login state. If users are not logged in when they visit these pages, Yii will redirect them to the login page.

Rules are executed one by one, starting from the top, until one matches. If nothing matches, then the action is treated as allowed.

The next task is to limit access to specific IPs. In this case, the following two access rules are involved:

[

'allow' => true,

'actions' => ['ip'],

'ips' => ['127.0.0.1'],

],

The first rule allows access to the IP action from a list of IPs specified. In our case, we are using a loopback address, which always points to our own computer. Try changing it to 127.0.0.2, for example, to see how it works when the address does not match. The second rule denies everything, including all other IPs.

Next, we limit access to one specific user role, as follows:

[

'allow' => true,

'actions' => ['user'],

'roles' => [ User::ROLE\_ADMIN],

],

The preceding rule allows a user with a role equal to admin to run the user action. Therefore, if you log in as admin, it will let you in, but if you log in as demo, it will not.



We have overridden the standard AccessRule class on our own, which is located in the