Identity management for the TUB Cloud

Thomas Hildmann, Odej Kao, Christopher Ritter

Technische Universität Berlin, IT service center tubIT, Einsteinufer 17, 10587 Berlin

Keywords
Cloud Computing, Identity Management.

1. ABSTRACT

Our students and researchers arrive nowadays at the university with a broad knowledge and expectations about the IT support and the IT technology. Notebooks, netbooks, smart phones together with a broad WiFi coverage enable a nearly unlimited freedom regarding information acquisition, selection, and processing regardless of the current working environment and the time of the day. A broad selection of available applications for smart phones removes even the necessity to be in a specific area in order to approach and use the services. Schools, colleges, and universities must adapt to the expectations of these digital natives and offer their services in a similar way. They must see the user as a customer in the middle of all processes and allow a maximum possible increase of efficiency in order to fulfill the complex requirements in study and research.

However, university such as TU Berlin is not comparable to a commercial provider of certain services, e.g. with a provider of flight tickets. The university unifies manifold services such as study, research, management, projects, patents, cooperation and many more. It also hosts different groups of users having different contexts and needs for services. The integrated service provision is to recognize the current user context, to identify the need, and to provide reliable access to the selected services regardless of the current working environment. In this paper, the path of the TU Berlin towards integrated service provision is described.

2. IDENTITY MANAGEMENT

An innovative, scalable and manageable infrastructure for online service provision in large organizations requires a powerful identity management (IDM) system, which supports an autonomous definition of responsibilities and assignment of roles to cover those responsibilities. The usually applied role-based access control (RBAC) model with classical role engineering builds an excellent foundation, but reaches its limits in the real world, if tens of thousands of users have to be managed. Therefore, we used our experience from running a large identity management system with more than 40,000 registered users to develop a novel model for distributed role definition and assignment as well as rules for checking and modification of the role model regarding desired redundancy, conflicts, and uncovered scenarios. Based on the traditional RBAC96 model (Sandhu 1996) the TU Berlin started the development of its own RBAC-System (Hildmann 1999, Gebhardt 2000) using extensions by Maranda (Poniszewska-Maranda 2005) and Ferrariolo (Ferraiolo 2007, Stanford model).

It defines three layers named identities, organization structure and applications. Each identity is characterized by the unique identifier and completed by data from the primary sources in the organization (Hildmann 2007). In case of TU Berlin, these sources are the database with the personal information of the students, the database with the personal information of the scientist and the staff as well as a further source with information about persons having some relationship with the university but without a legal contract with the university. The data is entered and managed by the responsible staff in the university departments and only pulled if needed by the application. This approach minimizes the data redundancy and defines a clear responsibility for the data quality. The entire provisioning process is implemented as a one-stop agency and uses the data from the legal agreements for building the structure. This part represents a work-intensive administration process, as structures change often and have to be re-built in the system. On the top, the application layer implements the assignment of application roles, which may include several access roles, to users. This is the interface to the application in the portal: the applications already define different roles, which are mapped on TUBIS roles and then assigned to users. Permissions associated with role

assignment are bounded to the context of the assigning organization unit. While the related permissions are limited to the context of a specific unit, the role assignment itself is not. Roles can be assigned from any organization unit to every registered user of every managed organization unit. On access, user information is transferred to the application and used to set the user in the corresponding role and context.

3. CLOUD MANAGEMENT

At the central IT-Service-Center tubIT we see our daily business changing to service oriented architecture. This is conflicting with our basic needs of providing reliability, flexibility and high availability for basic services like network, e-mail and web-infrastructure. To satisfy the rising demands from power users, we built up an infrastructure based on leading edge technologies, for the infrastructural computing as well as for the research and teaching part of our university (Berndt 2012). The system is fully integrated into our process of provisioning, operating, running, de-provisioning and accounting. This automatically provides cloud-services for every TU member. From security point of view, the infrastructure has to be able to integrate within the customer's security contexts and networks and has to provide a secure way of computing and storage of data for all customers. For using the infrastructure in the best way for all purposes, we decided to separate the hardware into two logical groups. We created a private cloud for supporting the basic infrastructure and set up the public cloud for the demands from research projects.

The private cloud is based up on VMware vSphere 5.x for infrastructure computing supporting the main services like Active Directory, MS Exchange, web, mail and some databases. Authentication of the services is completely managed over the centralized identity management system TUBIS by providing a bundle of widely supported services like LDAP, Kerberos or the Active Directory. Additionally several connectors provide up-to-date data to services needing customized information such as DNS appliances or university calendar system. The identity management system is also a part of the private cloud by itself. Authorization and accounting is managed by the role management of TUBIS where applicable by providing RMI or SOAP-WS interfaces. Otherwise authorization and accounting is left inside the service. The user-assignment to an organizational-unit and to basic roles enables automated accounting or limiting of resources like mail- and file-quota, access to the unit's homepage, etc. A major set of tasks and therefore needed access can be delegated using the self-management interface of TUBIS. This enables sickness cover and proxy persons during business trips. External research partner can be granted access to resources of the private cloud by any department using the online provisioning interface. The identity management system is not only covering the user lifecycle from provisioning to deprovisioning but also the lifecycle of each managed organization-unit. While provisioning of organization-unit automatically generates and assigns role packages and cloud resources, deprovisioning of organization-unit triggers the reassignment or release of assigned cloud-resources depending on the existence of a replacement unit.

The public cloud for supporting the research tasks and providing the resources for different upcoming customers is managed by Zimory middleware. For security reasons each customer gets his own virtual LAN segment where the instances for his environment are put into. The aim is to provide a cloud infrastructure for building up a public cloud that could be used by different companies and partners. It focuses on providing Compute resources for researchers within the TU Berlin, as well as providing "Easy-to-deploy" IT environment for start-up centers and supporting schools and public administration, by providing services for them. On-demand hardware and services are provided by the cloud while the self-managed RBAC system provides delegated access on-demand.

4. CONCLUSION

The infrastructure migration into the cloud is a way of solving the problems and fulfilling the demands of our customers with a modern and state-of-the-art technology. There are some problems to solve on the way, but in the end the infrastructure is capable of offering services as infrastructure on demand or infrastructure as a service while moving some parts of the administration and resource scheduling into the hands of the customers or users while using long existing resources like primary data sources and integrating (de-)provisioning in existing processes at the university. The installed infrastructure at TU Berlin is fully integrated in the operational concepts and the security models.

5. REFERENCES

Ravi S. Sandhu, Edward J. Coyne, Hal L. Feinstein, and Charles E. Youman (1996). ROLEBASED ACCESS CONTROL MODELS. Computer, Volume 29(2):38–47.

T. Hildmann and J. Bartholdt (1999). MANAGING TRUST BETWEEN COLLABORATING COMPANIES USING OUTSOURCED ROLE BASED ACCESS CONTROL. In Proceedings of the Fourth ACM RBAC Workshop.

T. Gebhardt and T. Hildmann (2000). ENABLING TECHNOLOGIES FOR ROLE BASED ONLINE DECISION ENGINES. In Fifth ACM Workshop on Role-Based Access Control.

Aneta Poniszewska-Maranda (2005). ROLE ENGINEERING OF INFORMATION SYSTEM USING EXTENDED RBAC MODEL. In WETICE'05, IEEE.

David F. Ferraiolo, D. Richard Kuhn, and Ramaswamy Chandramouli (2007). ROLE-BASED ACCESS CONTROL, Second Edition, Chapter 4.6, Artec House.

T. Hildmann and C. Ritter (2007). TUBIS-INTEGRATION VON CAMPUSDIENSTEN AN DER TECHNISCHEN UNIVERSITÄT BERLIN. *PIK-Praxis der Informationsverarbeitung und Kommunikation*, 30(3):145–151.

P. Berndt, M. Hovestadt, and O. Kao (2012). ARCHITECTURE FOR REAKIZING CLOUD-BASED IT INFRASTRUCTURES. In Proceedings of the 3rd Intl. Conference on Next Generation Information Technology (ICNIT), ICNIT 2012, pages 204–210. IEEE publishers.

6. AUTHORS' BIOGRAPHIES

Thomas Hildmann is with TU Berlin since 1999 and is head of Department Infrastructure at tubIT IT-Service-Center after receiving his PhD in the RBAC environment 2010. He studied computer science and graduated in 2002 with diploma thesis on the development of a secure, extended e-mail system. This work was a continuation of his developments for the E2S project (end-to-end-security over the internet). Thomas Hildmann came back to TU Berlin after he worked as the leader of software development for a small Berlin system vendor. His research work was permanently accompanied by system administration tasks and built the base for his current function as the head of over 20 system administrators responsible for the infrastructure for management and research.

Odej Kao is full professor at the Berlin University of Technology (TU Berlin) and director of the IT center tubIT. He received his PhD and his habilitation from the Clausthal University of Technology. Thereafter, he moved to the University of Paderborn as an associated professor for operating and distributed systems. His research areas include Grid and Cloud Computing, context-aware systems, service level agreements and operation of complex IT systems. Odej Kao is member of many program committees and editorial boards and has published more than 250 papers.

Christopher Ritter is head of department Identity Management at tubIT IT-Service Center of TU-Berlin. He is active in the field of IT-Security for more than 12 years today. During these years he started participating in national and international projects of T-Systems International, including topics like Security platforms, smartcard infrastructures, PKIs as well as biometric identification. 2003 he joined the smartcard project of TU-Berlin. After completion he started the design and development of an organization spanning role-based identity management system (TUBIS). With founding of tubIT in 2006 he took part as the lead developer of TUBIS and published some papers regarding role-based Identity Management and decentralized role management.