Código de Documento: TI-EA2023-12683 - REQ008 Nº PASE: 2024-14066

Código de Requerimiento: 2401009799

Desarrollado con Proveedor

1. **Datos Generales ￼**

Fecha de Solicitud Pase\_\_\_\_\_12/02/2024\_\_\_\_\_\_\_\_ Analista Solicitante \_\_\_\_\_Juan Gala\_\_\_\_\_

Usuario Final \_\_\_\_\_ Diego Asmat \_\_\_\_ Área Usuario Final \_\_Productos y servicios para empresas \_\_\_

Fecha y Hora programada de ejecución: \_\_\_\_\_\_14/02/2024 4:00 AM\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Descripción del cambio \_Implementación de la iniciativa TI-EA2023-12683

Nombre Empresa Proveedor \_\_\_\_\_\_\_\_\_\_\_\_\_ Responsable Proveedor\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. **Información de la Aplicación**  Nueva Aplicación: () Si ( x ) No

|  |  |  |  |
| --- | --- | --- | --- |
| **Nombre de la aplicación** | *banbif-seguridad-empresas-service* | | |
| **Lenguaje de Programación** | *JAVA* | | |
| **Ruta Carpeta de Desarrollo** | [\\serbiffilex64\Sistemas\_Distribuidos\CarpetaPase\APP\TI-EA2023-12683\2024-14067\CYBERLEGO-01.00.1](file:///\\serbiffilex64\Sistemas_Distribuidos\CarpetaPase\jgala\822-2023-13736\CYBERLEGO-01.00.134)40 | | |
| **Ruta Carpeta Pruebas UAT** | [\\serbiffilex64\Aseguramiento\_Calidad\_UAT\CYBERLEGO\CYBERLEGO-01.00.140](file:///\\serbiffilex64\Aseguramiento_Calidad_UAT\CYBERLEGO\CYBERLEGO-01.00.140) | | |
| **Nº Versión en producción** | **01.00.139** | **Nº Versión después del pase** | **01.00.140** |

1. **Alcance. (Marcar con una X)**

|  |  |  |  |
| --- | --- | --- | --- |
| Aplicaciones Web |  | Base de Datos |  |
| Componentes COM+ |  | Ejecutables |  |
| Instalación en PCs de usuario |  | Web Services |  |
| Aplicaciones Cliente Servidor |  | Otros | X |

1. **Recursos de Software/Aplicativo pre-instalado que requiere la aplicación**

|  |  |  |  |
| --- | --- | --- | --- |
| **Software / Aplicativo** | **Versión** | **En Cliente**  *(Marcar con una X)* | **En Servidor**  *(Marcar con una X)* |
| *Openshift 4.9 (namespace: FUSE)* |  |  | *X* |
|  |  |  |  |
|  |  |  |  |

#### *Archivos de despliegue*

|  |  |  |
| --- | --- | --- |
| **#** | **Nombre** | **Tipo**  **(Instalador o Deployment)** |
| 1 | *banbif-seguridad-empresas-service* | *Deployment* |
|  |  |  |

**Nombres y tipos de archivos a actualizar**

#### *Base de datos: \_\_\_\_ Servidor: \_\_\_\_\_\_\_*

(A Agregar, E Eliminar, M Modificar)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **#** | **Nombre de Script** | **Objeto** | **Tipo**  *(De la lista de tipos, ver instructivo)* | **A**  *(Marcar con una X)* | **E**  *(Marcar con una X)* | **M**  *(Marcar con una X)* |
|  |  |  |  |  |  |  |
| *Totales:* | |  |  |  |

#### *Aplicación*

(A Agregar, E Eliminar, M Modificar)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **#** | **Nombre Fuente** | **Nombre Compilado** | **A**  *(Marcar con una X)* | **E**  *(Marcar con una X)* | **M**  *(Marcar con una X)* | **Observaciones** |
| 1 | *banbif-seguridad-empresas-service* |  |  |  | *X* |  |
|  |  | *Totales:* |  |  | *1* |  |

1. **Procedimiento de ejecución del Pase a Producción – Plan de Instalación**

|  |  |
| --- | --- |
| **1** | Ingresar a la consola del openshift con su usuario y generar el token a través de la opción “copy login command”, ejemplo:  oc login --token=sha256~Gt6e3mTLaq9RzUHsK76cmtuAl-oiXpQp5PTk2LCjm0s --server=https://api.ocpprd01.dombif.peru:6443  URL: [https://console-openshift-console.apps.ocp01.dombif.peru/](https://console-openshift-console.apps.ocpuat01.dombif.peru/) |
| **2** | Ubicarnos en el proyecto **fuse** |
| **3** | 1. Seleccionar la siguiente opción:      1. Buscar el configmap “banbif-seguridad-empresas-configmap”      1. Editamos el configMap      1. Buscar la propiedad “*softtoken.wsdl.url*”      * Cambiar el valor de la propiedad “*softtoken.wsdl.url*”   ANTES**:** [**http://atx.dombif.peru:8080/detect/services/WSDetectMobileAuthService?wsdl**](http://atx.dombif.peru:8080/detect/services/WSDetectMobileAuthService?wsdl)  AHORA: [**http://atx3.dombif.peru:8080/detect/services/WSDetectMobileAuthService?wsdl**](http://atx3.dombif.peru:8080/detect/services/WSDetectMobileAuthService?wsdl)   1. Buscar la propiedad “*softtoken.wsdl.url.client.service*”      * Cambiar el valor de la propiedad “*softtoken.wsdl.url.client.service*”   ANTES**:** [**http://atx.dombif.peru:8080/detect/services/WSClientService?wsdl**](http://atx.dombif.peru:8080/detect/services/WSClientService?wsdl)  AHORA: [**http://atx3.dombif.peru:8080/detect/services/WSClientService?wsdl**](http://atx3.dombif.peru:8080/detect/services/WSClientService?wsdl)   1. Guardar los cambios del configmap |
| **4** | Por último, debemos reiniciar el pod del servicio “banbif-seguridad-empresas-service”   1. Buscar el servicio “banbif-seguridad-empresas-service”      1. Seleccionar el servicio “banbif-seguridad-empresas-service”      1. Bajar los pods a **0** 2. Subir los pods a 2 3. Esperar a que termine de iniciar el servicio y ejecutar las pruebas |
| **5** | Si no inicia, debemos realizar la siguiente modificación en el yml del servicio “*banbif-seguridad-empresas-service”* |

1. **Plan de Rollback**

|  |  |
| --- | --- |
| **1** | Ubicarnos en el proyecto namespace **fuse** |
| 2 | 1. Seleccionar la siguiente opción:      1. Buscar el configmap “banbif-seguridad-empresas-configmap”      1. Editamos el configMap      1. Buscar la propiedad “*softtoken.wsdl.url*”      * Cambiar el valor de la propiedad “*softtoken.wsdl.url*”   ANTES: [**http://atx.dombif.peru:8080/detect/services/WSDetectMobileAuthService?wsdl**](http://atx.dombif.peru:8080/detect/services/WSDetectMobileAuthService?wsdl)  AHORA**:** [**http://atx3.dombif.peru:8080/detect/services/WSDetectMobileAuthService?wsdl**](http://atx3.dombif.peru:8080/detect/services/WSDetectMobileAuthService?wsdl)   1. Buscar la propiedad “*softtoken.wsdl.url.client.service*”      * Cambiar el valor de la propiedad “*softtoken.wsdl.url.client.service*”   ANTES: [**http://atx.dombif.peru:8080/detect/services/WSClientService?wsdl**](http://atx.dombif.peru:8080/detect/services/WSClientService?wsdl)  AHORA**:** [**http://atx3.dombif.peru:8080/detect/services/WSClientService?wsdl**](http://atx3.dombif.peru:8080/detect/services/WSClientService?wsdl)   1. Guardar los cambios del configmap |
| 3 | Por último, debemos reiniciar el pod del servicio “banbif-seguridad-empresas-service”   * Buscar el servicio “banbif-seguridad-empresas-service”      * Seleccionar el servicio “banbif-seguridad-empresas-service”      * Bajar los pods a **0** * Subir los pods a 2 * Esperar a que termine de iniciar el servicio y ejecutar las pruebas |
| 4 | Si no inicia, debemos realizar la siguiente modificación en el yml del servicio “*banbif-seguridad-empresas-service”* |

1. **Observaciones**

Luego de realizado el pase a producción solo debemos de mantener 2 replication Controllers activos, eliminar los demás.

1. **Medición del Riesgo**

**Sustento de la valoración del riesgo:**

1. **Describa la complejidad del cambio**
2. **Conformidad y Autorizaciones.**

|  |  |  |
| --- | --- | --- |
| **Analista**  **Desarrollo** | **Especialista**  **Desarrollo**  **Juan Gala** | **Observaciones** |