Dispositif NAC (CCA) : Configurer et dépanner l'authentification unique de Windows Active Directory

Contenu

Introduction

Ce document décrit comment utiliser le Répertoire actif de Microsoft Windows (AD) simple se connectent (SSO) afin de configurer et dépanner l'appliance du Cisco Network Admission Control (NAC), autrefois connue sous le nom de Cisco Clean Access (CCA).

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Assurez-vous le Windows 2000 de passages C.C SP4 ou Windows 2003 (norme ou entreprise) SP1 ou Windows 2003 R2. Windows 2003 sans SP1 n'est pas pris en charge.
- Assurez-vous que Windows SSO est pris en charge dans un environnement d'AD seulement. L'environnement de Windows NT n'est pas pris en charge. Clean Access Agent est exigé.
- Installez le compte de Clean Access Server (CAS) comme décrit dans l'appliance de Cisco NAC - guide d'installation et de configuration de Clean Access Server, la version 4.1(2).

Composants utilisés

Les informations dans ce document sont basées sur la version de logiciel 4.x d'appareils NAC ou plus tard.

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.

Configurez Windows SSO

Les informations dans cette section décrivent comment configurer les caractéristiques présentées dans ce document.

Installez le fournisseur de l'AD SSO

- Vous ne pouvez pas réaliser un essai d'authentification à un fournisseur ou à un VPN SSO de l'AD SSO.
- Le serveur de consultation de LDAP est nécessaire seulement si les utilisateurs veulent faire des règles de mappage pour l'AD SSO, de sorte qu'après l'AD SSO, les utilisateurs soient placés dans les rôles basés sur des attributs d'AD. Ce n'est pas nécessaire pour obtenir le fonctionnement de base SSO (sans mappage de rôle).

Exécutez KTPass sur le C.C

KTPass est un outil disponible comme partie de Windows 2000/2003 outil d'assistance. Référez-vous à l'appliance de Cisco NAC - Le guide d'installation et de configuration de Clean Access Server, libèrent 4.1(2) le pour en savoir plus.

Quand vous exécutez KTPass, il est important de noter que le nom de l'ordinateur qui tombe toujours entre « / » et « @ » apparie le nom du C.C car il apparaîtrait sous le panneau de configuration > le système > le nom de l'ordinateur > complètement nom de l'ordinateur sur le C.C.

En outre, assurez-vous que le nom de royaume qui apparaît après @ mis en valeur est toujours

dans les lettres majuscules.

```
C:\Program Files\Support Tools>ktpass -princ
 ccasso/prem-vm-2003.win2k3.local@WIN2K3.LOCAL -mapuser ccasso -pass Cisco123 -out
c:\test.keytab -ptype KRB5_NT_PRINCIPAL +DesOnly Using legacy password setting method //confirms
ccasso acct is mapped Successfully mapped ccasso/prem-vm-2003.win2k3.local to ccasso. Key
created. Output keytab to c:\test.keytab Keytab version: 0x502 keysize 80 ccasso/prem-vm-
2003.win2k3.local@WIN2K3.LOCAL ptype 1 (KRB5_NT_PRINCIPAL) vno 3 etype 0x17 (RC4-HMAC) keylength
16 (0xf2e787d376cbf6d6dd3600132e9c215d) Account ccasso has been set for DES-only encryption.
```

Afin de prendre en charge le Windows 7, vous devez exécuter KTPASS suivant les indications de cet exemple :

```
C:\Program Files\Support Tools>KTPASS.EXE -princ
newadsso/[adserver.]domain.com@DOMAIN.COM -mapuser newadsso -pass PasswordText -out
c:\newadsso.keytab -ptype KRB5_NT_PRINCIPAL
```

En outre, assurez-vous que le nom de royaume qui apparaît après @ mis en valeur est toujours dans les lettres majuscules.

Configurez SSO sur CAS

Choisissez les **serveurs de CCA > gèrent > authentification > Windows authentique > le Répertoire actif SSO** afin d'ouvrir la fenêtre d'AD, et vérifient ces éléments :

- Domaine de Répertoire actif : Le nom de royaume de Kerberos = doit être majuscule.
- Serveur de Répertoire actif (FQDN) : Assurez-vous que CAS peut résoudre ce nom par l'intermédiaire des DN. Ce champ ne peut pas être une adresse IP. Utilisant les valeurs dans cet exemple, vous pouvez ouvrir une session à CAS par l'intermédiaire du Protocole Secure Shell (SSH), et exécutez le « nslookup prem-vm-2003.win2k3.local ». Puis, assurez-vous qu'il le résout avec succès.
- Assurez-vous que le FQDN apparie le nom du serveur d'AD (C.C) exactement pendant qu'il apparaît sous le panneau de configuration > le système > le nom de l'ordinateur | Plein nom de l'ordinateur sur l'ordinateur hôte d'AD (C.C).

Vérifiez le service SSO est commencé

Procédez comme suit :

1. Allez aux **serveurs de CCA > gèrent > état** afin de vérifier que le service SSO est commencé.
2. Exécutez cette commande afin de vérifier que CAS écoute maintenant sur le TCP 8910 (utilisé pour Windows SSO).`[root@cs-ccas02 ~]#netstat -a | grep 8910 tcp 0 0 *:8910 *:* LISTEN`

Ports ouverts au C.C

Afin d'ouvrir les ports appropriés au C.C, terminez-vous ces étapes :

Remarque: Pour tester, ouvrez toujours l'accès complet au C.C. Puis, une fois que SSO fonctionne, vous pouvez l'attacher pour avaler aux ports spécifiques.

1. Assurez-vous qu'on permet les ports suivants dans le rôle non approuvé au Répertoire actif :**TCP** : 88, 135, 445, 389/636, 1025, 1026**UDP** : 88, 389**Remarque:** *Le PORT TCP 445* doit

être ouvert pour le mot de passe de Windows remis à l'état initial pour fonctionner correctement.
2. Assurez-vous que le client exécute l'agent 4.0.0.1 de CCA ou plus tard.
3. Ouvrez une session au PC avec les qualifications de domaine windows.**Remarque:** Assurez-vous que vous vous connectez dans le domaine et pas le compte local.

Le client voit l'agent exécuter SSO

SSO terminé

Utilisateur SSO vu sur la liste d'utilisateur en ligne

Dépannez Windows SSO

Erreur : N'a pas pu commencer le service SSO. Veuillez vérifier la configuration.

Problème

Vous recevez cette erreur :

Solution

Pour résoudre ce problème, exécutez les étapes suivantes :

1. Vérifiez pour s'assurer des passages de KTPass correctement. Il est important de vérifier les champs comme mentionné dans diapositive X. Si KTPass était exécuté inexactement, supprimez le compte et créez un nouveau compte sur l'AD et le passage KTPass de nouveau.
2. Assurez-vous que le temps sur CAS est synchronisé avec le C.C.Cette étape peut être exécutée en les indiquant chacun des deux le même Serveur de synchronisation. Dans des installations de laboratoire, indiquez CAS le C.C lui-même pendant le temps (le C.C exécute le temps de Windows). Le Kerberos est sensible pour synchroniser et la distorsion ne peut pas être plus grande que 5 minutes (300 sec).**Remarque:** Quand vous essayez de commencer le service de l'AD SSO de CAS, une question pourrait se produire avec le syncronization de temps, NTP. Si le NTP est configuré, et des horloges pas syncronized, les services ne fonctionneront pas. Une fois que réparé les services devraient fonctionner.
3. Assurez-vous que le domaine de Répertoire actif est dans le haut de casse (royaume) et CAS peut résoudre le FQDN dans des DN. Pour des installations de laboratoire, vous pouvez indiquer un C.C qui exécute des DN (l'AD exige au serveur DNS du bail un).
4. Connectez-vous dans CAS directement comme <CAS-IP-adresse >/admin de https://. Puis, les **logs de support de** clic et changent le niveau se connectant pour la transmission de Répertoire actif se connectant aux **informations**.
5. Recréez le problème et téléchargez les logs de support.

L'authentification client ne fonctionne pas

Problème

Le service de l'AD SSO est commencé, mais l'authentification client ne fonctionne pas.

Solution

Les ports UDP n'étaient pas ouverts dans le rôle unauthenticated. Après que vous ajoutiez ces ports aux stratégies de trafic, l'authentification devrait fonctionner.

Incapable d'exécuter SSO sur le PC des fenêtres 7

Problème

SSO ne fonctionne pas pour les ordinateurs qui exécutent le Windows 7 du système d'exploitation.

Solution 1

Afin de résoudre ce problème, le chiffrement DES d'enable sur l'ordinateur qui exécute le système d'exploitation de Windows 7, et réexécutent alors le KTPass. Terminez-vous ces étapes afin d'activer le DES sur un PC de Windows 7 :

1. Procédure de connexion à la machine cliente de Windows 7 en tant qu'administrateur.
2. Allez au **début > au panneau de configuration > au système et à la Sécurité > aux outils d'administration > à la stratégie de sécurité locale > des stratégies locales/Sécurité > options**.
3. Choisissez la **sécurité des réseaux > configurent des types de cryptage permis**.
4. Sur l'onglet Settings de sécurité locale, vérifiez les cases pour activer toutes les options, à moins que le futur cryptage tape l'option.

Solution 2

Afin de résoudre ce problème, exécutez cette commande sur le serveur Windows 2003 (s'il doit prendre en charge le Windows 7 aussi bien) :

```
C:\Program Files\Support Tools> ktpass.exe -princ
casuser/cca-eng-domain.cisco.com@CCA-ENG-DOMAIN.CISCO.COM-mapusercasuser -pass
Cisco123 -out c:\casuser.keytab -ptype KRB5_NT_PRINCIPAL
```

Le pour en savoir plus, se rapportent configurent l'AD SSO dans un environnement de Windows 7.

Incapable de configurer le soutien de client Linux d'un utilisateur dans l'environnement NAC

Problème

Incapable de configurer le soutien de client Linux d'un utilisateur dans l'environnement NAC.

Solution

L'agent de Web ou l'agent ne sont pas pris en charge sur le Linux. Le NAC prend en charge le Linux avec la procédure de connexion de Web seulement sans n'importe quelle estimation de posture. Une fois l'ordinateur est authentifié par la procédure de connexion de Web, l'utilisateur devrait être assigné à un rôle de l'utilisateur final que vous configurez. L'utilisateur aura alors accès selon la stratégie de trafic du rôle de l'utilisateur. Référez-vous au pour en savoir plus de la bogue Cisco CSCti54517 (clients enregistrés seulement).

Le service SSO est commencé, mais le client n'exécute pas SSO

C'est habituellement dû à une certaine question de transmission entre le PC DC/client ou entre le PC client et le CAS.

Voici quelques choses à vérifier :

- Le client a des clés de Kerberos.
- Les ports sont ouverts de C.C ainsi le client peut se connecter, recevoir des logs d'agent, et recevoir ouvre une session CAS.
- Le temps ou l'horloge sur le PC client est synchronisé avec le C.C.
- Confirmez CAS écoute sur le port 8910. Un tracé de renifleur sur le PC client aidera également.
- L'agent de CCA est 4.0.0.1 ou plus tard.
- L'utilisateur est ouvert une session réellement utilisant le compte de domaine et pas utilisant le compte local.

Kerbtray

Kerbtray peut être utilisé pour confirmer que le client a obtenu les tickets Kerberos (TGT et St). Le souci est pour le ticket de service (St), qui est pour le compte de CAS que vous avez créé sur le C.C.

Kerbtray est un outil gratuit fourni par des outils d'assistance de Microsoft. Il peut également être utilisé pour purger les tickets Kerberos sur une machine cliente.

Une icône verte de Kerbtray sur la barre d'état système indique que le client a les tickets Kerberos actifs. Cependant, vous devez vérifier que le ticket est correct (valide) pour le compte de CAS.

Logs de CAS – Ne peut pas commencer le service SSO

Le fichier journal d'intérêt sur CAS est /perfigo/logs/perfigo-redirect-log0.log.0.

Le service de l'AD SSO ne commence pas sur CAS est une question de transmission CAS-DC :

1. `SEVERE: startServer - SSO Service authentication failed. Clock skew too great (37)` `Aug 3, 2006 7:52:48 PM com.perfigo.wlan.jmx.admin.GSSServer loginToKDC` Ceci signifie que l'horloge n'est pas synchronisée entre CAS et le contrôleur de domaine.
2. `Aug 21, 2006 3:39:11 PM com.perfigo.wlan.jmx.admin.GSSServer loginToKDC INFO: GSSServer - SPN : [ccass/PreM-vM-2003.win2k3public.local@WIN2K3PUBLIC.LOCAL] Aug 21, 2006 3:39:11 PM com.perfigo.wlan.jmx.admin.GSSServer loginToKDC SEVERE: startServer - SSO Service authentication failed. Client not found in Kerberos database (6) Aug 21, 2006 3:39:11 PM com.perfigo.wlan.jmx.admin.GSSServer startServer WARNING: GSSServer loginSubject could not be created.` Ceci signifie que le nom d'utilisateur est incorrect. Notez le nom d'utilisateur erroné « ccass », code d'erreur 6 et le dernier avertissement.
3. `Aug 21, 2006 3:40:26 PM com.perfigo.wlan.jmx.admin.GSSServer loginToKDC INFO: GSSServer - SPN : [ccasso/PreM-vM-2003.win2k3public.local@WIN2K3PUBLIC.LOCAL] Aug 21, 2006 3:40:26 PM com.perfigo.wlan.jmx.admin.GSSServer loginToKDC SEVERE: startServer - SSO Service authentication failed. Pre-authentication information was invalid (24) Aug 21, 2006 3:40:26 PM com.perfigo.wlan.jmx.admin.GSSServer startServer WARNING: GSSServer loginSubject could not be created.` Le mot de passe est incorrect ou le

royaume est non valide (pas dans le haut de casse ?). Mauvais FQDN ? KTPass s'exécute inexactement ? Notez l'erreur 24 et le dernier avertissement.**Remarque:** Assurez-vous que la version de KTPass est 5.2.3790.0. À moins qu'il y ait une mauvaise version de KTPass qui même si le script est exécuté correctement, le service SSO ne commencera pas.

Client – Question de transmission de CAS :

```
Aug 3, 2006 10:03:05 AM com.perfigo.wlan.jmx.admin.GSSHandler run
         SEVERE: GSS Error: Failure unspecified at GSS-API level (Mechanism level: Clock skew
too great (37))
```

Cette erreur est vue quand le temps de PC client n'est pas synchronisé avec le C.C.

Remarque: La différence entre cette erreur et celle où le temps de CAS n'est pas synchronisé avec le C.C.

Problèmes identifiés

- L'agent 4.0 de l'ID de bogue Cisco CSCse64395 (clients enregistrés seulement) — ne résout pas des DN pour Windows SSO.Cette question est résolue dans l'agent 4.0.0.1 de CCA.
- L'ID de bogue Cisco CSCse46141 (clients enregistrés seulement) — SSO échoue au cas où CAS ne pourrait pas atteindre le serveur d'AD pendant le startup.Le contournement est d'aller aux **serveurs de CCA > gèrent l'authentification [CAS_IP] > le Windows authentiques > le Répertoire actif SSO**, et cliquent sur la **mise à jour** afin de redémarrer le service de l'AD SSO.
- Exécutez une reprise de perfigo de service sur CAS. Il y a une question de mise en cache quand les vieilles qualifications sont cachées sur CAS et il n'utilise pas le neuf jusqu'à ce que Tomcat soit redémarré.
- Vous ne pouvez pas limiter la procédure de connexion de seul utilisateur pour SSO. C'est le comportement normal pour SSO parce que c'est un protocole de Kerberos, et il n'y a aucune option de limiter la procédure de connexion de seul utilisateur un protocole de Kerberos.
- *Le Windows 7* et le *Windows 2008* ne prennent en charge pas SSO pendant que SSO utilise le **chiffrement DES** qui n'est pas pris en charge par le Windows 7 ou le Windows 2008.

Informations connexes

- Page de support de Dispositif Cisco NAC (Clean Access)
- Support et documentation techniques - Cisco Systems