Tworzenie grupy dla administratorów posiadających MFA

Aby dodatkowo podnieść bezpieczeństwo konta, wprowadzimy wymóg korzystania z MFA przez użytkowników z wysokimi uprawnieniami.

1. Przejdź do usługi IAM i z menu po lewej stronie wybierz `Policies`
2. Naciśnij przycisk `Create policy`
3. Polityki można tworzyć za pomocą edytora wizualnego lub jako pliki json. Otwórz zakładkę JSON i wklej poniższy kod:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "aws:MultiFactorAuthPresent": true
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:ChangePassword",
                "iam:GetLoginProfile",
                "iam:ListMFADevices",
                "iam:CreateLoginProfile",
                "iam:EnableMFADevice"
            ],
            "Resource": [
                "arn:aws:iam::*:user/${aws:username}"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreateVirtualMFADevice"
            ],
            "Resource": [
                "arn:aws:iam::*:mfa/${aws:username}"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
```

```
                "iam:GetAccountPasswordPolicy",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Teraz wykonanie działań na zasobach będzie możliwe tylko wtedy, gdy użytkownik użyje MFA do uwierzytelnienia się.

4. Przejdź do `Tags` a następnie do `Review`
5. Wpisz nazwę polityki: `AdminAccessWithMfa` lub `admin-access-with-mfa`
6. Dodaj opis polityki
7. Naciśnij `Create`

Następnie przypisz nową politykę do nowej grupy i przenieś użytkowników z wysokimi uprawnieniami do tej grupy:

8. Przejdź do zakładki `User groups`
9. Utwórz nową grupę `AdministratorsWithMfa`
10. Przejdź do `Add permissions` i dodaj utworzoną właśnie politykę
11. Przejdź do zakładki Users, naciśnij `Add users` i dodaj do grupy użytkowników o najwyższych uprawnieniach. Jednocześnie usuń ich z grupy `Administrators` (lub innej, do której jest przypisana polityka zezwalająca na wszystkie działania, ale niewymuszająca stosowania MFA).

Używanie długoterminowych kluczy programistycznych (Access Keys) powinno być możliwe tylko dla użytkowników posiadających aktywne MFA i po wdrożeniu tego zabezpieczenia.

Testowanie

1. Utwórz użytkownika
2. Dodaj go do grupy `AdministratorsWithMfa`
3. Zaloguj się jako użytkownik
4. Zmień hasło
5. Przejdź do usługi IAM
6. Zobaczysz szereg komunikatów wskazujących na brak uprawnień do wyświetlenia niektórych zasobów - to znaczy, że polityka działa
7. Dodaj MFA
8. Wyloguj się
9. Zaloguj się ponownie
10. Po dodaniu MFA komunikaty o braku uprawnień powinny zniknąć

Praca w CLI z użyciem tej polityki

Najpierw skonfiguruj AWS CLI.

Aby używać MFA w konsoli AWS trzeba "przesiąść" się z używania stałych poświadczeń na poświadczenia tymczasowe. Przygotuj ARN twojego MFA (znajdziesz go w konsoli AWS w miejscu, gdzie dodaje się urządzenie mfa).

Są 2 opcje:

Mniej wygodna

Użyj polecenia:

```
aws sts get-session-token \
    --serial-number $ARN_OF_MFA_DEVICE \
    --token $TOKEN_FROM_MFA_DEVICE \
    --output json \
    --profile $PROFILE_NAME
```

W wyniku tej operacji otrzymasz zestaw poświadczeń.

```
{
    "Credentials": {
        "SecretAccessKey": "secret-access-key",
        "SessionToken": "temporary-session-token",
        "Expiration": "expiration-date-time",
        "AccessKeyId": "access-key-id"
    }
}
```

Ustaw je jako zmienne środowiskowe:

```
export AWS_ACCESS_KEY_ID=example-access-key-as-in-previous-output
export AWS_SECRET_ACCESS_KEY=example-secret-access-key-as-in-previous-output
export AWS_SESSION_TOKEN=example-session-token-as-in-previous-output
```

Po godzinie poświadczenia wygasną i trzeba będzie je odnowić.

Testowanie: Wykonaj dowolne polecenie, do którego użytkownik przypisany do profilu ma uprawnienia (np. `aws s3 ls`)

Więcej informacji

Bardziej wygodna - dla zaawansowanych

- Zainstaluj narzędzie `awsume` - zgodnie z informacjami na tej stronie: awsume
- W folderze ~/.aws/config pod Twoim profilem dodaj wiersz:

```
mfa_serial=$ARN_OF_MFA_DEVICE
```

- Użyj polecenia: `source awsume PROFILE_NAME` Zostaniesz poproszony o podanie tokena z urządzenia MFA.

- Testowanie: Wykonaj dowolne polecenie, do którego użytkownik przypisany do profilu ma uprawnienia (np. `aws s3 ls`)