



Keeping your data secure
is as important to us
as it is to you.

Team Portal Online – Platform and Security

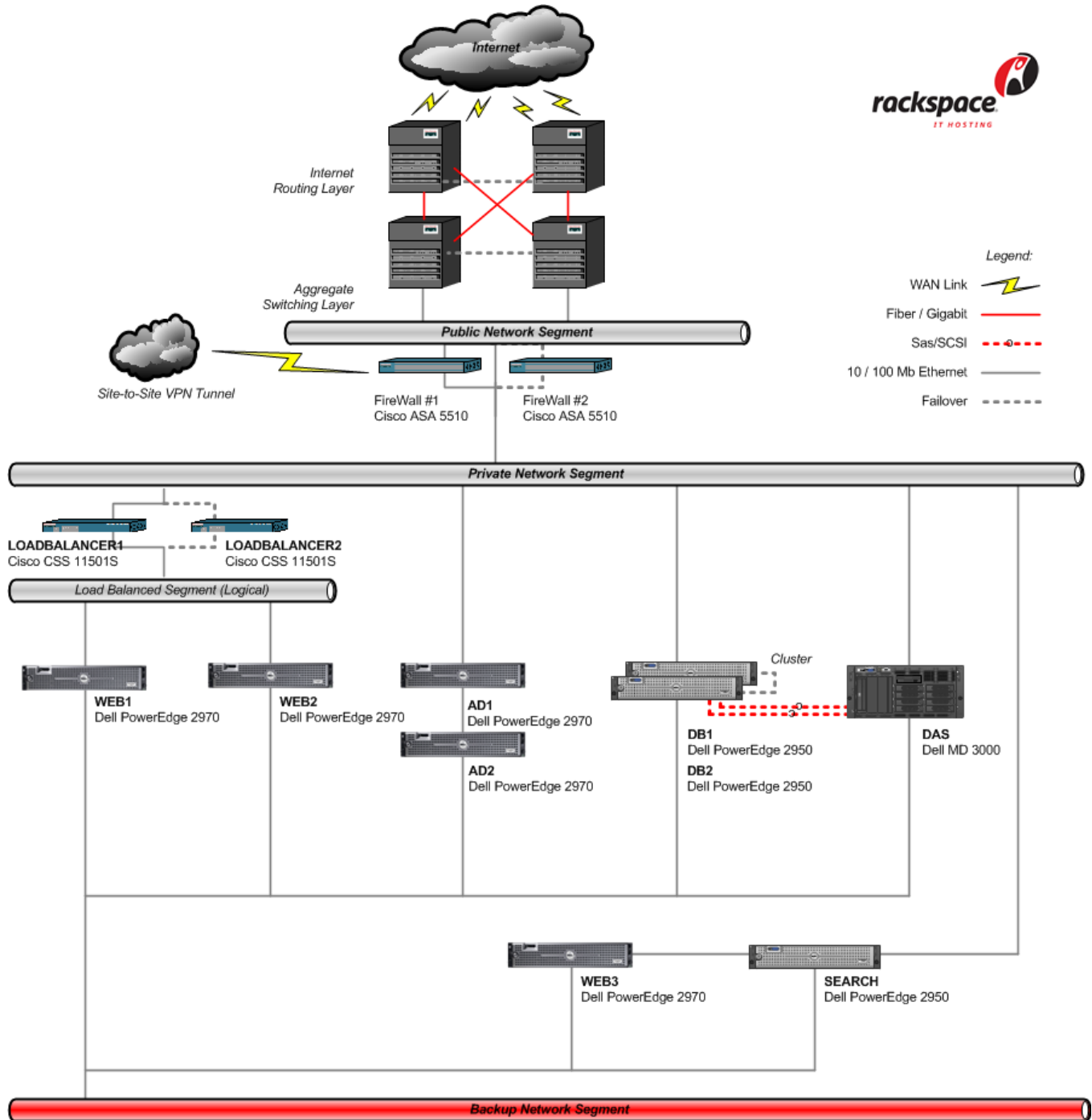
Securing our customers

We take security very seriously, and strive to make our solutions and hosting environment as secure as possible.

Features

- Today's platform is built to host millions of users
- Team Portal can manage N SharePoint 2003, 2007 and 2010 farms
- High availability (100% network, 99,9% application)
- 2 x Firewall
- 2 x LB
- 3 x SharePoint
- 2 x AD
- MS SQL Cluster
- 2,8 TB storage
- Platform hosting and security by Rackspace

Logical Diagram



Legend:

WAN Link

Fiber / Gigabit

Sas/SCSI

10 / 100 Mb Ethernet

Failover

Team Portal Security

“This is the best security documentation from a hosting provider I’ve ever seen, and I’ve seen a lot...”

Artea Beirn CISSP CISA, Information Security Officer, XL Global Services

Systems Security

We have extensive experience in developing solutions with a high degree of security. Using only market leading tools and software, we ensure the stability and security of our infrastructure. This foundation enables us to develop services of tomorrow.

Our services and solutions have several built-in security features, including:

- SSL Encryption: End-to-end encryption to keep you and your data secure
- Recycle Bin: Never lose a document again with the SharePoint recycle bin
- Data protection including secure backup and restore from CommVault

Hosting Security

NetConnect use Rackspace for all hosting, ensuring the highest level of security for all our customer data. Rackspace are serious about security, guaranteeing the systems, the operational environment, and the physical environment. They employ strict routines for monitoring and accessing data, and only the most advanced and secure software and hardware.

Some of the Rackspace hosting environment features:

- SAS 70 type II, the review report can be provided
- ISAE 3402 (International) and SSAE 16 (US) will replace SAS 70 from June 2011
- Safe Harbor certified (EU Directive on Privacy (95/46/EC))
- ISO 27002, 27001 and 9001:2008
- PCI-DSS compliant as a Level 1 Payment Card Industry (PCI) Service Provider
- Microsoft Gold Certified Partner
- **Leverages energy efficient hardware in data centers to reduce CO₂ emissions**

Security Standards and Certifications

Security standards / Certifications	YES
SAS 70 type II, the review report can be provided	✓
ISAE 3402 (International) and SSAE 16 (US) will replace SAS 70 from June 2011	✓
Safe Harbor certified(EU Directive on Privacy (95/46/EC))	✓
ISO 27002 , 27001 and 9001:2008	✓
PCI-DSS compliant as a Level 1 Payment Card Industry (PCI) Service Provider	✓
Microsoft Gold Certified Partner	✓

ISAE 3402 (International) and SSAE 16 (US) Replacing the SAS 70

Service Organization Reports – End of an Era

SAS 70 A Brief History

The Statement on Auditing Standards (SAS) No. 70, was developed by the American Institute of Certified Public Accountants (AICPA) as the guide to independent auditors in the issuance of an opinion on a service organization's description of controls in the form of a Service Auditor's Report. Section 404 of the Sarbanes-Oxley (SOX) Act of 2002 brought the report to prominence.

Why Replace the SAS 70?

SAS 70 is just one of many periodic statements issued by the AICPA's Auditing Standards Board. With the passage of SOX there came new auditing standards from the Public Company Oversight Board (PCOAB). There was also a need to have a report that could be used internationally. This led to the creation of two new reports.

ISAE 3402 (International)

The International Standard on Assurance Engagements (ISAE) No. 3402 was developed by the International Auditing Standards Board (IAASB) and goes into effect June 2011.

SSAE 16 (US)

The Statement on Standards for Attestation Engagements (SSAE) No. 16 developed by the AICPA and designed to mirror the ISAE 3402 goes into effect June 2011.

What Changes will affect Rackspace?

There are some minor changes such as the addition of an attestation by the management of Rackspace. However, most of changes are in the area of guidance to the Service Auditor.

What remained the same?

There are still two types of Service Auditors Reports; a Type I and a Type II. In the Type I report, the service auditor will opine on whether the controls were in place on a specific date and if the controls are suitably designed to achieve the control objectives. In the Type II report the auditor opines on whether the controls were in place during the audit period, if they are suitably designed to achieve the control objectives and tested to note if they are were operating with sufficient effectiveness to provide, reasonable, but not absolute, assurance that the control objectives were achieved during the period of examination (typically 6, 9, or 12 months).

Rackspace and the Service Organization Reports

Rackspace is a global company and recognizes the need to assist all of their customers. Rackspace will have a single Type II Report on controls issued by our service auditor which will have an opinion to satisfy both customers needing ISAE 3402 and those that need SSAE 16. Rackspace is also changing its audit period for this report from a 9 month (January 1 to September 30) to a 12 month audit period (October 1 – September 30).

Customers can expect the ISAE 3402 (International) and SSAE 16 (US) report to issue in mid-to-late November, 2011

ISO 27002 / 27001

ISO 27002 is a collection of industry standard information security best practices and guidelines. As such the standard is non-prescriptive and no audit against it exists.

ISO 27001 defines how to design and implement an Information Security Management System. This system can then be audited for compliance against the standard, resulting in certification.

You should hopefully be able to download a copy of the ISO 27001 via the below link

<http://client.certificationeurope.com/print/5053>

ISO 9001:2008

The Rackspace quality management system is presently being structured to meet the requirements of the ISO 9001:2008 (standard for quality management). Although we currently do not have a quality management policy for public consumption, this policy document will be a key output of the compliance exercise.

A recent ISO 9001 gap analysis, conducted by an external certification body, identified the existence of quality processes and procedures at Rackspace. These processes and procedures form part of our commitments to other compliance initiatives (SAS 70, ISO 27001) that include elements of quality management. We hope to build on this foundation to ensure the implementation of a quality management system that provides the appropriate level of assurance in our service delivery.

We currently use Six Sigma and Kaizen as our approach to continuous improvement and quality management. We believe that the customer experience is the reason we are here and we use various feedback mechanisms as the input to Kaizen projects that we execute.

We have a Lean Six Sigma Process Excellence team in the UK and US, as well as a Service Innovation Team mandated to deliver step changes in the way Rackspace delivers Managed Hosting. We rely on a Net Promoter Score (NPS) driven customer loyalty approach to ensure that our customers are heard and our best practices reflect the diverse needs of our customers. Rackspace currently has a number of suitable procedures for quality control that are assessed annually as part of our SAS70 review.

PCI-DSS

Rackspace is certified as PCI-DSS compliant as a Level 1 Payment Card Industry (PCI) Service Provider; we are not given a certificate on accreditation, but could provide a letter of acceptance if you require this?

The scope of Rackspace's accreditation is: Physical security for:

- All US and UK Offices
- All UK Data Centres
- Hong Kong Data Centre
- US Data Centres:
 - Herndon, VA
 - Chicago, IL
 - Dallas, TX
 - San Antonio, TX (SAT2 only)
- Network Infrastructure (Routers and Switches)
- Rackspace employee access to Network Devices

Excluded from the scope are:

- Any US Data Centre not listed above
- Amsterdam Office
- Customer hosted solutions

Team Portal Security Measures

Security Measures	YES
All transactions are logged, including read-only access. For example, logging of read, modify and delete transactions including a timestamp.	✓
All changes to data values are tracked. For example, capturing information such as created by, created date, modified by, modified date, and old value in a history table in a database is considered sufficient.	✓
All Team Portal access is retained for at least 90 days	✓
Team Portal uses a role based access control and/or discretionary access control mechanism and has a designated administrator.	✓
Administrative changes are logged for account and auditing review.	✓
The data is behind a firewall and conforms to documented Threat Management Standards.	✓
The Company requires that all stakeholders and support personnel read and comply with the established IT Security Standards.	✓
All administration changes and functions are fully logged.	✓
All access failures, including failure to log into the Team Portal, are recorded and maintained.	✓
Strong password methods are enforced and in compliance with company Password Standards.	✓
Unsuccessful login attempts will temporarily disable or suspend accounts.	✓
All applications are in compliance and meet the company password standards.	✓
Passwords in storage are protected by an encryption algorithm.	✓
Passwords are encrypted in transit during the authentication process.	✓
Shared IDs are NOT used with Team Portal.	✓
An IT Termination Procedure is in place, and the application/system administrators follow the established procedures.	✓
Idle session timeouts are implemented and timeouts are provided.	✓
The web service keeps a valid access log.	✓