CzechIdM Features

Provisioning and automated synchronization

What would CzechIdM be without automation? Synchronization, i.e. data flow from source systems to the identity manager, is essential for every identity manager. In CzechIdM you can synchronize the following types of entities:

- identities (users) - we fully support identity synchronization with their contracts
- roles (privileges) - automatic synchronization of roles is a must if role settings are to vary in time - e.g. AD/LDAP groups
- organizations (org. trees) - we support tree structure synchronization to be able to represent organizational divisions, and place users in their working positions.

Synchronization is fully audited and supports multiple synchronizations for every entity. Synchronization can be started on demand, or as planned scheduled task.

Another essential data flow in almost all IdM deployments is provisioning. This involves data flow from IdM to managed systems. All entities that support synchronization can also be pushed to end systems via provisioning. Our robust provisioning implementation brings the following benefits:

- Fully audited provisioning queue - Every push operation and its result is audited and audit is available to admins via GUI.
- Retry mechanism - Queue pushes the data into managed systems. If the system encounters any problem or is simply offline, the data stays in a queue and keeps trying the operation again until the system is available.
- Read-only systems - If the system is in read-only mode, all operations are stored in a provisioning queue. An administrator can see changes, but nothing is sent. This is very useful for new managed system link-up and cutover, or debugging.

Detailed auditing

CzechIdM provides complete audit history of all entities in CzechIdM. The major audit features are:

- entity audit - all entity-related (identities,roles, treenodes etc...) changes are audited. Naturally, CzechIdM also keeps track of mutual relation changes - identity x role, identity x contracted position, etc.
- separate audit for identities - CzechIdM GUI has a special agenda that filters all changes on identities and their relations so that the administrator can work with it in a more convenient way, e.g. filter identities by user login
- provisioning audit - every operation with data sent to a managed system is audited in a provisioning queue audit
- synchronization audit - every synchronization run has its own audit history. Administrator can find the overall status of the synchronization as well as detail information about every synchronized entity.
- workflow audit - workflows (e.g. identity life cycle process) runs are documented, and their process is kept in workflow history available via GUI

- scheduled task history - every task run along with its process is kept in scheduled task history

Role-based access control

CzechIdM represents user's privilege in managed system as a role. From the CzechIdM point of view, there is no difference: the user has specific right in a managed system, is a member of a group of users (AD/LDAP) or has an account with basic access. All of that is represented by one CzechIdM entity - ROLE.

This paradigm is really effective and easy to understand. It allows IdM to apply general rules for roles management and distribution like automatic roles, roles requests approval, synchronization and provisioning.

Automatic roles

With CzechIdM you can automate role assignment process. You can link roles to organization structure (tree structure) in:

- roles agenda
- organizations agenda

If you link a role with the user's working position, this operation is subject to approval. Once an authorized person has approved the operation, from that time on all users placed in the working position get the role without approvement.

This also means they get the role without delay. This is essential if you require a new user (e.g. employee) to get access to managed systems on the very first working day.

Of course, the reverse process works the same way. When a user leaves their working position they lose their roles/access to systems immediately.

Web GUI

CzechIdM provides web interface for convenient work of users and administrators.

User Self-service

Users benefit from using CzechIdM especially in following classes of tasks:

- Password management - Password change or reset in CzechIdM as well as in managed systems.
- Role requests - Users can request for new roles (privileges) and access to managed systems. Requests are approved by entrusting users e.g. role owner or user's manager.
- Subordinates management - Managers can rule their subordinates and request for role change for them too.
- User Task agenda - entrusted users resolve the user task in CzechIdM GUI. The CzechIdM

notification system informs users about new tasks.

Administrator agenda

CzechIdM provides a wide variety of identity management features in its GUI. Most important ones are:

- Entity management - manage entities like identities, tree structures, scheduled tasks etc… Change their relations e.g. add roles to identities, setup entity synchronization and provisioning.
- Role management - define roles, manage the role approval workflow (who approves the role assignment), catalogue the roles, prepare the role synchronization and provisioning or set automatic roles to organization structure
- Account management - manage the users with their accounts in managed systems
- Systems management - define data sources, managed systems, data synchronization and provisioning, attributes set for each entity
- Passwords - define multiple passwords policies for managed systems.
- Modules - enhance CzechIdM functions by enabling additional modules
- Create your own notifications - manage notification templates for sms,email or websocket
- Manage scheduled tasks - plan the run of identity lifecycle processes and data synchronization
- Audit - have all the audit information at one place. CzechIdM uses time machine principle - all changes of its entities are stored as snapshots. GUI provides tool to see the differences of chosen snapshots.

RESTful API

RESTful API is the preferred communication API for CzechIdM. All application services are available via this API. It means that even the application frontend uses it for communicating with a backend. This approach has many advantages:

- REST is quick and flexible
- It is also widely used in many current applications
- one API brings the possibility of centralized audit of communication
- automatically documented endpoint documentation is available online
- build your own application frontend

See more in (online CzechIDM RESTful API doc).

Identity lifecycle processes

CzechIdM contains standardized lifecycle processes management for identities.

Default processes which provide basic automatic management of identities are as follows:

- Enabled contract - enable identity when its contracted position starts,
- End of contract - remove roles, disable identity if last contracted position ends,
- Contract exclusion - disable identity if contract is disabled, e.g. user started maternity leave.

All processes are implemented as long running tasks and operated by workflows. Thus:

- their start can be easily scheduled in LRT agenda,
- their progress and status can be monitored,
- their history is audited in workflow history agenda,
- new processes can be implemented and deployed easily.

In addition to these processes, it is worth mentioning that

- assignment
- change
- removal

of identity to work position (organization structure) is also supported in CzechIdM. It is managed by the automatic roles feature.

The implementation of standard processes can be enhanced, and new processes can be added to CzechIdM as well. More details about HR processes in CzechIdM can be found in Identity lifecycle processes of Administrator's guide.

A wide range of supported connectors

An identity manager is usually the central system in the company's systems hierarchy. So it should be easy to deploy the IdM system into existing IT environment with minimal changes to the current environment.

When communicating with other systems, CzechIdM uses their native API. This approach has a massive benefit in that there is usually no need to alter the systems. All you need to do is to choose the right connector from our many supported connectors. If there is no connector available for your system yet, we can develop a new one.

CzechIdM manages various systems like LDAP, MS AD, databases, Unix-like systems, file servers, HR systems, Helpdesk, Windows servers, MS Exchange, postfix, and many others.

Parallel organizational structures supported

CzechIdM is a robust identity manager and can deal with difficult organizational structures.

Imagine a situation when a company or organization, e.g. hospital, consists of five smaller regional hospitals or other detached workplaces with some elements of autonomy. Then there are, in fact, 5 organizations that have to be managed by CzechIdM, but it is desirable that users from one regional hospital are managed by their dedicated administrator within CzechIdM, who of course cannot manage users from other hospitals.

CzechIdM comes with the REALM paradigm. It can synchronize organizational structure from HR system(s), and it keeps them separate in 5 trees (like in our stated case above). Each tree then represents the organizational structure of one hospital. As a result, the mechanism of roles permissions can be used to grant access for administrators to only a specified tree and the users placed within it.

Authentication

CzechIdM offers several means of users' authentication. Users can authenticate locally or against some remote system. CzechIdM in its basic modules supports authentication against:

- LDAP
- MS Active Directory

The architecture of CzechIdM is prepared for adding other authentication methods just be implementing their protocol.

SSO support

Out of the box, CzechIdM supports HTTP basic authentication as an authentication method for SSO. We can make CzechIdM to authenticate agains MS AD (kerberos) using SSO.

CzechIdM Modules

CzechIdM is heavily modular. It means that the whole application - frontend and backend alike - is divided into modules. Some are really essential like CORE, ACC and IC and, in fact, constitutes the application itself.

Modularity brings many pluses:

- ease of deployment and use - one can install CzechIdM with essential modules really quickly. Then add only those modules one really needs.
- quick update/upgrade - you can update only specified modules
- clear configuration - every module has its own configuration properties
- project specific changes in a separate module - every project-specific implementation can be compiled in one projspec module. Thus you keep differences apart from the product in one place, and you can easily upgrade CzechIdM while your changes remain untouched.

Also, CzechIdM offers optional modules which include REG, OPENAM, PWD-RESET, CA.

Self registration module

CzechIdM is a powerful system for identity management. There are many ways of creating an identity, for instance through Synchronization or via REST API. However, those are more or less automatic ways of identity import.

Sometimes it is desirable to let the users register for themselves, say if you use CzechIdM for external contractors account management, or company customers accounts management. The user registration module enables the self-registration of the user with optional validation steps - email validation, entrusting user approval. The module consists of GUI module - registration form and

backend module - logic and notifications.

Read more on how to setup and use the module in administrator's guide.

Password reset module

Users can authenticate themselves in CzechIdM with their login and password. The password is, of course, a secret information. It happens sometimes that user does not remember the password and cannot log in to CzechIdM. The pwd-reset module provides GUI form that is available via a link from CzechIdM login page and users can use it to initialize the lost password reset process. The module handles the complete lost password process:

- Process user data from reset password form
- Generate email notification - with a unique link to new password set form.
- Set new password to managed systems - sets the password to all managed systems that support it (including CzechIdM itself).

Read more about the module setup and usage.

OpenAM authentication and SSO module

OpenAM authentication and SSO module offer the integration with OpenAM - centralized access manager. The integration serves for:

- CzechIdM to OpenAM authentication
- SSO
- user data exchange via REST API

Read more about the module setup and usage.

Certificate management module

The module provides a set of tools to work with certificates:

- certificate request management
- certificate revocation
- certificate validity check
- key management
- multiple CA servers support
- REST API endpoint
- GUI module to CzechIdM
- CA Drivers - ensures the communication with specific CA

The module is dependent on particular CA implementation (try out CAW). It uses a set of drivers to communicate with CA.

Certificates modul documentation.

SCIM - System for Cross-domain Identity Management

The System for Cross-domain Identity Management (SCIM) specification is designed to make managing user identities in applications and services easier. SCIM - the open API based on REST for managing identities, by defining a schema for representing users and groups for all the necessary CRUD operations.

CzechIDM Scim module exposes interface by the SCIM 2.0 specification. Read more about SCIM model, operations and endpoints.

Read more about the module.