Configuration de la connexion à authentification unique Active Directory pour NAC Guest Server

Contenu

Introduction

Le Kerberos simple d'utilisations de caractéristique d'ouverture de session de Répertoire actif (AD SSO) entre le navigateur Web du client et le Cisco NAC Guest Server afin d'authentifier automatiquement un invité contre un contrôleur de domaine de Répertoire actif.

Remarque: Afin de ce document, le NTP et les serveurs DNS sont également sur le C.C, mais ce n'est probablement pas le cas dans votre environnement.

Conditions préalables

Conditions requises

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

- Des DN doivent être configurés et travail sur le Cisco NAC Guest Server.
- Des DN doivent être configurés et travail sur le contrôleur de domaine.
- Les entrées DNS pour le Cisco NAC Guest Server doivent être définies :Un enregistrementEnregistrement *PTR*
- Les entrées DNS pour le contrôleur de domaine doivent être définies :Un enregistrementEnregistrement *PTR*
- Des paramètres horaires de Cisco NAC Guest Server doivent être synchronisés avec le domaine de Répertoire actif.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- NAC Guest Server 2.0
- Microsoft Windows XP avec l'Internet Explorer 6.0
- Windows Server 2003

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

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

Configurations

Ce document utilise ces adresses IP :

- Contrôleur de domaine — 172.23.117.46 (w2k3-server.cca.cisco.com)
- NAC Guest Server — 172.23.117.42 (ngs.cca.cisco.com)
- Ordinateur de sponsor — 172.23.117.45

Procédez comme suit :

1. Accédez à l'interface d'admin NGS. Du navigateur, allez à **http://172.23.117.42/admin**
2. **Configuration réseau NGS**Choisissez le **serveur > les paramètres réseau**.Adresse Internet — ngsDomaine — cca.cisco.comDNS principal — 172.23.117.46
3. **Installation de NTP**Dans le **serveur > le date/heure**, configurez le serveur de NTP à IP **172.23.117.46** C.C.
4. **Installation de l'AD SSO**Avant que vous configuriez la section SSO, veillez les enregistrements A et PTR pour exister pour le serveur de contrôleur de domaine et d'invité NAC.Dans l'AuthServer > la section authentique SSO, configurent ceci :Si la configuration est réussie, vous devriez voir un message de succès.

5. **Validez la caractéristique SSO**De l'ordinateur d'utilisateur, log dans le domaine. Dans cet exemple, cet ordinateur fait partie du domaine de cca. Seulement l'Internet Explorer est pris en charge pour la caractéristique SSO. Vous devez s'assurer que le NAC Guest Server fait partie d'intranet local et l'automatique-procédure de connexion est activée.**Remarque:** Employez le FQDN pour le serveur d'invité afin de tester SSO du navigateur. Par exemple, l'adresse IP ne fonctionne pas.Vérifiez les configurations de navigateur Web :Du navigateur Web, allez à **http://ngs.cca.cisco.com**. Vous devriez être automatiquement ouvert une session aux ngs avec les qualifications de domaine.**Remarque:** Le lien **http://ngs.cca.cisco.com** fonctionnera seulement si vous avez configuré le NAC en mode d'admin avec les identifiants utilisateurs.Sous les journaux d'audit de NAC Guest Server, vous pouvez voir l'utilisateur Niall connecté dans le groupe par défaut :
6. **Mappage de groupe d'utilisateurs avec l'AD SSO (facultatif)***Dans cette section vous apprendrez tracer l'utilisateur SSO à un groupe spécifique autre que le groupe par défaut.*Pour tracer le groupe d'utilisateurs avec ADSSO, vous devez configurer le serveur de Répertoire actif en tant que serveur authentique et puis tracer le groupe d'AD avec le groupe d'utilisateurs de sponsor.Choisissez **NGS (les authentifications de http://172.23.117.42/admin) > commandite > des serveurs de Répertoire actif**. Ajoutez un nouveau contrôleur de domaine.L'option de connexion de test a été introduite dans NGS 2.0 pour la facilité du dépannage. Il t'indique si vous avez configuré le C.C correctement.**Configurez le groupe d'utilisateurs**Ajoutez un nouveau nom de groupe d'utilisateurs **— tme**. Dans cet exemple, vous choisissez **AUCUN** afin d'entasser en vrac création de compte. De cette façon vous savez immédiatement si l'utilisateur a été placé au groupe de tme *ou au* groupe par défaut.Dans le mappage de Répertoire actif, l'utilisateur Niall de test est déjà une partie d'admins de domaine.

Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

Vérifiez le mappage de groupe d'utilisateurs ADSSO

Afin d'accéder à l'ordinateur de sponsor, ouvrez un nouveau navigateur et allez à http://ngs.cca.cisco.com.

Niall devrait être placé dans le groupe de tme sans l'accès pour entasser en vrac création de compte.

Si vous regardez les journaux d'audit, vous pouvez vérifier que le sponsor est placé dans le rôle correct.

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Ce sont des messages d'erreur dans les logs. Les erreurs de Kerberos a comme conséquence une de ces erreurs :

- `Le format de domaine incorrect/contrôleur de domaine doit être un FQDN, pas une adresse IP` Le domaine n'a pas été écrit dans un format correct (devrait être de la forme CCA.CISCO.COM).
- `L'adresse Internet doit être un FQDN, pas une adresse IP` L'adresse Internet du serveur d'invité NAC ne peut pas être une adresse IP que ce doit être un nom de domaine complet par exemple nac.cca.cisco.com.
- `Ne peut pas déterminer l'adresse IP pour le contrôleur de domaine` Il y a une question de configuration DNS.
- `Ne peut pas obtenir des DN un enregistrement pour le contrôleur de domaine` Il y a une question de configuration DNS.
- `Ne peut pas obtenir l'enregistrement des DN A pour l'adresse Internet` Il y a une question de configuration DNS.
- `Ne peut pas obtenir l'enregistrement PTR de DN pour l'adresse IP de contrôleur de domaine` Il y a une question de configuration DNS.
- `Ne peut pas obtenir l'enregistrement PTR de DN pour l'adresse IP d'adresse Internet` Il y a une question de configuration DNS.
- `Pour créer l'ordinateur expliquez ce serveur sur le contrôleur de domaine. Voir le journal d'application pour des détails` . Visualisez le journal d'application pour voir les détails complets de l'erreur.
- `Nom d'utilisateur/mot de passe non valide` Le nom d'utilisateur/mot de passe d'administrateur est incorrect.
- `Le domaine non valide ou ne peut pas résoudre l'adresse réseau pour le C.C` Il y a un problème de DN sur le serveur d'AD.
- `Le temps de contrôleur de domaine n'apparie pas le temps de ce serveur` Assurez la correspondance de temps de serveur, il vous est recommandé NTP d'utilisation pour synchroniser des temps de serveur.
- `Le C.C ne peut pas déterminer l'adresse Internet pour le serveur d'invité par consultation inverse. Il peut y a une question avec votre confiugration de DN.` Il y a une question de configuration DNS sur votre serveur d'AD.

Informations connexes

- Support et documentation techniques - Cisco Systems