有生云

数字底座配置文件详解

产品版本：V1.0

文档版本：202401

北京有生博大软件股份有限公司

目录

1.risenet-y9boot-webapp-sso-server-6.6.x

说明：未提及的配置使用默认的即可

序号	配置参数	参数说明
1	cas.audit.engine.useServerHostAddress	是否应进行本地 DNS 查找以查询 CAS 服务器地址，默认为 false，数字底座设置为 true 更多 audit 配置请参考：https://apereo.github.io/cas/development/audits/Audits.html
2	cas.authn.throttle.failure.rangeSeconds	时间范围，以秒为单位；-1 代表无时间限制
3	cas.authn.throttle.failure.threshold	在上述时间段内允许的失败登录尝试次数；-1 代表不限制次数
4	cas.authn.oauth.refreshToken.timeToKillInSeconds	refreshToken 的过期时长，默认为 P14D，即 14 天
5	cas.authn.oauth.code.timeToKillInSeconds	code 的过期时长，默认为 30 秒
6	cas.authn.oauth.code.numberOfUses	code 的使用次数，默认为 1，即使用一次后该 code 就会失效
7	cas.authn.oauth.accessToken.timeToKillInSeconds	accessToken 存活时间，默认为 PT2H，即 2 小时
8	cas.authn.oauth.accessToken.maxTimeTo	accessToken 最大存活时

	LiveInSeconds	间,默认为 PT8H,即 8 小时
9	**cas.authn.oauth.sessionReplication.cookie.secure**	sameSitePolicy 有三个值,分别是 Strict、Lax、None。 Strict: 最为严格,表示完全禁止“第三方 Cookie”,只有当前网页的 URL 与请求目标一致时,才会带上 Cookie,一般用于保证系统的封闭性和安全性。 Lax: 是目前大多数现代浏览器的默认值,他在保证安全性的前提下,也可以避免一些不好的用户体验,比如从别的网站跳转过时会没有登录态。 None:是最为宽松的一种设定,通常用于开放我们的服务给不同的第三方接入,同时又需要追踪用户的场景,比如广告,设置为 None 时需要考虑开放的安全性。 如果存在第三方系统跨域做单点登录认证的时候,需要设置为 None,如果所有系统都是同一个域名下,可以设置为 Lax。

10	cas.theme.defaultThemeName	参数说明：默认的主题名称，数字底座设置为y9-apereo，该字段配合y9.login.casLoginView使用。当被注册的服务没有指定主题时，使用该默认的主题。如果想要更改默认主题的名字，需要定制主题并放在risenet-y9boot-webapp-sso-server-6.6.x\src\main\resources\templates文件夹下,且在该主题文件夹下定制名称为y9.login.casLoginView指定的名称的html类型的登录页面。
11	cas.view.defaultRedirectUrl	客户端进行登录认证时，如果service参数为空，则使用该地址作为认证成功后的重定向地址。
12	cas.view.authorizedServicesOnSuccessfulLogin	当service为空、并且defaultRedirectUrl参数为空时，自动计算service，建议设置为true。
13	cas.serviceRegistry.core.initFromJson	参数说明：是否初始化服务注册信息，建议本地首次运行时设置为true,其

		他环境设置为 false。设置为 true 后，程序会自动加载 risenet-y9boot-webapp-sso-server-6.6.x/src/main/resources/services 文件夹下面的 json 数据插入至数据库表。非本地环境建议通过导出本地的数据，并修改 ip 和端口进行初始化。修改后不会生效，需要执行 http://ip:port/sso/api/service/reload 更改内存中的服务注册信息。
14	cas.ticket.st.numberOfUses	st 使用的次数，一般设置为 1 即可。增加容错的情况下可以设置为 10
15	cas.ticket.st.timeToKillInSeconds	st 有效时间，一般使用一次的话,设置为 30 秒即可。增加容错可以设置为 600，即 10 分钟
16	cas.ticket.tgt.primary.maxTimeToLiveInSeconds	tgt 的最大活跃时间。数字底座设置为 28800，即 8 个小时
17	cas.ticket.tgt.primary.timeToKillInSeconds	tgt 的活跃时间。数字底座设置为 7200，即 2 个小时
18	server.intranet.ip	服务端 ip 配置，需要把运行数字底座的服务器的地

		址配置上，否则会运行失败。
19	y9.login.casLoginView	登录页面名称,配合 theme 使用。数字底座配置该值为 casLoginView-y9-v3.0
20	y9.login.loginInfoSaveTarget	登录日志保存位置，可选值有 kafka，jpa。 kafka:向 kafka 发送消息，日志系统有监听该消息的队列，监听到消息后，会存入 es。 jpa:会直接保存至数据库。

2.risenet-y9boot-webapp-platform

说明：未提及的配置使用默认的即可

序号	配置参数	参数说明
1	server.intranet.ip	服务端 ip 配置，需要把运行数字底座的服务器的地址配置上，否则会运行失败。
2	spring.cloud.nacos.config.enabled	配置文件是否使用 nacos 管理，如果设置为 true 的话，需要自己搭建 nacos 服务。
3	spring.datasource.druid.y9-public	数字底座公共数据库配置
4	y9.systemName	数字底座系统英文名称，保存日志信息以及查找对应的数据源时会用到，不可更改。
5	y9.systemCnName	数字底座系统中文名称，保存日志信息时会用到，可以更改。
6	y9.common.cacheEnabled	是否开启缓存，配置为 true 则使用缓存，false 为不实用缓存。建议配置为 true,因为组织部门、人员、岗位使用缓存会大大提升查询效率减轻数据库负担。
7	y9.common.kafkaEnabled	是否启用 kafka,如果需要记录日志信息，需要开启

		设置为 true,设置为 false 不会向 kafka 日志消息队列发送日志消息。
8	y9.common.defaultPassword	数字底座添加人员时，人员的默认登录密码。
9	y9.feature.apisix.enabled	是否启用 apisix 作为接口网关，设置为 true 的话，需要自己搭建 apisix 服务。
10	y9.feature.security.enabled	是否启用安全组件，设置为 true 则会启用 csrf、xss、cors 等安全规则
11	y9.feature.security.csrf.accepted-referer	允许的请求来源
12	y9.feature.security.cors.allowedOriginPatterns	允许的跨域请求站点。如果前端或者第三方系统需要请求数字底座且不在同一个域下，需要配置前端或者第三方的地址正则表达式。
13	y9.feature.security.xss.ignoreParam	忽略的参数名称
14	y9.feature.oauth2.resource.enabled	是否开启 OAuth2.0 验证。非本地环境必须设置为 true。本地环境添加自己的过滤器设置为固定用户登录时可以设置为 false。
15	y9.feature.oauth2.resource.saveLogMessage	是否保存日志信息，设置为 true，不管有没有添加日志注解 Riselog 都会保

		存日志操作信息。设置为false，只有添加了注解Riselog的才会保存日志。建议设置为true.
16	y9.feature.oauth2.resource.saveOnlineMessage	是否开启用户在线状态检测，数字底座标准版本需要设置为false。设置为true也不会展示用户在线信息。
17	y9.feature.oauth2.resource.protectedUrlPatterns	受保护url的正则表达式，/*表示所有地址都受保护/api/*表示url中包含/api/的才受保护
18	y9.feature.oauth2.resource.opaque.client-id	客户端唯一标示，由数字底座运维人员分配，统一认证服务启动时默认会添加一对client-id: clientid client-secret: secret 建议正式使用时请分配不同的密钥对给不同的系统。
19	y9.feature.oauth2.resource.opaque.client-secret	客户端密钥，由数字底座运维人员分配，统一认证服务启动时默认会添加一对client-id: clientid client-secret: secret 建议正式使用时请分配不同的密钥对给不同的系

		统。
20	y9.feature.oauth2.resource.opaque.introspection-uri	统一认证检测令牌地址，可以查询给定访问令牌的状态
	y9.feature.oauth2.resource.opaque.profile-uri	统一认证获取登录用户信息地址

3.risenet-y9boot-webapp-log

说明：未提及的配置使用默认的即可

序号	配置参数	参数说明
1	server.intranet.ip	服务端 ip 配置，需要把运行数字底座的服务器的地址配置上，否则会运行失败。
2	spring.cloud.nacos.config.enabled	配置文件是否使用 nacos 管理，如果设置为 true 的话，需要自己搭建 nacos 服务。
3	y9.systemName	数字底座系统英文名称，保存日志信息以及查找对应的数据源时会用到，不可更改。
4	y9.common.kafkaEnabled	是否启用 kafka,如果需要记录日志信息，需要开启设置为 true,设置为 false

		不会向 kafka 日志消息队列发送日志消息。
5	y9.feature.apisix.enabled	是否启用 apisix 作为接口网关，设置为 true 的话，需要自己搭建 apisix 服务。
6	y9.feature.security.enabled	是否启用安全组件，设置为 true 则会启用 csrf、xss、cors 等安全规则
7	y9.feature.security.csrf.accepted-referer	允许的请求来源
8	y9.feature.security.cors.allowedOriginPatterns	允许的跨域请求站点。如果前端或者第三方系统需要请求数字底座且不在同一个域下，需要配置前端或者第三方的地址正则表达式。
9	y9.feature.security.xss.ignoreParam	忽略的参数名称
10	y9.feature.oauth2.resource.enabled	是否开启 OAuth2.0 验证。非本地环境必须设置为 true。本地环境添加自己的过滤器设置为固定用户登录时可以设置为 false。
11	y9.feature.oauth2.resource.saveLogMessage	是否保存日志信息，设置为 true，不管有没有添加日志注解 Riselog 都会保存日志操作信息。设置为 false，只有添加了注解 Riselog 的才会保存日志。

		建议设置为 true.
12	y9.feature.oauth2.resource.saveOnlineMessage	是否开启用户在线状态检测，数字底座标准版本需要设置为 false。设置为 true 也不会展示用户在线信息。
13	y9.feature.oauth2.resource.protectedUrlPatterns	受保护 url 的正则表达式，/*表示所有地址都受保护 /api/*表示 url 中包含 /api/的才受保护
14	y9.feature.oauth2.resource.opaque.client-id	客户端唯一标示，由数字底座运维人员分配，统一认证服务启动时默认会添加一对 client-id: clientid client-secret: secret 建议正式使用时请分配不同的密钥对给不同的系统。
15	y9.feature.oauth2.resource.opaque.client-secret	客户端密钥，由数字底座运维人员分配，统一认证服务启动时默认会添加一对 client-id: clientid client-secret: secret 建议正式使用时请分配不同的密钥对给不同的系统。
16	y9.feature.oauth2.resource.opaque.introspection-uri	统一认证检测令牌地址，可以查询给定访问令牌的

		状态
	y9.feature.oauth2.resource.opaque.profile-uri	统一认证获取登录用户信息地址