Security recommendations for Blob storage - Azure Storage

By normesta

Archived: 2026-04-05 21:55:05 UTC

This article contains security recommendations for Blob storage. Implementing these recommendations will help you fulfill your security obligations as described in our shared responsibility model. For more information on how Microsoft fulfills service provider responsibilities, see Shared responsibility in the cloud.

Some of the recommendations included in this article can be automatically monitored by Microsoft Defender for Cloud, which is the first line of defense in protecting your resources in Azure. For information on Microsoft Defender for Cloud, see What is Microsoft Defender for Cloud?

Microsoft Defender for Cloud periodically analyzes the security state of your Azure resources to identify potential security vulnerabilities. It then provides you with recommendations on how to address them. For more information on Microsoft Defender for Cloud recommendations, see Review your security recommendations.

Recommendation	Comments	Defender for Cloud
Use the Azure Resource Manager deployment model	Create new storage accounts using the Azure Resource Manager deployment model for important security enhancements, including superior Azure role-based access control (Azure RBAC) and auditing, Resource Manager-based deployment and governance, access to managed identities, access to Azure Key Vault for secrets, and Microsoft Entra authentication and authorization for access to Azure Storage data and resources. Migrate all existing storage accounts that use the classic deployment model to use Azure Resource Manager. For more information about Azure Resource Manager, see Azure Resource Manager overview.	-
Enable Microsoft Defender for all of your storage accounts	Microsoft Defender for Storage provides an additional layer of security intelligence that detects unusual and potentially harmful attempts to access or exploit storage accounts. Security alerts are triggered in Microsoft Defender for Cloud when anomalies in activity occur and are also sent via email to subscription administrators, with details of suspicious activity and recommendations on how to investigate and remediate threats. For more information, see Configure Microsoft Defender for Storage.	Yes
Turn on soft delete for blobs	Soft delete for blobs enables you to recover blob data after it has been deleted. For more information on soft delete for blobs, see	-

Recommendation	Comments	Defender for Cloud
	Soft delete for Azure Storage blobs.	
Turn on soft delete for containers	Soft delete for containers enables you to recover a container after it has been deleted. For more information on soft delete for containers, see Soft delete for containers.	-
Lock storage account to prevent accidental or malicious deletion or configuration changes	Apply an Azure Resource Manager lock to your storage account to protect the account from accidental or malicious deletion or configuration change. Locking a storage account does not prevent data within that account from being deleted. It only prevents the account itself from being deleted. For more information, see Apply an Azure Resource Manager lock to a storage account.	
Store business-critical data in immutable blobs	Configure legal holds and time-based retention policies to store blob data in a WORM (Write Once, Read Many) state. Blobs stored immutably can be read, but cannot be modified or deleted for the duration of the retention interval. For more information, see Store business-critical blob data with immutable storage.	-
Use Encryption to Protect Data	Azure Storage encrypts all data at rest by default using Microsoft-managed keys. For enhanced control, configure customer-managed keys with Azure Key Vault to manage encryption keys directly. To further strengthen security, implement client-side encryption before uploading data.	-
Require secure transfer (HTTPS) to the storage account	When you require secure transfer for a storage account, all requests to the storage account must be made over HTTPS. Any requests made over HTTP are rejected. Microsoft recommends that you always require secure transfer for all of your storage accounts. For more information, see Require secure transfer to ensure secure connections.	-
Limit shared access signature (SAS) tokens to HTTPS connections only	Requiring HTTPS when a client uses a SAS token to access blob data helps to minimize the risk of eavesdropping. For more information, see Grant limited access to Azure Storage resources using shared access signatures (SAS).	-
Disallow cross-tenant object replication	By default, an authorized user is permitted to configure an object replication policy where the source account is in one Microsoft Entra tenant and the destination account is in a different tenant. Disallow cross-tenant object replication to require that the source and destination accounts participating in an object replication	-

Recommendation	Comments	Defender for Cloud
	policy are in the same tenant. For more information, see Prevent object replication across Microsoft Entra tenants.	

Recommendation	Comments	Defender for Cloud
Use Microsoft Entra ID to authorize access to blob data	Microsoft Entra ID provides superior security and ease of use over Shared Key for authorizing requests to Blob storage. For more information, see Authorize access to data in Azure Storage.	-
Keep in mind the principle of least privilege when assigning permissions to a Microsoft Entra security principal via Azure RBAC	When assigning a role to a user, group, or application, grant that security principal only those permissions that are necessary for them to perform their tasks. Limiting access to resources helps prevent both unintentional and malicious misuse of your data.	-
Use a user delegation SAS to grant limited access to blob data to clients	A user delegation SAS is secured with Microsoft Entra credentials and also by the permissions specified for the SAS. A user delegation SAS is analogous to a service SAS in terms of its scope and function, but offers security benefits over the service SAS. For more information, see Grant limited access to Azure Storage resources using shared access signatures (SAS).	-
Secure your account access keys with Azure Key Vault	Microsoft recommends using Microsoft Entra ID to authorize requests to Azure Storage. However, if you must use Shared Key authorization, then secure your account keys with Azure Key Vault. You can retrieve the keys from the key vault at runtime, instead of saving them with your application. For more information about Azure Key Vault, see Azure Key Vault overview.	-
Regenerate your account keys periodically	Rotating the account keys periodically reduces the risk of exposing your data to malicious actors.	-
Disallow Shared Key authorization	When you disallow Shared Key authorization for a storage account, Azure Storage rejects all subsequent requests to that account that are authorized with the account access keys. Only secured requests that are authorized with Microsoft Entra ID will succeed. For more information, see Prevent Shared Key authorization for an Azure Storage account.	-

Recommendation	Comments	Defender for Cloud
Keep in mind the principle of least privilege when assigning permissions to a SAS	When creating a SAS, specify only those permissions that are required by the client to perform its function. Limiting access to resources helps prevent both unintentional and malicious misuse of your data.	-
Have a revocation plan in place for any SAS that you issue to clients	If a SAS is compromised, you will want to revoke that SAS as soon as possible. To revoke a user delegation SAS, revoke the user delegation key to quickly invalidate all signatures associated with that key. To revoke a service SAS that is associated with a stored access policy, you can delete the stored access policy, rename the policy, or change its expiry time to a time that is in the past. For more information, see Grant limited access to Azure Storage resources using shared access signatures (SAS).	-
If a service SAS is not associated with a stored access policy, then set the expiry time to one hour or less	A service SAS that is not associated with a stored access policy cannot be revoked. For this reason, limiting the expiry time so that the SAS is valid for one hour or less is recommended.	-
Disable anonymous read access to containers and blobs	anonymous read access to a container and its blobs grants read-only access to those resources to any client. Avoid enabling anonymous read access unless your scenario requires it. To learn how to disable anonymous access for a storage account, see Overview: Remediating anonymous read access for blob data.	-

Recommendation	Comments	Defender for Cloud
Configure the minimum required version of Transport Layer Security (TLS) for a storage account.	Require that clients use a more secure version of TLS to make requests against an Azure Storage account by configuring the minimum version of TLS for that account. For more information, see Configure minimum required version of Transport Layer Security (TLS) for a storage account	-
Enable the **Secure transfer required** option on all of your storage accounts	When you enable the **Secure transfer required** option, all requests made against the storage account must take place over secure connections. Any requests made over HTTP will fail. For more information, see Require secure transfer in Azure Storage.	Yes

Recommendation	Comments	Defender for Cloud
Enable firewall rules	Configure firewall rules to limit access to your storage account to requests that originate from specified IP addresses or ranges, or from a list of subnets in an Azure Virtual Network (VNet). For more information about configuring firewall rules, see Configure Azure Storage firewalls and virtual networks.	-
Allow trusted Microsoft services to access the storage account	Turning on firewall rules for your storage account blocks incoming requests for data by default, unless the requests originate from a service operating within an Azure Virtual Network (VNet) or from allowed public IP addresses. Requests that are blocked include those from other Azure services, from the Azure portal, from logging and metrics services, and so on. You can permit requests from other Azure services by adding an exception to allow trusted Microsoft services to access the storage account. For more information about adding an exception for trusted Microsoft services, see Configure Azure Storage firewalls and virtual networks.	-
Use private endpoints	A private endpoint assigns a private IP address from your Azure Virtual Network (VNet) to the storage account. It secures all traffic between your VNet and the storage account over a private link. For more information about private endpoints, see Connect privately to a storage account using Azure Private Endpoint.	-
Use VNet service tags	A service tag represents a group of IP address prefixes from a given Azure service. Microsoft manages the address prefixes encompassed by the service tag and automatically updates the service tag as addresses change. For more information about service tags supported by Azure Storage, see Azure service tags overview. For a tutorial that shows how to use service tags to create outbound network rules, see Restrict access to PaaS resources.	-
Limit network access to specific networks	Limiting network access to networks hosting clients requiring access reduces the exposure of your resources to network attacks.	Yes
Configure network routing preference	You can configure network routing preference for your Azure storage account to specify how network traffic is routed to your account from clients over the Internet using the Microsoft global network or Internet routing. For more information, see Configure network routing preference for Azure Storage.	-

Recommendation	Comments	Defender for Cloud
Track how requests are authorized	Enable logging for Azure Storage to track how requests to the service are authorized. The logs indicate whether a request was made anonymously, by using an OAuth 2.0 token, by using Shared Key, or by using a shared access signature (SAS). For more information, see Monitoring Azure Blob Storage with Azure Monitor or Azure Storage analytics logging with Classic Monitoring.	-
Set up alerts in Azure Monitor	Configure log alerts to evaluate resources logs at a set frequency and fire an alert based on the results. For more information, see Log alerts in Azure Monitor.	-

- Azure security documentation
- Secure development documentation.

Source: https://docs.microsoft.com/en-us/azure/storage/common/storage-security-guide