



**MINISTÈRE
DES ARMÉES**

*Liberté
Égalité
Fraternité*

NON PROTEGE

**Direction générale
de l'armement**

DOCUMENTATION 2

ANALYSER ET METTRE EN CONFORMITÉ SON PROJET

1/17

DGA Maîtrise de l'information

BP 7 – 35998 Rennes CEDEX 9

Téléphone : + 33 (0) 2 99 42 90 11 - Télécopie : + 33 (0) 2 99 42 91 01

NON PROTEGE

Ce document est la propriété de l'État, il ne peut être reproduit, copié ou utilisé sans autorisation écrite.

SOMMAIRE

Historique	3
Acronymes.....	4
Introduction	5
1. Analyser la conformité de son projet.....	6
1.1 Document d'Architecture Technique (DAT).....	6
1.2 Document d'Installation Applicative (DIA)	6
1.3 Analyse des machines virtuelles	7
2. Mettre en conformité son projet	8
3. Être compatible avec l'API d'Observabilité	9
3.1 Enrôlement à l'API OBS	10
4. Ajouter la connexion MinDefConnect	11
5. Prendre en compte les spécificités des C1	13
5.1 Proxy sortant	13
5.2 Serveur sortant SMTP.....	15
5.3 Certificats publics.....	16
Conclusion.....	17

Historique

Tableau 1 : Historique

Version	Date	Auteur	Commentaire
1.0.0	28/08/2024	Clément LIMOUSIN	
1.0.1	09/09/2024	Chloé PAGENEL	Relecture
1.0.2	11/09/2024	Chloé PAGENEL	Relecture
1.0.3	11/09/2024	Aurélie GRABAS-DOREMUS	
1.0.4	12/09/2024	Cindy PEREIRA	Relecture
1.0.5	12/09/2024	Chloé PAGENEL	Relecture
1.0.6	07/10/2024	Cindy PEREIRA	Correction de coquilles
1.0.7	16/10/2024	Maxime Heim	Ajout d'infos et d'un exemple sur l'API OBS
1.0.8	22/01/2025		Modification des liens morts
1.0.9	03/02/2025	Romain GUYOT	Suppression de la partir « Load Balancer »
2.0.0	17/02/2025	Anousa MYSAY	Ajout des NFR_MDC, NFR_PROXY_C1NP, NFR_SMTP_C1NP, NFR_OBSSUP_03
2.0.1	25/02/2025	Aurélie GRABAS-DOREMUS	Ajout informations C1DR

Acronymes

Tableau 2 : Acronymes

Acronyme	Description
API	Application Programming Interface
C1NP	Cloud Non Protégé
CCT	Cadre de Cohérence Technique
COTS	Commercial Off-The-Shelf (<i>produit informatique standard</i>)
DA	Direction d'Application
DAT	Document d'Architecture Technique
DIA	Document d'Installation Application (<i>équivalent du MIN</i>)
DP	Direction de Projet
GDS	Gestion Des Secrets
TME	Tierce Maintenance Exploitation
VM	Machine Virtuelle
ZP	Zone Projet

Introduction

L'objectif de ce **chapitre 2** est de vous accompagner dans la mise en conformité de votre SI avec le Cadre de Cohérence Technique, disponible ici :

<https://portail.intradef.gouv.fr/intranum/cadre-coherence-technique-cct>

Ce chapitre commence par vous présenter comment récupérer et analyser les **informations clés** de votre SI et de son environnement.

Vous devrez ensuite effectuer une étape de **mise en conformité** de votre SI. Il s'agira principalement d'une montée de version de vos applicatifs, si celle-ci s'avère nécessaire.

Par la suite, seront détaillés les prérequis et les attendus pour le développement de votre **API Observabilité** (à ne pas confondre avec l'utilisation du service Observabilité). Le but de cette API est la récolte des informations de gouvernance et de fonctionnement de votre SI.

Vous prendrez ensuite connaissance du service **MinDefConnect** (à mettre en place obligatoirement pour l'authentification des usagers) et des démarches à suivre pour relier votre SI à celui-ci.

En résumé, voici les **quatre parties majeures** abordées par ce document :

Charge	Titre de la partie	Description
20%	Analyser la conformité de son projet	Collecter, rassembler, identifier les informations clés de son SI et de son environnement
40%	Mettre en conformité son projet	Mes versions applicatives sont-elles à jour ? Quelles mises à jour sont requises ?
30%	Être compatible avec l'API observabilité	Comment rendre son SI compatible avec l'API observabilité ?
10%	Ajouter la connexion MinDefConnect	Comment relier la connexion à son SI avec MinDefConnect ?

1. Analyser la conformité de son projet

L'objectif de cette première partie est d'identifier les informations clés de votre SI qui vous permettront par la suite de vérifier sa conformité au CCT en vigueur.

La première étape consiste donc à faire un état des lieux de votre SI. L'objectif va être de récupérer les informations suivantes :

- Les **systèmes d'exploitation** des différentes machines virtuelles
- Le type et la version de la **base de données**
- La version de la **technologie**, du **moteur web** et des modules supplémentaires installés
- La **version** du COTS installée
- Les **modules** du COTS installés (modules personnalisés)

Pour récupérer ces informations, il est possible de se baser sur plusieurs sources, décrites dans les sous-parties suivantes.

1.1 Document d'Architecture Technique (DAT)

Le **DAT** doit fournir les informations suivantes :

- **Informations sur les machines :**
 - o Leur nombre
 - o vCPU/RAM
 - o La taille des disques
- **Les systèmes d'exploitation**
- **Les composants logiciels :**
 - o Langage
 - o Base de données
 - o Moteur Web
- **La version du COTS**
- Les **modules du COTS** installés ainsi que les dérogations si ces derniers ne sont pas dans la liste autorisée par le CCT
- Les **services supplémentaires** (exemple : serveur mail)
- Les **flux applicatifs**
- La liste des **ressources en ligne** consommées par le SI

1.2 Document d'Installation Applicative (DIA)

L'analyse du **DIA** ou manuel d'installation (MIN) doit fournir les informations suivantes :

- **Format du livrable** (site entier compressé ou différence par rapport à la version n-1)
- **Ordre d'installation/mise à jour** des composants logiciels
- **Tests de validations**

En supplément du DIA, la DA/DP transmet parfois des scripts liés à l'automatisation (en Shell ou en Ansible). L'analyse de ces scripts permet de connaître la méthode concrète de livraison.

Dans un objectif de standardisation des pratiques l'équipe Move2Cloud met à disposition des DA/DP en cours de migration vers les C1 un template de MIN à renseigner avec les informations de votre SI : https://portail-ct-mvl.intradef.gouv.fr/sites/DSI-Socle-Numerique_Move-to-Cloud/_layouts/15/WopiFrame.aspx?sourcedoc=%7b4565F2A3-53B5-4CE2-A596-D81C1159D9D2%7d&file=20241129_AND_Modele-MIN-C1NP_v2.docx&action=default

1.3 Analyse des machines virtuelles

La dernière étape pour récupérer les informations est l'analyse des machines virtuelles en production. L'objectif de cette étape est de **confirmer les informations récupérées** dans le corpus documentaire (DAT/DIA) ainsi que **d'identifier des informations manquantes**.

Les informations à récupérer sont :

- Les **versions de paquets** installés avec YUM, ou DNF (en fonction du système d'exploitation des machines)
- Éventuellement les **versions des modules** du COTS
- Éventuellement la **configuration des Virtual hosts**
 - o Pour HTTPD : les fichiers sont présents dans /etc/httpd/conf.d/
 - o Pour Nginx : les fichiers sont présents dans /etc/nginx/sites-enabled/
- Les **processus en cours d'exécution** sur les différentes machines

2. Mettre en conformité son projet

Une fois l'analyse de l'existant effectuée, il faut confirmer que les modules et les versions des composants logiciels sont autorisés par le **Cadre de Cohérence Technique (CCT)** :

<https://portail.intradef.gouv.fr/intranum/cadre-coherence-technique-cct>

Le CCT fixe les applicatifs et les versions **autorisées** sur les Cloud du ministère des Armées. Le CCT est présent afin de donner **un éventail de choix** de modules.

Dans le cas où un module ne serait pas présent, une demande de **dérogation** devra être faite au SC²A. Vous trouverez toutes les informations nécessaires en suivant cette URL :

<https://portail.intradef.gouv.fr/intranum/comite-coherence-architectures-sc2a>

Si des éléments ou des modules ont été identifiés comme **non conformes au CCT** et qu'une dérogation n'a pas été obtenue pour les conserver, une montée de version ou un remplacement de ces composants doivent être effectués préalablement à la migration.

Attention : Cette étape est très importante. **Vous ne pouvez pas passer à la suite de la migration si ce prérequis n'est pas rempli.** Assurez-vous que le SI fonctionne toujours correctement à la suite de cette opération.

De plus, si votre SI utilise un ou plusieurs **COTS**, il faut vous assurer de leur présence ou non parmi les collections RUCHE disponibles.

(Pour en savoir plus sur les collections RUCHE, cf Guide 1, chapitre 3.6)

Le lien vers les collections RUCHE : <https://ruce-galaxy.intradef.gouv.fr/>

Si une collection RUCHE couvre le/les COTS que vous utilisez, vous **DEVREZ** utiliser cette collection.

L'implémentation de collections sera abordé dans le Guide 5, lors du déploiement de votre SI avec Ansible.

3. Être compatible avec l'API d'Observabilité

Cette partie couvre le NFR suivant :

NFR_OBSSUP_03 : Le SI doit intégrer dans son implémentation les openAPI répondant aux API REST OBSERVABILITE /Health & /Info.

Attention : Il s'agit là de l'API d'Observabilité, à ne pas confondre avec le service Observabilité (cf. **chapitre 5 de la documentation M2C**)

L'objectif de cette partie est de **comprendre l'API d'Observabilité et les étapes à mettre en place pour l'utiliser**.

L'API Observabilité collecte des informations du SI, ces données sont restituées au travers d'un dashboard Kibana. Elle permet ainsi de :

- Faciliter la **récupération d'informations de gouvernance** (nom, version, niveau de classification, date de fin d'homologation ...).
- Faciliter la **récupération d'informations d'architecture et de fonctionnement** (statuts global UP ou DOWN, capacité à joindre les services et autres SI dont le SI dépend)

Un projet API observabilité est disponible sur la ZS_CONTINUITY, celui-ci est fonctionnel et détient un rôle permettant de l'installer facilement.

Ce rôle peut être trouvé au lien suivant :

https://scm-intradef.picsel.defense.gouv.fr/ZS_CONTINUITY/api-observabilite/api-observability-install

Un exemple d'API Observabilité peut être trouvé au lien suivant :

https://scm-intradef.picsel.defense.gouv.fr/ZS_CONTINUITY/api-observabilite/observability-php

Des informations sur l'API Observabilité peuvent être trouvées au lien suivant :

https://forge.intradef.gouv.fr/mediawiki/portail-service-desk-and/API_d%27observabilit%C3%A9

Vous trouverez des informations utiles dans les onglets « **MediaWiki de l'équipe** » et « **Git de l'API Observabilité** » qui donnent notamment accès à un kit d'exemple de fichiers à mettre en place.

3.1 Enrôlement à l'API OBS

Pour visualiser les appels de l'API Observabilité sur PICSEL, vous devrez faire une demande d'enrôlement (les VMs et le SI doivent être requêté, donc le SI doit être déployé sur des VMs stables) au lien suivant :

<https://forge.intradef.gouv.fr/plugins/tracker/?tracker=12443&func=new-artifact>

4. Ajouter la connexion MinDefConnect

Cette partie couvre le NFR suivant :

NFR_MDC : L'authentification des utilisateurs sur le SI sont OBLIGATOIREMENT réalisés via MindefConnect (Internet ou Intradef).

Un des prérequis à l'hébergement sur les C1 est la **délégation de l'authentification** des usagers au service « **MinDefConnect** » Internet pour **C1NP** et « **MinDefConnect** » Intradef pour **C1DR**. Il s'agit d'un service d'authentification basé sur la solution **RedHatSSO** et le protocole **OpenID Connect** (mode d'authentification « **Authorization Code Flow** »).

La partie technique du raccordement sera abordée dans la documentation « **5. Déployer son projet grâce à Ansible** », certaines actions peuvent cependant être anticipées :

- Vous pouvez d'ores et déjà remplir et transmettre le « **formulaire d'enrôlement** » pour PICSEL : https://catalogue-services-dirisi.intradef.gouv.fr/sp?id=kb_article_view&sysparm_article=KB0615978

Ce formulaire est à envoyer au SAND à l'adresse mail : casid-sand-mindefconnect.exploitant.fct@intradef.gouv.fr

En réponse à votre formulaire, vous obtiendrez un **fichier** au format .json contenant votre **secret_id**, **realm**, et **url d'appel**. Ceux-ci vous seront utiles pour raccorder votre SI à MDC.

Vous trouverez également un formulaire semblable à remplir pour l'enrôlement à MDC sur les C1.

Vous pouvez étudier les options possibles pour raccorder votre SI à la solution MDC comme par exemple, l'utilisation de l'extension MiniOrange OAuth pour **Joomla** ou l'extension OpenID Connect Client (oidc) pour **Drupal**.

Si une extension compatible existe pour votre SI, vous pouvez la rajouter manuellement avant l'étape de package du SI, afin qu'elle soit incluse au sein de celui-ci.

Les étapes de configuration via playbooks Ansible seront détaillées dans la documentation « **5. Déployer son projet grâce à Ansible** ».

Dans le cas où il n'existe pas d'extension compatible avec votre SI, il est possible que vous ayez à réaliser des développements spécifiques.

En suivant ce lien, vous trouverez toutes informations utiles à connaître sur le sujet MDC :

https://portail-ct-mvl.intradef.gouv.fr/sites/DSI-Socle-Numerique_Move-to-Cloud/Ressourcesdocumentaires/Documentation-Pr%C3%A9requis/MindefConnect-internet

5. Prendre en compte les spécificités des C1

5.1 Proxy sortant

Cette partie couvre le NFR suivant :

NFR_PROXY_C1NP : Un SI C1NP doit OBLIGATOIREMENT utiliser le PROXY C1NP pour réaliser une interconnexion avec un système/service exposé sur INTERNET. L'usage de ce proxy est à prendre en compte dans l'implémentation. L'interconnexion avec le PROXY est une variable de l'inventaire technique.

Si votre SI à destination de **C1NP** à besoin de **consommer des ressources sur Internet**, il est **essentiel** de tenir compte du proxy sortant C1NP.

Le principe est d'utiliser le proxy en tant que « relai intermédiaire » pour transmettre les appels vers Internet, à des fins de **sécurité**, de **traçage**, et de **filtrage**.

Il vous appartient de définir la façon exacte de procéder à cette implémentation, selon votre SI et la technologie sur laquelle il se base.

Les points clés de cette intégration sont :

- Le positionnement des variables « **proxy_host** » et « **proxy_port** » dans votre inventaire (cf. documentation « 5. Déployer son projet grâce à Ansible »). Elles seront utilisées par l'exploitant C1NP.
- Un mécanisme pour permettre de **positionner un proxy en intermédiaire** des appels vers internet.
Les appels avec les ressources internet doivent être fait en HTTPS, mais la requête intermédiaire vers le proxy se fait en HTTP (avec la variable HTTP_PROXY par exemple, et non HTTPS_PROXY)
- La transmission préalable des **ressources consommées**, lors de la demande d'hébergement C1NP. Cela est nécessaire pour ajouter les autorisations dans la **Liste Blanche**.
Cette liste doit également être présente dans le **DAT**, et fournie aux exploitants C1NP avec le package de livraison.

Attention : même si votre SI ne consomme pas directement d'API en ligne, n'oubliez pas d'indiquer – si votre SI permet de publier des articles – tout lien qui pourrait être inclus dans ceux-ci, par exemple des liens Youtube, puisque votre SI devra pouvoir y accéder pour charger la miniature.

Concernant les déploiements sur **C1DR** il n'y a aucune possibilité de branchement sur Internet. A terme certains Cloud Services seront connectés à Internet (ex. Medusa/Artifactory) mais pas de SI.

5.2 Serveur sortant SMTP

Cette partie couvre le NFR suivant :

NFR_SMTP_C1NP : Un SI peut transmettre des mails via un service SMTP du C1NP. L'adresse de l'émetteur doit avoir un nom de domaine en **@cloud.defense.gouv.fr**.

C1NP possède un serveur SMTP pour permettre **l'envoi** de mails depuis votre SI.

- Les communications entre le SI et le serveur SMTP de C1NP sont chiffrés en SMTPS : il est donc requis de la part du SI d'implémenter le code nécessaire pour chiffrer le flux SMTP à destination du serveur, sur la base d'une clé privée accessible en arrière-plan de la couche applicative (par exemple au sein d'une Keystore dans le contexte Java). Pas de contraintes sur la nature de la clé privée.
- L'authentification SMTP n'est **pas en place** sur C1NP actuellement : la première partie de l'adresse mail (avant le @) n'a pas d'importance.
- En revanche, il y a bien une vérification sur la partie après le @ : pour être accepté par le serveur SMTP, il faut que l'adresse mail soit en **@cloud.defense.gouv.fr** pour attester de l'origine de l'expéditeur.
Il ne s'agit pas d'une vraie BAL, c'est déclaratif dans l'appel de votre SI au serveur SMTP : vous définissez l'adresse mail que vous souhaitez en tant qu'expéditeur (agira comme une no-reply).

C1DR ne propose pas de service SMTP. Si vous souhaitez un serveur SMTP vous devrez donc déployer votre propre solution et faire une demande d'ouverture de flux pour ce serveur.

5.3 Certificats publics

Vous devrez fournir aux exploitants **C1NP** les **certificats SSL** qu'ils devront appliquer lors de l'exposition en ligne de votre SI.

Pour un déploiement sur **C1DR** vous pouvez vous référer à la documentation 5 du Move2Cloud qui décrit l'utilisation de la Gestion des secrets à lier à la NFR suivante :

NFR_SECRET_02 : Les certificats HTTPS privés exposés par les frontaux WEB d'un SI doivent être récupérés en automatique auprès du serveur GDS. Le renouvellement des certificats doit aussi être pris en charge en automatique via l'usage d'un agent vault disponible au catalogue RUCHE.

Pour les obtenir, vous **pouvez dès à présent en faire la demande**, ou attendre plus tard dans le processus d'intégration si vous le souhaitez, sachant qu'ils ont une validité d'un an. Il s'agit d'une demande de type DSC « **Site WEB – Acquisition de certificat SSL** » à faire au POC concerné.

Plus d'informations sur ce lien :

https://catalogue-services-dirisi.intradef.gouv.fr/sp?sys_kb_id=508cf2e65d5a8e90d025c7b7b258bd55&id=kb_article_vie&sysparm_rank=1&sysparm_tsqueryId=73e45bd669ecde1085f38acb96e95a81

Conclusion

Vous avez terminé le chapitre 2 « Analyser et mettre en conformité son projet ». Grâce à celui-ci, vous avez pu remplir les objectifs suivants :

Avancement	Titre de la partie	Description
✓	Analyser la conformité de son projet	Collecter, rassembler, identifier les informations clés de son SI
✓	Mettre en conformité son projet	Mes versions applicatives sont-elles à jour ? Quelles mises à jour sont requises ?
✓	Être compatible avec l'API d'Observabilité	Comment rendre son SI compatible avec l'API observabilité ?
✓	Ajouter la connexion MinDefConnect	Comment relier la connexion à son SI avec MinDefConnect ?