WebSphere Cast Iron Live Security

January 2011

IBM

Contents

Introduction

WebSphere® Cast Iron Live has been designed from the ground-up to provide a secure, scalable, and robust means to accomplish data integration within and between the cloud and enterprise. This whitepaper discusses how we ensure that your security concerns are being addressed at various levels including the infrastructure we run on, the platform that runs the integrations and the secure access methods we use to connect to applications/data for integration needs.

Infrastructure security

The infrastructure on which WebSphere Cast Iron Live runs has been certified to be SAS-70 Type II compliant as per the stringent audit requirements of the American Institute of Certified Public Accountants. This audit ensures that the:

- Physical infrastructure is equipped with security and access controls
- Network infrastructure is equipped with mitigation techniques for DDoS (Distributed Denial of Service) attacks, prevention of unauthorized port-scans, IP spoofing, etc
- Redundancy is provided at several levels including network, power and storage

Platform security

The WebSphere Cast Iron Cloud integration platform has been designed on principles that mandate that our customers' security needs are never compromised. Specifically this is addressed as outlined below:

- **Logical access controls:** When a customer registers for an account on WebSphere Cast Iron Live, a tenant is provisioned to the customer along with a tenant administrator. Tenant administrators can provision additional internal users on an as-needed basis. Tenant administrators are the only ones that are authorized to provide IBM support personnel with access to the tenant. In addition, each tenant could have multiple environments (e.g. development, production) which are essentially isolated work-areas and the WebSphere Cast Iron Cloud integration security model allows users to be created with different levels of access to each environment.

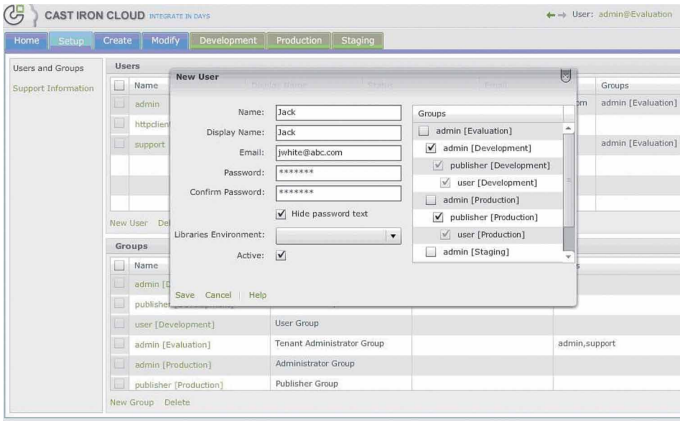

Figure 1: Each user can be assigned to the correct group with specific privileges.

- **Password policies:** All user passwords are encrypted with the SHA-1 algorithm. Passwords are required to be created with stringent policies such as including characters from at least three of the four categories: upper case, lower case, numeric and non-alphanumeric.

- **User groups and roles:** This is multi-tier role-based access that includes specific privileges. For example, there are the following three types of pre-defined roles:
  - **Admin**—Full administrative privileges are available. Admin may view and change all settings.
  - **Publisher**—Publisher may publish projects to the run-time. Publisher also has read-only access to all logs and settings.
  - **User**—User has read-only access to all logs and settings. This role is intended for users who need to view orchestration monitoring data, but should not have privileges to change any other settings.

  In addition, each of these is tied to different levels of access such as Tenant level and Environment level. Tenant level administrators have privileges across the entire tenant whereas Environment level administrators are restricted to administering a particular environment only such as Development or Production.

- Communication security: All traffic to and from WebSphere Cast Iron Live is protected by SSL 128 bit encryption.

- Data encryption: Tenant configuration and user information stored in redundant databases is protected by passwords. Periodic database dumps taken as backups are encrypted.

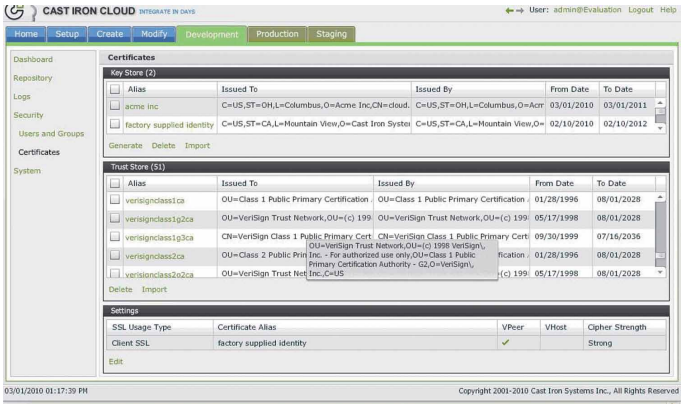

Figure 2: PKI implementation can be administered within the WebSphere Cast Iron Cloud integration management console by an administrator

- Public Key Infrastructure: WebSphere Cast Iron Live provides a PKI implementation that can be administered by a user with an admin role through the WebSphere Cast Iron Cloud integration management console. The following features are provided:
  - Support for X.509v3 certificates
  - Generation of self-signed certificates to enable SSL without a 3rd party Certificate Authority (CA)
  - Generation of a Certificate Signing Request (CSR) in PKCS #10 format for certification generation from a 3rd party Certificate Authority (CA)
  - Import of certificates and keys in PKCS#12 format
  - Management of trusted root Certificate Authority (CA) certificates

WebSphere Cast Iron Cloud integration secure connector

WebSphere Cast Iron Live accomplishes integration of on-premise data with cloud data using the WebSphere Cast Iron Cloud integration secure connector. The WebSphere Cast Iron Cloud integration secure connector is a light-weight piece of software that resides behind the firewall and connects databases, enterprise applications and message queues behind the firewall in a secure manner with the cloud.

To help ensure that you can securely and confidently connect your on-premise applications to the cloud, we have designed the WebSphere Cast Iron Cloud integration secure connector placing the highest possible bar on security. Some of these design principles include:

- The Secure Connector will always initiate communication with the WebSphere Cast Iron Live gateway and the gateway will validate the Secure Connector before attempting further processing.

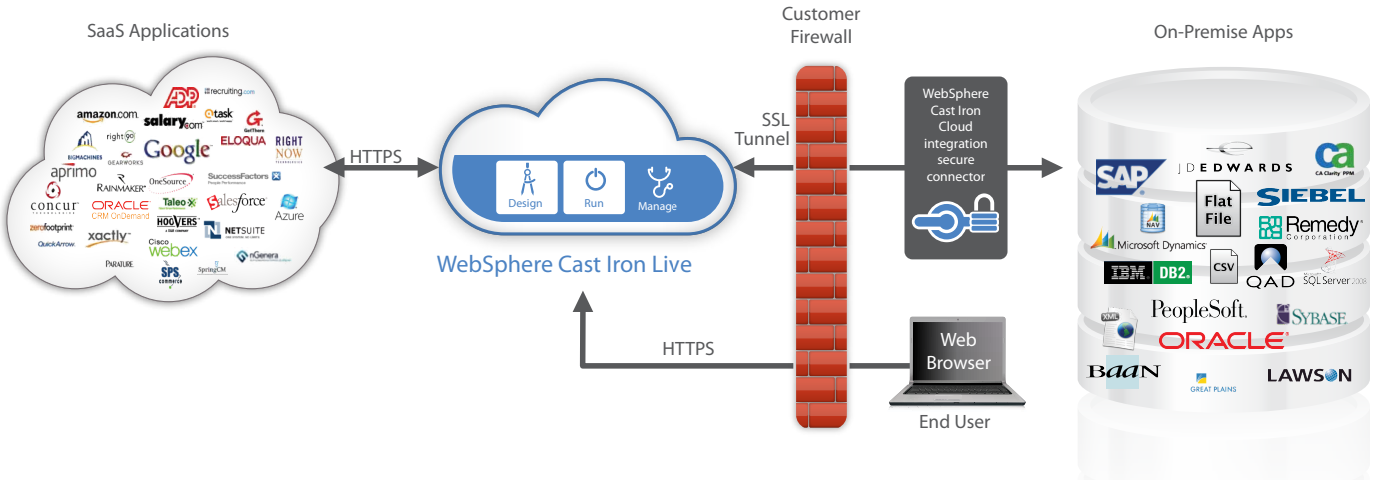

Figure 3: Data flowing between SaaS applications, WebSphere Cast Iron Live and on-premise applications is protected by industry standard encryption techniques

- Communication between the Secure Connector and WebSphere Cast Iron Live is based on the standard SSL 128 bit encryption over HTTPS through port 443. When the WebSphere Cast Iron Cloud integration secure connector starts up, it undergoes the SSL/TLS handshake and authenticates through standard X.509 certificates and establishes a TLS encrypted tunnel if everything else succeeds. Relying on these industry standards ensures protection against security threats such as eavesdropping, man-in-the-middle attacks, etc.

- Once the TLS connection is established successfully, Secure Connector sends a request to WebSphere Cast Iron Live for authentication. Based on information provided by the Secure Connector such as Tenant ID, Environment ID, Authentication key and a Private key, the WebSphere Cast Iron Live gateway ensures that only the right Secure Connector is granted access to a particular environment of a tenant. This guarantees an additional level of security while pulling and pushing data into the orchestrations for subsequent processing.

- In addition, the Secure Connector can be configured to allow only certain pre-defined & authorized white-listed IP address range(s) to communicate with it

- Data transmission and requests inbound to the WebSphere Cast Iron Cloud integration secure connector from the WebSphere Cast Iron Live gateway are limited to an available set of end-point connectors provided by WebSphere Cast Iron Cloud integration. Users would need to explicitly specify address and authentication information from each end-point they are connecting to.

- WebSphere Cast Iron Cloud integration explicitly does not provide NFS or other similar connectors to access flat-files directly from disk (instead users need to access these files through an FTP server that is password protected). Also we do not allow local scripts or executables to be executed directly through the Secure Connector.

- Network administrators can further secure the WebSphere Cast Iron Cloud integration secure connector by restricting network or IPs it can access internally. This can be accomplished either at the server level (Windows FW, Linux IPTables) or by restrictions on the switch/router.

Data access security

WebSphere Cast Iron Live acts as a mere conduit for your integration needs and only stores mapping rules and orchestration logic defined by your users. The solution does not by default store any of your application or database data on the persistent store in WebSphere Cast Iron Live.

When communicating with endpoint applications such as applications, databases and flat-files, the WebSphere Cast Iron Live is capable of communicating using a variety of secure communication protocols:

- HTTPS (HTTP over SSL)—Supports bi-lateral authentication, privacy and integrity

- Secure Web Services (SOAP/HTTP over SSL)—Supports bi-lateral authentication, privacy and integrity

- Secure FTP (FTP over SSH) and FTPS (FTP over SSL or Implicit FTPS)—Supports secure mechanisms for FTP server authentication, privacy and integrity

- Secure Databases (SSL)—Supports secure mechanism for database access

Contact us

To learn more about the WebSphere Cast Iron Cloud integration please call us at 650.230.0705 or visit us online at http://www.ibm.com/software/integration/cast-iron-cloud-integration/.

IBM Corporation
Software Group
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
January 2011

Please Recycle

WSW14139-USEN-01