Advanced GBS.Sandbox

Parameter Description and Configuration

Document Version 1.0
iQ.Suite for Domino as of Version 22.1

Inhalt

1 Advanced GBS.Sandbox

The Advanced GBS.Sandbox (shortly named *GBS.Sandbox*) is an iQ.Suite solution which can be used to integrate components such as Converters, Unpackers, Virus Scanners and Spam Analyzers into iQ.Suite.

The GBS.Sandbox improves the stability of the system environment by separating critical processes, such as virus check or file analysis, from the Grabber processing. Crashes or deadlocks of virus scanners do not fatally affect the stability of the Domino server.

In addition, the GBS.Sandbox is responsible for updating these components. It can stop, modify and restart components without aborting the Grabbers or Domino server.

1.1 Availability for Components

In iQ.Suite, a Sandbox solution is implemented for the following components:

Component	iQ.Suite Module
Virus scanners – integration and update of virus patterns	iQ.Suite Watchdog
Analyzer – integration and update of spam patterns	iQ.Suite Wall
Converters	iQ.Suite Wall
Unpackers	iQ.Suite Wall
	iQ.Suite Watchdog

> Changes regarding the GBS.Sandbox are described in the release notes until this documentation is updated.

1.2 Validity of the Advanced GBS.Sandbox

The Advanced GBS.Sandbox which is described in this TechDoc is used **as of iQ.Suite Version 22.1**.

Exceptions apply under one of the following conditions:

- A Virus Scanner Engine has been switched to the traditional Sandbox technology.

- The traditional Sandbox technology was used in an older iQ.Suite and has not been switched to the Advanced GBS.Sandbox after an iQ.Suite update.

> Sandboxes for Analyzers, Converters and Unpackers are automatically switched to the Advanced GBS.Sandbox when iQ.Suite is updated.

2 Functionality

The functions of each the iQ.Suite components mentioned above are provided by a DLL. The GBS.Sandbox is mainly a process which loads this DLL and makes its functions available to the other iQ.Suite processes.

2.1 Updates of Components

The GBS.Sandbox is also used to automatically update components. If an update has been downloaded, the Sandbox process is stopped, the update is applied and the Sandbox process is restarted. The other iQ.Suite processes can keep running, accesses to the component in the GBS.Sandbox need only to wait a short time during the update.

2.2 Number of Sandbox Processes

If several threads are using a component at the same time, several Sandbox processes are started for this component[1].

Particularly for virus scanners, the Sandbox processes can use a lot of RAM (main memory), so it often makes sense to limit the number of Sandbox processes. In case of a large iQ.Suite configuration with many different components, the number of Sandbox processes per component can be much lower than the number of iQ.Suite threads without affecting the performance significantly.

2.3 Sandbox Timeouts

The Sandbox timeout is the maximum time span which a Sandbox access may take. This timeout is used to identify hanging Sandbox processes. If an access takes more time than this time span, the Grabber assumes that the process is hanging. The access is aborted and the process is restarted.

---

[1] Here lies an important difference to the traditional GROUP.Sandbox, which started several Sandbox threads in a single Sandbox process for this purpose.

3 Configuration of the GBS.Sandbox

The maximum number of Sandbox processes and the Sandbox timeout can be configured for all components,

For some components, it is also possible to configure an automatic update of the component.

Depending on the component, Sandbox parameters can be configured at different places.

3.1 Global Configuration

The maximum number of Sandbox processes is defined via the following global parameter:

`ToolKit_SandboxMaxInstances`

The value of this parameter is used if no specific parameter is set for a component. If this global parameter is not set, the default value is '6'.

3.2 Configuration for Virus Scanners

Except for the parameter of the Sandbox timeout, the parameters can be found in the Virus Scanner Engine document:

- **Maximum number of Sandbox processes**:
  - ☐ Specify this number in the **Advanced** tab of the Engine document.
  - ☐ Unlike other components, the maximum value for virus scanners is '6'.
- **Sandbox timeout**: Global parameter `ToolKit_VS_<Type>_SandboxTimeout`
  - ☐ `<Type>`: Can take one of the following values:
    - ▷ kaspersky
    - ▷ mcafee3
    - ▷ savapi2
    - ▷ sophos3
  - ☐ The timeout is specified in seconds.

    <u>Default</u>: 300

> **Specialty of the Sophos Scan Engine:**
>
> If 'Sophos Sandboxing Protection' is enabled in the Virus Scanner Parameter document, the timeout of the GBS.Sandbox is automatically increased so that it is higher than the timeout which is set in the Parameter document for the Sophos Sandboxing Protection.

■ **Updates**: The virus scanner updates are configured in the **Update** tab of the Engine document.

3.3 Configuration for Analyzers and Converters

If required, these parameters can be added to the list of parameters in the **Settings** tab of the Analyzer or Converter document.

■ **Maximum number of Sandbox processes**:

    ☐ `sandbox-max-instances`

> If several jobs use the same Converter, the maximum number applies per job since different jobs use separate Sandbox processes.

■ **Sandbox timeout**:

    ☐ `sandbox-timeout`

The Sandbox timeout is specified in seconds.

Default: 90

■ **Update interval**:

    ☐ `EngineUpdateInterval`

The update interval is specified in minutes.

Default:

    ☐ For all Analyzers and Converters, except KAS and SASI:

    ▷ 0 (disabled)

    ☐ For KAS and SASI:

    ▷ 60

■ **Update source**:

    ☐ `EngineUpdateDownloadFrom`

Default:

    ☐ KAS: http://updater.gbs.com/kas

    ☐ SASI: http://updater.gbs.com/sasi

■ **Update timeout**:

  ☐ `EngineUpdateTimeout`

  The update timeout is specified in minutes.

  <u>Default</u>: 15

■ **Notifications in case of update errors**:

  ☐ `EngineUpdateErrorRecipients`

  The parameter value is a semicolon-separated list of email addresses to which notifications are sent in case of update errors.

  <u>Default</u>: Value of the global parameter `ToolKit_Admin`

  To disable the notifications in case of update errors, the value must be set to a space character. An empty string cannot be used here.

■ **Notification in case of a successful update**:

  ☐ `EngineUpdateSuccessRecipients`

  The parameter value is a semicolon-separated list of email addresses to which notifications are sent in case of a successful update.

  <u>Default</u>: empty

If more than one Analyzer document exists for an Analyzer for using different Analyzer parameters in different jobs, the parameters for Sandbox and update must not conflict.

Example: If, for example, `EngineUpdateDownloadFrom` is set in a document to http://updatemanager.example.com/sasi, this parameter must either not be set in another document or set to the same value. Otherwise, there is a configuration error.

3.4   Configuration for Unpackers

If required, these parameters can be added in the **Parameter** field of the **Settings** tab of the Unpacker document:

■ **Maximum number of Sandbox processes**:

  ☐ `--sandbox-max-instances`

If several jobs use the same Unpacker, the maximum number applies per job since different jobs use separate Sandbox processes.

■ **Sandbox timeout**:

    ☐ `--sandbox-timeout`

The Sandbox timeout is specified in seconds.

<u>Default</u>: 90

4   About GBS

GBS Europa GmbH is a leading vendor of solutions and services in the fields of messaging security and workflow for the Domino and Microsoft collaboration platforms. Over 5,000 customers and more than 4 million users worldwide trust in GBS expertise. The company operates in Europe, North America and Asia.

© 2020 GBS Europa GmbH

Our product descriptions are of a general and descriptive nature only. They do not stipulate any specific features nor do they represent any form of warranty or guarantee. We reserve the right to change the specifications and design of our products without notice at any time, in particular in order to keep abreast of technical developments.

The information contained in this document presents the topics from the viewpoint of GBS Europa GmbH (hereafter 'GBS') at the time of publishing. Since GBS needs to be able to react to changing market requirements, this is not an obligation for GBS and GBS cannot guarantee that the information presented in it is accurate after the publication date.

This document is intended for information purposes only. GBS does not extend warranty for this document, in either explicit or implied form. This also applies to quality, execution, standard commercial practice or suitability for a particular purpose.

All the product and company names that appear in this document may be trademarks of their respective owners.

Website:	www.gbs.com
Email address:	info@gbs.com
Locations:	www.gbs.com/en/locations