Step by step for using AAD for SOA job

Prerequisite

Enable HPC Pack AAD integration. See Manage an HPC Pack cluster in Azure using Azure Active Directory.

Use AAD Identity in HPC Echo Service

You can validate SOA AAD integration by starting EchoClient using an AAD identity as below:

1. Connect to HPC Pack 2016 Update 1 head node which enabled AAD integration.
2. Start command prompt.
3. Run following command:
   `EchoClient -useAad`
4. Login with AAD user account which is assigned HpcUsers or HpcAdminMirror role in prerequisite step if needed.
5. A SOA job named “CcpEchoSvc – WCF service” owned by the AAD user is started.
6. You can also pass user name and password of AAD account into EchoClient in a non-interactive manner using:
   `EchoClient -useAad -username <UserName> -password <Password>`

Use AAD Identity in Customized HPC SOA client

When implementing an HPC Client which intends to create SOA session under AAD identity, you need to construct a `SessionStartInfo` class and set `SessionStartInfo.UseAad` to true. This will prompt an interactive login window when a user start this SOA client with no AAD token cached in local. If `SessionStartInfo.Username` and `SessionStartInfo.Password` is also set, then login will be performed in a non-interactive way. Like following code snippet:

```
SessionStartInfo info = new SessionStartInfo(headnode, serviceName);
// Set UseAad to true to do authentication using AAD identity
info.UseAad = true;
// Set username and password to perform non-interactive authentication
info.Username = username;
info.Password = password;
```

Similarly, if you want to attach a session created under AAD identity in your client, set `SessionAttachInfo.UseAad` to true. Also set `SessionAttachInfo.Username` and `SessionAttachInfo.Password` if you need non-interactive authentication.

To read more about creating SOA service and client, see Write your first SOA service and client. You can download latest HPC Pack 2016 SDK from nuget.