

NAC : Configurer LDAP sur SSL sur Clean Access Manager (CAM)

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Configurez](#)

[Étapes pour configurer le LDAP au-dessus du SSL sur le CAM](#)

[Vérifiez](#)

[Dépannez](#)

[Informations connexes](#)

[Introduction](#)

Ce document décrit comment configurer le Protocole LDAP (Lightweight Directory Access Protocol) au-dessus du SSL sur Clean Access Manager (CAM).

[Conditions préalables](#)

[Conditions requises](#)

Cette configuration s'applique à la version 3.5 et ultérieures de CAM.

[Composants utilisés](#)

Les informations dans ce document sont basées sur la version 4.1 de Clean Access Manager.

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.

Note: Utilisez l'[Outil de recherche de commande](#) (clients [enregistrés](#) seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Étapes pour configurer le LDAP au-dessus du SSL sur le CAM

Procédez comme suit :

1. Obtenez le certificat racine du CA non approuvé qui a fourni le certificat au contrôleur de domaine et placez-le sur votre appareil de bureau. Choisissez l'**administrateur > le CAM > le certificat ssl**, et puis parcourez et téléchargez le certificat de CA de racine comme **confiance CA non standard**. Cliquez sur **vérifier** et installez le certificat de CA de racine.
2. Configurez le serveur LDAP sur le CAM. Choisissez la **gestion des utilisateurs > les serveurs authentiques** et choisissez **nouveau**. Choisissez le **LDAP** comme type d'authentification. Choisissez **ldaps://ip.address:636** comme URL de serveur. Choisissez le **SSL** comme type de Sécurité. Choisissez le **traitement (suivez) !** comme référence. Cette option est placée pour l'environnement de domaine de partition, par exemple, la racine et les domaines d'enfant. L'utilisateur et le mot de passe de privilège d'admin est requis de lier avec succès le CAM (client de LDAP) au serveur LDAP.
3. Obtenez le certificat sur le contrôleur de domaine (C.C). Quand vous demandez un certificat pour le C.C, veillez à mettre la NC comme nom de domaine complet de Répertoire actif. Les LDAP délivrent un certificat se trouve dans le stock personnel de certificat de l'ordinateur local. Référez-vous à [comment activer le LDAP au-dessus du SSL avec un](#) pour en savoir plus d'[autorité de certification de tierce partie](#).
4. Configurez le contrôleur de domaine pour le SSL. Sur votre C.C, choisissez le **début > tous les programmes > outils d'administration > utilisateurs et ordinateur de Répertoire actif**. Dans la fenêtre d'utilisateurs et d'ordinateurs de Répertoire actif, cliquez avec le bouton droit sur votre nom de domaine et choisissez **Propriétés**. Dans la boîte de dialogue **Propriétés de domaine**, choisissez l'onglet de **stratégie de groupe**. Choisissez la stratégie **par défaut de policy group de domaine** et puis cliquez sur **Edit**. Choisissez la **configuration de l'ordinateur > les paramètres de windows**. Choisissez les **paramètres de sécurité** et puis choisissez les **stratégies de clé publique**. Choisissez les **configurations automatiques de demande de certificat**. Utilisez l'assistant afin d'ajouter une stratégie pour le comme indiqué dans cet exemple de contrôleurs de domaine :
5. Vérifiez le contrôleur de domaine pour le LDAP au-dessus du SSL. Sur votre C.C, choisissez le **Start > Run** et tapez **ldp.exe**. Du menu de connexion, cliquez sur **Connectand** complètent les valeurs pour le serveur et le port. Ceci vérifie que le LDAP au-dessus du SSL est configuré correctement sur le C.C.
6. Choisissez la **gestion des utilisateurs > les serveurs authentiques > onglet AUTHENTIQUE de test** afin de vérifier la configuration de LDAP de CAM.

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- [Page de support d'appareils de Cisco NAC](#)
- [Support et documentation techniques - Cisco Systems](#)