IBM UrbanCode Cloud Services Security

IBM® UrbanCode Cloud Services Security
Version 4.0
Revised 2/7/2017

Before you use this information and the product it supports, read the information in "Notices" on page 10.

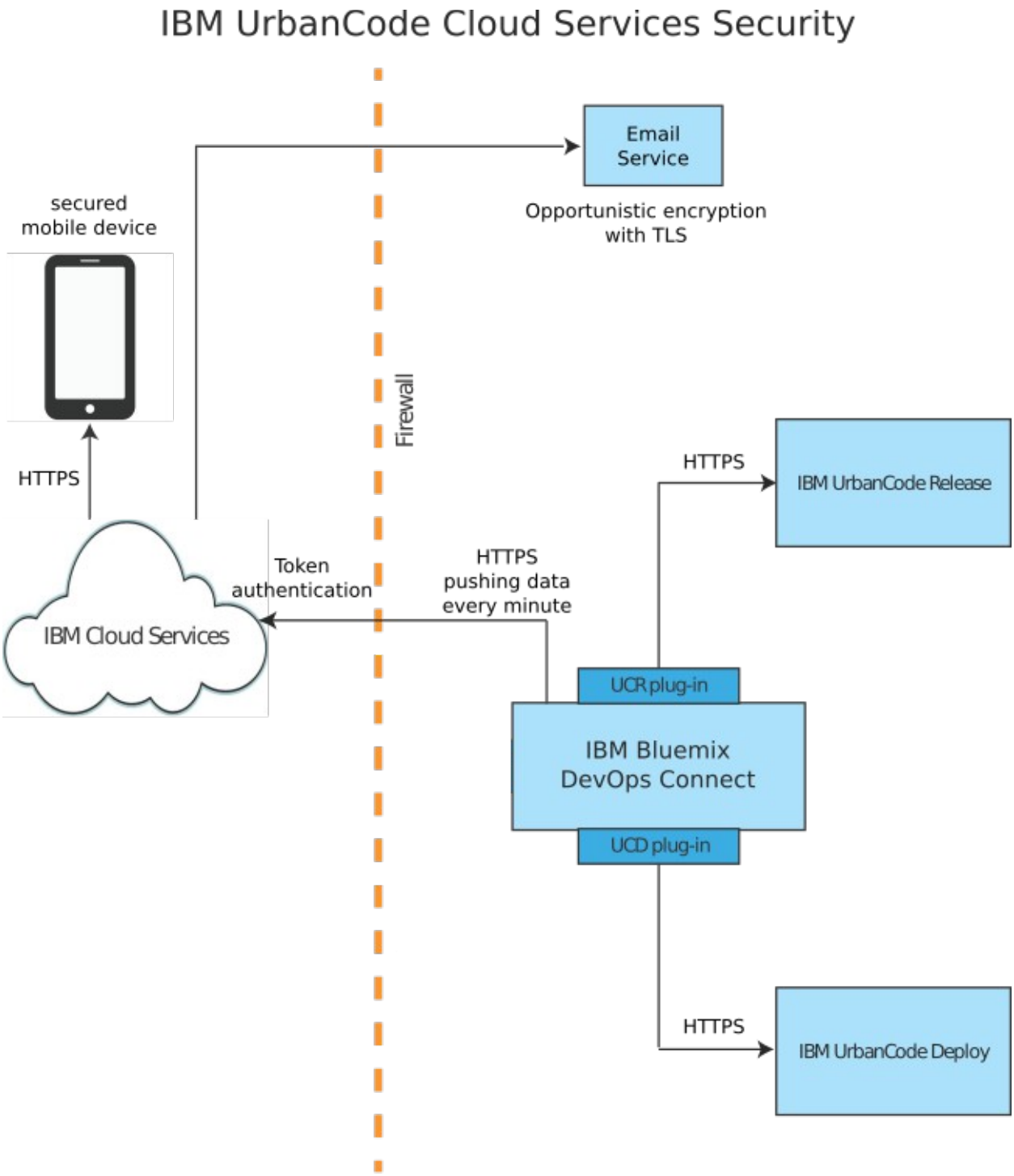
Contents

Overview of IBM Cloud Services architecture

The IBM® UrbanCode™ cloud service architecture consists of several parts:

- **On-premises**. Customers typically install IBM UrbanCode Release and IBM UrbanCode Deploy in their data center, and then often authenticate users through their LDAP system. To make data available to the cloud services, another utility, IBM Bluemix DevOps Connect, is installed in the customer's data center to broker communication between the IBM UrbanCode Release and IBM UrbanCode Deploy servers and the cloud services to which mobile devices and other external services connect.
- **Cloud Services**. An IBM-maintained set of cloud services that receives data from the IBM Bluemix DevOps Connect utility and provides data to other services by using REST APIs and push notifications.
- **Mobile devices**. Users receive deployment data and approval requests on their secured iOS 9 compatible devices.

The following figure illustrates the architecture.



On-premise security

IBM UrbanCode Release and IBM UrbanCode Deploy provide REST APIs that enable external systems to integrate with them. Administrators for those products authorize integrations and configure user access by issuing authorization tokens. Instead of requiring that customers provide access through their firewall, IBM provides a synchronization utility, IBM Bluemix DevOps Connect, that pushes data to an IBM-maintained cloud-hosted service where mobile devices connect. Data access for mobile devices continues to be controlled by the access controls that are provided in the IBM UrbanCode Release and IBM UrbanCode Deploy products. No additional administration is required.

What data is exchanged with IBM Cloud Services?

For integration with the mobile app, the following data elements are collected from IBM UrbanCode Release and IBM UrbanCode Deploy and then synchronized to the cloud service.

- Release summary statistics
- Release task names
- Task start times and estimates
- Approval names, descriptions, and assignees
- Task and approval assignees (display names and email addresses)
- Access control data: release and deployment teams and roles that are associated with users as designated by their email addresses

No personally identifiable information (PII), artifacts, or passwords are transmitted.

IBM Bluemix DevOps Connect authenticates itself with IBM UrbanCode Release and IBM UrbanCode Deploy with tokens that the administrators of those products issue. Customer-side certificates encrypt the tokens. DevOps Connect then transmits this data by HTTPS to a secure cloud service that IBM maintains.

The cloud service does not provide read access to any of this data to any client without identifying the requesting user and determining whether the user is permitted to access this data. The authentication and authorization mechanism is described in greater detail in *Cloud services security* later in this document.

Registration of IBM Bluemix DevOps Connect

Upon installing IBM Bluemix DevOps Connect, an administrator registers the installation with his or her IBM ID. During the registration process, DevOps Connect generates a 128-bit universally unique identifier (UUID) that identifies the DevOps Connect installation and receives a randomly generated 64-byte token from the cloud services that is Base64 encoded. The ID and token form the DevOps Connect credentials. The credentials are never displayed to users and are always transmitted by HTTPS.

Protocol

All further communication between the customer's network and cloud services are outbound HTTPS connections from the IBM Bluemix DevOps Connect utility, which are authenticated by cloud services by the unique ID and token transmitted in the HTTP header. Tokens never expire.

DevOps Connect periodically uses POST methods to send recently changed data from IBM UrbanCode Release and IBM UrbanCode Deploy to the cloud as described earlier. It also opens an outbound HTTPS web socket connection so that approvals and task status updates from mobile users can be relayed to IBM UrbanCode Release and IBM UrbanCode Deploy.

Cloud service security

Cloud services refer to IBM-maintained cloud-hosted REST API services. All communications to and from the cloud services is via HTTPS, and all data at rest is also encrypted. The email service uses opportunistic encryption with Transport Layer Security (TLS).

Security source scans and dynamic scans are routinely performed on the cloud services code base and running systems.

Mobile device security

When integrations run, eligible first-time users receive email invitations to download and register the UrbanCode Release and Deploy mobile application. The email contains a link where users can download the app from the Apple App Store. The invitation contains a unique access code to register their mobile application. The one-use access code expires after five days.

How trust is established

Trust is established when users register. When users register, their device IDs are sent to the IBM cloud service, and unique tokens are returned. These tokens are stored securely in the devices' keychains.

Subsequent communications with IBM Cloud Services use the secure token to identify the device. All communications to the mobile API, including registration, are under SSL. Read-only actions are authenticated by means of the device token. Actions which involve a write action, such as approving deployment requests or recording that a user is starting or completing a manual deployment activity, require that the user authenticate by using the device's passcode or a thumb-print.

How mobile access is restricted to authorized users

Mobile user access is controlled through IBM UrbanCode Release and IBM UrbanCode Deploy. The UrbanCode Release and Deploy mobile app uses the product's team- and role-based security system to determine user eligibility.

For IBM UrbanCode Release, users on teams with deployments for phases selected by the DevOps Connect administrator are eligible to receive deployment data. For IBM UrbanCode Deploy, users on teams with deployments receive deployment data. Users only receive data for deployments that their team or teams own.

When a user is removed from teams, they stop receiving team data starting the next time data is synced with the cloud service. When users are removed from LDAP or other backend authentication systems, their user accounts are not closed until they are explicitly disabled in IBM UrbanCode Deploy or IBM UrbanCode Release.

How approvals and task activates are secured

1. Approval requests and tasks are sent to the cloud along with the owning team and role.
1. Eligible users receive approval and task notifications in their app's inbox. Users are eligible if they registered their secured device, and they are in the expected role for the owning team.
2. Users must have a device passcode or touch ID enabled to authenticate any approval response from the mobile app.
3. Cloud services send approvals and task activities and user credentials to the on-premises products.

Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785 US

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions; therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

The performance data and examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM’s future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Trademarks