Technical Architecture Overview

TMS Analysis system

Last modified: 29/01/2018 12:15:00 PM

1. Management Summary

This document provides a functional and architectural overview of the smartanalysis system.

Smartanalysis is, first and foremost, a comprehensive data analysis and reporting platform for commercial Transport Operator companies. The system captures, stores and manages, analyses and reports on data captured from multiple sources - which currently is primarily analogue and digital Tachographs.

Smartanalysis has been operational for over 20 years. TMS analysis software is today in use for analysing data for over 2000 companies with a combined total of over 8,000 depots.

2. System Architecture

The TMS Digital Tachograph Solution (smartanalysis) is hosted on fully operational mirrored servers located at Rackspace in Slough, https://www.rackspace.com/en-gb/managed-hosting these became operational 07/11/2009.

To this end the detailed system architecture beyond the 'Consumer' layer (i.e the client interface layer) is not discussed in detail in this document.

Please see Figure 1 for an overview of the Smartanalysis architecture.

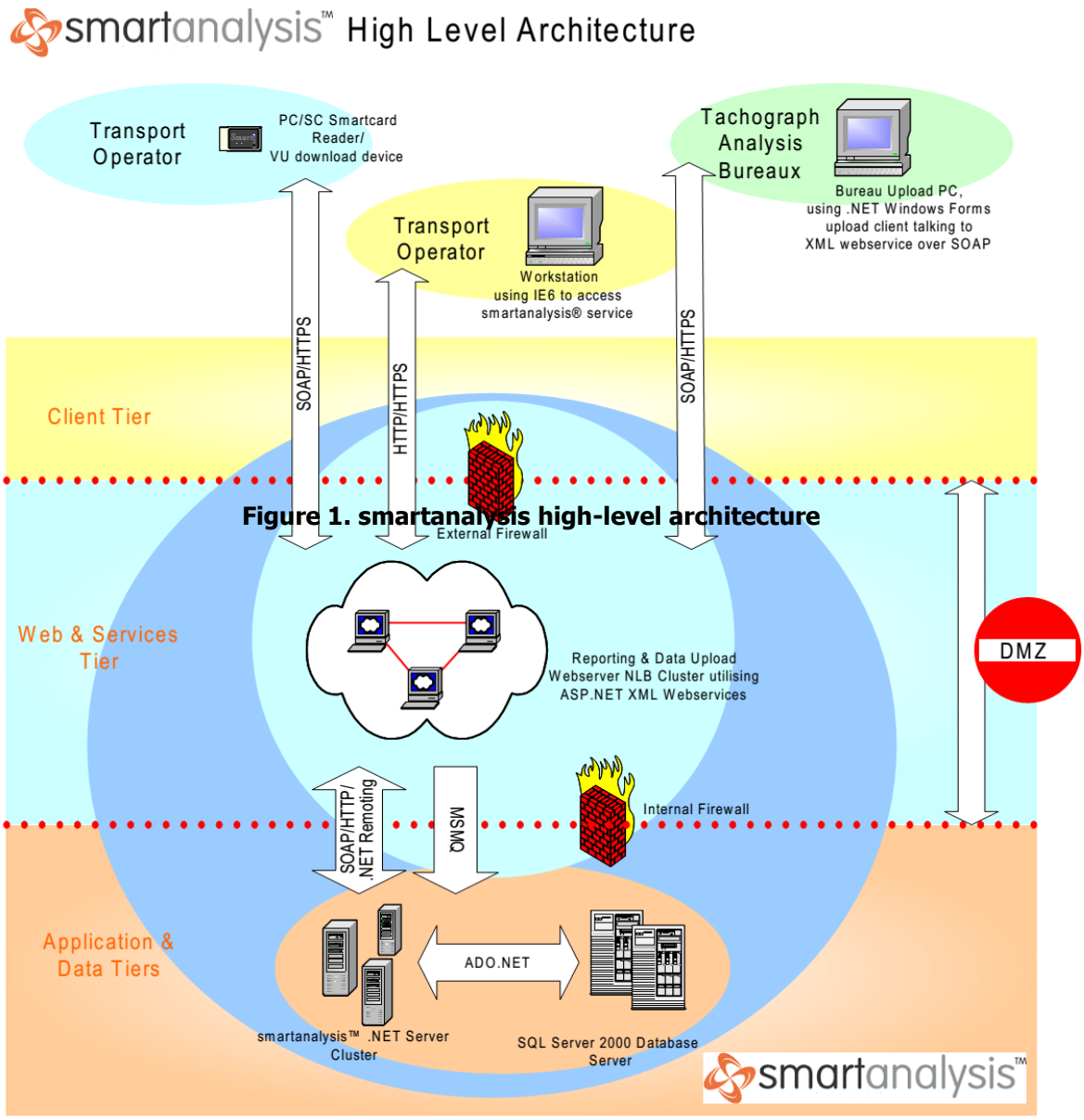

Figure 1. smartanalysis high-level architecture

Figure 1. Smartanalysis high-level architecture

Smartanalysis is based on n-tier architecture, utilising the following technologies:

- Microsoft .NET 1.1, 2.0 and 3.5 platform for all server components
- Microsoft .NET 1.1 platform for downloader clients deployed at company locations.
- ASP.NET website providing the client interface to user authentication and authorisation, system administration, data management and reporting
- ASP.NET XML webservices providing an external services interface layer to the smartanalysis server functionality
- HTTPS/SSL (128 bit) for encryption and secure connection protecting sensitive data
- SQL Server 2008 DBMS for enterprise database performance (upgraded from SQL Server 2005 to 2008 in November 2009)
- SQL Server Reporting Services 2008 for highly flexible and scalable management information reporting
- ADO.NET for data-tier integration with SQL Server
- Windows Network Load Balancing (NLB) for management of server capacity and redundancy. NLB manages load distribution and server failover at the webserver (IIS) level for the smartanalysis website and ASP.NET webservices. Web session state management is managed by SQL Server.
- Microsoft Message Queuing (MSMQ). MSMQ is used where interprocess data communication is asynchronous – primarily for data upload from remote locations. MSMQ receives and stores messages containing compressed data from digital and analogue tachographs. MSMQ ensures reliable receipt and buffering of data between asynchronous processes running in locations either local or remote to each other.

1.1. Web & Services Tier

This tier provides the interfaces to the external world.

The smartanalysis website forms the system-user interface for access to most of the functionality described in the use cases in the Functional Specification section of this document. This functionality includes the following key features:

- System user administration tasks
- Management Information reporting (digital & analogue tachographs)
- Compliance reporting (digital & analogue tachographs)
- Report and subscription administration

The website is built on the ASP.NET 3.5 platform. The following subsections detail the key components of the website.

1.1.1. Security – Authentication and Authorisation

Smartanalysis website security is divided into two key areas: Authentication and Authorisation.

Authentication is concerned with the identification and verification of users that have permission to access the smartanalysis system. Smartanalysis, in common with most other secured software systems, uses a combination of user-unique username and password for identification. Usernames must be unique across the system, and passwords are stored on the smartanalysis in encrypted form. Future developments of smartanalysis could include other methods of authentication such as smartcards or biometrics. These developments would be undertaken in response to customer requirements.

Authorisation is concerned with identifying what a user is allowed to do within smartanalysis once they have been successfully authenticated. smartanalysis is built around a 'user-role-permissions' authorisation model, where users – when they are added to the system - are assigned to an existing role or roles. Roles, in turn, are assigned permissions and it is ultimately these permissions that govern what features and functionality a role (and therefore the users assigned to the role) can see and access within smartanalysis.

Smartanalysis uses a 'User Manager' webservice component to control authentication and authorisation, the API and core of which is common across all applications developed by Exentra. This means that for future developments the application security can be changed, adapted and updated as necessary in isolation from other applications.

In addition access to the website is managed by IIS 7 security, and ASP.NET 'Forms' authentication. Forms authentication works in conjunction with the smartanalysis authorisation components to ensure that access to web pages through web browsers is impossible without the correct credentials. The following additional features are provided by smartanalysis:

- Attempts to browse to bookmarked pages or reports within the smartanalysis website without logging in will be blocked, and redirected to the login page.
- Attempts to login with a known username but an incorrect password are counted and logged by smartanalysis, and after 3 rejected attempts the user account is locked – preventing further access by the username in question. The account can only be unlocked by a system administrator.
- If a user forgets their password, they can request that it be sent to them at their previously specified email address.
- System administrators can disable user accounts at any time – preventing access by the specified user.

Deployment Infrastructure & Disaster Recovery Architecture

The smartanalysis system is deployed in two geographically separate datacentres, operated by Rackspace (www.rackspace.co.uk) who are the 'World's leading' provider of hosting solutions.

This is an extract from Rackspace documentation:

"The Rackspace® network has been engineered from the ground up to accommodate the high-availability demands of our customers' mission-critical Web applications. Our Cisco-powered, Zero-Downtime Network with unique self-healing attributes is based on multiple bandwidth providers and BGP4 (Border Gateway Protocol) for best case routing. This ensures the data reaches the end user in the fastest, most efficient manner possible. This allows us to deliver on our 100% infrastructure availability guarantee.

Rackspace provides a fully resilient and redundant network infrastructure. Our entirely switched network employs Cisco chassis based switches running HSRP (N+1 hot failover) to ensure that data can be routed even in the event of device or link failure.

Key Features of the Rackspace Network Infrastructure:

- Multiple Tier 1 providers
- 3 Data centres in West London and 1 in Slough
- Fully redundant network at many different levels
- Power redundancy
    - Provider redundancy and diversity
    - Fibre carrier redundancy and diverse entrances to our facilities
    - Hardware redundancy through the use of redundant routers with failover links (fully meshed)
    - Multiple routing protocols for scalability, stability and failover routing in the event of a hardware or uplink failure
- Total of 27 Gbps aggregate bandwidth across the four data centres
- Network traffic is constantly monitored and usage remains significantly below capacity at all times (currently approximately 20%) to the network to accommodate even the largest spikes in traffic.

- Rackspace utilise tools to monitor traffic anomalies, such as DDoS attacks. We also collect traffic statistics to best determine where the majority of our traffic comes from - this helps in the future planning of adding new providers that can best serve our customers
- As network utilisation reaches 30% we automatically add more network capacity to ensure customers never experience network degradation
- Peering with LINX (London Internet Exchange) ensures superior connection speeds through direct links with all major European Service Providers.
- 100% Network Availability SLA"

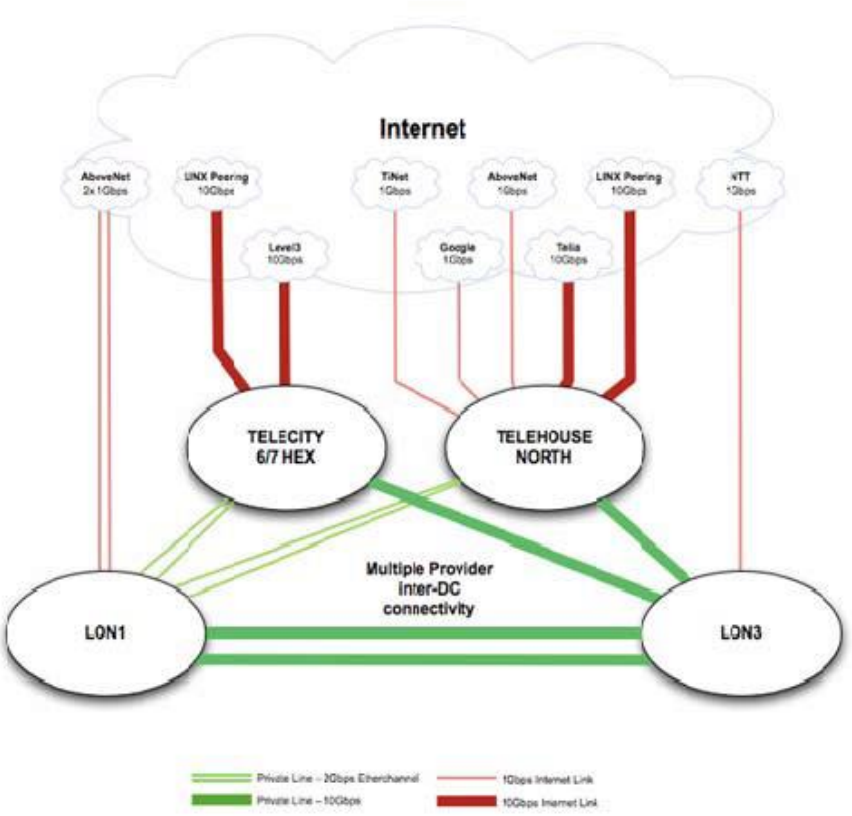

Figure 2. Rackspace network infrastructure

We work with Rackspace because they provide a second-to-none hosting solution that could only be offered by an organisation of their size and experience.

We maintain a 'primary' server setup, and a 'mirror' server setup. The primary servers reside in the 'LON3' datacentre, and the mirror servers reside in the 'LON1' datacentre. We employ two technologies to ensure latency between primary and mirror sites is typically of the order of <2 minutes (for large bulk inserts, this can be longer):

- SQL Server 2008 Mirroring. Operating in high-performance mode, with auto-failover ensuring that maximum performance is maintained whilst ensuring data latency is kept to an absolute minimum.
- Microsoft SyncToy. A Microsoft power utility used to synchronise files and folders between the primary and mirror locations. Latency is in the order of <1 minute.

See Figure 3 for an overview diagram of how the smartanalysis system is deployed.

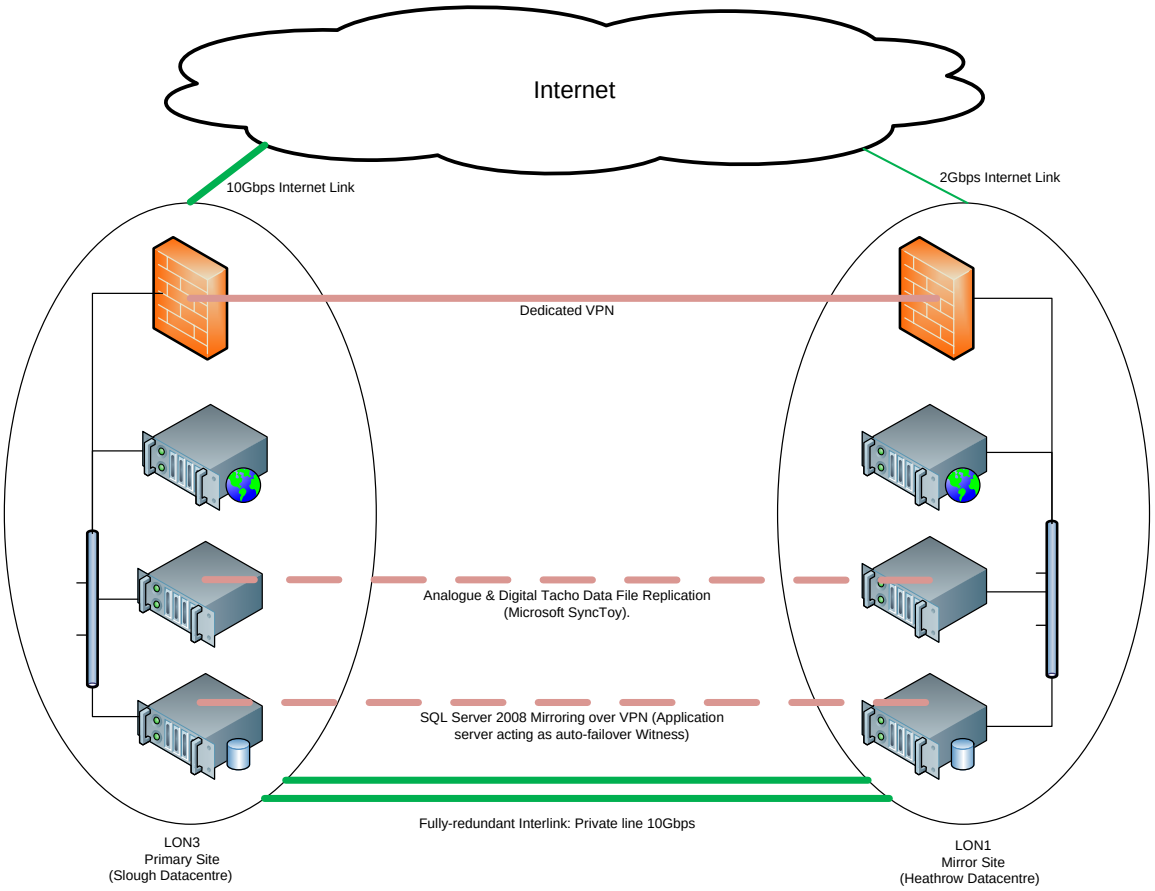

Figure 3. smartanalysis deployment infrastructure

Additional Information on Access Controls, Procedures & Technologies

- All web user access is protected using HTTPS over TLS. The encryption algorithm is SHA256 using key length 2048 bits.
- Access to Smartanalysis is role based used access using username and password. Password polices are applied.
- Communication over our web service API is also protected using HTTPS over TLS. The encryption algorithm is SHA256 using key length 2048 bits. This service also requires user authentication.
- Communication between data layer and user layer is secured by encryption.
- Access to database is permitted to authorized and authenticated users only controlled by secure VPN, etc.
- FTP connections are SFTP