

CoSolvent Community Server Implementation and Management Summary

Server Setup and Hosting

This CoSolvent Community Server is hosted on a dedicated server instance leased from Amazon Web Services that resides in Amazon's Elastic Compute Cloud (EC2). The client has access to all administrative accounts on the server and to any server "control panel" which may be provided by the hosting provider. To facilitate management of the server, iPOV will link the server instance and all other resources (S3 and EBS storage, etc...) to a management account created by iPOV, at any time the client may choose to have iPOV transfer control over the server instance account and any other resources directly to the client, or to any third party that the client may choose to designate; however the client will still be obligated to pay iPOV's maintenance and upgrade fees if the client wishes to receive any future upgrades to the software. Normal leases are month-to-month and may be terminated with 30 days written notice. Yearly contracts may be terminated by providing written notice within 30 days of the end of the contract year.

The major features of the server hosting are:

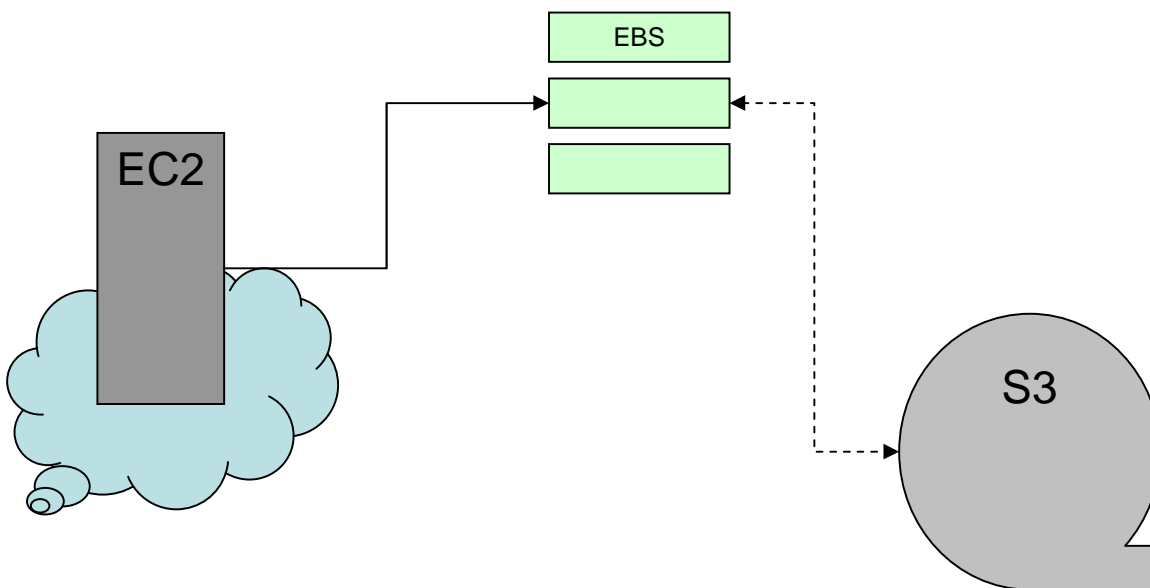
- Data Center management by hosting provider (Amazon Web Services Ltd.)
- Virtualized server running latest release of Ubuntu Linux Server Edition.
 - Our normal server is the AWS "Standard" Server instance.
- All direct management is done via encrypted Secure Shell connection; AWS enforces use of X.509 security certificates to protect against password brute force attack.
- Remote management and server login are associated with different logins and passwords to minimize exposure should one login be compromised.

Account login "end points" are listed below. Login names and passwords have been supplied to MRT via a separate document to help maintain security.

Account Type	Connect To
Server Secure Shell	Connect to instance using X.509 certificate
CoSolvent Community Server	https://SERVERNAME/cc/
Amazon Web Services (S3 backup)	Web login to http://aws.amazon.com

AWS Components

The diagram below presents a simplified version of the Amazon Web Services components which we use in our hosting solution.



While other configurations are possible, our solution is designed to work with the minimal amount of "lock-in" to the Amazon Web Services proprietary pieces.

Component	Use
EC2	The Elastic Compute Cloud (EC2) provides the hosting environment to run a virtualized server providing web serving and video transcoding functionality.
EBS	Elastic Block Storage (EBS) is essentially a SAN disk, sitting between the EC2 server, which has no persistent storage of its own, and the redundant, distributed storage offered by S3
S3	The Simple Storage Service (S3) is used for long term backups of the data from the EBS 'disk' and for storing the server 'instance' definition (required to start the EC2 instance)

The current server specifications (see <http://aws.amazon.com/ec2/instance-types/>) are:

Hardware: Virtualized x86 CPU w/ 1.7 GB RAM

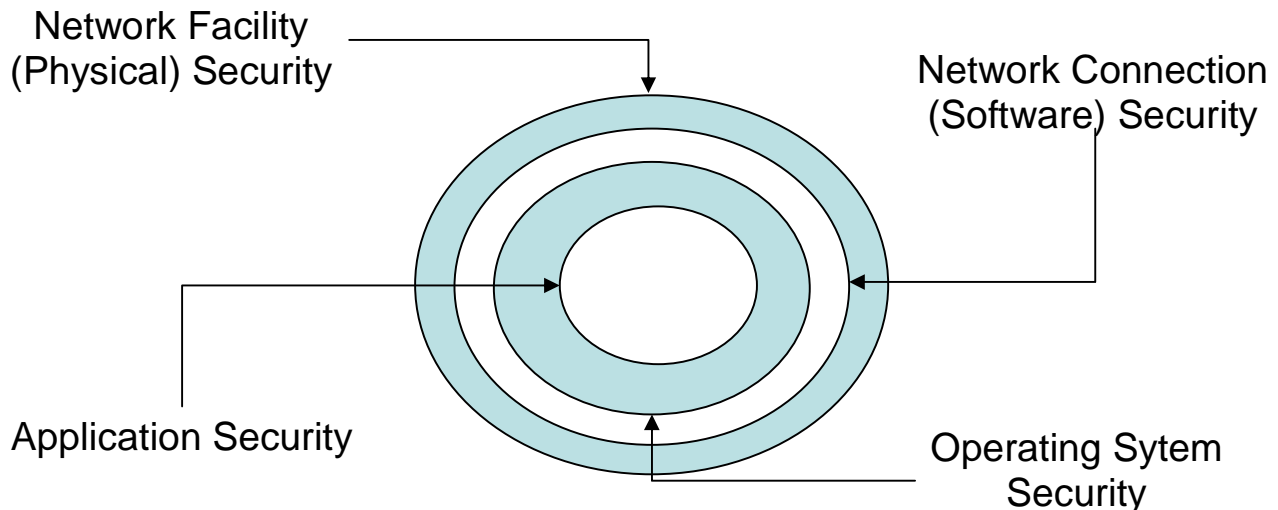
Operating System: Ubuntu 8.10 x86

250 Mbps (burst) Uplink

AWS offers various types or sizes of EC2 instances, making scaling the server a quick and relatively painless exercise.

Server Security Provisions

iPOV visualizes server security as a series of security layers:



The outer layer concerns physical security (from natural disaster or human attack). If someone can gain physical access to the server, it can mount an attack, either physically, or by inserting malicious boot media, etc. Also, natural disasters could knock services off-line for extended periods of time. Amazon Web Services provides the physical and basic network layers of security and redundancy; please refer to "AWS Security Whitepaper" for full details, but we will excerpt:

Amazon has many years of experience in designing, constructing, and operating large-scale data centers. This experience has been applied to the AWS platform and infrastructure. AWS data centers are housed in nondescript facilities, and critical facilities have extensive setback and military grade perimeter control berms as well as other natural boundary protection. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, state of the art intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication no fewer than three times to access Amazon Web Services Security data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

For more go to <http://aws.amazon.com/> and look for "Business Managers" or search for "Amazon Web Services: Overview of Security Processes"

Network security is provided by:

- Using Amazon's stateful packet inspection and limiting the ports that can be connected to on the server to SSH for management and HTTPS for web access.
- Limiting the number of network "services" that the server runs to the minimum required
- Using encrypted connections whenever logging in to management accounts
- Keeping server software updated to the latest security releases.

While there is much discussion on the topic of the “most secure” operating system, there is a strong argument that the security of any operating system is mainly derived from how effectively it is configured. Operating System Security is implemented as follows:

- IPOV uses Ubuntu, a popular Linux distribution with a good security history, accessible and easily installable security updates, and good security defaults.
- Only the “services” required (OpenSSH, the Apache2 Web Server, MySQL database, and PHP scripting engine) are run.
- Automatic updates are enabled that will install security related patches without human intervention.
- Tripwire, an open source security auditing tool, is installed and run during regular, scheduled maintenance.

The MRT Community Server is built on “Gallery 2” PHP code that has been subjected to formal security audits prior to each major release. The following table lists the releases and the auditors.

Release	Audit Company	Company URL
2.3	Gotham Digital Science	www.gdssecurity.com
2.2	Gulftech Research and Development	www.gulftech.org
2.1	Intershot Limited	www.intershot.com/security/

One of the areas of great concern for all applications, but web applications in particular, is the validation of user input, as the un-validated, or not inadequately validated inputs that lead to the vast majority of security holes. The Gallery2 development community is well aware of the need for strict input validation as a means of security. Indeed, the design of Gallery2 provides for validating user input reliably and without exception. This is done by providing a set of utilities for obtaining and sanitizing request information and integrating that process with that of URL generation within the code. For more information on input validation see

http://www.ibm.com/developerworks/opensource/library/os-php-secure-apps/?S_TACT=105AGY46&S_CMP=PCTAB.

iPOV has followed the recommendations for securing Gallery 2 in our configuration process. The full recommendation can be found online <http://codex.gallery2.org/Gallery2:Security> but the list below summarizes the configuration objectives.

- Each instance of CoSolvent Community Server is hosted on a dedicated server instance and access is limited to iPOV and MRT employees with valid administrative accounts.
- File system permissions on config.php are set to 444 (read-only) except during system upgrades.
- The web server is configured to disallow access to source (.inc and .class) files
- File system permissions for the web file folder are set to 550 (access only allowed by web server application).
- PHP errors are logged to a file rather than printed to web pages. This helps to prevent disclosure of potentially sensitive file system information.

Backup

The CoSolvent database and data files are stored on a EBS disk instance, providing physical safeguards beyond that of a standard server disk drive. Additionally, "snapshots" (incremental backups) of the EBS data are stored to S3 providing redundant storage on a weekly basis.

S3 provides a relatively low cost and highly reliable backup solution. Full details of the security and reliability designed into Amazon S3 can be found in the document published by Amazon Web Services, <http://developer.amazonwebservices.com/connect/entry.jspa?externalID=1697&categoryID=55>.

The primary features are summarized below:

- S3 conforms to Sarbanes Oxley (SOX) compliance and certifications such as recurring Statement on Auditing Standards No. 70: Service Organizations, Type II (SAS70 Type II)
- AWS data centers are housed in nondescript facilities, and critical facilities have extensive setback and military grade perimeter control berms as well as other natural boundary protection. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, state of the art intrusion detection systems, and other electronic means.
- Data is redundantly stored in multiple physical locations as a normal part of those services and at no additional charge.
- For maximum security, Amazon S3 is accessible via SSL encrypted endpoints.
- Data stored within Amazon S3 can be encrypted to ensure data integrity and security.

Software Ownership and Licensing

- CoSolvent Community Server is offered as Software as a Service (SaaS), not licensed.
- The core components of the CoSolvent Community Server are available as Open Source from various vendors.
- iPOV has developed the following additional, specialized modules that fall under direct CoSolvent Community Server licensing:

Module	Description
Praxis Theme	Provides a business oriented 'skin' for the application.
FfmpegSwf	Provides the logic and assets for transforming "raw" video uploads into web streamable FLV files.
SWFUpload	Provides advanced upload control to improve and enrich the user experience when uploading files. This module uses the open source SWFUpload.org component to implement the upload logic.

Support Customizations	Various additions to assist users and provide an improved user experience. Includes code to display PDFs "inline" inside the site, a web based email sender, and a personal navigation history 'bread crumb' component.
Permissions Management	Tools to assist in managing Users, Groups, and permission assignments in a workgroup or enterprise level.
Help Module	Module to provide context sensitive help links.
Template Customizations	Modifications to the various templates which ship as part of the core Gallery 2 modules to improve the user experience.

- IPOV's **CoSolvent Player** is bundled with the CoSolvent Community Server to enable web streamable video playback. CoSolvent Player is licensed to the client for use only with the CoSolvent Community Server under perpetual, non-exclusive, royalty-free terms. For other uses licenses may be purchased from www.cosolvent.biz
- The CoSolvent Community Server relies on a collection of open-source software applications that each have their own licensing requirements. The following table lists the software and licenses that apply.

Software	License	Author	Description
Community Server	GPL 2	IPOV.net	Consists of the custom modules, theme, and library files used to transform the Gallery2 image sharing system into a video and document collaboration tool. Since it relies on the Gallery 2 libraries, the code for the Community Server falls under the GPL.
Dojo Toolkit	Modified BSD	Dojo Foundation	Javascript library used to provide advanced web page user interfaces in the Community Server.
phpSniff	LGPL 2	Roger Raymond	PHP library used to detect and support the user's web browser version.
SWFUploader	MIT License	swfupload.org	Provides SWF control and JS library used in the improved upload module.
CoSolvent Player	Proprietary, non-exclusive, royalty-free use.	iPOV.net	Provides web streamable video playback controls.
Gallery 2	GPL 2	Gallery 2 Dev. Team (Bharat Mediratta et.al.)	An open source platform for creating image and document sharing sites.
YUI	BSD	Yahoo	Javascript library used by Gallery 2
Smarty	LGPL	New Digital	Templating engine used by Gallery 2

		Group, Inc.	
ADODB	BSD & LGPL	John Lim	Database access layer used by Gallery 2
FFMPEG	GPL*	Fabrice Bellard et. al.	Used by Community Server to process video files into streamable format. FFMPEG core is LGPL, however full functionality depends on several modules falling under the GPL as well as code which falls under various other licenses.
ImageMagick	Custom (free)	ImageMagick Studio LLC	License can be accessed at http://www.imagemagick.org/script/license.php . The library is used by the Community Server to process images.
NetPBM	GPL	NetPBM Team	The library used by the Community Server to process images.
GD	Free	Thomas Boutell et. al.	License information available at http://www.boutell.com/gd/manual2.0.33.html#notice . The library is used by the Community Server to process images.
PHP	Apache-style	The PHP Group	Programming language and script engine used to run the Community Server.
Apache	Apache 2	Apache Foundation	Primary web server for Gallery 2, although it can be run on Windows using IIS.
MySQL	GPL with PHP exception	MySQL, now SUN	Database used to run the Community Server.
Linux	GPL		Operating System used to run the Community Server. The 'kernel' is GPL, but many system library interfaces are LGPL.

Risk Management Plan

The Community Server source code embeds the open source Gallery 2 software project (<http://gallery.menalto.com/>). Consequently, there is a ready community of developers familiar with the underlying architecture, should a client desire to transfer maintenance or development to other vendors.

While iPOV is confident that it will remain the developer of choice for the Community Server, the terms of the license allow the client to take immediate possession of the leased server account and all source code at the client's sole discretion. All source code for the CoSolvent Community Server is included in the standard install and is available at all times for review and maintenance "as is" on the hosting server.

The combination of full source code and the fact that the source code is based on public, open-source projects, gives clients additional protection. Competent PHP programmers should be able to find and fix operational bugs, from scratch, in a few days to a few weeks depending on the nature of the bug. Consequently, there are numerous programming sources that could maintain the CoSolvent Community Server at the status quo – and make occasional incremental improvements. Nonetheless, it is doubtful that most third parties will be as committed as iPOV to making aggressive system improvements.

Software Migration

It is relatively easy to move an instance of the CoSolvent Community Server application to a new web server host. The underlying software platform currently requires a "LAMP" (Linux, Apache, MySQL, PHP) host configuration, but this is very common and widely supported. Any migration should take into account the built in redundancy of the AWS hosting platform and either use a provider with similar hosting or find other solutions to assure availability.