



# THE 10 MOST COMMON AZURE MISCONFIGURATIONS AND HOW TO FIX THEM

# OVERVIEW

Ensuring optimal configuration of the cloud environment is of paramount importance for organizations embarking on a cloud adoption journey. Microsoft Azure provides a consistent cloud experience for customers, backed by enterprise-class technologies, excellent security, and customizable configuration options to meet diverse customer requirements. Azure has several built-in features and services that can be leveraged by organizations to meet most of their security and compliance requirements. Following best practices with these services will help organizations ensure that their cloud environment is operating at optimal efficiency levels.

This whitepaper will discuss the 10 most common Azure misconfigurations that are overlooked by cloud engineers and how they can be addressed efficiently. The typical misconfigurations are broadly classified under three categories: security, cost, and operational best practices.

## SECURITY BEST PRACTICE CHECKS

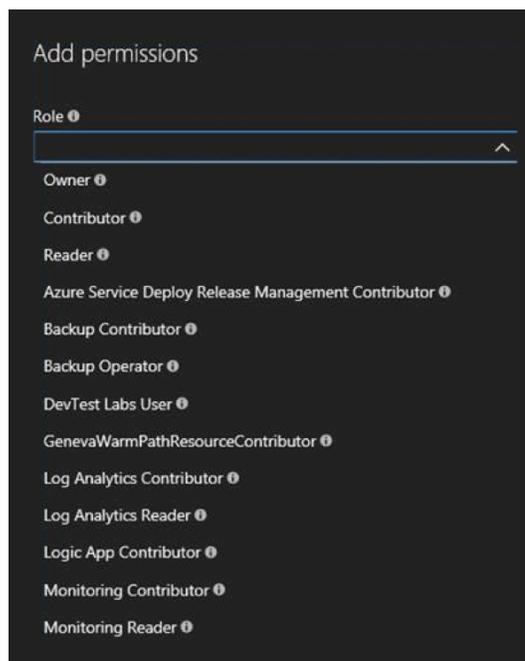
Security of infrastructure in Azure is dependent on many configurations. The most important ones are secure user access, data encryption, network level security, and activity log monitoring. Let's look at some of the common security misconfigurations in Azure and how to address them.

### 1. Failing to Enable RBAC and MFA for Users

The most common misconfiguration when it comes to user access control is providing permissions to users that are often broader than the scope of what's required to handle their jobs. Role Based Access Control (RBAC) was introduced in the Azure Resource Manager (ARM) model of Azure. RBAC facilitates Fine-Grained Access Control to resources hosted in Azure. The roles can be assigned to different security scopes such as subscription, resource group, or to individual resources like VM, VNet, Storage, etc. Roles are assigned to Azure AD users, groups, or applications. There are several roles available out of the box in Azure with predefined permission levels.

Alternatively, you can create custom roles with specific permission levels and assign roles. The three basic, built-in roles in Azure are owner, contributor, and reader. The owner and contributor roles have full access to all of the resources within the assigned scope. The only difference is that users who have the owner role can also provide access to other users. The reader role has its access restricted to viewing resources.

▶  
**There are multiple built-in roles for targeting specific resources in Azure.**



While assigning roles to users, follow the principle of least privilege and select a role that provides the user only with the amount of permission they need to do their job. Failing to follow the principle of least privilege is the most common pitfall leading to excess access permission. However, this problem can easily be avoided.

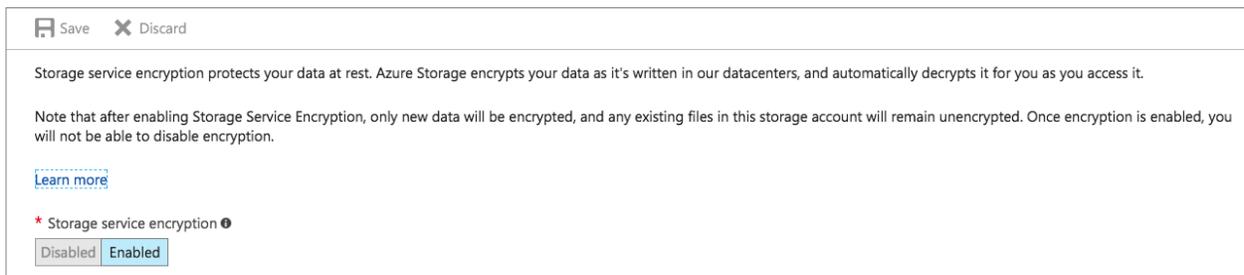
[Azure Multi-Factor Authentication](#) (MFA) enables two-factor authentication for Azure administrators who are authorized to access the Azure portal. One common misconfiguration found in Azure infrastructures is the failure of administrators to leverage MFA. MFA provides an extra layer of security where the administrators are asked for additional authentication via phone call, SMS, mobile app, or third-party OATH tokens before they can log into the portal. This ensures security in scenarios where the administrator account is compromised and is at risk of being misused.

## 2. Failing to Enable Encryption for Data at Rest

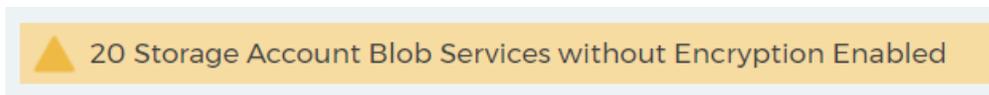
Enabling RBAC secures the data stored in Azure on the management plane by requiring that only the necessary privileges are assigned to users for data access. In addition, the security of the data at rest itself should be enhanced by using features such as storage-side encryption and Azure Disk Encryption. Organizations often overlook these settings, which can result in security misconfigurations.

Azure Storage Service Encryption can be used to encrypt all data using a Microsoft platform-managed key before saving it to Azure Storage. Now, encryption is enabled by default for all newly created storage accounts in Azure. We recommend that you retain this configuration as a default for newly created storage. You may also want to check older storage accounts and enable encryption wherever it isn't enabled. The keys used for encryption are managed by the Azure platform.

The status of Storage Service Encryption can be checked on the storage settings in the Azure portal. It's recommended that you enable this setting for all storage accounts in your Azure subscription.



You can also review the settings using third-party tools like CloudCheckr, which analyzes the Azure environment and gives a warning if there's a misconfiguration related to encryption.

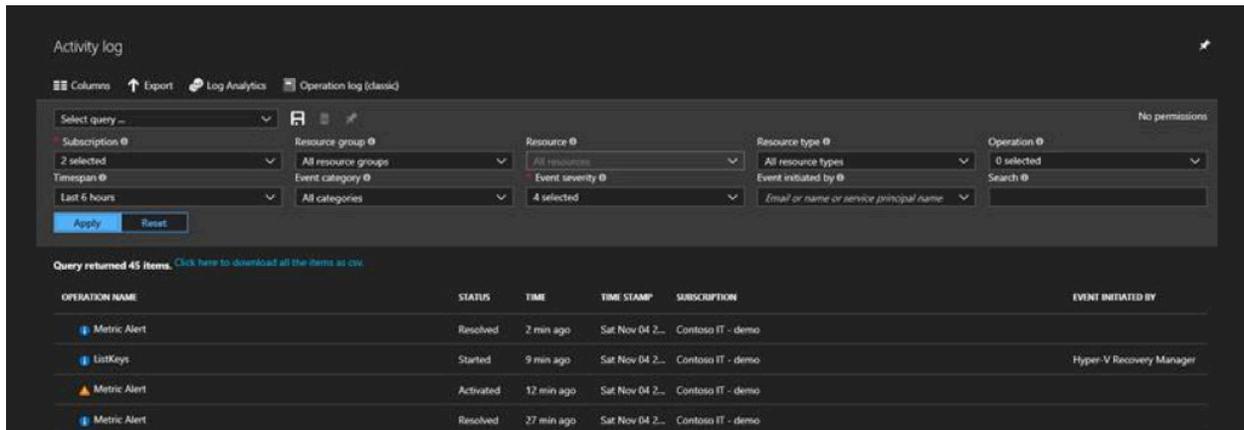


The disk encryption service uses industry standard technologies like Bitlocker and DMCAcrypt for encrypting the OS/data disks of Windows and Linux VMs hosted in Azure. One common misconfiguration found in Azure environments is having this feature disabled. Disk encryption leverages the Azure Key Vault service, which securely stores the keys used for encryption in an HSM module. It's recommended that you enable the disk encryption for VMs for secure storage of data at rest. The status of disk encryption can be monitored using tools like Azure Security Center or Azure Advisor. Third-party tools like CloudCheckr also provide a dashboard view of these settings where administrators can view warnings about VMs with unencrypted disks.

**18 Virtual Machines with Unencrypted Disks**

### 3. Failing to Monitor Activity Logs

Azure Activity Log provides insight into what's happening in your Azure subscription in terms of resource access and management. This service tracks all create, update, delete, and action activities performed on resources in the ARM model.



These activity logs can be integrated with multiple monitoring solutions like [Power BI](#) and [Operations Management Suite \(OMS\)](#) for advanced analysis and reporting. Cloudcheckr provides continuous monitoring capabilities of your Azure environment using best practices and raises alerts when best practice deviations are identified.

### 4. NSGs with Overly Permissive Rules

Network Security Groups (NSGs) provide the same functionality as a basic network firewall, with rules to filter the incoming and outgoing traffic from virtual networks and VMs. NSGs contain basic quintuple rules that can be configured to permit or deny traffic to or from a subnet, port, or an IP in an Azure network. You can assign NSGs at two levels: in the NIC card of VM and in subnets in VNet.

Organizations often configure NSGs with broader permissions, which can invite unwanted access into their Azure environment. We recommend that you use the least permissive settings for incoming and outgoing traffic while you're configuring NSGs. CloudCheckr can identify and report these security loopholes, which helps administrators take the necessary corrective actions.

**9 Network Security Groups Outbound Rules with Dangerous Ports Exposed**

## CHECKING COST MANAGEMENT BEST PRACTICES

One of the key attractions of cloud computing is conversion of capital expense (CapEx) to operational expense (OpEx), which bring organizations significant financial benefits. However, it's very important to keep an eye on specific configuration settings in Azure to ensure optimization of your OpEx.

### 5. Failing to Monitor Metrics for Tracking Resource Usage

It's often the case that resources in Azure are over-provisioned and wasted when the hosted application is only using a fraction of what's available. This leads to significant increases on the monthly bill. Because of over-provisioning, organizations end up paying for more than what was necessary to keep their applications up and running in Azure.

Azure has metrics associated with resources where administrators can set thresholds to generate alerts based on resource usage. Administrators should keep an eye on these metrics and alerts to identify and scale down unused resources. An easier method is to use the readily available reports in CloudCheckr (which are generated by monitoring the usage of resources in Azure) and take the necessary actions to remedy the problem.

Security (28 issues)	Cost (8 issues)	Availability (8 issues)	Usage (7 issues)	Azure Advisor (7 issues)	Azure Security Center (15 issues)
▲ App Service without AutoHeal Enabled					
▲ App Service without Backup Scheduling Enabled					
▲ 38 Storage Accounts without Secondary Location					

CloudCheckr also identifies idle resources that can be removed from the environment, which will help you save on OpEx.

Security (28 issues)	Cost (8 issues)	Availability (8 issues)	Usage (7 issues)	Azure Advisor (7 issues)	Azure Security Center (15 issues)
	16 Idle SQL Database Instances				
	4 Redis Cache Idle				
	6 Idle Virtual Machines				

For example, if unused VMs exist in your environment, you might incur storage charges, even in the deallocated state. The same is true of unattached managed disks, even though they aren't being used effectively by any VMs in your environment.

## 6. Failing to Migrate Resources to the ARM Model

Microsoft recommends using the Azure Resource Manager model for all new deployments in Azure. It's also possible to migrate the majority of resources from the classic model to ARM, thereby enabling customers to leverage the latest features in Azure, such as RBAC, tags, template deployment, etc.

All new Azure services will be available in the ARM model, so [migrating to the ARM model](#) can help you leverage these services as soon as they're available. There are many alternative, cost-effective options in ARM to replace existing cloud resources in the classic portal. You can explore these options and migrate the resources appropriately.

## 7. Failing to Use the Azure Hybrid Benefit

Compute charges in Azure normally include license charges for the OS and charges for bundled software like SQL, Biztalk, etc. Organizations often already have Windows operating system licenses for their on-premises environments. [Azure Hybrid Benefit](#) allows you to bring your own Windows Server OS licenses to Azure, thereby reducing monthly charges. Customers who have purchased these licenses with Software Assurance (SA) can make use of this benefit. This is one cost savings option that organizations often overlook, which results in significant overspending in monthly cloud charges. We recommend that you leverage the Azure Hybrid Benefit option when possible to decrease cloud expenses.

# OPERATIONAL BEST PRACTICE CHECKS

Along with security and cost optimization measures, it's imperative to implement certain operational best practices to reap better returns on Azure investments.

## 8. Failing to Track Inventory Utilization

It's very important to track the utilization status of resources in Azure and fine-tune them according to usage. For example, you can do inline scaling down of individual VMs to an instance of lower spec for the Azure portal.

The right sizing reports available in CloudCheckr make this process very easy by analyzing the usage pattern and recommending the right sizes for resources like VMs, App Service Plans, SQL Databases, and Redis caches.

SQL Databases	Hourly Costs	Projected Hourly Costs	Possible Hourly Savings	Estimated Monthly Savings
11	\$0.19	\$0.10	\$0.09	\$68.75

SQL Database	Resource Group	Hourly Cost	Projected Hourly Cost	Possible Hourly Savings	Estimated Monthly Savings	Current Plan	Recommended Plan	DTUs 30-Day Average	Storage 30-Day Average	Score
CC_Common	Api-Default-Central-US	\$0.02	\$0.01	\$0.01	\$9.82	S0 Standard	Basic	0.00%	0.00%	0
CC_Job	Api-Default-Central-US	\$0.02	\$0.01	\$0.01	\$9.82	S0 Standard	Basic	0.00%	0.00%	0
CC_Log	Api-Default-Central-US	\$0.02	\$0.01	\$0.01	\$9.82	S0 Standard	Basic	0.00%	0.00%	0
CC_Root	Api-Default-Central-US	\$0.02	\$0.01	\$0.01	\$9.82	S0 Standard	Basic	0.00%	0.00%	0
CC_Shard_0001	Api-Default-Central-US	\$0.02	\$0.01	\$0.01	\$9.82	S0 Standard	Basic	0.00%	0.00%	0
CC_ShardBilling_0001	Api-Default-Central-US	\$0.02	\$0.01	\$0.01	\$9.82	S0 Standard	Basic	0.00%	0.00%	0
CC_ShardCloudTrail_0001	Api-Default-Central-US	\$0.02	\$0.01	\$0.01	\$9.82	S0 Standard	Basic	0.00%	0.00%	0
CC_ShardLogFile_0001	Api-Default-Central-US	\$0.02	\$0.01	\$0.01	\$9.82	S0 Standard	Basic	0.00%	0.00%	0
CC_ShardStarling_0001	Api-Default-Central-US	\$0.02	\$0.01	\$0.01	\$9.82	S0 Standard	Basic	0.00%	0.00%	0
CcTest	Api-Default-Central-US	\$0.01	\$0.02	(\$0.01)	(\$9.82)	Basic	S0 Standard	0.00%	91.00%	5

We recommend that you leverage these reports and reconfigure the resources to the ideal size to ensure operational efficiency. Doing so will result in significant cost savings in the long-run.

## 9. Failing to Use Resource Tags

Azure resource tags can be used to logically organize resources in the Azure Resource Manager using name-value pairs. Along with logical grouping of resources, tags are also commonly used to segregate billing data. The tags that are added to the resources will be reflected in the Azure usage CSV file that you get from the Azure account center or EA portal. This will help you filter the resources and their costs using the tag. For example, you can tag resources that are being used for development with a key-value pair in order to identify the expenses incurred for development activities from the usage CSV by sorting with the tag.

Tags can also be used as input parameters for Azure Automation runbooks being used for automation of time-consuming administrative tasks. It's important to maintain a naming standard for tags and to review them regularly for compliance. CloudCheckr provides insightful reports based on tags that can help you get a high-level picture of tagged resources and their distribution across the Azure environment. It also allows you to create tagging rules to filter out tags that don't align with the organization's tagging strategy.

## 10. Unintentionally Exposing Resources to the Public

One common security misconfiguration found in public cloud environments is usage of inadequate security boundaries, which leaves hosted resources exposed. If an organization fails to clear security audits due to inadequate security boundaries, they risk loss of business and a damaged reputation.

We recommend that you follow the [Azure Network Security best practice guidelines](#) with regards to segregation of networks, usage of network security groups, specialized virtual network appliances, etc., to secure your Azure environment. Tools like Azure Security Center and OMS security solutions analyze the environment according to security best practices and flag compliance issues. Third-party tools like CloudCheckr can also check for any exposed public endpoints in your cloud environment and provide a comprehensive report on this information.

### Perimeter Assessment [Show Help](#)

Filter out any Location with no publicly accessible resources or VPCs

Location name	
	Central US
<a href="#">Collapse All Details</a>	
	Publicly Accessible IP Addresses (6 items)
	Virtual Networks (8 items)
	East US
<a href="#">Expand All Details</a>	
	Publicly Accessible IP Addresses (1 item)
	Virtual Networks (3 items)

## TAKE ACTION TODAY

In addition to the configurations mentioned above, there are guidelines associated with specific resources in Azure for security, operations, and optimal ROI. It's important for organizations to avoid common misconfigurations, and to be aligned with best practices as much as possible by leveraging native Azure tools or third-party tools like CloudCheckr. Below are some helpful reference links.

- › **Azure security guidelines:**  
<https://docs.microsoft.com/en-us/azure/security/security-best-practices-and-patterns>
- › **Azure resource tagging:**  
<https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-using-tags>
- › **Azure data security:**  
<https://docs.microsoft.com/en-us/azure/security/azure-security-data-encryption-best-practices>
- › **Azure Security Center:**  
<https://azure.microsoft.com/en-in/services/security-center/>

## ABOUT CLOUDCHECKR

CloudCheckr is a comprehensive cloud management platform that helps organizations manage and monitor diverse cloud environments from a single pane of glass view. CloudCheckr helps ensure security compliance, optimize resource usage, and reduce cloud expenses by providing value-added insights and reports.

CloudCheckr has proven itself as a valuable asset for organizations, helping them meet compliance standards like FedRAMP, DFARS, HIPAA, PCI, etc. The proactive analysis, monitoring, recommendations, and automation provided by CloudCheckr are of great assistance to customers in maintaining strong cloud security and operational quality.

---

Need CloudCheckr for your organization?  
Learn more at [www.cloudcheckr.com](http://www.cloudcheckr.com)