



DH2i DxEnterprise 21.0 Software: AWS Load Balancer Quick Start Guide

DH2i Company

Support: +1 (800) 380-5405 ext. 2

<https://dh2i.com/support/>

eFax: +1 970-295-4505

Email: support@dh2i.com

<https://www.dh2i.com>

AWS Load Balancer

This quick start guide describes how to set up and configure a load balancing solution for DxEnterprise running in AWS. Using this guide, the user will create virtual machines and a security group, configure applications, and create and configure an AWS load balancer that will allow access to the resources assigned to the DxEnterprise Vhost.

Prerequisites

- Access to Amazon Web Services (AWS) with permissions to launch instances, create and modify security groups, and create load balancers.

Create the Virtual Machine and Security Group

1. Login to the AWS Management Console.
2. Search for **EC2** under AWS Services > Find Services.
3. On the left of the window, select **Instances**.
4. Select **Launch Instance** at the top of the window.
5. Select **AWS Marketplace** on the left of the window.
6. Search for **DxEnterprise** using the search bar near the top of the window.
7. Select one of the DxEnterprise offerings listed in the results.
8. Create the VM.
 - a. Choose an instance type.
NOTE: SQL Server requires at least 2GB of free RAM.
 - b. Select **Next: Configure Instance Details** at the bottom right of the window.
 - c. Select a subnet for the VM. Note the selected subnet for later use.

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances: 1 Launch into Auto Scaling Group

Purchasing option: Request Spot instances

Network: vpc-c0c257b6 (default) Create new VPC

Subnet: subnet-009f65d3 (Default in us-west-2c) 4091 IP Addresses available Create new subnet

Auto-assign Public IP: Use subnet setting (Enable)

Placement group: Add instance to placement group

Capacity Reservation: Open Create new Capacity Reservation

IAM role: None Create new IAM role

Shutdown behavior: Stop

Stop - Hibernate behavior: Enable hibernation as an additional stop behavior

Enable termination protection: Protect against accidental termination

Monitoring: Enable CloudWatch detailed monitoring Additional charges apply

Tenancy: Shared - Run a shared hardware instance Additional charges may apply when launching Dedicated instances

Elastic Inference: Add an Elastic Inference accelerator Additional charges apply

T3/T3 Unlimited: Enable Additional charges may apply

File systems: Add file system Create new file system

Device	Network interface	Subnet	Primary IP	Secondary IP addresses	IPv6 IPs
eni0	New network interface	subnet-009f65d3	Auto-assign	Add IP	Add IP

Advanced Details

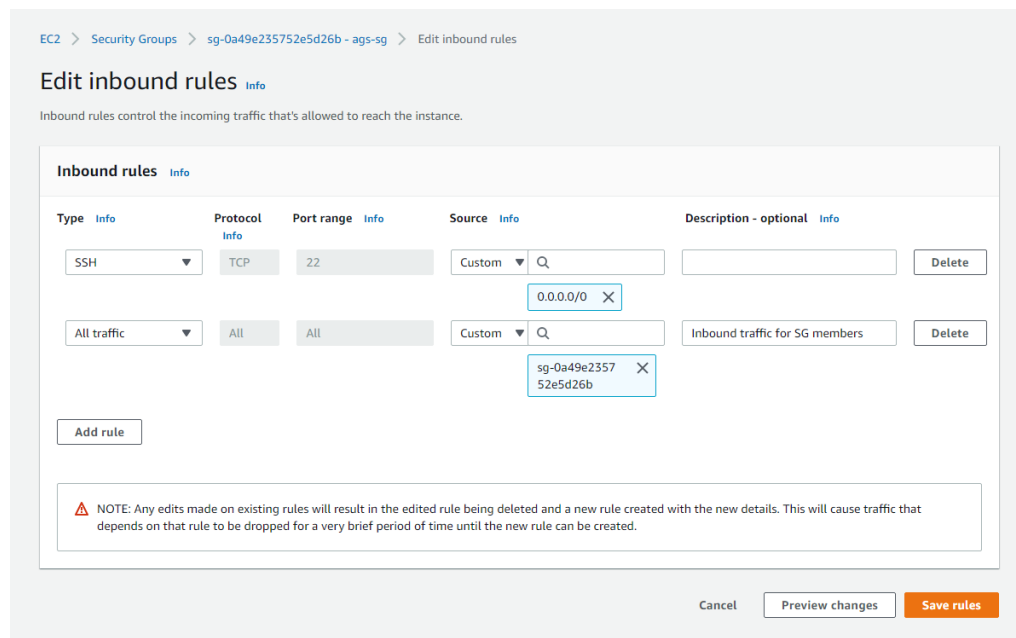
Metadata accessible: Enabled

Metadata version: /V1 and /V2 (token optional)

Buttons: Cancel Previous Review and Launch Next: Add Storage

- d. Select **6. Configure Security Group** from the options at the top of the window.
- e. Assign a name and description for the security group.
- f. If desired, modify the SSH rule to allow access from known IP addresses only.

- g. Select **Review and Launch** at the bottom-right of the window, then **Launch**.
 - h. Create a new key pair or select an existing key pair, then launch the instance.
9. Repeat steps 8a-c for additional VM(s). Assign the VMs to the same subnet from step 8c of the first VM.
- a. Select **6. Configure Security Group** from the options at the top of the window and assign the VM to the existing security group configured during the setup of the first VM.
 - b. Select **Review and Launch** at the bottom-right of the window, then **Launch**.
 - c. Create a new key pair or select an existing key pair, then launch the instance.
10. The EC2 instances have been created and are initializing. Return to the EC2 landing page by clicking the AWS icon in the top-left corner and searching for **EC2** under AWS Services > Find Services.
11. Edit the security group.
- a. Select **Security Groups** under Network & Security.
 - b. Select the security group from the list, then select **Edit inbound rules**.
 - c. Add a rule to allow all inbound traffic originating from members of the security group and save the rule.



12. Return to the AWS Console by selecting the AWS icon in the top-left corner.

Configure DxEnterprise and Applications

1. The application must be installed and DxEnterprise configured before continuing. DH2i provides quick start guides for some applications – such as Microsoft SQL Server – running on physical or virtual machines; hyperlinks for these guides are provided below. Various other DxEnterprise configurations may take advantage of the AWS Load Balancer. After configuring the application, leave the console or DxAdmin window open for the second step.
 - [SQL Server Availability Groups with DxCLI Quick Start Guide](#)
 - [SQL Server Availability Groups with DxAdmin Quick Start Guide](#)

- [SQL Server High Availability Instances on Linux Quick Start Guide](#)
2. After configuring DxEnterprise and your application on the VM, add a probe port to the Vhost using DxCli or DxAdmin.
 - For DxAdmin:
 - i. Right-click on the Vhost and select **Update virtual host**.
 - ii. Select the pencil icon to the right of the Probe Port field, then enter a port number into the field. More than one probe port may be added to the Vhost by separating the ports with a comma.
 - iii. Note the Vhost IP and probe port for later use. Save the changes by selecting **OK** at the bottom of the window.
 - For DxCli:
 - i. Run the command `sudo dxcli set-vhost-ilbports` to add a load balancer port to the Vhost.

Syntax

```
dxcli set-vhost-ilbports <vhost> <ilb_ports>
```

Parameters

Name	Description	Required
vhost	The name of the Vhost.	True
ilb_ports	List of ports to use for internal load balancer probing (Comma-separated list for multiples).	True

Example

```
sudo dxcli set-vhost-ilbports VHOST1 50000
```

- ii. Run the command `sudo dxcli get-vhost` to gather the Vhost IP address and verify the load balancer port is correct. Save these two items for later use.

Syntax

```
dxcli get-vhost <vhost>
```

Parameters

Name	Description	Required
vhost	The name of the Vhost.	True

Example

```
sudo dxcli get-vhost VHOST1
```

3. After adding the probe port to the Vhost, return to the AWS Management Console for the next section.

Create and Configure the AWS Load Balancer

1. Search for **EC2** under AWS Services > Find Services.
2. Edit the security group.
 - a) Select **Security Groups** under Network & Security.

- b) Select the security group from the list, then select **Edit inbound rules**.
- c) Add the following rules:
 - Allow traffic on the application listener port from all VMs in the Vhost using their IP addresses. To find a VMs IP address, select **Instances** from the left panel and select one of the instances that belong to the Vhost. The IP address will be listed under Private IPs.
 - Allow traffic on the Vhost probe port from the subnet the VMs belong to. To find the correct CIDR for the subnet, select **Instances** from the left panel, select one of the instances that belong to the Vhost, then select the **Subnet ID** in the information pane. The CIDR for the subnet will be listed in the subnet information pane.

The screenshot shows the AWS Management Console interface. On the left is a navigation menu with categories like EC2 Dashboard, INSTANCES, IMAGES, ELASTIC BLOCK STORE, and NETWORK & SECURITY. The main content area displays the details for a security group named 'ags-sg' with ID 'sg-0a49e235752e5d26b'. A green notification banner at the top indicates that inbound security group rules were successfully modified. Below the details, there are tabs for 'Inbound rules', 'Outbound rules', and 'Tags'. The 'Inbound rules' tab is active, showing a table with the following data:

Type	Protocol	Port range	Source	Description - optional
All traffic	All	All	sg-0a49e235752e5d26b (ags-sg)	Inbound traffic for SG members
SSH	TCP	22	0.0.0.0/0	-
Custom TCP	TCP	50000	172.31.15.81/32	dxe1
Custom TCP	TCP	50000	172.31.4.2/32	dxe2
Custom TCP	TCP	50000	172.31.0.0/20	Subnet

3. Under Load Balancing, select **Load Balancers**.
4. Create a load balancer and register the target(s).
 - a) At the top-left of the window, select **Create Load Balancer**.
 - b) Select **Create** under Network Load Balancer.
 - c) Under basic configuration, assign the load balancer a name and change the scheme to **internal**.
 - d) Under Listeners, change the Load Balancer Port to the Vhost probe port.
 - e) Under Availability Zones, select the availability zone and subnet the VMs belong to.

1. Configure Load Balancer 2. Configure Security Settings 3. Configure Routing 4. Register Targets 5. Review

Step 1: Configure Load Balancer

Basic Configuration

To configure your load balancer, provide a name, select a scheme, specify one or more listeners, and select a network. The default configuration is an Internet-facing load balancer in the selected network with a listener that receives TCP traffic on port 80.

Name

Scheme internet-facing internal

Listeners

A listener is a process that checks for connection requests, using the protocol and port that you configured.

Load Balancer Protocol	Load Balancer Port
TCP	50000

Add listener

Availability Zones

Specify the Availability Zones to enable for your load balancer. The load balancer routes traffic to the targets in these Availability Zones only. You can specify only one subnet per Availability Zone. You may also add one Elastic IP per Availability Zone if you wish to have specific addresses for your load balancer.

VPC

Availability Zones

- us-west-2a subnet-aa6087d2
- us-west-2b subnet-97c6c6dc
- us-west-2c subnet-009f5e5d
 - IPv4 address** Assigned from CIDR 172.31.0.0/20
 - Private IPv4 address** Assigned from CIDR 172.31.0.0/20
- us-west-2d subnet-07aec72c

f) Select **Next: Configure Security Settings**, then **Next: Configure Routing**.

g) Under **Target Group**, assign a name and set the port to Vhost probe port.

1. Configure Load Balancer 2. Configure Security Settings 3. Configure Routing 4. Register Targets 5. Review

Step 3: Configure Routing

Your load balancer routes requests to the targets in this target group using the protocol and port that you specify, and performs health checks on the targets using these health check settings. Note that each target group can be associated with only one load balancer.

Target group

Target group

Name

Target type Instance IP

Protocol

Port

Health checks

Protocol

▼ **Advanced health check settings**

Port traffic port override

Healthy threshold

Unhealthy threshold

Timeout seconds

Interval 10 seconds 30 seconds

h) Select **Next: Register Targets**.

i) Under **Instances**, select the instances that belong to the Vhost and select **Add to registered**. More information on registering targets can be found in the references section at the end of this document.

Step 4: Register Targets

Configure Security Groups

The security groups for your instances must allow traffic from the VPC CIDR on the health check port.

Register targets with your target group. If you register a target in an enabled Availability Zone, the load balancer starts routing requests to the targets as soon as the registration process completes and the target passes the initial health checks.

Registered targets

To deregister instances, select one or more registered instances and then click Remove.

Remove

<input type="checkbox"/>	Instance	Name	Port	State	Security groups	Zone
<input type="checkbox"/>	i-0229a3c2170d7b476	dx1	50000	● running	ags-sg	us-west-2c
<input type="checkbox"/>	i-02d15766d7057a52	dx2	50000	● running	ags-sg	us-west-2c

Instances

To register additional instances, select one or more running instances, specify a port, and then click Add. The default port is the port specified for the target group. If the instance is already registered on the specified port, you must specify a different port.

Add to registered on port 50000

Search Instances

<input type="checkbox"/>	Instance	Name	State	Security groups	Zone	Subnet ID	Subnet CIDR
<input checked="" type="checkbox"/>	i-0229a3c2170d7...	dx1	● running	ags-sg	us-west-2c	subnet-009f6e5d	172.31.0.0/20
<input checked="" type="checkbox"/>	i-02d15766d705...	dx2	● running	ags-sg	us-west-2c	subnet-009f6e5d	172.31.0.0/20

- j) Select **Next: Review**, then **Create**.
5. AWS will begin provisioning the load balancer and registering the targets. To view the status of the targets, select Load Balancing > Target Groups, then select the **Targets** tab in the information pane.

References

- [DxEnterprise DxCli Guide](#)
- [DxEnterprise Admin Guide](#)
- [Amazon – Register Targets with Your Target Group on AWS](#)
- [Amazon – What is a Network Load Balancer?](#)