Disaster Recovery/Business Continuity Plan Summary

Overview: Business Continuity Management at Salesforce.com (SFDC) is under the direction of the Vice President of Enterprise Risk Management and Business Continuity Planning. The Executive Vice President and Chief Financial Officer is the executive sponsor.

Crisis Management Team: SFDC has a Crisis Management Team (CMT) that is comprised of select executives from key departments at SFDC. The CMT is activated or enabled when a crisis or significant event occurs, and is responsible for evaluating the situation and responding accordingly. Depending on the severity of an incident the CMT Leader may request engagement from various support teams to assist with the mitigation of the incident. The CMT meets on a periodic basis for training, education, and review of the documented CMT Action Guide, or as required due to a crisis or significant event. CMT members have a specific role and set of responsibilities and are expected to be available at all times (24/7/365). The CMT conducts table-top exercises, at minimum, once per annum.

Emergency Response: SFDC has Emergency preparedness plans that provide additional emergency preparedness, response information, instructions, and guidelines to protect the safety and well-being of employees and guests if an emergency situation transcends the Landlord's facility emergency plan.

Pandemic Planning: SFDC has implemented a pandemic preparedness plan, which was created and validated by International SOS, a world leading provider of medical assistance, international healthcare, security and travel services. The plan enables employees to respond effectively and efficiently to a pandemic using a phased approach, helping to ensure essential operations are maintained and minimizing transmission of the pandemic virus among employees, customers, and partners.

Business Continuity Planning: SFDC has business continuity plans (BCP) for critical business functions. BCPs are reviewed at least twice a year, and are tested on an annual basis.

Enterprise Risk Management: SFDC conducts an annual enterprise risk assessment, focusing primarily on operational risks. The enterprise risk management program also incorporates business continuity planning, SOX Compliance, and ISO 27001. A risk assessment council meets periodically to discuss current and emerging risks.

Production Site Recovery Methodology: To maximize availability of the SFDC service, the service is delivered using top tier, enterprise-class data centers. Each data center provides production services for a set of points of delivery (PODs) and disaster recovery (DR) services to other PODs. Salesforce.com also maintains a separate production-class research and development lab and data backup archive facility. All data centers utilize carrier-grade components designed to support millions of users at the highest levels of performance and availability. Extensive use of high availability servers and network technologies, combined with multi-carrier and carrier-neutral network strategy, mitigate the risk of single points of failure and provide a highly resilient environment with maximum up-time and high performance.

In terms of data integrity, salesforce.com performs remote data vaulting of all production PODs to a geographically remote, full-scale DR site. Should there be a catastrophic failure at the PODs' primary facility or another type of disaster affecting that facility, SFDC would initiate its disaster recovery process. Recovery would be performed locally on-site at the PODs' primary production data center if the recovery could be completed within SFDC's recovery time objective (RTO) and recovery point objective (RPO). If recovery could not be completed at the PODs' primary production data center within SFDC's RTO and RPO, recovery would be performed at the PODs' remote DR site data center.

SFDC utilizes "tiered" storage solutions in very large SAN storage arrays from Hitachi and EMC. Hitachi's Shadow Image and EMC's TimeFinder technologies are used to perform real-time disk-disk snapshot replication of the data within each individual SAN storage array at each data center, while Hitachi's True Copy and EMC's Symmetrix Remote Data Facility (SRDF) technologies are used to perform near real-time data replication between the PODs' primary production data center and the PODs' remote DR site. Data is transmitted across a dedicated encrypted link.

Nightly tape backups are also performed at all the production data centers, and a copy of each nightly backup is transmitted to our secure data center archive facility. Tapes never leave our secure data center facility.

Revision Date: December 28, 2011

Focus on Infrastructure

Near real-time replication

Validated disaster recovery strategy

Tape Backup Schedule- Multiple Full / Multiple Incremental

Customer facing - Carrier neutral network strategy

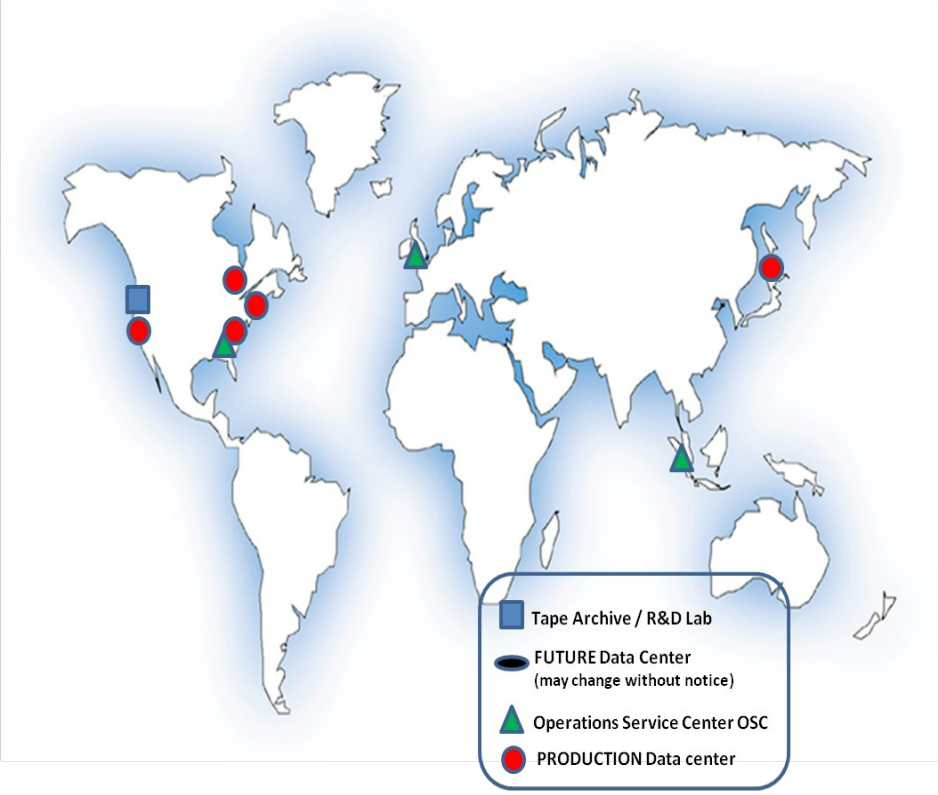
Internal - Secure encrypted MPLS / VPLS Network Architecture (point-to-point data replication)

Recovery Time Objective (RTO) = 12 hours, after "declaration"..

Damage Assessment Time = "up-to" 4 hours.

Recovery Point Objective (RPO) = 4 hours

NOTE: Total time to a Recovery state of core services from time of event is 12-16 hours depending on damage assessment time.



Data Center Recovery Planning Progress: As a part of developing a viable disaster recovery plan and program for the production environment and platforms, SFDC conducts a disaster recovery exercise at least once per annum.

The scope of the disaster recovery exercise is to validate the ability to failover (simulated) a production POD from the primary data center to the secondary data center utilizing developed operational and disaster recovery procedures and documentation.

Key elements of proof include:

- Network access
- Hardware and / or server component accessibility (POD)
- Application(s) accessibility
- Data currency (RPO)
- Plan elements are reviewed and updated
- Task, script and procedures remain current

The disaster recovery teams, on numerous occasions, have successfully brought up a production POD instance in a secondary data center with customer participation; run-book, script processes and individual tasks were validated; data-loss potential was measured and well within current stated limits; customers have successfully completed their disaster recovery exercise tasks in the secondary data center in an extended maintenance window.
Additionally, disaster communication processes were exercised utilizing the mass notification system, which included call-outs with response requests to SFDC's Crisis Management Team (CMT) and the production disaster recovery teams.

SFDC will continue to test its disaster recovery plan at least once per annum.

Data Center Facilities: The Salesforce.com service runs from various enterprise-grade data centers globally. Cameras (static, PTZ and IR based) provide interior and exterior surveillance, monitored by onsite security guards

around the clock. Various combinations of Card-key access, PIN-based & bio-metric system restrict access to and within the data center. Electrical power, telecommunications, and environmental systems (cooling, fire suppression, etc.) are fully redundant with redundant uninterruptible power supply units, diesel generators, and water supplies available for emergency use. Heat, smoke, fire detecting and suppression systems are strategically located throughout the facility with special attention paid to the reliability of the support systems. Advanced building logic control systems monitor temperature, humidity, and other environmental conditions. Notification via email/paging mechanisms and onscreen dashboards display all critical functions and any alarm conditions.

Power: Various UPS solutions are used including chemical based battery strings and rotary based flywheel technology setup in a N+1 at the UPS level and N+1 at the emergency/generator power level. Both solutions can provide Salesforce.com an uninterrupted power supply while the load is being transitioned to emergency/generator power in the case of a utility outage. All data centers have power capacity to support the load for the entire facility for a minimum of 48 hours on emergency generator power with multiple vendors to supply fuel as required. In the event of a critical data center facility service impacting failure or disaster, Salesforce.com has the ability to transition to a full scale, data replicated, geographically diverse alternate data center.

Staffing in the Event of a Disaster: The services provided by SFDC are based on a multi-tenant application. All staff resources would be dedicated to restoring the service of the SFDC site if the site were to go down. Each customer's org would be recovered in unison with the instance that contains its org.

Activation/Notification: The SFDC Premier Support Team has processes to contact Premier Support customers' designated representatives in the event of a declaration of a disaster. In such an event, SFDC Premier Support will maintain communications with Premier Support customers, and provide feedback to SFDC's operations teams regarding the effectiveness of recovery.

In the event of an actual declared disaster (including a force majeure event), and such disaster is not fully addressed in this Disaster Recovery/Business Continuity Plan, SFDC will use commercially reasonable efforts to provide disaster recovery services to restore the service to customer as quickly as possible.