

Configure

Groups

Default

Hosts

App Servers

*index_http [HTTP]

*index_webdav

[WebDAV]

Admin [HTTP]

agint_webdav [WebDAV]

ama_http [HTTP]

ama-cme-http [HTTP]

AMA-cme-lms [HTTP]

ama-cme-webdav

[WebDAV]

App-Services [HTTP]

HealthCheck [HTTP]

Manage [HTTP]

para-app [WebDAV]

para-http [HTTP]

para-webdav [WebDAV]

PayNet [HTTP]

samplestack [HTTP]

STNG [HTTP]

STNGtake2 [HTTP]

Namespaces

Module Locations

Schemas

Request Blackouts

Output Options

*index_java [XDBC]

agint_java [XDBC]

ama_cpt_demo_xdbc

[XDBC]

ama_java [XDBC]

ama-cme-xdbc [XDBC]

para-modules-xcc

[XDBC]

para-xcc [XDBC]

*index_odbc [ODBC]

ama-cme-odbc [ODBC]

Task Server

Scheduled Tasks

Schemas

Namespaces

Module Locations

Diagnostics

Auditing

Databases

Hosts

Forests

Mimetypes

Clusters

Security

HTTP Server: STNGtake2

ok

cancel

http server -- A HTTP server specification.

delete

disable

server name

STNGtake2

The server name.

root

/

The root document directory pathname.

port*

8092

The server socket bind internet port number.

modules

STNGtake2-modules

The database that contains application modules.

database

paramount

The database name.

last login

(none)

The database that contains users' last login information.

display last login

☐ true ☒ false

Indicates whether an appserver should display users' last login information.

address*

0.0.0.0

The server socket bind numeric internet address.

backlog*

512

The socket listen backlog.

threads*

32

The maximum number of server threads allowed.

request timeout

30

The request socket recv timeout, in seconds.

keep alive timeout

5

The keep-alive socket recv timeout, in seconds.

session timeout

3600

The session expiration timeout, in seconds.

max time limit

3600

The upper bound for a request's time limit, in seconds.

default time limit

600

The default time limit for a request, in seconds.

max inference size

500

The upper bound for a request's inference size, in megabytes.

default inference size

The default inference size for a request, in megabytes.

static expires

Add an "expires" HTTP header for static content to expire after this many seconds.

pre-commit trigger depth

The maximum depth of pre-commit trigger invocation.

pre-commit trigger limit

The maximum number of triggers a single statement can invoke.

collation

collation builder

The default collation for queries.

authentication

The authentication scheme to use for this server

internal security

☒ true ☐ false

Whether or not the security database is used for authentication and authorization.

external security

External authentication and authorization configuration.

default user

The user used as the default user in application level authentication. Using the admin user as the default user is equivalent to turning security off.

privilege

The privilege restricting access to the server.

concurrent request limit

The maximum number of concurrent requests per user.

log errors

☐ true ☒ false

Log uncaught request processing errors to ErrorLog.txt.

debug allow

☒ true ☐ false

Allow debugging on this server.

profile allow

☒ true ☐ false

Allow profiling on this server.

default xquery version

The default XQuery language version for this server.

multi version concurrency control

Specifies concurrency control of read-only queries.

distribute timestamps

Specifies the distribution of commit timestamps after updates.

default error format

The default error format for protocol errors. One of html,xml,json,compatible

error handler

/MarkLogic/rest-api/error-handler.xqy

The script that handles 400 and 500 errors for this server.

module locations -- *The module location specifications.*

url rewriter

/MarkLogic/rest-api/rewriter.xml


The script that rewrites URLs for this server.

rewrite resolves globally

☒ true ☐ false

Allow rewritten URLs to be resolved from the global MarkLogic Modules/ directory.

ssl certificate template

(none) 

The certificate template. When a certificate template is specified, the App Server uses an SSL encrypted protocol (e.g. https, davs, xccs). The certificate template specifies the common information for the individual SSL certificates needed for each host in the group.

You can add a new certificate template by navigating to [Security > Certificate Templates > Create](#)

ssl hostname

The host name for the server's SSL certificate. This is useful when many servers are running behind a load balancer. If not specified, each host will use a certificate specifying its own hostname. Note that per RFC 2459, hostnames must not exceed 64 characters in length.

ssl ciphers

ALL:!LOW:@STRENGTH

A colon separated list of ciphers (e.g. ALL:!LOW:@STRENGTH)

ssl require client certificate

☒ true ☐ false

Whether or not a client certificate is required. This only has an effect when one or more more client certificate authorities are specified, in which case a value of true will refuse a client request if it does not present a valid client certificate.

ssl client certificate authorities -- *Certificate authorities that may sign client certificates for this server. Selecting one or more certificate authorities when SSL is enabled will require all clients to present a valid certificate signed by one of the selected authorities. Clicking on an organization below will reveal the certificate authorities for that organization.*

Show

* -- requires restart of one or more hosts

ok

cancel