Cadre de cohérence technique (CCT)

Cette page liste les nouveautés du Wiki CCT.

Nouveautés

10/02/2021 Comité d'architecture n°8
03/12/2020 Comité d'architecture n°7
10/09/2020 **Comité d'architecture n°6**
17/08/2020 CCT au format PDF
08/07/2020 Comité d'architecture n°5
18/05/2020 Comité d'architecture n°4 (en visio)
22/01/2020 Comité d'architecture n°3
03/12/2019 Comité d'architecture n°2
30/09/2019 Présentation Docker
03/09/2019 Comité d'architecture n°1

Sommaire

Pourquoi un cadre de cohérence technique ?

Dans un contexte d'évolution rapide de l'environnement (législatif, réglementaire, organisationnel, technique, etc.), l'objectif principal de la sous-direction informatique des services centraux (SEP1) du secrétariat général (SG) des ministères économiques et financiers (MEF) est de **disposer d'un système d'information adapté et adaptable** de manière à répondre rapidement aux besoins du moment avec des budgets de plus en plus contraints.Le cadre de cohérence technique a donc pour vocation de :

- **permettre aux applications de partager de manière optimale l?infrastructure du système d'information** en termes d'hébergement, de réseaux, d'équipements matériels et de composants logiciels;
- **permettre aux applications d?interopérer entre elles et avec les acteurs externes (partenaires);**;
- **assurer la pérennité des composants de base**, limiter la variabilité des plates-formes et des configurations par une évolution concertée des composants;
- **maîtriser les coûts d?acquisition des progiciels et des composants logiciels** ainsi que ceux des services d?intégration et d?administration en évitant que chaque application n?impose ses propres composants de base.

Le cadre de cohérence technique est le résultat d'une activité continue du groupe de travail CCT du projet interSEP, qui veille à **garantir la cohérence, la maintenabilité et l?évolutivité du système d'information**. Il est donc nécessaire que ce cadre de cohérence soit :

- **partagé** : le cadre de cohérence technique sera d'autant mieux adapté qu'il répondra aux besoins de SEP1 et des acteurs externes (partenaires) d'une part, qu?il sera à l'état de l'art, d'autre part.
- **visible** : la visibilité du cadre de cohérence technique apparaît comme une condition de son respect par les acteurs et parties prenantes de SEP1. La publication du cadre apparaît donc nécessaire, sa mise en ligne sur ce wiki y contribuera.
- **évolutif** : les choix faits correspondent à l'état de l'art, dont on sait qu'il est évolutif. Une actualisation au minimum trimestrielle du cadre de cohérence technique est envisagée.

Enfin, Il **remplace les socles techniques internes existants de SEP1**, à savoir :

- Le socle technique et sécurité des développements informatiques (SEP1B),
- L'environnement technologique des infrastructures réseaux et serveurs (SEP1C),
- Le socle technologique des postes de travail (SEP1D).

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

Il constitue le cadre de référence pour toute personne désireuse de connaître les règles sur les différents composants du système d'information de SEP1. Ces règles sont formulées de manière à ce qu'elles renvoient à différents niveaux de préconisations, conformément à la *RFC 2119'* 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

Il convient de privilégier les règles avec le niveau de préconisation "**Obligatoire**" et "**Interdit**".

Comment est structuré le cadre de cohérence technique ?

Le cadre de cohérence technique est structurée autour de deux vues :

- la **vue infrastructure** décrivant les règles qui s'appliquent aux équipements et à l'infrastructure technique du système d'information;
- la **vue applicative** décrivant les règles qui s'appliquent aux applications et aux composants logiciels du système d'information.

Vue infrastructure du système d'information

Les principales thématiques au sein de la vue Infrastructure du système d'information sont listées ci-dessous. Chaque thématique fait l'objet d'une page spécifique où sont listées l'ensemble des règles.

Hébergement

Centre de données

Réseaux

Commutateur réseau - Zone démilitarisée (DMZ) - Répartiteur de charge
Serveur NTP

Equipements matériels

Serveur physique - Poste de travail physique - Terminal mobile
Equipement de stockage - Equipement de sauvegarde
Badgeuse
Commutateur KVM

Composants logiciels système, virtualisation et conteneurisation

Système d'exploitation serveur - Système d'exploitation poste de travail
Serveur virtuel
Poste de rebond virtuel (VPR) - Poste d'administration virtuel (VPC)
Conteneur logiciel

Vue applicative du système d'information

Les principales thématiques identifiées au sein de la vue applicative du système d'information sont listées ci-dessous. Chaque thématique fait l'objet d'une page spécifique où sont listées l'ensemble des règles.

Fonctions et services de sécurité applicative

Serveur d'authentification unique (SSO) - Serveur mandataire inverse (SMI)
Chiffrement de flux
Protection antivirus des postes de travail - Protection antipourriel des serveurs
Scanner de vulnérabilité

Espace utilisateur & canal

Navigateur web - Client de messagerie

Présentation

Serveur web

Orchestration et logique métier

Serveur d'application
Environnement d'exécution PHP - Environnement d'exécution JAVA
Serveur de messagerie - Serveur de relais de messagerie

Intégration et échanges

Intégration de données (ETL)

Données et contenus

Annuaire Active Directory (AD) - Annuaire LDAP

Protection des données (RGPD)
Système de gestion de base de données (SGBD)

Conception et développement

Gestion du code source - Gestion des anomalies
Environnement de développement intégré (IDE)
Qualité et sécurité du code source - Tests et intégration

Opérations

Gestion des environnements
Sauvegarde et restauration des données (serveurs)
Accès à distance (des prestataires) - Accès à distance (des agents)
Exploitation et administration des serveurs

Ressources transverses

Marchés publics

Quelle gouvernance autour de ce cadre de cohérence technique ?

La gouvernance du cadre de cohérence technique est organisée de la manière suivante :

- un **comité de validation technique,** composé d'agents des quatre bureaux de SEP1. Il se réunira **une fois par mois** et aura pour mission :
  - d'analyser les nouvelles propositions de règle;
  - de proposer les règles à valider par le comité de pilotage;
  - de saisir les règles validées dans le présent WIKI.

- un **comité d'architecture,** composé du sous-directeur informatique, des chefs de bureau et du comité de validation technique. Il se réunira **une fois par trimestre** et aura pour mission de :
  - d'entériner les règles à valider proposées par le comité de validation technique;
  - de statuer sur les règles ne nécessitant pas de consensus au niveau du comité de validation technique.

Qui est concerné par le cadre de cohérence technique ?

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

- principalement aux **agents de la sous-direction informatique des services centraux SEP1**,
- mais également aux **services informatiques des directions métiers** ainsi qu'aux **prestataires de service** en lien avec les agents de SEP1.

Qui peut contribuer à la mise à jour du cadre de cohérence technique ?

Tout agent de SEP1 a la possibilité dans son domaine d'expertise de faire des suggestions en termes de :

- création de nouvelle contrainte,
- modification d'une contrainte existante,
- suppression d'une contrainte existante.

Chaque proposition sera étudiée par le comité de validation technique.

Comment faire une suggestion ?

SI vous souhaitez soumettre une suggestion au comité de validation technique, veuillez formuler votre demande auprès de la BAL Wiki

Glossaire

Les principaux termes utilisés dans ce wiki sont regroupés dans le glossaire

Centre de données

Un **centre de données** est un lieu (et un service) regroupant des équipements constituants 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, 2020 (https://fr.wikipedia.org/wiki/Centre_de_donn%C3%A9es))

Un **centre de données** est un lieu où sont regroupées des ressources informatiques et de télécommunication afin d'offrir des services de gestion, de stockage et de traitement des données informatiques. Les centres de traitement de données disposent généralement de plusieurs mesures de sécurité (système contre l'incendie ou contre le vol, système d'alimentation d'urgence, etc.). La température et l'humidité y sont contrôlées.

(source : Office québécois de la langue française, 2019 (http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8874188))

Un **centre de données** est un site physique où sont regroupées des infrastructures informatiques et de télécommunication destinées à stocker, à traiter ou à distribuer des données de façon sécurisée.

(source : FranceTerme, 2019 (https://www.legifrance.gouv.fr/jo_pdf.do?id=JORFTEXT000039384954))

Termes privilégiés :**centre de données**, **centre de traitement de données**, **centre de traitement informatique**

Equivalent étranger: **data center** (en), **data centre** (en), **data processing center** (en), **DPC** (en), **data processing centre** (en)

Sommaire

Contexte

Les offres d'hébergement (https://monalize.alize/sites/Alize/accueil/vie-quotidienne/hebergement-informatique/mon-service-souhaite-beneficier.html) proposées par SEP1 aux directions des MEF s'appuient sur plusieurs centres de données répartis sur les sites géographiques suivants :

- Site géographique de Bercy
  - **Centre de données principal de Bercy** - Bâtiment Vauban - Salles 5001 et 5002 - Corridor Nord 5 - 139 Rue de Bercy 75012 PARIS
  - **Centre de données de sauvegarde de Sully** - Bâtiment Sully - Salle 526F - 64 Allée de Bercy – 75012 Paris
- Site géographique d'Ivry
  - **Centre de données de secours d'Ivry** - Bâtiment Irène Joliot-Curie - Salles S1-343 et S1-345 - 67 Rue Barbès 94200 Ivry-sur-seine
- Site géographique d'Osny
  - **Centre de données d'Osny** (Centre informatique douanier) - Bâtiment 2 - 27 Rue des Beaux Soleils 95520 Osny

D'autres offres d'hébergement sont proposées au sein des MEF, à savoir :

- Le Cloud interministériel NUBO (https://portailnubo.dgfip.finances.rie.gouv.fr/)proposée par la DGFIP en tant que solution cloud de niveau 1.

Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_1_1_1_001	Les centres de données de référence de SEP1 doivent respecter le standard ministériel Centres 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).	Validé	01/07/2019	Zone protégée Convention d'hébergement Reporting (notifications et statistiques)
	1_1_1_1_002	Les directions des MEF peuvent s'appuyer sur les offres d'hébergement suivantes : ▪ Hébergement sec (https://monalize.alize/sites/Alize/accueil/vie-quotidienne/hebergement-informatique/mon-service-souhaite-beneficier.html) , ▪ Hébergement managé (https://monalize.alize/sites/Alize/accueil/vie-quotidienne/hebergement-informatique/mon-service-souhaite-beneficier.html).	Validé	01/07/2019	

Solution de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_1_1_2_001				

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_1_1_3_001	La surveillance et de gestion des centres de données de référence de SEP1 doit 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	Les directions et services du secrétariat général (SG) des ministères économiques et financiers (MEF) peuvent s'appuyer sur le cahier des clauses simplifiées de cybersécurité (https://www.legifrance.gouv.fr/eli/arrete/2018/9/18/ECOP1825228A/jo/texte/fr) en cas d'Infogérance.	Validé	01/07/2019	

Contraintes techniques

Centre de données de Bercy

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_1_1_4_001	Les nouvelles applications nécessitant un plan de continuité informatique (PCI) doivent être installées sur des serveurs à vocation applicative localisés dans le centre de données de Bercy.	Validé	01/07/2019	
	1_1_1_4_002	Les nouvelles applications exposées sur le réseau internet ne nécessitant pas de plan de continuité informatique (PCI) doivent être installées sur des serveurs à vocation applicative localisés dans le centre de données de Bercy.	Validé	01/07/2019	

Centre de données d'Ivry

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_1_1_5_001	Les nouvelles applications nécessitant un plan de continuité informatique (PCI) doivent être secourues sur des serveurs à vocation applicative localisés dans le centre de données d'Ivry.	Validé	01/07/2019	

Centre de données d'Osny

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_1_1_6_001	Les nouvelles 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 localisés dans le centre de données d'Osny.	Validé	01/07/2019	
	1_1_1_6_002	Les nouvelles 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 localisés dans le centre de données d'Osny.	Validé	01/07/2019	

Centre de données de la DGFIP (Cloud NUBO)

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_1_1_7_001	Les nouvelles applications hébergées dans le cloud interministériel DGFIP NUBO ne peuvent être interfacées qu'avec : ▪ les serveurs de relais de messagerie (externes et RIE) de SEP1 si le domaine de messagerie est géré par SEP1.	Validé	08/07/2020	Il n'est pas prévu d'autres interfaces avec les b du SI de SEP1 : - SSO, Annuaires, applications métiers...

- La dernière modification de cette page a été faite le 11 décembre 2020 à 07:51.

Commutateur réseau

Un **commutateur réseau** 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.

(source : wikipedia, 2020 (https://fr.wikipedia.org/wiki/Commutateur_r%C3%A9seau))

Un **commutateur réseau** est un équipement de réseau, installé à différents nœuds, qui a pour fonction d'établir d'un point à un autre les connexions nécessaires à l'acheminement des signaux.

(source : Office québécois de la langue française, 2001 (http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8391612))

Terme privilégié : **commutateur réseau**

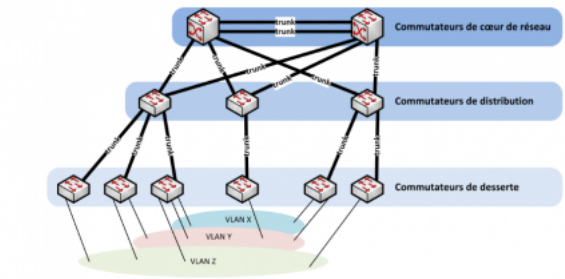
Equivalent étranger: **switch** (en)

Sommaire

Contexte

Les offres de commutateur réseau Ethernet proposées par SEP1 s'appuient sur les équipements de la marque **HPE FlexFabric**. On distingue trois types de commutateurs réseau :

- **les commutateurs de coeur 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, ...).



Source : Guide ANSSI "Recommandations pour la sécurisation d'un commutateur de desserte (https://www.ssi.gouv.fr/uploads/2016/07/nt_commutateurs.pdf)"

Remarque : La note technique « Recommandations pour la sécurisation d'un commutateur de desserte » sert de référence pour la configuration de nos commutateurs réseau.

Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_2_1_1_001	Les commutateurs réseaux 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
	1_2_1_2_001	Les commutateurs réseaux installés dans les centres de données de référence de SEP1 doivent s'appuyer sur les modèles suivants : ▪ Commutateurs HPE FlexFabric 5700 (https://www.hpe.com/fr/fr/product-catalog/networking/networking-switches/pip.models.fixed-port-l3-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-l3-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_1_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	L'administration et l'exploitation des commutateurs réseaux de référence doivent se faire au travers du logiciel propriétaire **HPE Intelligent Management Center (IMC) 7.3**	Validé	22/01/2020	
	1_2_1_4_002	Les ports cuivre 100/1000/10000 des commutateurs réseaux doivent être utilisés pour les connexions : ▪ des terminaux (endpoints) sur le Campus, ▪ des serveurs sur les commutateurs de travée sur le centre de données.	Validé	22/01/2020	
	1_2_1_4_003	Les ports SFP+ des commutateurs réseaux doivent être utilisés pour : ▪ 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_004	Les ports QSFTP+ des commutateurs réseaux doivent être utilisés pour : ▪ la création de commutateurs logiques nécessitant du 40 Go.	Validé	22/01/2020	
	1_2_1_4_005	Les commutateurs d'accès doivent utiliser la nome 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_006	Les commutateurs coeur de réseau doivent s'appuyer sur les protocoles suivants : ▪ 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) ▪ VRRP (https://fr.wikipedia.org/wiki/Virtual_Router_Redundancy_Protocol)	Validé	22/01/2020	

- La dernière modification de cette page a été faite le 13 juillet 2020 à 14:58.

Zone démilitarisée (DMZ)

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.

(source : wikipedia,2020 (https://fr.wikipedia.org/wiki/Zone_d%C3%A9militaris%C3%A9e_(informatique)))

Une **zone démilitarisée** est utilisée pour désigner un sous-réseau séparant deux zones de confiance hétérogène notamment grâce à des pare-feux réalisant un filtrage périmétrique de part et d'autre.

(source : Anssi,2012 (https://www.ssi.gouv.fr/uploads/2012/01/anssi-guide-passerelle_internet_securisee-v2.pdf))

Une **zone démilitarisée** est une zone tampon d'un réseau d'entreprise, située entre le réseau local et Internet, derrière le coupe-feu, qui correspond à un réseau intermédiaire regroupant des serveurs publics (HTTP, SMTP, FTP, DSN, etc.), et dont le but est d'éviter toute connexion directe avec le réseau interne et de prévenir celui-ci de toute attaque extérieure depuis le Web.

(source : Office québécois de la langue française, 2001 (http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8367770))

Terme privilégié : **zone démilitarisée**

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

Sommaire

Contexte

Le centre de données 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 serveurs 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.

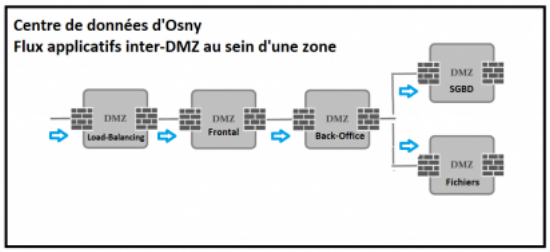
La DMZ Service permet aux serveurs des différentes zones un accès contrôlé à internet via le serveur mandataire ASTRAL (port 8080). L'accès s'effectue au travers des protocoles HTTP ou HTTPS et se base sur une liste blanche d'URL. Les serveurs du RG sont proxifiés sur proxyserveurs.alize qui sert de rebond vers ASTRAL, port 8080. Elle permet la résolution par les internautes des noms de domaine propriété du ministère via nos DNS publics.

Le centre de données d'Osny est segmenté en plusieurs zones réseaux logiques :

- Une zone mutualisée contenant les serveurs intranet de développement de SEP1
- Une zone mutualisée contenant les serveurs intranet de recette et de production de SEP1
- Une zone dédiée contenant les serveurs intranet d'infrastructure de SEP1
- Des zones dédiées contenant les serveurs intranet de certaines directions et services (AFA, Associations, Cabinet, DAE, DB, DGE, DSI, IGPDE et SHFDS).

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

- d'une DMZ Load-Balancing (nouveau !) contenant les répartiteurs de charge
- d'une DMZ Frontale contenant les serveurs mandataires inverses (SMI)
- 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
Nouveauté	1_2_2_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_2_1_002	Les serveurs des zones situées sur le centre de données d'Osny doivent s'appuyer sur un serveur mandataire 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_2_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_2_2_001				

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_2_2_3_001				

Contraintes techniques

Centre de données d'Osny - DMZ Frontale

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_2_2_4_001	La DMZ Frontale située sur le centre de données d'Osny doit être utilisée pour héberger : ▪ les serveurs mandataires inverses (SMI) mutualisés.	Validé	03/09/2019	
	1_2_2_4_002	Les flux applicatifs entrants autorisés de la DMZ Frontale située sur le centre de données d'Osny doivent être basés sur : ▪ Le protocole HTTP (port 80) redirigé vers le protocole HTTPS (port 443), ▪ Le protocole HTTPS (port 443).	Validé	03/09/2019	
	1_2_2_4_003	Les flux applicatifs sortants autorisés de la DMZ Frontale située sur le centre de données d'Osny doivent être basés sur : ▪ le protocole HTTPS (port 443), ▪ le protocole LDAP, ▪ le protocole LDAPS.	Validé	18/05/2020	Ajout des protocoles LDAP et LDAPS
	1_2_2_4_004	Les flux applicatifs sortants de la DMZ Frontale située sur le centre de données d'Osny ne peuvent être dirigés que vers : ▪ la DMZ Back-Office située sur le centre de données d'Osny.	Validé	03/09/2019	
	1_2_2_4_005	Les applications avec des utilisateurs dont l'origine est le réseau intranet doivent passer par un serveur mandataire inverse (SMI) spécifique.	Validé	18/05/2020	
	1_2_2_4_006	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	

Centre de données d'Osny - DMZ Back-Office

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_2_2_5_001	La DMZ Back-Office située sur le centre de données d'Osny doit être utilisée pour héberger les serveurs à vocation applicative exposés sur : ▪ le réseau général (RG), ▪ le réseau interministériel de l'Etat (RIE).	Validé	03/09/2019	
	1_2_2_5_002	Les flux applicatifs entrants autorisés de la DMZ Back-Office située sur le centre de données d'Osny doivent être basés sur : ▪ le protocole HTTPS (port 443).	Validé	03/09/2019	
	1_2_2_5_003	Les flux applicatifs sortants de la DMZ Back-Office située sur le centre de données d'Osny doivent être dirigés uniquement vers les DMZ suivantes : ▪ La DMZ SGBD située sur le centre de données d'Osny, ▪ La DMZ Fichiers située sur le centre de données d'Osny, ▪ Le Réseau général (RG) , ▪ La DMZ Data située sur le centre de données de Bercy.	Validé	03/09/2019	

Centre de données d'Osny - DMZ SGBD

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_2_2_6_001	La DMZ SGBD située sur le centre de données d'Osny doit être utilisée pour héberger les serveurs à vocation applicative (serveurs SBGD) exposés sur : ▪ le réseau général (RG), ▪ le réseau interministériel de l'Etat (RIE) si l'une des conditions suivantes est vérifiée : ▪ la base de données est Oracle, ▪ la base de données est PostgreSQL et si : ▪▪ 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_2_6_002	Les flux applicatifs entrants autorisés de la DMZ SGBD située sur le centre de données d'Osny doivent être basés sur : ▪ le protocole TCP pour les système de bases de données de référence de SEP1.	Validé	22/01/2020	
	1_2_2_6_003	Les flux applicatifs entrants autorisés de la DMZ SGBD située sur le centre de données d'Osny doivent provenir de : ▪ de la DMZ Back-Office (située dans la même zone que la DMZ Data) du centre de données d'Osny.	Validé	18/05/2020	

Centre de données d'Osny - DMZ Fichiers

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_2_2_7_001	La DMZ Fichiers située sur le centre de données d'Osny doit être utilisée pour héberger les serveurs à vocation applicative (serveurs de fichiers) exposés sur : ▪ le réseau général (RG), ▪ le réseau interministériel de l'Etat (RIE) si l'une des conditions suivantes est vérifiée : ▪ l'espace de fichiers est supérieur à 100Go, ▪ l'espace de fichiers est partagée avec plusieurs serveurs.	Validé	03/09/2019	
	1_2_2_7_002	Les flux applicatifs entrants autorisés de la DMZ Fichiers située sur le centre de données d'Osny doit être basés sur : ▪ 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	

Centre de données de Bercy - DMZ Web

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_2_2_8_001	La DMZ Web située sur le centre de données de Bercy doit être utilisée pour héberger : ▪ 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). exposés sur : ▪ le réseau internet.	Validé	22/01/2020	
	1_2_2_8_001	Les flux applicatifs entrants autorisés de la DMZ Web située sur le centre de données de Bercy doivent être basés sur : ▪ le protocole HTTPS (port 443).	Validé	22/01/2020	
	1_2_2_8_002	Les flux applicatifs sortants autorisés de la DMZ Web doivent être redirigés uniquement vers les DMZ suivantes : ▪ la DMZ Data du centre de données de Bercy, ▪ la DMZ Fichiers du centre de données de Bercy.	Validé	22/01/2020	

Centre de données de Bercy - DMZ Data

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_2_2_9_001	La DMZ Data située sur le centre de données de Bercy doit être utilisée pour héberger : ▪ les serveurs à vocation applicative, ▪ les serveurs d'annuaire (LDAP) exposés sur : ▪ le réseau internet ▪ le réseau internet ou le réseau général (RG)	Validé	18/05/2020	Remplacement de "Serveur à vocation applica au lieu de "serveurs de nouvelles applications
	1_2_2_9_002	Les flux applicatifs entrants autorisés de la DMZ Data située sur le centre de données de Bercy doivent être basés sur : ▪ 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	Ajout des protocoles LDAP, LDAPS et TCP p les SGBD

Centre de données de Bercy - DMZ Fichiers

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_2_2_10_001	La DMZ Fichiers située sur le centre de données de Bercy doit être utilisée pour héberger les serveurs mutualisés de fichiers des nouvelles applications web exposées sur : ▪ le réseau internet, ▪ le réseau internet et le réseau général (RG).	Validé	22/01/2020	
	1_2_2_10_002	Les flux applicatifs entrants autorisés de la DMZ Fichiers située sur le centre de données de Bercy doit être basés sur : ▪ 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	

Centre de données de Bercy - DMZ Service

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_2_2_11_001	Les serveurs situés sur les DMZ Web et Data du centre de données de Bercy doivent synchroniser leur horloge sur le serveur mandataire ASTRAL via le protocole NTP.	Validé	22/01/2020	Le serveur mandataire ASTRAL se met à jou serveur ntp.obs.pm.fr

---

- La dernière modification de cette page a été faite le 25 septembre 2020 à 20:15.

Répartiteur de charge

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, 2020 (https://fr.wikipedia.org/wiki/R%C3%A9partition_de_charge))

Un **répartiteur de charge** est un dispositif matériel ou logiciel qui a pour fonction de distribuer les tâches ou les communications au sein d'un réseau, pour en améliorer la performance.

(source : Office québécois de la langue française, 2002 (http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8364096))

Terme privilégié : **répartiteur de charge**, **répartiteur de charges**, **équilibreur de charge**, **équilibreur de charges**

Equivalent étranger: **load balancer** (en)

Sommaire

Contexte

Les offres de répartiteur de charge proposées par SEP1 s'appuient sur les équipements de la marque **F5 Networks**.

Sur le centre de données d'Osny, il y a 3 instances virtuelles de répartition de charge au sein des répartiteurs de charge

- 1 instance virtuelle pour l'environnement de développement,
- 1 instance virtuelle pour l'environnement de recette hors RG,
- 1 instance virtuelle pour l'environnement de production hors RG.

Remarque : 2 autres instances virtuelles s'ajouteront bientôt à l'existant :

- 1 instance virtuelle pour l'environnement de recette RG
- 1 instance virtuelle pour l'environnement de production RG

Sur les centres de données de Bercy et d'Ivry, il y aura 11 instances virtuelles de répartition de charge correspondant aux 11 instances physiques de répartition de charge Brocade.

Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_2_3_1_001	Les répartiteurs de charge doivent être installés dans des versions à jour des correctifs de sécurité.	Validé	22/01/2020	CERTFR-2020-AVI-819 (https://www.cert.ssi fr/avis/CERTFR-2020-AVI-819/) **BIG-IP 14.1.2.8**
	1_2_3_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	Chaque instance virtuelle de répartition de ch est présente sur 2 répartiteurs de charge physi différents.

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_2_3_2_001	Les nouveaux répartiteurs de charge installés dans les centres de données de référence doivent s'appuyer sur le modèle suivant : - F5 BIG-IP i5800 (https://www.f5.com/pdf/products/big-ip-platforms-datasheet.pdf) - F5 BIG-IP i7800 (https://www.f5.com/pdf/products/big-ip-platforms-datasheet.pdf)	Validé	10/09/2020	Cette solution remplace le modèle BROCAD 1008-1-PREM.

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_2_3_3_001	L'acquisition des répartiteurs de charge doit se faire au travers du marché "Solutions d'infrastructure LAN et WLAN et prestations associées"	Validé	22/01/2020	

Contraintes techniques

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_2_3_4_001	Les nouvelles applications nécessitant un dispositif de répartition de charge doivent s'appuyer sur la solution de référence de SEP1.	Validé	22/01/2020	

- La dernière modification de cette page a été faite le 14 décembre 2020 à 19:56.

Serveur NTP

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**

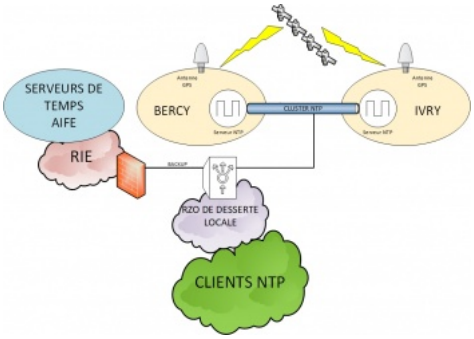
Equivalent étranger: **NTP server** (en)

Sommaire

Contexte

Les offres de serveurs NTP proposées par SEP1 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: ▪ 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 : ▪ Meinberg LANTIME M300 (https://www.meinbergglobal.com/english/products/rack-mount-1u-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: ▪ 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 : ▪ 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 : ▪ 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 : ▪ 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 8 juin 2020 à 21:46.

Serveur physique

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

Un **serveur** est un matériel, logiciel ou système informatique destiné à fournir un service déterminé à d'autres systèmes informatiques ou à des utilisateurs connectés sur un réseau. (source :Commission d'enrichissement de la langue française (France), FranceTerme, 2007 (http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26538397))

Terme privilégié : **serveur**

Equivalent étranger: **server** (en)

Sommaire

Contexte

Les offres de serveurs physiques proposées par SEP1 s'appuient sur les équipements de la marque **Dell PowerEdge.**

Compte tenu de la politique de rationalisation de SEP1, 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). SEP1 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	CERTFR-2020-AVI-557 (https://www.cert.ssi fr/avis/CERTFR-2020-AVI-557/) **Produits INTEL**

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_3_1_2_001	Les nouveaux serveurs physiques installés sur le centre de données d'Osny doit être choisis parmi les 3 modèles suivants : ▪ DELL PowerEdge R640 (https://www.dell.com/fr-fr/work/shop/povw/poweredge-r640) ▪ DELL PowerEdge R740 (https://www.dell.com/fr-fr/work/shop/povw/poweredge-r740) ▪ DELL PowerEdge R740RD (https://www.dell.com/fr-fr/work/shop/povw/poweredge-r740xd)	Validé	01/07/2019	

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	
	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	

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 : ▪ 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 : ▪ 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_de_bus) des serveurs physiques localisés sur le centre de données d'Osny doivent être de type : ▪ 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

<table>
<tr><th></th><th>Identifiant</th><th>Libellé de la règle</th><th>Statut</th><th>Date d'effet</th><th>Commentaires</th></tr>
<tr><td></td><td>1_3_1_5_001</td><td>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 :
<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>où [numéro] est un numéro d'ordre sur 2 caractères.</td><td>Validé</td><td>01/07/2019</td><td></td></tr>
<tr><td></td><td>1_3_1_5_002</td><td>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 :
<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></td><td>Validé</td><td>01/07/2019</td><td></td></tr>
<tr><td></td><td>1_3_1_5_003</td><td>Les noms des serveurs physiques à vocation technique (SGBD) localisés sur le centre de données d'Osny doivent respecter les règles de nommage suivantes :
<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>où [numéro] est un numéro d'ordre sur 2 caractères.
où [équipe] est le nom de l'équipe (COM, INT ou RHC).</td><td>Validé</td><td>01/07/2019</td><td></td></tr>
<tr><td></td><td>1_3_1_5_004</td><td>Les noms des serveurs physiques à vocation applicative localisés sur le centre de données d'Osny doivent respecter les règles suivantes :
<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>où [appli] est le nom de l'application.
où [env] est l'environnement concerné (prd, rec, dev et pprd)
où [tiers] est le nom du tiers (fr, app, ora, msql, psql, ged, idx)
où [numéro] est un numéro sur 2 caractères.</td><td>Validé</td><td>01/07/2019</td><td></td></tr>
</table>

- La dernière modification de cette page a été faite le 9 septembre 2020 à 20:05.

Poste de travail physique

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 : wikiedia,2020 (https://fr.wikipedia.org/wiki/Poste_de_travail))

Termes privilégiés : **poste de travail**

Equivalent étranger: **workstation** (en), **computer workstation** (en)

Sommaire

Contexte

Les offres de postes de travail physiques proposées par SEP1 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%20d%c3%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%c3%a9pertoires/S%c3%a9curit%c3%a9%20des%20syst%c3%a8mes%20d'information/documents/Textes%20de%20r%c3%a9f%c3%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%c3%a9pertoires/S%c3%a9curit%c3%a9%20des%20syst%c3%a8mes%20d'information/documents/Textes%20de%20r%c3%a9f%c3%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%c3%a9pertoires/S%c3%a9curit%c3%a9%20des%20syst%c3%a8mes%20d'information/documents/Textes%20de%20r%c3%a9f%c3%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%c3%a9pertoires/S%c3%a9curit%c3%a9%20des%20syst%c3%a8mes%20d'information/documents/Textes%20de%20r%c3%a9f%c3%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%c3%a9pertoires/S%c3%a9curit%c3%a9%20des%20syst%c3%a8mes%20d'information/documents/Textes%20de%20r%c3%a9f%c3%a9rences/180503_standard-teletravail_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 : ▪ 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	Les postes de travail des agents d'administration centrale doivent être choisis parmi ceux indiqués dans la liste ci-dessous : - **Poste de travail fixe** (Lenovo M710Q, Lenovo M720T), - **Poste de travail portable** (Dell Vostro 3568), - **Poste de travail PC ultra-portable** (Dell Latitude 5310), - **Poste de travail PC hybride** (HP Elitebook X2 G4), dans l'une des configurations standards décrites dans le CCTP du marché d'acquisition.	A valider		En cours de réécriture

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	La configuration matérielle minimale des postes de travail des agents d'administration centrale doit être basée sur les éléments suivants : - 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

Décommisionnement 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 réalisée par les Gestionnaires des Ressources Informatiques Déconcentrées (GRID).	Validé	01/07/2019	processus
	1_3_2_7_002	Le décommissionnement des postes de travail des agents d'administration centrale doit faire l'objet d'un courrier électronique adressé aux équipes suivantes : - SEP1D - TCMP (partie antivirus et télédistribution) - SEP1C - Applications Windows. Les informations suivantes doivent être obligatoirement fournies: - Le nom poste de travail - L'entité d'appartenance	Validé	01/07/2019	processus

Règle de nommage des postes de travail physiques

<table>
<tr><th></th><th>Identifiant</th><th>Libellé de la règle</th><th>Statut</th><th>Date d'effet</th><th>Commentaires</th></tr>
<tr><td></td><td>1_3_2_8_001</td><td>Le nom des postes de travail doit respecter les règles de nommage suivantes :
<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>où [préfixe] est le nom de la direction,
où [suffixe] est le numéro d'inventaire.</td><td>Validé</td><td>01/07/2019</td><td>Exemple : SGSEP1D-258560</td></tr>
</table>

- La dernière modification de cette page a été faite le 7 décembre 2020 à 10:22.

Terminal mobile

Un **mobile multifonction** est un terminal mobile qui assure la téléphonie et l'accès à l'internet par voie radioélectrique, ainsi que d'autres fonctions informatiques ou multimédias.

(source : FranceTerme,2018 (http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26544581))

Un **terminal mobile** est un petit appareil informatique ou de communication qu'on peut transporter avec soi dans ses déplacements et utiliser comme terminal donnant accès sans fil à un ou plusieurs réseaux.

(source : Office québécois de la langue française, 2010 (http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8360495))

Termes privilégiés : **mobile multifonction**, **mobile**

Equivalent étranger: **smartphone** (en)

Sommaire

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 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_3_3_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_3_3_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_3_3_2_001	La solution MODUS doit s'appuyer sur : ▪ 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_3_3_2_002	La solution MOTUS doit s'appuyer sur : ▪ 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_3_3_3_001				

Contraintes techniques

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_3_3_4_001	La solution MODUS doit remplir les conditions suivantes pour pouvoir fonctionner : ▪ 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.	Valdé	22/01/2020	
	1_3_3_4_002	La solution MOTUS doit remplir les conditions suivantes pour pouvoir fonctionner : ▪ 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.	Validé	22/01/2020	

- La dernière modification de cette page a été faite le 20 juin 2020 à 13:04.

Equipement de stockage

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

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

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

Sommaire

Contexte

Les offres d'équipements de stockage proposées par SEP1 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				

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 SEP1 doivent s'appuyer sur les modèles suivants : ▪ NetApp FAS8020 (https://www.netapp.com/us/media/ds-3546.pdf) ▪ NetApp FAS8040 (https://www.netapp.com/us/media/ds-3546.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 "Fourniture d'éléments d'infrastructures informatiques".	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 solutions de stockage et prestations associées".	Validé	03/09/2019	

Contraintes techniques

Réseau SAN FC

Liaison d'un serveur physique à l'infrastructure SAN FC

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_3_4_4_001	Afin de pouvoir être relié à l'infrastructure SAN FC, un serveur physique doit impérativement être équipé d'au moins deux ports HBA à 4, 8 ou 16 Gb/s.	Validé	03/09/2019	
	1_3_4_4_002	Toute liaison d'un serveur physique à l'infrastructure SAN FC doit faire l'objet d'une demande à l'équipe d'exploitation stockage du bureau SEP1C. Cette demande doit mentionner : - Le nom du serveur, - Sa localisation physique précise, - Son système d'exploitation, Pour les serveurs hébergés sur le site physique de Bercy, sa localisation réseau (Réseau Général ou DMZ), - Les adresses physiques (WWPN) de ses ports HBA.	Validé	03/09/2019	

Affectation d'une LUN à un serveur physique

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_3_4_4_011	Toute affectation d'un disque virtuel (LUN) à un serveur physique doit faire l'objet d'une demande à l'équipe d'exploitation stockage du bureau SEP1C. Cette demande doit mentionner : - Le nom du serveur, - Son système d'exploitation, - La justification technique du besoin, - Le type de données à stocker, - La volumétrie souhaitée, - Le niveau de performance en lecture/écriture nécessaire.	Validé	03/09/2019	
	1_3_4_4_012	La reconnaissance de la LUN par le système d'exploitation client et la configuration du système de fichiers sont de la responsabilité de l'exploitant du serveur.	Validé	03/09/2019	
	1_3_4_5_013	La volumétrie d'une LUN ne peut en aucun cas dépasser 50 To.	Validé	03/09/2019	

Agrandissement d'une LUN affectée à un serveur physique

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_3_4_4_021	Tout agrandissement d'une LUN affectée à un serveur physique doit faire l'objet d'une demande à l'équipe d'exploitation stockage du bureau SEP1C. Cette demande doit mentionner : - Le nom du serveur, - L'identifiant de la LUN (LUN ID) à agrandir, - La justification technique du besoin, - La volumétrie à ajouter.	Validé	03/09/2019	
	1_3_4_4_022	La prise en compte par le système d'exploitation client de l'augmentation de volumétrie de la LUN est de la responsabilité de l'exploitant du serveur.	Validé	03/09/2019	

Retrait d'une LUN d'un serveur physique

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_3_4_4_031	Tout retrait d'une LUN affectée à un serveur physique doit faire l'objet d'une demande à l'équipe d'exploitation stockage du bureau SEP1C. Cette demande doit mentionner : ▪ Le nom du serveur, ▪ L'identifiant de la LUN (LUN ID) à retirer.	Validé	03/09/2019	
	1_3_4_4_032	La LUN doit impérativement être démontée du système d'exploitation client du serveur avant l'opération de retrait. Cette manipulation est de la responsabilité de l'exploitant du serveur.	Validé	03/09/2019	

Espace de partage de fichiers NFS

Création d'un serveur de partage de fichiers NFS

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_3_4_5_001	Toute création d'un serveur de partage de fichiers NFS doit faire l'objet d'une demande à l'équipe d'exploitation stockage du bureau SEP1C. Cette demande doit mentionner : ▪ La justification technique du besoin, ▪ La localisation physique des clients, ▪ Leur localisation réseau.	Validé	03/09/2019	

Création d'un espace de partage de fichiers NFS

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_3_4_5_011	Toute création d'un espace de partage de fichiers NFS doit faire l'objet d'une demande à l'équipe d'exploitation stockage du bureau SEP1C. Cette demande doit mentionner : ▪ Le serveur de partage de fichiers à utiliser ou à défaut les clients de l'espace cible, ▪ La justification technique du besoin, ▪ La volumétrie souhaitée, ▪ Le type de données à stocker.	Validé	03/09/2019	

Modification de volumétrie d'un espace de partage de fichiers NFS

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_3_4_5_021	Toute modification de volumétrie d'un espace de partage de fichiers NFS existant doit faire l'objet d'une demande à l'équipe d'exploitation stockage du bureau SEP1C. Cette demande doit mentionner : ▪ Le chemin d'accès de l'espace de partage, ▪ La justification technique du besoin, ▪ La volumétrie à ajouter.	Validé	03/09/2019	
	1_3_4_5_022	La prise en compte de la modification de volumétrie par les clients est automatique. Elle ne nécessite aucune manipulation au niveau du système d'exploitation des clients.	Validé	03/09/2019	

Gestion des accès à un espace de partage de fichiers NFS

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_3_4_5_031	La liste des systèmes d'exploitation supportés en tant que clients d'un espace de partage de fichiers NFS est : ▪ RedHat Entreprise Linux (RHEL), ▪ CentOS, ▪ Suse Linux Entreprise Server (SLES), ▪ IBM AIX, ▪ HP UX, ▪ Solaris, ▪ VMware ESXi.	Validé	03/09/2019	
	1_3_4_5_032	Toute autorisation d'accès à un espace de partage de fichiers NFS par un client doit faire l'objet d'une demande à l'équipe d'exploitation stockage du bureau SEP1C. Cette demande doit mentionner : ▪ Le serveur de partage de fichiers concerné, ▪ Le chemin d'accès complet à l'espace de partage à accéder, ▪ L'adresse IP du client, ▪ L'identifiant numérique de l'utilisateur (UID) utilisé pour le montage côté client, ainsi que son groupe primaire (GID), ▪ Les droits d'accès souhaités (lecture seule ou lecture/écriture).	Validé	03/09/2019	
	1_3_4_5_033	Les éventuelles manipulations de configuration clientes nécessaires à l'accès à un espace de partage de fichiers NFS sont de la responsabilité de l'exploitant du client.	Validé	03/09/2019	
	1_3_4_5_034	L'éventuelle demande d'ouverture de flux nécessaire à l'accès au serveur de partage de fichiers est de la responsabilité de l'exploitant du client.	Validé	03/09/2019	
	1_3_4_5_035	Toute modification d'accès à un espace de partage de fichiers NFS doit faire l'objet d'une demande à l'équipe d'exploitation stockage du bureau SEP1C. Cette demande doit mentionner : ▪ Le serveur de partage concerné, ▪ Le chemin d'accès complet à l'espace de partage concerné, ▪ L'adresse IP du client, ▪ La nature de la modification d'accès (modification d'UID et/ou de GID, modification de droits d'accès, ...).	Validé	03/09/2019	
	1_3_4_5_036	Tout retrait d'un droit d'accès à un espace de partage de fichiers NFS doit faire l'objet d'une demande à l'équipe d'exploitation stockage du bureau SEP1C. Cette demande doit mentionner : ▪ Le serveur de partage concerné, ▪ Le chemin d'accès complet à l'espace de partage concerné, ▪ L'adresse IP du client.	Validé	03/09/2019	

Destruction d'un espace de partage de fichiers NFS

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_3_4_5_041	Toute destruction d'un espace de partage de fichiers NFS doit faire l'objet d'une demande à l'équipe d'exploitation stockage du bureau SEP1C. Cette demande doit mentionner : ▪ Le serveur de partage de fichiers concerné, ▪ Le chemin d'accès complet à l'espace de partage.	Validé	03/09/2019	
	1_3_4_5_042	L'espace de partage de fichiers doit être démonté de l'ensemble des clients avant sa destruction. Cette opération est de la responsabilité des exploitants des clients.	Validé	03/09/2019	

Espace de partage de fichiers CIFS

Création d'un serveur de partage CIFS

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_3_4_6_001	Toute création d'un serveur de partage de fichiers CIFS doit faire l'objet d'une demande à l'équipe d'exploitation stockage du bureau SEP1C. Cette demande doit mentionner : ▪ La justification technique du besoin, ▪ La localisation physique des clients, ▪ Leur localisation réseau, ▪ Leur domaine Active Directory d'appartenance.	Validé	03/09/2019	

Création d'un espace de partage de fichiers CIFS

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_3_4_6_011	Toute création d'un espace de partage de fichiers CIFS doit faire l'objet d'une demande à l'équipe d'exploitation stockage du bureau SEP1C. Cette demande doit mentionner : ▪ Le serveur de partage de fichiers à utiliser ou à défaut les clients de l'espace cible, ▪ La justification technique du besoin, ▪ La volumétrie souhaitée, ▪ Le type de données à stocker.	Validé	03/09/2019	

Modification de volumétrie d'un espace de partage de fichiers CIFS

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_3_4_6_021	La prise en compte de la modification de volumétrie par les clients est automatique. Elle ne nécessite aucune manipulation au niveau du système d'exploitation des clients.	Validé	03/09/2019	

Gestion des accès à un espace de partage de fichiers CIFS

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_3_4_6_031	L'accès à un espace de partage de fichiers CIFS est exclusivement réservé aux clients Windows membres d'un domaine Active Directory.	Validé	03/09/2019	
	1_3_4_6_032	Toute autorisation d'accès à un espace de partage de fichiers CIFS doit faire l'objet d'une demande à l'équipe d'exploitation stockage du bureau SEP1C. Cette demande doit mentionner : ▪ Le serveur de partage concerné, ▪ Le nom du partage, ▪ L'adresse IP du client, ▪ L'utilisateur ou le groupe AD devant être autorisé, ▪ Les droits d'accès souhaités (lecture seule, lecture/écriture ou contrôle total).	Validé	03/09/2019	
	1_3_4_6_033	L'éventuelle demande d'ouverture de flux nécessaire à l'accès à un espace de partage de fichiers CIFS est de la responsabilité de l'exploitant du client.	Validé	03/09/2019	
	1_3_4_6_034	Toute modification d'accès à un espace de partage de fichiers CIFS doit faire l'objet d'une demande à l'équipe d'exploitation stockage du bureau SEP1C. Cette demande doit mentionner : ▪ Le serveur de partage concerné, ▪ Le nom du partage, ▪ L'adresse IP du client concerné, ▪ La nature de la modification à effectuer (ajout/suppression d'un utilisateur ou d'un groupe AD, modification de droits d'accès, ...).	Validé	03/09/2019	
	1_3_4_6_035	Tout retrait d'un droit d'accès à un espace de partage de fichiers CIFS doit faire l'objet d'une demande à l'équipe d'exploitation stockage du bureau SEP1C. Cette demande doit mentionner : ▪ Le serveur de partage concerné, ▪ Le nom du partage, ▪ L'adresse IP du client concerné.	Validé	03/09/2019	

Destruction d'un espace de partage de fichiers CIFS

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_3_4_6_041	Toute destruction d'un espace de partage de fichiers CIFS doit faire l'objet d'une demande à l'équipe d'exploitation stockage du bureau SEP1C. Cette demande doit mentionner : ▪ Le serveur de partage concerné, ▪ Le nom du partage.	Validé	03/09/2019	
	1_3_4_6_042	Le partage de fichiers à supprimer doit être démonté de l'ensemble des clients avant sa suppression. Cette opération est de la responsabilité des exploitants des clients.	Validé	03/09/2019	

Maintenance des équipements de stockage

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_3_4_7_001	L'appel à la maintenance pour un équipement de stockage doit être réalisé par une équipe d'exploitation du bureau SEP1C, via la transmission au mainteneur d'un formulaire spécifique (https://documento.alize.finances.rie.gouv.fr/share/s/AXccAfuFSb2TN5KgROyMmw).	Validé	03/09/2019	

- La dernière modification de cette page a été faite le 18 février 2020 à 12:51.

Equipement de sauvegarde

La **sauvegarde** est l'opération qui consiste à dupliquer et à mettre en sécurité les données contenues dans un système informatique.

(Source : wikipedia,2020 (https://fr.wikipedia.org/wiki/Sauvegarde_(informatique)))

La **sauvegarde informatique** est une opération qui consiste à recopier un ou plusieurs fichiers de données, généralement sur un support externe, afin d'en prévenir la perte systématique ou accidentelle.

(source : Office québécois de la langue française,2002 (http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=2074332))

Terme privilégié : **sauvegarde informatique**, **sauvegarde**

Equivalent étranger: **data backup** (en), **backup** (en), **safeguard** (en), **saving** (en)

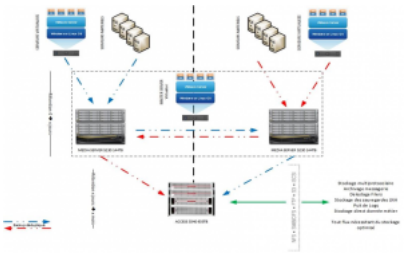
Sommaire

Contexte

Les offres de solution de sauvegarde et de restauration des données (serveurs) proposées par SEP1 s'appuient respectivement sur :

- des équipements de sauvegarde de la société **Veritas**
- le logiciel propriétaireNetBackup de la société ***Veritas***

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



Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_3_5_1_001	Les équipements de sauvegarde doivent être installés dans des versions à jour des correctifs de sécurité.	Validé	03/12/2019	
	1_3_5_1_002	Les flux techniques de sauvegarde doivent être acheminés via des liens réseaux dédiés.	Validé	03/09/2019	

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_3_5_2_001	Les équipements de sauvegarde de type Veritas Netbackup 5230 Appliance (https://www.symantec.com/content/en/us/enterprise/fact_sheets/b-netbackup_appliance_5230_DS_21273484-1.en-us.pdf) et Veritas Access 3340 Appliance (https://www.veritas.com/content/dam/Veritas/docs/data-sheets/V0594_GA_ENT_DS_Veritas-Access-3340-Appliance-EN.pdf) doivent être utilisés respectivement pour : - les sauvegardes à rétention courte (**maximum 7 jours**), - les sauvegardes à rétention longue (**maximum 60 jours**).	Validé	10/09/2020	Passage de 45 jours à 60 jours pour les sauveg à rétention longue.

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_3_5_3_001	L'acquisition des équipements de sauvegarde doit se faire au travers du marché " Fourniture d'éléments d'infrastructures informatiques (matériels, logiciels et prestations associées) en environnement X86 pour centres de données.	Validé	03/09/2019	
	1_3_5_3_002	La maintenance des équipements de sauvegarde doit se faire au travers du marché "Tierce maintenance des serveurs x86 et de solutions de sauvegarde ainsi que les prestations associées".	Validé	03/09/2019	Portail support VERITAS (https://www.verita support/en_US/article.100045773)

Contraintes techniques

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_3_5_4_001				

- La dernière modification de cette page a été faite le 7 décembre 2020 à 10:59.

Badgeuse

Une **badgeuse**, également appelée pointeuse ou timbreuse (en Suisse), est une machine qui permet d'enregistrer le temps de travail d'un salarié.

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

Termes privilégiés : **badgeuse**, **pointeuse**, **équipement de pointage**

Equivalent étranger: **timecard reader** (en), **badge reader** (en)

Sommaire

Contexte

Les offres de badgeuses proposées par SEP1 s'appuient sur les équipements de la marque **Pyrescom** .

Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_3_6_1_001				

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_3_6_2_001	Les badgeuses installées dans les bâtiments gérés par le secrétariat général des MEF doivent s'appuyer sur le modèle suivant : ▪ **PYRESCOM TERMOD 3**	Validé	22/01/2020	

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_3_6_3_001	L'acquisition des badgeuses doit se faire hors marché.	Validé	22/01/2020	
	1_3_6_3_002	La maintenance des badgeuses doit se faire hors marché via le service après-vente (ma ilto:mail:sav@pyres.com) de la société PYRESCOM.	Validé	10/09/2020	

Contraintes techniques

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_3_6_4_001				

- La dernière modification de cette page a été faite le 14 décembre 2020 à 12:40.

Commutateur KVM

Un **commutateur KVM** est un commutateur qui permet de partager clavier, écran et souris entre plusieurs ordinateurs.

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

Un **commutateur KVM** est un commutateur offrant la possibilité d'utiliser un seul ensemble de périphériques, formé d'un écran, d'un clavier et d'une souris, pour entrer et consulter des données dans plusieurs ordinateurs.

(source : Office québécois de la langue française, 2001 (http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8367753))

Termes privilégiés : **commutateur KVM**, **commutateur écran-clavier-souris**, **commutateur écran/clavier/souris**

Equivalent étranger: **KVM switch** (en), **keyboard-video-mouse switch** (en), **keyboard/video/mouse switch** (en)

Sommaire

Contexte

Les offres de commutateurs KVM proposées par SEP1 s'appuient sur les équipements de la marque **Dell**.

Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_3_7_1_001				

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_3_7_2_001	Les commutateurs KVM installés sur le centre de données d'Osny doivent être choisis parmi les modèles suivants : ▪ DELL KVM DMPU2016-G01 (https://www.dell.com/fr-fr/shop/commutateur-dell-kvm-dmpu2016-g01à-distance-à-16-ports-avec-deux-utilisateurs-à-distance-un-utilisateur-local-et-deux-blocs-d-alimentation/apd/a7485893/mise-en-réseau)	Validé	22/01/2020	

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_3_7_3_001				

Contraintes techniques

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_3_7_4_001				

- La dernière modification de cette page a été faite le 8 juin 2020 à 22:00.

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 applicatif.

(source : wikipedia,2020 (https://fr.wikipedia.org/wiki/Syst%C3%A8me_d%27exploitation))

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'entrée-sortie 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

Contexte

Les offres de systèmes d'exploitation serveur proposées par SEP1 s'appuient 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.

Certains serveurs Linux à vocation applicative et technique peuvent nécessiter l'usage du logiciel propriétaire **Red Hat Enterprise Linux (RHEL)**. C'est le cas notamment pour les serveurs physiques hébergeant les systèmes de bases de données SGBD (ORACLE) ou encore la solution de sauvegarde VERITAS Netbackup

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	**CentOS 7.9** CERTFR-2020-ALE-020 (https://www.cert.ss fr/alerte/CERTFR-2020-ALE-020/) CERTFR-2020-AVI-807 (https://www.cert.ssi r/avis/CERTFR-2020-AVI-807/) **Microsoft Windows**

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** doit être utilisée pour : ▪ les nouveaux serveurs à vocation technique, ▪ les nouveaux serveurs à vocation applicative.	Validé	18/05/2020	Dates de fin de support CentOS (https://wiki. 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 : ▪ les nouveaux serveurs à vocation applicative nécessitant l'utilisation de cette distribution.	Validé	30/09/2019	Dates de fin de support full RHEL (https://ac dhat.com/support/policy/updates/errata) : - **RHEL 7** : 06/08/2019 Dates de fin de support 1 et 2 RHEL (https:// redhat.com/support/policy/updates/errata) : - **RHEL 7** : 06/08/2020 - 30/06/2024 Date de fin de support étendu RHEL (https:// 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 : ▪ 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.co r/lifecycle/search) : - **Windows Server 2016** :11/01/2022 Dates de fin de support étendu MIcrosoft Wir Server (https://support.microsoft.com/fr-fr/lif 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://doc o.alize.finances.rie.gouv.fr/share/page/site/sep document-details?nodeRef=workspace://Spac e/120d763d-b5f5-41f1-b042-6319e53d30af) **Noyau CentOS 3.10** Portail support Linagora (https://sll.08000linu m/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.co work/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.pre 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 : ▪ 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 : ▪ 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 : ▪ 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				

- La dernière modification de cette page a été faite le 14 décembre 2020 à 17:53.

Serveur virtuel

Un **serveur virtuel** est une méthode de partitionnement d'un serveur en plusieurs serveurs virtuels indépendants qui ont chacun les caractéristiques d'un serveur dédié, en utilisant des techniques de virtualisation. Chaque serveur peut fonctionner avec un système d'exploitation différent et redémarrer indépendamment.

(source : wikipedia,2020 (https://fr.wikipedia.org/wiki/Serveur_d%C3%A9di%C3%A9_virtuel))

Un **serveur virtuel** est un serveur Internet possédant plusieurs adresses IP associées à la même carte réseau. (source : Office québécois de la langue française, 1999 (http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8374456))

Terme privilégié : **serveur virtuel**

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

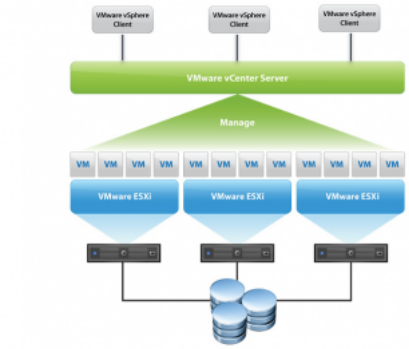
Sommaire

Contexte

Les offres de serveurs virtuels proposées par SEP1 s'appuient sur le logiciel propriétaire **VMware vSphere** composé de :

- du serveur de virtualisation ESXi,
- du serveur vCenter,
- du client vSphere.

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



Source : Plateforme de virtualisation VMware vSphere (https://docs.vmware.com/fr/VMware-vSphere/index.html)

Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_4_2_1_001	Toute demande de serveur virtuel doit être accompagnée : ▪ d'une demande de ressources, ▪ d'un dossier d'architecture technique (DAT) (https://documento.alize.finances.rie.gouv.fr/share/s/TuQwZJ-qQcqHp0AlnUgiug).	Validé	03/09/2019	
	1_4_2_1_002	L'installation des nouvelles applications sur des serveurs virtuels doit être privilégiée par rapport aux serveurs physiques.	Validé	01/07/2019	
	1_4_2_1_003	Les serveurs virtuels doivent être installés dans des versions à jour des correctifs de sécurité.	Validé	03/09/2019	CERTFR-2020-AVI-767 (https://www.cert.ssi.gouv.fr/avis/CERTFR-2020-AVI-767/) **ESXi670-202011101-SG**

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_4_2_2_001	La suite logicielle **VMware vSphere 6.7** doit être utilisée pour les nouveaux serveurs virtuels installés sur le centre de données d'Osny.	Validé	03/09/2019	Dates de fin de support (https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/support/product-lifecycle-matrix.pdf) : **VMware vSphere 6.7** : 15/11/2021

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_4_2_3_001	Toute demande d'acquisition de licences et de support sur le logiciel propriétaire VMware vSphere doit se faire auprès 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	03/09/2019	

Contraintes techniques

Caractéristiques techniques

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_4_2_4_001	Les serveurs virtuels à vocation applicative localisés sur le centre de données d'Osny doivent disposer de 3 interfaces réseaux : ▪ 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_4_2_4_002	Les serveurs virtuels à vocation technique localisés sur lecentre de données d'Osny doivent disposer de 2 interfaces réseaux : ▪ 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_4_2_4_003	La configuration CPU et RAM 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 : ▪ CPU : 1, 2, 4 ou 8 vCPU ▪ RAM : 1,2, 4, 6, 8, 10, 12, 14 ou 16 Go L'extension des ressources matérielles au delà des valeurs ci-dessus doit faire l'objet d'une justification technique.	Validé	01/07/2019	
	1_4_2_4_004	Les ressources attribuées à un serveur virtuel ne doivent pas être réutilisées pour d'autres besoins.	Validé	01/07/2019	

Installation des serveurs virtuels

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_4_2_5_001				

Mise à jour des serveurs virtuels

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_4_2_6_001	La demande de modification des ressources (CPU, RAM, interface réseau, espace disque) d'un serveur virtuel doit faire l'objet d'une justification technique.	Validé	01/07/2019	

Administration et exploitation des serveurs virtuels

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_4_2_7_001				

Décommissionnement des serveurs virtuels

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	1_4_2_8_001	Le décommissionnement d'un serveur virtuel doit préciser les informations suivantes : ▪ le nom du serveur virtuel, ▪ l'infrastructure de virtualisation sur lequel il est hébergé, ▪ l'ensemble de ces adresses IP.	Validé	01/07/2019	

Règles de nommage des serveurs virtuels

<table>
<tr><th></th><th>Identifiant</th><th>Libellé de la règle</th><th>Statut</th><th>Date d'effet</th><th>Commentaires</th></tr>
<tr><td></td><td>1_4_2_9_001</td><td>Les serveurs virtuels localisés sur le centre de données d'Osny doivent respecter les règles de nommage suivantes :
<table><tr><th>Type de serveur</th><th>Règle de nommage</th></tr><tr><td>Serveur "clone"</td><td>VVC-[NOM-APPLI]</td></tr><tr><td>Serveur de développement</td><td>VVD-[NOM-APPLI]</td></tr><tr><td>Serveur de recette</td><td>VVR-[NOM-APPLI]-[SUFFIXE]</td></tr><tr><td>Serveur de formation</td><td>VVF-[NOM-APPLI]</td></tr><tr><td>Serveur de test</td><td>VVT-[NOM-APPLI]</td></tr><tr><td>Serveur de pré-production</td><td>VVPP-[NOM-APPLI]-[SUFFIXE]</td></tr><tr><td>Serveur de production</td><td>VVP-[NOM-APPLI]-[SUFFIXE]</td></tr></table>
où [NOM-APPLI] est le nom de l'application en majuscule sans l'usage du caractère "_".
où [SUFFIXE] est le type de serveur (WEB, APP, BDD, IDX).</td><td>Validé</td><td>01/07/2019</td><td></td></tr>
</table>

- La dernière modification de cette page a été faite le 20 novembre 2020 à 17:22.

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'entrée-sortie 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

Contexte

Les offres de systèmes d'exploitation postes de travail et proposées par SEP1 s'appuient sur le logiciel propriétaire **Microsoft Windows 10**.

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	CERTFR-2020-AVI-807 (https://www.cert.ssi.gouv.fr/avis/CERTFR-2020-AVI-807/) **Windows 10 version 1909**
	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 SEP1D-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 7 32 bits Service Pack 1 (jusqu'au 14/01/2020), - Microsoft Windows 7 64 bits Service Pack 1 (jusqu'au 14/01/2020), - Microsoft Windows 10 Professionnel 64 bits, - Microsoft Windows 10 Entreprise LTSC 2016 64 bits.	Validé	03/09/2019	Date de fin de support (https://support.microsoft.com/fr-fr/help/13853/windows-lifecycle-fact-sheet) : **Windows 7** : 14 janvier 2020

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_001~~	~~Les postes de travail déployés en Administration Centrale doivent être installés à partir d'un master.~~	Obsolète	23/09/2019	
	~~1_4_3_6_002~~	~~Les masters des postes de travail qui regroupent les principaux paramétrages du système d'exploitation ainsi que les logiciels du socle doivent être réalisés par l'équipe SEPID - TCMP.~~	Obsolète	23/09/2019	
	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 LTSB, 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	

- La dernière modification de cette page a été faite le 11 décembre 2020 à 15:17.

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. (Source : SEP1)

Termes privilégiés :**poste de rebond virtuel, VPR**

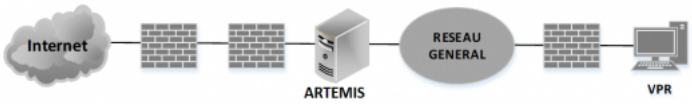
Equivalent étranger:

Sommaire

Contexte

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

L'architecture 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
Nouveauté	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
Nouveauté	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 ontent/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
Nouveauté	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	
Nouveauté	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	
Nouveauté	1_4_4_4_003	Chaque société prestataire peut disposer d'un seul poste de rebond virtuel (VPR).	Validé	18/05/2020	
Nouveauté	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	

- La dernière modification de cette page a été faite le 17 juin 2020 à 14:25.

Poste d'administration virtuel (VPC)

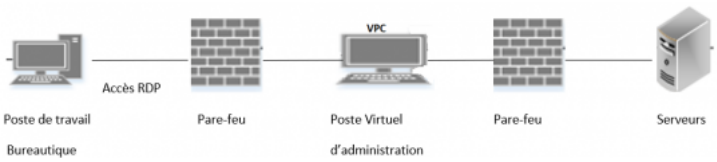
Le **poste d'administration virtuel (VPC)** est un poste de travail virtuel permettant de réaliser des tâches d'exploitation et d'administration informatique. (source : SEP1)

Sommaire

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
Nouveauté	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
Nouveauté	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 ontent/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
Nouveauté	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
Nouveauté	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	

- La dernière modification de cette page a été faite le 7 décembre 2020 à 14:57.

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, librairies, 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,2020 (https://fr.wikipedia.org/wiki/Conteneur_(informatique)))

Un **conteneur** est en programmation orientée objet, un espace de référence dans lequel on dépose et on assemble des composants logiciels qui peuvent ainsi y interagir, et qui sert de moule pour créer des applications. . (source : Office québécois de la langue française, 2004 (http://http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8875587))

Terme privilégié :**conteneur**

Equivalent étranger: **container** (en)

Sommaire

Contexte

Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
Nouvelle règle	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 12 juillet 2020 à 06:55.

Chiffrement de flux

Le **chiffrement** (ou cryptage) 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,2020 (https://fr.wikipedia.org/wiki/Chiffrement))

Le **chiffrement** est l'opération par laquelle est substitué, à un texte en clair, un texte inintelligible, inexploitable pour quiconque ne possède pas la clé permettant de le ramener à sa forme initiale.

(source : Office québécois de la langue française, 2011 (http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8387607))

Termes privilégiés : **chiffrement**, **cryptage**

Equivalent anglais: **encryption** (en), **encipherment** (en), **enciphering** (en), **ciphering** (en)

Sommaire

Contexte

Les offres de chiffrement de flux proposées par SEP1 s'appuient sur le logiciel libre **OpenSSL**.

Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_1_2_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	CERTFR-2020-AVI-803 (https://www.cert.ssi r/avis/CERTFR-2020-AVI-803/) OpenSSL 1.0.2

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_1_2_2_001	Le logiciel libre **OpenSSL 1.0.2 (LTS)** doit être utilisé pour la solution de chiffrement.	Validé	03/09/2019	Dates de fin de support (https://www.openssl. icies/releasestrat.html) : **- OpenSSL 1.0.2 (LTS)** : 31/12/2019 sauf contrat de support spécifique.

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 OpenSSL doit se faire au travers du marché "Support à l'usage des logiciels libres" (SLL).	Validé	03/09/2019	Versions OpenSSL supportées (https://docum ize.finances.rie.gouv.fr/share/page/site/sep1-c ument-details?nodeRef=workspace://SpacesS 0d763d-b5f5-41f1-b042-6319e53d30af) **OpenSSL 1.0** Portail support (https://www.otrs.aosc-portal.c rs/customer.pl)

Contraintes techniques

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_1_2_4_001	Le logiciel libre OpenSSL doit être installé à partir du serveur de dépôt interne Linux.	Validé	03/09/2019	

- La dernière modification de cette page a été faite le 9 décembre 2020 à 16:36.

Serveur d'authentification unique (SSO)

L'**authentification** est une procédure consistant à vérifier ou à valider l'identité d'une personne ou l'identification de toute autre entité, lors d'un échange électronique, pour contrôler l'accès à un réseau, à un système informatique ou à un logiciel.

(source :Office québécois de la langue française, 2003 (http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8374339))

L'**authentification unique** est une solution logicielle basée sur un annuaire, qui permet aux utilisateurs d'un réseau d'entreprise d'accéder, en toute transparence, à l'ensemble des ressources autorisées, sur la base d'une authentification unique effectuée lors de l'accès initial au réseau.

(source : Office québécois de la langue française, 2001 (http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8368235))

Termes privilégiés : **signature unique**, **authentification unique**

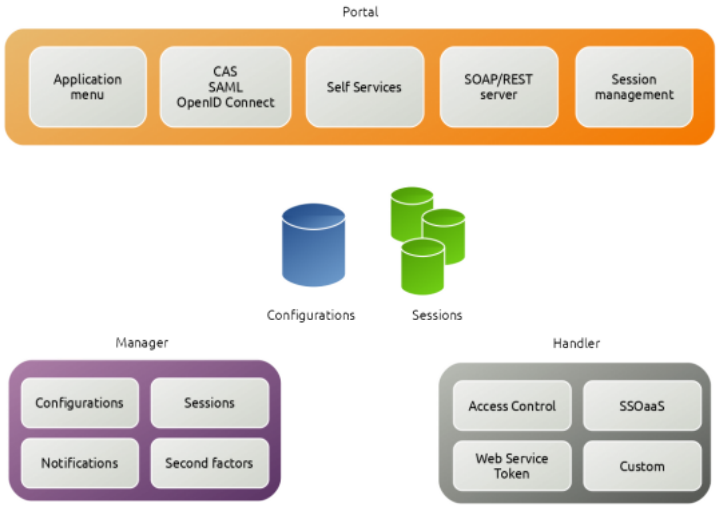
Equivalent anglais: **single sign-on** (en), **SSO** (en)

Sommaire

Contexte

Les offres de serveurs d'authentification unique proposées par SEP1 s'appuient sur le logiciel libre **LemonLDAP::NG**.

L'architecture technique du serveur d'authentification unique LemonLDAP::NG se décline de la manière suivante :



(Source : Site officiel LemonLDAP::NG (https://lemonldap-ng.org/documentation/presentation))

SEP1 propose trois systèmes d'authentification unique (SSO) :

- Le **SSO RG** à destination des utilisateurs du réseau général (RG).
- Le **SSO RIE** à destination des utilisateurs du réseau interministériel de l'Etat (RIE).
- Le **SSO WEB** à destination des utilisateurs du réseau internet,

Les serveurs d'authentification unique SSO de l'administration centrale sont connectés aux annuaires Anaïs et / ou Angie selon les SSO auxquels l'application est raccordée.

L'annuaire Angie couvre la population de l'administration centrale ayant une BAL dans l'annuaire Active-Directory Solano et les comptes externes parrainés uniquement par les agents d'administration centrale.

Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_1_1_1_001	Les nouvelles 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%a8mes%20d'information/documents/Textes%20de%20r%c3%a9f%c3%a9rences/180503_authentification-mdp_v3.1.pdf).	Validé	01/07/2019	
	2_1_1_1_002	Les nouvelles applications doivent s'interfacer avec les serveurs d'authentification unique (SSO).	Validé	01/07/2019	En lien avec la règle 2_1_1_1_003
	2_1_1_1_003	Les nouvelles 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	En lien avec la règle 2_1_1_1_002
	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	
	2_1_1_1_005	Les serveurs d'authentification unique (SSO) doivent respecter les règles décrites dans le Guide de paramétrage SSL et entête HTTP (https://documento.alize.finances.rie.gouv.fr/share/s/C0lP3D2IQpu-9pXX31mdLA).	Validé	22/01/2020	source : SEP1C/PSSI

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 1.9.19**.	Validé	01/07/2019	Site officiel LemonLDAP::NG (https://lemong.org/welcome/)

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 marché "Support à l'usage des logiciels libres" (SLL).	Validé	01/07/2019	Versions supportées au SLL (https://document.finances.rie.gouv.fr/share/page/site/sep1-cct/document-details?nodeRef=workspace://SpacesStore/d763d-b5f5-41f1-b042-6319e53d30af) **LemonLDAP::NG 1.9** Portail SLL (https://www.otrs.aosc-portal.com/customer.pl)

Contraintes techniques

Protocoles d'authentification

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_1_1_4_001	Les nouvelles applications interfacées avec les serveurs d'authentification unique (SSO) doivent utiliser l'un des protocoles d'authentification suivants : ▪ Protocole Kerberos (https://fr.wikipedia.org/wiki/Kerberos_(protocole)) (authentification sur l'annuaire SOLANO) ▪ Protocole LDAP (https://fr.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol) (authentification sur les annuaires ANAIS et ANGIE) ▪ Protocole SSL (https://fr.wikipedia.org/wiki/Transport_Layer_Security) (authentification par certificat client) ▪ Protocole SAML (https://fr.wikipedia.org/wiki/Security_assertion_markup_language) ▪ Protocole OpenID Connect (https://fr.wikipedia.org/wiki/OpenID_Connect)	Validé	01/07/2019	

Règles de nommage des URL

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_1_1_5_001	Les nouvelles applications interfacées avec les serveurs d'authentification unique (SSO RG) doivent utiliser les règles de nommage des URL suivantes : **Environnement de développement** URL https://[nom_application].dev.monalize.alize redirigée vers : URL https://[nom_application]-dev-bo.alize.finances.rie.gouv.fr **Environnement de recette** URL https://[nom_application].monalizeitg.alize redirigée vers : URL https://[nom_application]-rec-bo.alize.finances.rie.gouv.fr **Environnement de production** URL https://[nom_application].monportail.alize redirigée vers : URL https://[nom_application]-bo.alize.finances.rie.gouv.fr où [nom_application] est le nom de l'application.	Validé	01/07/2019	
	2_1_1_5_002	Les nouvelles applications interfacées avec les serveurs d'authentification unique (SSO RIE) doivent utiliser les règles suivantes de nommage des URL : **Environnement de développement** URL https://[nom_application].dev.monportail.alize.finances.rie.gouv.fr redirigée vers : URL https://[nom_application]-dev-bo.alize.finances.rie.gouv.fr **Environnement de recette** URL https://[nom_application].itg.monportail.alize.finances.rie.gouv.fr redirigée vers : URL https://[nom_application]-rec-bo.alize.finances.rie.gouv.fr **Environnement de production** URL https://[nom_application].monportail.alize.finances.rie.gouv.fr redirigée vers : URL https://[nom_application]-bo.alize.finances.rie.gouv.fr où [nom_application] est le nom de l'application.	Validé	01/07/2019	
	2_1_1_5_003	Les nouvelles applications interfacées avec les serveurs d'authentification unique (SSO WEB) doivent utiliser les règles suivantes de nommage des URL : **Environnement de recette** URL https://[nom_application].itg.finances.gouv.fr redirigée vers : URL https://[nom_application]-rec-bo.finances.gouv.fr **Environnement de production** URL https://[nom_application].finances.gouv.fr redirigée vers : URL https://[nom_application]-bo.finances.gouv.fr où [nom_application] est le nom de l'application.	Validé	01/07/2019	
	2_1_1_5_004	Les nouvelles [[Glossaire#Application|applications] interfacées avec les serveurs d'authentification unique (SSO DGFIP) doivent utiliser les règles de nommage des URL suivantes : **Environnement de production** URL https://[nom_application].appli.impots/[nom_application] redirigée vers : URL https://[nom_application]-bo.alize.finances.rie.gouv.fr où [nom_application] est le nom de l'application.	Validé	01/07/2019	

Chaînage des méthodes d'authentification

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_1_1_6_001	Les méthodes d'authentification du système d'authentification unique (SSO RG) doivent être chaînées de la manière suivante : ▪ Kerberos ▪ LDAP (Annuaire Anaïs Centrale) si la méthode d'authentification Kerberos a échoué.	Validé	03/12/2019	
	2_1_1_6_002	Les méthodes d'authentification du système d'authentification unique (SSO RIE) doivent être chaînées de la manière suivante : ▪ LDAP (Annuaire Anais Centrale) ▪ LDAP (Annuaire Angie) si la méthode d'authentification LDAP (Annuaire Anaïs Centrale) a échoué.	Validé	03/12/2019	
	2_1_1_6_003	Les méthodes d'authentification du système d'authentification unique (SSO Web) doivent être chaînées de la manière suivante : ▪ SSL avec certificat client ▪ LDAP (Annuaire Angie) si la méthode d'authentification SSL a échoué.	Validé	03/12/2019	

Framework d'authentification

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_1_1_7_001	Toute application mettant en oeuvre une solution d'authentification unique (SSO) de l'administration centrale, doit : ▪ Utiliser les frameworks existants, à savoir : ▪ 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 : ▪ 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 suivant : KERBEROS, SA France Connect

Stratégie de sécurité des contenus

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_1_1_8_001	Les stratégies de sécurité des contenus (CSP) spécifiées dans le "Guide de paramétrage SSL et entête HTTP" doivent être appliquées sur les SSO telles que rédigées dans le fichier "sep1c-pssi-1.2-B de reference.conf".	Validé	03/12/2020	
	2_1_1_8_002	La règle 2_1_1_8_001 ne s'applique pas aux applications intranet : sont toujours acceptées des non-conformités de type default-src 'self' ou équivalent comme script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'.	Validé	03/12/2020	
	2_1_1_8_003	Les stratégies de sécurité des contenus (CSP) spécifiées dans le "Guide de paramétrage SSL et entête HTTP" étant appliquées sur les SSO, ne doivent pas être appliquées sur les serveurs web hébergeant les applications.	Validé	03/12/2020	

- La dernière modification de cette page a été faite le 14 décembre 2020 à 12:49.

Protection antivirus des postes de travail

Les **antivirus** sont des logiciels conçus pour identifier, neutraliser et éliminer des logiciels malveillants (dont les virus informatique1 ne sont qu'une catégorie.

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

Un **logiciel antivirus** est un logiciel de sécurité qui procède, automatiquement ou sur demande, à l'analyse des fichiers et de la mémoire d'un ordinateur, soit pour empêcher toute introduction parasite, soit pour détecter et éradiquer tout virus dans un système informatique.

(source : Office québécois de la langue française, 2005 (http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8869443))

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

Contexte

Les offres de protection antivirus des postes de travail proposées par SEP1 s'appuient sur le logiciel propriétaire **Symantec Endpoint Security**.

Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_1_3_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	

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_1_3_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 console Symantec.

Contraintes juridiques et réglementaires

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

Contraintes techniques

<table>
<tr><th></th><th>Identifiant</th><th>Libellé de la règle</th><th>Statut</th><th>Date d'effet</th><th>Commentaires</th></tr>
<tr><td></td><td>2_1_3_4_001</td><td>L'application des correctifs de sécurité Microsoft mensuels doit s'effectuer selon le rythme suivant :<table><tr><th>Calendrier</th><th>Rythme mensuel normal</th></tr><tr><td>Jour J</td><td>Réception des correctifs de sécurité.</td></tr><tr><td>J+7</td><td>Publication des correctifs de sécurité sur les postes de test du secteur SEP1D TCMP (Télédistribution Copieur Master Protection).</td></tr><tr><td>J+8</td><td>Publication des correctifs de sécurité sur les groupes de recette.</td></tr><tr><td>J+15</td><td>GoNogo de publication générale des correctifs de sécurité.</td></tr><tr><td>J+16</td><td>Publication générale des correctifs de sécurité.</td></tr></table></td><td>Validé</td><td>03/12/2019</td><td></td></tr>
<tr><td></td><td>2_1_3_4_002</td><td>L'application des correctifs de sécurité Microsoft urgents doit s'effectuer selon le rythme suivant :<table><tr><th>Calendrier</th><th>Rythme d'urgence</th></tr><tr><td>Jour J</td><td>Réception des correctifs de sécurité.
Publication des correctifs sur les postes de test du secteur SEP1D TCMP (Télédistribution Copieur Master Protection).</td></tr><tr><td>J+3</td><td>Publication des correctifs de sécurité sur les groupes de recette.</td></tr><tr><td>J+8</td><td>GoNogo de publication générale des correctifs de sécurité.</td></tr></table></td><td>Validé</td><td>03/12/2019</td><td></td></tr>
</table>

- La dernière modification de cette page a été faite le 17 février 2020 à 18:27.

Protection antipourriel des serveurs

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.

(source : Office québécois de la langue française, 2012 (http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8349831)

Un **filtre antipourriel** est un logiciel qui, selon des règles de filtrage prédéfinies, analyse le contenu des courriels reçus, détecte les pourriels et les déplace automatiquement dans un dossier spécifique ou les supprime sur le serveur de messagerie avant réception.

(source : Office québécois de la langue française, 2008 (http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=35314)

Termes privilégiés : **pourriel**, **courriel non sollicité**, **courriel indésirable**

Equivalent étranger: **spam** (en), **spam message** (en), **e-mail spam** (en)

Sommaire

Contexte

Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_1_4_1_001				

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_1_4_2_001	Les serveurs de relais de messagerie (internes) doivent s'appuyer sur le logiciel libre **SpamAssassin 3.4.0-4.**	Validé	03/12/2019	
	2_1_4_2_002	Les serveurs de relais de messagerie (internes) doivent s'appuyer sur le logiciel libre **Amavis 2.11.1-1**.	Validé	03/12/2019	
	2_1_4_2_003	Les serveurs de messagerie doivent s'appuyer sur le logiciel propriétaire **Scanmail for Microsoft Exchange 12.5 SP1** 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_4_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	Version supportée au SLL (https://documento inances.rie.gouv.fr/share/page/site/sep1-cct/d nt-details?nodeRef=workspace://SpacesStore/ 63d-b5f5-41f1-b042-6319e53d30af) **SpamAssassin 3.4** Portail support Linagora (https://sll.08000linu m/otrs/customer.pl)
	2_1_4_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	Version supportée au SLL (https://documento inances.rie.gouv.fr/share/page/site/sep1-cct/d nt-details?nodeRef=workspace://SpacesStore/ 63d-b5f5-41f1-b042-6319e53d30af) **Amavis 2.11** Portail support Linagora (https://sll.08000linu m/otrs/customer.pl)
	2_1_4_3_003	Toute demande de support sur le logiciel propriétaire Scanmail doit se faire au travers du marché "multi-éditeurs".	Validé	03/12/2019	Portail support Trend Micro

Contraintes techniques

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_1_4_4_001				

- La dernière modification de cette page a été faite le 17 février 2020 à 19:37.

Serveur mandataire inverse (SMI)

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

Terme privilégié : **serveur mandataire inverse**, **serveur frontal mutualisé**

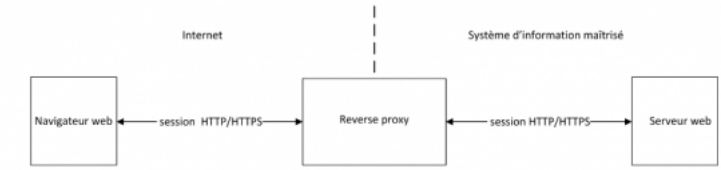
Equivalent étranger : **reverse proxy server** (en), **reverse proxy** (en)

Sommaire

Contexte

Les offres de serveurs mandataires inverses (SMI) proposées par SEP1 s'appuient sur le logiciel libre **Apache**.

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



(source : Note technique ANSSI (https://www.ssi.gouv.fr/uploads/IMG/pdf/NP_TLS_NoteTech.pdf))Les serveurs mandataires inverses (SMI) sont respectivement situés :

- sur le RG du centre de données de Bercy
- dans la DMZ Web du centre de données de Bercy
- dans la DMZ Frontale du centre de données d'Osny

Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_1_5_1_001	Les nouvelles 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_5_1_002	Les serveurs mandataires inverses doivent être installés dans des versions à jour des correctifs de sécurité.	Validé	22/01/2020	CERTFR-2020-AVI-490 (https://www.cert.ss r/avis/CERTFR-2020-AVI-490/): **Apache 2.4.46**
	2_1_5_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/C0lP3D2IQpu-9pXX31mdLA).	Validé	22/01/2020	source : SEP1C/PSSI

Solutions de référence

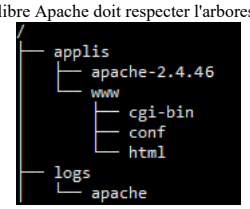
	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_1_5_2_001	Les serveurs mandataires inverses doivent s'appuyer sur le logiciel libre **Apache 2.4**	Validé	22/01/2020	Dates de fin de support (https://httpd.apache.c **Apache 2.4** : - Version non supportée (https://httpd.apache.o **Apache 2.2**

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 libre Apache doit se faire au travers du marché "Support à l'usage des logiciels libres".	Validé	22/01/2020	Versions supportées au SLL (https://document e.finances.rie.gouv.fr/share/page/site/sep1-cct ment-details?nodeRef=workspace://SpacesSto 0d763d-b5f5-41f1-b042-6319e53d30af) : **Apache 2.4** Portail SLL (https://www.otrs.aosc-portal.com ustomer.pl)

Contraintes techniques

Installation des serveurs mandataires inverses

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_1_5_4_001	L'installation des serveurs mandataires inverses basés sur le logiciel libre Apache doit être réalisée à partir du script interne "build-httpd-frontal".	Validé	22/01/2020	
	2_1_5_4_002	L'installation du logiciel libre Apache 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	22/01/2020	

Montée de version des serveurs mandataires inverses

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_1_5_5_002				

Administration et exploitation des serveurs mandataires inverses

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_1_5_6_001	Les droits et les permissions qui s'appliquent aux répertoires et aux fichiers des serveurs mandataires inverses doivent respecter les propriétés suivantes : ▪ Les répertoires doivent avoir des droits positionnés en 755 avec comme propriétaire "root" et groupe "root". ▪ Les fichiers doivent avoir des droits positionnées en 644 avec propriétaire "root" et groupe "root".	Validé	22/01/2020	
	2_1_5_6_002	Les droits et les permissions qui s'appliquent aux répertoires et aux fichiers des serveurs mandataires inverses dans lesquels l'application a besoin d'écrire doivent respecter les propriétés suivantes : ▪ Les répertoires doivent avoir des droits positionnés en 775 avec comme propriétaire "root" et groupe "apache" ▪ Les fichiers doivent avoir des droits positionnés en 664 avec comme propriétaire "root" et groupe "apache"	Validé	22/01/2020	
	2_1_5_6_003	La racine des documents (DocumentRoot) doit être située dans le répertoire /applis/www/html/[nom_application] où [nom_application] est le nom de l'application web.	Validé	22/01/2020	
	2_1_5_6_004	La création de serveurs virtuels (VirtualHost) doit se faire à partir du fichier exemple /applis/extra/httpd-vhost-[nom_application].MODELE où [nom_application] est le nom de l'application web. Une fois finalisé, ce fichier doit être renommé en /applis/extra/httpd-vhost-[nom_application].conf où [nom_application] est le nom de l'application web.	Validé	22/01/2020	
	2_1_5_6_005	Les fichiers log du serveur mandataires inverses doivent être situés dans le répertoire /logs/apache	Validé	22/01/2020	

Règles de nommage des URL des serveurs mandataires inverses

<table>
<tr><th></th><th>Identifiant</th><th>Libellé de la règle</th><th>Statut</th><th>Date d'effet</th><th>Commentaires</th></tr>
<tr><td></td><td>2_1_5_7_001</td><td>Les nouvelles applications exposées sur :
le réseau général (RG)
le réseau interministériel de l'Etat (RIE)
et interfacées avec les serveurs mandataires inverses doivent utiliser les règles de nommage des URL suivantes :
Environnement de développement<table><tr><td>URL</td><td>https://[nom_application]-dev.alize.finances.rie.gouv.fr</td></tr><tr><td colspan="2">redirigée vers :</td></tr><tr><td>URL</td><td>https://[nom_application]-dev-bo.alize.finances.rie.gouv.fr</td></tr></table>Environnement de recette<table><tr><td>URL</td><td>https://[nom_application]-rec.alize.finances.rie.gouv.fr</td></tr><tr><td colspan="2">redirigée vers :</td></tr><tr><td>URL</td><td>https://[nom_application]-rec-bo.alize.finances.rie.gouv.fr</td></tr></table>Environnement de production<table><tr><td>URL</td><td>https://[nom_application].alize.finances.rie.gouv.fr</td></tr><tr><td colspan="2">redirigée vers :</td></tr><tr><td>URL</td><td>https://[nom_application]-bo.alize.finances.rie.gouv.fr</td></tr></table>où [nom_application] est le nom de l'application.</td><td>Validé</td><td>08/07/2020</td><td>Modification du préfixe -itg en -rec</td></tr>
<tr><td></td><td>2_1_5_7_002</td><td>Les nouvelles applications exposées sur :
le réseau internet
et interfacées avec les serveurs mandataires inverses doivent utiliser les règles de nommage des URL suivantes :
Environnement de développement<table><tr><td>URL</td><td>https://[nom_application]-dev.alize.finances.rie.gouv.fr</td></tr><tr><td colspan="2">redirigée vers :</td></tr><tr><td>URL</td><td>https://[nom_application]-dev-bo.alize.finances.rie.gouv.fr</td></tr></table>Environnement de recette<table><tr><td>URL</td><td>https://[nom_application]-rec.finances.gouv.fr</td></tr><tr><td colspan="2">redirigée vers :</td></tr><tr><td>URL</td><td>https://[nom_application]-rec-bo.finances.gouv.fr</td></tr></table>Environnement de production<table><tr><td>URL</td><td>https://[nom_application].finances.gouv.fr</td></tr><tr><td colspan="2">redirigée vers :</td></tr><tr><td>URL</td><td>https://[nom_application]-bo.finances.gouv.fr</td></tr></table></td><td>Validé</td><td>08/07/2020</td><td>Modification du préfixe -itg en -rec</td></tr>
</table>

Stratégie de sécurité des contenus

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_1_5_8_001	Les stratégies de sécurité des contenus (CSP) spécifiées dans le "Guide de paramétrage SSL et entête HTTP" doivent être appliquées sur les SMI telles que rédigées dans le fichier "sep1c-pssi-1.2-B de reference.conf".	Validé	03/12/2020	
	2_1_5_8_003	La règle 2_1_5_8_001 ne s'applique pas aux applications intranet : sont toujours acceptées des non-conformités de type default-src 'self' ou équivalent comme script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'.	Validé	03/12/2020	
	2_1_5_8_003	Les stratégies de sécurité des contenus (CSP) spécifiées dans le "Guide de paramétrage SSL et entête HTTP" étant appliquées sur les SMI, ne doivent pas être appliquées sur les serveurs web hébergeant les applications.	Validé	03/12/2020	

- La dernière modification de cette page a été faite le 7 décembre 2020 à 13:23.

Scanner de vulnérabilité

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

(source : wikipedia,2020 (https://fr.wikipedia.org/wiki/Scanneur_de_vuln%C3%A9rabilit%C3%A9))

Une **vulnérabilité informatique** est une faiblesse d'un système informatique se traduisant par une incapacité partielle de celui-ci à faire face aux attaques ou aux intrusions informatiques.

(source : Office québécois de la langue française, 2017 (http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8354651))

Termes privilégiés : **scanner de vulnérabilité**,

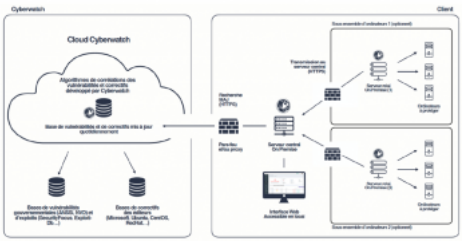
Equivalent étranger: **vulnerability scanner** (en)

Sommaire

Contexte

Les offres de scanners de vulnérabilité proposées par SEP1 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) 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 Vulnerabiity 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.

Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_1_6_1_001	Tous les serveurs doivent être intégrés dans le logiciel propriétaire Cyberwatch, y compris : ▪ 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_6_1_002	Un scan de découverte doit être lancé périodiquement sur le logiciel propriétaire Cyberwatch,afin d'identifier les serveurs non encore enrôlés : ▪ tous les mois pour la DMZ Web, ▪ tous les 6 mois pour les autres zones.	Validé	18/05/2020	
	2_1_6_1_003	Les serveurs aux contraintes de sécurité élevées doivent être enrôlés avec l'agent Cyberwatch. Sont identifiés : ▪ 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_6_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_6_2_001	Les scanners de vulnérabilité doivent s'appuyer sur l'un des logiciels suivants : ▪ le logiciel propriétaire Cyberwatch, ▪ le logiciel propriétaire Tenable Nessus Professional.	Validé	18/05/2020	

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_1_6_3_001				

Contraintes techniques

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_1_6_4_001				

- La dernière modification de cette page a été faite le 4 décembre 2020 à 16:17.

Navigateur web

Un **navigateur web** est un logiciel conçu pour consulter et afficher le World Wide Web. Techniquement, c'est au minimum un client HTTP.

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

Un **navigateur web** est un logiciel client capable d'exploiter les ressources hypertextes et hypermédias du Web ainsi que les ressources d'Internet dans son ensemble, qui permet donc la recherche d'information et l'accès à cette information.

(source : Office québécois de la langue française, 2004 (http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=1299148))

Termes privilégiés : **navigateur web**, **navigateur**, **navigateur internet**

Equivalent étranger: **web browser** (en), **browser**(en), **internet browser** (en)

Sommaire

Contexte

Les offres de navigateurs web proposées par SEP1 s'appuient sur le logiciel libre **Firefox** et le logiciels propriétaires **Microsoft Internet Explorer** et **Microsoft Edge**.

Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_2_1_1_001	Les agents de l'administration centrale peuvent définir le navigateur web par défaut de leur poste de travail.	Validé	01/07/2019	
	2_2_1_1_002	Les nouvelles applications basées sur un serveur web doivent être compatibles avec le navigateur web Firefox ESR.	Validé	01/07/2019	
	2_2_1_1_003	Les navigateurs web doivent être installés dans des versions à jour des correctifs de sécurité.	Validé	03/09/2019	CERTFR-2020-AVI-755 (https://www.cert.ssi r/avis/CERTFR-2020-AVI-755/) **Firefox ESR 78.5** CERTFR-2020-AVI-735 (https://www.cert.ssi r/avis/CERTFR-2020-AVI-735/) **Microsoft Internet Explorer 11** CERTFR-2020-AVI-752 (https://www.cert.ssi r/avis/CERTFR-2020-AVI-752/) **Microsoft Edge 86.0.622.69**

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_2_1_2_001	Les navigateurs web déployés sur les postes de travail des agents de l'administration centrale doivent s'appuyer sur : ▪ le logiciel libre Firefox ESR ▪ le logiciel propriétaire Microsoft Edge 80 ▪ ~~Microsoft Internet Explorer 11 (uniquement dans le cas d'applications nécessitant l'utilisation d'applets JAVA)~~.	Validé	03/12/2020	Ajout du navigateur web Microsoft Edge.

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_2_1_3_001	Toute demande de support sur le logiciel libre Firefox doit se faire au travers du marché "Support à l'usage des logiciels libres" (SLL).	Validé	01/07/2019	Versions Firefox supportées au SLL (https://d nto.alize.finances.rie.gouv.fr/share/page/site/s t/document-details?nodeRef=workspace://Spa re/120d763d-b5f5-41f1-b042-6319e53d30af) **Firefox 60 ESR** Portail support Linagora (https://sll.08000linu otrs/customer.pl)

Contraintes techniques

Installation des navigateurs web

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_2_1_4_001	Le navigateur web installé par défaut sur les postes de travail des agents de l'administration centrale doit être le logiciel libre Mozilla Firefox.	Validé	03/12/2020	

Montée de version des navigateurs web

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_2_1_5_001				

Administration et exploitation des navigateurs web

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_2_1_6_001				

- La dernière modification de cette page a été faite le 7 décembre 2020 à 21:36.

Client de messagerie

Un **client de messagerie** est un logiciel qui sert à lire et envoyer des courriers électroniques. Ce sont en général des clients lourds mais il existe aussi des applications web (messagerie web) qui offrent les mêmes fonctionnalités.

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

Termes privilégiés : **Client de messagerie**

Equivalent étranger: **email client** (en), **email reader**(en), **mail user agent (MUA)** (en)

Sommaire

Contexte

Les offres de clients de messagerie proposées par SEP1 s'appuient sur le logiciel propriétaire **Microsoft Outlook**.

Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_2_2_1_001				

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_2_2_2_001	Les clients de messagerie déployés sur les postes de travail des agents de l'administration centrale doivent s'appuyer sur le logiciel propriétaire **Microsoft Outlook 2013.**	Validé	22/01/2020	

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_2_2_3_001				

Contraintes techniques

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_2_2_4_001				

- La dernière modification de cette page a été faite le 17 février 2020 à 18:29.

Serveur web

Un **serveur web** est spécifiquement un serveur multi-service utilisé pour publier des sites web sur Internet ou un intranet. L'expression « serveur Web » désigne également le logiciel utilisé sur le serveur pour exécuter les requêtes HTTP, le protocole de communication employé sur le World Wide Web.

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

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

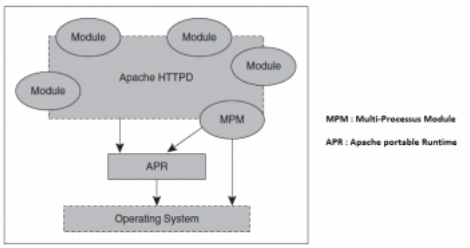
Equivalent étranger: **web server** (en), **HTTP server** (en)

Sommaire

Contexte

Les offres de serveurs web proposées par SEP1 s'appuient sur le logiciel libre **Apache 2.4.46**

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



Source : The Apache module books (Nick Kew) - Pearson Open Source Software Development Series

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 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%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	Guide de paramétrage SSL et entête HTTP (h ocumento.alize.finances.rie.gouv.fr/share/s/C IQpu-9pXX31mdLA) source : SEP1C/PSSI
	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	CGU Authentification renforcée Vérification des obligations légales
	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-signalement_v2.1.pdf).	Validé	01/07/2019	Mode maintenance URI /heartbeat, URI /metrics URI /.well-known/security.txt
	2_3_1_1_005	Les nouvelles applications basées sur des serveurs web doivent respecter le standard ministériel Déploiement du protocole TLS (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/180122_TLS_v10.1.pdf)	Validé	01/07/2019	Guide de paramétrage SSL et entête HTTP (h ocumento.alize.finances.rie.gouv.fr/share/s/C IQpu-9pXX31mdLA) source : SEP1/PSSI
	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	CERTFR-2020-AVI-490 (https://www.cert.ssi r/avis/CERTFR-2020-AVI-490/) **Apache 2.4.46**

Solutions de référence

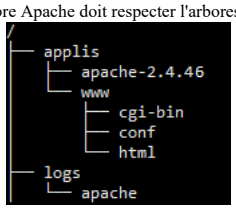
	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_3_1_2_001	Les serveurs web doivent s'appuyer sur le logiciel libre **Apache 2.4.**	Validé	03/09/2019	Dates de fin de support (https://httpd.apache. **Apache 2.4** : NC Version Apache non supportée (https://httpd.a org/) **Apache 2.2**
	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	Exemple : Nginx

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 marché "Support à l'usage des logiciels libres".	Validé	01/07/2019	Versions supportées au SLL (https://document e.finances.rie.gouv.fr/share/page/site/sep1-cct ment-details?nodeRef=workspace://SpacesSt d763d-b5f5-41f1-b042-6319e53d30af) **Apache 2.4** Portail SLL (https://www.otrs.aosc-portal.com ustomer.pl)

Contraintes techniques

Installation des serveurs web

	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 du script "build-http".	Validé	03/09/2019	
	2_3_1_4_002	L'installation du logiciel libre Apache 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	

Montée de version des serveurs web

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_3_1_5_001				

Administration et exploitation des serveurs web

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_3_1_6_001	Les droits et les permissions qui s'appliquent aux répertoires et aux fichiers des serveurs web basés sur le logiciel libre Apache doivent respecter les propriétés suivantes : ▪ Les répertoires doivent avoir des droits positionnés en 755 avec comme propriétaire "root" et groupe "root". ▪ Les fichiers doivent avoir des droits positionnées en 644 avec propriétaire "root" et groupe "root".	Validé	03/09/2019	
	2_3_1_6_002	Les droits et les permissions qui s'appliquent aux répertoires et aux fichiers des serveurs web basés sur le logiciel libre Apache dans lesquels l'application a besoin d'écrire doivent respecter les propriétés suivantes : ▪ Les répertoires doivent avoir des droits positionnés en 775 avec comme propriétaire "root" et groupe "apache" ▪ Les fichiers doivent avoir des droits positionnés en 664 avec comme propriétaire "root" et groupe "apache"	Validé	03/09/2019	
	2_3_1_6_003	La racine des documents (DocumentRoot) doit être située dans le répertoire /applis/www/html/[nom_application] où [nom_application] est le nom de l'application web.	Validé	03/09/2019	
	2_3_1_6_004	La création de serveurs virtuels (VirtualHost) doit se faire à partir du fichier exemple /applis/extra/httpd-vhost-[nom_application].MODELE où [nom_application] est le nom de l'application web. Une fois finalisé, ce fichier doit être renommé en /applis/extra/httpd-vhost-[nom_application].conf où [nom_application] est le nom de l'application web.	Validé	03/09/2019	
	2_3_1_6_005	Les fichiers log des serveurs web basés sur le logiciel libre Apache doivent être situés dans le répertoire /logs/apache	Validé	03/09/2019	

Règles de nommage des URL des serveurs web

<table>
<tr><th></th><th>Identifiant</th><th>Libellé de la règle</th><th>Statut</th><th>Date d'effet</th><th>Commentaires</th></tr>
<tr><td></td><td>2_3_1_7_001</td><td>Les nouvelles applications web exposées sur :
le réseau général (RG)
le réseau interministériel de l'Etat (RIE)
et interfacées avec les serveurs mandataires inverses mutualisés doivent utiliser les règles de nommage des URL suivantes :
Environnement de développement<table><tr><td>URL</td><td>https://[nom_application]-dev.alize.finances.rie.gouv.fr</td></tr><tr><td colspan="2">redirigée vers :</td></tr><tr><td>URL</td><td>https://[nom_application]-dev-bo.alize.finances.rie.gouv.fr</td></tr></table>Environnement de recette<table><tr><td>URL</td><td>https://[nom_application]-itg.alize.finances.rie.gouv.fr</td></tr><tr><td colspan="2">redirigée vers :</td></tr><tr><td>URL</td><td>https://[nom_application]-rec-bo.alize.finances.rie.gouv.fr</td></tr></table>Environnement de production<table><tr><td>URL</td><td>https://[nom_application].alize.finances.rie.gouv.fr</td></tr><tr><td colspan="2">redirigée vers :</td></tr><tr><td>URL</td><td>https://[nom_application]-bo.alize.finances.rie.gouv.fr</td></tr></table>où [nom_application] est le nom de l'application.</td><td>Validé</td><td>01/07/2019</td><td></td></tr>
<tr><td></td><td>2_3_1_7_002</td><td>Les nouvelles applications web exposées sur :
sur le réseau intenet
et interfacées avec les serveurs mandataires inverses mutualisés doivent utiliser les règles de nommage des URL suivantes :
Environnement de développement<table><tr><td>URL</td><td>https://[nom_application]-dev.alize.finances.rie.gouv.fr</td></tr><tr><td colspan="2">redirigée vers :</td></tr><tr><td>URL</td><td>https://[nom_application]-dev-bo.alize.finances.rie.gouv.fr</td></tr></table>Environnement de recette<table><tr><td>URL</td><td>https://[nom_application]-itg.finances.gouv.fr</td></tr><tr><td colspan="2">redirigée vers :</td></tr><tr><td>URL</td><td>https://[nom_application]-rec-bo.finances.gouv.fr</td></tr></table>Environnement de production<table><tr><td>URL</td><td>https://[nom_application].finances.gouv.fr</td></tr><tr><td colspan="2">redirigée vers :</td></tr><tr><td>URL</td><td>https://[nom_application]-bo.finances.gouv.fr</td></tr></table></td><td>Validé</td><td>01/07/2019</td><td></td></tr>
</table>

Gestion des codes erreurs HTTP

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
Nouveauté	2_3_1_8_001	Un code erreur 404 renvoyé par un serveur web d'une nouvelle application doit donner lieu à la redirection vers une page d'erreur prédéfinie : Page introuvable	Validé	18/05/2020	
Nouveauté	2_3_1_8_002	Un code erreur 503 renvoyé par un serveur web d'une nouvelle application doit donner lieu à la redirection vers une page d'erreur prédéfinie : Indisponible provisoirement	Validé	18/05/2020	
Nouveauté	2_3_1_8_003	Un code erreur 504 renvoyé par un serveur web d'une nouvelle application doit donner lieu à la redirection vers une page d'erreur prédéfinie : Application en maintenance	Validé	18/05/2020	

- La dernière modification de cette page a été faite le 24 novembre 2020 à 11:22.

Serveur d'application

Un **serveur d'application** est un logiciel d'infrastructure offrant un contexte d'exécution pour des composants applicatifs.

(source : Wikipedia,2020 (https://fr.wikipedia.org/wiki/Serveur_d%27applications))

Termes privilégiés :**serveur d'application**

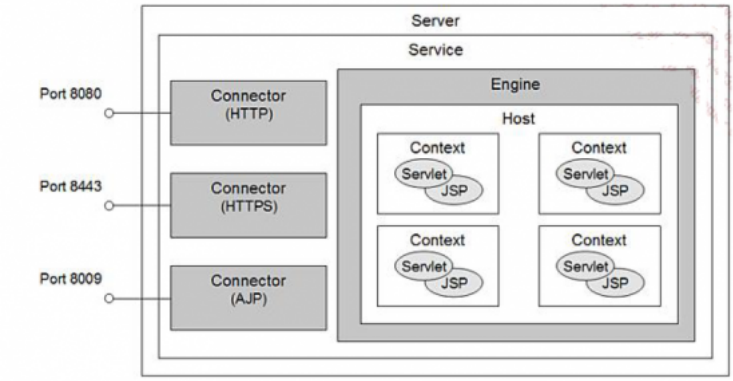
Equivalent étranger: **application server** (en)

Sommaire

Contexte

Les offres de serveurs d'application proposées par SEP1 s'appuient sur le logiciel libre **Apache Tomcat 8.5.56**

L'architecture technique du serveur d'application Apache Tomcat se décline de la manière suivante :



Source : Apache Tomcat 8 (Edition ENI - Etienne Langlet)

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 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_4_1_1_002	Les nouvelles applications nécessitant l'usage d'un serveur d'application doivent 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%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_4_1_1_003	Les nouvelles applications nécessitant l'usage d'un serveur d'application 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_4_1_1_004	Les nouvelles applications nécessitant l'usage d'un serveur d'application 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-signalement_v2.1.pdf).	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 Déploiement du protocole TLS (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/180122_TLS_v10.1.pdf)	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	CERTFR-2020-AVI-397 (https://www.cert.ss fr/avis/CERTFR-2020-AVI-397/) **Tomcat 8.5.56**

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 le logiciel libre **Apache Tomcat v8.5.**	Validé	01/07/2019	Dates de fin de support (http://tomcat.apache. hichversion.html) **- Tomcat 8.5** : NC
	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	Exemple : logiciel libre JBoss

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 marché "Support à l'usage des logiciels libres".	Validé	01/07/2019	Versions Tomcat supportées au SLL (https://d nto.alize.finances.rie.gouv.fr/share/page/site/s t/document-details?nodeRef=workspace://Spa re/120d763d-b5f5-41f1-b042-6319e53d30af) **Tomcat 7.0, 8.5 et 9.0** Portail SLL (https://www.otrs.aosc-portal.com ustomer.pl)

Contraintes techniques

Installation des serveurs d'application

	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 script "build-tomcat".	Validé	18/05/2020	
	2_4_1_4_002	L'installation du logiciel libre Apache Tomcat doit respecter l'arborescence suivante: /applis └── apache-tomcat-8.5.55 ├── bin ├── conf ├── lib ├── logs ├── temp └── work ▪ Répertoire des fichiers binaires: /applis/apache-tomcat-[version] où [version] correspond au numéro de version du logiciel.	Validé	18/05/2020	
	2_4_1_4_003	Les fichiers log du logiciel libre Apache Tomcat doivent être localisés dans le répertoire /logs/tomcat /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	Validé	18/05/2020	La rotation des fichiers log est gérée par le dém apache-tomcat et non par le démon logrotate.
	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/webapps	Validé	18/05/2020	Ce répertoire est indiqué dans le fichier de configuration du serveur /applis/apache-tomcat-$version/conf/server.xml .

Montée de version des serveurs d'application

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

Administration et exploitation des serveurs d'application

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_4_1_6_001	Les droits et les permissions qui s'appliquent aux répertoires et aux fichiers des serveurs d'application basés sur le logiciel libre Apache-tomcat doivent respecter les propriétés suivantes: ▪ Les répertoires doivent avoir des droits positionnés en 755 avec comme propriétaire "tomcat${version}" et groupe "tomcat". ▪ Les exécutables *.sh dans le répertoire bin doivent avoir les droits positionnés en 755 avec comme propriétaire "tomcat${version}" et groupe "tomcat". Les fichiers doivent avoir des droits positionnées en 644 avec propriétaire "tomcat${version}" et groupe "tomcat".	Validé	18/05/2020	${version} est le premier digit du numéro de version apache-tomcat
	2_4_1_6_002	Les droits et les permissions qui s'appliquent aux répertoires et aux fichiers des serveurs d'application basés sur le logiciel libre Apache-tomcat dans lesquels l'application a besoin d'écrire doivent respecter les propriétés suivantes: ▪ Les répertoires doivent avoir des droits positionnés en 755 avec comme propriétaire "tomcat${version}" et groupe "tomcat" Les fichiers doivent avoir des droits positionnés en 644 avec comme propriétaire " tomcat${version}" et groupe "tomcat"	Validé	18/05/2020	

- La dernière modification de cette page a été faite le 23 octobre 2020 à 14:22.

Environnement d'exécution PHP

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

(source : Wikipedia,2020 (https://fr.wikipedia.org/wiki/Environnement_d%27ex%C3%A9cution)).

Le **langage PHP** (Hypertext Preprocessor) est un langage de programmation libre, principalement utilisé pour produire des pages Web dynamiques via un serveur HTTP5, mais pouvant également fonctionner comme n'importe quel langage interprété de façon locale. PHP est un langage impératif orienté objet.

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

Termes privilégiés :**environnement d'exécution**

Equivalent étranger: **execution environment** (en), **runtime** (en)

Sommaire

Contexte

Les offres d'environnement d'exécution PHP proposées par SEP1 s'appuient sur les logiciels libres **APACHE 2.4.46** et **PHP 7.2.34**

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%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_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%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_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%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_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%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-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 (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/180122_TLS_v10.1.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	CERTFR-2020-AVI-615 (https://www.cert.ss r/avis/CERTFR-2020-AVI-615/) **PHP 7.2.34, PHP 7.3.23 et PHP 7.4.11**

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 7.4.**	Validé	03/12/2020	Dates de fin de support (https://www.php.net/rted-versions.php) **- PHP 7.2** : 30/11/2020 **- PHP 7.4** : 28/11/2022 Versions PHP non supportées (https://www.pheol.php) **- PHP 3.x, 4.x, 5.x, 7.0, 7.1 et 7.2**

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 marché "Support à l'usage des logiciels libres" (SLL).	Validé	01/07/2019	Versions PHP supportées au SLL (https://docuo.alize.finances.rie.gouv.fr/share/page/site/sepdocument-details?nodeRef=workspace://Space/120d763d-b5f5-41f1-b042-6319e53d30af) **- PHP 5.4, 5.6, 7.1 et 7.2** Portail SLL (https://www.otrs.aosc-portal.comustomer.pl)

Contraintes techniques

Installation de l'environnement d'exécution PHP

	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 du script "build-php".	Validé	03/09/2019	

Montée de version de l'environnement d'exécution PHP

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_4_2_5_001				

Administration et exploitation de l'environnement d'exécution PHP

	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 4 décembre 2020 à 15:50.

Serveur de messagerie

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.

(source : wikipedia,2020 (https://fr.wikipedia.org/wiki/Serveur_de_messagerie_%C3%A9lectronique))

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

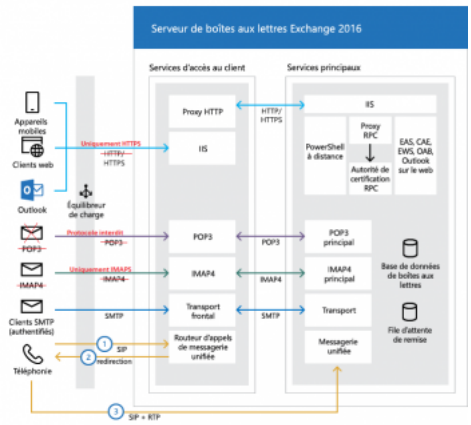
Equivalent étranger: **e-mail server** (en), **electronic mail server** (en), **mail server** (en), **messaging server** (en), **post office server** (en)

Sommaire

Contexte

Les offres de serveurs de messagerie proposées par SEP1 s'appuient sur le logiciel propriétaire **Microsoft Exchange**.

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



Source : Microsoft

Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_4_3_1_001	Les serveurs de messagerie de la sous-direction informatique des services centraux (SEP1) doivent respecter le standard ministériel Homologation de services Email (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-email_v1.0.0.pdf).	Validé	01/07/2019	
	2_4_3_1_002	Les serveurs de messagerie de la sous-direction informatique des services centraux (SEP1) doivent respecter le standard ministériel Standard SPF et lutte contre l'usurpation d'email (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_standard-SPF_v4.pdf).	Validé	01/07/2019	
	2_4_3_1_003	Les serveurs de messagerie de la sous-direction informatique des services centraux (SEP1) doivent respecter le standard ministériel Relais SMTP, authenticité et confidentialité des courriels (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/180213_standard-relais-SMTP_v2.pdf).	Validé	01/07/2019	
	2_4_3_1_004	Les serveurs de messagerie de la sous-direction informatique des services centraux (SEP1) doivent respecter le standard ministériel Guide technique DKIM, DMARC, STARTTLS, MIME (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/170307_guide-technique-DKIM-DMARC-STARTTLS-MIME_v1.pdf).	Validé	01/07/2019	
	2_4_3_1_005	Les serveurs de messagerie de la sous-direction informatique des services centraux (SEP1) doivent respecter le standard ministériel Déploiement du protocole TLS (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/180122_TLS_v10.1.pdf).	Validé	01/07//2019	
	2_4_3_1_006	Les serveurs de messagerie doivent être installés dans des versions à jour des correctifs de sécurité.	Validé	03/09/2019	CERTFR-2020-AVI-808 (https://www.cert.ssi fr/avis/CERTFR-2020-AVI-808/) **Microsoft Exchange 2016 Server** (Cumulati Update 17 et 18)

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
Règle modifiée	2_4_3_2_001	Les serveurs de messagerie doivent s'appuyer sur les logiciels suivants : ▪ le logiciel propriétaire **Microsoft Exchange Server 2016,** ▪ le logiciel propriétaire **Scanmail pour Microsoft Exchange v14.**	A valider	10/09/2020	Date de fin de support standard (https://suppo rosoft.com/fr-fr/lifecycle/search) : **MS Exchange 2016** : 13/10/2020 Date de fin de support étendu (https://suppor soft.com/fr-fr/lifecycle/search) : **MS Exchange 2016** : 14/10/2025

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_4_3_3_001				

Contraintes techniques

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_4_3_4_001	Les nouvelles applications interfacées avec les serveurs de messagerie doivent utiliser l'un des protocoles suivants : ▪ 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_3_4_002	Les nouvelles applications interfacées avec les serveurs de messagerie ne doivent pas utiliser les protocoles suivants : ▪ 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	
Nouveauté	2_4_3_4_003	Les nouvelles applications devant accéder aux données d'une boite aux lettres électroniques (BAL) doivent s'interfacer avec les serveurs de messagerie suivants : **Environnement** / **Serveur** Développement : webmail.caradev.finances.gouv.fr Recette : webmail.caradev.finances.gouv.fr Production : mel.finances.gouv.fr	Validé	18/05/2020	

- La dernière modification de cette page a été faite le 11 décembre 2020 à 15:19.

Environnement d'exécution JAVA

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,2020 (https://fr.wikipedia.org/wiki/Environnement_d%27ex%C3%A9cution))

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,2020 (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)

Sommaire

Contexte

Les offres d'environnement d'exécution JAVA proposées par SEP1 s'appuient 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_4_1_001	Toute nouvelle application développée en JAVA 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%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	03/12/2019	
	2_4_4_1_002	Toute nouvelle application développée en JAVA 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%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	03/12/2019	
	2_4_4_1_003	Toute nouvelle application développée en JAVA 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%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	03/12/2019	
	2_4_4_1_004	Toute nouvelle application développée en JAVA 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%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-signalement_v2.1.pdf).	Validé	03/12/2019	
	2_4_4_1_005	Toute nouvelle application développée en JAVA doit respecter le standard ministériel Déploiement du protocole TLS (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/180122_TLS_v10.1.pdf)	Validé	03/12/2019	
	2_4_2_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_4_2_001	L'environnement d'exécution JAVA doit s'appuyer sur le logiciel libre **OpenJDK 11.**	Validé	03/12/2019	

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 OpenJDK doit se faire au travers du marché "Support à l'usage des logiciels libres" (SLL).	Validé	01/07/2019	Versions OpenJDK supportées au SLL (https:/ mento.alize.finances.rie.gouv.fr/share/page/sit -cct/document-details?nodeRef=workspace://S Store/120d763d-b5f5-41f1-b042-6319e53d30 **OpenJDK 8 et 11** Portail support Linagora (https://sll.08000linu otrs/customer.pl)

Contraintes techniques

Installation de l'environnement d'exécution JAVA

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_4_4_4_001	L'installation du logiciel libre OpenJDK doit se faire à partir des fichiers sources disponibles depuis le site officiel.	Validé	03/12/2020	

Montée de version de l'environnement d'exécution JAVA

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_4_4_5_001				

Administration et exploitation de l'environnement d'exécution JAVA

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_4_4_6_001				

- La dernière modification de cette page a été faite le 8 juin 2020 à 11:59.

Serveur de relais de messagerie

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

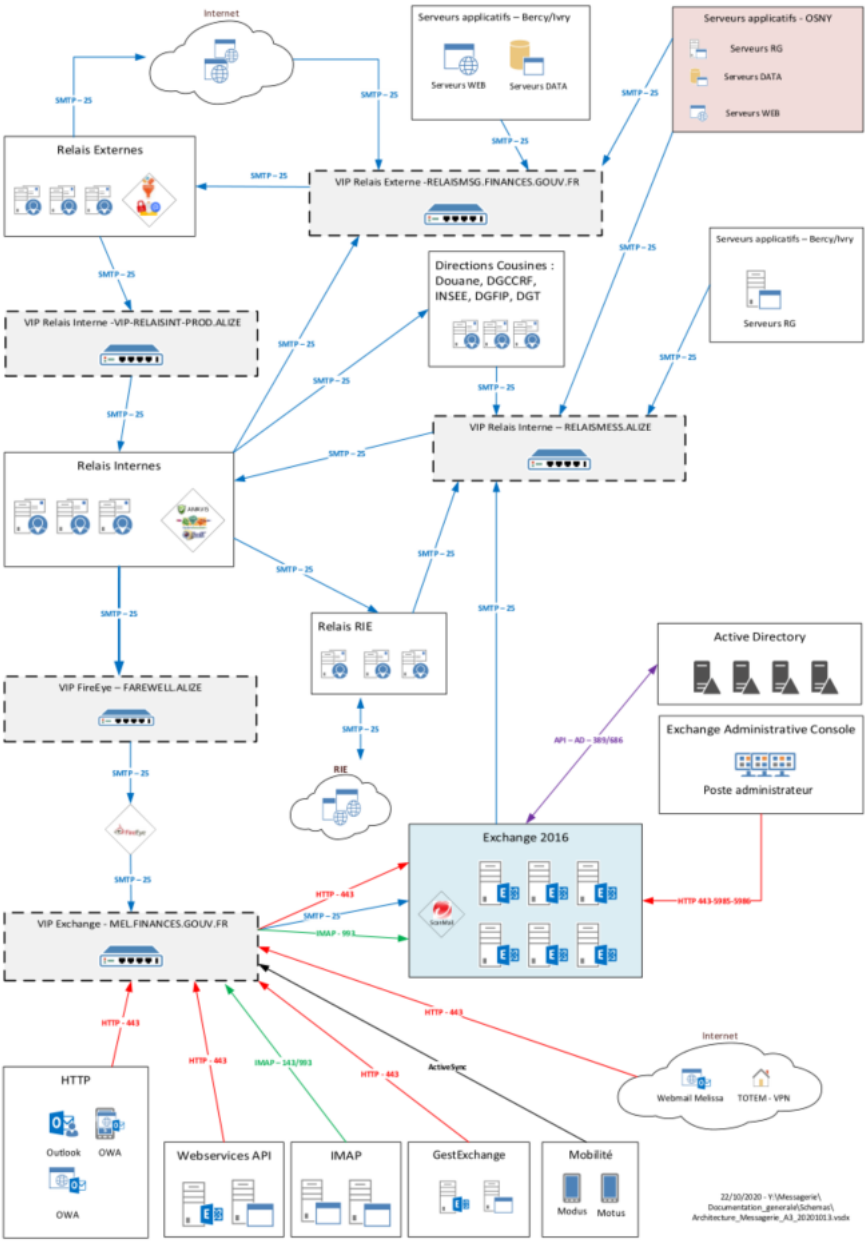
Contexte

Les offres de serveurs de relais de messagerie proposées par SEP1 s'appuient sur le logiciel libre **Postfix**.

On distingue trois types de serveurs de relais de messagerie :

- Serveurs de relais de messagerie interne,
- Serveurs de relais de messagerie externe,
- Serveurs de relais de messagerie RIE.

L'architecture technique de la plateforme de messagerie se décline de la manière suivante :



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 informatique des services centraux (SEP1) doivent respecter le standard ministériel Homologation de services Email (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-email_v1.0.0.pdf) .	Validé	01/07/2019	
	2_4_5_1_002	Les serveurs de relais de messagerie de la sous-direction informatique des services centraux (SEP1) doivent respecter le standard ministériel Standard SPF et lutte contre l'usurpation d'email (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_standard-SPF_v4.pdf).	Validé	01/07/2019	
	2_4_5_1_003	Les serveurs de relais de messagerie de la sous-direction informatique des services centraux (SEP1) doivent respecter le standard ministériel Relais SMTP, authenticité et confidentialité des courriels (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/180213_standard-relais-SMTP_v2.pdf).	Validé	01/07/2019	
	2_4_5_1_004	Les serveurs de relais de messagerie de la sous-direction informatique des services centraux (SEP1) doivent respecter le standard ministériel Guide technique DKIM, DMARC, STARTTLS, MIME (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/170307_guide-technique-DKIM-DMARC-STARTTLS-MIME_v1.pdf).	Validé	01/07//2019	
	2_4_5_1_005	Les serveurs de relais de messagerie de la sous-direction informatique des services centraux (SEP1) doivent respecter le standard ministériel Déploiement du protocole TLS (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/180122_TLS_v10.1.pdf).	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	Les serveurs de relais de messagerie doivent s'appuyer sur les logiciels suivants :
		▪ Au niveau des relais de messagerie externe
		  ▪ le logiciel libre Postfix (https://fr.wikipedia.org/wiki/Postfix)
		  ▪ le logiciel libre OpenDMARC (https://fr.wikipedia.org/wiki/DMARC)
		  ▪ le logiciel libre OpenDKIM (https://fr.wikipedia.org/wiki/DomainKeys_Identified_Mail)
		▪ Au niveau des relais de messagerie interne
		  ▪ le logiciel libre Postfix (https://fr.wikipedia.org/wiki/Postfix)
		  ▪ le logiciel libre Amavis (https://en.wikipedia.org/wiki/Amavis)
		  ▪ le logiciel libre ClamAV (https://fr.wikipedia.org/wiki/ClamAV)
		  ▪ le logiciel libre SpamAssassin (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	Versions Postfix supportées au SLL (https://d nto.alize.finances.rie.gouv.fr/share/page/site/s t/document-details?nodeRef=workspace://Spa ore/120d763d-b5f5-41f1-b042-6319e53d30af **- Postfix 2.10 et 2.11** Portail support (https://www.otrs.aosc-portal.c rs/customer.pl)
	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	Versions Postfix supportées au SLL (https://d nto.alize.finances.rie.gouv.fr/share/page/site/s t/document-details?nodeRef=workspace://Spa ore/120d763d-b5f5-41f1-b042-6319e53d30af **- OpenDMARC 1.3** Portail support (https://www.otrs.aosc-portal.c rs/customer.pl)
	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	Versions Postfix supportées au SLL (https://d nto.alize.finances.rie.gouv.fr/share/page/site/s t/document-details?nodeRef=workspace://Spa ore/120d763d-b5f5-41f1-b042-6319e53d30af **- OpenDKIM 2.10** Portail support (https://www.otrs.aosc-portal.c rs/customer.pl)
	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	Versions Postfix supportées au SLL (https://d nto.alize.finances.rie.gouv.fr/share/page/site/s t/document-details?nodeRef=workspace://Spa ore/120d763d-b5f5-41f1-b042-6319e53d30af **- SpamAssassin 3.1, 3.3 ET 3.4** Portail support (https://www.otrs.aosc-portal.c rs/customer.pl)
	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	Versions Postfix supportées au SLL (https://d nto.alize.finances.rie.gouv.fr/share/page/site/s t/document-details?nodeRef=workspace://Spa ore/120d763d-b5f5-41f1-b042-6319e53d30af **- Amavisd-new 2.9, 2.10** Portail support (https://www.otrs.aosc-portal.c rs/customer.pl)
	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	Versions Postfix supportées au SLL (https://d nto.alize.finances.rie.gouv.fr/share/page/site/s t/document-details?nodeRef=workspace://Spa ore/120d763d-b5f5-41f1-b042-6319e53d30af **- ClamAV 0.100** Portail support (https://www.otrs.aosc-portal.c rs/customer.pl)

Contraintes techniques

<table>
<tr><th></th><th>Identifiant</th><th>Libellé de la règle</th><th>Statut</th><th>Date d'effet</th><th>Commentaires</th></tr>
<tr><td></td><td>2_4_5_4_001</td><td>Les nouvelles applications interfacées avec les serveur de relais de messagerie doivent utiliser le protocole SMTP.</td><td>Validé</td><td>03/12/2019</td><td></td></tr>
<tr><td></td><td>2_4_5_4_002</td><td>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 suivants :
<table><tr><th>Environnement</th><th>Relais interne</th><th>Relais externe</th></tr><tr><td>Développement</td><td>vvr-rel-iag.alize</td><td>rec-re.finances.gouv.fr</td></tr><tr><td>Recette</td><td>vvr-rel-iag.alize</td><td>rec-re.finances.gouv.fr</td></tr><tr><td>Production</td><td>relaismess.alize</td><td>relaismsg.finances.gouv.fr</td></tr></table></td><td>Validé</td><td>10/09/2020</td><td>Mise à jour des noms des serveurs de relais d messagerie internes de développement et de r</td></tr>
<tr><td></td><td>2_4_5_4_003</td><td>Les nouvelles applications envoyant des courriers électroniques (https://fr.wikipedia.org/wiki/Courrier_%C3%A9lectronique) doivent respecter la règle de nommage suivante :
<table><tr><th>Environnement</th><th>Nom de l'émetteur</th></tr><tr><td>Recette</td><td>[fonction.direction]@recette.finances.gouv.fr</td></tr><tr><td>Production</td><td>[fonction.direction]@applications.finances.gouv.fr</td></tr></table>où [fonction] est le nom de l’application et [direction] le nom de l’entité.</td><td>Validé</td><td>10/09/2020</td><td></td></tr>
</table>

- La dernière modification de cette page a été faite le 4 décembre 2020 à 08:45.

Intégration de données (ETL)

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

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 17 février 2020 à 19:33.

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 personnel1. 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 : **Réglement général sur la protection des données**, **RGPD**

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

Sommaire

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				

- La dernière modification de cette page a été faite le 17 février 2020 à 19:26.

Système de gestion de base de données (SGBD)

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,2020 (https://fr.wikipedia.org/wiki/Syst%C3%A8me_de_gestion_de_base_de_donn%C3%A9es))

Un **système de gestion de base de données** est un système matériel et logiciel dont la fonction est d'assurer la gestion automatique d'une base de données et de permettre la création, la modification, l'utilisation et la protection des données.

(source : Office québécois de la langue française,2001 (http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8871183))

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

Contexte

Les offres de système de gestion de base de données (SGBD) proposées par SEP1 s'appuient par défaut sur :

- le logiciel libre **PostgreSQL** pour les serveurs Linux à vocation applicative,
- le logiciel propriétaire **Microsoft SQL Server** 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) .

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	CERTFR-2020-AVI-744 (https://www.cert.ssi r/avis/CERTFR-2020-AVI-744/) **PostgreSQL 11.10** **CERTFR-2020-AVI-433 (https://www.cert.s v.fr/avis/CERTFR-2020-AVI-433/)** **Oracle Database Server** 11.2.0.4, 12.1.0.2, 1 et 18c

Solutions de référence

<brdata-attributes="" />	**Identifiant**<brdata-attributes="" />	**Libellé de la règle**<brdata-attributes="" />	**Statut**<brdata-attributes="" />	**Date d'effet**<brdata-attributes="" />	**Commentaires**<brdata-attributes=""
<brdata-attributes="" />	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 11**<brdata-attributes="" />	Validé<brdata-attributes="" />	18/05/2020	Date de fin de support (https://www.postgr g/support/versioning/) :<brdata-attributes= />**PostgreSQL 11** : 09/11/2023<brdata-attributes="" />
	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.**<brdata-attributes="" />	Validé	10/09/2020	Microsoft SQL Server 2017<brdata-attribu />(Cumulative Update 21)<brdata-attribute />
	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	Serveur Linux à vocation applicative<brda attributes="" />Exemples : Oracle, MariaD MySQL

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	Versions supportées au SLL (https://documen e.finances.rie.gouv.fr/share/page/site/sep1-cct ment-details?nodeRef=workspace://SpacesSt 0d763d-b5f5-41f1-b042-6319e53d30af) : **PostgreSQL 9,5, 9.6, 10 et 11** Portail support (https://www.otrs.aosc-portal. rs/customer.pl)
	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 des fichiers sources disponibles depuis le site officiel de l'éditeur.	Validé	01/07/2019	Code source PostgreSQL (https://www.postgr rg/ftp/source/)
	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
Nouveauté	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	
Nouveauté	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 14 décembre 2020 à 13:19.

Annuaire Active Directory (AD)

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

Termes privilégiés : **Active Directory**, **AD**

Equivalent étranger: **Active Directory** (en), **AD**(en)

Sommaire

Contexte

Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_6_3_1_001	L'annuaire Active Directory (AD) de SEP1 doit respecter le standard ministériel Active Directory (https://hfds-bercy.alize.finances.rie.gouv.fr/sites/hfds-bercy/accueil/ssi/textes-de-reference-1.html).	Validé	10/09/2020	

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 : ▪ **[pnom]-adc** pour les comptes utilisateurs de l'administration centrale sans privilège, ▪ **[fonction.direction]-adc** pour les comptes utilisateurs génériques de l'administration centrale, ▪ **ADMIN-[pnom]** pour les comptes utilisateurs destinés à l'élévation des privilèges sur les postes de travail windows de l'administration centrale, ▪ **[pnom]-ADMIN** pour les comptes utilisateurs avec privilèges destinés à l'administration des serveurs windows, ▪ **ADMIN-[application]** pour les comptes de service hors gMSA de l'administration centrale, ▪ **gMSA-[nomappli][environnement]** pour les comptes de service gMSA de l'administration centrale. ▪ **GRID-[pnom]** pour les comptes utilisateurs avec privilèges attribués aux Grids. ▪ **PDT-[pnom]** pour les comptes utilisateurs avec privilèges attribués aux utilisateurs SEP1D. ▪ **88000-[pnom]** pour les comptes utilisateurs avec privilèges attribués aux opérateurs du centre de service pour le support des utilisateurs de l'administration centrale.	Validé	03/12/2020	
	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	

Gestion des mots de passe

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_6_3_5_001				

Gestion des annuaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_6_3_6_001	Toute application utilisant le protocole d'authentification Kerberos (https://fr.wikipedia.org/wiki/Kerberos_(protocole)) doivent s'interfacer avec les annuaires suivants : **Environnement** / **Annuaire AD** Développement / caradev.alize Recette / caradev.alize Production / solano.alize	Validé	10/09/2020	

- La dernière modification de cette page a été faite le 4 décembre 2020 à 17:02.

Annuaire LDAP

Un annuaire est une base de données spécialisée, accessible en tout ou en partie pour consultation, et qui rend disponibles les attributs des entités qui interagissent au sein de l'organisation..

(Source : Office québécois de la langue française,2005 (http://http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8355499))

Termes privilégiés : **Annuaire**, **Répertoire**

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

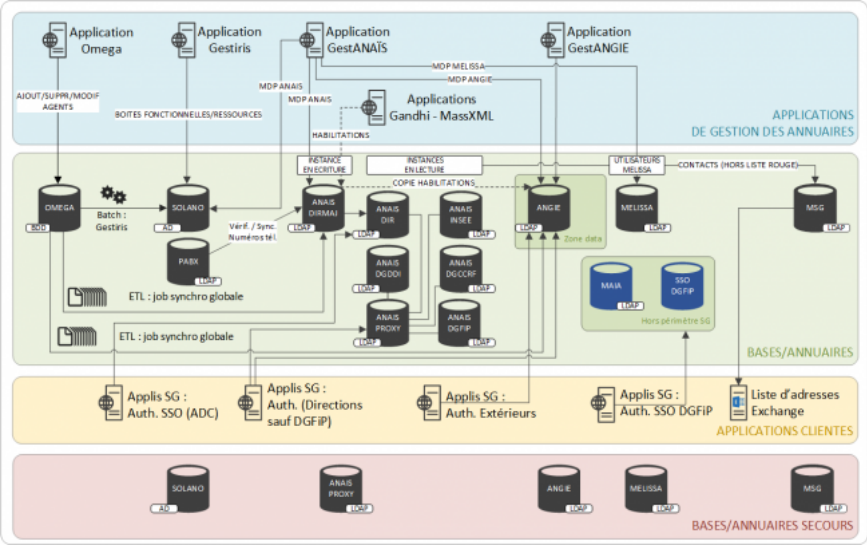
Sommaire

Contexte

SEP1 dispose de plusieurs annuaires LDAP de type Active Directory (AD), OpenLDAP (OL) et RedHat Directory Server (RHDS) :

- L'annuaire **Solano (AD)** répertorie les éléments tels que les comptes des utilisateurs, les serveurs, les postes de travail, les dossiers partagés (en), les imprimantes, etc. Il couvre la population des agents d'administration centrale . Il est également utilisé pour des entités matériels comme des ordinateurs, des imprimantes et des locaux.
- L'annuaire **Anais central** (RHDS) couvre la population des agents d'administration centrale des MEF qui dispose d'un compte dans l'annuaire Solano.Il est accessible sur le réseau général et est interfacé avec les applications intranet. L'identifiant est le compte -adc.
- L'annuaire **Angie** (OL) couvre la population de l'administration centrale ayant une BAL dans l'annuaire Solano et les comptes externes parrainés. Il est situé en DMZ Data et est interfacé avec les applications disponibles sur le réseau internet. L'identifiant est l'email. La gestion des mots de passe s'effectue au travers de l'application GestAngie. La gestion des comptes parrainés s'effectue au travers de l'application GestAnais.
- L'annuaire **ProxyLdap** (OL) propose une vue consolidée de l'ensemble des annuaires LDAP des directions à réseau DGFIP, DGDDI, DGCCRF, INSEE et Anais centrale. C'est un annuaire OpenLdap situé sur le réseau général.
- L'annuaire **MELISSA** (OL) couvre la population disposant d'un accès à l'application de messagerie Melissa.
- L'annuaire **MSG** (OL) est l'annuaire ministériel au format de la messagerie (o=gouv,c=fr).

Certains comptes sont classés en liste rouge : les comptes de prestataires, les comptes devant restés "anonymes", les comptes applicatifs. Ils n'apparaissent pas dans les interfaces de consultation.



Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
Création	2_6_4_1_001	Toute application des ministères économiques et financiers doit pouvoir accéder aux annuaires Ldap du secrétariat général.	A valider	10/09/2020	

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_6_4_2_001				

Contraintes juridiques et réglementaires

	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 (AD) SOLANO.	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 Anaïs et Angie doivent contenir 14 caractères minimum.	Validé	10/09/2020	
	2_6_4_4_003	Les mots de passe stockés dans les annuaires Anaïs et Angie 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 Anaïs et Angie doivent impérativement respecter 3 des 4 critères suivants : ▪ 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 Anaïs et Angie 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 Anaïs et Angie doivent être différents.	Validé	10/09/2020	

Gestion des annuaires

<table>
<tr><th></th><th>Identifiant</th><th>Libellé de la règle</th><th>Statut</th><th>Date d'effet</th><th>Commentaires</th></tr>
<tr><td></td><td>2_6_4_5_001</td><td>Les applications exposées sur le réseau général (RG) et sur le réseau interministériel de l'Etat (RIE) doivent s'interfacer avec les annuaires suivants :
<table><tr><th>Environnement</th><th>Annuaire Anais</th><th>Annuaire Proxy</th></tr><tr><td>Développement</td><td>dv-ae2-dir1.alize</td><td>dv-ae2-proxy.alize</td></tr><tr><td>Recette</td><td>pp-ae2-dir.alize</td><td>pp-ae2-proxy.alize</td></tr><tr><td>Production</td><td>nm-ae2-dir.alize</td><td>nm-ae2-proxy.alize</td></tr></table></td><td>Validé</td><td>03/12/2020</td><td>Modification de l'annuaire Anais de développe
dv-ae2-dir.alize en dv-ae2-dir1.alize</td></tr>
<tr><td></td><td>2_6_4_5_002</td><td>Les applications exposées sur le réseau internet doivent s'interfacer avec les annuaires suivants :
<table><tr><th>Environnement</th><th>Annuaire Angie</th></tr><tr><td>Développement</td><td>angiedev.alize</td></tr><tr><td>Recette</td><td>angie-rec-store.alize</td></tr><tr><td>Production</td><td>angie.alize</td></tr></table></td><td>Validé</td><td>10/09/2020</td><td></td></tr>
</table>

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 : ▪ l'annuaire Active Directory Solano de production ▪ le serveur de messagerie de production.	Validé	03/12/2020	
	2_6_4_6_002	L'annuaire Anais centrale recette doit être synchronisé avec : ▪ l'annuaire Active Directory Solano de recette/développement ▪ le serveur de messagerie de recette/développement.	Validé	03/12/2020	
Création	2_6_4_6_003	Tous les annuaires LDAP doivent être synchronisés à partir de la base de données OMEGA.	A valider	03/12/2020	en Attente source OMEGA

- La dernière modification de cette page a été faite le 7 décembre 2020 à 15:06.

Gestion du code source

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

Contexte

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
Nouveauté	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 29 mai 2020 à 16:01.

Gestion des anomalies

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

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	Versions supportées au SLL (https://documento inances.rie.gouv.fr/share/page/site/sep1-cct/doc -details?nodeRef=workspace://SpacesStore/120 -b5f5-41f1-b042-6319e53d30af) **Mantis 2.12** Portail support Linagora (https://sll.08000linux. trs/customer.pl)

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 :
		▪ Catégorie : nom du projet
		▪ Impact : Bloquant, Majeur ou Mineur
		▪ Type :
		  ▪ 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 17 février 2020 à 16:36.

Environnement de développement intégré (IDE)

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

(source : wikipedia,2020 (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)

Sommaire

Contexte

Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_7_4_1_001				

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	03/09/2019	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 14 décembre 2020 à 13:21.

Qualité et sécurité du code source

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)

Sommaire

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 de SEP1.	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
Nouveauté	2_7_5_4_401	L'encodage des contenus et du code sources doivent être de type UTF-8 (https://fr.wikipedia.org/wiki/UTF-8).	Validé	18/05/2020	

- La dernière modification de cette page a été faite le 29 mai 2020 à 16:03.

Tests et intégration

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)))

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))

Sommaire

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 : ▪ 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	Toute demande de support sur le logiciel propriétaire Squash TM doit se faire auprès 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	03/09/2019	

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 18 février 2020 à 21:35.

Sauvegarde et restauration des données (serveurs)

La **sauvegarde de données** est l'opération qui consiste à dupliquer et à mettre en sécurité les données contenues dans un système informatique.

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

La **sauvegarde de données** est l'opération qui consiste à recopier un ou plusieurs fichiers de données, généralement sur un support externe, afin d'en prévenir la perte systématique ou accidentelle.La restauration est l'opération qui consiste à reproduire sur un disque dur des données provenant d'une copie de sauvegarde.

(source : Office québécois de la langue française, 2002 (http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=2074332))

La **restauration de données** est une opération informatique qui consiste à retrouver les données perdues à la suite d'une erreur humaine, une défaillance matérielle, un accident ou au moment opportun d'un test de récupération de données défini dans une procédure de stratégie de sauvegarde et d'archive, également appelé plan de sauvegarde.

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

La **restauration de données** est une opération qui consiste à reproduire sur un disque dur des données provenant d'une copie de sauvegarde.

(source : Office québécois de la langue française,2002 (http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8370190))

Termes privilégiés : sauvegarde informatique, sauvegarde, restauration

Anglais : data backup, backup, safeguard, saving, restoration

Sommaire

Contexte

Les offres de solution de sauvegarde et de restauration des données (serveurs) proposées par SEP1 s'appuient sur :

- les équipements de sauvegarde de la société **Veritas**
- le logiciel propriétaire **NetBackup** de la société **Veritas**

Règles de base

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_8_1_1_001	La solution de référence de sauvegarde et de restauration des données (serveurs) doivent être installée dans des versions à jour des correctifs de sécurité.	Validé	03/09/2019	**Veritas Netbackup 8.1.2**

Solutions de référence

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_8_1_2_001	La sauvegarde et la restauration de données (serveurs) doivent s'appuyer sur le : - logiciel propriétaire **Veritas NetBackup Enterprise Server 8.1.2** - logiciel propriétaire **Veritas NetBackup OpsCenter 8.1.2** - logiciel propriétaire **Veritas InfoScale 7.3.10.0** - logiciel propriétaire **Veritas NetBackup 3.1.2 (Appliance 5230)** - logiciel propriétaire **Veritas NetBackup 7.4.2 (Access 3340)**	Validé	10/09/2020	Date de fin de support NetBackup (support de base) (https://sort.veritas.com/eosl) : - **NetBackup 8.2** : à déterminer - **NetBackup 8.1** : à déterminer Date de fin de support NetBackup (support ét (https://sort.veritas.com/eosl) : - **NetBackup 8.2** : à déterminer - **NetBackup 8.1** : à déterminer

Contraintes juridiques et réglementaires

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_8_1_3_001	L'assistance à l'administration de la plateforme de sauvegarde doit se faire au travers du marché "Assistance à l'administration de la plateforme de sauvegarde NetBackup des données serveurs" :	Validé	03/09/2019	

Contraintes techniques

Installation

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_8_1_6_001	Tout nouveau serveur doit être installé avec le logiciel propriétaire **NetBackup client 8.1.2**	Validé	10/09/2020	

Politique de sauvegarde des données (serveurs)

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_8_1_4_001	Pour les **données de type fichiers**, la politique de sauvegarde décrite ci-dessous doit être appliquée : ▪ Sauvegarde totale : hebdomadaire, le week-end ▪ Sauvegarde incrémentale : quotidienne en semaine, entre 19h et 5h.	Validé	03/09/2019	
	2_8_1_4_002	Pour les **données de type Oracle et SQL Server**, la politique de sauvegarde décrite ci-dessous doit être appliquée : ▪ Sauvegarde totale : quotidienne, entre 20h et 05h ▪ Sauvegarde incrémentale : quotidienne, entre 12h et 14h.	Validé	03/09/2019	
	2_8_1_4_003	Pour les **données de type Microsoft Exchange**, la politique de sauvegarde décrite ci-dessous doit être appliquée : ▪ Sauvegarde totale : quotidienne, entre 20h et 05h ▪ Sauvegarde incrémentale : sans objet.	Validé	03/09/2019	
	2_8_1_4_004	Pour les **données de type VMware**, la politique de sauvegarde décrite ci-dessous doit être appliquée : ▪ Sauvegarde totale : hebdomadaire, le week-end ▪ Sauvegarde incrémentale : quotidienne en semaine, entre 19h et 05h.	Validé	03/09/2019	
	2_8_1_4_005	Pour les **données de type Bare Metal Restore (BMR)**, la politique de sauvegarde décrite ci-dessous doit être appliquée : ▪ Sauvegarde totale : hebdomadaire, le week-end ▪ Sauvegarde incrémentale : quotidienne en semaine, entre 19h et 05h.	Validé	03/09/2019	
	2_8_1_4_006	La politique de sauvegarde des données (serveurs) peut être adaptée en fonction des contraintes métiers moyennant justification technique dans le dossier d'architecture technique (DAT) (https://documento.alize.finances.rie.gouv.fr/share/s/TuQwZJ-qQcqHp0AlnUgiug).	Validé	03/09/2019	
	2_8_1_4_007	Pour les **données de type SGBD (autre que Oracle et SQL Server)**, la politique de sauvegarde décrite ci-dessous doit être appliquée : ▪ Sauvegarde totale : hebdomadaire, le week-end ▪ Sauvegarde incrémentale : quotidienne en semaine, entre 19h et 5h.	Validé	10/09/2020	**Exemple** : PostgreSQL, MariaDB, MySQL...

Politique de restauration

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_8_1_5_001	Afin de vérifier régulièrement la consistance des sauvegardes, des tests de restauration doivent être réalisés pour chaque type de données: ▪ Test de restauration d'un fichier, ▪ Test de restauration d'un SGBD, ▪ Test de restauration d'une boite aux lettres électronique (BAL), ▪ Test de restauration d'un serveur virtuel (partiel ou dans sa totalité).	Validé	10/09/2020	La fréquence de ces tests est à définir sachant qu'une périodicité annuelle est généralement conseillée.

Durée de rétention

	Identifiant	Libellé de la règle	Statut	Date d'effet	Commentaires
	2_8_1_7_001	La durée de rétention des données (serveurs) sauvegardées doit être de **60 jours**.	Validé	10/09/2020	

- La dernière modification de cette page a été faite le 25 septembre 2020 à 09:23.

Accès à distance (des prestataires)

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,2020 (https://fr.wikipedia.org/wiki/Acc%C3%A8s_%C3%A0_distance))

L'**accès à distance** est la possibilité de relier un ordinateur à un réseau ou à un poste de travail éloigné géographiquement.

(source : Institut Canadien des Comptables Agréés, 2006 (http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=504724))

Termes privilégiés :**accès à distance**, **téléaccès**, **accès distant**

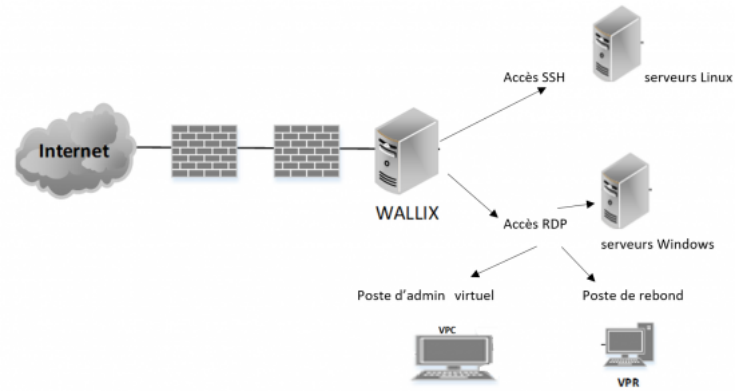
Equivalent étranger: **remote access** (en)

Sommaire

Contexte

L'offre d'accès à distance (des prestataires) proposées par SEP1 s'appuie sur la solution ARTEMIS. L'accès à la solution ARTEMIS se fait au travers de l'URL suivante : https://www.artemis.finances.gouv.fr

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



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 : ▪ 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	

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	Formulaire de demande d'accès Artemis (http umento.alize.finances.rie.gouv.fr/share/s/dbc2 Qr2kFh-9pvUrUw)

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 : ▪ depuis un poste de travail 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 confiance référencées (http://www.lsti-certification.fr/index.php/fr/certification/psce).	Validé	22/01/2020	Guide d'accès ARTEMIS (https://documento. nances.rie.gouv.fr/share/s/1NL0JIkkQ5mU-A sqA)

- La dernière modification de cette page a été faite le 30 novembre 2020 à 16:04.

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,2019 (https://fr.wikipedia.org/wiki/Environnement_(informatique)))

Un environnement est un ensemble de caractéristiques matérielles et logicielles d'un système informatique, qui est basé sur le système d'exploitation utilisé et qui a des implications sur la façon dont les logiciels d'application peuvent être exploités. (source : Office québécois de la langue française, 2005 (http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8355571))

Terme privilégié : **environnement**

Equivalent étranger: **environment** (en)

Sommaire

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 : ▪ 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 propriètaires (progiciels) développement basé sur un progiciel doit s'appuyer au moins sur les deux environnements : ▪ 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 décembre 2020 à 13:50.

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

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).	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) : ▪ 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: ▪ 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: ▪ 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 : ▪ 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 : ▪ Protocole FTP, ▪ Protocole FTPS.	Validé	03/12/2020	

Accès à distance (des agents)

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,2020 (https://fr.wikipedia.org/wiki/Acc%C3%A8s_%C3%A0_distance))

L'**accès à distance** est la possibilité de relier un ordinateur à un réseau ou à un poste de travail éloigné géographiquement.

(source : Institut Canadien des Comptables Agréés, 2006 (http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=504724))

Termes privilégiés :**accès à distance**, **téléaccès**, **accès distant**

Equivalent étranger: **remote access** (en)

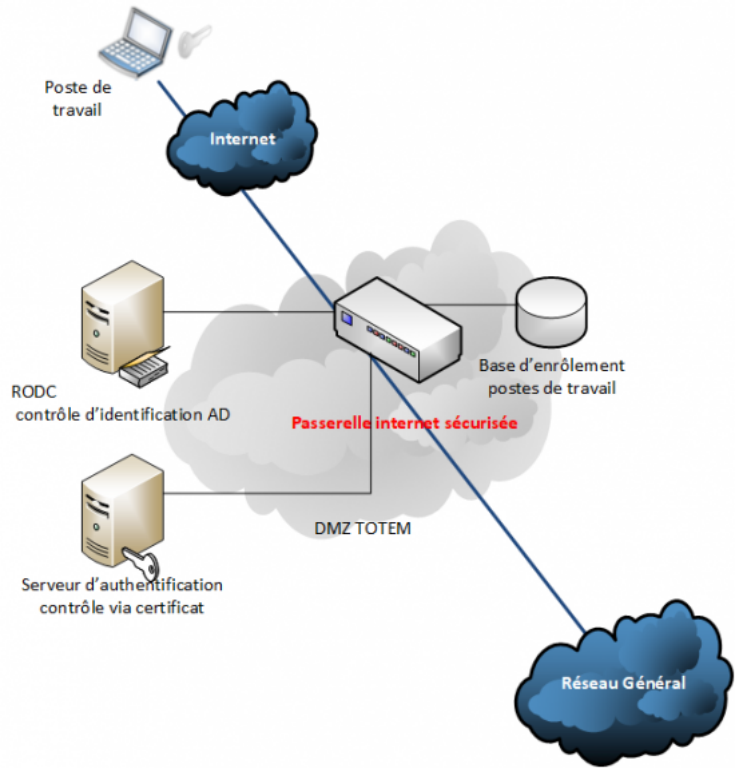
Sommaire

Contexte

L'offre d'accès à distance des agents de l'administration centrale proposée par SEP1 s'appuie sur la **solution TOTEM**.

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
Nouveauté	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
Nouveauté	2_8_6_4_001	L'accès à la solution TOTEM doit se faire : ▪ 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	
Nouveauté	2_8_6_4_002	Le package Client TOTEM doit être installé sur le poste de travail de l'Administration Centrale.	Validé	08/07/2020	

- La dernière modification de cette page a été faite le 13 juillet 2020 à 14:11.