windmill-labs / **windmill** Public

Code | Issues 533 | Pull requests 169 | Discussions | Actions | Projects

Commit c621a74

rubenfiszel committed on Jan 24 · ✓ 16 / 22

```
fix: tighten operator permissions
```

main · v1.687.0 ••• pr-assets

1 parent 05f5ef9 commit c621a74

4 files changed +45 -0 lines changed

Top

Filter files…

- backend/windmill-api/src
  - apps.rs
  - flows.rs
  - raw_apps.rs
  - scripts.rs

4 files changed +45 -0 lines changed

Search within code

backend/windmill-api/src/apps.rs

```
@@ -1042,6 +1042,11 @@ async fn create_app_raw<'a>(
1042 1042         Path(w_id): Path<String>,
1043 1043         multipart: Multipart,
1044 1044     ) -> Result<(StatusCode, String)> {
     1045 +     if authed.is_operator {
     1046 +         return Err(Error::NotAuthorized(
     1047 +             "Operators cannot create apps for security reasons".to_string(),
     1048 +         ));
     1049 +     }
```

```
1045  1050          let (path, _id) = process_app_multipart!(
1046  1051              authed,
1047  1052              user_db,
      @@ -1094,6 +1099,11 @@ async fn create_app(
1094  1099          Path(w_id): Path<String>,
1095  1100          Json(app): Json<CreateApp>,
1096  1101      ) -> Result<(StatusCode, String)> {
      1102  +     if authed.is_operator {
      1103  +         return Err(Error::NotAuthorized(
      1104  +             "Operators cannot create apps for security reasons".to_string(),
      1105  +         ));
      1106  +     }
1097  1107          let path = app.path.clone();
1098  1108          check_scopes(&authed, || format!("apps:write:{}", &path))?;
1099  1109
      @@ -1413,6 +1423,11 @@ async fn update_app(
1413  1423          Path((w_id, path)): Path<(String, StripPath)>,
1414  1424          Json(ns): Json<EditApp>,
1415  1425      ) -> Result<String> {
      1426  +     if authed.is_operator {
      1427  +         return Err(Error::NotAuthorized(
      1428  +             "Operators cannot update apps for security reasons".to_string(),
      1429  +         ));
      1430  +     }
1416  1431          // create_app_internal(authed, user_db, db, &w_id, &mut app).await?;
1417  1432          let path = path.to_path();
1418  1433          check_scopes(&authed, || format!("apps:write:{}", path))?;
      @@ -1441,6 +1456,11 @@ async fn update_app_raw<'a>(
1441  1456          Path((w_id, path)): Path<(String, StripPath)>,
1442  1457          multipart: Multipart,
1443  1458      ) -> Result<String> {
      1459  +     if authed.is_operator {
      1460  +         return Err(Error::NotAuthorized(
      1461  +             "Operators cannot update apps for security reasons".to_string(),
      1462  +         ));
      1463  +     }
1444  1464          let path = path.to_path();
```

```
1445  1465          check_scopes(&authed, || format!("apps:write:{}", path))?;
1446  1466          let opath = path.to_string();
```

backend/windmill-api/src/flows.rs

```
@@ -421,6 +421,11 @@ async fn create_flow(
421  421          Path(w_id): Path<String>,
422  422          Json(nf): Json<NewFlow>,
423  423      ) -> Result<(StatusCode, String)> {
     424  +       if authed.is_operator {
     425  +           return Err(Error::NotAuthorized(
     426  +               "Operators cannot create flows for security reasons".to_string(),
     427  +           ));
     428  +       }
424  429          check_scopes(&authed, || format!("flows:write:{}", nf.path))?;
425  430          validate_flow(&nf).await?;
426  431          if *CLOUD_HOSTED {
@@ -846,6 +851,11 @@ async fn update_flow(
846  851          Path((w_id, flow_path)): Path<(String, StripPath)>,
847  852          Json(nf): Json<NewFlow>,
848  853      ) -> Result<String> {
     854  +       if authed.is_operator {
     855  +           return Err(Error::NotAuthorized(
     856  +               "Operators cannot update flows for security reasons".to_string(),
     857  +           ));
     858  +       }
849  859          let flow_path = flow_path.to_path();
850  860          check_scopes(&authed, || format!("flows:write:{}", flow_path))?;
851  861          validate_flow(&nf).await?;
```

backend/windmill-api/src/raw_apps.rs

```
@@ -156,6 +156,11 @@ async fn create_app(
156  156          Path(w_id): Path<String>,
157  157          Json(app): Json<CreateApp>,
158  158      ) -> Result<(StatusCode, String)> {
     159  +       if authed.is_operator {
     160  +           return Err(Error::NotAuthorized(
```

```
      161 +             "Operators cannot create raw apps for security
          reasons".to_string(),
      162 +         ));
      163 +     }
159   164       check_scopes(&authed, || format!("raw_apps:write:{}", app.path))?;
160   165       if *CLOUD_HOSTED {
161   166           let nb_apps = sqlx::query_scalar!(
          @@ -272,6 +277,11 @@ async fn update_app(
272   277       Path((w_id, path)): Path<(String, StripPath)>,
273   278       Json(app): Json<EditApp>,
274   279   ) -> Result<String> {
      280 +     if authed.is_operator {
      281 +         return Err(Error::NotAuthorized(
      282 +             "Operators cannot update raw apps for security
          reasons".to_string(),
      283 +         ));
      284 +     }
275   285       use sql_builder::prelude::*;
276   286
277   287       let path = path.to_path();
```

backend/windmill-api/src/scripts.rs

```
          @@ -589,6 +589,11 @@ async fn create_script_internal<'c>(
589   589       Transaction<'c, Postgres>,
590   590       Option<HandleDeploymentMetadata>,
591   591   )> {
      592 +     if authed.is_operator {
      593 +         return Err(Error::NotAuthorized(
      594 +             "Operators cannot create scripts for security reasons".to_string(),
      595 +         ));
      596 +     }
592   597       check_scopes(&authed, || format!("scripts:write:{}", ns.path))?;
593   598
594   599       guard_script_from_debounce_data(&ns).await?;
```

Comments 0

Please sign in to comment.