

Mitten in der dynamischen Metropolregion Ruhrgebiet, im Herzen Europas gelegen, ist die Ruhr-Universität-Bochum (RUB) mit ihren 21 Fakultäten Heimat von 42.600 Studierenden aus über 130 Ländern. Sie hat einen starken Fokus auf Naturwissenschaften, aber auch Studierende können sich Student*innen natürlich auch für einen Abschluss in einem der vielen geisteswissenschaftlichen Fächern entscheiden.

ORGANISATION

Ruhr Universität Bochum

BRANCHE

Higher Education

WEB

www.ruhr-uni-bochum.de

CASE STUDY

ÜBERBLICK

Die Ruhr-Universität-Bochum wünschte sich eine moderne IdM-Lösung, die deren in die Jahre gekommene Eigenentwicklung ablösen sollte.

Herausforderung: Beim Ersatz des Vorgängersystems galt es, die bisherige hochspezifische Funktionalität beizubehalten.

Vorgehensweise: Es wurden mehrere Instanzen von midPoint aufgesetzt, um zunächst das vorhandene System zu ergänzen. Danach wurde mit der Übergangsphase begonnen.

Ergebnis: Die Universität betreibt inzwischen die neue midPoint-Instanz sowie das alte System parallel. Zu einem späteren Zeitpunkt soll midPoint schließlich das alte System vollständig ersetzen.

DAS ZIEL

Das von der Universität selbst entwickelte und inzwischen veraltete IdM-System sollte ersetzt werden, sodass es den Anforderungen modernen Identitätsmanagements wieder entspricht.

DIE HERAUSFORDERUNG

Schnell wurde ersichtlich, dass die beiden IdM-Systeme über einen längeren Zeitraum parallel betrieben werden müssen. Die Herausforderung bestand hierbei nicht nur darin, die einmalige

Migration der Daten aus dem Altsystem zu realisieren, sondern auch die permanente Synchronisation der Daten nach midPoint sicherzustellen. Diese Vorgehensweise war unter anderem deshalb notwendig, da nicht alle Prozesse gleichzeitig in midPoint überführt werden konnten. Stattdessen wurde der Übergang über einen längeren Zeitraum durchgeführt. Des Weiteren war es notwendig, einen neuen OpenLDAP-Cluster einzurichten, der ausschließlich von midPoint provisioniert werden durfte. Da das alte System auf einer sehr verschachtelten Datenbankstruktur basierte, war der Anschluss des Systems und die Provisionierung von Daten nach OpenLDAP eine der größten Problemstellungen im frühen Projektverlauf.

DIE VORGEHENSWEISE

Um die Übergangsphase einzuleiten ohne Datenverluste oder einen Funktionsausfall zu riskieren, stellte die DAASI International drei midPoint-Instanzen zur Verfügung, jeweils eine Test- bzw. Staging-Instanz sowie die produktive Installation. Zunächst mussten einige Ressourcendienste neu konfiguriert werden, sodass sie die relevanten Informationen aus verschiedenen Datenbanktabellen des alten Systems beziehen konnten. Dies schuf die Grundlage für die Verbindung von midPoint mit dem alten IdM-System. Um den Informa-

tionsumfang für das neue Identitätsmanagement zu erweitern, wurden zusätzliche Datenquellen konfiguriert und an midPoint angebunden. Anschließend mussten mehrere Archetypen und Rollen (inkl. Meta-Rollen) konfiguriert werden, um eine bedingte Provisionierung zu realisieren. Dieser Schritt ermöglichte es zudem, die Quelldaten in verschiedene Kategorien einzuordnen. Schließlich wurde OpenLDAP als Zielsystem angeschlossen. Prozesse wie unter anderem die komplexe Zuweisung von Rechten basierend auf Organisationsstruktur, Mitgliedschaften und Account Management wurden umgesetzt. Zuletzt konnten viele weitere Systeme wie das Active Directory erfolgreich angebunden werden.

AUSBLICK

Die RUB und die DAASI International sind sehr optimistisch, das finale Ziel der vollständigen Ablösung des alten Systems in absehbarer Zeit zu erreichen. Derzeit betreibt die Universität eine funktionierende midPoint-Instanz produktiv und parallel zu ihrem alten IdM-System, das schließlich vollständig ersetzt werden soll. Bei Störungen jeglicher Art können DAASI International als Second-Level-Support-Provider und Evolveum als Third-Level-Service-Provider schnell helfend eingreifen.

