**Nom du fichier :**

INC-N2\_ALPRO\_PROD\_RESEAU\_NAC\_BlocagePC

# Prérequis / Habilitation

**Liste des prérequis pour effectuer la procédure :**

|  |  |
| --- | --- |
| **Accès pwadmsr1** | **Oui** |
| **Accès panacsr1** | **Oui** |
| **Accès oanacsr1** | **Oui** |
| **Accès pwadmsr1** | **Oui** |

# Paramètre d’entrée

**Liste des différents paramètres d’entrée afin de pouvoir réaliser la procédure :**

|  |  |  |
| --- | --- | --- |
|  | **Détails du paramètres** | **Valeurs possibles** |
| 1 | Ouverture d’incident par le pilotage | [DOI- Doc- Réseau- New - NAC PROBTP - Forescout - Procedure d'exploitation pour deblocage d'un host (pilotage)](Notes://PWDOMBR02.DWPROBTP.probtp/C1256FA4004B6AD7/CBBA547FACD8FE75C1256D1F0055564D/DF7F12257D4CD6B2C125838B00514B6E) |
| 2 | Console forescout via pwadmsr1 ou sur poste de travail [DOI- Doc- Réseau- New - NAC COMMUN- Forescout - Installation Client Manager](Notes://PWDOMBR02.DWPROBTP.probtp/C1256FA4004B6AD7/CBBA547FACD8FE75C1256D1F0055564D/C2055F126025B2CEC12584C6004BADAA) | **panacsr1 pour Probtp** |
| 3 | Console forescout via pwadmsr1 ou sur poste de travail [DOI- Doc- Réseau- New - NAC COMMUN- Forescout - Installation Client Manager](Notes://PWDOMBR02.DWPROBTP.probtp/C1256FA4004B6AD7/CBBA547FACD8FE75C1256D1F0055564D/C2055F126025B2CEC12584C6004BADAA) | **oanacsr1 pour Audiens** |
|  |  |  |

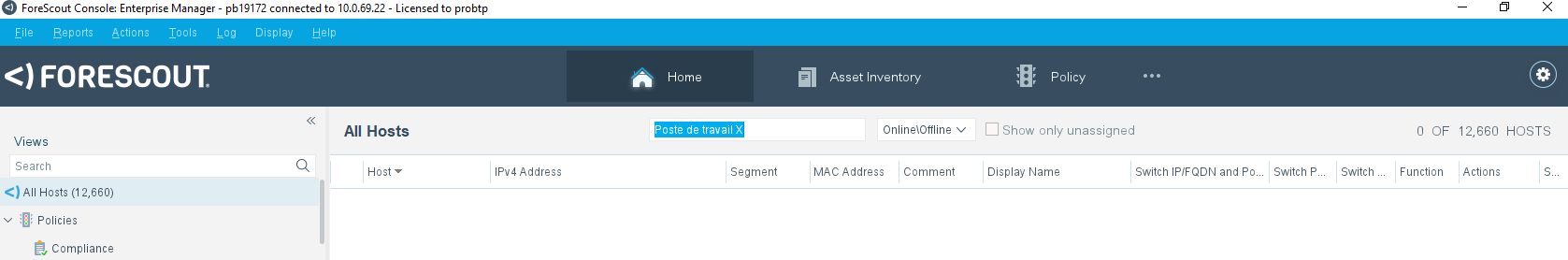
# Impact

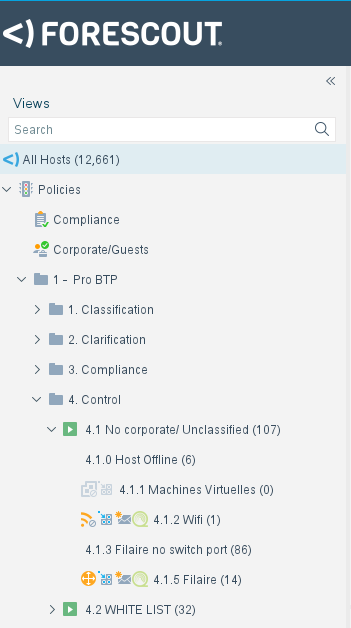
|  |  |  |
| --- | --- | --- |
| **Service non impacté** | **Service dégradé** | **Service indisponible** |
| **X** |  |  |

**Liste des impacts liés à la réalisation de procédure :**

La procédure s’applique lorsqu’un équipement n’est plus joignable sur le réseau. Le service est donc déjà indisponible pour les utilisateurs concernés. L’application de cette procédure n’aura pas d’autre impact.

# procédure a dérouler

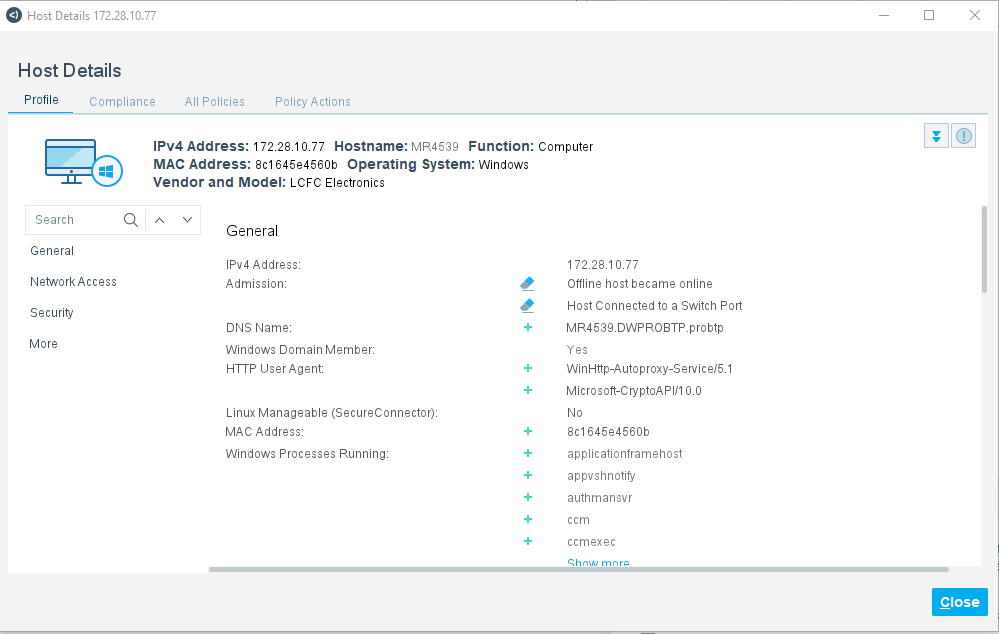
1. **Vérifier l’état de l’équipement concernée dans la console :**
   1. **Soit utiliser la recherche en haut au centre de la fenêtre : **
   2. **Soit dérouler l’arborescence et trouver l’équipement concernée dans la policy 4. Control puis rechercher l’équipement, il devrait se trouver en 4.1.2 pour les blocages wifi et 4.1.5 pour les blocages filaires**

****

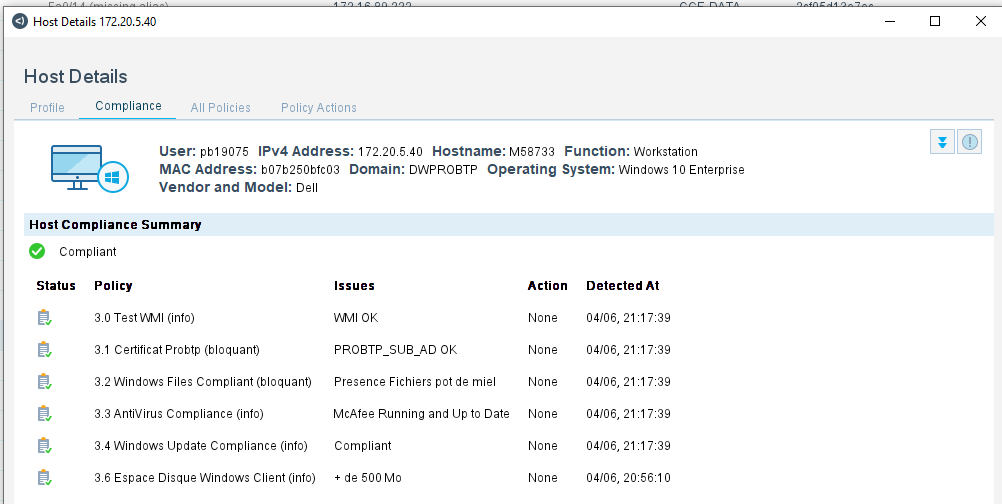
**Exemple d’équipements bloqué en filaire ou wifi **

****

1. **Etudier l’équipement en double cliquant dessus**
   1. **Onglet Profile (permet de retrouver toutes les informations remontées par le NAC sur l’équipement)**

****

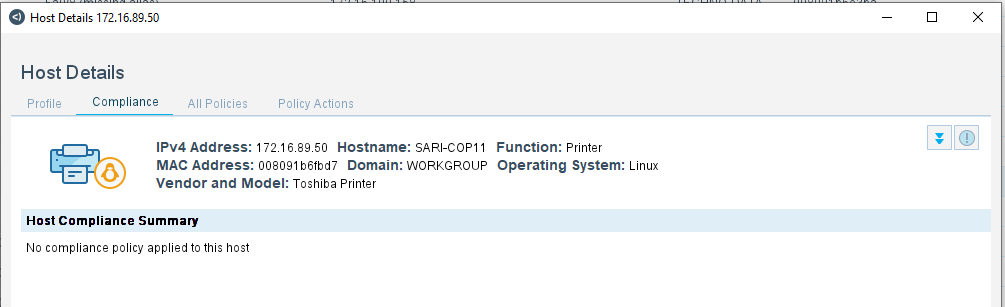
* 1. **Voir l’état de l’onglet Compliance afin de définir si c’est un poste de travail du domaine Probtp**

****

**Si le poste est bien sur le domaine Probtp, vous aurez des informations dans la partie compliance avec leurs statuts. ->poursuivre sur 4.3**

**Si ce n’est pas le cas vous aurez une indication « No Compliance policy applied to this host » comme pour l’exemple d’une imprimante ci-dessous.**

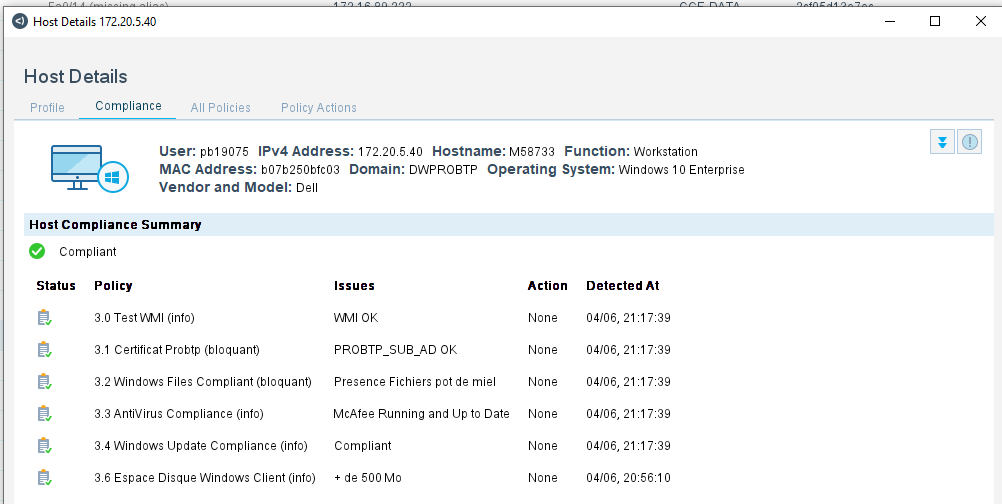
**Dans le cas où un poste de travail Probtp se retrouve dans cet état il semble avoir un problème de relation d’approbation au domaine ou ne fait plus partie du domaine, l’incident est à transférer à PDTGEST pour cause de poste Hors domaine ou en erreur d’approbation sur le domaine.**

****

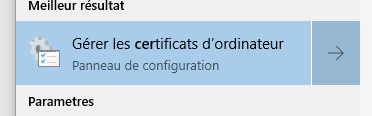
1. **Définir le point de blocage dans la compliance**

**Les différentes statues sont soit des infos soit bloquant. Les points bloquants sont soit 3.1 le certificat machine probtp, soit le 3.2 fichier Windows de compliance**

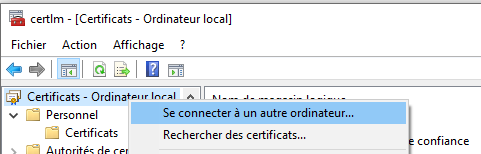
**Ce fichier est un pot de miel qui est mis en place sur le poste via un GPO, si le fichier n’est pas présent, c’est que le poste n’est potentiellement pas un poste Probtp, d’où le blocage.**

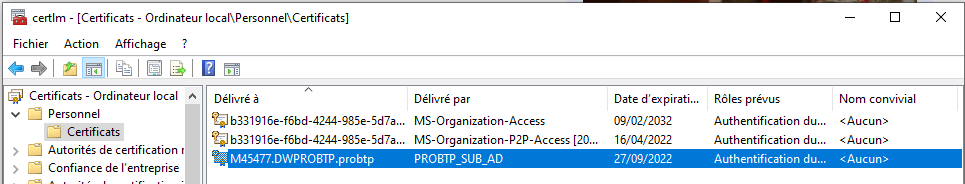
****

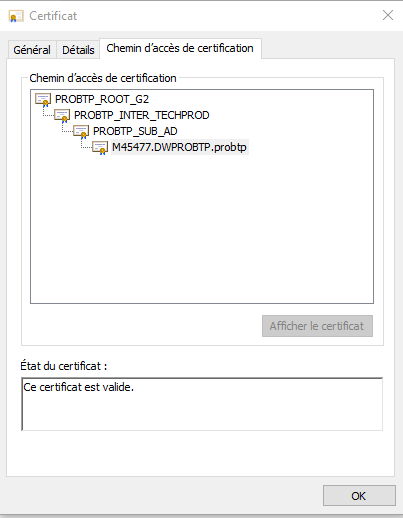
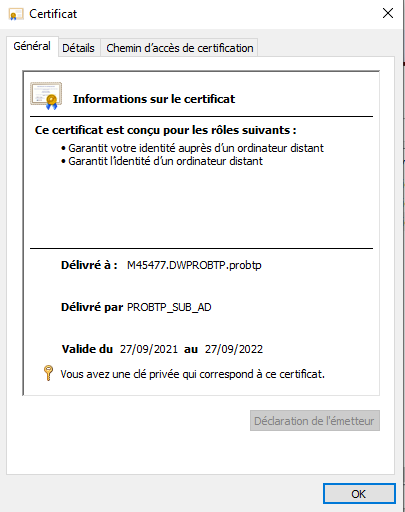
**3.1 Le certificat doit être accessible depuis le réseau.**

****

**Se connecter directement au poste qui est problématique via votre poste**

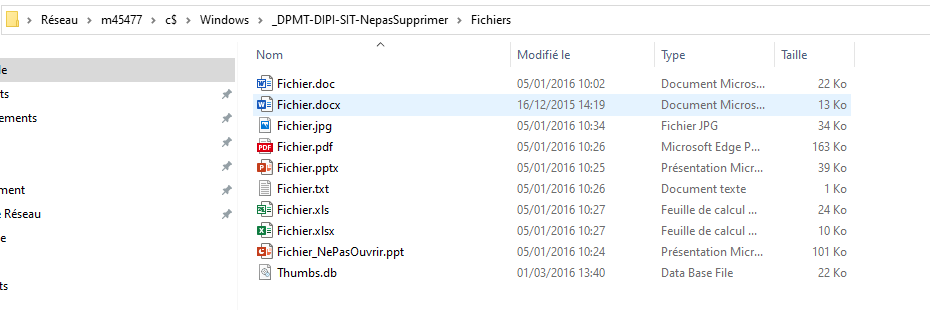
****

****

****

**3.2 le fichier windows de compliance doit être accessible depuis le réseau.**

**Vérification de présence du fichier « Fichier.docx » dans le répertoire \\Nom\_de\_la\_machine\c$\Windows\\_DPMT-DIPI-SIT-NepasSupprimer\Fichiers**

****

**Attention cette vérification doit être faite via le réseau pour confirmer la possibilité d’accès au fichier depuis le serveur Forescout.**

**Pour ces 2 situations si inaccessible via le réseau alors que la machine est en ligne vous pouvez mettre le poste de travail en white list, pour les postes PROBTP/Audiens/MME, appliquer la procédure INC-N2\_PROBTP\_PROD\_PDT-WATCHDOG\_Deblocage-Machine pour débloquer la machine, si ce n’est pas un poste corporate transmettre à l’équipe SOC pour analyse sans déblocage.**

# Vérification

**Liste des vérifications à effectuer :**

1. **Vérification de l’appartenance au domaine**
2. **Vérification de l’accès au certificat machine**
3. **Vérification de l’accès au certificat machine**