**Authentication POC2**

**Steps followed to do Basic Authentication verification**

* Setup IIS server on window server with Basic Auth enabled and Disabled Anonymous access
* Deployed Sample api (/api1/\*) on port 90 and api (/api2/\*) on port 100 on IIS server
* Installed AAD extensions on Window server
* Setup webapp (serviceaccount as a user) in AzureAD and gave RBAC - VM access to IIS Server created above
* Installed postman on window server
* Tested Scenario 1 – Access APIs outside the server - three test cases through postman – no auth, wrong credentials in basic auth header and valid credentials (setup earlier) in basic auth header for api1/\*
* Tested Scenario 2 – Access APIs inside the server - Tested three test cases through postman – no auth, wrong credentials in basic auth header and valid credentials (setup earlier) in basic auth header for api2/\* within window server

Authentication worked as expected. Attaching screenshots.

**Screenshots**

***Test Scenario 1 – Access APIs outside the server***

**Test case 1 – No Auth - Failure**

**Graphical user interface, text, application, email

Description automatically generated**

**Test case 2 – Wrong credentials in Basic Auth – Failure**

**Graphical user interface, text, application, email

Description automatically generated**

**Test case 3 – Valid credentials in Basic Auth - Success**

**Graphical user interface, text, application, email

Description automatically generated**

***Test Scenario 2 – Access APis within the server***

**Test case 1 – No Auth - Failure**

**Graphical user interface, text, application, email

Description automatically generated**

**Test case 2 – Wrong credentials in Basic Auth - Failure**

**Graphical user interface, application

Description automatically generated**

**Test case 3 – Valid credentials in Basic Auth - Success**

**Graphical user interface, application

Description automatically generated**

***Test Scenario 3 – calling api2 from api1 programmatically***

**Test case 1 – No Auth - Failure**

**Graphical user interface, text, application, email

Description automatically generated**

**Test case 2 – Wrong credentials in Basic Auth - Failure**

**Graphical user interface, text, application, email

Description automatically generated**

**Test case 3 – Valid credentials in Basic Auth - Success**

Basic Auth is working programmatically, and we are getting valid response with valid credentials

**Graphical user interface, text, application, email

Description automatically generated**

**Workaround to create different authentication**

To cater needs of different authentication for different set of apis, we can design different vmss pools. For example, for one set of apis can be put in vmsspool1 and they can be authenticated with one set of Azure AD credentials and second set of apis can be put in vmsspool2 and they can be authenticated with other set of Azure AD credentials.

**Other Authentication options**

1. Multiple SSL profiles can be added in Application gateway. Reference link is below

[Configure mutual authentication on Azure Application Gateway through portal | Microsoft Docs](https://docs.microsoft.com/en-us/azure/application-gateway/mutual-authentication-portal)

1. **Programmatical way**

* In order to replace basic authentication, credentials can be stored in key vault or config files and using Azure SDKs in api codes, passed credentials can be validated.
* Use modern authentication methods (oauth/openid), where tokens are issued for authentication and authorization.

**Drawback**: -

All api programs need to accommodate these changes.

1. **AD DS service accounts**

If synced with Azure AD using AD Connect, then existing set of credentials which are used in on-permise applications can be used for basic authentication.