

Cannot open or view Vulnerability Assessment Reports

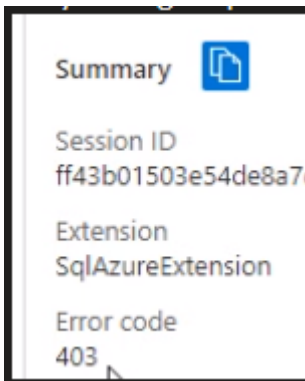
Last updated by | Soma Jagadeesh | Sep 3, 2020 at 1:25 PM PDT

Contents

- [Issue](#)
- [Investigation/Analysis](#)
- [Mitigation](#)
- [More Information](#)
- [Public Doc Reference](#)
- [Root Cause Classification](#)

Issue

Cannot open the vulnerability assessment report by clicking on the email hyperlink or viewing it directly on the portal. Portal displays HTTP errors 401 or 403.



Investigation/Analysis

1. Role membership of the user accessing the assessment
2. Review permissions on storage account and on the SQL provider

Mitigation

Owner role gives the user full access to all resources in a subscription. If customer wants to limit the permissions granted to specific users or groups the below may help implement the principle of least privilege.

Vulnerability assessments are stored on blob containers if permissions are not granted the account will not be authorized to access the files.

A quick and easy mitigation from the storage side is to add role membership to built-in roles **"Storage Blob Data Reader"** and **"Reader and Data Access"**.

Note: "Reader and Data Access" is not visible through the Portal but you can add it with Azure CLI or Azure PowerShell. Be mindful of the scope required. In Azure, you can specify a scope at multiple levels: management group, subscription, resource group, or resource.

Azure CLI

```
az role assignment create --assignee-object-id <User/Group> --role 'Reader and Data access' --scope '/subscrip
```

Azure PowerShell

```
New-AzRoleAssignment -ObjectId <User/Group> -RoleDefinitionName 'Reader and Data Access' -Scope '/subscription
```

To be able to view the Vulnerability Assessment you will also need permission on the Microsoft.Sql provider. You can use the built-in role **"Monitoring Reader"**

Additional Information:

Two models to work with storage account permissions

Method 1 (works everywhere): using listkeys permissions on storage

Management Actions	Permissions
Read: List/Get Storage Account(s) ⓘ	✓
Write: Create/Update Storage Account ⓘ	✓
Delete: Delete Storage Account ⓘ	✓
Other actions	
Approve Private Endpoint C	
List Storage Account Keys ⓘ	✓
Regenerate Storage Account Keys ⓘ	✓
Restore blob ranges ⓘ	✓
Returns Storage Account SAS Token ⓘ	✓
Returns Storage Service SAS Token ⓘ	✓
Revoke Storage Account User Delegation Keys ⓘ	✓

Tooltip for List Storage Account Keys: Returns the access keys for the specified storage account. Action:Microsoft.Storage/storageAccounts/listkeys/action

Which will allow the UI to Generate SAS keys to load the results from the storage.

Method 2 (works only in public cloud):

Using data plan permissions on storage (not control plane permissions, and I have no idea if this is supported using custom RBAC and it's probably not - notice that it's a data action and not a normal action - but it can be achieved by using storage data reader build in role)


Home > storageincwus > Storage Blob Data Reader > Permissions (preview) > Microsoft Storage >

Storage Blob Service Blobs

Permitted actions - Storage Blob Data Reader (built-in role)

Data Actions

Returns a blob or a list of blobs.
Action:Microsoft.Storage/storageAccounts/blobServices/containers/blobs/read

Read: Read Blob ⓘ 

Write: Write Blob ⓘ

Delete: Delete blob ⓘ

Other actions

Add blob content ⓘ
and other basic permissions that storage blob data reader needs are required as well.

More Information

If more granular permissions are needed customer can create a custom role and grant permissions on the necessary actions.

For more details, see the [Custom Role with Azure CLI](#) ⓘ or [Custom Role with Azure PowerShell](#) ⓘ reference.

Public Doc Reference

- [Built-in roles](#) ⓘ
- [Storage resource provider operations](#) ⓘ
- [SQL resource provider operations](#) ⓘ

Root Cause Classification

Azure SQL DB v2\Security\User Issue/Error\Vulnerability Assessment

How good have you found this content?

