NTT DATA

Permisos BFF

Recursos azure y demás tecnologías.

FUTURE
AT HEART

Permisos BFF

Este archivo se elabora con propósito de establecer una descripción de los permisos y recursos requeridos a nivel BFF (Backend-For-Frontend) para acceso a las diversas tecnologías manejadas por la APP en capa media.

1. Como primera medida y con propósito de comprobar el funcionamiento de los servicios entregados por back-core, es necesaria la habilitación por firewall de los dominios del BUS de servicios en ambientes de pruebas y producción (se usa en producción como última instancia de monitoreo, cuando las trazas capturadas en los LOGS capa media no logran atribuir conflictos a una fuente especifica), esta habilitación es necesaria desde la máquina del líder técnico o desarrollador en capacidad de su uso.

2. Es necesaria la habilitación por firewall de GITHUB desde las máquinas de los desarrolladores, así mismo acceso a los repositorios de la organización “PorvenirAFP”, además tener en cuenta que al menos 2 miembros del equipo deben contar con rol de aprobador.

3. Es necesaria la habilitación por firewall de JENKINS desde las máquinas de los desarrolladores, además usuario y contraseña a un perfil que permita visualización, ejecución y detención de los PIPELINES usados por la APP.

4. Es necesaria la habilitación por firewall de SONARQUBE desde las máquinas de los desarrolladores, con propósito de validar posibles problemas con calidad del código y Test unitarios.

5. Se necesita un usuario de RED con privilegios para conectar al “Azure Bastion” que a su vez establezca una conexión RDP, permitiendo el uso de la base de datos “Azure CosmosDB”, para la obtención de LOGS Producción.

6. Se necesita un usuario de RED con privilegios para conectar al “Azure Bastion” que a su vez establezca una conexión RDP, permitiendo el uso de la base de datos “SQL”, esto para todos los ambientes. Con la finalidad de actualizar la funcionalidad “parametria”, pensada para inactivar módulos de la aplicación en base a los permisos de un usuario.

7. Se necesita un usuario de RED con privilegios para conectar por SSH al “Azure Bastion” mismo que accede al grupo de recursos que contiene el servicio/recurso k8s, esto para todos los ambientes (PT, QA, PRD y DRP), con ánimo de monitorear la salud o estado de los PODS.

8. Se requiere la habilitación por Firewall de “portal.azure” desde la máquina de los desarrolladores, además un usuario que permita la visualización de los siguientes recursos en todos los ambientes (PT, QA, PRD y DRP):

   - Kubernetes services
   - API Management
   - Azure Cosmos DB