## Audit de la gestion des comptes utilisateurs AD sur le contrôleur de domaine

Ouvrez la gestion des stratégies de groupe et sélectionnez la GPO « Default Domain Controllers Policy ».

| Gestion de stratégie de groupe          | Default Domain Controllers Policy   |                                |  |  |  |  |
|---|---|--------------------------------|--|--|--|--|
| A Forêt: learn.local                    | Barrier Direct Description Delivery But   |                                |  |  |  |  |
| v 🚠 Domaines                            | territor Debes Paranetes Deegenn ina  |                                |  |  |  |  |
| v (j) isem.local                        | Liaisons  |                                |  |  |  |  |
| Default Domain Policy                   | Alfohen ins laavons à oot explorement : Jaan local<br>Les stes, domaines et untée d'organisation suivants sont liés à cet daget GPO : |                                |  |  |  |  |
| > Domain Controllers                    |   |                                |  |  |  |  |
| 👻 🔟 lyon                                | Enderson A Robert Harvert   | Danie Junie                    |  |  |  |  |
| > 🛋 Achat                               | Emplacement Apprique Lien active  | Unemen d'acces                 |  |  |  |  |
| > Z Direction                           | Comain Controllers Non Qui  | learn.local/Domain Controllers |  |  |  |  |
| > informatique                          |   |                                |  |  |  |  |
| Production                              |   |                                |  |  |  |  |
| > 🖆 Marseille                           |   |                                |  |  |  |  |
| 🗸 🌍 Objets de stratégie de groupe       |   |                                |  |  |  |  |
| i audit                                 |   |                                |  |  |  |  |
| Default Domain Controllers Policy       |   |                                |  |  |  |  |
| Default Domain Policy                   |   |                                |  |  |  |  |
| Dossier partagé Achat                   |   |                                |  |  |  |  |
| Gestion de compte                       |   |                                |  |  |  |  |
| info_DP                                 |   |                                |  |  |  |  |
| Nouvel objet de stratégie de groupe     | <u></u>   |                                |  |  |  |  |
| Panneau de configuration                | Filtrage de sécurité  |                                |  |  |  |  |
| text aplication                         | Les paramètres dans ce GPO s'appliquent uniquement aux groupes, utilisateurs et ordinateurs suivants :                                |                                |  |  |  |  |
| > Fritres WMI                           |   |                                |  |  |  |  |
| > Califier OPO Starter                  | Non   |                                |  |  |  |  |
| ) 🙀 Mes                                 | St. Utisateurs authentifics   |                                |  |  |  |  |
| (g) Modelisation de stratégie de groupe |   |                                |  |  |  |  |
| Résultats de strategie de groupe        |   |                                |  |  |  |  |

Activez l'audit de la gestion des comptes utilisateurs en la modifiant pour cocher la case "Succès".



Dans l'Observateur d'événements, vérifiez que l'utilisateur a été correctement créé avec l'ID 4720.

|   | and 1 bland in  | THE MAY WART I WITH MAY   |  | menant minera accurg was  | No. 4  | The same excession managements   |
|---|---|---|--|---|--|--|
| Succès :  | de l'audit  | 16/05/2024 16:40:09   |  | Microsoft Windows security audit  | 6  | 4738 User Account Management   |
| Succès  | de l'audit  | 15/05/2024 16:40:08   |  | Microsoft Windows security audit  | ti   | 4720 User Account Management   |
| Succès  | de l'audit  | 16/05/2024 16:38:25   |  | Microsoft Windows security audit  | 6  | 4719 Audit Policy Change   |
| Événement   | t 4720, Microsoft Windows s   | ecurity auditing.   |  |   |  |  |
| Général   | Détails   |   |  |   |  |  |
| Un con<br>Sujet :   | ID de sécurité :<br>Nom du compte :<br>Domaine du compte :<br>D d'ouverture de session  | LEARN\Administrateur<br>Administrateur<br>LEARN<br>0x20E10B   |  |   |  |  |
| Nouve<br>Attribu  | au compte :<br>ID de sécurité :<br>Nom du compte :<br>Domaine du compte :<br>ts :<br>Nom du compte SAM :<br>Nom compte :<br>Nom compte :  | LEARN/kestaudit<br>testaudit<br>LEARN<br>testaudit<br>testaudit<br>war : hestaudit@lear   | n local  |   |  |  |
| Journal   | : Sécurité<br>Microsoft Windows   | security Connecté: 1  | 6/05/2024 16:40:08   |   |  |  |
| Événem<br>Niveau :  | ent: 4720<br>Information  | Catégorie : U<br>Mots-clés : S  | Jser Account Management<br>auccès de l'audit                       |   |  |  |
| Source :<br>Événem<br>Niveau :  | ent: 4720<br>Information  | Catégorie : U<br>Mots-clés : S  | lser Account Management<br>luccés de l'audit                       | launa.  | Datation   | Calculation and Annual   |
| Source :<br>Événem<br>Niveau :<br>Mats clés   | ent: 4720<br>Information  | Catégorie : U<br>Mots-clés : S<br>Date et heure   | Jser Account Management<br>iuccès de l'audit                       | Source  | D de l'événement   | Catégorie de la tâche  |
| Source :<br>Événem<br>Niveau :<br>Mots clés   | ent: 4720<br>: Information<br>de l'augn   | Catégorie : U<br>Mots-clés : S<br>Date et heure<br>19/05/2004 17/03/06  | lser Account Management<br>iuccès de l'audit                       | Source<br>Microsoft Windows security auditu.  | ID de l'événement<br>4272  | Catégorie de la tâche<br>User Account Management   |
| Source :<br>Événem<br>Niveau :<br>Mots clés<br>Succés<br>Succés   | ent : 4720<br>: Information<br>de Faude<br>de Faude   | Catégorie : U<br>Mots-clés : S<br>Date et heure<br>16/05/2024 17/0366<br>16/05/2024 17/0366   | Jser Account Management<br>iuccés de l'audit                       | Source<br>Microsoft Windows security auditu.<br>Microsoft Windows security auditu.  | ID de l'événement<br>4722<br>4718<br>527   | Catégorie de la tâche<br>User Account Management<br>User Account Management  |
| Source :<br>Événem<br>Niveau :<br>Mats clés<br>Q Succés<br>Q Succés<br>Q Succés   | ent : 4720<br>information<br>de l'audit<br>de l'audit<br>de l'audit   | Catégorie : U<br>Motr-clés : S<br>Date et heure<br>16/05/2024 12:03:06<br>16/05/2024 12:03:06<br>16/05/2024 15:1:05   | Jser Account Management<br>iuccès de l'audit                       | Source<br>Microsoft Windows security audit<br>Microsoft Windows security audit i<br>Microsoft Windows security audit<br>Microsoft Windows security audit  | ID de l'événement<br>472<br>4710<br>5377   | Catégorie de la tâche     User Account Management     User Account Management     User Account Management     User Account Management  |
| Source :<br>Événem<br>Niveau :<br>Mots clés<br>Succés<br>Succés<br>Succés<br>Succés   | ent : 4720<br>information<br>de l'audit<br>de l'audit<br>de l'audit<br>de l'audit   | Catégorie U<br>Mots-clés S<br>Date et heure<br>16/05/2024 17/0300<br>16/05/2024 15/050<br>16/05/2024 16:51:05<br>16/05/2024 16:51:05  | Jser Account Management<br>Juccès de l'audit                       | Source<br>Microsoft Windows security auditu-<br>Microsoft Windows security auditu-<br>Microsoft Windows security auditu-<br>Microsoft Windows security auditu-<br>Microsoft Windows security auditu-  | ID de l'événement<br>4720<br>4711<br>5370<br>3370<br>3370                                      | Catégorie de la tâche     User Account Management  |
| Source :<br>Événem<br>Niveau :<br>Mats clés<br>G Succès<br>G Succès<br>G Succès<br>G Succès<br>G Succès   | de l'audit<br>de l'audit<br>de l'audit<br>de l'audit  | Catégorie U<br>Mots-cles I S<br>Date et heure<br>16/05/2024 17/03/00<br>16/05/2024 17:01/00<br>16/05/2024 16:51:05<br>16/05/2024 16:51:05<br>16/05/2024 16:51:05  | Jser Account Management<br>Juccès de l'audit                       | Source<br>Microsoft Windows security auditu-<br>Microsoft Windows security auditu-<br>Microsoft Windows security auditu-<br>Microsoft Windows security auditu-<br>Microsoft Windows security auditu-  | ID de l'événement<br>472<br>537<br>537<br>537<br>537<br>537<br>537<br>537                      | Catégorie de la tâche     User Account Management  |
| Source :<br>Événem<br>Niveau :<br>Mots clár<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès   | ent : 4720<br>information<br>de Faudit<br>de Faudit<br>de Faudit<br>de Faudit<br>de Faudit  | Catégorie : U<br>Mots-clés : S<br>Date et heure<br>16/05/2024 16:51:05<br>16/05/2024 16:51:05<br>16/05/2024 16:51:05<br>16/05/2024 16:51:05   | Jser Account Management<br>iuccès de l'audit                       | Source<br>Microsoft Windows security auditu.<br>Microsoft Windows security auditu.<br>Microsoft Windows security auditu.<br>Microsoft Windows security auditu.<br>Microsoft Windows security auditu.  | ID de l'événement<br>479<br>537<br>537<br>537<br>537<br>537<br>537<br>537                      | Certégorie de la tâche     User Account Management                             |
| Source :<br>Événem<br>Niveau :<br>Mats cláe<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Su | ent : 4720<br>information<br>de l'audit<br>de l'audit<br>de l'audit<br>de l'audit<br>de l'audit<br>de l'audit<br>de l'audit   | Catégorie : U<br>Mots-clés : S<br>Date et heure<br>16/05/2024 16:51:05<br>16/05/2024 16:51:05<br>16/05/2024 16:51:05<br>16/05/2024 16:51:05<br>16/05/2024 16:50:54<br>16/05/2024 16:50:54   | Jser Account Management<br>iuccès de l'audit                       | Source<br>Microsoft Windows security auditu.<br>Microsoft Windows security auditu.        | ID de l'événement<br>479<br>537<br>537<br>537<br>537<br>537<br>537<br>537<br>537<br>537<br>537 | Certégorie de la tâche     User Account Management     User Account Management |
| Source :<br>Événem<br>Nivezu :<br>Mats clés<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès   | ent : 4720<br>Information<br>de l'audit<br>de l'audit   | Catégorie : U<br>Mots-clés : S<br>Date et heure<br>16/05/2024 16:51:05<br>16/05/2024 16:51:05<br>16/05/2024 16:51:05<br>16/05/2024 16:51:05<br>16/05/2024 16:50:54<br>16/05/2024 16:50:54<br>16/05/2024 16:50:54  | Iser Account Management  | Source<br>Microsoft Windows security auditu.<br>Microsoft Windows security auditu.        | ID de l'événement<br>472<br>537<br>537<br>537<br>537<br>537<br>537<br>537<br>537<br>537<br>537 | Cartégorie de la tâche<br>User Account Management<br>User Account Management         |
| Source :<br>Événem<br>Nivezu :<br>Mots clés<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès   | ent : 4720<br>Information<br>de l'audit<br>de l'  | Catégorie : U<br>Motr-clés : S<br>Date et heure<br>16/05/2024 15:005<br>16/05/2024 16:51:05<br>16/05/2024 16:51:05<br>16/05/2024 16:51:05<br>16/05/2024 16:50:54<br>16/05/2024 16:50:54<br>16/05/2024 16:50:54<br>16/05/2024 16:50:54   | Jser Account Management<br>Juccès de l'audit                       | Source<br>Microsoft Windows security audit<br>Microsoft Windows security audit                      | ID de l'événement<br>472<br>471<br>537<br>537<br>537<br>537<br>537<br>537<br>537<br>537        | Catégorie de la tâche User Account Management                                  |
| Source :<br>Événem<br>Nivesu :<br>Mots clés<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Succès<br>Su | ent : 4720<br>Information<br>de l'audit<br>de l'audit | Catégorie : U<br>Mots-clés : S<br>Date et heure<br>16/05/2024 12:03:06<br>16/05/2024 16:51:05<br>16/05/2024 16:51:05<br>16/05/2024 16:51:05<br>16/05/2024 16:50:54<br>16/05/2024 16:50:54<br>16/05/2024 16:50:54<br>16/05/2024 16:50:54<br>16/05/2024 16:50:54<br>16/05/2024 16:50:54 | Jser Account Management<br>iuccés de l'audit<br>: a été difectuée. | Source<br>Microsoft Windows security auditi -<br>Microsoft Windows security auditi - | ID de l'événement<br>479<br>537<br>537<br>537<br>537<br>537<br>537<br>537<br>537<br>537<br>537 | Cetégorie de la tâche     User Account Management     User Account Management  |