Auto-launch Remote Desktop Sessions with APM

Jason Rahm, 2011-20-04

In my spare time, I do volunteer IT work and for quite some time my users have used the SSL-Explorer fork AditoVPN to get remote access to their work machines remotely. Adito does the job, but it requires a server (albeit virtual, but still) that must be maintained, seems to have been forked again (OpenVPN ALS) and occasionally locks up and requires more hands-on attention than I really have time for. I bought a copy of LTM VE last year to handle the web/mail services and was excited about moving users off the Adito solution when I learned that APM VE would be available when version 10.2.1 was released. I never have more than a handful of users accessing at the same time, so the base APM Limited license that is included with LTM VE suited me just fine. This article will show users how to configure APM to auto-launch a remote desktop session to an Active Directory user's specified computer.

APM Required Components

The network access wizard does a tremendous job of getting the configuration kicked off, so I'd recommend that as a starting point. A couple things however that weren't exactly obvious or just didn't work:

- If you already have your domain controller defined and in use on another application, you'll need to define a dummy AD scenario or the wizard will fail. After the configuration is complete, you can reselect the proper server in your policy and then you can delete the dummy config.
- The ssl certificates/profiles are absent from the wizard, so you'll need to configure these separately.

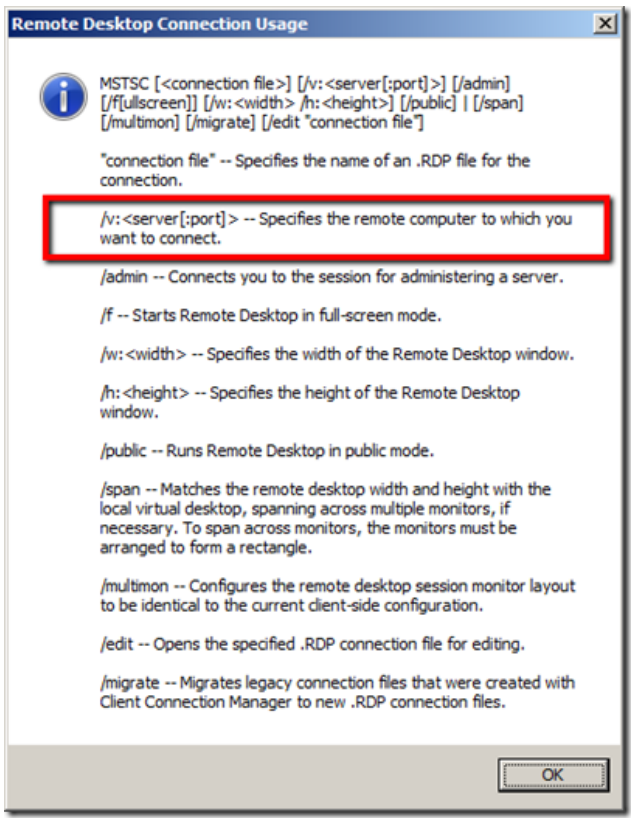
After the wizard is complete, you end up with these configuration objects:

- Access Profile w/ Policy
- AAA Server
- Network Access Resource
- Lease Pool
- Webtop
- Virtual Server (or two if configuring the redirect from http)
- Connectivity Profile

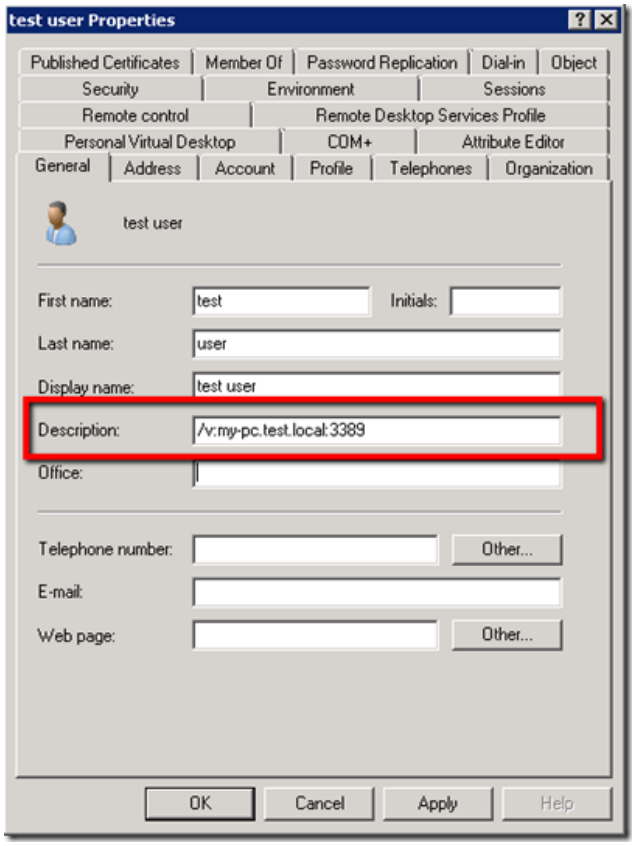
As stated previously, you'll need to separately configure your ssl certificate and profile and update your virtual server accordingly.

Preparing Active Directory

The goal here is to minimize the amount of work required of remote users. Once a user is logged in, the remote desktop client should launch for the user and be populated with the server (or desktop) name/ip. If you choose, you can also have the users store credentials in an rdp file on their desktop so it would only require a single logon, but since that's not a secure practice I won't cover that here. To auto-launch rdp, you need to call the mstsc.exe executable with the /v option:

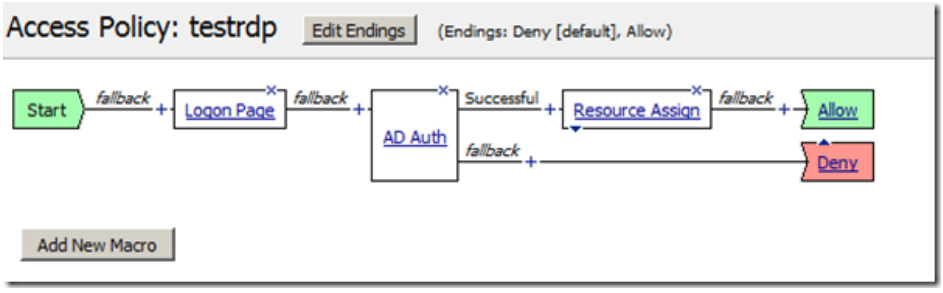


Any attribute on the account will do, but for this example I'm using the description attribute on the test.user AD account:

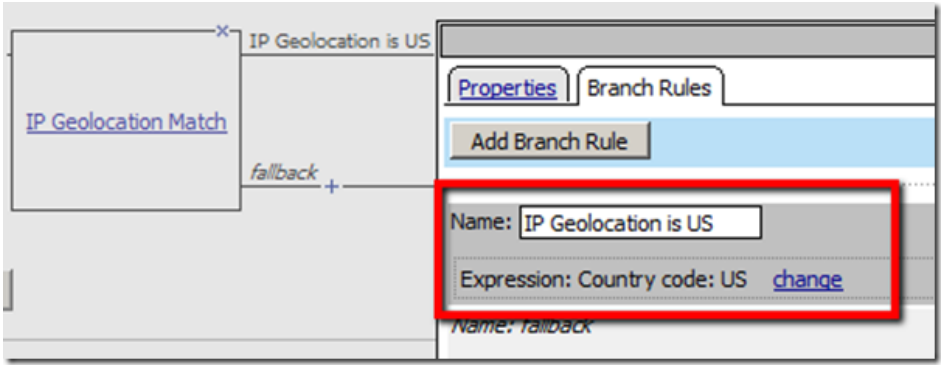


Access Policy Configuration

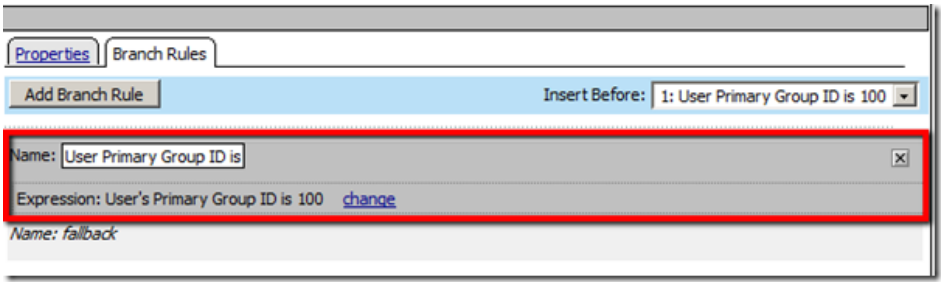
The network access wizard created an access policy that looks like this:



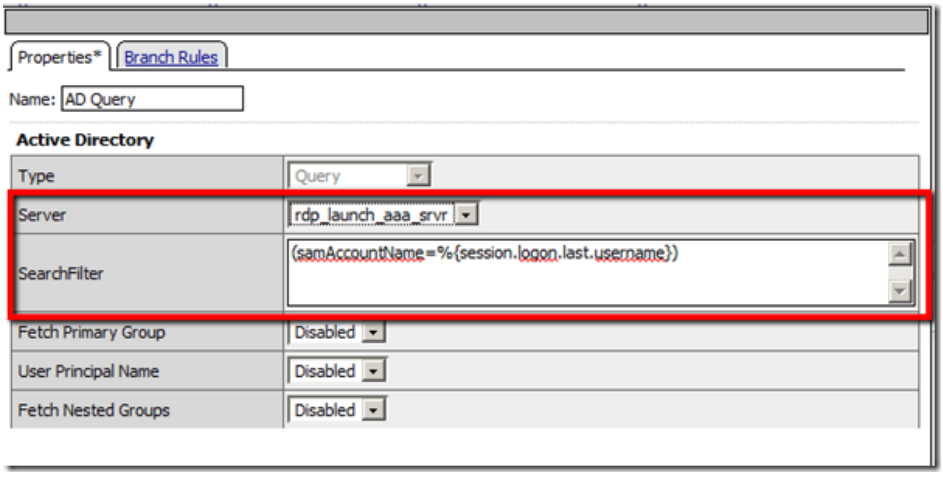
If you created your real AD server, you won't need to update the AD Auth object. However, if you created a dummy AD in the network wizard, you'll need to open AD Auth, select your real server, then click save. Because I know where my users are, I'm going to start the policy with an IP Geolocation Match object and restrict to the United States.



You can see the actual object on the left and the configuration of the "successful" branch in the expression above. If the location data matches the US, the logon page is presented. I used a standard Logon Page object here. After the logon page is the AD_Auth object, and then I added an AD Query object immediately after on the Successful branch of the AD Auth object. First, I removed the first branch rule (highlighted) from the object as it is unnecessary:



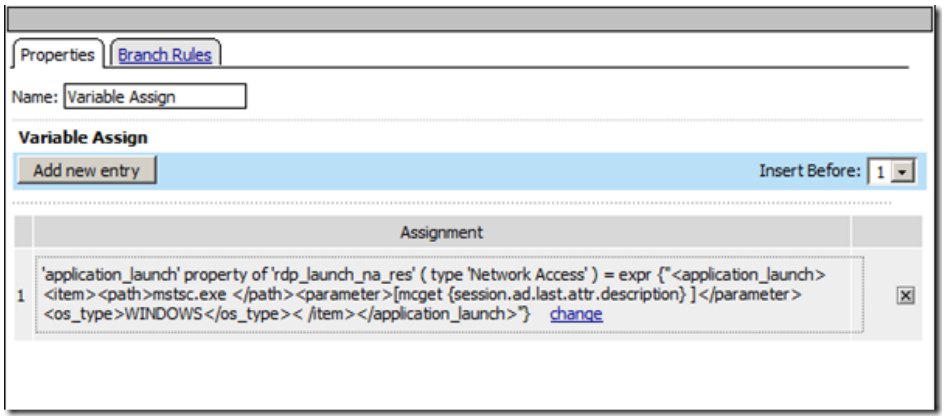
Then, I entered the search filter for the username:



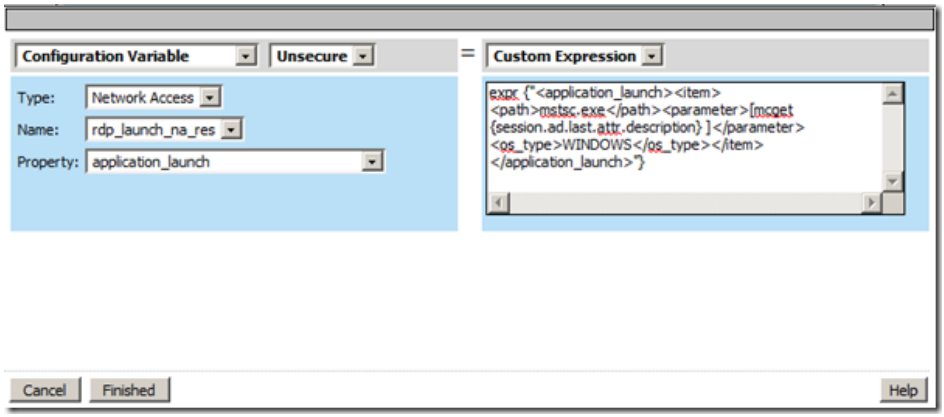
Text in the above image is:

> (samAccountName=%{session.logon.last.username})

On the fallback path of the AD Query object, insert a Variable Assign object (should sit in between AD Query and the already present Resource Assign objects):



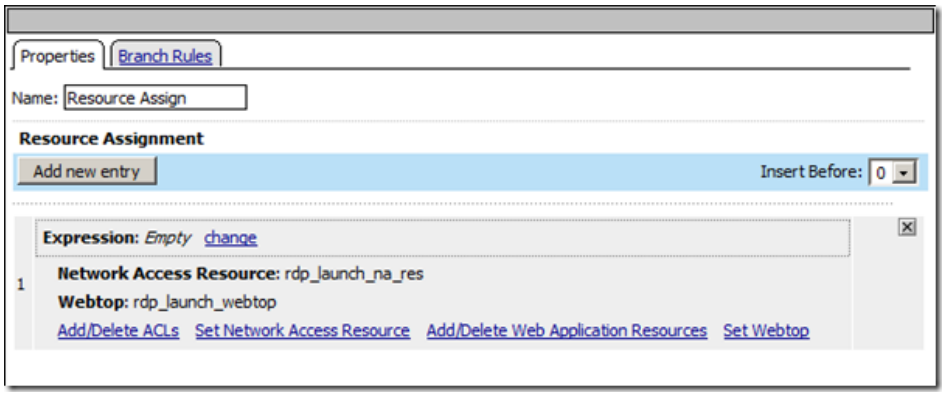
Add an entry as shown above. Change to a configuration variable and set the type/name/property as shown below:



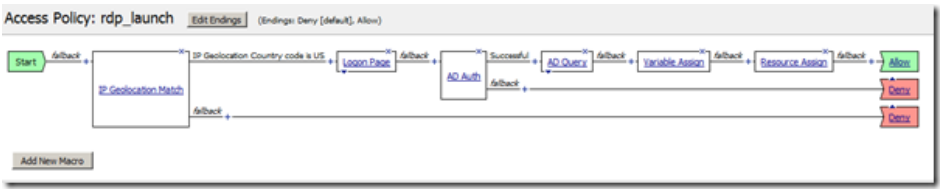
The expression text is:

```
expr {"<application_launch><item><path>mstsc.exe</path><parameter>[mcget
{session.ad.last.attr.description} ]</parameter><os_type>WINDOWS</os_type></item>
</application_launch>"}
```

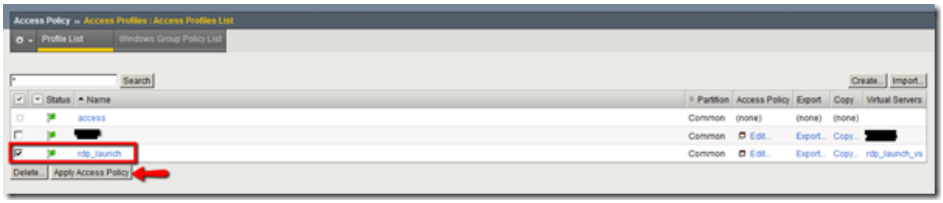
If you used the network access wizard, the Resource Assign object is already complete, but if starting from scratch, you'll want to assign a network access resource and a webtop from your configuration:



Final step is to change the Deny flag after the Resource Assign object to Allow. This should result in an overview of the Access Policy as such:



On the Access Profiles list, make sure you apply the access policy if you haven't:



That should do it!

Testing RDP Auto-Launch

Enough of configuration…does it work? Let's give it a try:

APM RDP Auto-Launch

Conclusion

The APM module for BIG-IP is an amazing access solution. The default behavior in this scenario is to auto-launch the remote desktop session, but in addition to that functionality the user also has normal network-level access to whatever networks you defined while working through the wizard. Much thanks to F5er Doug Lohf for configuration details and insight.

Related Articles

- Pete Silva - apm
- DevCentral Wiki: BIG-IP Access Policy Manager (APM) Wiki Home
- Does LTM any advanced health monitor for RDP service? - DevCentral ...
- F5 Tutorial: BIG-IP APM with SecureAuth
- Web Application Login Integration with APM > DevCentral > F5 ...
- Set APM Cookies to HttpOnly - DevCentral - F5 DevCentral ...
- nested virtuals with APM - DevCentral - F5 DevCentral > Community ...
- RDP acceleration - DevCentral - F5 DevCentral > Community > Group ...
- DevCentral Wiki: APM
- NTLM/ Outlook Anywhere/ Big-IP APM - DevCentral - F5 DevCentral ...

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