Network Working Group
Internet-Draft
Intended status: Experimental
Expires: January 6, 2011

C. Hoff
Cisco Systems
S. Johnston
Google
G. Reese
enStratus
B. Sapiro
TELUS

July 5, 2010

CloudAudit 1.0 - Automated Audit, Assertion, Assessment, and Assurance API (A6)
draft-hoff-cloudaudit-00

Abstract

CloudAudit provides an open, extensible and secure interface that allows cloud computing providers to expose Audit, Assertion, Assessment, and Assurance (A6) information for cloud infrastructure (IaaS), platform (PaaS), and application (SaaS) services to authorized clients.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 6, 2011.

Copyright Notice

Table of Contents

1. Introduction

CloudAudit provides a common interface, naming convention, set of processes and technologies utilizing the HTTP protocol to enable cloud service providers to automate the collection and assertion of operational, security, audit, assessment, and assurance information. This provides duly authorized and authenticated consumers and brokers of cloud computing services to automate requests for this data and metadata.

CloudAudit supports the notion of requests for both structured and unstructured data and metadata aligned to compliance and audit frameworks. Specific compliance framework definitions and namespaces ("compliance packs")) will be made available incrementally.

The first CloudAudit release is designed to be as simple as possible so as it can be implemented by creating a consistent namespace and directory structure and placement of files to a standard web server that implements HTTP [RFC2616]. Subsequent releases may add the ability to write definitions and assertions, and to request new assertions be generated (e.g. a network scan). That is, while 1.x versions are read-only, subsequent releases may be read-write.

A duly authorized and authenticated client will typically interrogate the service and verify compliance with local policy before making use of it. It may do so by checking certain pre-defined parameters (for example, the geographical location of the servers, compliance with prevailing security standards, etc.) or it may enumerate some/all of the information available and present it to an operator for a manual decision. This process may be fully automated, for example when searching for least cost services or for an alternative service for failover.

As it is impossible to tell in advance what information will be of interest to clients and what service providers will be willing to expose, a safely extensible mechanism has been devised which allows

any domain name owner to publish both definitions and assertions.

2. Notational Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14, [RFC2119], as scoped to those conformance targets.

This document uses the Augmented Backus-Naur Form (ABNF) notation of [RFC2616].

Additionally, the following rules are included from [RFC3986]: URI.

3. Discovery

3.1. Repository

Clients SHOULD detect support for CloudAudit by verifying that a HTTP GET or HEAD for the repository root (e.g. /.well-known/cloudaudit) is successful (e.g. "200 OK"). Clients MAY also verify that requests for invalid URLs (e.g. /.well-known/<random>) return an error (e.g. "404 Not Found").

If clients do not confirm the existence of a CloudAudit repository then they may be susceptible to false negatives (e.g. falsely assuming an assertion is absent when in fact the entire repository is absent) and if they do not confirm the absence of errors for invalid URLs then they may be susceptible to false positives (e.g. falsely assuming an assertion is present when in fact any assertion is present).

3.2. Links

Servers MAY specify the root of a CloudAudit repository in the HTTP Link: header and/or HTML LINK element with rel="http://cloudaudit.org". This allows one or more services to delgate requests to a single local or remote/third-party server. Clients SHOULD check for the presence of these links before assuming that there is a local CloudAudit repository.

```
<link rel="http://cloudaudit.org" href="http://example.com/.well-known/cloudaud
```

HTML Discovery

```
Link: <http://example.com/.well-known/cloudaudit/com.example.ec2>; rel="http://
```

HTTP Discovery

4. Enumeration

Servers MAY render a HyperText Markup Language (HTML) response to a HTTP request for a directory containing an A or LINK element for every child with a HREF attribute containing the relative URL of the child. Clients MUST NOT rely on this functionality, which will vary from server to server.

5. Namespaces

CloudAudit defines two namespaces; the glossary namespace which contains definitions and the service namespace which contains assertions. It relies on the Domain Name Service (DNS) to divide the glossary and service namespaces in an extensible fashion without relying on registries.

A domain name (e.g. example.com) under the control of the party is broken into its components (e.g. example, com), reversed (e.g. com, example) and recombined (e.g. com.example). That party "owns" this namespace so long as the domain is registered to them and they may subdivide it with components in order to reference and/or categorise glossary definitions and service assertions. These MAY or MAY NOT represent valid hosts in the DNS.

URI schemes and paths are NOT supported (e.g. https://example.com/cloud), however it is possible for a service to advertise an alternate name (e.g. cloud.example.com) via the HTTP Link header and/or HTML LINK element (Section 3).

5.1. Glossary namespace

The glossary allows clients to enumerate and/or resolve definitions, and to obtain additional documentation. Servers MUST provide a plain text representation and MAY provide alternative representations (such as HTML) via HTTP content negotiation.

5.1.1. Examples

5.1.1.1. Generic

The following shows a client obtaining a definition for org.iso.3166-1.

```
< GET /.well-known/cloudaudit/glossary/org/iso/3166-1 HTTP/1.1
< Host: iso.org
<
> HTTP/1.1 200 OK
> Content-Length: 24
> Content-Type: text/plain
>
> ISO 3166-1 Country Codes
```

5.1.1.2. Compliance

The following shows a client obtaining a defintion for gov.nist.crc.sp800-53.r2.


```
< GET /.well-known/cloudaudit/glossary/gov/nist/crc/sp800-53/r2 HTTP/1.1
< Host: nist.gov
<
> HTTP/1.1 200 OK
> Content-Length: 102
> Content-Type: text/plain
>
> NIST SP800-53 (Rev. 2) Recommended Security Controls for Federal Information
```

5.2. Service namespace

Assertions can be made about the local service and/or remote service(s).

5.2.1. Local Assertions

Local assertions refer to the service(s) sharing the same URL end-point as the CloudAudit repository. They can be identified by the absence of a '/-/' component in the URL (which is used as a delineator for Remote Assertions Section 5.2.2) and can normally be implemented using symbolic links or web server configuration.

5.2.1.1. Examples

5.2.1.1.1. Generic

This example shows a client retrieving the ISO 3166-1 country code(s) from which the cloud.example.com service is being provided.

```
< GET /.well-known/cloudaudit/service/org/iso/3166-1 HTTP/1.1
< Host: cloud.example.com
<
> HTTP/1.1 200 OK
> Content-Length: 3
> Content-Type: text/plain
>
> US
```

5.2.1.1.2. Compliance - Human Readable Response

This example shows a client retrieving a response to a control section 15.3.1 of ISO 27002 (v2005) from which the cloud.example.com service is being provided. The response is valid HTML and intended to be human readable.


```
< GET /.well-known/cloudaudit/service//org/iso/27002/v2005/15/3/1 HTTP/1.1
< Host: cloud.example.com
<
> HTTP/1.1 200 OK
> Content-Length: 822
> Content-Type: text/html
>
> <html>
```

```
> <body>
> <head>
> <title>ISO 27002 v2005 15.3.1</title>
> </head>
> <H1>Information systems audit controls</H1>
> <UL>
> <LI><a href="http://www.cloudhosting.com/.well-known/cloudaudit/org/iso/27002
> <LI><a href="http://www.cloudhosting.com/.well-known/cloudaudit/org/iso/27002
> <LI><a href="http://www.cloudhosting.com/.well-known/cloudaudit/org/iso/27002
> </UL>
> </body>
> </html>
```

5.2.1.1.3. Compliance - Atom Response

This example shows a client retrieving a response to a control section 15.3.1 of ISO 27002 (v2005) from which the cloud.example.com service is being provided. The response is in an ATOM format [RFC4287] and intended to be machine processed.

```
< GET /.well-known/cloudaudit/service//org/iso/27002/v2005/15/3/1/manifest.xml
< Host: cloud.example.com
<
> HTTP/1.1 200 OK
> Content-Length: 3432
> Content-Type: text/xml
>
> <?xml version="1.0" encoding="UTF-8"?>
> <feed xmlns="http://www.w3.org/2005/Atom">
>    <title>ISO 27002 v2005 15.3.1</title>
>    <link href="http://www.cloudhosting.com/.well-known/cloudaudit/org/iso/270
>    <id>http://www.cloudhosting.com/.well-known/cloudaudit/org/iso/27002/v2005
>    <subtitle>Information systems audit controls</subtitle>
>    <updated>2010-01-13T18:30:02Z</updated>
>    <generator uri="http://cloudaudit.org/development/bootstrap.tgz" version="
>    <author>
>        <name>Jon James</name>
>        <email>jonjames@cloudhosting.com</email>
>    </author>
>    <rights type="text">Copyright (c) 2009, Cloud Hosting Inc.</rights>
>    <category term="/iso/27002/v2005/" label="ISO 27002 v5"/>
```



```
>
```

```
>    <entry>
>        <title>Audit Schedule</title>
>        <link href="http://www.cloudhosting.com/.well-known/cloudaudit/org/iso
>        <id>http://www.cloudhosting.com/.well-known/cloudaudit/org/iso/27002/v
>        <updated>2009-12-28T12:24:02Z</updated>
>        <summary>the 2010 audit schedule for cloud hosting inc.</summary>
>        <author>
>            <name>Eric Smith</name>
>            <email>ericsmith@cloudhosting.com</email>
>        </author>
>        <contributor>
>            <name>Mary Huxley</name>
>            <email>maryhuxley@kpwey.com</email>
>            <uri>http://www.kpwey.com</uri>
>        </contributor>
>    </entry>
>
>    <entry>
>        <title>KPWEY LLP Audit Contract</title>
>        <link href="http://www.cloudhosting.com/.well-known/cloudaudit/org/iso
>        <id>http://www.cloudhosting.com/.well-known/cloudaudit/org/iso/27002/v
>        <updated>2009-01-12T11:45:02Z</updated>
>        <summary>The audit contract with KPWEY for external audit services</su
>        <content type="text" xml:lang="en">
>            The document details the services procured to support the audit pl
>        </content>
>        <author>
>            <name>Eric Smith</name>
>            <email>ericsmith@cloudhosting.com</email>
>        </author>
>        <contributor>
>            <name>Mary Huxley</name>
>            <email>maryhuxley@kpwey.com</email>
>            <uri>http://www.kpwey.com</uri>
>        </contributor>
>    </entry>
>
>    <entry>
>        <title>Audit Scope</title>
>        <link href="http://www.cloudhosting.com/.well-known/cloudaudit/org/iso
>        <id>http://www.cloudhosting.com/.well-known/cloudaudit/org/iso/27002/v
>        <updated>2009-12-28T12:25:02Z</updated>
>        <summary>The audit scope for the planned audits in 2010</summary>
>        <author>
>            <name>Sarah Chan</name>
>            <email>sarahchan@cloudhosting.com</email>
>        </author>
```

```
>        <contributor>
>            <name>David Kohl</name>
>            <email>davidkohl@kpwey.com</email>
>        </contributor>
>        <contributor>
>            <name>Mary Huxley</name>
>            <email>maryhuxley@kpwey.com</email>
>            <uri>http://www.kpwey.com</uri>
>        </contributor>
>    </entry>
> </feed>
```

5.2.1.1.4. Compliance - Non-Existent

This example shows a client atempting to retrieve a non existent response to a control section of NIST SP800-53 (Rev 2) from which the cloud.example.com service is being provided.

```
< GET /.well-known/cloudaudit/glossary/gov/nist/crc/sp800-53/r2/cp-2 HTTP/1.1
< Host: cloud.example.com
<
> HTTP/1.1 404 Not Found
> Content-Length: 148
> Content-Type: text/html
>
> <html>
> <head>
> <title>404 Not Found</title>
> </head><body><h1>Error: Not Found</h1>
> <h2>The requested URL was not found on this server.</h2>
> </body>
> </html>
```

5.2.2. Remote Assertions

There are a number of scenarios where it is necessary to answer CloudAudit queries on behalf of others, including:

- Responding to queries on behalf of multiple servers
- Responding to queries from multiple clients
- Proxying in order to supplement or override assertions
- Incompatibilities with existing systems and software that prevents co-location

Remote assertions are supported by embedding both the name (e.g. cloud.example.com) and the assertion queried (e.g. 3166-1.iso.org) in

the URL. The name and assertion MUST be delineated with a '/-/' URL component as they may vary in length.

5.2.2.1. Examples

This example shows a client retrieving the ISO 3166-1 country code(s) from which the cloud.example.com service is being provided, from the remote server cloudaudit.net.

```
< GET /.well-known/cloudaudit/service/com/example/cloud/-/org/iso/3166-1 HTTP/1
< Host: cloudaudit.net
<
> HTTP/1.1 200 OK
> Content-Length: 3
> Content-Type: text/plain
>
> US
```

5.2.3. Third-party Assertions

It may be necessary for third-parties to make assertions, for example where an auditor certifies compliance with a given standard at a given time. This can be achieved either by retrieving a trusted representation (for example, an image containing a physical signature, or a digitally signed document) from the first-party or by being redirected to a third-party and retrieving the assertion directly from them.

6. Digital Signatures

Digital signatures allow clients to verify the integrity of the assertions (both first-party and third-party).

7. IANA Considerations

This document makes no request of IANA.

Note to RFC Editor: this section may be removed on publication as an

RFC.

8. Security Considerations

The content of CloudAudit repositories MAY NOT be secure, private or integrity-guaranteed, and due caution should be exercised. Clients SHOULD use Transport Layer Security (TLS) [RFC5246] or equivalent to ensure confidentiality and integrity when accessing CloudAudit

repositories over a public network such as the Internet.

The Domain Name System (DNS) MAY be susceptible to attacks and care should be taken to authenticate servers, for example by verifying the chain of trust and infromation contained in SSL certificates provided, by using a Virtual Private Network (VPN) service, by relying on DNSSEC [RFC4033], etc.

Malicious clients MAY seek to obtain sensitive information via CloudAudit which could then be used to launch an attack. Such information should only be made available to authorised clients who have been authenticated via HTTP authentication [RFC2617] or equivalent.

Servers may make false first-party assertions or may refer to third-party assertions that do not apply to them, or that expand the scope of the intended meaning. Clients that do not trust servers may choose only to rely on trusted third-party assertions, in which case the integrity of the assertion SHOULD be verified by transferring it over Transport Layer Security (TLS) [RFC5246] or equivalent or by verifying a digital signature applied to the assertion using OpenPGP [RFC4880] or equivalent

9. Acknowledgements

The authors would like to acknowledge all members of the CloudAudit Working Group, editors of framework specification documents (including Doug Barbin, Mike Versace, James Arlen and Dave Lewis), the publishers of frameworks (including ISACA, HHS, ISO, NIST and PCI) and early adopters of the standard.

10. References

10.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2616] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999.

[RFC2617] Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P., Luotonen, A., and L. Stewart, "HTTP Authentication: Basic and Digest Access Authentication", RFC 2617, June 1999.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, January 2005.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[RFC4287] Nottingham, M., Ed. and R. Sayre, Ed., "The Atom Syndication Format", RFC 4287, December 2005.

[RFC4880] Callas, J., Donnerhacke, L., Finney, H., Shaw, D., and R. Thayer, "OpenPGP Message Format", RFC 4880, November 2007.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[W3C.REC-html401-19991224] Hors, A., Jacobs, I., and D. Raggett, "HTML 4.01 Specification", World Wide Web Consortium Recommendation REC-html401-19991224, December 1999, <http://www.w3.org/TR/1999/REC-html401-19991224>.

10.2. Informative References

Appendix A. Initial Registry Contents

The CloudAudit registry's initial contents are:

- Assertion Name: org.iso.3166-1
- Description: Codes for the representation of names of countries and their subdivisions -- Part 1: Country codes
- Reference: http://www.iso.org/iso/iso-3166-1_decoding_table

Authors' Addresses

Christofer Hoff
Cisco Systems
200 Beaver Brook Road
Building 200
Boxborough, MA 01719
USA

Phone: +1.9786310302
Email: hoffc@cisco.com

Sam Johnston
Google
Brandschenkestrasse 110
Zurich, 8002
Switzerland

Phone: +41.446681679
Email: sj@google.com

George Reese
enStratus
1201 Marquette Ave
Suite 150
Minneapolis, MN 55403
USA

Phone: +1.6127463091
Email: george.reese@enstratus.com

Ben Sapiro
TELUS Security Labs
25 York Street
Toronto M5J 2V5
Canada

Phone: +1.6478899432
Email: ben@sapiro.net