Know which authentication methods to use for your hybrid cloud

How IBM Cloud users are managed in hybrid environments

Martin Smolny
Michael Beck

December 12, 2017
(First published July 06, 2017)

The different options within IBM Cloud bear diverse requirements to the authentication of users. This article explains the various possibilities on how IBM Cloud users are managed and authenticated. We focus on developers, administrators, or operators that need to log in to the IBM Cloud platform to develop and maintain their applications. Applications that run on top of IBM Cloud can use any authentication method that is appropriate for the application’s purpose.

Editor’s note: Bluemix is now IBM Cloud. All the Bluemix products, services, support, and more will continue being offered with no changes. Find out more.

Introduction

The different options within IBM Cloud bear diverse requirements to the authentication of users. This article explains the various possibilities on how IBM Cloud users are managed and authenticated. If you are using a dedicated or local cloud, then this article is for you.

Types of IBM Cloud environments

Before we cover the different authentication methods, know which environment best suits your application. There are two deployment methods that are available in IBM Cloud:

1. IBM Cloud Public provides more than 130 unique services, including offerings like Weather.com, and millions of running applications, containers, servers, and more. Developers can start running their applications on IBM Cloud right away.
2. **IBM Cloud Dedicated** provides enterprises with their own cloud environment with physically isolated hardware in a data center. A single tenant and provisioned on a combination of bare metal and virtual machines, this IBM Cloud environment is created for a single customer.

These different methods within IBM Cloud bear diverse requirements to the management of users. We explain the various possibilities on how you can manage and authenticate users.

**Supported authentication methods**

**IBMid**

**Availability:** Public and Dedicated

An IBMid provides access to several IBM applications, service trials, communities, support, online purchasing, and more. An IBMid is managed by the owner of the IBMid and its properties, including profile information and password, both of which are stored on IBM servers. Password management (changing a password or retrieving a new password if the old one is forgotten) is done through IBM pages. The password policy for IBMids must follow certain restrictions, which are described [here](#).

**IBMid with SAML federation**

**Availability:** Public and Dedicated

IBMid also provides support for IBM customers and partners to incorporate IBMid authentication to their organizations’ SAML identity provider through IBMid federation. This support allows an organization’s SAML identity provider to handle all of the users who are leveraging IBM web applications and cloud services. The organization handles all password-related tasks and the authentication of its users. With IBMid federation, a company can use its own login page and security controls to secure access to IBM Cloud apps or IBM services.

For details on IBMid federation, the prerequisites, and the adoption process, refer to the [IBMid Enterprise Federation Adoption Guide](#).

**Clients and authentication methods**

**Authentication for the browser-based IBM Cloud client**

The IBM Cloud console is a browser-based application. For authenticating a user in IBM Cloud, the OAuth 2.0 protocol is used. This means that the IBM Cloud Authentication component issues an OAuth 2.0 token containing the user’s identity to the IBM Cloud Console—dependent on the selected authentication method.

More on OAuth 2.0

Check out our wildly popular series, “OAuth 2.0 clients in Java programming.”
Figure 1. General authentication flow for the browser-based IBM Cloud client

In case of IBMid or IBMid with SAML federation, the IBM Cloud authentication component redirects the user's browser to another server and retrieves the identity of the user from the response of that server.

Authentication for command line and native applications

Widely known native applications that leverage IBM Cloud authentication are:

- **IBM Cloud and Cloud Foundry Command Line Interface**: This tool helps you to automate repeated tasks like starting, stopping, updating, and deleting applications.
- **IBM Eclipse Tools for IBM Cloud**: This tool allows for interaction with an IBM Cloud instance from any Eclipse-based tooling.

All applications, including the above, are not based on a browser interaction to authenticate to IBM Cloud and share these common characteristics:

- Prompting for credentials: These applications show an own dialog to enter the user name and password. Be aware that you have to trust the source of your application, as you are providing your credentials. A malware version of this application can capture your credentials.
- Authentication validation: These applications send the user name and password directly to the IBM Cloud authentication component with the OAuth 2.0 “password grant” method.

The IBM Cloud authentication component will send the user name and password to the back-end authentication server, if possible. This works for IBMid without federation, but not for IBMid with SAML federation. The underlying authentication protocol does not support a compatible authentication mechanism.

To allow those clients to authenticate with IBM Cloud (and with those configurations), you can use your web browser to get a “one-time passcode” to log in with those applications. This login
requires support for this interaction type by the native application. The following flow diagram shows the sequence to successfully log in for those environments:

**Figure 2. Authentication flow with one-time password**

![Authentication flow diagram]

**Summary**

To summarize, we provide characteristics for each of the four different authentication methods in one table.

**Table 1. Characteristics of the different authentication methods**

<table>
<thead>
<tr>
<th></th>
<th>IBMid</th>
<th>IBMid with federated users</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Availability</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IBM Cloud Public</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>IBM Cloud Dedicated</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td><strong>Password management and policy</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IBM</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Customer</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td><strong>Application types supported</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Browser-based</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>CLI/native with credentials</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>CLI/native with one-time passcode</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>Enabled for customer-provided two-factor authentication</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td><strong>Authentication to IBM Cloud Public without re-login</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
Appendix

Required information for IBMid/IBMid with federated users

IBMid is active in IBM Cloud Public by default and is automatically used for IBM Cloud Dedicated without providing any further details.

Customers who want to federate their SAML Identity Provider with IBMid need to follow this process.

The steps in the federation process are independent of the configuration of the Dedicated or Local instance and can be executed before or after the IBM Cloud environment is configured for the customer.
Related topics

- Code pattern: Create a hybrid cloud with API Connect and Secure Gateway
- Try IBM Cloud for free
- Connect with IBM Cloud developers

© Copyright IBM Corporation 2017
Trademarks
(www.ibm.com/developerworks/ibm/trademarks/)