Partie 5 :

La disponibilité

Formateur : Azer Zairi
(azer.zairi@gnet.tn)

Partie 5 – Sections et objectifs

5.1 La haute disponibilité

Expliquer le concept de haute disponibilité.

5.2 Les mesures pour améliorer la disponibilité

Expliquer comment les mesures relatives à la haute disponibilité permettent d'améliorer la disponibilité.

5.3 Gestion des incidents

Décrire comment un plan de gestion des incidents améliore la haute disponibilité.

5.4 Reprise après sinistre

Décrire l'importance du plan de reprise après sinistre sur l'amélioration de la haute disponibilité.

5.1 La haute disponibilité

La haute disponibilité

Les cinq neuf

À quoi correspondent les cinq neuf ?

- L'expression **cinq neuf** signifie que les **systèmes** et les **services** sont **disponibles 99,999 % du temps**.
- Elle signifie également que les **interruptions** planifiées et non planifiées représentent **moins** de **5,26 minutes par an**.
- **La haute disponibilité** fait référence à un **système** ou un **composant** qui est **opérationnel sans interruption** sur une période donnée.
- Pour assurer la **haute disponibilité** il est important de :
  - **Supprimer** les **points** de **défaillance uniques**
  - **Concevoir** un **système** assurant la **fiabilité**
  - **Détecter** les **défaillances avant** qu'elles ne **surviennent**

Disponibilité	Temps d'arrêt/an
99 %	87 heures et 36 minutes
99,5 %	43 heures et 48 minutes
99,95 %	4 heures et 23 minutes
99,99 %	53 mins
99,999 %	5 mins

La haute disponibilité

Les cinq neuf (suite)

Environnements qui exigent les cinq neuf

Même si préserver la **haute disponibilité** peut être **coûteux** dans certains secteurs, **plusieurs environnements** ont **besoin** d'atteindre ces **99,999 %**.

- Le **secteur de la finance** doit préserver la haute disponibilité de ses systèmes pour garantir les opérations commerciales, la conformité et la confiance des clients.
- La haute disponibilité est indispensable dans le **secteur de la santé** pour soigner les patients 24 h/24.
- Le **secteur de la sécurité publique** compte des agences qui assurent la sécurité d'une ville, d'une région ou d'un pays.
- Le secteur du **commerce** dépend de l'efficacité des **chaînes d'approvisionnement** et de la **livraison** de produits aux clients.

Toute interruption peut être **catastrophique**, notamment pendant les périodes de forte affluence, comme les fêtes.

Secteur de la finance


Établissements de santé


Sécurité publique

La haute disponibilité

Les cinq neuf (suite)

Les menaces qui pèsent sur la disponibilité

Différents types de **menaces** peuvent **affecter** la **haute disponibilité**, de la **défaillance** d'une application **critique** à un **événement climatique** grave comme un ouragan ou une tornade.

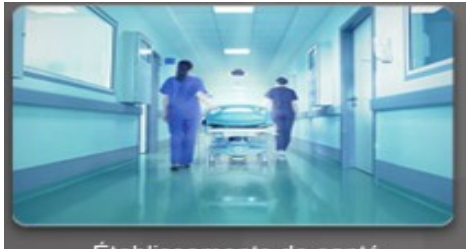
Les menaces peuvent également inclure un événement catastrophique comme une **attaque terroriste**, **l'explosion** ou **l'incendie** d'un bâtiment.

Conception d'un système à haute disponibilité

La haute disponibilité intègre **trois principes majeurs** pour garantir un accès ininterrompu aux données et aux services :

- **L'élimination** ou la réduction des **points** de **défaillance uniques**
- La **résilience** du **système**
- La **tolérance** aux **pannes**

Secteur de la finance


Établissements de santé


Sécurité publique

5.2 Les mesures pour améliorer la disponibilité

Mesures visant à améliorer la disponibilité

La gestion des ressources

Une entreprise doit savoir **quelles sont** les **ressources** matérielles et logicielles dont elle dispose afin de **mieux** les **protéger**.

La gestion des ressources implique un **inventaire complet** du **matériel** et des **logiciels**.

L'entreprise doit **connaître tous** les **composants** qui peuvent **courir** des **risques** en matière de sécurité, notamment :

- Chaque système matériel
- Chaque système d'exploitation
- Chaque périphérique réseau
- Chaque système d'exploitation des périphériques réseau
- Chaque application logicielle
- Tous les micrologiciels
- Tous les environnements d'exécution
- Toutes les bibliothèques individuelles

La plupart des entreprises choisissent une **solution automatisée** pour **suivre** leurs **ressources**.

Mesures visant à améliorer la disponibilité

La gestion des ressources (suite)

- **Classification des ressources : affecte toutes** les **ressources** d'une entreprise **à un groupe** en fonction de **caractéristiques communes**.
  - Une entreprise **doit mettre en place un système de classification des ressources** (documents, dossiers de données, fichiers de données et disques).
- **Standardisation des ressources :** dans le cadre d'un système de gestion des ressources informatiques, une entreprise spécifie les **ressources** informatiques **acceptables** répondant à ses objectifs.
- **Identification des menaces :** l'équipe **CERT** (Computer Emergency Readiness Team) et le **Département** de la **Sécurité intérieure** des États-Unis commanditent un **dictionnaire** des **vulnérabilités** et **expositions courantes** (CVE).
  - L'identification **CVE** associe un **numéro d'identifiant standard** avec une **brève description** et des **références** aux **rapports** et **conseils** sur les vulnérabilités.

Mesures visant à améliorer la disponibilité

La gestion des ressources (suite)

- **Analyse des risques :** il s'agit de l'analyse des **risques liés aux événements naturels** ou **provoqués** par l'homme pour les ressources d'une entreprise.
  - Un **utilisateur identifie les ressources pour savoir lesquelles protéger**.
- **Atténuation :** l'atténuation implique de **réduire** la **gravité** ou la **probabilité** d'une **perte**.
  - De **nombreux contrôles techniques** réduisent les risques, comme les **systèmes d'authentification**, les **autorisations** de fichiers et les **pare-feu.**

Les mesures pour améliorer la disponibilité

Une protection avancée

La protection avancée **ne fournit pas une barrière** informatique **infranchissable**, mais elle permet aux entreprises de **minimiser les risques** en gardant un **temps d'avance** sur les **cybercriminels**.

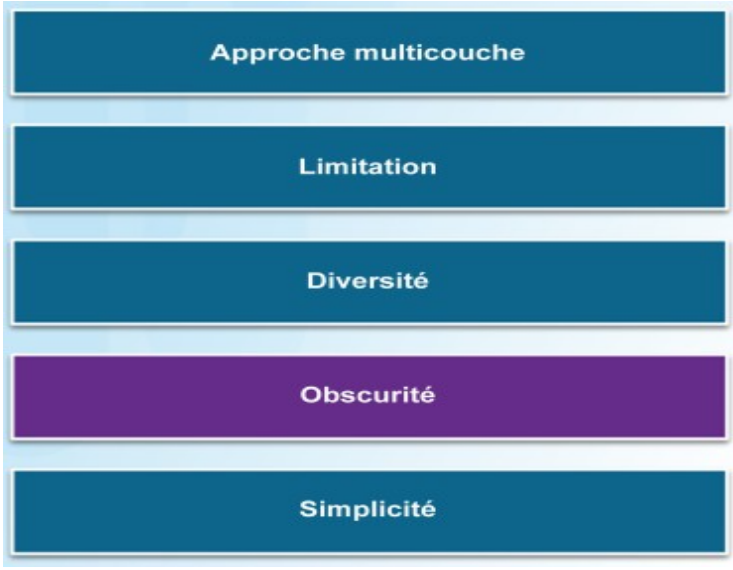
Pour **garantir** que les données et les informations **restent disponibles**, une entreprise doit créer différentes couches de protection :

- Une approche **multicouche** fournit la protection la plus complète.
  - Lorsque des cybercriminels **pénètrent une couche**, ils doivent encore **franchir plusieurs couches supplémentaires** plus **complexes** les unes que les autres.
  - Les **diverses couches** créent une **barrière** de **protections multiples** qui se coordonnent pour **éviter** les **attaques**.
- **Limiter** l'accès aux données et aux informations réduit les possibilités de menace.
  - Il est conseillé aux entreprises de **restreindre l'accès aux utilisateurs** et de ne leur permettre que d'accéder aux **ressources** dont ils ont **besoin** pour accomplir leur mission.

Les mesures pour améliorer la disponibilité

Une protection avancée (Suite)

- La **diversité** consiste à **changer** les **contrôles** et les **procédures** en fonction des différentes **couches**.
  - Une attaque qui touche une seule couche de sécurité ne compromet pas l'intégralité du système.
  - Une entreprise peut utiliser divers algorithmes de chiffrement ou systèmes d'authentification afin de protéger les données à différents états.
- La **dissimulation** d'informations permet également de protéger les données et les informations.
  - Une entreprise **ne doit pas dévoiler d'informations** que les cybercriminels peuvent utiliser pour déterminer le système d'exploitation qu'un serveur exécute ou le type d'équipement qu'il utilise.
- La **complexité n'est pas** nécessairement une **garantie** de la **sécurité**.
  - Un processus ou une technologie **trop complexes** peuvent être à **l'origine d'erreurs** de configuration ou de non conformités.
  - La **simplicité** peut réellement améliorer la disponibilité.

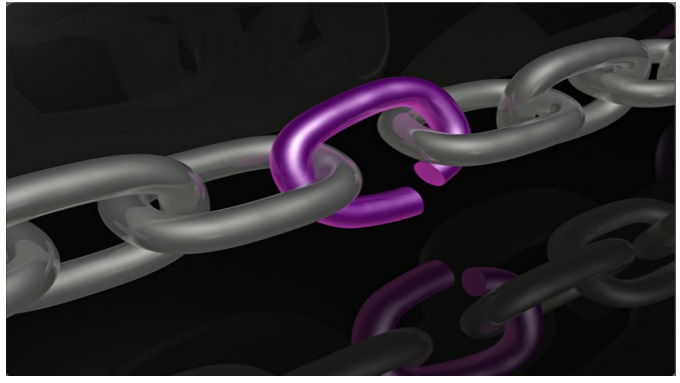


Mesures visant à améliorer la disponibilité

Redondance

Tout **point de défaillance unique** doit être identifié et corrigé.

Il peut s'agir d'un matériel spécifique, d'un processus, de données spécifiques ou même d'un utilitaire essentiel.



- Les points de défaillance uniques sont les **liens faibles de la chaîne** qui peuvent **perturber l'activité** de l'entreprise.
- Généralement, **en cas de point de défaillance unique**, la solution consiste à **modifier l'activité critique** de façon qu'elle ne s'appuie pas sur un seul élément.
- L'entreprise peut également **intégrer** dans **l'opération critique** des **composants redondants** qui **prendront le relais** du processus en cas de défaillance de l'un de ces points.

Mesures visant à améliorer la disponibilité

Redondance (Suite)

- La **redondance N+1** garantit la disponibilité du système en cas de défaillance d'un composant.
- Les composants (N) doivent comporter au moins un composant de secours (+1).
- C'est le cas, par exemple, d'une voiture à quatre roues (N) disposant d'une roue de secours dans le coffre en cas de crevaison (+1).

Mesures visant à améliorer la disponibilité

Redondance (Suite)

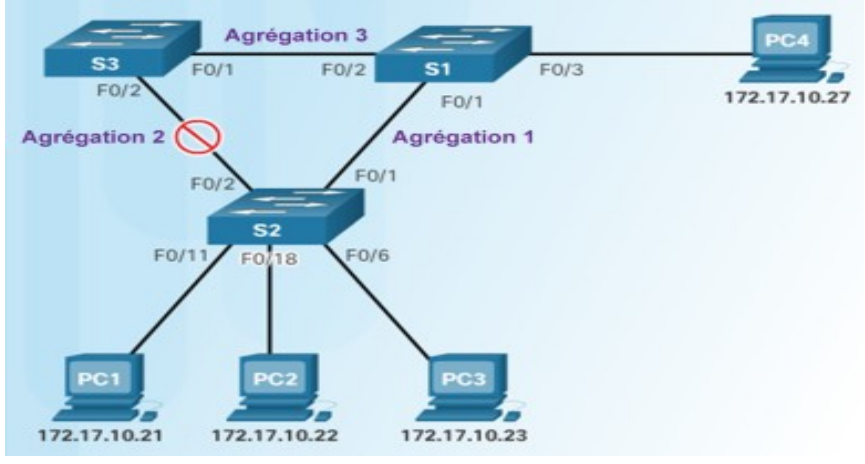
- Un **RAID (redundant array of independent disks)** combine plusieurs disques durs physiques en une seule unité logique pour assurer la redondance des données et améliorer les performances.
- Le système RAID prend les données normalement stockées sur un seul disque et les répartit sur plusieurs disques.
  - Si l'un des disques est défaillant, l'utilisateur peut récupérer les données à partir des autres disques sur lesquels elles résident également.
- Le système RAID permet également d'accélérer la récupération des données.
- L'utilisation de plusieurs disques accélère la récupération des données demandées.
- Plus besoin de se fier à un seul disque pour effectuer cette tâche.
- Une solution RAID peut reposer sur le matériel ou le logiciel.
- Les termes suivants expliquent comment le système RAID stocke les données sur les différents disques :
  - **Parité** : détecte les erreurs de données.
  - **Entrelacement :** écrit les données sur plusieurs disques.
  - **Mise en miroir :** duplique les données sur un second disque.

Mesures visant à améliorer la disponibilité

Redondance (Suite)

Spanning Tree est un protocole réseau qui assure la redondance :

- La fonction de base de STP est d'empêcher les boucles dans un réseau lorsque plusieurs chemins connectent les commutateurs entre eux.
- STP garantit que les liaisons physiques redondantes sont dépourvues de boucles.
- Il permet qu'il n'y ait qu'un seul chemin logique entre toutes les destinations du réseau.
- STP bloque intentionnellement les chemins d'accès redondants susceptibles d'engendrer une boucle.



Mesures visant à améliorer la disponibilité

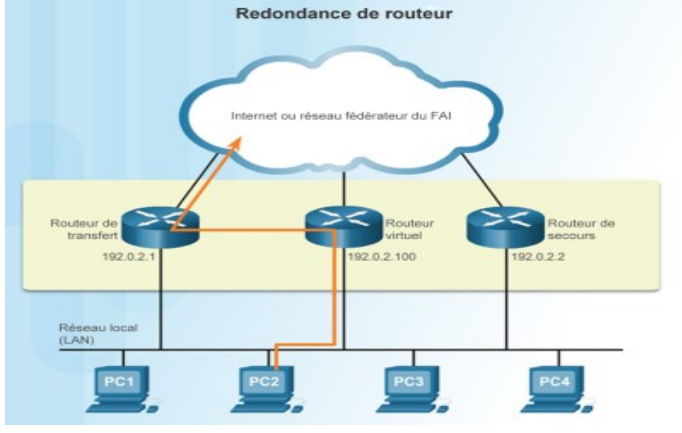
Redondance (Suite)

La passerelle par défaut est généralement le routeur, qui assure l'accès des appareils au reste du réseau ou à Internet.

Si un seul routeur sert de passerelle par défaut, il constitue un point de défaillance unique.

La redondance du routeur implique les éléments suivants :

- Le choix d'installer un routeur de secours supplémentaire.
- La capacité d'un réseau à effectuer une reprise dynamique après la défaillance d'un routeur jouant le rôle de passerelle par défaut est appelée « redondance au premier saut ».



Mesures visant à améliorer la disponibilité

Redondance (Suite)

Options de redondance du routeur : les options disponibles pour la redondance du routeur sont les suivantes :

- **Protocole HSRP (Hot Standby Router Protocol)** : HSRP assure la haute disponibilité du réseau en fournissant la redondance au premier saut du routeur.
- **Protocole VRRP (Virtual Router Redundancy Protocol)** : un routeur VRRP exécute le protocole VRRP en conjonction avec un ou plusieurs autres routeurs attachés au LAN.
  - Dans une configuration VRRP, le routeur choisi est le routeur virtuel principal, les autres routeurs servant de routeurs de secours en cas de défaillance de celui-ci.
- **Protocole GLBP (Gateway Load Balancing Protocol)** : GLBP protège le trafic de données en provenance d'un routeur ou d'un circuit défaillant, tel que HSRP et VRRP, tout en permettant un équilibrage de la charge (également appelé partage de charge) au sein d'un groupe de routeurs redondants.

Mesures visant à améliorer la disponibilité

Redondance (Suite)

Redondance de site : une entreprise peut être amenée à envisager la redondance de site en fonction de ses besoins.

Voici **trois formes** de **redondance** de **site** :

- **Synchrone :** synchronise les deux sites en temps réel et exige une bande passante élevée.
  - En outre, les sites doivent être proches pour réduire la latence.
- **Réplication asynchrone :** pas de synchronisation en temps réel mais presque, exige moins de bande passante et les sites peuvent être plus éloignés les uns des autres car la latence pose moins de problèmes.
- **Réplication ponctuelle :** met régulièrement à jour le site des données de sauvegarde.
  - Cette option est celle qui préserve le plus la bande passante car elle n'exige pas une connexion constante.

Mesures visant à améliorer la disponibilité

La résilience du système

La résilience définit les **méthodes** et les **configurations** utilisées pour qu'un système ou un réseau soit **résistant aux pannes**.

Les **protocoles de routage assurent** la **résilience**.

La **redondance ne suffit pas** pour parvenir à une **conception résiliente**.

La **résilience** est **critique** pour **comprendre** les **besoins** de l'entreprise, **puis incorporer** la **redondance** pour **créer** un **réseau résilient**.

5.3 Phases de gestion des incidents

Gestion des incidents

Phases de gestion des incidents

La **gestion** des **incidents** définit les **procédures suivies** par une entreprise **après** un **événement hors norme**.

Lorsqu'un incident se produit, l'entreprise **doit savoir comment y répondre**.

Les entreprises doivent **développer un plan de gestion des incidents** et **former une équipe CSIRT** (Computer Security Incident Response Team) pour prendre en charge cette gestion.

La gestion des incidents se déroule en **quatre phases** :

1. **Préparation :** planification des incidents potentiels
2. **Détection et analyse :** découverte de l'incident
3. **Maîtrise et éradication, puis restauration :** efforts pour maîtriser ou éradiquer la menace, puis efforts de restauration
4. **Suivi post-incident :** enquêter sur la cause de l'incident et poser des questions pour mieux comprendre la nature de la menace

Gestion des incidents

Technologies de gestion des incidents

Les **technologies** utilisées pour la **gestion** des **incidents** sont **nombreuses** :

- **Contrôle de l'accès au réseau (NAC) :** permet aux utilisateurs autorisés d'accéder au réseau avec des systèmes conformes.
  - Un système conforme satisfait à toutes les exigences de la politique de l'entreprise.
- **Systèmes de détection des intrusions (IDS) :** surveillent le trafic sur le réseau. Les systèmes IDS sont passifs.
- **Systèmes de prévention des intrusions :** fonctionne en mode en direct.
  - Il est capable de détecter et de remédier immédiatement aux problèmes du réseau.
- **Netflow et IPFIX :** NetFlow est une technologie Cisco IOS qui fournit des statistiques sur les paquets traversant un routeur ou un commutateur multicouche Cisco.
  - L'IETF (Internet Engineering Task Force) s'est appuyé sur NetFlow Version 9 de Cisco pour l'exportation des informations du flux IP (IP Flow Information Export - IPFIX).
- **Threat Intelligence avancée :** permet aux entreprises de détecter les attaques pendant l'une de leurs phases (et parfois avant, si les bonnes informations sont disponibles).

5.4 Reprise après sinistre

Reprise après sinistre

Planification de la reprise après sinistre

Types de sinistres : en cas de sinistre, une entreprise doit pouvoir continuer à fonctionner.

Les sinistres comprennent tous les événements naturels ou provoqués par l'homme qui endommagent les ressources ou les biens et nuisent à la capacité de l'entreprise de poursuivre son activité.

- **Catastrophes naturelles :** catastrophes **géologiques** (tremblements de terre, glissements de terrain, éruptions volcaniques et tsunamis), catastrophes **météorologiques** (ouragans, tornades, tempêtes de neige, foudre et grêle), catastrophes **sanitaires** (maladies contagieuses, quarantaines et pandémies) et catastrophes **diverses** (incendies, inondations, tempêtes solaires et avalanches).
- **Catastrophes provoquées par l'homme :** événements dans **l'environnement** de **travail** (grèves, abandons de poste et ralentissements), événements **socio-politiques** (vandalisme, blocages, protestations, sabotage, terrorisme et guerre), **événements matériels** (incendies et déversements dangereux) et perturbations des services publics (coupures d'électricité, pannes de communication, pénuries de carburant et retombées radioactives).

Reprise après sinistre

Planification de la continuité de l'activité

Importance de la continuité de l'activité : la continuité d'activité est l'un des concepts les plus importants de la sécurité informatique.

Même si les entreprises mettent tout en œuvre pour éviter les catastrophes et la perte de données, elles ne peuvent pas prévoir chaque scénario.

Pour les entreprises, il est essentiel de mettre en place des plans garantissant la continuité de l'activité, quels que soient les événements qui surviennent.

Considérations relatives à la continuité de l'activité : les contrôles de continuité d'activité ne se limitent pas à la sauvegarde de données et à la redondance des matériels. Les considérations relatives à la continuité de l'activité doivent inclure les éléments suivants :

- **Documenter** les configurations
- Mettre en place des **canaux** de **communications alternatifs**
- **Garantir l'approvisionnement** en **électricité**
- **Identifier** toutes les **dépendances** des **applications** et des **processus**
- **Apprendre comment gérer manuellement** les **tâches** automatisées

Reprise après sinistre

Planification de la continuité de l'activité

Bonnes pratiques en matière de continuité de l'activité

1. **Rédigez** une **politique** fournissant des **instructions** de développement du plan de **continuité de l'activité** et **répartissant** les **tâches** en fonction des **rôles**.
2. **Identifiez** les **systèmes** et **processus critiques**, et **hiérarchisez-les** en fonction des besoins.
3. **Identifiez** les **vulnérabilités** et les **menaces**, et **calculez** les **risques**.
4. **Identifiez** et **mettez** en **œuvre** des **contrôles** et des **contre-mesures** afin de **réduire** les **risques**.
5. **Élaborez** des **méthodes** pour **rétablir rapidement** les systèmes **stratégiques**.
6. **Rédigez** des **procédures** pour **assurer** le **bon fonctionnement** de l'entreprise même dans des **situations chaotiques**.
7. **Testez** le **plan**.
8. **Mettez** le **plan** à jour **régulièrement**.

5.5 Résumé de la cinquième partie

Résumé de la cinquième partie

Résumé

- Ce chapitre a commencé par exposer le concept des cinq neuf, un standard de haute disponibilité qui autorise 5,26 minutes de panne par an.
- Ce chapitre a abordé les approches diverses que les entreprises adoptent pour assurer la disponibilité des systèmes.
- Pour une conception de système fiable, il convient de prendre des mesures assurant la redondance et la résilience, afin de permettre à l'entreprise de se rétablir rapidement et de poursuivre son activité.
- Ce chapitre a également abordé la façon dont une entreprise doit répondre à un incident en établissant les procédures qu'elle doit suivre après un événement.
- Ce chapitre s'est terminé par une discussion sur la reprise sur sinistre et la planification de la continuité d'activité.