



A collage of various paper scraps pinned to a brown background with pushpins. The scraps include a white spiral-bound page, a yellow page with a scalloped edge, a yellow page with a red wavy line, a white page with horizontal stripes, and a yellow page with a blue pushpin. The overall aesthetic is a mix of personal notes and found papers.

**MDT, WHERE ARE  
YOU ?**

Guillaume DAUMAS - @BlWasp-  
Auditeur chez Advens   
• TI interne  
• Red Team

whoami /all

## Projets parallèles

- Auteur de cheatsheets AD / AD - Python / ADCS / SCCM / Pivoting
- Participant au projet The Hacker Recipes de Shutdown (@\_nwodtuhs)
- GitHub : BlackWasp, quelques projets et PRs (Impacket, CME / NXC, Responder ...)



# MDT, c'est quoi ?

D'après Microsoft :

*“MDT is a unified collection of tools, processes, and guidance for automating desktop and server deployment. You can use it to create reference images or as a complete deployment solution. MDT is one of the most important tools available to IT professionals today.”*

**En gros, c'est une version allégée et gratuite de SCCM**

# Background

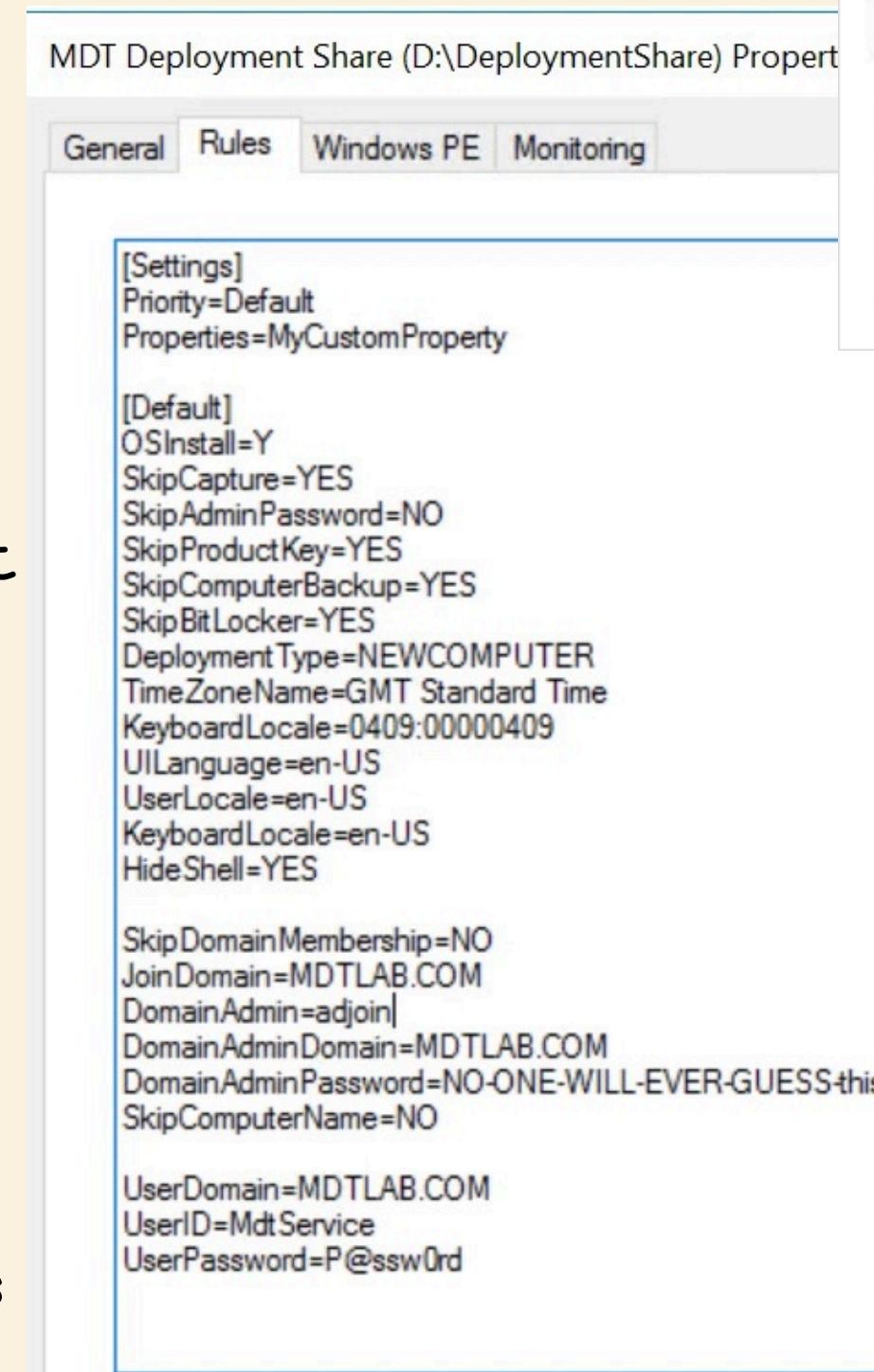
TrustedSec a publié un article de blog très intéressant sur les partages MDT

Microsoft Deployment Toolkit (MDT) est souvent négligé par rapport à SCCM.

Il stocke fréquemment des informations d'identification **en clair** dans les fichiers de configuration, notamment dans **Bootstrap.ini** et **CustomSettings.ini**.

Partages mal configurés : accès trop permissif !

Les identifiants trouvables ( DomainAdmin, AdminPassword,...) peuvent faciliter la compromission du domaine ou les mouvements latéraux.



```
MDT Deployment Share (D:\DeploymentShare) Properties  
General Rules Windows PE Monitoring  
[Settings]  
Priority=Default  
Properties=MyCustomProperty  
[Default]  
OSInstall=Y  
SkipCapture=YES  
SkipAdminPassword=NO  
SkipProductKey=YES  
SkipComputerBackup=YES  
SkipBitLocker=YES  
DeploymentType=NEWCOMPUTER  
TimeZoneName=GMT Standard Time  
KeyboardLocale=0409:00000409  
UILanguage=en-US  
UserLocale=en-US  
KeyboardLocale=en-US  
HideShell=YES  
SkipDomainMembership=NO  
JoinDomain=MDTLAB.COM  
DomainAdmin=adjoin  
DomainAdminDomain=MDTLAB.COM  
DomainAdminPassword=NO-ONE-WILL-EVER-GUESS-this-password-1234!  
SkipComputerName=NO  
UserDomain=MDTLAB.COM  
UserID=Mdt Service  
UserPassword=P@ssw0rd
```



## Red Team Gold: Extracting Credentials from MDT Shares

First you setup a Windows server and then you simply download the MSI installation from the Microsoft page and run it. In addition, you need to install the Windows ADK. Once everything is installed, you fire up the...

TrustedSec

Edit Bootstrap.ini

# ok, mais du coup, ils sont où ces partages ?

En général, lorsque des services sont déployés dans un Active Directory, des opérations LDAP sont effectuées afin de configurer des attributs, des conteneurs, etc.

Le plan est donc :

- déployer un serveur MDT
- surveiller toute l'activité LDAP afin de trouver des éléments qui pourraient être ciblés lors d'une reconnaissance.

# LDAPMonitor

Outil développé par  
@podalirius\_

Permet de moniterer toute  
l'activité LDAP en temps  
réel

<https://github.com/p0dalirius/LDAPmonitor>

## installation WDS

Microsoft **WDS** (Windows Deployment Services) est un rôle de serveur permettant de faciliter le déploiement en réseau des systèmes d'exploitation Windows.

Il permet de déployer des images à l'aide du démarrage PXE (Preboot Execution Environment).

Dans le cas d'un serveur MDT, le rôle WDS est primordiale pour le déploiement d'images !

On tape ces commandes

Et les opérations LDAP suivantes apparaissent

```
PS C:\> Install-WindowsFeature -Name WDS -IncludeManagementTools  
PS C:\> WDSUTIL.exe /Verbose /Progress /Initialize-Server /Server:MDTServer /RemInst:"C:\RemoteInstall"  
PS C:\> WDSUTIL.exe /Set-Server /AnswerClients:All
```

```
[2025-06-27 13:51:43] 'CN=MDTSERVER-Remote-Installation-Services,CN=MDTSERVER,CN=Computers,DC=lab,DC=local' was added.  
[2025-06-27 13:51:43] CN=MDTSERVER,CN=Computers,DC=lab,DC=local  
| Attribute "netbootSCPBL" = '['CN=MDTSERVER-Remote-Installation-Services,CN=MDTSERVER,CN=Computers,DC=lab,DC=local']'  
[2025-06-27 13:53:06] CN=MDTSERVER-Remote-Installation-Services,CN=MDTSERVER,CN=Computers,DC=lab,DC=local  
| Attribute "whenChanged" changed from '2025-06-27 11:51:00+00:00' to '2025-06-27 11:52:57+00:00'  
| Attribute "uSNChanged" changed from '28758' to '28760'  
| Attribute "netbootAnswerRequests" changed from 'False' to 'True'
```

Un nouveau conteneur, nommé MDTSERVER-Remote-Installation-Services, est ajouté sous le conteneur de serveur MDTSERVER.

# En vérifiant de plus près

Un nouvel attribut 'netbootServer' est aussi apparu

## Et un partage REMINST

The screenshot displays three windows related to MDT configuration:

- Left Window (Shares):** Shows a list of shares. One share, "REMINST" located at "C:\Remotelinstall" with protocol "SMB" and availability "Not Clustered", is highlighted.
- Middle Window (Active Directory):** Shows the LDAP browser. A connection to "CN=MDT SERVER-Remote-Installation-Services" is selected. The "CN=Computers" container is expanded, showing "CN=MDT SERVER". This node is highlighted with a red box.
- Right Window (Attribute Editor):** A modal dialog titled "CN=MDT SERVER-Remote-Installation-Services Properties" shows the "Attribute Editor" tab. It lists an attribute named "netbootServer" with the value "CN=MDT SERVER,CN=Computers,DC=lab,DC=local".

# Et de nouvelles interfaces RPC

```
$ rpcdump.py LAB/B1Wasp:'Password123!'@'192.168.56.20' |grep -i WDS -A 5 -B 5
```

```
UUID      : D4051BDE-9CDD-4910-B393-4AA85EC3C482 v1.0
```

```
Bindings:
```

```
ncalrpc:[LRPC-5433bff7016b7e884b]
```

```
ncalrpc:[OLE6B13C9DAA4D10A03B4288A5131B1]
```

```
Protocol: [MS-WDSC]: Windows Deployment Services Control Protocol
```

```
Provider: wdssrv.dll
```

```
UUID      : 1A927394-352E-4553-AE3F-7CF4AAFCA620 v1.0
```

```
Bindings:
```

```
ncacn_ip_tcp:192.168.56.20[5040]
```

```
Protocol: [MS-FASP]: Firewall and Advanced Security Protocol
```

# Installation de MDT

Lors du déploiement de MDT, aucune nouvelle opération LDAP apparaît

En revanche, plusieurs comptes de services sont nécessaires :

- Le compte de compilation MDT est utilisé pour l'environnement de préinstallation Windows (Windows PE) afin de se connecter au serveur MDT
- Un deuxième compte de service est mentionné dans la documentation : utilisé pour ajouter les nouvelles machines à Active Directory

```
PS C:\> New-ADUser -Name MDT_BA -UserPrincipalName MDT_BA -path "CN=Users,DC=LAB,DC=LOCAL" -Description "MDT Build Account"
```

```
PS C:\> New-ADUser -Name MDT_JD -UserPrincipalName MDT_JD@lab.local -path "CN=Users,DC=LAB,DC=LOCAL" -Description "MDT joï"
```

# Installation de MDT

Lors du déploiement de MDT, aucune nouvelle opération LDAP apparaît

Et des partages spécifiques à MDT sont nécessaires : **logs**, et partages contenant les images

Pour le deuxième, le nom par défaut est **DeploymentShare\$**, mais la documentation propose **MDTProduction\$**

```
$ nxc smb 192.168.56.20 -u BlWasp -p Password123! --shares
SMB      192.168.56.20  445    MDTSERVER          [*] Windows Server 2022 Build 20348 x64 (name:MDTSERVER) (domain:lab.)
SMB      192.168.56.20  445    MDTSERVER          [+] lab.local\BlWasp:Password123!
SMB      192.168.56.20  445    MDTSERVER          [*] Enumerated shares
SMB      192.168.56.20  445    MDTSERVER          Share           Permissions        Remark
SMB      192.168.56.20  445    MDTSERVER          -----          -----
SMB      192.168.56.20  445    MDTSERVER          ADMIN$           Remote Admin
SMB      192.168.56.20  445    MDTSERVER          C$              Default share
SMB      192.168.56.20  445    MDTSERVER          DeploymentShare$   MDT Deployment Share
SMB      192.168.56.20  445    MDTSERVER          IPC$             READ            Remote IPC
SMB      192.168.56.20  445    MDTSERVER          Logs$            READ,WRITE
SMB      192.168.56.20  445    MDTSERVER          REMINST         READ            Windows Deployment Services Share
```

## Réponse

# Ldeep

Idée principale:

Trouver le serveur WDS !

<https://github.com/franc-pentest/ldeep>

WDS est nécessaire pour MDT

1. L'installation de ce service crée un nouveau noeud sous le conteneur du serveur : CN=MDTSERVER-Remote-Installation-Services

2. Avec une classe d'objets spécifique : intellimirrorSCP.

Les serveurs WDS peuvent être utilisés à d'autres fins que les partages MDT !

Egalement utilisés dans les environnements SCCM pour les serveurs de point de distribution et PXE.

# Recherche du classObject Spécifique

```
$ pdm run ldeep ldap -u BlWasp -p Password123! -d LAB.LOCAL -s 192.168.56.10 search '(objectclass=intelliMirrorSCP)'

[{
    "cn": "MDT SERVER-Remote-Installation-Services",
    "dSCorePropagationData": [
        "1601-01-01T00:00:00+00:00"
    ],
    "distinguishedName": "CN=MDT SERVER-Remote-Installation-Services,CN=MDT SERVER,CN=Computers,DC=lab,DC=local",
    "dn": "CN=MDT SERVER-Remote-Installation-Services,CN=MDT SERVER,CN=Computers,DC=lab,DC=local",
    "instanceType": 4,
    "name": "MDT SERVER-Remote-Installation-Services",
    "netbootAllowNewClients": true,
    "netbootAnswerOnlyValidClients": false,
    "netbootAnswerRequests": true,
    "netbootCurrentClientCount": 0,
    "netbootLimitClients": false,
    "netbootMaxClients": 100,
    "netbootNewMachineNamingPolicy": [
        "%61Username%#"
    ],
    "netbootNewMachineOU": "CN=MDT SERVER,CN=Computers,DC=lab,DC=local",
    "netbootServer": "CN=MDT SERVER,CN=Computers,DC=lab,DC=local",
```

# wDSFinder

- Permet de rechercher tous les serveurs WDS via LDAP avec ldap3
- Liste les partages SMB de chaque serveur identifié avec smbclient

<https://github.com/BIWasp/WDSFinder>

- Outil développé en Rust
- Cross-platform
- Gère la signature LDAP et le Channel Binding LDAPS
- Authentification SImple Bind et Kerberos GSSAPI



**BIWasp/WDSFinder: A simple tool to identify WDS servers in Active Directory**

A simple tool to identify WDS servers in Active Directory - BIWasp/WDSFinder

GitHub

# Outils et lien

PR ldeep : <https://github.com/franc-pentest/ldeep/pull/139>

WDSFinder : <https://github.com/BlWasp/WDSFinder>

TrustedSec : <https://trustedsec.com/blog/red-team-gold-extracting-credentials-from-mdt-shares>

HideAndSec : <https://hideandsec.sh/books/windows-sNL/page/mdt-where-are-you>

Any  
Questions?