Regional Data Collection

SiteCatalyst 14.6

OMNITURE®
An Adobe company

Transition White Paper

14.6 12102009

Table of Contents

1 Preface

The Omniture® *Regional Data Collection Transition Whitepaper* describes and introduces Regional Data Collection (RDC), the transition process, and what to expect once the transition is complete.

This guide includes the following sections:

- RDC Overview
- Transitioning to RDC
- Post-Transition Expectations

1.1 Intended Audience

This guide is intended for Web Marketers and Web site engineers that are familiar with Omniture SiteCatalyst and implementing SiteCatalyst beacons (image requests).

1.2 Document Conventions

To increase accessibility and readability, this document uses the following conventions:

- File names and code samples use a Courier font. For example, `autoexec.bat`.
- Replaceable text is enclosed in angle brackets and italicized. For example, <*version*>.

NOTE: A Note draws attention to helpful information.

CAUTION: A Caution specifies the results of an action. The results might not be damaging, but they are important to understand.

WARNING! A Warning identifies an action that might result in system damage and data loss.

2 RDC Overview

To understand the need for RDC, you must understand the current method Omniture uses to collect data.

- Omniture maintains two Data Processing Centers (DPC) in the United States, one in Texas and one in California.
- Omniture assigns each of its clients to a specific DPC, and your Web site's data collection code identifies the DPC that should receive the collected data.
- Omniture uses a data collection domain together with a DPC identifier to map Web beacons to the appropriate DPC. For example: `client.112.2o7.net` or `client.122.2o7.net`.
- When a Web site "hit" generates an image request, the image request travels from the visitor's Web browser to the appropriate Omniture DPC, regardless of the visitor's physical location.

The potential network latency associated with "long distance" image requests can result in data loss, particularly if the visitor doesn't have a tracking cookie because visitors without tracking cookies go through additional redirections in an effort to set tracking cookies.

Omniture Regional Data Collection (RDC) is a network of regional Data Collection Centers (DCC) that aims to reduce latency and data loss associated with Omniture image requests.

- Modify your Omniture collection code (`s_code.js`, ActionSource, etc.) to use the new RDC domain `omtrdc.net`. For example: `mysite.d1.sc.omtrdc.net`.
- Using advanced DNS technology, Omniture maps the `omtrdc.net` domain to the data collection center nearest the visitor.
- When a Web site "hit" occurs, the Omniture image request automatically routes to the data collection center nearest the visitor's browser.
- The data collection center uses a secure data pipe to immediately forward the data to your DPC, where it is processed and made available to the Omniture Suite of products.

  NOTE: The RDC domain also routes Data Insertion API requests through the nearest data collection center.

In the case of a disruption in communication between the data collection center and your DPC, Omniture's RDC infrastructure behaves as follows:

- Attempts to route data to your DPC through another data collection centers.
- Saves data locally, then forwards it to the DPC when communications are restored. Due to limits on storage space, this option is available only for short-term disruptions.
- For major disruptions, the Omniture Network Operations team reconfigures the global DNS system used by RDC to forward your data through another data collection center.

2.1 Performance Improvements with RDC

The following table illustrates the observed improvements in response time after migrating to RDC.

Regions	Response Time Removed by RDC
Asia	**36%**
Australia	5%
China and Russia	41%
Japan	41%
Europe	**83%**
British Isles	94%
Central and Eastern Europe	84%
Northern Europe	73%
Western Europe	89%
North America	**38%**
Canada	26%
Central US	48%
Eastern US	46%
Western US	20%
Global	**50%**

3 Transitioning to RDC

The transition from traditional Omniture data collection to RDC is not difficult, but if you have a large or complex environment you should plan carefully to make sure that all collection code updates simultaneously.

NOTE: Organizations with multiple report suites should transition all report suites at the same time to avoid inflated visitor counts and data accuracy problems.

The RDC transition varies based on your current Omniture implementation. During the RDC roll-out, use the following procedures to migrate to the RDC domain:

- SSL Certificates
- Current CNAME and New CNAME Implementations
- New Third-Party Cookie Implementations
- Migrating Current 2o7.net Implementations

3.1 SSL Certificates

If you use a CNAME implementation and measure secure traffic, you must provide sufficient SSL certificate licenses to support the RDC implementation.

Currently, your SSL certificate licenses must support five load balancers worldwide. However, as Omniture brings additional DCCs online, SSL certificate needs will change. How this affects your certificate licensing needs over time depends on the type of certificate license you own:

- Server-based licenses: License requirements for RDC deployments will grow over time.
- Volume-based licenses: License requirements will not be affected by infrastructure changes, but only as your traffic volume changes over time.
- Unlimited licenses: License requirements should remain relatively stable over time.

IMPORTANT: It is your sole responsibility to purchase and maintain these SSL certificates. It is also your responsibility to check the certificate provider's contract to confirm that SSL certificates can be installed in multiple data centers.

3.2 Current CNAME and New CNAME Implementations

1. Contact Omniture ClientCare, or your Omniture consultant, and ask to be placed in the RDC migration queue.
2. (Conditional) If you are using SSL, send Omniture a new SSL certificate with sufficient licenses (currently, at least 4) to support the RDC implementation, or verify that your current SSL certificate can support the distributed RDC architecture (see SSL Certificates).
3. Provide Omniture with the appropriate CNAME information for the RDC transition, including the CNAME, the current A Record and the new A Record. For example:

CNAME	Current A Record	New A Record*
`metrics.mysite.com`	`mysite.com.112.2o7.net`	`mysite.com.d1.sc.omtrdc.net`
`smetrics.mysite.com`	`mysite.com.102.112.2o7.net`	`mysite.com.ssl.d1.sc.omtrdc.net`
`metrics.mysite.co.uk`	`mysite.co.uk.112.2o7.net`	`mysite.co.uk.d1.sc.omtrdc.net`
`smetrics.mysite.co.uk`	`mysite.co.uk.112.2o7.net`	`mysite.co.uk.ssl.d1.sc.omtrdc.net`

* If you have multiple cookie domains, you must provide a separate CNAME/ARec for each domain.

4. Omniture deploys your SSL certificates to all load balancers and makes the appropriate DNS updates for the new A Record.
5. Update the CNAME settings in your DNS system.

3.3 New Third-Party Cookie Implementations

1. Contact Omniture ClientCare, or your Omniture consultant, and ask to be placed in the RDC migration queue.
2. Ask Omniture ClientCare, or your Omniture consultant, for an updated `s_code.js` file that includes, or update your existing `s_code.js` to include, the RDC domain (`omtrdc.net`) in the `trackingServer` command.
3. Deploy the updated Omniture collection code (`s_code.js`).

3.4 Migrating Current 2o7.net Implementations

If possible, plan on migrating from a third-party cookie implementation to a first-party cookie implementation (CNAME) as part of the RDC transition. CNAME implementations always result in more accurate measurement of your Web traffic. For more information, see Knowledgebase article 804, *First-Party Cookie Migration Whitepaper*, or contact ClientCare or your Omniture Consultant.

NOTE: Genesis integrations are largely unaffected by the RDC migration, unless you are using a Genesis integration where the Genesis partner hosts your JavaScript file (see Step 4).

1. Contact Omniture ClientCare, or your Omniture consultant, and ask to be placed in the RDC migration queue.
2. Perform a standard first-party cookie migration, using the RDC domain (`omtrdc.net` instead of `2o7.net`).
3. Update your `s_code.js` to include the RDC domain (`omtrdc.net`) in the `trackingServer` command (or ask ClientCare, or your Omniture consultant, for an updated `s_code.js` file).
4. Generate the new JavaScript collection code version H.19 or later that includes appropriate settings for managing the cookie domain migration.

   WARNING! You must update all collection code simultaneously to avoid data collection errors. This includes all `s_code.js` files, ActionSource media files, etc.

   During the migration time period, `omtrdc.net` automatically redirects the request to `207.net` if `omtrdc.net` doesn't recognize the visitor ID cookie. This helps identify Web site visitors during the migration, and reduces false "new visitor" hits in Web site reporting.

   Cookie domain migration settings include the following:

   - **vmk** or **visitorMigrationKey:** Defines the time period during which SiteCatalyst performs domain redirection when attempting to identify a visitor ID cookie. Supported settings include `1 month`, `2 months`, `3 months`, `6 months`, and `1 year`).
   - **trackingServer** and **trackinServerSecure:** Specifies the fully qualified hostname of the new cookie domain server. For the `omtrdc.net` conversion, this is something like: `mysite.d1.sc.omtrdc.net`.
   - **visitorMigrationServer** and **visitorMigrationServerSecure:** Specifies the fully qualified host name of the old cookie domain server. For the `2o7.net` to `omtrdc.net` conversion, this is something like: `mysite.112.2o7.net`.
5. Deploy the updated Omniture collection code (`s_code.js`).

4 Post-Transition Expectations

The purpose of the RDC environment is to increase the performance and accuracy of Omniture data collection activities. However, external issues such as Web site configuration, network infrastructure configuration, and transition decisions can affect overall RDC performance.

The following topics can affect data collection accuracy in the RDC environment:

- First-Party Domains, Third-Party Domains, and Firewalls
- omtrdc.net vs. 2o7.net
- RDC vs. Traditional DNS

4.1 First-Party Domains, Third-Party Domains, and Firewalls

Regardless of the data collection domain used, first-party cookies typically provide better performance and more accurate data collection.

- Third-party cookies are more often blocked or deleted from a visitor's system due to Web browser settings, personal firewalls, and Spyware software.
- Data sent to third party domains, such as `2o7.net` and `omtrdc.net` might be blocked by corporate firewalls. This not only prevents setting cookies, but can also prevent data from being collected within a company. Blocked image requests can cause a drop in hits from call centers and other internal traffic. If you notice a drop in traffic as a result of an RDC migration, corporate firewalls are almost always the cause.
- Some browsers, such as Apple* Safari*, block third-party cookies by default.

Blocked or deleted cookies result in increased latency due to redirects and other mechanisms used to identify the visitor.

4.2 omtrdc.net vs. 2o7.net

In most cases, the RDC domain (`omtrdc.net`) provides better performance and more accurate data collection than the traditional Omniture collection domain (`2o7.net`).

- Third-party cookie domains, including `207.net`, are more often blacklisted and therefore blocked, by Web browsers and firewalls.
- If `2o7.net` is explicitly whitelisted for data collection, make sure to do the same for `omtrdc.net`. You can also eliminate the need for whitelisting by using a first-party cookie implementation.

Blocked cookie domains result in increased latency due to blocked requests, redirects, and secondary mechanisms used to identify the visitor. Initial Omniture analysis indicates that `omtrdc.net` collects up to **4%** more hit data than `2o7.net`.

4.3 RDC vs. Traditional DNS

RDC leverages regional DNS entries to direct data collection to different DCCs based on the visitor's physical location. Initial Omniture analysis indicates that the RDC system delivers **.3%** more hit data than using traditional DNS.