Remote Authorization via Active Directory

Jason Rahm, 2011-27-04

A while back I wrote an article on remote authorization via tacacs+. I got a question in the comments yesterday about the same functionality with active directory. I hadn't done anything with active directory outside of APM, so I wasn't sure I could help. However, after reading up on a few solutions on askF5 (10929 and 11072 specifically), I gave it a shot and turns out it's not so difficult at all. For more details on the roles themselves, reference the tacacs+ article. This tech tip will focus solely on defining the administrator and guest roles in the remoterole configuration on BIG-IP and setting up the active directory attributes.

Mapping AD Attributes

The attribute in the remoterole for active directory will look like this:

> memberOF=cn=<common name>, ou=<organizational unit>,dc=x,dc=y

Let's break down the attribute string:

- The cn can be a single account, or a group. For example, jason.rahm (single account) or grp-Admins (security group) In the string, they're represented as such:
  - memberOF=cn=jason.rahm
  - memberOF=cn=grp-Admins
- The ou is the organization unit where the cn is defined. It can be deeper than one level (So if the OU organization was IT->Ops and IT->Eng, the ou part of the string would like this:
  - ou=Ops,ou=IT
  - ou=Eng,ou=IT
- The dc is the domain component. So for a domain like devcentral.test, the dc looks like this
  - dc=devcentral,dc=test

Putting the examples all together, one attribute would look like this:

> memberOF=cn=grp-Admins,ou=Ops,ou=IT,dc=devcentral,dc=test

Defining the Remote Role Configuration

In tmsh, the remote-role configuration is under the auth module. The configuration options available to a specific role (defined under role-info) are shown below

```
(tmos.auth.remote-role)# modify role-info add { F5Guest { ?
Properties:
  "}"            Close the left brace
  attribute      Specifies the name of the group of remotely-authenticated users for whom you are
configuring specific access rights to the BIG-IP system.
                 This value is required.
  console        Enables or disables console access for the specified group of remotely
authenticated users. You may specify bpsh, disabled, tmsh or use
                 variable substitution as describe in the help page. The default value is disabled.
  deny           Enables or disables remote access for the specified group of remotely authenticated
users. The default value is disable.
  line-order     Specifies the order of the line in the file, /config/bigip/auth/remoterole. The LDAP
and Active Directory servers read this file line by
                 line. The order of the information is important; therefore, F5 recommends that you set
the first line at 1000. This allows you, in the
                 future, to insert lines before the first line. This value is required.
  role           Specifies the role that you want to grant to the specified group of remotely
authenticated users. The default value is no-access. The
                 available roles and the corresponding number that you use to specify the role are: admin
(0), resource-admin (20), user-manager (40),
                 manager (100), application-editor (300), operator (400), guest (700), policy-editor (800)
and no-access (900).
  user-partition  Specifies the user partition to which you are assigning access to the specified
group of remotely authenticated users. The default value
                 is Common.
```

With that syntax information and the AD attribute strings, I can define both roles:

```
tmsh modify auth remote-role role-info add { F5Admins { attribute memberOF=cn=grp-F5Admins,ou=Groups,dc=devcentral,dc=test console enable line-order 1 role administrator user-partition all } }

tmsh modify auth remote-role role-info add { F5Guests { attribute memberOF=cn=grp-F5Staff,ou=Groups,dc=devcentral,dc=test console disabled line-order 2 role guest user-partition all } }
```

Next I confirm the settings took.

```
tmsh show running-config /auth remote-role

auth remote-role {
    role-info {
        F5Admins {
            attribute memberOF=cn=grp-F5Admins,ou=Groups,dc=devcentral,dc=test
            console enable
            line-order 1
            role administrator
            user-partition all
        }
        F5Guests {
            attribute memberOF=cn=grp-F5Staff,ou=Groups,dc=devcentral,dc=test
            console disabled
            line-order 2
            role guest
            user-partition all
        }
    }
}
```

Configure the BIG-IP to Use Active Directory

Here I set the BIG-IP to use ldap authentication, defining my base-dn and the login attribute (samaccountname) and the user template (%s@devcentral.test).

```
tmsh modify auth ldap system-auth login-attribute samaccountname search-base-dn dc=devcentral,dc=test servers add { 192.168.202.110 } user-template %s@devcentral.test
```

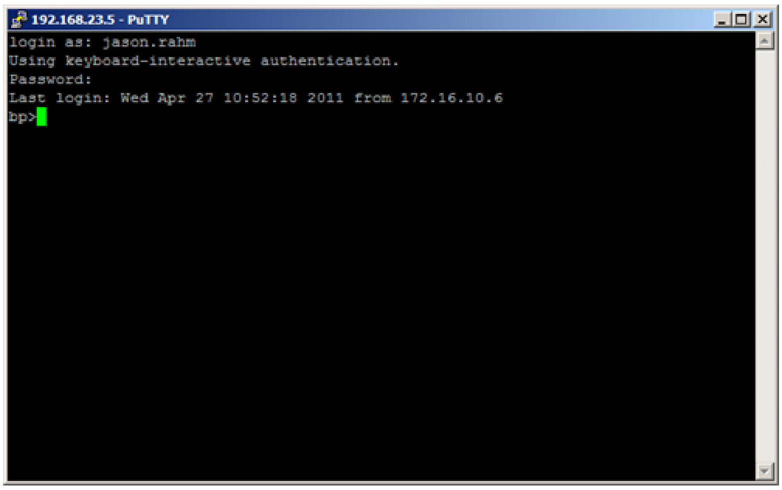
And once again confirming the settings:

```
tmsh show running-config /auth ldap system-auth

auth ldap system-auth {
   login-attribute samaccountname
   search-base-dn dc=devcentral,dc=test
   servers { 192.168.202.110 }
   user-template %s@devcentral.test
}
```

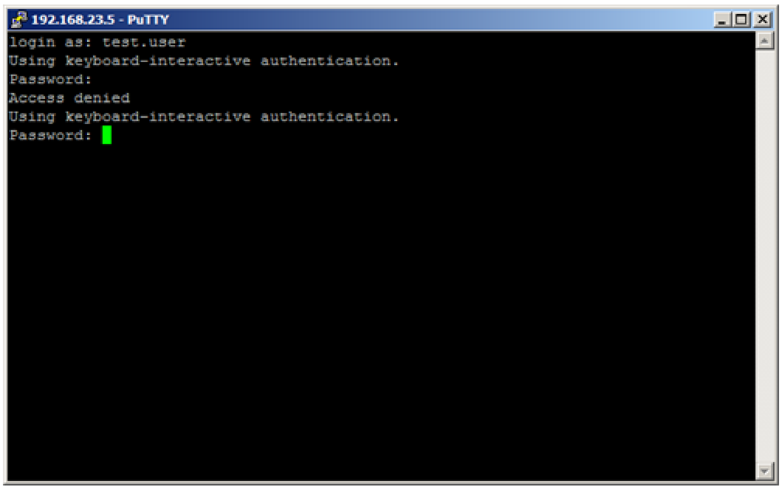
Testing the Configuration

For the test there are two users. test.user belongs the grp-F5Staff cn, and jason.rahm belongs to the grp-F5Admins cn. Therefore, test.user should have Guest access to the GUI and no access to the console, whereas jason.rahm should have Administrator access to the GUI and console access. Let’s see if that’s the case.



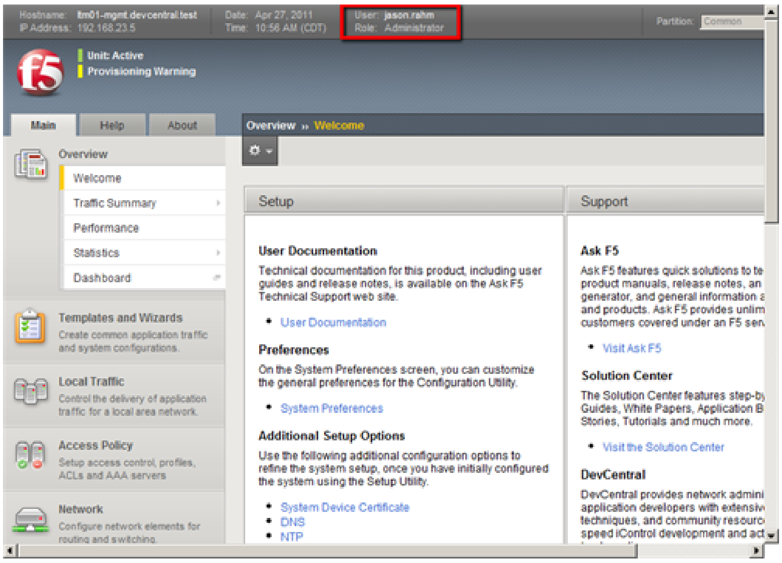
```
login as: jason.rahm
Using keyboard-interactive authentication.
Password:
Last login: Wed Apr 27 10:52:18 2011 from 172.16.10.6
bp>
```

grp-F5Admins access to console confirmed



```
login as: test.user
Using keyboard-interactive authentication.
Password:
Access denied
Using keyboard-interactive authentication.
Password:
```

grp-F5Staff disabled console confirmed



Hostname: ltm01-mgmt.devcentral.test
IP Address: 192.168.23.5

Date: Apr 27, 2011
Time: 10:56 AM (CDT)

User: jason.rahm
Role: Administrator

Partition: Common

Unit: Active
Provisioning Warning

Main
Help
About
Overview » Welcome
Overview
Welcome
Traffic Summary
Performance
Statistics
Dashboard
Templates and Wizards
Create common application traffic and system configurations.
Local Traffic
Control the delivery of application traffic for a local area network.
Access Policy
Setup access control, profiles, ACLs and AAA servers
Network
Configure network elements for routing and switching.
Setup
Support

User Documentation

Technical documentation for this product, including user guides and release notes, is available on the Ask F5 Technical Support web site.

- User Documentation

Preferences

On the System Preferences screen, you can customize the general preferences for the Configuration Utility.

- System Preferences

Additional Setup Options

Use the following additional configuration options to refine the system setup, once you have initially configured the system using the Setup Utility.

- System Device Certificate
- DNS
- NTP

Ask F5

Ask F5 features quick solutions to te
product manuals, release notes, an
generator, and general information a
and products. Ask F5 provides unlim
customers covered under an F5 serv

- Visit Ask F5

Solution Center

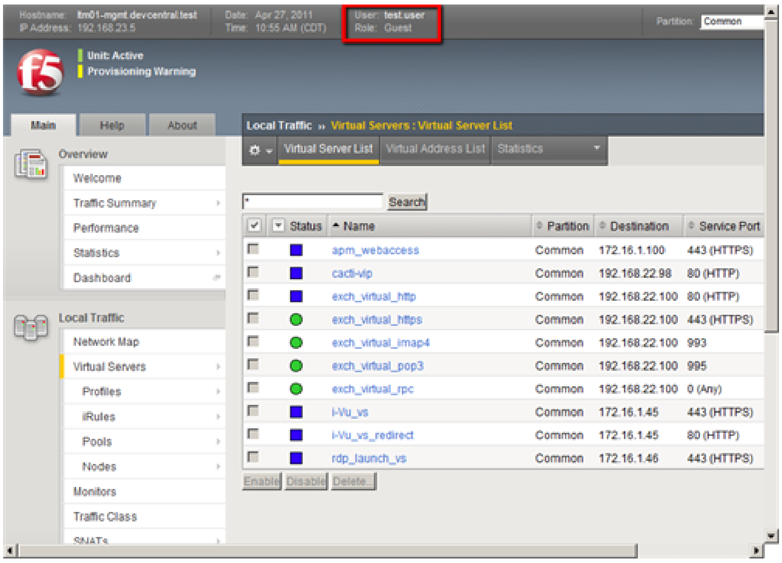
The Solution Center features step-by
Guides, White Papers, Application B
Stories, Tutorials and much more.

- Visit the Solution Center

DevCentral

DevCentral provides network admini
application developers with extensiv
techniques, and community resourc
speed iControl development and act

grp-F5Admins GUI Administrator role confirmed



Hostname: ltm01-mgmt.devcentral.test
IP Address: 192.168.23.5
Date: Apr 27, 2011
Time: 10:55 AM (CDT)
User: test.user
Role: Guest
Partition: Common

Unit: Active
Provisioning Warning

Local Traffic » Virtual Servers : Virtual Server List

Search: *

☑	Status	Name	Partition	Destination	Service Port
□	■	apm_webaccess	Common	172.16.1.100	443 (HTTPS)
□	■	cacti-vip	Common	192.168.22.98	80 (HTTP)
□	■	exch_virtual_http	Common	192.168.22.100	80 (HTTP)
□	●	exch_virtual_https	Common	192.168.22.100	443 (HTTPS)
□	●	exch_virtual_imap4	Common	192.168.22.100	993
□	●	exch_virtual_pop3	Common	192.168.22.100	995
□	●	exch_virtual_rpc	Common	192.168.22.100	0 (Any)
□	■	i-Vu_vs	Common	172.16.1.45	443 (HTTPS)
□	■	i-Vu_vs_redirect	Common	172.16.1.45	80 (HTTP)
□	■	rdp_launch_vs	Common	172.16.1.46	443 (HTTPS)

grp-F5Staff GUI Guest role confirmed

Conclusion

In this tech tip I walked through the steps required to configure remote authorization utilizing the BIG-IP remoterole configuration and Active Directory. I didn't cover the custom attributes like the in tacacs+ article, but the same process applies, so if you'd rather define the roles within Active Directory that can be done as well.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com