ITSENSE

SWISS MADE IAM

Willkommen im IAM-Circle!

abraxas

ti&m

COPEBIT

white rabbit Communications

netzmedien

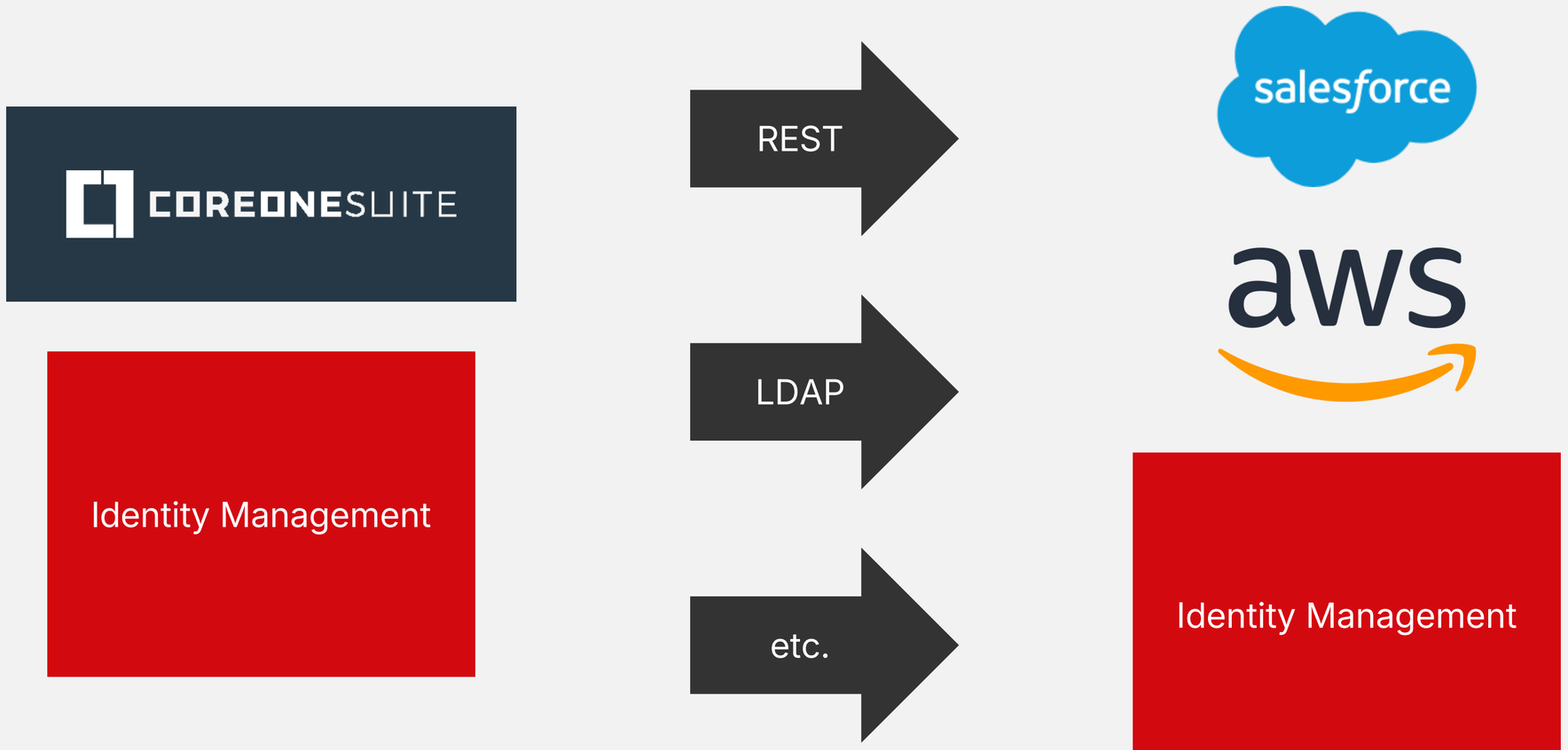
#8

#Fokusthema heute

SCIM: Universelle Provisionierungs-Schnittstelle oder unterschätzter Alptraum?

ITSENSE

Problemstellung: Schnittstellen Benutzerverwaltung



Beispiel Microsoft Active Directory – LDAP

```
using System;
using System.DirectoryServices;

class Program
{
    static void Main()
    {
        string ldapPath = "LDAP://OU=Users,DC=example,DC=com"; // Change to your AD structure
        string username = "NewUser";
        string password = "P@ssw0rd123"; // Set a strong password

        try
        {
            using (DirectoryEntry entry = new DirectoryEntry(ldapPath, "adminUser", "adminPassword")) // Change to your AD admin credentials
            {
                DirectoryEntry newUser = entry.Children.Add($"CN={username}", "user");
                newUser.Properties["samAccountName"].Value = username;
                newUser.Properties["userPrincipalName"].Value = $"{username}@example.com"; // Change domain accordingly
                newUser.Properties["givenName"].Value = "John";
                newUser.Properties["sn"].Value = "Doe";
                newUser.Properties["displayName"].Value = "John Doe";
                newUser.Properties["mail"].Value = "john.doe@example.com";
                newUser.Properties["userAccountControl"].Value = 0x200; // Enable the account
                newUser.CommitChanges();

                // Set the password
                newUser.Invoke("SetPassword", password);
                newUser.CommitChanges();

                // Enable the account
                int val = (int)newUser.Properties["userAccountControl"].Value;
                newUser.Properties["userAccountControl"].Value = val & ~0x2; // Remove the 'account disabled' flag
                newUser.CommitChanges();

                Console.WriteLine("User created successfully.");
            }
        }
        catch (Exception ex)
        {
            Console.WriteLine("Error: " + ex.Message);
        }
    }
}
```

ITSENSE

Beispiel Microsoft Active Directory – Directory Services

```
using System;
using System.DirectoryServices.AccountManagement;

class Program
{
    static void Main()
    {
        string domain = "example.com";  // Change this to your domain
        string container = "OU=Users,DC=example,DC=com"; // Change to your AD structure
        string username = "johndoe";
        string password = "P@ssw0rd123";
        string firstName = "John";
        string lastName = "Doe";
        string email = "johndoe@example.com";

        try
        {
            using (PrincipalContext context = new PrincipalContext(ContextType.Domain, domain, container))
            {
                UserPrincipal user = new UserPrincipal(context);
                user.SamAccountName = username;
                user.UserPrincipalName = $"{username}@{domain}";
                user.GivenName = firstName;
                user.Surname = lastName;
                user.DisplayName = $"{firstName} {lastName}";
                user.EmailAddress = email;
                user.SetPassword(password);
                user.Enabled = true;
                user.ExpirePasswordNow(); // Force password change on first login
                user.Save();

                Console.WriteLine($"User {username} created successfully in AD.");
            }
        }
        catch (Exception ex)
        {
            Console.WriteLine("Error creating user: " + ex.Message);
        }
    }
}

```

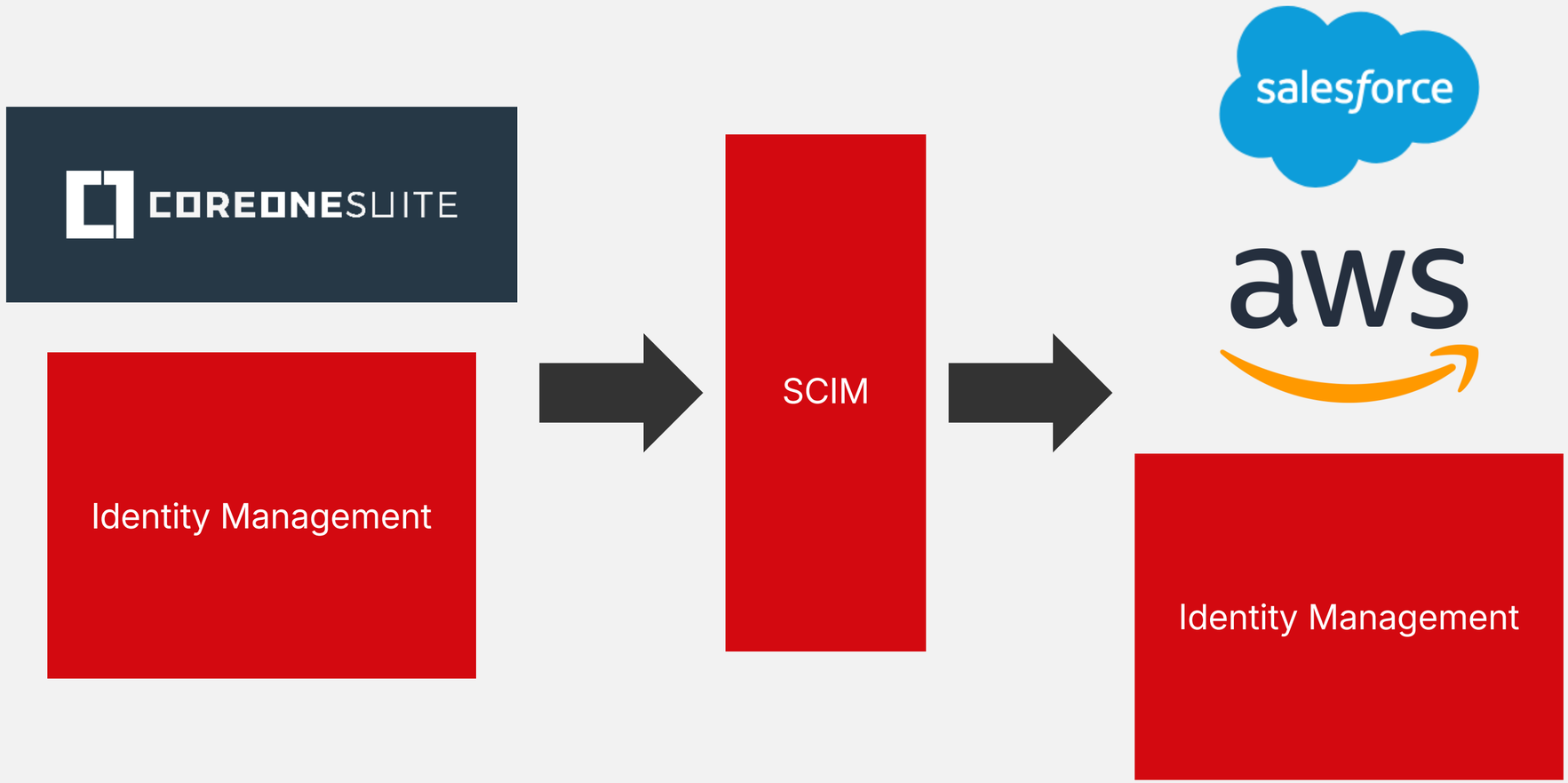
ITSENSE

Beispiel Microsoft Entra ID – Graph API

```
using System;
using System.Net.Http;
using System.Threading.Tasks;
using Microsoft.Graph;
using Microsoft.Identity.Client;

class Program
{
    static async Task Main(string[] args)
    {
        var clientId = "YOUR_CLIENT_ID";
        var tenantId = "YOUR_TENANT_ID";
        var clientSecret = "YOUR_CLIENT_SECRET";

        var graphClient = GetGraphClient(clientId, tenantId, clientSecret);

        var newUser = new User
        {
            AccountEnabled = true,
            DisplayName = "John Doe",
            UserPrincipalName = "johndoe@example.com",
            MailNickname = "johndoe",
            PasswordProfile = new PasswordProfile
            {
                ForceChangePasswordNextSignIn = true,
                Password = "P@ssw0rd123"
            }
        };

        try
        {
            var createdUser = await graphClient.Users.Request().AddAsync(newUser);
            Console.WriteLine($"User created successfully: {createdUser.Id}");
        }
        catch (Exception ex)
        {
            Console.WriteLine("Error creating user: " + ex.Message);
        }
    }

    static GraphServiceClient GetGraphClient(string clientId, string tenantId, string clientSecret)
    {
        var confidentialClientApplication = ConfidentialClientApplicationBuilder
            .Create(clientId)
            .WithClientSecret(clientSecret)
            .WithAuthority(new Uri($"https://login.microsoftonline.com/{tenantId}"))
            .Build();

        var authProvider = new DelegateAuthenticationProvider(async (requestMessage) =>
        {
            var authResult = await confidentialClientApplication.AcquireTokenForClient(new[] { "https://graph.microsoft.com/.default" }).ExecuteAsync();
            requestMessage.Headers.Authorization = new System.Net.Http.Headers.AuthenticationHeaderValue("Bearer", authResult.AccessToken);
        });

        return new GraphServiceClient(authProvider);
    }
}

```

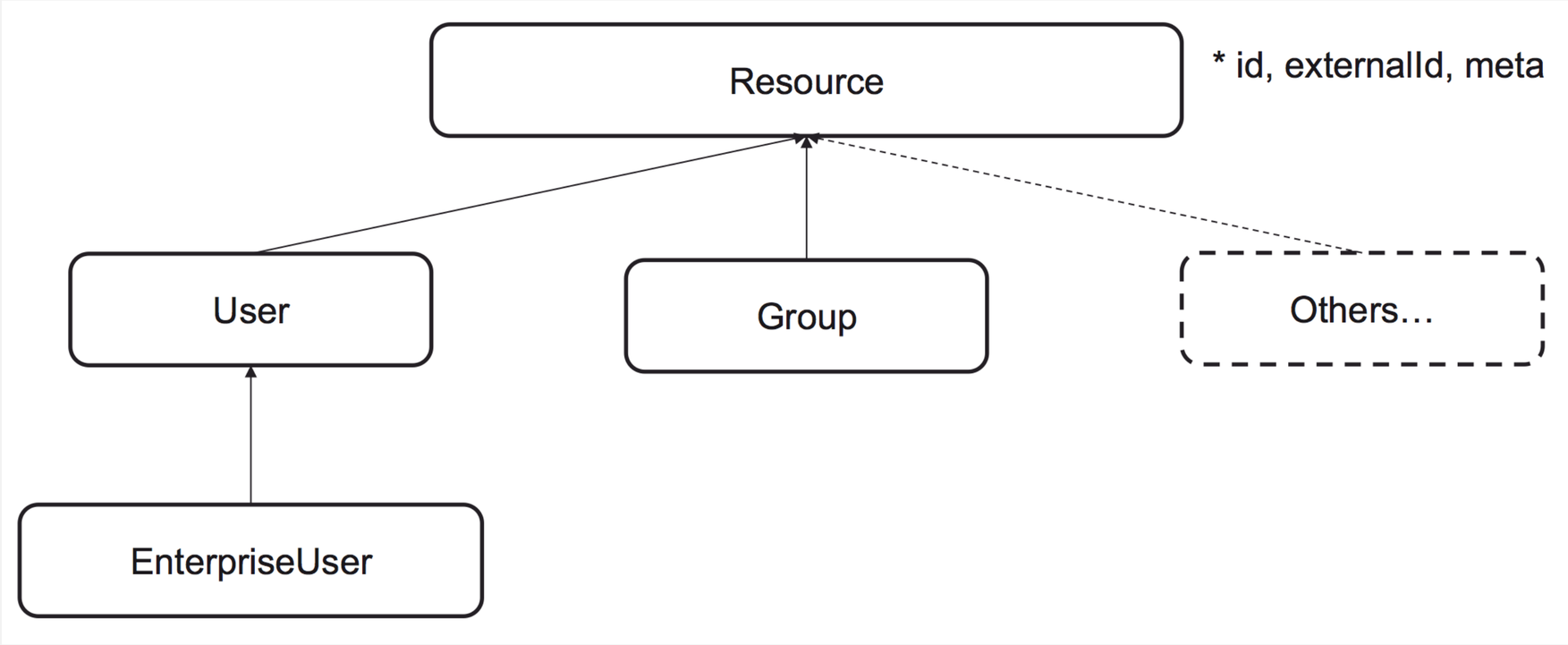
ITSENSE

Was ist System for Cross-domain Identity Management (SCIM)?



ITSENSE

Wie ist SCIM aufgebaut?



ITSENSE

SCIM 1.1 vs. SCIM 2.0

	SCIM 1.1	SCIM 2.0
Veröffentlichungsjahr	2011	2015
Standardisierung	Kein offizieller IETF-Standard	IETF-Standard (RFC 7642, RFC 7643, RFC 7644)
Protokoll	REST-basiert, unterstützt XML und JSON	Vollständig RESTful, nur JSON
Schema	Statisch, begrenzte Erweiterbarkeit	Flexibler und erweiterbar
Endpoints	Unterschiedliche Endpunkte für verschiedene Operationen	Einheitlicher, ressourcenorientierter Ansatz
Filterung	Eingeschränkte Filtermöglichkeiten	Erweiterte Filterung mit komplexeren Abfragen
Massenoperationen (Bulk)	Nicht klar definiert	Unterstützt über den Bulk-Endpunkt
Teilaktualisierung (Patch)	Eingeschränkt oder nicht vorhanden	Unterstützt vollständige PATCH-Operationen
Gruppenverwaltung	Grundlegend	Verbesserte Gruppen- und Rollenverwaltung
Sicherheit	Basis-Authentifizierung	Verbesserte Sicherheit mit OAuth 2.0 und Bearer-Tokens

ITSENSE

Schema – Standard Schema

urn:ietf:params:scim:schemas:core:2.0:User

Attribut	Beschreibung	Beispielwert
id	Eindeutige Benutzer-ID	"aabbcc-12345"
userName	Benutzername (Pflichtfeld)	"jdoe"
name	Struktur für Namen	{ "givenName": "John", "familyName": "Doe" }
displayName	Anzeigename	"John Doe"
nickName	Spitzname	"Johnny"
profileUrl	URL zum Benutzerprofil	"https://example.com/jdoe"
title	Titel/Position	"Software Engineer"
userType	Benutzer-Typ (z. B. employee, contractor)	"employee"
preferredLanguage	Bevorzugte Sprache	"de-DE"
locale	Lokale Einstellungen	"de"
timezone	Zeitzone	"Europe/Berlin"
active	Ob Benutzer aktiv ist	true oder false
emails	E-Mail-Adressen (Liste)	[{"value": "jdoe@example.com", "type": "work"}]
phoneNumbers	Telefonnummern (Liste)	[{"value": "+49123456789", "type": "mobile"}]
addresses	Adressen (Liste)	[{"streetAddress": "Musterstraße 1", "locality": "Berlin", "postalCode": "10115"}]
groups	Zugehörige Gruppen	[{"value": "admin-group", "display": "Administrators"}]
entitlements	Berechtigungen	["premium-user"]
roles	Rollen im System	["admin"]
meta	Metadaten zur Ressource	{"resourceType": "User", "created": "2023-01-01T12:00:00Z"}

urn:ietf:params:scim:schemas:core:2.0:Group

Attribut	Beschreibung	Beispielwert
id	Eindeutige Gruppen-ID	"abcd-1234"
displayName	Anzeigename der Gruppe (Pflichtfeld)	"Admins"
members	Liste der Gruppenmitglieder (Benutzer oder andere Gruppen)	[{"value": "12345", "type": "User"}]
externalId	Externe ID für die Synchronisierung mit anderen Systemen	"ext-5678"
meta	Metadaten zur Gruppe (z. B. Erstellungszeitpunkt)	{"resourceType": "Group", "created": "2023-01-01T12:00:00Z"}

Schema – Erweitertes Schema

Mögliche Schema Erweiterungen:

1. Attribute zu vorhandenen Ressourcen hinzufügen
2. Eigene Ressourcen erstellen → eigene Objekte, eigene Endpunkte

Beispiel:

Die Attribute **birthdate** und **preferredOfficeLocation** sollen erweitert werden.

Definition des Schemas:
urn:ietf:params:scim:schemas:extension:custom:2.0:User


```
{
  "schemas": [
    "urn:ietf:params:scim:schemas:core:2.0:User",
    "urn:ietf:params:scim:schemas:extension:custom:2.0:User"
  ],
  "id": "12345",
  "userName": "jdoe",
  "name": {
    "givenName": "John",
    "familyName": "Doe"
  },
  "emails": [
    {
      "value": "jdoe@example.com",
      "type": "work"
    }
  ],
  "urn:ietf:params:scim:schemas:extension:custom:2.0:User": {
    "birthDate": "1990-01-15",
    "preferredOfficeLocation": "Berlin"
  }
}
```

Demo SCIM

SCIM-Server

- https://scim.dev
- Lokal Microsoft SCIM Example

SCIM-Client

- Postman

ITSENSE

Vorteile

- **Standardisierung:**
  Schnelle Anbindung von zusätzlichen SCIM-Systemen.
- **Offenere Standard:**
  Wird von einigen Anbietern unterstützt.
- **Skalierbarkeit:**
  Der Standard ist auf grosse Datenmengen ausgelegt.
- **Erweiterbar:**
  Der Standard kann erweitert werden, mit zusätzlichen Schemas.

ITSENSE

Nachteile

- **Komplexität der Implementierung:**
  Der Standard ist Komplex, bestehende System müssen angepasst werden.
- **Flexibler Standard:**
  Nicht alle Endpoints und Funktionen müssen implementiert werden,
  daher sind auch nicht alle SCIM-Systeme gleich.
- **Verbreitung:**
  Nicht alle Systeme unterstützen SCIM, noch werden sie dies jemals tun.

Workshop – Einsatz SCIM in euren Unternehmen

Gruppenarbeit

Wählt zu Beginn den Moderator, der die Resultate der Community präsentiert.

Zeit

15 Min. Vorbereitung, 15 Min. Vorstellung Resultate

Fragestellungen

1. Wo besteht in eurem Unternehmen Bedarf an der Verwaltung von Identitäten und Gruppen?
2. Welche Schnittstellen bieten eure bestehenden Systeme?
3. In welchen Szenarien seht ihr Potenzial für den Einsatz von SCIM?
4. Welche Chancen und Risiken ergeben sich für euch durch die Nutzung von SCIM?

ITSENSE

ITSENSE

Stay tuned, stay secure!

SWISS MADE IAM

abraxas

ti&m

COPEBIT

white rabbit Communications

netzmedien

#8