

Byteman

Programmer's Guide

Version 1.2.0

1st December 2009

Table of Contents

Introduction to Byteman.....	4
Running an Application with the Byteman agent.....	4
Event Condition Action Rules.....	4
Rule Bindings and Parameterization.....	5
Built-in Conditions and Actions.....	6
Extending or Replacing the Byteman Language Built-ins.....	6
Agent Transformation.....	7
Agent Retransformation.....	8
ECA Rule Engine.....	8
The Byteman Rule Language.....	10
Rule Events.....	10
Class Rules vs Interface Rules.....	11
Overriding Rules.....	11
Location Specifiers.....	12
Rule Bindings.....	14
Rule Expressions.....	15
Rule Conditions.....	16
Rule Actions.....	17
Built-In Calls.....	18
User-Defined Rule Helpers.....	18
Byteman Rule Language Standard Built-Ins.....	20
Thread Coordination Operations.....	20
Waiters.....	20
Rendezvous.....	21
Joiners.....	22
Aborting Execution.....	22
Rule State Management Operations.....	23
CountDowns.....	23
Flags.....	24
Counters.....	24
Recursive Triggering.....	25
Trace and Debug Operations.....	26
Debugging.....	26
Tracing.....	26
Using Byteman.....	28
Downloading a binary release.....	28
Obtaining the sources.....	28
Building Byteman from the sources.....	28
Running Applications with Byteman.....	28
Available -javaagent Options.....	29
Running Byteman Using Script bmjava.sh.....	30
Submitting Rules Dynamically Using Script submit.sh.....	30
Checking Rules Offline Using Script bytemancheck.sh.....	32
Environment Settings.....	32

Legal Notices

The information contained in this documentation is subject to change without notice. Red Hat Middleware LLC makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Red Hat Middleware LLC shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Copyright

JBoss, Home of Professional Open Source. Copyright 2008, Red Hat Middleware LLC, and individual contributors by the @authors tag. See the copyright.txt in the distribution for a full listing of individual contributors.

This copyrighted material is made available to anyone wishing to use, modify, copy, or redistribute it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.. This material is distributed in the hope that it will be useful, but WITHOUT A WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

See the GNU General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this software; if not, write to the Free Software Foundation, Inc., 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA, or see the FSF site: <http://www.fsf.org>.

Restricted Rights Legend

Use, duplication, or disclosure is subject to restrictions as set forth in contract subdivision (c)(1)(ii) of the Rights in Technical Data and Computer Software clause 52.227-FAR14.

Introduction to Byteman

Byteman is a scripting tool designed primarily to support automation of tests for multi-threaded and multi-JVM Java applications via fault injection. It uses bytecode transformation to modify the runtime execution of the application without having to modify the source code. The possible modifications are essentially unlimited but the tool provides explicit support for test automation in three main areas:

- tracing application execution
- short-circuiting normal method execution via early returns or exceptions
- orchestrating the timing of activities performed by independent application threads

Byteman is actually more general than this description appears to suggest. The core engine which underlies Byteman is a general purpose code injection program based around Event Condition Action (ECA) rules. Obviously, tracing code or short-circuiting execution can be useful for a variety of purposes. The thread management functionality in the Byteman script language which is specifically geared towards test automation is provided via a simple POJO plug-in. It is trivial to modify and/or extend the script language to support language operations which are specific to other application domains. Indeed this can be done on a piecemeal basis for individual rules. So, it is possible to use Byteman to inject ad hoc modifications into all sorts of applications.

Running an Application with the Byteman agent

In order to use Byteman to test a Java application the JVM must be started using the `-javaagent` command line argument. The trailing text appended to this argument points the JVM at a jar containing the Byteman rule engine. It also identifies the location of one or more Byteman rule scripts, files comprising a sequence of ECA rules specifying the side-effects to be introduced into the application under test. The engine reads these scripts when the application is launched and applies the rules to any code which matches a rule in the supplied scripts. Breaking up rules into separate scripts makes it easier to manage independent rules and enables reuse of rules across related tests. It is also possible to upload scripts containing new rules or new definitions of existing rules while the application is running. Full details are provided in subsection Running Applications with Byteman.

Event Condition Action Rules

The Byteman rule engine operates by introducing side-effects at specified points during execution. A Byteman script comprises a sequence of Event Condition Action (ECA) rules which specify precisely how the application behaviour should be transformed at runtime. The three components of these rules, event, condition and action, are used, respectively, to define:

- *where* during application execution a side-effect should occur
- *whether* the side-effect should happen or not
- *what* the side effect should be

For example, in the following example rule the event is defined by the `CLASS`, `METHOD` and `AT INVOKE` clauses. It specifies a trigger point in method `get()` of class `BoundedBuffer`. The example assumes that the definition of method `get()` includes a call to `Object.wait()` (this would be appropriate if the buffer were empty). The location specifier `AT INVOKE` places the trigger point just before the call to this method.

```

RULE throw on Nth empty get
CLASS org.my.BoundedBuffer
METHOD get()
AT INVOKE Object.wait()
BIND buffer = $this
IF countdown(buffer)
DO throw org.my.ClosedException(buffer)
ENDRULE

```

The event also includes a BIND clause which establishes a binding for local variable `buffer` assigning it with the value `$this` (a rather artificial thing to do but this is an example). `$this` is an automatic binding which refers to the target of the `get()` call which triggered the rule. `buffer` can be referred to later in the rule; in this case it is passed as an argument to the exception constructor in the DO clause.

The condition is defined by the IF clause. It invokes the standard Byteman built-in `countdown(Object)` which decrements a `CountDown` associated with the `buffer` — the example assumes some other rule has called `createCountDown(buffer, N)` to create this `CountDown` and initialise it with value `N`. The `countdown` built-in returns true when the value of the `CountDown` decrements to zero.

The action is defined by the DO clause. It causes an instance of `ClosedException` to be created and thrown from the `get()` call which triggered the rule.

So, in this example the condition will evaluate to false the first `N-1` times that a getter attempts to wait. At the `N`th triggering the condition will evaluate to true and the rule will fire, running the built-in action `throw`. This will cause the triggering thread to throw a `ClosedException` to the caller of method `get()`.

Rule Bindings and Parameterization

The corresponding rule to set up the `countDown` might be defined as follows

```

RULE set up buffer countDown
CLASS org.my.BoundedBuffer
METHOD <init>(int)
AT EXIT
BIND buffer = $0,
      size = $1
IF $1 < 100
DO createCountDown(buffer, size - 1)
ENDRULE

```

This rule is attached to the constructor for class `BoundedBuffer` which takes a single `int` parameter. The `AT EXIT` location means it is triggered just before the constructor returns. The BIND clause employs the indexed notation to refer to the method target, `$0`, and the first argument `$1`. The latter is assumed for the sake of the example to be the buffer size. If the buffer size is less than 100 then the rule creates a `countDown` with count `size - 1` using the buffer as a key to identify it.

Notice how the parameterization of the `createCountDown` and `countDown` calls with the bound variable `buffer` restricts the scope of these rules to specific cases. If there are two buffers, `buffer1` and `buffer2`, but only `buffer1` has size less than 100 then the condition for the set up rule will return false when `buffer2` is created. This means the action will not run and a `countDown` will not be associated with `buffer2`. When a

subsequent call is made to `buffer2.get()` the throw rule will be triggered but the condition will always return false and the rule will not fire.

If instead both buffers have size less than 100 then two `countDowns` will be created. The throw rule will be triggered when either `buffer1.get()` and `buffer2.get()` is called and in both cases will eventually fire and throw an exception. However, each `countDown` will still decrement independently.

Built-in Conditions and Actions

Byteman provides a suite of built-in conditions and actions used to coordinate the activities of independent threads e.g. delays, waits and signals, countdowns, flag operations and so on. These are particularly useful for testing multi-threaded programs subject to arbitrary scheduling orders. Judicious insertion of byteman actions can guarantee that thread interleavings in a given test run will occur in a desired order, enabling test code to reliably exercise parallel execution paths which do not normally occur with synthetic workloads.

Tracing operations are also provided so that test scripts can track progress of a test run and identify successful or unsuccessful test completion. Trace output can also be used to debug rule execution. The use of local context data in rule conditions allows trace output to be quite finely tuned. Trace actions can insert this data into message strings, allowing detailed scrutiny of test execution paths.

A few special built-in actions can be used to subvert the behaviour of application code by modifying execution paths. This is particularly important in a test environment where it is often necessary to force application methods to generate dummy results or simulate an error.

A *return* action forces an early return from the code location targeted by the rule. If the method is non-void then the return action supplies a value to use as the method result.

A *throw* action enables runtime exceptions (i.e. instances of `RuntimeException` or its subclasses) to be thrown from any target location, effectively either aborting a thread or, at least, where a catch-all handler is employed, the portion of the thread's call tree between the rule location and the catch block. Other exceptions may be thrown so long as the method in which the rule is located declares the exception in its throws list. Finally, a *kill* action allows a machine crash to be simulated by configuring an immediate exit from the JVM.

It is worth noting that rules are not just restricted to using built-in operations. Application-specific side-effects can also be introduced by invoking public Java methods in rule events, conditions or actions. The obvious target for such methods is objects supplied from the triggering method using bindings. However, it is also possible to access static data and invoke static methods of any class accessible from the classloader of the triggering method. So, it is quite feasible to use Byteman rules to apply arbitrary modifications to the original program.

Extending or Replacing the Byteman Language Built-ins

Another option to bear in mind is that the set of built-in operations available to Byteman rules is not fixed. The rule engine works by mapping built-in operations which occur in a given rule to public instance methods of a helper class associated with the rule. By default, this helper class is `org.jboss.byteman.rule.helper.Helper`, which provides the standard set of built-ins designed to simplify management of threads in a multi-threaded application. For example, the builtin operations `createCountDown()` and `countDown()`

used in the example rules provided above are just public methods of class `Helper`. The set of built-ins available for use in a given rule can be changed merely by specifying an alternative helper class for that rule.

Any non-abstract class may be specified as the helper. Its public instance methods automatically become available as built-in operations in the rule event, condition and action. For example, by specifying a helper class which extended the default class, `Helper`, a rule would be able to use any of the existing built-ins and/or also make rule-specific (or application-specific) built-in calls. So, although the default ByteMan rule language is oriented towards orchestrating the behaviour of independent threads in multi-threaded tests, ByteMan can easily be reconfigured to support a much wider range of application requirements.

Agent Transformation

The bytecode modifications performed by ByteMan are implemented using a *Java agent* program. JVM class loaders provide agents with an opportunity to modify loaded bytecode just prior to compilation (see package `java.lang.Instrumentation` for details of how Java agents work). The ByteMan agent reads the rule script at JVM bootstrap. It then monitors method code as it is loaded looking for *trigger points*, locations in the method bytecode which match the locations specified in rule events.

The agent inserts *trigger calls* into code at each point which matches a rule event. Trigger calls are calls to the rule execution engine which identify:

- the *trigger method*, i.e. the method which contains the trigger point
- the rule which has been matched
- the arguments to the trigger method

If several rules match the same trigger point then there will be a sequence of trigger calls, one for each matching rule. In this case rules are mostly triggered in the order they appear in their script(s). The only exception is rules which specify an AFTER location, such as `AFTER READ myField` or `AFTER INVOKE someMethod`, which are executed in reverse order of appearance.

When a trigger call occurs the rule execution engine locates the relevant rule and then executes it. The rule execution engine establishes bindings for variables mentioned in the rule event and then *tests* the rule condition. If the condition evaluates to true it *fires* the rule, executing each of the rule actions in sequence.

Trigger calls pass the method recipient (this) and method arguments to the rule engine. These values may be referred to in the condition and action with a standard naming convention, `$0`, `$1` etc. The event specification can introduce bindings for additional variables. Bindings for these variables may be initialized using literal data or by invoking methods or operations on the method parameters and/or static data. Variables bound in the event can simply be referred to by name in the condition or action. Bindings allow arbitrary data from the triggering context to be tested in the condition in order to decide whether to fire the rule and to be employed as a target or parameter for rule actions. Note that where the trigger code is compiled with the relevant debug options enabled the agent is able to pass local variables which are in scope at the trigger point as arguments to the trigger call, making them available as default bindings. Rules may refer to in-scope variables (including the method recipient and arguments) by prefixing their symbolic names with the `$` character e.g. `$this`, `$arg1`, `$i` etc.

The agent also compiles exception handler code around the trigger calls in order to deal

with exceptions which might arise during rule processing. This is not intended to handle errors detected during operation of the rule execution engine (they should all be caught and dealt with internally). Exceptions are thrown out of the execution engine to alter the flow of control through the triggering method. Normally, after returning from a trigger call the triggering thread continues to execute the original method code. However, a rule can use the `return` and `throw` built-in actions to specify that an early return or exception throw should be performed *from the trigger method*. The rule language implementation achieves this by throwing its own private, internal exceptions below the trigger call. The handler code compiled into the trigger method catches these internal exceptions and then either returns to the caller or recursively throws a runtime or application-specific exception. This avoids normal execution of the remaining code in the body of the triggering method. If there are other trigger calls pending at the trigger point then these are also bypassed when a return or throw action is executed.

Agent Retransformation

The agent also allows rules to be uploaded while the application is still running. This can be used to redefine previously loaded rules as well as to introduce new rules on the fly. In cases where no currently loaded class matches the uploaded rule the agent merely adds the new rule to the current rule set. This may possibly replace an earlier version of the rule (rules are equated if they have the same name). When a matching class is loaded the latest version of the rule will be used to transform it.

In cases where there are already loaded classes which match the rule the agent will retransform them, modifying the relevant target methods to include any necessary trigger calls. If an uploaded rule replaces an existing rule in this situation then when the previous rule is deleted all trigger calls associated with it are removed from the affected target methods. Note that retransforming a class does not associate a new class object with existing instances of the class. It merely installs a different implementation for their methods.

An important point where retransformation may occur automatically without an explicit upload is during bootstrap of the agent. The JVM needs to load various of its own bootstrap classes before it can start the agent and allow it to register a transformer. Once the agent has processed the initial rule set and registered a transformer it scans all currently loaded classes and identifies those which match rules in the rule set. It automatically retransforms these classes, causing subsequent calls to bootstrap code to trigger rule processing.

ECA Rule Engine

The Byteman rule execution engine consists of a rule parser, type checker and interpreter/compiler. The rule parser is invoked by the agent during bootstrap. This provides enough information to enable the agent to identify potential trigger points.

Rules are not type checked and compiled during trigger injection. These steps are delayed until the class and method bytecode they refer to has been loaded. Type checking requires identifying properties of the trigger class and, potentially, of classes it mentions using reflection. To do this the type checker needs to identify properties of loaded classes such as the types and accessibility of fields, method signatures etc. So, in order to ensure that the trigger class and all its dependent classes have been loaded before the type checker tries to access them, rules are type checked and compiled the first time they are triggered. This also avoids the cost of checking and compiling rules included in the rule set which do not actually get called.

A single rule may be associated with more than one trigger point. Firstly, depending upon how precisely the rule specifies its event, it may apply to more than one class or more than one method within a class. But secondly, even if a rule specifies a class and method unambiguously the same class file may be loaded by different class loaders. So, the rule has to be type checked and compiled for each applicable trigger point.

If a type check or compile operation fails the rule engine prints an error and disables execution of the trigger call. Note that in cases where the event specification is ambiguous a rule may type check successfully against one trigger point but not against another. Rule execution is only disabled for cases where the type check fails.

In the basic operating mode, trigger calls execute a rule by interpreting the rule parse tree. It is also possible to configure the rule engine to translate the rule bindings, condition and actions to bytecode which can then be passed by the JIT compiler. In either case, execution is performed with the help of an auxiliary class generated at runtime by the Byteman agent called a *helper adapter*. This class is actually a subclass of the helper class associated with the rule. It inherits from the helper class so that it knows how to execute built-in operations defined by the helper class. A subclass is used to add extra functionality required by the rule system, most notably method `execute` which gets called at the trigger point and a local bindings field which stores a hashmap mapping method parameters and event variables to their bound values.

When a rule is triggered the rule engine creates an instance of the rule's helper adapter class to provide a context for the trigger call. It uses setter methods generated by the Byteman agent to initialise the rule and bindings fields and then it calls the adapter instance's `execute` method. Since each rule triggering is handled by its own adapter instance this ensures that concurrent triggers of the same rule from different threads do not interfere with each other.

The interpreted version of `execute` locates the triggered rule and, from there, the parse tree for the event, condition and action. It traverses the parse trees of these three rule components evaluating each expression recursively. Bindings are looked up or assigned during rule execution when they are referred to from within the rule event, condition or action. When the `execute` method encounters a call to a built-in it can execute this call using reflection to invoke one of the methods inherited from its helper superclass.

When compilation of rules is enabled the Byteman agent generates an `execute` method which contains inline bytecode derived from the rule event condition and action. This directly encodes all the operations and method invocations defined in the rule. This code accesses bindings and executes built-ins in the same way as the interpreted code except that calls to built-in are compiled as direct method invocations on this rather than relying on reflective invocation.

Although compilation takes slightly more time to generate it should provide a performance pay off where the trigger method gets called many times. Ideally, compilation should be selectable per rule or across the board for all rules in a rule set. At present it can only be enabled or disabled globally.

The Byteman Rule Language

Rules are defined in scripts which consists of a sequence of rule definitions interleaved with comment lines. Comments may occur within the body of a rule definition as well as preceding or following a definition but must be on separate lines from the rule text.

Comments are lines which begin with a # character:

```
#####  
# Example Rule Set  
#  
# a single rule definition  
RULE example rule  
# comment line in rule body  
.  
.  
.  
ENDRULE
```

Rule Events

Rule event specifications identify a specific *location* in a *target* method associated with a *target* class. Target methods can be either static or instance methods or constructors. If no detailed location is specified the default location is entry to the target method. So, the basic schema for a single rule is as follows:

```
# rule skeleton  
RULE <rule name>  
CLASS <class name>  
METHOD <method name>  
BIND <bindings>  
IF <condition>  
DO <actions>  
ENDRULE
```

The name of the rule following the RULE keyword can be any free form text with the restriction that it must include at least one non-white space character. Rule names do not have to be unique but it obviously helps when debugging rule scripts if they clearly identify the rule. The rule name is printed whenever an error is encountered during parsing, type checking, compilation or execution.

The class and method names following the CLASS and METHOD keywords must be on the same line. The class name can identify a class either with or without the package qualification. The method name can identify a method with or without an argument list or return type. A constructor method is identified using the special name <init>. For example,

```
# class and method example  
RULE any commit on any coordinator engine  
CLASS CoordinatorEngine  
METHOD commit  
.  
.  
.  
ENDRULE
```

matches the rule with any class whose name is CoordinatorEngine, irrespective of the package it belongs to. When any class with this name is loaded then the agent will insert a trigger point at the beginning of any method named commit. If there are several occurrences of this method, with different signatures then each method will have a trigger

point inserted.

More precise matches can be guaranteed by adding more detail. For example,

```
# class and method example 2
RULE commit with no arguments on wst11 coordinator engine
CLASS com.arjuna.wst11.messaging.engines.CoordinatorEngine
METHOD State commit()
AT LINE 324
. . .
ENDRULE
```

This rule will only match the `CoordinatorEngine` class in package `com.arjuna.wst11.messaging.engines` and only match a method `commit` with no arguments and with a return type whose name is `State`. Note that the package for class `State` is left unspecified. The type checker infers this information from the matched method.

The previous example also employs the location specifier `AT LINE`. The text following the line keyword must be able to be parsed to derive an integer line number. This directs the agent to insert the trigger call at the start of a particular line in the source code.

Note:

The Byteman agent *will not* transform any classes in package `java.lang` nor classes in package `org.jboss.byteman`, the byteman package itself (it is possible to remove the first of these restrictions by setting a System property, but you need to be really sure you know what you are doing – see below for details).

Class Rules vs Interface Rules

Byteman rules can be attached to interfaces as well as classes. If the `CLASS` keyword is replaced with the keyword `INTERFACE` then the rule applies to any class which implements the specified interface. For example, the following rule

```
# interface rule example
RULE commit with no arguments on any engine
INTERFACE com.arjuna.wst11.messaging.engines.Engine
METHOD commit()
. . .
ENDRULE
```

is attached to method `commit` of interface `Engine`. If `Engine` is implemented by classes `CoordinatorEngine` and `ParticipantEngine` then the rule implies two trigger points, one at the start of method `CoordinatorEngine.commit()` and another at the start of method `ParticipantEngine.commit()`. The agent ensures that each implementing class is transformed to include a trigger call for the rule.

Overriding Rules

Normally, Byteman only injects rule code into methods which are defined by the class identified in the `CLASS` clause. This is sometimes not very helpful. For example, the following rule is not much use

```

RULE trace Object.finalize
CLASS java.lang.Object
METHOD finalize
IF TRUE
DO System.out.println("Finalizing " + $0)
DONE

```

The print statement gets inserted into method `Object.finalize()`. However, the JVM only calls `finalize` when an object's class overrides `Object.finalize()`. But with this rule these overriding methods are not modified. So, the rule will not be triggered in the precise case where the trace would be useful (n.b. this is not quite the full story – overriding method implementations which call `super.finalize()` *will* trigger the rule). There are many other situations where it might be desirable to inject code into overriding method implementations. For example, class `Socket` is specialised by various classes which provide their own implementation of methods `bind`, `accept` etc. So, a rule attached to `Socket.bind()` will not be triggered when the `bind` method of one of these subclasses is called (not unless the subclass method calls `super.bind()`).

Of course, it is always possible to define a specific rule for each overriding class. However, this is tedious and may possibly miss some cases when the code base is changed. So, Byteman provides a simple bit of syntax for specifying that rules should also be injected into overriding implementations.

```

RULE trace Object.finalize
CLASS ^java.lang.Object
METHOD finalize
IF TRUE
DO System.out.println("Finalizing " + $0)
DONE

```

The `^` prefix attached to the class name tells the agent that the rule should apply to implementations of `finalize` defined either by class `Object` or by any class which extends `Object`. This prefix can also be used with interface rules, requiring the agent to inject the rule code into methods of classes which implement the interface and also into overriding methods on subclasses of the implementing classes.

Note that if an overriding method invokes a super method then this style of injection may cause the injected rule code to be triggered more than once. In particular, injecting into constructors (which, inevitably, invoke some form of super constructor) will often result in multiple triggerings of the rule.

Location Specifiers

The examples above either specified the precise location of the trigger point within the target method to a specific line number using `AT LINE` or defaulted it to the start of the method. Clearly, line numbers can be used to specify almost any point during execution and are easy and convenient to use in code which is not subject to change. However, this approach is not very useful for test automation where the code under test will frequently be modified. Obviously when code is edited the associated tests need to be revised. But modifications to the code base can easily shift the line numbers of unmodified code invalidating test scripts unrelated to the edits. Luckily, there are several other ways of specifying where a trigger point should be inserted into a target method. For example,

```
# location specifier example
RULE countdown at commit
CLASS CoordinatorEngine
METHOD commit
AT READ state
. . .
ENDRULE
```

In this rule the trigger point will be inserted just before the first location in the bytecode where a `getField` operation is performed on field called `state`. This is effectively the same as saying that the trigger point will occur at the first point in the source code of the method where field `state` is accessed. By contrast, the following rule would locate the trigger point after the first write to field `recovered`:

```
# location specifier example 2
RULE add countdown at recreate
CLASS CoordinatorEngine
METHOD <init>
AFTER WRITE CoordinatorEngine.recovered
. . .
ENDRULE
```

Note that in the last example the field type is qualified to ensure that the write is to the field belonging to an instance of class `CoordinatorEngine`.

The full set of location specifiers is as follows

```
AT ENTRY
AT EXIT
AT LINE number
AT READ [ type . ] field [ count ]
AFTER READ [ type . ] field [ count ]
AT WRITE [ type . ] field [ count ]
AFTER WRITE [ type . ] field [ count ]
AT INVOKE [ type . ] method [ ( argtypes ) ] [ count ]
AFTER INVOKE [ type . ] method [ ( argtypes ) ] [ count ]
AT SYNCHRONIZE [ count ]
AFTER SYNCHRONIZE [ count ]
AT THROW [ typename ] [ count ]
```

If a location specifier is provided it must immediately follow the `METHOD` specifier. If no location specifier is provided it defaults to `AT ENTRY`.

An `AT ENTRY` specifier normally locates the trigger point before the first executable instruction in the trigger method. An exception to this occurs in the case of a constructor method in which case the trigger point is located before the first instruction following the call to the super constructor or redirection call to an alternative constructor. This is necessary to ensure that rules do not attempt to bind and operate on the instance before it is constructed

An `AT EXIT` specifier locates a trigger point at each location in the trigger method where a normal return of control occurs (i.e. wherever there is an implicit or explicit return but not where a throw exits the method).

An `AT LINE` specifier locates the trigger point before the first executable bytecode instruction in the trigger method whose source line number is greater than or equal to the line number supplied as argument to the specifier. If there is no executable code at (or

following) the specified line number the agent will not insert a trigger point (note that it does not print an error in such cases because this may merely indicate that the rule does not apply to this particular class or method).

An `AT READ` specifier locates the trigger point before the first mention of an object field whose name matches the supplied field name i.e. it corresponds to the first occurred of a corresponding `getField` instruction in the bytecode. If a type is specified then the `getField` instruction will only be matched if the named field is declared by a class whose name matches the supplied type. If a count N is supplied then the N th matching `getField` will be used as the trigger point. Note that the count identifies to the N th textual occurrence of the field access, not the N th field access in a particular execution path at runtime.

An `AFTER READ` specification is identical to an `AT READ` specification except that it locates the trigger point after the `getField` bytecode.

`AT WRITE` and `AFTER WRITE` specifiers are the same as the corresponding `READ` specifiers except that they correspond to assignments to the named field in the source code i.e. they identify `putField` instructions.

`AT INVOKE` and `AFTER INVOKE` specifiers are like `READ` and `WRITE` specifiers except that they identify invocations of methods or constructors within the trigger method as the trigger point. The method may be identified using a bare method name or the name may be qualified by a, possibly package-qualified, type or by a descriptor. A descriptor consists of a comma-separated list of type names within brackets. The type names identify the types of the method parameters and may be prefixed with package qualifiers and employ array bracket pairs as suffixes.

`AT SYNCHRONIZE` and `AFTER SYNCHRONIZE` specifiers identify synchronization blocks in the target method, i.e. they correspond to `MONITORENTER` instructions in the bytecode. Note that `AFTER SYNCHRONIZE` identifies the point immediately after entry to the synchronized block rather than the point immediately after exit from the block.

An `AT THROW` specifier identifies a throw operation within the trigger method as the trigger point. The throw operation may be qualified by a, possibly package-qualified, typename identifying the lexical type of the thrown exception. If a count N is supplied then the location specifies the N th textual occurrence of a throw. n.b. the exception typename is ignored in the current release.

n.b. as mentioned previously, when several rules specify the same location the order of injection of trigger calls usually follows the order of the rules in their respective scripts. The exception to this is `AFTER` locations where the the order of injection is the reverse to the order of occurrence.

n.b.b. when a location specifier (other than `ENTRY` or `EXIT`) is used with an overriding rule the rule code is only injected into the original method or overriding methods if the location matches the method in question. So, for example, if location `AT READ myField 2` is employed then the rule will only be injected into implementations of the method which include two loads of field `myField`. Methods which do not match the location are ignored.

n.b.b.b. for hysterical reasons `CALL` may be used as a synonym for `INVOKE`, `RETURN` may be used as a synonym for `EXIT` and the `AT` in an `AT LINE` specifier is optional.

Rule Bindings

The event specification includes a binding specification which computes values for

variables which can subsequently be referenced in the rule body. These values will be computed each time the rule is triggered before testing the rule condition. For example,

```
# binding example
RULE countdown at commit
CLASS com.arjuna.wst11.messaging.engines.CoordinatorEngine
METHOD commit
AT READ state
BIND engine:CoordinatorEngine = $0,
    recovered:boolean = engine.isRecovered(),
    identifier:String = engine.getId()
. . .
ENDRULE
```

creates a variable called `engine`. This variable is bound to the recipient of the `commit` method call which triggered the rule, identified by the parameter reference `$0` (if `commit` was a static method then reference to `$0` would result in a type check exception). Arguments to the trigger method can be identified using parameter references with successive indices, `$1`, `$2` etc. The declaration of `engine` specifies its type as being `CoordinatorEngine` though this is not strictly necessary since it can be inferred from the type of `$0`.

Similarly, variables `recovered` and `identifier` are bound by evaluating the expressions on the right of the `=` operator. Note that the binding for `engine` has been established before these variables are bound so it can be referenced in the evaluated expression. Once again, type specifications are provided but they could be inferred.

The special syntax `BIND NOTHING` is available for cases where the rule does not need to employ any bindings. Alternatively, the `BIND` clause may be omitted.

Rule Expressions

Expressions which occur on the right hand side of the `=` operator in event bindings can be simple expressions i.e.

- references to previously bound variables
- references to the trigger method recipient or arguments
- references to the local variables in scope at the trigger point
- static field references
- primitive literals
- field accesses
- static or instance method invocations
- built-in operation invocations

n.b. built-in operations are explained in more detail below.

Expressions can also be complex expressions composed from other expressions using the usual Java operators: `+`, `-`, `*`, `/`, `%`, `&`, `|`, `^`, `&&`, `||`, `!`, `==`, `!=`, `<`, `<=`, `>`, `>=`, etc. The ternary conditional expression operator, `? :`, can also be employed. The type checker does its best to identify the types of simple and complex expressions wherever possible. So, for example, if it knows the type of bound variable `engine` then it will be able to employ reflection to infer the type of a field access `engine.recovered`, a method invocation

`engine.isRecovered()`, etc.

Note:

- The assignment operator is not available for use in expressions. It can only be employed at the top level in binding specifications.
- Use of the new operator is not currently allowed in expressions.
- `throw` and `return` operations are only allowed as the last action in a sequence of rule actions (see below).
- Expressions should obey the normal rules regarding associativity and precedence.
- The trigger method recipient and arguments may be referred to by index using the symbols `$0` (invalid for a static method), `$1` etc. If the method has been compiled with the relevant debug options then symbolic references may also be used. So, for example, `$this` may be used as an alias for `$0` and `$myArg` may be used as an alias for `$1` if the method first parameter is declared with name `myArg`,
- If the trigger method has been compiled with the relevant debug options then local variables may be referenced symbolically using the same syntax to method parameters. So, for example, if variable `idx` is in scope at the trigger point then `$idx` can be used to obtain its value.

Rule Conditions

Rule conditions are nothing more than rule expressions with boolean type. For example,

```
# condition example
RULE countdown at commit
CLASS com.arjuna.wst11.messaging.engines.CoordinatorEngine
METHOD commit
AT READ state
BIND engine:CoordinatorEngine = $this,
      recovered:boolean = engine.isRecovered(),
      identifier:String = engine.getId()
IF   recovered
. . .
ENDRULE
```

merely tests the value of bound variable `recovered`. The same effect could be achieved by using the following condition

```
# condition example 2
RULE countdown at commit
CLASS com.arjuna.wst11.messaging.engines.CoordinatorEngine
METHOD commit
AT READ state
BIND engine:CoordinatorEngine = $this,
. . .
IF   engine.isRecovered()
. . .
ENDRULE
```

Alternatively, if, say, the instance employed a public field, `recovered`, to store the boolean value returned by method `isRecovered` then the same effect would be achieved by the following condition.


```

# condition example 3
RULE countdown at commit
CLASS com.arjuna.wst11.messaging.engines.CoordinatorEngine
METHOD commit
AT READ state
BIND engine:CoordinatorEngine = $this,

    . . .
IF    engine.recovered
    . . .
ENDRULE

```

Note that the boolean literal `true` is available for use in expressions so a rule which should always fire can use this as the condition expression.

Rule Actions

Rule actions are either a rule expression or a return or throw expression or a comma-separated sequence of rule expressions, possibly ending with a return or throw expression. Rule expressions occurring in an action list may have arbitrary type, including void type.

A return expressions is the `return` keyword possibly followed by a rule expression which is used to compute a return value. A return expression causes a return from the triggering method so it may omit a return value if and only if the method is void. If a return value is employed then the type checker will ensure that it's type is assignable to the return type of the trigger method. So, for example, the following use of `return` is legitimate assuming method `commit` has return type `boolean`:

```

# return example
RULE countdown at commit
CLASS com.arjuna.wst11.messaging.engines.CoordinatorEngine
METHOD commit
AT READ state
    . . .
DO  debug("returning early with failure"),
    return false
ENDRULE

```

A throw expression is the `throw` keyword followed by an exception constructor expression. An exception constructor expression is the class name of the exception which is to be thrown followed by an argument list. The argument list may be empty i.e. it may consist of an open and close bracket pair. Alternatively, the brackets may include a single rule expression or a sequence of rule expressions separated by commas. If no arguments are supplied the exception type must implement an empty constructor. If arguments are supplied then the exception type must implement a constructor whose signature is type-compatible.

A throw expression causes an exception of the type named in the exception constructor to be created and thrown from the triggering method. In order for this to be valid the expression type must either be assignable to `java.lang.RuntimeException` or be explicitly declared in the triggering method's `throws` list. The type checker will throw a type exception if either of these conditions is not met. So, for example, the following use of `throw` is legitimate assuming method `commit` includes `WrongStateException` in its `throws` list.

```

# throw example
RULE countdown at commit
CLASS com.arjuna.wst11.messaging.engines.CoordinatorEngine
METHOD commit
AT READ state
    . . .
DO debug("throwing wrong state"),
    throw WrongStateException()
ENDRULE

```

An empty action list may be specified using the keyword NOTHING.

Built-In Calls

Built-in calls are written without a recipient as though they were invocations of a method on `this`. The rule engine identifies calls in this format and translates them to runtime invocations of helper class instance methods. So, referring back to the last few examples, it is apparent that the helper class implements a debugging method with signature

```
boolean debug(String message)
```

This method prints the supplied string to `System.out` and always returns true. It can be used in a rule action to display a trace message, for example:

```
DO    debug("killing JVM"), killJVM()
```

When the debug built-in is executed the rule engine calls the corresponding method of the current helper instance passing it the string "killing JVM". Method `killJVM` is another built-in implemented by an instance method of the default helper class `Helper`.

Note that method `debug` has a boolean signature so that tracing can also be performed in rule conditions. This would normally occur in combination with a test of some bound variable or method parameter, for example:

```

IF    debug("checking for recovered participant")
    AND
    participant.isRecovered()
    AND
    debug("recovered participant " + participant.getId())

```

n.b. AND is an alternative token for the Java `&&` operator.

The rule language implementation automatically exposes all public instance methods of class `Helper` as built-in operations. So when the rule type checker encounters an invocation of `debug` with no recipient supplied it identifies that `debug` is a method of class `Helper` and automatically type checks the call against this method. At execution time the call is executed by invoking the implementation of `debug` on the helper instance created under the rule trigger call.

This feature allows additional built-ins to be added to the rule engine simply by adding new helper implementations. No changes are required to the parser, type checker and compiler in order for this to work.

User-Defined Rule Helpers

A rule can specify its own helper class if it wants to extend, override or replace the set of built-in calls available for use in its event, condition or action. For example, in the following

rule, class `FailureTester` is used as the helper class. Its boolean instance method `doWrongState(CoordinatorEngine)` is called from the condition to decide whether or not to throw a `WrongStateException`.

```
# helper example
RULE help yourself
CLASS com.arjuna.wst11.messaging.engines.CoordinatorEngine
METHOD commit
HELPER com.arjuna.wst11.messaging.engines.FailureTester
AT EXIT
IF doWrongState($0)
DO throw WrongStateException()
ENDRULE
```

A helper class does not need to implement any special interface or inherit from any pre-defined class. It merely needs to provide instance methods to resolve the built-in calls which occur in the rule. By sub-classing the default helper it is possible to extend or override the default set of methods. For example, the following rule employs a helper which adds emphasis to the debug messages printed by the rule.

```
# helper example 2
RULE help yourself but rely on others
CLASS com.arjuna.wst11.messaging.engines.CoordinatorEngine
METHOD commit
HELPER HelperSub
AT ENTRY
IF NOT flagged($this)
DO debug("throwing wrong state"),
    flag($this)
    throw WrongStateException()
ENDRULE
```

```
class HelperSub extends Helper
{
    public boolean debug(String message)
    {
        super("!!! IMPORTANT EVENT !!! " + message);
    }
}
```

The rule is still able to employ the built-in methods `flag` and `flagged` defined by the default helper class.

Byteman Rule Language Standard Built-Ins

The default helper class provides the following standard suite of built-in calls for use in rule expressions. These are primarily intended for use in condition and action expressions but they may also be called in event bindings. They provide features which are designed to make it easy to perform complex tests, in particular to coordinate the actions of threads in multi-threaded applications. Built-in operations divide into three categories, thread coordination operations, rule state management operations and trace and debug operations

Thread Coordination Operations

Waiters

The rule engine provides Waiters used to suspend threads during rule execution and then have other threads wake them up. The wakeup can simply allow the suspended thread to resume execution of the rule which suspended it. Alternatively, it can force the waiting thread to exit from the triggering method with an exception. The API defined by the helper class is

```
public void waitFor(Object identifier)
public void waitFor(Object identifier, long millisecsWait)
public boolean waiting(Object identifier)
public boolean signalWake(Object identifier)
public boolean signalWake(Object identifier, boolean
mustMeet)
public boolean signalThrow(Object identifier)
public boolean signalThrow(Object identifier, boolean
mustMeet)
```

As with CountDowns, Waiters are identified by an arbitrary object. Note that the wait operation is not performed by invoking `Object.wait` on `identifier`. Doing so might interfere with locking and synchronization operations performed by the triggering method or its callers. The identifier is merely used by the rule engine to associate wait and signal operations. The Helper class employs it's own private Waiter object to manage the synchronization activity.

`waitFor` is intended for use in a rule action. It suspends the current thread on the Waiter associated with the identifier until either a `signalWake` or a `signalThrow` is called with the same identifier. In the former case the thread will continue processing any subsequent actions and then return from the trigger call. In the latter case the thread will throw a runtime exception from the triggering method call frame. The version without a wait parameter will never time out. The version which employs a wait parameter will time out after the specified number of milliseconds.

`waiting` is intended for use in rule conditions. it will return true if any threads are waiting on the relevant Waiter for a signal. It returns false if there are no threads waiting.

`signalWake` is intended for use in rule conditions or actions. If there are threads waiting on the Waiter associated with `identifier` it wakes them and returns true. If not it returns false. Note this behaviour ensures that a race between multiple threads to signal waiting threads from a rule condition can only have one winner.

`signalWake` takes an optional argument `mustMeet` which is useful in situations where it

cannot be guaranteed that the waiting thread will reach its trigger point before the signalling thread arrives at its trigger point. If this argument is supplied as `true` then the signalling thread will not deliver its signal until another thread is waiting. If necessary the signalling thread will suspend until a waiting thread arrives. Supplying value `false` is equivalent to omitting the optional argument.

`signalThrow` is identical to `signalWake` except that it does not just wake any waiting threads. It also causes them to throw a runtime exception of type `ExecuteException` from their triggering method call frame when they wake up.

`signalThrow` also takes an optional argument `mustMeet` which enables the same behaviour as for `signalWake`.

Rendezvous

Waiters are useful in situations where there is an asymmetrical relationship between threads: one or more threads need to wait for an event which will be signalled by the thread in which the event happens. A rendezvous provides a way of synchronizing where there is no such asymmetry. A rendezvous also provides a way of introducing asymmetry since it sorts threads by order of arrival. The value returned from the rendezvous built-in can be checked to identify, say, the first (or last) thread to arrive and that thread can be the one whose action is triggered.

```
public boolean createRendezvous(Object identifier,
                                int expected)
public boolean createRendezvous(Object identifier,
                                int expected,
                                boolean rejoinable)
public boolean rendezvous(Object identifier)
public boolean isRendezvous(Object identifier, int expected)
public int getRendezvous(Object identifier, int expected)
public int deleteRendezvous(Object identifier, int expected)
```

`createRendezvous` creates a rendezvous identified by `identifier`. `count` identifies the number of threads which must meet at the rendezvous before any one of them is allowed to continue execution. The optional argument `rejoinable` defaults to `false` in which case any attempt to meet once the first `count` threads have arrived will fail. If it is supplied as `true` then once `count` threads have arrived the rendezvous will be reset, enabling another round of meetings to occur. `createRendezvous` returns `true` if the rendezvous is created. If a rendezvous identified by `identifier` already exists it returns `false`. Note that it is legitimate (although pathological) to supply a count of 1.

`rendezvous` is called to meet other threads at a rendezvous identified by `identifier`. If the number of threads (*including the calling thread*) arrived at the rendezvous is less than the expected count then the calling thread is suspended. If the number of threads equals the expected count then all suspended threads are awoken. A rejoinable rendezvous has its arrived count reset to 0 at this point. If the rendezvous is not rejoinable then it is deleted and any subsequent call to `rendezvous` using the original identifier will return -1.

`isRendezvous` will return `true` if a rendezvous identified by `identifier` with the expected count is currently active. If there is no active rendezvous identified by `identifier` or it exists but has a different expected count then `getRendezvous` will return `false`.

`getRendezvous` will return the number of threads waiting at the rendezvous identified by

`identifier` or 0 if no threads are currently waiting. If there is no rendezvous identified by `identifier` or it exists but has a different expected count then `getRendezvous` will return -1.

`deleteRendezvous` deletes a rendezvous, breaking the association between `identifier` and the rendezvous and forcing any threads waiting under a call to rendezvous to return immediately with result -1. If a rendezvous with the correct expected count is found and successfully deleted it returns true. If there is no such rendezvous or if it is deleted either by another concurrent call to `deleteRendezvous()` or because a concurrent call to `rendezvous()` completes the rendezvous it returns false.

Joiners

Joiners are useful in situations where it is necessary to ensure that a thread does not proceed until one or more related threads have exited. This is not always a requirement for an application to execute correctly but may be necessary to validate a test scenario. For example, a socket listener thread may create connection manager threads to handle incoming connection requests. The listener might use the connection object to notify connection manager threads of a forced exit. It does not necessarily have to retain a handle on the connection thread and explicitly call `Thread.join()` to be sure the thread will exit when notified. However, a test may want to check the thread pool to be sure all activity has completed. This means the test needs to be able to accumulate a list of managed threads and then subsequently join them either from the manager thread or from a test thread.

```
public boolean createJoin(Object identifier, int expected)
public boolean isJoin(Object identifier, int expected)
public boolean joinEnlist(Object identifier, int expected)
public boolean joinWait(Object identifier, int expected)
```

`createJoin` creates a Joiner which can subsequently be referenced by `identifier`. `expected` identifies the number of threads which are to be joined. If a Joiner is created it returns true. If a Joiner is currently identified by `identifier` it returns false.

`isJoin` tests whether `identifier` identifies a Joiner with the given expected count. If a Joiner with the given expected count is currently identified by `identifier` it returns true otherwise it returns false

`joinEnlist` adds the calling thread to the list of threads associated with a Joiner and returns true, allowing the thread to proceed towards exit. If `identifier` does not identify a Joiner or identifies a Joiner with the wrong expected count it returns false. It also returns false if the calling thread is already contained in the Joiner's thread list or if the number of threads added to the list has reached the expected count.

`JoinWait` suspends the calling thread until the number of threads in the list associated with the Joiner reaches the expected count. It then joins each thread in the list and returns true. If `identifier` does not identify a Joiner or identifies a Joiner with the wrong expected count it returns false.

Aborting Execution

The rule engine provides two built-ins for use in rule actions which allow execution of the triggering method to be aborted. The API defined by the helper class is

```
public void killThread()  
public void killJVM()  
public void killJVM(int exitCode)
```

`killThread` causes a runtime exception of type `ExecuteException` to be thrown from the triggering method call frame. This will effectively kill the thread unless a catch-all exception handler is installed somewhere up the call stack.

`killJVM` results in a call to `java.lang.Runtime.getRuntime().halt()`. This effectively kills the JVM without any opportunity for any registered exit handlers to run, simulating a JVM crash. If `exitCode` is not supplied it is defaulted to `-1`

Rule State Management Operations

CountDowns

The rule engine provides `CountDowns` which can be used to ensure that firing of some given rule will only occur after other rules have been triggered or fired a certain number of times. The API defined by the helper class is

```
public boolean createCountDown(Object identifier, int count)  
public boolean getCountDown(Object identifier)  
public boolean countDown(Object identifier)
```

`CountDowns` are identified by an arbitrary object, allowing successive calls to the `countDown` API to apply to the same or different cases. This identification can be made across different rule and helper instances. For example, one rule might include action `createCountDown($0, 1)` and another rule might include condition `countDown($0)`. A `CountDown` created by the first rule would only be decremented if the second rule was triggered from a method call with the same value for `this`. `CountDowns` created by invocations with distinct values for `this` would match up accordingly. However, if the `CountDown` was identified using a common `String` literal (i.e. action and condition were `createCountDown("counter", 1)` and `countDown("counter")`, respectively), then the `CountDown` created by the first rule would be decremented by the next firing of the second rule irrespective of whether the trigger method calls were on related instances.

`createCountDown` is used to create a `CountDown`. `count` specifies how many times the `CountDown` will be decremented before a decrement operation fails i.e. if `count` is `1` then the `CountDown` will decrement once and then fail at the next decrement. If `count` is supplied with a value less than `1` it will be replaced with value `1`. `createCountDown` would normally be employed in a rule action. However, it is defined to return `true` if a new `CountDown` is created and `false` if there is already a `CountDown` associated with the identifier. This allows it to be used in rule conditions where several rules may be racing to create a `CountDown`.

`getCountDown` is for use in a rule condition to test whether a `CountDown` associated with a given identifier is present, returning `true` if so otherwise `false`.

`countDown` is for use in a rule condition to decrement a `CountDown`. It returns `false` if the decrement succeeds or if there is no `CountDown` associated with identifier. It returns `true` if the `CountDown` fails i.e. it has count `0`. In the latter case the association between the identifier and the `CountDown` is removed, allowing a new `CountDown` to be started using the same identifier. Note that this behaviour ensures that a race between multiple threads to decrement a counter from one or more rule conditions can only have one

winner.

Flags

The rule engine provides a simple mechanism for setting, testing and clearing global flags. The API defined by the helper class is

```
public boolean flag(Object identifier)
public boolean flagged(Object identifier)
public boolean clear(Object identifier)
```

As before, Flags are identified by an arbitrary object. All three methods are designed to be used either in conditions or actions.

`flag` can be called to ensure that the Flag identified by `identifier` is set. It returns `true` if the Flag was previously clear otherwise `false`. Note that the API is designed to ensure that race conditions between multiple threads trying to set a Flag from rule conditions can only have one winner.

`flagged` tests whether the Flag identified by `identifier` is set. It returns `true` if the Flag is set otherwise `false`.

`clear` can be called to ensure that the Flag identified by `identifier` is clear. It returns `true` if the Flag was previously set otherwise `false`. Note that the API is designed to ensure that race conditions between multiple threads trying to clear a Flag from rule conditions can only have one winner.

Counters

The rule engine provides Counters which maintain global counts across independent rule triggerings. They can be created and initialised, read, incremented and decremented in order track and respond to the number of times various triggerings or firings have happened. Note that unlike CountDowns there are no special semantics associated with decrementing a Counter to zero. They may even have negative values. The API defined by the helper class is

```
public boolean createCounter(Object o)
public boolean createCounter(Object o, int count)
public boolean deleteCounter(Object o)
public int readCounter(Object o)
public int incrementCounter(Object o)
public int decrementCounter(Object o)
```

As before, Counters are identified by an arbitrary object. All methods are designed to be used in rule conditions or actions.

`createCounter` can be called to create a new Counter associated with `identifier`. If argument `count` is not supplied then the value of the new Counter defaults to 0.

`createCounter` returns `true` if a new Counter was created and `false` if a Counter associated with `identifier` already exists. Note that the API is designed to ensure that race conditions between multiple threads trying to create a Counter from rule conditions can only have one winner.

`deleteCounter` can be called to delete any existing Counter associated with `identifier`. It returns `true` if the Counter was deleted and `false` if no Counter was associated with `identifier`. Note that the API is designed to ensure that race conditions

between multiple threads trying to delete a Counter from rule conditions can only have one winner.

`incrementCounter` can be called to increment the Counter associated with `identifier`. If no such Counter exists it will create one with value 0 before incrementing it. It returns the new value of the Counter.

`decrementCounter` can be called to decrement the Counter associated with `identifier`. If no such Counter exists it will create one with value 0 before decrementing it. It returns the new value of the Counter.

`readCounter` can be called to read the value of the Counter associated with `identifier`. If no such Counter exists it will create one with value 0.

Recursive Triggering

When a rule is triggered it executes the Java code in the event, condition and action and this may include calls to Helper methods or methods defined by the application under test or by the JVM runtime. If any of these methods match Byteman rules then this may result in a recursive entry to the rule execution engine. In some cases this may be desirable. However, in other cases this recursive entry may cause an infinite triggering chain and it is necessary to disable triggering while the rule executes. For example, the following rule will fail because of this problem:

```
RULE infinite triggering chain
CLASS java.io.FileOutputStream
METHOD open(String, int)
AT EXIT
BIND filename = $1
IF TRUE
DO traceLn("openlog", "Opened " + $1 + " for write")
ENDRULE
```

The problem is that on the first call to builtin method `traceLn(Object, String)` the default helper class attempts to open a trace file which it will then associate with key "openlog". In doing so it calls `FileOutputStream.open` and retriggers the rule.

One way round this is to specify a condition which will break the chain. The trace file will have a name of the form "traceNNN.txt" so the following version of the rule works as desired:

```
RULE infinite triggering chain broken using IF test
CLASS java.io.FileOutputStream
METHOD open(String, int)
AT EXIT
BIND filename = $1
IF !filename.matches("trace.*")
DO traceLn("openlog", "Opened " + $1 + " for write")
ENDRULE
```

With this version the rule is triggered recursively under the call to `traceLn` but the condition stops it being fired, breaking the recursion.

Of course in other cases it may not be so simple to come up with a condition which avoids recursive firing. So, the default helper provides the following method which allows triggering to be disabled or re-enabled while the rule is executing

```
public void setTriggering(boolean enabled)
```

If enabled is false then triggering is disabled during execution of subsequent expressions in the rule body. If it is true then triggering is re-enabled.

This can be used to implement the behaviour shown in the example above without the need to identify a suitable conditional

```
RULE infinite triggering chain broken using IF test
CLASS java.io.FileOutputStream
METHOD open(String, int)
AT EXIT
BIND filename = $1
IF TRUE
DO setTriggering(false),
   println("openlog", "Opened " + $1 + " for write")
ENDRULE
```

Note that once execution of the rule has completed triggering is automatically re-enabled so, in this case, there is no need to call `setTriggering(true)` at the end of the DO clause.

Trace and Debug Operations

Debugging

The rule engine provides a simple built-in debug method to support conditional display of messages during rule execution. The API defined by the helper class is

```
public boolean debug(String message)
```

`debug` prints the supplied message to `System.out`, prefixed with the name of the rule being executed. It always returns true, allowing debug messages to be used in conditions by ANDing them with other boolean expressions.

Generation of debug messages can be switched on by setting the following system property on the JVM command line:

```
org.jboss.byteman.debug
```

Tracing

The rule engine provides a set of built-in methods to support logging of trace messages during execution. Messages may be logged to `System.out`, `System.err` or to a named file. The API defined by the helper class is

```
public boolean traceOpen(Object identifier, String filename)
public boolean traceOpen(Object identifier)
public boolean traceClose(Object identifier)
public boolean trace(Object identifier, String message)
public boolean println(Object identifier, String message)
public boolean trace(String message)
public boolean println(String message)
```

`traceOpen` opens the file identified by `fileName` and associates it with `identifier`, returning true. `filename` can be either a relative or absolute path. Relative file names are located relative to the current working directory of the JVM. If there is already a file associated with `identifier` then `traceOpen` immediately returns false. If a file with the given name already exists it is opened in append mode. If `filename` is omitted then a

unique name is generated for the file which is guaranteed not to match any existing trace file in the current working directory.

`traceClose` closes the file associated with `identifier` and removes the association, returning `true`. If no open file is associated with `identifier` it returns `false`.

`trace` prints message to file associated with `identifier`, returning `true`. If no open file is associated with `identifier` then a file will be opened and associated with `identifier` as if a call to `trace` had been made with no file name supplied. If `identifier` is omitted then the output is written to `System.out`.

`println` prints message to file associated with `identifier` and appends a newline to the file, returning `true`. If no open file is associated with `identifier` then a file will be opened and associated with `identifier` as if a call to `trace` had been made with no file name supplied. If `identifier` is omitted then the output is written to `System.out`.

A caveat applies to the above descriptions for three special cases. If `identifier` is `null` or the string `"out"`, then `trace` and `println` write to `System.out`. If `identifier` is the string `"err"`, then `trace` and `println` write to `System.err`. `traceOpen` and `traceClose` always return `false` immediately if `identifier` has any of these values. Calls to `trace(message)` and `println(message)` which omit `identifier` are implemented by calling, respectively, `trace("out", message)` and `println("out", message)`.

Using Byteman

Downloading a binary release

The latest Byteman binary release is available from the Byteman project downloads page at

<http://www.jboss.org/byteman/downloads>

The page also contains a link to downloads for older binary release versions. Note that from Byteman 1.1 onwards the agent can only be run in JDK 6 or 7. Previous releases can also be run in JDK 5. The rest of this document assumes that environment variable `BYTEMAN_HOME` identifies the directory into which the binary release is unzipped.

Obtaining the sources

The latest Byteman sources are available from the Byteman project downloads page at

<http://www.jboss.org/byteman/downloads>

The page also contains a link to downloads for older source release versions.

Alternatively, sources may be checked out of the JBoss svn repository, where they are currently stored at

<http://anonsvn.jboss.org/repos/labs/labs/jbosstm/workspace/adinn/byteman/>

The source tree includes an `ext` directory containing the external javacup, JFlex and ObjectWeb asm jars needed by the agent and rule code.

Building Byteman from the sources

Byteman can be built by executing `ant` (or equivalently `ant install`) in the top level directory of the source tree. This installs the build products into directory `install`. The byteman jar is located in `install/lib/byteman.jar`. This jar contains the Java agent and rule engine code. This jar currently also bundles in the contents of the external Jflex, javacup runtime and ObjectWeb asm package libraries for ease of use. These could be unbundled so long as they are available in the classpath of the JVM being used to run the test application and the rule code.

Other useful targets include `'parser'` which rebuilds the javacup/JFlex parser from the grammar rules in `dd/grammar`. The source tree also contains a `bin` directory which contains an offline script parser and type checker, a program to install, uninstall and check the status of rules while the Java application is running and a program to run (see below for details)

The install tree contains several useful bash shell scripts in directory `install/bin`. These are documented in the following subsections. There are also some sample scripts and an associated helper jar located below directory `install/sample`.

Running Applications with Byteman

Using Byteman is refreshingly simple. It requires only extra argument when you run your Java application using the `java` command. This argument points the JVM at the agent code in the byteman jar and at the script files containing your byteman rules. This is specified using the `java` command flag

`-javaagent:agentlib=options`

This is a standard option for JDK 1.6 and upwards.

agentlib is a path to the byteman jar. The build process inserts a metadata file in the jar which allows the JVM to identify the agent program entry point so everything else is shrink-wrapped.

options is a comma-separated sequence of options which are passed to the agent.

For example, setting

```
export JAVA_OPTS="-javaagent:$BYTEMAN_HOME/lib/byteman.jar=
script:$SCRIPT_HOME/HeuristicSaveAndRecover.txt,
script:$SCRIPT_HOME/JBossTSTrace.txt"
```

will cause the JVM to pick up the byteman jar file from the install root, BYTEMAN_HOME and inject all rules found in the two scripts HeuristicSaveAndRecover and JBossTSTrace.txt located in directory SCRIPT_HOME. (n.b. the command should actually be all on one line without any line breaks – these have been inserted merely as an aid to readability)

Normally, the script option is all that is required. However there are several other options provided to configure more sophisticated features of the agent such as dynamic rule upload. The `bmjava.sh` command script (see below) can be used to simplify the task of concatenating these options into a valid `-javaagent` argument.

Available -javaagent Options

Each option comprises a keyword prefix, identifying the type of the option, and a suffix, identifying the value of the option. Prefix and suffix are separated by a colon, `:`. Multiple options are separated by commas. Valid options include

script:scriptfile where *scriptfile* is a path to a file containing Byteman rules. This option causes the agent to read the rules in *scriptfile* and apply them to subsequently loaded classes. Multiple `script` arguments may be provided to ensure that more than one rule set is installed. It is possible to start the agent with no initial script arguments but this only makes sense if the `listener` option is supplied with value `true`.

listener:boolean where *boolean* is either `true` or `false`. This option causes the agent to start a listener thread at startup. The listener can be talked to using the `submit` script, either to provide listings of rule applications performed by the agent or to dynamically load, reload or unload rules. Loading or reloading of a rule causes any matching classes which have already been loaded into the JVM to be retransformed, inserting a trigger call for the newly loaded rules into their target methods. Unloading a rule causes trigger code to be removed from any matching classes.

port:portnum where *portnum* is a positive whole number. This option selects the port used by the agent listener when opening a server socket to listen on. If not supplied the port defaults to 9091. Supplying this option defaults the `listener` option to `true`.

address:host where *host* is a host name. This option selects the address used by the agent listener when opening a server socket to listen on. If not supplied the address defaults to 9091. Supplying this option defaults the `listener` option to `true`.

sys:jarfile where *jarfile* is a path to a jar file to be added to the JVM system class path. This option makes classes contained in the jar file available for use when type checking, compiling and executing rule conditions and actions. It provides a useful way to

ensure that Helper classes mentioned in rules are able to be resolved. If a rule's trigger class is loaded by some other class loader this loader will normally have the system loader as a parent so references to the Helper class should resolve correctly.

boot:jarfile where *jarfile* is a path to a jar file to be added to the JVM *bootstrap* class path. This option provides a similar facility to the *sys* option but it ensures that the classes contained in the *jar* file are loaded by the bootstrap class loader. This is only significant when rules try to inject code into JVM classes which are loaded by the bootstrap class loader (which is a parent of the system loader).

Note that when injecting into JVM classes it is necessary to install the byteman jar into the boot classpath by passing option `boot:${BYTEMAN_HOME}/lib/byteman.jar`. Without it compilation of the transformed class will fail because it cannot locate classes `Rule`, `ExecuteException`, `ThrowException` and `ReturnException`. Script `bmjava.sh` automatically take care of this requirement.

Running Byteman Using Script `bmjava.sh`

The installed `bin` directory contains a script `bmjava.sh` which can be used to assemble the options passed to the byteman agent and combine them with other java options supplied on the `java` command line. The command line syntax for this script is

```
bmjava.sh [-p port] [-h host] \  
          [-l script|-b jar|-s jar|-nb|-nl|-nj]* [--] javaargs
```

where terms between `[]` are optional, terms separated by `|` are alternatives, `*` means zero or more repetitions and

- l *script* means load the rules in file *script* during program start up
- b *jar* means add jar file *jar* to the bootstrap class path
- s *jar* means add jar file *jar* to the system class path
- p *port* means use *port* as the port when opening the listener socket (the default is 9091)
- h *host* means use *host* as the host name when opening the listener socket (the default is localhost)
- nb means don't add the byteman jar to the bootstrap class path (it is added by default)
- nl means don't start the agent listener (it is started by default)
- nj means don't inject into java.lang classes (this is allowed by default)

Note that `bmjava.sh` expects to find the byteman agent jar to in directory `$BYTEMAN_HOME/lib/byteman.jar`. If `BYTEMAN_HOME` is not set it looks for a `lib` directory in the parent of the directory from which it is run.

Submitting Rules Dynamically Using Script `submit.sh`

The byteman jar includes a class `org.jboss.byteman.agent.submit.Submit`. This class provides a main routine which communicates with the listener class started up when option `listener:true` is passed to the agent. It can be invoked via bash shell script `submit.sh` located in the `bin` directory of the release source tree. This script expects to find the byteman agent jar to be located in `$BYTEMAN_HOME/lib/byteman.jar`. If `BYTEMAN_HOME` is not set it looks for a `lib` directory in the parent of the directory from

which it is run.

The command line syntax for the submit script is:

```
submit [-p port] [-h host] [-l|-u] [script1 . . . scriptN]
submit [-p port] [-h host] [-b|-s] jarfile1 . . .
```

Flags -p and -h can be used to supply the port and host address used to connect to the Byteman agent listener. If not supplied they default to 9091 and localhost, respectively.

Flag -l selects the default execution mode for submit. If no other flag is supplied this mode will be used. When run with no arguments submit lists all currently applied transformations. This listing includes details of failed transformations, typechecks and compiles.

When run with a list of script files submit uploads the scripts to the agent:

1. If any of the uploaded rules have the same name as an existing rule then the old rule is replaced with the new rule and all classes transformed by the rule are automatically retransformed. This includes the case where a target class was transformed but a subsequent typecheck or compile of the rule failed. This will (eventually) cause all threads executing target methods to trigger the new rule instead of the old rule. Depending upon when the compiler installs the new method code and when executing threads switch to this new code there may be a small window following the upload where neither the old nor the new rule is triggered.
2. If any of the uploaded rules apply to already loaded classes which were not previously successfully transformed (because no rule applied to them or because attempts to transform them failed) then those classes will be retransformed. Once again, depending upon when the compiler installs the new method code and when executing threads switch to this new code there may be a small window following the upload where neither the old nor the new rule is triggered
3. Any other rules will be stored in the agents rule set and applied to newly loaded classes which match the rule.

Flag -u selects the uninstall mode for submit. When run with no arguments submit uninstalls *all* currently loaded rules. When run with a list of script files submit uninstalls each installed rule whose name matches a rule definition contained in one of the supplied script files. submit does not check that rules in the supplied scripts are well formed, it merely looks for lines starting with the text RULE.

Flags -b and -s request installation of jar files into the bootstrap or system classpath, respectively. This is useful if rules which are to be submitted dynamically need to be provided with access to helper classes which were not in the original class path. There is no undo operation for this mode; jar files cannot be uninstalled once they have been installed. Also, it is not possible to use this option to install the byteman jar into the bootstrap classpath if it was omitted at agent startup. By the time the listener responds to this request the system class loader will already have loaded classes from the byteman jar so adding the jar to the bootstrap classpath will result in classloader conflicts.

n.b. Due to a bug in Sun's JDK 6 and 7 and in OpenJDK 6 and 7 errors may occur when installing a script in case 2 above (where an uploaded rule is applied to an already loaded class which has not yet been transformed). Scripts which employ references to local variables or method parameters by name will fail to compile. These JDKs retain the original bytecode for classes which are successfully transformed. However, where classes are not transformed the bytecode is discarded. When a retransform is requested the JVM's in-memory representation of the class (a C++ class instance) is used to reconstitute the

bytecode. Unfortunately the current reconstitute code does not recreate the local variable tables which were in the originally loaded bytecode. There is an OpenJDK bugzilla (#100100) and fix for this problem but the fix has not yet been incorporated into a release.

Checking Rules Offline Using Script `bytemancheck.sh`

The byteman jar includes a class which exposes a rule parser and type checker. This can be run offline before testing an application to check that rules are valid. It can be driven using a bash shell script `bytemancheck.sh` located in the `bin` directory of the release source tree. This script expects to find the byteman agent jar to be located in `$BYTEMAN_HOME/lib/byteman.jar`. If `BYTEMAN_HOME` is not set it looks for a `lib` directory in the parent of the directory from which it is run. It needs to be supplied with a classpath locating any application classes mentioned in the rules.

The command line syntax for the submit script is:

```
bytemancheck [-cp classpath] [script1 . . . scriptN]
```

Flag `-cp` provides a classpath used to locate classes mentioned in the scripts.

Environment Settings

The agent is sensitive to various environment settings which configure its behaviour.

If system property

`org.jboss.byteman.compileToBytecode`

is set (with *any* value) then the rule execution engine will compile rules to bytecode before executing them. If this property is unset it will execute rules by interpreting the rule parse tree.

Transformations performed by the agent can be observed by setting several environment variables which cause the transformed bytecode to be dumped to disk.

If system property

`org.jboss.byteman.dump.generated.classes`

is set the agent transformer code will dump a class file containing the bytecode of any class it has modified. The class file is dumped in a directory hierarchy derived from the package of the transformed class. So, for example, class `com.arjuna.Foo` will be dumped to file `com/arjuna/Foo.class`.

If system property

`org.jboss.byteman.dump.generated.classes.directory`

is set to the name of a directory writeable by the JVM then class files will be dumped in a package directory hierarchy below this directory. For example, if this property is set with value `/tmp/dump` then class `com.arjuna.Foo` will be dumped to file `/tmp/dump/com/arjuna/Foo.class`. If this property is unset or does not identify a writeable directory then class files will be dumped below the current working directory of the JVM.

If system property

`org.jboss.byteman.verbose`

is set then the rule execution engine will display a variety of trace messages to the `System.out` as it parses, typechecks, compiles and executes rules.

Note that the debug built-in is sensitive to this system property as well as to its own configuration switch

org.jboss.byteman.debug

If either of these properties is set then debug calls will print to `System.out`.

If system property

org.jboss.byteman.quodlibet

is set then the agent will allow rules to be injected into methods of classes in the `java.lang` hierarchy. Note that this will require the Byteman jar to be installed in the bootstrap classpath using the `boot:` option to the `-javaagent` JVM command line argument.

If system property

org.jboss.byteman.skip.overriding.rules

is set then the agent will not perform injection into overriding method implementations. If an overriding rule is installed the agent will print a warning to `System.err` and treat the rule as if it applies only to the class named in the `CLASS` clause. This setting is not actually provided to allow rules to be misused in this way. It is a performance tuning option. The agent has to check every class as it is loaded in order to see if there are rules which apply to it. It also has to check all loaded classes when rules are dynamically loaded via the agent listener. This requires traversing the superclass chain to locate overriding rules attached to superclasses. This increases the cost of running the agent (testig indicates that the cost goes from *negligible* (<< 1%) to, at worst, *noticeable* (~ 2%) but **not** to *significant*) So, if you do not intend to use overriding rules then setting this property helps to minimise the extent to which the agent perturbs the timing of application runs. This is particularly important when testing multi-threaded applications where timing is highly significant.