Guía del usuario de BPA Permisos de RBAC v5.1

Introducción

El control de acceso basado en roles (RBAC) es un método para restringir el acceso basado en los roles de los usuarios dentro de una empresa. Las funciones predeterminadas están disponibles y se pueden crear nuevas funciones seleccionando los permisos preferidos y asignando estas funciones a grupos de usuarios. La asignación de funciones a grupos de usuarios permite a todos los usuarios de ese grupo realizar las operaciones asociadas a la función.

Nuevos permisos

Esta sección describe cómo un microservicio puede definir su propio conjunto de permisos RBAC.

Definir permisos estáticos

Para definir permisos estáticos:

1. Cree un archivo JSON que enumere todos los permisos en la ruta de acceso microservice/src/config/device-permissions-spec.json.
2. Ejecute el siguiente código JSON para enumerar un permiso:

```
{
    "service":"service-name",
    "permissions": [
        {
            "group": "group-name",
            "actions": [
```

```
                {"name":"action-name","displayName":"Display name to be shown in roles page"}
            ]
        }
    ]
}
```

Consulte el ejemplo siguiente para crear, ver, administrar y quitar permisos dentro de un grupo de credenciales.

Ejemplo de creación de permisos

Registro de permisos en BPA

Para registrar permisos:

1. Importe rbacSpecProcessorHelper desde @cisco-bpa-platform/mw-util-common-app.

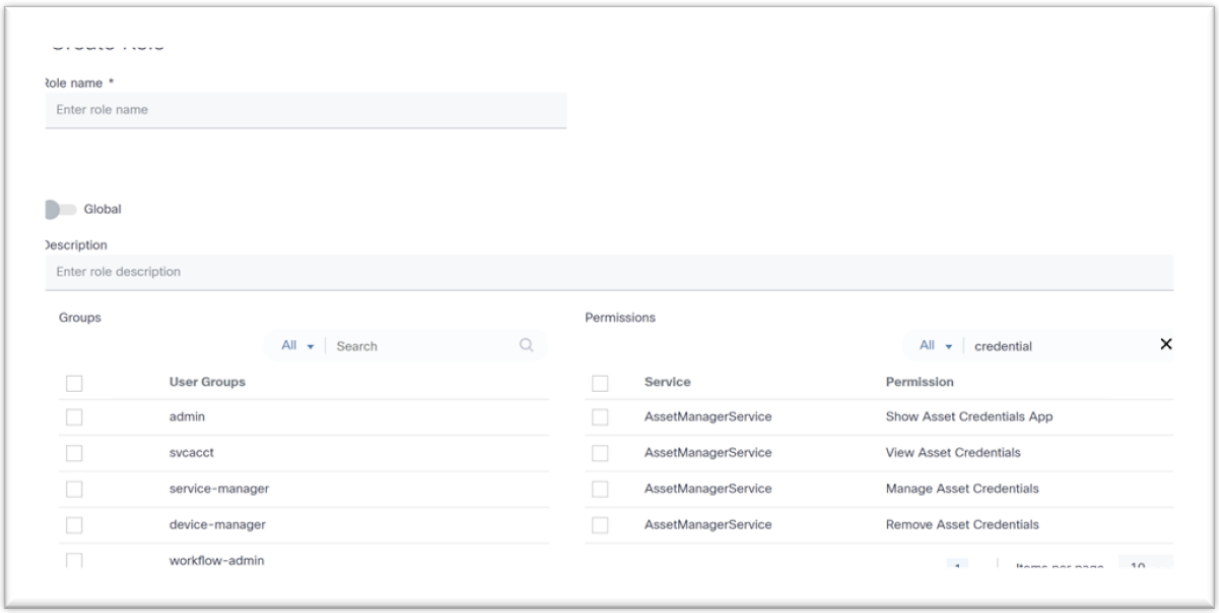
```
const { rbacHelper, rbacSpecProcessorHelper } = require('@cisco-bpa-platform/mw-util-common-app');
```

2. Ejecute el siguiente comando para utilizar rbacSpecProcessorHelper para procesar los permisos enumerados en el archivo JSON.

```
let resources = require('./config/asset-manager-permissions-spec');
let rbacSpecProcessorObj = rbacSpecProcessorHelper.getRbacSpecProcessorUtil();
rbacSpecProcessorObj.setSpec(resources);
await rbacSpecProcessorObj.process();
```

Nota: Los usuarios también pueden consultar los métodos compartidos en @cisco-bpa-platform/mw-util-common-app para registrar, ver, administrar y quitar permisos.

Los usuarios pueden ver los permisos registrados en las páginas Crear rol y Editar rol.



Crear rol

Permisos de asignación

Los permisos creados en la sección anterior se pueden asignar a funciones de forma predeterminada o definiendo la asignación con funciones.

Definición de asignación de permisos

Para asignar permisos definidos a funciones predeterminadas, cree un nuevo archivo JSON en la ruta de acceso microservice/src/config/device-role-permissions-mapping-spec.json.

En el ejemplo siguiente, se asignan tres (3) permisos al rol de superadministrador de BPA, dos (2) al rol de administrador de arrendatarios y uno (1) al rol de operador de red.

Nota: El nombre de servicio, el nombre de grupo y el nombre de acción deben definirse de la misma forma que en el archivo JSON.

```
{
    "service": "AssetManagerService",
    "roles": [
        {
            "name": "BPA Super Admin",
            "permissions": [
                {"name":"view","displayName":"View Asset Credentials","group": "credential"},
```

```
                {"name":"remove","displayName":"Remove Asset Credentials","group": "credential"},
                {"name":"manage","displayName":"Manage Asset Credentials Add, Update and Delete Asset C
            ]
        },
        {
            "name": "Tenant Admin",
            "permissions": [
                {"name":"view","displayName":"View Asset Credentials","group": "credential"},
                {"name":"remove","displayName":"Remove Asset Credentials","group": "credential"}
            ]
        },
        {
            "name": "Network Operator",
            "permissions": [
                {"name":"view","displayName”:"View Asset Credentials","group": "credential"}
            ]
        }
    ]
}
```

Actualizando asignación de permisos

Para actualizar la asignación de permisos:

1. Importe rbacHelper, rbacPermissionMappingHelper de @cisco-bpa-platform/mw-util-common-app.

```
const { rbacHelper, rbacPermissionMappingHelper } = require('@cisco-bpa-platform/mw-util-common-app');
```

2. Ejecute el siguiente comando para actualizar la asignación de permisos con funciones:

```
let rbacUtilObj = rbacHelper.getRbacUtilObj();
let registryDetails = await rbacUtilObj getRegistryByName({}, 'device-role-permissions-mapping-spec');
if (Array.isArray(registryDetails) && registryDetails.length === 0) {
    let rbacPermissionMappingSpecProcessorObj = rbacPermissionMappingHelper.getRbacSpecProcessorUtil()
    let rolePermissions = require('./config/device-role-permissions-mapping-spec');
    rbacPermissionMappingSpecProcessorObj.setSpec(rolePermissions);
    await rbacPermissionMappingSpecProcessorObj.process();
    let rbacUtilObjRegister = rbacHelper.getRbacUtilObj();
    await rbacUtilObjRegister addRegistry({}, 'device-role-permissions-mapping-spec');
}
```

3. Ejecute el comando siguiente para procesar los archivos, crear una lista de permisos y asignar permisos con funciones:

```
async function permissionsSpecProcessor() {
    let resources = require('./config/device-permissions-spec');
    let rbacSpecProcessorObj = rbacSpecProcessorHelper.getRbacSpecProcessorlltil();
    rbacSpecProcessorObj.setSpec(resources);
    await rbacSpecProcessorObj.process();

    let rbacUtilObj = rbacHelper.getRbacUtilObj();
    let registryDetails = await rbacUtilObj.getRegistryByName({} 'device-role-permissions-mapping-spec'
    if (Array.isArray(registryDetails) && registryDetails.length === 0) {
        let rbacPermissionMappingSpecProcessorObj = rbacPermissionMappingHelper.getRbacSpecProcessorUti
        let rolePermissions = require('./config/device-role-permissions-mapping-spec');
        rbacPermissionMappingSpecProcessorObj.setSpec(rolePermissions);
        await rbacPermissionMappingSpecProcessorObj.process();
        let rbacUtilObjRegister = rbacHelper.getRbacUtilObj();
        await rbacUtilObjRegister.addRegistry({}, 'device-role-permissions-mapping-spec');
    }
}
```

Nota: Los usuarios también pueden consultar los métodos compartidos en @cisco-bpa-platform/mw-util-common-app para actualizar la asignación de permisos con funciones.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).