

nevisIDM – Identity Management

Kurzbeschreibung

Die Identitätsmanagement-Lösung nevisIDM von NEVIS ermöglicht die flexible, benutzerspezifisch anpassbare und zentrale Verwaltung von Benutzern, Anwendungen, Rollen und Berechtigungen.

Vorteile

nevisIDM verwaltet die Benutzer, Rollen und Berechtigungen Ihrer Geschäftsanwendungen an zentraler Stelle. Diese **zentrale Kontrolle und Verwaltung der Daten** macht Ihr System **sicherer** und **senkt die Kosten**. Darüber hinaus eröffnet es die Möglichkeit eines **unternehmensweiten Single Sign-on** (Einmalanmeldung). nevisIDM unterstützt neben vielen Arten von Benutzer-Zugangsdaten auch die **Einführung starker Authentisierungsmechanismen**.

Das ausgefeilte Datenmodell öffnet den Weg für ein **feingranuliertes Autorisierungskonzept**, das „Gewaltenteilung“ unterstützt und somit **die Sicherheit Ihres Systems verbessert**. Die zusätzliche Komponente nevisWorkflow erleichtert die Aufgabenteilung noch weiter. Sie lässt auch Self Services (Selbstbedienung) der Benutzer zu, die beispielsweise eigenständig ihre Passwörter zurücksetzen oder ihre Profile einsehen können.

Der vollständige Auditpfad gestattet die **komplette Nachverfolgung aller Benutzeraktionen**, was dazu beiträgt, **Compliance-Anforderungen zu erfüllen**. Ein weiteres Merkmal ist die Fähigkeit von nevisIDM, mit **Multi-Tenant-Situationen mit vollständig getrennten Benutzergruppen** umzugehen. Sie benötigen damit nur eine einzige Identitätsmanagement-Lösung, um mehrere Benutzerpopulationen gleichzeitig abzudecken.

Worum geht es?

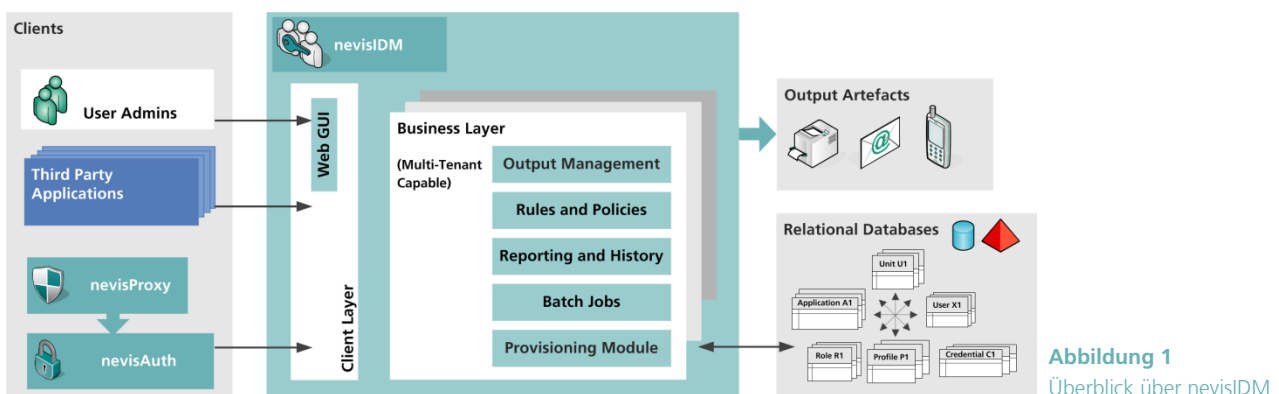


Abbildung 1
Überblick über nevisIDM

Identitätsmanagement (IM) ist die Verwaltung individueller Identitäten, ihrer Authentisierung, Autorisierung, Rollen und Privilegien innerhalb der Grenzen eines Systems und Unternehmens oder über diese Grenzen hinweg. Ziel des Identitätsmanagements ist es, die Sicherheit und Produktivität zu steigern und gleichzeitig Kosten, Ausfallzeiten und Aufwand für sich wiederholende Aufgaben zu senken.

Gemeinsam mit nevisProxy und nevisAuth gestattet nevisIDM die Einführung eines hochgradig ausgefeilten, hochmodernen Systems für das Identitäts- und Zugangsmanagement. *nevisProxy* stellt innerhalb dieses Systems den alleinigen Zugangspunkt zu Ihren Geschäftsanwendungen im Backend dar und kontrolliert damit den gesamten ankommenden und abgehenden HTTP-Datenverkehr. *nevisAuth* kümmert sich um die Identifikation und Authentisierung der Benutzer. An dieser Stelle kommt nevisIDM ins Spiel: Es stellt alle Informationen zur Verfügung, die nevisAuth benötigt, um Benutzer zu identifizieren und zu authentisieren. Dies schliesst auch die Autorisierung der Benutzer ein, in deren Rahmen ihnen die richtigen

Berechtigungen und Rollen zugeordnet werden, die sie für die Arbeit mit der betreffenden Anwendung brauchen.

nevisIDM beinhaltet alle Prozesse und unterstützenden Tools, die für die Verwaltung Ihrer Anwendungs- und Benutzerdaten erforderlich sind, Rollen und Berechtigungen eingeschlossen. Das Produkt kann die verschiedensten Benutzer-Zugangsdaten verarbeiten, wie (Einmal-)Passwörter, Zertifikate, URL-Tickets, Sicherheitsfragen, mTANs oder Kerberos. Somit können Sie Ihre Geschäftsanwendungen mit starken Authentisierungsmechanismen schützen.

nevisIDM speichert alle Benutzer- und Anwendungsdaten in einer zuverlässigen Datenbank auf Grundlage eines hochentwickelten Datenmodells. Dieses Datenmodell definiert sämtliche zur Verfügung stehenden Dateninstanzen mit ihren Attributen sowie die Beziehungen zwischen den einzelnen Instanzen.

Für die Datenspeicherung können Sie die mitgelieferte oder Ihre eigene Datenbank verwenden. Ausserdem unterstützt nevisIDM die Bereitstellung von

Benutzerdaten an externe Datenbestände wie LDAP-Verzeichnisse.

Die Web-Schicht der Anwendung enthält alle für die Erstellung und Aktualisierung der Daten nötigen Schnittstellen. Für den Informationsaustausch mit Anwendungen (Dritter) unterstützen diese Schnittstellen unter anderem das Simple Object Access

Protocol (SOAP). Demnächst werden auch Representational State Transfers (REST) unterstützt werden. Volltextsuchen mittels des Query REST Service sind bereits jetzt möglich.

Die Zugangskontrollfunktionen der Unternehmens-Kernschicht garantieren, dass der Benutzer nur Operationen ausführen kann, zu denen er autorisiert ist.

Web-Benutzerschnittstelle

Abbildung 2
nevisIDM-
Web-Anwendung

Die Anwendungsadministratoren verwalten die in nevisIDM angelegten Instanzen über dessen leistungsfähige grafische Benutzerschnittstelle. Dies umfasst nicht nur das Erstellen und Ändern von Benutzer- und Anwendungsinstanzen, sondern auch eine Reihe weiterer Funktionen:

- Die *Unit* (Abteilungs)-Instanzen helfen Ihnen, die Verwaltung von Benutzerdaten an die Struktur Ihrer Organisation anzupassen. Dies vereinfacht die Zuweisung von Rollen und Berechtigungen und ermöglicht das Delegieren der Benutzerverwaltung.
- Die Möglichkeit, Richtlinien für die Zugangsdaten festzulegen, gestatten den Aufbau eines feingranulierten Authentisierungssystems. Sie könnten beispielsweise eine Richtlinie für ein *einfaches Passwort* und eine Richtlinie für ein *starkes Passwort* mit unterschiedlichen Anforderungen an die Länge des Passworts, die zu verwendenden Zeichen, die zulässige Häufigkeit des Zurücksetzens usw. festlegen. Welche der beiden Passwortrichtlinien für eine Anwendung im Backend

einzuhalten ist, hinge dann von den Sicherheitsanforderungen dieser Anwendung ab.

- Benutzerspezifisch anpassbare E-Mail- und SMS-Vorlagen helfen Ihnen, die Benutzer zu benachrichtigen, wenn beispielsweise ein Passwortwechsel ansteht. Bei entsprechender Einstellung können Nachrichten in verschiedenen Sprachen erstellt werden.
- Über das Suchfeld sind Volltextsuchen über sämtliche Benutzer-, Anwendungs-, Unit- und Client-Instanzen hinweg möglich, die in nevisIDM gespeichert sind.

Darüber hinaus bietet das Web-GUI die Möglichkeit der Selbstadministration, mit deren Hilfe die Benutzer Ihrer Anwendung(en) selbst ihre Profile einsehen oder ihre Passwörter ändern können.

Auf Wunsch können Sie das Erscheinungsbild der Web-Schnittstelle mit den passenden (Hintergrund-) Farben, Schriftarten und Logos an Ihr Corporate Design anpassen.

Sonstige Merkmale

- Fernadministration über die Web-Schnittstelle.
- Umsetzung Ihres Autorisierungskonzepts mittels Zuordnung der Benutzer zu Profilen und Rollen.
- Realisierung komplexer Prozesse mittels einer Workflow-Engine (nevisWorkflow).
- Gesammelter Import von Benutzerdaten über Excel-Dateien.
- Leistungsfähiges Ausgabe-Management (E-Mail, SMS, Anschreiben).
- Vereinfacht dank versionierter Speicherung von Dokumenten und sicherheitsrelevanten Ereignissen die Auditierbarkeit. Alle Zugangsrechte jederzeit vollständig auditierbar.