PREMIÈRE MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Paris, le 05/02/2024
N°

Déploiement de FastFind via une GPO et une tâche planifiée

Procedure

ANSSI/SDO
05/02/2024

TLP:CLEAR

Version : 1.0
Nombre de pages : 27


AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

Niveau de diffusion

TLP:CLEAR	Pas de restriction, partage libre entre les différentes communautés (publication large, y compris Internet)

1 Présentation du document

Ce document vise à vous assister au déploiement de l'outil FastFind dans un système d'information géré dans un domaine *Active-Directory* (AD).

Il explique comment déployer FastFind sur l'ensemble des machines d'un domaine (ou un sous-ensemble) via une tâche planifiée à exécution immédiate configurée dans une *Stratégie de groupe* ou GPO [1].

Cette procédure permet d'effectuer une recherche sur toutes ou partie des machines du domaine et d'en récupérer les résultats de manière centralisée.

1.1 Avertissement

FastFind peut embarquer des marqueurs susceptibles d'être détectés par des antivirus. Il peut être utile de déclarer en liste blanche les condensats (*hash*) du fichier déployé dans la console de l'anti-virus.

Avant tous déploiement de FastFind, il est nécessaire d'avoir une compréhension de l'infrastructure réseau : en particulier de la présence de proxy et de pare-feu, de la visibilité des points de collecte visés.

Il est également important de réfléchir à la sécurité du paramétrage de la GPO qui sera utilisée : choisir le propriétaire de la GPO (qui aura donc le droit de la modifier) et préciser les délégations permettant de la lier à des *OU* [2] Ceci afin de ne pas aller à l'encontre du modèle de sécurité employé sur le système d'information. Si besoin, il faudra définir explicitement des permissions pour empêcher tout lien non désiré ou tout droit implicite dangereux.

1. Les GPO, *Group Policy Objects*, ou Stratégies de Groupe en français sont des règles destinées à être appliquées à une ou plusieurs machines sous Windows pour y déclencher des changements de configuration, voire des exécutions. Le déploiement GPO est le principal mécanisme d'administration centralisée disponible dans un domaine *Active-Directory*
2. Les *OU* pour *Organisational Unit* sont des entités organisationnelles dans l'annuaire *Active-Directory* qui permettent de distinguer des groupes d'utilisateurs ou de machines afin de leur appliquer une politique particulière.

2 Prérequis

2.1 Prérequis au déploiement

Pour effectuer l'opération, vous aurez besoin :
— d'un compte membre du groupe "Administrateurs de domaine" ou disposant d'une délégation de droit pour créer la GPO ;
— d'un compte avec les permissions suffisantes pour créer et gérer le partage de déploiement et de collecte ;
— d'un exécutable FastFind et son éventuel fichier de configuration locale `.xml` ; (voir modèle en annexe, page 25)
— d'un espace de stockage accessible en lecture et visible de toutes les machines qui doivent exécuter FastFind.

2.2 Prérequis à la récupération des résultats

Pour le stockage des archives de résultats générées par FastFind, deux solutions sont proposées :
— utiliser un serveur *BITS* [3] ;
— utiliser un partage Windows accessible en écriture et visible de toutes les machines qui doivent exécuter FastFind.

3. *BITS* pour *Background Intelligent Transfer Service* est un service de distribution de fichiers sous système Windows. Ce service permet de transférer des fichiers entre machines de façon fiable et en tenant compte de la charge réseau. Ce dispositif est notablement utilisé pour le téléchargement des mises à jours par *Windows update*.

3 Étapes de la procédure

4 Dépôt de l'exécutable FastFind et du fichier de configuration dans l'espace partagé

On utilise si possible le partage Windows `\\<nom_du_domaine>\SYSVOL\` déjà configuré sur un domaine AD.

Dans le répertoire `\\<nom_du_domaine>\SYSVOL\<nom_du_domaine>\scripts\` on crée un répertoire `fastfind` dans lequel on dépose l'exécutable FastFind et son fichier de configuration locale.

⚠ **Attention** de vérifier que le nom du fichier de configuration est le même que celui du binaire, modulo son extension `.xml`.

Pour vérifier le condensat(*hash*) de l'exécutable FastFind, on peut utiliser la commande suivante :

```
certutil -hashfile <executable_fastfind> sha1
```

⚠ **Attention**, les fichiers déposés dans le `SYSVOL` d'un domaine sont répliqués par DFS [4] sur l'ensemble des contrôleurs de domaine. Sur un domaine possédant des contrôleurs de domaine sur des sites distants ou disposant d'une faible bande passante réseau, cette réplication peut prendre plusieurs minutes/heures (même avec une bande passante suffisante). Il est donc judicieux de déposer rapidement l'outil dans l'espace partagé (par exemple une ou deux heures avant de créer la GPO) et de vérifier sa présence sur le Contrôleur de domaine (*DC*) supposé le plus "lent" à répliquer avant de lier la GPO. La commande `dcdiag` permet de vérifier l'état de la réplication entre les contrôleurs de domaine.

En cas d'urgence, une solution consiste à utiliser dans la tâche planifiée le chemin explicite vers le `SYSVOL` d'un des contrôleurs de domaine joignable depuis toutes les machines. Pour éviter un afflux de connexions sur ce contrôleur de domaine, on pourra limiter cette solution à un ensemble de machines ciblées pour lesquelles on souhaite avoir des résultats de FastFind rapidement et, une heure plus tard, utiliser le chemin `\\<nom_du_domaine>\SYSVOL\...` dans une tâche planifiée destinée aux autres machines.

Si on ne souhaite pas utiliser le partage SYSVOL, on peut créer un répertoire partagé en suivant la procédure de création d'un partage qui suit. Sinon, on peut passer à la Préparation de l'espace de stockage des archives résultats de FastFind page 10.

Il est également possible d'utiliser un partage existant mais il faut vérifier que les droits sur le répertoire et le partage sont corrects. On peut s'appuyer sur la procédure qui suit pour vérifier.

4. *Distributed File System* : système de fichier distribué en environnement Windows, utilisé notablement pour répliquer le `SYSVOL` entre contrôleurs de domaine

4.1 Création d'un partage pour l'exécutable FastFind et son fichier de configuration

⚠ **Attention** Cette opération n'est requise que si le partage `SYSVOL` ne convient pas.

Pour héberger l'exécutable FastFind et son fichier de configuration, on crée un partage Windows accessible en lecture au groupe "Tout le monde" et on configure les autorisations sur le répertoire pour donner le droit en lecture (et pas en écriture) au groupe "Ordinateurs du domaine" (ou "Tout le monde" dans le cas d'un déploiement multi-forêts).

4.2 Autorisations sur le répertoire

Pour configurer les autorisations sur le répertoire à partager, on peut suivre les étapes suivantes :
— sur le répertoire faire un clic-droit puis choisir "Propriétés"
— dans la fenêtre de propriétés, cliquer sur l'onglet "Sécurité" puis sur le bouton "Modifier..."
— dans la nouvelle fenêtre, cliquer sur le bouton "Ajouter..."
— dans la nouvelle fenêtre, saisir "Ordinateurs du domaine" (ou "Tout le monde" dans le cas d'un déploiement multi-forêts) comme nom de l'objet (vérifier éventuellement avec le bouton "Vérifier les noms") et valider en cliquant sur "OK" (la fenêtre disparaît)
— dans la fenêtre "Autorisations pour `nom du répertoire`", dans la section "Autorisations pour Ordinateurs du domaine", vérifier que "Ecriture" n'est **pas** coché
— fermer toutes les fenêtres en cliquant sur "OK"

4.2.1 Partage du répertoire

Puis, le répertoire doit être partagé en lecture pour "Tout le monde" :
— sur le répertoire à partager faire un clic-droit puis choisir "Propriétés"
— dans la fenêtre de propriétés, cliquer sur l'onglet "Partage" puis sur le bouton "Partage avancé..."
— dans la fenêtre qui apparaît, cocher "Partager ce dossier"
— vérifier que le nombre d'utilisateurs simultanés maximum convient
— fermer les fenêtres en cliquant sur les boutons "OK" et "Fermer" (le répertoire est automatiquement accessible en lecture à "Tout le monde")
Enfin, il faut copier l'exécutable FastFind et son fichier de configuration dans le répertoire.

4.3 Téléchargement de l'exécutable FastFind et du fichier de configuration depuis un serveur BITS

⚠ **Attention** : cette étape est facultative mais contribue à fiabiliser les déploiements.

L'exécution de FastFind depuis un répertoire partagé (par exemple le partage `SYSVOL`), implique que ce partage doit être accessible pendant l'exécution de FastFind.

En cas d'utilisation d'une liaison instable, susceptible de subir des coupures, il peut être intéressant d'utiliser un serveur BITS pour télécharger FastFind et son fichier de configuration au début de l'exécution afin de ne plus être dépendant de la qualité du réseau et de la disponibilité du partage.

⚠ Attention à bien évaluer l'intérêt d'utiliser cette fonctionnalité car elle complexifie le déploiement de FastFind et augmente les risques de faire une erreur.

Pour configurer FastFind pour qu'il télécharge son exécutable et sa configuration, il faut ajouter les lignes suivantes au fichier de configuration locale `.xml`

Attention à bien mettre cet extrait dans une balise racine/englobante

```
    <dfir-orc></dfir-orc>}
```

voir le **modèle** en annexe page 25 :

```
<download job="fastfind_download" method="bits"
    server="http://__ip_or_fqdn__"
    path="__virtual_folder__"
    command="__local_folder__\FastFind.exe" >
    <file name="FastFind.exe" localpath="__local_folder__\FastFind.exe" delete="yes"/>
    <file name="FastFind.xml" localpath="__local_folder__\FastFind.xml" delete="yes"/>
</download>
```

Avec :

- `__virtual_folder__` : le répertoire virtuel du serveur IIS dans lequel l'exécutable FastFind et son fichier de configuration sont stockés
- `__local_folder__` : le répertoire de travail sur les machines examinées dans lequel FastFind sera exécuté
- l'attribut `name` des éléments `<file>` : indique les noms de l'exécutable FastFind et du fichier de configuration stockés dans le répertoire virtuel du serveur IIS
- l'attribut `command` de l'élément `<download>` : indique la commande à exécuter à la fin du téléchargement (le FastFind.exe se trouvant dans `__local_folder__` dans notre exemple)

Il faut donc placer l'exécutable FastFind et le fichier de configuration `.xml` dans le répertoire virtuel du serveur IIS (répertoire pointé par `__virtual_folder__` dans la configuration ci-dessus). Les deux fichiers seront téléchargés et placés sur chaque machine dans le répertoire `__local_folder__` (créé automatiquement s'il n'existe pas). L'attribut `delete` avec la valeur `yes` permet d'effacer les fichiers à la fin de l'exécution.

À la fin de cette partie facultative de la procédure, l'exécutable FastFind et son fichier de configuration `.xml` doivent être présents :

- dans un répertoire partagé accessible depuis toutes les machines (par exemple `SYSVOL`);
- dans un répertoire virtuel du serveur IIS configuré pour accepter le protocole BITS.

De plus, le fichier de configuration `.xml` présent dans le répertoire partagé doit contenir au minimum un élément `<download></download>` avec les paramètres nécessaires pour télécharger les deux fichiers.

Remarque : la présence de l'élément `<download></download>` dans le fichier de configuration de FastFind dans le répertoire virtuel du serveur IIS n'entraîne pas de boucle de téléchargement car

dans le cas d'une exécution dans un répertoire local d'une machine, FastFind ne tient pas compte de cet élément.

5 Préparation de l'espace de stockage des archives FastFind

5.1 Utilisation d'un serveur BITS

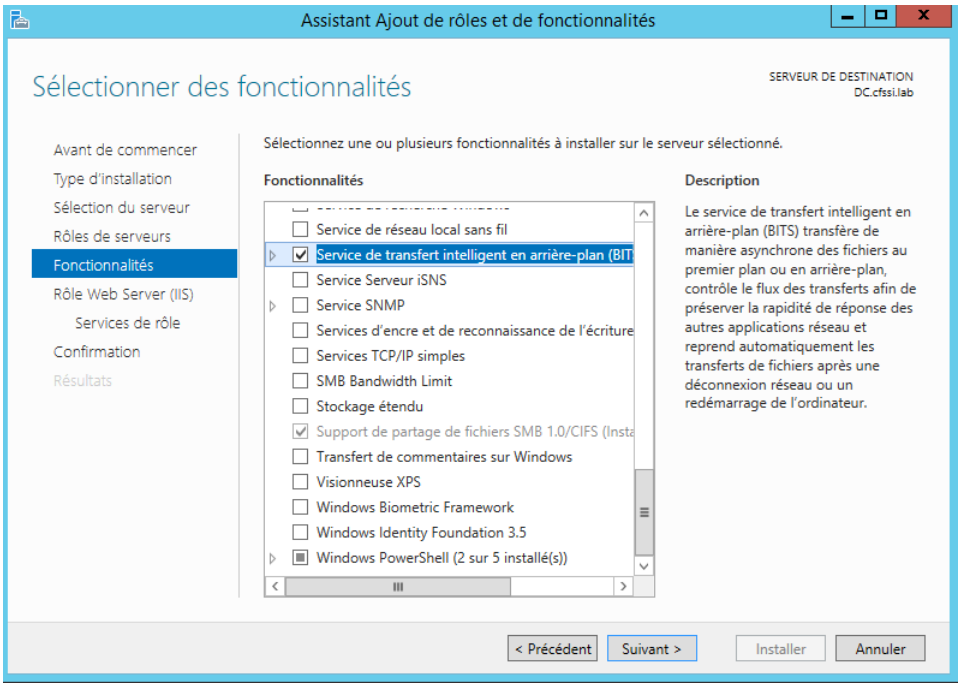
La solution à privilégier pour rapatrier les archives de résultats FastFind dans un répertoire centralisé est d'utiliser le protocole *BITS* sur HTTP. Cette solution nécessite la configuration d'un serveur web IIS dédié à la réception des données appelé "serveur BITS" dans la suite du document.

5.1.1 Installation d'un serveur BITS

Si la fonctionnalité "Service de transfert intelligent en arrière-plan (BITS)" n'est pas installée sur la machine, il faut l'installer.

La procédure suivante est compatible avec Windows Server 2012 R2 :

— lancer l'outil d'activation de fonctionnalités Windows (rechercher par exemple "fonctionnalités" et choisir "Activer ou désactiver des fonctionnalités Windows")
— cliquer sur le bouton "Suivant" pour aller jusqu'à la partie "Fonctionnalités"
— cocher "Service de transfert intelligent en arrière-plan (BITS)"

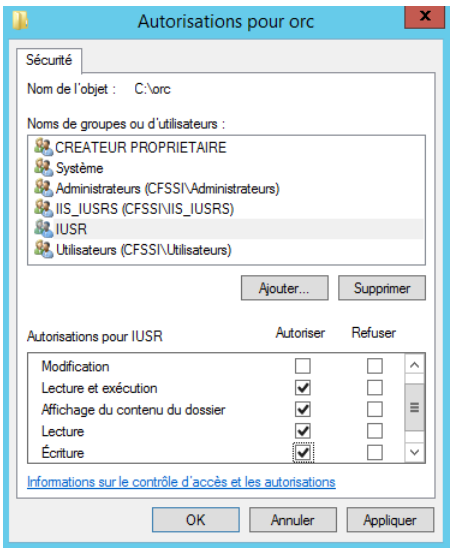


— valider la fenêtre qui apparaît en cliquant sur le bouton "Ajouter des fonctionnalités"
— continuer l'installation en cliquant sur le bouton "Suivant" tant qu'il est utilisable
— terminer l'installation en cliquant sur le bouton "Installer" dès qu'il est disponible
— fermer la fenêtre une fois l'installation terminée (le bouton "Fermer" apparait avant la fin de l'installation mais fermer la fenêtre n'interrompt pas l'installation)

5.1.2 Création du répertoire de stockage BITS

Puis il faut créer le répertoire dans lequel les archives seront stockées et donner les droits de lecture et d'écriture au groupe `IIS_IUSRS` et à l'utilisateur `IUSR`.

Pour cela, on peut suivre les étapes suivantes :
— sur le répertoire faire un clic-droit puis choisir "Propriétés"
— dans la fenêtre de propriétés, cliquer sur l'onglet "Sécurité" puis sur le bouton "Modifier..."
— dans la nouvelle fenêtre, cliquer sur le bouton "Ajouter..."
— dans la nouvelle fenêtre, saisir `IIS_IUSRS` comme nom de l'objet, vérifier avec le bouton "Vérifier les noms" et si le nom n'est pas trouvé, indiquer l'ordinateur courant comme emplacement (bouton "Emplacements") pour la recherche. Puis valider en cliquant sur "OK" (la fenêtre disparaît)
— cliquer de nouveau sur le bouton "Ajouter..."
— dans la nouvelle fenêtre, saisir `IUSR` comme nom de l'objet (vérifier éventuellement avec le bouton "Vérifier les noms") et valider en cliquant sur "OK" (la fenêtre disparaît)
— dans la fenêtre "Autorisations pour **nom du répertoire**", dans la section "Autorisations pour IUSR", cocher "Écriture" (en plus des droits de lecture normalement déjà sélectionnés) comme indiqué par l'image suivante

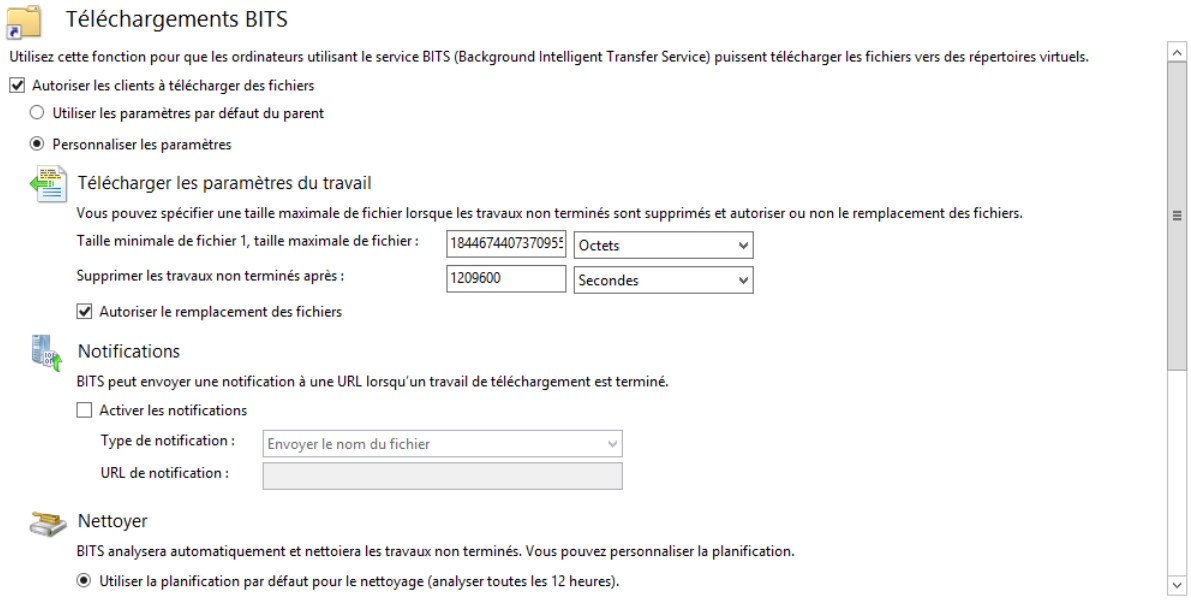


— fermer toutes les fenêtres en cliquant sur "OK"

5.1.3 Configuration du serveur BITS

Enfin, pour configurer le serveur *BITS*, il faut suivre les étapes suivantes :
— lancer le Gestionnaire des services Internet (rechercher "IIS" pour trouver l'application)
— trouver le site par défaut ("Default Web Site") dans l'arborescence (normalement sous "nom de la machine -> Sites")
— cliquer avec le bouton droit sur "Default Web Site" et choisir "Ajouter un répertoire virtuel..."
— dans la fenêtre qui apparaît, choisir pour alias un nom qui sera utilisé par la suite dans le fichier de configuration `.xml` comme paramètre `path` et sélectionner le répertoire créé précédemment comme chemin physique ; valider en cliquant sur "OK" (la fenêtre disparaît)

— pour ce répertoire virtuel, dans la rubrique ”Téléchargement BITS” (double-clic pour ouvrir), autoriser le téléchargement *BITS* et le remplacement des fichiers (il faut cocher ”Personnaliser les paramètres”)



— cliquer de nouveau sur le nom du répertoire virtuel à gauche et accepter l’enregistrement des modifications
— dans la rubrique ”Authentification”, vérifier que l’authentification anonyme est activée
— cliquer de nouveau sur le nom du répertoire virtuel à gauche
— dans la rubrique ”Types MIME”, ajouter (action ”Ajouter...” à droite) une entrée pour l’extension ”.7z” avec comme type MIME `application/octet-stream`
— en cas de configuration de FastFind pour utiliser *BITS* pour télécharger son exécutable et son fichier de configuration (facultatif), ajouter également une entrée pour l’extension `.xml` avec comme type MIME `application/octet-stream`
— quitter l’application de configuration d’IIS

5.2 Utilisation d'un partage Windows

Si la configuration d'un serveur *BITS* n'est pas possible, il reste faisable d'utiliser le protocole BITS sur *SMB* [5] et de stocker les archives dans un partage Windows. Il est également possible d'utiliser un partage Windows sans utiliser le protocole *BITS*.

Dans les deux cas (utilisation du protocole *BITS* ou non), il faut créer un partage Windows et configurer les autorisations pour donner les droits en lecture et écriture au groupe "Ordinateurs du domaine" (ou "Tout le monde" dans le cas d'un déploiement multi-forêt).

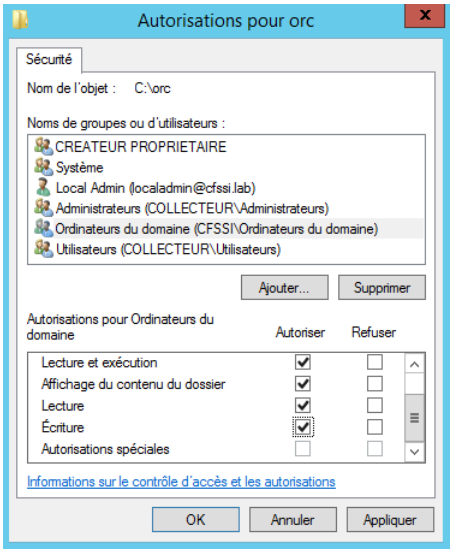
⚠ **Attention** à ne pas utiliser un partage en DFS : l'espace de stockage sous-jacent pourrait être limité et la réplication inutile et générera un trafic réseau supplémentaire indésirable.

Il est également possible d'utiliser un partage existant mais il faut vérifier que les droits sur le répertoire et le partage sont corrects. On peut s'appuyer sur la procédure qui suit pour vérifier.

5.2.1 Autorisations sur le répertoire

Pour configurer les autorisations sur le répertoire à partager, on peut suivre les étapes suivantes :
- sur le répertoire faire un clic-droit puis choisir "Propriétés"
- dans la fenêtre de propriétés, cliquer sur l'onglet "Sécurité" puis sur le bouton "Modifier..."
- dans la nouvelle fenêtre, cliquer sur le bouton "Ajouter..."
- dans la nouvelle fenêtre, saisir "Ordinateurs du domaine" (ou "Tout le monde" dans le cas d'un déploiement multi-forêt) comme nom de l'objet (vérifier éventuellement avec le bouton "Vérifier les noms") et valider en cliquant sur "OK" (la fenêtre disparaît)
- dans la fenêtre "Autorisations pour `nom du répertoire`", dans la section "Autorisations pour Ordinateurs du domaine", s'assurer que les permissions suivantes sont cochées :
  - "Modification"
  - "Lecture et exécution"
  - "Affichage du contenu du dossier"
  - "Lecture"
  - "Écriture"

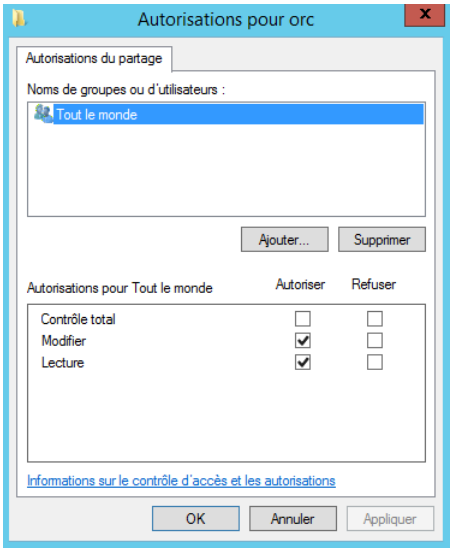
5. *SMB* pour *Server Message Block* est le principal protocole utilisé pour les partages de fichiers en réseau dans un environnement Windows



— fermer toutes les fenêtres en cliquant sur ”OK”

5.2.2 Partage du répertoire

Puis, le répertoire doit être partagé en lecture et en écriture (”Modifier”) pour ”Tout le monde” :
— sur le répertoire à partager faire un clic-droit puis choisir ”Propriétés”
— dans la fenêtre de propriétés, cliquer sur l'onglet ”Partage” puis sur le bouton ”Partage avancé...”
— dans la fenêtre qui apparaît, cocher ”Partager ce dossier”
— vérifier que le nombre d'utilisateurs simultanés maximum convient
— cliquer sur le bouton ”Autorisations”
— dans la fenêtre qui apparaît, vérifier que ”Tout le monde” est sélectionné et cocher ”Modifier” dans les autorisations (”Lecture” doit déjà être coché)



— fermer les fenêtres en cliquant sur les boutons ”OK” et ”Fermer”

6 Modification du fichier de configuration de FastFind

Cette étape consiste à éditer le fichier de configuration `\\<nom_du_domaine>\SYSVOL\<nom_du_domaine>\scripts\fastfind\<nom_du_binaire_fastfind>.xml` pour paramétrer la copie des archives dans l'espace de stockage prévu à cet effet.

Trois solutions sont possibles (dans l'ordre de préférence) :
— utilisation d'un serveur *BITS* (protocole HTTP)
— utilisation du protocole *BITS* et d'un partage Windows
— utilisation d'un partage Windows

Il peut être judicieux de tester que la solution choisie fonctionne correctement en exécutant "manuellement" FastFind (sans *GPO* et tâche planifiée et avec le fichier de configuration présent) sur une machine de test.

⚠ En cas d'utilisation d'un serveur *BITS* avec le protocole HTTP, il faut vérifier que l'éventuelle configuration d'un serveur mandataire HTTP(*proxy*) sur la machine de test n'empêche pas de joindre le serveur. Cette configuration ne devrait pas gêner le déploiement avec la *GPO* car la tâche planifiée est exécutée par le compte "Système local" qui n'a probablement pas de telle configuration.

6.1 Utilisation d'un serveur BITS

Dans le cas d'une utilisation de *BITS*, on ajoute (ou on modifie) les lignes suivantes dans le fichier de configuration locale `.xml`

Attention à bien mettre cet extrait dans une balise racine/englobante

```
<dfir-orc>
...
</dfir-orc>
```

voir le **modèle** en annexe, page 25 :

```
<upload job="fastfind" method="bits"
   server="http://__ip_or_fqdn__"
   path="__virtual_folder__"
   mode="async"
   operation="move" />
```

6.2 Utilisation du protocole BITS et d'un partage Windows

Dans le cas d'une utilisation du protocole *BITS* et d'un partage Windows, il faut ajouter (ou modifier) les lignes suivantes dans le fichier de configuration locale `.xml`

attention à bien mettre cet extrait dans une balise racine/englobante

```
<dfir-orc>
...
</dfir-orc>
```

voir le **modèle** en annexe, page 25 :

```
<upload job="fastfind" method="bits"
    server="file://__ip_or_fqdn__"
    path="__share_name__[/__subfolder__]"
    mode="async"
    operation="move" />
```

Remarque : la seule différence par rapport à la configuration pour une utilisation d'un serveur *BITS* est le remplacement du préfixe `http:` par `file:` dans le paramètre "server".

6.3 Utilisation d'un partage Windows

Dans le cas de l'utilisation d'un répertoire partagé sans utilisation du protocole *BITS*, on ajoute (ou on modifie) les lignes suivantes dans le fichier de configuration locale `.xml`.

attention à bien mettre cet extrait dans une balise racine/englobante

```
<dfir-orc>
...
</dfir-orc>
```

voir le **modèle** en annexe, page 25 :

```
 <upload method="filecopy"
   server="file://__ip_or_fqdn__"
   path="__share_name__[/__subfolder__]"
   mode="sync"
   operation="move" />
```

Avec cette configuration, les archives sont déplacées dans le répertoire partagé une fois qu'elles sont terminées.

Une alternative consiste à écrire directement les archives dans le répertoire partagé. Mais cette solution est plus sensible aux pertes de connexion avec le serveur qui héberge le partage. La ligne suivante permet de configurer cette solution :

```
<output>\\__ip_or_fqdn__\__share_name__</output>
```

⚠ **Attention** à vérifier que le nombre de clients simultanés autorisés n'est pas trop limité (dépend de la version de Windows ; par exemple 20 au maximum pour les versions "Pro" ; seules les versions serveur garantissent un grand nombre d'accès simultanés).

7 Création de la GPO et de la tâche planifiée

Il faut créer une *GPO* qui lancera FastFind avec une tâche planifiée **à exécution immédiate**. La tâche doit :

— être exécutée par `S-1-5-18` (correspondant au compte "Système local")
— sortir les ordinateurs du mode veille pour exécuter la tâche
— s'arrêter si elle dure plus de 12 heures (et forcer l'arrêt)
— être appliquée une fois et ne pas être ré-appliquée

Pour créer cette *GPO*, on peut suivre les étapes détaillées qui suivent.

Après s'être authentifié en tant qu'administrateur du domaine (ou assimilé) sur un contrôleur de domaine ou une machine d'administration disposant des outils d'administration à distance (*RSAT*[6]), ouvrir le gestionnaire de stratégie de groupe (touche `Win + R`, saisir `gpmc.msc` et valider) :

1. Dans l'arborescence à gauche, déplier l'élément qui porte le nom du domaine puis cliquer avec le bouton droit sur "Objets de stratégie de groupe" et choisir "Nouveau" dans le menu contextuel.
2. Dans la fenêtre "Nouvel objet GPO" qui apparaît, saisir le nom de la *GPO* : par exemple `FastFind`.
3. Dans l'arborescence de la fenêtre "Gestion de stratégie de groupe", sous "Objets de stratégie de groupe", cliquer avec le bouton droit sur la *GPO* créée précédemment et choisir "Modifier..." dans le menu contextuel.
4. Dans la fenêtre d'édition qui apparaît :
   — aller dans "Configurations ordinateur" -> "Préférences" -> "Paramètres du Panneau de configuration" -> "Tâches planifiées"
   — dans la partie droite de la fenêtre, cliquer avec le bouton droit et choisir "Nouveau" -> "Tâche immédiate (au minimum Windows 7)" dans le menu contextuel
   Remarque : en cas de présence de versions antérieures à Windows 7 sur le parc, il faut également définir une tâche planifiée (avec un nom différent) qui leur sera destinée.
5. Dans la fenêtre de propriétés de la tâche planifiée qui apparaît :
   — saisir un nom pour la tâche : par exemple `FastFind`
   — saisir le SID du compte avec lequel la tâche sera exécutée : `S-1-5-18` (correspondant au compte "Système local")
   — en haut de la fenêtre cliquer sur l'onglet "Actions" puis sur le bouton "Nouveau..."
6. Dans la fenêtre "Nouvelle action" qui apparaît :
   — saisir dans le champ "Programme/script" le nom de l'exécutable FastFind avec son chemin complet : par exemple `\\<nom_du_domaine>\SYSVOL\<nom_du_domaine>\scripts\fastfind\<binaire_fastfind>`
   — ajouter les éventuelles options de FastFind dans le champ "Ajouter arguments"
   — valider avec le bouton "OK"
7. En haut de la fenêtre de propriété de la tâche planifiée :

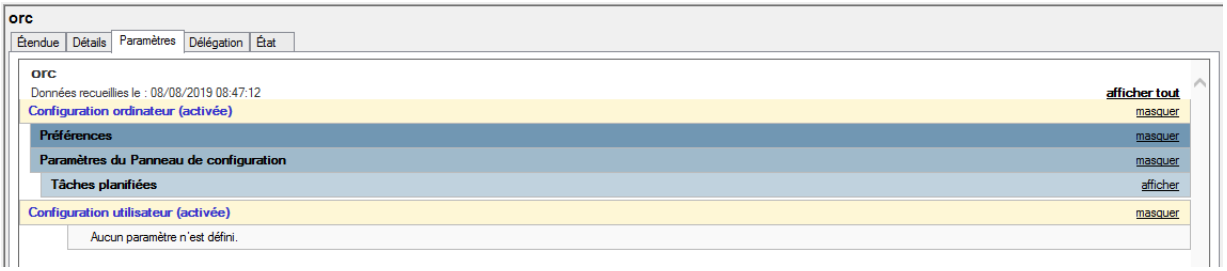
6. *RSAT* pour *Remote Server Administration Tools* est une fonctionnalité optionnelle disponible pour les versions professionnelles de Windows destinée à faciliter les actes d'administration système à distance.

- cliquer sur l'onglet "Conditions" et cocher l'option "Sortir l'ordinateur du mode veille pour exécuter cette tâche" ; il peut également être intéressant, en particulier pour les ordinateurs portables, de cocher l'option "Ne démarrer que si la connexion réseau suivante est disponible" (et choisir le bon réseau en dessous) pour s'assurer que les partages seront disponibles
- cliquer sur l'onglet "Paramètres", cocher l'option "Arrêter la tâche si elle s'exécute plus de" et choisir "12 heures", puis cocher l'option "Si la tâche ne se termine pas au moment demandé, forcer son arrêt"
- cliquer sur l'onglet "Commun" puis cocher l'option "Appliquer une fois et ne plus réappliquer"
- enfin, valider la tâche en cliquant sur le bouton "OK"

8. A ce stade, la tâche planifiée est créée et la fenêtre d'édition de la *GPO* peut être fermée.
   ⚠ Il peut arriver que la tâche planifiée soit mal définie, il est donc utile de vérifier les paramètres de la *GPO* comme expliqué ci-après.

Pour vérifier que les paramètres de la *GPO* ont correctement été définis, il est possible de les procéder comme suit :

- après avoir sélectionné la *GPO*, cliquer sur le bouton "Actualiser"  (en dessous du menu)
- dans la partie droite de la fenêtre, cliquer sur l'onglet "Paramètres"
- dans la partie droite de la fenêtre, cliquer sur "afficher tout"



- vérifier que les paramètres sont corrects et en particulier qu'une action "Démarrer un programme" est configurée pour lancer FastFind

8 Test de la GPO

En cas de doute concernant la définition de la *GPO* ou du résultat de l'exécution de la tâche planifiée et de FastFind, il peut être judicieux de faire un test en limitant le déploiement de la *GPO* à une seule machine.

⚠ Le test de la *GPO* est l'occasion de vérifier que l'exécution de FastFind n'est pas gênée par un antivirus ou des restrictions logicielles.

⚠ Si la tâche planifiée a bien été exécutée mais que le FastFind a échoué, il faut recréer la tâche planifiée avant de ré-appliquer la *GPO* (sinon, la tâche planifiée ne sera pas exécutée). Il n'est pas nécessaire de changer de nom pour la nouvelle tâche planifiée.

Pour restreindre la prise en compte de la *GPO* à une machine particulière, il faut faire les modifications suivantes sur la *GPO* :

— enlever au groupe "Utilisateurs authentifiés" le droit d'appliquer la *GPO*
— ajouter la machine de test dans la liste des machines qui doivent appliquer la *GPO* (limiter la liste à quelques machines pour ne pas excéder la taille de la DACL)

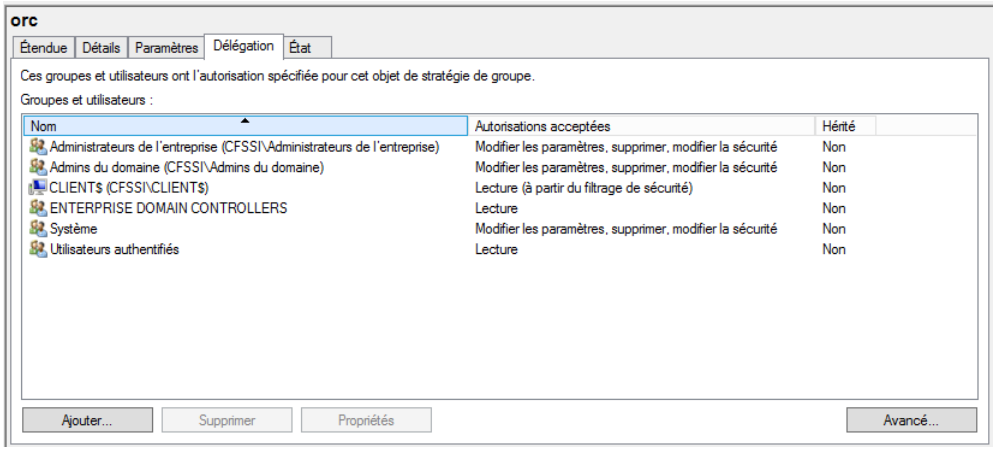
Les étapes suivantes permettent de réaliser ces opérations.

8.1 Suppression du droit d'appliquer la *GPO* pour "Utilisateurs authentifiés"

Remarque : pour ne pas risquer d'appliquer la *GPO* par erreur, cette opération peut également être réalisée immédiatement après avoir créé la *GPO* (avant de la modifier pour créer la tâche planifiée).

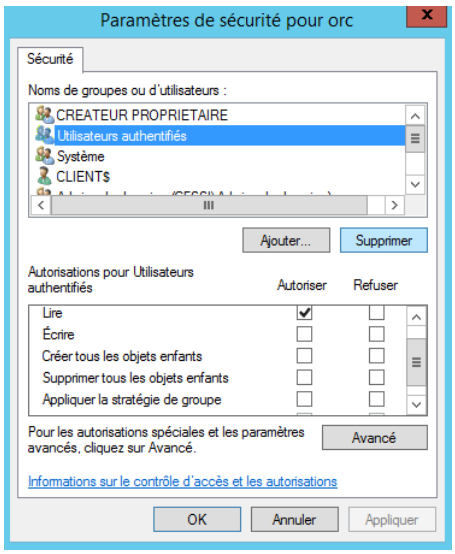
Mais il faudra penser à faire l'opération inverse lorsqu'on voudra déployer la *GPO*.

— sélectionner la *GPO* de FastFind
— dans la partie droite de la fenêtre, cliquer sur l'onglet "Délégation"
— cliquer sur le bouton "Avancé..." en bas à droite



— dans la liste des groupes et utilisateurs, sélectionner ”Utilisateurs authentifiés”
— décocher l’autorisation ”Appliquer la stratégie de groupe” (et laisser ”Lire” coché)

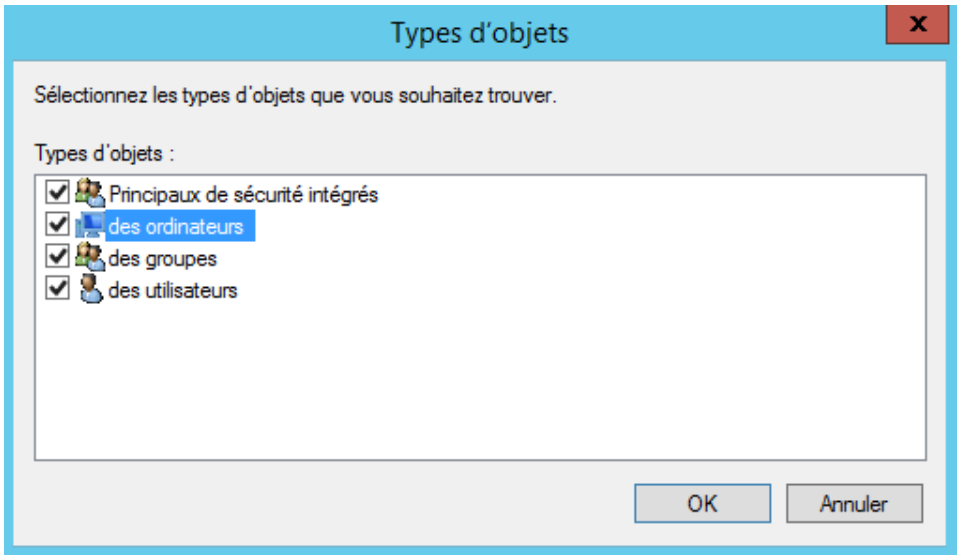
Le droit de lecture est laissé pour permettre à d’éventuels autres utilisateurs qui auraient des droits sur différentes *OU* de lier la *GPO* (il faut pouvoir la voir pour la lier).



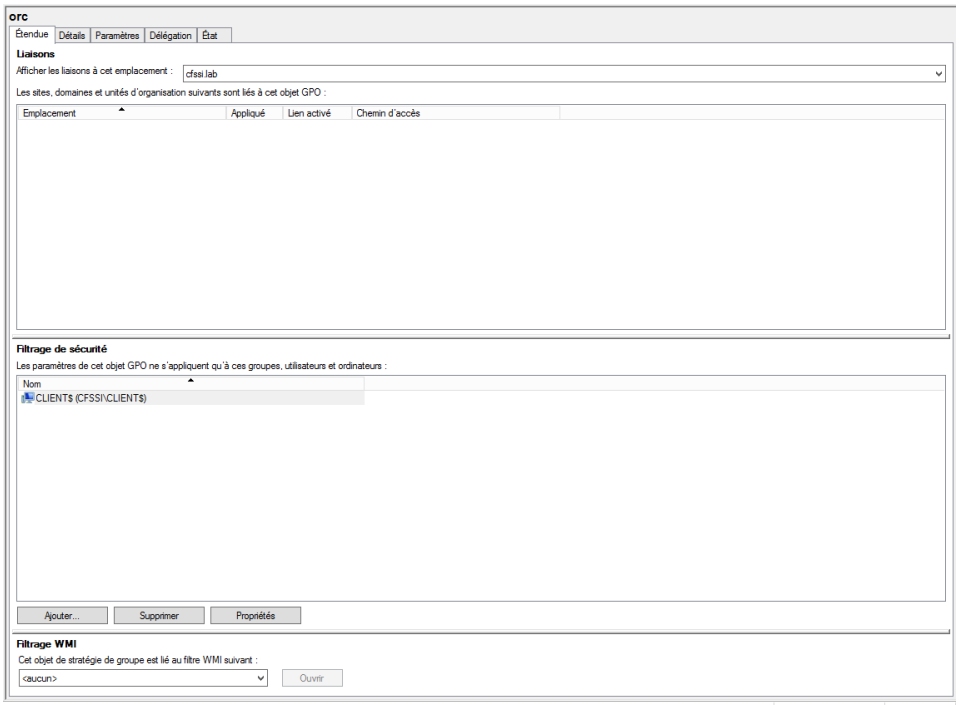
— valider en cliquant sur le bouton ”OK”

8.1.1 Autoriser la machine de test à appliquer la GPO

— sélectionner la *GPO* de FastFind
— dans la partie droite de la fenêtre, cliquer sur l’onglet ”Étendu”
— cliquer sur le bouton ”Ajouter...”
— dans la fenêtre qui apparaît, cliquer sur le bouton ”Types d’objets...”, cocher ”des ordinateurs” et valider



— dans le champs ”Entrez les noms des objets ...”, saisir le nom de la machine sur laquelle on veut tester la *GPO* et cliquer sur le bouton ”Vérifier les noms” pour vérifier que la machine est bien connue
— cliquer sur le bouton ”OK” pour valider



La *GPO* peut maintenant être déployée comme indiquée dans la partie *Utilisation de la GPO* page 23.

Une fois le test terminé, le lien vers la *GPO* (sur le domaine ou une *OU*) peut être supprimé (mais pas la *GPO* dans ”Objets de stratégie de groupe”).

8.1.2 Réautoriser ”Utilisateurs authentifiés” à appliquer la GPO

Une fois les tests terminés, pour autoriser la *GPO* à l'ensemble des machines, il suffit de redonner l'autorisation ”Appliquer la stratégie de groupe” aux ”Utilisateurs authentifiés” :
— sélectionner la *GPO* de FastFind (dans ”Objets de stratégie de groupe”)
— dans la partie droite de la fenêtre, cliquer sur l'onglet ”Délégation”
— cliquer sur le bouton ”Avancé...” en bas à droite
— dans la liste des groupes et utilisateurs, sélectionner ”Utilisateurs authentifiés”
— cocher l'autorisation ”Appliquer la stratégie de groupe” (”Lire” doit toujours être coché)
— supprimer éventuellement la machine de test de la liste
— valider en cliquant sur le bouton ”OK”

La *GPO* peut maintenant être déployée sur le domaine ou sur certaines *OU* comme indiquée dans la partie *Utilisation de la GPO* 23.

9 Utilisation de la GPO

Pour déployer la *GPO*, il faut la lier aux OU auxquelles on souhaite l'appliquer.

On peut par exemple suivre les étapes suivantes :

1. Dans la fenêtre "Gestion de stratégie de groupe" :
   — cliquer avec le bouton droit sur une *OU* sur laquelle on souhaite appliquer la *GPO*
   — puis, choisir "Lier un objet de stratégie de groupe existant..." dans le menu contextuel
2. Dans la fenêtre qui apparaît, sélectionner la *GPO* créée lors des étapes précédentes (par exemple "FastFind") et valider avec le bouton "OK" en bas.

La *GPO* est maintenant liée à l'*OU* et lors de la mise à jour automatique de la stratégie de groupe sur chaque machine de cette OU, la tâche planifiée sera immédiatement exécutée.

⚠ Les bonnes pratiques préconisent de ne pas déployer de *GPO* à la racine du domaine (où seules celles "par défaut" doivent résider, sans délégation) mais de les déployer *OU* par *OU*.

⚠ Si certaines sous-OU bloquent l'héritage des GPO, il faut vérifier auprès d'experts et des équipes locales d'administration s'il est possible de forcer l'application de la *GPO* (*Enforced/Appliqué*).

Le délai de mise à jour des *GPO* est par défaut de 90 minutes (avec un delta de 30 minutes) pour les stations de travail et de 5 minutes pour les contrôleurs de domaine.
Mais il est possible de forcer la mise à jour des *GPO* (par exemple pour la tester rapidement) en utilisant la commande suivante sur les machines concernées :

```
gpupdate /force
```

⚠ **Remarque :** La commande `gpupdate` ne nécessite qu'un compte d'utilisateur du domaine, même non privilégié. Il convient d'éviter d'utiliser un compte à privilèges sur des machines potentiellement compromises.

10 Récupération des résultats

L'application de la *GPO* nouvellement créée n'étant pas faite au même moment sur l'ensemble des machines, les archives doivent apparaître machine par machine, espacées dans le temps.

Il n'est pas possible de prévoir le temps d'exécution de FastFind, mais il est configuré par défaut pour ne pas dépasser 8 heures (temps d'exécution total, ne prend pas en compte les éventuels mises en veille du poste qui rallongeront d'autant ce temps). Après ce délai, pour vérifier que la collecte s'est bien passée, on peut vérifier s'il y a une archive pour chaque machine dans le répertoire de stockage.

Une fois l'exécution terminée, copier les résultats vers un support amovible inscriptible. Il est recommandé d'utiliser la commande `robocopy` pour permettre la reprise sur erreur et la mise à jour de la collecte en plusieurs lots.

11 Suppression de la GPO

Après le déploiement de la *GPO* avec succès sur toutes les machines, le ou les liens de la *GPO* peuvent être supprimés. Une fois l'intervention terminée, la *GPO* elle-même peut également être supprimée.

⚠ **Remarque :** Il est important de supprimer la *GPO* afin d'éviter son utilisation par erreur ou pire avec une intention malveillante par la suite.

Pour supprimer un lien vers la *GPO*, dans la console Gestion de stratégie de groupe :
— faire un clic-droit sur le lien de la *GPO* de déploiement dans la section `<nom_du_domaine>`
— dans le menu contextuel, cliquer sur "Supprimer"
— confirmer que c'est bien le lien que vous voulez supprimer
Pour supprimer la *GPO* entière, dans la console Gestion de stratégie de groupe :

— faire un clic-droit sur la *GPO* de déploiement dans la section "Objets de stratégie de groupe" (et non dans la section `<nom_du_domaine>` directement)
— dans le menu contextuel, cliquer sur "Supprimer"
— confirmer la suppression

De même, il faut penser à supprimer les partages et leurs contenus ainsi que la configuration IIS éventuellement créée pour le déploiement.

12 Annexe - modèle de fichier de configuration locale

Vous trouverez ci-dessous un modèle de configuration locale.

Pour l'utiliser, il suffit de :
— le copier dans un fichier ayant le même nom que l'exécutable FastFind avec `.xml` comme extension ;
— placer ce fichier dans le même répertoire que l'exécutable FastFind ;
— le personnaliser, en décommentant et complétant les différentes parties en fonction des besoins.

La documentation complète de ce fichier est disponible à l'adresse `https://dfir-orc.github.io/orc_local_config.html`.

```
<!--
  Complete documentation of this file can be found here :
  https://dfir-orc.github.io/orc_local_config.html -->
<dfir-orc priority="low" powerstate="SystemRequired,AwayMode">
    <!--
    Make FastFind download itself via BITS
    (much more reliable but might trigger AV detection)
    <download job="fastfind_download" method="bits"
        server="http://_ip_or_fqdn_"
        path="_virtual_dir_"
        command="_execution_folder_\FastFind.exe" >
        <file name="FastFind.exe" localpath="_execution_folder_\FastFind.exe" delete="yes"/>
        <file name="FastFind.xml" localpath="_execution_folder_\FastFind.xml" delete="yes"/>
    </download>
    -->

    <output>%temp%</output>
    <!--
    Default temporary directory is %temp%.
    Change the value to a whitelisted directory
    if some software restriction policies (SRP, Applocker, etc...)
    will not allow embedded tools to run from %temp%.
    <temporary>C:\whitelisted_temp_dir</temporary>
    -->

    <!--
    Upload results via BITS over HTTP
    (recommended but requires IIS with BITS_upload
    configured on the collection server)
    <upload job="FastFind" method="BITS"
           server="http://_ip_or_fqdn_"
           path="_virtual_dir_"
           operation="move"
```

```
        mode="async"
    />
    -->
    <!--
    Upload results via BITS over SMB
    (does not require IIS but usually requires
    the collection server to be domain-joined,
    or else explicit credentials must be provided here)
    <upload job="FastFind" method="BITS"
        server="file://_ip_or_fqdn_"
        path="_share_name_"
        operation="move"
        mode="async"
    />
    -->

    <!--
    Encryption is **mandatory** for security reasons !
    Please provide at least one public key to enable it.
    Insert the whole PEM-encoded public key here
    (including "BEGIN CERTIFICATE" header and "END CERTIFICATE" footer)
    <recipient name="DR" archive="*">
    </recipient>
    <recipient name="third_party" archive="*">
    </recipient>
    -->

</dfir-orc>
```

ANSSI/SDO
Version 1.0- 2024-02-05

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP
cyber.gouv.fr