

IS-TVA: ddl1-4 C1 Spécifications du site de secours

Table of Contents

- IS-TVA: ddl1-4 C1 Spécifications du site de secours
 - Infrastructures et architectures de secours
 - Catégories d'infrastructures
 - Liste des chantiers d'infrastructures
 - Le site de secours
 - Choix du site de secours
 - Remarques
- Préparation du site de secours
 - Serveurs de secours et périphériques
 - Règles relatives au site de secours CIP
 - Règles relatives aux applicatifs
 - Quartier de la feuille de route
 - Architecture de sauvegardes / restaurations sur le site de secours
 - Règles relatives aux données
 - Règles relatives au dispositif de réplication des données
 - Quartier de la feuille de route
 - Infrastructure nécessaire aux opérations de secours
 - Règles relatives aux utilisateurs (agents, usagers, partenaires)
 - Règles relatives aux exploitants (GTS, G2A, PSN, Assistance)
 - Quartier de la feuille de route
 - Architecture des réseaux locaux sur le site de secours
 - Règles relatives aux réseaux d'accès aux sites de production et de secours
 - Quartier de la feuille de route
 - Points d'accès sur le réseau longue distance ;
 - Quartier de la feuille de route
 - Architecture sécurisée pour les accès Internet entrant et sortant sur le site de secours
 - Quartier de la feuille de route

Infrastructures et architectures de secours

Catégories d'infrastructures

“Les infrastructures et architecture de secours sont constituées par :

- les serveurs de secours et leurs périphériques ;
- l'architecture de sauvegardes / restaurations sur le site de secours ;

- les postes nécessaires aux opérations de secours ;
- les réseaux locaux sur le site de secours ;
- les points d'accès sur le réseau longue distance ;
- l'architecture sécurisée pour les accès Internet entrant et sortant sur le site de secours,"

(050186_Spec_Dispositif_Secours_COPERNIC_V1.03.doc)

Liste des chantiers d'infrastructures

Num.	Catégorie	Quartier	N° CHANTIER	MOE / MOE Déléguée	Format
1	Serveurs de secours et périphériques	Infrastructure de secours			
		Serveurs d'applications			
		Transfert de fichiers	CT11	SI2B - Division des infrastructures et applications de communications (DIACOM) bureau.si2b-diacom@dgfip.finances.gouv.fr Denis Chesneau (01 57 33 71 84 Xavier Wavelet (01 57 33 64 52)	stf - Philippe Guntz
		Annuaire des services	CT21	SI1A - Division de l'architecture du Système et des Projets (DASP) bureau.si1a-dasp@dgfip.finances.gouv.fr Prothée-Dejouhanet (01.57.33.69.91)	vespa - ???
		Administration, supervision et exploitation	CT14	SI2B - Normes et stratégie des systèmes et des infrastructures (NESSIE) bureau.si2b-nessie@dgfip.finances.gouv.fr Michel Coudray (01 57 33 65 60)	supervision - groupe
			CT11	SI2B - Division des infrastructures et applications de communications (DIACOM) bureau.si2b-diacom@dgfip.finances.gouv.fr Denis Chesneau (01 57 33 71 84 - absent du 11/09 au 19/09) Xavier Wavelet (01 57 33 64 52)	sppc - groupe
2	Architecture de sauvegardes / restaurations	Réplication des données critiques	CT15	SI2B - Déclinaison des socles - Des infrastructures génériques normalisées (DESIGN) bureau.si2b-design@dgfip.finances.gouv.fr	sauvegardes restaurations - Patrick Moragues
		Sauvegarde sur support physique			
3	Infrastructure nécessaire aux opérations de secours	Pilotage du déploiement	CT14	SI2B - Normes et stratégie des systèmes et des infrastructures (NESSIE) bureau.si2b-nessie@dgfip.finances.gouv.fr Olivier Mazain	Déploiement - Frédéric Lapoele
4	Réseaux locaux	Réseaux applicatifs	CT12	SI2B - Division des infrastructures et applications de communications (DIACOM) bureau.si2b-diacom@dgfip.finances.gouv.fr	Réseau - Jacques
		Réseaux d'administration	CT12		
		Basculement réseau	CT12		

Num.	Catégorie	Quartier	N° CHANTIER	MOE / MOE Déléguée	Format
5	Points d'accès sur le réseau longue distance	Passerelles d'accès sécurisé	CT13	SI2B - Division messagerie outils collaboratifs - Poste de travail - Sécurité - (DMOCSS) bureau.si2b-dmocss@dgfip.finances.gouv.fr	PAS - groupe
		Poseidon	CT11	SI2B - Division des infrastructures et applications de communications (DIACOM) bureau.si2b-diacom@dgfip.finances.gouv.fr Patrick Guyot (01 57 33 73 69)	Poseidon - groupe
6	Architecture sécurisée pour les accès entrant et sortant	Portail	CT31	SI1G - Section Gestion des Outils Transverses d'Habilitation et d'Authentification - GOTHIA (annuaires pro, agents, partenaires, applications MADHRAS, APEX, ASPASIE et Mon profil, projets France connect, ENSAP et accès croisés) bureau.si1g-annuaire-dgfip@dgfip.finances.gouv.fr Vincent Landrea (01 57 33 65 68) vincent.landrea@dgfip.finances.gouv.fr	Portail Annuaire - Groupe
		Annuaire	CT32		
		Sécurité	CT41	SI1C NANTES - DIVISION TECHNIQUE TRANSVERSE - SPEP - ITM - Osatis - Composants communs - Assistance MAD Emmanuel Bezagu (0240125183)	ITM - groupe
			CT13	SI2B - Division messagerie outils collaboratifs - Poste de travail - Sécurité - (DMOCSS) bureau.si2b-dmocss@dgfip.finances.gouv.fr	ADP - Groupe
		Adhésion et inscription	CT42	SI1C- DIVISION DES APPLICATIONS PROFESSIONNELLES 1 (D.A.P.1) - OPALE - REFCB/REF DELEG Béatrice Kerbaul	Habilitation - Philippe Cardona

Le site de secours

Choix du site de secours

“Le site de secours est le site d'ISIQ du bureau Copernic 7 qui est déjà (ou sera) pourvu de toutes ou d'une grande partie des configurations matérielles de secours au titre de l'ISIQ. De même, le CDS devrait être pourvu de toutes ou d'une grande partie des configurations matérielles utiles aux recettes des solutions de secours au titre de l'IRA et de l'IRIA. Ainsi, il est probable qu'un projet à secourir puisse s'appuyer entièrement sur les configurations matérielles de l'IRA, IRIA et de l'ISIQ pour la mise au point et l'exploitation de sa ou ses solution(s) de secours.”

(050079_Charte_du_Secours_COPERNIC_V2.2.doc)

Remarques

Le choix du CIP comme site de secours peut exercer une contrainte forte sur le DMIA du palier 1 :

- L'arrêt de la plate forme d'ISIQ implique la mise en oeuvre de procédures en amont de la préparation de la plate forme de secours (arrêt propre des services, sauvegardes préalables, opérations de nettoyage, modification du découpage de la baie de disques, ...)
- Le maintien de certains services de l'ISIQ peut nécessiter un arbitrage délicat à prendre.

Afin de minimiser l'impacte des opérations préalables à l'activation du site de secours, il est préférable de disposer d'un site prêt, ou de matériels dédiés à cette fin sur un site disposant des éléments techniques recensés dans le tableau ci-dessus.

Préparation du site de secours

Serveurs de secours et périphériques

Règles relatives au site de secours CIP

- **SB_PRA_8** Le plateau informatique de secours constitue au sein du CIP un site de production Copernic conforme aux principes généraux en la matière : sécurité physique et des accès, servitudes, exploitation à distance... Il est constitué des éléments suivants :
 - **8.a** - infrastructure partagée du site de Noisiel ;
 - **8.b** - sous-ensemble de la plate-forme technique de l'ISIQ limité aux équipements des applicatifs et services transverses du périmètre du PRA ;
 - **8.c** - équipements dédiés au secours, hors plate-forme d'ISIQ, comme par exemple les baies de réplication.
- **SB_PRA_9** Les équipements de la plate-forme informatique d'ISIQ hors périmètre du PRA (applicatifs ou services qui ne sont pas ou pas encore en production sur le SPS, équipements propres aux activités d'ISIQ ...) ne font pas partie du plateau informatique de secours.
- **SB_PRA_10** Le plateau informatique de secours reconstitue l'intégralité du périmètre du PRA (mêmes vues applicative et technique), avec une stricte identité (mêmes équipements, mêmes quantités, mêmes règles de montage et câblage...) pour les applicatifs et les services transverses.
- **SB_PRA_11** La reconstitution de la production sur la plate-forme technique d'ISIQ dans le périmètre du PRA se fait par réinstallation sur tous les équipements des socles techniques et paquets applicatifs avec reprise des configurations et personnalisations de production.

(050188_Guide_general_du_PRA COPERNIC.doc.)

Règles relatives aux applicatifs

- **SB_PRA_25** L'ensemble des applicatifs de la salle 3 du SPS est traité comme un site externe au PRA, avec la particularité d'être (potentiellement) détruit en cas de sinistre déclenchant le PRA :
 - **25.a** en cas d'exercice l'accès et la continuité de production doivent être assurés ;
 - **25.b** en cas de sinistre, tout (ou partie) de ces applicatifs ne sont plus disponibles.
- **SB_PRA_26** L'impact des modifications sur l'ensemble des briques du SI de la DGI et des interfaces avec les partenaires doit être le plus faible possible.
- **SB_PRA_27** Les applicatifs du périmètre du PRA doivent être installés et personnalisés conformément aux règles de production Copernic via un serveur de déploiement et en s'appuyant sur les outils DGI (global-tools, confmanager...).
 - **27.a** Les procédures d'installation prennent en compte l'installation initiale lors de la mise en production et l'installation à chaud (baies déconnectées) lors de la reprise d'activité.
- **SB_PRA_28** L'installation des socles techniques (serveurs, équipements de réseau...) et leur personnalisation est, sauf exception, automatisée.
 - **28.a** Toutes les images nécessaires à l'installation des socles techniques sont archivées dans le référentiel6 de production.

- **SB_PRA_29** Les règles de nommage sont respectées et si nécessaires adaptées pour tenir compte du PRA.

Quartier de la feuille de route

Quartier	N°	Libellé de la tâche
Infrastructure de secours	SB_PRA_8	Le plateau informatique de secours constitue au sein du CIP un site de production Copernic conforme aux principes généraux en la matière : sécurité physique et des accès, servitudes, exploitation à distance... Il est constitué des éléments suivants :
		- 8.a - infrastructure partagée du site de Noisiel ;
		- 8.b - sous-ensemble de la plate-forme technique de l'ISIQ limité aux équipements des applicatifs et services transverses du périmètre du PRA ;
		- 8.c - équipements dédiés au secours, hors plate-forme d'ISIQ, comme par exemple les baies de réplication.
	SB_PRA_9	Les équipements de la plate-forme informatique d'ISIQ hors périmètre du PRA (applicatifs ou services qui ne sont pas ou pas encore en production sur le SPS, équipements propres aux activités d'ISIQ ...) ne font pas partie du plateau informatique de secours.
	SB_PRA_10	Le plateau informatique de secours reconstitue l'intégralité du périmètre du PRA (mêmes vues applicative et technique), avec une stricte identité (mêmes équipements, mêmes quantités, mêmes règles de montage et câblage...) pour les applicatifs et les services transverses.
	SB_PRA_11	La reconstitution de la production sur la plate-forme technique d'ISIQ dans le périmètre du PRA se fait par réinstallation sur tous les équipements des socles techniques et paquets applicatifs avec reprise des configurations et personnalisations de production.
Serveurs d'applications	SB_PRA_25	L'ensemble des applicatifs de la salle 3 du SPS est traité comme un site externe au PRA, avec la particularité d'être (potentiellement) détruit en cas de sinistre déclenchant le PRA :
		- 25.a en cas d'exercice l'accès et la continuité de production doivent être assurés ;
		- 25.b en cas de sinistre, tout (ou partie) de ces applicatifs ne sont plus disponibles.
	SB_PRA_27	Les applicatifs du périmètre du PRA doivent être installés et personnalisés conformément aux règles de production Copernic via un serveur de déploiement et en s'appuyant sur les outils DGI (global-tools, confmanager...).
		- 27.a Les procédures d'installation prennent en compte l'installation initiale lors de la mise en production et l'installation à chaud (baies déconnectées) lors de la reprise d'activité.
Transfert de fichiers		
Annuaire des services		
Administration, supervision et exploitation	POS81 *	Administration et supervision
	POS82 *	Socle de pilotage de la production : SPPC

(*) POS SECURITE - 050186_Spec_Dispositif_Secours_COPERNIC_V1.03.doc

Architecture de sauvegardes / restaurations sur le site de secours

Règles relatives aux données

- **SB_PRA_30** En cas de sinistre, les pertes de données critiques sont nulles ou minimales.
- **SB_PRA_31** Toutes les données des applicatifs et des services transverses jugées critiques sont centralisées sur les baies de disques répliquées en synchrone sur les baies du site de secours dédiées à cet usage.
- **SB_PRA_32** Les modalités d'activation de la réplication des données (avant ou après le démarrage effectif de la production) minimisent les risques de pertes ou de corruption des données.
- **SB_PRA_33** Il conviendra de définir pour chaque applicatif ou module applicatif Copernic, les données critiques à répliquer ainsi que le point de synchronisation intra et inter applicatifs permettant de garantir une cohérence globale du SI lors d'une reprise d'activité sur le site de secours avec ces données répliquées.

Règles relatives au dispositif de réplication des données

- **SB_PRA_34** Le dispositif de réplication doit assurer en cas de sinistre l'absence de perte de données critiques ou bien une perte minimale.
- **SB_PRA_35** Le redémarrage en secours est fiable notamment grâce à une cohérence globale des données répliquées sur les baies du site de secours.
- **SB_PRA_36** La perte du processus de réplication quelque soit le type d'incident ne bloque pas les accès aux baies locales en lecture et en écriture. Les impacts sur la production en cas d'incidents du dispositif de réplication sont minimaux. Une très haute résilience du dispositif est requise.
- **SB_PRA_37** La maîtrise du dispositif de réplication par les exploitants de la DGI est assurée par la mise en œuvre de procédures et d'outils de production (administration, exploitation, supervision, «capacity planning»).
- **SB_PRA_38** La solution retenue pour le dispositif de réplication est évolutive pour tenir compte de la croissance prévisible du périmètre applicatif et des volumes des données.
- **SB_PRA_39** Le dispositif de réplication respecte les principes et règles de l'architecture technique et de l'exploitation du programme Copernic notamment ceux concernant la séparation des zones Agents et Usagers, la télé exploitation depuis la zone 4 d'administration ou la sécurité des flux inter zones.
- **SB_PRA_40** Le dispositif de réplication ne nécessite pas de la part des maîtrises d'ouvrage métiers de développements applicatifs spécifiques, mais peut imposer certaines contraintes ou limites d'exploitation.
- **SB_PRA_41** Les baies de réplication sont des baies de production destinées à assurer :
 - **41.a** la réplication des données en temps normal,
 - **41.b** la production en cas d'exercice ou de sinistre.
- **SB_PRA_42** S'il y a lieu le dispositif de réplication inter site s'applique prioritairement à toute de la réplication.
- **SB_PRA_43** Les baies d'une même paire de réplication sont identiques : même modèle, même firmware, mêmes parity group...

- **SB_PRA_44** Les baies d'une zone (Agent ou Usager) n'hébergent que des données pour cette zone.
- **SB_PRA_45** L'administration des baies est centralisée sous la responsabilité d'un seul GTS (et d'un seul G2A s'il y a lieu). Il n'y a par zone qu'un seul réseau d'administration (T-ADMZ ou ADMZ) des baies.

Quartier de la feuille de route

Quartier	N°	Libellé de la tâche
Réplication des données critiques	SB_PRA_31	Toutes les données des applicatifs et des services transverses jugées critiques sont centralisées sur les baies de disques répliquées en synchrone sur les baies du site de secours dédiées à cet usage.
	SB_PRA_33	Pour chaque applicatif ou module applicatif, les données critiques à répliquer ainsi que le point de synchronisation intra et inter applicatifs doivent permettre de garantir une cohérence globale du SI lors d'une reprise d'activité sur le site de secours avec ces données répliquées.
	SB_PRA_41	Les baies de réplication sont des baies de production destinées à assurer :
		- 41.a la réplication des données en temps normal, - 41.b la production en cas d'exercice ou de sinistre.
	SB_PRA_43	Les baies d'une même paire de réplication sont identiques : même modèle, même firmware, mêmes parity group...
	SB_PRA_44	Les baies d'une zone (Agent ou Usager) n'hébergent que des données pour cette zone.
	SB_PRA_45	L'administration des baies est centralisée sous la responsabilité d'un seul GTS (et d'un seul G2A s'il y a lieu). Il n'y a par zone qu'un seul réseau d'administration (T-ADMZ ou ADMZ) des baies.
Sauvegarde sur support physique		

Infrastructure nécessaire aux opérations de secours

Règles relatives aux utilisateurs (agents, usagers, partenaires)

- **SB_PRA_20** Les utilisateurs sont prévenus de l'indisponibilité des applicatifs lors des opérations de bascule d'un site sur un autre par des procédures mises en œuvre dans les portails d'accès.
- **SB_PRA_21** Les modifications demandées aux utilisateurs (usagers, agents, partenaires) pour accéder aux applicatifs après bascule d'un site sur l'autre sont minimales.

Règles relatives aux exploitants (GTS, G2A, PSN, Assistance)

- **SB_PRA_22** Les exploitants jouent leurs rôles habituels (pour les opérations de reconstitution comme pour celles d'exploitation, d'administration ou d'assistance) ; les modifications des procédures d'exploitation courantes sont minimales.
- **SB_PRA_23** En cas d'exercice, les accès d'administration des applicatifs du SPS doivent être assurés, avec éventuellement des procédures particulières⁵ pour ceux du périmètre du PRA et sans changement de procédure pour ceux hors périmètre du PRA (salle 3 du SPS).

- **SB_PRA_24** Les GTS et G2A peuvent accéder simultanément aux deux sites via le réseau d'administration.

Quartier de la feuille de route

Quartier	N°	Libellé tâche
Pilotage du déploiement	SB_PRA_28	L'installation des socles techniques (serveurs, équipements de réseau...) et leur personnalisation est, sauf exception, automatisée.
		- 28.a Toutes les images nécessaires à l'installation des socles techniques sont archivées dans le référentiel ⁶ de production.
Pilotage du déploiement Exploitation en secours	SB_PRA_22	Les exploitants jouent leurs rôles habituels (pour les opérations de reconstitution comme pour celles d'exploitation, d'administration ou d'assistance) ; les modifications des procédures d'exploitation courantes sont minimales.
	SB_PRA_23	En cas d'exercice, les accès d'administration des applicatifs du SPS doivent être assurés, avec éventuellement des procédures particulières ⁵ pour ceux du périmètre du PRA et sans changement de procédure pour ceux hors périmètre du PRA (salle 3 du SPS).
	SB_PRA_24	Les GTS et G2A peuvent accéder simultanément aux deux sites via le réseau d'administration.

Architecture des réseaux locaux sur le site de secours

Règles relatives aux réseaux d'accès aux sites de production et de secours

- **SB_PRA_12** Le plan d'adressage IP et plus généralement les paramètres réseaux du site de production sont, en cas d'exercice ou de sinistre, réaffectés au site de secours.
- **SB_PRA_13** L'accès au site de secours pour les utilisateurs et les applicatifs (hors liens spécifiques) est assuré par l'opérateur avec :
 - **13.a** réaffectation des adresses IP publiques de l'accès internet du SPS à l'accès internet du CIP ;
 - **13.b** annonce des adresses IP du site SPS dans le réseau Rubis3 par les routeurs du CIP.
- **SB_PRA_14** Les solutions de bascule relatives aux liens spécifiques (extension DMZ, liens partenaires, flux spécifiques...) minimisent les impacts sur les applicatifs.
- **SB_PRA_15** Les réseaux (applicatifs et d'administration) de la salle 3 du SPS sont séparés de ceux des salles Agents et Usagers.
- **SB_PRA_16** En cas d'exercice tous les accès (applicatifs et administration) aux applicatifs de la salle 3 du SPS doivent être assurés sans changement.
- **SB_PRA_17** Le réseau d'administration (ADMZ ou TADMZ) de tout équipement en production⁴ n'est accessible à distance qu'à partir de la zone d'administration du site effectivement en production.
- **SB_PRA_18** Les réseaux d'administration (ADMZ ou TADMZ) des équipements des salles Agents et Usagers du SPS sont toujours accessibles à partir de la zone d'administration du SPS que le site soit en production ou non.
- **SB_PRA_19** Les réseaux d'administration (ADMZ ou TADMZ) des équipements de l'ISIQ du périmètre du PRA sont accessibles aux exploitants pendant les exercices pour assurer la reconstruction de la production.

Quartier de la feuille de route

Quartier	N°	Libellé de la tâche
Réseaux applicatifs	SB_PRA_12	Le plan d'adressage IP et plus généralement les paramètres réseaux du site de production sont, en cas d'exercice ou de sinistre, réaffectés au site de secours.
	SB_PRA_15	Les réseaux (applicatifs et d'administration) de la salle 3 du SPS sont séparés de ceux des salles Agents et Usagers.
	SB_PRA_16	En cas d'exercice tous les accès (applicatifs et administration) aux applicatifs de la salle 3 du SPS doivent être assurés sans changement.
Basculement réseau	SB_PRA_13	L'accès au site de secours pour les utilisateurs et les applicatifs (hors liens spécifiques) est assuré par l'opérateur avec :
		- 13.a réaffectation des adresses IP publiques de l'accès internet du SPS à l'accès internet du CIP ;
	SB_PRA_14	- 13.b annonce des adresses IP du site SPS dans le réseau Rubis3 par les routeurs du CIP.
Réseaux d'administration	SB_PRA_15	Les réseaux (applicatifs et d'administration) de la salle 3 du SPS sont séparés de ceux des salles Agents et Usagers.
	SB_PRA_17	Le réseau d'administration (ADMZ ou TADMZ) de tout équipement en production ⁴ n'est accessible à distance qu'à partir de la zone d'administration du site effectivement en production.
	SB_PRA_18	Les réseaux d'administration (ADMZ ou TADMZ) des équipements des salles Agents et Usagers du SPS sont toujours accessibles à partir de la zone d'administration du SPS que le site soit en production ou non.
	SB_PRA_19	Les réseaux d'administration (ADMZ ou TADMZ) des équipements de l'ISIQ du périmètre du PRA sont accessibles aux exploitants pendant les exercices pour assurer la reconstruction de la production.

Points d'accès sur le réseau longue distance ;

Quartier de la feuille de route

Quartier	N°	Libellé de la tâche
Passerelles d'accès sécurisé	POS73 *	Sécurisation PAS

(*) POS SECURITE - 050186_Spec_Dispositif_Secours_COPERNIC_V1.03.doc

Architecture sécurisée pour les accès Internet entrant et sortant sur le site de secours

Quartier de la feuille de route

Quartier	N°	Libellé de la tâche
Portail		
Annuaire		

Quartier	N°	Libellé de la tâche
Sécurité	POS71 *	Gestion des traces (IGT)
	POS72 *	Signature électronique (ADP)
Adhésion et inscription		

(*) POS SECURITE - 050186_Spec_Dispositif_Secours_COPERNIC_V1.03.doc

From:
<http://www.ouarte.garden/> - dwndoc

Permanent link:
<http://www.ouarte.garden/doku.php?id=secours:is-tva:pca-p1-ddl1-4-c1-specifications>

Last update: 2025/02/19 10:59

