

Manuel d'installation et d'exploitation

TMA BDRTM web

ONF

Propriétés du document

Référence du document	TMA-BDRTM-2023-MIEX-087-MAG
Edition Révision	1.0
Date d'émission	29/09/2026
Client	ONF
Marché	
Réf. consultation	Ref. Consultation

	Nom	Entité	Date	Visa
Rédaction	Kévork TARAKJIAN	Magellium	21/09/2026	Ok
Vérification	Jonathan LEBEAU	Magellium	29/09/2026	Ok
Approbation	Mannaïg L'HARIDON	Magellium	29/09/2026	Ok

Liste de diffusion

	Nom	Entité	Nb. Exemplaires
Destinataire	ONF	Dossier Client	1 (numérique)
Destinataire			1 (numérique)
Copies internes	Dossier Client	Magellium	1 (numérique)
Copies externes	Sans Objet	Magellium	1 (numérique)

Fiche d'évolution du document

Ed.	Rév.	Date	Objet de l'évolution	Observations
1	0	29/09/2026	Diffusion du rapport	Sans Objet

Ce document est la propriété de Magellium Artal Group.
Il ne peut être ni reproduit, ni communiqué sans autorisation écrite préalable.

Table des matières

Table des matières 3
1 Introduction 5
1.1 Objet du document 5
1.2 Documents associés 5
1.3 Structure globale applicative 5
1.5 Terminologie / Glossaire 7
2 Disponibilité 8
2.1 Ouverture de services 8
2.2 Arrêts planifiés 8
2.3 Gestion des incidents 8
2.4 Gestion des sinistres 8
2.5 Maintenance corrective / Gestion des tickets 8
2.6 Responsabilités / contacts d'exploitation 9
3 Utilisateurs 10
3.1 Configuration des utilisateurs selon l'environnement 10
3.2 Comptes techniques 10
3.3 Habilitations / Rôles applicatifs 10
4 Versions de l'application 12
4.1 Liste des composants logiciels 12
5 Architecture physique 14
5.1 Schéma 14
5.2 Flux avec d'autres SI 15
5.2.1 Flux serveur 15
5.2.2 Flux navigateur 16
5.3 Bases de données 17
5.3.1 Schéma des tables 17
5.3.2 Données 18
5.3.3 Intégrité des données 18
5.3.4 Connexions à la base de données 19
5.4 Les Logs 19
6 Spécifications d'infrastructure 21
6.1 Configuration système 21
6.2 Paramétrage 21
6.2.1 Variables globales 21

Ce document est la propriété de Magellium Artal Group.
Il ne peut être ni reproduit, ni communiqué sans autorisation écrite préalable.

6.2.2 Variables locales à la machine 22
6.2.3 Paramètres par instance (dans bdrtm__instances) 22
6.2.4 Variables d'environnement de l'instance (génèrent le fichier .env) : 22
6.3 HTTPS/Certificats 23
6.4 Spécificités SIG (Map-Server, Map-Proxy) 23
6.5 Sécurité (pare-feu, fail2ban) 23
6.6 Déploiement et maintenance (nouvelle instance, mise à jour, retour arrière) 24
6.7 Sauvegarde et restauration 25
6.8 Copie des environnements (Prod → Recette/Formation) 25
6.9 Surveillance et supervision 26
6.9.1 Métriques système 26
6.9.2 Tâches de fond et interactions SI ONF 26
6.9.3 Métriques applicatives (par instance) 26
7 Procédures et outils d'exploitation 28
7.1 Consignes sur incident 28
7.2 Pose/retrait de la page de maintenance 28
7.3 Arrêt/relance de l'application 28
7.4 Tests de bon fonctionnement 29
7.4.1 Accès général 29
7.4.2 Authentification ONF (Genepi) 29
7.4.3 Synchronisation LDAP 29
7.4.4 Envoi de mail (SMTP) 29
7.4.5 Services cartographiques (MapServer/MapProxy) 29
7.4.6 Métriques applicatives (login, images cartographiques, endpoints JSON/OWS) 30
7.5 Modification des mots de passe 30
7.6 Liens utiles 31

Ce document est la propriété de Magellium Artal Group.
Il ne peut être ni reproduit, ni communiqué sans autorisation écrite préalable.

1 Introduction

1.1 Objet du document

Ce document constitue le Manuel d'installation et d'exploitation (MIEX) de l'application BD-RTM (Base de Données sur les Risques naturels des Terrains en Montagne), une solution cartographique Web connectée à une base de données centralisée, développée et maintenue par Magellium (TMA) pour le compte de l'ONF.

L'application est hébergée sur l'infrastructure de l'ONF pour l'ensemble des environnements officiels (Recette ONF, Recette Mobile ONF, Formation ONF et Production ONF). Magellium conserve en interne ses propres environnements de développement (Développement, Recette et Iso-Prod), utilisés pour ses besoins internes avant livraison à l'ONF.

Il décrit les informations nécessaires à l'exploitation et au maintien en conditions opérationnelles de l'application, à savoir :

- les prérequis en termes d'architecture matérielle et logicielle,
- l'ensemble des composants nécessaires à son fonctionnement,
- les procédures d'installation, de mise à jour et de maintenance,
- les tâches d'exploitation courantes (gestion des données, paramétrage, sauvegarde, supervision).

1.2 Documents associés

L'ensemble de la documentation applicable et de référence au projet BDRTM est décrit dans le document « Liste Documentaire du projet BDRTM » (réf. ONF-BDRTM-LD), qui présente de façon exhaustive la documentation applicable et de référence au projet.

Les spécifications fonctionnelles de la solution sont détaillées dans le CCTP et ses annexes, notamment :

- Annexe 1 « Présentation de la BDRTM » : modèle métier (objets gérés, cartographie, requêteur) ;
- Annexe 2 « Fil conducteur » : guide utilisateur pas-à-pas des principales fonctionnalités;
- Annexe « Composants » : liste des composants logiciels et de leurs versions.

1.3 Structure globale applicative

La BDRTM constitue un système structuré d'information sur les risques naturels en montagne. Il permet aux Agences RTM de répondre aux commandes passées à l'ONF par ses ministères de tutelle. Les premiers événements ont été répertoriés dès la fin des années 1980 ; le suivi des ouvrages de protection a été intégré en 2003, puis celui des terrains domaniaux RTM en 2006.

L'application gère les principaux types d'objets suivants :

Ce document est la propriété de Magellium Artal Group.
Il ne peut être ni reproduit, ni communiqué sans autorisation écrite préalable.

- Sites : zones d'étude d'un phénomène naturel, indépendantes des limites communales (un site « Territoire communal » existe pour chaque commune, pour rattacher les événements non localisés) ;
- Zones d'enjeux : intersections géographiques entre une limite de commune et un site, pouvant être impactées par des événements ;
- Événements : manifestation observée d'un phénomène naturel à une date et un lieu donnés, avec ses caractéristiques et impacts cartographiables ;
- Dispositifs : regroupements d'un ou plusieurs ouvrages sur un site, participant à une stratégie de lutte contre un phénomène ;
- Ouvrages : entités destinées à limiter les effets d'un phénomène naturel, avec un suivi régulier de leur état ;
- Expertises / visites de dispositif : diagnostics d'ensemble sur l'état des ouvrages d'un dispositif ;
- Interventions : actions d'entretien, de correction ou de complément sur un ouvrage ou un dispositif, suivies du stade « proposé » à « réalisé » ;
- Entités de gestion (dont les Divisions Domaniales) : entités administratives de l'ONF assurant la programmation et l'exécution des interventions.

Chaque objet dispose d'une fiche détaillée (cartographiable pour certains, avec ajout de documents/photos), exportable en Word/Excel/CSV/DBF. La cartographie propose un lien dynamique avec les fiches objets, ainsi qu'un requêteur universel permettant de filtrer et d'exporter les résultats par type d'objet.

Techniquement, l'application est déployée sous forme de conteneurs Docker sur une machine hôte, et repose sur les briques suivantes :

- nginx : serveur HTTP
- PostgreSQL / PostGIS : base de données, avec cartouche spatiale
- Symfony (PHP) : framework applicatif
- MapServer : production des données cartographiques (raster, vecteur)
- MapProxy : relais vers des données cartographiques externes (IGN…) et interface WMTS

La BDRTM a une API interne (le frontend échange des données en JSON avec le backend) qui sert uniquement à faire fonctionner l'application en elle-même. Elle n'est pas documentée (pas de Swagger), et n'est pas prévue pour être utilisée par d'autres applications — elle peut changer sans prévenir. C'est pour cette raison qu'il n'a pas de sous-partie "Structure des APIs".

Ce document est la propriété de Magellium Artal Group.
Il ne peut être ni reproduit, ni communiqué sans autorisation écrite préalable.

1.5 Terminologie / Glossaire

Terme	Désignation
API	Application Programming Interface
Borg	Outil de sauvegarde utilisé pour les sauvegardes BDRTM
BDRTM	Base de Données sur les Risques naturels des Terrains en Montagne
CCTP	Cahier des Clauses Techniques Particulières
DNS	Domain Name System
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IGN	Institut national de l'information géographique et forestière
LDAP	Lightweight Directory Access Protocol, protocole d'accès à un service d'annuaire
LD	Liste Documentaire (du projet)
LVM	Logical Volume Manager
MIEX	Manuel d'installation et d'exploitation
OWS	OGS Web Service
PostGIS	Extension spatiale de PostgreSQL
RTM	Restauration des Terrains en Montagne
SIG	Système d'Information Géographique
SSH	Secure Shell
SMTP	Simple Mail Transfer Protocol
WFS	Web Feature Service
WMS	Web Map Service
WMTS	Web Map Tile Service

Ce document est la propriété de Magellium Artal Group.
Il ne peut être ni reproduit, ni communiqué sans autorisation écrite préalable.

2 Disponibilité

2.1 Ouverture de services

Le service est disponible en continu, 24h/24 et 7j/7. Il n'est jamais arrêté : en cas d'intervention nécessaire, l'application est basculée en mode maintenance (cf. 7.2) plutôt que stoppée.

2.2 Arrêts planifiés

Aucun créneau fixe n'est défini : les passages en mode maintenance sont déclenchés selon le besoin (mise à jour, correctif), sans horaire imposé.

D'une manière générale, les mises en production des versions correctives sont effectuées les jeudis entre 12h et 14h. Cependant les dates sont à définir avec l'équipe projet de l'ONF.

En cas de planification d'une mise en production, le référent du projet côté DSI doit en être avisé, en plus de l'équipe projet, pour que la demande soit faite au niveau du CAC (procédure interne de l'ONF).

2.3 Gestion des incidents

Incident : dysfonctionnement bloquant d'un serveur ou d'une brique applicative (conteneur Docker, base de données, service cartographique...) rendant le service indisponible ou dégradé.

Le service étant disponible en continu (cf. 2.1), tout incident bloquant fait l'objet d'une prise en charge dans les meilleurs délais. Les SLA sont définis au chapitre 2.5.

2.4 Gestion des sinistres

Sinistre : destruction partielle ou totale de la machine hébergeant une instance BDRTM (panne matérielle grave, incident sur le site d'hébergement...).

En cas de sinistre, la reprise s'appuie sur les sauvegardes Borg (cf. 6.7), permettant une restauration complète des données et de l'application sur une nouvelle machine.

2.5 Maintenance corrective / Gestion des tickets

La maintenance corrective consiste à identifier et corriger les anomalies affectant l'application BDRTM.

Le support de niveau 1 est directement pris en charge par le chef de projet ONF. Celui-ci qualifie l'anomalie et crée un ticket dans Jira, dans le projet BDRTM : Jira BDRTM – ONF

Le ticket est ensuite pris en charge par l'équipe de TMA pour analyse et traitement.

Ce document est la propriété de Magellium Artal Group.
Il ne peut être ni reproduit, ni communiqué sans autorisation écrite préalable.

Une anomalie peut notamment être liée à l'application BDRTM, aux données exploitées par l'application ou à une technologie ou un composant externe à l'application (infrastructure, logiciel tiers, navigateur, etc.). L'analyse réalisée par l'équipe de TMA permet d'identifier l'origine de l'anomalie et de déterminer les actions correctives appropriées.

Le traitement d'un ticket de maintenance corrective comprend, selon la nature de l'anomalie :

- l'analyse et la qualification de l'anomalie ;
- l'identification de sa cause ;
- la mise en œuvre d'une solution de contournement lorsque cela est nécessaire ;
- la réalisation et le test de la correction ;
- le déploiement de la correction ;
- la validation de la correction ;
- la clôture du ticket Jira.

Délais de prise en charge et de correction

Les délais applicables dépendent de la criticité de l'anomalie.

Type d'anomalie	Délai de prise en charge	Solution de contournement	Correction définitive
Bloquante	4h	1 j	3 j
Majeure	3h ouvrées	4 j	15 j ouvrés
Mineure	10 j ouvrés	15 j ouvrés	30 j ouvrés

Les délais et leur caractère ouvré ou calendaire sont ceux définis dans les engagements contractuels de la TMA.

2.6 Responsabilités / contacts d'exploitation

Activité	ONF	TMA
Support N1	X	
Création ticket Jira	X	
Analyse anomalie		X
Correction		X
Validation correction	X	X
Déploiement		X
Infrastructure	X	X
Mise à jour des certificats	X	X

Ce document est la propriété de Magellium Artal Group.
Il ne peut être ni reproduit, ni communiqué sans autorisation écrite préalable.

3 Utilisateurs

3.1 Configuration des utilisateurs selon l'environnement

L'accès à BDRTM repose sur l'annuaire LDAP de l'ONF. Un fichier LDAP est déposé quotidiennement par l'ONF sur les serveurs BDRTM (dépôt SSH, authentification par clé publique uniquement), et l'application s'interface avec le serveur d'authentification ONF (genepi.onf.fr) pour valider les connexions.

Ce mécanisme est identique sur l'ensemble des environnements, y compris les environnements internes Magellium (Recette Magellium, Iso-Prod) : ils sont fonctionnellement similaires aux environnements ONF, mais restent dédiés aux besoins de développement internes de Magellium avant livraison.

Des comptes de test ONF dédié (exemple : bt06808) existe dans le LDAP, réservé aux tests de connexion et de débogage réalisés par l'équipe Magellium.

Cette section sera à modifier au deuxième semestre 2026, suite à l'évolution de la connexion au LDAP et au nouveau Socle RH de l'ONF.

3.2 Comptes techniques

Compte	Usage
onfdsi	Dépôt SSH quotidien du fichier LDAP fourni par l'ONF (/home/onfdsi/ldap) et mise à jour de la base utilisateurs
Pgbdrtmonf	Accès via tunnel SSH aux bases de données PostgreSQL

L'utilisateur onfdsi ne peut pas déployer lui-même de nouvelles clés SSH : c'est l'ONF qui génère une clé et la transmet aux administrateurs BDRTM pour intégration au playbook Ansible de déploiement.

3.3 Habilitations / Rôles applicatifs

Un utilisateur BDRTM est rattaché à un organisme. Un utilisateur non rattaché à un organisme est simple visiteur (accès en lecture aux données diffusées uniquement).

Chaque organisme gère les objets RTM (sites, événements, ouvrages…) selon trois rôles possibles :

- Origine : organisme à l'origine de la donnée ;Responsable : organisme responsable de la donnée ;De Rattachement : détermine l'organisme « gestionnaire » de l'objet et ses descripteurs complémentaires.

L'accès aux objets dépend par ailleurs de leur statut, dans un workflow de validation à 5 étapes :

Ce document est la propriété de Magellium Artal Group.
Il ne peut être ni reproduit, ni communiqué sans autorisation écrite préalable.

Statut	Visibilité
Brouillon	Le créateur uniquement
Enregistré	Les utilisateurs de l'organisme à l'origine
Soumis à validation	Les utilisateurs des organismes à l'origine et responsable
Validé	Tous les utilisateurs rattachés à un organisme
Validé diffusé	Tous les utilisateurs, y compris les visiteurs

Mais cela se fait aussi en fonction des rôles attribué l'utilisateur d'une part et à l'organisme d'autre part :

Code	Libellé	Niveau	Rôle
VISITOR	Visiteur	Utilisateur	Consulte seulement
PRODUCTOR	Producteur	Utilisateur	Crée, modifie, soumet à validation
VALIDATOR	Validateur	Utilisateur	Vérifie et approuve
CREATEUR	Créateur	Organisme	Autorise la production sur ce type d'objet
VALIDATEUR	Validateur	Organisme	Autorise la validation sur ce type d'objet

La combinaison des deux fait que l'utilisateur a ou non le droit de faire l'action en question.

Action	Droit utilisé	Organisme a le droit ?	Utilisateur a le droit ?	Résultat
Créer ou Modifier	Producteur/Créateur (même droit pour les deux)	✅ Oui	✅ Oui	✅ Peut agir
Créer ou Modifier	Producteur/Créateur	✅ Oui	❌ Non	❌ Ne peut rien faire
Valider	Validateur/Validateur	❌ Non	✅ Oui	❌ Ne peut rien faire
Créer/Modifier/Valider	—	❌ Non	❌ Non	❌ Ne peut rien faire

Le passage au statut "Validé" nécessite des droits de validateur, distincts des droits de simple créateur/producteur.

Ce document est la propriété de Magellium Artal Group.
Il ne peut être ni reproduit, ni communiqué sans autorisation écrite préalable.

4 Versions de l'application

4.1 Liste des composants logiciels

Résumé de la stack technique

- Système : Debian 12, conteneurs Docker
- Serveur web : nginx (reverse proxy) + PHP-FPM 8.3
- Framework applicatif : Symfony 6.4 (back-end)
- Base de données : PostgreSQL 14 + PostGIS (extension spatiale)
- Cartographie serveur : MapServer (production raster/vecteur) + MapProxy (relais fonds de carte externes, IGN)
- Front-end : Backbone.js / jQuery (interface historique) + OpenLayers (cartographie navigateur)

Le détail complet des composants (dépendances JS annexes, outils de test) figure dans le tableau ci-dessous avec leur version actuellement en Production (2.5.2.0). Il sert de référence pour le suivi des mises à jour, la vérification des fins de vie des composants, et le diagnostic en cas d'incident.

Instance	Fonction	Composant	Version
Système	Système d'exploitation de la machine hôte (hors conteneurs)	Debian	12.15
Serveur applicatif	Serveur HTTP/HTTPS – reverse proxy, sert le statique et relaie PHP-FPM (front de l'appli)	nginx	stable-alpine (non figée)
Serveur applicatif	Exécution PHP (FastCGI)	PHP-FPM	8.3.14
Serveur applicatif	Framework applicatif (back-end)	Symfony	6.4.11
Serveur applicatif	Environnement d'exécution / build front	Node.js	16.16.0
Base de données	SGBD relationnel	PostgreSQL	14.13
Base de données	Cartouche spatiale de la base	PostGIS	3.3.4
Cartographie (serveur)	Serveur de données cartographiques (raster, vecteurs)	MapServer	7.4.0
Cartographie (serveur)	Serveur HTTP interne du conteneur MapServer (image camptocamp/mapserver:7.4)	Apache httpd	2.4.39
Cartographie (serveur)	Relais / cache de données externes (scans), interface WMTS communes	MapProxy	1.13.2
Cartographie (serveur)	Export de cartes — configuration MapProxy dédiée, identique au conteneur mapproxy mais paramétrée pour l'export	MapProxy (export)	1.13.2
Front web (navigateur)	Framework JS front (IHM)	Backbone.js	1.1.0
Front web (navigateur)	Relations entre modèles Backbone	Backbone-relational.js	0.10.0
Front web (navigateur)	Associations entre modèles Backbone	Backbone-associations.js	0.6.2

Ce document est la propriété de Magellium Artal Group.
Il ne peut être ni reproduit, ni communiqué sans autorisation écrite préalable.

Front web (navigateur)	Upload de fichiers via modèle Backbone	backbone-model-file-upload	1.0.0
Front web (navigateur)	Fermeture automatique de vues Backbone	Backbone-autocloseable	5.3
Front web (navigateur)	Bibliothèque utilitaire JS	Underscore.js	1.13.4
Front web (navigateur)	Bibliothèque DOM / AJAX + plugins	jQuery	3.6.0
Front web (navigateur)	Validation de formulaires	form-validator	N/R
Front web (navigateur)	Tableaux de données	jQuery DataTables	1.12.1
Front web (navigateur)	Réordonnancement de colonnes DataTables	dataTables.colReorder	1.5.6
Front web (navigateur)	Upload via iframe (compatibilité)	jquery-iframe-transport	1.0.1
Front web (navigateur)	Masques de saisie	jquery-inputmask	5.0.7
Front web (navigateur)	Arborescence (tree)	jquery-jqtree	1.6.3
Front web (navigateur)	Arborescence (tree)	jquery-jstree	3.3.12
Front web (navigateur)	Gestion de layout / panneaux	jquery.layout	1.4.4
Front web (navigateur)	Composants d'interface	jQuery UI	1.13.2
Front web (navigateur)	Chargement de modules AMD	r.js (require.js)	2.3.6
Front web (navigateur)	Gestion des dates	moment.js	2.29.4
Front web (navigateur)	Éditeur de texte riche (WYSIWYG)	CKEditor	35.0.1
Front web (navigateur)	Sélecteur de plage de dates	DateRangePicker	1.3.21
Front web (navigateur)	Auto-complétion / suggestions	typeahead.js	0.11.1
Front web (navigateur)	Framework CSS / composants UI	Bootstrap	5.1.3
Front web (navigateur)	Sélection multiple (multiselect)	Bootstrap Multiselect	1.1.2
Front web (navigateur)	Liaison de données (MVVM)	Knockout	3.5.1
Front web (navigateur)	Icônes	Font Awesome	6.1.1
Cartographie (front)	Bibliothèque cartographique JS (carte navigateur)	OpenLayers	6.14.1
Cartographie (front)	Transformation de projections	proj4js	2.8
Tests (dev)	Framework de tests JS	Mocha	10.0.0
Tests (dev)	Bibliothèque d'assertions	Chai	4.3.6
Tests (dev)	Assertions Backbone	chai-backbone	1.12.7
Tests (dev)	Assertions sur changements	chai-changes	2.1.2
Tests (dev)	Assertions jQuery	chai-jquery	2.0.1
Tests (dev)	Intégration sinon/chai	sinon-chai	3.7.0
Tests (dev)	Mocks / stubs / spies	Sinon	14.0.0

Ce document est la propriété de Magellium Artal Group.
Il ne peut être ni reproduit, ni communiqué sans autorisation écrite préalable.

5 Architecture physique

5.1 Schéma

BDRTM est déployée sur une machine hôte Debian, au moyen de conteneurs Docker. Plusieurs instances de l'application peuvent cohabiter sur la même machine (par exemple une instance recette et une instance formation), chacune isolée du reste du système (fichiers, réseau, processus, mémoire).

La machine hôte expose un socle de services partagés entre toutes les instances :

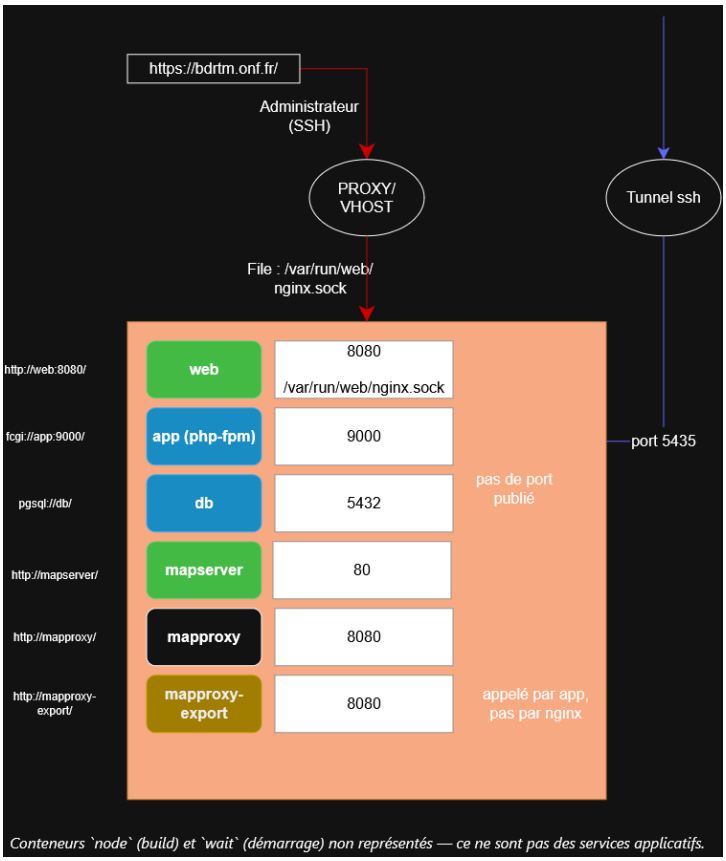
- Ntpd : synchronisation de l'horloge
- Sshd : administration à distance et dépôt de la liste des utilisateurs
- Postfix : relais mail (messages systèmes/supervision et courriels applicatifs)
- Nginx : reverse proxy, chiffrement HTTPS et routage vers la bonne instance (via vhosts)
- Dockerd : gestion des conteneurs applicatifs

Conteneur	Rôle
rtm_production_db	**Base de données PostgreSQL/PostGIS**
rtm_production_mapserver	**Production des données cartographiques**
rtm_production_mapproxy	**Relais de données cartographiques externes**
rtm_production_mapproxy-export	**Identique à mapproxy, dédié à l'export de cartes**
rtm_production_app	**Exécution du code applicatif PHP**
rtm_production_web	**Sert les fichiers statiques, fait le lien entre app, mapserver et mapproxy**

Côté ONF, cette mutualisation se traduit concrètement par deux machines :

- Une machine hébergeant les instances Recette, Formation et Recette Mobile (xrtm98-000.linux.onf.fr) ;
- Une machine dédiée uniquement à la Production (xrtm98-001.linux.onf.fr), isolée sur son propre hôte.

Ce document est la propriété de Magellium Artal Group.
Il ne peut être ni reproduit, ni communiqué sans autorisation écrite préalable.



5.2 Flux avec d'autres SI

L'application BDRTM établit plusieurs flux réseau sortants vers des systèmes d'information externes, de deux natures :

- Flux serveur : émis par les conteneurs applicatifs (app, mapproxy-export), soumis au filtrage réseau du serveur (cf. matrice de filtrage en 6.5).
- Flux navigateur : émis directement par le poste client de l'utilisateur, hors périmètre réseau du serveur BDRTM.

5.2.1 Flux serveur

Système cible	Adresse	Usage	Prérequis / remarques
Serveur d'authentification ONF	https://genepi.onf.fr	Authentification des utilisateurs (login/logout), HTTPS Basic Auth	Sources autorisées : xrtm98-000.linux.onf.fr (Recette/Formation/Recette Mobile) et xrtm98-001.linux.onf.fr (Production). Peut sortir en direct ou via proxy HTTP ; si proxy actif, c'est son IP qui doit être autorisée côté ONF, pas celle de BDRTM.
IGN – Géoplateforme	https://data.geopf.fr	Export cartographique : récupération des tuiles (orthophotos,	Nécessite une clé API IGN et un Referer dédié

Ce document est la propriété de Magellium Artal Group.
Il ne peut être ni reproduit, ni communiqué sans autorisation écrite préalable.

		SCAN, cadastre) par le conteneur d'export MapProxy	
IGN – Géoplateforme	https://data.geopf.fr	Appel serveur au service WMTS privé	Nécessite une clé API IGN et un Referer dédié
Serveur de messagerie	Relais SMTP sur l'hôte	Envoi des courriels applicatifs (notifications, demandes d'accès)	Le conteneur contacte le serveur mail de l'hôte via son IP Docker

5.2.2 Flux navigateur

Système cible	Adresse	Usage
IGN – Géoplateforme	https://data.geopf.fr	Affichage des fonds de carte (WMTS/WMS) et géocodage/autocomplétion de communes

Note : l'ancien endpoint IGN wxs.ign.fr n'est plus utilisé en production, remplacé par data.geopf.fr (Géoplateforme IGN).

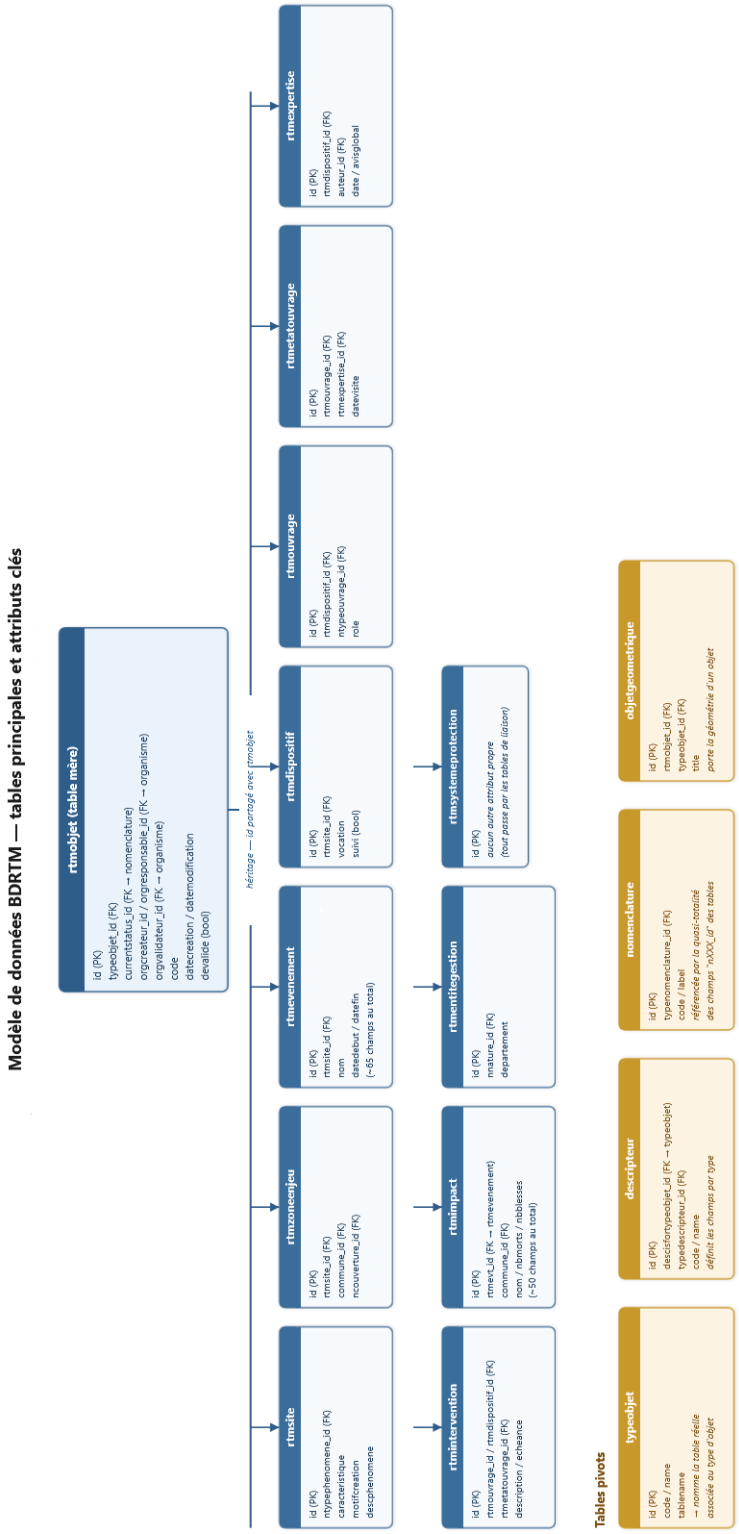
L'accès au serveur d'authentification genepi.onf.fr est autorisé par adresse IP fixe (et non par résolution de nom), pour les sources suivantes : xrtm98-000.linux.onf.fr (172.22.204.97), xrtm98-001.linux.onf.fr (172.22.76.97), et les machines internes Magellium (172.30.1.172).

L'accès à l'application Web de BDRTM est possible depuis n'importe où, sans connexion VPN. L'accès aux machines hébergeant BDRTM (administration SSH) nécessite en revanche une connexion préalable au VPN de l'ONF.

Ce document est la propriété de Magellium Artal Group.
Il ne peut être ni reproduit, ni communiqué sans autorisation écrite préalable.

5.3 Bases de données

5.3.1 Schéma des tables



Ce document est la propriété de Magellium Artal Group.
Il ne peut être ni reproduit, ni communiqué sans autorisation écrite préalable.

Le cœur du modèle repose sur un héritage par tables jointes : la table mère rtmobjet porte les attributs communs, chaque type d'objet a sa table fille, le type étant déterminé par discriminator_id :

Id	Code	Objet métier	Table fille
7	EG	Entité de gestion	rtmentitegestion
8	SI	Site	rtmsite
9	DI	Dispositif	rtmdispositif
10	OU	Ouvrage	rtmouvrage
11	EO	État d'ouvrage	rtmetatouvrage
12	EX	Expertise	rtmexpertise
13	IN	Intervention	rtmintervention
14	EV	Événement	rtmevenement
15	ZE	Zone d'enjeux	rtmzoneenjeu
16	SP	Système de protection	rtmsystemeprotection
60	IP	Impact	rtmimpact

Le catalogue de champs n'est pas figé dans le schéma SQL : la table typeobjet définit les types d'objets, descripteur définit les champs disponibles pour chaque type, et nomenclature (avec nomenclature_liens pour les dépendances entre valeurs) porte les listes de valeurs possibles. Ce mécanisme permet d'ajouter ou modifier des champs métier sans modification du schéma SQL.

Deux autres hiérarchies suivent la même logique : le référentiel administratif (refadmin → region, departement, commune, rdf) et la géométrie (objetgeometrique → geompoint, geomline, geompolygone).

5.3.2 Données

Au-delà des objets métier, le schéma comprend des tables de nomenclatures/types (référentiels de valeurs), des descripteurs dynamiques (champs configurables par type d'objet), des tables filles par objet (impacts, pathologies, matériaux...), des tables d'association N-N, la gestion documentaire (fichier), la sécurité (userbdrtm, organisme, droits), et un cache cartographique dérivé (prefetch_*).

Le schéma actuel (préfixe rtm*) coexiste avec d'anciennes tables tb_* héritées de la V1 (migration 2019), non alimentées par l'application actuelle.

Tables résiduelles hors périmètre fonctionnel, à vérifier avant purge : sauvegardes ponctuelles datées (ex. entitegestion_organisme_backup_20240326), tables temporaires de reprise (temp_import_sites...), table test.

5.3.3 Intégrité des données

L'audit est centralisé sur rtmobjet, commun à tous les objets métier :

Rôle	Colonne
Création / modification	datecreation, datemodification

Ce document est la propriété de Magellium Artal Group.
Il ne peut être ni reproduit, ni communiqué sans autorisation écrite préalable.

Créateur / dernier éditeur	ser_id, lasteditor_id (→ userbdrtm)
Organisme créateur / validateur / responsable	orgcreateur_id, orgvalidateur_id, orgresponsable_id
Origine de création	creationorigin

Il n'y a pas de mécanisme d'audit automatique (pas d'extension Gedmo, pas de trigger SQL) — ces colonnes sont positionnées par la couche applicative.

Cycle de vie : chaque objet a un statut (currentstatus, référence nomenclature) suivant le workflow déjà documenté en 3.3 (brouillon → enregistré → soumis à validation → validé/publié), plus un indicateur devalide. Un objet dévalidé reste en base — ce n'est pas une suppression.

Suppression : physique (DELETE), pas de soft-delete. Encadrée par un contrôle applicatif des dépendances avant suppression (checkDelete()) et par les contraintes de clés étrangères PostgreSQL.

Point de vigilance : au niveau base (contraintes SQL, hors couche applicative), plusieurs clés étrangères de rtmobjet vers organisme et userbdrtm sont en ON DELETE CASCADE — une suppression directe en SQL (hors application) d'un organisme ou d'un utilisateur supprimerait donc en cascade les objets RTM qui lui sont rattachés. Le contrôle applicatif (checkDelete()) ne protège que les suppressions passant par l'application.

Cas des utilisateurs : les comptes (userbdrtm) sont désactivés (isactive = false) plutôt que supprimés.

5.3.4 Connexions à la base de données

Chaque instance dispose de son propre conteneur db (PostgreSQL/PostGIS), isolé des autres instances. Le serveur PostgreSQL n'est jamais exposé directement sur le réseau : il est accessible uniquement en local sur la machine hôte (redirection de port Docker).

- **Depuis l'extérieur du réseau ONF** : via tunnel SSH (authentification par clé publique + filtrage IP), puis mot de passe pour la base elle-même.
- **Depuis le réseau interne ONF** (plage 172.16.0.0/16) : connexion directe autorisée via le tunnel SSH sans authentification SSH supplémentaire.

Les procédures de sauvegarde/restauration sont détaillées en partie 6.7.

5.4 Les Logs

Source	**Conteneur**	Chemin (conteneur)	Chemin hôte (prod)*	Remarque
nginx (accès/erreurs)	web	/var/log/nginx	${LOG_DIR}/web	—
Applicatif Symfony (Monolog)	app	/srv/var/log/prod.log	${LOG_DIR}/app/prod.log	N'écrit qu'en cas d'erreur : bufferise les messages puis vide les 50 derniers dès qu'une erreur survient (404/405 exclus)

Ce document est la propriété de Magellium Artal Group.
Il ne peut être ni reproduit, ni communiqué sans autorisation écrite préalable.

Trace applicatif (audit fin)	app	var/log/trace/bdrtm_trace.log	${LOG_DIR}/app/trace/bdrtm_trace.log	Trace entrée/sortie des méthodes, durées, session, paramètres. Purgé au-delà de 10 Mo (rotation propre à l'appli, pas logrotate). ⚠️ Fichier généré au déploiement, pas versionné — à vérifier qu'il est bien actif en production
PHP-FPM	app	/var/log/php-fpm	${LOG_DIR}/app/php-fpm	—
MapServer	mapserver	/tmp/mapserver	${LOG_DIR}/mapserver	—
Tâche planifiée (app:logout-expired-users, horaire)	app	/srv/var/log/logout_cron_debug.log	${LOG_DIR}/app/logout_cron_debug.log	Seule tâche cron définie dans le code de l'application
PostgreSQL	db	(aucun fichier)	—	Sortie uniquement via syslog de l'hôte, pas de fichier dédié
MapProxy	mapproxy	*(aucun fichier)*	—	
MapProxy-export	mapproxy-export	*(aucun fichier)*	—	
Node	node	*(aucun fichier)*	—	

***LOG_DIR = /data/bdrtm/prod/log** en production (c'est une variable d'environnement : ./var/log en dev, /data/bdrtm/prod/log en prod).*

Ce document est la propriété de Magellium Artal Group.
Il ne peut être ni reproduit, ni communiqué sans autorisation écrite préalable.

6 Spécifications d'infrastructure

6.1 Configuration système

Ressources recommandées pour la machine hôte :

- Processeur : 4 vCPU minimum
- Mémoire : 8 Go par instance déployée
- Disque : 60 Go (système) + 210 Go par instance

Partitionnement (LVM, groupe de volumes unique main) :

Volume	Taille	Point de montage
main	25 Go	/
docker	20 Go	/var/lib/docker
swap	4 Go	swap
data_NOM_INSTANCE	200 Go	/data/bdrtm/NOM_INSTANCE
srv_NOM_INSTANCE	10 Go	/srv/bdrtm/NOM_INSTANCE
—	10 Go	réservé pour snapshots LVM (sauvegarde)

6.2 Paramétrage

6.2.1 Variables globales

Le déploiement est piloté par Ansible/DebOps (dépôt : https://gitana-ext.magellium.com/tma-bdrtm/ansible).

Variable	Description
magellium_pub_ips	Liste des IP publiques Magellium autorisées en SSH sur la machine déployée, et à accéder au serveur SMTP local (supervision)
bdrtm__pub_ips	Liste des IP publiques ONF autorisées en SSH pour accéder aux bases de données et mettre à jour la liste des utilisateurs applicatifs
bdrtm__monitoring_mail	Adresse mail utilisée pour l'obtention du certificat Let's Encrypt et la réception des erreurs SMTP
core__admin_private_email	Liste des adresses email recevant les mails systèmes (alias de l'utilisateur root local)
bdrtm__backup_borg_repo	Chemin vers le dépôt Borg pour les sauvegardes (cf. 6.7). false désactive la sauvegarde
bdrtm__backup_when	Fréquence des sauvegardes (par défaut : tous les jours à 01h00) — voir le paramètre when de backupninja.conf
bdrtm__backup_prune_options	Rétention des sauvegardes. Par défaut : toutes les sauvegardes des 7 derniers jours + 1/semaine sur 4 semaines + 1/mois sur 12 mois

Ce document est la propriété de Magellium Artal Group.
Il ne peut être ni reproduit, ni communiqué sans autorisation écrite préalable.

Déclaration d'une nouvelle machine dans ansible/inventory/host (format ini), section [bdrtm] :

```
NOM_COURT ansible_host=ADRESSE_DE_LA_MACHINE ansible_user=root


Puis copier le dossier modèle ansible/inventory/host_vars/template en
ansible/inventory/host_vars/NOM_COURT, et éditer
ansible/inventory/host_vars/NOM_COURT/definitions.yml.
```

6.2.2 Variables locales à la machine

Variable	Description
ansible_domain / netbase__domain	Domaine de base de la machine (ex. si la machine est NOM_COURT.example.net, mettre example.net)
postfix__fqdn	Nom de domaine utilisé dans les adresses expéditrices des mails système (généralement le FQDN de la machine)
pki_default_domain	Nom de domaine principal du certificat généré (généralement le FQDN de la machine)
pki_domains	Domaines supplémentaires ajoutés au certificat — les noms DNS d'accès aux instances hébergées
bdrtm__instances	Liste des instances applicatives à déployer sur la machine
bdrtm__backup_borg_repo	Surcharge par machine du paramètre global (cf. ci-dessus)

6.2.3 Paramètres par instance (dans bdrtm__instances)

Paramètre	Description
name	Nom de l'instance — doit correspondre au NOM_INSTANCE choisi lors du partitionnement (cf. 6.1)
nginx.name	Liste des noms DNS permettant d'accéder à l'instance
nginx.filename	Nom du fichier de configuration nginx généré
nginx.redirect_to_ssl	Si True (par défaut), force l'utilisation d'HTTPS
start_app	Si True, le script Ansible démarre l'application automatiquement ; sinon démarrage manuel
git	Adresse du dépôt du code applicatif (paramètres du module Ansible git, update vaut no par défaut)
users	UID/GID utilisés par les conteneurs web, app, mapserver, mapproxy, db — différents par conteneur ET par instance
docker_login	Registres Docker à authentifier pour déployer l'instance (+ paramètre enabled: True pour l'activer)
docker_override	Surcharge du docker-compose.yml, notamment pour exposer le port de la base de données

6.2.4 Variables d'environnement de l'instance (génèrent le fichier .env) :

Variable	Description
APP_ENV	prod ou dev (défaut : dev)
APP_SECRET	Chaîne aléatoire ≥ 32 caractères, unique par instance
MAILER_URL / MAILER_DSN	Serveur mail utilisé (smtp://adresse:port) — par défaut, le Postfix local de la machine
POSTGRES_USER	Utilisateur admin de la base (défaut : postgres)
POSTGRES_PASSWORD	Mot de passe admin (généré aléatoirement par défaut)

Ce document est la propriété de Magellium Artal Group.
Il ne peut être ni reproduit, ni communiqué sans autorisation écrite préalable.

POSTGRES_IMAGE	Image Docker de la base : postgis/postgis:9.6-2.5-alpine (base vide) ou registry-ext.magellium.com:443/tma-bdrtm/webapp/db:1.4 (avec données de test/démo, utilisée par défaut, nécessite une authentification registre)
POSTGRES_APP_DB	Nom de la base applicative (défaut : bdrtm)
POSTGRES_APP_USER / POSTGRES_APP_PASSWORD	Identifiants utilisés par l'application (par défaut : postgres / POSTGRES_PASSWORD)
DOCKER_NETWORK	Réseau Docker dédié à l'instance (défaut : 172.16.25.0/24) — sur le réseau ONF, doit être dans 192.168.0.0/16 pour éviter les conflits : Recette 192.168.0.0/24, Formation 192.168.1.0/24, Production 192.168.2.0/24

6.3 HTTPS/Certificats

Depuis 2026, les certificats BDRTM sont fournis par **Certigna (DHIMYOTIS)**. Un script (install_certificate.sh) automatise leur installation pour 4 environnements :

Environnement	Chemin d'installation
Production	/etc/pki/realms/bdrtm.onf.fr
Recette	/etc/pki/realms/bdrtm-recette.onf.fr
Recette Mobile	/etc/pki/realms/bdrtm-recette-mobile.onf.fr
Formation	/etc/pki/realms/bdrtm-formation.onf.fr

Procédure : dépôt des certificats fournis par l'ONF ou le Support de l'ONF, vérification de la chaîne de certification, exécution du script (vérifie correspondance certificat/clé, installe, recharge nginx). Détail des commandes dans GITANA.

6.4 Spécificités SIG (Map-Server, Map-Proxy)

L'accès aux services cartographiques (MapServer en WFS/WMS, MapProxy en WMTS) nécessite une authentification préalable au portail Web — ce ne sont pas des endpoints publics. Des URLs de test dédiées existent pour valider leur fonctionnement (cf. partie 7).

Mapproxy-export, en revanche, n'est pas accessible via le portail Web : il n'est pas routé par nginx et n'est appelé qu'en interne par le conteneur app, uniquement lors des opérations d'export de cartes.

6.5 Sécurité (pare-feu, fail2ban)

Le système est durci selon les recommandations ANSSI pour les conteneurs Docker et le CIS Docker Benchmark v1.2.0. L'accès à la machine est protégé par un pare-feu et fail2ban. Le pare-feu isole les instances hébergées sur une même machine entre elles et limite les communications des conteneurs vers le reste du réseau.

Matrice de filtrage réseau :

Source	Destination	Protocole	Port dest	Statut	Commentaire
Un conteneur	Un conteneur de la même instance	-	-	ACCEPT	
Hôte local	Un conteneur	-	-	ACCEPT	

Ce document est la propriété de Magellium Artal Group.
Il ne peut être ni reproduit, ni communiqué sans autorisation écrite préalable.

Un conteneur	-	TCP	443	ACCEPT	HTTPS sortant (CDN fond de carte)
Un conteneur	-	TCP	80	ACCEPT	HTTP sortant (CDN fond de carte)
Un conteneur	-	TCP/UDP	53	ACCEPT	DNS sortant
Un conteneur	Hôte local	TCP	25	ACCEPT	Mails sortants
Un conteneur	-	-	-	REJECT	Tout autre trafic sortant refusé
-	Un conteneur	-	-	REJECT	Tout trafic entrant direct refusé
IPs en liste blanche	Hôte local	TCP	22	ACCEPT	Accès SSH sur liste blanche
-	Hôte local	ICMP	-	ACCEPT	10 paquets/s/IP acceptés
IPs en liste blanche	Hôte local	TCP	25	ACCEPT	Accès serveur mail (monitoring)
-	Hôte local	TCP	443	ACCEPT	Accès principal à l'application (HTTPS)
-	Hôte local	TCP	80	ACCEPT	Redirection HTTP → HTTPS
Hôte local	-	-	-	ACCEPT	Pas de limitation en sortie de l'hôte local

6.6 Déploiement et maintenance (nouvelle instance, mise à jour, retour arrière)

Nouvelle instance : déploiement via Ansible/DebOps depuis une machine dédiée, en 3 étapes (initialisation système, configuration globale, déploiement de l'instance).

Mise à jour applicative : reconstruction et démarrage des images, migrations si nécessaires, sortie du mode maintenance, sauvegarde des images validées pour rollback rapide (make build/make start, mode maintenance, tests, make save_images) :

```
cd /srv/bdrtm/NOM_INSTANCE/webapp/
. env.sh
make build          # reconstruit les images Docker
make start           # démarre l'instance
```

Retour à une version antérieure : restauration des images archivées, retour au tag Git correspondant, redémarrage.

```
cd /srv/bdrtm/NOM_INSTANCE/webapp/
. env.sh
make stop
docker image prune -a
docker volume prune
make clean
zstdcat archives/docker_images_..._HASH.tar.zst | docker load
```


Ce document est la propriété de Magellium Artal Group.
Il ne peut être ni reproduit, ni communiqué sans autorisation écrite préalable.

```
git checkout vX.X.X
git rev-parse --short HEAD
make start
```

Transfert d'images entre instances (ex. Recette → Production) : sauvegarde des images sur l'instance source, transfert et import sur l'instance cible, renommage.

```
# 1. Sur la machine source, dans /srv/bdrtm/recette/webapp
. env.sh
make save_images


# 2. Copier l'archive vers la machine cible, puis l'importer
zstdcat archives/docker_images_..._HASH.tar.zst | docker load


# 3. Renommer les images (recette -> production)
docker image ls | grep recette | awk '{print $1}' | while read line; do
docker image tag $line:latest $(echo $line | sed
's/recette/production/'):latest; done


# 4. Démarrer
cd /srv/bdrtm/production/webapp && . env.sh && make start
Détail des commandes : manuel technique BDRTM(GITANA), sections
"Déploiement d'une instance" et "Gestion d'une instance".
```

6.7 Sauvegarde et restauration

Outils : backupninja (ordonnancement) + borgbackup (stockage/transfert). Sauvegarde par snapshot LVM + CHECKPOINT PostgreSQL, garantissant une vue cohérente sans interruption de service. Fréquence et rétention paramétrables (cf. 6.2).

Détail des commandes d'installation et de restauration : manuel technique BDRTM(GITANA), section "Sauvegarde et restauration".

6.8 Copie des environnements (Prod → Recette/Formation)

Mécanisme automatisé de copie de la base de données et des fichiers, à déclenchement manuel, exécuté depuis la machine ONF concernée :

```
# Prod -> Recette
sh /root/bdrtm_script/copieEnvironnementBDRTM/sync_prod_to_recette.sh
# Prod -> Formation
sh
/root/bdrtm_script/copieEnvironnementBDRTM/root/sync_prod_to_formation.sh
```


Ce document est la propriété de Magellium Artal Group.
Il ne peut être ni reproduit, ni communiqué sans autorisation écrite préalable.

6.9 Surveillance et supervision

6.9.1 Métriques système

Métrique	Warning	Critical	Graphe
Mises à jour système	disponible	critique disponible	-
Charge CPU	-	-	OUI
Nb de sessions utilisateur ouvertes	10	15	-
Entrées/Sorties (I/O) disques	-	-	OUI
Espace disque (octets et inodes)	80% utilisé	90% utilisé	OUI
Charge moyenne (load average)	-	-	OUI
Utilisation mémoire	80% utilisé	90% utilisé	OUI
Utilisation swap	80% utilisé	90% utilisé	OUI
Synchronisation date/heure	1s de décalage	10s de décalage	OUI
Accessibilité réseau (ping)	80% de perte	100% de perte	-
Nombre de processus	50 × (Nb instances + 1)	100 × (Nb instances + 1)	OUI
Librairie obsolète / nouveau noyau (needrestart)	-	Services ou machine à redémarrer	-
Accessibilité SSH	-	SSH inaccessible	-
Uptime	-	-	OUI
Mails en file d'envoi	2 mails	20 mails	OUI

S'il s'agit d'un serveur physique, superviser également la santé des disques.

6.9.2 Tâches de fond et interactions SI ONF

Métrique	Warning	Critical
Statut de la sauvegarde	Pas réussie depuis 1 jour	Pas réussie depuis 2 jours
Expiration des certificats	Moins de 27 jours	Moins de 7 jours
Statut du service Docker	Non fonctionnel depuis 10 min	Non fonctionnel depuis 1h
Export LDAP ONF	Dernière modif. il y a plus de 30h	Plus de 48h
Authentification Genepi	Authentification échouée	Genepi inaccessible

6.9.3 Métriques applicatives (par instance)

Métrique	Warning	Critical
Page de login	-	Erreur HTTP ou titre différent de « BDRTM: Authentification | ONF »
URL image MapProxy	Image < 1 Ko	PNG invalide
URL image OWS	Image < 1 Ko	PNG invalide
URL image région	Image < 1 Ko	PNG invalide
URL image IGN	Image < 1 Ko	PNG invalide

Ce document est la propriété de Magellium Artal Group.
Il ne peut être ni reproduit, ni communiqué sans autorisation écrite préalable.

URL JSON (nomenclatures)	-	JSON invalide / pas de clé data / pas de liste / liste ≠ 11 éléments
URL OWS GetCapabilities	-	XML invalide / pas d'élément Service / Title sans « ONF BDRTM WS Server »
URL OWS GetFeature	-	XML invalide / pas de balise featureMember / structure incorrecte

Note : l'URL "image IGN" du manuel pointe vers l'ancien endpoint wxs.ign.fr, remplacé en production par data.geopf.fr (cf. 5.2) — à corriger avant usage.

Ce document est la propriété de Magellium Artal Group.
Il ne peut être ni reproduit, ni communiqué sans autorisation écrite préalable.

7 Procédures et outils d'exploitation

7.1 Consignes sur incident

En production, les conteneurs applicatifs redémarrent automatiquement en cas de plantage (configuration docker-compose.prod.yaml). Les consignes ci-dessous concernent les incidents nécessitant une intervention manuelle.

Incident	Criticité	Action	Renvoi
Sauvegarde échouée depuis 2 jours	Critique	Vérifier backupninja/borgbackup, relancer manuellement (backupninja -d --now)	6.7
Certificat expirant dans moins de 7 jours	Critique	Redéployer un nouveau certificat	6.3
Service Docker non fonctionnel depuis 1h	Critique	Vérifier l'état des conteneurs, redémarrer l'instance	6.6
Export LDAP ONF non reçu depuis plus de 48h	Critique	Vérifier le dépôt SSH depuis l'ONF, relancer synchroldap manuellement	3.1/3.2
Authentification Genepi inaccessible	Critique	Tester avec curl -u <LDAPUID>:<MDP> -k https://genepi.onf.fr (cf. 7.4) ; si échec persistant, contacter l'infra ONF	5.2
Espace disque ≥ 90%	Critique	Identifier et purger (anciennes images Docker, sauvegardes obsolètes)	6.1

À compléter avec l'équipe d'exploitation si d'autres incidents types sont rencontrés en pratique.

7.2 Pose/retrait de la page de maintenance

Le mode maintenance repose sur la présence d'un fichier maintenance.txt à la racine de l'instance :

```
# Activer la page de maintenance
cd /srv/bdrtm/NOM_INSTANCE/webapp/
touch maintenance.txt

# Désactiver la page de maintenance
rm maintenance.txt
make save_images
docker image prune   # nettoyage des anciennes images
```

7.3 Arrêt/relance de l'application

```
cd /srv/bdrtm/NOM_INSTANCE/webapp/
```


Ce document est la propriété de Magellium Artal Group.
Il ne peut être ni reproduit, ni communiqué sans autorisation écrite préalable.

```
. env.sh
make stop     # arrêt de l'instance
make start    # relance de l'instance
```

7.4 Tests de bon fonctionnement

7.4.1 Accès général

Ouvrir https://bdrtm.onf.fr/ dans un navigateur — la page doit s'afficher sans erreur.

7.4.2 Authentification ONF (Genepi)

```
curl -u <LDAPUID>:<MDP_CONTEXT> -k https://genepi.onf.fr
# Réponse attendue : <html><head><title>Auth
BDRTM</title></head><body>OK</body></html>


php ./bin/console bdrtm:LDAPTest <login>
# Résultat attendu : "Authentification réussie sur le LDAP ONF"
```

7.4.3 Synchronisation LDAP

```
php ./bin/console bdrtm:synchroldap
```

7.4.4 Envoi de mail (SMTP)

```
php ./bin/console bdrtm:SMTPTest prenom.nom@onf.fr
```

7.4.5 Services cartographiques (MapServer/MapProxy)

Vérifie que les services cartographiques répondent correctement, sachant qu'une authentification préalable au portail Web est requise pour y accéder (ce ne sont pas des endpoints publics).

```
# MapServer – WFS
https://{hostname}/carto/proxy/?request=GetFeature&service=wfs&version=1.0.
0&typeName=site&srs=epsg%3A3857&USERID=6&BBOX=225086.88636254,5217558.39036
,282491.09459672,5263497.044353&WIDTH=751&HEIGHT=601



# MapServer – WMS (style dans un fichier)
https://{hostname}/carto/proxy/?LAYERS=site&TRANSPARENT=true&FORMAT=png24&S
LD=http://web:8080/sld/wms_sld_sites_code_risque.xml&CODESRISQUE=&USERID=6&
SERVICE=WMS&VERSION=1.1.1&REQUEST=GetMap&STYLES=&SRS=EPSG:3857&BBOX=225086.
88636254,5217558.39036,282491.09459672,5263497.044353&WIDTH=751&HEIGHT=601


# MapServer – WMS (style dans la requête, {SLD_BODY} = style textuel)
https://{hostname}/carto/proxy/?LAYERS=site&TRANSPARENT=true&FORMAT=png24&C
ODESRISQUE=&USERID=6&SERVICE=WMS&VERSION=1.1.1&REQUEST=GetMap&STYLES=&SRS=E
```


Ce document est la propriété de Magellium Artal Group.
Il ne peut être ni reproduit, ni communiqué sans autorisation écrite préalable.

```
PSG:3857&BBOX=225086.88636254,5217558.39036,282491.09459672,5263497.044353&
WIDTH=751&HEIGHT=601&SLD_BODY={SLD_BODY}


# MapServer – Légende

https://{hostname}/mapserver?REQUEST=GetLegendGraphic&SERVICE=WMS&VERSION=1
.3.0&SLD_VERSION=1.1.0&FORMAT=image/png&LAYER=site&SLD=http://web:8080/sld/
wms_sld_sites_code_risque.xml&map=/etc/mapserver/bdrtm_leg_3857.map


# MapProxy – génération d'image

https://{hostname}/mapproxyrefadmin/service?SERVICE=WMTS&REQUEST=GetTile&VE
RSION=1.0.0&LAYER=commune&STYLE=normal&TILEMATRIXSET=GLOBAL_WEBMERCATOR&TIL
EMATRIX=10&TILEROW=378&TILECOL=520&FORMAT=image/png
```

7.4.6 Métriques applicatives (login, images cartographiques, endpoints JSON/OWS)

Vérifie le bon fonctionnement de l'application via ces URLs ({hostname} = adresse de l'instance testée) ; les seuils d'alerte associés sont en 6.9.3.

Nom	URL
Image OWS	https://{hostname}/map/ows?service=wms&request=getMap&layers=site&version=1.3.0&crs=EPSG:3857&BBOX=-27833.401802664,5300850.0945279,-26960.34762034,5301159.4256267&WIDTH=731&HEIGHT=259&FORMAT=png24
Image région	https://{hostname}/carto/proxy/?LAYERS=region&TRANSPARENT=true&FORMAT=png24&SLD=https%3A%2F%2F{hostname}%2Fwms_sld_regions_defaut.xml&SERVICE=WMS&VERSION=1.1.1&REQUEST=GetMap&STYLES=&SRS=EPSG%3A3857&BBOX=-65630.392967202,5457810.4712569,157871.47770754,5536999.2325493&WIDTH=731&HEIGHT=259
JSON (nomenclatures)	https://{hostname}/api/nomenclatures/typecode/nTypePhenomene
OWS GetCapabilities	https://{hostname}/map/ows?service=wms&request=getCapabilities&version=1.3.0
OWS GetFeature	https://{hostname}/map/ows?service=wfs&request=getfeature&layers=site&typename=site&version=1.1.0&crs=EPSG:3857&BBOX=-27833.401802664,5300850.0945279,-26960.34762034,5301159.4256267&WIDTH=731&HEIGHT=2591
Image IGN	https://data.geopf.fr/... *(ancien endpoint wxs.ign.fr obsolète, cf. 5.2 — URL exacte à reconfirmer sur data.geopf.fr)*

7.5 Modification des mots de passe

Mot de passe personnel (connexion à l'application, et à la VM en SSH) : géré via le compte LDAP ONF, en dehors de BDRTM — ce n'est pas une procédure propre à cette application. Sa modification se fait via les outils de gestion de compte de l'ONF (hors périmètre de ce document).

Ce document est la propriété de Magellium Artal Group.
Il ne peut être ni reproduit, ni communiqué sans autorisation écrite préalable.

Mots de passe des comptes techniques de la base de données (ex. bdrtmonf, exportmassif, pgbdrtmonf, utilisés par l'application/les scripts, pas par un utilisateur humain) :

```
\password <USERNAME>
```

Autres secrets applicatifs (APP_SECRET...) : définis via Ansible (cf. 6.2), aucune procédure de rotation documentée.

7.6 Liens utiles

Outil	Lien / accès
Dépôt Ansible (déploiement)	https://gitana-ext.magellium.com/tma-bdrtm/ansible
Depot GIT	https://gitana-ext.magellium.com/tma-bdrtm
Production	https://bdrtm.onf.fr
Recette ONF	https://bdrtm-recette.onf.fr
Recette Mobile ONF	https://bdrtm-recette-mobile.onf.fr / https://bdrtmrecette-officenationaldesforets.msappproxy.net/login
Formation ONF	https://bdrtm-formation.onf.fr
Recette Magellium	https://recette.bdrtm-v2.magellium.fr
Iso prod Magellium	https://bdrtm-v2.magellium.fr
Serveur d'authentification ONF	https://genepi.onf.fr/
IGN - Géoplateforme	https://data.geopf.fr

Ce document est la propriété de Magellium Artal Group.
Il ne peut être ni reproduit, ni communiqué sans autorisation écrite préalable.



L'ingénierie de la donnée au service de la Planète et des Territoires

Pour plus d'informations

Adresses

1, rue Ariane
31520 Ramonville-Saint-Agne

90, boulevard National
92250 La Garenne-Colombes

Site internet www.magellium.com

Suivez-nous @magellium