Installation Poste informatique

Installation et préparation d’un poste informatique

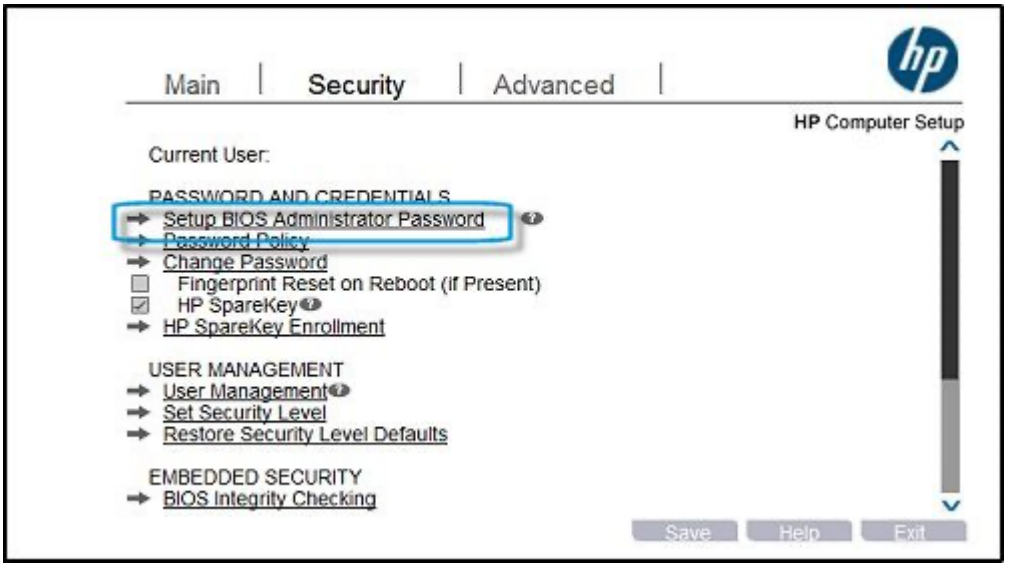
Contexte

Dans le cadre de mon alternance en tant que technicien support informatique, j’ai été amené à préparer et déployer des postes de travail destinés aux collaborateurs de l’entreprise. Afin d’optimiser le temps d’installation et de garantir une configuration homogène, l’entreprise utilise une solution de déploiement d’image système.

L’objectif de ce projet est de présenter l’installation complète d’un ordinateur portable, de la préparation de l’image jusqu’à la mise en production du poste utilisateur.

Pour commencer au moment du démarrage de l’ordinateur il faut que nous accédions au BIOS

Il faut maintenant que nous changions le mot de passe du BIOS pour plus de sécurité.



Une fois que le mot de passe BIOS est changé il faut déployer une image en PXE (il faut vérifier l'authentification sur le réseau de l’entreprise), concrètement, une image contient le **système d’exploitation** (par exemple Windows 11), les **logiciels installés** (comme Microsoft Office), les **paramètres système**, les mises à jour, les pilotes, et parfois certaines configurations réseau ou règles de sécurité. C’est donc un modèle prêt à l'emploi d'un ordinateur configuré selon les standards de l’entreprise.

Pour cela nous utilisons BMC Software

Architecture

Le système repose sur :

- Un serveur BMC : il centralise les images système, les packages logiciels et les tâches de déploiement.
- Un agent BMC installé sur les postes : il permet la communication entre le poste et le serveur.
- Un environnement de démarrage (PXE ou clé USB) pour les machines neuves.

Fonctionnement du déploiement

Le processus se déroule en plusieurs étapes :

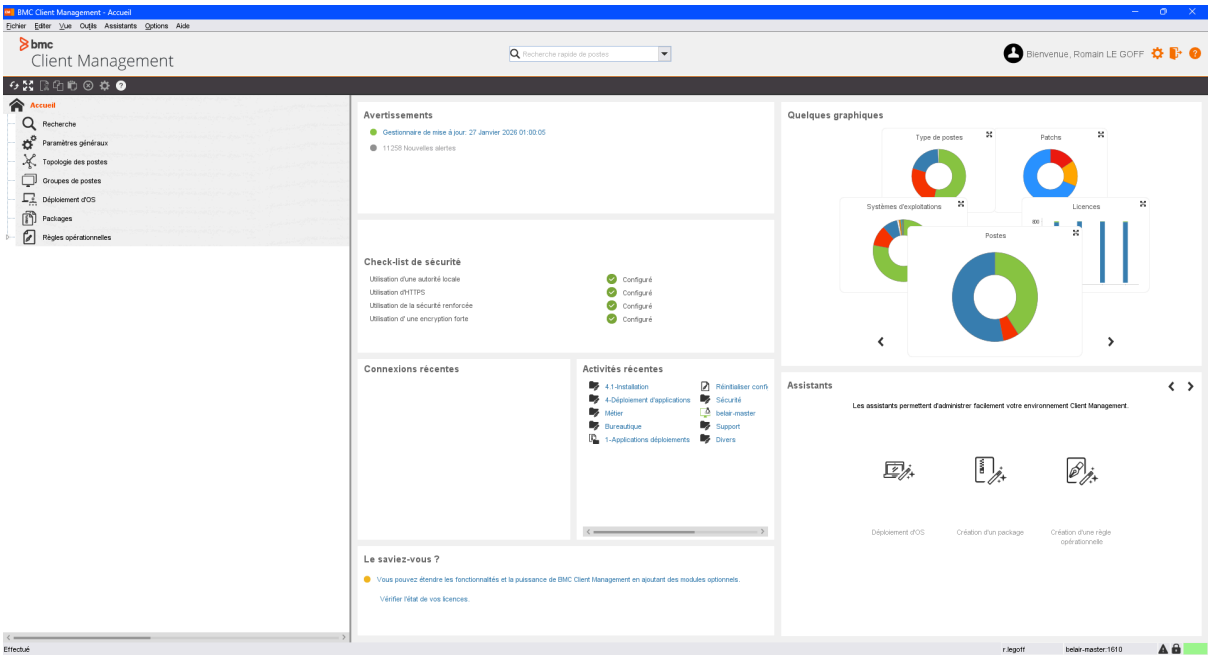
1. Le poste démarre via le réseau (PXE) ou un média boot.
2. Il charge un environnement de préinstallation.
3. Il contacte le serveur BMC.
4. Le serveur lui assigne une tâche de déploiement.
5. Le disque est automatiquement formaté et partitionné.
6. L'image système est copiée sur le poste.
7. Les pilotes et logiciels sont installés.
8. La machine est intégrée au domaine Active Directory.

Objectif principal

BMC permet :

- La standardisation des postes
- La réduction du temps d'installation
- La gestion centralisée du parc
- Une meilleure sécurité et traçabilité

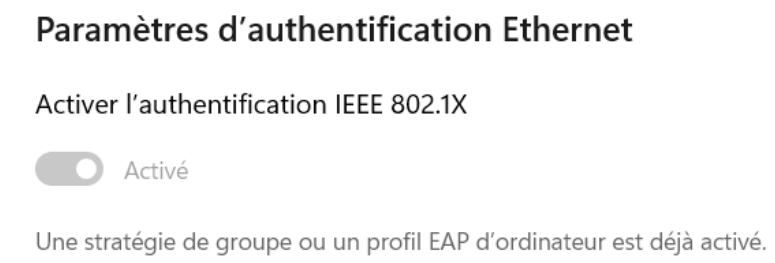
Application BMC :



Déploiement d'Image (actif/non actif) :

Windows-10-Pro-Redaction	Déploiement par installation	UEFI uniquement	Installation de Windows	1	1
Windows-10-Pro-Viamedia	Déploiement par installation	UEFI uniquement	Installation de Windows	1	1
Windows-10-Pro-Ventes	Déploiement par installation	UEFI uniquement	Installation de Windows	1	1
Windows-10-Pro-Commun	Déploiement par installation	UEFI uniquement	Installation de Windows	1	1
Windows-10-Pro-Eco	Déploiement par installation	UEFI uniquement	Installation de Windows	1	1
Windows-10-Pro-Comptabilite	Déploiement par installation	UEFI uniquement	Installation de Windows	1	1
Windows-11-Pro-Commun	Déploiement par installation	UEFI uniquement	Installation de Windows	1	3
Windows-11-Pro-Ventes	Déploiement par installation	UEFI uniquement	Installation de Windows	1	2
Windows-11-Pro-Redaction	Déploiement par installation	UEFI uniquement	Installation de Windows	1	3
Windows-11-Pro-Viamedia	Déploiement par installation	UEFI uniquement	Installation de Windows	1	1
Windows-11-Pro-Vierge	Déploiement par installation	UEFI uniquement	Installation de Windows	1	1
Windows-11-Pro-Comptabilité	Déploiement par installation	UEFI uniquement	Installation de Windows	1	1
Win11-Pro-24H2-07-25	Capture par image WIM	UEFI uniquement	Image WIM standard	1	2
W11-Prod-Deploy	Déploiement par image WIM	UEFI uniquement	Image WIM standard	1	1
Aomei_Backupper_Workstation	Déploiement personnalisé	UEFI uniquement	Image personnalisée	1	1

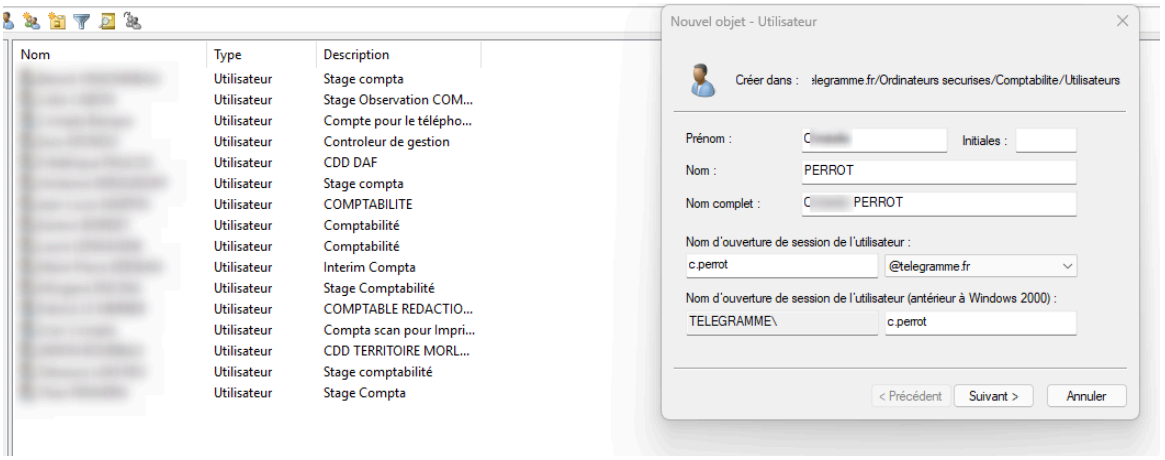
L’authentification **IEEE 802.1X** est un mécanisme de sécurité qui oblige un utilisateur ou un appareil à s’authentifier avant d’accéder au réseau (filaire ou Wi-Fi).
Lorsqu’un poste se connecte, l’accès est bloqué jusqu’à ce qu’un serveur d’authentification valide ses identifiants.
Ce système permet d’empêcher tout équipement non autorisé d’accéder au réseau de l’entreprise.



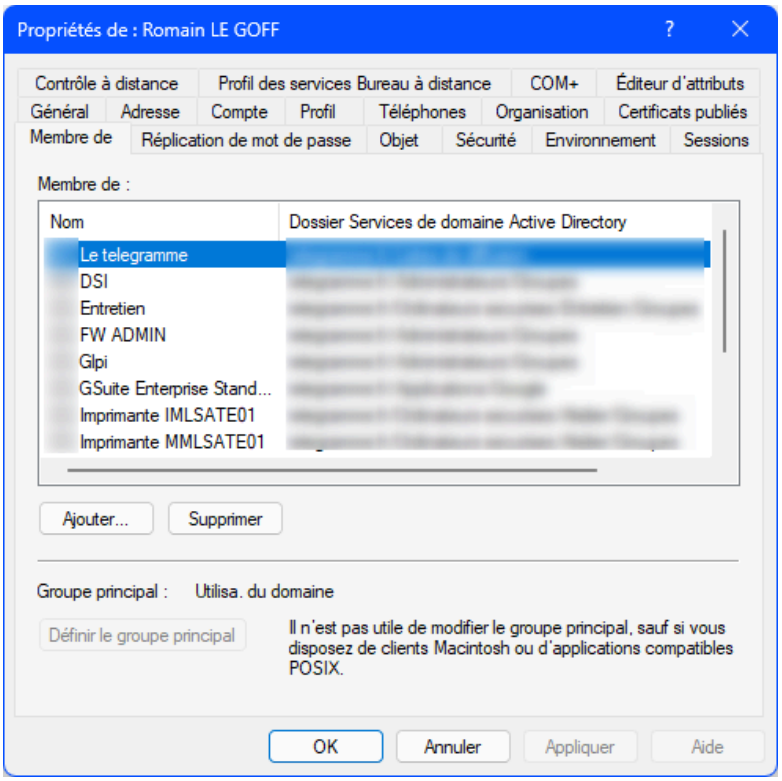
Vérifier la fonctionnalité des applications avec le compte de l’employé ensuite il reste à ajouter les imprimante en fonction du site auquel l’employé est rattaché pour ça il faut ajouter le compte utilisateur sur le groupe d’imprimante en particulier sur l’AD dans “membre de “.

Active Directory - arborescence

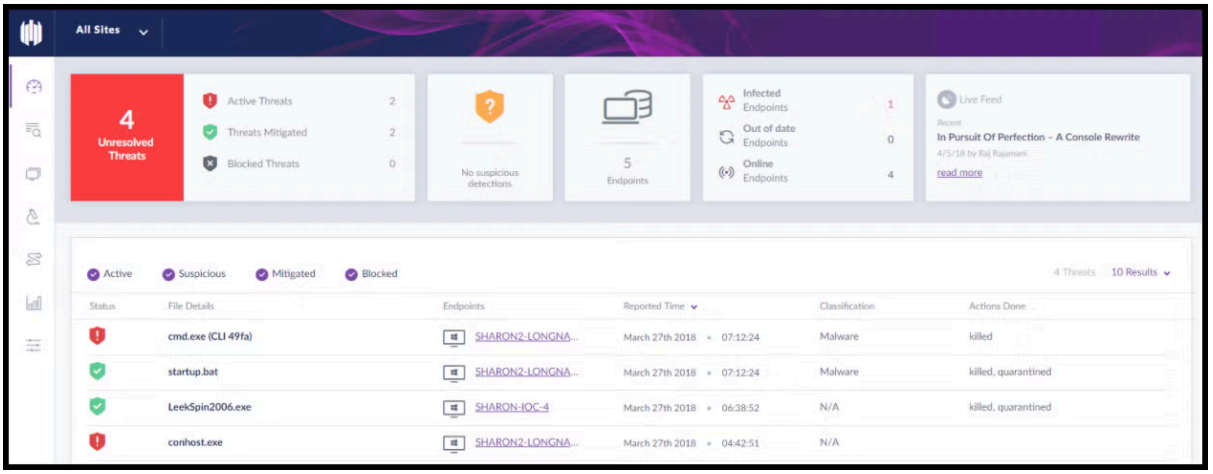
Exemple de création de compte dans l’AD



groupe attribué à un compte :



[Sentinelle One]



BMC Software

BMC Software

BMC Software est une entreprise américaine d'édition de logiciels d'entreprise spécialisée dans la gestion des services informatiques, l'automatisation et l'intelligence artificielle appliquée aux systèmes hybrides et mainframe. Basée à Houston (Texas), elle fournit des solutions à plus de 10 000 organisations dans le monde, dont la majorité des sociétés du Forbes Global 100.

Faits clés

- Fondation : 1980, Houston (États-Unis)
- Fondateurs : John J. Moores, Scott Boulette et Dan Cloer
- PDG : Ayman Sayed (depuis 2019)
- Propriétaire : KKR (depuis 2018, société non cotée)
- Effectif : ≈ 6 500 employés dans 40+ pays
- Chiffre d'affaires : ≈ 2,3 milliards USD (2024)

Historique et propriété

Créée par trois anciens ingénieurs de Shell, BMC Software s'est d'abord concentrée sur les outils d'optimisation pour ordinateurs IBM mainframe avant d'élargir son portefeuille à la gestion de services et à l'automatisation. Cotée au NASDAQ puis au NYSE de 1988 à 2013, elle a été privatisée par un consortium conduit par Bain Capital et Golden Gate Capital, puis acquise par le fonds KKR en 2018 pour environ 8 à 10 milliards USD .

Activités et produits

Les solutions de BMC couvrent deux grands segments : Enterprise Service Management (ESM) et Mainframe Service Management (MSM) .
Ses gammes phares incluent :

- BMC Helix : plateforme SaaS de gestion des services informatiques intégrant IA générative et automatisation.
- Control-M : orchestrateur de flux applicatifs multi-cloud.
- BMC AMI (Automated Mainframe Intelligence) : modernisation et sécurité des environnements mainframe.
  BMC Helix et AMI reposent sur des technologies AI-driven pour la supervision, la conformité et la cybersécurité des systèmes critiques.

Position de marché et innovations récentes

Présente dans plus de 40 pays et partenaire de grands acteurs comme Microsoft ou IBM, BMC a investi plus de 10 milliards USD en R&D depuis sa création . L'entreprise est reconnue par Gartner comme « Leader » du Magic Quadrant 2025 pour les plateformes d'orchestration et d'automatisation des services. En 2024-2025, KKR a annoncé une scission stratégique en deux entités — BMC (pôle mainframe et automatisation) et BMC Helix (pôle IA et services numériques) — afin d'accélérer la spécialisation sectorielle .

SentinelOne

SentinelOne

SentinelOne est une plateforme de cybersécurité autonome alimentée par l'intelligence artificielle, spécialisée dans la protection et la gestion des points d'extrémité (endpoints), des identités et des environnements cloud. Elle est conçue pour détecter, prévenir et répondre automatiquement aux menaces en temps réel grâce à l'analyse comportementale et à l'apprentissage automatique.

Faits clés

- Fondation : 2013
- Siège : Mountain View, Californie (États-Unis)
- PDG : Tomer Weingarten (cofondateur)
- Employés : Environ 3 000
- Produit principal : Plateforme Singularity XDR (Extended Detection & Response)

Technologie et fonctionnement

La plateforme Singularity de SentinelOne combine la prévention des menaces (EPP), la détection et réponse aux incidents (EDR/XDR), et la gestion centralisée des informations de sécurité (SIEM) dans une solution unifiée. Chaque point d'extrémité est protégé par un agent autonome capable d'identifier des comportements suspects sans dépendre de signatures préétablies, permettant une défense efficace contre les attaques de type ransomware, zero-day et les menaces persistantes avancées (APT).
Les modules incluent Singularity Endpoint (protection poste de travail), Singularity Cloud (sécurité des workloads et conteneurs) et Purple AI, un assistant d'analyse et de réponse basé sur l'IA générative.

Innovation et positionnement

SentinelOne a été reconnu à plusieurs reprises comme leader du Magic Quadrant™ de Gartner pour les plateformes de protection des endpoints et a obtenu des performances maximales dans les évaluations MITRE ATT&CK®, avec un taux de détection de 100 %. Son approche de la sécurité autonome vise à réduire le temps moyen de réponse (MTTR) tout en simplifiant les opérations des équipes de sécurité.

Adoption et impact

Adoptée par des organisations figurant parmi les Fortune 500 et des administrations publiques, SentinelOne offre une visibilité complète et des capacités de réponse automatisée. La solution aide les entreprises à renforcer leur résilience face à l'évolution rapide des cybermenaces, tout en diminuant les coûts opérationnels et la dépendance aux interventions humaines.

BIOS

BIOS

Définition

Le **BIOS** (Basic Input/Output System) est un microprogramme stocké sur la carte mère d’un ordinateur.

Son rôle principal est de **démarrer la machine** et de préparer le matériel avant le lancement du système d’exploitation (ex : Windows).

PXE

PXE

Le **PXE** (Preboot Execution Environment) est une technologie qui permet à un ordinateur de **démarrer via le réseau au lieu de démarrer sur son disque dur ou une clé USB**.
Autrement dit, le PC va chercher un système de démarrage directement sur un serveur, grâce à sa carte réseau.