Web Services and Applications Deployment Guide

Configuring Web Services settings

12/15/2025

Configuring Web Services settings

> **Important**
> If you are deploying Web Services and Applications version 8.5.201.09 or earlier, complete the steps on Configuring Web Services for 8.5.201.09 or earlier instead.

Contents

As part of Deploying the web application, you created the **application.yaml** file (or Web Services created it for you). To configure basic Web Services and Applications settings, you need to update the **application.yaml** file on each of your Web Services nodes. In later topics, you'll learn more about modifying this file to configure additional features and security. For now, review the contents below for details about each section in the **application.yaml** configuration file.

Logging settings

The purpose of the **logging** section is to tell Web Services where to find the **logback.xml** file you created (or Web Services created for you) as part of Deploying the web application and where to save logs.

The **application.yaml.sample** file includes the following default **logging** section:

```
logging:
  config: logback.xml
  file: cloud.log
  path: /var/log/jetty9
```

See logging for details about all supported configuration settings for this section.

Jetty settings

You use the **jetty** section of the **application.yaml.sample** file to tell Web Services how Jetty should behave. The **application.yaml.sample** file includes the following default **jetty** section:

```
jetty:
  host:
  port: 8090
  idleTimeout: 30000
  soLingerTime: -1
  sessionMaxInactiveInterval: 1800
  enableWorkerName: true
  enableRequestLog: true
  requestLog:
    filename: yyyy_mm_dd.request.log
    filenameDateFormat: yyyy_MM_dd
    logTimeZone: GMT
    retainDays: 90
    append: true
    extended: false
    logCookies: false
    logLatency: true
    preferProxiedForAddress: true
  enableSsl: false
```

See jetty for details about supported configuration settings for this section.

Cassandra cluster settings

The settings in the **cassandraCluster** section correspond to the contents of the **cassandra-cluster.yaml** file in version 8.5.201.09 or earlier of Web Services and Applications. This section tells Web Services how your Cassandra cluster should be managed and accessed.

The **application.yaml.sample** file includes the following default **cassandraCluster** section:

```
cassandraCluster:
  thrift_port: 9160
  jmx_port: 7199
  nodes: [ToBeChanged: <CASSANDRA_PRIMARY_DC_NODES>]
  backup_nodes: [ToBeChanged: <CASSANDRA_BACKUP_DC_NODES>]
  replication_factor: [ToBeChanged: <REPLICATION_FACTOR>]
  write_consistency_level: [ToBeChanged: "CL_LOCAL_QUORUM" for multi-datacenters env,
"CL_QUORUM" for single-DC env.]
  read_consistency_level: [ToBeChanged: "CL_LOCAL_QUORUM" for multi-datacenters env,
"CL_QUORUM" for single-DC env.]
  max_conns_per_host: 16
  max_cons: 48
  max_pending_conns_per_host: 80
  max_blocked_threads_per_host: 160

  cassandraVersion: [ToBeChanged: "1.1" | "1.2"]
  useSSL: [ToBeChanged: supporting only for 1.2 Cassandra "false" | "true"]
```

Make sure that you update all settings marked as [ToBeChanged]. See cassandraCluster for details about all supported configuration settings for this section.

Server settings

The settings in the serverSettings section correspond to the contents of the **server-settings.yaml** file in version 8.5.201.09 or earlier of Web Services and Applications. This section provides the core settings Web Services needs to run your node.

The **application.yaml.sample** file includes the following default **serverSettings** section:

```
serverSettings:
  # URLs
  externalApiUrlV2: [ToBeChanged: public URL including protocol, address and port,
<PUBLIC_SCHEMA_BASE_URL>]/api/v2
  internalApiUrlV2: [ToBeChanged: internal URL including protocol, address and port,
<INTERNAL_SCHEMA_BASE_URL>]/internal-api
  undocumentedExternalApiUrl: [ToBeChanged: public URL including protocol, address and port,
<PUBLIC_SCHEMA_BASE_URL>]/internal-api

  # Paths
  pathPrefix: [ToBeChangedOrRemoved: <PATH_PREFIX>]
  internalPathPrefix: [ToBeChangedOrRemoved: <INTERNAL_PATH_PREFIX>]

  # General
  iwsDispositionCodeSync: [ToBeChanged: "true"|"false"]
  temporaryAuthenticationTokenTTL: [ToBeChangedOrRemoved:
<TEMPORARY_AUTHENTICATION_TOKEN_TTL>]
  enableCsrfProtection: [ToBeChanged: "true"|"false"]
  salesforceAuthenticationMode: [ToBeChanged: "true"|"false"]
```

```
enableOpenIDConnect: [ToBeChanged: "true"|"false"]

# Timeouts
activationTimeout: 12000
configServerActivationTimeout: 35000
configServerConnectionTimeout: 15000
connectionTimeout: 4000
contactCenterSynchronizationTimeout: 60000
inactiveUserTimeout: [ToBeChangedOrRemoved: <INACTIVE_USER_TIMEOUT>]
reconnectAttempts: 1
reconnectTimeout: 10000

# OPS account
opsUserName: [ToBeChanged: <OPS_USER_NAME>]
opsUserPassword: [ToBeChanged: <OPS_USER_PASSWORD>]

# Configuration Server credentials
applicationName: Cloud
applicationType: CFGGenericClient
cmeUserName: [ToBeChanged: <CONFIG_SERVER_USER_NAME>]
cmePassword: [ToBeChanged: <CONFIG_SERVER_USER_PASSWORD>]
syncNode: [ToBeChanged: "true"|"false"]
synchronizationCmeEventsPrefilterEnabled: [ToBeChanged: "true"|"false"]
enableVirtualQueueSynchronization: [ToBeChanged: "true"|"false"]

# Statistics
statConnectionTimeout: [ToBeChangedOrRemoved: <STAT_CONNECTION_TIMEOUT>]
statReconnectAttempts: [ToBeChangedOrRemoved: <STAT_RECONNECT_ATTEMPTS>]
statReconnectTimeout: [ToBeChangedOrRemoved: <STAT_RECONNECT_TIMEOUT>]
statOpenTimeout: [ToBeChangedOrRemoved: <STAT_OPEN_TIMEOUT>]
statisticsWritesCL: [ToBeChangedOrRemoved: <STATISTICS_WRITE_SCL>]
reportingSyncInterval: [ToBeChangedOrRemoved: <REPORTING_SYNC_INTERVAL>]
enableElasticSearchIndexing: [ToBeChanged: "true"|"false"]
statisticsOpenRetryInterval: [ToBeChangedOrRemoved: <STATISTICS_OPEN_RETRY_INTERVAL>]

# Multi regional supporting
nodePath: [ToBeChanged: node position in cluster, example: /<REGION>/HOST
nodeId: [ToBeChangedOrRemoved: unique value in cluster <NODE_ID>]

# SSL and CA
caCertificate: [ToBeChangedOrRemoved: <CA_CERTIFICATE>]
jksPassword: [ToBeChangedOrRemoved: <JKS_PASSWORD>]

# SAML
samlSettings:
  encryptionKeyName: [ToBeChangedOrRemoved: <SAML_ENCRYPTION_KEY_NAME>]
  signingKeyName: [ToBeChangedOrRemoved: <SAML_SIGNING_KEY_NAME>]
  identityProviderMetadata: [ToBeChangedOrRemoved: <SAML_IDENTITY_PROVIDER_METADATA>]
  serviceProviderEntityId: [ToBeChangedOrRemoved: <SAML_SERVICE_PROVIDER_ENTITY_ID>]
  encryptionKeyPassword: [ToBeChangedOrRemoved: <SAML_ENCRYPTION_KEY_PASSWORD>]
  signingKeyPassword: [ToBeChangedOrRemoved: <SAML_SIGNING_KEY_PASSWORD>]
  tlsKeyName: [ToBeChangedOrRemoved: <SAML_TLS_KEY_NAME>]
  tlsKeyPassword: [ToBeChangedOrRemoved: <SAML_TLS_KEY_PASSWORD>]
  responseSkewTime: [ToBeChangedOrRemoved: <SAML_RESPONSE_SWEW_TIME>]

# CORS
crossOriginSettings:
  allowedOrigins: [ToBeChangedOrRemoved: <CROSS_ALLOWED_ORIGINS>]
  allowedMethods: [ToBeChangedOrRemoved: <CROSS_ALLOWED_METHODS>]
  allowedHeaders: [ToBeChangedOrRemoved: <CROSS_ALLOWED_HEADERS>]
  exposedHeaders: [ToBeChangedOrRemoved: <CROSS_EXPOSED_HEADERS>]
  allowCredentials: [ToBeChangedOrRemoved: <CROSS_ALLOW_CREDENTIALS>]
  corsFilterCacheTimeToLive: [ToBeChangedOrRemoved:
```

```
<CROSS_ORIGIN_CORS_FILTER_CACHE_TIME_TO_LIVE>]

  # Elastic Search
  elasticSearchSettings:
    clientNode: [ToBeChangedOrRemoved: "true"|"false"]
    indexPerContactCenter: [ToBeChangedOrRemoved: "true"|"false"]
    enableScheduledIndexVerification: [ToBeChangedOrRemoved: "true"|"false"]
    indexVerificationInterval: [ToBeChangedOrRemoved:
<ELASTIC_SEARCH_INDEX_VERIFICATION_INTERVAL>]
    retriesOnConflict: [ToBeChangedOrRemoved: <ELASTIC_SEARCH_RETRIES_ON_CONFICT>]
    waitToIndexTimeout: [ToBeChangedOrRemoved: <ELASTIC_SEARCH_WAIT_TO_INDEX_TIMEOUT>]
    enableIndexVerificationAtStartUp: [ToBeChangedOrRemoved: "true"|"false"]

  # Caching Settings
  cachingSettings:
    enableSystemWideCaching: [ToBeChangedOrRemoved: "true"|"false"]
    agentStatesTTL: [ToBeChangedOrRemoved: <CACHING_AGENT_STATES_TTL>]
    businessAttributesTTL: [ToBeChangedOrRemoved: <CACHING_BUSINESS_ATTRIBUTES_TTL>]
    transactionsTTL: [ToBeChangedOrRemoved: <CACHING_TRANSACTIONS_TTL>]
    skillsTTL: [ToBeChangedOrRemoved: <CACHING_SKILLS_TTL>]
    virtualAgentGroupsTTL: [ToBeChangedOrRemoved: <CACHING_VIRTUAL_AGENT_GROUPS_TTL>]
    contactCenterFeaturesTTL: [ToBeChangedOrRemoved: <CACHING_CONTACT_CENTER_FEATURES_TTL>]
    contactCenterSettingsTTL: [ToBeChangedOrRemoved: <CACHING_CONTACT_CENTER_SETTINGS_TTL>]
    voiceContextCaching: [ToBeChangedOrRemoved: "true"|"false"]
    voiceContextRefreshInterval: [ToBeChangedOrRemoved:
<CACHING_VOICE_CONTEXT_REFRESH_INTERVAL>]

    dedicatedCacheSettings:
      - cacheName: ContactServerCategoriesCache
        timeToLiveSeconds: [ToBeChangedOrRemoved: <TTL_FOR_CATEGORIES_CACHE>]
        maxEntriesLocalHeap: [ToBeChangedOrRemoved: <MAX_LOCAL_HEAP_FOR_CATEGORIES_CACHE>]
      - cacheName: ContactServerStandardResponsesCache
        timeToLiveSeconds: [ToBeChangedOrRemoved: <TTL_FOR_STANDARD_RESPONSES_CACHE>]
        maxEntriesLocalHeap: [ToBeChangedOrRemoved:
<MAX_LOCAL_HEAP_FOR_STANDARD_RESPONSES_CACHE>]

  # DoS Filter Settings
  enableDosFilter: [ToBeChanged: "true"|"false"]
  dosFilterSettings:
    maxRequestsPerSec: [ToBeChangedOrRemoved: <DOS_FILTER_MAX_REQUESTS_PER_SEC>]
    delayMs: [ToBeChangedOrRemoved: <DOS_FILTER_DELAY_MS>]
    maxWaitMs: [ToBeChangedOrRemoved: <DOS_FILTER_MAX_WAIT_MS>]
    throttledRequests: [ToBeChangedOrRemoved: <DOS_FILTER_THROTTLED_REQUESTS>]
    throttleMs: [ToBeChangedOrRemoved: <DOS_FILTER_THROTTLE_MS>]
    maxRequestMs: [ToBeChangedOrRemoved: <DOS_FILTER_MAX_REQUEST_MS>]
    maxIdleTrackerMs: [ToBeChangedOrRemoved: <DOS_FILTER_MAX_IDLE_TRACKER_MS>]
    insertHeaders: [ToBeChangedOrRemoved: <DOS_FILTER_INSERT_HEADERS>]
    trackSessions: [ToBeChangedOrRemoved: <DOS_FILTER_TTACK_SESSIONS>]
    remotePort: [ToBeChangedOrRemoved: <DOS_FILTER_REMOTE_PORT>]
    ipWhitelist: [ToBeChangedOrRemoved: <DOS_FILTER_IP_WHITE_LIST>]

  # Statistics Settings

  # Account Management
  accountManagement:
    forgotPasswordEmailTemplate:
      from: [ToBeChangedOrRemoved: <PASSWORD_MESSAGE_FROM>]
      subject: [ToBeChangedOrRemoved: <PASSWORD_MESSAGE_SUBJECT>]
      body: [ToBeChangedOrRemoved: <PASSWORD_MESSAGE_BODY>]
    accountCreatedEmailTemplate:
      from: [ToBeChangedOrRemoved: <ACCOUNT_MESSAGE_FROM>]
      subject: [ToBeChangedOrRemoved: <ACCOUNT_MESSAGE_SUBJECT>]
      body: [ToBeChangedOrRemoved: <ACCOUNT_MESSAGE_BODY>]
```

```
    smtpServer:
      host: [ToBeChangedOrRemoved: <SMTP_SERVER_HOST>]
      port: [ToBeChangedOrRemoved: <SMTP_SERVER_PORT>]
      userName: [ToBeChangedOrRemoved: <SMTP_SERVER_USER_NAME>]
      password: [ToBeChangedOrRemoved: <SMTP_SERVER_PASSWORD>]
      timeout: [ToBeChangedOrRemoved: <SMTP_SERVER_TIMEOUT>]

  # CometD Settings
  cometDSettings:
    maxSessionsPerBrowser: [ToBeChangedOrRemoved: <MAX_SESSIONS_PER_BROWSER>]
    multiSessionInterval: [ToBeChangedOrRemoved: <MULTI_SESSION_INTERVAL>]

  # OAuth2 Settings

  # Session Persistence Settings

  # Multimedia Disaster Recovery
  drMonitoringDelay: [ToBeChangedOrRemoved: <DR_MONITORING_DELAY>]

  # Stale CometD Session monitoring

  # Node Settings Refresh

  # Log Header Settings
  logHeaderSettings:
    enableLogHeader: [ToBeChangedOrRemoved: "true"|"false"]
    updateOnPremiseInfoInterval: [ToBeChangedOrRemoved: <UPDATE_ON_PREMISE_INFO_INTERVAL>]

  # Update on startup settings
  updateOnStartup:
    opsCredentials: true
    features: true
    statistics: true
```

Make sure that you update all settings marked as [ToBeChanged]. You must also do the following:

- Set the applicationName to the name of the application you created in Configuring the Web Services applications — for example, WS_Node.

- In each Web Services cluster, you must configure one node as the synchronization node — syncNode: true. All other nodes in the cluster must have syncNode: false.

See serverSettings for details about supported configuration settings for this section.

On-premises settings

The settings in the **onPremiseSettings** section correspond to the contents of the **onpremise-settings.yaml** file in version 8.5.201.09 or earlier of Web Services and Applications. This section tells Web Services where Configuration Server is located.

For example:

```
onPremiseSettings:
  cmeHost: localhost
  cmePort: 8888
  countryCode: US
```

The **application.yaml.sample** file doesn't include a default **onPremiseSettings** section, so you'll need to add it yourself.

> ### Warning
>
> Ensure that you add the **onPremiseSettings** section to the top of the **application.yaml.sample** file. Web Services does not read the section if it is located elsewhere in the file.

See onPremiseSettings for details about all supported configuration settings for this section.

Tuning the Web Services host performance

Complete the steps below on each Web Services node to tune the performance of the host environment.

1. To optimize TCP/IP performance, you can run the following commands:

   ```
   sudo sysctl -w net.core.rmem_max=16777216
   sudo sysctl -w net.core.wmem_max=16777216
   sudo sysctl -w net.ipv4.tcp_rmem="4096 87380 16777216"
   sudo sysctl -w net.ipv4.tcp_wmem="4096 16384 16777216"
   sudo sysctl -w net.core.somaxconn=4096
   sudo sysctl -w net.core.netdev_max_backlog=16384
   sudo sysctl -w net.ipv4.tcp_max_syn_backlog=8192
   sudo sysctl -w net.ipv4.tcp_syncookies=1
   sudo sysctl -w net.ipv4.tcp_congestion_control=cubic
   ```

2. After providing for some means of starting Jetty, determine the user or group that will start Jetty and increase the file descriptors available to that user or group by adding the following to the **/etc/security/limits.conf** file:

   ```
   <user_name>                    hard nofile       100000
   <user_name>                     soft nofile        100000
   ```

   Where <user_name> is the name of the user or group that is starting Jetty.

Configuring Web Services as a System Service on Red Hat Linux Enterprise Linux 6

1. Open the **/etc/default/gws** file.

2. Update the following environment variables to values appropriate for your Web Services node:

   • **GWS_HOST**: Match this value to the Jetty host that you configured in the **jetty** section of the **application.yaml** configuration file.

- **GWS_PORT**: Match this value to the Jetty port that you configured in the **jetty** section of the **application.yaml** configuration file.

SameSite cookies

To handle sameSite cookie attribute, you must configure options for both Jetty and CometD.

If the value of **SameSite** is set to None, Chrome browser also checks if the Secure cookie attribute is present, and if not, then warn user.

To mitigate this issue, make the following edits in `application.yaml`:

```
...
jetty:
  ...
  cookies:
    ...
    secure: true
    sameSite: None
...
serverSettings:
  ...
  cometDSettings:
    ...
    cookieSecure: true
    cookieSameSite: None
```

Important

If cookies are configured to be secure, the browser applies them to a secure connection only (https); therefore, these options take effect only if **enableSsl** is set to `true`.

If the value of **SameSite** is set to Lax or `Strict`, a secured connection is not required, for example:

```
...
jetty:
  ...
  cookies:
...
    ...
    httpOnly: true
    secure: false
    sameSite: Lax
...
serverSettings:
  ...
  cometDSettings:
    ...
    cookieHttpOnly: true
    cookieSecure: false
    cookieSameSite: Lax
```

However, it is important to note the following:

- If **SameSite** is set to Lax, the cookie is sent only on same-site requests or by top-level navigation with a safe HTTP method. That is, it will not be sent with cross-domain POST requests or when loading the site in a cross-origin frame, but it will be sent when the user navigates to the site via a standard top-level <a href=...> link.

- If **SameSite** is set to `Strict`, the cookie is never sent in cross-site requests. Even if the user clicks a top-level link on a third-party domain to your site, the browser refuses to send the cookie.

Important

You can choose an insecure connection by specifying a different type of SameSite (Lax or Strict), but this means that it will be impossible to embed Workspace Web Edition in an iframe or use it for any other cross-domain integrations. For example, applications like Genesys CRM Workspace/Adapter will not work with this configuration.

Next step

- Configuring features