

Dossier de projet

Titre professionnel : **Administrateur d'infrastructure sécurisé.**

Nom : **Malet**

Prénom : **Raphaël**



En formation à La Plateforme_, 8 rue d'hozier 13002 Marseille

1. Introduction	4
1.1 Présentation personnelle :	4
1.2 Présentation personnelle en anglais :	5
1.3 résumé :	6
1.4 Présentation de l'entreprise :	7
1.5 présentation de l'équipe SI RER :	8
2. Mon rôle au sein du département RER /SI :	9
2.1 Présentation de mon poste et des missions :	9
3. Changement de politique cyber sur des machines industrielle :	11
3.1 Introduction / Présentation du projet	11
3.2 Installation des nouvelles machines :	12
Résumé de l'installation de la Baie ATESS sous Windows 10	12
3.3 Création d'un script powershell pour gérer les droits d'accès à notre machine :	14
3.3.1 Contexte :	14
3.3.2 Fonctionnement du script PowerShell	15
3.3.3 Variables initiales et préparation de l'environnement	15
3.3.4 Détection du type de compte utilisateur :	17
3.3.5 Contrôle du nombre de sessions ouvertes :	18
3.3.6 Vérification des droits d'accès via les groupes AD :	19
3.3.7 Connexion au serveur SYLEX :	20
3.3.8 Fonctionnement de notre programme :	21
3.4 Mise en place d'un outils de supervision pour ce parc de machine	23
3.4.1 Introduction à la supervision :	24
1. Qu'est-ce qu'un serveur de supervision ?	24
2. Pourquoi la supervision est-elle essentielle dans un environnement industriel ou critique ?	24
3. Pourquoi avoir choisi Zabbix ?	25
3.4.2 Architecture de Zabbix :	25
1. Serveur Zabbix	25
2. Base de données (MySQL)	26
3. Interface web (Apache/PHP)	26
4. Zabbix Agent (Windows/Linux)	26
3.4.3. Installation de zabbix serveur :	26
Présentation de l'environnement de travail	26
Type d'hyperviseur	27
Avantages du type 1 (bare metal) :	27
Contexte d'installation	27
Stack technique mise en place	27
Objectifs atteints	28
1. Téléchargement et transfert des fichiers sources d'installation :	28
2. Installation des dépendances :	28
3. Crédit de l'utilisateur système zabbix :	29
4. Installation et configuration de MySQL :	29

5. Création de notre base de données zabbix + configuration :	31
6. Chiffrement de notre base de données MySQL :	33
7. Configuration des sources pour la compilation de Zabbix	34
8. Installation du serveur HTTP (Apache) :	35
9. Installation de zabbix agent :	44
10. Configuration d'une règle pour surveiller le trafic réseau d'une machine	51
11. Vérifier que le serveur est correctement connecté à notre machine.	53
12. Surveiller le cache de notre service SFTP Drive :	54
13. Interface de supervision final :	56
14. réponse à incident, problème de transfert :	58
Étude de cas : incident du 4 au 10 décembre 2024	58
Symptômes observés :	58
Analyse et diagnostic :	59
Résolution et actions correctives	60
Mise en œuvre technique	61
4. Administration Sharepoint :	61
4.1 Structuration de l'environnement documentaire	61
4.2 Gestion des accès et administration des droits	62
4.3 Bonnes pratiques mises en œuvre	63
5. Mise en place d'un Plan de Continuité d'Activité (PCA) Plateforme SharePoint	64
5.1 Qu'est-ce qu'un PCA ?	64
5.2 Objectif du SharePoint "Ma Vie Sans le Digital"	64
6. Mise en œuvre d'une infrastructure réseau simulée (projet DIVOC)	68
Configuration du serveur DHCP	68
Mise en place du DNS	69
Filtrage du trafic sortant (proxy simulé)	70
VLAN VoIP et Data	70
Résultat final	71
6. Conclusion	72

1. Introduction

1.1 Présentation personnelle :

Je m'appelle Raphaël MALET, je suis actuellement en formation à La Plateforme_ à Marseille, une école du numérique et des nouvelles technologies fondée en 2019. Cette école se distingue par une pédagogie axée sur des projets concrets et une forte proximité avec le monde professionnel. J'y ai choisi de suivre le cursus "Administrateur des systèmes et des réseaux".

Passionné par l'informatique depuis mon plus jeune âge, j'ai suivi un parcours atypique qui m'a permis d'explorer différents secteurs professionnels. Ces expériences m'ont été précieuses, car elles m'ont permis d'identifier avec certitude ce que je souhaitais faire : travailler dans le domaine de l'informatique.

j'ai commencé ma formation à La Plateforme_ dans le tronc commun général. Cette première année m'a permis de découvrir plusieurs domaines de l'informatique, comme le développement web, le développement logiciel et l'administration systèmes et réseaux. C'est cette dernière spécialité qui m'a le plus captivé, car elle englobe une vision complète de l'écosystème informatique, allant du développement à l'infrastructure.

À l'issue de cette première année, j'ai choisi de me spécialiser en administration systèmes et réseaux. j'ai ensuite poursuivi mon cursus en alternance, en intégrant la RATP, au sein du pôle RER, en tant qu'assistant RSSI (Responsable de la Sécurité des Systèmes d'Information).

1.2 Présentation personnelle en anglais :

My name is Raphaël MALET, and I am currently studying at La Plateforme_ in Marseille, a digital and new technologies school founded in 2019. This school stands out for its project-based learning approach and strong connection with the professional world. I chose to follow the "System and Network Administrator" track.

Passionate about IT since a young age, I have had an atypical career path that allowed me to explore various professional sectors. These experiences have been valuable, as they helped me clearly identify what I wanted to do: work in the field of information technology.

I began my studies at La Plateforme_ with a general foundation year. During this first year, I explored several areas of IT, such as web development, software development, and system and network administration. It was this last field that captivated me the most, as it provides a comprehensive view of the IT ecosystem, from development to infrastructure.

At the end of this first year, I decided to specialize in system and network administration. I then continued my training through a work-study program by joining RATP, in the RER division, as an assistant to the Chief Information Security Officer (CISO).

1.3 résumé :

Durant mon alternance, j'ai eu l'opportunité d'occuper le poste d'assistant RSSI au sein de la RATP. Avec environ 71 000 collaborateurs répartis dans 15 pays sur 5 continents, la RATP est aujourd'hui le troisième opérateur mondial de transports urbains. En Île-de-France, elle exploite notamment le réseau de métro parisien, plusieurs lignes de tramway, une partie des lignes A et B du RER, ainsi qu'un vaste réseau de bus.

j'ai intégré le pôle RER/Systèmes d'Information, dont la mission est de piloter et de sécuriser les projets informatiques liés à l'exploitation du RER. Mon rôle consistait à contribuer à la bonne gestion et à la sécurisation des ressources numériques utilisées dans cette branche. Cela allait de la protection de machines industrielles à la gestion de données sensibles hébergées sur un espace SharePoint interne à la RATP, plus spécifiquement destiné au pôle RER.

Cette expérience m'a permis de comprendre la complexité et les exigences liées à la mise en œuvre de projets informatiques à grande échelle. j'ai notamment appris que la réussite d'un projet repose sur une préparation rigoureuse, un accompagnement structuré, et une phase de déploiement minutieusement planifiée.

1.4 Présentation de l'entreprise :

La RATP, un acteur de référence dans le secteur des transports urbains. Fondée en 1948 à Paris, la Régie Autonome des Transports Parisiens est aujourd'hui l'un des plus grands opérateurs de mobilité urbaine au monde.

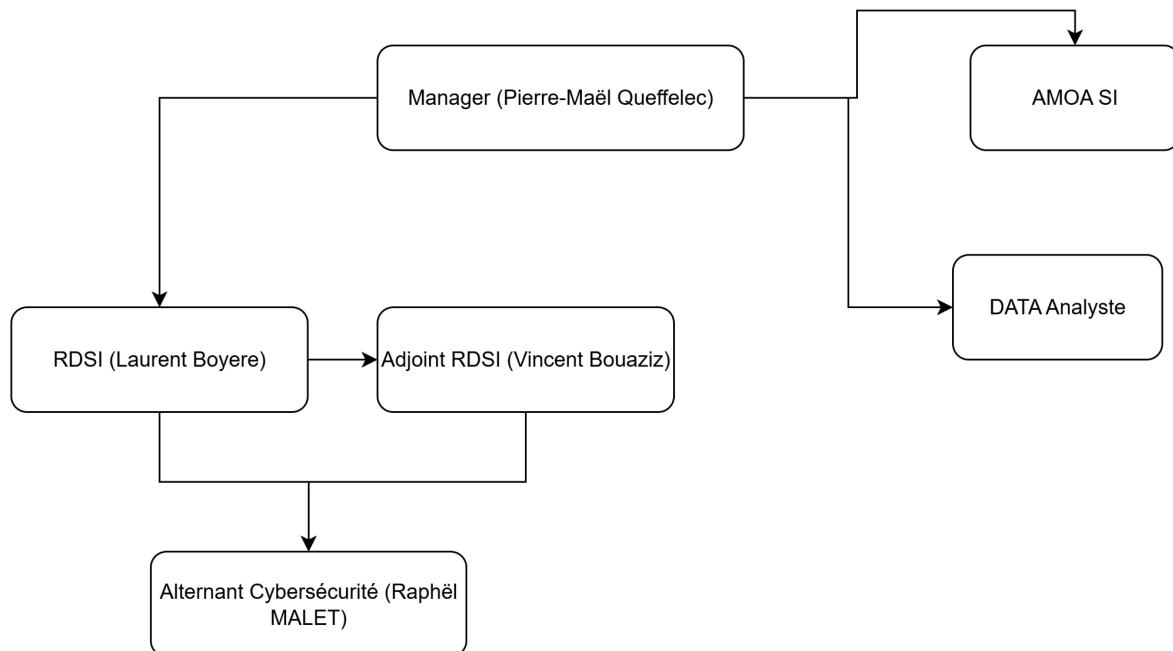
La RATP conçoit, exploite, modernise et entretient l'un des réseaux multimodaux les plus denses au monde, comprenant métro, RER, tramway et bus, principalement en Île-de-France. Elle joue un rôle clé dans la mobilité quotidienne de millions de voyageurs.

Présente dans 15 pays sur 5 continents, l'entreprise emploie environ 71 000 collaborateurs et opère à l'échelle mondiale via sa filiale RATP Dev. Elle transporte plus de 14 millions de personnes chaque jour et œuvre activement pour une mobilité plus durable, plus innovante et plus accessible.



1.5 présentation de l'équipe SI RER :

Au sein de la RATP, j'ai intégré l'équipe Systèmes d'Information (SI) du RER. Cette équipe est composée d'un Responsable des Systèmes d'Information (RSI), d'un Responsable de la Sécurité des Systèmes d'Information (RSSI), et est supervisée par une cheffe de projet, manager de l'équipe SI RER. Elle inclut également plusieurs AMOA (Assistants à la Maîtrise d'Ouvrage), chargés de veiller au bon déroulement des projets SI, en assurant le lien entre les besoins métiers et les solutions techniques mises en œuvre



2. Mon rôle au sein du département RER /SI :

2.1 Présentation de mon poste et des missions :

En tant qu'alternant administrateur systèmes et réseaux, j'étais placé sous la responsabilité du RDSI du département, Laurent Boyere, ainsi que de son assistant RSSI, Vincent Bouaziz. Au cours de mon alternance, plusieurs missions m'ont été confiées, mêlant sécurité, administration système, gestion documentaire et projet réseau :

1. Refonte de machines industrielles dans le cadre des JOP 2024

L'un des projets principaux qui m'a accompagné durant mes deux années d'alternance a été la refonte complète de machines industrielles critiques. Ce projet s'inscrivait dans une nouvelle politique de cybersécurité mise en place en vue des Jeux Olympiques et Paralympiques de Paris 2024.

j'ai pu intervenir techniquement à différentes étapes :

Mise en place de nouvelles machines

- Mise à jour des systèmes d'exploitation
- Déploiement d'une nouvelle politique d'authentification
- Installation d'un serveur de supervision dédié à ces équipements

2. Mise en place d'un plan de continuité d'activité (PCA) pour les JOP 2024

j'ai contribué à la création d'un PCA spécifique pour anticiper les risques liés aux événements critiques, comme une attaque cyber ou une panne majeure. Initialement pensé pour l'événement olympique, ce dispositif est aujourd'hui conservé comme solution pérenne.

3. Implémentation et administration de SharePoint

Dans le cadre d'une migration documentaire, j'ai participé à l'implémentation de nouveaux environnements SharePoint. Cela incluait :

- La structuration des espaces documentaires
- L'application de bonnes pratiques (droits, sécurité, arborescence)
- La proposition de solutions innovantes en lien avec les métiers pour renforcer l'usage, la gouvernance et la sécurité

4. Projet personnel : Mise en place d'une infrastructure réseau simulée

Bien que mon alternance n'ait pas inclus directement d'administration réseau, j'ai souhaité approfondir ces compétences à travers un projet personnel. j'ai conçu et configuré une maquette réseau d'entreprise à l'aide de Cisco Packet Tracer.

Ce projet incluait :

- Un plan d'adressage optimisé pour 13 utilisateurs et 10 appareils supplémentaires
- La mise en place de services essentiels : DHCP, DNS, proxy (via ACL)
- La configuration de VLAN pour isoler la voix (VOIP) et les données
- L'utilisation d'ACL pour simuler un filtrage réseau

Ce travail m'a permis de pratiquer l'administration réseau dans un contexte concret et structuré.

En tant qu'alternant au sein de la RATP, j'ai eu l'opportunité de participer à plusieurs projets liés à l'administration des systèmes et réseaux, avec un fort accent sur la cybersécurité. j'ai contribué à la refonte et à la sécurisation de machines industrielles, à la mise en place d'un plan de continuité d'activité (PCA) pour les JOP 2024, à l'administration documentaire via SharePoint, et à un projet personnel réseau structurant.

Mon rôle m'a amené à collaborer avec différents acteurs internes et externes, à proposer des solutions techniques adaptées, et à garantir la conformité des infrastructures aux nouvelles exigences en matière de cybersécurité.

3. Changement de politique cyber sur des machines industrielles :

3.1 Introduction / Présentation du projet

Comme mentionné précédemment, le projet qui m'a occupé le plus durant mon alternance concerne le changement de politique de cybersécurité sur des machines industrielles.

Problématique :

Le protocole de connexion aux machines ne respectait plus les normes de cybersécurité en vigueur au sein de l'entreprise. Il était donc nécessaire de revoir entièrement le mode d'authentification des utilisateurs pour garantir la conformité et la sécurité des données traitées.

Contexte :

Les machines concernées permettent de vider les « boîtes noires » des RER. Ces données sont d'une importance cruciale, que ce soit en cas d'incident, pour la reconstitution de trajets en cas d'infraction, ou encore pour la création et l'optimisation de l'offre de transport.

Une fois extraites, ces données sont transférées vers un serveur dédié pour traitement. Cependant, dans leur état initial, l'accès à ces machines s'effectuait via des comptes locaux. Chaque site disposait de ses propres identifiants, souvent peu sécurisés (mots de passe faibles, partagés, et parfois notés sur des feuilles accessibles dans les locaux). Cela représentait un risque majeur en matière de cybersécurité.

Objectif du projet :

L'objectif principal était de permettre aux utilisateurs autorisés de se connecter à ces machines à l'aide de leur compte nominatif (compte matricule rattaché à l'Active Directory de l'entreprise).

Pour cela, plusieurs actions ont été nécessaires :

- Remplacement des anciennes machines : les systèmes d'exploitation en place étaient obsolètes et ne permettaient pas une intégration dans l'Active Directory (AD).
- Enrôlement dans le domaine : les nouvelles machines ont été configurées pour être intégrées à l'AD, afin de centraliser la gestion des comptes et des droits d'accès.
- Mise en œuvre d'une politique de gestion des accès : seules les personnes autorisées peuvent se connecter aux machines/
- Déploiement d'une supervision : un outil de supervision a été installé pour assurer un suivi des événements et détecter tout incident ou comportement anormal sur les machines.

3.2 Installation des nouvelles machines :

Résumé de l'installation de la Baie ATESS sous Windows 10

L'installation de la nouvelle Baie ATESS s'inscrit dans un projet de mise en conformité des équipements industriels avec les politiques de cybersécurité de l'entreprise. Ce processus visait à remplacer les anciennes machines, souvent obsolètes ou non intégrables à l'Active Directory, par des postes modernes sous Windows 10, capables de s'intégrer dans l'environnement informatique sécurisé de la RATP.

La phase préparatoire a consisté à recueillir l'ensemble des informations nécessaires au déploiement : identification du site, nom de machine, configuration réseau (IP, DNS, passerelle), liste des utilisateurs locaux à recréer, ainsi que les droits et groupes associés. Une attention particulière a été portée à la sauvegarde des données de l'ancienne machine, afin d'assurer la continuité de service après bascule.

L'installation a commencé par la configuration de base du système : changement du nom de l'ordinateur pour reprendre celui de l'ancienne baie, création des comptes utilisateurs avec des droits différenciés (administrateur ou standard), et mise en place des groupes de sécurité locaux. Une fois les nouveaux comptes testés et validés, le compte administrateur natif a été désactivé pour renforcer la sécurité du poste.

Sur le plan réseau, la machine a été configurée en IP fixe lorsque cela était nécessaire, avec en complément les paramètres DNS et WINS adaptés au réseau interne. Les règles du pare-feu Windows ont été modifiées pour autoriser certaines communications, notamment le ping (ICMPv4) pour des raisons de supervision, ainsi que le bureau à distance, permettant une prise de main à distance si besoin. Un effort particulier a été fourni pour que ces opérations soient reproductibles sur d'autres machines.

L'intégration au domaine Active Directory a constitué une étape majeure du projet. Elle a permis aux utilisateurs de se connecter avec leur compte matricule, en supprimant le recours aux comptes locaux faiblement protégés. Des groupes AD spécifiques ont été ajoutés aux groupes locaux de la machine afin de contrôler les droits d'accès à l'application ATESS : administrateurs, formateurs, opérateurs. Cette granularité a facilité la délégation des rôles tout en conservant une traçabilité des actions.

Plusieurs outils ont ensuite été installés pour garantir le bon fonctionnement du système. L'application SFTP Drive 2022 a été déployée pour assurer la connexion au serveur SYLEX. Elle permet de monter un lecteur réseau sécurisé (lettre X:) utilisé pour le transfert automatisé des fichiers. L'installation a nécessité la configuration du service au démarrage, l'enregistrement de la licence, la définition du dossier cible, ainsi que la gestion des logs. PowerChute, un logiciel de gestion des coupures électriques, a également été installé et paramétré pour permettre un arrêt propre du système en cas de perte d'alimentation.

Le lecteur ATESS, application centrale pour le traitement des données des cassettes, a été configuré pour se lancer automatiquement à chaque ouverture de session. Des tests ont permis de vérifier que les utilisateurs affectés aux bons groupes AD accédaient bien à leurs fonctionnalités selon leur profil.

Enfin, un script PowerShell personnalisé a été développé et intégré à la stratégie locale de la machine pour s'exécuter à chaque ouverture de session. Ce script permet de contrôler dynamiquement les droits des utilisateurs et de bloquer l'accès en cas de non-conformité. De plus, un redémarrage quotidien a été planifié via le Planificateur de tâches de Windows afin de garantir la stabilité du poste dans le temps, avec un fichier XML importé standardisant le comportement.

Cette procédure, bien que très détaillée techniquement, reflète la volonté de standardiser, sécuriser et documenter le processus d'installation des baies ATESS dans un environnement de production critique. L'ensemble des étapes, tests et

vérifications ont été réalisés avec l'objectif de fiabiliser le dispositif dans un contexte à haute sensibilité opérationnelle.

3.3 Création d'un script PowerShell pour gérer les droits d'accès à notre machine :

Dans le cadre de ce projet, une des missions qui m'a été confiée consistait à mettre en place un mécanisme de gestion des accès sur les machines ATESS. Étant donné qu'il s'agit de postes dédiés à une tâche critique, à savoir le vidage des boîtes noires des RER, il est impératif que seuls les agents dûment formés et habilités puissent y accéder.

Pour répondre à cette exigence, j'ai conçu et développé un script PowerShell permettant de contrôler dynamiquement les droits des utilisateurs lors de leur connexion. Ce script s'exécute automatiquement à l'ouverture de session et vérifie si l'utilisateur appartient bien à un groupe Active Directory autorisé. En cas de non-conformité, l'accès est immédiatement restreint, empêchant toute utilisation non autorisée de la machine.

3.3.1 Contexte :

Les machines ATESS sont déployées sur les lignes A et B du RER pour permettre le vidage des boîtes noires des trains. Ce processus est critique, car les données collectées sont utilisées à des fins de traçabilité, de contrôle ou encore d'analyse en cas d'incident. Afin de renforcer la sécurité de ces postes, j'ai développé un script PowerShell personnalisé, exécuté à l'ouverture de session, pour garantir que :

- seuls les utilisateurs habilités puissent accéder à la machine
- aucun conflit ne survienne en cas de sessions multiples
- la connexion au serveur SYLEX soit bien établie avant le démarrage de l'application critique
- des interfaces compréhensibles soient affichées aux utilisateurs (non techniques)

3.3.2 Fonctionnement du script PowerShell

Le script repose sur une architecture modulaire : chaque étape ou contrôle est isolée dans une fonction distincte. Voici une description structurée fidèle au code source.

3.3.3 Variables initiales et préparation de l'environnement

Avant d'aborder les fonctions, plusieurs variables sont définies pour préparer l'environnement graphique et le comportement du script :

Définition de la fenêtre de dialogue

```
# Fonction qui nous permet de faire appelle à l'outil de fenêtre de dialogue sous powershell.
@('System.Drawing', 'System.Windows.Forms') |ForEach-Object { [reflection.Assembly]::LoadWithPartialName($_) | Out-Null }
[System.Windows.Forms.Application]::EnableVisualStyles() | Out-Null
# Définition des propriétés de notre fenêtre de dialogue.
$form = New-Object System.Windows.Forms.Form -Property @{
    WindowState      = 'Maximized'          # Avoir la fenêtre de dialogue en fullscreen
    MaximizeBox       = $false              # Doit être mis sur "True" pour que la fenêtre puisse être agrandie et réduite.
    KeyPreview        = $true               # Permet au formulaire de recevoir des événements de touche avant qu'ils ne soient envoyés aux contrôles enfant.
    TopMost           = $true               # Met en haut cette fenêtre au premier plan
    ControlBox        = $false              # Permet de ne pas avoir les boutons de contrôle
    FormBorderStyle   = 'None'              # Remplacer 1 par 'None' pour ne pas avoir les boutons pour fermer ou réduire la fenêtre.
    Name              = "check baie ATTESS"  # Nom de notre fenêtre de dialogue
    StartPosition     = 1                  # Détermine la position de notre fenêtre de dialogue
    BackColor         = [System.Drawing.Color]::FromArgb(255, 240, 240, 240)
}
$form.DataBindings.DefaultDataSourceUpdateMode = 0
$timer = New-Object System.Windows.Forms.Timer -Property @{Interval = 1000}
$script:ptnum = 0
# Permet l'update de la fenêtre de dialogue.
# Fonction qui permet de définir le tick de notre timer en ms.
```

Dans cette section, nous initialisons l'outil PowerShell permettant d'afficher une fenêtre de dialogue destinée aux utilisateurs. Plusieurs paramètres sont définis :

- Mise en plein écran de la fenêtre.
- Blocage de la redimension de la fenêtre par l'utilisateur.
- Suppression des boutons classiques (fermer, réduire).
- Affichage en mode "premier plan", afin qu'aucune autre application ne passe par-dessus.
- Initialisation d'un minuteur (**Timer**) qui sera utilisé plus tard dans le script.

Définition des éléments de l'interface utilisateur

```
#definition de la largeur de notre ecran
$tailleX = [System.Windows.Forms.Screen]::PrimaryScreen.Bounds.Width
$tailleY = [System.Windows.Forms.Screen]::PrimaryScreen.Bounds.Height

#definition de nos position et largeur de notre zone de texte par rapport a la taille de notre ecran
$PositionXTexte= [Math]::round($tailleX/4)
$PositionYTexte = [Math]::round($tailleY/3)
$largeurZoneTexte = [Math]::round($tailleX/2)

# definition de nos position par rapport a la taille de notre ecran pour nos boutonContinuer
$PositionXBoutonContinuer = [Math]::round($tailleX/2 - 75)
$PositionYBoutonContinuer = [Math]::round($tailleY/2)

# defintion de la position de notre bouton Quitter
$PositionXBoutonQuitter = [Math]::round($tailleX/2 + $tailleX/10)
$PositionYBoutonQuitter = [Math]::round($tailleY/2)

# definition de la position de notre bouton Reboot
$PositionXBoutonReboot = [Math]::round($tailleX/2 - $tailleX/10)
$PositionYBoutonReboot = [Math]::round($tailleY/2)

#definition de notre Zone de TEXTE
|$ZoneTexte = New-Object System.Windows.Forms.Label -Property @{
    Location = "$PositionXTexte,$PositionYTexte"
    Width   = $largeurZoneTexte
    Height  = 100
    TextAlign = 'MiddleCenter'
    Font = New-Object System.Drawing.Font("Arial", 15, [System.Drawing.FontStyle]::Regular)
}

#Définition de notre bouton continuiez
|$BoutonContinuer = New-Object System.Windows.Forms.Button -Property @{
    Location = "$PositionXBoutonContinuer,$PositionYBoutoncontinuer"
    Text     = "Continuez"
}

|$BoutonQuitter = New-Object System.Windows.Forms.Button -Property @{
    Location = "$PositionXBoutonQuitter,$PositionYBoutonQuitter"
    Text     = 'Déconnexion'
}

|$BoutonReboot = New-Object System.Windows.Forms.Button -Property @{
    Location = "$PositionXBoutonReboot,$PositionYBoutonReboot"
    Text     = "Redémarrer"
}

|$BoutonContinuerSylex = New-Object System.Windows.Forms.Button -Property @{
    Location = "$PositionXBoutonContinuer,$PositionYBoutoncontinuer"
    Text     = "Continuez"
}
```

Nous définissons ici la taille, la position et les différents éléments présents dans notre fenêtre (zone de texte, boutons, etc.).

Comme ce script est destiné à être déployé sur plusieurs machines avec des résolutions d'écran différentes, j'ai fait le choix de calculer dynamiquement la position des éléments en fonction de la taille de l'écran. Cela garantit un rendu correct, quelle que soit la configuration matérielle.

Par exemple :

- La zone de texte s'affiche toujours au centre de l'écran.
- Les boutons sont également positionnés proportionnellement (et non en coordonnées absolues), pour éviter les débordements ou les écrasements.

Ce choix permet de rendre l'interface graphique du script plus souple, adaptable, et donc plus robuste.

Récupération du matricule utilisateur connectés

```
#permet d'obtenir le matricule de l'utilisateur connecté
$UtilisateurConnecte = whoami
$MatriculeUtilisateur = $UtilisateurConnecte.Split("\")[1]
```

Nous devons identifier précisément l'utilisateur connectés afin de déterminer ses droits.

- Pour cela, nous utilisons la commande whoami, qui renvoie une chaîne du type :
RATP\RM764520 (compte Active Directory) ou ATESS\UTILUT (compte local).
- Ce résultat est ensuite découpé afin de ne conserver que la partie utile : le nom de l'utilisateur.
Dans notre exemple, seule la valeur **RM764520** sera conservée dans la variable **\$MatriculeUtilisateur**.

Définition de l'emplacement de notre programme à exécuter :

```
#Chemin de l'application que l'on doit lancer
$CheminApplication = "C:\Lecteur_6.00.06_FR\lecteur.exe" #C:\Program Files\Mozilla Firefox\firefox.exe"
```

Enfin, nous définissons le chemin absolu du programme principal que la machine devra exécuter automatiquement après la validation de l'utilisateur.

Ce programme est essentiel au fonctionnement de la baie ATESS, car c'est lui qui permet de lire et de transférer les données des boîtes noires.

3.3.4 Détection du type de compte utilisateur :

Fonction : Utilisateur_Local_AD :

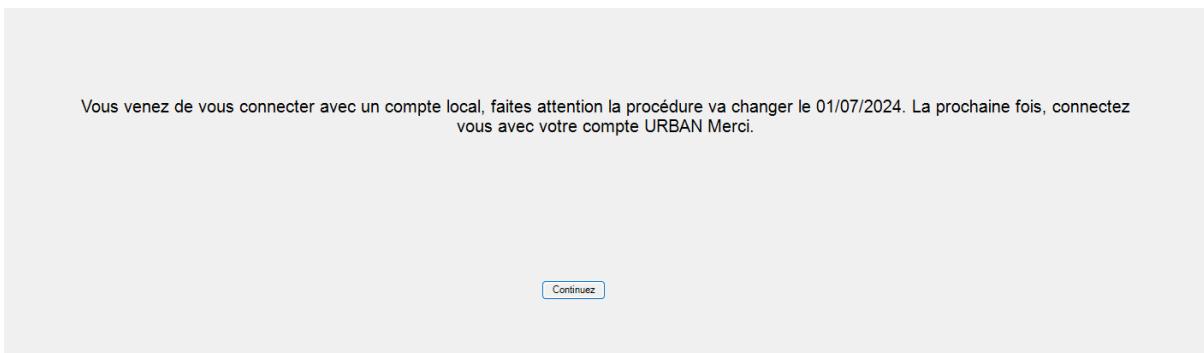
Cette fonction identifie si l'utilisateur est connectés avec un compte Active Directory (matricule RATP) ou un compte local propre à la machine.

```
function Utilisateur_Local_AD {
    if ($UtilisateurConnecte -like "ratp*") {
        #condition qui permet de savoir si un user est un user de l'AD.
        Return 1
    }
    if ($UtilisateurConnecte -like "ATESS*") {
        # Connexion avec un utilisateur local
        Return 0
    }
}
```

Fonction : AvertissementCompteLocal :

Cette fonction permet d'afficher un message d'avertissement si un utilisateur utilise encore un compte local :

```
# Fonction qui permet de prévenir l'utilisateur local que les procédures vont changer
function AvertissementCompteLocal {
    #Définition de notre Texte dans notre zone de texte
    $ZoneTexte.Text = "Vous venez de vous connecter avec un compte local, faites attention
                      la procédure va changer le 01/07/2024. La prochaine fois,
                      connectez vous avec votre compte URBAN Merci."
    $BoutonContinuer.Add_Click({
        $form.Controls.Remove($BoutonContinuer)
        $form.Close()
        Return
    })
    $form.Controls.AddRange(@($ZoneTexte, $BoutonContinuer))
    $form.ShowDialog()
}
```



3.3.5 Contrôle du nombre de sessions ouvertes :

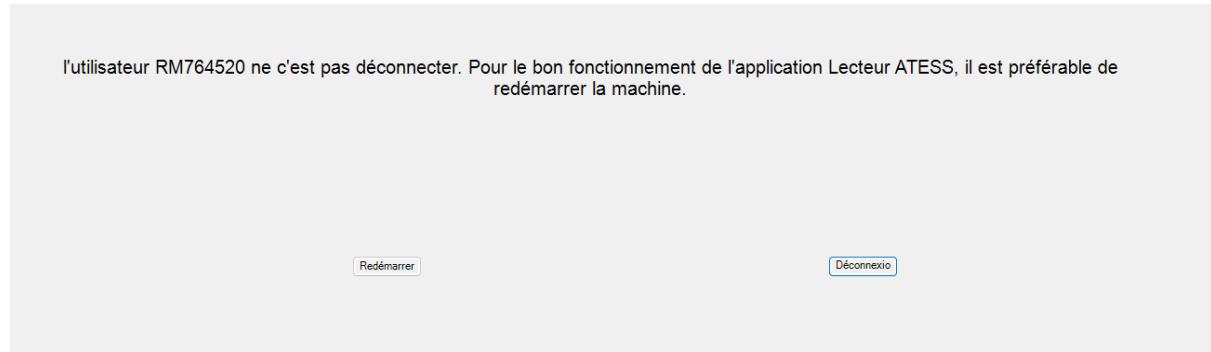
Fonction : CheckNombreUtilisateur :

Cette fonction vérifie qu'un seul utilisateur est connectés à la machine. Si ce n'est pas le cas, l'utilisateur actif est invité à choisir entre redémarrer la machine ou continuer malgré le risque de dysfonctionnement de l'application ATESS.

```

#Fonction qui permet de voir si plusieurs utilisateurs connecte a la machine
function CheckNombreUtilisateur {
    # Nous permet d'avoir tous les utilisateurs connecte a la machine.
    $NbUtilisateur = quser
    if ($NbUtilisateur.count -ne 2) {
        #Condition qui verifie si il y a plus de 2 utilisateurs connecte a la machine
        foreach ($Utilisateur in $NbUtilisateur) {
            #Nous permet de recuperer uniquement le matricule ou nom de l'utilisateur connecte
            $NomUtilisateur = $Utilisateur.Split(">")
            $UtilisateurFinal = $NomUtilisateur.Split(" ")[1]
            if ($UtilisateurFinal -eq $MatriculeUtilisateur) {
                # confirmation qui verifie si c'est l'utilisateur connecte
            }
            if ($UtilisateurFinal -eq "UTILISATEUR") {
                # Correspond a la ligne UTILISATEUR
            }
            else {
                #Ne correspond pas a l'utilisateur connecte donc c'est le matricule de la personne qui ne c'est pas connecte.
                $UtilisateurNonDeconnecte = $UtilisateurFinal
                break
            }
        }
        #definition de notre bouton pour quitter et lancer l'application lecteur ATESS
        $ButtonQuitter.Add_Click({
            logoff
        })
        # Definition de notre Bouton pour reboot la baie ATESS
        $ButtonReboot.Add_Click({
            shutdown /r /t 10 /c "La machine va redémarrer dans 10 secondes veuillez patienter."
        })
        #Definition de notre texte dans notre zone de texte.
        $ZoneTexte.Text = "l'utilisateur $UtilisateurNonDeconnecte ne c'est pas déconnecter.  
Pour le bon fonctionnement de l'application Lecteur ATESS,  
il est préférable de redémarrer la machine."
        $form.Controls.AddRange(@($ZoneTexte, $ButtonQuitter, $ButtonReboot))
        $form.ShowDialog()
    }
    else {
        #On lance la fenetre et donc le timer pour attendre la connexion au serveur Sylex.
        Return
    }
}

```



3.3.6 Vérification des droits d'accès via les groupes AD :

Fonction : GroupeUtilisateurAD :

Cette fonction contrôle que l'utilisateur appartient bien à l'un des groupes autorisés à utiliser la machine (administrateurs, formateurs ou opérateurs ATESS). Si ce n'est pas le cas, sa session est immédiatement fermée.

```

function GroupeUtilisateurAD {
    # Variable pour prendre les groupes de securite de notre utilisateur
    $Groupesutilisateur = Get-ADUser -Identity $Matriculeutilisateur -Properties memberof | select-object memberof -ExpandProperty memberof
    # Condition pour voir si l'utilisateur est dans le groupe Admin de la machine, si oui, on quitte le script
    foreach ($Groupe in $Groupesutilisateur) {
        $SIDGroupe = Get-ADGroup $Groupe
        if ($SIDGroupe.SID -like "$$SIDAdmin") {
            Exit
        }
    }
    # Condition pour voir si notre utilisateur fait partie des groupes de securite autorise a utiliser la machine
    foreach ($Groupe in $Groupesutilisateur) {
        $SIDGroupe = Get-ADGroup $Groupe
        if (($SIDGroupe.SID -like "$$AdminBandeurs") -or ($SIDGroupe.SID -like "$$FormateurBandeurs") -or ($SIDGroupe.SID -like "$$OperateurBandeurs")) {
            return
        }
    }
    logoff
}

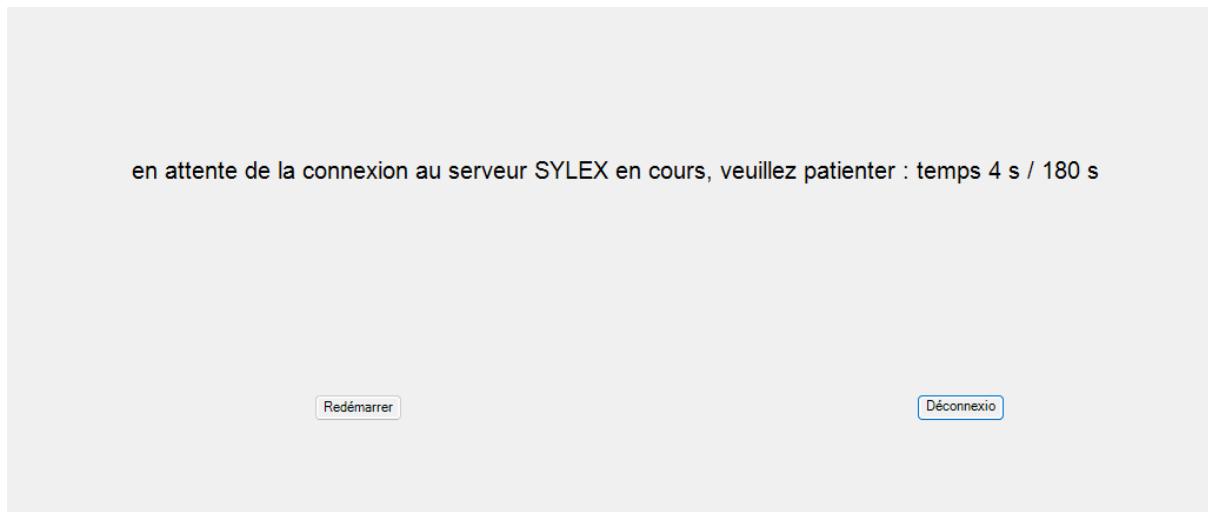
```

3.3.7 Connexion au serveur SYLEX :

Fonction : ConnexionServeurSylex :

Cette fonction tente de monter le disque réseau X: (serveur SFTP SYLEX). En cas d'échec, elle attend jusqu'à 3 minutes avant d'afficher un message d'alerte à l'utilisateur.

```
#Fonction pour la connexion au serveur SYLEX
Function ConnexionServeurSylex {
    $BoutonContinuerSylex.Visible = $False #permet de ne pas afficher notre bouton tant qu'on en a pas besoin
    #on essaie dans un premier temps de se rendre sur le serveur.
    Try {
        Set-Location X: -ErrorAction Stop
        $form.Close()
        Return
    }
    # Si impossible alors on lance notre time de 3 minute
    catch {
        $timer.Start() # on démarre notre time
        $timer.add_Tick({ #permet d'effectuer une action entre chaque tick de notre serveur.
            try {
                # si Connexion au serveur, on stop le timer et on ajoute un bouton pour lancer l'application lecteur ATESS
                Set-Location X: -ErrorAction Stop
                $BoutonContinuerSylex.Add_Click({
                    #lance l'application
                    $form.Close()
                    Return
                })
                $ZoneTexte.Text = "Connexion au serveur SYLEX réussie, vous pouvez vider vos cassettes"
                $BoutonContinuerSylex.Visible = $True
                $timer.Stop()
            }
            catch {
                #Si le serveur n'est pas directement connecté, on commence notre timer.
                $script:timertimer = $script:num -lt $TempsLimiteTimer
                if ($script:timertimer) {
                    #Le temps de notre timer, si inférieur alors on actualise toutes les secondes notre fenêtre de dialogue avec le timer.
                    $ZoneTexte.Text = "en attente de la connexion au serveur SYLEX
en cours, veuillez patienter : temps $script:num s / $TempsLimiteTimer s "
                }
                else {
                    # Si impossible de se connecter au serveur Sylex, message + Bouton pour lancer dans tous les cas l'application même si aucune connexion au serveur.
                    $ZoneTexte.Text = "La connexion au serveur SYLEX a échouée.
Lors du transfert des fichiers vers le serveur SYLEX n'aura pas
lieu après le déchargement des Cassettes. Prenez contact avec votre responsable
hierarchique qui prendra contact avec nous."
                    $BoutonContinuerSylex.Add_Click({
                        $form.Close()
                        Return
                    })
                    $BoutonContinuerSylex.Visible = $True
                    $timer.Stop()
                }
            }
        })
        # Fonction qui nous permet d'enlever la combinaison de touche ALT + F4
        $form.Add_KeyDown({
            param($sender, $e)
            if ($e.Alt -and $e.KeyCode -eq 'F4') {
                $e.Handled = $True
            }
        })
        $form.Controls.AddRange(@($ZoneTexte, $BoutonContinuerSylex))
        $form.ShowDialog()
        $timer.Stop()
    }
}
```



La connexion au serveur SYLEX a échouée. Le transfert des fichiers vers le serveur SYLEX n'aura pas lieu après le déchargement des Cassettes. Prenez contact avec votre responsable hiérarchique qui prendra contact avec nous.

Redémarrer

Continuer

Déconnexion

3.3.8 Fonctionnement de notre programme :

Fonction : Main :

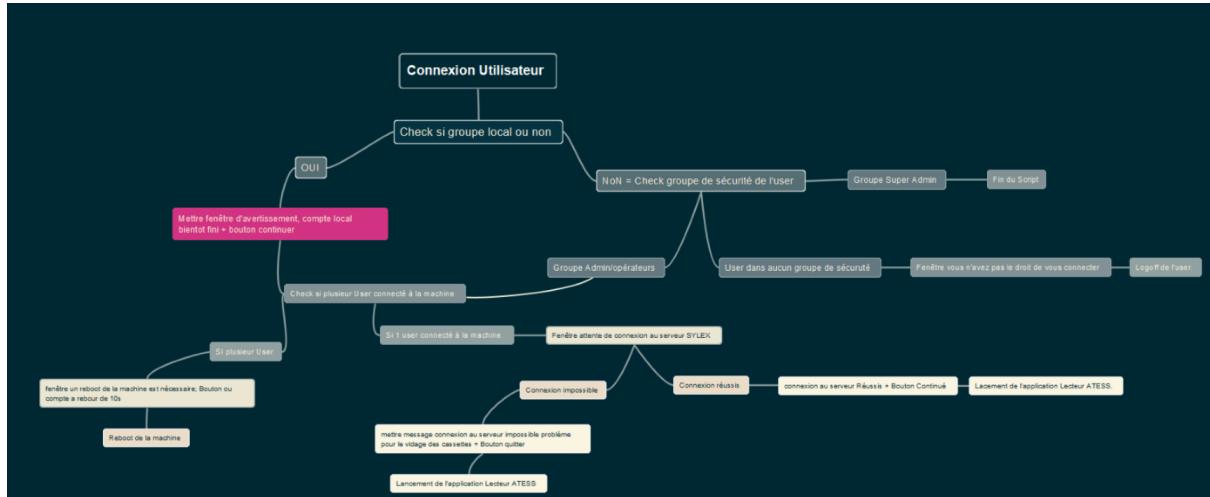
```
function Main {
    # on regarde dans un premier temps la disponibilité de notre module AD
    $DisponibiliteModule = CheckModule
    # Si notre fonction CheckModule retourne 0 alors c'est un fonctionnement nominal
    if ($DisponibiliteModule -eq 0){
        $Utilisateur_Ad_Local = Utilisateur_Local_AD
        if ($Utilisateur_Ad_Local -eq 0) {
            AvertissementCompteLocal
        }
        else {
            # Variable qui aura comme valeur le return de notre fonction Ligne, soit A ou B
            $Infoligne = Ligne
            if ($Infoligne -eq 'A'){
                # Notre fonction Ligne return B donc on se trouve sur la ligne B
                # on met les groupes de s@curit@ de la ligne B
                $SIAdmin = "S-1-5-21-1999524357-323959633-329593862-201540" # 039 RER-SI Admin
                $AdminBandeurs = "S-1-5-21-1999524357-323959633-329593862-542177" # 039 RER-A-Administrateurs-Bandeurs
                $FormateurBandeurs = "S-1-5-21-1999524357-323959633-329593862-542165" # 039 RER-A-Formateurs-Bandeurs
                $OperateurBandeurs = "S-1-5-21-1999524357-323959633-329593862-542164" # 039 RER-A-Operateurs-Bandeurs
            }
            else { # La fonction Ligne return A, cela veut dire qu'on se trouve sur la ligne A
                # on met les groupes de s@curit@ de la ligne A.
                $SIAdmin = "S-1-5-21-1999524357-323959633-329593862-201540" # 039 RER-SI Admin
                $AdminBandeurs = "S-1-5-21-1999524357-323959633-329593862-564156" # 039 RER-B-Administrateurs-Bandeurs
                $FormateurBandeurs = "S-1-5-21-1999524357-323959633-329593862-564157" # 039 RER-B-Formateurs-Bandeurs
                $OperateurBandeurs = "S-1-5-21-1999524357-323959633-329593862-564158" # 039 RER-B-Operateurs-Bandeurs
            }
            GroupeUtilisateurAD
        }
        CheckNombreUtilisateur
        ConnexionServeurSylex
        LancementApplication
        Exit
    }
    # Si notre fonction CheckModule retourne 1, alors il manque notre module AD
    else {
        $Utilisateur_Ad_Local = Utilisateur_Local_AD
        # condition pour avertir notre utilisateur si il se connecte avec un compte local
        if ($Utilisateur_Ad_Local -eq 0) {
            AvertissementCompteLocal
        }
        # on lance les autre application, on ne peut pas regarder si notre utilisateur peut utiliser la machine
        # donc on lance un fonctionnement dégradé, qui lance l'application pour tous les utilisateurs.
        # Si l'utilisateur n'est pas dans un groupe de sécurité qui peut utiliser l'application, alors elle ne se lancera pas
        # et la session se fermera automatiquement.
        CheckNombreUtilisateur
        ConnexionServeurSylex
        LancementApplicationModuleNonPresent
        Exit
    }
}
```

Cette fonction est le cœur du script. Elle orchestre toute la logique métier :

- Elle détecte si l'utilisateur est local ou membre de l'Active Directory.
- Elle détermine la ligne (A ou B) selon le nom de la machine, ce qui ajuste dynamiquement les groupes autorisés.
- Elle vérifie l'appartenance à ces groupes via **GroupeUtilisateurAD**.
- Elle gère les utilisateurs déjà connectés avec CheckNombreUtilisateur.
- Elle teste la connexion au serveur SYLEX avec gestion du temps d'attente.
- Si toutes les conditions sont réunies, l'application ATESS est lancée.

Les autres fonctions appelées seront détaillées dans les prochaines sections.

Voici un diagramme qui permet d'expliquer et de visualiser le fonctionnement du script pour la connexion au baie ATESS :



3.4 Mise en place d'un outils de supervision pour ce parc de machine

Dans le cadre de la sécurisation et de la fiabilité des systèmes industriels utilisés au sein du département RER de la RATP, il était indispensable de mettre en place une solution de supervision centralisée. L'objectif principal était de garantir un suivi en temps réel de l'état des machines critiques, notamment celles utilisées pour le déchargement des données des boîtes noires (baies ATESS), tout en assurant une capacité de réaction rapide en cas d'incident.

Pour répondre à ce besoin, j'ai installé et configuré un serveur de supervision basé sur Zabbix, une solution libre, robuste et extensible, particulièrement adaptée aux environnements mixtes (Linux / Windows) et aux contextes industriels.

Ce serveur a été déployé dans un environnement sans accès Internet, ce qui a nécessité une installation entièrement à partir des sources, ainsi qu'une configuration manuelle de l'ensemble des composants nécessaires : base de données, serveur web, agents clients, modules de sécurité et outils de visualisation.

Cette section détaille toutes les étapes de la mise en œuvre :

- l'installation de Zabbix et de ses dépendances (MySQL, Apache, PHP),
- la configuration de la supervision des postes industriels,
- la mise en place d'un chiffrement des données,
- la sécurisation de l'interface web (SSL),
- ainsi que le déploiement de scripts personnalisés pour le monitoring avancé des machines clientes.

L'ensemble de cette infrastructure vise à fournir une vision claire, centralisée et sécurisée de l'état des systèmes critiques, tout en respectant les contraintes spécifiques du réseau interne de la RATP.

3.4.1 Introduction à la supervision :

1. Qu'est-ce qu'un serveur de supervision ?

Un serveur de supervision est un système centralisé chargé de surveiller en temps réel l'état de santé, les performances et la disponibilité des équipements informatiques, réseaux ou industriels. Il collecte en continu des données provenant de différentes sources (machines, services, équipements réseau, etc.), les analyse, et génère des alertes en cas d'anomalies ou de dépassement de seuils définis.

La supervision permet ainsi :

- d'anticiper les pannes,
- de réagir rapidement en cas d'incident,
- et d'optimiser la disponibilité et les performances des systèmes supervisés.

2. Pourquoi la supervision est-elle essentielle dans un environnement industriel ou critique ?

Dans un environnement industriel tel que celui de la RATP, certaines machines jouent un rôle stratégique. C'est notamment le cas des baies ATESS, utilisées pour le déchargement des données des boîtes noires des RER. Si l'une de ces machines devient indisponible ou défaillante, cela peut compromettre la traçabilité des événements ferroviaires ou retarder les interventions techniques.

La supervision permet ici de :

- s'assurer que les postes ATESS sont accessibles et fonctionnels en permanence,
- vérifier que les disques de transfert (comme le serveur SYLEX) sont bien montés,
- surveiller l'espace disque, l'état du réseau, ou encore les processus critiques liés à l'application **Lecteur ATESS**,
- et fournir une visibilité centralisée aux équipes SI ou aux référents techniques.

La supervision agit donc comme un outil de prévention et d'aide à la décision, indispensable pour garantir la continuité de service sur des systèmes critiques.

3. Pourquoi avoir choisi Zabbix ?

Plusieurs solutions de supervision open source ou commerciales existent aujourd’hui, parmi lesquelles Nagios, Centreon, Prometheus, ou Zabbix.

Le choix de **Zabbix** s’est imposé pour plusieurs raisons :

- **Interface moderne** : contrairement à Nagios (plus rudimentaire), Zabbix offre une interface web ergonomique, claire et entièrement personnalisable.
- Installation autonome : contrairement à Centreon qui repose sur Nagios et nécessite plusieurs briques logicielles, Zabbix est une solution complète intégrée, plus facile à déployer dans un environnement sans accès Internet.
- **Supervision hybride** : Zabbix permet de superviser aussi bien des postes Linux que Windows, avec une prise en charge native des agents, SNMP, IPMI, scripts, etc.
- **Tableaux de bord avancés** : les fonctionnalités de dashboard permettent de construire des vues métiers lisibles pour les opérateurs.
- **Capacité à fonctionner hors ligne** : tous les paquets nécessaires peuvent être installés à partir des sources, sans dépendance à des dépôts distants.

Dans le cadre de ce projet, où l’environnement réseau est clos et restreint, Zabbix répond donc parfaitement aux exigences de sécurité, de modularité et d’autonomie.

3.4.2 Architecture de Zabbix :

Zabbix est une solution de supervision modulaire, dont l’architecture repose sur plusieurs composants interconnectés. Dans le cadre de ce projet, une installation complète et autonome a été mise en place, adaptée à un environnement sans accès à Internet.

L’architecture déployée repose sur les éléments suivants :

1. Serveur Zabbix

Le serveur Zabbix est le cœur du système. Il interroge les agents installés sur les machines clientes, collecte les métriques, évalue les conditions de

déclenchement d'alertes (triggers) et enregistre les données dans la base de données. Il pilote également l'interface web.

2. Base de données (MySQL)

La base de données contient :

- les paramètres de configuration de Zabbix,
- les métadonnées liées aux hôtes (hosts, items, triggers, etc.),
- l'historique et les tendances des données collectées.

Dans notre cas, un serveur MySQL sécurisé a été mis en place et les données sont chiffrées.

3. Interface web (Apache/PHP)

L'interface web permet aux administrateurs, superviseurs et techniciens :

- de consulter l'état des machines et des équipements supervisés,
- de créer ou modifier des hôtes, dashboards, items et alertes,
- d'afficher des graphiques et de recevoir des notifications.

Le serveur Apache héberge cette interface, en mode HTTPS sécurisé par un certificat SSL.

4. Zabbix Agent (Windows/Linux)

Les agents Zabbix sont installés sur les machines à superviser, y compris sur les baies ATESS. Ils collectent localement des informations (charge CPU, espace disque, services en cours, fichiers montés, utilisateurs connectés, etc.) et les transmettent au serveur Zabbix.

3.4.3. Installation de zabbix serveur :

Présentation de l'environnement de travail

La RATP dispose d'un environnement informatique centralisé, orienté vers la virtualisation d'infrastructure, afin de faciliter la gestion, la maintenance et la

sécurisation des services critiques (comme la supervision, les applications industrielles ou encore la gestion documentaire).

Les serveurs que j'ai utilisés dans le cadre de mon alternance étaient déployés sur une infrastructure virtualisée via Proxmox VE, une solution d'hypervision open source couramment utilisée dans les environnements professionnels.

Type d'hyperviseur

Proxmox utilise un hyperviseur de type 1 (bare-metal). Ce type d'hyperviseur s'installe directement sur le matériel physique, sans système d'exploitation intermédiaire, contrairement à un hyperviseur de type 2 qui fonctionne au-dessus d'un OS hôte (comme VirtualBox sur Windows, par exemple).

Avantages du type 1 (bare metal) :

- Performances optimisées (accès direct aux ressources physiques)
- Meilleure isolation des machines virtuelles (VM)
- Administration centralisée et sécurisée (interface web, gestion des rôles et des accès)
- Support des fonctionnalités avancées comme les snapshots, la haute disponibilité (HA), et la réPLICATION

Contexte d'installation

Dans notre cas, la machine sur laquelle Zabbix est installée est isolée du réseau Internet, ou du moins restreinte aux dépôts Red Hat Enterprise (via un proxy d'entreprise). Il a donc été nécessaire de procéder à une installation hors ligne à partir des fichiers sources officiels de Zabbix.

La version choisie est la 7.0.5, une version LTS (Long-Term Support) stable, maintenue à long terme et adaptée aux environnements critiques comme celui du RER.

Stack technique mise en place

- **Système d'exploitation** : Red Hat Enterprise Linux 8.6
- **Base de données** : MySQL 8.0 (installée localement)
- **Serveur web** : Apache (httpd)
- **Langage serveur** : PHP 8.2 avec modules compatibles

- **Chiffrement SSL** : Certificats auto-signés et configuration du fichier ssl.conf pour sécuriser l'interface web

Objectifs atteints

- Installation manuelle (hors ligne) du serveur Zabbix et de ses dépendances
- Configuration du serveur MySQL pour accepter la connexion depuis Zabbix
- Création et gestion des utilisateurs Zabbix sur la base de données
- Intégration à l'interface web d'administration Zabbix
- Surveillance des équipements critiques (machines industrielles, réseaux, disques, services)
- Personnalisation des dashboards, alertes, templates

Cette expérience m'a permis de mieux comprendre les enjeux de la supervision dans un environnement d'exploitation critique et m'a donné une vision complète du cycle de déploiement d'un outil de supervision dans un environnement sécurisé et restreint.

1. Téléchargement et transfert des fichiers sources d'installation :

Les sources de Zabbix sont disponibles sur le site officiel :

https://www.zabbix.com/download_sources

Une fois le fichier zabbix-7.0.5.tar.gz téléchargé sur une machine avec accès à Internet, il est transféré manuellement (via clé USB ou réseau interne) vers le serveur cible.

```
tar -xzf zabbix-7.0.5.tar.gz
```

Shell

```
rm zabbix-7.0.5.tar.gz
```

Shell

2. Installation des dépendances :

Zabbix nécessite plusieurs paquets de développement et bibliothèques. Étant sur une distribution **Red Hat 8.x**, voici les commandes exécutées :

```
subscription-manager repos --enable codeready-builder-for-rhel-8-x86_64-rpms
dnf clean all
dnf makecache
dnf install OpenIPMI OpenIPMI-devel libcurl-devel libevent* mysql* libxml* net-snmp* httpd
```

3. Crédit de l'utilisateur système zabbix :

Pour sécuriser l'exécution du processus Zabbix, un utilisateur système dédié est créé :

```
# permet de créer un groupe zabbix
groupadd --system zabbix

# permet de créer notre utilisateur zabbix mais il ne peut pas se connecter, il ne possède pas aussi de dossier home
useradd --system -g zabbix -d /usr/lib/zabbix -s /sbin/nologin -c "Zabbix Monitoring System" zabbix
```

4. Installation et configuration de MySQL :

Maintenant que nous avons créé notre utilisateur **zabbix**, il est temps d'installer **MySQL** sur notre serveur, pour se faire, on utilise la commande :

```
dnf install mysql-server
```

Package	Architecture	Version	Repository	Size
mysql-server	x86_64	8.0.30-1.module.el8.0+16523+5cb0e808	rhel-8-for-x86_64-appstream-rpms	25 M
Installing dependencies:				
mysql-libs	x86_64	2.0.9-1.el8	rhel-8-for-x86_64-baseos-rpms	346 k
mecab	x86_64	0.996-2.module.el8.0+16523+5cb0e808	rhel-8-for-x86_64-appstream-rpms	393 k
mysql	x86_64	8.0.30-1.module.el8.0+16523+5cb0e808	rhel-8-for-x86_64-appstream-rpms	13 M
mysql-common	x86_64	8.0.30-1.module.el8.0+16523+5cb0e808	rhel-8-for-x86_64-baseos-rpms	137 k
mysql-libsmsg	x86_64	8.0.30-1.module.el8.0+16523+5cb0e808	rhel-8-for-x86_64-appstream-rpms	620 k
polycoreutils-python-utils	noarch	2.0-19.el8	rhel-8-for-x86_64-baseos-rpms	253 k
protobuf-lite	x86_64	3.0.7-1.el8	rhel-8-for-x86_64-appstream-rpms	145 k
python3	x86_64	3.0.7-1.el9.2	rhel-8-for-x86_64-baseos-rpms	97 k
python3-lbsmanage	x86_64	2.0-9.el8_6	rhel-8-for-x86_64-baseos-rpms	128 k
python3-polycoreutils	noarch	2.0-19.el8	rhel-8-for-x86_64-baseos-rpms	2.2 M
python3-setuptools	x86_64	4.3.0-3.el8	rhel-8-for-x86_64-baseos-rpms	624 k
Enabling module streams:				
mysql		8.0		
Transaction Summary				
Install 12 Packages				
Total download size: 42 M				
Installed size: 208 M				
Is this ok [y/N]:				

Une fois cette commande lancée, elle nous montre les services qu'elle va installer sur notre machine, on entre Y pour confirmer et continuer notre installation.

Une fois **MySQL** installer sur notre serveur, il faut le configurer correctement, pour se faire on entre la commande suivante :

Ce script permet :

- de définir un mot de passe root,
- de désactiver les connexions anonymes,
- d'interdire l'accès root distant,
- de supprimer la base de test,
- et de recharger les privilèges.

```
Press y|Y for Yes, any other key for No: y
There are three levels of password validation policy:
LOW    Length >= 8
MEDIUM Length >= 8, numeric, mixed case, and special characters
STRONG Length >= 8, numeric, mixed case, special characters and dictionary file
Please enter 0 = LOW, 1 = MEDIUM and 2 = STRONG: 1
Please set the password for root here.

New password:
Re-enter new password:
Estimated strength of the password: 100
Do you wish to continue with the password provided?(Press y|Y for Yes, any other key for No) : y
By default, a MySQL installation has an anonymous user,
allowing anyone to log into MySQL without having to have
a user account created for them. This is intended only for
testing, and to make the installation go a bit smoother.
You should remove them before moving into a production
environment.

Remove anonymous users? (Press y|Y for Yes, any other key for No) : y
Success.

Normally, root should only be allowed to connect from
'localhost'. This ensures that someone cannot guess at
the root password from the network.

Disallow root login remotely? (Press y|Y for Yes, any other key for No) : y
Success.

By default, MySQL comes with a database named 'test' that
anyone can access. This is also intended only for testing,
and should be removed before moving into a production
environment.

Remove test database and access to it? (Press y|Y for Yes, any other key for No) : y
- Dropping test database...
Success.

- Removing privileges on test database...
Success.

Reloading the privilege tables will ensure that all changes
made so far will take effect immediately.

Reload privilege tables now? (Press y|Y for Yes, any other key for No) : y
Success.

All done!
[root@hb001316 mysql-server-8.4]# clear
[root@hb001316 mysql-server-8.4]#
```

5. Création de notre base de données zabbix + configuration :

Maintenant que le serveur MySQL est installé et fonctionnel sur notre machine, nous allons procéder à la création de la base de données Zabbix, qui sera utilisée par le serveur de supervision.

Dans un premier temps, nous nous connectons à MySQL avec le compte administrateur :

```
mysql -u root -p
```

Shell

Lors de la connexion, il faut renseigner le mot de passe root défini précédemment.

Une fois connectés au service MySQL, nous créons la base de données zabbix avec l'encodage et le collationnement requis par Zabbix :

```
create database zabbix character set utf8mb4 collate utf8mb4_bin;
```

MySQL

On peut vérifier que la base de données a bien été créée en listant l'ensemble des bases disponibles :

```
show databases;
```

MySQL

```
mysql> create database zabbix character set utf8mb4 collate utf8mb4_bin;
Query OK, 1 row affected (0.00 sec)

mysql> show databases;
+-----+
| Database      |
+-----+
| information_schema |
| mysql          |
| performance_schema |
| sys            |
| zabbix         |
+-----+
5 rows in set (0.00 sec)
```

Nous créons ensuite un utilisateur zabbix dédié à cette base de données, avec un mot de passe sécurisé :

```
create user 'zabbix'@'localhost' identified by [REDACTED]
```

MySQL

```
mysql> create user 'zabbix'@'localhost' identified by '[REDACTED]';  
Query OK, 0 rows affected (0.00 sec)
```

L'utilisateur zabbix a maintenant besoin de droits complets sur la base de données zabbix. Nous appliquons les priviléges avec la commande suivante :

```
grant all privileges on zabbix.* to 'zabbix'@'localhost';  
SET GLOBAL log_bin_trust_function_creators = 1;
```

MySQL

```
mysql> SET GLOBAL log_bin_trust_function_creators = 1;  
Query OK, 0 rows affected (0.00 sec)
```

Pour vérifier que les droits ont bien été appliqués, nous utilisons la commande :

```
show grants for 'zabbix'@'localhost';
```

MySQL

```
mysql> show grants for 'zabbix'@'localhost';  
+-----+  
| Grants for zabbix@localhost |  
+-----+  
| GRANT USAGE ON *.* TO `zabbix`@`localhost` |  
| GRANT ALL PRIVILEGES ON `zabbix`.* TO `zabbix`@`localhost` |  
+-----+  
2 rows in set (0.00 sec)
```

Enfin, nous devons importer les fichiers SQL fournis avec les sources de Zabbix, afin d'initialiser les tables nécessaires au bon fonctionnement du serveur.

Nous nous plaçons dans le répertoire suivant :

/root/zabbix/zabbix-7.0.5/database/mysql

Puis, nous exécutons les trois commandes suivantes pour injecter les structures de tables, les images et les données initiales :

```
mysql -u zabbix -p<password> zabbix < schema.sql  
mysql -u zabbix -p<password> zabbix < images.sql  
mysql -u zabbix -p<password> --default-character-set=utf8mb4 zabbix < data.sql
```



```
[root@hb001316 mysql]# mysql -u zabbix -p'RERzabbix2MY$QL' zabbix < schema.sql  
mysql: [Warning] Using a password on the command line interface can be insecure.  
[root@hb001316 mysql]# mysql -u zabbix -p'RERzabbix2MY$QL' zabbix < images.sql  
mysql: [Warning] Using a password on the command line interface can be insecure.  
[root@hb001316 mysql]# mysql -u zabbix -p'RERzabbix2MY$QL' zabbix < data.sql  
mysql: [Warning] Using a password on the command line interface can be insecure.  
[root@hb001316 mysql]#
```

Shell

6. Chiffrement de notre base de données MySQL :

Dans un environnement sensible comme celui de la RATP, la protection des données stockées en base est primordiale. Pour renforcer la sécurité de notre solution de supervision, nous avons mis en place le chiffrement des tables MySQL utilisées par Zabbix.

Avant toute opération de chiffrement, il est essentiel d'effectuer une sauvegarde complète de la base de données pour éviter toute perte de données.

```
mysqldump -u zabbix -p zabbix > sauvegarde_zabbix.sql
```

Shell

Cette commande crée un fichier de sauvegarde contenant l'ensemble des données de la base zabbix.

MySQL propose un plugin natif pour gérer le chiffrement des données : keyring_file.

Nous éditons le fichier de configuration principal du serveur MySQL :

```
nano /etc/my.cnf.d/mysql-server.cnf
```

Shell

Et nous ajoutons les lignes suivantes dans la section [mysqld] :

```
#chiffrement de la base de données
innodb_file_per_table=ON
early-plugin-load=keyring_file.so
keyring_file_data=/var/lib/mysql-keyring/keyring
```

Properties files

- **innodb_file_per_table** permet d'appliquer le chiffrement table par table.
- **early-plugin-load** charge le plugin keyring au démarrage du serveur.
- **keyring_file_data** définit l'emplacement du fichier contenant les clés de chiffrement.

Une fois le fichier modifié, nous redémarrons le service MySQL pour appliquer la configuration :

```
systemctl restart mysqld.service
```

Shell

Nous nous reconnectons ensuite au service MySQL pour vérifier que le plugin est bien actif :

```
SHOW VARIABLES LIKE 'keyring%'
```

```
mysql> SHOW VARIABLES LIKE 'keyring%';
+-----+-----+
| Variable_name | Value
+-----+-----+
| keyring_file_data | /var/lib/mysql-keyring/keyring
| keyring_operations | ON
+-----+
2 rows in set (0.00 sec)
```

MySQL

Pour chiffrer toutes les tables de la base **zabbix**, nous exécutons cette commande SQL qui génère dynamiquement les requêtes ALTER nécessaires :

```
SELECT CONCAT('ALTER TABLE `', TABLE_SCHEMA, '`.', TABLE_NAME, '`',
  ENCRYPTION='Y';') AS stmt FROM information_schema.TABLES WHERE TABLE_SCHEMA =
  'zabbix' AND TABLE_TYPE = 'BASE TABLE';
```

MySQL

Pour s'assurer que le chiffrement a bien été appliqué, nous lançons la commande suivante :

```
SELECT TABLE_NAME, CREATE_OPTIONS FROM information_schema.TABLES WHERE
  TABLE_SCHEMA = 'zabbix' AND CREATE_OPTIONS LIKE "%ENCRYPTION='Y'" ;
```

MySQL

Toutes les tables de la base **zabbix** doivent alors afficher l'option : **ENCRYPTION='Y'**.

Le chiffrement de la base de données est désormais en place. Cette mesure permet de protéger les métriques sensibles stockées par Zabbix, notamment en cas d'intrusion physique sur le serveur ou de compromission des fichiers disques.

7. Configuration des sources pour la compilation de Zabbix

Avant de procéder à la compilation, il est nécessaire d'indiquer au compilateur que l'on souhaite utiliser la norme **C99 avec les extensions GNU**, ce qui est requis pour Zabbix.

```
export CFLAGS="-std=gnu99"
```

Shell

Une fois cela défini, on peut lancer le script de configuration :

```
./configure --enable-server --enable-agent --with-mysql --enable-ipv6 --with-net-snmp --with-libcurl --with-libxml2 --with-openipmi
```

8. Installation du serveur HTTP (Apache) :

L'interface web de Zabbix repose sur un serveur HTTP. Dans notre cas, nous utiliserons **Apache (httpd)**, accompagné de **PHP 8.0**.

Installation d'Apache

Sur une distribution Red Hat, le serveur Apache se nomme **httpd**. Pour l'installer :

```
yum install httpd
```

Une fois le service installé, on peut lancer le lancer et l'activer au boot de notre serveur, pour se faire, on lance les commandes suivantes :

```
systemctl start httpd #permet de lancer le service
systemctl enable httpd # Permet de le lancer au boot
systemctl status httpd # Vérifier le status de notre service
```

On peut vérifier que le serveur Apache est fonctionnel en accédant à son IP locale, par exemple : <http://172.18.147.39>

Après avoir vérifié l'affichage correct de notre page web, nous allons ajouter la page Zabbix pour y accéder. Pour cela, nous nous rendons dans le dossier **/var/www/html** et créons un dossier **zabbix** avec la commande suivante :

```
mkdir zabbix
```

Puis on copie l'interface utilisateur de Zabbix dans ce dossier :

```
cp -a /root/zabbix/zabbix-7.0.5/ui/* /var/www/html/zabbix
```

Une fois la copie effectuée, on peut accéder à l'interface depuis un navigateur :
<http://172.18.147.39/zabbix>

À cette étape, une erreur peut apparaître indiquant que PHP n'est pas installé.

On commence par lister les versions disponibles :

```
dnf module list php
```



Name	Stream	Profiles	Summary
php	7.0	common [d], devel, minimal	PHP scripting language
php	7.3	common [d], devel, minimal	PHP scripting language
php	7.4	common [d], devel, minimal	PHP scripting language
php	8.0 [e]	common [d], devel, minimal	PHP scripting language

Hint: [d]efault, [e]nabled, [x]disabled, [i]nstalled

Cette commande va nous permettre de voir les différentes version de PHP disponible, dans notre cas nous allons sélectionner la version 8.0 avec la commande :

```
dnf module enable php:8.0
```

Puis on installe PHP :

```
dnf install php
```

Une fois cela fait, on peut relancer notre service httpd, avec la commande :

```
systemctl restart httpd
```

Certaines options doivent être ajustées dans la configuration PHP pour permettre le bon fonctionnement de Zabbix.

		Current value	Required	
PHP version		8.0.13	8.0.0	OK
PHP option "memory_limit"		128M	128M	OK
PHP option "post_max_size"		16M	16M	OK
PHP option "upload_max_filesize"		2M	2M	OK
PHP option "max_execution_time"		300	300	OK
PHP option "max_input_time"		300	300	OK
PHP databases support		MySQL		OK
PHP bcmath		off		Fail
PHP mbstring		on		OK
PHP gd		unknown	2.0	Fail
PHP gd PNG support		off		Fail
PHP gd JPEG support		off		Fail
PHP gd GIF support		off		Warning
PHP gd FreeType support		off		Fail
PHP libxml		2.9.7	2.6.15	OK
PHP xmlwriter		on		OK
PHP xmlreader		on		OK
PHP LDAP		off		Warning
PHP OpenSSL		on		OK

Pour palier à ce problème, nous allons éditer le fichier suivant :

```
nano /etc/php.ini
```

Shell

Et on modifie les paramètres suivants :

```
memory_limit=128
post_max_size=16
max_execution_time=300
extension=Mysql.io
bcmath.scan=2
```

Properties files

Une fois ces options correctement modifier, nous allons installer un dernier module avec la commande suivante :

```
Shell
yum install php-gd

langpacks-en_GB.noarch : English (United Kingdom) langpacks meta-package
[root@hb001316 etc]# yum search php-gd
Updating Subscription Management repositories.
=====
Name Exactly Matched: php-gd ==
php-gd.x86_64 : A module for PHP applications for using the gd graphics library
[root@hb001316 etc]# yum install php-gd
```

Ce module est nécessaire pour certaines fonctionnalités graphiques de l'interface Zabbix.

Pour appliquer toutes les modifications, nous allons effectuer un redémarrage de notre machine avec la commande :

```
Shell
sudo reboot
```

Une fois le système redémarré, on se reconnecte à l'interface web :

<http://172.18.147.39/zabbix>

Si PHP est correctement configuré, la première page de configuration s'affiche :

ZABBIX

Configure DB connection

Please create database manually, and set the configuration parameters for connection to this database.
Press "Next step" button when done.

Welcome	Database type	MySQL
Check of pre-requisites	Database host	localhost
Configure DB connection	Database port	0 - use default port
Settings	Database name	zabbix
Pre-installation summary	Store credentials in	Plain text HashiCorp Vault CyberArk Vault
Install	User	zabbix
	Password	RERzabbix2MYSQL

Database TLS encryption Connection will not be encrypted because it uses a socket file (on Unix) or shared memory (Windows).

[Back](#) [Next step](#)

On renseigne ici les paramètres de la base de données (nom de la base, utilisateur, mot de passe).

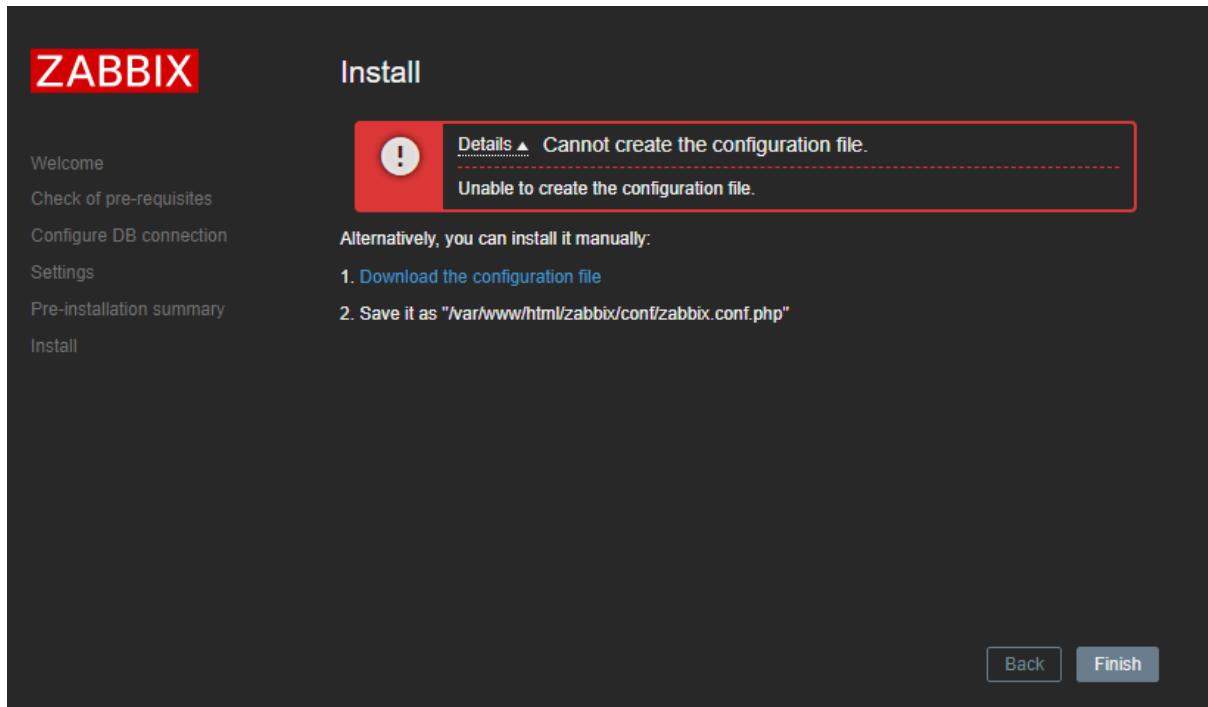
Ensuite, on définit le nom du serveur et la zone géographique :

The screenshot shows the Zabbix Settings page. On the left, there's a sidebar with links: Welcome, Check of pre-requisites, Configure DB connection, Settings, Pre-installation summary (which is highlighted in blue), and Install. The main area has a title "Settings". It contains three input fields: "Zabbix server name" with the value "Supervision ATESS", "Default time zone" set to "(UTC+01:00) Europe/Paris", and "Default theme" set to "Dark". At the bottom right are two buttons: "Back" and "Next step".

Un récapitulatif des paramètres apparaît ensuite :

The screenshot shows the Zabbix Pre-installation summary page. On the left, there's a sidebar with links: Welcome, Check of pre-requisites, Configure DB connection, Settings, Pre-installation summary (highlighted in blue), and Install. The main area has a title "Pre-installation summary" and a note: "Please check configuration parameters. If all is correct, press "Next step" button, or "Back" button to change configuration parameters." It lists several configuration parameters with their values: Database type (MySQL), Database server (localhost), Database port (default), Database name (zabbix), Database user (zabbix), Database password (redacted), Database TLS encryption (false), and Zabbix server name (Supervision ATESS). At the bottom right are two buttons: "Back" and "Next step".

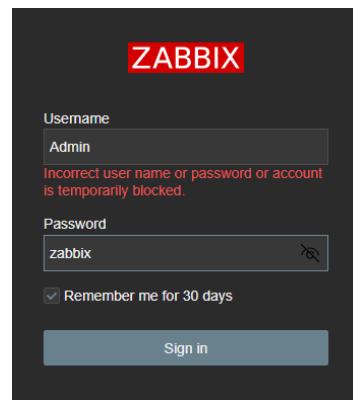
À cette étape, un message d'erreur peut apparaître, demandant de télécharger manuellement le fichier **zabbix.conf.php**:



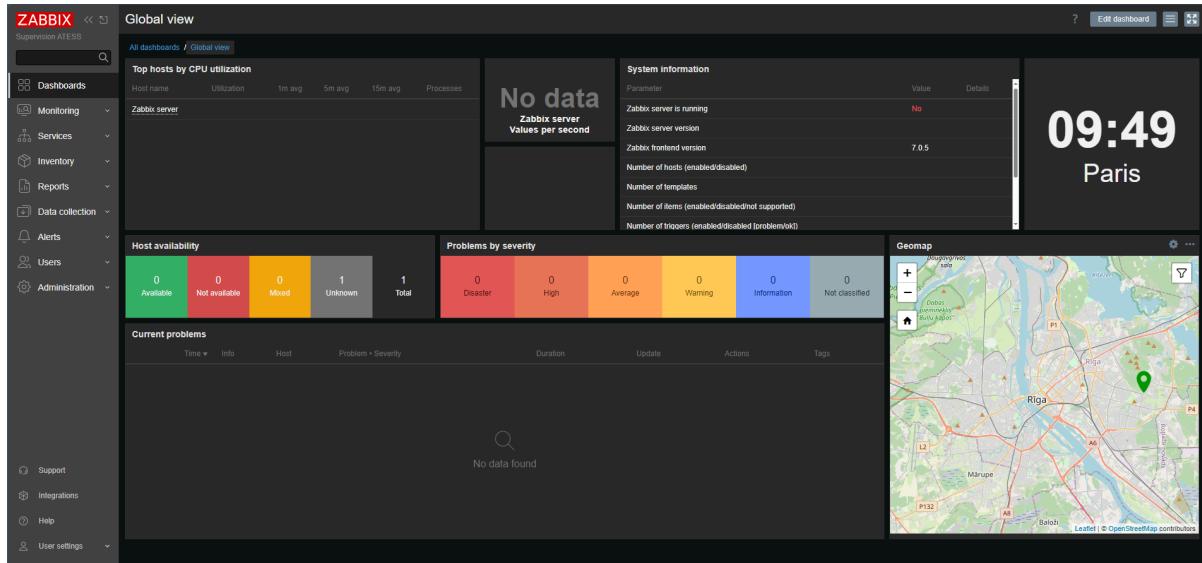
On place ce fichier dans le répertoire suivant : **/var/www/html/zabbix/conf**

```
[root@hb001316 conf]# pwd
/var/www/html/zabbix/conf
[root@hb001316 conf]# ls
certs maintenance.inc.php zabbix.conf.php zabbix.conf.php.example
[root@hb001316 conf]#
```

Une fois la configuration finalisée, on clique sur "Finish". On est alors redirigé vers la page de connexion :



Une fois connectés, on accède à la page d'accueil du tableau de bord Zabbix :



Mise en place d'un certificat SSL

Objectif

Afin de sécuriser les connexions vers l'interface web de Zabbix, nous allons mettre en place un certificat SSL auto-signé. Cela permettra d'établir une communication chiffrée entre le navigateur de l'utilisateur et le serveur, évitant ainsi toute interception de données sensibles.

On commence par installer le module mod_ssl d'Apache, nécessaire à la prise en charge des connexions HTTPS :

```
yum install mod_ssl
```

Shell

Pour stocker proprement notre clé privée et notre certificat, nous créons deux répertoires sécurisés dans /etc/httpd :

```
# nous permet de créer nos différent répertoire
mkdir /etc/httpd/ssl
mkdir /etc/httpd/ssl/private

# mettre s'assurer que mettre des droits uniquement pour root
chmod 700 /etc/httpd/ssl
chmod 700 /etc/httpd/ssl/private
```

Shell

Nous générerons maintenant un certificat SSL auto-signé valable 365 jours avec une clé RSA 2048 bits. Ce certificat sera stocké dans le dossier précédemment créé :

Pendant l'exécution de la commande, plusieurs informations vous seront demandées. **Le champ le plus important est le FQDN (nom DNS complet)** du serveur, qui doit correspondre à celui que vous utiliserez dans le navigateur.

Dans notre cas : **hb001316.info.ratp**

```
sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/httpd/ssl/zabbix-autosigne.key -out /etc/httpd/ssl/zabbix-autosigne.crt

[root@hb001316 ssl]# openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/httpd/ssl/private/certificat-zabbix-autosigne.key -out /etc/httpd/ssl/certificat-zabbix-autosigne.crt
Generating a RSA private key
.....+++++
.....+++++
writing new private key to '/etc/httpd/ssl/private/certificat-zabbix-autosigne.key'

-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

-----
Country Name (2 letter code) [XX]:FR
State or Province Name (full name) []:ile-de-france
Locality Name (eg, city) [Default City]:Paris
Organization Name (eg, company) [Default Company Ltd]:RATP
Organizational Unit Name (eg, section) []:RER
Common Name (eg, your name or your server's hostname) []:hb001316.info.ratp
Email Address []:
[root@hb001316 ssl]#
```

On modifie le fichier **/etc/httpd/conf.d/ssl.conf** pour spécifier le chemin du certificat et de la clé :

```
42 # General setup for the virtual host, inherited from global configuration
43 DocumentRoot "/var/www/html/zabbix"
44 ServerName hb001316.info.ratp:443
45
46 # Point SSLCertificateFile at a PEM encoded certificate. If
47 # the certificate is encrypted, then you will be prompted for a
48 # pass phrase. Note that restarting httpd will prompt again. Keep
49 # in mind that if you have both an RSA and a DSA certificate you
50 # can configure both in parallel (to also allow the use of DSA
51 # ciphers, etc.)
52 # Some ECC cipher suites (http://www.ietf.org/rfc/rfc4492.txt)
53 # require an ECC certificate which can also be configured in
54 # parallel.
55 SSLCertificateFile /etc/httpd/ssl/certificat-zabbix-autosigne.crt
56
57 # Server Private Key:
58 # If the key is not combined with the certificate, use this
59 # directive to point at the key file. Keep in mind that if
60 # you've both a RSA and a DSA private key you can configure
61 # both in parallel (to also allow the use of DSA ciphers, etc.)
62 # ECC keys, when in use, can also be configured in parallel
63 SSLCertificateKeyFile /etc/httpd/ssl/private/certificat-zabbix-autosigne.key
64
```

Une fois la configuration terminée et le service relancé, on peut accéder à l'interface web sécurisée de Zabbix via : <https://hb001316.info.ratp>

Pour forcer l'utilisation de HTTPS, nous allons rediriger automatiquement tout le trafic entrant sur le port 80 (HTTP) vers le port 443 (HTTPS).

Modifier le fichier **/etc/httpd/conf/httpd.conf** (ou créer un fichier dédié dans **/etc/httpd/conf.d/**) et y ajouter le bloc suivant :

```
<VirtualHost *:80>
    ServerName hb001316.info.ratp
    Redirect permanent / https://hb001316.info.ratp/
</VirtualHost>
```

Properties files

Cela permet :

- De spécifier le nom DNS du serveur
- De rediriger de manière permanente tous les accès en HTTP vers la version sécurisée HTTPS.

Après modification, il est nécessaire de relancer Apache :

```
systemctl restart httpd.service
systemctl status httpd.service
```

Shell

Une fois la redirection active, toute tentative d'accès via <http://hb001316.info.ratp> sera automatiquement redirigée vers <https://hb001316.info.ratp>.

L'interface web Zabbix est désormais accessible de manière sécurisée.

9. Installation de zabbix agent :

Dans un premier temps, nous allons télécharger l'exécutable d'installation de **Zabbix Agent**.

Pour cela, rendez-vous sur le site officiel de Zabbix à l'adresse suivante :

https://www.zabbix.com/download_agents

Téléchargez la version suivante : **Windows AMD64 7.0 TLS OpenSSL MSI**

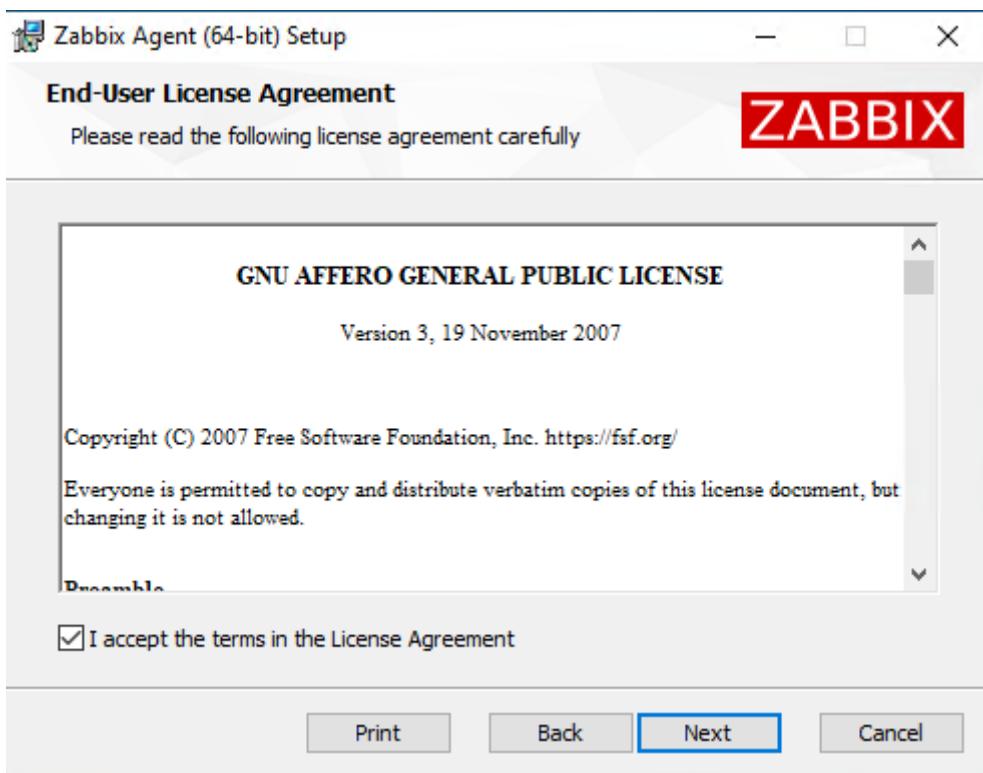
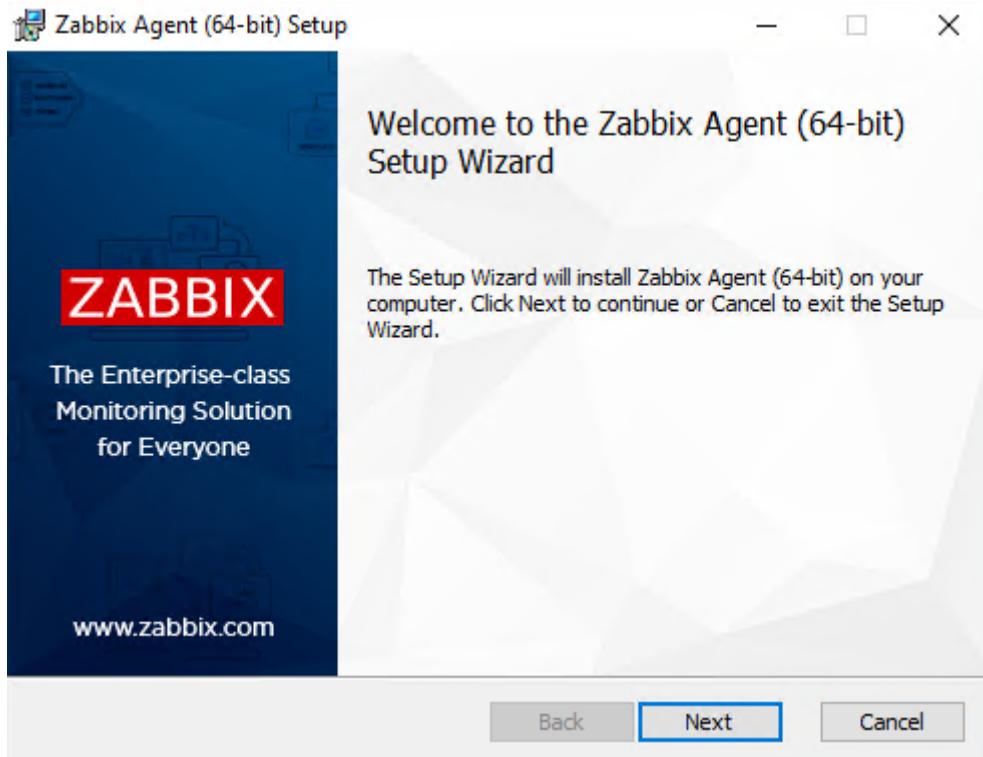
The screenshot shows the Zabbix download page. At the top, there are seven options: 'Zabbix Packages', 'Zabbix Cloud' (with a 'Free trial' badge), 'Third-Party cloud vendors', 'Zabbix Containers', 'Zabbix Appliance', 'Zabbix Sources', and 'Zabbix Agents'. The 'Zabbix Agents' option is highlighted with a large blue arrow pointing to it. Below this, a section titled 'Download pre-compiled Zabbix agent binaries' is shown. It includes a table with columns: OS DISTRIBUTION, OS VERSION, HARDWARE, ZABBIX VERSION, ENCRYPTION, and PACKAGING. The table lists various operating systems and their corresponding Zabbix versions and packaging formats.

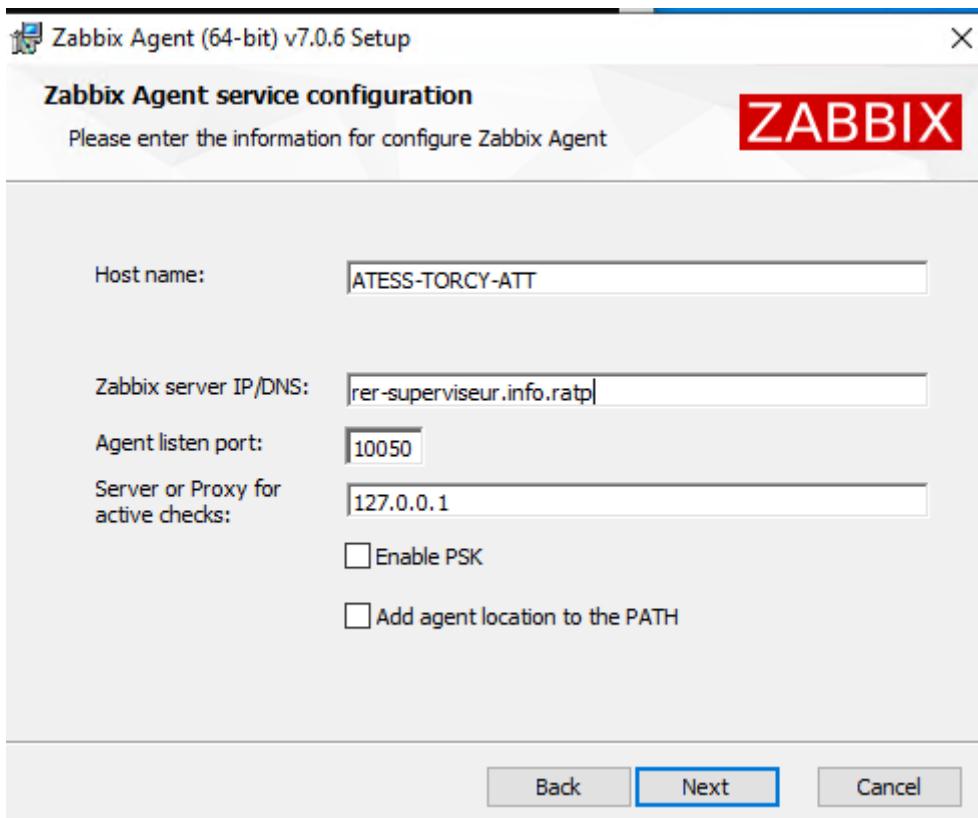
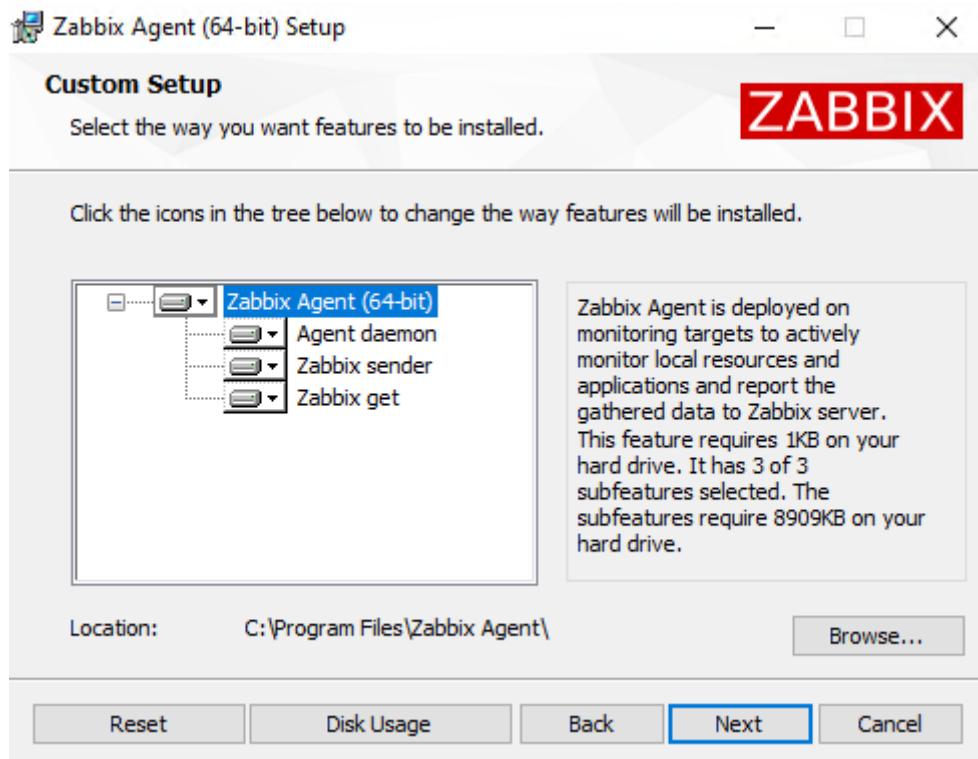
OS DISTRIBUTION	OS VERSION	HARDWARE	ZABBIX VERSION	ENCRYPTION	PACKAGING
Windows	Any	amd64	7.0 LTS	OpenSSL	MSI
Linux		i386	6.4	No encryption	Archive
macOS			6.2		
AIX			6.0 LTS		
FreeBSD			5.4		
OpenBSD			5.2		
Solaris			5.0 LTS		
			4.4		
			4.2		
			4.0 LTS		
			3.0 LTS		

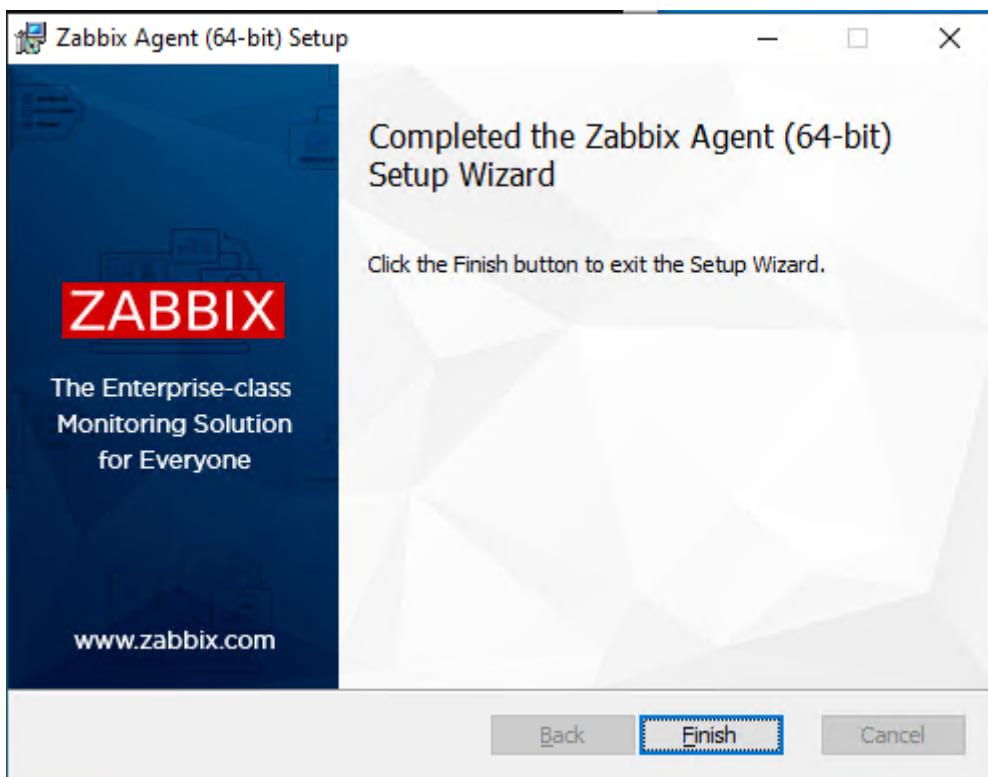
Une fois le fichier téléchargé, connectez-vous à une baie ATESS ou à une autre machine cliente sur laquelle vous souhaitez installer l'agent.

Lancez l'installation de l'agent avec l'exécutable **.msi**.

Durant l'installation, renseignez les informations suivantes :







L'agent installé, nous allons désormais lui appliquer une configuration complète.
Pour cela, accédez à l'espace suivant sur le SharePoint :

Sharepoint de RER/documents

RDSI/RDSI/Supervision/Zabbix/installation_Zabbix_agent/Configuration_type

documents RDSI > RDSI > Supervision > Zabbix > Installation_Zabbix_agent > Configuration_type

Nom	Modifié	Modifié par	+ Ajouter une colonne
certificat SSL	25 novembre 2024	MALET Raphael	
Script	25 novembre 2024	MALET Raphael	
<u>zabbix_agentd.conf</u>	19 février	MALET Raphael	

Dans ce répertoire, vous trouverez :

- Un **fichier de configuration par défaut (zabbix_agentd.conf)** prêt à l'emploi
- Les **certificats SSL** nécessaires pour le chiffrement
- Les **scripts** utilisés pour récupérer certaines métriques système

Ce fichier de configuration contient :

- Les paramètres de connexion au serveur Zabbix
- Les chemins vers les certificats SSL
- La configuration pour permettre l'exécution de commandes à distance via l'interface Zabbix

```
#####
# GENERAL PARAMETERS #####
### Option: LogFile
LogFile=C:\Program Files\Zabbix Agent\zabbix_agentd.log

### Option: AllowKey
EnableRemoteCommands=1
AllowKey=system.run[*]

### Option: Server
Server=172.18.147.39

##### Active checks related
### Option: ServerActive
ServerActive=172.18.147.39

### Option: Hostname
Hostname=<Mettre_hostname_machine>

### Option: Include
Include=C:\Program Files\Zabbix Agent\zabbix_agentd.d\

#####
# USER-DEFINED MONITORED PARAMETERS #####
### Option: UnsafeUserParameters
UserParameter= Nombre.utilisateurs,powershell.exe -ExecutionPolicy Bypass -File "C:\Program Files\Zabbix Agent\Script\NombreUtilisateur.ps1"

#####
# TLS-RELATED PARAMETERS #####
### Option: TLSConnect
TLSConnect=cert

### Option: TLSAccept
TLSAccept=cert

### Option: TLSCAFile
TLSCAFile=C:\Progra~1\Zabbix~1\certif~1\ca.crt

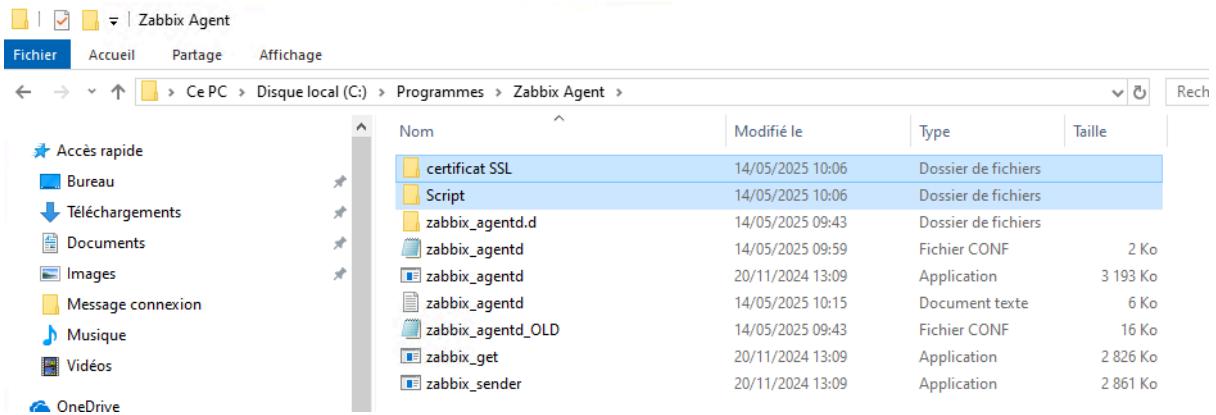
### Option: TlSCertFile
TlSCertFile=C:\Progra~1\Zabbix~1\certif~1\zabbix_server.crt
TLSKeyFile=C:\Progra~1\Zabbix~1\certif~1\zabbix_server.key
```

Téléchargez l'ensemble du contenu du répertoire Configuration_type puis copiez-le sur la machine cliente.

Accédez ensuite au répertoire d'installation de Zabbix Agent :

C:\Program Files\Zabbix Agent.

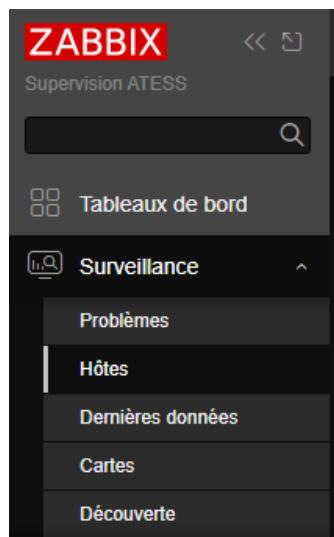
Nous y insérerons le fichier de configuration de zabbix, puis les différents dossier de configuration Script et certificat SSL :



Une fois cela fait, nous pouvons effectuer un redémarrage de notre machine, pour que les modifications soient correctement prises en compte par l'application Zabbix agent.

Une fois cela fait, nous pouvons donc nous rendre sur notre interface web zabbix : <https://rer-superviseur.info.ratp/>

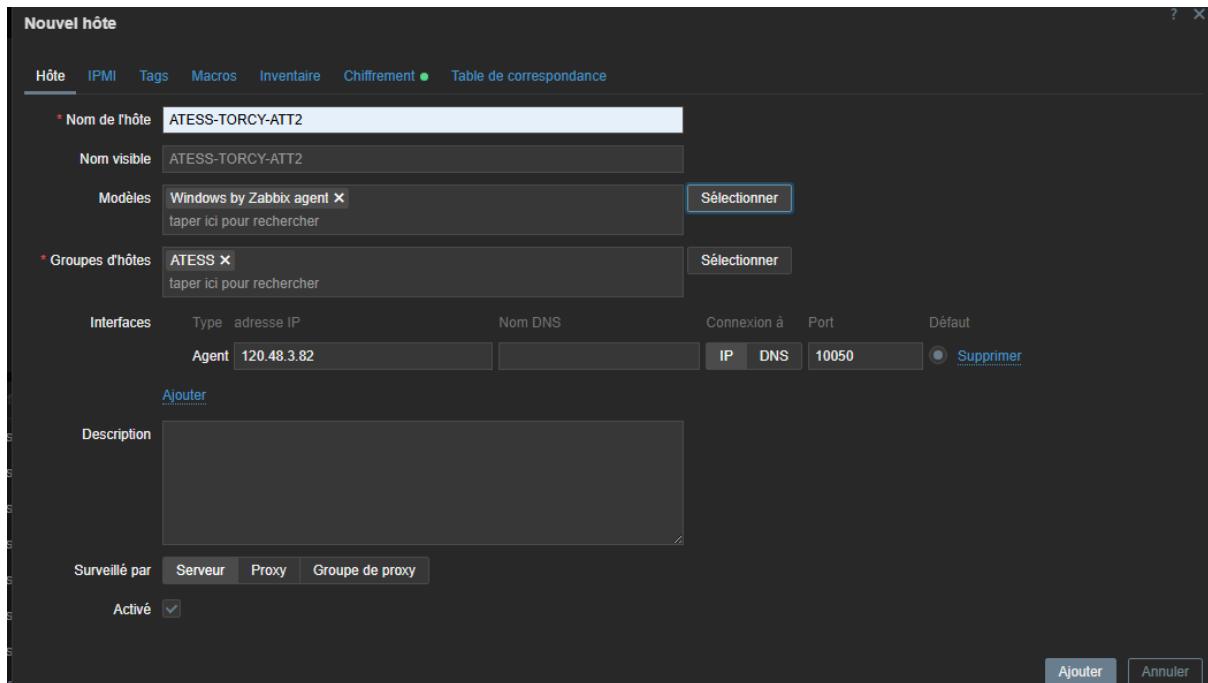
Une fois sur notre interface, nous allons nous rendre dans l'onglet suivant pour y ajouter une machine à superviser : Surveillance > Hôtes



Cliquez sur le bouton **Créer un hôte**, puis remplissez les champs suivants :

- Nom de l'hôte : nom de la machine sur laquelle l'agent est installé
- Modèle : Templates > Windows by Zabbix agent
Ce modèle inclut déjà des éléments de supervision prêts à l'emploi.
- **Groupe d'hôtes** : ATESS

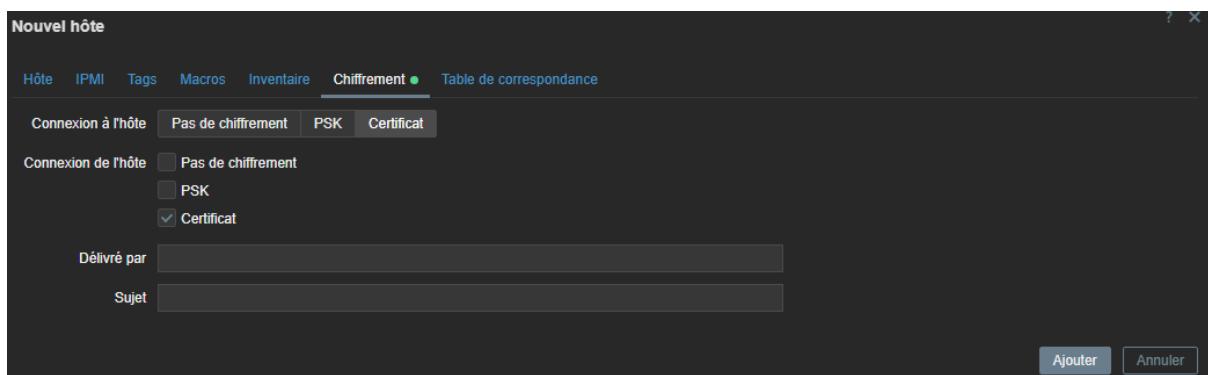
- Interface : adresse IP de la machine (ou nom DNS si disponible)



Dans l'onglet **Chiffrement** :

- Mode de connexion : Certificat
- Cochez l'option **Certificat**

Cela permettra de chiffrer les communications entre l'agent et le serveur à l'aide des certificats SSL.



Une fois la configuration terminée, redémarrez la machine cliente pour valider le bon démarrage de l'agent et s'assurer que le fichier de configuration est bien pris en compte.

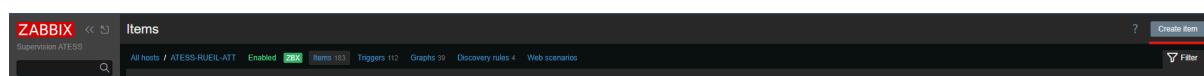
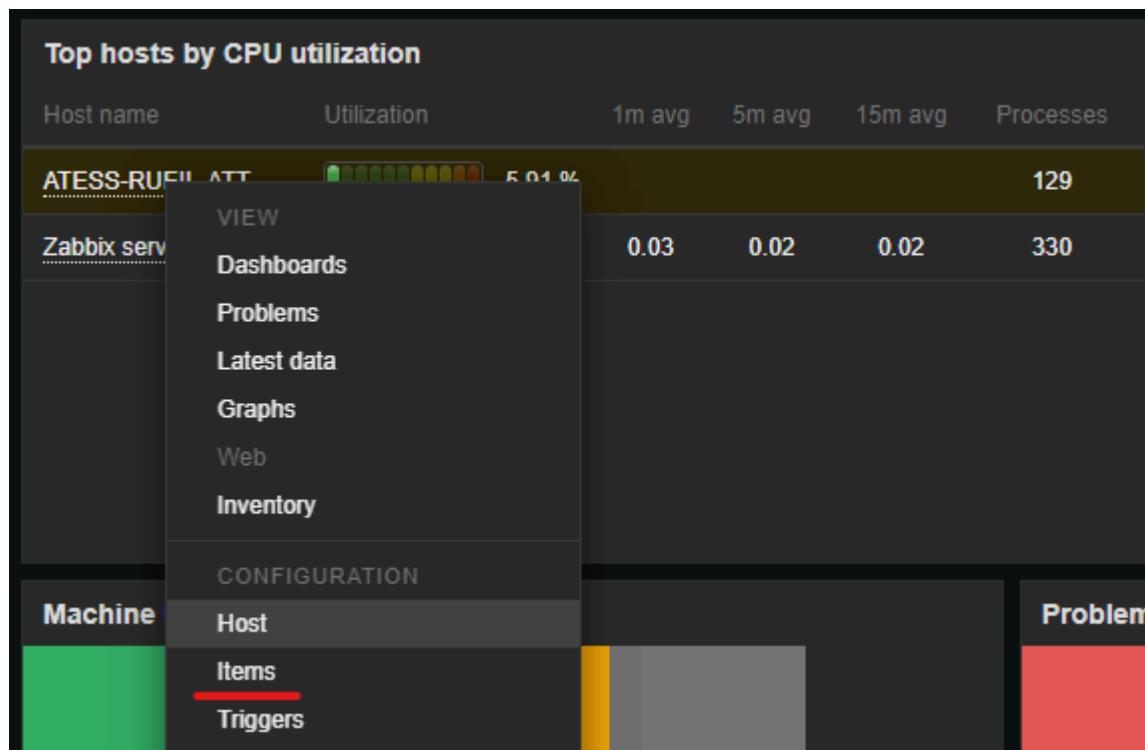
L'hôte devrait alors apparaître automatiquement sur l'interface de supervision Zabbix, avec un statut actif si la connexion est bien établie.

10. Configuration d'une règle pour surveiller le trafic réseau d'une machine

Par défaut, les règles de supervision réseau sur certaines machines peuvent ne pas fonctionner correctement, notamment si les interfaces ne sont pas reconnues par le modèle utilisé. Pour corriger cela, nous allons créer deux nouveaux items personnalisés permettant de suivre le trafic réseau entrant et sortant d'une machine supervisée.

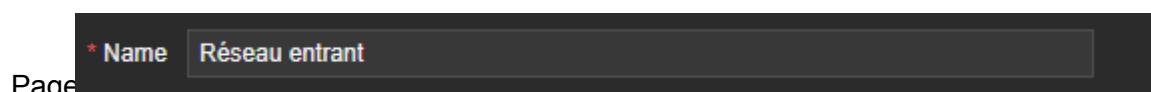
Depuis l'interface Zabbix, accédez à la liste de vos hôtes, puis cliquez sur le nom de la machine concernée pour accéder à sa configuration.

- Allez dans l'onglet **Items**.
- Cliquez sur le bouton **Create Item** en haut à droite.

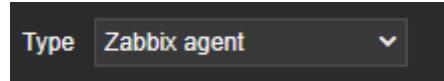


Dans la fenêtre de création :

- **Nom de l'item** : Réseau entrant

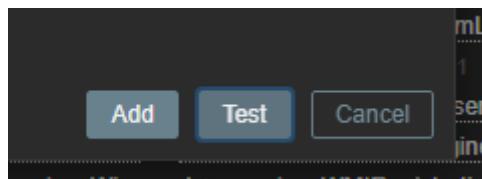


- **Type** : Zabbix agent



- **Key** : commencez par entrer la clé suivante pour identifier les interfaces disponibles : **net.if.list**

Cliquez ensuite sur le bouton Test puis sur Get value and test. Cela vous affichera la liste des interfaces réseau disponibles pour la machine sélectionnée.



1	Ethernet	enabled - Intel(R) Ethernet Controller (3) I225-V #4-WFP Native MAC Layer LightWeight Filter-0000
2	Ethernet	enabled - Intel(R) Ethernet Controller (3) I225-V #4-Zscaler LightWeight Filter-0000
3	Ethernet	enabled - Intel(R) Ethernet Controller (3) I225-V #4-QoS Packet Scheduler-0000
4	Ethernet	enabled - Intel(R) Ethernet Controller (3) I225-V #4-WFP 802.3 MAC Layer LightWeight Filter-0000
5	Ethernet	enabled - Intel(R) Ethernet Controller (3) I225-V #3-WFP Native MAC Layer LightWeight Filter-0000
6	Ethernet	enabled - Intel(R) Ethernet Controller (3) I225-V #3-Zscaler LightWeight Filter-0000
7	Ethernet	enabled - Intel(R) Ethernet Controller (3) I225-V #3-QoS Packet Scheduler-0000
8	Ethernet	enabled - Intel(R) Ethernet Controller (3) I225-V #3-WFP 802.3 MAC Layer LightWeight Filter-0000
9	Ethernet	enabled - WAN Miniport (IP)-WFP Native MAC Layer LightWeight Filter-0000
10	Ethernet	enabled - WAN Miniport (IP)-Zscaler LightWeight Filter-0000
11	Ethernet	enabled - WAN Miniport (IP)-QoS Packet Scheduler-0000
12	Ethernet	enabled - WAN Miniport (IPv6)-WFP Native MAC Layer LightWeight Filter-0000
13	Ethernet	enabled - WAN Miniport (IPv6)-Zscaler LightWeight Filter-0000
14	Ethernet	enabled - WAN Miniport (IPv6)-QoS Packet Scheduler-0000
15	Ethernet	enabled - WAN Miniport (Network Monitor)-WFP Native MAC Layer LightWeight Filter-0000
16	Ethernet	enabled - WAN Miniport (Network Monitor)-Zscaler LightWeight Filter-0000
17	Ethernet	enabled - WAN Miniport (Network Monitor)-QoS Packet Scheduler-0000
18	Ethernet	unknown - Microsoft Kernel Debug Network Adapter
19	Ethernet	enabled - WAN Miniport (IP)
20	Ethernet	enabled - WAN Miniport (IPv6)
21	Ethernet	enabled - WAN Miniport (Network Monitor)
22	Ethernet	unknown - Intel(R) Ethernet Controller (3) I225-V
23	Ethernet	unknown - Intel(R) Ethernet Controller (3) I225-V #2
24	Ethernet	enabled 120.5.3.78 Intel(R) Ethernet Controller (3) I225-V #3
25	Ethernet	enabled - Intel(R) Ethernet Controller (3) I225-V #4
26	PPP	enabled - WAN Miniport (PPPOE)
27	Software Loopback	enabled 127.0.0.1 Software Loopback Interface 1
28	Tunnel type encapsulation unknown	- Microsoft Teredo Tunneling Adapter
29	Tunnel type encapsulation unknown	- Microsoft IP-HTTPS Platform Adapter
30	Tunnel type encapsulation unknown	- Microsoft 6to4 Adapter
31	Tunnel type encapsulation enabled	- WAN Miniport (SSTP)
32	Tunnel type encapsulation enabled	- WAN Miniport (IKEv2)
33	Tunnel type encapsulation enabled	- WAN Miniport (L2TP)
34	Tunnel type encapsulation enabled	- WAN Miniport (PPTP)
35		

143 characters

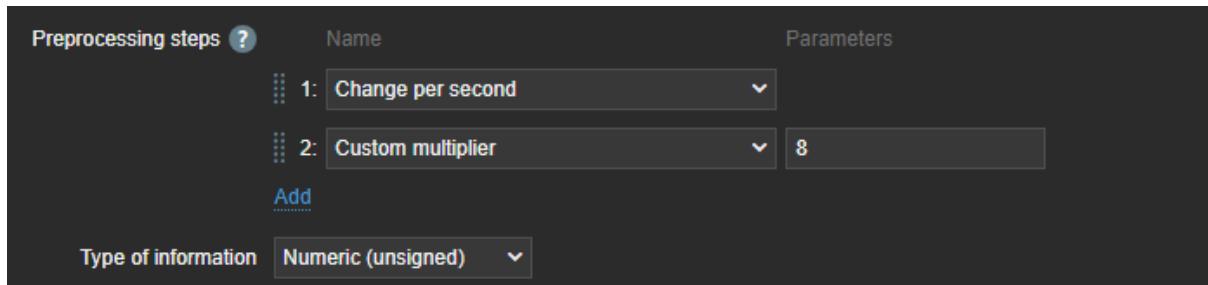
Apply Cancel

- Une fois l'interface identifiée, remplacez la clé par :
- net.if.in["Nom_de_l_interface",bytes]**
- Type of information : **Numeric (unsigned)**

- Units : **bps**

Allez dans l'onglet Preprocessing et ajoutez les étapes suivantes :

- Change per second : permet de calculer la différence de trafic entre deux collectes (taux).
- Multiplier : valeur **8**, pour convertir les bits en octets.



Une fois cet item de surveillance correctement créé, nous pouvons maintenant voir le trafic réseaux sur notre machine en temps réel.

11. Vérifier que le serveur est correctement connectés à notre machine.

Nous allons maintenant créer un item pour vérifier que le disque réseau utilisé pour le vidding des boîtes noires (par exemple X:) est monté sur la machine cliente. Cela permet de s'assurer que la connexion avec le serveur de vidding est bien établie et fonctionnelle.

Cette vérification est essentielle pour éviter toute perte de données ou échec de transfert lors du vidding des fichiers critiques.

Item Tags Preprocessing 4

* Name	disque X utilisation												
Type	Zabbix agent												
* Key	vfs.fs.size["X:",free]												
Type of information	Text												
* Host interface	120.5.3.78:10050												
* Update interval	1m												
Custom intervals	<table border="1"> <thead> <tr> <th>Type</th> <th>Interval</th> <th>Period</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td>Flexible</td> <td>50s</td> <td>1-7,00:00-24:00</td> <td>Remove</td> </tr> <tr> <td>Add</td> <td></td> <td></td> <td></td> </tr> </tbody> </table>	Type	Interval	Period	Action	Flexible	50s	1-7,00:00-24:00	Remove	Add			
Type	Interval	Period	Action										
Flexible	50s	1-7,00:00-24:00	Remove										
Add													
* Timeout	Global Override 3s												
* History	Do not store Store up to 31d												
Populates host inventory field	-None-												
Description	(Empty text area)												
Enabled	<input checked="" type="checkbox"/>												
Latest data													

Preprocessing steps ?

Name	Parameters	Cus
1: Check for not supported value	any error	
Custom on fail	Discard value Set value to Set error to 0	
2: Boolean to decimal		
3: Replace	0	Indisponible
4: Replace	1	Disponnible
Add		
Type of information	Text	

12. Surveiller le cache de notre service SFTP Drive :

Dans cette partie, nous allons mettre en place une supervision du cache utilisé par le service SFTP Drive 2022. Ce cache stocke temporairement les fichiers en attente de transfert vers le serveur distant.

L'objectif est de s'assurer qu'aucun fichier ne reste bloqué dans le cache, ce qui pourrait indiquer une erreur de transfert ou une déconnexion du serveur SFTP. En

cas de détection d'un cache non vide, une intervention manuelle ou un redémarrage du service pourra être envisagé.

Localisation du dossier de cache

Le dossier de cache du service **SFTP Drive 2022** se trouve à l'emplacement suivant : **C:\ProgramData\SFTPDrive\SYLEX**

C'est ce répertoire que nous allons surveiller pour suivre l'évolution de son contenu.

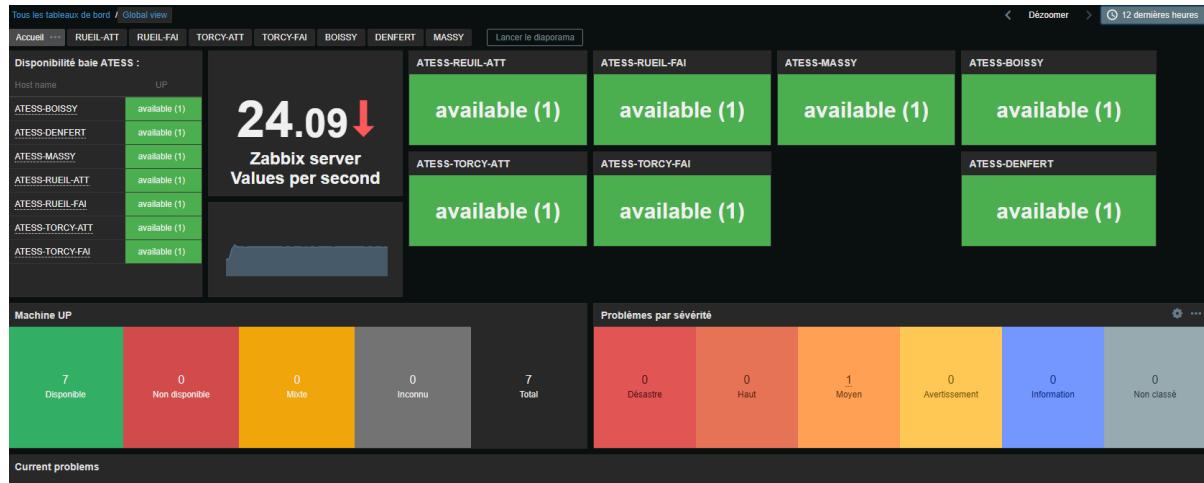
Pour superviser ce cache, nous allons créer un item dans la fiche de la machine concernée, avec les paramètres suivants :

The screenshot shows the 'Item' configuration page in Zabbix. The 'Item' tab is selected. Key configuration parameters include:

- Name:** Cache Sylex
- Type:** Zabbix agent
- Key:** vfs.dir.size["C:\ProgramData\SFTPDrive\SYLEX"]
- Type of information:** Numeric (unsigned)
- Host interface:** 120.48.3.82:10050
- Units:** (empty)
- Update interval:** 1m
- Custom intervals:** A table showing one entry: Type: Flexible, Interval: 50s, Period: 1-7:00:00-24:00, Action: Remove. An 'Add' button is available.
- Timeout:** Global, Override, 3s
- History:** Do not store, Store up to, 31d
- Trends:** Do not store, Store up to, 365d
- Value mapping:** type here to search
- Populates host inventory field:** -None-
- Description:** (empty text area)
- Enabled:** checked

13. Interface de supervision final :

Maintenant que tout est en place dans notre parc informatique, notre interface de supervision finale ressemble à ceci, après quelques personnalisations :

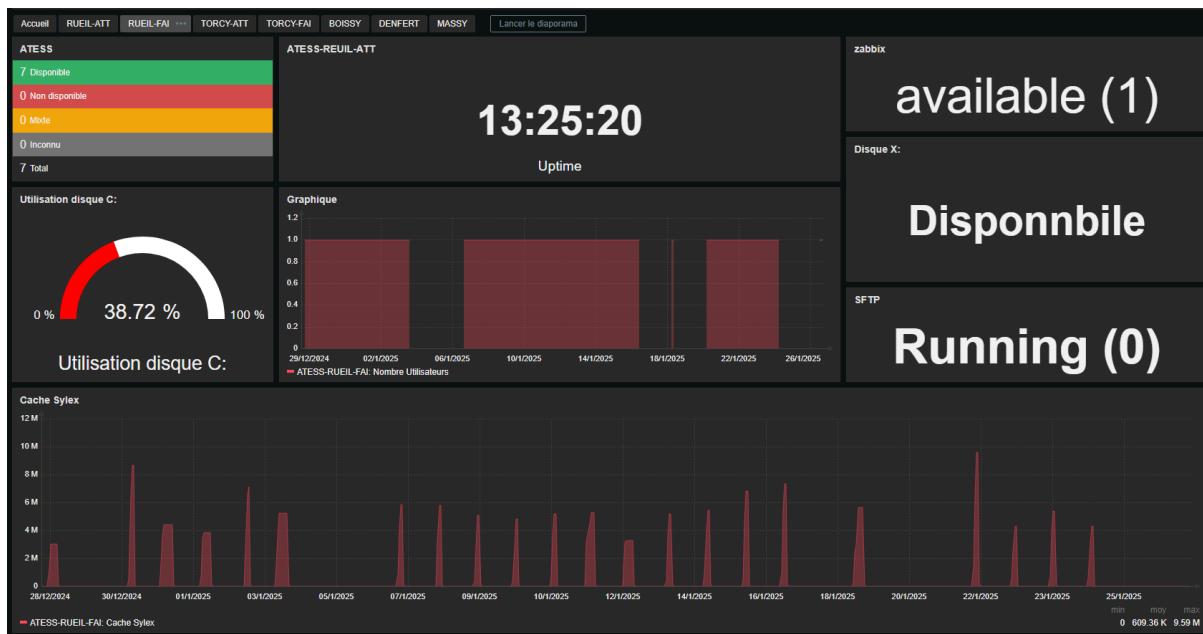


Cette page nous sert de page d'accueil. Elle nous permet, en un seul coup d'œil, de savoir s'il y a un problème sur l'une de nos baies.

Deux métriques sont particulièrement critiques dans notre cas :

- La disponibilité de la machine (est-elle UP ou DOWN ?).
- Le cache de l'application de transfert SFTP : s'il n'est pas vide, cela signifie qu'un ou plusieurs fichiers n'ont pas été transférés, ce qui indique un problème de transfert sur la machine.

Depuis ce dashboard, nous pouvons également naviguer entre différents onglets ou vues pour consulter des détails plus précis sur chaque machine.



Parmi les informations visibles, on retrouve :

- **L'espace disque C:** : utile à surveiller car ces machines sont utilisées par plusieurs opérateurs ; une saturation pourrait bloquer l'usage normal.
- Le temps d'uptime de la machine : cela nous permet de vérifier que la machine n'a pas été redémarrée anormalement ou qu'elle reste active sans interruption.
- Le nombre d'utilisateurs connectés : pour éviter toute action de maintenance pendant qu'un opérateur travaille, mais aussi pour détecter une éventuelle utilisation abusive (ces machines étant exclusivement réservées au vidage des boîtes noires ATESS).
- La présence du disque réseau X: (serveur SYLEX) : s'il est monté correctement, les transferts peuvent avoir lieu ; sinon, un dysfonctionnement est probable.
- Le bon fonctionnement du service de transfert SFTP sur la machine : élément critique pour assurer la disponibilité des données.
- **La taille du cache de l'application de transfert** : comme dit plus haut, un cache non vide est synonyme de fichier(s) bloqué(s) ou en attente, donc d'un transfert échoué ou non terminé.

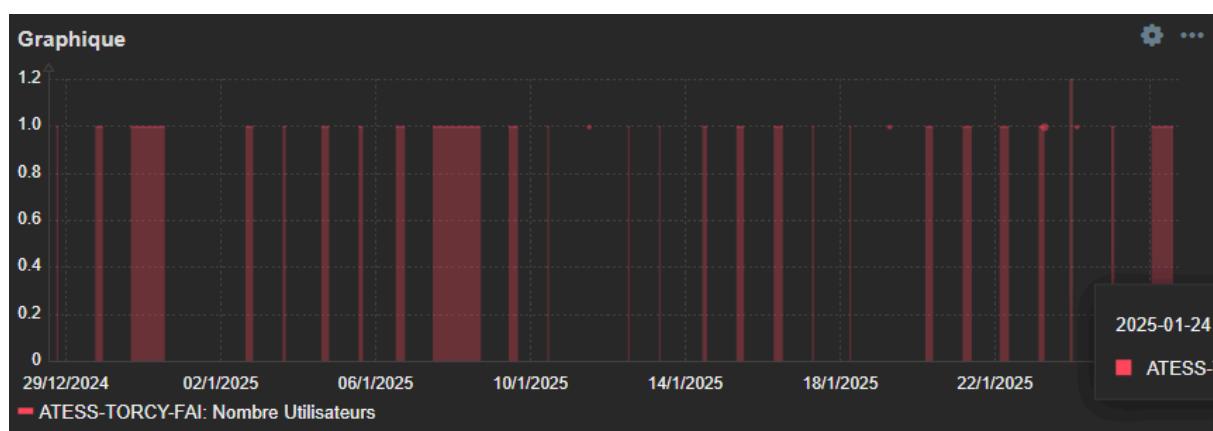
Grâce à cette interface personnalisée, nous avons une vue centralisée, synthétique et efficace sur l'état global de notre infrastructure dédiée au traitement et à la supervision des boîtes noires des RER.

14. réponse à incident, problème de transfert :

Dans cette première capture d'écran, nous pouvons observer que les graphiques liés aux utilisateurs connectés et au cache Sylex se sont correctement mis à jour sur la période observée. Ces courbes sont représentatives du fonctionnement habituel de nos baies ATESS :

- un cache qui se remplit en début de session lors du vidage des boîtes noires,
- puis qui se vide dans la journée, une fois les transferts réalisés vers le serveur SYLEX.

Concernant les utilisateurs connectés, nous constatons ici qu'un utilisateur est resté connecté pendant une période relativement longue. Cela peut être lié à la taille du graphique, qui compresse visuellement les durées. Voici ci-dessous un exemple plus classique de courbes concernant les connexions utilisateurs :



On y voit des connexions et déconnexions régulières, caractéristiques d'un usage normal des baies.

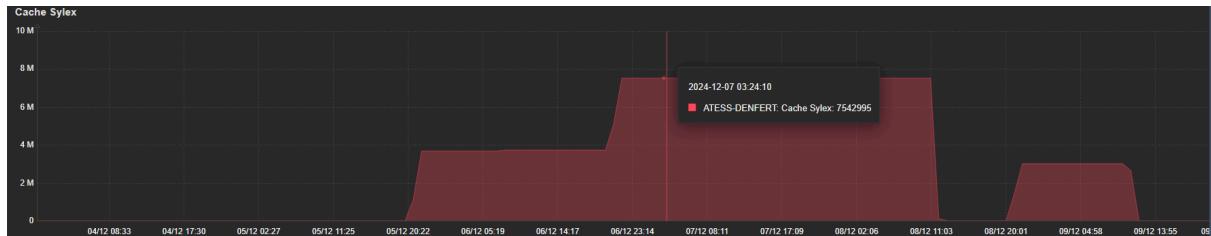
Étude de cas : incident du 4 au 10 décembre 2024

Lors de la semaine du **4 au 10 décembre 2024**, nous avons rencontré un incident de transfert critique sur plusieurs baies ATESS. Celui-ci est survenu à la suite d'une **mise à jour réseau** au sein de notre infrastructure.

Symptômes observés :

- Le dossier **cache** de l'application **SFTP Drive** sur les machines clientes se remplissait anormalement, sans jamais se vider ;
- Le serveur SYLEX ne recevait plus les fichiers de vidage, bien que la connexion semblait toujours active.

Voici un exemple représentatif de graphique durant cette période :

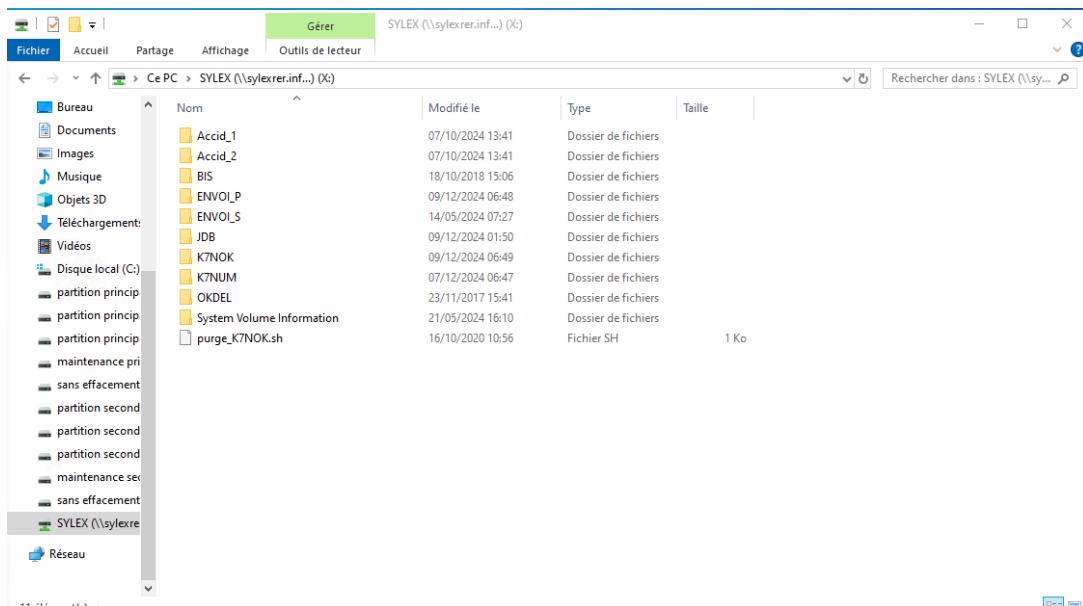


Analyse et diagnostic :

Dans un premier temps, le comportement a été pris pour un dysfonctionnement local. Toutefois, en observant que **plusieurs machines présentaient le même comportement**, nous avons écarté la piste d'une défaillance ponctuelle.

Deux hypothèses ont alors été explorées :

1. Défaillance de l'application SFTP Drive 2022
 - Analyse des journaux applicatifs : aucun message d'erreur critique, connexion toujours "établie", mais aucun transfert effectué.



2. Changement réseau impactant la session SFTP

→ Hypothèse d'un timeout réseau nouvellement appliqué (dans un objectif de sécurité), provoquant la fermeture silencieuse des connexions inactives.

Nom	Modifié le	Type	Taille
SftpDrive-2024-12-08	08/12/2024 23:59	Document texte	3 480 748 Ko
SftpDrive-2024-12-07	07/12/2024 23:59	Document texte	580 520 Ko
SftpDrive-2024-12-06	06/12/2024 23:59	Document texte	6 519 907 Ko
SftpDrive-2024-12-05	05/12/2024 23:59	Document texte	1 256 957 Ko
SftpDrive-2024-12-04	04/12/2024 23:59	Document texte	57 523 Ko
SftpDrive-2024-12-03	03/12/2024 23:59	Document texte	54 577 Ko
SftpDrive-2024-12-02	02/12/2024 23:59	Document texte	60 430 Ko
SftpDrive-2024-12-01	01/12/2024 23:59	Document texte	57 322 Ko
SftpDrive-2024-11-30	30/11/2024 23:59	Document texte	58 803 Ko
SftpDrive-2024-11-29	29/11/2024 23:59	Document texte	58 595 Ko
SftpDrive-2024-11-28	28/11/2024 23:59	Document texte	59 874 Ko
SftpDrive-2024-11-27	27/11/2024 23:59	Document texte	59 805 Ko
SftpDrive-2024-11-26	26/11/2024 23:59	Document texte	58 854 Ko
SftpDrive-2024-11-25	25/11/2024 23:59	Document texte	58 091 Ko
SftpDrive-2024-11-24	24/11/2024 23:59	Document texte	57 943 Ko
SftpDrive-2024-11-23	23/11/2024 23:59	Document texte	56 040 Ko
SftpDrive-2024-11-22	22/11/2024 23:59	Document texte	57 170 Ko
SftpDrive-2024-11-21	21/11/2024 23:59	Document texte	58 061 Ko
SftpDrive-2024-11-20	20/11/2024 23:59	Document texte	58 222 Ko
SftpDrive-2024-11-19	19/11/2024 23:59	Document texte	57 709 Ko
SftpDrive-2024-11-18	18/11/2024 23:59	Document texte	57 686 Ko
SftpDrive-2024-11-17	17/11/2024 23:59	Document texte	44 483 Ko
SftpDrive-2024-11-16	16/11/2024 23:59	Document texte	32 212 Ko
SftpDrive-2024-11-15	15/11/2024 23:59	Document texte	32 580 Ko
SftpDrive-2024-11-14	14/11/2024 23:59	Document texte	32 838 Ko
SftpDrive-2024-11-13	13/11/2024 23:59	Document texte	38 984 Ko
SftpDrive-2024-11-12	12/11/2024 23:59	Document texte	57 832 Ko
SftpDrive-2024-11-11	11/11/2024 23:59	Document texte	57 357 Ko
SftpDrive-2024-11-10	10/11/2024 23:59	Document texte	57 869 Ko
SftpDrive-2024-11-09	09/11/2024 23:59	Document texte	56 706 Ko
SftpDrive	09/12/2024 08:57	Document texte	2 520 827 Ko

Cette seconde piste a été confirmée après plusieurs tests. Bien que la session paraisse maintenue, les transferts échouaient silencieusement à cause de l'expiration imposée par les nouvelles règles réseau.

Résolution et actions correctives

Une fois la cause identifiée, liée à une mise à jour du réseau ayant introduit un timeout sur les connexions persistantes, nous avons mis en place une solution simple et efficace : automatiser le redémarrage quotidien des machines clientes.

Ce redémarrage quotidien permet de forcer la fermeture et la réinitialisation des connexions vers le serveur SFTP Sylex, de s'assurer que chaque nouvelle session de transfert part d'un état sain, sans dépendre d'une connexion antérieure

potentiellement interrompue, et de vider le cache local tout en relançant les processus internes de l'application SFTP Drive 2022.

Mise en œuvre technique

Pour cela, nous avons configuré une tâche planifiée Windows, présente sur chaque machine, qui déclenche un redémarrage automatique chaque jour à 4h00 du matin, heure à laquelle les utilisateurs ne sont normalement pas connectés.

Un script PowerShell a été mis en place avec les vérifications suivantes :

- Vérification qu'aucun utilisateur n'est actuellement connectés à la machine
- Envoi d'une notification en cas de session active, afin de permettre un report manuel du redémarrage si nécessaire
- Lancement sécurisé du redémarrage via shutdown /r /f

Cette mesure a permis de résoudre durablement les incidents de transfert liés à ce comportement réseau. Elle reste en place tant qu'aucune mise à jour de l'application SFTP Drive ou exception réseau spécifique n'est mise en œuvre.

4. Administration Sharepoint :

Dans le cadre de ma mission à la RATP, j'ai été chargé de l'implémentation et de l'administration d'un environnement SharePoint. Cette solution a été choisie pour centraliser et sécuriser la documentation critique du plan de continuité d'activité (PCA) lié aux Jeux Olympiques 2024, mais aussi pour structurer l'organisation documentaire des différents métiers du RER.

SharePoint est un outil de collaboration développé par Microsoft, qui permet de stocker, organiser, partager et accéder à des documents depuis n'importe quel appareil. Il est particulièrement adapté dans un contexte d'entreprise pour créer des espaces partagés entre différents métiers tout en maîtrisant les droits d'accès de manière fine et granulaire.

4.1 Structuration de l'environnement documentaire

L'une de mes premières tâches a été d'établir une architecture logique et fonctionnelle des bibliothèques et pages de contenu. L'objectif était de proposer

une interface claire, cohérente et adaptée aux besoins spécifiques des utilisateurs, tout en assurant la confidentialité des documents sensibles.

Pour cela, j'ai créé :

- Une page d'accueil servant de point d'entrée central pour les agents du RER ;
- Un tronc commun regroupant les documents transverses utiles à tous les métiers ;
- Trois pages dédiées aux fonctions clés du PCA (RH, Sécurité ferroviaire, Gestion circulation), permettant un cloisonnement logique et organisationnel.

Chaque page a été personnalisée pour accueillir les documents, procédures et informations spécifiques à la mission du métier concerné.

4.2 Gestion des accès et administration des droits

La gestion des droits dans SharePoint repose sur l'intégration avec l'Active Directory de l'entreprise. Cela permet de gérer les accès via des groupes de sécurité dynamiques, tout en maintenant une gouvernance claire.

j'ai mis en place une politique d'accès basée sur les rôles métiers. Chaque bibliothèque documentaire ou page spécifique n'est accessible qu'aux agents concernés. Les droits sont attribués selon plusieurs niveaux :

- Lecture seule pour les utilisateurs finaux ;
- Édition pour les référents de chaque métier ;
- Contrôle total pour les administrateurs SI, avec la possibilité de gérer les groupes, d'ajouter ou supprimer des membres, et de modifier la structure des pages.

j'ai aussi proposé la création d'un groupe d'administration SharePoint, avec des droits élargis pour les responsables métiers. Chaque référent peut ainsi gérer l'accès à sa propre documentation, tout en respectant les politiques de sécurité globales.

4.3 Bonnes pratiques mises en œuvre

Pour garantir la pérennité et la sécurité de l'environnement SharePoint, plusieurs bonnes pratiques ont été appliquées :

- Structuration claire des bibliothèques (nommage, arborescence simple) ;
- Mise en place de modèles de documents standardisés pour les procédures critiques ;
- Création d'un mode opératoire pour chaque administrateur métier (ajout d'un membre à un groupe, mise à jour d'un fichier, etc.) ;
- Présence de contacts sur chaque page en cas de problème d'accès ou de besoin d'assistance.

Cette approche a permis non seulement de sécuriser l'accès aux documents stratégiques, mais aussi de responsabiliser chaque métier dans la gestion de son propre espace SharePoint.

La mise en œuvre de cette solution SharePoint s'est révélée essentielle pour structurer efficacement les ressources critiques du PCA au sein du département RER. Elle a renforcé la résilience de l'organisation face à des incidents informatiques ou cyberattaques, tout en assurant une collaboration fluide et sécurisée entre les équipes. Grâce à cette centralisation et à la gestion fine des droits, chaque métier peut désormais accéder en toute autonomie aux informations dont il a besoin, sans risquer de compromettre la confidentialité ou l'intégrité des autres espaces.

5. Mise en place d'un plan de continuité d'activité (PCA) Plateforme SharePoint

5.1 Qu'est-ce qu'un PCA ?

Un plan de continuité d'activité (PCA) est un dispositif stratégique permettant à une organisation de maintenir ses fonctions essentielles en cas d'incident majeur, tel qu'une cyberattaque, une panne réseau, ou un dysfonctionnement critique des systèmes informatiques. L'objectif est d'éviter l'arrêt complet de l'activité et de garantir la continuité des services essentiels, en particulier dans les environnements sensibles comme les transports publics.

Dans le cadre de la RATP, et plus précisément du réseau RER, ce PCA vise à garantir la continuité des activités vitales permettant de faire circuler les trains, assurer la sécurité des voyageurs, et maintenir la coordination interne, même en situation de crise informatique.

5.2 Objectif du SharePoint "Ma Vie Sans le Digital"

Pour centraliser les informations nécessaires à la mise en œuvre du PCA, un espace SharePoint dédié a été conçu sous le nom "Ma Vie Sans le Digital" (MVSD). Cet espace est conçu pour rester accessible et opérationnel en cas de coupure ou de défaillance du système d'information, et pour permettre aux agents d'accéder rapidement aux procédures d'urgence adaptées à leur métier.

La page d'accueil de MVSD présente une organisation claire, permettant une navigation rapide vers les documents utiles, tout en respectant les règles de sécurité et de cloisonnement des accès.

Dans le cadre du projet de sécurisation informatique à la RATP, nous avons participé à la mise en place d'un plan de continuité d'activité (PCA) Cyber, permettant à certains services critiques de continuer à fonctionner même en cas de cyberattaque impactant le système d'information. Pour cela, un espace SharePoint dédié, nommé "Ma Vie Sans le Digital" (MVSD), a été conçu. Il regroupe toutes les ressources documentaires essentielles pour maintenir les activités de transport ferroviaire sur les lignes A et B.

Ce SharePoint a pour but d'offrir une interface claire et accessible, même en mode dégradé, permettant à chaque service de retrouver les procédures, les documents de secours et les consignes à appliquer en cas d'incident. L'ensemble est structuré de façon logique, en combinant une page centrale (tronc commun) et des pages spécifiques selon les métiers.

L'organisation repose sur deux principes clés : la centralisation de l'information et la gestion des accès sécurisés. Chaque métier critique dispose d'une page dédiée, visible uniquement par les groupes de sécurité correspondants. Les métiers identifiés comme prioritaires dans ce PCA sont :

- les Ressources Humaines (gestion des présences et du personnel en crise)
- la Gestion de la circulation (maintien de l'exploitation ferroviaire)
- le Contrôle de gestion (pilotage financier pendant la crise)
- l'Information voyageur (communication avec les usagers)
- la Sécurité ferroviaire (prévention des incidents et gestion des risques)

Ces pages métiers sont directement accessibles depuis la page d'accueil de MVSD. Chacune d'elles regroupe des documents spécifiques (PDF, fiches pratiques, tableaux de suivi) organisés dans des ressources documentaires structurées. Pour chaque métier, les documents sont classés par process afin de permettre une navigation rapide et efficace.

Sharepoint de RER Groupe privé
Bienvenu Administrateur CODIR Vigilance SST RER RPO Cyber PCA cyberattaque Gestion de flotte PSI Urbanisation Les projets Qualité PSG Retranscription audio Corbeille Modifier

Ma Vie Sans le Digital CYBERATTAQUE Plan de continuité d'activité

Si l'informatique RATP a été attaquée, en tout ou partie, l'exploitation de nos lignes A et B doit continuer et il faut être en mesure de reprendre les données après le retour à la normale.
Vous trouverez dans cette page les procédures de contournement spécifiques à vos métiers et les documents permettant la continuité puis la reprise des activités.

Accès à vos Plans de continuité d'activité en cas de cyberattaque

CODIR Ressources Humaines PFO - Contrôle de gestion SCE - Sécurité ferroviaire
Exploitation Information voyageur

Trucs et astuces Lien vers la page d'administration pour les droits d'accès aux différentes ressources
Ajouter une ressource dans le SharePoint Page d'administration Mode opératoire pour ajouter un utilisateur



Bienvenue sur l'espace SharePoint réservé aux interlocuteurs RH de la Ligne A. Vous pourrez ici faire une sauvegarde des documents pour le plan de continuité d'activité, mais aussi partager vos documents pour travailler de manière collaborative. Vous avez aussi la possibilité de partager des documents à l'ensemble des interlocuteurs de la communauté RH dans l'espace "transverse".

RH Ligne A				Afficher tout
+ Nouveau	Charger	Modifier en mode grille	Synchroniser	Exporter vers Excel
Nom	Modifié	Modifié par	montant	
PCA-CYBER	5 juillet 2024	QUEIFFELC Pierre-M	10	
Suivi activité Lignes Autxx	5 juillet 2024	QUEIFFELC Pierre-M	22	
Somme 32				

RH transverse				Afficher tout
+ Nouveau	Charger	Modifier en mode grille	Synchroniser	Exporter vers Excel

Une page d'administration a été mise en place pour permettre aux référents de chaque groupe de gérer les membres de leur groupe de sécurité. Cette page contient :

- des liens directs vers l'administration des groupes (via Active Directory)
- un mode opératoire pour ajouter ou retirer un utilisateur
- une fiche de contact à utiliser en cas de souci d'accès ou de demande de droits

Page d'administration

Voici la page d'administration des différents groupes de sécurité. Vous pourrez ici ajouter ou supprimer des utilisateurs dans vos groupes de sécurité respectifs.

Bonne navigation, et n'oubliez pas de regarder le **Mode OP** pour ajouter ou supprimer des personnes d'un groupes.

Mode OP administrateur :



Ajout utilisateur groupe
SharePoint.

✓ Mode OP pour Supprimer des utilisateurs à un groupe de sécurité SharePoint.

✓ Centre d'administration du groupes Administrateur PCA_Cyber

✗ Centre d'administration des groupes pour les RH



RH Centrales



RH LA



RH LB



L'organisation documentaire a été pensée en amont. Dès la racine, les documents sont séparés entre ressources communes et spécifiques. Cela permet de garantir que chaque utilisateur n'accède qu'aux informations utiles à son métier, sans surcharge visuelle.

Enfin, la mise en place de ce PCA sur SharePoint a nécessité de nombreuses réunions d'organisation, d'ateliers de tests utilisateurs et de vérifications de cohérence entre la documentation, les accès, et les processus métiers.

6. Mise en œuvre d'une infrastructure réseau simulée (projet DIVOC)

Contexte et objectifs

Dans le cadre de ma formation, j'ai participé à un projet visant à concevoir le cœur de réseau d'une entreprise fictive nommée DIVOC. Cette entreprise nouvellement implantée devait accueillir 13 employés, ainsi que divers périphériques réseau (NAS, imprimantes, téléphone IP). Le projet consistait à simuler une infrastructure réseau fonctionnelle et sécurisée à l'aide de l'outil Cisco Packet Tracer. L'objectif était de mettre en œuvre une topologie réseau complète avec :

- Un adressage optimisé
- Un serveur DHCP avec exclusions
- Un serveur DNS
- Un proxy simulé par ACL
- La gestion de la VoIP avec VLAN dédié

Plan d'adressage

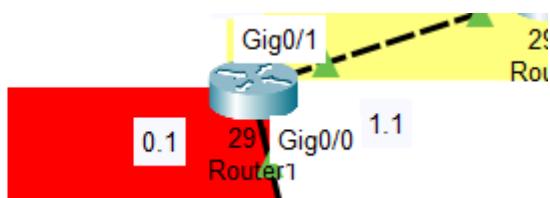
Après analyse, un plan d'adressage en /27 a été jugé optimal, car il permet d'accueillir jusqu'à 30 hôtes ($2^5 - 2 = 30$), couvrant les 13 employés et les 10 équipements prévus, avec une marge pour la croissance.

Configuration du serveur DHCP

Le serveur DHCP a été configuré directement sur le **Routeur 1**, en créant deux pools distincts :

- **POOL-DATA** pour les postes utilisateurs
- **POOL-VOIP** pour les téléphones IP

```
interface GigabitEthernet0/0
  no ip address
  ip access-group 1 in
  ip access-group 1 out
  duplex auto
  speed auto
```



Afin de répondre à la contrainte de réservation d'adresse IP pour certains équipements (NAS, imprimante, téléphone SIP), et en raison des limites de Packet Tracer, j'ai appliqué des exclusions manuelles pour simuler ces réservations.

Exemple de configuration DHCP :

```
ip dhcp pool DHCP
network 192.168.0.0 255.255.255.0
default-router 192.168.0.1
option 150 ip 192.168.0.1
dns-server 192.168.0.20
ip dhcp pool VOICE
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
option 150 ip 192.168.1.1
```

et voici les exclusions mise en place sur le DHCP :

```
ip dhcp excluded-address 192.168.0.1 GATEWAY VLAN 10
ip dhcp excluded-address 192.168.0.20 192.168.0.21 DNS + PRINTER
ip dhcp excluded-address 192.168.1.1 GATEWAY VLAN 20
ip dhcp excluded-address 192.168.1.2 SIP TELEPHONE IP
```

Mise en place du DNS

Un serveur DNS interne a été installé pour résoudre les noms internes. j'ai également configuré un sous-domaine spécifique pour le NAS (ex: nas.divoc.local).

Entrées configurées :

No.	Name	Type	Detail
0	gw	A Record	192.168.0.1
1	nas	A Record	172.16.0.10
2	pc0	A Record	192.168.0.3
3	pc1	A Record	192.168.0.4
4	printer	A Record	192.168.0.21
5	server	A Record	192.168.0.20
6	fesse.com	A Record	172.16.0.12
7	travail.com	A Record	172.16.0.11

Filtrage du trafic sortant (proxy simulé)

L'utilisation d'un proxy n'étant pas possible dans Packet Tracer, j'ai simulé cette fonctionnalité à l'aide d'Access Lists (ACLs) pour interdire l'accès à un site non autorisé (par exemple : xxx.com → 172.16.0.12).

Configuration de l'ACL :

```
access-list 1 deny host 172.16.0.12
access-list 1 permit any
```

VLAN VoIP et Data

Pour isoler la voix des données, j'ai mis en place deux VLAN :

- **VLAN 10** : Data
- **VLAN 20** : Voice

Configuration VLAN :

```
interface FastEthernet0/1
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/2
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/3
switchport mode access
switchport voice vlan 20
tx-ring-limit 20
!
interface FastEthernet0/4
switchport trunk allowed vlan 10,20
switchport mode trunk
!
interface FastEthernet0/5
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/6
switchport access vlan 10
switchport mode access
```

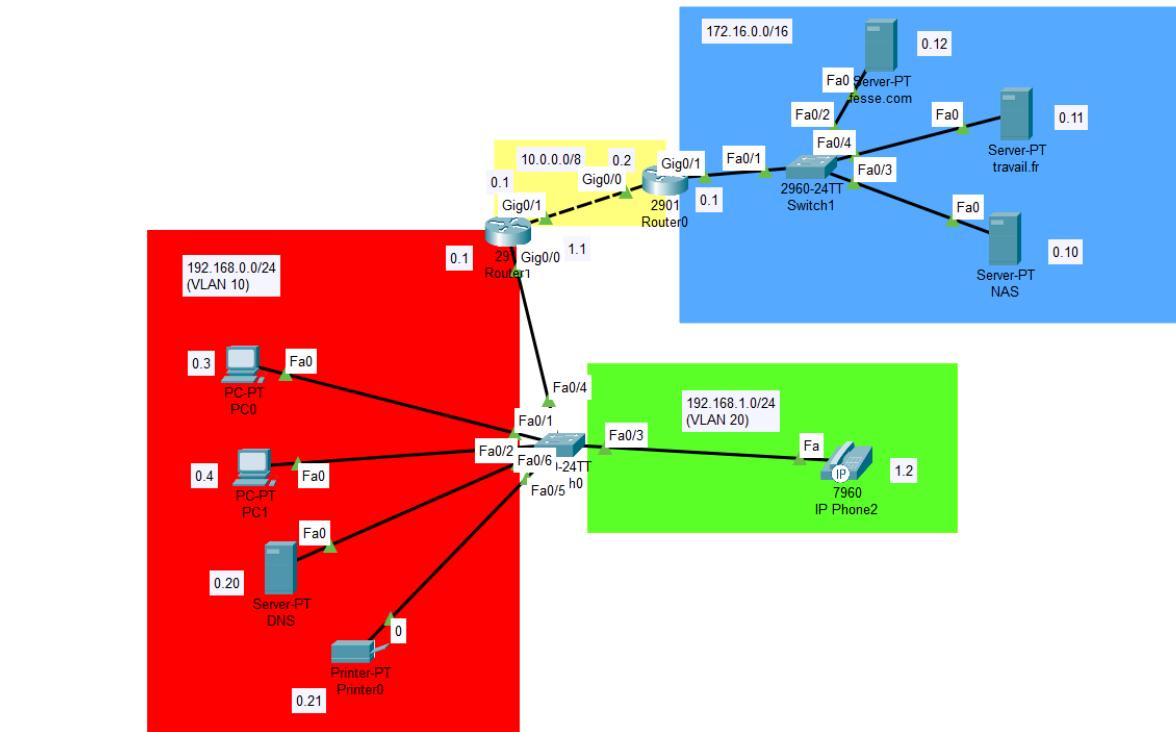
```

ip dhcp pool DHCP
  network 192.168.0.0 255.255.255.0
  default-router 192.168.0.1
  option 150 ip 192.168.0.1
  dns-server 192.168.0.20
ip dhcp pool VOICE
  network 192.168.1.0 255.255.255.0
  default-router 192.168.1.1
  option 150 ip 192.168.1.1

```

Résultat final

Le réseau permet une connectivité complète entre les postes clients, les services (DNS, DHCP, NAS), tout en appliquant des politiques de sécurité minimales (réservations IP, VLAN, filtrage). Le projet a permis de mettre en pratique des compétences réelles en administration réseau, en intégrant adressage IP, DHCP, DNS, VLAN, ACL, et gestion de la VoIP.



6. Conclusion

Au cours de ces deux années d'alternance à la RATP, j'ai pu mettre en pratique les compétences acquises durant ma formation, tout en développant une réelle autonomie sur des projets concrets et critiques pour l'entreprise. De la refonte de machines industrielles à la mise en place d'un plan de continuité d'activité, en passant par l'administration de plateformes collaboratives et la supervision d'infrastructures, chaque mission a contribué à enrichir mon expertise en administration et sécurisation des systèmes d'information.

Cette expérience m'a permis de mieux appréhender les enjeux liés à la cybersécurité, à la disponibilité des services informatiques et à la rigueur nécessaire dans la gestion d'infrastructures sensibles. Elle a aussi renforcé ma volonté de poursuivre dans le domaine de la sécurité des systèmes d'information, avec une attention particulière portée à la prévention des risques, à la résilience et à l'amélioration continue des environnements techniques.

Je suis aujourd'hui prêt à m'investir dans de nouveaux défis professionnels, en apportant mes compétences, ma curiosité, et ma capacité à apprendre rapidement au sein d'équipes techniques exigeantes et dynamiques.