Interopérabilité scripts Windows GPO et Cisco NAC

Contenu

Introduction

Ce document fournit une configuration d'échantillon pour Windows GPO au startup PC et à la connexion d'utilisateur au domaine. Windows GPO peut être configuré pour exécuter de divers scripts au startup PC et à la connexion d'utilisateur au domaine. Les scripts sont employés souvent par entreprise pour configurer des variables d'environnement, pour tracer les lecteurs etc. de distant.

Le Cisco NAC contrôle l'accès au réseau quand l'utilisateur se connecte d'abord et des essais pour ouvrir une session à l'ordinateur Windows.

Les scripts peuvent être classifiés comme scripts de startup/arrêt et de connexion/déconnexion.

Passages startup de Windows et scripts d'arrêt dans le contexte d'ordinateur. Ceci fonctionne seulement si l'appliance NAC ouvre les ressources de réseau appropriées exigées par le script pour le rôle particulier quand ces scripts sont exécutés au démarrage ou à l'arrêt PC, qui sont typiquement le rôle unauthenticated.

Des scripts de connexion et de déconnexion sont exécutés dans le contexte d'utilisateur, ainsi il signifie que le script de connexion exécute après que l'utilisateur ait ouvert une session par des fenêtres GINA. Le script de connexion peut pour exécuter et/ou se terminer l'exécution si l'authentification de l'utilisateur ou l'estimation de posture d'ordinateur ne se termine pas et l'accès au réseau n'est pas accordé à temps. Ces scripts peuvent également être interrompus par l'adresse IP régénèrent initié par l'agent NAC après qu'un événement de connexion OOB.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

Recommandations générales pour des scripts GPO

Ce sont des recommandations générales pour des scripts GPO :

1. Exécutez les scripts en mode visible quand vous mettez au point. Ceci permet l'indication visuelle que les scripts de connexion sont exécutés réellement.Cette stratégie GPO peut être configurée sous la **stratégie > la configuration utilisateur de domaine > les modèles > le système > les scripts administratifs**.
2. Assurez-vous que les attentes d'ordinateur le réseau pour être disponible au startup et à la connexion d'ordinateur.Cette stratégie GPO peut être configurée sous la **stratégie > la configuration de l'ordinateur de domaine > les modèles > le système > la connexion administratifs**.

Recommandations générales pour l'installation NAC

Ce sont des recommandations générales pour le NAC installé si utilisé avec le GPO :

1. Permettez au trafic requis pour circuler à travers CAS dans un rôle unauthenticated pour permettre la connexion de domaine windows et la copie des scripts de connexion de l'AD à la machine cliente au-dessus du réseau pour l'exécution.`Ports are TCP : 88,123,135,137,139,389,445,1025,1026,3268`
   `Ports are UDP : 88,123,135,137,139,389,445,1025,1026,3268`
   `Allow Fragmented packets and ICMP to all domain controllers.` **Remarque:** Windows emploie le processus de découverte de PING pour trouver le C.C le plus proche où il y a plus d'un C.C pour un domaine donné. Au cas où l'ICMP ne serait pas permis à deux DCS, le client peut prendre plus long pour ouvrir une session puisqu'il prend un C.C aléatoire si la

découverte initiale échoue.
2. Puisque c'est un environnement d'AD de Windows, utilisez ADSSO comme méthode d'authentification, si possible. Ceci automatise et accélère le processus de connexion d'utilisateur, aussi bien qu'améliore l'expérience utilisateur globale.

Configurez

Plusieurs scénarios et configurations du NAC suggérées suivent.

Scénario 1

Les scripts de connexion de Windows sont exécutés du contrôleur d'AD et sont exécutés asynchrone.

L'exécution asynchrone de script est le comportement par défaut pour l'AD Win2003. Quand le script de connexion de Windows est exécuté asynchrone, il contrôle de transmission de nouveau au processus de connexion de Windows après qu'il appelle le script. Il n'attend pas le script pour terminer l'exécution. Ceci permet à d'autres programmes de démarrage et à l'agent NAC pour charger normalement.

Si les scripts de connexion exigent l'accès au réseau, qui sont contrôlés par l'appliance NAC et sont accessibles après que connexion réussie d'utilisateur au NAC, le script de connexion peut éprouver un certain retard. Vérifiez le script de connexion pour apprendre la Disponibilité de réseau avant que le script de connexion réel exécute, par exemple :

```
:CHECK
@echo off
echo Please wait....
ping -n 1 -l 1 10.10.10.10
if errorlevel 1 goto CHECK
@echo on

# Now the actual Logon script:

net use L: \\fileserver\share
```

Remarque: Modifiez le script selon la topologie du réseau.

Puisque ce contournement est simple, il fonctionne bien tant que les scripts de connexion sont exécutés asynchrone, et il n'y a aucune modification d'adresse IP impliquée en raison de hors du déploiement de la bande NAC ou autrement.

Si les scripts sont exécutés synchroniquement, ce contournement échoue parce que l'agent NAC ne charge pas en la mémoire avant que le script de connexion termine l'exécution, et le script de connexion ne se termine jamais l'exécution parce qu'il attend la Disponibilité de ressource de réseau, qui devient disponible seulement après que l'agent NAC authentifie le PC client.

Cette copie d'écran prouve que le PC client reste dans cet état de boucle infinie pour la raison mentionnée.

Ce scénario peut également échouer dans une situation où les scripts sont exécutés asynchrone au-dessus d'une liaison WAN lente où les scripts eux-mêmes peuvent prendre un moment pour les télécharger, et le NAC est déployé dans la topologie OOB où l'IP régénèrent peut être configuré. Un IP régénèrent au milieu de l'exécution de script peut potentiellement casser

l'exécution de script. Dans comme le scénario, Cisco recommande vivement que vous exécutiez des scripts synchroniquement de sorte que l'IP régénèrent le processus ne gêne pas l'exécution de script. Ce scénario dépeint une telle situation.

Scénario 2

Les scripts de connexion de Windows fonctionnent du contrôleur d'AD synchroniquement.

Des scripts synchrones sont recommandés dans le déploiement NAC OOB où l'IP régénèrent a lieu.

L'idée de base est de couper la fonctionnalité du script de connexion d'origine en deux scripts.

Le script *un*, qui est exécuté comme script de connexion, copie juste le deuxième script sur l'ordinateur local pour l'exécution à une date ultérieure quand l'agent NAC a authentifié, et on accorde l'accès au réseau.

Le deuxième script peut s'appeler par le programme de startup de Windows automatiquement si vous placez le deuxième script dans le répertoire de démarrage de l'utilisateur, par exemple :

Script 1 :

Le script de connexion exécuté de l'AD a copié le script réel appelé le « mount.bat » sur le répertoire de démarrage de l'utilisateur pour l'exécution postérieure.

```
echo Please wait....
sleep 20
copy \\1.1.1.11\SHARE\mount.bat
   "c:\Documents and Settings\All users\Start Menu\Programs\Startup\mount.bat"
```

Remarque: Modifiez le script pour adapter à la topologie du réseau.

Remarque: Permettez au trafic requis pour circuler à travers CAS dans un rôle unauthenticated pour permettre la connexion de domaine windows et la copie des scripts de connexion de l'AD à la machine cliente au-dessus du réseau pour l'exécution.

Script 2

Le script secondaire, où l'action réelle se produit est exécuté localement du système et supprimé après exécution pour des raisons de sécurité.

```
ipconfig
:CHECK
@echo off
echo Please wait....
sleep 10
Ping -n 1 -l 1 10.10.10.10
if errorlevel 1 goto CHECK
@echo on
# Now the actual Logon script:

net use L: \\fileserver\share
del c:\Documents and Settings\All users\Start Menu\Programs\Startup\mount.bat"
```

Cette copie d'écran dépeint que le deuxième script qui fonctionne à l'arrière-plan est lancé du répertoire de démarrage de l'utilisateur, et l'agent NAC fait un IP régénèrent après qu'il authentifie. Le deuxième script fait une boucle et attend l'agent pour se terminer l'authentification et l'IP

régénèrent le processus avant qu'il se termine et trace les lecteurs.

Dépannez

Le dépannage doit être fait sur le cas par cas, toutefois capturer des paquets outre du switchport sur lequel le PC client est connecté est une grande manière de commencer. Ceci te donnera la vue au sujet des événements réseau et des activités.

Informations connexes

- Support et documentation techniques - Cisco Systems