Setup MFA enforcement

Below You can find instructions on how to set up MFA enforcement that forbids any AWS user from using any service without:

1. Setting up an MFA device.
2. Signing in using MFA. Any user that signs in without MFA must not be allowed to manage any resource on AWS.

Policy Creation

Navigate to **Policies** section, under the **IAM** service, and create the following policy:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowViewAccountInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetAccountPasswordPolicy",
                "iam:GetAccountSummary",
                "iam:ListVirtualMFADevices"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowManageOwnPasswords",
            "Effect": "Allow",
            "Action": [
                "iam:ChangePassword",
                "iam:GetUser"
            ],
            "Resource": "arn:aws:iam::*:user/${aws:username}"
        },
        {
            "Sid": "AllowManageOwnAccessKeys",
            "Effect": "Allow",
            "Action": [
                "iam:CreateAccessKey",
                "iam:DeleteAccessKey",
                "iam:ListAccessKeys",
                "iam:UpdateAccessKey"
```

```
        ],
        "Resource": "arn:aws:iam::*:user/${aws:username}"
    },
    {
        "Sid": "AllowManageOwnSigningCertificates",
        "Effect": "Allow",
        "Action": [
            "iam:DeleteSigningCertificate",
            "iam:ListSigningCertificates",
            "iam:UpdateSigningCertificate",
            "iam:UploadSigningCertificate"
        ],
        "Resource": "arn:aws:iam::*:user/${aws:username}"
    },
    {
        "Sid": "AllowManageOwnSSHPublicKeys",
        "Effect": "Allow",
        "Action": [
            "iam:DeleteSSHPublicKey",
            "iam:GetSSHPublicKey",
            "iam:ListSSHPublicKeys",
            "iam:UpdateSSHPublicKey",
            "iam:UploadSSHPublicKey"
        ],
        "Resource": "arn:aws:iam::*:user/${aws:username}"
    },
    {
        "Sid": "AllowManageOwnGitCredentials",
        "Effect": "Allow",
        "Action": [
            "iam:CreateServiceSpecificCredential",
            "iam:DeleteServiceSpecificCredential",
            "iam:ListServiceSpecificCredentials",
            "iam:ResetServiceSpecificCredential",
            "iam:UpdateServiceSpecificCredential"
        ],
        "Resource": "arn:aws:iam::*:user/${aws:username}"
    },
    {
        "Sid": "AllowManageOwnVirtualMFADevice",
        "Effect": "Allow",
        "Action": [
```

```
                "iam:CreateVirtualMFADevice",
                "iam:DeleteVirtualMFADevice"
            ],
            "Resource": "arn:aws:iam::*:mfa/${aws:username}"
        },
        {
            "Sid": "AllowManageOwnUserMFA",
            "Effect": "Allow",
            "Action": [
                "iam:DeactivateMFADevice",
                "iam:EnableMFADevice",
                "iam:ListMFADevices",
                "iam:ResyncMFADevice"
            ],
            "Resource": "arn:aws:iam::*:user/${aws:username}"
        },
        {
            "Sid": "DenyAllExceptListedIfNoMFA",
            "Effect": "Deny",
            "NotAction": [
                "iam:CreateVirtualMFADevice",
                "iam:EnableMFADevice",
                "iam:ListMFADevices",
                "iam:ListVirtualMFADevices",
                "iam:ResyncMFADevice",
                "sts:GetSessionToken",
                "iam:ChangePassword",
                "iam:GetUser"
            ],
            "Resource": "*",
            "Condition": {
                "BoolIfExists": {
                    "aws:MultiFactorAuthPresent": "false"
                }
            }
        }
    ]
}
```

The policy above allows a user to only perform certain actions related to their account such as changing the password, or setting an MFA device. Moreover, the

Registration code: 304155531 · VAT: LT100009892318
Address: V. Nagevičiaus g. 3, LT-08237 Vilnius

policy denies every other action for the user, if signed in without an MFA device. This policy allows any user to login for the first time, and set their own MFA device.

Give the policy a name and finalize its creation.

New User Creation

Navigate to **Users** section, under the **IAM** service, and add a new user with the following options:

1. Name: <username>
2. AWS Credential Type: autogenerated password that should be changed on first signed in for the AWS Management Console.
3. Under the permissions section, navigate to "Attach existing policies directly", search for the name of the policy created previously, and add it to the user.
4. Attach any other policies as well, giving the user desired permissions.
5. Leave the remaining options as defaults, and create the user.
6. A password will be generated. Use this password to login to the console with the new user.

MFA setup and Validation

In order for the user to be able to perform any action he should first:

1. Login to the AWS management console using the new username. For the first time, he will be able to login using only the password. Moreover, he will be asked to change the password.
2. To setup MFA, navigate to the dashboard of the **IAM** section. The dashboard will be filled with permission error messages. Perform the steps from the instructions on how to set up MFA. The MFA Device name must be the same as the username.
3. Sign out, and sign back in. This time, he will be prompted to enter the code from the authentication device.