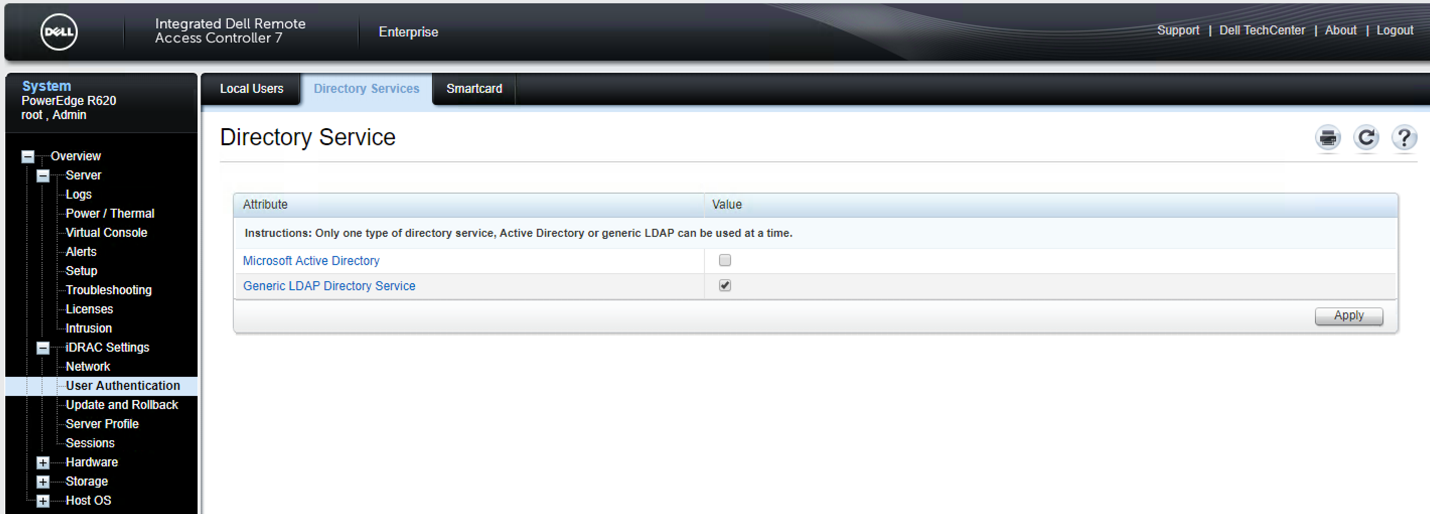
**iDrac Configuration Guide**

1. Configure Directory Services for iDrac.

In the case of PUA. iDrac User Interface Must be point “back” to an LDAP VIP on the PUA system for Authentication.

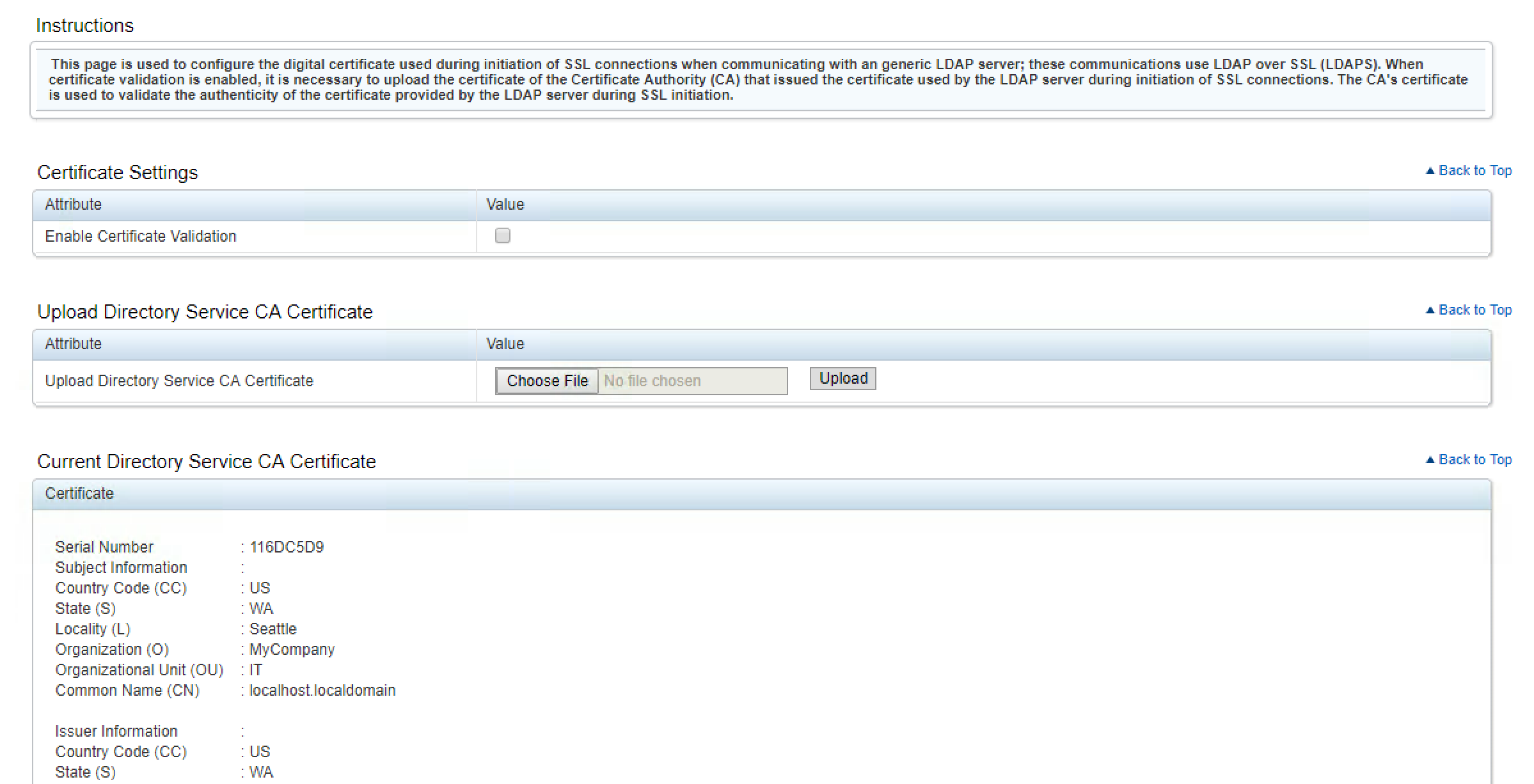
Select System/User Authentication/Directory Services

Click on “Generic LDAP Directory Service”



Select the “Configure Generic LDAP” button..

Upload the Directory Service CA Certificate – in this case the generic F5 self-signed CA Certificate was selected as this was CA Certificate that was associated with the “636” or LDAPS VIP.



Step2 of 3

These are the settings that worked in our case.. depending up on the ultimate Directory these setting may be different. Our “ultimate” back end directory was a Windows Directory.

Enable Generic LDAP “checked”

Use Distinguished Name

LDAP Server Address:- IP of LDAPS VIP for PUA

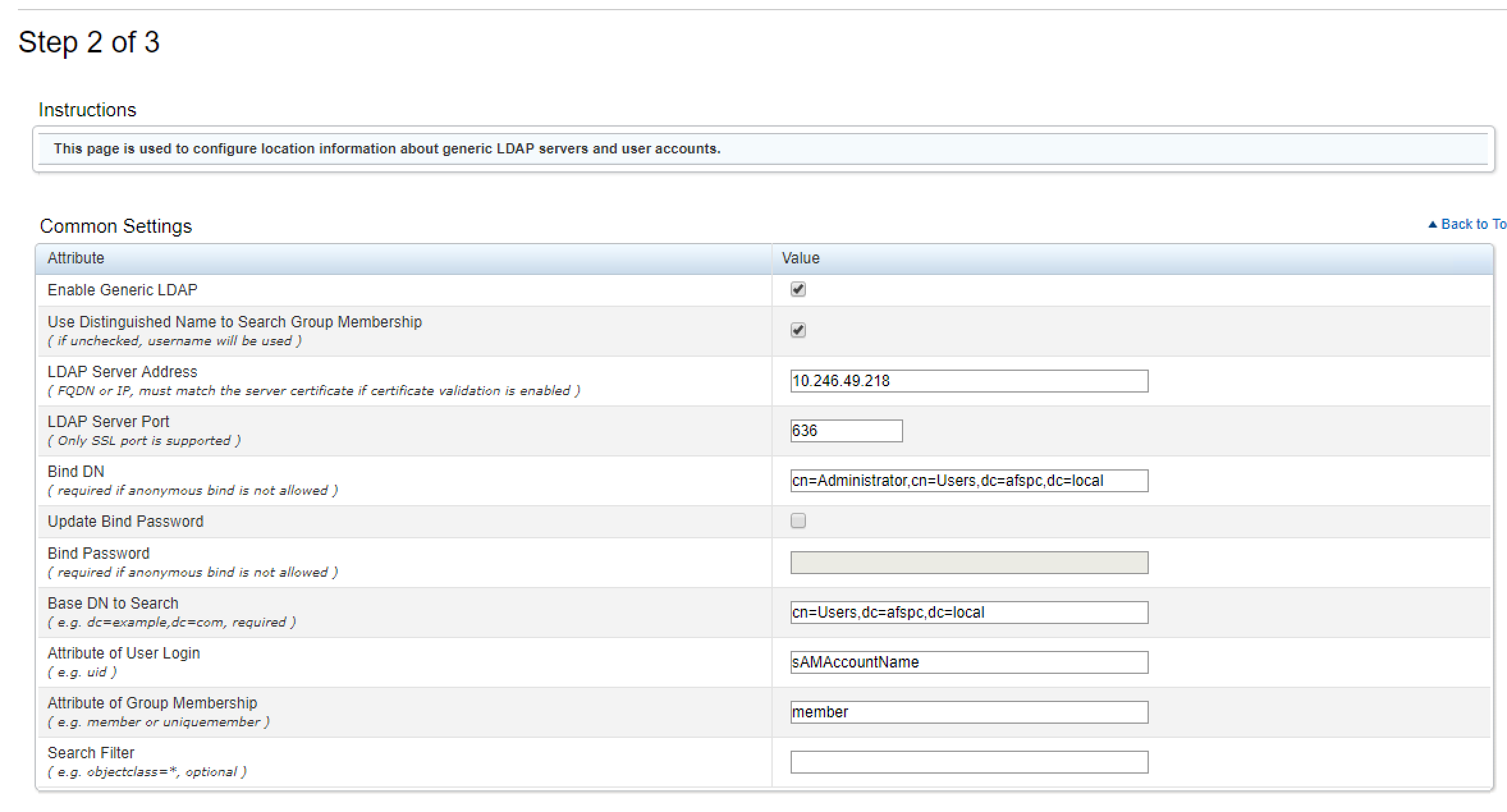
LDAP Server PORT:- 636.. could be configured to be a different port if the VIP was listening on something other than default.

Bind DN: Whatever you BIND DN would be for your directory… in our case it was

cn=Administrator,cn=Users,dc=afspc,dc=local

Attribute of User Login :- sAMAccountName

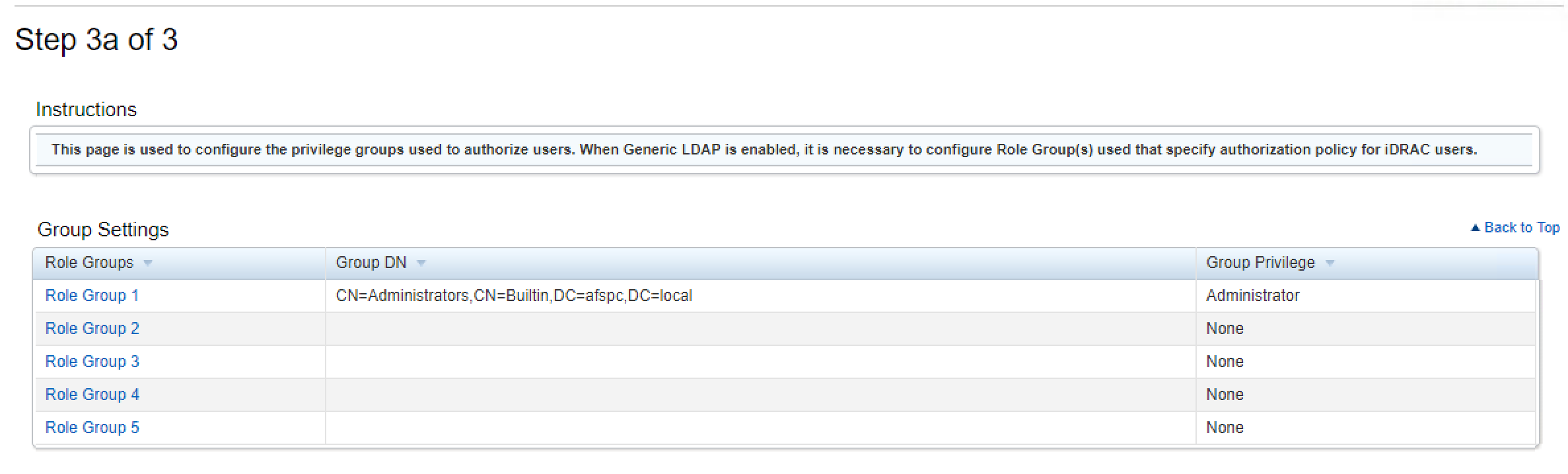
Attribute of Group Membership:- member



Create a Role Group.

Your configuration may be different but each role group will have a role within the iDrac which will have certain group privileges associated with it.

In our case we create a single “Administrator” role group that was associated with a specific group in the Windows Active Directory Server

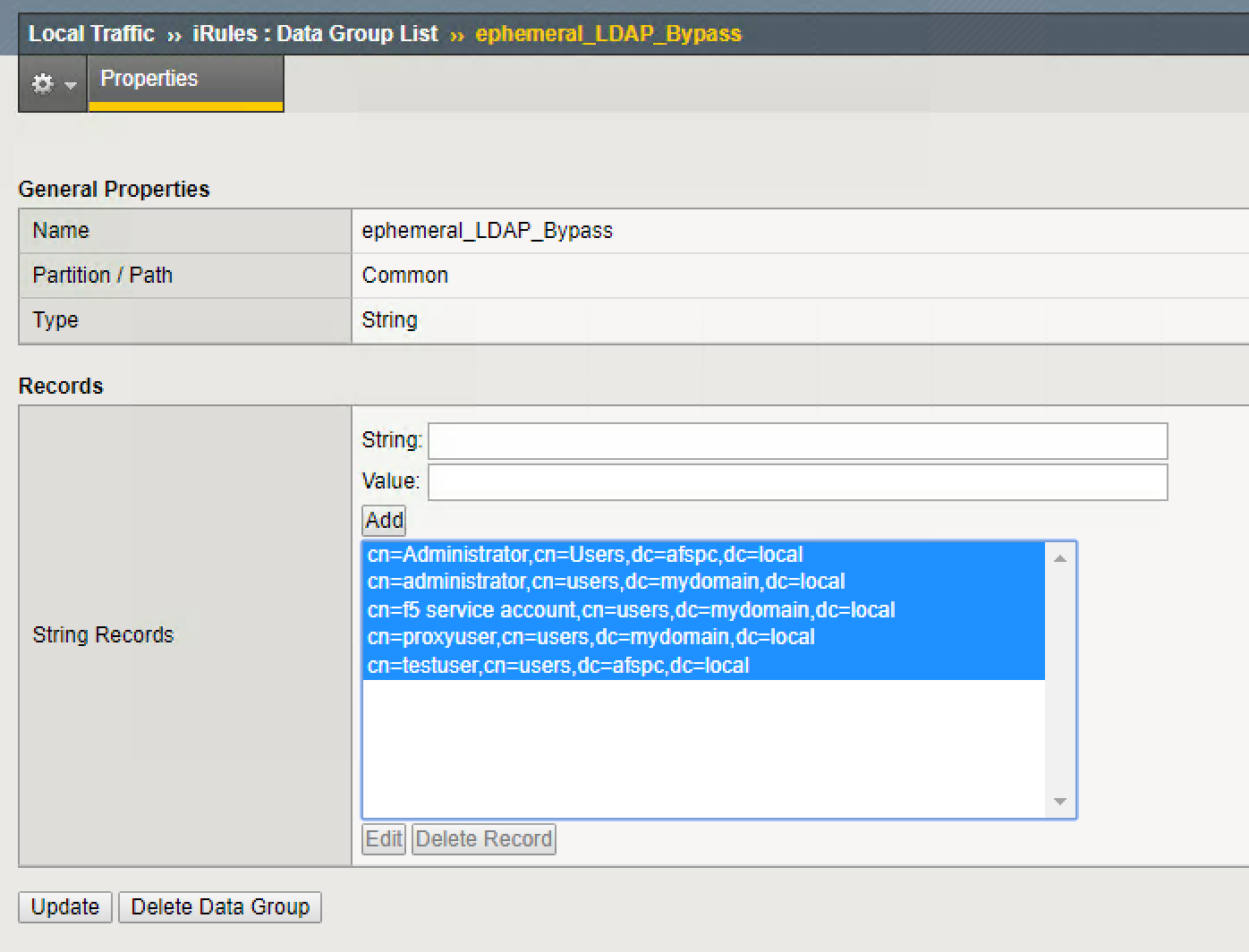


Click Finish..

Select the “Test Settings Button”

Then enter a username and password of an active directory user. If the test passes then you can continue with the F5 Configuration.

**Note: The DN that username translates to must be in the ephemeral\_LDAP\_Bypass data-group. Otherwise the PUA system will intercept the authentication and generate an ephemeral credential and the authentication will fail. This data group is under iRules/DataGroup List**

****

​

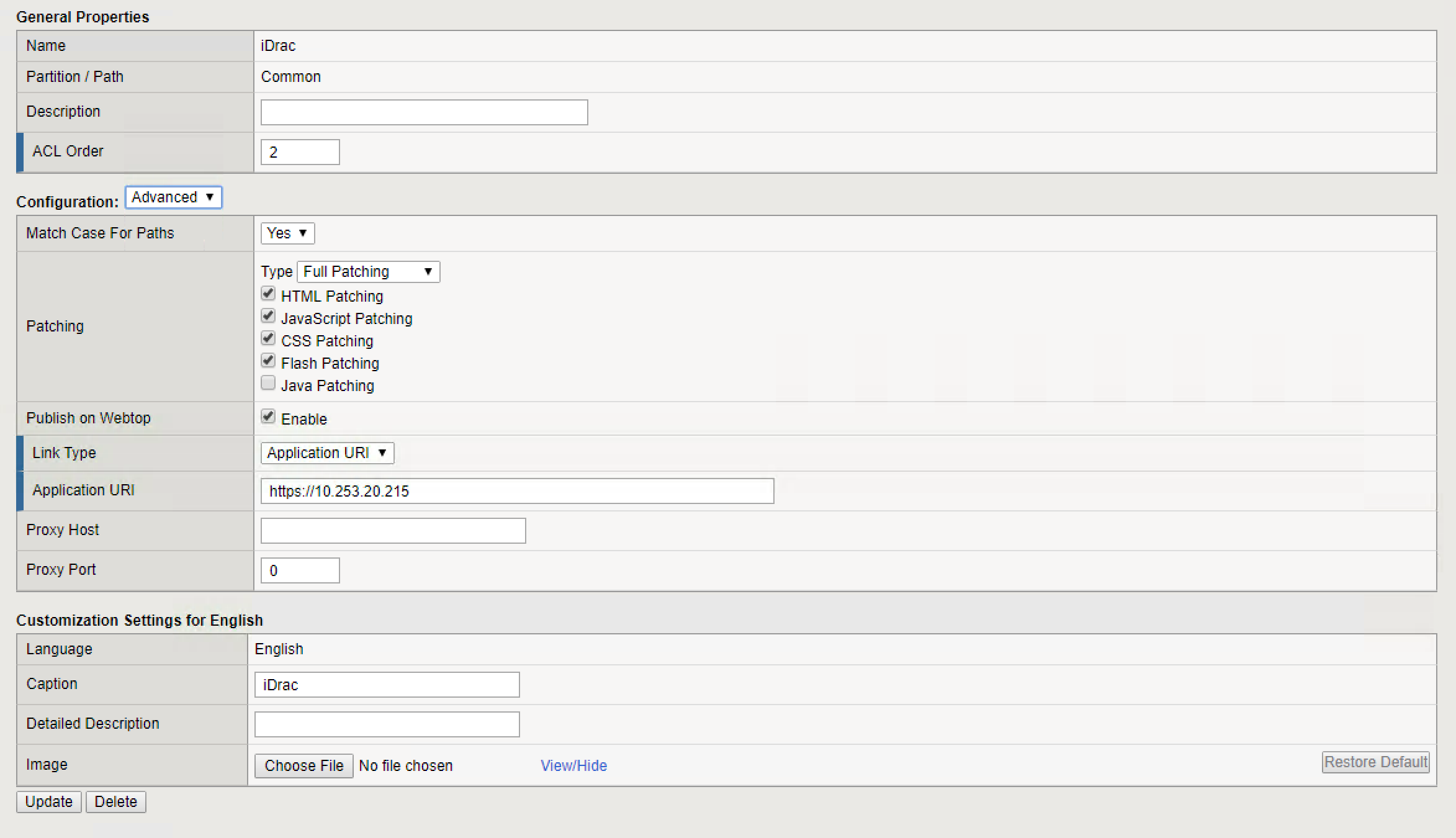
1. Create Portal Access Resource for iDrac

In the APM menu select Connectivity / VPN : Portal Access : Portal Access Lists

Name: Your choice “iDrac” for example

Leave Patching to be default.

Application URI: Needs to be the IP or hostname of the iDrac Server



1. Create a Resource Item withing the portal Access Resource.

For resource type use the IP Address.

For Link Type Select “Paths”

For the Paths Entry Field type /\*

Scheme = https

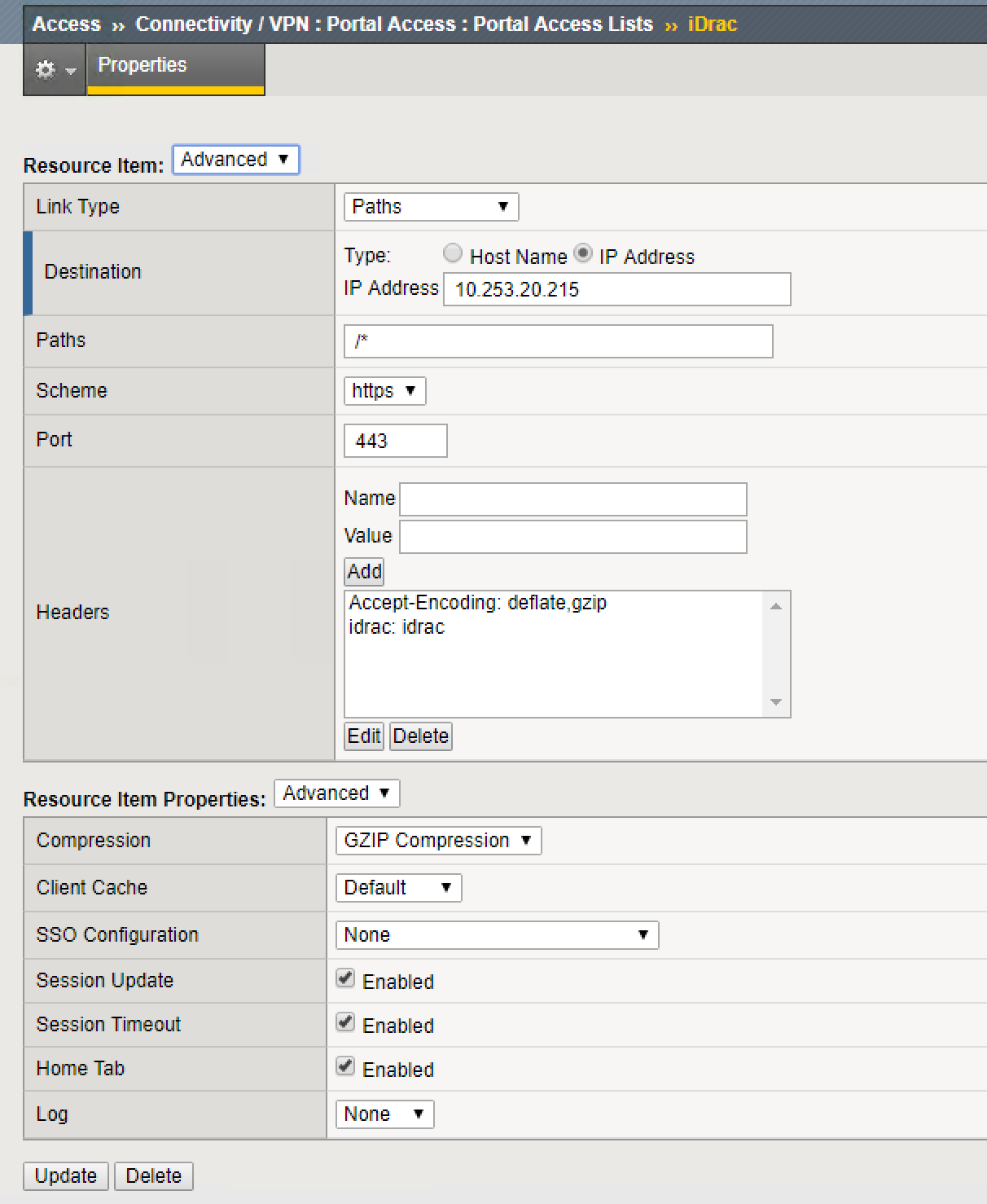
For Headers Add

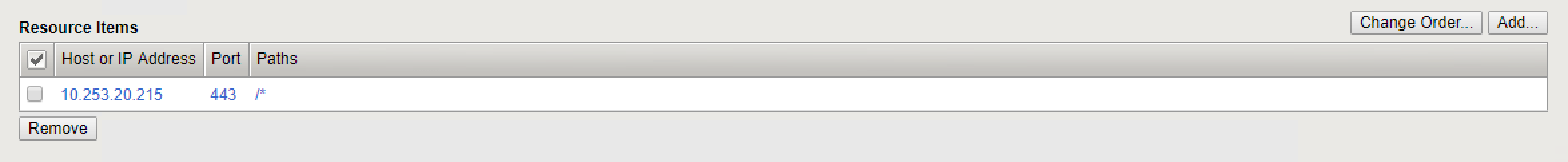
Name: Accept-Encoding

Value:deflate, gzip

Name: idrac

Vlaue: idrac





1. Apply the iDrac iRule to the VIP .. for example a “PUA Webtop” VIP

Note: This iRule depends on session variables existing in the APM policy.

session.logon.last.username

session.custom.ephemeral.last.password\_sso

Insert iRule Below

when REWRITE\_REQUEST\_DONE {

#check for the existence of the correct uri

if { [HTTP::uri] ends\_with "/login.html" || [HTTP::header exists idrac] } {

set workaround 1

REWRITE::post\_process 1

} elseif { [info exists workaround] } {

unset workaround

}

}

when REWRITE\_RESPONSE\_DONE {

if { [info exists workaround] } {

unset workaround

set location [string last "</body>" [REWRITE::payload]]

if { $location > 0 && \

$location < [expr {[REWRITE::payload length] - 5}]

} {

set username [ACCESS::session data get session.logon.last.username]

set password [ACCESS::session data get session.custom.ephemeral.last.password\_sso]

set newstring "<script>

var checkExist = setInterval(function() {

if (document.body.contains(document.getElementById(\"user\"))) {

clearInterval(checkExist);

document.getElementById(\"user\").value = \"$username\";

document.getElementById(\"password\").value = \"$password\";

frmSubmit();

}

}, 2000); // check every 2 seconds. Can be adjusted if timing is an issue.

</script>"

REWRITE::payload replace $location 0 $newstring

}

unset location

}

}

1. You can then associate the portal access resource item with the Webtop Policy.

* Click Access/Profiles
* Click “Edit” under Per-Session Policy
* Select the Webtop. This will be associated with an “Advanced Resource Assign Webtop Item”
* Then Select the Add/Delete Button
* Then select the Portal Access Tab
* Then Select the Portal Access webtop Item that you want to display on the webtop… for Example. “Unity”

