# Scan

| Scan items | failed | success | manual |
| --- | --- | --- | --- |
| 15 | 5 | 9 | 1 |

# Results

## microsoft.storage

| name | failed | success | manual |
| --- | --- | --- | --- |
| [EAST\_Storage\_BlobDiagnostics](#east_storage_blobdiagnostics) | ❌[1](#healthy_false) |  |  |
| [EAST\_Storage\_EnableFirewall](#east_storage_enablefirewall) | ❌[1](#healthy_false) |  |  |
| [EAST\_Storage\_httpsOnly](#east_storage_httpsonly) |  | ✅[1](#healthy_true) |  |
| [EAST\_Storage\_PublicAccess](#east_storage_publicaccess) |  | ✅[2](#healthy_true) |  |

## microsoft.web

| name | failed | success | manual |
| --- | --- | --- | --- |
| [ASB\_diagnostic\_logs\_in\_app\_service\_should\_be\_enabled](#Xdea14a603472191e0b1eafd24512bc1d28162b4) | ❌[1](#healthy_false) |  |  |
| [ASB\_managed\_identity\_should\_be\_used\_in\_web\_apps](#X0084e83d8bd72f6ea8827c29ccd078cbeab4a6b) |  | ✅[1](#healthy_true) |  |
| [ASB\_remote\_debugging\_should\_be\_turned\_off\_for\_web\_applications](#X8c853c75cc2d0a0a69115ead1067dd63a77a3c0) |  | ✅[1](#healthy_true) |  |
| [ASB\_tls\_should\_be\_updated\_to\_the\_latest\_version\_for\_web\_apps](#X3db529c262cab869d438123a93ff9275a46d7bb) |  | ✅[1](#healthy_true) |  |
| [ASB\_web\_application\_should\_only\_be\_accessible\_over\_https](#Xf6a5e1c92bc79ae1b3e322940e4d474ab694232) | ❌[1](#healthy_false) |  |  |
| [AZSK\_Azure\_AppService\_AuthN\_Use\_AAD\_for\_Client\_AuthN](#Xff73f250a3774b0b92db9aa121fbef51339a93d) |  |  | 📑[1](#healthy_manual) |
| [AZSK\_Azure\_AppService\_Config\_Disable\_Remote\_Debugging](#X72c88e4db5f951c126af85ec38e59b6409388d1) |  | ✅[1](#healthy_true) |  |
| [AZSK\_Azure\_AppService\_Config\_Disable\_Web\_Sockets](#X72423ee853857aecbb399f1c0ebdbd1ab9c5510) |  | ✅[1](#healthy_true) |  |
| [AZSK\_Azure\_AppService\_Deploy\_Use\_Latest\_Version](#X21b5af091406fec247678935dd9270ecc93004a) |  | ✅[1](#healthy_true) |  |
| [AZSK\_Azure\_AppService\_DP\_Use\_CNAME\_With\_SSL](#X02821083bf5c4084f808a604ebbe70ac37d46ac) | ❌[1](#healthy_false) |  |  |

# Explanations and metadata

## microsoft.storage

### east\_storage\_blobdiagnostics

**Descriptions**

Ensure important blobs are logged for access

**Metadata**

#### healthy\_false

* [storageacc12345](https://portal.azure.com/#@/resource/subscriptions/00000000-0000-0000-0000-000000000000/resourcegroups/rg-development/providers/microsoft.storage/storageaccounts/storageacc12345) - [metadata](#Xeba4c6eb8df939410cd0261cd34ee89eed1e746)

**metadata\_storageacc12345\_east\_storage\_blobdiagnostics**

{  
 "BlobDiagnostics": ["No diagnostic settings enabled"]  
}

[back to top](#Scan)

[back to control EAST\_Storage\_BlobDiagnostics](#east_storage_blobdiagnostics)

### east\_storage\_enablefirewall

**Descriptions**

Review storage for network bypasses, and non IP limited access

**Metadata**

#### healthy\_false

* [storageacc12345](https://portal.azure.com/#@/resource/subscriptions/00000000-0000-0000-0000-000000000000/resourcegroups/rg-development/providers/microsoft.storage/storageaccounts/storageacc12345) - [metadata](#X781cb591622fee88857fb52c2140f2dc4140306)

**metadata\_storageacc12345\_east\_storage\_enablefirewall**

{  
 "bypass": "AzureServices",  
 "virtualNetworkRules": [],  
 "ipRules": [],  
 "defaultAction": "Allow"  
}

[back to top](#Scan)

[back to control EAST\_Storage\_EnableFirewall](#east_storage_enablefirewall)

### east\_storage\_httpsonly

**Descriptions**

Ensure storage access requires HTTPS

**Metadata**

#### healthy\_true

* [storageacc54321](https://portal.azure.com/#@/resource/subscriptions/00000000-0000-0000-0000-000000000000/resourcegroups/rg-development/providers/microsoft.storage/storageaccounts/storageacc54321) - [metadata](#X0c98199ff585563670fdaed6aa57f35ee6c4c97)

**metadata\_storageacc54321\_east\_storage\_httpsonly**

{  
 "supportsHttpsTrafficOnly": true  
}

[back to top](#Scan)

[back to control EAST\_Storage\_httpsOnly](#east_storage_httpsonly)

### east\_storage\_publicaccess

**Descriptions**

Review storage for public access

**Metadata**

#### healthy\_true

* [storageacc54321](https://portal.azure.com/#@/resource/subscriptions/00000000-0000-0000-0000-000000000000/resourcegroups/rg-development/providers/microsoft.storage/storageaccounts/storageacc54321) - [metadata](#Xf14ef3f4e5798caeec6e638e901de217e10efa3)
* [storageacc12345](https://portal.azure.com/#@/resource/subscriptions/00000000-0000-0000-0000-000000000000/resourcegroups/rg-development/providers/microsoft.storage/storageaccounts/storageacc12345) - [metadata](#Xdefae283473b4256e606150aa132d09506b8729)

**metadata\_storageacc54321\_east\_storage\_publicaccess**

{  
 "count": 1,  
 "Public": []  
}

[back to top](#Scan)

[back to control EAST\_Storage\_PublicAccess](#east_storage_publicaccess)

**metadata\_storageacc12345\_east\_storage\_publicaccess**

{  
 "count": 2,  
 "Public": []  
}

[back to top](#Scan)

[back to control EAST\_Storage\_PublicAccess](#east_storage_publicaccess)

## microsoft.web

### asb\_diagnostic\_logs\_in\_app\_service\_should\_be\_enabled

**Descriptions**

Audit enabling of diagnostic logs on the app.This enables you to recreate activity trails for investigation purposes if a security incident occurs or your network is compromised

**Remediation**

To enable resource logs for an App Service: 1. Navigate to your App Service. 2. Go to ‘Diagnostic Settings’ tab. 3. Enable necessary auditing services for your specified apps. For more information, please go to https://aka.ms/enabling-diagnostic-settings.

**Metadata**

#### healthy\_false

* [app-dev](https://portal.azure.com/#@/resource/subscriptions/00000000-0000-0000-0000-000000000000/resourcegroups/rg-development-web/providers/microsoft.web/sites/app-dev) - [metadata](#Xd4f6afb8f96013757bcd394944a36afd633521d)

**metadata\_app-dev\_asb\_diagnostic\_logs\_in\_app\_service\_should\_be\_enabled**

[back to top](#Scan)

[back to control ASB\_diagnostic\_logs\_in\_app\_service\_should\_be\_enabled](#Xdea14a603472191e0b1eafd24512bc1d28162b4)

### asb\_managed\_identity\_should\_be\_used\_in\_web\_apps

**Descriptions**

For enhanced authentication security, use a managed identity.On Azure, managed identities eliminate the need for developers to have to manage credentials by providing an identity for the Azure resource in Azure AD and using it to obtain Azure Active Directory (Azure AD) tokens.

**Remediation**

To create a managed identity for your web app:1. Go to the App Service for your API app 2. Scroll to the Settings group in the left navigation 3. Select Identity 4. Use System assigned or User assigned identity following the steps described in this doc: https://aka.ms/managed-identity

**Metadata**

#### healthy\_true

* [app-dev](https://portal.azure.com/#@/resource/subscriptions/00000000-0000-0000-0000-000000000000/resourcegroups/rg-development-web/providers/microsoft.web/sites/app-dev) - [metadata](#X0f9bac59e358a6ef42e3c64fc2d4f7154e2a67d)

**metadata\_app-dev\_asb\_managed\_identity\_should\_be\_used\_in\_web\_apps**

[back to top](#Scan)

[back to control ASB\_managed\_identity\_should\_be\_used\_in\_web\_apps](#X0084e83d8bd72f6ea8827c29ccd078cbeab4a6b)

### asb\_remote\_debugging\_should\_be\_turned\_off\_for\_web\_applications

**Descriptions**

Remote debugging requires inbound ports to be opened on a web application. Remote debugging is currently enabled. If you no longer need to use remote debugging, it should be turned off.

**Remediation**

To turn off remote debugging, we recommend the following steps:1. Go to the app service applications settings page2. In the remote debugging toggle select Off3. Click Save

**Metadata**

#### healthy\_true

* [app-dev](https://portal.azure.com/#@/resource/subscriptions/00000000-0000-0000-0000-000000000000/resourcegroups/rg-development-web/providers/microsoft.web/sites/app-dev) - [metadata](#Xa952379845952bfa69849051456aa1716b3ea4e)

**metadata\_app-dev\_asb\_remote\_debugging\_should\_be\_turned\_off\_for\_web\_applications**

[back to top](#Scan)

[back to control ASB\_remote\_debugging\_should\_be\_turned\_off\_for\_web\_applications](#X8c853c75cc2d0a0a69115ead1067dd63a77a3c0)

### asb\_tls\_should\_be\_updated\_to\_the\_latest\_version\_for\_web\_apps

**Descriptions**

Upgrade to the latest TLS version

**Remediation**

To update your web app to the latest TLS version:1. Navigate to Azure App Service 2. Select TLS/SSL settings 3. Under the Protocol Settings section, choose the latest Minimum TLS Version.For more information on managing TLS/SSL settings, visit here: https://aka.ms/add-tls

**Metadata**

#### healthy\_true

* [app-dev](https://portal.azure.com/#@/resource/subscriptions/00000000-0000-0000-0000-000000000000/resourcegroups/rg-development-web/providers/microsoft.web/sites/app-dev) - [metadata](#X328876700e93f26bf55d5abff4552f8b5228287)

**metadata\_app-dev\_asb\_tls\_should\_be\_updated\_to\_the\_latest\_version\_for\_web\_apps**

[back to top](#Scan)

[back to control ASB\_tls\_should\_be\_updated\_to\_the\_latest\_version\_for\_web\_apps](#X3db529c262cab869d438123a93ff9275a46d7bb)

### asb\_web\_application\_should\_only\_be\_accessible\_over\_https

**Descriptions**

Use of HTTPS ensures server/service authentication and protects data in transit from network layer eavesdropping attacks.

**Remediation**

To redirect all HTTP traffic to HTTPS, we recommend the following steps:1. Go to the app service custom domains page2. In the HTTPS Only toggle select On

**Metadata**

#### healthy\_false

* [app-dev](https://portal.azure.com/#@/resource/subscriptions/00000000-0000-0000-0000-000000000000/resourcegroups/rg-development-web/providers/microsoft.web/sites/app-dev) - [metadata](#X4463fd9c1f9205f5862de0e1d05a0151c577039)

**metadata\_app-dev\_asb\_web\_application\_should\_only\_be\_accessible\_over\_https**

[back to top](#Scan)

[back to control ASB\_web\_application\_should\_only\_be\_accessible\_over\_https](#Xf6a5e1c92bc79ae1b3e322940e4d474ab694232)

### azsk\_azure\_appservice\_authn\_use\_aad\_for\_client\_authn

**Descriptions**

Using the native enterprise directory for authentication ensures that there is a built-in high level of assurance in the user identity established for subsequent access control.All Enterprise subscriptions are automatically associated with their enterprise directory (xxx.onmicrosoft.com) and users in the native directory are trusted for authentication to enterprise subscriptions.

**Remediation**

(The status for this control has been marked as ‘Manual’ because elevated (Co-Admin/Owner/Contributor, as applicable) permission is required to check security configuration for this resource. You can re-run the control with the appropriate privilege.) Go to Azure Portal –> your App Service –> Settings –> Authentication/Authorization –> turn on ‘App Service Authentication’ –> Click on ‘Azure Active Directory’ under Authentication Providers to configure the AAD authentication. There will be a list of options to choose from under ‘Action to take when request is not authenticated’. Please make sure that this value is not set to ‘Allow Anonymous requests (no action)’. Note: If you are implementing this control via code, then you can attest to the same and mark this as passed. Note: In case of Functions apps, AAD authentication is required only for ‘Http Trigger’ functions.

**Metadata**

#### healthy\_manual

* [func-dev](https://portal.azure.com/#@/resource/subscriptions/00000000-0000-0000-0000-000000000000/resourcegroups/rg-development/providers/microsoft.web/sites/func-dev) - [metadata](#Xbb892ec9e02c969224f88eeda0ce0fe8cc382d1)

**metadata\_func-dev\_azsk\_azure\_appservice\_authn\_use\_aad\_for\_client\_authn**

[back to top](#Scan)

[back to control AZSK\_Azure\_AppService\_AuthN\_Use\_AAD\_for\_Client\_AuthN](#Xff73f250a3774b0b92db9aa121fbef51339a93d)

### azsk\_azure\_appservice\_config\_disable\_remote\_debugging

**Descriptions**

Remote debugging requires inbound ports to be opened on App Service. These ports become easy targets for compromise from various internet based attacks.

**Remediation**

Go to Azure Portal –> your App Service –> Settings –> Configuration –> General Settings –> Remote Debugging –> Click on ‘OFF’.

**Metadata**

#### healthy\_true

* [func-dev](https://portal.azure.com/#@/resource/subscriptions/00000000-0000-0000-0000-000000000000/resourcegroups/rg-development/providers/microsoft.web/sites/func-dev) - [metadata](#X2297df8d4ca3db595bb1a6a98fe77fff24a2998)

**metadata\_func-dev\_azsk\_azure\_appservice\_config\_disable\_remote\_debugging**

[back to top](#Scan)

[back to control AZSK\_Azure\_AppService\_Config\_Disable\_Remote\_Debugging](#X72c88e4db5f951c126af85ec38e59b6409388d1)

### azsk\_azure\_appservice\_config\_disable\_web\_sockets

**Descriptions**

WebSockets protocol (WS) is vulnerable to different types of security attacks. Usage of Web Sockets with in web applications has to be carefully reviewed.

**Remediation**

Run command ‘Set-AzWebApp -Name’’ -ResourceGroupName ‘’ -WebSocketsEnabled $false’. Run ‘Get-Help Set-AzWebApp -full’ for more help. Refer: https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/HTML5\_Security\_Cheat\_Sheet.md#websockets

**Metadata**

#### healthy\_true

* [func-dev](https://portal.azure.com/#@/resource/subscriptions/00000000-0000-0000-0000-000000000000/resourcegroups/rg-development/providers/microsoft.web/sites/func-dev) - [metadata](#Xfeef4c087f7549c3a584fc74e5666cd97d37583)

**metadata\_func-dev\_azsk\_azure\_appservice\_config\_disable\_web\_sockets**

[back to top](#Scan)

[back to control AZSK\_Azure\_AppService\_Config\_Disable\_Web\_Sockets](#X72423ee853857aecbb399f1c0ebdbd1ab9c5510)

### azsk\_azure\_appservice\_deploy\_use\_latest\_version

**Descriptions**

Running on older .Net versions could mean you are not using latest security classes. Usage of such old classes and types can make your application vulnerable.

**Remediation**

Run command ‘Set-AzWebApp -Name’’ -ResourceGroupName ‘’ -NetFrameworkVersion ‘v4.7’‘. Run ’Get-Help Set-AzWebApp -full’ for more help.

**Metadata**

#### healthy\_true

* [func-dev](https://portal.azure.com/#@/resource/subscriptions/00000000-0000-0000-0000-000000000000/resourcegroups/rg-development/providers/microsoft.web/sites/func-dev) - [metadata](#Xaa355a868afbcaa1ab19415dd7c063982a2540e)

**metadata\_func-dev\_azsk\_azure\_appservice\_deploy\_use\_latest\_version**

[back to top](#Scan)

[back to control AZSK\_Azure\_AppService\_Deploy\_Use\_Latest\_Version](#X21b5af091406fec247678935dd9270ecc93004a)

### azsk\_azure\_appservice\_dp\_use\_cname\_with\_ssl

**Descriptions**

Use of custom domain protects a web application from common attacks such as phishing, session hijacking and other DNS-related attacks.

**Remediation**

Go to Azure Portal –> your App Service –> Settings –> Custom Domains and follow the steps mentioned to configure a custom domain. Run command ‘New-AzWebAppSSLBinding’ to enable the SSL binding for your custom domain. Run ‘Get-Help New-AzWebAppSSLBinding -full’ for more help.

**Metadata**

#### healthy\_false

* [func-dev](https://portal.azure.com/#@/resource/subscriptions/00000000-0000-0000-0000-000000000000/resourcegroups/rg-development/providers/microsoft.web/sites/func-dev) - [metadata](#X062b956d7dce10de69bcbd31647fb1813cc1d13)

**metadata\_func-dev\_azsk\_azure\_appservice\_dp\_use\_cname\_with\_ssl**

[back to top](#Scan)

[back to control AZSK\_Azure\_AppService\_DP\_Use\_CNAME\_With\_SSL](#X02821083bf5c4084f808a604ebbe70ac37d46ac)