Integration von Amazon Web Services mit DoubleClue via SAML

1. Einführung

Diese Dokumentation ist für Nutzer von Amazon Web Services (AWS) gedacht, die möchten, dass sich ihre Mitarbeiter per DoubleClue Multi-Faktor-Authentifizierung (MFA) unter der Verwendung von SAML 2.0 in AWS einloggen. Für weitere Informationen zu diesem Produkt besuchen Sie bitte https://aws.amazon.com/

Anforderungen:

- AWS Root-Benutzeraccount
- Installation des DoubleClue Enterprise Management-Systems (DCEM)

2. Vorbereitung von DCEM als Identitäts-Provider

Um DCEM als Identitäts-Provider vorzubereiten, schlagen Sie bitte in Kapitel 12 des DCEM-Handbuchs („DCEM_Manual_DE.pdf“) nach.

3. Einrichtung von Amazon Web Services

1. Loggen Sie sich in die AWS Root-Benutzerkonsole auf https://aws.amazon.com/ ein.
2. Gehen Sie zu „Services“ > „IAM“ (unter „Security, Identity & Compliance“).
3. Wählen Sie aus dem Menü auf der linken Seite „Identity Providers“ aus.
4. Klicken Sie auf „Create Provider“.
5. Wählen Sie „SAML“ als „Provider Type“ aus.
6. Geben Sie einen Provider-Namen Ihrer Wahl ein, z.B. „DoubleClue“.
7. Laden Sie die IdP-Metadaten-Datei, welche Sie während des SAML-Setups heruntergeladen haben, bei „Metadata Document“ hoch (siehe Kapitel 12.1.4 des DCEM-Handbuchs, „DCEM_Manual_DE.pdf“).
8. Klicken Sie auf „Next Step“.
9. Klicken Sie auf „Create“.
10. Klicken Sie in der Liste auf Ihren neu erstellten Provider und kopieren Sie die „Provider ARN“ für zukünftigen Gebrauch.
11. Wählen Sie aus dem Menü auf der linken Seite „Roles“ aus.
12. Klicken Sie auf „Create Role“.

13. Wählen Sie „SAML 2.0 federation“ bei „Select type of trusted entity“ aus.
14. Wählen Sie als “SAML provider” denjenigen Provider aus, den Sie gerade erstellt haben.
15. Wählen Sie „Allow programmatic and AWS Management Console access“.
16. Klicken Sie auf “Next: Permissions”.
17. Klicken Sie auf „Next: Review“.
18. Geben Sie einen Rollennamen Ihrer Wahl ein, z.B. „dcuser“.
19. Klicken Sie auf „Create role“.
20. Klicken Sie in der Liste auf Ihre neu erstellte Rolle und kopieren Sie die „Role ARN“ für zukünftigen Gebrauch.

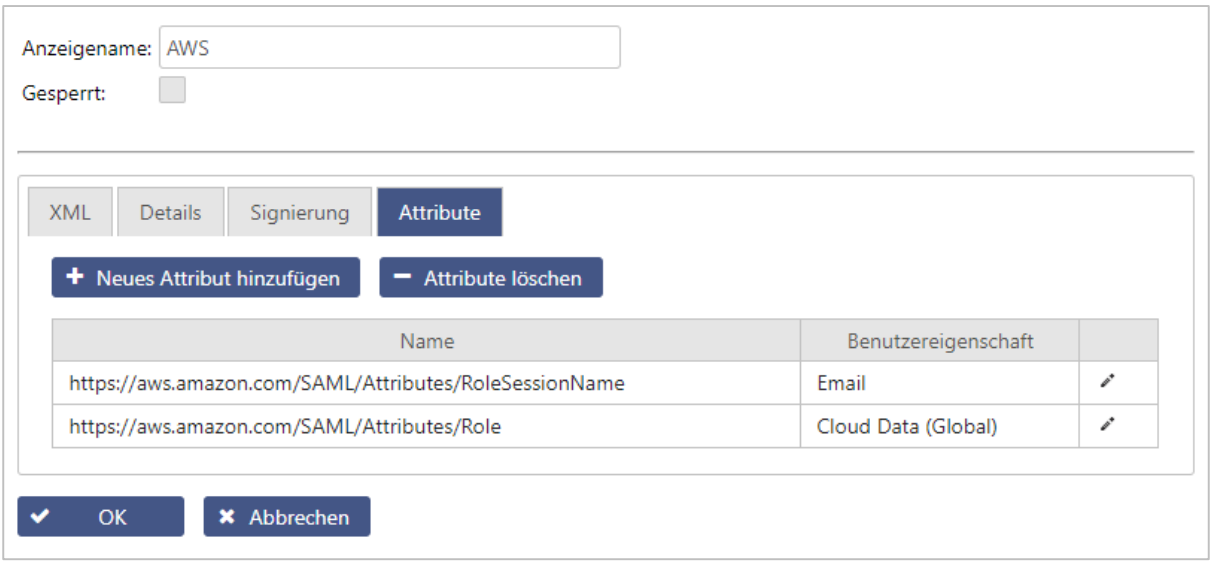
4. Einrichtung von Amazon Web Services als Service-Provider für DCEM

Option 1: Verwendung der voreingestellten Konfiguration

1. Gehen Sie in DCEM zum Hauptmenüpunkt „SAML“, Untermenü „SP-Metadaten“.
2. Klicken Sie auf „Hinzufügen“.
3. Wählen Sie aus dem Dropdown-Menü „AWS“ aus und klicken Sie dann auf „Fortfahren“.
4. Klicken Sie auf „OK“.

Option 2: Verwendung einer benutzerdefinierten Konfiguration

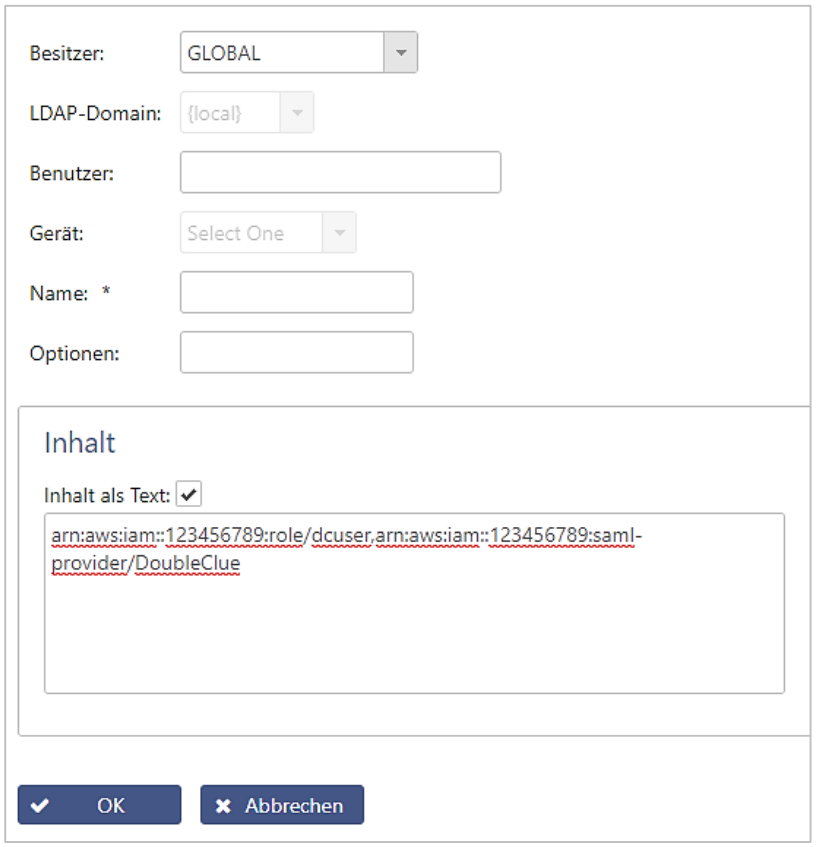
1. Laden Sie die XML-Datei unter https://signin.aws.amazon.com/static/saml-metadata.xml herunter.
2. Gehen Sie in DCEM zum Hauptmenüpunkt „SAML“, Untermenü „SP Metadaten“.
3. Klicken Sie auf „Hinzufügen“.
4. Wählen Sie aus dem Dropdown-Menü „Benutzerdefiniert“ aus und klicken Sie dann auf „Fortfahren“.
5. Laden Sie die heruntergeladene Datei mittels des „Upload“-Buttons hoch.
6. Gehen Sie zum Tab „Attribute“.
7. Klicken Sie in der Zeile, welche den „RoleSessionName“ enthält, auf das Bleistift-Symbol und ändern Sie die „Benutzereigenschaft“ zu „Email“. Klicken Sie auf das Häkchen-Symbol, um die Änderung zu speichern.
8. Wiederholen Sie das Ganze für „Role“, aber wählen Sie als „Benutzereigenschaft“ „Cloud Data (Global)“.
9. Klicken Sie auf „OK“.



Nach jeder Option:

1. Gehen Sie zum Hauptmenüpunkt „Identity-Management“, Untermenü „Cloud-Data“.
2. Klicken Sie auf „Hinzufügen“.
3. Wählen Sie „GLOBAL“ bei „Besitzer“.
4. Geben Sie https://aws.amazon.com/SAML/Attributes/Role bei „Name“ ein.
5. Setzen Sie einen Haken neben „Inhalt als Text“, falls er nicht schon gesetzt ist.
6. Fügen Sie die ARN-Werte, die Sie in Kapitel 3 gespeichert haben, im folgenden Format ein:

<role_arn_from_3(2nd value)>,<provider_arn_from_3(1st value)>



7. Klicken Sie auf „OK“.

AWS ist nun als Service-Provider für DCEM registriert.