CHARM Network Security Architecture

Contents

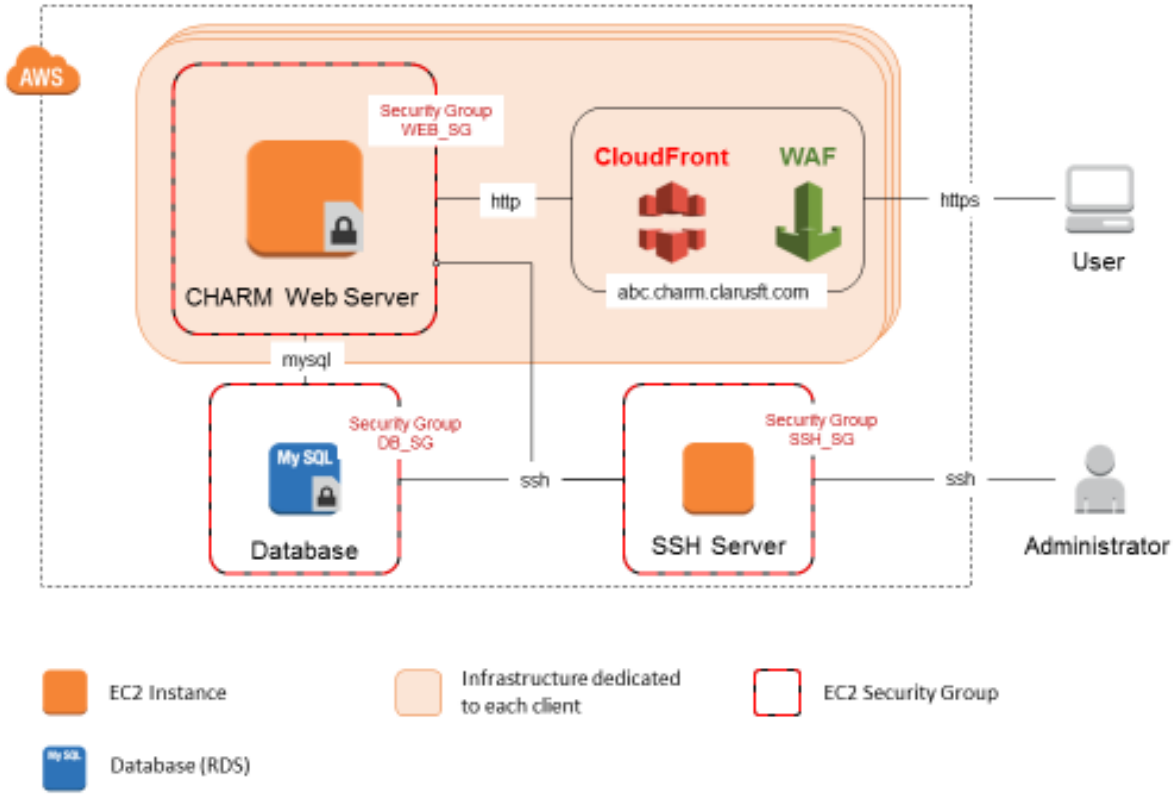
Introduction

- CHARM is hosted on Amazon Web Services (AWS) Elastic Compute Cloud (EC2). It can be accessed via a web GUI or a REST API.
- Each Customer has access to a dedicated server (EC2 instance) running CHARM
- A database hosted on Amazon Relational Database Service (RDS) is used to store market data and CHARM configuration data. This database is shared between CHARM servers and is for data that is common to all customers (e.g. market data). There is no private customer data in this database.
- This document sets out controls that shall be in place to minimise the risk of the CHARM application or confidential data being compromised by unauthorized network access

Scope

This policy applies to all CHARM application and database servers deployed on Amazon EC2, including all development, testing and demo/evaluation servers as well as production servers.

Architecture Overview



Implementation Details

Use a Dedicated EC2 instance per client

Each Clarus customer will be provided with a dedicated EC2 instance running CHARM, configured to only accept logins from user accounts belonging to that organisation.

Use a Dedicated SSH Server for Admin Access

Direct SSH access from the Internet is permitted only to a single specific bastion host (SSH Server), and only from a set of known IP addresses (e.g. Clarus offices). Connections to other servers may be tunnelled through the SSH Server. See below for details of how EC2 Security Groups are configured to achieve this objective.

Where a user wishes to connect from outside the pre-approved IP ranges (for example when they are remote working) they must make a request to a Network Administrator who may grant access on a temporary basis. These temporary grants must be regularly reviewed by Network Administrators and removed when no longer required.

Login to the SSH server must use SSH keys (no password-based logins allowed). The SSH keys must be protected by strong passwords and only designated Clarus administrators have access to them.

The ssh server will log all commands issued through. These logs will be persisted on a secure Amazon S3 bucket and accessible to designated Clarus admins.

The SSH Server should not run any unnecessary services and should have the latest security patches applied at all times.

Use Amazon CloudFront to provide access to CHARM Web Servers

Amazon CloudFront is used to provide access to CHARM Web Servers instead of exposing these to the public Internet directly. A dedicated CloudFront distribution with a specific DNS name (e.g. abc.charm.clarusft.com) will be configured for each Clarus customer.

All CloudFront Distributions are configured to only accept HTTPS connections (or to redirect HTTP to HTTPS) in order to encrypt data in transit.

AWS Web Application Firewall (WAF) rules are used to filter out common attacks such as SQL injection and cross-site scripting. NB: this is in addition to, and not a replacement for, correct programming practices to defend against such attacks.

Optionally, WAF can be configured to accept connections only from known set of IP addresses (where customers have provided this information to Clarus).

Use EC2 Security Groups to restrict access by protocol and IP

EC2 Security Groups are configured in order to limit exposure of EC2 and RDS servers to the public Internet as much as possible.

SSH Server Security Group (SSH_SG)

The SSH Server is the only EC2 instance that is directly exposed to the public Internet.

Source	Protocol	Comments
Known Clarusft IP addresses	SSH	Allow SSH access to Clarusft Admins

Web Server Security Group (WEB_SG)

Web servers should accept incoming connections from the SSH server and CloudFront servers only. This ensures that they are not directly exposed to the public internet, and also segregated from any other EC2 instances on the network.

Source	Protocol	Comments
SSH_SG Security Group	SSH	Allow SSH access to Clarusft Admins
CloudFront Servers	HTTP, HTTPS	Allow access to CloudFront CDN

Database Security Group (DB_SG)

Source	Protocol	Comments
SSH_SG Security Group	MySQL	Allow MySQL access to Clarusft Admins
WEB_SG Security Group	MySQL	Allow MySQL access to Web Server