Zitec's Quick Guide to **Microsoft Azure Security** for organizations

ZITEC
MAKE IT SOFTWARE

Azure

TABLE OF CONTENTS

The 101 of cloud computing

If we were to look back at the words that have become part of our vocabulary in recent years, the term “cloud” would pop up quickly, without it being related to weather all that much. We interact with clouds every day, even if we are not always aware of it. Your personal photos are somewhere in a cloud, just like a lot of the data, files and apps on your work laptop.

So, what is a cloud? How did clouds become so present in our lives? And how are businesses using them? Let’s take a trip down tech memory lane.

The origins of the cloud

It is said the first time the term “cloud” was used in tech was back in 1996 in...an internal Compaq document that covered the topic of distributed computing.

But we will get back to the history lesson in a minute. To better understand the concept of the cloud, how it emerged and became the standard of operating for businesses as well as the preferred storage option for the general public, let’s do a mental exercise.

If you had a great idea for an app in the early 2000s and wanted to bring it to the (then emerging) market, the efforts would have been gargantuan by today’s standards. Apart from developing the actual app, you would have had to handle some serious logistic challenges.

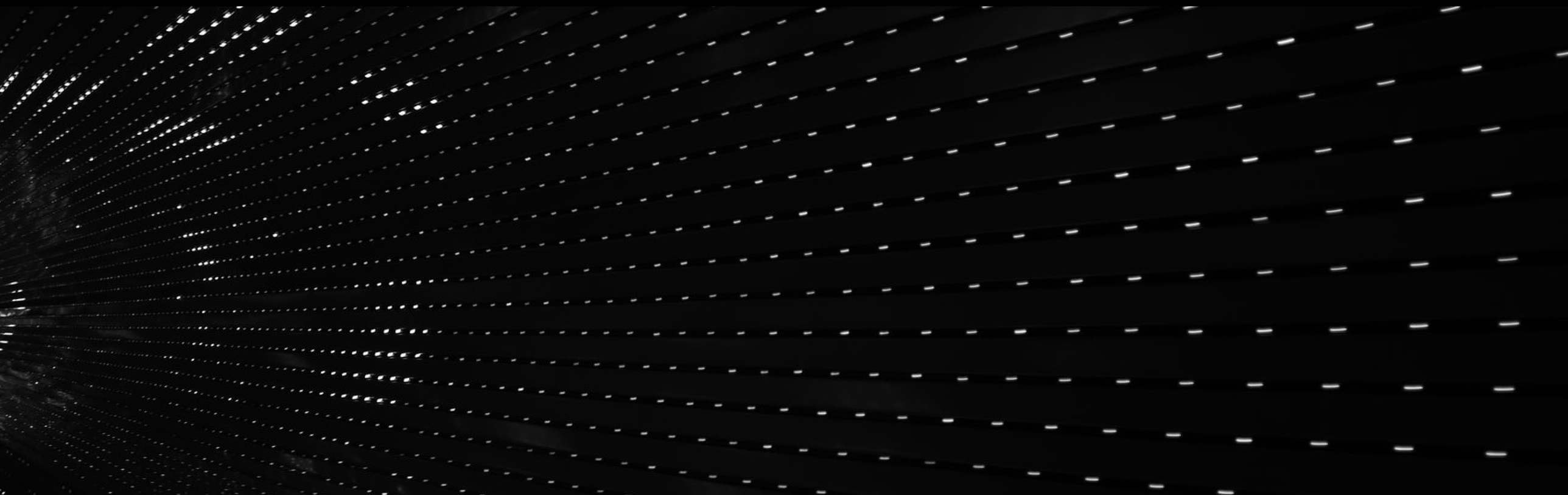
Back then you needed to buy, store and operate your own servers, using trained professionals. The bills would have clogged up your mailbox before you even got a chance to monetize.

This huge effort would have had to been replicated in any area where you were planning to launch your product.

It used to be a very restrictive environment where creating an app or providing a global service required massive financial resources.

Things began to change in the mid to late 2000s, when technology giants came to the realization that they could make their massive, unused resources available to the rest of the world, in exchange for a subscription plan. In no time, companies across the world started switching from conventional operating models, with massive costs in hardware and maintenance, to employing cloud computing services. For the first time, remote areas with emerging economies began experiencing prosperity. Small startups started making a dent in the universe and some of the biggest brands in today's tech were born.

Think of this as the point of no return.



Why use a cloud to run your business?

The more accurate question would probably be “why not”? If we maintain the frame of the previous example, where you have an app that is doing well locally, but could potentially be very successful overseas, a cloud-based approach seems logical. You no longer have to travel to, let’s say South America, and setup an expensive datacenter that also implies the high maintenance costs. The alternative of subscribing to a cloud computing service removes all these logistic issues from the equation, leaving your valuable resources available for refining your product and customer experience.

Cloud computing is great not only because it is the financially sane thing to do, but it also provides a wide range of benefits that become must-haves once your product or service reaches a certain position in the market.

Things like limited to no downtime, fast load speeds and instant global reach have become the standard, making cloud services the go-to option for both maverick SaaS startups and corporate enterprises.

Not only are cloud services optimized to allow a quick entry into the market for new businesses, but they are also the responsible environmental choice. Instead of creating a new, resource draining infrastructure from scratch, the possibility of renting an already existing infrastructure is far less demanding of the environment.

Cloud types

Cloud computing services are commonly divided in three categories:

Public clouds – a public cloud is a service offered by a 3rd party publicly over the Internet, to anyone willing to purchase and use it.

Private clouds – a private cloud is a service provided over the Internet for specific needs, often where sensitive data needs to be stored and shared. Most commonly it features a controlled security system to protect the sensitive data.

Hybrid Clouds – a hybrid cloud service mixes resources from both public and private clouds.

Cloud security

No solution is ever perfect and cloud computing is no exception. Cloud security is one of the biggest, yet reasonable concerns for all companies who employ this type of service. The myriad of potential vulnerabilities can be daunting, and this makes vigilance mandatory for anyone storing assets and operating with sensitive data via a cloud service. There are several major concerns companies have regarding cloud security.

1. Identity management

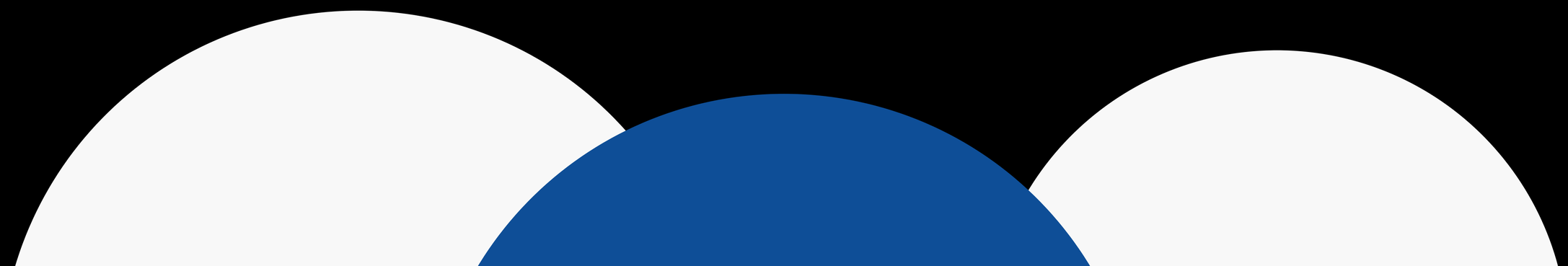
A cloud can be a crowded place. It is therefore imperative that all users who are granted access to the cloud have clearly defined roles. Mixing roles and responsibilities can produce damage and open the door for other threats. Although it is a key security concern, it is also one of the most avoidable threats. Basic requirements such as multi-factor authentication should be required to access any sensitive information. While the measures themselves are not necessarily difficult to implement, maintaining them can lead to fatigue within teams.

2. Data management and encryption

All sensitive data stored on a cloud should first be encrypted, and for this general purpose there are several security tools to discover and organize the data that needs to be encrypted. They can also be useful in managing data, based on labels, characteristics, etc.

3. Skilled experts scarcity

One of the more pressing, yet difficult issues to resolve is the shortage of skilled cloud security professionals. As it is one of the newest and fastest growing fields in the security market, finding the necessary human resources poses a challenge for many companies. There is the additional risk of error coming from newer security professionals, with identity mismanagement being one of their more common and likely mistakes.



4. Fast changing workloads

With regards to workloads, there are two sides to the coin. On the one hand, the evolution of workloads can give cloud users more possibilities. On the other, with ever changing services it can be difficult to always keep them at company security standards.

5. The evolution of cybercrime

Probably the most predictable challenge of using cloud services has to do with attacks. The more complex the workloads, the more sophisticated the attacks will be. Cybercrime is evolving at a very fast rate and keeping data safe is an ongoing challenge. Not surprisingly, public clouds are the most vulnerable.

MICROSOFT AZURE

According to Gartner's Magic Quadrant in 2020, Microsoft Azure is one of the top 3 most used cloud services globally. Microsoft first announced Azure in October 2008 and it followed with the formal release in February 2010. Azure is a highly versatile public cloud platform that supports a wide range of operating systems, frameworks, programming languages and databases. This is one of the reasons why it is being used by developers worldwide. Azure can simultaneously host millions of users and it is highly configurable, enabling a high degree of customization according to a company's specific needs.

It is used for developing apps with JavaScript, Python, PHP, .NET, Java, for building back-ends for Android, iOS and Windows. Azure is the go-to solution for Forbes 500 organizations, leading universities and institutions, as well as upcoming ventures.

With 58 worldwide regions, Azure is present in 140 countries and provides a solid foundation for storing and securing assets.

AZURE SECURITY

One of the most important things to consider about Microsoft Azure, and cloud security in general, is that it is a shared responsibility. Azure provides its customers with a wide range of capabilities for data protection allowing full control over access and management of user identities.

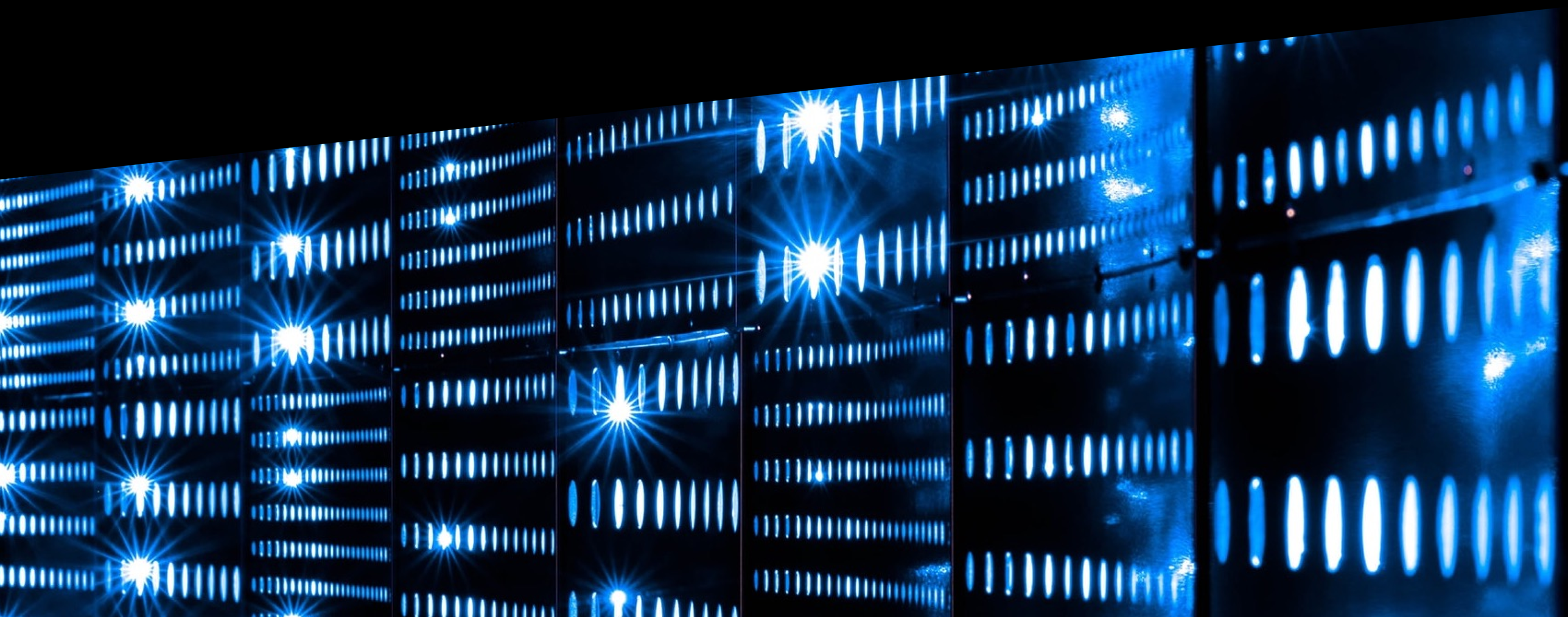
The data centers

Microsoft is highly invested in providing a maximum level of protection for customer data. The very first layer of this protection is the physical one. The company operates a division dedicated to building and maintaining a state-of-the- art security infrastructure for its datacenters. It is designed to make sure that only approved staff has access to the hardware, and it is guarded by highly trained security experts. For example, if you want to visit the datacenter that stores your data, you must provide a valid reason, like an audit. Without going into too much detail about the physical security, let's just say they are safe places.

Access Management

There are two ways in which you can control access in Microsoft Azure: **Azure AD Roles** and **Azure Roles.**

Azure roles control permissions to manage Azure resources, while **Azure AD** roles control permissions to manage Azure Active Directory resources.



Azure Active Directory (Azure AD)

The Azure Active Directory enables IT experts to manage access to data and resources migrated into Azure by using multi-factor authentication and a Conditional Access policy. When an application or sensitive data is stored in a cloud, it is essential to be as accurate as possible in designating roles and access on the cloud. As mentioned previously, mixing roles is one of the most common security vulnerabilities with a high potential of inducing damage to an organization.

Azure AD roles are used to manage Azure AD resources in a directory such as create or edit users, assign administrative roles to others, reset user passwords, manage user licenses, and manage domains. Here are some of the most important Azure AD roles.

Global administrator

- Manages access to all administrative features in Azure Active Directory, as well as services that federate to Azure Active Directory.
- Assigns administrator roles to others.
- Resets the password for any user and all other administrators.

Billing administrator

- Makes purchases.
- Manages subscriptions.
- Manages support tickets.
- Monitors service health.

User administrator

- Creates and manages all aspects of users and groups.
- Manages support tickets.
- Monitors service health.
- Changes passwords for users, Helpdesk administrators, and other User Administrators.

Azure role-based access control (Azure RBAC)

Role assignments enable you to control access to Azure resources. **Azure role-based access control (Azure RBAC)** has several Azure built-in roles that you can assign to users, groups, service principals, and managed identities. If the built-in roles don't meet the specific needs of your organization, you can create your own **Azure custom roles**. Here is an overview of built-in roles on a subscription level.

Owner - Grants full access to manage all resources, including the ability to assign roles in Azure RBAC.

Contributor - Grants full access to manage all resources but does not allow you to assign roles in Azure RBAC, manage assignments in Azure Blueprints, or share image galleries.

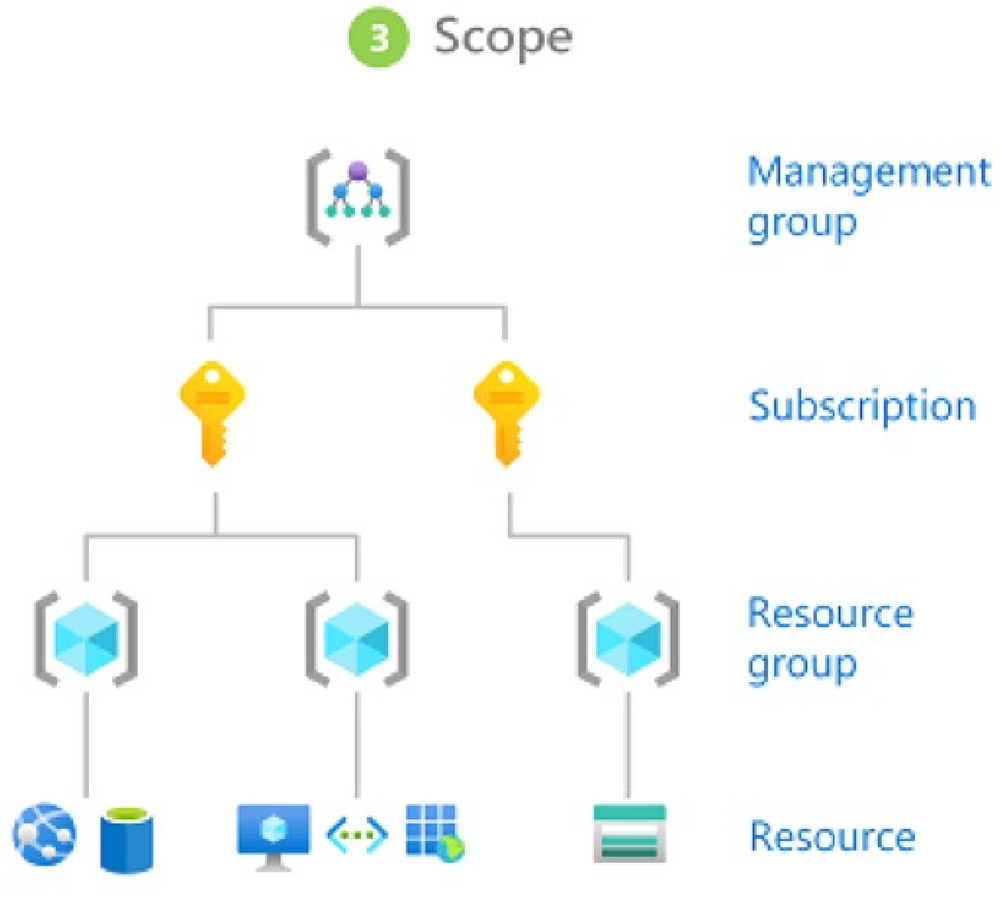
User Access Administrator - Allows managing user access to Azure resources.

Reader - Views all resources but does not allow making changes.

Depending on your organization's specific needs, Azure RBAC enables providing **built-in-roles** for users or groups: General, Compute, Networking, Storage, Web, Containers, Databases, etc. Azure RBAC works based on inheritance, if you provide Owner rights at the management group level, it will be inherited on all subscriptions and all resource groups.

Azure **RBAC** works based on **inheritance**, therefore, if you provide Owner rights at the management group level, it will be inherited on all subscriptions and all resource groups.

Follow the **least privilege** principle when you give access to members. **Assign** the least privileged role at the management group/subscription level and give specific privileged roles at the resource group level.



Managed identities for Azure resources

A common challenge for developers is the management of secrets and credentials used to secure communication between different components making up a solution. Managed identities eliminate the need for developers to manage credentials. It provides an identity for applications to use when connecting to resources that support Azure Active Directory (Azure AD) authentication. Applications may use the managed identity to obtain Azure AD tokens. For example, an application may use a managed identity to access resources like **Azure Key Vault** where developers can store credentials in a secure manner or to access storage accounts.

I can use Managed Identities when...

As a Developer, I want to build an application using

Source:

Azure Resources
Azure VMs
Azure App Services
Azure Functions
Azure Container instances
Azure Kubernetes Service
Azure Logic Apps
Azure Storage
....

that accesses

Target:

Any target that supports Azure Active Directory Authentication:
- **Your applications**
- **Azure Services:**
  - Azure Key Vault
  - Azure Storage
  - Azure SQL...

without having to manage any credentials!

For example, I want to build an application using ***Azure App Services*** that accesses **Azure Storage** without having to manage any credentials.

A final word

All this might seem like a lot to take in and it probably feels like there is a real reason why there is a global shortage of Azure security experts. **Zitec is a Microsoft Gold Cloud Platform Partner**. Our expertise covers all potential cloud needs, from data migration through to Azure security and more.

If you want to learn more about how Microsoft Azure can transform your business or how it can be the perfect solution to launch your next product, **send us a message** and our certified experts will get in touch shortly.