WAK BCM

Instalační manuál aplikace

Informační systém WAK BCM je softwarovým produktem, jehož nástroje umožňují podporu procesního řízení.

WAK System

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Systém je spolufinancován v rámci
Programu bezpečnostního výzkumu
České republiky BV III/1 – VS

Obsah

1 Úvod

Systém BCM je softwarovou aplikací, kterou lze charakterizovat jako softwarovou dynamickou procesní mapu.

Dynamickou procesní mapu tvoří vlastní diagram procesu a funkční rozhraní umožňující spuštění vykonání procesu. V rámci spuštěného procesu v závislosti na jeho definovaných vazbách jsou postupně a posloupně vykonávány jednotlivé prvky procesu, tzn. události, činnosti a rozhodovací brány. Realizace procesu probíhá na základě definovaných parametrů, které jsou vytvořeny za účelem vykonání procesu, zaznamenání výsledků procesu a v neposlední řadě za účelem stanovení klíčových referenčních hodnot.

Funkce systému umožňují aplikaci komunikovat pomocí uživatelských dotazů resp. oznámení.

Součástí systému BCM je také mobilní aplikace, která umožňuje provádět realizaci výkonu jednotlivých prvků procesů pomocí mobilních IT zařízení.

Následující kapitoly tohoto instalačního manuálu popisují způsob instalace systému BCM.

2 Instalace systému BCM

2.1 Instalace systému

Systém BCM je distribuován jako archiv ve formátu ZIP. Instalace spočívá v rozbalení archivu do vybraného adresáře se zachováním struktury podadresářů. Po rozbalení je zapotřebí vytvořit databázi a provést prvotní konfiguraci systému. Po konfiguraci lze systém přímo spustit z příkazové řádky v adresáři aplikace příkazem: web.exe.

Aplikace po spuštění kontroluje existenci databáze a shodu schématu a dat s očekávaným stavem pro danou verzi aplikace. Jestliže tedy databáze neexistuje a zadaný SQL účet má oprávnění pro vytvoření databáze, systém ji vytvoří a naplní výchozími daty. Databáze je však vytvořena výchozím způsobem pro daný SQL server, proto doporučujeme jí vytvořit před spuštěním systému manuálně s požadovaným nastavením a zároveň vytvořit dedikovaný SQL účet pro aplikaci.

Aplikace si pak sama vytvoří databázové tabulky a výchozí datovou náplň. Před prvním spuštění aplikace je tedy vhodné nastavit účet s právem na spuštění DDL příkazů, pro rutinní provoz stačí oprávnění pro čtení a zápis dat.

Kontrolu a aktualizaci databázového schématu lze potlačit v konfiguračním souboru atributem *App:InitDb*.

Aplikace je ve výchozím nastavení přístupná na http tcp portu 5000 a https portu 5001. Tyto hodnoty lze změnit nastavením proměnné prostředí ASPNETCORE_URLS.

Pro spuštění pod IIS je nutné ve správci internetové informační služby nadefinovat aplikační pool a site. V nastavení aplikačního poolu se verze .NET Framework nastavuje na „no managed“. Pro provoz .NET Core aplikace pod IIS je zapotřebí mít nainstalovaný .NET Core runtime včetně hostitele IIS (instalační soubor dotnet-hosting-verze.exe).

Pro provoz pod operačním systémem Linux je doporučeno hostovat aplikaci pomocí webových serverů Apache, nebo Nginx nastavených jako reverzní proxy.

Po podrobnější informace odkazujeme na dokumentaci k operačnímu systému a k prostředí .NET Core na adrese https://docs.microsoft.com/cs-cz/aspnet/core.

2.2 Konfigurace systému

Systém se konfiguruje editací souboru appsettings.json v adresáři aplikace. Je ve formátu JSON a má následující obsah:

```
{
  "DbConnect": {
    "//": "SqlServer, MySql",
    "DbType": "SqlServer",
    "ConnectionStringID": "SqlServerConnection"
  },
  "ConnectionStrings": {
    "SqlServerConnection": "Server=(local);Database=bcm;Trusted_Connection=True;
                            MultipleActiveResultSets=true",
    "SqlServerTrustedConnection": "Server=(local);Database=bcm; User Id=bcm;
                                   Password=bcm; MultipleActiveResultSets=true",
    "MySqlConnection": "Server=localhost;Database=bcm;User Id=bcm;Password=bcm"
  },
  "App": {
    "InitDb": true,
    "SMTPServer": "mailserver",
    "IMAPServer": "mailserver",
    "RunMailImport": true,
    "MailFrom": "bcm@firma.cz"
  },
  "ServerConfig": {
    "DefaultServerName": "mailserver",
    "ServerList": [
      {
        "Name": "mailserver",
```

```
        "Server": "mail.firma.cz",
        "Port": 0,
        "User": "bcm@firma.cz",
        "Pass": "xxxxxxxxxxxxxxxxxxx",
        "EnableSSL": true,
        "CertValidationPolicy": "ssl",
        "CertThumbprint": "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
      }
    ]
  },
  "Jwt": {
    "Key": "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx",
    "Issuer": "http://bcm.firma.cz/",
    "Expires": 30
  }
}
```

Následuje popis jednotlivých sekcí a atributů konfiguračního souboru:

Sekce **DbConnect**
Atribut **DbType** označuje typ databázového serveru. Povoleny jsou hodnoty „SqlServer“ pro Microsoft SQL Server a „MySql“ pro SQL servery MySQL a MariaDB.

Atribut **ConnectionStringID**
Jméno aktivní hodnoty připojovacího řetězce pro SQL server. Hodnota musí odpovídat některé hodnotě z pole „ConnectionStrings“.

Sekce **ConnectionStrings**
Pole připojovacích řetězců k SQL serveru. Systém může mít definovaných více databázových připojení a z nich vybrané jedno aktivní. Jméno atributu definuje jméno připojení, které se zapíše do hodnoty atributu ConnectionStringID. Jména připojení lze zvolit libovolné. Příklad konfiguračního souboru obsahuje tyto položky:

- SqlServerConnection – připojení k MS SQL serveru jménem a heslem.
- SqlServerTrustedConnection – připojení k MS SQL serveru integr. ověřením.
- MySqlConnection – připojení k MySQL, nebo MariaDB serveru.

Pro instalaci je nutné nastavit atributy *Server*, *Database*, *User ID* a *Password* na platné hodnoty. Atribut *MultipleActiveResultSets=true* pro MS SQLpřipojení je povinný.

Sekce **App**
obsahuje obecná aplikační nastavení a obsahuje následující atributy.

Atribut **InitDb**
povoluje (hodnota “true”), nebo zakazuje (hodnota “false”) kontrolu aktualizaci databáze po startu aplikace. Před prvním spuštěním je nutné mít nastaveno na „true“, aby si aplikace vytvořila SQL tabulky a naplnila databázi systémovými daty. Pro rutinní provoz je pak možné nastavit hodnotu „false“, což může nevýznamně urychlit start aplikace.

Atribut **SMTPServer**
definuje jméno konfigurace mail serveru pro odesílání mailů. Jestliže je požadováno odlišné nastavení pro SMTP a IMAP, je zapotřebí vytvořit pojmenovanou konfiguraci v sekci *ServerConfig* a do hodnoty atributu *SMTPServer* nastavit její jméno. V opačném případě lze nastavit prázdnou hodnotu, nebo atribut úplně vynechat, pak se použije konfigurace určená hodnotou atributu *DefaultServerName* ze sekce *ServerConfig*.

Atribut **IMAPServer**
definuje jméno konfigurace mail serveru pro import mailů protokolem IMAP. Platí obdobné doporučení, jako pro nastavení SMTP serveru.

Atribut **RunMailImport**
povoluje, nebo zakazuje import mailů protokolem IMAP. Funkce importu je nutná pro funkční běh modelů používající aktivity Přijmout zprávu, doporučujeme tedy ponechat hodnotu „true“.

Atribut **MailFrom**
definuje mailovou adresu, která bude použita jako adresa odesílatele v mailech odesílaných systémem.

Sekce **ServerConfig**
obsahuje konfiguraci připojení mail klienta k mail serveru. Systém může mít definovaných více konfigurací klienta a jedno z nich nastavené jako aktivní.

Atribut **DefaultServerName**
Jméno aktivní konfigurace klienta mail serveru. Konfigurace mail serveru má následující atributy:

Name
Jméno konfigurace mail serveru.

Server
DNS jméno serveru.

Port
TCP port serveru, 0 pro výchozí hodnoty pro SMTP a IMAP klienta.

User, Pass
Jméno a heslo pro přihlášení k serveru.

EnableSSL
Povolené hodnoty jsou „true“, nebo „false“. Hodnota „true“ zapíná šifrovanou komunikaci se serverem. Pro SMTP přístup se protokol StartTLS a port 587, pro IMAP protokol SSL a port 993. Pokud je nastavené na „false“, na SMTP se přistupuje anonymně, na IMAP nešifrovaně na port 110.

CertValidationPolicy
Definuje způsob ověřování certifikátu serveru. Povolené hodnoty jsou „ssl“, „hash“ a „none“. V případě hodnoty „ssl“ se certifikát serveru ověřuje dle doménového jména serveru. V případě hodnoty „hash“ je nutné mít v atributu „CertThumbPrint“ otisk platného certifikátu serveru. Tato možnost se využívá pro připojení k serveru se „self-signed“ certifikátem. Konečně hodnota „none“ vypíná ověřování certifikátu serveru.

CertThumbPrint
Otisk platného certifikátu serveru. Má význam pro CertValidationPolicy = „hash“.

Sekce **Jwt**
konfigurace JSON web token pro zabezpečení přístupu mobilní aplikace. Atributy je zapotřebí nastavit takto:

Key
Náhodný text, dlouhý alespoň 40 znaků.

Issuer
Nastavit na URL webu aplikace

Expires
Doba v minutách, po které vyprší platnost tokenu. Hodnotu není třeba měnit.

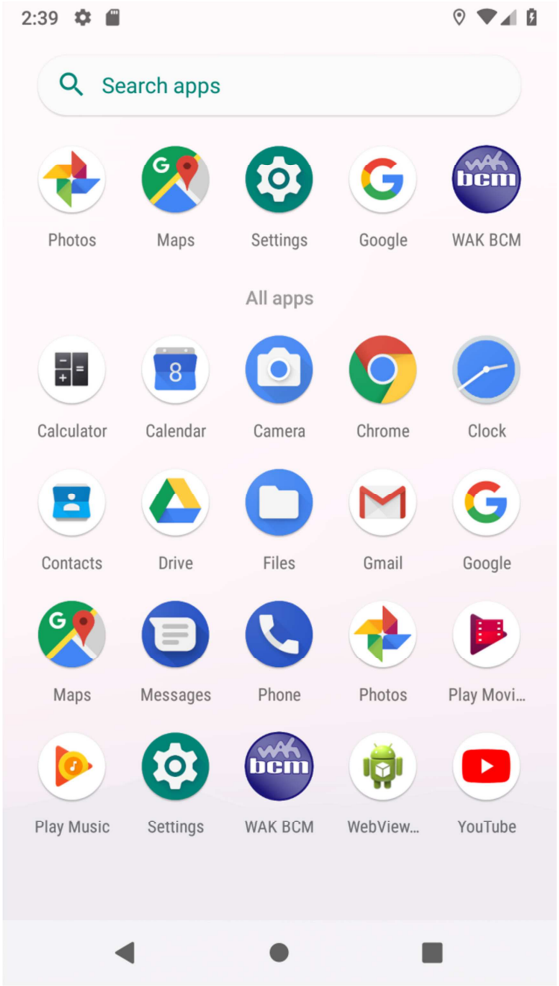
3 Mobilní aplikace

Mobilní aplikace BCM je aplikace umožňující jednoduchým způsobem zpracovávat dotazy - úkoly vyplývající z jednotlivých činností a událostí prvků procesních map.

3.1 Instalace mobilní aplikace

Mobilní aplikace BCM je dostupná pomocí standardního instalačního souboru Android aplikací (instalační soubor s příponou .apk).
Aplikace není dostupná v obchodě Google Play, protože se jedná o mobilní rozšíření systému BCM. Samostatně není tato aplikace využitelná. Aplikace je dostupná pouze jako součást dodávky systému BCM.

Instalaci aplikace je možno provést v případě, že je v mobilním zařízení povolena instalace z neznámých zdrojů. Toto povolení lze ve většině mobilních zařízení nastavit v sekci “Nastavení / Zabezpečení“.
Instalaci lze provést spuštěním souboru WakBcm.apk.
Po instalaci je na ploše zařízení zobrazena ikona aplikace.



Obrázek 1 – Plocha mobilního zařízení s instalovanou aplikací WAK BCM