CHARM Access Control Policy

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 measures that shall be in place to control access to CHARM application servers and related systems, such as database servers. The goal is to ensure that only those employees who have a business need to have access to these systems are permitted to do so, and that such employees are assigned the least level of access privileges that allows them to carry out their duties.

Prerequisites

This document assumes the reader has already familiar with the document “CHARM Network Security Architecture”; several concepts discussed in that document are referred to here without further explanation.

Scope

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

Policy

Resources Subject to Control

The following resources will be subject to access control.

- CHARM Application Servers (AWS EC2)
- CHARM Database Servers (AWS RDS)
- Network Infrastructure (AWS VPC, CloudFront, WAF, SSH Bastion Host)
- CHARM Information Assets

Application and Database Servers will be categorized as Production, Development, or Sales depending on whether they are used by Clarus customers, developers/testers, or the sales team respectively.

Ownership of Resources

Management shall ensure each resource or category of resource has an Owner assigned. The Owner of each resource will be responsible for the determining the level of protection and controls the resource requires, and the application of access control policies to that resource. Note that the owner is not necessarily the same as the resource administrator, who is the individual responsible for the implementation of policies to the resources under their care at the direction of the resource owner.

Roles

Employees can be assigned to one or more of the following roles depending on their responsibilities and access requirements. An employee may be assigned more than one role as long as management is satisfied that the potential for conflict of interest or improper activities is sufficiently low.

- AWS Administrator

  Includes the AWS root account holder and other designated individuals. Has overall control of AWS resources, including provisioning user accounts (AWS IAM accounts) for other employees.
- Systems Administrator

  Manages CHARM application servers (AWS EC2 instances), including provisioning of Linux logins for other users
- Database Administrator

  Manages CHARM database servers (AWS RDS instances), including provisioning database logins for other users
- Network Administrator

  Manages AWS networking and network security configuration, including bastion hosts.

- Developer
- Tester
- Sales
- Support

Access Controls

The following summarizes the level of access privileges that would be appropriate for individuals with a particular role. Note that this is a guide only; it is the responsibility of the resource owner to determine the suitable level of access control required for resources under their care.

Application Servers

	System Admin	Developer/Tester	Sales	Support
Application Server - Production				
Create	Yes			
Control (Start/Stop)	Yes			Yes
Control (Destroy)	Yes			
Configure	Yes			
Shell access	Yes			Limited[1]
Monitor	Yes			Yes
Application Server - Development				
Control (Start/Stop)	Yes	Yes		
Control (Destroy)	Yes			
Configure	Yes	Yes		
Shell access	Yes	Limited[1]		
Monitor	Yes	Yes		
Application Server - Sales				
Control (Start/Stop)	Yes		Yes	Yes
Control (Destroy)	Yes			
Configure	Yes			
Shell access	Yes		Limited[1]	Limited[1]
Monitor	Yes		Yes	Yes

Notes:

1. Limited shell access means access to a non-administrative account (no SUDO) which permits a limited set of operations related to CHARM, such as monitoring log files, modifying CHARM configuration files, and starting/stopping CHARM services. The user will not be permitted to make alterations to system settings or install new software. In addition if the system has access to restricted Information Assets, access to those assets must not be granted automatically unless explicitly authorized by the asset owner; see section on Information Assets below

Database Servers

	DBA	Developer	Support
Database Server - Production			
Create	Yes		
Control (Destroy)	Yes		
Configure	Yes		
Write (DML)	Yes		Limited[1]
Write (DDL)	Yes		
Read	Yes		Limited[1]
Monitor	Yes		Yes
Database Server - Development			
Create	Yes		
Control (Destroy)	Yes		
Configure	Yes	Yes	
Write (DML)	Yes	Yes	
Write (DDL)	Yes	Yes	
Read	Yes	Yes	
Monitor	Yes	Yes	
Database Server - Sales			
Create	Yes		
Control (Destroy)	Yes		
Configure	Yes		
Write (DML)	Yes		Limited[1]
Write (DDL)	Yes		
Read	Yes		Limited[1]
Monitor	Yes		Yes

Notes:

1. Limited read/write access granted to a limited set of tables that may aid in the diagnosis of problems or allow certain settings to be modified. Further controls will apply for tables containing data with a restrictive information classification; see section on Information Assets below

Network Infrastructure

No user apart from Network Administrators may be granted control of any aspect of the network infrastructure, including security/firewall settings and administrator access to the SSH Bastion Host.

Information Assets

Information Assets that are classified according to the Information Classification Policy will be subject to access controls. The Owner of Information Assets will be responsible for establishing what access controls shall apply with respect to both individuals and systems that require access to said asset. For instance, any data classified as “Private - Client Confidential” should only be accessible to systems provisioned for the client to whom that data belongs.

Refer to the Information Classification Policy document for further details.

Authentication and Account Management

Depending on assigned roles one or more of the following types of accounts may be created for an individual employee:

- AWS IAM Account
- Non-privileged Linux login for Application Servers
- Privileged Linux login for Application Servers
- Non-privileged MySql Database login
- Privileged MySql database login
- Logins for Information Asset Repositories (document storage, source code, etc)

Password policy for AWS IAM accounts must be configured to be sufficiently strong. At a minimum 8 characters including one numeric character will be required.

AWS Administrators are required to enable two-factor authentication (2FA) for their accounts. 2FA is also recommended but not mandatory for other AWS accounts.

Database and Information Asset repository login passwords should follow a similar policy to AWS IAM passwords.

Linux logins must always use public key authentication and never password based authentication. Users are required to protect their private keys with strong passwords.

Remote Access

Access to the AWS Console will generally be granted from remote IP addresses without restriction. However certain operations, such as terminating EC2 or RDS instances, may require the user to log in using 2FA.

Shell access to EC2 instances and access to RDS database instances must be made through the SSH Bastion Host, which will only permit connections from pre-defined IP ranges. The only IP ranges that are permanently granted access will be those for Clarus offices. Any user wishing to access these resources from outside these IP ranges 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.

Responsibilities

Where an employee requires access to one or more controlled resources, his or her manager shall communicate this requirement, along with the roles the employee should be assigned, to the Information Security Officer. Similarly any changes to existing permissions, including cases where access must be revoked due to an employee changing roles or leaving the company, must be communicated by the manager to the Information Security Officer.

The Information Security Officer will co-ordinate with the relevant resource owners and administrators in order to create any required account(s) and assign permissions to those accounts in accordance with this policy.

Employee role assignments shall be reviewed periodically by senior management. Assignment of an employee to any Administrator role must always be approved by a senior manager before being applied.

Monitoring

- AWS CloudTrail will be utilized to monitor operations on AWS resources.
- Shell access to Application Servers will be permitted only through the SSH Bastion Host, which will log all commands executed by each user.
- MySQL query logs will not be enabled due to performance concerns. However tables containing sensitive configuration or other data will have associated “audit” tables which automatically record a trail of changes made using database triggers or similar mechanisms.
- AWS CloudWatch alerts will be configured to detect suspicious access patterns such as repeated login failures. Administrators should review any alerts and respond appropriately (e.g. by instituting IP bans)