rfc3829

Contrôles d'identité d'autorisation

Ce document définis le support pour le contrôle de demande d'identité d'autorisation et le contrôle de réponse d'identité d'autorisation pour demander et retourner l'autorisation établie dans une opération bind. C'est utile quand il y a des étapes de mappage ou d'autre indirection durant le bind, le client peut savoir quelle identité a été autorisée. L'authentification client avec certificats est la principale situation où cela s'applique.

Le support pour le contrôle de demande d'identité d'autorisation et le contrôle de réponse d'identité d'autorisation est indiqué par la présence de l'OID **2.16.840.1.113730.3.4.16** et **2.16.840.1.113730.3.4.15**, respectivement, dans supportedControl du rootDSE.

Request

Ce contrôle peut être inclus dans une demande bind dans le champ contrôles du LDAPMessage. Dans une opération bind a plusieurs étapes, le client doit fournir ce contrôle à chaque demande bind. **controlType** est **2.16.840.1.113730.3.4.16** et **controlValue** est absent.

Response

Ce contrôle peut être inclus dans la réponse bind finale où la première demande bind a inclus de contrôle de demande. **controlType** est **2.16.840.1.113730.3.4.15**. Si le bind a réussi et résulte en une identité (non anonyme), **controlValue** contient l'identité d'autorisation (authzId). Si le bind résulte en une association anonyme, **controlValue** est une chaîne vide. Si le bind résulte en plusieurs authzId, l'autzId primaire est retourné dans **controlValue**. Le contrôle est inclus uniquement dans une réponse bind dont le resultCode est success.

Si le serveur nécessite des protections de confidentialité avant d'utiliser ce contrôle, le serveur reporte une erreur et retourne le code de retour confidentialityRequired.

Si le client n'a pas les droits suffisants pour demander les informations d'autorisation, le serveur retourne le code insufficientAccessRights.

Les identités présentés par un client comme partie du processus d'authentification peuvent être mappsé par le serveur à une ou plusieurs identités d'autorisation. Le contrôle de réponse bind peut être utilisé pour récupérer l'authzId primaire.

Par exemple, durant l'authentification du client avec des certificats, un client peut posséder plus d'un certificat et ne peut pas être en mesure de déterminer lequel a été sélectionné pour l'authentification auprès du serveur. Le DN du champ sujet dans le certificat sélectionné peut ne pas correspondre exactement au DN dans l'annuaire, mais est passé par un processus de mappage dans le serveur. Une fois l'authentification par certificat complétée, le client peut fournir un bind SASL, spécifiant le mécanisme externe et incluant le contrôle de demande d'identité d'autorisation. La réponse peut inclure le contrôle de réponse d'identité d'autorisation indiquant le DN dans le DIT qui a été mappé.

Approche alternative

L'opération étendue Who am I ? fournis un mécanisme pour demander l'identité d'autorisation associée avec une connexion. Utiliser une opération étendue permet à un client d'apprendre d'identité d'autorisation après que le bind ait établis les protections d'intégrité et de confidentialité. Pour les environnements multithreadé ou à fort traffic, le contrôle étendu est préférable.