

Cadre de Cohérence Technique (CCT)	4
1.1.1 Centre de données (Datacenter)	5
1.1.2 Baie (Rack)	7
1.1.3 Commutateur écran-clavier-souris (Keyboard-video-monitor switch - KVM)	9
1.1.4 Unité de distribution électrique (Power distribution unit - PDU)	10
1.1.5 Système de transfert statique (Static transfert system - STS)	11
1.1.10 Informatique en nuage (Cloud computing)	12
1.2.1 Câblage structuré (Structured Cabling)	14
1.2.4 Service réseau DNS (DNS network service)	15
1.2.6 Serveur NTP	17
1.2.7 Commutateur réseau (Switch)	19
1.2.8 Zone démilitarisée (DMZ)	21
1.2.9 Répartition de charge (Load balancing)	25
1.3.1 Serveur physique (Server)	26
1.3.2 Poste de travail (Workstation)	29
1.3.4 Equipement de stockage	32
1.4.1 Système d'exploitation serveur	33
1.4.2 Terminal mobile (Mobile phone)	36
1.4.3 Système d'exploitation poste de travail	38
1.4.4 Poste de rebond virtuel (VPR)	40
1.4.5 Poste d'administration virtuel (VPC)	41
1.4.6 Conteneur logiciel	42
1.4.7 Application matérielle (Appliance)	43
1.5.1 Hyperviseur (Hypervisor)	44
1.5.2 Système_d'exploitation_serveur_Linux_(Operating_system_Linux_server)	46
1.5.3 Système d'exploitation serveur Windows (Operating System Windows Server)	48

1.5.4 Système d'exploitation poste utilisateur (Operating System User Workstation) _____	50
2.1.1 Authentification unique (Single sign-on, SSO) _____	52
2.1.2 Serveur mandataire inverse, SMI (Reverse proxy) _____	54
2.1.3 Serveur mandataire (Proxy server) _____	56
2.1.4 Protection antivirus des postes de travail (Workstation antivirus protection) _____	58
2.1.5 Protection antivirus des serveurs (Server antivirus protection) _____	60
2.1.6 Protection antipourriel des serveurs (Server antispam protection) _____	61
2.1.7 Scanner de vulnérabilité (Vulnerability scanner) _____	62
2.1.8 Chiffrement (Encryption) _____	64
2.3.1 Serveur web (Web server) _____	66
2.4.1 Serveur d'application (Application server) _____	69
2.4.2 Environnement d'exécution PHP (PHP runtime environment) _____	72
2.4.3 Environnement d'exécution JAVA (JAVA runtime environment) _____	74
2.4.4 Environnement d'exécution .NET (.NET runtime environment) _____	76
2.4.5 Serveur de relais de messagerie _____	78
2.4.6 Serveur de messagerie _____	80
2.5.1 Intégration de données (ETL) _____	82
2.6.1 Protection des données (RGPD) _____	83
2.6.2 Système de gestion de base de données, SGBD (Database management system) _____	84
2.6.3 Active directory (AD) _____	86
2.6.4 Annuaire LDAP _____	88
2.7.2 Gestion du code source _____	90
2.7.3 Gestion des anomalies _____	91
2.7.4 Environnement de développement intégré (IDE) _____	92
2.7.5 Qualité et sécurité du code source _____	93
2.7.6 Tests et intégration _____	95
2.8.1 Sauvegarde informatique _____	96

2.8.2 Accès à distance des prestataires (Provider remote access)	98
2.8.3 Gestion des environnements	99
2.8.4 Plan de continuité d'activité (Business continuity planning)	100
2.8.5 Exploitation et administration des serveurs	103
2.8.6 Accès à distance (Remote access)	105
2.8.7 Supervision Système	107
2.8.8 Gestion de logs serveurs	109

CADRE DE COHERENCE TECHNIQUE

Le cadre de cohérence technique (CCT) a pour but de fixer un cadre de référence pour la conception, la réalisation, l'hébergement et l'exploitation de tout système d'information mis en œuvre au sein du SNUM. Cet outil de standardisation commun est applicable à l'ensemble des acteurs des ministères économiques et financiers et doit répondre aux enjeux actuels, à savoir permettre à chacun de disposer d'un système d'information robuste, efficient, sécurisé, évolutif et à moindre coût.

Qu'est-ce que le cadre de cohérence technique (CCT) ?

Il constitue le cadre de référence pour toute personne désireuse de connaître les règles sur les différents composants du système d'information du SNUM. Ces règles sont formulées de manière à ce qu'elles renvoient à différents niveaux de préconisations, conformément à la *RFC 2119* (<https://www.ietf.org/rfc/rfc2119.txt>)' et décrites dans le tableau ci-dessous :

Niveau de préconisation	Description	Formulation de la règle
obligatoire	La règle est une exigence absolue.	Sujet + DOIT + verbe + complément
recommandé	La règle peut être ignorée après évaluation des conséquences tenant compte de circonstances particulières.	Sujet + DEVRAIT + verbe + complément
déconseillé	La règle est une interdiction qu'il est possible de ne pas suivre en maîtrisant bien les conséquences et dans des circonstances particulières.	Sujet + NE DEVRAIT PAS + verbe + complément
interdit	La règle est une interdiction absolue.	Sujet + NE DOIT PAS + verbe + complément
facultatif	La règle est facultative.	Sujet + PEUT + verbe + complément

Comment est structuré le cadre de cohérence technique (CCT) ?

Chaque rubrique du cadre de cohérence technique est catégorisée en fonction :

- du **thème abordé** (logiciels, matériels, réseaux ou services)
- du **bureau concerné** (BENA, BITS ou BPAN)



Qui est concerné par le cadre de cohérence technique (CCT) ?

Le cadre de cohérence technique (CCT) s'adresse :

- principalement aux **agents du service du numérique (SNUM)**,
- mais également aux **services informatiques des directions métiers** ainsi qu'aux **prestataires de service** en lien avec les agents du SNUM

Centre de données (Datacenter) version diffusable

Un **centre de données** (Datacenter) est un lieu regroupant des équipements constituant du système d'information d'une ou plusieurs entreprise(s) (ordinateurs centraux, serveurs, baies de stockage, équipements réseaux et de télécommunications, etc.). Il peut être interne et/ou externe à l'entreprise, exploité ou non avec le soutien de prestataires. Il fournit des services informatiques en environnement contrôlé (climatisation) et sécurité (système anti-incendie, contre le vol et l'intrusion, etc.), avec une alimentation d'urgence et redondante. (source : Wikipedia, 2023 (https://fr.wikipedia.org/wiki/Centre_de_données))

-  Termes privilégiés :**centre de données, centre de traitement de données, centre de traitement informatique, centre informatique, centre d'hébergement**
-  Equivalent étranger : **data center** (en), **data centre** (en), **data processing center** (en), **DPC** (en), **data processing centre** (en)

La version de base de cette rubrique est accessible [ici](#)

Sommaire

1

Contexte

2

Règles de base

3

Centre de données de référence

4

Contraintes juridiques et réglementaires

5

Contraintes techniques

Contexte

L'**offre d'hébergement informatique** proposées par le service du numérique (SNUM) s'appuient actuellement sur 3 centres de données répartis respectivement sur les sites géographiques de Bercy, Ivry et Osny.

Le site géographique de Bercy est le point central des interconnexions des sites distants des ministères économiques et financiers (MEF).

Centre de données	Fonction	Commentaire
BERCY	Site principal	Site principal d'hébergement.
IVRY	Site de secours	Site hébergeant les applications s'inscrivant dans le plan de continuité informatique.
OSNY	Site secondaire	Site hébergeant les nouvelles applications ne s'inscrivant pas dans le plan de continuité informatique .

Règles de base

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_1_1_1_001	Les centres de données de référence doivent respecter le standardministérielCentres d'hébergement (https://hfds-bercy.alize.finances.rie.gouv.fr/files/live/sites/hfds-bercy/files/r%c3%a9pertoires/S%c3%a9curit%c3%a9%20des%20syst%c3%a8mes%20d'information/documents/Textes%20de%20r%c3%a9f%c3%a9rences/190205_centres-hebergement_v1.1.pdf) en termes de zone protégée, de convention d'hébergement et de reporting.	Validé	01/07/2019	
1_1_1_1_002	Les directions et services d'administration centrale du secrétariat général des MEF peuvent bénéficier de l'une des offre de services d'hébergement suivantes : <ul style="list-style-type: none">Hébergement sans plan de continuité informatique et sans exploitation informatique (également appelé hébergement "sec non secours"),Hébergement sans plan de continuité informatique mais avec exploitation informatique réalisée par le SNUM également appelé hébergement "managé non secours"),Hébergement avec plan de continuité informatique mais sans exploitation informatique (appelé hébergement "sec secours"),Hébergement avec plan de continuité informatique et avec exploitation informatique réalisée par le SNUM (également appelé hébergement "managé secours").	Validé	01/07/2019	

Centre de données de référence

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_1_1_2_001	Les centres de données référencés ci-dessous doivent être utilisés pour l'hébergement des applications à destination des agents de l'administration centrale du secrétariat général des MEF : <ul style="list-style-type: none">les centres de données de Bercy et d'Ivry pour les hébergements avec plan de continuité informatique.le centre de données d'Osny pour les hébergements sans plan de continuité informatique,	Validé	14/04/2021	

Contraintes juridiques et réglementaires

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_1_1_3_001	La surveillance et la gestion des équipements informatiques localisés sur le site de Bercy (bâtiments Vauban et Sully) doivent se faire au travers du marché Prestations de surveillance et de gestion de plateaux informatiques et de biens .	Validé	01/07/2019	
1_1_1_3_002	Le service d'hébergement sans exploitation informatique proposé aux directions et services de l'administration centrale du secrétariat général du ministère de l'économie, des finances et de la relance (MEFR) doit faire l'objet d'une convention de services signée entre le service du numérique (SNUM) et le bénéficiaire.	Validé	14/04/2021	
1_1_1_3_003	Le service d'hébergement proposé par la direction générale des droits directs et indirects (DGDDI) au travers du site d'Osny doit faire l'objet d'une convention de services signée entre la DGDDI et le service du numérique (SNUM).	Validé	30/11/2021	Portail support CID (https://datacenter.cid.douane.gouv.fr)

Contraintes techniques

Centre de données de Bercy

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_1_1_4_001	Les applications nécessitant un plan de continuité informatique (PCI) doivent être installées sur des serveurs à vocation applicative hébergées sur le site de Bercy.	Validé	01/07/2019	

Centre de données d'Ivry

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_1_1_4_101	Les applications nécessitant un plan de continuité informatique (PCI) doivent être secourues sur des serveurs à vocation applicative hébergés sur le site d'Ivry.	Validé	01/07/2019	

Centre de données d'Osny

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_1_1_4_201	Les applications exposées sur le réseau général (RG) ne nécessitant pas de plan de continuité informatique (PCI) doivent être installées sur des serveurs à vocation applicative hébergés sur le site d'Osny.	Validé	01/07/2019	
1_1_1_4_202	Les applications exposées sur le réseau interministériel de l'Etat (RIE) ne nécessitant pas de plan de continuité informatique (PCI) doivent être installées sur des serveurs à vocation applicative hébergés sur le site d'Osny.	Validé	01/07/2019	
1_1_1_4_203	Les applications exposées sur le réseau internet ne nécessitant pas de plan de continuité informatique (PCI) doivent être installées des serveurs à vocation applicative hébergés sur le site d'Osny.	Validé	30/11/2021	

Baie (Rack) version diffusable

Une **baie** (Rack) est une armoire très souvent métallique parfois à tiroirs mais généralement à glissières (ou rails) destinée à recevoir les boîtiers d'appareils, généralement électroniques, réseau ou informatiques de taille normalisée.

Les baies permettent d'optimiser l'encombrement, d'assurer la cohérence du câblage (ségrégation des tensions à risque par exemple), de mutualiser les systèmes d'alimentations et de refroidissement entre les équipements. Elles permettent également une maintenance facilitée du fait de leur modularité. Elles sont systématiquement utilisées dans les centres de données, pour les superordinateurs et les serveurs.

Différents secteurs industriels (télécommunications, ferroviaire, marine, etc.) possèdent leurs propres dimensions normalisées. Mais la norme des baies 19 pouces est réputée être la plus répandue : 19 pouces (48,26 cm) de largeur pour 17 pouces (43,18 cm) de profondeur.. (source : Wikipedia, 2024 (https://fr.wikipedia.org/wiki/Rack_19_pouces))

- ✓ Termes privilégiés : **baie**
- ✓ Equivalent étranger: **rack** (en)

La version de base de cette rubrique est accessible [ici](#)

Sommaire

- 1 Contexte
- 2 Règles de base
- 3 Solutions de référence
- 4 Contraintes juridiques et réglementaires
- 5 Contraintes techniques

Contexte

Les offres de baies proposées par le service du numérique (SNUM) s'appuient sur des **baies 19 pouces en métal grillagé**, permettant une meilleure ventilation entre la baie, le couloir chaud et le couloir froid, de façon à refroidir les différents équipements. Ces baies sont situées dans les centres de données du SNUM pour héberger différents types d'équipements au format rack (19 pouces) tels que :

- les unités de distribution électrique (PDU) ▪ les systèmes de transfert statique (STS) ▪ les commutateurs écran-clavier-souris (KVM)
- les équipements réseaux et télécommunications
 - les commutateurs réseaux
 - les répartiteurs de charge
- les équipements de sécurité (parefeux ...)
- les serveurs physiques
- les équipements de stockage
- les équipements de sauvegarde

Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_1_2_1_001	Les baies doivent être étiquetées et enregistrées dans l'outil de gestion de parc PROMETHEE (https://promethee-gestion.alize.finances.rie.gouv.fr/).	Validé	16/12/2022	

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_1_2_2_001	<p>Les nouvelles baies doivent être choisies parmi celles référencées dans la liste ci-dessous :</p> <ul style="list-style-type: none">▪ Baie réseau équipé 19 pouces - 24U - Modèle 1 (https://www.ugap.fr/achatpublic/baie-reseau-equipee-19-24u-lienk-600-x-600-mm-av-vitree-ar-pleine-tre-e-montee_3200249.html)▪ Baie réseau équipe 19 pouces - 24U - Modèle 2 (https://www.ugap.fr/achatpublic/baie-reseau-equipee-19-24u-lienk-600-x-600-mm-av-vitree-ar-pleine-tre-e-en-kit_3200250.html)▪ Baie réseau équipe 19 pouces - 24U - Modèle 2 (https://www.ugap.fr/achatpublic/baie-reseau-equipee-19-24u-lienk-600-x-600-mm-av-vitree-ar-pleine-tre-e-en-kit_3200251.html)▪ Baie réseau équipe 19 pouces - 24U - Modèle 4 (https://www.ugap.fr/achatpublic/baie-reseau-equipee-19-24u-lienk-600-x-800-mm-av-vitree-ar-pleine-tre-e-en-kit_3200252.html)	Validé	16/12/2022	

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_1_2_3_001	L'acquisition de nouvelles baies peut se faire auprès du marché UGAP "Offre LAN et WAN et prestations associées".	Validé	16/12/2022	N° de marché: 617036 Date de fin de validité: 19/01/2026

Contraintes techniques

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_1_2_4_001				

-
- La dernière modification de cette page a été faite le 25 février 2024 à 07:13.

Commutateur écran-clavier-souris (Keyboard-video-monitor switch - KVM)

version diffusable

Un **commutateur écran-clavier-souris** (KVM) est un commutateur qui permet de partager clavier, écran et souris entre plusieurs ordinateurs. (source : Wikipedia,2022 (https://fr.wikipedia.org/wiki/Commutateur_%C3%A9cran-clavier-souris))



- ✓ Termes privilégiés : **commutateur écran-clavier-souris** , **commutateur KVM**
- ✓ Equivalent étranger: **KVM switch** (en), **keyboard-video-mouse switch** (en)

La version de base de cette rubrique est accessible [ici](#)

Sommaire

- 1 Contexte
- 2 Règles de base
- 3 Solutions de référence
- 4 Contraintes juridiques et réglementaires ▪
- 5 Contraintes techniques

Contexte

Les offres de commutateur KVM du service du numérique (SNUM) s'appuient sur des commutateurs de type **DELL KVM DMPU2016-G01**.

Ces commutateurs KVM sont localisés dans les baies informatiques des centres de données de référence. Ils permettent de choisir l'équipement (de la baie informatique) que l'on souhaite contrôler et de commuter de l'un à l'autre en fonction des besoins.

⚠ Dans certaines baies informatiques, on peut également trouver des **commutateurs de type clavier-écran-souris (KMM)** en lieu et place des commutateurs KVM.

Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_1_3_1_001	Les commutateurs KVM doivent être étiquetées et enregistrées dans l'outil de gestion de parc PROMETHEE (https://promethee-gestion.alize.finances.rie.gouv.fr/).	Validé	16/12/2022	

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_1_3_2_001				

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_1_3_3_001	L'acquisition de nouveaux commutateurs KVM peut se faire auprès du marché UGAP "Offre LAN et WAN et prestations associées".	Validé	16/12/2022	

Contraintes techniques

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_1_3_4_001	Les commutateurs KVM doivent être au format rack 19 pouces (1U) de manière à être installées dans lesbaies des centres de données concernés.	Validé	16/12/2022	

• La dernière modification de cette page a été faite le 25 février 2024 à 07:13.

Unité de distribution électrique (Power distribution unit - PDU) version diffusable

Une **unité de distribution d'énergie** ou **unité de distribution d'alimentation** - également connu sous le nom anglais de power distribution unit (PDU) ou mains distribution unit (MDU) - est un dispositif équipé de plusieurs sorties permettant la distribution d'électricité, en particulier des serveurs montés en rack et des équipements de réseaux et de télécommunications, situé dans les centres de traitement de données.

Ces dispositifs (PDU) permettent une distribution fiable de l'énergie pour les dispositifs de puissance faible à moyenne, intégrés dans des baies informatiques monté soit en rack utilisant des « U » pour quantifier l'espace utilisé, ou attaché latéralement sur le montant d'un rack, cette dernière option ne nécessite aucun espace en termes de « U ». (source : Wikipedia, 2022 (https://fr.wikipedia.org/wiki/Unit%C3%A9_de_distribution_d%27%C3%A9nergie))



✓ Termes privilégiés : **Unité de distribution électrique**

✓ Equivalent étranger: **Power distribution unit** (en), **PDU** (en) La version de base de cette rubrique est accessible ici

Sommaire

- 1 Contexte
- 2 Règles de base
- 3 Solutions de référence
- 4 Contraintes juridiques et réglementaires
- 5 Contraintes techniques

Contexte

L'offre de services d'unités de distribution électrique proposée par le service du numérique (SNUM) s'appuie actuellement sur les équipements suivants :

- 4T766 / APC AP6022 PDU 16A de la société DELL
- 9306-RTP PDU16A de la société IBM

Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_1_4_1_001	Les unités de distribution électrique doivent être étiquetées et enregistrées dans l'outil de gestion de parc PROMETHEE (https://promethee-gestion.alize.finances.rie.gouv.fr/).	Validé	16/12/2022	

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_1_4_2_001	Les nouvelles unités de distribution électrique doivent être choisies parmi les modèles référencés dans la liste ci-dessous : <ul style="list-style-type: none">■ PDU Basique Eaton FlexPDU 1U (https://www.ugap.fr/achat-public/pdu-basique-eaton-flexpdu-1u-entree-c20-sortie-12c13-et-1c19-monophas_290773.html)■ PDU supervision globale Eaton EPDU Metered 1U (https://www.ugap.fr/achat-public/pdu-supervision-globale-eaton-epdu-metered-1u-entree-c20-sortie-12c13-monophas_2907741.html)■ PDU supervision et gestion Eaton EPDU Managed 1U (https://www.ugap.fr/achat-public/pdu-supervision-et-gestion-eaton-epdu-managed-1u-entree-c20-sortie-12c13-monophas_2907744.html&idCategorieVente=0)	Validé	16/12/2022	

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_1_4_3_001	L'acquisition d'unités de distribution électrique peut se faire au travers du marché UGAP "Offre onduleurs et solutions de protection et prestations associées".	Validé	16/12/2022	

Contraintes techniques

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_1_4_4_001	Les unités de distribution électrique doivent être au format rack 19 pouces (1U) de manière à être installées dans les baies des centres de données concernés.	Validé	16/12/2022	

Système de transfert statique (Static transfert system - STS) version diffusable

Un **système de transfert statique** est un système à courant alternatif autonome destiné à assurer la continuité de l'alimentation d'une charge par un transfert manuel ou automatique, avec ou sans coupure, à partir d'au moins deux sources indépendantes à courant alternatif. On parle également de système de transfert automatique (ATS).

(source : EN 62310-1:2005 (<https://standards.iteh.ai/catalog/standards/clc/8f0bdf31-f96c-40af-8ed2-d03c3eb7bd2d/en-62310-1-2005>))



- Termes privilégiés : **Système de transfert statique**
- Equivalent étranger: **Static transfert system** (en), **STS** (en)

La version de base de cette rubrique est accessible [ici](#)

Sommaire

- 1 Contexte
- 2 Règles de base
- 3 Solutions de référence
- 4 Contraintes juridiques et réglementaires
- 5 Contraintes techniques

Contexte

L'**offre de services de système de transfert statique** proposée par le service du numérique (SNUM) s'appuie actuellement sur les équipements suivants :

- ATS ASYS ATS 16A-230 (https://www.socomec.fr/sites/default/files/2020-11/ASYC_CATALOGUE---PAGES_2016-07_DCG142021_FR-FR.pdf)

Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_1_5_1_001	Les systèmes de transfert statique doivent être étiquetés et enregistrés dans l'outil de gestion de parc PROMETHEE (https://promethee-gestion.alize.finances.rie.gouv.fr/).	Validé	16/12/2022	

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_1_5_2_001	Les nouveaux systèmes de transfert statique doivent être choisis parmi celles référencées dans la liste ci-dessous : <ul style="list-style-type: none"> ATS Eaton ATS 16 Netpack - 6A (https://www.ugap.fr/achat-public/ats-eaton-ats-16-netpack-16-a-rackable-19-monophas-avec-carte-de-managementeseau_2907751.html) ATS Eaton ATS 30 Netpack - 8A (https://www.ugap.fr/achat-public/ats-eaton-ats-30-netpack-30-a-rackable-19-monophas-avec-carte-de-managementeseau_2907752.html) 	Validé	16/12/2022	

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_1_5_3_001	L'acquisition de systèmes de transfert statique peut se faire au travers du marché UGAP "Offre onduleurs et solutions de protection et prestations associées".	Validé	16/12/2022	

Contraintes techniques

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_1_5_4_001	Les systèmes de transfert statique doivent être au format rack 19 pouces (1U) de manière à être installées dans lesbaies des centres de donnéesconcernés.	Validé	16/12/2022	

Informatique en nuage (Cloud computing) version diffusable

L'**informatique en nuage** (cloud computing) correspond à l'accès à des services informatiques (serveurs, stockage, mise en réseau, logiciels) via internet (le "cloud" ou "nuage") à partir d'un fournisseur.(source : Wikipedia, 2023 (https://fr.wikipedia.org/wiki/Cloud_computing))

- Une **plateforme peut être qualifiée de cloud** si elle répond aux 5 caractéristiques suivantes :
- élasticité rapide, c'est-à-dire la capacité à redimensionner la plateforme en fonction de la charge, mutualisation des ressources (serveurs, réseaux, stockage, ...), mesure en permanence
 - du service (qui permet notamment la facturation à l'usage), accès au travers de mécanismes réseaux standards,
 - possibilité pour les utilisateurs d'être autonomes dans leur utilisation (à la demande, en self-service)

(source : National Institute of Standards and Technology (NIST))

Termes privilégiés :**informatique en nuage**

Equivalent étranger: **cloud computing** (en)

Sommaire

1

Contexte

2

Règles de base

3

Solution de référence

4

Contraintes juridiques et réglementaires


5

Contraintes techniques

Contexte

Les **offres d'hébergement informatique** proposées par le direction interministérielle du numérique de l'Etat (DINUM) se déclinent de la manière suivante :

- le "**Cloud interne**" (Cercle 1)
 - Deux offres de services IaaS conçues, hébergées, exploitées et surveillées par :
 - le ministère de l'intérieur (cloud PI), associé à un niveau de sécurité "diffusion restreinte"
 - le ministère de l'économie, des finances et de la relance (cloud NUBO (<https://portailnubo.dgfip.finances.rie.gouv.fr/>)) associé au standard de l'ANSSI SecNumCloud (https://www.ssi.gouv.fr/uploads/2014/12/secnumcloud_referentiel_v3.1_anssi.pdf)
 - Ces offres s'appuient sur le logiciel libre Openstack
- le "**Cloud externe**" (Cercle 3)
 - Une offre de service proposée dans le cadre de la convention UGAP/DAE d'informatique en nuage (IaaS et PaaS)

 Il convient de préciser que ces **offres d'hébergement distant** de type Cloud se distinguent des offres d'hébergement proposées par le service du numérique (SNUM).

Règles de base

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_1_10_1_001				

Solution de référence

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_1_10_2_001				

Contraintes juridiques et réglementaires

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_1_10_3_001	Le support relatif à la fourniture de prestations IaaS sur le cloud interne NUBO doit se faire sur la base d'une convention de services signée entre la DGFIP et le bénéficiaire.	Validé	30/11/2021	
1_1_10_3_002	Le support relatif à la fourniture de prestations IaaS ou PaaS sur le cloud externe doit se faire sur le marché "Achat de prestations Cloud Cercle 3 (https://www.ugap.fr/catalogue-marche-pu-blic/services-dinformatique-en-nuage-cloud-externe_103007.html#ancre_fournisseurs/)".	Validé	30/11/2021	

Contraintes techniques

Cercle 1 - le "cloud interne"

Cloud NUBO

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_1_10_4_001	Les applications hébergées sur le cloud interne NUBO peuvent s'interfacer avec les services mutualisés du service du numérique (SNUM) suivants : <ul style="list-style-type: none">▪ le service réseau DNS,▪ le service de sécurité PROXY,▪ le service de relais de messagerie (externe et interne)	Validé	14/04/2021	
1_1_10_4_002	Les bénéficiaires des applications hébergées sur le cloud interne NUBO doivent prendre en charge les services suivants : <ul style="list-style-type: none">▪ le service de sauvegarde et de restauration des données des serveurs,▪ le service de génération et de délivrance de certificats,▪ le service de supervision système.	Validé	14/04/2021	

Cercle 3 - le "cloud externe"

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_1_10_5_001	Le Cloud externe (Cercle 3) n'est accessible que sur dérogation accordée par la PSSI du service du numérique (SNUM).	Validé	09/02/2022	

Câblage structuré (Structured Cabling)

Le **câblage structuré** est l'ensemble des techniques, méthodes et normes permettant de réaliser l'interconnexion physique des différents locaux d'une entreprise, d'un centre de données ou d'une zone plus large (campus ou ville). On peut lister un ensemble de sujets concernant le câblage structuré :

- Connexions entrantes : là où un bâtiment est connecté au reste du monde ("arrivée télécom").
 - Salles d'équipements réseaux : là où sont connectés les équipements servant aux utilisateurs (serveurs par exemple).
 - Salles de télécommunication (ou Sous-répartiteur, Local Technique d'Etage, etc.) : là où l'interconnexion se fait entre le câblage vertical et le câblage horizontal.
 - Câblage vertical : tous les liens reliant les salles de télécommunications entre elles, ainsi que les bâtiments et les réseaux extérieurs.
 - Câblage horizontal : Lien entre les salles de télécommunications et chaque connecteur individuel dans les bureaux. ▪
- Composants utilisateur : câble de raccordement des équipements qui connectent l'utilisateur au câblage horizontal.

(source : Wikipedia, 2023 ([- ✓ Terme privilégié : **Câblage structuré**
- ✓ Equivalent étranger: **Structured Cabling** \(en\)](https://fr.wikipedia.org/wiki/C%C3%A2blage_structur%C3%A9#:~:text=Le%20c%C3%A2blage%20structur%C3%A9%20est%20l,large%20(campus%20ou%20ville).)))</p></div><div data-bbox=)

La version diffusable de cette rubrique est accessible ici

Sommaire

- 1 Contexte
- 2 Règles de base
- 3 Solutions de référence
- 4 Contraintes juridiques et réglementaires
- 5 Contraintes techniques

Contexte

L'**offre de services de câblage structuré** proposée par le service du numérique (SNUM) s'appuie sur du câble catégorie 6 (https://fr.wikipedia.org/wiki/C%C3%A2ble_cat%C3%A9gorie_6).



Règles de base

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_2_1_1_001				

Solutions de référence

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_2_1_2_001				

Contraintes juridiques et réglementaires

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_2_1_3_001	Les prestations de câblage informatiques peuvent se faire au travers du marché UGAP.	Validé	02/02/2024	Echéance du marché : septembre 2024

Contraintes techniques

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_2_1_4_001				

Récupérée de « [https://wiki.monportail.alize/cct/w/index.php?title=Câblage_structuré_\(Structured_Cabling\)&oldid=17353](https://wiki.monportail.alize/cct/w/index.php?title=Câblage_structuré_(Structured_Cabling)&oldid=17353) »

• La dernière modification de cette page a été faite le 25 avril 2024 à 16:09.

Le Domain Name System, généralement abrégé DNS, qu'on peut traduire en « système de noms de domaine », est le service informatique distribué utilisé pour traduire les noms de domaine Internet en adresse IP ou autres enregistrements. (source : Wikipedia, 2022 (https://fr.wikipedia.org/wiki/Domain_Name_System))

✓ Equivalent étranger: **Domain Name Server** (en), **name server** (en), **DNS Server** (en), **DNS name server** (en)

Contexte

- **Service DNS interne** à destination des applications exposées sur le réseau général,
- **Service DNS externe** à destination des applications exposées sur le réseau internet.

Enregistrement	Code IANA	RFC	Signification
A	1	RFC 1035 (http://data.iana.org/doc/html/rfc1035)	Etablissement d'une correspondance entre un nom DNS et une adresse IP (IPv4).
NS	2	RFC 1035 (http://data.iana.org/doc/html/rfc1035)	Délégation de la gestion d'une zone à un serveur de nom faisant autorité.
CNAME	5	RFC 1035 (http://data.iana.org/doc/html/rfc1035)	Etablissement d'une correspondance entre deux noms DNS
SOA	6	RFC 1035 (http://data.iana.org/doc/html/rfc1035)	Définition du serveur maitre du domaine.
MX	15	RFC 1035 (http://data.iana.org/doc/html/rfc1035)	Configuration pour une zone de DNS donnée des serveurs de relais de messagerie sous la forme d'un nom DNS.
SOA	16	RFC 1035 (http://data.iana.org/doc/html/rfc1035)	Stockage d'une chaîne de 1024 caractères max.

La version de base de cette rubrique est accessible [ici](#)

Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_2_4_1_001	Les services DNS de référence doivent respecter le standard ministériel Sécurisation des services DNS (https://hfdcs-bercy.alize.finances.rie.gouv.fr/files/live/sites/hfdcsbercy/files/r%20a9pertoires/S%20c%20curit%20c%20a920des%20syst%20c%20a8mes%20d'information/documents/Textes%20de%20r%20c%20a9f%20c%20a9rences/210203_stand-dns_v3.4.pdf).	Validé	09/02/2022	hors protocole DNSSEC
	1_2_4_1_002	Les services DNS de référence doivent être installés dans des versions à jour de correctif de sécurité.	Validé	09/02/2022	

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_2_4_2_001	Les serveurs DNS installés dans les baies des centres de données de référence doivent s'appuyer sur les modèles suivants : <ul style="list-style-type: none">▪ Appliances SOLIDserver 1100 pour les serveurs DNS internes exposés sur le RG▪ Appliances SOLIDserver 550 pour les serveurs DNS internes exposés sur le GAS▪ Appliances SOLIDserver 570 pour les serveurs DNS externes exposés sur le réseau internet.	Validé	09/02/2022	

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_2_4_3_001				

Contraintes techniques

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_2_4_4_001	Les services DNS interne et externe doivent être inscrits dans le plan de continuité informatique REMPART.	Validé	09/02/2022	

▪ La dernière modification de cette page a été faite le 25 février 2024 à 07:47.

Serveur NTP version diffusable

Un **serveur NTP** est un serveur permettant de synchroniser l'horloge d'un ordinateur avec celle d'un serveur de référence lié à une horloge atomique.

(source : Office québécois de la langue française, 2014 (http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26528971))

- ✓ Terme privilégié : **serveur NTP**
- ✓ Equivalent étranger: **NTP server** (en)

La version de base de cette rubrique est accessible [ici](#)

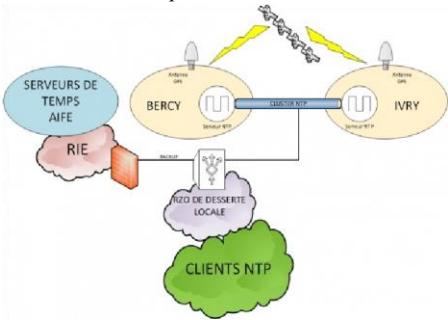
Sommaire

- 1 Contexte
- 2 Règles de base
- 3 Solutions de référence
- 4 Contraintes juridiques et réglementaires
- 5 Contraintes techniques

Contexte

Les offres de serveurs NTP proposées par le service du numérique (SNUM) s'appuient sur les équipements de la marque **Meinberg**.

L'architecture technique des serveurs NTP se décline de la manière suivante :



Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_2_6_1_001	Les serveurs NTP doivent être installés dans des versions à jour des correctifs de sécurité.	Validé	22/01/2020	
	1_2_6_1_002	Afin de garantir une homogénéité temporelle, les équipements suivants doivent récupérer leur référence de temps sur la solution NTP de référence: <ul style="list-style-type: none">▪ Les éléments actifs de réseaux,▪ Les équipements de sécurité,▪ Les serveurs,▪ Les postes clients du domaine solano.alize via le contrôleur de domaine,▪ Les badgeuses via leur serveur d'administration,▪ Les téléphones via les IPBX et les PABX.	Validé	22/01/2020	

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_2_6_2_001	Les serveurs NTP doivent s'appuyer sur les modèles suivants : <ul style="list-style-type: none">▪ Meinberg LANTIME M300 (https://www.meinbergglobal.com/english/products/rack-mount-lu-ntp-server.htm)	Validé	22/01/2020	

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_2_6_3_001	L'acquisition et la maintenance des serveurs NTP de référence se font hors marché.	Validé	22/01/2020	

Contraintes techniques

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_2_6_4_001	Les serveurs NTP installés dans les centres de données de référence doivent être intégrés au sein d'un cluster NTP.	Validé	22/01/2020	
	1_2_6_4_002	Les serveurs NTP Meinberg M300 (ne possédant pas de double alimentation) doivent être alimentés par un système de transfert de source (STS).	Validé	22/01/2020	
	1_2_6_4_003	Les interfaces réseaux des serveurs NTP doivent être déclinées de la manière suivante: <ul style="list-style-type: none">▪ Une interface réseau dédiée pour les flux d'administration,▪ Une interface réseau dédiée pour les flux de production et la mise en cluster,▪ Une interface réseau virtuelle allouée au cluster.	Validé	22/01/2020	
	1_2_6_4_004	Les interfaces réseaux physiques des serveurs NTP doivent être de type RJ45 et avoir un débit maximum de 100Mbits/s.	Validé	22/01/2020	
	1_2_6_4_005	Les protocoles activés sur l'interface d'administration du serveur NTP doivent être : <ul style="list-style-type: none">▪ le protocole HTTPS,▪ le protocole SSH.	Validé	22/01/2020	
	1_2_6_4_006	Le protocole activé sur l'interface de production du serveur NTP doit être : <ul style="list-style-type: none">▪ le protocole NTP.	Validé	22/01/2020	

Règles de nommage

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_2_6_5_001	Les serveurs NTP doivent respecter la règle de nommage suivante : <ul style="list-style-type: none">▪ HORLOGE-[Nom_du_centre_de_données] où [Nom_du-site_hébergeur]est le nom du centre de données (BERCY ou IVRY ou OSNY).	Validé	22/01/2020	

• La dernière modification de cette page a été faite le 25 février 2024 à 07:47.

Commutateur réseau (Switch) version diffusable

Un **commutateur réseau** (switch) est un équipement qui relie plusieurs segments (câbles ou fibres) dans un réseau informatique et de télécommunication et qui permet de créer des circuits virtuels. La commutation est un des deux modes de transport de trame au sein des réseaux informatiques et de communication, l'autre étant le routage.(source : wikipedia, 2023 (https://fr.wikipedia.org/wiki/Commutateur_r%C3%A9seau))

- ✓ Terme privilégié : **commutateur réseau**
- ✓ Equivalent étranger: **switch** (en)

Sommaire

- 1 Contexte
- 2 Règles de base
- 3 Commutateur réseau de référence
- 4 Contraintes juridiques et réglementaires
- 5 Contraintes techniques

Contexte

Les offres de services proposées par le service du numérique (SNUM) en termes de **commutateur réseau Ethernet** s'appuient sur les matériels **FlexFabric** et **FlexNetwork** de la société **HPE** .

On distingue trois types de commutateurs réseau (Source : "ANSSI,2016 (https://www.ssi.gouv.fr/uploads/2016/07/nt_commutateurs.pdf)") :

- **les commutateurs de cœur de réseau** : équipements directement reliés aux serveurs, aux commutateurs de distribution ou aux routeurs;
- **les commutateurs de distribution** : équipements regroupant le trafic venant des commutateurs de desserte afin de transmettre les données vers les équipements du cœur de réseau comme les commutateurs de réseau ou les routeurs;
- **les commutateurs de desserte ou d'accès** : équipements directement reliés aux prises réseau auxquelles se connectent les terminaux du système d'information (poste de travail, téléphones IP, ...).

C'est sur ces équipements que la configuration des réseaux locaux virtuels (VLAN) est réalisée.

Règles de base

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_2_7_1_001	Les commutateurs réseaux doivent être étiquetées et enregistrées dans l'outil de gestion de parc PROMETHEE (https://promethee-gestion.alize.finances.rie.gouv.fr/).	Validé	16/12/2022	
1_2_7_1_002	Les commutateurs réseaux de référence doivent être installés dans des versions à jour des correctifs de sécurité.	Validé	03/12/2019	

Commutateur réseau de référence

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_2_7_2_001	Les commutateurs réseaux installés dans les centres de données de référence doivent s'appuyer sur les modèles suivants : <ul style="list-style-type: none">▪ Commutateurs HPE FlexFabric 5700 (https://www.hpe.com/fr/fr/product-catalog/networking/networking-switches/pip.models.fixed-port-13-managed-ethernet-switches.7268889.html),▪ Commutateurs HPE FlexFabric 5710 (https://www.hpe.com/fr/fr/product-catalog/networking/networking-switches/pip.hpe-flexfabric-5710-switch-series.1010868971.html),▪ Commutateurs HPE FlexNetwork 5510 (https://www.hpe.com/fr/fr/product-catalog/networking/networking-switches/pip.fixed-port-13-managed-ethernet-switches.1008652960.html),▪ Commutateurs HPE FlexFabric 5940 (https://www.hpe.com/fr/fr/product-catalog/networking/networking-switches/pip.hpe-flexfabric-5940-switch-series.1009148840.html).	Validé	03/09/2019	

Contraintes juridiques et réglementaires

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_2_7_3_001	L'acquisition des commutateurs réseaux doit se faire au travers du marché "Solutions d'infrastructure LAN et WLAN et prestations associées"	Validé	03/12/2019	

Contraintes techniques

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_2_1_4_001	Les commutateurs réseaux doivent être au format rack 19 pouces (1U) de manière à être installés dans les baies des centres de données concernés.	Validé	16/12/2022	
	1_2_1_4_002	L'administration et l'exploitation des commutateurs réseaux de référence doivent se faire au travers du logiciel propriétaire HPE Intelligent Management Center (IMC) .	Validé	09/02/2022	
	1_2_1_4_003	Les ports cuivre 100/1000/10000 des commutateurs réseaux doivent être utilisés pour les connexions : <ul style="list-style-type: none"> des terminaux (endpoints) sur le Campus, des serveurs sur les commutateurs de trémie sur le centre de données. 	Validé	22/01/2020	
	1_2_1_4_004	Les ports SFP+ des commutateurs réseaux doivent être utilisés pour : <ul style="list-style-type: none"> la création de commutateurs logiques la connexion des serveurs sur les commutateurs Top of Rack nécessitant du 10 Go. 	Validé	22/01/2020	
	1_2_1_4_005	Les ports QSFP+ des commutateurs réseaux doivent être utilisés pour : <ul style="list-style-type: none"> la création de commutateurs logiques nécessitant du 40 Go. 	Validé	22/01/2020	
	1_2_1_4_006	Les commutateurs d'accès doivent utiliser la norme POE+ (https://fr.wikipedia.org/wiki/Alimentation_%C3%A9lectrique_par_c%C3%A2ble_Ethernet) pour l'alimentation des points d'accès wifi et des téléphones IP.	Validé	22/01/2020	
	1_2_1_4_007	Les commutateurs cœur de réseau doivent s'appuyer sur les protocoles suivants : <ul style="list-style-type: none"> VLAN (https://fr.wikipedia.org/wiki/R%C3%A9seau_local_virtuel), VRF (https://fr.wikipedia.org/wiki/Virtual_routing_and_forwarding), OSPF (https://fr.wikipedia.org/wiki/Open_Shortest_Path_First), RIP (https://fr.wikipedia.org/wiki/Routing_Information_Protocol), LLDP (https://fr.wikipedia.org/wiki/Link_Layer_Discovery_Protocol) et VRRP (https://fr.wikipedia.org/wiki/Virtual_Router_Redundancy_Protocol) 	Validé	22/01/2020	

Zone démilitarisée (DMZ) version diffusable

Une **zone démilitarisée** est un sous-réseau séparé du réseau local et isolé de celui-ci et d'Internet (ou d'un autre réseau) par un pare-feu. Ce sous-réseau contient les machines étant susceptibles d'être accédées depuis Internet, et qui n'ont pas besoin d'accéder au réseau local. Le but d'une DMZ est d'ajouter une couche de sécurité supplémentaire au réseau local (LAN) d'une organisation : un nœud de réseau externe ne peut accéder qu'à ce qui est exposé dans la DMZ, tandis que le reste du réseau de l'organisation est protégé par un parefeu (source : wikipedia,2023 ([https://fr.wikipedia.org/wiki/Zone_démilitarisée_\(informatique\)\)\)](https://fr.wikipedia.org/wiki/Zone_démilitarisée_(informatique)))))

✓ Terme privilégié : **zone démilitarisée**

✓ Equivalent étranger: **demilitarized zone** (en), **DMZ**(en)

La version de base de cette rubrique est accessible [ici](#)

Sommaire

- 1 Contexte
- 2 Règles de base
- 3 Solutions de référence
- 4 Contraintes juridiques et réglementaires
- 5 Contraintes techniques

Contexte

Le site de Bercy est segmenté en plusieurs zones réseaux logiques :

- Une **DMZ Web** contenant :
 - les serveurs mandataires inverses (SMI) et les serveurs d'authentification unique (SSO)
 - des serveurs applicatifs (qui doivent progressivement être déplacés vers la DMZ Data une fois interfacés avec les serveurs mandataires inverses (SMI))
- Une **DMZ Data** contenant :
 - les serveurs de base de données,
 - les annuaires LDAP,
 - les serveurs applicatifs (interfacés avec les serveurs mandataires inverses ou les serveurs d'authentification unique)
- Une **DMZ Fichiers** contenant :
 - les serveurs mutualisés de fichiers utilisés par des applications ayant des contraintes fortes en termes de volumétrie,
- Une **DMZ Service** permettant aux serveurs des autres DMZ d'accéder :
 - aux serveurs NTP,
 - aux serveurs DNS.
- une **DMZ Messagerie** contenant :
 - les serveurs de relais de messagerie externes.
- une **DMZ RIE** exposée sur le RIE contenant :
 - les serveurs de relais de messagerie,
 - les serveurs Anael,

Le site d'Osny est segmenté en plusieurs zones réseaux logiques :

- Une zone mutualisée contenant les serveurs intranet de développement du service du numérique (SNUM)
- Une zone mutualisée contenant les serveurs intranet de recette et de production du service du numérique (SNUM)
- Une zone dédiée contenant les serveurs intranet d'infrastructure du service du numérique (SNUM)
- Des zones dédiées contenant les serveurs intranet de certaines directions et services.
- Une zone mutualisée contenant les serveurs internet du service du numérique (SNUM) Chaque

zone réseau logique du centre de données d'Osny est constitué :

- d'une **DMZ Load-Balancing** contenant les répartiteurs de charge
- d'une **DMZ Frontale** contenant les serveurs mandataires inverses (SMI)
 - Remarque : Cette DMZ n'existe pas pour les 2 zones mutualisées contenant les serveurs intranet du service du numérique (SNUM)
- d'une **DMZ Back-Office** contenant les serveurs à vocation applicative (serveur web, serveur d'application, serveur d'indexation, serveur de base de données, serveur de fichiers...)
- d'une **DMZ SGBD** contenant les serveurs mutualisés de base de données ORACLE et SQL Server et utilisés par des applications ayant des contraintes fortes en termes de volumétrie.
- d'une **DMZ Fichiers** contenant les serveurs mutualisés de fichiers et utilisés par des applications ayant des contraintes fortes en termes de volumétrie.

Règles de base

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_2_8_1_001	Les flux applicatifs ne doivent pas être ouverts entre les zones situées sur le centre de données d'Osny sauf pour les serveurs de base de données mutualisés.	Validé	10/09/2020	Ajout d'une exception
1_2_8_1_002	Les serveurs des zones situées sur le centre de données d'Osny doivent s'appuyer sur un re pour accéder au réseau internet. Seuls les flux applicatifs HTTP, HTTPS sur les ports standards et une liste blanche d'URL sont autorisés.	Validé	18/05/2020	
1_2_8_1_003	Les applications d'une même direction faisant l'objet d'un hébergement sec (https://monalize.alize/sites/Alize/accueil/vie-quotidienne/hebergement-informatique/mon-service-souhaite-beneficier.html) ou d'un hébergement managé (https://monalize.alize/sites/Alize/accueil/vie-quotidienne/hebergement-informatique/mon-service-souhaite-beneficier.html) doivent se trouver dans la même zone du centre de données d'Osny.	Validé	18/05/2020	

Solutions de référence

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_2_8_2_001				

Contraintes juridiques et réglementaires

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_2_8_3_001				

Contraintes techniques

Site d'Osny

Site d'Osny - DMZ Load-Balancing

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_2_8_4_001	Les accès applicatifs via le réseau internet et le réseau interministériel de l'Etat (RIE) doivent transiter par la DMZ Load-Balancing pour attaquer les VIP hébergées sur les répartiteurs de charge.	Validé	09/02/2022	

Site d'Osny - DMZ Frontale

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_2_8_4_051	La DMZ Frontale située sur lesite d'Osny doit être utilisée pour héberger : <ul style="list-style-type: none">les serveurs mandataires inverses (SM) mutualisés.	Validé	03/09/2019	
1_2_8_4_052	Les flux applicatifs entrants autorisés de la DMZ Frontale située sur lesite d'Osny doivent être basés sur : <ul style="list-style-type: none">Le protocole HTTP (port 80) redirigé vers le protocole HTTPS (port 443),Le protocole HTTPS (port 443).	Validé	03/09/2019	
1_2_8_4_053	Les flux applicatifs sortants autorisés de la DMZ Frontale située sur lesite d'Osny doivent être basés sur : <ul style="list-style-type: none">le protocole HTTPS (port 443),le protocole LDAP,le protocole LDAPS.	Validé	18/05/2020	
1_2_8_4_054	Les flux applicatifs sortants de la DMZ Frontale située sur laite d'Osny ne peuvent être dirigés que vers : <ul style="list-style-type: none">la DMZ Back-Office située sur lesite d'Osny.	Validé	03/09/2019	
1_2_8_4_055	Les applications avec des utilisateurs dont l'origine est le réseau intranet doivent passer par un serveur mandataire inverse (SM) spécifique.	Validé	18/05/2020	
1_2_8_4_056	Les applications avec des utilisateurs dont l'origine est le réseau RIE ou mixte (RIE et réseau intranet) doivent passer par un serveur mandataire inverse (SMI) distinct.	Validé	18/05/2020	

Site d'OSNY- DMZ Back-Office

1_2_8_4_101	La DMZ Back-Office située sur le site d'Osny doit être utilisée pour héberger les serveurs à vocation applicative exposés sur : <ul style="list-style-type: none"> le réseau général (RG), le réseau interministériel de l'Etat (RIE). 	Validé	03/09/2019	
1_2_8_4_102	Les flux applicatifs entrants autorisés de la DMZ Back-Office située sur le site d'Osny doivent être basés sur : <ul style="list-style-type: none"> le protocole HTTPS (port 443). 	Validé	03/09/2019	
1_2_8_4_103	Les flux applicatifs sortants de la DMZ Back-Office située sur le site d'Osny doivent être dirigés uniquement vers les DMZ suivantes : <ul style="list-style-type: none"> La DMZ SGBD située sur le site d'Osny, La DMZ Fichiers située sur le site d'Osny, Le Réseau général (RG) , La DMZ Data située sur le site d'Osny. 	Validé	03/09/2019	

Site d'Osny - DMZ SGBD

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_2_8_4_151	La DMZ SGBD située sur le site d'Osny doit être utilisée pour héberger les serveurs à vocation applicative (serveurs SGBD) exposés sur : <ul style="list-style-type: none"> le réseau général (RG), le réseau interministériel de l'Etat (RIE) si l'une des conditions suivantes est vérifiée : <ul style="list-style-type: none"> la base de données est Oracle, la base de données est PostgreSQL et si : <ul style="list-style-type: none"> la taille de la base de données est supérieure à 100Go, l'utilisation de la RAM de la machine virtuelle > 64Go, la base de données est commune à plusieurs serveurs. 	Validé	03/09/2019	
1_2_8_4_152	Les flux applicatifs entrants autorisés de la DMZ SGBD située sur le site d'Osny doivent être basés sur : <ul style="list-style-type: none"> le protocole TCP pour les systèmes de bases de données de référence. 	Validé	22/01/2020	
1_2_8_4_153	Les flux applicatifs entrants autorisés de la DMZ SGBD située sur le site d'Osny doivent provenir de : <ul style="list-style-type: none"> de la DMZ Back-Office (située dans la même zone que la DMZ Data) du site d'Osny. 	Validé	18/05/2020	

Site d'Osny - DMZ Fichiers

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_2_8_4_201	La DMZ Fichiers située sur le site d'Osny doit être utilisée pour héberger les serveurs à vocation applicative (serveurs de fichiers) exposés sur : <ul style="list-style-type: none"> le réseau général (RG), le réseau interministériel de l'Etat (RIE) si l'une des conditions suivantes est vérifiée : <ul style="list-style-type: none"> l'espace de fichiers est supérieur à 100Go, l'espace de fichiers est partagée avec plusieurs serveurs. 	Validé	03/09/2019	
1_2_8_4_202	Les flux applicatifs entrants autorisés de la DMZ Fichiers située sur le site d'Osny doivent être basés sur : <ul style="list-style-type: none"> le protocole NFS pour les partages de fichiers sous Linux, le protocole SMB pour les partages de fichiers sous Microsoft Windows. 	Validé	22/01/2020	

Site de Bercy

Site de Bercy - DMZ Web

1_2_8_5_001	<p>La DMZ Web située sur le Site de Bercy doit être utilisée pour héberger :</p> <ul style="list-style-type: none"> ▪ les serveurs mandataires inverses (SMI), ▪ les serveurs d'authentification unique (SSO) , ▪ les serveurs à vocation applicative en accès direct (sans passer par les serveurs mandataires inverses ou les serveurs d'authentification unique). <p>exposés sur :</p> <ul style="list-style-type: none"> ▪ le réseau internet. 	Validé	22/01/2020	
1_2_8_5_002	<p>Les flux applicatifs entrants autorisés de la DMZ Web située sur le site de Bercy doivent être basés sur :</p> <ul style="list-style-type: none"> ▪ le protocole HTTPS (port 443). 	Validé	22/01/2020	
1_2_8_5_003	<p>Les flux applicatifs sortants autorisés de la DMZ Web doivent être redirigés uniquement vers les DMZ suivantes :</p> <ul style="list-style-type: none"> ▪ la DMZ Data du site de Bercy, ▪ la DMZ Fichiers du site de Bercy. 	Validé	22/01/2020	

Site de Bercy - DMZ Data

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_2_8_5_051	<p>La DMZ Data située sur le site de Bercy doit être utilisée pour héberger :</p> <ul style="list-style-type: none"> ▪ les serveurs à vocation applicative, ▪ les serveurs d'annuaire (LDAP) <p>exposés sur :</p> <ul style="list-style-type: none"> ▪ le réseau internet ▪ le réseau internet ou le réseau général (RG) 	Validé	18/05/2020	
1_2_8_5_052	<p>Les flux applicatifs entrants autorisés de la DMZ Data située sur le site de Bercy doivent être basés sur :</p> <ul style="list-style-type: none"> ▪ le protocole HTTPS (port 443), ▪ les protocoles LDAP et LDAPS sur les serveurs d'annuaire, ▪ le protocole TCP pour les SGBD. 	Validé	18/05/2020	

Site de Bercy - DMZ Fichiers

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_2_8_5_101	<p>La DMZ Fichiers située sur le site de Bercy doit être utilisée pour héberger les serveurs mutualisés de fichiers des nouvelles applications web exposées sur :</p> <ul style="list-style-type: none"> ▪ le réseau internet, ▪ le réseau internet et le réseau général (RG). 	Validé	22/01/2020	
1_2_8_5_102	<p>Les flux applicatifs entrants autorisés de la DMZ Fichiers située sur le site de Bercy doit être basés sur :</p> <ul style="list-style-type: none"> ▪ le protocole NFS pour les partages de fichiers sous Linux, ▪ le protocole SMB pour les partages de fichiers sous Microsoft Windows. 	Validé	22/01/2020	

Site de Bercy - DMZ Service

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_2_8_5_151	<p>Les serveurs situés sur les DMZ Web et Data du site de Bercy doivent synchroniser leur horloge sur le serveur mandataire via le protocole NTP.</p>	Validé	22/01/2020	

Site de Bercy - DMZ Messagerie

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_2_8_5_201	<p>La DMZ Messagerie doit être utilisée pour héberger :</p> <ul style="list-style-type: none"> ▪ les serveurs de relais de messagerie externes <p>exposés sur :</p> <ul style="list-style-type: none"> ▪ le réseau internet. 	Validé	09/02/2022	

▪ La dernière modification de cette page a été faite le 25 février 2024 à 07:47.

Répartition de charge (Load balancing) version diffusable

La **répartition de charge** est l'ensemble de techniques permettant de distribuer une charge de travail entre différents ordinateurs d'un groupe. Ces techniques permettent à la fois de répondre à une charge trop importante d'un service en la répartissant sur plusieurs serveurs, et de réduire l'indisponibilité potentielle de ce service que pourrait provoquer la panne logicielle ou matérielle d'un unique serveur. (source : wikipedia, 2023 (https://fr.wikipedia.org/wiki/Répartition_de_charge))

- ✓ Terme privilégié : **répartiteur de charge, répartiteur de charges, équilibreur de charge, équilibreur de charges**
- ✓ Equivalent étranger: **load balancer** (en)

Sommaire

- 1 Contexte
- 2 Règles de base
- 3 Solutions de référence
- 4 Contraintes juridiques et réglementaires
- 5 Contraintes techniques

Contexte

Les **offres de répartition de charge** proposées par le service du numérique (SNUM) s'appuient sur les équipements BIG-IP LTM (https://www.f5.com/fr_fr/products/big-ip-services/local-traffic-manager) et le logiciel BIG-IQ (console centralisée de management des équipements BIG-IP) de la marque **F5 Networks**. Il sont principalement utilisés sur des équipements d'infrastructures mutualisés nécessitant un dispositif de répartition de charge.

Bien que plusieurs **algorithmes d'ordonnancement** soient proposés, il convient de privilégier l'algorithme "**Moins de connexion**" (**Least connections**) qui assigne davantage de requêtes aux serveurs en exécutant le moins.

⚠ En cas de besoin de **répartition de charge applicative avec persistance de session**, il convient de privilégier une solution basée sur le logiciel libre Apache et les modules proxy_module, proxy_balancer_module et proxy_http_module.

Règles de base

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_2_9_1_001	Les répartiteurs de charge doivent être installés dans des versions à jour des correctifs de sécurité.	Validé	22/01/2020	
1_2_9_1_002	Toute les instances virtuelles de répartition de charge doivent être doublées pour assurer la haute disponibilité en mode actif/passif.	Validé	10/09/2020	

Solutions de référence

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_2_9_2_001	Les nouveaux répartiteurs de charge installés dans les centres de données de référence doivent s'appuyer sur : <ul style="list-style-type: none">les appliances F5 BIG-IP i5800 (https://www.f5.com/pdf/products/big-ip-platforms-data-sheet.pdf), F5 BIG-IP i7800 (https://www.f5.com/pdf/products/big-ip-platforms-datasheet.pdf) et F5 BIG-IP i2600 (https://www.f5.com/pdf/products/big-ip-platforms-datasheet.pdf) et le logiciel propriétaire F5 BIG-IQ pour les solutions d'infrastructures mutualisées;le logiciel libre Apache avec les modules proxy_module, proxy_balancer_module et proxy_http_module pour les solutions applicatives.	Validé	10/09/2020	

Contraintes juridiques et réglementaires

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_2_9_3_001	L'acquisition des répartiteurs de charge doit se faire au travers du marché UGAP "Solutions de cybersécurité réseaux et prestations associées" (https://centraledesmarches.com/marches-publics/Marne-la-vallee-cedex-2-Union-des-Groupements-d-Achats-Publics-Solutions-de-Cybersecurite-reseaux-et-prestations-associees/4242818)".	Validé	22/01/2020	
1_2_9_3_002	Toute demande de support sur les répartiteurs de charge doit se faire au travers du portail constructeur (https://nomios.force.com/NomiosCustomerPortal/).	Validé	06/06/2023	

Contraintes techniques

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_2_9_4_001	Les nouvelles applications nécessitant un dispositif de répartition de charge doivent s'appuyer sur les solutions de référence	Validé	22/01/2020	

▪ La dernière modification de cette page a été faite le 11 décembre 2023 à 10:42.

Serveur physique (Server) version diffusable

Un **serveur** est un dispositif informatique (matériel ou logiciel) qui offre des services, à un ou plusieurs clients (parfois des milliers. Un serveur fonctionne en permanence, répondant automatiquement à des requêtes provenant d'autres dispositifs informatiques (les clients), selon le principe dit client-serveur. Le format des requêtes et des résultats est normalisé, se conforme à des protocoles réseaux et chaque service peut être exploité par tout client qui met en œuvre le protocole propre à ce service. (source : wikipedia,2022 (https://fr.wikipedia.org/wiki/Serveur_informatique))

✓ Terme privilégié : **serveur**

✓ Equivalent étranger: **server** (en)

La version de base de cette rubrique est accessible [ici](#)

Sommaire

- 1 Contexte
- 2 Règles générales
- 3 Solutions de référence
- 4 Contraintes juridiques et réglementaires
- 5 Contraintes techniques

Contexte

Les offres de serveurs physiques proposées par le service du numérique (SNUM) s'appuient désormais sur les équipements de la marque **HPE** en lieu et place des serveurs DELL précédemment référencés.

Compte tenu de la politique de rationalisation, le parc de serveurs s'inscrit dans une logique de consolidation. De ce fait, il existe de moins en moins de serveurs physiques dédiés à une seule direction ou à une seule fonction.

Par contre, la structure des espaces de travail sur ces serveurs permet de distinguer les environnements alloués sur un même serveur :

- à une direction (pour un serveur à vocation bureautique),
- à une fonction (pour un serveur à vocation applicative).

⚠ Le service du numérique (SNUM) recourt de manière systématique à la virtualisation des serveurs.

Règles générales

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_3_1_1_001	L'installation des nouvelles applications sur des serveurs virtuels doivent être privilégiés par rapport aux serveurs physiques.	Validé	01/07/2019	
1_3_1_1_002	Les serveurs physiques doivent être installés dans des versions à jour des correctifs de sécurité.	Validé	03/12/2019	Vulnérabilités dans les produits INTEL 16/11/2023 : CERTFR-2023-AVI-093 (https://www.cer.t.ssi.gouv.fr/avis/CERTFR-2023-AVI-093)

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_3_1_2_001	Les nouveaux serveurs physiques installés dans les baies informatiques des centres de données de référence doivent être choisis parmi les modèles HPE proposés sur l'espace HERMES dédié au suivi du marché DAE serveur.	Validé	09/02/2022	

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_3_1_3_001	L'acquisition des serveurs physiques doit se faire au travers du marché "Fournitures de serveurs de technologie X86, d'accessoires, de prestation et de garantie".	Validé	01/07/2019	Espace HERMES (https://services.fr.scc.com/dae/) dédié au suivi du marché DAE serveur
	1_3_1_3_002	La maintenance des serveurs physiques doit se faire au travers du marché "Tierce maintenance des serveurs x86 et de solutions de sauvegarde ainsi que les prestations associées".	Validé	01/07/2019	Portail de maintenance (https://sccfrprodcs.service-now.com/scc_maintenance_sp)

Contraintes techniques

Caractéristiques techniques des serveurs physiques



	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_3_1_4_001	Le format des serveurs physiques localisés sur le centre de données d'Osny doit être de type rack et compatible avec les dimensions des baies du site (600 x 1000 mm).	Validé	01/07/2019	
	1_3_1_4_002	Le système d'alimentation des serveurs physiques localisés sur le centre de données d'Osny doit être redondé (2 blocs d'alimentation minimum).	Validé	01/07/2019	
	1_3_1_4_003	Les interfaces réseaux des serveurs physiques localisés sur le centre de données d'Osny doivent être déclinées de la manière suivante : <ul style="list-style-type: none">■ Une interface réseau dédiée pour les flux de production,■ Une interface réseau dédiée pour les flux d'administration,■ Une interface réseau dédiée pour les flux de sauvegarde.	Validé	01/07/2019	
	1_3_1_4_004	Les ports réseaux des serveurs physiques localisés sur le centre de données d'Osny peuvent être de type : <ul style="list-style-type: none">■ RJ45 (https://fr.wikipedia.org/wiki/RJ45) avec un débit maximum de 1Gb/s,■ RJ45 avec un débit maximum de 10Gb/s,■ SFP+ (https://fr.wikipedia.org/wiki/Small_form-factor_pluggable) avec un débit maximum de 16Gb/s	Validé	01/07/2019	
	1_3_1_4_005	Les ports HBA (https://fr.wikipedia.org/wiki/Contr%C3%B4leur_h%C3%B4te_d%C3%B9s) des serveurs physiques localisés sur le centre de données d'Osny doivent être de type : <ul style="list-style-type: none">■ SFP+ (https://fr.wikipedia.org/wiki/Small_form-factor_pluggable) avec un débit maximum de 4Gb/s,■ SFP+ avec un débit maximum de 8Gb/s,■ SFP+ avec un débit maximum de 16Gb/s. si les serveurs physiques sont raccordés à l'infrastructure de stockage centralisée via 2 réseaux de stockage SAN FC (https://fr.wikipedia.org/wiki/R%C3%A9seau_de_stockage_SAN).	Validé	01/07/2019	

Règles de nommage des serveurs physiques

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires																
	1_3_1_5_001	<p>Les noms des serveurs physiques à vocation technique (contrôleurs de domaines Windows) localisés sur le centre de données d'Osny doivent respecter les règles de nommage suivantes :</p> <table><tr><th>Type de serveur physique</th><th>Règle de nommage</th></tr><tr><td>Contrôleur de domaine</td><td>do-adak-[numéro]</td></tr><tr><td>Contrôleur de domaine en mode RODC</td><td>do-diodeme-[numéro]</td></tr></table> <p>où [numéro] est un numéro d'ordre sur 2 caractères.</p>	Type de serveur physique	Règle de nommage	Contrôleur de domaine	do-adak-[numéro]	Contrôleur de domaine en mode RODC	do-diodeme-[numéro]	Validé	01/07/2019											
Type de serveur physique	Règle de nommage																				
Contrôleur de domaine	do-adak-[numéro]																				
Contrôleur de domaine en mode RODC	do-diodeme-[numéro]																				
	1_3_1_5_002	<p>Les noms des serveurs physiques à vocation technique (hyperviseurs VMware) localisés sur le centre de données d'Osny doivent respecter les règles de nommage suivantes :</p> <table><tr><th>Type de serveur physique</th><th>Règle de nommage</th></tr><tr><td>Serveur mutualisé windows</td><td>do-esx-mut-win[numéro]</td></tr><tr><td>Serveur interne de recette</td><td>do-esx-int-rec[numéro]</td></tr><tr><td>Serveur interne de production</td><td>do-esx-int-prd[numéro]</td></tr><tr><td>Serveur mutualisé en attente</td><td>do-esx-mut-tmp[numéro]</td></tr><tr><td>Serveur externe frontal</td><td>do-esx-ext-fr[numéro]</td></tr><tr><td>Serveur externe Back-Office</td><td>do-esx-ext-bo[numéro]</td></tr></table>	Type de serveur physique	Règle de nommage	Serveur mutualisé windows	do-esx-mut-win[numéro]	Serveur interne de recette	do-esx-int-rec[numéro]	Serveur interne de production	do-esx-int-prd[numéro]	Serveur mutualisé en attente	do-esx-mut-tmp[numéro]	Serveur externe frontal	do-esx-ext-fr[numéro]	Serveur externe Back-Office	do-esx-ext-bo[numéro]	Validé	01/07/2019			
Type de serveur physique	Règle de nommage																				
Serveur mutualisé windows	do-esx-mut-win[numéro]																				
Serveur interne de recette	do-esx-int-rec[numéro]																				
Serveur interne de production	do-esx-int-prd[numéro]																				
Serveur mutualisé en attente	do-esx-mut-tmp[numéro]																				
Serveur externe frontal	do-esx-ext-fr[numéro]																				
Serveur externe Back-Office	do-esx-ext-bo[numéro]																				
	1_3_1_5_003	<p>Les noms des serveurs physiques à vocation technique (SGBD) localisés sur le centre de données d'Osny doivent respecter les règles de nommage suivantes :</p> <table><tr><th>Type de serveur physique</th><th>Règle de nommage</th></tr><tr><td>Serveur interne Oracle</td><td>do-ora-di-prd[numéro]</td></tr><tr><td>Serveur externe Oracle</td><td>do-ora-de-prd[numéro]</td></tr><tr><td>Serveur interne SQL Server</td><td>do-msql-di-p[numéro]</td></tr><tr><td>Serveur externe SQL Server</td><td>do-msql-de-p[numéro]</td></tr><tr><td>Serveur interne SQL Server (application Appach)</td><td>do-appachsql-di</td></tr><tr><td>Serveur interne PostgreSQL</td><td>do-psql-di-[équipe][numéro]</td></tr><tr><td>Serveur externe PostgreSQL</td><td>do-psql-de-[équipe][numéro]</td></tr></table> <p>où [numéro] est un numéro d'ordre sur 2 caractères.</p> <p>où [équipe] est le nom de l'équipe (COM, INT ou RHC).</p>	Type de serveur physique	Règle de nommage	Serveur interne Oracle	do-ora-di-prd[numéro]	Serveur externe Oracle	do-ora-de-prd[numéro]	Serveur interne SQL Server	do-msql-di-p[numéro]	Serveur externe SQL Server	do-msql-de-p[numéro]	Serveur interne SQL Server (application Appach)	do-appachsql-di	Serveur interne PostgreSQL	do-psql-di-[équipe][numéro]	Serveur externe PostgreSQL	do-psql-de-[équipe][numéro]	Validé	01/07/2019	
Type de serveur physique	Règle de nommage																				
Serveur interne Oracle	do-ora-di-prd[numéro]																				
Serveur externe Oracle	do-ora-de-prd[numéro]																				
Serveur interne SQL Server	do-msql-di-p[numéro]																				
Serveur externe SQL Server	do-msql-de-p[numéro]																				
Serveur interne SQL Server (application Appach)	do-appachsql-di																				
Serveur interne PostgreSQL	do-psql-di-[équipe][numéro]																				
Serveur externe PostgreSQL	do-psql-de-[équipe][numéro]																				
	1_3_1_5_004	<p>Les noms des serveurs physiques à vocation applicative localisés sur le centre de données d'Osny doivent respecter les règles suivantes :</p> <table><tr><th>Type de serveur physique</th><th>Règle de nommage</th></tr><tr><td>Serveur applicatif</td><td>do-[appli]-[env]-[tiers]-[numéro]</td></tr></table> <p>où [appli] est le nom de l'application.</p> <p>où [env] est l'environnement concerné (prd, rec, dev et pprd)</p> <p>où [tiers] est le nom du tiers (fr, app, ora, msql, psql, ged, idx)</p> <p>où [numéro] est un numéro sur 2 caractères.</p>	Type de serveur physique	Règle de nommage	Serveur applicatif	do-[appli]-[env]-[tiers]-[numéro]	Validé	01/07/2019													
Type de serveur physique	Règle de nommage																				
Serveur applicatif	do-[appli]-[env]-[tiers]-[numéro]																				

Poste de travail (Workstation) version diffusable

Un **poste de travail** représente principalement le point d'accès à toutes les fonctionnalités d'une application informatique et d'un système d'exploitation, en particulier aux ressources informatiques (messagerie, bureautique, applications web, mais aussi imprimante, numériseur de document, ...). (source : wikipedia,2023 (https://fr.wikipedia.org/wiki/Poste_de_travail))

-  Termes privilégiés : **poste de travail**
-  Equivalent étranger: **workstation** (en), **computer workstation** (en)

La version de base de cette rubrique est accessible [ici](#)

Sommaire

1

Contexte

2

Règles générales

3

Postes de travail physiques de référence

4

Contraintes juridiques et réglementaires

5

Contraintes techniques

Contexte

Les offres de postes de travail physiques proposées par le service du numérique (SNUM) s'appuient sur les équipements des marques **Lenovo**, **Dell** et **HP**.

Règles générales

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_3_2_1_001	Les postes de travail des agents d'administration centrale doivent respecter le standard ministériel Charte informatique (https://monalize.alize/files/live/sites/Alize/files/contributed/Accueil/Ressources/Publications/Chartes/charte-utilisation-outils-num_220318_version%20dc3%a9finitive.pdf)	Validé	01/07/2019	
	1_3_2_1_002	Les postes de travail des agents d'administration centrale doivent respecter le standard ministériel Mémento agent (http://hfds-bercy.monportail.alize/files/live/sites/hfds-bercy/files/r%cc3%a9pertoires/S%cc3%a9curit%cc3%a9%20des%20syst%cc3%a8mes%20d'information/documents/Textes%20de%20r%cc3%a9f%cc3%a9rences/bro-agents-secu-info.pdf).	Validé	01/07/2019	
	1_3_2_1_003	Les postes de travail des agents d'administration centrale doivent respecter le standard ministériel Protéger les documents sensibles, même sans moyens gouvernementaux (http://hfds-bercy.monportail.alize/files/live/sites/hfds-bercy/files/r%cc3%a9pertoires/S%cc3%a9curit%cc3%a9%20des%20syst%cc3%a8mes%20d'information/documents/Textes%20de%20r%cc3%a9f%cc3%a9rences/170922_secrets-documents-sensibles_v1.1.pdf)	Validé	01/07/2019	
	1_3_2_1_004	Les postes de travail des agents d'administration centrale doivent respecter le standard ministériel Homologation des postes de travail (http://hfds-bercy.monportail.alize/files/live/sites/hfds-bercy/files/r%cc3%a9pertoires/S%cc3%a9curit%cc3%a9%20des%20syst%cc3%a8mes%20d'information/documents/Textes%20de%20r%cc3%a9f%cc3%a9rences/170112_guide-homologation-postes-de-travail_v1.0.0.pdf).	Validé	01/07/2019	
	1_3_2_1_005	Les postes de travail des agents d'administration centrale doivent respecter le standard ministériel Sécurisation des poste de travail Windows 10 (http://hfds-bercy.monportail.alize/files/live/sites/hfds-bercy/files/r%cc3%a9pertoires/S%cc3%a9curit%cc3%a9%20des%20syst%cc3%a8mes%20d'information/documents/Textes%20de%20r%cc3%a9f%cc3%a9rences/170112_standard-poste-de-travail-windows-10_v1.0.0.pdf).	Validé	01/07/2019	
	1_3_2_1_006	Les postes de travail des agents d'administration centrale doivent respecter le standard ministériel Télétravail (http://hfds-bercy.monportail.alize/files/live/sites/hfds-bercy/files/r%cc3%a9pertoires/S%cc3%a9curit%cc3%a9%20des%20syst%cc3%a8mes%20d'information/documents/Textes%20de%20r%cc3%a9f%cc3%a9rences/180503_standard-teletavail_v1.0.pdf).	Validé	01/07/2019	
	1_3_2_1_007	Les postes de travail des agents d'administration centrale doivent être étiquetés et enregistrés dans le logiciel de gestion de parc avant tout déploiement.	Validé	01/07/2019	
	1_3_2_1_008	Les postes de travail des agents d'administration centrale doivent suivre le cycle de vie suivant : <ul style="list-style-type: none">■ 5 ans pour les postes de travail fixes,■ 5 ans pour les postes de travail portables,■ 4 ans pour les postes de travail ultra-portables,■ 4 ans pour les postes de travail hybrides.	Validé	01/07/2019	

Postes de travail physiques de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_3_2_2_001	<p>Les postes de travail des agents d'administration centrale doivent être choisis parmi ceux indiqués dans la liste ci-dessous :</p> <ul style="list-style-type: none"> ■ Poste de travail fixe(Lenovo M710Q, Lenovo M720T), ■ Poste de travail portable(Aucun modèle actuellement), ■ Poste de travail PC ultra-portable(Dell Latitude 5310), ■ Poste de travail PC hybride(HP Elitebook X2 G4), <p>dans l'une des configurations standards décrites dans le CCTP du marché d'acquisition.</p>	Validé	10/02/2021	

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_3_1_3_001	La fourniture des postes de travail doit se faire au travers du marché " SAD Micro-informatique".	Validé	01/07/2019	
	1_3_1_3_002	La maintenance des postes de travail (fixes, portables, ultra-portables et hybrides) doit se faire au travers du marché " Assistance aux utilisateurs dans les domaines informatiques, audiovisuel et téléphonie et maintenance de matériel informatique".	Validé	01/07/2019	

Contraintes techniques

Caractéristiques techniques des postes de travail physiques

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_3_2_4_001	<p>La configuration matérielle minimale des postes de travail des agents d'administration centrale doit être basée sur les éléments suivants :</p> <ul style="list-style-type: none"> ■ Microprocesseur : Double cœur, 2.5 Ghz ■ Mémoire vive : 8 Go ■ Disque dur : 256 Go ■ Résolution d'écran : 1366x768 ■ Port Ethernet : RJ45 10/100 Mo ■ Port USB : 2.0 ■ Pas de lecteur DVD ni de disquette 	Validé	03/12/2020	

Installation des postes de travail physiques

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_3_2_5_001	L'installation des postes de travail des agents d'administration centrale doit être réalisée par les Gestionnaires des Ressources Informatiques Déconcentrées (GRID).	Validé	01/07/2019	processus

Maintenance des postes de travail physiques

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_3_2_6_001	La maintenance des postes de travail des agents d'administration centrale doit être réalisée par les Gestionnaires des Ressources Informatiques Déconcentrées (GRID) via un ticket saisi dans le logiciel de gestion des services d'assistance ITSM.	Validé	01/07/2019	processus

Décommissionnement des postes de travail physiques

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_3_2_7_001	Le décommissionnement des postes de travail des agents d'administration centrale doit être réalisé par les Gestionnaires des Ressources Informatiques Déconcentrées (GRID).	Validé	01/07/2019	processus
	1_3_2_7_002	<p>Le décommissionnement des postes de travail des agents d'administration centrale doit faire l'objet d'un courrier électronique adressé aux équipes suivantes :</p> <ul style="list-style-type: none"> ■ BENA - TCPM (partie antivirus et télédistribution) ■ BITS - Applications Windows. <p>Les informations suivantes doivent être obligatoirement fournies:</p> <ul style="list-style-type: none"> ■ Le nom poste de travail ■ L'entité d'appartenance 	Validé	01/07/2019	processus

Règle de nommage des postes de travail physiques

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires				
	1_3_2_8_001	<div>Le nom des postes de travail doit respecter les règles de nommage suivantes :</div> <table><tr><th>Type de poste de travail</th><th>Règle de nommage</th></tr><tr><td>Poste de travail (fixe, portable, ultra-portable et hybride)</td><td>[préfixe]-[suffixe]</td></tr></table> <div>où [préfixe] est le nom de la direction, où [suffixe] est le numéro d'inventaire.</div>	Type de poste de travail	Règle de nommage	Poste de travail (fixe, portable, ultra-portable et hybride)	[préfixe]-[suffixe]	Validé	01/07/2019	
Type de poste de travail	Règle de nommage								
Poste de travail (fixe, portable, ultra-portable et hybride)	[préfixe]-[suffixe]								

• La dernière modification de cette page a été faite le 25 février 2024 à 07:17.

Equipement de stockage version diffusable

Une **baie de stockage** est un équipement composé d'un ensemble de disques regroupé (standard ou dense), un ou plusieurs contrôleurs composés de ports de liaisons avec les serveurs d'application, d'un bus.

(source : wikipedia,2022 (https://fr.wikipedia.org/wiki/Baie_de_stockage))

✓ Terme privilégié : **stockage, stockage de données**

✓ Equivalent étranger: **storage** (en), **data storage** (en)

La version de base de cette rubrique est accessible ici

Sommaire

- 1 Contexte
- 2 Règles de base
- 3 Solutions de référence
 - 4 Contraintes juridiques et réglementaires

Contexte

Les offres d'équipements de stockage proposées par le service du numérique (SNUM) s'appuient sur les équipements de la marque **NetApp**.

Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_3_4_1_001	Les solutions de référence de stockage des données (serveurs) doivent être installées dans des versions à jour descorrectifs de sécurité.	Validé	16/12/2022	

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_3_4_2_001	Les équipements de stockage installés dans les centres de données de référence de SNUM doivent s'appuyer sur les modèles suivants : <ul style="list-style-type: none">NetApp FAS8020 (https://www.netapp.com/us/media/ds-354.pdf)NetApp FAS8040 (https://www.netapp.com/us/media/ds-354.pdf)NetApp AFF A300 (https://www.netapp.com/us/media/na-382.pdf)	Validé	03/09/2019	
	1_3_4_2_002	Pour les serveurs physiques ayant besoin d'un espace de stockage de données non partagé, la solution de prédilection est la fourniture d'un disque virtuel accédé via un réseau SAN FC.	Validé	03/09/2019	
	1_3_4_2_003	Pour les serveurs physiques sous Linux ayant besoin d'un espace de stockage partagé, ou pour les serveurs virtuels Linux ayant besoin d'un espace de stockage de plus de 1 To (partagé ou non), la solution de prédilection est la fourniture d'un espace de partage de fichiers NFS.	Validé	03/09/2019	
	1_3_4_2_004	Pour les serveurs physiques sous Windows ayant besoin d'un espace de stockage partagé, ou pour les serveurs virtuels Windows ayant besoin d'un espace de stockage de plus de 1 To (partagé ou non), la solution de prédilection est la fourniture d'un espace de partage de fichiers CIFS.	Validé	03/09/2019	
	1_3_4_2_005	Les équipements de stockage de type NetApp All Flash FAS AFF A300 doivent être utilisés pour stocker les données des serveurs à vocation applicative situés sur les DMZ Fichiers du centre de traitement d'Osny.	Validé	03/12/2019	

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_3_4_3_001	L'acquisition des équipements de stockage doit se faire au travers du marché UGAP "Solutions de stockage des données, de sauvegarde et d'archivage des données, systèmes convergés, serveurs, logiciels et prestations associés".	Validé	03/09/2019	
	1_3_4_3_002	La maintenance des équipements de stockage doit se faire au travers du marché "Tierce maintenance de matériels d'infrastructure de stockage".	Validé	03/09/2019	
	1_3_4_4_003	Les demandes de support sur les équipements de stockage de référence doivent se faire via par courriel (mailto:NETAPP-SUPPORT@fr.scc.com).	Validé	16/12/2022	

Système d'exploitation serveur

Un **système d'exploitation** est un ensemble de programmes qui dirige l'utilisation des ressources d'un ordinateur par des logiciels applicatifs. Il reçoit des demandes d'utilisation des ressources de l'ordinateur — ressources de stockage des mémoires (par exemple des accès à la mémoire vive, aux disques durs), ressources de calcul du processeur central, ressources de communication vers des périphériques (pour parfois demander des ressources de calcul au GPU par exemple ou tout autre carte d'extension) ou via le réseau — de la part des logiciels applicatifs. Le système d'exploitation gère les demandes ainsi que les ressources nécessaires évitant les interférences entre les logiciels l. (source : wikipedia,2022 (https://fr.wikipedia.org/wiki/Syst%C3%A8me_d%27exploitation))



Termes privilégiés : **système d'exploitation, SE**



Equivalent étranger: **operating system** (en), **OS** (en)

Sommaire

- 1 Contexte
- 2 Règles de base
- 3 Solutions de référence
- 4 Contraintes juridiques et réglementaires
- 5 Contraintes techniques

Contexte

Les offres de systèmes d'exploitation serveur proposées par le service du numérique (SNUM) s'appuient actuellement sur :

- le logiciel libre **CentOS** pour les serveurs Linux à vocation applicative et technique, le logiciel propriétaire
- **Microsoft Windows Server** pour les serveurs Windows à vocation applicative et technique.



La société REDHAT ayant annoncé fin 2020 la fin de la distribution CentOS 8, le SNUM s'orienterait sur le logiciel libre **Rocky Linux**.

Certains serveurs Linux à vocation applicative et technique peuvent nécessiter l'usage du logiciel propriétaire **Red Hat Enterprise Linux RHEL**. C'est le cas pour les serveurs physiques mutualisés utilisant :

- le logiciel propriétaire Oracle Database Server le logiciel
- propriétaire Veritas Netbackup et pour certains serveurs

virtuels d'infrastructure et applicatifs critiques

Règles de base

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_4_1_1_001	Les systèmes d'exploitation des serveurs doivent être installés dans des versions à jour des correctifs de sécurité.	Validé	03/09/2019	<p>13/01/2023 : CERTFR-2023-AVI-0028 (https://www.cert.ssi.gouv.fr/avis/CERTFR-2023-AVI-0028/)</p> <p>- Red Hat Enterprise Linux for x86_64 x86_64</p> <p>10/05/2023 : CERTFR-2023-AVI-0373 (https://www.cert.ssi.gouv.fr/avis/CERTFR-2023-AVI-0373/)</p> <p>- Windows Server 2008 R2 pour systèmes x 64 Service Pack 1</p> <p>- Windows Server 2008 R2 pour systèmes x 64 Service Pack 1 (Server Core installation)</p> <p>- Windows Server 2008 pour systèmes 32 bits Service Pack 2</p> <p>- Windows Server 2008 pour systèmes 32 bits Service Pack 2 (Server Core installation)</p> <p>- Windows Server 2008 pour systèmes x 64 Service Pack 2</p> <p>- Windows Server 2008 pour systèmes x 64 Service Pack 2 (Server Core installation)</p> <p>- Windows Server 2012</p> <p>- Windows Server 2012 (Server Core installation)</p> <p>- Windows Server 2012 R2- Windows Server 2012 R2 (Server Core installation)</p> <p>- Windows Server 2016</p> <p>- Windows Server 2016 (Server Core installation)</p> <p>- Windows Server 2019</p> <p>- Windows Server 2019 (Server Core installation)</p> <p>- Windows Server 2022</p> <p>- Windows Server 2022 (Server Core installation)</p>

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_4_1_2_001	Le logiciel libre GNU/Linux CentOS 7.9 doit être utilisée pour : <ul style="list-style-type: none"> les nouveaux serveurs à vocation technique, les nouveaux serveurs à vocation applicative. 	Validé	18/05/2020	Dates de fin de support CentOS (https://wiki.centos.org/About/Product) : - CentOS 7 : 30/06/2024 - CentOS 8 : 31/12/2021
	1_4_1_2_002	Le logiciel propriétaire Red Hat Enterprise Linux (RHEL) 7 doit être utilisée pour : <ul style="list-style-type: none"> les nouveaux serveurs à vocation applicative nécessitant l'utilisation de cette distribution. 	Validé	30/09/2019	Dates de fin de support full RHEL (https://access.redhat.com/support/policy/updates/errata) : - RHEL 7 : 06/08/2019 Dates de fin de support 1 et 2 RHEL (https://access.redhat.com/support/policy/updates/errata) : - RHEL 7 : 06/08/2020 - 30/06/2024 Date de fin de support étendu RHEL (https://access.redhat.com/support/policy/updates/errata) : - RHEL 7 : Non applicable
	1_4_1_2_003	Le logiciel propriétaire Microsoft Windows Server standard 2016 ou 2019 doit être utilisé pour : <ul style="list-style-type: none"> les nouveaux serveurs à vocation bureautique, les nouveaux serveurs à vocation technique nécessitant l'utilisation de ce système d'exploitation. les nouveaux serveurs à vocation applicative nécessitant l'utilisation de ce système d'exploitation. 	Validé	01/07/2019	Dates de fin de support standard Microsoft Windows Server (https://support.microsoft.com/fr-fr/lifecycle/search) : - Windows Server 2016 : 11/01/2022 Dates de fin de support étendu Microsoft Windows Server (https://support.microsoft.com/fr-fr/lifecycle/search) : - Windows Server 2016 : 12/01/2027

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_4_1_3_001	Toute demande de support sur le système d'exploitation serveur CentOS doit se faire au travers du marché "Support à l'usage des logiciels libres (SLL)".	Validé	01/07/2019	Version supportée au marché SLL (https://document.o.alize.finances.rie.gouv.fr/share/s/JTvQNR2DQCa6uBxx4V-Mww) Noyau CentOS 3.10 Portail SSL (https://www.otrs.aosc-portal.com/otrs/customer.pl)
	1_4_1_3_002	Toute demande d'acquisition de licences et de support sur le système d'exploitation serveur Red Hat Enterprise Linux (RHEL) doit se faire au travers du marché "Mise à disposition d'une bibliothèque multi éditeurs permettant l'acquisition de logiciels, de mises à jour, de supports d'installation, de documentations, de maintenance-support éditeur et de prestations éditeurs annexes".	Validé	01/07/2019	Portail support Red Hat (https://rhn.redhat.com/network/software/index.pxt)
	1_4_1_3_003	Toute demande d'acquisition de licences et de support sur le système d'exploitation Microsoft Windows Server doit se faire au travers du marché "Fourniture de licences Microsoft dans le cadre des programmes d'acquisition de licences en volume et programme partenaires CSP. Fourniture ETLA ADOBE et exécution de prestations éditeurs" .	Validé	01/07/2019	Portail support Microsoft (https://services.premier.microsoft.com/)

Contraintes techniques

Installation des systèmes d'exploitation serveur

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_4_1_4_001	L'installation du système d'exploitation CentOS sur des nouveaux serveurs virtuels localisés sur le centre de données d'Osny doit se faire sur la base des templates suivants : <ul style="list-style-type: none"> template-centos76-2nic(s'il s'agit de serveurs à vocation technique), template-centos76-3nic(s'il s'agit de serveurs à vocation applicative). 	Validé	01/07/2019	
	1_4_1_4_002	L'installation du système d'exploitation Microsoft Windows Server sur des nouveaux serveurs virtuels localisés sur le centre de données d'Osny doit se faire sur la base des templates suivants : <ul style="list-style-type: none"> TEMP-2016-EN-2NIC (s'il s'agit de serveurs à vocation technique), TEMP-2016-EN-3NIC (s'il s'agit de serveurs à vocation applicative), TEMP-2016-FR-2NIC (s'il s'agit de serveurs à vocation technique), TEMP-2016-FR-3NIC (s'il s'agit de serveurs à vocation applicative). 	Validé	01/07/2019	
	1_4_1_4_003	L'installation de la distribution Linux Red Hat Enterprise Linux (RHEL) doit se faire à partir : <ul style="list-style-type: none"> des fichiers images ISO disponibles sur le portail client Red Hat. 	Validé	01/07/2019	

Montée de version des systèmes d'exploitation serveur

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_4_1_5_001	La mise à jour de la distribution GNU/Linux CentOS doit se faire depuis le serveur de dépôt Linux interne (synchronisé avec le serveur de dépôt officiel CentOS sur internet 1 fois par jour).	Validé	01/07/2019	
	1_4_1_5_002	La mise à jour du système d'exploitation Windows Server doit se faire depuis le serveur interne Windows Server Update Services (WSUS).	Validé	01/07/2019	
	1_4_1_5_003	La mise à jour de la distribution Red Hat Enterprise Linux (RHEL) doit se faire depuis le serveur de dépôt officiel Red Hat sur internet.	Validé	01/07/2019	

Administration et exploitation des systèmes d'exploitation serveur

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_4_1_6_001				

Récupérée de « https://wiki.monportail.alize/cct/w/index.php?title=Systeme_d%27exploitation_serveur&oldid=15077 »

- La dernière modification de cette page a été faite le 14 mai 2023 à 19:49.

Terminal mobile (Mobile phone) version diffusable

Un téléphone mobile, téléphone portable ou téléphone cellulaire est un appareil électronique de télécommunication, normalement portatif, offrant une fonction de téléphonie mobile et pouvant être utilisé sur de grandes distances sous réserve d'une couverture réseau. (source : Wikipedia,2023 (https://fr.wikipedia.org/wiki/T%C3%A9l%C3%A9phone_mobile))

✓ Termes privilégiés : **téléphone mobile, téléphone portable, téléphone cellulaire**

✓ Equivalent étranger: **Smartphone, Mobile phone** (en)

La version de base de cette rubrique est accessible [ici](#)

Sommaire

- 1 Contexte
- 2 Règles de base
- 3 Solutions de référence
- 4 Contraintes juridiques et réglementaires ▪
- 5 Contraintes techniques

Contexte

L'administration centrale des MEF a mis en place une offre de service de téléphonie mobile sécurisée qui s'appuie sur 2 solutions :

MODUS, une solution d'accès aux ressources du ministère depuis des terminaux mobiles (ordiphones et tablettes) basée sur l'application de gestion des terminaux mobiles (MDM) MobileIron supporté par la société Orange Business Service (OBS). Sa particularité est de créer un conteneur chiffré et étanche renfermant les applications et les données professionnelles. Le reste du terminal est laissé libre à l'utilisateur. Les services accessibles dans le conteneur d'applications sécurisé sont :

- Messagerie (courriels, agenda, contacts, tâches),
- Navigateur Intranet et internet (filtré),
- Suite bureautique (compatible Microsoft Office).

MOTUS, une solution de téléphonie mobile sécurisée basée sur la technologie de chiffrement des données Cryptosmart version 5.2.119 de la société ERCOM et l'application de gestion des terminaux mobiles (MDM) MobileIron supporté par la société Orange Business Service (OBS). Elle a pour but de chiffrer les données (Data ou Data/Voix) des hautes autorités du Ministère. Les services proposés sont :

- Téléphonie mobile sécurisé (Data),
- Voix mobile chiffrée,
- Catalogue de logiciels approuvés.

Règles de base

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_4_2_1_001	L'utilisation d'un terminal mobile dans le cadre de la mobilité et de l'accès aux données professionnelles doit être sécurisée.	Validé	22/01/2020	
1_4_2_1_002	Le sécurisation d'un terminal mobile doit se faire au travers d'une solution MDM (Mobile Device Management) de gestion de terminaux mobiles.	Validé	22/01/2020	

Solutions de référence

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_4_2_2_001	La solution MODUS doit s'appuyer sur : <ul style="list-style-type: none">▪ le logiciel propriétaire de gestion des terminaux mobiles (MDM) MobileIron.▪ des terminaux compatibles avec la solution (actuellement les Samsung Galaxy J3 et Samsung Galaxy A8)	Validé	22/01/2020	
1_4_2_2_002	La solution MOTUS doit s'appuyer sur : <ul style="list-style-type: none">▪ le logiciel propriétaire de gestion des terminaux mobiles (MDM) MobileIron▪ le logiciel propriétaire de chiffrement des données Cryptosmart.▪ des terminaux compatibles avec la solution (actuellement les Samsung Galaxy A8 et Samsung Galaxy S9)	Validé	22/01/2020	

Contraintes juridiques et réglementaires

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_4_2_3_001				

Contraintes techniques

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_4_2_4_001	<div>La solution MODUSdoit remplir les conditions suivantes pour pouvoir fonctionner :</div> <div><ul style="list-style-type: none">▪ Disposer d'un compte Microsoft Exchange,▪ Disposer d'un compte dans la solution MODUS,▪ Disposer des droits Activesync sur Microsoft Exchange (action réalisée au moment de l'attribution du compte MODUS),▪ Disposer d'un point d'accès Wifi ou d'un abonnement avec l'option data 3G/4G.</div>	Validé	22/01/2020	
1_4_2_4_002	<div>La solution MOTUSdoit remplir les conditions suivantes pour pouvoir fonctionner :</div> <div><ul style="list-style-type: none">▪ Disposer d'un compte Microsoft Exchange,▪ Disposer d'un compte dans la solution MOTUS,▪ Disposer des droits Activesync sur Microsoft Exchange (action réalisée au moment de l'attribution du compte MOTUS),▪ Disposer d'un point d'accès Wifi ou d'un abonnement avec option data 3G/4G,▪ Disposer d'un certificat de chiffrement du terminal mobile,▪ L'utilisateur doit être membre d'un groupe Active Directory MOTUS,▪ Le terminal mobile utilisé doit être compatible avec la version Cryptosmart.</div>	Validé	22/01/2020	

• La dernière modification de cette page a été faite le 25 février 2024 à 07:19.

Système d'exploitation poste de travail

Un **système d'exploitation** est un logiciel de base d'un ordinateur chargé de commander l'exécution des programmes. Il assure la gestion des travaux, les opérations d'entréesortie sur les périphériques, l'affectation des ressources aux différents processus, l'accès aux bibliothèques de programmes et aux fichiers, ainsi que la comptabilité des travaux.

(source : Office québécois de la langue française, 2015 (http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8358548))

- ✓ Termes privilégiés : **système d'exploitation, SE**
- ✓ Equivalent étranger : **operating system** (en), **OS** (en)

Sommaire

1

Contexte

2

Règles de base

3

Solutions de référence

4

Contraintes juridiques et réglementaires

5

Contraintes techniques

Contexte

Les offres de systèmes d'exploitation postes de travail et proposées par le service du numérique (SNUM) s'appuient sur le logiciel propriétaire **Microsoft Windows 10**.

Le master **Microsoft Windows 10 version 21H2** est actuellement en pilote test dans les directions de l'administration centrale.

Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_4_3_1_001	Les poste de travail à vocation bureautique doivent s'appuyer sur le système d'exploitation Microsoft Windows.	Validé	03/09/2019	
	1_4_3_1_002	Les systèmes d'exploitation des postes de travail doivent être installés dans des versions à jour des correctifs de sécurité.	Validé	03/09/2019	10/05/2023 :CERTFR-2023-AVI-0373 (https://www.cert.ssi.gouv.fr/avis/CERTFR-2023-AVI-0373) - Windows 10 Version 21H2 pour systèmes x 64
	1_4_3_1_003	Les postes de travail déployés en Administration Centrale doivent être installés à partir d'un master réalisé par l'équipe BENA-TCMP.	Validé	23/09/2019	

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_4_3_2_001	Les systèmes d'exploitation utilisés sur les postes de travail des agents de l'administration centrale sont : - Microsoft Windows 10 Professionnel 64 bits, - Microsoft Windows 10 Entreprise LTSC 2016 64 bits (par héritage).	Validé	10/02/2021	

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_4_3_3_001	Toute demande d'acquisition de licences et de support sur le système d'exploitation Microsoft Windows 10 doit se faire au travers du marché "Fourniture de licences Microsoft dans le cadre des programmes d'acquisition de licences en volume et programme partenaires CSP. Fourniture ETLA ADOBE et exécution de prestations éditeurs" .	Validé	03/09/2019	Portail support Microsoft (https://services.premier.microsoft.com/?Culture=fr-FR&CultureAutoDetect=true)

Contraintes techniques

Paramétrage des systèmes d'exploitation Windows

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_4_3_4_001	Les composants et service Windows inutiles doivent être désactivés en application des consignes de l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI).	Validé	03/09/2019	
	1_4_3_4_002	Les mécanismes de sécurité Windows suivants doivent être mis en œuvre : - Data Execution Prevention (DEP) (https://fr.wikipedia.org/wiki/Data_Execution_Prevention) pour protéger les postes de travail de l'exécution de code dans certaines zones de mémoire. - Enhanced Mitigation Experience Toolkit (EMET) (https://en.wikipedia.org/wiki/Enhanced_Mitigation_Experience_Toolkit) pour protéger les logiciels du socle contre l'exploitation de vulnérabilités (pour les postes de travail disposant d'un système d'exploitation antérieur à Microsoft Windows 10 1709).	Validé	03/09/2019	
	1_4_3_4_003	Les modifications de paramétrage impactant l'ensemble des postes de travail doivent être déployées par stratégie de groupe puis intégrées dans les masters.	Validé	03/09/2019	

Mise à jour des systèmes d'exploitation

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_4_3_5_001	Les mises à jour des postes de travail sous le système d'exploitation Microsoft Windows 10 doivent se faire au travers du logiciel Microsoft Windows Server Update Services (WSUS).	Validé	03/09/2019	
	1_4_3_5_002	Les mises à jour de sécurité des postes de travail sous le système d'exploitation Windows 10 doivent être effectuées régulièrement via les serveurs WSUS après une période de qualification.	Validé	03/09/2019	
	1_4_3_5_003	Les "Service Pack" mis à disposition par Microsoft doivent être télédistribués via la solution de télédistribution ZCM après une période de qualification.	Validé	03/09/2019	
	1_4_3_5_004	Les mises à jour majeures du système d'exploitation Microsoft Windows des postes de travail (release Microsoft Windows 10) doivent être déployés via les serveurs WSUS après une période de qualification pouvant aller jusqu'à 6 mois. Pour les postes de travail sous le système d'exploitation Microsoft Windows 10 professionnel, l'administration centrale utilise le canal de mise à jour semi-annuel de Microsoft.	Validé	03/09/2019	

Masterisation

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_4_3_6_003	Les masters doivent être réalisés via la solution Microsoft Deployment Toolkt (MDT) (https://fr.wikipedia.org/wiki/Microsoft) et ms à disposition des GRID de toutes les directions d'administration centrale. La procédure de masterisation doit se terminer par la mise à jour des composants logiciels via la solution de télédistribution ZCM.	Validé	03/09/2019	
	1_4_3_6_004	Les masters doivent être mis à jour 2 fois par an pour les versions professionnelles et une fois par an pour la version LTSC, en intégrant les mises à jour Microsoft Windows et des logiciels.	Validé	23/09/2019	
	1_4_3_6_005	La procédure de masterisation doit se terminer par la mise à jour des composants logiciels via la solution de télédistribution ZCM.	Validé	03/09/2019	

Système d'exploitation obsolètes

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_4_3_6_006	Les postes de travail installés avec une version inférieure à Windows 7 ne doivent pas être connectés au réseau.	Validé	14/04/2021	
	1_4_3_6_007	Les postes de travail installés avec le système d'exploitation Windows 7 ne peuvent être connectés au réseau que s'ils permettent de faire fonctionner une application non compatible avec le système d'exploitation Windows 10 et que cette exception a été validée par SEP1.	Validé	14/04/2021	
	1_4_3_6_008	Les postes de travail installés avec Windows 7 ne doivent pas avoir accès à internet, ni à la messagerie, ni au VPN TOTEM.	Validé	14/04/2021	

- La dernière modification de cette page a été faite le 14 mai 2023 à 19:49.

Poste de rebond virtuel (VPR)

Le **poste de rebond virtuel** (VPR) est un poste de travail virtuel fonctionnant avec le système d'exploitation Microsoft Windows 10. Ce poste de travail est restreint en consultation Web sur des URL applicatives autorisées. Il est accessible par la solution d'accès à distance Artemis.

✓ Termes privilégiés :poste de rebond virtuel, VPR

✓ Equivalent étranger:

Sommaire

- 1 Contexte
- 2 Règles de base
- 3 Solutions de référence
- 4 Contraintes juridiques et réglementaires
- 5 Contraintes techniques

Contexte

Un poste de rebond virtuel (VPR) permet aux prestataires d’accéder aux applications web autorisés par la solution d’accès à distance Artémis.


L'architecture simplifiée technique d'un poste de rebond (VPR) se décline de la manière suivante:



Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_4_4_1_001	Les postes de rebond virtuels (VPR) doivent être installés dans des versions à jour des correctifs de sécurité.	Validé	18/05/2020	

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_4_4_2_001	La suite logicielle VMware vSphere 6.7 doit être utilisée pour les postes de rebond virtuels (VPR) installés sur le centre de données de Bercy.	Validé	18/05/2020	Dates de fin de support (https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/t/product-lifecycle-matrix.pdf) : - vSphere 6.7 : 15/11/2021

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_4_4_3_001				

Contraintes techniques

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_4_4_4_001	L'accès aux applications depuis un poste de rebond virtuel (VPR) doit se faire au travers de la solution ARTEMIS via le protocole RDP.	Validé	18/05/2020	
	1_4_4_4_002	Le système d'exploitation des postes de rebond virtuel (VPR) doit s'appuyer sur le logiciel propriétaire Microsoft Windows 10 Entreprise 2016 LTSB.	Validé	18/05/2020	
	1_4_4_4_003	Chaque société prestataire peut disposer d'un seul poste de rebond virtuel (VPR).	Validé	18/05/2020	
	1_4_4_4_004	Le poste de rebond virtuel (VPR) ne doit permettre d'accéder qu'aux seules URL des applications web du périmètre de la société prestataire.	Validé	18/05/2020	

Récupérée de « [https://wiki.monportail.alize/cct/w/index.php?title=Poste_de_rebond_virtuel_\(VPR\)&oldid=12644](https://wiki.monportail.alize/cct/w/index.php?title=Poste_de_rebond_virtuel_(VPR)&oldid=12644) »

Poste d'administration virtuel (VPC)

Le **poste d'administration virtuel (VPC)** est un poste de travail virtuel permettant de réaliser des tâches d'exploitation et d'administration informatique. (source : SNUM)

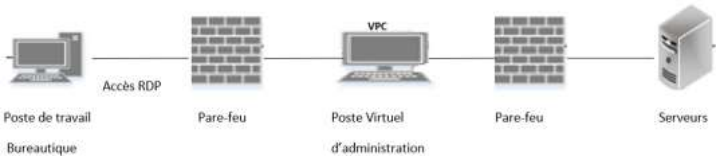
Sommaire

- 1 Contexte
- 2 Règles de base
- 3 Solutions de référence
- 4 Contraintes juridiques et réglementaires
- 5 Contraintes techniques

Contexte

Le poste d’administration virtuel (VPC) permet d’accéder depuis son poste de travail aux réseaux d’administration des équipements informatiques.

L'architecture technique d'un poste d'administration virtuel se décline de la manière suivante:



Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
<div>Nouveauté</div>	1_4_5_1_001	Les postes d'administration virtuels doivent être installés dans des versions à jour des correctifs de sécurité.	Validé	18/05/2020	

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
<div>Nouveauté</div>	1_4_4_2_001	La suite logicielle VMware vSphere 6.7 doit être utilisée pour les postes d'administration virtuels (VPC) installés sur le centre de données de Bercy.	Validé	18/05/2020	Dates de fin de support (https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/t/product-lifecycle-matrix.pdf) : - vSphere 6.7 : 15/11/2021

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_4_5_3_001				

Contraintes techniques

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
<div>Nouveauté</div>	1_4_5_4_001	Le système d'exploitation des postes d'administration virtuels (VPC) doit s'appuyer sur le logiciel propriétaire Microsoft Windows 10 Entreprise LTSC 2016	Validé	03/12/2020	LTSB par remplacé LTSC changement nom p Microsoft
<div>Nouveauté</div>	1_4_5_4_002	Un poste d'administration virtuel (VPC) ne doit pas disposer d'accès sur le réseau internet.	Validé	18/05/2020	

Récupérée de « [https://wiki.monportail.alize/cct/w/index.php?title=Poste_d%27administration_virtuel_\(VPC\)&oldid=12645](https://wiki.monportail.alize/cct/w/index.php?title=Poste_d%27administration_virtuel_(VPC)&oldid=12645) »

▪ La dernière modification de cette page a été faite le 1 mars 2022 à 14:11.

Conteneur logiciel

Un **conteneur** est une structure de données, une classe, ou un type de données abstrait, dont les instances représentent des collections d'autres objets. Autrement dit, les conteneurs sont utilisés pour stocker des objets sous une forme organisée qui suit des règles d'accès spécifiques. On peut implémenter un conteneur de différentes façons, qui conduisent à des complexités en temps et en espace différentes. On choisira donc l'implémentation selon les besoins.

Un conteneur est une enveloppe virtuelle qui permet de distribuer une application avec tous les éléments dont elle a besoin pour fonctionner : fichiers source, environnement d'exécution, bibliothèques, outils et fichiers. Ils sont assemblés en un ensemble cohérent et prêt à être déployé sur un serveur et son système d'exploitation (OS). Contrairement à la virtualisation de serveurs et à une machine virtuelle, le conteneur n'intègre pas de noyau, il s'appuie directement sur le noyau de l'ordinateur sur lequel il est déployé. (source : wikipedia,2022 ([\)](https://fr.wikipedia.org/wiki/Conteneur_(informatique))

- ✓ Terme privilégié : **conteneur**
- ✓ Equivalent étranger: **container** (en)

Sommaire

- 1 Contexte
- 2 Règles de base
- 3 Solutions de référence
- 4 Contraintes juridiques et réglementaires
- 5 Contraintes techniques

Contexte

Il n'y a pas pour l'instant de solution d'orchestration de conteneurs proposée au sein du service du numérique (SNUM). Par contre, une expérimentation sous forme de POC est en cours au sein du SNUM avec le logiciel libre **Kubernetes**.

Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_4_6_1_001	Le déploiement des nouvelles applications doit se faire sans utiliser de solutions basées sur des conteneurs logiciels.	Validé	08/07/2020	

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_4_6_2_001				

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_4_6_3_001				

Contraintes techniques

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_4_6_4_001				

▪ La dernière modification de cette page a été faite le 2 juin 2022 à 14:11.

Application matérielle (Appliance) version diffusable

Un **appliance** est un équipement informatique dédié à une fonctionnalité. (source : wikipedia,2022 (<https://fr.wiktionary.org/wiki/appliance>))

Un **appliance** est un serveur généralement installé à l'intérieur d'un boîtier qui est destiné à exécuter une seule ou quelques fonction, au sein d'un réseau et qu'on peut commander à distance . (source : Office québécois de la langue française, 2001 (<http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?IdFiche=8358313>))

✓ Terme privilégié :**Serveur Monofonctionnel**

✓ Equivalent étranger: **Virtual Appliance** (en)

La version de base de cette rubrique est accessible [ici](#)

Sommaire

- 1 Contexte
- 2 Règles de base
- 3 Solutions de référence
- 4 Contraintes juridiques et réglementaires
- 5 Contraintes techniques

Contexte

Il n'y a pas d'offres d'appliance proposées en standard au sein du service du numérique (SNUM). En effet, elles sont aujourd'hui utilisées pour certaines solutions ne s'inscrivant pas dans le cadre de cohérence technique (CCT).

Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_4_7_1_001	Les appliances doivent être installés dans des versions à jour des correctifs de sécurité.	Validé	21/06/2021	
	1_4_7_1_002	Les appliances virtuels doivent être installés à partir d'un fichier OVA (Open Virtual Appliance).	Validé	21/06/2021	
	1_4_7_1_003	Les appliances virtuels doivent autoriser l'installation de l'outil VMware Tools.	Validé	21/06/2021	
	1_4_7_1_004	Les appliances doivent être enrôlés dans l'outil Cyberwatch si supportées par ce dernier.	Validé	21/06/2021	

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_4_7_2_001				

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_4_7_3_001	L'acquisition d'un appliance doit se faire dans un marché en cours de validité, l'éditeur devant préciser la roadmap de son produit.	Validé	28/09/2021	
	1_4_7_3_002	Le marché contracté en règle 1_4_7_3_001 doit prévoir le maintien dans le cadre de la maintenance et du support de l'appliance, le maintien en condition opérationnel et le maintien en condition de sécurité et les durées pendant lesquelles ces derniers sont garantis.	Validé	28/09/2021	

Contraintes techniques

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_4_7_4_001	Le fournisseur d'un appliance doit décrire les principes de fonctionnement, les mécanismes de mise à jour de son produit et la nature des échanges.	Validé	28/09/2021	

Hyperviseur (Hypervisor) version diffusable

Un **hyperviseur** (Hypervisor) est une plate-forme de virtualisation qui permet à plusieurs systèmes d'exploitation de travailler sur une même machine physique en même temps. On distingue deux types d'hyperviseurs :

- Un **hyperviseur de type 1**, natif, voire « bare metal » (littéralement « métal nu »), est un logiciel qui s'exécute directement sur une plateforme matérielle ; cette plateforme est alors considérée comme outil de contrôle de système d'exploitation. Un système d'exploitation secondaire peut, de ce fait, être exécuté au-dessus du matériel.
- Un **hyperviseur de type 2** est un logiciel qui s'exécute à l'intérieur d'un autre système d'exploitation. Un système d'exploitation invité s'exécutera donc en troisième niveau au-dessus du matériel. Les systèmes d'exploitation invités n'ayant pas conscience d'être virtualisés, ils n'ont pas besoin d'être adaptés. (source :

Wikipedia, 2023 (<https://fr.wikipedia.org/wiki/Hyperviseur>))

✓ Termes privilégiés :**hyperviseur**

✓ Equivalent étranger: **hypervisor** (en),

Sommaire

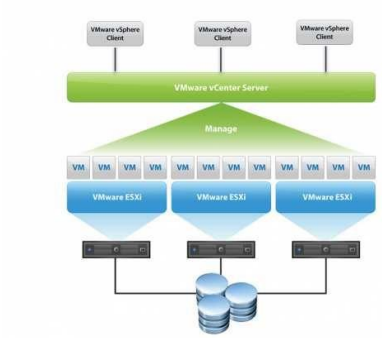
- 1 Contexte
- 2 Règles de base
- 3 Solutions de référence
- 4 Contraintes juridiques et réglementaires
- 5 Contraintes techniques

Contexte

L'offre de service proposée par le service du numérique (SNUM) en termes d'**hyperviseur** s'appuie sur :

- le logiciel propriétaire **VMware vSphere ESXi**
- le logiciel propriétaire **VMware vRealize Orchestrator**
- le logiciel propriétaire **VMware vCenter**

Il s'agit d'**hyperviseurs de type 1**.



Règles de base

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_5_1_1_001	Les hyperviseurs de référence doivent être installés dans des versions à jour des correctifs de sécurité.	Validé	06/07/2022	
1_5_1_1_002	L'installation des nouvelles applications sur des plateformes virtualisées doit être privilégiée par rapport aux plateformes physiques.	Validé	06/07/2022	

Solutions de référence

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_5_1_2_001	Les hyperviseurs de référence doivent s'appuyer sur le logiciel propriétaire VMWare ESXi .	Validé	06/07/2022	Cycle de vie du logiciel VMware ESXi (https://lifecycle.vmware.com/#/)

Contraintes juridiques et réglementaires

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_5_1_3_001	Toute demande de support doit se faire au travers du Portail support VMware (https://customerconnect.vmware.com/fr/login).	Validé	16/12/2022	

Contraintes techniques

Contraintes d'installation

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_5_1_4_001	Les serveurs virtuels à vocation applicative localisés sur le centre de données d'Osny doivent disposer de 3 interfaces réseaux: <ul style="list-style-type: none">▪ Une interface réseau dédiée pour les flux de production,▪ Une interface réseau dédiée pour les flux d'administration,▪ Une interface réseau dédiée pour les flux de sauvegarde.	Validé	01/07/2019	
1_5_1_4_002	Les serveurs virtuels à vocation technique localisés sur le centre de données d'Osny doivent disposer de 2 interfaces réseaux: <ul style="list-style-type: none">▪ Une interface réseau dédiée pour les flux de production et d'administration,▪ Une interface réseau dédiée pour les flux de sauvegarde.	Validé	01/07/2019	
1_5_1_4_003	Les ressources (vCPU, RAM et espace de stockage) attribuées à un serveur virtuel ne doivent pas être réutilisées pour d'autres besoins.	Validé	01/07/2019	
1_5_1_4_004	La configuration CPU, RAM et espace de stockage des serveurs virtuels doit être adaptée au mieux des composants applicatifs hébergés dessus. Les quantités de ressources matérielles configurables en standard sur un serveur virtuel sont: <ul style="list-style-type: none">▪ CPU: 1, 2, 4 ou 8 vCPU▪ RAM: 1,2, 4, 6, 8, 10, 12, 14 ou 16 Go▪ Espace de stockage système: 60 go (serveur Linux) et 100 Go (serveurs Windows) L'extension des ressources matérielles au delà des valeurs ci-dessus doit faire l'objet d'une justification technique.	Validé	06/06/2023	
1_5_1_4_005	Les systèmes d'exploitation déployés sur les serveurs virtuels doivent être choisis parmi la liste ci-dessous : <ul style="list-style-type: none">▪ Microsoft Windows Server 2019▪ RockyLinux 9▪ RHEL 8 (en cas d'incompatibilité avec RockyLinux 9)	Validé	06/06/2023	

Contraintes de mise à jour

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_5_1_5_001	Les demandes de modification des ressources (CPU, RAM, interface réseau, espace disque) d'un serveur virtuel doivent faire l'objet d'une justification technique.	Validé	01/07/2019	

Contraintes d'administration et d'exploitation

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_5_1_6_001				

Récupérée de « [https://wiki.monportail.alize/cct/w/index.php?title=Hyperviseur_\(Hypervisor\)_version_diffusable&oldid=15914](https://wiki.monportail.alize/cct/w/index.php?title=Hyperviseur_(Hypervisor)_version_diffusable&oldid=15914) »

▪ La dernière modification de cette page a été faite le 11 décembre 2023 à 11:28.

Système d'exploitation serveur Linux (Operating system Linux server) version diffusable

Un **système d'exploitation** est un ensemble de programmes qui dirige l'utilisation des ressources d'un ordinateur par des logiciels applicatif. Il reçoit des demandes d'utilisation des ressources de l'ordinateur — ressources de stockage des mémoires (par exemple des accès à la mémoire vive, aux disques durs), ressources de calcul du processeur central, ressources de communication vers des périphériques (pour parfois demander des ressources de calcul au GPU par exemple ou tout autre carte d'extension) ou via le réseau — de la part des logiciels applicatifs. Le système d'exploitation gère les demandes ainsi que les ressources nécessaires évitant les interférences entre les logiciels. (source : wikipedia,2023 (https://fr.wikipedia.org/wiki/Syst%C3%A8me_d%27exploitation))

- ✓ Termes privilégiés : **système d'exploitation**, **SE**
- ✓ Equivalent étranger: **operating system** (en), **OS** (en)

La version de base de cette rubrique est accessible [ici](#)

Sommaire

1 Contexte

2 Règles de base

3 Solutions de référence

4 Contraintes juridiques et réglementaires

5 Contraintes techniques

Contexte

Les offres de systèmes d'exploitation proposées par le service du numérique (SNUM) s'appuient actuellement sur :

- le logiciel libre **Rocky Linux 9** pour les serveurs Linux à vocation applicative et technique,

La sécurité du système d'exploitation **Rocky Linux 9** a été renforcée en implémentant les règles indiquées dans le Benchmark du CIS.

Certains serveurs Linux à vocation applicative et technique peuvent nécessiter l'usage du logiciel propriétaire **Red Hat Enterprise Linux RHEL 8**.

Règles de base

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_5_2_1_001	Les systèmes d'exploitation des serveurs Linux doivent être installés dans des versions à jour des correctifs de sécurité.	Validé	03/09/2019	

Solutions de référence

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_5_2_2_001	Le système d'exploitation Rocky Linux 9 doit être utilisée pour : <ul style="list-style-type: none">▪ les nouveaux serveurs Linux à vocation technique,▪ les nouveaux serveurs Linux à vocation applicative.	Validé	11/09/2023	
1_5_2_2_002	Le système d'exploitation Red Hat Enterprise Linux (RHEL) 8 peut être utilisée pour les nouveaux serveurs Linux à vocation technique ou applicative nécessitant l'utilisation de cette distribution.	Validé	11/09/2023	

Contraintes juridiques et réglementaires

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_5_2_3_001	Toute demande de support sur le système d'exploitation Rocky Linux doit se faire au travers du portail support SL (https://www.otrs.aosc-portal.com/otrs/customers/).	Validé	01/07/2019	
1_5_2_3_002	Toute demande de support sur le système d'exploitation Red Hat Enterprise Linux (RHEL) doit se faire au travers du portail support éditeur (https://rhn.redhat.com/network/software/index.php).	Validé	01/07/2019	

Contraintes techniques

Installation des systèmes d'exploitation serveur Linux

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_5_2_4_001	L'installation du système d'exploitation Rocky Linux sur des serveurs virtuels doit se faire sur la base du template interne.	Validé	11/09/2023	
1_5_2_4_002	L'installation de la distribution Linux Red Hat Enterprise Linux (RHEL) doit se faire à partir : <ul style="list-style-type: none">des fichiers images ISO disponibles sur le portail client Red Hat.	Validé	01/07/2019	

Montée de version des systèmes d'exploitation serveur Linux

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_5_2_5_001	La mise à jour du système d'exploitation Rocky Linux doit se faire depuis le serveur de dépôt Linux interne (synchronisé avec le serveur de dépôt officiel sur internet 1 fois par jour).	Validé	11/09/2023	
1_5_2_5_002	La mise à jour du système d'exploitation Red Hat Enterprise Linux (RHEL) doit se faire depuis le serveur de dépôt officiel Red Hat sur internet.	Validé	01/07/2019	

Administration et exploitation des systèmes d'exploitation serveur Linux

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_5_2_6_001				

• La dernière modification de cette page a été faite le 25 février 2024 à 07:39.

Système d'exploitation serveur Windows (Operating System Windows Server)

version diffusable

Un **système d'exploitation** est un ensemble de programmes qui dirige l'utilisation des ressources d'un ordinateur par des logiciels applicatif. Il reçoit des demandes d'utilisation des ressources de l'ordinateur — ressources de stockage des mémoires (par exemple des accès à la mémoire vive, aux disques durs), ressources de calcul du processeur central, ressources de communication vers des périphériques (pour parfois demander des ressources de calcul au GPU par exemple ou tout autre carte d'extension) ou via le réseau — de la part des logiciels applicatifs. Le système d'exploitation gère les demandes ainsi que les ressources nécessaires évitant les interférences entre les logiciels. (source : wikipedia,2023 (https://fr.wikipedia.org/wiki/Syst%C3%A8me_d%27exploitation))

- ✓ Termes privilégiés : **système d'exploitation, SE**
- ✓ Equivalent étranger: **operating system** (en), **OS** (en)

La version de base de cette rubrique est accessible [ici](#)

Sommaire

- 1 Contexte
- 2 Règles de base
- 3 Solutions de référence
- 4 Contraintes juridiques et réglementaires
- 5 Contraintes techniques

Contexte

Les offres de systèmes d'exploitation proposées par le service du numérique (SNUM) s'appuient actuellement sur :

- le logiciel propriétaire **Microsoft Windows Server 2019** pour les serveurs Windows à vocation applicative et technique,

Règles de base

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_5_3_1_001	Les systèmes d'exploitation des serveurs Windows doivent être installés dans des versions à jour des correctifs de sécurité.	Validé	03/09/2019	

Solutions de référence

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_5_3_2_001	Le système d'exploitation Microsoft Windows Server 2019 doit être utilisée pour : <ul style="list-style-type: none">▪ les nouveaux serveurs Windows à vocation technique,▪ les nouveaux serveurs Windows à vocation applicative.	Validé	11/09/2023	

Contraintes juridiques et réglementaires

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_5_3_3_001	Toute demande de support sur le système d'exploitation Microsoft Windows Server doit se faire au travers du portail support éditair (https://serviceshub.microsoft.com/).	Validé	01/07/2019	- : .

Contraintes techniques

Installation des systèmes d'exploitation serveur Windows

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_5_3_4_001	L'installation du système d'exploitation Windows Server sur des serveurs virtuels doit se faire sur la base du template suivant : <ul style="list-style-type: none">▪ template-WS2019STD(s'il s'agit de serveurs à vocation technique et applicative)	Validé	11/09/2023	

Montée de version des systèmes d'exploitation serveur Windows

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_5_3_5_001	La mise à jour du système d'exploitation Microsoft Windows Server doit se faire depuis le serveur de dépôt interne Windows Server Update Services (WSUS).	Validé	11/09/2023	

Administration et exploitation des systèmes d'exploitation serveur Windows



Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_5_2_6_001				

• La dernière modification de cette page a été faite le 14 mars 2024 à 07:13.

Système d'exploitation poste utilisateur (Operating System User Workstation)

version diffusable

Un **système d'exploitation** est un ensemble de programmes qui dirige l'utilisation des ressources d'un ordinateur par des logiciels applicatif. Il reçoit des demandes d'utilisation des ressources de l'ordinateur — ressources de stockage des mémoires (par exemple des accès à la mémoire vive, aux disques durs), ressources de calcul du processeur central, ressources de communication vers des périphériques (pour parfois demander des ressources de calcul au GPU par exemple ou tout autre carte d'extension) ou via le réseau — de la part des logiciels applicatifs. Le système d'exploitation gère les demandes ainsi que les ressources nécessaires évitant les interférences entre les logiciels. (source : wikipedia,2023 (https://fr.wikipedia.org/wiki/Syst%C3%A8me_d%27exploitation))

-  Termes privilégiés : **système d'exploitation**, **SE**
-  Equivalent étranger : **operating system** (en), **OS** (en)

La version de base de cette rubrique est accessible [ici](#)

Sommaire

- 1 Contexte
- 2 Règles de base
- 3 Solutions de référence
- 4 Contraintes juridiques et réglementaires
- 5 Contraintes techniques

Contexte

Les offres de systèmes d'exploitation proposées par le service du numérique (SNUM) s'appuient actuellement sur :

- le logiciel propriétaire **Microsoft Windows 10 22H2.1** pour les postes utilisateurs de l'administration centrale, ▪ le logiciel propriétaire **Microsoft Windows 11 23H2.2** pour les postes utilisateurs de l'administration centrale,

Règles de base

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_5_4_1_001	Les systèmes d'exploitation des postes utilisateurs doivent être installés dans des versions à jour des correctifs de sécurité.	Validé	03/09/2019	
1_5_4_1_002	Les postes utilisateurs déployés en Administration Centrale doivent être installés à partir du master réalisé par BENA.	Validé	23/09/2019	

Solutions de référence

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_5_4_2_001	Les postes utilisateurs de l'administration centrale doivent s'appuyer sur les systèmes d'exploitation suivants : - Microsoft Windows 10 Professionnel 64 bits, - Microsoft Windows 10 Entreprise LTSC 2016 64 bits (par héritage	Validé	10/02/2021	

Contraintes juridiques et réglementaires

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_5_4_3_001	Toute demande d'acquisition de licences et de support sur le système d'exploitation Microsoft Windows 10 doit se faire au travers du portail support éditeur (https://serviceshub.microsoft.com/home).	Validé	03/09/2019	

Contraintes techniques

Paramétrage des systèmes d'exploitation Windows

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	Les composants et service Windows inutiles doivent être désactivés en application des			
1_5_4_4_001	consignes de l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI).	Validé	03/09/2019	
1_5_4_4_002	Les mécanismes de sécurité Windows suivants doivent être mis en œuvre : - Data Execution Prevention (DEP) (https://fr.wikipedia.org/wiki/Data_Execution_Prevention) pour protéger les postes de travail de l'exécution de code dans certaines zones de mémoire. - Enhanced Mitigation Experience Toolkit (EMET) (https://en.wikipedia.org/wiki/Enhanced_Mitigation_Experience_Toolkit) pour protéger les logiciels du socle contre l'exploitation de vulnérabilités (pour les postes de travail disposant d'un système d'exploitation antérieur à Microsoft Windows 10 1709).	Validé	03/09/2019	
1_5_4_4_003	Les modifications de paramétrage impactant l'ensemble des postes de travail doivent être Validé 03/09/2019 déployées par stratégie de groupe puis intégrées dans les masters.			

Mise à jour des systèmes d'exploitation

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
1_5_4_5_001	Les mises à jour des postes utilisateurs sous le système d'exploitation Microsoft Windows 10 doivent se faire au travers du logiciel Microsoft Windows Server Update Services (WSUS).	Validé	03/09/2019	
1_5_4_5_002	Les mises à jour de sécurité des postes de travail sous le système d'exploitation Windows 10 doivent être effectuées régulièrement via les serveurs WSUS après une période de qualification.	Validé	03/09/2019	
1_5_4_5_003	Les "Service Pack" mis à disposition par Microsoft doivent être télédistribués via la solution de télédistribution ZCM après une période de qualification.	Validé	03/09/2019	
1_5_4_5_004	Les mises à jour majeures du système d'exploitation Microsoft Windows des postes de travail (release Microsoft Windows 10) doivent être déployés via les serveurs WSUS après une période de qualification pouvant aller jusqu'à 6 mois. Pour les postes de travail sous le système d'exploitation Microsoft Windows 10 professionnel, l'administration centrale utilise le canal de mise à jour semi-annual de Microsoft.	Validé	03/09/2019	

• La dernière modification de cette page a été faite le 25 février 2024 à 07:39.

Authentification unique (Single sign-on, SSO) version diffusable

L'**authentification unique** est une méthode permettant à un utilisateur d'accéder à plusieurs applications informatiques (ou sites web sécurisés) en ne procédant qu'à une seule authentification. Les objectifs sont multiples :

- simplifier pour l'utilisateur la gestion de ses mots de passe ;
- simplifier la gestion des données personnelles détenues par les différents services en ligne, en les coordonnant par des mécanismes de type méta-annuaire ;
- simplifier la définition et la mise en œuvre de politiques de sécurité.

(source :Wikipedia, 2023 (https://fr.wikipedia.org/wiki/Authentification_unique))

✓ Termes privilégiés : **Authentification unique**

✓ Equivalents anglais: **single sign-on** (en), **SSO** (en)

Sommaire

- 1 Contexte
- 2 Règles de base
- 3 Solutions de référence
- 4 Contraintes juridiques et réglementaires
- 5 Contraintes techniques

Contexte

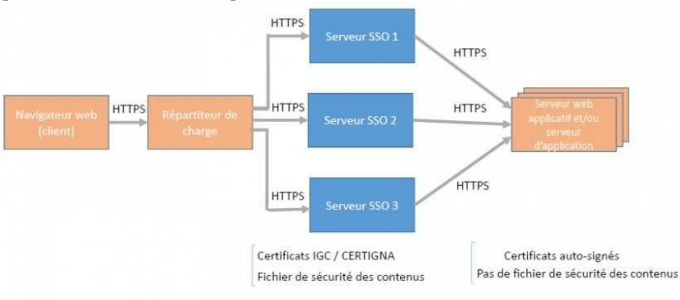
L'offre de services proposée par le service du numérique (SNUM) en termes d'**authentification unique (SSO)** s'appuie sur :

- les logiciels libres **LemonLDAP::NG** et **Apache** .

Elle se décline en plusieurs variantes selon la population visée :

- **SSO RG** raccordé à l'annuaire à destination des utilisateurs du réseau général (RG),
- **SSO RIE** raccordé aux annuaires à destination des utilisateurs du réseau interministériel de l'Etat (RIE),
- **SSO INTERNET** raccordé à l'annuaire à destination des utilisateurs du réseau internet.

La haute-disponibilité de ce service est assurée au travers de la redondance des serveurs SSO, l'utilisation d'une solution de répartition de charge et la mise en œuvre d'un plan de continuité informatique.



Règles de base

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
2_1_1_1_001	Les applications nécessitant l'usage d'une solution d'authentification doivent respecter le standard ministériel Authentification par mot de passe (http://hfds-bercy.monportail.alize/files/live/sites/hfds-bercy/files/r%c3%a9pertoires/S%c3%a9curit%c3%a9%20des%20syst%c3%a8me s%20d'information/documents/Textes%20de%20r%c3%a9f%c3%a9rences/180503_authentic ation-mdp_v3.1.pdf).	Validé	01/07/2019	
2_1_1_1_002	Les applications doivent s'interfacer avec les serveurs d'authentification unique (SSO).	Validé	01/07/2019	Voir également la règle 2_1_1_1_003 décrites ci-dessous en cas d'incompatibilité technique.
2_1_1_1_003	Les applications doivent s'interfacer avec les serveurs mandataires inverses (SMI) si elles ne sont pas interopérables avec les serveurs d'authentification unique (SSO).	Validé	01/07/2019	
2_1_1_1_004	Les serveurs d'authentification unique (SSO) doivent être installés dans des versions à jour des correctifs de sécurité.	Validé	03/09/2019	

Solutions de référence

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
2_1_1_2_001	Les serveurs d'authentification unique (SSO) doivent s'appuyer sur le logiciel libre LemonLDAP::NG 2.0 .	Validé	01/07/2019	Le cycle de vie du logiciel LemonLDAP::NG (https://projects.ow2.org/bin/view/lemonldap-ng/)

Contraintes juridiques et réglementaires

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
2_1_1_3_001	Toute demande de support sur le logiciel libre LemonLDAP::NG doit se faire au travers du portail support SLL (https://www.otrs.aosc-portal.com/otrs/customer.pl).	Validé	01/07/2019	

Contraintes techniques

Contraintes d'installation

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
2_1_1_4_001	Les applications s'interfaçant avec les serveurs d'authentification unique (SSO) doivent respecter les règles décrites dans le guide de paramétrage SSL et entête HTTP (https://documents.alize.finances.rie.gouv.fr/share/s/COIP3D2IQpu-9pXX31mdLA).	Validé	03/09/2019	

Contraintes de mise à jour

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
2_1_1_5_001				

Contraintes d'administration et d'exploitation

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
2_1_1_6_001				

Protocoles d'authentification

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
2_1_1_7_001	Les applications interfacées avec les serveurs d'authentification unique (SSO) doivent utiliser l'un des protocoles d'authentification suivants : <ul style="list-style-type: none">▪ Protocole Kerberos (https://fr.wikipedia.org/wiki/Kerberos_(protocole))▪ Protocole LDAP (https://fr.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol)▪ Protocole SSL (https://fr.wikipedia.org/wiki/Transport_Layer_Security)▪ Protocole SAML (https://fr.wikipedia.org/wiki/Security_assertion_markup_language)▪ Protocole AgentConnect (https://agentconnect.gouv.fr/)	Validé	01/07/2019	

Framework d'authentification

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
2_1_1_7_001	Les applications mettant en oeuvre une solution d'authentification unique (SSO) de l'administration centrale doivent : <ul style="list-style-type: none">▪ Utiliser les frameworks existants, à savoir :<ul style="list-style-type: none">▪ Le framework Java version 1.2 (compatibilité avec les versions 1.6 à 1.8 de Java).▪ Le framework PHP version 1.9.1 (compatibilité avec les versions 3 à 7 de PHP).▪ Ou mettre en oeuvre les fonctionnalités équivalentes :<ul style="list-style-type: none">▪ Lecture par l'application des adresses IP des serveurs SSO dans les annuaires Anais ou Angie.▪ Rejet des requêtes hors SSO.▪ Lecture du header SSO.	Validé	03/12/2019	Cette règle ne s'applique pas aux protocoles d'authentification suivants : KERBEROS, SAML et AgentConnect

▪ La dernière modification de cette page a été faite le 12 décembre 2023 à 17:40.

Serveur mandataire inverse, SMI (Reverse proxy) version diffusable

Un **serveur mandataire inverse** est un type de serveur, habituellement placé en frontal de serveurs web. Contrairement au serveur mandataire qui permet à un utilisateur d'accéder au réseau Internet, le serveur proxy inverse permet à un utilisateur d'Internet d'accéder à des serveurs internes. (source : wikipedia,2023 (https://fr.wikipedia.org/wiki/Proxy_inverse))

- ✓ Terme privilégié : **serveur mandataire inverse, serveur frontal mutualisé**
- ✓ Equivalents étrangers : **reverse proxy server** (en), **reverse proxy** (en)

Sommaire

1

Contexte

2

Règles de base

3

Solutions de référence

4

Contraintes juridiques et réglementaires

5

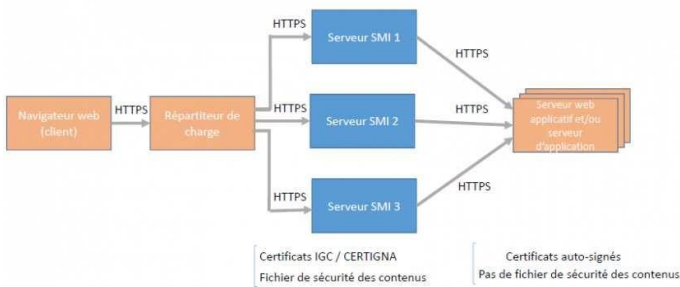
Contraintes techniques

Contexte

L'offre de services proposée par le service du numérique (SNUM) en termes de **serveur mandataire inverse (SMI)** s'appuie sur :

- le logiciel libre **Apache** avec le module mod_proxy.

La haute-disponibilité de ce service est assurée au travers de la redondance des serveurs SMI et l'utilisation d'une solution de répartition de charge.



Règles de base

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
2_1_2_1_001	Les applications doivent s'interfacer avec les serveurs mandataires inverses en cas d'incompatibilité avec les serveurs d'authentification unique (SSO).	Validé	22/01/2020	
2_1_2_1_002	Les serveurs mandataires inverses doivent être installés dans des versions à jour des correctifs de sécurité.	Validé	22/01/2020	
2_1_2_1_003	Les serveurs mandataires inverses doivent respecter les règles décrites dans le Guide de paramétrage SSL et entête HTTP (https://documento.alize.finances.rie.gouv.fr/share/s/COIP3D2IQpu-9pXX31mdLA).	Validé	22/01/2020	

Solutions de référence

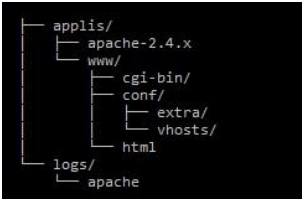
Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
2_1_2_2_001	Les serveurs mandataires inverses doivent s'appuyer sur le logiciel libre Apache 2.4	Validé	22/01/2020	

Contraintes juridiques et réglementaires

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
2_1_2_3_001	Toute demande de support sur le logiciel libre Apache doit se faire au travers du portail support SLL (https://www.otrs.aosc-portal.com/otrs/customer.pl).	Validé	22/01/2020	

Contraintes techniques

Contraintes d'installation

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
2_1_2_4_001	L'installation des serveurs mandataires inverses basés sur le logiciel libre Apache doit être réalisée à partir du script interne .	Validé	22/01/2020	
2_1_2_4_002	<div>L'installation du logiciel libre Apache doit respecter l'arborescence suivante :</div> <div><pre>graph LR applis[applis/] --> apache[apache-2.4.x] applis --> www[www/] www --> cgi-bin[cgi-bin/] www --> conf[conf/] www --> extra[extra/] www --> vhosts[vhosts/] www --> html[html] applis --> logs[logs/] logs --> apache2[apache]</pre></div> <div><ul style="list-style-type: none">▪ Répertoire des fichiers binaires : /applis/apache-[version]où [version] correspond au numéro de version du logiciel</div> <div><ul style="list-style-type: none">▪ Répertoire des fichiers de configuration : /applis/www/conf</div>	Validé	22/01/2020	

Contraintes de mise à jour

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
2_1_2_5_002	La montée de version du serveur mandataire inverse doit être réalisée à partir d'un script interne.	Validé	30/11/2021	

▪ La dernière modification de cette page a été faite le 11 décembre 2023 à 14:03.

Serveur mandataire (Proxy server) version diffusable

Un **serveur mandataire (proxy server)** est un serveur,faisant office d'intermédiaire entre un réseau local et d'autres serveurs, généralement des serveurs Web, permettant ainsi à des données de sortir du réseau local et d'y entrer, sans mettre en danger la sécurité du réseau.

(source : wikipedia,2023 (https://fr.wikipedia.org/wiki/Proxy_inverse))

✓ Terme privilégié : **serveur mandataire**

✓ Equivalent étranger : **proxy server** (en)

Sommaire

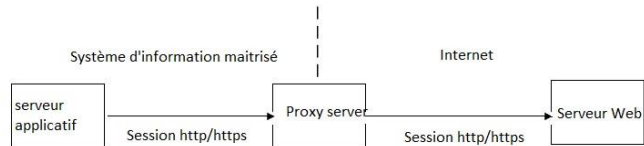
- 1 Contexte
- 2 Règles de base
- 3 Solutions de référence
- 4 Contraintes juridiques et réglementaires
- 5 Contraintes techniques

Contexte

L'offres de services proposée par le service du numérique (SNUM) en termes de **serveur mandataire** s'appuie sur

Le serveur mandataire sert de passerelle d'accès à la zone réseau internet.

L'architecture technique d'un serveur mandataire se décline de la manière suivante :



La haute-disponibilité de ce service est assurée au travers de la redondance des serveurs mandataires, l'utilisation d'une solution de répartition de charge et la mise en œuvre d'un plan de continuité informatique.

Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_1_3_1_001	Le serveur mandataire doit respecter les règles décrites dans le standard ministériel Contrôle de flux sortants et navigation internet (https://hfds-bercy.monportail.alize/files/live/sites/hfds-bercy/files/r%c3%a9pertoires/S%c3%a9curit%c3%a9%20des%20sy st%c3%a8mes%20d'information/documents/Textes%20de%20r%c3%a9f%c3%a9ren ces/180207_controle-flux-sortant_v3.0.pdf)	Validé	21/06/2021	
	2_1_3_1_002	Les serveurs mandataires inverses doivent être installés dans des versions à jour des correctifs de sécurité.	Validé	21/06/2021	

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_1_3_2_001				

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_1_3_3_001				

Contraintes techniques

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_1_3_4_001	Un serveur doit transiter par un serveur mandataire (Proxy Server) pour accéder au réseau internet. L'accès à internet est limité aux usages suivants : - la mise à jour de composants système ou applicatif, - la récupération de données métier, - le fonctionnement des captcha xxx et yyyy	Validé	21/06/2021	
	2_1_3_4_002	L'accès à internet doit être limité à une liste blanche de domaines et s'effectue uniquement via les protocoles HTTP/HTTPS (ports standards 80 et 443).	Validé	21/06/2021	

-
- La dernière modification de cette page a été faite le 23 novembre 2023 à 10:51.

Protection antivirus des postes de travail (Workstation antivirus protection)

version diffusable

Les **antivirus** sont des logiciels conçus pour identifier, neutraliser et éliminer des logiciels malveillants (dont les virus informatique ne sont qu'une catégorie. Ces derniers peuvent se baser sur l'exploitation de failles de sécurité, mais il peut également s'agir de logiciels modifiant ou supprimant des fichiers, que ce soit des documents de l'utilisateur stockés sur l'ordinateur infecté, ou des fichiers nécessaires au bon fonctionnement de l'ordinateur (le plus souvent ceux du système d'exploitation).

(source : wikipedia,2023 (https://fr.wikipedia.org/wiki/Logiciel_antivirus))



Termes privilégiés : **logiciel antivirus**, **antivirus**, **logiciel antiviral**, **logiciel AV**, **logiciel de protection antivirus**



Equivalent anglais: **antivirus software** (en), **antiviral program** (en), **AV program** (en)

Sommaire

- 1 Contexte
- 2 Règles de base
- 3 Solutions de référence
- 4 Contraintes juridiques et réglementaires
- 5 Contraintes techniques

Contexte

L'offre de service proposée par le service du numérique (SNUM) en termes de **protection antivirus des postes de travail** s'appuie sur :

- le logiciel propriétaire **Symantec Endpoint Security 14.3 RU7**.

Elle assure :

- une prévention contre les virus et les malwares et les spywares, une
- protection comportementale avancées contre les menaces, une
- protection contre les menaces web et réseau et les exploitas Zero day

Règles de base

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
2_1_4_1_001	Les postes de travail des agents d'administration centrale doivent être dotés d'un logiciel antivirus et d'un logiciel pare-feu.	Validé	03/12/2019	
2_1_4_1_002	Les logiciels antivirus installés sur les postes de travail des agents d'administration centrale doivent être à jour en termes de correctifs de sécurité.	Validé	03/12/2019	

Solutions de référence

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
2_1_4_2_001	Les postes de travail des agents d'administration centrale doivent être dotés de l'antivirus et du pare-feu Symantec Endpoint Security .	Validé	03/12/2019	Ce logiciel est géré de manière centralisée via la console Symantec.

Contraintes juridiques et réglementaires

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
2_1_4_3_001	Toute demande de support sur le logiciel propriétaire Symantec Endpoint Security doit se faire au travers du marché UGAP multi-éditeurs.	Validé	03/12/2019	Portail support Broadcom (https://support.broadcom.com/)

Contraintes techniques

Contraintes d'installation

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
2_1_4_4_001	Le master déployé sur les postes de travail des agents de l'administration centrale doit intégrer: <ul style="list-style-type: none">■ le logiciel propriétaire Symantec Endpoint protection	Validé	03/12/2019	

Contraintes de mise à jour

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_1_4_5_001	La mise à jour du logiciel propriétaire Symantec endpoint security doit se faire au travers du logiciel propriétaire ZENworks Configuration Management (ZCM).	Validé	03/12/2019	
	2_1_4_5_002	L'application des correctifs de sécurité Microsoft mensuels doit s'effectuer selon le rythme défini par le SNUM.	Validé	03/12/2019	
	2_1_4_5_003	L'application des correctifs de sécurité Microsoft urgents doit s'effectuer selon le rythme défini par le SNUM.	Validé	03/12/2019	

Contraintes d'administration et d'exploitation



	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires

▪ La dernière modification de cette page a été faite le 12 décembre 2023 à 17:52.

Protection antivirus des serveurs (Server antivirus protection) version diffusable

Les **antivirus** sont des logiciels conçus pour identifier, neutraliser et éliminer des logiciels malveillants (dont les virus informatique ne sont qu'une catégorie. Ces derniers peuvent se baser sur l'exploitation de failles de sécurité, mais il peut également s'agir de logiciels modifiant ou supprimant des fichiers, que ce soit des documents de l'utilisateur stockés sur l'ordinateur infecté, ou des fichiers nécessaires au bon fonctionnement de l'ordinateur (le plus souvent ceux du système d'exploitation).

(source : wikipedia,2023 (https://fr.wikipedia.org/wiki/Logiciel_antivirus))

-  Termes privilégiés : **logiciel antivirus, antivirus, logiciel antiviral, logiciel AV, logiciel de protection antivirus**
-  Equivalent anglais: **antivirus software** (en), **antiviral program** (en), **AV program** (en)

Sommaire

1

Contexte

2

Règles de base

3

Solutions de référence

4

Contraintes juridiques et réglementaires

5

Contraintes techniques

Contexte

L'offre de services proposée par le service du numérique (SNUM) en termes de protection antivirus serveurs s'appuie actuellement sur :

- les logiciels propriétaires **Trend Micro Apex One et Apex Central** (pour les serveurs Windows), le logiciel libre **ClamAV** (pour les serveurs Linux).

Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_1_5_1_001	Les serveurs Windows hébergés dans les centres de données de référence du SNUM doivent être dotés d'un logiciel antivirus.	Validé	07/04/2022	
	2_1_5_1_002	Les logiciels antivirus des serveurs Windows hébergés dans les centres de données de référence du SNUM doivent être installés dans des versions à jour des correctifs de sécurité.	Validé	07/04/2022	

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_1_5_2_001	Les antivirus déployés sur les serveurs hébergés dans les centres de données de référence doivent s'appuyer sur : <ul style="list-style-type: none">▪ le logiciel propriétaire Trend Micro Apex One pour les serveurs Windows,▪ le logiciel libre ClamAV pour les serveurs Linux.	Validé	07/04/2022	

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_1_5_3_001	Toute demande de support sur le logiciel propriétaire Trend Apex One doit se faire au travers du marché UGAP multi-éditeurs.	Validé	16/12/2022	
	2_1_5_3_002	Toute demande de support sur le logiciel libre ClamAV doit se faire au travers du marché "Support aux logiciels libres (SLL)".	Validé	16/12/2022	

- La dernière modification de cette page a été faite le 11 décembre 2023 à 15:07.

Protection antipourriel des serveurs (Server antispam protection) version diffusable

Un **pourriel** est un message électronique importun et souvent sans intérêt, constitué essentiellement de publicité, qui est envoyé à un grand nombre d'internautes, sans leur consentement, et que l'on destine habituellement à la poubelle. Le spam, courriel indésirable ou pourriel2 est une communication électronique non sollicitée, en premier lieu via le courrier électronique. Il s'agit en général d'envois en grande quantité effectués à des fins publicitaires.

(source : Wikipedia, 2023 (<https://fr.wikipedia.org/wiki/Spam>))

- ✓ Termes privilégiés : **pourriel**, **courriel non sollicité**, **courriel indésirable**
- ✓ Equivalent étranger: **spam** (en), **spam message** (en), **e-mail spam** (en)

Sommaire

1

Contexte

2

Règles de base

3

Solutions de référence

4

Contraintes juridiques et réglementaires

5

Contraintes techniques

Contexte

Les offres de services proposées par le service du numérique (SNUM) en termes de protection antipourriel des serveurs s'appuient actuellement sur :

- le logiciel libre **SpamAssassin** , le logiciel libre
- **Amavis** , le logiciel libre **Scanmail for**
- **Microsoft Exchange** .

Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_1_6_1_001	Les logiciels de protection antipourriel des serveurs hébergés dans les centres de données de référence du SNUM doivent être installés dans des versions à jour des correctifs de sécurité.	Validé	03/12/2019	

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_1_6_2_001	Les serveurs de relais de messagerie (internes) doivent s'appuyer sur le logiciel libre SpamAssassin .	Validé	03/12/2019	
	2_1_6_2_002	Les serveurs de relais de messagerie (internes) doivent s'appuyer sur le logiciel libre Amavis .	Validé	03/12/2019	
	2_1_6_2_003	Les serveurs de messagerie doivent s'appuyer sur le logiciel propriétaire Scanmail for Microsoft Exchange de la société Trend Micro.	Validé	03/12/2019	

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_1_6_3_001	Toute demande de support sur le logiciel libre SpamAssassin doit se faire au travers du marché "Support à l'usage des logiciels libres".	Validé	03/12/2019	
	2_1_6_3_002	Toute demande de support sur le logiciel libre Amavis doit se faire au travers du marché "Support à l'usage des logiciels libres".	Validé	03/12/2019	[
	2_1_6_3_003	Toute demande de support sur le logiciel propriétaire Scanmail doit se faire au travers du marché "multi-éditeurs".	Validé	03/12/2019	

▪ La dernière modification de cette page a été faite le 11 décembre 2023 à 15:10.

Scanner de vulnérabilité (Vulnerability scanner) version diffusable

Un **scanner de vulnérabilité** est un programme conçu pour identifier des vulnérabilités dans une application, un système d'exploitation, ou un réseau.

(source : wikipedia,2023 (https://fr.wikipedia.org/wiki/Scanneur_de_vuln%C3%A9rabilit%C3%A9))



Termes privilégiés : **scanner de vulnérabilité**,



Equivalent étranger: **vulnerability scanner** (en)

Sommaire

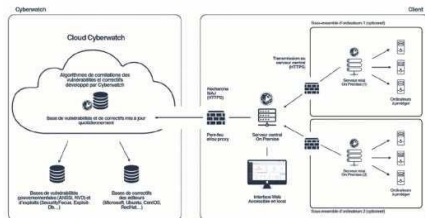
- 1 Contexte
- 2 Règles de base
- 3 Solutions de référence
- 4 Contraintes juridiques et réglementaires
- 5 Contraintes techniques

Contexte

Les offres de services proposées par le service du numérique (SNUM) en termes de scanners de vulnérabilité s'appuient sur :

- le logiciel propriétaire **Cyberwatch** .

L'architecture technique se décline de la manière suivante :



La solution s'articule autour d'un contrôleur central (noeud maître) sur le réseau général (RG) et de satellites installés dans les différentes zones démilitarisées (DMZ)

Elle s'appuie sur les logiciels libres Docker, Kibana, ElasticSearch et la suite logicielle Cyberwatch VM / CM.

Cette suite logicielle Cyberwatch VM / CM est une application de gestion de sécurité des infrastructures informatiques composée :

- du logiciel propriétaire Cyberwatch Vulnerability Manager, logiciel de détection et de supervision des vulnérabilités,
- du logiciel propriétaire Cyberwatch Compliance Manager, logiciel de gestion et de contrôle des conformités.

Cette suite logicielle interagit avec la base de connaissances de Cyberwatch, hébergée en France, dans le Cloud Cyberwatch. Tout utilisateur autorisé à accéder au service

Cyberwatch doit respecter la charte d'utilisation du service Cyberwatch. (<https://documento.alize.finances.rie.gouv.fr/share/s/x5wOp346S0i63TTU5tjHeg>)

Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_1_7_1_001	Les serveurs doivent être intégrés dans le logiciel propriétaire Cyberwatch, y compris : <ul style="list-style-type: none">■ les serveurs inscrits dans une offre d'hébergement sec (https://monalize.alize/sites/Alize/accueil/vie-quotidienne/hebergement-informatique/mon-service-souhaite-beneficier.html),■ les serveurs directionnels.	Validé	18/05/2020	
	2_1_7_1_002	Un scan de découverte doit être lancé périodiquement sur le logiciel propriétaire Cyberwatch, afin d'identifier les serveurs non encore enrôlés : <ul style="list-style-type: none">■ tous les mois pour la DMZ Web,■ tous les 6 mois pour les autres zones.	Validé	18/05/2020	
	2_1_7_1_003	Les serveurs aux contraintes de sécurité élevées doivent être enrôlés avec l'agent Cyberwatch, à savoir : <ul style="list-style-type: none">■ les serveurs de messagerie (Microsoft Exchange),■ les serveurs Windows,■ les serveurs Microsoft Windows Server avec le rôle Services Active Directory Domain Services (AD DS) en mode hors ligne,■ les serveurs ESXi en mode hors ligne.	Validé	03/12/2020	
	2_1_7_1_004	Le logiciel propriétaire Cyberwatch ne doit pas être utilisé pour corriger directement les vulnérabilités des serveurs.	Validé	18/05/2020	

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_1_7_2_001	Les scanners de vulnérabilité doivent s'appuyer sur l'un des logiciels suivants : <ul style="list-style-type: none">le logiciel propriétaire Cyberwatch ,le logiciel propriétaire Tenable Nessus Professional .	Validé	18/05/2020	Cycle de vie du logiciel Cyberwtach (https://docs.cyberwatch.fr/en/10_general_administration_software/latest/release_lifecycle.html)

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_1_7_3_001	Toute demande de support sur le logiciel propriétaire Cyberwatch doit se faire au travers du marché multi-éditeurs.	Validé	18/05/2020	Portail support Cyberwatch

▪ La dernière modification de cette page a été faite le 11 décembre 2023 à 15:12.

Chiffrement (Encryption) version diffusable

Le **chiffrement** est un procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de (dé)chiffrement. Ce principe est généralement lié au principe d'accès conditionnel.

(source : wikipedia,2023 (<https://fr.wikipedia.org/wiki/Chiffrement>))

- ✓ Termes privilégiés : **chiffrement**, **cryptage**
- ✓ Equivalents anglais: **encryption** (en), **encipherment** (en), **enciphering** (en), **ciphering** (en)

Sommaire

1

Contexte

2

Règles de base

3

Solutions de référence

4

Contraintes juridiques et réglementaires

5

Contraintes techniques

Contexte

L'offre de services proposée par le service du numérique (SNUM) en termes de **chiffrement** s'appuie sur :

- le logiciel libre **OpenSSL**.

Quelques liens utiles sur les recommandations et les bonnes pratiques autour du chiffrement :

- OWASP : Sensitive Data Exposure (https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure)

Règles de base

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
2_1_8_1_001	Les solutions de référence de chiffrement de flux doivent être installés dans des versions à jour des correctifs de sécurité.	Validé	03/09/2019	

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_1_8_2_001	Les solutions de chiffrement doivent s'appuyer sur le logiciel libre OpenSSL .	Validé	03/09/2019	Cycle de vie du logiciel OpenSSL (https://www.openssl.org/policies/releasestrat.html)

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_1_8_3_001	Toute demande de support sur le logiciel libre OpenSSL doit se faire au travers du marché "Support à l'usage des logiciels libres" (SLL).	Validé	03/09/2019	

Contraintes techniques

Contraintes d'installation

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_1_8_4_001	Le logiciel libre OpenSSL doit être installé à partir du serveur de dépôt interne Linux.	Validé	03/09/2019	
	2_1_8_4_002	Les communications HTTP doivent être réalisées sur un canal chiffré en utilisant TLS 1.2 ou 1.3 sur l'ensemble du trafic.	Validé	08/03/2023	

Contraintes de mise à jour

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_1_8_5_001				

Contraintes d'administration et d'exploitation

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_1_8_6_001				

Contraintes techniques

Suites cryptographiques

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires												
	2_1_8_7_001	<div>Les suites cryptographiques ci-dessous doivent être utilisées avec le protocole TLS 1.2 :</div> <table><tr><th>Code TLS</th><th>Suite cryptographique</th></tr><tr><td>0xC02C</td><td>TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384</td></tr><tr><td>0xC02B</td><td>TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256</td></tr><tr><td>0xC0AD</td><td>TLS_ECDHE_ECDSA_WITH_AES_256_CCM</td></tr><tr><td>0xC0AC</td><td>TLS_ECDHE_ECDSA_WITH_AES_128_CCM</td></tr><tr><td>0xCCA9</td><td>TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256</td></tr></table>	Code TLS	Suite cryptographique	0xC02C	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	0xC02B	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	0xC0AD	TLS_ECDHE_ECDSA_WITH_AES_256_CCM	0xC0AC	TLS_ECDHE_ECDSA_WITH_AES_128_CCM	0xCCA9	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	Validé	28/09/2021	
Code TLS	Suite cryptographique																
0xC02C	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384																
0xC02B	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256																
0xC0AD	TLS_ECDHE_ECDSA_WITH_AES_256_CCM																
0xC0AC	TLS_ECDHE_ECDSA_WITH_AES_128_CCM																
0xCCA9	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256																
	2_1_8_7_002	<div>Les suites cryptographiques ci-dessous doivent être utilisées avec le protocole TLS 1.3 :</div> <table><tr><th>Code TLS</th><th>Suite cryptographique</th></tr><tr><td>0x1302</td><td>TLS_AES_256_GCM_SHA384</td></tr><tr><td>0x1303</td><td>TLS_CHACHA20_POLY1305_SHA256</td></tr><tr><td>0x1301</td><td>TLS_AES_128_GCM_SHA256</td></tr><tr><td>0x1304</td><td>TLS_AES_128_CCM_SHA256</td></tr></table>	Code TLS	Suite cryptographique	0x1302	TLS_AES_256_GCM_SHA384	0x1303	TLS_CHACHA20_POLY1305_SHA256	0x1301	TLS_AES_128_GCM_SHA256	0x1304	TLS_AES_128_CCM_SHA256	Validé	28/09/2021			
Code TLS	Suite cryptographique																
0x1302	TLS_AES_256_GCM_SHA384																
0x1303	TLS_CHACHA20_POLY1305_SHA256																
0x1301	TLS_AES_128_GCM_SHA256																
0x1304	TLS_AES_128_CCM_SHA256																

▪ La dernière modification de cette page a été faite le 11 décembre 2023 à 15:15.

Serveur web (Web server) version diffusable

Un **serveur web** est soit un logiciel de service de ressources web (serveur HTTP), soit un serveur informatique (ordinateur) qui répond à des requêtes du World Wide Web sur un réseau public (Internet) ou privé (intranet) en utilisant principalement le protocole HTTP.

Un serveur informatique peut être utilisé à la fois pour servir des ressources du Web et pour faire fonctionner en parallèle d'autres services liés, comme l'envoi d'e-mails, l'émission de flux en streaming, le stockage de données dans des bases de données, le transfert de fichiers par FTP.

(source : wikipedia,2023 (https://fr.wikipedia.org/wiki/Serveur_web))



Termes privilégiés : **serveur web**, **serveur HTTP**



Equivalent étranger: **web server** (en), **HTTP server** (en)

Sommaire

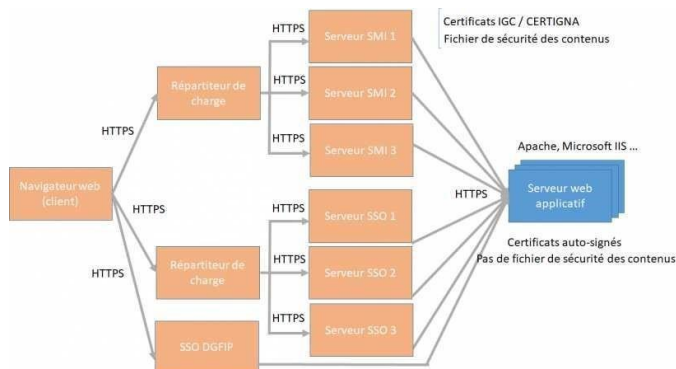
- 1 Contexte
- 2 Règles de base
- 3 Solutions de référence
- 4 Contraintes juridiques et réglementaires
- 5 Contraintes techniques

Contexte

L'offre de services proposée par le service numérique (SNUM) en termes de serveurs web applicatifs s'appuie actuellement sur :

- le logiciel libre **Apache 2.4** pour les serveurs applicatifs Linux, le logiciel propriétaire **Microsoft IIS 10** pour les serveurs applicatifs Windows.

Comme indiqué dans le schéma ci-dessous, les **serveurs web applicatifs** sont interfacés avec des serveurs mandataire inverses (SMI) et/ou des serveurs d'authentification unique (SSO) . Pour répondre à des besoins spécifiques, ils peuvent être également interfacés avec d'autres systèmes d'authentification tels que le **SSO DGFIP**.



Il convient de préciser que les **règles de stratégie de sécurité des contenus** s'appliquent systématiquement sur les environnements de recette et de production des serveurs mandataires inverses (SMI) et/ou des serveurs d'authentification unique (SSO).

Par contre, ces règles doivent s'appliquer sur les environnements de développement des serveurs web applicatifs et/ou des serveurs d'application afin de faciliter le travail d'intégration des projets et des applications.



L'installation du serveur web Apache étant spécifique (**installation à partir du code source** et non à partir de paquets RPM), il sera donc préinstallé sur les serveurs virtuels (VM) au travers de l'orchestrateur VMware.

Règles de base

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
2_3_1_1_001	Les nouvelles applications basées sur des serveurs web doivent respecter le standard ministériel Homologation d'une application web hébergée sur Internet. (http://hfds-bercy.monportail.alize/files/live/sites/hfds-bercy/files/r/%c3%a9pertoires/S%c3%a9curit%c3%a9%20des%20syst%c3%a8mes%20d'information/documents/Textes%20de%20r%c3%a9f%c3%a9rences/170112_guide-homologation-appli-web-hebergee_v2.0.0.pdf)	Validé	01/07/2019	
2_3_1_1_002	Les nouvelles applications basées sur des serveurs web doivent respecterle standard ministériel Protections contre les injections de contenu, code, XSS et autres menaces sur les applications et sites web (http://hfds-bercy.monportail.alize/files/live/sites/hfds-bercy/files/r/%c3%a9pertoires/S%c3%a9curit%c3%a9%20des%20syst%c3%a8mes%20d'information/documents/Textes%20de%20r%c3%a9f%c3%a9rences/180503_standard-HTTP-headers_v4.2.pdf).	Validé	01/07/2019	
2_3_1_1_003	Les nouvelles applications basées sur des serveurs web doivent respecter le standard ministériel Protections des systèmes d'information accessibles par API (http://hfds-bercy.monportail.alize/files/live/sites/hfds-bercy/files/r/%c3%a9pertoires/S%c3%a9curit%c3%a9%20des%20syst%c3%a8mes%20d'information/documents/Textes%20de%20r%c3%a9f%c3%a9rences/170505_protections-API_v1.pdf).	Validé	01/07/2019	
2_3_1_1_004	Les nouvelles applications basées sur des serveurs web doivent respecter le standard ministériel URI et supervision pour diagnostiquer l'indisponibilité de services web (http://hfds-bercy.monportail.alize/files/live/sites/hfds-bercy/files/r/%c3%a9pertoires/S%c3%a9curit%c3%a9%20des%20syst%c3%a8mes%20d'information/documents/Textes%20de%20r%c3%a9f%c3%a9rences/180503_standard-URI-diagnostic-signalment_v2.1.pdf).	Validé	01/07/2019	
2_3_1_1_005	Les nouvelles applications basées sur des serveurs web doivent respecter le standard ministériel Déploiement du protocole TLS (https://hfds-bercy.monportail.alize/files/live/sites/hfds-bercy/files/r/%c3%a9pertoires/S%c3%a9curit%c3%a9%20des%20syst%c3%a8mes%20d'information/d ocuments/Textes%20de%20r%c3%a9f%c3%a9rences/171026_TLS_v12.0.pdf)	Validé	01/07/2019	
2_3_1_1_006	Les nouvelles applications basées sur des serveurs web doivent s'interfacer avec les serveurs mandataires inverses en cas d'incompatibilité avec les serveurs d'authentification unique (SSO).	Validé	01/07/2019	
2_3_1_1_007	Les serveurs web doivent être installés dans des versions à jour des correctifs de sécurité.	Validé	03/09/2019	

Solutions de référence


Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
2_3_1_2_001	Les serveurs web doivent s'appuyer sur : - le logiciel libre Apache 2.4 pour les serveurs applicatifs Linux - le logiciel propriétaire Microsoft IIS 10 pour les serveurs applicatifs Windows	Validé	03/09/2019	
2_3_1_2_002	Les nouvelles applications nécessitant l'usage d'un serveur web ne s'appuyant pas sur le logiciel libre Apache doivent faire l'objet d'une justification.	Validé	01/07/2019	

Contraintes juridiques et réglementaires

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
2_3_1_3_001	Toute demande de support sur le logiciel libre Apache doit se faire au travers du portail support SLL (https://www.otrs.aosc-portal.com/otrs/customer.pl).	Validé	01/07/2019	-

Contraintes techniques

Contraintes d'installation

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
2_3_1_4_001	L'installation des serveurs web basés sur le logiciel libre Apache doit être réalisée à partir d'un script interne au SNUM.	Validé	30/11/2021	
2_3_1_4_002	L'installation du logiciel libre Anache doit respecter l'arborescence suivante :  ▪ Répertoire des fichiers binaires : /applis/apache-[version] où [version] correspond au numéro de version du logiciel ▪ Répertoire des fichiers de configuration : /applis/www/conf	Validé	03/12/2019	

Contraintes de mise à jour

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
2_3_1_5_001	La montée de version du serveur web doit être réalisée à partir d'un script interne au SNUM.	Validé	30/11/2021	

Serveur d'application (Application server) version diffusable

Un **serveur d'application** est un logiciel d'infrastructure offrant un contexte d'exécution pour des composants applicatifs. Au sens strict les composants hébergés par le serveur d'applications ne sont pas de simples procédures ou scripts mais de réels composants logiciels conformes à un modèle de composants (EJB, COM, Fractal, etc.). (source : Wikipedia,2023 (https://fr.wikipedia.org/wiki/Serveur_d%27applications))

✓ Termes privilégiés : **serveur d'application**

✓ Equivalent étranger: **application server** (en)

La version de base de cette rubrique est accessible [ici](#)

Sommaire

- 1 Contexte
- 2 Règles de base
- 3 Solutions de référence
- 4 Contraintes juridiques et réglementaires
- 5 Contraintes techniques

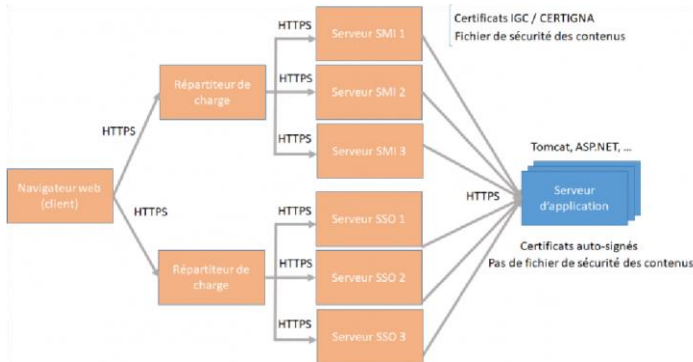
Contexte

Les offres de services proposées par le service du numérique (SNUM) en termes de serveurs d'application s'appuient sur :

- le logiciel libre **Apache Tomcat 10.1** pour les serveurs d'application Linux,
- le logiciel propriétaire **Microsoft ASP.NET Core 6.0** pour les serveurs d'application Windows.

⚠ L'installation du serveur d'application Tomcat étant spécifique (**installation à partir du code source** et non à partir de paquets RPM), il sera donc préinstallé sur les serveurs virtuels (VM) au travers de l'orchestrateur VMware.

Comme indiqué dans le schéma ci-dessous, les **serveurs d'application** sont interfacés avec des serveurs mandataire inverses (SMI) et/ou des serveurs d'authentification unique (SSO). Pour répondre à des besoins spécifiques, ils peuvent être également interfacés avec d'autres systèmes d'authentification tels que le **SSO DGFIP** ou encore **AgentConnect**.



⚠ Il convient de préciser que les **règles de stratégie de sécurité des contenus** s'appliquent systématiquement sur les environnements de recette et de production. Par contre, elles ne doivent pas s'appliquer sur les environnements de développement afin de faciliter le travail d'intégration des projets et des applications.

Règles de base

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
2_4_1_1_001	Les nouvelles applications nécessitant l'usage d'un serveur d'application doivent respecter le standard ministériel (170112_guide-homologation-appli-web-hebergee_v2.0.0.pdf) Homologation d'une application web hébergée sur Internet.	Validé	01/07/2019	
2_4_1_1_002	Les nouvelles applications nécessitant l'usage d'un serveur d'application doivent respecter le standard ministériel (180503_standard-HTTP-headers_v4.2.pdf) Protections contre les injections de contenu, code, XSS et autres menaces sur les applications et sites web.	Validé	01/07/2019	
2_4_1_1_003	Les nouvelles applications nécessitant l'usage d'un serveur d'application doivent respecter le standard ministériel (170505_protections-API_v1.pdf) Protections des systèmes d'information accessibles par API.	Validé	01/07/2019	
2_4_1_1_004	Les nouvelles applications nécessitant l'usage d'un serveur d'application doivent respecter le standard ministériel (180503_standard-URI-diagnostic-signalement_v2.1.1.pdf) URI et supervision pour diagnostiquer l'indisponibilité de services web.	Validé	01/07/2019	
2_4_1_1_005	Les nouvelles applications nécessitant l'usage d'un serveur d'application doivent respecter le standard ministériel (171026_TLS_v12.0.pdf) Déploiement du protocole TLS.	Validé	01/07/2019	
2_4_1_1_006	Les serveurs d'application doivent être installés dans des versions à jour des correctifs de sécurité.	Validé	03/09/2019	
2_4_1_1_007	Les serveurs d'application doivent récupérer le champ X-Forwarded-For transmis par les serveurs mandataires inverses (SMI) ou les serveurs d'authentifications (SSO) et le faire figurer dans les journaux.	Validé	09/02/2022	

Solutions de référence

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
2_4_1_2_001	Les serveurs d'application doivent s'appuyer sur : <ul style="list-style-type: none">le logiciel libre Apache Tomcat v10.1 pour les serveurs Linuxle logiciel propriétaire Microsoft ASP.NET 4.8 pour les serveurs Windows	Validé	08/03/2023	
2_4_1_2_002	Les nouvelles applications nécessitant l'usage d'un serveur d'application ne s'appuyant pas sur le logiciel libre Apache Tomcat doivent faire l'objet d'une justification technique.	Validé	01/07/2019	

Contraintes juridiques et réglementaires

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
2_4_1_3_001	Toute demande de support sur le logiciel libre Apache Tomcat doit se faire au travers du portail SLL (https://www.otrs.aosc-portal.com/otrs/customers).	Validé	01/07/2019	
2_4_1_3_002	Toute demande de support sur le logiciel propriétaire Microsoft ASP.NET Core doit se faire au travers du portail support Microsoft (https://serviceshub.microsoft.com/home).	Validé	08/03/2023	

Contraintes techniques

Contraintes d'installation

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
2_4_1_4_001	L'installation du logiciel libre Apache Tomcat doit être réalisée à partir du playbook Ansible "sep1c.apache-tomcat.yml".	Validé	09/02/2022	
2_4_1_4_002	<p>L'installation du logiciel libre Apache Tomcat doit respecter l'arborescence suivante:</p> <pre>apache-tomcat ├── bin ├── conf -> /applis/apache-tomcat-files/conf ├── conf_original ├── lib ├── logs ├── temp ├── webapps ├── webapps-javaee └── work</pre> <ul style="list-style-type: none">▪ Répertoire des fichiers binaires: /applis/apache-tomcat-[version]/bin▪ Répertoire des fichiers externalisés de Tomcat (conf, bin (setenv.sh seulement), keystore et webapps): /applis/apache-tomcat-files▪ Lien symbolique pointant vers la dernière version de Tomcat installée: /applis/apache-tomcat <p>où [version] correspond au numéro de version du logiciel.</p>	Validé	11/09/2023	
2_4_1_4_003	<p>Les fichiers log du logiciel libre Apache Tomcat doivent être localisés dans le répertoire /logs/tomcat</p> <pre>/logs/tomcat/ ├── catalina.2020-03-03.log ├── catalina.2020-03-04.log ├── catalina.2020-03-06.log ├── host-manager.2020-03-03.log ├── host-manager.2020-03-04.log ├── localhost.2020-03-03.log ├── localhost.2020-03-04.log ├── localhost.2020-03-06.log ├── localhost_access_log.2020-03-03.log ├── localhost_access_log.2020-03-04.log ├── manager.2020-03-03.log └── manager.2020-03-04.log</pre>	Validé	18/05/2020	
2_4_1_4_004	Les applications web sous forme de fichiers WAR (https://fr.wikipedia.org/wiki/WAR_(format_de_fichier)) doivent être installées dans le répertoire /applis/apache-tomcat-files/webapps	Validé	11/09/2023	
2_4_1_4_005	<p>Un lien symbolique nommé "apache-tomcat" doit pointer sur le dossier d'installation de la dernière version de Tomcat installée et doit être placé dans le répertoire /applis</p> <p>Ci-dessous un exemple d'arborescence du répertoire /applis avec plusieurs versions de Tomcat installées:</p> <pre>/applis/ ├── apache-tomcat -> apache-tomcat-10.1.13/ ├── apache-tomcat-10.1.13 ├── apache-tomcat-8.5.93 └── apache-tomcat-files</pre>	Validé	11/09/2023	

Contraintes de mise à jour

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
2_4_1_5_001				

Environnement d'exécution PHP (PHP runtime environment) version diffusable

Un **environnement d'exécution** est un logiciel responsable de l'exécution des programmes informatiques écrits dans un langage de programmation donné.

Le **langage PHP** (Hypertext Preprocessor) est un langage de programmation libre, principalement utilisé pour produire des pages Web dynamiques via un serveur HTTP, mais pouvant également fonctionner comme n'importe quel langage interprété de façon locale. PHP est un langage impératif orienté objet. (source : Wikipedia,2023 (<https://fr.wikipedia.org/wiki/PHP>))

- ✓ Termes privilégiés :**environnement d'exécution**
- ✓ Equivalent étranger: **execution environment** (en), **runtime** (en) La

version de base de cette rubrique est accessible ici

Sommaire

1 Contexte

2 Règles de base

3 Solutions de référence

4 Contraintes juridiques et réglementaires 5 Contraintes techniques

Contexte

L'offre de services proposée par le service du numérique (SNUM) en termes d'**environnement d'exécution PHP** s'appuie sur :

- le logiciel libre **APACHE 2.4**
- le logiciel libre **PHP 8.2**

La version 8 du langage PHP s'appuie sur la version 4 du moteur Zend et propose de nouvelles fonctionnalités comme la gestion des types, la gestion des erreurs ou encore l'amélioration des performances.

Règles de base

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
2_4_2_1_001	Toute nouvelle application développée en PHP doit respecter le standard ministériel Homologation d'une application web hébergée sur Internet. (http://hfds-bercy.monportail.alize/files/live/sites/hfds-bercy/files/r/c3a9pertoires/S/c3a9curit% c3a9%20des%20syst% c3a8mes%20d'information/documents/Textes%20de%20r% c3a9f% c3a9rences/170112_guide -homologation-appli-web-hebergee_v2.0.0.pdf)	Validé	01/07/2019	
2_4_2_1_002	Toute nouvelle application développée en PHP doit respecter le standard ministériel Protections contre les injections de contenu, code, XSS et autres menaces sur les applications et sites web (http://hfds-bercy.monportail.alize/files/live/sites/hfds-bercy/files/r/c3a9pertoires/S/c3a9curit% c3a9%20des%20syst% c3a8mes%20d'information/documents/Textes%20de%20r% c3a9f% c3a9rences/180503_standard-HTTP-headers_v4.2.pdf).	Validé	01/07/2019	
2_4_2_1_003	Toute nouvelle application basée sur un serveur web doit respecter le standard ministériel respecter le standard ministériel Protections des systèmes d'information accessibles par API (http://hfds-bercy.monportail.alize/files/live/sites/hfds-bercy/files/r/c3a9pertoires/S/c3a9curit% c3a9%20des%20syst% c3a8mes%20d'information/documents/Textes%20de%20r% c3a9f% c3a9rences/170505_protections-API_v1.pdf).	Validé	01/07/2019	
2_4_2_1_004	Toute nouvelle application développée en PHP doit respecter le standard ministériel URI et supervision pour diagnostiquer l'indisponibilité de services web (http://hfds-bercy.monportail.alize/files/live/sites/hfds-bercy/files/r/c3a9pertoires/S/c3a9curit% c3a9%20des%20syst% c3a8mes%20d'information/documents/Textes%20de%20r% c3a9f% c3a9rences/180503_standard-URI-diagnostic-signalement_v2.1.pdf).	Validé	01/07/2019	
2_4_2_1_005	Toute nouvelle application développée en PHP doit respecter le standard ministériel Déploiement du protocole TLS (https://hfds-bercy.monportail.alize/files/live/sites/hfds-bercy/files/r/c3a9pertoires/S/c3a9curit% c3a9%20des%20syst% c3a8mes%20d'information/documents/Textes%20de%20r% c3a9f% c3a9rences/171026_TLS_v12.0.pdf)	Validé	01/07/2019	
2_4_2_1_006	L'environnement d'exécution PHP doit être installé dans des versions à jour des correctifs de sécurité.	Validé	03/09/2019	

Solutions de référence

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
2_4_2_2_001	L'environnement d'exécution PHP doit s'appuyer sur le logiciel libre PHP version 8.2 .	Validé	08/03/2023	

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_4_2_3_001	Toute demande de support sur le logiciel libre PHP doit se faire au travers du portail SLL (https://www.otrs.aosc-portal.com/otrs/customerspl).	Validé	01/07/2019	

Contraintes techniques

Contraintes d'installation

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
2_4_2_4_001	L'installation de l'environnement d'exécution PHP doit être réalisée à partir d'un script interne.	Validé	30/11/2021	

Contraintes de mise à jour

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
2_4_2_5_001	La montée de version de l'environnement d'exécution PHP doit être réalisée à partir du script interne.	Validé	30/11/2021	

Contraintes d'administration et exploitation

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
2_4_2_6_001				



▪ La dernière modification de cette page a été faite le 25 février 2024 à 07:27.

Environnement d'exécution JAVA (JAVA runtime environment) version diffusable

Un **environnement d'exécution** est un logiciel responsable de l'exécution des programmes informatiques écrits dans un langage de programmation donné. Il offre des services d'exécution de programmes tels que les entrées-sorties, l'arrêt des processus, l'utilisation des services du système d'exploitation, le traitement des erreurs de calcul, la génération d'événements, l'utilisation de services offerts dans un autre langage de programmation, le débogage, le profilage et le ramasse-miette.

Un **environnement d'exécution Java** est une famille de logiciels qui permet l'exécution des programmes écrits en langage de programmation Java, sur différentes plateformes informatiques.

(source : wikipedia,2023 (https://fr.wikipedia.org/wiki/Environnement_d%27ex%C3%A9cution_Java))

-  Termes privilégiés : **environnement d'exécution**
-  Equivalent étranger: **execution environment** (en), **JAVA Runtime Environment** (en), **JRE** (en) La version de base de cette rubrique est accessible ici

Sommaire

1

Contexte

2

Règles de base

3

Solutions de référence

4

Contraintes juridiques et réglementaires

5

Contraintes techniques

Contexte

L'offre de services proposée par le service du numérique (SNUM) en termes d'**environnement d'exécution JAVA** s'appuie sur :

- le logiciel libre **Open JRE** (sous-ensemble du logiciel libre **OpenJDK**).

Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_4_3_1_001	Toute nouvelle application développée en JAVA doitrespecter le standard ministériel (guide-homologation-appli-web-hebergee_v2.0.0.pdf) Homologation d'une application web hébergée sur Internet.	Validé	03/12/2019	
	2_4_3_1_002	Toute nouvelle application développée en JAVA doitrespecter le standard ministériel (standard-HTTP-headers_v4.2.pdf) Protections contre les injections de contenu, code, XSS et autres menaces sur les applications et sites web.	Validé	03/12/2019	
	2_4_3_1_003	Toute nouvelle application développée en JAVA doitrespecter le standard ministériel (protections-API_v1.pdf) Protections des systèmes d'information accessibles par API.	Validé	03/12/2019	
	2_4_3_1_004	Toute nouvelle application développée en JAVA doitrespecter le standard ministériel (standard-URI-diagnostic-signalment_v2.1.pdf) URI et supervision pour diagnostiquer l'indisponibilité de services web.	Validé	03/12/2019	
	2_4_3_1_005	Toute nouvelle application développée en JAVA doitrespecter le standard ministériel (TLS_v12.0.pdf) Déploiement du protocole TLS.	Validé	03/12/2019	
	2_4_3_1_006	L'environnement d'exécution JAVA doit être installé dans des versions à jour des correctifs de sécurité.	Validé	03/12/2019	-

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_4_3_2_001	L'environnement d'exécution JAVA doit s'appuyer sur le logiciel libre OpenJDK 17 (LTS) .	Validé	08/03/2023	

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_4_3_3_001	Toute demande de support sur le logiciel libre OpenJDK doit se faire au travers du marché "Support à l'usage des logiciels libres" (SIL).	Validé	01/07/2019	

Contraintes techniques

Contraintes d'installation

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
2_4_3_4_001	L'installation du logiciel libre OpenJDK doit se faire depuis le serveur de dépôt interne Linux via les fichiers au format RPM (Red Hat Package Manager).	Validé	11/09/2023	

Contraintes de mise à jour

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
2_4_3_5_001	La mise à jour du logiciel libre OpenJDK doit se faire depuis le serveur de dépôt interne Linux via les fichiers au format RPM (Red Hat Package Manager).	Validé	11/09/2023	

Contraintes d'administration et d'exploitation

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
2_4_3_6_001				

▪ La dernière modification de cette page a été faite le 25 février 2024 à 07:26.

Environnement d'exécution .NET (.NET runtime environment) version diffusable

Un **environnement d'exécution** est un logiciel responsable de l'exécution des programmes informatiques écrits dans un langage de programmation donné. Il offre des services d'exécution de programmes tels que les entrées-sorties, l'arrêt des processus, l'utilisation des services du système d'exploitation, le traitement des erreurs de calcul, la génération d'événements, l'utilisation de services offerts dans un autre langage de programmation, le débogage, le profilage et le ramasse-miette.

(source : wikipedia,2023 (https://fr.wikipedia.org/wiki/Environnement_d%27ex%C3%A9cution))

Microsoft .NET est un environnement d'exécution pouvant s'exécuter sur un système d'exploitation Microsoft Windows (source : wikipedia,2022 (https://fr.wikipedia.org/wiki/Framework_.NET))

- ✓ Termes privilégiés : **environnement d'exécution**
- ✓ Equivalent étranger: **execution environment** (en), **Microsoft .NET** (en)

La version de base de cette rubrique est accessible [ici](#)

Sommaire

1

Contexte

2

Règles de base

3

Solutions de référence

4

Contraintes juridiques et réglementaires

5

Contraintes techniques

Contexte

L'offre de services proposée par le service du numérique (SNUM) en termes d'**environnement d'exécution Microsoft .NET** s'appuie sur :

- le logiciel propriétaire **Microsoft .NET Framework**
- **4.8.** le logiciel propriétaire **Microsoft .NET Core 7.0.**

Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_4_4_1_001	Toute application développée avec l'environnement Microsoft .NET doit respecter le standard ministériel (guide-homologation-appli-web-hebergee_v2.0.0.pdf) Homologation d'une application web hébergée sur Internet.	Validé	14/04/2021	
	2_4_4_1_002	Toute application développée avec l'environnement Microsoft .NET doit respecterle standard ministériel (standard-HTTP-headers_v4.2.pdf) Protections contre les injections de contenu, code, XSS et autres menaces sur les applications et sites web.	Validé	14/04/2021	
	2_4_4_1_003	Toute application développée avec l'environnement Microsoft .NET doit respecter le standard ministériel respecter le standard ministériel (protections-API_v1.pdf) Protections des systèmes d'information accessibles par API].	Validé	14/04/2021	
	2_4_4_1_004	Toute application développée avec l'environnement Microsoft .NET doit respecter le standard ministériel (standard-URI-diagnostic-signalment_v2.1.pdf) URI et supervision pour diagnostiquer l'indisponibilité de services web.	Validé	14/04/2021	
	2_4_4_1_005	Toute application développée avec l'environnement Microsoft .NET doit respecter le standard ministériel (TLS_v12.0.pdf) Déploiement du protocole TLS]	Validé	14/04/2021	
	2_4_4_1_006	L'environnement d'exécution Microsoft .NET doit être installé dans des versions à jour des correctifs de sécurité.	Validé	14/04/2021	

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_4_4_2_001	La solution de référence doit s'appuyer sur le logiciel propriétaire Microsoft .NET 4.8	Validé	16/12/2022	

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_4_4_3_001	Toute demande de support sur le logiciel propriétaire Microsoft .NET doit se faire au travers du marché UGAP multi-éditeur.	Validé	14/04/2021	

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_4_4_4_001	L'installation du logiciel propriétaire Microsoft .NET doit se faire à partir des fichiers sources disponibles depuis le site officiel.	Validé	14/04/2021	

Contraintes techniques

Contraintes d'installation

Montée de version

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_4_6_5_001	La mise à jour du logiciel propriétaire Microsoft .NET Framework doit se faire depuis le serveur de dépôt interne Windows Server Update Services (WSUS).	Validé	14/04/2021	

Administration et exploitation

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_4_6_6_001				

▪ La dernière modification de cette page a été faite le 13 décembre 2023 à 11:09.

Serveur de relais de messagerie version diffusable

Un **serveur de relais de messagerie** est un serveur de courrier électronique utilisé pour rediriger, vers des destinataires externes, des messages en transit provenant de l'extérieur, tout en leur attribuant une nouvelle adresse d'expéditeur.

(source : Office québécois de la langue française,2002 (http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8362090))



Termes privilégiés : **relais de messagerie**



Equivalent étranger: **mail relay** (en)

Sommaire

- 1 Contexte
- 2 Règles de base
- 3 Solutions de référence
- 4 Contraintes juridiques et réglementaires
- 5 Contraintes techniques

Contexte

Les offres de serveurs de relais de messagerie proposées par le SNUM BITS s'appuient sur le logiciel libre **Postfix 3.5**

On distingue trois types de serveurs de relais de messagerie :

- Serveurs de relais de messagerie interne,
- Serveurs de relais de messagerie externe (exposés sur le réseau internet),
- Serveurs de relais de messagerie RIE.

Règles de base

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
2_4_5_1_001	Les serveurs de relais de messagerie de la sous-direction du numérique d'administration centrale (SDNAC) doivent respecter le standard ministériel (guide-homologation-email_v1.0.0.pdf) Homologation de services Email .	Validé	01/07/2019	
2_4_5_1_002	Les serveurs de relais de messagerie de la sous-direction du numérique d'administration centrale (SDNAC) doiventrespecter le standard ministériel (170112_standard-SPF_v4.pdf) Standard SPF et lutte contre l'usurpation d'email.	Validé	01/07/2019	
2_4_5_1_003	Les serveurs de relais de messagerie de la sous-direction du numérique d'administration centrale (SDNAC) doivent respecter le standard ministériel (180213_standard-relais-SMTP_v2.pdf) Relais SMTP, authenticité et confidentialité des courriels.	Validé	01/07/2019	
2_4_5_1_004	Les serveurs de relais de messagerie de la sous-direction du numérique d'administration centrale (SDNAC) doiventrespecter le standard ministériel (170307_guide-technique-DKIM-DMARC-STARTTLS-MIME_v1.pdf) Guide technique DKIM, DMARC, STARTTLS, MIME.	Validé	01/07//2019	
2_4_5_1_005	Les serveurs de relais de messagerie de la sous-direction du numérique d'administration centrale (SDNAC) doivent respecter le standard ministériel (171026_TLS_v12.0.pdf) Déploiement du protocole TLS.	Validé	01/07//2019	
2_4_5_1_006	Les serveurs de relais de messagerie doivent être installés dans des versions à jour des correctifs de sécurité.	Validé	03/12/2019	

Solutions de référence

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
2_4_5_2_001	<p>Les serveurs de relais de messagerie doivent s'appuyer sur les logiciels suivants :</p> <ul style="list-style-type: none">▪ Au niveau des relais de messagerie externe<ul style="list-style-type: none">▪ le logiciel librePostfix (https://fr.wikipedia.org/wiki/Postfix)▪ le logiciel libreOpenDMARC (https://fr.wikipedia.org/wiki/DMARC)▪ le logiciel libreOpenDKIM (https://fr.wikipedia.org/wiki/DomainKeys_Identified_Mail)▪ Au niveau des relais de messagerie interne<ul style="list-style-type: none">▪ lelogiciel librePostfix (https://fr.wikipedia.org/wiki/Postfix)▪ le logiciel libreAmavis (https://en.wikipedia.org/wiki/Amavis)▪ le logiciel libreClamAV (https://fr.wikipedia.org/wiki/ClamAV)▪ le logiciel libreSpamAssassin (https://fr.wikipedia.org/wiki/SpamAssassin)	Validé	03/12/2019	

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_4_5_3_001	Toute demande de support sur le logiciel libre Postfix doit se faire au travers du marché "Support à l'usage des logiciels libres".	Validé	03/12/2019	
	2_4_5_3_002	Toute demande de support sur le logiciel libre OpenDMARC doit se faire au travers du marché "Support à l'usage des logiciels libres".	Validé	03/12/2019	
	2_4_5_3_003	Toute demande de support sur le logiciel libre OpenDKIM doit se faire au travers du marché "Support à l'usage des logiciels libres".	Validé	03/12/2019	
	2_4_5_3_004	Toute demande de support sur le logiciel libre SpamAssassin doit se faire au travers du marché "Support à l'usage des logiciels libres".	Validé	03/12/2019	
	2_4_5_3_005	Toute demande de support sur le logiciel libre Amavis doit se faire au travers du marché "Support à l'usage des logiciels libres".	Validé	03/12/2019	
	2_4_5_3_006	Toute demande de support sur le logiciel libre ClamAV doit se faire au travers du marché "Support à l'usage des logiciels libres".	Validé	03/12/2019	

Contraintes techniques

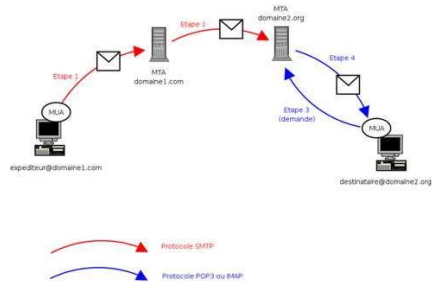
	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires														
	2_4_5_4_001	Les nouvelles applications interfacées avec les serveur de relais de messagerie doivent utiliser le protocole SMTP.	Validé	03/12/2019															
	2_4_5_4_002	Les nouvelles applications envoyant des courriers électroniques (https://fr.wikipedia.org/wiki/Courrier_%C3%A9lectronique) doivent s'interfacer avec les serveurs de relais de messagerie du SNUM	Validé	10/09/2020															
	2_4_5_4_003	<div>Les nouvelles applications envoyant des courriers électroniques doivent respecter la règle de nommage suivante :</div> <table><tr><th>Environnement</th><th>Nom de l'émetteur</th></tr><tr><td colspan="2">Relais externes</td></tr><tr><td>Recette et Développement</td><td>[fonction.direction]@recette.finances.gouv.fr</td></tr><tr><td>Production</td><td>[fonction.direction]@applications.finances.gouv.fr</td></tr><tr><td colspan="2">Relais internes</td></tr><tr><td>Recette et Développement</td><td>[fonction.direction]@interne-rec.finances.gouv.fr</td></tr><tr><td>Production</td><td>[fonction.direction]@interne.finances.gouv.fr</td></tr></table> <div>où [fonction] est le nom de l'application et [direction] le nom de l'entité.</div> <div>Le nom de domaine (par défaut en finances.gouv.fr) peut varier si ce domaine existe et est autorisé pour cette structure.</div>	Environnement	Nom de l'émetteur	Relais externes		Recette et Développement	[fonction.direction]@recette.finances.gouv.fr	Production	[fonction.direction]@applications.finances.gouv.fr	Relais internes		Recette et Développement	[fonction.direction]@interne-rec.finances.gouv.fr	Production	[fonction.direction]@interne.finances.gouv.fr	Validé	21/06/2021	Distinction entre les serveurs de relais internes et externes
Environnement	Nom de l'émetteur																		
Relais externes																			
Recette et Développement	[fonction.direction]@recette.finances.gouv.fr																		
Production	[fonction.direction]@applications.finances.gouv.fr																		
Relais internes																			
Recette et Développement	[fonction.direction]@interne-rec.finances.gouv.fr																		
Production	[fonction.direction]@interne.finances.gouv.fr																		
	2_4_5_4_004	Les serveurs de relais de messagerie "privés" utilisés pour les applications exposées sur le réseau internet et s'interfaçant avec nos serveurs de relais de messagerie externes du domaine applications.finances.gouv.fr doivent se conformer aux standards SPF, DKIM et DMARC.	Validé	28/09/2021															
	2_4_5_4_005	Les nouvelles applications hébergées sur le réseau général (RG) envoyant des courriers électroniques en masse (mass-mailing) doivent s'interfacer avec les serveurs de relais de messagerie du SNUM.	Validé	08/03/2023															

▪ La dernière modification de cette page a été faite le 13 décembre 2023 à 11:18.

Serveur de messagerie version diffusable

Un **serveur de messagerie** électronique est un logiciel serveur de courrier électronique. Il a pour vocation de transférer les messages électroniques d'un serveur à un autre. Un utilisateur n'est jamais en contact direct avec ce serveur mais utilise soit un client de messagerie installé sur son terminal (ordinateur ou smartphone), soit une messagerie web, qui se charge de contacter le serveur pour envoyer ou recevoir les messages.

L'envoi d'un courrier électronique de l'utilisateur au premier serveur de messagerie s'effectue généralement via le protocole SMTP. Ensuite ce serveur envoie le message au serveur du destinataire (serveur MX), cette fonction est appelée Mail Transfer Agent (MTA).



(source : wikipedia,2023 (https://fr.wikipedia.org/wiki/Serveur_de_messagerie_électronique))

✓ Termes privilégiés : **serveur de messagerie, serveur de courrier électronique, serveur de courrier, serveur de courriel**

✓ Equivalents étranger: **e-mail server (en), electronic mail server (en), mail server (en), messaging server (en), post office server (en)**

Sommaire

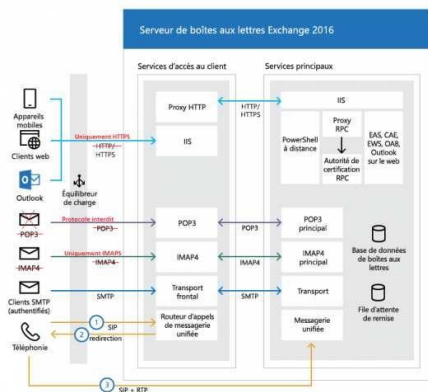
- 1 Contexte
- 2 Règles de base
- 3 Solutions de référence
- 4 Contraintes juridiques et réglementaires
- 5 Contraintes techniques

Contexte

Les **offres de serveurs de messagerie** proposées par le service du numérique (SNUM) s'appuient sur le logiciel propriétaire **Microsoft Exchange 2016**.

L'installation de Microsoft Exchange est basée sur le modèle d'autorisation «Shared permissions» et non «AD split permissions».

L'architecture technique de la solution Microsoft Exchange 2016 se décline de la manière suivante :



Règles de base

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
2_4_6_1_001	Les serveurs de messagerie de référence doivent respecter le standard ministériel (170112_guide-homologation-email_v1.0.0.pdf) Homologation de services Email.	Validé	01/07/2019	
2_4_6_1_002	Les serveurs de messagerie de référence doivent respecter le standard ministériel (170112_standard-SPF_v4.pdf) Standard SPF et lutte contre l'usurpation d'email.	Validé	01/07/2019	
2_4_6_1_003	Les serveurs de messagerie de référence doivent respecter le standard ministériel (180213_standard-relais-SMTP_v2.pdf) Relais SMTP, authenticité et confidentialité des courriels.	Validé	01/07/2019	
2_4_6_1_004	Les serveurs de messagerie de référence doivent respecter le standard ministériel (170307_guide-technique-DKIM-DMARC-STARTTLS-MIME_v1.pdf) Guide technique DKIM, DMARC, STARTTLS, MIME.	Validé	01/07/2019	
2_4_6_1_005	Les serveurs de messagerie de référence doivent respecter le standard ministériel (180122_TLS_v10.1.pdf) Déploiement du protocole TLS .	Validé	01/07//2019	
2_4_6_1_006	Les serveurs de messagerie de référence doivent être installés dans des versions à jour des correctifs de sécurité.	Validé	03/09/2019	

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_4_6_2_001	Les serveurs de messagerie doivent s'appuyer sur les logiciels suivants : <ul style="list-style-type: none">le logiciel propriétaire Microsoft Exchange Server 2016,le logiciel propriétaire Scanmail pour Microsoft Exchange v14.	Validé	10/09/2020	

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_4_6_3_001	Toute demande de support sur le logiciel propriétaire Microsoft Exchange doit se faire au travers du portail support Microsoft.	Validé	30/11/2021	

Contraintes techniques

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_4_6_4_001	Les nouvelles applications interfacées avec les serveurs de messagerie doivent utiliser l'un des protocoles suivants : <ul style="list-style-type: none">Service web REST (API),EWS (Exchange web services),Protocole IMAPS (https://fr.wikipedia.org/wiki/Internet_Message_Access_Protocol).	Validé	01/07/2019	
	2_4_6_4_002	Les nouvelles applications interfacées avec les serveurs de messagerie ne doivent pas utiliser les protocoles suivants : <ul style="list-style-type: none">Protocole POP (https://fr.wikipedia.org/wiki/Post_Office_Protocol) ,Protocole IMAP (https://fr.wikipedia.org/wiki/Internet_Message_Access_Protocol) .	Validé	01/07/2019	
	2_4_6_4_003	Les nouvelles applications devant accéder aux données d'une boîte aux lettres électroniques (BAL) doivent s'interfacer avec les serveurs de messagerie du SNUM.	Validé	18/05/2020	

▪ La dernière modification de cette page a été faite le 13 décembre 2023 à 13:37.

Intégration de données (ETL) version diffusable

Extract-transform-load connu sous le sigle ETL, ou extracto-chargeur, est une technologie informatique intergicielle (comprendre middleware) permettant d'effectuer des synchronisations massives d'information d'une source de données (le plus souvent une base de données) vers une autre. Selon le contexte, on est amené à exploiter différentes fonctions, souvent combinées entre elles : « extraction », « transformation », « constitution » ou « conversion », « alimentation ».

(source : wikipedia,2020 (<https://fr.wikipedia.org/wiki/Extract-transform-load>))

L'**ETL** est un processus de stockage de données pour lequel la transformation ou le traitement des données sont réalisés lors de leur déplacement vers une base de données de destination.

(source : Office québécois de la langue française, 2020 (http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26552195))

- ✓ Termes privilégiés : **processus ETC, ETC, processus d'extraction, de traitement et de chargement de données**
- ✓ Equivalent étranger: **ETL process** (en), **ETL** (en), **extraction, transformation, loading process** (en), **extract, transform, load process** (en)

Sommaire

- 1 Contexte
- 2 Règles de base
- 3 Solutions de référence
- 4 Contraintes juridiques et réglementaires
- 5 Contraintes techniques

Contexte

Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_5_1_1_001				

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_5_1_2_001	Tout nouveau traitement de type ETL doit être fait avec le logiciel libre Talend Open Studio 7.2.	Validé	03/12/2019	

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_5_1_3_001				

Contraintes techniques

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_5_1_4_001				

-
- La dernière modification de cette page a été faite le 6 décembre 2023 à 10:33.

Protection des données (RGPD)

Le **règlement général sur la protection des données (RGPD)** est un règlement de l'Union européenne qui constitue le texte de référence en matière de protection des données à caractère personnel. Il renforce et unifie la protection des données pour les individus au sein de l'Union européenne.

(Source : Wikipedia,2020 (https://fr.wikipedia.org/wiki/R%C3%A8glement_g%C3%A9n%C3%A9ral_sur_la_protection_des_donn%C3%A9es))

✓ Termes privilégiés : **Règlement général sur la protection des données, RGPD**

✓ Equivalent étranger: **General Data Protection Regulation (en), GDPR (en)**

Sommaire

- 1 Contexte
- 2 Règles de base
- 3 Solutions de référence
- 4 Contraintes juridiques et réglementaires
- 5 Contraintes techniques

Contexte

Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_6_1_1_001	Les nouvelles applications qui traitent des données personnelles doivent appliquer le règlement général sur la protection des données personnelles (RGPD (https://www.cnil.fr/fr/reglement-europeen-protection-donnees)).	Validé	01/07/2019	

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_6_1_2_001				

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_6_1_3_001				

Contraintes techniques

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_6_1_4_001				

Récupérée de « [https://wiki.monportail.alize/cct/w/index.php?title=Protection_des_données_\(RGPD\)&oldid=12609](https://wiki.monportail.alize/cct/w/index.php?title=Protection_des_données_(RGPD)&oldid=12609) »

- La dernière modification de cette page a été faite le 1 mars 2022 à 10:57.

Système de gestion de base de données, SGBD (Database management system) version diffusable

Un **système de gestion de base de données** est un logiciel système servant à stocker, à manipuler ou gérer, et à partager des informations dans une base de données, en garantissant la qualité, la pérennité et la confidentialité des informations, tout en cachant la complexité des opérations.

(source : wikipedia,2023 (https://fr.wikipedia.org/wiki/Syst%C3%A8me_de_gestion_de_base_de_donn%C3%A9es))

- ✓ Termes privilégiés : **système de gestion de base de données, SGBD, moteur SGBD**
- ✓ Equivalent étranger: **database management system (en), DBMS (en), database manager (en), DBMS engine (en)**

Sommaire

1

Contexte

2

Règles de base

3

Solutions de référence

4

Contraintes juridiques et réglementaires

5

Contraintes techniques

Contexte

Les offres de système de gestion de base de données (SGBD) relationnelles proposées par le service du numérique (SNUM) s'appuient par défaut sur :

- le logiciel libre **PostgreSQL version 15** pour les serveurs Linux à vocation applicative, le logiciel
- propriétaire **Microsoft SQL Server version 2017** pour les serveurs Windows à vocation applicative.

Il est néanmoins possible moyennant justification technique pour certaines applications de s'appuyer sur d'autres systèmes de gestion de base de données (SGBD) relationnelles telles que :

- le logiciel propriétaire **Oracle.Server 19C** et les logiciels libres **MariaDB version 10** et **MySQL version 8** pour les serveurs Linux à vocation applicative.

Règles de base

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
2_6_2_1_001	Les systèmes de gestion de base de données (SGBD) doivent être installés dans des versions à jour des correctifs de sécurité.	Validé	03/09/2019	

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_6_2_2_001	Les systèmes de gestion de base de données (SGBD) installés sur des serveurs Linux à vocation applicative doivent s'appuyer sur le logiciel libre PostgreSQL version 15 .	Validé	08/03/2023	
	2_6_2_2_002	Les systèmes de gestion de base de données (SGBD) installés sur des serveurs Windows à vocation applicative doivent s'appuyer sur le logiciel propriétaire Microsoft SQL Server 2017 .	Validé	10/09/2020	
	2_6_2_2_003	Les nouvelles applications nécessitant l'usage d'un système de gestion de base de données (SGBD) ne s'appuyant pas sur le logiciel libre PostgreSQL doivent faire l'objet d'une justification technique.	Validé	01/07/2019	

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_6_2_3_001	Toute demande de support sur le logiciel libre PostgreSQL doit se faire au travers du marché "Support à l'usage des logiciels libres (SLL)".	Validé	01/07/2019	
	2_6_2_3_002	Toute demande de support sur le logiciel propriétaire ORACLE Database Server doit se faire au travers du marché " Acquisition de licences, support et de support personnalisé".	Validé	01/07/2019	

Contraintes techniques

Installation des SGBD

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_6_2_4_001	L'installation du logiciel libre PostgreSQL doit se faire à partir d'un script interne au SNUM.	Validé	30/11/2021	
	2_6_2_4_002	L'installation du logiciel propriétaire Oracle Database Server se faire à partir des fichiers disponibles depuis le site officiel de l'éditeur.	Validé	01/07/2019	
	2_6_2_4_003	L'installation du logiciel propriétaire Microsoft SQL Server doit se faire à partir des fichiers disponibles depuis le site officiel de l'éditeur.	Validé	01/07/2019	

Montée de version des SGBD

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_6_2_5_001				

Administration et exploitation des SGBD

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_6_2_6_001				

Encodage

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_6_2_7_001	Le codage des caractères informatiques dans les systèmes de gestion de bases de données (SGBD) doit être basé sur UTF-8.	Validé	18/05/2020	
	2_6_2_7_002	Le codage des caractères informatiques dans les systèmes de gestion de bases de données (SGBD) ORACLE avec des clients Windows doit être basé sur Windows-1252.	Validé	18/05/2020	

▪ La dernière modification de cette page a été faite le 13 décembre 2023 à 14:35.

Active directory (AD) version diffusable

Active Directory (AD) est la mise en œuvre par Microsoft des services d'annuaire LDAP pour les systèmes d'exploitation Windows. L'objectif principal d'Active Directory est de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows, MacOS et encore Linux. Il permet également l'attribution et l'application de stratégies ainsi que l'installation de mises à jour critiques par les administrateurs. Active Directory répertorie les éléments d'un réseau administré tels que les comptes des utilisateurs, les serveurs, les postes de travail, les dossiers partagés (en), les imprimantes, etc. Un utilisateur peut ainsi facilement trouver des ressources partagées, et les administrateurs peuvent contrôler leur utilisation grâce à des fonctionnalités de distribution, de duplication, de partitionnement et de sécurisation de l'accès aux ressources répertoriées.

(Source : Wikipedia,2024 (https://fr.wikipedia.org/wiki/Active_Directory))

- ✓ Termes privilégiés : **Active Directory, AD**
- ✓ Equivalent étranger: **Active Directory** (en), **AD** (en)

La version de base de cette rubrique est accessible [ici](#)

Sommaire

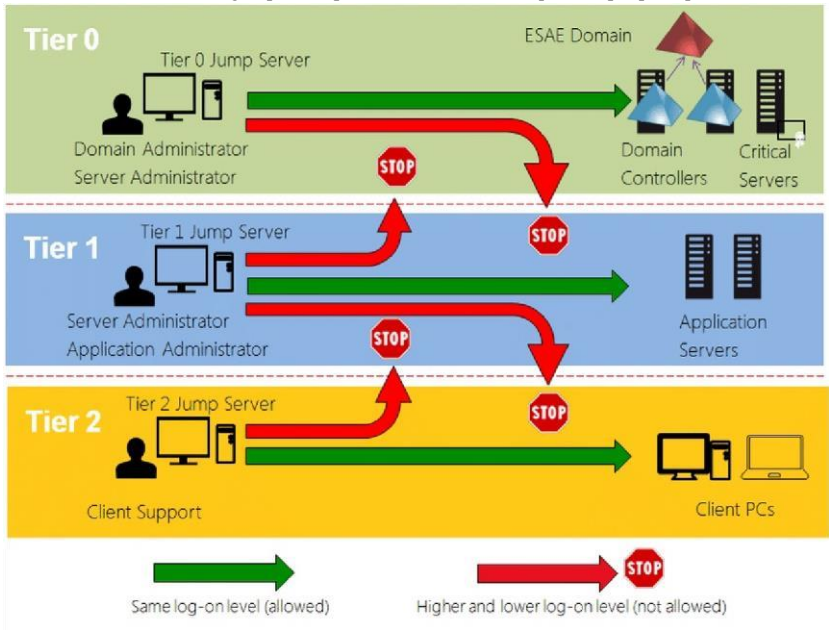
- 1 Contexte
- 2 Règles de base
- 3 Solutions de référence
- 4 Contraintes juridiques et réglementaires
- 5 Contraintes techniques
- 6 Gestion des comptes
- 7 Gestion des annuaires

Contexte

L'**architecture Microsoft Active Directory (AD)** mise en oeuvre au sein du service du numérique (SNUM) s'appuie actuellement sur : ▪ **1 forêt** partageant un schéma d'annuaire commun, ▪ **des contrôleurs de domaine.**

Afin d'être en conformité avec le standard ministériel, le **modèle en couches (Tiering model)** est en cours de mise en oeuvre.afin de séparer les composants de l'infrastructure selon le niveau d'importance et de rendre ces couches étanches les unes des autres. Ce modèle propose trois couches organisées de la manière suivante :

- **Couche de niveau 0** regroupant les composants de l'infrastructure de l'AD les plus importants : les contrôleurs de domaine, les serveurs d'infrastructure, les administrateurs AD ...
- **Couche de niveau 1** regroupant les serveurs applicatifs, les administrateurs des serveurs applicatifs, ...
- **Couche de niveau 2** regroupant les postes de travail bureautiques, les périphériques, les utilisateurs, ...



	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_6_3_1_001	L'annuaire Active Directory (AD) du service du numérique (SNUM) doit respecter le standard ministériel Active Directory en termes de sécurisation des accès d'administration et de gestion de comptes et de sécurisation des environnements AD .	Validé	10/09/2020	

Règles de base

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_6_3_2_001				

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_6_3_3_001				

Contraintes techniques Gestion des comptes

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_6_3_4_001	Toute création de compte sur l'annuaire Active Directory (AD) doit respecter les règles de nommage du SNUM.	Validé	11/09/2023	
	2_6_3_4_002	Les comptes de service gMSA (https://docs.microsoft.com/fr-fr/windows-server/security/group-managed-service-accounts/group-managed-service-accounts-overview) doivent être privilégiés aux comptes de service classiques.	Validé	03/12/2020	
	2_6_3_4_003	Les comptes de service hors gMSA (https://docs.microsoft.com/fr-fr/windows-server/security/group-managed-service-accounts/group-managed-service-accounts-overview) doivent être restreints à leur fonction (utilisable uniquement sur le(s) machine(s) pour qui ils ont été créés).	Validé	03/12/2020	
	2_6_3_4_004	Les comptes à privilèges de type [préfixe]-[pnom] (où préfixe = ADMIN,88000,GRID,PDT) doivent être destinés à l'administration des postes de travail	Validé	03/12/2020	
	2_6_3_4_005	Les comptes à privilèges de type [pnom]-ADMIN doivent être destinés uniquement à l'administration des serveurs.	Validé	03/12/2020	
	2_6_3_4_006	Les comptes à privilèges élevés doivent être de type [pnom]-[suffixe] où suffixe est différent de "ADMIN"	Validé	03/12/2020	
	2_6_3_4_007	Les comptes de service gMSA utilisés pour une application donnée doivent être différents selon l'environnement utilisé(développement, recette et production)	Validé	10/02/2021	
	2_6_3_4_008	Les objets de l'Active Directory de type «ordinateur» (serveurs) n'ayant pas fait l'objet d'une authentification depuis plus de 90 jours ou n'ayant pas fait l'objet d'un changement de passe depuis plus de 45 jours doivent être sanctuarisés dans une unité organisationnelle (OU) dédiée.	Validé	06/07/2022	
	2_6_3_4_009	Tout objet de l'Active Directory sanctuarisé dans une unité organisationnelle dédiée depuis plus de 6 mois doit être supprimé par l'intermédiaire de la corbeille Active Directory.	Validé	06/07/2022	

Gestion des annuaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_6_3_5_001	Toute application utilisant le protocole d'authentification Kerberos (https://fr.wikipedia.org/wiki/Kerberos_(protocole)) doivent s'interfacer avec les annuaires du SNUM.	Validé	10/09/2020	

Annuaire LDAP version diffusable

Un **annuaire** est un système de stockage de données, dérivé des bases de données hiérarchisées, permettant en particulier de conserver les données pérennes, c'est-à-dire les données n'étant que peu mises à jour (historiquement, sur une base annuelle, d'où le nom), comme les coordonnées des personnes, des partenaires, des clients et des fournisseurs d'une entreprise, les adresses électroniques. La recherche peut se faire selon de multiples critères et les données peuvent être utilisées par des logiciels clients comme des applications serveurs (serveur de messagerie : Postfix, Sendmail, etc.). En outre, certaines versions de service d'annuaires savent gérer les droits sur les données mais aussi les services proposés sur les machines clientes par une identification grâce à un couple login / mot de passe. Aujourd'hui, ces données sont centralisées sur une ou plusieurs machines et les données sont transférées entre les machines via des protocoles réseaux.

(Source : Wikipedia,2022 (<https://fr.wikipedia.org/wiki/Annuaire>))

Lightweight Directory Access Protocol (LDAP) est à l'origine un protocole permettant l'interrogation et la modification des services d'annuaire (il est une évolution du protocole DAP). Ce protocole repose sur TCP/IP. Il a cependant évolué pour représenter une norme pour les systèmes d'annuaires, incluant un modèle de données, un modèle de nommage, un modèle fonctionnel basé sur le protocole LDAP, un modèle de sécurité et un modèle de réplication. C'est une structure arborescente dont chacun des nœuds est constitué d'attributs associés à leurs valeurs. LDAP est moins complexe que le modèle X.500 édicté par l'UIT-T.

(Source : Wikipedia,2022 (https://fr.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol#Serveurs_LDAP))

✓ Termes privilégiés : **Annuaire, Répertoire**

✓ Equivalent étranger: **Directory** (en),

La version de base de cette rubrique est accessible ici

Sommaire

- 1 Contexte
- 2 Règles de base
- 3 Solutions de référence
- 4 Contraintes juridiques et réglementaires
- 5 Contraintes techniques
- 6 Gestion des comptes
- 7 Gestion des annuaires

Contexte

L'offre de service d'annuaires LDAP proposée par le service de numérique (SNUM) s'appuie sur :

- le logiciel propriétaire **Microsoft Active Directory**
- Les logiciels libres **OpenLDAP** et **389 Directory Server**

Cette offre est constituée de plusieurs annuaires. qui proposent les fonctionnalités suivantes :

Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_6_4_1_001	Les annuaires LDAP doivent être installés dans des versions à jour des correctifs de sécurité.	Validé	06/07/2022	
	2_6_4_1_002	Les annuaires LDAP doivent être inscrits dans le plan de continuité informatique REMPART.	Validé	06/07/2022	

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_6_4_2_001	Les annuaires LDAP de référence doivent s'appuyer sur : <ul style="list-style-type: none">▪ le logiciel libre OpenLDAP version 2.5.x▪ le logiciel libre 389 Directory Server version 2.0.x	Validé	06/07/2022	

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_6_4_3_001	La tierce maintenance applicative des annuaires LDAP doit se faire au travers du marché Tierce maintenance applicative (TMA) et maintien en conditions opérationnelles (MCO) de la plateforme Annuaires sauf pour l'annuaire Active Directory.	Validé	10/09/2020	

Contraintes techniques Gestion des comptes

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_6_4_4_001	Les nouvelles applications interfacées avec les serveurs d'annuaire doivent privilégier le protocole LDAPS sauf contrainte technique à justifier.	Validé	10/09/2020	
	2_6_4_4_002	Les mots de passe stockés dans les annuaires doivent contenir 14 caractères minimum.	Validé	10/09/2020	
	2_6_4_4_003	Les mots de passe stockés dans les annuaires doivent être composés de caractères alphanumériques non-accentués et de caractères spéciaux.	Validé	10/09/2020	
	2_6_4_4_004	Les mots de passe stockés dans les annuaires doivent impérativement respecter 3 des 4 critères suivants : <ul style="list-style-type: none">contenir une lettre minuscule,contenir une lettre majuscule,contenir un caractère numérique,contenir un des caractères suivants : + - * /,; : . ! ? = % \$ & " ' (_) @ # { } \ []	Validé	10/09/2020	
	2_6_4_4_005	Les mots de passe stockés dans les annuaires ne doivent pas comporter ni le prénom ni le nom de l'utilisateur.	Validé	10/09/2020	
	2_6_4_4_006	Les mots de passe stockés dans l'annuaire doivent être différents.	Validé	10/09/2020	
	2_6_4_4_007	Le mot de passe d'un compte de service applicatif de recette doit être différent d'un compte de service de production.	Validé	10/02/2021	
	2_6_4_4_008	Les applications interfacées à l'annuaire doivent utiliser un compte dédié : <ul style="list-style-type: none">qui respecte la règle de nommage [nom_de_l'application]-adcqui est positionné dans l'unité organisationnellequi respecte le standard ministériel authentification par mot de passe.	Validé	28/09/2021	
	2_6_4_4_009	Les applications interfacées à l'annuaire doivent utiliser un compte dédié : <ul style="list-style-type: none">qui respecte la règle de nommage [nom_de_l'application]-adcqui est positionné dans l'unité organisationnelle :qui respecte le standard ministériel Authentification par mot de passe]	Validé	28/09/2021	

Gestion des annuaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_6_4_5_001	Les applications exposées sur le réseau général (RG) et sur le réseau interministériel de l'Etat (RIE) doivent s'interfacer avec les annuaires du SNUM.	Validé	16/12/2022	
	2_6_4_5_002	Les applications exposées sur le réseau internet doivent s'interfacer avec les annuaires Internet du SNUM .	Validé	10/09/2020	

Contraintes juridiques et réglementaires
Synchronisation des annuaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_6_4_6_001	L'annuaire Anais centrale de production doit être synchronisé avec : <ul style="list-style-type: none">l'annuaire Active Directory Solao de productionle serveur de messagerie de production.	Validé	03/12/2020	
	2_6_4_6_002	L'annuaire Anais centrale recette doit être synchronisé avec : <ul style="list-style-type: none">l'annuaire Active Directory Solao de recette/développementle serveur de messagerie de recette/développement.	Validé	03/12/2020	

Gestion du code source version diffusable

Le **code source** est un texte qui représente les instructions d'un programme telles qu'elles ont été écrites dans un langage de programmation sous une forme humainement lisible par un programmeur. Le code source se matérialise souvent sous la forme d'un ensemble de fichiers textes. Il est souvent traduit par un assembleur ou un compilateur en code binaire — composé d'instructions machine exécutables par un processeur. Il peut aussi être interprété pour être exécuté immédiatement. Une autre possibilité est qu'il soit traduit en code intermédiaire qui sera ensuite interprété.

(source : wikipedia,2020 (https://fr.wikipedia.org/wiki/Code_source))

✓ Termes privilégiés : **code source**, **code d'origine**

✓ Equivalent étranger: **source code** (en)

Sommaire

- 1 Contexte
- 2 Règles de base
- 3 Solutions de référence
- 4 Contraintes juridiques et réglementaires
- 5 Contraintes techniques

Contexte

Les codes sources peuvent être déposés sur le Gitlab interministériel de la DGFIP (<https://forge.dgfip.finances.rie.gouv.fr>).

Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_7_2_1_001	Les codes sources doivent être fournis à chaque livraison de prestataires.	Validé	03/09/2019	
	2_7_2_1_002	La génération du code doit pouvoir être obtenue à partir des codes sources livrés.	Validé	03/09/2019	

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
<div>Nouveauté</div>	2_7_2_2_001	Les codes sources doivent être enregistrés au sein du gestionnaire de codes sources GIT de la DGFIP.	Validé	18/05/2020	

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_7_2_3_001				

Contraintes techniques

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_7_2_4_001				

▪ La dernière modification de cette page a été faite le 6 décembre 2023 à 10:49.

Gestion des anomalies version diffusable

Un **système de suivi des bugs** est un logiciel qui permet d'effectuer un suivi des bugs signalés dans le cadre d'un projet de développement de logiciel.

(source : wikipedia,2020 (https://fr.wikipedia.org/wiki/Syst%C3%A8me_de_suivi_des_bugs))

- ✓ Termes privilégiés : **système de suivi des bugs**
- ✓ Equivalent étranger: **tracking system** (en)

Sommaire

1

Contexte

2

Règles de base

3

Solutions de référence

4

Contraintes juridiques et réglementaires

5

Contraintes techniques

Contexte

Les offres de solution de gestion des anomalies proposées par SEP1 s'appuient sur le logiciel libre **Mantis**.

Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_7_3_1_001				

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_7_3_2_001	Le logiciel libre Mantis 2.12 (également appelé "SAMA") doit être utilisé pour l'enregistrement et le suivi des anomalies liées aux applications ou à leurs infrastructures.	Validé	03/09/2019	

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_7_3_3_001	Toute demande de support sur le logiciel libre Mantis doit se faire au travers du marché "Support à l'usage des logiciels libres (SLL)".	Validé	03/09/2019	

Contraintes techniques

Marché de TMMA

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_7_3_4_001	Toute demande d'intervention du prestataire chargé de la TMMA doit faire l'objet d'une saisie d'un ticket Mantis dans l'application SAMA.	Validé	03/09/2019	
	2_7_3_4_002	Les tickets Mantis doivent a minima respecter les règles de saisie suivantes : <ul style="list-style-type: none">▪ Catégorie : nom du projet▪ Impact : Bloquant, Majeur ou Mineur▪ Type :<ul style="list-style-type: none">▪ INI pour les demandes d'initialisation des nouvelles applications,▪ EVO pour les demandes d'évolution,▪ SEC pour les demandes d'évolution du socle technique des applications intranet,▪ Résumé : description succincte de la demande, préfixée du nom du projet, date de la demande▪ Environnement : Développement, Recette ou Production	Validé	03/09/2019	

- La dernière modification de cette page a été faite le 11 décembre 2023 à 17:10.

Environnement de développement intégré (IDE) version diffusable

Un environnement de développement est un ensemble d'outils qui permet d'augmenter la productivité des programmeurs qui développent des logiciels.

(source : wikipedia,2024 (https://fr.wikipedia.org/wiki/Environnement_de_d%C3%A9veloppement))

- ✓ Termes privilégiés : **environnement de développement intégré, EDI**
- ✓ Equivalent étranger: **integrated development environment** (en), **IDE** (en) La version de base de cette rubrique est accessible ici

Sommaire

- 1 Contexte
- 2 Règles de base
- 3 Solutions de référence
- 4 Contraintes juridiques et réglementaires
- 5 Contraintes techniques

Contexte

L'offre d'environnement de développement informatique du service du numérique (SNUM) s'appuie sur:

- le logiciel libre **Eclipse** pour les développements basés sur le langage JAVA.
- le logiciel libre **VSCode** pour les développements basés sur le langage Javascript,

Règles de base

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
2_7_4_1_001	Les environnements de développement intégré (IDE) doivent être installés dans des versions à jour des correctifs de sécurité.	Validé	16/12/022	

Solutions de référence

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
2_7_4_2_001	L'environnement de développement intégré pour le développement des applications Java doit d'appuyer sur le logiciel libre Eclipse .	Validé	04/12/2023	jee-oxygen-3a-win32-x86_64-1

Contraintes juridiques et réglementaires

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
2_7_4_3_001				

Contraintes techniques

Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
2_7_4_4_001				

• La dernière modification de cette page a été faite le 25 février 2024 à 07:27.

Qualité et sécurité du code source version diffusable

Le **code source** est un texte qui représente les instructions d'un programme telles qu'elles ont été écrites dans un langage de programmation sous une forme humainement lisible par un programmeur. Le code source se matérialise souvent sous la forme d'un ensemble de fichiers textes. Il est souvent traduit par un assembleur ou un compilateur en code binaire — composé d'instructions machine exécutables par un processeur. Il peut aussi être interprété pour être exécuté immédiatement. Une autre possibilité est qu'il soit traduit en code intermédiaire qui sera ensuite interprété.

(source : wikipedia,2020 (https://fr.wikipedia.org/wiki/Code_source))

Instructions originales d'un programme écrites dans un langage lisible par l'humain et qui doivent être compilées pour être lues par un ordinateur.

(source : Office québécois de la langue française, 2000 (http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8391804))

✓ Termes privilégiés : **code source**, **code d'origine**

✓ Equivalent étranger: **source code** (en)

La version de base de cette rubrique est accessible [ici](#)

Sommaire

1

Contexte

2

Règles de base

3

Solutions de référence

4

Contraintes juridiques et réglementaires

5

Contraintes techniques

Contexte Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_7_5_1_001				

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_7_5_2_001				

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_7_5_3_001				

Contraintes techniques

Interface Homme-Machine (IHM)

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_7_5_4_001	Les applications web doivent signaler en cas de besoin à l'utilisateur la nécessité d'activer Javascript et les cookies dans la mesure où ceux-ci ne seraient pas interdits	Validé	03/09/2019	
	2_7_5_4_002	Les fonctions Javascript doivent être listées et documentées.	Validé	03/09/2019	
	2_7_5_4_003	Tout plug-in doit pouvoir être installé en mode utilisateur (sans nécessiter les droits "administrateur" du poste de travail).	Validé	03/09/2019	
	2_7_5_4_004	Tout plug-in doit être compatible avec les navigateurs web en vigueur au sein du SNUM.	Validé	03/09/2019	

Gestion des sessions

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_7_5_4_101	Toute application web doit disposer d'une fonction de déconnexion automatique au delà d'un délai d'inactivité (timeout de session).	Validé	03/09/2019	
	2_7_5_4_102	L'utilisateur doit pouvoir se déconnecter manuellement.	Validé	03/09/2019	


Saisie des données

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_7_5_4_201	Tout contrôle effectué sur le client doit être également reporté sur le serveur.	Validé	03/09/2019	

Adresse URL relative

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_7_5_4_301	Toute application web doit pouvoir fonctionner avec des adresses URL relatives et supporter les redirections d'URL.	Validé	03/12/2019	

Encodage

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_7_5_4_401	L'encodage des contenus et du code sources doivent être de typeUTF-8 (https://fr.wikipedia.org/wiki/UTF-8).	Validé	18/05/2020	

• La dernière modification de cette page a été faite le 25 février 2024 à 07:49.

Tests et intégration version diffusable

Un **test** désigne une procédure de vérification partielle d'un système. Son objectif principal est d'identifier un nombre maximum de comportements problématiques du logiciel. Il permet ainsi, dès lors que les problèmes identifiés seront corrigés, d'en augmenter la qualité. D'une manière plus générale, le test désigne toutes les activités qui consistent à rechercher des informations quant à la qualité du système afin de permettre la prise de décisions.

(source : wikipedia,2020 ([https://fr.wikipedia.org/wiki/Test_\(informatique\)\)](https://fr.wikipedia.org/wiki/Test_(informatique))))

Un **test d'intégration** est une phase dans les tests, qui est précédée des tests unitaires et est généralement suivie par les tests de validation. Dans le test unitaire, on vérifie le bon fonctionnement d'une partie précise d'un logiciel ou d'une portion d'un programme (appelée « unité » ou « module ») ; dans le test d'intégration, chacun des modules indépendants du logiciel est assemblé et testé dans l'ensemble.

(source : wikipedia,2020 (https://fr.wikipedia.org/wiki/Test_d%27int%C3%A9gration)))) La version de base de cette rubrique est accessible ici

Sommaire

- 1 Contexte
- 2 Règles de base
- 3 Solutions de référence
- 4 Contraintes juridiques et réglementaires
- 5 Contraintes techniques

Contexte Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_7_6_1_001				

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_7_6_2_001	Le logiciel propriétaire Squash TM doit être utilisé : <ul style="list-style-type: none">▪ lorsqu'une application fait l'objet d'une industrialisation de ses campagnes de tests;▪ lorsqu'une application nécessite la gestion d'un patrimoine de test à partir de la définition des exigences.	Validé	03/09/2019	

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_7_6_3_001				

Contraintes techniques

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_7_6_4_001				

• La dernière modification de cette page a été faite le 2 mai 2024 à 13:42.

Sauvegarde informatique

La **sauvegarde informatique** est l'opération qui consiste à dupliquer et conserver de manière sécurisée des données contenues dans un système informatique et/ou des logiciels présents sur ce système afin d'assurer leur disponibilité sur une forme non altérée (intégrité) et ainsi la possibilité de les réinstaller sur un système informatique après un incident, une erreur de manipulation ou un acte de malveillance portant atteinte à leur disponibilité ou à leur intégrité. (source : ANS,2022 (https://esante.gouv.fr/sites/default/files/media_entity/documents/PGSSI-S_Guide_Pratique-Sauvegarde-V1.1.pdf))

✓ Termes privilégiés : **sauvegarde de données**, **sauvegarde informatique**, **sauvegarde**

✓ Equivalent étranger: **backup** (en), **data backup** (en)

Info : La démarche de définition et de mise en oeuvre de la sauvegarde passe par :

• **l'identification du besoin de sauvegarde et de restauration** à savoir la définition du périmètre métier concerné et le niveau de service attendu pour la sauvegarde et la restauration (perte admissible de données non sauvegardées entre deux sauvegardes (PDMA), délai maximum de restauration des données, durée de conservation des sauvegardes, besoin d'intégrité et de confidentialité des sauvegardes)

- **la formalisation des procédures** en définissant une méthode permettant d'élaborer et faire vivre le plan de sauvegarde. Il faut notamment identifier de manière exhaustive les composants logiciels, systèmes et applicatifs, et les données à sauvegarder, formaliser les procédures de sauvegarde et de restauration.
- **l'adoption de recommandations à l'état de l'art** tout en maintenant une veille continue sur les bonnes pratiques en matière de sauvegarde et sur les solutions utilisées.
- **la restauration et le contrôle** en s'assurant que le dispositif de sauvegarde et de restauration permette de revenir à un état stable antérieur.

Attention ! Il convient de ne pas confondre les concepts de sauvegarde et de snapshot.

⚠ **Une sauvegarde** est une copie complète des données réalisée à des intervalles réguliers dans le but de protéger contre la perte de données, tandis qu'**un snapshot** est une capture instantanée de l'état actuel des données qui peut être utilisée pour restaurer un système ou un volume de stockage à un état précédent sans avoir besoin d'une copie complète des données.

Attention ! Certains cas d'usage ne sont pas couverts par la sauvegarde :

- **lorsque la PDMA est de moins de 24 heures**, il faut alors privilégier des solutions de réplication de données, qui traitent en priorité la problématique de l'indisponibilité de la plateforme nominale sauf pour les SBGD Oracle Server et Microsoft SQL Server où les sauvegardes sont exécutées quotidiennement entre 12h00 et 14h00 pour revenir aux données de la demi-journée précédente en cas de sinistre;
- **lorsqu'il y a un besoin d'archivage au sens légal**, il faut alors privilégier des solutions d'archivage, qui traitent de la conservation à moyen et long terme des informations numériques afin de les accessibles et exploitables.

Contexte

Le service du numérique (SNUM) a mis en place une offre de services dénommée **OASIS** dédiée à la **sauvegarde des données hébergées sur des serveurs**.

Cette infrastructure de sauvegarde repose sur :


- des appliances **Veritas 5250** (https://www.veritas.com/support/en_US/doc/140865876-140865884-0/index) pour la prise en charge des sauvegardes ensuite répliquées sur une appliance **Veritas Access 3340** (https://www.veritas.com/support/en_US/doc/125460431-134247411-0/index),
- le logiciel propriétaire **Veritas Netbackup 10.3** (https://www.veritas.com/support/fr_FR/downloads/detail.REL199519),
- le logiciel propriétaire **Veritas InfoScale Availability 8.0** (https://www.veritas.com/support/fr_FR/downloads/detail.REL333811) pour assurer les fonctions de haute disponibilité,

- le logiciel propriétaire **Veritas Netbackup OPS Center 10.0** (https://www.veritas.com/support/fr_FR/article.100052742) pour assurer les fonctions de surveillance, de génération d'alertes et de rapports.

Un **plan de sauvegarde** spécifique est mis en oeuvre afin de tenir compte de la nature de données à sauvegarder (fichiers, SGBD, BMR, ...) et des contraintes de sauvegarde associées (fenêtre de sauvegarde, sauvegarde à chaud, sauvegarde à froid, ...) :

Nature de données	Type de sauvegarde	Périodicité de la sauvegarde	Contraintes de sauvegarde
Fichiers	Sauvegarde totale	Hebdomadaire - le week-end	
	Sauvegarde incrémentale	Quotidienne en semaine, entre 18h00 et 08h30	
SGBD Oracle et Microsoft	Sauvegarde totale	Quotidienne - entre 18h00 et 08h30	Un script de sauvegarde des bases de données Microsoft SQL Server SQL Server
	Sauvegarde incrémentale	Quotidienne en semaine - entre 12h00 et 14h00	doit être fourni par la maîtrise d'oeuvre en charge de l'application.
Autres SGBD	Sauvegarde totale	Hebdomadaire - le week-end	Un script de sauvegarde des bases de données non référencées dans le
	Sauvegarde incrémentale	Quotidienne en semaine - entre 18h00 et 08h30	CCT doit être fourni par la maîtrise d'oeuvre en charge de l'application
Microsoft Exchange Server	Sauvegarde totale	Quotidienne - entre 18h00 et 08h30	
Bare Metal Restore (BMR)	Sauvegarde totale	Hebdomadaire - le week-end	
	Sauvegarde incrémentale	Quotidienne en semaine - entre 18h00 et 08h30	
VMware	Sauvegarde totale	Hebdomadaire - le week-end	
	Sauvegarde incrémentale	Quotidienne en semaine - entre 18h00 et 08h30	

Ce plan de sauvegarde comporte également une politique de conservation des données spécifiant la durée pendant laquelle on conserve les données de sauvegarde avant de les archiver, de les effacer on encore les détruire. **Le délai de conservation des sauvegardes est actuellement de 60 jours.**

- 

Info : Il existe également une autre solution dénommée **LINA** mise en place au sein du SNUM dédiée à la sauvegarde en continu des données des postes de travail bureautiques. Cette solution repose sur le logiciel propriétaire Atempo Lina.

Recommandations relatives à la sécurisation des infrastructures de sauvegarde mises en oeuvre

Info : Les règles listées ci-dessous sont principalement extraites des documents :

- de l'ANSSI : "Sauvegarde des systèmes d'information - Les fondamentaux" (<https://cyber.gouv.fr/publications/fondamentaux-sauvegarde-systemes-dinformation>) et
 - "Sauvegarde des systèmes d'information - Les essentiels" (<https://cyber.gouv.fr/publications/sauvegarde-des-systemes-dinformation>).
 - du SHFDS : "Politiques de sauvegardes" (https://www.economie.gouv.fr/files/170922_politiques-sauvegardes_v1.1.pdf)

Elles sont complétées de règles spécifiques validées lors des précédents comités d'architecture du SNUM.

- La dernière modification de cette page a été faite le 14 mai 2024 à 20:35.

Accès à distance des prestataires (Provider remote access) version diffusable

L'accès à distance, la commande à distance ou encore le contrôle à distance sont des méthodes qui permettent, depuis un ordinateur éloigné et sans limite théorique de distance, de prendre le contrôle d'un autre ordinateur en affichant l'écran de celui-ci et en manipulant les fonctions d'un périphérique d'entrée comme un clavier. Cet accès peut être effectué vers des postes de travail ou des serveurs informatique en fonction des possibilités du logiciel utilisé.

(source : wikipedia,2022 (https://fr.wikipedia.org/wiki/Acc%C3%A8s_%C3%A0_distance))

- ✓ Termes privilégiés :accès à distance, téléaccès, accès distant
- ✓ Equivalent étranger: remote access (en)

La version de base de cette rubrique est accessible ici

Sommaire

- 1 Contexte
- 2 Règles de base
- 3 Solutions de référence
- 4 Contraintes juridiques et réglementaires
- 5 Contraintes techniques

Contexte

L'offre de services d'accès à distance des prestataires proposées par le service du numérique (SNUM) s'appuie actuellement sur la solution ARTEMIS.

Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_8_2_1_001	L'accès à distance des prestataires aux systèmes d'exploitation des serveurs situés sur le site d'hébergement d'Osny ne peut se faire que sur des environnements de développement et au travers des protocoles suivants : <ul style="list-style-type: none">▪ Protocole RDP (Remote Desktop Protocol) pour les systèmes d'exploitation de type Windows Server,▪ Protocole SSH (Secure Shell) pour les systèmes d'exploitation de type Linux.	Validé	03/12/2019	
	2_8_2_1_002	L'accès à distance des prestataires aux applications web (protocole HTTPS) situés sur le site d'hébergement d'Osny doit se faire au travers de poste de rebond virtuel (VPR) sur les environnements de développement, de recette et de production avec des comptes nominatifs communiqués par la maîtrise d'ouvrage de l'application.	Validé	03/12/2019	
	2_8_2_1_003	L'accès à distance des prestataires aux serveurs de base de données situés sur le site d'hébergement d'Osny ne peut se faire qu'avec un compte en lecture seule.	Validé	03/12/2019	
	2_8_2_1_004	La solution d'accès à distance des prestataires doit être installée dans des versions à jour des correctifs de sécurité	Validé	21/06/2021	

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_8_2_2_001	L'accès à distance des prestataires aux serveurs doit se faire au travers de la solution de référence ARTEMIS	Validé	05/12/2019	

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_8_2_3_001				

Contraintes techniques

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_8_2_4_001	L'accès à distances des prestataires via la solution ARTEMIS doit se faire : <ul style="list-style-type: none">▪ depuis un poste de trava il disposant du système d'exploitation Microsoft Windows 10 et d'un logiciel antivirus à jour,▪ via un certificat d'authentification personnel sur clé cryptographique conforme RGS une * (ou plus) acquis auprès de l'une des autorités de confian ce référencées (https://www.lsti-certification.fr/fr/certifications/pse/).	Validé	22/01/2020	

Gestion des environnements

En informatique, un environnement désigne, pour une application, l'ensemble des matériels et des logiciels système, dont le système d'exploitation, sur lesquels sont exécutés les programmes de l'application. (source : wikipedia,2022 ([https://fr.wikipedia.org/wiki/Environnement_\(informatique\)\)](https://fr.wikipedia.org/wiki/Environnement_(informatique)))))

- ✓ Terme privilégié : **environnement**
- ✓ Equivalent étranger: **environment** (en)

La version diffusable de cette rubrique est accessible ici

Sommaire

1 Règles de base

2 Solutions de référence

3 Contraintes juridiques et réglementaires

4 Contraintes techniques

Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_8_3_1_001	Les environnements de recette/intégration et de production doivent utiliser les mêmes versions des éléments d'infrastructures (messagerie, annuaire LDAP, SGBD, serveur Web, serveur applicatif, JVM, PHP, Framework, etc.) et du système d'exploitation cible.	Validé	03/12/2020	
	2_8_3_1_002	Toute application basée sur des logiciels libres (hors progiciels) doit s'appuyer sur trois environnements : <ul style="list-style-type: none">■ Environnement de développement■ Environnement de recette ou d'intégration■ Environnement de production	Validé	03/12/2020	
	2_8_3_1_003	Toute application basée sur des logiciels propriétaires (progiciels) développement basé sur un progiciel doit s'appuyer au moins sur les deux environnements : <ul style="list-style-type: none">■ Environnement de recette ou d'intégration■ Environnement de production	Validé	03/12/2020	

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_8_3_2_001				

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_8_3_3_001				

Contraintes techniques


Accès aux logs

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_8_3_4_001	Les logs de recette et de production doivent pouvoir être mis à disposition de la maîtrise d'oeuvre.	Validé	10/09/2020	

• La dernière modification de cette page a été faite le 8 février 2024 à 14:42.

Plan de continuité d'activité (Business continuity planning)

Un plan de continuité d'activité (informatique) a pour but de garantir la survie de l'entreprise après un sinistre important touchant le système informatique. Il s'agit de redémarrer l'activité le plus rapidement possible avec le minimum de perte de données. Ce plan est un des points essentiels de la politique de sécurité informatique d'une entreprise. (source :Wikipedia, 2023 (Termes privilégiés :**plan de continuité d'activité, PCA**

 Equivalent étranger: **business continuity plan** (en), **BCP** (en)

Sommaire

- 1 Contexte
- 2 Règles de base
- 3 Solutions de référence
- 4 Contraintes juridiques et réglementaires
- 5 Contraintes techniques

Contexte

Un **plan de continuité informatique** (appelé **REMPART**) est actuellement mis en oeuvre au sein du service du numérique (SNUM) afin d'assurer une continuité informatique pour les systèmes (matériels et logiciels) informatiques jugés sensibles. Les modalités d'intégration d'un projet ou d'une application informatique dans **REMPART** sont à prévoir avant le lancement du projet.

Tableau des attributs de qualité:

Caractéristiques	Attribut de qualité Mesuré	Valeur
Fiabilité	Durée maximale d'interruption admissible (DMIA)	< 1 journée

Les systèmes concernés par ce plan de continuité informatique sont listés dans le tableau ci-dessous :

Système	Description	Direction	DMIA	PDMA	Criticité	Plage de service	Commentaire
AD	Annuaire LDAP Microsoft Active Directory	SNUM	24h	24h	Critique	8h - 20h	
AFT Web	Application métier	AFT	4h	24h (*)	Critique	8h - 22h	(*) Clone
Annuaire	Annuaire LDAP hors AD	SNUM					
Artemis	Accès à distance VPN	SNUM	4h	SO (*)	Elevée	24h24 - 7j/7 (**)	(*) Réplication temps réel (**) Paramétrable par les gestionnaires
PLATEAUX	Réseau - Service de routage	SNUM	0	0	Critique	24h/24 - 7j/7	
WAN	Réseau - Réseau étendu WAN	SNUM	?	SO	Critique ?	?	
MAN	Réseau - Réseau métropolitain MAN	SNUM	?	SO	Critique ?	?	
WIFI	Réseau - Réseau sans fil WIFI	SNUM					
DHCP - DNS	Réseau - Services DHCP et DNS	SNUM	0	0	Critique	24h/24 - 7j/7	
NTP	Réseau - Service de synchronisation du temps	SNUM	0	0	Critique	24h/24 - 7j/7	
MOTUS	Téléphonie - Téléphonie mobile sécurisée MOTUS	SNUM	0	SO (*)	Critique	24h/24 - 7j/7	(*) SO pour la gateway / VM pour mobileiron et pushmanager

MODUS	Téléphonie - Téléphonie mobile de base MODUS	SNUM	0	SO (*)	Critique	24h/24 - 7j/7	(*) Cluster pour mobileiron
PAC	Sécurité - Service de proxy	SNUM	0	SO	Critique	24h/24 - 7j/7	
SIEM	Sécurité - Gestion de l'information des événements de sécurité	SNUM					
IGC	Sécurité - Infrastructure de gestion de clés	SNUM	-	72h (*) 2h (**)	Elevée	24h/24 - 7j/7	(*) pour le serveur IGC-CMS (**) pour la révocation depuis le réseau internet
SSO	Sécurité - Authentification SSO	SNUM	0	SO	Critique	24h/24 - 7j/7	Via script à chaque action
TOTEM	Sécurité - Accès à distance TOTEM	SNUM	0	SO (*)	Critique	24h/24 - 7j/7	(*) Cluster
ANGIE - GESTANGIE	Annuaire ANGIE et application GESTANGIE	SNUM					
CEPHALONIE	Espace bureautique du bureau des cabinets	SNUM	24h	1h (*)	Critique	9h - 17h	(*) Temps réel DT Asynchrone storage repliquat Microsoft
BOUNTY	Espace bureautique des cabinets	SNUM	24h	1h (*)	Critique	9h - 17h	(*) Temps réel DT Asynchrone storage repliquat Microsoft
BALI	Espace bureautique des directions	SNUM	24h	4h (*)	Critique	9h - 17h	(*) Miroir NetApp
EXCHANGE	Messagerie Microsoft Exchange	SNUM	0	0 (*)	Critique	24h/24 - 7j/7	(*) Réplication temps réel
RELAIS	Relais de messagerie	SNUM	0	0	Critique	24h/24 - 7j/7	
GESTEXCHANGE	Application de gestion de l'annuaire Exchange	SNUM					
ZCM	Application de télédistribution ZCM	SNUM					
RVR PARAD	Application destinée à définir les plans de continuité et d'aider à piloter leur exécution	SNUM	24h	24h (*)	Elevée	9h - 18h	(*) Clone pour APP et Dump pour BDD
UNISSON	Application métier de la DB	DB	0,5h	2h	Critique	09h - 18h	Réplication des données toutes les 2 heures avec DoubleTake
SIGED	Application de gestion électronique de documents	DB					
DOSSIEL	Application de gestion des courriers	SNUM					
EGIDE	Application métier de la DGE	DGE	1J (*) 6h (**)	1h	Critique	24h/24 - 7j/7	(*) sur le frontoffice (**) sur le back-
							office
SYMPA	Application de gestion des listes de diffusion	SNUM	4h	24h (*)	Critique	9h - 18h	(*) Clone
SILLAGE	Application métier de la DAJ	SNUM					
ARCHIMED - HARMONIE	Application métier du bureau des cabinets	SNUM					

Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_8_3_1_001	Tout système intégrant le plan de continuité informatique (REMPART) doit faire l'objet d'un exercice annuel planifiée consistant : <ul style="list-style-type: none">▪ à la relecture des procédures et à leur mise à jour avant :▪ d'une part à basculer le système du site nominal vers le site de secours▪ et d'autre part à faire un retour du système du site de secours vers le site nominal.	Validé	12/09/2022	
	2_8_3_1_002	Tout système souhaitant intégrer le plan de continuité informatique (REMPART) doit définir un certain nombre de critères qui va permettre de choisir la solution de secours la plus adaptée : - DMIA (Durée Maximale d'Interruption Admissible) - PDMA (Perte de Données Maximales Admissibles) - Criticité (Faible, Moyenne, Elevée, Critique)	Validé	12/09/2022	

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_8_3_2_001	Le plan de continuité informatique du SG/SNUM doit être suivi au travers du logiciel propriétaire RVR PARAD.	Validé	06/07/2022	

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_3_8_3_001				

Contraintes techniques

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_3_8_4_001				

▪ La dernière modification de cette page a été faite le 8 février 2024 à 15:31.

Exploitation et administration des serveurs

L'**exploitation informatique** est l'activité qui consiste à maintenir opérationnel de manière stable, sûre et sécurisée un outil informatique dans un environnement de développement, de qualification, de formation, ou de production, dans ses parties matérielles et logicielles.

(source : wikipedia,2020 (https://fr.wikipedia.org/wiki/Exploitation_informatique))

L'**exploitation** est l'ensemble des tâches nécessaires au bon fonctionnement d'un ou de plusieurs ordinateurs.

(source : Office québécois de la langue française,2001 (http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8369642))

En informatique, l'**administration** ou le poste d'administrateur renvoie à la notion de gestion (installation, maintenance, amélioration, supervision, sécurité). L'administrateur reçoit pour cela des droits d'accès aux données et aux fonctionnalités plus étendus que les autres utilisateurs. On distingue en général : l'administration système (du système d'exploitation : processus, fichiers, utilisateurs...), l'administration réseau (du réseau informatique, l'administration de base de données, l'administration des applications. (source : wikipedia,2020 (<https://fr.wikipedia.org/wiki/Administration>))

✓ Terme privilégié : **exploitation, administration**

✓ Equivalent étranger: **operation** (en), **operating** (en),

Sommaire

- 1 Contexte
- 2 Règles de base
- 3 Solutions de référence
- 4 Contraintes juridiques et réglementaires
- 5 Contraintes techniques
- 6 Transfert de fichiers

Contexte Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_8_5_1_001	Toute nouvelle application doit faire l'objet d'un dossier d'exploitation (DEX) (https://documento.alize.finances.rie.gouv.fr/share/s/SC12dkRrTiGpu69M7p6uQ).	Validé	22/01/2020	
	2_8_5_1_002	Un poste d'administration physique ou virtuel doit être positionné dans une DMZ	Validé	03/12/2020	
	2_8_5_1_003	Un poste d'administration physique ou virtuel ne doit pas accéder à Internet.	Validé	03/12/2020	

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_8_5_2_001				

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_8_5_3_001				

Contraintes techniques

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_8_5_4_001	L'exploitation et l'administration des serveurs doit se faire depuis un poste d'administration (physique ou virtuel) : <ul style="list-style-type: none">■ via le protocole RDP pour les serveurs Windows,■ via le protocole SSH pour les serveurs Linux.	Validé	08/07/2020	
	2_8_5_4_002	L'exploitation et l'administration des serveurs doivent se faire depuis un poste d'administration (physique ou virtuel) avec les logiciels suivants: <ul style="list-style-type: none">■ le logiciel libre Bitvise SSH client pour accéder à distance aux serveurs Linux,■ le logiciel libre Remote Desktop Service pour accéder à distance aux serveurs Windows,■ le logiciel libre Keepass pour gérer les mots de passe des serveurs.	Validé	08/07/2020	
	2_8_5_4_003	L'exploitation et l'administration des serveurs ne doit pas se faire avec le protocole suivant: <ul style="list-style-type: none">■ Telnet (Terminal Network) pour émuler un terminal distant	Validé	03/12/2020	source: SEP1C/PSSI

Transfert de fichiers

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_8_5_5_001	Le transfert de fichiers réalisé depuis un poste d'administration (physique ou virtuel) doit se faire au travers de l'un des protocoles suivants : <ul style="list-style-type: none">■ Protocole SFTP,■ Protocole CFT.	Validé	03/12/2020	
	2_8_5_5_002	Le transfert de fichiers réalisé depuis un poste d'administration (physique ou virtuel) ne doit pas se faire au travers des protocoles suivants : <ul style="list-style-type: none">■ Protocole FTP,■ Protocole FTPS.	Validé	03/12/2020	

• La dernière modification de cette page a été faite le 8 février 2024 à 14:12.

Accès à distance (Remote access) version diffusable

L'accès à distance, la commande à distance ou encore le contrôle à distance sont des méthodes qui permettent, depuis un ordinateur éloigné et sans limite théorique de distance, de prendre le contrôle d'un autre ordinateur en affichant l'écran de celui-ci et en manipulant les fonctions d'un périphérique d'entrée comme un clavier. Cet accès peut être effectué vers des postes de travail ou des serveurs informatique en fonction des possibilités du logiciel utilisé.

(source : wikipedia,2022 (https://fr.wikipedia.org/wiki/Acc%C3%A8s_%C3%A0_distance)).

- ✓ Termes privilégiés :accès à distance, téléaccès, accès distant
- ✓ Equivalent étranger: remote access (en)

La version de base de cette rubrique est accessible ici

Sommaire

- 1 Contexte
- 2 Règles de base
- 3 Solutions de référence
- 4 Contraintes juridiques et réglementaires ▪
- 5 Contraintes techniques

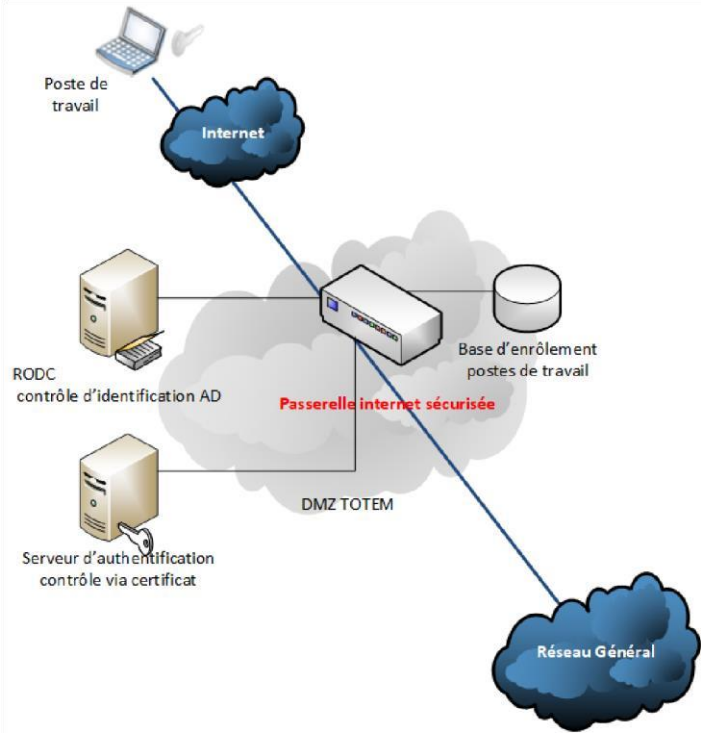
Contexte

L'offre d'accès à distance des agents de l'administration centrale proposée par le service du numérique SNUM s'appuie sur la solution TOTEM.

- le logiciel propriétaire Serveur BIG-IP (TOTEM Serveur)
- le logiciel propriétaire Client BIP-IP Edge 7220.2022 (TOTEM Client)

L'accès à cette solution se fait depuis un logiciel "agent" VPN préconfiguré et installé sur le poste de travail de l'agent, pour se connecter au serveur VPN. Une fois connecté, l'agent peut accéder à ses applications courantes et ses ressources bureautiques avec la même ergonomie que lorsqu'il est connecté à son bureau.


L'architecture technique simplifiée de la solution d'accès à distance (des agents) se décline de la manière suivante :



Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_8_6_1_001				

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_8_6_2_001	L'accès à distance des agents de l'administration centrale doit se faire au travers de la solution de référence TOTEM .	Validé	08/07/2020	

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_8_6_3_001				

Contraintes techniques

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_8_6_4_001	L'accès à la solution TOTEM doit se faire : <ul style="list-style-type: none">▪ depuis un poste de travail de l'Administration Centrale, préalablement enrôlé, disposant d'un pare-feu actif, d'un OS et de signatures antivirus à jour,▪ via un certificat d'authentification personnel sur clé cryptographique ou puce TPM valide.	Validé	08/07/2020	
	2_8_6_4_002	Le package Client TOTEM doit être installé sur le poste de travail de l'Administration Centrale à partir du logiciel propriétaire ZCM.	Validé	08/07/2020	

• La dernière modification de cette page a été faite le 25 février 2024 à 07:41.

Supervision Système version diffusable

La supervision est la «surveillance du bon fonctionnement d'un système ou d'une activité». Elle permet de surveiller, rapporter et alerter les fonctionnements normaux et anormaux des systèmes informatiques. (source : wikipedia,2022 ([\)](https://fr.wikipedia.org/wiki/Supervision_(informatique))

✓ Terme privilégié : **supervision**

✓ Equivalent étranger: **monitoring** (en)

La version de base de cette rubrique est accessible [ici](#)

Sommaire

- 1 Contexte
- 2 Règles de base
- 3 Solutions de référence
- 4 Contraintes juridiques et réglementaires ▪
- 5 Contraintes techniques

Contexte

L'offre de supervision système dénommée **OSIRIS** proposée par le service du numérique (SNUM) s'appuient sur le logiciel libre **Centreon**.

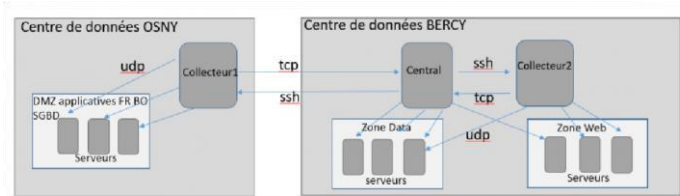
L'architecture technique est constituée:

- d'un serveur de supervision Central,
- d'un serveur «collecteur1» situé à OSNY avec pour fonction la supervision des serveurs du centre de données d'OSNY
- d'un serveur «collecteur 2" situé à BERCY avec pour fonction la supervision des serveurs du centre de données de BERCY.

Ce montage a plusieurs intérêts :

- il permet de répartir la charge sur plusieurs serveurs de supervision;
- Il permet de limiter l'impact du flux de supervision sur les interconnexions de réseaux; ▪ il permet l'isolation de réseau.

L'architecture technique de cette solution se décline de la manière suivante :



Source : Centreon (<https://docs.centreon.com/current/fr/>)

Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_8_7_1_001	Tous les serveurs doivent être intégrés dans l'logiciel libre Centreon, exceptés : <ul style="list-style-type: none">▪ les serveurs inscrits dans une offre d'hébergement sec (https://monalize.alizeites/Alize/accueil/vie-quotidienne/hebergement-informatique/mon-service-adhaite-beneficier.html),▪ les serveurs directionnels.	Validé	10/09/2020	
	2_8_7_1_002	La solution de référence de supervision système doit être installée dans des versions à jour des correctifs de sécurité.	Validé	10/09/2020	

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_8_7_2_001	La solution de supervision système appelée OSIRIS doit s'appuyer sur le logiciel Libre Centreon.	Validé	10/09/2020	

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_8_7_3_001	Toute demande de support sur le logiciel libre Centreon doit se faire au travers du marché "Support à l'usage des logiciels libres".	Validé	10/09/2020	

Contraintes techniques

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_8_7_4_001	La solution de référence de supervision système doit s'appuyer sur le protocole suivant : - protocole SNMP	Validé	10/09/2020	
	2_8_7_4_002	Un flux SNMP doit être ouvert depuis les serveurs OSIRIS vers les serveurs supervisés.	Validé	10/09/2020	
	2_8_7_4_003	Les services supervisés par défaut sur les serveurs Linux doivent être : - check_ping, cpu_linux, load_linux, memory_linux, proc_crond_linux, proc_ntpd_linux, storage_linux, swap_linux et uptime_linux.	Validé	10/09/2020	
	2_8_7_4_004	Les services supervisés par défaut sur les serveurs Windows doivent être : - check_ping, cpu_windows, memory_windows, storage_windows, swap_windows et uptime_windows.	Validé	10/09/2020	

• La dernière modification de cette page a été faite le 2 mai 2024 à 16:10.

Gestion de logs serveurs

La **gestion de logs** (LM pour *Log Management*) comprend une approche de la gestion de grands volumes des messages de log générés par l'ordinateur (aussi connu comme journaux d'évènements, journalisation, etc.). La gestion des logs concerne en général:

- La collecte des logs
- L'agrégation centralisée des logs
- Le stockage à long terme et la durée de rétention des logs
- La rotation des fichiers de logs
- L'Analyse des logs
- Les rapports et l'étude des logs.

Sommaire

- 1 Contexte
- 2 Règles de base
- 3 Solutions de référence
- 4 Contraintes juridiques et réglementaires ▪
- 5 Contraintes techniques

Contexte Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_8_8_1_001				

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_8_8_2_001				

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_8_8_3_001	Les journaux des événements de sécurité doivent être conservés sur douze mois glissants hors contraintes légales et réglementaires imposant des durées de conservation spécifique (extrait PSSI ANSSI.pdf exp-cons-jou PSSI ANSSI.pdf (https://www.ssi.gouv.fr/uploads/2014/11/pssie_anssi.pdf))	Validé	29/09/2021	

Contraintes techniques

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_8_8_4_001				

▪ La dernière modification de cette page a été faite le 20 février 2024 à 21:50.