Karelia University of Applied Sciences
Degree Programme in Business Information Technology

Antti Miettinen

Centralized Identity Management in a Decentralized Organization

Thesis
February 2017

Karelia
AMMATTIKORKEAKOULU

OPINNÄYTETYÖ
Helmikuu 2017
Tietojenkäsittelyn koulutusohjelma

Karjalankatu 3
80200 JOENSUU
013 260 600

Tekijä(t)
Antti Miettinen

Nimeke
Keskitetty identiteetinhallinta hajautetussa organisaatiossa

Toimeksiantaja
Tietoturvaratkaisuja tarjoava yritys

Tiivistelmä

Opinnäytetyön tavoitteena on tutkia keskitettyä digitaalista identiteetinhallintaa. Työn tarkoituksena on auttaa toimeksiantajaa kehittämään identiteetinhallintaprosessia. Työssä esitellään entinen ja kehitteillä oleva identiteetinhallintaprosessi ja suurimmat tietoturvariskit entisessä identiteetinhallintaprosessissa. Opinnäytetyö on tutkimuksellinen.

Opinnäytetyössä esitellään Microsoftin identiteetinhallinta-infrastruktuuriin liittyvät tekniset alustat ja käsitteet. Niitä ovat Active Directory, Azure Active Directory, Microsoft Azure, Office 365 ja Microsoft Enterprise Mobility + Security kokonaisuus. Työssä esitellään myös identiteetti ja identiteetinhallinta.

Opinnäytetyön tuloksena esitellään kehittämisehdotuksia kehitteillä olevaan identiteetinhallintaprosessiin. Työssä esitellään entisen identiteetinhallintaprosessin ongelmakohtia. Ongelmakohtina esitellään tietoturvaongelmat ja hallittavuuden puute käyttäjän ja laitehallinnan alueilla. Opinnäytetyön tuloksen on tarkoitus auttaa toimeksiantajan Informaatioteknologia osastoa ja johtoa, kun identiteetinhallintaprosessia kehitetään eteenpäin.

Kieli englanti	Sivuja 48 Liitteet

Asiasanat
identiteetinhallinta, tutkimus, tietoturva, Microsoft Azure

THESIS
February 2017
Degree Programme in Business Information Technology

Karjalankatu 3
80200 Joensuu
013 260 600

Author(s)
Antti Miettinen

Title
Centralized Identity Management in a Decentralized Organization

Commissioned by
Information security service provider

Abstract

The purpose of this thesis is to research centralized identity management at information security organization. The research presents the former and the prospective identity management processes and the most significant information security risks in the former identity management process. This thesis is a research to support the commissioner when developing the prospective identity management process.

This thesis explicates the technical platforms and concepts that are present in Microsoft's identity management infrastructure. The technical platforms and concepts include Active Directory, Azure Active Directory, Microsoft Azure, Office 365 and Microsoft Enterprise Mobility + Security. In addition, the identity and the identity management concepts are presented.

As a result of this thesis changes in the prospective identity management process are inevitable due to issues arisen in the research. These issues concern specifically information security and lack of management, for example in use and device management. This thesis should be perceived as a guide for Information Technology department and Management at information security service provider to assist and to support the decision making when developing the identity management process.

Language English	Pages 48 Appendices

Keywords

identity management, research, information security, Microsoft Azure

Contents

1 Introduction

The commissioner, an information security service provider, provides information security solutions for private and public sector organizations. The information security service provider is a local company located in Joensuu, where the development, technical support and information technology and finance teams are located. This thesis will introduce the technical platforms and concepts that are present in Microsoft’s identity management infrastructure. The commissioner has a centralized identity management project, which aims to improve identity management process by centralizing employees of the company to Azure Active Directory. Azure Active Directory is a cloud based directory and identity management service. The research questions in the thesis are, how the prospective process will change identity management at information security service provider and what are the most significant parts of the identity management from the commissioner point-of-view?

The second chapter introduces information about Active Directory, a directory service which was released with Microsoft Windows Server 2000. Since then, it has been serving as an identity and network resource management service of many companies. In addition, Azure Active Directory is introduced in the chapter, with an illustration, how it can be integrated with an on-premise server. ‘On-premise’ in this thesis means servers or other networking related applications that operate in organizations self-hosted environments. These services are explicated in this thesis, because user and device information is stored in Active Directory and in Azure Active Directory.

The third chapter introduces Microsoft Azure cloud platform, which is the centerpiece in Microsoft cloud infrastructure. The complete Microsoft Azure infrastructure in its current form is presented. It is possible to visualize all the Azure services and capabilities at a glance. When considering to expand Microsoft Azure cloud platform services from Azure Active Directory to other services, it is effortless to notice the basics of Azure from the chapter.

The fourth chapter introduces Office 365 and points out the relation between Office 365 and Azure Active Directory. The mentioned relation is that Azure Active Directory serves as a directory service for Office 365. It is useful to understand Office 365 concept and especially what it is capable of with Azure Active Directory. Office 365 offers various identity models to meet the cloud market requirements for multiple customer segments. Some of the commissioner's employees are in Office 365 and users in the cloud are managed from Office 365 web portal.

The fifth chapter introduces Microsoft Enterprise Mobility and Security suite. The product suite features Azure Active Directory Premium, Microsoft Intune and Azure Information Protection. Azure Active Directory Premium provides a subscription based version of Azure Active Directory with two Premium editions, P1 and P2. Microsoft Intune enables cloud-based device and application management features. And Azure Information Protection is a cloud-based information security solution to offer various methods for managing document and data security. The Microsoft Enterprise Mobility and Security suite complements the features of Azure Active Directory, which is the reason why it is involved.

The sixth chapter introduces identity and management, in which the identity and digital identity is explicated. The chapter also covers identity management and identity access management processes that are the basis of this thesis. To understand identity management processes at information security service provider, identity and identity management concepts are important to know. In the chapter, identity management processes are introduced with illustrative examples of the processes. And the information security issues that existed in the former process, are illustrated in an interview with the management. Moreover, a comparison of the identity management processes is included in the last subchapter.

After describing the technical platforms, the concepts and the former and the prospective state of identity management, a conclusion of the identity management at information security service provider is introduced in the seventh chapter. In the chapter, a question is raised how the prospective identity management process will eventually change the identity management at information security service provider and the researcher's observations of the complete identity management infrastructure. The expected result is that a lot will change due to the presented issues in this thesis about information security, lack of management in specific areas, such as user and device management. For user management challenges Azure Active Directory alongside with Active Directory will improve the former user management process by offering a combined set of tools to manage users from cloud. Microsoft Enterprise Mobility and Security (EMS) offers a major potential to improve application and device management with built-in processes and capabilities that were not even featured in this thesis. Microsoft EMS features application and device lifecycles that will assist, when standardizing application and device management processes. And as the most significant part of the Identity Management is presented chief of Information Technology department and Management. The persons, who are responsible, have the knowledge and can understand the complete process well enough to make the final decision.

2 Active Directory and Azure Active Directory

Active Directory is a directory service, that is used to store and manage information about network resources. Active Directory can handle information and data, such as user and device information and application-specific data in a network. Username or first and last name can be considered as user information and Windows PC list of components as device information. Application specific data is data that is associated with particular application and its users, who are stored users in Active Directory. The described information in Active Directory acts as an object that a system administrator can organize into a hierarchical collection of containers. The containers are known as the logical structure, which is a standardized way to present information stored in Active Directory in a useful way. (Microsoft TechNet 2014.)

With Active Directory, it is easy to manage all users, computers and other network resources. It operates as a centralized management tool for distributed computing environments. Because of that it is effortless for the user to locate and use the distributed network resources and the system administrator can manage the way the resources are used. Active Directory authorizes access for users to login to a workstation. It is responsible for managing and controlling identities and the relationships between network resources. The user or system administrator can locate and use file servers, printers or other resources in the network with Active Directory. The more the network grows in a company, the more there are network resources to manage, which makes the directory service significant. (Stanek & Associates 2014, 7-9.)

2.1 Azure Active Directory

According to Collier and Shahan, Azure Active Directory is a multitenant directory and identity management service in the cloud that has quite a similar purpose as traditional Active Directory, with extended capabilities to manage and control identities. Multitenant concept is introduced in the e-book Microsoft Azure Essentials: Fundamentals of Azure, Second Edition by Collier and Shahan. In computer science multitenant means that a software runs on a server and serves multiple tenants. A tenant is a group of users who have access to the software with specific privileges. The most significant difference between the directory services is that while Active Directory is an on-premise solution and the consumer is responsible for the whole infrastructure, Microsoft is responsible of the infrastructure of Azure Active Directory. For example, the server maintenance, the reliability of the servers and access to the network resources are all controlled through the directory service. Although there are similar features between the two directory services, Azure Active Directory should not be contemplated a full replacement for Active Directory. They are both able to run separately and along with each other, when the services complement the features of themselves. (Collier & Shahan 2016, 181-182.)

Azure Active Directory has an important role as a key factor for identity management in the Microsoft cloud. It comes with many different capabilities to improve the information security of the identities such as multi-factor authentication. (Collier & Shahan 2016, 182.) Multi-factor authentication requires more than one verification method to user sign-ins and transactions. It adds a second level of security to the authentication process. Generally, the additional verification method is a password, a trusted device or biometric identifier. (Gremban 2016.) Basic example of multi-factor authentication method is that after a verified login, the user is required to authenticate the correct identity with a fingerprint.

2.2 Operational principle

Figure 1 illustrates, basic operational principles of Azure Active Directory, it contains two parts that complement each other. First part is from Windows Server Active Directory to Single sign-on (upper illustration) and the second part is from On-premises to Cloud (lower illustration). The figure is meant to read from left-to-right to show how Azure Active Directory can be used. For example, the first part of the figure presents that if there is an on-premise **Windows Server Active Directory** already in use, it is possible to use Azure AD Connect to synchronize user credentials from the Active Directory to Azure Active Directory. **Simple connection** mirrors the Azure AD Connect connection in the figure. Identities that the Active Directory contains, can be self-managed by an employee as the **Self-service** mirrors. The identities can also be configured to have **a single sign-on** feature enabled, to access cloud applications that an organization has. When user gains instant access to cloud and on-premise with a single verification of password, the feature is known as single-sign-on (SSO).

The second part of the figure presents that if an organization uses Office 365 or other SaaS applications, the organization is using **Microsoft Azure Active Directory**. The SaaS application tenant is an Azure Active Directory tenant. And **On-premises** SaaS applications can be integrated with Azure Active Directory tenant to access cloud applications that an organization has and that are supported by Azure Active Directory and Access Panel. The Access Panel is presented in the eighth chapter.

An example of authentication process in Azure Active Directory in a basic scenario works the following way. As identity provider Azure Active Directory is responsible for verifying that the identity of users and applications exist in organizational directories. Application that wants to authenticate via Azure Active Directory must be registered to the directory service, it then registers and identifies application. Also, multi-factor authentication is possible to enable, to use it as additional verifying method. The method can be seen as a fingerprint from the figure, under the **Self-service** and illustration of mobile devices.

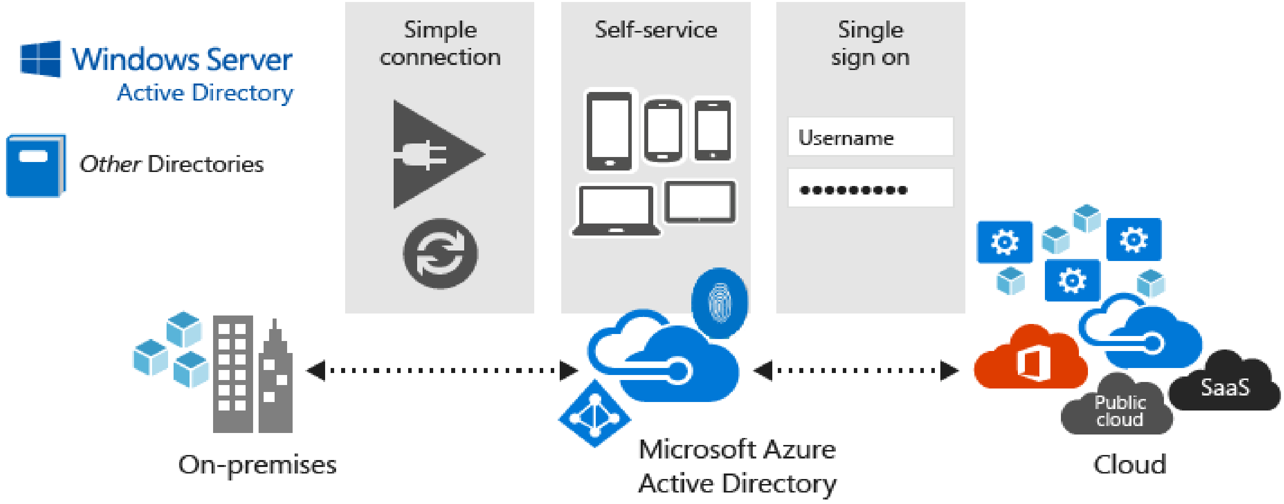


Figure 1. Operational principle of Azure Active Directory. (Figure: Vilcinskas 2016.)

3 Microsoft Azure

Microsoft Azure, created by Microsoft, is a cloud computing and services platform to build, deploy and manage applications in the public cloud. Azure is hosted in multiple data centers all over the world, which are managed by Microsoft. (Microsoft 2016.) In 2008, three independent development teams from Microsoft started to work together to create the foundation for Azure platform and later that year Microsoft published the platform. Two years later in February

2010, general availability of Azure is announced in 21 countries. (Mitch Tulloch 2013, 9-12.) Due to strategical reasons, Microsoft renamed Windows Azure to Microsoft Azure in 2014 (Martin 2014).

There are many services in Azure and most of the services can be accessed via Management Portal. The Management Portal is a web portal for managing the Azure services. System administrator can administrate and access the services from the Management Portal web interface. (Boucher 2015.) In general, that seems to be the most common way in today's cloud computing to manage, access and use the cloud services.

Figure 2 shows all of the many service categories in Microsoft Azure and all the services under the categories. First three of the most significant services are introduced in the chapter one and after the introduces, the other Azure services are explicated in outline. It is important to understand the Azure platform, especially if usage of the Azure services comes topical.

Identity and Access consists of **Azure Active Directory** and **Multi-Factor Authentication**. Identity and Access service category, in the figure 2, is beneath the Developer and IT Services service category and its services are found by reading from left-to-right. Both services are presented in the previous chapter, Multi-Factor Authentication in the Azure Active Directory subchapter. **Compute** consists of **Virtual Machines**, **Websites** and **Cloud Services**. Compute service category, in the figure 2, is the uppermost category and services are found by reading from left-to-right. **Virtual Machine** service adds the ability for Azure subscriber to create virtual machines running in Azure cloud. **Websites** offer a managed web environment without need to worry administration of websites or web applications. **Cloud Services** provides technology for scalable, reliable and low level-administration applications. **Commerce** consists of **Store and Marketplace** that are portals where organization can buy Azure cloud applications or other commercial datasets that are possible to add to expand the functionality of developed applications. Commerce service category, in the figure 2, is the bottom service category and its services are found by reading from left-to-right.

Data Management consists of **SQL Database**, **Storage Blobs**, **Storage Tables**, **Import / Export** and **File Service**. Data management service category, in the figure 2, is beneath the Compute service category and its services are found by reading from left-to-right. **SQL Database** provides relational database management system in the cloud. **Storage Blobs** gives the possibility to store unstructured binary data. **Storage Tables** is a typed key or a value store, it can handle many data types such as integers and dates. With **Import and Export,** it is possible to send encrypted 3.5” hard drives to Azure datacenter, where Microsoft’s engineers can transfer the data to a Storage Blob. Microsoft will send the hard drive back after uploading the contents of the hard drive to Azure. **File Service** adds the ability for applications to share files between Virtual Machines running in Azure cloud.

Networking consists of **Virtual Network**, **Traffic Manager** and **ExpressRoute**. Networking service category, in the figure 2, is beneath the Data Management service category and its services are found by reading from left-to-right. **Virtual Network** adds capability to create virtual private networks (VPN) between local internet connection and virtual machines network. **Traffic Manager** is a network traffic routing tool to assist and manage applications network traffic. **ExpressRoute** is a networking service that benefits of Azure Virtual Network to add more bandwidth and security to virtual private networks created with Virtual Network services.

Developer and IT Services consists of **Visual Studio Online**, **Azure SDK**, **Azure Tools for Visual Studio**, **Automation** and **API management**. Developer and IT Services service category, in the figure 2, is beneath the Networking service category and its services are found by reading from left-to-right. **Visual Studio Online** and **Azure Tools for Visual Studio** forms Visual Studio Team Services. The services adds tools for Visual Studio for example load balancing and a version control system called Team Foundation Service. **Azure SDK**, software development kit, provides different programming language support to build, deploy and manage Azure applications. With **Automation** user can automate frequently repeated work tasks in Azure to save time, it is possible to create, monitor, manage and deploy the automated processes. **Application Programming Interface Management** (API) helps organization to publish APIs to whoever needs them.

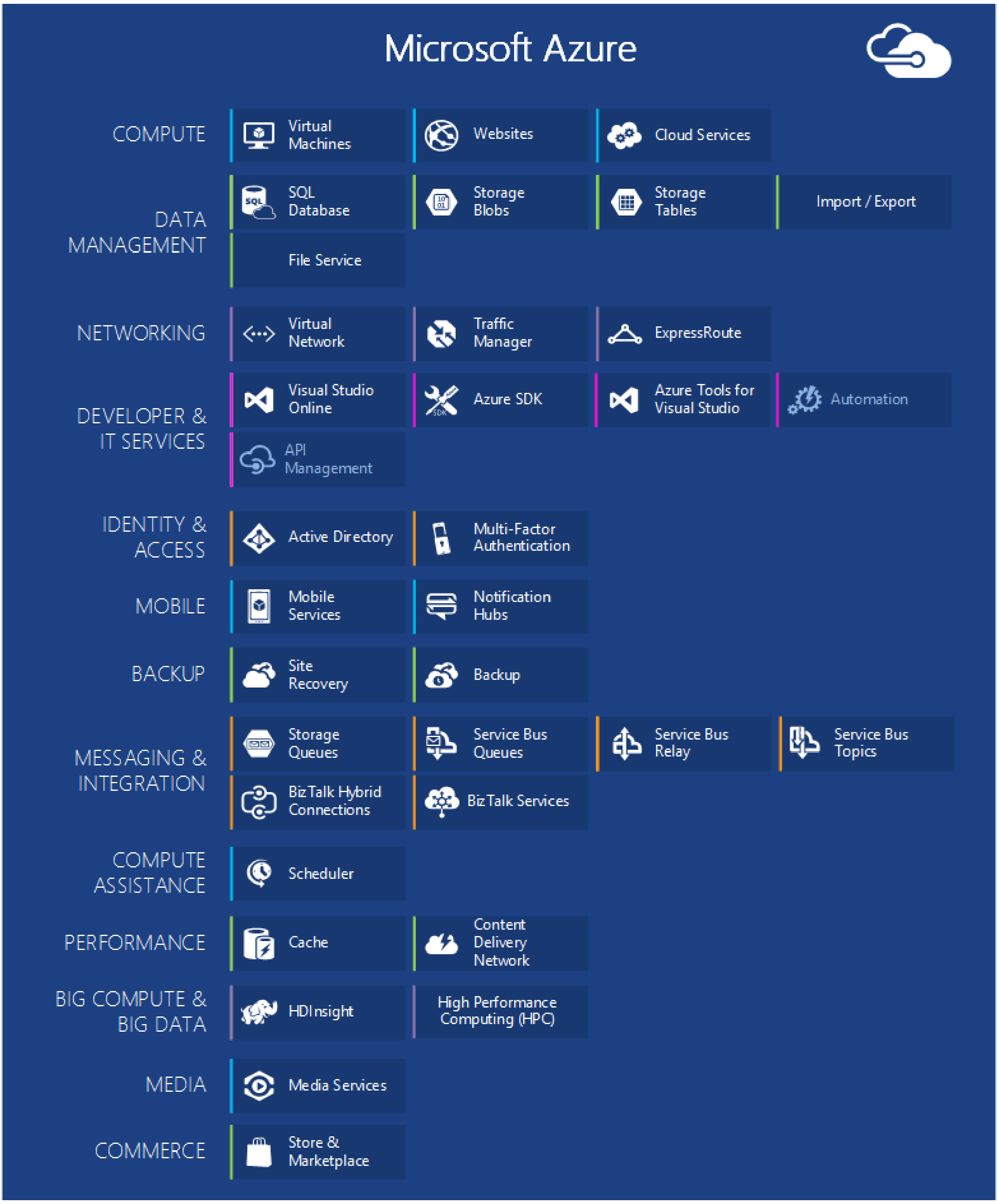
Mobile consists of **Mobile Services** and **Notification Hubs**. Mobile service category, in the figure 2, is beneath the Identity and Access service category and its services are found by reading from left-to-right. **Mobile Services** offers a mobile development platform in Azure cloud. **Notification Hubs** eliminates writing programming code for notifications in mobile applications and offers API that can handle the notifications. **Backup** consists of **Site Recovery** and **Backup**. Backup service category, in the figure 2, is beneath the Mobile service category and its services are found by reading from left-to-right. **Site Recovery** is a tool of services that can recover application to normal working condition, for example from very high workload. **Backup** adds the ability to backup data from on-premise server to Azure cloud. Backup data is encrypted during the transmission and at the data storing phase in the Azure cloud.

Messaging and Integration consists of **Storage Queues**, **Service Bus Queues**, **Service Bus Relay**, **Service Bus Topics**, **BizTalk Hybrid Connections** and **BizTalk Services**. Messaging and Integration service category, in the figure 2, is beneath the Backup service category and its services are found by reading from left-to-right. **Storage Queues** and **Service Bus Queues** adds queued messages that application is able to read whenever there is a need. **Service Bus Relay** adds the possibility for application to communicate directly with another application in a secure way through firewalls. **Service Bus Topics** contains a publish and subscribe mechanic, one application can send a message for specific topic and other application can subscribe to that topic, it allows one-to-many communication within different applications. **BizTalk Hybrid Connections** offers a way to connect web application feature and mobile application feature from Azure Cloud to an on-premise server. With **BizTalk Services,** user can integrate different systems to do actions that are possible without the need to write custom program code.

Compute Assistance consists of **Scheduler** to schedule application to run only on exact time, if there is no need to keep the application running all the time, consuming Azure resources paid by an organization. Compute Assistance service category, in the figure 2, is beneath the Messaging and Interaction service category and its services are found by reading from left-to-right. **Performance** consists of **Cache** and **Content Delivery Network**. Performance service category, in the figure 2, is beneath the Compute Assistance service category and its services are found by reading from left-to-right. **Cache** is Azures in-memory caching technology for caching application data, it aims to reduce the time to retrieve usually needed data. **Content Delivery Network** (CDN) copies an Azure storage blob from Azure Cloud into local CDN storage. It aims to give faster access to data for users that are geographically located in different locations around the world.

Big Compute and **Big Data** consists of **HDInsight** and **High Performance Computing**. Big Compute and Big Data service category, in the figure 2, is beneath the Performance service category and its services are found by reading from left-to-right. **HDInsight** is a service based on Hadoop, technology for handling big data, it helps to process data across the Azure cloud. **High Performance Computing** in Azure cloud offers a set of tools to distribute work resources across multiple virtual machines. **Media** consists of **Media Services**, which is a platform that tries to help when developing applications that require video or other media. Media service category, in the figure 2, is beneath the Big Compute and Big Data service category and its services are found by reading from left-to-right.

Microsoft Azure offers a wide scale of various services and with Azure, organization can move its Information Technology infrastructure to the cloud. Software company has the tools to create web store for its products by using Azure Websites and use Azure SQL Database to store all the web store's data in a relational database. The webstore can be hosted on Azure Virtual Machine to run on Microsoft cloud and Information Technology team can balance the heavy load, created by customers, with Traffic Manager for better availability and performance to customers from all over the world.



Microsoft Azure

COMPUTE	Virtual Machines	Websites	Cloud Services	
DATA MANAGEMENT	SQL Database	Storage Blobs	Storage Tables	Import / Export
	File Service			
NETWORKING	Virtual Network	Traffic Manager	ExpressRoute	
DEVELOPER & IT SERVICES	Visual Studio Online	Azure SDK	Azure Tools for Visual Studio	Automation
	API Management			
IDENTITY & ACCESS	Active Directory	Multi-Factor Authentication		
MOBILE	Mobile Services	Notification Hubs		
BACKUP	Site Recovery	Backup		
MESSAGING & INTEGRATION	Storage Queues	Service Bus Queues	Service Bus Relay	Service Bus Topics
	BizTalk Hybrid Connections	BizTalk Services		
COMPUTE ASSISTANCE	Scheduler			
PERFORMANCE	Cache	Content Delivery Network		
BIG COMPUTE & BIG DATA	HDInsight	High Performance Computing (HPC)		
MEDIA	Media Services			
COMMERCE	Store & Marketplace			

FIGURE 2: Components of Microsoft Azure. (Figure: Boucher 2015.)

4 Office 365

Office 365 is a cloud based service, by Microsoft, that comes with Microsoft's products and services. As it is a subscription based service, there are two different subscription plans available for both segments, business and consumers. With consumer edition comes the original Microsoft Office applications and business edition adds applications such as Skype for Business, online hosted email for business and OneDrive for Business. Although there are only two different subscription plans, it does not mean that a single consumer or company cannot buy tailored versions of the Office 365 service. Most of the Office 365 subscription plans come with the latest desktop versions of the applications in the Microsoft Office product family. The subscriber can install and distribute the additional licenses of desktop versions to multiple devices, not only to Windows PC but for example to Mac or to Android smartphone. (Microsoft 2016.)

The online applications in Office 365 can be accessed via web browser from the web portal. At the present time, Microsoft has developed the online versions for Word, Excel, PowerPoint and OneNote. Of course, there are other applications like OneDrive and Yammer, social networking service for enterprise level organizations, that can be accessed with web browser. When working with the online applications, all modifications are automatically saved and synchronized to OneDrive cloud storage.

Office 365 and Azure Active Directory share some of the foundation between each other. The relation between Office 365 and Azure Active Directory is that the users in Office 365 are managed through the Azure Active Directory service. In other words, it serves as a database for Office 365 user identities. The enterprise subscription plan for Office 365 includes a free subscription to Azure Active Directory. Though, the subscription must be activated from the Azure Management Portal. After activating the subscription, Azure Active Directory can be used to create and manage user and group accounts from the Office 365 admin portal. (Microsoft 2016.)

In Office 365, there are three identity alternatives to choose from, **cloud identity, synchronized identity and federated identity**. In **cloud identity model**, identity and authentication are managed completely in the cloud. On-premise servers are not required, since Azure Active Directory is the directory service for user identities and verifier of the passwords. **Synchronized identity** offers the possibility to synchronize directory objects from an on-premise server with Office 365. User identities can be configured to have the same password in both, on-premise and cloud servers. **Federated identity** acts the same way as the synchronized identity model, but users have the same password in on-premise and cloud with no exception. (Microsoft 2016.)

5 Microsoft Enterprise Mobility and Security

Microsoft Enterprise Mobility and Security (Microsoft EMS), released in 2014 as Microsoft Enterprise Mobility Suite, was created to face the challenges in this cloud and mobile first world. At the present time, people are using more of their own devices to complete work tasks with, the management of devices, applications and especially data can be challenging for Information Technology department in a company. Microsoft has claimed that increasing number of the company's partners and customers are using mobile devices and Software as a Service (SaaS) applications for work. The Microsoft EMS is a combination of the mentioned two trends and is intended to assist the market, between those two major trends. (Kelly 2015.)

Microsoft EMS has four main functions, identity and access management, mobile device and mobile application management, identity-driven security and information protection. It is built on Microsoft’s already existing cloud platforms, Azure Active Directory Premium, Microsoft Intune and Azure Information Protection. (Conway 2016.)

5.1 Azure Active Directory Premium

Azure Active Directory Premium is a paid edition of Azure Active Directory with extended identity and access management capabilities. It is suitable for enterprise level subscribers by providing additional features to Azure Active Directory. At the moment, there are two different premium editions available, Premium P1 and Premium P2, where Premium P2 expands the Premium P1. (Love 2016.)

Chart 1 illustrates Azure Active Directory Premium P1 and P2 editions premium features. Premium features in the chart are listed one below another and on the right side, on top of the chart from left-to-right is listed Premium P1 and P2. “Yes” or green color indicates that the feature is available in the specific edition and “No” or red color indicates that the feature is not available in the specific edition.

		Azure Active Directory Premium P1	**Azure Active Directory Premium P2**
Premium features	Self-service group and application management/self-service application additions/dynamic groups	Yes	Yes
	Self-service password reset/change/unlock with write-back to on-premises directories	Yes	Yes
	Multi-Factor Authentication (cloud and on-premises)	Yes	Yes
	Microsoft Identity Manager Client Access License + Microsoft Identity Manager Server	Yes	Yes

	Cloud app discovery	Yes	Yes
	Azure AD Connect Health	Yes	Yes
	Automatic password rollover for group accounts	Yes	Yes
	Identity Protection	No	Yes
	Privileged Identity Management	No	Yes

Chart 1: Azure Active Directory Premium editions. (Chart reference: Love 2016.)

From the top to the bottom, both Azure Active Directory Premium editions enables the following features. Self-service network group and application management, self-service application additions and dynamic groups. Support for password change, reset or unlock for users as a self-service with password write-back to on-premises directories. Multi-Factor Authentication which was described earlier in the fourth chapter. Microsoft Identity Manager Client Access License and Microsoft Identity Manager Server. Microsoft Identity Manager is an on-premises identity and access management suite. Cloud application discovery to search for unmanaged cloud applications in organization. Azure Active Directory Connect Health, to monitor on-premises identity infrastructure from cloud. Automatic password rollover for group accounts. The last two features are Identity Protection and Privileged Identity Management, both features are described in the following section.

The difference between the Premium editions is that Premium P2 contains two extra features, Azure Active Directory Identity Protection and Azure Active Directory Privileged Identity Management. Identity Protection is a feature to monitor for vulnerabilities and security risks in organization's identities. The feature calculates risk level for each user in organization and assists system administrator to create additional risk-based policies to protect the identities in organization. (Vilcinskas 2016.) In this case, when users are distributed globally to various countries, Identity Protection can assist Information Technology department at information security service provider to monitor and protect user identities against digital identity thefts. The feature adds machine learning and heuristic rules and therefore removes manual work from employees of the department. With Privileged Identity Management feature, it is possible to manage, control and monitor the access to resources in Azure Active Directory or other Microsoft cloud services. For example, system administrator in organization can view Azure Active Directory user with administrator rights and get access history of a certain administrator. (Gremban 2016.) Presumably Privileged Identity Management complements the features of Identity Protection by adding just in time administrator access possibility and other management resources to Azure Active Directory. With just in time administrator access is possible to grant user as administrator of a certain application, if the user needs a privileged access randomly.

5.2 Microsoft Intune

Microsoft Intune is a cloud-based device and application management solution. It is integrated to the Microsoft Enterprise Mobility and Security product suite, where Intune is used to manage mobile devices and applications, Windows devices and applications and Mac devices and applications. Intune leverages Azure Active Directory for identity and access control, and Azure Information Protection for data protection. There are three primary tools that Intune consists of, mobile device management, mobile application management and mobile application security.

Mobile device management enables the ability to manage devices in a company. To manage a device with Microsoft Intune, first, a device must be enrolled to Intune. Enrolling a device enables the mobile device management capabilities. The main capabilities consist of factory resetting a device, associating devices with users and remote locking a device. Remote locking a phone or laptop is useful when the device is lost. Supported device platforms are Apple iOS 8.0 and later, Google Android 4.0 and later, Android for Work, Windows Phone 8.1 and later, Windows RT 8.1, Windows 8.1, 10 (Home, Pro, Education, and Enterprise versions), Windows IoT Enterprise and Mobile Enterprise, Windows Holographic and Holographic Enterprise and Mac OS X 10.9 and later. (Barnett 2016.) The market demand for various device platforms is widely-recognized with the platform support from Microsoft.

Mobile application management and mobile application security helps organization to protect its data on employee’s devices, even if devices are not managed by Information Technology department. The solutions offers application policies that Information Technology department can configure to match the organizational data policies. An example of application policy is to prevent saving organization owned worksheet to a personal storage location on an iPhone. Benefits of the application policies are that the critical work applications can be configured to have a PIN code to access and data used by work applications is protected without need to reveal user’s personal data on a device. (Raman 2016.) PIN code in this context is application-specific personal identification number.

5.3 Azure Information Protection

Azure Information Protection is a cloud-based solution for document and data security. With the solution organization can classify, label and protect its documents or emails to prevent data leakage or misuse. Administrator can set rules that labels documents as classified with a known word or a word combination like ‘internal’. When the document is in classified state, it means the document is protected by regulations and user should be aware of it. Supported email service can then inspect the metadata of attachments, added by Azure Information

Protection, in clear text to email header and prevent sending the file outside of user's organization. (Bailey 2016.)

Protection technology used in Azure Information Protection solution is called Azure Rights Management, which is a cloud-based technology. The technology utilizes encryption, identity and authorization policies to protect documents and emails. Protected data can be secured inside and outside of target organization, if the protected data leaves the target organization, the protection will remain with the data. Only authorized users can view the protected document. The protection technology works in Windows and Mac computers, on mobile supported operating systems are iOS, Android and Windows Phone. (Bailey 2016.)

Microsoft claims that Azure Rights Management and Microsoft as a company are not able to see protected data at any stage of the information protection process. Unless the user is not using Azure cloud storage to store protected documents or a cloud storage that sends protected documents to Azure. Decryption of encrypted document will only happen, when the document is used by a rightful user or processed by an authorized service. (Bailey 2016.)

6 Identity and Identity Management

This chapter introduces identity and identity management concepts and the former identity management process at a general level at information security service provider. The involved topics in the process are user management, software management and asset management. When introducing the former identity management process, security risks in the process are introduced with organization point of view and end user point of view. After the information security risks, the prospective identity management process, which introduces user management, software management and asset management capabilities with Azure Active Directory and Microsoft Intune, is introduced. The last sections are about application and device lifecycles and a comparison of the identity management processes is included.

To understand identity management, understanding ‘identity’ is a must. In Information Technology, identity and more specifically digital identity, signifies descriptive characteristics of object. The objects in the most cases are humans, the users of information systems, who has got different descriptive characteristics of itself, a one example of that is a username. In the real world, user’s digital identity is a general concept of a person. A person can have multiple digital identities located physically in different information systems, one digital identity in workplace’s information systems and another one in webstore as a regular customer. (Linden 2015.)

Identity management signifies a process, where objects are represented as digital identities in information systems. The process consists of information systems, agreements about syntax and semantics along with different methods how data is maintained and how data runs on between different information systems. With identity management is occasionally mentioned ‘access management’ concept. Access management is the function of information system that authorizes user and checks, if the user has suitable rights to access the information system. One popular example of that is that web application requires to enter username and password in order to access the web application, if authorization is successful, user is notified. Together identity management and access management forms a concept titled identity and access management. (Linden 2015.)

6.1 User management in the former process

At information security service provider, the former user management process had two alternatives to control the users in the organization, either the user was located in an on-premise Active Directory or at Office 365 with cloud identity model or synchronized identity model. The mentioned identity models are explained previously in the fifth chapter. One additional group was formed of users who were not located in Active Directory, in other directory service or in Office 365.

On-premise Active Directory users were distributed across the globe to multiple servers. As an example, all the users in Joensuu were in the on-premise Active Directory or all the users in India, because some of the regional offices had Active Directory in use. The users located in Office 365 had the cloud identity model or synchronized identity model. Cloud identity model users were located only in the cloud. Synchronized identity model users were synchronized to Office 365 from the on-premise Active Directory. In both separate cases, Information Technology team could then manage those users from Office 365 via web browser.

The last remaining group of users was formed of users who are in countries that does have a regional office, but does not have Active Directory, other directory service or Office 365 in use. In this thesis those users are referred as non-directory service user.

6.2 Software and asset management in the former process

The software management and hardware management at information security service provider was limited to be done within one specific software, Samanage. Samanage is an Information Technology Asset Management (ITAM) and service desk Software as a Service (SaaS) provider (Samanage 2016). The company's Samanage ITAM software offers capabilities to manage organization’s hardware and software inventories with web-based software. The software works on operating systems including Windows, Mac and Unix and on mobile operating systems, iOS and Android are supported. (Samanage 2016.)

Software management with Samanage adds the possibility for system administrator to automatically track software in organization. For that matter, Samanage provides its own tracking software, Samanage agent. The Samanage agent is possible to deploy from Active Directory or with email (Samanage 2016). When the tracking software is deployed, it will start to ‘track software’ and place the software to the repository, which system administrator has created earlier. The repository can contain information about different software, for example software name, vendor and detection date is displayed. (Samanage 2016.)

Hardware management with Samanage works the same way as the company's software management solution. The Samanage agent collects also hardware information. The software can detect hardware information including vendor, memory and storage information and warranty information of computers. As with software management part of the Samanage ITAM solution, the hardware management part of the solution collects all the information to the repository, what system administrator has created earlier. This way the Information Technology team is possible to track the assets, what is the location of a certain computer, to who does the specific computer belong and what is the status of warranty. (Samanage 2016.)

With ITAM solution, it can be useful to manage the IT assets effectively in a decentralized organization. From the third figure, can be visualized the fact that managing information security service provider's users, assets and software can be challenging without ITAM solution. Particularly, if the Information Technology team and its resources are limited to one team and country. The figure illustrates the computers at a global level in the organization. From left-to-right, in the North America region there are about 16% of global computer amount. In the Europe, the middle East and Africa region there are about 50% of global computer amount. And in the Asia Pacific and Japan region there are about 34% of global computer amount.

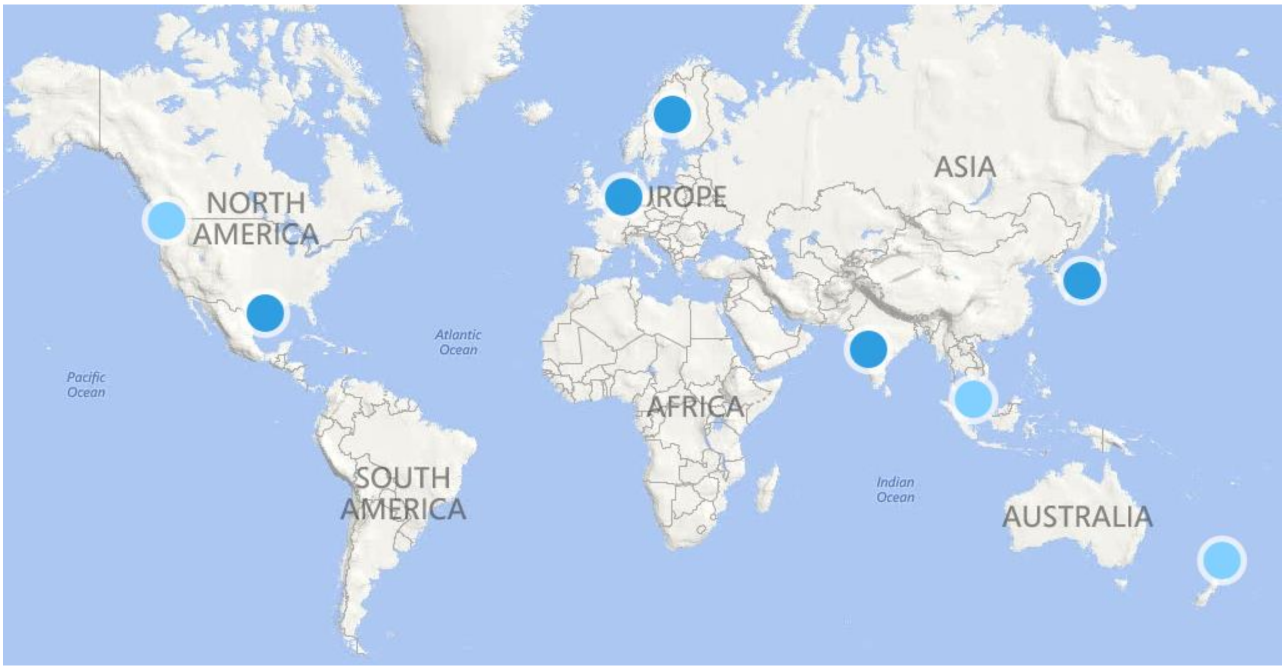


Figure 3: Computers at information security service provider. (Figure: From Samanage, 2016.)

6.3 Information security risks in the former process

According to the Management at information security service provider, the first and the most significant goal of the centralized identity management project at information security service provider is to improve the user management process. Improved and better user management process will also improve the information security at information security service provider. The second goal is to improve software and application management in the organization. In the former process, there were no capabilities to manage applications in user's mobile devices. As well as managing software on devices was not organized well. The organization had the possibility to track down applications that were installed on self-owned mobile devices and software installed on computers. But the Management and the Information Technology department was not able to control, what applications and software the users could install. When an employee exited, that was by itself a considerable information security risk, because Information Technology department could not control the employee's device or its software and applications. (Management of information security service provider 2016.)

By putting Azure Active Directory and Microsoft Intune into operation, these services will assist with the software and application management in the organization. In the prospective identity management process, Information Technology department is capable to control commercial services and the access to these services, such as version control, issue tracking and customer relationship management, from various service producers. Information Technology department has the capabilities to minimize the information security risks by recognizing the applications and software that are information security threats. And the team has the tools to remove the possible threat with remote accessing the target device. Installing only applications and software to a device that are required to complete work tasks, improves the prospective identity management process information security. (Management of information security service provider 2016.)

The project, at this phase, will simplify the user management process as the users are in the Azure Active Directory cloud service. Probably one of the worst-case scenarios in the former identity management process was when an employee left. The employee had the opportunity to leak confidential information such as organizational secrecies and proprietary source code anonymously to the Internet or to a competitor. That could imperil the competitive position of information security service provider. (Management of information security service provider 2016.)

6.4 User management in the prospective process

User management in the prospective identity management process benefits of Azure Active Directory to store and manage users in the cloud service. In the prospective process, all of information security service provider’s users are located in the cloud service. The user management in the former process had multiple directories where users were located or some users were non-directory service users. The prospective user management process is centralized to Azure Active Directory. There will not be users who are not located in any directory service, because all of the users are stored in Azure Active Directory.

Information security service provider uses Azure Active Directory Connect to integrate on-premises directories with Azure Active Directory. The Connect is a tool to provide a common identity for users to access Software as a service applications that are integrated with Azure Active Directory. Common identity is a single identity to access cloud and on-premises resources, if there are applications that cannot be accessed from the cloud. The mentioned applications can consist of tools that are developed only to handle a specific task or tasks internally, inside organization’s network. Because Azure Active Directory Connect enables the opportunity to let user have one common identity, the user does not have to use multiple user credentials to access cloud applications or on-premises software. (Mathers 2016.)

6.5 Software and asset management in the prospective process

Managing software and applications in the prospective identity management process takes advantage of Azure Active Directory and Microsoft Intune. More specifically explicated, Access Panel in Azure Active Directory and Microsoft Intune mobile application and device management. The Access Panel is a web portal for end users to view and launch cloud based applications that are integrated with Azure Active Directory and granted to access by system administrator. For clarification, if system administrator has granted end users access to Salesforce.com, an Azure Active Directory integrated cloud application, end users have the Salesforce.com application button available in the Access Panel user interface. End users are capable to click the application button to access the resource with single sign-on (SSO) enabled, if the application that end user desires to access awaits for password input for accepted authentication. (Vilcinskas 2016.)

The fourth figure below illustrates the user interface of Access Panel for fictional organization “Wingtip Toys”. Below the Wingtip Toys logo, are controls to change the view between applications, groups, approvals and profile. Applications is a view for various cloud-based applications that are used in organization. Groups is a view to self-manage groups in organization. And approvals is a view to check, if an system administrator approval is required to self-assign access to an application. In the profile view, end user can manage organizational account settings such as password change or reset.

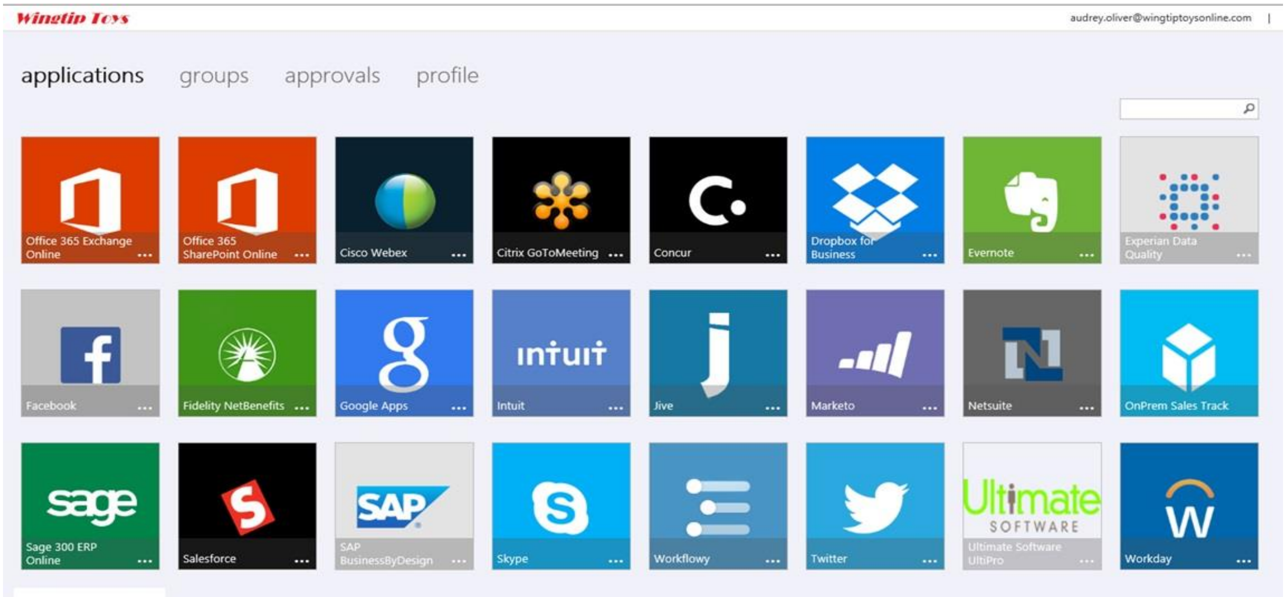


Figure 4: Access Panel user interface for fictional organization. (Figure: Vilcinskas 2016.)

To use supported Access Panel applications with mobile devices running Android or iOS, Azure Active Directory development team has developed My Apps mobile application. My Apps is supported on Android versions 4.1 or later and on iOS versions 7 or later. On Android devices, My Apps is available in the Google Play Store and on iOS in the Apple App Store. My Apps supports applications that are supported by Azure Active Directory and granted for access by system administrator. Supported applications can be used from web browser or with native mobile application. (Vilcinskas 2016.) Native mobile application, in this context, is an application that is developed for specific mobile operating system.

6.6 Application lifecycle

This subchapter explicates application lifecycle process in Microsoft Intune. The process should be perceived as a standard process that all organizations should take with Intune. With Intune organization's Management and Information Technology department has the tools to manage the application lifecycle process. The process consists of five phases that are adding an application to organization, deploying an application for organizational use, configuring an application to meet organizational policies, protecting an application against misuse and information security issues and retiring an application. (Stack 2016.) All the mentioned phases are presented in the fifth figure below.

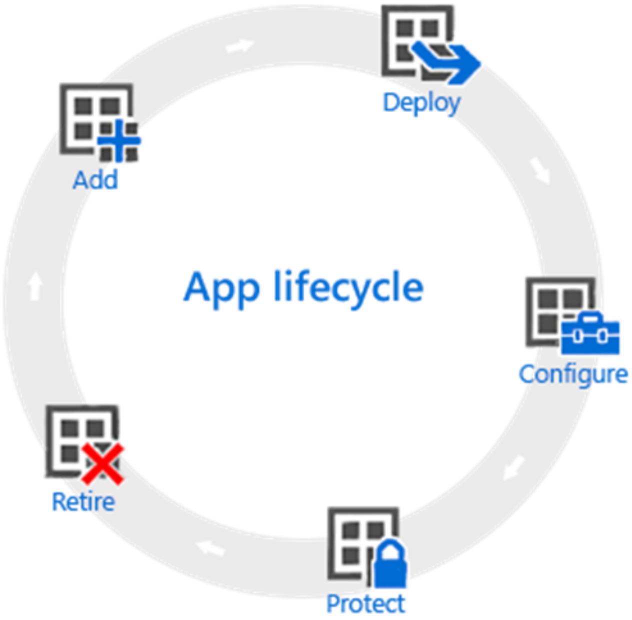


Figure 5: Application lifecycle in Microsoft Intune. (Figure: Stack 2016.)

Adding an application is a phase where Information Technology department reviews an application that is a candidate to become application for organizational use. The department will make sure that Intune supports the application or software format and it works on required devices. Intune supports various installer formats including Android, iOS and Windows Phone installers and Windows installers. Universal Windows Platform applications are supported. These applications will run on all Windows-based devices. (Stack 2016.)

Deploying an application is a phase where reviewed applications are deployed for organizational use. Intune has four deployment actions for application deployment. Required install is about an action, where an application is installed to a device without user actions. Available install displays an application in Intune's Company Portal, an additional application for Intune, that users are capable to install. Uninstall action is an action to uninstall an application from user's device. Not applicable action is an action, where applications are not displayed in Company Portal and cannot be installed to devices. (Stack 2016.) Along with application deployments, Intune offers monitoring capabilities via Intune administration console. System administrator has a tool to monitor various details about certain applications such as information about application installations, information about devices and users, who have installed targeted deployment of an application. (Stack 2016.)

Configuring an application to meet organizational policies is a phase where deployed applications are managed with organizational policies in mind. In configuration phase, it is possible to update applications, configure iOS or Android for Work applications with mobile application configuration policies, use iOS mobile application provisioning policies to prevent applications from expiring and manage Internet access with Intune. Configuring the updating process of applications that are deployed basically features opportunity for system administrator to update an application before end user can download the update. Mobile application configuration policies contain modifiable settings, such as localization and a custom port number. To prevent iOS mobile business applications from expiring, Intune offers a way to manage the expiring applications and create iOS mobile provisioning profile policies. To manage Internet access Intune features a tool for Android and iOS, Microsoft Intune Managed Browser. It is a deployable web browser application to restrict or allow website access. The application is available on Android devices with 4.0 versions or later and on iOS devices with 8.0 versions or later. (Stack 2016.)

Protecting an application against violation and information security issues is a phase where with Intune is possible to protect organizational data with two technology layers. The two technology layers are identity layer and client application layer. The identity layer protects accessing services by allowing users to access only from managed devices. The client application layer tries to prevent data perishing with device wipe, if a device is stolen or lost, and moving data to non-protected storage locations or to non-protected applications. Both technology layers combined produces maximal protection for organizational data that Intune can offer. As a practical example system administrator can create rules to restrict access to encrypted devices and on application layer copy, paste or backup to personal storage can be restricted. (Raman 2016.)

Retiring an application is a phase, where an application is uninstalled from target device. Lifecycle of an application ends to this phase, if a certain application is not valuable, market offers a better replacement to the application or the application does not meet organization’s policies. The process for uninstalling is the same for Windows PCs and mobile devices. (Stack 2016.)

6.7 Device lifecycle

Device lifecycle process clarifies the device management and adds capabilities to Microsoft Intune that are explicated in this subchapter. As with the application lifecycle, the process should be perceived as a standard process that all organizations should take with Intune. The process consists of four phases that are enrolling a device to Intune, configuring enrolled devices to meet organizational policies, protecting a device against misuse and information security issues and retiring a device. All the four phases are presented in the sixth figure.

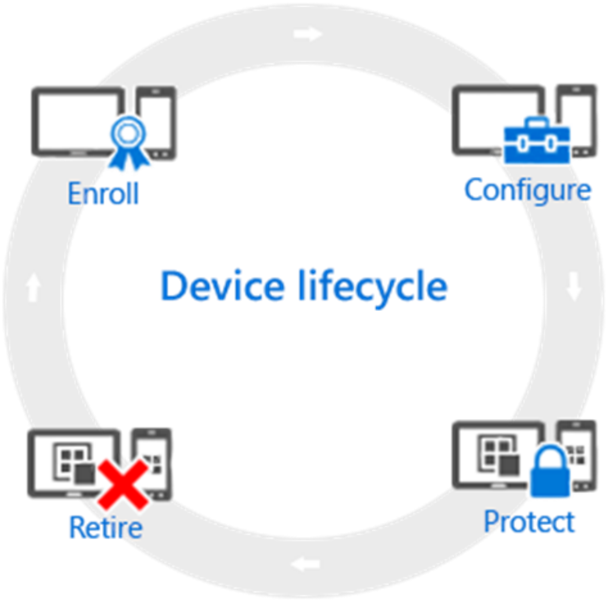


Figure 6: Device lifecycle in Microsoft Intune. (Figure: Stack 2016.)

Enrolling a device to Intune is a phase where Information Technology team enrolls an organization or an employee owned device to Intune. Enrollable devices consist of mobile phones, tablets and PCs and enrolling a device to Intune enables mobile device management capabilities. (Stack 2016.) Device management with Intune were mentioned and introduced earlier in the fifth chapter.

Configuring enrolled devices to meet organizational policies is a phase where organizational standards are managed through Intune’s configurable policies to improve devices information security and to support of organization values. Intune features three types of policies, configuration, company resource access and Windows PC management policies. With configuration policies, it is possible to disable application on a device such as camera or set up Microsoft Outlook email profile. (Stack 2016.) Company resources access policies provides access to network resources and files that employee must use to get work tasks done, for example, controlling access to user’s Microsoft Outlook mailbox. Windows PC management policies expands system administrator’s capabilities to manage and control PCs (Barker 2016).

Protecting a device against misuse and information security issues is a phase to protect enrolled devices to follow rules added in the configuration phase. There are three methods available in Intune to protect devices. Multi-factor authentication is one of the methods and the concept was described earlier in this thesis in the second chapter. Microsoft Passport works as an additional sign-in method to let users authorize identity to sign-in to applications and services by using user gestures. User gesture is a biometrical authentication method, such as fingerprint or facial recognition. The last method consists of policies to protect Windows PCs with Intune, the mentioned policies includes controlling software updates, Windows Firewall settings and Endpoint Protection. Endpoint Protection is a real-time malware protection software built-into Microsoft Intune, including automatic computer scan and malware definition update. (Stack 2016.)

Retiring a device is a phase where employee leaves organization, device is lost or when there is a need to repurpose a device for another use. With Intune, it is possible to fully wipe the mass storage or selectively wipe the mass storage of a device. Wiping in Intune removes target device from Intune management. After the wipe, the target device has no credentials to sign-in to organizational resources. Selective wipe method is useful when employee has used its own device to complete work tasks, removing only corporate data. Full wipe will reset the target device to factory default settings. In retirement phase, it is also possible to block the access to a device, in case the device is lost. Intune offers a way to remotely lock a device. Misuse of the device and its data will be temporarily or permanently prevented. (Barker 2016.)

6.8 Comparison of the identity management processes

As there was Samanage ITAM solution in use in the former identity management process, the prospective identity management process provides improved opportunities to user, software and hardware management processes. Azure Active Directory introduces cloud-based multitenant directory and identity management service. With Samanage Management and Information Technology department at information security service provider could track software and hardware information on mobile and desktop devices. The agent collected the information to the repository as introduced earlier in the sixth chapter. That was basically all the visibility and control Management and Information Technology department had. The user management in the former process was intractable to control. User directories located in various Active Directory servers across the globe, with lack of knowledge who is responsible of the user management in a certain country. Also, lack of centralized management and obscure responsibilities in the cases were inside the organization. Azure Active Directory provides a solution for the mentioned reasons, because of its scalability and cloud-based service.

The prospective identity management process introduced the Access Panel as the application user interface. It can be considered as a tool for both parties, end users and system administrators. End users have the visibility to all the applications that are relevant to their needs. Clicking or touching on Salesforce.com logo forwards an end user to the cloud application and signs the user in, if SSO is enabled. In case the password is lost, an end user can change or reset the organizational account password without the system administrator's help. These self-management capabilities increase the productivity of Information Technology department. The department can focus on more important tasks and issues, instead of solving issues that end users can solve by themselves.

Microsoft Intune entails the application and device lifecycle processes with as strict information security policies as information security service provider desires. The application lifecycle with adding, deploying, configuring, protecting and retiring an application. And the device lifecycle with enrolling, configuring, protecting and retiring a device, illustrates two processes that are built with information security policies in mind. Various phases help the department to manage and built Information Technology infrastructure in a controlled and secure way. If there are couple of applications that can be used to handle identical tasks, the preferable can retain and its competitor can be retired.

7 Conclusion of the identity management

This chapter is a conclusion of the identity management at information security service provider. The chapter and the subchapters features main missions of the study and research, a comparison about how the prospective process will eventually change the identity management at information security service provider, the most significant factors in the identity management process at information security service provider and the researcher's observations of the complete identity management infrastructure.

In this thesis, the main missions were to study the identity management at information security service provider, by introducing the technical platforms and concepts, what are present in Microsoft’s identity management infrastructure, the former and the prospective identity management processes and the most significant information security risks in the former process. The technical platforms were about understanding the Active Directory, Microsoft Azure, Azure Active Directory, Office 365 and Microsoft Enterprise Mobility and Security. The concepts were about understanding identity and identity management. The prospective identity management process explicates the Azure Active Directory as the user management tool. It should not be considered as a full replacement for Active Directory and its services. These two services combine cloud-based and on-premises directories to encounter the requirements of a global decentralized organization. Understanding the technical platforms, the concepts, the identity management processes and the information security risks in the former process, will help to understand what must be done for the Information Technology infrastructure to control and manage identities from the cloud.

7.1 Improvements in the identity management process

Chart 2 illustrates the comparable features between the former and the prospective identity management processes at information security service provider. The former process features in the chart are listed on the left side, below the title “Former process”. On the right side, next to the former process title are the prospective process features, below the title “Prospective process”. “Yes” or green color indicates that the feature is available in the specific process. “No” or red color indicates that the feature is not available in the specific process. “Moderately” or light green color indicates that the feature has been available in the former process with moderate capabilities.

Identity Management Comparison Chart			
Former process		**Prospective process**	
Centralized management of users	No	Centralized management of users	Yes
Software and application tracking	Yes	Software and application tracking	Yes
Device tracking	Yes	Device tracking	Yes
Capabilities to control software and applications and remotely control devices	No	Capabilities to control software and applications and remotely control devices	Yes
Desktop and mobile portal for cloud-based applications	No	Desktop and mobile portal for cloud-based applications	Yes
End user self-management capabilities	Moderately	End user self-management capabilities	Yes
Single-sign-on for cloud-based applications	No	Single-sign-on for cloud-based applications	Yes
Application lifecycle	Moderately	Application lifecycle	Yes
Device lifecycle	Moderately	Device lifecycle	Yes

Chart 2: Identity Management Comparison Chart.

The former user management process, described the two alternative platforms of the user management, Active Directory and Office 365. Also, to remember that some of the users were non-directory service users. Therefore, based on the available information, it is declared that centralized management of users was not available in the former process. In this thesis, centralized management indicates availability and management for all the resources, such as knowledge of all employees and ability to control the employee leave. Because lack of the centralized user management in the former process, it was obviously one of the goals to improve the user management in the prospective process. Azure Active Directory, will aim to work better for information security service provider’s identity management requirements, because it functions in the cloud to serve as a resource for centralized management of the users with on-premise Active Directory alongside. With Azure Active Directory, network resources such as cloud applications in the Access Panel, can be accessed from anywhere, where Internet connection is enabled.

In the sixth chapter were introduced the former software and application management, as well as the former asset management processes. Samanage operated in the center of the processes to provide a solution for solving software and application management and device management issues. In other words, Samanage provided software and application tracking and device tracking. Even though there were the mentioned tracking capabilities, Samanage was used only to track and report data about the software and asset resources. However, Microsoft Intune provides the tracking features that were part of Samanage. But also, more features to manage and control software on PC, applications on iOS device or to get control of an entire device. For example, after a device is enrolled to Intune, it assists system administrator to visualize what kind of devices are enrolled to an organization and enables device management features such as wiping a tablet remotely, if the device is stolen.

To control software and applications and remotely control devices, Information Technology department probably had the skills, but management policies or technical platforms were not strictly defined. Samanage was decent at tracking and reporting, but for application control and data control policies it was not the best solution. It is also about the data that these software or applications produces. To this question and need Microsoft Enterprise Mobility and Security will presumably answer, if the services and tools are utilized as built to. Microsoft Intune provides mobile application management and mobile application security to support decentralized organization need for scalability and security. As it was stated earlier in the sixth chapter, Intune offers a solution to create application policies that Information Technology department can configure to match the organizational data policies (Raman 2016). The application policies assists to manage organization licensed applications in a more secure way, such as preventing employee copying a text document about unreleased products of information security service provider and releasing it to the mass media. Therefore, Azure Information Protection service secures document and data integrity on a device that might not be available physically. For device control demand, Intune supports remote assistance, alongside with wiping a device that was earlier mentioned in the previous section. Remote assistance is an Information Technology Support tool to provide technical support for employees in organization. For that matter, Microsoft has connected an opportunity to separately buy TeamViewer remote assistance software, which is then integrated with Intune (Stack 2016). Employee with a Windows PC, can request technical support remotely and system administrator is then notified by an alert via Intune. If the preceding feature is launched and used at information security service provider, Information Technology department can take the responsibility and assist employees requesting technical support. That should then separate the blurred border between Information Technology and Technical Support departments, where the Technical Support operates on the client interface.

The prospective process presumably facilitates accessing applications, by way of Azure Active Directory Access Panel. When all cloud-based applications are in a particular location, an employee does not have to use bookmarks in a browser to memorize the application website. Access Panel probably standardizes the repository for cloud-based applications, with simplified management and self-management along with SSO on certain applications. The capabilities were introduced more thoroughly in the sixth chapter. Cloud-based applications are available in both, mobile and desktop devices.

Application and device lifecycles in the former process were not introduced nor described. The most significant reason is that the lifecycles were not a strict part of the software and asset management. “Moderately” in the second chart is to indicate the loosely controlled lifecycles. Employees in the organization could download a software to a workstation and start using it as a standard tool that is not accepted by Management or Information Technology department. That ‘standard tool’ could then spread worldwide, even if there was an applicable software for that specific matter, it was first downloaded. In the worst-case scenario, the downloaded ‘standard tool’ could cause an information security risk, if no critical judgment were present at the time, when the decision was made. The prospective process introduces application and device lifecycles that were earlier introduced in the sixth chapter. The strictness should increase information security by providing built-in phases to follow, with critical judgment to evaluate, if an application is required in long term. The lifecycles allegedly becomes a management tool to globally assist streamlining management of software, applications and devices.

7.2 The most significant factors in the infrastructure

Based on the information that was available at the time of writing and information that is described in this thesis, the most significant factors in the identity management process at information security service provider are chief of Information Technology department and Management. First, to explicate this proposition thoroughly, before any decisions are made in projects that are as substantial as the identity management project at information security service provider, chief of Information Technology department and Management must be able to register the main reasons behind the project. The reason or reasons, for example, can be information security risk in controlling employee arrival and leave or a practical urge to improve identity management process. After the reasons are discovered, both mentioned parties evaluate together what kind of solutions there are available in the market and is there something that can be done inside the company. Or does the company order the whole solution from a third party as a turnkey project. Probably it is time-consuming to try to start and finish a project outside of expertise of information security service provider. As in this project, the whole solution was ordered from an Information Technology infrastructure company that has done similar projects earlier. After the mentioned phases and bureaucracy, comes the phase when a third-party solution provider and information security service provider starts to discuss more specifically about the actual plan of the project. When everything is settled, the plan probably contains practical steps that are executed in monthly and weekly basis, until the project is ready.

To successfully navigate through all the phases to a phase where the final product is launched, decision-makers must understand a lot about various technologies and technical platforms, which are represented in this thesis, from the second chapter to the sixth chapter. Understanding the technologies and technical platforms that are present helps to find an alternative service, for example, to improve a complete process and to improve productivity or information security. That may become necessary, when thinking through a replacement for Samanage, introduced in the sixth chapter as a core element of the former software and asset management service. Also, if the Information Technology infrastructure is not scalable to meet requirements of the global company, it should be considered that is there precisely a need for Infrastructure as a Service solutions, such as Microsoft Azure.

Of course, understanding how the current or in this thesis the past, identity management solution worked in Information Technology infrastructure, at least at a general level is important. Because, to understand the better identity management solution, first the decision-makers should have a clear picture of the past solution and its issues. If there are no discovered issues there probably is a reason for that and the reason delivers an answer to the question, why to improve the current identity management solution?

For the settlement of all the mentioned needs and the questions that must be answered, presumably, will be entrusted either a chief of Information Technology department or Management or both together. The entrusted parties will decide the final technologies, technical-platforms and solutions. To make the decision that changes a lot in Information Technology infrastructure, it takes all the mentioned points and the fact that behind the decision is an actual reasonable cause.

7.3 Researcher's observations

First, user management in the former identity management process, was not organized well. The process in question had users that were distributed to Active Directories and then integrated to Office 365 cloud service. In some countries, there were no such user management possibilities and that could create a situation where the user does not exist in directories of the company, as stated in the sixth chapter. It directly challenges responsible parties, who are trying to figure out how to grant access to a specific application with different user rights, how Human Resources Management stays up to date with employee information and other challenges that could be imagined. By centralizing all the company users to Azure Active Directory cloud service, the user information stays up to date and it is secured and the cloud service eliminates the mentioned issues. Naturally, to achieve the best outcome, the Azure Active Directory admin must make sure that the configuration is carefully done.

Secondly, software and asset management in the former identity management process had a lack of management capabilities, as stated in the sixth chapter. It introduced Samanage, which features software and hardware repositories and visual reporting tools, for what the Samanage in practice was used. In the same chapter was also stated that without Information Technology Asset Management solution it can be challenging to manage software and hardware resources in the company. When the resources are manageable at high-level, it does not automatically mean that the same resources are manageable at the lower-level. Samanage did not offer a full control of customer’s applications and devices. There are many information security issues introduced in this thesis, for example in the seventh chapter. I personally think that data leakage is one of the major issues, when trying to make a global breakthrough in information security business. If an average Joe has the possibilities to leak company secrets to a competitor, when the company has no keys to control user's device and the software of the device, I consider it as a very high information security risk. With the new tools, Azure Active Directory and Microsoft Enterprise Mobility and Security licenses, the company is able to begin standardizing the user, software and asset management processes, as well the complete identity management process and develop the processes to meet the requirements of information security service provider. The service provider also should remember to create appropriate policies signed by employees, if employees are adapting bring your own device (BYOD) possibility. Because Microsoft Intune supports the function to let employee use hers or his own laptop, and to use the device to access privileged company information or applications.

The identity management topic of this thesis is truly very wide and has a lot of angles that requires analyzing. For example, access management was left off from this thesis, because it would have affected the extent of the research. There are many researches and theses that covers Active Directory and user and access management, but only a few of them introduces Azure Active Directory. By developing the Identity Management and its sub processes, it allows to create various operations models that were not possible to think about before. Also, productivity should increase in operations that were causing bottlenecks. Increasing productivity saves time an employee spends on working with a particular work task and customer can enjoy for better and faster customer service. The same outcome has been noticed in many researches§ and theses that covers identity management or identity and access management. For example, Mikael Linden from Tampere University of Technology has researched and reported about identity and access management in 2015.

At the time of writing, information security service provider started the centralized identity management project to improve identity and access management inside the organization. The first deadline of the project was on late September in 2016, which could not be reached. Presumably this thesis will assist to get to know with various technical concepts and platforms. This document also provides possible hints and ideas, when developing the complete identity management process and with this document it should be easier to justify the decisions behind the centralized identity management project.

7.4 Thesis as a process

For the writer, the topic was a bit unclear and sometimes lack of knowledge caused frustration. Many topics of this thesis were not familiar at all. But after the difficulties were defeated, everything became clearer by studying and it is very rewarding for a student who aims to be a specialist someday. Topic of this thesis was selected from the commissioner, information security service provider, as thought it would be a great opportunity to do a thesis about a ‘real’ project in Information Technology field. After the bureaucracy phase, which included contracts between Karelia University of Applied Sciences, the commissioner and writer, planning the writing process began. Completion of this thesis was originally scheduled to 15th of December 2016. At the time of writing, it is 21st of December 2016 and there will still be the last seminar in January 2017. Also, there are minor grammar issues and corrections to be made. After all, writing is a creative process, which can be scheduled and done within the schedule. Personally, I wanted to serve the commissioner and myself the best possible way. Most likely that is the main reason for the minor delay, from the originally scheduled due date.

At the beginning of the writing process, the fact was faced that original idea of this thesis changed. The original idea was to create a guide for employees of information security service provider, about Azure Active Directory domain join for Windows, Linux and OS X (macOS). That guide could then be used to school the employees. But the project changed in the company and it turned this thesis into a research without functional part. Adapting changes in everyday changing working life is one of the skills that Information Technology student or specialist must have. This research about centralized identity management and how the project will eventually change identity management at information security service provider, was not wrecked by that change. It offered a gateway to learn about Microsoft Azure infrastructure, what it contains and how its various services are challenging on-premises Information Technology infrastructures with cloud services. The matters are represented in this thesis, from the second to fifth chapters.

As mentioned earlier, during the planning and writing processes, there have been unclear topics, which are now transformed into lucid reading experience. Amongst this, learning about Microsoft and its Information Technology and cloud infrastructures will presumably assist to bring new ideas for a company, who decides to employ me. This thesis is made up of hours and hours of research, unclearness, success and urge to show that there are potential in interns, who are not employed directly after the internship.

References

Barker, S. 2016. Common Windows PC management tasks with the Intune software client. Microsoft. https://docs.microsoft.com/en-us/intune/deploy-use/common-windows-pc-management-tasks-with-the-microsoft-intune-computer-client. 11.11.2016.

Barker, S. 2016. Retire devices from Intune management. Microsoft. https://docs.microsoft.com/en-us/intune/deploy-use/retire-devices-from-microsoft-intune-management. 11.11.2016.

Barnett, N. 2016. Enroll Devices For Management In Intune. Microsoft. https://docs.microsoft.com/en-us/intune/deploy-use/enroll-devices-in-microsoft-intune. 28.10.2016.

Bailey, C. 2016. How Does Azure RMS Work? Under The Hood. Microsoft. https://docs.microsoft.com/en-us/information-protection/understand-explore/how-does-it-work. 28.10.2016.

Bailey, C. 2016. What is Azure Information Protection. Microsoft. https://docs.microsoft.com/en-us/information-protection/understand-explore/what-is-information-protection. 27.10.2016.

Bailey, C. 2016. What is Azure Rights Management. Microsoft. https://docs.microsoft.com/en-us/information-protection/understand-explore/what-is-azure-rms. 28.10.2016.

Boucher, B. 2015. Introducing Microsoft Azure. Microsoft. https://azure.microsoft.com/en-us/documentation/articles/fundamentals-introduction-to-azure/#the-components-of-azure. 5.10.2016.

Collier, M. Shahan, R. 2016. Fundamentals of Azure, Second Edition. Washington. Microsoft Press a division of Microsoft Corporation.

Conway, A. 2016. Introducing Enterprise Mobility + Security. Microsoft. https://blogs.technet.microsoft.com/enterprisemobility/2016/07/07/introducing-enterprise-mobility-security/. 10.10.2016.

Gremban, K. 2016. Azure AD Privileged Identity Management. Microsoft. https://azure.microsoft.com/en-us/documentation/articles/active-directory-privileged-identity-management-configure/. 25.10.2016.

Gremban, K. 2016. What is Azure Multi-Factor Authentication. Microsoft. https://azure.microsoft.com/en-us/documentation/articles/multi-factor-authentication/. 7.10.2016.

Karthika, R. 2016. Protect App Data Using Mobile App Management Policies With Microsoft Intune. https://docs.microsoft.com/en-us/intune/deploy-use/protect-app-data-using-mobile-app-management-policies-with-microsoft-intune. 28.10.2016.

Kelly, W. 2015. Improving BYOD security with Microsoft Enterprise Mobility Suite. TechRepublic. http://www.techrepublic.com/article/improving-byod-security-with-microsoft-enterprise-mobility-suite/. 10.10.2016.

Linden, M. 2015. Identiteetin- ja pääsynhallinta. Tampere. Tampere University of Technology.

Love, C. 2016. Azure Active Directory editions. Microsoft. https://azure.microsoft.com/en-us/documentation/articles/active-directory-editions/#premium-features. 25.10.2016.

Mathers, B. 2016. Integrating your on-premises identities with Azure Active Directory. Microsoft. https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnect/. 8.11.2016.

Martin, S. 2014. Upcoming Name Change for Windows Azure. Microsoft. https://azure.microsoft.com/en-us/blog/upcoming-name-change-for-windows-azure/. 5.10.2016.

Microsoft. 2016. Azure integration with Office 365. Microsoft. https://support.office.com/en-us/article/Azure-integration-with-Office-365-a5efce5d-9c9c-4190-b61b-fd273c1d425f?ui=en-US&rs=en-US&ad=US. 9.10.2016

Microsoft. 2016. Office 365 Frequently Asked Questions. Microsoft. https://products.office.com/en-us/microsoft-office-for-home-and-school-faq#managingOffice365-section. 8.10.2016

Microsoft. 2016. Understanding Office 365 identity and Azure Active Directory. Microsoft. https://support.office.com/en-us/article/Understanding-Office-365-identity-and-Azure-Active-Directory-06a189e7-5ec6-4af2-94bf-a22ea225a7a9. 9.10.2016.

Microsoft. 2016. What is Azure. Microsoft. https://azure.microsoft.com/en-us/overview/what-is-azure/. 5.10.2016.

Microsoft TechNet. 2014. What Are Domains And Forests? Microsoft. https://technet.microsoft.com/en-us/library/cc759073(v=ws.10).aspx#w2k3tr_logic_what_pwxq. 1.10.2016.

Raman, K. 2016. Protect apps and data with Microsoft Intune. Microsoft. https://docs.microsoft.com/en-us/intune/deploy-use/protect-apps-and-data-with-microsoft-intune. 10.11.2016.

Samanage. 2016. Hardware Inventory Management. Samanage. https://www.samanage.com/products/computer-inventory/. 2.11.2016.

Samanage. 2016. ITSM Software, IT Asset Management, Help Desk Software, Samanage. Samanage. https://www.samanage.com/. 1.11.2016.

Samanage. 2016 It Asset Management (ITAM). Samanage. https://www.samanage.com/products/it-asset-management/. 1.11.2016.

Samanage. 2016. Deployment. Samanage. https://www.samanage.com/support/quick-start-guide/. 1.11.2016.

Samanage. 2016. Software Inventory Management. Samanage. https://www.samanage.com/products/software-inventory/. 1.11.2016.

Stanek & Associates. 2014. Active Directory Fast Start: A Quick Start Guide for Active Directory. Stanek & Associates.

Stack, R. 2016. Add apps. Microsoft. https://docs.microsoft.com/en-us/intune/deploy-use/add-apps#intune-software-publisher. 10.11.2016.

Stack, R. 2016. Deploy Apps. Microsoft. https://docs.microsoft.com/en-us/intune/deploy-use/deploy-apps. 10.11.2016.

Stack, R. 2016. Monitor app deployments in Microsoft Intune. Microsoft. https://docs.microsoft.com/en-us/intune/deploy-use/monitor-apps-in-microsoft-intune 10.11.2016.

Stack, R. 2016. Overview of device and app lifecycles. Microsoft. https://docs.microsoft.com/en-us/intune/deploy-use/overview-of-device-and-app-lifecycles-in-microsoft-intune. 9.11.2016.

Stack, R. 2016. Overview of the mobile device management (MDM) lifecycle . Microsoft. https://docs.microsoft.com/en-us/intune/deploy-use/overview-of-device-lifecycle-in-microsoft-intune. 10.11.2016.

Stack, R. 2016. Retire Apps. Microsoft. https://docs.microsoft.com/en-us/intune/deploy-use/retire-apps-using-microsoft-intune. 10.11.2016.

Stack, R. 2016. Update apps. Microsoft. https://docs.microsoft.com/en-us/intune/deploy-use/update-apps-using-microsoft-intune. 10.11.2016.

Stack, R. 2016. Request and provide remote assistance for Windows PCs. Microsoft. https://docs.microsoft.com/en-us/intune/deploy-use/common-windows-pc-management-tasks-with-the-microsoft-intune-computer-client#request-and-provide-remote-assistance-to-windows-pcs-that-use-the-intune-client-software. 23.11.2016.

Synergy Research Group. 2016. Amazon Leads; Microsoft, IBM & Google Chase; Others Trail. Synergy Research Group. https://www.srgresearch.com/articles/amazon-leads-microsoft-ibm-google-chase-others-trail. 5.10.2016.

Management of information security service provider. 2016. Management. Information security service provider. 10.8.2016.

Tulloch, M. 2013. Introducing Windows Azure. Washington. Microsoft Press a division of Microsoft Corporation.

Vilcinskas, M. 2016. Azure Active Directory Identity Protection. Microsoft. https://azure.microsoft.com/en-us/documentation/articles/active-directory-identityprotection/. 25.10.2016.

Vilcinskas, M. Introduction to the Access Panel. Microsoft. https://azure.microsoft.com/en-us/documentation/articles/active-directory-saas-access-panel-introduction/. 9.11.2016.

Vilcinskas, M. What is Azure Active Directory? Microsoft. https://azure.microsoft.com/en-us/documentation/articles/active-directory-whatis/. 11.10.2016.