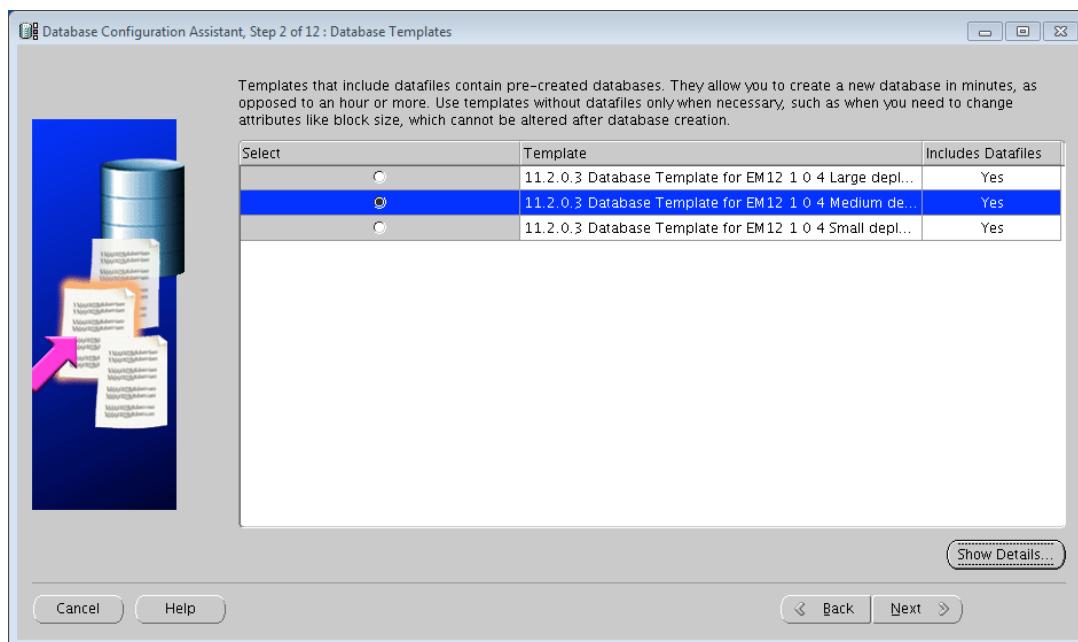
```
dbca
```



Click on Next

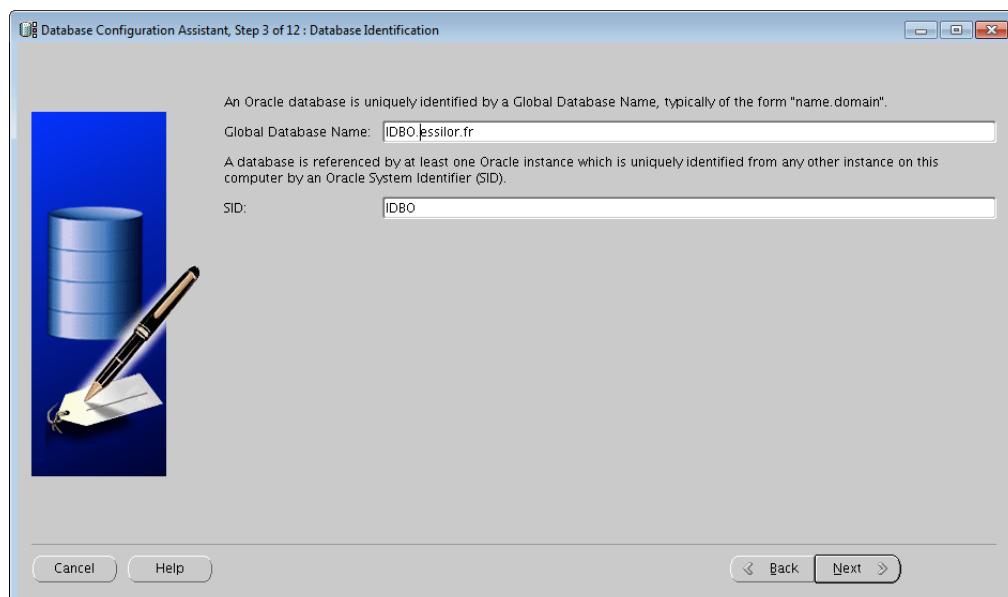


Select "Create a Database" option and click on Next



Select the second option: 11.2.0.3 “Database Template for EM12 1 0 4 Medium deployment”

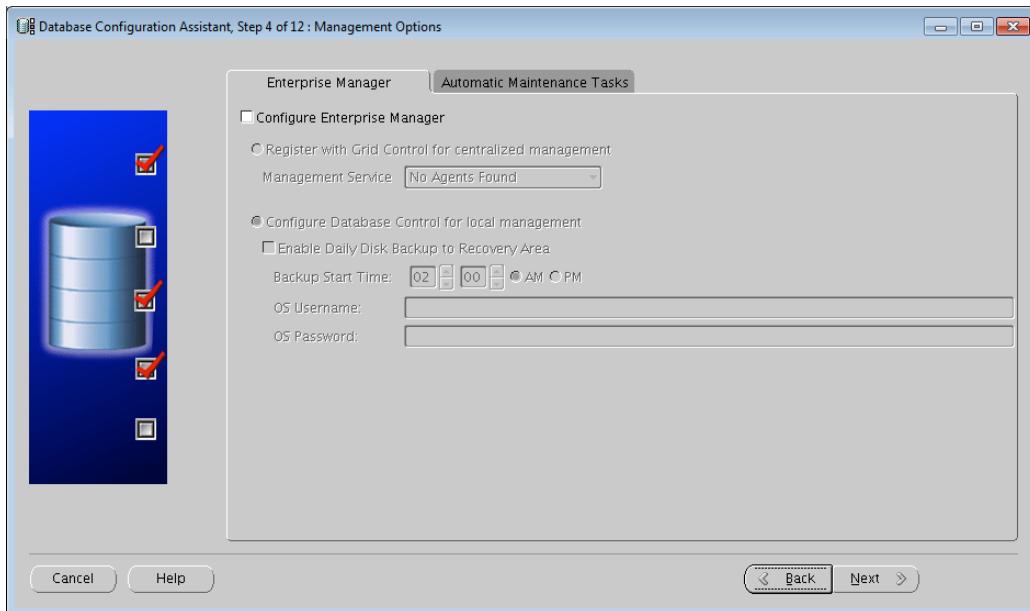
Click on Next



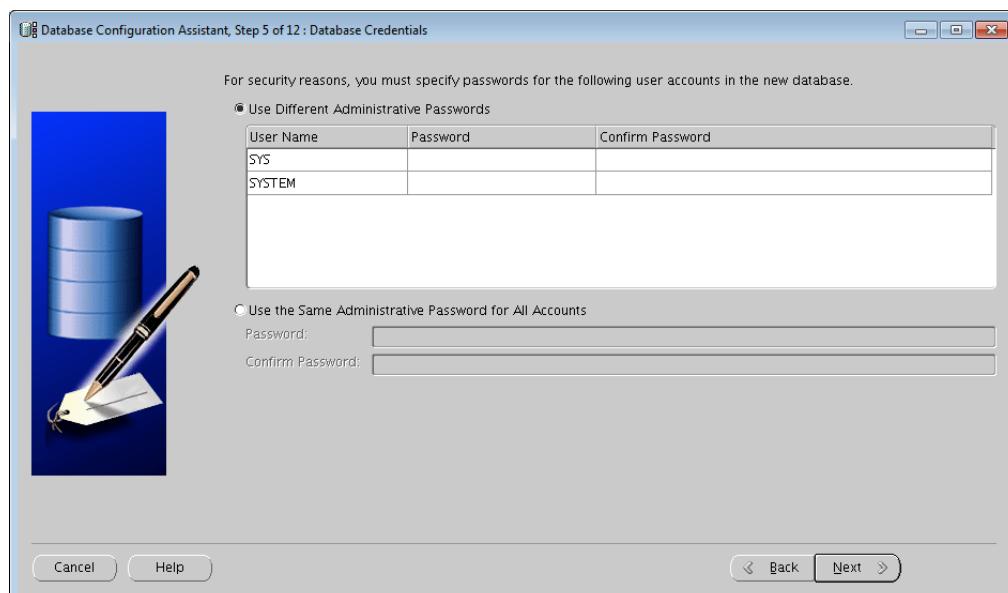
Global Database Name: IDBO.essilor.fr

SID: IDBO

Click on Next



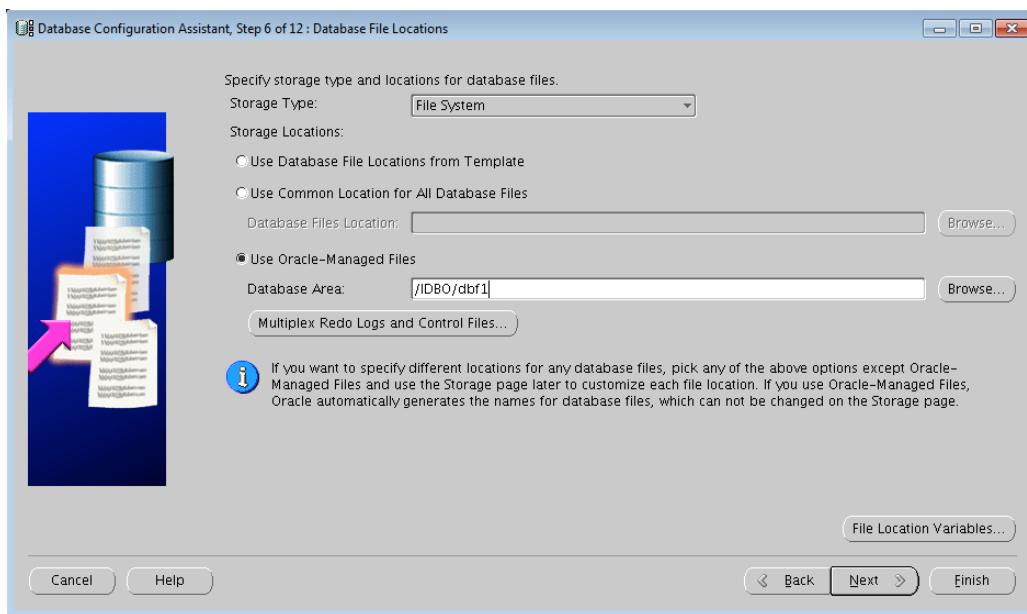
Unselect all options and click on next



Type the SYS user password

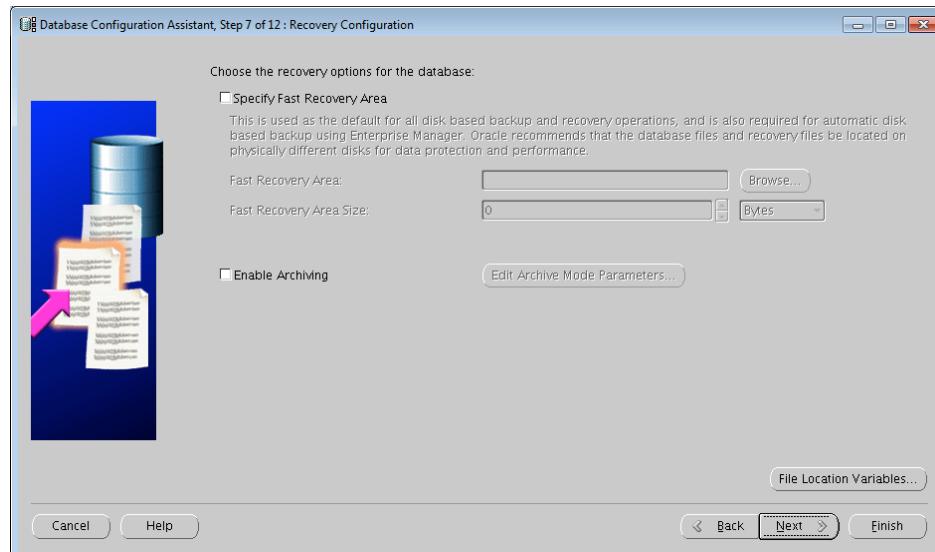
Type the SYSTEM user Password

Click on Next

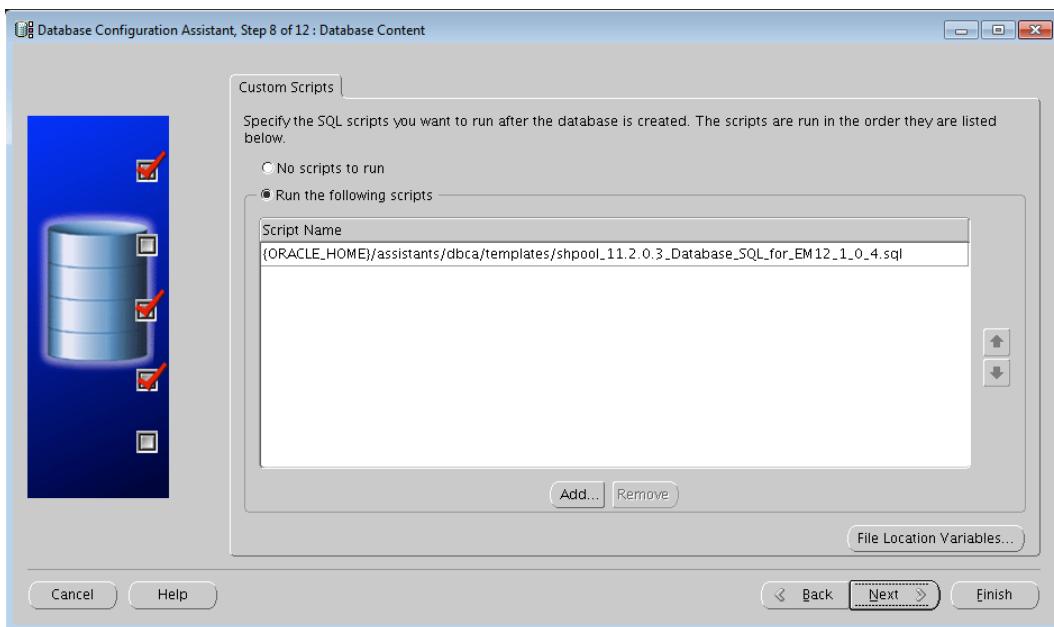


Select the “Use Oracle-Managed Files” option and enter:

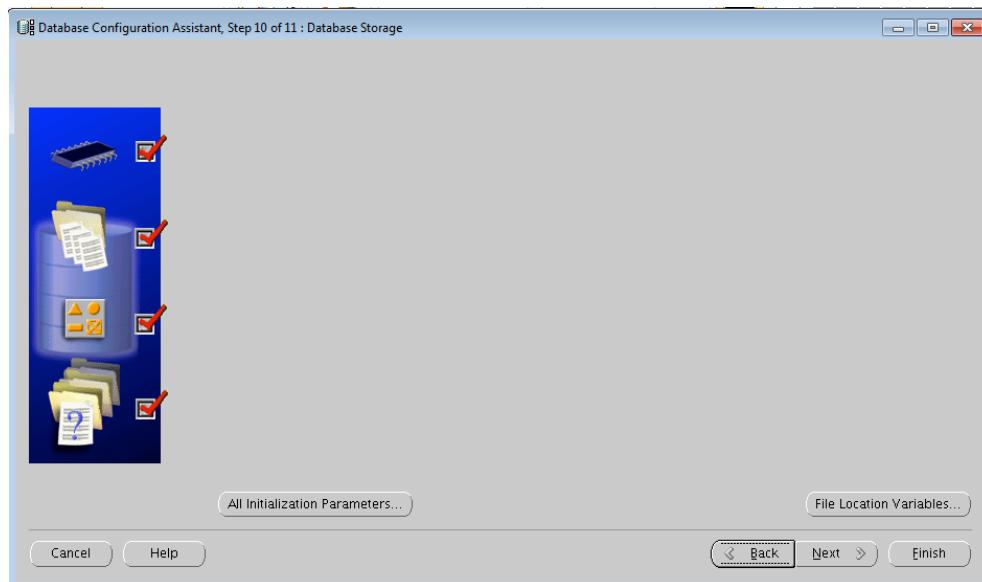
/IDBO/dbf1



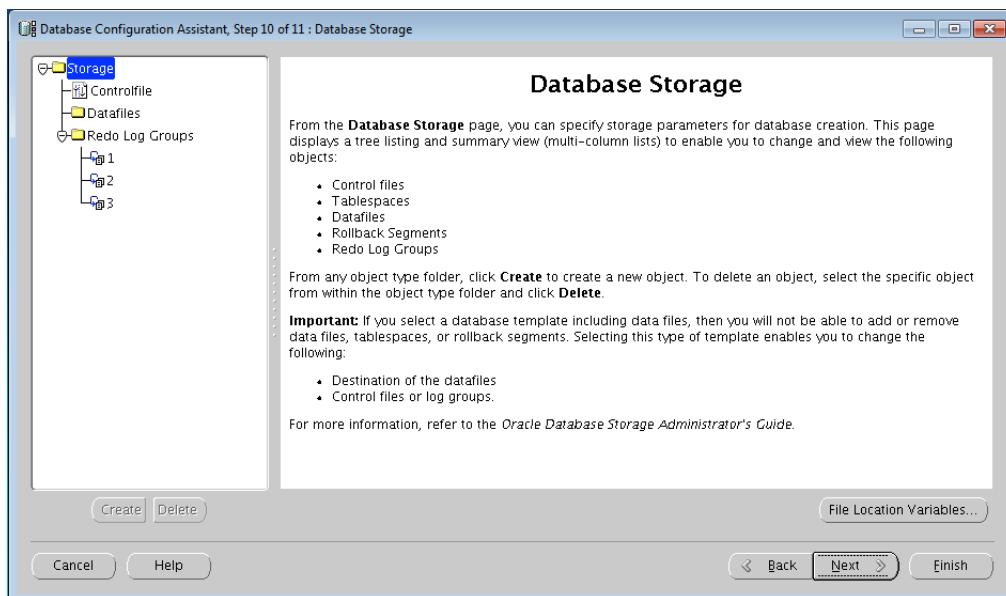
Unselect all option and click on Next



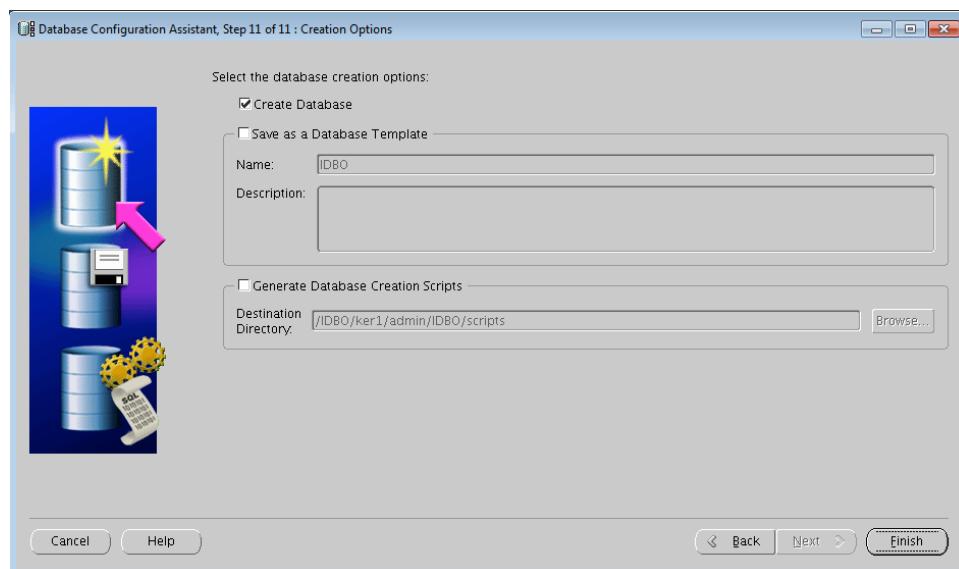
Select the “Run the following scripts” option and click on Next



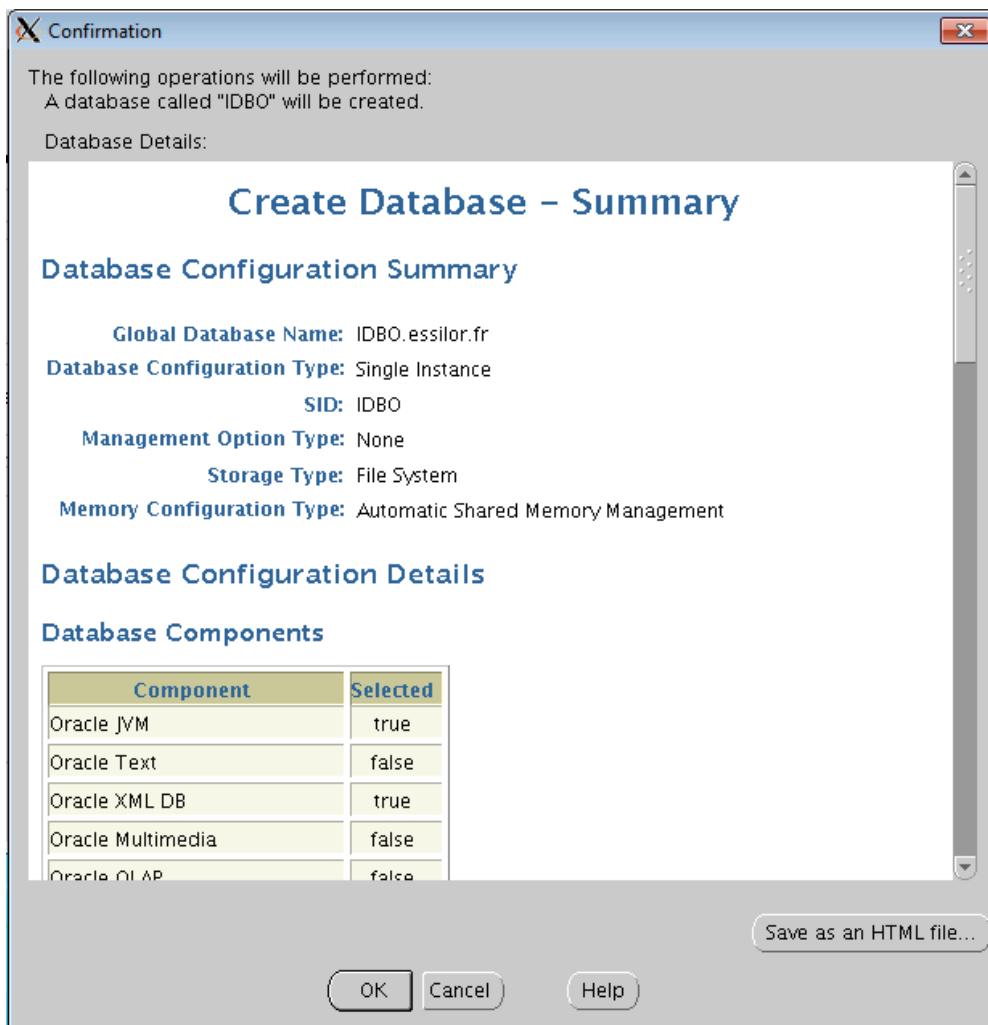
Just click on Next



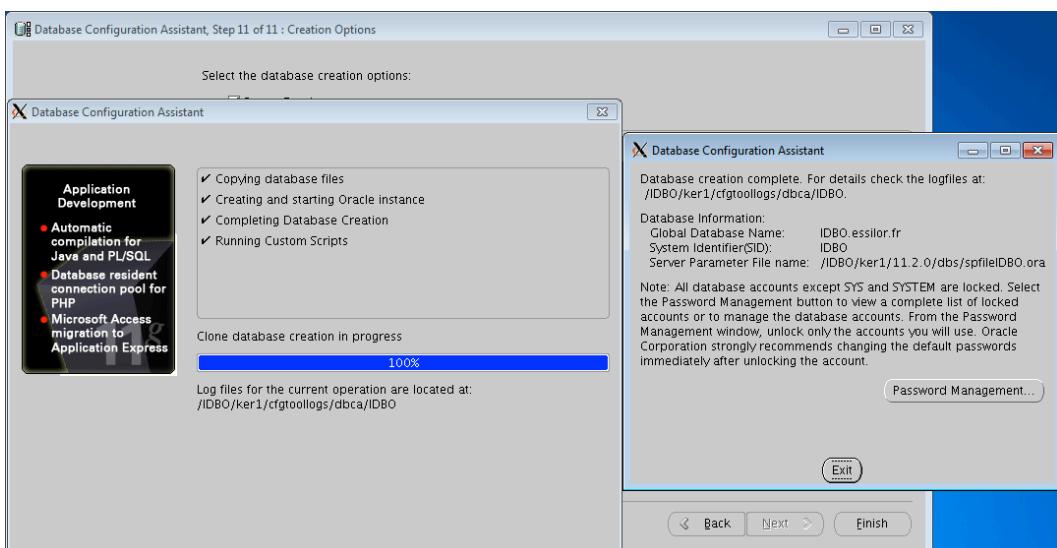
Click on Next



Select the “Create Database” Option and click on “Finish”



Click on Ok



Click on Exit, it's over.

II. Oracle Enterprise Manager Cloud Control 12c Installation

Start putty with Xming

oraInst.loc Setup

You'll need to check if the oraInst.loc file has been correctly set. Follow the steps below:

```
cd /etc  
cat oraInst.loc
```

The oraInst.loc should be set as :

```
inventory_loc=/IDBO/ker1/oraInventory  
inst_group=dbdb
```

If you have to change the content of oraInst.loc, don't forget to save the information first:

```
mv oraInst.loc oraInst_XXXX.loc  
mv oraInst.loc_IDBO oraInst.loc
```

Now you need to configure the environment that is necessary for the OEM installation

IDBO Environment Setup

```
export TEMP=/IDBO/tmp0/tmp  
export TMPDIR=/IDBO/tmp0/tmp  
export TMP=/IDBO/tmp0/tmp  
export TEMPDIR=/IDBO/tmp0/tmp  
export ORACLE_HOME=/IDBO/ker1/11.2.0/  
export ORACLE_SID="IDBO"  
export OMS_HOME=/IDBO/ker3/oem12cMHL/oms  
export AGENT_HOME=/IDBO/ker3/oem12cA/core/12.1.0.4.0/  
export PATH=$ORACLE_HOME/bin:$PATH  
export TNS_ADMIN=/IDBO/ker1/11.2.0/network/admin  
export ORACLE_UNQNAME=IDBO
```

Or run the IDBO environment script

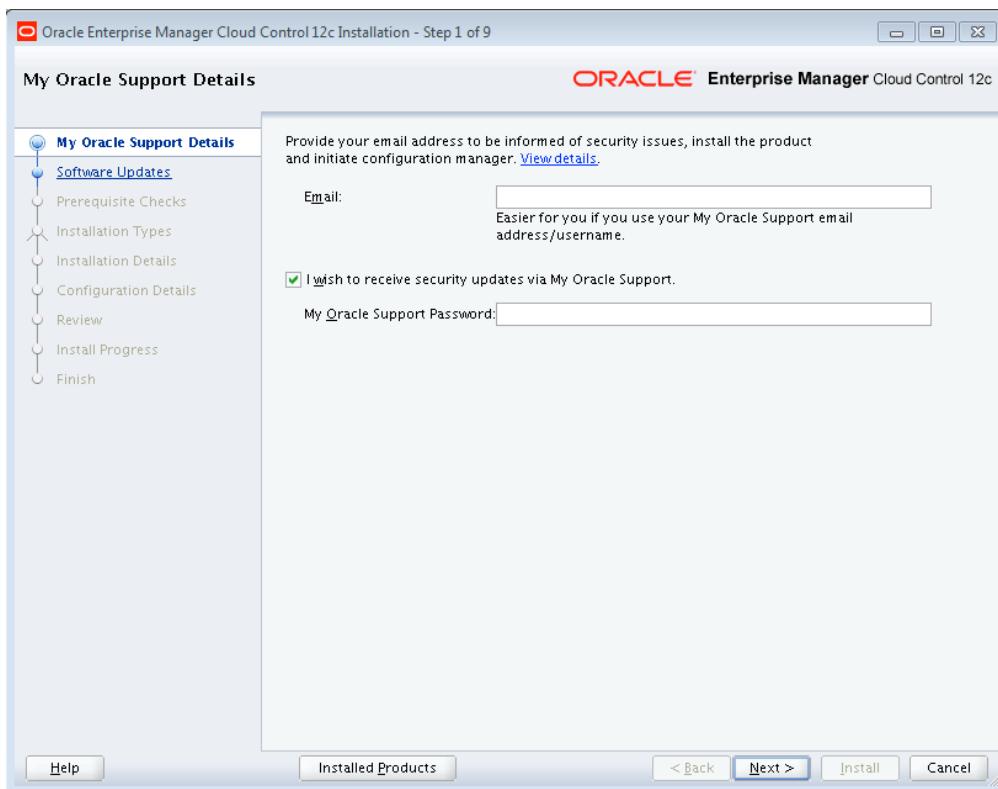
```
cd /IDBO/ker1/11.2.0/IDBO  
vi IDBO_fre01124.env
```

Then check / edit the listener

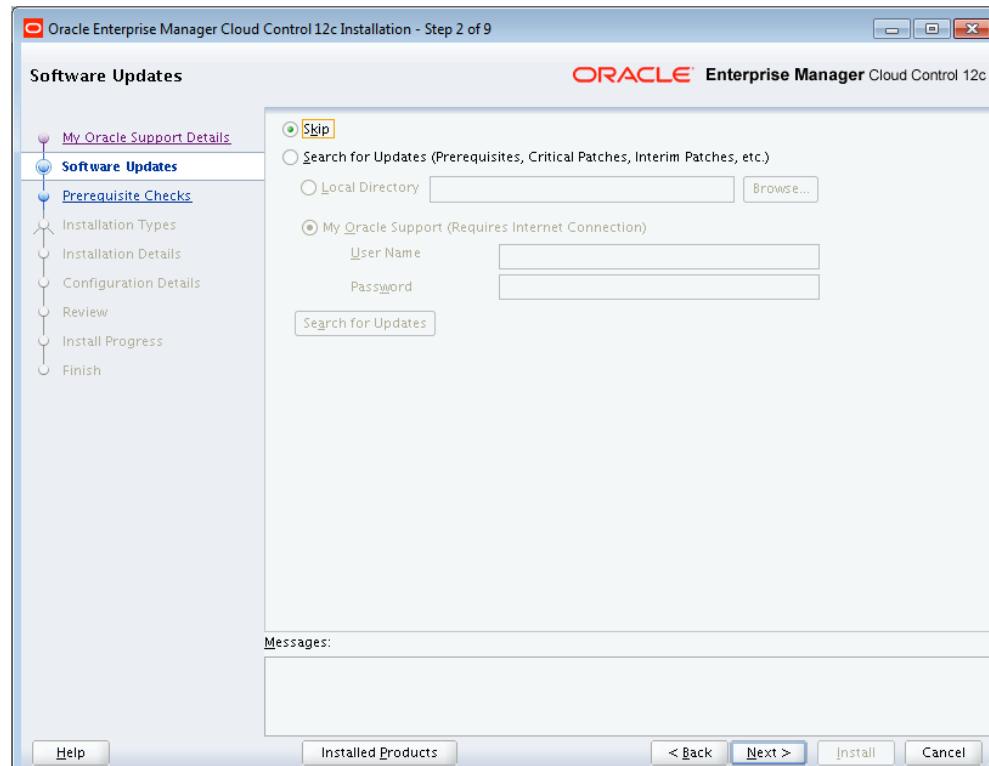
```
cd /IDBO/ker1/11.2.0/network/admin  
vi listener.ora
```

```
====  
#           listener.ora          Network          Configuration      File:  
/IDBO/oem12c/ker1/11.2.0/network/admin/listener.ora  
# Generated by Oracle configuration tools.  
  
IDBO =  
(DESCRIPTION_LIST =  
(DESCRIPTION =  
  (ADDRESS = (PROTOCOL = TCP) (HOST = freo1124.essilor.fr) (PORT = 1521))  
  (ADDRESS = (PROTOCOL = IPC) (KEY = EXTPROC1521))  
)  
)  
  
ADR_BASE_EM12 = /IDBO/ker1  
====  
vi tnsnames.ora  
====  
IDBO =  
(DESCRIPTION_LIST =  
(DESCRIPTION =  
  (ADDRESS = (PROTOCOL = TCP) (HOST = freo1124.essilor.fr) (PORT = 1521))  
  (ADDRESS = (PROTOCOL = IPC) (KEY = EXTPROC1521))  
)  
)  
====  
  
lsnrctl start IDBO  
cd /IDBO  
mkdir ker3  
chmod 775 ker3  
  
cd /oraclestg/soft/linux/OEM/12c14  
.runInstaller
```

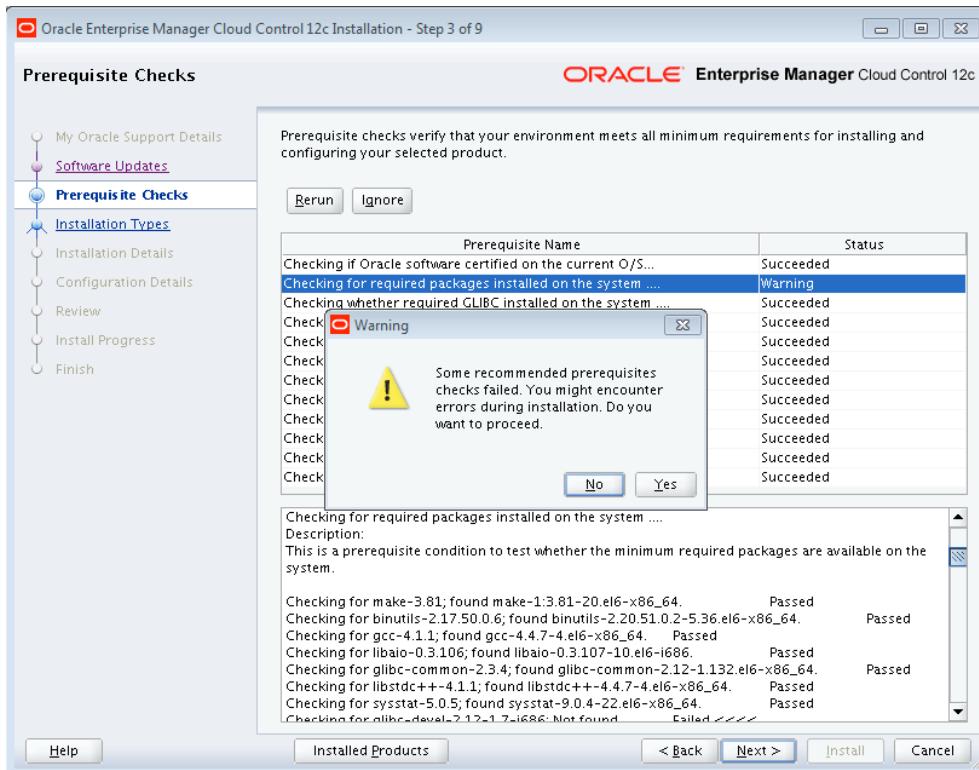
Follow the installation instructions as below:



Click on Next and confirm your choice by clicking “Yes” when the warning window appears.

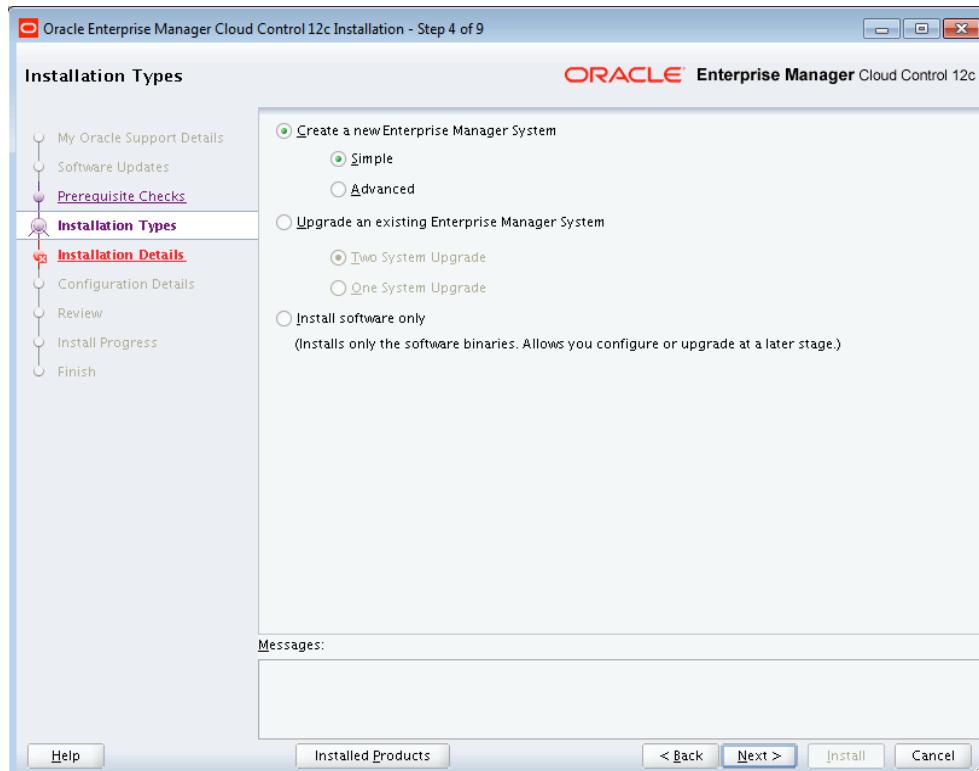


Select “Skip” and click on Next



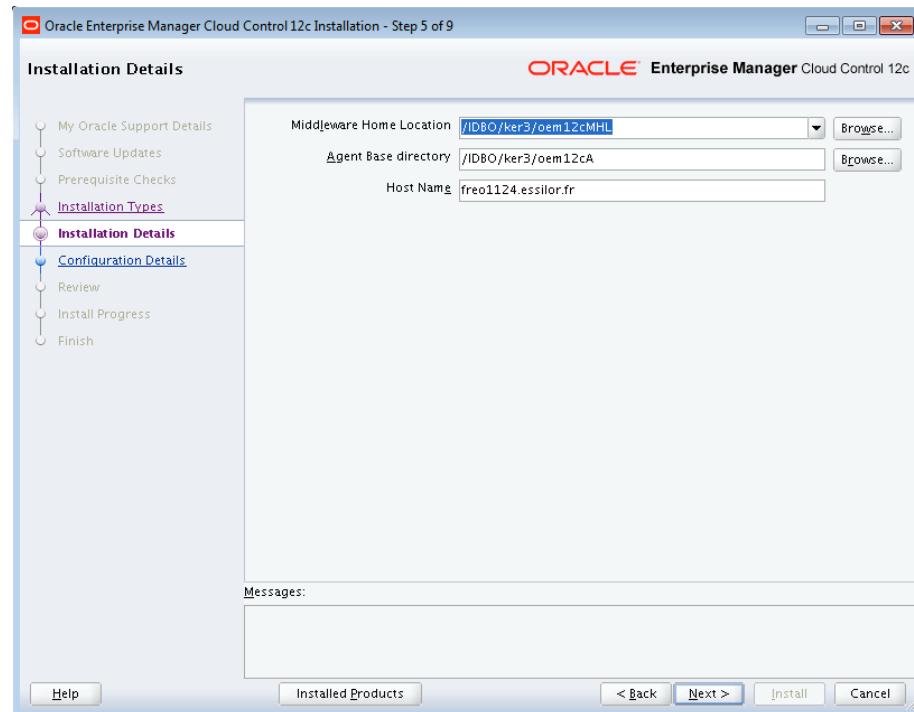
You can choose to ignore the package warning, but it can be troublesome for the installation.

Click on Next



Select the “Create a new Enterprise Manager System > Simple” options

Click on Next

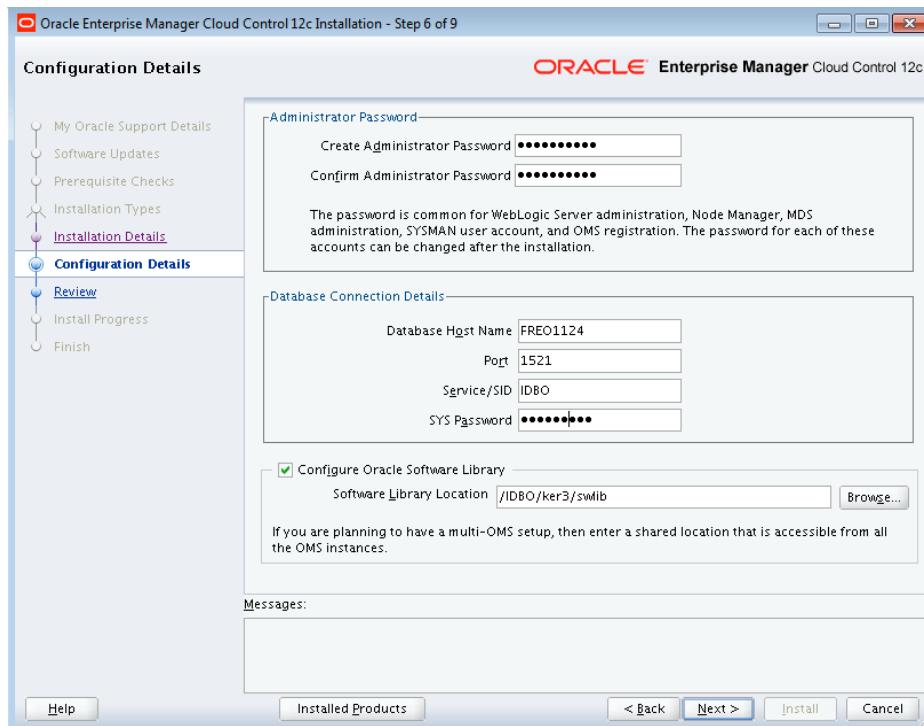


Middle Home Location: /IDBO/ker3/oem12cMHL

Agent Base directory: /IDBO/ker3/oem12cA

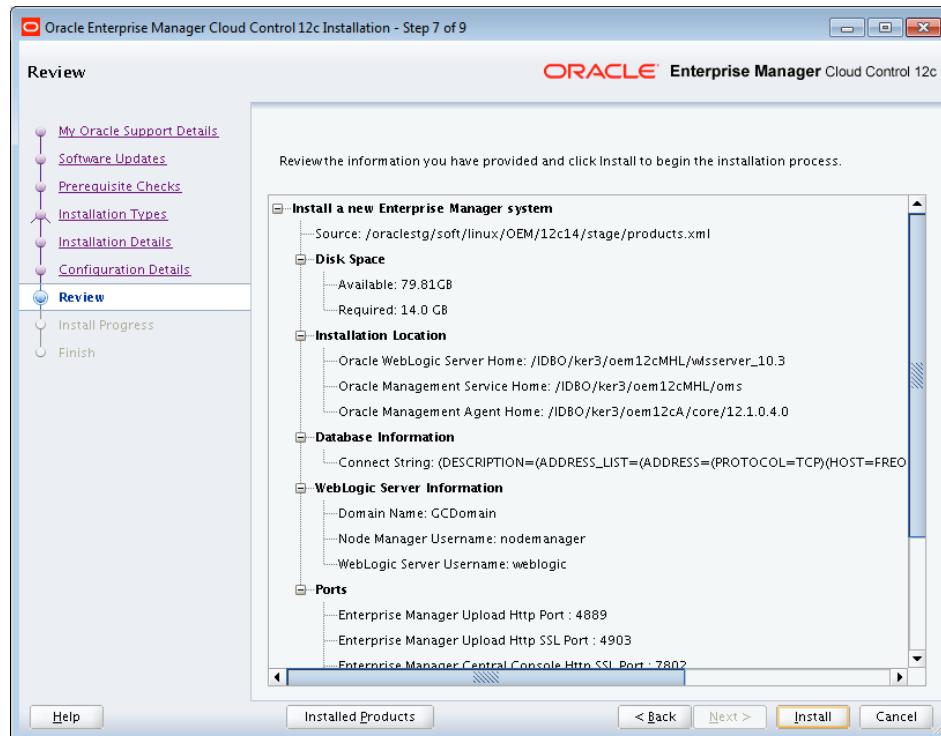
Host Name: freo1124.essilor.fr

Click on Next

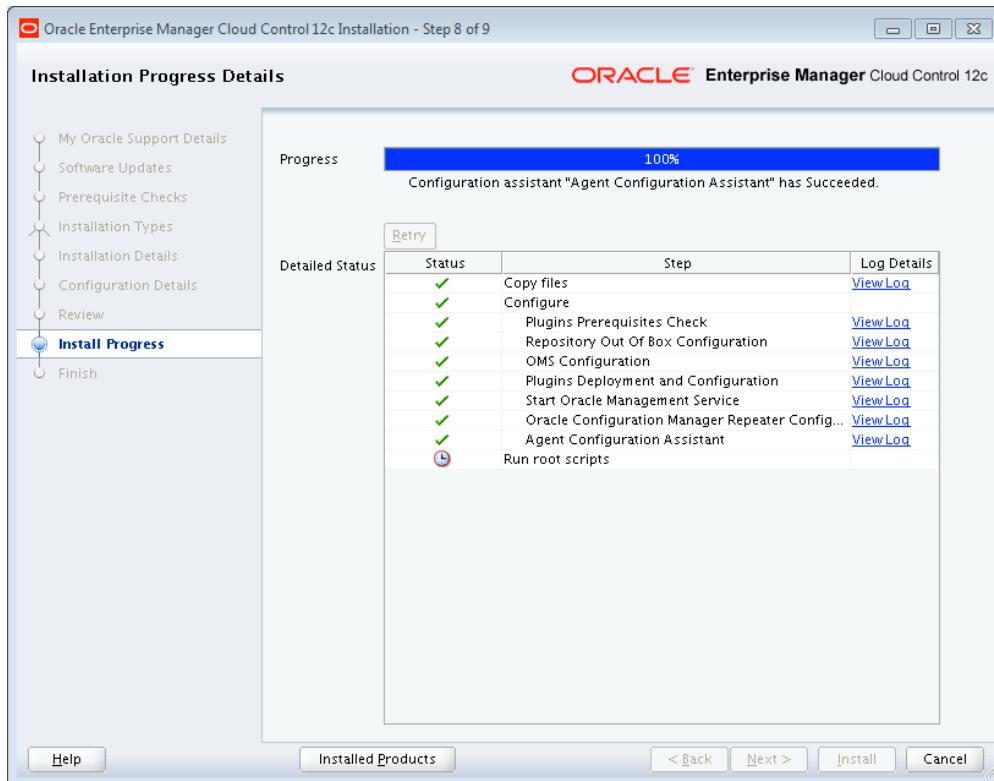


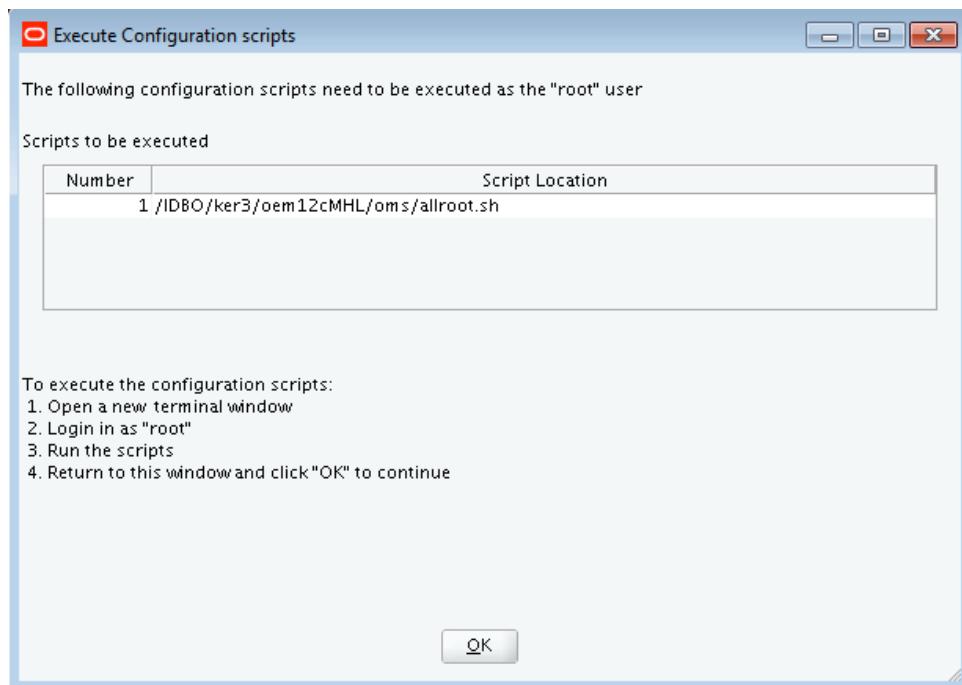
Admin PWD = oem12c1234 Database Host Name: FREO1124

Service SID: IDBO Sys PWD = sysoem12c Port: 1521



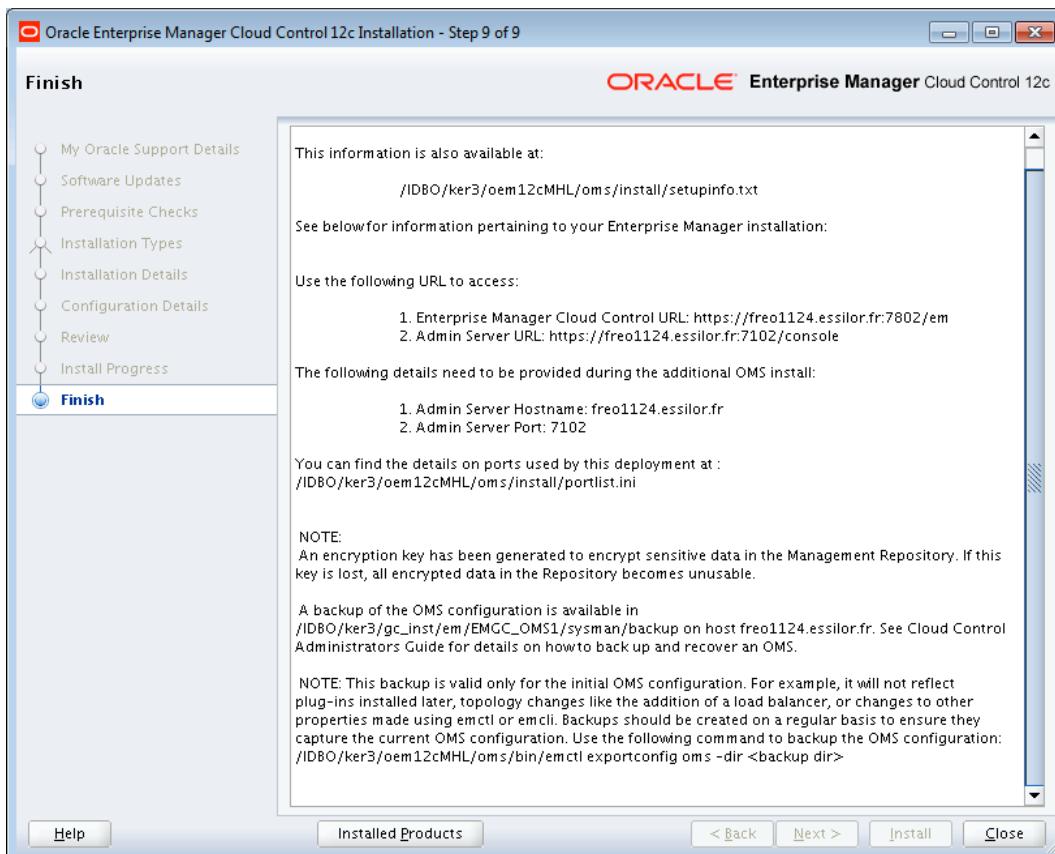
Check “Disk Space” and click on next if it’s ok.





You'll need to connect as root to execute the script "allroot.sh" located in:

/IDBO/ker3/oem12cMHL/oms/allroot.sh



The installation finished successfully, just click on "Close"

1. Starting Cloud Control and all Its Components

The following procedure summarizes the steps required to start all the components of the Cloud Control. For example, use this procedure if you have restarted the host computer and all the components of the Cloud Control have been installed on that host.

To start all the Cloud Control components on a host, use the following procedure.

If your Oracle Management Repository resides on the host, change directory to the Oracle Home for the database where you installed the Management Repository and start the database and the Net Listener for the database:

- Set the ORACLE_HOME environment variable to the Management Repository database home directory.
- Set the ORACLE_SID environment variable to the Management Repository database SID (default is asdb).
- Start the Net Listener:
- \$PROMPT> \$ORACLE_HOME/bin/lsnrctl start

Start the Management Repository database instance:

- sqlplus « /as sysdba » ;
- SQL> startup
- SQL> quit

Start the Oracle Management Service:

- \$PROMPT> OMS_HOME/bin/emctl start oms

"Controlling the Oracle Management Service"

- Change directory to the home directory for the Oracle Management Agent and start the Management Agent:
- \$PROMPT> AGENT_HOME/bin/emctl start agent

"Controlling the Oracle Management Agent"

Be sure to run the emctl start agent command in the Oracle Management Agent home directory and not in the Management Service home directory.

2. Stopping Cloud Control and all Its Components

The following procedure summarizes the steps required to stop all the components of the Cloud Control. For example, use this procedure if you have installed all the components of the Cloud Control on the same host you want to shut down or restart the host computer.

To stop all the Cloud Control components on a host, use the following procedure :

Stop the Oracle Management Service :

- \$PROMPT> \$ORACLE_HOME/bin/emctl stop oms -all

"Controlling the Oracle Management Service"

Change directory to the home directory for the Oracle Management Agent and stop the Management Agent:

- \$PROMPT> AGENT_HOME/bin/emctl stop agent

"Controlling the Oracle Management Agent"

Be sure to run the emctl stop agent command in the Oracle Management Agent home directory and not in the Oracle Management Service home directory.

If your Oracle Management Repository resides on the same host, change directory to the Oracle Home for the database where you installed the Management Repository and stop the database and the Net Listener for the database:

- Set the ORACLE_HOME environment variable to the Management Repository database home directory.
- Set the ORACLE_SID environment variable to the Management Repository database SID (default is asdb).

Stop the database instance:

1. \$PROMPT> ORACLE_HOME/bin/sqlplus /nolog
2. SQL> connect SYS as SYSDBA
3. SQL> shutdown
4. SQL> quit

- Stop the Net Listener:

```
$PROMPT> $ORACLE_HOME/bin/lsnrctl stop
```

III. OEM 12c Agent installation & Database Discovery with Cloud Control

URL OEM 12c sur Freo1124: <https://freo1124.essilor.fr:7802/em/>

1°) Log into the system with the SYSMAN User



You have now access to the Home Page

The screenshot shows the Oracle Enterprise Manager Cloud Control 12c home page. At the top, there's a navigation bar with links for 'Enterprise', 'Gîtes', 'Favoris', and 'Historique'. The main title is 'ORACLE Enterprise Manager Cloud Control 12c'. Below the title, a large '12c' watermark is visible. On the left, there's a sidebar with 'Aperçu d'Enterprise Manager' and 'Dernières fonctionnalités'. The main content area has a 'Bienvenue dans Enterprise Manager Cloud Control' section with a brief introduction about Oracle Enterprise Manager being a line of enterprise management products. It also features a 'Cloud Control total' summary with three items: 'Gestion du cycle de vie Cloud complet', 'Gestion de l'application au disque intégrée', and 'Gestion des applications orientées entreprise'. To the right, there's a 'Mise en route' sidebar with several items listed. At the bottom, there's a section titled 'Selectionner la page d'accueil Enterprise Manager' with a note about selecting a personal start page. Below this, there are several thumbnail previews of different dashboards, each labeled with its purpose: 'Page de bienvenue', 'Toutes les cibles', 'Plan du site', 'Recapitulatif', 'Bases de données', 'Incidents', 'SOA', 'Middleware', 'Application de composite', and 'Services'. A 'CONSEIL' note at the bottom left suggests using the 'SYSMAN > Page de bienvenue' menu.

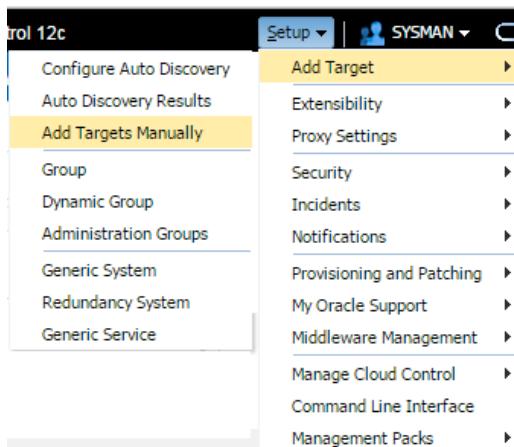
Warning: Before deploying the agent, you need to follow these steps:

- ➔ Create a orPDBO user ,group dbdb, on the targeted server
- ➔ Create a filesystem. Example : /PDBO
- ➔ Create a directory. Example : /PDBO/oem12c
- ➔ Configure the /etc/oralInst.loc file as following:

```
====                                     cat                               /etc/oralInst.loc
inventory_loc=/PDBO/oralInventory
inst_group=dbdb
```

====

2°) Select the Setup menu and click on « Add Target Manually »



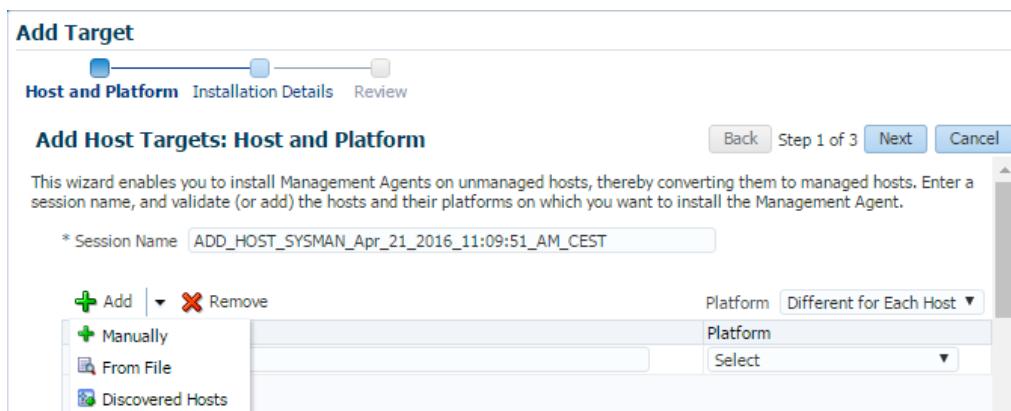
3°) Choose “Ass Host Targets” and click on “Add Host ...”

The screenshot shows the 'Add Targets Manually' page. At the top, there are navigation links for 'Enterprise', 'Targets', 'Favorites', and 'History'. Below that, the title is 'Add Targets Manually' with a refresh icon. A message at the top right says 'Page Refreshed Apr 21, 2016 11:06:51 AM CES'. The main content area has a heading 'Instruction' with a blue arrow icon. It contains three radio button options:

- Add Host Targets
- Add Targets Using Guided Process
- Add Targets Declaratively by Specifying Target Monitoring Properties

At the bottom of the page are two buttons: 'Add Host ...' and 'Add Host Results'.

4°) Click on the “Add” Menu and Select “Manually” as below



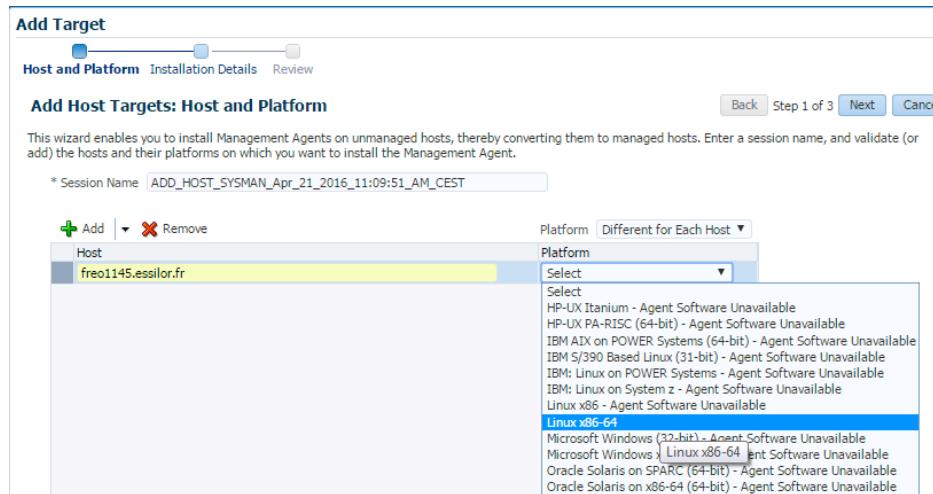
5°) a°) As **Host**, you need to enter a complete host name.

Example: freo1145 IS NOT CORRECT.

freo1145.essilor.fr IS CORRECT

b°) Under the **Platform** section, select the **Linux x86-64** option

Click on “Next”



Example of deployment Agent on freo1151:

=====

Installation Base Directory : **/PDBO/oem12c**

Instance Directory : (Automatic)

Named Credential: Choose a Sudo user

Privileged Delegation Setting: *Do not touch*

Port : *Do not touch*

=====

Add Target

Host and Platform **Installation Details** Review

Add Host Targets: Installation Details

On this screen, select each row from the following table and provide the installation details in the Installation Details section.

Deployment Type: Fresh Agent Install

Platform	Agent Software Version	Hosts	Mandatory Inputs
Linux x86-64	12.1.0.4.0	freo1142.essilor.fr	

Linux x86-64: Agent Installation Details

* Installation Base Directory: /PDBO/oem12c
* Instance Directory: /PDBO/oem12c/agent_inst
* Named Credential: Select
Privileged Delegation Setting: /usr/bin/sudo -u %RUNAS% %COMMAND%
Port: 3872

Optional Details

Click on the Blue Cross

6°) Enter the asked information

Example:

UserName : emPDBO

Password: *****

Confirm Password: *****

Run Privilege: None

Check the “Save As” Box and rename it as you want

Create new Named Credential

Enter the user name and password you want to save as a Named Credential.

* UserName	emPDBO
* Password	*****
* Confirm Password	*****
Run Privilege	None
Save As	NC_freo1145_2016-04-20-190139

OK Cancel

7°) Before this step, as it has been reminded earlier, you need to:

- ➔ Create a emPDBO user ,group dbdb, on the targeted server
- ➔ Create a filesystem. Example : /PDBO
- ➔ Create a directory. Example : /PDBO/oem12c
- ➔ Configure the /etc/oralinst.loc file as following:

8°) You can now deploy the agent by clicking on the « Deploy Agent » button.

Add Target

Host and Platform Installation Details Review

Add Host Targets: Review

Back Step 3 of 3 Next Deploy Agent Cancel

Review the details you have provided for this deployment session and click Deploy Agent.

Session Name ADD_HOST_SYSMAN_Apr_20_2016_6:32:38_PM_CEST

Deployment Type Fresh Agent Install

OMS Host freo1124.essilor.fr

OMS Upload Port 4903

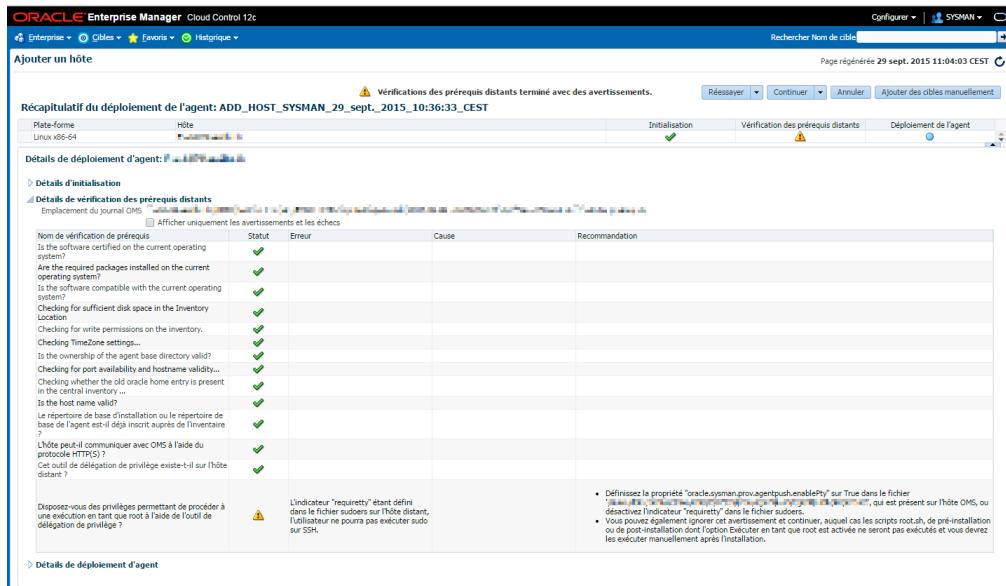
Host Information

Linux x86-64

Hosts	freo1145.essilor.fr
Agent Software Version	12.1.0.4.0
Installation Base Directory	/PDBO/oem12c
Instance Directory	/PDBO/oem12c/agent_inst
Port	3872
Named Credential	NC_FREO1145_2016-04-20-190139:SYSMAN
Privileged Delegation Setting	/usr/bin/sudo -u %RUNAS% %COMMAND%
Preinstallation Script	Not Provided
Postinstallation Script	Not Provided
Additional Parameters	Not Provided

9°) An advice will appear. Save this advice and keep it in your system. You will need this to run the root.sh script later. Then Select the “Continue” Menu and click on “Continue on all hosts”

Example: [/PDBO/oem12c/core/12.1.0.4.0/root.sh](#) is the location of the root.sh script that you will need to run.



10°) Click on the “Done” button.

The screenshot shows the 'Agent Deployment Summary' for the host 'freo1145.essilor.fr'. The summary indicates 'Agent Deployment Succeeded' with a timestamp of 'Apr 20, 2016 6:32:38 PM CEST'. The deployment status table shows 'Initialization' as successful, while 'Remote Prerequisite Check' has a warning icon. Below the summary, the 'Agent Deployment Details' section provides a log location: 'freo1124.essilor.fr:/DBO/kar3/gc_inst/en/EMGC_OMS1/sysman/agentpush/2016-04-20_18-32-38-PM/applogs/freo1145.essilor.fr_deploy.log'. It also includes a table of deployment phases: Installation and Configuration, Secure Agent, Root.sh, Collect Log, and Clean up, all marked as successful.

We will now proceed to the database discovery with the OEM 12c user interface

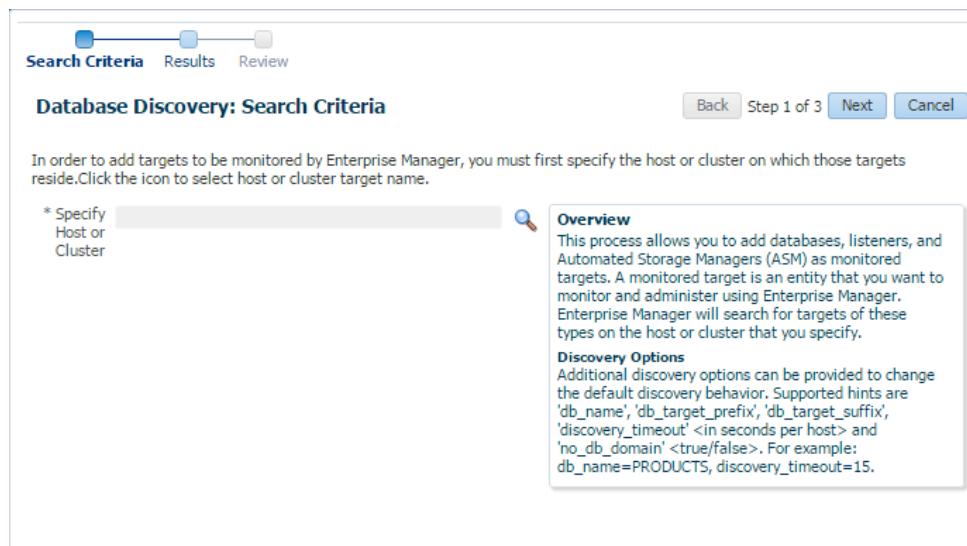
Click on « Enterprise Manager » on this upper side on the screen

The screenshot shows the 'Targets' navigation menu in the Oracle Enterprise Manager. The 'Databases' option is highlighted with a yellow background. Other options like 'Groups', 'Systems', 'Services', and 'Hosts' are also listed.

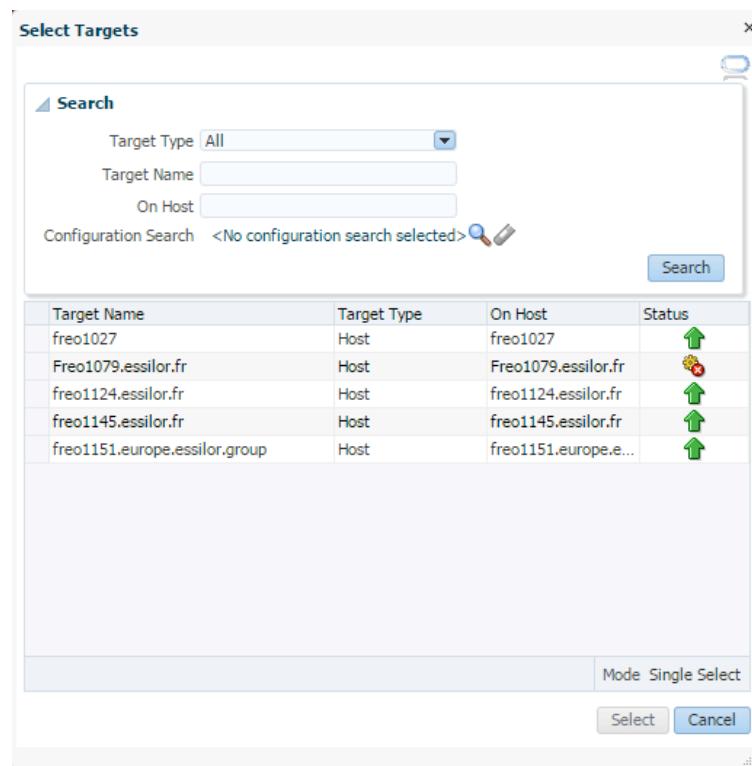
1°) Click on “Target”, “Databases”

The screenshot shows the 'Databases' page in the Oracle Enterprise Manager. The 'Name' column lists 'DIC1_freo1124.essilor.fr', 'DIC2_freo1124.essilor.fr', and 'DUA2_freo1124.essilor.fr'. The 'Type' column indicates they are all 'Database Instances'. The 'Add' button is highlighted with a yellow background.

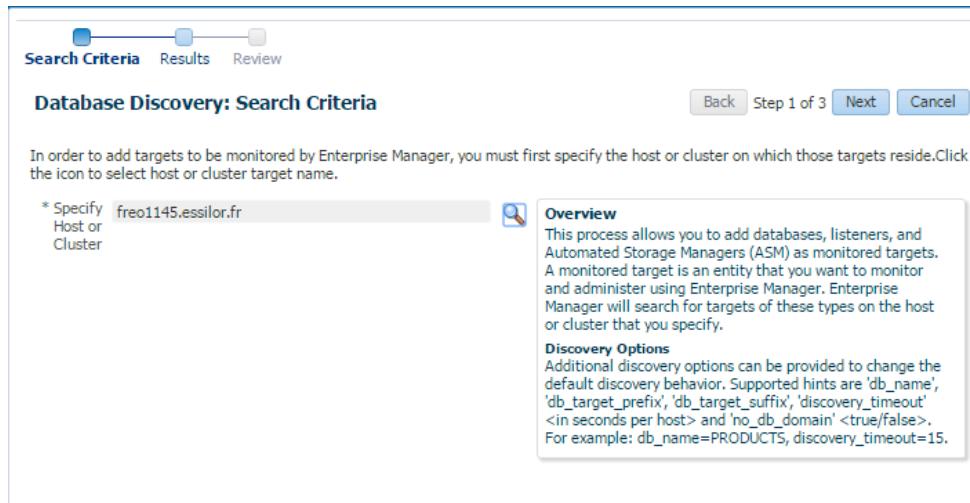
2°) Click on “Add”, “Oracle Database”



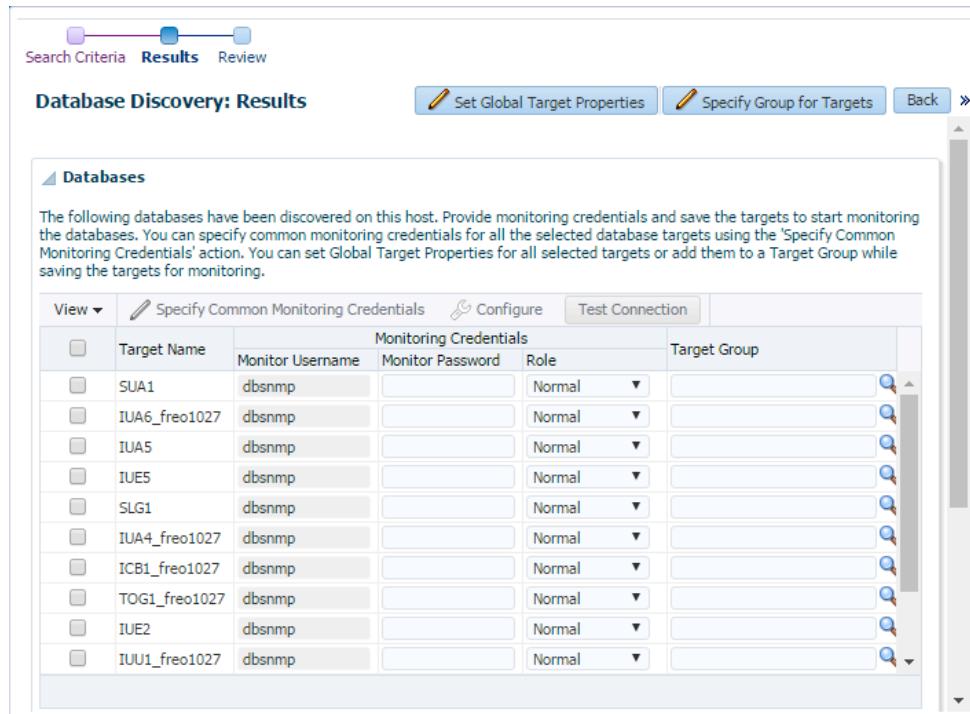
3°) Click on the magnifying glass



4°) Now you just need to select the host server on which you have deployed the agent. The server is normally on the list. Then, click on the "Select" Button.



5°) Check if you have selected the right host and proceed by clicking on the “Select” button.



6°) You need to configure the Database connection you want to add. To do so, in the “view” section, check the box corresponding to the database you are interested in. The “Configure” Button will enable. Click on it.

Configure Database Instance

General

Target Name	SUA1
Target Type	Database Instance
Database System	SUA1_sys
View ▾	
Test Connection	
Name	Value
Monitor Username	dbsnmp
Monitor Password	
Role	Normal ▾
Listener Machine Name	freo1027
Oracle Home Path	/SUA1/ker1/sua1db/11.2.0
Port	1521
Preferred Connect String	Enter the connection string that OMS should use when connecting to the target database. If blank, the OMS would automatically construct one using the host, port, SID provided above.
Database SID	SUA1

[Save](#)

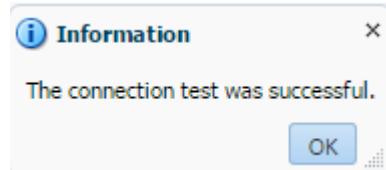
You need to enter the following information:

Monitor password:

Port:

You have to check what password and port number to enter

Then, TEST the connection by clicking on the « test » button



The following message will appear. It means that you have added correctly your database to OEM.

Search Criteria [Results](#) [Review](#)

Database Discovery: Results

[Set Global Target Properties](#) [Specify Group for Targets](#) [Back](#) Step 2 of 3 [Next](#) [Cancel](#)

[Databases](#)

The following databases have been discovered on this host. Provide monitoring credentials and save the targets to start monitoring the databases. You can specify common monitoring credentials for all the selected database targets using the "Specify Common Monitoring Credentials" action. You can set Global Target Properties for all selected targets or add them to a Target Group while saving the targets for monitoring.

<input type="checkbox"/>	Target Name	Monitoring Credentials	Target Group
<input checked="" type="checkbox"/>	PUU1	dbsnmp	*****

Click on « Next »

Search Criteria Results Review

Database Discovery: Review

Please review the targets below and click on 'Save' to start monitoring the targets.

Database Systems

Following Database systems will be created for the discovered databases and related targets.

Target Name	Target Type	Host
PUU1_sys	Database System	
PUU1	Database Instance	freo1145.essilor.fr

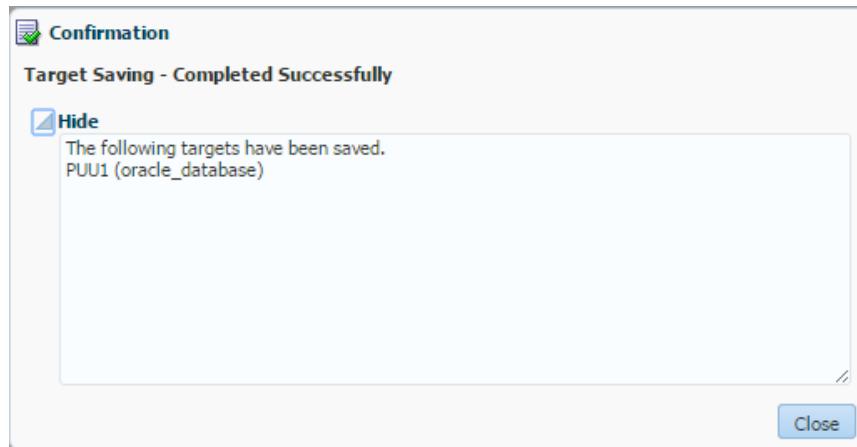
Other Targets

Following targets will not be part of any database system

Target Name	Target Type	Host
No data to display		

Back Step 3 of 3 Next Save Cancel

Click on « Save »



Click on « Close »

Starting - Stopping the Agent

1°) You need to enter the following exports:

```
export AGENT_HOME=/IDBO/oem/core/12.1.0.4.0
export ORACLE_HOME=/IDBO/oem/core/12.1.0.4.0
export PATH=$ORACLE_HOME/bin:$PATH
```

2°) Enter the following command line to **START** the agent:

emctl start agent

Expected answer: *"Agent is Running and Ready"*

Enter the following command line to **STOP** the agent:

emctl stop agent

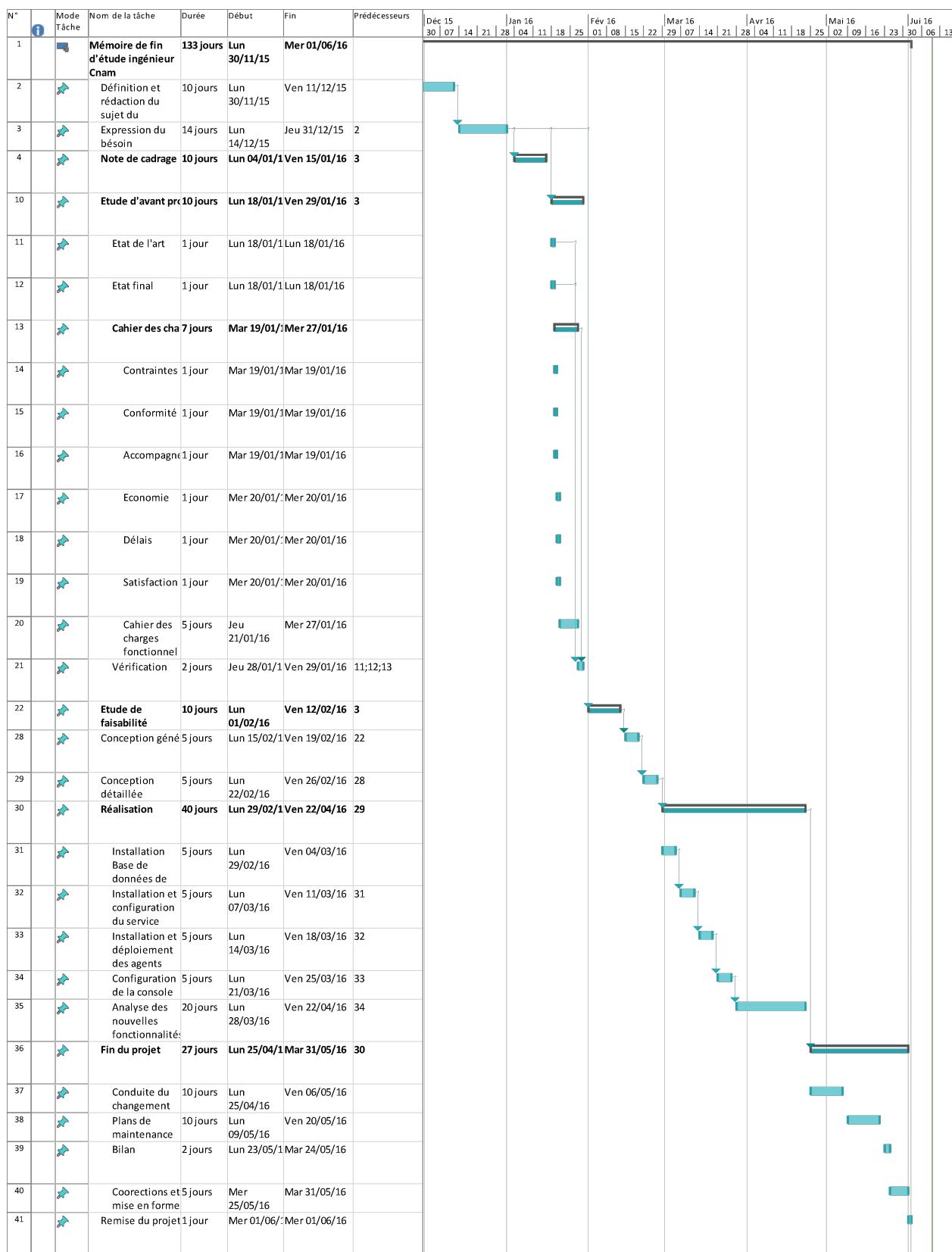
Expected answer: *"Agent is not Running"*

3°) Check the status the agent:

emctl status agent

Expected answer: *"Agent is Running and Ready"*

IV Planning prévisionnel



Implémentation et exploitation d'Oracle Enterprise Manager CC v12c

L'équipe DBA d'Essilor France dont je fais partie est chargée d'administrer plus d'une trentaine de bases de données Oracle. Afin de maintenir nos différents environnements informatiques de façon efficace, nous avons besoin d'un logiciel de supervision sophistiqué pouvant à la fois détecter et signaler rapidement tout comportement anormal de nos bases de données. Oracle Enterprise Manager est la solution logicielle que notre équipe a adoptée pour des raisons de fiabilité, de maintenabilité et flexibilité.

Dans ce mémoire nous exposerons les principales étapes qui nous ont permis de déployer et d'exploiter la nouvelle version d'OEM Cloud Control :

- Identification des choix d'architectures logiciels les plus adaptés à Essilor
- Identification des prérequis propres à la nouvelle version
- Installation et configuration de la base de données Repository pour OEM 12c
- Installation de Cloud Control et de ses fonctionnalités avancées
- Configuration des méthodes de notification, de seuils d'alertes et des règles d'incident

Installing and exploiting Oracle Enterprise Manager CC v12c

The Essilor DBA team I am part of can be tasked with the administration and management of hundreds of systems. In order to maintain our databases and to be quickly and efficiently alerted in the event of a problem, sophisticated tools must be deployed. We have chosen to deploy Oracle Enterprise Manager Cloud Control 12c to supervise our environment because it is a scalable and reliable solution that has proven its worth for almost ten years from now.

This memoire will explain how to install and take advantage of the features of OEM Cloud Control 12c. In order to achieve this purpose, the following tasks had to be performed:

- Identification of the CC components topology that suits the best to the Essilor system environments
- Identification of Cloud Control special prerequisites
- Installation and configuration of the Repository database for OEM 12c
- Installation of Cloud Control along with its advanced functionalities
- Configuration of notification methods, alert thresholds and incident rules