



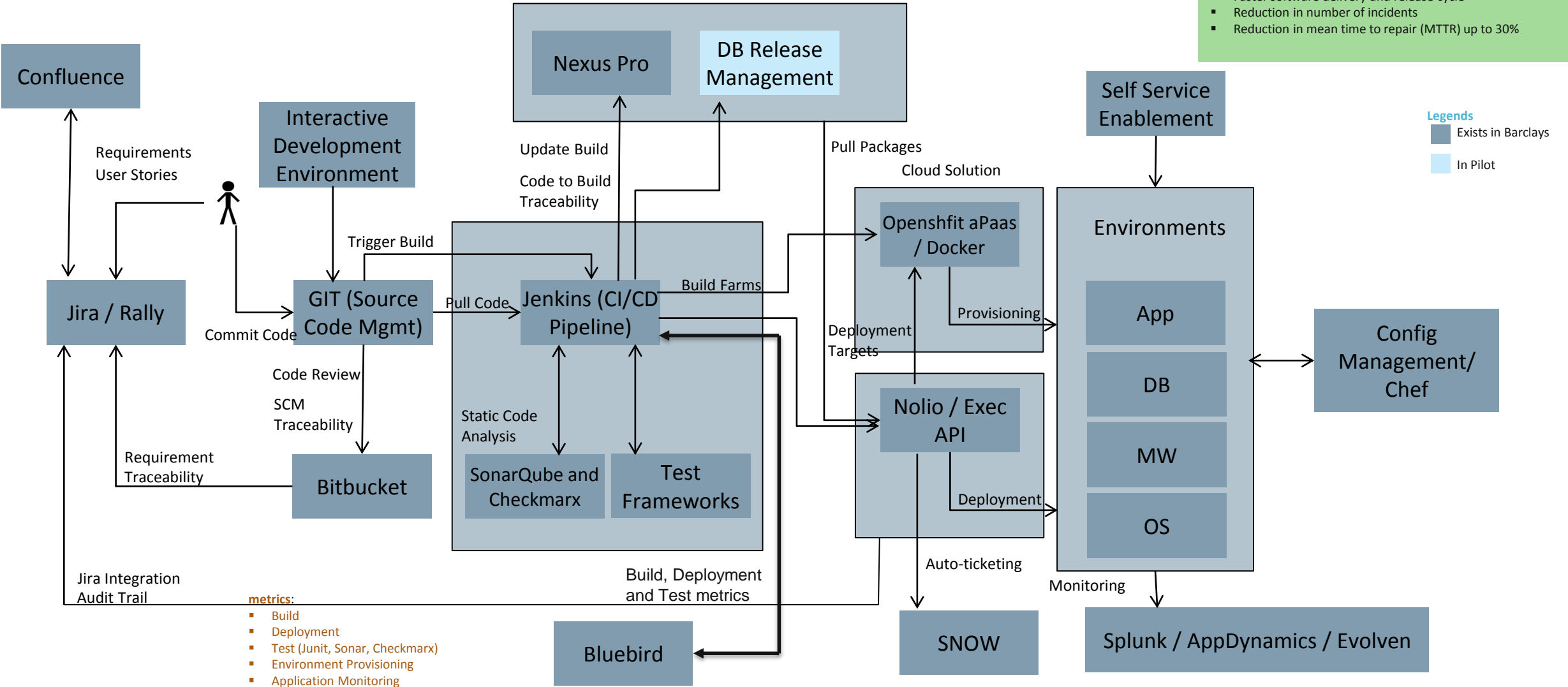
Cognizant

09 July 2018

Barclays DevOps – DB Deployment

Dilip Kumar

DevOps Solution Architecture



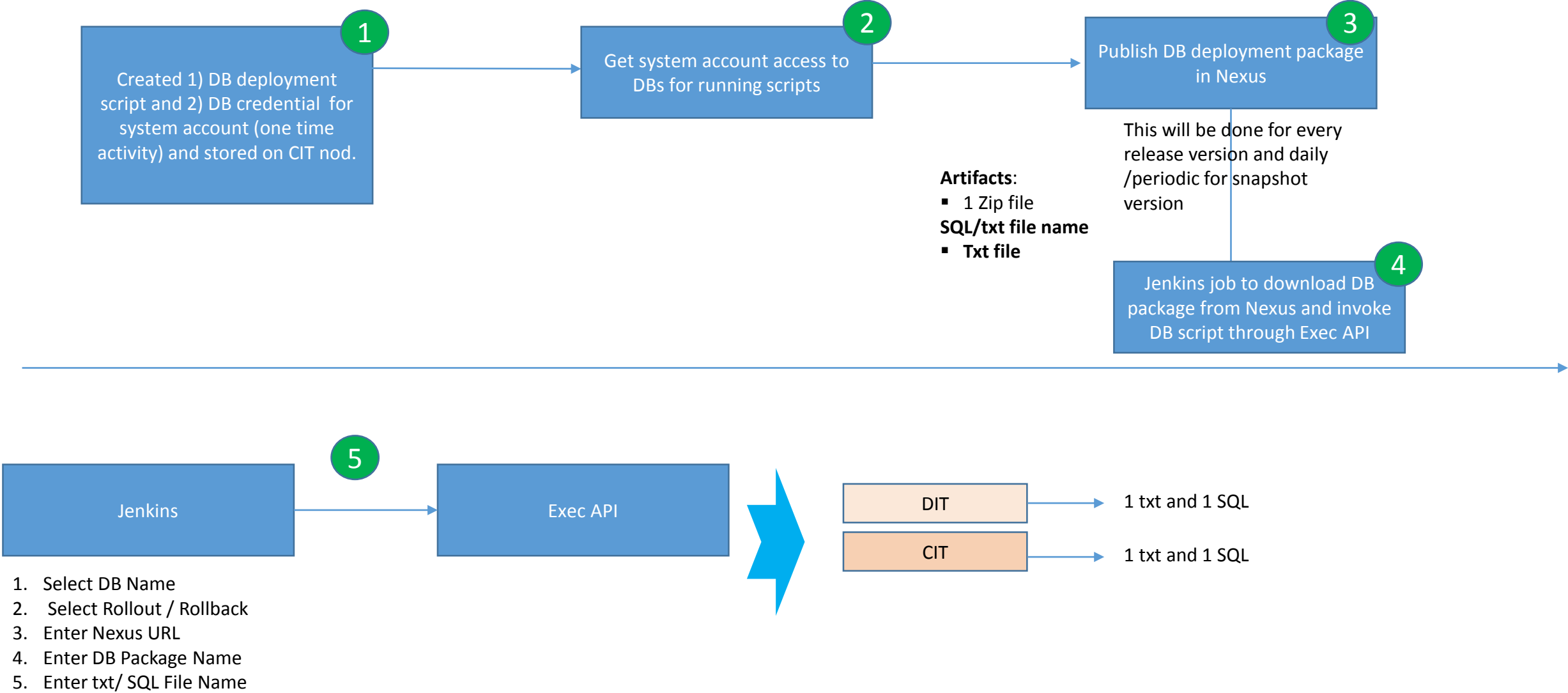
DB Deployment using Execution API

- Execution API has been rolled out to iPortal CIPE for application and properties files deployment across all environments (CIT, SIT, NFT, PROD, FOF, DR)
- Execution API agents have been installed and configured on all environments and configured for application deployment and utilities (cluster stop/start, service stop/ start, JVM stop/ start etc.)
- For DB deployment – we did pilot leveraging Execution API on DIT DB using sqlplus for connecting to DB server
- Post pilot on DIT DB, we extended this on 5 DBs of CIT environment and have tested DB deployment successfully

Tools Requirements:

- Jenkins
- Bitbucket
- Nexus
- Execution API
- SQL PLUS on App server / DB server

DB Deployment using Execution API - workflow



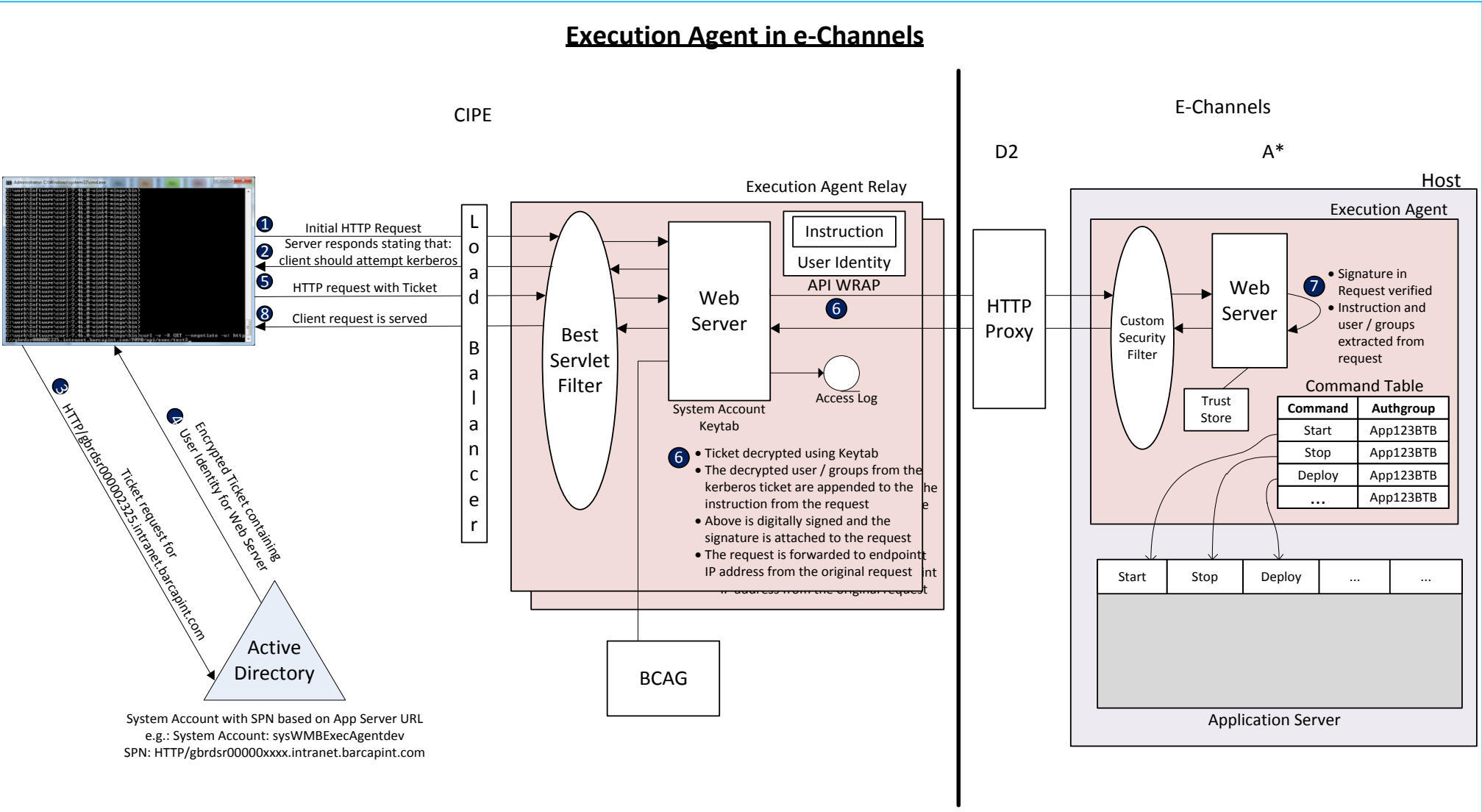
Execution API Technical Overview

- Execution API is getting rebranded to Multi-platform API (mAPI).
- The mAPI is a set of executable files and scripts aimed at providing self-service capability to project-based teams from Build the Bank and Run the Bank areas. The nature of the tools modular enabling the tool set to be deployed to multiple platform types. More scope is expected as the tool is developed, but currently in scope platforms are:
 - Legacy Middleware supported platforms - i.e. Application Hosting tools (e.g. WAS, JBoss & Tomcat) and MQ on internally hosted Linux systems
- Using the executables and scripts, known as wrapper scripts, there are distinct functions available via whitelisted commands. These enable integration with tools, such as Jenkins, to allow project teams to go seamlessly from code development to application deployment, maintain applications installed on target servers and retrieve logs. Enabling that DevOps way of working.
- DevOps teams can:
 - Execute predefined remote commands on restricted/privileged environments. For example, deploy an application, stop/start an environment, etc.
 - Securely transfer a file from a source location, specified by a URL, to a restricted/privileged destination path on a target server.
 - Allow the retrieval of files from restricted/privileged destination paths.
 - This is done by exposing a REST endpoint protected by BEST, which uses an Apache HTTP client to perform the file transfer. All activity can be finely access controlled through the use of AD groups
- Through the use of native shell script wrappers for Middleware target client technologies, we are able to allow execution of Middleware approved Whitelist Commands as privileged users on the target servers. These scripts are designed to be called through multiple technologies providing a single point of maintenance for client execution.
- There are encapsulated technology-specific scripts have been created to allow Middleware approved functionality from a single entry point.

The Execution API is implemented using the following Java components:

Product	Supplier	Function
Jetty	eclipse.org	Web server / servlet container
Jersey	glassfish.org	RESTful Web Services framework
Best	Barclays	Kerberos authentication / SSO
vsj	Vintela	Kerberos implementation; dependency of Best
Best-filter	Barclays	Kerberos authentication / SSO
commons-logging	apache.org	Logging
commons-codec	apache.org	Base64 / Hex encoding / decoding
slf4j	slf4j.org	Logging
log4j	apache.org	Logging
gson	google.com	Serialise / deserialise Java objects to JSON
jopt-simple		Command line parsing
http-client	apache.org	File transfer
chp-client	Cryptomathic	Digital signing
jminix		JMX console
QuartzScheduler	quartz-scheduler.org	Job scheduling

Execution API Architecture



Benefits

- Reduce dependencies on DB SME for DB deployment
- Single source of trigger through Jenkins
- Complete audit trail and log output
- Different access level (Developer, Run only, Read only) in Jenkins
- This can be part of large orchestration for release and reduce human error



Q& A

KEEP CHALLENGING™

Dilip Kumar
Dilip.kumar4@cognizant.com