Le Sénat

CONCOURS D'INFORMATICIEN PROFILS « ADMINISTRATEUR SYSTÈMES » ET « DÉVELOPPEUR »

SUJETS DONNÉS AU CONCOURS 2018-2019

IMPORTANT

Le programme étant toujours susceptible d'être modifié, cette brochure est fournie à titre purement indicatif.

Pour tout renseignement complémentaire concernant ce concours les candidats peuvent s'adresser à la :
Direction des Ressources humaines et de la Formation du Sénat
15, rue de Vaugirard – 75291 Paris cedex 06
Internet : http://www.senat.fr/emploi – Courriel : concours-rhf@senat.fr

SÉNAT

SOMMAIRE

ÉPREUVES ÉCRITES D'ADMISSIBILITÉ

1. Questionnaire à choix multiples

Ce questionnaire à choix multiples est destiné à tester les connaissances de culture informatique générale des candidats.

(durée 1 heure – coefficient 2)

2. Épreuve technique

Cette épreuve est destinée à tester les connaissances techniques et informatiques des candidats.

Selon le profil d'emploi pour lequel ils concourent, les candidats devront répondre :

Pour le profil « développement », à des questions portant sur la programmation, la logique, l'algorithmie. Pour répondre aux questions de programmation, les candidats devront choisir parmi les langages suivants : C/C++, Java.

Pour le profil « administration des systèmes », à des questions portant sur les infrastructures informatiques, les systèmes d'exploitation, les bases de données, le réseau, la sécurité, la gestion de postes de travail et la téléphonie IP.

(durée 2 heures – coefficient 3)

3. Étude de cas

Selon le profil pour lequel ils concourent, les candidats devront réaliser :

Pour le profil « développement », l'étude d'un projet applicatif comportant l'analyse du besoin, la conception, les choix techniques, le détail de la réalisation proposée (diagrammes pertinents en fonction de la méthode d'analyse et de conception choisie par le candidat, choix des modules) ;

Pour le profil « administration des systèmes », l'étude d'un projet d'évolution d'architecture, comportant des choix techniques et leur justification par rapport aux besoins, et prenant en compte les aspects systèmes, bases de données, réseaux, exploitation, déploiement, sécurité, optimisation des processus productifs.

Le dossier remis aux candidats pour cette épreuve pourra comporter des documents rédigés en anglais.

(durée 4 heures – coefficient 5)

1. Questionnaire à choix multiples

(durée 1 heure – coefficient 2)

1 Quelle est l'espérance mathématique pour une question répondue au hasard, si une bonne réponse rapporte 1 point et une mauvaise -0,5 point, lorsque le nombre de choix possibles du QCM est de trois ?

A. 0,5
B. 0,33
C. 0
D. -0,5

2 Que signifie le sigle IP ?

A. Internet Protocol
B. Internal Protocol
C. Internet Package

3 Qu'est ce qui caractérise des câbles en fibre optique ?

A. Ils conduisent l'électricité
B. Ils ne conduisent pas l'électricité
C. Ils sont très flexibles (rayon de courbure faible)

4 Parmi les adresses IP suivantes, laquelle n'est pas valide ?

A. 169.36.125.0
B. 1.2.3.4
C. 147.126.256.9

5 La commande « ping » sert à :

A. Compter le nombre de routeurs permettant d'atteindre une machine distante
B. Vérifier le temps de réponse d'une machine distante
C. Connaître le chemin pour atteindre une machine distante

6 Pour communiquer au niveau IP, deux ordinateurs ont besoin :

A. D'être dans le même réseau IP avec le même masque de sous réseau
B. D'avoir au moins 200Mbps de bande passante
C. D'avoir une adresse IP configurée manuellement

7 Qu'est-ce que le SMTP ?

A. Un protocole de transmission de courrier électronique
B. Un protocole de réception de courrier électronique sécurisé
C. Un protocole réseau pour internet

8 Dans la commande « chmod o+r fichier », « o » désigne :

A. Les propriétaires
B. Les groupes
C. Les autres

9 Quelle est la signification du sigle HTML ?

A. HyperText Markup Language
B. HardText Markup Language
C. HardText Marketing Learning

10 Quelle proposition ne fait pas partie de la version officielle du « Manifeste pour le développement Agile de logiciels » publié en 2001 ?

A. Une usine logicielle plus que du développement artisanal
B. Les individus et leurs interactions plus que les processus et les outils
C. Des logiciels opérationnels plus qu'une documentation exhaustive
D. La collaboration avec les clients plus que la négociation contractuelle

11 Dans un sélecteur CSS, quel caractère permet de sélectionner un élément du DOM par son identifiant ?

A. # (« dièse »)
B. . (« point »)
C. $ (« dollar »)

12 Sélectionnez la phrase correcte :

A. TCP utilise IP
B. IP et TCP sont inséparables
C. IP utilise TCP

13 À quoi sert l'attribut « alt » de la balise « img » en HTML ?

A. À définir la hauteur de l'image à afficher à l'écran
B. À définir une version basse définition de l'image en cas d'utilisation sur mobile
C. À définir une alternative textuelle à l'image
D. Cet attribut n'existe que pour la balise « input »

14 En JavaScript, quelle est la valeur de retour de l'instruction suivante : 4 + "3" ?

A. "43"
B. 7
C. NaN
D. NaNNaN

15 Un site en « responsive design » permet de s'adapter en fonction :

A. De la résolution de l'écran du périphérique qui le consulte
B. Du nombre d'utilisateurs qui le consultent
C. Du temps de réponse avec le client

16 Laquelle de ces propositions est valide ?

A. HTTP est un protocole dit « stateless » mais les serveurs HTTP implémentent des techniques permettant de gérer des sessions
B. HTTP est un protocole dit « stateful »
C. Le protocole HTTP peut être « stateful » ou « stateless »
D. Depuis HTTP/2, on ne peut plus considérer que HTTP est « stateless »

17 Lequel des éléments suivants n'est pas nécessaire pour pratiquer le DevOps ?

A. Des outils de suivi d'indicateurs
B. Une boucle d'amélioration courte (« feed-back rapide »)
C. Les méthodologies de programmation orientées objet
D. De la communication entre équipes

18 Que permet le protocole IPv4 ?

A. D'accélérer le trafic sur des réseaux, comme par exemple internet
B. De donner une adresse à des ordinateurs sur des réseaux, comme par exemple Internet
C. D'augmenter la bande passante disponible sur des réseaux, comme par exemple Internet

19 Quel est le principal service du protocole DNS ?

A. La transformation d'un nom de domaine en adresse IP
B. La réparation des réseaux à distance
C. La transmission des paquets sur internet

20 Les serveurs informatiques professionnels sont placés dans :

A. Des baies 19 pouces
B. Des armoires frigorifiques
C. Des baies 42 pouces

21 Quelle est la signification du sigle CSS ?

A. Cascading Style Sheet
B. Cascading Super Sayan
C. Crowding Super Sheet

22 Un arbre équilibré, c'est à dire qui maintient une profondeur équilibrée entre ses branches, permet dans le pire des cas :

A. Une recherche en temps constant
B. Une recherche en temps linéaire
C. Une recherche en temps logarithmique
D. Une recherche en temps quadratique

23 L'utilisation massive de la fibre optique en salle informatique permet :

A. D'améliorer la qualité de la lumière dans les salles informatiques
B. D'éviter les perturbations électromagnétiques sur les câbles
C. De diminuer la pollution de l'air à l'intérieur

24 Que permet le protocole TCP ?

A. De vérifier que l'ordinateur ayant reçu les paquets est le bon
B. De vérifier l'identité de l'expéditeur des paquets
C. De contrôler l'intégrité des paquets réseau transmis

25 Laquelle de ces affirmations est vraie ?

A. Il n'y a pas de différence entre un logiciel libre et un logiciel gratuit
B. Le code source d'un logiciel libre est disponible
C. Une licence est la même chose qu'un pilote

26 L'adoption de DevOps représente principalement :

A. Des changements méthodologiques et culturels au sein d'une organisation
B. L'acquisition de certifications
C. Plus de dix déploiements de logiciels par jour
D. Le fait qu'une personne fasse à la fois le développement et les opérations

27 Une famille de Colonnes peut s'appliquer :

A. À une structure dans du SGBD-R Oracle 9c
B. À un type de base de données type NoSQL
C. À un mode d'affichage du Finder sur macOS

28 Soit le document HTML suivant. Quelle est la couleur du texte “Bonjour !” si on affiche ce document dans un navigateur ?

```
<html>
 <head>
  <style>
   .contenu .paragraphe {
    color: red;
   }
   p.paragraphe {
    color: blue;
   }
   body div p.paragraphe {
    color: green;
   }
   .paragraphe {
    color: yellow;
   }
  </style>
 </head>
 <body>
  <div class="contenu">
   <p class="paragraphe">Bonjour !</p>
  </div>
 </body>
</html>
```

A. Rouge
B. Bleu
C. Vert
D. Jaune

29 Dans « /dev/sdb », « sd » indique :

A. La partition étendue
B. Le disque est en SCSI
C. Le disque est en IDE

30 Que signifie le sigle TCP ?

A. Transmission Control Protocol
B. Transformation Control Preparation
C. Transmission Calendar Protocol

31 Quelle est la licence la moins contraignante ?

A. AGPL
B. Apache
C. GPL
D. LGPL

32 Vous travaillez sur un projet de classification binaire (positif / négatif). Vous avez entraîné un modèle sur un corpus d'apprentissage et vous le testez sur un corpus de validation. Vous obtenez la matrice de confusion suivante entre vos prévisions et la réalité observée. Quelle est la précision du modèle ?

n = 165	Prédiction : négatif	Prédiction : positif
Observé : négatif	50	10
Observé : positif	5	100

A. 9%
B. 60%
C. 91%
D. 95%

33 Dans les salles informatiques professionnelles, il faut trouver au moins :

A. Deux alimentations électriques distinctes
B. Un système de recyclage d'air
C. Un système de purification de l'eau

34 Quelle méthode ne fait pas partie de la norme HTTP 1.1 ?

A. POST
B. RETURN
C. CONNECT

35 Quel logiciel n'est pas utilisé pour l'automatisation des infrastructures IT ?

A. Ansible
B. Cook
C. Puppet
D. Vagrant

36 La valeur maximale d'un entier signé sur 32 bits est de :

A. $2^{31} - 1$
B. 2^{31}
C. $2^{32} - 1$
D. 2^{32}

37 Quelle instruction n'est pas valide dans un fichier Dockerfile ?

A. FROM
B. TO
C. COPY
D. RUN

38 Pour séparer un disque dur physique en deux disques logiques, il faut :

A. Formater le disque
B. Partitionner le disque
C. Partager le disque

39 En quelle année a été créé le noyau Linux ?

A. 1986
B. 1991
C. 1997

40 Quel est le système de fichier utilisé par Windows ?

A. NTFS
B. EXT2
C. BFS

41 UML est :

A. La partie « données » de la méthode MERISE
B. Un standard de communication
C. Un langage de modélisation

42 Combien y'a-t-il d'octets dans un Kio (kibioctet) ?

A. 1000
B. 1024
C. 1048

43 Une mémoire ne peut pas être de type :

A. ROM
B. RUM
C. RAM

44 Sous Windows, qu'est-ce qu'un UAC ?

A. Un rôle
B. Un composant de sécurité
C. Une application

45 Lequel de ces extraits HTML est valide ?

A. <html><body>Texte</body></html>
B. <html><bodyguard>Texte</guardbody></html>
C. </html></body>Texte<body><html>

46 Combien de terminaux le bloc CIDR 192.0.0.0/8 permet-il d'adresser ?

A. 16 777 214 adresses
B. 65 534 adresses
C. 254 adresses

47 Que signifie le sigle SSD ?

A. Solid State Drive
B. Secure System Drive
C. Solid State Disk

48 En traitement de la langue naturelle, la tâche qui consiste à rechercher des objets textuels (c'est-à-dire un mot, ou un groupe de mots) catégorisables dans des classes telles que noms de personnes, noms d'organisations ou d'entreprises, noms de lieux, quantités, distances, valeurs, dates, s'appelle :

A. La classification
B. La reconnaissance d'entités nommées (Named Entity Recognition)
C. La casuistique
D. L'extraction sémantique

49 TIFF est un format :

A. D'images
B. De base de données
C. De Terminal Informatique de type FF

50 On cherche à mesurer le risque de collisions pour des mots de passe de 4 chiffres pour un groupe de personnes dont les membres utiliseraient tous leur date d'anniversaire (jour et mois). À partir de quelle taille de groupe y aurait-il au moins 50% de chances qu'au moins deux membres quelconques aient le même mot de passe ?

A. 23
B. 183
C. 253
D. 730

51 Que contient la variable « $* » en shell bash ?

A. Le premier paramètre
B. La liste de tous les paramètres
C. Le nombre de paramètres

52 Le fichier pg_hba.conf est :

A. Utilisé pour la configuration de PostgreSQL dans le cadre de la High Balanced Availability. On y définit les membres d'un cluster équivalent à Oracle RAC.
B. Utilisé pour la configuration du Host Bus Adapter en conjonction avec udev. On y définit les membres de la chaine SCSI ou FibreChannel.
C. Utilisé pour la configuration de PostgreSQL dans le cadre de l'authentification et de l'application des droits des clients.

53 Qu'est-ce qui caractérise un processus « daemon » ?

A. Il n'a pas de PPID
B. Il n'a pas de terminal de contrôle
C. On ne peut pas le « tuer »
D. Il a déjà été « tué » mais ne s'arrête pas

54 Le nombre qui suit le nombre 4 en base 5 est :

A. 10
B. 5
C. 0

55 Le mouvement DevOps date depuis :

A. 1984
B. 2000
C. 2008
D. 2017

56 La commande « uname » :

A. Permet de créer un alias
B. Indique l'ID d'un fichier
C. Informe sur l'OS et sa version

57 Quelle est l'utilité de la commande « file » ?

A. Elle dresse la liste de tous les fichiers d'un utilisateur
B. Elle modifie le format d'un fichier
C. Elle détermine le type de contenu d'un fichier

58 En shell bash, quelle variable contient le code de retour de la dernière commande exécutée ?

A. $1
B. $?
C. $$
D. $!

59 Quelle commande permet d'obtenir le nombre de mots d'un fichier texte en shell bash ?

A. cat -w fichier
B. ls -w fichier
C. wc -w fichier
D. sed -w fichier

60 Quel est le nom de l'utilitaire permettant d'accéder à la base de registre ?

A. Registre
B. Register
C. Regedit

61 Quelle proposition décrit le mieux le concept de "dette technique" ?

A. C'est le coût supplémentaire engendré par l'achat de machines beaucoup plus puissantes que la moyenne permettant d'exécuter des programmes pour lesquels l'attention a été portée sur le temps rapide de développement, au détriment de la performance.
B. C'est une analogie entre les coûts futurs liés à des choix court-termistes de conception logicielle et une dette financière, que le seul remboursement ne suffira pas à éponger puisqu'elle va aussi générer des intérêts.
C. Cela représente le temps de développement perdu en réunions et pauses café.
D. C'est la dette contractée auprès de collègues plus compétents pour compenser un manque de connaissances techniques.

62 Que retourne cette requête LDAP ? (&(direction=DSI)(!(grade=stagiaire)))

A. Tous les stagiaires de la DSI
B. Toute la DSI sauf les stagiaires
C. Toute la DSI et tous les stagiaires
D. Tous les stagiaires hors DSI

63 Quelle commande me permet d'accéder à la stratégie de groupe local ?

A. gpedit.msc
B. stgroupe.msc
C. gplocaledit.msc

64 Dans le cadre de MySQL, version inférieure à 5, en utilisant le super utilisateur nommé root, suite à la séquence suivante de commandes :

```
create database exemple ;

use exemple ;

CREATE TABLE u
(
   id INT PRIMARY KEY NOT NULL,
   nom VARCHAR(100),
   prenom VARCHAR(100),
   email VARCHAR(255),
   date_naissance DATE
);

insert into u set id=1, nom='QUALITY', prenom='Control', email='qc@senat.fr', date_naissance='01/01/1970';

GRANT INSERT, DELETE, SELECT ON exemple.u to qc01@'localhost' identified by 'QualCont';

drop table u ;

CREATE TABLE u
(
   id INT PRIMARY KEY NOT NULL,
   name VARCHAR(100),
   firstname VARCHAR(100),
   email VARCHAR(255),
   birthday DATE
 );
```

L'utilisateur qc01, utilisant la connexion via localhost à la base test, verra la requête :

```
select firstname from exemple.u ;
```

A. Lui renvoyer une erreur car qc01 ne dispose pas des droits sur la table u.

```
ERROR 1142 (42000): SELECT command denied to user 'qc01'@'localhost' for table 'u'
```

B. Lui renvoyer une table vide.

```
Empty set (0.00 sec)
```

C. Lui renvoyer une ligne contenant Control.

```
+-----------+
| firstname |
+-----------+
| Control   |
+-----------+
1 row in set (0.00 sec)
```

65 Une URL permet :

A. De localiser une ressource sur internet
B. De diminuer le temps de chargement d'un site
C. De sécuriser les transactions d'un site web

66 Quelle option de la commande « grep » affiche toutes les lignes qui ne correspondent pas à l'expression passée en paramètre ?

A. -u
B. -a
C. -r
D. -v

67 Dans le cadre d'Oracle 11g, la requête suivante :

```
select vts.ts#, vts.name, sum(vdf.bytes), to_char((select nvl(sum(dsg.bytes),0.0)
  from dba_segments dsg
 where  vts.name = dsg.tablespace_name
)/sum(vdf.bytes)*100,'999.9')
 from v$datafile vdf, v$tablespace vts
 where vdf.ts# = vts.ts#
 group by vts.ts#, vts.name
 order by vts.name
;
```

renvoie :

A. Une erreur concernant le nom du lien de base de données.

```
ERREUR à la ligne 6 :
ORA-01729: nom de lien de base de données attendu
```

B. Une erreur concernant l'existence d'une table ou vue.

```
ERREUR à la ligne 5 :
ORA-00942: Table ou vue inexistante
```

C. Une sortie du type :

```
     TS# NAME                           SUM(VDF.BYTES) TO_CHA
---------- ------------------------------ -------------- ------
         4 IDX                          1048576000    9.9
         1 SYSAUX                         1073741824   58.8
         0 SYSTEM                         1073741824   38.8
         5 TAB                          1048576000    9.7
         2 UNDOTBS1                       1610612736     .7
```

68 Le nombre binaire 1011 vaut en décimal :

A. 7
B. 9
C. 11

69 On considère quatre cartes posées sur une table. Chaque carte a une face avec une lettre et une face avec un chiffre. Les faces visibles indiquent : 1, 8, A, B.
Soit l'assertion "Si une face est paire, alors l'autre face est une voyelle". Quel est le nombre minimum de cartes à retourner pour être sûr que l'assertion soit vraie ?

A. 1
B. 2
C. 3
D. 4

70 On a une application qui insère des données dans une table PostgreSQL à un rythme moyen de 10 insertions par seconde. La clé primaire de cette table est un identifiant stocké sous forme d'un entier signé de 64 bits. Cet identifiant est incrémenté à chaque insertion. Au bout de combien de temps notre application sera-t-elle à court d'identifiants ?

A. Environ 13 ans
B. Environ 1229 ans
C. Environ 29 millions d'années
D. Plus que l'âge de l'univers

71 Quelle est la traduction usuelle de « garbage collector » en français ?

A. Collecteur de déchets
B. Défragmenteur
C. Éboueur
D. Ramasse-miettes

72 Quel est le comportement le plus probable de l'instruction suivante dans la plupart des langages, si a et b sont des flottants double précision non nuls ?

```
return ((a+b)*(a+b) - a*a - b*b - 2*a*b) / ((a+b)*(a+b) - a*a - b*b - 2*a*b);
```

A. Retourne le flottant double précision 0.0
B. Retourne le flottant double précision 1.0
C. Retourne NaN (Not a Number)

73 Dans l'acronyme CAMP (« CAMS », en anglais), la lettre A signifie :

A. Agglomération
B. Automatisation
C. Approbation
D. Accréditation

74 Laquelle de ces assertions est vraie ?

A. En UTF-8, tous les caractères occupent deux octets
B. En UTF-8, tous les caractères ASCII occupent un octet et les autres deux octets
C. En UTF-8, tous les caractères ASCII occupent un octet et les autres plusieurs
D. En UTF-8, tous les caractères ASCII utilisent au moins deux octets

75 Parmi les expressions régulières suivantes, laquelle capture les locutions latines bis et ter, et seulement elles, dans la phrase : « Le terrier de Rominagrobis est au 15 bis rue de Vaugirard et non au 15 ter. » ?

A. (bis|ter)
B. \s(bis|ter)\s
C. [\s\.](bis|ter)[\s\.]
D. ^(bis|ter)$

76 À quoi peut servir un point de restauration sous Windows ?

A. À revenir à un point antérieur dans le temps
B. À restaurer tous les documents perdus
C. À restaurer des fichiers du système

77 On recherche tous les couples de personnes de même âge dans une table relationnelle. On suppose que les personnes sont décrites dans une table Personne avec, comme clé primaire, un entier appelé id et leur âge dans une colonne age. Quelle requête SQL renvoie le résultat ?

A. SELECT a, b FROM Personne a JOIN Personne b ON a.age = b.age
B. SELECT a, b FROM Personne a LEFT JOIN Personne b ON a.age = b.age and a.id < b.id
C. SELECT a, b FROM Personne a INNER JOIN Personne b ON a.age = b.age and a.id < b.id
D. SELECT a, b FROM Personne a FULL JOIN Personne b ON a.age = b.age and a.id < b.id

78 En cryptographie, RSA est une méthode de chiffrement :

A. symétrique
B. asymétrique
C. hybride
D. sur courbe elliptique

79 Dans le contexte du RGPD, qu'est-ce qu'une donnée à caractère personnel ?

A. Une donnée que l'on a achetée pour son usage personnel
B. Une donnée qui se rapporte directement ou indirectement à une personne physique
C. Une donnée qui permet d'identifier une personne
D. Une donnée qui peut être vendue aux entreprises

80 On cherche à réaliser une fonction de hachage permettant aussi bien de développer une table de hachage que d'être utilisée dans un contexte de cryptographie. Parmi les caractéristiques suivantes, quelle est celle qui n'est absolument pas souhaitable pour cette fonction ?

A. La fonction de hachage utilise tous les champs de l'objet d'entrée
B. La fonction de hachage distribue uniformément les données
C. La fonction de hachage génère des valeurs voisines pour des objets quasi identiques

81 Soit le programme en pseudo-code suivant. Quelle est la complexité de cet algorithme ?

```
maxsofar = 0
for i = [0,n)
            sum = 0
for j= [i, n)
   sum += x[j]
   maxsofar = max(maxsofar, sum)
```

A. O(log n)
B. O(n)
C. O(n.log n)
D. O(n2)

82 Prouver qu'un programme n'a pas d'erreurs est :

A. Possible en temps logarithmique
B. Possible en temps linéaire
C. NP-complet
D. Indécidable

83 Le développement piloté par les tests (Test Driven Development, TDD) est le mieux décrit par :

A. Test once, develop anywhere
B. Rédiger les tests avant d'implémenter le code
C. Tester la fonctionnalité précédente avant de développer la suivante
D. Code, test and run

84 En HTML5, la balise utilisée pour faire des liens hypertextes est :

A. <a>
B.
C. <p>

85 Qu'est-ce que le droit d'accès (contexte de la Loi Informatique et libertés) ?

A. La possibilité pour une personne de prendre connaissance de l'intégralité des données la concernant, en s'adressant à ceux qui la détiennent
B. La possibilité pour une personne d'accéder aux applications qui traitent des données qui la concernent, pour les consulter et en vérifier la validité
C. La possibilité pour une personne de prendre connaissance des informations concernant son conjoint, en s'adressant directement à ceux qui les traitent
D. La possibilité pour les entreprises d'accéder aux données à caractère personnel de la personne, à partir du moment où celle-ci consulte leur site internet

86 On désire colorer des circonscriptions électorales sur une carte en utilisant le moins de couleurs possibles. Sans autre information que le caractère connexe de chaque circonscription, de combien de couleurs avez-vous besoin pour être sûr que deux circonscriptions adjacentes soient de couleurs différentes ?

A. 3
B. 4
C. 5
D. 6

87 Qu'affiche le programme en pseudo code suivant ?

```
int t[10][10];
for( int i = 0; i < 10; i++ )
  for( int j = 0; j < 10; j++ )
    t[i][j] = i+j;

int s = 0;
for( int i= 0; i < 10; i++ )
  s = s + t[i][i];

afficher(s);
```

A. 90
B. 100
C. 110
D. 120

88 Quelle phrase suivante n'est pas correcte ?

A. Les technologies de conteneurisation LXC existent depuis plus de 10 ans.
B. Pour Docker, les « namespaces » du noyau hôte sont mis en œuvre pour isoler les conteneurs.
C. Pour Docker, les « control groups » du noyau hôte sont mis en œuvre pour limiter les ressources des conteneurs.
D. Un conteneur Docker peut embarquer des versions distinctes du système hôte pour le noyau, le système d'exploitation et les applicatifs.

89 Comment s'appelle l'abstraction qui permet de référencer un résultat encore inconnu car son calcul se fera plus tard au cours de l'exécution ?

A. Une promesse
B. Un passage par référence
C. Un passage par valeur
D. Un passage en différé

90 Quelle définition de code HTTP 1.0 est fausse ?

A. 200 : la requête s'est déroulée correctement
B. 404 : la ressource demandée n'existe pas
C. 500 : requête acceptée, traitement en cours

91 Huit philosophes assemblés autour d'une table ronde veulent manger des spaghettis en utilisant deux fourchettes. Il existe une seule fourchette entre deux philosophes assis côte à côte. Les actions de chaque philosophe sont exécutées dans un fil d'exécution (thread) séparé. Après avoir mangé une bouchée en 5 minutes, un philosophe repose ses fourchettes et pense pendant 5 minutes. Comment assurer que tous les philosophes mangent deux bouchées en 20 minutes ?

A. Chaque philosophe teste la disponibilité de la fourchette de gauche puis s'en saisit. Chaque philosophe fait ensuite de même pour la fourchette de droite.
B. Un sémaphore existe pour chaque fourchette et rend atomique le test de disponibilité et la prise d'une fourchette.
C. Une section critique rend atomique le test de la disponibilité et la saisie des deux fourchettes.
D. Un sémaphore unique permet de tester, prendre les fourchettes, manger et reposer les fourchettes en une seule opération.

92 Qu'affiche le programme en pseudo code suivant ?

```
int i = 20;
while ( i > 1 )
{
  if( est_pair(i) )
    i = i/2;
  else
    i = (i-1) * 2;

  afficher(i);
}
```

A. 10 5 8 3 2 1
B. 10 5 4 2 1
C. 10 5 3 2 1
D. 10 5 8 4 2 1

93 Que signifie l'acronyme RGPD ?

A. Règlement général sur la protection des données
B. Règlementation générale de protection des données
C. Regulation for general protection of data
D. Regulation for great privacy defense

94 Sélectionner la syntaxe HTML5 valide :

A. Texte vert
B. <h1>Titre 1</1h>
C. éléments divers

95 Les réseaux de type LAN sont couramment utilisés pour des étendues géographiques :

A. Petites : bâtiments
B. Grandes : pays
C. Très grandes : continents

2. EPREUVE TECHNIQUE – PROFIL « ADMINISTRATION DES SYSTEMES »

(durée 2 heures - coefficient 3)

- *Il est possible de répondre aux questions dans le désordre*
- *Ne pas recopier la question mais bien indiquer le numéro de la question*
- *Les brouillons ne seront pas pris en compte*

1 Virtualisation / Containerisation (*10 points*)

1.1 En quoi consiste la virtualisation de serveurs ? (*2 points*)

1.2 Citez 3 solutions de virtualisation. (*0,5 point*)

1.3 Expliquer ce qu'est la contention CPU et mémoire sous VMware. Est-ce qu'un de ces mécanismes est plus dangereux que l'autre ? Expliquer pourquoi. (*2,5 points*)

1.4 Quel est la différence entre virtualisation et containerisation ? (*2,5 points*)

1.5 En quoi consiste l'hyper-convergence ? Quel est l'intérêt de cette technologie ? (*2,5 points*)

2 Stockage / Sauvegarde (*5 points*)

2.1 Qu'est-ce qu'un réseau de stockage centralisé ? (*1 point*)

2.2 Dans un réseau de stockage centralisé de type iSCSI, est-il possible que plusieurs initiateurs écrivent en même temps sur une cible ? Justifiez votre réponse. (*2 points*)

2.3 Lors d'une sauvegarde, décrivez le principe de déduplication à la source. Qu'apporte-t-il en matière d'utilisation processeur et réseau sur les serveurs sauvegardés et sur le serveur de sauvegarde ? (*2 points*)

3 Surveillance / Journalisation (*4 points*)

3.1 Qu'est-ce qu'un SIEM et quel est son intérêt ? (*2 points*)

3.2 Citer les indicateurs principaux à surveiller sur : (*1 point*)

- un serveur.
- un pare-feu.
- un commutateur.

3.3 Citer et décrire sommairement un protocole commun permettant de superviser ces équipements ? (*1 point*)

4 ToIP (*4 points*)

4.1 Vous mettez en place une infrastructure réseau pour de la téléphonie sur IP. Quels sont les principaux critères de ce réseau à considérer pour la qualité de la voix ? (*2 points*)

4.2 Vous avez le choix entre deux CODEC pour la téléphonie sur le réseau local : G.711 et G.729. Lequel choisissez-vous et pour quelle(s) raison(s) ? (*2 points*)

5 Réseau / Sécurité (*10 points*)

5.1 Décrivez le mode de fonctionnement d'un pare-feu à états (stateful). (*2 points*)

5.2 Sur un pare-feu on dispose des règles suivantes. Que permet la ligne n° 7 ? (*2 points*)

	Source	**Destination**	**Port Destination**	**Action**
1	Clients Windows : 172.19.0.0/24	Serveurs Windows:172.18.1.0/24	SMB	Accepter
2	Clients Windows : 172.19.0.0/24	Tous : 0.0.0.0/0	SMB	Refuser
3	Clients Annuaires : 172.17.0.0/24	Serveurs annuaires : 172.17.2.0/24	LDAPS	Accepter
4	Tous : 0.0.0.0/0	Serveurs annuaires : 172.17.2.0/24	LDAPS	Refuser
5	Clients Messagerie:172.19.1.0/24	Tous : 0.0.0.0/0	HTTPS	Accepter
6	Clients Messagerie:172.19.1.0/24	Tous : 0.0.0.0/0	HTTP	Refuser
7	Clients Messagerie:172.19.1.0/24	Serveurs Windows:172.18.1.0/24	HTTPS	Refuser
8	Clients Messagerie:172.19.1.0/24	Serveurs Windows:172.18.1.0/24	HTTP	Refuser

5.3 Les clients de messagerie doivent accéder à l'annuaire LDAP interne (ldap.senat.fr) indiquez la/les règle(s) à ajouter et à quel niveau elle(s) s'insère(nt). (*2 points*)

5.4 Décrivez les étapes principales d'une connexion TCP et celles d'une connexion UDP. Quelles sont les différences ? (*2 points*)

5.5 Quelles sont les principales différences entre IPv4 et IPv6 ? Quelles sont les conséquences au niveau des diffusions de masse sur les réseaux ? (*2 points*)

6 Serveur Web (*5 points*)

6.1 Quelles sont les principales différences entre HTTP 1.1 et HTTP/2, notamment sur la sécurité et la performance ? (*2 points*)

6.2 Quelles peuvent être les conséquences de la généralisation du protocole HTTP/2 en termes de filtrage sur un réseau d'entreprise ? (*1 point*)

6.3 Quels sont les avantages à mettre des applications web derrière un répartiteur de charge ? (*2 points*)

7 Linux (*10 points*)

7.1 Que signifie l'acronyme SSH ? Que permet ce protocole (citer 3 utilisations) ? (*1 point*)

7.2 Écrivez un script shell bash permettant d'extraire les éléments suivants du fichier de log ci-dessous seulement lorsqu'il y a une erreur : IP, login s'il existe, heure. Écrire ce que votre script doit afficher. (*3 points*)

```
192.168.17.71 - vhugo [01/Dec/2018:17:57:49 +0100] "POST /info-mail/print.php HTTP/1.1" 200 1981
"https://serveur.senat.fr/info-mail/index.php?param=cn=*user*" "Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/70.0.3538.113 Safari/537.36 Vivaldi/2.1.1337.51"
192.168.17.71 - vhugo [01/Dec/2018:17:57:50 +0100] "GET /info-mail/styles.css HTTP/1.1" 200 2367
"https://serveur.senat.fr/info-mail/print.php" "Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/70.0.3538.113 Safari/537.36 Vivaldi/2.1.1337.51"
192.168.17.169 – wamozart [01/Dec/2018:17:58:56 +0100] "GET /favicon.ico HTTP/1.1" 404 209 "-" "Mozilla/4.0 (compatible;
MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729;
.NET4.0C; .NET4.0E; Media Center PC 6.0)"
192.168.17.204 - wamozart [01/Dec/2018:18:16:41 +0100] "GET /info-mail/styles.css HTTP/1.1" 200 2367
"https://serveur.senat.fr/info-mail/index.php?param=m.audit" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:60.0) Gecko/20100101
Firefox/60.0"
192.168.17.204 - wamozart [01/Dec/2018:18:16:41 +0100] "GET /info-mail/index.php?param=m.vaspar HTTP/1.1" 200 217133
"https://serveur.senat.fr/info-mail/index.php?param=" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:60.0) Gecko/20100101
Firefox/60.0"
192.168.17.204 - wamozart [01/Dec/2018:18:16:50 +0100] "GET /info-
mail/index.php?param=manager=uid=marcel,ou=personnes,dc=senat,dc=fr&joli=off HTTP/1.1" 200 60237
"https://serveur.senat.fr/info-mail/index.php?param=m.vaspar" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:60.0)
Gecko/20100101 Firefox/60.0"
192.168.17.249 - edelacro [01/Dec/2018:18:29:43 +0100] "GET /info-mail/index.php?param=dsi-dsi&joli=on HTTP/1.1" 200
3404 "https://serveur.senat.fr/info-mail/index.php?param=dsi-dsi&joli=on" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:60.0)
Gecko/20100101 Firefox/60.0"
192.168.17.200 - - [01/Dec/2018:18:30:27 +0100] "GET /favicon.ico HTTP/1.1" 404 209 "-" "Mozilla/5.0 (Windows NT 6.1;
Win64; x64; rv:63.0) Gecko/20100101 Firefox/63.0"
192.168.17.169 - arodin [01/Dec/2018:23:23:04 +0100] "GET /info-mail/fdgdg HTTP/1.1" 418 213 "-" "Mozilla/5.0 (Windows NT
6.1; Win64; x64; rv:60.0) Gecko/20100101 Firefox/60.0"
192.168.17.169 - - [01/Dec/2018:23:24:51 +0100] "GET /info-mail/ HTTP/1.1" 401 401 "-" "Mozilla/4.0 (compatible; MSIE 7.0;
Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; .NET4.0C;
.NET4.0E; Media Center PC 6.0)
```

7.3 D'après les extraits de l'exécution de plusieurs commandes sur un serveur physique Linux RedHat Entreprise ci-dessous, présentez sommairement le rôle de chaque commande et des paramètres utilisés. (*1 point*)

```
[root@serveur wwwwww]# pwd
/var/wwwwww
[root@serveur wwwwww]# uname -a
Linux serveur.senat.fr 2.6.18-194.11.3.el5 #1 SMP Mon Aug 23 15:51:38 EDT 2010 x86_64 x86_64 x86_64 GNU/Linux
[root@serveur wwwwww]# df -k
Sys. de fich.       1K-blocs       Occupé Disponible Capacité Monté sur
/dev/mapper/VolGroup00-LogVol01
                     1015704    498300    464976  52% /
/dev/sda1             194442     48741    135662  27% /boot
tmpfs                8216000         0   8216000   0% /dev/shm
/dev/mapper/VolGroup00-LogVol05
                     7110136   5570468   1466292  80% /home
/dev/mapper/VolGroup00-LogVol06
                     2031440    174056   1752528  10% /opt
/dev/mapper/VolGroup00-LogVol02
                     2031440    101920   1824664   6% /tmp
/dev/mapper/VolGroup00-LogVol04
                     3047184   2378168    511744  83% /usr
/dev/mapper/VolGroup00-LogVol03
                     5078656   3681832   1134720  77% /var
/dev/mapper/VolGroup00-mysqldb
                    41284928  22311744  16876160  57% /var/lib/mysql
/dev/mapper/VolGroup00-www
                     2231543   2231303       240 100% /var/wwwwww
/dev/mapper/VolGroup00-var--tomcat
                     1032088     79344    900316   9% /var/lib/tomcat5
/dev/mapper/VolGroup00-syslog
                     2064208    172180   1787172   9% /opt/syslog-ng
[root@serveur wwwwww]# ls -l
```

```
total 44
drwxr-xr-x 129 webm apache  4096 sept. 20 18:45 apps
drwxr-xr-x   2 webm webm    4096 mai 27  2011 cgi-bin
drwxr-xr-x   4 webm apache  4096 févr. 12  2014 html
drwxr-xr-x  13 root root    4096 nov. 27 08:55 logs
drwx------   2 root root   16384 nov.  7  2008 lost+found
drwxr-xr-x   2 webm webm    4096 juin 29  2010 phperreur
drwxr-xr-x   2 webm webm    4096 juin 29  2010 sessions
drwxr-xr-x   2 webm webm    4096 juin 29  2010 tmp
[root@serveur wwwwww]# du -sh *
800K    apps
56K     cgi-bin
136K    html
1,2G    logs
16K     lost+found
4,0K    phperreur
4,0K    sessions
4,0K    tmp
[root@serveur wwwwww]# du -s logs/*
113672  logs/2018.01
100212  logs/2018.02
112688  logs/2018.03
107248  logs/2018.04
111640  logs/2018.05
114488  logs/2018.06
120440  logs/2018.07
112620  logs/2018.08
104516  logs/2018.09
114208  logs/2018.10
99936   logs/2018.11
[root@serveur wwwwww]# vgdisplay
  --- Volume group ---
  VG Name               VolGroup00
  System ID
  Format                lvm2
  Metadata Areas        1
  Metadata Sequence No  67
  VG Access             read/write
  VG Status             resizable
  MAX LV                0
  Cur LV                15
  Open LV               15
  Max PV                0
  Cur PV                1
  Act PV                1
  VG Size               274,03 GB
  PE Size               32,00 MB
  Total PE              8768
  Alloc PE / Size       8480 / 265,00 GB
  Free  PE / Size       288 / 9,21 GB
  VG UUID               7DlBcA-3WaW-u6G1-jZfd-6N6z-jZIG-GJ8NeE
```

7.4 Dans ces mêmes extraits, quel est le problème ? (*2 points*)

7.5 Quelles sont les solutions possibles ? (*3 points)*

8 Windows / Poste de travail (*8 points*)

8.1 Que signifie RDP ? Que permet ce protocole (citer 3 utilisations)? (*1 point*)

8.2 Écrire un script PowerShell permettant d'enregistrer dans un fichier comptes.log la liste des comptes locaux d'une machine donnée. (*3 points*)

8.3 Qu'est-ce qu'une GPO ? De quoi est-elle constituée ? Où se trouvent les GPO dans un domaine Active Directory ? Quelle ligne de commande permet d'afficher sur un poste de travail les GPO qui s'appliquent ? Peut-on forcer leur mise en œuvre ? Si oui, comment ? (*4 points*)

9 Cryptographie (*4 points*)

9.1 Quel est le principe de la cryptographie à clés asymétriques ? (*1 point*)

9.2 Quelles sont les deux actions majeures permises par ce principe cryptographique ? (*1 point*)

9.3 Décrivez l'utilisation faite des clés lors de la mise en pratique de ces deux actions. (*2 points*)

2. EPREUVE TECHNIQUE – PROFIL « DEVELOPPEMENT

(durée 2 heures – coefficient 3)

Le langage choisi devra être clairement indiqué au début de votre copie.
Il est interdit aux candidats de changer de langage en cours d'épreuve.

On pourra utiliser les classes des bibliothèques fournies avec ces langages. Lorsque le candidat n'est pas sûr du nom d'une méthode d'une classe, il devra le mentionner dans sa copie et expliquer brièvement ce que fait la méthode, en utilisant, par exemple, un commentaire.

Pour le C++, la STL est considérée comme faisant partie du langage. Par ailleurs, toujours pour le C++, lorsqu'il est demandé d'écrire une fonction qui retourne un objet, le candidat qui souhaiterait mettre en œuvre la technique appelée "Resource Acquisition Is Initialization" pourra passer plutôt l'objet par référence en tant que premier paramètre de la fonction. Il devra, bien entendu, être cohérent avec ce choix, s'il utilise la fonction dans une question ultérieure.

Le cas échéant, le candidat prendra soin d'expliciter ses hypothèses, en particulier si l'énoncé lui semble ambigu.
Concernant les questions nécessitant l'écriture d'une « fonction », le code devra non seulement être correct mais aussi le plus lisible possible, c'est-à-dire correctement présenté (avec indentations et un minimum de rayures) et commenté. Les noms des fonctions et des variables devront également être choisis pour faciliter la compréhension du code. La lisibilité du code étant prise en compte dans la correction, il est vivement recommandé de préparer les réponses au brouillon.

Problème 1 : Lecture de Code (*4 points*)

Ce problème porte sur un code C++ ou Java, selon le choix de langage initial du candidat.

1. Sans réécrire le code, décrire le plus clairement et le plus précisément possible les modifications que vous proposeriez pour faciliter la maintenance de ce programme. (*2 points*)

2. Proposer une phrase en remplacement de « XXX » (et une pour « YYY ») pour décrire ce qu'a déterminé le programme sur l'entier n en fonction de la valeur du test (z==y). (*2 points*)

Pour les candidats ayant choisi C++

```
#include <iostream>
using namespace std;
int main()
{int x,y=0,z;
int n=454256731;
z=n;
while(n>0){
x=n%10;
y=(y*10)+x;
n=n/10;}
if(z==y)cout<<"XXX\n";
else cout<<"YYY\n";
n=5225;
z=n;
y=0;
while(n>0){
x=n%10;
y=(y*10)+x;
n=n/10;}
if(z==y)cout<<"XXX\n";
else cout<<"YYY\n";
return 0;}
```

Pour les candidats ayant choisi Java

```
public class Exemple{
public static void main(String args[]){
int x,y=0,z;
int n=454256731;
z=n;
while(n>0){
x=n%10;
y=(y*10)+x;
n=n/10;}
if(z==y)System.out.println("XXX");
else System.out.println("YYY");
n=5225;
z=n;
y = 0;
while(n>0){
x=n%10;
y=(y*10)+x;
n=n/10;}
if(z==y)System.out.println("XXX");
else System.out.println("YYY");
}}
```

Problème 2 : Découpage électoral (*8 points*)

Le ministère de l'Intérieur a la responsabilité de découper le territoire national en circonscriptions législatives, ou bien les départements en cantons. Dans l'exercice ci-dessous, on imagine que, devant les contestations dont font l'objet ces découpages, le Sénat, dans son rôle de contrôle de l'action du gouvernement, décide de se saisir de ce problème pour l'analyser scientifiquement en construisant un simulateur.
Pour simplifier, on considère des élections uninominales à un seul tour.
Chaque circonscription est composée d'exactement deux bureaux de vote sur les N que compte une localité. On cherche à découper les circonscriptions. On connaît les intentions de vote pour les P partis politiques dans chacun des bureaux. Par exemple, pour P = 3 et N = 6, on pourrait avoir :

Intentions de vote	Parti 0	Parti 1	Parti 2
Bureau 0	1170	1340	820
Bureau 1	1180	820	970
Bureau 2	830	500	1050
Bureau 3	1270	1580	660
Bureau 4	950	1060	680
Bureau 5	760	1220	880

Chaque parti politique présente un candidat par circonscription. Chaque circonscription est représentée par un siège. En fonction des regroupements des bureaux en circonscriptions, le résultat en nombre de sièges peut être fort différent. Exemple :

Nombre de sièges	Parti 0	Parti 1	Parti 2
Découpage n°0 (0-1, 2-3, 4-5)	2	1	0
Découpage n°1 (2-4, 0-3, 1-5)	1	2	0
Découpage n°2 (1-2, 0-4, 3-5)	0	2	1

1) Ecrire une fonction simuler simulant le nombre de sièges obtenus par parti en fonction d'un découpage. Cette fonction prend deux arguments :
   - intentions un tableau bidimensionnel d'entiers tel que intentions[b][p] représente les intentions de vote dans le bureau b pour le parti p.
   - decoupage un tableau d'entiers tel que l'appartenance du bureau b à une circonscription c équivaut à c == decoupage[b] où c est un entier compris entre 0 et le nombre de circonscriptions moins un.

   La fonction simuler retourne un tableau d'entiers indexé par le numéro du parti, chaque case du tableau indiquant le nombre de sièges obtenus par le parti correspondant. (*2 points*)

2) Ecrire le test unitaire correspondant à l'exemple de l'énoncé pour le découpage n°1 (2-4, 0-3, 1-5). (*1 point*)

3) On admet qu'on dispose de la fonction decouper retournant la liste de tous les découpages possibles. Écrire une fonction optimiser `qui` retourne un découpage maximisant pour un parti p donné son résultat en nombre de sièges connaissant

tous les découpages possibles. La fonction optimiser prend en argument le tableau des intentions de vote et le numéro du parti. (*1 point*)

4) On considère maintenant qu'une circonscription doit être connexe, c'est à dire qu'il doit exister un chemin pour passer d'un de ses bureaux de vote à l'autre en ne traversant que des bureaux adjacents appartenant à la circonscription. Le caractère adjacent de deux bureaux est donné par le tableau de booléens topologie. Les bureaux b1 et b2 sont adjacents si et seulement si topologie[b1][b2] est vrai.

    a. Ecrire une classe Bureau permettant d'associer à un bureau ses bureaux voisins. Initialiser un tableau des N instances de Bureau. La classe Bureau devra être écrite de façon que le tableau de N instances soit une représentation alternative de topologie avec une empreinte mémoire moindre. (*2 points*)

    b. On considère maintenant qu'une circonscription peut avoir un à trois bureaux de vote. Expliquer, sans la coder, comment modifier la fonction optimiser ou quelle technique pourrait être employée pour tenir compte de la contrainte de connexité. (*2 points*)

Problème 3 : Ségrégation territoriale (*8 points*)

Dans ce problème, on se propose d'évaluer si des phénomènes de ségrégation territoriale peuvent apparaître dans une ville, sans volonté manifeste de chaque individu, et malgré la mise en place de politiques de mixité sociale. Pour ce faire, on suppose que les logements dans une ville sont représentés par un tableau NxN, chaque case représentant un logement. Un logement peut être soit vide, soit occupé par un individu vert, soit occupé par un individu rouge.

On suppose que l'on dispose d'une fonction rnd() qui génère un nombre flottant double précision pseudo aléatoire compris entre 0 et 1.

1) Écrire la structure de données Ville, correspondant au tableau NxN mentionné ci-dessus, et expliquer comment est codé le fait qu'un logement est vide, occupé par un vert ou occupé par un rouge. (*1 point*)

2) On suppose que l'on doive loger V individus verts et R rouges, le reste des logements restant inoccupé. Écrire la fonction initialiser prenant en arguments V et R, et qui réalise cette opération de manière aléatoire. (*1 point*)

3) On suppose qu'un individu donné retire :
   - une satisfaction égale à 2 s'il est entouré d'autant d'individus verts que d'individus rouges,
   - une satisfaction égale à 1 s'il est entouré d'une majorité d'individus de la même couleur que lui,
   - une satisfaction égale à 0 s'il est entouré d'une majorité d'individus de couleur opposée.

   L'entourage d'un logement est constitué par les logements qui partagent avec lui une arête ou un sommet.

Logement NO	Logement N	Logement NE
Logement O	Logement X	Logement E
Logement SO	Logement S	Logement SE

   L'entourage du logement X est constitué des 8 logements suivants : NO, N, NE, O, E, SO, S, SE.

   Écrire la fonction calsat qui prend en argument la ville et les coordonnées i et j d'un appartement et retourne la satisfaction de l'habitant de cet appartement. (*1 point*)

4) Proposer, sans la programmer mais en l'expliquant, une fonction calmix qui retourne un flottant double précision entre 0 et 1 représentant la mixité de la ville, 0 correspondant à une ville très ségrégée (avec un non mélange des verts et des rouges) et 1 correspondant à une ville mixte (mélange complet entre les verts et les rouges). (*1 point*)

5) À partir de cette question, on essaie de modéliser le déplacement des populations en fonction de leurs préférences.

   Écrire une fonction iter qui prend en argument la ville et qui choisit un individu au hasard et un appartement vide au hasard, et qui déplace l'individu si et seulement si la satisfaction de ce dernier augmente. (*1 point*)

6) Est-ce que la satisfaction globale augmente nécessairement à chaque appel de iter ? Expliquer. (*1 point*)

7) Écrire une fonction simuler qui initialise aléatoirement une ville, fait M itérations et retourne le taux de mixité de la ville (au sens de la question 4). (*1 point*)

8) Écrire une fonction calres qui appelle P fois simuler, calcule la moyenne de la mixité et affiche combien de simulations ont donné un résultat entre 0 et 0,1 entre 0,1 et 0,2, …, entre 0,9 et 1. (*1 point*)

3. ETUDE DE CAS - PROFIL "ADMINISTRATION DES SYSTEMES"

(durée 4 heures - coefficient 5)

CONSIGNES

Une attention toute particulière sera portée à l'argumentation de vos réponses et à la justification des différentes solutions que vous pourrez proposer.

La qualité de la rédaction et de la présentation seront également prises en compte. Les textes et schémas ne doivent pas être réalisés en couleur.

Les brouillons ne seront pas pris en compte.

CONTEXTE

Nous sommes le 1er janvier 2017.

Le système de gestion de la paye SIRH du Sénat est un progiciel édité par « SIRH Solutions ». Il permet la gestion des payes des sénateurs, des collaborateurs de sénateurs, des collaborateurs des groupes politiques, des personnels contractuels et des fonctionnaires du Sénat.

Il est en exploitation au Sénat depuis 2009. Le support et le paramétrage sont assurés à la fois par une équipe de développement interne et par une équipe de TMA.

PROJET

Une modification majeure dans le système de paye doit être réalisée : la mise en place du prélèvement de l'impôt à la source, notamment via la DSN. Ce projet de longue durée va nécessiter un travail en profondeur sur les différents environnements SIRH tout en continuant de faire évoluer le progiciel pour les besoins courants.

Il est décidé de profiter de ce projet pour faire évoluer l'infrastructure de la solution qui a de nombreuses lacunes.

Les évolutions du progiciel sont confiées aux développeurs du Sénat et à la TMA.

En tant qu'ingénieur au sein de l'équipe systèmes et réseaux, vous êtes en charge de l'évolution de l'infrastructure de la solution avec l'appui de vos collègues.

INFRASTRUCTURE

Ce progiciel complexe doit souvent être mis à jour, en particulier pour être adapté aux changements de règlementations (une à deux versions mineures par trimestre, une version majeure par an). Deux environnements sont disponibles :

- sirh-deve : version N du progiciel incluant les spécifiques dont certains en cours de développement
- sirh-prod : version N en production

Cette application n'est accessible que par le personnel du Sénat ou la TMA. Il y a environ 600 utilisateurs quotidiens et moins d'une dizaine d'administrateurs de la solution.

Les services sont accessibles aux utilisateurs à travers un navigateur web exclusivement, aux URLs http://paye-deve.senat.fr/ et https://paye.senat.fr .

Les développeurs accèdent également aux différents environnements via un navigateur et doivent par ailleurs accéder au serveur à travers un accès SSH.

Il existe un compte SSH unique par environnement qui permet aux développeurs de se connecter au serveur (sirhdeve, sirhprod). Les mots de passe de ces comptes sont tous identiques et connus des développeurs et de la TMA.

Chaque environnement a besoin d'une instance de base de données Oracle dédiée pour son exécution (respectivement sora-deve et sora-prod). En plus des instances de bases de données utilisées par la solution SIRH, d'autres instances sont également utilisées par d'autres applications qui ne sont pas sur ce serveur (AMELO, THIT, IFM). Chaque instance est accessible en SSH par l'administrateur de base de données avec un compte dédié par instance (dont dbasirhdeve, et dbasirhprod).

L'ensemble de la solution (application SIRH Solutions et moteur de base de données Oracle) est installé sur un serveur physique unique : srv-sirh.senat.fr.

Ce serveur est sur le même VLAN que l'ensemble des postes des utilisateurs.

QUESTIONS

Question 1 (*1 point*)

Définir les acronymes suivants :

- TMA
- URL
- SSH
- VLAN
- DSN

Question 2 (*2 points*)

Selon vous, pour quelles raisons y-a-t-il plusieurs environnements mis à disposition des développeurs ? D'autres pourraient-ils être nécessaires dans le cadre du projet ?

Question 3 (*4 points*)

Expliquez de façon technique pourquoi il serait nécessaire de faire évoluer l'infrastructure de la solution.

Question 4 (*10 points*)

Vous proposez une nouvelle solution d'infrastructure.

Votre proposition doit couvrir l'ensemble des besoins de la solution SIRH, pour son développement continu et pour son évolution dans le cadre de ce projet. Vous prendrez en compte l'ensemble des besoins et contraintes, notamment réseaux, systèmes, base de données, sauvegarde, sécurité et tests.

Vous êtes libre de faire évoluer tous les éléments qui vous semblent pertinents en adéquation avec les besoins exprimés mais l'exploitation quotidienne ne doit pas être interrompue plus que nécessaire.

Vous proposerez un calendrier de migration indiquant en particulier les principaux jalons du projet et en estimant la part de travail nécessaire à l'équipe systèmes et réseaux.

Vous accompagnerez votre réponse d'au moins un schéma technique de l'infrastructure cible qui devra être expliqué.

Tous vos choix doivent être justifiés et argumentés.

Question 5 (*3 points*)

Pour le 1er mars 2017, vous rédigez une note de synthèse dans des termes non techniques, à destination du Secrétaire Général du Sénat pour le tenir informé du projet. Vous en présentez les grandes lignes, les risques et les enjeux. Si des choix ont été tranchés, ils doivent être présentés dans cette note.

Cette note ne doit pas dépasser une page dactylographiée (environ 500 mots).

LISTE DES ANNEXES AU SUJET

Annexe 1 : Description technique du serveur

srv-sirh.senat.fr *SIRH Solutions (deve et prod)* *Oracle Entreprise (multi instances)*	
Localisation	Salle Palais
Marque	Dell
Modèle	PowerEdge R710
N° de série	D1LSB5K
Date d'achat	25/05/2009
Maintenance	Pro Support 5 ans sous 4h avec conservation des disques
Processeur	2 Intel Xeon X5570
Mémoire	48 Go (12 x 4 Go) (Les emplacements A1/A4/A7 & B1/B4/B7 ne peuvent pas être utilisés sur la configuration mémoire actuelle)
Espace disque	4 x 146 Go SAS en RAID 5 + 4 x 300 Go 10 krpm SAS en RAID 5
Système d'exploitation	Red Hat Enterprise Linux 5.4
Équipements particuliers	4 ports Gb, Controleur Perc 6i 256 Mo Ram

1 Applications Installées

- Oracle
- SIRH solutions

2 Organisation des disques

2.1 Volumes RAID

```
/dev/sda
        type : RAID-5
        composants : disques 0:0:0, 0:0:1, 0:0:2, 0:0:3
        capacité : 408.38 GB
/dev/sdb
        type : RAID-5
        composants : disques 0:0:4, 0:0:5, 0:0:6, 0:0:7
        capacité : 836.63 GB
```

2.2 Partitionnement

```
Disque /dev/sda: 438.4 Go, 438489317376 octets
255 heads, 63 sectors/track, 53309 cylinders
Unités = cylindres de 16065 * 512 = 8225280 octets

Périphérique Amorce    Début        Fin      Blocs    Id  Système
/dev/sda1   *          1          25      200781   83  Linux
/dev/sda2              26       53309   428003730   8e  Linux LVM
```

2.3 Volumes LVM

2.3.1 Groupes de volumes

```
# vgdisplay
 --- Volume group ---
 VG Name               VolGroup00
 System ID
 Format                lvm2
 Metadata Areas        2
 Metadata Sequence No  33
 VG Access             read/write
 VG Status             resizable
 MAX LV                0
 Cur LV                10
 Open LV               9
 Max PV                0
 Cur PV                2
 Act PV                2
 VG Size               1,22 TB
 PE Size               32,00 MB
 Total PE              39832
 Alloc PE / Size       39392 / 1,20 TB
 Free  PE / Size       440 / 13,75 GB
 VG UUID               24YVsO-gojd-Wjel-WHDA-2Ut4-5yPW-gW0ePh
```

2.3.2 Volumes physiques

```
# pvdisplay
 --- Physical volume ---
 PV Name               /dev/sda2
 VG Name               VolGroup00
 PV Size               408,18 GB / not usable 20,39 MB
 Allocatable           yes
 PE Size (KByte)       32768
 Total PE              13061
 Free PE               0
 Allocated PE          13061
 PV UUID               zo7aVt-maM9-2f39-A9Te-CsYV-bqNb-n4CkMK

 --- Physical volume ---
 PV Name               /dev/sdb
 VG Name               VolGroup00
 PV Size               836,62 GB / not usable 32,00 MB
 Allocatable           yes
 PE Size (KByte)       32768
 Total PE              26771
 Free PE               2104
 Allocated PE          24667
 PV UUID               vvfUkD-hHHT-0CWK-jOkK-SfrK-H7P1-rO90WE
```

2.3.3 Volumes logiques

```
# lvdisplay
 --- Logical volume ---
 LV Name                /dev/VolGroup00/LogVol01
 VG Name                VolGroup00
```

```
LV UUID                COwfyr-capk-TjPQ-xEBt-3EL3-hHyC-juT879
LV Write Access        read/write
LV Status              available
# open                 1
LV Size                1,00 GB
Current LE             32
Segments               1
Allocation             inherit
Read ahead sectors     auto
- currently set to     256
Block device           253:0

--- Logical volume ---
LV Name                /dev/VolGroup00/LogVol03
VG Name                VolGroup00
LV UUID                Nfdq3L-ufkU-mtco-enJh-0Dvq-ESYT-pWNDV3
LV Write Access        read/write
LV Status              available
# open                 1
LV Size                4,00 GB
Current LE             128
Segments               2
Allocation             inherit
Read ahead sectors     auto
- currently set to     256
Block device           253:1

--- Logical volume ---
LV Name                /dev/VolGroup00/LogVol02
VG Name                VolGroup00
LV UUID                i8uhVO-pODK-0Vzo-CNYQ-AhAP-cNfU-7P6TVs
LV Write Access        read/write
LV Status              available
# open                 1
LV Size                2,00 GB
Current LE             64
Segments               1
Allocation             inherit
Read ahead sectors     auto
- currently set to     256
Block device           253:2

--- Logical volume ---
LV Name                /dev/VolGroup00/opt
VG Name                VolGroup00
LV UUID                4XmKP8-T9OT-tzxk-a099-0NYB-QO0y-wwqbeu
LV Write Access        read/write
LV Status              available
# open                 1
LV Size                600,00 GB
Current LE             19200
Segments               6
Allocation             inherit
Read ahead sectors     auto
- currently set to     256
Block device           253:3

--- Logical volume ---
LV Name                /dev/VolGroup00/vol2
VG Name                VolGroup00
LV UUID                LjNj1q-3OmP-DgKJ-Pwot-NJVc-iulc-swAWXN
LV Write Access        read/write
LV Status              available
# open                 1
LV Size                200,00 GB
Current LE             6400
Segments               3
Allocation             inherit
Read ahead sectors     auto
- currently set to     256
Block device           253:4

--- Logical volume ---
LV Name                /dev/VolGroup00/vol1
VG Name                VolGroup00
LV UUID                M8q400-jmuR-adWI-k9jM-QrtB-1tDg-Ua2tHc
```

```
LV Write Access        read/write
LV Status              available
# open                 1
LV Size                200,00 GB
Current LE             6400
Segments               3
Allocation             inherit
Read ahead sectors     auto
- currently set to     256
Block device           253:5

--- Logical volume ---
LV Name                /dev/VolGroup00/LogVol04
VG Name                VolGroup00
LV UUID                Lru6W1-AbJc-YLts-e2mg-DPY9-GPVC-6saG91
LV Write Access        read/write
LV Status              available
# open                 1
LV Size                4,00 GB
Current LE             128
Segments               2
Allocation             inherit
Read ahead sectors     auto
- currently set to     256
Block device           253:6

--- Logical volume ---
LV Name                /dev/VolGroup00/LogVol06
VG Name                VolGroup00
LV UUID                H0JdsG-GrYF-4rZO-IAWN-WMWv-6APo-45Be0u
LV Write Access        read/write
LV Status              available
# open                 0
LV Size                2,00 GB
Current LE             64
Segments               1
Allocation             inherit
Read ahead sectors     auto
- currently set to     256
Block device           253:7

--- Logical volume ---
LV Name                /dev/VolGroup00/LogVol05
VG Name                VolGroup00
LV UUID                auC2op-KHya-Iy7i-h6rD-P0rB-7N7y-hDvpYf
LV Write Access        read/write
LV Status              available
# open                 1
LV Size                10,00 GB
Current LE             320
Segments               1
Allocation             inherit
Read ahead sectors     auto
- currently set to     256
Block device           253:8

--- Logical volume ---
LV Name                /dev/VolGroup00/LogVol00
VG Name                VolGroup00
LV UUID                lRwexR-pwXq-M3wl-zC07-dgA6-kFUk-H8FLp2
LV Write Access        read/write
LV Status              available
# open                 1
LV Size                8,00 GB
Current LE             256
Segments               1
Allocation             inherit
Read ahead sectors     auto
- currently set to     256
Block device           253:9
```

2.4 Points de montages

```
swap on /dev/VolGroup00/LogVol00
/dev/sda1 on /boot type ext3 (rw)
/dev/mapper/VolGroup00-opt on /opt type ext3 (rw)
/dev/mapper/VolGroup00-vol1 on /var/opt/oradata/vol1 type ext3 (rw)
/dev/mapper/VolGroup00-vol2 on /var/opt/oradata/vol2 type ext3 (rw)
/dev/mapper/VolGroup00-LogVol01 on / type ext3 (rw)
/dev/mapper/VolGroup00-LogVol02 on /tmp type ext3 (rw)
/dev/mapper/VolGroup00-LogVol03 on /var type ext3 (rw)
/dev/mapper/VolGroup00-LogVol04 on /usr type ext3 (rw)
/dev/mapper/VolGroup00-LogVol05 on /home type ext3 (rw)
```

3 Liste des comptes

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
nscd:x:28:28:NSCD Daemon:/:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin
smmsp:x:51:51::/var/spool/mqueue:/sbin/nologin
rpc:x:32:32:Portmapper RPC user:/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin
avahi:x:70:70:Avahi daemon:/:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
bb:x:103:103:Big Brother:/home/bb:/bin/bash
oracle11g:x:511:500::/home/oracle11g:/bin/ksh
xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin
gdm:x:42:42::/var/gdm:/sbin/nologin
avahi-autoipd:x:104:104:avahi-autoipd:/var/lib/avahi-autoipd:/sbin/nologin
dbasirhdeve:x:514:511::/opt/oracle/admin/dbasirhdeve:/bin/bash
sirhdeve:x:1001:1000::/opt/sirhdeve:/bin/ksh
dbasirhprod:x:551:511::/opt/oracle/admin/dbasirhprod:/bin/bash
sirhprod:x:1005:1000::/opt/sirhprod:/bin/ksh
dbaifm:x:1011:511::/opt/oracle/admin/dbaifm:/bin/bash
dbaamelo:x:516:511::/opt/oracle/admin/dbaamelo:/bin/bash
dbathit:x:555:511::/opt/oracle/admin/dbathit:/bin/bash
apache:x:48:48:Apache:/var/www:/sbin/nologin
oracle12c:x:701:700::/home/oracle12c:/bin/bash
```

Annexe 2 : Dell end of life list

Model	EOSL Date
Dell Equallogic PS100E	04 / 18 / 2013
Dell Equallogic PS4000E	10 / 10 / 2016
Dell EqualLogic PS4000x	
Dell Equallogic PS5000E	08 / 19 / 2014
Dell Equallogic PS5000X	08 / 19 / 2014
Dell Equallogic PS5000XV	08 / 19 / 2014
Dell Equallogic PS5500E	08 / 19 / 2014
Dell Equallogic PS6000E	11 / 11 / 2016
Dell Equallogic PS6000X	11 / 11 / 2018
Dell Equallogic PS6000XV	11 / 11 / 2018
Dell Equallogic PS6010E	06 / 26 / 2017
Dell Equallogic PS6010X	06 / 26 / 2019
Dell Equallogic PS6010XV	06 / 26 / 2019
Dell PowerConnect 2724 24 Port Gb Ethernet Switch	11 / 19 / 2015
Dell PowerConnect 2824 24 port Gb Ethernet Switch	01 / 31 / 2020
Dell PowerEdge 1400SC	07 / 01 / 2007
Dell PowerEdge 1550	07 / 01 / 2007
Dell PowerEdge 1550	07 / 01 / 2007
Dell PowerEdge 1650	07 / 01 / 2008
Dell PowerEdge 1650	09 / 01 / 2008
Dell PowerEdge 1655MC Blade Server	10 / 31 / 2016
Dell PowerEdge 1750	08 / 01 / 2010
Dell PowerEdge 1800	04 / 01 / 2011
Dell PowerEdge 1850	04 / 01 / 2011
Dell PowerEdge 1855 Blade	04 / 01 / 2011
Dell PowerEdge 1950	12 / 12 / 2014
Dell PowerEdge 2400	04 / 01 / 2006
Dell PowerEdge 2450	04 / 01 / 2006
Dell PowerEdge 2500	07 / 01 / 2007
Dell PowerEdge 2550	07 / 01 / 2007
Dell PowerEdge 2600	07 / 01 / 2007
Dell PowerEdge 2650	02 / 01 / 2010
Dell PowerEdge 2800	01 / 01 / 2010
Dell PowerEdge 2850	07 / 01 / 2011
Dell PowerEdge 2950	10 / 19 / 2015
Dell PowerEdge 4300	12 / 31 / 2007
Dell PowerEdge 4400	01 / 01 / 2006
Dell PowerEdge 4600	07 / 01 / 2009
Dell PowerEdge 6400	04 / 01 / 2006
Dell PowerEdge 6450	04 / 01 / 2006
Dell PowerEdge 6650	07 / 01 / 2010
Dell PowerEdge 6800	09 / 01 / 2012
Dell PowerEdge 6850	09 / 01 / 2012
Dell PowerEdge 6950	12 / 31 / 2013
Dell PowerEdge 8450	04 / 01 / 2006
Dell PowerEdge M600 Blade	09 / 01 / 2009

Dell PowerEdge M610 Blade	09 / 01 / 2012
Dell PowerEdge M710 Blade	09 / 01 / 2012
Dell PowerEdge M710HD Blade	09 / 01 / 2012
Dell PowerEdge R310	09 / 01 / 2012
Dell PowerEdge R410	09 / 01 / 2012
Dell PowerEdge R510	09 / 01 / 2012
Dell PowerEdge R610	10 / 10 / 2016
Dell PowerEdge R620	05 / 25 / 2018
Dell PowerEdge R710	05 / 18 / 2016
Dell PowerEdge R720 XD	05 / 18 / 2018
Dell PowerEdge R900	07 / 23 / 2015
Dell PowerEdge R905	07 / 29 / 2004
Dell PowerEdge R910	03 / 29 / 2015
Dell PowerEdge T310	09 / 01 / 2012
Dell PowerEdge T410	09 / 01 / 2012
Dell PowerEdge T610	09 / 01 / 2012
Dell PowerEdge T710	09 / 01 / 2012
Unity 300F	01 / 31 / 2023
Unity 400F	01 / 31 / 2023
VNX7600	01 / 31 / 2023

Annexe 3 : article de presse SIRH Solutions

Prélèvement à la source : SIRH Solutions signe la charte de partenariat Éditeurs avec la Direction Générale des Finances Publiques

31 décembre 2016 - La Rédaction

L'entrée en vigueur du prélèvement à la source de l'impôt sur le revenu au 1er janvier 2019 était confirmée le 13 novembre 2016 par le ministère des Comptes publics. Dans ce cadre, SIRH Solutions, acteur global et leader des ressources humaines, vient de signer la charte de partenariat Éditeurs avec la Direction Générale des Finances Publiques (DGFiP).

La charte a pour objet de définir les engagements réciproques des éditeurs de solutions de logiciels de paie et de la DGFiP pour sécuriser la mise en place de cette réforme.

Depuis 2016, SIRH Solutions suit au plus près la réforme du prélèvement à la source et a participé à la première phase d'expérimentation en décembre 2017, comme employeur du secteur privé, mais également auprès de ses clients pilotes. En signant cette charte, SIRH Solutions s'engage à participer à la deuxième phase qui débutera le 1er mars 2018.

Les équipes de SIRH Solutions, entièrement mobilisées sur ce projet, déploient des offres complètes afin d'accompagner les entreprises dans la mise en œuvre du prélèvement à la source.

À propos de SIRH Solutions

SIRH Solutions offre des solutions RH complètes parfaitement adaptées aux besoins des Directions des Ressources Humaines et aux organisations de moyennes et grandes tailles, des secteurs public et privé. Spécialiste du pilotage des RH de la paie et du talent management dans un contexte local et international, SIRH Solutions accompagne plus de 850 clients, dans plus de 54 pays, en mode « on-premise » ou services d'outsourcing.
Partenaire de la réussite de la transformation digitale de ses clients vers la RH 3.0, SIRH Solutions, acteur global des Ressources Humaines, privilégie la co-innovation, favorise les enjeux de performance RH et met en avant l'expérience collaborateur.

Annexe 4 : Schémas de principe du réseau

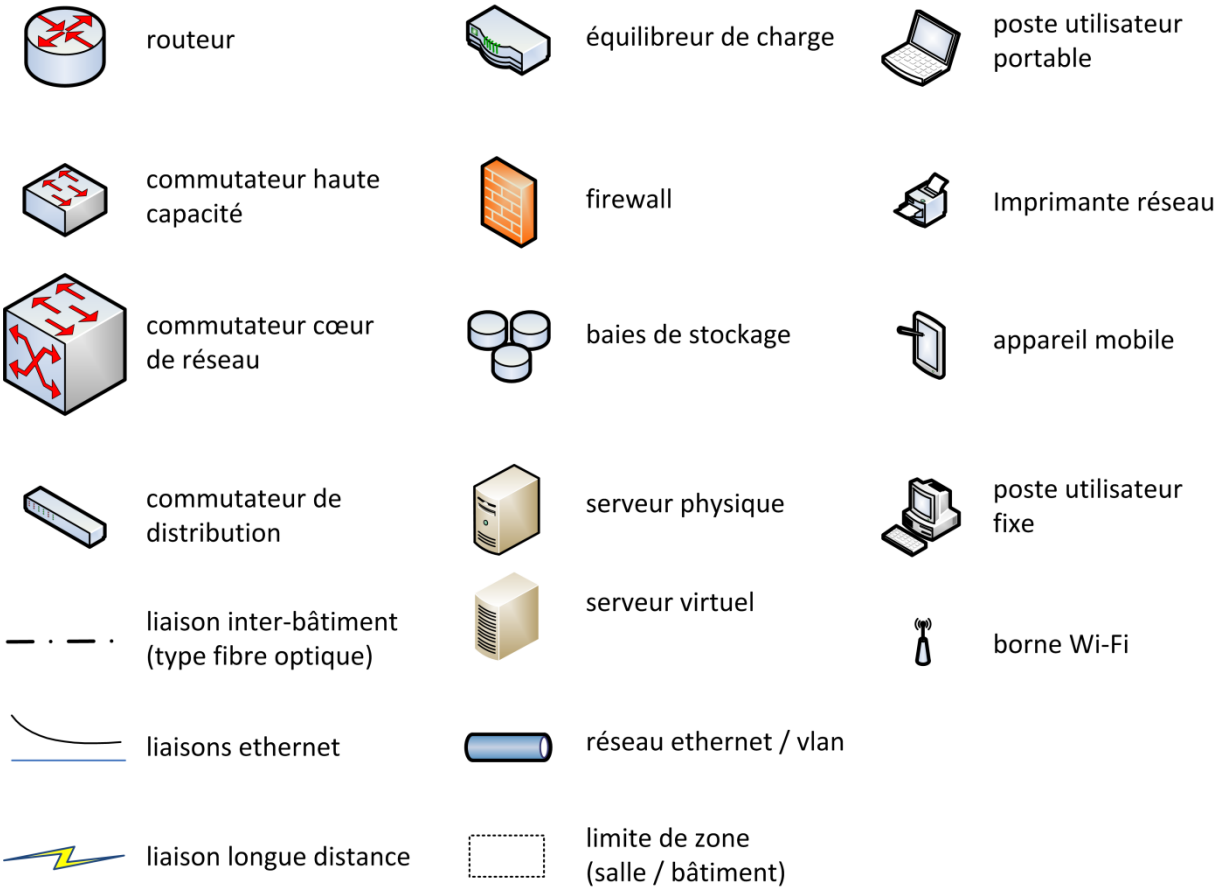


Schéma réseau

Vue physique

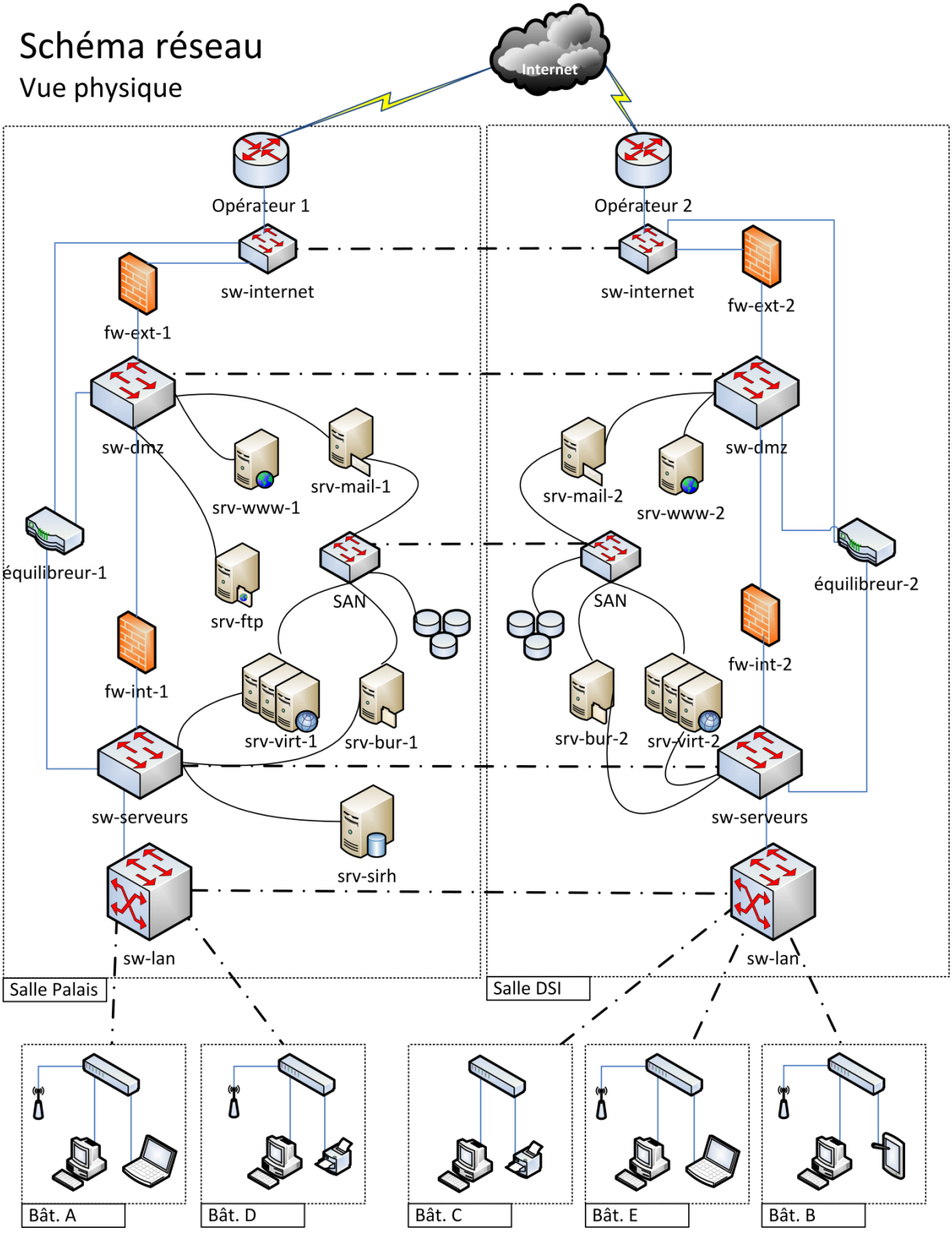
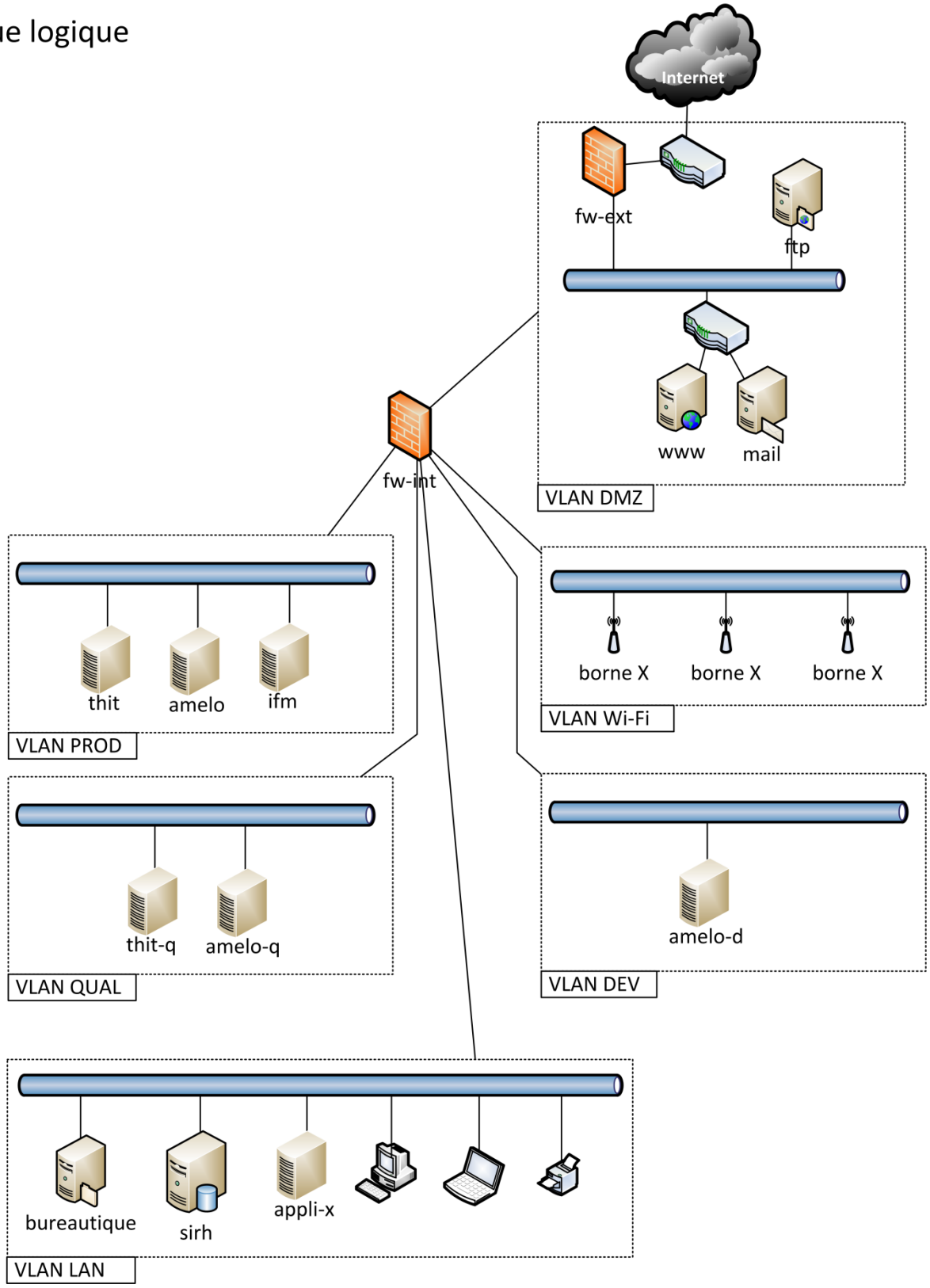


Schéma réseau

Vue logique



RECOMMANDATIONS POUR LA MISE EN PLACE DE CLOISONNEMENT SYSTÈME

GUIDE ANSSI

ANSSI-PG-040
14/12/2017

PUBLIC VISÉ :

Développeur Administrateur RSSI DSI Utilisateur

Informations

Attention

Ce document rédigé par l'ANSSI présente les **« Recommandations pour la mise en place de cloisonnement système »**. Il est téléchargeable sur le site `www.ssi.gouv.fr`. Il constitue une production originale de l'ANSSI. Il est à ce titre placé sous le régime de la « Licence ouverte » publiée par la mission Etalab (`www.etalab.gouv.fr`). Il est par conséquent diffusable sans restriction.

Ces recommandations n'ont pas de caractère normatif, elles sont livrées en l'état et adaptées aux menaces au jour de leur publication. Au regard de la diversité des systèmes d'information, l'ANSSI ne peut garantir que ces informations puissent être reprises sans adaptation sur les systèmes d'information cibles. Dans tous les cas, la pertinence de l'implémentation des éléments proposés par l'ANSSI doit être soumise, au préalable, à la validation de l'administrateur du système et/ou des personnes en charge de la sécurité des systèmes d'information.

Évolutions du document :

VERSION	DATE	NATURE DES MODIFICATIONS
1.0	14/12/2017	Version initiale du document

Table des matières

1
Préambule

La fonction de sécurité de cloisonnement bénéficie d'une popularité bien moindre que celles de confidentialité et d'intégrité. Un mécanisme de cloisonnement permet de compartimenter un environnement d'exécution en plusieurs parties ne comportant pas les mêmes éléments et ne bénéficiant ni des mêmes droits ni des mêmes ressources. Intuitivement, il s'agit de découper un environnement monolithique à la manière d'un puzzle, sans impact sur le service rendu. L'avantage d'une telle démarche tient alors dans la possibilité de restreindre chaque partie de l'environnement aux actions dont elle a besoin. En d'autres termes, l'intérêt du découpage découle de l'application du principe de moindre privilège sur chaque sous-partie de l'environnement. Une fois ceci mis en œuvre, la compromission d'une sous-partie devient plus difficile car sa surface d'attaque est réduite. De plus, une corruption ne peut avoir que des conséquences limitées.

Cette démarche peut être appliquée à tout niveau, à l'échelle d'un système d'information entier comme à l'intérieur d'un processeur matériel dédié à des traitements spécifiques. Dans tous les cas, le même objectif est poursuivi : effectuer un découpage pertinent et choisir des mécanismes adaptés à la restriction des actions possibles pour chaque pièce du puzzle. Les mécanismes de cloisonnement se répartissent en trois grandes catégories qui sont complémentaires : le cloisonnement réseau, le cloisonnement cryptographique et le cloisonnement système. Seul le cloisonnement système est traité ici, bien qu'une grande majorité du document s'applique indifféremment aux trois catégories.

L'ambition de ce document est d'aborder le cloisonnement système de manière générique, en présentant l'intérêt et ses objectifs. En effet, il n'existe pas de méthode universelle de mise en place du cloisonnement. Le lecteur est donc invité à s'approprier une démarche et à développer un esprit critique sur des choix de découpage et de mécanismes. Des définitions et des critères de comparaison sont proposés au fil du document.

Le document débute, en chapitre 2, par la présentation générale de ce en quoi consiste le cloisonnement, de manière à en présenter son intérêt au lecteur. Cette première partie introduit de nombreuses définitions. Formelles, elles sont cependant indispensables pour clarifier les propos développés. De multiples exemples viennent agrémenter ce chapitre pour concrétiser les notions abordées. La détermination des besoins en cloisonnement est détaillée dans le chapitre 3. Il s'agit d'évaluer la pertinence du découpage en fonction des objectifs visés. Après la lecture des chapitres 2 et 3, le lecteur est familier avec les enjeux liés à la mise en place de cloisonnement. Il reste à lui fournir des outils concrets d'analyse de la sécurité apportée par un choix d'architecture donné. Le chapitre 4 propose ainsi une série de critères d'évaluation de mises en oeuvre de cloisonnement. Enfin, l'approche du document dans sa globalité est illustrée dans le dernier chapitre par une brève analyse d'architecture de sonde réseau de détection des incidents de sécurité.

2
Le cloisonnement, qu'est-ce que c'est ? Quel en est l'intérêt ?

Composant, système

Pour éviter les confusions, le terme *composant* désigne dans la suite ce qui est développé ou évalué, par opposition au mot *système*, employé pour désigner l'écosystème (machine, système d'information, etc.) dans lequel le composant va être utilisé.

L'exception notable à cette règle concerne l'expression « composants de confiance » définie ci-après, qui ne coïncident pas avec le composant développé ou évalué.

Exemples. Un composant, au sens du document, recouvre donc des réalités aussi variées qu'un chiffreur, un composant cryptographique embarqué, un navigateur Internet, ou un hyperviseur.

2.1 Une implémentation du principe de moindre privilège

De l'utilisation d'un composant logiciel ou matériel résulte un certain nombre d'effets de bord sur son environnement. Idéalement, l'environnement d'exécution du composant ne doit jamais être mis en défaut, ni du point de vue fonctionnel ni du point de vue de la sécurité.

Deux conditions doivent être remplies pour fournir de telles garanties. Premièrement, être en mesure de spécifier parfaitement tous les comportements possibles du composant sans abstraire aucun détail, et en toutes circonstances. Deuxièmement, garantir que le composant se conforme toujours à ce qui est spécifié. Si ces deux critères sont remplis, rien de fâcheux ne peut se produire : tout est prévu. Néanmoins, une telle situation n'existe évidemment pas en pratique.

Objectif

Le cloisonnement est implémenté pour *restreindre les conséquences possibles de comportements inattendus* d'un composant, qu'il s'agisse d'un bogue ou de son détournement par un attaquant.

Pour ce faire, il est habituel de restreindre l'environnement d'exécution du composant aux ressources strictement nécessaires à ses besoins. Ce principe classique est connu sous le nom de principe de moindre privilège.

2.1.1 Rappels sur le principe de moindre privilège

Ce principe constitue l'un des fondements du développement sécurisé. Pour être complet, ce document en fournit un rappel en définissant les termes utilisés.

Les concepts utilisés ici sont issus de la littérature académique portant sur le contrôle d'accès. Ces travaux utilisent généralement la terminologie suivante : des *sujets* peuvent être autorisés à effectuer des *actions* sur des *objets* ou d'autres sujets. Dans ce document, les sujets sont des *tâches* et les objets des *ressources*.

Tâche

Une tâche est un ensemble d'instructions chargées en mémoire au fur et à mesure pour être exécutées.

Exemples. L'exemple le plus classique de tâche est celui d'un processus s'exécutant en espace utilisateur au sein d'un système d'exploitation implémentant une séparation entre espace utilisateur et espace noyau. Une machine virtuelle dans un hyperviseur est un autre exemple.

Ressource

La notion de ressource correspond ici à une information, et par extension à l'objet logiciel ou matériel qui la contient et permet de la manipuler.

Exemples. Un descripteur de fichier, une clé cryptographique, un fichier, une socket réseau sont autant d'exemples de ressources logicielles. La mémoire RAM, les registres du processeur, les caches du processeur, les unités de stockage de type disque dur ou encore les périphériques externes constituent des exemples de ressources matérielles.

Action (agir)

Toutes les formes d'accès, d'utilisation ou de transmission des ressources constituent des actions.

Exemples. Le concept d'action sur des ressources recouvre des réalités aussi diverses que l'ouverture de fichiers, l'émission et la réception de signaux, l'usage de sockets réseau ou la génération et le traitement d'interruptions.

Privilège

Un privilège permet à une tâche qui en dispose de mener légitimement à bien une action sur une ressource, autrement dit sur tout ou partie d'un composant ou des informations qu'il utilise.

Lorsqu'un attaquant élève illégitimement ses privilèges, il devient alors en capacité de mener à bien des actions normalement interdites par un mécanisme de sécurité.

Dans tout le document, sauf mention contraire, les termes tâche, ressource, action (ou le verbe agir) et privilège gardent leur sens très général défini ici.

Principe de moindre privilège

Le principe de moindre privilège stipule qu'une tâche ne doit bénéficier que des privilèges strictement nécessaires à l'exécution du code menant à bien ses fonctionnalités.

En d'autres termes, une tâche ne devrait avoir la possibilité de mener à bien que les actions dont l'utilité fonctionnelle est avérée.

En général, on ne peut pas appliquer des restrictions à un tel niveau de granularité, mais l'idée est bien de s'en rapprocher le plus possible.

R1

Appliquer le principe de moindre privilège dès la conception

Interdire par défaut toute action et procéder à l'autorisation exclusive de ce qui est nécessaire aux tâches constitue la stratégie la plus efficace de mise en œuvre du principe de moindre privilège. Il convient de s'y conformer autant que possible dès la phase de conception du composant.

Le principe de moindre privilège va de pair avec l'idée de séparation des privilèges. Comme présenté en préambule du document, réduire les privilèges d'un composant monolithique est toujours profitable, mais souvent insuffisant. Les stratégies de découpage, qui relèvent plus de la séparation des privilèges que de l'application du principe de moindre privilège, sont discutées plus loin, en chapitre 3.

Cette manière de faire n'est pas toujours possible - en particulier lorsque l'on intègre des produits sur étagère. Cependant, s'y prendre ainsi permet d'éviter d'oublier d'interdire des accès.

2.1.2 Aperçu de la mise en place de cloisonnement

Le cloisonnement peut être appréhendé comme la mise en œuvre du principe de moindre privilège au sein d'un composant. Pour l'implémenter, il faut suivre les étapes suivantes :

- *identifier des privilèges nécessaires à un composant.* C'est identifier une liste d'actions qu'il doit être capable de mener à bien dans son environnement d'exécution ;
- *créer un environnement d'exécution réduit à cette liste d'actions (ou s'en rapprocher le plus possible).* Des mécanismes de cloisonnement, disponibles au niveau de l'environnement d'exécution, sont mis en œuvre dans ce but.
  Beaucoup d'exemples peuvent être cités : dispositifs de contrôle d'accès (dans le système de fichiers, pour les accès réseau, etc.), utilisation de modes du processeur pour différencier les pages accessibles en mode privilégié des pages accessibles en mode utilisateur, usage de machines virtuelles différentes au sein d'un hyperviseur, etc. ;
- *itérer cette pratique sur chaque composant.* Scinder l'environnement d'exécution global d'un ensemble de composants en une série de sous-environnements appauvris.

Il existe en général plusieurs manières de parvenir à un même résultat, mais qui ne sont pas équivalentes du point de vue de la sécurité. Ce document vise à mettre en exergue une démarche de

conception qui respecte la philosophie dictée par les principes de moindre privilège et de défense en profondeur. Appliquer ces principes influe profondément sur l'architecture choisie.

R2

Tenir compte de ses besoins en cloisonnement dès l'initiation d'un projet

Les besoins en cloisonnement d'un composant doivent faire l'objet d'un diagnostic et être considérés comme des besoins au même titre que les besoins fonctionnels, et ce dès le début du projet.

Attention

Les conséquences sur l'architecture du composant peuvent être importantes et engendrer des surcoûts imprévus en cas de prise en compte tardive de besoins de sécurité.

Dans une démarche d'intégration, la qualité de la solution globale dépend également de la prise en compte des bonnes pratiques au niveau de chaque brique élémentaire. Plus particulièrement en ce qui concerne les besoins en cloisonnement, utiliser des briques nécessitant des privilèges trop élevés par rapport à leur fonction va dégrader la qualité de la solution globale.

R3

Préférer des composants implémentant un cloisonnement pertinent

Lors d'un choix entre différentes solutions, celles qui démontrent la meilleure prise en compte du principe du moindre privilège devront être préférées.

2.2 Formalisation en tant que fonction de sécurité

Cette section présente une approche générale du cloisonnement, certes un peu abstraite, mais qui permet de fixer le vocabulaire qui sera utilisé dans la suite du document.

Domaine

Un domaine est l'environnement d'exécution d'une tâche. Il est défini par l'ensemble des ressources (logicielles et matérielles) sur lesquelles la tâche peut effectuer des actions. Par opposition, une ressource sur laquelle la tâche ne peut pas agir ne fait pas partie de son domaine.

Information

Il est possible que plusieurs tâches cohabitent dans un domaine. Quelle que soit la réalité désignée, par abus de langage, ce document utilise systématiquement « tâche » au singulier. Ainsi, l'entité logique vis-à-vis du cloisonnement est une tâche.

Exemples. En considérant comme exemple de tâche un processus s'exécutant en espace utilisateur, un domaine est formé par toutes les ressources que le processus peut utiliser : tous les fichiers accessibles, les appels système possibles, les périphériques utilisables, etc.

Politique de sécurité

Cloisonner des tâches consiste à définir pour chacune son domaine d'exécution, ce qui a vocation à séparer les ressources en deux catégories :

- les *ressources partagées* entre plusieurs domaines, i.e. sur lesquelles plusieurs tâches peuvent légitimement agir ;
- les *ressources propres* à un domaine donné, i.e. sur lesquelles seule la tâche s'exécutant dans ce domaine doit être en capacité d'agir.

Cette spécification précise des domaines constitue une *politique de sécurité*.

Fonction de sécurité de cloisonnement (ou confinement)

Le cloisonnement est la fonction de sécurité garantissant qu'une tâche ne peut effectuer que les actions spécifiées par la politique de sécurité sur les ressources.

Exemples. Dans le cas des processus, les ressources partagées sont toutes celles auxquelles plusieurs processus peuvent accéder, parmi lesquelles le noyau du système d'exploitation, le matériel physique, etc. En l'absence de mesure particulière, les processus lancés par un utilisateur ont accès à tous les fichiers de l'utilisateur [1] : ces derniers constituent des ressources partagées.
Par défaut, un processus a pour ressources propres, l'espace mémoire utilisateur que le noyau lui a fourni, ainsi que le contexte d'exécution qui lui est associé. Ce contexte contient tout ce qui est mis en place par le noyau à chaque ordonnancement du processus : table de pages, pointeurs de pile, valeurs des registres du processeur, etc. Comme mentionné plus haut, le code du noyau est par contre une ressource partagée entre processus, et non une ressource propre : il n'est en effet pas dupliqué.

Attaquant de la fonction de sécurité de cloisonnement

L'attaquant d'une solution de cloisonnement est supposé être en contrôle d'un ou plusieurs domaines, et donc des tâches qui s'y exécutent. Son but est d'effectuer une action sur une ressource, interdite par la politique de sécurité.

Exemples. Un attaquant contrôlant un processus a réussi une attaque lorsque, par exemple, il peut écrire ou lire dans l'espace mémoire réservé à un autre processus, disons la valeur de secrets. Attention, si ces secrets sont en fait stockés dans un fichier auquel le processus compromis a accès par défaut selon la politique de sécurité, ce n'est pas le cloisonnement entre processus qui a été mis en défaut ! C'est la politique de sécurité qui n'est pas définie de manière satisfaisante.

Information

Même si le cloisonnement s'entend généralement comme existant entre au moins deux entités, il reste fréquent de parler de cloisonner ou confiner une tâche vis-à-vis du reste du système. Le cas échéant, deux domaines existent : celui de la tâche à confiner, et celui de toutes les autres tâches sur le système.

Mettre en place du cloisonnement implique d'implémenter concrètement les domaines, c'est-à-dire d'exercer un contrôle sur les actions effectuées par les tâches, de manière à interdire ce qui

1. On parle du cas par défaut sous Linux et Windows. Le positionnement de droits particuliers est abordé dans les exemples en section 2.3.

doit l'être. Sans un arbitre dont le rôle est de prendre la décision pour chaque action de chaque tâche de l'autoriser ou non, la politique de sécurité serait définie à titre indicatif et n'aurait aucun effet pour se protéger de comportements malveillants.

Moniteur de référence

Le moniteur de référence est l'entité qui implémente le mécanisme de contrôle d'accès et qui prend la décision d'autoriser ou d'interdire une action d'une tâche sur une ressource. C'est donc le moniteur de référence qui met en œuvre la politique de sécurité pour chaque domaine.

Il peut être complexe d'isoler ce code concrètement, auquel cas identifier un composant l'englobant est satisfaisant.

Exemples. En poursuivant sur l'exemple des processus utilisateurs, le moniteur de référence est constitué par le code du noyau qui gère les changements entre processus et les accès à la mémoire de chaque processus. C'est parce qu'un contexte d'exécution différent, propre à chaque processus, existe et est mis à jour par le noyau à chaque ordonnancement d'un processus, qu'il y a une isolation entre les espaces mémoire des processus. Le moniteur de référence est dans ce cas le noyau partagé par les processus ; même si tout le code du noyau n'est pas concerné, cette approximation est considérée comme valide.

Tâche	Processus utilisateur
Ressources propres	Contexte d'exécution du processus Mémoire en espace utilisateur
Ressources partagées	Objets système visibles par d'autres processus (fichiers, périphériques, etc.) Noyau, matériel physique
Moniteur de référence	Noyau du système d'exploitation

Tab. 2.1 – Exemple des processus utilisateurs

2.3 Application des définitions sur quelques exemples

Cette partie développe d'autres exemples de mécanismes de cloisonnement de manière à illustrer les concepts assez abstraits introduits précédemment.

2.3.1 Systèmes d'hypervision

Le premier exemple est celui d'un hyperviseur exécutant plusieurs machines virtuelles. Il existe deux types d'hyperviseurs, dits de type 1 et 2. Les hyperviseurs de type 1 s'exécutent nativement sur le matériel, contrairement aux hyperviseurs de type 2, qui s'exécutent au sein d'un système d'exploitation pour hyperviser des systèmes invités. Pour simplifier le propos, seuls les hyperviseurs de type 1 sont traités ici. Concrètement, Xen, KVM, ESXi ou encore Hyper-V sont des hyperviseurs de type 1, tandis que Qemu (utilisé seul) et VirtualBox sont de type 2.

Dans ce cas de figure, une machine virtuelle, dite aussi invitée, constitue une tâche. Les ressources propres à une machine virtuelle regroupent toutes les ressources virtuelles telles que vues par le

système invité [2], son espace mémoire, fourni par l'hyperviseur, ainsi que toutes les informations de contexte stockées par l'hyperviseur entre deux ordonnancements. Les ressources partagées comprennent les composants matériels communs à plusieurs machines virtuelles, l'hyperviseur qui les exécute, ainsi que les éventuels partages mis en place entre machines virtuelles. Le domaine d'une machine virtuelle regroupe donc toutes ses ressources propres et ce qu'elle partage avec d'autres machines virtuelles.

Dans les faits, un système d'hypervision est rarement réduit à un hyperviseur seul. En effet, les rôles d'analyse des actions effectuées par les machines virtuelles et d'émulation des périphériques réels sont rarement effectués par l'hyperviseur lui-même. En pratique, c'est classiquement un noyau ou une machine invitée ayant un statut un peu particulier qui remplit ces rôles, tout en s'exécutant avec moins de privilèges que l'hyperviseur lui-même. Concrètement, c'est le cas du dom0 de Xen, du noyau Linux hôte de KVM, ou de VMkernel dans ESXi. Il convient de considérer cette ressource particulière, utilisée par toutes les autres machines virtuelles, comme une ressource partagée. Dans la suite, pour éviter les confusions, les tâches désignent les machines virtuelles sans rôle particulier.

En ce qui concerne Windows 10, le parti pris de ce document est de considérer Hyper-V comme seul élément du système d'hypervision, dont la vocation est de fournir du cloisonnement mémoire entre la machine invitée « Virtual Secure Mode » et celle contenant l'environnement Windows standard.

Dans ces différents cas, le moniteur de référence est le système d'hypervision : sollicité lors d'accès par une machine virtuelle au matériel partagé, en particulier la mémoire physique, il est garant du respect de l'isolation entre les tâches. D'ailleurs, la terminologie VMM (pour Virtual Machine Monitor) est aussi employée pour parler d'hyperviseurs, ce qui illustre bien cette idée de moniteur.

Tâche	Machine virtuelle
Ressources propres	Contexte d'exécution Mémoire occupée par la machine virtuelle Ressources virtuelles dans le système invité
Ressources partagées	Partages configurés Système d'hypervision, matériel physique
Moniteur de référence	Système d'hypervision

Tab. 2.2 – Exemple des hyperviseurs

2.3.2 Utilisateurs distincts dans un système d'exploitation

Au sein des systèmes d'exploitation classiques comme Windows, ou les systèmes type UNIX, il existe une notion d'utilisateur et de privilèges dont bénéficie cet utilisateur. Typiquement, un contrôle d'accès est exercé par le noyau du système d'exploitation pour décider si un processus lancé par un utilisateur a le droit d'accéder à une ressource du système. Différents modèles de contrôle d'accès existent. Dans le cadre d'un contrôle d'accès discrétionnaire (dit DAC pour *Discretionary Access Control* en anglais), le propriétaire d'une ressource peut configurer les permissions d'accès à celle-ci. Ce genre de contrôle d'accès est souvent complété d'un contrôle d'accès obligatoire (dit MAC pour *Mandatory Access Control*), qui consiste en une politique de sécurité imposée sur toute ressource du

2. et également, s'il y en a, l'ensemble des composants matériels exclusivement accessibles à la machine virtuelle (dits périphériques délégués).

système indépendamment de son propriétaire. Parmi les implémentations classiques de contrôles d'accès obligatoires figurent le mécanisme MIC (*Mandatory Integrity Control*) dans les systèmes Windows, ainsi que SELinux ou encore AppArmor dans les systèmes Linux.

Dans ce contexte, un domaine est constitué de tout ce qui est utilisable par un utilisateur donné. Une tâche est formée de tous les processus d'un utilisateur donné. Elle regroupe donc autant de processus qu'il s'en exécute sous l'identité à laquelle elle correspond, au contraire de l'exemple détaillé en 2.2, selon lequel une tâche est un processus donné. En effet, ici on s'attache à instancier les définitions dans le cadre du cloisonnement entre utilisateurs, et non entre processus.

Les ressources propres à une tâche sont celles accessibles exclusivement à l'utilisateur auquel la tâche correspond (certains fichiers, données d'authentification, etc.). Les ressources partagées regroupent tous les objets système partagés par configuration, ainsi que l'intégralité du code noyau et l'ensemble des composants matériels.

Enfin, l'entité qui gère le contrôle d'accès dans le noyau est ici le moniteur de référence. Plus généralement, le noyau peut être considéré comme moniteur de référence garant du respect des permissions sur les objets système, qu'il met à disposition des utilisateurs.

Tâche	Tout ce qui s'exécute sous l'identité de l'utilisateur
Ressources propres	Objets systèmes accessibles exclusivement à l'utilisateur
Ressources partagées	Objets systèmes accessibles à d'autres utilisateurs Noyau, matériel physique
Moniteur de référence	Noyau du système d'exploitation

Tab. 2.3 – Exemple des utilisateurs d'un système d'exploitation

2.3.3 Conteneurs et bacs à sable

Il existe de multiples solutions de conteneurisation et autres bacs à sable, parmi lesquelles LXC, CoreOS Rkt, Docker ou Kubernetes. Ces solutions ne sont pas équivalentes d'un point de vue de la sécurité apportée. Pour comprendre en détail les enjeux des conteneurs Linux, les documents rédigés par NCC Group ([7] et [8]) constituent un bon point de départ. Il s'agit seulement ici d'établir ce à quoi correspondent les définitions de manière assez générique.

Les conteneurs ou bacs à sable créés par une solution sont nommés *cages* dans la suite. Les cages constituent des domaines, et tout ce qui s'exécute à l'intérieur d'une cage forme une tâche.

Suivant les solutions, les ressources propres et partagées peuvent varier ; souvent les cages ont leur propre instance de système de fichiers. Un fichier de configuration par cage permet en général de mettre en place les partages désirés.

Les cages sont contrôlées par un ou plusieurs programmes qui les initialisent et permettent de les gérer. Ceux-ci peuvent être intégrés ou non, suivant les implémentations, au noyau du système d'exploitation qui supporte la solution. Ils s'appuient sur le noyau du système pour isoler les cages entre elles (positionnement de permissions dédié, usage de solutions de contrôle d'accès intégrées au noyau, etc.). Ces programmes gestionnaires et le noyau du système d'exploitation constituent le moniteur de référence pour cet exemple.

Tâche	Tout ce qui s'exécute dans une cage
Ressources propres	Configuration de la cage Ressources auxquelles seule la cage peut accéder (par choix d'implémentation ou par configuration)
Ressources partagées	Programme de gestion des cages Noyau du système d'exploitation Matériel physique Autres, suivant les implémentations
Moniteur de référence	Noyau et programmes de gestion des cages

Tab. 2.4 – Exemple des cages (conteneurs ou bacs à sable)

3
Identifier ses besoins en cloisonnement

Ce chapitre a pour but de dégager une manière de dresser un inventaire des besoins d'un composant en matière de cloisonnement. L'identification de ces besoins permet d'orienter son développement, ou encore de choisir entre plusieurs composants déjà disponibles.

Le cahier des charges fonctionnel définissant le composant est supposé établi. Le composant est, à ce stade, encore appréhendé de manière imprécise et monolithique.

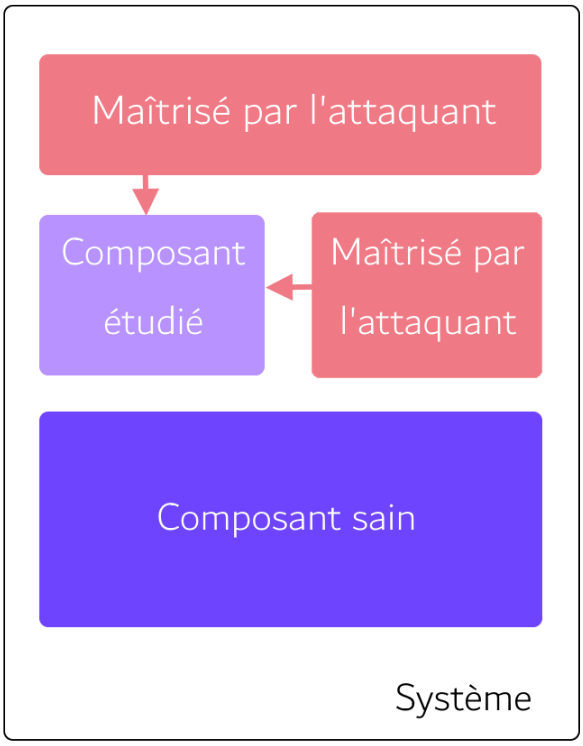


FIG. 3.1 – Perception initiale du composant au sein du système qui l'accueille

Il n'existe pas de méthode absolue à recommander inconditionnellement. Par conséquent, ce document aspire à expliquer précisément *comment* la mise en place d'un cloisonnement pertinent permet d'augmenter la sécurité d'un composant. Le lecteur du document est encouragé à s'approprier les raisonnements présentés pour les décliner dans son propre contexte.

Dans un premier temps, ce document rappelle des fondamentaux de la sécurité du composant dans sa globalité, avant d'aborder l'introduction du cloisonnement pour augmenter le niveau de sécurité du composant.

Exemples. Pour illustrer les concepts présentés, l'exemple choisi est celui du développement d'une application métier sur un modèle client-serveur, permettant à des utilisateurs de travailler sur des projets en commun. La partie serveur de l'application, vouée à s'exécuter en espace utilisateur sur un serveur accessible par plusieurs machines distantes, est plus précisément celle évoquée.

Attention

Cet exemple n'a en aucun cas valeur d'architecture recommandée : il s'agit d'un outil pédagogique permettant d'illustrer les définitions et les raisonnements utiles à l'évaluation d'une architecture en matière de sécurité.

3.1 Généralités sur la sécurité du composant

Spécifier la sécurité attendue d'un composant consiste à identifier quatre éléments fondamentaux :

- les biens sensibles que le composant doit protéger ;
- les capacités de l'attaquant duquel le composant se protège ;
- le périmètre exact du composant ;
- les fonctions de sécurité à remplir par le composant.

Ces quatre éléments sont interdépendants.

D'autres documents de référence peuvent aider à formuler les attentes en matière de sécurité à divers niveaux de précision et d'abstraction (par exemple [5] ou [6]). Le présent document ne prétend pas détailler l'élaboration de l'analyse de la sécurité attendue. Seules les définitions et les précisions qui sont utiles pour la suite sont explicitées ici.

3.1.1 Biens sensibles à protéger par le composant

Biens sensibles

Les biens à protéger sont constitués des informations sensibles manipulées par le composant. Bien souvent, il s'agit directement d'informations métier utilisées par le composant. D'une façon plus générale, cela inclut aussi les informations dont l'obtention permet celle d'informations métier utiles.

C'est en particulier classiquement le cas des clés cryptographiques et de secrets d'authentification. Souvent, ces informations ne sont pas les objets protégés in fine. Cependant, il faut les protéger d'un attaquant au même titre que les données métier car elles peuvent permettre à l'attaquant d'élargir son périmètre d'influence.

Exemples. Dans le cas de l'application serveur métier, les biens à protéger sont les données métier manipulées par les utilisateurs. Un contrôle d'accès sur ces données doit être imposé, permettant que seuls les utilisateurs autorisés puissent lire et/ou modifier des données. Ceci va engendrer la nécessité d'authentifier les utilisateurs auprès de l'application, et les secrets cryptographiques utilisés pour cette authentification seront alors ajoutés à la liste des biens sensibles.

3.1.2 Composants de confiance

Lors de l'analyse de sécurité d'un composant donné, d'autres composants sont considérés comme *de confiance*. Ceci ne signifie **pas** qu'ils ne soient pas corruptibles dans l'absolu ; il s'agit d'une hypothèse de travail. Prendre des mesures assurant leur intégrité n'est pas superflu, bien au contraire.

Composants de confiance

Les composants de confiance sont les composants logiciels et matériels supposés parfaits dans l'analyse de la sécurité attendue d'un composant. En d'autres termes, l'analyse de sécurité repose sur l'hypothèse que les composants de confiance ne peuvent pas être corrompus par un attaquant tel que défini dans cette analyse.

Attention

L'analyse de sécurité d'un composant ne peut pas être construite sur l'hypothèse que le composant entier est lui-même de confiance.

Il serait faux d'affirmer que le composant développé ne peut pas contenir de composants de confiance. Typiquement, c'est le cas s'il dispose de l'accès au matériel au plus bas niveau existant dans le contexte d'utilisation envisagé, sans contrôle possible d'une autre entité système. Cette éventualité se présente si le composant comprend un noyau de système d'exploitation non hypervisé ou un hyperviseur. Dans ce cas de figure, il convient en réalité d'effectuer une analyse de sécurité par niveau d'abstraction couvert. Par exemple, la sécurité est d'abord étudiée en supposant que le système d'hypervision et les noyaux des systèmes hypervisés sont de confiance, au contraire des espaces utilisateurs des systèmes hypervisés qui peuvent être compromis. Dans un second temps, appliquant une démarche de défense en profondeur, la sécurité est examinée en prenant pour hypothèse que seul le système d'hypervision est de confiance, et que l'attaquant est capable de compromettre les systèmes hypervisés complets.

Dans ce chapitre, le propos tenu s'applique à un niveau d'abstraction donné, supposé pour simplifier contenir tout le composant étudié. Ce dernier s'appuie donc sur des composants de confiance et un moniteur de référence externes.

Attention

Le raisonnement justifiant la sécurité du composant étudié repose sur l'hypothèse de l'intégrité des composants de confiance. Il faut donc faire en sorte que dans la réalité, cette hypothèse soit vérifiée.

R4

Garantir l'intégrité des composants de confiance

Il est impératif de garantir concrètement l'intégrité des composants de confiance pour que la sécurité de l'ensemble du composant soit assurée. Des recommandations plus précises sont fournies en 4.1.

Exemples. Dans le cas de l'application serveur, le noyau du système d'exploitation du serveur physique (et les couches d'hypervision éventuelles qui l'exécutent), ainsi que le matériel sur lequel ceci est installé font partie des composants de confiance. Les périphériques matériels (et leurs micrologiciels) utilisés par le serveur physique font également partie des composants de confiance.

3.1.3 Périmètre du composant

Dans le système au sein duquel il sera utilisé, le composant va partager des *interfaces* avec d'autres composants, ce qui peut mettre en péril les fonctions de sécurité visées. Décrire le périmètre exact du composant à sécuriser, c'est notamment dresser la liste de ses *interfaces externes*.

Interfaces du composant

Une interface de programmation définit la manière d'échanger de l'information entre deux composants.

Les interfaces externes sont des interfaces entre le composant pris dans sa globalité et son environnement d'exécution. Elles contiennent au moins toutes les interfaces exposées par le composant à ses utilisateurs.

Exemples. Dans l'exemple du chapitre, les API (Application Programming Interface) mises à disposition par l'application serveur pour ses clients sont des interfaces externes exposées. Les appels système au système d'exploitation au-dessus duquel s'exécute l'application et le système de fichiers utilisé par l'application pour stocker les données métier constituent des exemples d'interfaces externes utilisées par le composant.

Une interface externe ne sépare pas forcément deux éléments logiciels. L'interface entre un pilote de périphérique d'une part et le matériel qu'il contrôle d'autre part est mixte.

Surface d'attaque et surface de friction

La *surface d'attaque* d'un composant est constituée de toutes les interfaces externes du composant lui permettant de communiquer avec un environnement contrôlé par l'attaquant. Dans l'immense majorité des cas, toutes les interfaces exposées par le composant à ses utilisateurs en font partie.

Les autres interfaces externes du composant forment la *surface de friction* du composant avec le reste du système. La surface de friction comprend entre autres les interfaces du composant avec les composants de confiance.

Ces concepts sont illustrés sur la figure 3.2. Identifier la surface d'attaque et la surface de friction du composant avec le système global est essentiel pour permettre une prise en compte de tous les besoins en sécurité du composant. Bien définir la surface de friction permet aussi de garantir l'innocuité du composant pour le système global.

Exemples. Dans le cas de l'application serveur, la surface d'attaque est constituée de l'interface utilisateur de l'application. La surface de friction comprend tous les appels système.

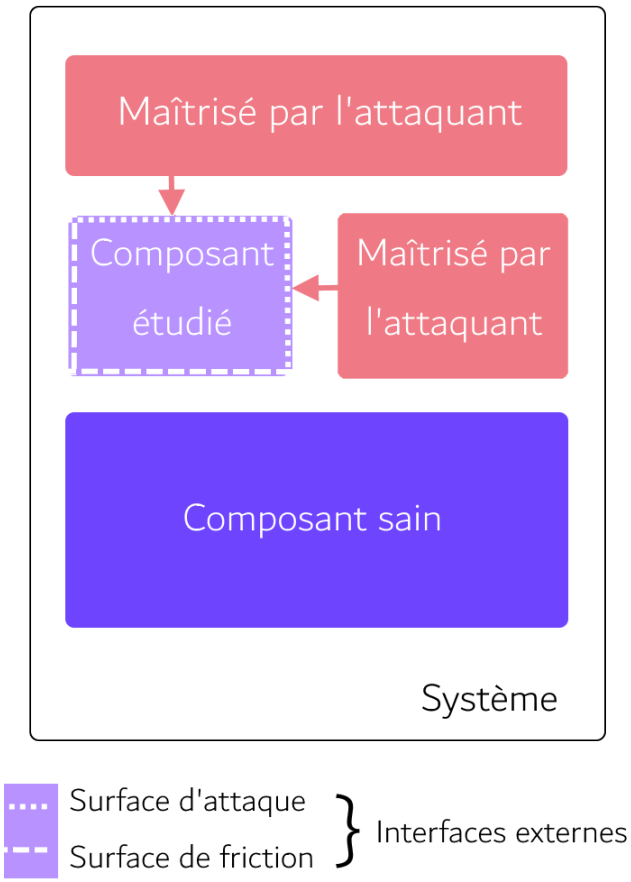


FIG. 3.2 – Interfaces externes du composant

Les appels système forment une interface entre le noyau du système d'exploitation, composant de confiance dans l'exemple du chapitre, et l'application métier. Évidemment, le noyau n'est pas « dangereux » pour l'application. Il est de confiance, et donc réputé non corruptible par un attaquant du composant.
Cependant, les appels système ne sont pas tous équivalents du point de vue de l'application développée. Ceux qui permettent d'utiliser le système de fichiers ont beau s'exécuter exactement comme prévu, ils peuvent permettre l'accès à des données métier gérées par cette application via d'autres applications s'exécutant sur le serveur, sans que l'attaquant ait corrompu l'aaplication développée. Inversement, la compromission dudit composant ne devrait idéalement pas permettre d'accéder à toutes les données du serveur.

3.1.4 Formaliser la sécurité attendue du composant

Pour définir les besoins de sécurité d'un composant, il sera donc nécessaire de réaliser une analyse de la sécurité attendue, qui présentera le bilan de tous les éléments évoqués dans les paragraphes précédents.

R5

Rédiger l'analyse de la sécurité attendue du composant

Une analyse de la sécurité attendue du composant doit faire partie des documents de conception ou intégration mis à disposition.

Elle doit comporter les définitions des quatre éléments cités ci-dessus :

- la liste des biens sensibles à protéger ;
- le modèle d'attaquant pris en compte (duquel découle en particulier l'identification des composants de confiance) ;
- le périmètre du composant, c'est-à-dire sa surface d'attaque et sa surface de friction avec le système global ;
- les fonctions de sécurité attendues.

3.2 Définition des usages du composant

Cette section et la suivante ont pour but d'expliciter le principe global d'architecture consistant à mettre en oeuvre, au sein d'un composant, du cloisonnement entre chacun de ses usages. Mais comment déterminer ce qui relève d'un même usage ? Quand deux contextes d'utilisation font appel à des ressources de sensibilité différente, il est pertinent de séparer ceux-ci en des usages distincts. De même, la disparité des risques de compromission provenant de la manière d'interagir avec le reste du système constitue un critère de séparation. L'exemple typique est l'administration d'un composant, qu'il convient d'appréhender comme un usage particulier.

Usages d'un composant

Des scénarios d'utilisation du composant dans lesquels les ensembles de ressources utilisées diffèrent notablement constituent des usages distincts du composant. Pour mesurer cette différence, il convient d'examiner entre autres :

- les formes et sources d'interaction du composant avec l'extérieur, qui représentent autant de vecteurs de compromission potentiels : par exemple, une différence de connectivité réseau (un usage demande une connection Internet et l'autre une connexion Intranet), ou encore l'exécution de traitements compliqués de données provenant de l'extérieur (du *parsing* par exemple) pour lesquels la présence d'une vulnérabilité ne peut être écartée ;
- la criticité et la sensibilité des ressources utilisées ;
- la périodicité de l'exécution des actions. Par exemple, certaines actions uniquement effectuées lors d'une initialisation sont à distinguer des actions utiles par la suite ;
- s'il s'agit de fonctionnalités liées uniquement au cycle de vie du composant, par opposition au service qu'il rend : administration, mise à jour, journalisation forment autant d'exemples d'usages.

R6

Caractériser des usages du composant

Réaliser une liste des usages du composant à partir de ses fonctionnalités et de la liste des ressources auxquelles il accède.

Une fois les usages identifiés, le composant peut mettre en oeuvre un cloisonnement entre usages en s'appuyant sur un moniteur de référence. L'architecture qui en résulte est représentée dans la figure 3.3 .

Exemples. Quelques exemples génériques ont déjà été mentionnés, tels que les usages d'administration, de journalisation, ou de mise à jour.
Des usages liés aux particularités métier du composant seront évidemment dépendants du service rendu. Dans l'exemple de ce chapitre, il y a un usage par utilisateur de l'application. En effet, d'une part, chaque utilisateur de l'application devrait avoir exclusivement accès aux fichiers qui le concernent. D'autre part, les postes que les utilisateurs de l'application utilisent pour se connecter sont a priori distincts et non-homogènes. Avant authentification d'un utilisateur ou d'un administrateur de l'application, aucun des usages ci-dessus n'est identifié. Cependant, il faut rester à l'écoute de nouvelles connexions, il y a donc un usage d'écoute.

Il est difficile de définir de manière générique ce qui constitue un même usage pour un composant, car l'analyse peut être réitérée à des niveaux de granularité différents et à des niveaux d'abstraction différents. Cela suppose également de placer le composant dans son contexte réel d'utilisation pour s'assurer qu'il ne viole pas le cloisonnement global mis en place au sein du système d'information qui l'accueillerait.

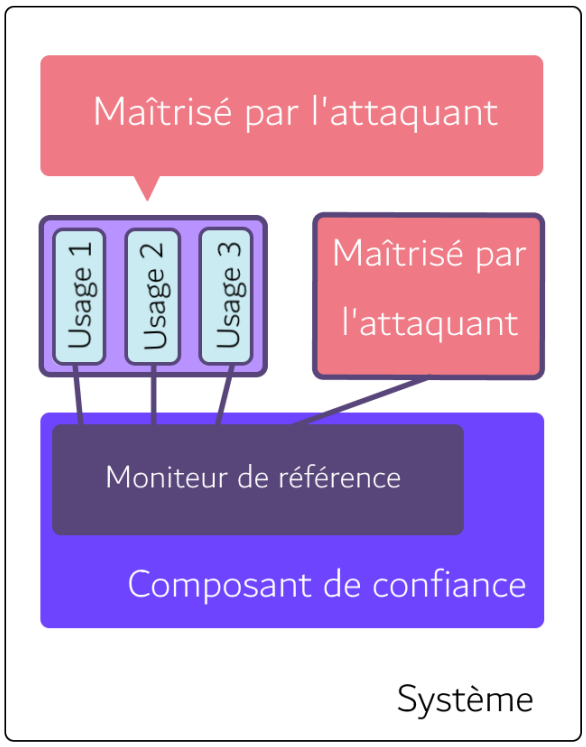


FIG. 3.3 – Nouvelle perception du composant au sein du système qui l'accueille

3.3 Objectifs de la mise en place de cloisonnement

Tous les concepts nécessaires ayant été définis et illustrés précédemment, les objectifs recherchés par la mise en place de cloisonnement peuvent être formulés. Une mise en oeuvre pertinente du cloisonnement doit remplir tous ces objectifs.

R7

Minimiser de la surface d'attaque

Réduire systématiquement la surface d'attaque pour chaque usage, de manière à n'exposer que les interfaces externes utiles pour l'usage considéré.

Exemples. Dans l'exemple, l'API exposée aux clients sera divisée en trois parties : celle dédiée à l'administration de l'application, celle dédiée à l'écoute et celle dédiée aux utilisateurs authentifiés. Chaque domaine exposera une et une seule de ces API, suivant l'usage qui lui correspond.

Objectif

Limiter les possibilités offertes à l'attaquant de prendre le contrôle du composant pendant son utilisation.

R8

Cloisonner les usages entre eux

Mettre en place un moniteur de référence en s'appuyant sur les composants de confiance pour faire en sorte que chaque usage soit confiné dans un domaine.

R9

Minimiser la surface de friction

Réduire systématiquement les actions possibles pour chaque domaine aux seuls besoins liés à l'usage, c'est-à-dire réduire la surface de friction avec le système global.

Exemples. Dans le cas d'étude du chapitre, il est fait en sorte que l'application serveur, quel que soit l'usage considéré, s'exécute sans privilège particulier (car elle n'en a pas besoin) : possibilité d'effectuer uniquement les appels systèmes qui lui sont utiles (gestion des fichiers, sockets, etc.), impossibilité d'utiliser d'autres fichiers que ceux des utilisateurs légitimes et ses propres fichiers (configuration, etc.). Cela peut par exemple être mis en place au moyen de techniques de bacs à sable ou conteneurs.

Objectif

Minimiser les conséquences d'une compromission du composant dans un usage donné :

1. minimiser les conséquences d'une compromission sur les fonctions de sécurité assurées par le composant ;
2. minimiser les conséquences d'une compromission sur le système global.

Exemples. Si un attaquant contrôle une session utilisateur, seuls les fichiers de ce dernier sont à disposition de l'attaquant. Le cloisonnement mis en place garantit que contrôler une session utilisateur ne permet pas de s'arroger les privilèges d'administration de l'application ou d'interférer avec les sessions des autres utilisateurs. La compromission est alors circonscrite au domaine de l'utilisateur compromis.
Concernant le deuxième point, l'absence de privilège particulier requis ou le contrôle d'accès sur les fichiers des utilisateurs empêchent une progression de l'attaquant en cas de compromission du serveur applicatif. En l'absence de cloisonnement, tous les fichiers ou appels systèmes seraient librement accessibles à l'attaquant qui contrôle les domaines du serveur. De même, l'exécution du serveur avec des privilèges inutiles les octroie systématiquement à l'attaquant.

Objectif

Protéger le composant d'une compromission par d'autres composants (non de confiance) appartenant au système global.

Exemples. Les domaines utilisateur du composant étudié sont les seuls environnements applicatifs capables d'accéder aux fichiers métier gérés dans le composant. Par conséquent, la compromission d'une application tierce s'exécutant au sein du même système d'exploitation n'entraîne pas la fuite de ces données métier.

Les usages définis doivent être cohérents pour que le système reste utilisable, mais ils doivent également se prêter de manière efficace à l'application du principe de moindre privilège. Un usage sera considéré trop vaste si la proportion d'actions possibles dans son domaine est grande par rapport à la totalité des actions disponibles en l'absence de cloisonnement.

4
Analyser la sécurité apportée par le cloisonnement mis en place

Ce chapitre énonce les critères d'évaluation du cloisonnement mis en place dans un composant. Tout d'abord, la démarche d'analyse d'un mécanisme de cloisonnement donné est explicitée, avant d'aborder les éléments permettant de se prononcer sur la sécurité de sa mise en oeuvre.

4.1 Analyse d'un mécanisme de cloisonnement

Cette section établit des éléments génériques d'analyse de la sécurité d'un mécanisme de cloisonnement donné. L'évaluation porte sur le cloisonnement en tant que fonction de sécurité, comme défini précédemment en 2.2.

La sécurité d'un composant dépend directement de l'absence de vulnérabilités dans les composants de confiance qu'il utilise. Après avoir détaillé ce qu'il est nécessaire de considérer de manière générique comme composant de confiance, le document aborde les recommandations qu'un tel composant doit respecter. Il convient de noter que certaines recommandations ne sont pas possibles à respecter en intégrant des composants sur étagère ; aussi le document distingue-t-il ce qui doit être appliqué aux composants développés de ce qui doit être appliqué systématiquement.

4.1.1 Le moniteur de référence parmi les composants de confiance

Lorsque l'environnement d'exécution d'un composant est scindé en domaines cloisonnés entre eux, le moniteur de référence est garant du respect de la politique de sécurité dans chaque domaine. C'est parce qu'il y a un moniteur que les domaines existent : c'est le moniteur qui autorise ou empêche chaque action d'une tâche sur une ressource.

R10

Considérer le moniteur comme un composant de confiance

Vis-à-vis d'un attaquant de la fonction de sécurité de cloisonnement, le moniteur de référence fait partie des composants de confiance. Ainsi, il doit respecter les recommandations de cette section.

R11

Identifier les composants de confiance

Tout composant du système qui dispose d'un privilège lui permettant de porter atteinte à l'intégrité du moniteur, ou des politiques de sécurité qu'il met en place, est à considérer comme faisant partie des composants de confiance vis-à-vis du composant analysé.
Tous ces composants doivent donc vérifier les exigences propres aux composants de confiance.

Exemples. Dans le cas du contrôle d'accès obligatoire implémenté dans le noyau d'un système d'exploitation classique, le moniteur de référence est le code gérant le contrôle d'accès obligatoire. En pratique, le code du noyau responsable d'autres choses, comme l'ordonnancement ou la gestion des périphériques, ne fait pas partie du moniteur de référence utilisé pour ce type de cloisonnement. Cependant, tout ce code s'exécute avec des privilèges suffisants pour modifier le moniteur de référence ou la politique qu'il applique. Il faut donc avoir le même niveau de confiance dans tout ce code que dans celui du moniteur à proprement parler.

4.1.2 Composants de confiance développés

Les recommandations fournies pour les composants de confiance développés sont le cahier des charges d'un composant de confiance idéal. Même s'il existe très peu de cas réels dans lesquels toutes ces recommandations sont respectées, il est important de disposer de cette liste de recommandations pour y revenir et se forger un avis sur la sécurité et la robustesse d'un composant de confiance donné.

R12

Concevoir des composants simples et concis

Les composants de confiance doivent être conçus en suivant des spécifications claires et complètes, permettant de définir et combiner des éléments simples (suivant le principe « Keep It Short and Simple ») qui facilitent développement et validation.

L'utilisation de langages fortement typés (tels Ada, OCaml, Rust, Go, etc.) permet de réduire notablement le nombre de vulnérabilités exploitables dans un composant.

R13

Choisir un langage approprié

Utiliser un langage de programmation fortement typé, qui entre autres prévient les débordements de tableau, d'entier, ou l'utilisation de pointeurs invalides, est fortement souhaitable pour le développement des composants de confiance.

R14

Développer selon un référentiel de sécurité

Un référentiel de développement sécurisé doit être utilisé systématiquement lors du développement de composants de confiance.

La vérification du respect du référentiel de codage doit être assurée.

Le respect de cette recommandation est critique dans le cas du choix d'un langage ne respectant pas les critères conseillés ci-dessus.

Des exemples de tels référentiels incluent les standards SEI CERT Coding Standard ([2]) et le guide mis à disposition par MISRA ([1]).

R15

Auditer le code de l'implémentation des composants de confiance

L'intégralité du code des composants de confiance devra faire l'objet d'un audit de code par des personnels qui n'en sont pas développeurs, de préférence indépendants du projet concerné.

R16

Valider l'implémentation des composants de confiance

Des tests fonctionnels complets devront permettre de valider le bon fonctionnement des fonctions de sécurité implémentées. Une attention particulière sera portée à tester aussi bien les opérations qui doivent être refusées que celles qui doivent être menées à bien avec succès.

R17

Prouver l'implémentation des composants de confiance

Il est fortement recommandé de compléter les tests par une preuve formelle de l'absence d'erreur à l'exécution d'un composant de confiance, par exemple à l'aide d'outils d'analyse (statique ou dynamique) pour prévenir certains types de vulnérabilités.

4.1.3 Recommandations portant sur tous les composants de confiance

Les recommandations précédentes sont très exigeantes, et sont très rarement applicables aux composants sur étagère intégrés. Qu'un composant de confiance respecte ou non le cahier des charges établi par ces recommandations, il doit respecter les recommandations suivantes.

R18

Supprimer toute partie inutilisée d'un composant de confiance

Un composant de confiance doit être minimal. Dès que possible, la suppression du code inutilisé sera privilégiée. A défaut, sa désactivation par configuration sera effectuée.

R19

Appliquer des techniques de durcissement aux composants de confiance

Les composants de confiance doivent se voir appliquer des techniques de durcissement à l'état de l'art afin de compliquer l'exploitation d'une vulnérabilité et le détournement du flot de contrôle, comme par exemple :

- présence de motifs d'intégrité de la pile et du tas (canaris) ;
- principe W $\oplus$ X : au cours de toute son utilisation par le système, une zone mémoire donnée ne doit pas être inscriptible et exécutable, que ce soit simultanément ou non ;
- répartition aléatoire de l'espace d'adressage (ou Address Space Layout Randomization (ASLR)).

Exemples. Dans le cas d'un système Linux, le respect de ces deux recommandations peut impliquer une recompilation d'un noyau minimal avec les options satisfaisantes. Consulter le document rédigé sur la sécurité de ces systèmes [4] est recommandé.

4.1.4 Recommandations spécifiques à un moniteur de référence

Dans son ouvrage sur la sécurité des systèmes d'exploitation [9], Trent Jaeger définit et présente en détails chacune des propriétés exigées ci-dessous. Comme plus haut, il s'agit d'un idéal vers lequel tendre, en particulier lors de l'intégration de solutions sur étagère. Tout ce qui est détaillé ici peut fournir des critères de choix entre solutions ou dans leurs configurations. Tout moniteur de référence développé devrait suivre ces recommandations.

R20

Justifier le respect des propriétés fondamentales du moniteur de référence

Le développement, l'intégration et la validation du moniteur de référence doivent permettre de garantir qu'il vérifie les propriétés suivantes.

1. *Complétude du contrôle exercé* : le moniteur est impliqué pour chaque tentative d'accès à une ressource, et ce au moment opportun (i.e. absence d'attaques TOCTTOU (Time Of Check To Time Of Use), liées à une évolution des propriétés de l'objet entre le moment de la requête au moniteur et l'action effective).
2. *Maintien de l'intégrité du moniteur*.
3. *Validation et audit de la politique de sécurité*. La possibilité de consulter la politique de sécurité implémentée par le moniteur à un instant donné permettra l'audit de celle-ci.

Des justifications construites confirmant le respect de ces propriétés doivent figurer dans les documents de conception du composant utilisant le moniteur de référence.

Comme vu en section 2.2, l'attaquant de la fonction de sécurité de cloisonnement mise en place par le moniteur est supposé contrôler une ou plusieurs tâches. Le but est de s'assurer, en présence de cet attaquant, que les tâches cloisonnées soient dans l'incapacité de s'arroger des permissions supplémentaires en modifiant l'environnement d'exécution du moniteur. Pour protéger le moniteur, il faut donc garantir qu'un attaquant contrôlant une tâche **ne dispose pas** des privilèges nécessaires à une modification en sa faveur.

R21

Assurer au moniteur de référence un niveau de privilège supérieur à celui des tâches cloisonnées

De manière à préserver l'intégrité du moniteur et des politiques de sécurité qu'il met en application, les tâches cloisonnées ne doivent pas disposer des privilèges nécessaires à la relaxe de la politique de sécurité appliquée.

Une façon de garantir ceci est d'assurer que les politiques sont non-modifiables par les tâches cloisonnées et que le moniteur s'exécute à un niveau de privilège supérieur à celui des tâches qu'il cloisonne.

Exemples. Effectuer une comparaison de deux choix architecturaux sur l'exemple du serveur applicatif présenté dans le chapitre précédent permet d'illustrer cette recommandation. Dans les

deux cas, une session utilisateur correspond à un processus. Ce n'est pas sur cet aspect que porte la comparaison, mais sur la mise en place du contrôle d'accès sur les fichiers utilisateur.
Le premier choix consiste à écrire un module de code dédié à la prise de décision, qui s'exécutera au sein du processus gérant un utilisateur du serveur. A chaque fois qu'un utilisateur veut accéder à un fichier, un appel est effectué aux fonctions du module, qui retourne un refus ou un descripteur de fichier vers le fichier demandé.
Le second choix consiste à exécuter chaque session utilisateur dans un processus distinct sous une identité (uid) qui lui est propre, et à s'appuyer sur le noyau pour implémenter le contrôle d'accès sur les fichiers.
Contrairement à la seconde solution, la première alternative **ne cloisonne pas** les sessions utilisateur entre elles. En effet, l'attaquant est supposé contrôler un ou plusieurs domaines cloisonnés. Ici, rien n'isole le module dédié au contrôle d'accès du reste du code des sessions utilisateur. Il est donc impossible de garantir que les ouvertures de fichiers passent par le module, et il est impossible de garantir son intégrité. Un attaquant en capacité d'exécuter du code arbitraire au sein de l'environnement d'une session utilisateur a le contrôle du processus, et donc peut modifier le code exécuté à sa guise.

En terme de sécurité, un moniteur de référence bénéficiera à l'usage de configurations par défaut le moins permissives possible. Même dans le cas de l'utilisation d'un moniteur de référence sur étagère, ces recommandations peuvent être appliquées.

R22

Appliquer le principe d'interdiction par défaut

Un moniteur de référence doit être configurable pour que toute action soit interdite à une tâche, sauf à lui être explicitement autorisée.

L'application de ce précepte prétend éviter l'oubli d'interdiction d'actions que le développeur ou l'utilisateur du composant n'aurait pas envisagées, en obligeant à dresser la liste des actions qu'un composant doit pouvoir effectuer.

Pouvoir appliquer une telle configuration au moniteur de référence est salutaire, surtout lorsque la politique de sécurité est difficilement auditable. Pourtant, les mécanismes de cloisonnement ne respectent pas tous ce principe. Par exemple, dans le cadre du cloisonnement entre processus présenté précédemment, il est quasiment impossible sans s'appuyer sur d'autres mécanismes de cloisonnement supplémentaires de s'assurer que deux processus ne communiquent pas entre eux.

R23

Minimiser le nombre et l'impact des configurations possibles

Dans une démarche de durcissement du moniteur, les options de configuration laissées au choix de l'utilisateur (même privilégié) en production doivent être restreintes au strict minimum, de manière à réduire l'impact possible d'une erreur sur la sécurité globale du système. Pour les choix laissés à l'utilisateur, les messages d'avertissement sur les conséquences en terme de sécurité doivent être suffisamment explicites.

Exemples. Ne pas permettre de désactiver les alertes, la journalisation, ou d'activer les fonctions de débogage dans une version de production est pertinent. Demander une confirmation lors d'un changement de configuration, documenter les options de configuration de manière extensive pour qu'elles puissent être maîtrisées par les administrateurs du produit sont également de bonnes pratiques.

4.1.5 Évaluer un mécanisme de cloisonnement

Évaluer un mécanisme de cloisonnement, c'est mesurer l'effort nécessaire à un attaquant pour le mettre en défaut. Pour quantifier la difficulté de contourner un mécanisme, il est recommandé d'appliquer la démarche suivante.

1. Identifier ce à quoi correspondent les définitions de tâches, ressources propres et partagées et moniteur de référence dans le contexte du mécanisme de cloisonnement étudié.
2. Déduire du contexte d'emploi (générique ou souhaité) l'ensemble des composants de confiance.
3. Mesurer l'écart entre les caractéristiques réelles de l'implémentation du moniteur de référence et les recommandations fournies.
4. Mesurer l'écart entre les caractéristiques réelles des composants de confiance et les recommandations à respecter listées dans ce document. Des critères de mesure de cet écart peuvent aussi comprendre la mesure de la maturité du produit, le niveau d'assurance quant à son maintien en conditions opérationnelle et de sécurité, ou encore son historique en termes de parution de vulnérabilités, etc.
5. Evaluer la possibilité de réduire les écarts identifiés en appliquant des techniques de durcissement, comme la minimisation de l'ensemble des composants de confiance par désinstallation de programmes inutiles, l'usage de versions durcies des composants de confiance... Le combinaison de plusieurs mécanismes traitant divers types de ressources peut également être envisagée [3].

4.2 Analyse de la mise en place du cloisonnement

Tous les outils permettant de mener une analyse de la sécurité apportée par l'implémentation de cloisonnement sont maintenant à disposition du lecteur.

3. à la manière des conteneurs Linux combinant espaces de noms et cgroups pour aboutir à une solution.

4.2.1 À niveau d'abstraction donné

Une telle analyse débutera par une spécification claire de ce qui est mis en oeuvre, avant de procéder à la vérification du respect de tous les points recommandés précédemment.

R24

Spécifier le cloisonnement proposé

Pour présenter le cloisonnement mis en place, il est recommandé de procéder de la manière suivante.

1. Expliciter les usages identifiés.
2. Décrire le mécanisme de cloisonnement mis en oeuvre en explicitant ce à quoi correspondent les définitions de tâches, ressources propres et partagées et moniteur de référence.
3. Expliciter la politique de sécurité mise en place pour chaque usage. Pour chaque domaine, il faut reprendre la liste des interfaces externes dressées précédemment et caractériser les actions autorisées.

Pour structurer l'évaluation de la sécurité apportée par le cloisonnement mis en place au sein d'un composant, la liste de critères suivante peut être suivie :

1. adéquation entre les scénarios vraisemblables d'utilisation du composant et les usages définis ;
2. pertinence du choix du mécanisme de cloisonnement. Vérifier la compatibilité de l'ensemble des composants de confiance issus de la définition du mécanisme de cloisonnement avec la définition des composants de confiance telle que donnée par l'analyse de sécurité. Vérifier que la difficulté de la mise en défaut du mécanisme utilisé correspond au moins au niveau estimé de l'attaquant duquel le système doit être protégé ;
3. vérification que la politique de sécurité des domaines implémente bien le principe de moindre privilège (minimisation de la surface d'attaque et de la surface de friction) ;
4. vérification de la complétude du cloisonnement : garantie de la couverture de toutes les interfaces externes du composant ;
5. évaluation de l'innocuité du composant pour le système qui l'exécute, par l'évaluation des conséquences de sa compromission.

R25

Assurer l'innocuité du composant pour le système qui l'accueille

Un composant ne doit pas dégrader la sécurité globale du système, notamment en limitant la mise en place du cloisonnement par d'autres composants utilisés sur le même système.

En particulier, un composant ne doit pas exiger pour fonctionner d'abaisser le niveau de sécurité du système qui l'héberge : le composant doit être compatible avec un niveau de durcissement à l'état de l'art au moment de sa mise en production.

4.2.2 Raffinement du cloisonnement à l'intérieur du composant

Dans une démarche de durcissement et défense en profondeur, il est pertinent de mettre en place du cloisonnement interne dans les différents domaines. Ceci est d'autant plus important que les

domaines sont de taille importante, par exemple s'il s'agit de machines virtuelles ou de conteneurs. Il suffit de se placer dans un domaine donné et d'itérer l'analyse de sécurité présentée ci-dessus à l'intérieur du domaine.

Par exemple, à l'intérieur d'une machine virtuelle ayant pour fonction d'héberger un serveur Web, il convient d'isoler dans un conteneur ce qui relève des fichiers et programmes nécessaires au serveur Web.

Le cloisonnement dépend du niveau d'abstraction envisagé, et sa mise en place peut être faite par divers moyens. Des solutions de cloisonnement emboîtées comme des poupées russes forment autant de barrières entre la compromission par un attaquant du maillon le plus faiblement sécurisé présent sur un système et le contrôle complet du système par cet attaquant.

5
Éléments d'analyse d'une architecture de sondes de détection réseau

Cette section a pour vocation d'illustrer, à partir d'un exemple concret, la démarche que ce document vise à transmettre. L'étude porte sur la conception hypothétique d'une sonde réseau de détection d'incidents de sécurité, nommée exIDS dans la suite.

La suite de cette section s'appuie fortement sur deux documents que le lecteur est invité à consulter. D'une part, l'article « Architecture système sécurisée de sonde IDS réseau » ([10]) fournit une description assez détaillée de choix architecturaux. D'autre part, la cible de sécurité générique pour ce type de produits ([3]) présente l'analyse de sécurité nécessaire à la bonne conception d'exIDS. L'article étant paru avant et indépendamment du travail de rédaction de cette cible de sécurité, il existe quelques détails à adapter pour que les deux documents soient parfaitement conciliables. L'exemple exIDS est le simple fruit de cette adaptation. Une première architecture est envisagée, puis modifiée pour satisfaire des contraintes de performance.

L'étude proposée ici n'a pas pour objet de recommander une architecture plutôt qu'une autre. Il s'agit plutôt d'un prétexte à un exercice d'architecture comparée. D'autres solutions satisfaisant la cible de sécurité pourraient être envisagées, par exemple plus raffinées dans le cloisonnement proposé, ou s'appuyant sur de la virtualisation plutôt que des conteneurs Linux.

5.1 Première proposition d'architecture pour exIDS

La cible générique prévoit quatre utilisateurs de la sonde : auditeur et administrateur local d'une part, opérateur et administrateur système d'autre part [4]. Chacun de ces utilisateurs correspond à un usage dans l'architecture proposée. La capture des flux réseau bruts entrants nécessite des privilèges inutiles aux autres usages ; elle est identifiée dans un premier temps comme un usage particulier. Par ailleurs, comme dans l'article cité, chaque logiciel IDS utilisé constitue un usage distinct. Enfin, la collecte des alertes relevées par les logiciels IDS et leur transmission à l'opérateur est également un usage. Les logiciels IDS effectuent des traitements complexes sur les données issues des captures, et sont donc potentiellement porteurs de vulnérabilités. Ainsi, il convient de les séparer du reste du composant, et de les séparer entre eux : ceci permet de circonscrire la compromission éventuelle d'un de ces logiciels au domaine de celui-ci. De surcroît, cela permet de n'exposer aucune interface réseau à ces domaines, puisque les logiciels IDS n'en ont pas besoin. En rendant inaccessible le réseau dans ces domaines, le risque de rebond depuis la sonde dans les réseaux qui lui sont reliés suite à une compromission des logiciels IDS est couvert. Enfin, comme

4. L'administration est ici divisée en usages distincts. L'administrateur système agit a priori à distance et ne peut que mettre à jour et redémarrer la sonde. L'administrateur local peut effectuer toutes les autres actions, tenant ainsi plus un rôle d'administrateur métier. Ce document suit la terminologie du document cible générique [3].

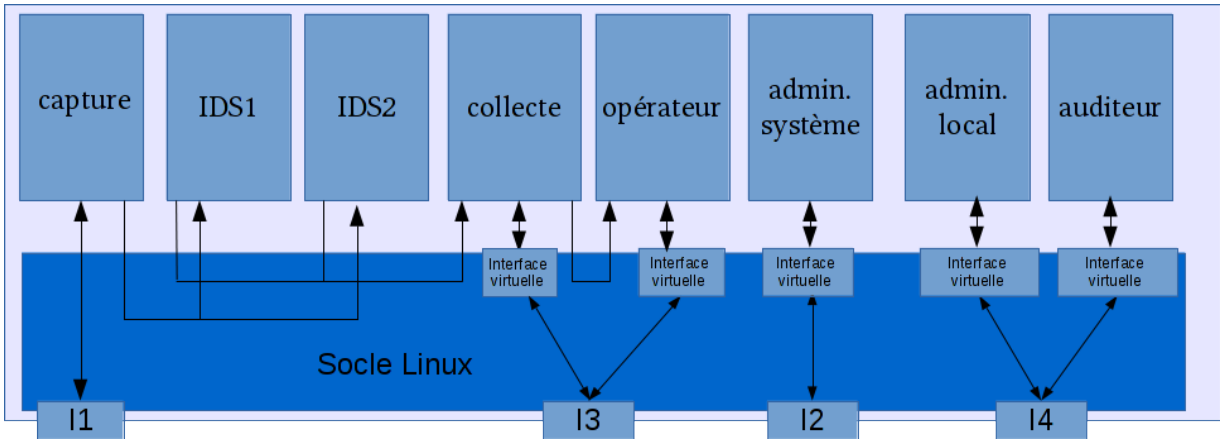


FIG. 5.1 – Première architecture envisagée pour la sonde exIDS

souligné dans l'article, la capacité à mettre à jour le composant est fondamentale ; elle n'est pas détaillée ici car aucun élément nouveau n'est intégré à exIDS.

À l'instar de ce qui est choisi dans l'article, exIDS présente un socle constitué d'un noyau Linux recompilé avec des options de durcissement adéquates, les patches PaX et grsecurity et la suppression de tous les modules, fonctionalités et options du noyau inutilisés. Les protections système décrites dans l'article sont appliquées. Chaque usage listé est associé à un conteneur ; les conteneurs vérifient les prescriptions de l'article également. Les flux autorisés entre usages sont limités à ceux spécifiés dans les documents référencés. L'architecture envisagée est présentée dans la figure 5.1.

Le cloisonnement entre usages repose donc dans exIDS sur des conteneurs. Le socle constitue le moniteur de référence. Les tâches sont les programmes s'exécutant dans les conteneurs, les ressources partagées comprennent les partages de fichiers documentés dans l'article, ainsi que le socle et le matériel en commun. Certains répertoires sont partagés entre domaines, mais il n'existe pas de partage de fichiers dans lequel deux domaines distincts peuvent écrire. Ceci permet de créer des communications unidirectionnelles entre domaines. Les interfaces réseau virtuelles éventuellement disponibles dans les conteneurs sont des ressources propres. Les conteneurs n'ont pas accès à des interfaces réseau physiques, à l'exception de l'usage de capture qui nécessite les privilèges adéquats à la récupération bas-niveau de paquets réseau. Un pare-feu local est mis en place au sein du socle de manière à restreindre aux stricts flux spécifiés les flux réseau possibles entre interfaces.

Disposer d'interfaces réseau distinctes comme exigé par la cible de sécurité permet de prolonger le cloisonnement au niveau matériel : seule l'interface utilisée par l'usage, lorsqu'elle existe, est accessible dans le conteneur adéquat. En adoptant le point de vue du cloisonnement réseau, la présence de plusieurs interfaces physiques et le cloisonnement entre les domaines qui les utilisent permet de ne pas créer de jonctions facilement exploitables entre réseaux physiques disjoints. Comme mentionné précédemment, le fait qu'aucune interface ne soit disponible dans les conteneurs liés aux usages IDS joue également en faveur de l'innocuité du composant pour le système. Pour finir le tour des définitions, les composants de confiance sont constitués du matériel, dans son intégralité cette fois, ainsi que du socle.

Concernant les interfaces externes, seules les interfaces entre domaines destinées à servir les flux

documentés dans l'article ou la cible seront à disposition dans chaque conteneur. En particulier, les fichiers exposés dans les conteneurs sont en lecture seule, sauf dans le cas particulier d'un besoin d'écriture dans un répertoire bien défini. Ceci sera utilement complété par l'interdiction des appels système inutilisés par les processus légitimes, la réduction des capacités disponibles aux programmes dans les conteneurs au strict nécessaire, ainsi que la limitation de l'utilisation de ressources système.

Dans une analyse d'un produit réellement développé, les détails d'implémentation devraient être explicités. Cependant, il convient d'insister sur le fait que l'analyse architecturale haut niveau présentée ici est réalisable avant tout développement de preuve de concept qui permettrait de valider la faisabilité et l'impact sur les performances des choix effectués. A contrario, introduire après une première phase de développement le cloisonnement impliquerait vraisemblablement des changements drastiques sur le produit final difficiles à maîtriser et coûteux.

5.2 Architecture retenue pour exIDS

Après avoir prototypé le projet exIDS, les développeurs concluent que l'architecture proposée initialement s'avère trop ambitieuse au niveau du cloisonnement pour que le produit puisse offrir des performances satisfaisantes. Ceci est dû à la manière dont fonctionnent la plupart des logiciels IDS. D'une part, pour fonctionner, un tel logiciel a besoin des données acquises par la carte. Recopier ces données pour les mettre à disposition prendrait un temps considérable non-compatible avec le niveau de performances attendu de plusieurs gigabits par seconde. D'autre part, le logiciel, au moins au début de son exécution, a en général besoin d'accès à des registres de configuration de la carte qu'il utilise. Régler ces deux problèmes en préservant l'architecture précédente et en satisfaisant les attentes en termes de performances, sans modifier de manière assez invasive les logiciels IDS utilisés est jugé irréaliste par les concepteurs d'exIDS.

Une solution envisagée pour régler les difficultés consiste à supprimer l'usage de capture (et donc le conteneur correspondant) et à mettre à disposition des logiciels IDS la carte réseau I1. Le reste de l'architecture peut être conservé ; la figure 5.2 présente le nouveau projet. Pour valider un tel changement architectural, il est impératif de vérifier que les deux risques que couvraient l'usage de capture sont traités par d'autres mesures. Premièrement, l'effort nécessaire à un attaquant exploitant une vulnérabilité dans un logiciel IDS pour prendre le contrôle de la sonde devrait être similaire. Deuxièmement, il doit rester impossible en toutes circonstances d'utiliser la sonde pour pénétrer le réseau qu'elle est supposée surveiller.

Concernant le premier risque, en s'appuyant sur les espaces de noms réseau et les conteneurs dédiés à chaque logiciel IDS, il est raisonnable de considérer que l'accès à l'interface I1 n'augmente pas significativement le risque de prise de contrôle d'autres conteneurs ou du socle de la sonde. Cependant, la surface de friction des conteneurs IDS est clairement plus importante que dans l'architecture initiale. Aussi, faire en sorte que les logiciels IDS n'aient que les capacités réellement utiles et perdent droits et accès dès qu'ils n'en ont plus besoin [5] s'avère une précaution supplémentaire profitable.

Quant au second risque, il est impossible de garantir au sein du produit l'absence de flux de communication initiés par la sonde vers le réseau surveillé. Dans ce contexte, utiliser un autre produit

5. Typiquement, après avoir effectué les opérations de configuration du matériel requises à leur lancement.

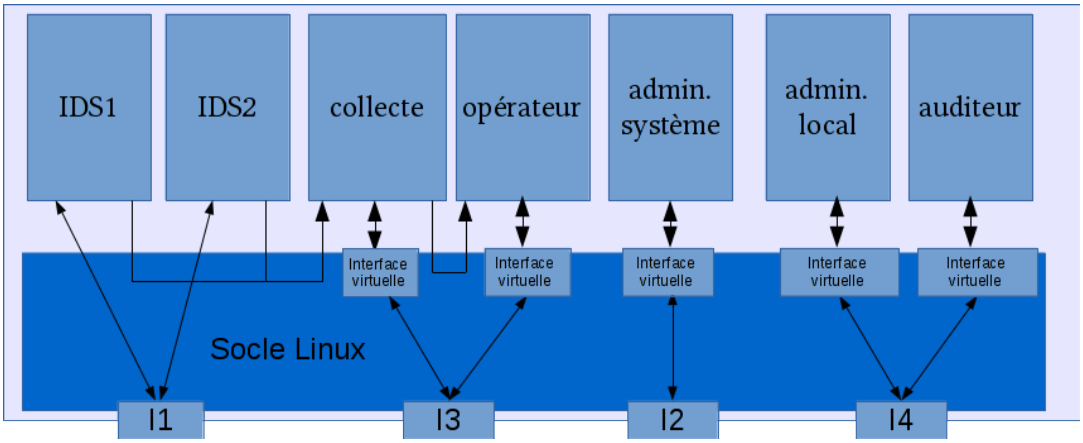


FIG. 5.2 – Architecture retenue pour la sonde exIDS

à même de garantir des communications unidirectionnelles pour relier l'interface I1 au réseau surveillé offre une solution. Cette mesure organisationnelle est d'ailleurs déjà connue du lecteur attentif de la cible de sécurité citée précédemment, où apparaît l'hypothèse sur l'environnement H2 de l'existence d'un TAP unidirectionnel qualifié.

En conclusion, les risques ouverts par la modification architecturale sont considérés couverts. La nouvelle architecture est retenue comme présentant une solution satisfaisante en terme de cloisonnement vis-à-vis du besoin spécifié.

Bibliographie

[1] *MISRA Publications*.
https://www.misra.org.uk/Publications/tabid/57/Default.aspx.

[2] *SEI CERT Standard*.
https://www.securecoding.cert.org/confluence/x/BgE.

[3] *Sonde réseau de détection des incidents de sécurité*.
Cible de sécurité, ANSSI, mai 2017.
https://www.ssi.gouv.fr/uploads/2015/03/20170512-profil-de-protection-cspn-np_v1.41.pdf.

[4] *Recommandations de sécurité relatives à un système GNU/Linux*.
Note technique DAT-NT-002/ANSSI/SDE/NP v1.1, ANSSI, juillet 2012.
https://www.ssi.gouv.fr/reco-securite-systeme-linux.

[5] *Expression des besoins et identification des objectifs de sécurité*.
Guide Version 1.1, ANSSI, janvier 2010.
https://www.ssi.gouv.fr/ebios/.

[6] *Instruction - Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau*.
Référentiel ANSSI-CSPN-CER-I-02 v1.1, ANSSI, avril 2014.
https://www.ssi.gouv.fr/uploads/2015/01/ANSSI-CSPN-CER-I-02_Criteres_pour_evaluation_en_vue_d_une_CSPN_v1-1.pdf.

[7] *Understanding and Hardening Linux Containers*.
Aaron Grattafiori.
Rapport technique, NCC Group, 2016.
https://www.nccgroup.trust/globalassets/our-research/us/whitepapers/2016/april/ncc_group_understanding_hardening_linux_containers-1-1.pdf.

[8] *Abusing Privileged and Unprivileged Linux Containers*.
Jesse Hertz.
Rapport technique, NCC Group, 2016.
https://www.nccgroup.trust/globalassets/our-research/us/whitepapers/2016/june/abusing-privileged-and-unprivileged-linux-containers.pdf.

[9] *Operating System Security*.
Trent Jaeger.
Ouvrage scientifique, 2008.

[10] *Architecture système sécurisée de sonde IDS réseau*.
Arnaud Fontaine Pierre Chifflier.
Publication scientifique, ANSSI, novembre 2014.
https://www.ssi.gouv.fr/publication/architecture-systeme-securisee-de-sonde-ids-reseau.

ANSSI-PG-040
Version 1.0 - 14/12/2017
Licence ouverte/Open Licence (Étalab - v1)

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP
www.ssi.gouv.fr / conseil.technique@ssi.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
SGDSN

Annexe 6 : Explication prélèvement à la source

Qu'est-ce que le prélèvement à la source de l'impôt sur le revenu ?

Le prélèvement à la source consiste à faire payer l'impôt en même temps que vous percevez ces revenus. Le prélèvement à la source permet donc de rendre le paiement de l'impôt contemporain de la perception des revenus et d'éviter ainsi un décalage d'un an. C'est ce qui le différencie de la simple mensualisation de l'impôt.

Si vous êtes salarié ou retraité, l'impôt sera alors collecté par votre employeur ou votre caisse de retraite.

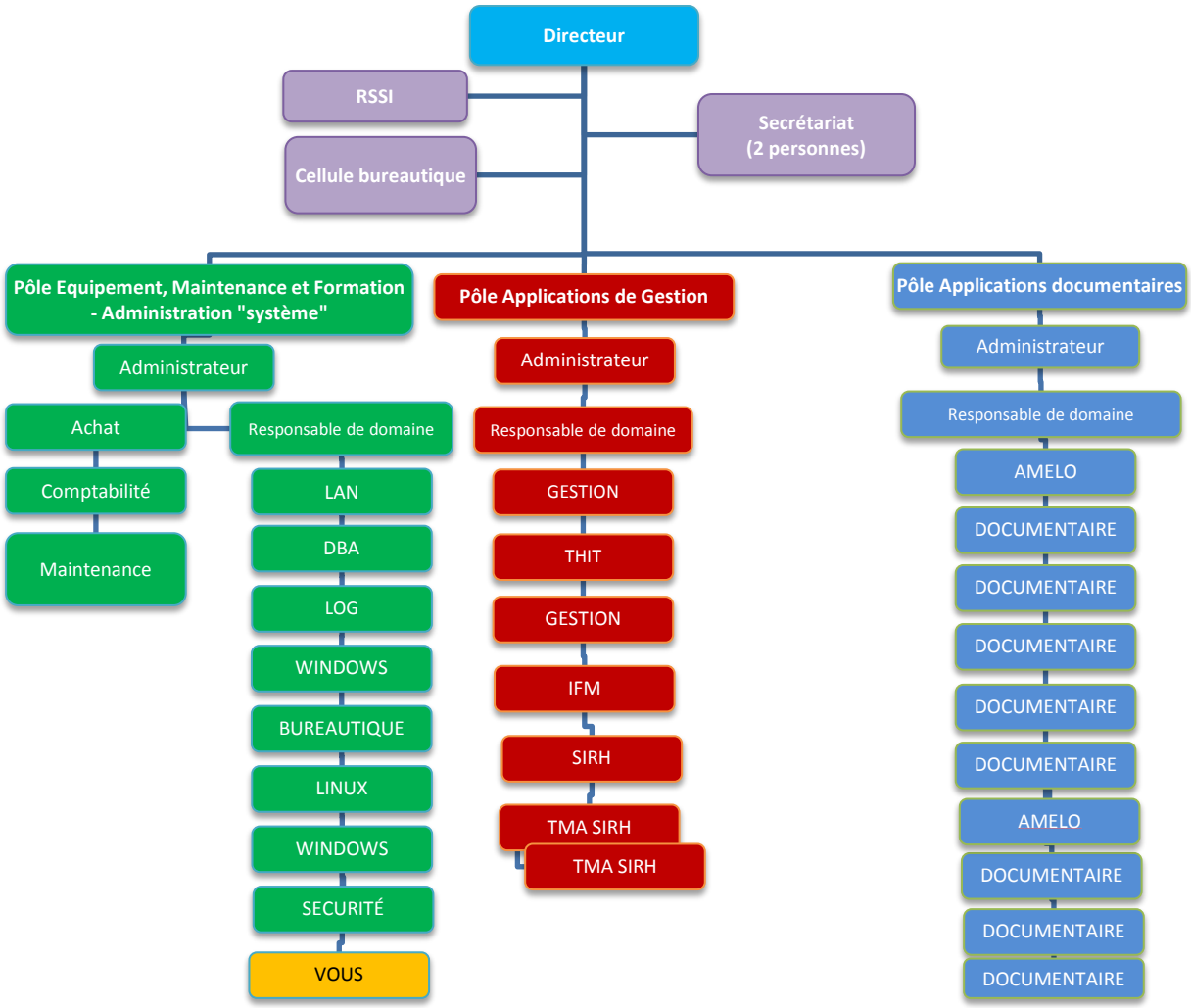
Si vous êtes travailleur indépendant, agriculteur ou bénéficiez de revenus fonciers, vous paierez l'impôt sur le revenu correspondant par des acomptes prélevés directement par l'administration fiscale.

Le prélèvement à la source commencera à partir du 1er janvier 2019.

En pratique, comment cela fonctionne pour les entreprises ?

Pour les entreprises privées, la mise en œuvre est simplifiée grâce au déploiement de la déclaration sociale nominative (DSN), qui sera généralisée à l'été 2018. Pour mettre en œuvre le prélèvement à la source, quelques données seront ajoutées à la DSN mensuelle. L'assiette du calcul du prélèvement à la source sera le salaire net imposable, qui est déjà calculé par les logiciels de paie et qui figure déjà sur les bulletins mensuels de paye.

Annexe 7 : Organigramme



Annexe 8 : Environnement informatique (extrait)

1 Serveurs

252 serveurs sont installés au Sénat (58 serveurs physiques et 194 serveurs virtuels).

Ces serveurs sont principalement sous *Linux* (très majoritairement RHEL 6 et 7, mais il existe d'autres versions), sous *Windows* (2003/2008/2012/2016), quelques serveurs *Novell OES* (2015sp1 et 2018) et *Solaris* (10).

Voici le détail de l'ensemble du parc serveurs :

Serveurs physiques

RedHat Entreprise Linux (5 + 6 + 7)	43
Suse Linux (OES11 + OES 2015)	4
Solaris (10)	3
ESXi	8
Total	58

Serveurs virtuels

Windows (XP + 7 + 10)	21
Windows Server (2003 + 2008R2 + 2012 + 2016)	45
RedHat Entreprise Linux (5 + 6 + 7)	92
Suse Linux Entreprise 11	16
Divers *Linux* (*CentOS* + *Debian* + *Oracle*, etc.)	20
Total	194

Les machines virtuelles sont hébergées dans deux clusters *VMware* constitués au total de 8 hôtes (deux nouveaux hôtes étant en cours d'installation).

L'infrastructure de virtualisation est en version 6.0.0 *build* 5572656, et un passage en 6.7 est envisagé à court terme.

2 Réseau et salles informatiques

Les serveurs du Sénat sont répartis dans trois salles informatiques, dont deux principales, situées dans des bâtiments différents pour des raisons de sécurité.

Les salles sont interconnectées par un réseau local Ethernet, constitués de commutateurs équipés de ports 1 Gbit/s. Il n'existe pas de réseau de sauvegarde dédié ; les données transitent par le réseau local, y compris à travers les pare-feu pour les équipements qui ne sont pas sur le même réseau que les serveurs de sauvegarde.

La liaison entre les salles est de 2 x 1 Gbit/s. Une refonte complète du réseau et des salles informatiques est en cours ; elle permettra, au cours de l'année 2018, de connecter les équipements compatibles sur des interfaces 10 Gbit/s avec des cœurs de réseau agrégeant plusieurs interfaces 40 Gbit/s.

3 Postes de travail et équipements bureautique

3.1 Parc des directions du Sénat

- 1084 postes de travail environ ;
- 1046 écrans plats ;
- 576 imprimantes ;
- 86 télécopieurs ;
- 125 copieurs ;
- 35 scanners ;
- autres dispositifs attachés (webcams, lecteurs de cartes SD, imprimantes à badges, pédaliers, etc.)

Le parc informatique des directions du Sénat équipé du système d'exploitation Windows 7 et de la suite bureautique Office 2010. Tous les postes sont connectés au réseau interne du Sénat.

Les principaux logiciels actuellement déployés sur les postes informatiques des directions du Sénat (liste non exhaustive) :

- logiciel de gestion du système d'exploitation : Microsoft Windows 7, Windows XP de manière résiduelle (moins de 10 postes) ;
- logiciels de bureautique : Microsoft Office 2010 et suivants (avec Word, Excel, PowerPoint, Access, Publisher, Outlook), Libre office, Acrobat Pro, PDF Creator ;
- logiciels de navigation Internet : Internet Explorer, Mozilla Firefox ;
- logiciels de messagerie : Thunderbird de Mozilla, Microsoft Outlook ;
- logiciels spécialisés : Autodesk Autocad (LT, True View…), suite Adobe Photoshop (CS, Elements…), Bosch Meeting Recorder, Vision Media Solution WinMagneto, Cegedim Esquif, etc. ;
- logiciels utilitaires divers : 7-Zip, Adobe Acrobat Reader, Adobe Flash Player, Client Java, etc. ;
- logiciels d'administration : Micro Focus ZENworks Configuration Management (ZCM), Micro Focus Client for Open Enterprise Server, Micro Focus Client iPrint, F-Secure Client Security, Microsoft Deployment Toolkit (MDT), etc. ;

- logiciel d'enregistrement et de suivi des demandes d'assistance des utilisateurs, ainsi que de gestion des parcs informatique et téléphonique : iTop. Il est couplé à l'outil ZCM pour la remontée des informations et l'inventaire des matériels déployés ;
- agenda partagé : Zimbra Collaboration Server.

3.2 Le parc informatique des Sénateurs

Le parc informatique des Sénateurs sur le site du Sénat est estimé entre 800 et 900 postes de travail.

Les Sénateurs disposent, pour l'acquisition des équipements informatiques utiles à l'exercice de leur mandat, d'un système d'avances spécifiques auquel ils recourent librement. Aussi le parc des Sénateurs est-il assez hétérogène, qu'il s'agisse des postes de travail, des périphériques, tablettes et des logiciels.

Les postes des Sénateurs sont connectés au réseau Ethernet du Sénat, de manière indépendante les uns des autres. Ils ne sont pas connectés au LAN des directions du Sénat, mais ils accèdent aux applications du Sénat, à Internet, ainsi qu'aux serveurs de messagerie.

3. ETUDE DE CAS - PROFIL "DEVELOPPEMENT"

(durée 4 heures - coefficient 5)

Prenez soin de justifier vos réponses et d'expliciter vos hypothèses. Il sera tenu compte dans la notation du soin apporté à la propreté de votre copie et à la clarté de vos réponses.

Si vous utilisez des formalismes connus dans vos schémas, nommez-les. Sinon, prenez soin de légender.

N'utilisez pas de couleur dans votre rédaction ni vos schémas.

INTRODUCTION ET OBJECTIF

La direction des Systèmes d'Information du Sénat souhaite refondre sa gestion des identités et des accès.

Aujourd'hui, les comptes utilisateurs, profils et droits d'accès aux ressources et applications du Sénat sont éclatés dans différentes applications.

Les demandes d'accès aux applications sont effectuées à l'aide de l'outil interne de suivi de tickets.

L'objectif de ce projet est de développer une application qui permette de centraliser et de gérer les identités et les droits d'accès aux applications du Sénat.

Vous êtes l'informaticien en charge de ce projet.

DESCRIPTION DE L'EXISTANT

ORGANISATION LÉGISLATIVE

LE BUREAU DU SÉNAT

Le Bureau du Sénat est constitué du Président du Sénat et de 25 sénateurs. Le Bureau a de larges compétences pour présider aux délibérations du Sénat et pour en organiser et diriger tous les services.

LES QUESTEURS

Membres du Bureau du Sénat, les Questeurs gèrent tous les aspects matériels et administratifs de la vie du Sénat. Sous le contrôle du Bureau du Sénat, ils disposent, à cet effet, d'un pouvoir financier, réglementaire et de nomination qu'ils exercent, le cas échéant conjointement avec le Président du Sénat, à travers des arrêtés et des décisions.

LES GROUPES POLITIQUES

Les groupes politiques sont librement constitués par les sénateurs qu'unissent les mêmes affinités d'idées et, le plus souvent, l'appartenance à un même parti dont ils forment, en quelque sorte, la fraction parlementaire. Les groupes, qui doivent chacun réunir au moins 10 sénateurs, se constituent ou se reconstituent après chaque renouvellement triennal.

Les sénateurs n'étant pas assez nombreux pour former un groupe parlementaire sont aujourd'hui regroupés dans la Réunion administrative des sénateurs ne figurant sur la liste d'aucun groupe (RASNAG).

LES COMMISSIONS

Le Sénat comporte sept commissions permanentes composées d'un nombre limité de sénateurs. Tous les sénateurs, à l'exception du Président du Sénat, font partie d'une commission permanente.

Les commissions permanentes jouent un rôle essentiel dans la préparation du travail législatif, dans le contrôle du Gouvernement et dans l'information des sénateurs.

Les sept commissions permanentes sont :

- Commission des affaires économiques
- Commission des affaires étrangères, de la défense et des forces armées
- Commission des affaires sociales
- Commission de la culture, de l'éducation et de la communication
- Commission de l'aménagement du territoire et du développement durable
- Commission des finances
- Commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale

De plus, le Sénat comprend aussi :

- la commission des affaires européennes, qui a un rôle d'information et de contrôle sur les affaires européennes ;
- des commissions spéciales qui peuvent être créées par le Sénat, à la demande du Gouvernement, du Président du Sénat ou du président d'une commission permanente ou d'un groupe politique, pour examiner un texte spécifique (le recours à cette formule est exceptionnel) ;
- des commissions mixtes paritaires (les «CMP»), réunies, en cas de désaccord entre le Sénat et l'Assemblée nationale, à l'initiative du Premier ministre. Elles regroupent 7 sénateurs et 7 députés ;
- des commissions d'enquête, qui peuvent être formées pour recueillir des informations soit sur des faits déterminés, soit sur la gestion des services publics ou des entreprises nationales ; à la différence des précédentes, elles n'ont aucune fonction législative.

ORGANISATION ADMINISTRATIVE

Parallèlement aux structures d'organisation des parlementaires, le Sénat comporte des structures administratives propres à donner aux sénateurs les moyens matériels et humains nécessaires à l'exercice de leur mandat au sein de la Haute Assemblée.

Chaque membre du personnel, fonctionnaire ou contractuel, est affecté à un poste RH qui définit un emploi. Les personnels sont soumis à des règles de mobilité, ce qui les amène à changer de poste en moyenne tous les sept ans.

L'organigramme du Sénat est présenté en annexe.

LES DIRECTIONS

L'administration du Sénat est divisée en deux directions générales elles-mêmes composées de plusieurs directions :

- la Direction générale des Missions Institutionnelles :
  - Direction de la Séance
  - Direction de la Législation et du Contrôle
  - Direction de l'Initiative parlementaire et des Délégations
  - Direction du Secrétariat du Bureau, du Protocole et des Relations internationales
  - Direction des Comptes rendus
- la Direction générale des Ressources et Moyens :
  - Direction des Ressources humaines et de la Formation
  - Direction de l'Accueil et de la Sécurité
  - Direction des Affaires financières et sociales
  - Direction de la Communication
  - Direction des Systèmes d'Information
  - Direction de la Logistique et des Moyens généraux
  - Direction de la Bibliothèque et des Archives
  - Direction de l'Architecture, du Patrimoine et des Jardins
  - Cabinet médical

LA DIRECTION DES SYSTÈMES D'INFORMATION

Au sein de la direction générale des Ressources et Moyens, la Direction des Systèmes d'Information est principalement composée de trois pôles :

- Le pôle « Documentaire » : responsable de la conception, du développement et de la maintenance des applications informatiques en matière législative et documentaire.
- Le pôle « Gestion » : responsable de la conception, du développement et de la maintenance des applications informatiques de gestion.
- Le pôle « Administration système » : responsable de la définition, de l'administration et de la sécurité des systèmes d'information et des réseaux ainsi que de la gestion des équipements informatiques.

Chaque pôle assure en plus une assistance aux utilisateurs et leur formation.

CONTEXTE LOGICIEL

ANNUAIRE

La direction des Systèmes d'Information maintient un annuaire LDAP. Cet annuaire contient les comptes et des données relatives à différentes populations : fonctionnaires, contractuels, sénateurs, collaborateurs de groupes politiques et collaborateurs de sénateurs. Parmi ces données, on trouve l'identifiant utilisateur (uid).

Aujourd'hui, l'annuaire est alimenté principalement par deux applications :

- RHPAIE, le logiciel de gestion des ressources humaines et de la paye
- SEN, l'application de gestion documentaire des sénateurs

Vous trouverez, en annexe, un schéma simplifié des données de ces deux applications.

Un logiciel de « provisionning », LDAP Sync, permet d'effectuer la synchronisation depuis ces deux bases de données vers l'annuaire LDAP.

Certains utilisateurs des applications du Sénat ne sont pas répertoriés dans cet annuaire, leurs comptes sont créés directement et uniquement dans les bases de données des applications auxquelles ils doivent avoir accès.

Les données de l'annuaire diffèrent selon la population concernée :

- Les **fonctionnaires** sont régis par un statut qui fixe leurs conditions de recrutement, d'avancement, et de rémunération. Tout comme les agents **contractuels** (dont les missions sont fixées par des normes réglementaires et un contrat), ils participent à l'organisation et à la mise en œuvre des procédures liées aux travaux parlementaires ou assurent des tâches administratives et financières. Ils appartiennent à un cadre d'emploi (agent, administrateur adjoint, informaticien,…) et sont rattachés à une direction et parfois à un service.
- Les **sénateurs** sont rattachés ou non à un groupe politique et sont membres d'une commission permanente. Ils peuvent être membres d'une ou plusieurs commissions spéciales ou temporaires.
- Les **collaborateurs de sénateurs** peuvent être employés par un ou plusieurs sénateurs. Ils les secondent dans les tâches personnelles directement liées à l'exercice du mandat.
- Les **collaborateurs de groupes politiques** sont rattachés au secrétariat d'un groupe politique. Ils dépendent du groupe pour leur recrutement et leur mode de rémunération. Un collaborateur de sénateur peut également être collaborateur de groupe politique.

Vous trouverez en annexe une note interne décrivant de manière simplifiée les attributs de l'annuaire du Sénat.

L'annuaire LDAP ne conserve aucun historique des informations qu'il contient.

APPLICATIONS

La direction des Systèmes d'Information du Sénat met à disposition des utilisateurs et assure le support et la maintenance d'environ 190 applications, réparties entre progiciels et applications développées en interne. La plupart de ces applications effectuent l'authentification des utilisateurs via l'annuaire et assignent des rôles en fonction du cadre d'emploi, de la direction, du service ou d'attributs spécifiques définis dans l'annuaire. D'autres applications utilisent leur propre base de données des utilisateurs.

À titre d'exemple, vous trouverez dans la suite de ce chapitre une description de la gestion des droits de cinq applications du Sénat.

CHRONOTIME

CHRONOTIME est une application spécifique interne utilisée par les personnels pour enregistrer et comptabiliser leurs horaires de travail.

Les personnels fonctionnaires et contractuels du Sénat saisissent leurs horaires dans CHRONOTIME. Chaque membre du personnel voit ses déclarations validées dans CHRONOTIME par son responsable hiérarchique.

CHRONOTIME enregistre également les congés et les absences des personnels.

CHRONOTIME se base sur LDAP pour l'authentification. Il existe une interface de gestion des droits qui permet d'associer chaque droit applicatif CHRONOTIME à une requête LDAP : À chaque connexion, CHRONOTIME joue l'ensemble des requêtes LDAP enregistrées dans cette interface pour vérifier quels sont les droits applicatifs de l'utilisateur.

DALI

DALI (Dépôt d'Amendements en LIgne) est l'application web de dépôt d'amendements.

Les utilisateurs de DALI peuvent être classés en deux groupes :

1. Les « déposants », auteurs des amendements sur les textes qui seront examinés en séance publique ou en commission. Il s'agit des sénateurs et du Gouvernement.
2. Les « gestionnaires » qui se chargent de traiter les amendements déposés dans DALI, du dépôt jusqu'à leur examen en séance publique ou en commission. Ils travaillent à la direction de la Séance ou à la direction de la Législation et du Contrôle (DLC). Ils ont, entre autres tâches :
    a. la confection du « dérouleur », une liste des amendements à examiner qui sera distribuée à l'ensemble des sénateurs en séance publique ou en commission ;
    b. la saisie des avis des commissions et du Gouvernement sur les amendements : favorable, défavorable ;
    c. la saisie des sorts des amendements en commission et en séance publique : adopté, rejeté.

    Un gestionnaire de la DLC ne peut agir que sur les amendements des commissions dans lesquelles il est affecté. Les gestionnaires de la Séance agissent sur les amendements de toutes les commissions.

DALI se base en grande partie sur l'annuaire pour l'identification et l'authentification de ses utilisateurs. L'application permet également de créer des comptes hors annuaire, stockés uniquement dans sa base de données. Cette fonctionnalité est utilisée par exemple pour les détenteurs de droits au nom du Gouvernement qui se connectent à DALI depuis l'extérieur du Sénat.

DATAWARE

DATAWARE est un progiciel d'infocentre et de requête transverse aux applications. Il offre un portail sur lequel les utilisateurs peuvent lancer des rapports (appelés aussi « états ») et des tableaux de bord qui interrogent les données des différentes applications du Sénat. Ces rapports sont développés et mis à disposition des utilisateurs par la DSI.

Le logiciel interroge l'annuaire LDAP pour l'authentification des utilisateurs. Les droits d'accès aux états sont définis dans le progiciel lui-même. Ils sont accordés par direction et par application.

Les demandes d'accès des directions à DATAWARE précisent rarement les domaines applicatifs concernés.

DELEGA

DELEGA est une application web qui permet le dépôt et la gestion des délégations de vote en commission et en séance publique.

Les utilisateurs de DELEGA sont les collaborateurs de groupes politiques, les collaborateurs de sénateurs et les personnels de la direction de la Séance et de la direction de la Législation et du Contrôle.

Un collaborateur de sénateur peut déposer une délégation uniquement pour le ou les sénateurs auxquels il est rattaché.

Un collaborateur de groupe politique peut déposer une délégation pour l'un des sénateurs du groupe politique qui l'emploie.

Les personnels du Sénat se connectent à l'application pour visualiser les délégations déposées au sein de leur commission.

Cette application se base uniquement sur l'annuaire LDAP pour l'authentification des utilisateurs. Les droits d'accès sont accordés par certains membres de la direction de la Séance qui sont administrateurs de cette application. Les droits d'accès peuvent être accordés à une personne en particulier (uid LDAP), une direction, un cadre d'emploi ou un cadre d'emploi d'une direction.

Les droits d'accès disponibles sont les suivants :

- Administrer : possibilité de définir les droits et de modifier et visualiser toutes les délégations de vote
- Visualiser les délégations de vote d'une commission
- Créer ou modifier des délégations de vote d'une commission dans le futur

ALLODSI

ALLODSI est un progiciel qui permet le dépôt et le suivi des demandes de support adressées à la DSI. Les demandes s'adressent aux informaticiens du pôle documentaire et du pôle des applications de gestion pour la maintenance corrective et évolutive des applications. Elles s'adressent au pôle système pour tout ce qui concerne les ordinateurs, les logiciels de base, l'infrastructure, les serveurs et la sécurité.

Un premier portail permet aux utilisateurs (personnels, sénateurs, collaborateurs) d'enregistrer une demande et de suivre son avancement. Cela peut être une demande de service ou la déclaration d'un incident en rapport avec les applications, l'infrastructure ou la fourniture de matériels et accessoires.

Certains types de demandes, comme l'arrivée d'un fonctionnaire, affichent un formulaire de saisie d'informations complémentaires pour préciser la demande.

Les personnels de la DSI disposent d'une interface « technicien » au logiciel qui leur permet de qualifier les demandes, d'échanger avec l'utilisateur pour préciser sa demande ou demander sa validation, de décrire les actions réalisées et de documenter la méthode de résolution employée.

L'ensemble des actions dans ALLODSI sont tracées et horodatées.

ALLODSI utilise uniquement l’annuaire LDAP pour l’authentification.

PROCÉDURES

PROCESSUS D'AJOUT D'UN UTILISATEUR

Lors de l'entrée d'un nouvel arrivant, la direction des Ressources humaines et de la Formation crée une entrée dans RHPAIE. Le logiciel LDAP Sync interroge régulièrement RHPAIE pour créer une entrée dans l'annuaire LDAP des nouveaux.

Une demande est déposée dans ALLODSI pour signaler l'arrivée de cette personne, en précisant notamment les accès aux applications dont elle aura besoin. Les informaticiens en charge des applications accordent les accès et profils demandés, après s'être assurés que la demande a bien été validée par le directeur d'emploi du nouvel entrant.

Les demandes d'accès aux applications par les collaborateurs sont soumises à validation de leur sénateur ou de leur groupe politique. Elles sont déposées dans ALLODSI.

Voici quelques exemples de tickets ALLODSI :

1. Nouvel arrivant

Informations générales

Client	Support
Créateur	SIROIS Harriette
Demandeur	GOSSELIN Raoul
Lieu	A1343e
Direction	D.L.M.G.
Division	Division de la logistique
Statut	Résolu
Origine	portail
Service	Mouvements de personnels / Déménagements

Type de Requête	demande de service
Sous catégorie de service	Arrivée d'un nouveau fonctionnaire / contractuel ou changement d'affectation
Titre	Changement d'affectation - GOSSELIN Raoul - 01/07/2017
Description	Changement d'affectation - GOSSELIN Raoul - 01/07/2017

2017-06-21 12:45:34 - Harriette SIROIS :

Nom du nouvel arrivant : GOSSELIN
Prénom du nouvel arrivant : Raoul
Direction d'accueil : DLC
Date d'arrivée dans la direction : 2017-07-01
Nom de la personne remplacée : cf autres informations utiles
Numéro d'unité centrale ou de portable : UC 891278 (cette UC est partie en réparation cf ticket 145325) si elle est réparée ou une nouvelle UC
Numéro d'écran : Ecran 1 : 222564- Ecran 2 : 181512 (difficile à lire car écrit à la main) anciennement 182544

Le cas échéant, groupes de messagerie (alias) dont le nouvel arrivant devra faire partie dans sa direction : info-direction-dlc@senat.fr

Si aucun matériel existant ne peut être affecté, type d'équipement demandé : Matériel déjà sur place
Local du nouvel arrivant : A0809
Accès réseau : Différent (merci de préciser)
Autres informations utiles : A terme, elle devrait remplacer Armand Laboissonnière (secrétaire administratif) quand il partira. Pour le moment, elle prend le matériel de Marie Martin (administratrice adjointe) qui n'est pas encore remplacée.
Il lui faudra avoir accès à :
COMPTA
DATAWARE

2017-06-22 13:02:27 - Serge QUESSY:

Raison escalade DSI : pour création du compte windows et envoi des identifiants ldap svp

2017-06-22 17:23:17 - Henry LAFORGE:

Paramètres envoyés par mail.

2017-07-02 10:37:08 - Daniel MAILLY:

Raison escalade DSI : Escalade pour accès aux applications :

COMPTA
DATAWARE
consultation base DecQus

2017-07-03 00:28:32 - Arthur DESILETS:

Raison escalade DSI : Bonjour Camille,
Peux-tu donner à Raoul GOSSELIN des droits d'accès comparables à ceux de Armand Laboissonnière, sur :
- DATAWARE
- COMPTA
Sachant que c'est provisoire, vu que Raoul est en tuilage avant de prendre le poste de Armand.
Poste de Raoul GOSSELIN : JD93255619
Poste de Armand Laboissonnière : LO67432199

Ensuite tu passes la main à Jean pour eMission.
Pour la base DecQus, je ne pense pas que l'on puisse donner des droits sans un accord du SGQ.
Merci,

2017-07-05 15:37:47 - Camille LAZURE:

Je l'ai ajoutée dans MAJANN

2017-07-12 10:56:29 - Camille LAZURE:

Raison escalade DSI : M GOSSELIN ne peut pas accéder à RESA gestion des Salles.

2017-07-12 10:57:31 - Camille LAZURE:

j'ai ajouté dans MAJANN les droits d'accès à RESA. Apparemment, ce n'est pas suffisant !

2017-11-13 13:14:54 - Arthur DESILETS:

Raison escalade DSI : Un vieux ticket de fin juin/début juillet.
Je pense qu'il est résolu (accès à RESA). Dans ce cas, tu pourras fermer ce ticket.
Merci.
Arthur.

2. Demande d'accès gestionnaire à l'application « Concours »

Informations générales

Client	Support
Créateur	QUIRON Louise
Demandeur	QUIRON Louise
Direction	D.R.H.F.
Division	Division du dialogue social
Service	Applications de gestion
Sous catégorie de service	Concours
Titre	droits accès base concours
Description	Bonjour, M. Humot souhaiterait pouvoir avoir accès sur la base concours aux trois concours

d'administrateur actuellement en cours, mais il ne figure pas dans la liste des personnes pour lesquelles je peux, en tant que gestionnaire du concours, ouvrir les droits d'accès. Est-il possible de l'ajouter à cette liste svp ?
Merci beaucoup par avance,
Louise

2017-11-09 13:23:45 - François PALMIER:

Solution de résolution : Ajout du poste de M. HUMOT avec profil ADMIN RH comme les administrateurs-adjoints.

3. Demande d'accès à l'administration d'une commission dans DALI

Informations générales

Client	Support
Créateur	LAUX Laure
Demandeur	LAUX Laure
Lieu	NON DÉFINI
Direction	D.L.C.
Division	Commission des affaires économiques
Statut	Résolu
Origine	portail
Service	Applications parlementaires
Type de Requête	incident
Sous catégorie de service	DALI
Titre	Accès à DALI

Description	Pourriez-vous, s'il vous plait, me donner accès à l'application DALI (pour les commissions des affaires économiques et de l'aménagement du territoire) ? Merci

2017-11-08 13:29:47 - Pascal MOUSSEAU:

Solution de résolution : Bonjour,
votre accès DALI pour la commission du développement durable a été activé.
Vous disposez donc de 2 logins :
1) llaux => pour accéder à DALI pour la commission des affaires économiques
2) DEVDUR.llaux => pour accéder à DALI pour la commission de l'aménagement du territoire et du développement durable

Bien cordialement,
Pascal Mousseau

REVUE ANNUELLE

Chaque année, une revue des droits d'accès est organisée. Chaque Directeur doit valider la liste des droits d'accès de ses personnels aux différentes applications. Il valide également les droits d'accès distants en indiquant lesquels de ses personnels disposent d'un droit d'accès distant et pour quelles applications.

QUESTIONS

QUESTION 1 (*2 POINTS*)

Recensez de façon exhaustive tous les droits d'accès que l'on peut identifier dans le contexte décrit ci-avant.

QUESTION 2 (*1 POINT*)

Quels sont, à votre avis les problèmes, posés par la situation actuelle ?

QUESTION 3(*0,25 POINT*)

En analysant le contexte organisationnel, identifiez quels seront, selon vous, les utilisateurs de votre application.

QUESTION 4 (*1,5 POINT*)

Décrivez quelles doivent être, selon vous, les grandes étapes du projet.

QUESTION 5 (*0,5 POINT*)

Quelle méthodologie appliqueriez-vous pour gérer un projet de ce type ? Quels impératifs devez-vous respecter pour que votre méthodologie fonctionne ?

QUESTION 6 (*1 POINT*)

Quelles difficultés ou quels risques identifiez-vous a priori sur ce projet ? Que proposez-vous pour atténuer ces risques ?

QUESTION 7 (*1 POINT*)

Imaginez et décrivez dans les grandes lignes une solution technique répondant aux objectifs du projet.

QUESTION 8 (*3 POINTS*)

Afin d'illustrer votre solution, vous devez réaliser un schéma logique du modèle de données.

Vous devez fournir de préférence un diagramme de classes au formalisme UML (sans indiquer les attributs). Si vous utilisez un autre formalisme, merci d'indiquer celui que vous avez choisi.

QUESTION 9 (*0,5 POINT*)

Détaillez les interactions entre ce nouveau système et les composants actuels du système, tels que décrits dans le chapitre « Contexte logiciel ».

QUESTION 10 (*1 POINT*)

La gestion des droits par utilisateur et par application est chronophage.

Que proposez-vous pour remédier à ce problème ?

Décrivez les modifications à apporter en conséquence à votre solution.

QUESTION 11 (*1,25 POINT*)

Afin de s'assurer au mieux de la bonne ergonomie de l'application avant sa réalisation, on souhaite réaliser des maquettes des principales interfaces homme-machine.

Dessinez les maquettes des écrans permettant la mise à jour des droits d'un utilisateur.

QUESTION 12 (*1 POINT*)

Pour des besoins d'audit, on veut connaître la liste des droits dont une personne disposait à une date donnée.

Décrivez les modifications à apporter à votre solution pour répondre à ce besoin.

QUESTION 13 (*1 POINT*)

On souhaite maintenant pouvoir gérer les délégations d'accès. Une personne délégante peut désigner une personne délégataire qui va hériter de ses droits sur une ou plusieurs applications pour une période définie.

Décrivez les modifications à apporter à votre solution pour répondre à cette demande fonctionnelle.

QUESTION 14 (*0,25 POINT*)

Le Sénat dispose d'un portail web dit « VPN SSL » qui permet aux utilisateurs d'accéder aux applications du Sénat lorsqu'ils sont connectés depuis un réseau extérieur au Sénat. Ce portail d'accès se base exclusivement sur l'annuaire pour la gestion de l'authentification et des autorisations.

Le portail est administré par le pôle systèmes.

Les droits sont attribués aux personnes dans RHPAIE. Sont définis : une date de début et de fin d'accès distant au portail et une date de début et de fin d'accès distant, application par application. Les applications sont identifiées par un code qui alimente un attribut multivalué de l'annuaire.

Le portail d'accès interroge l'annuaire pour autoriser l'accès aux applications depuis l'extérieur.

Il est possible d'accorder à un utilisateur l'accès à une application depuis le réseau interne sans que cela lui ouvre automatiquement l'accès à cette même application par le VPN SSL. La réciproque n'est pas vraie : un utilisateur qui dispose des droits d'accès à une application via le VPN SSL dispose nécessairement des mêmes droits d'accès sur cette application en interne.

Indiquez comment modifier votre solution pour gérer les droits d'accès « VPN SSL » des utilisateurs aux applications.

QUESTION 15 (*0,25 POINT*)

Vous devez écrire une requête LDAP pour interroger l'annuaire.

Cette requête doit trouver les personnes :

- Qui sont collaborateurs d'un sénateur
    - et
- Qui ne sont pas collaborateurs de groupe politique ou qui sont collaborateurs du groupe politique RASNAG

Vous trouverez en annexe le schéma de l'annuaire ainsi que la syntaxe des requêtes LDAP.

QUESTION 16 (*1,5 POINT*)

Proposez un modèle physique des données de type relationnel. Précisez les tables, attributs (sans les types) et contraintes que vous envisagez.

Exemple de présentation d'une table : MATABLE (COL1, COL2, COL3, COL4)

QUESTION 17 (*0,5 POINT*)

Votre solution est en place depuis le 1er janvier 2019.

Nous sommes le 1er janvier 2021.

En vous basant sur les tables décrites dans la question précédente, écrire les requêtes SQL pour répondre aux questions suivantes (une seule requête par question) :

- À quelles applications a droit actuellement le collaborateur David MARTIN du groupe Socialiste ?
- À quelles applications avaient accès les collaborateurs du sénateur KOLTER au 15 juin 2020 ?

QUESTION 18 (*0,5 POINT*)

Certaines applications doivent pouvoir être utilisées par des personnes extérieures au Sénat qui n'appartiennent à aucune des populations citées précédemment.

Comment intégrez-vous ces personnes dans votre Solution pour leur donner les droits nécessaires ?

Quelles évolutions fonctionnelles seraient, selon vous, nécessaires dans les autres composantes du système qui sont décrites dans l'énoncé ?

QUESTION 19 (*1,5 POINT*)

On souhaite que les autres applications du système d'information du Sénat puissent interroger votre solution à travers une API REST.

- Expliquez ce qu'est une API REST.
- Documentez l'API que pourrait proposer votre solution, en vous limitant à cinq méthodes parmi les plus importantes.

QUESTION 20 (*0,5 POINT*)

On souhaite sécuriser l'accès à l'API REST de la question précédente.

- Citez au moins deux techniques permettant de répondre à ce besoin.
- Quelle technique utiliseriez-vous ? Pourquoi ?

ANNEXES

DOCUMENTATION DE L'ANNUAIRE LDAP

PRÉSENTATION DU SCHÉMA

Le schéma d'un annuaire LDAP est un ensemble de règles qui définissent comment les données peuvent être stockées dans l'annuaire.

Les données sont stockées sous la forme d'entrées d'annuaire. Chaque entrée est constituée d'un ensemble d'attributs et de leurs valeurs. Chaque entrée doit posséder une classe d'objet. Une classe d'objet spécifie le type d'objet qui est décrit par l'entrée et définit l'ensemble des attributs qu'elle peut contenir.

Le schéma définit les types d'entrées autorisés, leur structure en termes d'attributs ainsi que la syntaxe des attributs. Le schéma peut être modifié et étendu.

SCHÉMA DES CLASSES ET DES ATTRIBUTS LDAP

Le tableau suivant énumère les classes d'objet (objectClass) et, pour chacune, les attributs associés.

Une classe d'objets hérite des attributs de sa classe parente. Ainsi, la classe Contractuel hérite de l'attribut nomPersonne via la classe Personnel, qui hérite elle-même de la classe Personne.

Classes et attributs LDAP			
Classe (objectClass)	**Hérite de**	**Attributs**	**Description**
Personne		uid nomPersonne prenomPersonne mailPersonne applicationsVPN (multivalué) desactive	Identifiant utilisateur Nom Prénom Mail Liste des applications distantes (pour le VPN SSL) desactive=oui/non
Senateur	Personne	groupePolitique commissionPermanente	Groupe politique du sénateur Commission permanente
Personnel	Personne	societe matricule cadre posteHR direction service manager	Société Matricule Cadre d'emploi Identifiant de l'emploi (poste) occupé Direction d'emploi Service d'emploi Responsable hiérarchique
Fonctionnaire	Personnel	debutFonction	Date d'entrée

		finFonction	Date de sortie
Contractuel	Personnel	debutContrat finContrat	Date de début de contrat Date de fin de contrat
Stagiaire	Personne	debutStage finStage	Date de début de stage Date de fin de stage
CollaborateurGroupe	Personne	groupePolitiqueCol	Groupe politique du collaborateur
CollaborateurSenateur	Personne	senateurCol (multivalué)	Sénateur du collaborateur

Exemple de requête LDAP :

- Recherche des stagiaires dont le nom commence par A
    - `(&(objectClass=Stagiaire)(nomPersonne=A*))`

La syntaxe des requêtes d'interrogation est décrite dans l'annexe « syntaxe des requêtes LDAP ».

DOCUMENTATION DES APPLICATIONS HRPAIE ET SEN

SCHÉMA DES DONNÉES HRPAIE

Description fonctionnelle sommaire pour la compréhension de schéma des données :

- Dans HRPAIE, les personnes sont regroupées par société : Sénateurs, Fonctionnaires, Contractuels, Collaborateurs de sénateurs, Collaborateurs de groupes.
- Toutes les personnes sont identifiées par un matricule, unique au sein de chaque population.
- Les personnels – fonctionnaires et contractuels – sont affectés à un poste (ou « emploi ») qui détermine la Direction d'emploi et le Service.
- Un poste n'est occupé que par un seul personnel à une date donnée.
- Inversement, un personnel n'est affecté qu'à un seul poste à une date donnée.

Voici un schéma simplifié des tables du progiciel HRPAIE (les clefs sont en gras souligné).

- PERSONNE (**Societe**, **Matricule**, Nom, Prenom, …)
    - Societe parmi : SEN, FONC, CONT, COLSEN, COLGRP.
- POSTE (**CodePoste**, LibellePoste)
- AFF_PER_POSTE (**Societe**, **Matricule**, **DateDebut**, DateFin, CodePoste)
- AFF_POSTE_DIR (**CodePoste**, **DateDebut**, DateFin, CodeDirection, CodeService, …)

SCHÉMA DES DONNÉES SEN

Voici un schéma simplifié des tables de l'application SEN.

- SENATEUR (**idSen**, Nom, Prenom, MatriculeHR, …)
- MEMBRE_COM (**idSen**, CodCom, **DatDeb**, DatFin)
- MEMBRE_GRP (**idSen**, CodGrpPol, **DatDeb**, DatFin)

- COMMISSION (**CodCom**, TypCom, …)
    - TypCom parmi : Permanente, Spéciale, Enquête, CMP.
- MANDAT_SEN (**idSen, DatDeb**, DatFin, …)
- FONCTION_SEN (**idSen**, CodFct, **DatDeb**, DatFin, …)
- FONCTION (**CodFct**, LibFct, …)
- GROUPE_POL (**CodGrpPol**, LibGrpPol,…)

Description fonctionnelle :

- Dans SEN, les personnes sont identifiée par un identifiant interne. Le matricule issu d'HRPAIE est cependant présent.
- Les commissions ont été présentées en introduction du sujet.
- La table MANDAT_SEN permet de retrouver l'historique des mandats sénatoriaux.
- La table FONCTION_SEN permet de retrouver l'historique des fonctions des sénateurs (Président du Sénat, Président de Commission, Questeur, etc.)

SYNTAXE DES REQUÊTES LDAP

La syntaxe des requêtes d'interrogation LDAP est définie par la RFC2254 (Représentation sous forme de chaîne des filtres de recherche LDAP).

La forme générale d'une requête LDAP est une série de filtres placés entre parenthèses et précédés d'un opérateur :

`(operateur(filtre)(filtre)...)`

Les opérateurs sont booléens :

- ET est représenté par une esperluette (&).
- OU est représenté par une barre oblique (|).
- NON est représenté par un point d'exclamation (!).

Les filtres expriment une condition :

- Égalité attribut=valeur
- Supérieur attribut>valeur
- Inférieur attribut<valeur

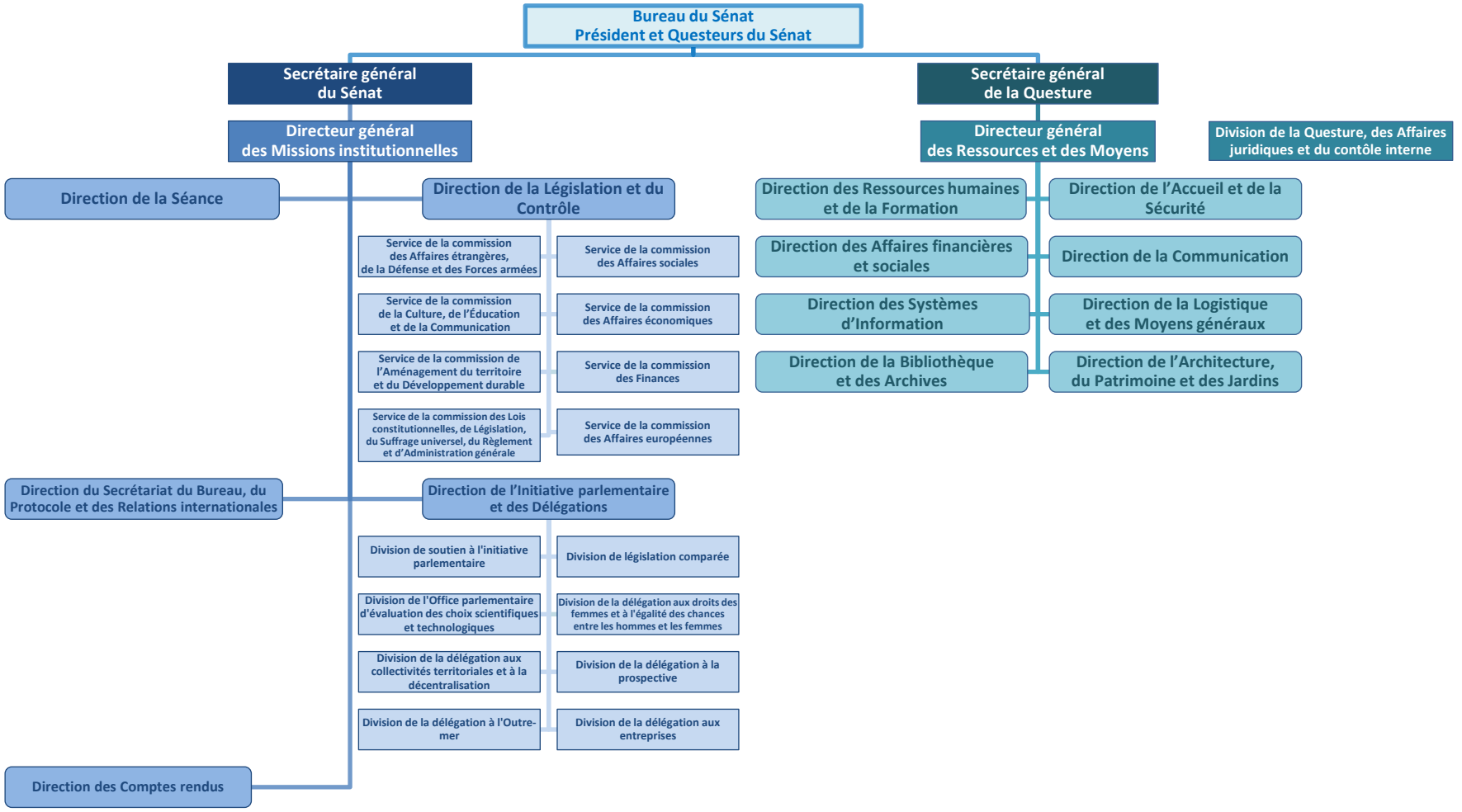
Le caractère générique astérisque (*) représente toute chaîne de caractères et permet d'effectuer des recherches approchées :

- Commence par attribut=valeur*
- Contient attribut=*valeur*
- N'est pas vide attribut=*

Exemple :

- `(&(objectClass=Senateur)(nomPersonne=Bou*)(!(prenomPersonne=Martin)))`
- Recherche toutes les entrées
    - Qui sont de la classe « Senateur »
    - ET dont le nom commence par « Bou »
    - ET dont le prénom n'est pas « Martin ».

ORGANIGRAMME DU SÉNAT



ÉPREUVES ORALES D'ADMISSION

1. Épreuve orale portant sur des connaissances techniques

Cette épreuve est constituée par :

- un exposé oral d'une durée de dix minutes sur un sujet tiré au sort ;

- des questions, pendant trente minutes, ayant pour point de départ l'exposé oral et pouvant porter sur d'autres sujets.

(préparation 20 minutes – durée 40 minutes – coefficient 4)

2. Entretien libre avec le jury

Cette épreuve est constituée par :

- un exposé oral d'une durée de cinq minutes présentant un cas concret tiré de l'expérience professionnelle du candidat (projet, stage ou travail d'étude) ;

- un entretien d'une durée de vingt-cinq minutes environ visant à apprécier l'adéquation du candidat à l'emploi d'informaticien et sa motivation pour exercer ces fonctions, ainsi que sa culture générale et sa perception des orientations et des enjeux des technologies de l'information.

Pour cette épreuve, le jury dispose d'une fiche de renseignements individuelle, préalablement remplie par les candidats et ne faisant l'objet d'aucune notation.

(durée 30 minutes – coefficient 6)

ÉPREUVE ORALE PORTANT SUR DES CONNAISSANCES TECHNIQUES

PROFIL « ADMINISTRATION DES SYSTÈMES »

(préparation 20 minutes – durée 40 minutes – coefficient 4)

SUJET N° 1

Vous pouvez faire les hypothèses techniques qui vous semblent appropriées. Vous devrez les indiquer. Tous les choix doivent être justifiés

Le Sénat dispose de deux salles informatiques dont l'une est équipée avec l'ensemble des serveurs et la seconde, plus récente, n'est pour le moment connectée qu'à l'infrastructure réseau. Le Sénat pouvant être amené à siéger tous les jours de la semaine, en journée et la nuit, il existe une contrainte de disponibilité forte. Pour certaines applications, la Direction des Systèmes d'Information (DSI) doit donc assurer un service sans interruption même en cas de problème ou de sinistre (énergétique / matériel / réseau / système / logiciel / sanitaire /...) et souhaite utiliser les deux salles. Les applications concernées s'appuient sur une solution de virtualisation. Elles sont multi-tiers (avec ou sans base de données) et proposent aux utilisateurs des services Web accessibles en HTTPS.

<u>Questions</u> :
- Quelle est la différence entre un PCA et un PRA ? Qu'évoquent pour vous les termes de RPO (ou PDMA) et de RTO (ou DMIA) ?
- Que faut-il mettre en œuvre pour assurer cette continuité de service ?

ÉPREUVE ORALE PORTANT SUR DES CONNAISSANCES TECHNIQUES

PROFIL « ADMINISTRATION DES SYSTÈMES »

(préparation 20 minutes – durée 40 minutes – coefficient 4)

SUJET N° 2

Vous pouvez faire les hypothèses techniques qui vous semblent appropriées. Vous devrez les indiquer. Tous les choix doivent être justifiés

Le Sénat dispose d'une solution de stockage centralisé en iSCSI utilisée avec son infrastructure de virtualisation. La solution matérielle est aujourd'hui abandonnée par son éditeur/constructeur. Il est donc nécessaire de réfléchir à son remplacement, en utilisant ou non la même technologie.
Le commercial de l'éditeur/constructeur nous présente sa nouvelle solution à base d'hyper-convergence. Par ailleurs, au cours des prochaines années, le Sénat envisage de virtualiser son parc de 1200 postes de travail.

<u>Questions</u> :
- Présentez succinctement les technologies de stockage adaptées à la virtualisation de serveurs.
- L'hyper-convergence serait-elle adaptée au projet de virtualisation des postes de travail ?

ÉPREUVE ORALE PORTANT SUR DES CONNAISSANCES TECHNIQUES

PROFIL « ADMINISTRATION DES SYSTÈMES »

(préparation 20 minutes – durée 40 minutes – coefficient 4)

SUJET N° 3

Vous pouvez faire les hypothèses techniques qui vous semblent appropriées. Vous devrez les indiquer. Tous les choix doivent être justifiés

Le Sénat met à disposition de ses utilisateurs internes plusieurs applications accessibles depuis Internet : webmail, gestion d'agendas, accès à certaines applications métiers. Il n'est pas possible de mettre à jour certaines de ces applications et pour d'autres la gestion des droits est très complexe. Il est envisagé la mise en place d'un VPN, mais la très grande majorité des utilisateurs n'a pas de profil technique, peu ont un mot de passe complexe, et aucun n'utiliserait un ordinateur fourni par le Sénat pour cet accès VPN.

<u>Questions</u> :
- Qu'est-ce qu'un VPN ? Décrivez plusieurs technologies de VPN.
- Quelle technologie choisissez-vous ? Quelles nouvelles contraintes cela impose-t-il ?

ÉPREUVE ORALE PORTANT SUR DES CONNAISSANCES TECHNIQUES

PROFIL « DEVELOPPEMENT »

(préparation 20 minutes – durée 40 minutes – coefficient 4)

SUJET N° 1

Le Sénat produit trois types de comptes rendus des débats en utilisant le traitement de texte Microsoft Word :
- le compte rendu intégral de la séance publique (CRI), qui est un verbatim (compte rendu en termes exacts) de ce qui se dit en séance publique ;
- le compte rendu analytique (CRA) qui est un compte rendu résumé de ce qui se dit en séance publique ;
- le compte rendu détaillé des commissions (CRED).
Ces trois types de compte rendu sont publics et font l'objet d'une publication HTML sur le site web du Sénat, ainsi qu'en *open data* sur une plateforme dédiée.

Chaque type de compte rendu est réalisé à partir de développements de macros sous Word, mal documentées et mal maintenues par la Direction des Systèmes d'Information (DSI) du Sénat. Les utilisateurs souhaiteraient des évolutions :

- les rédacteurs du CRI, s'inspirant de ce que l'Assemblée nationale a développé, souhaiteraient un produit plus structuré qui permettrait non seulement de manipuler chapitre, sous chapitre, citations,… plus clairement, mais également de bénéficier des données présentes dans le SI du Sénat (nom des sénateurs, intitulé des différents organes du Sénat, titres des projets de lois, points de l'ordre du jour, extraits présents en base de données à insérer dans le compte rendu…) sans être obligé de faire du copier-coller à partir du site web du Sénat ;

- les rédacteurs du CRA souhaiteraient que leur travail soit mieux inséré dans le site web du Sénat (accès à partir des fiches biographiques des sénateurs, accès à partir des textes en cours de discussion,…), mais leur compte rendu, en Word, ne permet pas de faire le lien avec diverses données du SI qui servent à générer ces accès sur le site Internet ;

- les rédacteurs du CRED sont très attachés à la convivialité et à la facilité d'utilisation de Word et craignent que tout changement de leur outil conduise à rendre plus difficile leur travail. Par ailleurs, férus de nouvelles technologies, ils se demandent s'il ne serait pas possible, compte tenu des progrès récents, d'utiliser des techniques de transcription automatique de la parole pour les aider ;

- les sénateurs trouvent que leurs interventions ne sont pas suffisamment mises en valeur et souhaiteraient que leurs propos soient regroupés de manière intelligible sur la notice biographique de chacun.

La DSI, en raison de ses effectifs réduits, a du mal à maintenir trois produits différents. Elle constate, par ailleurs, que les rédacteurs sont amenés à changer de rôle (rédacteur du CRI puis du CRED par exemple) en cours de carrière, et sont perdus lorsqu'ils passent d'un outil de rédaction à un autre. C'est pourquoi, elle souhaiterait remplacer les trois outils de compte rendu par un seul produit en l'inscrivant dans sa stratégie d'abandon de Word au profit d'outils permettant de produire des données structurées.

Vous êtes chargé de mener à bien ce projet : comment l'abordez-vous ? Quels en sont les points clefs ? Quelles étapes et quelle organisation du projet souhaiteriez-vous mettre en place ?

ÉPREUVE ORALE PORTANT SUR DES CONNAISSANCES TECHNIQUES

PROFIL « DEVELOPPEMENT »

(préparation 20 minutes – durée 40 minutes – coefficient 4)

SUJET N° 2

À l’occasion de la refonte de son site internet, le Sénat souhaite rénover le moteur de recherche de ce dernier.

Ce moteur a été mis en place il y a quinze ans. Le cœur de ce moteur a été développé par un petit éditeur logiciel français. Le Sénat a développé autour, en Java, de nombreuses interfaces avec ses bases de données documentaires afin de donner accès à l’ensemble de leur contenu public. Cette brique logicielle est aussi utilisée dans des développements internes au Sénat pour des applications dont les données ne sont pas publiques. L’interface utilisateur pour effectuer les recherches est également un développement spécifique en Java.

Serveur web du Sénat et moteur de recherche sont hébergés sur les infrastructures techniques du Sénat. Lors de la refonte, la Direction des Systèmes d’Information (DSI) s’interroge sur l’intérêt et la possibilité d’une externalisation partielle ou totale de ces infrastructures.

Lors d’un contact commercial avec l’éditeur, la DSI comprend que la recherche documentaire n’est plus vraiment la priorité de ce dernier qui s’oriente plutôt vers tout ce qui tourne autour du « Big-Data ». Par ailleurs, l’Assemblée nationale nous fait part de ses projets d’externaliser son propre moteur de recherche vers un fournisseur de solution en mode SaaS, solution moins précise en termes de pertinence mais indexant beaucoup plus rapidement et permettant de mettre en place des alertes en temps réel (le fait de pouvoir enregistrer une recherche et d’être prévenu par mail lors de la publication d’un nouveau document qui correspond à la recherche). Des chercheurs auditionnés par le Sénat ont fait état de leurs travaux permettant d’améliorer les recherches documentaires par de l’IA. Les informaticiens de la DSI avouent ne pas être très au courant des derniers développements en matière de recherche documentaire.

Beaucoup d’utilisateurs internes nous font savoir qu’ils utilisent plus volontiers Google pour trouver des informations. Nos bases documentaires publiant systématiquement leurs informations sur le site web du Sénat, toutes les informations sont bien indexées par Google. *A contrario*, la Direction de la Bibliothèque et des Archives nous précise qu’elle tient absolument à notre approche, qui à la différence de Google, regroupe dans les résultats de recherche les documents qui sont structurellement liés (par exemple, les différentes versions d’un texte au cours de la navette entre l’Assemblée nationale et le Sénat).

La Cellule Internet qui gère le site nous fait savoir que plusieurs internautes se plaignent de ne pas trouver par le moteur les pages les plus importantes du site web. Aucune statistique globale d’utilisation du moteur n’est disponible.

La Direction de la Législation et du Contrôle nous fait savoir qu’elle regrette le manque de visibilité des travaux parlementaires du Sénat.

Plusieurs sénateurs se plaignent du manque de maniabilité du moteur de recherche sur tablette ou sur smartphone et se plaignent également de la lenteur des alertes qui ne sont générées qu’une fois par jour.

Vous êtes chargé de mener à bien ce projet, comment l’abordez-vous ? Quels en sont les points clefs ? Quelles étapes et quelle organisation du projet souhaiteriez-vous mettre en place ?

ÉPREUVE ORALE PORTANT SUR DES CONNAISSANCES TECHNIQUES

PROFIL « DEVELOPPEMENT »

(préparation 20 minutes – durée 40 minutes – coefficient 4)

SUJET N° 3

Au sein de la Direction des Affaires financières et sociales (DAFS) du Sénat, deux divisions sont chargées des prestations sociales.

- La Division de la protection sociale (DPS) assure la gestion du Régime autonome de sécurité sociale du Sénat et liquide les prestations familiales versées aux sénateurs et aux fonctionnaires.
- La Division du budget et de la paie (DBP) liquide les prestations familiales versées aux contractuels qui sont par ailleurs affiliés au régime général.

Les prestations familiales sont gérées dans le progiciel de gestion RH/Paie « HRAccess » installé dans les locaux de la Direction des Systèmes d'Information (DSI) du Sénat et dont le paramétrage est assuré par cette direction.
Les prestations assurance-maladie sont gérées dans le progiciel ESQUIF hébergé sur un site distant et sous contrat d'infogérance.

Chaque année, au début du mois d'octobre, la DAFS adresse une « déclaration sur l'honneur » à l'ensemble des sénateurs et des personnels pour actualiser leur situation. Il s'agit d'un formulaire papier permettant de recueillir diverses informations personnelles et confidentielles - concernant les enfants et les conjoints - nécessaires à la liquidation des prestations familiales dans HRAccess et à la mise à jour du dossier des assurés dans ESQUIF. Les assurés retournent le formulaire signé, accompagné des pièces justificatives utiles.

À leur réception par la DAFS, les formulaires des contractuels sont remis à la DBP tandis que les autres sont remis à la DPS. La DPS contrôle le formulaire et les pièces jointes, met à jour les données ESQUIF puis les données HRAccess. La DBP contrôle le formulaire et les pièces jointes puis met à jour les données HRAccess.

Ce processus papier est chronophage avec la préparation des formulaires, le publipostage, l'ouverture des enveloppes, la photocopie des documents et leur transmission à la division concernée, la tenue d'un tableau de suivi des documents reçus et des lettres de relance émises et enfin, la mise à jour manuelle des informations dans les progiciels.

C'est pourquoi la DAFS souhaite dématérialiser les déclarations sur l'honneur. Un formulaire en ligne serait ouvert à destination des sénateurs et des personnels pour établir leur déclaration sur l'honneur et déposer leurs pièces justificatives sous forme numérique. Les données collectées seraient accessibles à la DAFS pour validation et une interface est envisagée vers le progiciel HRAccess pour une mise à jour automatique des données.

L'Assemblée nationale a mis en place un module ESQUIF pour des déclarations dématérialisées. Si ce système convenait à la DPS, il ne couvrirait en revanche pas tous les besoins de la DBP pour qui l'interface vers le système RH/Paie est un point important du projet.

Vous êtes chargé de mener à bien ce projet : comment l'abordez-vous ? Quels en sont les points clefs ? Quelles étapes et quelle organisation du projet souhaiteriez-vous mettre en place ?