|  |  |
| --- | --- |
| C:\Users\tavis\Desktop\siteassets\header.png | IDEA  EIS Infrastructure Design Engineering & Architecture |

Azure Key Vault ARM Template (101-SQL-DB-Basic-Key-Vault)

February 1, 2017

Authors: Rob Scott

Version: 0.5 (draft)

Azure key vault deployment

**Table of Contents**

[**Introduction** 1](#_Toc462132193)

[**azure key vault arm template usage** 2](#_Toc462132194)

[post arm deployment configuration 3](#_Toc462132195)

[**service documentation** 3](#_Toc462132196)

**Introduction**

The Azure Key Vault ARM template (101-SQL-DB-Basic-Key-Vault.json) is intended to be used in conjunction with the Azure SQL Database ARM template (101-SQL-DB-Basic.json) to hold secrets associated with the Azure SQL authentication administrative account. Secure storage of the administrative account password in a key vault allows secure storage of the password along with limited access by security administrators. Once the Azure SQL Database ARM template (and associated PowerShell script) is used to deploy an Azure SQL database using the password in the vault, Azure Active Directory integration will be configured, allowing all further access to databases and Azure SQL capabilities to be controlled via Active Directory users and groups. Following this process ensures that the Azure SQL administrative account’s password is never used in the clear. The Azure Key Vault ARM template deploys the following:

1. Azure Key Vault.
2. An initial Azure Key Vault secret to be used as the Azure SQL Database administrative password.
3. A storage account to contain Azure Key Vault auditing events.

A post-deployment PowerShell script is provided which does the following:

1. Sets the audit policy for the Key Vault to log all audit event types.
2. Sets the audit event retention policy for all audit event types for the Key Vault for a specified number of days.

The Azure Key Vault ARM template is initially configured to deploy a single secret to be used in the deployment of an Azure SQL Database. The template can easily be adapted for other types of deployments.

**azure key vault arm template usage**

The Azure Key Vault template is intended for use with the associated Azure SQL Database ARM template but can be adapted for use with other templates. When used in conjunction with this template, the Key Vault name and the secret name must be the same as the name of the logical SQL Server. The Azure Key Vault ARM template will also deploy an Azure storage account which will be configured by a post-deployment PowerShell script to be used for logging audit events associated with use of the Azure Key Vault. The storage account name will be automatically generated by appending the literal string ‘kvstg’ to the name of the Key Vault. This will allow the correct storage account name to be used by the associated PowerShell script.

The following parameters are used by the template:

**keyVaultName**

This parameter contains the name of the key vault. When used in conjunction with the Azure SQL Database ARM template, this name must be the same as the name of the logical SQL Server to be deployed.

**tenantID**

This parameter is the name of the Azure subscription to be initially assigned access to the key vault. The value can be obtained by using the Get-AzureRmSubscription PowerShell cmdlet.

**objectID**

This parameter is the object ID of the AAD user or service principal that will have access to the vault. The object ID can be obtained by using the Get-AzureRmADUser or the Get-AzureRmADServicePrincipal cmdlets.

**keysPermissions**

This array lists the permissions that will be granted to the user to any keys within the vault. Valid values are all, create, import, update, get, list, delete, backup, restore, encrypt, decrypt, wrapkey, unwrapkey, sign and verify. Keys are not used in the initial version of the ARM templates for Azure SQL deployment.

**secretsPermissions**

This array lists permissions to grant to secrets within the vault. Valid values are all, get, set, list and delete.

**vaultSku**

Options are standard or premium.

**enabledForDeployment**

This bool value indicates whether the vault is enabled for VM or Service Fabric deployment. The default value is false for this template which is intended for secrets to be used in deployment of Azure SQL Databases.

**enabledForTemplateDeployment**

This bool value specifies whether the vault is enabled for template deployments. The default value is true.

**enableVaultForVolumeEncryption**

This bool value specifies wither the vault is enabled for volume encryption. The default value for this template is false.

**secretName**

The name of the secret to be stored in the vault. For use with the Azure SQL Database ARM template, this value should be the same as the name of the Azure logical SQL server.

**secretValue**

The value of the secret to store in the vault and is of type securestring.

**keyVaultAuditingStorageAccountType**

This string value specifies the storage account type for the storage account that will be deployed for containing key vault auditing events. The default value is Standard\_LRS.

post arm deployment configuration

A PowerShell script is provided (PostARMKeyVault.ps1) to perform post ARM deployment configuration associated with the template. The PowerShell script performs the following configurations:

1. Configure audit event logging for the vault using the storage account deployed by the ARM template.
2. Configure audit event retention for the vault.

For proper execution of the PowerShell script, the following variables must be set prior to execution:

**resourceGroupName**

This variable must be set to the name of the resource group that contains the vault.

**azureSubscriptionName**

The name of the Azure subscription that owns the key vault.

**retentionDays**

This variable must be set to the number of days to retain audit events.

**service documentation**

Information about the Azure Key Vault service can be found at <https://azure.microsoft.com/en-us/documentation/services/key-vault>.

The key vault ARM template schema is documented here: <https://azure.microsoft.com/en-us/documentation/articles/resource-manager-template-keyvault>.