Overview

Scan Result

Application Name	Project Name	Application Type	Application Components
DemoCpApp	DemoProject	Web Application	4

Code Lines	Application Platform	Scanned Date
56363	.Net	01/26/2018

Recommended Platform

AppService enables you to build and host web applications in the programming language of your choice without managing infrastructure. It offers auto-scaling and high availability, supports both Windows and Linux, and enables automated deployments from GitHub, Visual Studio Team Services, or any Git repo.
Why : This application is a good choice to move to Azure app services, as it has no blockers & has additional features without any cost.
Other Option : Azure Container Instance, Azure Kubernetes Service, Service Fabric and Virtual Machine.

Recommendations Result

Azure App Service	18
Virtual Machine	17
Azure Container(AKS)	18

Azure Infrastructure Cost

Azure App Service	S2 (USD $ 146.40)
Azure Container(AKS)	DS2 v2: 2 vCPUs (2 Nodes) (USD $ 367.92)
Virtual Machine	DS2 v2 (USD $ 184.46)

Migration Effort

Azure App Service	68 Hours
Azure Container(AKS)	58 Hours
Virtual Machine	50 Hours

App Service Assessment

Application Migration Recommendation

Azure Web Apps Azure App Service enables you to build and host web applications in the programming language of your choice without managing infrastructure. It offers auto-scaling and high availability, supports both Windows and Linux, and enables automated deployments from GitHub, Visual Studio Team Services, or any Git repo.
Why : This application is a good choice to move to Azure app services, as it has no blockers & has additional features without any cost.
Cost : - S2 (USD $ 146.40)
Other Option : Azure Container Instance, Azure Kubernetes Service, Service Fabric and Virtual Machine.

Recommendations Result

1 Day = 8 Hours

	Count	
Configuration :	9	42 Hours
Security :	6	17 Hours
Network & Availability :	0	0
Storage :	3	9 Hours

Recommendation by Size Estimate

1 Day = 8 Hours

	Count	
Small :	16	6 Days 4 Hours
Medium :	2	2 Days 0 Hours
Large :	0	0 Days

Recommendations

S1M.EventManagement

Category : Application & Platform Design **DataPoint :** AppSettingsSection

Reason for change

AppSettingsSection is used for storing sensitive information of application.

Code block	Line no.	File path
<appSettings> <add key="Email" value="gifting@s1mgift.com" /> <add key="Password" value="********" /> <add key="MailServer" value="smtp.office365.com" /> <add key="MailPort" value="587" /> <add key="IsSSLEnabled" value="true" /> <add key="EncryptionKey" value="D8215811-32B0-4276-9766-0984D6F53AD7" /> <add key="webpages:Version" value="3.0.0.0" /> <add key="webpages:Enabled" value="false" /> <add key="ClientValidationEnabled" value="true" /> <add key="UnobtrusiveJavaScriptEnabled" value="true" /> <add key="ApiPath" value="https://s1mapi.azurewebsites.net/" /> <add key="powerbi:AccessKey" value="HgnbWB2Q98MNWV+EKFNtDWNo7GiQq/b1Fx4wUN60mjk7y3Yq8rd+lwCdyTl78joPYJ1fBwRixaQnzBi4btte5A==" /> <add key="powerbi:ApiUrl" value="https://api.powerbi.com" /> <add key="powerbi:WorkspaceCollection" value="s1mws" /> <add key="powerbi:WorkspaceId" value="a4e0e2ed-5d4b-45fb-9173-a4a77dc4cba9" /> <add key="powerbi:reportId" value="59315de6-bc92-425b-985f-de37de3e6131" /> <add key="BlobStorage" value="https://s1mblob.blob.core.windows.net/s1m/" /> <add key="StorageConnectionString" value="DefaultEndpointsProtocol=https;AccountName=s1mblob;AccountKey=********" /> <add key="appURL" value="https://s1mclientapp.azurewebsites.net/?campaignid=" /> <add key="aspnet:MaxJsonDeserializerMembers" value="21407483647" /> </appSettings>	69	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\Web.config

Recommendation

The "appSettings" section in application is used to store and retrieve application-specific settings or configuration values.It provides a convenient way to store key-value pairs that can be accessed by the application at runtime. We are always recommended to replace sensitive configuration settings with references to Azure Key Vault secrets or encrypt.This helps in keeping the sensitive information out of your application source code and configuration files. Azure Key Vault is a cloud service offered by Microsoft Azure that allows you to securely store and manage cryptographic keys, secrets, and certificates. It provides a centralized repository for storing sensitive information used by your applications, such as API keys, connection strings, passwords, and encryption keys. Here is a high-level overview of the steps involved:

1. Create an Azure Key Vault instance in the Azure portal or using Azure CLI/PowerShell commands.
2. Define access policies for your Key Vault, specifying the permissions required for your application to read or manage secrets.
3. Install the Azure.Security.KeyVault.Secrets NuGet package to enable interaction with the Key Vault.
4. Install the Azure.Security.KeyVault.Secrets NuGet package to enable interaction with the Key Vault.
5. To authenticate application with Azure Key Vault, you need to create an Azure Active Directory (AD) application and retrieve its client ID (Application ID) and client secret (or a certificate).
6. Retrieve Azure AD Application Credentials: To authenticate your application with Azure Key Vault, you need to create an Azure Active Directory (AD) application and retrieve its client ID (Application ID) and client secret (or a certificate).
7. Authenticate with Azure Key Vault: In your ASP.NET application code, create an instance of the SecretClient class from the Azure.Security.KeyVault.Secrets namespace. Use the Azure AD application credentials obtained in the previous step to authenticate the client.
8. Access Secrets: Once authenticated, you can use the SecretClient instance to access secrets stored in the Key Vault. Retrieve secrets by their names using the GetSecretAsync method, specifying the name of the secret to retrieve.

Here is a sample code snippet demonstrating how to retrieve a secret from Azure Key Vault in an ASP.NET application: **using Azure.Identity; using Azure.Security.KeyVault.Secrets; var keyVaultUrl = "https://your-key-vault-name.vault.azure.net"; var clientId = "your-client-id"; var clientSecret = "your-client-secret"; var secretClient = new SecretClient(new Uri(keyVaultUrl), new ClientSecretCredential("", clientId, clientSecret)); var secretName = "your-secret-name"; KeyVaultSecret secret = await secretClient.GetSecretAsync(secretName); var secretValue = secret.Value; // Make use of the retrieved secret value in your application**

Estimated Efforts

8.00 Hours **Size :** Medium

Impact

Optional

Help URL

https://docs.microsoft.com/en-us/dotnet/azure/dotnet-howto-migrate-app-service?view=azure-dotnet#connection-strings-and-application-settings

Category : Application & Platform Design **DataPoint :** SessionStateSection

Reason for change

In Proc, Session mode will not support when you scale up your Application.

Code block	Line no.	File path
loginInfo = Session["LoginInfo"] as LoginResponse;	43	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\Areas\S1M\Controllers\CampaignSubCategoriesController.cs
loginInfo = Session["LoginInfo"] as LoginResponse;	85	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\Areas\S1M\Controllers\CampaignSubCategoriesController.cs
loginInfo = Session["LoginInfo"] as LoginResponse;	46	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\Areas\S1M\Controllers\CampaignTypeMasterController.cs

loginInfo = Session["LoginInfo"] as LoginResponse;	94	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\Areas\S1M\Controllers\CampaignTypeMasterController.cs
loginInfo = Session["LoginInfo"] as LoginResponse;	22	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\Areas\Sponsors\Controllers\SponsorsGiftController.cs

Recommendation

In Proc, Session mode will not support when the application is Scaled-Up. Use other session options to support the scalability of your application.

1- **Use OutProc Session** where Session State is stored In the StateServer and SqlServer modes.

2- **Azure Redis Cache:** Azure Redis Cache provides a session state provider that you can use to store your session state in a cache rather than in memory or in a SQL Server database. To use the caching session state provider, first, configure your cache, and then configure your ASP.NET application for the cache using the Redis Cache Session State NuGet package.

To configure a client application in Visual Studio using the Azure Cache for Redis Session State NuGet package, click NuGet Package Manager, Package Manager Console from the Tools menu.

Run the following command from the Package Manager Console window.

Install-Package Microsoft.Web.RedisSessionStateProvider

The NuGet package downloads and adds the required assembly references and adds the following section into your web.config file. This section contains the required configuration for your ASP.NET application to use the Redis Cache Session State Provider.

Configure Azure Cache for Redis settings.
Configure the attributes with the values from your cache blade in the Microsoft Azure portal, and configure the other values as desired.

Sample Code

```
<sessionState mode="Custom" customProvider="MySessionStateStore">
  <providers>
 <add name="MySessionStateStore" type="Microsoft.Web.Redis.RedisSessionStateProvider"
         host=""
         accessKey=""
         ssl="true" />
</sessionState>
```

Estimated Efforts

4.00 Hours **Size :** Small

Impact

Conditionally_Mandatory

Help URL

https://docs.microsoft.com/en-us/azure/redis-cache/cache-aspnet-session-state-provider https://docs.microsoft.com/en-us/azure/azure-cache-for-redis/cache-configure#configure-azure-cache-for-redis-settings

Category : Application & Platform Design **DataPoint :** Email

Reason for change

Mailing services is being used by your application.

Code block	Line no.	File path
SmtpClient smtp = new SmtpClient();	194	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\Areas\S1M\Controllers\ManageSponsorController.cs
SmtpClient smtp = new SmtpClient();	108	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\Controllers\HomeController.cs

Recommendation

SendGrid is a cloud-based email service that provides reliable transnational email delivery, scalability, and real-time analytics along with flexible APIs that make custom integration easy.

Create a SendGrid Account

To sign up for a SendGrid account:

1. Log in to the Azure portal.
2. In the menu on the left, click Create a resource.
3. Click Add-ons and then SendGrid Email Delivery.
4. Complete the signup form and select Create.
5. Enter a Name to identify your SendGrid service in your Azure settings. Names must be between 1 and 100 characters in length and contain only alphanumeric characters, dashes, dots, and underscores. The name must be unique in your list of subscribed Azure Store Items.
6. Enter and confirm your Password.
7. Choose your Subscription.
8. Create a new Resource group or use an existing one.
9. In the Pricing tier section select the SendGrid plan you want to sign up for.
10. Enter a Promotion Code if you have one.
11. Enter your Contact Information.
12. Review and accept the Legal terms.
13. After confirming your purchase you will see a Deployment Succeeded pop-up and you will see your account listed in the All resources section.

After you have completed your purchase and clicked the Manage button to initiate the email verification process, you will receive an email from SendGrid asking you to verify your account.

To send an email using SendGrid, you must supply your API Key.

To find your SendGrid API Key:

1. Click Manage.
2. In your SendGrid dashboard, select Settings and then API Keys in the menu on the left.
3. Click the Create API Key.
4. At a minimum, provide the name of this key and provide full access to Mail Send and select Save.
5. Your API will be displayed at this point at one time. Please be sure to store it safely.

How to: Send an Email

After creating an email message, you can send it using SendGrid's API. Alternatively, you may use. NET's built-in library.

Sending email requires that you supply your SendGrid API Key.

```
var apiKey = System.Environment.GetEnvironmentVariable("SENDGRID_APIKEY");
var client = new SendGridClient(apiKey);
```

The sample code shows how to send an email message using the SendGrid Web API with a console application.

Sample Code

```
using System;
using System.Threading.Tasks;
using SendGrid;
using SendGrid.Helpers.Mail;

namespace Example
{
    internal class Example
    {
        private static void Main()
        {
            Execute().Wait();
        }

        static async Task Execute()
        {
            var apiKey = System.Environment.GetEnvironmentVariable("SENDGRID_APIKEY");
            var client = new SendGridClient(apiKey);
            var msg = new SendGridMessage()
            {
                From = new EmailAddress("test@example.com", "DX Team"),
                Subject = "Hello World from the SendGrid CSharp SDK!",
                PlainTextContent = "Hello, Email!",
                HtmlContent = "Hello, Email!"
            };
            msg.AddTo(new EmailAddress("test@example.com", "Test User"));
            var response = await client.SendEmailAsync(msg);
        }
    }
}
```

Estimated Efforts

2.00 Hours **Size :** Small

Impact

Optional

Help URL

http://azure.microsoft.com/en-in/documentation/articles/sendgrid-dotnet-how-to-send-email/

Category : Application & Platform Design **DataPoint :** API Integration

Reason for change

External or In-House application url or API is being called in your code.

Code block	Line no.	File path
using (var client = new WebClient())	28	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\DataManager\ApiMethod.cs
using (var client = new WebClient())	47	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M

		.EventManagement\DataManager\ApiMethod.cs
using (var client = new WebClient())	66	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\DataManager\ApiMethod.cs
using (var client = new WebClient())	86	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\DataManager\ApiMethod.cs
using (var client = new WebClient())	111	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\DataManager\ApiMethod.cs

Recommendation

When migrating an .NET application to Azure App Service and considering the API calls to external or in-house applications, there are a few steps to ensure a successful transition:

1. Dependency management: Identify the APIs that your .NET application depends on. This includes any external or in-house APIs that are being called. Make a list of these APIs and note their specific details such as endpoint URLs, required authentication mechanisms, and any additional configuration settings.
2. Move APIs as dependencies: Once you have identified the APIs, you need to move them as dependencies to Azure. The exact process will depend on whether the APIs are external or in-house.
    - External APIs: If your application relies on external APIs, ensure that the API endpoints are accessible from the Azure App Service environment. You may need to update any hard-coded URLs to reflect the new environment. If there are any API keys or authentication tokens required, make sure they are properly configured and securely stored in the Azure App Service configuration.
    - In-house APIs: If the APIs are in-house and hosted within your organization network, you may need to set up a virtual network (VNet) in Azure and configure a virtual network gateway to establish connectivity between Azure and your organization network. This allows the Azure App Service to communicate with the in-house APIs securely. Consult Azure documentation for detailed guidance on setting up VNets and gateways.
3. Verify connectivity and ports: Once the APIs are moved as dependencies, verify the connectivity between your .NET application in Azure App Service and the APIs.
    - External APIs: Check if the Azure App Service environment has outbound internet access to communicate with the external APIs. Ensure that any required ports (e.g., HTTPS port 443) are open for outbound traffic.
    - In-house APIs: Verify that the connectivity is established between the Azure VNet and your organization network. Ensure that any necessary ports are open to allow communication between Azure and your in-house APIs.

By carefully managing dependencies, moving the APIs to Azure, and verifying connectivity and port requirements, you can ensure that your .NET application can seamlessly call the external or in-house APIs after migrating to Azure App Service.

Estimated Efforts

4.00 Hours **Size :** Small

Impact

Conditionally_Mandatory

Help URL

http://msdn.microsoft.com/en-us/library/ms751515%28v=vs.110%29.aspx

Category : Application & Platform Design **DataPoint :** Hard Coded URL

Reason for change

The Application uses Hard Coded Urls. These URLs may not be accessible after deployment in Azure App Service.

Code block	Line no.	File path
<script src="https://maps.googleapis.com/maps/api/js?AIzaSyCl2RZXFqqoJl-kUwwzY6GwWrn6GEzdWx8=&libraries=places&callback=initAutocomplete" async defer></script>	10	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\obj\Release\Package\PackageTmp\Areas\Sponsors\Views\Sponsor\OfferEntry.cshtml
@*<link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.4.0/css/font-awesome.min.css">	7	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\obj\Release\Package\PackageTmp\Areas\Sponsors\Views\SponsorsGift\Index.cshtml
<script src="http://ajax.aspnetcdn.com/ajax/jQuery/jquery-2.0.3.min.js"></script>*@	8	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\obj\Release\Package\PackageTmp\Areas\S1M\Views\Campaign\CampaignList.cshtml
<a href="#x" class="thumbnail"><img src="http://placehold.it/250x250" alt="Image" class="img-responsive"></a>	51, 52, 53, 54, 57, 58, 59, 60	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\obj\Release\Package\PackageTmp\Areas\S1M\Views\Campaign\CampaignList.cshtml
@*<div class="col-xs-6 "><img src="https://s1m.blob.core.windows.net/s1m/f4d16505-9339-4df5-b3ac-0b5f89fb0364" /></div>	389	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\obj\Release\Package\PackageTmp\Areas\S1M\Views\Campaign\SponsorEntry.cshtml

Recommendation

External or In-House application URL or API is being called in your code. Make sure about connectivity with the requested URL.

If these URLs are part of the application (Web Service/WCF Services/Web API) then also host these applications on Azure App Service based on Binding and Application Requirement and update the URL on the application.

Estimated Efforts

6.00 Hours **Size :** Small

Impact

Conditionally_Mandatory

Help URL

https://docs.microsoft.com/en-us/azure/app-service/environment/app-service-web-how-to-create-a-web-app-in-an-ase

Category : Security **DataPoint :** Connection Strings Section

Reason for change

ConnectionStringSection is use for storing database connectivity credential.It is very sensitive information of application.

Code block	Line no.	File path
<add name="defaultcon**	11	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\obj\Release\TransformWebConfig\transformed\Web.config
<add name="s1mmarketi**	17	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\obj\Release\TransformWebConfig\transformed\Web.config
<add name="defaultcon**	11	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\obj\Release\CSAutoParameterize\original\Web.config
<add name="s1mmarketi**	17	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\obj\Release\CSAutoParameterize\original\Web.config
<add name="defaultcon**	11	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\obj\Release\TransformWebConfig\original\Web.config

Recommendation

ConnectionStringSection uses for storing database connectivity credentials. It is very sensitive information about the application.

Azure Provide **Azure KeyVault**, to securely stores sensitive information of the application. So use that to store connection strings.

We are always recommended to encrypt the connection string of your application because the data we have there is highly sensitive. It must be secured.

Please find the following steps to encrypt the web. config.

1-Open Command Prompt with Administrator privileges
2-At the Command Prompt, enter
3-cd C:\Windows\Microsoft.NET\Framework\v4.0.30319
4-In case your web Config is located in "D:\Articles\EncryptWebConfig" directory path, then enter the following to encrypt the ConnectionString:

ASPNET_REGIIS -pef "connectionStrings" "D:\Articles\EncryptWebConfig

Sample Code

```
<configuration>
<connectionStrings
configProtectionProvider="RsaProtectedConfigurationProvider">
<EncryptedData Type="http://www.w3.org/2001/04/xmlenc#Element"
xmlns="http://www.w3.org/2001/04/xmlenc#">
```

```
<EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc">
<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
<EncryptedKey xmlns="http://www.w3.org/2001/04/xmlenc#">
<EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5" />
<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
<KeyName> RSA Key </KeyName>
 </KeyInfo>
 <CipherData>
 <CipherValue>
 WcFEbDX8VyLfAsVK8g6hZVAG1674ZFc1kWH0BoazgOwdBfinhcAmQmnIn0oHtZ5tO2EXGl+dyh10giEmO9NemH4Y
Zk+iMIln+ItcEay9CGWMXSen9UQLpcQHQqMJErZiPK4qPZaRWwqckLqriCl9X8x9OE7jKIsO2Ibapwj+1Jo=
 </CipherValue>
 </CipherData>
 </EncryptedKey>
 </KeyInfo>
 <CipherData>
 <CipherValue>
OpWQgQbq2wBZEGYAeV8WF82yz6q5WNFIj3rcuQ8gT0MP97aO9SHIZWwNggSEi2Ywi4omKOGA4mjqT0VZaXgb9tVeG
BDhjPh 5ZlrLMNfYSozeJ
m2Lsm7hnF6VvFm3fFMXa6+h0JTHeCXBdmzg/vQb0u3oejSGzB4ly+V9O0T4Yxkwn9KVDW58PHOeRT2//3iZfJ
WV2NZ4e6vj4Byjf8lo3JVNgRjmm9hr9blVbbT3Q8/j5zJ+TElCn6zPHvnuB70iG2KPJXqAj2GBzBk6cHq+WNebOQN
WIb7dTPumuZ K0yW1XDZ5gkfBuqgn8hm osTE7mCvieP9rgATf6qgLgdA6zYyVV6WDjo1qbCV807lczxa3bF5KzKa
VUSq5FS1SpdZKAE6/kkr0Ps++CE=
 </CipherValue>
 </CipherData>
</EncryptedData>
 </connectionStrings>
 </configuration>
```

Estimated Efforts

2.00 Hours **Size :** Small

Impact

Conditionally_Mandatory

Help URL

https://www.c-sharpcorner.com/article/encrypt-and-decrypt-connectionstring-in-web-config-file/

Category : Storage **DataPoint :** DB Connections

Reason for change

Database Connections might not work properly in Azure.

Code block	Line no.	File path
<add name="defaultcon***	11	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\obj\Release\TransformWebConfig\transformed\Web.config
<add name="s1mmarketi**	17	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M

**		.EventManagement\obj\Release\TransformWebConfig\transformed\Web.config
<add name="defaultcon***	11	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\obj\Release\CSAutoParameterize\original\Web.config
<add name="s1mmarketi***	17	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\obj\Release\CSAutoParameterize\original\Web.config
<add name="defaultcon***	11	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\obj\Release\TransformWebConfig\original\Web.config

Recommendation

Your current on-premises solution for Database Connectivity is unlikely to work in Azure.
Make sure Database Connectivity is publicly available.
Otherwise, migrate the database to Azure. Azure has the following options for migrating databases which are listed below:

1-SQL Server on Azure VMs
2-Azure SQL Database
3-Azure SQL Managed Instance
After migration, change Database Connectivity to Target platform.

Estimated Efforts

4.00 Hours **Size :** Small

Impact

Optional

Help URL

https://docs.microsoft.com/en-us/azure/sql-database/

Category : Security **DataPoint :** Encryption

Reason for change

The Application uses Encryption. These Encryption Algorithm may or may not be work in Azure App Service.

Code block	Line no.	File path
using (Aes encryptor = Aes.Create())	25	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\helperClass\Cryptography.cs
using (Aes encryptor = Aes.Create())	59	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M

		.EventManagement\helperClass\Cryptography.cs

Recommendation

Applications use encryption(cryptographic) keys and secrets to help keep information secure. Azure Key Vault safeguards these keys and secrets. When you use Key Vault, you can encrypt authentication keys, storage account keys, data encryption keys, .pfx files, and passwords by using keys that are protected by hardware security modules (HSMs).

Azure web application to read information from Azure Key Vault by using managed identities for Azure resources.
Below are steps How to use Azure Key Vault.

- Create a key vault.
- Store a secret in the key vault.
- Retrieve a secret from the key vault.
- Enable a managed service identity for the web app.
- Grant the required permissions for the web application to read data from the key vault.

For further assistance refer to the Help Url.

Estimated Efforts

4.00 Hours **Size :** Small

Impact

Conditionally_Mandatory

Help URL

https://docs.microsoft.com/en-us/azure/key-vault/key-vault-whatis

S1M.BAL

Category : Application & Platform Design **DataPoint :** SessionStateSection

Reason for change

In Proc, Session mode will not support when you scale up your Application.

Code block	Line no.	File path
LoginResponse sessionValue = HttpContext.Current.Session["LoginInfo"] as LoginResponse;	19	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.BAL\AssetMappingBL.cs

Recommendation

In Proc, Session mode will not support when the application is Scaled-Up. Use other session options to support the scalability of your application.

1- **Use OutProc Session** where Session State is stored In the StateServer and SqlServer modes.

2- **Azure Redis Cache:** Azure Redis Cache provides a session state provider that you can use to store your session state in a cache rather than in memory or in a SQL Server database. To use the caching session state provider, first, configure your cache, and then configure your ASP.NET application for the cache using the Redis Cache Session State NuGet package.

To configure a client application in Visual Studio using the Azure Cache for Redis Session State NuGet package, click NuGet Package Manager, Package Manager Console from the Tools menu.

Run the following command from the Package Manager Console window.

Install-Package Microsoft.Web.RedisSessionStateProvider

The NuGet package downloads and adds the required assembly references and adds the following section into your web. config file. This section contains the required configuration for your ASP.NET application to use the Redis Cache Session State Provider.

Configure Azure Cache for Redis settings.
Configure the attributes with the values from your cache blade in the Microsoft Azure portal, and configure the other values as desired.

Sample Code

```
<sessionState mode="Custom" customProvider="MySessionStateStore">
  <providers>
 <add name="MySessionStateStore" type="Microsoft.Web.Redis.RedisSessionStateProvider"
         host=""
         accessKey=""
         ssl="true" />
</sessionState>
```

Estimated Efforts

4.00 Hours **Size :** Small

Impact

Conditionally_Mandatory

Help URL

https://docs.microsoft.com/en-us/azure/redis-cache/cache-aspnet-session-state-provider https://docs.microsoft.com/en-us/azure/azure-cache-for-redis/cache-configure#configure-azure-cache-for-redis-settings

S1M.DAL

Category : Security **DataPoint :** Connection Strings Section

Reason for change

ConnectionStringSection is use for storing database connectivity credential.It is very sensitive information of application.

Code block	Line no.	File path
<add name="s1mmarketi*** *** ****	7	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.DAL\App.Config

Recommendation

ConnectionStringSection uses for storing database connectivity credentials. It is very sensitive information about the application.

Azure Provide **Azure KeyVault**, to securely stores sensitive information of the application. So use that to store connection strings.

We are always recommended to encrypt the connection string of your application because the data we have there is highly sensitive. It must be secured.

Please find the following steps to encrypt the web. config.

1-Open Command Prompt with Administrator privileges
2-At the Command Prompt, enter
3-cd C:\Windows\Microsoft.NET\Framework\v4.0.30319
4-In case your web Config is located in "D:\Articles\EncryptWebConfig" directory path, then enter the following to encrypt the ConnectionString:

ASPNET_REGIIS -pef "connectionStrings" "D:\Articles\EncryptWebConfig

Sample Code

```
<configuration>
<connectionStrings
configProtectionProvider="RsaProtectedConfigurationProvider">
<EncryptedData Type="http://www.w3.org/2001/04/xmlenc#Element"
xmlns="http://www.w3.org/2001/04/xmlenc#">
<EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc">
<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
<EncryptedKey xmlns="http://www.w3.org/2001/04/xmlenc#">
<EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5" />
<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
<KeyName> RSA Key </KeyName>
 </KeyInfo>
 <CipherData>
 <CipherValue>
 WcFEbDX8VyLfAsVK8g6hZVAG1674ZFc1kWH0BoazgOwdBfinhcAmQmnIn0oHtZ5tO2EXGl+dyh10giEmO9NemH4Y
Zk+iMIln+ItcEay9CGWMXSen9UQLpcQHQqMJErZiPK4qPZaRWwqckLqriCl9X8x9OE7jKIsO2Ibapwj+1Jo=
 </CipherValue>
 </CipherData>
 </EncryptedKey>
 </KeyInfo>
 <CipherData>
 <CipherValue>
OpWQgQbq2wBZEGYAeV8WF82yz6q5WNFIj3rcuQ8gT0MP97aO9SHIZWwNggSEi2Ywi4omKOGA4mjqT0VZaXgb9tVeG
BDhjPh 5ZlrLMNfYSozeJ
m2Lsm7hnF6VvFm3fFMXa6+h0JTHeCXBdmzg/vQb0u3oejSGzB4ly+V9O0T4Yxkwn9KVDW58PHOeRT2//3iZfJ
WV2NZ4e6vj4Byjf81o3JVNgRjmm9hr9blVbbT3Q8/j5zJ+TElCn6zPHvnuB70iG2KPJXqAj2GBzBk6cHq+WNebOQN
WIb7dTPumuZ K0yW1XDZ5gkfBuqgn8hm osTE7mCvieP9rgATf6qgLgdA6zYyVV6WDjo1qbCV807lczxa3bF5KzKa
VUSq5FS1SpdZKAE6/kkr0Ps++CE=
 </CipherValue>
 </CipherData>
</EncryptedData>
 </connectionStrings>
 </configuration>
```

Estimated Efforts

2.00 Hours **Size :** Small

Impact

Conditionally_Mandatory

Help URL

https://www.c-sharpcorner.com/article/encrypt-and-decrypt-connectionstring-in-web-config-file/

Category : Storage **DataPoint :** DB Connections

Reason for change

Database Connections might not work properly in Azure.

Code block	Line no.	File path
<add name="s1mmarketi***	7	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.DAL\App.Config

Recommendation

Your current on-premises solution for Database Connectivity is unlikely to work in Azure.
Make sure Database Connectivity is publicly available.
Otherwise, migrate the database to Azure. Azure has the following options for migrating databases which are listed below:

1-SQL Server on Azure VMs
2-Azure SQL Database
3-Azure SQL Managed Instance
After migration, change Database Connectivity to Target platform.

Estimated Efforts

4.00 Hours **Size :** Small

Impact

Optional

Help URL

https://docs.microsoft.com/en-us/azure/sql-database/

S1M.DTO

Questionnaire Result

Category : Application & Platform Design **DataPoint :** GAC Dependency

Reason for change

GAC Dependency is not supported on Azure App Service.

Recommendation

GAC Dependency is not supported on Azure App Service. Consider copying required assemblies to the app's \bin folder.

You can use the below option to resolve GAC Dependency

Right-click on the assembly reference, select properties, and change "Copy Local" to true. That will cause it to copy the assembly into the deployment directory

Estimated Efforts

4.00 Hours **Size :** Small

Impact

Mandatory

Help URL

https://www.c-sharpcorner.com/blogs/how-to-use-deployed-assembly-in-gac-or-assembly-resolution1

Category : Application & Platform Design **DataPoint :** Background Processing

Reason for change

Any batch process is running as a windows service or windows job, not support on Azure App Service.

Recommendation

Azure Web Apps and WebJobs
You can use Azure WebJobs to execute custom jobs as background tasks within an Azure Web App. WebJobs run within the context of your web app as a continuous process. WebJobs also run in response to a trigger event from Azure Scheduler or external factors, such as changes to storage blobs and message queues. Jobs can be started and stopped on demand, and shut down gracefully. If a continuously running WebJob fails, it is automatically restarted. Retry and error actions are configurable.

Azure WebJobs have the following characteristics:

- **Security:** WebJobs are protected by the deployment credentials of the web app.
- **Supported file types:** You can define WebJobs by using command scripts (.cmd), batch files (.bat), PowerShell scripts (.ps1), bash shell scripts (.sh), PHP scripts (.php), Python scripts (.py), JavaScript code (.js), and executable programs (.exe, .jar, and more).
- **Deployment:** You can deploy scripts and executables by using the Azure portal, by using Visual Studio, by using the Azure WebJobs SDK, or by copying them directly to the following locations:
  For triggered execution: site/wwwroot/app_data/jobs/triggered/{job name}
  For continuous execution: site/wwwroot/app_data/jobs/continuous/{job name}
- **Logging:** Console. Out is treated (marked) as INFO. Console. Error is treated as an ERROR. You can access monitoring and diagnostics information by using the Azure portal. You can download log files directly from the site. They are saved in the following locations:
  For triggered execution: Vfs/data/jobs/triggered/jobName
  For continuous execution: Vfs/data/jobs/continuous/jobName
- **Configuration:** You can configure WebJobs by using the portal, the REST API, and PowerShell. You can use a configuration file named settings. job in the same root directory as the job script to provide configuration information for a job.

Below are the steps to Configure it with a web job.

1. Open Azure portal using portal.azure.com.
2. Click on App service and Create a new web app with a suitable app service plan.
3. Now open the web app that you have created and then click on the web job.
4. Click on Add web job and provide your console app zip folder containing exe.
5. Choose Type as Triggered and Triggers as manually.
6. Now click on web job properties and copy the URL, username, and password.
7. Use URL, username, and password in your web application to run the web job.

To Schedule Web job continuously follow the steps below.

1. Open the Azure portal using portal.azure.com.
2. Click on App service and Create a new web app with a suitable app service plan.
3. Now open the web app that you have created and then click on the web job.
4. Click on Add web job and provide your console app zip folder containing exe.
5. Choose Type as Triggered and Triggers as Scheduled.
6. Provide a CRON Expression to schedule your web job.

Sample Code

```
var base64Auth = Convert.ToBase64String(Encoding.Default.GetBytes($"{username}:{password}
"));
using (var client = new HttpClient())
{
client.DefaultRequestHeaders. Add("Authorization", "Basic " + base64Auth);
var requestURl = new Uri (baseUrl)
var response = client.PostAsync(requestURl, null).Result;
}
```

Estimated Efforts

8.00 Hours **Size :** Medium

Impact

Mandatory

Help URL

https://docs.microsoft.com/en-us/azure/app-service/web-sites-create-web-jobs

Category : Storage **DataPoint :** Automatic Backup

Reason for change

Automatic Backup is used to minimize the risk of data loss and get backup automatic as per interval.

Recommendation

The Backup and Restore feature in Azure App Service lets you easily create app backups manually or on a schedule. You can restore the app to a snapshot of a previous state by overwriting the existing app or restoring it to another app.

Configure automated backups.

1. In the Azure portal, choose your web app from the Web Apps blade. This will display the details of your web app in a new blade.
2. Select the Settings option. The Settings blade will be displayed allowing you to modify your web app.
3. Choose the Backups option in the Settings blade. The Backups blade will be displayed.
4. On the Backups blade, set Scheduled Backup to ON.
5. Select the storage account to which you want to back up your web app. The storage account must belong to the same subscription as the web app that you are going to back up.
6. In the Frequency box, specify how often you want automated backups to be made. The number of days must be between 1 and 90, inclusive (from once a day to once every 90 days).
7. Use the Begin option to specify a date and time when you want the automated backups to begin.
8. In the Included Databases section, select the databases that are connected to your web app (SQL Server or MySQL) that you want to back up. For a database to appear in the list, its connection string must exist in the Connection strings section of the Web app settings blade in the portal.
9. Additionally, set the Retention (Days) value to the number of days you wish to retain the backup.
10. In the command bar, click the Save button to save your configuration changes.

How backups are stored

After you have made one or more backups for your app, the backups are visible on the Containers page of your storage account, and your app. In the storage account, each backup consists of an a.zip file that contains the backup data and a .xml file that contains a manifest of the .zip file contents. You can unzip and browse these files if you want to access your backups without actually performing an app restore.

Estimated Efforts

1.00 Hours **Size :** Small

Impact

Optional

Help URL

https://docs.microsoft.com/en-us/azure/app-service/web-sites-backup

Category : Security **DataPoint :** Firewall

Reason for change

Firewall configured in On-premise environment does not work for Azure App Service deployment

Recommendation

Web application firewalls (WAF) help secure your web applications by inspecting inbound web traffic to block SQL injections, Cross-Site Scripting, malware uploads & application DDoS, and other attacks.

To configure the firewall for app service deployment create an Application Gateway and use property Application Gateway WAF.

Steps to configure Application Gateway WAF are given below.

1. Create an application gateway.
2. Click Backend pools. A default pool was automatically created with the application gateway.
3. Click Add Backend pools and select App Service.
4. Select the App service on which the application is deployed.
5. Click Web Application Firewall, and Enable it.
6. Configure firewall rules and save.

Estimated Efforts

4.00 Hours **Size :** Small

Impact

Optional

Help URL

https://azure.microsoft.com/en-in/blog/azure-web-application-firewall-waf-generally-available/

Category : Security **DataPoint :** Secure Socket Layer (SSL)

Reason for change

Application defined some Secure Socket Layer(SSL) related settings.

Recommendation

Bind SSL certificate to Azure Web Apps

How to Configure

1. Log in to the Azure portal.
2. Navigate to â??App Servicesâ? in the left navigation pane.
3. Select your web application.
4. Click on â??Settingsâ? and select â??Custom domains and SSL.â?
5. A new frame will open on the right side. Click on â??Bring external domains.â?
6. Note the IP address located at the bottom. Go to your domain registrar website and create DNS entries using this IP address. It can take some time for the changes to propagate, depending on your DNS provider.
7. In the â??Domain Namesâ? text box, enter the custom domain name you bought from the domain registrar.
8. Save the changes.
9. Click on â??Upload certificate.â?
10. Locate and upload your .pfx certificate file.
11. Under â??SSL bindings,â? select the domain name to secure with SSL, and the certificate to use.
12. Save the changes.
13. You should be able to access the web app using your custom domain name over HTTPS.

Estimated Efforts

4.00 Hours **Size :** Small

Impact

Conditionally_Mandatory

Help URL

https://azure.microsoft.com/en-in/documentation/articles/cloud-services-configure-ssl-certificate/

Category : Application & Platform Design **DataPoint :** Com Import

Reason for change

Application using some COM+ Component that may or may not work properly

Recommendation

Application using some COM+ Component.

Follow the below steps to configure.

The component as an assembly
1. If You are using COM+ Component as an assembly, then Right click on assembly.
2. Select Property from Menu.
3. Select Copy to Output directory-> Copy Always.

The component as an exe
1. If You are using COM Component as an exe, then You need to create a startup script.
2. Create PowerShell script for COM+ Component.
3. Add Folder Startup in your Role.
4. Add All related files in the Startup folder.
5. Configure the startup task in your Service Definition file.

Sample Code

```
<sessionState mode="Custom" customProvider="MySessionStateStore">
  <providers>
 <add name="MySessionStateStore" type="Microsoft.Web.Redis.RedisSessionStateProvider"
          host=""
          accessKey=""
          ssl="true" />
</sessionState>
```

Estimated Efforts

2.00 Hours **Size :** Small

Impact

Optional

Help URL

https://stackoverflow.com/questions/14981830/asppdf-and-aspjpeg-on-windows-azure

Category : Security **DataPoint :** PII Information

Reason for change

Your application is storing or sharing PII Informations.

Recommendation

1. Use industry-standard AES encryption. 2. Use dual control and separation of duties to protect your encryption keys. 3. Encrypt sensitive data prior to moving and/or use encrypted connections (HTTPS, SSL, TLS, FTPS, etc) to protect the contents of data in transit. 4. Encrypt sensitive files prior to storing them and/or choose to encrypt the storage drive itself. 5. Use Azure Key Vault to Keep your encryption keys are separate from the data that is being protected.
Azure Key Vault helps safeguard cryptographic keys and secrets that cloud applications and services use. Key Vault streamlines the key management process and enables you to maintain control of keys that access and encrypt your data. Developers can create keys for development and testing in minutes, and then migrate them to production keys. Security administrators can grant (and revoke) permission to keys.

Estimated Efforts

1.00 Hours **Size :** Small

Impact

Optional

Help URL

https://docs.microsoft.com/en-us/azure/key-vault/key-vault-whatis

Container Assessment

Application Migration Recommendation

Container : It enables you to build and manage scalable and reliable applications composed of microservices that run at high density on a shared pool of machines, which is referred to as a cluster. It provides a sophisticated, lightweight runtime to build distributed, scalable, stateless, and stateful microservices running in containers. It also provides comprehensive application management capabilities to provision, deploy, monitor, upgrade/patch, and delete deployed applications including containerized services.

Why : This application can also move to Azure Container Service with minimal code or configuration change. Azure Container Service is costly but gives higher capability compare to Azure app service.
Cost : DS2 v2: 2 vCPUs (2 Nodes) (USD $ 367.92)
Other Option : Azure App Service and Virtual Machine

Recommendations Result

1 Day = 8 Hours

	Count	
Configuration :	9	36 Hours
Security :	6	17 Hours
Network & Availability :	0	0
Storage :	3	5 Hours

Recommendation by Size Estimate

1 Day = 8 Hours

	Count	
Small :	16	5 Days 2 Hours
Medium :	2	2 Days 0 Hours
Large :	0	0 Days

Recommendations

S1M.EventManagement

Category : Application & Platform Design **DataPoint :** AppSettingsSection

Reason for change

AppSettingsSection is used for storing sensitive information of application.

Code block	Line no.	File path
<appSettings> <add key="Email" value="gifting@s1mgift.com" /> <add key="Password" value="********" /> <add key="MailServer" value="smtp.office365.com" /> <add key="MailPort" value="587" /> <add key="IsSSLEnabled" value="true" /> <add key="EncryptionKey" value="D8215811-32B0-4276-9766-0984D6F53AD7" /> <add key="webpages:Version" value="3.0.0.0" /> <add key="webpages:Enabled" value="false" /> <add key="ClientValidationEnabled" value="true" /> <add key="UnobtrusiveJavaScriptEnabled" value="true" /> <add key="ApiPath" value="https://s1mapi.azurewebsites.net/" /> <add key="powerbi:AccessKey" value="HgnbWB2Q98MNWV+EKFNtDWNo7GiQq/b1Fx4wUN60mjk7y3Yq8rd+IwCdyTI78joPYJ1fBwRixaQnzBi4btte5A==" /> <add key="powerbi:ApiUrl" value="https://api.powerbi.com" /> <add key="powerbi:WorkspaceCollection" value="s1mws" /> <add key="powerbi:WorkspaceId" value="a4e0e2ed-5d4b-45fb-9173-a4a77dc4cba9" /> <add key="powerbi:reportId" value="59315de6-bc92-425b-985f-de37de3e6131" /> <add key="BlobStorage" value="https://s1mblob.blob.core.windows.net/s1m/" /> <add key="StorageConnectionString" value="DefaultEndpointsProtocol=https;AccountName=s1mblob;AccountKey=********" /> <add key="appURL" value="https://s1mclientapp.azurewebsites.net/?campaignid=" /> <add key="aspnet:MaxJsonDeserializerMembers" value="21407483647" /> </appSettings>	69	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\Web.config

Recommendation

AppSettingsSection uses for storing sensitive information of applications. Azure Provide **Azure KeyVault**, to securely stores sensitive information.

We are always recommended to encrypt the App Setting data. because the data we have there is highly sensitive. It must be secured.

Estimated Efforts

8.00 Hours **Size :** Medium

Impact

Optional

Help URL

https://docs.microsoft.com/en-us/dotnet/azure/dotnet-howto-migrate-app-service?view=azure-dotnet#connection-strings-and-application-settings

Category : Application & Platform Design **DataPoint :** SessionStateSection

Reason for change

InProc Mode. Change Session Mode from InProc to SQLServer or Custom

Code block	Line no.	File path
loginInfo = Session["LoginInfo"] as LoginResponse;	43	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\Areas\S1M\Controllers\CampaignSubCategoriesController.cs
loginInfo = Session["LoginInfo"] as LoginResponse;	85	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\Areas\S1M\Controllers\CampaignSubCategoriesController.cs
loginInfo = Session["LoginInfo"] as LoginResponse;	46	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\Areas\S1M\Controllers\CampaignTypeMasterController.cs
loginInfo = Session["LoginInfo"] as LoginResponse;	94	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\Areas\S1M\Controllers\CampaignTypeMasterController.cs
loginInfo = Session["LoginInfo"] as LoginResponse;	22	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\Areas\Sponsors\Controllers\SponsorsGiftController.cs

Recommendation

In Proc, Session mode will not support when the application is Scaled-Up. Use other session options to support the scalability of your application.

1- **Use OutProc Session** where Session State is stored In the StateServer and SqlServer modes.

2- **Azure Redis Cache:** Azure Redis Cache provides a session state provider that you can use to store your session state in a cache rather than in memory or in a SQL Server database. To use the caching session state provider, first, configure your cache, and then configure your ASP.NET application for the cache using the Redis Cache Session State NuGet package.

To configure a client application in Visual Studio using the Azure Cache for Redis Session State NuGet package, click NuGet Package Manager, Package Manager Console from the Tools menu.

Run the following command from the Package Manager Console window.

Install-Package Microsoft.Web.RedisSessionStateProvider

The NuGet package downloads and adds the required assembly references and adds the following section into your web. config file. This section contains the required configuration for your ASP.NET application to use the Redis Cache Session State Provider.

Configure Azure Cache for Redis settings.
Configure the attributes with the values from your cache blade in the Microsoft Azure portal, and configure the other values as desired.

Sample Code

```
<sessionState mode="Custom" customProvider="MySessionStateStore">
  <providers>
 <add name="MySessionStateStore" type="Microsoft.Web.Redis.RedisSessionStateProvider"
         host=""
         accessKey=""
         ssl="true" />
</sessionState>
```

Estimated Efforts

4.00 Hours **Size :** Small

Impact

Conditionally_Mandatory

Help URL

https://docs.microsoft.com/en-us/azure/redis-cache/cache-aspnet-session-state-provider https://docs.microsoft.com/en-us/azure/azure-cache-for-redis/cache-configure#configure-azure-cache-for-redis-settings

Category : Application & Platform Design **DataPoint :** Email

Reason for change

Mailing services is being used by your application.

Code block	Line no.	File path
SmtpClient smtp = new SmtpClient();	194	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\Areas\S1M\Controllers\ManageSponsorController.cs
SmtpClient smtp = new SmtpClient();	108	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M

	.EventManagement\Controllers\HomeController.cs

Recommendation

SendGrid is a cloud-based email service that provides reliable transnational email delivery, scalability, and real-time analytics along with flexible APIs that make custom integration easy.

Create a SendGrid Account

To sign up for a SendGrid account:

1. Log in to the Azure portal.
2. In the menu on the left, click Create a resource.
3. Click Add-ons and then SendGrid Email Delivery.
4. Complete the signup form and select Create.
5. Enter a Name to identify your SendGrid service in your Azure settings. Names must be between 1 and 100 characters in length and contain only alphanumeric characters, dashes, dots, and underscores. The name must be unique in your list of subscribed Azure Store Items.
6. Enter and confirm your Password.
7. Choose your Subscription.
8. Create a new Resource group or use an existing one.
9. In the Pricing tier section select the SendGrid plan you want to sign up for.
10. Enter a Promotion Code if you have one.
11. Enter your Contact Information.
12. Review and accept the Legal terms.
13. After confirming your purchase you will see a Deployment Succeeded pop-up and you will see your account listed in the All resources section.

After you have completed your purchase and clicked the Manage button to initiate the email verification process, you will receive an email from SendGrid asking you to verify your account.

To send an email using SendGrid, you must supply your API Key.

To find your SendGrid API Key:

1. Click Manage.
2. In your SendGrid dashboard, select Settings and then API Keys in the menu on the left.
3. Click the Create API Key.
4. At a minimum, provide the name of this key and provide full access to Mail Send and select Save.
5. Your API will be displayed at this point at one time. Please be sure to store it safely.

How to: Send an Email

After creating an email message, you can send it using SendGrid's API. Alternatively, you may use. NET's built-in library.

Sending email requires that you supply your SendGrid API Key.

var apiKey = System.Environment.GetEnvironmentVariable("SENDGRID_APIKEY");
var client = new SendGridClient(apiKey);

The sample code shows how to send an email message using the SendGrid Web API with a console application.

Sample Code

```
using System;
using System.Threading.Tasks;
using SendGrid;
using SendGrid.Helpers.Mail;

namespace Example
{
    internal class Example
    {
        private static void Main()
        {
            Execute().Wait();
        }
        static async Task Execute()
        {
            var apiKey = System.Environment.GetEnvironmentVariable("SENDGRID_APIKEY");
            var client = new SendGridClient(apiKey);
            var msg = new SendGridMessage()
            {
                From = new EmailAddress("test@example.com", "DX Team"),
                Subject = "Hello World from the SendGrid CSharp SDK!",
                PlainTextContent = "Hello, Email!",
                HtmlContent = "Hello, Email!"
            };
            msg.AddTo(new EmailAddress("test@example.com", "Test User"));
            var response = await client.SendEmailAsync(msg);
        }
    }
}
```

Estimated Efforts

2.00 Hours **Size :** Small

Impact

Optional

Help URL

http://azure.microsoft.com/en-in/documentation/articles/sendgrid-dotnet-how-to-send-email/

Category : Application & Platform Design **DataPoint :** Hard Coded URL

Reason for change

The Application uses Hard Coded Urls. These URLs may not be accessible after deployment in Azure Container.

Code block	Line no.	File path
<script src="https://maps.googleapis.com/maps/api/js?AIzaSyCI2RZXFqqoJI-kUwwzY6GwWrn6GEzdWx8=&libraries=places&callback=initAutocomplete" async defer></script>	10	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\obj\Release\Package\PackageTmp\Areas\Sponsors\Views\Sponsor\OfferEntry.cshtml
@*<link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.4.0/css/font-awesome.min.css">	7	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\obj\Release\Package\PackageTmp\Areas\Sponsors\Views\SponsorsGift\Index.cshtml
<script src="http://ajax.aspnetcdn.com/ajax/jQuery/jquery-2.0.3.min.js"></script>*@	8	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\obj\Release\Package\PackageTmp\Areas\S1M\Views\Campaign\CampaignList.cshtml

<a href="#x" class="thumbnail"><img src="http://placehold.it/250x250" alt="Image" class="img-responsive"></a>	51, 52, 53, 54, 57, 58, 59, 60	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\obj\Release\Package\PackageTmp\Areas\S1M\Views\Campaign\CampaignList.cshtml
@*<div class="col-xs-6 "><img src="https://s1m.blob.core.windows.net/s1m/f4d16505-9339-4df5-b3ac-0b5f89fb0364" /></div>	389	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\obj\Release\Package\PackageTmp\Areas\S1M\Views\Campaign\SponsorEntry.cshtml

Recommendation

External or In-House application URL or API is being called in your code. Make sure wherein connectivity with requested URL.

If these URLs are part of the application (Web Service/WCF Services/Web API) then also host these services on different Containers based on Binding and Application Requirement and update the URL on the application.

Estimated Efforts

2.00 Hours **Size :** Small

Impact

Conditionally_Mandatory

Help URL

https://docs.microsoft.com/en-us/azure/app-service/environment/app-service-web-how-to-create-a-web-app-in-an-ase

Category : Security **DataPoint :** Connection Strings Section

Reason for change

ConnectionStringSection is use for storing database connectivity credential.It is very sensitive information of application.

Code block	Line no.	File path
<add name="defaultcon***	11	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\obj\Release\TransformWebConfig\transformed\Web.config
<add name="s1mmarketi***	17	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\obj\Release\TransformWebConfig\transformed\Web.config
<add name="defaultcon***	11	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\obj\Release\CSAutoParameterize\original\Web.config
<add	17	D:\Project\S1mAdminPanel\S1mA

name="s1mmarketi**		dminPanel-kendo_15-09-2016\S1M.EventManagement\obj\Release\CSAutoParameterize\original\Web.config
<add name="defaultcon**	11	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\obj\Release\TransformWebConfig\original\Web.config

Recommendation

ConnectionStringSection uses for storing database connectivity credentials. It is very sensitive information about the application.

Azure Provide **Azure KeyVault**, to securely stores sensitive information of the application. So use that to store connection strings.

We are always recommended to encrypt the connection string of your application because the data we have there is highly sensitive. It must be secured.

Please find the following steps to encrypt the web. config.

1-Open Command Prompt with Administrator privileges
2-At the Command Prompt, enter
3-cd C:\Windows\Microsoft.NET\Framework\v4.0.30319
4-In case your web Config is located in "D:\Articles\EncryptWebConfig" directory path, then enter the following to encrypt the ConnectionString:

ASPNET_REGIIS -pef "connectionStrings" "D:\Articles\EncryptWebConfig

Sample Code

```
<configuration>
<connectionStrings
configProtectionProvider="RsaProtectedConfigurationProvider">
<EncryptedData Type="http://www.w3.org/2001/04/xmlenc#Element"
xmlns="http://www.w3.org/2001/04/xmlenc#">
<EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc">
<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
<EncryptedKey xmlns="http://www.w3.org/2001/04/xmlenc#">
<EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5" />
<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
<KeyName> RSA Key </KeyName>
 </KeyInfo>
 <CipherData>
 <CipherValue>
 WcFEbDX8VyLfAsVK8g6hZVAG1674ZFc1kWH0BoazgOwdBfinhcAmQmnIn0oHtZ5tO2EXGl+dyh10giEmO9NemH4Y
Zk+iMIln+ItcEay9CGWMXSen9UQLpcQHQqMJErZiPK4qPZaRWwqckLqriCl9X8x9OE7jKIsO2Ibapwj+1Jo=
 </CipherValue>
 </CipherData>
 </EncryptedKey>
 </KeyInfo>
 <CipherData>
 <CipherValue>
OpWQgQbq2wBZEGYAeV8WF82yz6q5WNFIj3rcuQ8gT0MP97aO9SHIZWwNggSEi2Ywi4omKOGA4mjqT0VZaXgb9tVeG
BDhjPh 5ZlrLMNfYSozeJ
m2Lsm7hnF6VvFm3fFMXa6+h0JTHeCXBdmzg/vQb0u3oejSGzB4ly+V9O0T4Yxkwn9KVDW58PHOeRT2//3iZfJ
WV2NZ4e6vj4Byjf81o3JVNgRjmm9hr9blVbbT3Q8/j5zJ+TElCn6zPHvnuB70iG2KPJXqAj2GBzBk6cHq+WNebOQN
WIb7dTPumuZ K0yW1XDZ5gkfBuqgn8hm osTE7mCvieP9rgATf6qgLgdA6zYyVV6WDjo1qbCV807lczxa3bF5KzKa
VUSq5FS1SpdZKAE6/kkr0Ps++CE=
 </CipherValue>
```

```
  </CipherData>
</EncryptedData>
  </connectionStrings>
  </configuration>
```

Estimated Efforts

2.00 Hours **Size :** Small

Impact

Conditionally_Mandatory

Help URL

https://www.c-sharpcorner.com/article/encrypt-and-decrypt-connectionstring-in-web-config-file/

Category : Storage DataPoint : DB Connections

Reason for change

Database Connections might not work properly in Azure.

Code block	Line no.	File path
<add name="defaultcon***	11	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\obj\Release\TransformWebConfig\transformed\Web.config
<add name="s1mmarketi**	17	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\obj\Release\TransformWebConfig\transformed\Web.config
<add name="defaultcon***	11	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\obj\Release\CSAutoParameterize\original\Web.config
<add name="s1mmarketi**	17	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\obj\Release\CSAutoParameterize\original\Web.config
<add name="defaultcon***	11	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\obj\Release\TransformWebConfig\original\Web.config

Recommendation

Your current on-premises solutions for Database Connectivity are unlikely to work in Azure.
Make sure Database Connectivity is available for application.

Or

Azure has the following options for migrating databases.
1-SQL Server on Azure VMs
2-Azure SQL Database
3-Azure SQL Managed Instance
After migration, change your Database Connectivity to the Target platform.

Estimated Efforts

2.00 Hours **Size :** Small

Impact

Optional

Help URL

https://docs.microsoft.com/en-us/azure/service-fabric/service-fabric-host-app-in-a-container

Category : Security **DataPoint :** Encryption

Reason for change

The Application uses Encryption. These Encryption Algorithm may or may not be work in Container.

Code block	Line no.	File path
using (Aes encryptor = Aes.Create())	25	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\helperClass\Cryptography.cs
using (Aes encryptor = Aes.Create())	59	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\helperClass\Cryptography.cs

Recommendation

Applications use encryption(cryptographic) keys and secrets to help keep information secure. Azure Key Vault safeguards these keys and secrets. When you use Key Vault, you can encrypt authentication keys, storage account keys, data encryption keys, .pfx files, and passwords by using keys that are protected by hardware security modules (HSMs).

Azure web application to read information from Azure Key Vault by using managed identities for Azure resources.
Below are steps How to use Azure Key Vault.

- Create a key vault.
- Store a secret in the key vault.
- Retrieve a secret from the key vault.
- Enable a managed service identity for the web app.
- Grant the required permissions for the web application to read data from the key vault.

For further assistance refer to the Help Url.

Estimated Efforts

4.00 Hours **Size :** Small

Impact

Conditionally_Mandatory

Help URL

https://docs.microsoft.com/en-us/azure/key-vault/key-vault-whatis

S1M.BAL

Category : Application & Platform Design **DataPoint :** SessionStateSection

Reason for change

InProc Mode. Change Session Mode from InProc to SQLServer or Custom

Code block	Line no.	File path
LoginResponse sessionValue = HttpContext.Current.Session["LoginInfo"] as LoginResponse;	19	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.BAL\AssetMappingBL.cs

Recommendation

In Proc, Session mode will not support when the application is Scaled-Up. Use other session options to support the scalability of your application.

1- **Use OutProc Session** where Session State is stored In the StateServer and SqlServer modes.

2- **Azure Redis Cache:** Azure Redis Cache provides a session state provider that you can use to store your session state in a cache rather than in memory or in a SQL Server database. To use the caching session state provider, first, configure your cache, and then configure your ASP.NET application for the cache using the Redis Cache Session State NuGet package.

To configure a client application in Visual Studio using the Azure Cache for Redis Session State NuGet package, click NuGet Package Manager, Package Manager Console from the Tools menu.

Run the following command from the Package Manager Console window.

Install-Package Microsoft.Web.RedisSessionStateProvider

The NuGet package downloads and adds the required assembly references and adds the following section into your web.config file. This section contains the required configuration for your ASP.NET application to use the Redis Cache Session State Provider.

Configure Azure Cache for Redis settings.
Configure the attributes with the values from your cache blade in the Microsoft Azure portal, and configure the other values as desired.

Sample Code

```
<sessionState mode="Custom" customProvider="MySessionStateStore">
  <providers>
 <add name="MySessionStateStore" type="Microsoft.Web.Redis.RedisSessionStateProvider"
         host=""
         accessKey=""
         ssl="true" />
</sessionState>
```

Estimated Efforts

4.00 Hours **Size :** Small

Impact

Conditionally_Mandatory

Help URL

https://docs.microsoft.com/en-us/azure/redis-cache/cache-aspnet-session-state-provider https://docs.microsoft.com/en-us/azure/azure-cache-for-redis/cache-configure#configure-azure-cache-for-redis-settings

S1M.DAL

Category : Security **DataPoint :** Connection Strings Section

Reason for change

ConnectionStringSection is use for storing database connectivity credential.It is very sensitive information of application.

Code block	Line no.	File path
<add name="s1mmarketi** *** ****	7	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.DAL\App.Config

Recommendation

ConnectionStringSection uses for storing database connectivity credentials. It is very sensitive information about the application.

Azure Provide **Azure KeyVault**, to securely stores sensitive information of the application. So use that to store connection strings.

We are always recommended to encrypt the connection string of your application because the data we have there is highly sensitive. It must be secured.

Please find the following steps to encrypt the web. config.

1-Open Command Prompt with Administrator privileges
2-At the Command Prompt, enter
3-cd C:\Windows\Microsoft.NET\Framework\v4.0.30319
4-In case your web Config is located in "D:\Articles\EncryptWebConfig" directory path, then enter the following to encrypt the ConnectionString:

ASPNET_REGIIS -pef "connectionStrings" "D:\Articles\EncryptWebConfig

Sample Code

```
<configuration>
<connectionStrings
configProtectionProvider="RsaProtectedConfigurationProvider">
<EncryptedData Type="http://www.w3.org/2001/04/xmlenc#Element"
xmlns="http://www.w3.org/2001/04/xmlenc#">
<EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc">
<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
<EncryptedKey xmlns="http://www.w3.org/2001/04/xmlenc#">
<EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5" />
<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
<KeyName> RSA Key </KeyName>
 </KeyInfo>
 <CipherData>
 <CipherValue>
 WcFEbDX8VyLfAsVK8g6hZVAG1674ZFc1kWH0BoazgOwdBfinhcAmQmnIn0oHtZ5tO2EXGl+dyh10giEmO9NemH4Y
```

```
Zk+iMIln+ItcEay9CGWMXSen9UQLpcQHQqMJErZiPK4qPZaRWwqckLqriCl9X8x9OE7jKIsO2Ibapwj+1Jo=
 </CipherValue>
 </CipherData>
 </EncryptedKey>
 </KeyInfo>
 <CipherData>
 <CipherValue>
OpWQgQbq2wBZEGYAeV8WF82yz6q5WNFIj3rcuQ8gT0MP97aO9SHIZWwNggSEi2Ywi4omKOGA4mjqT0VZaXgb9tVeG
BDhjPh 5ZlrLMNfYSozeJ
m2Lsm7hnF6VvFm3fFMXa6+h0JTHeCXBdmzg/vQb0u3oejSGzB4ly+V9O0T4Yxkwn9KVDW58PHOeRT2//3iZfJ
WV2NZ4e6vj4Byjf81o3JVNgRjmm9hr9blVbbT3Q8/j5zJ+TElCn6zPHvnuB70iG2KPJXqAj2GBzBk6cHq+WNebOQN
WIb7dTPumuZ K0yW1XDZ5gkfBuqgn8hm osTE7mCvieP9rgATf6qgLgdA6zYyVV6WDjo1qbCV807lczxa3bF5KzKa
VUSq5FS1SpdZKAE6/kkr0Ps++CE=
 </CipherValue>
 </CipherData>
</EncryptedData>
 </connectionStrings>
 </configuration>
```

Estimated Efforts

2.00 Hours **Size :** Small

Impact

Conditionally_Mandatory

Help URL

https://www.c-sharpcorner.com/article/encrypt-and-decrypt-connectionstring-in-web-config-file/

Category : Storage **DataPoint :** DB Connections

Reason for change

Database Connections might not work properly in Azure.

Code block	Line no.	File path
<add name="s1mmarketi**	7	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.DAL\App.Config

Recommendation

Your current on-premises solutions for Database Connectivity are unlikely to work in Azure.
Make sure Database Connectivity is available for application.

Or

Azure has the following options for migrating databases.
1-SQL Server on Azure VMs
2-Azure SQL Database
3-Azure SQL Managed Instance
After migration, change your Database Connectivity to the Target platform.

Estimated Efforts

2.00 Hours **Size :** Small

Impact

Optional

Help URL

https://docs.microsoft.com/en-us/azure/service-fabric/service-fabric-host-app-in-a-container

S1M.DTO

Questionnaire Result

Category : Application & Platform Design **DataPoint :** GAC Dependency

Reason for change

GAC dependency might not work properly in Azure Container Service.

Recommendation

Application deployed to Azure container service then verify the assemblies are working properly or not, if not then-

1. Install an assembly into the global assembly cache(GAC).

2. Move Assemblies to the BIN folder.

Estimated Efforts

4.00 Hours **Size :** Small

Impact

Optional

Help URL

https://docs.microsoft.com/en-us/dotnet/framework/app-domains/how-to-install-an-assembly-into-the-gac

Category : Application & Platform Design **DataPoint :** Background Processing

Reason for change

Background Processing might not work properly in Azure Container Service.

Recommendation

Containers can be useful for running background jobs. Some of the benefits include:

- Containers support high-density hosting. You can isolate a background task in a container while placing multiple containers in each VM.
- The container orchestrator handles internal load balancing, configuring the internal network, and other configuration tasks. Containers can be started and stopped as needed.

- Azure Container Registry allows you to register your containers inside Azure boundaries. This comes with security, privacy, and proximity benefits.

Estimated Efforts

2.00 Hours **Size :** Small

Impact

Optional

Help URL

https://docs.microsoft.com/en-us/dotnet/standard/microservices-architecture/multi-container-microservice-net-applications/background-tasks-with-ihostedservice

Category : Storage **DataPoint :** Automatic Backup

Reason for change

Automatic Backup is used to minimize the risk of data loss and get backup automatic as per interval.

Recommendation

AKS does not offer a financially backed service level agreement. We will strive to attain at least 99.5% availability for the Kubernetes API server. The availability of the agent nodes in your cluster is covered by the Virtual Machines SLA.

Using the Azure Backup service we can schedule the backup of the VM as per requirement.

Steps to configure a backup of Azure VM

1. Configure the backup job from the VM operations menu.
2. Configure the backup job from the Recovery Services vault
3. Create a recovery services vault for a VM
4. Select a backup goal, set policy, and define items to protect
5. Initial backup
6. Defining a backup policy
7. Install the VM Agent on the virtual machine

For further details refer to the below Help Url.

Estimated Efforts

1.00 Hours **Size :** Small

Impact

Optional

Help URL

https://docs.microsoft.com/en-us/azure/backup/backup-azure-vms-first-look-arm

Category : Security **DataPoint :** Firewall

Reason for change

Firewall configured in On-premise environment might not be accessible in Azure environment

Recommendation

There are two options to configure the firewall in azure-
1. Move existing firewall service to azure.
2. Configure Network Security Group(NSG) and Azure Firewall in Azure for the application.

Step to configure NSG in Azure

1. Create a network security group.
2. Create an inbound security rule. Add rules for the application.
3. Associate your network security group with a subnet.

Estimated Efforts

4.00 Hours **Size :** Small

Impact

Optional

Help URL

https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-filter-network-traffic#create-a-network-security-group

Category : Security **DataPoint :** Secure Socket Layer (SSL)

Reason for change

Application defined some Secure Socket Layer(SSL) related settings.

Recommendation

Bind SSL certificate to Azure Web Apps

How to Configure

1. Log in to the Azure portal.
2. Navigate to App Services in the left navigation pane.
3. Select your web application.
4. Click on Settings and select Custom domains and SSL.
5. A new frame will open on the right side. Click on Bring external domains.
6. Note the IP address located at the bottom. Go to your domain registrar website and create DNS entries using this IP address. It can take some time for the changes to propagate, depending on your DNS provider.
7. In the Domain Names text box, enter the custom domain name you bought from the domain registrar.
8. Save the changes.
9. Click on the Upload certificate.
10. Locate and upload your .pfx certificate file.
11. Under SSL bindings, select the domain name to secure with SSL, and the certificate to use.
12. Save the changes.
13. You should be able to access the web app using your custom domain name over HTTPS.

Estimated Efforts

4.00 Hours **Size :** Small

Impact

Conditionally_Mandatory

Help URL

https://docs.microsoft.com/en-us/azure/cloud-services/cloud-services-configure-ssl-certificate-portal

Category : Application & Platform Design **DataPoint :** Com Import

Reason for change

Application using some COM+ Component that may or may not work properly

Recommendation

Application using some COM+ Component.

Follow the below steps to configure.

1. If You are using COM+ Component as an assembly, then Right click on assembly.
2. Select Property from Menu.
3. Select Copy to Output directory-> Copy Always.
4. If You are using COM Component as an exe, then You need to create a startup script.
5. Create PowerShell script for COM+ Component.
6. Add Folder Startup in your Role.
7. Add All related files in the Startup folder.
8. Configure the startup task in your Service Definition file.

Estimated Efforts

2.00 Hours **Size :** Small

Impact

Optional

Help URL

https://stackoverflow.com/questions/14981830/asppdf-and-aspjpeg-on-windows-azure

Category : Security **DataPoint :** PII Information

Reason for change

Your application is storing or sharing PII Informations.

Recommendation

1. Use industry-standard AES encryption. 2. Use dual control and separation of duties to protect your encryption keys. 3. Encrypt sensitive data prior to moving and/or use encrypted connections (HTTPS, SSL, TLS, FTPS, etc) to protect the contents of data in transit. 4. Encrypt sensitive files prior to storing them and/or choose to encrypt the storage drive itself. 5. Use Azure Key Vault to Keep your encryption keys are separate from the data that is being protected.
Azure Key Vault helps safeguard cryptographic keys and secrets that cloud applications and services use. Key Vault streamlines the key management process and enables you to maintain control of keys that access and encrypt your data. Developers can create keys for development and testing in minutes, and then migrate them to production keys. Security administrators can grant (and revoke) permission to keys.

Estimated Efforts

1.00 Hours **Size :** Small

Impact

Optional

Help URL

https://docs.microsoft.com/en-us/azure/key-vault/key-vault-whatis

Container Basic Settings

Category : Application & Platform Design **DataPoint :** AppContainerization

Reason for change

Container need images for deploying the application

Recommendation

.NET Framework applications can host on Azure Kubernetes Service by creating windows containers without porting to .NET Core.

Steps for build image of application.

- Create a docker file. Docker file do not have any extension.
- Open docker file in any editor. Clear everything, if any, inside docker file.
- Write the following contents in docker file.

  ```
  FROM Microsoft/aspnet

  COPY yourPublishFolder/ /inetpub/wwwroot
  ```

- Save the file.
- Open Windows PowerShell (not Windows PowerShell ISE) and change the path to location of your publish folder. Then run the following commands :

  ```
  docker build –t randomname

  docker run –d --name webappname randomname
  ```

- The image will be created after the above process completes.
- Create an Azure Container Registry in https://portal.azure.com/.
- Push the created image to Azure Container Registry. Login to Azure portal in Windows PowerShell by running following command.

  ```
  az login –u username –p password
  ```

- Tag your image.

  ```
  docker tag randomname myregistry.azurecr.io/sample
  ```

- Push image to your registry.

  ```
  docker push myregistry.azurecr.io/sample
  ```

- Use the loginserver, username and password from Azure portal to pull the image.

Estimated Efforts

8.00 Hours **Size :** Medium

Impact

Mandatory

Help URL

https://docs.microsoft.com/en-us/aspnet/mvc/overview/deployment/docker-aspnetmvc

Virtual Machine Assessment

Application Migration Recommendation

Azure Windows Virtual Machines provides on-demand, high-scale, secure, virtualized infrastructure using Windows Server.More Info...
Why : This application can also move on Azure Virtual Machine with minimal code change. As compare to Azure app service & container service, you can have more control over the Azure Virtual Machine but you need to manage everything including your application & infrastructure.
Cost : DS2 v2 (USD $ 184.46)
Other Option : Azure App Service and Azure Container Service.

Recommendations Result

1 Day = 8 Hours

	Count	
Configuration :	8	28 Hours
Security :	6	17 Hours
Network & Availability :	0	0
Storage :	3	5 Hours

Recommendation by Size Estimate

1 Day = 8 Hours

	Count	
Small :	16	5 Days 2 Hours
Medium :	1	1 Days 0 Hours
Large :	0	0 Days

Recommendations

S1M.EventManagement

Category : Application & Platform Design **DataPoint :** AppSettingsSection

Reason for change

AppSettingsSection is used for storing sensitive information of application.

Code block	Line no.	File path
<appSettings> <add key="Email" value="gifting@s1mgift.com" /> <add	69	D:\Project\S1mAdminPanel\S1mA

key="Password" value="********" /> <add key="MailServer" value="smtp.office365.com" /> <add key="MailPort" value="587" /> <add key="IsSSLEnabled" value="true" /> <add key="EncryptionKey" value="D8215811-32B0-4276-9766-0984D6F53AD7" /> <add key="webpages:Version" value="3.0.0.0" /> <add key="webpages:Enabled" value="false" /> <add key="ClientValidationEnabled" value="true" /> <add key="UnobtrusiveJavaScriptEnabled" value="true" /> <add key="ApiPath" value="https://s1mapi.azurewebsites.net/" /> <add key="powerbi:AccessKey" value="HgnbWB2Q98MNWV+EKFNtDWNo7GiQq/b1Fx4wUN60mjk7y3Yq8rd+IwCdyTI78joPYJ1fBwRixaQnzBi4btte5A==" /> <add key="powerbi:ApiUrl" value="https://api.powerbi.com" /> <add key="powerbi:WorkspaceCollection" value="s1mws" /> <add key="powerbi:WorkspaceId" value="a4e0e2ed-5d4b-45fb-9173-a4a77dc4cba9" /> <add key="powerbi:reportId" value="59315de6-bc92-425b-985f-de37de3e6131" /> <add key="BlobStorage" value="https://s1mblob.blob.core.windows.net/s1m/" /> <add key="StorageConnectionString" value="DefaultEndpointsProtocol=https;AccountName=s1mblob;AccountKey=********" /> <add key="appURL" value="https://s1mclientapp.azurewebsites.net/?campaignid=" /> <add key="aspnet:MaxJsonDeserializerMembers" value="21407483647" /> </appSettings>		dminPanel-kendo_15-09-2016\S1M.EventManagement\Web.config

Recommendation

AppSettingsSection uses for storing sensitive information of applications. Azure Provide **Azure KeyVault**, to securely stores sensitive information.

We are always recommended to encrypt the App Setting data. because the data we have there is highly sensitive. It must be secured.

Estimated Efforts

8.00 Hours **Size :** Medium

Impact

Optional

Help URL

https://docs.microsoft.com/en-us/dotnet/azure/dotnet-howto-migrate-app-service?view=azure-dotnet#connection-strings-and-application-settings

Category : Application & Platform Design **DataPoint :** SessionStateSection

Reason for change

In Proc, Session mode will not support when you scale up your Application.

Code block	Line no.	File path
loginInfo = Session["LoginInfo"] as LoginResponse;	43	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\Areas\S1M\Controllers\CampaignSubCategoriesController.cs

loginInfo = Session["LoginInfo"] as LoginResponse;	85	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\Areas\S1M\Controllers\CampaignSubCategoriesController.cs
loginInfo = Session["LoginInfo"] as LoginResponse;	46	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\Areas\S1M\Controllers\CampaignTypeMasterController.cs
loginInfo = Session["LoginInfo"] as LoginResponse;	94	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\Areas\S1M\Controllers\CampaignTypeMasterController.cs
loginInfo = Session["LoginInfo"] as LoginResponse;	22	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\Areas\Sponsors\Controllers\SponsorsGiftController.cs

Recommendation

In Proc, Session mode will not support when the application is Scaled-Up. Use other session options to support the scalability of your application.

1- **Use OutProc Session** where Session State is stored In the StateServer and SqlServer modes.

2- Azure Redis Cache: Azure Redis Cache provides a session state provider that you can use to store your session state in a cache rather than in memory or in a SQL Server database. To use the caching session state provider, first, configure your cache, and then configure your ASP.NET application for the cache using the Redis Cache Session State NuGet package.

To configure a client application in Visual Studio using the Azure Cache for Redis Session State NuGet package, click NuGet Package Manager, Package Manager Console from the Tools menu.

Run the following command from the Package Manager Console window.

Install-Package Microsoft.Web.RedisSessionStateProvider

The NuGet package downloads and adds the required assembly references and adds the following section into your web.config file. This section contains the required configuration for your ASP.NET application to use the Redis Cache Session State Provider.

Configure Azure Cache for Redis settings.
Configure the attributes with the values from your cache blade in the Microsoft Azure portal, and configure the other values as desired.

Sample Code

```
<sessionState mode="Custom" customProvider="MySessionStateStore">
  <providers>
 <add name="MySessionStateStore" type="Microsoft.Web.Redis.RedisSessionStateProvider"
         host=""
         accessKey=""
         ssl="true" />
</sessionState>
```

Estimated Efforts

4.00 Hours **Size :** Small

Impact

Conditionally_Mandatory

Help URL

https://docs.microsoft.com/en-us/azure/redis-cache/cache-aspnet-session-state-provider https://docs.microsoft.com/en-us/azure/azure-cache-for-redis/cache-configure#configure-azure-cache-for-redis-settings

Category : Application & Platform Design **DataPoint :** Email

Reason for change

Mailing services is being used by your application.

Code block	Line no.	File path
SmtpClient smtp = new SmtpClient();	194	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\Areas\S1M\Controllers\ManageSponsorController.cs
SmtpClient smtp = new SmtpClient();	108	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\Controllers\HomeController.cs

Recommendation

If you have a secure SMTP relay service that's running on-premises that you can use it.

SendGrid is a cloud-based email service that provides reliable transnational email delivery, scalability, and real-time analytics along with flexible APIs that make custom integration easy.

Create a SendGrid Account

To sign up for a SendGrid account:

1. Log in to the Azure portal.
2. In the menu on the left, click Create a resource.
3. Click Add-ons and then SendGrid Email Delivery.
4. Complete the signup form and select Create.
5. Enter a Name to identify your SendGrid service in your Azure settings. Names must be between 1 and 100 characters in length and contain only alphanumeric characters, dashes, dots, and underscores. The name must be unique in your list of subscribed Azure Store Items.
6. Enter and confirm your Password.
7. Choose your Subscription.
8. Create a new Resource group or use an existing one.
9. In the Pricing tier section select the SendGrid plan you want to sign up for.
10. Enter a Promotion Code if you have one.
11. Enter your Contact Information.
12. Review and accept the Legal terms.
13. After confirming your purchase you will see a Deployment Succeeded pop-up and you will see your account listed in the All resources section.

After you have completed your purchase and clicked the Manage button to initiate the email verification process, you will receive an email from SendGrid asking you to verify your account.

To send an email using SendGrid, you must supply your API Key.

To find your SendGrid API Key:

1. Click Manage.
2. In your SendGrid dashboard, select Settings and then API Keys in the menu on the left.
3. Click the Create API Key.
4. At a minimum, provide the name of this key and provide full access to Mail Send and select Save.
5. Your API will be displayed at this point one time. Please be sure to store it safely.

How to: Send an Email

After creating an email message, you can send it using SendGrid's API. Alternatively, you may use. NET's built-in library.

Sending email requires that you supply your SendGrid API Key.

var apiKey = System.Environment.GetEnvironmentVariable("SENDGRID_APIKEY");
var client = new SendGridClient(apiKey);

The sample code shows how to send an email message using the SendGrid Web API with a console application.

Sample Code

```
using System;
using System.Threading.Tasks;
using SendGrid;
using SendGrid.Helpers.Mail;

namespace Example
{
    internal class Example
    {
        private static void Main()
        {
            Execute().Wait();
        }

        static async Task Execute()
        {
            var apiKey = System.Environment.GetEnvironmentVariable("SENDGRID_APIKEY");
            var client = new SendGridClient(apiKey);
            var msg = new SendGridMessage()
            {
                From = new EmailAddress("test@example.com", "DX Team"),
                Subject = "Hello World from the SendGrid CSharp SDK!",
                PlainTextContent = "Hello, Email!",
                HtmlContent = "Hello, Email!"
            };
            msg.AddTo(new EmailAddress("test@example.com", "Test User"));
            var response = await client.SendEmailAsync(msg);
        }
    }
}
```

Estimated Efforts

2.00 Hours **Size :** Small

Impact

Optional

Help URL

http://azure.microsoft.com/en-in/documentation/articles/sendgrid-dotnet-how-to-send-email/

Category : Application & Platform Design **DataPoint :** Hard Coded URL

Reason for change

The Application uses Hard Coded Urls. These URLs may not be accessible after deployment in Azure Virtual Machine.

Code block	Line no.	File path
<script src="https://maps.googleapis.com/maps/api/js?AIzaSyCI2RZXFqqoJI-kUwwzY6GwWrn6GEzdWx8=&libraries=places&callback=initAutocomplete" async defer></script>	10	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\obj\Release\Package\PackageTmp\Areas\Sponsors\Views\Sponsor\OfferEntry.cshtml
@*<link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.4.0/css/font-awesome.min.css">	7	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\obj\Release\Package\PackageTmp\Areas\Sponsors\Views\SponsorsGift\Index.cshtml
<script src="http://ajax.aspnetcdn.com/ajax/jQuery/jquery-2.0.3.min.js"></script>*@	8	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\obj\Release\Package\PackageTmp\Areas\S1M\Views\Campaign\CampaignList.cshtml
<a href="#x" class="thumbnail"><img src="http://placehold.it/250x250" alt="Image" class="img-responsive"></a>	51, 52, 53, 54, 57, 58, 59, 60	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\obj\Release\Package\PackageTmp\Areas\S1M\Views\Campaign\CampaignList.cshtml
@*<div class="col-xs-6 "><img src="https://s1m.blob.core.windows.net/s1m/f4d16505-9339-4df5-b3ac-0b5f89fb0364" /></div>	389	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\obj\Release\Package\PackageTmp\Areas\S1M\Views\Campaign\SponsorEntry.cshtml

Recommendation

External or In-House application URL or API is being called in your code. Make sure about connectivity with the requested URL.

If these URLs are part of the application (Web Service/WCF Services/Web API) then also host these services on the same Virtual machine or another VM as per requirement, based on service binding and requirement, and update the URL on the application.

Estimated Efforts

2.00 Hours **Size :** Small

Impact

Conditionally_Mandatory

Help URL

https://docs.microsoft.com/en-us/azure/app-service/environment/app-service-web-how-to-create-a-web-app-in-an-ase

Category : Security **DataPoint :** Connection Strings Section

Reason for change

ConnectionStringSection is use for storing database connectivity credential.It is very sensitive information of application.

Code block	Line no.	File path
<add name="defaultcon***	11	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\obj\Release\TransformWebConfig\transformed\Web.config
<add name="s1mmarketi**	17	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\obj\Release\TransformWebConfig\transformed\Web.config
<add name="defaultcon***	11	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\obj\Release\CSAutoParameterize\original\Web.config
<add name="s1mmarketi**	17	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\obj\Release\CSAutoParameterize\original\Web.config
<add name="defaultcon***	11	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\obj\Release\TransformWebConfig\original\Web.config

Recommendation

ConnectionStringSection uses for storing database connectivity credentials. It is very sensitive information about the application.

Azure Provide **Azure KeyVault**, to securely stores sensitive information of the application. So use that to store connection strings.

We are always recommended to encrypt the connection string of your application because the data we have there is highly sensitive. It must be secured.

Please find the following steps to encrypt the web. config.

1-Open Command Prompt with Administrator privileges
2-At the Command Prompt, enter
3-cd C:\Windows\Microsoft.NET\Framework\v4.0.30319
4-In case your web Config is located in "D:\Articles\EncryptWebConfig" directory path, then enter the following to encrypt the ConnectionString:

ASPNET_REGIIS -pef "connectionStrings" "D:\Articles\EncryptWebConfig

Sample Code

```
<configuration>
<connectionStrings
configProtectionProvider="RsaProtectedConfigurationProvider">
<EncryptedData Type="http://www.w3.org/2001/04/xmlenc#Element"
```

```
xmlns="http://www.w3.org/2001/04/xmlenc#">
<EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc">
<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
<EncryptedKey xmlns="http://www.w3.org/2001/04/xmlenc#">
<EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5" />
<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
<KeyName> RSA Key </KeyName>
 </KeyInfo>
 <CipherData>
 <CipherValue>
 WcFEbDX8VyLfAsVK8g6hZVAG1674ZFc1kWH0BoazgOwdBfinhcAmQmnIn0oHtZ5tO2EXGl+dyh10giEmO9NemH4Y
Zk+iMIln+ItcEay9CGWMXSen9UQLpcQHQqMJErZiPK4qPZaRWwqckLqriCl9X8x9OE7jKIsO2Ibapwj+1Jo=
 </CipherValue>
 </CipherData>
 </EncryptedKey>
 </KeyInfo>
 <CipherData>
 <CipherValue>
OpWQgQbq2wBZEGYAeV8WF82yz6q5WNFIj3rcuQ8gT0MP97aO9SHIZWwNggSEi2Ywi4omKOGA4mjqT0VZaXgb9tVeG
BDhjPh 5ZlrLMNfYSozeJ
m2Lsm7hnF6VvFm3fFMXa6+h0JTHeCXBdmzg/vQb0u3oejSGzB4ly+V9O0T4Yxkwn9KVDW58PHOeRT2//3iZfJ
WV2NZ4e6vj4Byjf81o3JVNgRjmm9hr9blVbbT3Q8/j5zJ+TElCn6zPHvnuB70iG2KPJXqAj2GBzBk6cHq+WNebOQN
WIb7dTPumuZ K0yW1XDZ5gkfBuqgn8hm osTE7mCvieP9rgATf6qgLgdA6zYyVV6WDjo1qbCV807lczxa3bF5KzKa
VUSq5FS1SpdZKAE6/kkr0Ps++CE=
 </CipherValue>
 </CipherData>
</EncryptedData>
 </connectionStrings>
 </configuration>
```

Estimated Efforts

2.00 Hours **Size :** Small

Impact

Conditionally_Mandatory

Help URL

https://www.c-sharpcorner.com/article/encrypt-and-decrypt-connectionstring-in-web-config-file/

Category : Storage **DataPoint :** DB Connections

Reason for change

Database Connections might not work properly in Azure.

Code block	Line no.	File path
<add name="defaultcon**	11	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\obj\Release\TransformWebConfig\transformed\Web.config

<add name="s1mmarketi***	17	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\obj\Release\TransformWebConfig\transformed\Web.config
<add name="defaultcon***	11	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\obj\Release\CSAutoParameterize\original\Web.config
<add name="s1mmarketi***	17	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\obj\Release\CSAutoParameterize\original\Web.config
<add name="defaultcon***	11	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\obj\Release\TransformWebConfig\original\Web.config

Recommendation

External or In-House Database Connectivity is being called in the application. Make sure Database Connectivity with the application.
Otherwise, Azure has the following options for migrating databases which are listed below:

1-SQL Server on Azure VMs
2-Azure SQL Database
3-Azure SQL Managed Instance
After migration, change Database Connectivity to Target Platform.

Estimated Efforts

2.00 Hours **Size :** Small

Impact

Optional

Help URL

https://docs.microsoft.com/en-us/azure/sql-database/

Category : Security **DataPoint :** Encryption

Reason for change

The Application uses Encryption. These Encryption Algorithm may or may not be work in Azure Virtual Machine.

Code block	Line no.	File path
using (Aes encryptor = Aes.Create())	25	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\helperClass\Cryptography.cs

using (Aes encryptor = Aes.Create())	59	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.EventManagement\helperClass\Cryptography.cs

Recommendation

Applications use encryption(cryptographic) keys and secrets to help keep information secure. Azure Key Vault safeguards these keys and secrets. When you use Key Vault, you can encrypt authentication keys, storage account keys, data encryption keys, .pfx files, and passwords by using keys that are protected by hardware security modules (HSMs).

Azure web application to read information from Azure Key Vault by using managed identities for Azure resources.
Below are steps How to use Azure Key Vault.

- Create a key vault.
- Store a secret in the key vault.
- Retrieve a secret from the key vault.
- Enable a managed service identity for the web app.
- Grant the required permissions for the web application to read data from the key vault.

For further assistance refer to the Help Url.

Estimated Efforts

4.00 Hours **Size :** Small

Impact

Conditionally_Mandatory

Help URL

https://docs.microsoft.com/en-us/azure/key-vault/key-vault-whatis

S1M.BAL

Category : Application & Platform Design **DataPoint :** SessionStateSection

Reason for change

In Proc, Session mode will not support when you scale up your Application.

Code block	Line no.	File path
LoginResponse sessionValue = HttpContext.Current.Session["LoginInfo"] as LoginResponse;	19	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.BAL\AssetMappingBL.cs

Recommendation

In Proc, Session mode will not support when the application is Scaled-Up. Use other session options to support the scalability of your application.

1- **Use OutProc Session** where Session State is stored In the StateServer and SqlServer modes.

2- Azure Redis Cache: Azure Redis Cache provides a session state provider that you can use to store your session state in a cache rather than in memory or in a SQL Server database. To use the caching session state provider, first, configure your cache, and then configure your ASP.NET application for the cache using the Redis Cache Session State NuGet package.

To configure a client application in Visual Studio using the Azure Cache for Redis Session State NuGet package, click NuGet Package Manager, Package Manager Console from the Tools menu.

Run the following command from the Package Manager Console window.

Install-Package Microsoft.Web.RedisSessionStateProvider

The NuGet package downloads and adds the required assembly references and adds the following section into your web.config file. This section contains the required configuration for your ASP.NET application to use the Redis Cache Session State Provider.

Configure Azure Cache for Redis settings.
Configure the attributes with the values from your cache blade in the Microsoft Azure portal, and configure the other values as desired.

Sample Code

```
<sessionState mode="Custom" customProvider="MySessionStateStore">
  <providers>
 <add name="MySessionStateStore" type="Microsoft.Web.Redis.RedisSessionStateProvider"
         host=""
         accessKey=""
         ssl="true" />
</sessionState>
```

Estimated Efforts

4.00 Hours **Size :** Small

Impact

Conditionally_Mandatory

Help URL

https://docs.microsoft.com/en-us/azure/redis-cache/cache-aspnet-session-state-provider https://docs.microsoft.com/en-us/azure/azure-cache-for-redis/cache-configure#configure-azure-cache-for-redis-settings

S1M.DAL

Category : Security **DataPoint :** Connection Strings Section

Reason for change

ConnectionStringSection is use for storing database connectivity credential.It is very sensitive information of application.

Code block	Line no.	File path
<add name="s1mmarketi*** ****	7	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.DAL\App.Config

Recommendation

ConnectionStringSection uses for storing database connectivity credentials. It is very sensitive information about the application.

Azure Provide **Azure KeyVault**, to securely stores sensitive information of the application. So use that to store connection strings.

We are always recommended to encrypt the connection string of your application because the data we have there is highly sensitive. It must be secured.

Please find the following steps to encrypt the web. config.

1-Open Command Prompt with Administrator privileges
2-At the Command Prompt, enter
3-cd C:\Windows\Microsoft.NET\Framework\v4.0.30319
4-In case your web Config is located in "D:\Articles\EncryptWebConfig" directory path, then enter the following to encrypt the ConnectionString:

ASPNET_REGIIS -pef "connectionStrings" "D:\Articles\EncryptWebConfig

Sample Code

```
<configuration>
<connectionStrings
configProtectionProvider="RsaProtectedConfigurationProvider">
<EncryptedData Type="http://www.w3.org/2001/04/xmlenc#Element"
xmlns="http://www.w3.org/2001/04/xmlenc#">
<EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc">
<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
<EncryptedKey xmlns="http://www.w3.org/2001/04/xmlenc#">
<EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5" />
<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
<KeyName> RSA Key </KeyName>
 </KeyInfo>
 <CipherData>
 <CipherValue>
 WcFEbDX8VyLfAsVK8g6hZVAG1674ZFc1kWH0BoazgOwdBfinhcAmQmnIn0oHtZ5tO2EXGl+dyh10giEmO9NemH4Y
Zk+iMIln+ItcEay9CGWMXSen9UQLpcQHQqMJErZiPK4qPZaRWwqckLqriCl9X8x9OE7jKIsO2Ibapwj+1Jo=
 </CipherValue>
 </CipherData>
 </EncryptedKey>
 </KeyInfo>
 <CipherData>
 <CipherValue>
OpWQgQbq2wBZEGYAeV8WF82yz6q5WNFIj3rcuQ8gT0MP97aO9SHIZWwNggSEi2Ywi4omKOGA4mjqT0VZaXgb9tVeG
BDhjPh 5ZlrLMNfYSozeJ
m2Lsm7hnF6VvFm3fFMXa6+h0JTHeCXBdmzg/vQb0u3oejSGzB4ly+V9O0T4Yxkwn9KVDW58PHOeRT2//3iZfJ
WV2NZ4e6vj4Byjf81o3JVNgRjmm9hr9blVbbT3Q8/j5zJ+TElCn6zPHvnuB70iG2KPJXqAj2GBzBk6cHq+WNebOQN
WIb7dTPumuZ K0yW1XDZ5gkfBuqgn8hm osTE7mCvieP9rgATf6qgLgdA6zYyVV6WDjo1qbCV807lczxa3bF5KzKa
VUSq5FS1SpdZKAE6/kkr0Ps++CE=
 </CipherValue>
 </CipherData>
</EncryptedData>
 </connectionStrings>
 </configuration>
```

Estimated Efforts

2.00 Hours **Size :** Small

Impact

Conditionally_Mandatory

Help URL

https://www.c-sharpcorner.com/article/encrypt-and-decrypt-connectionstring-in-web-config-file/

Category : Storage **DataPoint :** DB Connections

Reason for change

Database Connections might not work properly in Azure.

Code block	Line no.	File path
<add name="s1mmarketi** *** ****	7	D:\Project\S1mAdminPanel\S1mAdminPanel-kendo_15-09-2016\S1M.DAL\App.Config

Recommendation

External or In-House Database Connectivity is being called in the application. Make sure Database Connectivity with the application.
Otherwise, Azure has the following options for migrating databases which are listed below:

1-SQL Server on Azure VMs
2-Azure SQL Database
3-Azure SQL Managed Instance
After migration, change Database Connectivity to Target Platform.

Estimated Efforts

2.00 Hours **Size :** Small

Impact

Optional

Help URL

https://docs.microsoft.com/en-us/azure/sql-database/

S1M.DTO

Questionnaire Result

Category : Application & Platform Design **DataPoint :** GAC Dependency

Reason for change

GAC dependency might not work properly in Azure Virtual machine.

Recommendation

Application deployed using Lift and Shift, there is no need to change anything.

Application deployed to Azure virtual Machine then verify the assemblies are working properly or not, if not then-

1. Install an assembly into the global assembly cache(GAC).

Use syntex-> gacutil -i

2. Move Assemblies to BIN folder.

Estimated Efforts

4.00 Hours **Size :** Small

Impact

Optional

Help URL

https://docs.microsoft.com/en-us/dotnet/framework/app-domains/how-to-install-an-assembly-into-the-gac

Category : Application & Platform Design **DataPoint :** Background Processing

Reason for change

Background Processing might not work properly in Azure Virtual machine.

Recommendation

Background tasks in an Azure virtual machine provide flexibility and allow precise control over the initiation, execution, scheduling, and resource allocation. However, it will increase runtime cost if a virtual machine must be deployed just to run background tasks.

Background task in a virtual machine, you have a range of options:

- You can execute the task on-demand directly from your application by sending a request to an endpoint that the task exposes. This passes in any data that the task requires. This endpoint invokes the task.
- You can configure the task to run on a schedule by using a scheduler or timer that is available in your chosen operating system. For example, on Windows, you can use Windows Task Scheduler to execute scripts and tasks. Or, if you have SQL Server installed on the virtual machine, you can use the SQL Server Agent to execute scripts and tasks.
- You can use Azure Scheduler to initiate the task by adding a message to a queue that the task listens on, or by sending a request to an API that the task exposes.

Another Option: If the Application is deployed using Lift and Shift, there is no need to change anything.

Estimated Efforts

2.00 Hours **Size :** Small

Impact

Optional

Help URL

No Record Found

Category : Storage **DataPoint :** Automatic Backup

Reason for change

Automatic Backup is used to minimize the risk of data loss and get backup automatic as per interval.

Recommendation

Using the Azure Backup service we can schedule the backup of the VM as per requirement.

Steps to configure a backup of Azure VM

1. Configure the backup job from the VM operations menu.
2. Configure the backup job from the Recovery Services vault
3. Create a recovery services vault for a VM
4. Select a backup goal, set policy, and define items to protect
5. Initial backup
6. Defining a backup policy
7. Install the VM Agent on the virtual machine

For further details refer to the below Help Url.

Estimated Efforts

1.00 Hours **Size :** Small

Impact

Optional

Help URL

https://docs.microsoft.com/en-us/azure/backup/backup-azure-vms-first-look-arm

Category : Security **DataPoint :** Firewall

Reason for change

Firewall configured in On-premise environment might not be accessible in Azure environment

Recommendation

There are two options to configure a firewall in azure-
1. Move existing firewall service to azure.
2. Configure Network Security Group(NSG) and Azure Firewall in Azure for the application.

Step to configure NSG in Azure

1. Create a network security group.
2. Create an inbound security rule. Add rules for the application.
3. Associate your network security group with a subnet.

Estimated Efforts

4.00 Hours **Size :** Small

Impact

Optional

Help URL

https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-filter-network-traffic#create-a-network-security-group

Category : Security **DataPoint :** Secure Socket Layer (SSL)

Reason for change

Application defined some Secure Socket Layer(SSL) related settings.

Recommendation

Bind SSL certificate to Azure Web Apps

How to Configure

1. Log in to the Azure portal.
2. Navigate to â?? App Servicesâ? in the left navigation pane.
3. Select your web application.
4. Click on â??Settingsâ? and select â??Custom domains and SSL.â?
5. A new frame will open on the right side. Click on â?? Bring external domains.â?
6. Note the IP address located at the bottom. Go to your domain registrar website and create DNS entries using this IP address. It can take some time for the changes to propagate, depending on your DNS provider.
7. In the â??Domain Namesâ? text box, enter the custom domain name you bought from the domain registrar.
8. Save the changes.
9. Click on â??Upload certificate.â?
10. Locate and upload your .pfx certificate file.
11. Under â??SSL bindings,â? select the domain name to secure with SSL, and the certificate to use.
12. Save the changes.
13. You should be able to access the web app using your custom domain name over HTTPS.

Estimated Efforts

4.00 Hours **Size :** Small

Impact

Conditionally_Mandatory

Help URL

https://docs.microsoft.com/en-us/azure/cloud-services/cloud-services-configure-ssl-certificate-portal

Category : Application & Platform Design **DataPoint :** Com Import

Reason for change

Application using some COM+ Component that may or may not work properly

Recommendation

Application using some COM+ Component.

Follow the below steps to configure.

1. If You are using COM+ Component as an assembly, then Right click on assembly.
2. Select Property from Menu.
3. Select Copy to Output directory-> Copy Always.
4. If You are using COM Component as an exe, then You need to create a startup script.
5. Create PowerShell script for COM+ Component.
6. Add Folder Startup in your Role.
7. Add All related files in the Startup folder.
8. Configure the startup task in your Service Definition file.

Estimated Efforts

2.00 Hours **Size :** Small

Impact

Optional

Help URL

https://stackoverflow.com/questions/14981830/asppdf-and-aspjpeg-on-windows-azure

Category : Security **DataPoint :** PII Information

Reason for change

Your application is storing or sharing PII Informations.

Recommendation

1. Use industry-standard AES encryption. 2. Use dual control and separation of duties to protect your encryption keys. 3. Encrypt sensitive data prior to moving and/or use encrypted connections (HTTPS, SSL, TLS, FTPS, etc) to protect the contents of data in transit. 4. Encrypt sensitive files prior to storing them and/or choose to encrypt the storage drive itself. 5. Use Azure Key Vault to Keep your encryption keys are separate from the data that is being protected.
Azure Key Vault helps safeguard cryptographic keys and secrets that cloud applications and services use. Key Vault streamlines the key management process and enables you to maintain control of keys that access and encrypt your data. Developers can create keys for development and testing in minutes, and then migrate them to production keys. Security administrators can grant (and revoke) permission to keys.

Estimated Efforts

1.00 Hours **Size :** Small

Impact

Optional

Help URL

https://docs.microsoft.com/en-us/azure/key-vault/key-vault-whatis