
rfc5803

Schéma LDAP pour stocker les secrets SCRAM

Ce mémo décrit comment l'attribut LDAP **authPassword** peut être utilisé pour stocker des secrets utilisés par le mécanisme SCRAM dans SASL. La partie "**scheme**" de authPassword est le nom du mécanisme SCRAM. La partie "**authInfo**" est le compteur d'itération suivi par un ":" et un salt encodé base64. La partie "**authValue**" est la clé encodée en base64, suivi par ":" et la clé serveur encodé en base 64. La syntaxe de l'attribut peut être :

```
scram-mech = "SCRAM-SHA-1" / scram-mech-ext
scram-authInfo = iter-count ":" salt
scram-authValue = stored-key ":" server-key
iter-count = %x31-39 *DIGIT
salt = <base64-encoded value>
stored-key = <base64-encoded value>
server-key = <base64-encoded value>
scram-mech-ext = "SCRAM-" 1*9mech-char
mech-char = <Defined in RFC 4422>
```

Noter que authPassword est multivalué