Infrastructure - Task #7279

MN implementation documentation - need document management solution

2015-07-28 22:24 - Laura Moyers

Status:	New	**Start date:**	2015-07-28
Priority:	Normal	**Due date:**	
Assignee:	Dave Vieglais	**% Done:**	0%
Category:	Documentation	**Estimated time:**	0.00 hour
Target version:			
Milestone:	None	**Story Points:**	
Product Version:	*		

Description

Eric Fritzinger at NRDC (ericf@cse.unr.edu) sent us a write-up of what he had to do on his Windows front-end/Linux back-end setup to do a reverse proxy for the NRDC MN. We need to decide the best document management solution for this and similar user-contributed documentation. We expect some info from Ed Flathers at NKN documenting his implementation using Red Hat.

Eric's text:

Just as an addendum, and for your documentation in the future should you have any users with a similar setup (or who want a similar setup), we managed to get the reverse proxy working with https.

As you may recall, our server setup is a Windows Server 2012 IIS 8 server acting as a reverse proxy to the back-end GMN linux server. In order to get IIS 8 to work with using https on the back-end, there are a couple things that had to be done.

First, I had to update the IIS Application Request Routing module to 3.0 (I was previously using 2.0).

Secondly, I had to make sure the reverse proxy server trusted the certificate used by the target server. There are two ways to do this (the “target server” in these cases is the back-end GMN server that the reverse proxy is pointing to):

1.) Create a Certificate Root Authority server that the cluster recognizes and trusts (Windows Server OS has a Role that can be added for this purpose). Make sure the reverse proxy server recognizes the CRA as a Trusted source (explained below). Then, have the CRA issue the certificate requested by the target server and configure the target server to use that issued certificate.

2.) Create a self-signed certificate on the target server and export it. Have the IIS 8 server import the certificate as a Trusted Certificate Root Authority certificate (explained below), and it will be trusted.

To check the status of a Trusted CRA on a Windows Server OS, or to import a certificate into the TCRA:
1. Go to Start -> Run, type “mmc.exe” and click OK
2. When the console window comes up click File->Add/Remove Snap-In…
3. Add the “Certificates” module and click Next
4. Select the “Computer Account” option, click Next
5. Select the “Local Computer” option, click OK

If you expand the tree, you’ll see the “Trusted Certificate Root Authorities” folder to see all the trusted root authorities. This is where either the local Certificate Root Authority server certificate should be, or where you import the target server’s self-signed certificate (by right-clicking the folder and selecting Import from the context menu).

Option 1 is typically good for larger server clusters that will have a lot of servers behind a reverse proxy using https (which we eventually will be using). Option 2 is quick and easy. I went with Option 2 for now since I wanted to be sure it worked quickly without much hassle.

This write-up is mainly to let you all know how we got it to work (I’m not a fan of “magic”, myself =)). Also, I wanted to make sure it was written down somewhere in case of emergency.