**Manual steps to create Zaplify Splunk VM role in Azure**

6/19/12 – first draft (Omri)

1. Create a VM role via the Azure portal (in this document it’s called zaplify-splunk)
2. Give it a service name (zaplify-splunk) which will become zaplify-splunk.cloudapp.net
3. Give it the well-known password for the Administrator account (to be able to TS into the machine)
4. Use the Azure portal to attach a 100GB drive (which creates a new Azure Storage account and puts a blob in that account). Alternatively, attach a VHD of the existing drive.
5. MSTSC into the VM and format the 100GB and map it as the Z drive of the VM
6. Download the Splunk 64-bit full [installer](http://www.splunk.com/download?r=header) (e.g. link to 4.3.2 [version](http://www.splunk.com/index.php/download_track?file=4.3.2/splunk/windows/splunk-4.3.2-123586-x64-release.msi&platform=Windows&architecture=x86_64&version=4.3.2&typed=release&name=windows_installer&d=pro))
   1. Splunk account name: ogazitt, password is the well-known password
7. Install splunk via the MSI
8. Launch the product after install (or navigate to <http://zaplify-splunk:8000>)
   1. Log in as admin/changeme and change the password to the well-known password
9. Configure splunk’s data directory
   1. Cd \program files\splunk\bin
   2. Splunk stop
   3. Cd ..\etc
   4. Edit splunk-launch.conf
   5. Add line “SPLUNK\_DB=z:\splunk\_db”
   6. Cd ..\bin
   7. Splunk start
10. Configure Splunk forwarding via management portal:
    1. Click “manager” on top-right header nav-bar
    2. Click “Forwarding and receiving” under Data (right side of page)
    3. Click “Configure receiving” under Receive data
    4. Click “New” and type “9997” as the receiving port
11. Open up ports on the VM by going into Server Manager
    1. Go into Configuration :: Windows Firewall with Advanced Security :: Inbound Rules
    2. Create a new rule called “Splunk” which allows inbound access on TCP port 8000
    3. Create a new rule called “Splunk-receiver” allowing inbound access on TCP port 9997
12. Configure endpoints in Azure portal by clicking the VM role (which brings up the dashboard) and then clicking Endpoints (there should already be a “RemoteDesktop” endpoint
    1. Create an endpoint called “splunk” (TCP, public and private port 8000, not LB’ed)
    2. Create an endpoint called “splunkreceiver” (TCP, public and private port 9997, no LB)
13. If the Azure Service name that wraps this VM is different from “zaplify-splunk.cloudapp.net”, must also change the SplunkEndpoint config setting in the Zaplify Azure project to be the correct receiving TCP address (e.g. zaplify-splunk2.cloudapp.net:9997)
14. Test external access to the Splunk portal/search app by navigating to <http://zaplify-splunk.cloudapp.net>