Configurer LDAP sur Expressway pour l’accès Web, API et CLI

Table des matières

Introduction

Ce document décrit les étapes nécessaires pour activer le protocole LDAP (Lightweight Directory Access Protocol) sur le serveur Expressway et comment permettre aux groupes d’administrateurs d’accéder via le Web, l’interface de programmation d’application (API) et l’interface de ligne de commande (CLI) à Expressway avec vos utilisateurs de domaine.

Contribution de Jefferson Madriz et Elias Sevilla, Ingénieurs du centre d'assistance technique Cisco.

Conditions préalables

Exigences

- Connaissances de base sur Expressway.
- La configuration de base d’Expressway est déjà terminée.
- Active Directory (AD) déjà configuré.
- Règles de pare-feu prêtes, pour permettre la communication entre Expressway et le serveur AD.

Composants utilisés

- Active Directory installé sur Windows Server 2016.

- Serveur Expressway-C sur la version X14.0.3.

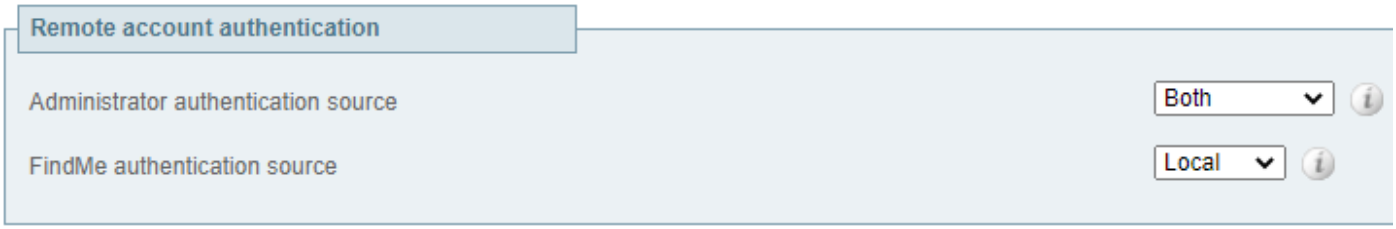
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configurer

Configuration LDAP

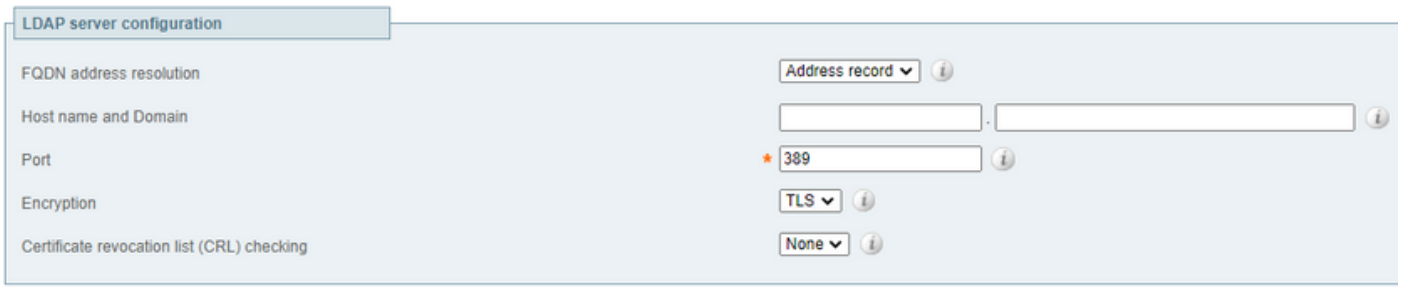
La page de configuration LDAP Users > LDAP configuration est utilisée pour configurer une connexion LDAP à un service d'annuaire distant pour l'authentification du compte administrateur.

- Authentification du compte distant : Cette section vous permet d'activer ou de désactiver l'utilisation du protocole LDAP pour l'authentification des comptes distants.



- Local uniquement : Les informations d'identification sont vérifiées par rapport à une base de données locale stockée sur le système.
- À distance uniquement : Les informations d'identification sont vérifiées par rapport à un répertoire externe.
- Les deux : Les informations d'identification sont d'abord vérifiées par rapport à une base de données locale stockée sur le système, puis s'il n'y a aucune correspondance avec le compte, le répertoire des informations d'identification externes est utilisé à la place.

- Configuration du serveur LDAP : cette section spécifie les détails de connexion au serveur LDAP.



Résolution d'adresse FQDN :

- Enregistrement SRV : recherche d'enregistrement de service (SRV) DNS (Domain Name Service).
- Enregistrement d'adresse : Recherche d'enregistrements DNS A ou AAAA.
- Adresse IP: saisie directement comme adresse IP.

Remarque : Si vous utilisez des enregistrements SRV, assurez-vous que _ldap._tcp. Les enregistrements utilisent le port LDAP standard 389. L'Expressway ne prend pas en charge les autres numéros de port pour LDAP.

Nom d'hôte et domaine :

- Enregistrement SRV: seule la partie Domaine de l'adresse du serveur est requise.
- Enregistrement d'adresse : saisissez le nom d'hôte et le domaine. Ils sont ensuite combinés pour fournir l'adresse complète du serveur pour la recherche d'enregistrement d'adresse DNS.
- Adresse IP: L'adresse du serveur est entrée directement en tant qu'adresse IP.

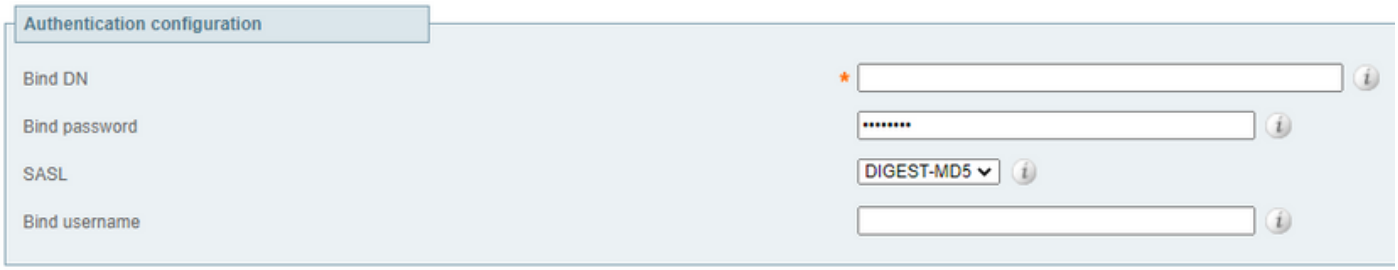
Port :

- Port IP à utiliser sur le serveur LDAP.

Chiffrement :

- TLS : utilise le cryptage TLS (Transport Layer Security) pour la connexion au serveur LDAP.
- Désactivé: aucun chiffrement n'est utilisé.

- Configuration de l'authentification: Cette section spécifie les identifiants d'authentification d'Expressway à utiliser pour effectuer la liaison avec le serveur LDAP.



DN de liaison : Nom unique (DN), non sensible à la casse, utilisé par l'Expressway pour établir une liaison avec le serveur LDAP. Il est important de spécifier le numéro de répertoire dans l'ordre cn=, then ou=, then dc=

Remarque : Le compte de liaison est généralement un compte en lecture seule sans privilèges spéciaux.

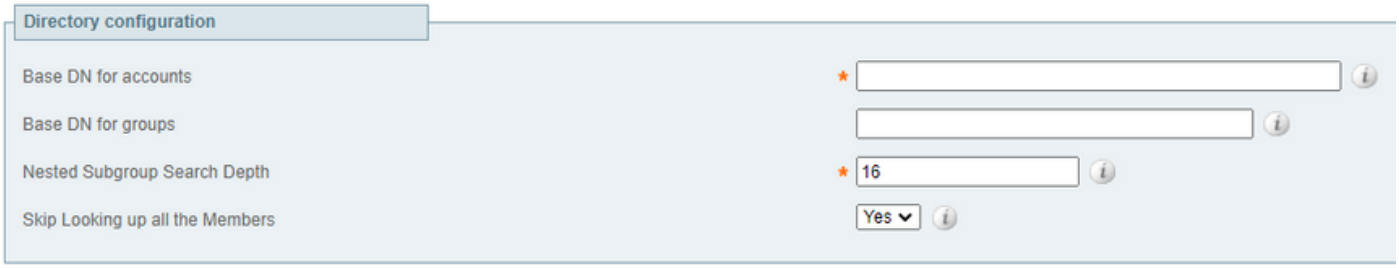
Mot de passe de liaison : Mot de passe (sensible à la casse) utilisé par l'Expressway pour établir une liaison avec le serveur LDAP.

SASL : Mécanisme SASL (Simple Authentication and Security Layer) à utiliser pour la liaison au serveur LDAP

- Aucune: aucun mécanisme n'est utilisé.
- DIGEST-MD5 : le mécanisme DIGEST-MD5 est utilisé.

Nom d'utilisateur : Nom d’utilisateur du compte utilisé par Expressway pour se connecter au serveur LDAP (sensible à la casse).

- Configuration du répertoire : Cette section spécifie les noms uniques de base à utiliser pour rechercher des noms de compte et de groupe.



DN de base pour les comptes : définition de l'unité d'organisation (OU) et du contrôleur de domaine (DC) du nom distinctif où la recherche de comptes d'utilisateurs commence dans la structure de base de données (non-respect de la casse).

Le DN de base des comptes et des groupes doit être au niveau DC ou sous celui-ci (inclure toutes les valeurs dc= et ou= si nécessaire). L'authentification LDAP ne recherche pas les comptes de sous-contrôleur de domaine, mais uniquement les niveaux d'unité d'organisation et de réseau commun (CN) inférieurs.

DN de base pour les groupes : définition de l'unité opérationnelle et du contrôleur de domaine du nom distinctif (Distinguished Name) selon laquelle la recherche de groupes doit commencer dans la structure de base de données (non sensible à la casse).

Si aucun DN de base pour les groupes n'est spécifié, le DN de base pour les comptes est utilisé pour les groupes et les comptes.

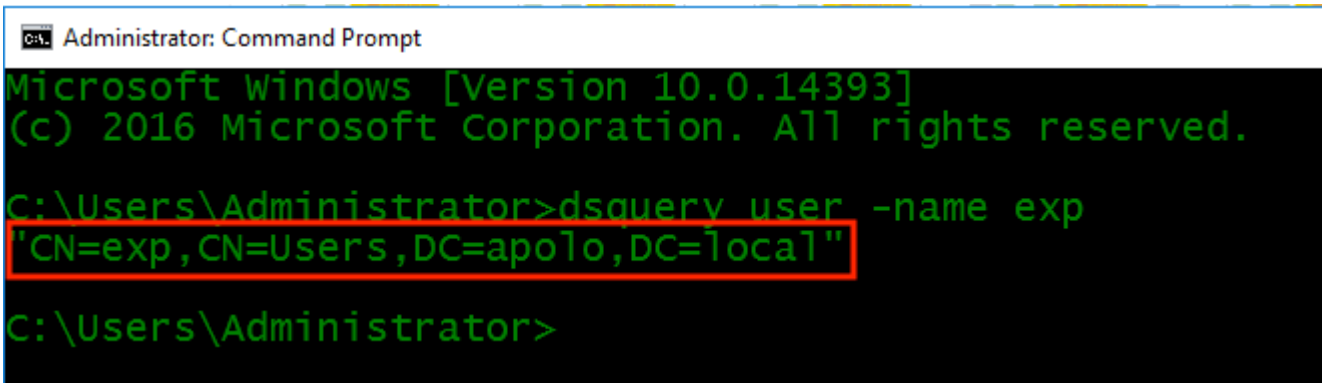
Profondeur de recherche de sous-groupes imbriqués : utilisée pour limiter la profondeur des groupes pour la recherche LDAP.

Ignorer la recherche de tous les membres : utilisé pour désactiver ou activer la recherche de membres d'un groupe d'administrateurs pendant le processus de recherche d'authentification. La valeur par défaut est Yes (Oui). Ignorez la recherche de membres.

Comment trouver le DN de base

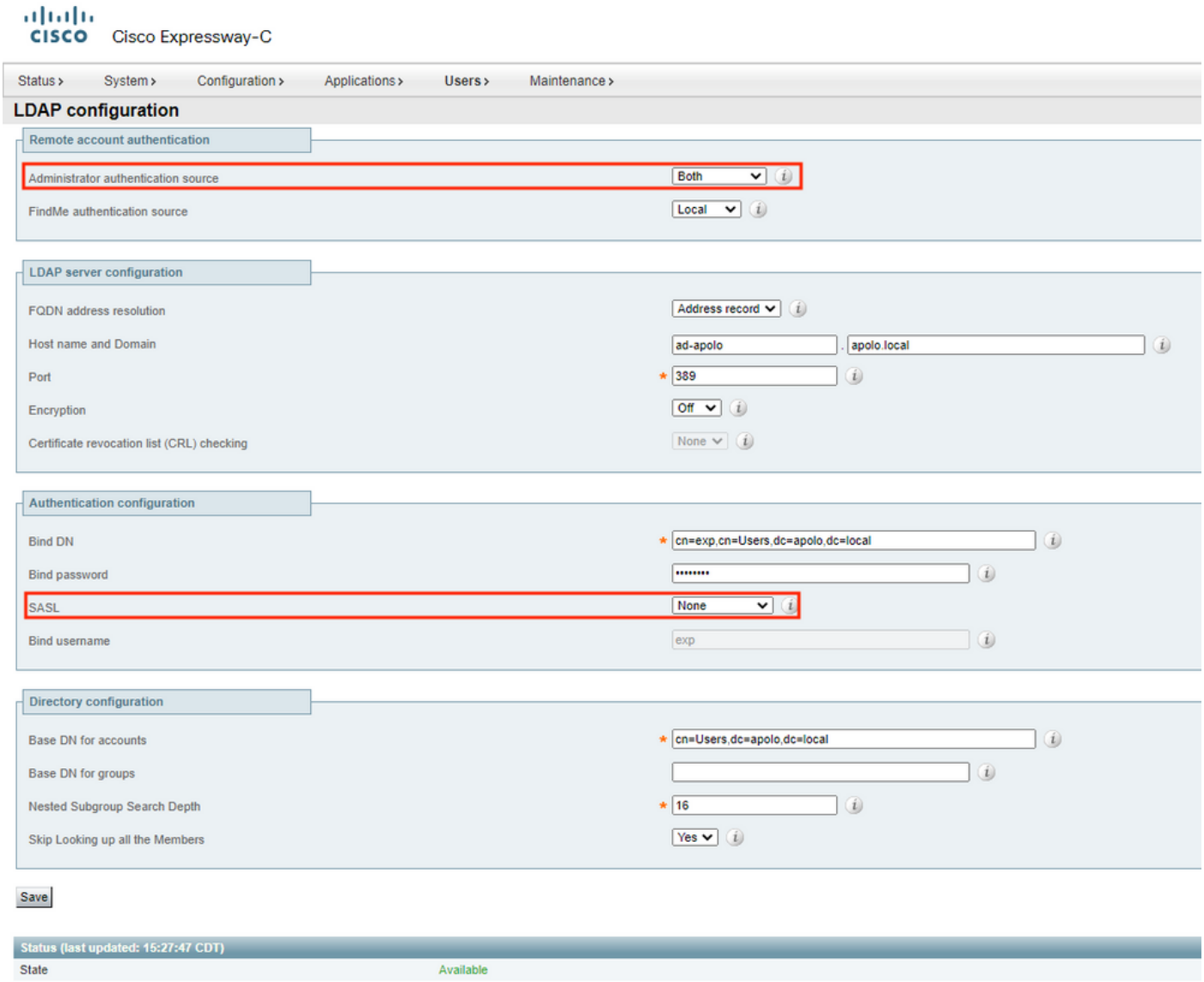
Sur le serveur AD, ouvrez Command Prompt (CMD) en tant qu'administrateur et exécutez la commande : **dsquery user -name**

.



Exemple de configuration LDAP

La source d'authentification administrateur est définie sur Les deux et SASL est définie sur Aucun dans cet exemple.



Vérifier l'état LDAP

Validez l'état de connexion du serveur LDAP :

- Disponible : Aucun message d'erreur ne s'affiche
- Échec : Les messages d'erreur s'affichent. Messages d'erreur LDAP

Configuration des groupes d'administrateurs

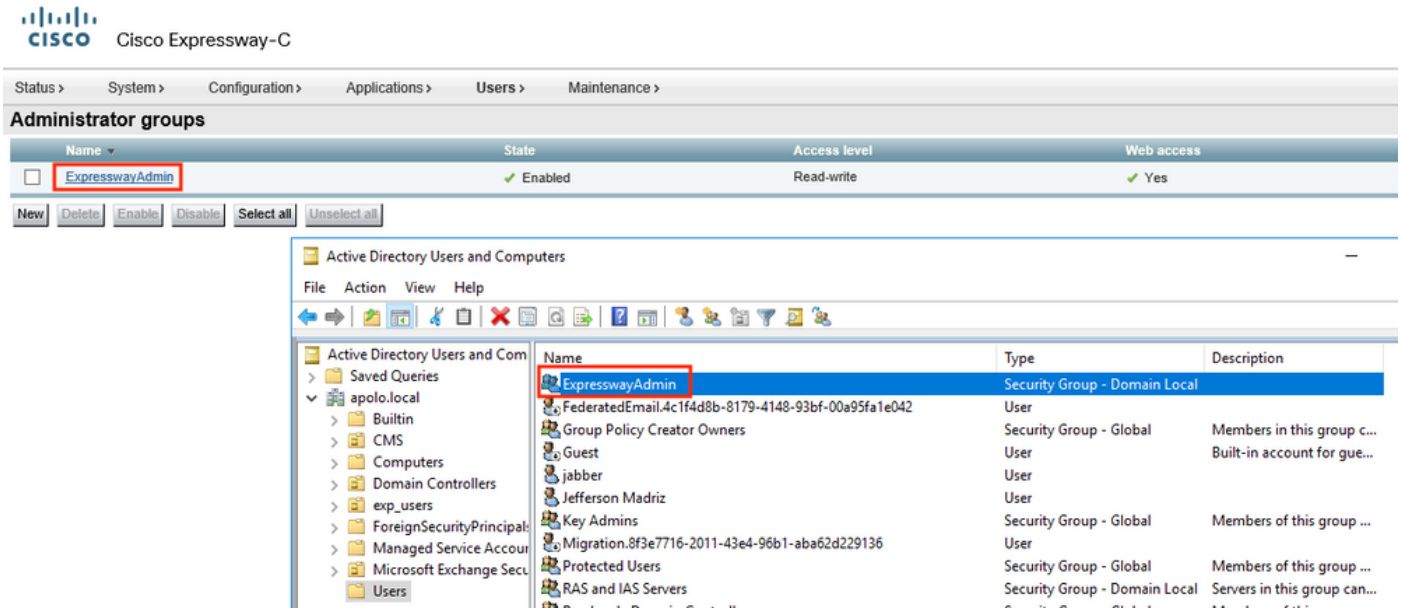
La page Groupes d’administrateurs Utilisateurs > Groupes d’administrateurs répertorie tous les groupes d’administrateurs qui ont été configurés sur l’Expressway et vous permet d’ajouter, de modifier et de supprimer des groupes.

Remarque : Les groupes d'administrateurs s'appliquent uniquement si l'authentification de compte distant via LDAP est activée.

Lorsque vous vous connectez à l’interface Web d’Expressway, vos informations d’identification sont authentifiées par rapport au service d’annuaire distant et vous disposez des droits d’accès associés au groupe auquel vous appartenez.

Options de configuration des groupes d’administrateurs sur Expressway

Name : Nom du groupe d’administrateurs. Les noms de groupe définis dans l’Expressway doivent correspondre aux noms de groupe configurés dans le service d’annuaire distant pour gérer l’accès administrateur à cet Expressway.



Niveau d'accès :

- Lecture-écriture : Permet d'afficher et de modifier toutes les informations de configuration. Les mêmes droits que pour le compte d'administrateur par défaut sont disponibles.
- Lecture seule : Permet d'afficher uniquement les informations d'état et de configuration et de ne pas les modifier. Certaines pages, telles que la page Mise à niveau, sont bloquées pour les comptes en lecture seule.
- Auditeur : Autorise l'accès aux pages Event Log, Configuration Log, Network Log, Alarms et Overview uniquement .

- Aucune: Aucun accès n'est autorisé

Accès Web : Détermine si les membres de ce groupe sont autorisés à se connecter au système à l'aide de l'interface Web.

Accès à l'API : Détermine si les membres de ce groupe sont autorisés à accéder à l'état et à la configuration du système à l'aide de l'API.

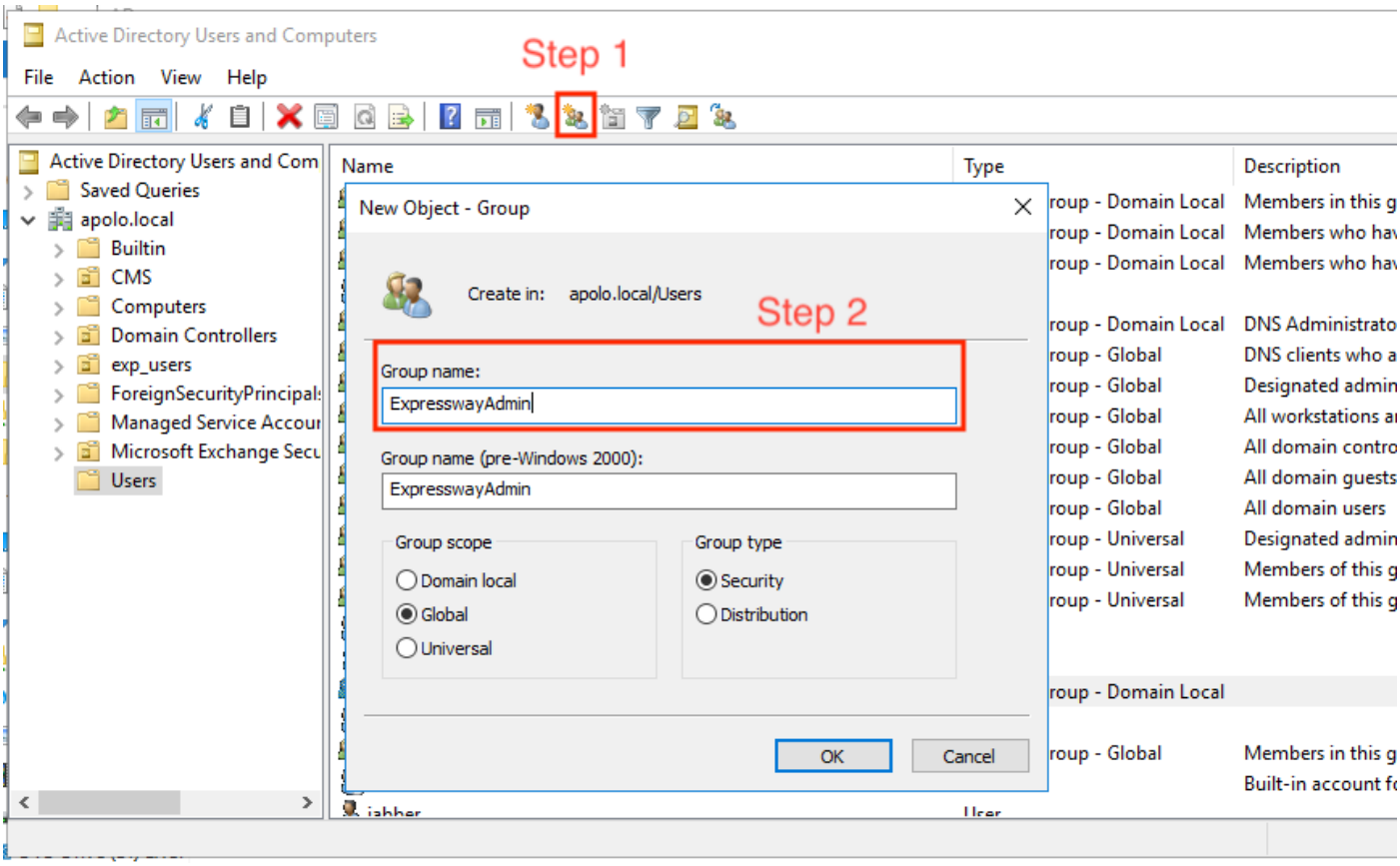
Accès CLI : Détermine si les membres de ce groupe sont autorisés à accéder au système via l'interface de ligne de commande.

Province: Indique si le groupe est activé ou désactivé.

Configuration du groupe d'administrateurs sur AD

1. Créez un nouveau groupe d'objets, sur le dossier dans lequel vous souhaitez stocker les utilisateurs.

2. Attribuez un nom au nom du groupe.

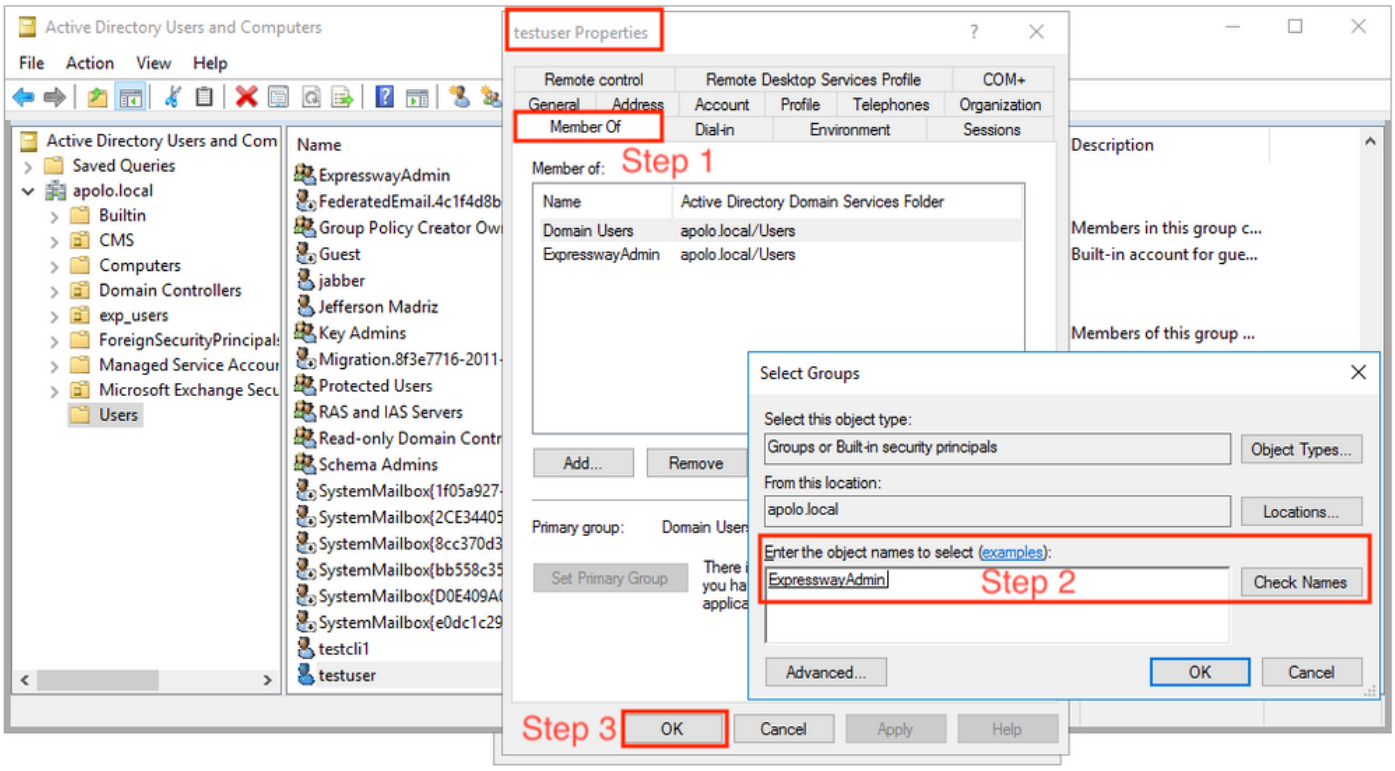


Attribuez le groupe configuré à l'utilisateur ou aux utilisateurs qui ont besoin d'accéder à Expressways via le Web, l'API ou la CLI. Dans ce cas, l'utilisateur est testuser.

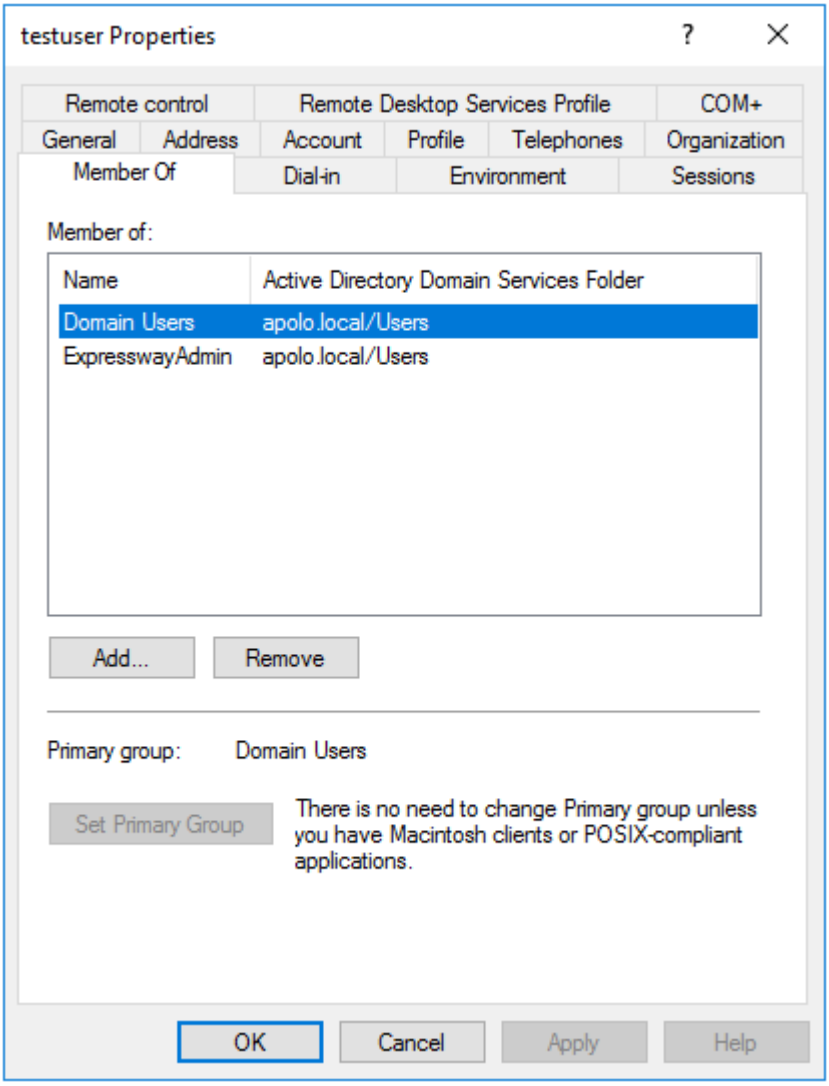
1. Ouvrez les propriétés de l'utilisateur, accédez à l'onglet Membre de,sélectionnez Ajouter

2. Recherchez le nom de groupe créé précédemment.

3. Sélectionnez ensuite OK.



À ce stade, l’utilisateur est membre de Domain Users et d’ExpresswayAdmin.

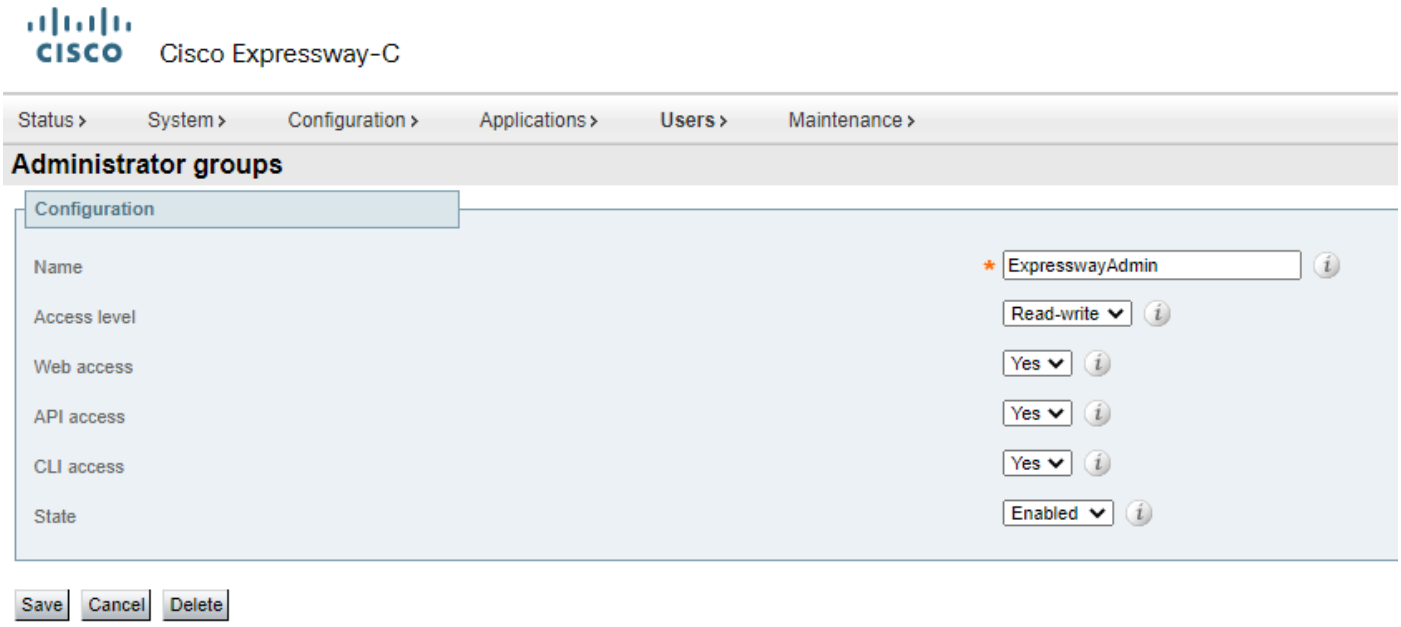


Configuration du groupe Administrateur sur Expressway

Une fois la configuration terminée, sur Expressway naviguez vers Users > Administrator groups, sélectionnez New

Nom : doit correspondre au nom du groupe configuré et associé à l'utilisateur LDAP qui doit accéder à l'Expressway. Dans cet exemple, le nom du groupe est ExpresswayAdmin, de sorte que le nouveau nom du groupe Administrateur est ExpresswayAdmin.

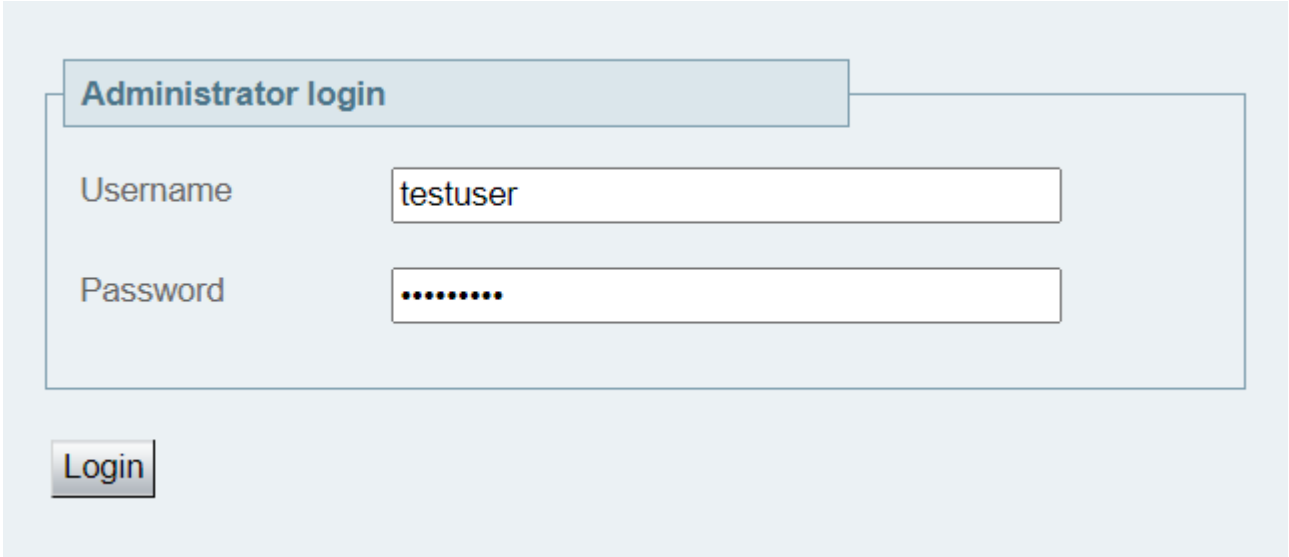
Ce groupe dispose de toutes les autorisations et de tous les accès disponibles.



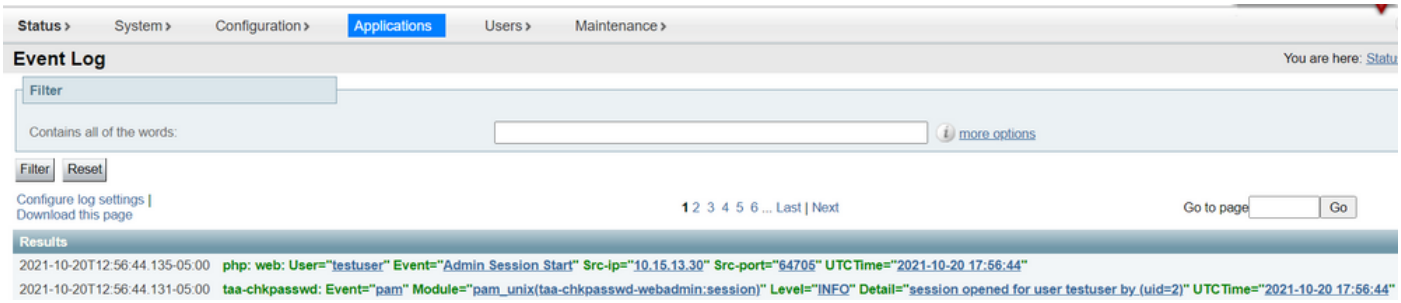
Sélectionnez Enregistrer.

Vérifier

Déconnectez-vous et essayez d'accéder via le Web avec l'utilisateur LDAP auquel le groupe d'administrateurs est associé. Dans cet exemple, l'utilisateur créé est testuser.



Vous pouvez le confirmer via Status > Event log :


Status › System › Configuration › Applications Users › Maintenance ›
Event Log
You are here: Statu
Filter
Contains all of the words:
more options
Filter Reset
Configure log settings |
Download this page
1 2 3 4 5 6 ... Last | Next
Go to page Go
Results
2021-10-20T12:56:44.135-05:00 php: web: User="testuser" Event="Admin Session Start" Src-ip="10.15.13.30" Src-port="64705" UTCTime="2021-10-20 17:56:44"
2021-10-20T12:56:44.131-05:00 taa-chkpasswd: Event="pam" Module="pam_unix(taa-chkpasswd-webadmin:session)" Level="INFO" Detail="session opened for user testuser by (uid=2)" UTCTime="2021-10-20 17:56:44"

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.