Secure DevOps and Web Application Security

Prerequisites

Instructor Edition

**Conditions and Terms of Use**

**Microsoft Confidential**

This training package is proprietary and confidential and is intended only for uses described in the training materials. Content and software is provided to you under a Non-Disclosure Agreement and cannot be distributed. Copying or disclosing all or any portion of the content and/or software included in such packages is strictly prohibited.

The contents of this package are for informational and training purposes only and are provided "as is" without warranty of any kind, whether express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement.

Training package content, including URLs and other Internet Web site references, is subject to change without notice. Because Microsoft must respond to changing market conditions, the content should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication. Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

**Copyright and Trademarks**

© 2019 Microsoft Corporation. All rights reserved.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

For more information, see Use of Microsoft Copyrighted Content at

<http://www.microsoft.com/en-us/legal/intellectualproperty/Permissions/default.aspx>

DirectX, Hyper-V, Internet Explorer, Microsoft, Outlook, OneDrive, SQL Server, Windows, Microsoft Azure, Windows PowerShell, Windows Server, Windows Vista, and Zune are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other Microsoft products mentioned herein may be either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks are property of their respective owners.

Contents

[Prerequisites 6](#_Toc13689782)

[Exercise 1.1: Setup Service Principal for the environment 7](#_Toc13689783)

[Exercise 1.2: Setup the environment 10](#_Toc13689784)

# Prerequisites

#### Introduction

In this module, you will prepare the lab environment.

#### Objectives

After completing this prerequisite, you will have an AKS environment that will be used for the rest of the Secure DevOps class.

#### Prerequisites

Microsoft Azure Subscription Account with admin access. If you do not already have an Azure subscription with admin access, one will be provided for you during the class.

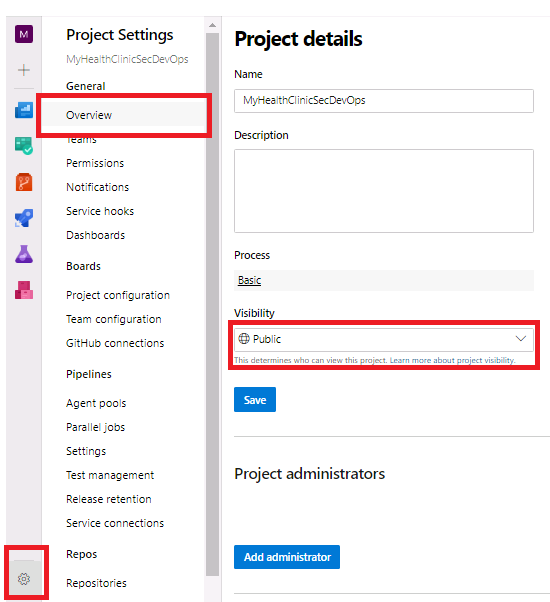
Azure DevOps Account

Azure DevOps Organization with Admin access

Clone the repo below into your subscription. <https://dev.azure.com/secureDevOpsDelivery/_git/MyHealthClinicSecDevOps-Public>

Step-by-Step [here](https://docs.microsoft.com/en-us/azure/devops/repos/git/import-git-repository?view=azure-devops)

Make sure your project is designated as a Public project



Install the ***Replace Tokens*** extension from the [Visual Studio Marketplace](https://marketplace.visualstudio.com/items?itemName=qetza.replacetokens).

* Navigate to the ***Replace Tokens*** extension in the Visual Studio Marketplace and click **Get it free** to install it.

Install the ***SonarCloud***extension from the [Visual Studio Marketplace](https://marketplace.visualstudio.com/items?itemName=SonarSource.sonarcloud).

* Navigate to the ***SonarCloud*** extension in the Visual Studio Marketplace and click **Get it free** to install it.

Install the ***Secure DevOps Kit for Azure*** from the [Visual Studio Marketplace](https://marketplace.visualstudio.com/items?itemName=azsdktm.AzSDK-task).

* Navigate to the ***Secure DevOps Kit for Azure*** extension in the Visual Studio Marketplace and click **Get it free** to install it.

Install the ***WhiteSource Bolt*** extension from the [Visual Studio Marketplace](https://marketplace.visualstudio.com/items?itemName=whitesource.ws-bolt).

#### Estimated Time to Complete This Prerequisite

35 minutes

# Exercise 1.1: Setup Service Principal for the environment

1. Start **Azure Cloud Shell**. [Click here](https://shell.azure.com/)  to launch Azure Cloud Shell. Log in with the proper credentials. If you are using your company’s subscription, select your company directory. If you are prompted to create an Azure storage container, please accept it.

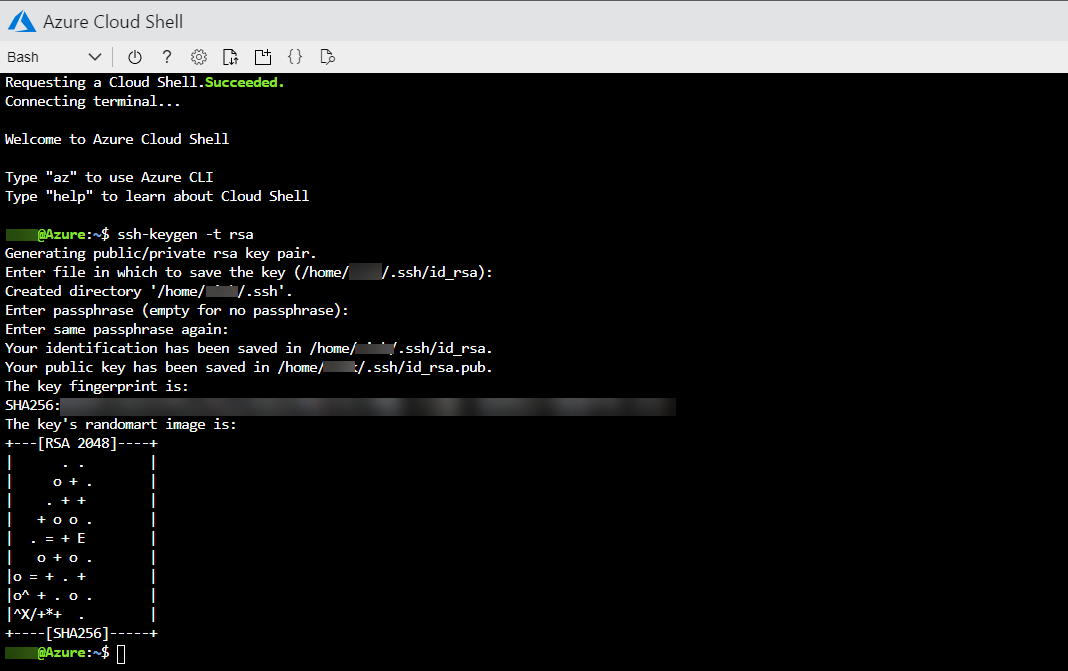
Check which subscription you are connected to by running the following command

**az account show**

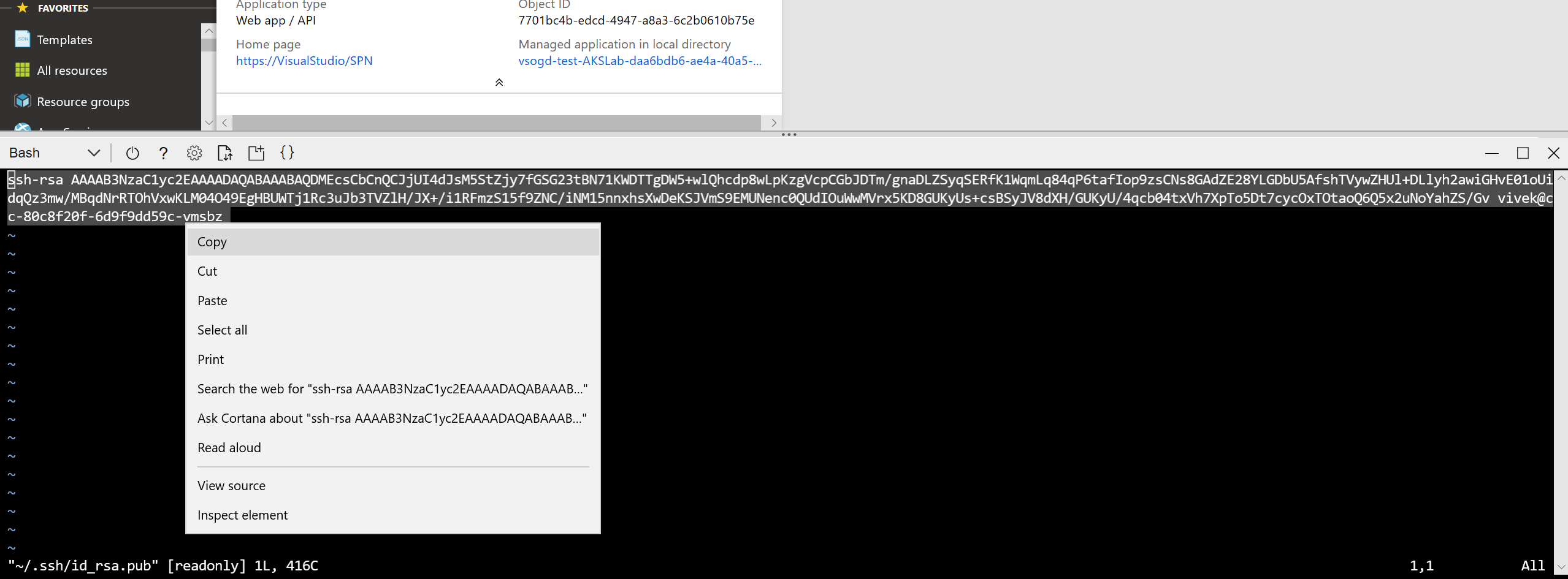
If you are not connected to the proper subscription, fix it by running the following command

**az account set --subscription YourSubscriptionID**

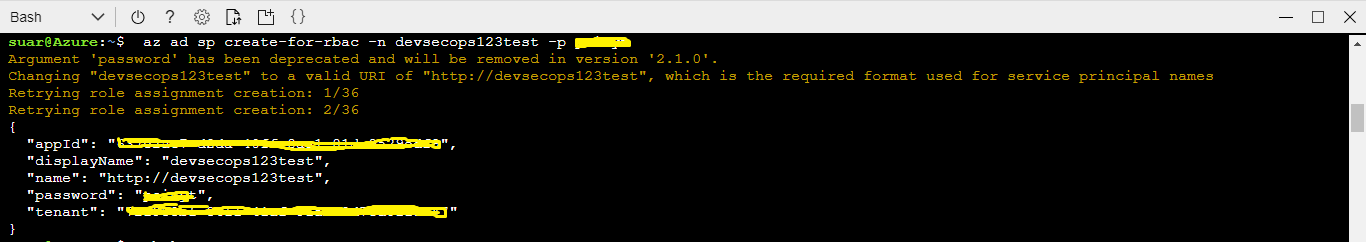
1. Follow the below instructions to create a pair of SSH RSA public & private keys which will be used in the next exercise.
   1. Type the command **ssh-keygen -t rsa** and press the **Enter** button.
   2. Provide the following values:
      1. **File path**: Leave it blank to save the file to default path.
      2. **Passphrase** : Provide a passphrase or leave it blank for an empty passphrase.
   3. Access the path where the keys are generated. The contents of the public key id\_rsa.pub is generated under the .ssh folder and is required for setting up the environment.



* 1. Execute **vi /home/###/.ssh/id\_rsa.pub** to read ssh token from id\_rsa.pub where ### is your respective name.
  2. Copy SSH key as shown below and paste it into a document as you will need it later.



1. Press “:” followed by “q” and press Enter key to exit from vi editor.
2. Create SPN
   1. Type **az ad sp create-for-rbac -n SecureDevOps-NNN** (Where **NNN** is a random number of **your choice**) to create a service principal with default access to Azure resources.



* 1. Copy the Service Principal **appID** and **password** from the output of the previous command and keep them in a safe place as we will use them in the next exercise.

# Exercise 1.2: Setup the environment

The following azure resources need to be configured for this lab:

| **Azure resources** | **Description** |
| --- | --- |
| Azure Container Registry | Used to store the Docker images privately |
| Azure Kubernetes Service | Docker images are deployed to Pods running inside AKS |
| Azure SQL Server | SQL Server on Azure to host databases |

The [ARM template](https://github.com/Microsoft/azuredevopslabs/blob/master/labs/vstsextend/kubernetes/armtemplate/azuredeploy.json)  used below for the deployment of these services is from the lab "Deploying to Azure Kubernetes Service (AKS)", which is one of the many hands-on Azure DevOps labs available at <https://github.com/microsoft/azuredevopslabs>

1. Please copy the url from the grey box (Triple click on the url selects the entire string) and paste in your browser to spin up **Azure Container Registry, Azure Kubernetes Service (AKS)** and **Azure SQL Server**.

https://portal.azure.com/#create/Microsoft.Template/uri/https%3A%2F%2Fraw.githubusercontent.com%2FMicrosoft%2Fazuredevopslabs%2Fmaster%2Flabs%2Fvstsextend%2Fkubernetes%2Farmtemplate%2Fazuredeploy.json

Enter the required details for the below fields, agree to the **Terms and Conditions**, and then Select the **Purchase** button.

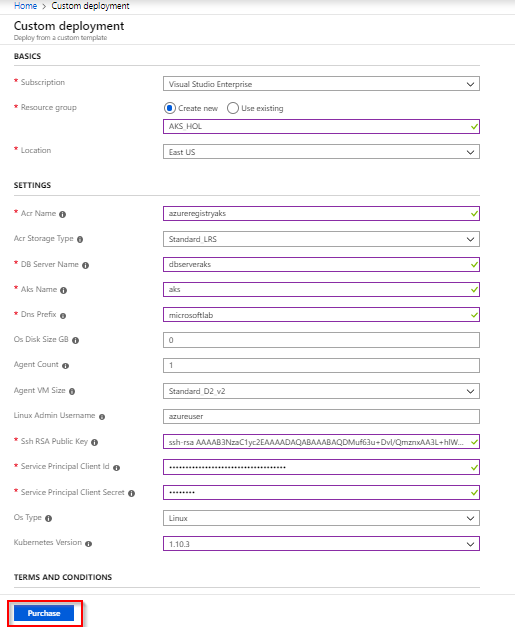
* 1. Subscription
  2. Resource Group (use **Create New** option)
  3. Location

Important: We have tested this lab with the "East US" location. We cannot guarantee that it will work with any other location as some Azure services may not be available in those locations.

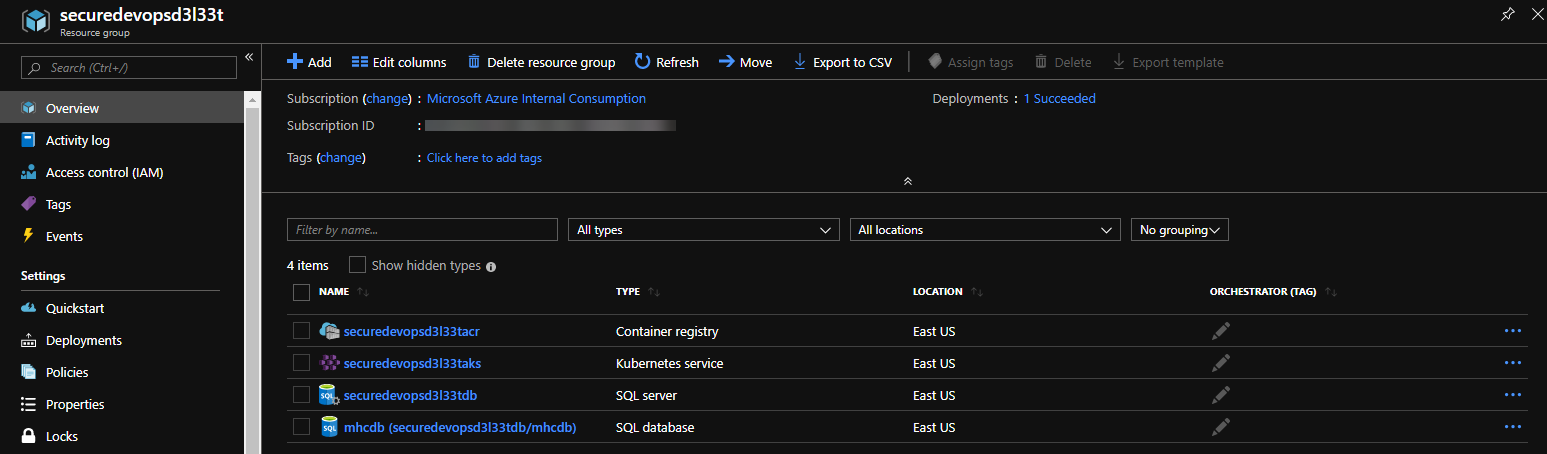
* 1. Acr Name: this name may contain alpha numeric characters only and must be between 5 and 50 characters. (Recommended name – devsecops**nnn**acr)

TIP: The **nnn** value can be any value you choose between 001-999.

* 1. DB Server Name: can only be made up of lowercase letters 'a'-'z', the numbers 0-9 and the hyphen. The hyphen may not lead or trail in the name. (Recommended name - devsecops**nnn**db)
  2. AKS Name (Recommended name - devsecops**nnn**aks)
  3. DNS Prefix (Recommended name - devsecops**nnn**dns)
  4. SSH RSA Public Key: use the contents of the public key id\_rsa.pub you generated in the previous exercise.
  5. Service Principal Client: use the appID of the Service Principal you created in the previous exercise.
  6. Service Principal Client Secret: use the password of the Service Principal you created in the previous exercise.
  7. Kubernetes version: Select the latest version

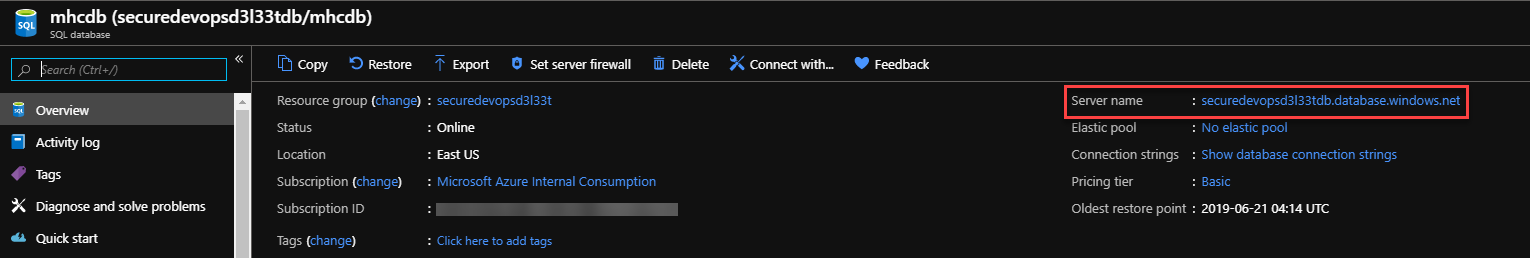


1. It takes about 5 minutes to provision the environment. Once the deployment succeeds, a notification is displayed in the Azure portal. Select the **Go to resource group** button.
   1. If the deployment fails, delete the resource group and redeploy.
2. Once the deployment successfully completes, you should see the following components from the Azure Portal when you select the Resource Group you specified in the deployment form above: **Storage account, Kubernetes service, Container registry, SQL server** along with **SQL database**.



Access each of these components individually and make a note of below mentioned details which will be used in the next exercises.

1. Select the **mhcdb** SQL database and make a note of the **Server name**.



1. Go back to the Resource Group, select the Container registry created and make a note of the **Login server** name.



1. Now let us grant permission to access ACR.

**Security Note**: AKS needs to authenticate with Azure Container Service (ACR) in order to pull images. You have two methods for configuring this: either grant AKS access to ACR through RBAC or use the Kubernetes image [pull secret mechanism](https://kubernetes.io/docs/concepts/configuration/secret/#using-imagepullsecrets) . The rest of this lab uses the second method. But if you want to use the first method and grant the service principal created for AKS permission to pull images from ACR instead of using its password, type the following commands:

1. Open a command prompt (if you do not have one already open from the previous exercise) and type **az login**. Wait for the browser to open up and enter your credentials.
2. Get the id of the service principal configured for AKS by typing **az aks show --resource-group YourResourceGroup --name YourAKSName --query "servicePrincipalProfile.clientId" --output tsv**. Replace YourResourceGroup and YourAKSName with the appropriate values.
3. Get the ACR registry resource id by tying **az acr show --name YourACRName --resource-group YourResourceGroup --query "id" --output tsv**. Replace YourACRName and YourResourceGroup with the appropriate values.
4. Create the role assignment by typing **az role assignment create --assignee Client\_ID --role acrpull --scope ACR\_ID**, where Client\_ID is the output of the command run in step b and ACR\_ID is the output of the command run in step c.

Additional information concerning this topic can be found [here](https://docs.microsoft.com/en-us/azure/container-registry/container-registry-auth-aks).