Salesforce.com Data Residency Option

Business Overview

Introduction

Many organizations are using applications like Sales Cloud, Service Cloud, and Chatter – or using the Salesforce Platform to build custom applications – in order to deliver critical business processes to their employees, partners, and customers. Very often the data required by those business processes is considered sensitive in nature, including personally identifying information (PII), personal health information (PHI), financial data such as credit card numbers, customer and sales data, and confidential or proprietary information such as product specifications.

When storing such data on the Salesforce Platform, an organization must have a good understanding of how their use of public cloud services affects their ability to comply with both external regulations and internal compliance policies. Often those regulations and policies prohibit storing sensitive data on the Salesforce Platform without first ensuring data protection and compliance controls are in place.

The simplest solution to this problem is to encrypt or tokenize sensitive data before it is sent to and stored on the Salesforce Platform. The most important aspect of this solution is to make sure the encryption keys used to encrypt or tokenize and decrypt that data are managed, stored, and maintained by the customer in their environment, not as a part of the core Salesforce services or stored in a Salesforce datacenter. This ability to separate the process of encryption and decryption from the storage of sensitive data is the key to giving customers greater control over their data and achieving compliance with regulations and policies while still leveraging and using public cloud services.

This white paper introduces Salesforce.com Data Residency Option (DRO), an ideal solution for helping customers maintain data privacy compliance and control when storing highly sensitive data on the Salesforce platform. Delivering a number of unique advantages, DRO:

- Comes pre-integrated with Salesforce applications and the Salesforce Platform.
- Gives customers the flexibility to choose which data is sensitive and decide exactly how and when to protect that data.
- Runs entirely in your network, so policies and encryption keys are entirely under your control.
- Complements existing Salesforce Platform security and compliance functionality such as Encrypted Custom Fields, Apex Crypto, MyDomains, & SSO.

Trust and security are cornerstones of the Salesforce platform, and built in security mechanisms are often more than sufficient to help an organization achieve data privacy, security, and compliance. Salesforce maintains public pages with information about availability, performance,

So how do you know whether to choose the native capabilities of the Salesforce Platform or Data Residency Option? There are several key requirements that would indicate a need for DRO. For example, your organization:

- Determines that sensitive data cannot be stored outside the firewall or offshore because of either internal compliance requirements or external regulations.

- Uses risk assessment frameworks and policies to determine that data stored in public cloud services must be encrypted at rest.
- Stores PII, PHI, or financial information and needs to comply with contractual or regulatory requirements for data privacy.
- Uses the Salesforce platform to collaborate on Intellectual Property or to store information related to accounts, sales information, pipeline, or sensitive IP and wants to ensure a higher level of protection for those data types.

What is Salesforce.com Data Residency Option

Salesforce.com Data Residency Option (DRO) is an advanced solution that lets your organization benefit from salesforce.com public cloud services even when your compliance policy requires that certain data fields are only readable within the boundaries of your organization, your country, or your region.

DRO is a proxy-based solution that is installed and configured in your network, not in a Salesforce data center. Once this proxy is configured, data is sent to and stored in an encrypted or tokenized form on the Salesforce Platform. Encrypted data elements will only be viewable in their plaintext form after they have been sent back through the proxy and decrypted.

DRO policies allow customers to determine which fields are sensitive and which encryption scheme to use on each data field. DRO's encryption schemes use standards-based encryption (Advanced Encryption Standard), or Tokenization – an encryption scheme that preserves order, format, and function characteristics of the data. Tokenization preserves Salesforce platform and application functionality that would otherwise be lost if standards-based encryption is used. When data fields pass through the proxy, DRO analyzes each message and then consults its policy to determine how to encrypt or tokenize each data field and forwards the message with the encrypted data fields to Salesforce. Only encrypted or tokenized values are stored on the Salesforce Platform.

DRO is deployed as a set of services made up of an Encryption Proxy Server, a Token Dictionary stored in an external database, and an Administration and Management Server. DRO has a flexible deployment architecture that allows the Proxy to be deployed in the DMZ or behind a firewall, while the Token Dictionary and the Administration Server are typically deployed in a protected internal zone.

Encryption Proxy Server

The Encryption Proxy server acts as a reverse proxy that is responsible for encrypting and decrypting data as it passes between user agents (e.g. a browser) and/or API clients and Salesforce.com cloud services. This server is a front-end server that handles various Web protocols (e.g., HTTP, HTTPS, SMTP) and formats (e.g., HTML, XML, JSON). DRO stateless architecture allows deploying it in a High Availability configuration, with
multiple Encryption Proxies set up and fronted by a load balancer.

Token Dictionary

The Token Dictionary is an external repository stored in a MySQL or an Oracle database that contains the Token Dictionary. The Token Dictionary is used for persistent storage of values that are tokenized and maintains a map between plaintext words and randomly generated tokens. The Token Dictionary is replicated to an in-memory database on the Encryption Proxy.

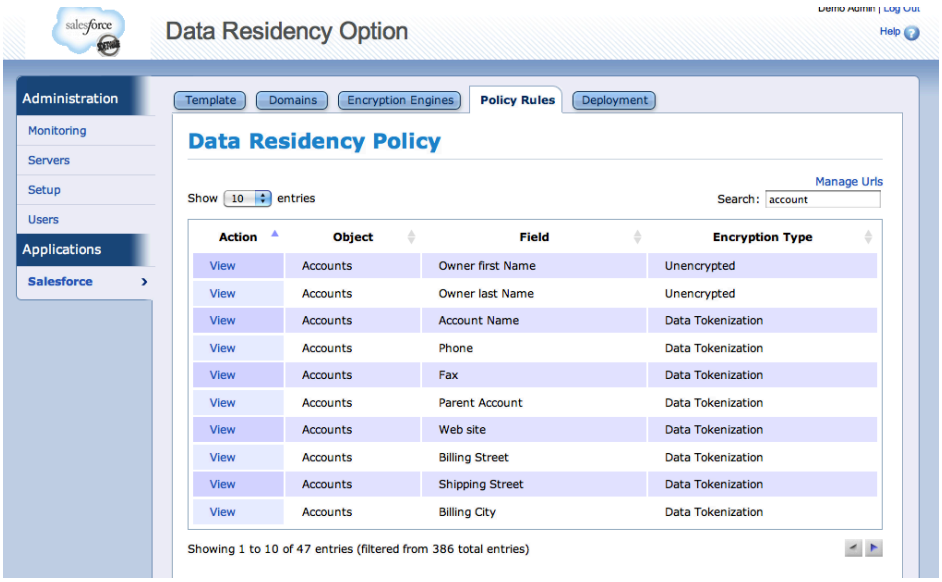
Administration Server

DRO's Administration server is a web application used to configure, manage, and monitor DRO servers, manage the data protection policy for your organization, and create, manage, and rotate the encryption keys used by DRO's Encryption Engines. From the Administration Server, you may deploy new or updated Data Protection Policies out to your Encryption Proxy servers.

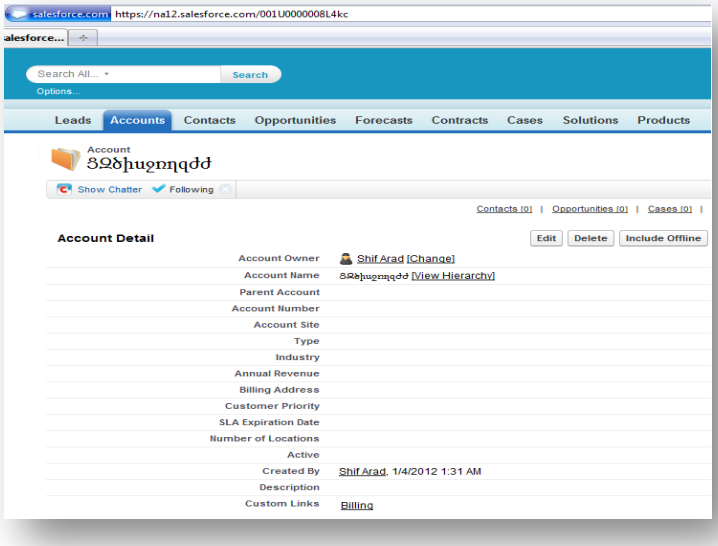
Feature	Benefit
Customer control of policies and encryption keys	Maintain control over your data even when using multi-tenant, public cloud services
Out of the box policy for standard Salesforce objects	Quickly and easily apply data compliance policies to sensitive data fields
Customize policy for your deployment	Easily add new custom objects and fields to your data compliance policy
Transparent data encryption/decryption	Data compliance policy enforcement with no impact to user experience
High performance, real-time data compliance	Maintain data compliance with negligible impact to system performance
Function/format preserving encryption	Preserves common Salesforce Platform functionality such as sort, search, and logical operations
Support for Web, Mobile and API	Regardless of where or how data is created, viewed, or managed, DRO policies are enforced
Seamlessly integrated with Salesforce Platform	Complements/extends native data compliance & encryption capabilities
Audit Trail and Event Logging	Compliance audit requirements met. Other tools can easily consume audit information.

How DRO Works

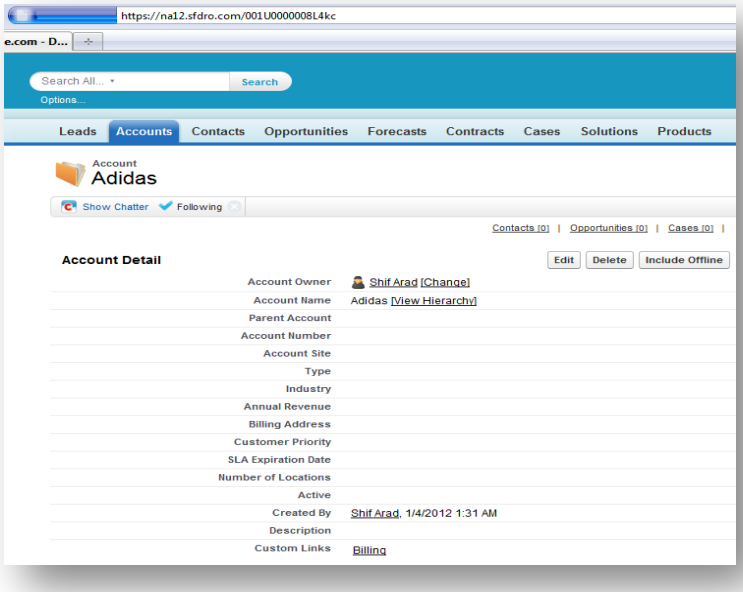
Let's take a look at a specific example: creating a new Account in your Salesforce organization. Using DRO's policy administration tool, you can create policies that define which data fields you want to protect and with which encryption scheme they should be protected. Typically these policies will be modeled either on internal compliance policies already in place or on specific external regulations. Here, we show a policy that specifies the Account Name field should be protected using the Data Tokenization engine.



Say we create a new account with the Account Name “Adidas”. The DRO Encryption Proxy tokenizes the account name value so that when stored on the Salesforce Platform, it looks like this:



However, when you view the same Account after the data has been decrypted by the DRO Encryption Proxy, it looks like this:



One of DRO's most important features is an out-of-the-box Policy Template that contains policy definitions for standard objects and fields. This Policy Template is easily extended to include custom objects and fields, giving you the ability to customize DRO to seamlessly integrated with the specific business processes you've implemented within your Salesforce organization. The DRO Policy Template is updated with each release of the Salesforce application and platform, ensuring that your data privacy and compliance policies are aligned with application functionality and updates. Using DRO's Administration Server, you can easily update, customize, or adjust data privacy policies to match the evolving needs of your business.

How Customers Use DRO

DRO is a very flexible solution that can be used by customers in nearly any region or industry to help overcome specific data privacy, compliance, and security concerns. Below are some examples of problems that can be solved using DRO in conjunction with Salesforce.

Financial Services

A large bank is leveraging the sales cloud and some custom Visualforce pages to gather "Know Your Client" (KYC) data about prospective customers and then push that data through complicated validation workflows. The bank's client services team then uses that KYC data to associate client information to an account, generate opportunities, and quote services back to the customer. After a careful evaluation of their business processes and the data they store in Salesforce as a result, the bank's data privacy group identified approximately 150 fields as sensitive. In this case, DRO can be used to tokenize those fields so that the bank can maintain their internal compliance posture – such as having to notify their customers if their data is stored offshore – as well as comply with regional banking privacy regulations
(e.g. Luxembourg, Switzerland).

Large Enterprise

A Fortune 500 company is leveraging service cloud to roll out an internal HR helpdesk to their employees. A wide variety of employee related data will be stored on the Salesforce platform, including pay inquiries, HR and personnel matters (especially sensitive would be HR complaints!), and other personally identifying information about employees. To mitigate worries about general exposure of employee data, and to address the specific concern about having their data subpoenaed by the government without them being notified, DRO allows customers to maintain complete control over their encryption keys. Since DRO's encryption keys are stored in the customer's environment and tokenized values are stored on the Salesforce platform, a separate subpoena would be required to obtain the encryption keys, serving as notification for this large enterprise customer.

Telecom

A regional telecom is building a custom Sites application on the force.com platform. This application will be used to create quotes to small business owners seeking fixed line and wireless services. In order to generate a quote the telecom needs to check the prospective customer's credit history. They use the custom application to collect and store personally identifying information (PII) about the customer, such as taxpayer ID, billing address, credit card numbers, and credit history. DRO may be used to tokenize the PII and credit data before it is stored on the platform, helping the telecom to meet data privacy and regional residency requirements while still leveraging the power of the Salesforce platform.

Summary

When storing sensitive data in the cloud, an organization must consider privacy, audit, and regulatory compliance requirements and determine the controls that satisfy those requirements. Sensitive data that cannot be stored outside the firewall, or offshore, should be encrypted or tokenized prior to being stored on the Salesforce Platform. DRO is a simple solution for providing data privacy, regulatory, and internal audit compliance for customers that store sensitive data in Salesforce. DRO is a proxy-based solution that is installed and configured in your network, not in a Salesforce data center to help an organization to achieve data compliance in more stringent regulatory or internal compliance environments. What makes DRO really different is the encryption keys are stored and managed where DRO is deployed – in your environment. As a result, DRO gives you control of how, when, and where you encrypt and decrypt your data.