Guia do usuário do BPA RBAC Permissions v5.1

Introdução

O Controle de Acesso Baseado em Atribuições (RBAC - Role Based Access Control) é um método de restringir o acesso baseado nas atribuições dos usuários dentro de uma empresa. As funções padrão estão disponíveis, e novas funções podem ser criadas selecionando permissões preferenciais e mapeando essas funções para grupos de usuários. O mapeamento de funções para grupos de usuários permite que todos os usuários desse grupo de usuários executem as operações associadas à função.

Novas permissões

Esta seção descreve como um microsserviço pode definir seu próprio conjunto de permissões RBAC.

Definir permissões estáticas

Para definir permissões estáticas:

1. Crie um arquivo JSON listando todas as permissões no caminho microservice/src/config/device-permissions-spec.json.
2. Execute o seguinte código JSON para listar uma permissão:

```
{
    "service":"service-name",
    "permissions": [
        {
            "group": "group-name",
            "actions": [
                {"name":"action-name","displayName":"Display name to be shown in roles page"}
```

```
            ]
        }
    ]
}
```

Consulte o exemplo a seguir para criar permissões de exibição, gerenciamento e remoção em um grupo de credenciais.

Exemplo de criação de permissões

Registrando permissões no BPA

Para registrar permissões:

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

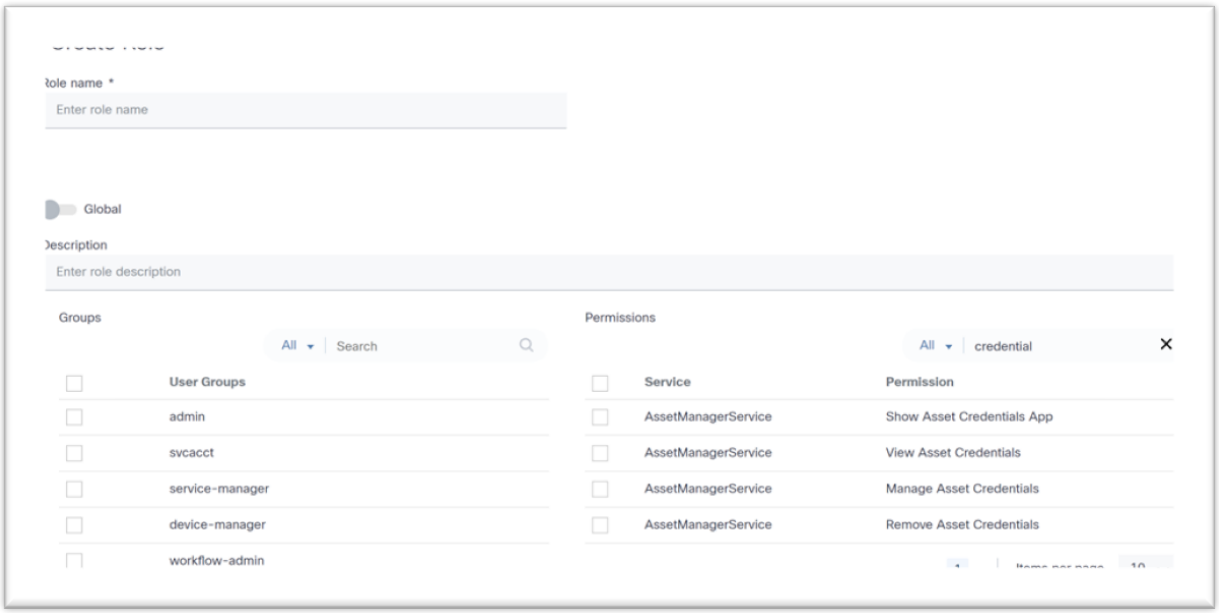
```
const { rbacHelper, rbacSpecProcessorHelper } = require('@cisco-bpa-platform/mw-util-common-app');
```

2. Execute o seguinte comando para usar rbacSpecProcessorHelper para processar as permissões listadas no arquivo JSON.

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

Note: Os usuários também podem consultar os métodos compartilhados em @cisco-bpa-platform/mw-util-common-app para registrar permissões de exibição, gerenciamento e remoção.

Os usuários podem exibir permissões registradas nas páginas Criar função e Editar função.



Criar função

Permissões de Mapeamento

As permissões criadas na seção anterior podem ser mapeadas para funções por padrão ou definindo o mapeamento com funções.

Definindo Mapeamento de Permissões

Para mapear permissões definidas para funções padrão, crie um novo arquivo JSON no caminho microservice/src/config/device-role-permissions-mapping-spec.json.

No exemplo abaixo, três (3) permissões são mapeadas para a função Super Admin do BPA, duas (2) são mapeadas para a função Admin de Locatário e uma (1) é mapeada para a função Operador de Rede.

Note: O nome do serviço, o nome do grupo e o nome da ação devem ser definidos da mesma forma que no arquivo 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"}
            ]
        }
    ]
}
```

Atualizando Mapeamento de Permissão

Para atualizar o mapeamento de permissão:

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

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

2. Execute o seguinte comando para atualizar o mapeamento de permissões com funções:

```
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. Execute o seguinte comando para processar os arquivos, criar uma lista de permissões e mapear permissões com funções:

```
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');
    }
}
```

Note: Os usuários também podem consultar os métodos compartilhados em @cisco-bpa-platform/mw-util-common-app para atualizar o mapeamento de permissões com funções.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.