Create demo/HOL environment

Required:

- Azure Pass code
- Azure Az Powershell Module installed
- Git CLI installed

1. Redeem Azure Pass

To redeem your Azure Pass, you should use an account that didn't ever redeem an Azure Pass before. DO NOT use your corporate account that is linked to your corporate Azure or M365 tenant!

The easiest way is to sign up for a new outlook.com (https://outlook.live.com/owa/?nlp=1&signup=1) email address and use that for management

Once you have your email, go to https://www.microsoftazurepass.com/ in an **in-private browser** window and redeem your pass. Make sure you are using the right account. Enter the promo code you received.

After your account is created, you will be redirected to the Azure portal. If this is not your default, it is highly recommenced to set the language of the Azure portal to English.

2. Create administrative account

Go to Azure Active Directory

Click on Add-User

Create a new administrative user (recommendation: call it "admin"). Assign a password.

Under roles, assign "Global Administrator".

Once the account is created, I recommend enabling MFA on this account. To do this, select the user, go to "Authentication Methods" and clock on "Require multifactor authentication"

Then, in the Azure portal, go to Subscriptions and select your Azure subscription. Go to Access Control (IAM) and add the Owner role to your admin account.

Copy the full account name (admin@xxx.onmicrosoft.com)

Sign out pf the Azure portal with your outlook.com (or other email) account and sign back in with the admin account. Set up MFA. I recommend creating a Microsoft Edge profile with this account. Change the password and finish MFA setup.

3. Clone the Github repository

Go to https://github.com/sk-bln/SQL-Hackathon and clone the repository to your local drive

```
git clone https://github.com/sk-bln/SQL-Hackathon
```

4. Set up Azure AD Users

Open Powershell and navigate to the folder “SubscriptionSetup”

The setup for the AAD accounts of the users (only used in the monitoring and security labs) is in CreateParticipantAccounts.ps1. Enter the default password. In the all hands-on material, the password is `Demo@pass1234567`

Ensure you have the Azure AZ Powershell module installed on the machine, if you don’t have it install it through the following commad in PowerShell
Install-Module -Name Az -Scope CurrentUser -Repository PSGallery -Force
Details can be found here
Also install the following module in a PowerShell window that’s open with “run as administrator” privileges
Install-Module Az.Resources

When you use a different password, please make sure you communicate that to the participants.

In an administrative Powershell, execute

```
Set-ExecutionPolicy RemoteSigned
```

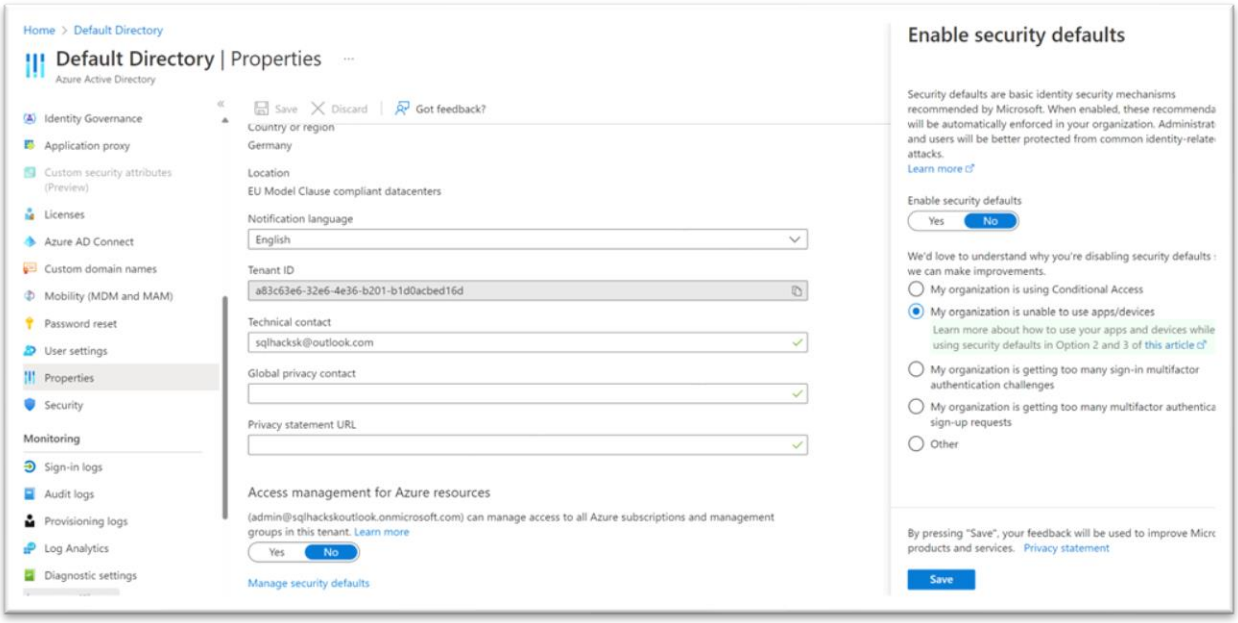
```
.\CreateParticipantAccounts.ps1
```

You will need to log in twice (using your admin@xxx.onmicrosoft.com account) – once for Azure sign in, once for Azure Active Directory management sign in.

The script takes a few minutes to complete. After this, wait another few minutes and then validate the accounts got created and assigned subscription contributor permissions

Notice: Azure now requires MFA for administrative accounts within 14 days. If you want to re-use the environment, you have to reset MFA for users, recreate users or disable security default

To disable security defaults, go to Azure Active Directory, Properties, Manage Security Defaults and set Enable security Defaults to No, then click Save



5. Register Resource Providers

To see your quota and to make the deployments successful, you need to register at least the following resource providers (under Subscription->Resource Providers):

- Microsoft.Compute
- Microsoft.Network
- Microsoft.Sql
- Microsoft.KeyVault
- Microsoft.Batch

6. Increase quota

If you want to create more than 3 participant VMs, your **vCore and Public IP Address quota** is probably insufficient

Go to your subscription->Usage+Quota. You only see the quota after you registered the resource providers

Select the region you chose (North Europe or West Europe) and select

- Total Regional vCPUs
- Standard Dv3 Family vCPUs

Click on “Request quota increase”

You need 2* Number of participant VMs Dv3 vCPUs and 10 more total vCPUs

So if you create 10 participant VMs (recommended maximum), you need 20 Dv3 vCPUs and 30 Total Regional vCPUs

Enter these values and submit the ticket. Wait until the request is finished. In most cases, this only takes a few minutes, but it may take days if the region has a capacity constraint. You may want to chose a different Azure region in this case

Then request quota for Public IP Addresses. Select Networking under Usage and Quota, then select Public IP addresses. You need # of participant VMs + 2 (i.e. 12 for 10 participant VMs). You need to create a support ticket for this by clicking on the icon right to “Public IP Adddresses”, you’ll also add some details as preferred way communication, name, email and country then click create. Wait with deployment until the quota is confirmed. This may take hours or days.

Also check if you have quota for SQL Managed Instance in the region selected. For this, go to SQL Managed Instances in the Azure portal and click “Create SQL Managed Instance”. Select the Azure region you want to use and see if there is an error message “Managed Instance is not available for the chosen subscription and region.” Shown directly below the region selection. If so, select a different Azure region.

7. Deploy the environment

In an **administrative** PowerShell, go to the folder SQL-Hackathon\Build and execute “ARM Deployment - SQL Hackathon v2.ps1”

When prompted, select the following:

Subscription: Make sure the shown subscription is the right one

Number of Team VM's: Select based on the maximum number of participants you expect. Remember you need to check them all, so don't do too many. 10 is a good number

Location: It needs to be an Azure region where you have a SQL Managed Instance quota. northeurope and westeurope are fine at the time of this writing. If you need another region, check quota beforehand

Username: **demouser**

Password: **Demo@pass1234567**

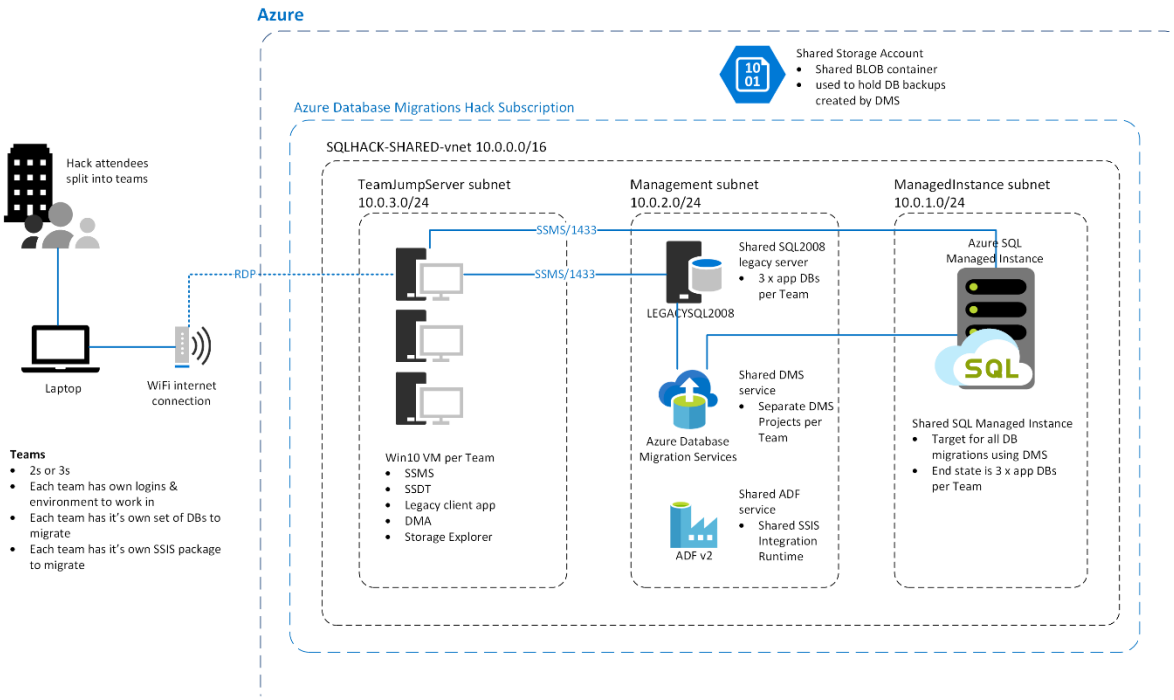
Resource group names: Confirm defaults

The complete deployment will take 4-6 hours. Go to both SQLHACK_ resource groups created and check under "Deployments" that all deployments are Succeeded. There need to be at least 5 deployments in the SQLHACK-SHARED resource group and 1 in SQLHACK-TEAM_VMs. If there are fewer, check the Activity Log of your resource group. Most likely the quota is insufficient.

If any of the deployments fail due to a transient error (like VPN Gateway timeout) delete both resource groups. You may need to delete the SQLHACK-SHARED two times before all resources are gone. Then wait at least 15 minutes after full deletion and deploy again

8. Post deployment check and setup

Once your environment is deployed, you have these components:



Start the VMs legacysql2008 and vm-TEAM01 if they are deallocated

8.1. Check legacy server

RDP into legacysql2008 (demouser/password see above)

8.1.1. Restore Databases

Open SQL Server Management studio and login through default windows authentication. Check that 60 databases (3 each for teams 1 to 20) have been created.

If the databases have not been restored follow these instructions:

1. Move the 60 .bak files from c:\ to c:\backups\
2. Do NOT use the scripts in the Backups folder.
3. Paste the content of `'SubscriptionSetup\Fixes\ 1- CREATE Logins.sql'` to a new SSMS Query Window and execute it. You may receive errors that the logins already exist. This is OK.
4. Paste the content of `'SubscriptionSetup\Fixes\2- RESTORE Databases.sql'` to a new SSMS Query Window and execute it.
   Validate that the 60 databases got restored
5. Paste the content of `'SubscriptionSetup\Fixes\3- RESTORE FIXES.sql'` to a new SSMS Query Window and execute it.

8.1.2.Enable CLR on legacy server

Enable CLR on the SQL 2008 Server and set permissions on system CLRs to "unrestricted", TRUSTWORTHY ON and change the owner
CLR assemblies in [TEAMXX_TenantDataDB] are reported as blockers in DMA due to CLR permission settings. This needs to be fixed in all 60 databases.

Connect to the LEGACYSQL2008 using the DemoUser account (which is sysadmin) and paste the content of `'SubscriptionSetup\Fixes\ EnableCLR.sql'` to a new SSMS Query Window and execute it.

8.2. General post-setup tasks

8.2.1. Enable CLR on the SQL Managed Instance

RDP into any of the team VMs

In SQL Server Management Studio, connect to the SQL Managed instance that was created in the SQLHACK_SHARED resource group (demouser/Demo@pass1234567)

Copy the content of `'SubscriptionSetup\Fixes\ EnableCLRinMI.sql'` to a new SSMS Query Window and execute it.

8.2.2. Prepare SSIS Demo

You need to run the Powershell script from the folder ...\SQL-Hackathon\Build\SQL SSIS Databases in an administrative Powershell to prepare the environment

This needs to be done from one of the team VMs.

RDP into any of the team VMs

Copy the folder "SQL SSIS Databases" to one of the Team VMs,

Open PowerShell in administrative mode. Execute the following:

```
Set-ExecutionPolicy RemoteSigned
'.\SSIS Build Script - TeamServer.ps1'
```

The installation of the Az and Sql PowerShell modules in the beginning can take a few minutes.

After this, log in to Azure using your admin@ account

Make sure the correct subscription is selected. You need to type the username (demouser) even though it is shown. Enter the password Demo@pass1234567, confirm resource group and managed instance.

Once completed check on the shared SQL Managed Instance that the [2008DW], [LocalMasterDataDb], [SharedMasterDataDB] and [TenantDataDb] databases have been restored to the SQL Managed Instance

8.2.3. Check SSIS integration runtime

Check that the SSIS integration runtime in the shared data factory is started.

To do this, go to the Azure Data Factory in the SQLHACK_SHARED resource group, click "Open Data Factory Studio". Click the Manage icon->Integration Runtimes. Select SSISIR and click Start

If it cannot be started, delete the SSISIR integration runtime and create a new SSIS integration runtime. The following parameters need to be set. Leave the rest at default

On Page 1

- Name: SSISIR

On page 2

- Admin username: demouser
- Admin password: Demo@pass12345467

On Page 3

- Subnet name: Select "Management"

Click Create and check the integration runtime starts

8.2.4. Prepare Security Demo – audit specification

1. Create a SAS token for the auditlogs container in the hack storage account (see 8.3.6 how to do this). You need the Blob SAS token, not the URL
2. Open SSMS, connect to the shared SQLMI and run the below SQL:
    a. Replace the **CEDENTIAL** name with the **URL** of the **Auditlogs** container in the shared storage account (you can get the URL from the properties blade of the container)
    b. Replace the **SECRET** parameter with the **SAS key** (labelled **BLOB SAS Token** in the Azure SAS Key creation blade) for the shared storage account container

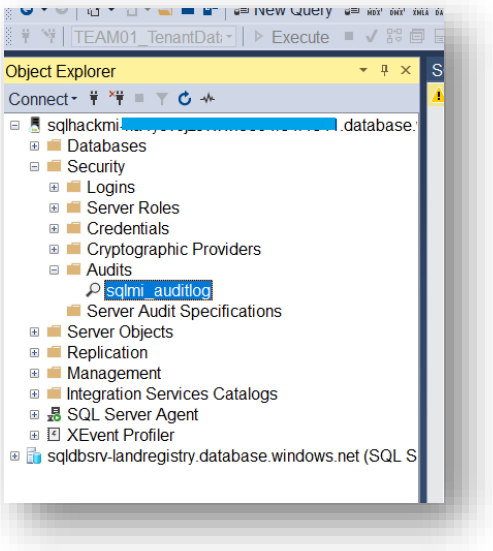
```
USE master;

CREATE CREDENTIAL [https://<<HACK SHARED STORAGE ACCOUNT HERE>>/auditlogs]
WITH IDENTITY='SHARED ACCESS SIGNATURE',
SECRET = '<<BLOB SAS TOKEN FOR THE SHARED STORAGE ACCOUNT CONTAINER HERE>>'
GO

CREATE SERVER AUDIT [sqlmi_auditlog]
TO URL ( PATH ='<<CREDENTIAL NAME HERE i.e. the URL used above>>'
       , RETENTION_DAYS = 30)
GO
```

```
ALTER SERVER AUDIT [sqlmi_auditlog]
WITH (STATE = ON)
GO
```

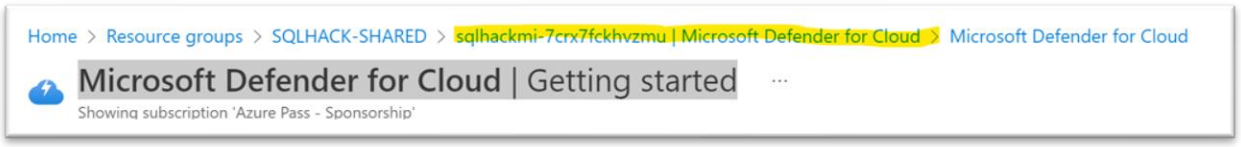
3. In SSMS you should now be able to see the Audit created



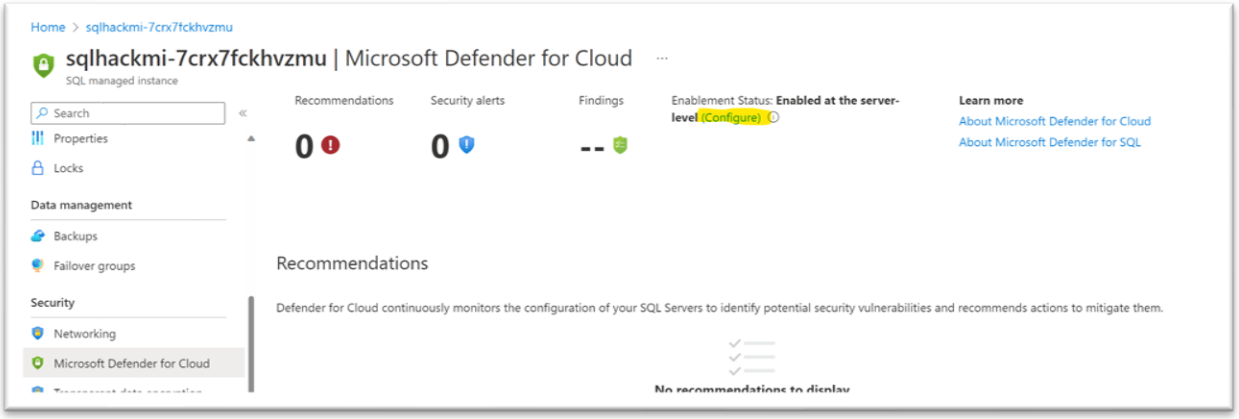
8.2.5. Prepare Security Demo – Azure Defender

For part 3 of the Security labs Azure Defender for SQL must be enabled on the shared SQL Managed Instance through the SQLMI Security Centre screen.

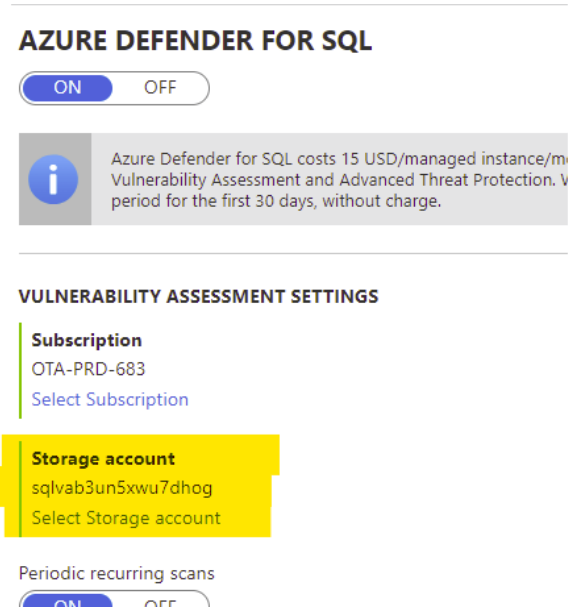
1. Enable Azure Defender for SQL
    a. SQLMI main blade – **Security\Microsoft Defender** for Cloud
    b. Click the blue **Enable Azure Defender for SQL** button
        i. If this gets you to the "Microsoft Defender for Cloud | Getting started" page instead of the Defender page for the SQL MI, click one step back at the breadcrumb navigation on the top of the page



2. Link the Vulnerability Assessment in Defender settings to one of the shared Storage Accounts
    a. At the top of the page click the "**(Configure)**" link next to the "Azure Defender for SQL: **Enabled at the server-level**" header



b. Under the **Storage account** settings check defender is linked to a Storage Account



8.2.6. Security Lab: Give Team accounts access to Key Vault

Security Lab 5 configures and tests Always Encrypted on a couple of columns in the [SalesLT].[Customer] table.

For this lab to work the Team ADD accounts must all have privileges in the shared Azure Key Vault.

Open the shared Key Vault and check that all required team AAD accounts have an Access Policy which gives them all permissions on Keys.

If not follow these instructions:

8.2.7. Prepare Security Demo – Set-up Key Vault Access

Notice: Lab 5 currently has an issue in the demo environment. Skip this lab

1. Navigate to the shared Azure Key Vault in the portal.
2. Under Settings select “Access Policies”
3. Click “**+Add Access Policy**”
4. Set “Key Permissions” to “Select All” for simplicity
5. Click the blue “**none selected**” link next to **Select principle**

6. In the **Principle** list search for **"sqlhack"** then click the TEAM01 account and click the blue **Select** button at the bottom.
7. Click **Add**. This will return you to the list of Access Policies and you should see your newly defined policy in the list.
8. Repeat for the other 19 Team logins or as many accounts as you have teams on the day (I'm not kidding – you have to do this painfully 1 at a time…
9. **When all team user accounts have a policy created click the Save button to apply your new policies.**

8.3. Check and update team VMs

The following steps need to be taken for each team VM

RDP into vm-TEAMXX as (demouser/password see above)

8.3.1. Check artifacts

On one of the Win10VMs check that the following software & artefacts are installed:

Artefact	Location	Notes
DMA	Desktop shortcut	
SQLHACK folder shortcut	Desktop shortcut	
SSMS	(start menu under SQL Server Tools 18)	Make sure SSMS launches – may need to reboot Win10 VMs

8.3.2. Check databases

Launch SSMS and connect to the LEGACYSQL2008 server using windows authentication. The server VM and SQL instance may need to be started.

Check the [TenantDataDb] has [SalesLT].[Customer] and [SalesLT].[Product] table and they are populated

a. Run this TSQL to check tables exists that they have data (check the Messages tab for errors).

```
DECLARE @cmd varchar(500)
SET @cmd='
	IF "?" LIKE "%TenantDataDb"
	BEGIN
		USE ?
		select DB_Name(), ''SalesLT.Customer'', count(*) from
SalesLT.Customer;
		select DB_Name(), ''SalesLT.Product'', count(*) from
SalesLT.Product;
	END'
EXEC sp_MSforeachdb @cmd;
```

If the data is missing, fix it according to \SubscriptionSetup\OriginalSetupInstructions\Hack Environment - SETUP AND RESET - MASTER.docx page 13

8.3.3. Test the sample app

Run the dummy SimpleTransReportApp application located at:

```
C:\_SQLHACK_\LABS\01-Data_Migration\SimpleTranReportApp.exe
```

On the Settings tab change the connection string details on the left using the following:

Server Name	LEGACYSQL2008	
Initial Catalog	TEAMxx_TenantDataDB	Where XX = a Team number between 01 and 20
Username	TEAMxx	
Password	TEAMxx	

Then click the "Change Connection String" button. The changes should be reflected in the window on the right.

Then go to the first tab and click "Run" to check the app is working. If you get a CLR error, validate that you have executed the CLR script from section 8.1

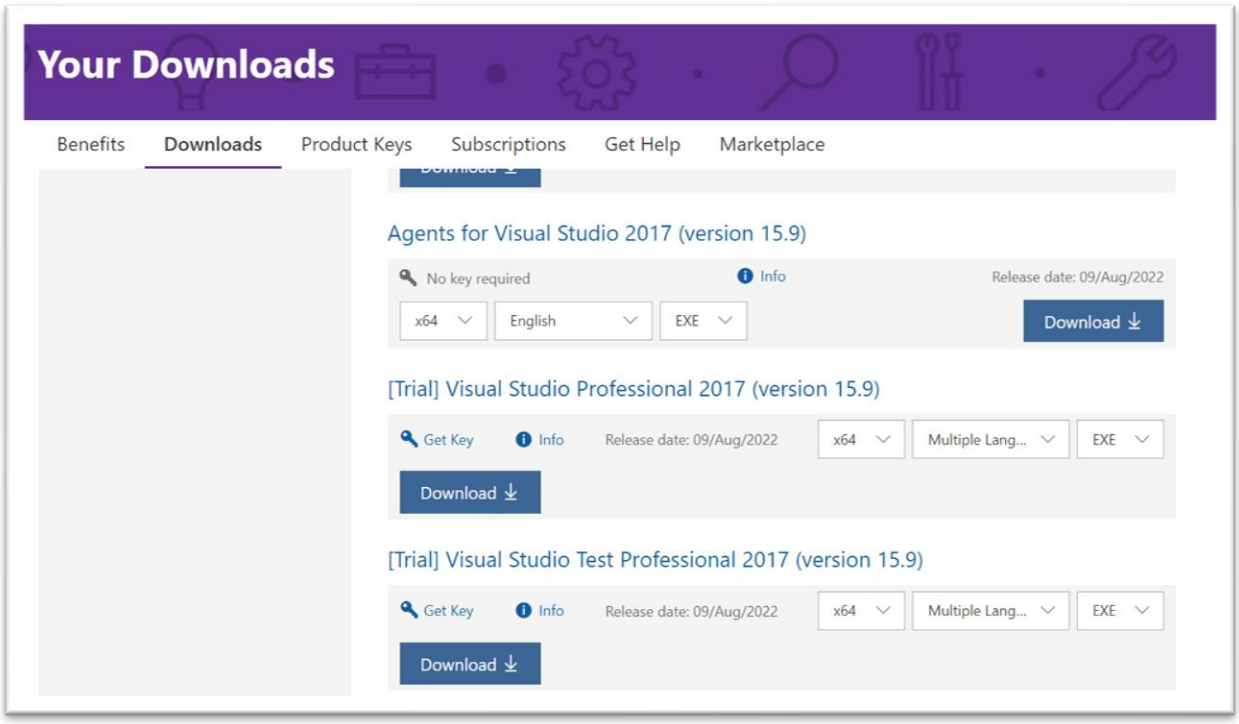
8.3.4. Install Visual Studio and SQL Server Data Tools

Visual Studio is not installed due to a conflict with newer Windows 10 builds. Install it if you want to do the SSIS lab

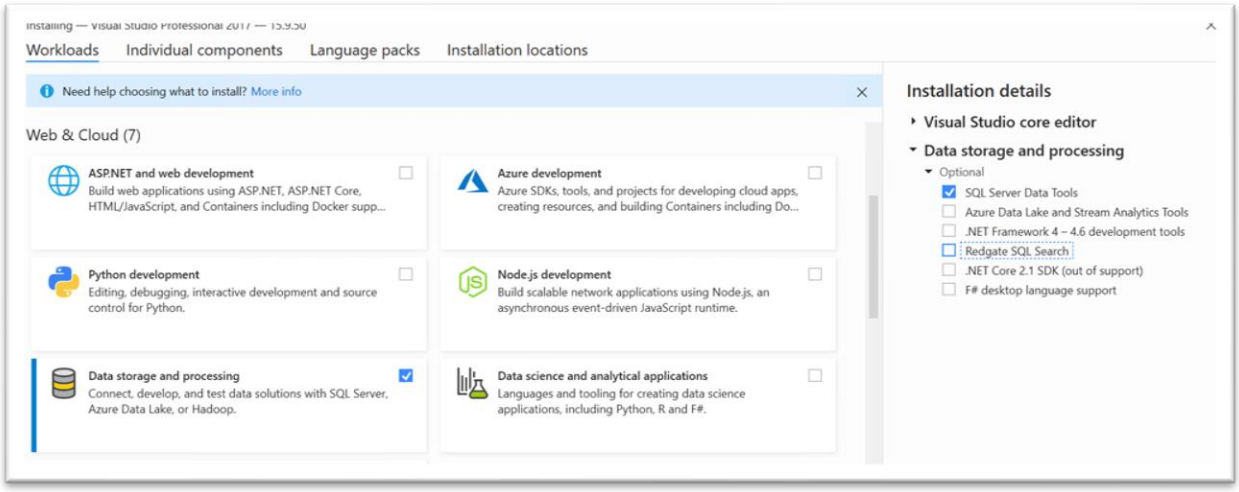
Go to

```
https://visualstudio.microsoft.com/vs/older-downloads/
```

Select 2017 Professional Trial (after logging in with your outlook.com account)



On installation, select SQL Server Data Tools:



After this, install SSIS from here:

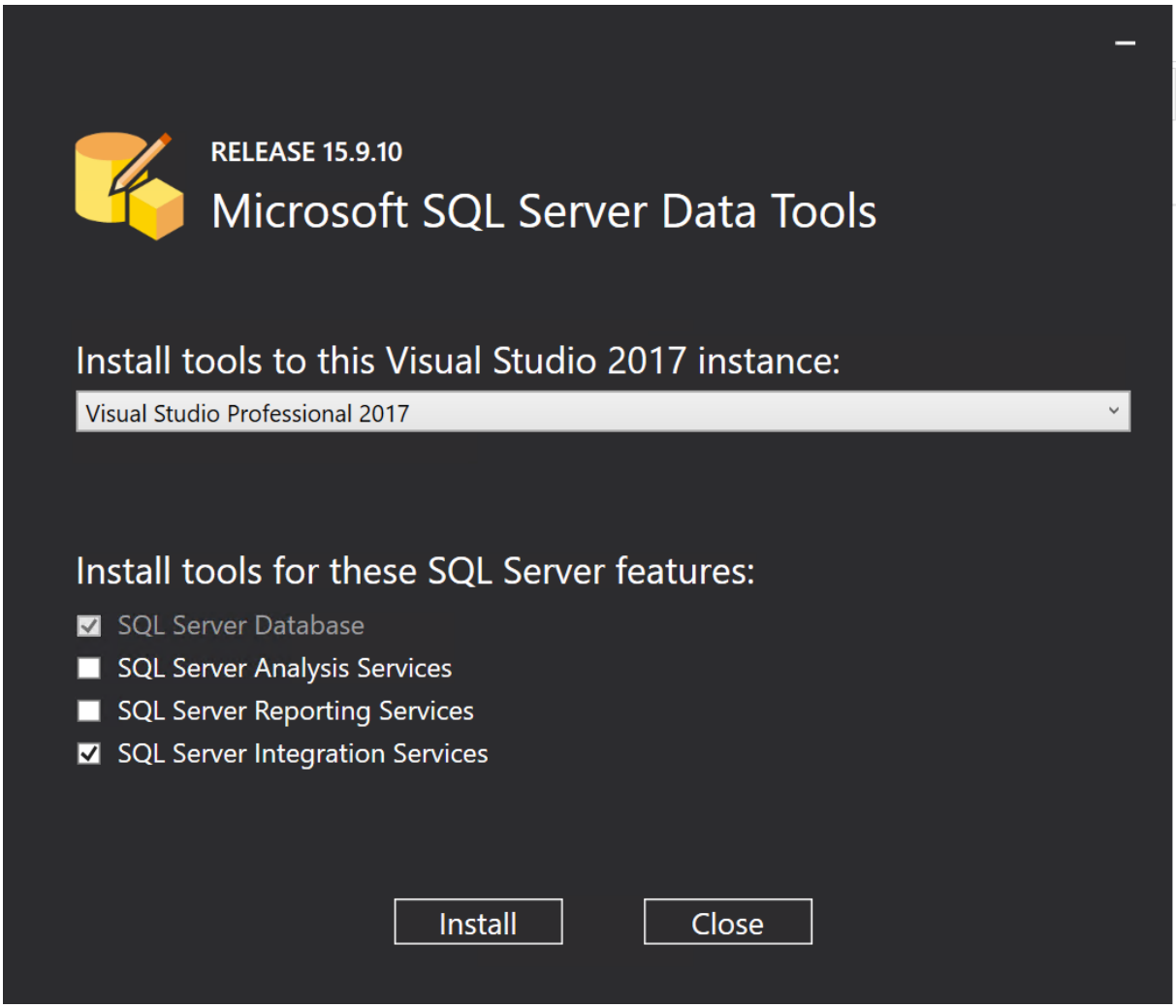
https://go.microsoft.com/fwlink/?linkid=2192400

Documentation is here:

https://docs.microsoft.com/en-us/sql/ssdt/previous-releases-of-sql-server-data-tools-ssdt-and-ssdt-bi?view=sql-server-2017#ssdt-for-vs-2017-standalone-installer

And here: How To: https://www.mssqltips.com/sqlservertip/6481/install-sql-server-integration-services-in-visual-studio-2019/

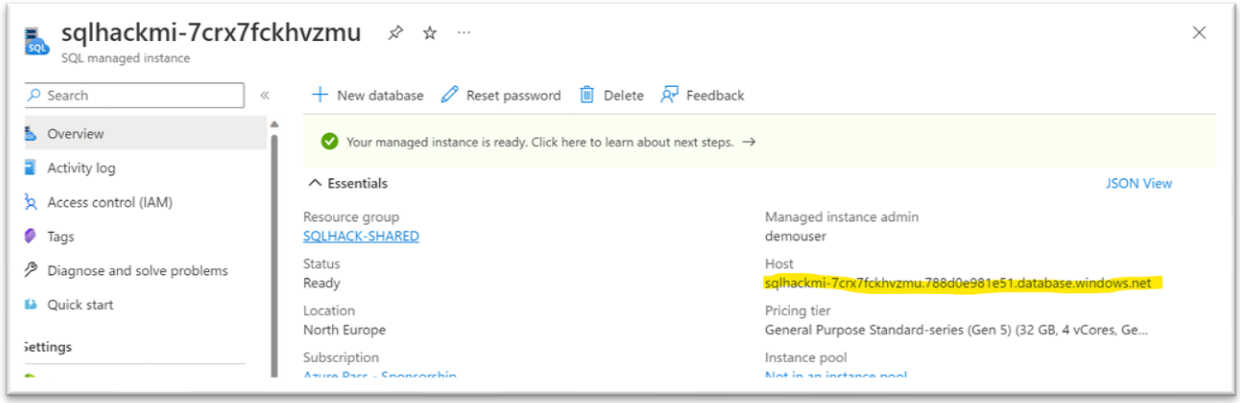
Select the existing Visual Studio install and SSIS on installation



8.3.5. Copy the SQL Managed Instance FQDN to the VM

In `C:\_SQLHACK_\LABS\01-Data_Migration\` create a text file named `ManagedInstanceFQDN.txt`

Find the FQDN/full host name of the created SQL Managed instance to this text file and save it:



8.3.6. Update the SAS Key

The SAS key generated by template is incorrect.

Generate a new SAS URI key for the SQLHack blob container

- Go to the storage account in the SQLHACK-SHARED resource group. Go to Containers->migration
- Click on “Shared access tokens”. Select **Read/Write/List/Delete** under permissions
- For expiry, select a long enough time (10 years in the future)
- Click “Generate SAS token and URL”

Paste the content of “Blob SAS URL” into C:_SQLHACK_\LABS\01-Data Migration\SASKey.txt on each Win10 VM and save the file

You can re-use the SAS key on all VMs.

9. Environment Reuse - Reset Tasks

If the same hack environment is to be reused, a number of quick tasks need to be performed to reset the environment for another run:

Check DMS is running	Do this manually through the Azure Portal
Start Win10 VMs (set to shut down at 7pm)	Do this manually through the Azure Portal
Start LEGACYSQL2008 VMs (set to shut down at 7pm)	Do this manually through the Azure Portal
Delete any existing DMS projects	Do this manually through the Azure Portal
Delete migrated DBs & migrated logins from the SQL MI	Run `reset/SQLMIReset.sql` TSQL script (below) to drop all previously migrated DBs and logins. Be sure to uncomment step 3 after you validated the databases are the correct ones
Delete any DB backups in \\\legacysql2008\FILESHARE	*This might be done automatically by DMS*
Delete backups from BLOB Storage	*This might be done automatically by DMS*
Check location Wi-Fi allows RDP	RDP outbound may not be enabled if doing a closed/private hack