**Document d’exploitation (DEX) « Application »**

|  |  |
| --- | --- |
| **VALIDATION DU DOCUMENT** | |
| Rédacteur(s) | Philippe Nakache |
| Validateur(s) | Exploitation Serveur |
| Approbateur(s) |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **HISTORIQUE DU DOCUMENT** | | | |
| Version | Date | Rédacteur(s) | Commentaires |
| 0.1 | 15/11/2021 | P.Nakache | Initialisation du document |

**Table des matières**

[1 Lecture du document 5](#_Toc61444602)

[1.1 Glossaire 5](#_Toc61444603)

[1.2 Conventions d’écriture 6](#_Toc61444604)

[2 Description de l’application 6](#_Toc61444605)

[2.1 Historique des versions déployées 6](#_Toc61444606)

[2.2 Finalité de l’application 6](#_Toc61444607)

[2.3 Communication avec d’autres applications 6](#_Toc61444608)

[2.4 Échanges de données 6](#_Toc61444609)

[2.4.1 Schéma des flux 7](#_Toc61444610)

[2.4.2 Liste des flux d’échange 7](#_Toc61444611)

[2.5 Acteurs principaux 8](#_Toc61444612)

[2.6 Synoptique et Architecture technique 8](#_Toc61444613)

[2.6.1 Synoptique 8](#_Toc61444614)

[2.6.2 Architecture technique 9](#_Toc61444615)

[2.6.3 Description détaillée des serveurs 9](#_Toc61444616)

[2.7 Stockage 9](#_Toc61444617)

[2.7.1 Liste des disques 9](#_Toc61444618)

[2.7.2 Configuration des VG et FS 9](#_Toc61444619)

[2.8 Politique de sauvegarde 10](#_Toc61444620)

[2.9 Environnements applicatifs 11](#_Toc61444621)

[2.9.1 Offres de service souscrites 11](#_Toc61444622)

[2.9.2 Environnements 11](#_Toc61444623)

[2.10 Gestion des certificats 12](#_Toc61444624)

[3 Procédures d’exploitation 12](#_Toc61444625)

[3.1 Plan batch 12](#_Toc61444626)

[3.2 Liste des procédures d’exploitation 12](#_Toc61444627)

[3.3 Ré Installation 12](#_Toc61444628)

[3.4 Plan de Reprise d’Activité (PRA) 13](#_Toc61444629)

[3.5 Interventions particulières 13](#_Toc61444630)

[3.5.1 Intervention particulière n°1 13](#_Toc61444631)

[3.5.2 Intervention particulière n°2 14](#_Toc61444632)

[4 Comptes & Sécurité 15](#_Toc61444633)

[4.1 Authentification 15](#_Toc61444634)

[5 Supervision 15](#_Toc61444635)

[5.1 Accès aux logs 15](#_Toc61444636)

[5.2 Outils de supervision 16](#_Toc61444637)

[5.3 Seuils et alertes 16](#_Toc61444638)

[6 Reprise sur incidents 16](#_Toc61444639)

[6.1 Type d’incident n°1 16](#_Toc61444640)

[6.2 Type d’incident n°2 17](#_Toc61444641)

[7 Reportings 17](#_Toc61444642)

[7.1 Reporting n°1 18](#_Toc61444643)

[7.2 Reporting n°2 18](#_Toc61444644)

[8 Annexes 18](#_Toc61444645)

**RÉDACTEUR ou SOURCE DE CHAQUE CHAPITRE .**

|  | **Chapitre** | **Rédacteur / Source** |
| --- | --- | --- |
| 1.2 | Convention d’écriture | POA |
| 2.1 | Historique des versions déployées | POA |
| 2.2 | Finalité de l’application | POA |
| 2.3 | Communication avec d’autres applications | POA |
| 2.4 | Échanges de données (Flux) | POA |
| 2.5 | Acteurs principaux | POA |
| 2.6.1 | Synoptique | DAT |
| 2.6.2 | Architecture technique | DAT |
| 2.6.3 | Description détaillée des serveurs | DIU + DAT |
| 2.7.1 | Liste des disques | MDS Stockage + DAT |
| 2.7.2 | Configuration des VG et FS | DAT pour les FS |
| 2.8 | Politique de sauvegarde | MDS Sauvegarde + DAT |
| 2.9.1 | Offres de service souscrites | MDS Sauvegarde + DAT |
| 2.9.2 | Environnements (un chapitre par environnement) | DIU + DAT |
| 2.10 | Gestion des certificats | POA + DAT |
| 3.1 | Plan batch | EBO |
| 3.2 | Arrêt de l’application | POA |
| 3.3 | Relance de l’application | POA |
| 3.4 | Test de fonctionnement | POA |
| 3.5 | Activation du mode maintenance | POA |
| 3.6 | Désactivation du mode maintenance | POA |
| 3.7 | Sauvegarde | POA |
| 3.8 | Restauration | POA |
| 3.9 | Purge des fichiers | POA |
| 3.10 | Changement d’heure | POA |
| 3.11 | Montée de version applicative standard | POA |
| 3.12 | Copie d’environnement (refresh) | POA |
| 3.13 | Ré Installation | POA |
| 3.14 | Plan de Reprise d’Activité (PRA) | POA |
| 3.15.1 | Intervention particulière n°1 | POA |
| 3.15.2 | Intervention particulière n°2 | POA |
| 4.1 | Comptes techniques | POA |
| 4.2 | Comptes applicatifs | POA |
| 5.1 | Accès aux logs | POA |
| 5.2 | Outils de supervision | POA |
| 5.3 | Seuils et alertes | SDS |
| 6 | Reprise sur incidents | POA |
| 6.1 | Type d’incident n°1 | POA |
| 6.2 | Type d’incident n°2 | POA |
| 7.1 | Reporting n°1 | POA |
| 7.2 | Reporting n°2 | POA |
| 8 | Annexes | POA |

# Lecture du document

Éléments de compréhension nécessaires pour la lecture du document

## Glossaire

Vocabulaire utilisé au sein du document

| **Terme / Sigle** | **Définition** |
| --- | --- |
| SI | Système d’Information, il s’agit d’un ensemble organisé de ressources (matériels, logiciels, personnel, données et procédures) qui permet de regrouper, de classifier, de traiter et de diffuser de l’information |
| DEX | Document d’Exploitation, il contient l’ensemble des informations et des procédures nécessaires pour exploiter l’application |
| ISD / DAT | Infrastructure Solution Design (ou Dossier d’Architecture Technique), il définit et justifie les hypothèses techniques structurant la solution. Il présente généralement l’architecture fonctionnelle (utilisateurs, traitements, données) et l’architecture technique (serveurs, postes de travail, réseau). |
| DIU | Dossier d’Infrastructure Unifié, il s’agit du document récapitulant la liste des serveurs d’un SI établi par l’expertise sur la base de l’ISD / DAT |
| MDS Stockage | Document portant les caractéristiques techniques du stockage nécessaire à l’installation des machines |
| MDS Sauvegarde | Document portant les caractéristiques techniques de la politique de sauvegarde à mettre en place |
| Configuration de référence (CMDB) | Document établi durant le design de la solution, récapitulant l’ensemble des caractéristiques techniques des machines à déployer au sein des différents environnements |
| EBO | Expression de Besoin Ordonnancement, document listant l’ensemble des traitements automatisés dans l’outil d’ordonnancement VTOM |
| PTI | Procédure Technique d’Installation, document récapitulant l’ensemble des gestes à réaliser pour une installation d’un composant ou d’une application entière. Elle peut être générique (pour les souches / masters maintenus par les experts ENGIE IT) ou spécifique (installation et configuration d’une application entière) |
| DRP / PRA | Disaster Recovery Plan, ou Plan de Reprise d’Activité, |
| PTR | Procédure Technique de Reprise, document listant l’ensemble des gestes pour réaliser un DRP / PRA |
| REX | Retour d’Expérience, dans le contexte de l’exploitation, document décrivant la résolution des incidents (root cause, gestes correctifs) permettant de résoudre les futures occurrences des incidents de même type |

## Conventions d’écriture

Conventions d’écriture présentes dans le document :

|  |  |
| --- | --- |
| **Style** | **Explication** |
|  |  |
|  |  |
|  |  |

Signification du nom des environnements :

|  |  |
| --- | --- |
| **Intitulé** | **Type d’environnement** |
|  |  |
|  |  |
|  |  |

# Description de l’application

## Historique des versions déployées

Liste des Mises En Production (MEP) majeures et mineures réalisées pour l’application

|  |  |  |
| --- | --- | --- |
| **Version** | **Date de MEP** | **Contenu de la version** |
| N/A | N/A | N/A |
|  |  |  |
|  |  |  |

## Finalité de l’application

Ansible est à la fois un outil d’automatisation (*control node*) et un langage d’automatisation (*playbook*).

Il permet de décrire les opérations (*tasks*) que l’on souhaite exécuter sur un ou plusieurs serveurs (Linux ou Windows, physiques ou virtuels, équipement réseau…) ou sur une API.

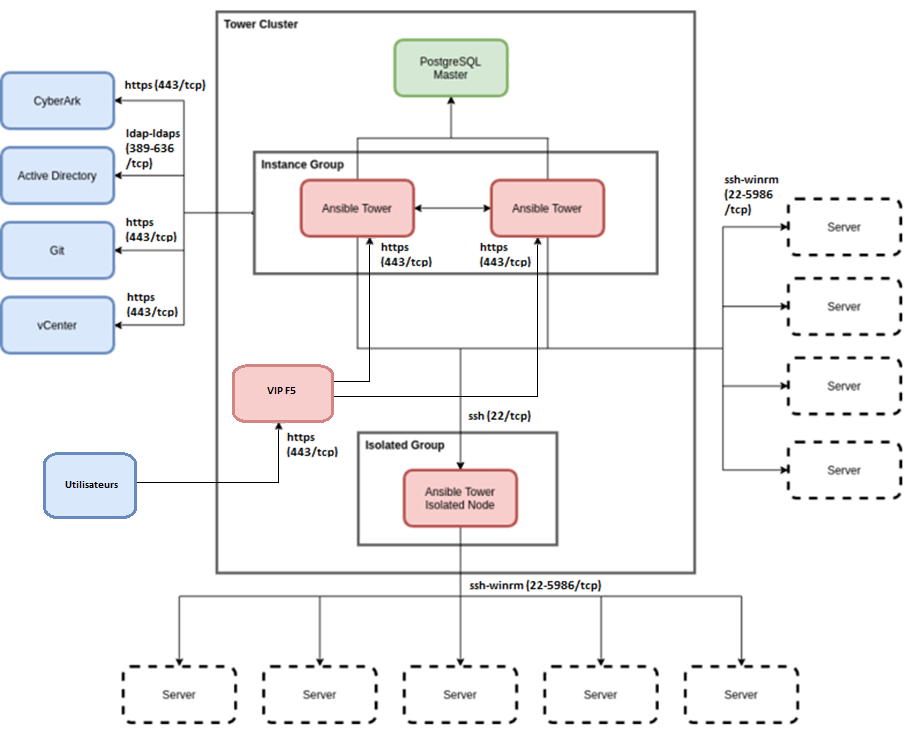
## Communication avec d’autres applications

Applications échangeant des informations avec l’application décrite dans ce DEX

|  |  |
| --- | --- |
| **Application** | **Description** |
| VRA | Opération de post provisioning et de déploiement |
| PAM | Création de coffre |
| Satellite | Enregistrement de la VM dans le serveur Satellite |
| AD | Création de l’OU et de la VM |
| GITLAB | Source control des roles ansible |
| Vcenter | Gestion de l’inventaire Vmware |

## Échanges de données

### Schéma des flux



### Liste des flux d’échange

| Source(s) | IP(s) Source | Destination(s) | IP(s) Destination | Protocole(s) | Motif |
| --- | --- | --- | --- | --- | --- |
| vlp1tow01.dc.infra-grdf.com  vlp1tow02.dc.infra-grdf.com | 10.40.9.37  10.40.9.38 | vlp1tow03.dc.infra-grdf.com | 10.40.9.39 | 5432/TCP, UDP | Accès à la base de données PGSQL de production |
| vlp1tow01.dc.infra-grdf.com  vlp1tow02.dc.infra-grdf.com | 10.40.9.37  10.40.9.38 | rhsat.dc.infra-grdf.com  vlp1rhs02.dc.infra-grdf.com | 10.236.197.160  10.40.9.64 | 443/TCP | Permet de récupérer les souscriptions «  Red Hat Ansible Automation » |
| vlp1tow01.dc.infra-grdf.com  vlp1tow02.dc.infra-grdf.com | 10.40.9.37  10.40.9.38 | AREA ADMIN  AREA INTERNE PROD  AREA INTERNE PROD  AREA INTERNE HML  AREA INTERNE HML  AREA INTERNE CCPT  AREA INTERNE CCPT  AREA INTERNE ST  AREA EXTERNE PROD  AREA EXTERNE HML  AREA EXTERNE ST  S4 groupe 1  S4 groupe 2 | 10.40.0.0/20  10.40.16.0/20  10.40.32.0/19  10.40.64.0/19  10.40.96.0/20  10.40.112.0/20  10.40.128.0/20  10.40.144.0/20  10.40.160.0/19  10.40.192.0/19  10.40.240.0/20  10.146.0/16  10.236.0/16 | 22/TCP  5986/TCP | Accès aux serveurs Linux (SSH) et Windows (WinRM) PGDC et S4 |
| vlp1tow01.dc.infra-grdf.com  vlp1tow02.dc.infra-grdf.com | 10.40.9.37  10.40.9.38 | vxh1vce01.dc.infra-grdf.com  vxp1vce02.dc.infra-grdf.com  vxp1vce03.dc.infra-grdf.com | 10.40.4.134  10.40.4.135  10.40.4.136 | 443/TCP | Génération des inventaires dynamiques sur les Vcenter d’administration, de production/homologation et de conception/innovation |
| vlp1tow01.dc.infra-grdf.com  vlp1tow02.dc.infra-grdf.com | 10.40.9.37  10.40.9.38 | chef-gitlab.grdf.net  vlp1scm01.dc.infra-grdf.com | 10.236.22.145  10.40.150.10 | 443/TCP | Permet de synchroniser les projets Gitlab |
| vlp1tow01.dc.infra-grdf.com  vlp1tow02.dc.infra-grdf.com | 10.40.9.37  10.40.9.38 | nova.infra-grdf.com | 10.236.13.11  10.236.13.12  10.236.13.13  10.236.13.14  10.236.13.69  10.236.13.70  10.236.13.71  10.236.13.72 | 389/TCP + UDP | Permet l’authentification des utilisateurs présents dans l’annuaire LDAP |
| vlp1tow01.dc.infra-grdf.com  vlp1tow02.dc.infra-grdf.com | 10.40.9.37  10.40.9.38 | mailapp.grdf.net | 10.236.30.11 | 25/TCP | Envoi de mail via SMTP (notification, reporting) |
| vxp1vau03.dc.infra-grdf.com | 10.40.9.25 | adam-homol.grdf.net | <IP> | 443/TCP | Permet d’exécuter des requêtes API pour piloter Tower |
| Accès utilisateur (Jump) | - | adam-homol.grdf.net | <IP> | 443/TCP | Permet aux utilisateurs de se connecter aux Web UI de Tower |

## Acteurs principaux

Les interlocuteurs suivants (personnes et/ou équipes) sont les principaux contributeurs de l’exploitation de l’application :

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Acteur** | **Entité** | **Fonction** | **Téléphone** | **BAL** |
| Equipe | POI Serveur | Exploitation Système | N/A | exploit\_serveur@grdf.fr |
| Equipe | AES Linux | Ingénierie Système | N/A | GRDF-DSI-ING-ExpertiseLinux  GRDF-DSI-ING-ExpertiseWindows |

RACI

<https://grdf.sharepoint.com/:x:/r/teams/Domaine_Ingenierie/Architecture%20et%20Expertise%20Systme/Regles%20d%27ingenieries/Ansible/RACI_Ansible.xlsx?d=w736a442f3cb14549a41f73d9a34d6102&csf=1&web=1&e=C3NxhB>

## Synoptique et Architecture technique

### Synoptique

Ce schéma technico-fonctionnel présente les composants applicatifs au sein du SI, leur répartition sur les différentes zones réseaux et les liens entre les composants.

Ces informations sont à récupérer dans l’ISD / DAT établi et validé en phase DESIGN du projet.

<https://grdf.sharepoint.com/:w:/r/teams/Domaine_Ingenierie/Architecture%20et%20Expertise%20Systme/Projets/Commun/Ansible/GRDF%20-%20Dossier%20d%27architecture%20Ansible%20Tower-GL109UXA.docx?d=wf2a92171675448fd933b460d25297bc1&csf=1&web=1&e=B0DezT>

Fonction des différents composants présentés dans le schéma technico-fonctionnel :

| Terme / composant | Description |
| --- | --- |
| Ansible Playbooks | Fichiers YAML dans lesquels sont mentionnés toutes les tâches qu'Ansible doit exécuter |
| Ansible CLI | L’outil en ligne de commande qui permet d’exécuter du code Ansible sans Tower |
| Web UI | Interface Web simple permettant de piloter l’ensemble de l’infrastructure gérée par Tower, d’exécuter des Job template et d’avoir une vue globale |
| Tower API | Inclut un service API RESTful qui permet aux administrateurs système et aux développeurs d'écrire des scripts et applications de tierce-partie personnalisés pouvant interagir avec Ansible Tower. |
| Inventory | Statique ou dynamique permettant de lister/classer les hosts sur lesquels ansible interviendra |
| Credential | Les credentials sont utilisés par Ansible Tower pour se connecter aux différentes sources extérieures. |
| Project | Les projects sont une collection logique de playbooks qu’utilisent Ansible Tower. Ils représentent généralement les repository SCM (Gitlab, Subversion, etc…) contenant les playbooks attenant au job\_template |
| Job Template | Ils permettent aux playbooks d’être contrôler, déléguer et d’être scalable en termes d’organisation.  Ils nécessitent un inventaire, un credential pour se connecter aux VM et un project (SCM ou local) dans lequel seront stockés les playbooks |
| Workflows | Possibilité de lancer un séquencement de playbooks pour aboutir in fine aux actions désirées |
| RBAC | RBAC (Role Based Access Control) permet de gérer les permissions des utilisateurs sur les objets Tower (Inventory, Credential, Projects, Job Templates …) |
| Centralisation des logs | Les logs d’exécution de Ansible Tower peuvent être centralisés sur un puit de log (splunk, logstash, etc...) |
| Modules | Bouts de codes écrits principalement en python pour modifier l’état de propriété d’un host. Les modules sont invoqués par l’exécution de taches soit directement en ligne de commande soit via des playbooks |
| Plugins | Les Plugins apportent des fonctionnalités complémentaires à Ansible (become ; action ; …) |

### Architecture technique

Ce schéma présente les composants techniques au sein du SI (machines physiques et virtuelles, équipements réseau) et leur répartition sur les différentes zones réseau.

Ces informations sont à récupérer dans l’ISD / DAT établi et validé en phase DESIGN du projet.

<https://grdf.sharepoint.com/:w:/r/teams/Domaine_Ingenierie/Architecture%20et%20Expertise%20Systme/Architectures/DATs/ANSIBLE/GRDF%20-%20Dossier%20d%27architecture%20Ansible%20Tower.docx?d=wff5364ffb2e74acab892e1ac4d126438&csf=1&web=1&e=ihwsgo>

### Description détaillée des serveurs

| Environnement | Nom du serveur | Fonction | CPU | Mémoire | Stockage | VLAN | Adresse IP |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Homologation | vlh1tow01.dc.infra-grdf.com | Nœud Tower | 4 | 8 | 50 | Front-3056 | 10.40.11.37 |
| Homologation | vlh1tow02.in.grdf.net | Nœud Tower | 4 | 8 | 50 | Front-3056 | 10.40.11.38 |
| Homologation | vlh1tow03.in.grdf.net | BDD | 4 | 8 | 100 | Front-3056 | 10.40.11.39 |
| Production | vlp1tow01.in.grdf.net | Nœud Tower | 4 | 8 | 50 | Front-3050 | 10.40.9.37 |
| Production | vlp1tow02.in.grdf.net | Nœud Tower | 4 | 8 | 50 | Front-3050 | 10.40.9.38 |
| Production | vlp1tow03.in.grdf.net | BDD | 4 | 8 | 100 | Front-3050 | 10.40.9.39 |

## Stockage

### Liste des disques

<https://grdf.sharepoint.com/:x:/r/teams/sitdoc-grdf/DIO/Documents%20partages/1-Domaine%20Ing%C3%A9nierie/Expertise%20Infra%20Serveurs/Projets/Satellite/DDS_SATELITE.xlsx?d=w48946010155a4c389ce84474d022a527&csf=1&web=1&e=AZhfWu>

|  |  |  |
| --- | --- | --- |
| Hostname | Adresse IP | Provisionné MB |

|  |  |  |
| --- | --- | --- |
| vlh1tow01.in.grdf.net | 10.40.11.37 | 100 Go |
| vlh1tow02.in.grdf.net | 10.40.11.38 | 100 Go |
| vlh1tow03.in.grdf.net | 10.40.11.39 | 100 Go |
| vlp1tow01.in.grdf.net | 10.40.9.37 | 100 Go |
| vlp1tow02.in.grdf.net | 10.40.9.38 | 100 Go |
| vlp1tow03.in.grdf.net | 10.40.9.39 | 100 Go |

## Politique de sauvegarde

<https://grdf.sharepoint.com/:w:/r/teams/Domaine_Ingenierie/Architecture%20et%20Expertise%20Systme/Architectures/DATs/ANSIBLE/GRDF%20-%20Dossier%20d%27architecture%20Ansible%20Tower.docx?d=wff5364ffb2e74acab892e1ac4d126438&csf=1&web=1&e=bNXhpw>

Deux types de sauvegardes sont mises en place.

### Via Hyperviseur

Comme toutes les VMs RHEL chez GRDF, une sauvegarde régulière est effectuée en utilisant la technologie Commvault.

Cette sauvegarde a l'avantage de travailler au niveau "macro" et de sauvegarder l'intégralité pour une reprise rapide sur incident. En revanche, il n'assure pas la cohérence des données.

Il faudrait arrêter les services de l'outil Tower (Nœuds + Base de données) durant une plage horaire et effectuer les sauvegardes (Nœuds + Base de données) durant cette plage pour éviter tout problème de cohérence des données. Pour cela, les fichiers de sauvegarde logicielle (détaillée ci-après) pourront être récupérés avec les outils Commvault et utilisés en cas de restauration Tower.

L’agent Commvault n’est pas nécessaire à la mise en place de cette sauvegarde.

### Logicielle

Une seconde sauvegarde doit être effectuée via l’outil mis à disposition de Tower.

Cet outil permet d'effectuer des sauvegardes full. Il intègre l’arrêt des services (Nœuds + Base de données), la sauvegarde de tous les éléments Tower puis le redémarrage des services.

Il est exécuté via un script planifié (cron) sur l’un des nœuds Tower. Son exécution est quotidienne et prévoit la conservation des 10 dernières sauvegardes. Le script utilisé est disponible dans GitLab et déployé via le Role Ansible role\_tower\_config.

Ces backups seront utilisés dans le cas de reprise sur un incident pour la reconstruction d'un cluster Tower complet (Nœuds + Base de données) à H-24 maximum pour la sauvegarde la plus récente et J-10 pour la plus ancienne.

Cette sauvegarde est exécutée sur chaque cluster Tower (Homologation et Production). Ces sauvegardes n’ont pas besoin d’être externalisées.

## Environnements applicatifs

### Offres de service souscrites

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Environnement** | **PRD300** | **PRD301** | **PRD302** | **PRD303** | **PRD304** | **PRD305** | **PRD306** | **PRD307** | **PRD310** | **Cloud** |
| Nom envt. | Oui/Non | Oui/Non | Oui/Non | Oui/Non | Oui/Non | Oui/Non | Oui/Non | Oui/Non | Oui/Non | Oui/Non |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |

N/A

### Environnements

#### Environnement n°1 (Production)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **PRODUCTION** | | | | |
| Hostname | Physique ou Virtuel | Liste des bases de données | Liste des MW au catalogue GRDF | Liste des MW hors catalogue GRDF |
| vlp1tow01.in.grdf.net | Virtuel | N/A | Ansible | N/A |
| vlp1tow02.in.grdf.net | Virtuel | N/A | Ansible | N/A |
| vlp1tow03.in.grdf.net | Virtuel | Postgres | N/A | N/A |

#### Environnement n°2 (Développement)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Developpement** | | | | |
| **Serveur** | **Type** | **Bases de données** | **Middlewares au catalogue ENGIE IT** | **Autres middlewares** |
| Hostname | Physique ou Virtuel | Liste des bases de données | Liste des MW au catalogue GRDF | Liste des MW hors catalogue GRDF |
| vlh1tow01.in.grdf.net | Virtuel | N/A | Ansible | N/A |
| vlh1tow02.in.grdf.net | Virtuel | N/A | Ansible | N/A |
| vlh1tow03.in.grdf.net | Virtuel | Postgres | N/A | N/A |

Le détail des caractéristiques techniques de chaque serveur est présent dans le DIU fourni au paragraphe « 2.6.3 Description des serveurs »

## Gestion des certificats

Le certificat n’est pas un auto-signé et est délivré et validé par la chaine de certification GRDF.

Fin de la date des certificats : 31/08/2023

AES sera en charge de veiller à l’expiration de la date des certificats.

# Procédures d’exploitation

## Plan batch

Tower gère ses propres plan batch d’execution.

**N/A**

## Liste des procédures d’exploitation

Ci-joint les PTE regroupant ces thèmes :

* Création d’un job template
* Création d’un projet
* Création d’un inventaire
* Création d’un utilisateur

## Plan de Reprise d’Activité (PRA)

Les serveurs Ansible Tower s’inscrivent dans le plan de continuité informatique par le socle de virtualisation VMware.

### Sinistre local (SL)

En cas d’incident sur l’un des nœuds Tower, la continuité informatique est garantie par la fonctionnalité « HA » de Tower. L’autre nœud (ou les autres nœuds dans le cas d’une extension du cluster dans le futur) gèrera-ont l’ensemble des accès des utilisateurs (Web UI ou API) jusqu’à la remise en fonction du nœud faisant défaut. La configuration de la VIP de chaque cluster Tower permet de détecter une erreur de communication avec les nœuds pour désactiver le(s) nœud(s) en erreur.

En cas d’incident sur la base de données Tower, une restauration de la VM Tower (Via Hyperviseur) devra être réalisée, et également, si besoin une restauration de la base de données. Ce type d’incident provoquera forcément une perte de service pouvant aller à plusieurs heures.

### Sinistre majeur (SM)

En cas de perte d’un hyperviseur, les mécanismes de haute disponibilité VMware se chargent automatiquement de la continuité de services des VMs Tower sur un autre hyperviseur.

Hébergées par le POD VMware d’Admin, les VMs Tower sont exécutées par défaut sur le site E3. En cas de la perte de ce site, les mécanismes de haute disponibilité VMware se chargent automatiquement de la continuité de services des VMs Tower sur le site distant (E4).

## Interventions particulières

Liste des opérations complémentaires nécessaires à l’exploitation de l’application. Il s’agit des interventions relatives aux spécificités de l’application du client.

**N/A**

# Comptes & Sécurité

Les accès sont génériques et donnent droits à certains privilèges en fonction des utilisateurs génériques. Cela nécessitera la création dans l’AD de ces comptes génériques

|  |  |  |
| --- | --- | --- |
| Profile | Offre | Description |
| ingsys | Prod et homologation | Profil de connexion pour gérer entièrement la plateforme |
| explsys | Prod | Profil de connexion à la plateforme de gestion pour créer et exécuter des jobs templates |
| CT « ida » | Prod | Profil de connexion à la plateforme de gestion lié aux **conduites techniques** pour créer et exécuter des jobs templates sur des inventaires VM en homol et prod |
| DA  « ida » | Prod | Profil de connexion à la plateforme de gestion lié aux **domaines applicatifs** pour créer et exécuter des jobs templates sur des inventaires VM en conception en build |

## Authentification

L’authentification permet de valider l'identité d'une personne ou d'un ordinateur afin d'autoriser l'accès de cette entité à des ressources (systèmes, réseaux, applications). Cette phase intervient après la phase dite d'identification.

|  |  |  |
| --- | --- | --- |
| Utilisateurs | Type accés | Authentification |
| INTERNE | En lecture / écriture | local |
| EXTERNE | Non |  |

**Gestion des mots de passe :**

*Il n’existe pas de gestion de mots de passe (pas de rotation)*

|  |  |
| --- | --- |
| Utilisateurs | |
| Qui peut changer le mot de passe ? | Utilisateur |
| Changement du mot de passe à la première connexion | Non |
| Est-ce une obligation du produit ? | Non |
| Obligation de changer le mot de passe tous les | N/A |
| Dictionnaire des mots de passe interdits | Non |
| Conservation historique des derniers mots de passe | Non |
| Mots de passe stockés chiffrés dans le référentiel des mots de passe : | Non |

La configuration de la gestion des mots passe est la suivante :

* Longueur minimale : 8 caractères
* 3 critères à respecter parmi : lettres majuscules, lettres minuscules, chiffres, caractères spéciaux
* Validité maximale des mots de passe : 3 mois
* Contrôle sur historique : 3 derniers mots de passe
* Nombre d’essais avant désactivation du compte : 7

# Supervision

## Accès aux logs

Emplacement des logs de l’application :

|  |  |
| --- | --- |
| **Type de logs** | **Accès** |
| Type de logs | Serveur & chemin, lien vers outil ou interface spécifique |
| Logs système | Tous les serveurs : /var/log |
| Logs techniques Tower | Tous les serveurs  /var/log/tower |

## Outils de supervision

Liste des outils de supervision utilisés pour sécuriser l’application.

Standards de supervision GRDF :

Les items systèmes seront supervisés par SNMP

Les items applicatifs seront supervisés par un agent NRPE

En plus des métriques systèmes classiques générales à toutes les VMs chez GRDF, les services suivants sont supervisés. Ceci permet de réagir rapidement lorsqu’un composant principal de Tower est hors service (frontal web, application, base de données).

| ***Fonction Tower*** | ***VM Tower*** | ***Services à superviser*** |
| --- | --- | --- |
| *Nœud Tower* | *vlh1tow01.dc.infra-grdf.com*  *vlh1tow02.dc.infra-grdf.com*  *vlp1tow01.dc.infra-grdf.com*  *vlp1tow02.dc.infra-grdf.com* | *ansible-tower.service*  *nginx.service*  *redis.service*  *supervisord.service* |
| *Base de données Tower* | *vlh1tow03.dc.infra-grdf.com*  *vlp1tow03.dc.infra-grdf.com* | *postgresql.service* |
|  | *VIP* | [*https://adam.grdf.net*](https://adam.grdf.net)  *https://adam-homol.grdf.net* |

## Seuils et alertes

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Elément  Supervisé | Warning | Critical | Frequency | Alert Threshold | Paramètres | Astreinte EXP | Remarques |
| ICMP  (Ping) | N/A | Ping KO | 1 min | 3 |  |  |  |
| CPU idle | 30% | 5% | 3 min | 5 |  |  |  |
| CPU steal time | 10% | 40% | 5 min | 6 |  |  |  |
| Load average 15 / nb CPUs | 0.7 | 3 | 5 min | 3 |  |  | Le load average 15 correspond à la commande uptime et au 3eme champ du résultat du load average |
| Used Memory | 70% | 90% | 5 min | 3 |  |  |  |
| FS disk space - System | 80% | 95% | 5 min | 6 | /, /var/log, /var/log/audit, /opt,  /boot, /root, /tmp  /var/tmp, /home |  |  |
| FS disk space - Appli | 80% | 95% | 6 min | 6 | Tout autre FS |  |  |
| Running Services |  |  | 5 min | 3 | dnsmasq.service, tcsd.service, , crond.service, irqbalance.service, sysstat.service, gssproxy.service, vmtoolsd.service, sshd.service, ntpd.service |  |  |
| Port |  | not opened | 1 min | 5 | ssh | Port |  |

# Reprise sur incidents

Liste des incidents récurrents et des méthodes de reprise documentées.

Cette section est à adapter durant le cycle de vie de l’application, sur la base des REX établis par les équipes d’exploitation

Les incidents liés à l’application seront gérés lors d’une première analyse par les POI en s’appuyant sur les PTE livrées et les connaissances d’administration systèmes (FS Full par exemple) puis éventuellement escaladés à l’expertise.

# Reportings

**N/A**

# Annexes

**N/A**