IT Infrastructure

The current IT infrastructure of the Autonomous Province of Bolzano

Ver. 1.0

IT Infrastructure - Ver. 1.0

The current IT infrastructure of the Autonomous Province of Bolzano

08. Mar. 2016

Author:

Andreas Santer, reviewed by Andrea Cuzzolin, Fabio Tirapelle e Zeno Moriggl

This document describes the current IT infrastructure of the Autonomous Province of Bolzano.

Content

1. Abstract

This document describes the **current IT infrastructure** of the production environment of the Autonomous Province of Bolzano.

2. Physical Infrastructure

This chapter describes the physical infrastructure of the production environment of the *Autonomous Province of Bolzano*.

2.1. Network

The topology of the network connecting the offices of the Public Administration of the Autonomous Province of Bolzano (PAB) is quite heterogeneous and characterized by

- different connection speed (offices are connected to the central data center through fiber link or xDSL with different bandwidth);
- limited transparency (technologies such as NAT and PAT are frequently used for masquerading and organizing subparts of the network);
- a considerable number of firewalls within the boundaries of the PAB;
- a huge number of routers owing to the physical segmentation and the resulting subnetting.

2.2. Sites

The concept of sites is supported by Microsoft® Windows supported by Active Directory (see Operating Systems). A site is a part of the network characterized by high and cheap bandwidth. LANs a are natural candidates, and a site may span multiple IP subnets.

The subdivision of the network into sites is the base for the "*site awareness*" approach (natively supported by Microsoft Windows and extended to in-house built applications), which allows clients to identify and access the most performing and the cheapest (mostly it is the "nearest") instance of redundantly deployed services.

The whole network of the *Autonomous Province of Bolzano* is subdivided in such sites. (usually there is one site for every geographical location, but in well connected central zones there are sites, like *bzbzmitte, bzbzamba, bzbzcris000100*, which include a huge number of offices and cover a wide territorial range).

Details on the concept of sites can be found in the chapter about "***Operating Systems***" and system services.

2.3. Operating Systems

When it comes to operating systems the landscape has started quite homogeneous and has in the last years seen a proliferation of versions. Currently we are in a phase of consolidation.

The following server versions are running in the production environment:

- **Microsoft® Windows Server 2003** through **2012 R2**
- **Red Hat Enterprise Linux 2** through **7**
- **CentOS**
- **IBM AS400**

The clients have all been migrated to **Windows 7 Enterprise SP1**.

ESX VMWare is used for virtualization.

Almost all servers and clients are members of the prov.bz forest (single domain).

Services:

The concept of the Windows 2003 domain has been adopted for various reasons, amongst other things for the distribution of the offices over the territory, connected by low bandwidth and originally burdened with high traffic costs. The operating system services offered by Windows (including authentication and access to distributed resources through the *Distributed File System / DFS*) are designed to support sites as described above: they are natively *site-aware* (see previous chapters). Of course this approach requires that every site must provide the most important services like *DC (Domain Controller), GC (Global Catalog)* and *DNS (Domain Naming System)*.

This system involves various key benefits:

- The connections that go outside the site are reduced to a minimum (with all related benefits, like less traffic and reduced costs);
- The system still works if the WAN-connection fails;
- The system still works if the site-servers cease working, as long as the WAN connectivity is in place: redundantly deployed services allow for a fail over concept.

Internet access and E-Mail services are centralized.

Active Directory:

Active Directory is multi master replicated with a hub-spoke topology and replication schedules varying from 15 minutes to 3 hours, depending on the bandwidth.

Client and software installation:

The clients (***Microsoft® Windows 7, SP1***) are automatically installed with *HEAT Client Management* which allows to run unattended installations through the network.

In most cases the installation process itself is performed by the **Windows Installer**; therefore software should be provided as .msi package (or .msp if it is a patch). The clients are installed with **Microsoft® Windows 7 SP1** in the English version and are localized by MUI-packages.

3. Logical Infrastructure

3.1. System Directory

The directory system and main configuration source used is ***Microsoft© Active Directory*** of Windows 2003, with a single forest and a single domain (prov.bz).

The original concept for a directory as intended by *Microsoft*, which is mainly focused on the administration of users and network resources, was amplified in order to implement companywide logic. The ***ProvLogon*** uses the Active Directory as a source to automatically configure a user's environment when he logs on to the system. The functionality to retrieve the configuration from Active Directory is also available through web services, which are part of the SOA used within the province. This is intended as simplification and standardization for all other applications which may need configuration information. (Active Directory would of course be accessible also directly through the open standard protocol *LDAP V.3,* but the additional logic that has been introduced would have to be interpreted).

The mentioned configuration logic follows these rules:

- Correlation one-to-many between **users** and **organizational units**.
- Definition of **administrative roles** and association of these roles with the **users** for every configured **organizational unit**; therefore a user who has multiple offices assigned might have different roles in different offices.
- Representation of the **physical position of hardware components** like computers or printers by considering the following detail information: region (province), city, street, house-number and physical subpart of the house (e.g. floor or room). This information is used to discover the resources that are available for a certain user due the fact that he/she is using a certain computer (in a specific location).
- Correlation many-to-many between **offices** and **house-numbers**, used to be able to offer certain offices to a user based on the physical position where the user is accessing the network (based on the mentioned known location of the computer).
- Definition of **server roles** and assigning these roles to a server offering certain services; therefore – by following the site-awareness concept of Windows 2003 – it is possible to discover the servers offering services within the own site.
- Correlation one-to-many of **computers** to "logical" **offices**. (This is an assignment which is not retrieved from the physical location of a computer, but which is assigned explicitly.)
- Configurations for "**site aware" applications**

4. Security Infrastructure

4.1. System Access / Authentication

It was the intention of the design team for the Windows 2003 domain *prov.bz* to provide and use single sign on (SSO) functionality to all important services of the information system of the *Autonomous Province of Bolzano*. Of course an immediate consequence of this approach is the need to strongly protect the access to the operating system.

The default authentication of the *Windows 2003* system is *Kerberos v5*, an open standard which provides functionality to assure that two partners (e.g. a client and a server) can authenticate to each other by using a third, reliable partner (the *Kerberos* service). *Kerberos 5* is considered very secure and was implemented also by various other operating systems (which would make it possible that also a non-Windows client could access a *Windows 2003* server).

In the domain *prov.bz* are active the following authentication policies:

- The authentication on the system is done through a **username and a password**.
- The password must be **at least 8 characters** long.
- The password must match certain **complexity rules**:
    - It must contain at least **3** of the following **4** character groups: *uppercase characters (A through Z) - lowercase characters (a through z) - Numerals (0 through 9) - Non-alphabetic characters (such as !, $, #, %)*
- The password can't be the same as one **of the last 5 passwords**.
- The password must be changed **every 90 days**.
- The password can be changed only **one time within 24 hours**.

4.2. File System Access

Access to the file system on a *Windows 2003* fileserver (there exists at least one in every site) is managed through Integrated Security. To access a certain resource/drive the client requests a ticket from the nearest *Key Distribution Center* (KDC – any domain controller). The server allows or denies access by comparing the *Security Principal* of the user (account and related groups) with the *Access Control Lists* (ACL) of the *NTFS* file system.

4.3. Active Directory Access

Accessing the ***Microsoft® Active Directory*** is possible with *Integrated Security* in the same way as already mentioned in the section *"**File System Access**"*. The only difference is that the *ACL's* are not related to *NTFS* file system objects but to *Active Directory* objects.

4.4. Public Key Infrastructure

There exists a hierarchical *Public Key Infrastructure (PKI)* within the domain *prov.bz*, which is used to release the certificates for the servers and computers of the provincial network. The *PKI* is installed on a central server and the certificates are released for the single domain controllers through the mechanism of *Auto Enrollment of Windows 2003*, which is offered by the *Group Policy Objects* (and therefore also to servers which are not using the certificates).

5. Software Infrastructure

5.1. Infrastructural Components

File Server - Distributed File System

The fileserver service is offered by the ***Microsoft® Windows 2003*** servers using DFS for site-aware access and unified serverless UNC names.

5.2. Standard Software

There is a lot of standard software that is automatically installed and available on a typical workstation within the network of the *Autonomous Province of Bolzano*. It is not possible to give a complete description of a typical workstation of the domain *prov.bz* here.

5.3. Specialized Software

There is a huge number of specialized software used by the different business functions and installed only where needed. Such software is requested by workflows and, however, assigned and distributed by the HEAT Client Management tool.

5.4. Other Applications and Tools

5.4.1. Office Automation

There are several ***Microsoft® Office*** (*Word, Excel* …) documents with macro code (which is document-integrated program code, written in *Visual Basic for Applications*, *VBA*) supporting the users on various administrative actions by providing a certain level of automation. Of course such "program" logic is neither reusable nor integrated with the whole application infrastructure.

Such documents were often created by the users themselves.

6. Integration and Maintenance

In order to give a complete overview of the Infrastructure of the *Autonomous Province of Bolzano* it is very important to understand that a core aspect for all of the mentioned products is the need of **integration between applications**. This is not only for technical reasons (related to data quality – e.g. to prevent data redundancy in different applications and therefore inconsistency): it is also one of the most important requirements for the future architecture from an organizational viewpoint, because different organizational units (Offices and Departments of the *Autonomous Province of Bolzano*) need to use and manage the same information.

6.1. Programming Languages and Platforms

There are a lot of different programming languages and platforms used for the applications in the *Autonomous Province of Bolzano*. This is due to different philosophies of development and architecture (of different offices and/or companies), different external software suppliers/companies (offering custom or 3rd party products for the province) and of course also simply by the fact that times are changing and technologies too (while the operational products sometimes last for many years).

Anyway in the last years great endeavor has been made within the *Department for Information Technology* to increase the homogeneity, to reduce the number of platforms and programming languages (and therefore to reduce maintenance costs), where possible, or to assure interoperability between them (with the intention to forward synergies and to produce globally reusable functionality). This last approach was especially successful regarding the interoperability through webservices developed in *Java* and *C# (.Net)*, which are at the same time the currently most promising technologies/programming languages on the market.

The following list gives an overview of programming languages used so far for products within the *Autonomous Province of Bolzano | Department for Information Technologies*.

6.1.1. Visual Basic Script (COM)

A lot of small command line maintenance or configuration tools were scripted in *Visual Basic Script (VBS)*; these are interpreted by the ***Windows Scripting Host*** and work on the *COM (DCOM/COM+)* platform. This technology was used in order to write transparent and comprehensible code for everyone, especially the system administrators, which use these tools.

6.1.2. Command Line Scripts (COM)

A lot of small command line maintenance or configuration tools were also written as *Command Line Scripts (CMD)*; these are executed through the *command line interpreter* ***cmd.exe***, which is part of *OS/2 and Windows operating systems*.

6.1.3. Powershell Scripts (.Net)

Few Powershell scripts exist for automating tasks of system administrators.

6.1.4. TSQL (MSSQL) / PL/SQL (Oracle)

There are a lot of *TSQL (Transactional SQL)* or PL/SQL scripts (to query data) used for maintenance and administration tasks on the ***Microsoft® SQL Servers*** and the ***Oracle DMBS***. The scripts are mainly developed and used by the developers and database administrators (DBA).

6.1.5. RPG (AS400)

Since there is an ***IBM AS400*** server in the province, there are also scripts written in *RPG (Report Program Generator)* for various processes within the execution environment of this server.

6.1.6. ABAP (SAP)

ABAP (Advanced Business Application Programming) is a language used for ***SAP*** applications, which is mainly used for automation purposes within *SAP ERP* systems.

6.1.7. Visual Basic for Applications (COM)

VBA code is mainly used within Microsoft Office files as macros.
(You can find details on such macro automations in the chapter ***"Office Automation"***.)

6.1.8. Visual Basic (COM)

There exist many applications developed in VB6 (Visual Basic 6) in the past years. Although since about 2003 no new applications have been developed, the most of these applications are still operational and are improved/maintained according to the requirements.

6.1.9. Delphi (COM)

There exist many applications developed on *Delphi* in the past years. Although it is no longer planned to develop new applications with this technology, the most of these applications are still operational and are improved/maintained according to the requirements.

6.1.10. Java (Java)

The services developed within the *eGovernment* project (from 2005 on) where mainly developed in *Java* with Jboss 7 as an application server.

6.1.11. C# (.Net)

Many of the more recent projects were developed in C# on the .Net platform.

6.1.12. Active Server Pages (COM)

While officially "classic" Active Server Pages (ASP – with HTML and script code like VBScript) have been replaced by the newer .NET based web page technology (ASP.Net pages), they are still in use on a lot of websites.

6.1.13. Active Server Pages (.NET)

Active Server Pages based on *.NET technology (ASPX)* are currently used for exposing Web Services of Business Components.

6.1.14. Java Server Pages/Faces (Java)

Java Server Pages/Faces (*JSP – HTML and java code*) are used for various services and pages within the intranet of the administration of the *Autonomous Province of Bolzano*.

6.1.15. JavaScript

JavaScript is used in many Single-Page-Applications. The first applications were based on jQuery and the JavascriptMVC framework and are still in use and continuously evolved. Since 2015 new applications will be developed using Google's AngularJs framework.

6.1.16. Oracle Forms and Reports

Oracle Forms and Reports was the reference language and reporting tool used by the *Autonomous Province of Bolzano.* For this reason there are a lot of application and system developed with this language

6.1.17. PowerBuilder

PowerBuilder is an environment owned by Sybase, now SAP. It is mainly used in the social sector of the *Autonomous Province of Bolzano.*

6.2. Middleware (Integration and Communication Systems)

The following part only describes **service oriented** middleware that has been (completely or at least partially) developed by the Department of Information Technology.
It doesn't mention the 3rd party products used for data integration (e.g. Data Transformation Services of **Microsoft® SQL Server** and similar **Oracle** functionality…) or are automatically provided as part of such products.

An important middleware developed in C#.Net and used for several newer (service oriented) applications is the so called **Component Execution Environment .NET** (**CEE.Net**).

A **Java** analog (CEE Java) has in the meantime been replaced by JBoss 7 with a proprietary residue consisting in a **service publishing component**.

7. System Infrastructure

7.1.1. Windows OS and Application Server:

- Windows 2012 R2
- Windows 2008 R2
- Windows 2003 R2
- IIS 6.0 with .net Framework 2.0 and 3.5
- IIS 7.5 with Integrated Mode applications and .Net Framework 4.5
- IIS 8.5 with Integrated Mode applications and .Net Framework 4.5

7.1.2. Linux OS and Application Server:

- RedHat 7 64 bit
- Centos 7 64 bit
- JBoss GA 6.2.3 - Java 7 / Wildfly 8.2 - Java 8
- Apache 2.2 and 2.4

7.1.3. Database:

- Oracle Database RAC 11gR2 (Enterprise Edition)
- MSSQL 2014 Enterprise or MSSQL 2008 R2 Enterprise
- PostgreSQL
- SAP-HANA

7.1.4. Storage and virtualization

- Storage FC high performances
- Storage NAS capacitive NL-SAS
- Server virtualization based on VMWare

7.1.5. Other remarks:

- Appliances and devices are installed in standard 19" 42U racks already present in the data center and approved for a maximum of 600 kg. External suppliers are not allowed to install proprietary racks.
- The ventilation of appliances and devices has to be of the type *front to back*.

- Appliances and devices have to be preferably supplied with single-phase currency. The maximum power consumption of a rack is 22 kVA (22 kW).
- Connecting cables must comply with the C13-C14 or C19-C20 specification.
- The data center connectivity is Gigabit Ethernet (copper) or 10 Gb Ethernet (fibre SFP+)

8. Obsolete technologies

The following table shows technologies declared obsolete by the *Autonomous Province of Bolzano.* The term "obsolete" is used to indicate a technology that should be avoided and used only for maintenance (Corrective, Adaptive, Perfective) reasons. The term does not indicate that using it is harmful, but that there will be no further use of it, and therefore those using the obsolete technology are advised to transition to the newer.

Technology	**Obsolete**
Visual Basic Script (COM)	X
Command Line Scripts (COM)	
Powershell Scripts (.Net)	
TSQL (MSSQL) / PL/SQL (Oracle)	
RPG (AS400)	X
ABAP (SAP)	
Visual Basic for Applications (COM)	X
Visual Basic (COM)	X
Delphi (COM)	X
Java (Java)	
C# (.Net)	
Active Server Pages (COM)	X
Active Server Pages (.NET)	
Java Server Pages/Faces (Java)	
JavaScript	
Oracle Forms and Reports	X
PowerBuilder	X
Windows OS and Application Server:	
Windows 2012 R2	
Windows 2008 R2	
Windows 2003 R2	X
IIS 6.0 with .net Framework 2.0 and 3.5	X

IIS 7.5 with Integrated Mode applications and .Net Framework 4.5	
IIS 8.5 with Integrated Mode applications and .Net Framework 4.5	
Linux OS and Application Server:	
RedHat 7 64 bit	
Centos 7 64 bit	
JBoss GA 6.2.3 - Java 7 / Wildfly 8.2 - Java 8	
Apache 2.2 and 2.4	
Database:	
Oracle Database RAC 11gR2 (Enterprise Edition)	
MSSQL 2014 Enterprise or MSSQL 2008 R2 Enterprise	
PostgreSQL	
SAP-HANA	
Storage and virtualization	
Storage FC high performances	
Storage NAS capacitive NL-SAS	
Server virtualization based on VMWare	