

CENTRE NATIONAL D'ETUDES SPATIALES**SOCLE TECHNIQUE****CENTRE NATIONAL D'ETUDES SPATIALES****DIRECTION DU SYSTEME D'INFORMATION**Réf. : **STSI-PR-SI-2010.3883-CNES**

Edition	: 01	Date	: 15/02/2010
Révision	: 05	Date	: 20/11/2013
MT	: X	Code diffusion	: E

**REGLES D'INTEGRATION ET D'UTILISATION
DES SERVICES D'INFRASTRUCTURE DU CNES**

Rédigé par : Groupe de travail DSI	le :	
Accepté par : François JOCTEUR MONROZIER DSI/IS/SY	le : 20/11/2013	
Pour application : Thierry DEMANGEOT DSI/IS/D	le : 17/12/2013	

C N E S

SOCLE TECHNIQUE

Edit. : 01

Date : 15/02/2010

Rév. : 05

Date : 20/11/2013

Référence : STSI-PR-SI-2010.3883-CNES

Page : i.2

BORDEREAU D'INDEXATION

CONFIDENTIALITE :
DLMOTS CLES : socle technique, système d'information, règles, exigences,
cadre de cohérence technique, infrastructures

TITRE DU DOCUMENT :

Règles d'intégration et d'utilisation des services d'infrastructure du CNES.

AUTEUR(S) : Groupe de travail DSI

RESUME : Ce document décrit les règles d'intégration des applications aux infrastructures du CNES. Ce document s'adresse en particulier aux Titulaires et aux responsables de projets dans le cadre du développement ou évolution d'un système « sol ». Il a pour objectif de définir un cadre de cohérence technique permettant de rationaliser et homogénéiser les pratiques relatives à l'utilisation des infrastructures du CNES.

DOCUMENTS RATTACHES : Ce document vit seul.

LOCALISATION :
DSI/IS (Portail DSI)

VOLUME : 1

NBRE TOTAL DE PAGES : 19

DOCUMENT COMPOSITE : N

LANGUE : FR

DONT PAGES LIMINAIRES : 9

NBRE DE PAGES SUPPL. : 0

GESTION DE CONF. : NG

RESP. GEST. CONF. :

CAUSE D'EVOLUTION : Création du document.

CONTRAT : Néant

SYSTEME HOTE :

Microsoft Word 10.0 (10.0.6838)

C : \Program Files\GDOC\GDOC\MODELES_GDOC\ModeleGDOC.dot

Version GDOC : v4.2.0.3b

Base projet : D : \DONNEES\GDOC_BasesLocales\AI\Secretariat_DSI_EA

C N E S

SOCLE TECHNIQUE

Edit. : **01**

Date : **15/02/2010**

Rév. : **05**

Date : **20/11/2013**

Référence : **STSI-PR-SI-2010.3883-CNES**

Page : i.3

DIFFUSION INTERNE

Nom	Sigle	Bpi	Observations
G. CAMPAN	DSI/D Sous-directions de la DSI Services de la DSI		
M. PIRCHER	DCT/D Sous-directions de la DCT Services de la DCT		
M. EYMARD	DLA/D Sous-directions de la DLA Services de la DLA		
V. ZORZI	DCS//SI		

DIFFUSION EXTERNE

Nom	Sigle	Observations

C N E S
SOCLE TECHNIQUE

 Edit. : **01**

 Date : **15/02/2010**

 Rév. : **05**

 Date : **20/11/2012**

 Référence : **STSI-PR-SI-2010.3883-CNES**

Page : 1

MODIFICATION

Ed.	Rév.	Date	Référence, Auteur(s), Causes d'évolution
01	00	15/02/2010	STSI-PR-SI-2010.3883-CNES Groupe de travail DSI Création du document.
01	01	06/07/2010	Prise en compte des actions/ recommandations issues du complément de revue Socle Technique : <ul style="list-style-type: none"> - A9 => Document rebaptisé « Règles d'intégration des applications aux infrastructures du CNES ». - A37 => Suppression du paragraphe sur le Poste de travail. - A38 => Intégration des modifications fournies par l'IPJ.
01	02	15/09/2010	Prise en compte des actions issues du complément de revue du Socle Technique (simplification et liens vers les FDS).
01	03	24/10/2011	Mise à jour du §2.1.2.1, §2.1.3.1, §2.2, §2.3, §2.4, §2.4.2, §2.4.3, §2.5.6, §2.5.7
01	04	19/07/2012	Mise à jour des références aux FDS et des modalités d'accès aux FDS. Suppression du service WINS et MIMESWEEPER (remplacé par Forefront intégré au service de messagerie). Ajout d'une vue d'ensemble au §1.1. Simplification de la description de certains services. Ajout en document de référence de la FDS WAF et de la FDS GESTINF. Ajout des chapitres concernant la gestion des OS Linux et Windows.
01	05	20/11/2013	Mise à jour du §GUID et DR4.(remplacement de SAFIR par GUID) - P. Espagnol Suppression du service GUR (arrêt du service)

SOMMAIRE

GLOSSAIRE ET LISTE DES PARAMÈTRES AC & AD	3
1 GÉNÉRALITÉS	4
1.1 OBJET DU DOCUMENT	4
1.2 DÉFINITIONS	5
1.3 DOCUMENTS DE RÉFÉRENCE	5
1.4 DOCUMENTS APPLICABLES	6
2 SERVICES D'INFRASTRUCTURE	7
2.1 SERVICES D'ANNUAIRE	7
2.1.1 Annuaire Technique Active Directory	7
2.1.2 LDAP Admin Unix	7
2.1.3 LDAP Extranet	7
2.1.4 Annuaire d'entreprise GUID	8
2.1.5 Annuaire Unix/Linux (NIS)	8
2.2 SERVICE DE MESSAGERIE	9
2.2.1 Messagerie d'entreprise	9
2.3 NOMMAGE ET SYNCHRONISATION	10
2.3.1 DNS	10
2.3.2 NTP	10
2.4 SERVICES DE RELAYAGE ET DE FILTRAGE APPLICATIF	10
2.4.1 PACCI Relais	10
2.4.2 Proxy Web	11
2.4.3 WAF (Web Applications Firewall)	11
2.5 SERVICES DE GESTION ET ADMINISTRATION D'INFRASTRUCTURE ...	12
2.5.1 Catalogue des produits et logiciels PIC (Asset Center)	12
2.5.2 Outil de Téléaction (LDMS)	12
2.5.3 Supervision des Systèmes Informatiques	13
2.5.4 Gestion des OS Linux (SPACEWALK)	13
2.5.5 Gestion des OS Windows (KMS, WSUS)	13
2.5.6 Plateforme Administration / Supervision / Métrologie des réseaux ..	14
2.5.7 Plateforme de Test Réseau (PATH)	15
2.6 SERVICES SSI	15
2.6.1 Antivirus Sophos	15
2.6.2 EPO	16
2.6.3 IGC Scytale	16

C N E S

SOCLE TECHNIQUE

Edit. : **01**

Date : **15/02/2010**

Rév. : **05**

Date : **20/11/2012**

Référence : **STSI-PR-SI-2010.3883-CNES**

Page : 3

GLOSSAIRE ET LISTE DES PARAMETRES AC & AD

SI	Système d'Information.
DDC	Demande de Changement : Document fourni dans le cadre de la mise en production d'un « produit » dont l'objectif est de décrire les actes techniques attendus de la part de l'infogérant.
FDS	Fiche Descriptive de Service.

Liste des paramètres AC :

Liste des paramètres AD :

1 GENERALITES

1.1 OBJET DU DOCUMENT

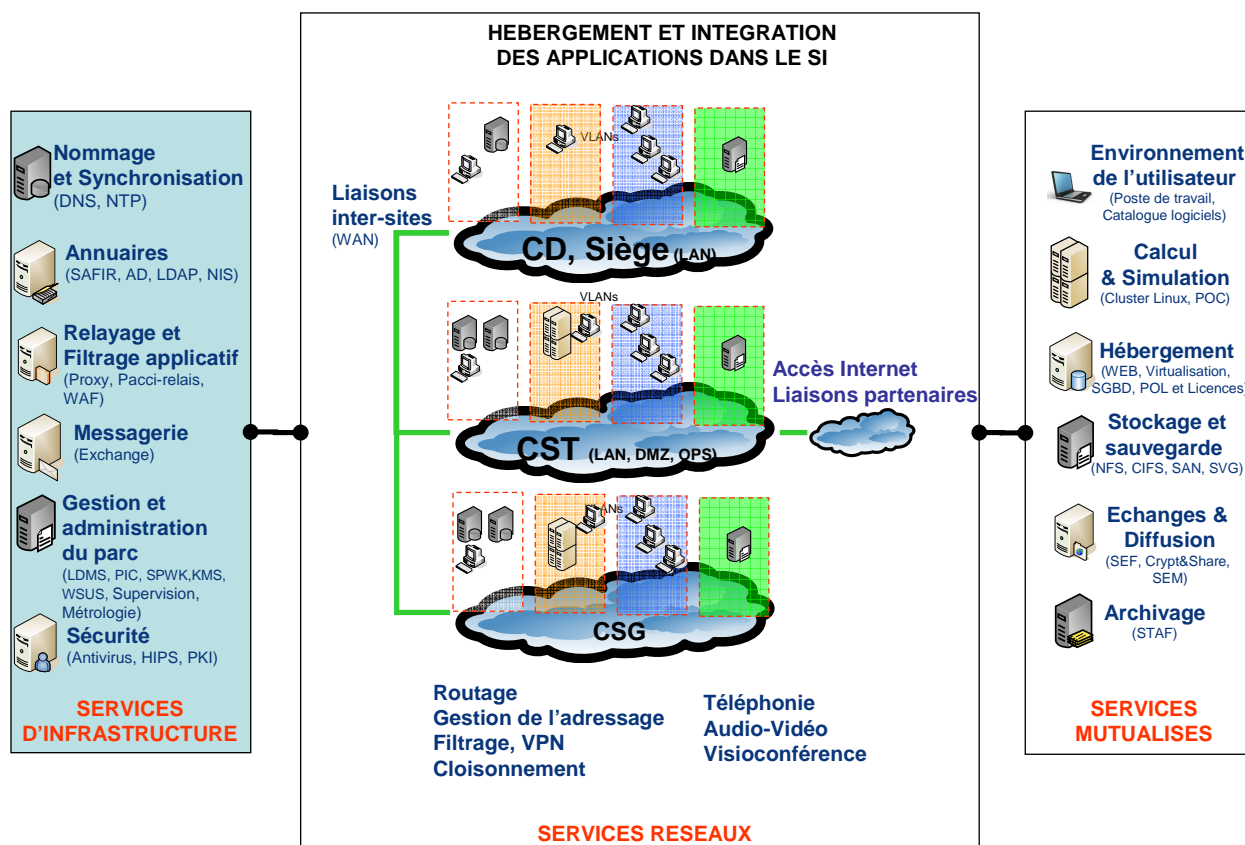
Ce document s'adresse en particulier aux Titulaires et aux responsables de projets dans le cadre du développement ou évolution d'un système « sol » devant s'interfacer avec un service d'infrastructure du SI, aux chargés d'affaires (CA) de la DSI, aux responsables d'exploitation (GA/GT) et à tout autre utilisateur potentiel des services d'infrastructure du SI, à qui il fournit un référentiel des informations techniques et bonnes pratiques d'utilisation de ces services.

Le cadre d'application du socle technique, et donc du présent document, est défini dans le document [DA1] et [DA2].

La procédure à suivre concernant les demandes d'utilisation des services mutualisés est décrit dans la documentation propre au service mutualisé concerné (cf. Portail > CNES Pratique). Ces documents sont rappelés dans le présent document.

La procédure concernant les demandes d'évolution des services d'infrastructure est décrite dans le document [DA3].

Le schéma suivant présente une vue d'ensemble des services du SI et le périmètre adressé dans ce document :



1.2 DEFINITIONS

Les définitions suivantes s'appliquent à tout le document.

Composant : Sous partie du système relativement autonome et qui rend un service de base. Par exemple un routeur, un serveur, etc. sont des composants. Un composant est en général indépendant des autres par l'alimentation électrique ou les accès réseau. Le terme composant est un terme qui peut aussi être utilisé de manière générique pour tout élément faisant parti d'un système.

Composant réseau : Composant qui assure des fonctions de communication.

Composant informatique : Composant qui assure des traitements informatiques, par opposition au composant réseau.

Interface : Désigne la frontière entre le système et un autre système du SI (les interfaces internes au système ne sont pas concernées).

Système : Au sens « système informatique », ensemble de moyens matériels et logiciels destinés à rendre un service du SI. Pour le CA, il s'agit du système dont il a assuré la réalisation, et dont il gère la mise en production. Le système est donc la cible sur laquelle les exigences du présent document s'appliquent.

Sous-système : Sous-partie du système.

Titulaire : On désigne par Titulaire, l'industriel (développeur, intégrateur, ...) en charge de la réalisation du produit concerné.

1.3 DOCUMENTS DE REFERENCE

L'accès à la documentation de référence est faite au travers du portail (CNES Pratique > Socle technique > Règles d'utilisation et d'intégration).

DR1	FDS du Service AD MCO-FDS-ACTD-2009.24895-CNES
DR2	FDS du service LDAP Admin Unix MCO-FDS-LDPU-2010.3095-CNES
DR3	FDS du service LDAP Extranet MCO-FDS-LDPE-2009.26523-CNES
DR4	FDS du service d'annuaire d'entreprise MCO-FDS-GUID-2012.02717-CNES
DR5	FDS du service de messagerie MCO-FDS-MESS-2010.1250-CNES
DR6	FDS du service NIS MCO-FDS-NIS-2010.3531-CNES
DR7	FDS du service DNS MCO-FDS-DNS-2010.967-CNES
DR8	FDS du service NTP

C N E S

SOCLE TECHNIQUEEdit. : **01**Date : **15/02/2010**Rév. : **05**Date : **20/11/2012**Référence : **STSI-PR-SI-2010.3883-CNES**

Page : 6

	MCO-FDS-NTP-2010.3507-CNES
<i>DR9</i>	FDS du service Pacci-relais
	MCO-FDS-PCCR-2010.1097-CNES
<i>DR10</i>	FDS du Service Proxy
	MCO-FDS-PROXHT-2009.24869-CNES
<i>DR11</i>	Guide d'intégration du service WAF
	DSI/EA/AR-2009.13
<i>DR12</i>	FDS du Service PİC
	MCO-FDS-PIC-2010-1133-CNES
<i>DR13</i>	FDS du service LDMS
	MCO-FDS-LDMS-2009.27718-CNES
<i>DR14</i>	FDS du service de supervision
	MCO-FDS-SPRV-2010.587-CNES
<i>DR15</i>	FDS du service d'administration des réseaux du CNES
	MCO-FDS-ADMRZ-2010.7102-CNES
<i>DR16</i>	FDS du service PATH
	MCO-FDS-ADMRZ-2010.7102-CNES
<i>DR17</i>	FDS du service SOPHOS
	MCO-FDS-SOPH-2009.24925-CNES
<i>DR18</i>	FDS du service EPO
	MCO-FDS-EPO-2009.24926-CNES
<i>DR19</i>	FDS du service SCYTALE
	MCO-FDS-SCYT-2009.24928-CNES
<i>DR20</i>	FDS du service WAF
	MCO-FDS-WAF-2012.10290-CNES
<i>DR21</i>	FDS du service de gestion de l'infrastructure systèmes informatiques
	MCO-FDS-GESTINF-2012.3146-CNES

1.4 DOCUMENTS APPLICABLES

<i>DA1</i>	APPLICATION DU SOCLE TECHNIQUE STSI-PR-SI-2010.8844-CNES
<i>DA2</i>	PROCEDURES DE GESTION DU SOCLE TECHNIQUE STSI-PR-SI-2010.6702-CNES
<i>DA3</i>	CCM DSI Traitement des DM DSI DSI-SQ-PR-30

2 SERVICES D'INFRASTRUCTURE

2.1 SERVICES D'ANNUAIRE

2.1.1 Annuaire Technique Active Directory

2.1.1.1 Description du service

Active Directory est l'annuaire Microsoft LDAP de référence au CNES. Il est utilisé pour les comptes machines Windows, les comptes Utilisateurs « bureautique », « groupes » et exchange (messagerie d'entreprise des clients CNES).

2.1.1.2 Règles d'intégration et documentation

Toutes les informations nécessaires sont rassemblées dans la FDS du Service AD (cf. [DR1]).

2.1.2 LDAP Admin Unix

2.1.2.1 Description du service

L'objet de ce service est d'offrir un service central pour les comptes d'administration. Cela répond à une préconisation de la sécurité. Le but est de simplifier le changement des mots de passe des administrateurs en centralisant la base de données de ces comptes. L'autre avantage sur une solution de type NIS est la capacité à encapsuler le trafic LDAP dans un flux SSL (auquel cas on parle de LDAPS) afin de garantir une meilleure sécurité.

2.1.2.2 Règles d'intégration et documentation

Toutes les informations nécessaires sont rassemblées dans la FDS du service LDAP Admin Unix (cf. [DR2]).

2.1.3 LDAP Extranet

2.1.3.1 Description du service

Le service LDAP EXTRANET est destiné aux services DSI ouverts sur internet, ayant besoin d'un système d'authentification pour ses utilisateurs.

Ce service est un service ancillaire offrant une gestion des comptes utilisateurs respectant les règles de gestion des mots de passe du CNES. Ce service est utilisé par le service SEF et le service WAF.

2.1.3.2 Règles d'intégration et documentation

Toutes les informations nécessaires sont rassemblées dans la FDS du service LDAP Extranet (cf. [DR3]).

2.1.4 Annuaire d'entreprise GUID

2.1.4.1 Description du service

GUID (Gestion Unifiée des Identités) est la solution de Gestion des Identités du CNES ; il maintient à jour les informations sur les salariés et les partenaires du CNES, et s'appuie sur des référentiels gérés par des tiers (locaux, structures) ou gérés par la solution (sociétés partenaires).

Il est alimenté par des logiciels producteurs de données de l'entreprise, et des vues métiers. Il alimente la majorité des applications du SI s'appuyant sur un référentiel d'utilisateurs.

GUID est un composant majeur du système d'information du CNES. Il intègre les informations relatives aux agents CNES et non CNES, ainsi que les informations administratives associées, telles que :

- structure
- téléphone
- localisation
- référence du contrat (prestataires / titulaires)
- date de fin d'activité
- adresse de messagerie

2.1.4.2 Règles d'intégration et documentation

Toutes les informations nécessaires sont rassemblées dans la FDS du service d'annuaire d'entreprise (cf. (DR4)).

2.1.5 Annuaire Unix/Linux (NIS)

2.1.5.1 Description du service

Le service NIS (pour Network Information Service) a pour objet d'assurer la gestion des utilisateurs en environnement Unix/Linux en mode centralisé (par opposition à la déclaration locale des utilisateurs sur chaque serveur).

2.1.5.1.1 Type d'utilisation

Service Commun	Service Dédié
Contrôle d'accès centralisé : Service disponible pour toute nouvelle installation de serveur ou de poste de travail / station de travail sur le réseau	Contrôle d'accès centralisé : Service pouvant être mis à disposition sur étude à toute nouvelle plate-forme sur des réseaux spéciaux ou dédiés.

C N E S

SOCLE TECHNIQUEEdit. : **01**Date : **15/02/2010**Rév. : **05**Date : **20/11/2012**Référence : **STSI-PR-SI-2010.3883-CNES**

Page : 9

CNES.	
	Conditions d'éligibilité :
Niveaux de Service associés :	Niveaux de Service associés :

Liste des services NIS communs :

- Un service NIS dédié au cluster de calcul linux-ci.
- Un service NIS dédié au cluster de calcul intensif AIX.
- Un service NIS dédié à tous les serveurs et stations de la DLA (Centre Spatial d'Evry).
- Un service NIS dédié aux serveurs Unix/Linux du domaine « Applications d'entreprise » en dehors du service Diapason qui dispose d'un autre NIS dédié.

2.1.5.2 Règles d'intégration et documentation

Toutes les informations nécessaires sont rassemblées dans la FDS du service NIS (cf. [DR6]).

2.2 SERVICE DE MESSAGERIE**2.2.1 Messagerie d'entreprise****2.2.1.1 Description du service**

Exchange est le système de messagerie d'entreprise Microsoft du CNES.

Exchange permet l'accès aux boîtes aux lettres via un client lourd outlook (MAPI), ou au travers de outlook web access (HTTP), ou depuis des clients Thunderbirds (POPs, IMAPs).

L'administration centralisée d'Exchange permet d'appliquer des stratégies, des règles d'utilisation de la messagerie (limite de boîtes aux lettres, limites de taille de messages, réplication des dossiers publics, etc.).

2.2.1.2 Règles d'intégration et documentation

Toutes les informations nécessaires sont rassemblées dans la FDS du service de Messagerie (cf. [DR5]).

2.3 NOMMAGE ET SYNCHRONISATION

2.3.1 DNS

2.3.1.1 Description du service

Ce service permet la résolution du nom d'une machine sur un réseau. L'association machine/adresse IP est référencée dans une base de données DNS.

L'architecture DNS du CNES est divisée en deux parties distinctes : le domaine « public » accessible depuis Internet et le domaine « privé » accessible uniquement depuis l'intranet CNES. Il n'y a pas d'échange de données concernant le domaine « cnes.fr » ou ses sous-domaines entre ces deux domaines.

2.3.1.2 Règles d'intégration et documentation

Toutes les informations nécessaires sont rassemblées dans la FDS du service DNS (cf. [DR7]).

2.3.2 NTP

2.3.2.1 Description du service

NTP (Network Time Protocol) est un protocole qui permet de synchroniser à travers un réseau informatique l'horloge locale d'une machine sur une référence souhaitée.

2.3.2.2 Règles d'intégration et documentation

Toutes les informations nécessaires sont rassemblées dans la FDS du service NTP (cf. [DR8]).

2.4 SERVICES DE RELAYAGE ET DE FILTRAGE APPLICATIF

2.4.1 PACCI Relais

2.4.1.1 Description du service

Ce dispositif est un relai applicatif pour les protocoles suivants : FTP, telnet, X11. Il assure le relayage générique de n'importe quel port TCP (actuellement ssh et sqlnet sur dérogation). Il est également possible de faire un ping ou un traceroute udp depuis Pacci-Relais.

Le relayage FTP est principalement utilisé, notamment par les chaînes de traitement des projets.

2.4.1.2 Règles d'intégration et documentation

Toutes les informations nécessaires sont rassemblées dans la FDS du service Pacci Relais (cf. [DR9]).

2.4.2 Proxy Web

2.4.2.1 Description du service

Le proxy Web est un dispositif de relayage des protocoles Web (http et https) pour les flux sortants. Il agit également comme un élément de protection des postes de travail du CNES :

- Seule l'adresse du proxy est connue des sites consultés; donc les postes de travail ne peuvent pas être repérés sur Internet.
- Antivirus : Les pages Internet consultées étant demandées par le proxy Web, il peut s'assurer que les sites consultés ne contiennent pas de virus avant de transmettre les informations à l'utilisateur
- Filtrage : Il permet au CNES de choisir les sites que l'ont peut consulter depuis son poste de travail. Certains sites peuvent être dangereux (piratage informatique, virus) ou tout simplement illégaux. Le CNES peut donc interdire leur accès pour protéger les utilisateurs, le système d'information du CNES et bien entendu, le CNES lui-même.
- Conservation des traces : Le code des postes des télécommunications et loi de lutte contre le terrorisme imposent la conservation des logs des accès Internet effectués depuis le CNES. Ainsi, le CNES a obligation de conserver 1 an les traces des accès Internet effectués. Ces éléments sont contrôlés par la déclaration à la CNIL effectués par le CNES et les accès à ces informations sont strictement réglementés : les administrateurs des boîtiers ne peuvent lire ces informations que dans un cadre très stricte.

2.4.2.2 Règles d'intégration et documentation

Toutes les informations nécessaires sont rassemblées dans la FDS du service PROXY (cf. [DR10]).

2.4.3 WAF (Web Applications Firewall)

2.4.3.1 Description du service

Le service WAF est un dispositif de « reverse proxy » entre les flux des clients sur Internet et les serveurs applicatifs hébergés au CNES. Ces serveurs applicatifs sont situés sur les DMZ externes du CNES (PACCI) ou sur le réseau interne (ROC) selon les spécifications de sécurité de l'application.

2.4.3.2 Règles d'intégration et documentation

Toutes les informations nécessaires sont rassemblées dans le document [DR11].

2.5 SERVICES DE GESTION ET ADMINISTRATION D'INFRASTRUCTURE

2.5.1 Catalogue des produits et logiciels PIC (Asset Center)

2.5.1.1 Description du service

L'ensemble du Parc informatique sous responsabilité de la DSI est géré par l'outil Asset Manager de HP.

La base parc regroupe les matériels et logiciels des sites de Métropoles et est centralisée sur Toulouse.

2.5.1.2 Règles d'intégration et documentation

Toutes les informations nécessaires sont rassemblées dans la FDS du service PIC (cf. [DR12]).

2.5.2 Outil de Téléaction (LDMS)

2.5.2.1 Description du service

LanDesk Management Suite (LDMS) est l'outil de télé-action mis en œuvre au CNES. L'objectif actuel de LDMS est de télé-distribuer, télé-inventorier et télé-assister le poste de travail du CNES. A terme des fonctions de gestion de patch et de déploiement d'OS seront mises en œuvre.

LDMS assure :

- Télédistribution d'application.
- Télé-inventaire.
- Téléassistance.
- Gestion et l'application de patch applicatif et de sécurité.

2.5.2.2 Règles d'intégration et documentation

Toutes les informations nécessaires sont rassemblées dans la FDS du service LDMS (cf. [DR13]).

2.5.3 Supervision des Systèmes Informatiques

2.5.3.1 Description du service

Nagios est le service de supervision des moyens centralisés de l'infrastructure du CNES métropole. Cet outil permet d'afficher les alertes identifiées dans les journaux d'évènements, ou par mails. La résolution des incidents est traitée par le biais de fiches réflexes. 2 modes d'utilisations sont possibles, NRPE (flux sortant) et NSCA (flux entrant).

Nagios est une application sous licence GPL permettant la surveillance système et réseau. Elle permet de surveiller les hôtes et les services souhaités, alertant lorsque ces derniers ne sont plus dans leur état nominal.

Nagios est modulaire et se décompose selon les briques logicielles suivantes :

- Un moteur applicatif permettant d'ordonnancer les tâches de supervision.
- Une interface WEB, qui permet d'avoir une vue d'ensemble du SI et de ces anomalies.

Des plugins, qui peuvent être utilisés tels que ou bien être modifiés en fonction des besoins de supervision souhaités au sein du SI.

2.5.3.2 Règles d'intégration et documentation

Toutes les informations nécessaires sont rassemblées dans la FDS du service de supervision (cf. [DR14]).

2.5.4 Gestion des OS Linux (SPACEWALK)

2.5.4.1 Description du service

Le serveur Spacewalk permet de gérer de manière centralisée tous les systèmes sous l'OS RedHat, CentOS ou Suse 11. Les serveurs situés sur le PACCI ne sont pas gérés de manière centralisée. Le serveur Spacewalk peut gérer des clients sur des OS SA et non SA.

2.5.4.2 Règles d'intégration et documentation

Toutes les informations nécessaires sont rassemblées dans la FDS du service de gestion de l'infrastructure système Informatique (cf. [DR21]).

2.5.5 Gestion des OS Windows (KMS, WSUS)

2.5.5.1 Description du service

Le service KMS permet d'activer automatiquement à l'installation d'un nouveau serveur Windows, la licence de ce serveur. Régulièrement, les serveurs viennent se ré-enregistrer auprès du serveur KMS pour valider à nouveau leur clé de licence. Un serveur d'administration Windows permet également de centraliser les logs des OS Windows.

Le service WSUS permet de gérer la mise à jour des patches logiciels pour les serveurs Windows.

2.5.5.2 Règles d'intégration et documentation

Toutes les informations nécessaires sont rassemblées dans la FDS du service de gestion de l'infrastructure système Informatique (cf. [DR21]).

2.5.6 Plateforme Administration / Supervision / Métrologie des réseaux

2.5.6.1 Description du service

La plateforme d'administration est le centre névralgique de pilotage et de contrôle du réseau d'entreprise, du réseau d'opérations et des réseaux annexes. Elle concentre toutes les fonctions pour la gestion des configurations, des événements, de la supervision.

Ce service permet de superviser en temps réel la totalité des équipements du parc réseau.

FONCTION 1 (critique) : L'accès aux équipements réseau et la gestion de configuration.

Accès aux équipements réseau :

- Ouverture d'une session sur les équipements réseau en consultation ou en modification pour réaliser une opération de configuration.
- L'accès peut-être réalisé à distance (telnet SSH, SNMP...) ou bien en local (port console série ou usb).

La gestion de configuration :

La gestion de configuration est avant tout un *ensemble de pratiques*. Elle permet :

- de contrôler l'évolution du système.
- d'archiver les états successifs des configurations.
- de récupérer ou télécharger une configuration.
- de comparer plusieurs fichiers de configuration.

FONCTION 2 : AAA (Authentification, Autorisation, Accounting)

- Assurer les 3A afin de garantir une authentification forte et centralisée des connexions des exploitants sur les équipements réseau.
- Traçabilité nominative des actions sur une période déterminée par la SSI centrale CNES.

FONCTION 3 : Supervision Réseau

Un système de Supervision Réseau a pour principale fonction d'aider les équipes d'exploitation réseau dans leur travail quotidien :

- Cartographier les réseaux physiques.
- Surveiller en quasi temps-réel l'état des réseaux (polling périodique des équipements).
- Détecter les pannes et localiser le ou les moyens en cause, identifier la nature de la panne.
- Disposer d'un historique lisible des événements survenus sur les réseaux durant les dernières heures (I.E collecteur et reporter d'alarmes / Traps).

FONCTION 4 : Métrologie Réseau

CNES

SOCLE TECHNIQUEEdit. : **01**Date : **15/02/2010**Rév. : **05**Date : **20/11/2012**Référence : **STSI-PR-SI-2010.3883-CNES**

Page : 15

4.1 : Outil de collecte de compteurs sur les équipements réseau et d'archivage de ces informations sur le long terme.

Un module permet généralement d'analyser ces données, de générer des alertes (dépassement de seuils), de fournir des rapports, de fournir des tendances...

4.2 : Sondes : utilisé pour remonter des informations détaillées sur les flux qui transitent sur les réseaux. Décomposition des trames couches 2 à 7 (par VLAN, QOS, Protocole, source/destination, ...).

FONCTION 5 : Gestion des traces (messages SYSLOG)

5.1 : Archivage des traces

5.2 : Outils d'analyse et de génération de rapports de traces:

2.5.6.2 Règles d'intégration et documentation

Toutes les informations nécessaires sont rassemblées dans la FDS du service d'administration des réseaux du CNES (cf. [DR15]).

2.5.7 Plateforme de Test Réseau (PATH)**2.5.7.1 Description du service**

La DSI dispose d'une plate-forme de pré-production représentative des équipements « réseaux » en production permettant de valider les changements de configuration majeurs dans le cadre des projets ou changements majeurs.

2.5.7.2 Règles d'intégration et documentation

Toutes les informations nécessaires sont rassemblées dans la FDS du service PATH (cf. [DR16]).

2.6 SERVICES SSI**2.6.1 Antivirus Sophos****2.6.1.1 Description du service**

L'antivirus Sophos est utilisé dans le cadre de la protection contre les virus en mode bouclier et scan de nuit des serveurs de l'infrastructure du CNES. La plateforme Sophos, permet les mises à jour des bases, moteurs, signatures, des serveurs pris en charge. Elle permet aussi de gérer les serveurs par des stratégies définies.

2.6.1.1.1 Type d'utilisation

CNES

SOCLE TECHNIQUE

Edit. : 01

Date : 15/02/2010

Rév. : 05

Date : 20/11/2012

Référence : STSI-PR-SI-2010.3883-CNES

Page : 16

Service Commun	Service Dédié
Intégrité des données : Service disponible pour toute nouvelle installation de serveur sur le réseau CNES.	Intégrité des données : Service pouvant être mis à disposition sur étude à toute nouvelle installation de serveur sur des réseaux spéciaux ou dédiés.
	Conditions d'éligibilité :
Niveaux de Service associés :	Niveaux de Service associés :

2.6.1.2 Règles d'intégration et documentation

Toutes les informations nécessaires sont rassemblées dans la FDS du service SOPHOS (cf. [DR17]).

2.6.2 EPO

2.6.2.1 Description du service

EPO permet d'assurer la protection antivirus locale des postes de travail Windows et de superviser de façon centralisée leur exploitation.

2.6.2.2 Règles d'intégration et documentation

Toutes les informations nécessaires sont rassemblées dans la FDS du service EPO (cf. [DR18]).

2.6.3 IGC Scytale

2.6.3.1 Description du service

Le système SCYTALE (Service de CrYpTage, Autorité de certification, et infrastructure de gestion de cLEs) est composé de :

- Une IGC : Infrastructure technique et organisationnelle permettant de produire et gérer les certificats.
- Des moyens de protections : Dispositifs utilisant les certificats produits par l'IGC afin de sécuriser des informations, connections, applications, authentications, etc.

La mission de l'IGC est de permettre de gérer les certificats numériques distribués par le CNES pour les environnements de production et de pré-production :

L'infrastructure à clé publique SCYTALE permet de délivrer des certificats pour sécuriser les éléments suivants :

- Certificats de chiffrement et de signature utilisateur pour chiffrer et signer des documents et des mails.

C N E S

SOCLE TECHNIQUE

Edit. : **01**

Date : **15/02/2010**

Rév. : **05**

Date : **20/11/2012**

Référence : **STSI-PR-SI-2010.3883-CNES**

Page : 17

- Certificats routeurs pour chiffrer et authentifier les communications du WAN du CNES.
- Certificats serveurs (SSL, LDAPS), afin de sécuriser les communications serveur-serveur et les communications client-serveur.
- Des certificats relai Sentinelle afin de sécuriser les protocoles applicatifs de HR-Access.
- Génération d'un OTP à partir d'un certificat pour l'authentification des nomades.
- Infrastructure d'authentification Radius via des serveurs Radius FreeRadius et IAS de Microsoft.
- Infrastructure VPN via un serveur ISA 2006 (bientôt abandonnée).
- Infrastructure de sécurisation HR-Access via des boitiers Arkoon A210.
- Infrastructure des moyens de protection via l'outil Security Box Suite

2.6.3.2 Règles d'intégration et documentation

Toutes les informations nécessaires sont rassemblées dans la FDS du service SCYTALE (cf. [DR19]).