sudoers.ldap

Configuration LDAP sudo

En plus du fichier standard sudoers, sudo peut être configuré via LDAP. sudo n'a plus besoin de lire sudoers.

La configuration sudoers est contenue dans le conteneur LDAP ou=SUDOers. Sudo recherche d'abord l'entrée cn=defaults dans le conteneur et parcours les attributs sudoOption.

L'équivalent d'un sudoers dans LDAP est un sudoRole. Il consiste des attributs suivants :

sudoUser Un nom d'utilisateur valide, #<UID>, %<group>, %#<GID>, +<netgroup>, ou % :<groupe non unix> % :#<ID de groupe non unix>

sudoHost Nom d'hôte, IP, réseau ou +<netgroup d'hôte>. ALL match tous les hôte.

sudoCommand Nom d'une commande et ses arguments, optionnellement préfixé par ' !'

sudoOption Identique aux options globales, mais spécifiques au sudoRole

sudoRunAsUser user sous lequel la commande est lancée

sudoRunAsGroup Groupe sous lequel la commande est lancée

sudoNotBefore horodatage de début de validité du sudoRole

sudoNotAfter horodatage de fin de validité du sudoRole

sudoOrder Les entrées sudoRole LDAP n'ont pas d'ordre. sudoOrder est un entier utilisé pour trier les entrées qui matchent.

Anatomie de la recherche LADP sudoers

En recherchant un sudoer utilisant LDAP il y a seulement 2 ou 3 requêtes LDAP par invocation. La première requête sert à parcourir les options globales. Le second sert à matche le nom de l'utilisateur et les groupes auquel l'utilisateur appartient. Si aucun match n'est retourné pour l'utilisateur ou les groupes, une 3ème requête retourne toutes les entrées contenant les netgroups de l'utilisateur et les groupes non-unix et vérifie si l'utilisateur appartient à l'un d'entre-eux.

Si les entrées timées sont activées avec la directive SUDOERS_TIMED, les requêtes LDAP incluent un sous-filtre qui limite la recherche aux entrées qui satisfont les contraintes de temps.

Si la directive NETGROUP_BASE est présente, les requêtes sont effectuées pour déterminer la liste des netgroups auquel l'utilisateur appartient avant la requête sudoers. Cela permet d'inclure la liste des netgroups dans les requêtes sudoers de la même manière qu'avec les groupes unix. La 3ème requête n'est pas effectuées sauf si un plugin group est également effectuée. Les requêtes LDAP sont effectuées par sudo comme suit :

1. Match tous les enregistrement nisNetgroup avec un nisNetgroupTriple contenant l'utilisateur, l'hôte et le domaine NIS. La requête matche les entrées nisNetgroupTriple avec la forme courte ou longue du nom de domaine ou aucun nom d'hôte. Si le domaine NIS est définis, la requête matche seulement les entrées qui incluent de domaine ou pour lequel il n'y a pas de domaine présent. Si le domaine NIS n'est pas définis, un wildcard est utilisé pour matcher tous domaine pas prend en compte que le schéma NIS utilisé par les serveurs LDAP peuvent ne pas supporter les wildcard pour nisNetgroupTriple.
2. Les requêtes répétées sont effectuées pour trouver tout enregistrement nisNetgroup imbriqués avec une entrée memberNisNetgroup qui réfère à un enregistrement déjà matché.

Différence entre les sudoers LDAP et non-LDAP

Il y a quelques subtiles différences dans la comportement de sudoers utilisant LDAP. La plus grosse différence étant l'ordre des entrées et attributs retournés, qui sont contrôlés par sudoOrder.

Configurer ldap.conf

sudo lit le fichier /etc/ldap.conf. Seuls ces options sont supportés par sudo :

BIND_TIMELIMIT Spécifie le temps en secondes d'attente de connection à un serveur LDAP.
BINDDN Identité, sous la formate d'un DN, à utiliser pour effectuer les opérations LDAP
BINDPW Mot de passe de BINDDN
DEREF Spécifie comment déréférencer les alias
HOST Nom du serveur LDAP
KRB5_CCNAME Chemin du cache d'accréditifs Kerberos 5
LDAP_VERSION Version du protocole LDAP
NETGROUP_BASE DN de base pour les recherches des netgroups
NETGROUP_SEARCH_FILTER Filtre de recherche des netgroupes
PORT Port du serveur LDAP
ROOTBINDDN DN pour les opérations LDAP privilégiées
ROOTUSE_SASL Active l'authentification SASL pour les traitements privilégiés
SASL_AUTH_ID utilisateur SASL pour la connection LDAP
SASL_MECH Liste de mécanismes SASL à utiliser
SASL_SECPROPS Propriétés de sécurité SASL
SSL Active TLS pour les communications LDAP
SUDOERS_BASE DN de base pour les recherches SUDO
SUDOERS_DEBUG Niveaux de débuggage pour les requêtes sudo
SUDOERS_SEARCH_FILTER Filtre de recherche pour les requêtes sudo
SUDOERS_TIMED Spécifie si sudoNotBefore et sudoNotAfter sont évalués
TIMELIMIT Délai en secondes d'attente d'une réponse LDAP
TIMEOUT Délai en secondes d'attente d'une réponse depuis divers API LDAP
TLS_CACERTFILE Certificat de l'autorité
TLS_CACERTDIR Répertoire contenant les certificats d'autorité
TLS_CERT Certificat client
TLS_CHECKPEER Vérifie le certificat du serveur
TLS_KEY Clé privée du client
TLS_CIPHERS Liste d'algorithmes de chiffrement TLS à utiliser
TLS_KEYPW Mot de passe pour déchiffrer la clé privée. Peut être en base64 (base64 :dGVzdA==)
TLS_RANDFILE Source d'entropie
URI URI du serveur LDAP
USE_SASL Active l'authentification SASL
ROOTSASL_AUTH_ID Utilisateur SASL à utiliser avec ROOTUSE_SASL

Configurer nsswitch.conf

sudo consulte nsswitch.conf puor spécifie l'ordre de recherce sudoers. sudo recherche une ligne commençant par sudoers : et l'utilise pour déterminer l'ordre de recherche. Noter que sudo n'arrête pas sa recherche après le premier match et le dernier match a précédence. Les sources suivantes sont reconnus :

files Lit le fichier /etc/sudoers

ldap Lit sudoers depuis LDAP

De plus, l'entrée [NOTFOUND=return] court-circuite la recherche si l'utilisateur n'a pas été trouvé dans la source précédente

Intergration avec sssd

Dans les systèmes avec System Security Service Daemon il est possible d'utiliser SSSD pour cacher les règles sudoers LDAP. pour utiliser sssd, il faut utiliser sssd au lieu de ldap dans l'entrées sudoers dans /etc/nsswitch.conf. Noter que /etc/ldap.conf n'est pas utilisé par sssd.