

Mode opératoire (MOP) – Fabrication d'un poste de travail (Windows 11 22H2 via SCCM)

Objectif

Fabriquer un poste de travail "Macif" en déployant l'image Windows 11 22H2 via SCCM, puis vérifier le chiffrement BitLocker et la conformité du déploiement.

Périmètre

Postes de travail de l'entreprise intégrés au réseau interne et déployés via SCCM (OSD).

Prérequis

- Disposer d'un poste de travail "Macif" connecté au réseau interne de l'entreprise
- Avoir les habilitations nécessaires pour déclarer un poste de travail dans SCCM
- Avoir une clé USB disponible (support de démarrage)
- Utiliser un mini dock HP **USB-C** \rightarrow Ethernet / USB / HDMI) si la machine ne possède pas de port Ethernet

Procédure

1) Déclaration du poste dans SCCM (outil d'import)

1. Ouvrir l'outil d'import et renseigner les informations de profil nécessaires.
2. Sélectionner la collection de déploiement :
 - `C_Windows11_Deploiement_22H2`

Remarque : utiliser la version *Import-device* associée à la collection Windows 11 22H2

22H2. Emplacement :

- `\\groupe\app\PKG\Applications\MACIF\Import_Device\Import-Device_W11`

IMPORT DEVICE TO SCCM

MACIF Windows 11 Import Postes de Travail

SCCM Site : NAT CONNECT

Ajout Unitaire Ajout Multiple

Computer Name CXXXXXXXX

MAC Address 00:11:22:33:44:55

Environnement Production

Description

OU

Type de Poste Utilisateur

Profil Metier

Demarrage

Extinction

Collections de déploiement :

COLLECTION	DESCRIPTION
C_Windows11_Deploiement_22H2	Fabrication d'un poste de Travail Windows 11-22H2

RAZ AJOUTER

Cliquer sur Connect pour interroger l'infra SCCM

Connecte au site SCCM NAT

2) Déploiement de l'OS (boot USB + séquence de tâches)

1. Insérer la clé USB sur le poste à fabriquer.
2. Démarrer le poste et booter sur la clé USB.
3. Au menu de démarrage, sélectionner la séquence de tâches :
 - PROD_DEP_WKS_W11_PROFIL_22H2_V02
4. Suivre l'assistant jusqu'à la fin du déploiement.

Insérer capture : écran de sélection de la séquence de tâches.

The screenshot shows the 'Fin de Construction' (End of Construction) screen of the MACIF deployment wizard. It displays system information, domain details, and a list of installed applications.

Nom du Poste : C09507455

Modele : innotek GmbH - VirtualBox

N° Série : 0

Processeur : Intel(R) Core(TM) i7-6600U CPU @ 2.60GHz

Mémoire : 2Go **Disque :** 50 Go

Domaine : groupe.ad.macif.fr

OU : OU=H_DIT,OU=MACIF,OU=POSTES_DE_TRAVAIL_W10,OU=RESSOURCES,DC=groupe,DC=ad,DC=macif,DC=fr

Réseau : Intel(R) PRO/1000 MT Desktop Adapter - 10.245.12.46

Applications installées

Nom	Date Installation	Version
7-zip 64-bit	2019-11-18	9.20.0.0
360.TX	2019-11-18	4.00.0.000
Adobe Flash Player 32 NPAPI	2019-11-18	32.0.0.154
Autobase Reader 30 (11.0.20) ML1	2019-11-18	11.0.20
Agent d'administration de Kaspersky Security Center 10	2019-11-18	10.5.1761
Agent d'administration de Kaspersky Security Center 10	2019-11-18	10.5.1761
Backup - e Vintatation	2019-11-18	3.2.0.2234
Citrix Authentication Manager	2019-11-18	7.0.0.5249

Fin de Construction Appuyer sur Echap ou cliquer pour redémarrer

Point d'attention : l'installation est considérée finalisée lorsque la bannière (Wizard) "Fin de Construction" apparaît. Il est impératif de cliquer ou d'appuyer sur la touche « ECHAP » pour que le poste soit complètement terminé.

3) Vérification BitLocker (chiffrement)

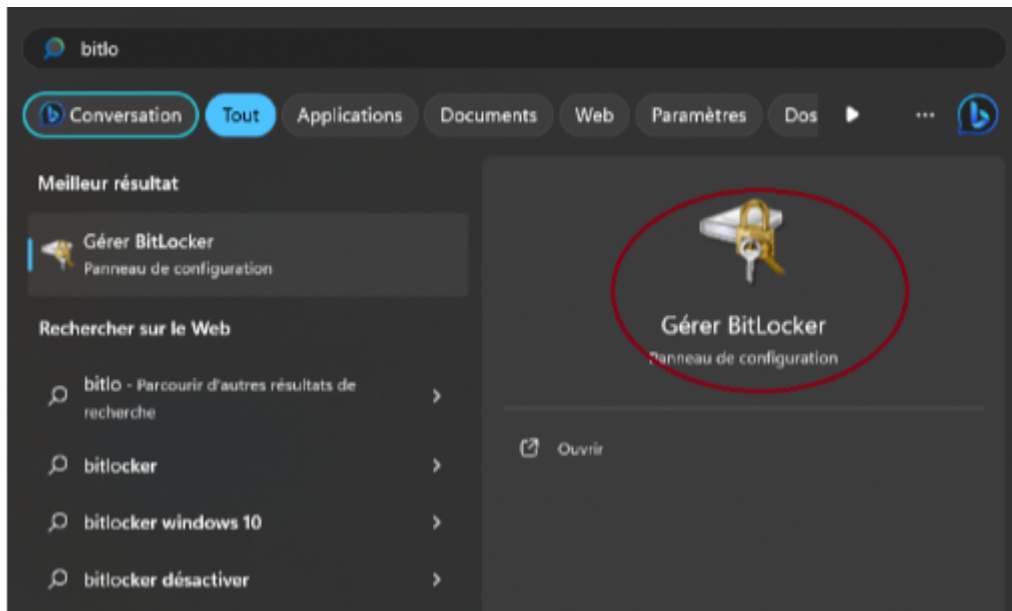
Le chiffrement BitLocker doit être actif sur le système. Deux méthodes de vérification :

- Via l'interface BitLocker (menu Démarrer), vérifier que le chiffrement est activé
- Via PowerShell, exécuter :
Get-BitLockerVolume | Format-List

Get-BitLockerVolume | Format-List

Puis vérifier que le champ `ProtectionStatus` est à On

exemple de sortie PowerShell / écran BitLocker.



de [Chiffrement de lecteur BitLocker](#)
Protégez vos fichiers et dossiers contre l'accès non autorisé en protégeant vos lecteurs avec BitLocker.

Lecteur du système d'exploitation

Windows (C:) BitLocker activé



- Suspendre la protection
- Modifier le mode de déverrouillage du lecteur au démarrage
- Sauvegarder votre clé de récupération
- Désactiver BitLocker

Lecteurs de données fixes

Lecteurs de données amovibles - BitLocker To Go

Insérez un lecteur flash USB amovible pour utiliser BitLocker To Go.

4) Rapport de conformité SCCM (contrôle post-déploiement)

1. Vérifier la présence du rapport dans le répertoire partagé :

- \\groupe\exploitation\conf\sccm\osd

2. Le fichier généré est nommé :

- NOM_DU_POSTE_DATE_CREATION-Heure.html

3. Exemple :

- C07211560_20220420-0945.html

Contenu du rapport : récapitulatif système, éléments SCCM utilisés, contrôle de conformité des applications socle. Si un ou plusieurs pilotes sont en erreur, ils apparaissent en rouge.

Informations générales

Propriété	Valeur
Sequence de tâche	PROD_DEP_WKS_W11_PROFIL_22H2_V02
Type de Media	BootMedia
Mode d'Installation	UFD
Numéro de Serie	S4EB8059
MAC	6C:4B:90:2F:DB:74
IP	10.233.149.127
Constructeur	LENOVO
Modele	10MQS77P00 - ThinkCentre M710q

Applications Runtime

Nom Application
Microsoft_Visual_C++_2005
Microsoft_Visual_C++_2008
Microsoft_Visual_C++_2010
Microsoft_Visual_C++_2012
Java(TM)_6
Java_7
Java_8

Applications Requises de Base - Macif

Application necessaire	Application trouvee
Adobe_Acrobat Reader DC_22.003.20322_01	Acrobat Reader DC
Citrix_Workspace_22.3.1000.1054_01	Workspace
Google_Chrome_100.0.4896.60_01	Google_Chrome
Igor Pavlov_7-Zip_22.01-x64_02	7-Zip
Ivanti_Secure Access Client_22.2_01	Ivanti Secure Access Client 22.2
Macif_Configuration_802.1x_04	802.1x
Macif_Configuration_Energie_02	Configuration_Energie
Macif_Disable_Features_Services_01	Macif_Disable_Features_Services
Macif_Disable_Tasks_01	Macif_Disable_Tasks
Macif_GPO_Locale_01	Macif_GPO_Locale

Résultat attendu (critères de réussite)

- Poste déclaré dans la bonne collection SCCM
- Windows1122H2
- *Windows1122H2*
- Déploiement terminé et sortie correcte via « ECHAP » à la fin de construction
- BitLocker actif avec `ProtectionStatus = On`
- Rapport de conformité présent au bon emplacement et sans erreurs bloquantes