

# Recommandations diffusables

Cette page recense l'ensemble des recommandations (règles) du cadre de cohérence technique (CCT) pouvant être diffusées à des tiers.

## Sommaire

- 1 Environnement d'exécution JAVA
- 2 Environnement d'exécution Microsoft .NET
- 3 Environnement d'exécution PHP
- 4 Gestionnaire d'accès à privilèges (ARTEMIS)
- 5 Gestionnaire d'anomalies (SAMA)
- 6 Gestionnaire de tests
- 7 Messagerie
- 8 Navigateur web
- 9 Sauvegarde
- 10 Serveur web Apache HTTP Server
- 11 Serveur d'application Apache Tomcat
- 12 Serveur mandataire inverse (SMI)
- 13 SGBD Microsoft SQL Server
- 14 SGBD Oracle Database Server
- 15 SGBD PostgreSQL
- 16 Suite bureautique
- 17 Système d'exploitation Red Hat Enterprise Linux (RHEL)
- 18 Système d'exploitation Rocky Linux
- 19 Système d'exploitation Microsoft Windows Server
- 20 Virtualisation

## Environnement d'exécution JAVA

**Info :** L'environnement d'exécution JAVA de référence s'appuie sur :

- le logiciel **JRE 21 et 17** pour les applications JAVA fonctionnant sur des serveurs Linux ou Windows
- le logiciel **JRE 8** pour les applications JAVA fonctionnant sur des postes de travail Windows

**Attention !** Il est déconseillé d'installer l'environnement d'exécution JAVA sur les postes de travail bureautiques pour des raisons de sécurité.

N° règle	Libellé de la règle	Statut	Commentaires
JAVA.2.201	L'environnement d'exécution JAVA <b>doit</b> être installé dans des versions à jour des correctifs de sécurité.	Validé	CERTFR : Vulnérabilités dans Oracle Java SE
JAVA.2.202	L'installation et la mise à jour de l'environnement d'exécution JAVA sur les serveurs Linux <b>doivent</b> être réalisées depuis la solution VMware Aria Automation Orchestrator.	Validé	Environnement d'exécution proposé avec le serveur d'application Tomcat.
JAVA.2.203	Les nouvelles applications <b>ne doivent pas</b> nécessiter l'installation de l'environnement d'exécution JAVA sur les postes de travail bureautiques.	Validé	
JAVA.2.204	L'installation et la mise à jour de l'environnement d'exécution JAVA sur les postes de travail <b>doivent</b> être réalisées depuis la solution Ivanti Endpoint Management (GAIA).	Validé	

## Environnement d'exécution Microsoft .NET

**Info :** L'environnement d'exécution Microsoft .NET de référence s'appuie sur :

- le logiciel **Microsoft .NET 8 (LTS)** pour les applications Microsoft .NET fonctionnant sur des serveurs Windows
- le logiciel **Microsoft .NET Framework 4.8** pour les applications Microsoft .NET fonctionnant sur des postes de travail Windows

N° règle	Libellé de la règle	Statut	Commentaires
NET.2.201	L'environnement d'exécution Microsoft .NET <b>doit</b> être installé dans des versions à jour des correctifs de sécurité.	Validé	CERT-FR : Vulnérabilités dans Microsoft .NET
NET.2.202	L'installation de l'environnement d'exécution Microsoft .NET sur les serveurs Windows <b>doit</b> être réalisée depuis le site officiel de l'éditeur.	Validé	
NET.2.203	La mise à jour de l'environnement d'exécution Microsoft .NET sur les serveurs Windows <b>doit</b> être réalisée depuis le serveur de dépôt interne WSUS.	Validé	Migration en cours de WSUS vers EPM avec une échéance prévue au 31/03/2025.
NET.2.204	L'installation de l'environnement d'exécution Microsoft .NET sur les postes de travail Windows <b>doit</b> être réalisée depuis le site officiel de l'éditeur.	Validé	
NET.2.205	La mise à jour de l'environnement d'exécution Microsoft .NET sur les postes de travail Windows <b>doit</b> être réalisée depuis le serveur de dépôt interne WSUS.	Validé	

## Environnement d'exécution PHP

**Info :** L'environnement d'exécution PHP de référence s'appuie sur :



- le logiciel **Apache HTTP Server 2.4**
- le logiciel **PHP 8.4 et 8.2**

pour les applications PHP fonctionnant sur des serveurs Linux

**Attention !** L'installation de l'environnement d'exécution PHP étant spécifique (**installation à partir du code source** et non à partir de paquets RPM), il sera donc préinstallé sur les serveurs virtuels (VM) Linux au travers la solution VMware Aria Automation Orchestrator.



Par ailleurs, compte tenu du nombre de versions proposées par la communauté PHP, il a été décidé de ne retenir qu'une version sur deux du logiciel PHP. La prochaine version éligible sera donc PHP 8.6

N° règle	Libellé de la règle	Statut	Commentaires
PHP.2.201	L'environnement d'exécution PHP <b>doit</b> être installé dans des versions à jour des correctifs de sécurité.	Validé	CERT-FR : Vulnérabilités dans PHP CERT-FR : Vulnérabilités dans Symfony
PHP.2.202	L'installation et la mise à jour de l'environnement d'exécution PHP sur les serveurs Linux <b>doivent</b> être réalisées depuis depuis la solution VMware Aria Automation Orchestrator.	Validé	Script shell spécifique "build-php" Liste des modules autorisés PHP ( <a href="https://documenta.alize.finances.rie.gouv.fr/share/s/zOvDrOaGSVaxkBw_Fqo4xA">https://documenta.alize.finances.rie.gouv.fr/share/s/zOvDrOaGSVaxkBw_Fqo4xA</a> )

## Gestionnaire d'accès à privilèges (ARTEMIS)

**Info :** Le gestionnaire d'accès à privilèges de référence pour les prestataires s'appuie sur :



- le logiciel **Wallix Access Bastion 10.9**
- le logiciel **Ivanti Secure Access Client 22.7**

N° règle	Libellé de la règle	Statut	Commentaires
PAM.2.201	Le gestionnaire d'accès à privilèges de référence <b>doit</b> être installée dans des versions à jour des correctifs de sécurité.	Validé	
PAM.2.301	L'accès à distance des prestataires aux serveurs <b>doit</b> se faire uniquement que sur les environnements de développement au travers des protocoles suivants: <ul style="list-style-type: none"><li>▪ Protocole RDP pour les serveurs Windows</li><li>▪ Protocole SSH pour les serveurs Linux</li></ul>	Validé	
PAM.2.302	L'accès à distance des prestataires aux serveurs au travers du protocole HTTPS <b>doit</b> se faire au travers d'un poste de rebond virtuel (VPR) et d'un compte nominatif communiqué par la maîtrise d'ouvrage de l'application.	Validé	
PAM.2.303	L'accès à distance des prestataires aux serveurs de base de données <b>doit</b> se faire avec un compte en lecture seule.	Validé	
PAM.2.304	L'accès à distance des prestataires au serveurs <b>doit</b> se faire au travers: <ul style="list-style-type: none"><li>▪ d'un poste de travail sous Microsoft Windows (10 ou 11) et d'un logiciel antivirus à jour</li><li>▪ d'un certificat d'authentification personnel conforme RGS (une * ou plus) acquis auprès l'une des autorités de confiance référencées.</li></ul>	Validé	

## Gestionnaire d'anomalies (SAMA)

**Info :** Le gestionnaire d'anomalies de référence (également appelé Suivi des anomalies logicielles - SAMA) s'appuie sur :



- le logiciel **Mantis Bug Tracker 2.25**

N° règle	Libellé de la règle	Statut	Commentaires
ANO.2.102	Toute demande d'intervention du prestataire chargé de la TMMA <b>doit</b> faire l'objet d'une saisie d'un ticket Mantis dans l'application SAMA.	Validé	
ANO.2.201	Le gestionnaire d'anomalies de référence <b>doit</b> être installé dans des versions à jour des correctifs de sécurité.	Validé	
ANO.2.301	<p>Les tickets Mantis saisis dans l'application SAMA (<a href="https://mantis.monportail.alize/index.php/">https://mantis.monportail.alize/index.php/</a>) <b>doivent</b> a minima respecter les règles de saisie suivantes:</p> <ul style="list-style-type: none"> <li>▪ Catégorie: nom du projet</li> <li>▪ Impact: Bloquant, Majeur ou Mineur</li> <li>▪ Type: <ul style="list-style-type: none"> <li>▪ INI pour les demandes d'initialisation des nouvelles applications,</li> <li>▪ EVO pour les demandes d'évolution,</li> <li>▪ SEC pour les demandes d'évolution du socle technique des applications intranet,</li> </ul> </li> <li>▪ Résumé: description succincte de la demande, préfixée du nom du projet, date de la demande</li> <li>▪ Environnement: Développement, Recette ou Production</li> </ul>	Validé	

## Gestionnaire de tests

**Info :** Le gestionnaire de tests de référence s'appuie sur :



- le logiciel **Squash TM 5.0**

N° règle	Libellé de la règle	Statut	Commentaires
TEST.2.201	Le gestionnaire de tests de référence <b>doit</b> être installé dans des versions à jour des correctifs de sécurité.	Validé	
TEST.2.301	<p>Le gestionnaire de tests de référence <b>doit</b> être utilisé:</p> <ul style="list-style-type: none"> <li>▪ lorsqu'une application fait l'objet d'une industrialisation de ses campagnes de tests;</li> <li>▪ lorsqu'une application nécessite la gestion d'un patrimoine de test à partir de la définition des exigences.</li> </ul>	Validé	

## Messagerie

**Info :** L'infrastructure mutualisée de messagerie de référence s'appuie sur :



- le logiciel **Microsoft Exchange Server 2016** pour les serveurs de boîte aux lettres
- le logiciel **Postix 3.9** pour les serveurs de relais de messagerie
- le logiciel **Microsoft Outlook LTSC 2021** pour les clients de messagerie

N° règle	Libellé de la règle	Statut	Commentaires
MSG.2.101	Les demandes d'interface avec le système de messagerie <b>doivent</b> être décrites dans le dossier d'architecture technique et complétées dans le formulaire de prise en charge associé.	Validé	
MSG.2.201	Les composants de l'infrastructure de messagerie <b>doivent</b> être installés dans des versions à jour des correctifs de sécurité.	Validé	
MSG.2.202	Les applications interfacées avec les serveurs de messagerie <b>doivent</b> privilégier le protocole EWS. A défaut, le protocole IMAP4 avec une connexion sécurisée via SSL/TLS peut être utilisé.	Validé	
MSG.2.203	Les applications devant accéder aux courriers électroniques d'une boîte aux lettres électroniques (BAL) <b>doivent</b> s'interfacer avec les serveurs de messagerie suivants: <ul style="list-style-type: none"> <li>Développement: webmail.caradev.finances.gouv.fr</li> <li>Recette: webmail.caradev.finances.gouv.fr</li> <li>Production: mel.finances.gouv.fr</li> </ul>	Validé	
MSG.2.204	Les applications envoyant des courriers électroniques <b>doivent</b> s'interfacer avec les serveurs de relais de messagerie suivants: <ul style="list-style-type: none"> <li>Développement <ul style="list-style-type: none"> <li>Relais internes: vvr-rel-iag.alize</li> <li>Mass-mailing: vvr-rel-iap.alize</li> <li>Relais externes: rec-re.finances.gouv.fr</li> </ul> </li> <li>Recette <ul style="list-style-type: none"> <li>Relais internes: vvr-rel-iag.alize</li> <li>Mass-mailing: vvr-rel-iap.alize</li> <li>Relais externes: rec-re.finances.gouv.fr</li> </ul> </li> <li>Production <ul style="list-style-type: none"> <li>Relais internes: relaismess.alize</li> <li>Mass-mailing: vip-vvp-rel-massmail</li> <li>Relais externes: relaismsg.finances.gouv.fr</li> </ul> </li> </ul>	Validé	
MSG.2.205	Les applications envoyant des courriers électroniques <b>doivent</b> respecter la règle de nommage suivante: <ul style="list-style-type: none"> <li>Développement <ul style="list-style-type: none"> <li>Relais internes: [fonction.direction]-dev@interne-rec.finances.gouv.fr</li> <li>Relais externes: [fonction.direction]-dev@recette.finances.gouv.fr</li> </ul> </li> <li>Recette <ul style="list-style-type: none"> <li>Relais internes: [fonction.direction]-rec@interne-rec.finances.gouv.fr</li> <li>Relais externes: [fonction.direction]-rec@recette.finances.gouv.fr</li> </ul> </li> <li>Production <ul style="list-style-type: none"> <li>Relais internes: [fonction.direction]@interne.finances.gouv.fr</li> <li>Relais externes: [fonction.direction]@applications.finances.gouv.fr</li> </ul> </li> </ul>	Validé	
MSG.2.206	Les serveurs de relais de messagerie "privés" (Exemple: les relais d'OVH) utilisés pour les applications exposées sur le réseau internet en utilisant un sous-domaine finances (exemple: applications.finances.gouv.fr) <b>doivent</b> se conformer aux standards SPF, DKIM et DMARC.	Validé	
MSG.2.207	Les postes de travail <b>ne doivent pas</b> s'interfacer directement sur les serveurs de relais de messagerie MTA via le protocole SMTP.	Validé	
MSG.2.208	Seuls les serveurs exposés sur les zones intranet <b>peuvent</b> s'interfacer avec les serveurs de messagerie MDA.	Validé	
MSG.2.209	<b>Il est interdit</b> de transférer automatiquement des courriels des boîtes aux lettres (BAL) utilisateur / partagée vers des boîtes aux lettres (BAL) externes (hors administration centrale).	Validé	

## Navigateur web

**Info** : Les navigateurs web de référence s'appuient sur :



- le logiciel **Firefox ESR** pour les postes de travail
- le logiciel **Microsoft Edge** pour les postes de travail
- le logiciel **Brave** pour les terminaux mobiles

N° règle	Libellé de la règle	Statut	Commentaires
NAVIG.2.201	Les navigateurs web de référence <b>doivent</b> être installés dans des versions à jour des correctifs de sécurité.	Validé	CERT-FR: Vulnérabilités dans Firefox CERT-FR : Vulnérabilités dans Microsoft Edge
NAVIG.2.202	Le master déployé sur les postes de travail des agents de l'administration centrale <b>doit</b> intégrer: <ul style="list-style-type: none"> <li>le navigateur web Microsoft Edge</li> <li>le navigateur web Firefox ESR</li> </ul>	Validé	
NAVIG.2.203	Le navigateur web Mozilla Firefox ESR <b>doit</b> être paramétré en tant que navigateur par défaut sur l'ensemble des postes de travail des agents de l'administration centrale.	Validé	
NAVIG.2.204	La mise à jour du navigateur web Mozilla Firefox ESR <b>doit</b> se faire au travers de la solution ZENworks Configuration Management (ZCM).	Validé	
NAVIG.2.205	La mise à jour du navigateur Microsoft Edge <b>doit</b> se faire au travers de la solution Microsoft WSUS.	Validé	

## Sauvegarde

**Info :** L'infrastructure mutualisée de sauvegarde de référence s'appuie sur :



- la solution **Veritas Netbackup 10**

N° règle	Libellé de la règle	Statut	Commentaires
SVG.2.001	Toute mise en production d'un nouveau système, d'une nouvelle application ou d'un nouvel espace de données <b>doit</b> faire l'objet d'une réflexion préalable sur sa sauvegarde et d'un ajout au plan de sauvegarde.	Validé	Les contraintes particulières de sauvegarde doivent être précisées dans le DAT. Pour rappel : PDMA = 1 jour par défaut et durée de rétention = 60 jours max.
SVG.2.102	Les demandes de modification de plan de sauvegarde <b>doivent</b> faire l'objet d'une justification technique et d'une mise à jour du dossier d'architecture technique (DAT).	Validé	
SVG.2.103	Les demandes de restauration <b>doivent</b> se faire au travers de l'application PROMETHEE.	Validé	

## Serveur web Apache HTTP Server

**Info :** Le serveur web de référence pour les applications fonctionnant sur des serveurs Linux s'appuie sur :



- le logiciel **Apache HTTP Server 2.4**

**Attention !** Le serveur web Apache HTTP Server est à privilégier pour tout nouveau projet numérique réalisé dans un environnement Linux. L'utilisation d'un autre serveur web doit faire l'objet d'une justification technique à insérer dans le Dossier d'Architecture Technique (DAT) (<https://documento.alize.finances.rie.gouv.fr/share/s/TuQwZJ-qQcqHp0AlnUgiug>).

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

N° règle	Libellé de la règle	Statut	Commentaires
APACHE.2.201	Le logiciel libre Apache HTTP Server <b>doit</b> être installé dans des versions à jour des correctifs de sécurité.	Validé	
APACHE.2.202	L'installation et la mise à jour du logiciel libre Apache HTTP Server doivent être réalisées depuis: <ul style="list-style-type: none"> <li>la solution VMware Aria Automation Orchestrator pour les serveurs virtuels Linux</li> <li>le serveur de dépôt Linux interne pour les serveurs physiques Linux</li> </ul>	Validé	Liste des modules autorisés Apache
APACHE.2.203	L'installation du logiciel libre Apache HTTP Server <b>doit</b> respecter l'arborescence spécifique suivante: <ul style="list-style-type: none"> <li>répertoire /applis/apache-[version] contenant les fichiers binaires avec [version] correspondant au numéro de version du logiciel</li> <li>répertoire /applis/www/conf contenant des fichiers de configuration</li> </ul>	Validé	
APACHE.2.204	Les droits et les permissions qui s'appliquent aux répertoires et aux fichiers des serveurs web basés sur le logiciel libre Apache HTTP Server <b>doivent</b> respecter les propriétés suivantes: <ul style="list-style-type: none"> <li>Les répertoires avec des droits positionnés en 755 avec comme propriétaire "root" et groupe "root".</li> <li>Les fichiers avec des droits positionnés en 644 avec propriétaire "root" et groupe "root".</li> </ul>	Validé	
APACHE.2.205	Les droits et les permissions qui s'appliquent aux répertoires et aux fichiers des serveurs web basés sur le logiciel libre Apache HTTP Server <b>doivent</b> respecter les propriétés suivantes: <ul style="list-style-type: none"> <li>Les répertoires avec des droits positionnés en 775 et avec comme propriétaire "root" et groupe "apache"</li> <li>Les fichiers avec des droits positionnés en 664 et avec comme propriétaire "root" et groupe "apache"</li> </ul>	Validé	
APACHE.2.206	La racine des documents (DocumentRoot) <b>doit</b> être située dans le répertoire /applis/www/html/[nom_application] où [nom_application] est le nom de l'application.	Validé	
APACHE.2.207	La création de serveurs virtuels (VirtualHost) <b>doit</b> se faire dans le fichier /applis/www/conf/extra/httpd-vhosts.conf. 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.	Validé	
APACHE.2.208	Les fichiers log des serveurs web basés sur le logiciel libre Apache HTTP Server <b>doivent</b> être situés dans le répertoire /logs/apache	Validé	
APACHE.2.209	Les certificats TLS des serveurs web basés sur le logiciel libre Apache HTTP Server <b>doivent</b> être situés dans les répertoires: <ul style="list-style-type: none"> <li>/root/certif/certificat_genere/[nom_certificat].crt</li> <li>/root/certif/certificat_key_serveur/[nom_certificat].key</li> </ul> où [nom_certificat] est le nom du certificat.	Validé	Les certificats auto-signés sont autorisés sur les serveurs web
APACHE.2.210	Les échanges entre le navigateur web et les serveurs web <b>doivent</b> transiter par des dispositifs mutualisés de sécurité de type: <ul style="list-style-type: none"> <li>Serveur mandataire inverse (SMI)</li> <li>Serveur d'authentification unique (SSO)</li> </ul>	Validé	Ces dispositifs de sécurité portent notamment la réécriture d'URL ainsi que la stratégie de sécurité de contenus.
APACHE.2.211	Le code erreur HTTP 404 renvoyé par un serveur web <b>doit</b> donner lieu à une redirection vers une page d'erreur prédéfinie indiquant "Page introuvable".	Validé	
APACHE.2.212	Le code erreur HTTP 503 renvoyé par un serveur web <b>doit</b> donner lieu à une redirection vers une page d'erreur prédéfinie indiquant "Page indisponible provisoirement"	Validé	
APACHE.2.213	Le code erreur HTTP 504 renvoyé par un serveur web <b>doit</b> donner lieu à une redirection vers une page d'erreur prédéfinie indiquant "Application en maintenance".	Validé	

## Serveur d'application Apache Tomcat

**Info :** Le serveur d'application de référence pour les applications fonctionnant sur des serveurs Linux s'appuie sur :



- le logiciel **Apache Tomcat 10.1**.



**Attention !** Le serveur d'application Apache Tomcat est à privilégier pour tout nouveau projet numérique réalisé dans un environnement Linux. L'utilisation d'un autre serveur d'application doit faire l'objet d'une justification technique à insérer dans le Dossier d'Architecture Technique (DAT) (<https://documento.alize.finances.rie.gouv.fr/share/s/TuQwZJ-qQcqHp0AlnUgiug>).



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

N° règle	Libellé de la règle	Statut	Commentaires
TOMCAT.2.201	Les serveurs d'application Apache Tomcat <b>doivent</b> être installés dans des versions à jour des correctifs de sécurité.	Validé	
TOMCAT.2.202	L'installation et la mise à jour des serveurs d'application Apache Tomcat sur les serveurs Linux <b>doivent</b> être réalisées depuis la solution VMware Aria Automation Orchestrator.	Validé	
TOMCAT.2.203	<p>L'installation du logiciel libre Apache Tomcat <b>doit</b> respecter l'arborescence suivante:</p> <ul style="list-style-type: none"> <li>▪ Répertoire des fichiers binaires: /applis/apache-tomcat-[version]/bin</li> <li>▪ Répertoire des fichiers externalisés de Tomcat (conf, bin (setenv.sh seulement), keystore et webapps): /applis/apache-tomcat-files</li> <li>▪ Lien symbolique pointant vers la dernière version de Tomcat installée: /applis/apache-tomcat</li> </ul> <p>où [version] correspond au numéro de version du logiciel.</p>	Validé	
TOMCAT.2.204	Les fichiers log du logiciel libre Apache Tomcat <b>doivent</b> être localisés dans le répertoire /logs/tomcat	Validé	La rotation des fichiers log est gérée par le démon apache-tomcat et non par le démon logrotate.
TOMCAT.2.205	Les applications livrées sous forme de fichiers WAR <b>doivent</b> être installées dans le répertoire /applis/apache-tomcat-files/webapps	Validé	Ce répertoire est indiqué dans le fichier de configuration du serveur /applis/apache-tomcat-\$version/conf/server.xml .
TOMCAT.2.206	Un lien symbolique nommé "apache-tomcat" <b>doit</b> pointer sur le dossier d'installation de la dernière version de Tomcat installée et <b>doit</b> être placé dans le répertoire /applis	Validé	
TOMCAT.2.207	<p>Les droits et les permissions qui s'appliquent aux répertoires et aux fichiers des serveurs d'application basés sur le logiciel libre Apache-tomcat <b>doivent</b> respecter les propriétés suivantes:</p> <ul style="list-style-type: none"> <li>▪ Les répertoires <b>doivent</b> avoir des droits positionnés en 755 avec comme propriétaire "tomcat" et groupe "tomcat".</li> <li>▪ Les exécutables *.sh dans le répertoire bin (applis/apache-tomcat-[version]/bin et /applis/apache-tomcat-files/bin) <b>doivent</b> avoir les droits positionnés en 755 avec comme propriétaire "tomcat" et groupe "tomcat".</li> </ul> <p>Les fichiers <b>doivent</b> avoir des droits positionnés en 644 avec propriétaire "tomcat" et groupe "tomcat".</p>	Validé	\$ {version} est le premier digit du numéro de version apache-tomcat
TOMCAT.2.208	<p>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 <b>doivent</b> respecter les propriétés suivantes:</p> <ul style="list-style-type: none"> <li>▪ Les répertoires <b>doivent</b> avoir des droits positionnés en 755 avec comme propriétaire "tomcat" et groupe "tomcat"</li> </ul> <p>Les fichiers <b>doivent</b> avoir des droits positionnés en 644 avec comme propriétaire " tomcat" et groupe "tomcat".</p>	Validé	
TOMCAT.2.209	Les certificats TLS des serveurs d'application et leur clé privée associée <b>doivent</b> être stockés dans un keystore.Ce keystore doit être placé dans le répertoire /applis/apache-tomcat-files/keystore/[nom_keystore].p12où [nom_keystore] est le nom du keystore.(L'extension du keystore peut varier entre .p11, .p12 et .jks selon le format utilisé).	Validé	
TOMCAT.2.210	<p>Les échanges entre le navigateur web et les serveurs web doivent transiter par des dispositifs mutualisés de sécurité de type:</p> <ul style="list-style-type: none"> <li>▪ Serveur mandataire inverse (SMI)</li> <li>▪ Serveur d'authentification unique (SSO)</li> </ul>	Validé	
TOMCAT.2.211	Le fichier de service de Tomcat (/etc/systemd/system/apache-tomcat.service) ne <b>doit</b> pas être modifié. La définition des différentes variables d'environnement utilisées par Apache Tomcat <b>doit</b> se faire dans le fichier setenv.sh situé dans /applis/apache-tomcat-files/bin	Validé	
TOMCAT.2.212	Les serveurs d'application <b>doivent</b> récupérer le champ X-Forwarded-For transmis par les serveurs mandataires inverses (SMI) ou les serveurs d'authentification (SSO) et le faire figurer dans les journaux.	Validé	

## Serveur mandataire inverse (SMI)

**Info :** L'infrastructure mutualisée de serveurs mandataires inverses (SMI) de référence pour les applications fonctionnant sur des serveurs Windows et Linux s'appuie sur :



- le logiciel **Apache HTTP Server 2.4.**

N° règle	Libellé de la règle	Statut	Commentaires
SMI.2.201	Les échanges entre le navigateur web et les serveurs web et applicatifs <b>doivent</b> transiter par des dispositifs mutualisés de sécurité de type: <ul style="list-style-type: none"> <li>▪ Serveur mandataire inverse (SMI)</li> <li>▪ Serveur d'authentification unique (SSO)</li> </ul>	Validé	
SMI.2.202	Les applications exposées sur le réseau général (RG),le réseau interministériel de l'Etat (RIE) et interfacées avec les serveurs mandataires inverses (SMI) <b>doivent</b> utiliser les règles de nommage des URL suivantes : <u>Environnement de développement</u> URL accessible en https://[nom_appli]-dev.alize.finances.rie.gouv.fr et redirigée vers l'URL https://[nom_appli]-dev-bo.alize.finances.rie.gouv.fr <u>Environnement de recette</u> URL accessible en https://[nom_appli]-rec.alize.finances.rie.gouv.fr et redirigée vers l'URL https://[nom_appli]-rec-bo.alize.finances.rie.gouv.fr <u>Environnement de production</u> URL accessible en https://[nom_appli].alize.finances.rie.gouv.fr et redirigée vers l'URL https://[nom_appli]-bo.alize.finances.rie.gouv.fr où [nom_appli] est le nom de l'application.	Validé	
SMI.2.203	Les applications exposées sur le réseau internet et interfacées avec les serveurs mandataires inverses (SMI) <b>doivent</b> utiliser les règles de nommage des URL suivantes: <u>Environnement de développement</u> URL accessible en https://[nom_appli]-internet-dev.alize.finances.rie.gouv.fr et redirigée vers l'URL https://[nom_appli]-internet-dev-bo.alize.finances.rie.gouv.fr <u>Environnement de recette</u> URL accessible en https://[nom_appli]-rec.finances.gouv.fr et redirigée vers l'URL https://[nom_appli]-rec-bo.finances.gouv.fr <u>Environnement de production</u> URL accessible en https://[nom_appli].finances.gouv.fr et redirigée vers l'URL https://[nom_appli]-bo.finances.gouv.fr où [nom_appli] est le nom de l'application.	Validé	
SMI.2.204	Les stratégies de sécurité des contenus (CSP) spécifiées dans le Guide de paramétrage SSL et entête HTTP (https://documento.alize.finances.rie.gouv.fr/share/s/C0IP3D2IQpu-9pXX31mdLA) <b>doivent</b> être appliquées sur les SMI telles que rédigées dans le fichier de références sepc-ssi-1.2-B.conf (https://documento.alize.finances.rie.gouv.fr/share/s/f7oaAdV6Qe0C4QostsjmQ).	Validé	Cette recommandation 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'.
SMI.2.205	Les stratégies de sécurité des contenus (CSP) spécifiées dans le Guide de paramétrage SSL et entête HTTP (https://documento.alize.finances.rie.gouv.fr/share/s/C0IP3D2IQpu-9pXX31mdLA) étant appliquées sur les serveurs mandataires inverses (SMI) <b>ne doivent pas</b> être appliquées sur les serveurs web hébergeant les applications.	Validé	
SMI.2.206	Les feuilles de style <b>doivent</b> être dans l'entête et non dans le corps de la page HTML. En cas d'usage des paramètres 'unsafe-eval' 'unsafe-inline' et style-src 'self', ils doivent être validés en comité d'homologation.	Validé	
SMI.2.207	Les serveurs mandataires inverses (SMI) <b>doivent</b> respecter les règles décrites dans le Guide de paramétrage SSL et entête HTTP (https://documento.alize.finances.rie.gouv.fr/share/s/C0IP3D2IQpu-9pXX31mdLA).	Validé	Fichier de stratégie de sécurité des contenus (https://documento.alize.finances.rie.gouv.fr/share/s/f7oaAdV6Qe0C4QostsjmQ)

## SGBD Microsoft SQL Server

**Info** : Le SGBD mutualisé de référence pour les applications fonctionnant sur des serveurs Windows s'appuie sur :



- le logiciel **Microsoft SQL Server 2017 standard**



**Attention** ! Cette version du SGBD Microsoft SQL Server est à privilégier pour tout nouveau projet numérique réalisé dans un environnement Windows. L'utilisation d'un autre SGBD doit faire l'objet d'une justification technique à insérer dans le Dossier d'Architecture Technique (DAT) (https://documento.alize.finances.rie.gouv.fr/share/s/TuQwZJ-qQcHp0AlnUgiug).

N° règle	Libellé de la règle	Statut	Commentaires
MSQL.2.201	Le logiciel propriétaire Microsoft Microsoft SQL Server <b>doit</b> être installé dans des versions à jour des correctifs de sécurité	Validé	
MSQL.2.202	L'installation du logiciel propriétaire Microsoft Microsoft SQL Server sur les serveurs Windows <b>doit</b> être réalisée depuis le site officiel de l'éditeur.	Validé	
MSQL.2.203	Les mises à jour du logiciel propriétaire Microsoft Microsoft SQL Server sur les serveurs Windows <b>doivent</b> être réalisées depuis le serveur de dépôt interne Microsoft WSUS.	Validé	

## SGBD Oracle Database Server

**Info** : Le SGBD mutualisé de référence pour les applications fonctionnant sur des serveurs Linux s'appuie sur le logiciel libre SGBD PostgreSQL. Cependant, certaines infrastructures ou applications peuvent nécessiter l'utilisation d'une autre SGBD. Elles doivent dans ce cas s'appuyer sur



- le logiciel propriétaire **Oracle Database Server 19C**.



**Attention !** L'utilisation de ce SGBD Linux doit faire l'objet d'une justification technique à insérer dans le Dossier d'Architecture Technique (DAT) (<https://document.o.alize.finances.rie.gouv.fr/share/s/TuQwZJ-qQcHp0AlnUgiug>).

N° règle	Libellé de la règle	Statut	Commentaires
ORA.2.201	Le SGBD Oracle <b>doit</b> être installé dans des versions à jour des correctifs de sécurité.	Validé	
ORA.2.202	L'installation et la mise à jour du SGBD Oracle sur les serveurs Linux <b>doivent</b> être réalisées depuis le site de l'éditeur.	Validé	
ORA.2.203	Le codage des caractères informatiques dans le SGBD Oracle avec des clients Windows <b>doit</b> être basé sur Windows-1252.	Validé	

## SGBD PostgreSQL

**Info :** Le SGBD de référence pour les applications fonctionnant sur des serveurs Linux s'appuie sur :



- le logiciel **PostgreSQL 17**.

**Attention !** Le SGBD PostgreSQL est à privilégier pour tout nouveau projet numérique réalisé dans un environnement Linux. L'utilisation d'un autre SGBD (Oracle, MySQL, etc.) doit faire l'objet d'une justification technique à insérer dans le Dossier d'Architecture Technique (DAT) (<https://document.o.alize.finances.rie.gouv.fr/share/s/TuQwZJ-qQcHp0AlnUgiug>).

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

**Attention !** Par ailleurs, compte tenu du nombre de versions proposées par la communauté PostgreSQL, il a été décidé de ne retenir qu'une version sur deux du logiciel PostgreSQL. La prochaine version éligible sera donc PostgreSQL 19

N° règle	Libellé de la règle	Statut	Commentaires
PSQL.2.201	Le SGBD PostgreSQL <b>doit</b> être installé dans des versions à jour des correctifs de sécurité	Validé	
PSQL.2.202	L'installation et la mise à jour du SGBD PostgreSQL sur les serveurs Linux <b>doivent</b> être réalisées depuis l'orchestrateur VMware Orchestrator.	Validé	
PSQL.2.203	Le codage des caractères informatiques dans le SGBD PostgreSQL <b>doit</b> être basé sur UTF-8.	Validé	

## Suite bureautique

**Info :** Les suites bureautiques de référence fonctionnant sur les postes de travail s'appuient sur :



- le logiciel **Libre Office 24**
- le logiciel **Microsoft Office LTSC Professionnel Plus 2021**

N° règle	Libellé de la règle	Statut	Commentaires
OFFICE.2.201	Les suites bureautiques de référence <b>doivent</b> être installés dans des versions à jour des correctifs de sécurité.	Validé	
OFFICE.2.202	Le master déployé sur les postes de travail des agents de l'administration centrale <b>doit</b> intégrer: <ul style="list-style-type: none"><li>la suite bureautique Libre Office</li><li>la suite bureautique Microsoft Office</li></ul>	Validé	
OFFICE.2.203	La mise à jour de la suite bureautique Libre Office <b>doit</b> se faire au travers de la solution ZENworks Configuration Management (ZCM).	Validé	Migration en cours de ZCM vers EPM avec une échéance prévue au 31/03/2025.
OFFICE.2.204	La mise à jour de la suite bureautique Microsoft Office <b>doit</b> se faire depuis un serveur bureautique.	Validé	La mise à jour de Microsoft Office n'est plus possible depuis WSUS.

## Système d'exploitation Red Hat Enterprise Linux (RHEL)

**Info :** Le système d'exploitation de référence pour les applications fonctionnant sur des serveurs Linux s'appuie sur le logiciel libre Rocky Linux. Cependant, certaines infrastructures ou applications peuvent nécessiter l'utilisation d'une distribution Linux commerciale. Elles doivent dans ce cas s'appuyer sur



- le logiciel propriétaire **Red Hat Enterprise Linux (RHEL) 8.10**.

**Attention !** L'utilisation de ce système d'exploitation Linux doit faire l'objet d'une justification technique à insérer dans le Dossier d'Architecture Technique (DAT) (<https://documento.alize.finances.rie.gouv.fr/share/s/TuQwZJ-qQcqHp0AInUgiug>).

N° règle	Libellé de la règle	Statut	Commentaires
RHEL.2.201	Le logiciel propriétaire Red Hat Enterprise Linux <b>doit</b> être installé dans des versions à jour des correctifs de sécurité.	Validé	
RHEL.2.202	L'installation du logiciel propriétaire Red Hat Enterprise Linux <b>doit</b> être réalisée à partir de l'image ISO depuis le serveur de dépôt officiel de l'éditeur.	Validé	
RHEL.2.203	La mise à jour du logiciel propriétaire Red Hat Enterprise Linux <b>doit</b> être réalisée à partir de l'image ISO depuis le serveur de dépôt officiel de l'éditeur.	Validé	

## Système d'exploitation Rocky Linux

**Info :** Le système d'exploitation de référence pour les applications fonctionnant sur des serveurs Linux s'appuie sur :



- le logiciel **Rocky Linux 9.5**

**Attention !** Le système d'exploitation Rocky Linux fait l'objet d'un durcissement (sécurisation du système) en appliquant les principales recommandations du CIS Rocky Linux 9 Benchmark].

**Attention !** L'utilisation d'un autre système d'exploitation Linux doit faire l'objet d'une justification technique à insérer dans le Dossier d'Architecture Technique (DAT) (<https://documento.alize.finances.rie.gouv.fr/share/s/TuQwZJ-qQcqHp0AInUgiug>).

N° règle	Libellé de la règle	Statut	Commentaires
ROCKY.2.201	Le logiciel libre Rocky Linux <b>doit</b> être installé dans des versions à jour des correctifs de sécurité.	Validé	
ROCKY.2.202	L'installation du logiciel libre Rocky Linux <b>doivent</b> être réalisée à partir de l'image ISO disponible depuis le serveur de dépôt Linux interne.	Validé	
ROCKY.2.203	La mise à jour du logiciel libre Rocky Linux <b>doivent</b> être réalisée à partir de l'image ISO disponible depuis le serveur de dépôt Linux interne	Validé	

## Système d'exploitation Microsoft Windows Server

**Info :** Le système d'exploitation de référence pour les applications fonctionnant sur des serveurs Windows s'appuie sur :



- le logiciel **Microsoft Windows Server 2019**

**Attention !** L'utilisation d'une autre version de ce système d'exploitation doit faire l'objet d'une justification technique à insérer dans le Dossier d'Architecture Technique (DAT) (<https://documento.alize.finances.rie.gouv.fr/share/s/TuQwZJ-qQcqHp0AInUgiug>).

N° règle	Libellé de la règle	Statut	Commentaires
MWS.2.201	Le logiciel propriétaire Microsoft Windows Server <b>doit</b> être installé dans des versions à jour des correctifs de sécurité.	Validé	
MWS.2.202	L'installation du logiciel propriétaire Microsoft Windows Server <b>doit</b> être réalisée depuis l'image ISO disponible sur le site de l'éditeur.	Validé	
MWS.2.203	La mise à jour du logiciel propriétaire Microsoft Windows Server <b>doit</b> être réalisée depuis le serveur de dépôt Windows interne (WSUS).	Validé	

## Virtualisation

**Info :** L'infrastructure mutualisée de virtualisation de référence pour les applications fonctionnant sur des serveurs Windows et Linux s'appuie sur :



- la solution **Broadcom VMware vSphere Foundation 8**

N° règle	Libellé de la règle	Statut	Commentaires
VRT.2.101	Les demandes de création de VM <b>doivent</b> se faire au travers de l'application PROMETHEE	Validé	
VRT.2.102	Les demandes de modification des ressources (CPU, RAM, interface réseau, espace disque) d'une VM <b>doivent</b> faire l'objet d'une justification technique et d'une mise à jour du dossier d'architecture technique (DAT).	Validé	
VRT.2.103	Les demandes de support logiciel sur l'infrastructure de virtualisation <b>peuvent</b> se faire auprès de l'éditeur.	Validé	
VRT.2.201	<p>La configuration des VM en termes de CPU, RAM et espace de stockage <b>doit</b> être adaptée au mieux des composants applicatifs hébergés dessus. Les quantités de ressources matérielles configurables en standard sur une VM sont:</p> <ul style="list-style-type: none"> <li>■ CPU: 1, 2, 4 ou 8 vCPU</li> <li>■ RAM: 1,2, 4, 6, 8, 10, 12, 14 ou 16 Go</li> <li>■ Espace de stockage système: 60 Go (serveurs Linux) et 100 Go (serveurs Windows).</li> </ul> <p>L'extension des ressources matérielles au delà des valeurs ci-dessus <b>doit</b> faire l'objet d'une justification technique.</p>	Validé	
VRT.2.202	Les ressources (vCPU, RAM et espace de stockage) attribuées à une VM <b>ne doivent pas</b> être réutilisées pour d'autres besoins.	Validé	
VRT.2.203	<p>Les VM <b>doivent</b> respecter les règles de nommage suivantes:</p> <ul style="list-style-type: none"> <li>■ VVC-[nom-appli] pour les serveurs "clone"</li> <li>■ VVD-[nom-appli] pour les serveurs de développement</li> <li>■ VVR-[nom-appli] pour les serveurs de recette</li> <li>■ VVF-[nom-appli] pour les serveurs de formation</li> <li>■ VVT-[nom-appli] pour les serveurs de test</li> <li>■ VVPP-[nom-appli] pour les serveurs de pré-production</li> <li>■ VVP-[nom-appli] pour les serveurs de production</li> <li>■ VVRS-[nom-appli] pour les serveurs de recette (environnement de secours)</li> <li>■ VVS-[nom-appli] pour les serveurs de production (environnement de secours)</li> <li>■ [Direction]-VPC[Numéro d'ordre] pour les postes d'administration</li> <li>■ [Direction]-VPR[numéro d'ordre] pour les postes de rebond</li> </ul>	Validé	
VRT.2.204	<p>Les appliances virtuelles <b>doivent</b> respecter les règles de nommage suivantes:</p> <ul style="list-style-type: none"> <li>■ APC-[nom-appli] pour les appliances "clone"</li> <li>■ APD-[nom-appli] pour les appliances de développement</li> <li>■ APR-[nom-appli] pour les appliances de recette</li> <li>■ APF-[nom-appli] pour les appliances de formation</li> <li>■ APT-[nom-appli] pour les appliances de test</li> <li>■ APPP-[nom-appli] pour les appliances de pré-production</li> <li>■ APP-[nom-appli] pour les appliances de production</li> <li>■ APRS-[nom-appli] pour les appliances de recette (environnement de secours)</li> <li>■ APS-[nom-appli] pour les appliances de production (environnement de secours)</li> </ul>	Validé	
VRT.2.205	<p>Les systèmes d'exploitation déployés sur les VM <b>doivent</b> être choisis parmi la liste ci-dessous:</p> <ul style="list-style-type: none"> <li>■ Microsoft Windows Server 2019</li> <li>■ Rocky Linux 9</li> <li>■ RHEL 9 (en cas d'incompatibilité avec Rocky Linux 9)</li> <li>■ Microsoft Windows 11 Pro</li> </ul>	Validé	

Récupérée de « [https://wiki.monportail.alize/cct/w/index.php?title=Recommandations\\_diffusables&oldid=22140](https://wiki.monportail.alize/cct/w/index.php?title=Recommandations_diffusables&oldid=22140) »

- La dernière modification de cette page a été faite le 29 avril 2025 à 07:22.