LDAP SCHEMA EXTENSIONS

LDAP Schema Extensions

Active Directory OpenLDAP Novell Schema DS389 LDS

1. Overview

This HowTo presents the schema extensions needed by WebADM with most of LDAP directories. Only Active Directory can work with WebADM without schema extensions. WebADM stores most of its related metadata into the LDAP directory on users accounts and into a specific container/OU.

2. Content of the Schema Extension

The schema extension is very minimal. It is composed of three object classes (*webadmAccount*, *webadmGroup* and *webadmConfig*) and three attributes (*webadmSettings*, *webadmData*, *webadmType* and *webadmVoice*).

Each attribute contains a registered object identifier. *34617* corresponds to the registered number for RCDevs at IANA.

Schema files for most LDAP directories are provided with WebADM installation. They are located in `/opt/webadm/lib/schema/` folder. Found below, the most used schema files :

2.1 Microsoft Active Directory

File ldap_schema.ads

```
dn: CN=webadmSettings
changetype: add
attributeID: 1.3.6.1.4.1.34617.2.3.1
attributeSyntax: 2.5.5.12
oMSyntax: 64
cn: webadmSettings
isSingleValued: TRUE
objectClass: attributeSchema
searchFlags: 0

dn: CN=webadmData
changetype: add
attributeID: 1.3.6.1.4.1.34617.2.3.2
attributeSyntax: 2.5.5.12
oMSyntax: 64
cn: webadmData
isSingleValued: TRUE
objectClass: attributeSchema
searchFlags: 0

dn: CN=webadmType
changetype: add
attributeID: 1.3.6.1.4.1.34617.2.3.3
```

attributeID: 1.3.6.1.4.1.34617.2.3.3
attributeSyntax: 2.5.5.12
oMSyntax: 64
cn: webadmType
isSingleValued: TRUE
objectClass: attributeSchema
searchFlags: 0

dn: CN=webadmVoice
changetype: add
attributeID: 1.3.6.1.4.1.34617.2.3.4
attributeSyntax: 2.5.5.10
oMSyntax: 4
cn: webadmVoice
isSingleValued: TRUE
objectClass: attributeSchema
searchFlags: 0

dn: -
changetype: modify
add: schemaUpdateNow
schemaUpdateNow: 1

dn: CN=webadmAccount
changetype: add
cn: webadmAccount
governsID: 1.3.6.1.4.1.34617.2.4.1
mustContain: cn
mustContain: sAMAccountName
mayContain: webadmSettings
mayContain: webadmData
mayContain: webadmVoice
mayContain: preferredLanguage
mayContain: mobile
mayContain: mail
mayContain: description
objectClass: classSchema
objectClassCategory: 3
subClassOf: top
possSuperiors: container
possSuperiors: domain
possSuperiors: builtinDomain
possSuperiors: domainDNS
possSuperiors: organization
possSuperiors: organizationalUnit

dn: CN=webadmConfig
changetype: add
cn: webadmConfig
governsID: 1.3.6.1.4.1.34617.2.4.2

```
mustContain: cn
mustContain: webadmType
mayContain: webadmSettings
mayContain: description
objectClass: classSchema
objectClassCategory: 1
subClassOf: top
possSuperiors: container
possSuperiors: domain
possSuperiors: builtinDomain
possSuperiors: domainDNS
possSuperiors: organization
possSuperiors: organizationalUnit

dn: CN=webadmGroup
changetype: add
cn: webadmGroup
governsID: 1.3.6.1.4.1.34617.2.4.3
mustContain: cn
mayContain: webadmSettings
mayContain: description
objectClass: classSchema
objectClassCategory: 3
subClassOf: top
possSuperiors: container
possSuperiors: domain
possSuperiors: builtinDomain
possSuperiors: domainDNS
possSuperiors: organization
possSuperiors: organizationalUnit

dn: -
changetype: modify
add: schemaUpdateNow
schemaUpdateNow: 1

dn: CN=User
changetype: modify
add: auxiliaryClass
auxiliaryClass: webadmAccount

dn: CN=Group
changetype: modify
add: auxiliaryClass
auxiliaryClass: webadmGroup

dn: -
changetype: modify
add: schemaUpdateNow
schemaUpdateNow: 1
```

schemaUpdateNow: 1

2.2 Microsoft LDS

File ldap_schema.lds

```
dn: CN=webadmSettings
changetype: add
attributeID: 1.3.6.1.4.1.34617.2.3.1
attributeSyntax: 2.5.5.12
oMSyntax: 64
cn: webadmSettings
isSingleValued: TRUE
objectClass: attributeSchema
searchFlags: 0

dn: CN=webadmData
changetype: add
attributeID: 1.3.6.1.4.1.34617.2.3.2
attributeSyntax: 2.5.5.12
oMSyntax: 64
cn: webadmData
isSingleValued: TRUE
objectClass: attributeSchema
searchFlags: 0

dn: CN=webadmType
changetype: add
attributeID: 1.3.6.1.4.1.34617.2.3.3
attributeSyntax: 2.5.5.12
oMSyntax: 64
cn: webadmType
isSingleValued: TRUE
objectClass: attributeSchema
searchFlags: 0

dn: CN=webadmVoice
changetype: add
attributeID: 1.3.6.1.4.1.34617.2.3.4
attributeSyntax: 2.5.5.12
oMSyntax: 64
cn: webadmVoice
isSingleValued: TRUE
objectClass: attributeSchema
searchFlags: 0

dn: -
changetype: modify
add: schemaUpdateNow
```

```
add: schemaUpdateNow
schemaUpdateNow: 1

dn: CN=webadmAccount
changetype: add
cn: webadmAccount
governsID: 1.3.6.1.4.1.34617.2.4.1
mustContain: cn
mustContain: sAMAccountName
mayContain: webadmSettings
mayContain: webadmData
mayContain: webadmVoice
mayContain: preferredLanguage
mayContain: mobile
mayContain: mail
mayContain: description
objectClass: classSchema
objectClassCategory: 3
subClassOf: top
possSuperiors: container
possSuperiors: domain
possSuperiors: builtinDomain
possSuperiors: domainDNS
possSuperiors: organization
possSuperiors: organizationalUnit

dn: CN=webadmConfig
changetype: add
cn: webadmConfig
governsID: 1.3.6.1.4.1.34617.2.4.2
mustContain: cn
mustContain: webadmType
mayContain: webadmSettings
mayContain: description
objectClass: classSchema
objectClassCategory: 1
subClassOf: top
possSuperiors: container
possSuperiors: domain
possSuperiors: builtinDomain
possSuperiors: domainDNS
possSuperiors: organization
possSuperiors: organizationalUnit

dn: CN=webadmGroup
changetype: add
cn: webadmGroup
governsID: 1.3.6.1.4.1.34617.2.4.3
mustContain: cn
mayContain: webadmSettings
```

```
mayContain: description
objectClass: classSchema
objectClassCategory: 3
subClassOf: top
possSuperiors: container
possSuperiors: domain
possSuperiors: builtinDomain
possSuperiors: domainDNS
possSuperiors: organization
possSuperiors: organizationalUnit

dn: -
changetype: modify
add: schemaUpdateNow
schemaUpdateNow: 1

dn: CN=User
changetype: modify
add: auxiliaryClass
auxiliaryClass: webadmAccount

dn: CN=Group
changetype: modify
add: auxiliaryClass
auxiliaryClass: webadmGroup

dn: -
changetype: modify
add: schemaUpdateNow
schemaUpdateNow: 1
```

2.3 RCDevs Directory

Schema is already extended when deploying RCDevs Directory.

```
attributetype ( 1.3.6.1.4.1.34617.2.3.1 NAME 'webadmSettings' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE )
attributetype ( 1.3.6.1.4.1.34617.2.3.2 NAME 'webadmData' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE )
attributetype ( 1.3.6.1.4.1.34617.2.3.3 NAME 'webadmType' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE )
attributetype ( 1.3.6.1.4.1.34617.2.3.4 NAME 'webadmVoice' SYNTAX 1.3.6.1.4.1.1466.115.121.1.40
SINGLE-VALUE )

objectclass ( 1.3.6.1.4.1.34617.2.4.1 NAME 'webadmAccount' SUP top AUXILIARY MUST (cn $ uid) MAY
(webadmSettings $ webadmData $ webadmVoice $ preferredLanguage $ mobile $ mail $ description) )
objectclass ( 1.3.6.1.4.1.34617.2.4.2 NAME 'webadmConfig' SUP top MUST (cn $ webadmType) MAY
(webadmSettings $ description) )
objectclass ( 1.3.6.1.4.1.34617.2.4.3 NAME 'webadmGroup' SUP top AUXILIARY MUST (cn) MAY
(webadmSettings $ description) )
```

2.4 OpenLDAP

File ldap_schema.ols. olc schema version.

```
dn: cn=webadm,cn=schema,cn=config
changetype: add
cn: webadm
objectClass: olcSchemaConfig
olcAttributeTypes: ( 1.3.6.1.4.1.34617.2.3.1 NAME 'webadmSettings' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
olcAttributeTypes: ( 1.3.6.1.4.1.34617.2.3.2 NAME 'webadmData' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE )
olcAttributeTypes: ( 1.3.6.1.4.1.34617.2.3.3 NAME 'webadmType' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE )
olcAttributeTypes: ( 1.3.6.1.4.1.34617.2.3.4 NAME 'webadmVoice' SYNTAX 1.3.6.1.4.1.1466.115.121.1.40
SINGLE-VALUE )
olcObjectClasses: ( 1.3.6.1.4.1.34617.2.4.1 NAME 'webadmAccount' SUP top AUXILIARY MUST (cn $ uid)
MAY (webadmSettings $ webadmData $ webadmVoice $ preferredLanguage $ mobile $ mail $
description) )
olcObjectClasses: ( 1.3.6.1.4.1.34617.2.4.2 NAME 'webadmConfig' SUP top MUST (cn $ webadmType) MAY
(webadmSettings $ description) )
olcObjectClasses: ( 1.3.6.1.4.1.34617.2.4.3 NAME 'webadmGroup' SUP top AUXILIARY MUST (cn) MAY
(webadmSettings $ description) )
```

2.5 389 Directory Server / DS389

File ldap_schema.389

```
dn: cn=schema
objectClass: top
objectClass: ldapSubentry
objectClass: subschema
cn: schema
attributeTypes: ( 1.3.6.1.4.1.34617.2.3.1 NAME 'webadmSettings' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE )
attributeTypes: ( 1.3.6.1.4.1.34617.2.3.2 NAME 'webadmData' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE )
attributeTypes: ( 1.3.6.1.4.1.34617.2.3.3 NAME 'webadmType' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE )
attributeTypes: ( 1.3.6.1.4.1.34617.2.3.4 NAME 'webadmVoice' SYNTAX 1.3.6.1.4.1.1466.115.121.1.40
SINGLE-VALUE )
objectClasses: ( 1.3.6.1.4.1.34617.2.4.1 NAME 'webadmAccount' SUP top AUXILIARY MUST (cn $ uid) MAY
(webadmSettings $ webadmData $ preferredLanguage $ mobile $ mail $ description) )
objectClasses: ( 1.3.6.1.4.1.34617.2.4.2 NAME 'webadmConfig' SUP top MUST (cn $ webadmType) MAY
(webadmSettings $ description) )
objectClasses: ( 1.3.6.1.4.1.34617.2.4.3 NAME 'webadmGroup' SUP top AUXILIARY MUST (cn) MAY
(webadmSettings $ description) )
```

2.6 Novell Directory Service

File ldap_schema.nds

```
dn: cn=schema
changetype: modify
add: attributetypes
attributetypes: ( 1.3.6.1.4.1.34617.2.3.1 NAME 'webadmSettings' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE )

dn: cn=schema
changetype: modify
add: attributetypes
attributetypes: ( 1.3.6.1.4.1.34617.2.3.2 NAME 'webadmData' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE )

dn: cn=schema
changetype: modify
add: attributetypes
attributetypes: ( 1.3.6.1.4.1.34617.2.3.3 NAME 'webadmType' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE )

dn: cn=schema
changetype: modify
add: attributetypes
attributetypes: ( 1.3.6.1.4.1.34617.2.3.4 NAME 'webadmVoice' SYNTAX 1.3.6.1.4.1.1466.115.121.1.40 )

dn: cn=schema
changetype: modify
add: objectclasses
objectclasses: ( 1.3.6.1.4.1.34617.2.4.1 NAME 'webadmAccount' SUP top AUXILIARY MUST (cn $ uid) MAY
(webadmSettings $ webadmData $ webadmVoice $ preferredLanguage $ mobile $ mail $ description) )

dn: cn=schema
changetype: modify
add: objectclasses
objectclasses: ( 1.3.6.1.4.1.34617.2.4.2 NAME 'webadmConfig' SUP top MUST (cn $ webadmType) MAY
(webadmSettings $ description) )

dn: cn=schema
changetype: modify
add: objectclasses
objectclasses: ( 1.3.6.1.4.1.34617.2.4.3 NAME 'webadmGroup' SUP top AUXILIARY MUST (cn) MAY
(webadmSettings $ description) )
```

2.7 PingDirectory

File ldap_schema.ping

```
dn: cn=schema
objectClass: top
objectClass: ldapSubentry
objectClass: subschema
cn: schema
attributeTypes: ( 1.3.6.1.4.1.34617.2.3.1 NAME 'webadmSettings' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE )
attributeTypes: ( 1.3.6.1.4.1.34617.2.3.2 NAME 'webadmData' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE )
attributeTypes: ( 1.3.6.1.4.1.34617.2.3.3 NAME 'webadmType' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE )
attributeTypes: ( 1.3.6.1.4.1.34617.2.3.4 NAME 'webadmVoice' SYNTAX 1.3.6.1.4.1.1466.115.121.1.40
SINGLE-VALUE )
objectClasses: ( 1.3.6.1.4.1.34617.2.4.1 NAME 'webadmAccount' SUP top AUXILIARY MUST (cn $ uid) MAY
(webadmSettings $ webadmData $ webadmVoice $ preferredLanguage $ mobile $ mail $ description) )
objectClasses: ( 1.3.6.1.4.1.34617.2.4.2 NAME 'webadmConfig' SUP top STRUCTURAL MUST (cn $
webadmType) MAY (webadmSettings $ description) )
objectClasses: ( 1.3.6.1.4.1.34617.2.4.3 NAME 'webadmGroup' SUP top AUXILIARY MUST (cn) MAY
(webadmSettings $ description) )
```

3. Automatic Schema Extension

This option is preferred and is very easy. It works with most of LDAP servers.

3.1 Active Directory Prerequisite

The first domain controller defined in `/opt/webadm/conf/servers.xml` should be a schema master.

We check which domain controller is the schema master with `Get-ADForest` in PowerShell:

```
PS C:\Users\administrator> (Get-ADForest).SchemaMaster
vagrant-2012-r2.test.local
```

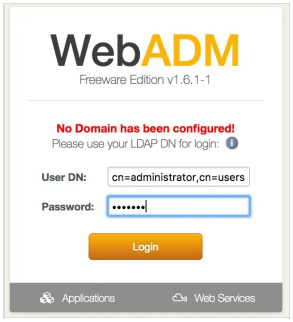
The WebADM admin should be a schema admin, we can add it temporarily in the *schema admins* group in the AD.

We check that we are a member of the schema admins group with `Get-ADGroupMember`:

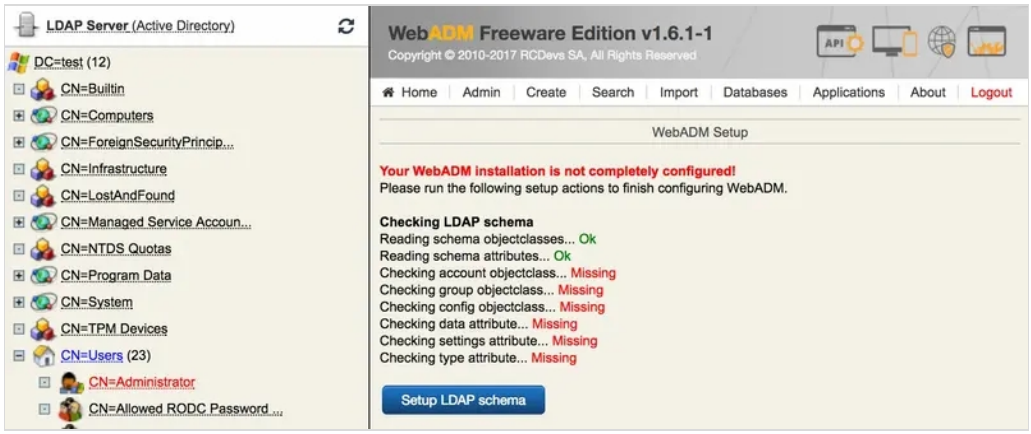
```
PS C:\Users\administrator> Get-ADGroupMember "schema admins"


distinguishedName : CN=Administrator,CN=Users,DC=test,DC=local
name              : Administrator
objectClass       : user
objectGUID        : 51be422c-e4cb-4463-a60f-fd9c4c0b63a3
SamAccountName    : Administrator
SID               : S-1-5-21-3541430928-2051711210-1391384369-500
```

3.2 Schema Extension

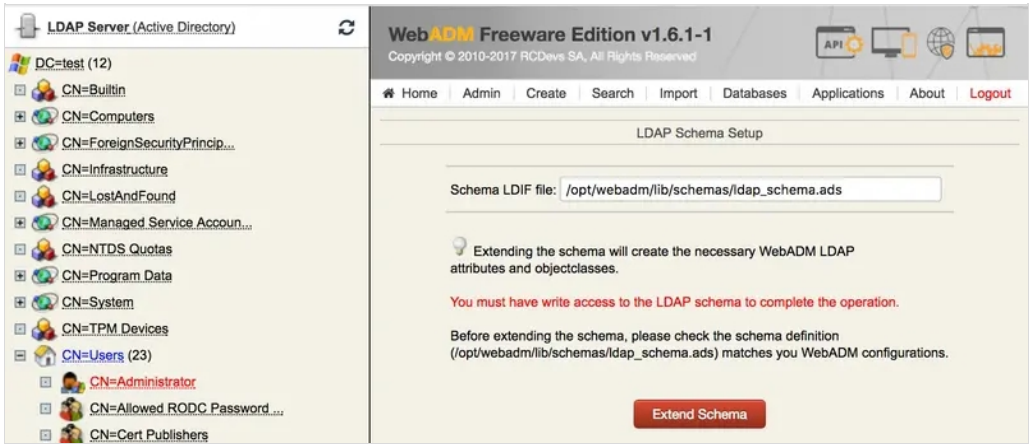
We log in to WebADM:



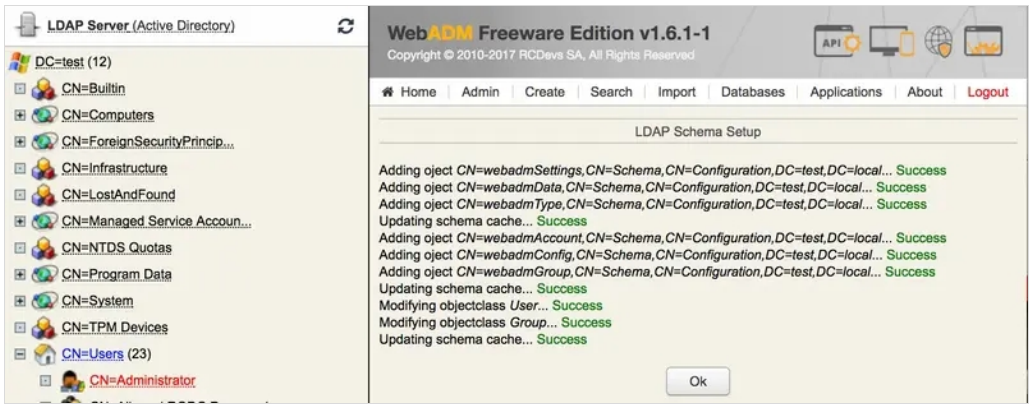
We click on `Setup LDAP schema`:



We click on `Extend Schema`:



That's it, the schema is extended:



4. Manual Schema Extension with Active Directory

This method is not recommended but, in some rare cases, it is not possible to extend the schema of Active Directory through WebADM for internal security restrictions.

Some modifications in the schema cannot be undone, so you need to understand well how the schema works. Errors are not permitted in this procedure.

For the schema extension, we need to connect to the schema master domain controller with a schema administrator.

We check which domain controller is the schema master with `Get-ADForest` in PowerShell:

```
PS C:\Users\administrator> (Get-ADForest).SchemaMaster
vagrant-2012-r2.test.local
```

We check that we are a member of the *schema admins* group with `Get-ADGroupMember`:

```
PS C:\Users\administrator> Get-ADGroupMember "schema admins"


distinguishedName : CN=Administrator,CN=Users,DC=test,DC=local
name              : Administrator
objectClass       : user
objectGUID        : 51be422c-e4cb-4463-a60f-fd9c4c0b63a3
SamAccountName    : Administrator
SID               : S-1-5-21-3541430928-2051711210-1391384369-500
```

We search for the schema naming context:

```
PS C:\Users\administrator> (Get-ADRootDSE).schemaNamingContext
CN=Schema,CN=Configuration,DC=test,DC=local
```

We create the `schema.ldif` file with the following content. `CN=Schema,CN=Configuration,DC=test,DC=local` must be replaced everywhere with the right schema naming context:

```
dn: CN=webadmSettings,CN=Schema,CN=Configuration,DC=test,DC=local
changetype: add
attributeID: 1.3.6.1.4.1.34617.2.3.1
attributeSyntax: 2.5.5.12
oMSyntax: 64
cn: webadmSettings
isSingleValued: TRUE
objectClass: attributeSchema
searchFlags: 0

dn: CN=webadmData,CN=Schema,CN=Configuration,DC=test,DC=local
changetype: add
attributeID: 1.3.6.1.4.1.34617.2.3.2
attributeSyntax: 2.5.5.12
oMSyntax: 64
cn: webadmData
isSingleValued: TRUE
objectClass: attributeSchema
searchFlags: 0

dn: CN=webadmType,CN=Schema,CN=Configuration,DC=test,DC=local
changetype: add
attributeID: 1.3.6.1.4.1.34617.2.3.3
attributeSyntax: 2.5.5.12
oMSyntax: 64
cn: webadmType
isSingleValued: TRUE
```

```
objectClass: attributeSchema
searchFlags: 0

dn: CN=webadmVoice,CN=Schema,CN=Configuration,DC=test,DC=local
changetype: add
attributeID: 1.3.6.1.4.1.34617.2.3.4
attributeSyntax: 2.5.5.10
oMSyntax: 4
cn: webadmVoice
isSingleValued: TRUE
objectClass: attributeSchema
searchFlags: 0

dn: -
changetype: modify
add: schemaUpdateNow
schemaUpdateNow: 1

dn: CN=webadmAccount,CN=Schema,CN=Configuration,DC=test,DC=local
changetype: add
cn: webadmAccount
governsID: 1.3.6.1.4.1.34617.2.4.1
mustContain: cn
mustContain: sAMAccountName
mayContain: webadmSettings
mayContain: webadmData
mayContain: webadmVoice
mayContain: preferredLanguage
mayContain: mobile
mayContain: mail
mayContain: description
objectClass: classSchema
objectClassCategory: 3
subClassOf: top
possSuperiors: container
possSuperiors: domain
possSuperiors: builtinDomain
possSuperiors: domainDNS
possSuperiors: organization
possSuperiors: organizationalUnit

dn: CN=webadmConfig,CN=Schema,CN=Configuration,DC=test,DC=local
changetype: add
cn: webadmConfig
governsID: 1.3.6.1.4.1.34617.2.4.2
mustContain: cn
mustContain: webadmType
mayContain: webadmSettings
mayContain: description
objectClass: classSchema
```

```
objectClassCategory: 1
subClassOf: top
possSuperiors: container
possSuperiors: domain
possSuperiors: builtinDomain
possSuperiors: domainDNS
possSuperiors: organization
possSuperiors: organizationalUnit

dn: CN=webadmGroup,CN=Schema,CN=Configuration,DC=test,DC=local
changetype: add
cn: webadmGroup
governsID: 1.3.6.1.4.1.34617.2.4.3
mustContain: cn
mayContain: webadmSettings
mayContain: description
objectClass: classSchema
objectClassCategory: 3
subClassOf: top
possSuperiors: container
possSuperiors: domain
possSuperiors: builtinDomain
possSuperiors: domainDNS
possSuperiors: organization
possSuperiors: organizationalUnit

dn: -
changetype: modify
add: schemaUpdateNow
schemaUpdateNow: 1

dn: CN=User,CN=Schema,CN=Configuration,DC=test,DC=local
changetype: modify
add: auxiliaryClass
auxiliaryClass: webadmAccount

dn: CN=Group,CN=Schema,CN=Configuration,DC=test,DC=local
changetype: modify
add: auxiliaryClass
auxiliaryClass: webadmGroup

dn: -
changetype: modify
add: schemaUpdateNow
schemaUpdateNow: 1
```

Now we extend the schema. The `schema.ldif` file must be correct, we cannot undo this operation:

```
PS C:\Users\administrator> ldifde -i -f schema.ldif
Connecting to "vagrant-2012-r2.test.local"
Logging in as current user using SSPI
Importing directory from file "schema.ldif"
Loading entries.............
11 entries modified successfully.
```

That's it, the schema is extended.

5. Manual schema extensions for other directories

For most of other directories, the schema extension consist on add one of the schema file previously described to your directory in a specific location in order to be loaded by the directory service. For some other like LDS, you need to perform an LDIF import. Please, refer to your LDAP Directory documentation for how to perform the schema extensions.