SECURE AND SCALABLE MAGENTO HOSTING ON AMAZON WEB SERVICES

White Paper

https://stackBuilder.stackArmor.com
solutions@stackarmor.com

stackArmor

Build your stack in minutes. We will armor it for you.

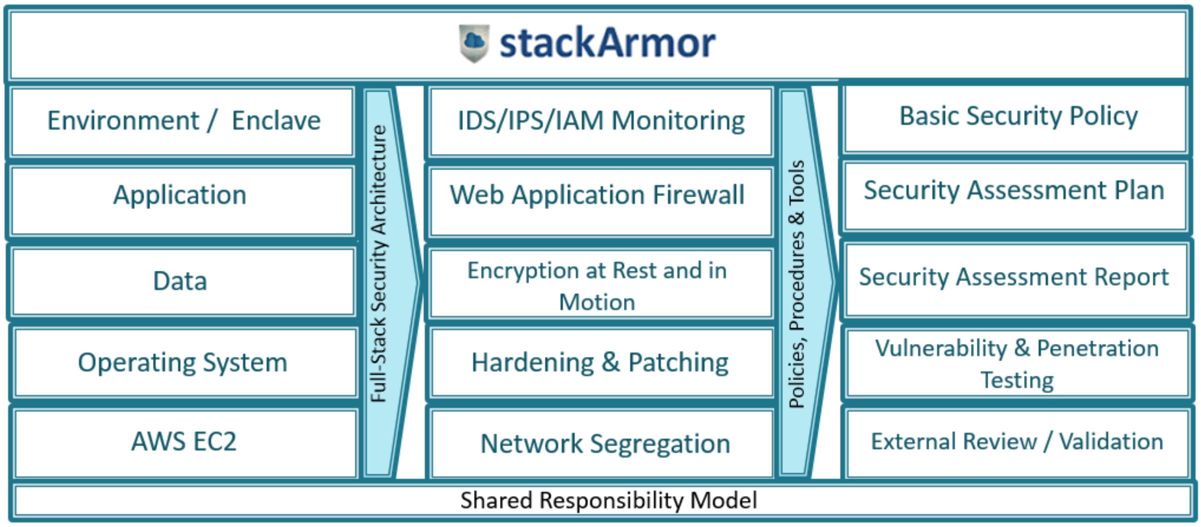
Contents

Abstract

Secured hosting and maintenance of e-commerce websites has become the need of the hour. Modern day websites are highly vulnerable to threats such as hacking, phishing, pharming, denial of access etc. Magento is considered to be one of the most secured e-commerce platform that is easy to install and ready to use. The inbuilt security features of Magento and the additional benefits of AWS makes it the safest and secured platform for modern applications.

Secure and Scalable Magento Hosting

Magento is an open source cloud based digital commerce platform that empowers merchants to integrate digital and physical shopping experiences. Magento enterprise edition provides an engaging shopping experience to the users by providing personalized content, fast checkout and a seamless shopper experience. However, in order to ensure the integrity of the user experience and sensitive customer data, it is important to follow security and deployment best practices. stackArmor's cybersecurity and cloud deployment experts have developed a proven and full-stack methodology to help protect and secure applications and data. The diagram below provides an overview of the key layers and security countermeasures.



stackArmor

Environment / Enclave
Application
Data
Operating System
AWS EC2

Full-Stack Security Architecture

IDS/IPS/IAM Monitoring
Web Application Firewall
Encryption at Rest and in Motion
Hardening & Patching
Network Segregation

Policies, Procedures & Tools

Basic Security Policy
Security Assessment Plan
Security Assessment Report
Vulnerability & Penetration Testing
External Review / Validation

Shared Responsibility Model

Additionally, it is important to follow Magento specific guidelines for creating a secure eCommerce platform that is compliant and protected.

1. Keep Magento and Extensions Up to Date: It is very important that you are always running the latest version of Magento as updates generally contain security fixes. It is also very important to keep your Magento extensions up to date.

2. Strong Usernames and Passwords: Commonly mistakes in selecting usernames and passwords is to use easy to guess patterns like using “admin” as your username. Always use non-obvious usernames and strong passwords.

3. Two-Factor Authentication: Given the number of breaches that occur due to weak passwords, installing a 2-factor authentication mechanism that uses a cellphone or email as an additional verification service for executing important user functions.

4. Block Bad Bots: There are always bad bots, scrapers, and crawlers hitting your Magento sites and stealing your bandwidth. You can see a comprehensive list of bots at botreports.com. Many of the security extensions mentioned above can work great to block bad bots, but sometimes you might need to do this at the server level. If you wanted to block multiple User-Agent strings at once, you could add the following to your .htaccess file.

```
RewriteEngine On

RewriteCond %{HTTP_USER_AGENT} ^.*(agent1|Wget|Catall Spider).*$ [NC]

RewriteRule .* - [F,L]
```

Or you can also use the BrowserMatchNoCase directive like this:

```
BrowserMatchNoCase "agent1" bots

BrowserMatchNoCase "Wget" bots

BrowserMatchNoCase "Catall Spider" bots
```

5. File Permissions: To protect your Magneto shop you want to make sure and use the correct file permissions. Each directory and file has different permissions which allow people to read, write and modify them. If your permissions are too loose this could open up a door for an intruder and if they are too restrictive this could break your Magento install as extensions and the Magento installation need to be able to write to certain directories. Magento has some great documentation on setting privileges and ownership after you install Magento. For example, lock Down local.xml File. It is also important to note that the local.xml file, located in app/etc/local.xml holds all of your database connection and should be configured with restricted access with file’s permissions to 600, or (-rw-------). These permissions restrict read-and-write access to your user alone.magento local xml file

6. Custom Path for Administrator Login: Changing the default admin and login pages can help deflect common attacks. To change the admin path in Magento, go to the app/etc/local.xml file, find the line with this code: <![CDATA[admin]]>, and change the string admin to the required admin string. For example, if you want to change the admin panel URL to https://your -magento-

site.com/backdoor, change the CDATA code to <![CDATA[backdoor]]> . You might also want to change the path for Magento Connect Manager, as this is another entry point for hackers.

7. Restrict Admin Access by IP Address: You can also restrict access to your admin area by IP address by using the following in your .htaccess file.

8. Hardened Hosting Enclave: Installing adequate network level protection using a Firewall is critical including Intrusion Prevention and Detection (IPS/IDS) & Web Application Firewall (WAF).

9. Enforcing Operational Hygiene: Applying continuous monitoring and logging of critical security events such as failed login attempts, patching the operating system, data and application servers as well as ensuring adequate level of backups of critical data are common activities.

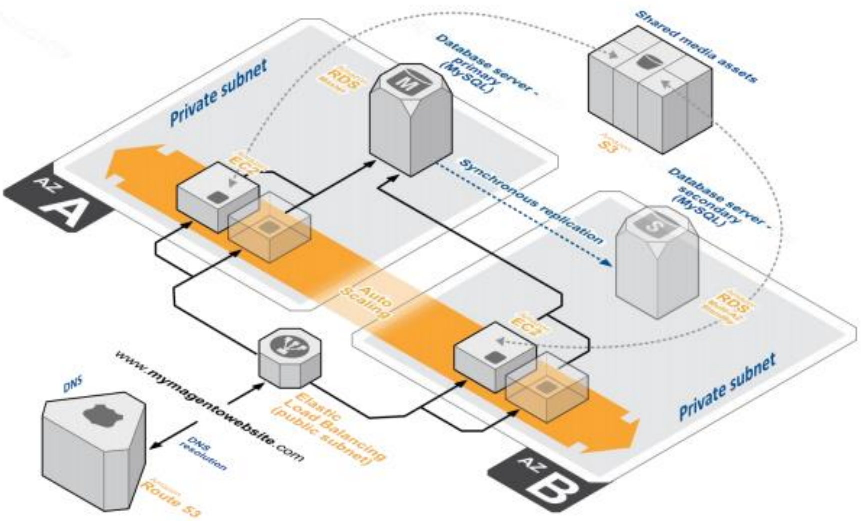
Configuring Amazon Web Services (AWS)

Amazon Web Services (AWS) provides the necessary infrastructure support for a secured deployment of Magento E-commerce platform. The process of deployment is highly scalable, cost effective and highly flexible. The AWS infrastructure takes up the responsibility of the operational security of the system, the user takes up the responsibility of the guest operating system.

The following steps should be executed to ensure a well architected solution.

1. An Amazon VPC with three subnets in multiple availability zones
2. A network translation instance deployed in the public subnets and configured with an Elastic IP address for out bound internet connectivity and inbound SSH access
3. A MySQL database engine deployed via Amazon RDS
4. Elastic Load balancing to distribute traffic across multiple web server instances
5. Amazon EC2 web server instances launched in the private subnet
6. Auto scaling to automatically increase the capacity if there is a sudden increase in the demand.
7. AWS Identity and Access Management (IAM) instance role that define access to AWS web services
8. Security Groups to restrict access to the various protocols and ports

The diagram below provides an overview of the hosting configuration using multiple availability zones and micro-segments using private and public subnets.



The above illustration shows a typical Magento architecture on AWS

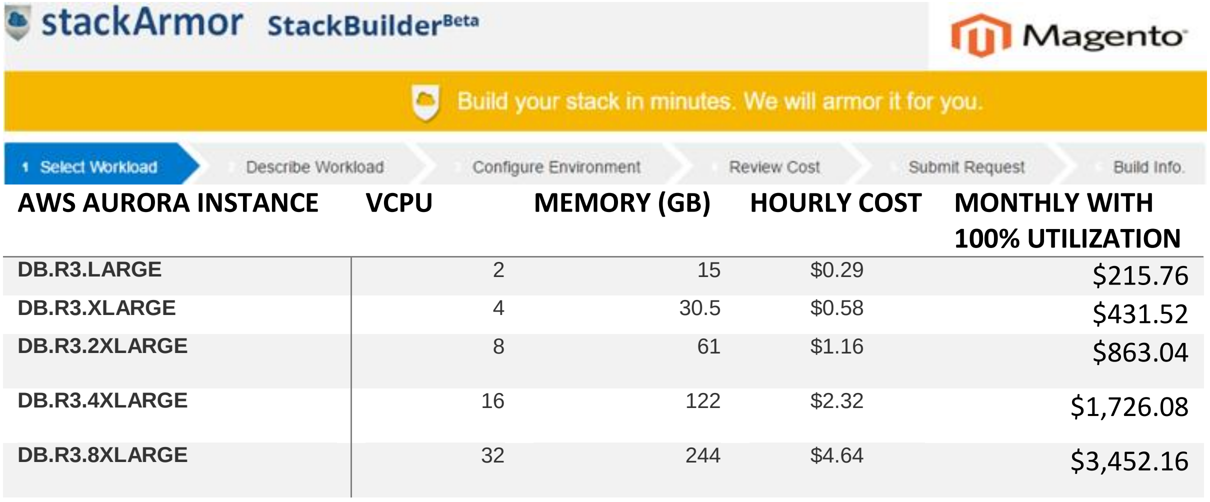
Turbo-charging Magento with AWS Aurora

Amazon Aurora is a MySQL-compatible relational database engine that combines the speed and availability of high-end commercial databases with the simplicity and cost-effectiveness of open source databases. Amazon Aurora provides up to five times better performance than MySQL with the security, availability, and reliability of a commercial database. AWS Aurora provides a high-performance database engine for Magento with a significant performance boost and reduced total cost of operations for large systems. Key highlights of AWS Aurora for Magento deployments include:

- MySQL 5.6 compatible
- 5X throughput of MySQL 5.6
- Single digit milliseconds replica lag time
- No modifications required to MySQL apps
- Hot failover for up to 15 read replicas
- Self-healing and fault tolerant storage
- DB storage auto scales to up to 64TB
- Easy to provision via AWS console

AWS Aurora offers 2 times the throughput of MySQL per node in real-world tests published by Magento with 20 rps (MySQL) vs. 40 rps (Aurora). The Replica lag on Aurora is critically lower vs. Master-to-Slave MySQL configuration with AWS Aurora < 40-100ms vs. MySQL > 500ms.

AWS Aurora pricing options are provided below for US East On-Demand rates. Associated storage is charged at $0.10 per GB and other charges per request apply.



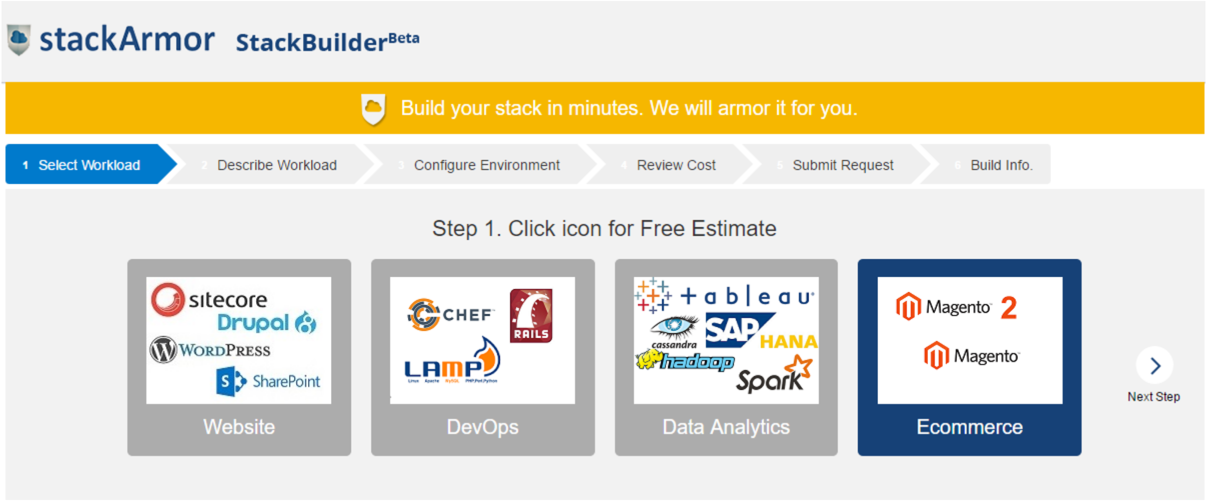
AWS AURORA INSTANCE	VCPU	MEMORY (GB)	HOURLY COST	MONTHLY WITH 100% UTILIZATION
DB.R3.LARGE	2	15	$0.29	$215.76
DB.R3.XLARGE	4	30.5	$0.58	$431.52
DB.R3.2XLARGE	8	61	$1.16	$863.04
DB.R3.4XLARGE	16	122	$2.32	$1,726.08
DB.R3.8XLARGE	32	244	$4.64	$3,452.16

Fully Managed and Secure Magento Hosting on AWS.

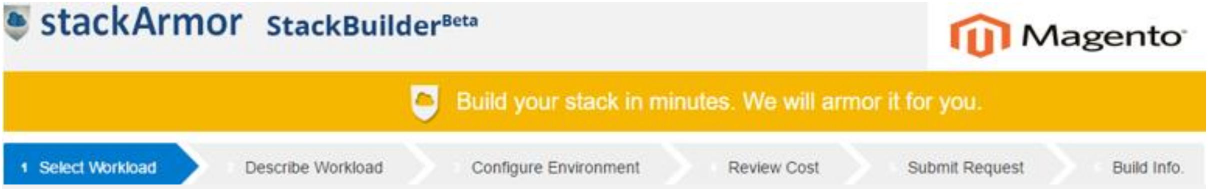
AWS offers a wide variety of configuration and deployment choices requiring infrastructure, systems engineering and AWS engineering expertise. The cloud experts at stackArmor, have developed an easy to use deployment automation harness called StackBuilder^{TM}. StackBuilder^{TM} allows users to quickly deploy and use their Magento e-commerce website hosted on AWS. StackBuilder's intelligent cloud deployment engine takes care of instance selection, AWS VPC configuration and software installation. The fully managed Magento service includes patching, vulnerability management, continuous monitoring, data encryption, and recovery & backup support.

In order to get started with Magento e-commerce website on AWS application go to https://stackbuilder.stackarmor.com

Step 1: Select E-commerce as the workload profile and click Next



Step 2: Describe the workload environment in terms of size, security by industry and management model

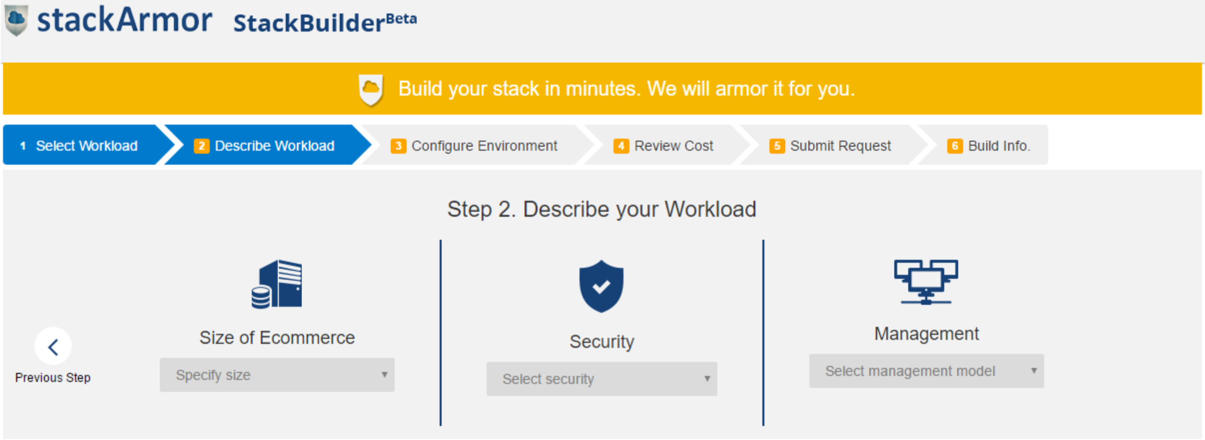


stackArmor StackBuilderBeta

Magento

Build your stack in minutes. We will armor it for you.

1 Select Workload | Describe Workload | Configure Environment | Review Cost | Submit Request | Build Info.



stackArmor StackBuilderBeta

Build your stack in minutes. We will armor it for you.

1 Select Workload | 2 Describe Workload | 3 Configure Environment | 4 Review Cost | 5 Submit Request | 6 Build Info.

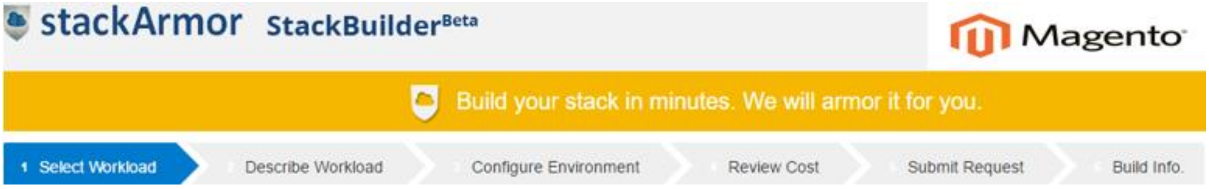
Step 2. Describe your Workload

Previous Step

Size of Ecommerce: Specify size ▾

Security: Select security ▾

Management: Select management model ▾



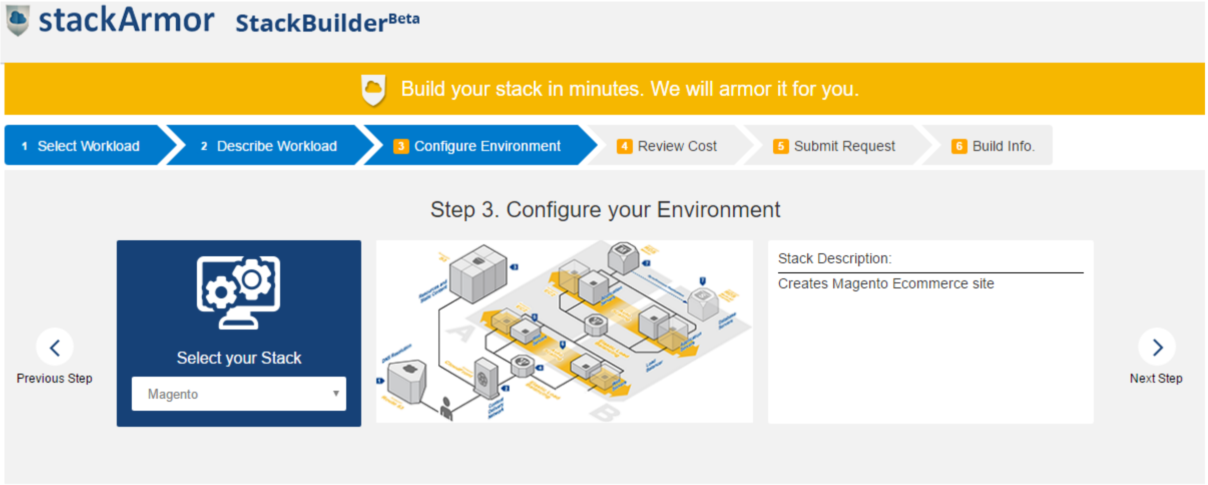
stackArmor StackBuilder^Beta

Magento

Build your stack in minutes. We will armor it for you.

1 Select Workload | Describe Workload | Configure Environment | Review Cost | Submit Request | Build Info.

Step 3: Configure environment by selecting stack – Magento or Magento 2



stackArmor StackBuilder^Beta

Build your stack in minutes. We will armor it for you.

1 Select Workload | 2 Describe Workload | 3 Configure Environment | 4 Review Cost | 5 Submit Request | 6 Build Info.

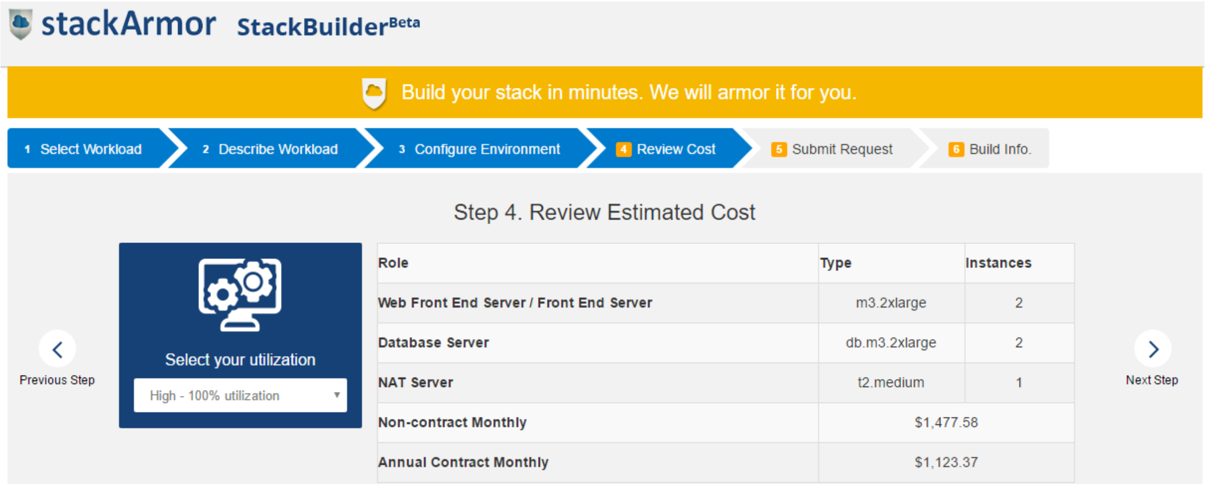
Step 3. Configure your Environment

Select your Stack: Magento

Stack Description:
Creates Magento Ecommerce site

Previous Step | Next Step

Step 4: Review Hosting Cost inclusive of software and maintenance fees



stackArmor StackBuilder^Beta

Build your stack in minutes. We will armor it for you.

1 Select Workload | 2 Describe Workload | 3 Configure Environment | 4 Review Cost | 5 Submit Request | 6 Build Info.

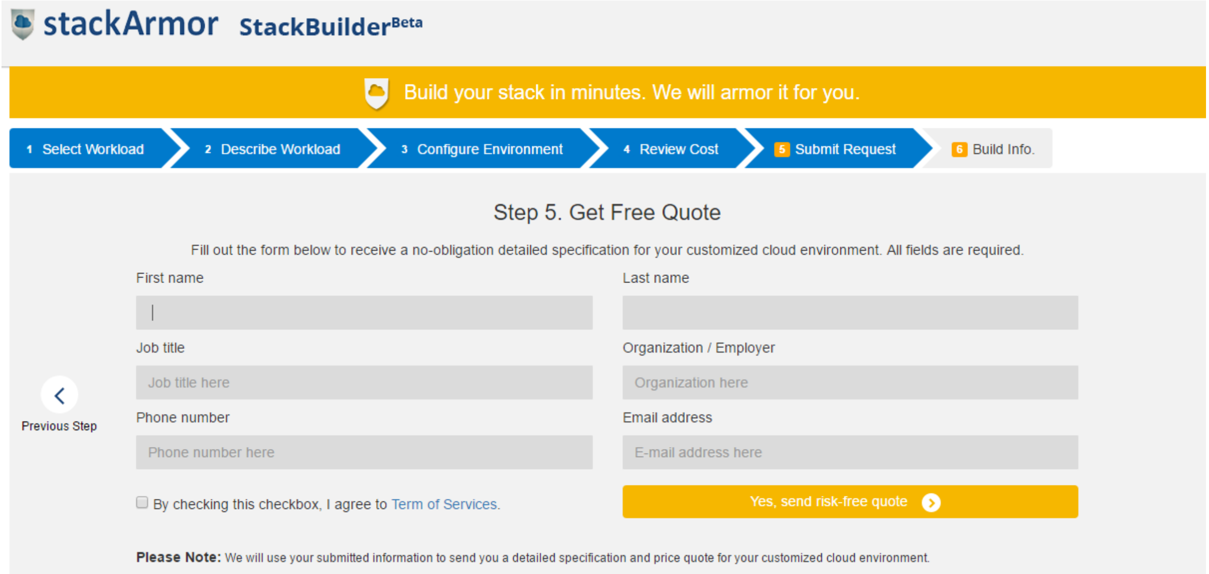
Step 4. Review Estimated Cost

Select your utilization: High - 100% utilization

Role	Type	Instances
Web Front End Server / Front End Server	m3.2xlarge	2
Database Server	db.m3.2xlarge	2
NAT Server	t2.medium	1
Non-contract Monthly	$1,477.58	
Annual Contract Monthly	$1,123.37	

Previous Step | Next Step

Step 5: Fill out form and submit request to provision environment. Once, the environment has been provisioned you will get an email with the access URL and a User Name & Password.



Step 5. Get Free Quote

Fill out the form below to receive a no-obligation detailed specification for your customized cloud environment. All fields are required.

First name

Last name

Job title: Job title here

Organization / Employer: Organization here

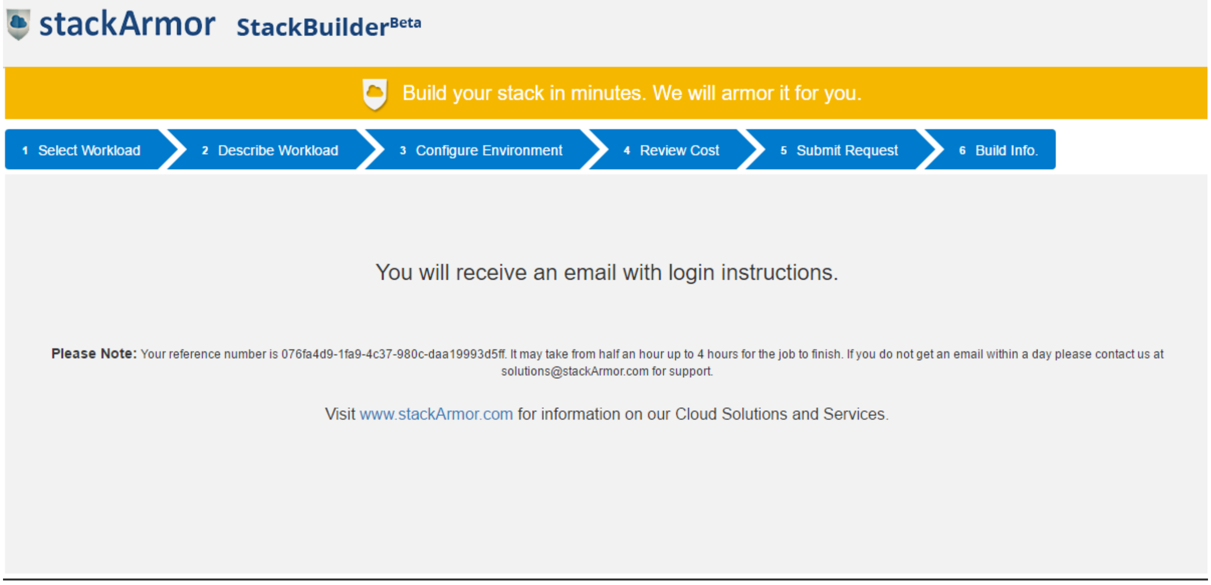
Phone number: Phone number here

Email address: E-mail address here

□ By checking this checkbox, I agree to Term of Services.

Please Note: We will use your submitted information to send you a detailed specification and price quote for your customized cloud environment.

Step 6: Login into the Magento e-commerce application



You will receive an email with login instructions.

Please Note: Your reference number is 076fa4d9-1fa9-4c37-980c-daa19993d5ff. It may take from half an hour up to 4 hours for the job to finish. If you do not get an email within a day please contact us at solutions@stackArmor.com for support.

Visit www.stackArmor.com for information on our Cloud Solutions and Services.

Step 7: Select appropriate dashboard and begin using the application

You will receive a call confirming your subscription and verifying your requirements and an email with your customized environment will sent to you.

StackBuilder, a turbo-tax like Wizard for AWS

StackBuilder^{TM} is a “Turbo Tax” like wizard for helping application owners quickly configure a fully functional AWS environment. The wizard walks the user through a series of simple questions through a 5 step process. Upon submission of the request, the user is presented with login credentials to a fully configured and operational environment ready to go.

StackBuilderTM has been designed and developed by cloud computing experts who have spent many years implementing secure cloud hosting environments for large security focused organizations such as the US Treasury, Defence, Healthcare, Commercial and Non-profit customers. StackBuilderTM automates the entire provisioning process using an advanced capacity planning and provisioning automation engine that makes it easy for users to leverage the power of the AWS cloud computing platform without having to get into the details of infrastructure estimation, provisioning and software media installation & configuration.

StackBuilderTM provides a rich and easy to use consumer-grade experience for non-technical users to jumpstart their projects by answering a series of simple questions. StackBuilder's intelligent provisioning and capacity estimation engine leverages the rich set of services provided by the AWS cloud platform including wide variety of EC2 instances, Virtual Private Cloud (VPC), Auto Scaling Groups, Clustering and Elastic Load Balancers (ELB) amongst others. The user of StackBuilderTM does not have to go through the various steps associated with configuring and setting up the AWS infrastructure as they are handled automatically. This allows the user to focus on his project without waiting for costly consultants or the need for cloud infrastructure expertise.

References

1. Magento and its security features
   https://magento.com/products/enterprise-edition
2. Magento on AWS cloud
   http://docs.aws.amazon.com/quickstart/latest/magento/welcome.html
3. Magento architecture
   http://docs.aws.amazon.com/quickstart/latest/magento/architecture.html