LANTERIA CLOUD AND INTEGRATION WITH MS AZURE

Table of Contents

1.   About Lanteria HR

1.1. Solution Overview

Lanteria HR is a SharePoint based HRM solution that facilitates and automates the entire HR management cycle in a company. Lanteria HR provides central storage for all HR information, guides and supports HR processes and increases the performance of each employee and organization as a whole.

The distinctive feature of Lanteria HR is establishing of collaborative environment between HR department, line managers and employees in a company. Lanteria HR has the unique features for all company members that help them work as a solid team, increase performance and efficiently achieve the company goals.

Lanteria HR provides the following features:

- Building organizational structure and chart
- HR administration (employee database, HR processes, documents and notifications)
- Absence management
- Compensation and benefits
- Competence and goal management
- Appraisal and reviews
- Learning and development
- Recruiting
- Career and talent management
- Employee and manager portals

1.2. Architectural Overview

Lanteria HR is based on SharePoint. It is installed to the Windows Server that must have MS SQL Server (used as a database) and SharePoint installed.

Lanteria HR is installed as a site of the SharePoint site collection. The following image shows the Lanteria HR environment.
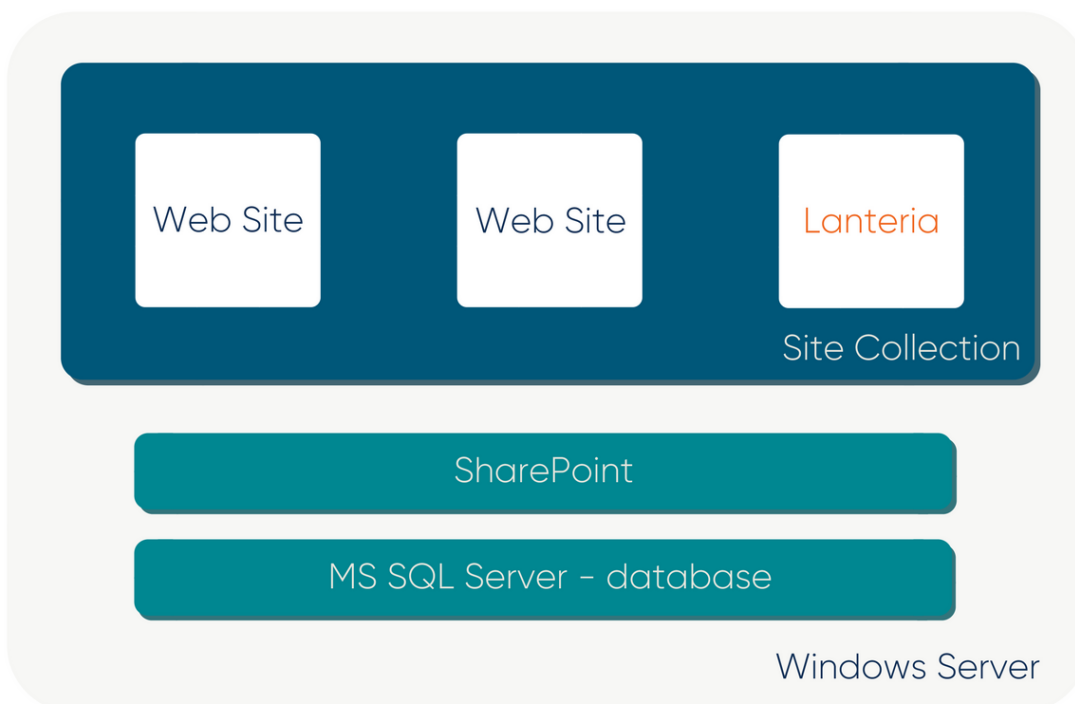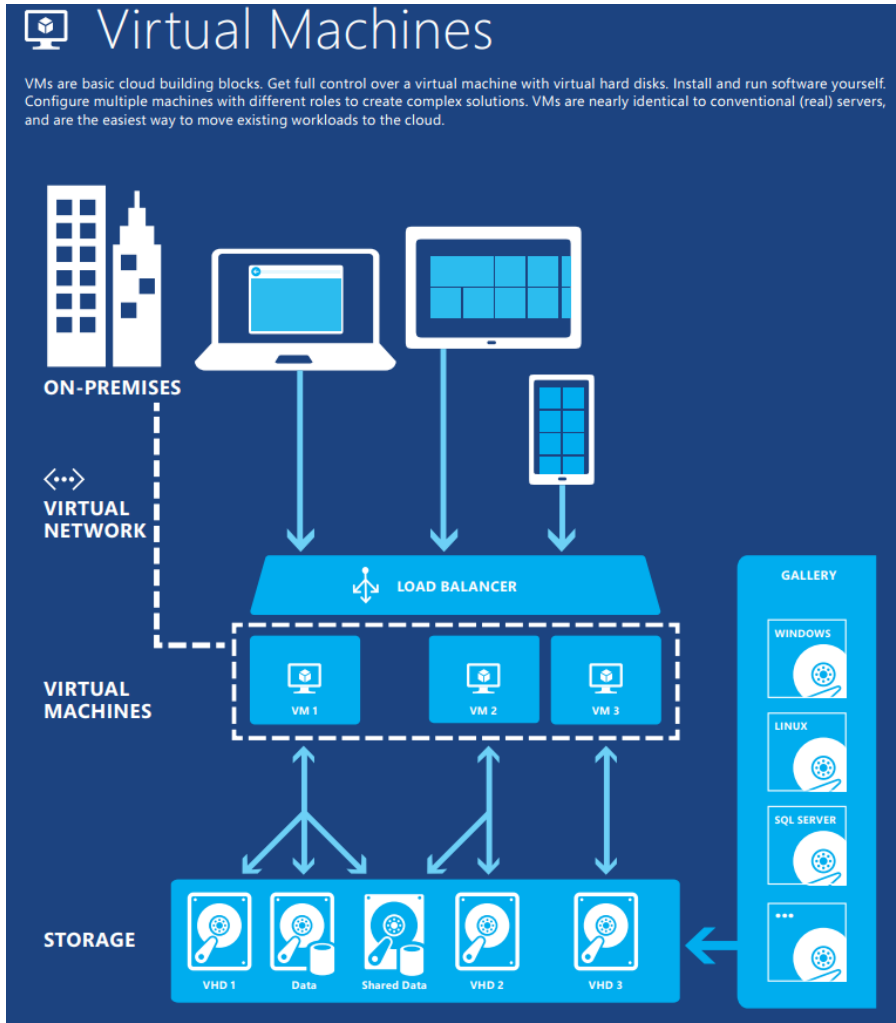
2.   Cloud Options

2.1.   Lanteria Cloud Introduction

Lanteria Cloud solution relies on the MS Azure services.

Lanteria uses services that are needed for the SharePoint web site hosting. The following image shows one of the most important compute services in the Lanteria HR Cloud environment.

Virtual Machines are combined into the Virtual Networks.

Lanteria Cloud consists of Virtual Machines with the SharePoint Foundation, SQL Web and Active Directory.

For backups, Lanteria uses Azure Backup Vault with Geo-redundant storage (GRS).

GRS replicates the data to a secondary region (hundreds of miles away from the primary location of the source data). It provides a higher level of durability for the data, even if there is a regional outage. Retention policy is two weeks.

The Cloud (SaaS – Software-as-a-Service) deployment benefits are as follows:

- Easier installation and updates
- Less initial investment
- System is fully supported by the vendor
- No infrastructure costs
- Accessible anywhere anytime

2.2. Shared Cloud

For small and medium HR solutions (< 500 employees), Lanteria offers a Shared Cloud (up to 5 clients per server). Shared Cloud is available in North Europe (Ireland) or East US (Virginia).

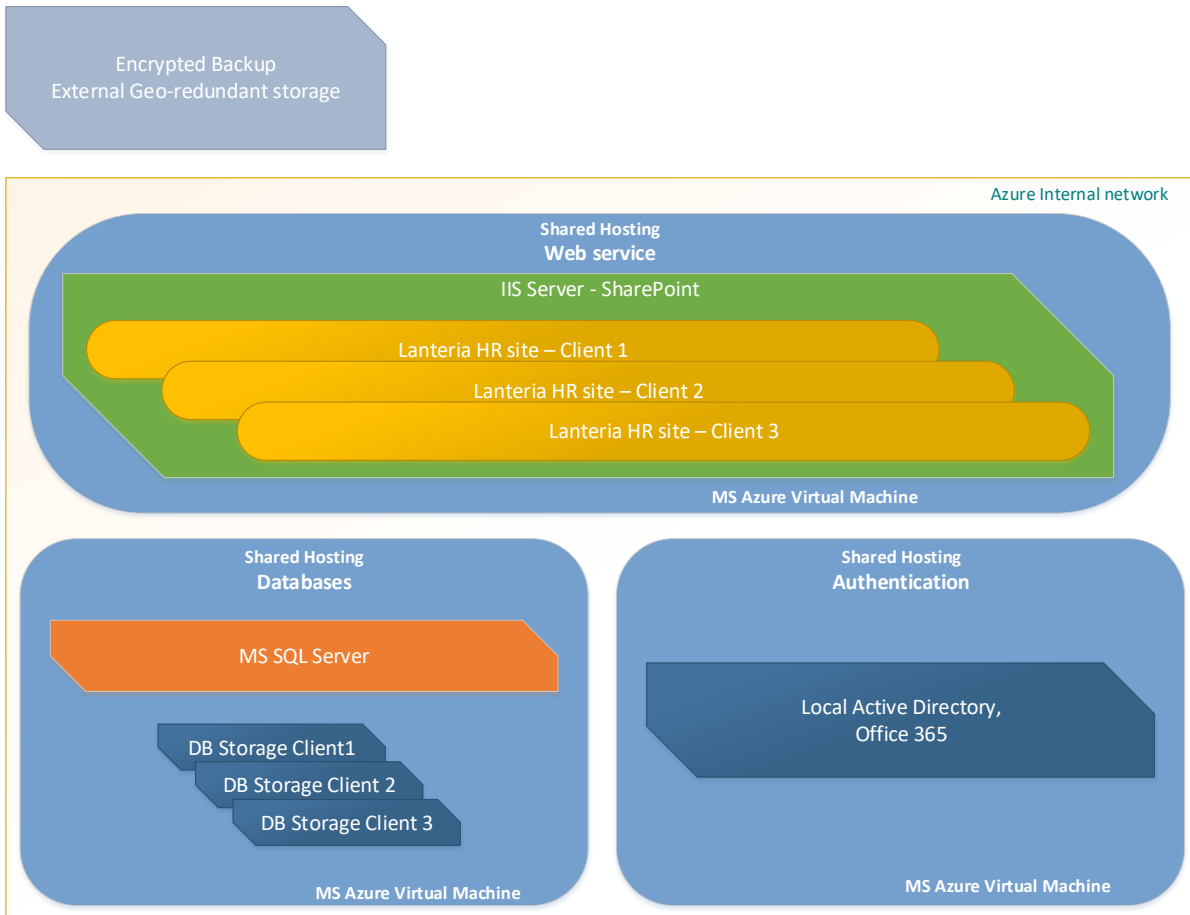Authentication is performed through the Local Active Directory or Office 365.

Shared Cloud allows sharing some cloud resources with other clients, while the customer data is separated and located on different physical storages.

Services that can be shared between the customers are as follows:

- Active Directory
- Web / SharePoint services
- SQL server

Every customer has its own SQL database, storage, DNS name, SharePoint site, Backup procedure. Client's Data can never be mixed up.

The following image shows typical outline of the Shared Lanteria HR Cloud environment.

Encrypted Backup
External Geo-redundant storage

Azure Internal network

Shared Hosting
Web service

IIS Server - SharePoint

Lanteria HR site – Client 1

Lanteria HR site – Client 2

Lanteria HR site – Client 3

MS Azure Virtual Machine

Shared Hosting
Databases

MS SQL Server

DB Storage Client1

DB Storage Client 2

DB Storage Client 3

MS Azure Virtual Machine

Shared Hosting
Authentication

Local Active Directory,
Office 365

MS Azure Virtual Machine

2.3. Private Cloud

For larger HR solutions, Lanteria offers a Private Cloud.

Authentication options are Local Active Directory, Client's Active Directory (via ADFS) or Office 365

It means that all the cloud resources are involved only for particular customer (usually on one server) and cannot be shared with anyone.

The following image shows typical outline of the Private Lanteria HR Cloud environment
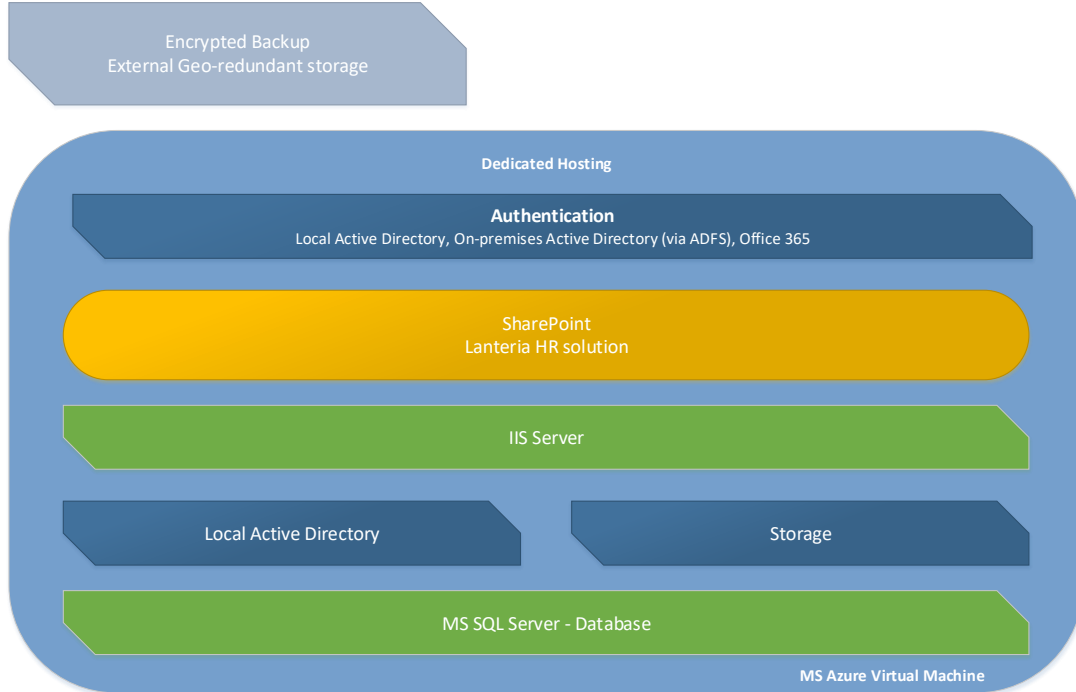
2.4. Server Technical Characteristics

For Lanteria Cloud, we use memory optimized VMs.

D-series VMs are designed to run applications that demand higher compute power and temporary disk performance. D-series VMs provide faster processors, a higher memory-to-vCPU ratio, and a solid-state drive (SSD) for temporary storage.

Size	vCPU	Memory: GiB	Temp storage (SSD) GiB	Max temp storage throughput: IOPS / Read MBps / Write MBps	Max data disks / throughput: IOPS	Max NICs / Expected network bandwidth (Mbps)
Standard_D11	2	14	100	6000 / 93 / 46	8 / 8x500	2 / 1000

Since 2018, Lanteria started using a new DS and B series. DS counterparts are ideal for applications that demand faster vCPUs, better temporary storage performance, or have higher memory demands. They offer a powerful combination for many enterprise-grade applications.

Size	vCPU	Memory: GiB	Temp storage (SSD) GiB	Max data disks	Max cached and temp storage throughput: IOPS / MBps (cache size in GiB)	Max uncached disk throughput: IOPS / MBps	Max NICs / Expected network bandwidth (Mbps)
Standard_DS11_v2	2	14	28	8	8,000 / 64 (72)	6,400 / 96	2 / 1500

The B-series VMs are ideal for workloads that do not need the full performance of the CPU continuously, like web servers, small databases. When the VM has accumulated credit, the VM can burst above the baseline using up to 100% of the vCPU when your application requires higher CPU performance.

Size	vCPU's	Memory: GiB	Temp storage (SSD) GiB	Base CPU Perf of VM	Max CPU Perf of VM
Standard_B4ms	4	16	32	90%	400%

3. About Microsoft Azure

3.1. What is Azure?

Azure is a comprehensive set of cloud services that developers and IT professionals use to build, deploy, and manage applications through our global network of datacenters. Integrated tools, DevOps, and a marketplace support you in efficiently building anything from simple mobile apps to internet-scale solutions.

Microsoft Azure is an integrated suite of tools, templates, and managed services to significantly improve the productivity of any developer or IT professional. With its massive set of features and functionalities, and build for the Microsoft platform, Azure makes it easier for IT professionals to build and manage enterprise, mobile, Web and Internet of Things (IoT) apps.

Microsoft has been investing heavily in the Microsoft Azure public cloud architecture and the efforts are paying off in the Infrastructure-as-a-Service (IaaS) field.

3.2. Why Azure

There are a lot of good reasons for enterprises to move to the cloud, such as greater business agility, keeping track with the speed of innovation, and cost savings. The current state of the various cloud surveys shows that cloud adoption is growing and has now hit its stride. The strong growth in the use of cloud means that the majority of organizations are now operating in a hybrid environment that consists of on-premises and cloud-based services.

The cloud is also changing how companies consume technology. Employees and business departments are more empowered than ever before to find and use cloud applications, often with limited or no involvement from the IT department, creating what's called "shadow IT." Despite the benefits of cloud computing, companies face numerous challenges including the integration of cloud services into the enterprise architecture, security and compliance of corporate data, managing employee-led cloud usage, establishing operational processes for cloud services, and even the development of necessary skills needed in the cloud era.

As companies move data to the cloud, IT departments are looking to put in place policies and processes so that employees and business departments can take advantage of cloud services that drive business growth without compromising the security, compliance, and governance of corporate data.

3.3. Managing Security and Data Privacy in Azure Cloud

Every business has different needs, and every business will reap distinct benefits from the cloud solutions. Still, customers of all kinds have the same basic concerns about moving to the cloud. They want to retain control of their data, and they want that data to be kept secure and private, all while maintaining transparency.

What customers want from the cloud providers is:

- Secure our data
  While acknowledging that the cloud can provide increased data security and administrative control, IT leaders are still concerned that migrating to the cloud will leave them more vulnerable to hackers than their current in-house solutions.
- Keep our data private

Cloud services raise unique privacy challenges for businesses. As companies look to the cloud to save on infrastructure costs and improve their flexibility, they also worry about losing control of where their data is stored, who is accessing it, and how it gets used.

- Give us control
  Even as they take advantage of the cloud to deploy more innovative solutions, companies are very concerned about losing control of their data. The recent disclosures of government agencies accessing customer data, through both legal and extra-legal means, make some CIOs wary of storing their data in the cloud.
- Promote transparency
  While security, privacy, and control are important to business decision-makers, they also want the ability to independently verify how their data is being stored, accessed, and secured.

MS Azure is working to keep the customer data safe. It provides:

- Infrastructure protection
- Network protection
- Data protection
- Identity and access
- Security design and operations

3.4. Managing Compliance and Data Privacy Regulations

Microsoft Azure offers the following certifications for all in-scope services:

- Content Delivery and Security Association (CDSA)
- Criminal Justice Information Services (CJIS)
- Cloud Security Alliance (CSA) Cloud Controls Matrix
- EU Model Clauses
- GDPR
- US Food and Drug Administration (FDA) Code of Federal Regulations (CFR) Title 21 P 11
- Federal Risk and Authorization Management Program (FedRAMP)
- Family Educational Rights and Privacy Act (FERPA)
- Federal Information Processing Standard (FIPS) Publication 140-2Azure Cloud Services
- Health Insurance Portability and Accountability Act (HIPAA)
- Information Security Registered Assessors Program (IRAP)
- ISO/IEC 27018
- ISO/IEC 27001/27002:2013
- Multi-Level Protection Scheme (MLPS)
- Multi-Tier Cloud Security Standard for Singapore (MTCS SS)
- Payment Card Industry (PCI) Data Security Standards (DSS)
- Service Organization Control (SOC) reporting framework for both SOC 1 Type 2 and SOC 2 Type 2.
- Trusted Cloud Service certification developed by the China Cloud Computing Promotion and Policy Forum (CCCPPF)
- UK Government G-Cloud