

WarpVM™ AWS Quickstart Guide

STEP 1

In EC2, launch a new instance.

- a. Choose an Amazon Machine Image: Select the AWS Marketplace tab and search for *WarpVM*. Select *WarpVM*.
- b. Choose Instance Type: Select the *c4.2xlarge* instance type. This is the only type supported for *WarpVM*.
- c. Configure Instance: Select the desired VPC and subnet for your instance. Note that the *eth0* interface will be your dedicated management interface.
- d. Add Storage: Use the defaults.
- e. Add Tags: Optionally add a name for your instance.
- f. Configure Security Group: Create/select a security group that allows TCP ports 80 and 443.
- g. Review: Verify your choices and then launch the instance.



STEP 2

Once the instance boots, you will need to attach 3 additional network interfaces.

- a. Create each network interface in a different subnet. You can use the same security group as in step 1.
- b. Note that *eth1* is not currently used, but it needs to be present.
- c. *eth2* and *eth3* will be the proxied interfaces. *eth2* is client side, *eth3* is server side. You can assign names to each interface to avoid confusion.
- d. Disable Source/Dest. Check on the *eth2* and *eth3* interfaces.
- e. Attach the interfaces in sequential order (*eth1*, then *eth2*, then *eth3*).

The screenshot shows the WarpEngine Proxy configuration interface. It features a central configuration area for two interfaces, eth2 and eth3. The interface for eth2 is connected to a 'Downstream Gateway' and eth3 to an 'Upstream Gateway'. Both interfaces have a 'Pair Name' of 'ip_0' and an 'MSS' field. The configuration also includes fields for 'VLAN Name', 'VLAN ID', and 'VLAN Priority'. There are checkboxes for 'Enable GTP', 'GTP Seq Num', and 'Spoof Mac'. A 'Verify Configuration' button is located at the bottom left of the interface. The interface also shows a 'Notes' section and a 'Selective Bypass Configuration' section.

STEP 3

Attach an elastic IP to your management interface (eth0)

- Navigate to that address in your browser
- You will be redirected to `https://<public_ip>/index.html`
- You may get a security warning from your browser, this is because we use a self-signed certificate. You can safely add an exception for this site.
- You will then be prompted to log in. Default user is admin, default password is your instance id.

STEP 4

Configure instance

- Click on the Interfaces tab, then click on the eth2 <-> eth3 subtab
- Gateway mode will already be selected. Enter the private IP addresses for the respective interfaces (these should match what was assigned when the network interfaces were created in AWS)
- Specify your gateways for both the client and server sides. These may be the subnet gateway, or it may be the IP of another instance in the corresponding subnet.
- (Optional) Add any desired bypass rules in the Selective Bypass Configuration
- (Optional) Add one or more redirect rules in the Redirect Configuration (should only apply when using SNAT)
- Click the Verify Config button to check the values. Make adjustments if needed.
- Click the Save button to reboot and apply changes. Rebooting may take up to 3 minutes.

STEP 5

Verify routing

- Make sure that your VPC and subnet routes are set correctly and then you should be able to begin proxying traffic through *WarpVM*.

The screenshot shows the BADU management interface for a device named 'jet5-proxy'. The top navigation bar includes 'Status', 'Interfaces', 'System', 'Diagnostics', and 'Help'. The 'System' tab is active, and the 'Alarms' section is displayed. The Alarms table shows three successful system events:

| Device | AI ID (12) | Start | End | Msg |
|--------|------------|----------------------|----------------------|------------------|
| SYSTEM | 111 | 06:04:14 AM 09/27/16 | 06:04:14 AM 09/27/16 | START SUCCESSFUL |
| SYSTEM | 110 | 02:33:04 PM 09/24/16 | 02:33:04 PM 09/24/16 | START SUCCESSFUL |
| SYSTEM | 109 | 10:48:58 AM 09/05/16 | 10:48:58 AM 09/05/16 | START SUCCESSFUL |

Below the Alarms table, there are tabs for 'Proxy Information', 'Utilities', 'System Metrics', and 'Administration'. The 'Administration' tab is selected, showing 'Access Control' buttons: 'WarpAdmin Admin Password', 'Generate New SSH Key', and 'Cancel SSH Key'. There is also a 'Current Key Expiration' field. On the right, the 'Badu Networks Website' section contains buttons for 'License Request', 'Apply License', and 'Upload Firmware'. A 'Report Problems' section includes the email 'support@badunetworks.com' and a 'Generate SOS File' button. The footer shows the copyright notice: '© Copyright BADU Networks Inc; 2014-2016; All rights reserved'.