Remote Role Groups

Introduction

The following QuickLabs are designed for the learner who has completed the *Administering BIG-IP* instructor-led training course and wants to continue learning about administering local user roles. The labs complement the learning concepts and tasks performed in the “User Roles and Admministration Partitions” portion of the training course.

Remote User Account Management Overview

About Remote User Accounts

Every BIG-IP system requires one or more administrative user accounts. Rather than store these BIG-IP user accounts on the BIG-IP system, you can store BIG-IP user accounts on a remote authentication server -- either LDAP, Active Directory, RADIUS, or TACACS+.

You create all of your standard user accounts (including user names and passwords) on the remote server, using the mechanism supplied by that server’s vendor. The remote server performs all authentication of those user accounts.

Configure your remote authentication server first, then configure the BIG-IP system. There are F5 solutions written for many of the remote authentication servers that you can access from the AskF5 Knowledge Base.

In this QuickLab, we have selected RADIUS authentication documented in the following solution:

SOL14324: Using F5 vendor-specific attributes with RADIUS authentication (11.x-12.x).

Prerequisites

You must have administrative access to the BIG-IP system and administrative access to the RADIUS server. Use F5 vendor-specific attributes (VSA) when configuring remote RADIUS authentication.

Procedures

- Adding the F5 dictionary file to the RADIUS server
- Configuring user accounts on the RADIUS server
- Specifying RADIUS server information on the BIG-IP system
- Configuring the remote role group on the BIG-IP system

Lab 1A: Specifying RADIUS server information

Lab Preparation: Restore UCS file on BIG-IP System

1. Click the **Firefox web browser** icon in the toolbar to access your BIG-IP system. The icon automatically opens a browser session to the BIG-IP system at https://192.168.1.31.
2. When prompted, log in with the credentials: Username: **admin** and Password: **admin**.
3. Navigate to **System » Archives**.
4. Click **Upload**, then click **Browse** and select the **Downloads** folder.
5. Select **QL_basic.ucs** and click **Open**, then click **Upload**.
6. Click **QL_basic.ucs**.
7. Click the **Restore** button.
   The restore process will take about a minute or two. Please wait until the Operation Status message indicates **Full configuration has been loaded successfully**. Be patient.
8. Click the **OK** button.

Configure Remote Authentication Server

The first step is to add the F5 dictionary file to the RADIUS server. Next configure user accounts on the RADIUS server.

The format of the RADIUS server varies by vendor. Refer to your RADIUS software documentation for the appropriate formatting.

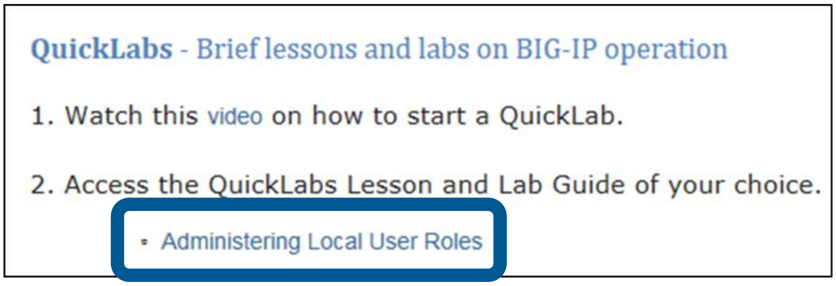
In our lab, the “heavy lifting” has been done for you. We have configured a RADIUS server with the following usernames, passwords, and roles:

Username	Password	User Role	Remote Group Name
admin1	admin1	Administrator	admin-group
admin2	admin2	Auditor	admin-group
admin3	admin3	User Manager	admin-group
admin4	admin4	Operator	admin-group

In this lab, we are using the Administrator, Auditor, User Manager, and Operator roles.

You can access all the user roles listed with a brief description of each in the BIG-IP System: User Account Administration manual.

If you’d like to practice performing the tasks that these roles can perform, you can access the QuickLab entitled *Administering Local User Roles* on F5.learn.com in the F5 Training Lab section.



QuickLabs - Brief lessons and labs on BIG-IP operation

1. Watch this video on how to start a QuickLab.

2. Access the QuickLabs Lesson and Lab Guide of your choice.

- Administering Local User Roles

Specify RADIUS Server Information

Since the BIG-IP system user accounts and user groups have already been created on the remote authentication server, you are ready to configure the BIG-IP system to communicate with the remote authentication server. Follow these steps:

1. Navigate to **System** » **Users** and click **Authentication**.

2. Configure the remote authentication with the following properties and leave all other values at the default:

System » Users: Authentication		
Authentication		
	User Directory	Click **Change.** Use the pull down menu and select **Remote – RADIUS**
	Server Configuration	**Primary Only**
	Primary	**Host: 172.16.20.1** **Port: 1812** **Secret: testing123** **Confirm: testing123**
When complete, click...	**Finished**	

You can configure a Primary and a Secondary remote server. In our example, we'll configure only the primary server.

Lab 1B: Create Remote Role Group on the BIG-IP system

Create Remote Role Group

Lab Requirements

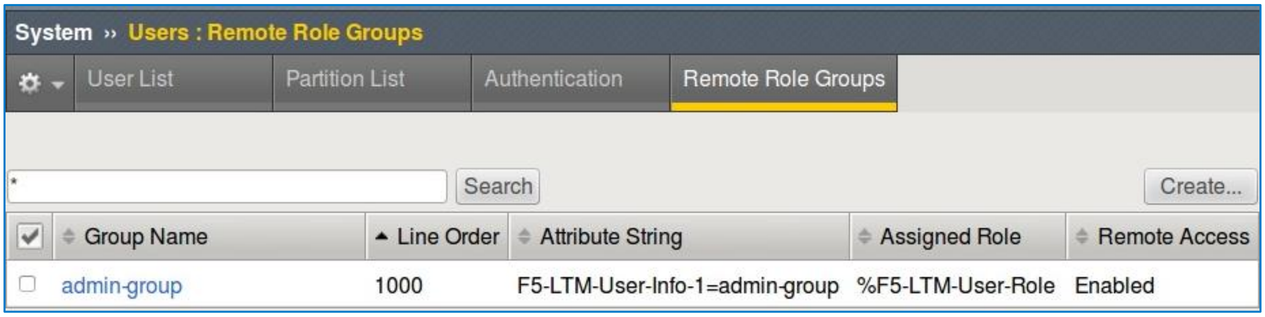
- You must have successfully completed *Lab 1A: Specifying RADIUS Server Information* prior to beginning this lab.

On the BIG-IP system, configure a remote role group to use the attributes provided by the RADIUS server using either the Configuration utility or TMSH.

a. If using the Configuration utility, navigate to **System » Users : Remote Role Groups** and click **Create**. Enter the following fields.

System » Users: Remote Role Groups » New Remote Role Group...	
Account Properties	
Group Name	**admin-group**
Line Order	**1000**
Attribute String	**F5-LTM-User-Info-1=admin-group**
Remote Access	**Enabled**
Assigned Role	**Other %F5-LTM-User-Role**
Partition Access	**Other %F5-LTM-User-Partition**
Terminal Access	**Other %F5-LTM-User-Shell**
When complete, click...	**Finished**

From the Configuration utility, your Remote Role Group should look like this:



☑	Group Name	Line Order	Attribute String	Assigned Role	Remote Access
□	admin-group	1000	F5-LTM-User-Info-1=admin-group	%F5-LTM-User-Role	Enabled

b. If you prefer using TMSH, click on the Putty SSH Client icon and open an SSH session to 192.168.1.31 and log in with the credentials: Username: **root** and Password: **default.** Enter the following:

```
tmsh modify auth remote-role role-info add { admin-group {
attribute F5-LTM-User-Info-1=admin-group console %F5-LTM-User-
Shell line-order 1000 role %F5-LTM-User-Role user-partition %F5-
LTM-User-Partition } }
```

Save the configuration by typing the following command:

```
tmsh save sys config
```

Continue with the next lab.

Lab 1C: Verify Communication between BIG-IP system and RADIUS server

Verify Communication between BIG-IP System and Remote Authentication Server

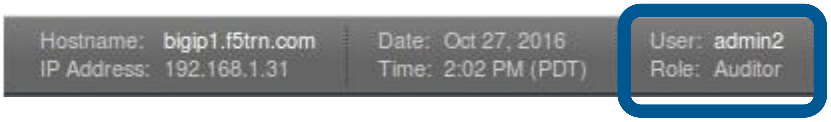
In this lab, you will test whether the BIG-IP system is communicating with the remote authentication server.

Lab Requirements

- You must have successfully completed *Lab 1B: Create Remote Role Group on the BIG-IP System* prior to beginning this lab.

You can do a quick test by logging out of the Configuration utility in your current role, and log back in as a different user. For example, login with these credentials: User: **admin2** and Password: **admin2**. You should see the role of Auditor as shown below.

Refer to the banner above the F5 icon.



Hostname: bigip1.f5trn.com
IP Address: 192.168.1.31

Date: Oct 27, 2016
Time: 2:02 PM (PDT)

User: admin2
Role: Auditor

Verifying handshake between BIG-IP system and RADIUS server

You may need to run **tcpdump** packet captures to troubleshoot communication between your authentication server and the BIG-IP system. In this lab, we'll use tcpdump to verify that you are receiving the authenticator fields known as **Request Authenticator** (sent in RADIUS request packets) and **Response Authenticator** (sent in RADIUS response packets).

For more information on troubleshooting the RADIUS server, refer to the solution: SOL15763: Troubleshooting RADIUS authentication for BIG-IP administrators.

In this lab you will use the PuTTy client to open an SSH session to the BIG-IP system. You will use tcpdump to capture packets to verify that the RADIUS server is communicating with the BIG-IP system.

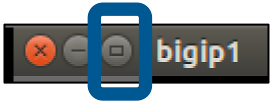
Usually you would use tcpdump to take the capture and store it in a binary file with a `pcap` extension. Subsequently, this `pcap` file could be opened in any packet analysis program for detailed debugging.

For the purposes of this lab, we'll view the output directly on the terminal screen.

To packet trace RADIUS traffic, perform the following procedure.

1. Log out of the Configuration utility.
2. Click the PuTTy icon and open an SSH session to BIG-IP at **192.168.1.31** and port **22**. Login with the credentials login: **root** and password: **default**.
3. At the bash prompt, enter the following command:

   ```
   tcpdump -s0 -ni internal port 1812 -v
   ```
4. Return to the Configuration utility and login as **admin2** with the password **admin2**.
5. Toggle back to PuTTy. To do that, you may have to click the PuTTy icon twice. To make it easier to read, click to expand the screen.

6. Use **Control-C** to terminate the tcpdump.
7. To interpret the output, look for the following. The ephemeral ports will vary.
   - **172.16.1.31.**12840 **> 172.16.20.1 radius** indicates the BIG-IP internal VLAN IP address is communicating with the IP address of the RADIUS server.
   - Next you'll notice the authenticator field is used to authenticate the user from the RADIUS server. First you'll see the RADIUS request packet called **Access Request**.
   - This is followed by a number of attributes containing information such as authentication, authorization, and configuration details.
   - Then, you'll see **172.16.20.1.radius > 172.16.1.31.**12840. This indicates the RADIUS server is communicating to the BIG-IP system on the internal VLAN.
   - Finally, the response authenticator sent in RADIUS response packet is sent indicated by **Access Accept**.
8. Enter **q** to quit the text file and **exit** to close the PuTTy session.

Expected Results

During Lab 1C: Verify Communication between BIG-IP system and RADIUS server, you will run tcpdump. After logging in to the BIG-IP system as admin2 (or any of the other accounts), you should be able to see the handshake between BIG-IP system and the RADIUS server as the output of the tcpdump as seen in the screen shots below.

We've highlighted in **bold** some of the key fields. Note that the ephemeral ports will vary.

```
172.16.1.31.10635 > 172.16.20.1.radius: RADIUS, length: 91
    Access Request (1), id: 0xa4, Authenticator: 8863b1781c9ac4d3534dd41c54102b8b
      Username Attribute (1), length: 8, Value: admin1
      Password Attribute (2), length: 18, Value:
      NAS IP Address Attribute (4), length: 6, Value: 192.168.1.31
      NAS ID Attribute (32), length: 7, Value: httpd
      NAS Port Attribute (5), length: 6, Value: 9610
      NAS Port Type Attribute (61), length: 6, Value: Virtual
      Service Type Attribute (6), length: 6, Value: Authenticate Only
```

```
                         Calling Station Attribute (31), length: 14, Value: 192.168.1.30 out slot1/tmm1 lis=
13:37:11.619281 IP (tos 0x0, ttl 64, id 30107, offset 0, flags [none], proto UDP (17), length 102)

                  172.16.20.1.radius > 172.16.1.31.10635: RADIUS, length: 74
                        Access Accept (2), id: 0xa4, Authenticator: d1ab0a66da81a095daf820256142ca20
                         Vendor Specific Attribute (26), length: 12, Value: Vendor: Unknown (3375)
                         Vendor Attribute: 1, Length: 4, Value: ....
                         Vendor Specific Attribute (26), length: 19, Value: Vendor: Unknown (3375)
                         Vendor Attribute: 12, Length: 11, Value: admin-group
                         Vendor Specific Attribute (26), length: 11, Value: Vendor: Unknown (3375)
                         Vendor Attribute: 3, Length: 3, Value: all
                         Vendor Specific Attribute (26), length: 12, Value: Vendor: Unknown (3375)
                          Vendor Attribute: 5, Length: 4, Value: tmsh in slot1/tmm1 lis=

   ^C

   2 packets captured

   2 packets received by filter

   0 packets dropped by kernel
```

This completes QuickLabs: *Remote Role Groups*